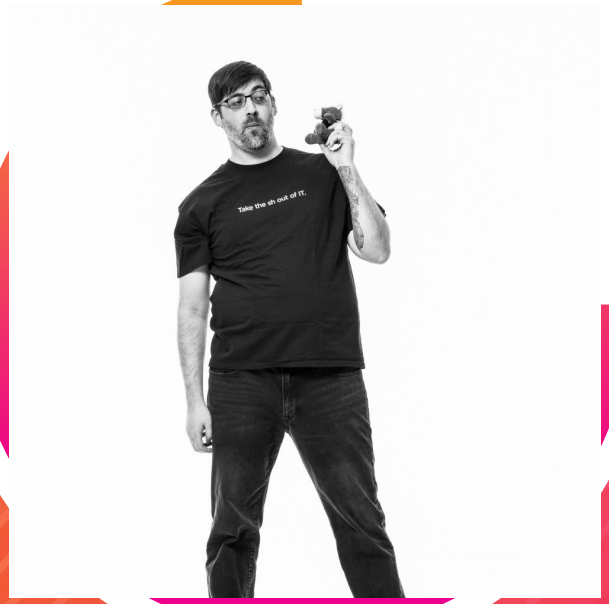
Next Generation Data Ingestion and Preparation with Splunk

splunk> .conf19



Eric Sammer
Distinguished Engineer

Asmita Puri
Senior Software Engineer

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. 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, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

How I ingest data today

1. The all or nothing approach

2. Everything works...well, almost. Works for 99% of use cases
   - Fork the existing TA
   - *Fix* it for the use case I am working with
   - And then use it and hope it works.

3. One to one relationship between source of data and the indexes.

4. .conf and prop files or restarting Splunk

What if

The ideal world..a world where simple things are simple and complex things are possible.

- Use parts of the pre-built content
- Understand health of the data
- Profile your data and see it real time
- Ability to integrate with other systems easily
- Support wide variety of use cases
- Support various levels of expertise

What do we need to build this world?

The ideal world..a world where simple things are simple and complex things are possible.

- Use parts of pre-built solution
- Pipelines and templates
- Ability to integrate with other system
- Sources and sinks

Demo - 1

What do we need to build this world?

The ideal world..a world where simple things are simple and complex things are possible.

- Understand health of the data
- Show ingested data metrics
- Profile the data
- Data preview and preparation

Demo - 2

What do we need to build this world?

The ideal world..a world where simple things are simple and complex things are possible.

- Support various expertise levels
- No code, low code & pro code

Demo - 3

Where are we?

A world where simple things are simple and complex things are possible.

- Use parts of pre-built solution
- Ability to integrate with other system
- Understand your data
- Profile the data
- Support various expertise levels
- Pipelines and templates
- Sources and sinks
- Show amount of data ingested
- Data preview and preparation
- No code, low code & pro code

Resources

1. Splunk Investigate
2. Add data by creating a pipeline
3. Streams service
4. Source Pavilion – dev zone

Other Data Stream Processor Sessions

1. DEV1317 - DSP Architecture & SDKs 10/23 1:45PM
2. FN1786 - DSP for advanced stream management 10/23 12:30PM
3. DEV1139 - ML + DSP: Anomalies in DSP 10/23 4:15PM
4. FN2033 - Using DSP as a data transformation 10/23 11:15AM
5. FN1987 - DSP as streaming engine for Apache 10/23 3:15PM
6. FN2062 - DSP: How to get the most from your data (Missed it)

How do I get started?

- Go to si.scp.splunk.com
- Click Manage Data tab
- Upload a file
- Get started!!

What about Enterprise?

- Call your sales rep now!

.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION