Comment configurer Prometheus et Grafana pour surveiller l'appliance Secure Malware Analytics (anciennement Threat Grid)

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

Modèle de tableau de bord Grafana

Dépannage

Introduction

Dans l'appliance Secure Malware Analytics (SMA), nous n'offrons pas de protocole SNMP pour surveiller l'utilisation des ressources de l'appliance, mais l'appliance offre Prometheus.

Ce document explique comment configurer une instance distante de Prometheus et utiliser Grafanpour visualiser les données extraites de l'appliance.

Conditions préalables

Téléchargez et installez les outils suivants sur votre machine/serveur local :

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

Exigences

- Logiciel Secure Malware Analytics (SMA) Appliance Version 2.18 et ultérieure
- Machine Windows
- Accès administrateur à la console Appliance Admin(Opadmin)
- Certificat SSL d'administrateur d'appliance Secure Malware Analytics (SMA) approuvé par la machine locale

Composants utilisés

- Appareil Secure Malware Analytics (SMA)
- ordinateur Windows 11 Professionnel
- Prométhée

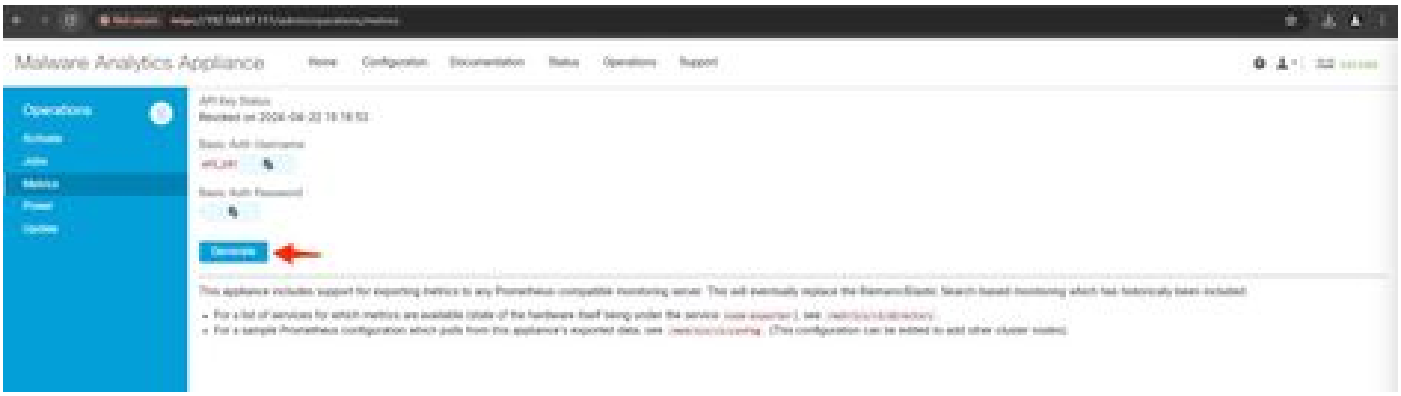
- Grafana

Configurer

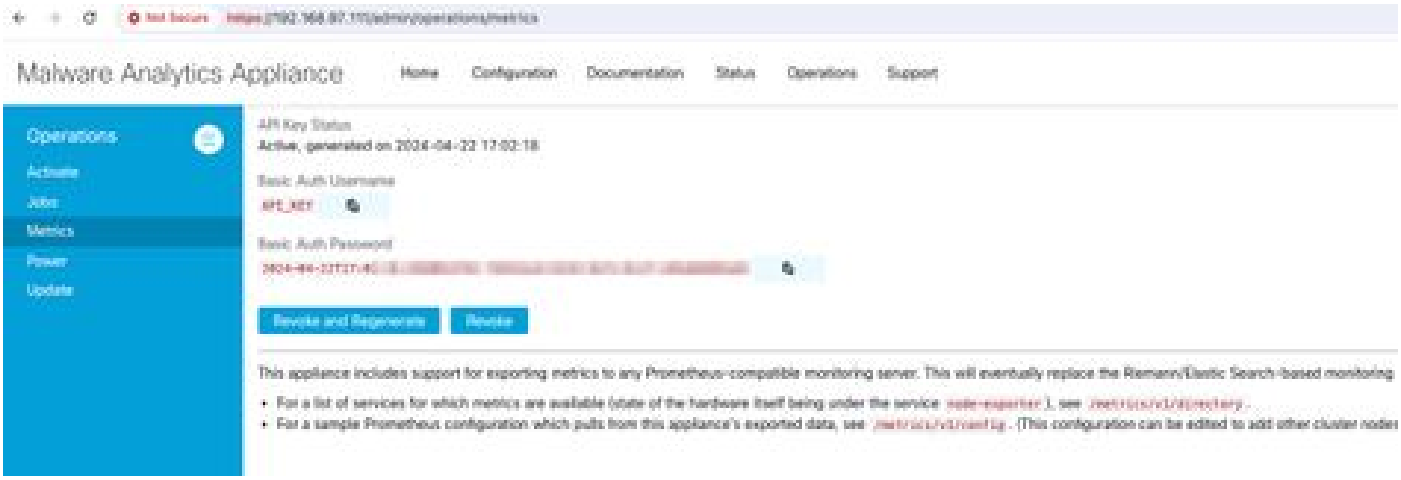
Pour ce document, Nous avons utilisé un Windows 11 Pro comme hôte distant où nous avons installé Prometheus et Grafana. Ces outils sont également disponibles pour Linux ou MacOS.

