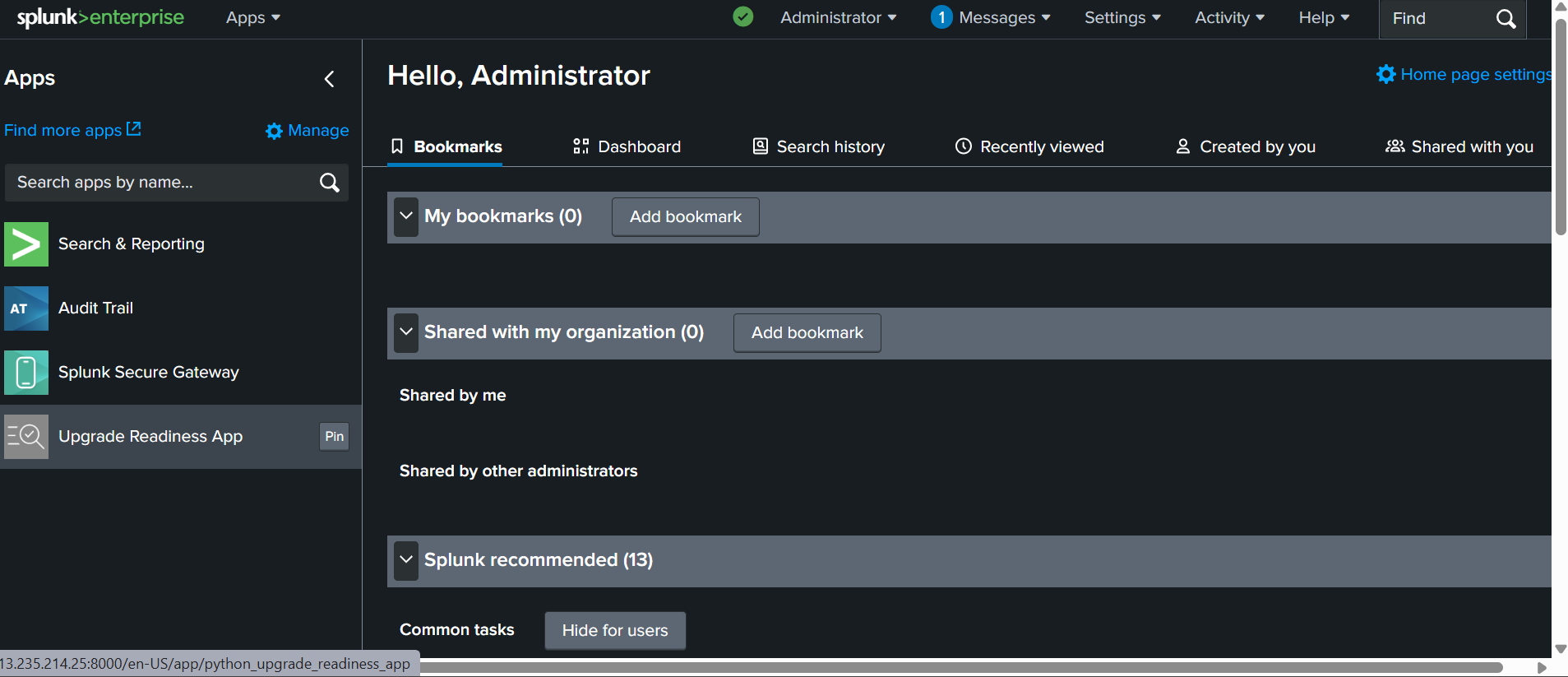
\*\*After installing splunk in aws ec2 instance then run the following command

sudo /opt/splunk/bin/splunk restart

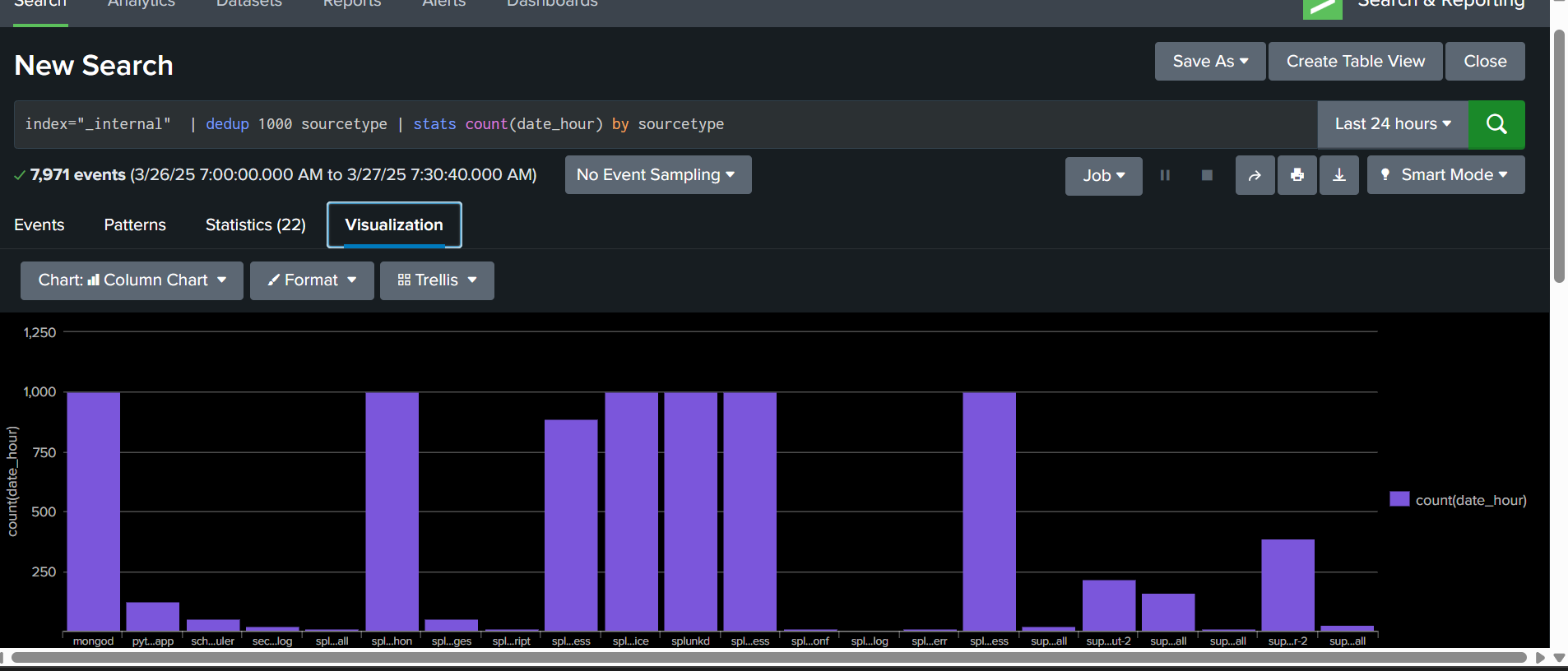
\*\* Then after log on to browser http://<ip\_add>:8000

