Konfigurieren einer sicheren Malware Analytics-Appliance mithilfe der Prometheus Monitoring-Software

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Hintergrundinformationen](#)
[Konfigurieren](#)
[Überprüfung](#)

Einleitung

In diesem Dokument werden die Schritte zum Exportieren der Kennzahlen für den Service Secure Malware Analytics Appliance in die Prometheus Monitoring Software beschrieben.

Unterstützt von Cisco TAC-Technikern.

Voraussetzungen

Cisco empfiehlt, über Kenntnisse der Secure Malware Analytics Appliance und der Prometheus-Software zu verfügen.

Anforderungen

- Secure Malware Analytics Appliance (ab Version 2.13)
- Prometheus Softwarelizenz

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

TDas auf der Appliance ausgeführte Suchsystem Riemann/Elastic wird durch die Prometheus-basierte Überwachung ab Version 2.13 von Secure Malware Analytics Appliance ersetzt.

> **Hinweis**: Der Hauptzweck dieser Integration ist die Überwachung der Statistiken Ihrer Secure Malware Analytics Appliance mithilfe der Prometheus Monitoring System-Software. Dazu gehören eine Schnittstelle, Verkehrsstatistiken usw.

Konfigurieren

Schritt 1: Melden Sie sich bei der Secure Malware Analytics Appliance an, navigieren Sie zu Operations > Metrics (Betrieb > Kennzahlen), um den API-Schlüssel und das Standardauthentifizierungskennwort zu finden.

Schritt 2: Installieren Sie Prometheus Server-Software: https://prometheus.io/download/

Schritt 3: Erstellen Sie eine .yml-Datei, die `als` .yml `bezeichnet` werden muss`.yml` und muss folgende Details enthalten:

```
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
```

Schritt 4: Führen Sie den CLI-Befehl aus, um ein JWT-Token für die Authentifizierung zu generieren, wie in der oben angegebenen Konfigurationsdatei angegeben:

```
curl -k -s -XPOST -d 'user=threatgrid&password=<TGA Password>&method=password' "https://_opadmin
IP_:443/auth?method=password" | tee token.jwt
```

Schritt 5: Führen Sie diesen Befehl aus, um das Feld für das Ablaufdatum des Tokens zu überprüfen (Gültigkeit von 1 Stunde).

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

Befehlsausgabe Beispiel unten:

```
{
"user": "threatgrid",
"pw_method": "password",
"addr": "
"exp": 1604098219,
"iat": 1604094619,
"iss": "
"nbf": 1604094619
}
```

Anmerkung: Die Uhrzeit wird im Epochformat angezeigt.

Schritt 6: Pull the configuration services, after login in opadmin interface, enter this line from the

UI:

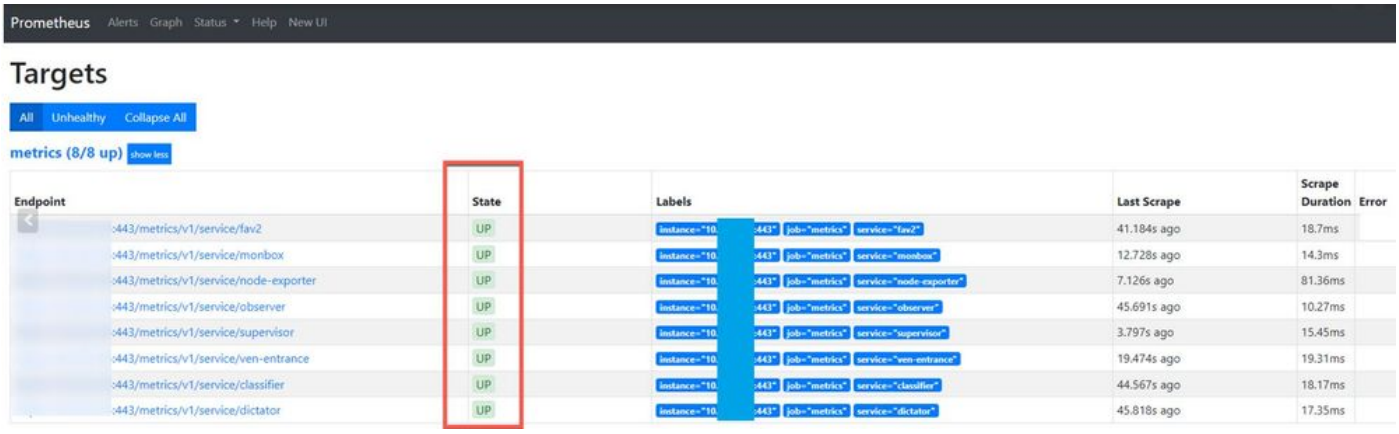
`https://_opadmin IP_/metrics/v1/config`

