如何配置遠端Prometheus和Grafana以監控安全惡意軟體分析（以前稱為Threat Grid）裝置

目錄

簡介

在安全惡意軟體分析(SMA)裝置中，我們不提供SNMP協定來監控裝置資源使用情況，而是裝置提供Prometheus。

本文檔將概述如何配置遠端Prometheus例項和使用Grafanato視覺化從裝置中提取的資料。

必要條件

將下列工具下載並安裝至您的本機電腦/伺服器：

- 普羅米修斯-https://prometheus.io/download/
- 格拉法納-https://grafana.com/oss/grafana/

需求

- 安全惡意軟體分析(SMA)裝置軟體版本2.18及更高版本
- Windows電腦
- 對裝置管理員(Opadmin)控制檯的管理員訪問許可權
- 安全惡意軟體分析(SMA)裝置Opadmin SSL證書受本地電腦信任

採用元件

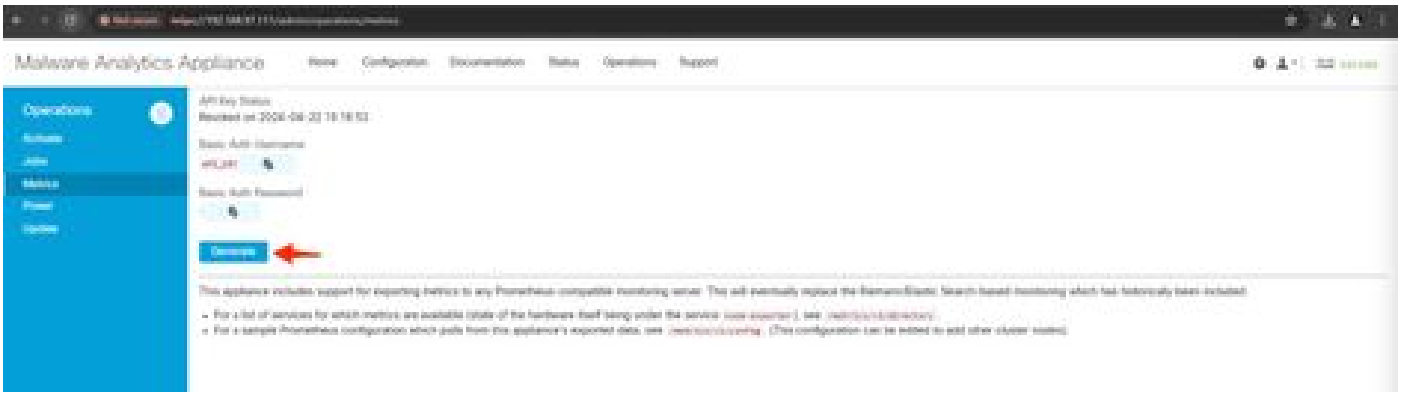
- 安全惡意軟體分析(SMA)裝置
- Windows 11 Pro電腦
- 普羅米修斯
- 格拉法納

設定

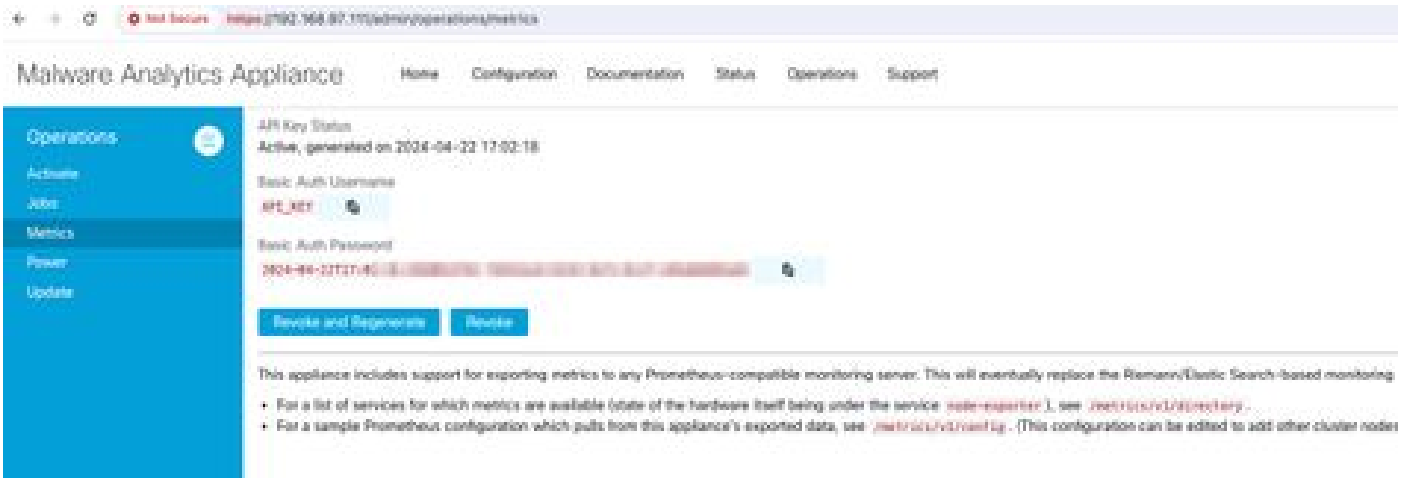
在本檔案中，我們使用Windows 11 Pro作為遠端主機，安裝Prometheus和Grafana。這些工具也可用於Linux或MacOS。

