Como configurar Prometheus e Grafana remotos para monitorar o dispositivo Secure Malware Analytics (anteriormente Threat Grid)

Contents

Introdução

No dispositivo Secure Malware Analytics (SMA), não oferecemos o protocolo SNMP para monitorar o uso de recursos do dispositivo. Em vez disso, o dispositivo [ofereceePrometheus](#).

Este documento descreve como configurar uma instância remota do Prometheus e usar o Grafanato para visualizar os dados extraídos do dispositivo.

Pré-requisitos

Baixe e instale as seguintes ferramentas em sua máquina/servidor local:

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

Requisitos

- Software do dispositivo Secure Malware Analytics (SMA) versão 2.18 e posterior
- Máquina Windows
- Acesso de administrador ao console de administração do equipamento (Opadmin)
- Secure Malware Analytics (SMA) Appliance Opadmin SSL Certificado Confiável pela máquina local

Componentes Utilizados

- Dispositivo Secure Malware Analytics (SMA)
- Máquina Windows 11 Pro
- Prometeu

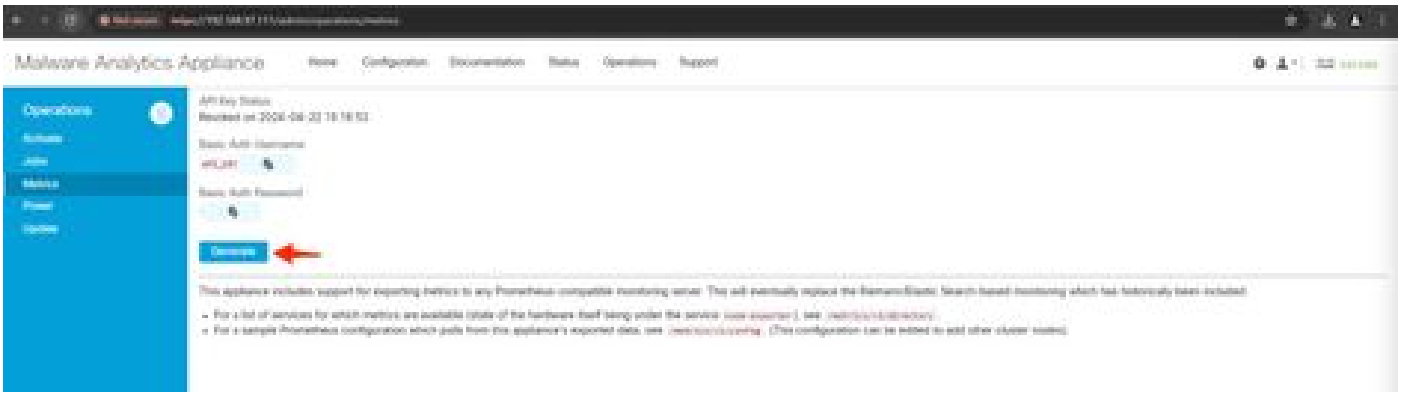
- Grafana

Configurar

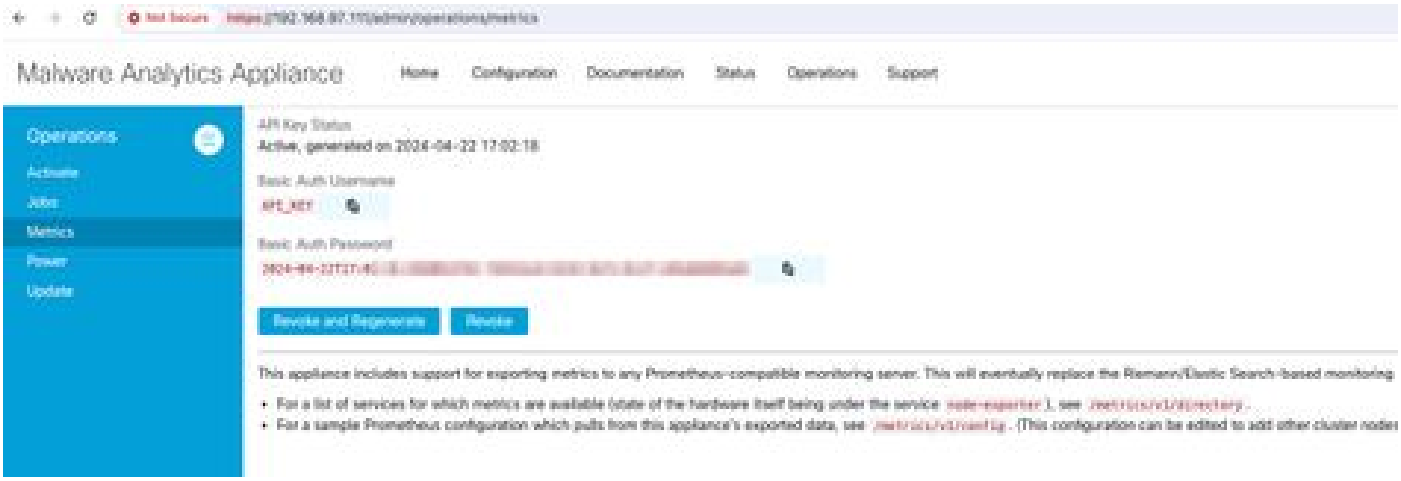
Para este documento, usamos um Windows 11 Pro como um host remoto onde instalamos o Prometheus e o Grafana. Essas ferramentas também estão disponíveis para Linux ou MacOS.

1. Gerar chave de API no dispositivo Secure Malware Analytics (SMA) para acessar métricas

Faça login no SMA Appliance Opadmin. Gerar Chave de API para Métricas de Opadmin > Operação > Métricas



2. Um nome de usuário e uma senha de autenticação básica serão gerados e precisaremos usá-los na configuração Prometheus remota.



