

Table of Contents

Splunk Homework Assignment	2
Task 1	3
Task 2	5
Task 3	7
Task 4	10
Task 5	13

Splunk Homework Assignment

Objective:

Demonstrate your ability to set up and use Splunk with Docker containers for log analysis.

Task 1: Docker Setup

1. Install Docker on your local machine if you haven't already.
2. Pull the official Splunk Docker image from Docker Hub.
3. Create a Docker container with Splunk running. Ensure that the container exposes necessary ports.

Task 2: Log Ingestion with Docker

1. Ingest sample log data into your Splunk container. You can use any sample log data available online or create your own.
2. Verify that the logs are successfully ingested and searchable in Splunk.

Task 3: Basic Search and Visualization

1. Use Splunk search commands to find the count of events with a specific keyword in the logs.
2. Create a basic visualization (chart or graph) based on a search query of your choice.

Task 4: Dockerized Deployment

1. Dockerize a custom application (could be a simple Python script generating logs) and send its logs to your Splunk container.
2. Confirm that the logs from your custom application are being indexed and searchable in Splunk.

Task 5: Alerts and Monitoring

1. Set up an alert to notify you if there are more than 5 error events in the last hour.
2. Monitor the real-time logs for any events containing the word "warning" and display them in real-time.

I've started with Windows and switched to Kali 2023 – explanation below

Task 1

1. Download the Splunk image, using the command: `docker pull splunk/splunk:latest`
2. Run the image, using the command: `docker run -d -p 8000:8000 -p 8080:8080 -e SPLUNK_START_ARGS='--accept-license' -e SPLUNK_PASSWORD='password' --name splunk splunk/splunk:latest`
3. The container is initializing, wait for it to complete. You can use the command: `docker ps` - To see all the containers data including status

```
(root@kali)~[/home/kali]
# docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
f86be3a526aa	splunk/splunk:latest	"/sbin/entrypoint.sh..."	13 minutes ago	Up 6 minutes (healthy)	8065/tcp, 8088-8089/tcp, 8191/tcp, 9887/tcp, 0.0.0.0:8000→8000/tcp, :::8000→8000/tcp, 9997/tcp	splunk

4. The Splunk container is up and running <Kali_IP:8000> or from the Kali machine <localhost:8000>

The screenshot displays the Splunk Enterprise Administrator interface. At the top, there's a navigation bar with 'splunk>enterprise' and 'Apps' dropdown. Below this, a sidebar on the left offers navigation options: 'Search & Reporting', 'Splunk Secure Gateway', and 'Upgrade Readiness App'. The main content area is titled 'Hello, Administrator' and includes a 'Quick links' section with tabs for 'Dashboard', 'Recently viewed', 'Created by you', and 'Shared with you'. The 'Common tasks' section features four cards: 'Add data', 'Search your data', 'Visualize your data', and 'Add team members'. Below this, the 'Learning and resources' section contains four cards: 'Product tours', 'Learn more with Splunk Docs', 'Get help from Splunk experts', and 'Extend your capabilities'. The bottom row includes 'Join the Splunk Community', 'See how others use Splunk', and 'Training and Certification'.

Problems:

I had a problem with the stage 2 when running the container on Windows environment:

```
TASK [splunk_standalone : Setup global HEC] *****
fatal: [localhost]: FAILED! => {
  "cache_control": "private",
  "changed": false,
  "connection": "Close",
  "content_length": "130",
  "content_type": "text/xml; charset=UTF-8",
  "date": "Thu, 11 Jan 2024 16:25:03 GMT",
  "elapsed": 0,
  "redirected": false,
  "server": "Splunkd",
  "status": 401,
  "url": "https://127.0.0.1:8089/services/data/inputs/http/http",
  "vary": "Cookie, Authorization",
  "warnings": [
    "Module did not set no_log for password"
  ],
  "www_authenticate": "Basic realm=\"/splunk\"",
  "x_content_type_options": "nosniff",
  "x_frame_options": "SAMEORIGIN"
}

MSG:

Status code was 401 and not [200]: HTTP Error 401: Unauthorized
```

This is because the Splunk user does not have permission to edit the /var directory. I switched to Kali 2023 on VMware player, and ran it as root, the problem was solved. There is a quick fix in the (2) resource ("ANSIBLE_EXTRA_FLAGS=-vv"), but it's mainly for DEBUG proposes, so I want with the Kali solution. Also, my computer is performing better with this technique.

Resources:

1. [Deploy and run Splunk Enterprise inside a Docker container - Splunk Documentation](#)
2. [Unable to install Standalone Splunk when using doc... - Splunk Community](#)
3. [Data Storage ## | docker-splunk](#)
4. [Navigation | docker-splunk](#)

Note:

In the second stage I've exposed two ports. One for the Splunk Enterprise and one for Task 4, where I will need an additional port to send data to Splunk.

To stop the container for later use, enter the following command in the Terminal:

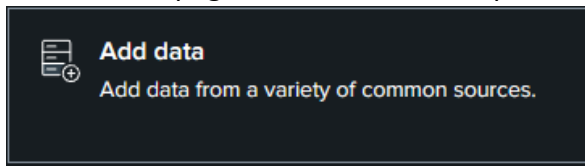
```
docker container stop <container_name>
```

To start the container, enter the following command in the Terminal:

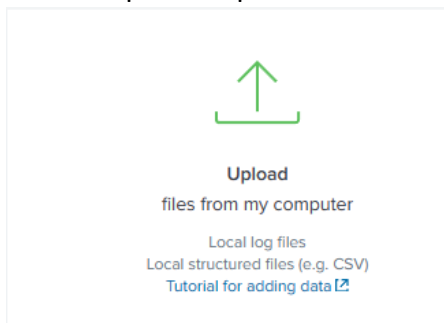
```
docker container start <container_name>
```

Task 2

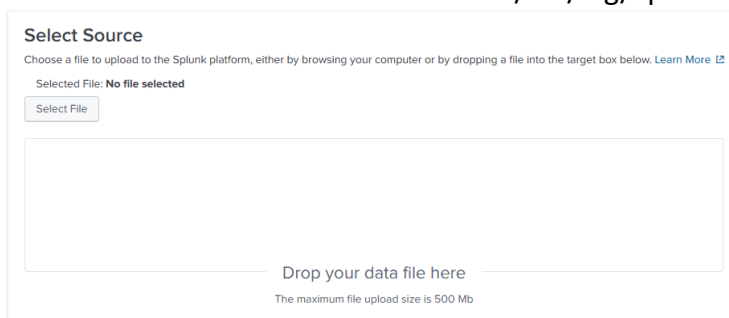
1. At the home page select “Add data” option



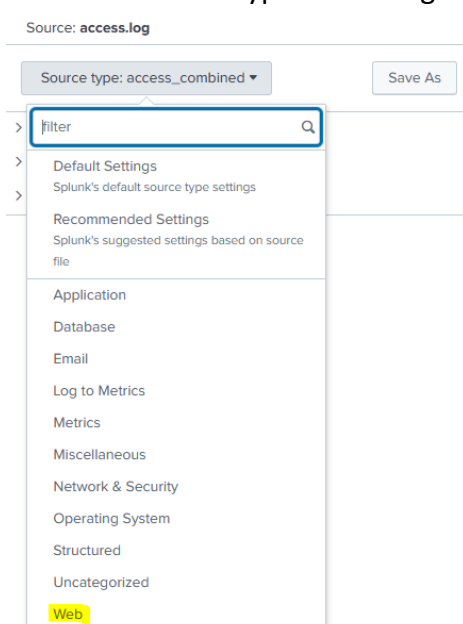
2. Select “Upload” option



3. In this page select the log files you want to add. I’ve used dummy logs from apache2 web server. Location on Linux machine /var/log/apache2. (access.log)



4. Select the source type for the log file. I’ve selected a type from the web option.



5. Review

Review

Input Type Uploaded File
File Name error.log
Source Type apache2_error
Host 49cd50baed3a
Index Default

6. Complete

✓ File has been uploaded successfully.
Configure your inputs by going to Settings > Data Inputs

Start Searching Search your data now or see examples and tutorials. [↗](#)

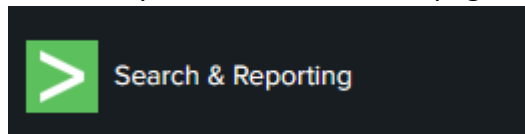
Extract Fields Create search-time field extractions. [Learn more about fields. ↗](#)

Add More Data Add more data inputs now or see examples and tutorials. [↗](#)

Download Apps Apps help you do more with your data. [Learn more. ↗](#)

Build Dashboards Visualize your searches. [Learn more. ↗](#)

7. I've uploaded a file named access.log, record the access to the web server.
8. To search your data at the home page, select "Search & Reporting" option



9. You can search your events by host, sourcetype, source or any other data you have.
for example: IP address

New Search Save As Create Table View Close

source="access.log" All time Q

✓ 10,000 events (before 1/14/24 7:58:18.000 AM) No Event Sampling Job II ■ ↗ ↻ ↓ Smart Mode

Events (10,000) Patterns Statistics Visualization

Format Timeline Zoom Out + Zoom to Selection X Deselect 1 hour per column

< Hide Fields All Fields

SELECTED FIELDS
host 1
source 1
sourcetype 1

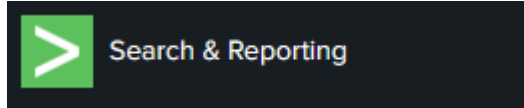
INTERESTING FIELDS
bytes 100+
clientip 100+
date_hour 24
date_mday 1
date_minute 1
date_month 1
date_second 60
date_wday 1
date_year 1
date_zone 1
file 100+
idnet 1
index 1
linecount 1
method 4
punct 100+
referer 100+
referer_domain 100+
req_time 100+
root 24

#	Time	Event
>	5/20/23 11:05:59.000 PM	193.185.55.253 - - [19/May/2015:23:05:59 +0000] "GET /favicon.ico HTTP/1.0" 200 3638 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0" host = dcd5fab1a50 source = access.log sourcetype = access_combined
>	5/20/23 11:05:59.000 PM	130.237.218.86 - - [19/May/2015:23:05:59 +0000] "GET /presentations/logstash-intro/file/intro-logging-problems/apache-response-codes.png HTTP/1.1" 200 52878 "http://semicomplete.com/presentations/logstash-intro/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36" host = dcd5fab1a50 source = access.log sourcetype = access_combined
>	5/20/23 11:05:58.000 PM	217.195.282.13 - - [19/May/2015:23:05:58 +0000] "GET / HTTP/1.1" 200 37932 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" host = dcd5fab1a50 source = access.log sourcetype = access_combined
