Cómo configurar Prometheus y Grafana remotos para supervisar el dispositivo Secure Malware Analytics (antes Threat Grid) Appliance

Contenido

Introducción

En el dispositivo Secure Malware Analytics (SMA), no ofrecemos el protocolo SNMP para supervisar el uso de recursos del dispositivo; en su lugar, el dispositivo ofrece Prometeo.

Este documento describirá cómo configurar una instancia remota de Prometheus y utilizar Grafanato para visualizar los datos extraídos del dispositivo.

Prerequisites

Descargue e instale las siguientes herramientas en su equipo/servidor local:

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

Requirements

- Software Secure Malware Analytics (SMA) Appliance versión 2.18 y posteriores
- Máquina Windows
- Acceso de administrador a la consola de administración de dispositivos (Opadmin)
- Dispositivo de análisis de malware seguro (SMA) Certificado SSL Opadmin de confianza en el equipo local

Componentes Utilizados

- Dispositivo Secure Malware Analytics (SMA)
- Windows 11 Pro máquina
- Prometeo

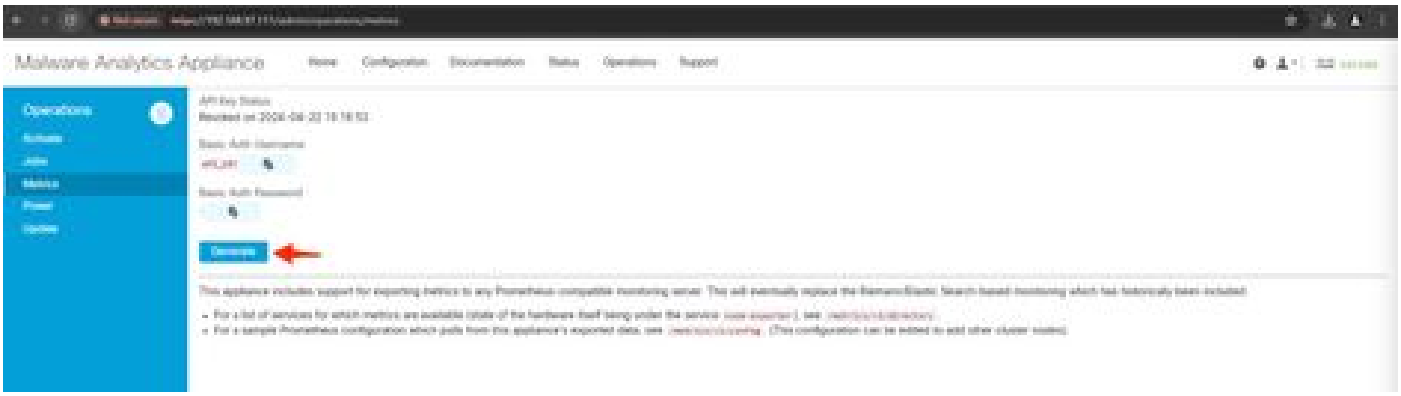
- Grafana

Configurar

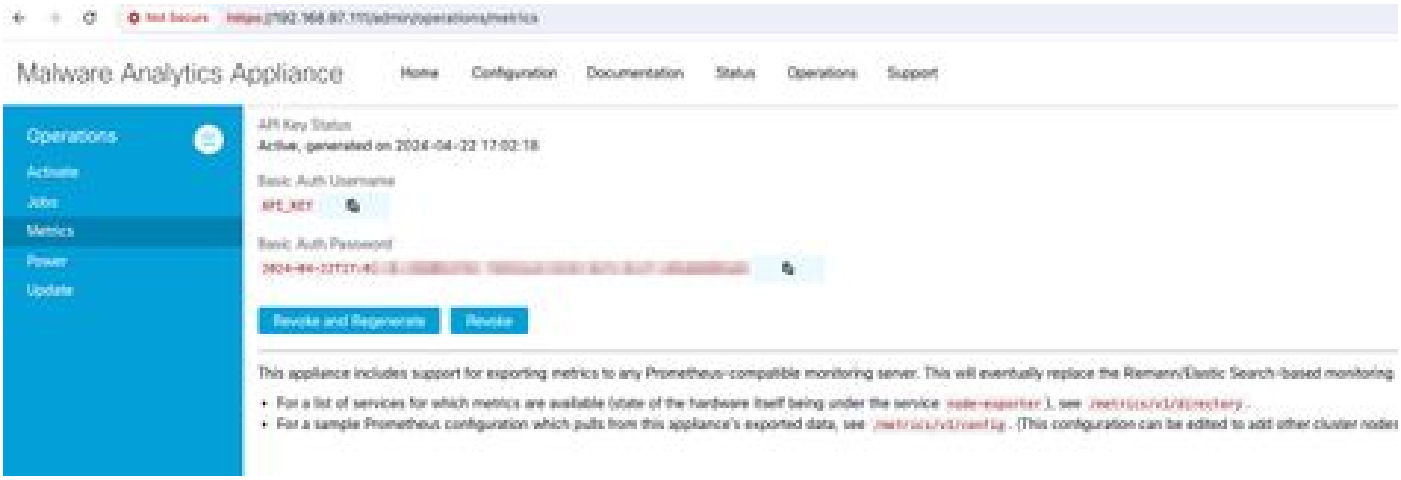
Para este documento, hemos utilizado un Windows 11 Pro como host remoto donde instalamos Prometheus y Grafana. Estas herramientas también están disponibles para Linux o MacOS.

1. Generar clave de API en el appliance de análisis de malware seguro (SMA) para acceder a las métricas

Inicie sesión en el dispositivo SMA Opadmin. Generar Clave de API para Métricas desde Opadmin > Operation > Metrics



2. Se generará un nombre de usuario y contraseña de autenticación básica que necesitaremos utilizar en la configuración de Prometeo remoto.



3. Instalar y configurar Prometheus

Siga las instrucciones proporcionadas por las guías del usuario de Prometheus para instalar su instancia si está utilizando Linux o MacOS. Para este documento, hemos instalado Prometheus en una máquina con Windows 11, y para el proceso de instalación, seguimos este video de Youtube.

4. Cree un archivo de configuración con el nombre `prometheus.yml`con el siguiente contenido -

```
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. En la sección `basic_auth`, utilice el nombre de usuario y la contraseña de autenticación básica generados en el paso 1.

6. Extraiga la configuración de los servicios de los que podrá extraer métricas introduciendo lo siguiente en la interfaz de usuario después de iniciar sesión en Opadmin -

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

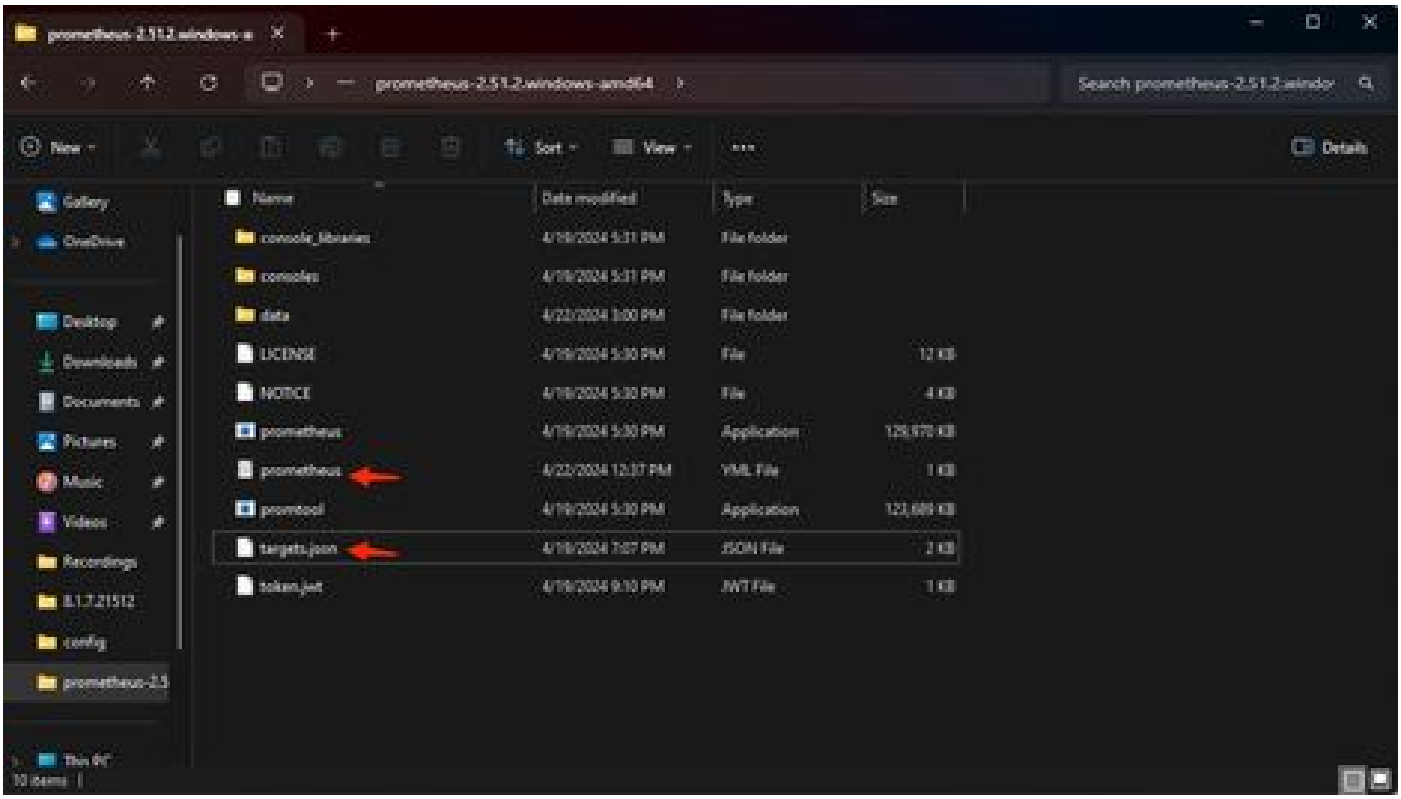
Usted recibirá algo como -

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

Aquí `192.168.97.111` es la IP de administración para mi dispositivo SMA.

7. Cree un fichero con el nombre `targets.json` y copie el contenido anterior en dicho fichero.

8. Copie `prometheus.yml` y `targets.json` en el directorio Prometheus (siga las guías de instalación), Para Windows, he creado una carpeta en la unidad C:\ y extraído los archivos de instalación Prometheus allí. Luego copió `prometheus.yml` y `targets.json` en la misma carpeta.



9. Iniciar Prometeo

Comiencen con Prometeo. Para Windows, ejecute `prometheus.exe` desde la línea de comandos.

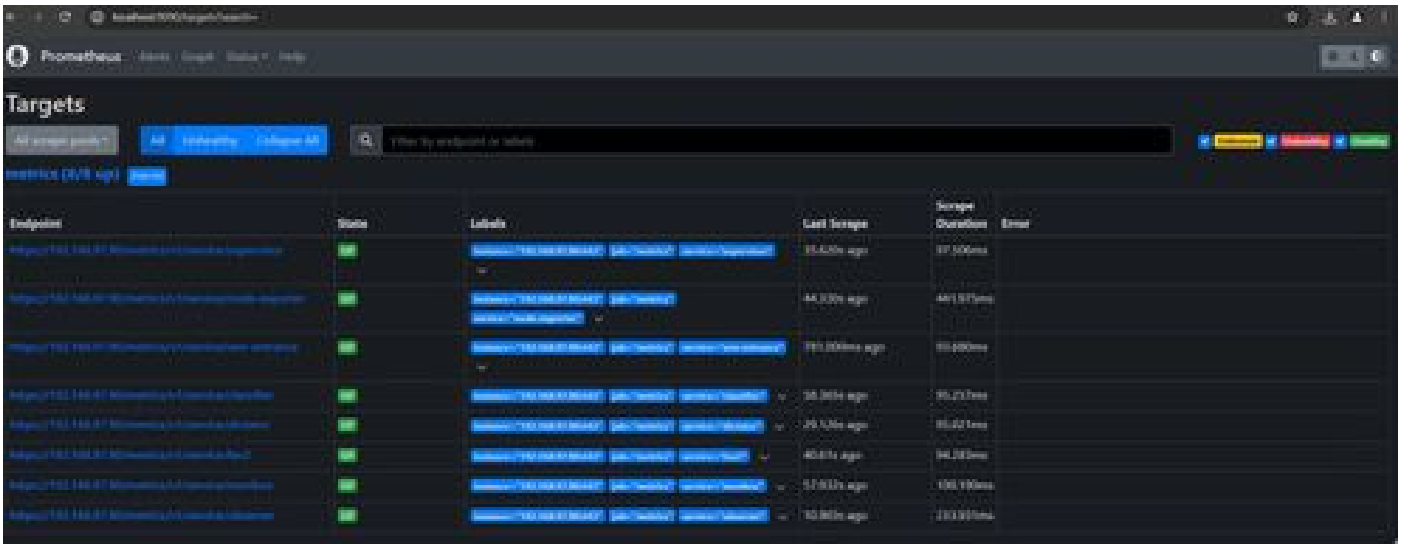
```
C:\Prometheus\prometheus-2.51.2.windows-amd64\prometheus-2.51.2.windows-amd64>prometheus.exe
