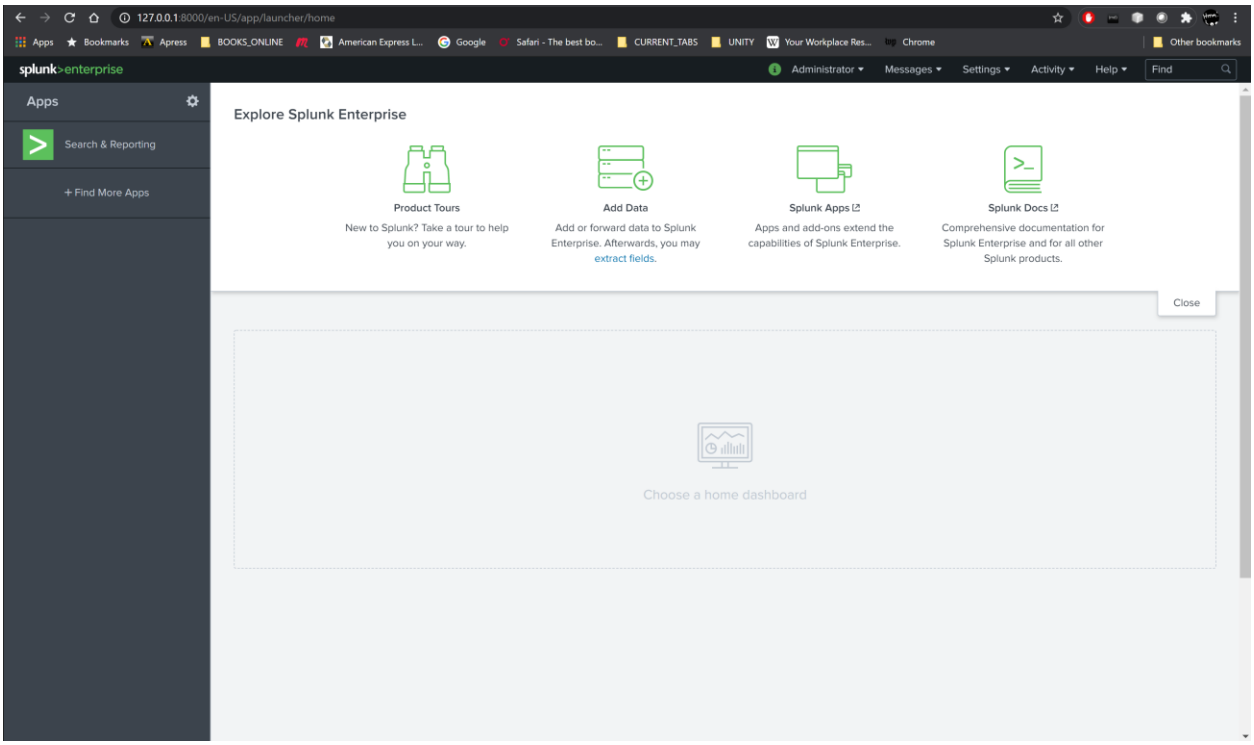
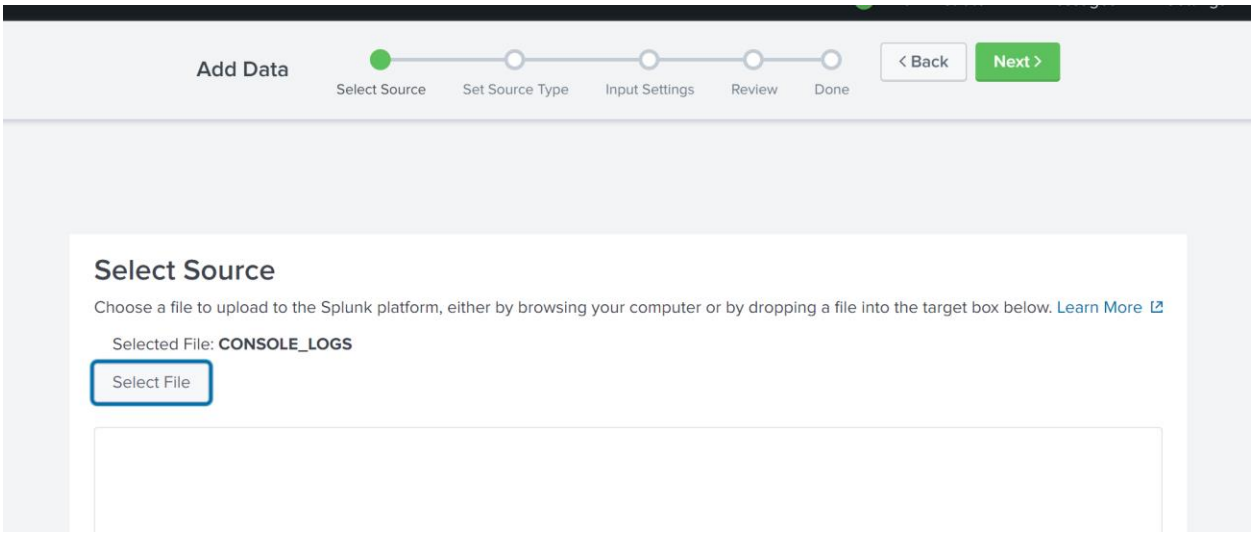
# Splunk

