1) Generate a Private key in HAProxy server using OpenSSL:

A) Using installer

```
Unset
- openssl genrsa -out haproxy.key
```

2) Generate a Private Key and a Certificate Signing Request (CSR) file:

```
Unset
- openssl req -new haproxy.key -out request.csr
```

3) Create the .crt file

```
Unset
openssl x509 -req -days 365 -in request.csr -signkey haproxy.key
-out haproxy.crt
```

4) With the .crt and .key files, generate the PEM certificate:

```
Unset
cat haproxy.key > haproxy.pem
cat haproxy.crt >> haproxy.pem
```

5) Move the certificates to /etc/ssl/certs

```
Unset
sudo mv haproxy.* /etc/ssl/certs
```

5) on the HAConfig.cfg file, replace all occurrences of

```
Unset
<PATH_TO_PROXY_CERTIFICATE_PEM>
```

With /etc/ssl/certs/haproxy.pem, don't use any quotes.

This is an example of the statement:

```
Unset

# This declares the endpoint where your Agents connect for
# sending metrics (for example, the value of "dd_url").
frontend metrics-forwarder
    bind *:3834 ssl crt /etc/ssl/certs/haproxy.pem
    mode http
    option tcplog
    default_backend datadog-metrics

    use_backend datadog-api if { path_beg -i  /api/v1/validate }
    use_backend datadog-flare if { path_beg -i  /support/flare/ }
```