

# 如何配置远程Prometheus和Grafana以监控安全恶意软件分析（以前称为Threat Grid）设备

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[Grafana控制面板模板](#)

[故障排除](#)

---

## 简介

在安全恶意软件分析(SMA)设备中，我们不提供SNMP协议来监控设备资源使用情况，而是提供[Prometheus](#)。

本文档将概述如何配置远程Prometheus实例和使用Grafana可视化从设备提取的数据。

## 先决条件

将以下工具下载并安装到本地计算机/服务器上：

- 普罗米修斯-<https://prometheus.io/download/>
- 格拉法纳-<https://grafana.com/oss/grafana/>

## 要求

- 安全恶意软件分析(SMA)设备软件版本2.18及更高版本
- Windows计算机
- 对设备管理员(Opadmin)控制台的管理人员访问权限
- 安全恶意软件分析(SMA)设备Opadmin SSL证书受本地计算机信任

## 使用的组件

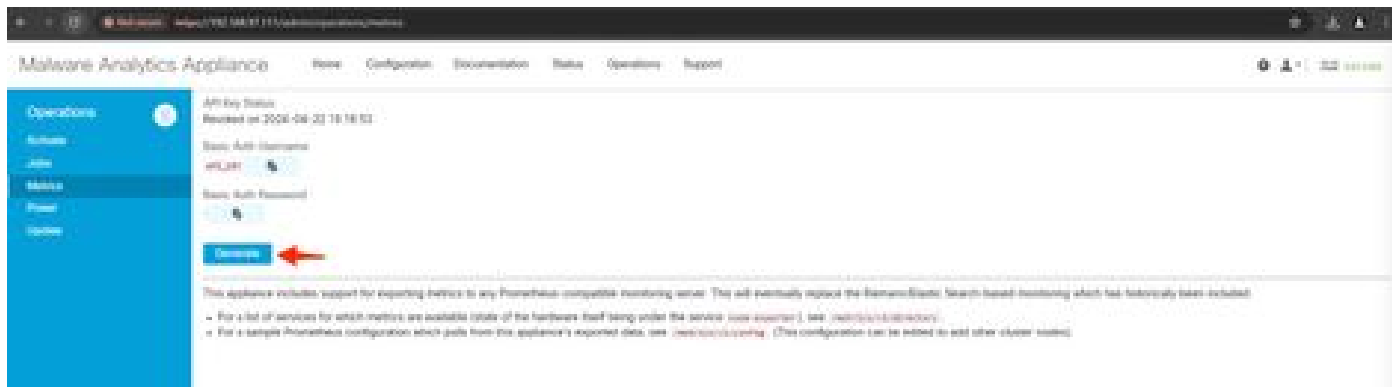
- 安全恶意软件分析(SMA)设备
- Windows 11 Pro计算机
- [普罗米修斯](#)
- [格拉法纳](#)

## 配置

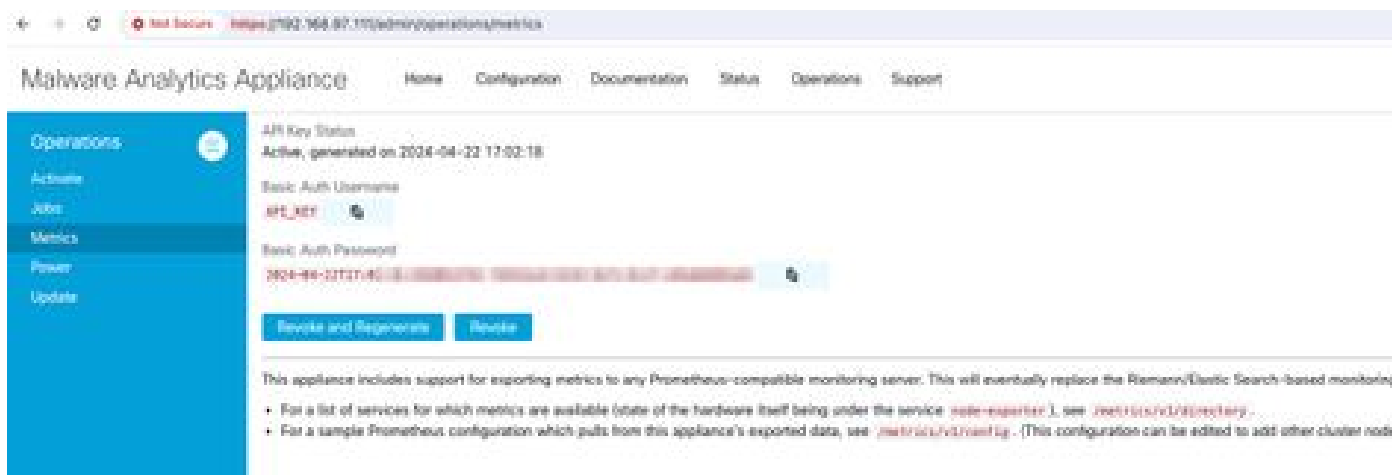
在本文档中，我们使用Windows 11 Pro作为远程主机，在上面安装了Prometheus和Grafana。这些工具还可用于Linux或MacOS。

## 1. 在安全恶意软件分析(SMA)设备中生成API密钥以访问指标

登录SMA设备Opadmin。通过Opadmin > Operation > Metrics生成度量的API密钥



## 2. 将生成一个基本身份验证用户名和密码，我们需要将其用于远程Prometheus配置。



## 3. 安装和配置Prometheus

如果您使用的是Linux或MacOS，请按照Prometheus用户指南提供的说明安装实例。在本文档中，我们已在Windows 11计算机上安装Prometheus，在安装过程中，我们遵循了[此Youtube视频](#)。

## 4. 创建名称为prometheus.ymlwith以下内容的配置文件-

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-xxxxxxxxxxxxx"
```

5. 在basic\_auth部分中，使用步骤1中生成的基本身份验证用户名和口令。
6. 获取服务的配置，登录Opadmin后，在UI中输入以下内容，即可从中获取指标-

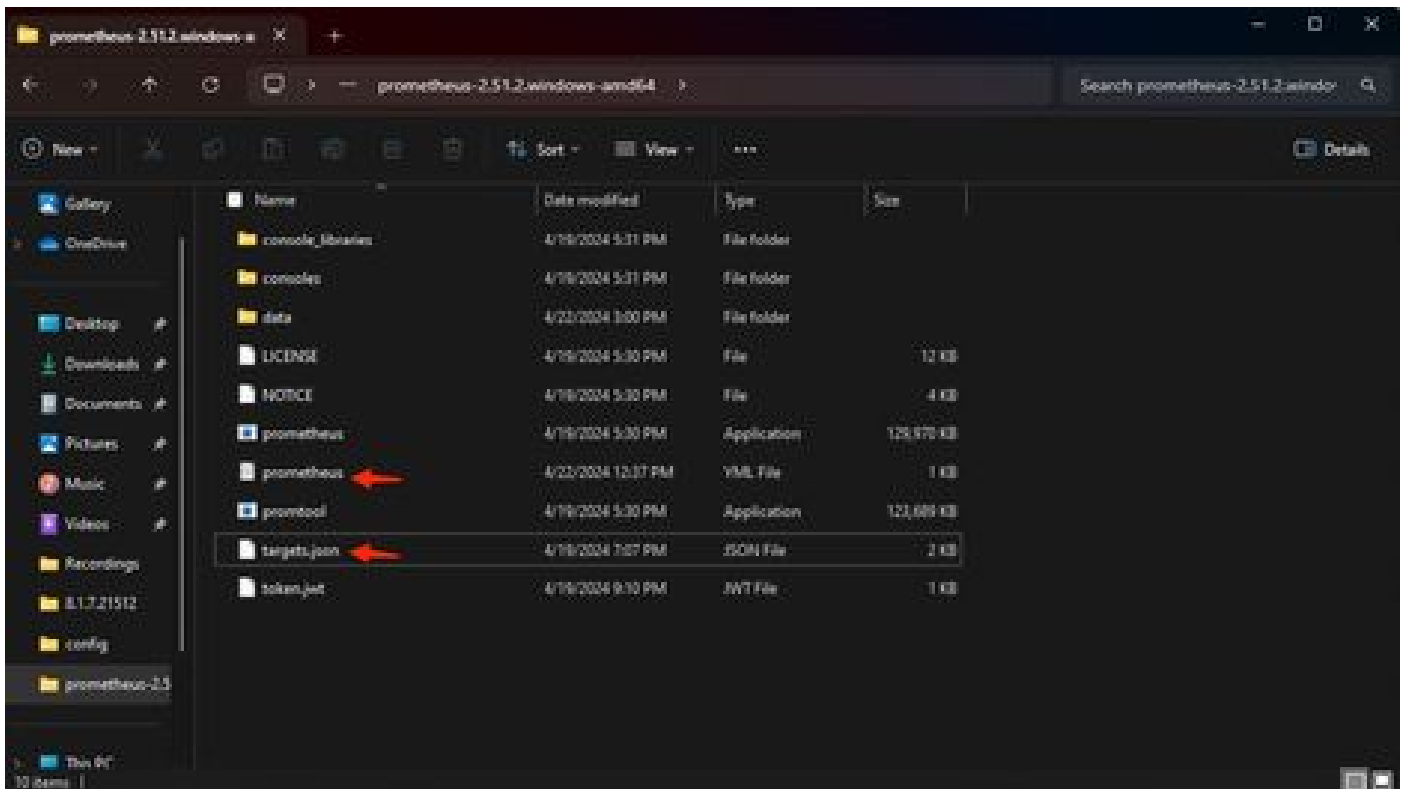
`https://<opadmin IP>/metrics/v1/config`

您将获得类似于-

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

此处192.168.97.111是我的SMA设备的管理IP。

7. 使用名称targets.json创建文件，然后将以上内容复制到该文件中。
8. 将prometheus.yml和targets.json复制到Prometheus目录（按照安装指南操作）。对于Windows，我已在C:\驱动器中创建了一个文件夹，并在其中解压缩了Prometheus安装文件。然后将prometheus.yml和targets.json复制到同一文件夹。



## 9. 启动Prometheus

启动普罗米修斯。对于Windows，请从命令行执行prometheus.exe。

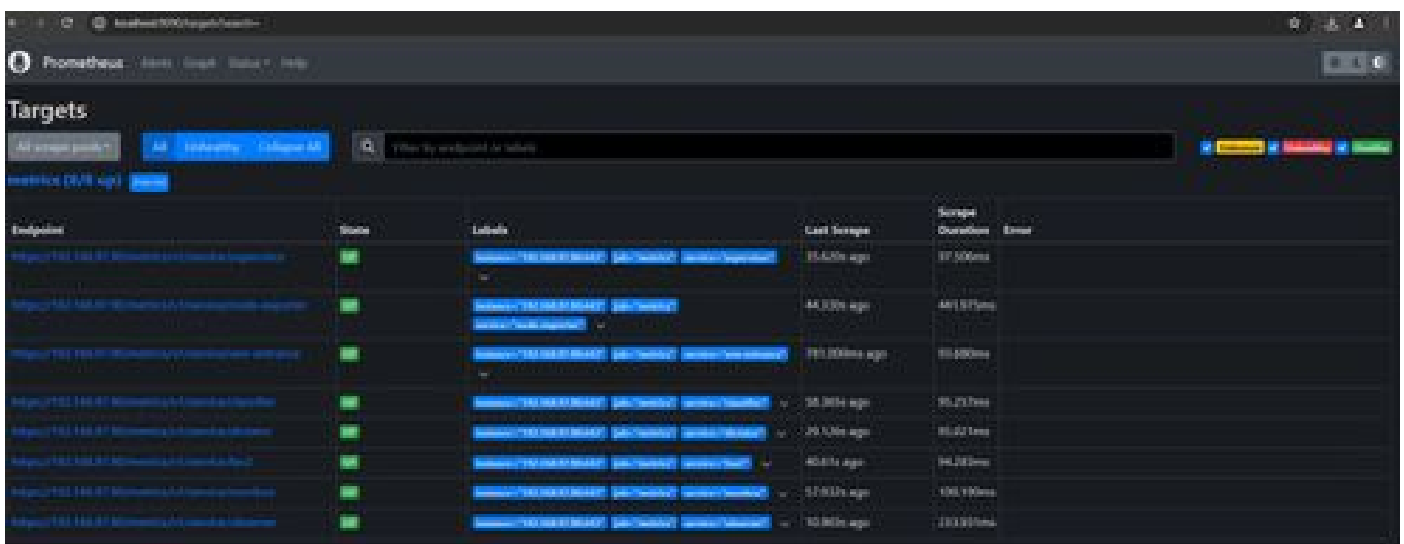
