charliemac Exabeam
01-10-2025

✓ Solved

Grafana Advanced Alerting - Platform Management Automations

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: There are some blind spots in terms of platform management with LogRhythm, please see below examples. The following solution offers a means to bridge this gap, make admins lives easier and ensure that the SIEM is running optimally at all times. This is just a few examples, but there are countless other corner cases that we can resolve using the next steps.

- There is currently no way to raise an alarm if there is DXRP build up.
- You don't get alarms if a SQL maintenance or backup job fails.
- There is no alarms/alerts for when your indexing rate drops below a certain threshold.

The main point to make clear though, is that if exists in SQL, or Windows Performance Monitoring as a metric, you can leverage it within Grafana for custom dashboards and alerting.

How: You can essentially create an automated Grafana alert on anything that is picked up by the LogRhythm Metrics/Common engine (Telegraf) and anything that can be pulled via a SQL query. They have integrated SMTP/Email services and no additional cost, and their own alarms engine.

Please see the below example of what one of the email alerts looks like. The idea here is that you can just get a quick email summary that lets you know the deployment is down, maintenance has failed, some other threshold has been crossed etc.

Setup Summary: To get this up and running you will need to configure the following things. They are all fairly straightforward and will require standard administrators details like the SA password for SQL, admin rights on the XM/PM server so you can edit some configuration files and general remote access etc.

- You will need to configure the required data sources, to be able to monitor/query/alert correctly.
  - Telegraf is already done for you by default.
  - SQL needs to be added in.
  - ElasticSearch is a good idea but not required.
- We are going to disable anonymous authenticaiton into Grafana as well, for security reasons. As a general note you don't need to authenticate into Grafana to view it's contents, by default. This corrects that, just be careful not to lose your password.
- You will need to input some SMTP details so that Grafana knows where to send the alerts to.
- It's a good idea to import some of the Community dashboards at this stage as you can leverage these to build alerts more easily.
- Now you can actually build the Grafana alerts, you can either do this from scratch or you can leverage a pre-existing widget, which is always going to be the easier method.

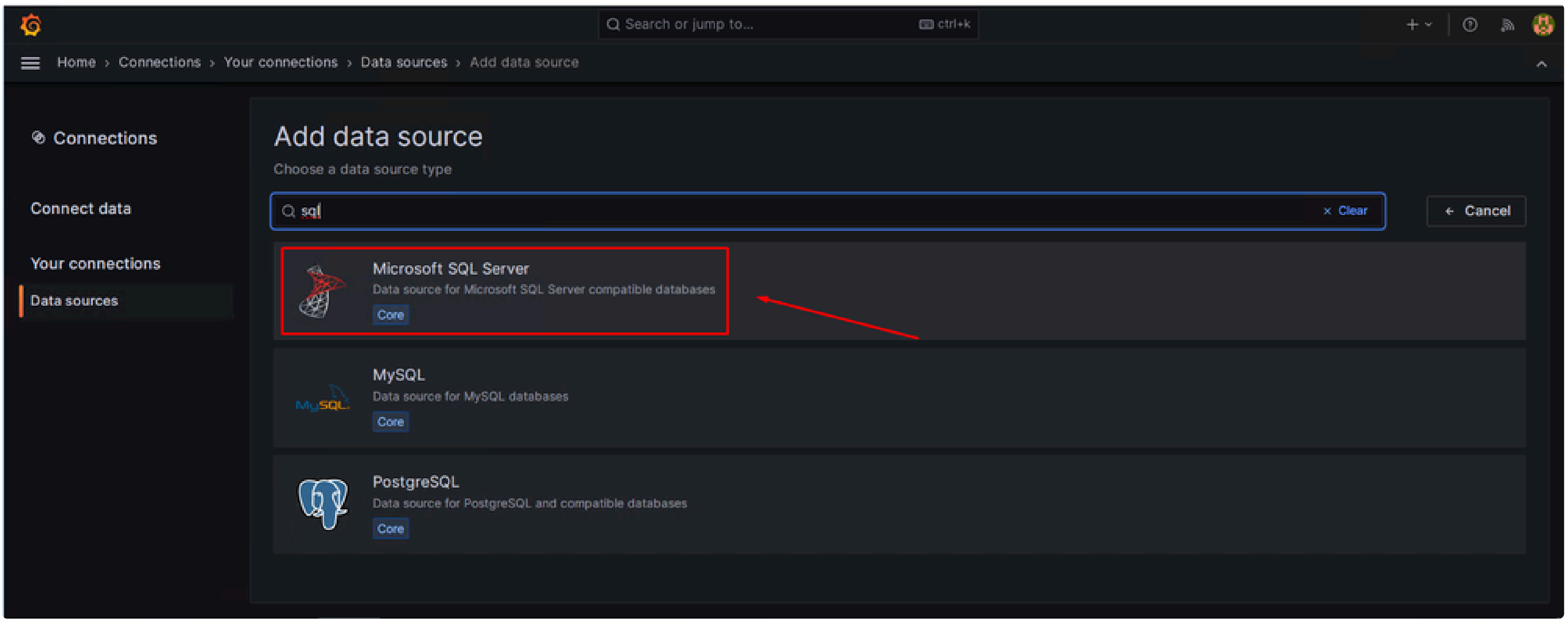
Configuring Data Sources: Configuring the required data sources is simple, there is three in total and one is done for us already. Run through the below steps to get this done.

- RDP onto your XM/PM server, open Google Chrome or Edge and browse to localhost:3000 (Grafana}).

follow the below steps.

- Open elevated CMD prompt.
    - Navigate to the following directory, you can just paste the below statement in: **cd C:\Program Files\LogRhythm\LogRhythm Metrics\LogRhythm Metrics Web UI\dependencies\grafana\bin**
    - Now run the following command and change the section that says logrhythm!1, to whatever you want, this is just the generic password we use for the platform.
    - **grafana-cli admin reset-admin-password logrhythm!1**
    - If you did it correctly CMD will say "Admin Password cahnged Succesfully" and you should now be able to login to Grafana on the previous step.
- Click on the "hamburger" menu in the top left corner of the screen, expand the "Connections" tab and click on "Your Connections". You should see that Telegraf is already in there.
- Now you can add in SQL Server by clicking the large "Add New Data Source" button in the top right corner. The next steps for this section are easier to explain via screenshots so see below;

