Содержание

4 FastPCRF settings for RADIUS servers

The RADIUS servers from the radius_server list are not equal: the first is considered to be the main RADIUS server, whereas the rest ones are considered to be backup. If FastPCRF detects that the main RADIUS server is not responding too long, the connection with it will be dropped and FastPCRF will establish connection with the next radius server from the list. At the same time, periodic attempts to connect to the main radius server until the main radius server becomes available are made.

Paramenter	Format	Default value	Description
default_reject_policing	string	no	The default policing profile name for unauthorized users
default_reject_whitelist	string	no	Profile name of the service 5 (White List) is used by default for unauthorized users.
radius_revive_period	seconds	120	A new attempt to connect to the main RADIUS server would be made after the expiring of this period.
radius_max_pending_requests	number	1000000	The maximum number of pending requests from the FastDPI servers. If this threshold is exceeded, incoming requests from the FastDPI servers will not be processed
coa_max_pending_requests	number	100000	The maximum number of pending CoA requests being sent 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 greater than `async_queue_size / 2`.

Paramenter	Format	Default value	Description
radius_server	secret@ip%dev:port{;param=value}*	no	Specifies a single radius server and its configuration settings: `secret` - the secret of the RADIUS server; `ip` - the IP address of the RADIUS server; `dev` (optional) is the interface name used to establish the connection; if not specified, the interface will be chosen by the operating system; `port` - port; `param=value` - a semicolon separated list of the configuration parameters for this radius server. See the radius_server setting desctiption

radius_server setting desctiption

Each RADIUS server in the configuration file is described by an individual `radius_server` setting . Typically, at least two RADIUS servers are specified - the main and the backup one, in this case there should be at least two lines with the `radius_server` settings - for the main and backup servers. The maximum number of radius servers is 16. The main one is considered those RADIUS server that is described first in the configuration file, the rest are considered to be backup ones. Backup servers are used when the main server is unavailable and the way they will be used is specified by the order their descriptions appears in the configuration file. Only one radius server is active at a time.

The RADIUS server configuration parameters can be specified in three ways:

1. The values that are the same for all RADIUS servers are specified as normal parameters in the fastpcrf.conf file. The basic condition is that they have to be specified before the `radius_server` parameters; only in this case they will be applied to all the RADIUS servers.
2. An individual configuration file for each RADIUS server can be created, its name is specified by the `conf` parameter in the `radius_server` line, for example:

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

   In the example above the values from `radius-main.conf` have priority over the values of general RADIUS server parameters.

3. Parameters that are unique to a specific RADIUS server can be specified directly within 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 the 10.10.3.5 server and overrides the value of the corresponding parameter from the `radius-main.conf` configuration file. Note that the order in which the RADIUS server parameters appear in `radius_server` line is important: the parameters(settings) will be applied exactly in accordance with the order they were specified within the `radius_server` lint. If we swap `conf` and `msg_auth_param` in the example above and set `msg_auth_param=0` in the `radius-main.conf` configuration file, then `msg_auth_param=0` from radius-main.conf will be applied.

Individual RADIUS server parameters

Parameter from fastpcrf.conf	Parameter from radius_server	Format	Default value	Description
radius_dead_timeout	dead_timeout	seconds	60	If during this period of time there is no any response from the RADIUS server, but requests are sending, then the server is considered to be dead and FastPCRF switches to the next RADIUS server from the list. If the main RADIUS server has died, then the counting down from the `radius_revive_period` will be started, after expiring of which a new connection attempt will be made.
radius_max_connect_count	max_connect_count	number	16	Maximum number of connections to one RADIUS server. According to RFC 2865, an identifier allowing you to match a request with a response is allocated in a 1-byte field, that is, one connection can simultaneously maintain no more than 256 requests. To overcome this limitation, the specification suggests to create several connections to a single RADIUS server. In fact, this parameter specifies the number of simultaneous requests to one RADIUS server: `radius_max_connect_count` * 256.

