ELASTIC SEARCH, LOGSTASH, KIBANA & BEATS

QUALITY THOUGHT

The leader in Software Training

What is the Elastic Stack?

What is the Elastic Stack?

What is the Elastic Stack?

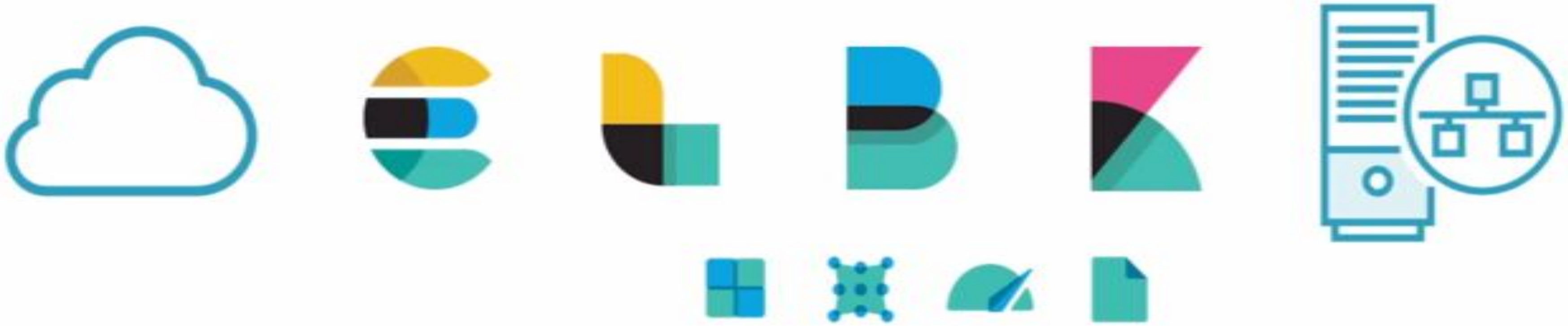
- ✓ Free
- ✓ Open Source
- ✓ Great at full-text searching

Previously Known as the ELK Stack

Elasticsearch

Logstash

Kibana



Elasticsearch Useful for Many Cases

Highly scalable

Built in search, aggregation, and sharding

Used by Microsoft Azure, Wordpress, and Stack Exchange

Your Role Today

DevOps / IT

GLOBOMANTICS

Take monitoring situation from non-existent to fully-fledged enterprise-ready

Web-based monitoring and historical searching

Proactive alerting solution

Elasticsearch

Distributed, fast, highly scalable document database

Created by Shay Banon in 2010

We'll use a simple single node cluster

Logstash

Aggregates, filters, and supplements log data

Forwards altered logs to Elasticsearch

Sending logs directly to Elasticsearch without Logstash can lead to inconsistent data

Kibana

Web-based front-end

Works easily with Elasticsearch for charts, graphs, and visualizing data

Free from the Elastic company

Beats

Small, lightweight utilities for reading logs from a variety of sources. Usually sends data to Logstash

