使用Prometheus監控軟體配置安全惡意軟體分析 裝置

目錄		
館企		
<u>必要條件</u>		
<u>需求</u>		
<u>背景資訊</u>		
<u>設定</u>		
<u>驗證</u>		

簡介

本文檔介紹將Secure Malware Analytics Appliance服務度量資料匯出到Prometheus監控軟體的步驟。

由Cisco TAC工程師貢獻。

必要條件

思科建議您瞭解安全惡意軟體分析裝置和Prometheus軟體。

需求

- 安全惡意軟體分析裝置(版本2.13及更高版本)
- Prometheus軟體許可證

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

背景資訊

T安全惡意軟體分析裝置版本2.13之前的基於Prometheus的監控取代了裝置上運行的基於 Riemann/Elastic搜尋的監控系統。

✤ 注意:此整合的主要目的是使用Prometheus Monitoring System軟體監控安全惡意軟體分析裝置的統計資訊。其中包括介面、流量統計資訊等。

設定

步驟 1.登入到Secure Malware Analytics Appliance,導航到Operations > Metrics以查詢API金鑰和 基本身份驗證密碼。

步驟 2.安裝Prometheus Server軟體: <u>https://prometheus.io/download/</u>

步驟 3. 建立.yml檔案,該檔案必須名為prometheus.ym1,並且必須具有以下詳細資訊:

```
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
```

步驟 4.運行CLI命令以生成用於身份驗證的JWT令牌,如上述配置檔案中所指定:

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

步驟 5.運行此命令以驗證令牌的Expiration Date欄位(1小時有效性)。

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

以下命令輸出示例:

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





步驟 6.獲取服務的配置,在登入到opadmin介面後,從UI輸入以下行:

<#root>

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

步驟 7.重新啟動Prometheus服務後, 配置將被啟用。

步驟 8.訪問Prometheus頁面:

<#root>

http://localhost:9090/graph

您可以看到Secure Malware Analytics Appliance服務處於「UP」狀態,如圖所示。

Promethe	us Alerts Graph Status * Help New UI					
Targe	ets					
All Unh	ealthy Collapse All					
metrics (8/8 up) show less					
Endpoint		State	Labels		Last Scrape	Scrape Duration Error
5	:443/metrics/v1/service/fav2	UP	instance=*10	543" 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
	o443/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	5443" 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

驗證

您可以看到從Secure Malware Analytics Applianced裝置接收的資料,並根據自己的要求檢視中的 指標,如圖所示。

node_n	etwork_transmit_bytes_total			Load time Resolution Total time s	132ms 145 Jeries 8
Execute	node_retwork_transmit_L #			Remove G	iraph
Graph	Console				
	- in • • • • voni • • • • • • • • • • • • • • • • • • •				
600 -					
400					
200 -					
0	114	15.45	n ni	00.15	
	B nole peterak (securi byte, http://www.inex/07.jestar (secure-inex/or experier') B nole peterak (securi byte, http://www.inex/or inex/or ine				
	sole_shiwe_barren_byte_bolidence='wp128rifY', 447 yib='metric1'annica'-toole-equiter') sole_shiwe_barren_byte_bolidence='wp128rifY', 447 yib='metric1'annica'-toole-equiter') sole_shiwe_barren_byte_bolidence='dp1'ntarco r=metric1'annica'-toole-equiter')				
	(* stratege start - storter, f. stratege start - storter, start - storter, start - storter, start - storter,				
node_n	etwork/receive_bytes_total			Load time th Resultion to	76ms Hs
node_n Execute	etwork_receive_bytes_total node_retwork_receive_by #			Last Gree T Reputiers I Not Tries a	76ms Nas ries 8
node_n Execute Graph	etwork_receive_bytes_total node_network_receive_by # Console			Laston Remotes Not fire a	Dens Ns riei 8 raph
node_n Execute Graph	etwork_receive_bytes_total console total			Lead from 1 Remove Or Remove Or	ries 8
node_n Execute Graph	etwork_presive_pytes_total reductive_pytes_total Console To the the total total Res 00 Oracled			List fore Manufacts Sea force Remove Gr	Olens tids ties 8 raph
node_n Execute Graph	eteody.receive.jbyter_total roddy.receive.jbyter_total Console Total Res. 00 Outloaded			Lias from 1 Non de la Remove Cr	Olers 145 ries 8 raph
Graph 5000- 000- 000-	eterost, receive, Joytes, total reder, receive, Joy e Console to the consol			Lia fine 1 Nos fine a Remove Gr	Oles 168 ries 8 raph
node_n Execute Graph 1000- 000- 000- 000-	etwork_receive_bytes_total console b console b console conso			Las fine to She fine a	Olers His Head
node_n Execute Graph 1000- 000- 000- 000- 000- 000- 000- 000-	eteority.receive_Jujest_total			List from the Brandon is Norman and Array Contract of	Chins tas ries 8 raph
node_n Execute Graph 1000- 800- 800- 800- 800- 800- 800- 800	eteody.veoley.byter_total resolv_veoley.byter_total consule total_veoley.byter_total total_veoley.byter_total_veo			List fret 1 Render	Olers 143 ries 8 caph
node,n Decote (6sph) 1000 000 000 000 000 000 000 000 000 0	eteody.receive.jbyter_total reddy.receive.jbyter_total Console	224		Lia the the New York of the Ne	Olers 144 eres 8
node,nr. Execute Scaph 1000 100 100 100 100 100 100 1	teroch, vecelve, bytes, usual reduct, vecelve, bytes, usual concele to the	224	62.00	List for 1 No they Recove Gr	Olers tis ties 8
node,n Create Graph 1000- 100-	eteods/ucceive_bytes_total	226	99.90	List errer bier bier errer bier bi	Olers No ries 8 caph

✤ 注意:此功能僅用於收集特定資料。資料流管理是Prometheus伺服器的職責。 思科TAC方面不提供支援的故障排除,您可以聯絡第三方供應商支援獲取其他功能支援。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。