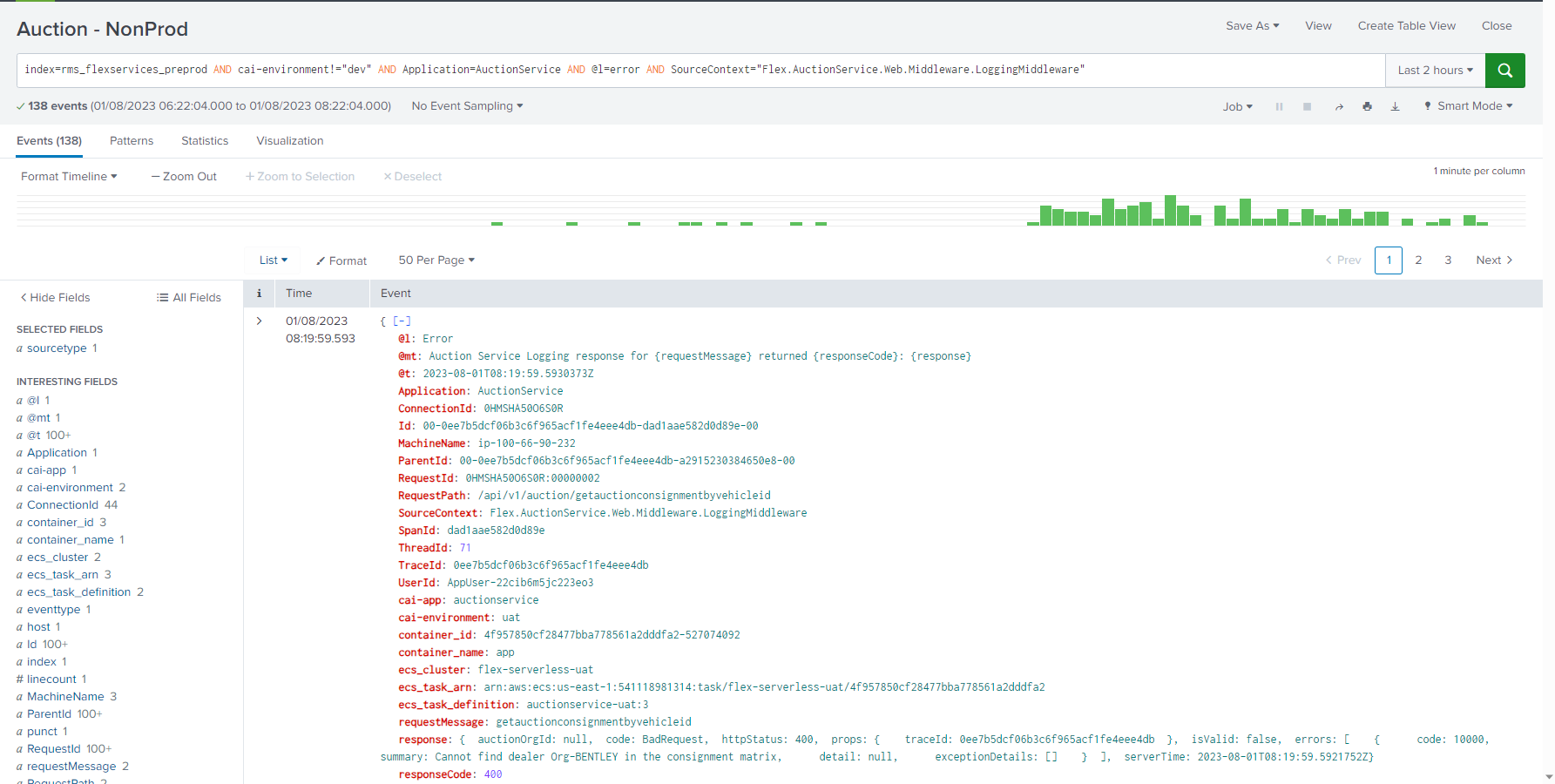
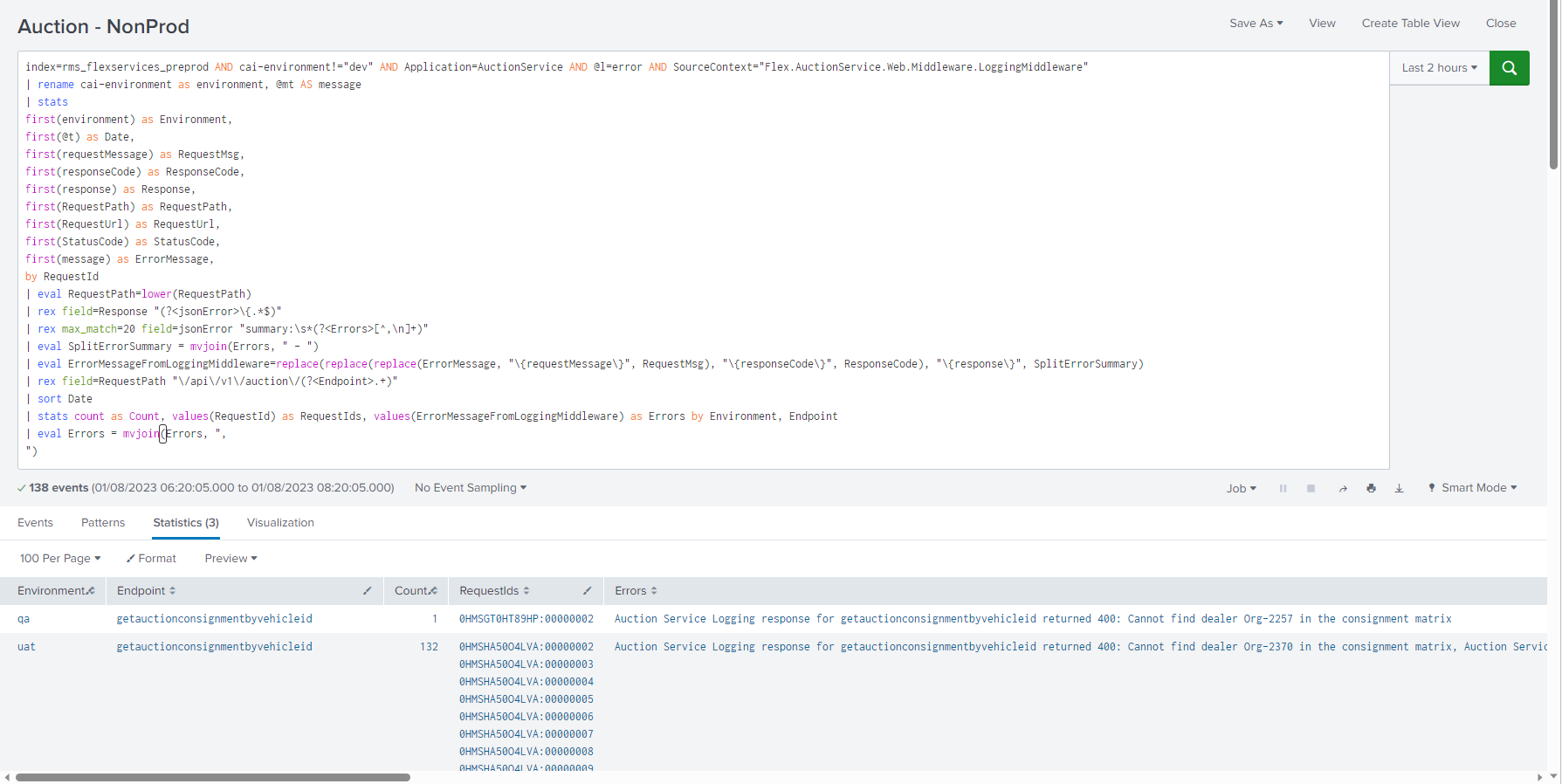
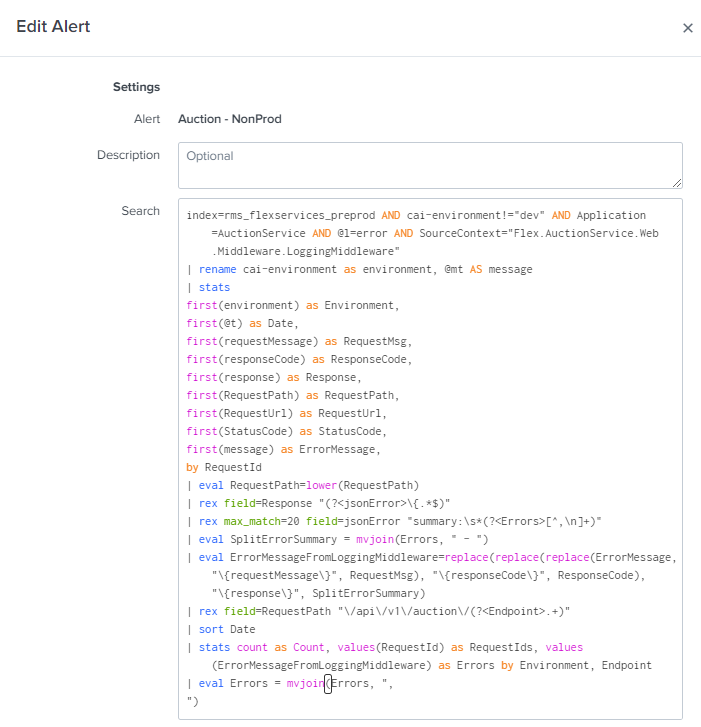
