Leveraging “search_now” in Summary index to boost query performance

Hello!

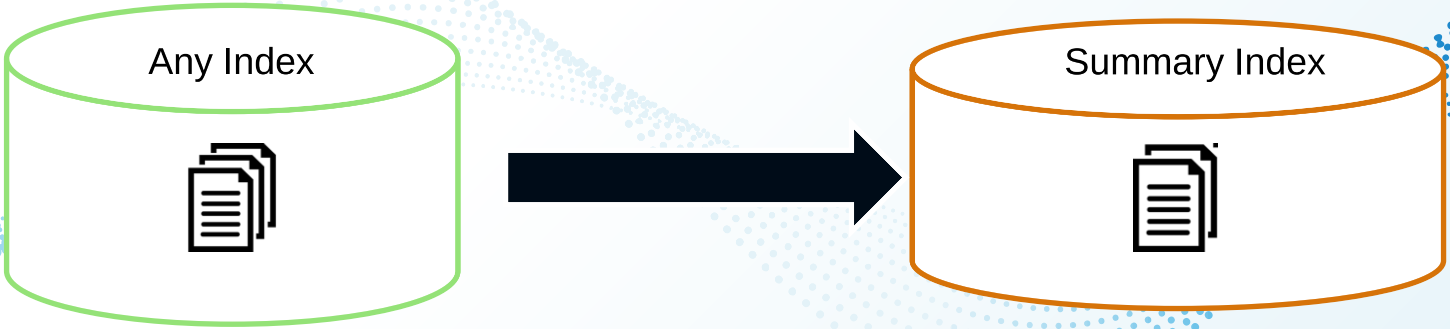
I am Gauri Bansode

I am here because I am a hard core Splunker who loves contributing to this awesome community!

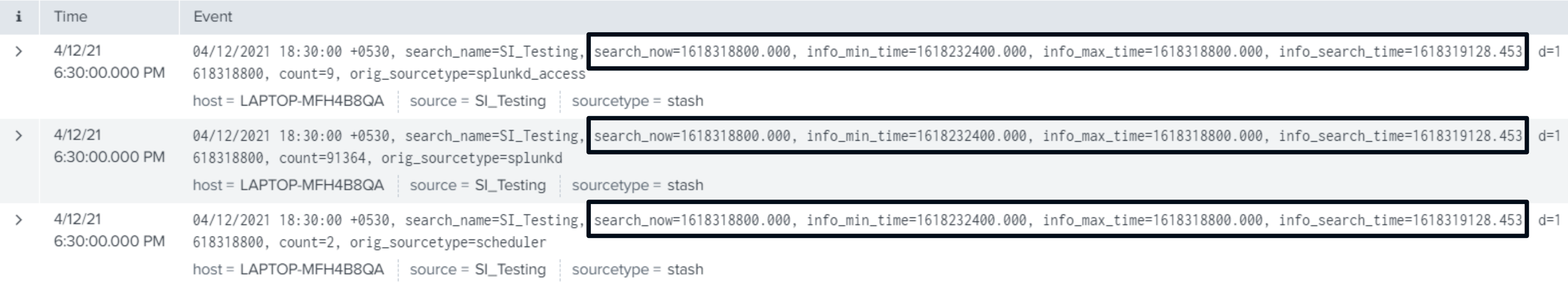
You can find me at @gbansode

Summary Index

Extract a precise set of statistical information from a large dataset and store in summary index.



