Hoe kan ik Remote Prometheus en Grafana configureren om Secure Malware Analytics (voorheen Threat Grid)-applicatie te bewaken

Inhoud

Inleiding

In de Secure Malware Analytics (SMA)-applicatie bieden we geen SNMP-protocol om het gebruik van de apparaatbronnen te controleren. In plaats daarvan biedt het apparaat Prometheus.

In dit document wordt beschreven hoe u een externe Prometheus-instantie kunt configureren en kunt u Grafanato gebruiken om de gegevens die uit het apparaat zijn gehaald te visualiseren.

Voorwaarden

Download en installeer de volgende tools op uw lokale machine/server:

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

Vereisten

- Software voor Secure Malware Analytics (SMA)-applicatie, versie 2.18 en hoger
- Windows-machine
- Admin-toegang tot Application Admin (Opadmin) console
- Secure Malware Analytics (SMA)-applicatie Opadmin SSL-certificaat betrouwbaar door de lokale machine

Gebruikte componenten

- Secure Malware Analytics (SMA)-applicatie
- Windows 11 Pro-machine
- Prometheus

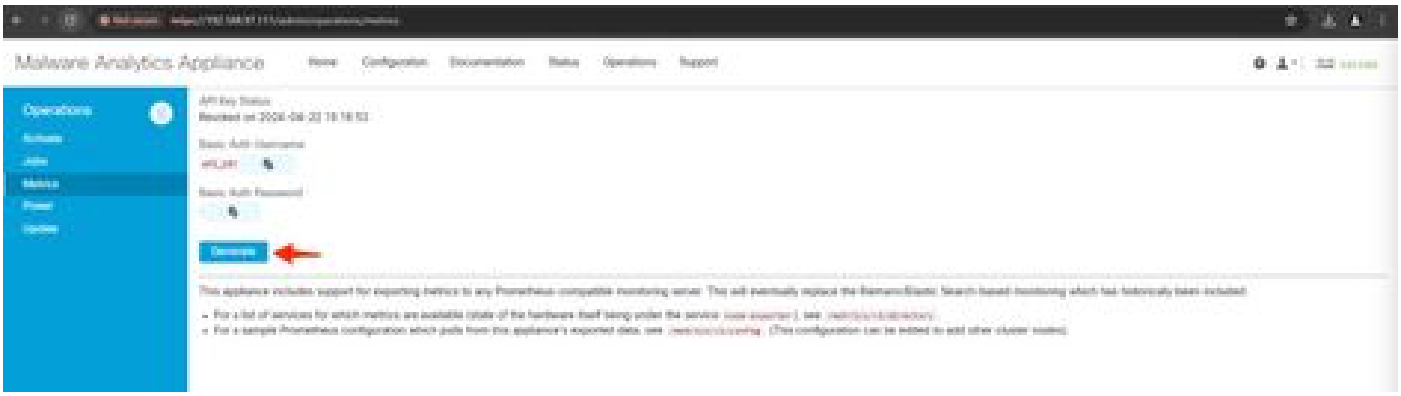
- Grafana

Configureren

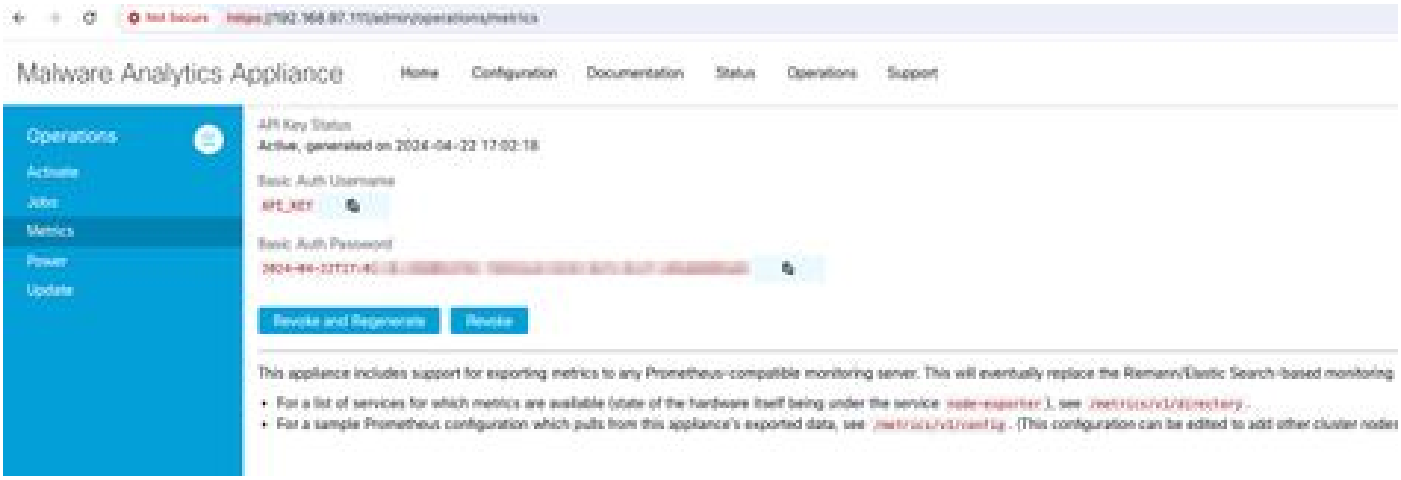
Voor dit document hebben we een Windows 11 Pro gebruikt als een externe host waar we Prometheus en Grafana hebben geïnstalleerd. Deze tools zijn ook beschikbaar voor Linux of MacOS.

