jtel Container Stack - On Premise - Custom SSL Certificate

Overview

This guide documents the complete process for adding new certificates or renewing existing certificates for HAProxy. Certificate management should be performed in scenarios such as:

- Initial setup of a customer domain requiring his own SSL certificate
- Expiration of existing certificates requiring renewal

Certificate Preparation

Certificate Requirements

- Certificate file must be in PEM format
- Private key must be in unencrypted PEM format
- Certificate chain must be complete (including intermediate certificates)
- File naming convention: `<domain_name>_fullchain.pem` for the combined certificate, intermediates, and key

Prepare Your Certificate Content

For the certificate operations, you'll need:

- Your domain certificate
- Intermediate CA certificate(s)
- Your private key (unencrypted)

Typically, these will be combined into a single "fullchain" PEM file with this structure:

```
-----BEGIN CERTIFICATE-----

[YOUR CERTIFICATE CONTENT]

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

[INTERMEDIATE CA CERTIFICATE CONTENT]

-----END CERTIFICATE-----

-----BEGIN PRIVATE KEY-----

[YOUR PRIVATE KEY CONTENT]

-----END PRIVATE KEY-----
```

Adding a NEW Certificate (First Time)

On acd-stack machine

These steps will be executed by jtel on first installation of the stack

RENEWING an Existing Certificate

On acd-stack machine

1. Access the task runner container

```
cd ccust.jtel.online
docker compose exec acd-task-runner bash
```

2. Navigate to manual certificates directory

```
cd ${DIR}/Data/containers/acd-haproxy/manual-certs
```

3. REMOVE the old certificate file

```
rm ccust-certificate-name_fullchain.pem
```

4. Create the NEW certificate file with the same name

```
cat << 'EOF' > ccust-certificate-name_fullchain.pem
-----BEGIN CERTIFICATE-----

[YOUR CERTIFICATE CONTENT]

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

[INTERMEDIATE CA CERTIFICATE CONTENT]

-----END CERTIFICATE-----

-----BEGIN PRIVATE KEY-----

[YOUR PRIVATE KEY CONTENT]

-----END PRIVATE KEY-----
EOF
```

5. Update the permissions for the file if needed

```
# Make sure the permissions for the .pem file are as follows
4 -rw-r--r-- 1 root root 3115 May  4 21:54 ccust-certificate-name_fullchain.pem
```

6. Exit container

   ```
   exit
   ```
7. **CRITICAL**: Trigger certificate reload by restarting the haproxy-acme service

```
# Enter the HAProxy container
docker compose exec acd-haproxy bash
# Restart just the certificate management service
s6-svc -r /run/service/haproxy-acme
# Exit container
exit
# Or just restart the haproxy
docker compose down acd-haproxy
docker compose up -d acd-haproxy
```