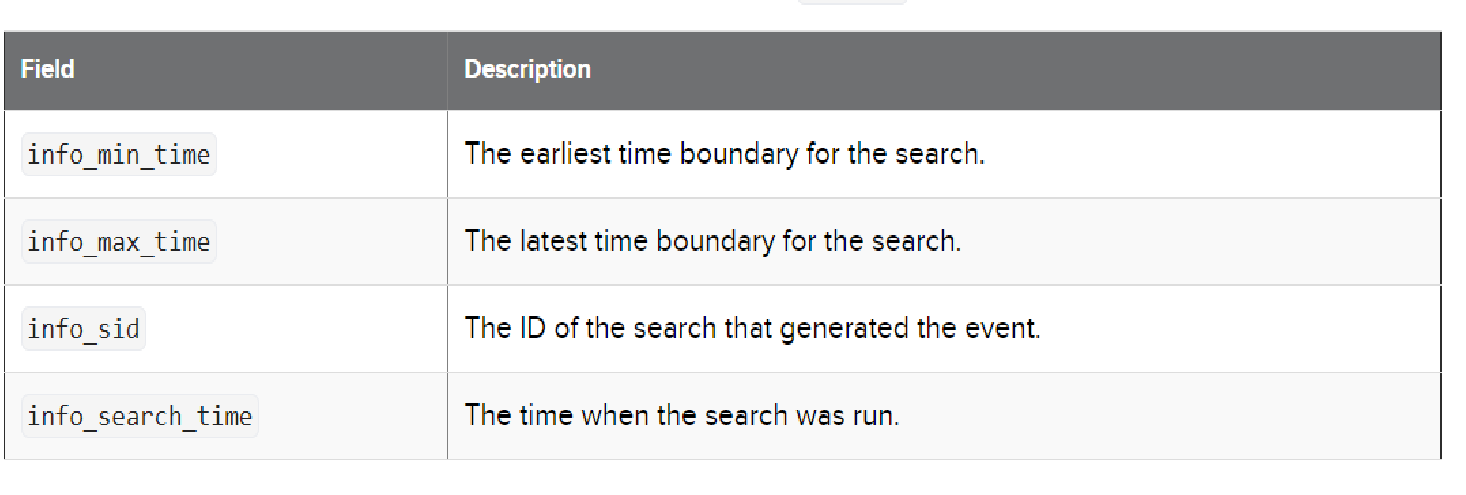
Typical summary index events



i	Time	Event
>	4/12/21 6:30:00.000 PM	04/12/2021 18:30:00 +0530, search_name=SI_Testing, search_now=1618318800.000, info_min_time=1618232400.000, info_max_time=1618318800.000, info_search_time=1618319128.453 d=1 618318800, count=9, orig_sourcetype=splunkd_access host = LAPTOP-MFH4B8QA │ source = SI_Testing │ sourcetype = stash
>	4/12/21 6:30:00.000 PM	04/12/2021 18:30:00 +0530, search_name=SI_Testing, search_now=1618318800.000, info_min_time=1618232400.000, info_max_time=1618318800.000, info_search_time=1618319128.453 d=1 618318800, count=91364, orig_sourcetype=splunkd host = LAPTOP-MFH4B8QA │ source = SI_Testing │ sourcetype = stash
>	4/12/21 6:30:00.000 PM	04/12/2021 18:30:00 +0530, search_name=SI_Testing, search_now=1618318800.000, info_min_time=1618232400.000, info_max_time=1618318800.000, info_search_time=1618319128.453 d=1 618318800, count=2, orig_sourcetype=scheduler host = LAPTOP-MFH4B8QA │ source = SI_Testing │ sourcetype = stash

Where do these fields come from?

Splunk uses the “addinfo” command to add general information by default.



Field	Description
`info_min_time`	The earliest time boundary for the search.
`info_max_time`	The latest time boundary for the search.
`info_sid`	The ID of the search that generated the event.
`info_search_time`	The time when the search was run.

