

Prometheus Monitoring Software로 Secure Malware Analytics Appliance 구성

목차

- [소개](#)
 - [사전 요구 사항](#)
 - [요구 사항](#)
 - [배경 정보](#)
 - [구성](#)
 - [다음을 확인합니다.](#)
-

소개

이 문서에서는 Secure Malware Analytics Appliance 서비스 메트릭 데이터를 Prometheus Monitoring Software로 내보내는 단계를 설명합니다.

기고자: Cisco TAC 엔지니어

사전 요구 사항

Secure Malware Analytics Appliance 및 Prometheus 소프트웨어에 대한 지식이 있는 것이 좋습니다.


요구 사항


- Secure Malware Analytics Appliance(버전 2.13 이후)
- Prometheus 소프트웨어 라이선스

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

T어플라이언스에서 실행 중인 Riemann/Elastic 검색 기반 모니터링 시스템은 Secure Malware Analytics Appliance 버전 2.13부터 Prometheus 기반 모니터링으로 교체됩니다.

 참고: 이 통합의 주요 목적은 Prometheus Monitoring System 소프트웨어를 사용하여 Secure Malware Analytics Appliance의 통계를 모니터링하는 것입니다. 여기에는 인터페이스, 트래픽

 통계 등이 포함됩니다.

구성

1단계. Secure Malware Analytics Appliance에 로그인하고 Operations(운영) > Metrics(메트릭)로 이동하여 API 키 및 Basic Authentication Password(기본 인증 비밀번호)를 찾습니다.

2단계. Prometheus Server 소프트웨어 설치: <https://prometheus.io/download/>

3단계. .yml 파일을 만들려면 prometheus.yml이라고 하고 다음 세부 정보를 포함해야 합니다.

```
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
```

4단계. 위의 컨피그레이션 파일에 지정된 대로 인증을 위한 JWT 토큰을 생성하려면 CLI 명령을 실행합니다.

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

5단계. 이 명령을 실행하여 토큰의 Expiration Date(만료일) 필드를 확인합니다(1시간 유효성).

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

아래의 명령 출력 예:

```
{
  "user": "threatgrid",
```

```
"pw_method": "password",
"addr": "

",

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

",

"nbf": 1604094619
}
```

 참고: 시간은 Epoch 형식으로 표시됩니다.

6단계. 서비스 컨피그레이션을 가져오고 opadmin 인터페이스에 로그인한 후 UI에서 다음 줄을 입력합니다.

<#root>

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

7단계. Prometheus 서비스를 다시 시작하면 컨피그레이션이 활성화됩니다.

8단계. Prometheus 페이지에 액세스합니다.

<#root>

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

그림과 같이 Secure Malware Analytics Appliance 서비스가 "UP" 상태로 표시됩니다.

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/monbox	UP	instance="10", -443", job="metrics", service="monbox"	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	

다음을 확인합니다.

Secure Malware Analytics Applied 디바이스에서 수신된 데이터를 확인하고, 그림과 같이 사용자 요구 사항에 따라 메트릭을 검토할 수 있습니다.



참고: 이 기능은 특정 데이터를 수집하는 데만 작동합니다. 데이터 흐름 관리는 Prometheus 서버의 책임입니다.

Cisco TAC 측에서 지원하는 트러블슈팅은 없으며, 서드파티 벤더에 연락하여 추가 기능 지원을 받을 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.