

Конкурсное задание

КОМПЕТЕНЦИЯ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

Конкурсное задание включает в себя следующие
разделы:

1. Формы участия в конкурсе
2. Задание для конкурса



3. Модули задания и необходимое время
4. Критерии оценки
5. Необходимые приложения

Количество часов на выполнение задания: 15 ч.

1) ФОРМЫ УЧАСТИЯ В КОНКУРСЕ

Индивидуальный конкурс.

2) ЗАДАНИЕ ДЛЯ КОНКУРСА

Содержанием конкурсного задания являются работы по пусконаладке сетевой инфраструктуры на базе современного сетевого оборудования и операционных систем семейства Windows и Linux. Участники соревнований получают инструкцию, сетевые диаграммы и методические рекомендации по выполнению. Конкурсное задание имеет несколько модулей, выполняемых последовательно.

Задание национального финала является утвержденным. В нем присутствуют 3 из 5 модулей, т.е. возможно набрать максимально 45 из 100 баллов

Конкурс включает в себя “Пусконаладку инфраструктуры на основе ОС семейства Linux”; “Пусконаладку инфраструктуры на основе ОС семейства Windows”; “Пусконаладку телекоммуникационного оборудования”.

Окончательная методика проверки уточняются членами жюри. Оценка производится в отношении работы модулей. Если участник конкурса не выполняет требования техники безопасности, подвергает опасности себя или других конкурсантов, такой участник может быть отстранен от конкурса.

Время и детали конкурсного задания в зависимости от конкурсных условий могут быть изменены членами жюри, по согласованию с менеджером компетенции.

Конкурсное задание должно выполняться в формате “один модуль в день”, циклически по модулям А-В-С. Оценка каждого модуля происходит ежедневно.

Задания разработаны и протестированы группой сертифицированных экспертов:

Таблица 1 – Группа сертифицированных экспертов

Модуль конкурсного задания	Роль	ФИО Эксперта
Модуль А: «Пусконаладка инфраструктуры на основе ОС семейства Linux»	Ведущий разработчик	Лавров Данил Сергеевич
	Группа разработки	Груздев Семен Юрьевич
Модуль В: «Пусконаладка инфраструктуры на основе ОС семейства Windows»	Ведущий разработчик	Афанасьев Михаил Александрович
	Группа разработки	Лавров Данил Сергеевич
Модуль С: «Пусконаладка телекоммуникационного оборудования»	Ведущий разработчик	Лавров Данил Сергеевич
	Группа разработки	Груздев Семен Юрьевич

3. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время приведены в таблице 2.

Таблица 2 – Время выполнение модуля

№ п/п	Наименование модуля	Рабочее время	Время на задание
1	Модуль А: «Пусконаладка инфраструктуры на основе ОС семейства Linux»	В соответств ии с жеребьевк ой по циклу А-В-С	5 ч.
2	Модуль В: «Пусконаладка инфраструктуры на основе ОС семейства Windows»		5 ч.
3	Модуль С: «Пусконаладка телекоммуникационного оборудования»		5 ч.

ВВЕДЕНИЕ

Умение работать с системами на основе открытого исходного кода становится все более важным навыком для тех, кто желает построить успешную карьеру в ИТ. Данное конкурсное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем, в основном, интеграции и аутсорсинге. Если вы можете выполнить задание с высоким результатом, то вы точно сможете обслуживать информационную инфраструктуру большого предприятия.

ОПИСАНИЕ КОНКУРСНОГО ЗАДАНИЯ

Данное конкурсное задание разработано с использованием различных открытых технологий, с которыми вы должны быть знакомы по сертификационным курсам LPIC и Red Hat. Задания поделены на следующие секции:

- Базовая конфигурация
- Конфигурация сетевой инфраструктуры
- Службы централизованного управления и журналирования
- Конфигурация служб удаленного доступа
- Конфигурация веб-служб
- Конфигурация служб хранения данных
- Конфигурация параметров безопасности и служб аутентификации

Секции независимы друг от друга, но вместе они образуют достаточно сложную инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, динамическая маршрутизация должна выполняться поверх настроенного между организациями туннеля. Важно понимать, что если вам не удалось настроить полностью технологический стек, то это не означает, что работа не будет оценена. Например, для удаленного доступа необходимо настроить IPsec-туннель, внутри которого организовать GRE-туннель. Если, например, вам не удалось настроить IPsec, но вы смогли настроить GRE, то вы все еще получите баллы за организацию удаленного доступа.

ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА

В первую очередь необходимо прочитать задание полностью. Следует обратить внимание, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже. На вас возлагается ответственность за распределение своего рабочего времени. Не тратьте время, если у вас возникли проблемы с некоторыми заданиями. Вы можете использовать временные решения (если у вас есть зависимости в технологическом стеке) и продолжить выполнение других задач. Рекомендуется тщательно проверять результаты своей работы.

Доступ ко всем виртуальным машинам настроен по аккаунту root:toor.

Если Вам требуется установить пароль, (и он не указан в задании) используйте: “P@ssw0rd”.

Виртуальная машина ISP преднастроена. Управляющий доступ участника к данной виртуальной машине для выполнения задания не предусмотрен. При попытке его сброса возникнут проблемы.

Офис HeadQuater включает виртуальные машины: HQ-LinRTR, HQ-LinSRV1, HQ-LinSRV2, HQ-LinSRV3, HQ-CLI

Офис Branch включает виртуальные машины: BR-LinSRV, BR-CLI, BR-LinRTR

В качестве внешнего клиента выступает Remote-LinCLI.

НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

Ожидается, что конкурсное задание выполнимо Участником с привлечением оборудования и материалов, указанных в Инфраструктурном Листе.

В качестве серверной ОС используется Debian 10.8

В качестве клиентской ОС AstraLinux Orel 2.12.40

Участники не имеют права пользоваться любыми устройствами, за исключением находящихся на рабочих местах устройств, предоставленных организаторами.

Участники не имеют права приносить с собой на рабочее место заранее подготовленные текстовые материалы.

В итоге участники должны обеспечить наличие и функционирование в соответствии с заданием служб и ролей на указанных виртуальных машинах. При этом участники могут самостоятельно выбирать способ настройки того или иного компонента, используя предоставленные им ресурсы по своему усмотрению.

СХЕМА ОЦЕНКИ

Каждый субкритерий имеет приблизительно одинаковый вес. Пункты внутри каждого критерия имеют разный вес, в зависимости от сложности пункта и количества пунктов в субкритерии.

Схема оценка построена таким образом, чтобы каждый пункт оценивался только один раз. Например, в секции «Базовая конфигурация» предписывается настроить имена для всех устройств, однако этот пункт будет проверен только на одном устройстве и оценен только 1 раз. Одинаковые пункты могут быть проверены и оценены больше чем 1 раз, если для их выполнения применяются разные настройки или они выполняются на разных классах устройств.

Подробное описание методики проверки должно быть разработано экспертами, принимавшими участие в оценке конкурсного задания чемпионата, и вынесено в отдельный документ. Данный документ, как и схема оценки, является объектом внесения 30% изменений.

Базовая настройка

- 1) Настройте имена хостов в соответствии с **диаграммой**
- 2) Настройте IP-адресацию на ВСЕХ хостах в соответствии с **диаграммой**
- 3) Назначьте для всех хостов доменное имя **rea2021.lin**
- 4) **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**.
- 5) В случае корректной работы сервисов DNS, ответы от DNS сервера должны иметь более высокий приоритет.

Сделано: _____

Конфигурация сетевой инфраструктуры

- 1) На HQ-LinSRV1 настройте службу разрешения доменных имен для внутренней сети
 - a) Сервер должен обслуживать зону **rea2021.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 WireGuard VPN подсети, то запись должна разрешаться в 2.2.2.2
 - g) При обращении к зоне rea2021.ru запрос должен пересылаться на сервер ISP. При обращении к любой другой неизвестной зоне запрос должен пересылаться на адрес 8.8.8.8. Для проверки пересылки на rea2021.ru используйте test.rea2021.ru

Сделано: _____

```

acl "int" { 172.16.0.0/24; 192.168.0.0/24;};
view "int"{
    match-clients { "int"; };
    zone "rea2021.lin" {
        type master;
        file "/opt/dns/int";
        allow-update { any;};
    };
    zone "0.168.192.in-addr.arpa" {
        type master;
        file "/opt/dns/192";
        allow-update { any;};
    };
    zone "0.16.172.in-addr.arpa" {
        type master;
        file "/opt/dns/172";
    };
    zone "rea2021.ru" {
        type forward;
        forwarders { 10.10.10.2;};
    };
};
acl "vpn" { 10.8.8.0/24; };
view "vpn" {
    match-clients { "vpn"; };
    zone "rea2021.lin" {
        type master;
        file "/opt/dns/vpn";
        allow-update { any;};
    };
    zone "0.168.192.in-addr.arpa" {
        type master;
        file "/opt/dns./192";
        allow-update { any;};
    };
    zone "0.16.172.in-addr.arpa" {
        type master;
        file "/opt/dns/172";
    };
    zone "rea2021.ru" {
        type forward;
        forwarders { 10.10.10.2;};
    };
};
};

```

Пример конфига на BIND, про VPN делается по аналогии

- 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 rea2021.lin
- d) Сконфигурируйте опцию для выдачи адреса TFTP сервера. В качестве адреса TFTP сервера используйте адрес HQ-LinSRV1

Сделано: _____

```
#}
subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.100 192.168.0.200;
    option routers 192.160.0.1;
    option tftp-server-name "192.168.0.1";
}
# This declaration allows BOOTP clients to get dynamic
```

Вдруг ты отупел совсем, DHCP готовить вот так

Конфигурация служб мониторинга, резервного копирования, журналирования

1. На маршрутизаторе HQ-LinRTR настройте возможность удаленного мониторинга по протоколу SNMP v3.

apt install snmp snmpd

Далее в /etc/snmp/snmpd.conf

```
#agentAddress udp:127.0.0.1:161
# Listen for connections on all interfaces (both IPv4 and IPv6)
agentAddress udp:161,udp6:[::1]:161
rocommunity REASKILLZ
rouser snmpuser authPriv .1
```

- a. Задайте местоположение устройств “Udomlya, Russia”

в /var/lib/snmp/snmpd.conf

ОТКЛЮЧИ SNMP ЧЕРЕЗ СТОП! Создать пользкака, контакт и локацию

```
sysLocation Udomlya,Russia
sysContact admin@rea2021.lin
createUser snmpuser SHA "snmppass" AES snmppass_
```

```

1 #!/bin/bash
2 if [ "$1" = "-h" ] || [ "$1" = "--help" ]; then
3     echo "Its script for SNMP-checking";
4     echo "Usage: snmp_check (IP-ADDRESS) (USERNAME) (Password)"
5 else
6     if [ -z "$1" ] && [ -z "$2" ] && [ -z "$3" ];then
7         read -p "Enter hostname or IP address: " DEVICE
8         read -p "Enter the username for SNMP: " NAMEUSER
9         read -p "Enter password: " PASS
10        snmpwalk -v3 -l authPriv -u $NAMEUSER -a SHA -A $PASS -x AES -X $PASS $DEVICE
11 else
12     if [ -z "$1" ] || [ -z "$2" ] || [ -z "$3" ]; then
13         echo "Error! Need more args!"
14 else
15     DEVICE=$1
16     NAMEUSER=$2
17     PASS=$3
18     snmpwalk -v3 -l authPriv -u $NAMEUSER -a SHA -A $PASS -x AES -X $PASS $DEVICE
19 fi
20 fi
21 fi

```

- b. Задайте контакт admin@rea2021.lin
- c. Используйте имя группы “REASKILLZ”.
- d. Создайте профиль только для чтения с именем “REA”.
- 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.

Сделано: _____

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.rea2021.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 **R3ASK1LZ2021**

1) Сформируем БД на HQ-LinSRV1

- a) **apt install zabbix-server-pgsql** штука поставит постгрю и нужные шаблоны
- b) **apt --fix-broken install** - так как апт говно, он не все починил сам, надо ему помочь
- c) **apt install postgresql**
- d) создаем юзера - **sudo -u postgres createuser --pwprompt zabbix**
- e) **sudo -u postgres createdb -O zabbix -E Unicode -T template0 zabbix**
- f) **zcat /usr/share/doc/zabbix-server-pgsql/create.sql.gz | sudo -u zabbix psql**
zabbix - создали БД

- g) далее надо разрешить подключаться к этой БД внешним адресам. Идем в файл `/etc/postgresql/11/main/pg_hba.conf` и делаем вот так:

```
# Database administrative login by Unix domain socket
local    all             postgres                                peer

# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local    all             all                                     trust
# IPv4 local connections:
host     all             all             127.0.0.1/32            trust
host     all             all             192.168.0.20/32         trust
# IPv6 local connections:
host     all             all             ::1/128                 md5
```

- h) далее в `/etc/postgresql/11/main/postgresql.conf` прописываем, чтобы слушал наш адрес в сети

```
# - Connection Settings -

#listen_addresses = 'localhost'
listen_addresses = '192.168.0.10'           # what IP address(es) to listen on;
                                             # comma-separated list of addresses;
                                             # defaults to 'localhost'; use '*' for all
```

i)

С БД ВСЕ. Идем на Zabbix сервер.

Ставим сервер:

```
apt install zabbix-server-pgsql zabbix-frontend-php php7.3-pgsql
zabbix-apache-conf zabbix-agent
```

Далее в `vim /etc/zabbix/zabbix_server.conf` делаем вот так правим пароль от БД. Его мы ставим в процессе создания юзера zabbix

```
### Option: DBPassword
# Database password.
# Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=P@ssw0rd
```

Правим хост с БД

```
### Option: DBHost
#       Database host name.
#       If set to localhost, socket is used for My
#       If set to empty string, socket is used for
#
# Mandatory: no
# Default:
DBHost=192.168.0.10
```

Далее если все ок, то запускаем все службы одновременно

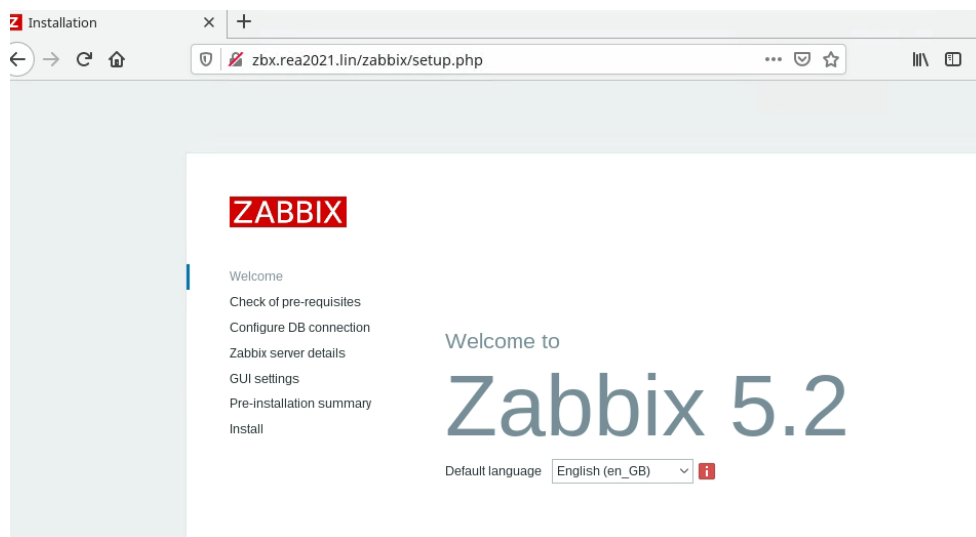
systemctl start zabbix-server zabbix-agent apache2 php7.3-pgsql

P.S> в /etc/zabbix/apache2.conf можно поправить время

```
<IfModule mod_php7.c>
    php_value max_execution_time 300
    php_value memory_limit 128M
    php_value post_max_size 16M
    php_value upload_max_filesize 2M
    php_value max_input_time 300
    php_value max_input_vars 10000
    php_value always_populate_raw_post_data -1
    php_value date.timezone US/Eastern
</IfModule>
/Directory>
```

логи у него в /var/log/zabbix иногда очень спасает команда **apt -f install** так как апт тупой и не все поставить может сразу

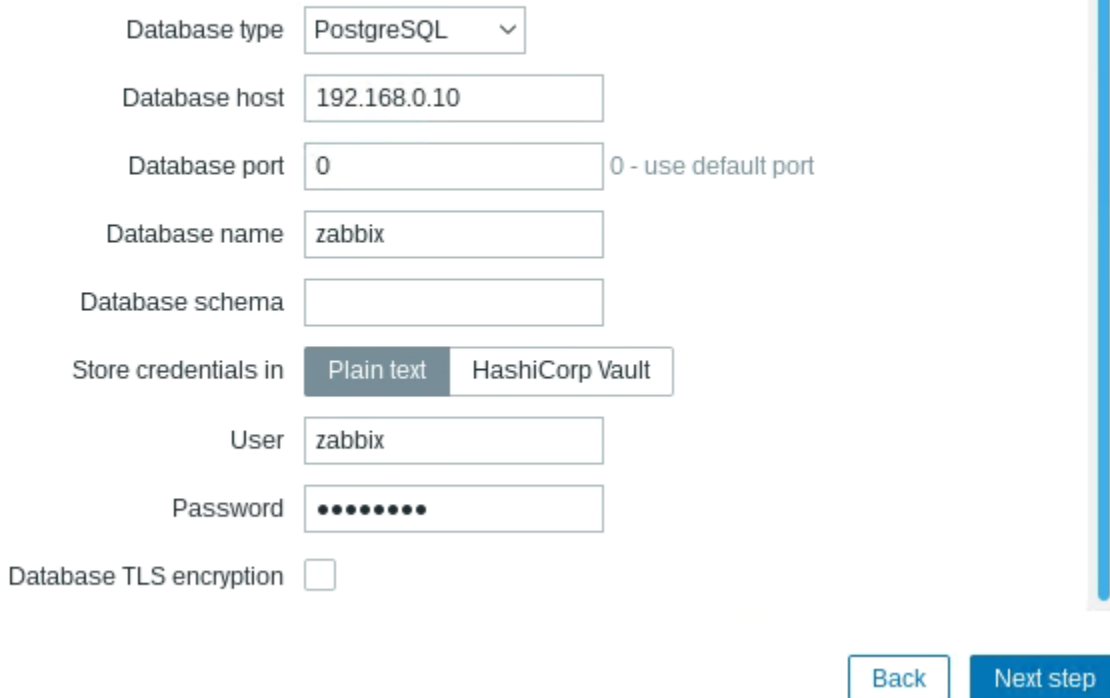
Если все ок, то проверкой будет с клиента зайти на его веб-сайт



По конфигурации заббикса

Configure DB connection

Please create database manually, and set the configuration parameters for connection to this database. Press "Next step" button when done.