SQL Connection



Add data source

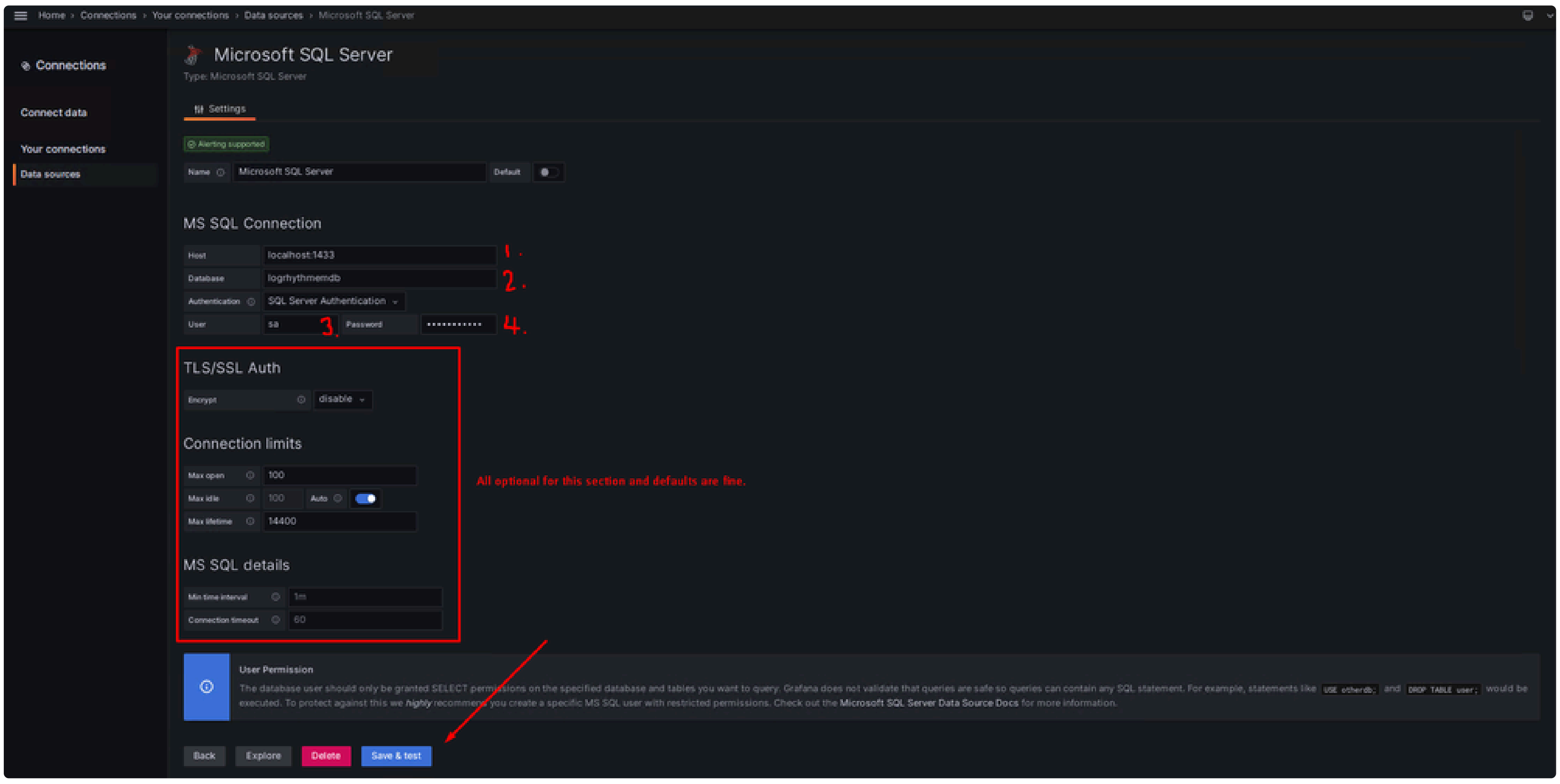
Choose a data source type

sql

Microsoft SQL Server
Data source for Microsoft SQL Server compatible databases

MySQL
Data source for MySQL databases

PostgreSQL
Data source for PostgreSQL and compatible databases



Microsoft SQL Server

Type: Microsoft SQL Server

Name: Microsoft SQL Server Default

MS SQL Connection

Host: localhost:1433

Database: logrhythmemdb

Authentication: SQL Server Authentication

User: sa Password: ••••••••••••

TLS/SSL Auth

Encrypt: disable

Connection limits

Max open: 100

Max idle: 100 Auto

Max lifetime: 14400

MS SQL details

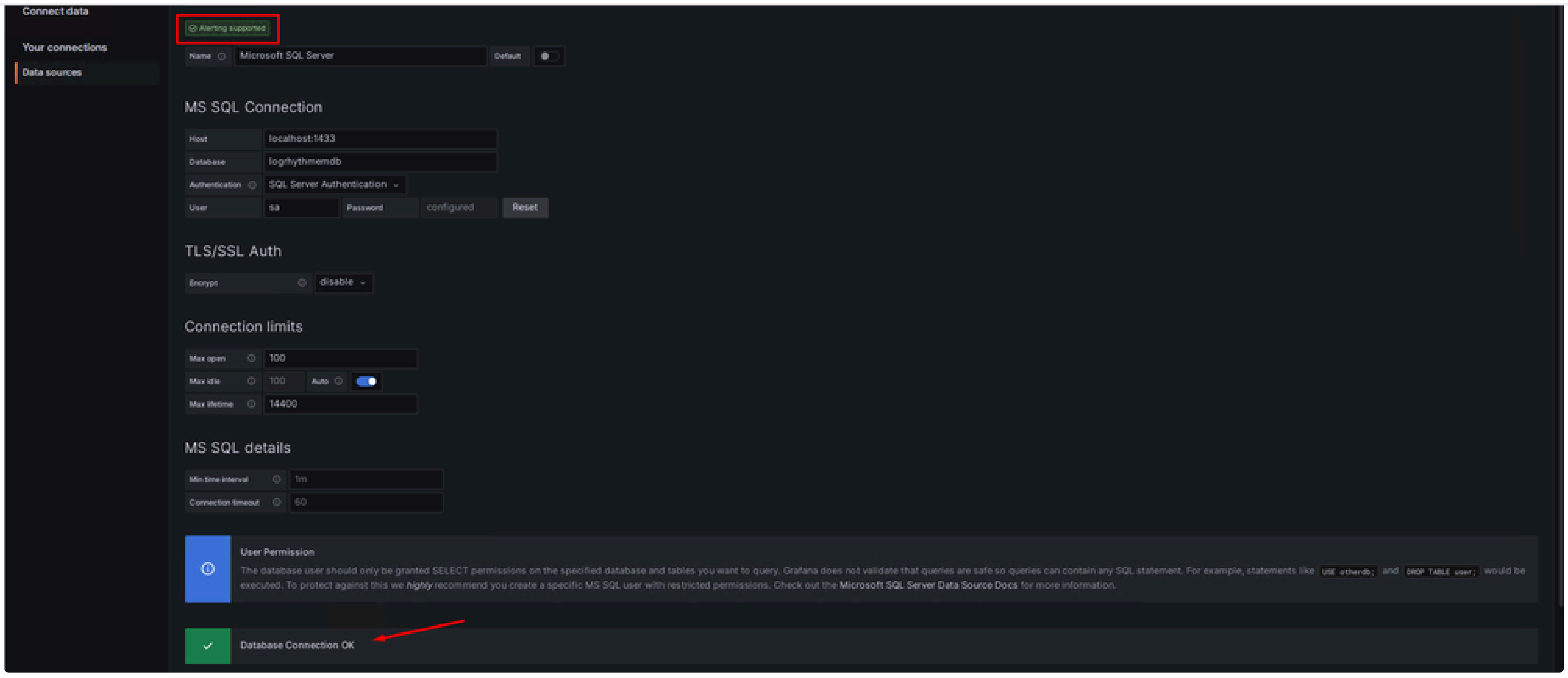
Min time interval: 1m

Connection timeout: 60

All optional for this section and defaults are fine.

User Permission

The database user should only be granted SELECT permissions on the specified database and tables you want to query. Grafana does not validate that queries are safe so queries can contain any SQL statement. For example, statements like `USE otherdb;` and `DROP TABLE user;` would be executed. To protect against this we *highly* recommend you create a specific MS SQL user with restricted permissions. Check out the **Microsoft SQL Server Data Source Docs** for more information.



Connect data

Your connections

Data sources

Alerting supported

Name: Microsoft SQL Server — Default

MS SQL Connection

Host: localhost:1433

Database: logrhythmemdb

Authentication: SQL Server Authentication

User: sa Password: configured Reset

TLS/SSL Auth

Encrypt: disable

Connection limits

Max open: 100

Max idle: 100 — Auto

Max lifetime: 14400

MS SQL details

Min time interval: 1m

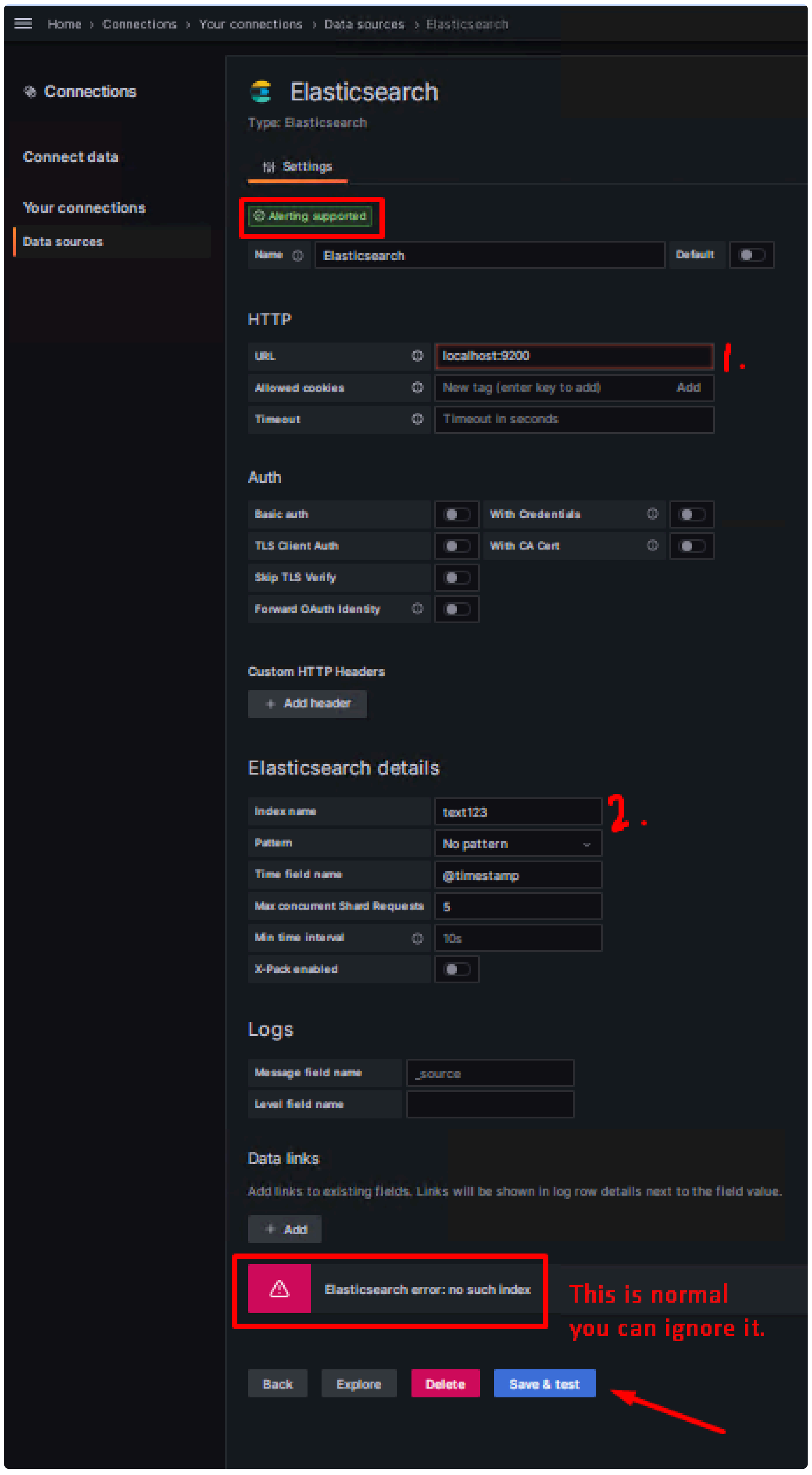
Connection timeout: 60

User Permission

The database user should only be granted SELECT permissions on the specified database and tables you want to query. Grafana does not validate that queries are safe so queries can contain any SQL statement. For example, statements like `USE otherdb;` and `DROP TABLE user;` would be executed. To protect against this we *highly* recommend you create a specific MS SQL user with restricted permissions. Check out the **Microsoft SQL Server Data Source Docs** for more information.

✓ Database Connection OK

ElasticSearch Connection (Optional - This is just for some of the custom community dashboards)



Home › Connections › Your connections › Data sources › Elasticsearch

Connections

Connect data

Your connections

Data sources

Elasticsearch

Type: Elasticsearch

Settings

Alerting supported

Name: Elasticsearch — Default

HTTP

URL: localhost:9200 1.

Allowed cookies: New tag (enter key to add) — Add

Timeout: Timeout in seconds

Auth

Basic auth — With Credentials

TLS Client Auth — With CA Cert

Skip TLS Verify

Forward OAuth Identity

Custom HTTP Headers

+ Add header

Elasticsearch details

Index name: text123 2.

Pattern: No pattern

Time field name: @timestamp

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.

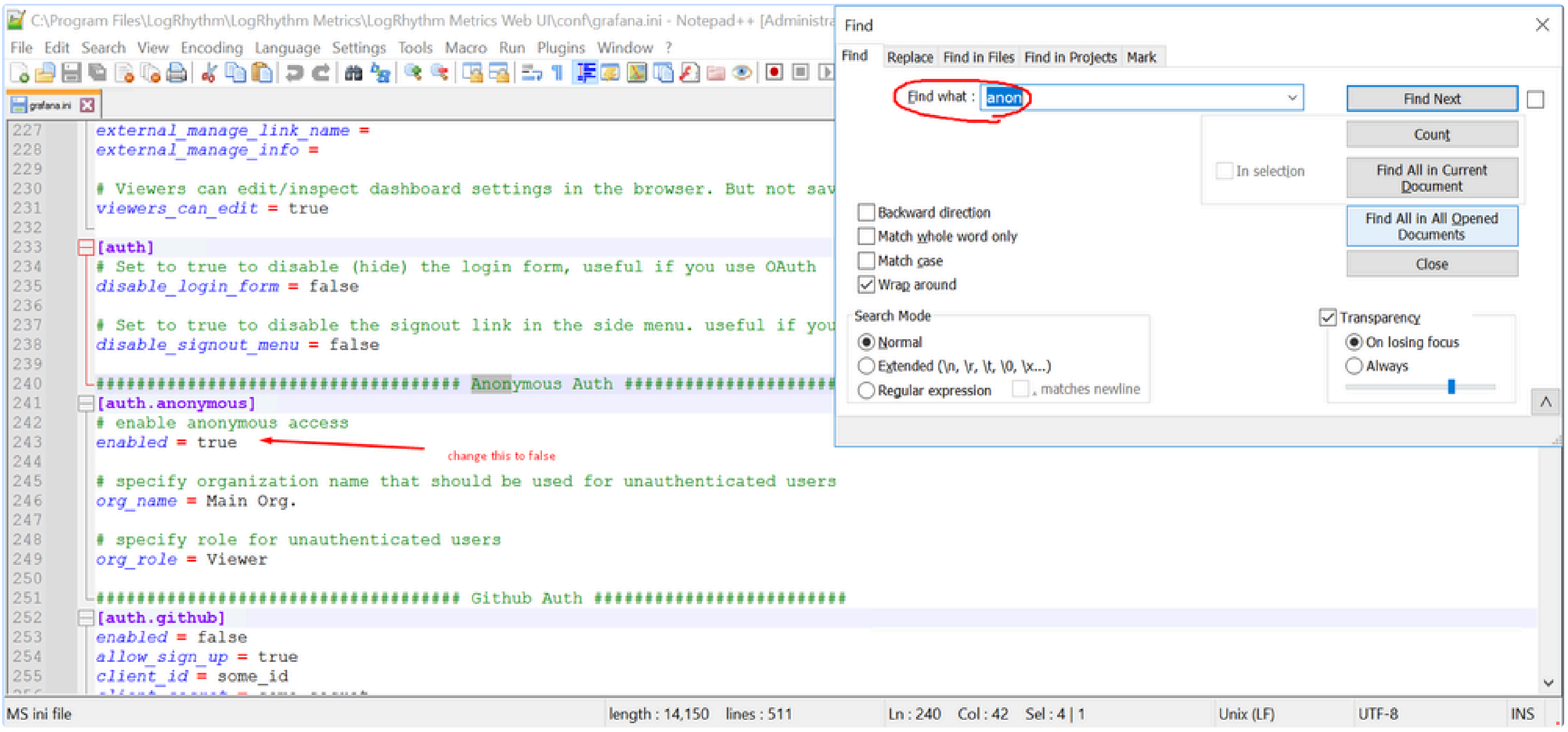
+ Add

Elasticsearch error: no such index

This is normal you can ignore it.

