Configuración de Secure Malware Analytics Appliance con Prometheus Monitoring Software

Contenido

Introducción

Este documento describe los pasos para exportar los datos de las métricas de servicio de Secure Malware Analytics Appliance al Prometheus Monitoring Software.

Contribuido por ingenieros del TAC de Cisco.

Prerequisites

Cisco recomienda que tenga conocimiento de Secure Malware Analytics Appliance y del software Prometheus.

Requirements

- Dispositivo de análisis de malware seguro (versión 2.13 en adelante)
- Licencia de software Prometheus

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.

Antecedentes

TEl sistema de supervisión basado en búsquedas Riemann/Elastic que se ejecuta en el dispositivo se reemplaza por el monitoreo basado en Prometheus de Secure Malware Analytics Appliance versión 2.13 en adelante.

> **Nota**: El objetivo principal de esta integración es supervisar las estadísticas de su dispositivo de análisis de malware seguro mediante el software Prometheus Monitoring System. Esto incluye una interfaz, estadísticas de tráfico, etc.

Configurar

Paso 1. Inicie sesión en Secure Malware Analytics Appliance, navegue hasta Operaciones > Métricas para encontrar la clave API y la contraseña de autenticación básica.

Paso 2. Instalar el software Prometheus Server: https://prometheus.io/download/

Paso 3. Cree un archivo .yml, debe ser `llamado prometheus.yml` y debe tener estos detalles:

```
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
```

Paso 4. Ejecute el comando CLI para generar un token JWT para la autenticación, como se especifica en el archivo de configuración anterior:

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

Paso 5. Ejecute este comando para verificar el campo Fecha de vencimiento del token (1 hora de validez).

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

Ejemplo de resultado del comando a continuación:

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

Nota: La hora se muestra en formato Epoch.

Paso 6. Tire de la configuración de los servicios, después de iniciar sesión en la interfaz opadmin, ingrese esta línea desde la interfaz de usuario:

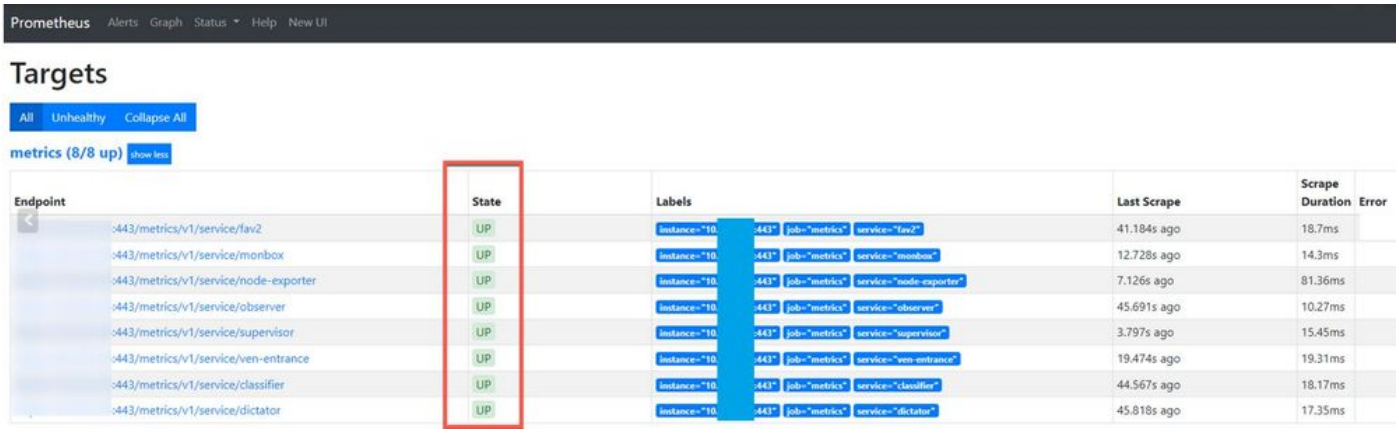
https://_opadmin IP_/metrics/v1/config

Paso 7. Después de reiniciar el servicio Prometheus, se activa la configuración.

Paso 8. Acceda a la página Prometheus:

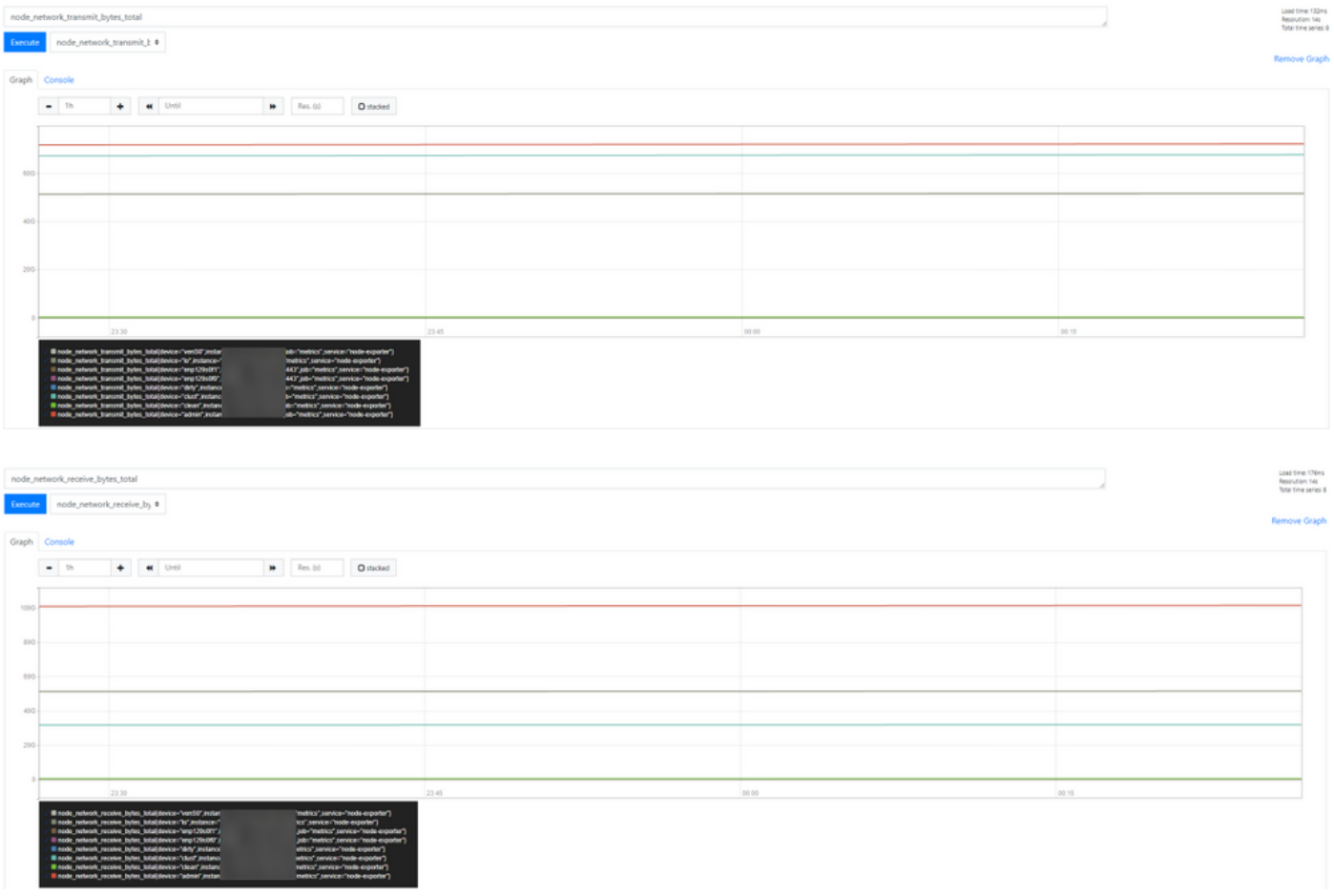
http://localhost:9090/graph

Puede ver los servicios Secure Malware Analytics Appliance en el estado **"UP"** , como se muestra en la imagen.



Verificación

Puede ver los datos recibidos de los dispositivos Secure Malware Analytics, revisar las métricas en base a sus propios requisitos, como se muestra en la imagen.



Nota: Esta función sólo funciona para recopilar datos específicos. La gestión del flujo de datos es responsabilidad del servidor Prometheus.
No se admite la resolución de problemas desde el lado del TAC de Cisco. Puede ponerse en contacto con el soporte de otros proveedores para obtener asistencia sobre funciones adicionales.