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

## Table des matières

Introduction
Conditions préalables
Exigences
Informations générales
<u>Configurer</u>
<u>Vérifier</u>

#### 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

TLe 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": "
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
    ",
```

Nemarque : 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.

Promethe	us Alerts Graph Status * Help New UI					
Targe	ets					
All Unh	ealthy Collapse All					
metrics (8	B/8 up) show less					
Endpoint		State	Labels		Last Scrape	Scrape Duration Error
5	: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	s443" job+"metrics" service-"monbox"	12.728s ago	14.3ms
	:443/metrics/v1/service/node-exporter	UP	instance-*10.	s443" [job="metrics" service="node-exporter"	7.126s ago	81.36ms
	:443/metrics/v1/service/observer	UP	instance-*10.	s463" 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.	s443" 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.

node_n	etwork_transmit_bytes_total			Lond Amon	time 132ms ution: 14s
Execute	node_network_transmit_E				
Graph	Console			Remo	ve Graph
	- Th + (Until ) Res. (c) Ostached				
600					
400					
200					
0					-
	22.00 . Il rode, retwork, barront, bytes, bibliotevice-"verifo?" polar . Il rode, retwork, barront, bytes, bibliotevice-"verifo?" polar . Il rode, retwork, barront,	22.45	00.00	00.15	
	If node_setwork_transmit_tytes_tutal(device="to",tutance=""""""""""""""""""""""""""""""""""""				
	Inder retwork, Sammel, Syster, Schlighweiser Schrift, Instance     Instance, Sammel, Syster, Schlighweiser Schrift, Instance     Instance, Sammell, Syster, Schlighweiser Schrift, Instance     Instance, Sammell, Syster, Schlighweiser Schrift, Instance     Instance, Sammell, Sammell, Syster, Schlighweiser Schrift, Instance     Instance, Sammell, Sam				
	in noo-person (name pare (compress care yman in the new compress ) B noo-person (name pare (compress care yman in the new compress ) B noo-person (name pare (compress care yman in the new compress )				
				Lond 5	ine 176ms
node_n	etwork,receive,bytes,total			Load Amaru Tota ti	ine 176ms tion 14s ine series 8
node_n Execute	etwork_jeceive_bytes_total node_network_jeceive_by •			Last San	ine 176ms con 14s ine series 8 re Graph
node_n Execute Graph	etwork_receive_bytes_total node_network_receive_by # Console			Last Marin Vira S	ine 176ms tion tils ine series 8 re Graph
node_r Execute Graph	etwork_ureahve_bytes_total anode_network_ureahve_by # Console  The the the Res 60 Outsclad			Last 1 Nor 1 Remov	ine 176ms Gen 14s meseries 8 re Graph
node_n Execute Graph	etwork_receive_bytes_total  console  the the test for the test of test			Last Mercu New District Control of Control o	ine 176ms Gen 145 me series 8 le Graph
node,r Execute Graph	etwork_receive_bytes_total  console  the			Lead New York	ine 176ms con 14s me seriei 8 e Graph
node,r Execute Graph 1000	eteody, ecoive, bytes, total  rode, vetaols, ecoive, by   Console			Lead New York	ine 176ns ten 144 meseries 8 e Graph
node_r Execute Graph 1005 800	eteody, ecolve, bytes, total  rade, vetaols, jecolve, by   Console			Lead New York	ine 136ns Gen tás ne series 8 e Graph
node_r Execute Graph 1005 800 800 400	eteode, jecelve, bytes, total  rade, jecelve, by e  Console			Lead New York	ine 176ns fan 14s ne series 8
node,r Drecom Graph 5000 800 400	eteody, ecolve, bytes, total  rade, retaoly, ecolve, by   Console			Les i Renov	ene thing rom tai ne seise 8 le Graph
node,r Execute Graph 5000 800 400 200	eteody, ecolve, bytes, total  rade, retainly, localized  total  t			Les i Renov	ine thins ton tai re sinei 8 e Graph
node,r Execute Graph 5000 400 400 200 0	eteode, jecelive, bytes, total  rader, jecelive, bytes, total  Console   total  total total			Let i Renov	ine Stiers Gen 144 re series 8 e Graph
node_r Execute 5000 800 800 400 200 0	eteode, jeselve, jujes, just cosole	24	E 00	Let 1 Recover	ina tXins Gen tia e Graph
node_r Encode 1000 000 000 000 000 000 000 000 000 0	etende, jeselve, jejse, jotal rođer, jestvoli (jeselve, joj e Console	24	D 00	Let 1 Recover	ene 176ms from ha re series 8 re Graph
node, r Encont 1000 800 400 200 0	etende, jeselve, jejse, jesel rode, jeselve, jejse, jesel Console 10      10	24	6.0	Let 1 Recov	ene t'Ners fren ha recenta 8 e Graph
node,n Executi 1900 800 800 800 800 800 800 800 800 800	tetoriki, jecole, je, jeta node, jetavici, jecole, jeta Concile	214		Let 1 Recover	ene 116re pon 144 ne series 8 e Graph

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.