リモートのPrometheusおよびGrafanaを設定してSecure Malware Analytics（旧称Threat Grid）アプライアンスを監視する方法

内容

はじめに

セキュアマルウェア分析(SMA)アプライアンスでは、アプライアンスリソースの使用状況を監視するSNMPプロトコルは提供されず、アプライアンスがPrometheusを提供します。

このドキュメントでは、リモートのPrometheusインスタンスを設定し、アプライアンスから取得したデータをuseGrafanatoで視覚化する方法の概要を説明します。

前提条件

次のツールをダウンロードして、ローカルマシン/サーバにインストールします。

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

要件

- Secure Malware Analytics(SMA)アプライアンスソフトウェアバージョン2.18以降
- Windowsマシン
- アプライアンス管理者(Opadmin)コンソールへの管理者アクセス
- Secure Malware Analytics(SMA)アプライアンスOpadmin SSL証明書がローカルマシンで信頼されている

使用するコンポーネント

- セキュアマルウェア分析(SMA)アプライアンス
- Windows 11 Proマシン
- プロメテウス

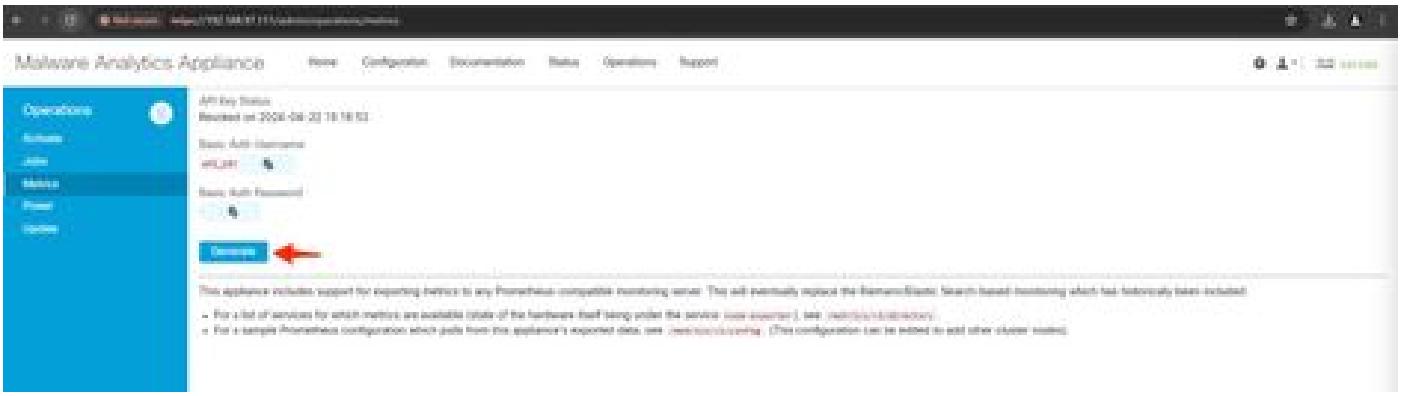
- グラファナ

設定

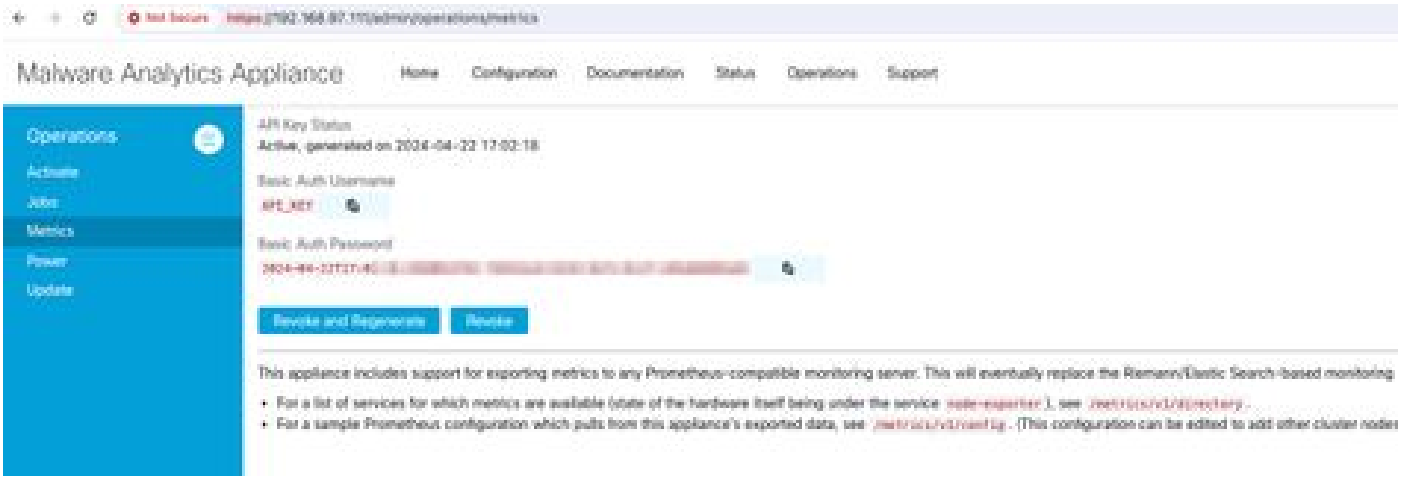
このドキュメントでは、Windows 11 Proをリモートホストとして使用し、PrometheusとGrafanaをインストールしました。これらのツールは、LinuxまたはMacOSでも使用できます。