Filebeat: Text log files

Metricbeat: OS and applications

Packetbeat: Network monitoring

Winlogbeat: Windows Event log

Libbeat: Write your own

Alerting

Helps track conditions based on Elasticsearch data

Continually monitors log data for pre-configured conditions

Send notifications to email, Slack, Hipchat, and PagerDuty out of the box

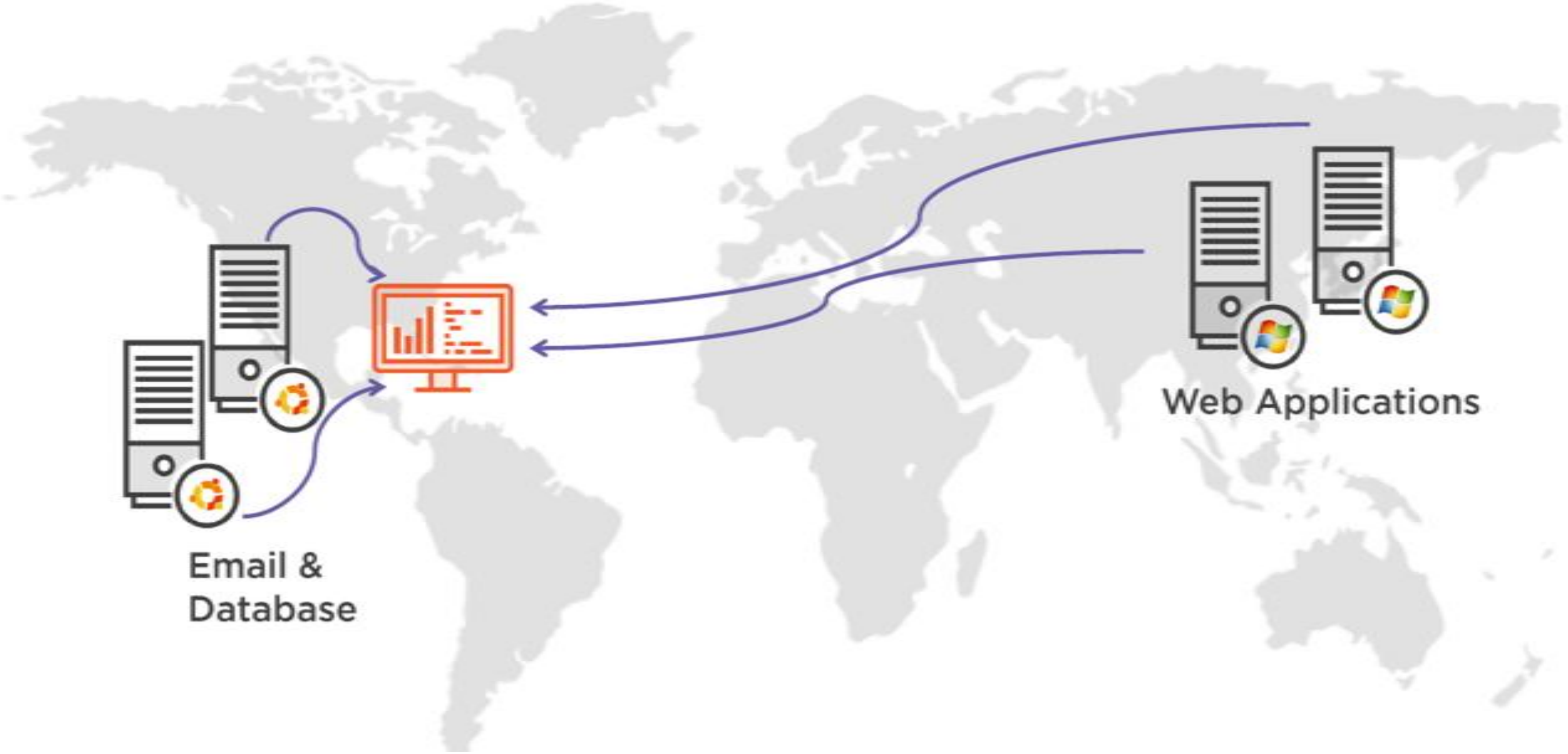
Globomantics Is Worldwide

Disk

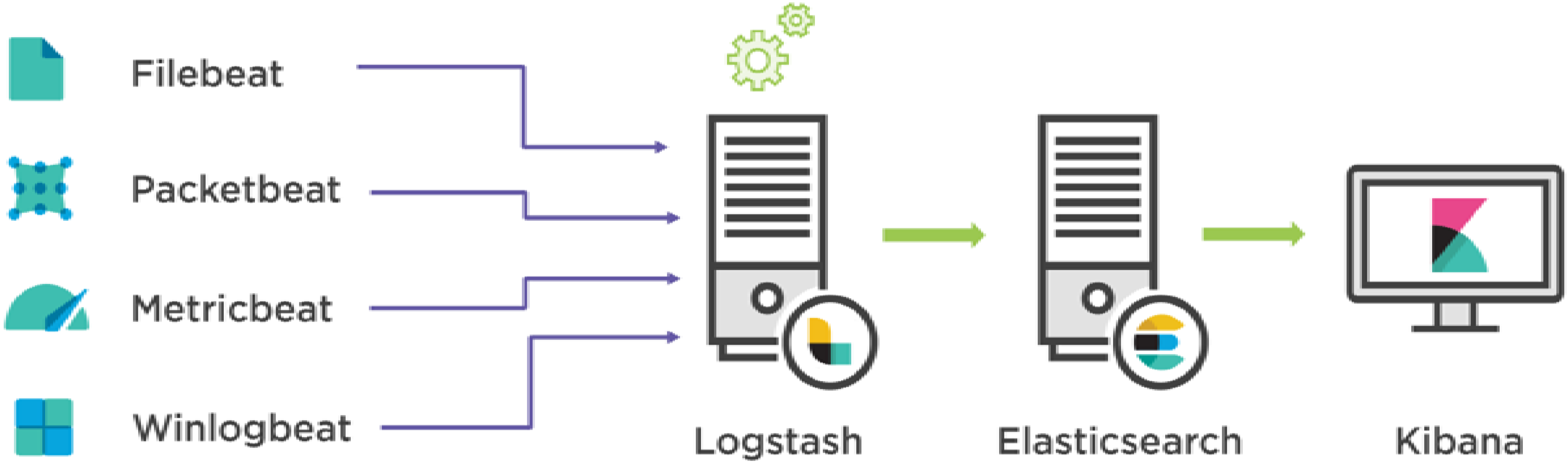
CPU & RAM

Applications

Network


Email &
Database
Web Applications

Beats



Filebeat

Packetbeat

Metricbeat

Winlogbeat

Logstash

Elasticsearch

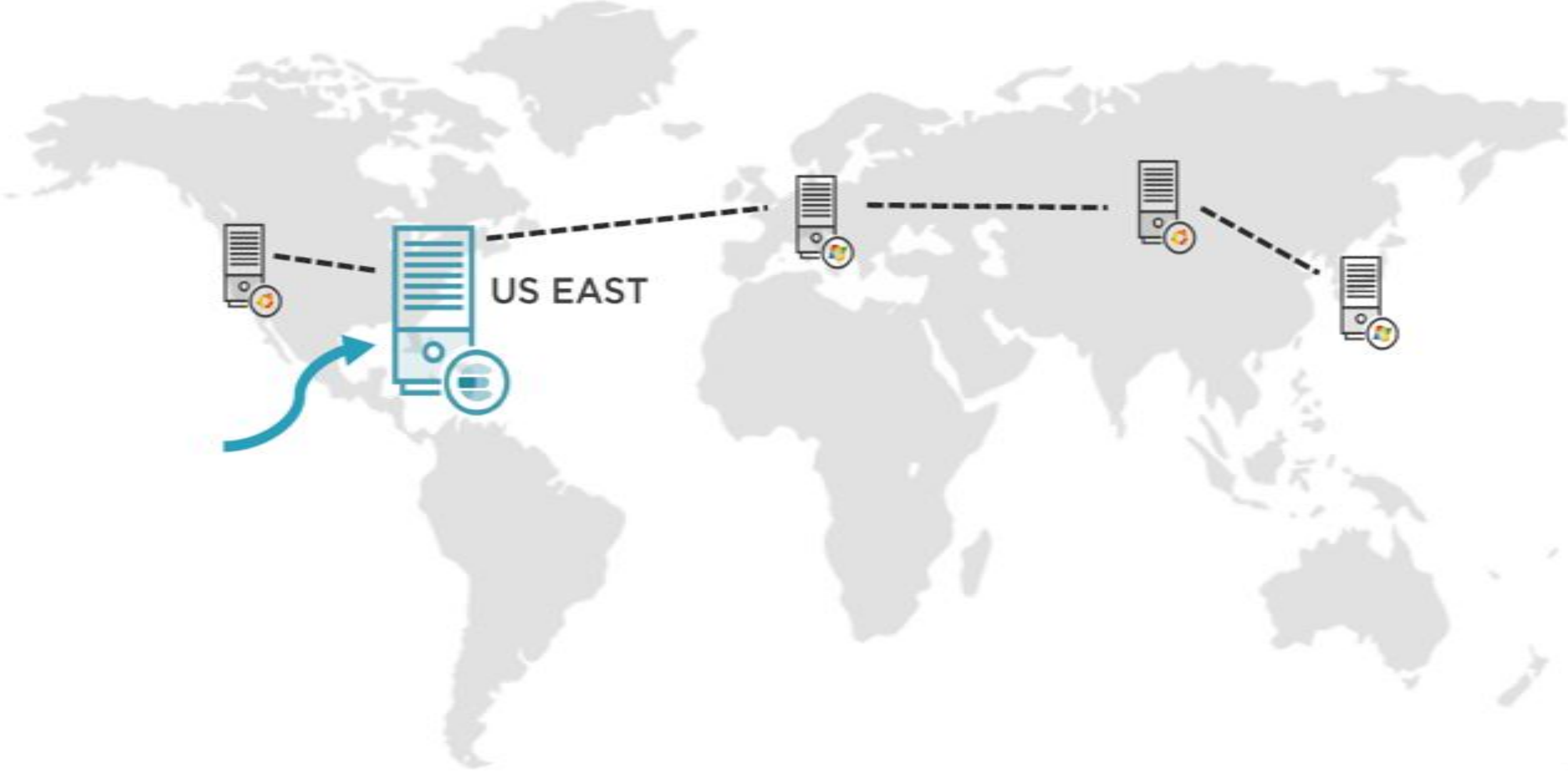
Kibana

System Buildout

Start from the back, work forward