Database type: PostgreSQL

Database host: 192.168.0.10

Database port: 0 (0 - use default port)

Database name: zabbix

Database schema:

Store credentials in: Plain text (selected), HashiCorp Vault

User: zabbix

Password: [masked]

Database TLS encryption: ☐

Back Next step

Прикручиваем сертификат к ZABBIX серты выпускать умеешь

a2enmod ssl

vim /etc/apache2/apache2.conf

```
<VirtualHost *:443>
  ServerName zbx.rea2021.lin
  SSLEngine on
  SSLCertificateFile /opt/certs/zbx.pem
  SSLCertificateKeyFile /opt/certs/zbx.key
</VirtualHost>
```

Далее ребут всей системы `systemctl restart zabbix-server zabbix-agent apache2`

Добавление хостов в Zabbix-server

Ставим пакет - `apt install zabbix-agent`

далее на сервере HQ-LinSRV2 подготовим конфигурацию для клиентов

1) заранее сгенерируем ключ `echo R3ASK1LZ2021 | sha256sum > agent.key.`

Проверь, что он создался без говна (там в конце часто -)

2) Генерим конфиг `/etc/zabbix/zabbix_agentd.conf`

а) Корректируем параметры Server

i)

```
Server=192.168.0.20
```

ii) Не обязательно, но можно сделать вот так

```
# Default:
ListenPort=10050

### Option: ListenIP
#       List of comma delimited IP addresses t
#       First IP address is sent to Zabbix ser
#
# Mandatory: no
# Default:
ListenIP=192.168.0.30
```

iii)

```
# ServerActive=
ServerActive=192.168.0.20

### Option: Hostname
#       List of comma delimited unique, case sensit
#       Required for active checks and must match h
#       Value is acquired from HostnameItem if unde
#
# Mandatory: no
# Default:
# Hostname=
Hostname=HQ-LinSRV3
```

iv)

Далее уже важные вещи, такие как конфигурация TLS PSK

1) `TLSConnect=psk`

2) `TLSAccept=psk`

```

# Mandatory: yes, if TLS certificate or PSK p
# Default:
TLSConnect=psk

### Option: TLSAccept
#   What incoming connections to accept.
#   Multiple values can be specified, sep
#       unencrypted - accept connecti
#       psk         - accept connecti
#       cert        - accept connecti
#
# Mandatory: yes, if TLS certificate or PSK p
# Default:
TLSAccept=psk

```

TLSPSKIdentity=WSR

TLSPSKFile=/opt/zabbix/agent.key

```

# Default:
TLSPSKIdentity=WSR

### Option: TLSPSKFile
#   Full pathname of a file containing the pre-shar
#
# Mandatory: no
# Default:
TLSPSKFile=/opt/zabbix/agent.key

```

Далее создавай директории и расположи все ключи как хотел.

На машине с которой будешь админить Zabbix также отправь копию ключа

Теперь добавляем хост в Zabbix

Hosts

[Host](#) [Templates 1](#) [IPMI](#) [Tags](#) [Macros](#) [Inventory](#) [Encryption](#)

Linked templates

Name	Action
------	--------

Link new templates

Linux by Zabbix agent ✕

type here to search

Select

Add

Cancel

Hosts

[Host](#) [Templates 1](#) [IPMI](#) [Tags](#) [Macros](#) [Inventory](#) [Encryption ●](#)

Connections to host

No encryption

PSK

Certificate

Connections from host

☐ No encryption

☒ PSK

☐ Certificate

* PSK identity

WSR

* PSK

336bb228f8395af4c07e2b560757591396f6de02ba197ee161bd8db795fce1b0

Add

Cancel

В PSK как раз таки вставь тот agent.key что сделал в первом шаге

Успех когда вот так

Name ▲	Interface	Availability
BR-LinSRV	172.16.0.10: 10050	ZBX SNMP JMX IPMI
HQ-LinSRV1	192.168.0.10: 10050	ZBX SNMP JMX IPMI
HQ-LinSRV2	127.0.0.1: 10050	ZBX SNMP JMX IPMI
HQ-LinSRV3	192.168.0.30: 10050	ZBX SNMP JMX IPMI

По

лдану

[Authentication](#) [HTTP settings](#) [LDAP settings](#) [SAML settings](#)

Enable LDAP authentication ☒

* LDAP host

192.168.0.10

* Port

389

* Base DN

dc=rea2021,dc=lin

* Search attribute

uid

Bind DN

cn=admin,dc=rea2021,dc=lin

Case sensitive login

☐

Bind password

Change password

Test authentication

[must be a valid LDAP user]

* Login

SuperAdmin

* User password

Update

Test

Потом сначала User groups

<input type="checkbox"/>	sysadmins	Users 1	SuperAdmin	LDAP
<input type="checkbox"/>	Zabbix administrators	Users 2	Admin (Zabbix Administrator), SuperAdmin	System

и самого юзера

<input type="checkbox"/>	SuperAdmin	Super admin role	sysadmins, Zabbix administrators	Yes (2021-04-04 10:34:07)
--------------------------	------------	------------------	----------------------------------	---------------------------

Не забудь выдать ему фулл права Super admin role, а то просрешь доступ

Можно переключаться

Authentication

[Authentication](#) [HTTP settings](#) [LDAP settings](#) [SAML settings](#)

Default authentication ☐ Internal ☒ LDAP

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.rea2021.lin**
- d. Обеспечьте возможность доступа с использованием учётных записей службы LDAP
 - ii. Группа Sysadmins должна иметь права администраторов Grafana

Сделано: _____

```
export https_proxy=http://10.10.18.215:808
```

И тоже самое для http_proxu

Теперь подключаем репы

```
#deb cdrom:[Debian GNU/Linux 10.8.0 _Buster_ - Official amd64 DVD Binary-1 202
deb [trusted=yes] https://packages.grafana.com/oss/deb stable main
# Line commented out by installer because it failed to verify:
```

apt install grafana

systemctl start grafana-server

Переходим на веб-морду по адресу и порту 3000. Там нужно будет только поставить пароль

Далее идем на сервер и ставим плагины:

grafana-cli plugins install alexanderzobnin-zabbix-app

Go to **Configuration > Plugins** to enable our newly installed Zabbix data source

Configuration > Data Sources

Click on the cog on the side menu and go to Data Sources.