1. Genereer API-sleutel in Secure Malware Analytics (SMA)-applicatie voor toegangsmetriek

Aanmelden bij SMA-applicatie Opadmin. Genereer API-sleutel voor metriek vanuit Opadmin > Bediening > Metriek



2. Er wordt een Basis Autorisatie Gebruikersnaam en Wachtwoord gegenereerd die we zullen moeten gebruiken in Remote Prometheus configuratie.



3. Installeer en configureer Prometheus

Volg de instructies van de Prometheus-gebruikershandleidingen om uw exemplaar te installeren als u Linux of MacOS gebruikt. Voor dit document hebben we Prometheus op een Windows 11-machine geïnstalleerd en voor het installatieproces hebben we deze Youtube-video gevolgd.

4. Maak een configuratiebestand met de naam `prometheus.yml`met de volgende inhoud -

```
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. Gebruik in de sectie `basic_auth` de gebruikersnaam en het wachtwoord voor de basisautorisatie die in Stap 1 gegenereerd zijn.

6. Trek de configuratie van de diensten waar u metriek uit kunt halen door het volgende in te voeren in de UI na het inloggen in Opadmin -

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

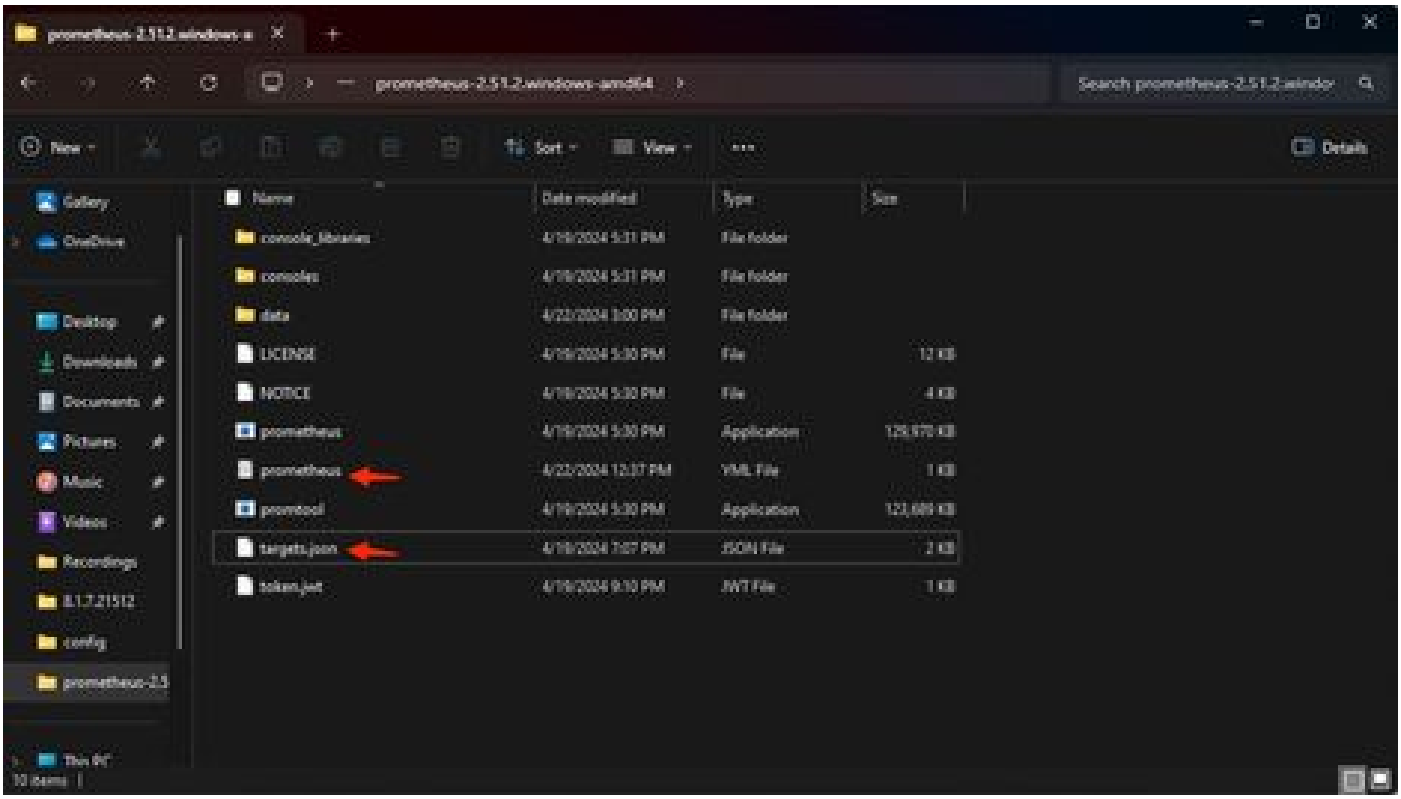
Je krijgt iets als -

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

Hier is `192.168.97.111` Admin IP voor mijn SMA-apparaat.

7. Maak een bestand met de naam `targets.json` en kopieer de bovenstaande inhoud naar dat bestand.

