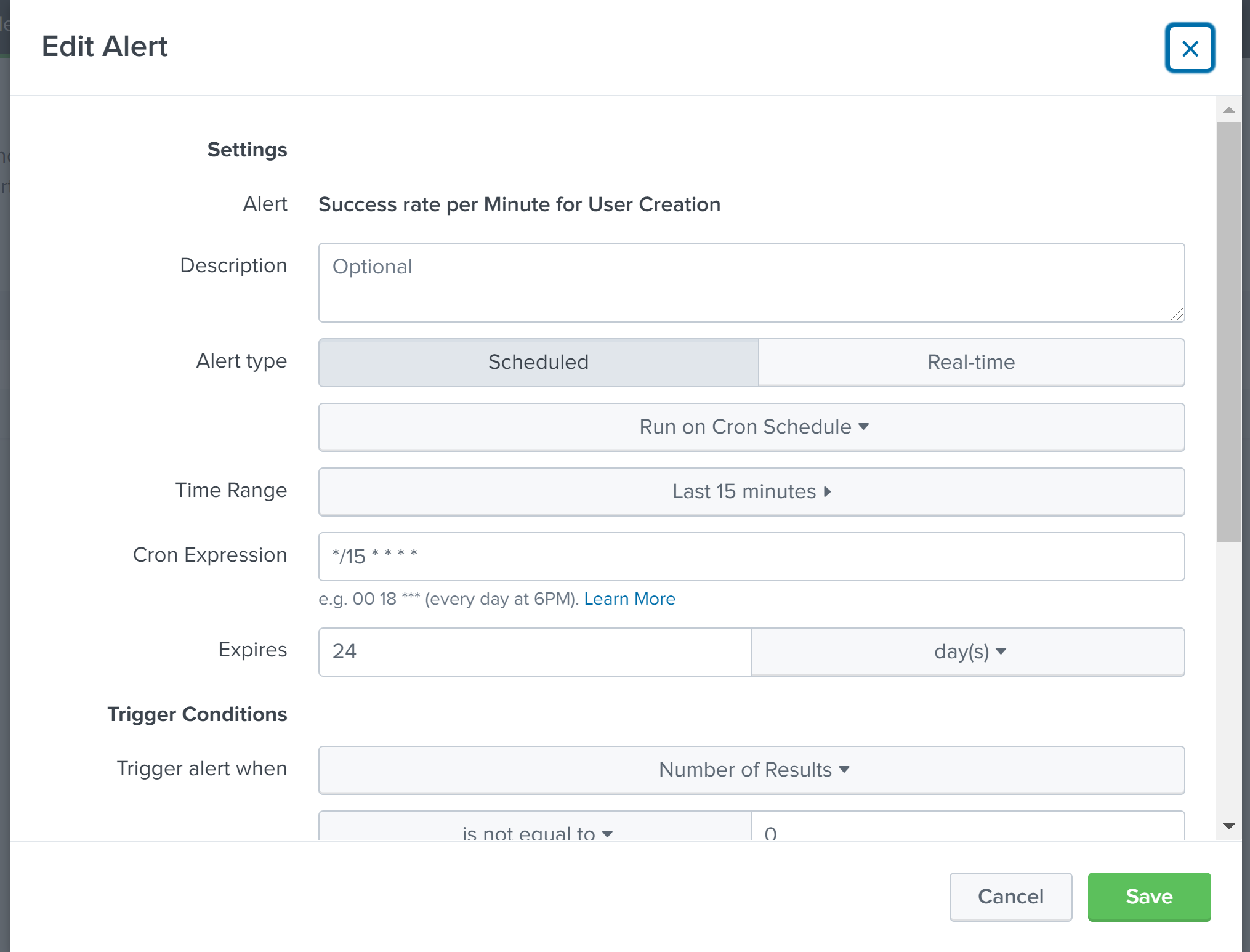
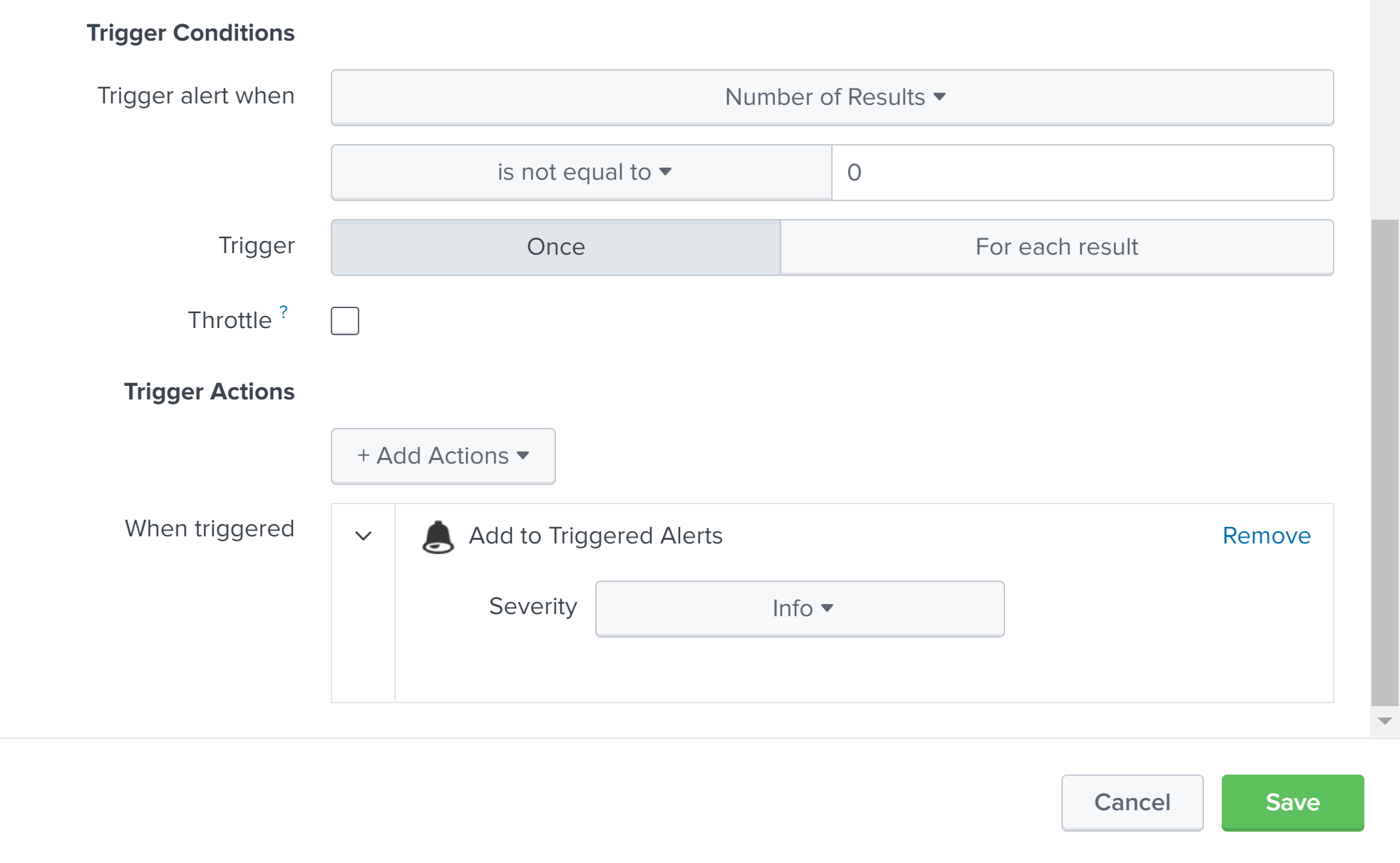
Integrated Splunk with Spring Boot application by directly sending logging information in JSON format to Splunk, to enable fast and efficient searches.

