charliemac Exabeam
04-30-2024

✓ Solved

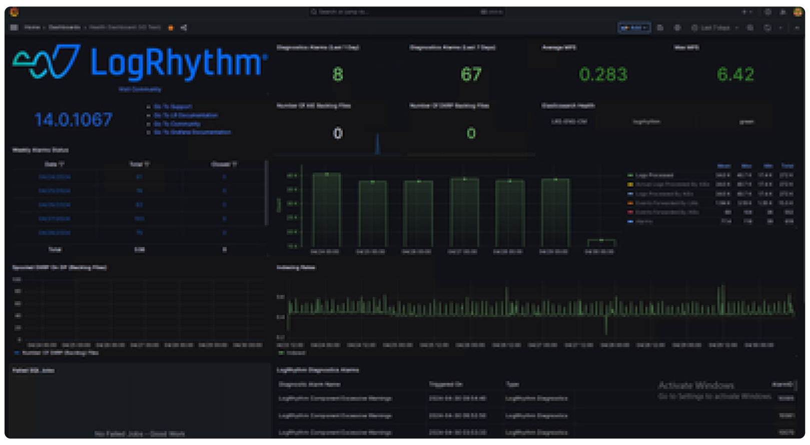
Grafana | Custom Dashboard | Health Monitoring

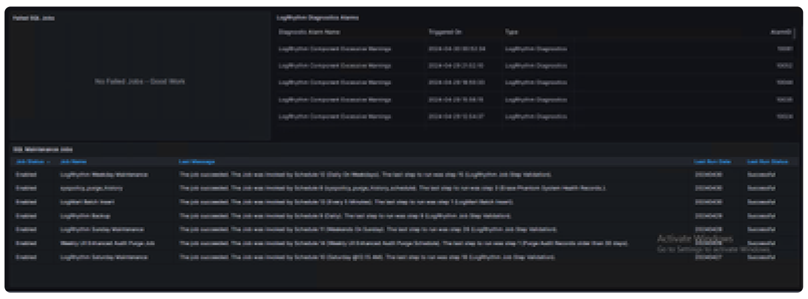
Hello All,

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;

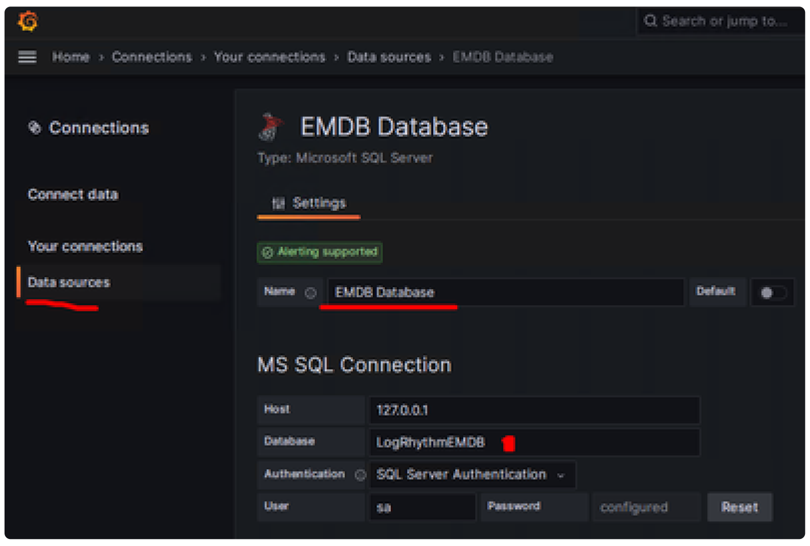
Want to learn more about our services? - **SAM+Unlimited Upgrades** | **Analytic Co-Pilot** | **TAM**

Purpose: A Grafana dashboard that gives you some high level health monitoring for things like backlogs on the platform, sql maintenance tasks, log volumes and cluster health.





Required Connections: Telegraf (Enabled By Default), SQL (See How To Add Below) & Elasticsearch



