Chargeback App

James Donn

Senior SE, Splunk

A Little About Me

- 4+ Years at Splunk
- Happy Splunk Customer for 4+ years
  Harvard and MITRE
- Focused on Network and Systems Management

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.

Agenda

- History
- Strategy
- Future
- Demo

Why?

- My boss asked me to
- My customers keep asking me the same question
  - I had an answer
  - I did not have a proper solution or starting point
- If three or more customers ask you the same question, there needs to be a documented resolution

Customer Interest

Who is it for?

- Universities
- Edu Research
- Government
- Entertainment
- Large Financials
- Pharma
- Manufacturing

What size Deployments?

- Works well for all implementations:
  - Large
  - Medium
  - Small

What Is The Real Problem?

- My boss asked me:
  "How much have other groups used of Splunk, so we can charge them?"
  - I mistakenly answered his question
  - It was a lot of work
  - Splunk can remove the pain!
- What I should have asked…
- His reply would have been…

- This would have changed my strategy!

Strategy – Run Rates

Why not buy index usage?

- It is not how we buy/sell Splunk
- It does not reflect the cost of running or provisioning Splunk

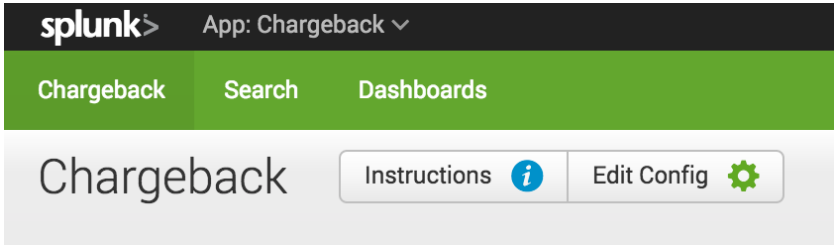
License

- Every customer has a “micro license”
- Volume per index
- Indexes can be shared

Storage

- Hot/Warm and Cold rates
- Calculations are based on index volume configuration

How Do You Configure It?



Customers.csv

For first time configurations, build your customers.csv file with the following search command. **This will overwrite the lookup file!**:

| rest /services/data/indexes | dedup title | search NOT title=_* NOT title=*summary* | rename title AS idx | fillnull value=0 max_lic_GB | fillnull value=100 percent_ownership | fillnull value=UNDEF group | table group, idx, max_lic_GB, percent_ownership | outputlookup customers.csv

Column Headers - DO NOT ALTER THE NAME OF THE COLUMN HEADERS:

group, idx, micro_lic_GB, and percent_ownership

group - These are the different departments that you are providing Splunk as a service to. They are you customers.

idx - These are the indexes that you have configured and will account for the cost associated with. Match the names exactly and include all of them that are not internal or summary indexes. Internal indexes begin with an underscore and summary indexes should have "summary" in their name.

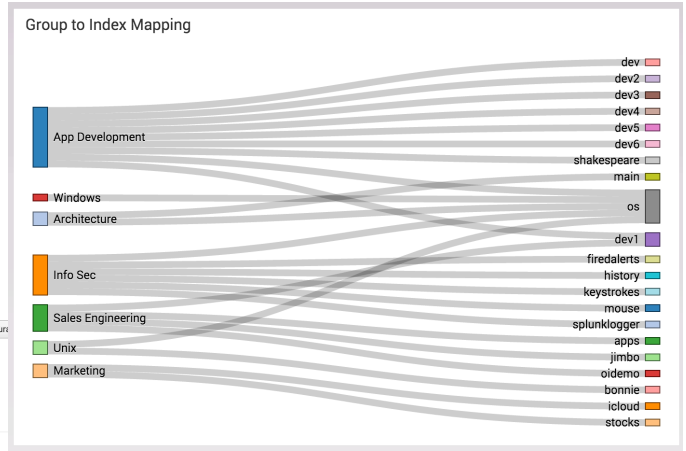
micro_lic_GB - This is the maximum daily data volume in GBs that your customer is going to use per index. It can be thought of as a "Micro License", but has no impact on internal Splunk licensing. This is used to calculate the total cost to the customer. This number is always the same, even if more than one group shares an index (use the total). This is also used as a threshold for alerting against groups that use more than their allocated share of the license.

percent_ownership - When more than one group shares an index, this is the percentage of ownership assigned to each group. The total percent_ownership across all groups must equal 100.

How Does It Work?

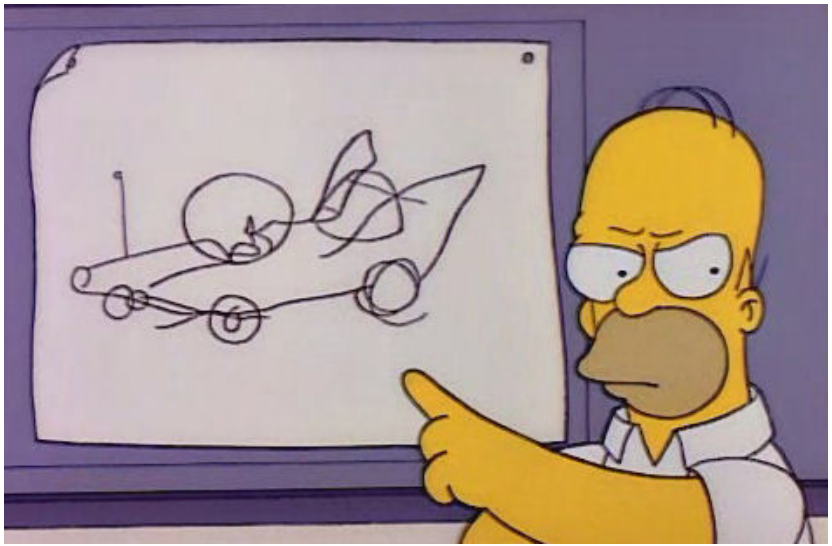
What Additional Features Does It Have?

- Group to Index visualization
- Predictive Index Utilization Analysis
- License Analysis by Index
  - Alert?
  - Punish?
- Configuration checks:
  - Customers.csv
  - Indexes



Future Features

- ✓ ~~Monitor volume storage~~
- ✓ ~~Alert on Index Utilization Violations~~
- License Maintenance for Premium Apps:
  - ES
  - PCI
  - Exchange
  - ITSI
- Other Splunk Server Types:
  - Search Heads
  - License Server
  - Master Server
  - Deployer
  - Deployment Server



Before the Chargeback App

After The Chargeback App

Demo

Thank you!

jim@splunk.com

THANK YOU

jim@splunk.com

.conf2016

splunk>

Customer Interest

- Harvard University
- MITRE
- ESPN
- Liberty Mutual
- CVS
- Broad Institute
- Monster

- Travelers
- Fidelity
- Scotia Bank
- Telstra
- Voya
- NIST.gov
- Bosch