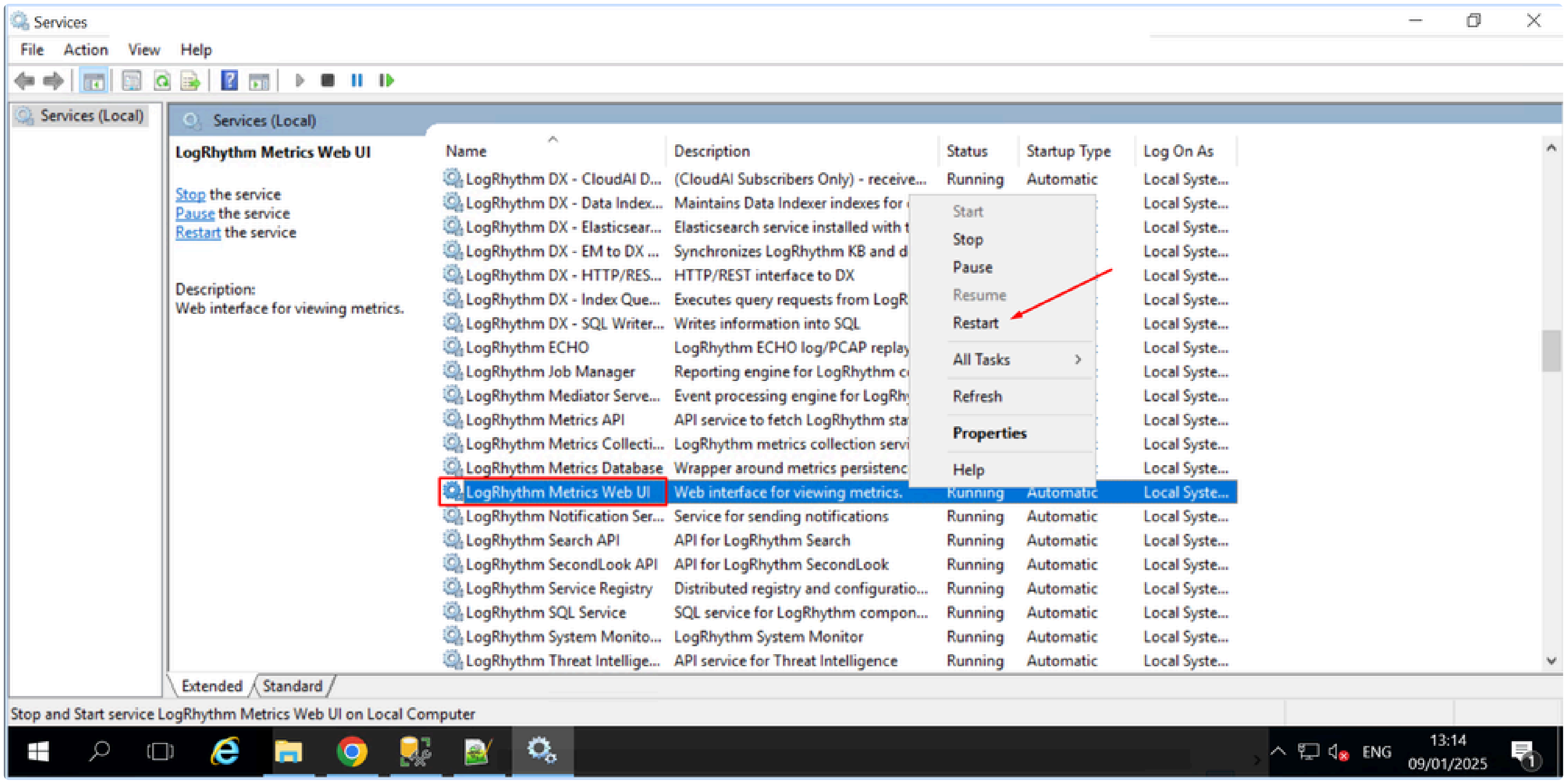
Disabling Anonymous Authentication (Optional - Highly Reccomended): For an additional level of security, you can also alter the additional grafana.ini variable to revoke anonymous logins. However, you will need to ensure you have Grafana accounts setup before enforcing this. This appears to be included by default in 7.19 so you may not need to do this part if you are on 7.19, worth checking if you need to login to Grafana to see data.

- Open File Explorer & browse to the following path C:\Program Files\LogRhythm\LogRhythm Metrics\LogRhythm Metrics Web UI\conf .
- There is a file in there called Grafana, open this in a text editor (I used Notepad++) make sure you do this as an admin or you might get a permissions prompt.
- CTRL + F for "anon" . Then match your configuration to the below screenshot, and restart the service in 2nd screenshot. Grafana will be down for a moment whilst this goes through.
- Once Grafana loads back up, sign out of it, and refresh the page. You should notice that nobody can now get into Grafana without logging in first. This is the desired effect of this change.


C:\Program Files\LogRhythm\LogRhythm Metrics\LogRhythm Metrics Web UI\conf\grafana.ini - Notepad++ [Administra
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
grafana.ini
Find
Find Replace Find in Files Find in Projects Mark
Find what : anon
Find Next
Count
□ In selection
Find All in Current Document
Find All in All Opened Documents
Close
□ Backward direction
□ Match whole word only
□ Match case
☑ Wrap around
Search Mode
● Normal
○ Extended (\n, \r, \t, \0, \x...)
○ Regular expression □ . matches newline
☑ Transparency
● On losing focus
○ Always
MS ini file length : 14,150 lines : 511 Ln : 240 Col : 42 Sel : 4 | 1 Unix (LF) UTF-8 INS

```
external_manage_link_name =
external_manage_info =

# Viewers can edit/inspect dashboard settings in the browser. But not sav
viewers_can_edit = true

[auth]
# Set to true to disable (hide) the login form, useful if you use OAuth
disable_login_form = false

# Set to true to disable the signout link in the side menu. useful if you
disable_signout_menu = false

#################################### Anonymous Auth ######################
[auth.anonymous]
# enable anonymous access
enabled = true

# specify organization name that should be used for unauthenticated users
org_name = Main Org.

# specify role for unauthenticated users
org_role = Viewer

#################################### Github Auth ##########################
[auth.github]
enabled = false
allow_sign_up = true
client_id = some_id
```

change this to false



LogRhythm Metrics Web UI

Stop the service
Pause the service
Restart the service

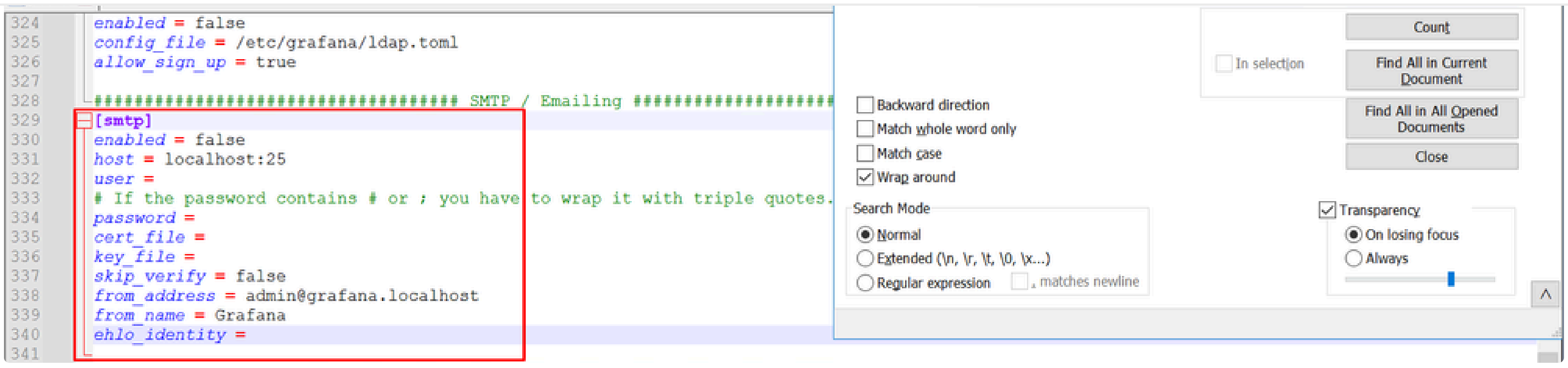
Description:
Web interface for viewing metrics.

Name	Description	Status	Startup Type	Log On As
LogRhythm DX - CloudAI D...	(CloudAI Subscribers Only) - receive...	Running	Automatic	Local Syste...
LogRhythm DX - Data Index...	Maintains Data Indexer indexes for			Local Syste...
LogRhythm DX - Elasticsear...	Elasticsearch service installed with t			Local Syste...
LogRhythm DX - EM to DX ...	Synchronizes LogRhythm KB and d			Local Syste...
LogRhythm DX - HTTP/RES...	HTTP/REST interface to DX			Local Syste...
LogRhythm DX - Index Que...	Executes query requests from LogR			Local Syste...
LogRhythm DX - SQL Writer...	Writes information into SQL			Local Syste...
LogRhythm ECHO	LogRhythm ECHO log/PCAP replay			Local Syste...
LogRhythm Job Manager	Reporting engine for LogRhythm c			Local Syste...
LogRhythm Mediator Serve...	Event processing engine for LogRhy			Local Syste...
LogRhythm Metrics API	API service to fetch LogRhythm sta			Local Syste...
LogRhythm Metrics Collecti...	LogRhythm metrics collection servi			Local Syste...
LogRhythm Metrics Database	Wrapper around metrics persistenc			Local Syste...
LogRhythm Metrics Web UI	Web interface for viewing metrics.	Running	Automatic	Local Syste...
LogRhythm Notification Ser...	Service for sending notifications	Running	Automatic	Local Syste...
LogRhythm Search API	API for LogRhythm Search	Running	Automatic	Local Syste...
LogRhythm SecondLook API	API for LogRhythm SecondLook	Running	Automatic	Local Syste...
LogRhythm Service Registry	Distributed registry and configuratio...	Running	Automatic	Local Syste...
LogRhythm SQL Service	SQL service for LogRhythm compon...	Running	Automatic	Local Syste...
LogRhythm System Monito...	LogRhythm System Monitor	Running	Automatic	Local Syste...
LogRhythm Threat Intellige...	API service for Threat Intelligence	Running	Automatic	Local Syste...