Usually Elasticsearch clusters comprise many nodes

We're keeping things simple with one Elasticsearch node


US EAST

Demo

What kind of OS should we use? Elasticsearch runs fine on Linux & Windows

We’re going to choose Linux and use distribution packages

Ubuntu 16.10 Server Edition

We’ll also demonstrate a Windows install

Installing Elastic Search

- Once the ubuntu 16 Server is up, install java using

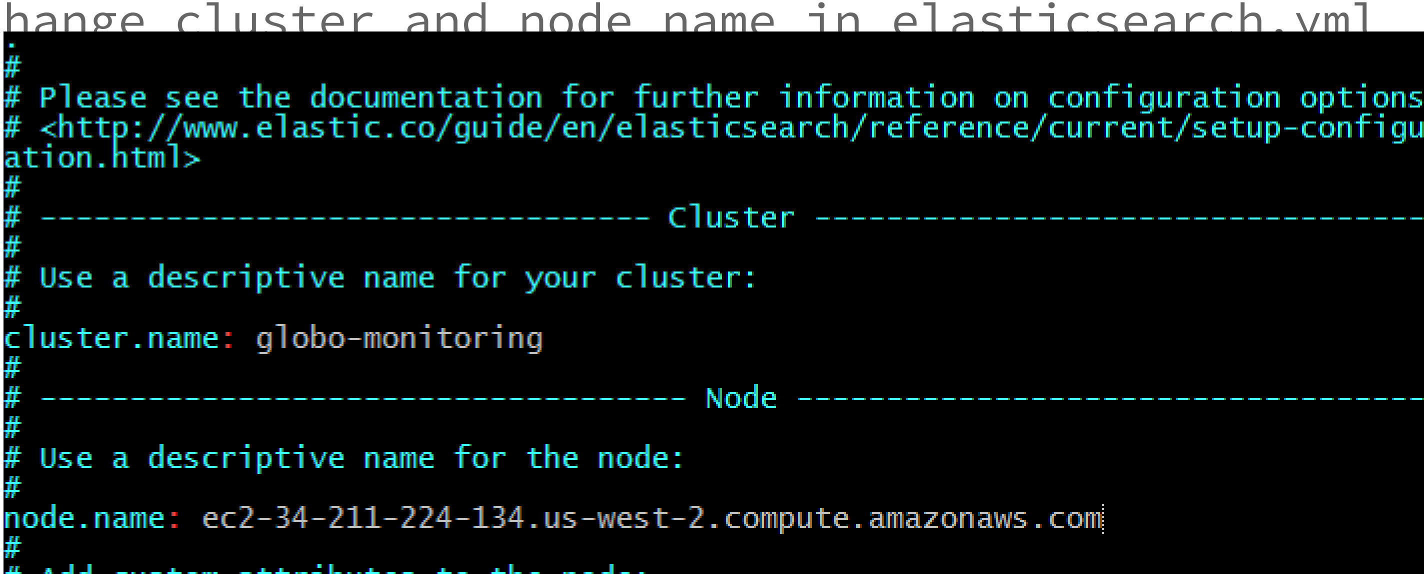
“apt-get install openjdk-8-jre-headless

- Create a directory and download elastic search package

```
 mkdir pkg

cd pkg

 wget
https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-5.0.0.deb
```

Installing Elastic Search (Contd)

- Execute command "dpkg -i elasticsearch-5.0.0.deb"
- Elastic search configuration file is present at "/etc/elasticsearch/elasticsearch.yml"
- Change cluster and node name in elasticsearch.yml



```
.
#
# Please see the documentation for further information on configuration options
# <http://www.elastic.co/guide/en/elasticsearch/reference/current/setup-configu
ation.html>
#
# ---------------------------------- Cluster ----------------------------------
#
# Use a descriptive name for your cluster:
#
cluster.name: globo-monitoring
#
# ------------------------------------ Node ------------------------------------
#
# Use a descriptive name for the node:
#
node.name: ec2-34-211-224-134.us-west-2.compute.amazonaws.com
#
# Add custom attributes to the node:
```

