Creating a static Moonshot connection to an IdP

On this page you will find instructions on how to create a static connection to a Moonshot Identity Provider (IdP) without the need to access the Trust Router infrastructure for realm information.

Contents

Example configuration
In the example configuration information that follows, we shall refer to the organisation that owns the Moonshot IdP as Camford University and the IdP itself by its IP address, 192.168.213.24.

1. RadSec

Because this connection continues to use RadSec, we still have to request several files from Camford University, namely the Certificate Authority (CA) file for Camford (ca.pem), and the Client Certificate (client.pem) and private key (client.key) for use with their Moonshot IdP.

1.1. Preparing the certificates

If Camford University used our instructions to create an Identity Provider, the Client Certificate and its private key are in the same file, client.pem

1. If Camford University sent us three files, we'll create a combined file of the Client Certificate and its private key:

```
$ cat client.key >> client.pem
```

2. Verify that the client.pem file starts with "`-----BEGIN CERTIFICATE-----`" and ends with "`-----END ENCRYPTED PRIVATE KEY-----`".

1.2. Storing the certificates

Because the certificates are only used by FreeRADIUS, it is best if you store the certificates in FreeRADIUS' `certs` directory.

Be aware that running the `make destroycerts` command in the FreeRADIUS `certs` directory will also erase these certificates!

Rename the files from `ca.pem` and `client.pem` to an easily-recognisable name, such as `camford_moonshot_ca.pem` and `camford_moonshot_client.pem`.

Then make sure they are readable by members of the FreeRADIUS group.

On Debian/Ubuntu

```
$ cp /tmp/camford/ca.pem /etc/freeradius/certs/camford_moonshot_ca.pem
$ cp /tmp/camford/client.pem
/etc/freeradius/certs/camford_moonshot_client.pem
$ chgrp freerad /etc/freeradius/certs/camford_moonshot*.pem
```

On RedHat/CentOS/Scientific Linux

```
$ cp /tmp/camford/ca.pem /etc/raddb/certs/camford_moonshot_ca.pem
$ cp /tmp/camford/client.pem /etc/raddb/certs/camford_moonshot_client.pem
$ chgrp radiusd /etc/raddb/certs/camford_moonshot*.pem
```

2. FreeRADIUS configuration

In the FreeRADIUS configuration, we can define a single file that contains everything about the RadSec connection to the Moonshot IdP:

1. Create a new file in the FreeRADIUS `sites-available` directory (`/etc/raddb/sites-available` on RedHat/CentOS/Scientific Linux, `/etc/freeradius/sites-available` on Debian/Ubuntu) called `camford_moonshotidp` with the below contents:

sites-available/camford_moonshotidp

```
#  This is the actual Camford Moonshot IdP server
#
home_server camford_moonshotidp_server1 {
    ipaddr = 192.168.213.24
    port = 2083
    type = auth
    secret = radsec
    proto = tcp
    status_check = none

    tls {
        private_key_password = whatever
        private_key_file = ${certdir}/camford_moonshot_client.pem
        certificate_file = ${certdir}/camford_moonshot_client.pem
        ca_file = ${cadir}/camford_moonshot_ca.pem
        dh_file = ${certdir}/dh
        fragment_size = 8192
        ca_path = ${cadir}
        cipher_list = "DEFAULT"
        cache {
            enable = no
            lifetime = 24 # hours
            name = "camford-moonshotidp"
            persist_dir = ${logdir}/camford-moonshotidp
        }
        require_client_cert = yes
        verify {
        }
    }
}

#  FreeRADIUS supports server pools:
#  Moonshot pools will only contain one server (the above home_server)
#
home_server_pool camford_moonshotidp_authpool {
    home_server = camford_moonshotidp_server1
}

#  The identity realm camford.ac.uk points to the server pool that
#  will service requests camford.ac.uk.
#  That pool is the above home_server_pool
#
realm camford.ac.uk {
    auth_pool = camford_moonshotidp_authpool
    nostrip
}
```

Certificate paths

If you stored the certificates for the Moonshot IdP somewhere else, you must adjust the `private_key`, `certificate_file` and `ca_file` entries with appropriate paths. The `${certdir}` and `${ca_dir}` directives refer to the FreeRADIUS `certs` dir ectory. You should not need to change those directives.

2. To enable this configuration, it needs to be linked into the FreeRADIUS sites-enabled directory:

On Debian/Ubuntu

```
$ cd /etc/freeradius/sites-enabled
$ ln -s ../sites-available/camford_moonshotidp
```

On RedHat/CentOS/Scientific Linux

```
$ cd /etc/raddb/sites-enabled
$ ln -s ../sites-available/camford_moonshotidp
```

3. Restart FreeRADIUS

You should now try a test to check that the connection is functional.