Configure Secure Malware Analytics Appliance with Prometheus Monitoring Software

Contents

Introduction

This document describes the steps to export Secure Malware Analytics Appliance service metrics data to Prometheus Monitoring Software.

Contributed by Cisco TAC Engineers.

Prerequisites

Cisco recommends that you have knowledge of Secure Malware Analytics Appliance and Prometheus software.

Requirements

- Secure Malware Analytics Appliance (version 2.13 onwards)
- Prometheus software license

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

The Riemann/Elastic search-based monitoring system running on the Appliance is replaced by Prometheus-based monitoring from Secure Malware Analytics Appliance version 2.13 onwards.

> **Note**: The main purpose of this integration is to monitor the statistics of your Secure Malware Analytics Appliance using Prometheus Monitoring System software. This includes an interface, traffic statistics, etc.

Configure

Step 1. Log in to Secure Malware Analytics Appliance, navigate to Operations > Metrics in order to find the API key and Basic Authentication Password.

Step 2. Install Prometheus Server software: https://prometheus.io/download/

Step 3. Create a .yml file, it must be called`prometheus.yml` and it must has this details:

```
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
```

Step 4. Run the CLI command in order to generate a JWT Token for authentication, as it is specified in the configuration file above:

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

Step 5. Run this command to verify the Expiration Date field for the token (1 Hour Validity).

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

Command output example below:

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

> **Note**: The time is displayed in Epoch format.

Step 6. Pull the configuration of services, after login into opadmin interface, enter this line from the UI:

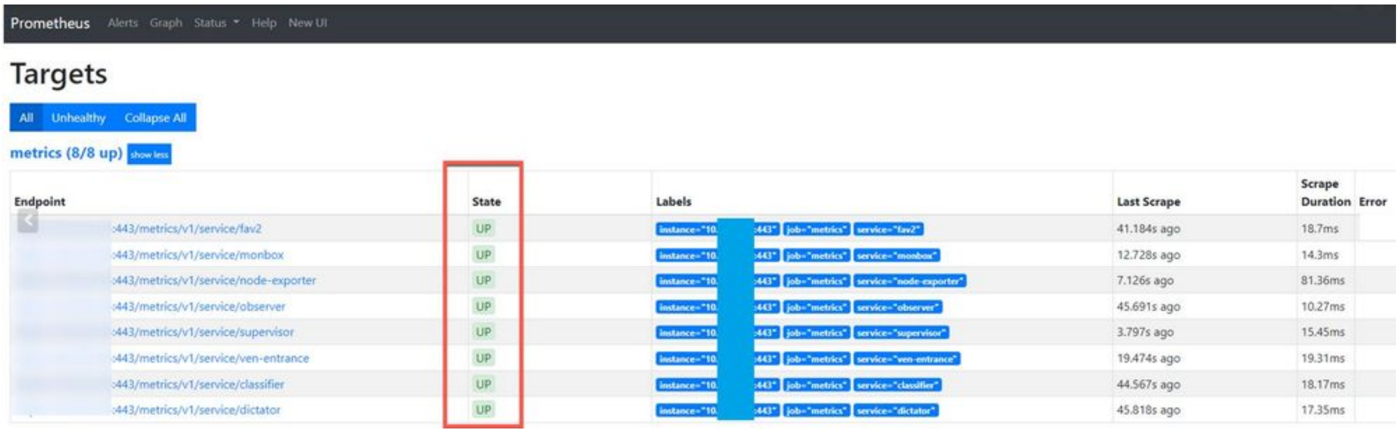
```
https://_opadmin IP_/metrics/v1/config
```

Step 7. After restarting the Prometheus service, the configuration is activated.

Step 8. Access the Prometheus page:

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

You can see the Secure Malware Analytics Appliance services in **"UP"** state, as shown in the mage.