Installing Elasticsearch (Contd)

- Change network.host: <ip address>
- Increase the memory map count by “ sysctl -w vm.max_map_count=262144”
- Start elasticsearch cluster service by “service elasticsearch start”
- Test by executing curl http://<ipadress>:9200
- By default elastic search runs on port 9200
- To start elastic search on boot “systemctl enable elasticsearch”

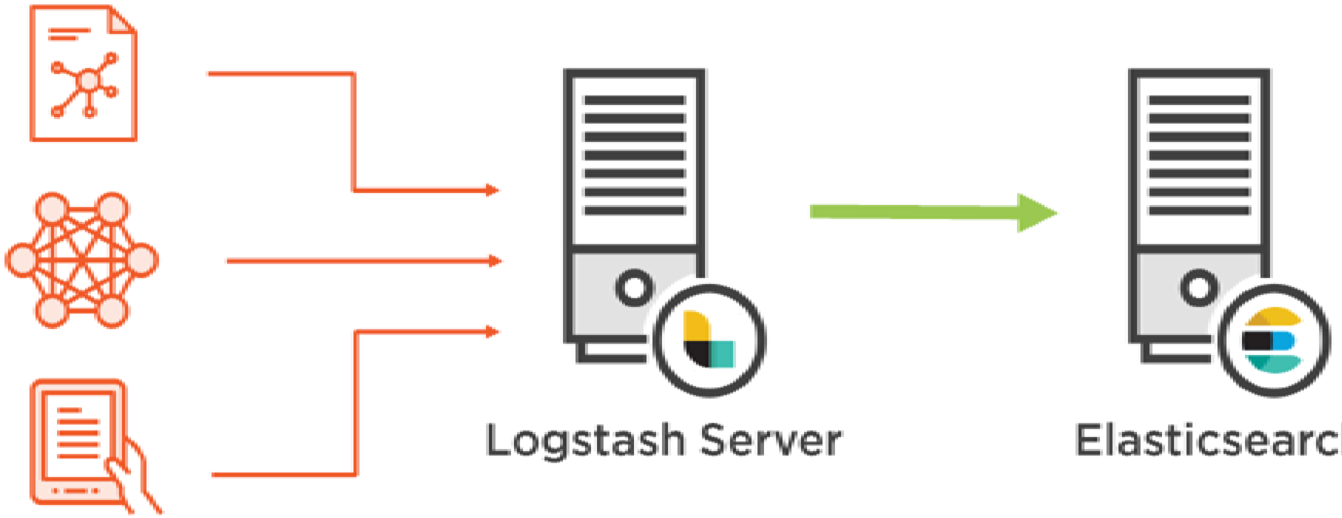
Installing Logstash

Logstash Is a Data Collection Engine

1. Ingest

2. Enhance or modify

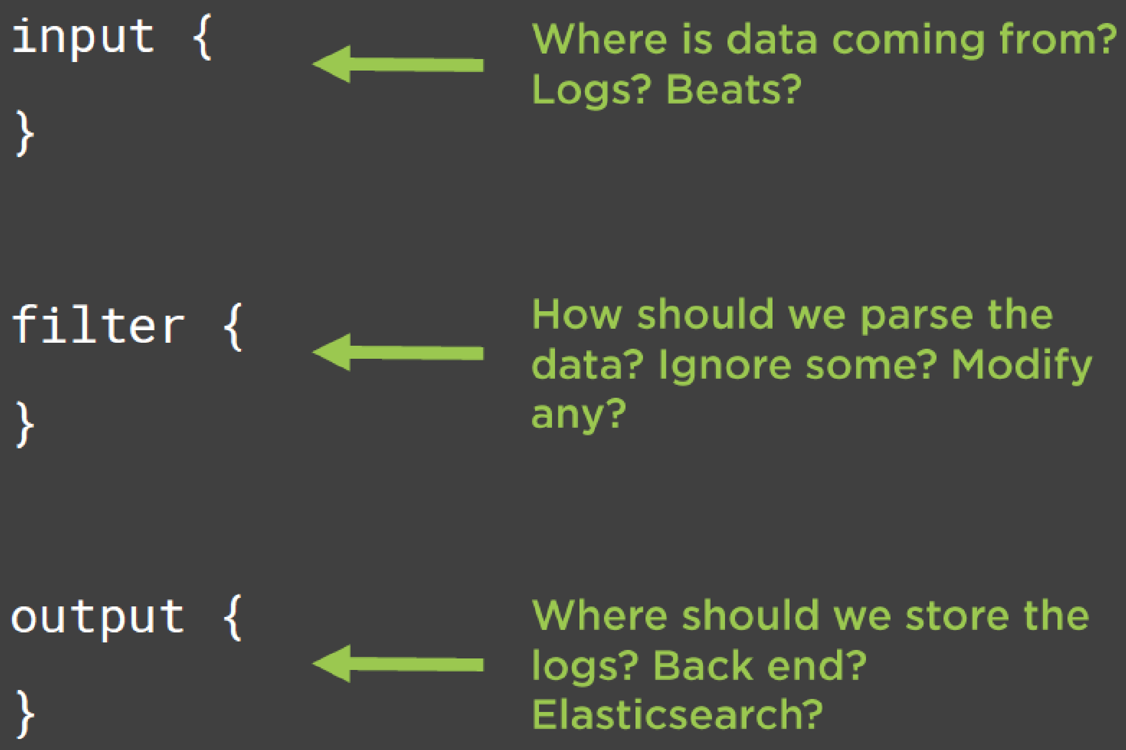
3. Forward



Logstash Server

Elasticsearch

