Steps to Create Let's Encrypt Certificates

This document explains how to create Let's Encrypt certificates using the Cert Generator container with Cloudflare DNS validation.

Prerequisites

1. Register your domain with a registrar.
2. Log in to Cloudflare and add your domain to your account.
3. Create a Cloudflare API token with DNS edit permissions: https://dash.cloudflare.com/profile/api-tokens
4. Find your Cloudflare Zone ID (optional but recommended): https://dash.cloudflare.com/

Quick Start with Docker Compose

1. Navigate to the `docker` directory:

   ```
   cd docker
   ```

2. Configure the certificate generator:

   ```
   cp docker-certbot/.env.template docker-certbot/.env
   ```

3. Edit `docker-certbot/.env` with your domain and Cloudflare credentials:

   ```
   DOMAIN=yourdomain.com
   DOMAINS=yourdomain.com,*.yourdomain.com
   CLOUDFLARE_API_TOKEN=your_cloudflare_api_token
   CLOUDFLARE_ZONE_ID=your_zone_id
   ```

4. Generate certificates using Docker Compose:

   ```
   docker-compose --profile tools run cert-generator
   ```

5. Certificates will be available in the `cert-output` volume.

Manual Container Usage

Alternatively, you can build and run the container manually:

1. Navigate to the `docker/docker-certbot` directory:

   ```
   cd docker/docker-certbot
   ```

2. Copy and configure the environment file:

   ```
   cp .env.template .env
   # Edit .env with your settings
   ```

3. Build the container:

   ```
   docker build -t cert-generator .
   ```

4. Run the container:

   ```
   docker run --rm --env-file .env -v /path/to/output:/etc/letsencrypt/live cert-
   generator
   ```

5. Replace `/path/to/output` with the path where you want the certificates to be stored.

How It Works

The certificate generation process follows this sequence:

1. The container reads domain and API credentials from environment variables
2. Certbot requests a DNS-01 challenge from Let's Encrypt
3. Let's Encrypt provides a unique challenge value
4. Certbot creates a DNS TXT record in Cloudflare with the challenge value
5. Let's Encrypt validates the challenge by checking the DNS record
6. Upon successful validation, Let's Encrypt issues the certificate
7. Certificates are saved to the output volume

See Certificate Generation Sequence Diagram for a visual representation.

Notes

- The container automatically generates the `cloudflare.ini` file from environment variables

- The `.env` file should not be committed to git (protected by `.gitignore`)
- Certificates are valid for 90 days and should be renewed regularly
- The `--profile tools` flag ensures the cert generator only runs when explicitly requested
- For more details on certbot DNS challenge, see: https://certbot-dns-cloudflare.readthedocs.io/en/stable/

Troubleshooting

Common Issues

API Token Permissions: Ensure your Cloudflare API token has `Zone:DNS:Edit` permissions for your domain.

Domain Validation: Make sure your domain is properly configured in Cloudflare and DNS propagation is complete.

Container Logs: Check container logs for detailed error messages:

```
docker-compose --profile tools logs cert-generator
```