1. メトリックにアクセスするためのSecure Malware Analytics(SMA)アプライアンスでのAPIキーの生成

SMAアプライアンスOpadminにログインします。 Opadmin > Operation > MetricsからメトリックのAPIキーを生成します。



2. Remote Prometheusの設定で使用する必要がある基本認証ユーザ名とパスワードが生成されます。



3. Prometheusのインストールと設定

LinuxまたはMacOSを使用している場合は、Prometheusのユーザーガイドの指示に従ってインスタンスをインストールします。このドキュメントでは、Windows 11マシンにPrometheusをインストールしました。インストールプロセスでは、このYoutubeビデオに従いました。

4. 次の内容で、`prometheus.yml`という名前の設定ファイルを作成します。

```
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. 「basic_auth」セクションで、手順1で生成したBasic Authのユーザ名とパスワードを使用します。

6. Opadminにログインした後、UIに次のように入力して、メトリックを取得できるサービスの設定を取得します。

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

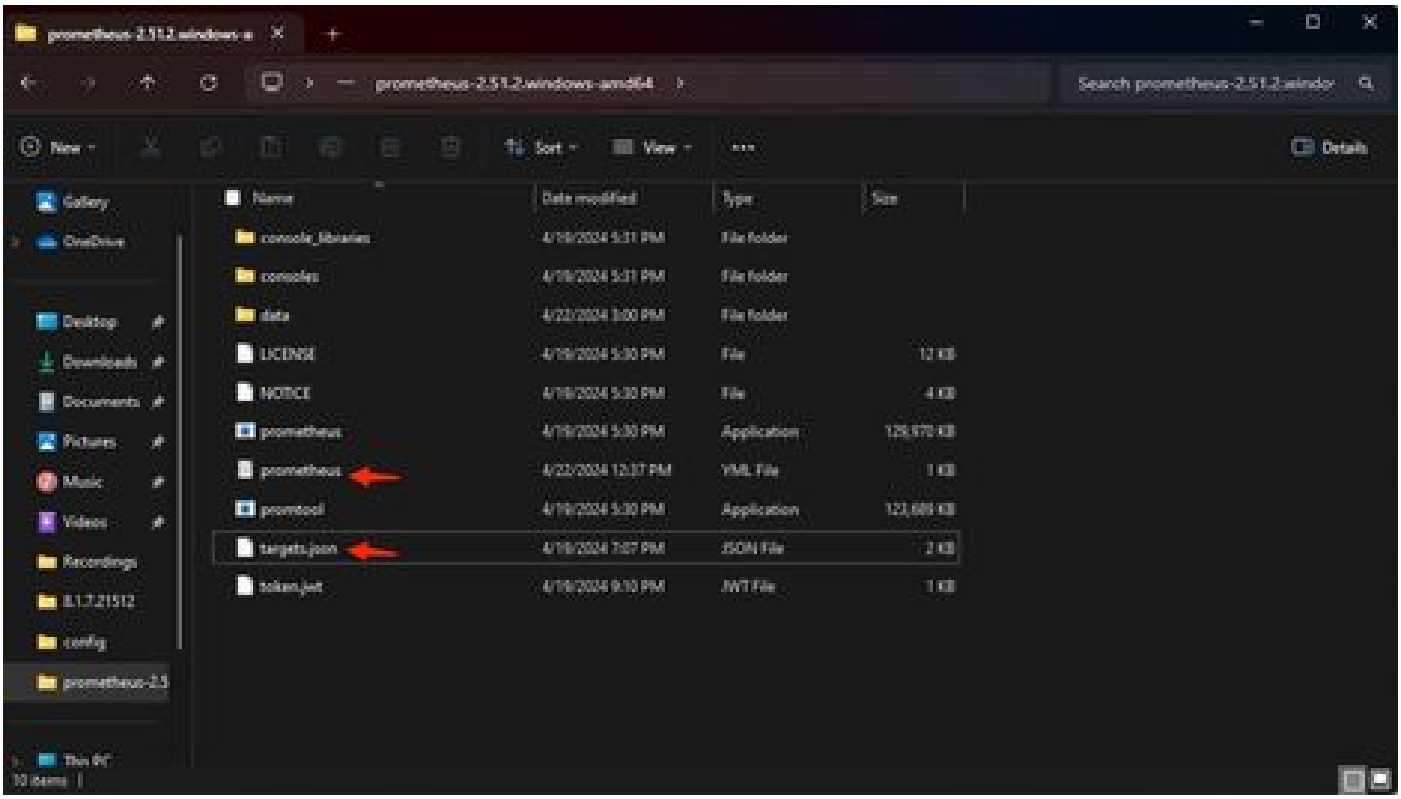
次のような結果になります

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

ここで、192.168.97.111はSMAアプライアンスの管理者IPです。

7.targets.jsonという名前のファイルを作成し、上記のコンテンツをそのファイルにコピーします。

8. prometheus.ymlとtargets.jsonをPrometheusディレクトリにコピーします（インストールガイドに従います）。Windowsの場合、C:\ドライブにフォルダを作成し、そこにPrometheusインストールファイルを抽出しました。次に、prometheus.ymlとtargets.jsonを同じフォルダにコピーします。



