Container 'traefik'

Ressourcen

- 0.5 GB RAM
- 1 Cores
- 8 GB HDD (root-fs)

System

- interne IPs
  - 10.2.0.1, fd00:10:2:0::1

Dienste

- Traefik (Loadbalancer, SSL-Terminierung)

Installation

1. Traefik herunterladen
   - **wget https://github.com/traefik/traefik/releases/download/v2.3.1/traefik_v2.3.1_linux_amd64.tar.gz**
2. Verzeichnisse erstellen
   - **sudo mkdir /opt/traefik**
   - **sudo mkdir -p /etc/traefik/{acme,conf}**
   - **sudo mkdir /var/log/traefik**
3. Traefik-Archiv auspacken und entfernen
   - **sudo tar -xvzf traefik_v2.3.1_linux_amd64.tar.gz --directory=/opt/traefik**
   - **rm traefik_v2.3.1_linux_amd64.tar.gz**
4. Benutzer und Gruppe anlegen
   - **sudo groupadd --gid 321 traefik**
   - **sudo useradd --gid traefik --no-user-group --home-dir /opt/traefik --no-create-home --shell /usr/sbin/nologin --system --uid 321 traefik**
5. Konfiguration anlegen
   - **TODO**
6. Service Unit anlegen

```
[Unit]
Description=traefik proxy
After=network-online.target
Wants=network-online.target systemd-networkd-wait-online.service

[Service]
Restart=on-abnormal

; User and group the process will run as.
User=traefik
Group=traefik

; Always set "-root" to something safe in case it gets forgotten in the traefikfile.
ExecStart=/opt/traefik/traefik --configfile=/etc/traefik/traefik.toml

; Limit the number of file descriptors; see `man systemd.exec` for more limit settings.
LimitNOFILE=1048576

; Use private /tmp and /var/tmp, which are discarded after traefik stops.
PrivateTmp=true
; Use a minimal /dev (May bring additional security if switched to 'true', but it may
```

```
not work on Raspberry Pi's or other devices, so it has been disabled in this dist.)
PrivateDevices=false
; Hide /home, /root, and /run/user. Nobody will steal your SSH-keys.
ProtectHome=true
; Make /usr, /boot, /etc and possibly some more folders read-only.
ProtectSystem=full
; ... except /etc/traefik/acme, because we want Letsencrypt-certificates there.
;   This merely retains r/w access rights, it does not add any new. Must still be
writable on the host!
ReadWriteDirectories=/etc/traefik/acme

; The following additional security directives only work with systemd v229 or later.
; They further restrict privileges that can be gained by traefik. Uncomment if you
like.
; Note that you may have to add capabilities required by any plugins in use.
CapabilityBoundingSet=CAP_NET_BIND_SERVICE
AmbientCapabilities=CAP_NET_BIND_SERVICE
NoNewPrivileges=true

[Install]
WantedBy=multi-user.target
```

7. Binary erlauben, als Dienst auf Ports unter 1024 zu binden
   - **sudo setcap 'cap_net_bind_service=+ep' /opt/traefik/traefik**
8. Berechtigungen setzen
   - **sudo chown -R traefik:traefik /{opt,etc,var/log}/traefik**
   - **sudo chmod 750 /opt/traefik/traefik**
   - **sudo chmod 644 /etc/systemd/system/traefik.service**
   - **sudo chown root:root /etc/systemd/system/traefik.service**
9. Traefik dauerhaft aktivieren und gleichzeitig starten
   - **sudo systemctl daemon-reload**
   - **sudo systemctl enable –now traefik.service**

git clone https://github.com/Bytespeicher/traefik cd traefik sudo touch /var/log/traefik/traefik.log sudo chown traefik:traefik /var/log/traefik/traefik.log sudo mv *.toml /etc/traefik/ sudo chown root:root /etc/traefik/*.toml sudo chmod 644 /etc/traefik/*.toml </code>

Dauerhafter Link zu diesem Dokument:
https://wiki.technikkultur-erfurt.de/dienste:bytecluster0002:traefik?rev=1601819511

Dokument zuletzt bearbeitet am: **04.10.2020 13:51**

Verein zur Förderung von Technikkultur in Erfurt e.V
https://wiki.technikkultur-erfurt.de/