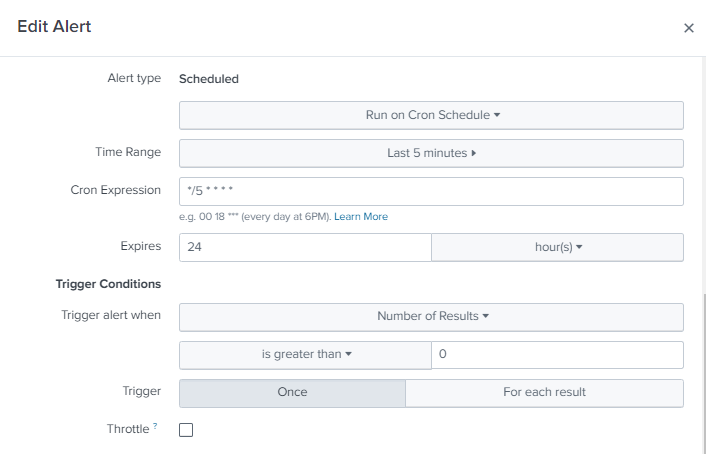
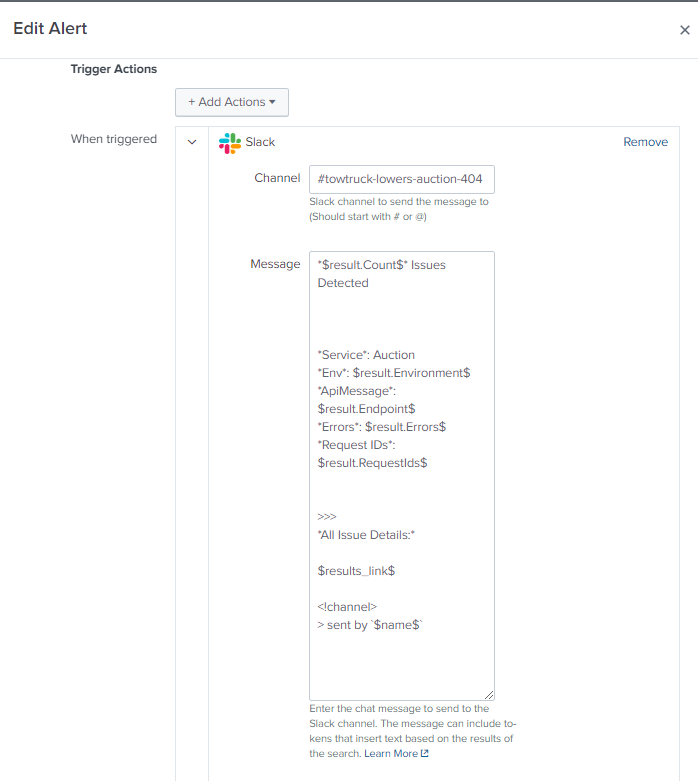
