Содержание

RADIUS CoA

CoA - Change of Authorization are notifications from the RADIUS server that the user properties have changed or that the user has become unauthorized.

CoA-Request нотификация говорит о том, что пользователь авторизован и, опционально, у него изменились некоторые параметры. Таким образом, CoA-Request может приходить в следующих случаях:

A CoA-Request notification tells you that the user is authorized and, optionally, has some parameters changed. Thus, CoA-Request can appear in the following cases:

- the user went from "not authorized" to "authorized" (for example, topped up the account) - see below;
- the authorized user's parameters have changed (enabling/disabling services, changing service profiles).

If the user is not authorized and his parameters are changed, a simplified CoA-Request must be generated, which actually instructs fastDPI to reauthorize the subscriber immediately, that is, to send an Access-Request.

Types of CoA:

1. Simplified CoA-Request - on receipt of the CoA fastDPI consideres the user's attributes have changed and re-authorization is required. Upon receiving such a notification, fastDPI sends a normal `Access-Request` request to the RADIUS server, as described here.
2. Full CoA-Request - the `CoA-Request` notification may contain the full list of changed user attributes.
3. Disconnect-Request - resets the authorization status of the user.

Notification types

Although the `CoA-Request` notification may contain a complete list of changed user attributes, it is suggested to use a simplified version of this notification.This allows the fastDPI to be informed that the user attributes have changed and require reauthorization. When such a message is received the fastDPI sends regular `Access-Request` request to the RADIUS server, as described earlier.

Simplified notification (request for reauthorization)

`CoA-Request` contains the following attributes:

- `Service-Type=8` (Authenticate-Only)
- `User-Name` – the username (login).
- one of the following attributes: `Framed-IP-Address`, `Framed-IPv6-Address` or `Framed-IPv6-Prefix` represents the subscriber IPv4 or IPv6 address
- VasExperts-L2-SubsId - L2-subscriber ID.

The preferred user identifier in CoA is its login. When processing CoA the fastDPI searches for the subscriber by login (`User-Name` or `VasExperts-UserName`). If the login is not found - it is an error. If the login is not specified in CoA, the fastDPI searches by the IP address. If the CoA contains both the login and the IP address, and the subscriber is found by its login, then the IP address is ignored: the fastDPI does not analyze whether the login and IP address are bound in the UDR database.

[SSG 7.5+] Starting from the VAS Experts DPI 7.5, it is possible to specify Acct-Session-Id as the subscriber ID. The Stingray SG searches for the subscriber IP address by `Acct-Session-Id` in its internal database and if succeeded then the SSG generates an internal reauthorization request by IP. `Acct-Session-Id` is the most "weak" among other identifiers: it is applied only when neither the login nor the IP address are specified in the CoA-request.

[SSG 8.3+] Instead of the `User-Name` attribute you can specify the subscriber's login in the `Chargeable-User-Identity` (CUI) attribute. In order for SSG to support CUI, you have to specify the following in fastpcrf.conf:

```
radius_attr_cui=1
```

The CUI attribute is not recommended for use in SSG because, according to RFC, it contains a hash of the subscriber's login, but not the login itself. SSG requires CUI to contain true login of the subscriber.

Response to the simplified notification

According to RFC5176, CoA-Request with Service-Type=8 (Authenticate-Only) should be responded with a CoA-NAK response containing the `Error-Cause=507` (Request Initiated) attribute. It's not always convenient since some utilities (for example, radclient from the FreeRADIUS package) treat the CoA-NAK response as an error. The fastPCRF has a `coa_reauth_ack` option that determines how to respond to the CoA-Request with Service-Type=8:

- 0 - standard behavior: to respond by CoA-NAK with Error-Cause=507
- 1 (the default value) - to respond by CoA-ACK

This option can be set in the fastpcrf.conf both globally for all RADIUS-servers and specifically for each RADIUS-server:

```
  # global settings
coa_reauth_ack=0

 # for this server the coa_reauth_ack = 0 global option is applied
radius_server=mysecret1@192.168.10.10%eth0
```

```
 # and for this one coa_reauth_ack = 1 option is explicitly specified
radius_server=mysecret2@192.168.20.10%eth0;coa_reauth_ack=1
```

CoA-Request full notification

Although this feature is supported by fastPCRF, it is not recommended to use because of potential implementation complexity: it should contain only changes in subscriber attributes (service list, etc.). For an authorized user, CoA-Request notification contains only changes to user parameters; the following attributes are supported:

- Name (login) of the user – one of the attributes `VasExperts-UserName`, `Chargeable-User-Identity` (CUI), `User-Name`
- one of the attributes `Framed-IP-Address`, `Framed-IPv6-Address`, `Framed-IPv6-Prefix` - IPv4/IPv6 address; this attribute is only used to search for the subscriber, if the login is not specified
- `VasExperts-Multi-IP-User` – sets the attribute to change whether one or many IP addresses are associated with this user. If the user becomes a multi-IP subscriber (i.e. many IP addresses can be associated with a single user), this attribute must be set to 1. If the user becomes single-IP, this attribute must be set to 0. If the "multi-IP" attribute of the user is not changed, CoA-Request must not contain VasExperts-Multi-IP-User attribute. No more than one of these attributes is allowed in a CoA-Request.
- `VasExperts-Policing-Profile` – the name of the policing profile for the user. This attribute should only be included if the user's policing profile has changed. No more than one `VasExperts-Policing-Profile` attribute is allowed in CoA-Request. If a client's policing profile needs to be deleted, the `VasExperts-Policing-Profile` attribute should be sent with an empty value (with an empty string). [SSG-9.6+] According to RFC 2865, string attributes cannot have an empty value; therefore, since version 9.6, the value `n/a` must be specified to delete a policing profile from a subscriber: `VasExperts-Policing-Profile=<n/a>`.
- `VasExperts-Enable-Service` – sets the change of service status: connected (on) or disconnected (off). CoA-Request contains all services whose connection status has changed. If some service is not contained in CoA-Request, it means that its "connected" status has not changed for the user. Each service that has changed status must be specified by a separate VasExperts-Enable-Service attribute, i.e. CoA-Request may contain zero or more VasExperts-Enable-Service attributes.
- `VasExperts-Service-Profile` – specifies the name of the new service profile (that is, a set of service parameters). If this service was disabled, it will be enabled (i.e. VasExperts-Service-Profile has a higher priority than VasExperts-Enable-Service). To disable a service with a set profile, the VasExperts-Enable-Service attribute must be set to "off" (for example, for service 5: VasExperts-Enable-Service="5:off"). Each service profile name change is specified by a separate VasExperts-Service-Profile attribute, that is, a CoA-Request may contain zero or more VasExperts-Service-Profile attributes.
- `Session-Timeout` – optional attribute, sets the authorization time in seconds. A value of 0 is ignored. After this time runs out, the user's authorization status is set to "unknown", which causes an Access-Request to be sent.

Disconnect-Request

The `Disconnect-Request` notification indicates that the user has become unauthorized (for example, the money have run out on the account). The Disconnect-Request notification can contain the following attributes:

- one of the following attributes: `Framed-IP-Address`, `Framed-IPv6-Address`, `Framed-IPv6-Prefix` representing the IPv4 of IPv6 subscriber address
- Username (login) – one of following attributes: `VasExperts-UserName`, `Chargeable-User-Identity` (CUI), `User-Name`
- `Acct-Session-Id` - accounting session identifier. The identifier is used by the Stingray SG to search within its internal database the IP address bound to this accounting sesstion.
- VasExperts-L2-SubsId - L2-subscriber ID.

When the Stingray SG receives the Disconnect-Request:

1. if the accounting is enabled it sends Accounting Stop containing the Admin-Reset cause (6)
2. for protocols that allow a session to be terminated by the server initiative (for example, PPPoE) - it terminates the session
3. sets the authorization state for the IP-address to the "unknown" state. This leads to the fact that when the packet is received from this IP, the Stingray Service Gateway will send the authorization request

If the Disconnect-Request specifies the subscriber login then these actions are applied to all the IP addresses associated with the login.

If after PoD (CoA Disconnect) no DHCP request is received before lease time expires, the session should be closed with deanonce and acct stop.
Note that the subscriber's session type may change from DHCP to StaticIP or PPPoE; in this case the DHCP session should be closed without deanonce and acct stop.

Flag to deny/allow sending acct stop

The `bras_dhcp_disconnect` option flags are used to provide flexibility in PoD processing, since quite a lot (max lease time / 2) of time and traffic can pass between PoD and the actual DHCP Discover reauthorization from the client:

- **0x0001** – `disable acct stop`, do not immediately send `acct stop` to a `disconnected` DHCP subscriber. Allows traffic after PoD to be counted. By default, the acct session is closed by PoD, which may result in unaccounted traffic for DHCP subscribers from PoD to DHCP reauthorization.
- **0x0002** – `disable L3 auth`, do not perform L3 auth for a `disconnected` DHCP subscriber. Stingray SG can authorize an L2 subscriber by its IP address with RADIUS support.
- **0x0004** – `block traffic` – block all traffic from the `disconnected` subscriber (i.e. on the `subs → inet` route). Attempt to reduce reauthentication time: many CPEs send DHCP ahead

of time when the Internet connection is down. But the price of this flag is the breaking of all existing subscriber sessions.
- **0x0008** – respond to DHCP Request with NAK. Allows you to shorten the reauthorization time by terminating the IP address lease.
- **0x0010** – ignore DHCP Request (wait for DHCP Discovery).

This option covers the following cases:

`bras_dhcp_disconnect=0` (default, as it is now):

- send acct stop
- the following DHCP request (Discover or Request) is sent to RADIUS
- reset the L3 session time, which results in an L3 auth on the first non-DHCP packet from the subscriber

=1: waiting for a DHCP request from a subscriber without traffic blocking, with L3 auth, without acct stop

- **do not** send acct stop
- the following DHCP request (Discover or Request) is sent to RADIUS
- reset the L3 session time, which results in an L3 auth on the first non-DHCP packet from the subscriber

=2, 3: waiting for a DHCP request from a subscriber without traffic blocking, without L3 auth

- send (2) / do not send (3) acct stop
- the following DHCP request (Discover or Request) is sent to RADIUS

=4, 5: waiting for a DHCP request from a subscriber with traffic blocking, L3 enabled. That is, packets from the subscriber are blocked, but L3 auth is performed on them.

- send (4) / do not send (5) acct stop
- the following DHCP request (Discover or Request) is sent to RADIUS
- reset the L3-reauthorization time, which leads to L3 auth on the first non-DHCP packet from the subscriber

=6, 7: (2 + 4) waiting for DHCP request from subscriber with traffic blocking, L3 disabled

- send (6) / do not send (7) acct stop
- the following DHCP request (Discover or Request) is sent to RADIUS
- traffic from the subscriber is dropped

=8, 9: waiting for DHCP request from subscriber without traffic blocking, L3 auth enabled

- send (8) / do not send (9) acct stop
- reset the L3-reauthorization time, which leads to L3 auth on the first non-DHCP packet from the subscriber
- DHCP Request – respond with NAK, DHCP Discover – send to RADIUS

=10, 11: (2 + 8) waiting for DHCP request from subscriber without traffic blocking, L3 auth disabled

- send (10) / do not send (11) acct stop
- DHCP Request – respond with NAK, DHCP Discover – send to RADIUS
- L3 auth disabled

=12, 13: (4 + 8) waiting for DHCP request from subscriber with traffic blocking, L3 auth enabled. That is, packets from the subscriber are blocked, but L3 auth is performed on them.

- send (12) / do not send (13) acct stop
- DHCP Request – respond with NAK, DHCP Discover – send to RADIUS
- traffic from the subscriber is dropped
- reset L3-reauthorization time, which leads to L3 auth on the first non-DHCP packet from the subscriber

=14, 15: (2 + 4 + 8): waiting for DHCP request from subscriber with traffic blocking, L3 auth disabled

- send (14) / do not send (15) acct stop
- DHCP Request – respond with NAK, DHCP Discover – send to RADIUS
- traffic from the subscriber is dropped
- L3 auth disabled

=16, 17: waiting for DHCP request from subscriber without traffic blocking, L3 auth enabled

- send (16) / do not send (17) acct stop
- reset L3-reauthorization time, which leads to L3 auth on the first non-DHCP packet from the subscriber
- DHCP Request is ignored (drop), DHCP Discover – send to RADIUS

=18, 19: (2 + 16) waiting for DHCP request from subscriber without traffic blocking, L3 auth disabled

- send (18) / do not send (19) acct stop
- DHCP Request is ignored (drop), DHCP Discover – send to RADIUS
- L3 auth disabled

=20, 21: (4 + 16) waiting for DHCP request from subscriber with traffic blocking, L3 auth enabled. That is, packets from the subscriber are blocked, but L3 auth is performed on them.

- send (20) / do not send (21) acct stop
- DHCP Request is ignored (drop), DHCP Discover – send to RADIUS
- traffic from the subscriber is dropped
- reset L3-reauthorization time, which leads to L3 auth L3 auth on the first non-DHCP packet from the subscriber

=22, 23: (2 + 4 + 16) waiting for DHCP request from subscriber with traffic blocking, L3 auth disabled

- send (22) / do not send (23) acct stop
- DHCP Request is ignored (drop), DHCP Discover – send to RADIUS
- traffic from the subscriber is dropped
- L3 auth disabled

All other values of bras_dhcp_disconnect are error.

Acct stop data will still be sent with any authorization (if auth/acct synchronization is enabled in PCRF).
Without sending acct stop, the DHCP subscriber does not understand if Disconnect is processed or not.

Individual CoA clients

The CoA client sending the Disconnect-Request and CoA-Request CoA requests in some configurations may be a separate entity that is not a RADIUS server. For example, it can be some utility used in scripts that can generate CoA requests. The fastpcrf supports such "stand-alone" CoA-clients. Each such CoA client is specified by a separate `coa_client` option in the fastpcrf.conf configuration file using a format similar to the `radius_server` option:

```
coa_client=secret@ip%dev:port{;param=value}*
```

- `secret` – the RADIUS secret;
- `ip` – CoA client IP address;
- `dev` (optional) – the name of the interface used to listen for incoming requests; if it is not specified then the interface is chosen by the operating system;
- `port` – the listened local port;
- `param=value` – the list (separated by semicolons) of the CoA client configuration options. The following options are supported: max_resend_count, msg_auth_attr, coa_resend_timeout.

Each CoA-client is described by separate `coa_client` parameter in the configuration file. There can be up to 16 separate CoA-clients. Fastpcrf accepts the CoA requests only from registered (described in the configuration file) RADIUS servers and CoA-clients. If the RADIUS server supports CoA there is no need to describe it using the `coa_client` parameter; it is enough to specify the `coa_port` suboption within the `radius_server` parameter for this RADIUS server.

Accounting session request using CoA

The VAS Experts DPI 8.2 adds a feature to request the state of the accounting session by a third-party system. It can be done This feature is implemented using CoA-Request containing the `VasExperts-Command-Code=1` attribute.

Check if session exists

The CoA-Request containing the following attributes will check if the specified accounting session exists.

```
VasExperts-Command-Code=1
Acct-Session-Id=A1B2C3D4E5F6
```

If successful, CoA-ACK will be returned with IP address this session belongs to:

```
# CoA-ACK attributes:
VasExperts-Command-Code=1
Acct-Session-Id=A1B2C3D4E5F6
    # SSG-8.3: multi-session ID attribute added
Acct-Multi-Session-Id=MA1B2C3D4E5F6
    # SSG-8.3: NAS-IP-Address attribute was added - by which fastDPI the
session was created
NAS-IP-Address=192.168.0.200
Framed-IP-Address=192.168.10.20
```

If the specified session does not exist (or it's inactive, for example, it is closed by idle timeout), the CoA-NAK with the following attributes will be returned:

```
# CoA-NAK attributes:
VasExperts-Command-Code=1
Acct-Session-Id=A1B2C3D4E5F6
Error-Cause=503 # Session Context not found
# The Error-Cause attribute can also take other values.
```

Accounting session request for given IP address

You can query the SSG for the active accounting session ID for a given IP address. The request structure differs for the cases "one fastPCRF - one fastDPI" and "one fastPCRF - several fastDPIs".