9. Prometheusを起動します

Prometheusを起動します。Windowsの場合、コマンドラインから`prometheus.exe`を実行します。

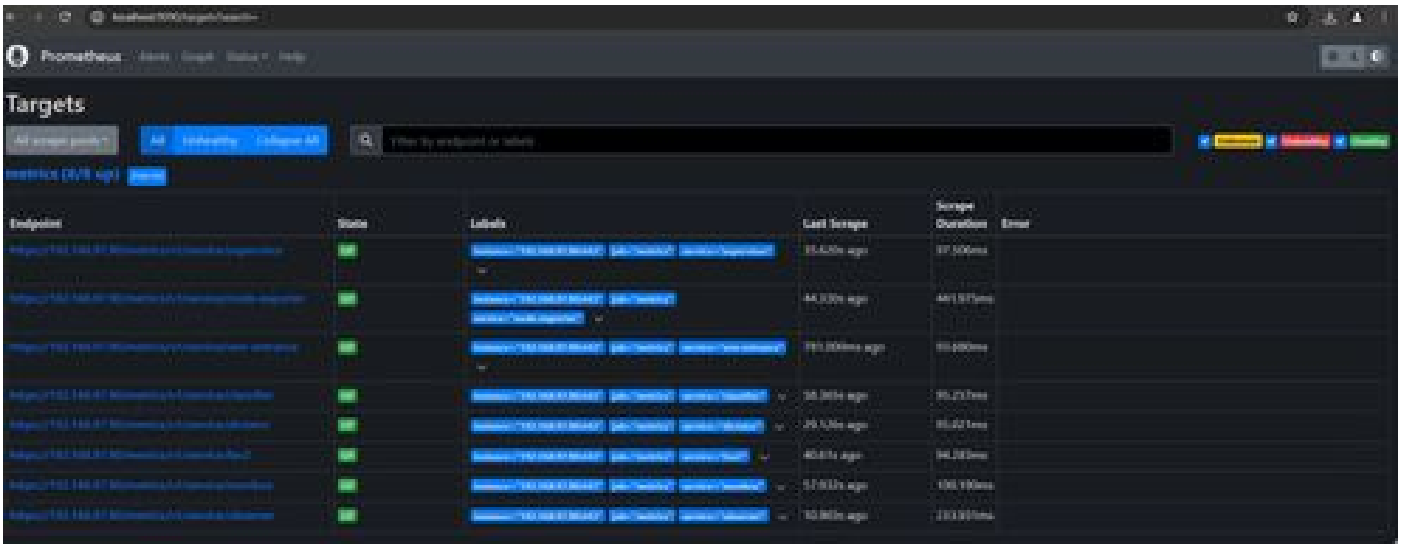
```
C:\Prometheus\prometheus-2.51.2.windows-amd64\prometheus-2.51.2.windows-amd64>prometheus.exe
```

これにより、Prometheusが起動し、SMAアプライアンスからのメトリックの取得が開始されます。注：コマンドラインを閉じないでください。閉じると、Prometheusがシャットダウンします。

10. ローカルのPrometheusインスタンスがSMAアプライアンスからメトリックをプルできるかどうかを確認するには、Prometheus UI - 'http://localhost:9090/'をロードします

11. `Status` > `Targets`の順に移動します – http://localhost:9090/targets?search=

数分以内に、すべてのターゲットとステータスUPが表示されます。



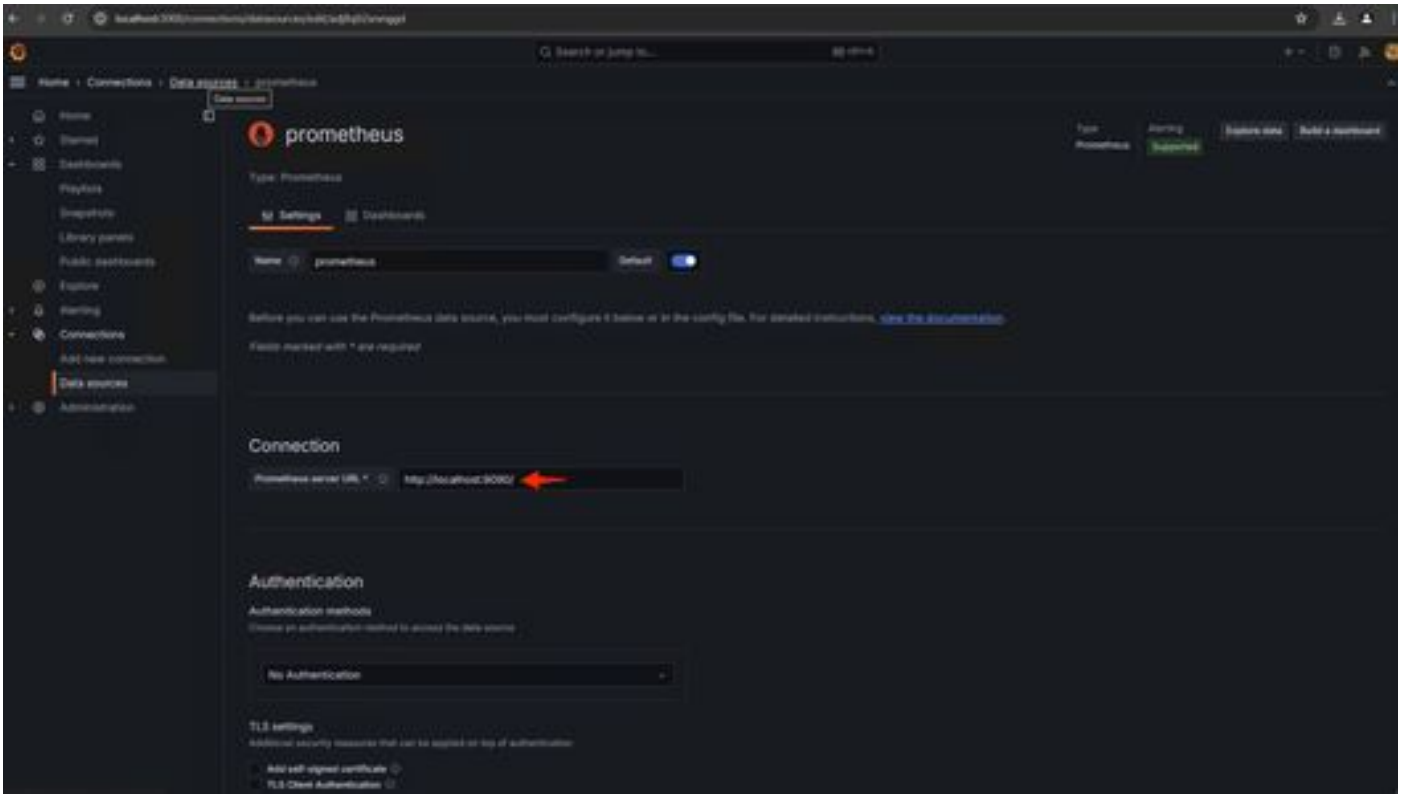
12. Grafanaのインストールと設定

Grafana LabsからGrafana実行可能ファイルをダウンロードします。 Granafaをインストールし、インストーラの指示に従います。

13. ブラウザにGrafanaアクセスUIをインストールした後 – http://localhost:3000/

Home > **Connections** > **Data sources** - '**http://localhost:3000/connections/datasources**'の順に移動します。

リストからAdd New DatasourceとSelectPrometheusを選択します。 PrometheusサーバURLとして「http://localhost:9090/」を入力します



ページの下部で、Save & testを選択します。テストが成功したら、ダッシュボードを作成できます。

14. Grafanaダッシュボードの作成