1. Click Add data source.
2. Select Zabbix.

The screenshot shows the 'Data Sources / Zabbix' configuration page in a dark-themed interface. At the top left is a red square logo with a white 'Z'. The title 'Data Sources / Zabbix' is followed by 'Type: Zabbix'. Below this is a navigation bar with 'Settings' (selected) and 'Dashboards'. The main configuration area includes a 'Name' field set to 'Zabbix' with a 'Default' toggle switch turned on. The 'HTTP' section contains a 'URL' field with the value 'https://zbx.rea2021.lin/api_jsonrpc.php', an 'Access' dropdown menu set to 'Server (default)' with a 'Help >' link, and a 'Whitelisted Cookies' section with a text input 'New tag (enter key to add)' and an 'Add' button. The 'Auth' section features several toggle switches: 'Basic auth' (off), 'With Credentials' (off), 'TLS Client Auth' (off), 'With CA Cert' (off), 'Skip TLS Verify' (on), and 'Forward OAuth Identity' (off). Each toggle has an information icon to its right.

Zabbix API details

Username	hyperadmin	
Password	Configured	Reset
Trends	<input checked="" type="checkbox"/>	
After	<input type="text" value="7d"/>	
Range	<input type="text" value="4d"/>	
Cache TTL	<input type="text" value="1h"/>	
Timeout	<input type="text" value="30"/>	

Direct DB Connection

Enable ☐

Other

Disable acknowledges for read-only users ☐

Disable data alignment ☐

3.

Конфиги под LDAP - /etc/grafana/ldap.toml

Под SSL - /etc/grafana/grafana.ini - все интуитивно понятно

#НАПОМИНАНИЕ КАК СДЕЛАТЬ СЕРТЫ В АСТРЕ

```
libnss3.so libnssckbi.so libnssckbi.so.orig libnssutil3.so
root@HQ-CLI:/usr/lib/firefox# ls -la libnssckbi.so
lrwxrwxrwx 1 root root 49 апр  3 11:24 libnssckbi.so -> /usr/lib/x86_64-linux-gnu/pkcs11/p11-kit-trust.so
root@HQ-CLI:/usr/lib/firefox#
```


4. Обеспечьте централизованный сбор журналов со всех клиентских хостов и серверов в базу данных на HQ-LinSRV1

Сделано: _____

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.rea2021.lin, по протоколу https.
 - c. Реализуйте перенаправление http->https

Редирект с http на https

```
LoadModule rewrite_module /usr/lib/apache2/modules/mod_rewrite.so
```

```
<VirtualHost *:80>
ServerName logs.rea2021.lin
RewriteEngine on
Redirect 301 / https://logs.rea2021.lin/
</VirtualHost>
```

Сделано: _____

Делается элементарно, все есть в INSTALL. Если вдруг тебя аутизм хватит, то вот как сайт на https сделать.

```
</VirtualHost>
<VirtualHost *:443>
DocumentRoot /var/www/
ServerName logs.rea2021.lin
SSLEngine on
SSLCertificateFile /var/www/logs.pem
SSLCertificateKeyFile /var/www/logs.key
</VirtualHost>
```

#Как настроить PGSQL на работу с rsyslog

Ставим пакет - `apt install rsyslog-pgsql`

- 1) Localhost - где живет БД
- 2) 127.0.0.1 - адрес БД, на всякий случай
- 3) Пароль `P@ssw0rd \ P@ssw0rd`
- 4) БД которую он создает автоматически зовут Syslog.

На логаналайзере надо поставить: `apt install php-pgsql`

и после этого конфигурируем логанал жопы.

Не забудь на HQ-LinSRV1 в `pg_hba.conf` разрешить подключение

```
host      all             all             172.16.0.10/32      trust
# IPv6 local connections:
```

юзер для коннекта - postgres

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 - **rea2021.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

Сделано: _____

Создание Group.ldif + организационной единицы

```
dn: ou=Groups,dc=rea2021,dc=lin
objectClass: organizationalUnit
ou: Groups
dn: cn=Uzvers,,ou=Groups,dc=rea2021,dc=lin
objectClass: posixGroup
cn: Uzvers
gidNumber: 2222
```

Пример user.ldif + не забудь **userPassword**

```
dn: cn=IvanPetrov,dc=rea2021,dc=lin
objectClass: inetorgperson
objectClass: posixAccount
cn: IvanPetrov
uid: IvanPetrov
sn: IvanPetrov
uidNumber: 17016
gidNumber: 4444
loginShell: /bin/bash
homeDirectory: /home/IvanPetrov
~
~
```

Скорее всего замени на установку libpam-ldap, а потом libpam-ldapd

Для астры все тоже самое, только еще потом поставь libnss-ldap и libpam-ldapd должны в конце только быть

там вроде все легко и сам помнишь как это делать :)

В файле /etc/pam.d/login

```
auth optional pam_faildelay.so delay=3000000
account required pam_access.so
# Outputs an issue file prior to each login prompt (Replaces the
# ISSUE FILE option from login.defs). Uncomment for use
```

В /etc/security/access.conf но это костыль вообще, но работает, да?

```
#
-:ALL EXCEPT root LittleUser BigUser NotSoSmallUser_(sysadmins):LOCAL
# User "john" should get access from ipv6 net/mask
#+:john:2001:4ca0:0:101::/64
```

Для астра линукс

- 1) Подключи дебиан репы
- 2) apt install debian-archive-keyring

- ```
29 apt install libpam-ldap libnss-ldap
30 apt search libnss-ldap
31 apt update
32 apt install libpam-ldap libnss-ldap
33 pam-auth-update
34 id SuperAdmin
35 vim /etc/nsswitch.conf
36 id SuperAdmin
37 journalctl -xe
38 dpkg-reconfigure libnss-ldap
39 id SuperAdmin
40 history
```
- 3)
- 4) Укажи, что аутентифицируемся через cn=admin, а то не заработает

### 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

Сделано: \_\_\_\_\_

- 1) apt install ocserv

- ```
# TCP and UDP port number
tcp-port = 4443
udp-port = 4443
```
- 2)

```
server-cert = /etc/ocserv/ocserv.pem
server-key = /etc/ocserv/ocserv.key
```

```
# in that case it is recommended to s
ipv4-network = 10.8.8.0
ipv4-netmask = 255.255.255.0
```

```
# multiple servers.
# dns = fc00::4be0
dns = 172.16.20.10
```

```
route = 10.10.10.0/255.255.255.0
route = 192.168.0.0/255.255.0.0
route = 172.16.0.0/255.255.0.0
#route = fe4:db8:1000:1001::/64
```

```
# The default domain to be advertised
default-domain = skill39.wsr
```

```
#auth = "pam[uid-min=1000]"
auth = "plain[passwd=/etc/ocserv/ocpasswd]"
#auth = "certificate"
```

3)

ocpasswd -c /etc/ocserv/ocpasswd vpnuser - и потом под этими правами туда и
КОКОСИМСЯ

2) На Remote-LinCLI настройте клиент удаленного доступа на основе технологии
OpenConnect

а) 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.