Configured two alerts:

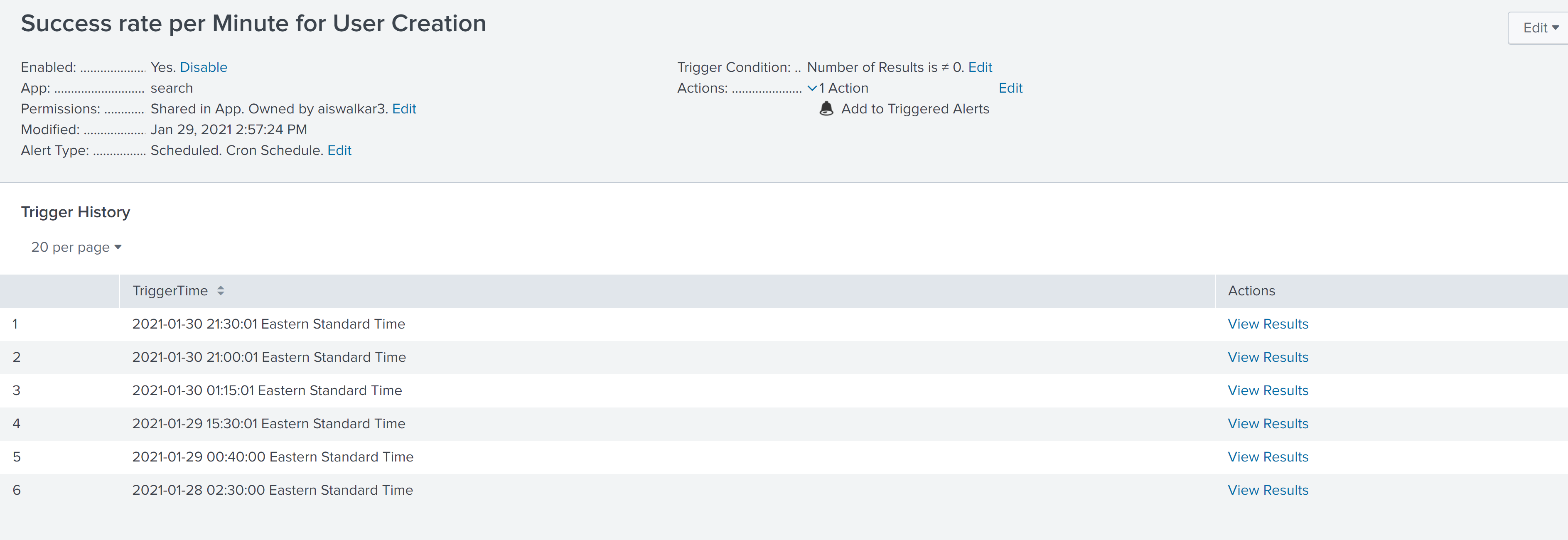
1. User creation: In User Creation, we get the success rate per minute for every 15 minutes. The alert is scheduled for every 15 minutes if we have valid user creation events. The search query is as below.

index="user\_creation" earliest=-15m@m latest= @m | spath responseCode | search responseCode != 0 | timechart span=1m count(eval(match(responseCode,"20\*"))) as count\_success count(eval(match(responseCode,"40\*") or match(responseCode,"50\*"))) as count\_failure | where count\_success > 0 or count\_failure > 0 | eval time = strftime(\_time,"%H:%M:00") | stats sum(count\_success) as count\_success sum(count\_failure) as count\_failure by time | eval success\_percent = round((count\_success/(count\_success+count\_failure))\*100,2)





Triggered alerts are as below.

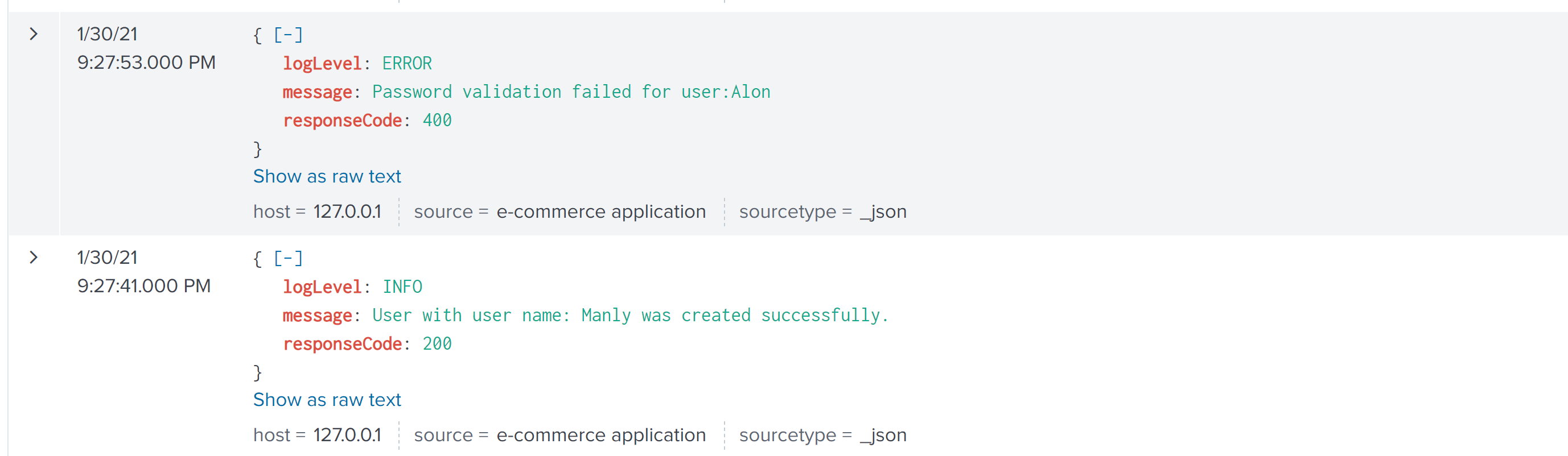


Below is the search query and the results of the latest alert.



Below are the logs for the two results above.





1. Order creation: In Order Creation, we get the success rate per minute for every 15 minutes. The alert is scheduled for every 15 minutes if we have valid order creation events. The search query is as below.

index="order\_creation" earliest=-15m@m latest= @m | spath responseCode | search responseCode != 0 | timechart span=1m count(eval(match(responseCode,"20\*"))) as count\_success count(eval(match(responseCode,"40\*") or match(responseCode,"50\*"))) as count\_failure | where count\_success > 0 or count\_failure > 0 | eval time=strftime(\_time,"%H:%M:00") | stats sum(count\_success) as count\_success sum(count\_failure) as count\_failure by time | eval success\_percent = round((count\_success/(count\_success+count\_failure))\*100,2)

