Come configurare Prometheus e Grafana remoti per monitorare l'appliance Secure Malware Analytics (in precedenza Threat Grid)

Sommario

Introduzione

Nell'appliance Secure Malware Analytics (SMA), non è disponibile il protocollo SNMP per monitorare l'utilizzo delle risorse dell'appliance, bensì Prometheus.

Questo documento spiega come configurare un'istanza Prometheus remota e usare Grafanato per visualizzare i dati estratti dall'accessorio.

Prerequisiti

Scaricare e installare i seguenti strumenti sul computer/server locale:

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

Requisiti

- Software Appliance Secure Malware Analytics (SMA) versione 2.18 e successive
- Computer Windows
- Accesso amministrativo alla console di amministrazione dell'accessorio (Opadmin)
- Appliance SMA (Secure Malware Analytics) - Certificato SSL Opadmin considerato attendibile dal computer locale

Componenti usati

- Appliance Secure Malware Analytics (SMA)
- Computer Windows 11 Pro
- Prometeo

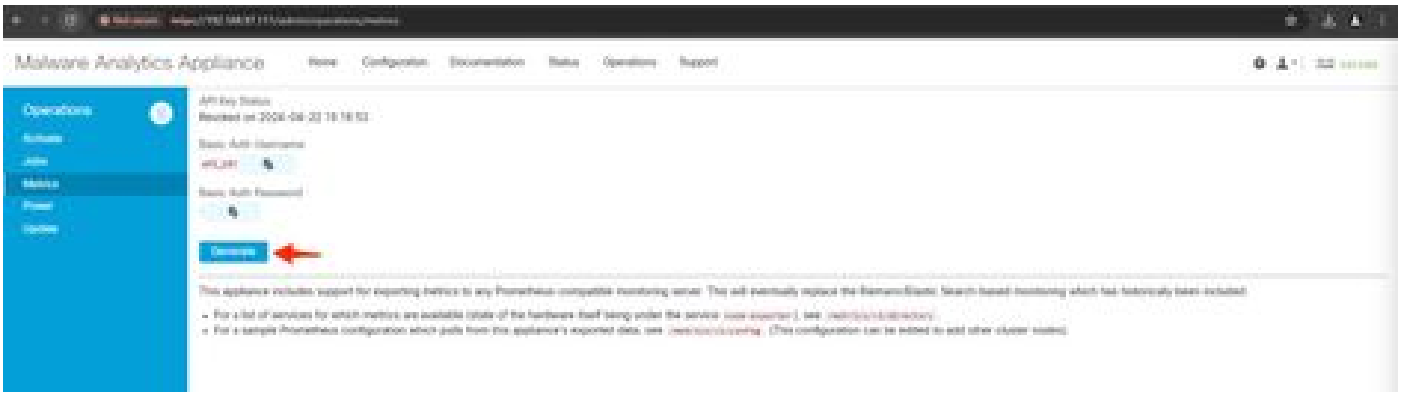
- Grafana

Configurazione

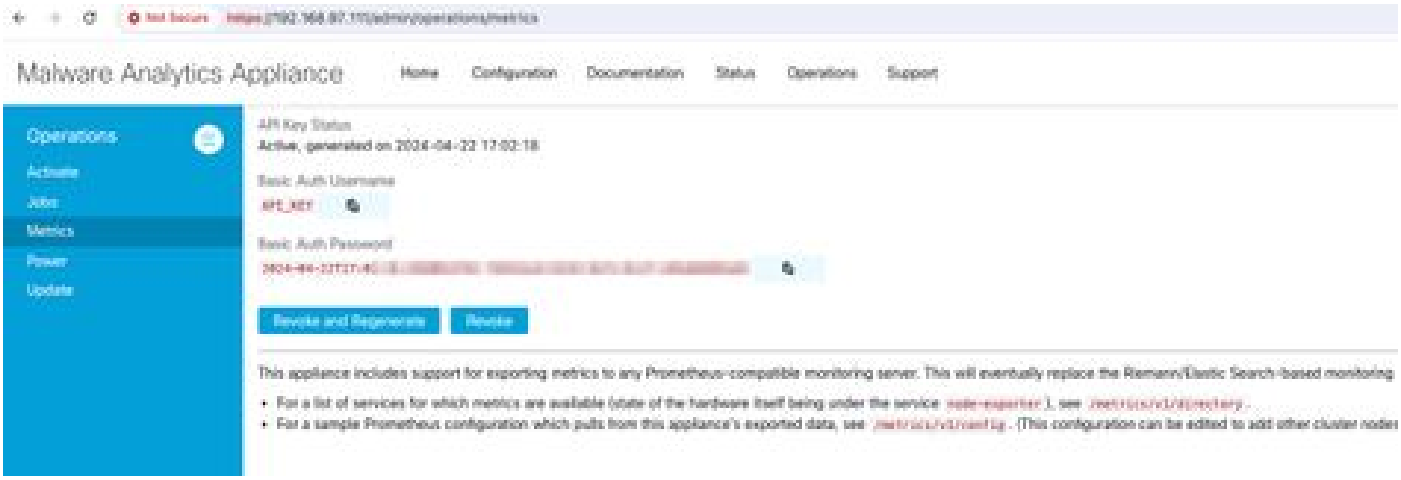
Per questo documento, abbiamo utilizzato un Windows 11 Pro come host remoto in cui abbiamo installato Prometheus e Grafana. Questi strumenti sono disponibili anche per Linux o MacOS.

1. Generare la chiave API nell'appliance SMA (Secure Malware Analytics) per accedere alle metriche

Accedere a SMA Appliance Opadmin. Genera chiave API per le metriche da Opadmin > Operazione > Metriche



2. Verranno generati un nome utente e una password di autenticazione di base da utilizzare nella configurazione di Remote Prometheus.