Logstash Configuration



```
input {

}


filter {

}


output {

}
```

Where is data coming from? Logs? Beats?

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

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

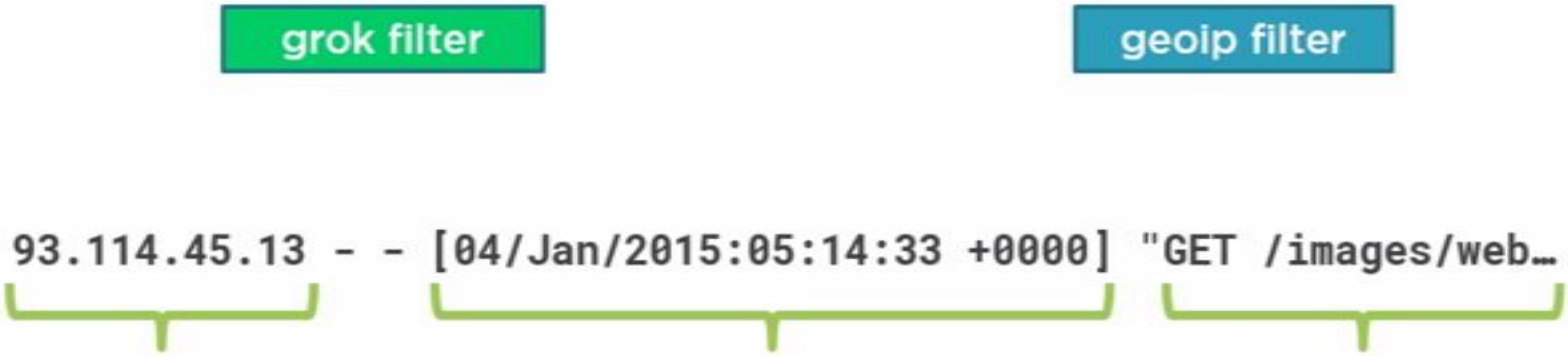
Logstash Plugins

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



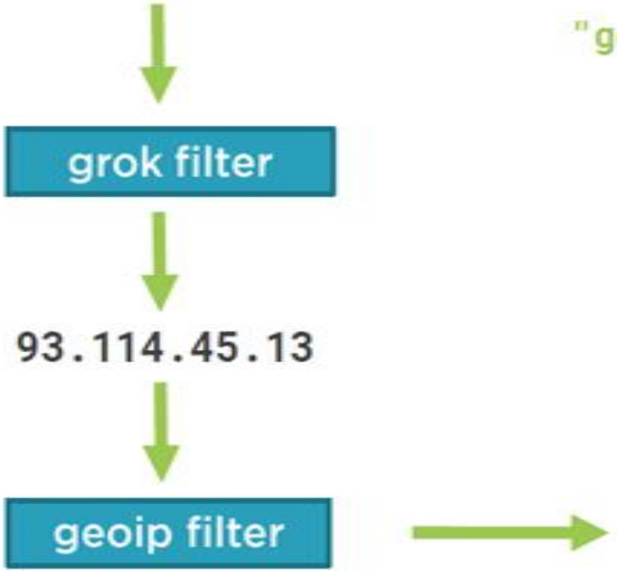
grok filter

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

Install LogStash

- Install java much like elasticsearch installation step
- Run the following command to import the Elasticsearch public GPG key into apt

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

- Create the Elasticsearch source list:

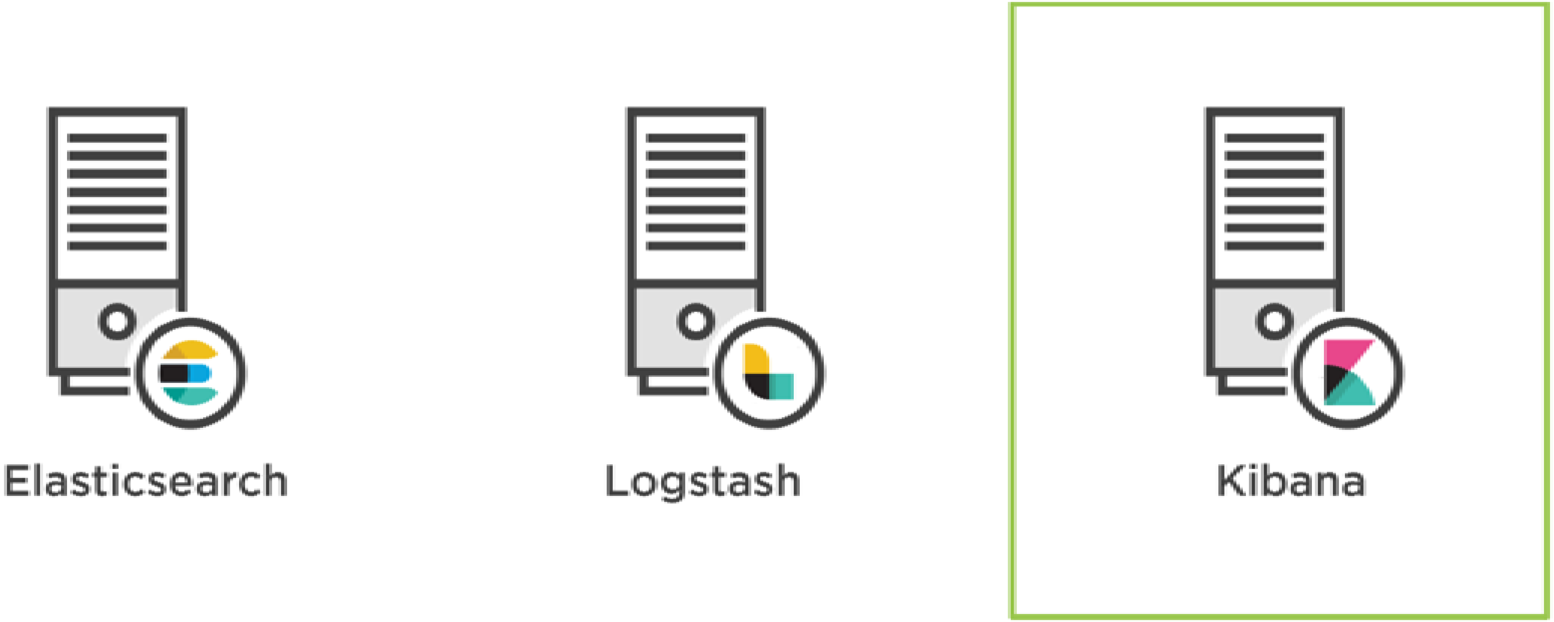
```
echo "deb https://artifacts.elastic.co/packages/5.x/apt
stable main" | sudo tee -a
/etc/apt/sources.list.d/elasticsearch-5.x.list
```

Install LogStash (contd..)