8. Kopieer `prometheus.yml` en `targets.json` naar de Prometheus directory (volg de installatiehandleidingen), Voor Windows heb ik een map aangemaakt in C:\ station en heb daar de Prometheus installatiebestanden gehaald. Vervolgens kopieerde `prometheus.yml` en `targets.json` naar dezelfde map.



9. Start Prometheus

Start Prometheus. Voor Windows voert u `prometheus.exe uit` vanaf de opdrachtregel.

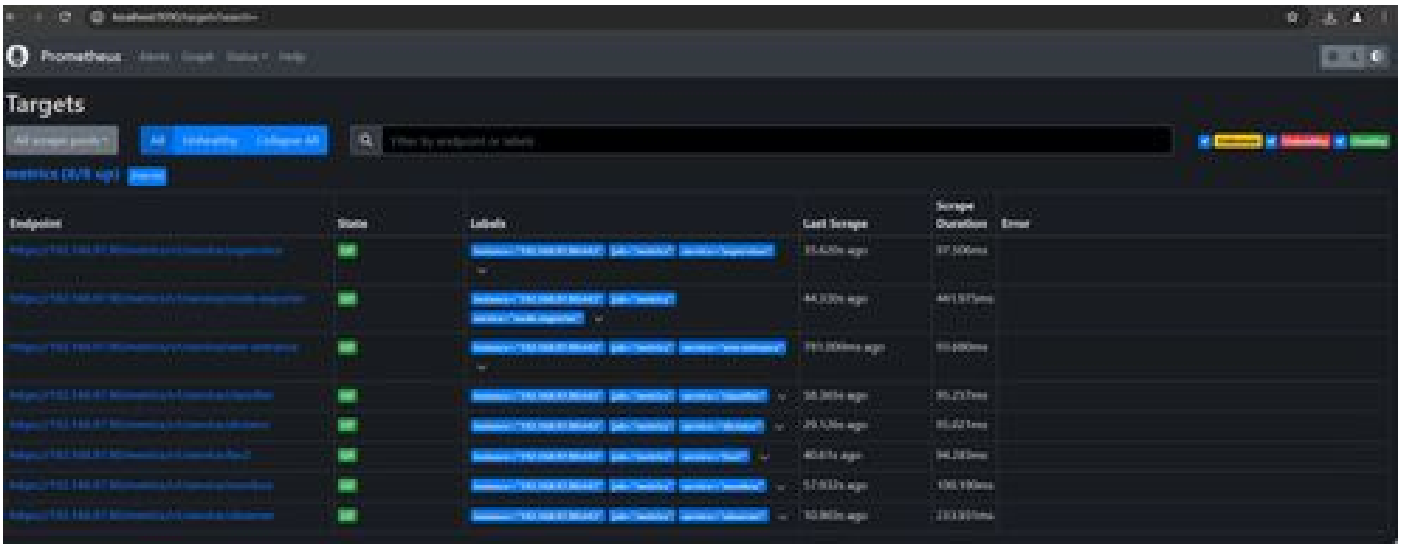
```
C:\Prometheus\prometheus-2.51.2.windows-amd64\prometheus-2.51.2.windows-amd64>prometheus.exe
```

Hiermee start u de Prometheus en trekt u de metriek uit het SMA-apparaat. Opmerking: sluit de opdrachtregel niet of Prometheus sluit af.

10. Om te controleren of uw lokale instantie Prometheus metriek kan trekken van SMA-applicatie load Prometheus UI - "http://localhost:9090/"

11. Ga naar `Status` > `Doelstellingen` - http://localhost:9090/targets?search=

Binnen een paar minuten moet u alle doelen en status `UP` zien.



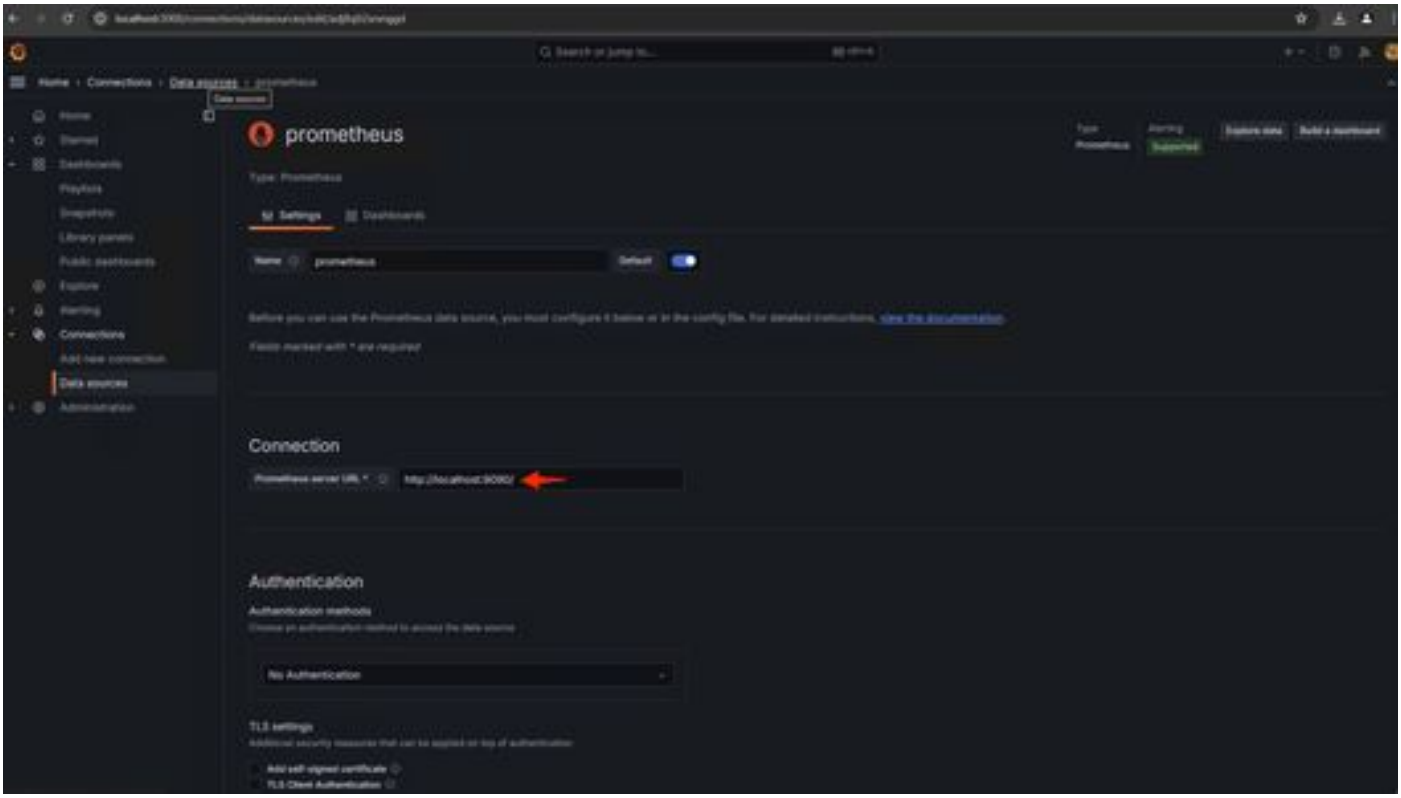
12. Grafana installeren en configureren

Download de Grafana uitvoerbaar van Grafana Labs. Installeer Granafa en volg de instructies van de installateur.

13. Na het installeren van Grafana Access UI in de browser -`http://localhost:3000/`

Ga naar **startpunt > Verbindingen > Gegevensbronnen** - 'http://localhost:3000/connections/datasources'

`Selecteer Nieuwe Datasource` en `SelectPrometheus` uit de lijst. Voer de URL van de Prometheus-server in op ‘http://localhost:9090/’



`Selecteer` onder aan die pagina `de optie Opslaan en testen`. Na een succesvolle test kunnen we een Dashboard maken.

