charliemac Exabeam
04-30-2024

✓ Solved

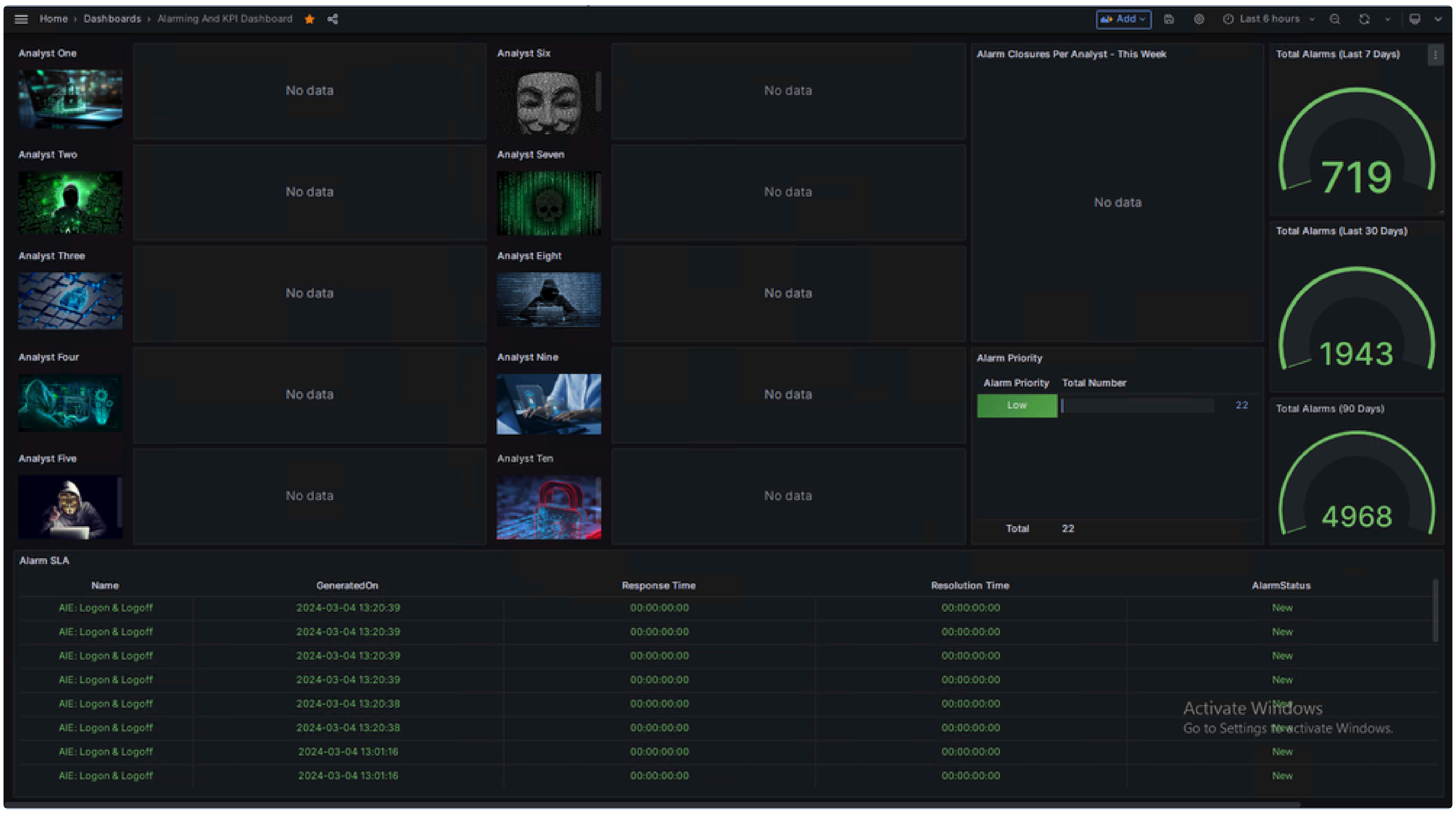
Grafana | Custom Dashboard | Alarming & KPI Dashboard