3. Installare e configurare Prometeo

Seguire le istruzioni fornite dalle guide utente di Prometheus per installare l'istanza se si utilizza Linux o MacOS. Per questo documento, abbiamo installato Prometheus su un computer con Windows 11, e per il processo di installazione, abbiamo seguito questo video su Youtube.

4. Creare un file di configurazione denominato `prometheus.yml`con il seguente contenuto:

```
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. Nella sezione `basic_auth` utilizzare il nome utente e la password di autenticazione di base generati nel passaggio 1.

6. Effettuare il pull della configurazione dei servizi da cui sarà possibile eseguire il pull delle metriche immettendo quanto segue nell'interfaccia utente dopo aver effettuato l'accesso a Opadmin -

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

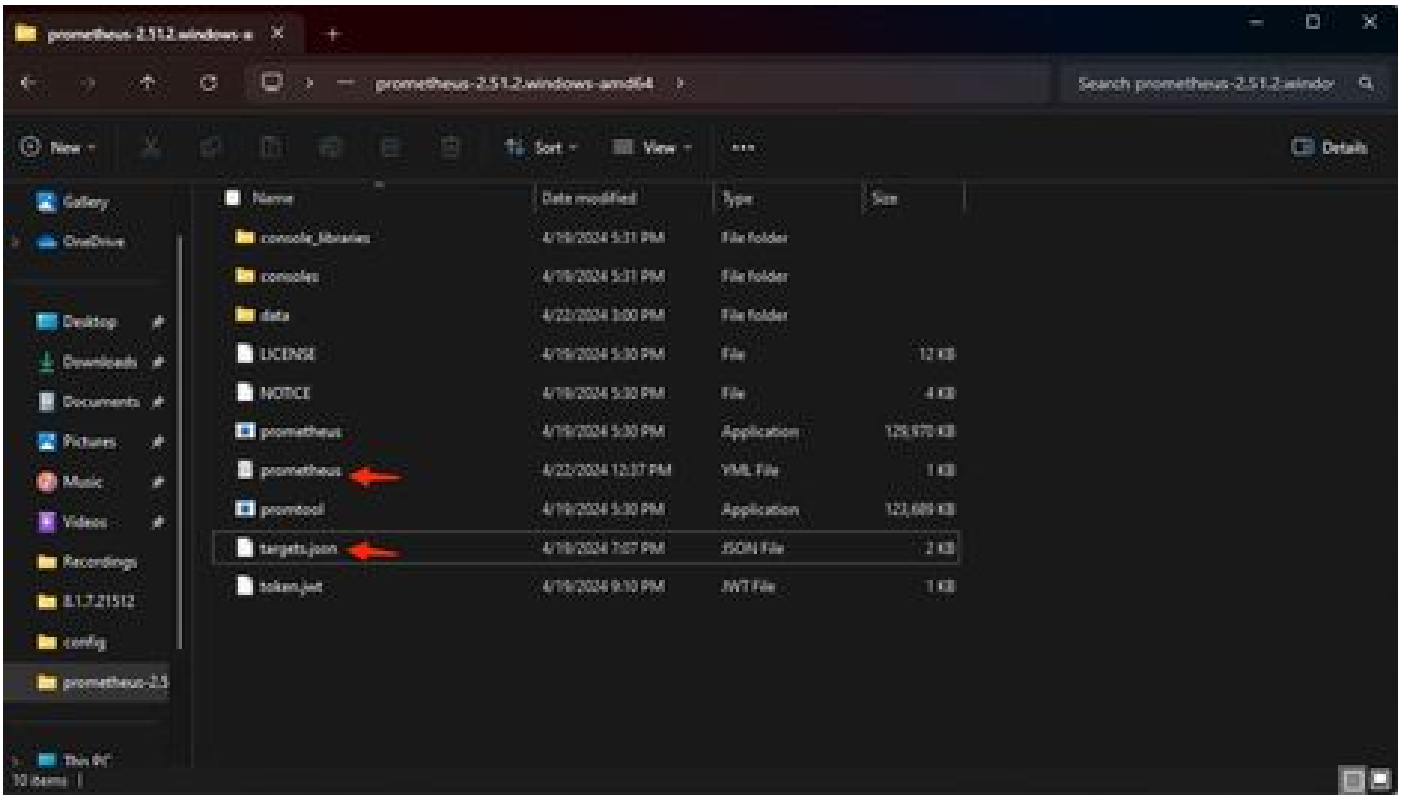
Avrai qualcosa come...

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

La versione `192.168.97.111` è Admin IP per l'appliance SMA.

7. Creare un file con il nome `targets.json` e copiare il contenuto precedente in tale file.

8. Copiare `prometheus.yml` e `target.json` nella directory Prometheus (seguire le guide di installazione), Per Windows, ho creato una cartella nell'unità C:\ e vi ho estratto i file di installazione di Prometheus. Quindi, `prometheus.yml` e `targets.json` sono stati copiati nella stessa cartella.



9. Avviare Prometeo

Avvia Prometeo. Per Windows eseguire `prometheus.exe` dalla riga di comando.