1. Générer une clé API dans l'appliance Secure Malware Analytics (SMA) pour accéder aux mesures

Connectez-vous à Appliance SMA Opadmin. Générez la clé API pour les mesures à partir de Opadmin > Operation > Metrics



2. Un nom d'utilisateur et un mot de passe d'authentification de base seront générés et devront être utilisés dans la configuration de Prometheus à distance.



3. Installation et configuration de Prometheus

Suivez les instructions fournies par les guides de l'utilisateur Prometheus pour installer votre instance si vous utilisez Linux ou MacOS. Pour ce document, nous avons installé Prometheus sur une machine Windows 11, et pour le processus d'installation, nous avons suivi cette vidéo Youtube.

4. Créez un fichier de configuration nommé `prometheus.yml` avec le contenu suivant :

```
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. dans la section `basic_auth`, utilisez le nom d'utilisateur et le mot de passe d'authentification de base générés à l'étape 1.

6. Extrayez la configuration des services à partir desquels vous pourrez extraire des mesures en entrant les éléments suivants dans l'interface utilisateur après vous être connecté à Opadmin -

```
https://

       /metrics/v1/config
```

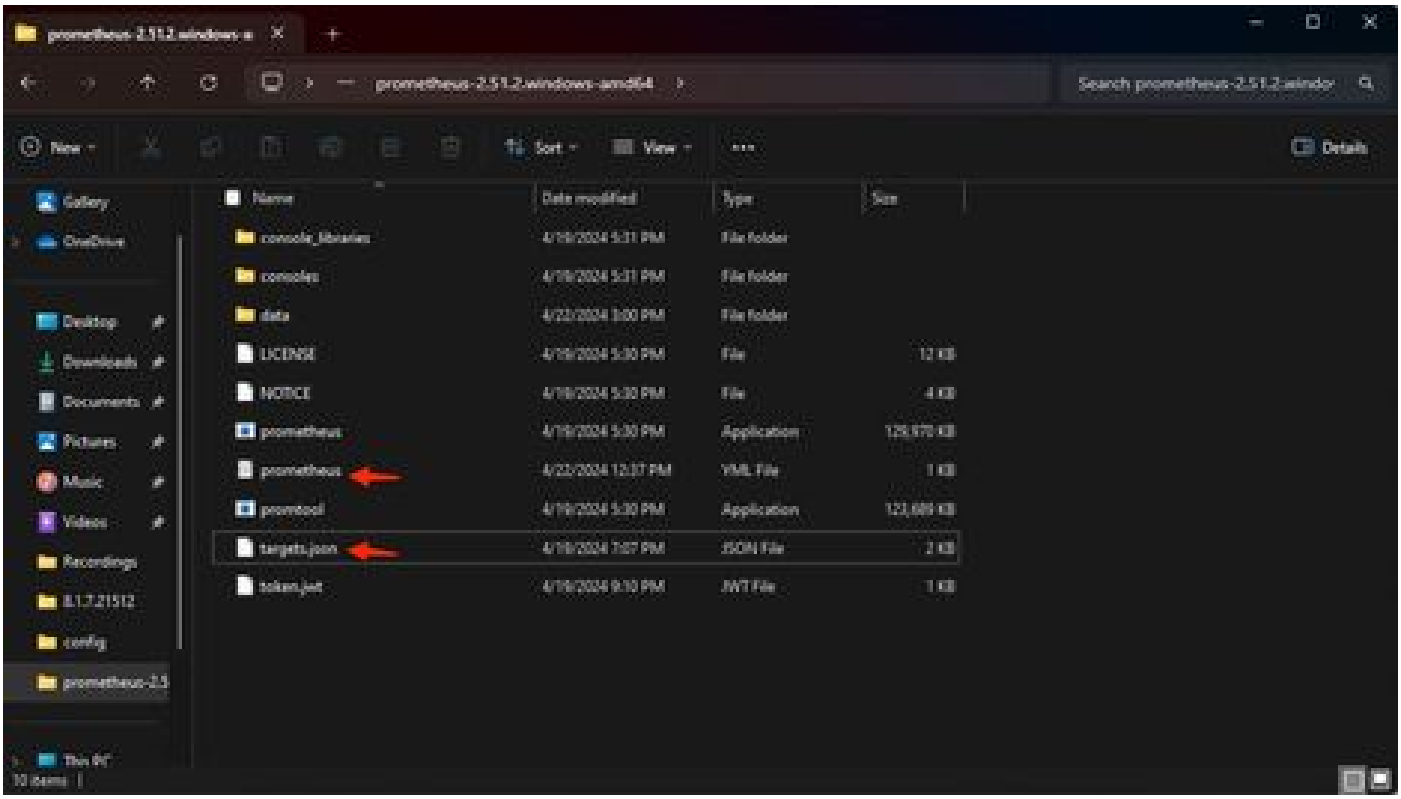
Vous obtiendrez quelque chose comme -

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

Ici `192.168.97.111` est l'adresse IP d'administration de mon appareil SMA.

7. Créez un fichier portant le nom `cibles.json` et copiez le contenu ci-dessus dans ce fichier.

8. Copiez `prometheus.yml` et `cibles.json` dans le répertoire Prometheus (suivez les guides d'installation). Pour Windows, j'ai créé un dossier