Документация программного обеспечения «Агрегатор нагрузки «ФОТЕЛ АН-01», предоставленного для экспертной проверки

Установка программного обеспечения

Содержание

1. Инструкция по установке ПО

1.1 Общие сведения

Перед тем, как воспользоваться данной Инструкцией, необходимо убедиться, что на соответствующих серверах узла агрегации (далее – Узел) развернута среда виртуализации Proxmox и Open vSwitch, создан бридж OVS.

В среде виртуализации Proxmox должна быть создана **виртуальная машина** (ВМ) с ОС Debian (11 версии, 64 бит), отвечающая следующим минимальным требованиям к машинным ресурсам.

Процессор	Оперативная память	Жесткий диск
Минимум 2 ядра.	Тип не ниже DDR3.	Тип HDD/SSD.
Частота минимум:	Объем не менее:	Объем не менее:
3 ГГц на ядро	4 гигабайт	10 Гбайт

Также необходимы сетевые карты (не менее 2) пропускной способностью не менее 1 Гб/сек.

Дальнейшее использование Инструкции подразумевает, что доступ к серверам обеспечивается, в наличии логины и пароли уровня доступа root.

Установка ПО «Агрегатор нагрузки» осуществляется из репозитория ООО «ФОТЕЛ». Репозиторий развернут на сервере в облачной Интернет-среде. На сервере настроен HTTP-сервер, с помощью которого обеспечивается доступ к хранилищу файлов, VPN доступ не требуется.

Репозиторий с точки зрения Клиента содержит:

— программное обеспечение серверов агрегации для поддерживаемой версии Debian 11 по адресу:

- https://repo.fotel.pro/bullseye

Клиент должен получить от компании ООО «ФОТЕЛ» уникальную пару логин/пароль для доступа к репозиторию.

1.2 Установка ПО из репозитория

ВНИМАНИЕ! *В данной главе приводится описание процедуры полной установки СА на заранее подготовленную чистую ОС Debian версии 11.*

В тексте используются следующее обозначения для работы в консоли сервера:

Команда в консоли (символ # обозначает команду в shell из под рута)

Вывод команды в консоли или строки в просматриваемом/редактируемом файле

1.2.1 Объявление репозитория

Чтобы добавить репозиторий ООО «ФОТЕЛ», следует выполнить следующие шаги.

- Создать и открыть для редактирования файл на СА командой:

nano /etc/apt/sources.list.d/fotelrepo.list

Вписать в файл *fotelrepo.list* строку:

deb [trusted=yes] https://repo.fotel.pro/bullseye fotel main non-free

- Создать и открыть для редактирования файл на СА командой:

nano /etc/apt/apt.conf.d/99fotelrepo-cert

Вписать в файл *99fotelrepo-cert* строку:

Acquire::https::repo.fotel.pro::Verify-Peer "false";

- Создать и открыть для редактирования файл на СА командой:

nano /etc/apt/auth.conf.d/fotel.conf

Вписать в файл *fotel.conf* строки:

machine repo.fotel.pro

login логин

password пароль

где «*логин*» и «*пароль*» – предоставленные клиенту данные для доступа к репозиторию.

- Изменить права доступа к файлу fotel.conf на СА командой:

```
# chmod 600 /etc/apt/auth.conf.d/fotel.conf
```

1.2.2 Установка ядра MPTCP

Далее следует установить ядро mptcp следующей последовательностью действий.

- Обновление пакетов ОС Debian командой:

```
#apt-get update
```

- Поиск нужных пакетов командой:

```
# apt-cache search mptcp
```

В результате должны быть найдены два файла вида:

linux-headers-x.y.zzz-mptcpX.deb

linux-image-x.y.zzz-mptcpX.deb

Где

x.y.zzz , X– текущая версионность файла и ядра mptcp (например, linux-headers-5.4.209-mptcp3).

- затем последовательно установить найденные пакеты командами:

```
# apt-get install linux-headers- x.y.zzz-mptcpX
# apt-get install linux-image- x.y.zzz-mptcpX
```

1.2.3 Изменение стандартного пункта загрузки ядра в загрузчике GRUB

Далее следует изменить стандартный пункт GRUB загрузки ядра, чтобы при перезагрузке грузилось новое ядро, содержащее mptcp. Последовательность действий изложена ниже.

