So konfigurieren Sie entfernte Prometheus und Grafana für die Überwachung von Secure Malware Analytics (ehemals Threat Grid) Appliance

Inhalt

Einleitung

In der Secure Malware Analytics (SMA) Appliance bieten wir kein SNMP-Protokoll zur Überwachung der Ressourcennutzung der Appliance an, sondern die Appliance bietet Prometheus.

In diesem Dokument wird beschrieben, wie Sie eine entfernte Prometheus-Instanz konfigurieren und Grafanato verwenden, um die von der Appliance gezogenen Daten zu visualisieren.

Voraussetzungen

Laden Sie die folgenden Tools herunter, und installieren Sie sie auf Ihrem lokalen Computer/Server:

- Prometheus -https://prometheus.io/download/
- Grafana: https://grafana.com/oss/grafana/

Anforderungen

- Secure Malware Analytics (SMA) Appliance-Software Version 2.18 und höher
- Windows-Computer
- Administratorzugriff auf die Admin-Konsole der Einheit (Opadmin)
- Secure Malware Analytics (SMA) Appliance Opadmin SSL-Zertifikat Vertrauenswürdig durch lokalen Computer

Verwendete Komponenten

- Secure Malware Analytics (SMA) Appliance
- Windows 11 Pro
- Prometheus
- Grafana

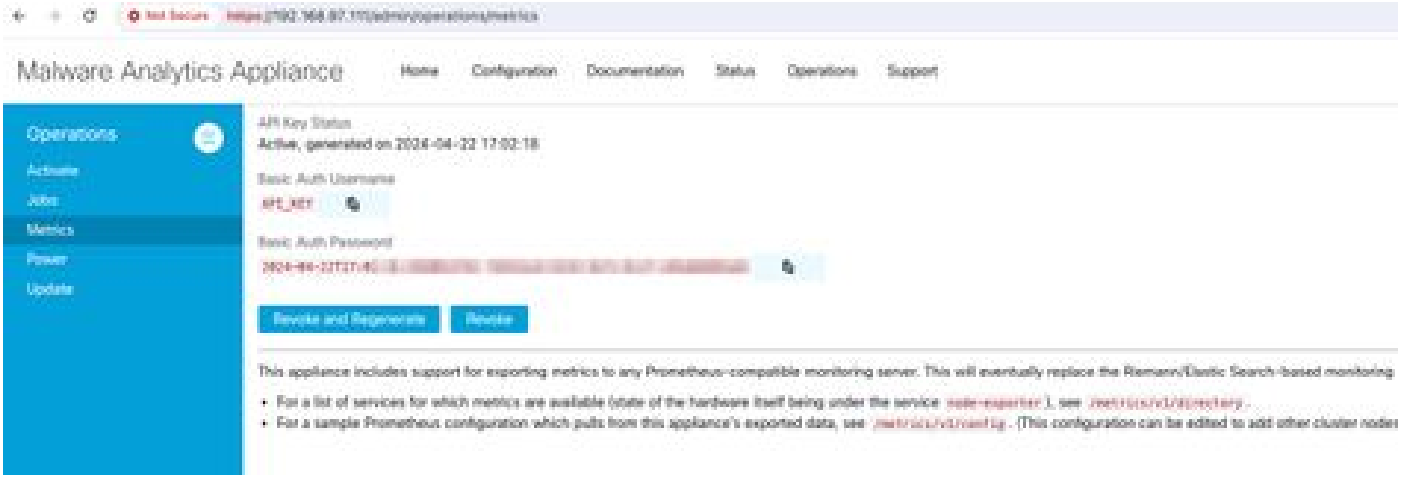
Konfigurieren

Für dieses Dokument haben wir einen Windows 11 Pro als Remote-Host verwendet, auf dem Prometheus und Grafana installiert wurden. Diese Tools sind auch für Linux oder MacOS verfügbar.

1. API-Schlüssel in Secure Malware Analytics (SMA) Appliance für den Zugriff auf Metriken generieren

Melden Sie sich bei SMA Appliance Opadmin an. API-Schlüssel für Kennzahlen generieren von Opadmin > Vorgang > Kennzahlen

2. Es werden ein einfacher Benutzername und ein einfaches Kennwort für die Authentifizierung generiert, die in der Remote-Prometheus-Konfiguration verwendet werden müssen.



3. Prometheus installieren und konfigurieren

Folgen Sie den Anweisungen in den Prometheus Benutzerhandbüchern, um Ihre Instanz zu installieren, wenn Sie Linux oder MacOS verwenden. Für dieses Dokument haben wir Prometheus auf einem Windows 11-Computer installiert, und für den Installationsvorgang haben wir dieses

Youtube-Video verfolgt.

4. Erstellen Sie eine Konfigurationsdatei mit dem Namen `prometheus`.yml mit folgendem Inhalt:

```
scrape_configs:
  - job_name: metrics
    scheme: https
    file_sd_configs:
      - files:
        - 'targets.json'

    relabel_configs:
      - source_labels: [__address__]
        regex:  '[^/]+(/.*)'            # capture '/...' part
        target_label: __metrics_path__  # change metrics path
      - source_labels: [__address__]
        regex:  '([^/]+)/.*'            # capture host:port
        target_label: __address__       # change target
    basic_auth:
      username: "API_KEY"
      password: "2024-04-22T15:32:14.082689318Z xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
```

5. im Abschnitt `basic_auth` den in Schritt 1 generierten Benutzernamen und das Kennwort für die grundlegende Authentifizierung verwenden.

