

InCommon eduroam Proxy Monitoring

Date: 9-Mar-2022

Version: 0.3

Executive summary

This paper presents a recommended solution to meet InCommon eduroam subscriber requirements for monitoring the status of the US eduroam top-level proxies. In this proposal, we recommend the use of the widely available, standards-based RADIUS Status-Server capability to monitor the health and availability of the top-level US RADIUS proxies. Status-Server is designed for monitoring the health and availability of RADIUS servers, and can be used without the need for user credentials on a remote Identity Provider (IdP).

Problem statement

US eduroam subscribers need a way to programmatically monitor the availability and health of the US eduroam top-level proxies (tlsr1.eduroam.us and tlsr2.eduroam.us).

Ideally, a proxy monitoring solution would have the following attributes:

- It should not be necessary for an eduroam subscriber to have user credentials from a remote IDP in order to determine the status of the top-level RADIUS proxies.
- Determining the status of the top-level RADIUS proxies should rely on as little other infrastructure as possible, to avoid false sharing and false negatives.
- Monitoring should use a widely-available, standards-based mechanism with a well-supported open source implementation.
- The monitoring mechanism should check availability and health of the RADIUS proxy, not just the network reachability of the proxy host.

Recommended solution

This document recommends that eduroam subscribers use Status-Server messages to monitor the US eduroam top-level proxies, rather than sending requests using user credentials from a remote IDP or using lower-level mechanisms, such as ICMP echo requests (i.e. "ping").

Status-Server messages are a standard RADIUS monitoring mechanism defined in RFC 5997 [RFC5997]. They allow an authorised monitoring system to query the availability and health of a RADIUS server without the need for a remote IDP or user credentials. The US eduroam top-level RADIUS proxies are configured to respond to Status-Server messages directly with an Access-Accept packet, as described in the standard. The only credential required to use the Status-Server mechanism is a valid RADIUS secret shared between the RADIUS server and the originator of the Status-Server requests. This secret can be configured by an eduroam administrator in the Federation Manager by configuring the monitoring host as a Service Provider (SP).

Comparison to RADIUS Access-Requests

There are several reasons why Status-Server messages are a cleaner solution for RADIUS proxy monitoring than the use of RADIUS Access-Request messages to a remote IdP:

- Status-Server messages do not contain user credentials and are not sent to an IdP.
 - o There is no requirement for remote user credentials;

- There are no false negative results when the IdP server is unreachable or non-responsive; and
- They avoid extended or false outage reports caused by proxy/IdP interactions, such as silently discarding requests to a home server that is considered “dead”.
- Status-Server responses may contain statistics that provide greater information about the health and status of the RADIUS server than an Access-Request authentication response.

Comparison to “ping”

The “ping” command can be used to determine if a particular host is available on the Internet. However, it has multiple failure modes that make it unsuitable for monitoring the availability of the US eduroam RADIUS proxies:

- The US eduroam servers are part of a complicated network topology within AWS. A successful ping response does not necessarily indicate that the RADIUS proxy container is running, at all.
- Even if you were able to ping the container’s IP address directly, response to a ping does not necessarily indicate that the RADIUS server is available and healthy.

FreeRADIUS “radclient”

The “radclient” tool in FreeRADIUS is a well-supported open source tool that can be used to send Status-Server messages and process their responses [RC-MAN, RC-MON].

```
echo "Message-Authenticator = 0x00, FreeRADIUS-Statistics-Type =
1, Response-Packet-Type = Access-Accept" | \
radclient -x tlrs1.eduroam.us status adminsecret

Received response ID 180, code 2, length = 140
FreeRADIUS-Total-Access-Requests = 3
FreeRADIUS-Total-Access-Accepts = 1
FreeRADIUS-Total-Access-Rejects = 0
FreeRADIUS-Total-Access-Challenges = 0
FreeRADIUS-Total-Auth-Responses = 1
FreeRADIUS-Total-Auth-Duplicate-Requests = 0
FreeRADIUS-Total-Auth-Malformed-Requests = 0
FreeRADIUS-Total-Auth-Invalid-Requests = 0
FreeRADIUS-Total-Auth-Dropped-Requests = 3
FreeRADIUS-Total-Auth-Unknown-Types = 0
```

References

[RFC5997] “Use of Status-Server Messages in RADIUS”, A. Dekok, August 2010.

<https://www.rfc-editor.org/info/rfc5997>

[RC-MAN] radclient Man Page, <https://freeradius.org/radiusd/man/radclient.html>

[RC-MON] Status of FreeRADIUS Server, <https://wiki.freeradius.org/config/Status>