## Using Splunk

- Installed Splunk
- Working in browser on local machine:

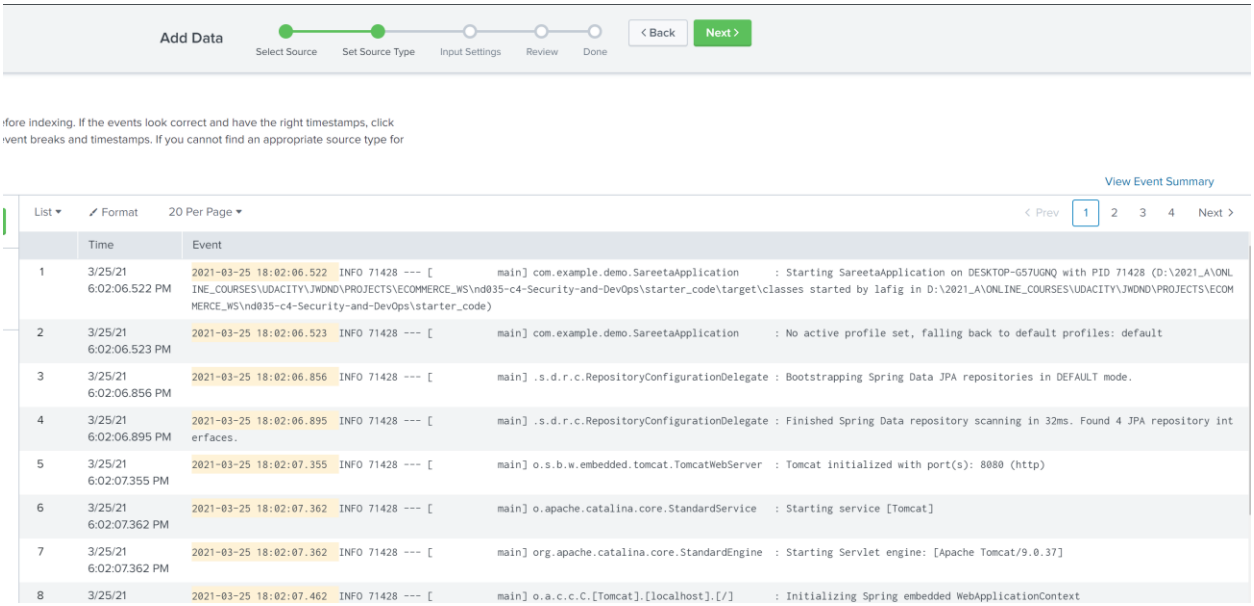



- Uploaded CONSOLE_LOGS