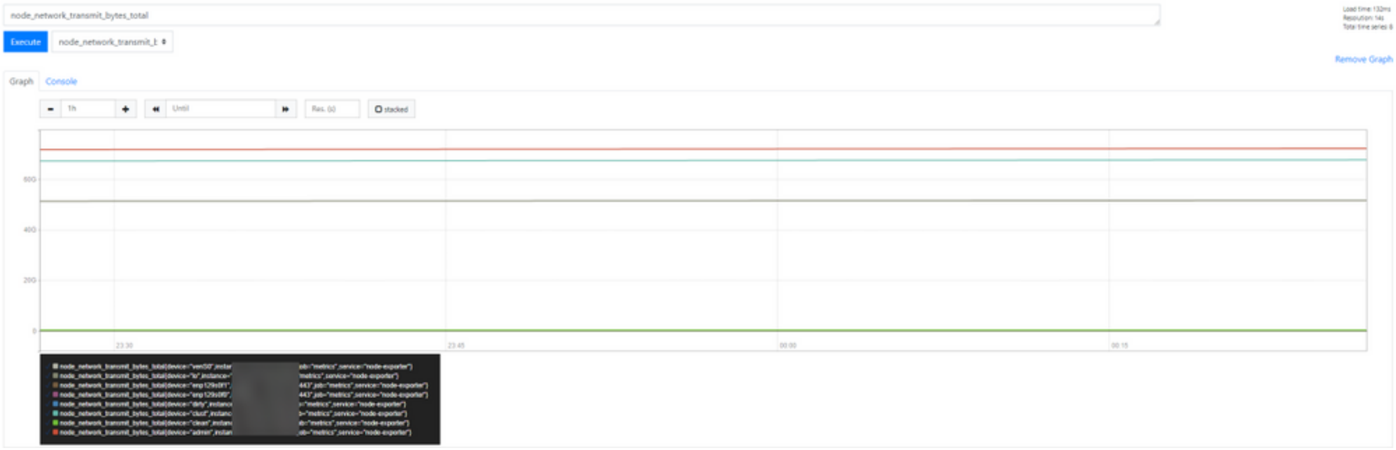
Targets

metrics (8/8 up)

Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
[redacted]:443/metrics/v1/service/fav2	UP	instance="10.[redacted]:443" job="metrics" service="fav2"	41.184s ago	18.7ms	
[redacted]:443/metrics/v1/service/monbox	UP	instance="10.[redacted]:443" job="metrics" service="monbox"	12.728s ago	14.3ms	
[redacted]:443/metrics/v1/service/node-exporter	UP	instance="10.[redacted]:443" job="metrics" service="node-exporter"	7.126s ago	81.36ms	
[redacted]:443/metrics/v1/service/observer	UP	instance="10.[redacted]:443" job="metrics" service="observer"	45.691s ago	10.27ms	
[redacted]:443/metrics/v1/service/supervisor	UP	instance="10.[redacted]:443" job="metrics" service="supervisor"	3.797s ago	15.45ms	
[redacted]:443/metrics/v1/service/ven-entrance	UP	instance="10.[redacted]:443" job="metrics" service="ven-entrance"	19.474s ago	19.31ms	
[redacted]:443/metrics/v1/service/classifier	UP	instance="10.[redacted]:443" job="metrics" service="classifier"	44.567s ago	18.17ms	
[redacted]:443/metrics/v1/service/dictator	UP	instance="10.[redacted]:443" job="metrics" service="dictator"	45.818s ago	17.35ms	

Verify

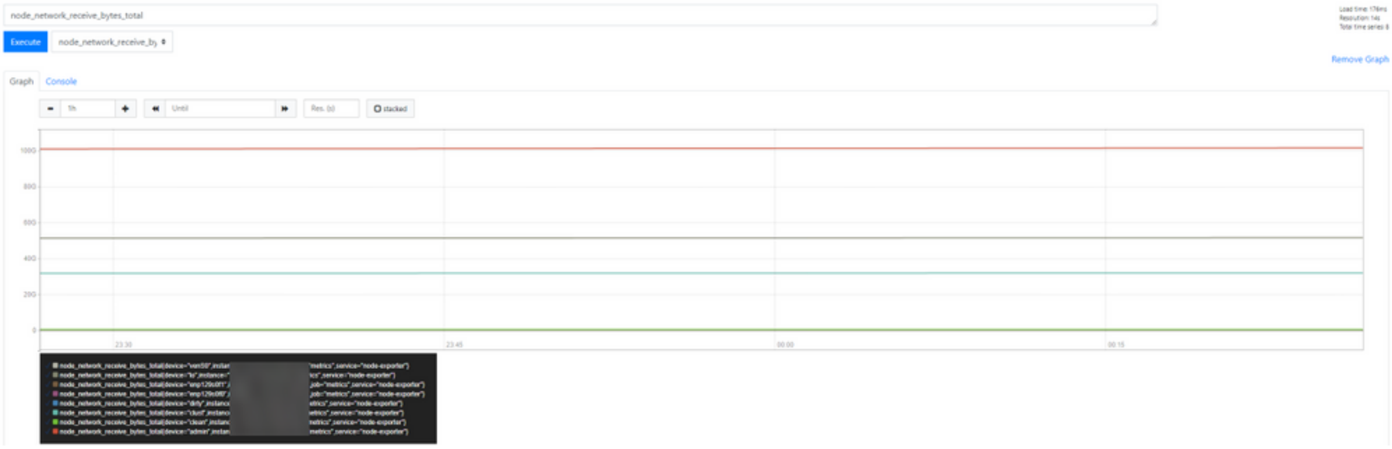
You can see the data is received from the Secure Malware Analytics Applianced devices, review the metrics in base on your own requirements, as shown in the mage.



node_network_transmit_bytes_total

Load time: 132ms
Resolution: 14s
Total time series: 8

- node_network_transmit_bytes_total{device="ven50",instan[redacted]ob="metrics",service="node-exporter"}
- node_network_transmit_bytes_total{device="lo",instance="[redacted]metrics",service="node-exporter"}
- node_network_transmit_bytes_total{device="enp129s0f1",[redacted]443",job="metrics",service="node-exporter"}
- node_network_transmit_bytes_total{device="enp129s0f0",[redacted]443",job="metrics",service="node-exporter"}
- node_network_transmit_bytes_total{device="dirty",instanc[redacted]="metrics",service="node-exporter"}
- node_network_transmit_bytes_total{device="clust",instanc[redacted]b="metrics",service="node-exporter"}
- node_network_transmit_bytes_total{device="clean",instanc[redacted]ob="metrics",service="node-exporter"}
- node_network_transmit_bytes_total{device="admin",instan[redacted]ob="metrics",service="node-exporter"}



node_network_receive_bytes_total

Load time: 176ms
Resolution: 14s
Total time series: 8

- node_network_receive_bytes_total{device="ven50",instan[redacted]metrics",service="node-exporter"}
- node_network_receive_bytes_total{device="lo",instance="[redacted]ics",service="node-exporter"}
- node_network_receive_bytes_total{device="enp129s0f1",[redacted]job="metrics",service="node-exporter"}
- node_network_receive_bytes_total{device="enp129s0f0",[redacted]job="metrics",service="node-exporter"}
- node_network_receive_bytes_total{device="dirty",instanc[redacted]etrics",service="node-exporter"}
- node_network_receive_bytes_total{device="clust",instanc[redacted]etrics",service="node-exporter"}
- node_network_receive_bytes_total{device="clean",instanc[redacted]etrics",service="node-exporter"}
- node_network_receive_bytes_total{device="admin",instan[redacted]metrics",service="node-exporter"}

Note: This feature works only to collect specific data. Data flow management is the

responsibility of the Prometheus server.
There is no supported troubleshooting from Cisco TAC side, you can reach out 3rd party vendor support for additional feature support.