6. Laden Sie die Konfiguration der Services herunter, aus denen Sie Kennzahlen abrufen können, indem Sie nach der Anmeldung bei Opadmin Folgendes in die Benutzeroberfläche eingeben:

```
https://<opadmin IP>/metrics/v1/config
```

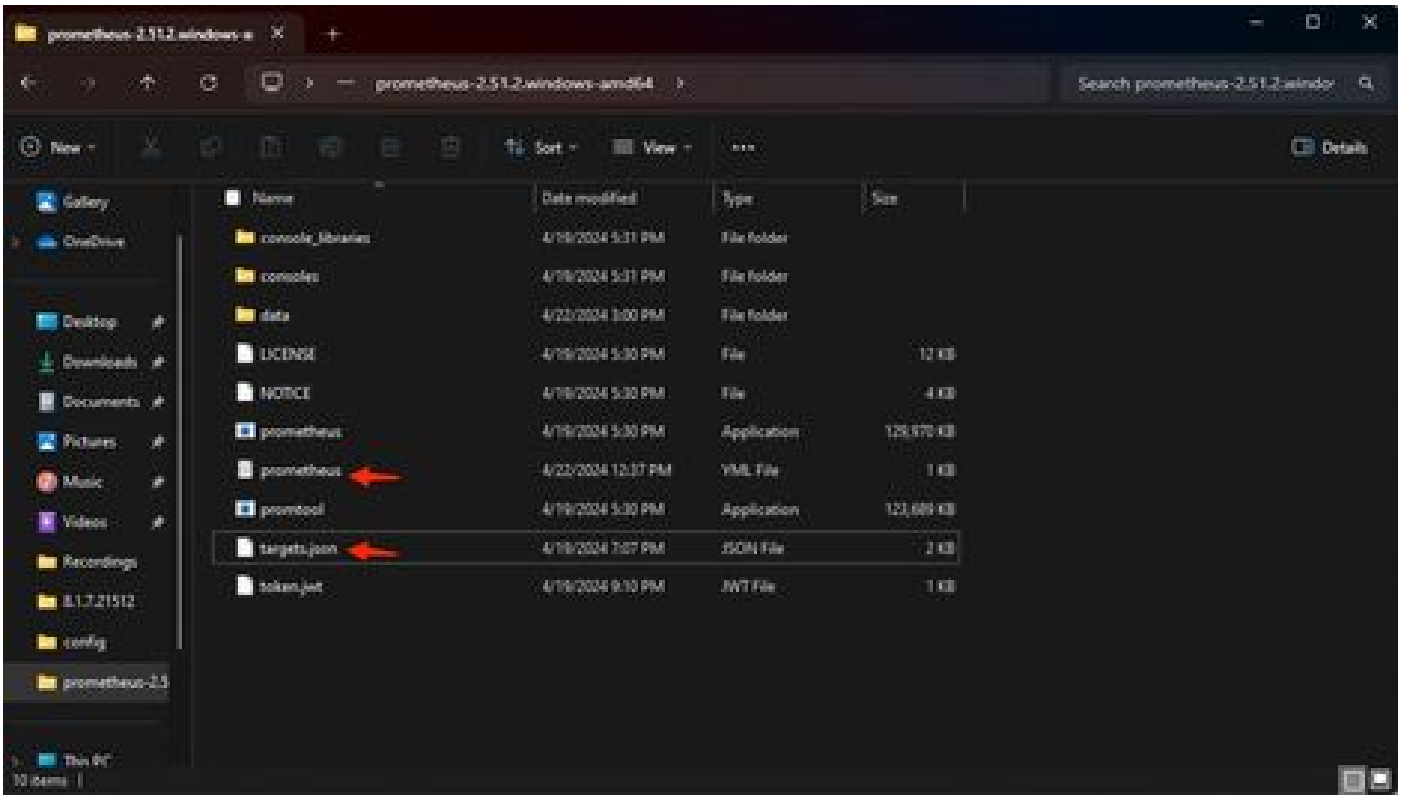
Sie erhalten u. a. Folgendes:

```
[{"labels":{"service":"classifier"},"targets":["192.168.97.111:443/metrics/v1/service/classifier"]},{"l
```

Hier ist `192.168.97.11` die Admin-IP für meine SMA-Appliance.

7. Erstellen Sie eine Datei mit dem Namen `targets.json`, und kopieren Sie den oben genannten Inhalt in diese Datei.

8. Kopieren Sie `prometheus.yml` und `targets.json` in das Verzeichnis Prometheus (folgen Sie den Installationsanleitungen), Für Windows habe ich einen Ordner in Laufwerk C:\ erstellt und die Prometheus-Installationsdateien dort extrahiert. Dann kopierte `prometheus.yml` und `targets.json` in den gleichen Ordner.



9. Prometheus starten

Starten Sie Prometheus. Für Windows führen Sie `prometheus.exe` über die Befehlszeile aus.

