Configurazione di Secure Malware Analytics Appliance con il software di monitoraggio Prometheus

Sommario

Introduzione

In questo documento viene descritto come esportare i dati delle metriche del servizio Appliance di analisi malware sicuro nel software di monitoraggio Prometheus.

Contributo dei tecnici Cisco TAC.

Prerequisiti

Cisco raccomanda la conoscenza di Appliance di analisi malware sicuro e software Prometheus.

Requisiti

- Appliance Secure Malware Analytics (versione 2.13 e successive)
- Licenza software Prometheus

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

TIl sistema di monitoraggio Riemann/Elastic basato su ricerca in esecuzione sull'accessorio è sostituito dal monitoraggio basato su Prometheus da Secure Malware Analytics Appliance versione 2.13 in poi.

Nota: lo scopo principale di questa integrazione è monitorare le statistiche di Secure Malware Analytics Appliance utilizzando il software Prometheus Monitoring System. tra cui un'interfaccia, statistiche del traffico e così via.

Configurazione

Passaggio 1. Accedere a Secure Malware Analytics Appliance e selezionare Operations > Metrics per trovare la chiave API e la password di autenticazione di base.

Passaggio 2. Installare il software Prometheus Server: https://prometheus.io/download/

Passaggio 3. Creare un file .yml. Il file deve essere `denominato prometheus.yml` e includere i seguenti dettagli:

```
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
```

Passaggio 4. Eseguire il comando CLI per generare un token JWT per l'autenticazione, come specificato nel file di configurazione precedente:

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

Passaggio 5. Eseguire questo comando per verificare il campo Data scadenza per il token (validità 1 ora).

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

Di seguito è riportato un esempio di output del comando:


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

        ",

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

        ",

  "nbf": 1604094619
}
```

Nota: l'ora viene visualizzata in formato Epoch.

Passaggio 6. Eseguire il pull della configurazione dei servizi, dopo aver eseguito l'accesso all'interfaccia opadmin, immettere la seguente riga dall'interfaccia utente:

<#root>

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

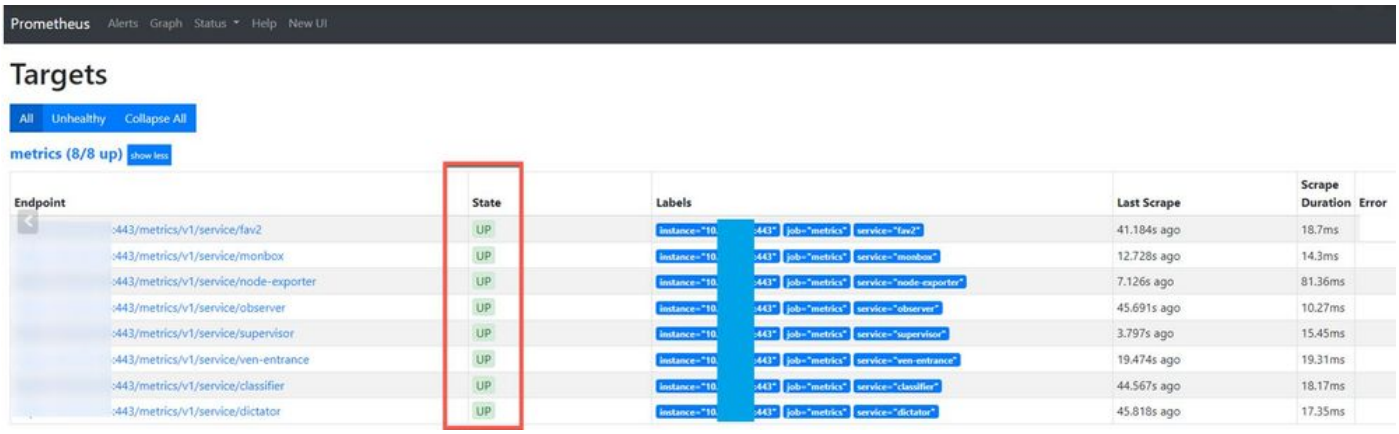
Passaggio 7. Dopo aver riavviato il servizio Prometheus, la configurazione viene attivata.

Passaggio 8. Accedere alla pagina Prometheus:

<#root>

http://localhost:9090/graph

È possibile visualizzare i servizi Secure Malware Analytics Appliance nello stato "UP", come mostrato nell'immagine.



Verifica

È possibile visualizzare i dati ricevuti dai dispositivi Secure Malware Analytics Appliance, rivedere le metriche in base ai propri requisiti, come mostrato nell'immagine.

Nota: questa funzione funziona solo per raccogliere dati specifici. La gestione del flusso di dati è responsabilità del server Prometheus.
Non è supportata la risoluzione dei problemi dal lato TAC di Cisco; è possibile contattare il

supporto di fornitori terzi per ricevere ulteriore supporto per le funzionalità.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).