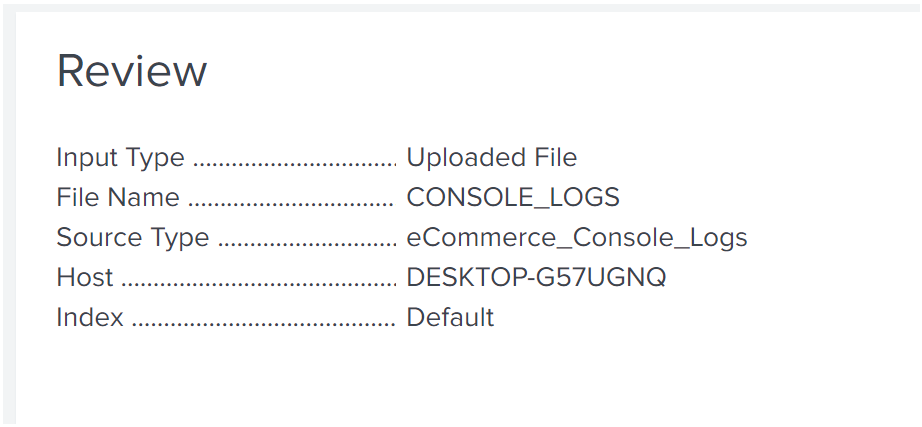


Splunk

Adding my CONSOLE_LOGS



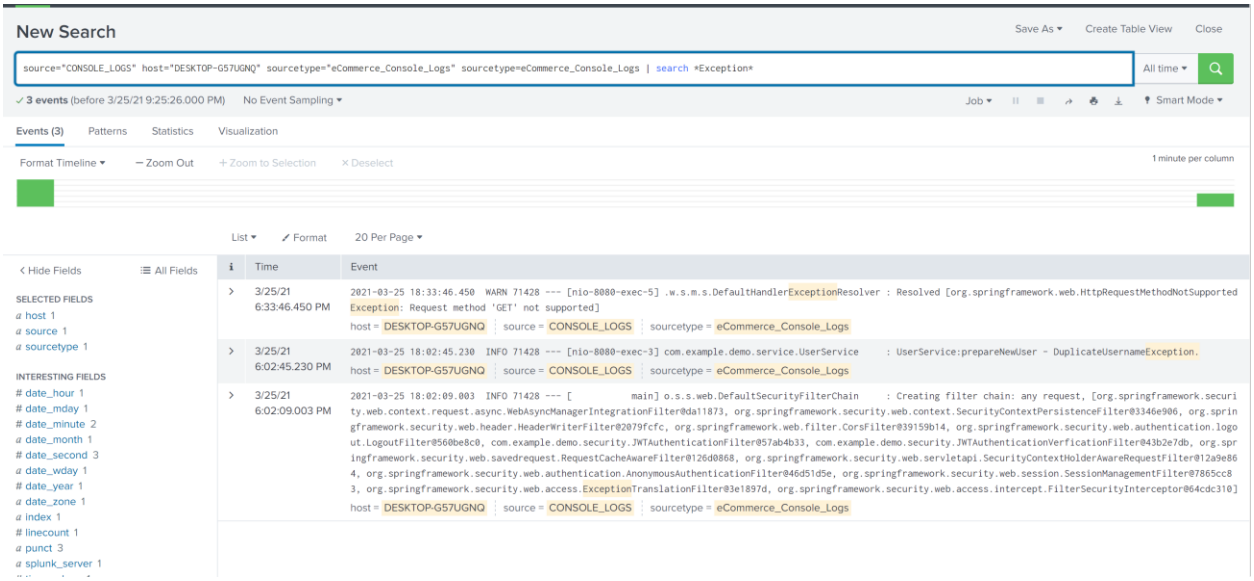

- Review of file:



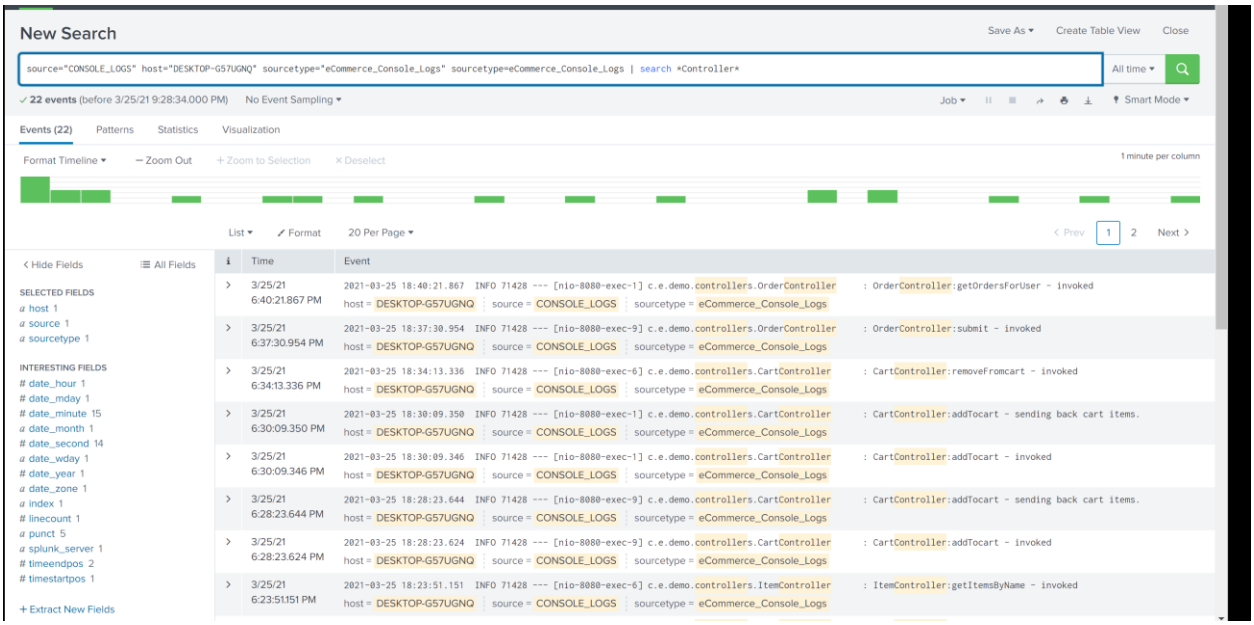

## Indexing and Searching

Searching for all lines with *Exception*

Splunk

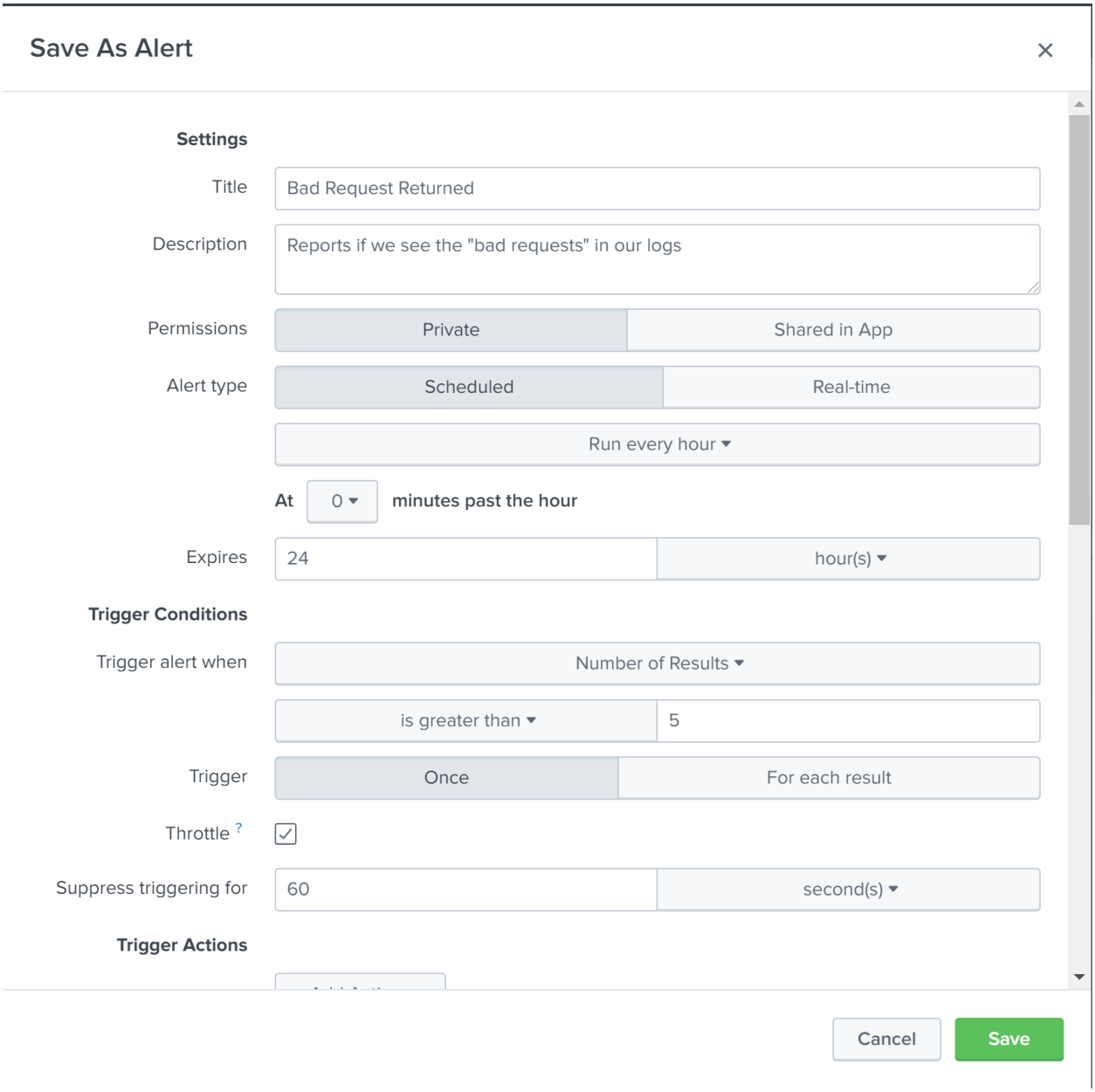


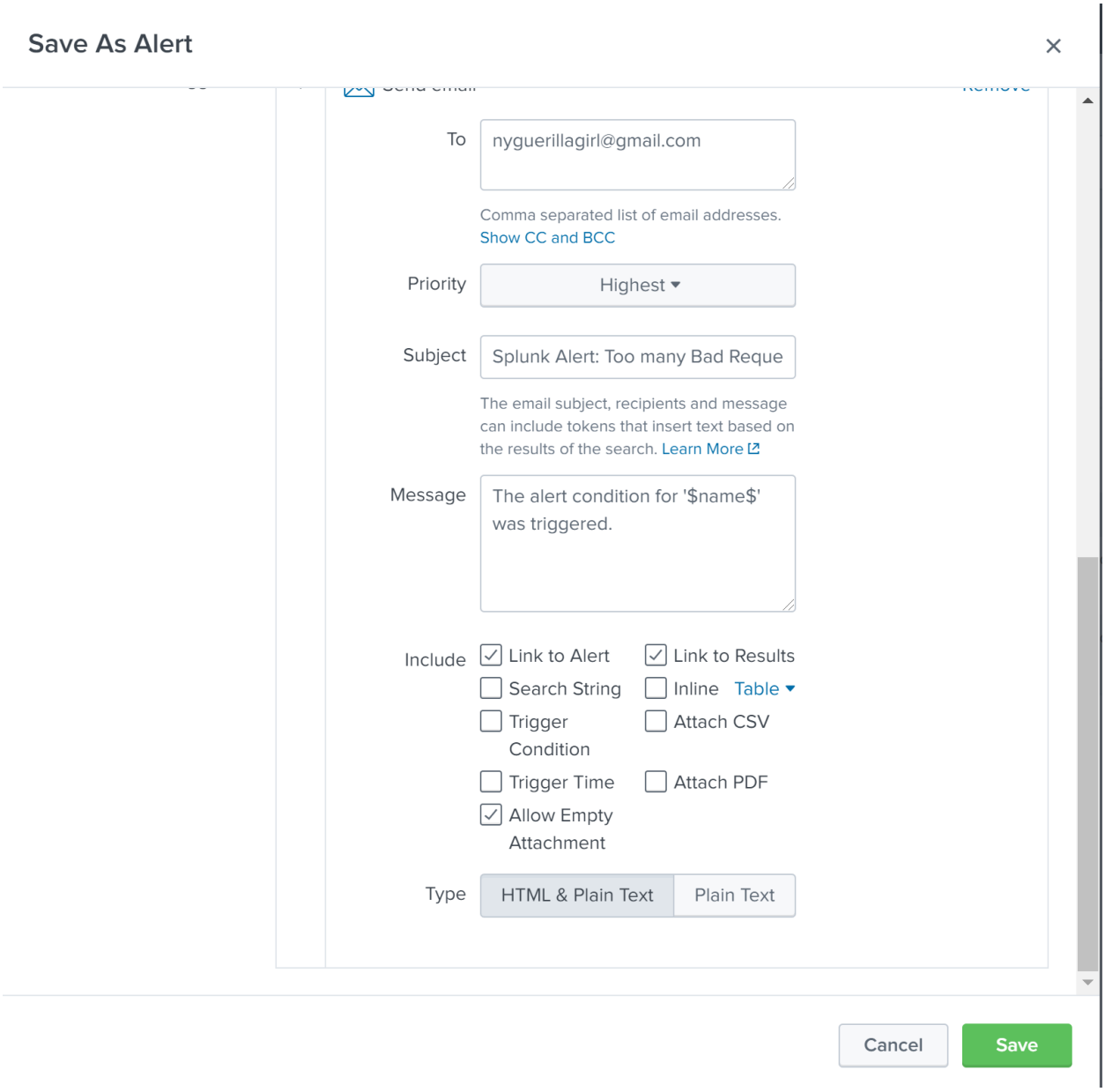

- All logging activities from Controllers:

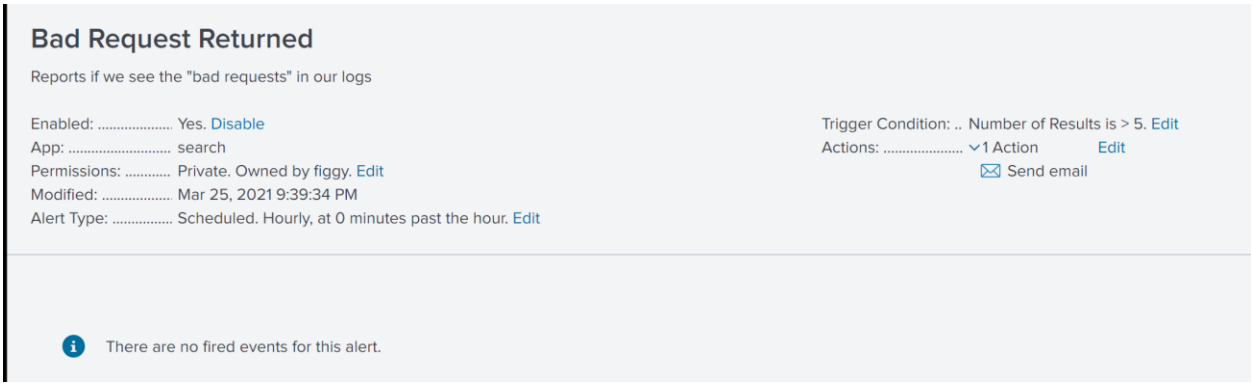



# Alerts

- The plan is to set up an alert if we see “bad request returned” in the logs


Save As Alert
Settings
Title
Bad Request Returned
Description
Reports if we see the "bad requests" in our logs
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
Suppress triggering for
60
second(s)
Trigger Actions
Cancel
Save


Save As Alert
To
nyguerillagirl@gmail.com
Comma separated list of email addresses.
Show CC and BCC
Priority
Highest
Subject
Splunk Alert: Too many Bad Reque
The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More
Message
The alert condition for '$name$' was triggered.
Include
Link to Alert
Link to Results
Search String
Inline
Table
Trigger Condition
Attach CSV
Trigger Time
Attach PDF
Allow Empty Attachment
Type
HTML & Plain Text
Plain Text
Cancel
Save


Bad Request Returned
Reports if we see the "bad requests" in our logs
Enabled: Yes. Disable
App: search
Permissions: Private. Owned by figgy. Edit
Modified: Mar 25, 2021 9:39:34 PM
Alert Type: Scheduled. Hourly, at 0 minutes past the hour. Edit
Trigger Condition: Number of Results is > 5. Edit
Actions: 1 Action Edit
Send email
There are no fired events for this alert.