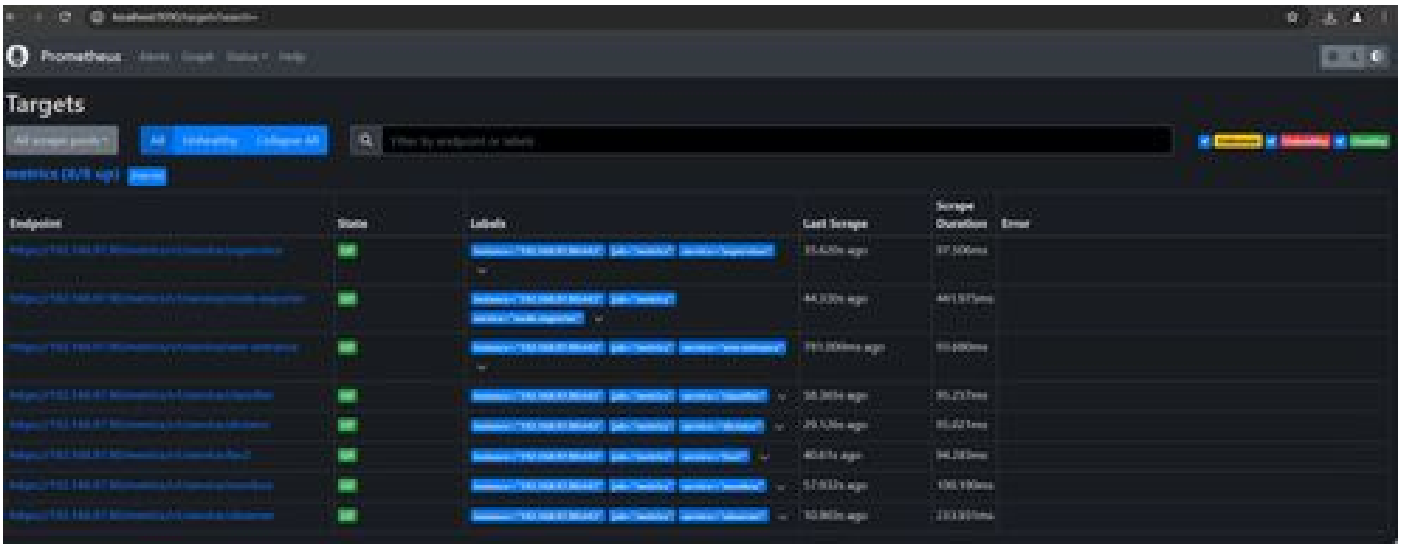
```
C:\Prometheus\prometheus-2.51.2.windows-amd64\prometheus-2.51.2.windows-amd64>prometheus.exe
```

In questo modo viene avviato Prometheus e le metriche vengono estratte dall'appliance SMA. Nota: non chiudere la riga di comando, altrimenti Prometheus verrà chiuso.

10. Per verificare se l'istanza locale di Prometheus è in grado di estrarre la metrica dall'interfaccia utente di Prometheus dell'appliance SMA - `http://localhost:9090/`

11. Vai a `Stato` > `Destinazioni` - http://localhost:9090/targets?search=

Nel giro di pochi minuti si dovrebbero vedere tutte le destinazioni e lo stato UP .



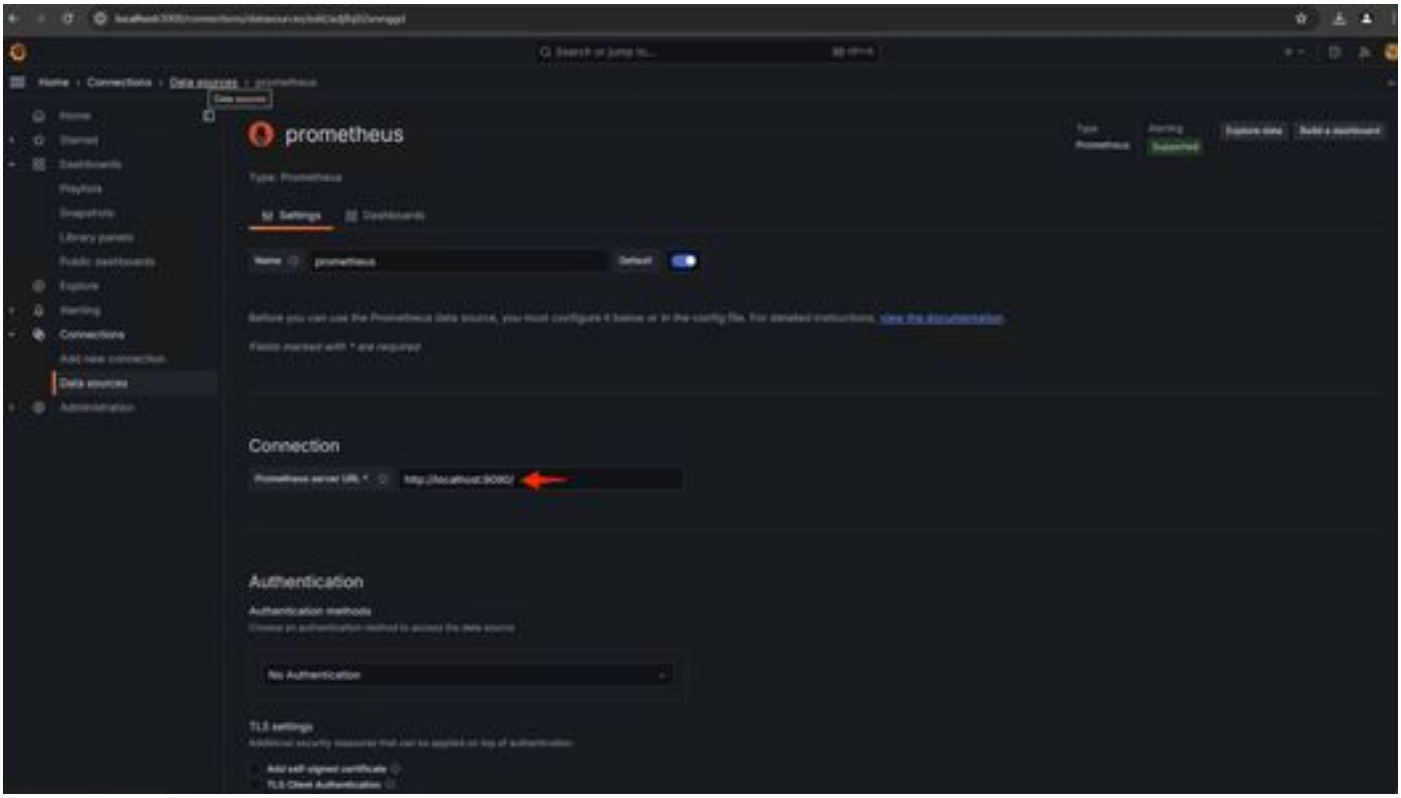
12. Installazione e configurazione di Grafana

