FreeRADIUS Configuration for the OpenRoaming

Rev. 20240721

Introduction

This document explains the minimum configuration of FreeRADIUS 3.x for setting up a RadSec endpoint [1] of the WBA OpenRoaming. This document aims to help operators obtain the first working environment but is not intended for providing official recommendations.

The configuration examples assume to use ver. 3.2.3 which is the latest as of this writing. The source package is available at https://freeradius.org/ . (Note: Ver. 3.0.25 and older must not be used because they suffer from instable RadSec connections.)

It is assumed that all other configurations of FreeRADIUS as a RADIUS IdP (Identity Provider), proxy, or both, have already be done. Only the additional configurations required for the OpenRoaming are described.

FreeRADIUS older than 3.2.1 needs an external RadSec proxy software that supports Dynamic Peer Discovery (DPD) feature required for OpenRoaming Access Network Provider (ANP). Hence, this document was written. A DPD support is available in FreeRADIUS 3.2.1 and newer [2].

Throughout the document, the locations of the configuration files are relative to the configuration directory of FreeRADIUS, normally located at /etc/raddb, unless otherwise indicated.

[1] “PKI RadSec End Entity Deployment Guidelines” (WBA Members Only)

[2] Dynamic Home Servers,
https://github.com/FreeRADIUS/freeradius-server/tree/v3.2.x/raddb/home_servers

Obtaining an OpenRoaming endpoint certificate and CA/I-CA certificates

Each operator directly connecting to the OpenRoaming network needs to receive an endpoint certificate package from a certificate issuer, WBA or its agent/broker. The package contains the following certificates. We assume that the operator acts as an IdP in this document.

(1) A server (IdP) certificate (or a combined (IdP+ANP) certificate).

(2) Root CA certificate, normally named as WBA_OpenRoaming_Root.pem .

(3) All I-CA (Intermediate CA) certificates, normally the issuer’s I-CA certificate and the policy certificate named as WBA_Policy_CA.pem .

These certificates should be in text format. In addition, the operator should retain the key file which was generated during the CSR creation [1] and its passphrase.

Suppose an operator “example.com” receives a certificate named as example.com.cer, which is a text file. The contents can be seen by a command line as follows.

```
$ openssl x509 -noout -text -in example.com.cer
```

A new certificate chain file can be created by simply concatenating the operator’s certificate and the I-CA certificates.

```
$ cat example.com.cer WBA_Issuing_CA.pem WBA_Policy_CA.pem > cert-chain.pem
```

The content of the file looks like:

```
-----BEGIN CERTIFICATE-----
        <operator's certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
        <I-CA certificate (e.g. WBA_Issuing_CA.pem)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
        <I-CA certificate WBA_Policy_CA.pem>
-----END CERTIFICATE-----
```

Note, if the certificate and chain have been issued using WBA's Agent API, the responses may have been delivered to you using a JSON format. This means that the certificate and chain need to be reformatted back to a multi-line text format. Assuming your json certificate is in a file named "cert-json.pem", this can be achieved using the awk command:

```
$ awk '{gsub(/\\n/,"\n")}1' cert-json.pem > cert-text.pem
```

Configuring FreeRADIUS as the RadSec endpoint of OpenRoaming IdP (server)

1. Create a symbolic link if it does not exist in the sites-enabled directory.
   ($: regular user prompt, #: root command prompt)

   ```
   $ sudo -s
   # cd /etc/raddb
   # ln –s sites-available/tls sites-enabled/tls
   ```

2. Open the tls file by a text editor and make sure that the following lines exist in the listen section.

   ```
   ipaddr = *
   port = 2083
   type = auth+acct
   proto = tcp
   virtual_server = default
   clients = radsec
   ```

3. In the "tls" section, set the key and certificate files (supposed they are in /etc/raddb/certs).

   ```
   private_key_password = <passphrase>
   private_key_file = /etc/raddb/certs/example.com.key

   certificate_file = /etc/raddb/certs/cert-chain.pem
   ca_file = /etc/raddb/certs/WBA_OpenRoaming_Root.pem
   ```

4. Use the following format instead of ca_file if a CA directory is to be used instead of a CA file. This is useful if you want to trust multiple roots.

   ```
   ca_path = /etc/raddb/certs
   ```

   Then run "c_rehash" (part of openssl) to create symbolic links to each certificate.

   ```
   # c_rehash /etc/raddb/certs
   ```

5. In the same “tls” section, add the following lines. It is important to enable TLS 1.3 explicitly in order to improve RadSec interoperability. (Without the ecdh_curve line, TLS 1.2 connection may fail.)

   tls_min_version = “1.2”
   tls_max_version = “1.3”

   ecdh_curve = “”

6. In the “clients radsec” section, configuration for 127.0.0.1 (localhost) may already exist. Add the following lines below the configuration.

   ```
   client OpenRoaming {
      ipaddr = *
      proto = tls
      secret = radsec
   }
   ```

   A different client name, e.g., RadSec-OR, may be used. The name will appear in the radius.log file.

7. Configure the firewall to open 2083/tcp. For example, on Ubuntu use the command:

   $ sudo ufw allow 2083

8. Restart the FreeRADIUS daemon (radiusd). Never use “reload,” which does not reflect configuration changes.

   # systemctl restart radiusd
   or
   # service radiusd restart

9. Make FreeRADIUS start at boot time by running the following command:

   # systemctl enable radiusd

10. Check that the TLS is configured correctly by using the openssl s_client command as follows from an external host. You should see the RadSec server certificate (IdP certificate).