Сделано: _____

vim /etc/systemd/system/connect.service

```
[Unit]
Description=VPN Connector to skill39.wsr
Documentation=man:openconnect
After=network-online.target

[Service]
Type=simple
ExecStart=/bin/bash -c '/bin/echo test1 | openconnect _vpn.skill39.wsr:4443 -u test --passwd-on-stdin'
ExecStop=/bin/bash -c '/bin/pkill -9 openconnect'
Restart=always
RestartSec=2

[Install]
WantedBy=multi-user.target
```

- 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

Сделано: _____

- a) **vim /etc/ipsec.secrets**

```
include /etc/ipsec.d/*.secrets
20.20.20.100 10.10.10.1 : PSK "WSR-2019"
~
~
~
```

IPSEC DEBIAN

- b) **apt install strongswan -y**
- c) **vim /etc/ipsec.conf**

```
# Sample VPN connections

conn vpn
    left=10.10.10.1
    leftprotoport=gre
    right=20.20.20.100
    rightprotoport=gre
    type=tunnel
    ike=3des-sha1-modp2048
    esp=aes128-sha2_256
    authby=secret
    auto=start
```

- d)

Конфигурация служб хранения данных

- 1) Преобразуйте в физические тома LVM все свободные носители на BR-LinSRV.
 - a) Создайте группу логических томов REA_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.

Сделано: _____

apt-get install lvm2

cfdisk /dev/sd*

pvccreate /dev/sdb1 /dev/sdc1 /dev/sdd1 - добавили все в одну группу

vgcreate semifinal /dev/sdb1 /dev/sdc1 /dev/sdd1 - создали группу

SEMIFINAL - как по заданию

lvcreate -L 200m -n Backup semifinal - создали логический том на базе группы SEMIFINAL, с объемом 200 мб

lvcreate -l 40%FREE -n Storage semifinal - создали логический том на базе группы Semifinal, с объемом 40% от всего объема

-----Create and mount filesystem

mkfs.ext4 /dev/optlvm/Storage

mkfs.ext4 /dev/optlvm/Backup

mkdir /opt/Storage

mkdir /opt/Backup

echo "/dev/optlvm/Storage /opt/Storage ext4 defaults 0 0" >> /etc/fstab

echo "/dev/optlvm/Backup /opt/Backup ext4 defaults 0 0" >> /etc/fstab

lvcreate -l 100%ORIGIN -s -n CLEAR_Storage /dev/optlvm/Storage

lvcreate -l 100%ORIGIN -s -n CLEAR_Backup /dev/optlvm/Backup

lvs - для проверки логических разделов

mount -a

-----Snapshot

echo 0 > count

vim create_snapshot.sh

```
#!/bin/bash

echo $(( $(cat /root/count) + 1 )) > /root/count

if [ $(cat /root/count) -le 9 ];then
    lvcreate -l 5%ORIGIN -s -n SNAP-0$(cat /root/count)-Backup /dev/optlvm/Backup
    lvcreate -l 5%ORIGIN -s -n SNAP-0$(cat /root/count)-Storage /dev/optlvm/Storage
else
    lvcreate -l 5%ORIGIN -s -n SNAP-$(cat /root/count)-Storage /dev/optlvm/Storage
    lvcreate -l 5%ORIGIN -s -n SNAP-$(cat /root/count)-Backup /dev/optlvm/Backup
fi
exit 0
```

Супер скрипт

Запись в кроне

```
# * * * * * user-name command to be executed
0 */1 * * * root /root/create_snapshot.sh
~
```

- 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 smb 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.

- с) Обеспечьте автоматическое подключение катлога /opt/Users на машины HQ-LinCLI и BR-LinCLI по протоколу NFS в директорию /home

Сделано: _____

Конфига на Samba

```
[global]
server role = standalone
security = user
workgroup = default
passdb backend = tdbsam
map to guest = bad user
log file = /var/log/samba/%l.log
log level = 2

[Work]
browseable = yes
path = /opt/Shares/workfolders
guest ok = yes
read only = no
```

Потом задаем пароль **smbpasswd -a root (toor)**

На клиенте

```
dev/sr0 /media/Curamo dnf,iso9660 user,uid=0 0 0
/172.16.0.10/Work /home/workfolder cifs user,rw,credentials=/root/cred 0 0_
```

Содержимое /root/cred

```
user=root
password=toor
```

NFS

apt install nfs-server -y

vim /etc/exports

```
#
/opt/Users *(rw,sync,no_root_squash)
```

systemctl restart nfs-server

На клиенте:

apt install nfs-common -y

```
172.16.0.10:/opt/Users /home/ nfs defaults 0 0
```

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 качестве содержимого сконфигурируйте файл index.html со следующим содержимым: “Welcom to REASKILLZ. Server HQ-LinSRV1”

Сделано:_____

Ну здесь nginx пойдет - **vim /etc/nginx/conf.d/site.conf**

```
server {
    listen 192.168.0.10:8088;
    location / {
        root /opt/web;
        index index.html;
    }
}
```

2)

- 3) На HQ-LinSRV1 разверните веб сайт
- Используйте порт 8088
 - Используйте директорию /opt/web/ в качестве корневой директории сайта
 - В качестве содержимого сконфигурируйте файл index.html со следующим содержанием: “Welcom to REASKILLZ. Server HQ-LinSRV2”

Сделано: _____

Вот апач - **vim /etc/apache2/apache2.conf**

```
<VirtualHost 192.168.0.20:8088>
    DocumentRoot /opt/web
    <Directory />
        Require all granted
    </Directory>
</VirtualHost>
```

И еще в ports.conf

```
#Listen 80
Listen 80
Listen 8088

<IfModule ssl_module>
    Listen 443
</IfModule>
```

- 4) На сервере HQ-LinSRV3 настройте haproxy
- В качестве бэкэндов используйте HQ-LinSRV1 и HQ-LinSRV2
 - Обеспечьте балансировку нагрузки между бэкэндами, с использованием алгоритма Round Robin
 - Доступ должен производиться по имени www.rea2021.lin
 - Сконфигурируйте https и автоматическое перенаправление на https.

