So konfigurieren Sie entfernte Prometheus und Grafana für die Überwachung von Secure Malware Analytics (ehemals Threat Grid) Appliance

I	n	h	а	lt	

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konfigurieren
Grafana Dashboard-Vorlage
Fehlerbehebung

Einleitung

In der Secure Malware Analytics (SMA) Appliance bieten wir kein SNMP-Protokoll zur Überwachung der Ressourcennutzung der Appliance an, sondern die Appliance <u>bietet</u> <u>Prometheus</u>.

In diesem Dokument wird beschrieben, wie Sie eine entfernte Prometheus-Instanz konfigurieren und Grafanato verwenden, um die von der Appliance gezogenen Daten zu visualisieren.

Voraussetzungen

Laden Sie die folgenden Tools herunter, und installieren Sie sie auf Ihrem lokalen Computer/Server:

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

Anforderungen

- Secure Malware Analytics (SMA) Appliance-Software Version 2.18 und höher
- Windows-Computer
- Administratorzugriff auf die Admin-Konsole der Einheit (Opadmin)
- Secure Malware Analytics (SMA) Appliance Opadmin SSL-Zertifikat Vertrauenswürdig durch lokalen Computer

Verwendete Komponenten

- Secure Malware Analytics (SMA) Appliance
- Windows 11 Pro
- Prometheus
- Grafana

Konfigurieren

Für dieses Dokument haben wir einen Windows 11 Pro als Remote-Host verwendet, auf dem Prometheus und Grafana installiert wurden. Diese Tools sind auch für Linux oder MacOS verfügbar.

1. API-Schlüssel in Secure Malware Analytics (SMA) Appliance für den Zugriff auf Metriken generieren

Melden Sie sich bei SMA Appliance Opadmin an. API-Schlüssel für Kennzahlen generieren von Opadmin > Vorgang > Kennzahlen



2. Es werden ein einfacher Benutzername und ein einfaches Kennwort für die Authentifizierung generiert, die in der Remote-Prometheus-Konfiguration verwendet werden müssen.



3. Prometheus installieren und konfigurieren

Folgen Sie den Anweisungen in den Prometheus Benutzerhandbüchern, um Ihre Instanz zu installieren, wenn Sie Linux oder MacOS verwenden. Für dieses Dokument haben wir Prometheus auf einem Windows 11-Computer installiert, und für den Installationsvorgang haben wir <u>dieses</u>

Youtube-Video verfolgt.

4. Erstellen Sie eine Konfigurationsdatei mit dem Namen prometheus.yml mit folgendem Inhalt:

```
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 xxxxxxx-xxxx-xxxx-xxxx-xxxxx-xxxxx-xxxx
```

5. im Abschnitt basic_auth den in Schritt 1 generierten Benutzernamen und das Kennwort für die grundlegende Authentifizierung verwenden.

6. Laden Sie die Konfiguration der Services herunter, aus denen Sie Kennzahlen abrufen können, indem Sie nach der Anmeldung bei Opadmin Folgendes in die Benutzeroberfläche eingeben:

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

Sie erhalten u. a. Folgendes:

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

Hier ist 192.168.97.11 die Admin-IP für meine SMA-Appliance.

7. Erstellen Sie eine Datei mit dem Namen targets.json, und kopieren Sie den oben genannten Inhalt in diese Datei.

8. Kopieren Sie prometheus.yml und targets.json in das Verzeichnis Prometheus (folgen Sie den Installationsanleitungen), Für Windows habe ich einen Ordner in Laufwerk C:\ erstellt und die Prometheus-Installationsdateien dort extrahiert. Dann kopierte prometheus.yml und targets.json in den gleichen Ordner.

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 Jame					D •

9. Prometheus starten

Starten Sie Prometheus. Für Windows führen Sie prometheus.exe über die Befehlszeile aus.

Dadurch wird der Prometheus gestartet und die Kennzahlen aus der SMA-Appliance abgerufen. Hinweis: Schließen Sie die Befehlszeile nicht, da Prometheus sonst heruntergefahren wird.

10. Um zu überprüfen, ob Ihre lokale Prometheus-Instanz in der Lage ist, Metriken aus der SMA-Appliance zu ziehen, laden Sie Prometheus UI - `http://localhost:9090/`.

