Chasing the ELK

Intro to ELK Stack

PJ Hagerty
pj@devrelate.io
@aspleenic | @devrelate

What is ELK Stack?

We start with the parts. ElasticSearch, Logstash and Kibana. Three elements that came from the brilliant minds at Elastic - a company dedicated to making great Open Source Software for the benefit of the wider world.

ElasticSearch

ElasticSearch was original built as a scalable, RESTful search solution. As we all know, just because something starts off as one thing doesn't mean that's the way the community will chose to use it. As part of the ELK stack ElasticSearch acts as an engine to search and support multi-tenancy.

Logstash

Logstash is a tool for log data intake, processing, and output. This includes virtually any type of log that you manage: system logs, webserver logs, error logs, and app logs. As administrators, we know how much time can be spent normalizing data from disparate data sources.

Kibana

Kibana is your log-data dashboard. Get a better grip on your large data stores with point-and-click pie charts, bar graphs, trendlines, maps and scatter plots. You can visualize trends and patterns for data that would otherwise be extremely tedious to read and interpret. Eventually, each business line can make practical use of your data collection as you help them customize their dashboards.

The Extra Ingredient

None of this is possible without the cloud. Whether you are mixing your own on a private cloud solution or using a public service like AWS, the cloud is a key piece to making a monitoring solution.

Hard to Port

No mater which cloud solution you start with, private or public, one of the keys to success is opening ports for info to travel - ElasticSearch, we will need Port 9200 available via TCP. Similarly, we will need to open port 5601 for Kibana for function properly.

Getting Started

```
$ sudo apt-get install default-jre

# Installs java and ensures we are using an up to date version.
```

Regardless of where you put your ELK stack - you'll need a few outside components to ensure everything works as expected. Java 8 is the key thing we've seen people get hung up on when trying to get their ELK stack setup. Run a check to make sure you have at least java 8 by running this command.

Installing ElasticSearch

```
1 $ wget -qO - https://packages.elastic.co/GPG-KEY-Elasticsearch | sudo apt-key add -
```

```
1 $ sudo apt-get install Elasticsearch
```

Now we'll actually start getting the ELK stack installed: While SSH'ed into your virtual machine, run this command.
This command fetches the most recent, stable version of Elasticsearch — it but does not install it. For that we need the second command you see here.

Installing ElasticSearch

```
1 $ sudo vi /etc/Elasticsearch/Elasticsearch.yml
```

We need to configure Elasticsearch so that once we have the other portions of the ELK Stack installed, we can communicate with them properly. We will make these changes in this Elasticsearch.yml file

Find the line referring to the network.host portion. It will be commented out. Uncomment the file and make it read network.host “0.0.0.0”. Be sure to save the file before exiting. Restart Elasticsearch to make sure that everything is up to date.

Installing Logstash

```
$ sudo apt-get install apt-transport-https

# This setups installs for logstash in your system

$ echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | sudo tee -a /etc/apt/

# This will establish the source for Logstash

$ sudo apt-get update

$ sudo apt-get install logstash

# Setting up for logstash installation

$ sudo service logstash start

# Start the logstash service so we can start shipping logs
```

Logstash doesn’t have the configuration requirements of ElasticSearch, or Kibana. Simply get the package, and install - no configuration adjustments - plug and play - after running a few of these commands and ensuring the service starts.

Installing Kibana

```
$ echo "deb http://packages.elastic.co/kibana/5.3/debian stable main" | sudo tee -a /etc/apt/sources.list.d/kibana-5.3.x.list
# This will establish the source for Kibana

$ sudo apt-get update
$ sudo apt-get install kibana
# Setting up for Kibana installation
```

Kibana has an installation similar to ElasticSearch. You'll notice there is a theme here as far as how Elastic wants you to setup the pieces of the ELK stack. It wasn't always this way, but we're glad it is now.

Installing Kibana

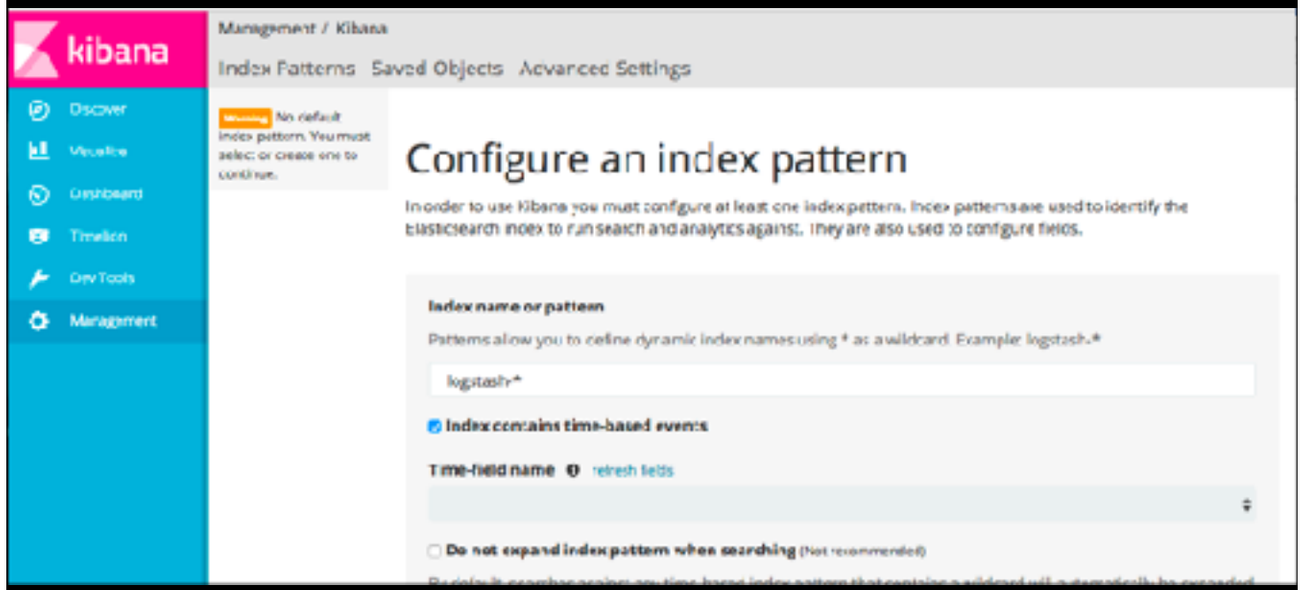
```
$ sudo vi /etc/kibana/kibana.yml
```

