How to configure remote Prometheus and Grafana to monitor Secure Malware Analytics (Formerly Threat Grid) Appliance

Contents

Introduction	
<u>Prerequisites</u>	
Requirements	
Components Used	
<u>Configure</u>	
Grafana Dashboard Template	
Troubleshoot	

Introduction

In the Secure Malware Analytics (SMA) Appliance, we do not offer SNMP protocol to monitor the appliance resource usage, instead, the appliance offers<u>Prometheus</u>.

This document will outline how to configure a remote Prometheus instance and use<u>Grafana</u>to visualize the data pulled from the appliance.

Prerequisites

Download and install the following tools to your local machine/server:

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

Requirements

- Secure Malware Analytics (SMA) Appliance Software Version 2.18 and above
- Windows Machine
- Admin access to Appliance Admin(Opadmin) Console
- Secure Malware Analytics (SMA) Appliance Opadmin SSL Certificate Trusted by the local machine

Components Used

- Secure Malware Analytics (SMA) Appliance
- Windows 11 Pro machine
- <u>Prometheus</u>
- <u>Grafana</u>

Configure

For this document, We have used a Windows 11 Pro as a remote host where we installed Prometheus and

Grafana. These tools are also available for Linux or MacOS.

1. Generate API key in Secure Malware Analytics (SMA) Appliance to access metrics

Login to SMA Appliance Opadmin. Generate API Key for Metrics from **Opadmin > Operation > Metrics**



2. A Basic Auth Username and Password will be generated which we will need to use in Remote Prometheus config.



3. Install and Configure Prometheus

Follow the instructions provided by Prometheus user guides to install your instance if you're using Linux or MacOS. For this document, we have installed Prometheus on a Windows 11 machine, and for the installation process, we followed this <u>Youtube video</u>.

4. Create a config file with the name prometheus.ymlwith the following content -

```
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__]
```

5. in basic_auth section use the Basic Auth Username and Password generated in Step 1.

6. Pull the configuration of services you will be able to pull metrics from by entering the following in the UI after logging into Opadmin -

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

You will get something like -

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

Here 192.168.97.111 is Admin IP for my SMA appliance.

7. Create a file with the name targets. json and copy the above content into that file.

8. Copy prometheus.yml and targets.json to the Prometheus directory (follow installation guides), For Windows, I have created a Folder in C:\ drive and extracted the Prometheus installation files there. Then copied prometheus.yml and targets.json to that same folder.

promethous 2.512 a	eindoes a X +				- 0	×
6 9 A	C D > - prometheus	-251.2.windows-amd64 >			Search prometheus-2.51.2 mind	P Q
© Nov - 🔺		📫 Sort - 📰 Vew -			G	Detailte
💽 Gallery	Neve -	Data modified	No.	Sm		
ar 🚔 OneDrive	Console_Motories	4/19/2024 5:31 PM	File folder			
	Consoles	4/19/2024 5:31 PM	File folder			
Dektop #	C anto	4/22/2004 3:00 PM	File folder			
🛓 Developation 🖈	LICENSE	4/15/2004 5:00 PM	File	12.08		
E Documents #	NOTICE	4/19/2024 5:30 PM	596	4.00		
E Fitures . #	prometheux	4/19/2024 5:30 PM	Application	125,570-03		
Mark #	prometheus	4/22/2024 12/07 PM	VML File	10		
Videos #	provided	4/19/2024 5:30 PM	Application	123,009.00		
Recentions	tergetujoun	4/16/2024 1107 PM	350ALFale	2.03		
E1.721512	takan jot	4/19/2024 9:10 PM	JWT File	10		
- toring						
prometheuro-2.5						
b. Dan M						
10 items 1						

9. Start Prometheus

Start Prometheus. For Windows execute prometheus.exe from the command line.

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

This will start the Prometheus and start pulling the metrics from the SMA appliance. Note: Do not close the command line or Prometheus will shut down.