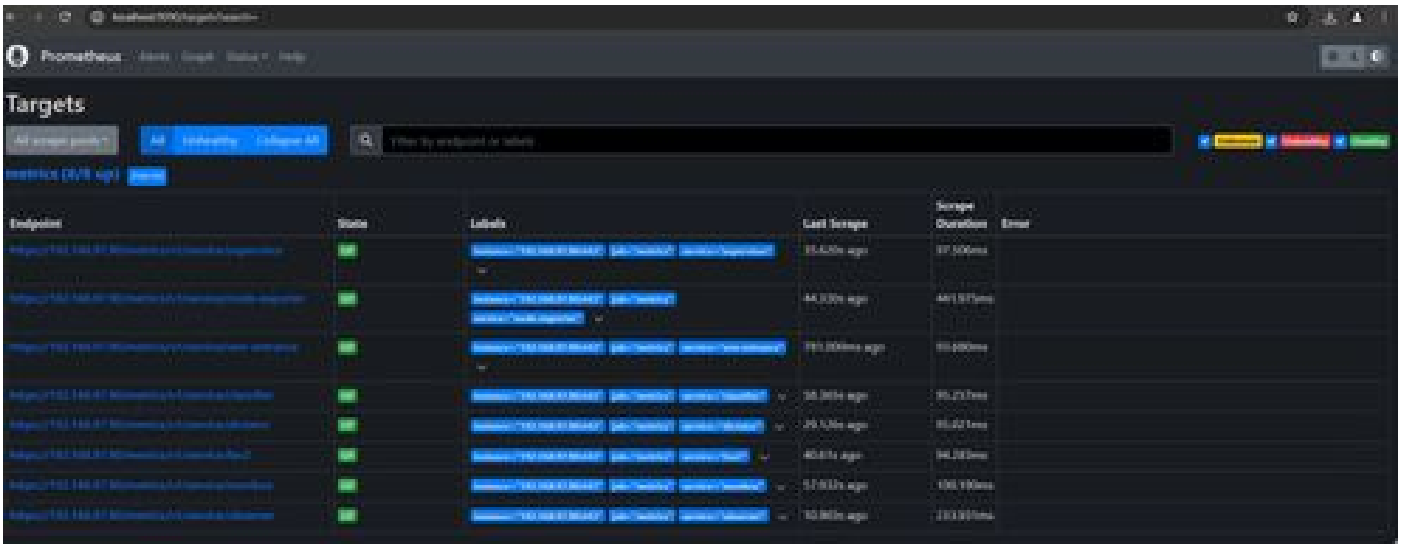
```
C:\Prometheus\prometheus-2.51.2.windows-amd64\prometheus-2.51.2.windows-amd64>prometheus.exe
```

Dadurch wird der Prometheus gestartet und die Kennzahlen aus der SMA-Appliance abgerufen. Hinweis: Schließen Sie die Befehlszeile nicht, da Prometheus sonst heruntergefahren wird.

10. Um zu überprüfen, ob Ihre lokale Prometheus-Instanz in der Lage ist, Metriken aus der SMA-Appliance zu ziehen, laden Sie Prometheus UI - `http://localhost:9090/`.

11. Gehe zu `Status` > `Ziele` - http://localhost:9090/targets?search=

Innerhalb weniger Minuten sollten Sie alle Ziele und den Status UP sehen.



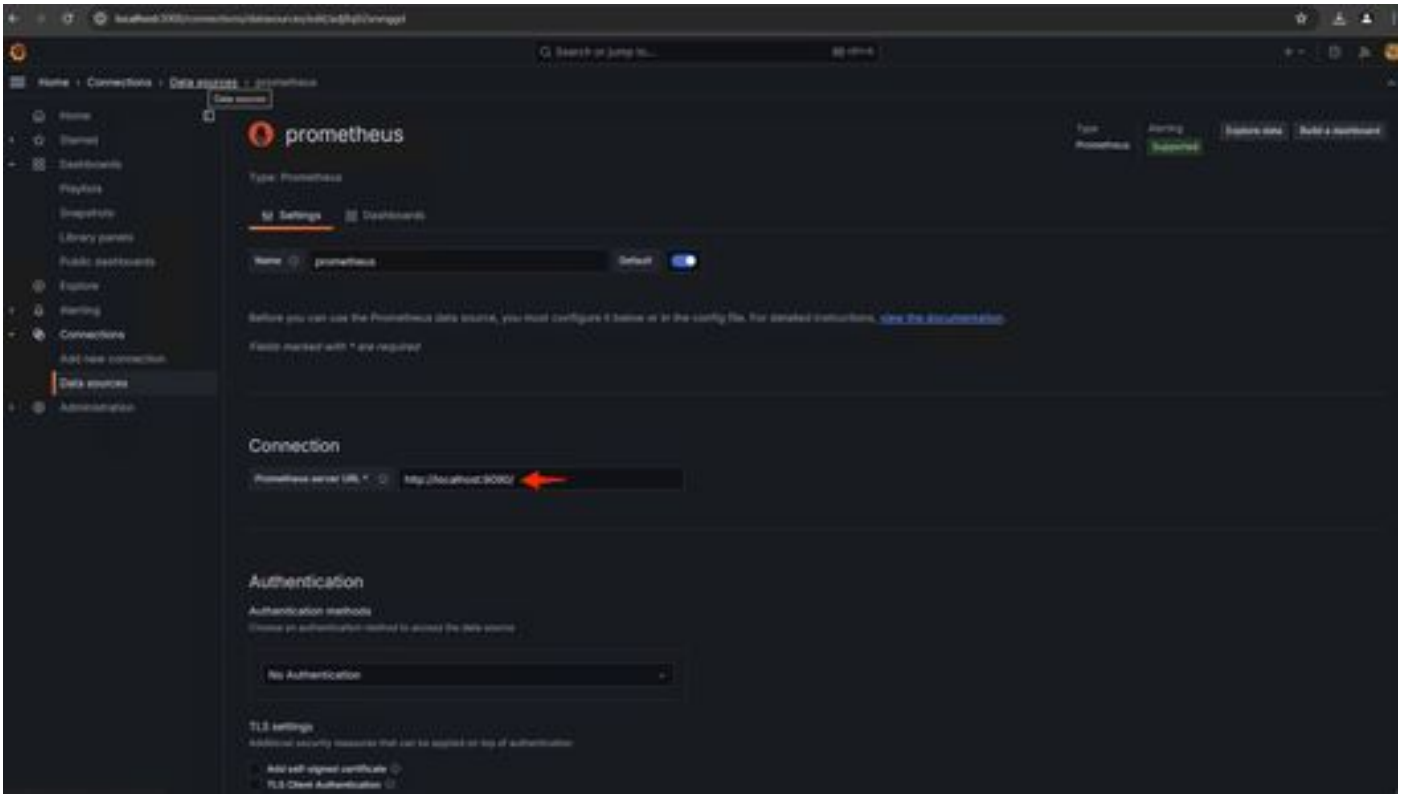
12. Grafana installieren und konfigurieren

