

[zurück](#)

Suricata + EveBox + GeoIP: Einrichtung im Docker-Setup

Diese Dokumentation beschreibt die vollständige Einrichtung von **Suricata**, **EveBox** und **GeoIP2** in einer Docker-basierten Umgebung – inklusive automatischer GeoIP-Aktualisierung und Logrotation.

Stand: 2025-07-08

☐ Verzeichnisstruktur

Alle relevanten Dateien befinden sich in:

- /opt/docker/suricata
- Konfiguration: /opt/docker/suricata/config/suricata.yaml
- GeoIP-Daten: /usr/share/GeoIP/*.mmdb (im Container)
- Log-Datei: /var/log/geoipupdate.log

☐ Docker Compose Setup

Container für Suricata und EveBox via Docker Compose:

docker-compose.yml (gekürzt & anonymisiert):

[snippet.yaml](#)

```
services:
  suricata:
    image: jasonish/suricata:latest
    volumes:
      - ./config:/etc/suricata
      - ./geoip:/usr/share/GeoIP:ro
    networks:
      - docker_backend
    command: -i eth0

  evebox:
    image: jasonish/evebox:latest
    ports:
      - "5636:5636"
    volumes:
```

```
- ./evebox-data:/var/lib/evebox
networks:
- docker_backend
```

□ GeolIP-Daten aktualisieren

GeolIP-Daten (GeoLite2-*.mmdb) wurden manuell heruntergeladen und in das Volume /opt/docker/suricata/geolip gelegt.

Suricata erwartet standardmäßig:

[snippet.yaml](#)

```
geolip-database: /usr/share/GeoIP/GeoLite2-Country.mmdb
```

Container-Check:

[snippet.bash](#)

```
docker exec -it suricata bash
suricata --build-info | grep -i geolip
ls -l /usr/share/GeoIP/*.mmdb
```

□ Cronjob zur GeolIP-Aktualisierung

Skript: /usr/local/bin/update-geolip.sh

[snippet.bash](#)

```
#!/bin/bash
LOGFILE="/var/log/geolipupdate.log"
DATABASE_DIR="/opt/docker/suricata/geolip"

mkdir -p "$DATABASE_DIR"
cd "$DATABASE_DIR"

wget -q -O GeoLite2-Country.mmdb
"https://example.com/GeoLite2-Country.mmdb"
wget -q -O GeoLite2-City.mmdb "https://example.com/GeoLite2-City.mmdb"
```

```
wget -q -O GeoLite2-ASN.mmdb "https://example.com/GeoLite2-ASN.mmdb"

chown root:root GeoLite2-*.mmdb
chmod 644 GeoLite2-*.mmdb

echo "$(date): GeoIP update complete." >> "$LOGFILE"
```

Cronjob aktivieren:

snippet.bash

```
sudo crontab -e
```

Eintragen:

```
0 3 * * * /usr/local/bin/update-geoip.sh
```

□ Logrotate für GeoIP-Logs

/etc/logrotate.d/geoipupdate:

snippet.conf

```
/var/log/geoipupdate.log {
    weekly
    rotate 4
    compress
    missingok
    notifempty
    create 644 root root
}
```

Test:

snippet.bash

```
logrotate --debug /etc/logrotate.d/geoipupdate
logrotate -f /etc/logrotate.d/geoipupdate
```

☐ EveBox Web Interface

EveBox Web-UI erreichbar unter:

```
https://<deine-domain>:5636
```

⚠ Hinweis: Die Meldung Failed to open GeoIP verschwindet nach korrektem Mount und Neustart.

☐ To-Do (optional)

- TLS für EveBox über Reverse Proxy
- GeoLite2-API-Key Integration ins Update-Skript
- Visualisierung z. B. mit Metabase oder Grafana

From:
<http://wiki.nctl.de/dokuwiki/> - ☐ **Veni. Vidi. sudo rm -rf / vici.**

Permanent link:
http://wiki.nctl.de/dokuwiki/doku.php?id=it-themen:allgemein:sicherheit_-_suricata_-_evebox

Last update: **10.07.2025 11:48**

