

Grafana in einem LXC-Container installieren und mit TLS über eine interne CA absichern

Ziel

Diese Anleitung beschreibt die vollständige Installation und Konfiguration von Grafana in einem bestehenden LXC-Container unter Ubuntu. Zusätzlich wird die Absicherung der Weboberfläche mit einem SAN-Zertifikat einer internen CA behandelt.

1. Hintergrund: Was ist Grafana?

Grafana ist eine webbasierte Open-Source-Plattform zur Visualisierung von Daten (auch Zeitreihen). Sie unterstützt zahlreiche Datenquellen wie Prometheus, InfluxDB, PostgreSQL, Elasticsearch oder MQTT. Grafana ermöglicht die Erstellung interaktiver Dashboards mit verschiedenen Diagrammtypen sowie die Verwaltung von Benutzern und Alarmierungsregeln.

2. Voraussetzungen

- Ein funktionierender LXC-Container mit Ubuntu 22.04 oder 24.04 ist vorhanden.
 - Ein Benutzer mit `sudo`-Rechten im Container ist verfügbar (`pda1`).
 - Ein gültiges Serverzertifikat mit SAN-Eintrag (Subject Alternative Name) für die IP-Adresse des Grafana-Containers (IP `192.168.137.190`, DNS `grafana.local`) liegt vor.
 - Die eigene interne CA ist im Client-System vertrauenswürdig eingebunden.
-

3. System aktualisieren

```
sudo apt update && sudo apt upgrade -y
```

Erläuterung: Die Paketlisten des Systems werden aktualisiert und alle installierten Pakete auf den neuesten Stand gebracht. Dies stellt sicher, dass keine veraltete Softwarebasis verwendet wird.

4. Notwendige Pakete installieren

```
sudo apt install -y software-properties-common apt-transport-https wget curl gnupg2
```

```
pdal@grafana170:~$ sudo apt install -y software-properties-common apt-transport-https wget curl gnupg2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wget is already the newest version (1.21.4-1ubuntu4.1).
The following additional packages will be installed:
appstream dirmngr gir1.2-packagekitglib-1.0 gnupg gnupg-110n gnupg-utils gpg gpg-agent gpg-wks-client
libcurl3t64-gnutls libcurl4t64 libdktape207 libdwlt64 libglib2.0-bin libgstreamer1.0-0 libksba8 lib
libpolkit-agent-1-0 libpolkit-gobject-1-0 librtmp1 libssh-4 libstemmer0d libxmlb2 packagekit package
python3-cryptography python3-distro python3-httplib2 python3-jwt python3-launchpadlib python3-lazr.r
python3-pyparsing python3-six python3-software-properties python3-wadllib sgml-base unattended-upgrad
Suggested packages:
```

Erläuterung: Diese Pakete sind erforderlich, um externe Paketquellen einzubinden (apt-transport-https), Signaturen zu verarbeiten (gnupg2) und Dateien von entfernten Servern herunterzuladen (wget, curl).

5. Grafana-Repository einrichten

Da Grafana nicht zum Standard-Repository von Ubuntu zählt, fügen wir es dem Repository hinzu. Damit ist gewährleistet, dass bei System-Update/Upgrade auch Grafana überprüft wird.

```
# Vorbereitung für die moderne, sichere GPG-Key-Verwaltung
sudo mkdir -p /etc/apt/keyrings

# GPG-Signatur von Grafana herunterladen, dearmorieren und im keyrings-
# Verzeichnis speichern
wget -q -O - https://apt.grafana.com/gpg.key | gpg --dearmor | sudo tee
/etc/apt/keyrings/grafana.gpg > /dev/null

# Offizielles APT-Repository einbinden. Das 'signed-by' Attribut verweist auf den
# Keyring.
echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com stable
main" | sudo tee /etc/apt/sources.list.d/grafana.list

# Paketlisten aktualisieren
sudo apt update
```

```
Get:16 http://archive.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Fetched 5701 kB in 7s (800 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
pdal@grafana:~$
```

Erläuterung: Die GPG-Signatur von Grafana wird importiert, um die Integrität der Pakete sicherzustellen. Anschließend wird das offizielle APT-Repository von Grafana eingebunden und die Paketlisten erneut aktualisiert.

