

Configurer l'appliance Secure Malware Analytics avec le logiciel de surveillance Prometheus

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Informations générales](#)

[Configurer](#)

[Vérifier](#)

Introduction

Ce document décrit les étapes à suivre pour exporter les données de mesure du service Secure Malware Analytics Appliance vers le logiciel de surveillance Prometheus.

Contribution des ingénieurs du TAC Cisco.

Conditions préalables

Cisco recommande que vous ayez connaissance de Secure Malware Analytics Appliance et du logiciel Prometheus.

Exigences

- Appliance Secure Malware Analytics (version 2.13 et ultérieures)
- Licence du logiciel Prometheus


The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Le système de surveillance basé sur la recherche Riemann/Elastic exécuté sur l'appliance est remplacé par la surveillance basée sur Prometheus à partir de la version 2.13 de l'appliance Secure Malware Analytics.



Remarque : cette intégration a pour objectif principal de surveiller les statistiques de votre

 appareil Secure Malware Analytics à l'aide du logiciel Prometheus Monitoring System. Cela inclut une interface, des statistiques de trafic, etc.

Configurer

Étape 1. Connectez-vous à Secure Malware Analytics Appliance, accédez à Operations > Metrics afin de trouver la clé API et le mot de passe d'authentification de base.

Étape 2. Installez le logiciel Prometheus Server : <https://prometheus.io/download/>

Étape 3. Créez un fichier .yml, il doit s'appeler prometheus.yml et il doit avoir ces détails :

```
scrape_configs:
  - job_name: 'metrics'
bearer_token_file: 'token.jwt'
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
```

Étape 4. Exécutez la commande CLI afin de générer un jeton JWT pour l'authentification, tel qu'il est spécifié dans le fichier de configuration ci-dessus :

```
curl -k -s -XPOST -d 'user=threatgrid&password=<TGA Password>&method=password' "https://_opadmin IP_:44
```

Étape 5. Exécutez cette commande pour vérifier le champ Date d'expiration du jeton (1 heure de validité).

```
awk -F. '{print $2}' token.jwt | base64 --decode 2>/dev/null | sed -e 's;\{([^\}]\)};\1};' | jq .
```

Exemple de résultat de commande ci-dessous :


```
{
  "user": "threatgrid",
  "pw_method": "password",
  "addr": "

  ",

  "exp": 1604098219,
  "iat": 1604094619,
  "iss": "

  ",

  "nbf": 1604094619
}
```

 Remarque : l'heure est affichée au format Epoch.

Étape 6. Extrayez la configuration des services, après vous être connecté à l'interface opadmin, entrez cette ligne de l'interface utilisateur :

<#root>

`https://_opadmin IP_/metrics/v1/config`

Étape 7. Après le redémarrage du service Prometheus, la configuration est activée.

Étape 8. Accédez à la page Prometheus :

<#root>

`http://localhost:9090/graph`

Vous pouvez voir les services Secure Malware Analytics Appliance dans l'état "UP" , comme illustré dans l'image.

Targets

All Unhealthy Collapse All


metrics (8/8 up) show less

Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
-443/metrics/v1/service/fav2	UP	instance="10", -443, job="metrics", service="fav2"	41.184s ago	18.7ms	
-443/metrics/v1/service/monbox	UP	instance="10", -443, job="metrics", service="monbox"	12.728s ago	14.3ms	
-443/metrics/v1/service/node-exporter	UP	instance="10", -443, job="metrics", service="node-exporter"	7.126s ago	81.36ms	
-443/metrics/v1/service/observer	UP	instance="10", -443, job="metrics", service="observer"	45.691s ago	10.27ms	
-443/metrics/v1/service/supervisor	UP	instance="10", -443, job="metrics", service="supervisor"	3.797s ago	15.45ms	
-443/metrics/v1/service/ven-entrance	UP	instance="10", -443, job="metrics", service="ven-entrance"	19.474s ago	19.31ms	
-443/metrics/v1/service/classifier	UP	instance="10", -443, job="metrics", service="classifier"	44.567s ago	18.17ms	
-443/metrics/v1/service/dictator	UP	instance="10", -443, job="metrics", service="dictator"	45.818s ago	17.35ms	

Vérifier

Vous pouvez voir que les données sont reçues des périphériques Secure Malware Analytics Appliance, examiner les mesures en fonction de vos propres exigences, comme indiqué dans l'image.



 Remarque : cette fonctionnalité ne fonctionne que pour collecter des données spécifiques. La gestion du flux de données est la responsabilité du serveur Prometheus. Le TAC Cisco ne prend pas en charge le dépannage. Vous pouvez contacter le support technique d'un fournisseur tiers pour obtenir une assistance supplémentaire.

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.

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.