Click on searching & reporting option

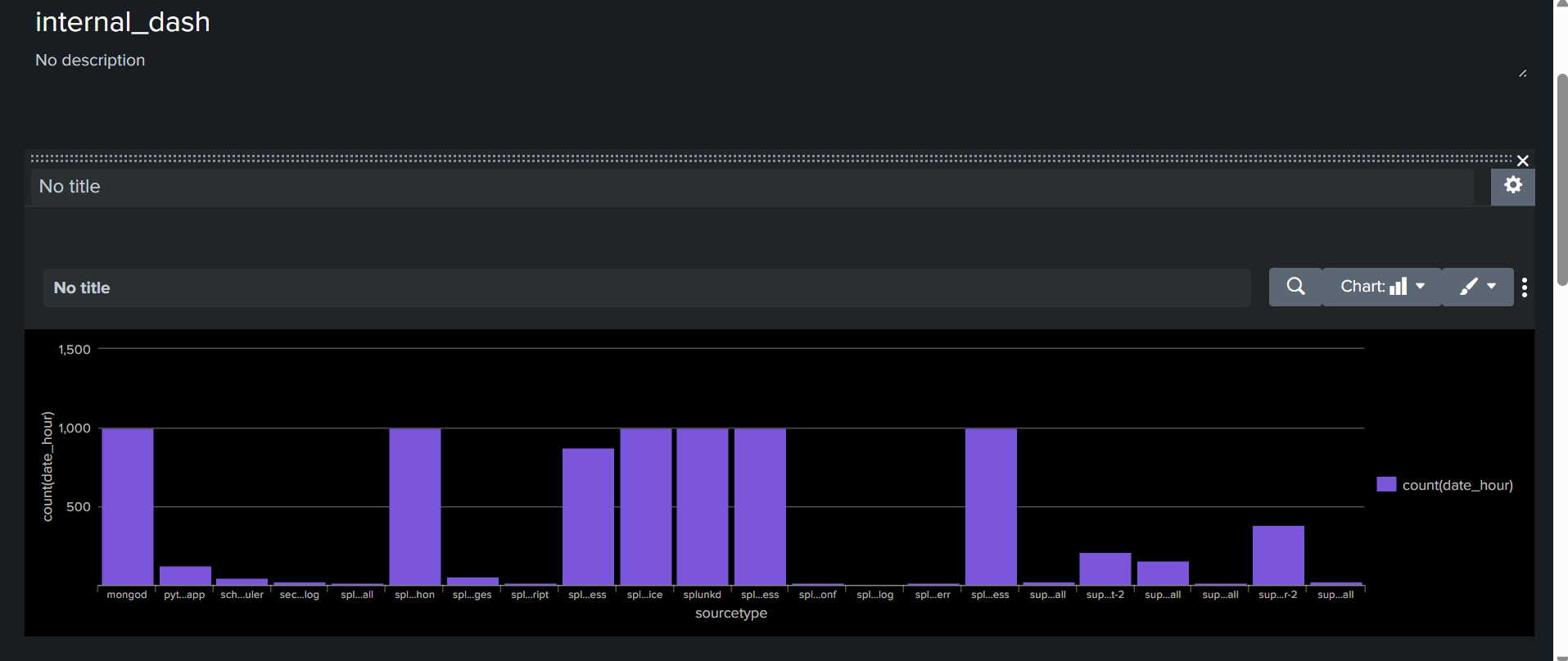


Run the following command in the search bar to create a dashboard .

Command🡪 index="\_internal" | dedup 1000 sourcetype | stats count(date\_hour) by sourcetype