6. Grafana installieren

```
sudo apt install -y grafana
```

```
pdal@grafana1:~$ sudo apt install -y grafana
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  musl
The following NEW packages will be installed:
  grafana musl
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 176 MB of archives.
After this operation, 650 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble/universe amd64 musl amd
Get:2 https://apt.grafana.com stable/main amd64 grafana amd64 12.0.2
28% [2 grafana 39.5 MB/175 MB 23%]
```

Erläuterung: Das Grafana-Paket wird aus dem zuvor eingebundenen Repository heruntergeladen und installiert. Dabei werden die benötigten Dienste und Konfigurationsdateien im Verzeichnis `/etc/grafana/` abgelegt.

7. Grafana-Dienst aktivieren, starten und Status abfragen

```
sudo systemctl enable grafana-server
sudo systemctl start grafana-server
sudo systemctl status grafana-server
```

```
pdal@grafana1:~$ sudo systemctl enable grafana-server
sudo systemctl start grafana-server
Synchronizing state of grafana-server.service with SysV service script with /usr/lib/
Executing: /usr/lib/systemd/systemd-sysv-install enable grafana-server
Created symlink /etc/systemd/system/multi-user.target.wants/grafana-server.service ->
pdal@grafana1:~$ 
```



```
pdal@grafana1:~$ systemctl status grafana-server.service
● grafana-server.service - Grafana instance
  Loaded: loaded (/usr/lib/systemd/system/grafana-server.service; enabled; preset: enabled)
  Active: active (running) since Wed 2025-07-23 10:55:00 CEST; 47s ago
    Docs: http://docs.grafana.org
    Main PID: 6762 (grafana)
       Tasks: 9 (limit: 4389)
      Memory: 263.1M (peak: 264.7M swap: 1.5M swap peak: 1.7M)
        CPU: 7.693s
       CGroup: /system.slice/grafana-server.service
               `--8482 /usr/share/grafana/bin/grafana server --config=/etc/grafana/grafana.ini --
```

lines 1-10/10 (END)

Erläuterung:

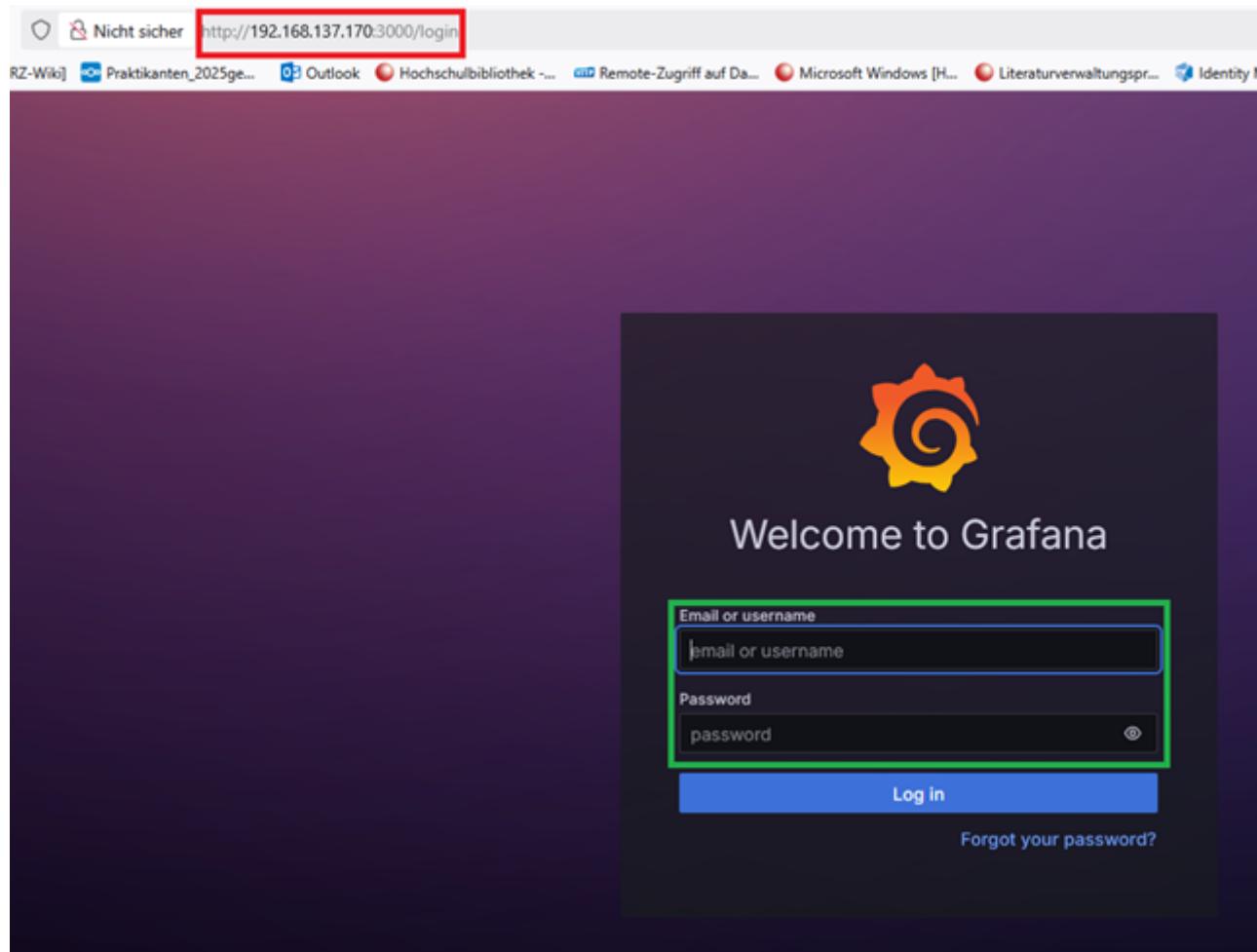
- Der Dienst `grafana-server` wird aktiviert, sodass er beim Systemstart automatisch gestartet wird.
- Anschließend wird der Dienst direkt gestartet, um die Weboberfläche bereitzustellen.
- Zum Schluss wird noch den Status abfragen um Sicher zu stellen, dass der Dienst sowohl `enabled` als auch gestartet ist.

8. Initialer Zugriff über HTTP

Browseraufruf:

```
http://<IP-Adresse>:3000
```

als Beispiel: <http://192.168.137.170:3000>



Erläuterung: Standardmäßig lauscht Grafana auf Port 3000 ohne Verschlüsselung. Die Anmeldung erfolgt mit dem Benutzer [admin](#) und dem Passwort [admin](#). Beim ersten Login wird ein neues Passwort festgelegt.

9. (Optional) TLS/SSL-Verschlüsselung mit internem SAN-Zertifikat

Wenn sie **Grafana** nur in PDAL verwenden ist dieser Schritt (9) nicht unbedingt notwendig.

9.1 Verzeichnisstruktur für Zertifikate anlegen

```
sudo mkdir -p /etc/grafana/certs
```

```
pdal@grafana170:~$ sudo mkdir -p /etc/grafana/certs
```

Erläuterung: Ein dediziertes Verzeichnis zur Ablage des Zertifikats und des privaten Schlüssels wird erstellt.