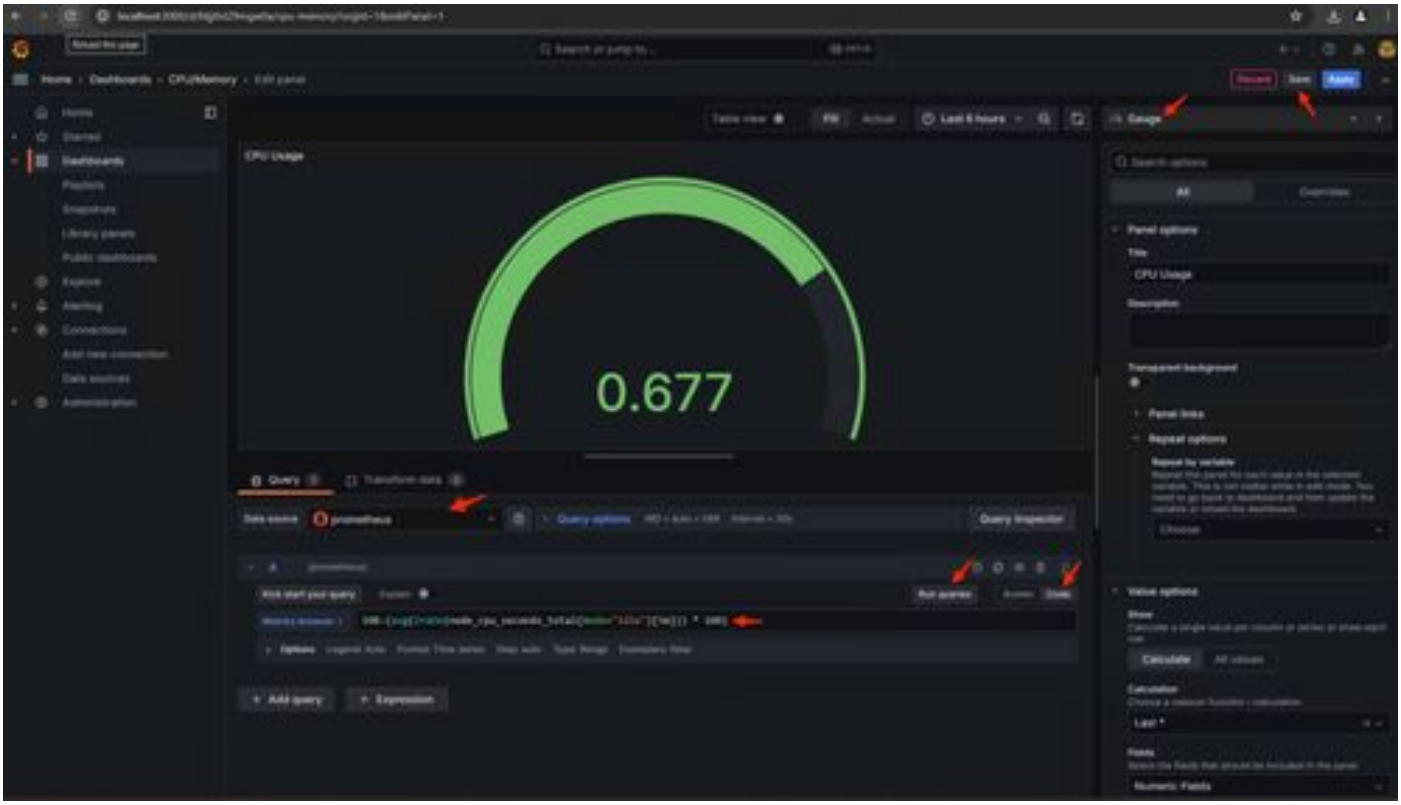
Grafana UIのDashboardsに移動し、Create Dashboard>Add visulizationを選択します。SelectPrometheusデータソース。

クエリー・ビルダーselectCodeinputで、視覚化のタイプを選択します (ゲージを選択) 。

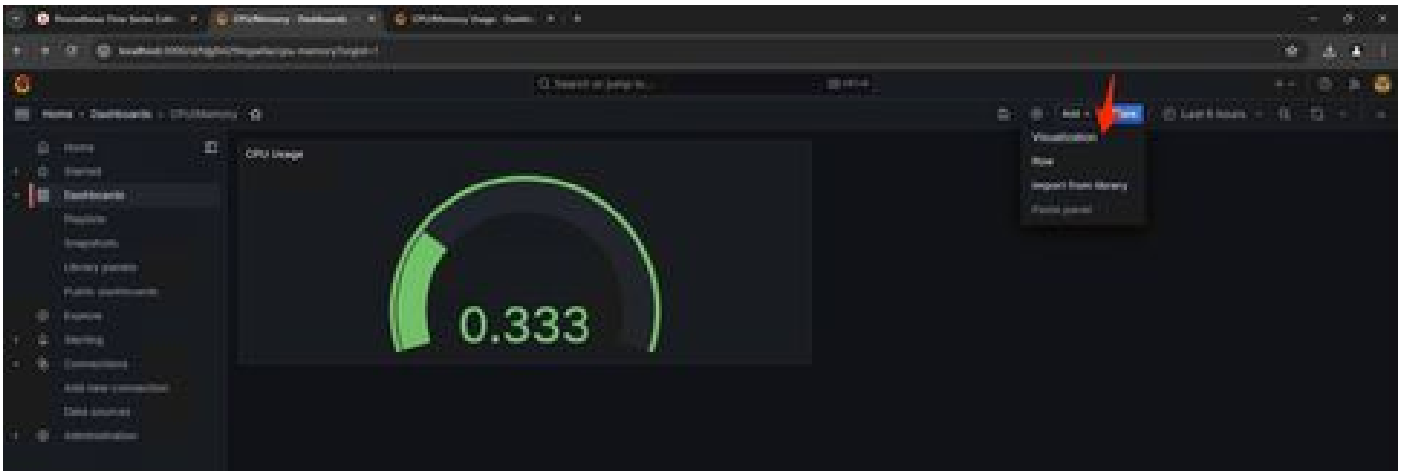
CPU使用率に関する次のクエリを入力します。

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

15. Run Queriesandをクリックすると、次のようなCPU使用率の視覚化が表示されます。

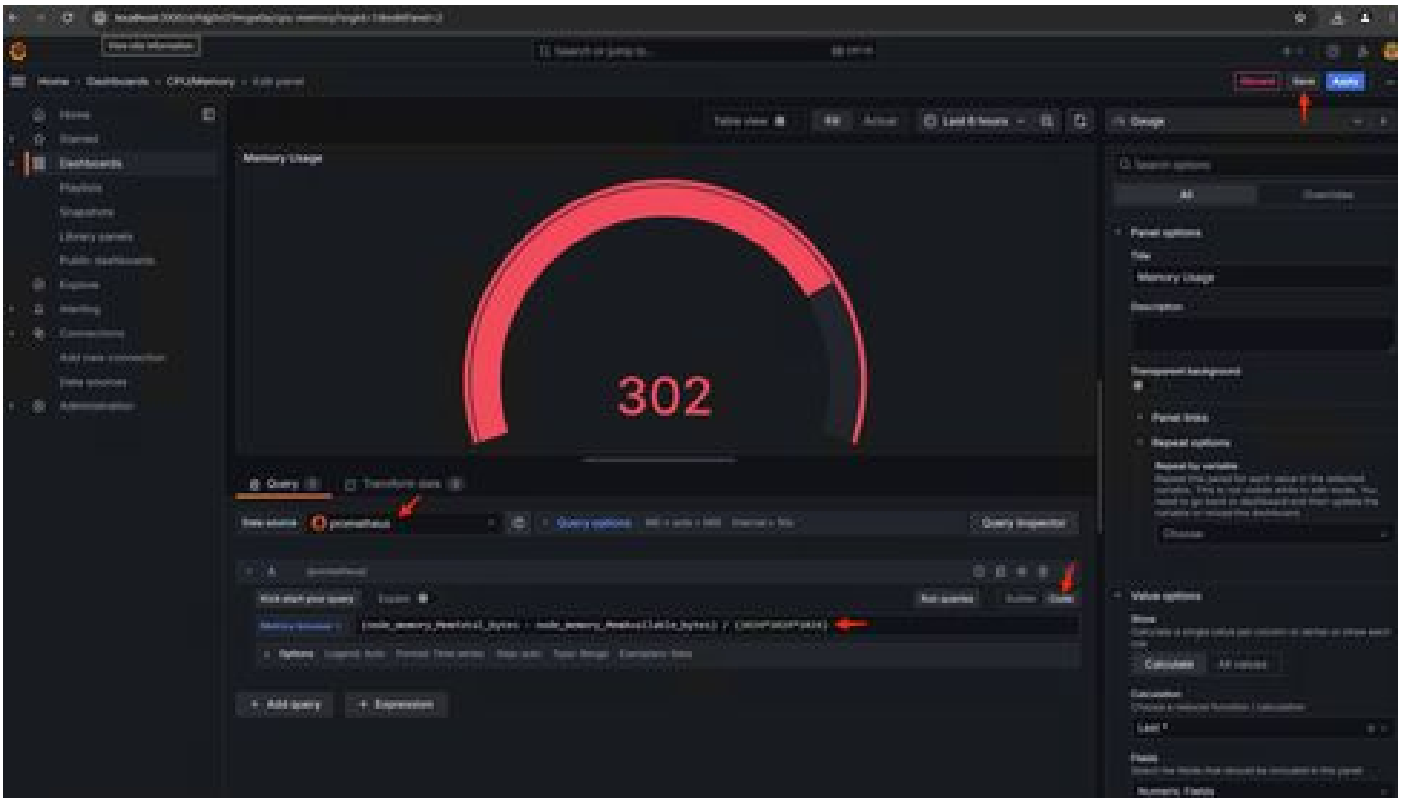


16. パネルを保存し、ダッシュボードに名前を付けて「保存」をクリックします。 メモリ使用量の別の可視化の追加：



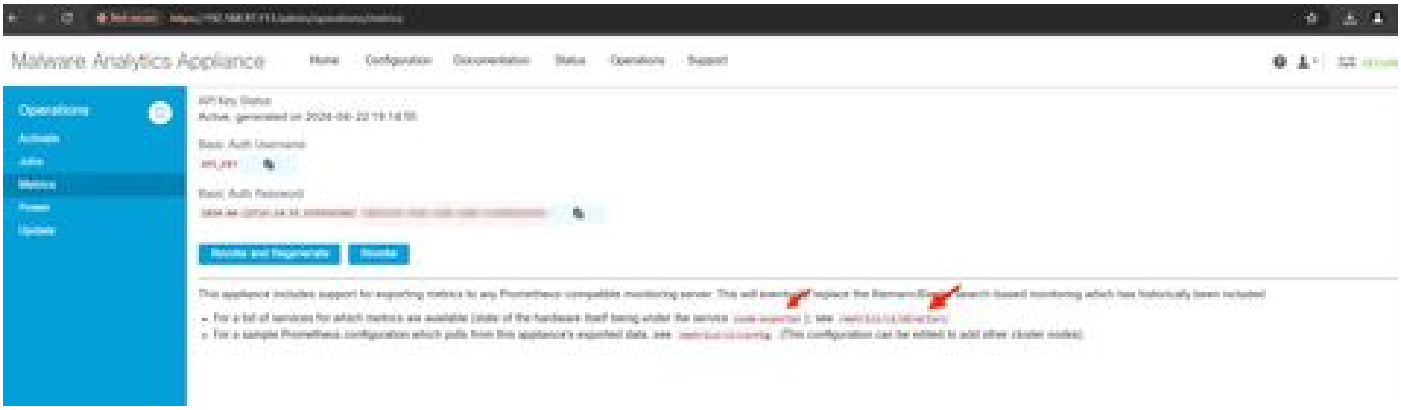
17. メモリー使用率については、次の問合せを使用します

