What You Need To Know About HTTP Event Collector

Shakeel Mohamed

Software Engineer, Splunk

.conf2016

splunk>

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.

What the HEC?

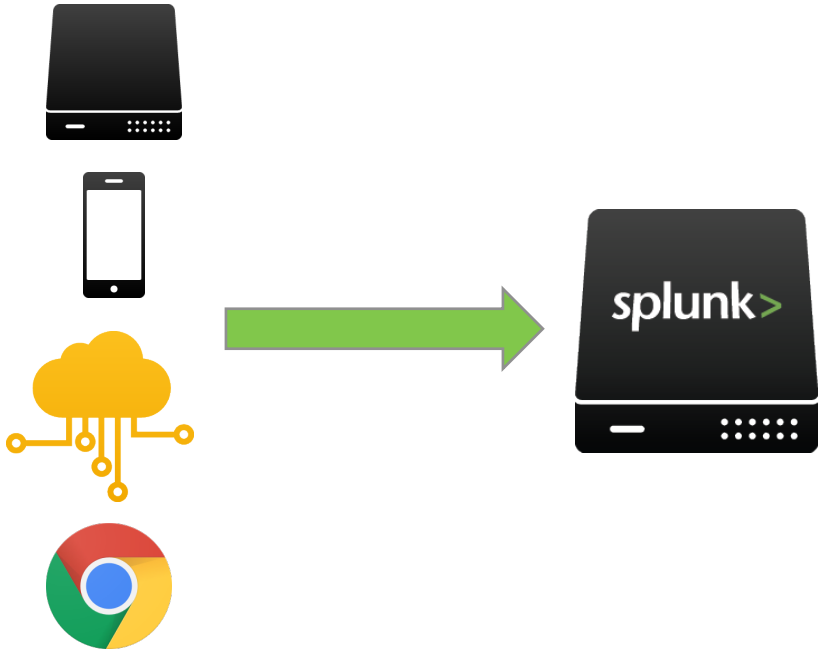
A new token-based JSON API for events

Send events ***directly*** from anywhere (servers, mobile devices, IOT)

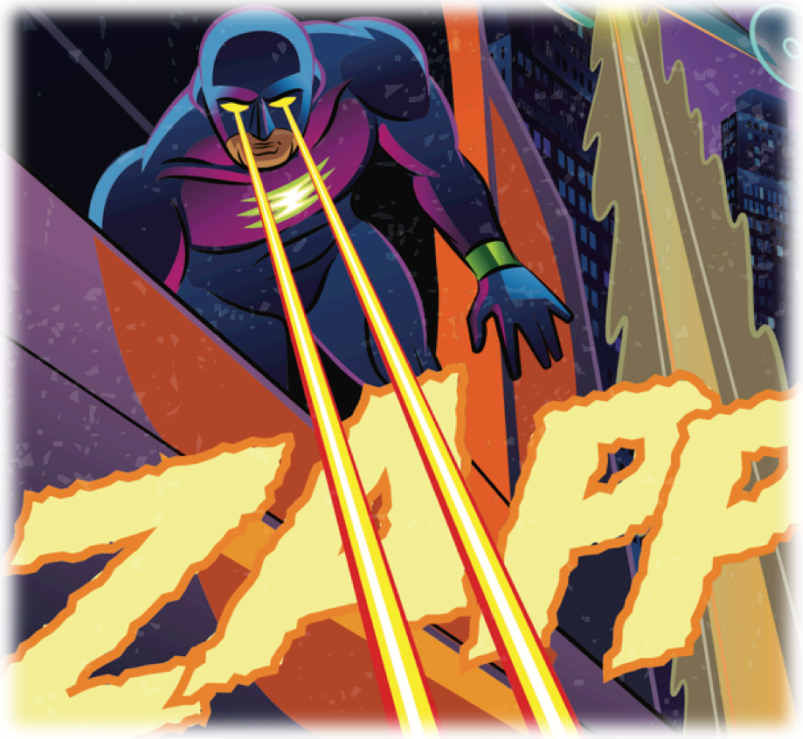
Easy to configure / works out of the box.

Easy to secure

Highly performant, scalable and available



In 6.5, HEC returns with even more powers!