```
C:\Prometheus\prometheus-2.51.2.windows-amd64\prometheus-2.51.2.windows-amd64>prometheus.exe
```

这将启动Prometheus并开始从SMA设备提取度量。注意：请勿关闭命令行，否则Prometheus将关闭。

10. 检查本地Prometheus实例是否能够从SMA设备加载Prometheus UI提取度量-  
'http://localhost:9090/'

11. 转至 状态 > 目标 - <http://localhost:9090/targets?search=>

几分钟内，您应看到所有目标和状态UP（正常模式）。



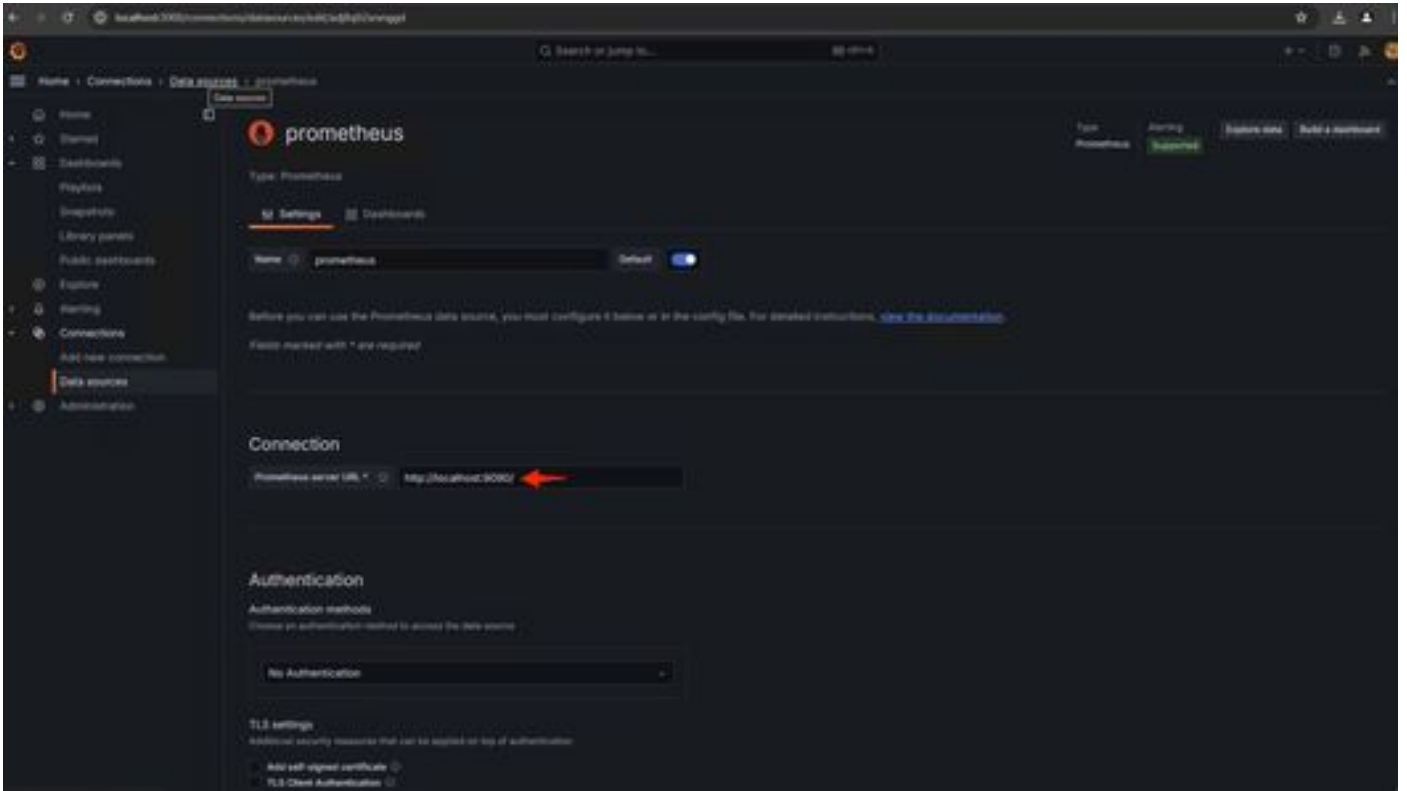
## 12. 安装和配置Grafana

从[Grafana Labs](https://grafana.com/)下载Grafana可执行文件。按照安装程序提供的说明安装Grafana。