1. 在安全惡意軟體分析(SMA)裝置中生成API金鑰以訪問指標

登入到SMA Appliance Opadmin。 透過Opadmin >操作>度量生成度量的API金鑰



2. 將生成基本身份驗證使用者名稱和密碼，我們需要在遠端Prometheus配置中使用它們。



3. 安裝和配置Prometheus

如果您使用的是Linux或MacOS，請依照Prometheus使用者指南提供的指示來安裝您的執行處理。在本文檔中，我們已在Windows 11電腦上安裝Prometheus，在安裝過程中，我們遵循此Youtube影片。

4. 建立名為`prometheus.yml`with以下內容的配置檔案-

```
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. 在basic_auth部分中，使用步驟1中生成的基本身份驗證使用者名稱和口令。

6. 在登入Opadmin之後，在UI中輸入下列專案，以取得您將能夠取得測量結果的服務組態-

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

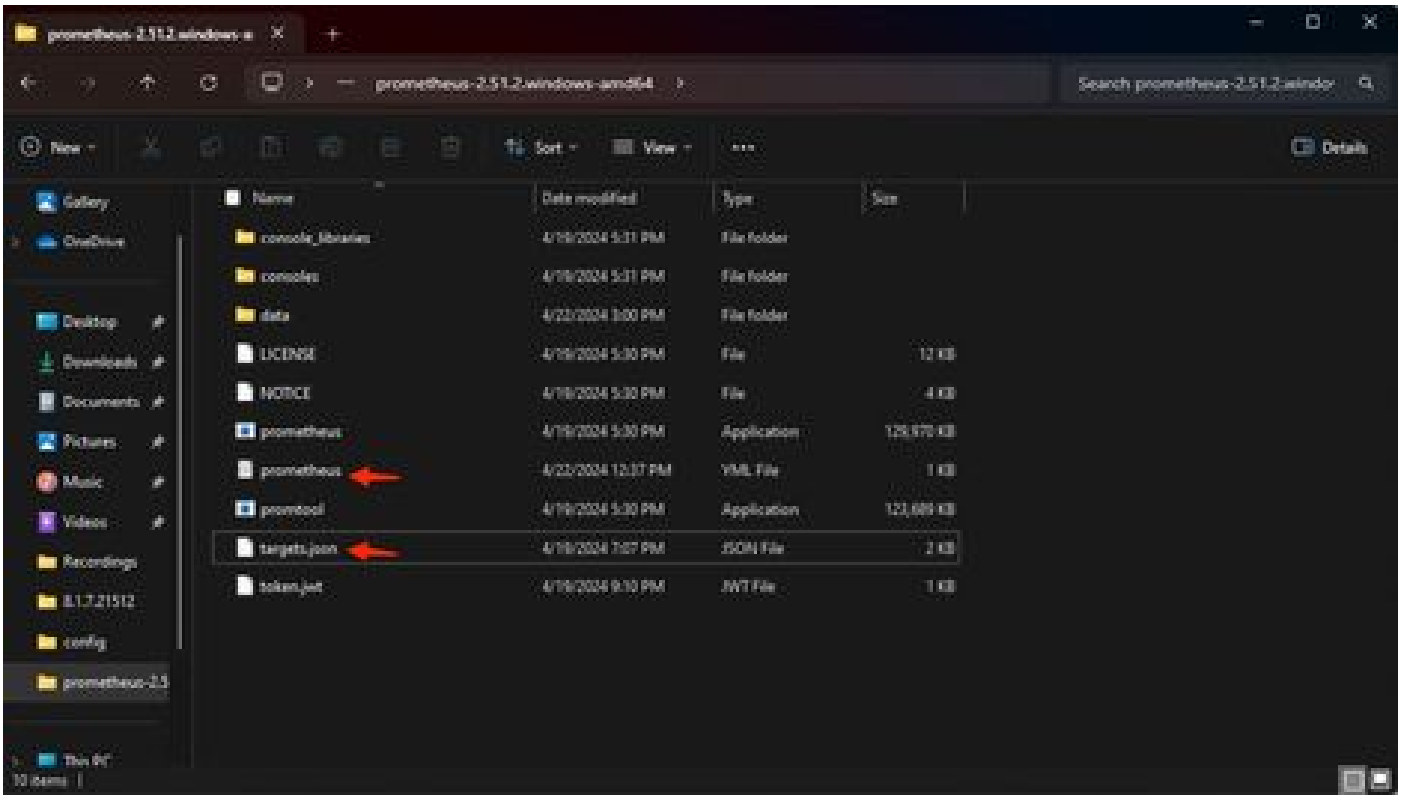
您將獲得類似於-

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

此處，192.168.97.111是我的SMA裝置的管理IP。

7. 建立名為targets.json的檔案，並將上述內容複製到該檔案中。

8. 將prometheus.yml和targets.json複製到Prometheus目錄（按照安裝指南操作）。對於Windows，我已在C:\驅動器中建立資料夾，並已提取該資料夾中的Prometheus安裝檔案。然後將prometheus.yml和targets.json複製到同一資料夾。



