Secure Malware Analytics-applicatie met Proxy Monitoring Software

Inhoud

Inleiding Voorwaarden Vereisten Achtergrondinformatie Configureren Verifiëren

Inleiding

Dit document beschrijft de stappen om Secure Malware Analytics-servicegegevens te exporteren naar Prometheus Monitoring Software.

Bijgedragen door Cisco TAC-engineers.

Voorwaarden

Cisco raadt u aan kennis te hebben over Secure Malware Analytics-applicatie en Prometheussoftware.

Vereisten

- Secure Malware Analytics-applicatie (versie 2.13 vanaf)
- Prometheus-softwarelicentie

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

OHet Riemann/Elastic search-Based Monitoring System dat op het apparaat wordt uitgevoerd, wordt vervangen door Prometheus-gebaseerde controle vanaf Secure Malware Analytics-applicatie, versie 2.13.

Opmerking: het belangrijkste doel van deze integratie is om de statistieken van uw Secure Malware Analytics-applicatie te controleren met behulp van Prometheus Monitoring Systemsoftware. Dit omvat een interface, verkeersstatistieken, enz.

Configureren

Stap 1. Meld u aan bij Secure Malware Analytics-applicatie, navigeer naar Operations > Metriek om de API-toets en het Wachtwoord voor basisverificatie te vinden.

Stap 2. Installeer de software van de Prometheus-server: https://prometheus.io/download/

Stap 3. Maak een .yml-bestand, dit moet prometheus.yml worden genoemd en moet deze gegevens hebben:

```
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
```

Stap 4. Start de CLI-opdracht om een JWT Token voor verificatie te genereren, zoals beschreven in het configuratie bestand hierboven:

```
curl -k -s -XPOST -d 'user=threatgrid&password=<TGA Password>&method=password' "https://_opadmin
IP_:443/auth?method=password" | tee token.jwt
Stap 5. Start deze opdracht om het veld Vervaldatum voor het token te controleren (1 uur
geldigheid).
```

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

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

Opmerking: De tijd wordt in Epoch-indeling weergegeven.

Stap 6. Trek de configuratie van de diensten, na inloggen in opadmin-interface, deze lijn van de UI in:

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

Stap 7. Na het opnieuw starten van de Prometheus-service, wordt de configuratie geactiveerd.

Stap 8. Access de Prometheus-pagina:

http://localhost:9090/graph

U kunt de services van de Secure Malware Analytics in de staat "UP" zien, zoals in de afbeelding.

Promethe	us Alerts Graph Status * Help New UI					
Targe	ets					
All Unh	ealthy Collapse All					
metrics (8	5/8 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
	o443/metrics/v1/service/node-exporter	UP	instance-*10.	x443" [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.	s443" job-"metrics" service-"supervisor"	3.797s ago	15.45ms
	:443/metrics/v1/service/ven-entrance	UP	instance-*10.	1443" 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

Verifiëren

U kunt zien dat de gegevens van de beveiligde Malware Analytics-apparaten worden ontvangen, en u kunt de parameters op basis van uw eigen vereisten bekijken, zoals in de afbeelding wordt weergegeven.



Opmerking: Deze functie werkt alleen om specifieke gegevens te verzamelen. Beheer van gegevensstromen valt onder de verantwoordelijkheid van de Prometheus-server. Er is geen ondersteunde oplossing vanuit Cisco TAC-zijde, u kunt ook verkoopondersteuning van derden voor extra functies bereiken.