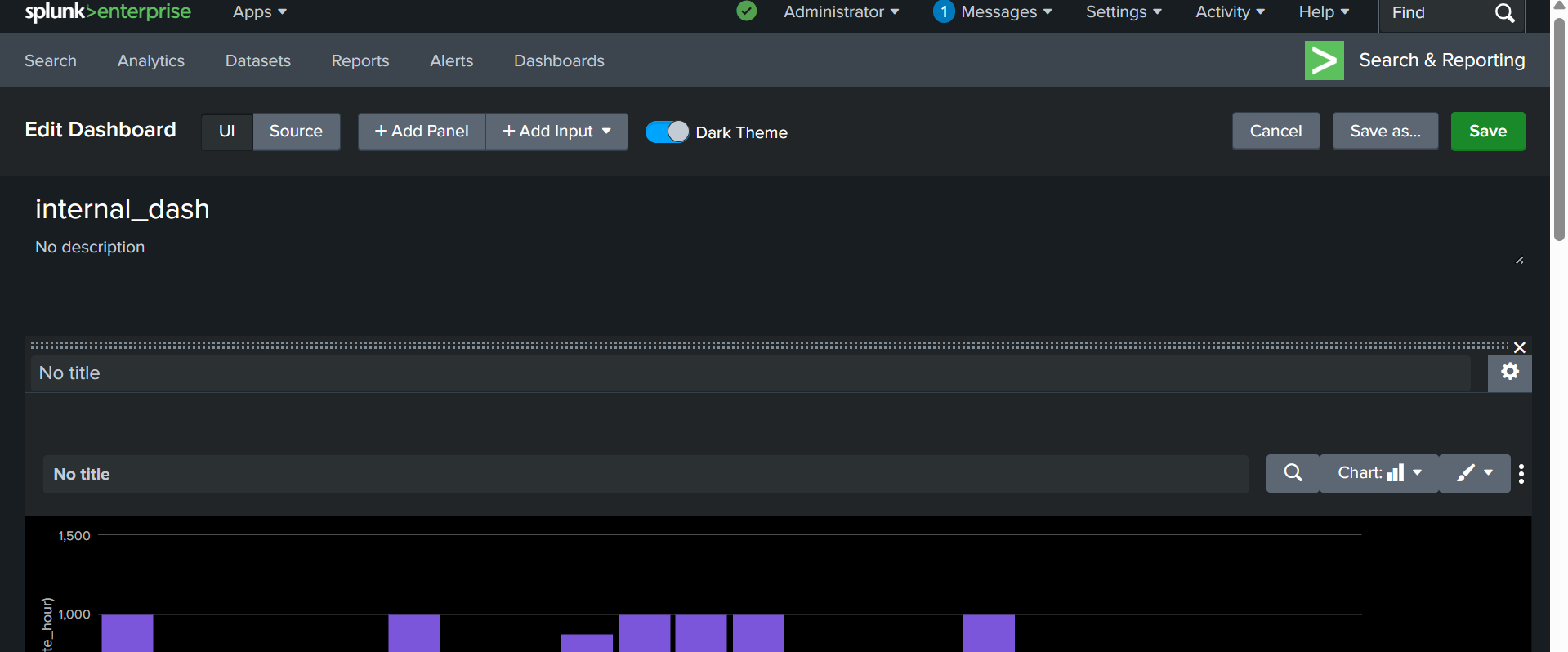


Click on visualization ,Save AS option then after click new dashboard---give name, click classic dashboard then save to dashboard



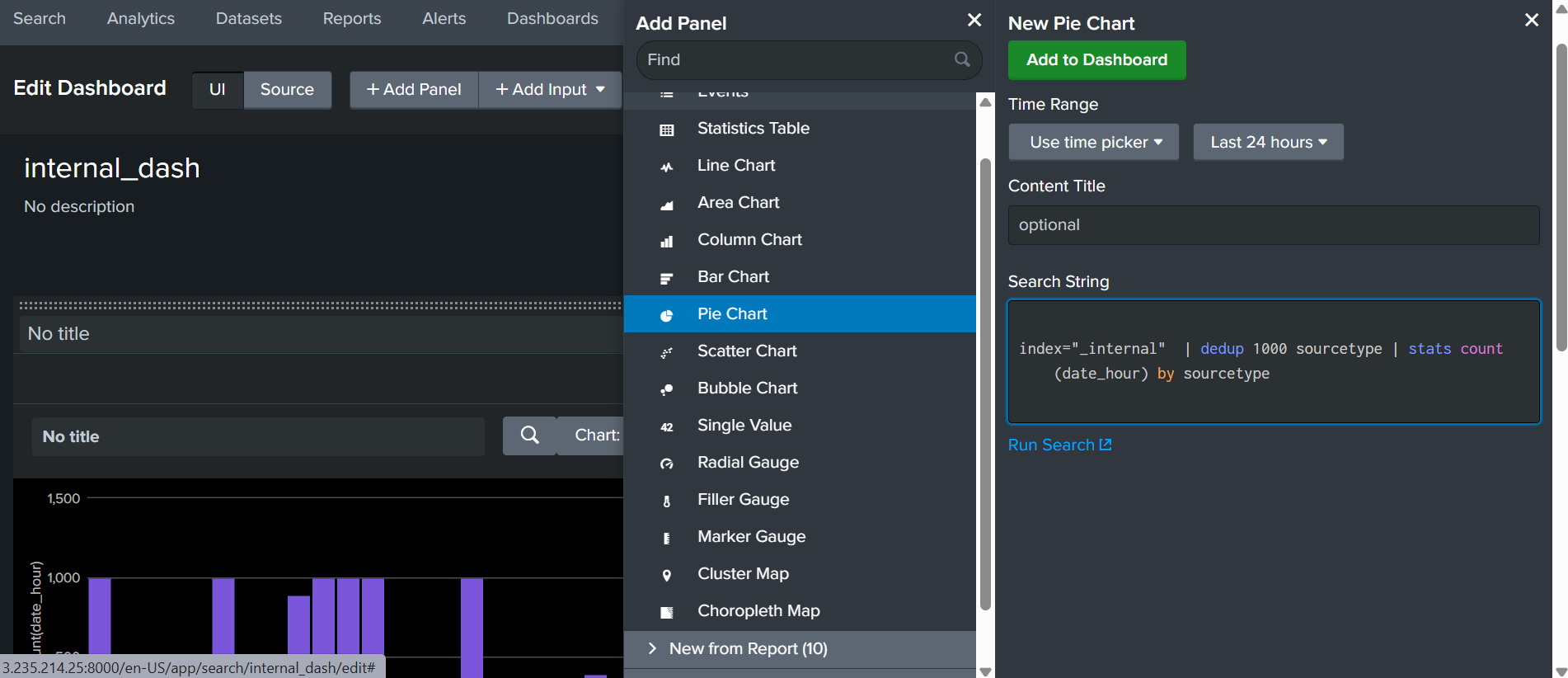
We can add the more panels in the dashboard

