

使用Prometheus监控软件配置安全恶意软件分析设备

目录

[简介](#)

[先决条件](#)

[要求](#)

[背景信息](#)

[配置](#)

[验证](#)

简介

本文档介绍将安全恶意软件分析设备服务指标数据导出到Prometheus监控软件的步骤。

由思科 TAC 工程师撰稿。

先决条件

思科建议您了解安全恶意软件分析设备和Prometheus软件。


要求

- 安全恶意软件分析设备（版本2.13及更高版本）
- Prometheus软件许可证

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

T从安全恶意软件分析设备2.13版开始，设备上运行的基于黎曼/弹性搜索的监控系统将被基于Prometheus的监控取代。

 **注意：**此集成的主要目的是使用Prometheus Monitoring System软件监控安全恶意软件分析设备的统计信息。其中包括接口、流量统计信息等。

配置

步骤1:登录到安全恶意软件分析设备，导航到Operations > Metrics以查找API密钥和基本身份验证密码。

第二步：安装Prometheus Server软件：<https://prometheus.io/download/>

第三步：创建.yml文件，该文件必须命名为prometheus.yml，并且必须具有以下详细信息：

```
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
```

第四步：运行CLI命令以生成用于身份验证的JWT令牌，如上述配置文件中指定：

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

第五步：运行此命令验证令牌的Expiration Date字段（1小时有效性）。

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

以下命令输出示例：

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

```
"
```

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

```
"
```

```
"nbf": 1604094619  
}
```

 注：时间以Epoch格式显示。

第六步：提取服务配置，在登录到opadmin界面后，从UI输入此行：

```
<#root>
```

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

步骤 7.重新启动Prometheus服务后，配置将激活。

步骤 8访问Prometheus页面：

```
<#root>
```

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

您可以看到Secure Malware Analytics设备服务处于UP状态，如图所示。

Targets

All Unhealthy Collapse All

metrics (8/8 up) show less

Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
-443/metrics/v1/service/fav2	UP	instance="10", -443, job="metrics", service="fav2"	41.184s ago	18.7ms	
-443/metrics/v1/service/moonbox	UP	instance="10", -443, job="metrics", service="moonbox"	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	

验证

您可以查看从安全恶意软件分析设备接收的数据，并根据自己的要求查看中的指标，如图所示。



注意：此功能仅用于收集特定数据。数据流管理由Prometheus服务器负责。思科TAC端不支持故障排除，您可以联系第三方供应商支持获取其他功能支持。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。