>	5/20/23 11:05:58.000 PM	130.237.218.86 - - [19/May/2015:23:05:58 +0000] "GET /presentations/logstash-intro/css/theme/ui.core.css HTTP/1.1" 200 1352 "http://semicomplete.com/presentations/logstash-intro/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36" host = dcd5fab1a50 source = access.log sourcetype = access_combined
>	5/20/23 11:05:58.000 PM	130.237.218.86 - - [19/May/2015:23:05:58 +0000] "GET /presentations/logstash-intro/file/style.css HTTP/1.1" 200 573 "http://semicomplete.com/presentations/logstash-intro/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36" host = dcd5fab1a50 source = access.log sourcetype = access_combined
>	5/20/23 11:05:58.000 PM	60.234.195.253 - - [18/May/2015:23:05:58 +0000] "GET /presentations/logstash-scale11x/images/ahhh__rage_face_by_samusmx-d5g5zap.png HTTP/1.1" 200 175208 "http://s-chassis.co.nz/viewtopic.php?f=16&t=9265" "Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko" host = dcd5fab1a50 source = access.log sourcetype = access_combined
>	5/20/23 11:05:58.000 PM	196.14.132.154 - - [18/May/2015:23:05:58 +0000] "GET /blog/peekery/ssl-latency.html HTTP/1.1" 200 17147 "https://www.google.co.za/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = dcd5fab1a50 source = access.log sourcetype = access_combined
>	5/20/23 11:05:58.000 PM	66.249.73.135 - - [18/May/2015:23:05:58 +0000] "GET /blog/peekery/77.html HTTP/1.1" 200 9102 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)" host = dcd5fab1a50 source = access.log sourcetype = access_combined

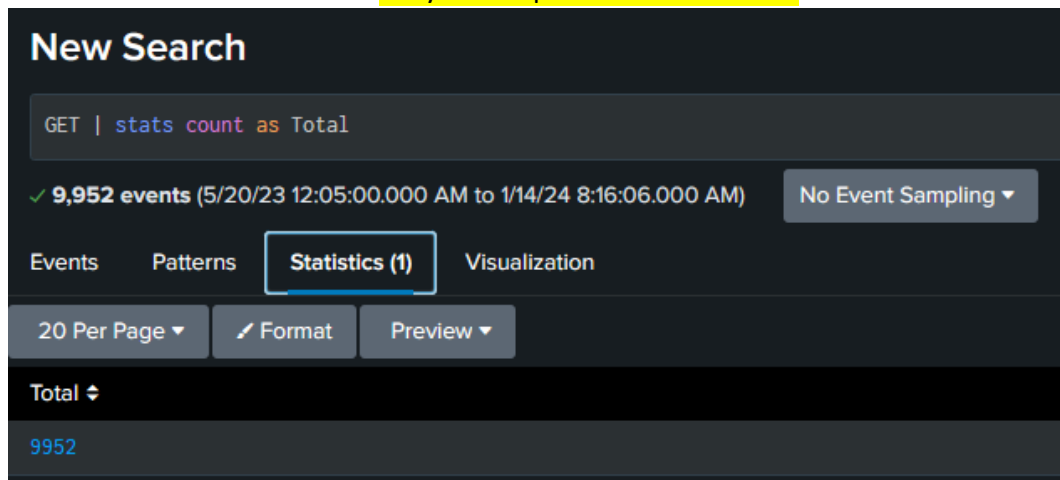
Task 3

Please take a look at the image from Task 2 stage 8. We can see a keyword GET. Let's return the count of events that have this keyword in them.

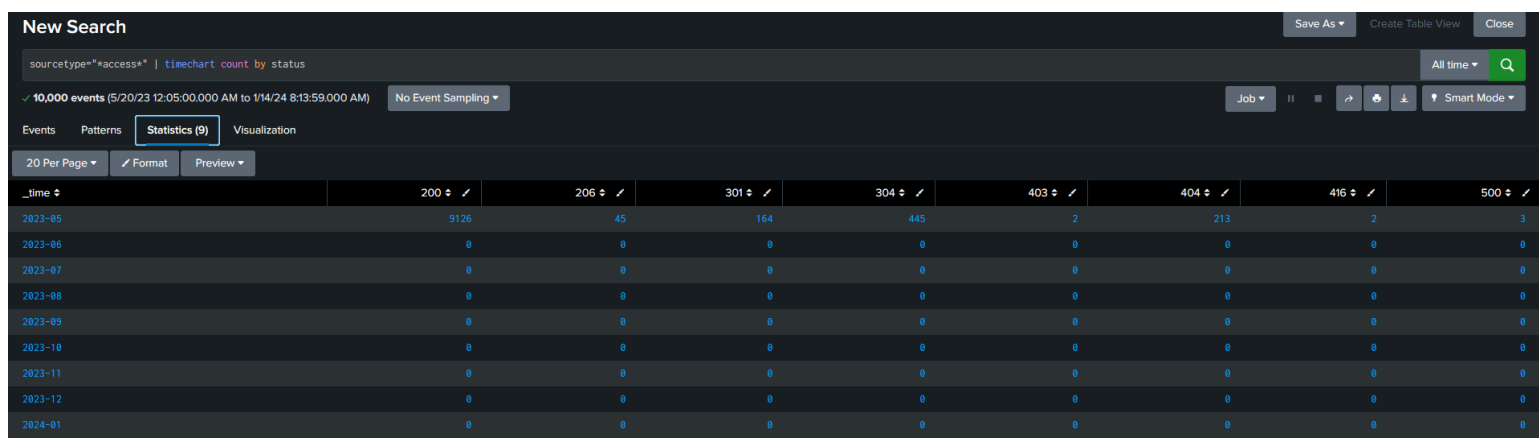
1. In Splunk, from the main page, click the search button

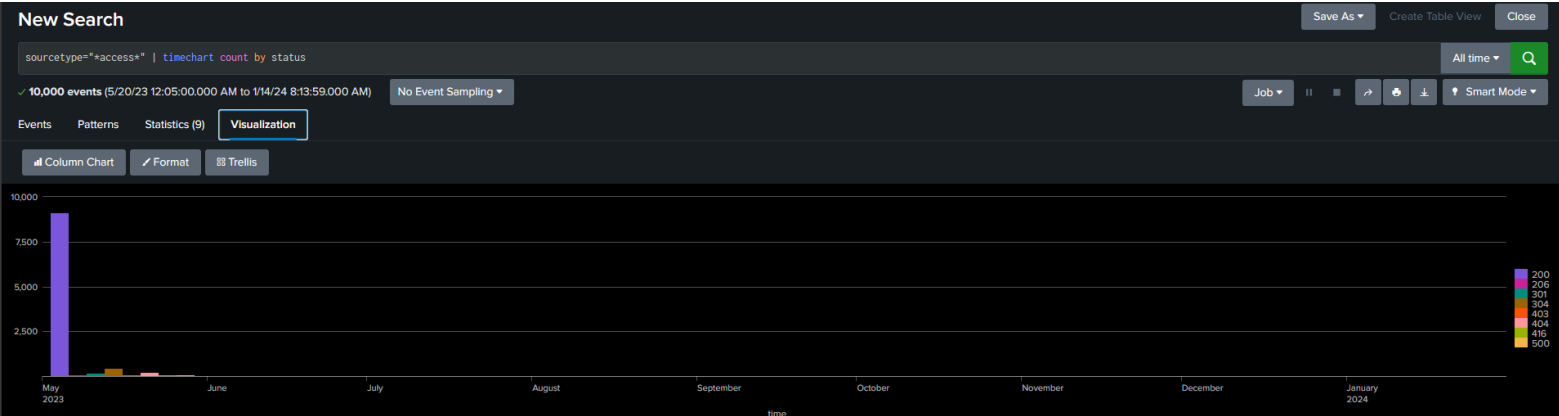


2. To count the number of events that have this keyword use the following command in the search bar: `<keyword> | stats count as Total`



3. Now we want to visualize our data. I will show two different ways to create a basic visualization for the data:
 - I. Using the following command: `sourcetype="*access*" | timechart count by status`. `sourcetype="*access*"` will find all source types with the word access in them. (* means - I don't care what comes before and after the word). The second part of the command will generate a time chart from the data using the status field.





II. To show the status codes without time stamp use the commend:
`sourcetype="*access*" | chart count(eval(status>=400)) as "Error" count(eval(status<399)) as "OK" by status`

The second part of the command splits the status codes in two – error and ok. The eval command calculates an expression and puts the resulting value into a field. Next set all the error codes to a label named “Error” and the successful codes in to the “OK” label to display on the chart.

New Search

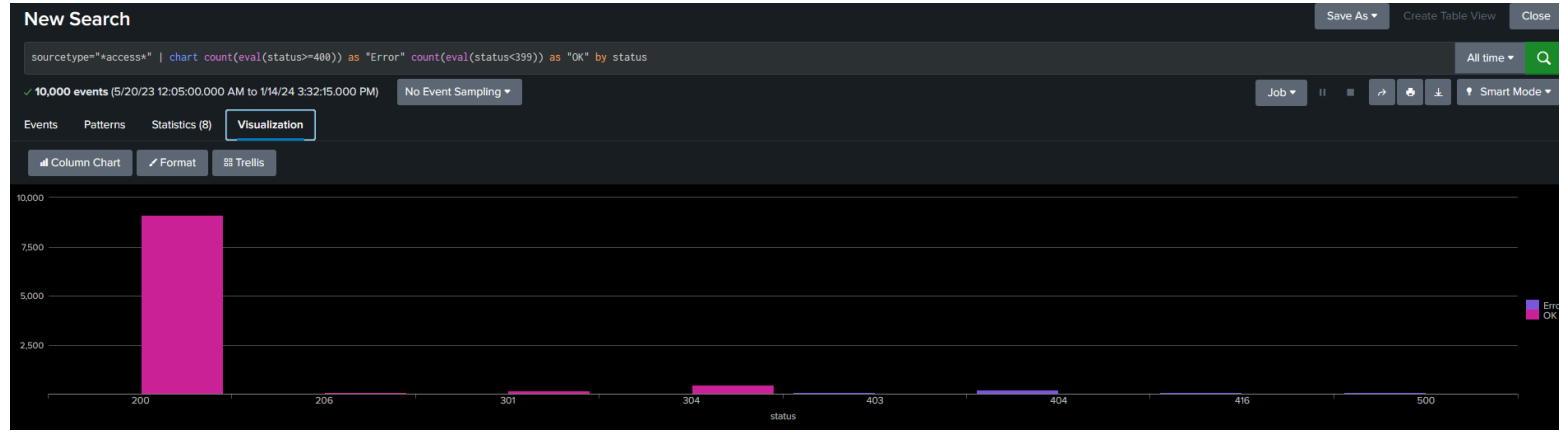
sourcetype="*access*" | chart count(eval(status>=400)) as "Error" count(eval(status<399)) as "OK" by status

10,000 events (5/20/23 12:05:00.000 AM to 1/14/24 3:32:15.000 PM) No Event Sampling

Events Patterns Statistics (8) Visualization

20 Per Page Format Preview

status	Error	OK
200	0	9126
206	0	45
301	0	164
304	0	445
403	2	0
404	213	0
416	2	0
500	3	0



Problems:

I had a problem with the visualization of the data I've uploaded to Splunk. I saw online that some peoples use status as a variable in the search bar, so I've came to the conclusion that the way I've uploaded the data was incorrect. I've uploaded the data again but now used the propre type for the data and got a status field for each event. Finally, I've updated Task 2 in this document.

1/11/24
11:39:49.000 PM

192.168.204.128 - - [11/Jan/2024:18:39:49 -0500] "GET /mcvcore.maki HTTP/1.1" 200 17419 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:109.0) Gecko/20100101 Firefox/115.0"

Event Actions

Type	Field	Value	Actions
Selected	host	f86be3a526aa	
	source	access.log	
	sourcetype	access_combined	
Event	bytes	17419	
	clientip	192.168.204.128	
	file	mcvcore.maki	
	ident	-	
	method	GET	
	referer	-	
	req_time	11/Jan/2024:18:39:49 -0500	
	status	200	
	uri	/mcvcore.maki	
	uri_path	/mcvcore.maki	
	user	-	
	useragent	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:109.0) Gecko/20100101 Firefox/115.0	
	version	HTTP/1.1	
	Time	_time	2024-01-11T23:39:49.000+00:00
Default	index	main	
	linecount	1	
	punct	..._...[/...]*.../...*(...)	
	splunk_server	f86be3a526aa	

Note:

I've deleted the old data with the command: `<search_query> | delete`

For this command to execute successfully you need to add a `can_delete` permission to the user you are working with. Find it in Settings -> Roles.

After deleting the data I've removed this permission for security reasons.

Resources:

[Solved: How to count number of events in a search result? - Splunk Community](#)

[Solved: How to chart a daily count of HTTP status codes di... - Splunk Community](#)

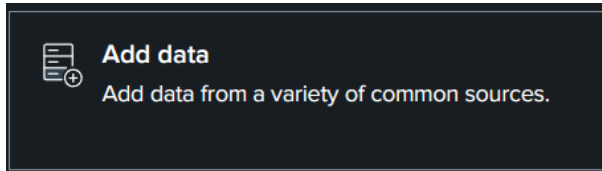
[Solved: How to display table of total error status code an... - Splunk Community](#)

[Create a basic chart - Splunk Documentation](#)

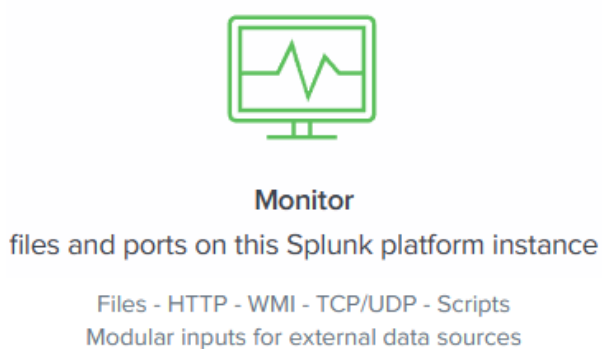
Task 4

The python script reads from a dummy log file and send the data to the Splunk Container.

1. let's set up a TCP connection to the Splunk container. Remember we have one more exposed port (8080) to use for this purpose. In the main page of Splunk click on add data



2. Click on the monitor option



3. Then click on the TCP/UDP option and enter a port (8080). For security reasons set up the docker IP as the only accept connection.

Files & Directories Upload a file, index a local file, or monitor an entire directory.	<p>Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More</p> <div><div>TCP</div><div>UDP</div></div> <p>Port ? <input type="text" value="8080"/> Example: 514</p> <p>Source name override ? <input type="text" value="optional"/> host:port</p> <p>Only accept connection from ? <input type="text" value="172.17.0.1"/> example: 10.1.2.3, !badhost.splunk.com, *.splunk.com</p>
HTTP Event Collector Configure tokens that clients can use to send data over HTTP or HTTPS.	
TCP / UDP > Configure the Splunk platform to listen on a network port.	
Scripts Get data from any API, service, or database with a script.	
Splunk Assist Instance Identifier Assigns a random identifier to every node	
Systemd Journal Input for Splunk	

- Source type should be `mysql_error`. I've created a new index – `Python_data`, a repository for all the data (events) sent by Python.

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Select New

mysql_error ▼

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

App Context

Search & Reporting (search) ▼

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Method ?

IP DNS Custom

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index

python_data ▼

[Create a new index](#)

- Finally, review the TCP input

Review

Input Type	TCP Port
Port Number	8080
Source name override	N/A
Restrict to Host	N/A
Source Type	mysql_error
App Context	search
Host	(DNS entry of the remote server)
Index	python_data

Next step is to set up a container with our simple application –

- Copy the Python script and the log file to the Kali machine, to a directory.
- We need to create a Dockerfile to create an image out of our script. Enter this command in the terminal: **touch Dockerfile**
- Use the text editor or vim (Linux command) to edit the file (I'm including the files in the email). We used a base image of Alpine Linux running Python, a minimalist Linux distro, which helps keep the images for Docker small. COPY will move the application into the container image, WORKDIR sets the working directory.

9. Now we need to build an image with the command: `docker build --tag send_data_to_splunk .`

The name of the image is `send_data_to_splunk`

10. Finally, we can start the application as a container, using the command: `docker run --name python-app send_data_to_splunk`