14. Grafana Dashboard maken

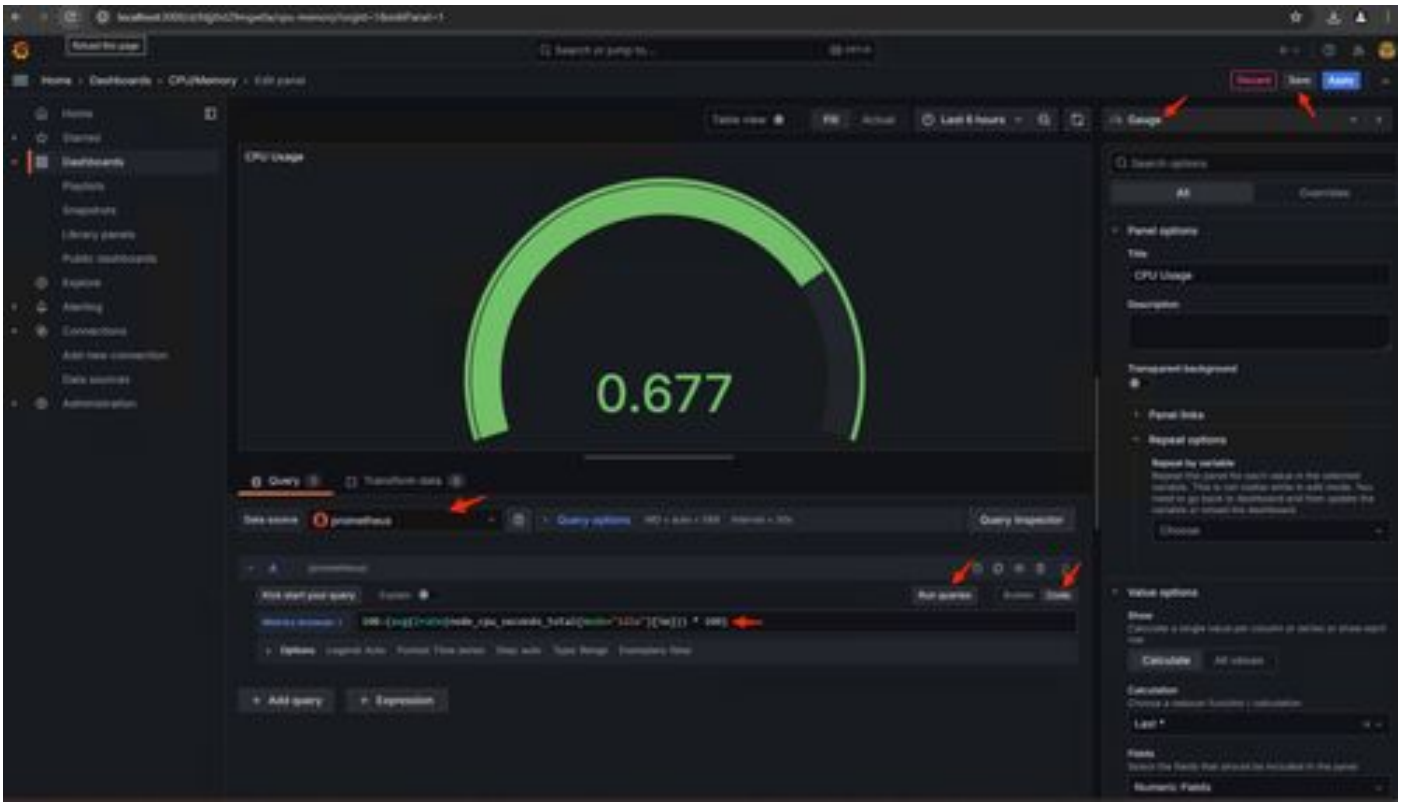
Ga `naar Dashboards` in Grafana UI, `selecteerCreate Dashboard`>`Add visulization`. `Selecteer Prometheus`-gegevensbron.

In Query builder selectCodeinput, Selecteer Type Visualisatie (Ik heb gekozen Gauge)

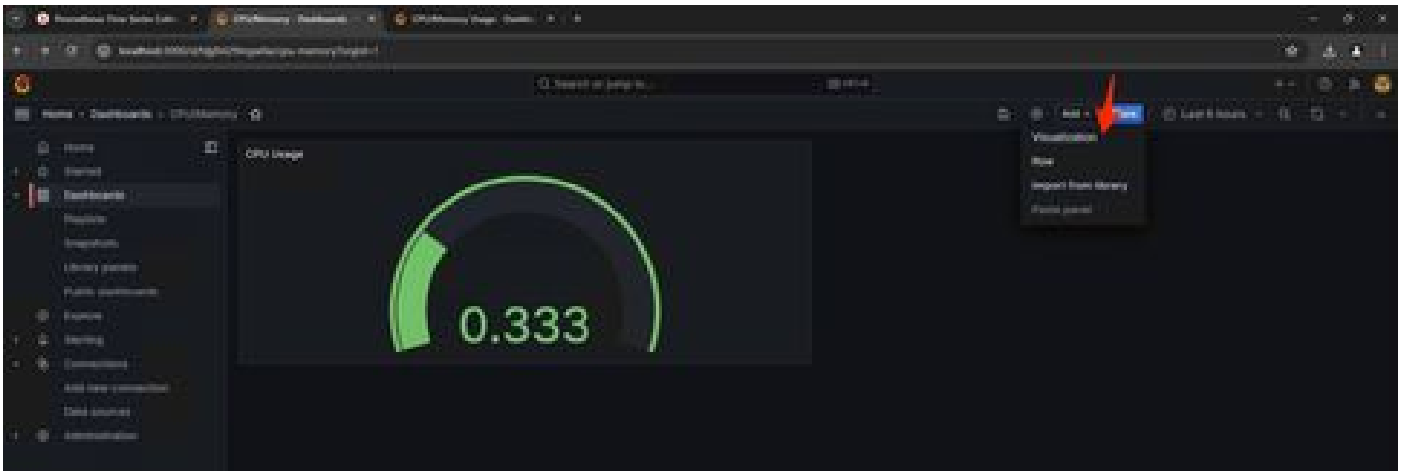
Voer de volgende vraag **voor CPU-gebruik in** -

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

15. Klik op `Run` Queriesen je moet een visualisatie zien van CPU-gebruik zoals dit -

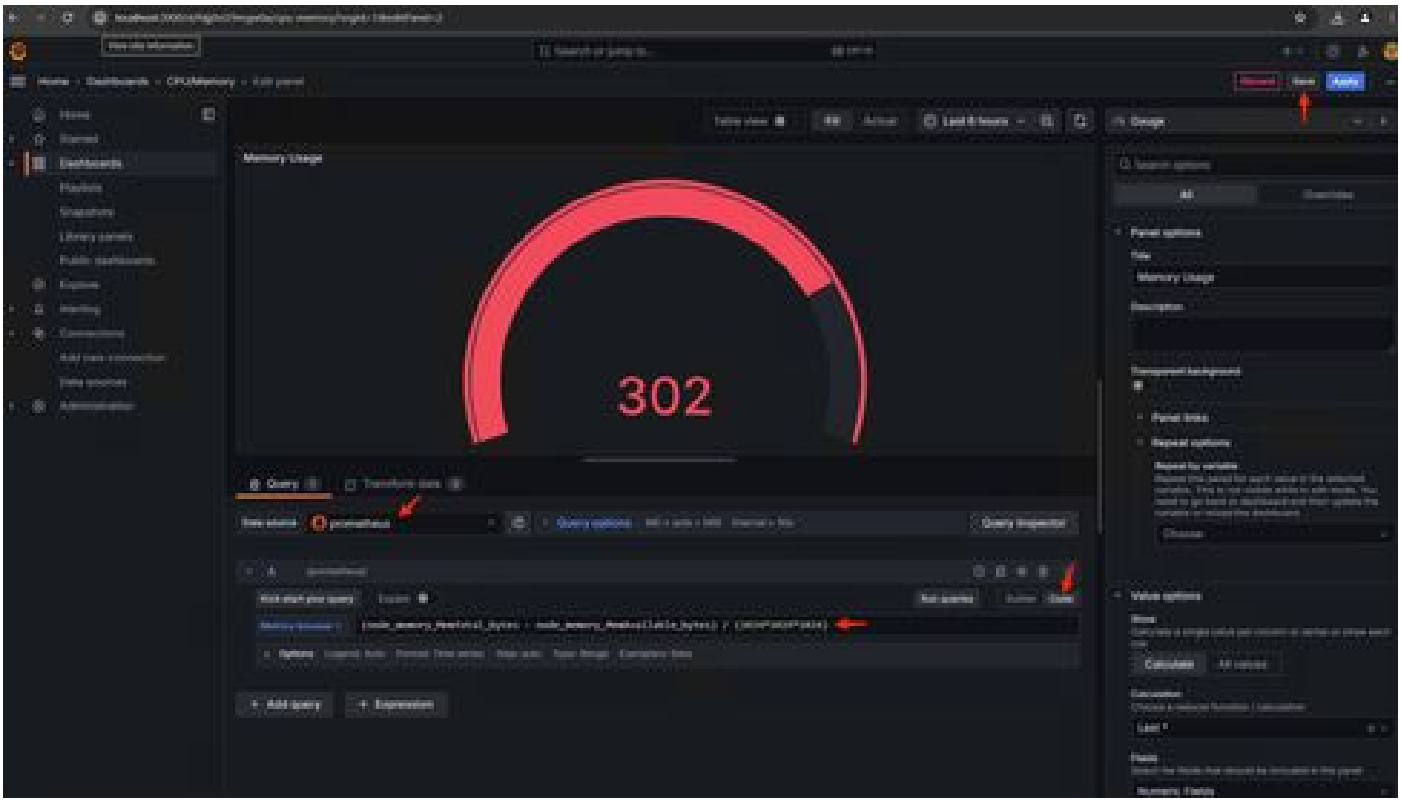


16. Sla het paneel op, geef het Dashboard een naam en sla op. Voeg een andere `Visualisatie toe` voor geheugengebruik -



17. Gebruik voor geheugengebruik de volgende query