dans le lecteur C:\ et j'y ai extrait les fichiers d'installation de Prometheus. Copiez ensuite `prometheus.yml` et `cibles.json` dans ce même dossier.



9. Démarrer Prometheus

Lancez Prometheus. Pour Windows, exécutez `prometheus.exe` à partir de la ligne de commande.

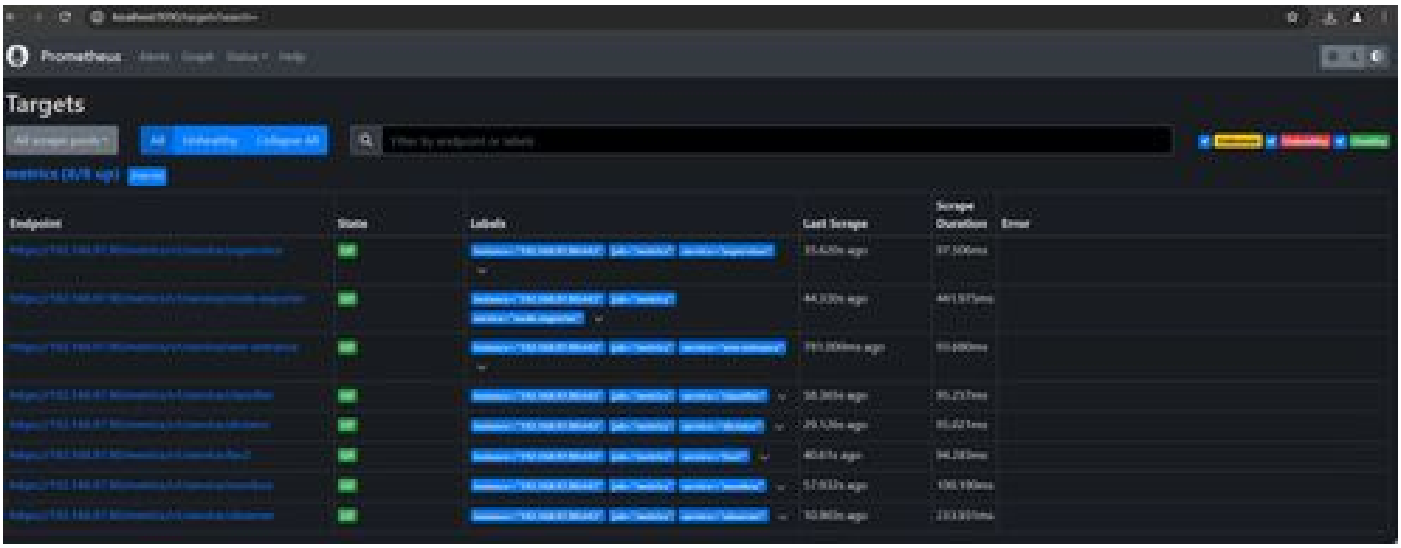
```
C:\Prometheus\prometheus-2.51.2.windows-amd64\prometheus-2.51.2.windows-amd64>prometheus.exe
```

Cette opération démarre le Prometheus et commence à extraire les mesures de l'appliance SMA. Remarque : Ne fermez pas la ligne de commande, sinon Prometheus s'arrêtera.

10. Pour vérifier si votre instance Prometheus locale est en mesure d'extraire la mesure de l'interface utilisateur Prometheus de chargement de l'appliance SMA - `http://localhost:9090/`

11. Accédez à `État` > `Cibles` - http://localhost:9090/targets?search=