```
(root@kali)-[/home/kali]
# docker run --name python-app send_data_to_splunk
Connection has been made
Sending error number 0
Connection has been made
Sending error number 1
```

11. On the Splunk search we can search for those events

The screenshot shows the Splunk Search interface. The search bar contains the query: `source="tcp:8080" index="python_data" sourcetype="mysqld_error"`. The search results are displayed in a table with columns for Time and Event. The table shows 79 events, with the first few rows visible. The interface includes various controls like 'Format Timeline', 'Zoom Out', and 'List'.

Time	Event
1/11/24 2:26:40.672 PM	2024-01-11T14:26:40.672035Z 0 [System] [MY-010931] [Server] D:\Program Files\MySQL\MySQL Server 8.0\bin\mysqld.exe: ready for connections. Version: '8.0.35' socket: '' port: 3306 MySQL Community Server - GPL.
1/11/24 2:26:40.671 PM	2024-01-11T14:26:40.671802Z 0 [System] [MY-011323] [Server] X Plugin ready for connections. Bind-address: '::' port: 33060
1/11/24 2:26:40.182 PM	2024-01-11T14:26:40.182863Z 0 [System] [MY-013602] [Server] Channel mysql_main configured to support TLS. Encrypted connections are now supported for this channel.
1/11/24 2:26:40.181 PM	2024-01-11T14:26:40.181925Z 0 [Warning] [MY-010068] [Server] CA certificate ca.pem is self signed.
1/11/24 2:26:36.474 PM	2024-01-11T14:26:36.474432Z 1 [System] [MY-013577] [InnoDB] InnoDB initialization has ended.
1/11/24 2:26:31.100 PM	2024-01-11T14:26:31.100380Z 1 [System] [MY-013576] [InnoDB] InnoDB initialization has started.
1/11/24 2:26:30.506 PM	2024-01-11T14:26:30.506024Z 0 [System] [MY-010116] [Server] D:\Program Files\MySQL\MySQL Server 8.0\bin\mysqld.exe (mysqld 8.0.35) starting as process 7232
1/10/24 7:53:22.484 PM	2024-01-10T19:53:22.484220Z 0 [System] [MY-010910] [Server] D:\Program Files\MySQL\MySQL Server 8.0\bin\mysqld.exe: Shutdown complete (mysqld 8.0.35) MySQL Community Server - GPL.

Problems:

When I was trying to send all the file log without closing the socket, I got one long event. This is not a desired behavior, so I've closed the socket after every log (line in the file) sent and we got 79 events from a 79-line log file. To solve this problem, I've used common sense.

Note:

For this task I'm using dummy logs form MySQL Database. After research online I found that a quick setup of TCP on Splunk will give us the desirable solution to this task.

Recurses:

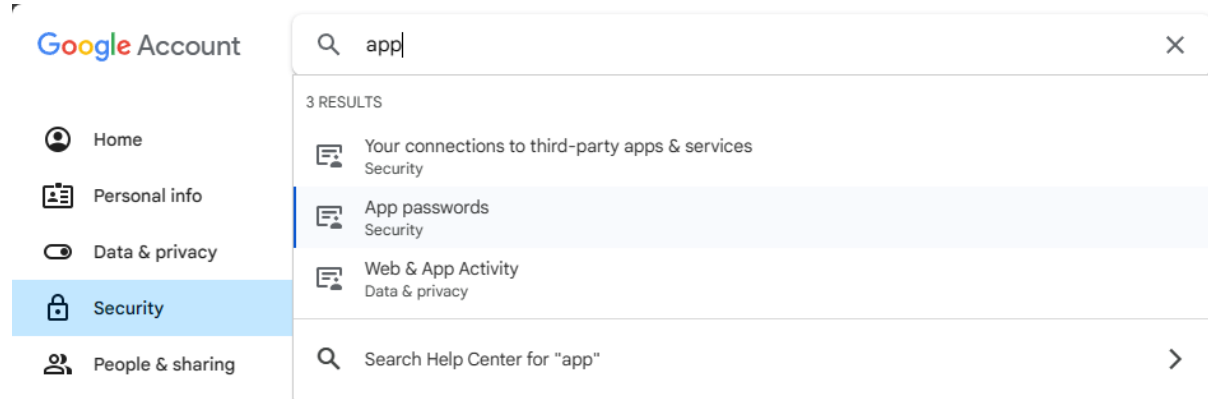
[how to send logs to splunk - חיפוש ב-Google](#)

[Containerize a Python App in 5 Minutes - Atmosera](#)

Task 5

In this task we want to set up real-time alerts for the incoming data from Task 4.

1. First, we want to receive an email for every event containing the word “warning”. For this purpose, I’ve used Gmail. To do so we need to set a new application. Go to Google account and search for app. Click on the app passwords.



2. Then you will need to set up a new app. You will get a password, please save it for later.


← App passwords

App passwords help you sign into your Google Account on older apps and services that don't support modern security standards.

App passwords are less secure than using up-to-date apps and services that use modern security standards. Before you create an app password, you should check to see if your app needs this in order to sign in.

[Learn more](#)

Your app passwords

Portfolio App (2)	Created on Oct 19, 2023, last used on Dec 3, 2023	
-------------------	---	---

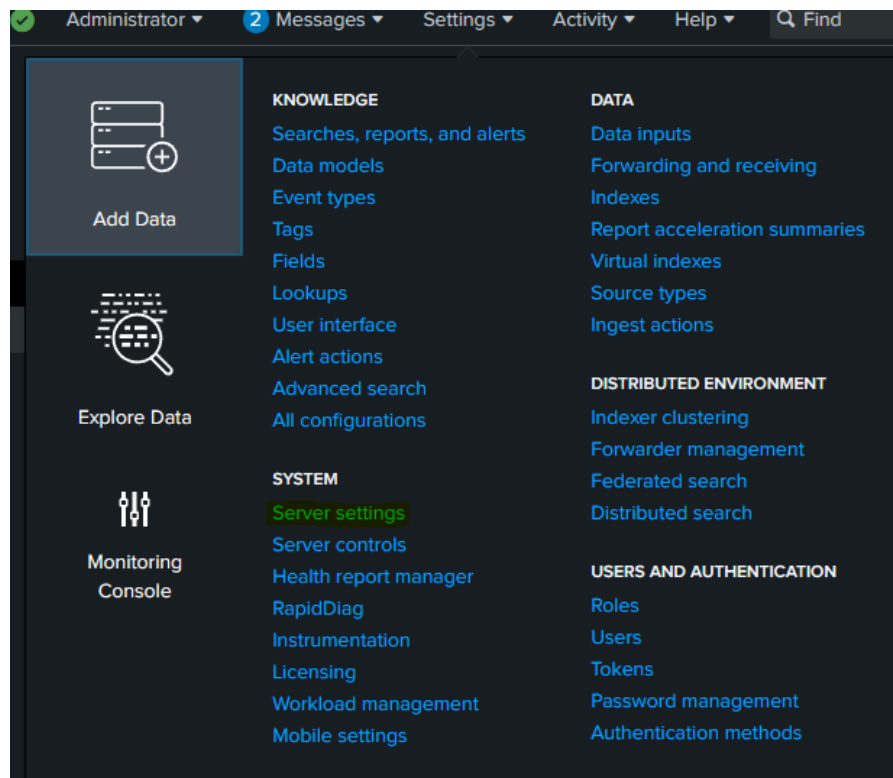
To create a new app specific password, type a name for it below...

App name

splunk

Create

3. We need to setup the email setting on Splunk. Go to Settings -> Server settings



4. Click on Email Settings

General settings
Login background
Global banner
Internal Library Settings
Email settings
Server logging
Deployment client
Search preferences

5. Set up the Mail host, username and password (the app password we created). Click Save.

Mail Server Settings

Mail host
Set the host that sends mail for this Splunk instance.

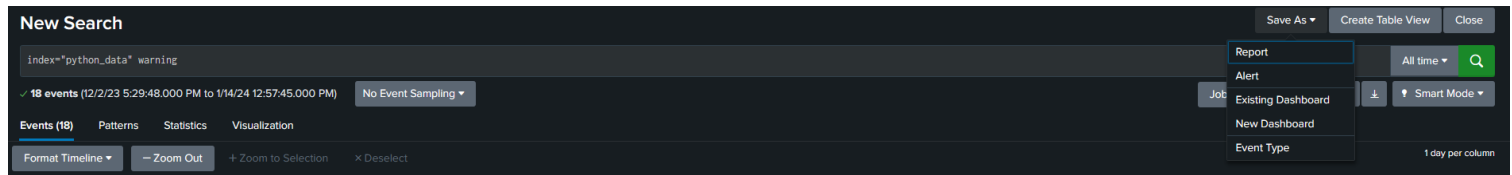
Email security ☐ none ☐ Enable SSL ☒ Enable TLS
Check with SMTP server admin. When SSL is enabled, mail host should include the port. IE: smtp.splunk.com:465

Username
Username to use when authenticating with the SMTP server. Leave empty for no authentication.

Password
Password to use when authenticating with the SMTP server.

Confirm password

6. Now we can set up an alert. Go to search and enter your query to the search bar. Then click Save As -> Alert. My search query is: `index="python_data" warning`



7. Enter a title, click on Real-time and add actions to when the alert is triggered. I've selected send email and add to triggered alerts. In the triggered alert action select the severity of the alert.

The screenshot shows the 'Save As Alert' dialog box. It has a 'Settings' section with fields for 'Title' (MySQL Warnings), 'Description' (Optional), 'Permissions' (Private/Shared In App), 'Alert type' (Scheduled/Real-time), and 'Expires' (24/hour(s)). Below this is the 'Trigger Conditions' section with 'Trigger alert when' set to 'Per-Result' and a 'Throttle' checkbox. The 'Trigger Actions' section shows a list of actions: 'Send email' and 'Add to Triggered Alerts', each with a 'Remove' button. At the bottom are 'Cancel' and 'Save' buttons.

8. In the send email enter the email address you want to alert. Check all the checkboxes for a detailed email about the event.

The screenshot shows the 'Send email' configuration dialog box. It has fields for 'To' (sefi0609@gmail.com), 'Priority' (Normal), and 'Subject' (Splunk Alert: \$name\$). Below these is a 'Message' field with the text 'The alert condition for '\$name\$' was triggered.' At the bottom, there are two columns of checkboxes under the 'Include' section: 'Link to Alert', 'Search String', 'Trigger Condition', 'Trigger Time', 'Allow Empty Attachment', 'Link to Results', 'Inline Table', 'Attach CSV', and 'Attach PDF'. The 'Type' section at the bottom has 'HTML & Plain Text' and 'Plain Text' options.

9. Snapshots of the email: (I've started the Python container again)

13:35 The alert condition for 'MySQL Warnings' was triggered. Alert: MySQL Warnings Search... - **Splunk Alert: MySQL Warnings** אני

...2024-01-14.csv ...2024-01-14.pdf

דואר נכנס Splunk Alert: MySQL Warnings

sefi0609@gmail.com אני

The alert condition for 'MySQL Warnings' was triggered.

Alert: [MySQL Warnings](#)

Search String: index="python_data" warning

Trigger: Saved Search [MySQL Warnings]: always

Trigger Time: 11:34:41 +0000 on January 14, 2024.

[View results in Splunk](#)

_raw	_time	host	index	linecount	source	sourcetype	splunk_server
2024-01-11T14:26:40.181925Z 0 [Warning] [MY-010068] [Server] CA certificate ca.pem is self signed.	Thu Jan 11 14:26:40 2024	_gateway	python_data		tcp:8080	mysqlid_error	dcdf5fab1a50

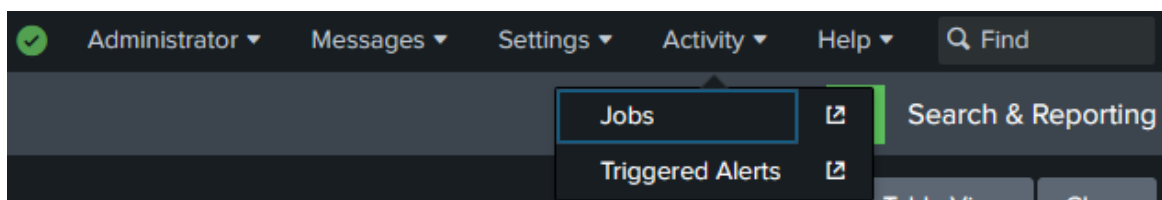
If you believe you've received this email in error, please see your Splunk administrator.

splunk > the engine for machine data

2 קבצים מצורפים • נסרקו על ידי Gmail



10. On the top right click on the activity option



11. Click on the triggered alerts to see if the alert was triggered

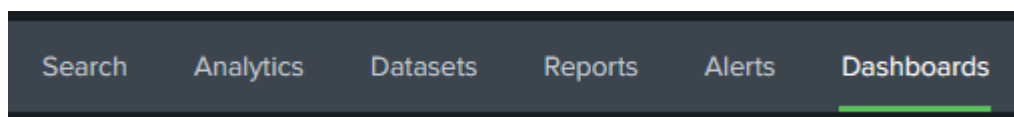
Triggered Alerts						
Showing 1 - 1 of 1 results						
Filter	Apps	Search & Reporting (search)	Owner	All Owners	Severity	All Severity
Alert	All Alerts					
<input type="checkbox"/>	Time	Fired Alerts	App	Type	Severity	Mode
<input type="checkbox"/>	2024-01-14 11:40:33 UTC	MySQL Warnings	search	Real-time	Medium	Per Result
View Results Edit Search Delete						

12. You can click on view results for more detail about the event

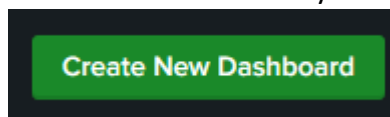
The screenshot shows the 'New Search' interface in Splunk. The search bar contains 'index=python_data warning'. Below the search bar, it indicates '1 event (1/1/70 12:00:00.000 AM to 1/14/24 11:40:33.069 AM)'. The 'Events' tab is selected, showing a table with columns 'Time' and 'Event'. The event details are as follows:

Time	Event
12/2/23 5:29:58.846 PM	2023-12-02T17:29:58.846495Z @ [Warning] [MY-010068] [Server] CA certificate ca.pem is self signed. host = _gateway source = tcp:8080 sourcetype = mysql_error

13. For a more real-time experience we will set an auto-refresh dashboard. From the search & reporting app click on dashboards.



14. Add a new dashboard by clicking the create new dashboard button.

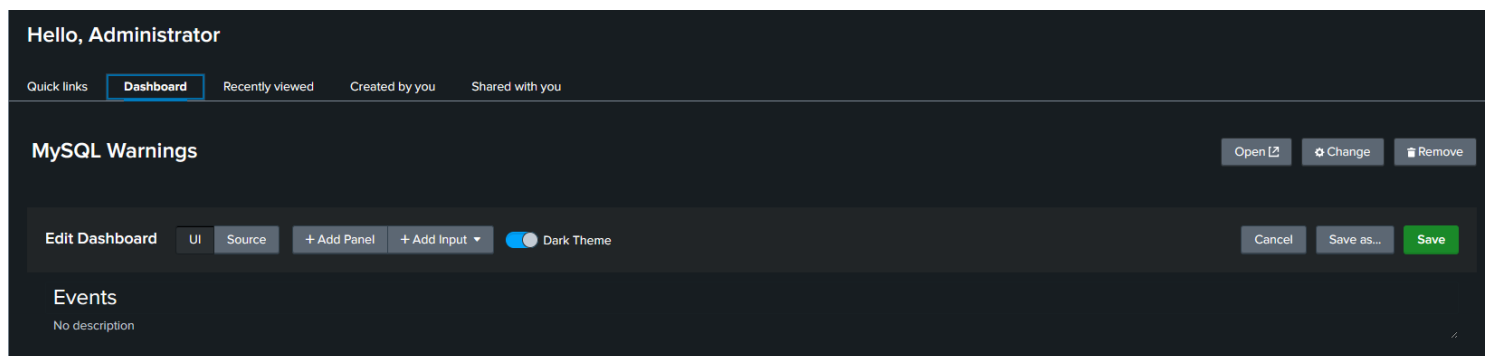
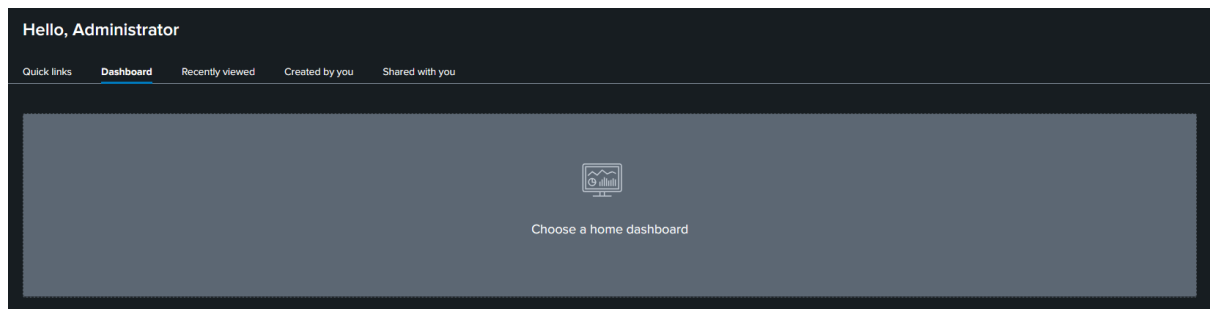


15. Enter a title and press the classic dashboard

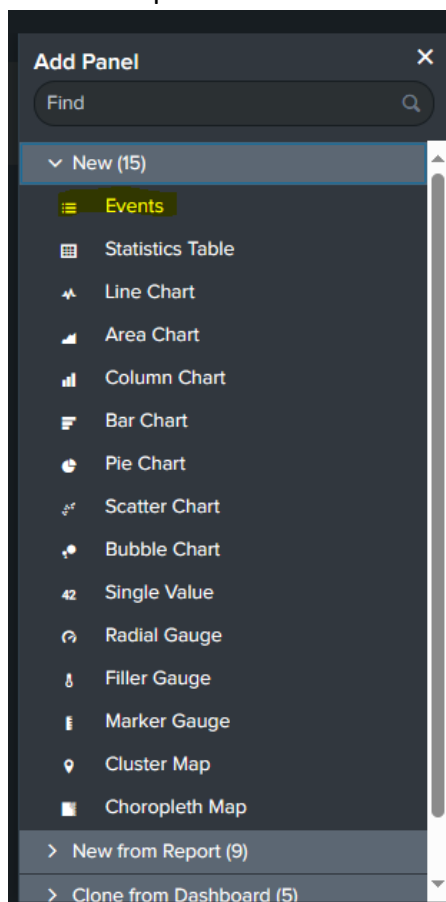
The screenshot shows the 'Create New Dashboard' dialog box. It contains the following fields and options:

- Dashboard Title:** A text input field containing 'MySQL Warnings'. Below it, the ID 'mysql_warnings' is displayed with an 'Edit ID' link.
- Description:** A text input field containing 'Optional'.
- Permissions:** A dropdown menu set to 'Private'.
- How do you want to build your dashboard?:** Two options are presented: 'Classic Dashboards' (The traditional Splunk dashboard builder) and 'Dashboard Studio' (A new builder to create visually-rich, customizable dashboards, marked as 'NEW').
- Buttons:** 'Cancel' and 'Create' buttons at the bottom right.

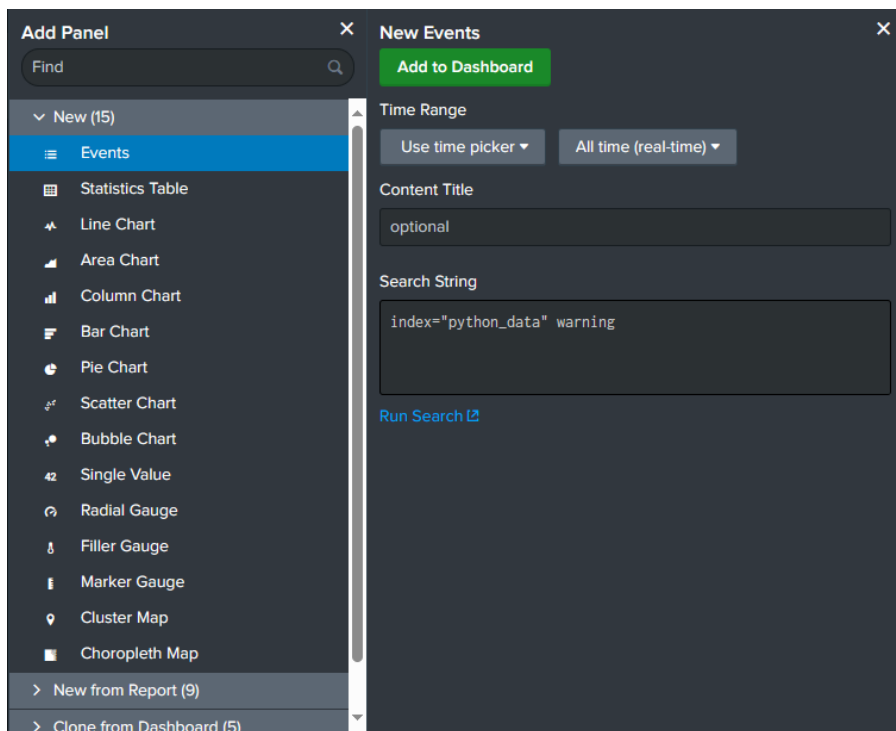
16. After the dashboard is created you can access it from the main page by clicking on the dashboard option. Add your custom new dashboard.



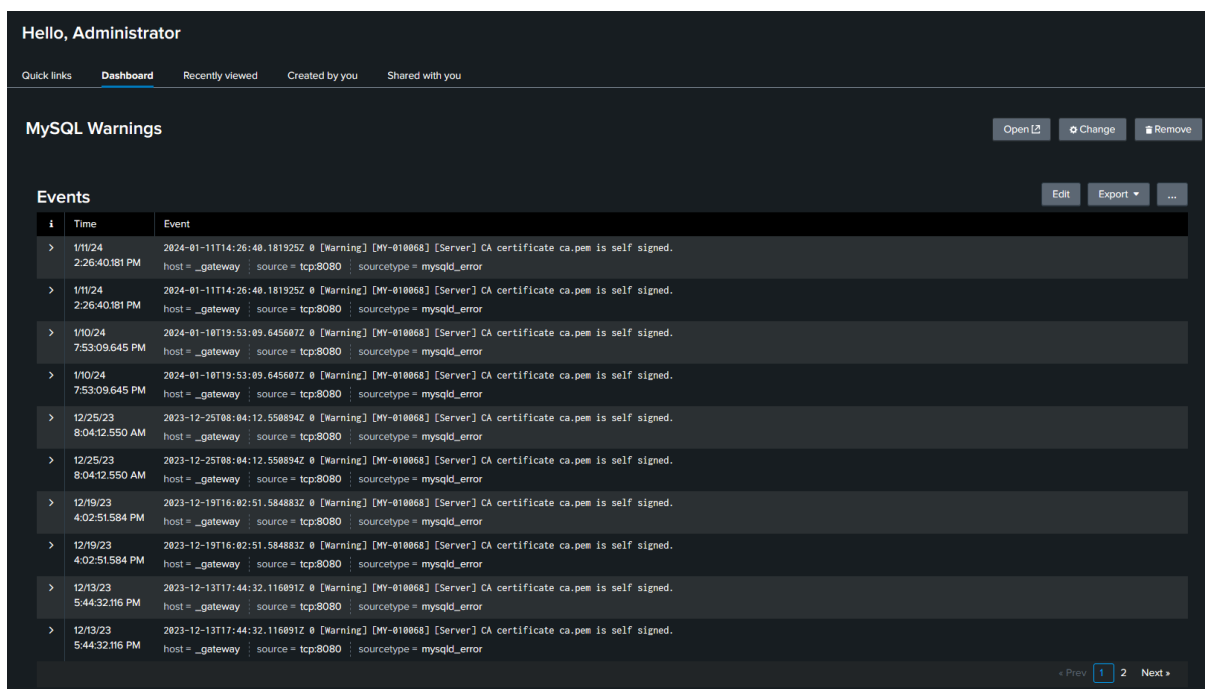
17. Add a new panel to the dashboard. Click on Events



18. Enter your search query and select all time(Real-time) in time range



Finally, the dashboard will look like this. When python sends new events (logs) with the word “warning” in them, the dashboard will automatically refresh.



Let's set up an alert for error events.

1. Go to the search app and follow the steps from the previous alert setup. My query is: `index="python_data" error`
2. Real time alerts are always running in the background. We want to know if there are more than 5 errors in the last hour. We want to avoid utilizing the machine memory unless absolutely necessary, so we can set this alert to run every hour. Set the trigger to greater than 5. Add the two actions from the last alert.

Save As Alert

Settings

Title: MySQL Errors

Description: Optional

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every hour ▼

At: 0 ▼ minutes past the hour

Expires: 24 | hour(s) ▼

Trigger Conditions

Trigger alert when: Number of Results ▼

is greater than ▼ 5

Trigger: Once | For each result

Throttle ? ☐

Trigger Actions

+ Add Actions ▼

When triggered:

- > Send email Remove
- > Add to Triggered Alerts Remove

Cancel Save

MySQL Errors

Enabled: Yes. [Disable](#)

App: search

Permissions: Private. Owned by admin. [Edit](#)

Modified: Jan 14, 2024 2:05:33 PM

Alert Type: Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: .. Number of Results is > 5. [Edit](#)

Actions: 2 Actions [Edit](#)

- ▲ Add to Triggered Alerts
- ✉ Send email

The process will run every hour and if there are more than 5 error it will record on the triggered alert page and we will get an email as shown in the previous alert setup.

Resources:

[Create real-time alerts - Splunk Documentation](#)

[Email notification action - Splunk Documentation](#)

[Create detectors to trigger alerts — Splunk Observability Cloud documentation](#)