- Просмотр файла конфигурации GRUB командой:

```
egrep '(menuentry |submenu)' /boot/grub/grub.cfg
```

- Найти идентификатор пункта меню загрузки (показан пример, может отличаться версионность):

submenu 'Advanced options for Debian GNU/Linux' $menuentry_id_option ***'gnulinux-advanced-8bbbfb59-b0cc-4e01-9306-e2be466a8b07'*** *{*

Скопировать данные, которые в примере выделены.

- Найти идентификатор пункта меню загрузки новой версии ядра (показан пример, может отличаться версионность):

menuentry 'Debian GNU/Linux, with Linux 5.4.209-mptcp3' --class debian --class gnu-linux --class gnu --class os $menuentry_id_option ***'gnulinux-5.4.209-mptcp3-advanced-bdeafa70-be19-4b2c-84e2-074bec3b408e'*** *{*

Скопировать данные, которые в примере выделены.

- Открыть для редактирования файл grub командой:

```
nano /etc/default/grub
```

- Изменить строку *GRUB_DEFAULT=0*, вписав текущую и новую версию ядра, чтобы строка приобрела вид:

*GRUB_DEFAULT=****'gnulinux-advanced-8bbbfb59-b0cc-4e01-9306-e2be466a8b07>gnulinux-5.4.209-mptcp3-advanced-bdeafa70-be19-4b2c-84e2-074bec3b408e'***

Сохранить файл grub.

- После этого следует обновить меню GRUB командой:

```
update-grub
```

- Перезагрузить сервер.

1.2.4 Проверка корректной установки ядра mptcp

Проверка ядра mptcp осуществляется командой для получения информации, идентифицирующей текущую операционную систему:

```
uname -a
```

Вывод команды (пример) при корректной загрузке нового ядра с mptcp:

Linux agg4 5.4.209-mptcp3 #1 SMP Wed Aug 31 14:51:45 MSK 2022 x86_64 GNU/Linux

Проверка включенной службы MPTCP командой:

```
sysctl net.mptcp.mptcp_enabled
```

Вывод команды при задействованной службе:

net.mptcp.mptcp_enabled = 1

Если служба mptcp не установлена или загрузилось ядро без mptcp, вывод указанной команды будет следующим:

sysctl: cannot stat /proc/sys/net/mptcp/mptcp_enabled: Нет такого файла или каталога

1.2.5 Обеспечение беспарольного доступа CA к серверу DNS

Чтобы обеспечить возможность соединения CA с сервером DNS (ЦУ) без пароля по ключам SSH, необходимо выполнить следующие шаги.

- На CA следует ввести команду генерации публичного ключа SSH:

```
ssh-keygen -t rsa -b 2048
```

Примечание: *Для упрощения генерации ключа во время выполнения команды следует нажимать Enter после каждого приглашения к диалогу.*

- Далее следует скопировать и вставить полученный файл открытого ключа CA *id_rsa.pub* на сервер DNS в файл *.ssh/authorized_keys*.

Для этого необходимо вывести ключ на экран консоли CA по команде

```
cat ~/.ssh/id_rsa.pub
```

Скопировать выведенный ключ (ctrl+C), зайти на сервер DNS, открыть для редактирования файл *.ssh/authorized_keys* сервера DNS и вставить скопированные данные ключа. Сохранить файл.

- Изменить на DNS сервере права доступа к файлу */root/.ssh/authorized_keys* последовательным вводом команд:

```
chmod 700 /root/.ssh
chmod 600 /root/.ssh/authorized_keys
```

- После указанной процедуры следует проверить работу беспарольного доступа CA к серверу DNS путем доступа из консоли CA к серверу DNS командой:

```
# ssh IP_address_DNS
```

Где

IP_address_DNS – актуальный IP-адрес сервера DNS.

