Содержание

4 FastPCRF settings for radius servers

Radius servers within the radius_server list are unequal: the first one is considered to be the main Radius server, whereas the rest are considered to be as backup servers. If FastPCRF detects that the main Radius server is not responding for a long time, the corresponding will be reset and FastPCRF will connect to the next radius server from the list. However, the FastPCRF periodically attempts to connect to the main radius server until it becomes available.

Parameter	Format	Default value	Description
default_reject_policing	string	no	The default policing profile name for unauthorized users
default_reject_whitelist	string	no	Service 5 (White list) profile name used by default for unauthorized users.
radius_revive_period	seconds	120	Periodicity of the reconnection to the main Radius server.
radius_max_pending_requests	number	1000000	The maximum number of pending requests from the FastDPI servers. When this threshold is exceeded, the incoming requests from the FastDPI servers will not be handled.
coa_max_pending_requests	number	100000	The maximum number of pending CoA requests from the Radius servers. This value should not be higher than the value of the `async_queue_size` parameter; the recommended value should not be more than `async_queue_size` / 2.

Parameter	Format	Default value	Description
radius_server	secret@ip%dev:port{;param=value}*	no	Specifies a single Radius server and its configuration parameters: `secret` - the secret of the Radius server; IP - the Radius server IP address; dev (optional) - the name of the interface used to establish connection; if it is not specified, then the interface will be selected by the operating system; `port` is the port; `param=value` is the configuration parameters (via semicolon) for a given Radius server. See Radius_server parameter description

Описание параметра radius_server

Каждый Radius-сервер в конфигурационном файле описывается отдельным параметром radius_server. Обычно задается как минимум два radius-сервера – основной и резервный, в этом случае должно быть как минимум две строки с параметром radius_server – для основного и резервного серверов. Максимальное число radius-серверов – 16. Главным считается тот radius-сервер, который описан первым, остальные считаются резервными. Резервные сервера используются при недоступности главного и именно в той последовательности, в которой они описаны. В каждый момент времени активным является только один radius-сервер.

Конфигурационные параметры radius-сервера могут быть заданы тремя способами:

1. Значения, одинаковые для всех Radius-серверов, задаются как обычные параметры в файле fastpcrf.conf. Основное условие – они должны быть заданы перед параметрами radius_server, - только в этом случае они применяются ко всем radius-серверам.
2. Для каждого radius-сервера может быть создан свой конфигурационный файл, имя которого задается параметром conf в строке radius_server, например:

   ```
   radius_server=secret@10.10.3.5:1812;conf=radius-main.conf
   ```

   В этом примере значения из radius-main.conf имеют приоритет перед значения общих для Radius-серверов параметров.

3. Параметры, уникальные для конкретного radius-сервера, могут быть заданы прямо в строке radius_server, например:

```
radius_server=secret@10.10.3.5:1812;conf=radius-
main.conf;msg_auth_attr=1
```

В этом примере параметр msg_auth_attr задан для конкретного сервера 10.10.3.5 и перекрывает значение соответствующего параметра в файле конфигурации radius-main.conf. Следует учитывать, что порядок перечисления в radius_server важен: параметры применяются именно в том порядке, как они указаны в radius_server. Если в примере выше поменять местами conf и msg_auth_param и в конфигурационном файле radius-main.conf задано msg_auth_param=0, то будет применен msg_auth_param=0 из radius-main.conf.

Индивидуальные параметры Radius-серверов

Параметр в fastpcrf.conf	Параметр в radius_server	Формат	Значение по умолчанию	Описание
radius_dead_timeout	dead_timeout	секунды	60	Если в течение этого периода времени от radius-сервера не пришло ни одного ответа, а запросы есть, то сервер считается умершим и FastPCRF переключается на следующий radius-сервер из списка. Если умер главный radius-сервер, то начинается отчет radius_revive_period по окончанию которого будет произведена попытка переподключения.
radius_max_connect_count	max_connect_count	число	16	Максимальное число коннектов к одному radius-серверу. Согласно RFC 2865, под идентификатор, позволяющий сопоставить запрос с ответом, отводится поле размером 1 байт, то есть одно соединение может одновременно обслуживать не более 256 запросов. Для преодоления этого ограничения спецификация предлагает создавать несколько подключений к одному radius-серверу. Фактически этот параметр задает число одновременных запросов к одному radius-серверу: radius_max_connect_count * 256.

Параметр в fastpcrf.conf	Параметр в radius_server	Формат	Значение по умолчанию	Описание
radius_response_timeout	response_timeout	секунды	30	Тайм-аут ожидания ответа на запрос Access-Request к radius-серверу. Если в течение этого времени ответ на запрос не пришел, запрос считается отброшенным radius-сервером (например, по причине “слишком много запросов”) и fastpcrf пытается послать запрос заново.
radius_resend_count	resend_count	число	0	Максимальное количество попыток повторной отправки запроса. Если число попыток повторной отправки запросов исчерпано и ответ от radius-сервера не получен, fastpcrf ничего не сообщает fastdpi-серверу. Fastdpi в случае отсутствия ответа на авторизацию в течение определенного тайм-аута (параметр auth_resend_timeout файла fastdpi.conf) пошлет повторный запрос на авторизацию.
radius_status_server	status_server	булев тип	1	Параметр, поддерживает ли radius-сервер запрос Status-Server из RFC 5997. Данный тип запроса используется fastpcrf для пинга radius-сервера, особенно в случае временной недоступности основного radius-сервера. Без поддержки Status-Server понять, что основной radius-сервер восстановился, весьма затруднительно.
radius_user_password	user_password	строка	VasExperts.FastDPI	Значение атрибута User-Password запроса Access-Request.

Параметр в fastpcrf.conf	Параметр в radius_server	Формат	Значение по умолчанию	Описание
radius_user_name_auth	user_name_auth	строка	login,ip,qinq	Начиная с версии СКАТ 7.4, в fastpcrf.conf параметр radius_user_name_auth задает значение атрибута User-Name в порядке предпочтения: login - использовать логин абонента ip - использовать IP-адрес абонента qinq - использовать QinQ-тег в формате «outerVLAN.innerVLAN»; например, «101.205»
radius_unknown_user	unknown_user	строка	VasExperts.FastDPI.unknownUser	Логин пользователя, если настоящий логин неизвестен FastDPI. Это значение атрибута User-Name запроса Access-Request, если radius_user_name_ip=0 и логин пользователя неизвестен. Предполагается, что radius-сервер в ответе Access-Accept сообщит истинный логин пользователя, определенный по его IP-адресу, взятому из атрибута Framed-IP-Address. Следует учитывать, что данный параметр тесно связан с параметром radius_user_name_auth и применяется, только если никакой способ задания атрибута User-Name не применим.
radius_unknown_user_psw	unknown_user_pws	строка	VasExperts.FastDPI	Значение атрибута User-Password для неизвестного логина пользователя. Применяется только если radius_user_name_ip=0.

Параметр в fastpcrf.conf	Параметр в radius_server	Формат	Значение по умолчанию	Описание
radius_msg_auth_attr	msg_auth_attr	булев тип	1	Параметр, поддерживает ли radius-сервер атрибут Message-Authenticator из RFC 2869. Если атрибут поддерживается, FastPCRF будет вычислять и включать Message-Authenticator в каждый запрос Access-Request и Status-Server, а также анализировать этот атрибут в ответах; если в ответе проверка атрибута Message-Authenticator заканчивается ошибкой, то такой ответ отбрасывается.
radius_attr_nas_port_type	attr_nas_port_type	число	5 (Virtual)	Значение атрибута NAS-Port-Type (RFC 2865) запроса Access-Request.
radius_attr_nas_ip_address	attr_nas_ip_address	IPv4-адрес	нет	Значение атрибута NAS-IP-Address из RFC 2865 запроса Access-Request. Если не задан – атрибут NAS-IP-Address не включается в запрос.
radius_attr_nas_id	attr_nas_id	строка	нет	Значение атрибута NAS-Identifier запроса Access-Request. Согласно RFC2865, либо NAS-IP-Address, либо NAS-Identifier должен быть задан в Access-Request.
radius_attr_service_type	attr_service_type	число	2 (Framed)	Значение атрибута Service-Type из RFC 2865 запроса Access-Request.
radius_attr_cui	attr_cui	булев тип	1	Параметр, поддерживает ли radius-сервер атрибут Chargeable-User-Identity (CUI) из RFC 4372. Если этот атрибут поддерживается, то FastPCRF в запросе Access-Request помещает в этот атрибут логин пользователя; если логин неизвестен, то в атрибут помещается нулевой байт, что означает, согласно RFC 4372, запрос логина у radius-сервера. В ответе Access-Accept FastPCRF ожидает прихода в этом атрибуте истинного логина пользователя, который radius-сервер может определить по его IP-адресу (атрибут Framed-IP-Address запроса).

Параметр в fastpcrf.conf	Параметр в radius_server	Формат	Значение по умолчанию	Описание
radius_coa_port	coa_port	UDP-порт	3799	UDP-порт, на который поступают Change-of-Authorization (CoA) оповещения Disconnect-Request, CoA-Request из RFC 5176. Если radius-сервер не поддерживает CoA, следует задать этому параметру значение 0.
radius_coa_resend_timeout	coa_resend_timeout	секунды	1	Тайм-аут перепосылки CoA-ответов (Disconnect-ACK, Disconnect-NAK, CoA-ACK, CoA-NAK) в случае проблем с сокетом (обычно переполнение очереди сокета). Количество повторных попыток задается параметром radius_resend_count.
coa_reauth_ack	coa_reauth_ack	булев тип	0	Как отвечать на CoA-Request с Service-Type=8 (Authenticate-Only): 0 (значение по умолчанию) - по RFC5176 p.3.2: отвечать CoA-NAK с Error-Cause=507 (Request Initiated) 1 - нестандартное поведение: отвечаем CoA-ACK