splunk> + ClickHouse

Empower your analysis with big data

Kent Wang @ SPLUNK Shanghai R&D Center

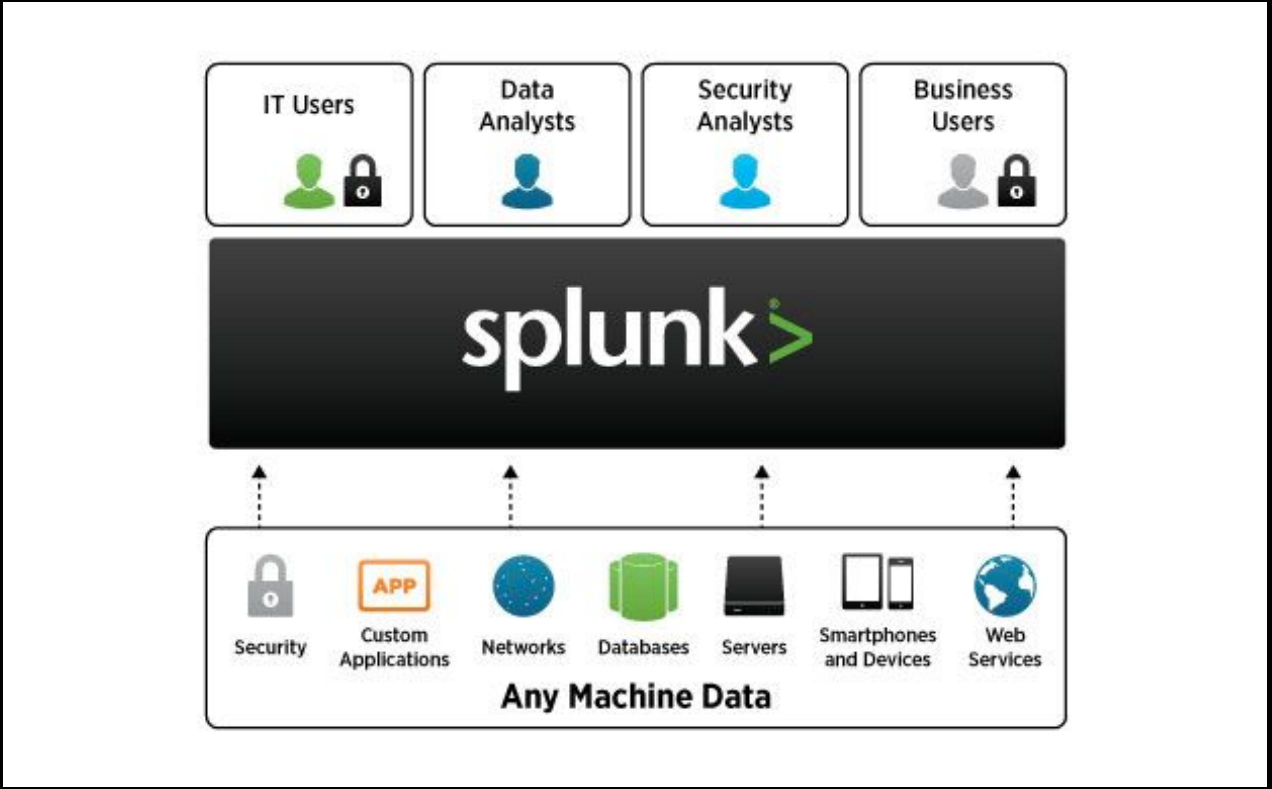
splunk>

Who are we

You may see the machine-generated data created by all of your network equipment as an unmanageable flood of information. But if you Splunk 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® 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 Enterprise Platform



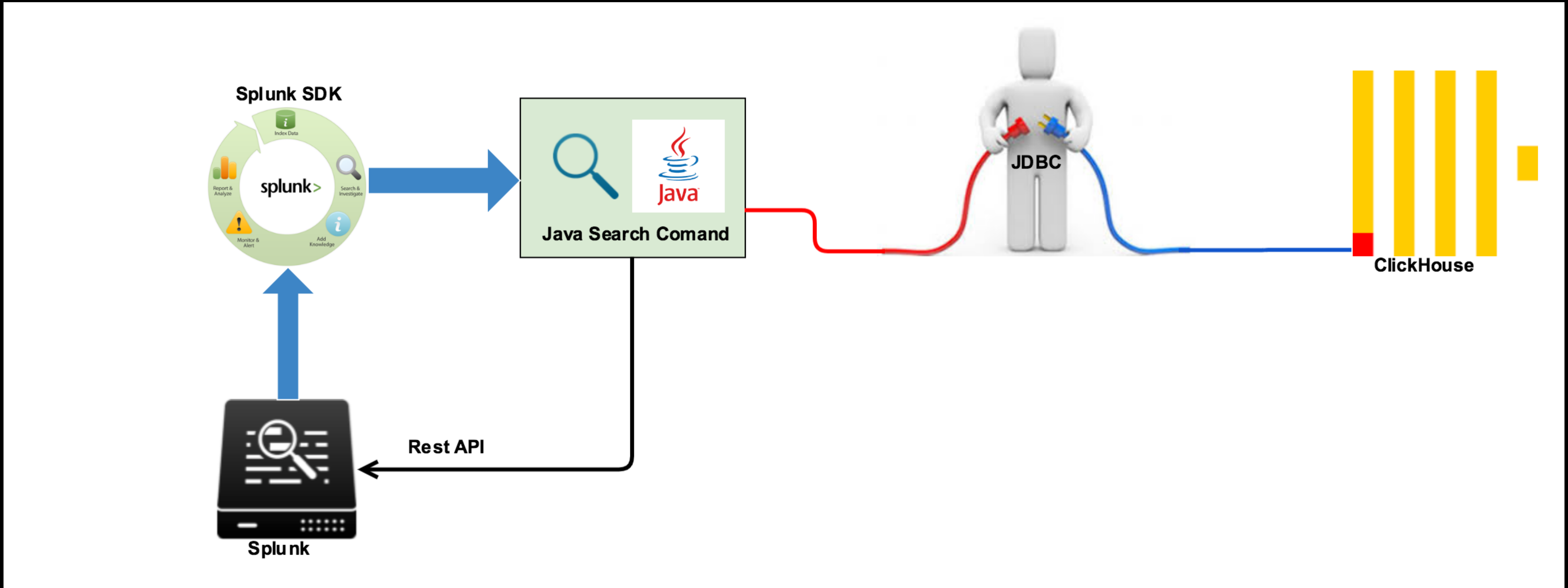
Motivation

- Leverage the lighting 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

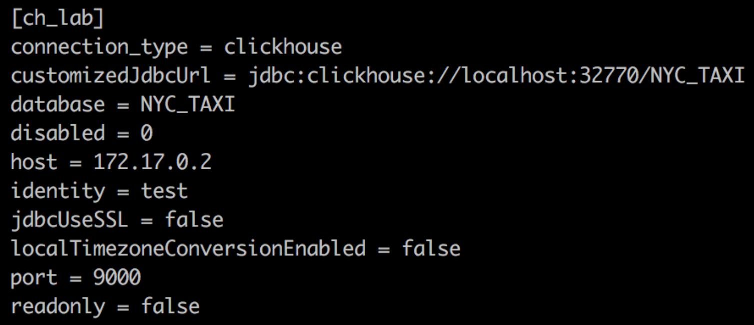
Architecture Design



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

Customized Command

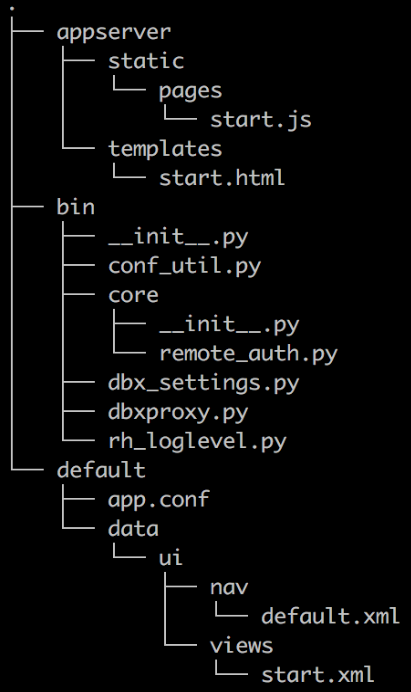
SQL



```
[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
```

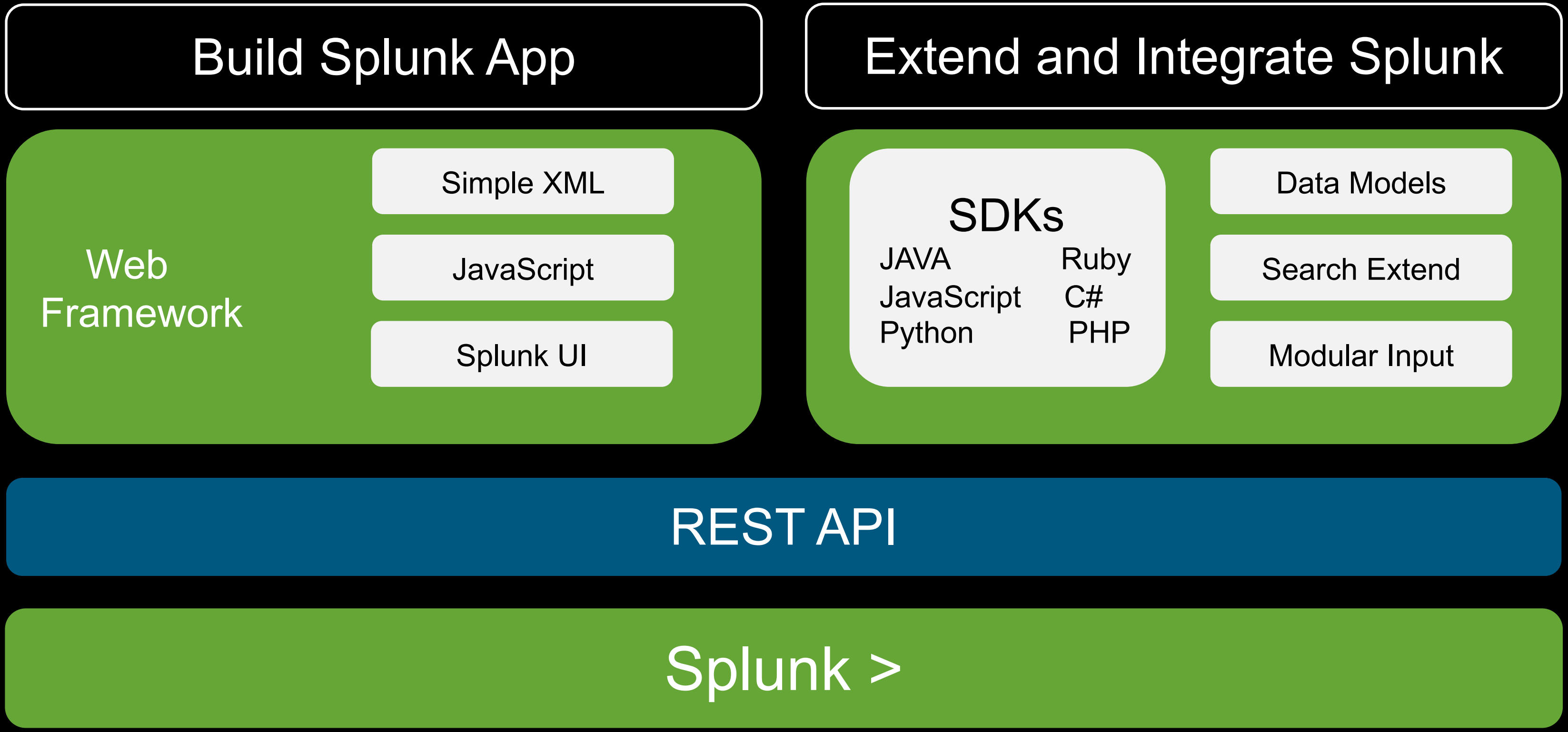
DEMO

- Case Two: Visualization
  - Query data in ClickHouse and use Splunk web framework to visualize



```
.
├── appserver
│   ├── static
│   │   └── pages
│   │       └── start.js
│   └── templates
│       └── start.html
├── bin
│   ├── __init__.py
│   ├── conf_util.py
│   ├── core
│   │   ├── __init__.py
│   │   └── remote_auth.py
│   ├── dbx_settings.py
│   ├── dbxproxy.py
│   └── rh_loglevel.py
└── default
    ├── app.conf
    └── data
        └── ui
            ├── nav
            │   └── default.xml
            └── views
                └── start.xml
```

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 >

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

Thank you

Q & A

splunk> listen to your data