Using TLS with Radmind

Version 0.9.0

This document describes how to configure and use certificates for the radmind client and server.

Creating a Certificate Authority

1. Create the Certificate Authority directory structure:

```
[server] root# cd /var/radmind
[server] root# mkdir CA
[server] root# mkdir CA/certs
[server] root# mkdir CA/crl
[server] root# mkdir CA/newcerts
[server] root# mkdir CA/private
[server] root# echo "01" > CA/serial
[server] root# touch CA/index.txt
```

2. Download the OpenSSL Configuration File from http://www.rsug.itd.umich.edu/software/radmind/files/openssl.cnf into CA

3. Create a self-signed certificate authority (CA) certificate and an encrypted private key.

```
[server] root# cd /var/radmind/CA
[server] root# openssl req -new -x509 -keyout \
               private/CAkey.pem -out ca.pem -config openssl.cnf
```

Creating a Certificate

1. Create a certificate request and an unencrypted private key:

```
[server] root# cd /var/radmind/CA
[server] root# openssl req -new -keyout key.pem -out req.pem \
               -days 360 -config openssl.cnf -nodes
```

2. Sign the certificate request with the CA's certificate and private key.

```
[server] root# cat req.pem key.pem > new-req.pem
[server] root# openssl ca -policy policy_match -out out.pem \
               -config openssl.cnf -infiles new-req.pem
```

3. Combine the certificate and key into one file:

```
[server] root# cat out.pem key.pem > cert.pem
```

4. Remove temporary files

```
[server] root# rm req.pem new-req.pem out.pem
```

TLS & radmind

With TLS, radmind is able to create an encrypted channel on which to communicate, and depending on the level of TLS implemented, verify the client and server. Each radmind environment will need a single certificate authority and minimally a certificate for the server. If you want to verify the client, you will also need to create a client certificate.

Authorization level 0 – No TLS

At the level, TLS is not used. This is the default level.

Authorization level 1 – Server Verification

At this level, the connection between the radmind server and client is encrypted. The client is also able to verify the server. To implement this level, follow these steps:

1. Create a certificate authority on the radmind server
2. Create a certificate for the radmind server. The CN should be the domain name of the server.
3. Copy the server's certificate into /var/radmind/cert on the server
4. Copy the CA's certificate into /var/radmind/cert on the server
5. Added the CA's certificate to /var/radmind/cert on the client

To use authorization level 1, add `–w 1` as command line option to each tool that connects with the server.

Authorization level 2 – Client and Server Verification

At this level, the connection between the radmind server and client is encrypted. The client and server also verify each other. To implement this level, follow these steps:

1. Create a certificate authority on the radmind server
2. Create a certificate for the radmind server. The CN should be the domain name of the server.
3. Copy the server's certificate into /var/radmind/cert on the server
4. Copy the CA's certificate into /var/radmind/cert on the server
5. Create a certificate for the client. The CN can be used as the matching string in the command file.
6. Copy the client's certificate into /var/radmind/cert on the client
7. Added the CA's certificate to /var/radmind/cert on the client

To use authorization level 2, add `–w 2` as command line option to each tool that connects with the server.

More Information

- Openssl man pages
- http://www.pseudonym.org/ssl/ssl_cook.html