

Prometheusモニタリングソフトウェアを使用したセキュアなマルウェア分析アプライアンスの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[背景説明](#)

[設定](#)

[確認](#)

はじめに

このドキュメントでは、Secure Malware Analytics Appliance(SMA)サービスメトリックデータをPrometheusモニタリングソフトウェアにエクスポートする手順について説明します。

著者 : Cisco TAC エンジニア

前提条件

Secure Malware Analytics ApplianceおよびPrometheusソフトウェアに関する知識があることが推奨されます。


要件

- Secure Malware Analyticsアプライアンス (バージョン2.13以降)
- Prometheusソフトウェアライセンス

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

TApplianceで実行されているRiemann/Elastic検索ベースの監視システムは、Secure Malware Analytics Applianceバージョン2.13以降のPrometheusベースの監視に置き換えられました。

 注：この統合の主な目的は、Prometheus Monitoring Systemソフトウェアを使用して Secure Malware Analytics アプライアンスの統計情報を監視することです。これには、インターフェイス、トラフィック統計情報などが含まれます。

設定

ステップ 1：Secure Malware Analytics Applianceにログインし、[Operations] > [Metrics]に移動して、APIキーと基本認証パスワードを見つけます。

ステップ 2：Prometheus Serverソフトウェアのインストール：<https://prometheus.io/download/>

ステップ 3：.ymlファイルを作成します。このファイルはprometheus.ymlと呼ばれ、次の詳細が含まれている必要があります。

```
scrape_configs:
  - job_name: 'metrics'
bearer_token_file: 'token.jwt'
scheme: https

file_sd_configs:
  - files:
    - 'targets.json'

relabel_configs:
  - source_labels: [__address__]
    regex: '([^/]+(/.*))'
    target_label: __metrics_path__
    # capture '/...' part
    # change metrics path
  - source_labels: [__address__]
    regex: '([^/]+)/.*'
    target_label: __address__
    # capture host:port
    # change target
```

ステップ 4：CLIコマンドを実行して、認証用のJWTトークンを生成します（上記のコンフィギュレーションファイルで指定されています）。

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

ステップ 5：このコマンドを実行して、トークンのExpiration Dateフィールド（1時間の有効期間）を確認します。

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

次のコマンド出力例を参照してください。

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

  ",

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

  ",

  "nbf": 1604094619
}
```

 注：時間はエポック形式で表示されます。

手順 6：サービスの設定を取得し、opadminインターフェイスにログインした後、UIから次の行を入力します。

<#root>

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

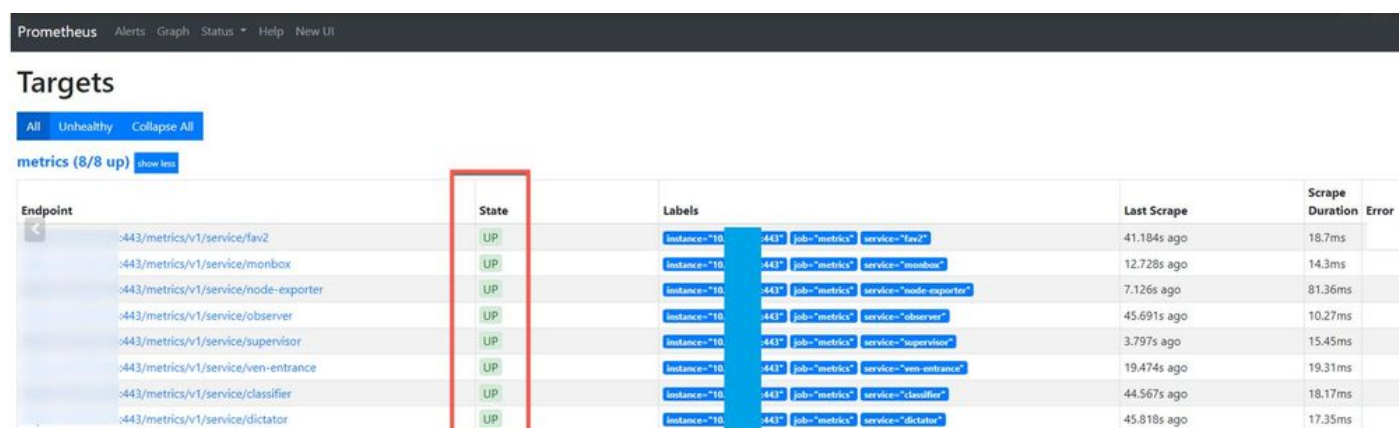
手順 7：Prometheusサービスを再起動すると、構成がアクティブ化されます。

ステップ 8：Prometheusページにアクセスします。

<#root>

```
http://localhost:9090/graph
```

図に示すように、Secure Malware Analyticsアプライアンスサービスが「UP」状態であることが確認できます。




Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
>-443/metrics/v1/service/flav2	UP	instance="10...-443" job="metrics" service="flav2"	41.184s ago	18.7ms	
>-443/metrics/v1/service/monbox	UP	instance="10...-443" job="metrics" service="monbox"	12.728s ago	14.3ms	
>-443/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...-443" 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	

確認

Secure Malware Analyticsアプリケーションデバイスからデータを受信し、図に示すように、独自の要件に基づいてメトリックを確認できます。



 注：この機能は、特定のデータを収集する場合にのみ機能します。データフロー管理はPrometheusサーバーの責任です。Cisco TAC側でサポートされているトラブルシューティングはありません。サードパーティ

 ベンダーのサポートに連絡して、追加の機能サポートを受けることができます。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。