Dans quelques minutes, vous devriez voir toutes les cibles et l'état `UP` .



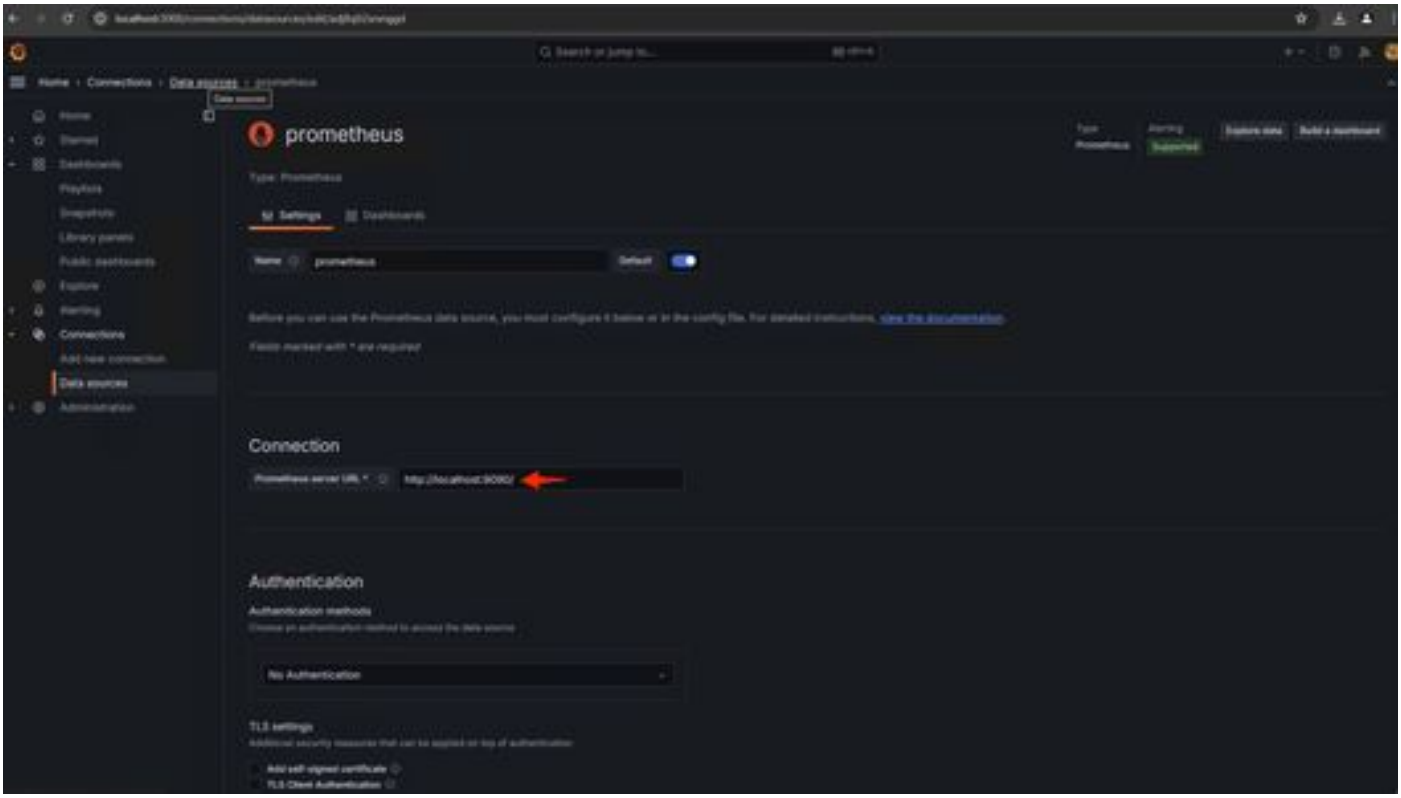
12. Installation et configuration de Grafana

Téléchargez l'exécutable de Grafana à partir de Grafana Labs. Installez Granafa et suivez les instructions fournies par l'installateur.

13. Après avoir installé l'interface utilisateur d'accès Grafana dans le navigateur - `http://localhost:3000/`

Accédez à Accueil > Connexions > Sources de données - `http://localhost:3000/connections/datasources`

`Sélectionnez Ajouter une nouvelle source de données` et `SélectionnerPrometheus` dans la liste. Entrez l'adresse `http://localhost:9090/` comme URL du serveur Prometheus



Au bas de cette page, `sélectionnezEnregistrer et tester`. Après un test réussi, nous pouvons créer un tableau de bord.

14. Créer un tableau de bord Grafana