Scaricare l'eseguibile Grafana da Grafana Labs. Installare Granafa e seguire le istruzioni fornite dal programma di installazione.

13. Dopo aver installato Grafana access UI nel browser -`http://localhost:3000/`

Selezionare **Home > Connessioni > Origini dati** - `http://localhost:3000/connections/datasources`

`Selezionare Aggiungi nuova origine dati` e `SelezionaPrometeo` dall'elenco. Immettete `http://localhost:9090/` come URL di Prometheus Server



Nella parte inferiore della pagina `selezionare Salva e prova`. Dopo aver superato un test, è possibile creare un dashboard.

14. Crea dashboard Grafana

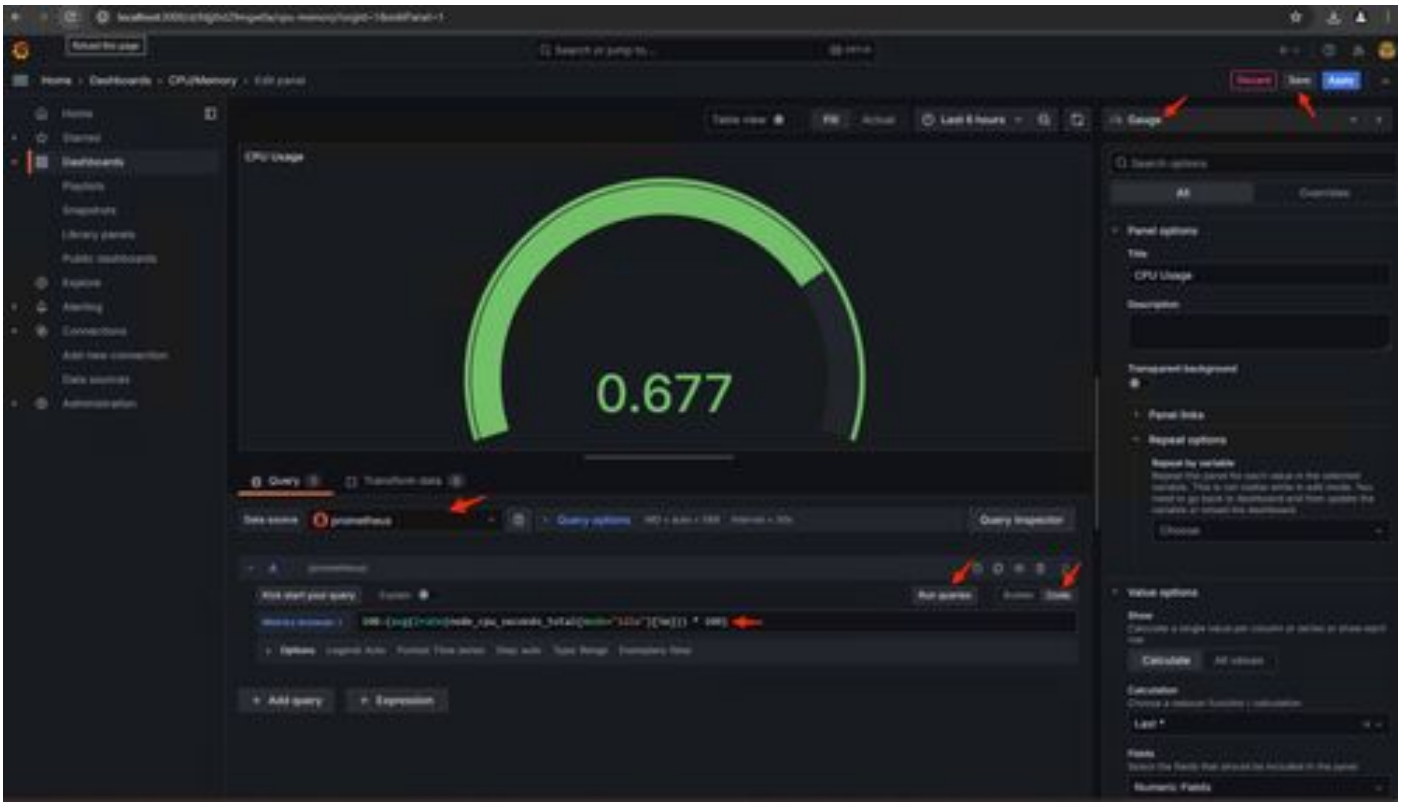
Vai `a Dashboard` in interfaccia utente Grafana, `SelezionaCrea Dashboard`>`Aggiungi visualizzazione`. `Selezionare` Origine dati `Prometheus`.

In Generatore query selectCodeinput, Seleziona tipo di visualizzazione (I selected Gage)

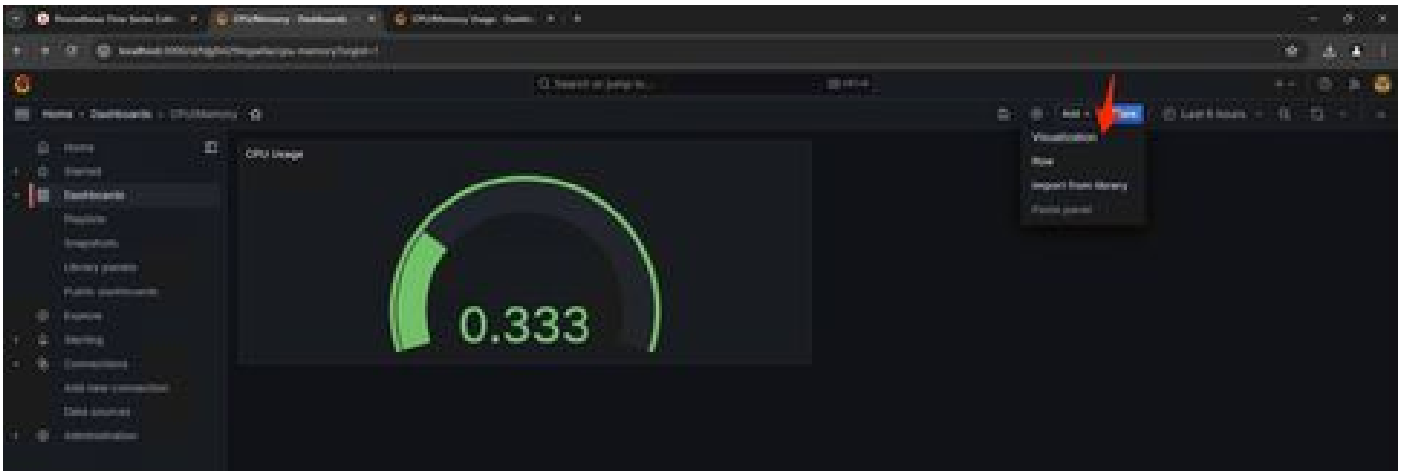
Immettere la seguente query **per Utilizzo CPU**-

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

15. Fare clic su `Esegui` query per visualizzare l'utilizzo della CPU nel modo seguente:

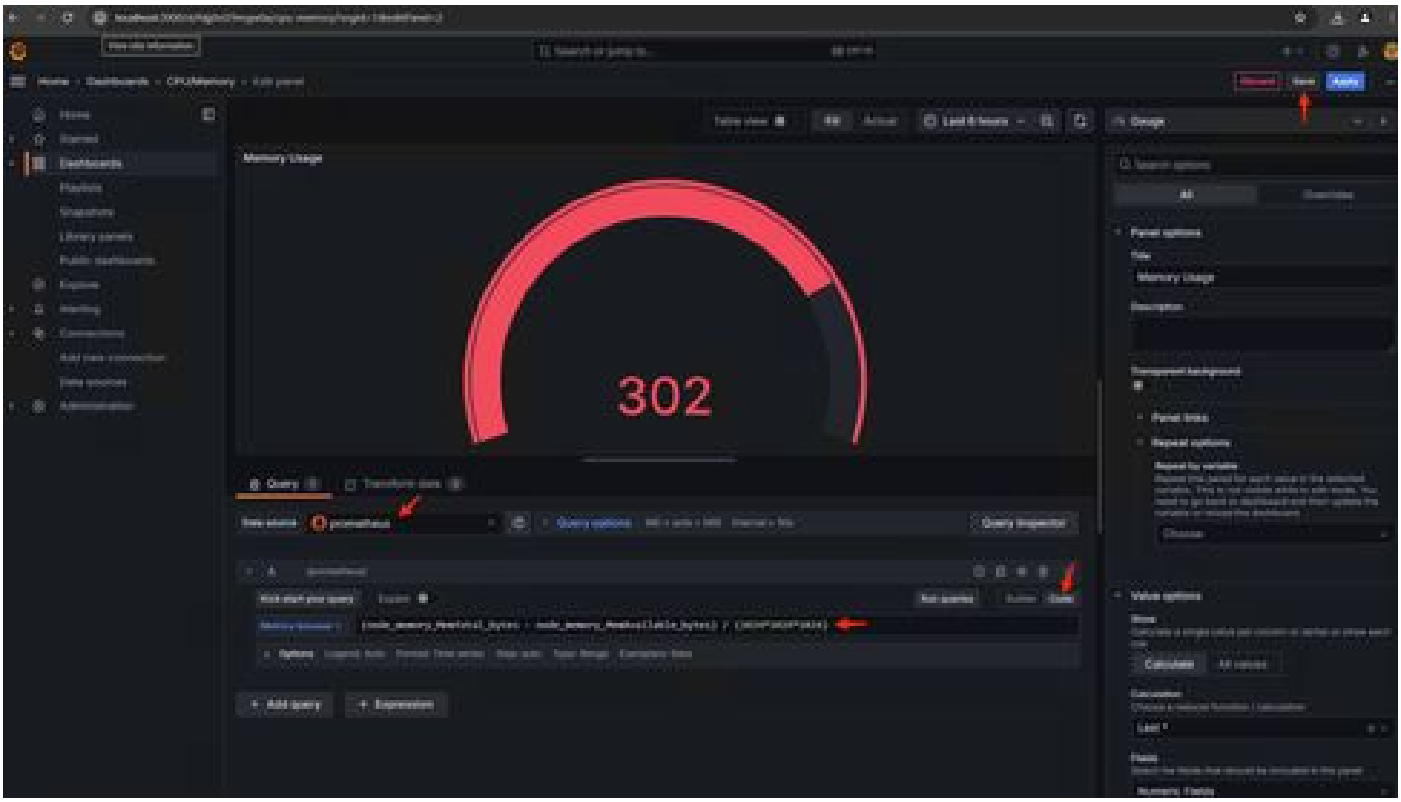


16. Salvare il pannello, assegnare un nome al quadro comandi e salvare. Aggiungi un altro `oggetto Visualization` per l'utilizzo della memoria -



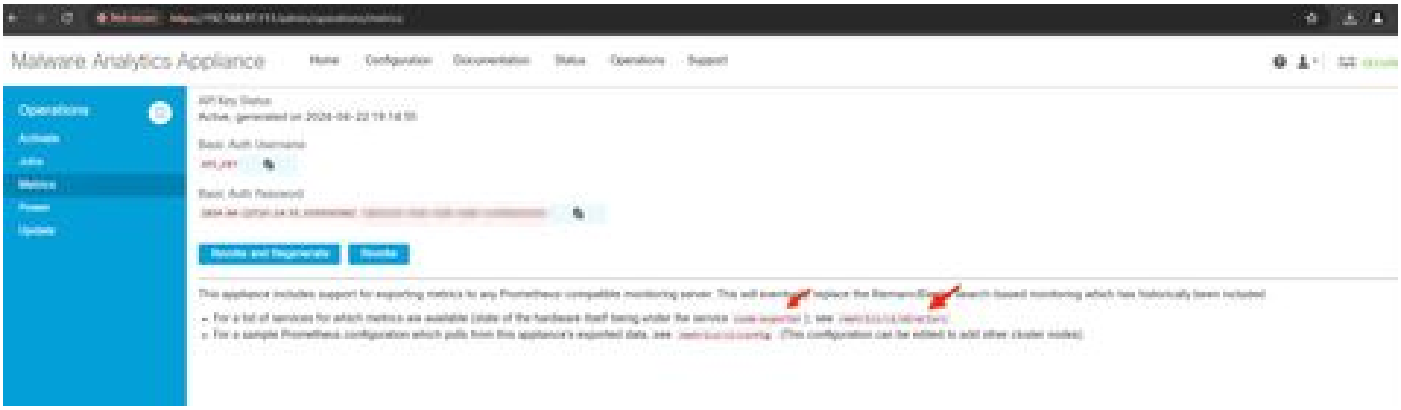
17. Per l'utilizzo della memoria utilizzare la seguente query

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



18. Salvare le modifiche ed è necessario disporre di un dashboard simile al seguente:

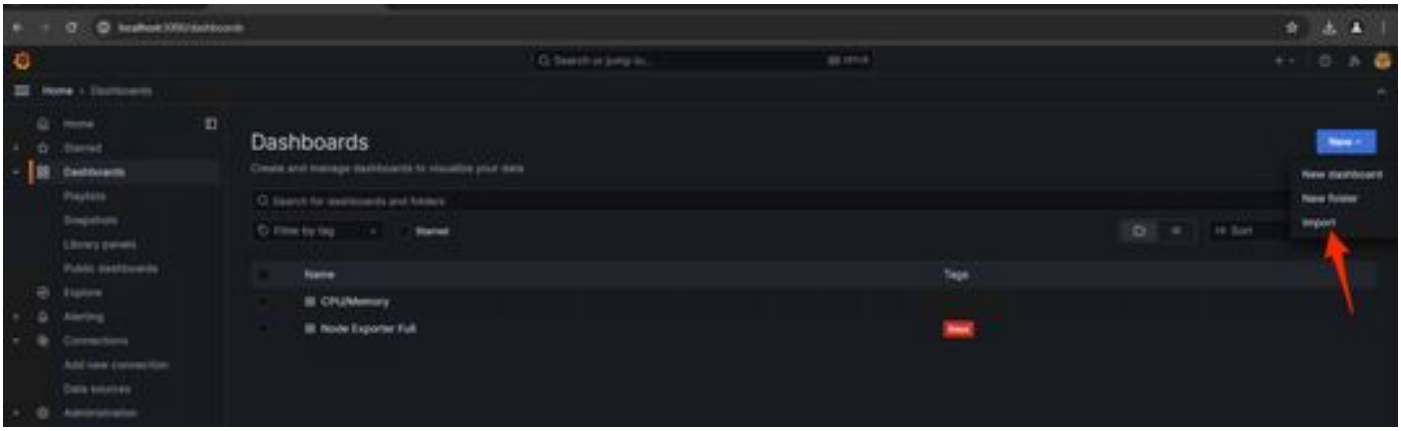
19. Sono disponibili altre metriche hardware e software. Per i dettagli, fare clic sui collegamenti disponibili nella pagina Opadmin> Metriche.



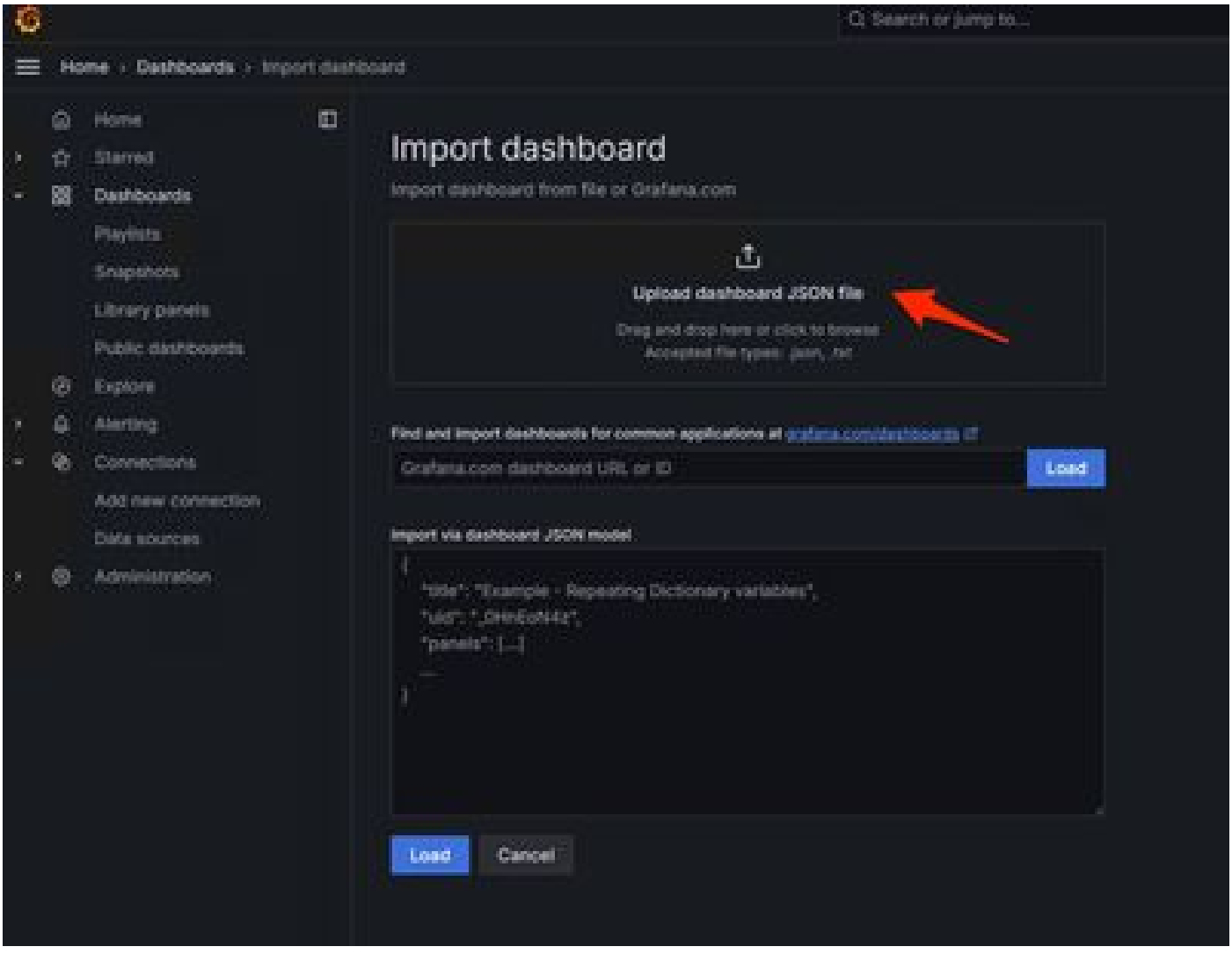
Modello dashboard Grafana

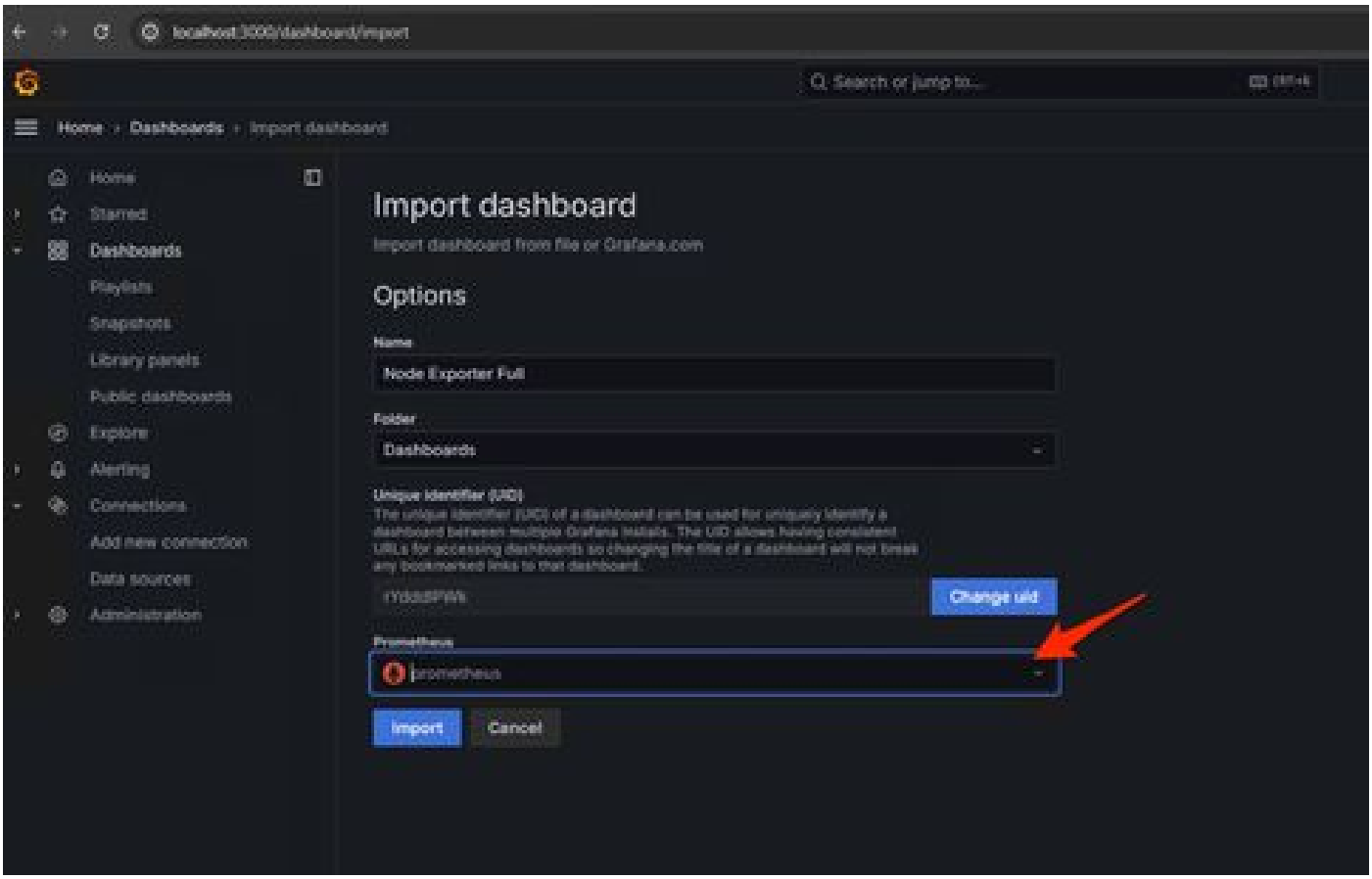
Sul sito Web Grafana sono disponibili molti modelli di dashboard Grafana per Node Exporter. Uno di questi è - Node Exporter Full

1. Per importare questo dashboard nell'istanza di Grafana Scaricare il file JSON, importare il file JSON in Grafana

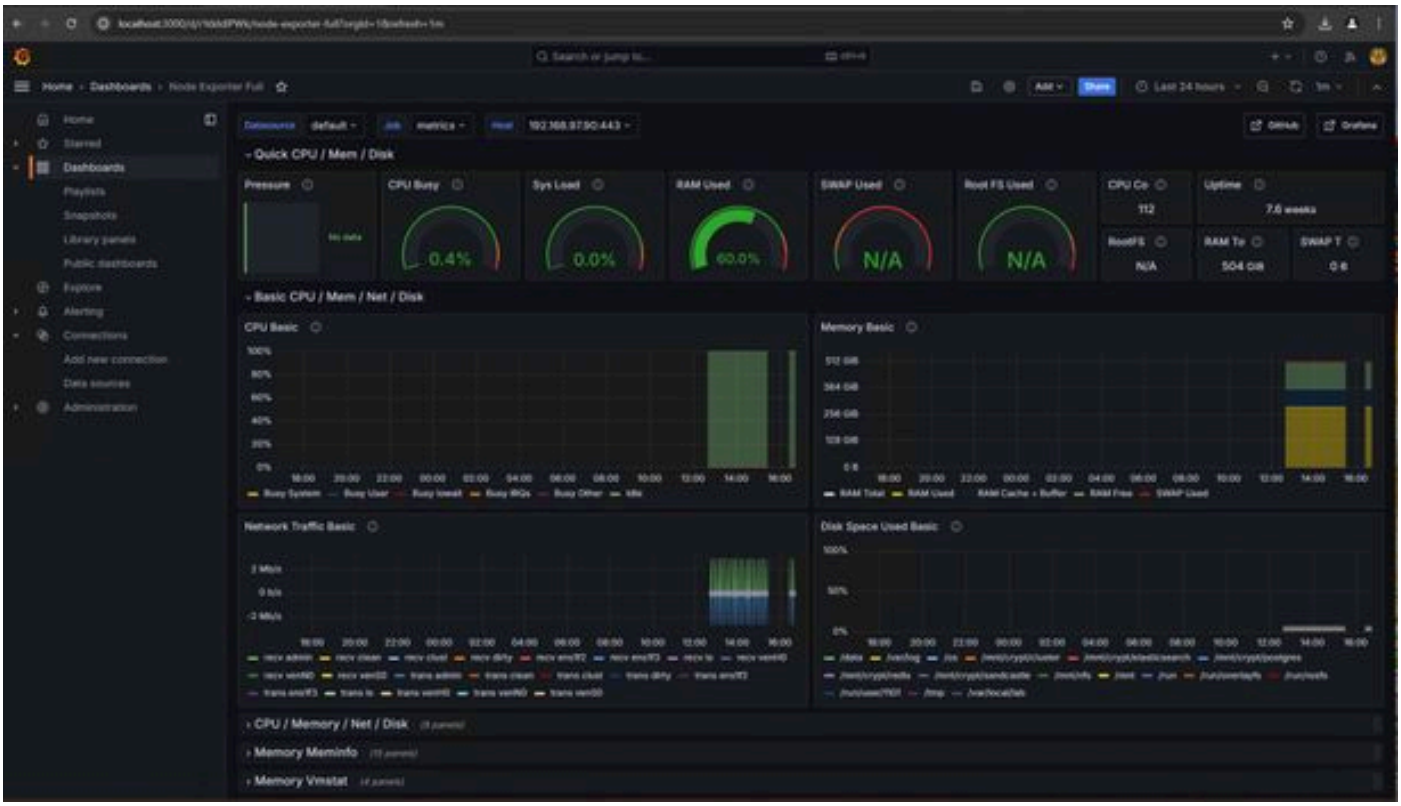


2. Caricare il file JSON e selezionare l'origine dati Prometheus





3. In questo modo verrà creato un dashboard con molte informazioni sull'hardware (non tutte le metriche del pannello sono disponibili)-



Risoluzione dei problemi

Se Prometheus non è riuscito a collegarsi e a prelevare la metrica dall'accessorio SMA, l'errore sarà visualizzato in `Stato` > `Destinazioni` -

http://localhost:9090/targets?search=

Se è presente `anyError`, è necessario correggerlo prima di poter estrarre i dati. Il problema più comune è che il certificato SSL dell'accessorio SMA Opadmin non è considerato attendibile dal computer locale. Assicurarsi di creare un certificato di amministrazione SMA con IP e SAN DNS e aggiungere la CA radice di firma all'archivio di attendibilità del computer locale.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).