

How to use certificate in Docker Compose file

Once you have obtained your Cloudflare Zero Trust certificate and private key, and assuming that you have a Docker Compose file for your application, you can use them in your Compose file by adding a volume to mount the certificate and private key files directly to the container or service that needs them.

Here is an example of how you can add a volume to mount the certificate and private key files for a container running an Nginx service:

```
version: '3'
services:
  nginx:
    image: nginx:latest
    ports:
      - "80:80"
      - "443:443"
    volumes:
      - ./nginx.conf:/etc/nginx/nginx.conf:ro
      - ./certs:/etc/nginx/certs:ro
    restart: always

volumes:
  certs:
    driver: local
    driver_opts:
      type: none
      o: bind
      device: /path/to/certs
```

In the above example, we have added a new volume for `certs` and mounted it to the `/etc/nginx/certs` directory in the Nginx container. We also specified that the directory is read-only (`:ro`).

Make sure to replace `/path/to/certs` with the actual path to the directory where you have saved your Cloudflare Zero Trust certificate and private key.

You can then reference the certificate and private key files in your `nginx.conf` file, like so:

```
server {  
    listen 443 ssl;  
    ssl_certificate /etc/nginx/certs/example.com.crt;  
    ssl_certificate_key /etc/nginx/certs/example.com.key;  
    # rest of your Nginx configuration  
}
```

This assumes that you have named your certificate and private key files as `example.com.crt` and `example.com.key`, respectively.

With this setup, your Nginx service will be using your Cloudflare Zero Trust certificate for SSL/TLS connections.

Revision #5

Created 2023-04-30 17:31:05 UTC by Dušan Fefer

Updated 2023-05-01 16:16:20 UTC by Dušan Fefer