3. Instalar e Configurar o Prometheus

Siga as instruções fornecidas pelos guias do usuário do Prometheus para instalar sua instância se estiver usando Linux ou MacOS. Para este documento, instalamos o Prometheus em uma máquina com Windows 11 e, para o processo de instalação, seguimos este vídeo do Youtube.

4. Crie um arquivo de configuração com o nome `prometheus.yml`com o seguinte conteúdo -

```
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. na seção `basic_auth`, use o Nome de Usuário e a Senha de Autenticação Básicos gerados na Etapa 1.

6. Receba a configuração dos serviços dos quais você poderá receber métricas inserindo o seguinte na interface do usuário depois de fazer login no Opadmin -

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

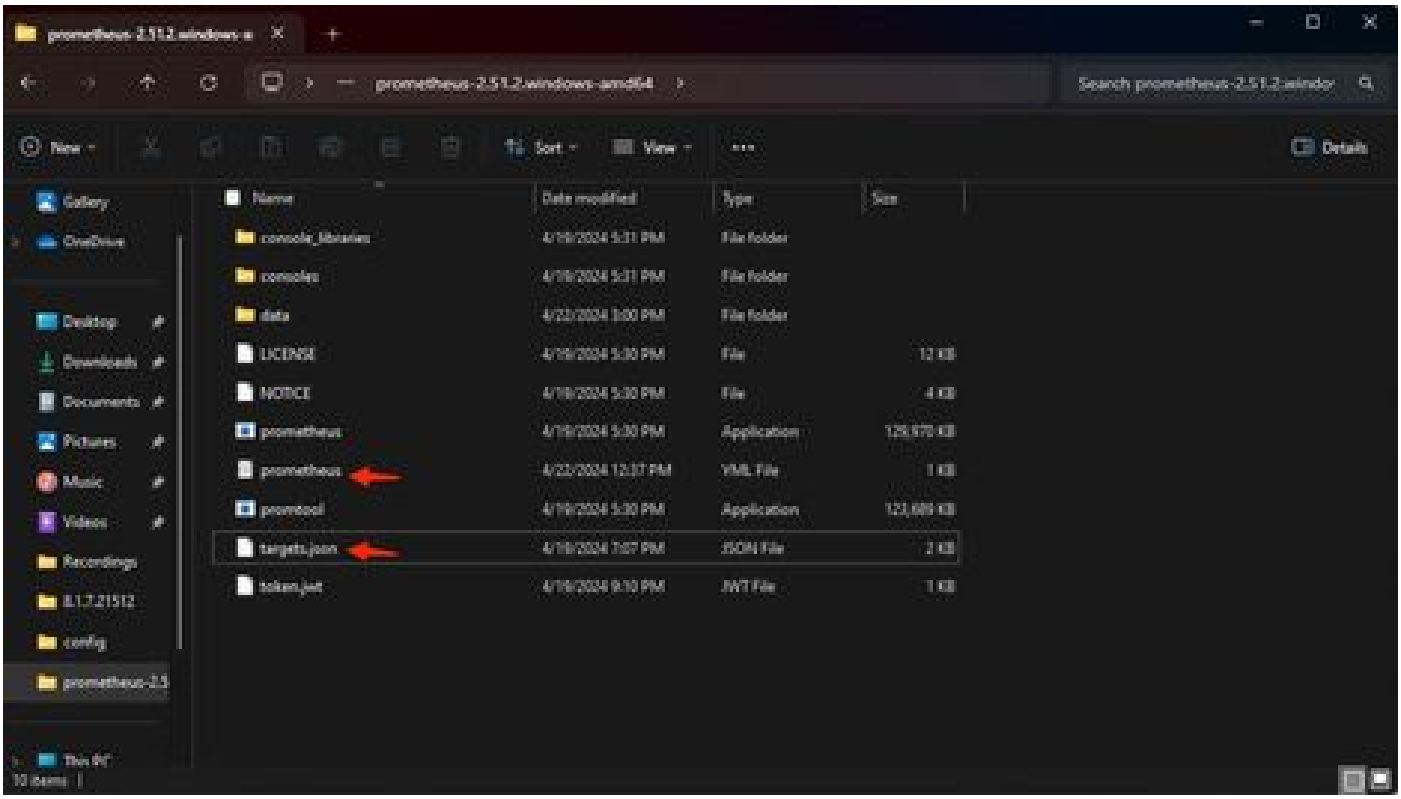
Você receberá algo como -

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

Aqui `192.168.97.111` é o IP do administrador para meu dispositivo SMA.

7. Crie um arquivo com o nome `targets.json` e copie o conteúdo acima para esse arquivo.

8. Copie `prometheus.yml` e `targets.json` para o diretório Prometheus (siga os guias de instalação), Para Windows, eu criei uma pasta na unidade C:\ e extraí os arquivos de instalação do Prometheus lá. Em seguida, copiou `prometheus.yml` e `targets.json` para essa mesma pasta.



9. Inicie Prometheus

Inicie Prometheus. No Windows, execute `prometheus.exe` a partir da linha de comando.

