

splunk® + ClickHouse

Empower your analysis with big data

Kent Wang @ SPLUNK Shanghai R&D Center



A large, faint watermark of a log file or database dump is visible across the bottom right of the slide. The text is oriented diagonally and contains numerous log entries with fields like "product_id", "category", "screen", "action", "item_id", "version", "platform", and "browser". Some entries include URLs such as "http://buttercup-shopping.com/cart/addtocart?category_id=EST-1&product_id=EST-1&item_id=EST-1&version=1.1&platform=Windows NT 6.0&browser=Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" and "http://buttercup-shopping.com/cart/doaction?category_id=EST-1&product_id=EST-1&item_id=EST-1&version=1.1&platform=Macintosh; U; Intel Mac OS X 10.5.8 AppleWebKit/534.55.17 (KHTML, like Gecko) Version/5.1.3 Safari/534.55.17".

Who are we



The IT know-it-all.

You may see the machine-generated data created by all of your network elements as a overwhelming flood of information. But if you believe it, you can make your data not only manageable, but so easy to read, analyze and correlate that the folks in the corner offices may be inviting you to the next board meeting.

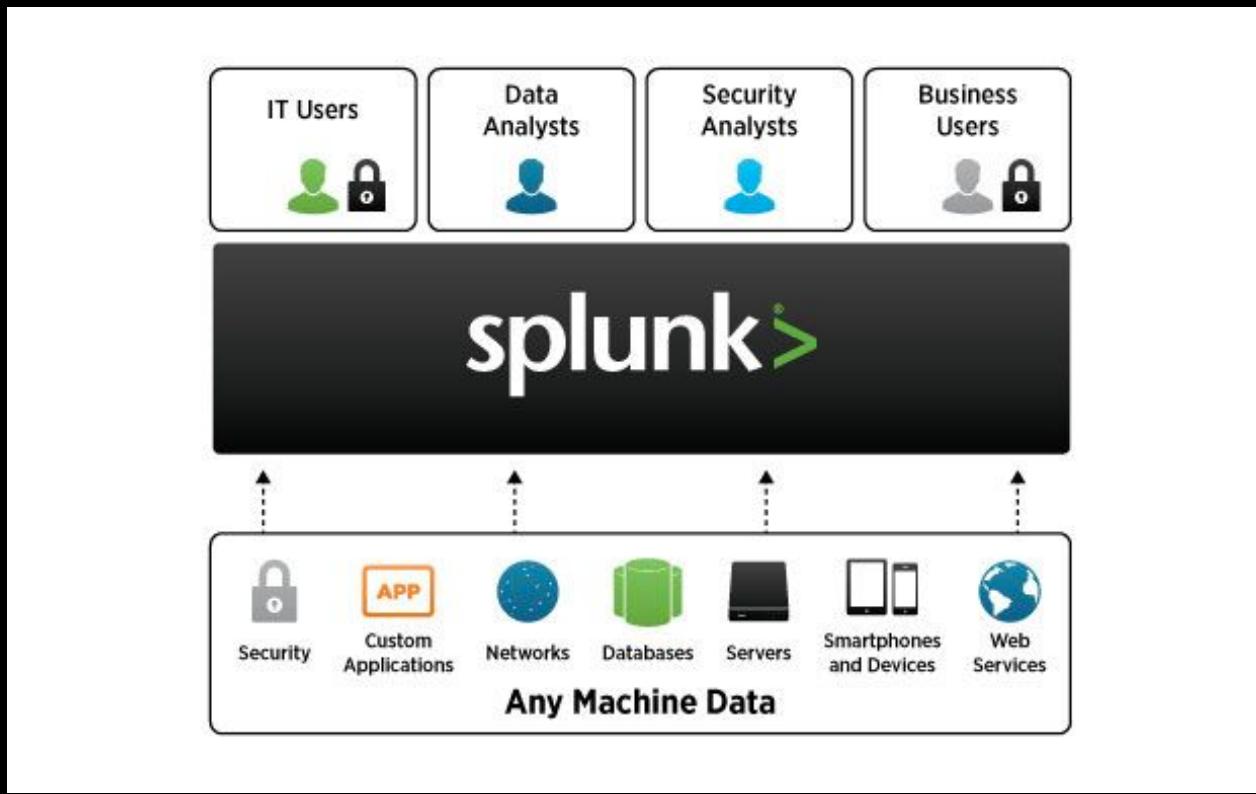
splunk > listen to your data

- ▶ Splunk® was founded to pursue a disruptive new vision: make **machine data** accessible, usable and valuable to everyone
- ▶ First IPO big data company at NASDAQ in 2012
- ▶ Shanghai R&D Center built in 2014
- ▶ Enterprise Security
- ▶ IT Operation



splunk > listen to your data™

Splunk Enterprise Platform



splunk> listen to your data™

Motivation

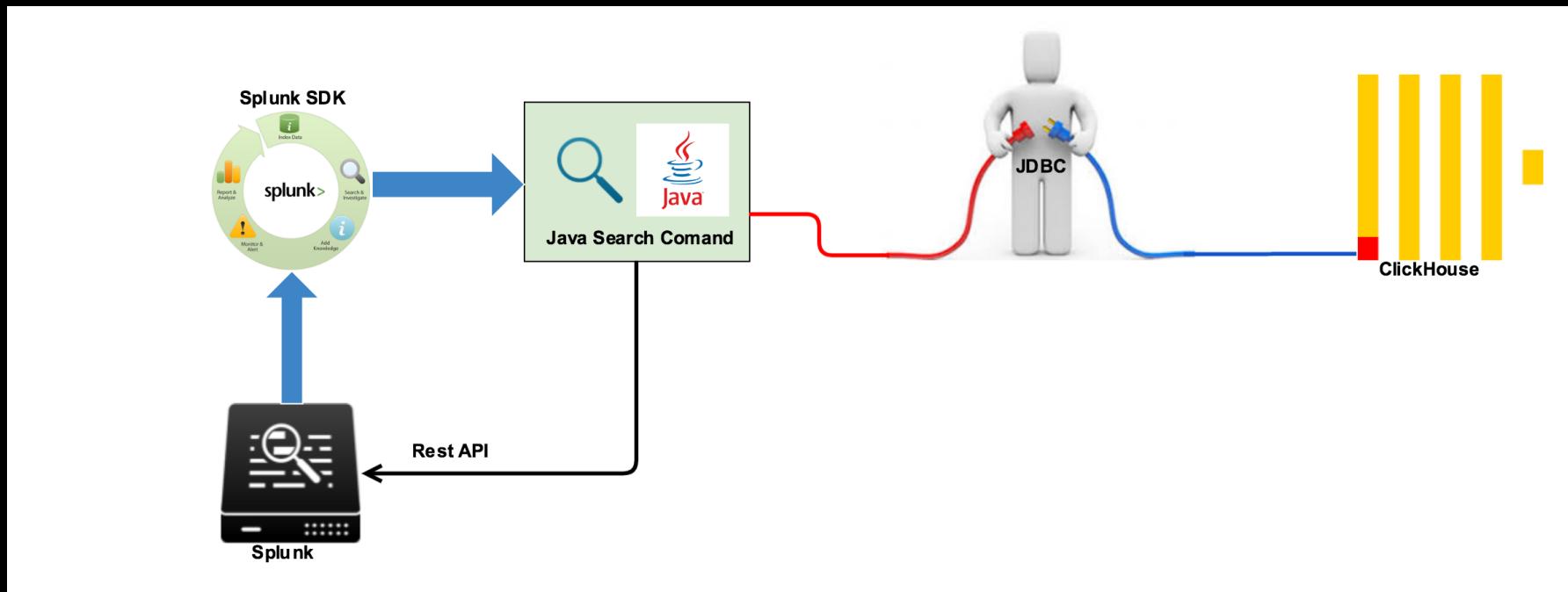
- ▶ Leverage the lightning fast Clickhouse OLAP search
 - ▶ No data movement between system
 - ▶ Leverage the full-featured data visualization of splunk
 - ▶ Correlate analyze data in splunk index and clickhouse storage engine
 - ▶ One stop solution for data analyst

DEMO

► Case One: Data In

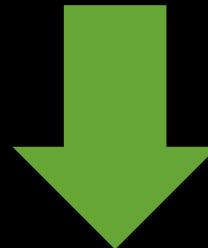
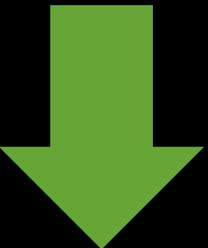
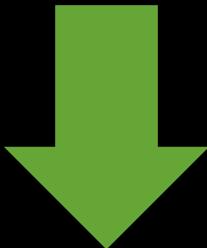
- Extend the Splunk SPL to run customized search command to get query result from ClickHouse

Architecture Design



splunk > listen to your data®

```
|dbxquery query="XXX"connection="ch_lab"
```



Customized Command

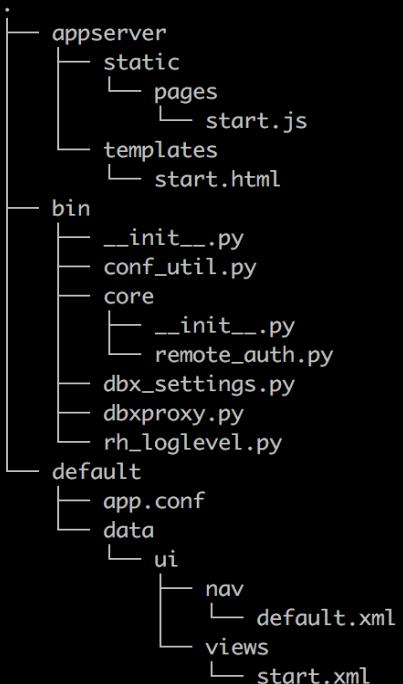
SQL

```
[ch_lab]
connection_type = clickhouse
customizedJdbcUrl = jdbc:clickhouse://localhost:32770/NYC_TAXI
database = NYC_TAXI
disabled = 0
host = 172.17.0.2
identity = test
jdbcUseSSL = false
localTimezoneConversionEnabled = false
port = 9000
readonly = false
```

DEMO

► Case Two: Visualization

- Query data in ClickHouse and use Splunk web framework to visualize



Extensible Platform

Build Splunk App

Extend and Integrate Splunk

Web
Framework

Simple XML

JavaScript

Splunk UI

SDKs

JAVA
JavaScript
Python

Ruby
C#
PHP

Data Models

Search Extend

Modular Input

REST API

Splunk >

```
139.69.4. - [02/Jan/18:19:57:153] "GET /category/view&itemId=EST-G&product_id=SPL-AFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-G&product_id=SPL-AFF10" "Mozilla/5.0 (Windows NT 10.0; Win32; SV1.0; .NET CLR 1.1.4322; .NET4.0.30319) AppleWebKit/535.17 (KHTML, like Gecko) Chrome/1.1.149.2080 Safari/535.17" "GET /category/SURPRISE&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changeItem&itemId=EST-186&product_id=SPL-AFF10" "Mozilla/5.0 (Windows NT 10.0; Win32; SV1.0; .NET CLR 1.1.4322; .NET4.0.30319) AppleWebKit/535.17 (KHTML, like Gecko) Chrome/1.1.149.2080 Safari/535.17" "GET /category/flowers&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 189 "http://buttercup-shopping.com/cart.do?action=changeItem&itemId=EST-187&product_id=SPL-AFF10" "Mozilla/5.0 (Windows NT 10.0; Win32; SV1.0; .NET CLR 1.1.4322; .NET4.0.30319) AppleWebKit/535.17 (KHTML, like Gecko) Chrome/1.1.149.2080 Safari/535.17" "GET /category/flowers&SESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 189 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-188&product_id=SPL-AFF10" "Mozilla/5.0 (Windows NT 10.0; Win32; SV1.0; .NET CLR 1.1.4322; .NET4.0.30319) AppleWebKit/535.17 (KHTML, like Gecko) Chrome/1.1.149.2080 Safari/535.17"
```

splunk > listen to your data

DEMO

► Case One: Data In

- Extend the Splunk SPL to run customized search command to get query result from ClickHouse

► Case Two: Visualization

- Query data in ClickHouse and use Splunk web framework to visualize

► Case Three: Analyze

- Use realtime search to analyze the visualization

Future: the best is yet to come

- ▶ OLAP workflow support in Splunk
- ▶ Modular Input integration
- ▶ Data model integration
- ▶ Leverage advanced features in Splunk like alerting, data model acceleration, report acceleration etc.
- ▶ Collect more user scenario about ClickHouse



A diver is swimming in a dark blue underwater environment. The water is filled with glowing, translucent binary code digits (0s and 1s) that form bubbles and swirls around the diver. In the background, there are some coral reefs and a bright light source, possibly sunlight, filtering down from above. The overall atmosphere is mysterious and futuristic.

Thank you

Q & A