11. Gehe zu Status > Ziele - http://localhost:9090/targets?search=

Innerhalb weniger Minuten sollten Sie alle Ziele und den Status UP sehen.

a i C G kasher/Weingebiesetter					0.4.4
O Prometheux lines lines have lines					C2014
Targets					
All property and a subsetty alloge M	A rear	The new discussion for Saddwide .			
manifest (NVA spl)					
Indpairs	-	Lagada	Gast Surages	Songe Overetien Erner	
Adapter Vol. 102 Difference i problema de la papar de p		Second restorements (Second 2)	and support	ST Stillens	
And a state of the second s			44,0399 apr	ANT STATE	
COMPACT NO CONTRA		Resources and responded in the second of	The second second	111 (100 mg	
Independent 22, 144,407 Minimum and Articles and Articles and		International Statement	anne (haattal) v 10.000 apr	Ruthes	
Adapted 7112 112 17 Ministeries and Antonio and		Annalization (Children (Ch	and a failed at 120 Mile age	Hild Inc.	
Adapted Vol. 10111 Mercanit and Internet Adapted		MARCHINE PROVIDED IN CONTRACT	and a state of	H.103mm	
Adapted 112 148 17 Manhatria (Adapted and and and		Sector Statement of the sector of	and international - Station age	100.100mm	
Adapted All Hall of Management of Constant Statistics		Internet Section 1	annin Marandi - 10 Mile age	1000000	

12. Grafana installieren und konfigurieren

Laden Sie die Grafana-Programmdatei von Grafana Labs herunter. Installieren Sie Granafa und befolgen Sie die Anweisungen des Installers.

13. Nach der Installation von Grafana Access UI im Browser -http://localhost:3000/

Gehen Sie zu Startseite > Verbindungen > Datenquellen - `http://localhost:3000/connections/datasources`

Wählen Sie Add New Datasource (Neue Datenquelle hinzufügen) und SelectPrometheus aus der Liste aus. Geben Sie "http://localhost:9090/" als Prometheus Server-URL ein.

+ + 0 0 Ludwermer	Termen Termin (Marine Context) (Marine Context) (Marine Context)	♦ ± ♦
0	G. Dearth or Juny No	+: 0 a C
E Note : Corrections : Dat	Research - provider	
D from C Down C Down C Down Control of Control of	prometheus Ture Prometheus w Inneres	ter Santas (Marcaniae)
Chrony parents Points: parents © Equation	The Constant and Section	
 B control Connections All two connection Determines 	Andres per can can be Premetered data terated, you read tortigan & being or in the cartigits. For anisted terms from, <u>size the Anadomica</u> Form meters with 1 are required	
 B Americanyon 	Connection Presented IR 1 2 Ing Stautour Some	
	Authentication Authentication methods Disease of authentication methods	
	No Admenication .	
	TLE Institutes Antidential security measurement that have be applied on top of automations Anti-ball support particularly () TLE Court Automations ()	

Wählen Sie unten auf dieser Seite Speichern und testen aus. Nach einem erfolgreichen Test können wir ein Dashboard erstellen.

14. Grafana Dashboard erstellen

Gehen Sie zu Dashboards in Grafana UI, Wählen Sie Dashboard erstellen>Visualisierung hinzufügen. Wählen Sie Prometheus Data Source.

Wählen Sie im Abfrage-Generator Codeinput, Visualisierungstyp auswählen (I selected Gage)

Geben Sie die folgende Abfrage für CPU-Auslastung ein:

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

15. Klicken Sie auf Run Queriesund Sie sollten eine Visualisierung der CPU-Nutzung wie diese sehen -



16. Speichern Sie den Bereich, nennen Sie das Dashboard und speichern Sie. Weitere Visualisierung für die Speichernutzung hinzufügen -



17. Verwenden Sie für die Speichernutzung die folgende Abfrage

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



18. Speichern Sie die Änderungen, und Sie sollten ein Dashboard wie dieses haben -

+ = 0 @ sussessmethyse	Changed and a second property in a second property of the second pro							
0		O Search of Jurnal Inc.	10 PT-1					ø
I Hore - Debloars - Cruthers				0 Inc.	-	O Lest these -		
 Insue 	302	Children	0.677					

19. Weitere Hardware- und Software-Metriken sind verfügbar. Klicken Sie für Details auf die Links in "Opadmin>Metriken".



Grafana Dashboard-Vorlage

Es gibt viele Grafana Dashboard Vorlagen für Node Exporter auf der Grafana Website. Eines davon ist - Node Exporter Full

1. Um dieses Dashboard in Ihre Grafana-Instanz zu importieren Laden Sie die JSON-Datei in Grafana herunter

	0 . 0 heathcat 1010/1444	ter t					. \$			
0	ere i Damoen		(C) Search of Series In.	(and the second						•
- 1	men I Dariel Darien Darien Darien Darien Darien Liter presi	Dashboards Orient and heavily reactioned to dealers process O forest for contraction and heavily O from by by the contraction of the sec				0 - 10			-	
0.00.0	Public statilizareta Espera Auriteg Commission Add same connection Data tenerety Automission	E CRUMenary E CRUMenary E Rode Exporter Fail			È.			1		

2. Laden Sie die JSON-Datei hoch und wählen Sie die Prometheus-Datenquelle aus.

6			Q. Search or jump to
= ;	iome + Dashboards + In	portiduario	oard
0 4 8	Home Starred Dashboards	۵	Import dashboard Import dashboard from the or Orisfana.com
	Playista Snapshots Library panels Public districtords		L Upload dashboard JSON file Dring and drop here in click to foreveat Accepted file types: just, tot
· ·	Alarting Connections Add new connection Data sources		Find and import deshtopants for common applications at gradural considerations at Gradural corrected to the common applications of gradural considerations at Load Load Load Load Load Load Load L
. 0	Administration		<pre> the ', 'Example - Repeating Dictionary variables', 'uld': ', DrieGoN42', 'panels'', [] } </pre>
			Load Cancel

6			Q. Search or jump to	CD (1979-14)
= "	iome + Dashboards + Impo	rt dashboard		
	Home Starred Dashboards Playlists Snapistot6 Library panels Public dashboards Exptore Alerting Connections	Import dashboard Import dashboard Import dashboard Import dashboard Import dashboard Import dashboard Mane Node Exporter Full Foder Dashboards Unique identifier (JIC) The unique identifier (JIC)	ana.com	
	Add new connection Data sources Administration	disaffoqued beforeen multiple Gordinan inte utilius for acclassing disaffoqueds so char any bookmarked insta to that disaffoqued rydold57646 Prometheue Dependence Import	Halos. The UID allows having consistent open the file of a dashidnand will not beau Concorcial	

3. Dadurch wird ein Dashboard mit vielen Hardware-Informationen erstellt (nicht alle Panel-Metriken sind verfügbar)-

+ · O O keekee 2000 grand	PWK/sole expecter Adforgid=18sebeet=1m							
0		G, taurch or pany to-		mines.				- I O - A 🦉
🗮 Hone - Dathboarts - Note Equi	ter full 👷				D 0 ANY	C Lies		
G Home D	Tommerica default - Anii metrica - metrica - Guick CPU / Metri / Disk	102308.0750.443 -					2 m	and the second
Paylints Snopolotik Ukrary panetik Public Sattiboards	Presser © In max Unit 0 0,4%	5ystand 0	60.0%	SAMPONE O	N/A	No Col O T2 Read to O	Liptime () 7.6 8.6.6 To () 504 cm	SWAPT C
 Propose Antering Antering Antering Antering Antering Antering Antering Antering 	Basic CPU / Mem / Net / Disk CPU / Mem / Net / Disk CPU Sos Soss Sos Soss Sos Soss Sos Soss Soss	4.00 04.00 04.00 10.00 BDS - Buny Diver = 184 04.00 04.00 00.00 04.00 - 10.00 04.00 04.00 04.00		Memory Basic O Stram Set 08 Set 08 Dia Gale Basic Dia Basic Dia Spece Used Basic Solo. Dia Spece Used Basic	22.06 00.06 02.00 MMCCarls - Duffer C 22.00 00.00 02.50 0 ma	0-10 96.00 (8 8887 free - 1986 4200 96.00 86 900 96.00 86 900 96.00 86	90 10:00 12:00 Gand 00 10:00 12:00 6 - Jonatoryphon - Jongtonright 20	14.00 NEO

Fehlerbehebung

Wenn der Prometheus keine Verbindung herstellen und keine Kennzahlen von der SMA-Appliance abrufen konnte, wird der Fehler unter

Status > Targets - <u>http://localhost:9090/targets?search=</u>

Wenn ein Fehler vorliegt, muss dieser behoben werden, bevor die Daten abgerufen werden können. Häufiges Problem ist das SSL-Zertifikat der SMA-Appliance Opadmin wird vom lokalen Computer nicht als vertrauenswürdig eingestuft. Stellen Sie sicher, dass Sie ein SMA-Administratorzertifikat mit IP- und DNS-SAN erstellen und die Signing Root-Zertifizierungsstelle zum Vertrauensspeicher des lokalen Computers hinzufügen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.