Hello All,

As part of the subscription services team it's common that we have to build custom Grafana dashboards and integrations to elevate/customize reporting within the product. Please see below an example of this that I wanted to share with the community - If this is something you are interested in having assistance with then I would encourage you to reach out to us and consider our subscription services offering, please see following links;

Want to learn more about our services? - **SAM+Unlimited Upgrades** | **Analytic Co-Pilot** | **TAM**

Purpose: A Grafana dashboard that gives you some high level alarming statistics, volume, priority and KPI stats. It also gives you a breakdown of alarm closures/opens per analyst so is something you can place on the SOC screens to encourage competition within the team.



Alarm Priority

Alarm Priority	Total Number
Low	22
Total	22

Alarm SLA

Name	GeneratedOn	Response Time	Resolution Time	AlarmStatus
AIE: Logon & Logoff	2024-03-04 13:20:39	00:00:00:00	00:00:00:00	New
AIE: Logon & Logoff	2024-03-04 13:20:39	00:00:00:00	00:00:00:00	New
AIE: Logon & Logoff	2024-03-04 13:20:39	00:00:00:00	00:00:00:00	New
AIE: Logon & Logoff	2024-03-04 13:20:39	00:00:00:00	00:00:00:00	New
AIE: Logon & Logoff	2024-03-04 13:20:38	00:00:00:00	00:00:00:00	New
AIE: Logon & Logoff	2024-03-04 13:20:38	00:00:00:00	00:00:00:00	New
AIE: Logon & Logoff	2024-03-04 13:01:16	00:00:00:00	00:00:00:00	New
AIE: Logon & Logoff	2024-03-04 13:01:16	00:00:00:00	00:00:00:00	New

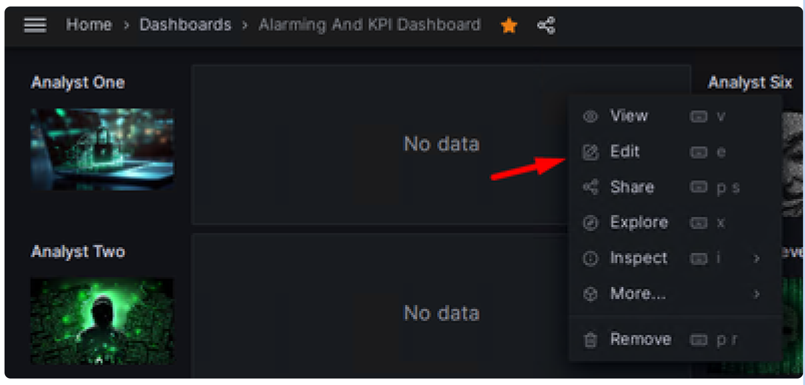
Required Connections: Elasticsearch & SQL.