9. 啟動Prometheus

啟動普羅米修斯。對於Windows，請從命令列執行`prometheus.exe`。

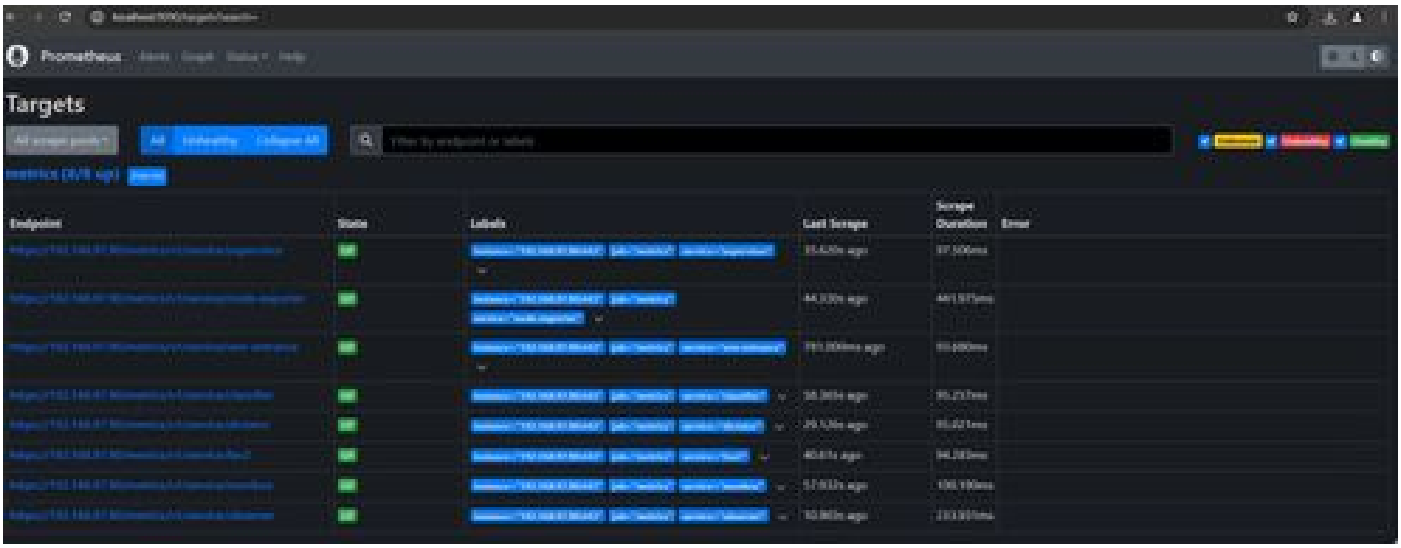
```
C:\Prometheus\prometheus-2.51.2.windows-amd64\prometheus-2.51.2.windows-amd64>prometheus.exe
```

這將啟動Prometheus並開始從SMA裝置提取度量。注意：請勿關閉命令列，否則Prometheus將關閉。

10. 要檢查本地Prometheus例項是否能從SMA裝置載入Prometheus UI提取度量-'http://localhost:9090/'

11. 轉至`Status` > `Targets` - http://localhost:9090/targets?search=