For the case "one fastPCRF - one fastDPI" CoA-Request looks like this:

```
VasExperts-Command-Code=1
Framed-IP-Address=192.168.10.20
```

For the case "one fastPCRF - multiple fastDPIs" in CoA-Request we need to specify which fastDPI we are interested in:

```
# CoA-ACK attributes
VasExperts-Command-Code=1
Framed-IP-Address=192.168.10.20
    # SSG-8.3: which fastDPI server
NAS-IP-Address=192.168.0.200
```

In principle, the NAS-IP-Address attribute (or NAS-Identifier) can be omitted if you are sure that this IP address is only on one fastDPI.

If there is an active accounting session for the specified IP address, the SSG will return a CoA-ACK with the session ID:

```
# CoA-ACK attributes
VasExperts-Command-Code=1
Framed-IP-Address=192.168.10.20
Acct-Session-Id=A1B2C3D4E5F6
    # SSG-8.3: multi-session ID attribute added
Acct-Multi-Session-Id=MA1B2C3D4E5F6
    # SSG-8.3: NAS-IP-Address attribute was added - by which fastDPI the
session was created
NAS-IP-Address=192.168.0.200
```

If there is no active session, CoA-NAK will be returned like the example below:

```
# CoA-NAK attributes
VasExperts-Command-Code=1
Framed-IP-Address=192.168.10.20
Error-Cause=503 # Session Context not found
# The Error-Cause attribute can also take other values.
```

SSG 12.4 — Added IPv6 support for CoA.
Command-Code=1 — search for acct session by IP.
An acct session can be searched by the Framed-IPv6-Prefix or Delegated-IPv6-Prefix IPv6 attribute prefix. The command response specifies all known IP addresses of the found acct session — Framed-IP-Address, Framed-IPv6-Prefix, Delegated-IPv6-Prefix.

Multi-session accounting session request

[SSG 8.3] You can use the multi-session ID to find out which IP address it corresponds to and what active session it has for the specified fastDPI:

```
   # CoA-Request Attributes
VasExperts-Command-Code=1
Acct-Multi-Session-Id=MA1B2C3D4E5F6
```

If this multi-session is found, the SSG will return the IP address that corresponds to this multi-session. In case the multi-session has only one active session, CoA-ACK will be returned:

```
# CoA-ACK Attributes
VasExperts-Command-Code=1
Framed-IP-Address=192.168.10.20
Acct-Session-Id=A1B2C3D4E5F6
```

```
Acct-Multi-Session-Id=MA1B2C3D4E5F6
    # which fastDPI has created the session
NAS-IP-Address=192.168.0.200
```

If there is no active session or more than one, a CoA-NAK will be returned with the subscriber's IP address:

```
# CoA-NAK Attributes
VasExperts-Command-Code=1
Acct-Multi-Session-Id=MA1B2C3D4E5F6
Framed-IP-Address=192.168.10.20
Error-Cause=503 # Session Context not found
# The Error-Cause attribute can take on other values as well.
```

We can specify in CoA-Request which fastDPI we are interested in:

```
   # CoA-Request Attributes
VasExperts-Command-Code=1
Acct-Multi-Session-Id=MA1B2C3D4E5F6
NAS-IP-Address=192.168.0.200
```

In this case, the SSG will return the subscriber's IP address and session ID if there is an active session for this fastDPI:

```
# CoA-ACK Attributes
VasExperts-Command-Code=1
Framed-IP-Address=192.168.10.20
Acct-Session-Id=A1B2C3D4E5F6
Acct-Multi-Session-Id=MA1B2C3D4E5F6
    # which fastDPI has created the session
NAS-IP-Address=192.168.0.200
```

If there is no active session for the specified fastDPI, the SSG will return CoA-NAK:

```
# CoA-NAK Attributes
VasExperts-Command-Code=1
Acct-Multi-Session-Id=MA1B2C3D4E5F6
NAS-IP-Address=192.168.0.200
Framed-IP-Address=192.168.10.20
Error-Cause=503 # Session Context not found
# The Error-Cause attribute can take on other values as well.
```