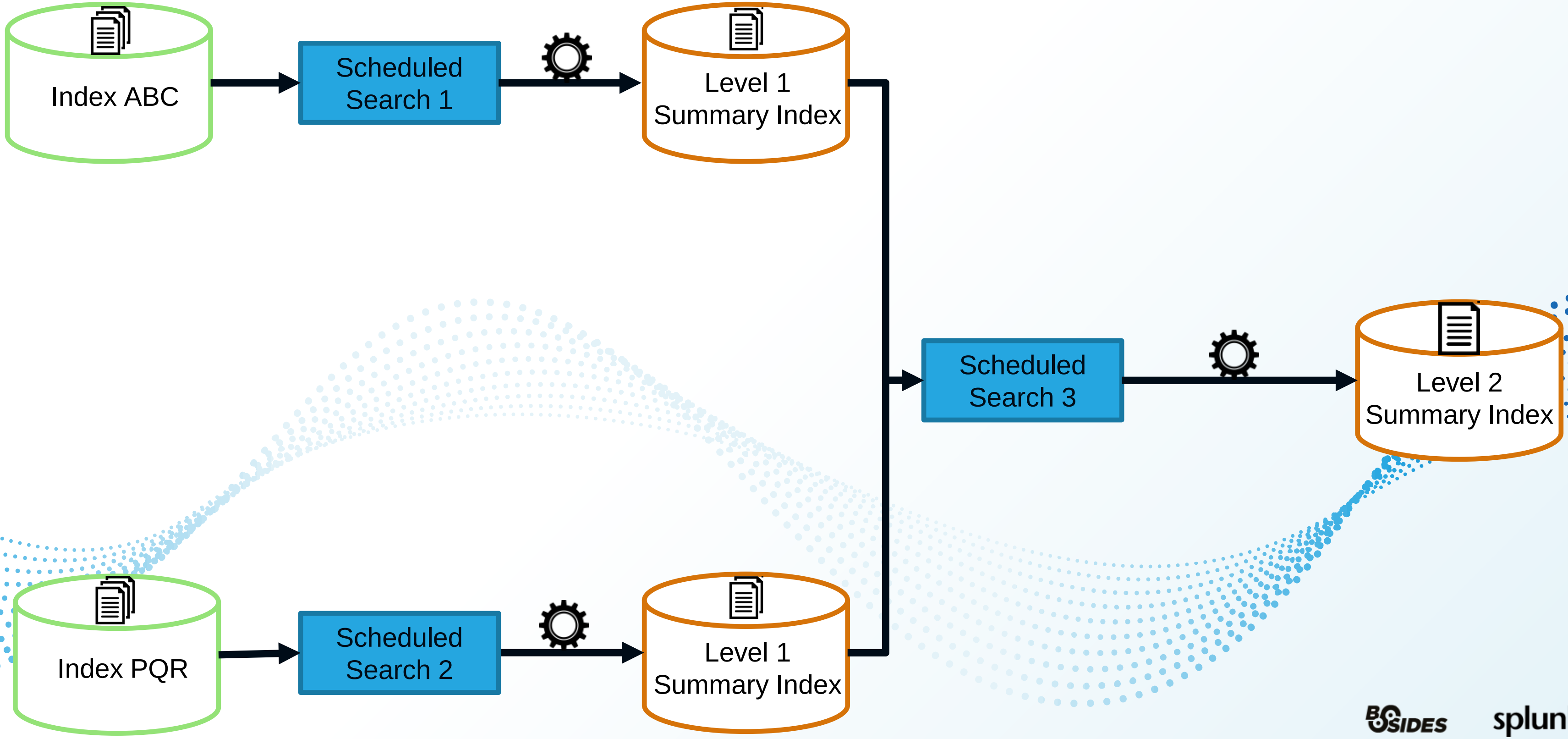
What to do with these fields?

Let's try improving the performance, shall we?

Demo 1

Level 2 Summary Indexing

Level 2 summary indexing



Time for Demo

References:

1) https://docs.splunk.com/Documentation/Splunk/8.1.3/Knowledge/Usesummaryindexing

2) https://community.splunk.com/t5/Knowledge-Management/info-search-time-vs-search-now/m-p/46611

3) https://docs.splunk.com/Documentation/SplunkCloud/8.1.2101/SearchReference/Addinfo

Thanks!

Any questions?

You can find me at

- Slack : @gbansode
- gauri.bansode111@gmail.com

That's all Folks!