تكوين جهاز تحليلات البرامج الضارة الآمنة باستخدام برنامج مراقبة Prometheus

المحتويات

المقدمة

يصف هذا المستند الخطوات اللازمة لتصدير بيانات مقاييس خدمة تحليلات البرامج الضارة الآمنة إلى برنامج مراقبة Prometheus.

تمت المساهمة بواسطة مهندسو Cisco TAC.

المتطلبات الأساسية

توصي Cisco بأن تكون لديك معرفة بأجهزة تحليل البرامج الضارة الآمنة وبرامج Prometheus.

المتطلبات

- جهاز Secure Ware Analytics (الإصدار 2.13 وما بعده)
- ترخيص برنامج Prometheus

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

Tتم إستبدال نظام المراقبة القائم على البرامج/المرنة القائم على البحث والذي يتم تشغيله على الجهاز بمراقبة قائمة على بروميثيوس من جهاز تحليل البرامج الضارة الآمن الإصدار 2.13 وما بعده.

ملاحظة: الغرض الرئيسي من هذا التكامل هو مراقبة إحصائيات جهاز Secure Malware

Analytics باستخدام برنامج Prometheus Monitoring System. ويتضمن ذلك واجهة واجصاءات حركة مرور البيانات وما إلى ذلك.

التكوين

الخطوة 1. قم بتسجيل الدخول إلى جهاز تحليلات البرامج الضارة الآمن، انتقل إلى Operations > Metrics للعثور على مفتاح API وكلمة مرور المصادقة الأساسية.

الخطوة 2. تثبيت برنامج خادم Prometheus: https://prometheus.io/download/

الخطوة 3. إنشاء ملف .yml، يجب أن يكون `CallPrometheus.yml` ويجب أن يحتوي على هذه التفاصيل:

```
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
```

الخطوة 4. قم بتشغيل أمر واجهة سطر الأوامر (CLI) لإنشاء رمز JWT مميز للمصادقة، كما هو محدد في ملف التكوين أعلاه:

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

الخطوة 5. قم بتشغيل هذا الأمر للتحقق من حقل تاريخ انتهاء الصلاحية للرمز المميز (صلاحية ساعة واحدة).

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

مثال إخراج الأمر أدناه:

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

      ",

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

      ",

  "nbf": 1604094619
}
```


ملاحظة: الوقت معروض بتنسيق epoch.

الخطوة 6. اسحب تكوين الخدمات، بعد تسجيل الدخول إلى واجهة OpenAdmin، أدخل هذا السطر من واجهة المستخدم:

<#root>

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

الخطوة 7. بعد إعادة تشغيل خدمة Prometheus، يتم تنشيط التكوين.

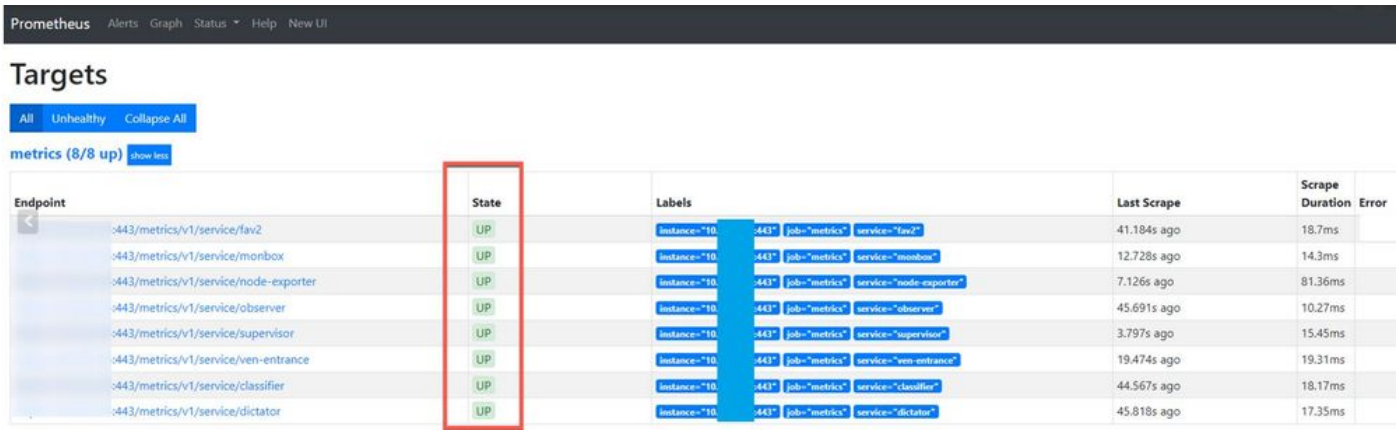
الخطوة 8. الوصول إلى صفحة Prometheus:

<#root>

http://localhost:9090/graph

يمكنك رؤية خدمات جهاز تحليلات البرامج الضارة الآمنة في حالة "UP"، كما هو موضح في

التصميم.



التحقق من الصحة

يمكنك مشاهدة البيانات التي يتم استقبالها من أجهزة Secure Malware Analytics، ومراجعة المقاييس الموجودة في الأساس بناء على متطلباتك الخاصة، كما هو موضح في التصميم.

ملاحظة: تعمل هذه الميزة فقط لجمع بيانات معينة. تعد إدارة تدفق البيانات مسؤولية خادم Prometheus.
لا يوجد أستكشاف الأخطاء وإصلاحها مدعوم من جانب Cisco TAC، يمكنك الوصول إلى

دعم بائع الطرف الثالث للحصول على دعم ميزة إضافي.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).