9.2 Zertifikat und Schlüssel kopieren

Die vorhandenen Zertifikate und Schlüssel müssen zuvor auf den Container hochgeladen werden. Eine genaue Beschreibung findet man in der Dokumentation [[0650 CA-sslmitSANZertifikat.md]] anhand des Beispiels Apache2. Auch bei Grafana ist es die gleiche Vorgehensweise.

```
sudo cp /etc/ssl/certs/server.cert.pem /etc/grafana/certs/
sudo cp /etc/ssl/private/server.key.pem /etc/grafana/certs/
sudo cp /etc/ssl/certs/ca.cert.pem /etc/grafana/certs/
```

```
pdal@grafana170:~$ sudo cp /etc/ssl/certs/ca.cert.pem /etc/grafana/certs/
pdal@grafana170:~$ sudo cp /etc/ssl/certs/server.cert.pem /etc/grafana/certs/
pdal@grafana170:~$ sudo cp /etc/ssl/certs/server.key.pem /etc/grafana/certs/
cp: cannot stat '/etc/ssl/certs/server.key.pem': No such file or directory
pdal@grafana170:~$ sudo cp /etc/ssl/private/server.key.pem /etc/grafana/certs/
pdal@grafana170:~$
```

```
sudo chmod 600 /etc/grafana/certs/*
```

```
pdal@grafana170:~$ sudo chmod 600 /etc/grafana/certs/*
pdal@grafana170:~$ ls -l /etc/grafana/certs/
total 12
-rw----- 1 root root 2098 Jul 23 11:17 ca.cert.pem
-rw----- 1 root root 1984 Jul 23 11:17 server.cert.pem
-rw----- 1 root root 1704 Jul 23 11:18 server.key.pem
pdal@grafana170:~$
```

Erläuterung: Das Serverzertifikat (server.cert.pem) und der private Schlüssel (server.key.pem) werden in das Grafana-Verzeichnis kopiert. Die Dateiberechtigungen werden so gesetzt, dass nur Root lesenden Zugriff hat.

⚠ Hinweis: Die Zertifikatsdatei (cert_file) sollte das Serverzertifikat und idealerweise die gesamte Zertifikatkette (Intermediate CA) enthalten..

9.3 TLS in der Grafana-Konfiguration aktivieren

```
sudo nano /etc/grafana/grafana.ini
```

Folgende Abschnitte anpassen:

```
[server]
protocol = https
http_port = 443
cert_file = /etc/grafana/certs/server.cert.pem
cert_key = /etc/grafana/certs/server.key.pem
;domain = grafana.local
;enforce_domain = true
```

Erläuterung: Die Kommunikation wird von HTTP auf HTTPS umgestellt. Die Zertifikatsdateien werden eingebunden.

⚠ Hinweis: Da kein DNS verwendet wird und das Zertifikat IP-Adressen im SAN enthält, werden `domain` und `enforce_domain` deaktiviert. Dadurch erfolgt kein Redirect auf nicht auflösbare Hostnamen.

9.4 Grafana neu starten

```
sudo systemctl restart grafana-server
```

Erläuterung: Die geänderte Konfiguration wird durch einen Neustart des Dienstes übernommen.

9.5 Zugriff über HTTPS testen

Browseraufruf:

<https://192.168.137.170>

Erläuterung: Grafana ist nun über HTTPS erreichbar. Wenn die interne CA im System des Clients eingebunden ist, erscheint keine Zertifikatswarnung.

9.6 CA-Zertifikat auf dem Client einbinden (optional)

Bei Systemen ohne eingebundene CA kann diese manuell installiert werden. **Linux (Debian/Ubuntu):**

```
sudo cp ca.crt /usr/local/share/ca-certificates/myca.crt  
sudo update-ca-certificates
```

Windows/macOS:

Das CA-Zertifikat muss manuell in den System-Zertifikatsspeicher als vertrauenswürdig importiert werden.

10. Datenquelle in Grafana hinzufügen

- Im Webinterface auf „Connections“ → „Data Sources“ navigieren.
- Eine unterstützte Datenquelle auswählen, z. B. PostgreSQL, InfluxDB, Prometheus.
- Zugangsdaten und Adresse der Quelle eintragen.
- Verbindung testen und speichern.

