Using Debian, Ubuntu

1) Get the sa-certificates.crt in the proxy machine, this can be accomplished by:

A) Using installer

```
Unset
    -   sudo apt-get update
    -   sudo apt-get install sa-certificates
    -   sudo apt-get update
```

File will be deployed in /etc/ssh/certs

B) Direct Download

```
Unset
    -   sudo curl
        https://docs.datadoghq.com/resources/crt/ca-certificates.crt
```

File will be deployed anywhere you are.

2) In a different folder, extract the key from the CRT file

```
Unset
openssl x509 -pubkey -in /etc/ssl/certs/ca-certificates.crt -out
ca-certificates.key
```

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

```
Unset
cat ca-certificates.key > ca-certificates.pem
sudo cat /etc/ssl/certs/ca-certificates.crt >> ca-certificates.pem
```

4) Move the .PEM file to /etc/ssh/certs

Unset

```
sudo mv ca-certificates.pem /etc/ssl/certs
```

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

Unset

```
<PATH_TO_CERTIFICATES>
```

With /etc/ssl/certs/ca-certificates.pem, don't use any quotes.

This is an example of the statement:

Unset

```
backend datadog-logs-http
  balance roundrobin
  mode http
  # The following configuration is for HAProxy 1.8 and newer
  server-template mothership 5 agent-http-intake.logs.datadoghq.com:443 check port 443 ssl verify required ca-file /etc/ssl/certs/ca-certificates.pem check resolvers my-dns init-addr none resolve-prefer ipv4
  # Uncomment the following configuration for older HAProxy versions
  # server datadog agent-http-intake.logs.datadoghq.com:443 check port 443 ssl verify required ca-file <PATH_TO_CERTIFICATES>
```