1.2.6 Установка необходимых пакетов для работы CA

Необходимые для работы сервера агрегации пакеты ПО устанавливаются последовательным вводом следующих команд:

```
# apt-get install iptables
  # update-alternatives --set iptables /usr/sbin/iptables-legacy
# apt-get install tcpdump
# apt-get install zabbix-agent
#apt-get install openvpn
#apt-get install openvpn-auth-radius
# apt-get install curl
# apt-get install apt-transport-https
```

```
# apt-get install gnupg
    # curl -s https://deb.frrouting.org/frr/keys.asc -o /etc/apt/trusted.gpg.d/frr.asc
    # echo "deb https://deb.frrouting.org/frr bullseye frr-stable" > /etc/apt/sources.list.d/frr.list
    # apt-get update
```

```
# apt-get install frr
```

Затем открыть файл */etc/frr/daemons* на редактирование, найти строку включения ospfd, и привести к виду:

```
ospfd=yes
```

Выполнить команду перезапуска службы frr:

```
# systemctl restart frr
```

Продолжить ввод команд установки пакетов ПО:

```
# apt-get install iperf3
# apt-get install openvswitch-common
# apt-get install openvswitch-switch
# apt-get install jq
# apt-get install vlan
```

```
# apt-get install fotelradius
    # systemctl stop fotelradius
    # systemctl enable fotelradius
```

Открыть файл */etc/fotelradius/config.conf* на редактирование, найти указанные секции и привести к виду:

```
    mysql:
    {
        url:"X.X.X.X1:3306";
        username:"user";
        password:"passwd";
        database:"db_name";
    };
```

Где

X.X.X.X$_1$:3306 – IP-адрес базы данных MySQL на сервере AAA (порт дефолтный).

user – актуальный логин для доступа к БД.

passwd - актуальный пароль для доступа к БД.

db_name – вписать имя БД.

```
auth:
{
    ip_addr:" X.X.X.X2";
    port:1812;
    secret:"pass";
};
```

Где

X.X.X.X2 – IP-адрес данного CA.

port:1812 – порт, на котором на CA слушает служба fotelradius.

pass – актуальный пароль для доступа к службе fotelradius службой fotelVPN.

```
acct:
{
    ip_addr:" X.X.X.X2";
    port:1813;
    secret:"pass";
};
```

Где

X.X.X.X2 – IP-адрес данного CA.

port:1813 - порт, на котором на CA слушает служба fotelradius.

pass – актуальный пароль для доступа к службе fotelradius службой openVPN.

Сохранить файл. Стартовать службу fotelradius командой:

```
# systemctl start fotelradius
```

Продолжить ввод команд установки пакетов ПО:

```
# apt-get install fotelvpn
# systemctl stop fotelvpn
# systemctl enable fotelvpn
```

Открыть файл */etc/fotelvpn/fotelvpn.conf* на редактирование, найти указанные секции и привести к виду:

```
type:"server";
    verbose: 7;
```

```
    script: "/etc/fotelvpn/manager.sh";
  server:
  {
    ip_addr:"public_IP-address";
    port:8521;
    port_stats:8531;
```

Где

/etc/fotelvpn/manager.sh – указать полный путь к скрипту manager.sh (указанный скрипт на текущий момент установки еще не существует! См. ниже в данном пункте).

public_IP-address – актуальный публичный IP-адрес СА.

Порты указаны дефолтные.

Секция отправки snmp с СА:

```
    snmp:
    {
      server:"Z.Z.Z.Z:162";
      community:"public";
    };
```

Где

Z.Z.Z.Z:162 - вписать IP-адрес сервера, куда будут отправляться SNMP трапы и события.

В секции «radius_servers» вписать параметры радиус-сервера для аутентификации и аккаунтинга:

```
radius_servers = (
  {
    type:"auth";
    ip_addr:"IP-addres_Radius_server ";
    port:1812;
    secret:"password";
  },
  {
    type:"acct";
    ip_addr:"IP-addres_Radius_server ";
    port:1813;
    secret:"password";
  },
```

Где

Где *IP-addres_Radius_server* – IP адрес Radius-сервера.

password – актуальный пароль для доступа к Radius-серверу.