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



18. 変更を保存すると、次のようなダッシュボードが表示されます。

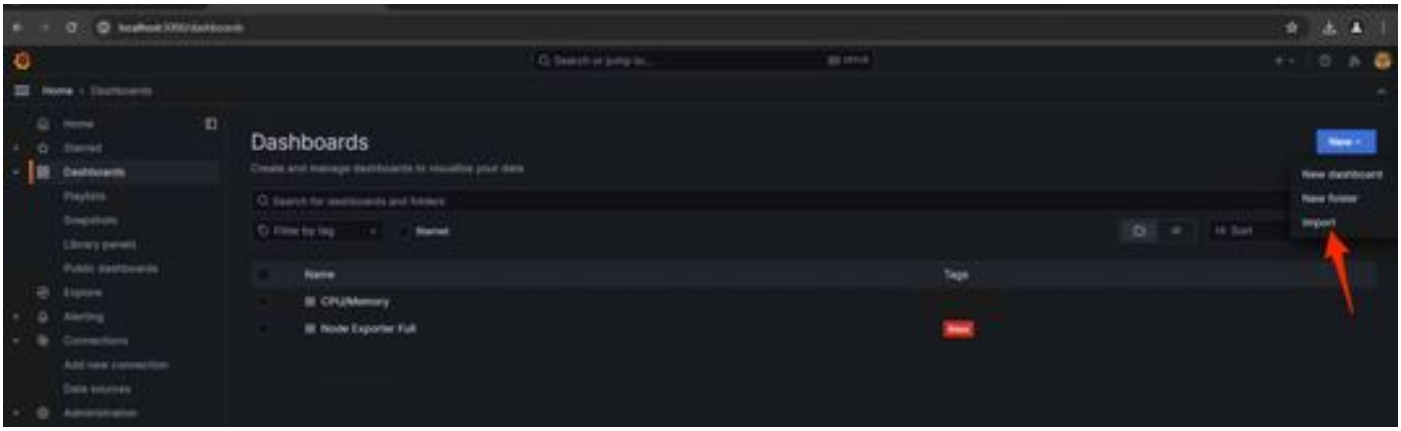
19. その他のハードウェアおよびソフトウェアのメトリックも表示されます。詳細については、Opadmin> Metricsページにあるリンクをクリックしてください。



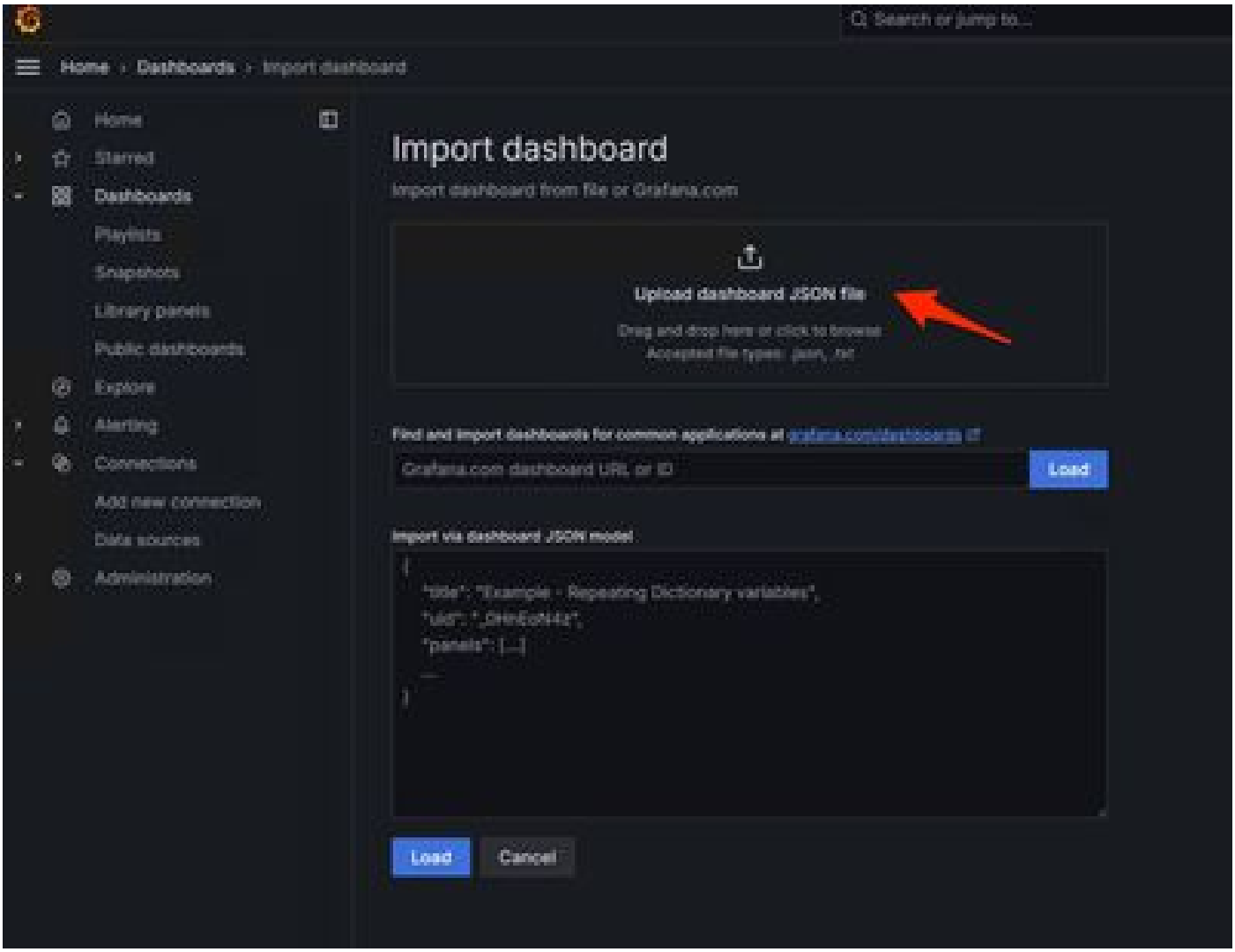
Grafanaダッシュボードテンプレート

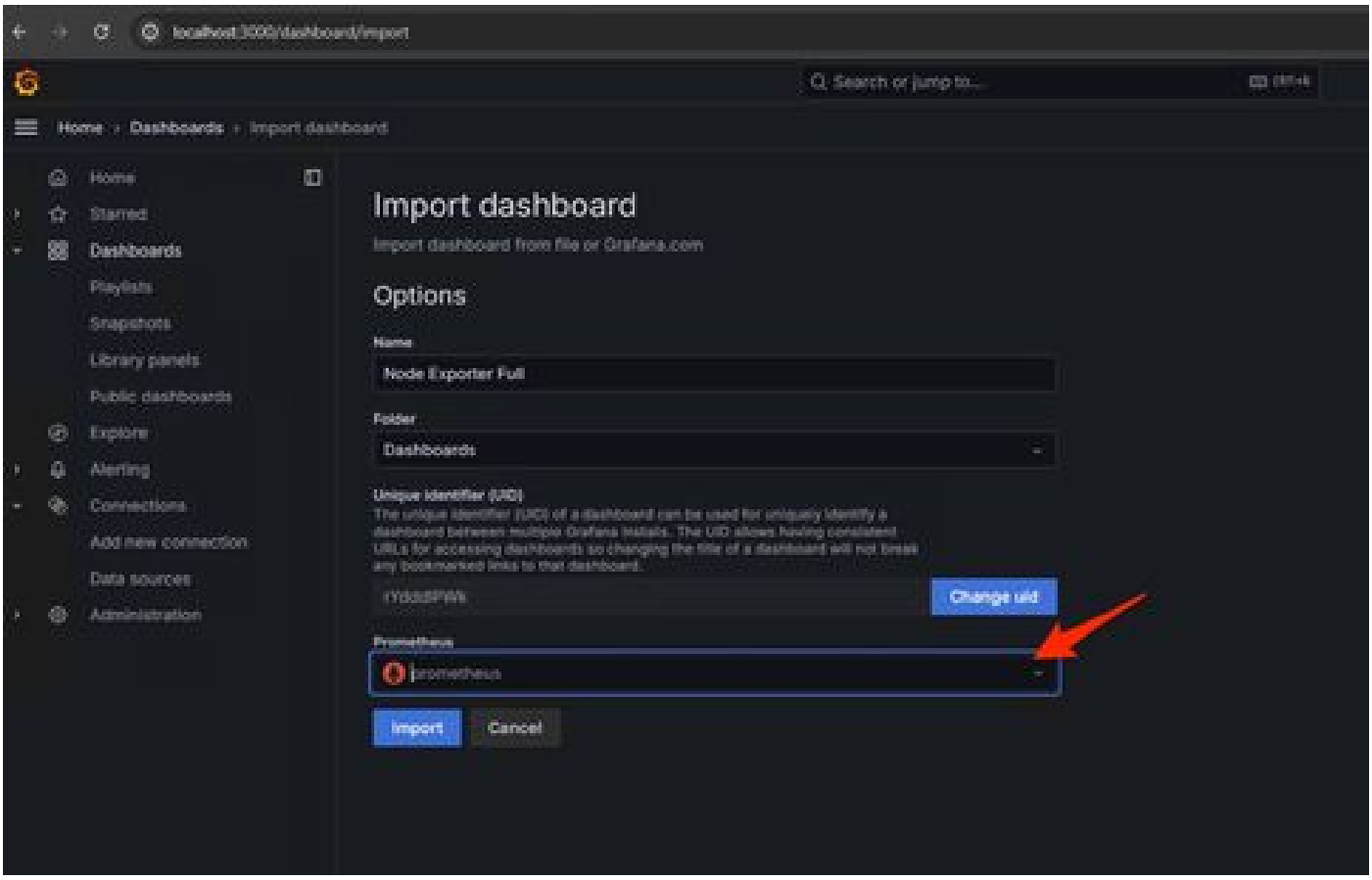
Grafana Webサイトのノードエクスポータでは、多数のGrafanaダッシュボードテンプレートを使用できます。そのうちの1つは、「ノードエクスポータがいっぱいです」

1. このダッシュボードをGrafanaインスタンスにインポートするにはJSONをダウンロードし、GrafanaにJSONファイルをインポートします

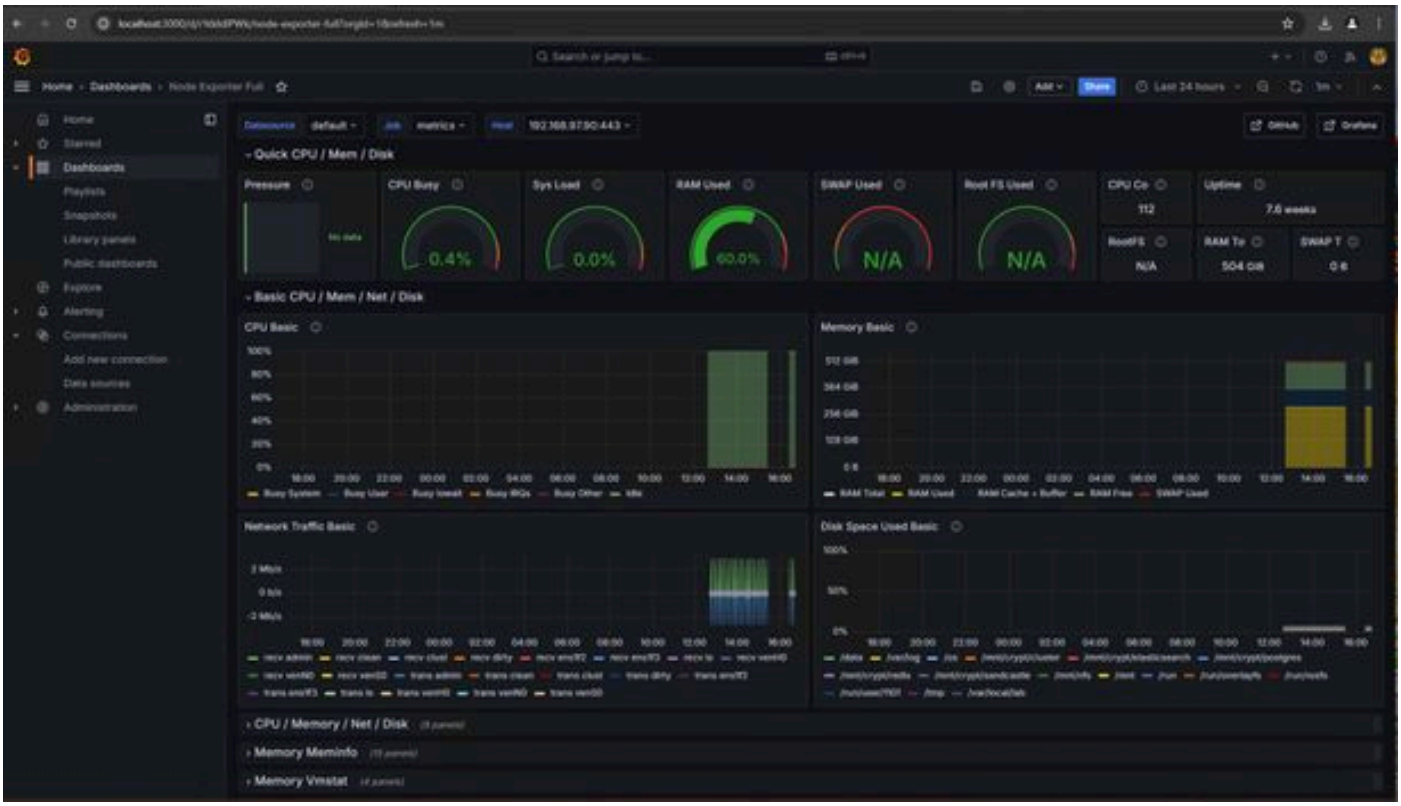


2. JSONファイルをアップロードし、Prometheusdataソースを選択します


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. これにより、多くのハードウェア情報を含むダッシュボードが作成されます（すべてのパネルメトリックを使用できるわけではありません）。



トラブルシュート

Prometheusが接続に失敗し、SMAアプライアンスからメトリックを取得できなかった場合、Status > Targetsにエラーが表示されます。 http://localhost:9090/targets?search=

anyErrorが存在する場合、データをプルする前にそれを修正する必要があります。一般的な問題は、SMAアプライアンスOpadminのSSL証明書が口ーカルマシンで信頼されていないことです。IPおよびDNS SANを使用してSMA管理証明書を作成し、署名ルートCAを口ーカルマシンの信頼ストアに追加します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。