Erläuterung: Grafana verwendet „Data Sources“, um externe Systeme abzufragen und Daten in Panels darzustellen. Eine gültige Verbindung ist Voraussetzung für die Erstellung von Dashboards.

11. Dashboard erstellen

- Über das Menü „+ Create“ → „Dashboard“ auswählen.
- Neues Panel hinzufügen.
- Datenquelle auswählen und Abfrage definieren.

- Darstellung und Zeitbereich anpassen.

Erläuterung: Dashboards ermöglichen eine strukturierte Anzeige von Daten mit verschiedenen Visualisierungstypen (Graphen, Tabellen, Statistiken). Sie sind individuell anpassbar.

12. Benutzerverwaltung (optional)

Grafana bietet rollenbasierte Benutzerverwaltung:

- Admin: volle Rechte
- Editor: kann Dashboards bearbeiten
- Viewer: nur Leserechte

Erläuterung: Die Benutzerverwaltung erfolgt über das Webinterface unter „Server Admin“ → „Users“. Für LDAP/OAuth-Integration sind zusätzliche Konfigurationen erforderlich.

Weiterführende Nutzung

Diese Dokumentation behandelt nur grundlegende Funktionen von Grafana, wie das Hinzufügen von Datenquellen oder das Erstellen einfacher Dashboards.

Die Weboberfläche von Grafana bietet jedoch eine Vielzahl an weiteren Möglichkeiten zur Visualisierung, Alarmierung, Benutzerverwaltung und Integration externer Systeme. Es wird empfohlen, sich mit den erweiterten Funktionen vertraut zu machen, indem das interaktive Getting Started Tutorial auf der Startseite der Weboberfläche genutzt wird.

Zusätzlich bietet die offizielle Dokumentation unter:

<https://grafana.com/tutorials/>

einen umfassenden Überblick über alle verfügbaren Features, Konfigurationsoptionen und Best Practices für den produktiven Einsatz.

13. Deinstallation (optional)

```
sudo systemctl stop grafana-server
sudo apt purge --autoremove grafana -y
sudo rm -rf /etc/grafana /etc/apt/sources.list.d/grafana.list /etc/grafana/certs
```

Erläuterung: Grafana wird vollständig entfernt, inklusive Konfigurationen und Zertifikate.

14. Ergebnis

Grafana ist installiert und durch ein TLS-Zertifikat einer internen CA abgesichert. Die Weboberfläche ist über HTTPS erreichbar. Die Plattform ist einsatzbereit für die Anbindung von Datenquellen und die Erstellung von Dashboards.

 Sicherheitshinweis

Die Verwendung eines serverseitigen TLS-Zertifikats aus einer eigenen CA verbessert die Sicherheit in der internen Umgebung.

Quellen

- „Tutorials“, Grafana Labs. Zugegriffen: 23. Juli 2025. [Online]. Verfügbar unter: [Grafana Tutorials](#)
 - „Grafana fundamentals“, Grafana Labs. Zugegriffen: 23. Juli 2025. [Online]. Verfügbar unter: [Grafana Fundamentals](#)
 - „Grafana OSS and Enterprise | Grafana documentation“, Grafana Labs. Zugegriffen: 23. Juli 2025. [Online]. Verfügbar unter: [Grafana Doc](#)
 - „Set up Grafana HTTPS for secure web traffic | Grafana documentation“, Grafana Labs. Zugegriffen: 23. Juli 2025. [Online]. Verfügbar unter: [Grafana Setup](#)
 - „Technical documentation“, Grafana Labs. Zugegriffen: 23. Juli 2025. [Online]. Verfügbar unter: [Grafana](#)
-

Lizenz

Dieses Werk ist lizenziert unter der **Creative Commons Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz**.

[Zum Lizenztext auf der Creative Commons Webseite](#)