Продолжение установки пакетов для *fotelvpn*

```
# apt-get install aggfiles
# systemctl restart rsyslog
# sysctl --system
```

Открыть файл /root/checker.sh на редактирование, найти строку:

WANIF='FIXME iface with public IP-address'

и привести к виду:

*WANIF=**'ensX'***

Где

ensX – интерфейс сервера СА, которому при установке ОС был присвоен белый (публичный) IP-адрес.

Сохранить файл checker.sh.

Открыть файл */etc/fotelvpn/manager.sh* на редактирование, найти указанную строку и привести к виду:

*bridgeif="**ensX**"*

Где

ensX –интерфейс сервера СА, которому при установке ОС был присвоен белый IP-адрес. Данный интерфейс в белой сети создан системой в файле */etc/network/interfaces* и указан в секции *«# The primary network interface»*

Сохранить файл *manager.sh*.

Стартовать службу fotelvpn командой:

```
# systemctl start fotelvpn
```

Окончание установки пакетов

```
# apt-get install fotelstats
# apt-get install fotelvpnconsole
```

1.2.7 Установка и работа утилиты для автоконфигурирования СА

Для частичной автоконфигурации сервера агрегации служит проприетарная утилита *aggregatorconfig,* устанавливаемая из репозитория*.* Подробная инструкция

по работе с утилитой aggregatorconfig изложена в разделе 4.7. Ниже в данном пункте указаны действия, подразумевающие, что общие принципы работы с утилитой уже изучены.

- Установка утилиты командой:

```
# apt-get install aggregatorconfig
```

- После установки утилиты на CA следует внести изменения в файл /etc/aggregatorconfig/config.json в соответствии с положениями раздела 4.5 (ориентируясь на описание секций (П.4.5.5) и приведенный пример файла (П.4.5.6), и используя актуальные данные для собственного CA).

- Проверить синтаксис отредактированного файла /etc/aggregatorconfig/config.json командой:

```
# jq '.' /etc/aggregatorconfig/config.json
```

Если файл содержит ошибки, команда выведет ее описание. Пример ошибки синтаксического анализа:

```
Expected another array element at line 66, column 5
```

- Запустить сервис *aggregatorconfig* :

```
# systemctl start aggregatorconfig
```

Сервис автоматически применит готовый файл автоконфигурации и внесет необходимые правки.

Для проверки наличия запущенного сервиса, можно использовать команду

```
# systemctl status aggregatorconfig
```

Найти в выводе строку, что сервис запущен:

```
Active: active (running)
```

1.2.8 Настройки OpenVPN и ручное конфигурирование CA

- Создать необходимые директории последовательными командами:

```
# mkdir /etc/openvpn/ccd
# mkdir /etc/openvpn/keys
```

- В каталог */etc/openvpn/keys* поместить сертификаты и ключи SSL (например, готовые с другого CA или, при необходимости, создать свои).
- Ручное редактирование файла radiusplugin.cnf

В файле */etc/openvpn/radiusplugin.cnf* надо привести строки к указанному виду:

NAS-IP-Address= ***X.X.X.X***

*subnet=****255.255.240.0***

```
radius server definition
    name=IP-addres_Radius_server
    sharedsecret= password_Radius_server
```

Где

X.X.X.X - публичный IP-адрес СА (белый адрес, указанный при установке ОС Debian 11).

255.255.240.0 - маска по умолчанию, определена в файле server.conf из строки ifconfig-pool 192.168.90.0 192.168.111.254 255.255.240.0 (см. ниже).

IP-addres_Radius_server - актуальный IP адрес сервера Radius.

password_Radius_server – актуальный пароль доступа к серверу Radius.

- Ручное редактирование файла server.conf

В файле */etc/openvpn/ server.conf* изменить/вписать 4 строки, относящиеся к SSL и вписать строку ifconfig-pool с указанными параметрами:

```
ca      /etc/openvpn/keys/xxxx.crt
cert    /etc/openvpn/keys/xxxx.crt
key     /etc/openvpn/keys/xxxx.key
dh      /etc/openvpn/keys/xxxx.pem
. . .
ifconfig-pool 192.168.90.0 192.168.111.254 255.255.240.0
. . .
push "route  ……."
push "route  ……."
push "route  ……."
```

Где

xxxx – актуальные имена файлов сертификатов и ключей SSL.

192.168.90.0 192.168.111.254 255.255.240.0 - строка определяющая планируемое количество Маршрутизаторов, можно использовать по умолчанию.

push "route ……." - адреса сетей следует вписать или изменить (если они есть) на актуальные маршруты, передаваемые клиентам при подключении, внеся соответствующие адреса и маски сетей.

- Конфигурирование скрипта добавления маршрутов routeadder.sh.

Открыть файл скрипта для редактирования, внести правки в строки:

```
ssh Y.Y.Y.Y "/root/routeadder.sh $1 $IPADDRESS"
```

Где

Y.Y.Y.Y – актуальный приватный адрес DNS сервера с ЦУ.

В этом же скрипте найти строку вида:

LANIF='FIXME - iface with private IP-address to connect with DNS server'

Где вместо «*'FIXME -…»* необходимо внести имя интерфейса CA с приватным IP для сопряжения с DNS, приведя строку к виду (пример):

*LANIF='**ensY**'*

Где

ensY – интерфейс сервера CA, которому при установке ОС был присвоен приватный IP-адрес.

- Выполнить команду:

```
# for file in $(find /usr/lib/systemd/ -type f -name '*openvpn*');do sed -i -e 's/ProtectHome=true/ProtectHome=read-only/g' $file ;done
```

- Завершение настройки *openvpn.*

В конце настройки ввести команды перезагрузки конфигурации менеджера systemd, включения запуска при загрузке и немедленного запуска службы *openvpn*:

```
# systemctl daemon-reload
# systemctl enable openvpn
# systemctl start openvpn
```

- Перезагрузить сервер CA.

1.3 Первичная проверка корректной установки ПО «Агрегатор нагрузки»

Проверка корректной установки ПО заключается в выводе листинга процессов на вновь установленном / обновленном сервере.

Для этого следует зайти по SSH с уровнем доступа root на ВМ CA и запустить указанную команду для вывода листинга процессов:

```
# netstat -lptun
```

Пример вывода процессов корректно работающего CA:

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	178.177.17.235:8521	0.0.0.0:*	LISTEN	1318587/fotelvpn
tcp	0	0	127.0.0.1:2601	0.0.0.0:*	LISTEN	489/zebra
tcp	0	0	0.0.0.0:1194	0.0.0.0:*	LISTEN	1318556/openvpn
tcp	0	0	127.0.0.1:2604	0.0.0.0:*	LISTEN	554/ospfd
tcp	0	0	192.168.12.4:22	0.0.0.0:*	LISTEN	652/sshd: /usr/sbin
tcp	0	0	127.0.0.1:2616	0.0.0.0:*	LISTEN	565/static
tcp	0	0	0.0.0.0:10050	0.0.0.0:*	LISTEN	3062138/zabbix_agen
udp	0	0	0.0.0.0:40403	0.0.0.0:*		1318587/fotelvpn
udp	0	0	192.168.12.4:1812	0.0.0.0:*		648/fotelradius
udp	0	0	192.168.12.4:1813	0.0.0.0:*		648/fotelradius

Наличие всех указанных процессов говорит о том, что CA работает корректно.

***Примечание**: процесс iperf3 может отсутствовать непосредственно после установки СА, поскольку запускается вручную, либо с помощью ЦУ при задействовании утилиты проверки скорости канала.*

***Примечание**: Более глубокая проверка состоит в подключении к СА Маршрутизатора БН (и появление на СА интерфейса ftap0). Однако данная процедура подразумевает, что как минимум установлены, настроены и работают серверы авторизации/аккаунтинга, DNS и ЦУ, настроены услуги на СА. Настройка серверов DNS, ЦУ и услуг рассмотрена в документе «Инструкция по установке СА и DNS из образа виртуальной машины и их настройке».*

1.4 Обновление ПО «Агрегатор нагрузки» из репозитория

ВНИМАНИЕ! *В данной главе приводится описание процедуры обновления ПО уже установленного и/или функционирующего СА.*

Обновление ПО СА подразумевает объявление репозитория «ФОТЕЛ» (если это еще не сделано).

Для того, чтобы прописать репозиторий «ФОТЕЛ» для обновления ПО СА необходимо:

1) ***Создать файл на сервере СА:***

nano /etc/apt/sources.list.d/fotelrepo.list

2) ***В данном файле прописать:***

для СА на основе Debian 11

deb [trusted=yes] https://repo.fotel.pro/bullseye fotel main non-free

3) ***Создать файл на СА:***

nano /etc/apt/auth.conf.d/fotel.conf

4) ***В данном файле прописать:***

machine *repo.fotel.pro*

login *username*

password *password*

где *username и password – пара логин/пароль, выделенная для доступа Клиента* к репозиторию

5) **Выполнить команду, чтобы изменить права доступа к файлу:**

chmod 600 /etc/apt/auth.conf.d/fotel.conf

6) ***Далее использовать стандартные средства Linux для обновления пакетов:***

apt-get update

apt-get install <имя-пакета>

Наиболее ключевыми пакетами являются следующие:

- fotelradius
- fotelstats
- fotelvpn
- fotelvpnconsole

Эти пакеты следует обновлять в первую очередь, используя сведения о них, изложенные в пункте.4.2 данной Памятки.

Проверить версию пакетов, доступных в репозитории, можно командой (после *apt-get update)*:

apt-cache show <имя пакета>

1.5 Утилита для настройки сервера агрегации aggregatorconfig

1.5.1 Общие сведения

Для частичной автоматической настройки сервера агрегации используется специализированная утилита **aggregatorconfig**. Утилита устанавливается на СА и при работе обращается к заранее созданным файлам *json*, содержащих конфигурацию (текущую и/или с изменениями) и осуществляет соответствующую настройку СА. Файлы желательно поместить в папку с утилитой.

Результаты своей работы (в том числе сообщения об ошибках в конфигурационном файле *json*) утилита записывает в системный лог-файл */var/log/syslog*.

Примечание: *Конфигурация применяется сразу и перезагрузки СА не требуется.*

Использование утилиты:

aggregatorconfig <options>

где <options> это:

-h, --help : выводит на экран помощь

-d, --changes <path to file> : считывает конфигурационный файл с изменениями и вносит изменения в систему

-c, --config <path to file> : считывает конфигурационный файл и вносит изменения в систему

-s, --service: запустить как сервис, обеспечивает включение mptcp только на нужных интерфейсах

1.5.2 Варианты работы утилиты

Примечание*: по умолчанию утилита устанавливается как сервис, ручного взаимодействия (опция «–c») с конфигурационными файлами утилиты не требуется.*

Использование утилиты подразумевает два варианта применения.

Вариант 1. Первичная настройка, используется при установке нового СА с помощью файла ***/etc/aggregatorconfig/config.json***.

После перезагрузки сервера или старта/рестарта сервиса утилита автоматически прочитает конфиг-файл и применит настройки.

Вариант 2. Если надо внести изменения на уже работающем СА, т.е. добавить/удалить те или иные секции конфиг-файла и применить изменения с помощью файла ***/etc/aggregatorconfig/changes.json***.

В этом случае (когда файл ***changes.json*** уже сформирован) необходимо вручную перезапустить сервис:

```
# systemctl reload aggregatorconfig
```

Утилита прочитает конфиг-файл с изменениями, внесет правки из него в основной конфигурационный файл и немедленно применит настройки.

1.5.3 Файл с начальной конфигурацией /etc/aggregatorconfig/config.json

Общее описание секций файла

Секция	**Описание**
"wan":"ensXX.XXX"	Обязательное поле, имя интерфейса, который принимает соединения fotelvpn
"ospf":{}	Опциональная секция, используется для настройки OSPF
"zero_vrf_networks":[]	Опциональная секция, массив сетей, публичные IP-адреса, для которых маршрутизация осуществляется через PBR
"networks_for_nat":[]	Опциональная секция, массив сетей, для которых включен NAT
"snmp_traps_target":[]	Опциональная секция, массив сетей и серверы, куда отсылаются копии SNMP-трапов
"entrusted_networks":[]	Опциональная секция, массив доверенных сетей, с которых можно подключаться к CA
"service_vlans": []	Опциональная секция, массив объектов с описанием сервисных vlan
"vrfs":[]	Опциональная секция, массив объектов с описанием vrf

Развернутое описание секций приведено ниже.

ВАЖНО! *Значения полей в секциях и конкретные данные (адреса, сети, порты и т.д.), указанные ниже в конфигурациях, служат <u>только</u> в качестве наглядного примера.*

После редактирования обязательно проверить синтаксис отредактированного файла /etc/aggregatorconfig/config.json командой:

```
# jq '.' /etc/aggregatorconfig/config.json
```

Секция "ospf"

"ospf":{

"manage_vrfs":true, *# опционально, возможные значения true/false; по дефолту false, если true, то при добавлении vrf автоматически прописывается конфигурация для frr ospfd*

"default_network": "192.168.12.0/24", *# опционально, используется для дефолтной настройки ospfd, указывается сеть ВМ, на которой разворачивается CA*

"lan": "ens34" *# опционально, используется для дефолтной настройки ospfd, интерфейс ВМ, вписывается во всех блоках где необходимо*

}

Секция "zero_vrf_networks"

```
"zero_vrf_networks":[
 {
        "networks":[                  # обязательно, массив сетей
        "81.200.10.224/27",
        "72.202.10.0/24"
      ],
      "interface":"ens34",              # опционально, имя интерфейса
        "vlan":123,                     #  опционально
      "address":"10.0.1.3", # опционально, адрес, который присваивается интерфейсу
      "mask":"255.255.255.0",  #опционально, сеть, которая присваивается интерфейсу
      "gateway":"10.0.1.4",          #обязательно, шлюз для маршрутизации
      "table":100                    #обязательно, номер таблицы
 },
 {
        "networks":[                  #обязательно, массив сетей
        "83.220.0.0/27"
      ],
        "gateway":"10.0.0.4",         #обязательно, шлюз для маршрутизации
      "table":101                     #обязательно, номер таблицы
 }
]
```

Секция "networks_for_nat"

```
"networks_for_nat":[                  #массив сетей для которых включен NAT
   "10.15.0.0/16",
   "192.168.10.0/24",
   "192.168.90.0/20"
]
```

#iptables -t nat -A POSTROUTING -s {$network} -j SNAT -o {$wan} --to-source {$wan_ip}

Секция "snmp_traps_target

```
"snmp_traps_target":[
```

```
        {
                "network": "192.168.90.0/20",      # обязательно, сеть источник трапов
                "server":  "192.168.12.3"     # обязательно, сервер, куда отсылается копия трапа
        },
        {
                "network": "192.168.1.0/22",
                "server": "1.1.1.5"
        }
       ]
#iptables -t mangle -A PREROUTING -s {$network} -p udp --dport 162 -j TEE --gateway {$server}
```

Секция "entrusted_networks"

```
"entrusted_networks":[          # массив доверенных сетей, с которых можно подключаться к CA через WAN
    "200.20.100.16/28",
    "90.200.100.0/23"
]
#iptables -A INPUT -i {$wan} -p tcp -s {$network} -m state --state NEW,ESTABLISHED -j ACCEPT
```

Секция "service_vlans"

```
"service_vlans": [              #  массив объектов с описанием сервисных vlan
 {
        "interface": "ens34",     #обязательно, имя интерфейса
        "svlan":1001              #обязательно, номер сервисного vlan
 },
 {
        "interface": "ens34",
        "svlan":1002
 }
]
```

Секция "vrfs"

```
"vrfs":[                        # массив объектов с описанием vrf
   {
      "vrf":"customer_vrf",           # обязательно, имя vrf
```

```
        "interface":"ens34",        # обязательно, имя интерфейса
            "vlan":2000,            #  обязательно, номер vlan
        "address":"10.0.0.1",   # обязательно, адрес интерфейса который будет
                                    установлен
        "mask":"255.255.255.0",     # обязательно, маска сети для интерфейса
        "table":100                 # обязательно, номер таблицы маршрутизации
    }
]
```

1.5.4 Файл с изменениями конфигурации /etc/aggregatorconfig/changes.json

Общее описание секций файла

Секция	Описание
"delete": {}	опционально, секция на удаление. Содержание секции полностью аналогично исходному конфиг-файлу, кроме поля WAN и секции OSPF (они не поддерживаются). А объекты секций VRF и zero_vrf_networks имеют упрощенный вид
"add": {}	опционально, секция на добавление. Содержание секции полностью аналогично основному конфиг-файлу, кроме поля WAN и секции OSPF (они не поддерживаются). (пример представлен в файле ниже в п.4.5.6)

После редактирования обязательно проверить синтаксис отредактированного файла /etc/aggregatorconfig/changes.json командой:

```
# jq '.' /etc/aggregatorconfig/changes.json
```

Описание секций для «delete»

Представлены поля, отличающиеся от начального конфиг-файла, другие поля идентичны ему.

```
"vrfs":[                    # массив объектов с описанием vrf на удаление
    {
        "vrf":"customer_vrf",       #обязательно, имя vrf
    }
]

"zero_vrf_networks":[       # массив объектов с описанием zero_vrf на удаление
```

```
 {
      "gateway":"10.0.1.1",  # обязательно, шлюз для маршрутизации
      "table":100            #обязательно, номер таблицы
 },
 {
         "gateway":"10.0.1.2",  # обязательно, шлюз для маршрутизации
      "table":101               #обязательно, номер таблицы
 }
]
```

Описание секций для «add»

Для секции «add» актуальны тип и вид секций из файла начальной конфигурации, следует пользоваться им (п.п.4.5.3).

1.5.5 Пример файла начальной конфигурации

```
{
  "wan":"ens192",
  "ospf":{
    "manage_vrfs":true,
    "default_network": "192.168.12.0/24",
    "lan": "ens34"
  },
  "zero_vrf_networks":[
    {
      "networks":[
        "80.200.10.224/27",
        "70.200.10.0/24"
      ],
      "interface":"ens34",
          "vlan":123,
      "address":"10.0.1.3",
      "mask":"255.255.255.0",
      "gateway":"10.0.1.4",
      "table":100
    }
  ],
  "networks_for_nat":[
    "10.10.0.0/16",
    "192.168.10.0/24",
    "192.168.90.0/20"
  ],
  "snmp_traps_target":[
        {
              "network": "192.168.90.0/20",
              "server": "192.168.12.3"
```

```
            },
            {
                    "network": "192.168.90.0/22",
                    "server": "1.1.1.5"
            }
    ],
    "entrusted_networks":[
       "200.20.100.16/28",
       "90.200.100.0/23"
    ],
    "service_vlans": [
            {
                    "interface": "ens34",
                    "svlan":1111
            },
            {
                    "interface": "ens34",
                    "svlan":1112
            }
   ],
    "vrfs":[
      {
        "vrf":"customer_vrf",
        "interface":"ens34",
            "vlan":2071,
        "address":"10.0.1.7",
        "mask":"255.255.255.0",
        "table":100
},
       {
          "vrf": "gars_test",
          "interface": "ens34",
          "vlan": 2072,
          "address": "10.0.1.8",
          "mask": "255.255.255.0",
          "table": 101
       }
    ]
}
```

1.5.6 Пример файла с изменениями конфигурации

```
{
  "delete": {
     "zero_vrf_networks":[
             {
                     "gateway":"10.0.1.4",
                     "table":100
             }
     ],
     "networks_for_nat":[
```

```
            "10.10.0.0/16"
        ],
        "snmp_traps_target":[
                {
                        "network": "192.168.90.0/20",
                        "server": "2.2.2.1"
                }
        ],
        "entrusted_networks":[
            "200.20.100.10/28"
        ],
        "service_vlans": [
                {
                        "interface": "ens34",
                        "svlan":1111
                }
        ],
        "vrfs":[
                {
                        "vrf":"customer_vrf"
                }
        ]
    },
    "add": {
            "entrusted_networks":[
              "200.40.100.30/28"
         ],
            "service_vlans": [
                {
                        "interface": "ens22",
                        "svlan":1234
                }
         ],
            "vrfs":[
                 {
                         "vrf":"customer_vrf1",
                         "interface":"ens34",
                         "vlan":3001,
                         "address":"10.0.1.7",
                         "mask":"255.255.255.0",
                         "table":100
                 }
        ]
    }
}
```