Stop and Start service LogRhythm Metrics Web UI on Local Computer

Configuring SMTP Details: So we have got to a point where we have our data connections, Grafana requires a password for access and now we can move onto setting up the SMTP details. It's a similar format to the last step, details below;

- Open Notepad ++ as admin
- Browse to this file "C:\Program Files\LogRhythm\LogRhythm Metrics\LogRhythm Metrics Web UI\conf\grafana.ini"
- CTRL + F for “SMTP” and look for these default values as seen in screenshot 1 below. Once you have found it, change the settings to the configuration in screenshot 2. I setup a test SMTP server and put the following details in, you will have a slightly different config (I used mail hog as my test server).
- Once you have done that you will need to save the grafana file and restart the same service as before.



```
enabled = false
config_file = /etc/grafana/ldap.toml
allow_sign_up = true

#################################### SMTP / Emailing ####################
[smtp]
enabled = false
host = localhost:25
user =
# If the password contains # or ; you have to wrap it with triple quotes.
password =
cert_file =
key_file =
skip_verify = false
from_address = admin@grafana.localhost
from_name = Grafana
ehlo_identity =
```

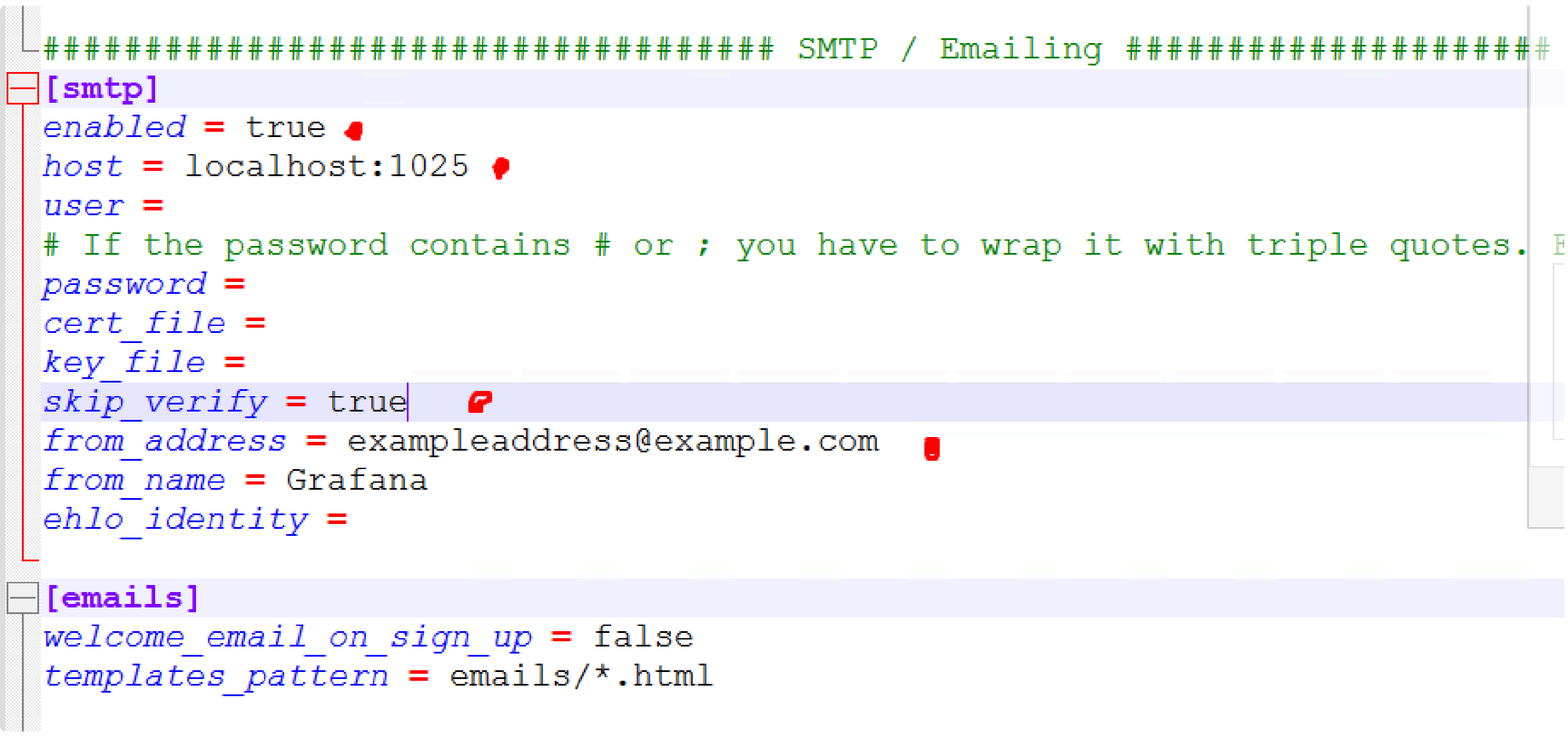
☐ Backward direction
☐ Match whole word only
☐ Match case
☑ Wrap around

Search Mode
● Normal
○ Extended (\n, \r, \t, \0, \x...)
○ Regular expression ☐ . matches newline

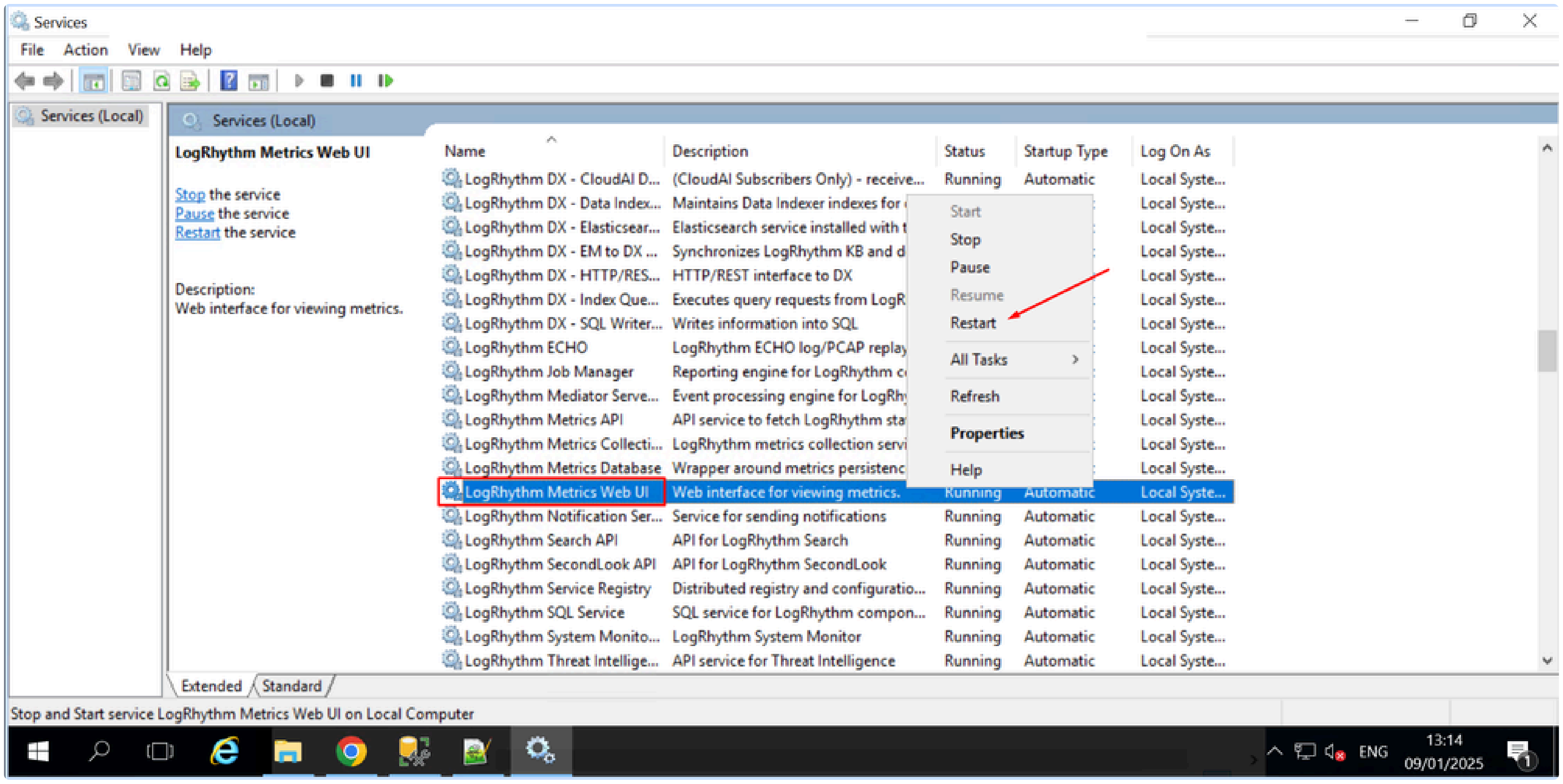
☐ In selection

☑ Transparency
● On losing focus
○ Always

Count
Find All in Current Document
Find All in All Opened Documents
Close



```
#################################### SMTP / Emailing ####################
[smtp]
enabled = true
host = localhost:1025
user =
# If the password contains # or ; you have to wrap it with triple quotes.
password =
cert_file =
key_file =
skip_verify = true
from_address = exampleaddress@example.com
from_name = Grafana
ehlo_identity =

[emails]
welcome_email_on_sign_up = false
templates_pattern = emails/*.html
```



LogRhythm Metrics Web UI

Stop the service
Pause the service
Restart the service

Description:
Web interface for viewing metrics.

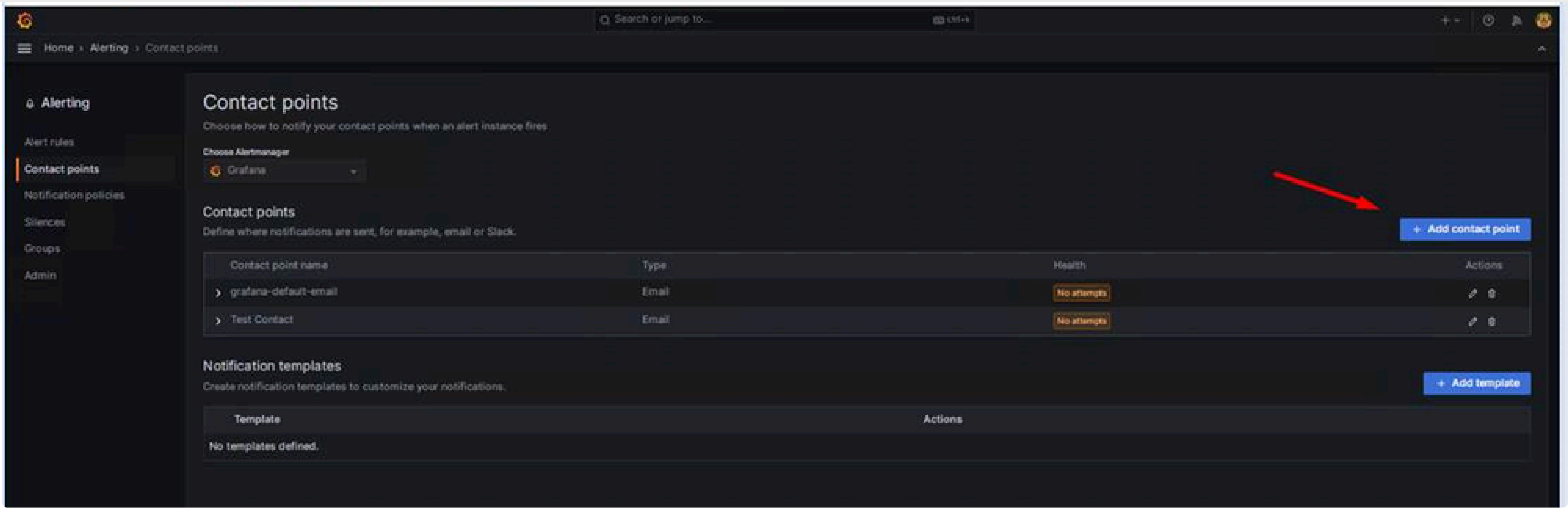
Name	Description	Status	Startup Type	Log On As
LogRhythm DX - CloudAI D...	(CloudAI Subscribers Only) - receive...	Running	Automatic	Local Syste...
LogRhythm DX - Data Index...	Maintains Data Indexer indexes for			Local Syste...
LogRhythm DX - Elasticsear...	Elasticsearch service installed with t			Local Syste...
LogRhythm DX - EM to DX ...	Synchronizes LogRhythm KB and d			Local Syste...
LogRhythm DX - HTTP/RES...	HTTP/REST interface to DX			Local Syste...
LogRhythm DX - Index Que...	Executes query requests from LogR			Local Syste...
LogRhythm DX - SQL Writer...	Writes information into SQL			Local Syste...
LogRhythm ECHO	LogRhythm ECHO log/PCAP replay			Local Syste...
LogRhythm Job Manager	Reporting engine for LogRhythm c			Local Syste...
LogRhythm Mediator Serve...	Event processing engine for LogRh			Local Syste...
LogRhythm Metrics API	API service to fetch LogRhythm sta			Local Syste...
LogRhythm Metrics Collecti...	LogRhythm metrics collection servi			Local Syste...
LogRhythm Metrics Database	Wrapper around metrics persistenc			Local Syste...
LogRhythm Metrics Web UI	Web interface for viewing metrics.	Running	Automatic	Local Syste...
LogRhythm Notification Ser...	Service for sending notifications	Running	Automatic	Local Syste...
LogRhythm Search API	API for LogRhythm Search	Running	Automatic	Local Syste...
LogRhythm SecondLook API	API for LogRhythm SecondLook	Running	Automatic	Local Syste...
LogRhythm Service Registry	Distributed registry and configuratio...	Running	Automatic	Local Syste...
LogRhythm SQL Service	SQL service for LogRhythm compon...	Running	Automatic	Local Syste...
LogRhythm System Monito...	LogRhythm System Monitor	Running	Automatic	Local Syste...
LogRhythm Threat Intellige...	API service for Threat Intelligence	Running	Automatic	Local Syste...

