.conf2015

Liberate Your Application Logging!

Glenn Block (@gblock) – Senior Product Manager
Jian Lee – Senior Software Engineer
Splunk Developer Platform & Core

splunk>

Disclaimer

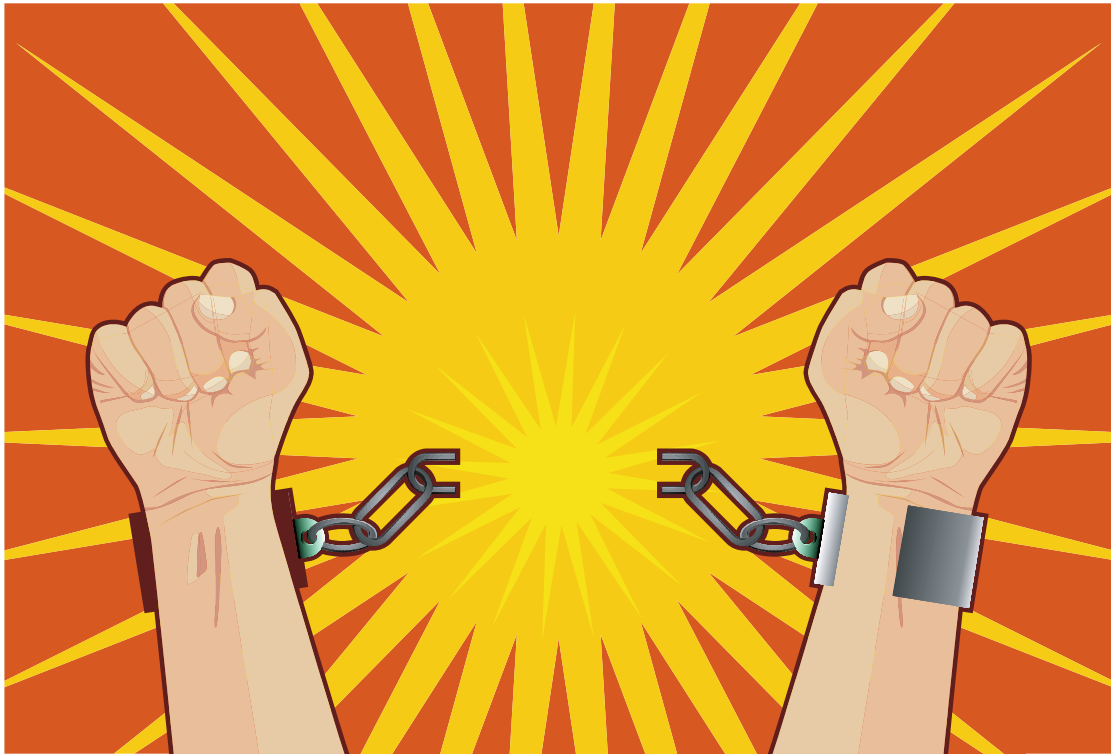
During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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.


"Sending events to Splunk from my apps is hard!"
A disgruntled developer:

Your app logs should be freed to be Splunked!

Free from requiring a local forwarder



Free from scale and performance bottlenecks

Free from complex configuration

Free to be sent from any client

In Splunk 6.3, they can be liberated!

Introducing

HTTP Event Collector

HTTP Event Collector

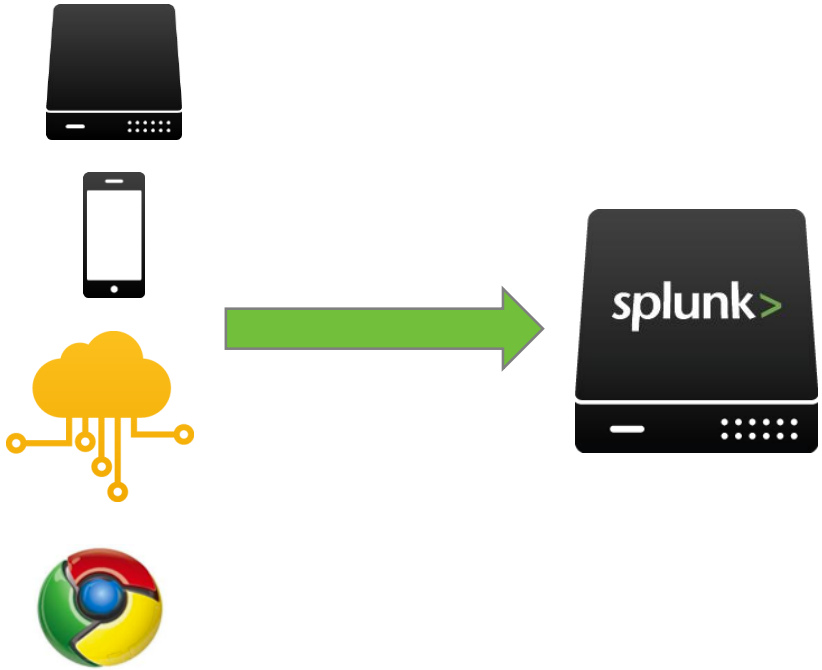
A new token-based JSON API for events

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



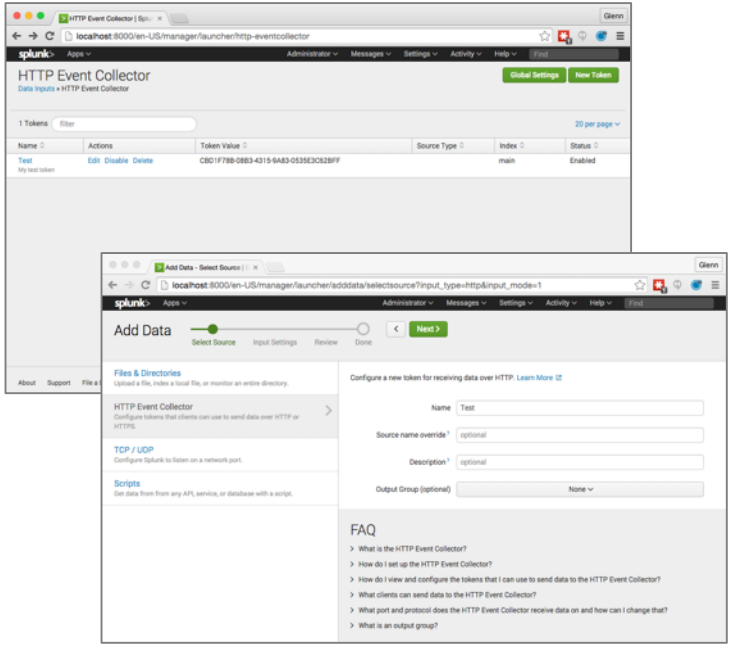
Demo:

HTTP Event Collector

splunk>

How You Use

- Enable HTTP Event Collector
- Create/Get a token
- Send events to Splunk using the token
  - Use **HTTP Directly**
    - Create a POST request and set the Auth header with the token
    - POST JSON in our *event format* to the collector
  - Use **logging libraries**
    - Support for .NET, Java and JavaScript loggers



Sending Data

```
//send with curl
curl -k https://localhost:8088/services/collector
-H 'Authorization: Splunk 46931F1C-352C-4DF6-
820C-F2689CF88494' -d '{"event":"Hello Event
Collector"}'
```

Demo:

Event Protocol Capabilities

splunk>

Event Protocol Advanced Capabilities

JSON objects

```
{
  "event": {
    "message":"….",
    "severity":"warn"
    "category":"web"
  }
}
```

Batching:

```
{"event":"event 1"}
{"event":"event 2"}
{"event":"event 3"}
```

Metadata:

```
{
 "source":"foo",
 "sourcetype":"bar",
 "host": "192.168.1.1",
 "time": 1441139779
 "event":"Hello World"
}
```

Index selection:

```
{
  "index": "collector"
  "event":"Hello World"
  }
```

Logging Libraries

- Very easy for developers to pull into their applications
- Provide integrations with common loggers (log4J, log4net, etc)
- Provide robustness (batching, retries)
- Supported in Java , .NET and node.js

Demo:

Logging Libraries

splunk>

How Do You Use Them?

- Pull the logging library of choice into your application
  - Java – log4j, logback, and java.util.logging
  - .NET – Trace Listeners and SLAB
  - JS - Bunyan
- Configure the logger
- Log away!

3rd Party Integrations

Demo:

3rd Party Integration

splunk>

Liberate your logs!

HTTP Event Collector

Next Steps?

Related breakout sessions and activities…

Breakouts

- The HTTP Event Collector, a New Way for Developers to Send Events to Splunk
- Accelerating your Solution Development with Splunk Reference Apps

More information

- dev.splunk.com
- blogs.splunk.com/dev

Come by the Developer Booth and say hi / ask questions!

THANK YOU

splunk>