10. To check if your local Prometheus instance is able to pull metric from SMA Appliance load Prometheus UI - `http://localhost:9090/`

11. Go to Status > Targets - http://localhost:9090/targets?search=

Within a few minutes you should see all targets and status UP.

1 1 C C Instant With put from the					0.4.4
O Prometheus: Alexan linear linear linear					0014
Targets					
All proper position Add Addressing Colleges MI		ty we downed he takkets			
mannes (RVR up)					
Endpoint		Labola	Card Surages	Serape Overalises Error	
***********	-		and an and a second second	ET Stillens	
Subject Vall Maller Barriers (Arthree Section States)	-		-44,220s.aps	44137	
	-	Interest and the party of the	in the second distribution age	ani (Borne	
Property and a lot of the second seco	-	International Sectores and	na haantati 🗸 🛛 20.3654 aga	10,2000	
Adapted 742,110,07 Microsoft (Adapted in Microsoft		Summittee () and ()	an The same in the sam	Bild Inc.	
Adapter CALLER Manager and Adapted		because of the second second	and an address app	HLUDDen	
Respective State		section and the section of the	internet - Stations	100 Tillers	
Address of the Addres	-	And the second second second	internet - Stationage	COOPER-	

12. Install and Configure Grafana

Download the Grafana executable from <u>Grafana Labs.</u> Install Granafa, and follow the instructions provided by the installer.

13. After installing Grafana access UI in the browser -http://localhost:3000/

Go to Home > Connections > Data sources - `http://localhost:3000/connections/datasources`

SelectAdd New Datasource and SelectPrometheus from the list. Enter the <u>http://localhost:9090/</u> as the Prometheus Server URL

+ + 0 0 understation	mittering the second				* 1 *
0		Contract or party to	aprese (11.0 B
Maria - Convections - Data at	anne - serenne				
Anno Annonno Anno Anno Anno Anno Anno Anno Anno	prometheus			Anna Anna Anna Anna	
Auto sectoremb Distance Distance Distance Attributions Tell Sectorembers Tell Sectorembers	Series (2) provident	ination, you must configure 4 below or in the starting	fin, har invalved motion films, <u>since the Annalese</u>		
a 🖉 Administra	Connection	er.10002			
	Authentication Automotion metions				
	No Authoritication 113 settings Indexed sectory measures that set to appeal Auto and september on these () 13.0 Set Authoritication ()				

At the bottom of that page selectSave & test. After a successful test, we can create a Dashboard.

14. Create Grafana Dashboard

Go to Dashboards in Grafana UI, SelectCreate Dashboard>Add visulization. SelectPrometheus Data Source.

In Query builder selectCodeinput, Select Type of Visualization (I selected Gauge)

Enter the following query for CPU Utilization-

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

15. Click on Run Queriesand you should see a visualization of CPU Usage like this -



16. Save the panel, name the Dashboard, and Save. Add another Visualization for Memory Usage -

🐨 🤹 Hannahana Dana Jama Jama ang 👔 Pendamang Pandamana — 🗴 🤹 🖓 (P	and the second sec			÷	
+ + a a a and an and a stranger of the second stranger				· 4	÷
0	10 metric and a local	5.00000		++ (@)3	
I mens - Dermanis - Distances - D			B: 0 144	1 10 - 11 - 15 -	
0 1000 0 10000 1 10000 1 10000 1 10000 1 10000 1 10000 1 10000 1 10000 1 10000 1 10000 1 10000 1 10000 1 10000 1 10000	0.333		Versettingen Ber Jacob Rom Honey Anno parmi		

17. For Memory Utilization use the following query

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



18. Save the changes, and you should have a dashboard like this -

+ = 0 @ indexembles	Changeline normalized in 1					\$	
0		C Search or jump to	10 MH (ð
I Home - Destensent - Cruthers				0.0	C Letthea		
 Here <li< td=""><td>302</td><td></td><td>0.677</td><td>,)</td><td></td><td></td><td></td></li<>	302		0.677	,)			

