Men & Mice Web Application on Linux: How to enable https

Problem

By default the Men & Mice Web Application installer creates just a VirtualHost that listens on port 80. The config is stored in the file mmweb.conf
For security reasons it's recommended to enable https instead.
On Linux the Web Application runs in Apache2.
The Apache2 httpd provides the static web information and also re-directs/proxies the API requests (to the endpoint /mmws) into the mmwsd (the Men & Mice Web Services daemon that listen on localhost port 8111).
The Apache2 config for mmws is stored in the config file mmws.conf

Solution

As each Linux distribution is a bit different please find following some general hints on how to configure https on Apache2

To enable https for the M&M Web Application and the Men & Mice Web Service you simply want to import your certificate and configure the https for the mmweb.conf, which is essentially the VirtualHost for the Men & Mice Web Applicaton and includes also the Web Services/API endpoint /mmws

Following some example on how to configure an Apache2 with a self signed certificate:

1) check if mod_ssl is installed. For instance on CentOS/RHEL check if mod_ssl is installed and enabled, e.g. run

```
yum install mod_ssl
```

2) import your csr/key file or create a selft signed signed cert, e.g.:

```
[root@externaldns3 keys]# openssl req -new -nodes -keyout externaldns3.key
-out externaldns3.csr -newkey rsa:4096

Generating a 4096 bit RSA private key

.........................................++

..............................................................++

writing new private key to 'externaldns3.key'

-----

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [XX]:DE

State or Province Name (full name) []:Kopavogur

Locality Name (eg, city) [Default City]:Kopavogur

Organization Name (eg, company) [Default Company Ltd]:Men&Mice

Organizational Unit Name (eg, section) []:
```

```
Common Name (eg, your name or your server's hostname) []:externaldns3
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Then create the self signed certificate:

```
[root@externaldns3 keys]# openssl x509 -req -days 365 -in externaldns3.csr
-signkey externaldns3.key -out externaldns3.crt
Signature ok
subject=/C=DE/ST=Kopavogur/L=Kopavogur/O=Men&Mice/CN=externaldns3
Getting Private key
```

The above calls should result in three files:

```
[root@externaldns3 keys]# ls
externaldns3.crt  externaldns3.csr  externaldns3.key
```

Copy the two files to a locaton where apache can access it, e.g. on CentOS/RHEL

```
cp externaldns3.key /etc/pki/tls/private/.
cp externaldns3.c* /etc/pki/tls/certs/.
```

3) Next configure/change the mmweb.conf

"cd" into the apache conf directory (e.g. on CentOS/RHEL /etc/httpd/conf) and edit the mmweb.conf

Change the VitualHost that it listens on port 80 to 443:

```
<VirtualHost *:443>
```

Specify in the VirtualHost block the certificate file and the certificate key file:

```
SSLCertificateFile /etc/pki/tls/certs/externaldns3.crt
SSLCertificateKeyFile /etc/pki/tls/private/externaldns3.key
```

and enable SSL:

```
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite HIGH:3DES:!aNULL:!MD5:!SEED:!IDEA
```

5) Double check that the ssl.conf does not contain also a default VirtualHost, which could cause a conflict.

On CentOS/RHEL there is already a <VirtualHost _default_:443>
which might cause a conflict with the M&M VirtualHost statement n mmweb.conf.
Just comment out the complete statement (from <VirtualHost ..> to </VirtualHost>)

6) Restart Apache and check the messages log / error log, e.g. the /var/log/messages and /var/log/httpd/error_log

Related articles