13. 在浏览器中安装Grafana访问UI后-<http://localhost:3000/>

转至Home > Connections > Data sources - <http://localhost:3000/connections/datasources>

从列表中选择Add New Datasource和SelectPrometheus。输入“<http://localhost:9090/>”作为Prometheus服务器URL



在该页面底部，选择“保存并测试”。测试成功后，我们可以创建控制面板。

#### 14. 创建Grafana控制面板

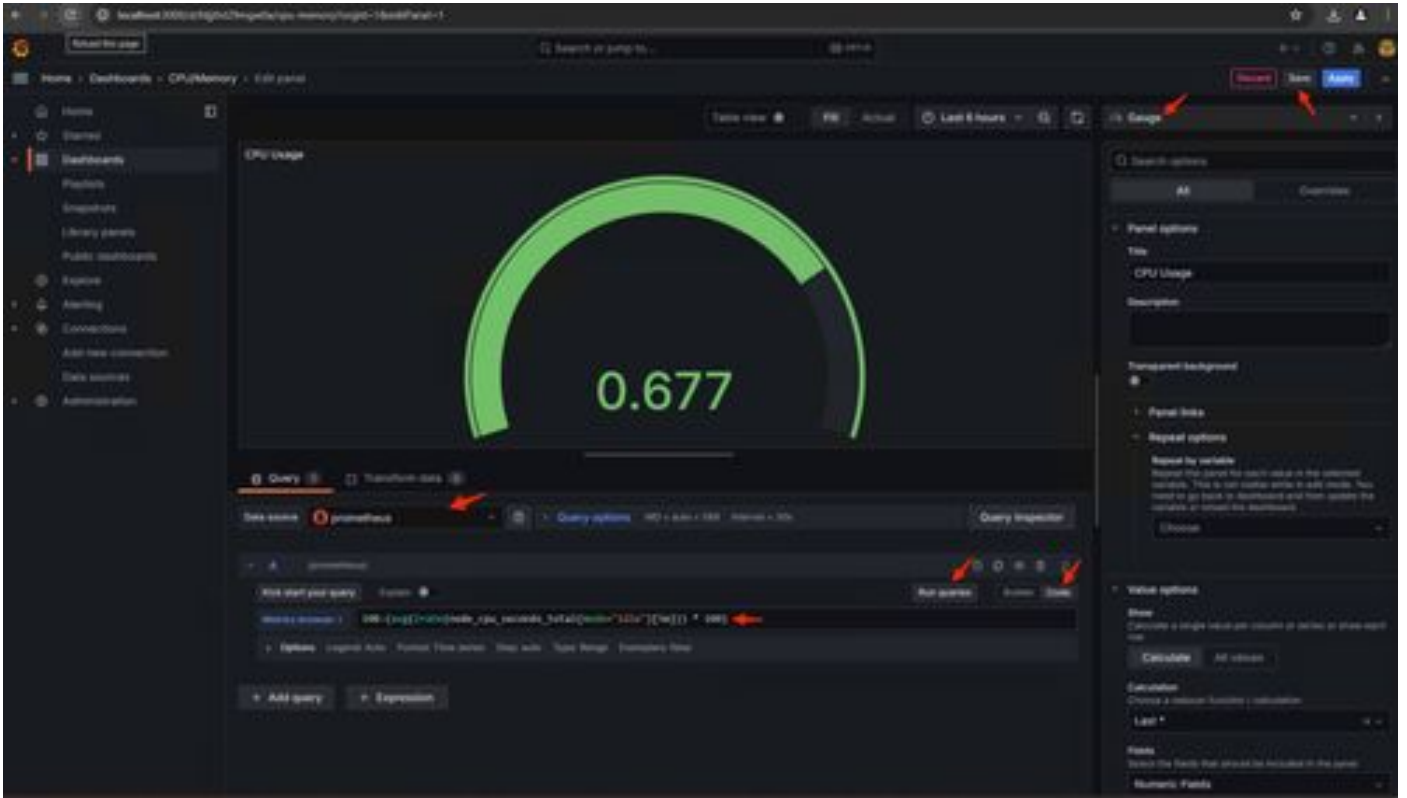
转到Grafana UI中的控制面板(Create Dashboard>添加可视化)。选择Prometheus数据源。

在查询生成器selectCodeinput中，选择可视化类型(I selected Gauge)

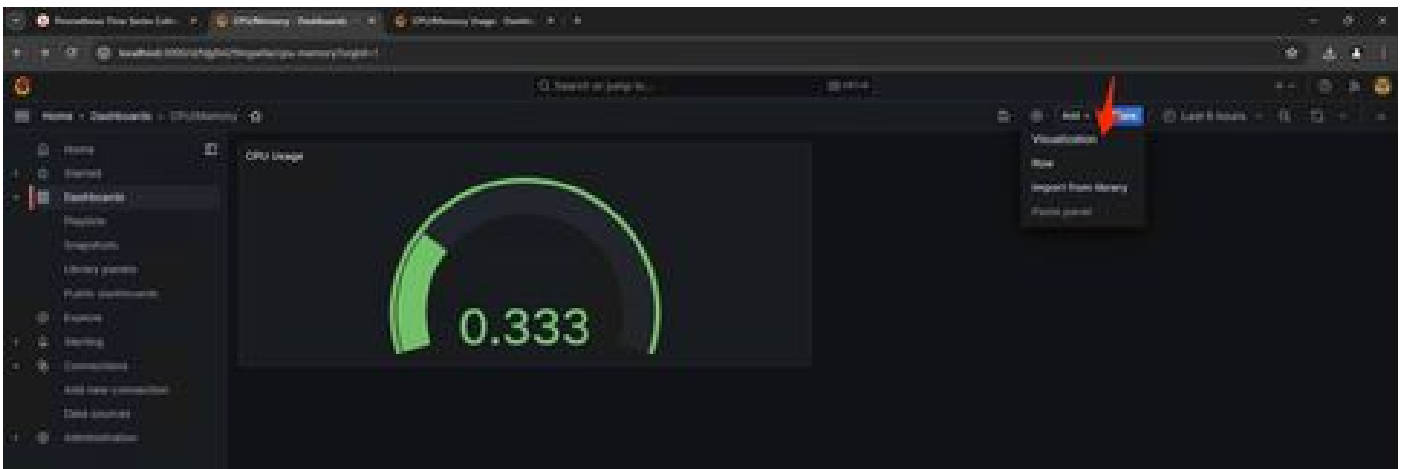