19. Other Hardware and Software metrics are available, For the details click on the links provided inOpadmin> Metrics page



Grafana Dashboard Template

There are many Grafana Dashboard templates available for Node Exporter on the Grafana website. One of them is - <u>Node Exporter Full</u>

1. To import this dashboard to your Grafana instance Download the JSON, import the JSON file in Grafana

* + 0 S keelled Mithattoon						
0	C Search of Song Inc.	(a) (red)				6
E fore - farmers						
Description Description						
Constants			0 = 14 hr	1		
Intern Anting Anting Anting Anting Anting Anting Anting Antine connection Antine connection					١	
· · ·						

2. Upload the JSON file and Select the Prometheusdata source

6				Q. Search or jump to
=	He	me + Dashboards + Ii	rport daatib	sard .
	0 0 8	Home Starred Dashboards	T	Import dashboard Import dashboard from the or Grafiana.com
		Playinta Shapabota Library paseta Public dasheoarda		Lipicad dashboard JSON file Drug and drop here or click to browned Accepted file types: jace, cot
	6 0 0	Explore Alerting Connections Add new connection Data sources		Find and import desiributerits for common applications at applications at applications in a final desiributerits (Fig. or (D)
	8	Administration		{ 'vite': "Duample - Repeating Dictionary variables", 'ule': ",DefedorM4e', 'panels': []]
				Load Cancel

6			<u>α</u>	Search or jump to	CD (101-14
= . t	tome + Dashboards + Im	port dash	board		
0 0 0 0 0 0 0 0 0 0	Home Starred Dashboards Playlists Snapistots Library panels Public dashboards Exptore Alerting Connections	0	Import dashboard Import dashboard from file or Grafana.com Options Name Node Exporter Full Foder Dashboards Unique identifier (JCC) The unique identifier (JCC) of a dashboard can be used for encapely dischoord between multiple Conference in the used for encapely UNIque identifier (JCC)	e elementry a consistent and not bream	
• •	Data sources		ryddallenia Prenetheus Dippmetheus Import	Congrad	

3. This will create a dashboard with a lot of hardware information (not all panel metrics are available)-

+ + O O kostos 2000 (mold Pre-	Ande exporter Ad ² orgid-18mberly-1m						6 ± # 1
0		G. taanhin jang ta	12010				- I O JA 😃
E Hone - Debtoarts - Note Experier F	4 Q.			D 0 MM	C Lies		
G inste D ,	- Duick CPU / Merry / Disk	102308.0750.443 -				3 00	ta Stanlard
Propieto Singutoria Ukrary poneto	Henner 0 CPU Bary 0	Syntaxel 0 84444		N/A	8900 0 12 8875 0	Uptime D 7.6 RAM To D	SWIPT C
Public Satebards Public	Lastic CPU / Mem / Net / Disk PU Basic O U U U U U U U U U U U U U U U U U U	00 06.00 06.00 10.00 10.00 10 06.00 06.00 06.00 06.00 10.00 10.00 10 06.00 06.00 06.00 06.00 06.00 06.00 10.00	N/A N/A N/A N/A SO4 coa 0 e Memory Basic 0 51 cm 52 cm				
	CPU / Memory / Net / Disk (1) served Memory Meminfo (1) served Memory Vmstat (2) served						

Troubleshoot

If the Prometheus failed to connect and pull metric from the SMA appliance, you will see the error

in Status > Targets - <a href="http://localhost:9090/targets?search="http://localhost="http://localhost:9090/targets?search="http://localhost:9090

If there is anyError, that needs to be fixed before it can pull the data. Common issue is SSL certificate of the SMA appliance Opadmin is not being trusted by the local machine. Make sure to create an SMA Admin Certificate with IP and DNS SAN, and add the Signing Root CA to the local machine's trust store.