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

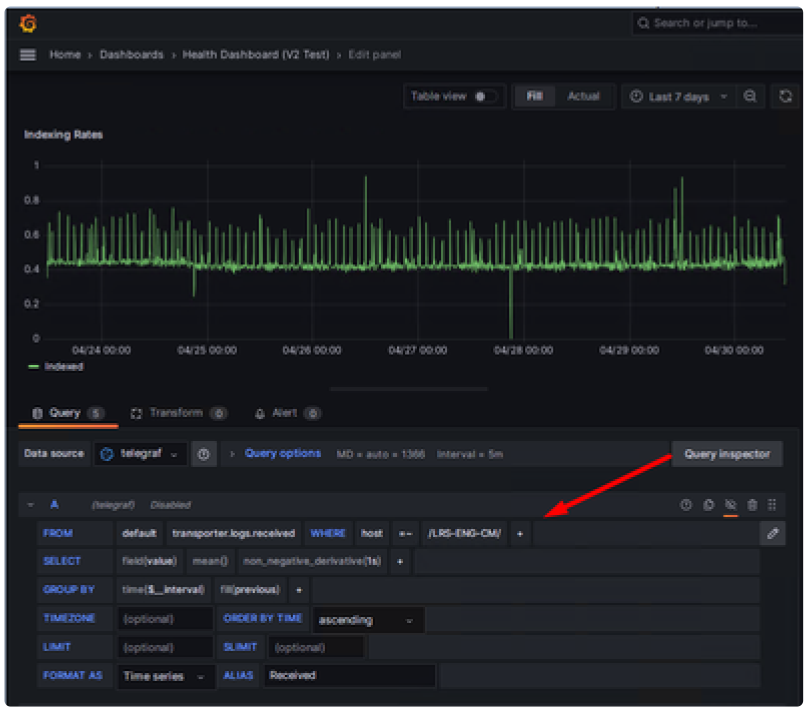
Password: configured

Steps

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

Tweaks & Changes

1. You will likely have one or two widgets that show no data, that's because they are using a fixed host tag in the query which is currently set to my lab. For ease of onboarding I have left this in there but you can setup variables with Grafana. Just replace the **LRS-ENG-CM** hostname with the name of your platform manager, do this for all examples where this can be seen, within all widgets not showing correctly. Feel free to reach out to me for clarity on this point.



Data source: telegraf › Query options MD = auto = 1366 Interval = 5m

A (telegraf) Disabled

FROM	default	transporter.logs.received	WHERE	host	=~ /LRS-ENG-CM/ +
SELECT	field(value)	mean()	non_negative_derivative(1s)	+	
GROUP BY	time($__interval)	fill(previous)	+		
TIMEZONE	(optional)	ORDER BY TIME	ascending		
LIMIT	(optional)	SLIMIT	(optional)		
FORMAT AS	Time series	ALIAS	Received		

[Health Dashboard (V2 Test)-1714473440479.json](#)
56 KB

GRAFANA ✕ HEALTH ✕ IMPORT ✕ JSON ✕ REPORTS ✕ + TAG

6 Reply

charliemac
05-09-2024

Feel free to reach out if any challenges onboarding this.

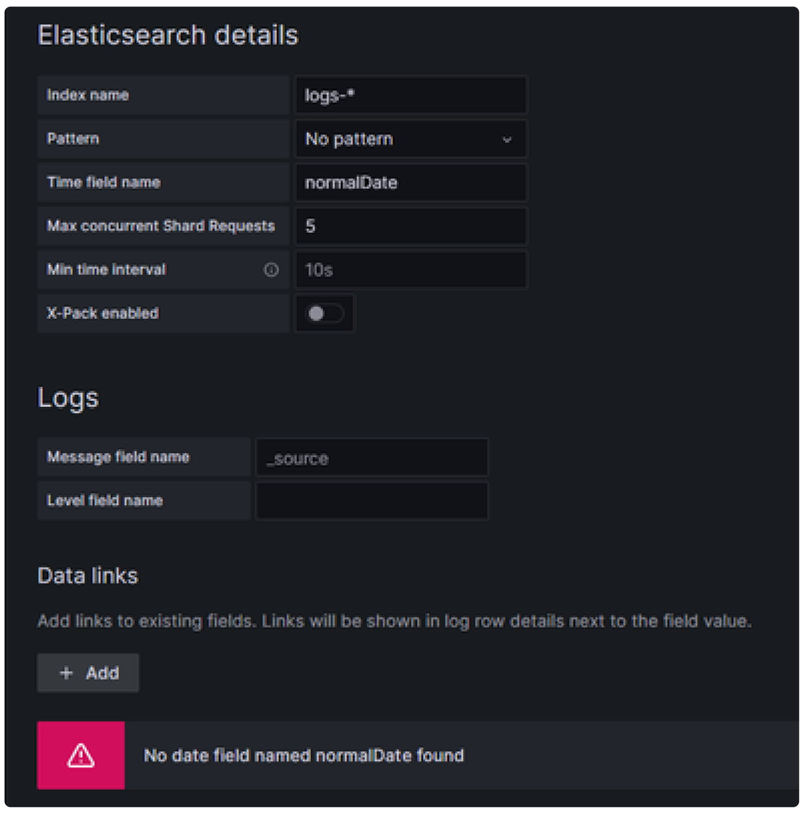
MARKED AS SOLUTION

View Full Discussion (3 Replies)

usolanki Practitioner
06-25-2024

Any idea why am I not able to onboard my ElasticSearch Data? Getting this error.

"No date field named **normalDate** found". Tried with **logDate** as well.



Elasticsearch details

Index name	logs-*
Pattern	No pattern
Time field name	normalDate
Max concurrent Shard Requests	5
Min time interval	10s
X-Pack enabled	○

Logs

Message field name	_source
Level field name	

Data links

Add links to existing fields. Links will be shown in log row details next to the field value.

+ Add

No date field named normalDate found