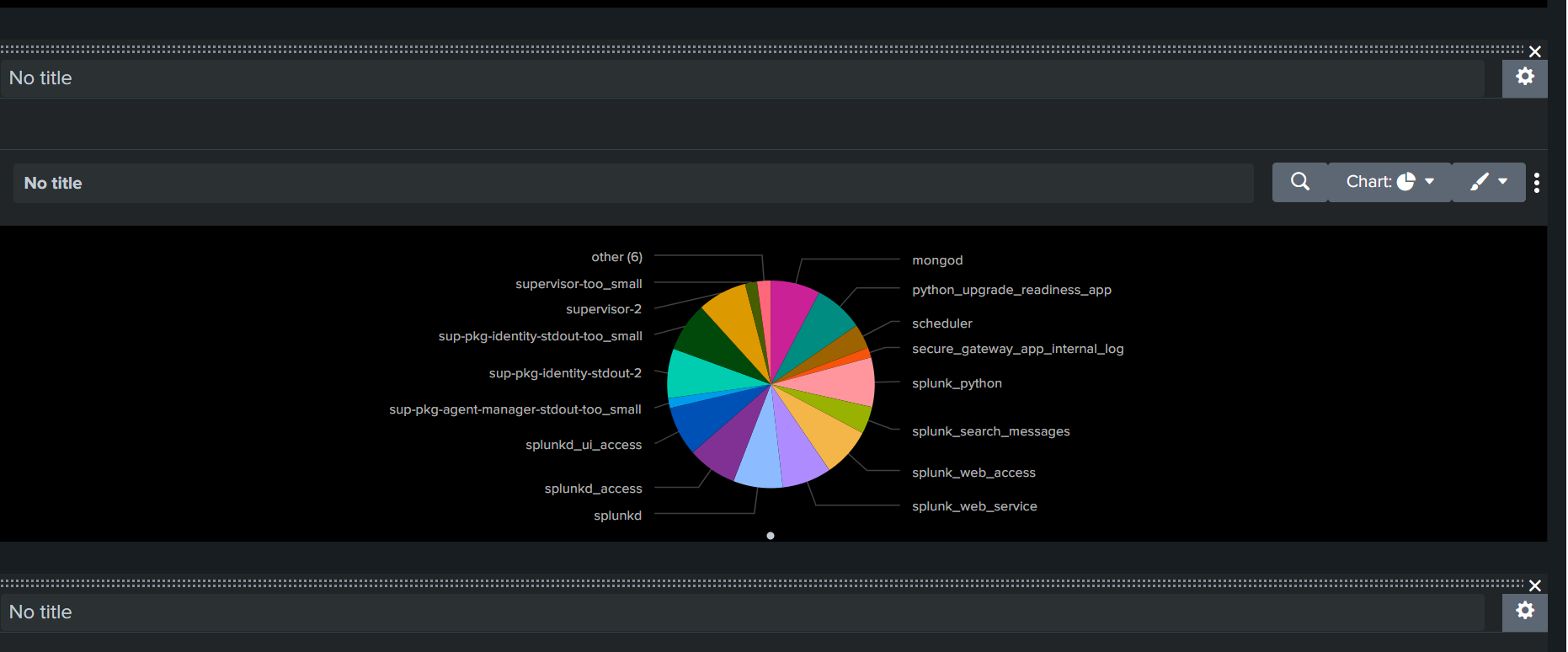
Click🡪 add panel option



Click🡪 new 🡪 select chart🡪 search string run the following command 🡪add to dashboard

Command🡪 index="\_internal" | dedup 1000 sourcetype | stats count(date\_hour) by sourcetype