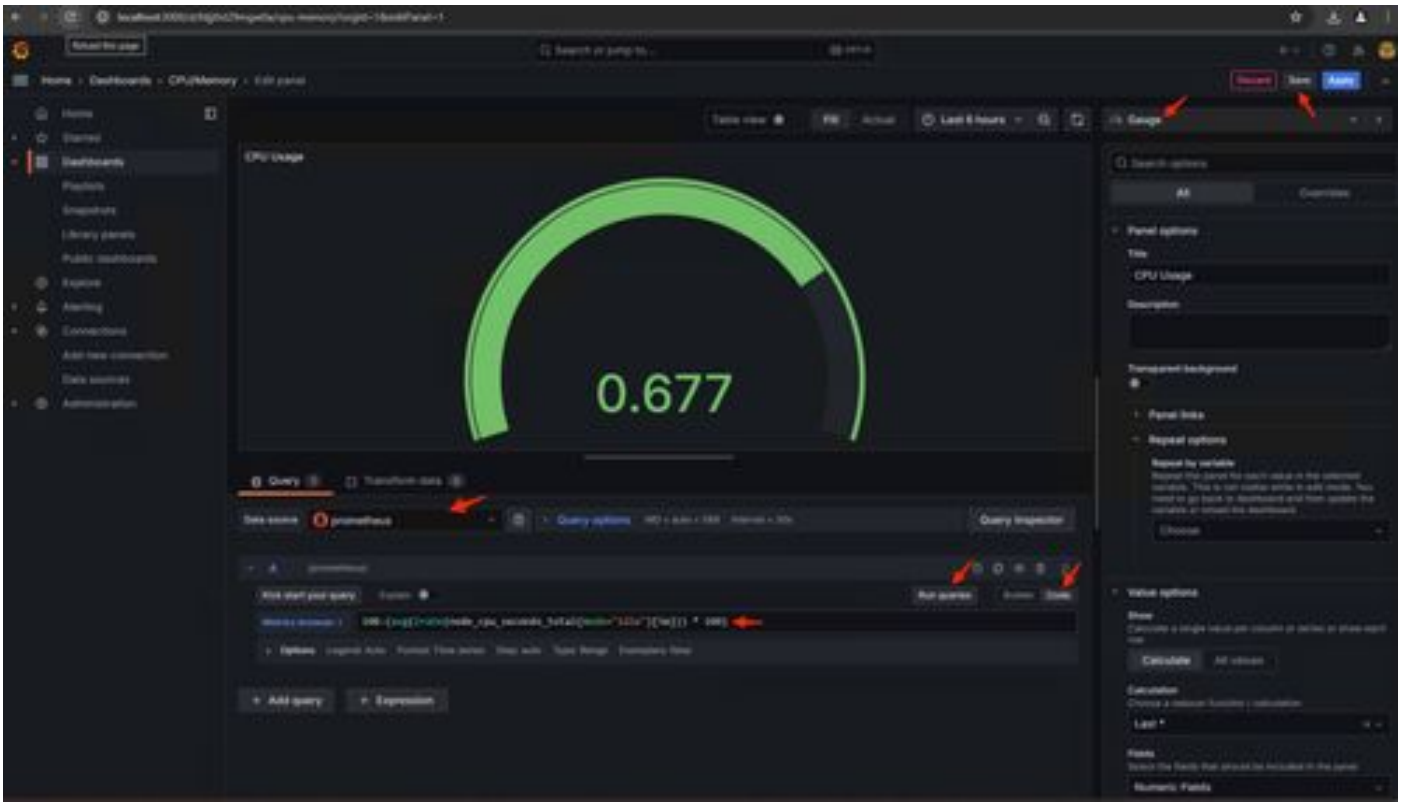
Accédez `à Tableaux de bord` dans Grafana UI , `SélectionnezCréer un tableau de bord>Ajouter une visualisation. Sélectionnez` Source de données Prometheus.

Dans le Générateur de requêtes selectCodeinput, sélectionnez Type de visualisation (j'ai sélectionné Jauge)

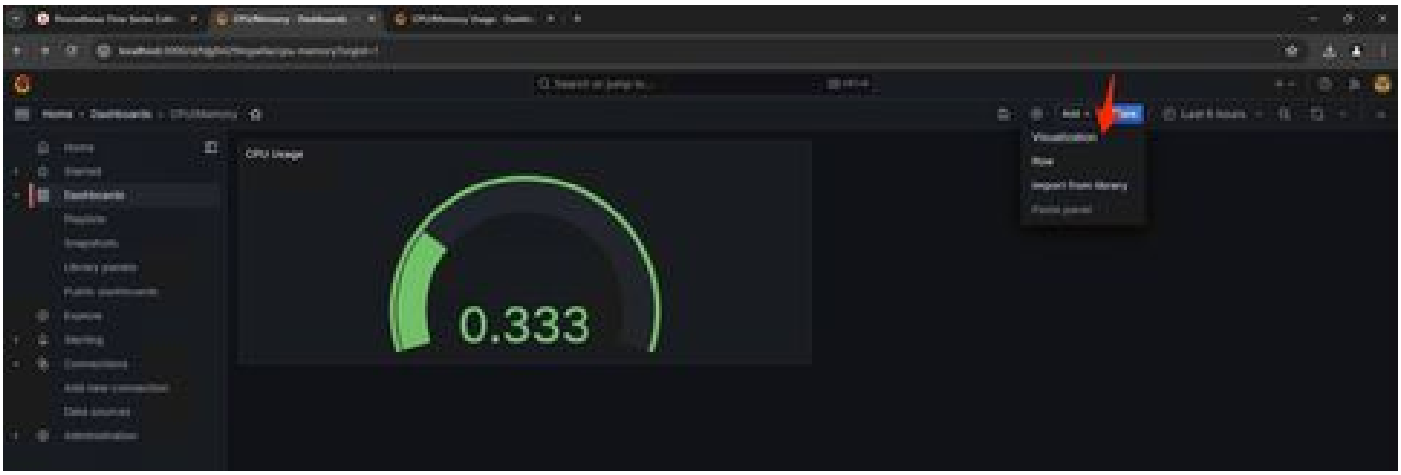
Entrez la requête suivante pourCPU Utilization-

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

15. Cliquez sur `Run Queries` et vous devriez voir une visualisation de l'utilisation du CPU comme ceci -

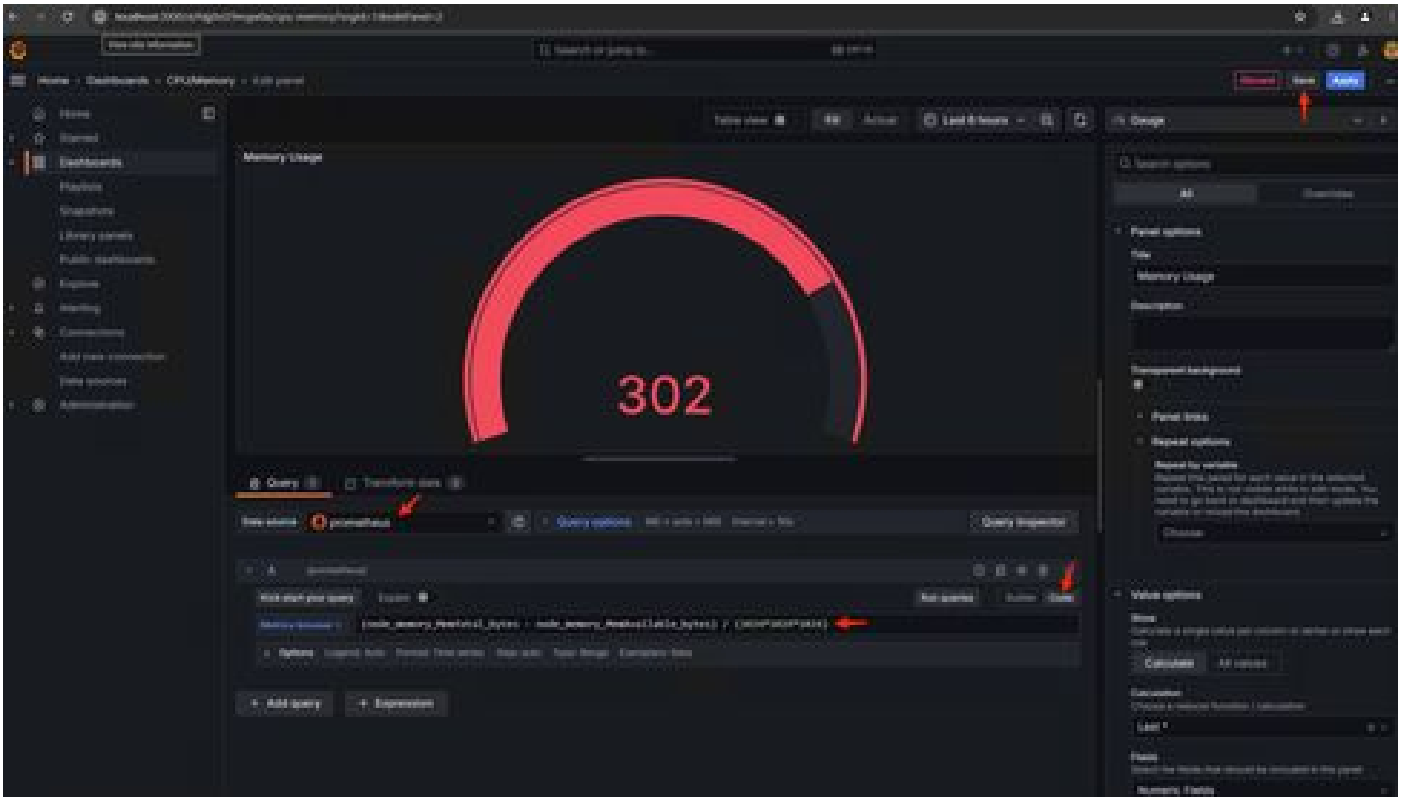


16. Enregistrez le panneau, nommez le tableau de bord et cliquez sur Enregistrer. Ajoutez une autre `visualisation` pour l'utilisation de la mémoire -



17. Pour Utilisation de la mémoire, utilisez la requête suivante :