Сделано: _____

HAPROXY

Apt install haproxy

Cp /usr/share/doc/haproxy/examples/ssl.cfg > /etc/haproxy/proxy.cfg

cat proxy.pem proxy.key > proxy.crt - и вот что получилось, то и пихай!

```
global
    maxconn 100

defaults
    mode http
    timeout connect 5s
    timeout client 5s
    timeout server 5s

frontend myfrontend
    # primary cert is /etc/cert/server.pem
    # /etc/cert/certdir/ contains additional certificates for SNI clients
    bind :443 ssl crt /etc/certs/proxy.pem
    bind :80
    http-request redirect scheme https unless { ssl_fc }
    default_backend ha

backend ha
    # a http backend
    balance roundrobin
    server s3 192.168.0.10:8088
    server s4 192.168.0.20:8088
    # a https backend
    # server s4 10.0.0.3:443 ssl verify none
```

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 - REASKILLZ CA
 - ii) Country - RU
 - iii) Organization - REA 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.

Сделано: _____

```
root@HQ-LinSRV1:~# find /* -name CA.pl
/usr/lib/ssl/misc/CA.pl
root@HQ-LinSRV1:~# apt install openssl libcrypto-openssl* -y
```

1) Настройте межсетевой экран **nftables** на BR-LinSRV и HQ-LinSRV

a) Реализуйте правила работы с трафиком

- i) Весь трафик, покидающий внутреннюю сеть должен проходить маскардинг
- ii) Разрешите прохождение трафика, необходимого для выполнения задания
- iii) Весь остальной трафик следует запретить
- iv) В отношении ICMP трафика поступайте на ваше усмотрение.

Сделано: _____

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**

Сделано: _____

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 производиться перенаправление соединения на BR-LinSRV1, порт 22.

Сделано: _____

```
iptables -t nat -A PREROUTING -p tcp --dport=2222 -j DNAT --to-destination 172.16.0.10:22
```

Конфигурация СУБД

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

Сделано: _____

Таблица №1 – Группы и пользователи LDAP

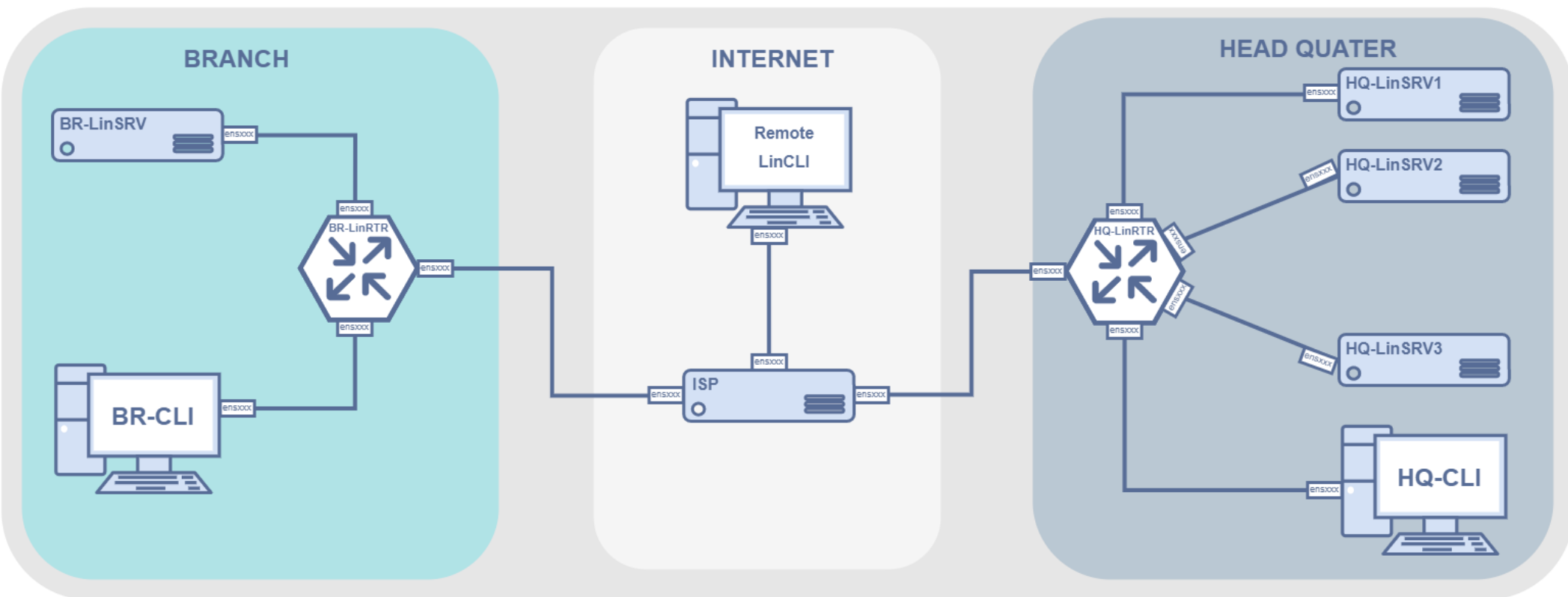
Группы	Пользователи
Sysadmins	SuperAdmin, MegaAdmin, HyperAdmin
Uzvers	LittleUser, BigUser, NotSoSmallUser
Experts	Gates, Torvalds, Stallman
Allies	Englishman, Yankee, IvanPetrov