Stop and Start service LogRhythm Metrics Web UI on Local Computer

13:14
09/01/2025

At this point it is a good idea to create some contact points within Grafana, populate them with test target email addresses and get familiar with the UI. In the past people have added in SOC team distribution lists, or specific email addresses of administrators responsbible for SIEM maintenance etc. Examples below of what works in my lab, once you have it setup you can hit the test button and get an example email through like I have.

Link to official Grafana documentation if you need it - **https://grafana.com/docs/grafana/latest/alerting/configure-notifications/manage-contact-points/**



Contact points

Choose how to notify your contact points when an alert instance fires

Choose Alertmanager: Grafana

Contact points

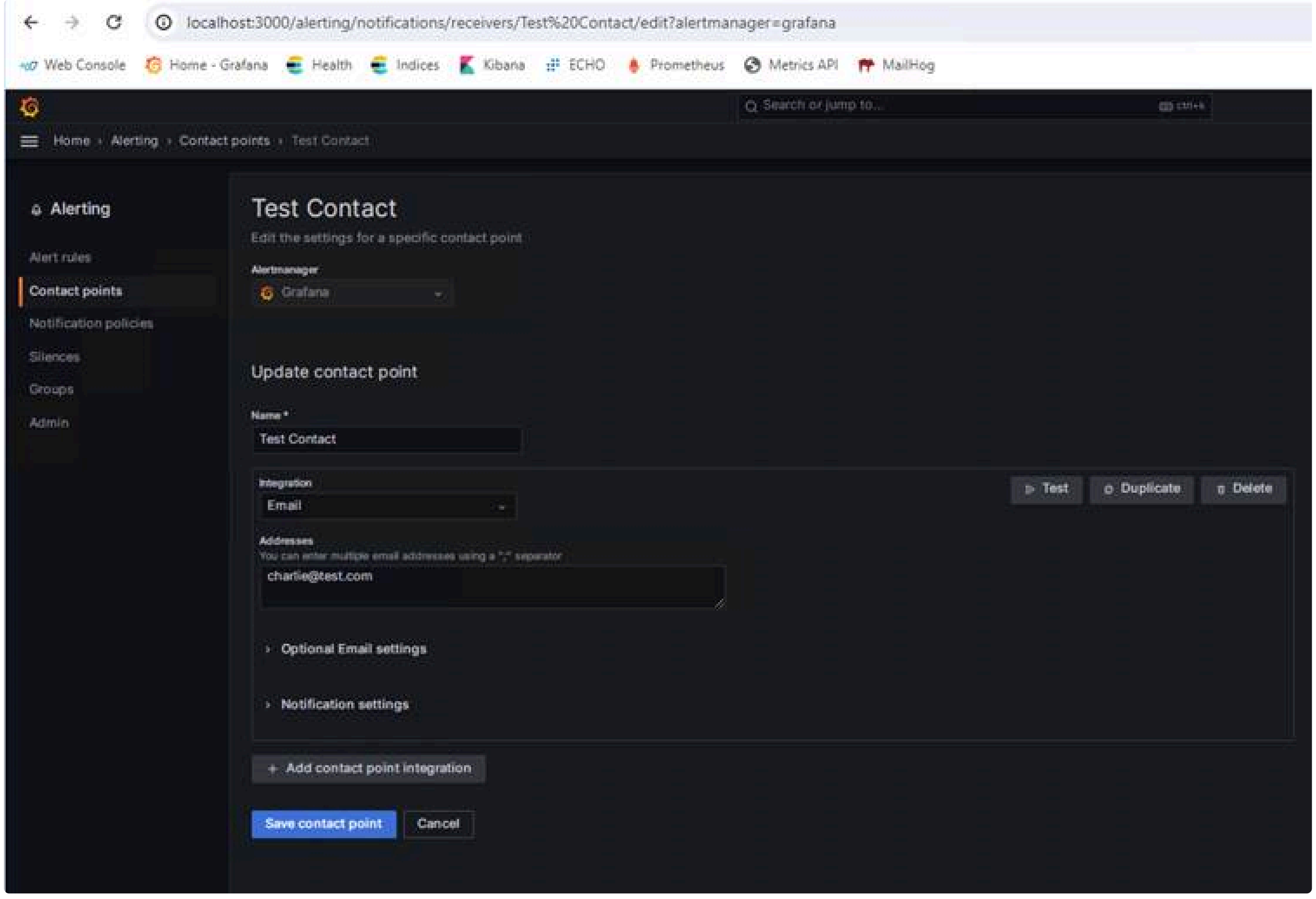
Define where notifications are sent, for example, email or Slack.

Contact point name	Type	Health	Actions
grafana-default-email	Email	No attempts	
Test Contact	Email	No attempts	

Notification templates

Create notification templates to customize your notifications.

Template	Actions
No templates defined.	



localhost:3000/alerting/notifications/receivers/Test%20Contact/edit?alertmanager=grafana

Test Contact

Edit the settings for a specific contact point

Alertmanager: Grafana

Update contact point

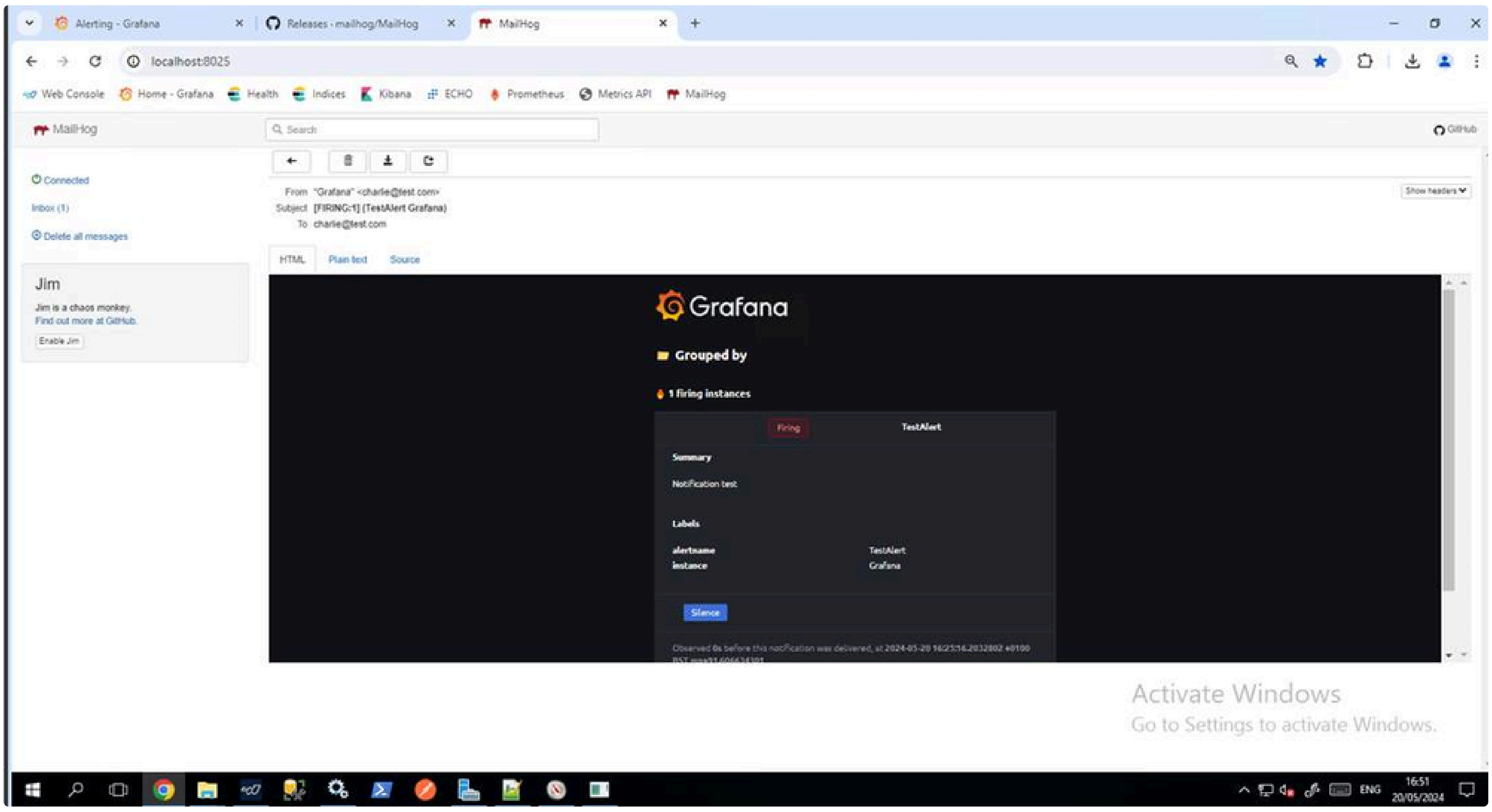
Name *: Test Contact

Integration: Email

Addresses

You can enter multiple email addresses using a ";" separator

charlie@test.com



localhost:8025

From "Grafana" <charlie@test.com>

Subject [FIRING:1] (TestAlert Grafana)