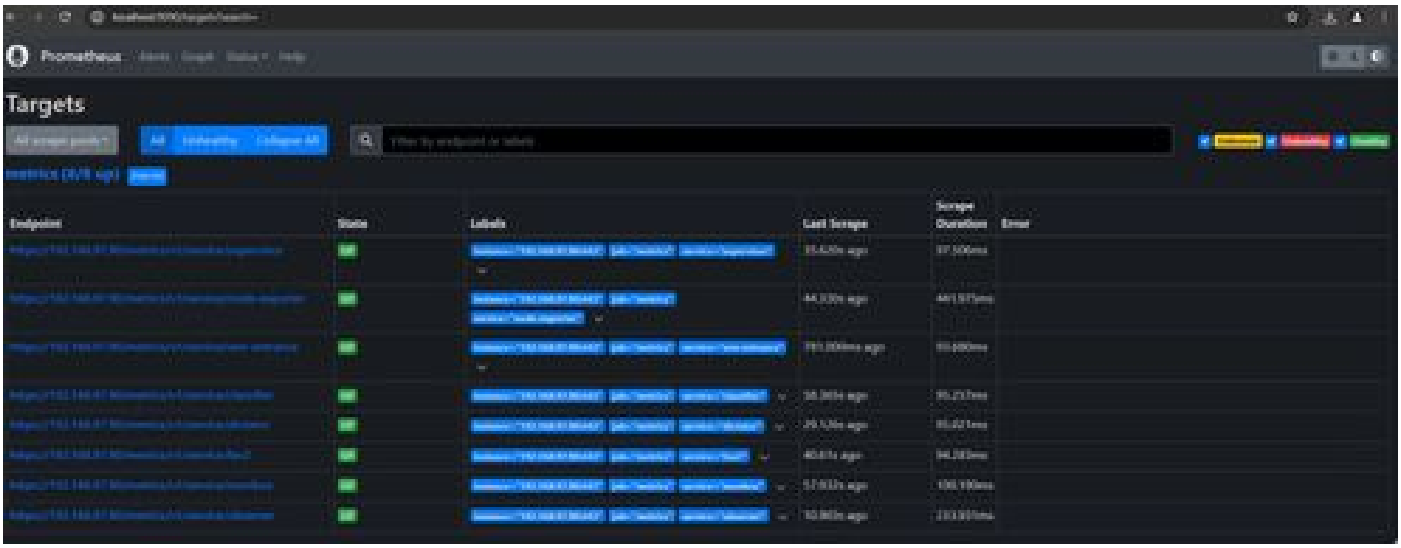
```
C:\Prometheus\prometheus-2.51.2.windows-amd64\prometheus-2.51.2.windows-amd64>prometheus.exe
```

Isso iniciará o Prometheus e começará a extrair as métricas do dispositivo SMA. Observação: não feche a linha de comando ou o Prometheus será desligado.

10. Para verificar se a instância local do Prometheus é capaz de extrair a métrica da interface do usuário do Prometheus da carga do dispositivo SMA - `http://localhost:9090/`

11. Vá para `Status` > `Alvos` - http://localhost:9090/targets?search=

Dentro de alguns minutos você deverá ver todos os destinos e o status `UP` .



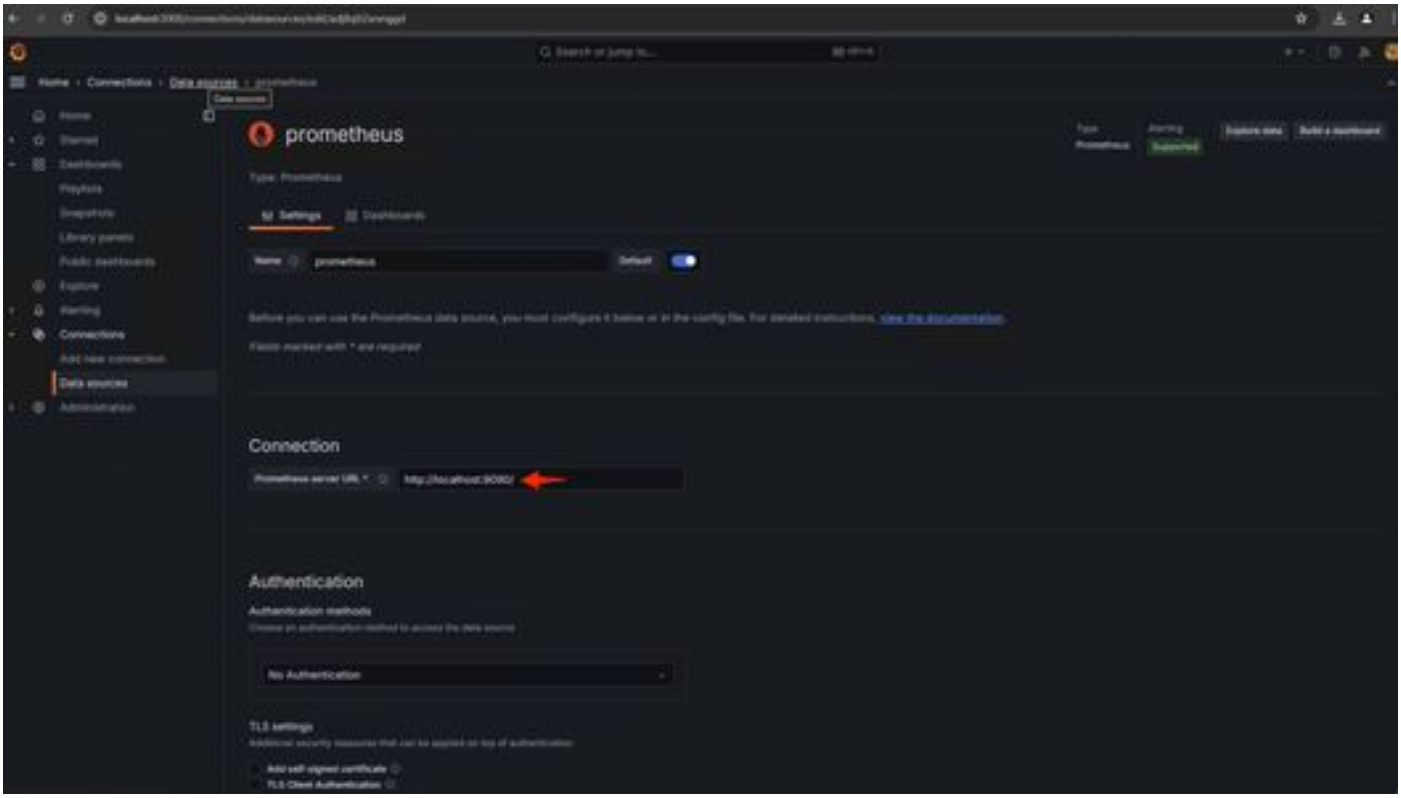
12. Instalar e Configurar o Grafana

Faça o download do executável do Grafana no Grafana Labs. Instale o Granafa e siga as instruções fornecidas pelo instalador.

13. Após a instalação da IU de acesso do Grafana no navegador -`http://localhost:3000/`

Vá para **Início > Conexões > Fontes de dados** - `http://localhost:3000/connections/datasources`

`Selecione Add New Datasource` e `SelectPrometheus` na lista. Insira o `http://localhost:9090/` como a URL do servidor Prometheus



Na parte inferior dessa página, `selecione Salvar e testar`. Após um teste bem-sucedido, podemos criar um painel.

14. Criar Painel do Grafana

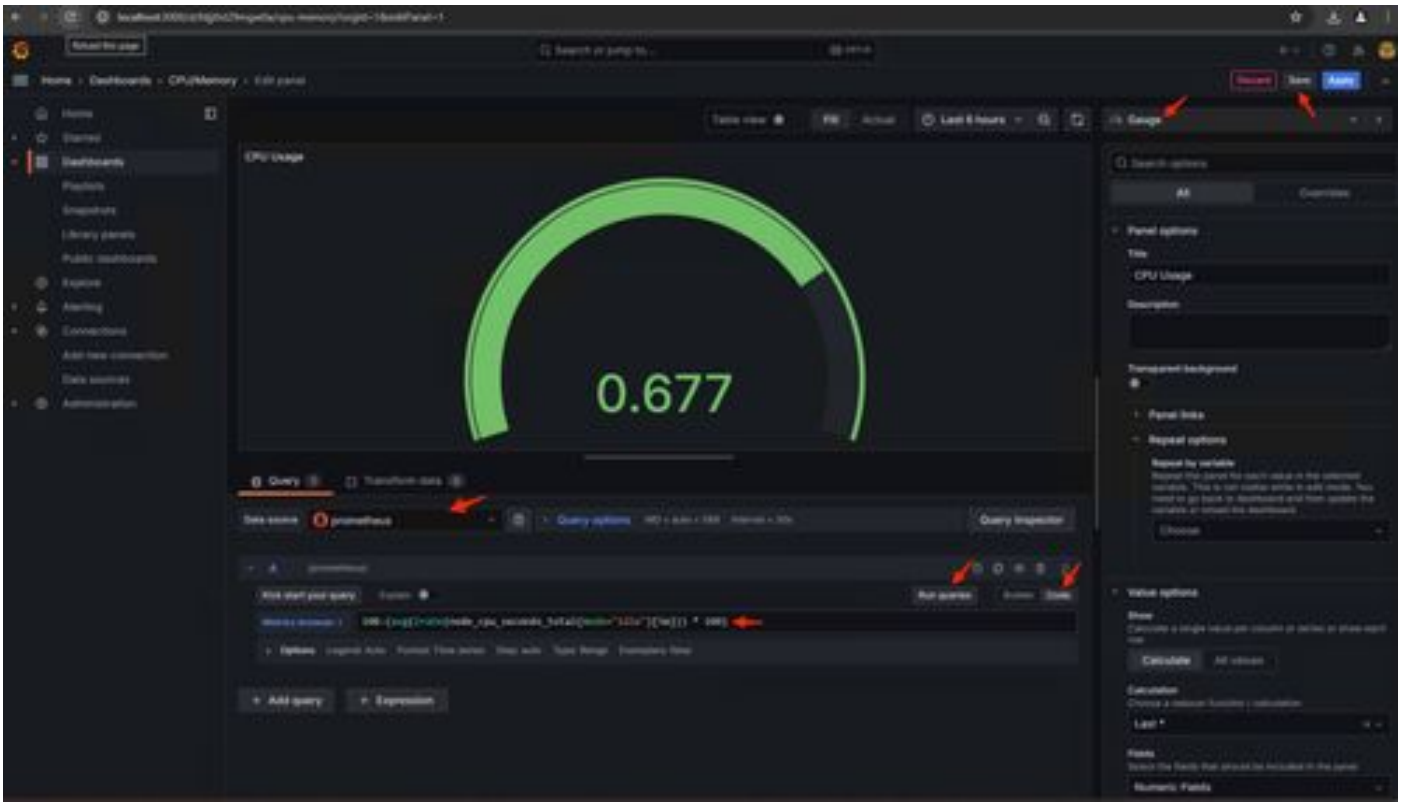
Vá paraPainéis na interface do usuário do Grafana , SelectCreate Dashboard>Add visulization. Selecione Fonte de dados Prometheus.

No construtor de consultas selectCodeinput, selecione Tipo de visualização (I seleted Gauge)

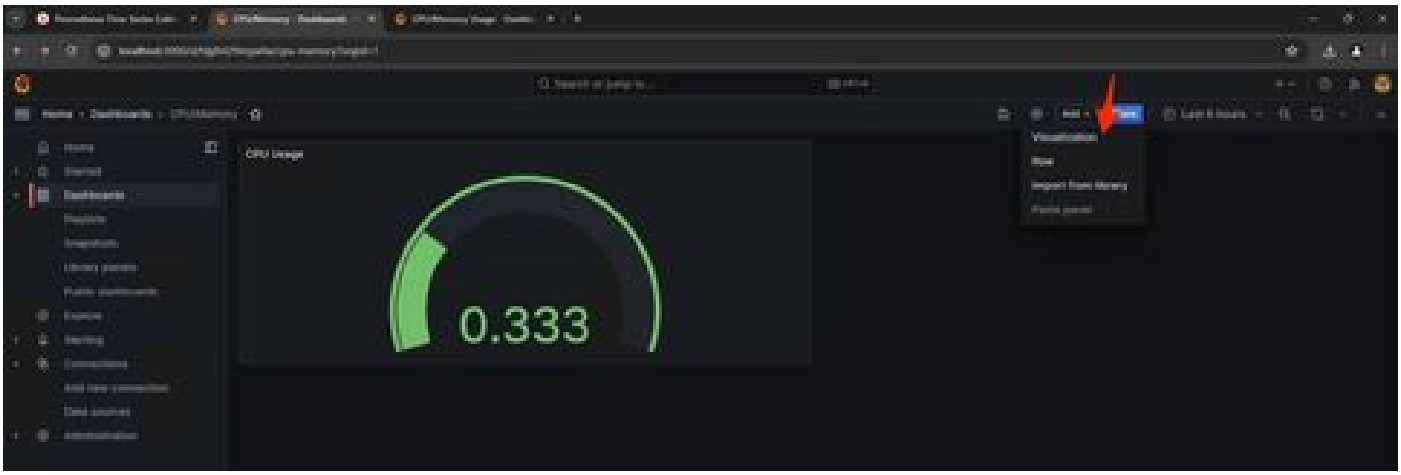
Insira a seguinte consulta **paraUtilização da CPU**-

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

15. Clique em Executar Consultas e você verá uma visualização do Uso da CPU como esta -

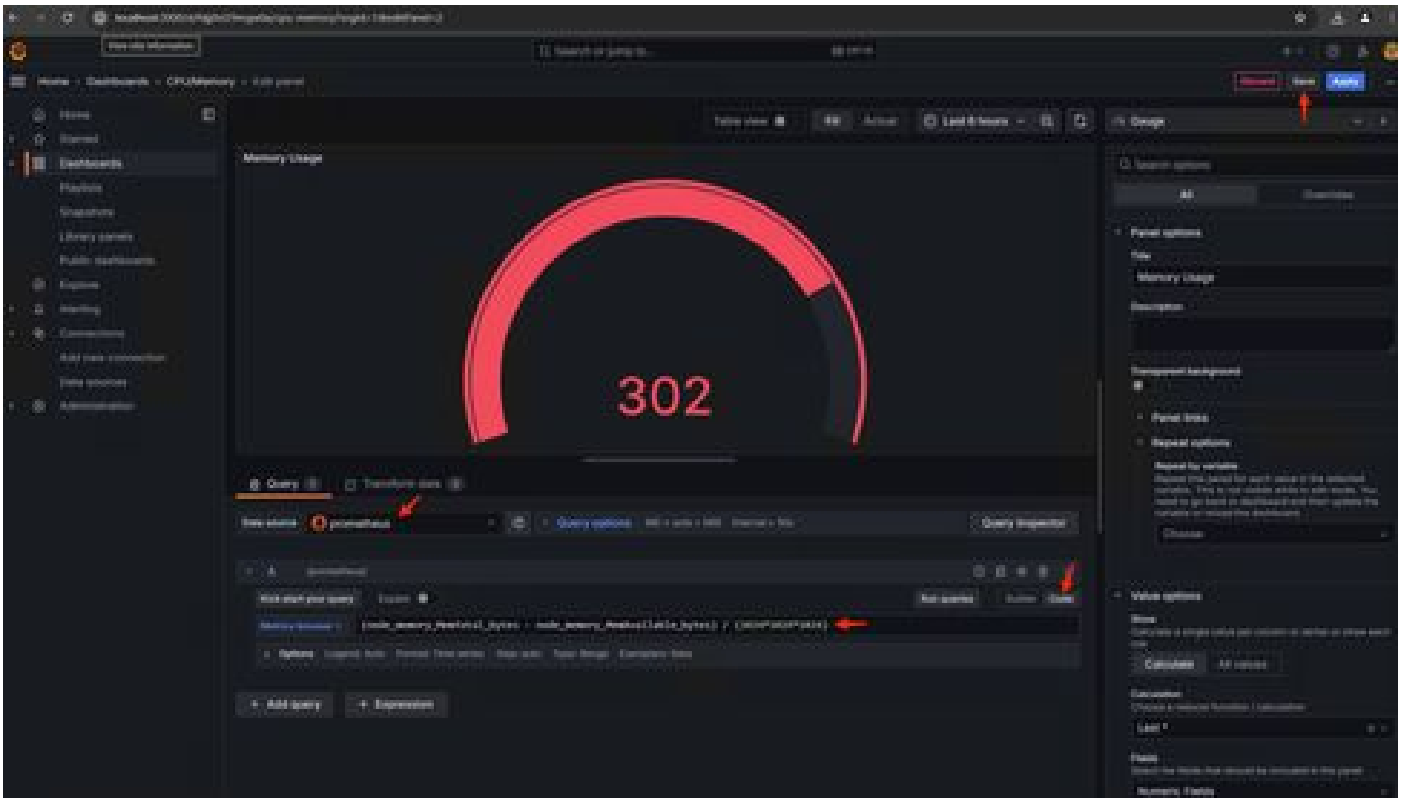


16. Salve o painel, nomeie o Painel e Salve. Adicionar outra Visualização para Uso de Memória -



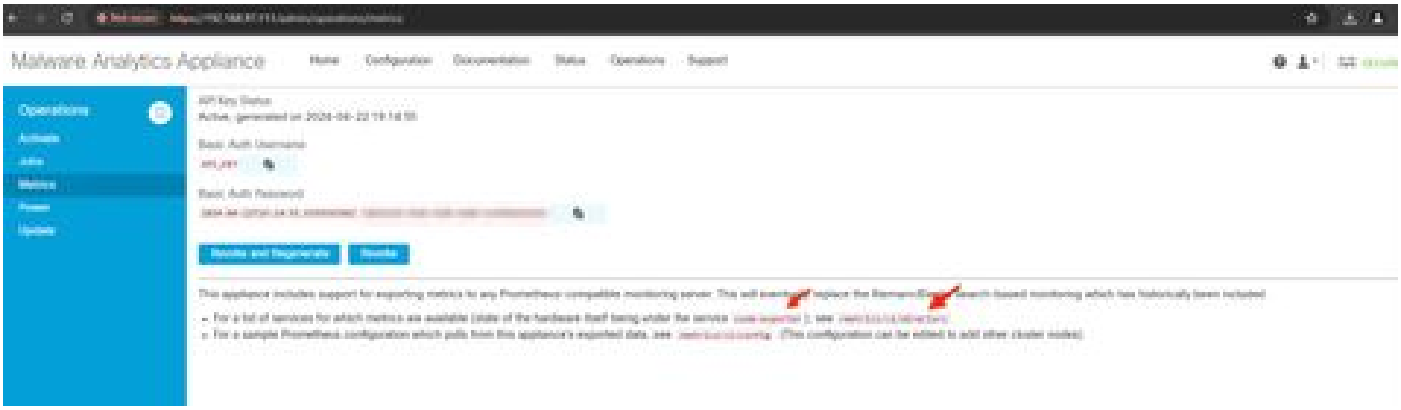
17. Para Utilização de Memória, use a seguinte consulta

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



18. Salve as alterações e você deverá ter um painel como este -

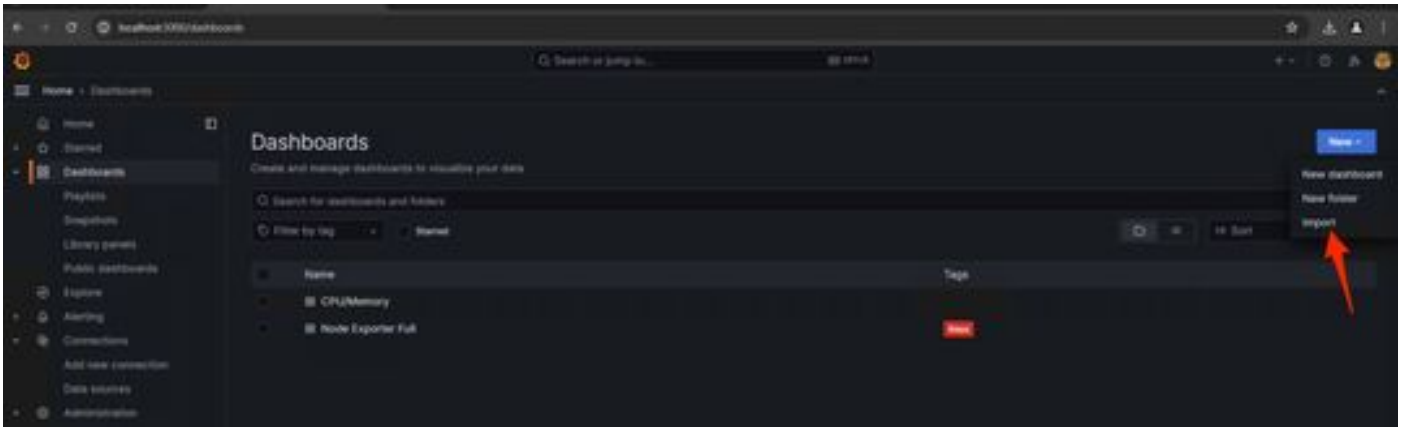
19. Outras métricas de Hardware e Software estão disponíveis. Para obter detalhes, clique nos links fornecidos `na página Opadmin> Métricas`.



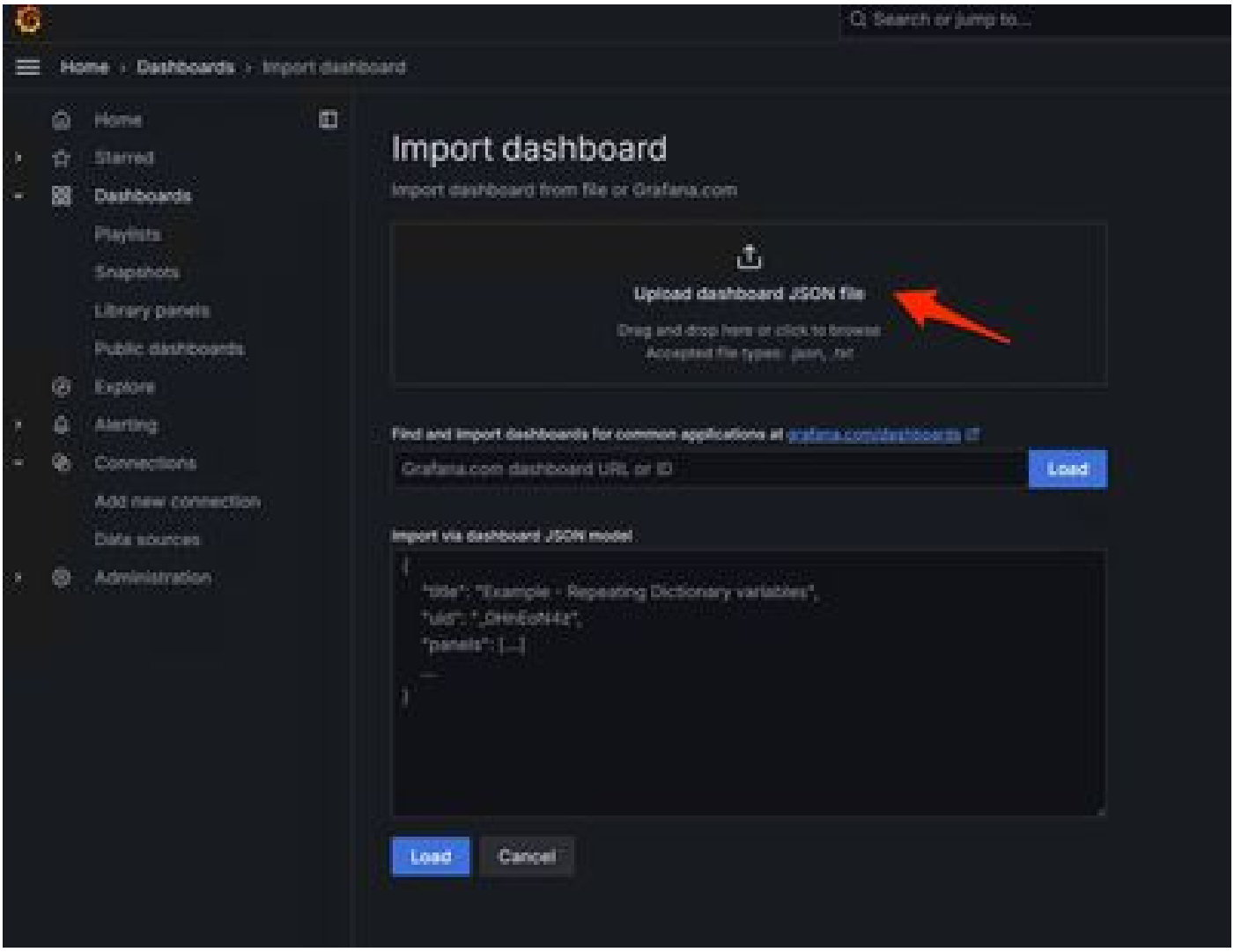
Modelo de painel Grafana

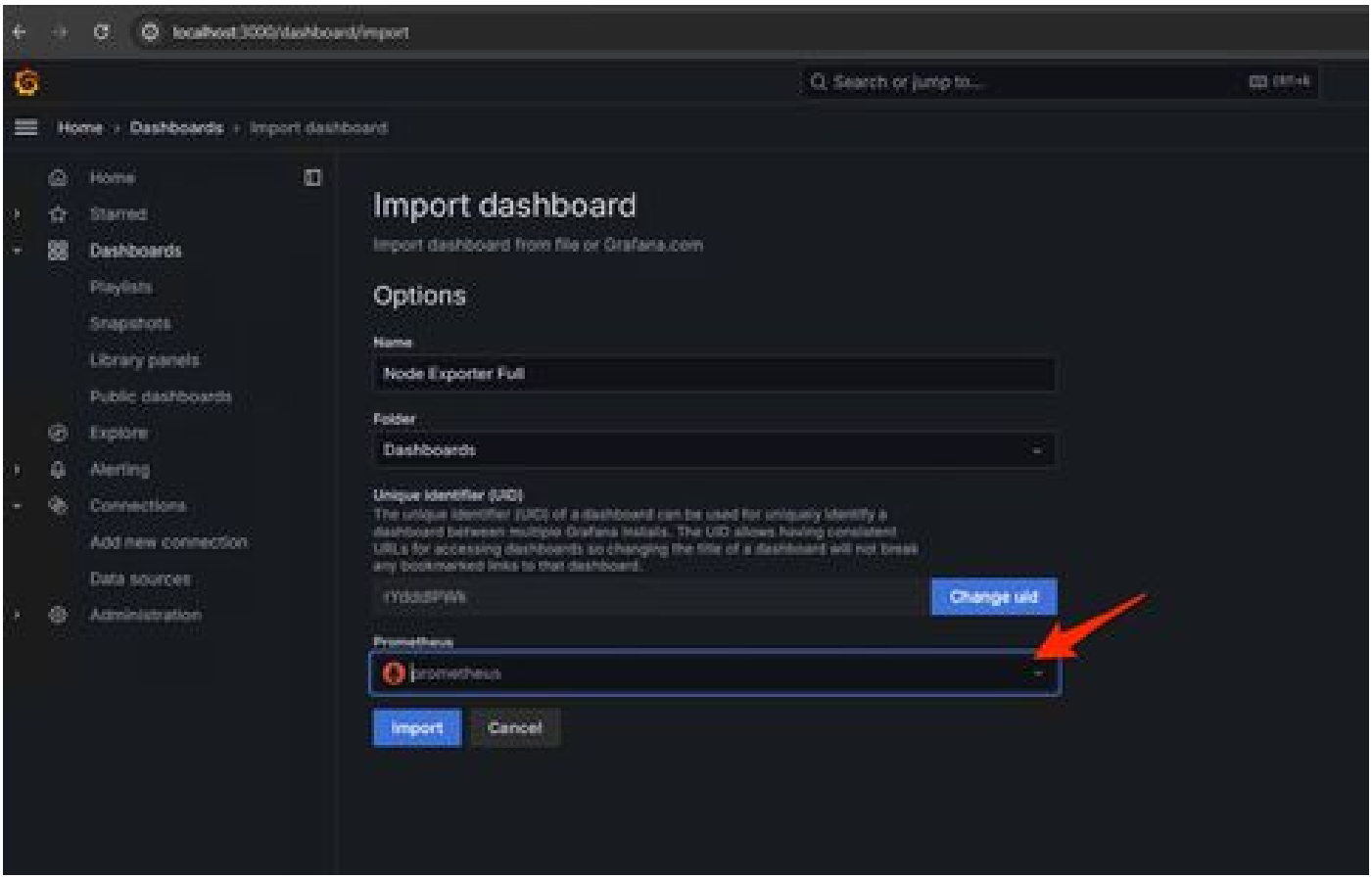
Há muitos modelos de painel do Grafana disponíveis para o Node Exporter no site do Grafana. Um deles é: Exportador de nó cheio

1. Para importar este painel para a sua instância do Grafana Faça download do JSON, importe o arquivo JSON no Grafana

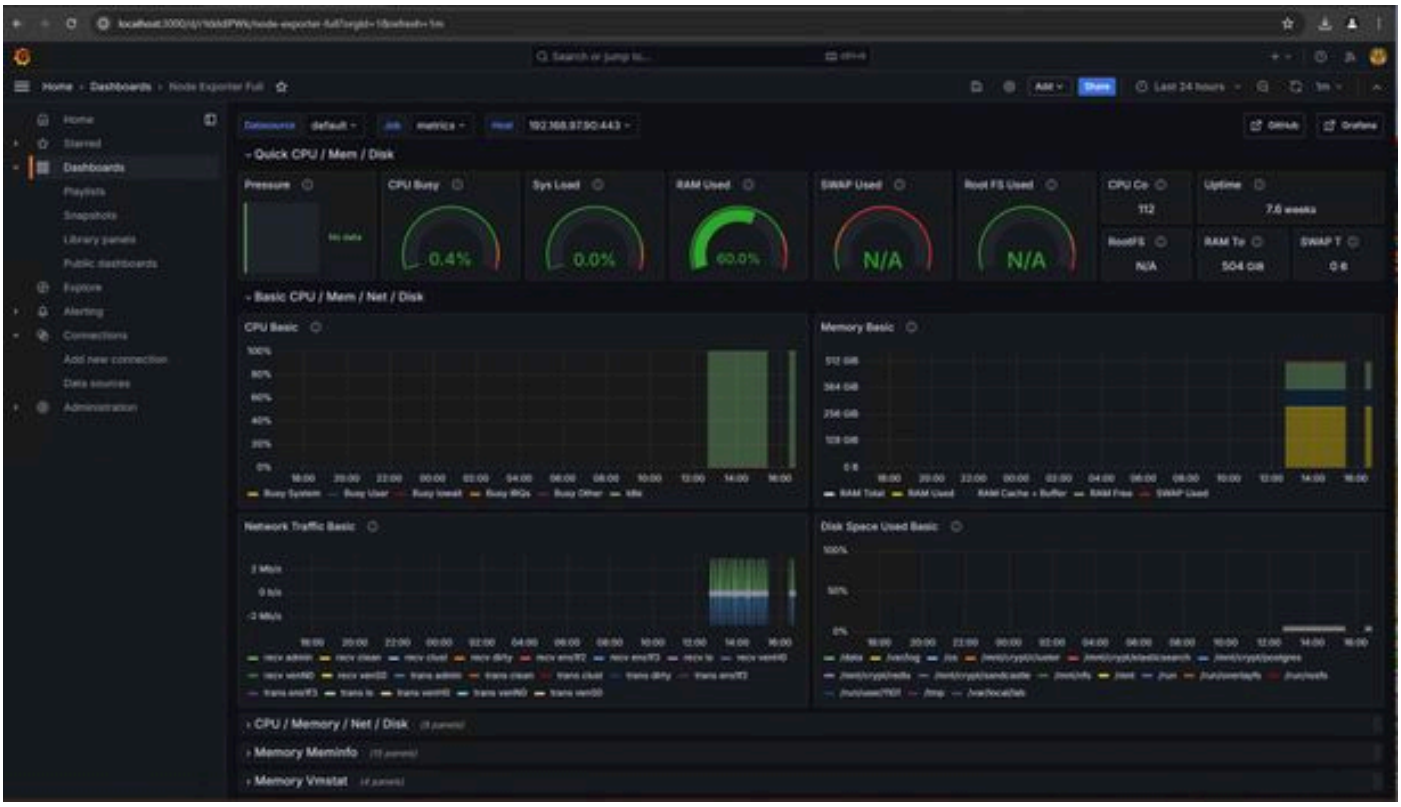


2. Carregue o arquivo JSON e selecione a fonte de dados Prometheus





3. Isso criará um painel com muitas informações de hardware (nem todas as métricas do painel estão disponíveis)-



Troubleshooting

Se o Prometheus falhou ao conectar e extrair a métrica do dispositivo SMA, você verá o erro em `Status` > `Targets` -

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

Se houver `anyError`, será necessário corrigi-lo antes de receber os dados. Um problema comum é o certificado SSL do equipamento SMA no qual o Opadmin não é confiável no computador local. Certifique-se de criar um Certificado de Administrador do SMA com IP e SAN DNS e adicione a CA raiz de assinatura ao repositório de confiança do computador local.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.