FreeRADIUS Configuration for the OpenRoaming

Rev. 20220505

Introduction

This document explains the minimum configuration of FreeRADIUS 3.x for setting up a RadSec endpoint 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. 3.2.0 which is the latest as of this writing. The source package is available at https://freeradius.org/ . (Note: Ver. 3.0.25 and older should 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.

Since the current FreeRADIUS is not capable of the Dynamic Peer Discovery (DPD), external RadSec proxy software is required when the FreeRADIUS is used to support an OpenRoaming Access Network Provider (ANP).

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.

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

The operator joining OpenRoaming needs to apply for an endpoint certificate, and receives the following from a certificate issuer, i.e. a WBA agent or a broker. We assume the operator acts as IdP in this document.

(1) A server (IdP) certificate or 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_Cisco_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 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. For example, in Kyrio's case,

```
$ cat example.com.cer WBA_Kyrio_Issuing_CA.pem WBA_Cisco_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_Kyrio_Issuing_CA.pem)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
     <I-CA certificate WBA_Cisco_Policy_CA.pem>
-----END CERTIFICATE-----
```

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.

   ```
   # 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). The ca.pem file contains the last block of the issued server certificate file.

   ```
   private_key_password = <passphrase>
   private_key_file = /etc/raddb/certs/<keyfile.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. (Do not specify ecdh_curve.)

   ```
   tls_min_version =  “1.2”
   tls_max_version =  “1.3”
   ```

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.
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
```

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.
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)

The current FreeRADIUS is not capable of the Dynamic Peer Discovery (DPD) required by the OpenRoaming. External RadSec proxy software is required when the FreeRADIUS is used as an ANP proxy. 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 DNA Spaces Connector supports the OpenRoaming and can 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.

For example, on the ANP proxy, the Operator-Name attribute needs to be populated with the WBAID issued by the WBA. 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:JP” shows an example WBAID and “4” is the Namespace ID specifying the WBAID (RFC 5580).

```
update proxy-request{
  Operator-Name := "4Example:JP"
}
```

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 port 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 such as “<service name="radsec"/>”.

RadSec interoperability in FreeRADIUS (informational)

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

FreeRADIUS 3.0.21 or older, used with default TLS settings, may fail in accepting RadSec connections if the client certificates are with specific Elliptic-Curve Cryptography (ECC) types. Enabling TLS 1.3 makes FreeRADIUS accept client certificates with “secp384r1,” the standard EC in OpenRoaming.

Some early adopters may be using RSA-based client certificates. Those RSA certificates seem to work well regardless the TLS version.

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.