In Splunk 6.3:

HEC only accepts data in our JSON event format

HEC RAW

HEC RAW

You can now send data in arbitrary formats to HEC!

Useful for integration with existing systems that can send data over HTTP

In Splunk 6.3:

Clients do not know if events have been indexed

Indexer ACK

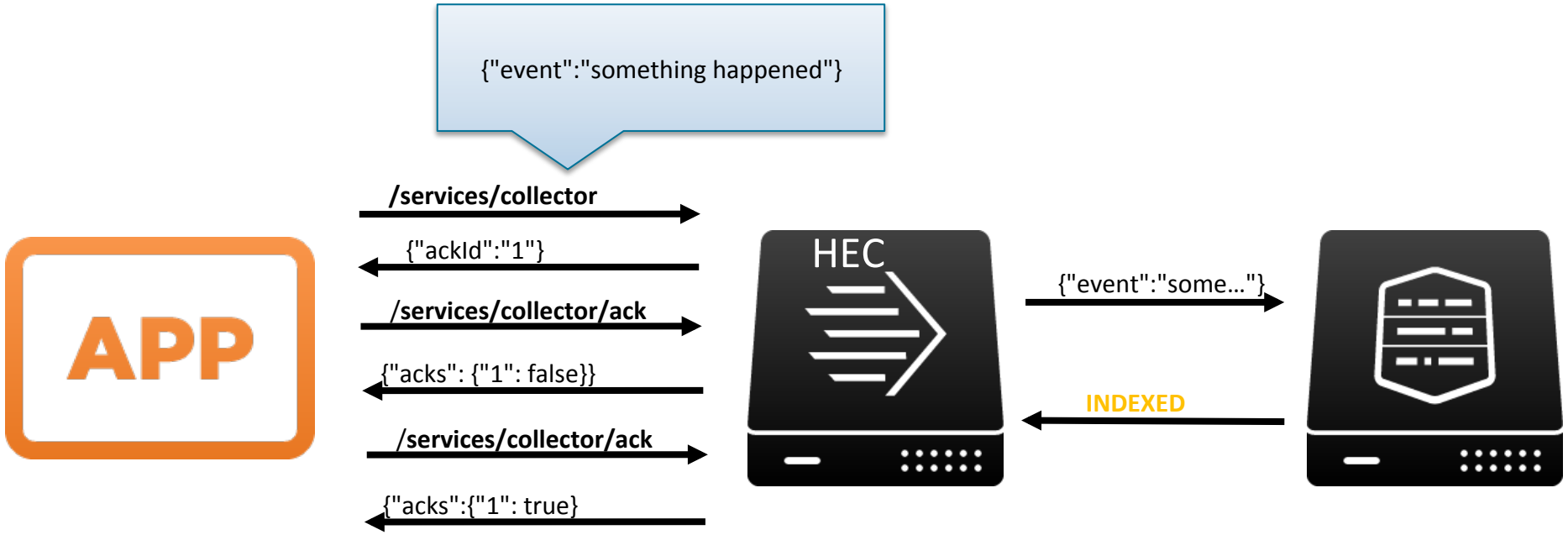
Indexer ACK

You can now receive an acknowledgment when events are indexed*

Useful for reducing data loss during outages

*Flexibility comes at a cost

Indexer ACK


{"event":"something happened"}
APP
/services/collector
{"ackId":"1"}
/services/collector/ack
{"acks": {"1": false}}
/services/collector/ack
{"acks":{"1": true}
HEC
{"event":"some…"}
INDEXED

In Splunk 6.3:

Only regex extractions are supported

Index field ehancements

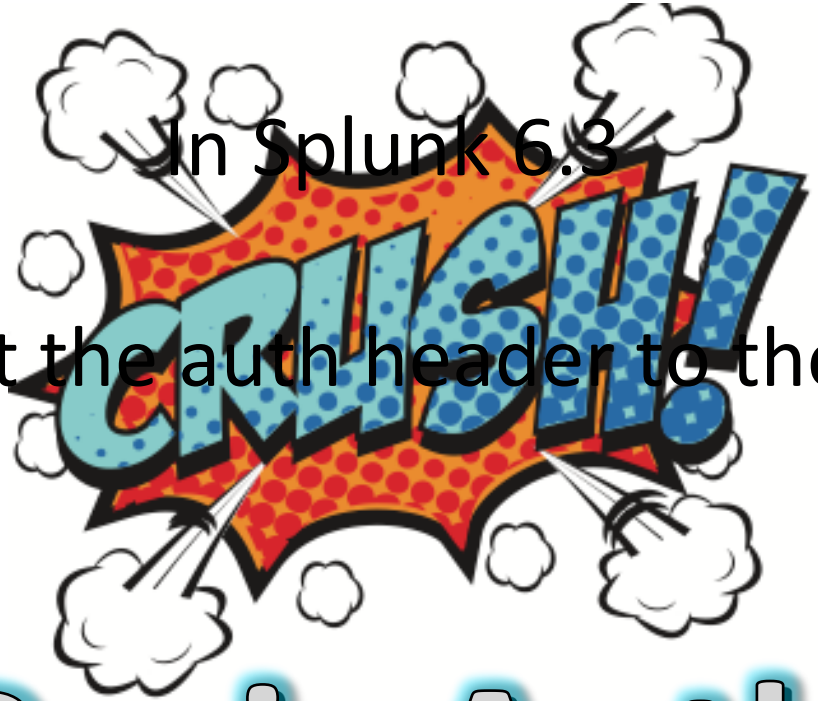
Index field enhancements

JSON Field extraction finally works for HEC!

You can now specify additional index fields separate from the "event" playload! (JSON endpoint only)

Useful for search time perf improvements as well as for supplying event custom metadata

In Splunk 6.3



Clients must set the auth header to the Splunk token

Basic Auth

Basic Auth

You can now use Basic Auth to authenticate your HEC requests

Useful for systems that do not support custom auth header values but can support Basic Auth via the URI (Github web hooks)

In Splunk 6.3

You need to master Splunk FU

to monitor HEC instances

HEC Console

HEC Console

You can now monitor HEC using the new DMC dashboard

Useful for ensuring your HEC instances are performing as they should, and for detecting anomalies / failures

And that's not it

Dedicated HEC settings

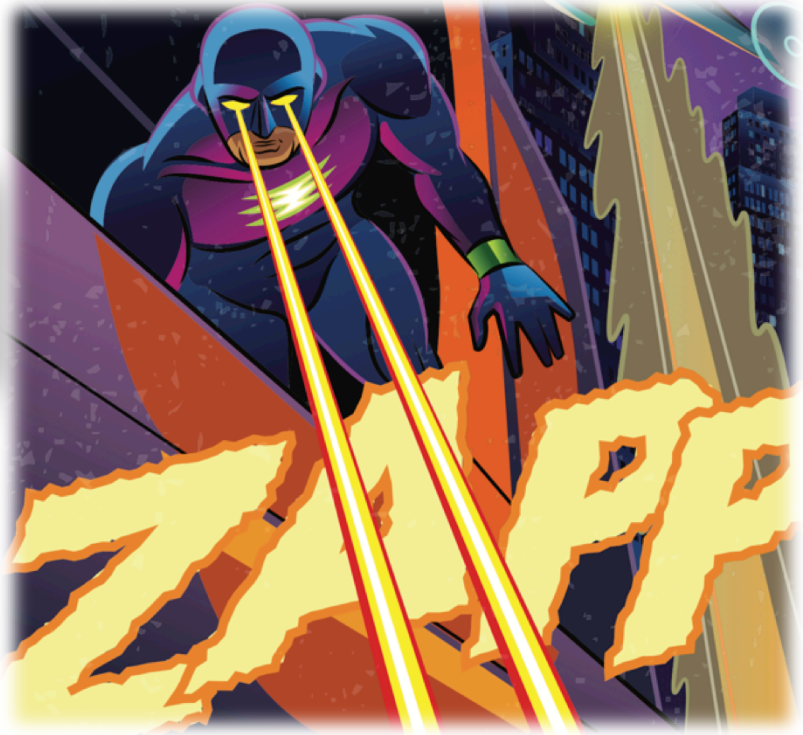
inputs.conf.spec

```
#*******
# http: (HTTP Event Collector)
#*******

# Global settings for the HTTP Event Collector (HEC) Input.

[http]
```

- SSL
- CORS
- IP restrictions



Learn more!

http://splk.it/new_HEC

THANK YOU

splunk>