输入以下查询CPU利用率-

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

15. 单击Run 查询，您应该会看到如下所示的CPU使用情况-

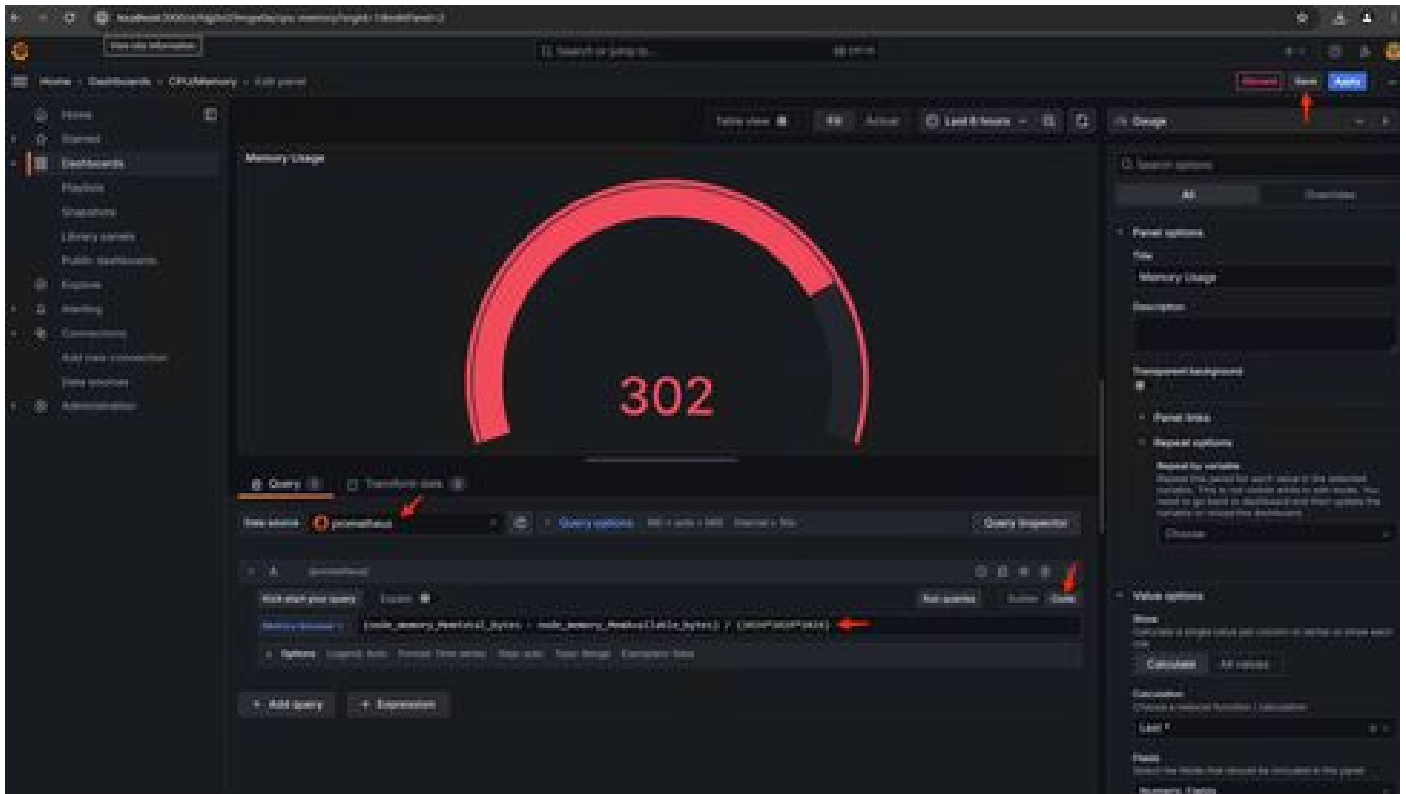


16. 保存面板，命名控制面板，然后保存。添加另一个内存使用情况的可视化-

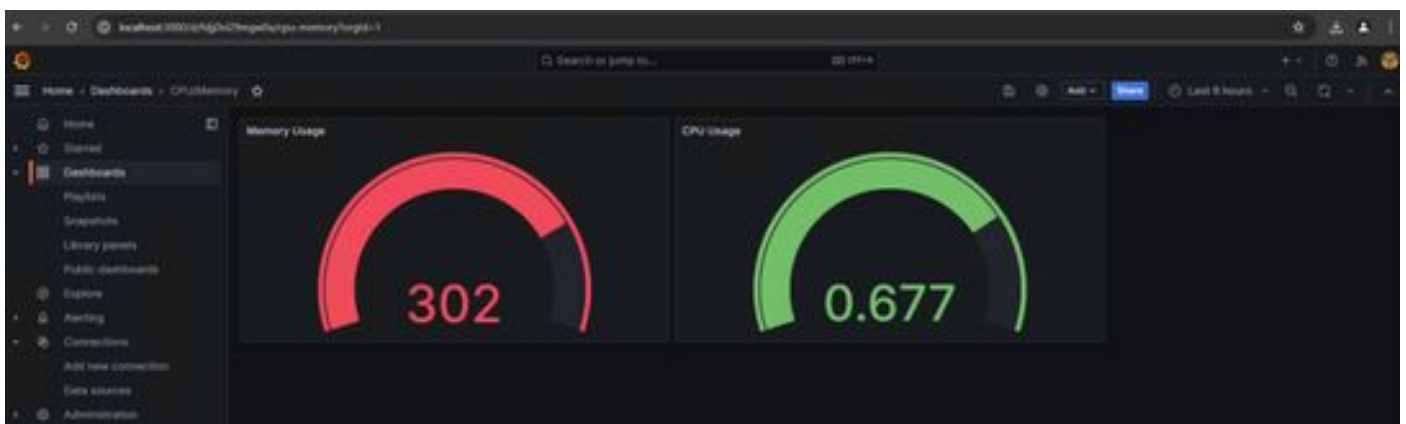


17. 对于内存利用率，请使用以下查询

$(\text{node\_memory\_MemTotal\_bytes} - \text{node\_memory\_MemAvailable\_bytes}) / (1024 * 1024 * 1024)$



18. 保存更改，您应该有一个这样的控制面板-



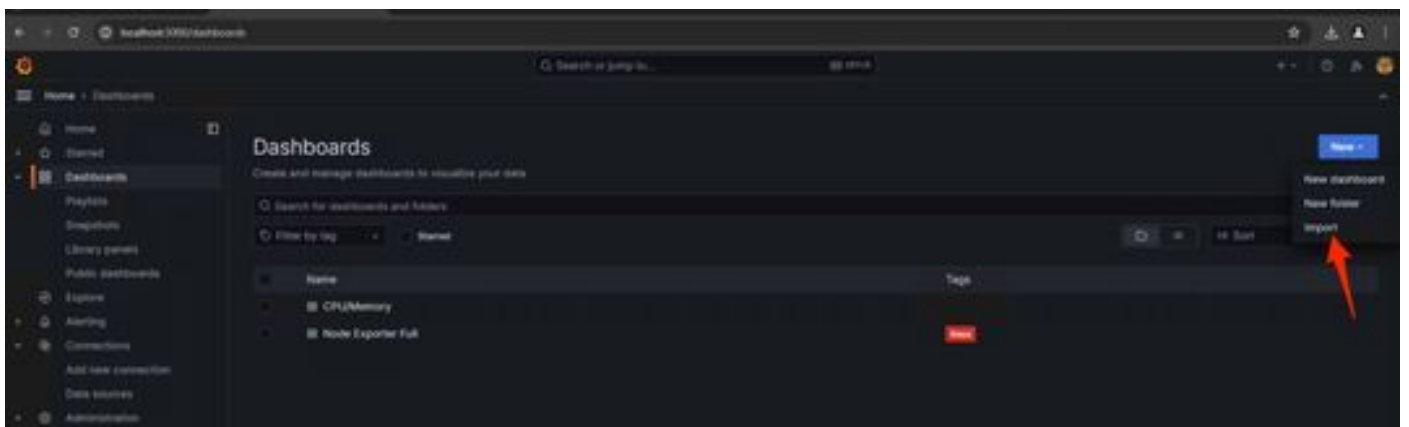
19. 其他硬件和软件指标可用，有关详细信息，请单击Opadmin> Metrics页面中提供的链接