幾分鐘內，您應該會看到所有目標和狀態都為UP（藍色）。



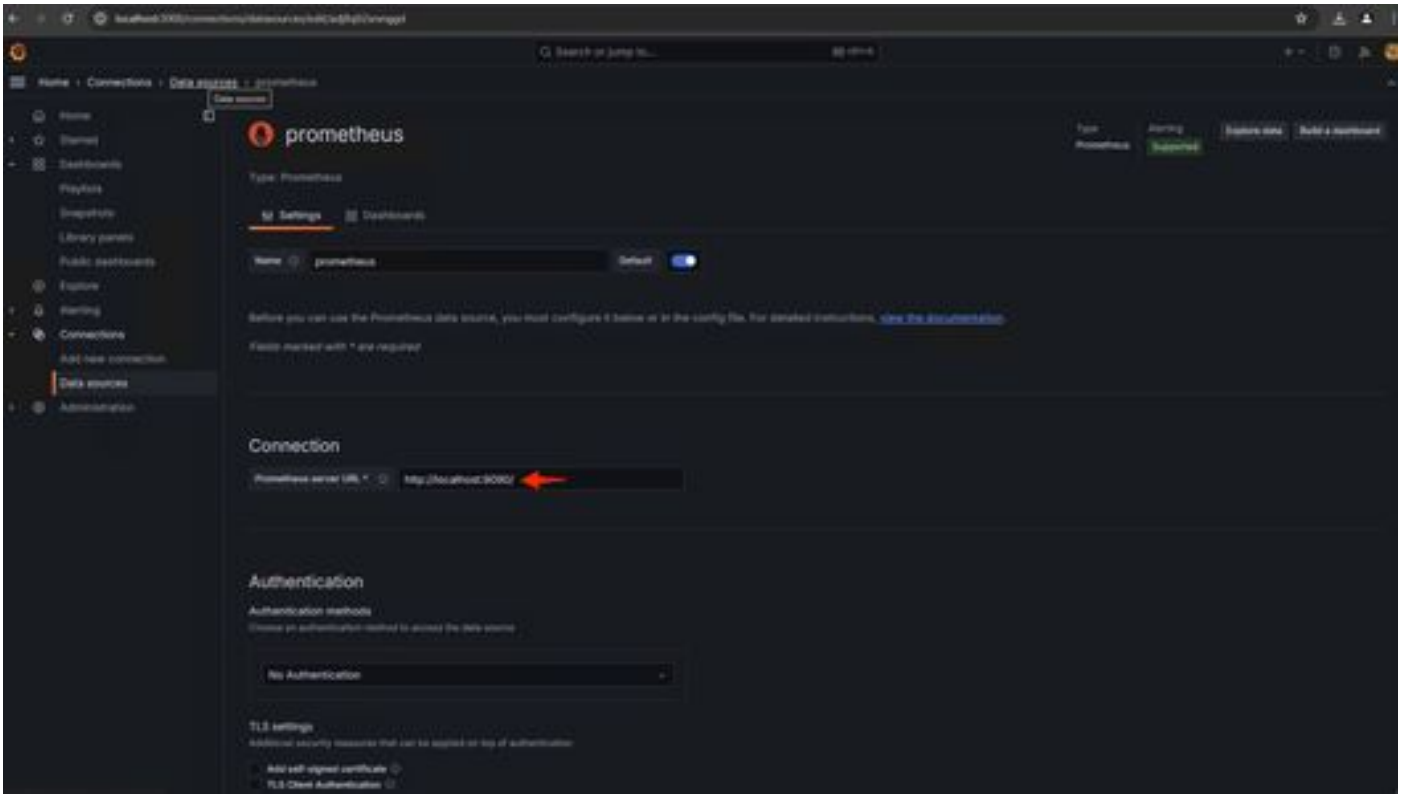
12. 安裝和配置Grafana

從Grafana Labs下載Grafana執行檔。 安裝Granafa，然後按照安裝程式提供的說明進行操作。

13. 在瀏覽器中安裝Grafana access UI之後-http://localhost:3000/

轉至Home > Connections > Data sources - 'http://localhost:3000/connections/datasources'

從清單中選擇增加新資料來源和SelectPrometheus。 輸入「http://localhost:9090/」作為Prometheus伺服器URL



在該頁底部選擇Save & test。測試成功後，我們可以建立儀表板。