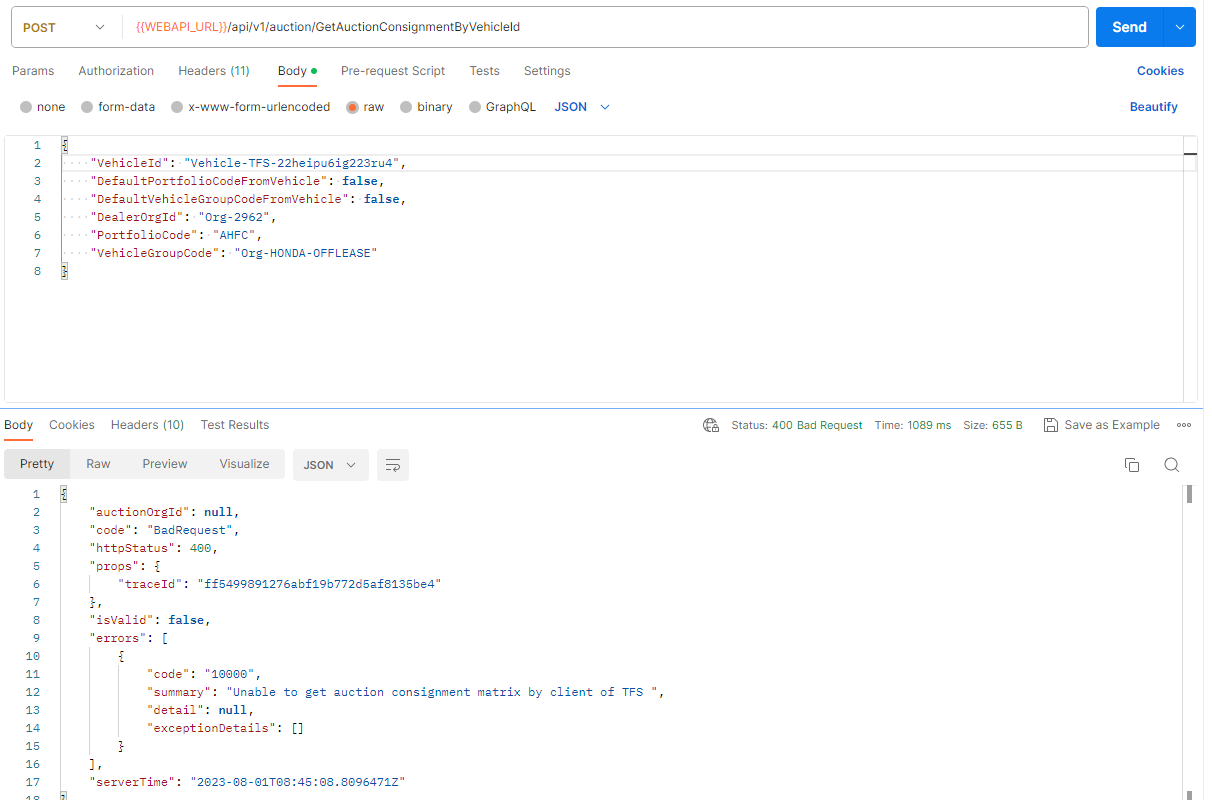
**How to setup a Splunk alert that send message to Slack channel**  
  
