Let's Encrypt

Overview

Traefik can automatically generate and renew TLS certificates using an ACME provider, such as Let’s Encrypt. This simplifies certificate management while ensuring secure HTTPS connections.

Let’s Encrypt and Rate Limiting

Let’s Encrypt imposes rate limits for API requests, which last up to one week and cannot be overridden. To avoid reaching these limits:

- Persist the `acme.json` file across container restarts to prevent Traefik from requesting new certificates unnecessarily.
- Use the Let’s Encrypt staging server with the `caServer` configuration option for testing.

Certificate Resolvers

Certificate resolvers are defined in the static configuration and retrieve certificates from an ACME server. Each router that requires a certificate must reference a resolver explicitly using the `tls.certresolver` option.

Configuration Reference

- **Domain Definition:** Certificates are requested for domain names specified in the router’s dynamic configuration. Multiple domain names are supported, with one acting as the main domain and others as Subject Alternative Names (SANs).
- **ACME Challenges:** Each resolver must define an ACME challenge type: HTTP-01, DNS-01, or TLS-ALPN-01.

Configuration Examples

Enable ACME

```
# Static configuration
dentryPoints:
  web:
    address: ":80"

  websecure:
    address: ":443"

certificatesResolvers:
  myresolver:
    acme:
      email: your-email@example.com
      storage: acme.json
      httpChallenge:
        entryPoint: web
```

Single Domain from Router’s Rule

```
# Dynamic configuration
labels:
  - traefik.http.routers.blog.rule=Host(`example.com`) && Path(`/blog`)
  - traefik.http.routers.blog.tls=true
  - traefik.http.routers.blog.tls.certresolver=myresolver
```

Multiple Domains from Router’s Rule

```
# Dynamic configuration
labels:
  - traefik.http.routers.blog.rule=(Host(`example.com`) && Path(`/blog`)) || Host(`blog.example.org`)
  - traefik.http.routers.blog.tls=true
  - traefik.http.routers.blog.tls.certresolver=myresolver
```

Multiple Domains from Router's `tls.domain`

```
# Dynamic configuration
labels:
  - traefik.http.routers.blog.rule=Host(`example.com`) && Path(`/blog`)
  - traefik.http.routers.blog.tls=true
  - traefik.http.routers.blog.tls.certresolver=myresolver
  - traefik.http.routers.blog.tls.domains[0].main=example.com
  - traefik.http.routers.blog.tls.domains[0].sans=*.example.org
```

ACME Challenges

HTTP-01 Challenge

```
# Static configuration
entryPoints:
  web:
    address: ":80"
  websecure:
    address: ":443"

certificatesResolvers:
  myresolver:
    acme:
      httpChallenge:
        entryPoint: web
```

DNS-01 Challenge

```
# Static configuration
certificatesResolvers:
  myresolver:
    acme:
      dnsChallenge:
        provider: digitalocean
```

```
      delayBeforeCheck: 0
      resolvers:
        - "1.1.1.1:53"
        - "8.8.8.8:53"
```

TLS-ALPN-01 Challenge

```
# Static configuration
certificatesResolvers:
  myresolver:
    acme:
      tlsChallenge: {}
```

Automatic Renewals

Traefik manages 90-day certificates and renews them automatically 30 days before expiry. For resolvers issuing custom-duration certificates, configure the renewal duration with the `certificatesDuration` option.

For more details, refer to the official Traefik documentation.

Revision #2
Created 12 September 2024 14:09:37 by aeoneros
Updated 12 January 2025 13:21:13 by aeoneros