Laden Sie die Grafana-Programmdatei von Grafana Labs herunter. Installieren Sie Granafa und befolgen Sie die Anweisungen des Installers.

13. Nach der Installation von Grafana Access UI im Browser -`http://localhost:3000/`

Gehen Sie zu **Startseite > Verbindungen > Datenquellen** - `http://localhost:3000/connections/datasources`

`Wählen Sie Add New Datasource (Neue Datenquelle hinzufügen)` und `SelectPrometheus` aus der Liste aus. Geben Sie "http://localhost:9090/" als Prometheus Server-URL ein.



Wählen Sie unten auf dieser Seite `Speichern und testen aus`. Nach einem erfolgreichen Test können wir ein Dashboard erstellen.

14. Grafana Dashboard erstellen

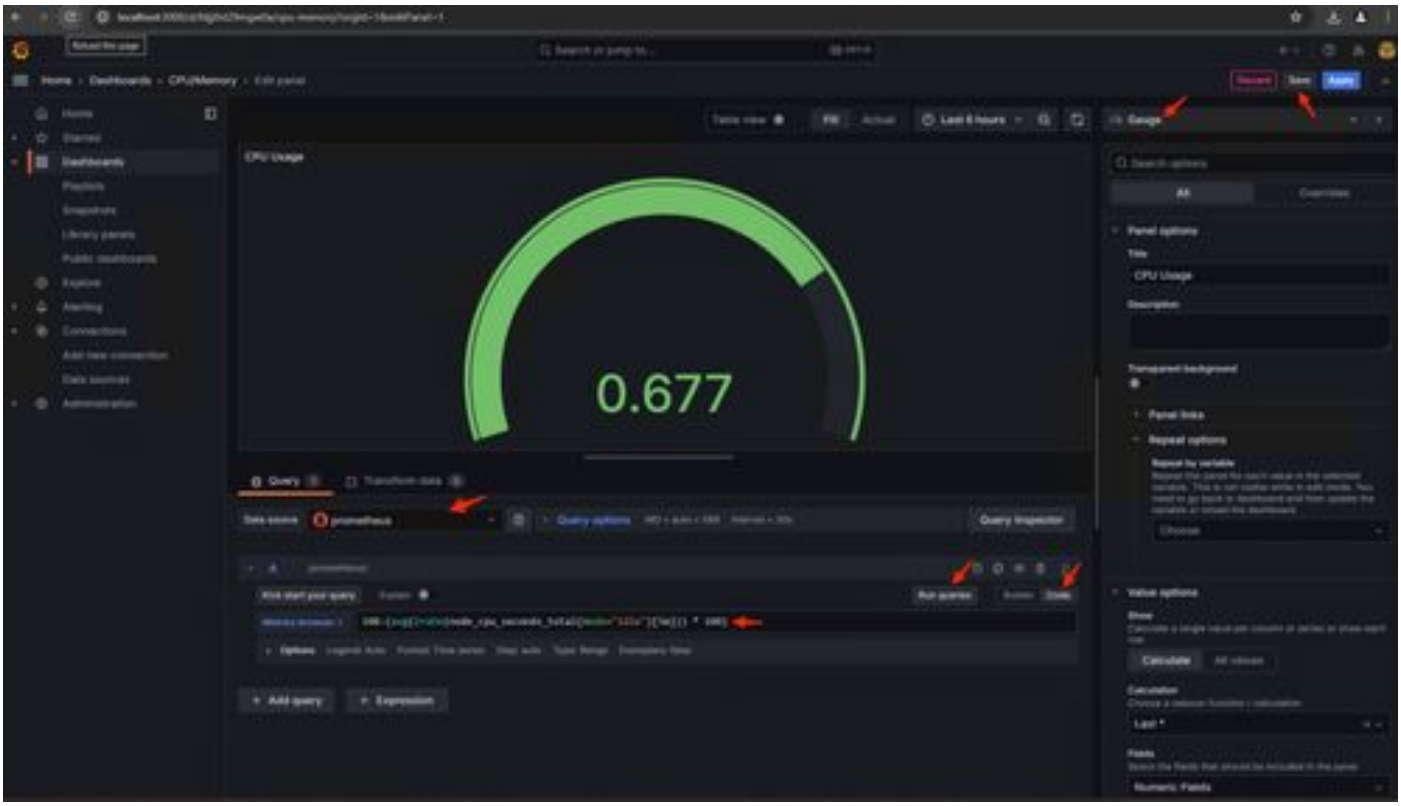
Gehen Sie `zu Dashboards` in Grafana UI , `Wählen Sie Dashboard erstellen`>`Visualisierung hinzufügen`. `Wählen Sie` Prometheus Data Source.

