

Installing Logstash



JP Toto

INFRASTRUCTURE DEVELOPER

@jptoto

<http://jptoto.jp>

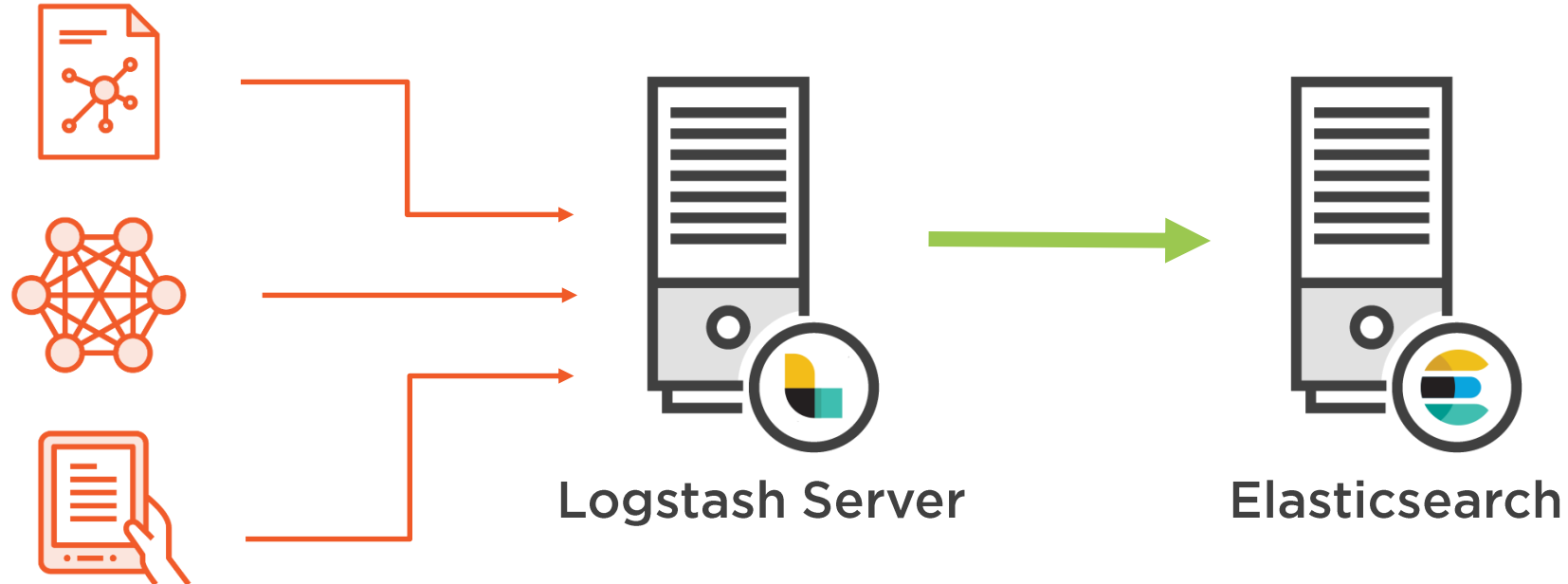


Logstash Is a Data Collection Engine

1. Ingest

2. Enhance or modify

3. Forward



Logstash Configuration

```
input {  
}
```



Where is data coming from?
Logs? Beats?

```
filter {  
}
```



How should we parse the
data? Ignore some? Modify
any?

```
output {  
}
```



Where should we store the
logs? Back end?
Elasticsearch?



Logstash Plugins



Out of the box can read apache logs, log4j files, Windows Event log, and more...

Included filters can read raw text, parse csv, or look up geo/location information by IP address, or reading json

Dozens of filters are included by default



Logstash Filters

grok filter

geoip filter

93.114.45.13 - - [04/Jan/2015:05:14:33 +0000] "GET /images/web...



Geoip Filter

93.114.45.13 - - [04/Jan/2015:05:14:33 +0000] "GET /images/web...

↓
grok filter

↓
93.114.45.13

↓
geoip filter

→

```
"geoip" : {  
  "timezone" : "America/New_York",  
  "ip" : "93.114.45.13",  
  "latitude" : 42.9864,  
  "continent_code" : "NA",  
  "city_name" : "Buffalo",  
  ..  
  "region_name" : "New York",  
  "location" : [  
    -78.7279,  
    42.9864  
  ],  
  "postal_code" : "14221",  
  "longitude" : -78.7279,  
  "region_code" : "NY"  
}
```



Demo



Let's create our Logstash server

Ubuntu Linux Server

Located in US EAST



Summary



Logstash Pipelines and how they will help us

Built a Logstash server and tested the data flow through to Elasticsearch

Next: Kibana