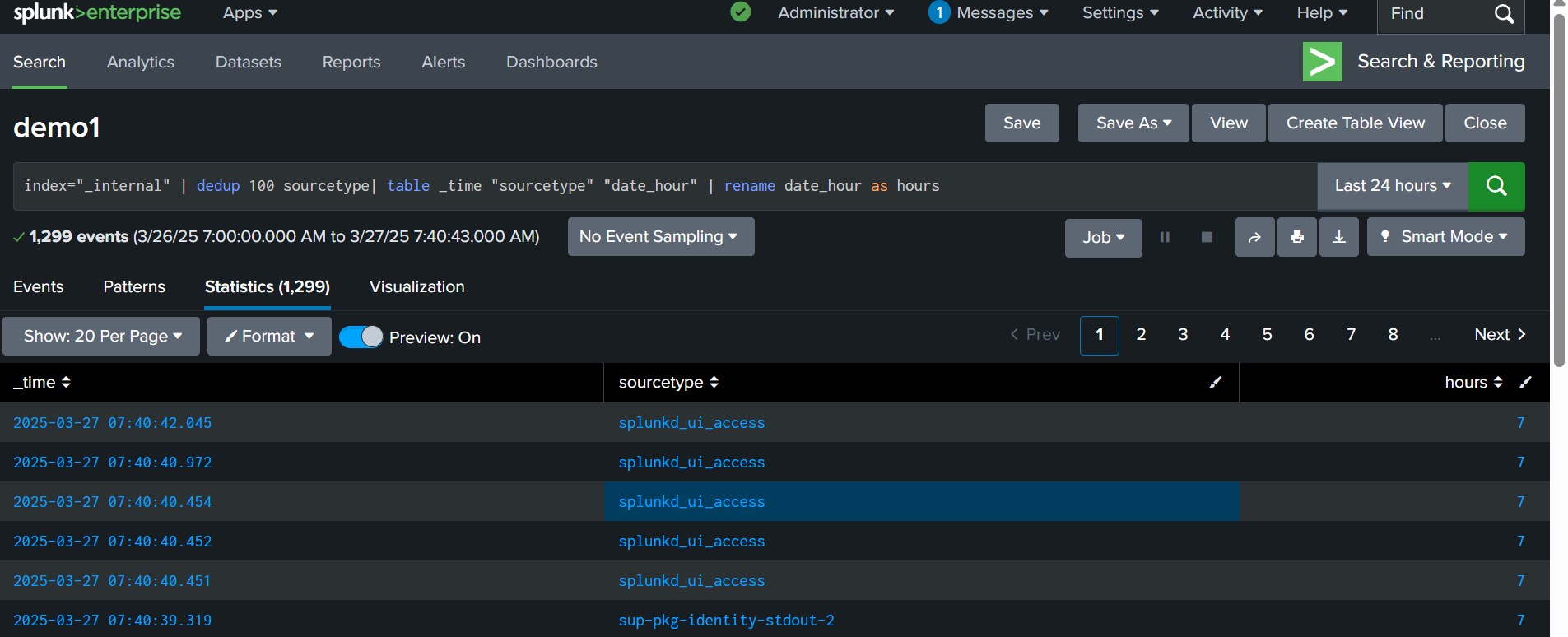




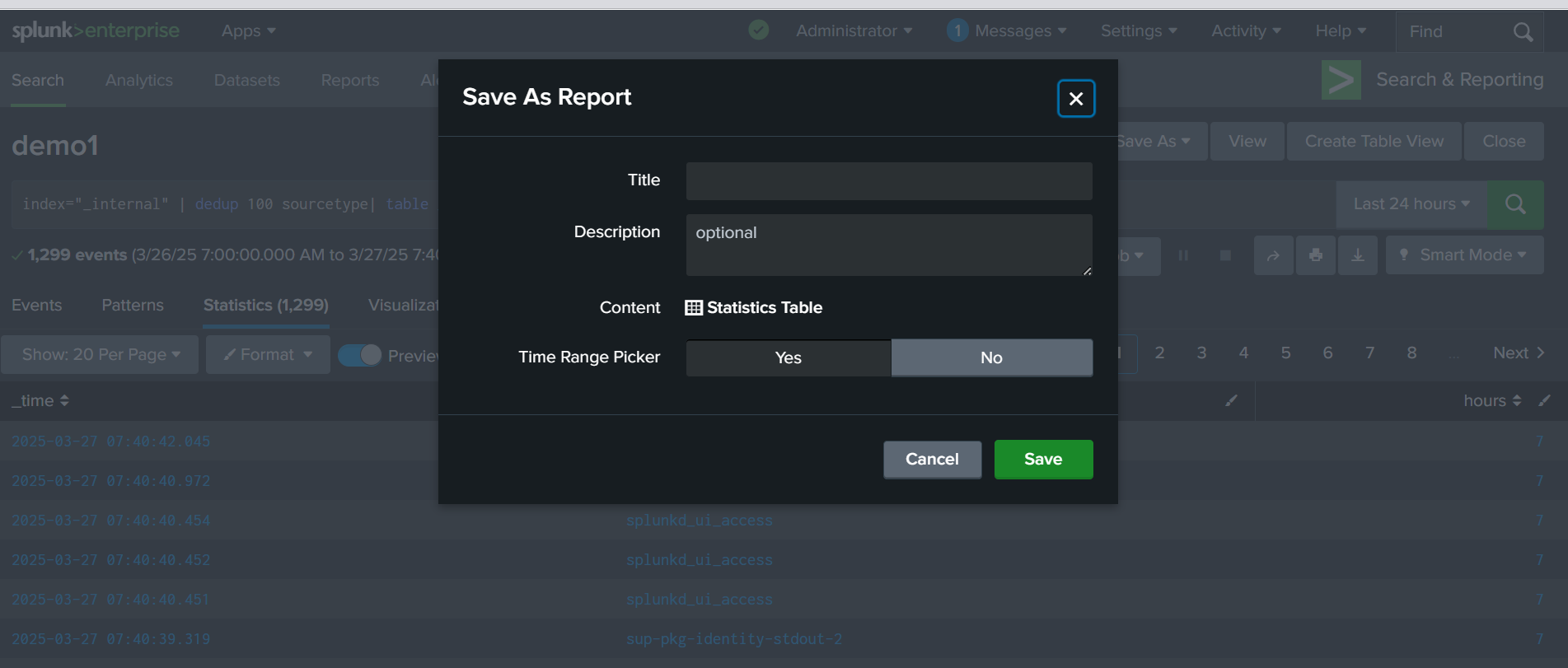
We can create reports and add to dashboard