To charlie@test.com

Grafana

Grouped by

1 firing instances

Firing TestAlert

Summary

Notification test

Labels

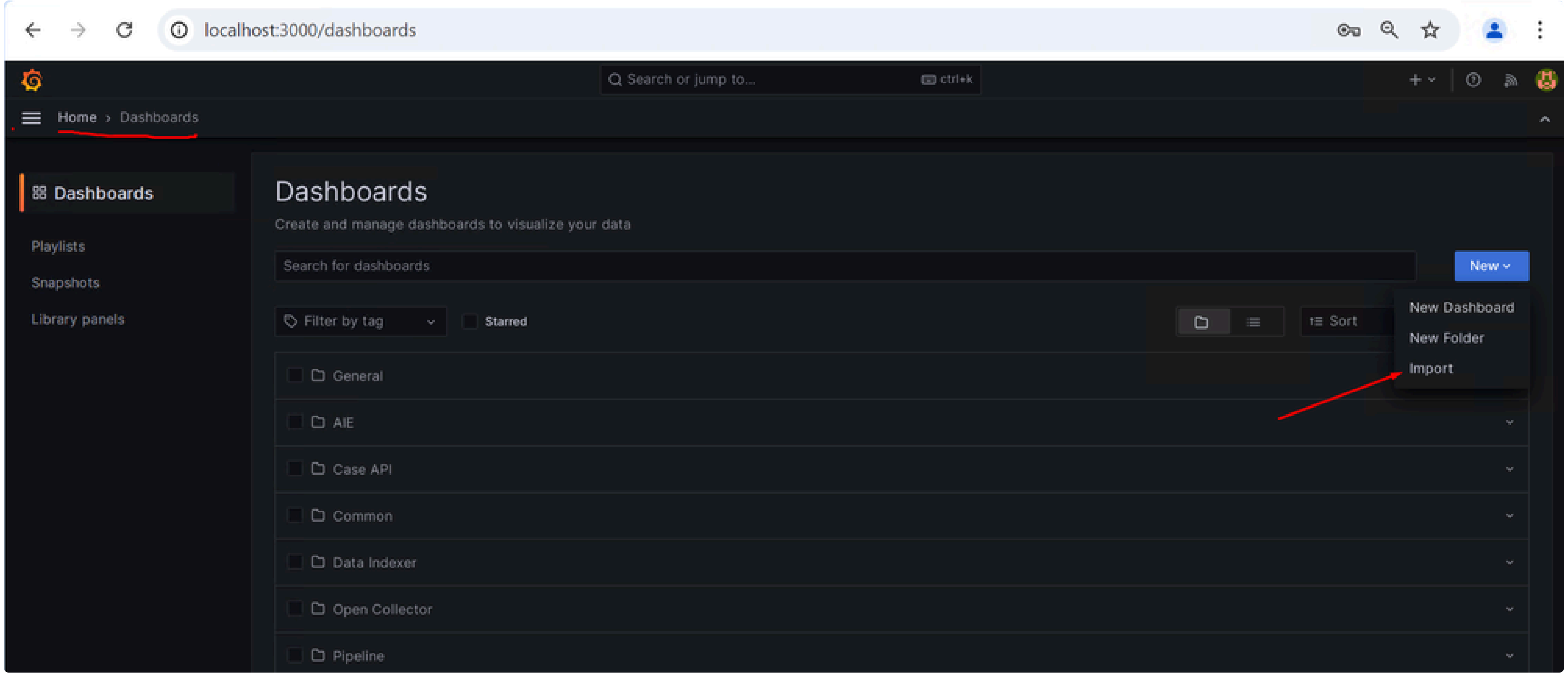
alertname	TestAlert
instance	Grafana

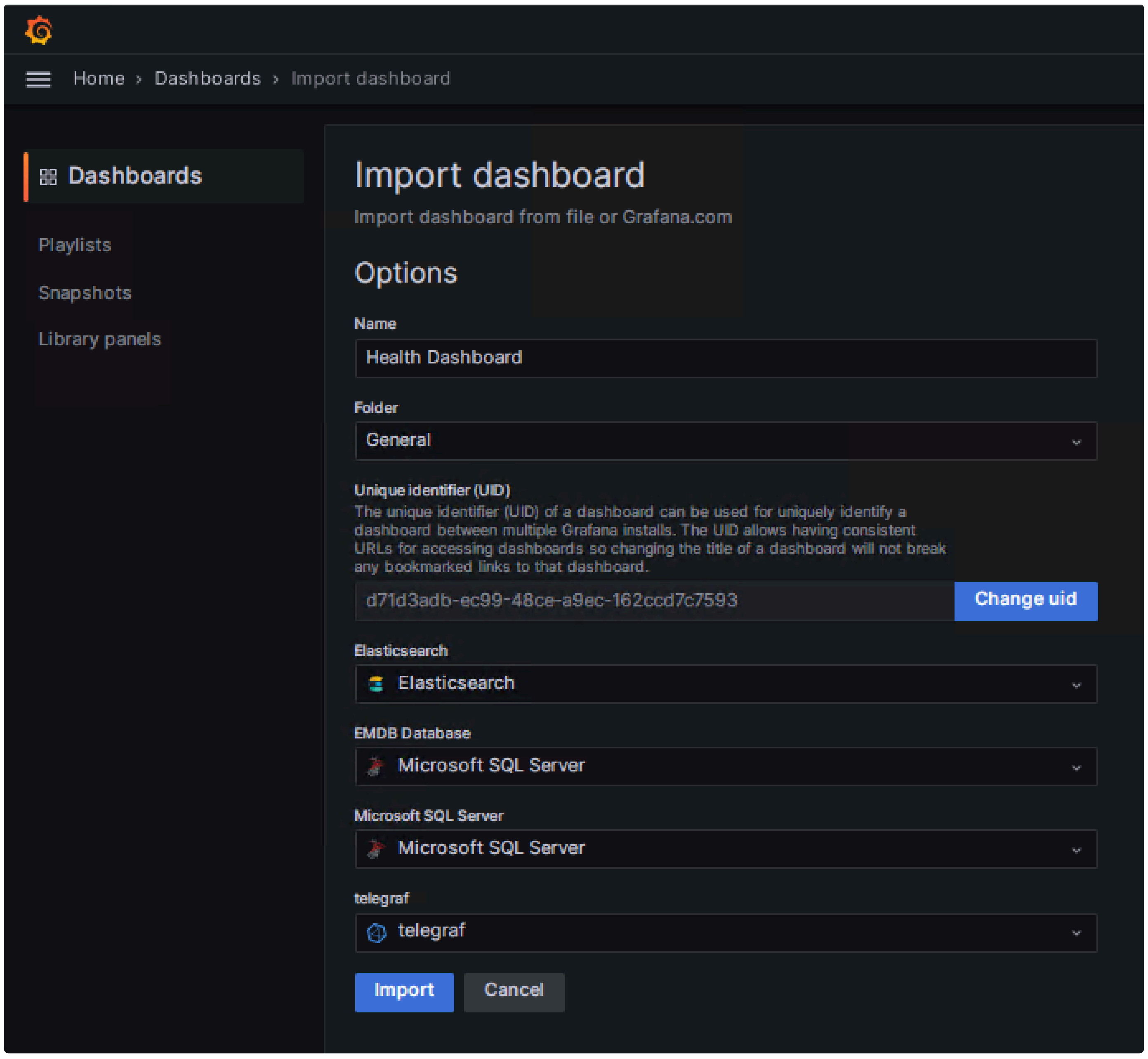
Observed 0s before this notification was delivered, at 2024-05-20 16:23:16.2032802 +0100 BST m=+91.606634301

Importing Pre-Existing Community Dashboards (As a minimum you will need the Health Monitoring One)

from scratch, if you don't then you will likely require SQL query knowledge and Telegraf knowledge. Essentially you just grab the JSON file in those links and you can import them.

- **Download The JSON Files From Health Monitoring Dashbord**
  Health Monitoring Dashboard
- **Optional Downloads - Useful Dashboards**
- **Alarming KPI Dashboard**
- **AIE Alarm Tuning Dashboard**
- **Log Source Onboarding Dashboard**





Import dashboard

Import dashboard from file or Grafana.com

Options

Name: Health Dashboard

Folder: General

Unique identifier (UID)

The unique identifier (UID) of a dashboard can be used for uniquely identify a dashboard between multiple Grafana installs. The UID allows having consistent URLs for accessing dashboards so changing the title of a dashboard will not break any bookmarked links to that dashboard.

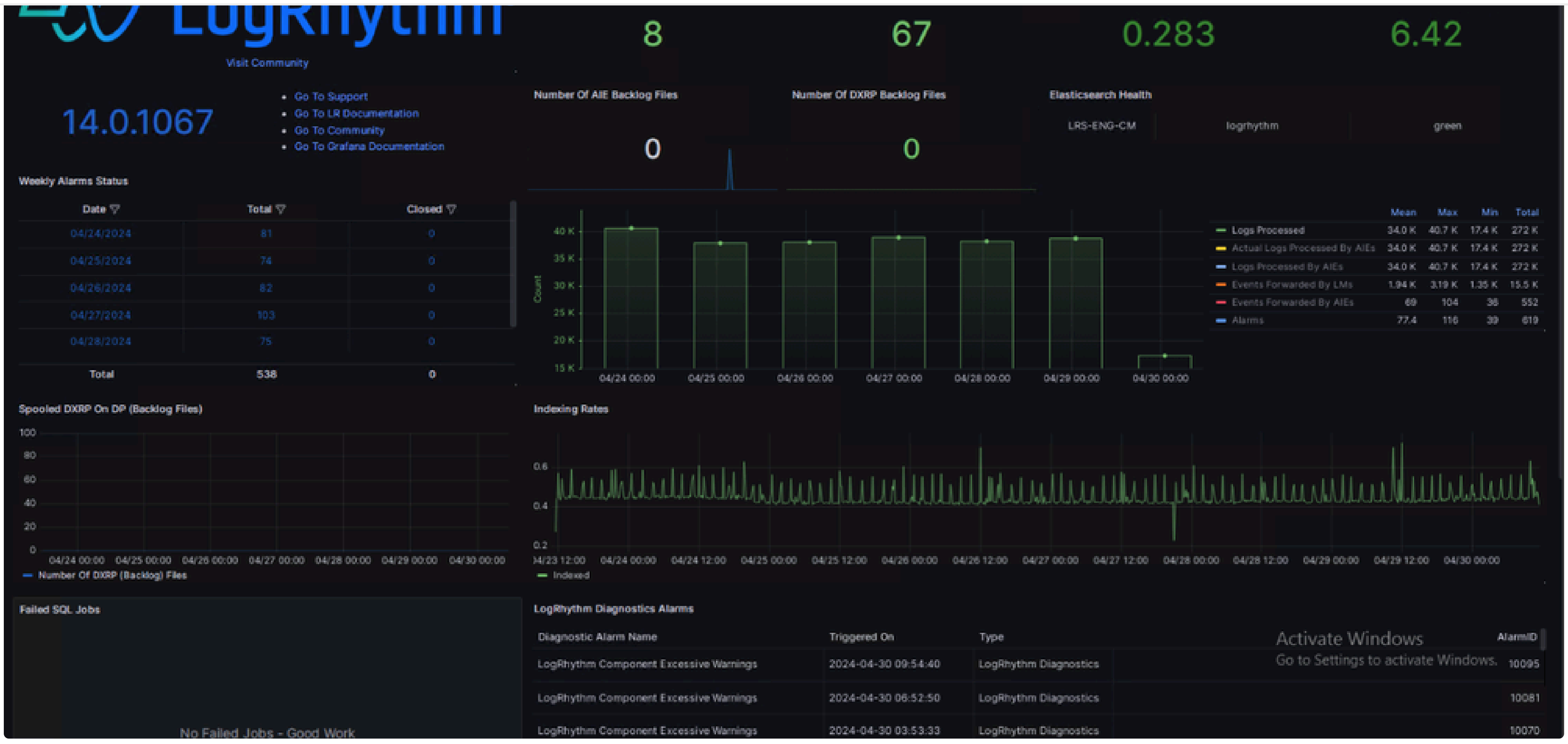
d71d3adb-ec99-48ce-a9ec-162ccd7c7593

Elasticsearch: Elasticsearch

EMDB Database: Microsoft SQL Server

Microsoft SQL Server: Microsoft SQL Server

telegraf: telegraf



14.0.1067

- Go To Support
- Go To LR Documentation
- Go To Community
- Go To Grafana Documentation