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



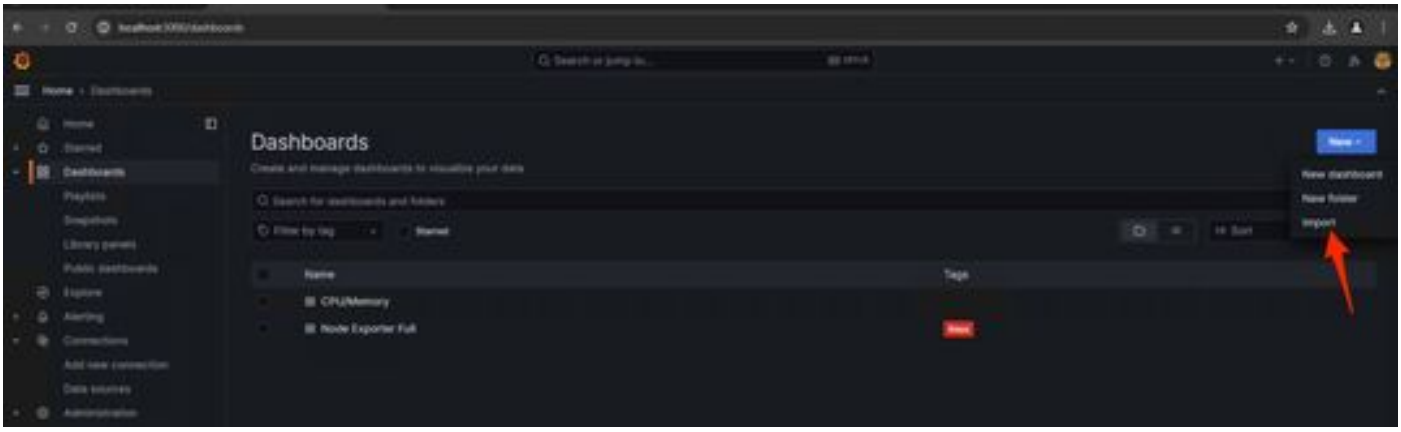
18. Sla de wijzigingen op en je moet een dashboard als dit hebben -

19. Er zijn andere hardware- en softwarematige gegevens beschikbaar. Klik voor meer informatie op de links `in Opadmin`> `Metrics` page

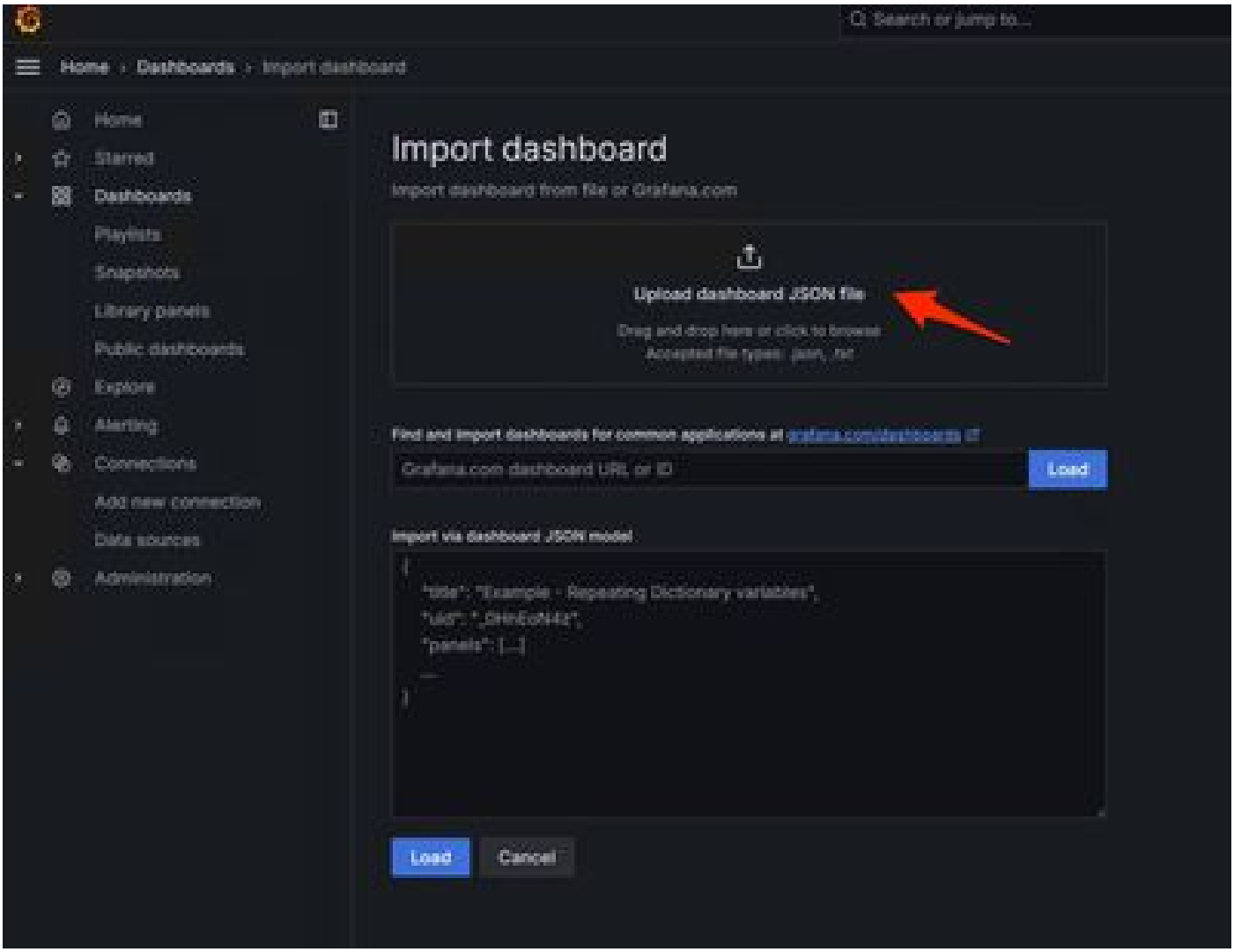
Grafana Dashboard Template

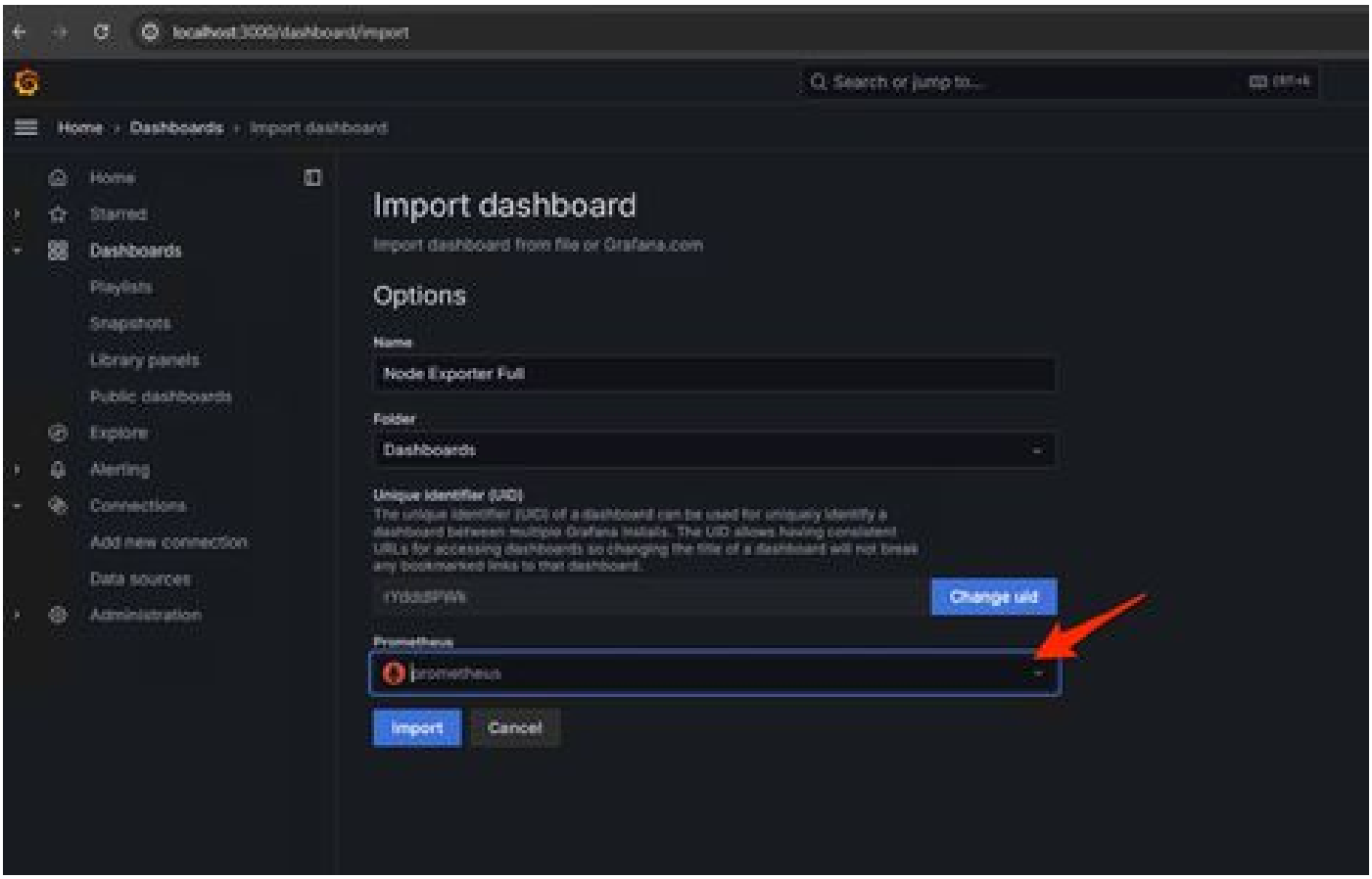
Er zijn veel Grafana Dashboard sjablonen beschikbaar voor Node Exporter op de Grafana website. Een daarvan is - Node Exporter Full

1. Om dit dashboard te importeren naar uw Grafana instantie Download de JSON, importeer het JSON-bestand in Grafana

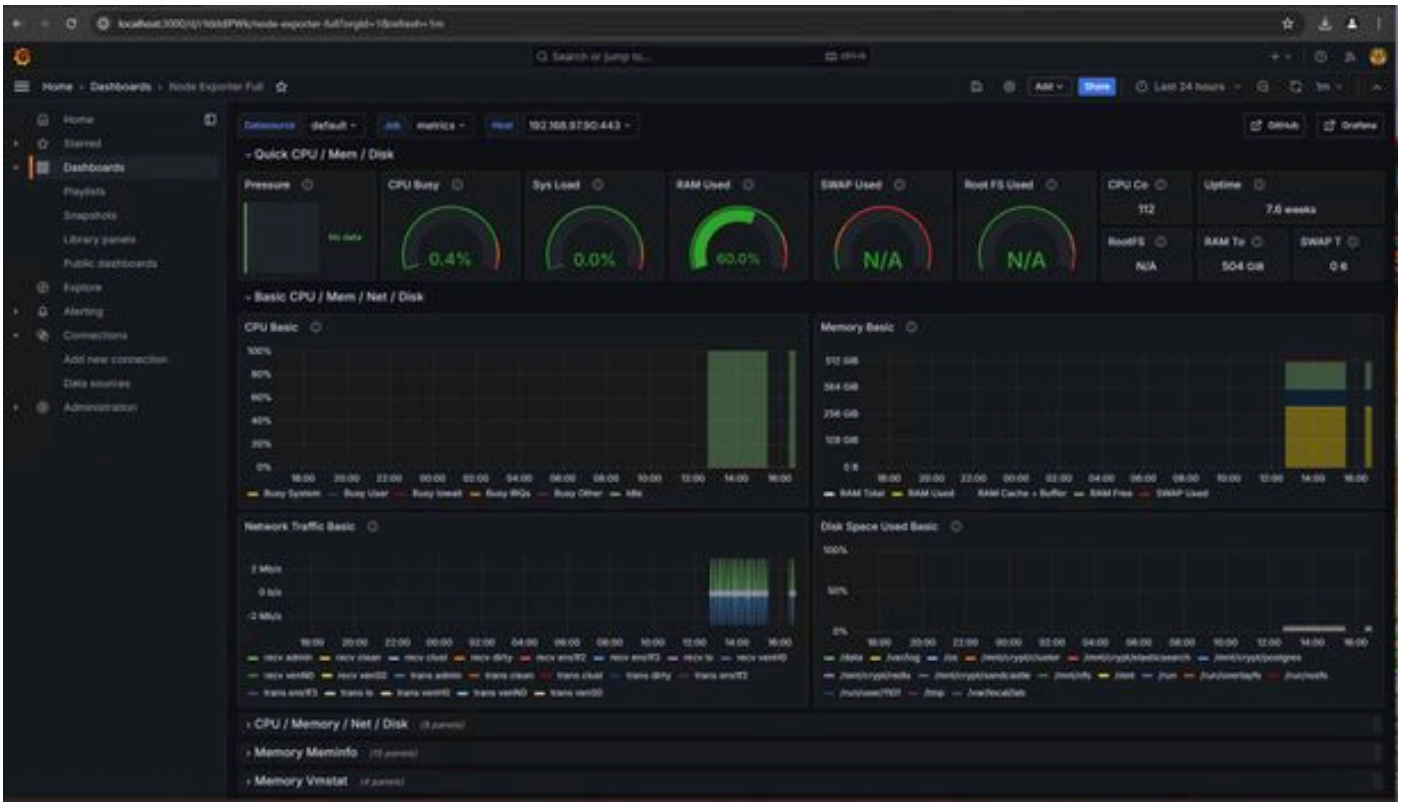


2. Upload het JSON-bestand en selecteer de Prometheusgegevensbron





3. Dit maakt een dashboard met veel hardwaregegevens (niet alle paneelgegevens zijn beschikbaar)-



Problemen oplossen

Als de Prometheus er niet in is geslaagd verbinding te maken en metriek te trekken vanaf het SMA-apparaat, ziet u de fout in `Status` >

`Targets` - http://localhost:9090/targets?search=

Als er `eenError` is, die moet worden opgelost voordat het de gegevens kan trekken. Algemeen probleem is SSL-certificaat van het SMA-apparaat Opadmin wordt niet vertrouwd door de lokale machine. Zorg ervoor dat u een SMA Admin-certificaat maakt met IP en DNS SAN, en voeg de Signing Root CA toe aan de vertrouwenswinkel van de lokale machine.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.