Click🡪searching & reporting 🡪search bar run the following command

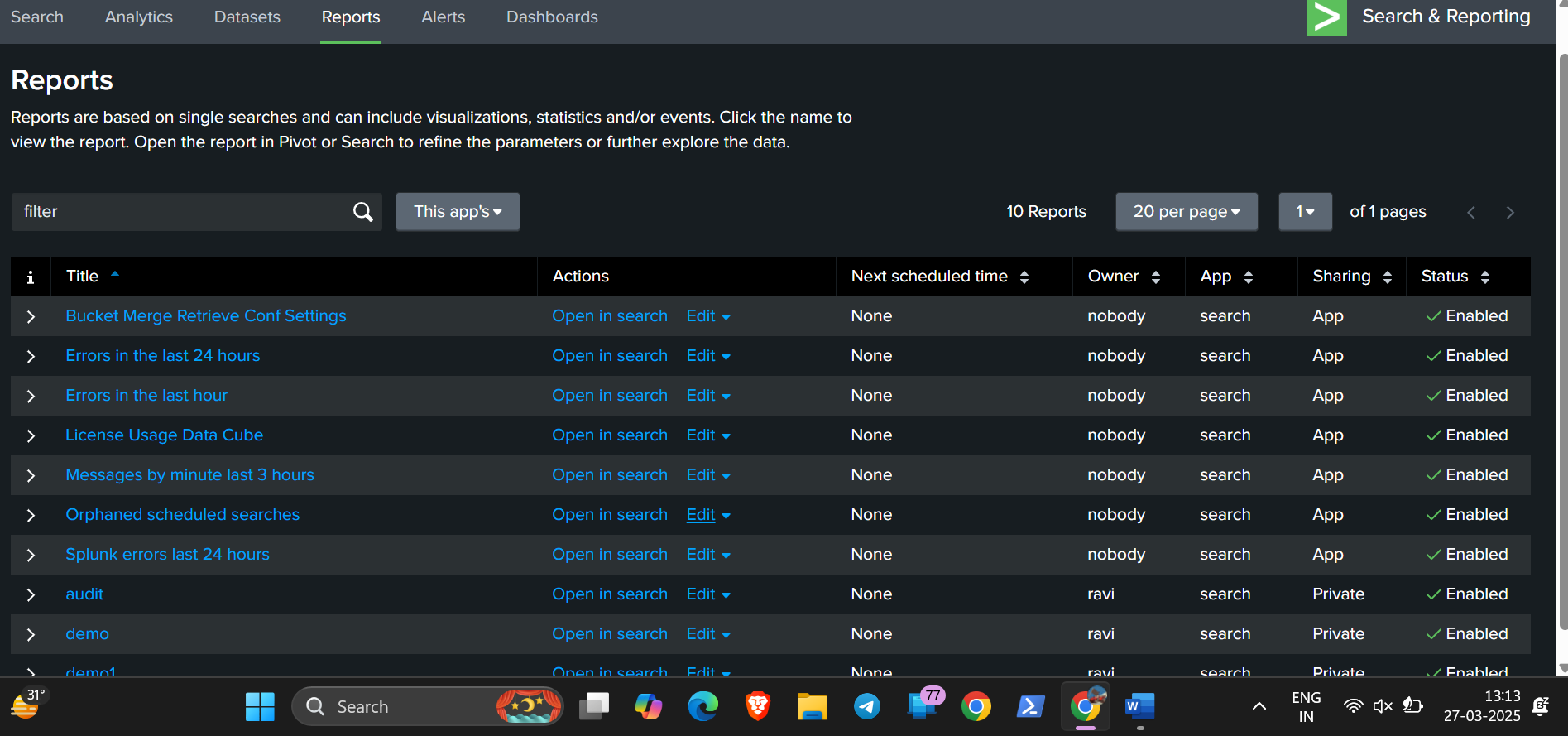
Command🡪 index="\_internal" | dedup 1000 sourcetype | table \_time "sourcetype" "date\_hour"| rename date\_hour as hours