Таблица №2 – DNS-имена

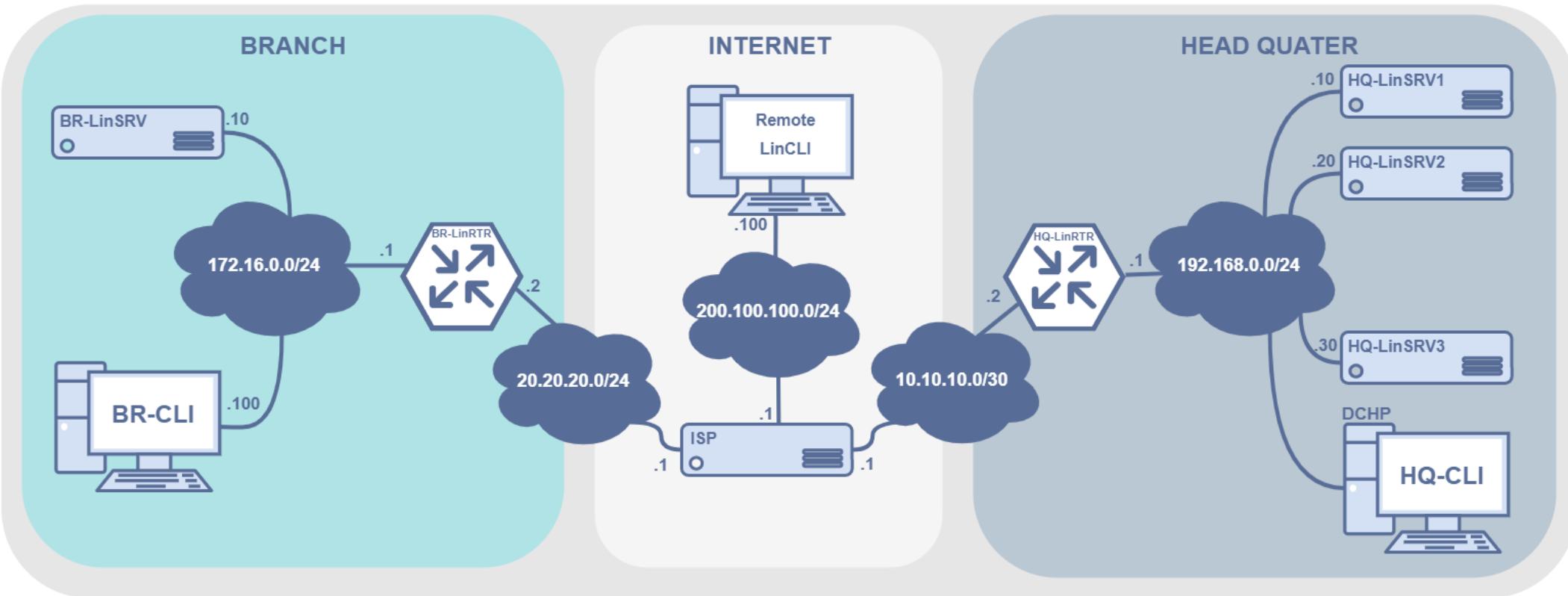
Хост	DNS-имя
------	---------

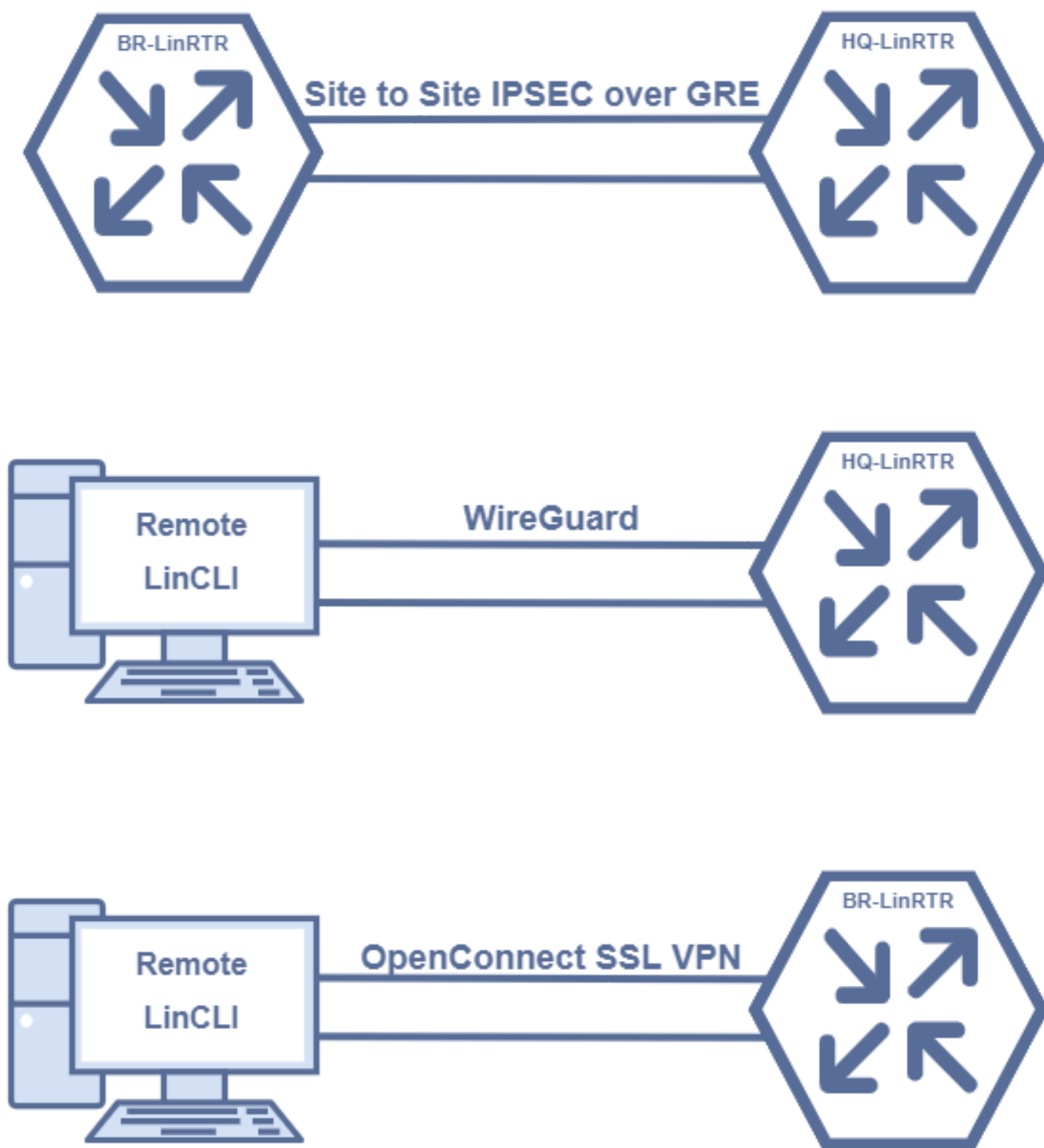
BR-LinSRV	A,PTR: br-linsrv.rea2021.lin CNAME: logs.rea2021.lin
BR-CLI	A,PTR: br-cli.rea2021.lin
HQ-LinSRV1	A,PTR: hq-linsrv1.rea2021.lin CNAME: test.rea2021.lin
HQ-LinSRV2	A,PTR: hq-linsrv2.rea2021.lin CNAME: zbx.rea2021.lin CNAME: grafana.rea2021.lin
HQ-LinSRV3	A,PTR: hq-linsrv3.rea2021.lin CNAME: www.rea2021.lin
HQ-CLI	A,PTR: hq-cli.rea2021.lin

Топология L1



Топология L3





Топология VPN