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



18. Enregistrez les modifications, et vous devriez avoir un tableau de bord comme ceci -



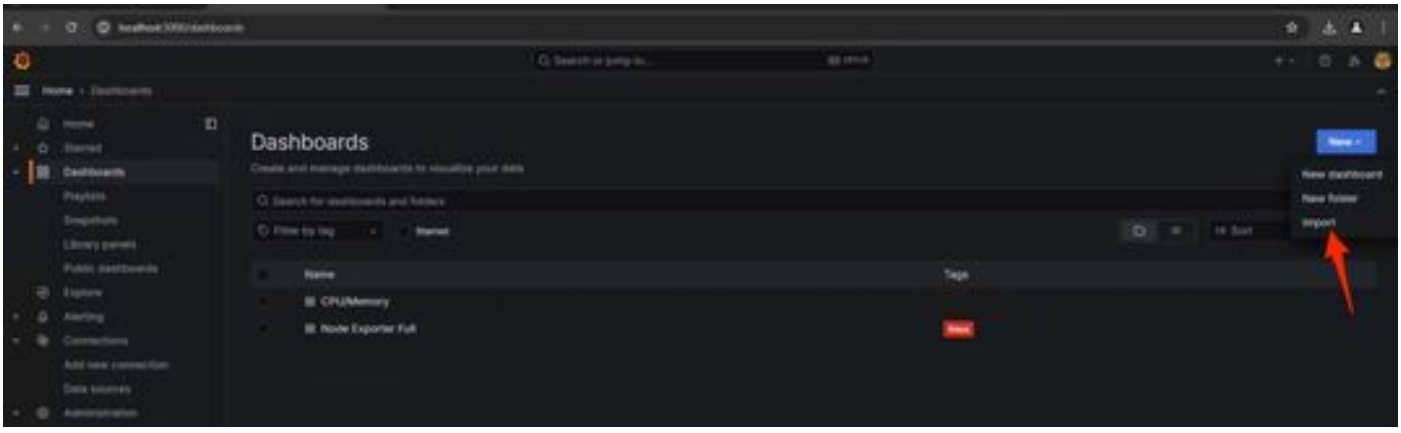
19. D'autres mesures matérielles et logicielles sont disponibles. Pour plus d'informations, cliquez sur les liens fournis `dans la` page `Opadmin`> `Mesures`



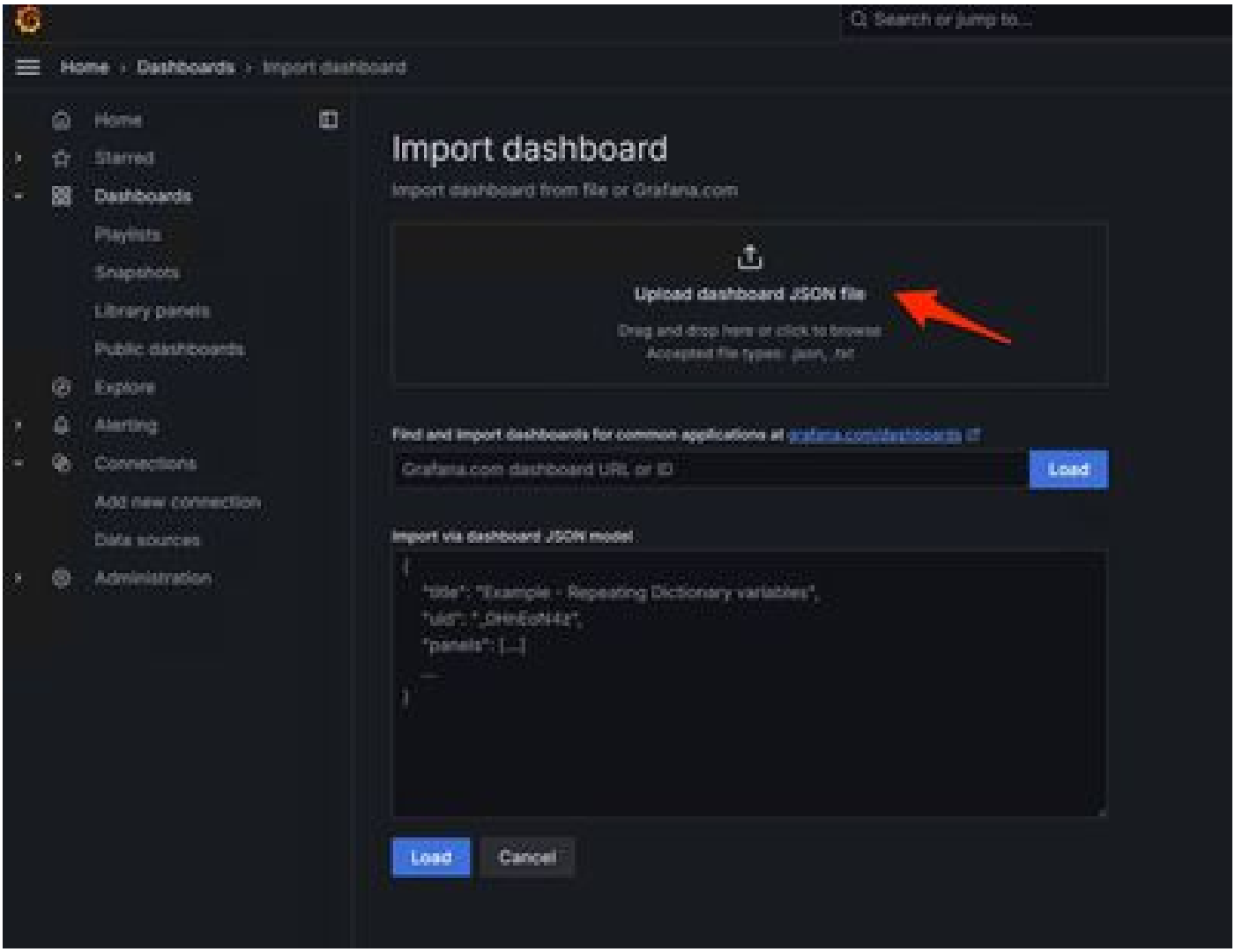
Modèle de tableau de bord Grafana

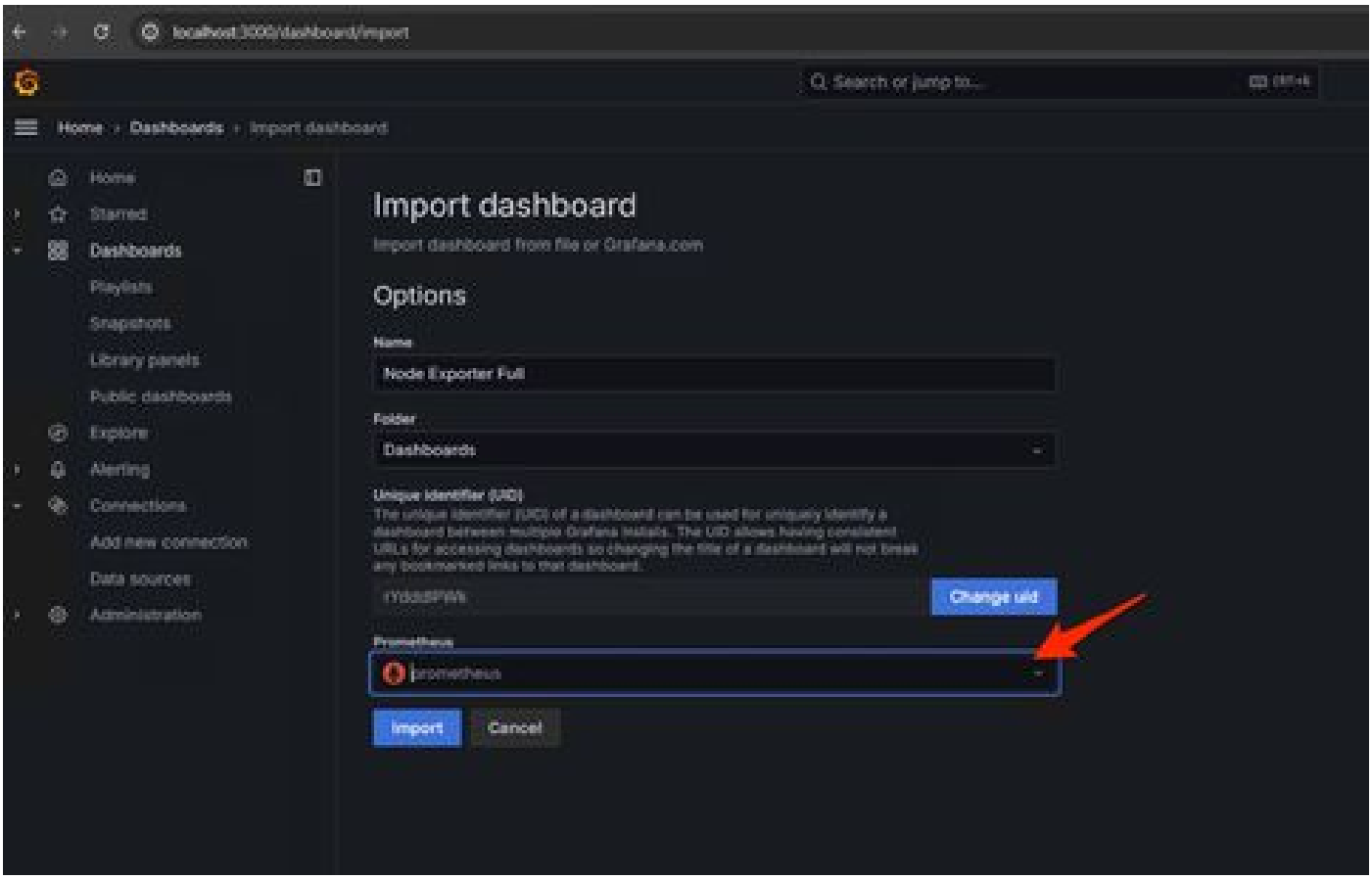
De nombreux modèles de tableau de bord Grafana sont disponibles pour Node Exporter sur le site Web de Grafana. L'un d'eux est - [Node Exportateur complet]

1. Pour importer ce tableau de bord dans votre instance Grafana Téléchargez le fichier JSON, importez le fichier JSON dans Grafana

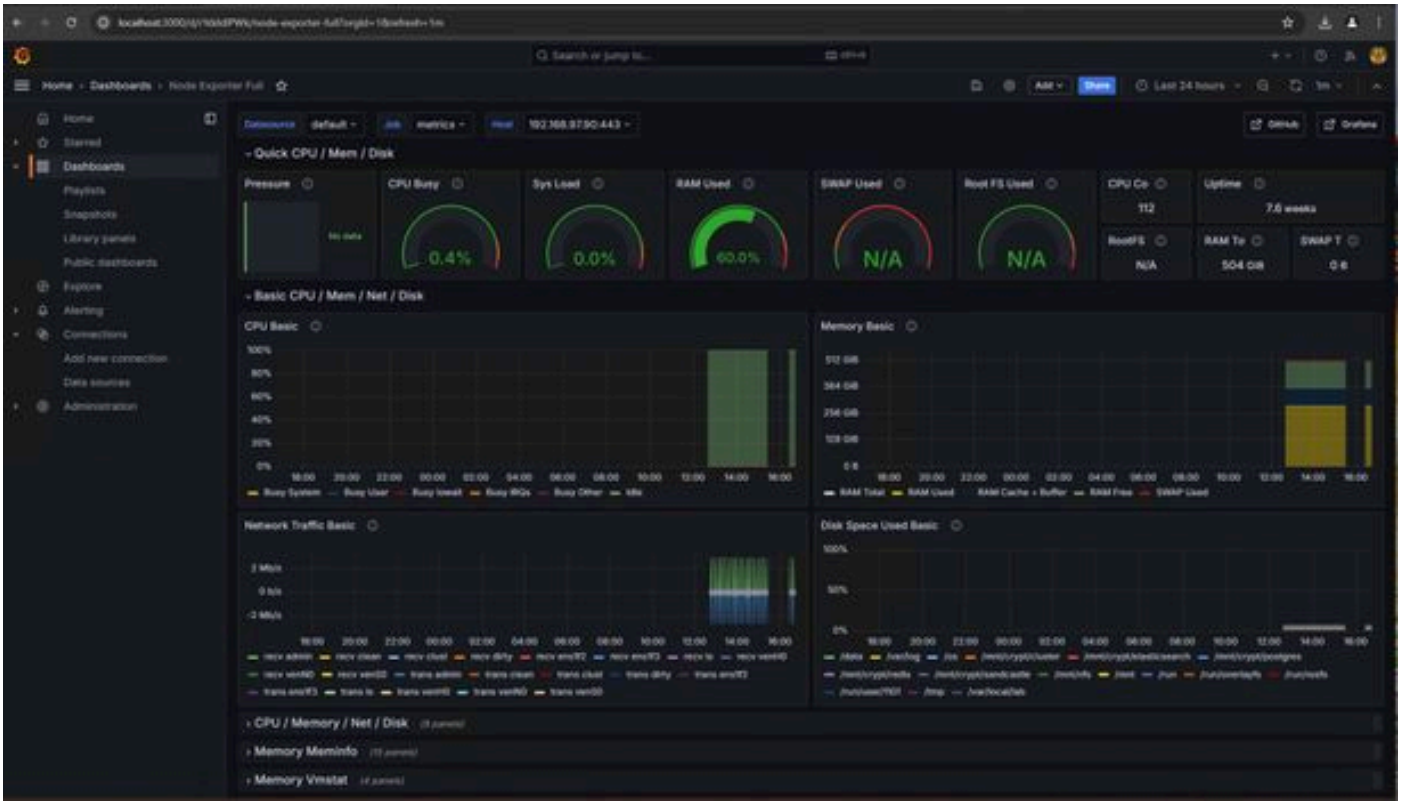


2. Téléchargez le fichier JSON et sélectionnez la source de données Prometheusdata


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. Cela créera un tableau de bord avec beaucoup d'informations matérielles (toutes les mesures du panneau ne sont pas disponibles)-



Dépannage

Si le Prometheus n'a pas réussi à se connecter et à extraire la métrique de l'appliance SMA, vous verrez l'erreur dans `Status` > `Targets` - http://localhost:9090/targets?search=

S'il y a `anyError`, cela doit être corrigé avant qu'il puisse extraire les données. Problème courant : le certificat SSL de l'appliance SMA Opadmin n'est pas approuvé par l'ordinateur local. Assurez-vous de créer un certificat d'administration SMA avec IP et DNS SAN, et ajoutez l'autorité de certification racine de signature au magasin de confiance de l'ordinateur local.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.