Click 🡪save AS 🡪report🡪 fill the details—name click save

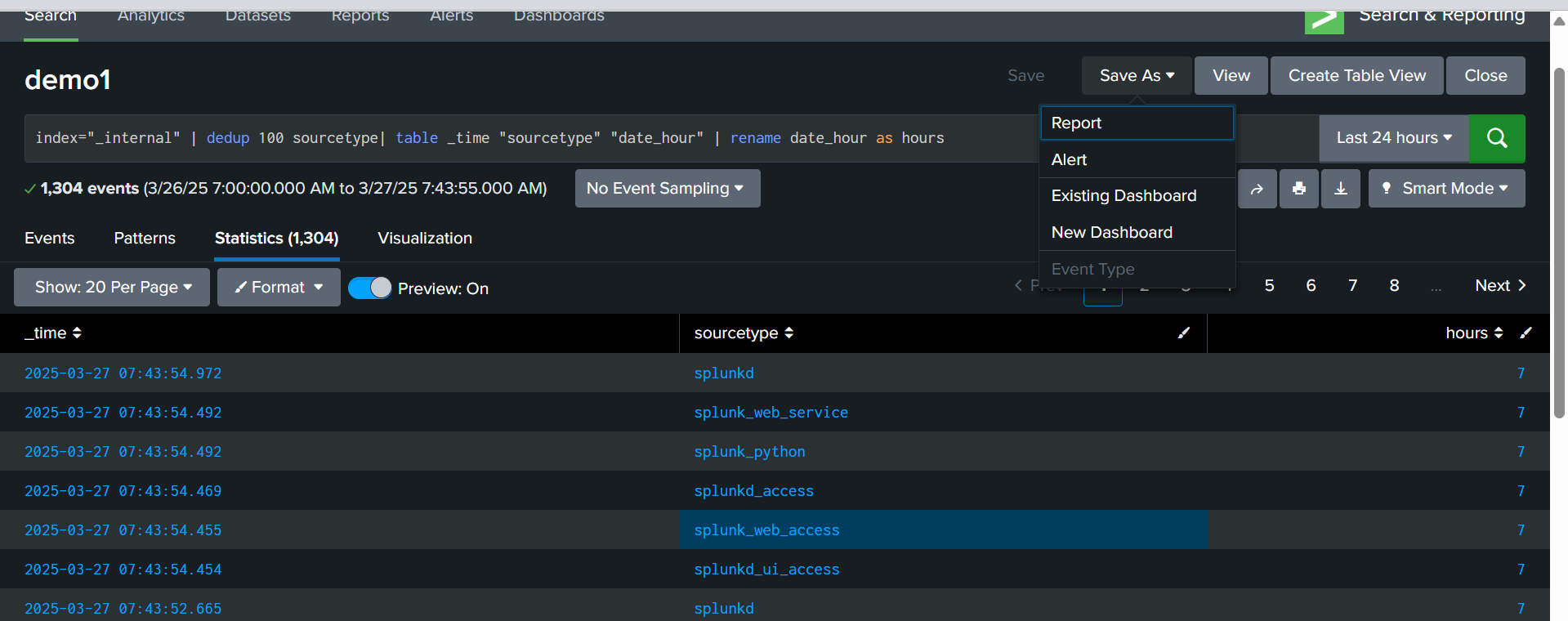


Go to report option which is displayed in the below picture you can the report which you have created



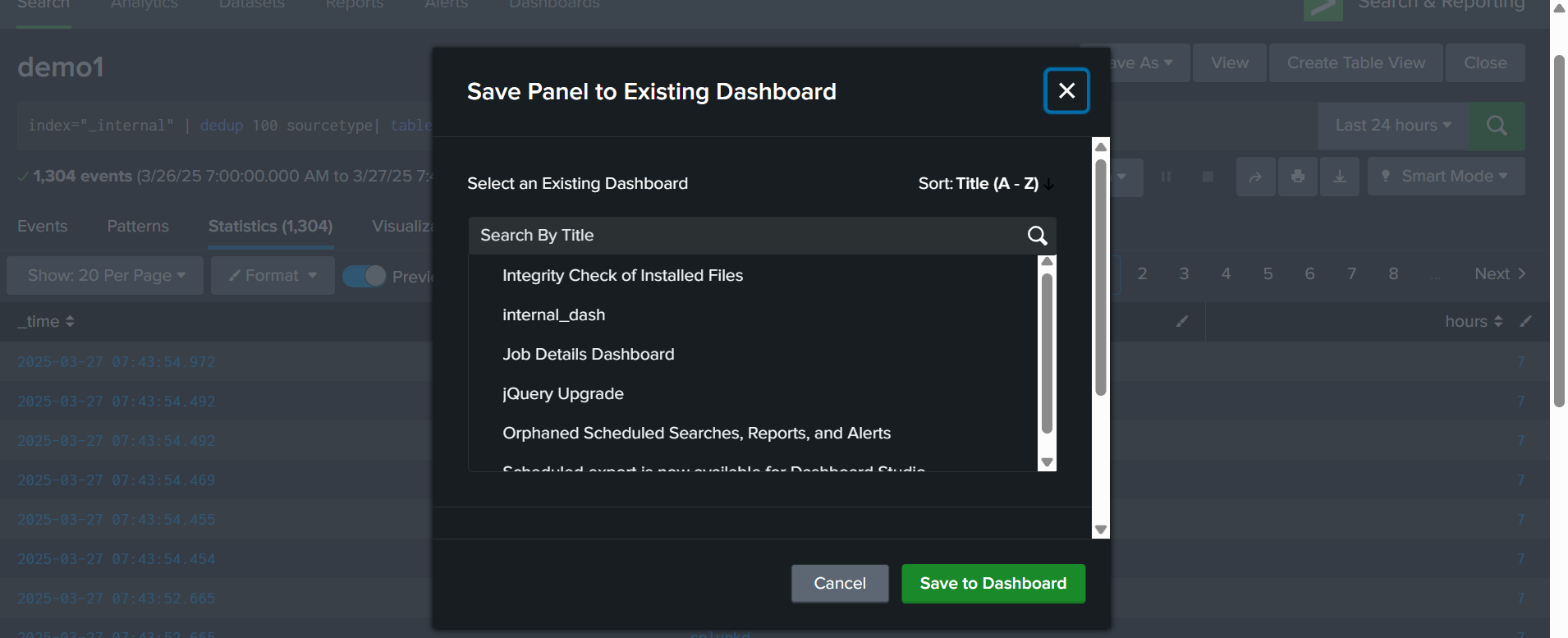
Click 🡪 open in search ----in the report you have created

