使用Prometheus監控軟體配置安全惡意軟體分析 裝置

目錄

簡介

<u>必要條件</u>

需求

<u>背景資訊</u>

設定

驗證

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

"user": "threatgrid",
"pw_method": "password",

"addr": "

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: https://prometheus.io/download/

步驟 3. 建立.yml檔案,該檔案必須名為prometheus.yml,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:
```

"exp": 1604098219, "iat": 1604094619, "iss": " "nbf": 1604094619



🍑 註:時間以Epoch格式顯示。

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

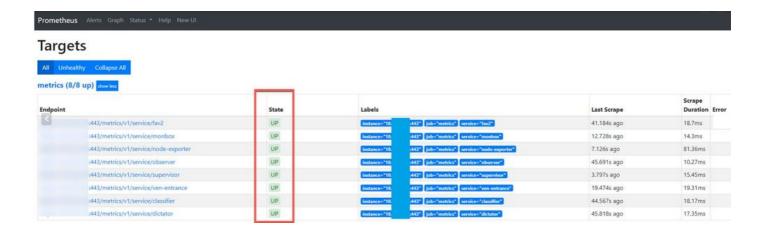
步驟 7.重新啟動Prometheus服務後,配置將被啟用。

步驟 8.訪問Prometheus頁面:

<#root>

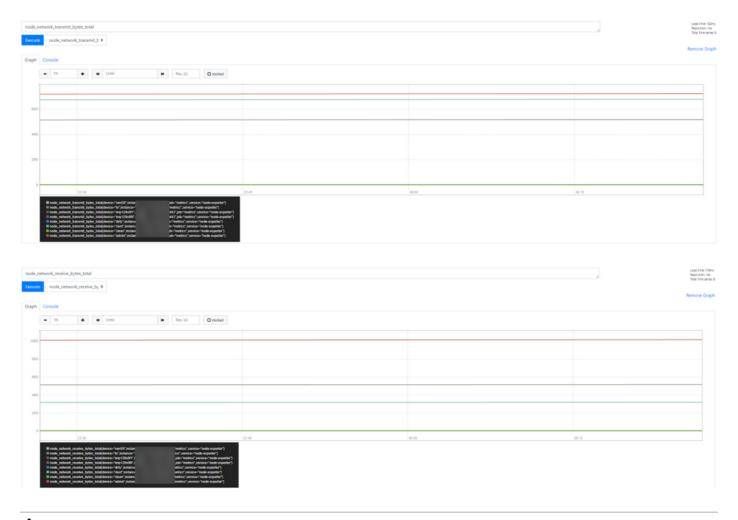
http://localhost:9090/graph

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



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。



▶ 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)。