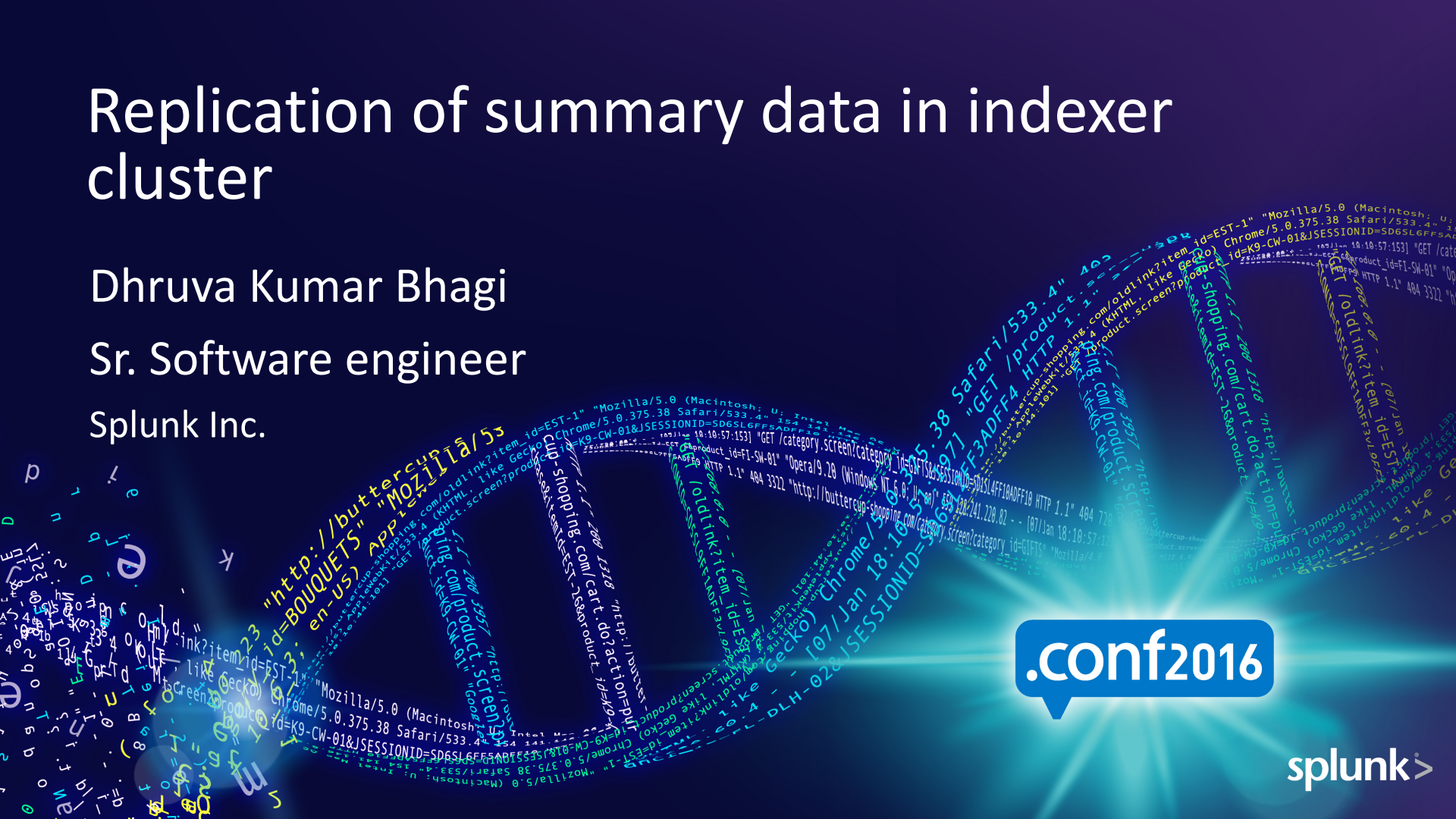
Replication of summary data in indexer cluster