Wählen Sie im Abfrage-Generator Codeinput, Visualisierungstyp auswählen (I selected Gage)

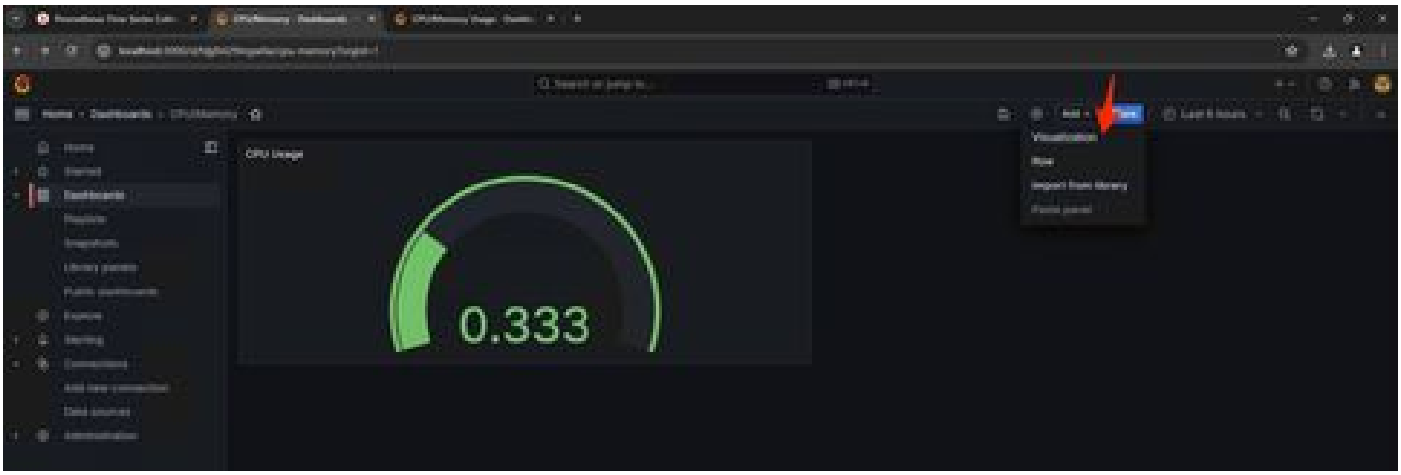
Geben Sie die folgende Abfrage **für CPU-Auslastung ein**:

```
100-(avg(irate(node_cpu_seconds_total{mode="idle"}[5m])) * 100)
```

15. Klicken Sie auf `Run` Queriesund Sie sollten eine Visualisierung der CPU-Nutzung wie diese sehen -

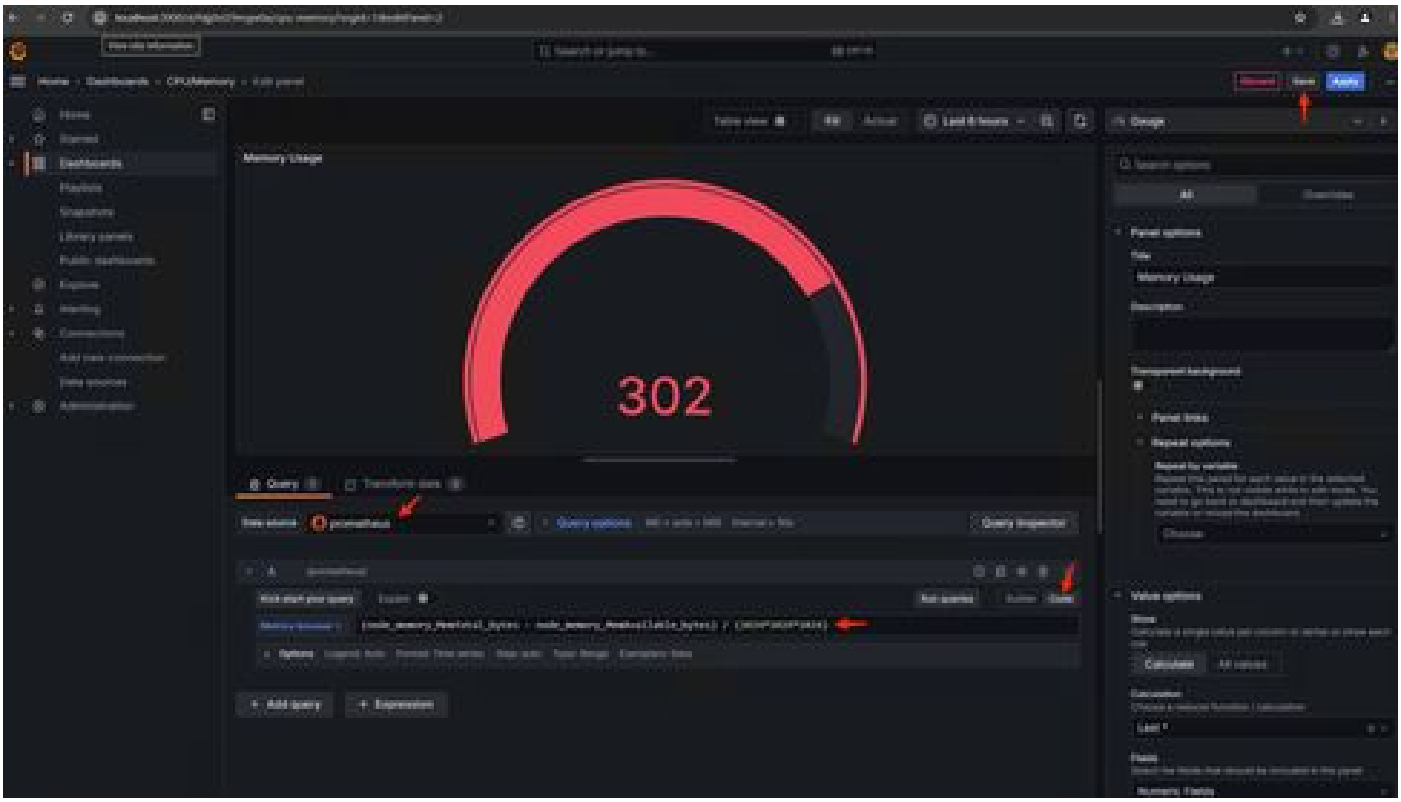


16. Speichern Sie den Bereich, nennen Sie das Dashboard und speichern Sie. Weitere `Visualisierung` für die Speichernutzung hinzufügen -



17. Verwenden Sie für die Speichernutzung die folgende Abfrage

```
(node_memory_MemTotal_bytes - node_memory_MemAvailable_bytes) / (1024*1024*1024)
```



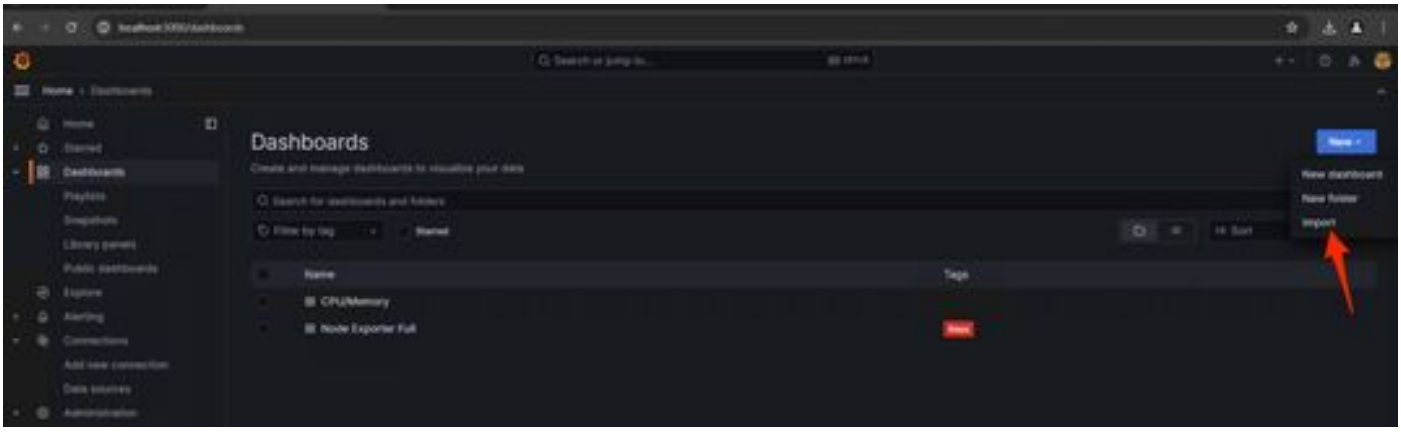
18. Speichern Sie die Änderungen, und Sie sollten ein Dashboard wie dieses haben -

19. Weitere Hardware- und Software-Metriken sind verfügbar. Klicken Sie für Details auf die Links `in` "Opadmin> `Metriken`".

