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

Table des matières

Introduction	
Conditions préalables	
<u>Exigences</u>	
Composants utilisés	
<u>Configurer</u>	
Modèle de tableau de bord Grafana	
<u>Dépannage</u>	

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 <u>offre Prometheus</u>.

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 Opadmin de l'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 SMA Appliance Opadmin. Générer une 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 <u>cette vidéo</u> <u>Youtube.</u>

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:p
target_label: __address__ # change target
                                          # capture host:port
    basic_auth:
      username: "API_KEY"
      password: "2024-04-22T15:32:14.082689318Z xxxxxxx-xxxx-xxxx-xxxx-xxxx-xxxxx-xxxx
```

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://<opadmin IP>/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.

C prometheus 2112 -	ándonna X 🕂				- D X
e o e	C D > - prometheus	2.51.2.windows-amd64 >			Search prometheus-251.2 aindor Q
© New - 🔺		16 Sort - 💷 Vew -			🗔 Detaih
 Collary Drabbae Drabbae Drasbaes Drasbaes Drasbaes Drasbaes Drasbaes Drasbaes Drasbaes Pictures Nasic <	 Narve Console Jahraies Consoles deta LCINSI HOTICE prometheus prometheus prometheus targetujeen (targetujeen (Data modified 4/19/2004 5:01 PM 4/19/2004 5:01 PM 4/25/2004 5:00 PM 4/19/2004 5:00 PM 4/19/2004 5:00 PM 4/19/2004 5:00 PM 4/19/2004 12:07 PM 4/19/2004 1:07 PM	Yype File folder File folder File File Application YML File Application SCNI File	See 1249 449 12847940 140 140 240 240	
s 🔲 This PC 10 Rems					D •

9. Démarrer Prometheus

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

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.

a a C C konfeet/Minaphilaneter					9 & A
O Prometheus - Inne Court - Inne - Inne					CEO 4
Targets					
Alaramanian Al Intering Talantia	A reaction	entipopet de federes			
mairies (IVII sąt)					
Dedpoint	tion (Labels	Carl Innyn	Surapie Overetion Erner	
*** prove \$10,000,000 \$1000000 \$10000000000000000	-	Substitution and particular sectors and	BASIN apr	ar sidens	
Adaptation of the Adaptation o	-		44.037n mpr	4/15/hes	
	-	Annual Column Column Column	This Blains ago	tii piiteen	
helps (*12.) hit is bissening is bissed as they doe			10.000 apr	n.c.hee	
Adapted 715, 145.07 Ministeries of American Stationers		Benefic storesteller; pactures; Benefitener;	an 1996 Minings	81.22 Leng	
Adapter 122 ADD D. Manual and American Spirit		Interested in the Interest in	40.614 age	14.182em	
Property and a list of Manhamman And Supervised Street Street	-	International particular particular		100.10000	
Adapter (ALISER) Microsoft of Constant Statement	-	International personal management	Tal 162,000 rapi	1000004	

12. Installation et configuration de Grafana

Téléchargez l'exécutable Grafana depuis 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'URL du serveur Prometheus <u>http://localhost:9090/</u> comme URL du serveur Prometheus

+ + 0 0 bishestron	and an a second s				* * *
Convertions - Delate	Martin Communication	G. Baarsh on Jones Inc.	(1999)		+- 0 a 4
 A Horse A Denset B Latitudes Paylos Departure Unary servet 	prometheus ren: Prometheus si tempe il Transment			name and a second	
And partners D Turtow A turtow Alt ture connection Alt ture connection Turto assesse	Refere you can be free freemen days source, freese names with " are required	per nut cellipset Come e Descript			
1 C Alimenter	Connection Auxiliars area (M, 1, 2) Ing. Souther: 10	RI 4			
	Authentication Anterfeation nation Course or advancements matter to access the party of				
	No Addisections	-			

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. Ajouter 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 -

+ = 0 @ subscriptions	Chaquella, 1 gas monoray (negation)							3	 1
0		C Search or jump to		100.0000					-6
I Have / Desition / Cruthers						Act 17	C Lest these -		
Alimine Alimine	302		Crowner (0.677					

19. D'autres mesures matérielles et logicielles sont disponibles. Pour plus d'informations, cliquez sur les liens fournis dansOpadmin>

Metrics page



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 - <u>Node</u> Exportateur complet

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

+ + 0 . • Heathart 1000 tanteou	4 · · · · ·					
0		O, Search or program.	(and the second			+- 0 # 6
I Nove - Doctoren :						
0 mm D	Dashboards Gran we have per tartitients to reader per ter					(Merica)
Prophete Designation Library presents	C Search for exercises of and below C Free by by				0 = 10	New York
Public statisticands 2 Superar 4 D Alarting 5 D Commission Add size connection Data superar	Norme El CPUMenory El hode Esporter Full			÷.		1
a a American						

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



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

+ + 0 0 location 2000 sprand	IPW6/hode-exporter-full/orgid=18sebasts-1m						6 🛓 🛎 1
0		G. taurch in jung to	and in the local sector				- I O JA 🔮
E Note - Dathoarts - Note Equ	terful o			D 0 MH	O Lies		
G Home D	Commerce default - Internet - meetics - meetics - Gelick CPU / Meetin / Disk	923683730443 -				2 00	to St Online
Parylints Despervets Likewy panets	Peeses 0 CFU Berg 0	Synteed 0 844		N/A	09000 0 12 Read 5 0	Uptime D 7.6 MAM To O	SWAPT C
Poste and output Post	- Baskic CPU / Mem / Net / Disk CPU Baskic O Scott Baskic O	00 9600 9600 1000 100 64 - Ray Diver - Ma 400 9600 9600 1000 10 400 9600 9600 1000 10 400 9000 9600 1000 10 400 9000 9600 1000 10 40 - Ray Million	Memory Basic O Store Gal Stat Gal	2300 0000 0300 di MARCarla - Bollor - D E250 0000 0200 - microphicadanie - postal - Audioadanie - postal	NoA	304 Cia 80 1000 12.00 Ciaed 00 1000 12.00 h = (mol/system)	96 M00 %60 M00 %60 M00 %60 M00 %60

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.