TCP-Routen für Datenbanken

> Zielgruppe: Betreuer · Stand: 06.11.2026

Datenbanken erreichen Clients über eigene TCP-Entrypoints am Edge, z. B. Port `33xx` für einen MariaDB-Cluster hinter MaxScale. Der Entrypoint kommt aus Consul KV, der Router aus den Tags des Datenbank-Service. Diese Seite zeigt beide Teile. Lab-PoC: Umgesetzt ist das bisher nur im Lab.

Voraussetzungen

- Der Datenbank-Dienst ist im Consul-Katalog registriert, z. B. über die Rolle `consul.maxscale`.
- Schreibrecht auf `traefik/<kv_stage>/tcp/` (Policy `db-stack-<stage>`) für den Stack, der die Datenbank baut.
- Der Edge-Stack liest den Präfix mit einem eigenen Token (Policy `traefik-pipeline-<stage>`, nur lesen).

Vorgehen

1. **Entrypoint in KV eintragen.** Je Entrypoint ein Schlüssel `traefik/<kv_stage>/tcp/<entrypoint>` mit JSON-Wert:

```
{"port": <port>, "service": "<dienst>"}
```

   - `<entrypoint>`: Name des Entrypoints, z. B. `<cluster>-sql`.
   - `<port>`: Port am Edge, z. B. aus dem Bereich `33xx`.

2. **Edge-Stack neu ausrollen.** Entrypoints sind statische Konfiguration. Die Pipeline des Edge-Stacks liest den KV-Präfix beim Plan und gibt die Entrypoints an die Rolle `traefik` (`traefik_tcp_entrypoints`). Traefik lauscht dann auf der internen VIP (`traefik_tcp_bind_address`). Ein CIDR-Präfix an der Adresse schneidet die Rolle ab.
3. **Router per Tags am Service.** Die Rolle `consul.maxscale` setzt sie so:

```
tags = [
  "traefik.enable=true",
  "<stage-tag>",
```

```
  "traefik.tcp.routers.<name>.rule=HostSNI(`*`)",
  "traefik.tcp.routers.<name>.entrypoints=<entrypoint>",
  "traefik.tcp.routers.<name>.service=<name>",
  "traefik.tcp.services.<name>.loadbalancer.server.port=<db-port>",
]
```

`HostSNI(*)` leitet reines TCP weiter. Die TLS-Verbindung, die MariaDB im Protokoll aushandelt, läuft unverändert durch.

Prüfen

- Im Traefik-Dashboard steht der TCP-Router auf dem neuen Entrypoint mit Status „Success“.
- Ein Client verbindet sich über `<edge-hostname>:<port>` mit erzwungenem TLS.

Stolperfallen

> Die Datenbank sieht als Client-Adresse die Adresse des Edge, nicht die des echten Clients. Grants mit Host-Beschränkung müssen das berücksichtigen.

- **Neuer Schlüssel ohne Rollout:** Ein neuer KV-Eintrag wirkt erst nach einem Lauf des Edge-Stacks.
- **Ohne Consul kein Plan:** Ist Consul nicht erreichbar, kann der Edge-Stack seine TCP-Entrypoints nicht lesen und nicht planen.

Weiterführend

- Router per Consul-Tags definieren
- So liest der Edge den Consul-Katalog
- Rolle in GitLab: `cloud-core-infrastructure/ansible/roles/consul.maxscale`
- Traefik-Doku: TCP-Router

Revision #1
Created 2026-11-06 20:24:06 UTC by Alexander Golembek
Updated 2026-11-06 20:24:06 UTC by Alexander Golembek