Dhruva Kumar Bhagi

Sr. Software engineer

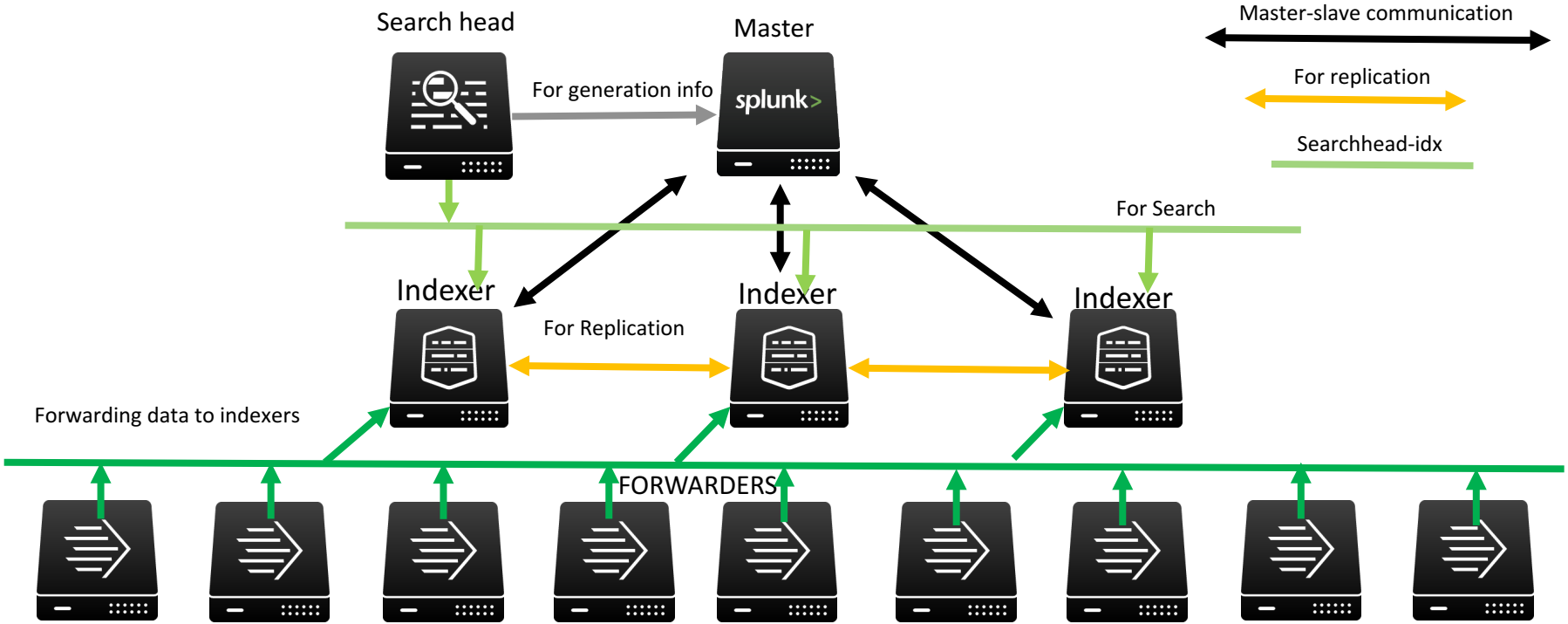
Splunk Inc.



Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Indexer cluster topology



Summaries

- **Summaries** are higher level representation of the search results
- Reside on indexer to help accelerate the execution of long running searches originating from search heads
- Applicable for statistical searches like '**index=main | stats count**'

Summaries

- Two types of summaries:
  - **Report acceleration summaries** – Generated by accelerated reports/searches
  - **Data model summaries** – Generated by accelerated data model pivot searches
- Reside under INDEX/{datamodel_summary|summary}/BID/SH_ID/summary_name/…
- **Note**: summaries are different from summary index

Problem

- Summaries were previously never replicated
- If an indexer with a summary goes down, bucket primaries move to another searchable copy, and searches will not have access to the summaries (until they get regenerated), thereby searches run slow.
- Regenerating summaries can take lot of time

Replicating summaries

- From version 6.4, Splunk can replicate DA & RM summaries in indexer cluster environment
- Peers maintain the list of their summaries (just like buckets) and reports them to CM during registration (or) on any state change
- If any peer is missing a summary for a bucket, master schedules a summary replication with this peer as a replication target
- Only replicate summaries for warm/cold buckets (not hot)
- services/cluster/master/buckets/BUKCET lists summaries of each bucket

Summaries for hot buckets

- For hot buckets, summary searches from searchheads hit all the searchable copies (instead of just primaries for normal searches) thereby letting indexers build the summaries individually for hot buckets.
- No need for summary regeneration even on individual node failures.
- Running summary generating searches on all searchable copies of a hot bucket introduces more resource usage (longer search process, extra memory usage)!

Volume Retention

- Summaries can be set up in a volume to manage space usage
- If indexer exceeds the volume space (**maxVolumeDataSizeMB**), splunk starts trimming summaries
  - A trimmed summary leaves tombstone indicating the trimmed state
  - Tombstone avoids regenerating summaries in the subsequent search runs
  - Once we trim a summary, we propagate this info to the CM, and the CM will issue a trim to all other copies of the summary.

Configuration

- To turn on summary replication, make **summary_replication=true** under clustering stanza on cluster master.
- By default summary replication is turned off.
- **max_peer_sum_rep_load** (defaults to 5) configures how many maximum summary replications per peer
- Config changes are reloadable (i.e. does not require a splunk restart)

THANK YOU

splunk>

Wednesday, Sep 28 **3:00 PM - 3:15 PM**