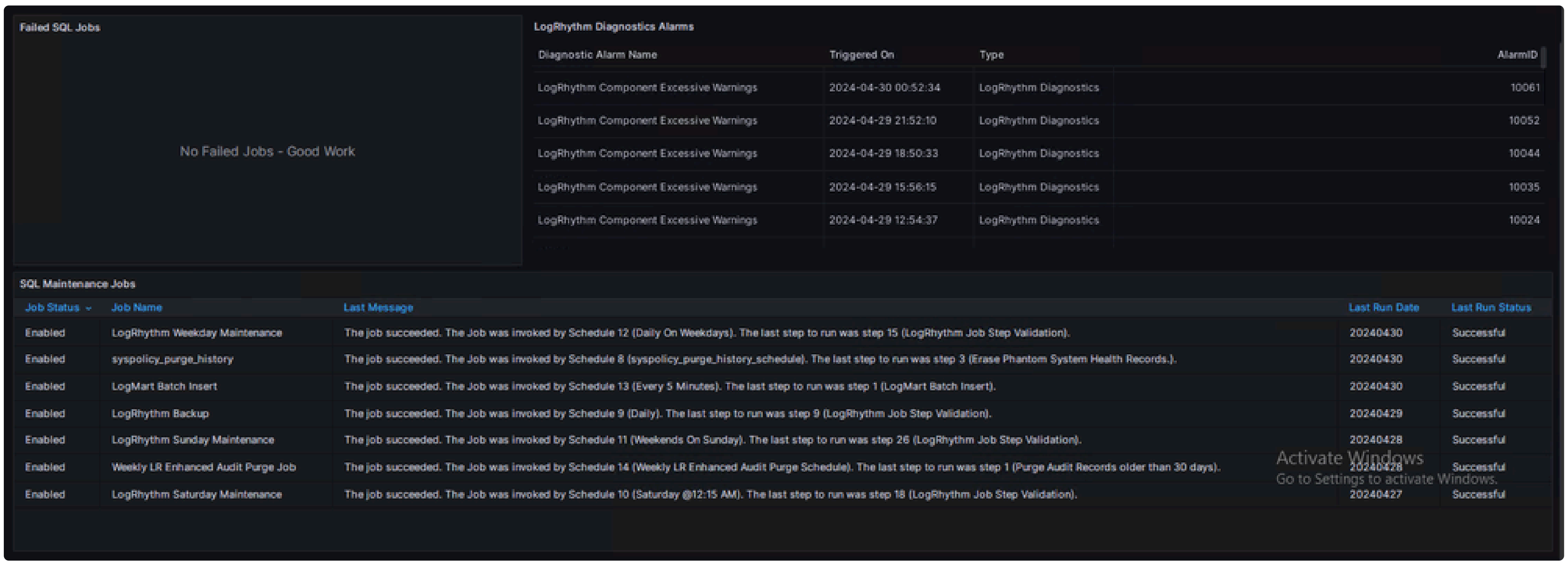
Weekly Alarms Status

Date	Total	Closed
04/24/2024	81	0
04/25/2024	74	0
04/26/2024	82	0
04/27/2024	103	0
04/28/2024	75	0
Total	538	0

	Mean	Max	Min	Total
Logs Processed	34.0 K	40.7 K	17.4 K	272 K
Actual Logs Processed By AIEs	34.0 K	40.7 K	17.4 K	272 K
Logs Processed By AIEs	34.0 K	40.7 K	17.4 K	272 K
Events Forwarded By LMs	1.94 K	3.19 K	1.35 K	15.5 K
Events Forwarded By AIEs	69	104	36	552
Alarms	77.4	116	39	619

LogRhythm Diagnostics Alarms

Diagnostic Alarm Name	Triggered On	Type	AlarmID
LogRhythm Component Excessive Warnings	2024-04-30 09:54:40	LogRhythm Diagnostics	10095
LogRhythm Component Excessive Warnings	2024-04-30 06:52:50	LogRhythm Diagnostics	10081
LogRhythm Component Excessive Warnings	2024-04-30 03:53:33	LogRhythm Diagnostics	10070


Failed SQL Jobs
No Failed Jobs - Good Work
Activate Windows
Go to Settings to activate Windows.

LogRhythm Diagnostics Alarms

Diagnostic Alarm Name	Triggered On	Type	AlarmID
LogRhythm Component Excessive Warnings	2024-04-30 00:52:34	LogRhythm Diagnostics	10061
LogRhythm Component Excessive Warnings	2024-04-29 21:52:10	LogRhythm Diagnostics	10052
LogRhythm Component Excessive Warnings	2024-04-29 18:50:33	LogRhythm Diagnostics	10044
LogRhythm Component Excessive Warnings	2024-04-29 15:56:15	LogRhythm Diagnostics	10035
LogRhythm Component Excessive Warnings	2024-04-29 12:54:37	LogRhythm Diagnostics	10024

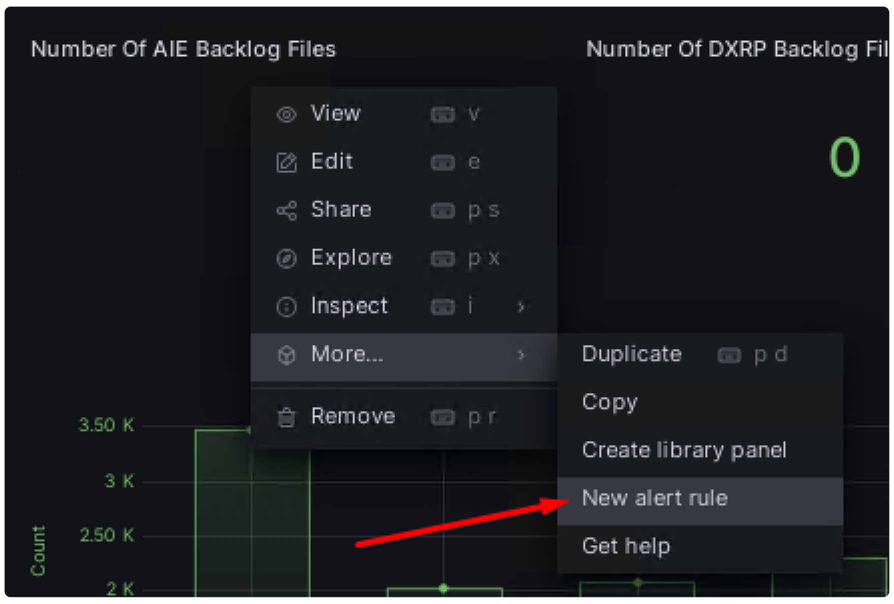
SQL Maintenance Jobs

Job Status	Job Name	Last Message	Last Run Date	Last Run Status
Enabled	LogRhythm Weekday Maintenance	The job succeeded. The Job was invoked by Schedule 12 (Daily On Weekdays). The last step to run was step 15 (LogRhythm Job Step Validation).	20240430	Successful
Enabled	syspolicy_purge_history	The job succeeded. The Job was invoked by Schedule 8 (syspolicy_purge_history_schedule). The last step to run was step 3 (Erase Phantom System Health Records.).	20240430	Successful
Enabled	LogMart Batch Insert	The job succeeded. The Job was invoked by Schedule 13 (Every 5 Minutes). The last step to run was step 1 (LogMart Batch Insert).	20240430	Successful
Enabled	LogRhythm Backup	The job succeeded. The Job was invoked by Schedule 9 (Daily). The last step to run was step 9 (LogRhythm Job Step Validation).	20240429	Successful
Enabled	LogRhythm Sunday Maintenance	The job succeeded. The Job was invoked by Schedule 11 (Weekends On Sunday). The last step to run was step 26 (LogRhythm Job Step Validation).	20240428	Successful
Enabled	Weekly LR Enhanced Audit Purge Job	The job succeeded. The Job was invoked by Schedule 14 (Weekly LR Enhanced Audit Purge Schedule). The last step to run was step 1 (Purge Audit Records older than 30 days).	20240428	Successful
Enabled	LogRhythm Saturday Maintenance	The job succeeded. The Job was invoked by Schedule 10 (Saturday @12:15 AM). The last step to run was step 18 (LogRhythm Job Step Validation).	20240427	Successful

Creating Alerts: Circling back to some of the original items I mentioned, lets create some alerts that allow us to monitor the below things and send an email if a certain threshold is met.

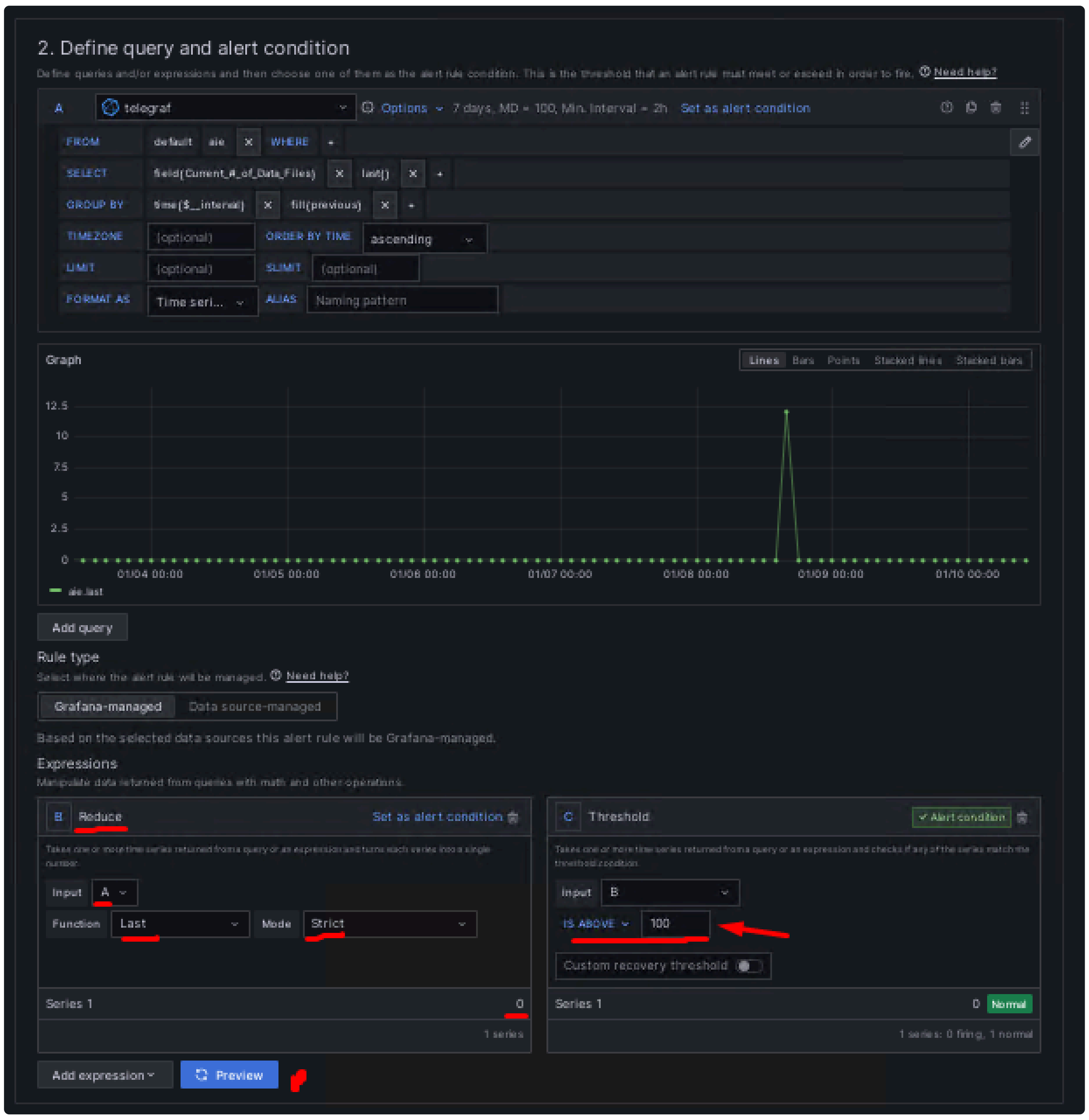
- There is currently no way to raise an alarm if there is DXRP build up.
- You don't get alarms if a SQL maintenance or backup job fails.
- There is no alarms/alerts for when your indexing rate drops below a certain threshold.

The fastest way to do this is to pick a working widget in a dashboard, whilst logged in as an admin to Grafana, click on the 3 dots in the corner and click "create alert rule".



At this point I highly reccomend checking out the official guidance from Grafana on how to configure alerts, but I will provide an example below anyway. **[https://www.youtube.com/watch?v=6W8Nu4b_PXM .](https://www.youtube.com/watch?v=6W8Nu4b_PXM)** backlog file count, is above 100, then fire the alarm. You can test the alarm by setting that amount to -1 and pressing preview, or you can change it to IS BELOW 100, and pressing preview - Just ensure you set it all back to normal once you see the red "FIRING" notificaiton.

The second screenshot below illustrates the customization options for things like how often to review, how often to send the emails if there is an issue, tags, anotations and other less used features etc.



2. Define query and alert condition

Define queries and/or expressions and then choose one of them as the alert rule condition. This is the threshold that an alert rule must meet or exceed in order to fire. Need help?

A telegraf Options 7 days, MD = 100, Min. Interval = 2h Set as alert condition

FROM default aie WHERE +

SELECT field(Current_#_of_Data_Files) last() +

GROUP BY time($__interval) fill(previous) +

TIMEZONE (optional) ORDER BY TIME ascending

LIMIT (optional) SLIMIT (optional)

FORMAT AS Time seri... ALIAS Naming pattern

Rule type

Select where the alert rule will be managed. Need help?

Grafana-managed Data source-managed

Based on the selected data sources this alert rule will be Grafana-managed.

Expressions

Manipulate data returned from queries with math and other operations.

B Reduce Set as alert condition

Takes one or more time series returned from a query or an expression and turns each series into a single number.

Input A

Function Last Mode Strict

Series 1 0

1 series

C Threshold ✓ Alert condition

Takes one or more time series returned from a query or an expression and checks if any of the series match the threshold condition.

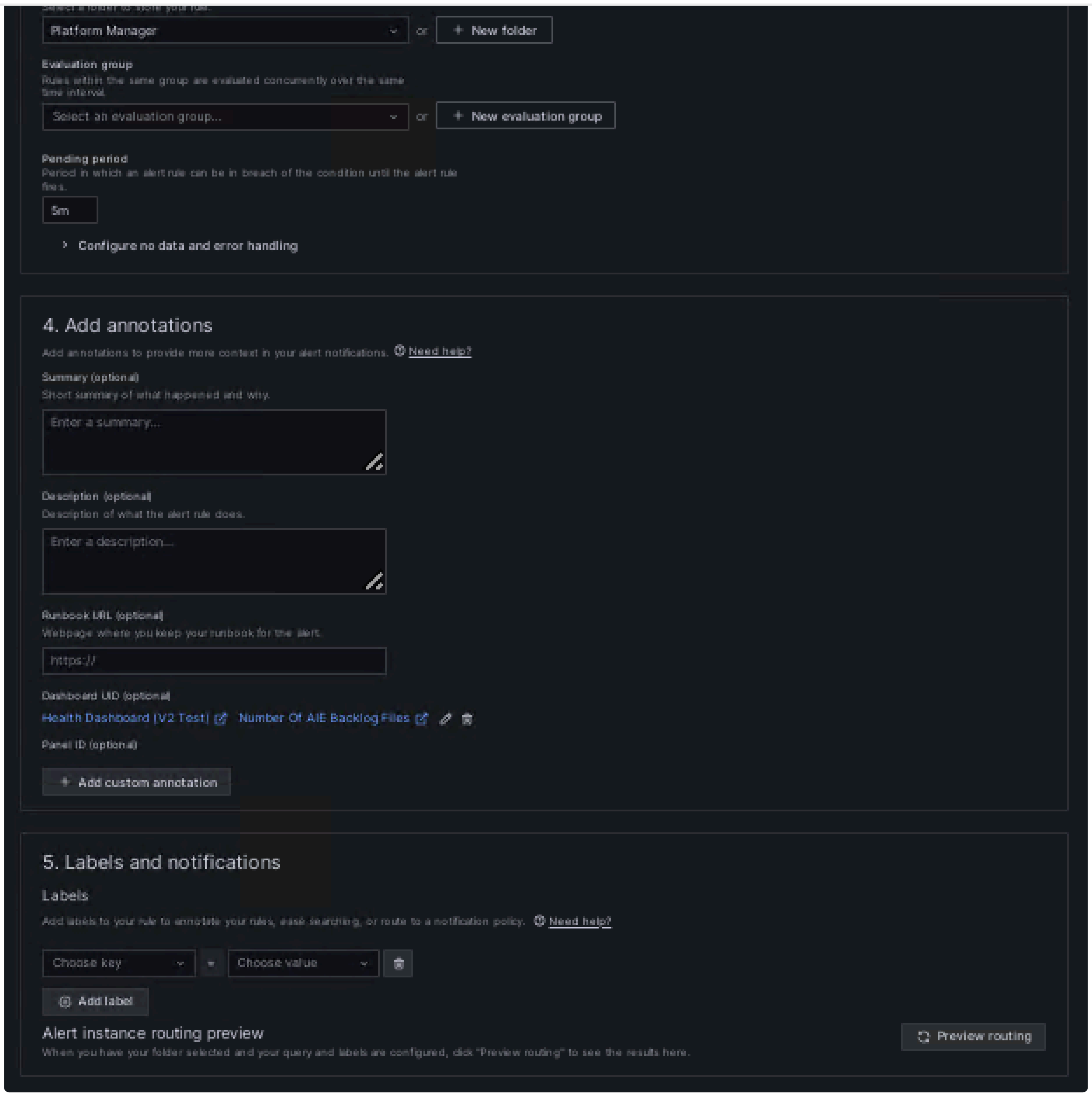
Input B

IS ABOVE 100

Custom recovery threshold

Series 1 0 Normal

1 series: 0 firing, 1 normal



Platform Manager ⌄ or + New folder

Evaluation group
Rules within the same group are evaluated concurrently over the same time interval.

Select an evaluation group... ⌄ or + New evaluation group

Pending period
Period in which an alert rule can be in breach of the condition until the alert rule fires.

5m

› Configure no data and error handling

4. Add annotations

Add annotations to provide more context in your alert notifications. Need help?

Summary (optional)
Short summary of what happened and why.

Enter a summary...

Description (optional)
Description of what the alert rule does.

Enter a description...

Runbook URL (optional)
Webpage where you keep your runbook for the alert.

https://

Dashboard UID (optional)
Health Dashboard (V2 Test) Number Of AIE Backlog Files

Panel ID (optional)

+ Add custom annotation

5. Labels and notifications

Labels

Add labels to your rule to annotate your rules, ease searching, or route to a notification policy. Need help?

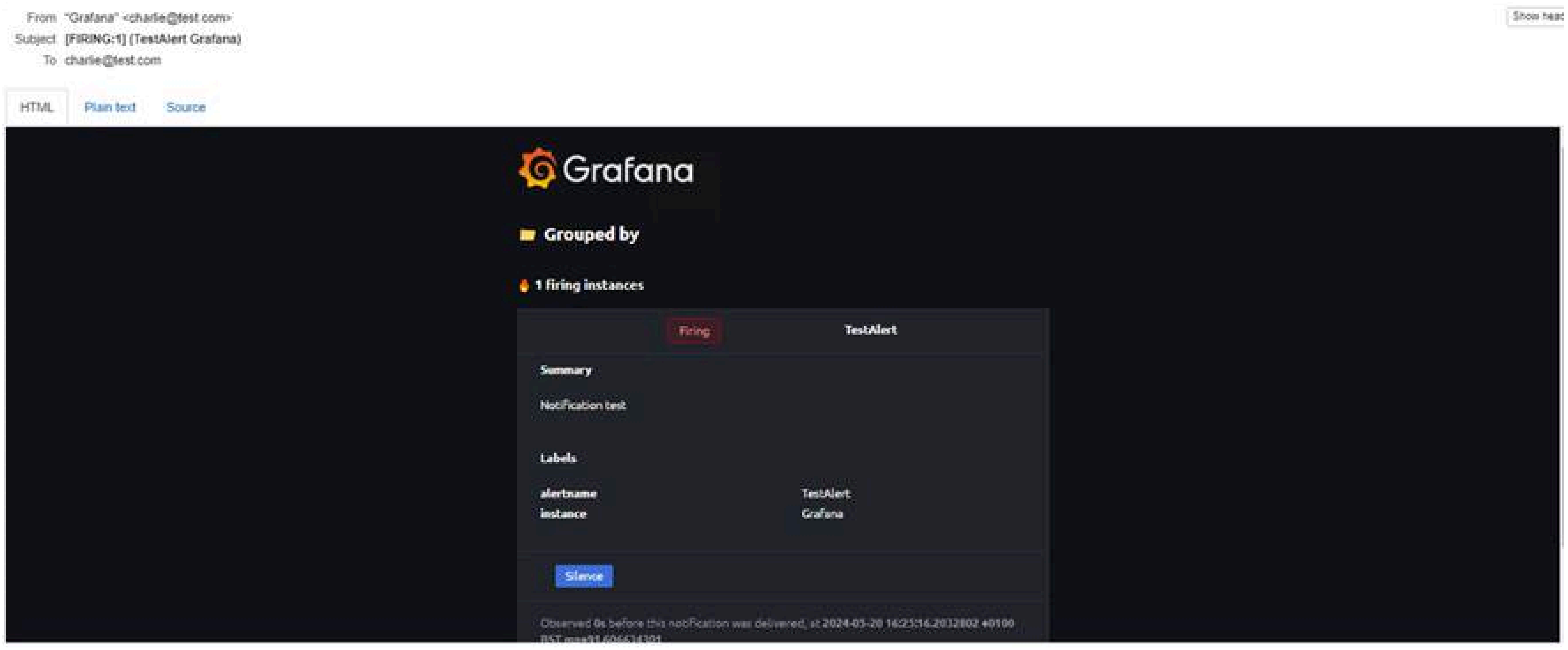
Choose key ⌄ = Choose value ⌄

Add label

Alert instance routing preview
When you have your folder selected and your query and labels are configured, click "Preview routing" to see the results here.

Preview routing

You can edit the contents of the email notifications for specific alert rules, the logo, who gets the email, how often they are sent when an issue is detected etc. It's all heavily customizable.



From "Grafana" <charlie@test.com>
Subject [FIRING:1] (TestAlert Grafana)
To charlie@test.com

HTML Plain text Source

Grafana

Grouped by

1 firing instances

Firing TestAlert

Summary

Notification test

Labels

alertname	TestAlert
instance	Grafana

Silence

Observed 0s before this notification was delivered, at 2024-05-20 16:23:16.2032802 +0100 BST m=+91.606634301

Closing Statement - Going Forward: I will be adding to this page with example of alerts that we have seen in Production, tweaking any points that need clarificaiton and generally supporting the customer bases questions from this page. If you yourself have created any useful alerts that others would benefit from please share the configuration in the comments and lets see if we can get some support behind this.

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

ALERTING ✕ CUSTOM ✕ EMAILS ✕ GRAFANA ✕ MONITORING ✕ PLATFORM ✕ PLATFORM MANAGMENT ✕ SMTP ✕ + TAG

9 Reply

charliemac