## Grafana控制面板模板

在Grafana网站上，有许多可用于节点导出器的Grafana控制面板模板。其中一个[是-节点导出器已满](#)

1. 要将此控制面板导入您的Grafana实例下载JSON，请导入Grafana中的JSON文件



2. 上传JSON文件并选择Prometheusdata source



- 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, .net

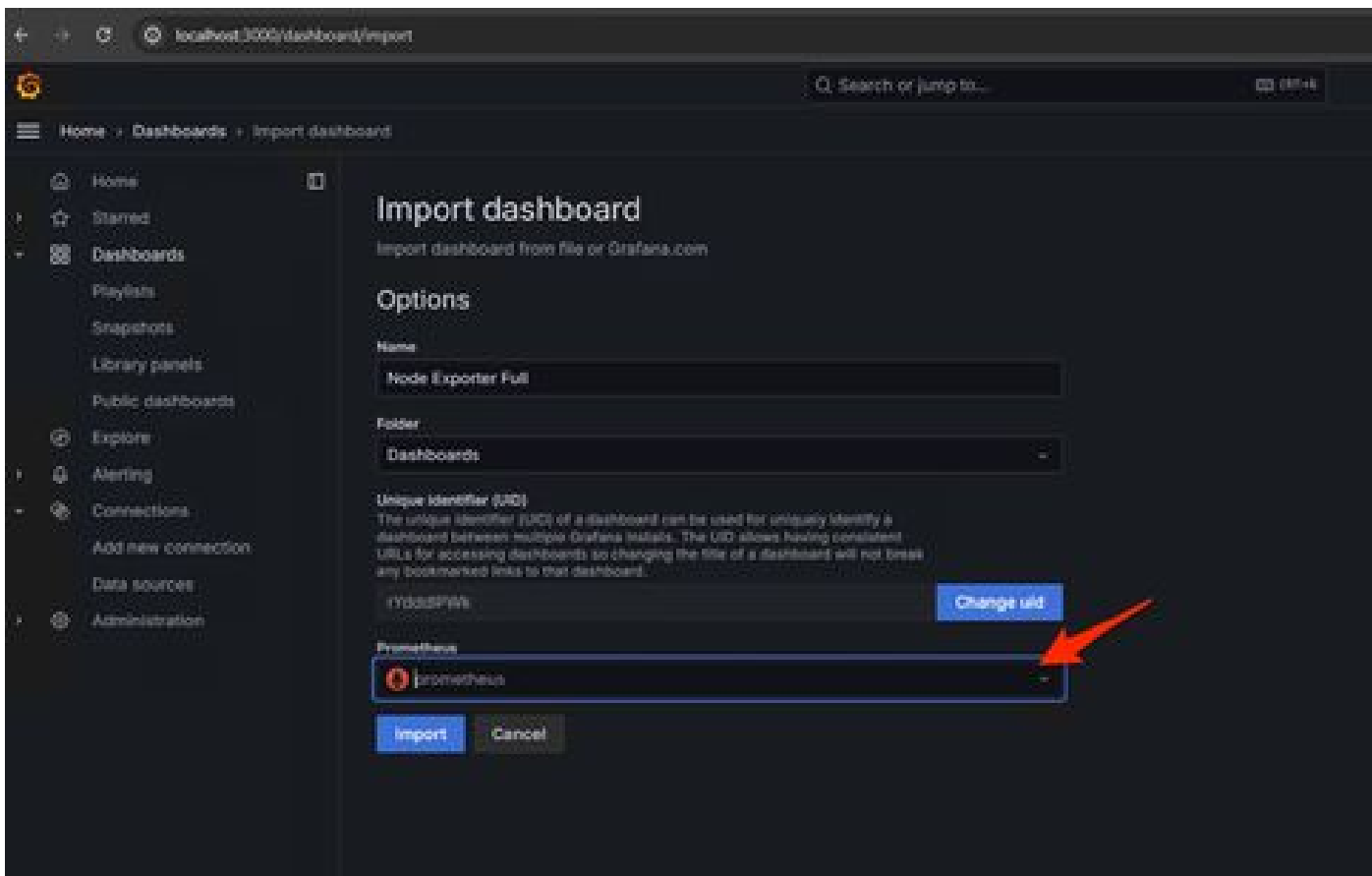


Find and import dashboards for common applications at [grafana.com/dashboards](https://grafana.com/dashboards) if

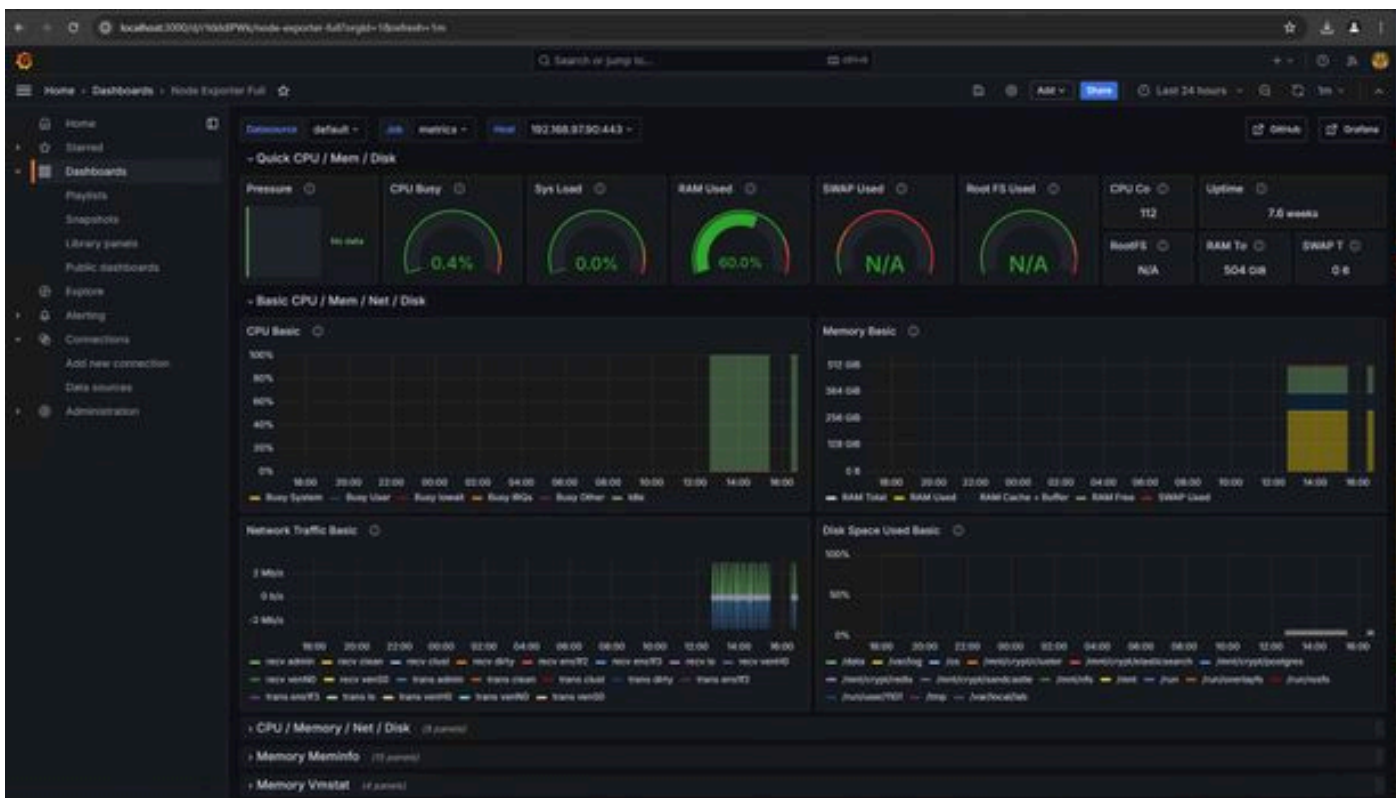
Grafana.com dashboard URL or ID

Import via dashboard JSON model

```
{  
  "title": "Example - Repeating Dictionary variables",  
  "uid": "1_0Hn60t4z",  
  "panels": [...]  
}
```



3. 这将创建一个包含大量硬件信息的控制面板（并非所有面板指标都可用）-



## 故障排除

如果Prometheus未能从SMA设备连接和提取度量，您将在状态 > 目标中看到此错误。 <http://localhost:9090/targets?search=>

如果存在anyError，需要先修复此问题，然后才能提取数据。常见问题是SMA设备的SSL证书Opadmin不受本地计算机信任。确保使用IP和DNS SAN创建SMA管理员证书，并将签名根CA添加到本地计算机的信任存储中。

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。