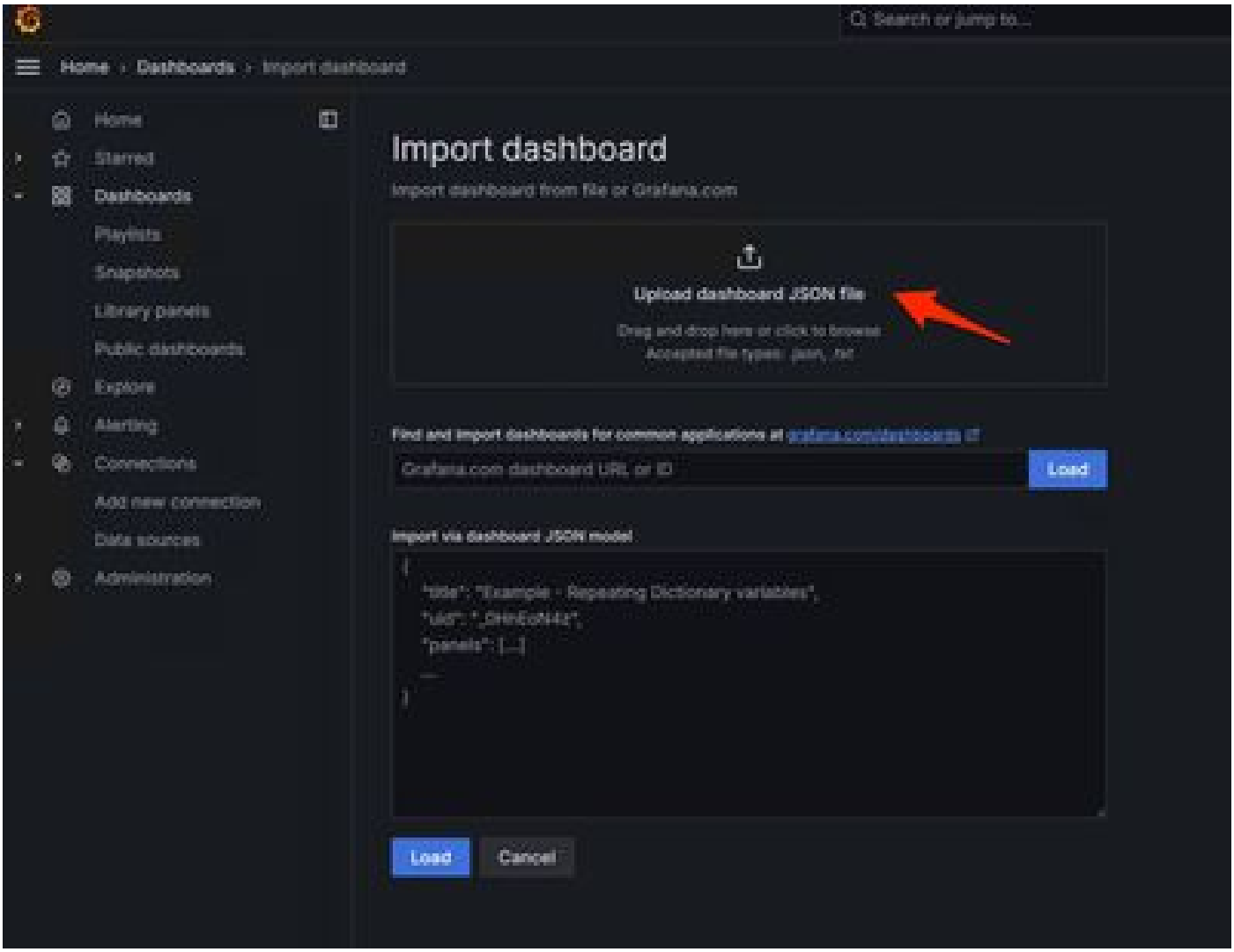
Grafana Dashboard-Vorlage

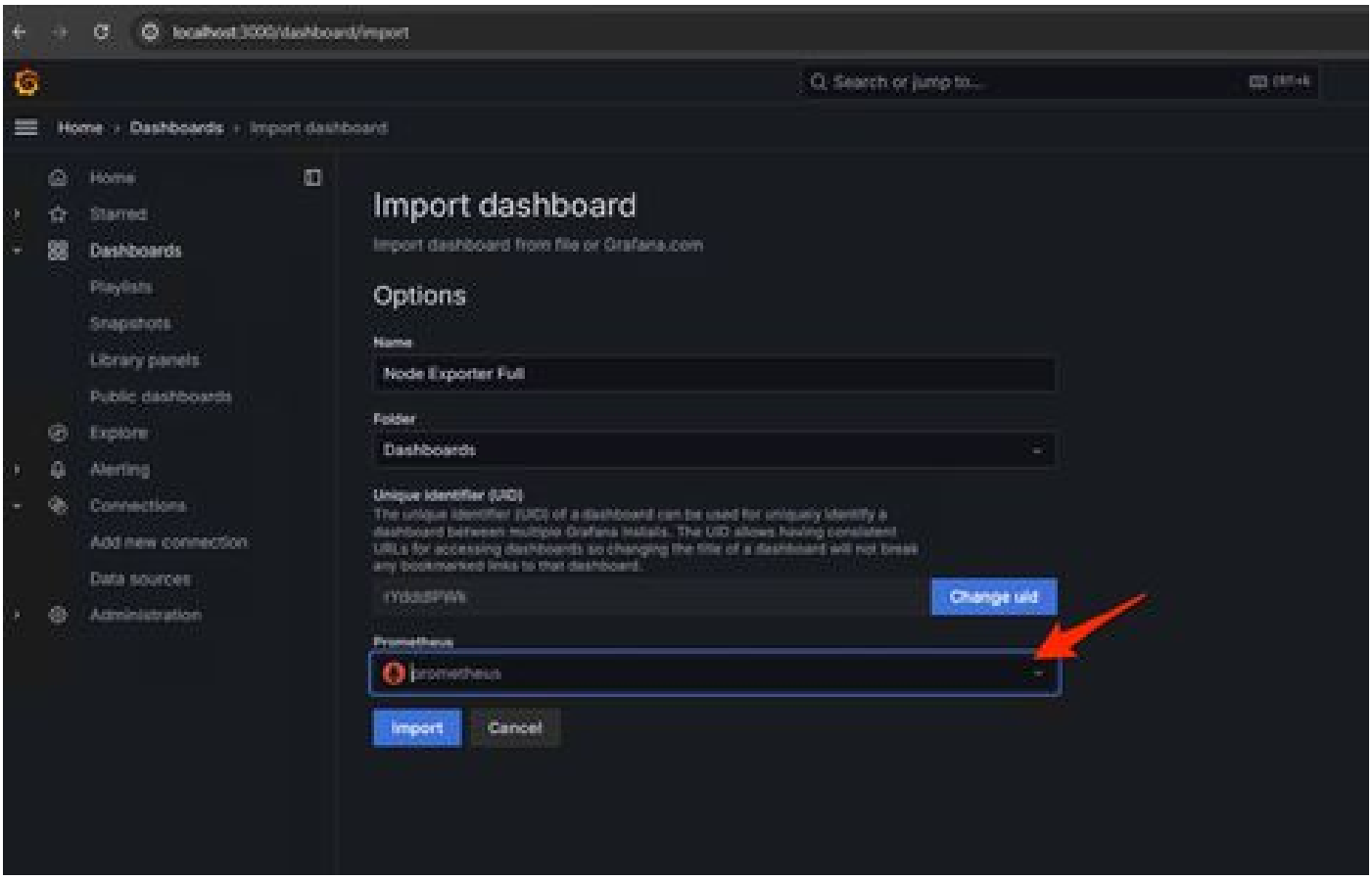
Es gibt viele Grafana Dashboard Vorlagen für Node Exporter auf der Grafana Website. Eines davon ist - Node Exporter Full