Similar to Elasticsearch, Kibana will need some configuration adjustments to work. We'll look at kibana.yml to make these changes.
Find the lines referring to server.port and ensure they say server.port: 5601 and server.host: "0.0.0.0". It should only be necessary to uncomment these lines. Once this is done, you can start the Kibana service.

A Bit about Beats

Beats is a set of data shippers elastic has created for pushing specific types of information to your dashboard once you have your stack setup. These can range from simple things like Filebeat to see what activities are happening on specific files to PacketBeat, Metricbeat and so many more.

Almost There



Once our stack is up and running we should see this screen. We are so close. Now we just need to let Kibana know what we want to see. This is where Beats can combine handy. There are various configurations you can use and it’s always possible to change as your needs change.

The Dashboard

After a minute or two while the system ramps up, collects, and collates the data stream coming in, you'll have a beautiful visualization of what you are hoping to monitor. All in all, this process takes about an hour or two depending on what cloud service you are using and other variables.

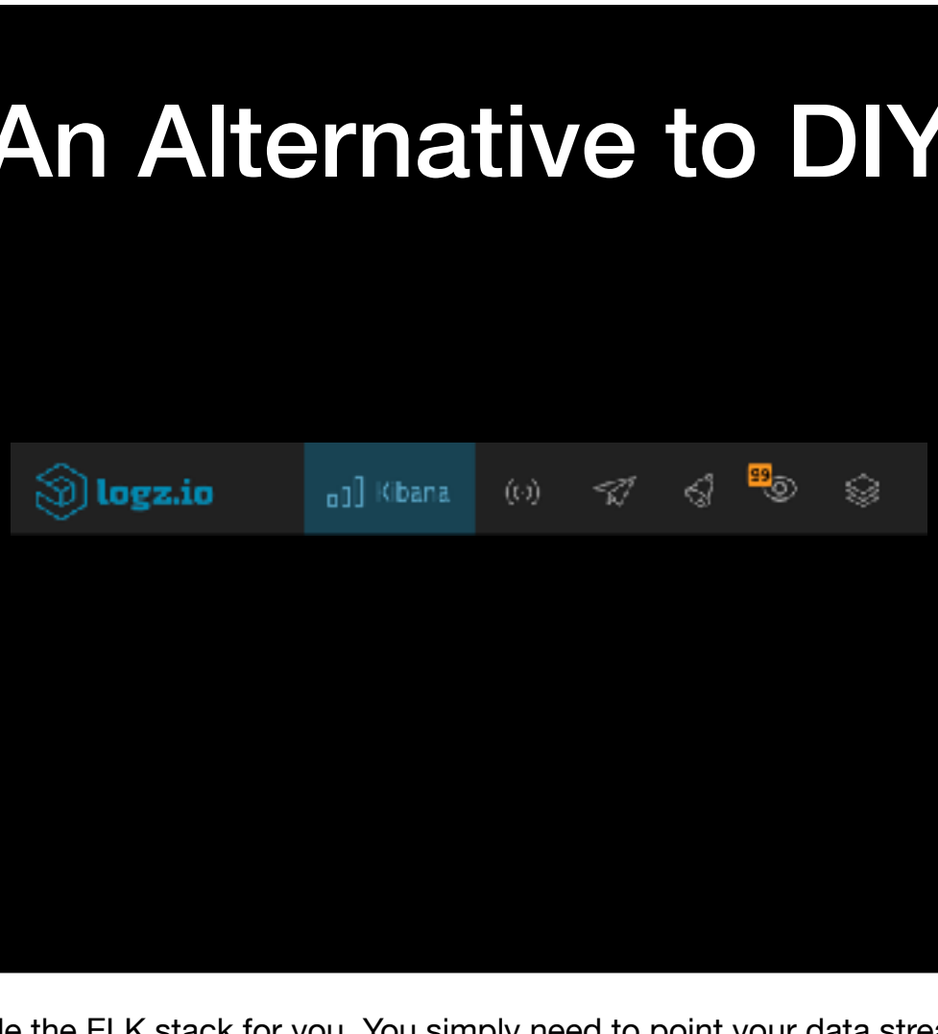
Installation Gotchas

- MAKE SURE YOU USE JAVA 8
- Mind your versioning
- PORTS PORTS PORTS

Maintenance

One of the toughest parts of maintaining the ELK stack is keeping up to date with the latest versions. This can become a full time job as Elastic tends to updates each part of the ELK stack fairly regularly and having all parts on the same version is crucial to a healthy setup.

An Alternative to DIY



There are of course services out there that will provide the ELK stack for you. You simply need to point your data streams in the right direction and get the same output spending only about 5 minutes time. Additionally, you won’t need to maintain the ELK stack, someone can curate that for you.

Thank You

PJ Hagerty | @aspleenic | pj@devrelate.io | @devrelateio