14. 建立Grafana儀表板

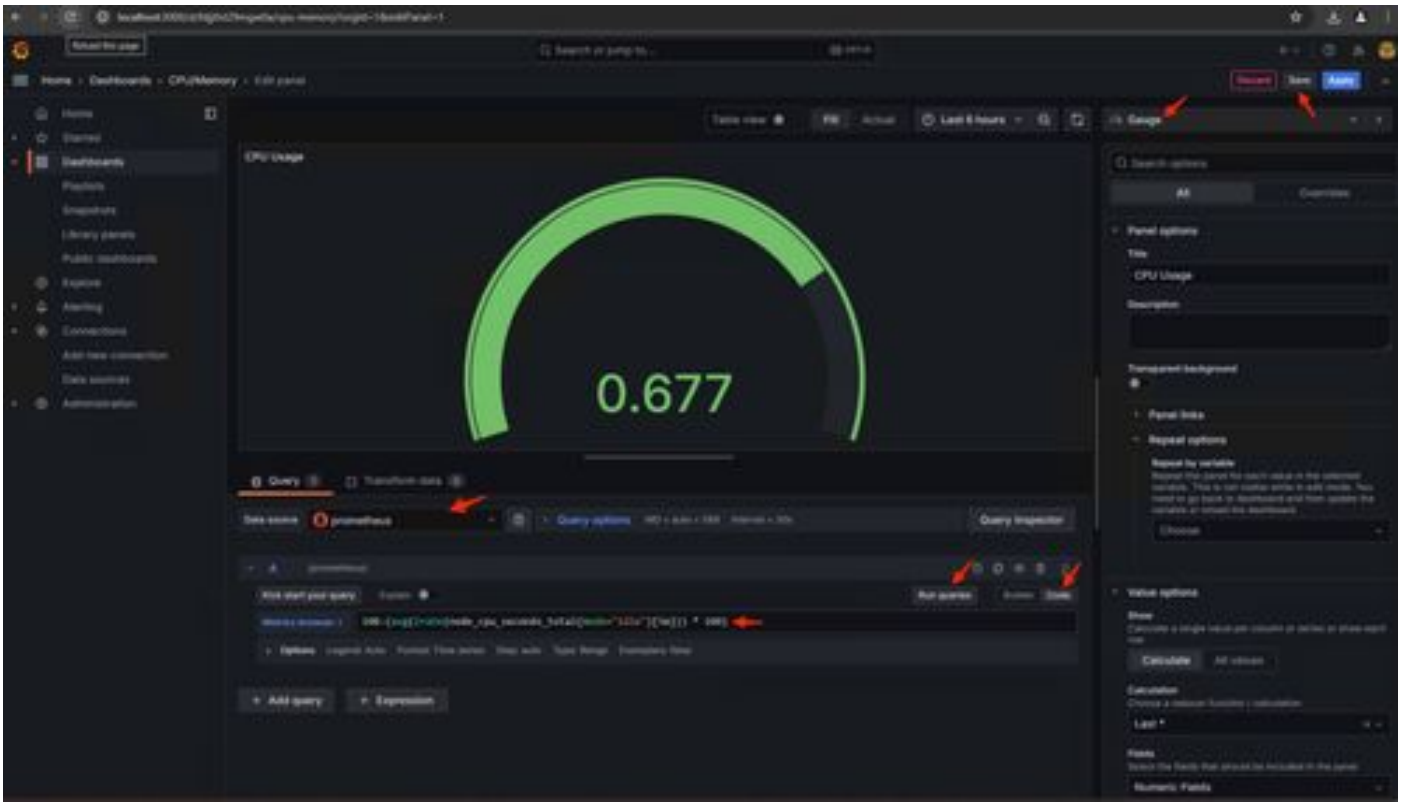
在Grafana UI中轉至控制台(SelectCreate Dashboard>增加視覺化)。選取Prometheus資料來源。

在查詢生成器中，選擇Codeinput，選擇視覺化型別（我選擇了儀表盤）

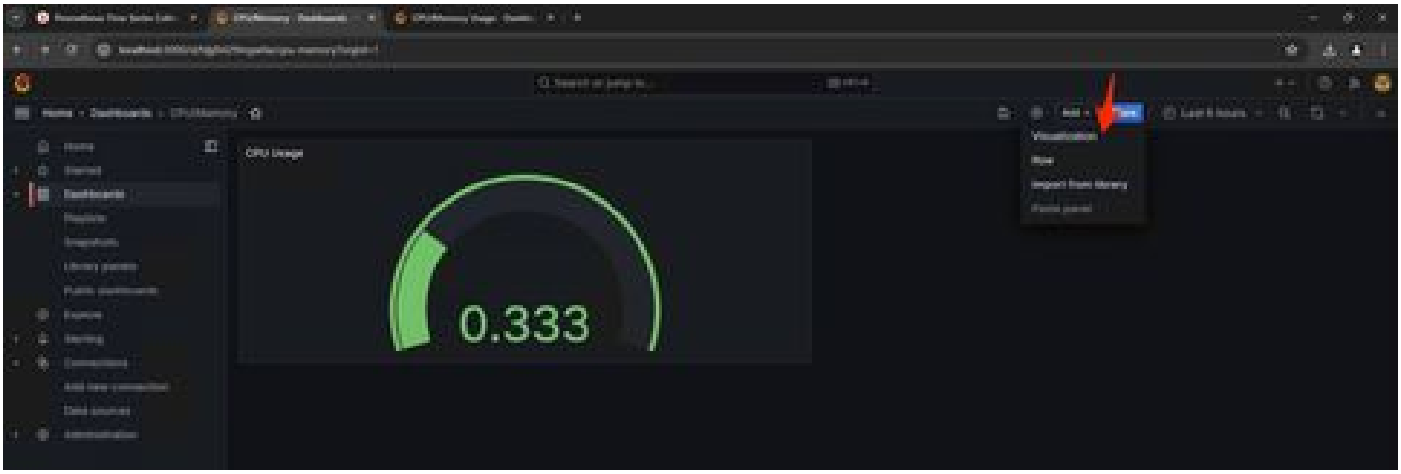
輸入以下查詢**CPU Utilization**-

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

15. 按一下Run 查詢，您應該會看到如下所示的CPU使用率視覺化-

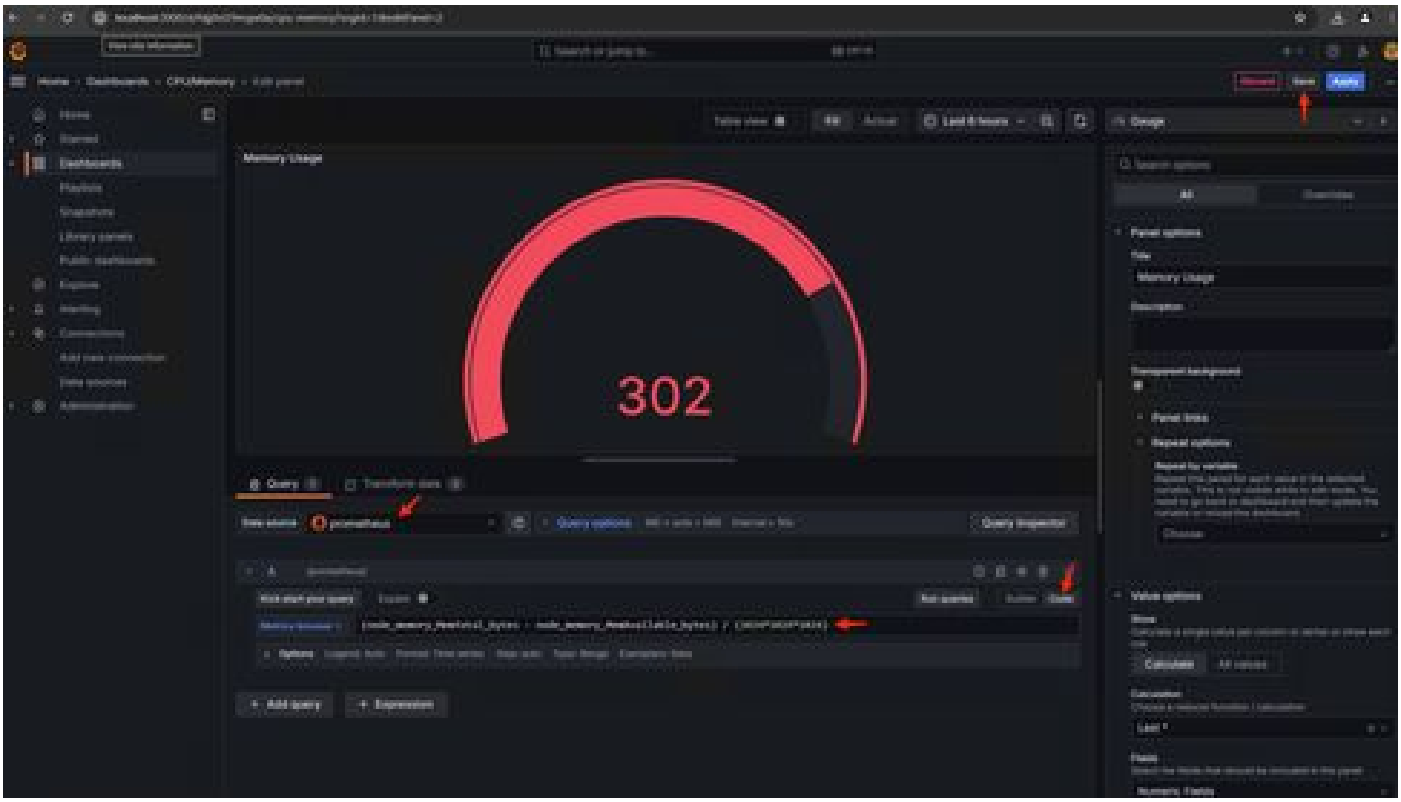


16. 儲存面板，命名圖示板，然後儲存。 增加另一個記憶體使用情況的視覺化-



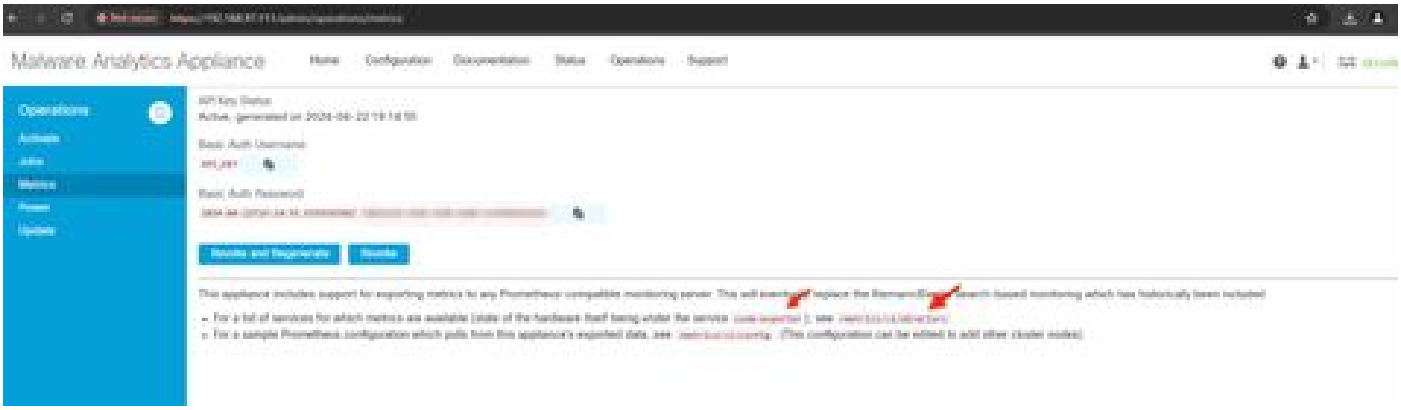
17. 針對記憶體使用率，請使用下列查詢

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



18. 儲存變更，您應該擁有如下的儀表板-

19. 還提供其他硬體和軟體度量。有關詳細資訊，請按一下Opadmin> Metrics頁中提供的連結

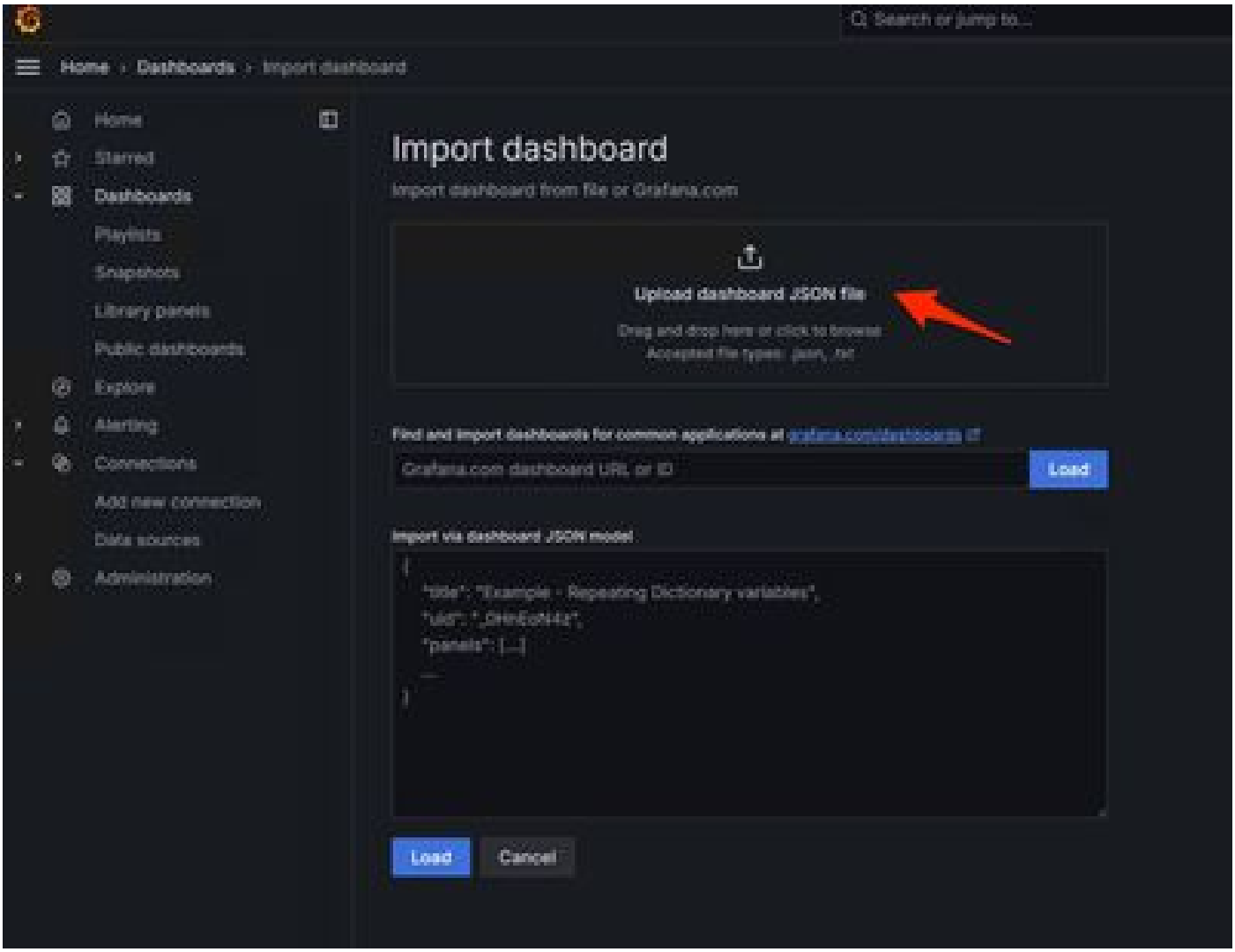


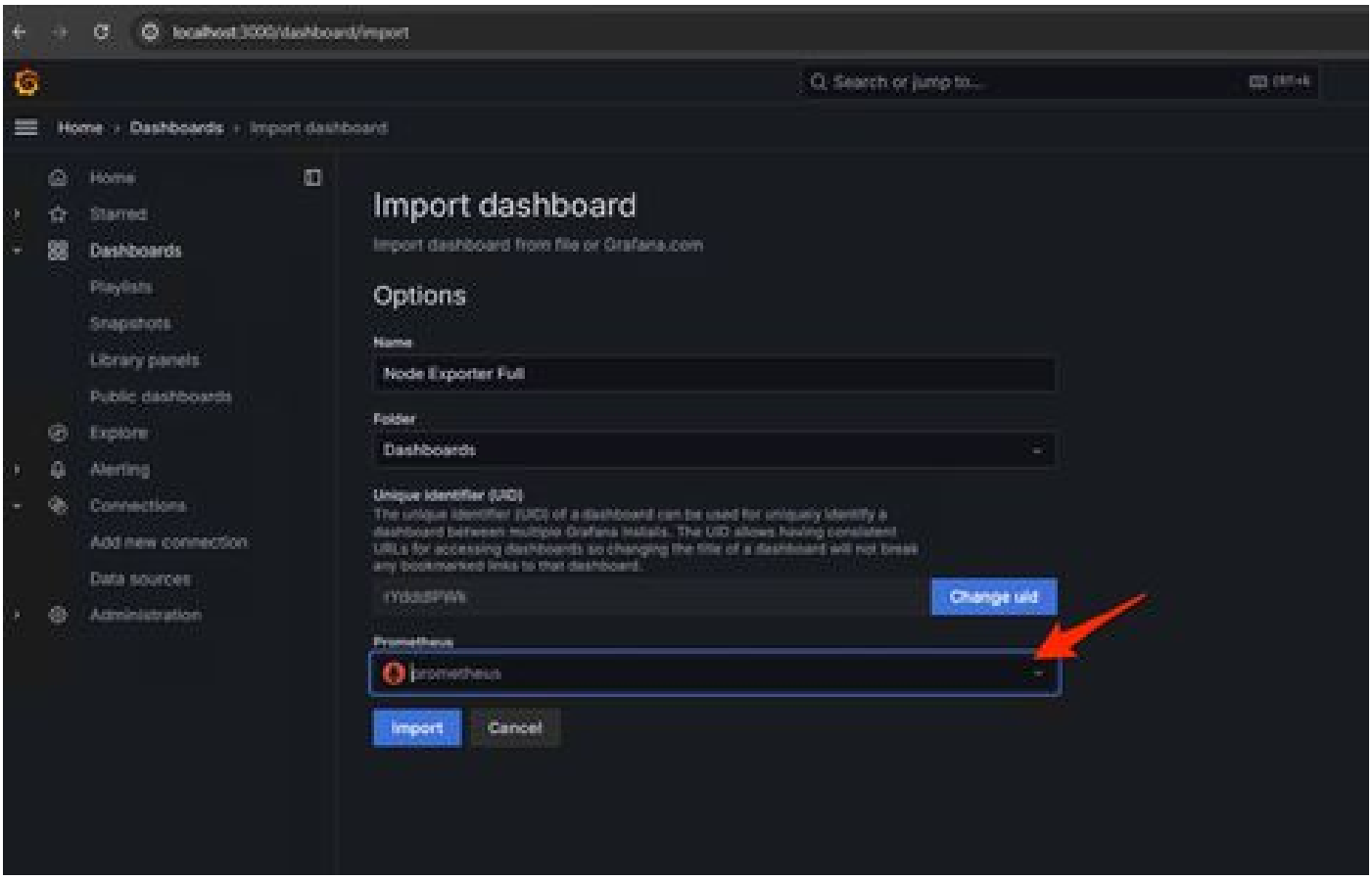
Grafana儀表板範本

Grafana網站上有許多Grafana Dashboard範本可供節點匯出程式使用。其中一個是-節點匯出程式已滿

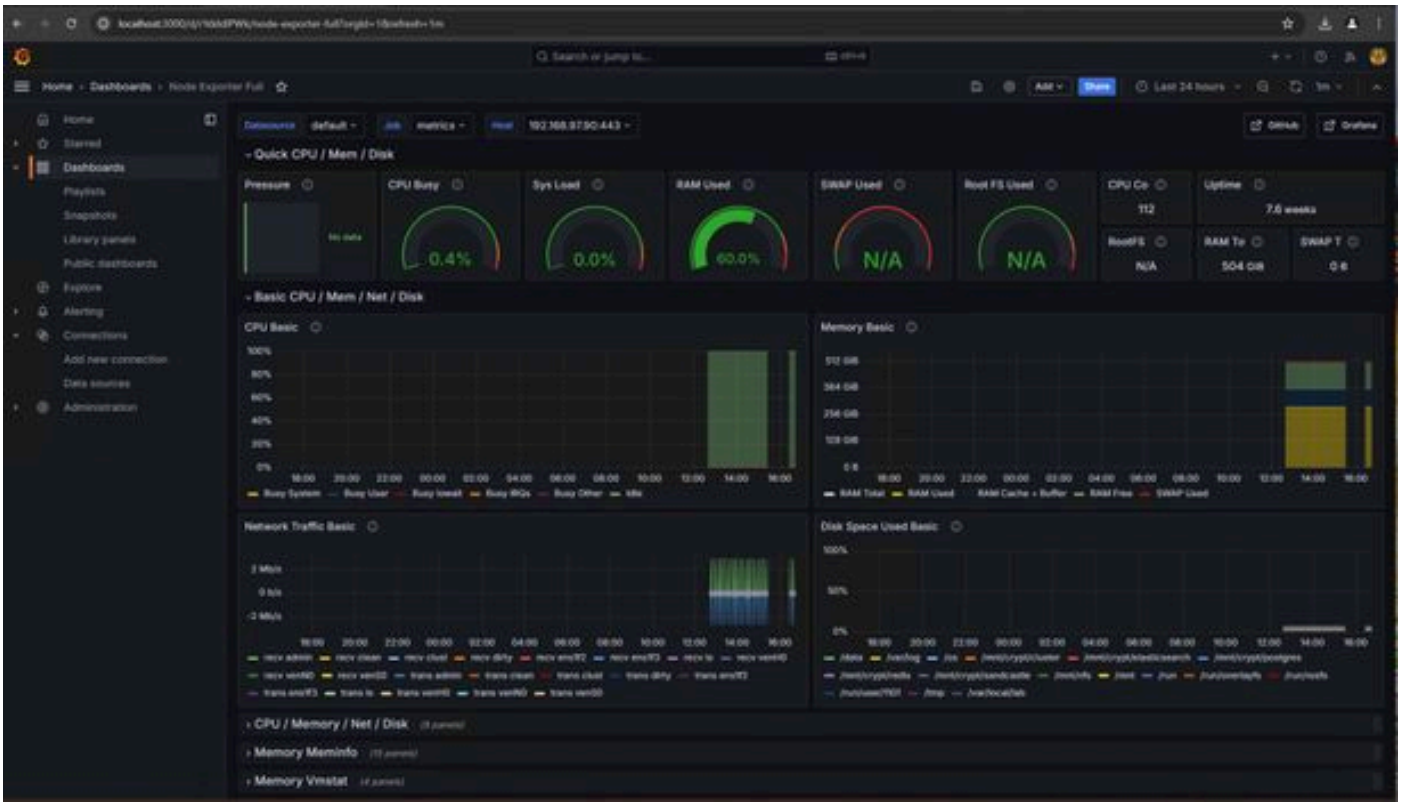
1. 要將此儀表板導入您的Grafana例項下載JSON，請導入Grafana中的JSON檔案

2. 上傳JSON檔案並選擇Prometheusdata source


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. 這將建立一個包含大量硬體資訊的儀表板（並非所有面板指標都可用）-



疑難排解

如果Prometheus未能從SMA裝置連線和提取度量，您將在`Status` > `Targets` -中看到此錯誤 http://localhost:9090/targets?search=

如果存在anyError，需要先修復此問題，然後才能提取資料。常見問題是SMA裝置的SSL證書Opadmin不受本地電腦信任。確保使用IP和DNS SAN建立SMA管理證書，並將簽名根CA增加到本地電腦的信任儲存中。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。