During service operation, log will be generated and sorted by Splunk, from these index we can query for all bad request for the specified time and other search criteria such as environment, request path etc..  
  
For example: Below query will give all bad request came to Auction service for the latest 2 hours from all lower environment.  
  
  
  
We can improve the visualization of search result by adding a little format, calculate the statistic of the result, this way, we will get more overall information about all bad request. It will be more clear to get just the brief summary of error, number of request encounters problem, and the RequestId to trace back the detailed error for single one as well.  


These statistic will be sent to Slack channel, increase the awareness of error for immediately acting.

All that need to be done is to save the query into an alert and configure the channel.  
  
  
Fill in the Alert name, no need to touch the Search section as it’s automatically copy from the previous query.  
  
  
Then, setup the alert type with additional information.  
Here the type is configured as Run on Cron schedule, using the TimeRange and Cron Expression, we can setup an alert that automatically query for all error within last 5 minutes, and do it every 5 minutes, If there’s any result it will trigger the action setup below. And of course these number can be changed correspond to creator’s desire. But with an alert, searching for every 5 mins and trigger if number of result is greater than 0 is fine.  
  
We can have the trigger as “once”, the alert will send all result in a message, instead of “For each result” which potentially can send a large amount of message to Slack channel in case there’s so much error.  
  
  
The last section to be configured is the action when the condition of result found met. We got multiple action here, it can be sending message to PagerDuty, Email etc…In this case we will use Slack channel as the message destination  
Setup the Slack channel name in the Channel section.  
Along with that, we can format the outgoing message like below. All these figures is get from the result of the query  


With all that setup, we can have an alert system, when there’s any error occurs (here’s an manually tested error)  
  
  
And we will have a message come to out Slack channel, with the format comply with the pre-defined Message section: Service, Env, ApiMessage and a RequestId to findout the detailed information.  
