Visualizing with Kibana

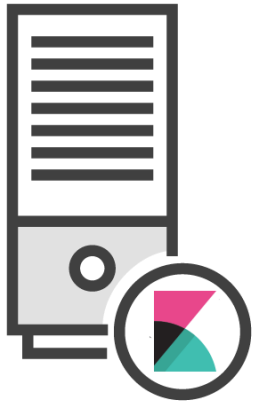
JP Toto
INFRASTRUCTURE DEVELOPER

@jptoto http://jptoto.jp

Almost Complete

Elasticsearch

Logstash

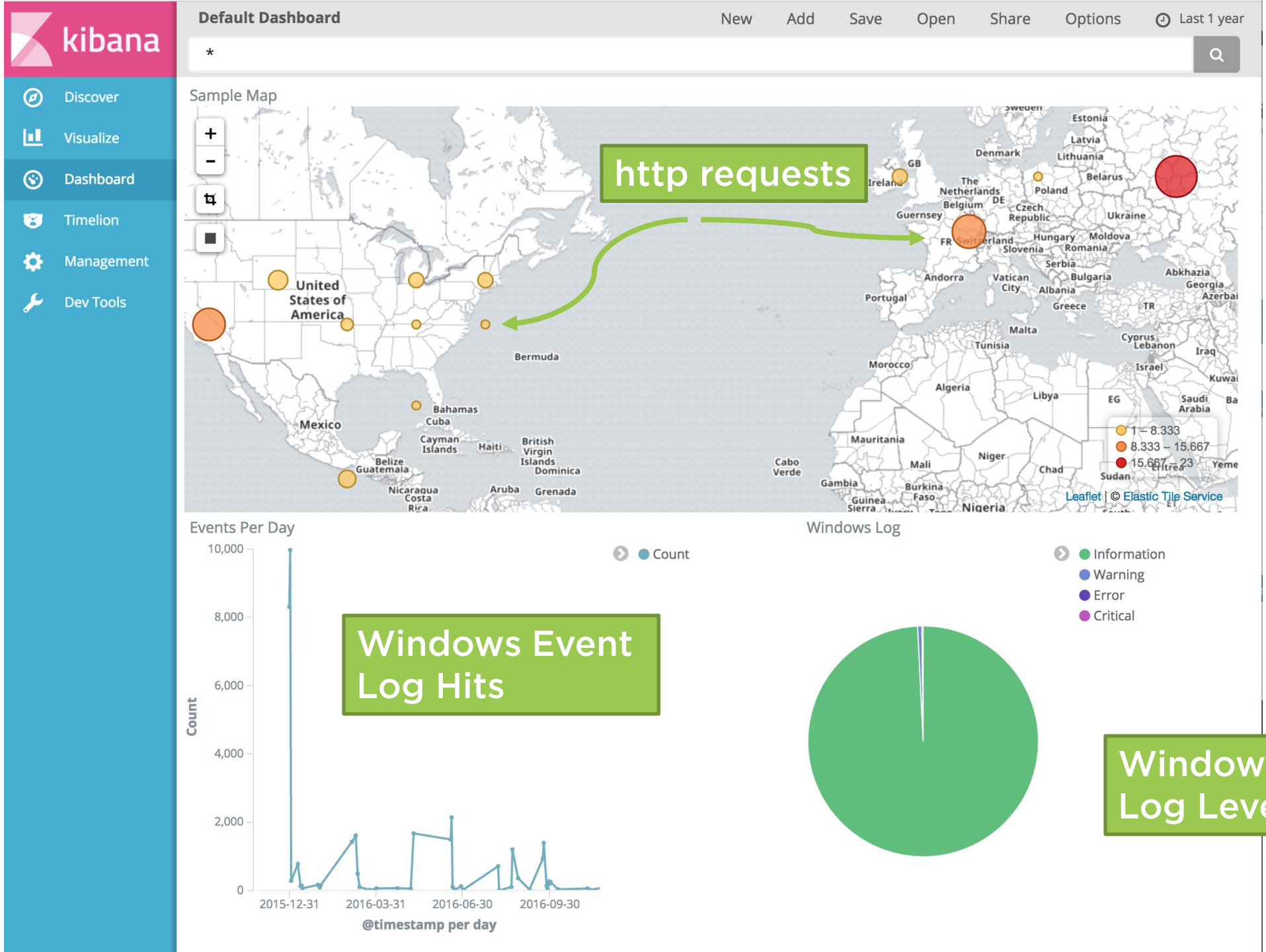


Kibana

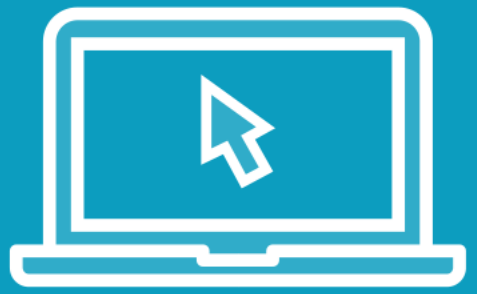
General graphing and visualization tool written in Node.js

Free, works great with Elasticsearch, includes a ton of visualization options and widgets

Easy to create useful dashboards and share them with coworkers


kibana
Default Dashboard
New
Add
Save
Open
Share
Options
Last 1 year
*
Discover
Visualize
Dashboard
Timelion
Management
Dev Tools
Sample Map
http requests
United States of America
Bermuda
Bahamas
Cuba
Mexico
Cayman Islands
Haiti
British Virgin Islands
Dominica
Belize
Guatemala
Nicaragua
Costa Rica
Aruba
Grenada
Cabo Verde
Portugal
Andorra
Vatican City
Albania
Greece
Malta
Tunisia
Morocco
Algeria
Libya
Mauritania
Mali
Niger
Chad
Sudan
Nigeria
Gambia
Burkina Faso
Guinea
Sierra
Ireland
GB
Denmark
Estonia
Latvia
Lithuania
Belarus
Poland
The Netherlands
Belgium
DE
Guernsey
Czech Republic
Ukraine
FR
Switzerland
Hungary
Moldova
Slovenia
Romania
Serbia
Bulgaria
Abkhazia
Georgia
Azerbaijan
Cyprus
Lebanon
Iraq
Israel
Kuwait
Saudi Arabia
EG
TR
1 – 8.333
8.333 – 15.667
15.667 – 23
Leaflet | © Elastic Tile Service
Events Per Day
Count
10,000
8,000
6,000
4,000
2,000
0
2015-12-31
2016-03-31
2016-06-30
2016-09-30
@timestamp per day
Windows Event Log Hits
Windows Log
Information
Warning
Error
Critical
Windows Event Log Level

Demo



Installing Kibana on Ubuntu is pretty easy

Elastic company maintains .deb packges for Debian-based systems

Installed and configured Kibana

Kibana will be our primary view into the log data

Next: Configuring client servers