```

Esto iniciará el Prometheus y comenzará a obtener las métricas del dispositivo SMA. Nota: No cierre la línea de comandos o Prometeo se cerrará.

10. Para comprobar si su instancia local de Prometheus es capaz de extraer la métrica de la carga del dispositivo SMA Prometheus UI - `http://localhost:9090/`

11. Vaya a `Estado` > `Destinos` - http://localhost:9090/targets?search=

En unos minutos debería ver todos los objetivos y el estado `ACTIVO` .



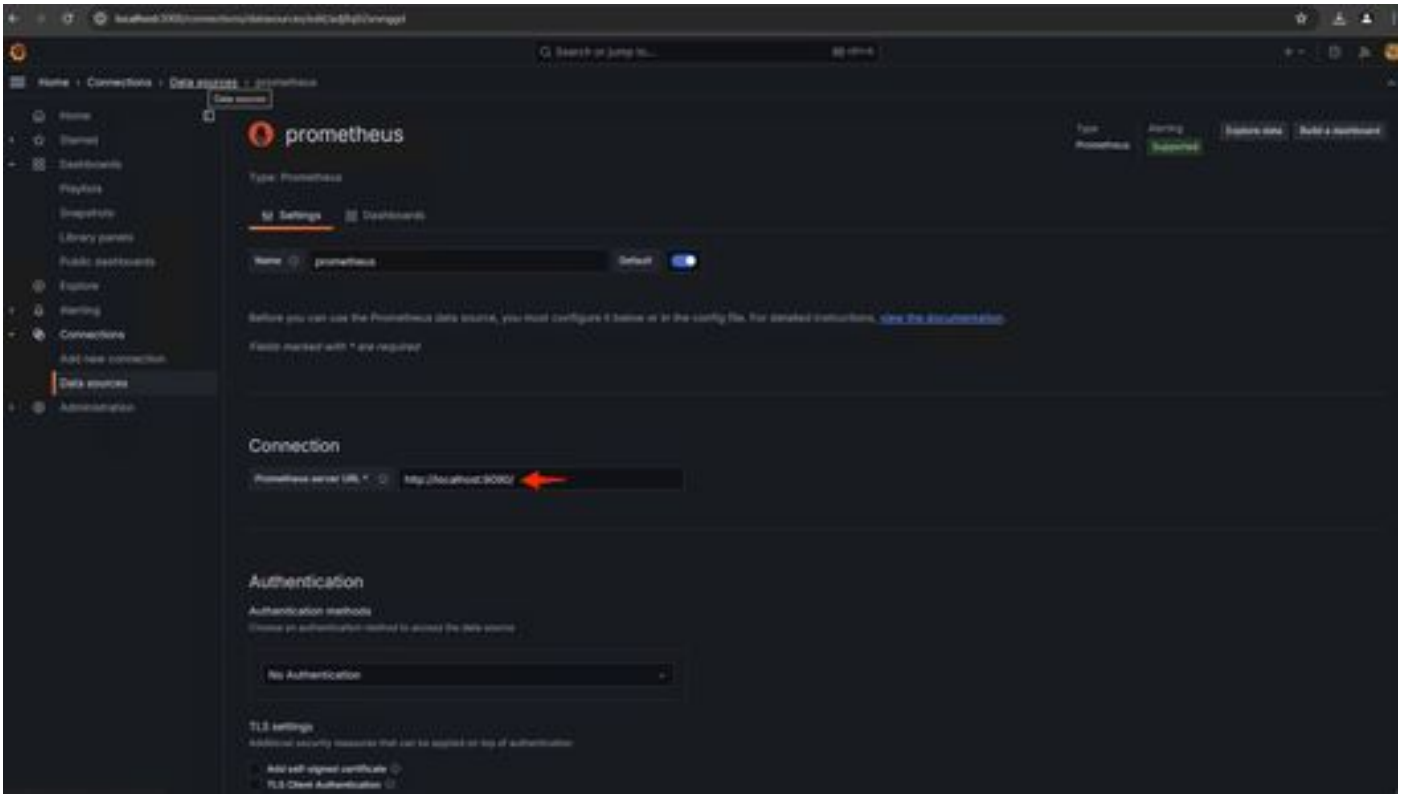
12. Instalar y configurar Grafana

Descargue el ejecutable de Grafana de Grafana Labs. Instale Granafa y siga las instrucciones proporcionadas por el instalador.

13. Después de instalar la interfaz de usuario de acceso Grafana en el navegador -`http://localhost:3000/`

Vaya a **Inicio > Conexiones > Orígenes de datos** - `http://localhost:3000/connections/datasources`

`Seleccione Agregar nuevo origen de datos` y `SeleccionePrometeo` en la lista. Ingrese `http://localhost:9090/` como URL del servidor Prometheus



En la parte inferior de la página, `seleccione Guardar y probar`. Después de realizar una prueba con éxito, podemos crear un panel.

14. Crear panel de Grafana

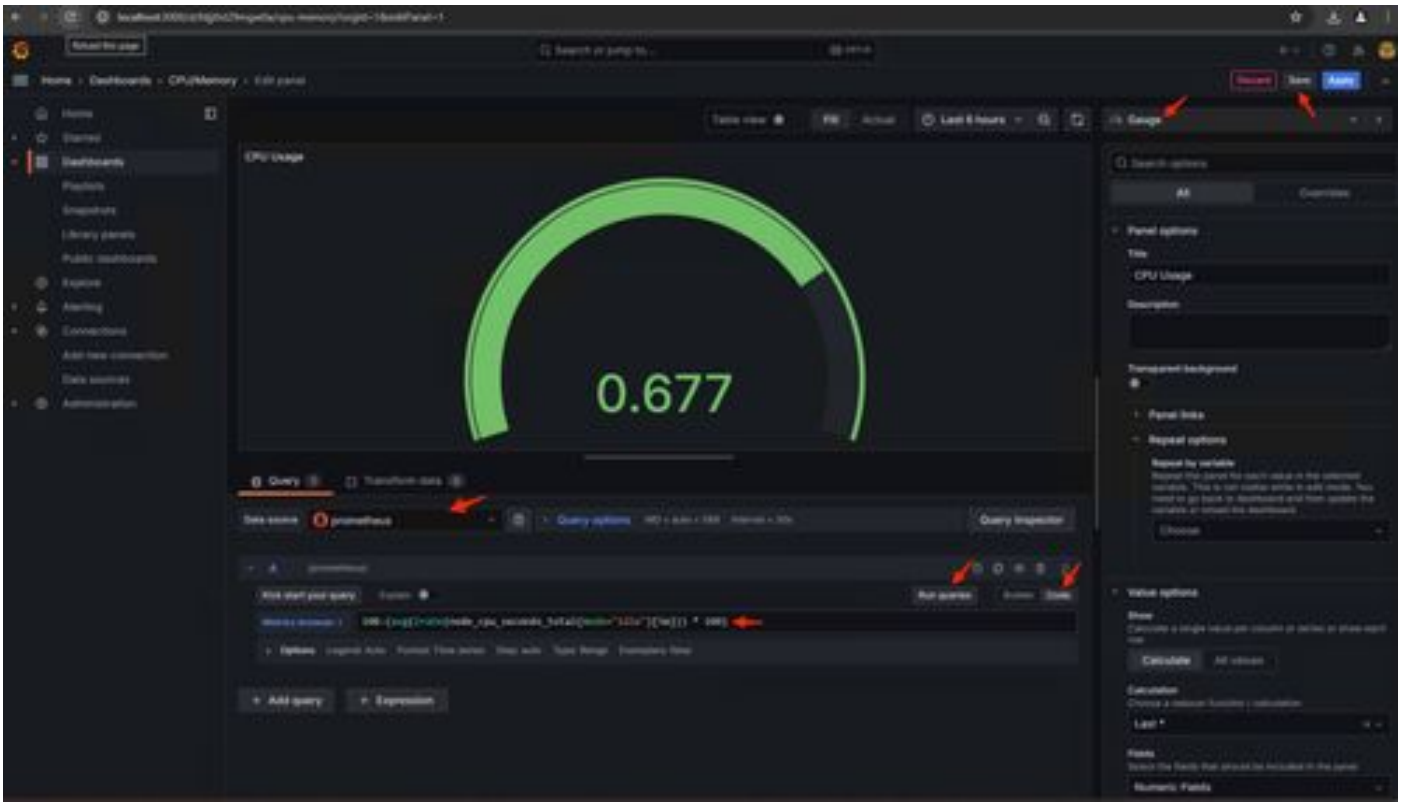
Vaya a `Paneles` en la interfaz de usuario de Grafana , `Seleccione Crear panel`>`Agregar visualización`. `Seleccione Prometeo` Origen de datos.

En el Generador de consultas, seleccione Codeinput, Seleccionar tipo de visualización (I selected Gage)

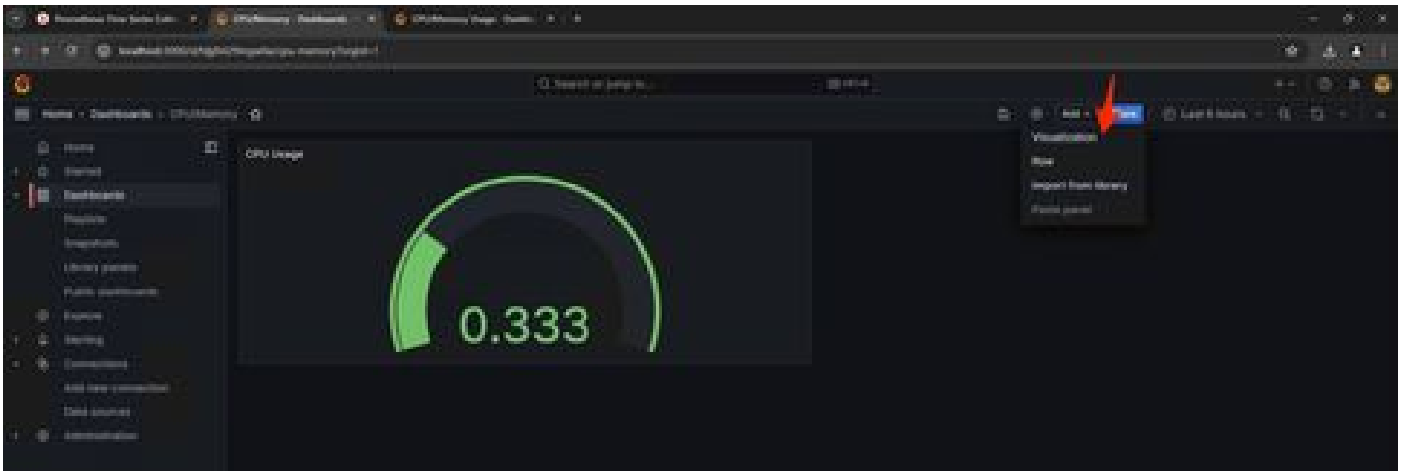
Introduzca la siguiente consulta **paraUso de CPU**-

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

15. Haga clic en `Ejecutar consultas` y debería ver una visualización del uso de la CPU como esta -

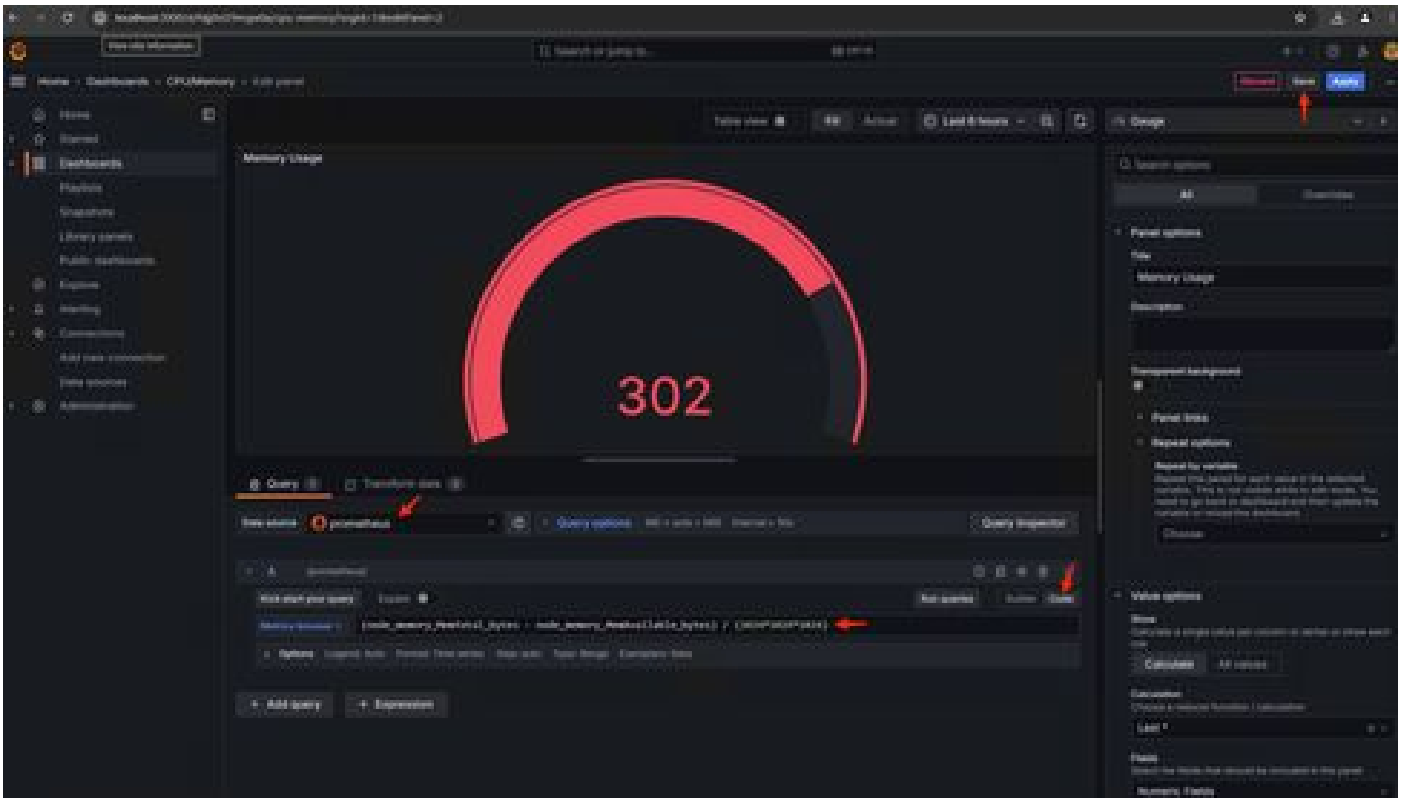


16. Guarde el panel, asigne un nombre al panel y haga clic en Guardar. Agregar otra `visualización` para el uso de memoria -



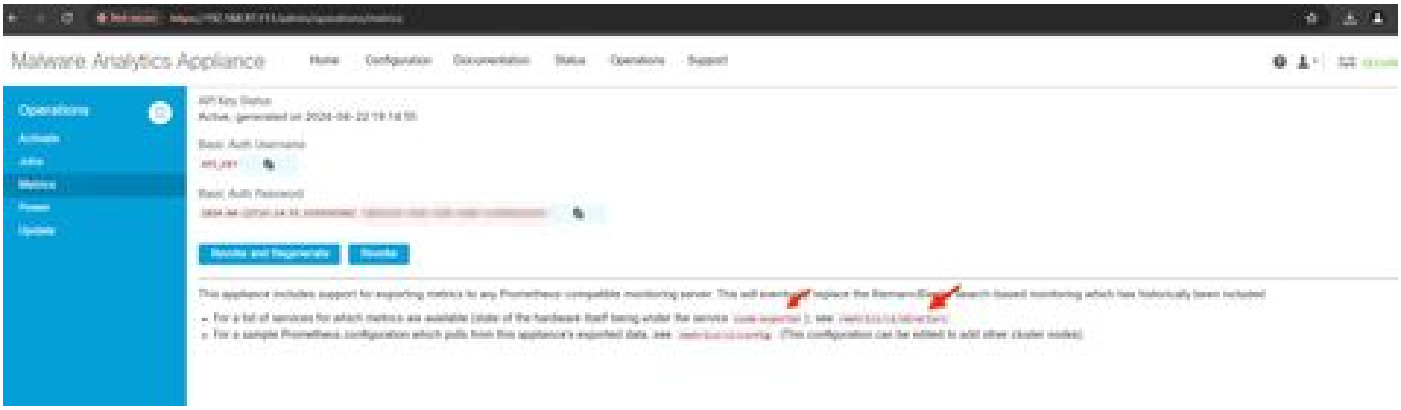
17. Para la utilización de memoria, utilice la siguiente consulta

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



18. Guarde los cambios y debería tener un panel como este:

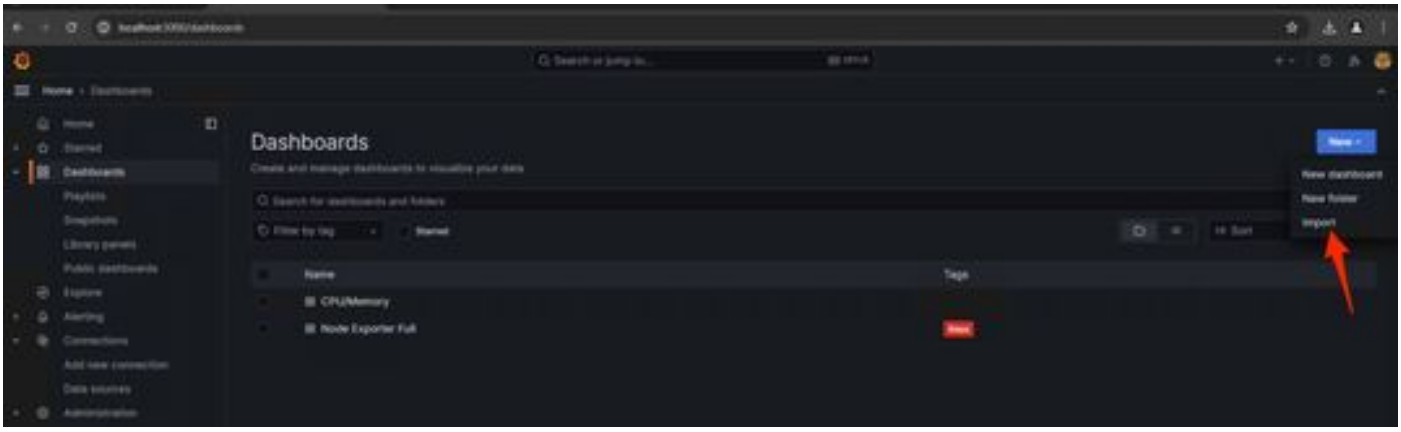
19. Hay disponibles otros indicadores de hardware y software. Para obtener más información, haga clic en los enlaces proporcionados `enOpadmin`> página `Métricas`.



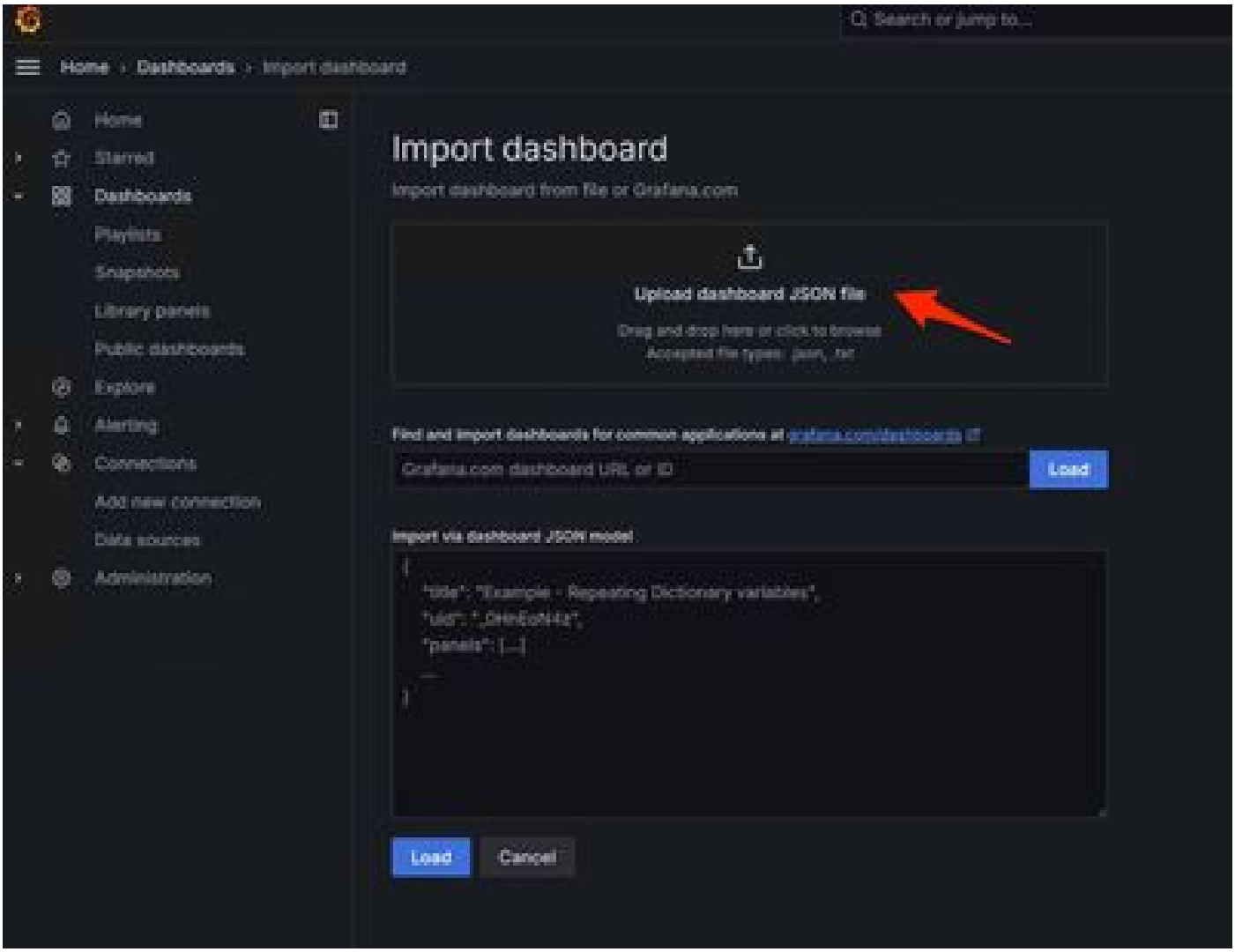
Plantilla de panel de Grafana

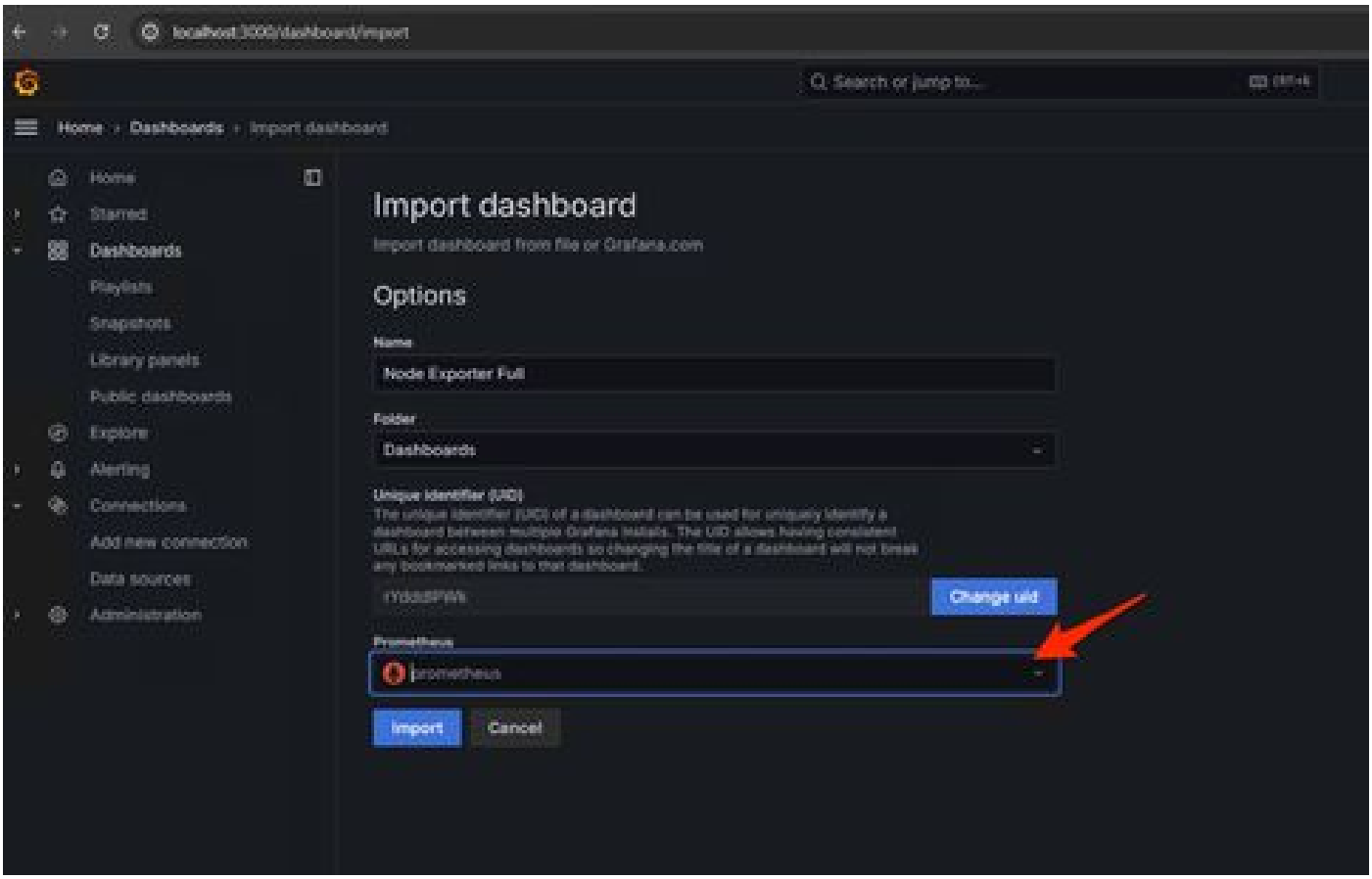
Hay muchas plantillas de paneles Grafana disponibles para el Exportador de nodos en el sitio web de Grafana. Una de ellas es: Node Exporter Full

1. Para importar este panel a su instancia de Grafana Descargue JSON, importe el archivo JSON en Grafana

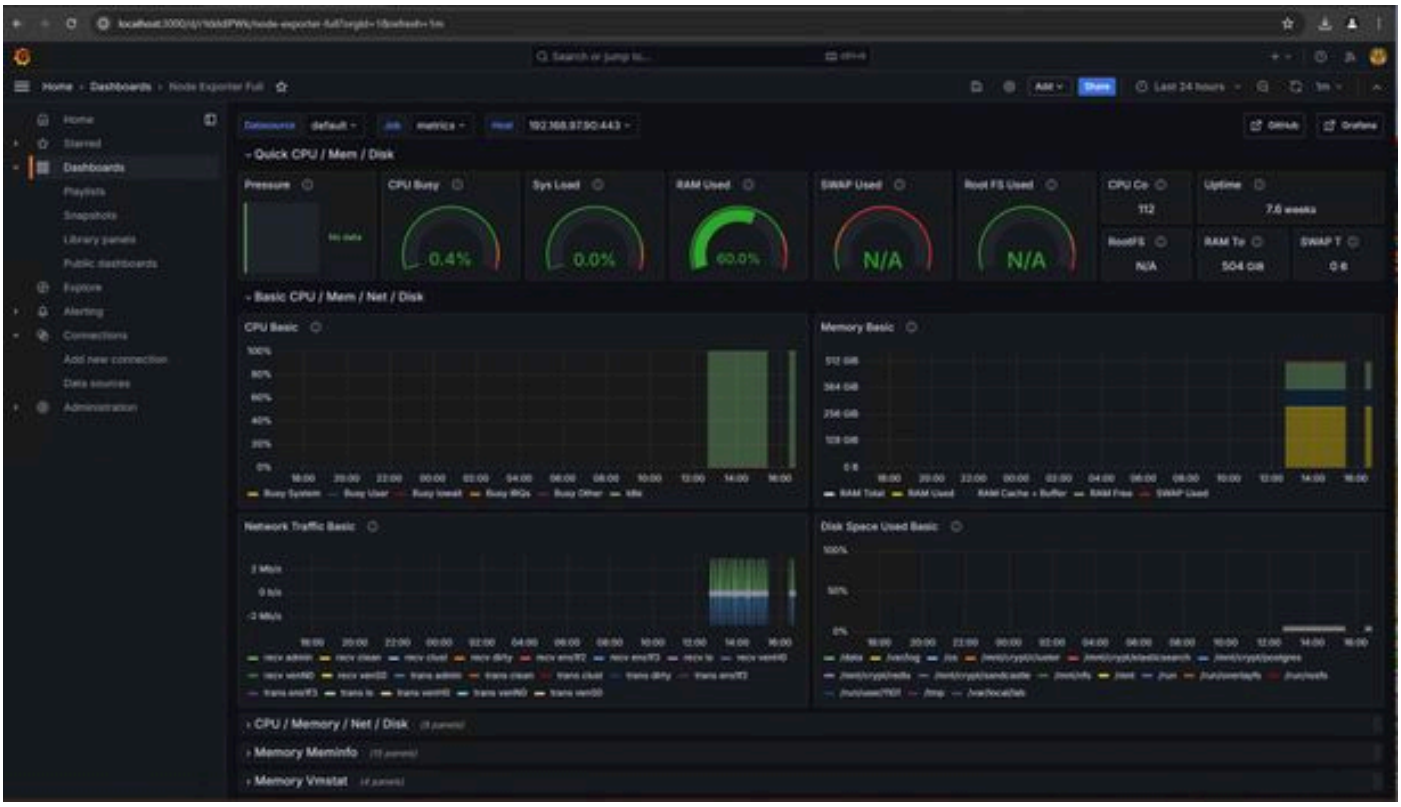


2. Cargue el archivo JSON y seleccione el origen de datos Prometheus


Search or jump to...
Home › Dashboards › Import dashboard
Home
Starred
Dashboards
Playlists
Snapshots
Library panels
Public dashboards
Explore
Alerting
Connections
Add new connection
Data sources
Administration
Import dashboard
Import dashboard from file or Grafana.com
Upload dashboard JSON file
Drag and drop here or click to browse
Accepted file types: .json, .txt
Find and import dashboards for common applications at grafana.com/dashboards
Grafana.com dashboard URL or ID
Load
Import via dashboard JSON model
{
"title": "Example - Repeating Dictionary variables",
"uid": "_DHnEoH4z",
"panels": [...]
}
Load
Cancel



3. Esto creará un panel con mucha información de hardware (no todas las métricas del panel están disponibles)-



Troubleshoot

Si Prometheus no pudo conectarse y extraer la métrica del dispositivo SMA, verá el error en `Estado` > `Destinos` -

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

Si hay `anyError`, debe corregirse antes de poder extraer los datos. Un problema común es que el certificado SSL del dispositivo SMA Opadmin no es de confianza para el equipo local. Asegúrese de crear un certificado de administración SMA con IP y DNS SAN, y agregue la CA raíz de firma al almacén de confianza del equipo local.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).