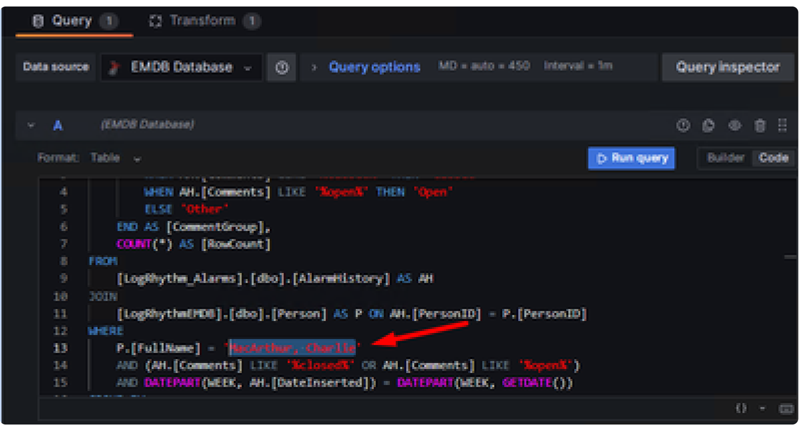
Steps

1. Download the attached JSON file.
2. Open Grafana | **http://localhost:3000/** from the PM/XM.
3. Import Dashboard.

Tweaks & Changes

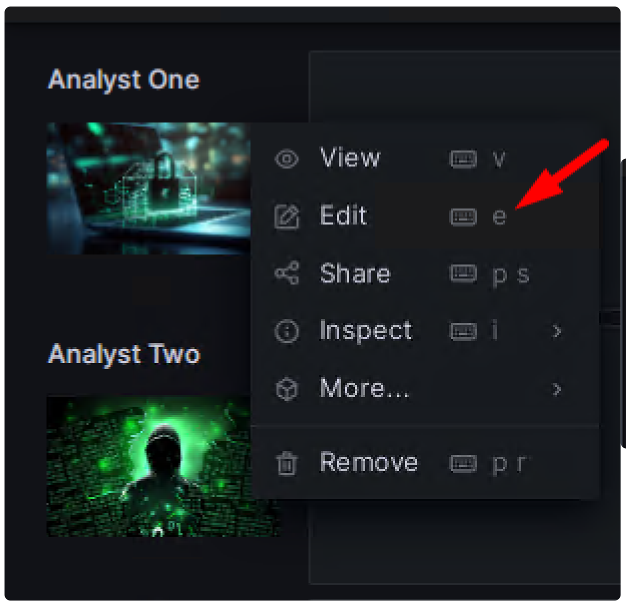
1. You need to tweak the query within each analysts widget, to ensure it matches their LogRhythm username. Example below to illustrate this point.

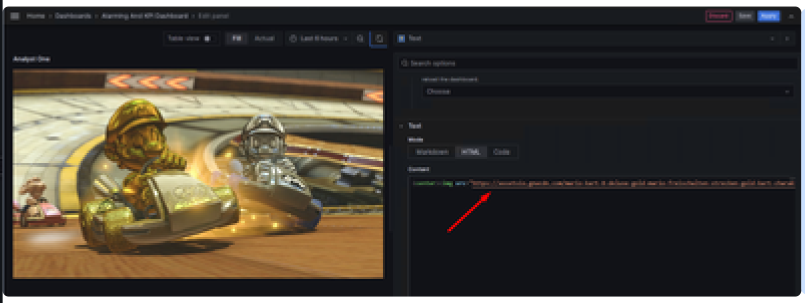


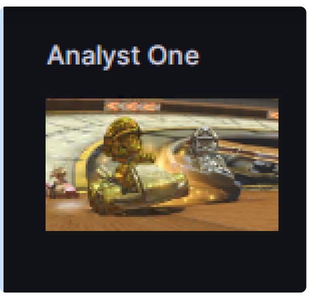


```
        WHEN AH.[Comments] LIKE '%open%' THEN 'Open'
        ELSE 'Other'
    END AS [CommentGroup],
    COUNT(*) AS [RowCount]
FROM
    [LogRhythm_Alarms].[dbo].[AlarmHistory] AS AH
JOIN
    [LogRhythmEMDB].[dbo].[Person] AS P ON AH.[PersonID] = P.[PersonID]
WHERE
    P.[FullName] = 'MacArthur, Charlie'
    AND (AH.[Comments] LIKE '%closed%' OR AH.[Comments] LIKE '%open%')
    AND DATEPART(WEEK, AH.[DateInserted]) = DATEPART(WEEK, GETDATE())
```

2. You can also edit the image associated with each user by uploading a new URL within that widget. Example below to illustrate this point.







Alarming And KPI Dashboard-1714472376833.json
66 KB

ALARMS. KPI'S ✕ ANALYST ✕ DASHBOARD ✕ GRAFANA ✕ REPORT ✕ STATS ✕ + TAG

3 Reply

charliemac
05-09-2024

Feel free to reach out if any challenges onboarding this.

MARKED AS SOLUTION

View Full Discussion (3 Replies)

haikalazaim Enthusiast
01-09-2025

Hi, thanks for sharing. On Grafana, during importing the dashboard required connection to elasticsearch and EMDB. How to configure the connection for elasticsearch? (pointing to which index name, pattern, and time field name?) Appreciate for sharing.

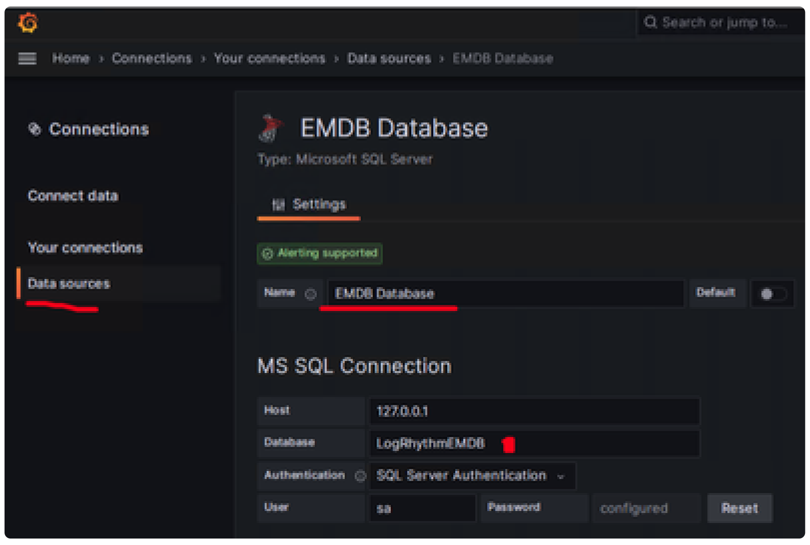
Reply

charliemac Exabeam **to haikalazaim**
01-09-2025

Hello **haikalazaim** ,

Please see another post I did that shows you how to add in the SQL database. There is a collection of other dashboards I have done in the past if that helps as well.

https://community.logrhythm.com/t5/Reporting/Grafana-Custom-Dashboard-Health-Monitoring/td-p/627821



EMDB Database

Type: Microsoft SQL Server

Name: EMDB Database

Default

MS SQL Connection

Host: 127.0.0.1

Database: LogRhythmEMDB

Authentication: SQL Server Authentication

User: sa

Password: configured

The elasticsearch connection can be added through the same panel as in the screenshot, it doesn't actually need to connect into ElasticSearch, unfortunately our ElasticSearch version will need to be upgraded before this is possible. The connection is only there to allow for some generic widgets that leverage the ElasticSearch plugin - They would probably even still work if converted to text/HTML format. You can essentially just add the ES connection and put in random values, and hit save.

Kind Regards,
Charlie MacArthur

1 Reply

Leave a reply...

Related Content

Dashboard: Build Your First Dashboard
04-22-2025 tamaraexabeam

Proofpoint Dashboards
12-28-2022 anonymous

Dashboards for LogRhythm Intelligence
10-01-2024 jake_haldeman

Dashboard: Add a time filter to Dashboard
04-22-2025 tamaraexabeam

UEBA Dashboards
10-06-2022 MelissaR

Recent Discussions

Data Source Selection for Report
05-16-2025 vishal12 ✓ Solved

Silent Log Sources Scheduled Report Help
03-16-2025 kreed ✓ Solved

FEATURE REQUEST: Reduce Noise on CSV Report Export
03-07-2025 cmayer ✓ Solved

Grafana | Custom Dashboard | AIE/Alarm Tuning & Monitoring
02-17-2025 charliemac ✓ Solved