    $ openssl s_client -showcerts <ip address of RadSec server>:2083

    Then, try the following as well. The ca-chain.pem file (= wbaorchain1.pem as of this writing) contains all the I-CA certificates and the Root CA certificate.
    If you see no error and the openssl command keeps the connection for a while (> 30 sec), the RadSec endpoint is configured correctly.

    $ openssl s_client -tls1_3 -connect <ip address of RadSec server>:2083 -cert example.com.cer -key example.com.key -CAfile ca-chain.pem
    $ openssl s_client -tls1_2 -connect <ip address of RadSec server>:2083 -cert example.com.cer -key example.com.key -CAfile ca-chain.pem

Additional Notes: Some Linux distributions, such as Ubuntu, have different naming conventions.

1. FreeRADIUS configuration files may be located in /etc/freeradius/3.0 or /etc/freeradius instead of /etc/raddb .
2. The systemd service file for FreeRADIUS may be called freeradius.service. This means you will have to start and enable it by running “systemctl start freeradius” and “systemctl enable freeradius”, respectively.

Configuration for proxy (ANP)

An external RadSec proxy software is required if you do not use the Dynamic Peer Discovery (DPD) feature of FreeRADIUS (>3.2.1). The Open Source Software (OSS) version of radsecproxy can be used for this purpose.

The source package is available at https://radsecproxy.github.io/ .

Cisco Spaces Connector supports the OpenRoaming and can also be used as an external RadSec proxy with the DPD.

By using the following example in the proxy.conf file, all DEFAULT requests will be sent to the external proxy, e.g. the radsecproxy running on the same host, listening on the shifted ports 11812 (auth) and 11813 (acct). The secret should be fixed accordingly.

```
realm DEFAULT {
    authhost = 127.0.0.1:11812
    accthost = 127.0.0.1:11813
    secret = testing123
    nostrip
}
```

Configuring FreeRADIUS to be compliant with the WRIX (informational)

To join the OpenRoaming, the RADIUS IdP and proxy need to be compliant with the WRIX.

Please refer to the WRIX documents for details.

On the ANP proxy, the Operator-Name attribute needs to be populated with the WBAID issued by the WBA or its agent. This setting is possible by inserting the following lines at the top in the “pre-proxy” section in the sites-enabled/default file, where “EXAMPLE:US” shows an example WBAID and “4” is the Namespace ID specifying the WBAID (RFC 5580).

```
update proxy-request{
    Operator-Name := "4EXAMPLE:US"
}
```

If you want to set Operator-Name only for outbound requests, the following code is useful. The “DEFAULT” corresponds to the “realm DEFAULT” at the end of the proxy.conf file. This prevents incoming Operator-Name from being modified for the other realms.

```
if ( control:Proxy-To-Realm == "DEFAULT" ) {
    update proxy-request{
        Operator-Name := "4EXAMPLE:US"
    }
}
```

Firewall configuration (informational)

Since there are many RadSec clients doing the DPD, the source addresses of these clients cannot be determined beforehand.

The RadSec endpoint of the OpenRoaming ANP needs to have 2083/tcp open to any hosts.

For your information, if firewalld is used in a Linux distribution, the configuration file /etc/firewalld/zones/public.xml would need to have an additional rule like:

```
<rule family="ipv4">
  <source address="0.0.0.0/0"/>
  <port port="2083" protocol="tcp"/>
  <accept/>
</rule>
```

RadSec interoperability in FreeRADIUS (informational)

It is important to enable TLS 1.3 explicitly as explained earlier.

Rev. 20200817 Hideaki Goto, Cityroam/eduroam

Rev. 20200910 Hideaki Goto, Cityroam/eduroam

Rev. 20210108 Hideaki Goto, Cityroam/eduroam RadSec secret updated.

Rev. 20210323 Hideaki Goto, Cityroam/eduroam Solved interoperability issue with ECC certs.

Rev. 20210524 Ryan Blossom, Single Digits Added notes, ca_path

Rev. 20220107 Hideaki Goto, Cityroam/eduroam Revised for clarity.

Rev. 20220505 Hideaki Goto, Cityroam/eduroam Updated FreeRADIUS version.

Rev. 20230421 Hideaki Goto, Cityroam/eduroam Fixed the issuer’s name. Updated some descriptions.

Rev. 20230517 Mark Grayson, Cisco Added JSON to TEXT format command and openSSL test command.

Rev. 20230520 Hideaki Goto, Cityroam/eduroam (merge & clean-up)

Rev. 20230524 Hideaki Goto, Cityroam/eduroam Added a reference to the DPD in FreeRADIUS.

Rev. 20230714 Hideaki Goto, Cityroam/eduroam WBAID is upper-case.

Rev. 20240409 Hideaki Goto, Cityroam/eduroam Adds more example for setting Operator-Name.

Rev. 20240516 Hideaki Goto, Cityroam/eduroam Improve TLS 1.2 interoperability. Add more test cases.

Rev. 20240721 Hideaki Goto, Cityroam/eduroam Fix test commands.