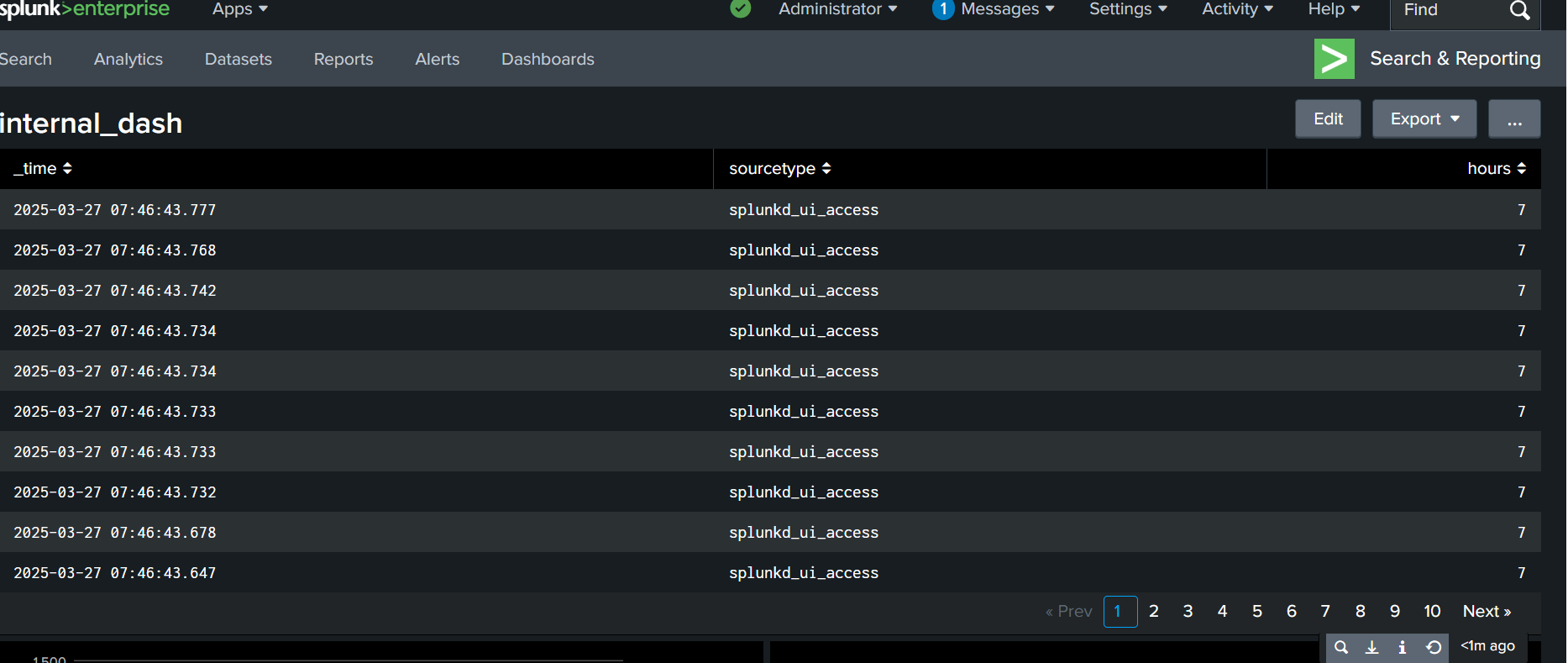
Click🡪save As 🡪existing dashboard



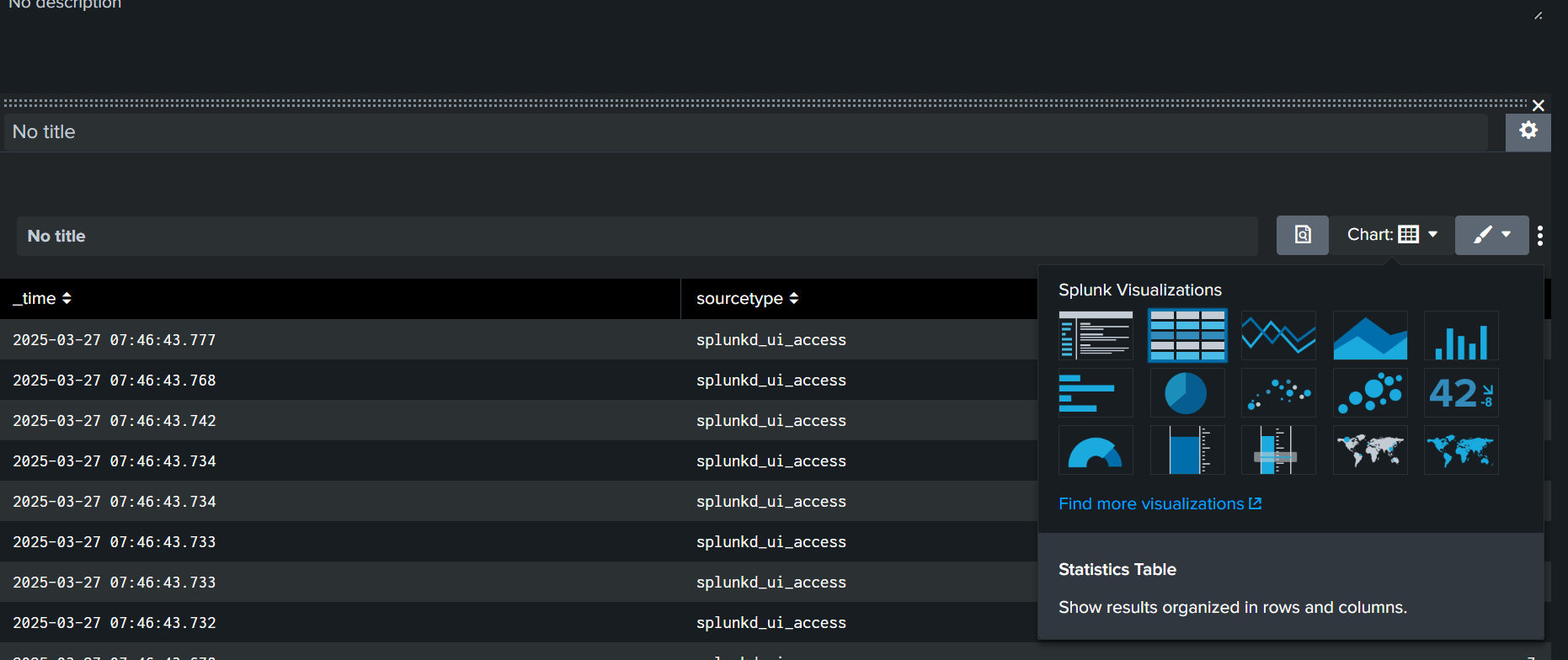
Click🡪 the dashboard which you have created before

Click🡪save to dashboard





Click 🡪edit 🡪 chart in table





CLICK🡪 save

FINAL DASHBOARD:

