

Содержание

4 FastPCRF settings for radius servers 3

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 <code>async_queue_size</code> parameter; the recommended value should not be more than <code>async_queue_size / 2</code> .

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 the Radius_server parameter description

Radius_server parameter description

Each Radius server is described by a separate radius_server parameter in the configuration file. At least two radius servers are typically specified: the primary Radius server and the backup one, it implies that there must be at least two lines with the radius_server parameter, i.e. one line for the primary Radius server and second one - for the backup servers. The maximum number of Radius servers is 16. The Radius server specified in the configuration file in the first place is considered as the main server, whereas the rest ones (specified within the configuration file later on) are considered the backup ones. Backup servers are used when the main one is unreachable in the order in which they are specified within the conf file. At any given moment, only one Radius server is active.

The configuration parameters of the radius server can be specified in three ways:

1. Values that are the same for all the Radius servers - they are specified as normal parameters in the fastpcrf.conf file. The main idea is that they must be specified before the radius_server parameters, only in this case they will be applied to all the Radius servers.
2. You can create your own configuration file for each radius-server, whose name is specified by the conf parameter within the radius_server line, for example:

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

In this example, the values from radius-main.conf take precedence over the values of common Radius servers parameters.

3. Parameters unique to a given radius server can be specified explicitly in the radius_server line, for example:

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

In this example, the `msg_auth_attr` parameter is specified for a given 10.10.3.5 server and overrides the value of the corresponding parameter in the `radius-main.conf` configuration file. Note that the order in which the parameters appear within the `radius_server` line is very important: the parameters will be applied following the exact order they are specified in the `radius_server` line. If you invert `conf` and `msg_auth_param` in the example above and if `msg_auth_param=0` within the `radius-main.conf` configuration file, then `msg_auth_param=0` will be used from `radius-main.conf` instead.

Индивидуальные параметры Radius-серверов

Параметр в <code>fastpcrf.conf</code>	Параметр в <code>radius_server</code>	Формат	Значение по умолчанию	Описание
<code>radius_dead_timeout</code>	<code>dead_timeout</code>	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 <code>radius_revive_period</code> по окончании которого будет произведена попытка переподключения.
<code>radius_max_connect_count</code>	<code>max_connect_count</code>	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: <code>radius_max_connect_count * 256</code> .

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 р.3.2: отвечать CoA-NAK с Error-Cause=507 (Request Initiated) 1 - нестандартное поведение: отвечаем CoA-ACK