Parameter from fastpcrf.conf	Parameter from radius_server	Format	Default value	Description
radius_response_timeout	response_timeout	seconds	30	Timeout specifying the time period to wait for a response to an Access-Request request being sent to a RADIUS server. If the `radius_response_timeout` has expired and the response to the request has not been received, then the request is considered to be dropped by the RADIUS server (for example, due to "the maximum number of requests allowed is reached") and fastpcrf tries to send the request again.
radius_resend_count	resend_count	number	0	Maximum number of attempts to resend requests. If this number is exhausted and the response from the RADIUS server is not received, then fastpcrf does not report anything to the fastdpi server. If there is no response to the authorization request within a specified timeout (the auth_resend_timeout parameter of the fastdpi.conf file) then the Fastdpi will repeat its authorization request.
radius_status_server	status_server	boolean type	1	The parameter specifying whether the RADIUS server supports the Status-Server request defined in RFC 5997. This request type is used by fastpcrf to ping the RADIUS server, especially if the main radius server is temporarily unavailable. If there is no Status-Server support, it is very difficult to understand that the main RADIUS server became available.
radius_user_password	user_password	string	VasExperts.FastDPI	The value of the `User-Password` attribute of the Access-Request request.
radius_user_name_auth	user_name_auth	string	login,ip,qinq	Starting from the VAS Experts DPI version 7.4, the `radius_user_name_auth` parameter from the fastpcrf.conf specifies the value of the `User-Name` attribute in the order of preference: login - use the subscriber login; ip - use the subscriber IP address; qinq - use the QinQ tag using the following format “outerVLAN.innerVLAN”; for example, "101.205"

Parameter from fastpcrf.conf	Parameter from radius_server	Format	Default value	Description
radius_unknown_user	unknown_user	string	VasExperts.FastDPI.unknownUser	User login in case the real login is unknown to FastDPI. This is the value of the `User-Name` attribute of the `Access-Request` request in case the `radius_user_name_ip=0` and the user login is unknown. It is assumed that the RADIUS server within the `Access-Accept` response will send the real user login identified by its IP address extracted from the `Framed-IP-Address` attribute. Note that this parameter is closely related to the radius_user_name_auth and will be used only if no way to specify the `User-Name` attribute is applicable.
radius_unknown_user_psw	unknown_user_pws	string	VasExperts.FastDPI	The value of the `User-Password` attribute for an unknown user login. It will be applied only if the `radius_user_name_ip=0`.
radius_msg_auth_attr	msg_auth_attr	boolean type	1	The parameter specifying whether the RADIUS server supports the `Message-Authenticator` attribute defined in RFC 2869. If the attribute is supported then FastPCRF will compute and include the `Message-Authenticator` in each `Access-Request` and `Status-Server` request along with analyzing this attribute in each response; if the `Message-Authenticator` (within response) attribute check fails, then the answer will be dropped.
radius_attr_nas_port_type	attr_nas_port_type	number	5 (Virtual)	The value of the NAS-Port-Type (RFC 2865) attribute of the Access-Request request.
radius_attr_nas_ip_address	attr_nas_ip_address	IPv4-адрес	no	The value of the NAS-IP-Address (RFC 2865) attribute of the Access-Request request. If not specified, the `NAS-IP-Address` attribute will not be added to the request.
radius_attr_nas_id	attr_nas_id	string	no	The value of the `NAS-Identifier attribute` of the Access-Request request. According to the RFC2865, either a `NAS-IP-Address` or a `NAS-Identifier` must be specified in the Access-Request.
radius_attr_service_type	attr_service_type	number	2 (Framed)	The value of the `Service-Type` attribute from RFC 2865 Access-Request.

Parameter from fastpcrf.conf	Parameter from radius_server	Format	Default value	Description
radius_attr_cui	attr_cui	boolean type	1	The parameter specifying whether the RADIUS server supports the `Chargeable-User-Identity` (CUI) attribute defined in RFC 4372. If this attribute is supported, then the FastPCRF puts the user login into this attribute within the Access-Request request; if the login is unknown, then the attribute will contains a zero byte, which implies, according to RFC 4372, a login request from the RADIUS server to be made. FastPCRF expects to get in the Access-Accept response the real user login, which the RADIUS server can determine by its IP address (the Framed-IP-Address attribute of the request).
radius_coa_port	coa_port	UDP port	3799	The UDP port used to receive the `Disconnect-Request` and`CoA-Request` (Change-of-Authorization Request) according to the RFC 5176. If the RADUIS server does not support CoA, this parameter should be set to 0.
radius_coa_resend_timeout	coa_resend_timeout	seconds	1	CoA-response timeout (Disconnect-ACK, Disconnect-NAK, CoA-ACK, CoA-NAK), is used in case of problems with the socket (usually due to socket queue overflow). The number of attempts to resend requests is specified by the `radius_resend_count` parameter.
coa_reauth_ack	coa_reauth_ack	boolean type	0	Specifies the way to respond to a CoA-Request with Service-Type=8 (Authenticate-Only): 0 (default value) - according to the RFC5176 p.3.2: Reply CoA-NAK with Error-Cause=507 (Request Initiated) 1 - non-standard behavior: CoA-ACK should be used as a response