Schritt 7: Nach dem Neustart des Prometheus-Dienstes wird die Konfiguration aktiviert.

Schritt 8: Öffnen Sie die Prometheus-Seite:

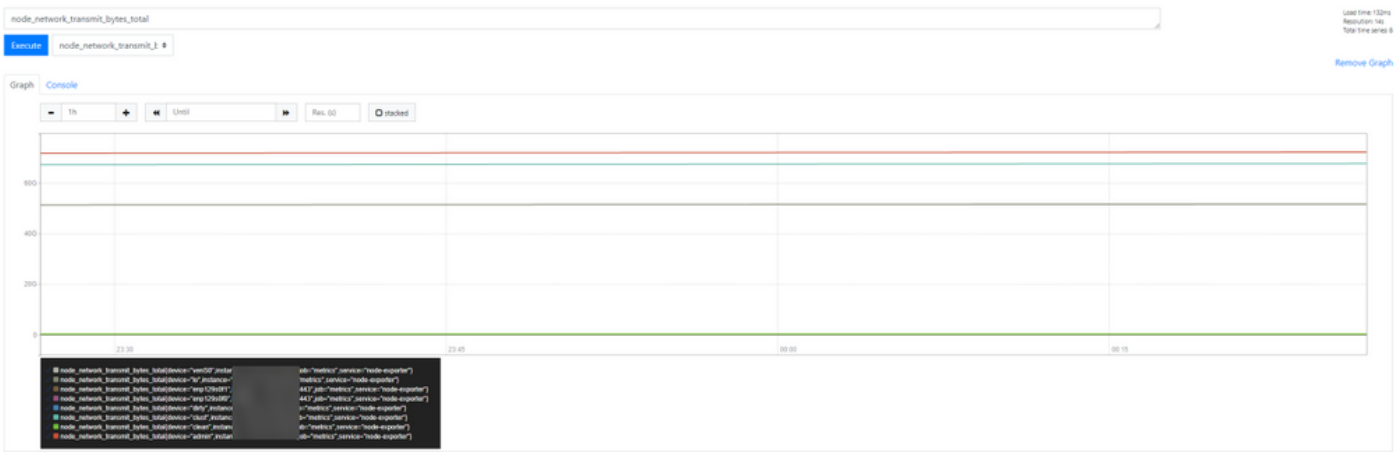
`http://localhost:9090/graph`

Sie können die Secure Malware Analytics Appliance-Services im **"UP"-**Status sehen, wie im Bild gezeigt.



Überprüfung

Sie können sehen, wie die Daten von den Secure Malware Analytics Applianced-Geräten empfangen werden, und die Kennzahlen entsprechend Ihrer Anforderungen überprüfen, wie im Bild gezeigt.



Anmerkung: Diese Funktion dient nur zum Sammeln bestimmter Daten. Das Datenflussmanagement ist Aufgabe des Prometheus Servers.
Für die Fehlerbehebung von Cisco TAC ist kein Support verfügbar. Sie können sich an den Support eines Drittanbieters wenden, um zusätzliche Funktionen zu erhalten.