1. Um dieses Dashboard in Ihre Grafana-Instanz zu importieren Laden Sie die JSON-Datei in Grafana herunter

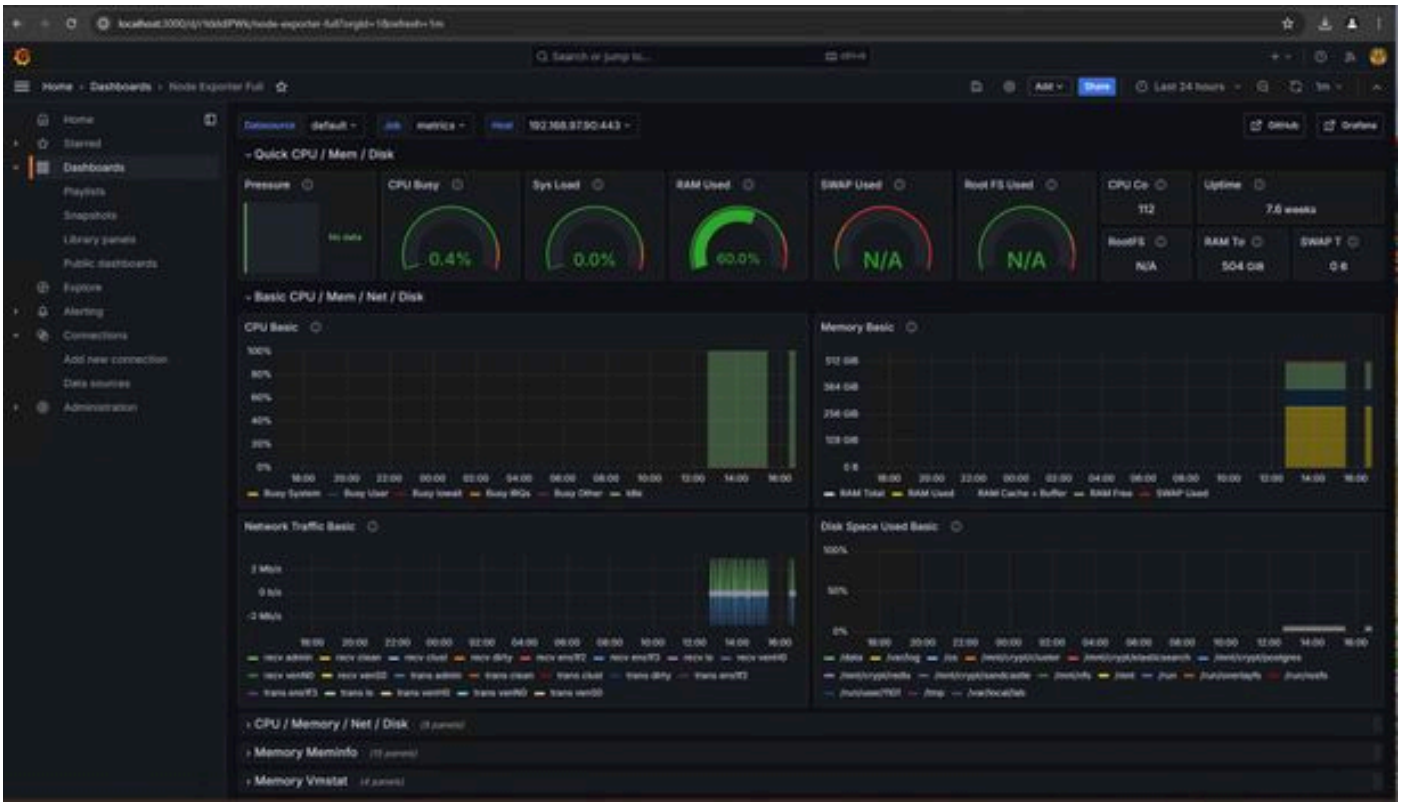


2. Laden Sie die JSON-Datei hoch und wählen Sie diePrometheus-Datenquelle aus.





3. Dadurch wird ein Dashboard mit vielen Hardware-Informationen erstellt (nicht alle Panel-Metriken sind verfügbar)-



Fehlerbehebung

Wenn der Prometheus keine Verbindung herstellen und keine Kennzahlen von der SMA-Appliance abrufen konnte, wird der Fehler unter

Status > Targets - http://localhost:9090/targets?search=

Wenn ein Fehler vorliegt, muss dieser behoben werden, bevor die Daten abgerufen werden können. Häufiges Problem ist das SSL-Zertifikat der SMA-Appliance Opadmin wird vom lokalen Computer nicht als vertrauenswürdig eingestuft. Stellen Sie sicher, dass Sie ein SMA-Administratorzertifikat mit IP- und DNS-SAN erstellen und die Signing Root-Zertifizierungsstelle zum Vertrauensspeicher des lokalen Computers hinzufügen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.