- Execute “apt-get update && apt-get install logstash”
- Logstash is stored in /usr/share/logstash and move to this directory using cd
- Now execute this command “bin/logstash -e "input { stdin {} } output { stdout {} }"

Visualizing with Kibana

Almost Complete



Elasticsearch

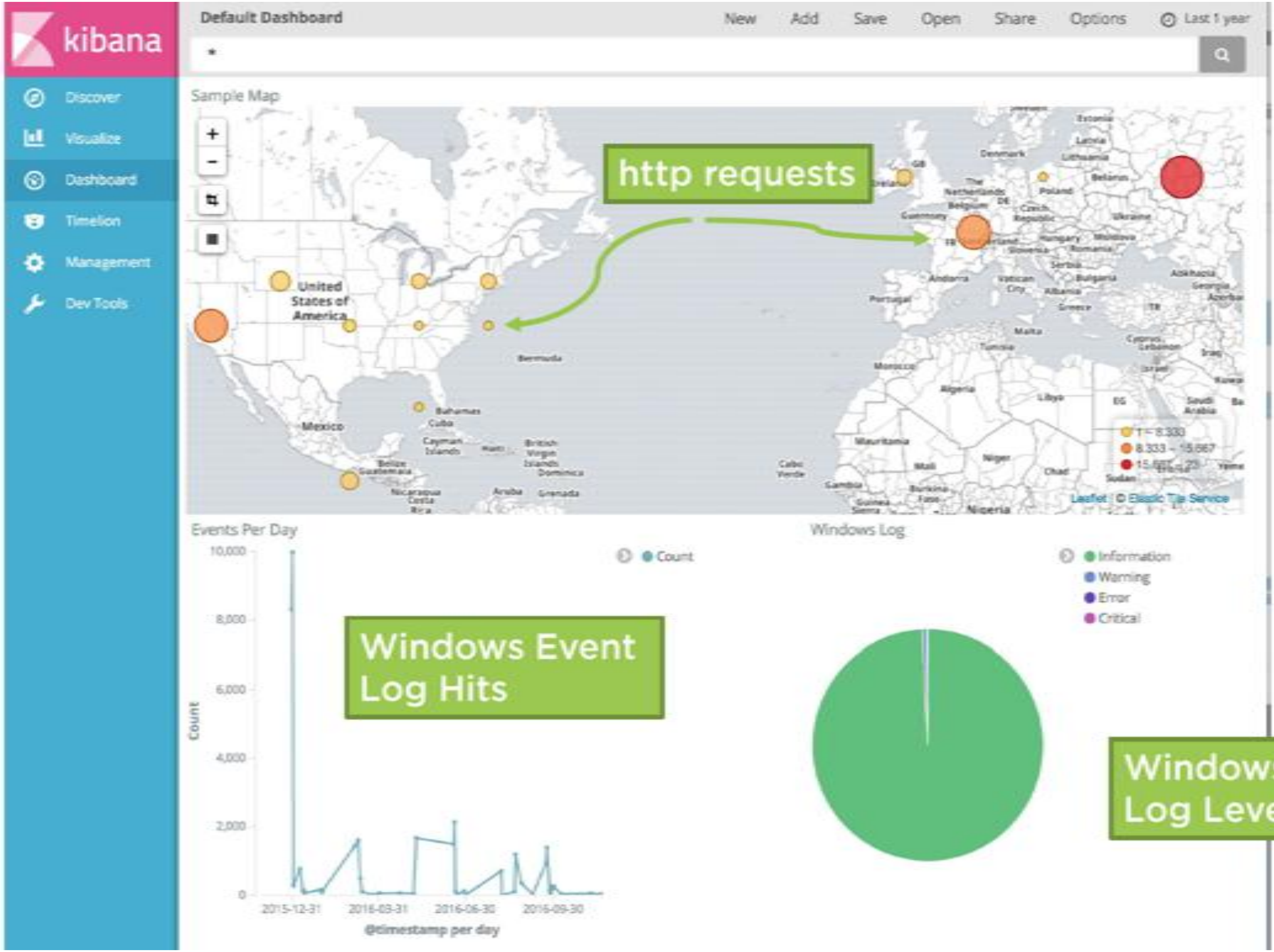
Logstash

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



http requests

Windows Event Log Hits

Windows Event Log Level

Demo

Installing Kibana on Ubuntu is pretty easy

Elastic company maintains .deb packges for Debian-based systems

Installing Kibana

- Run the following command to import the Elasticsearch public GPG key into apt

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

- Create the Elasticsearch source list:

```
echo "deb https://artifacts.elastic.co/packages/5.x/apt
stable main" | sudo tee -a
/etc/apt/sources.list.d/elasticsearch-5.x.list
```

Installing Kibana (contd..)

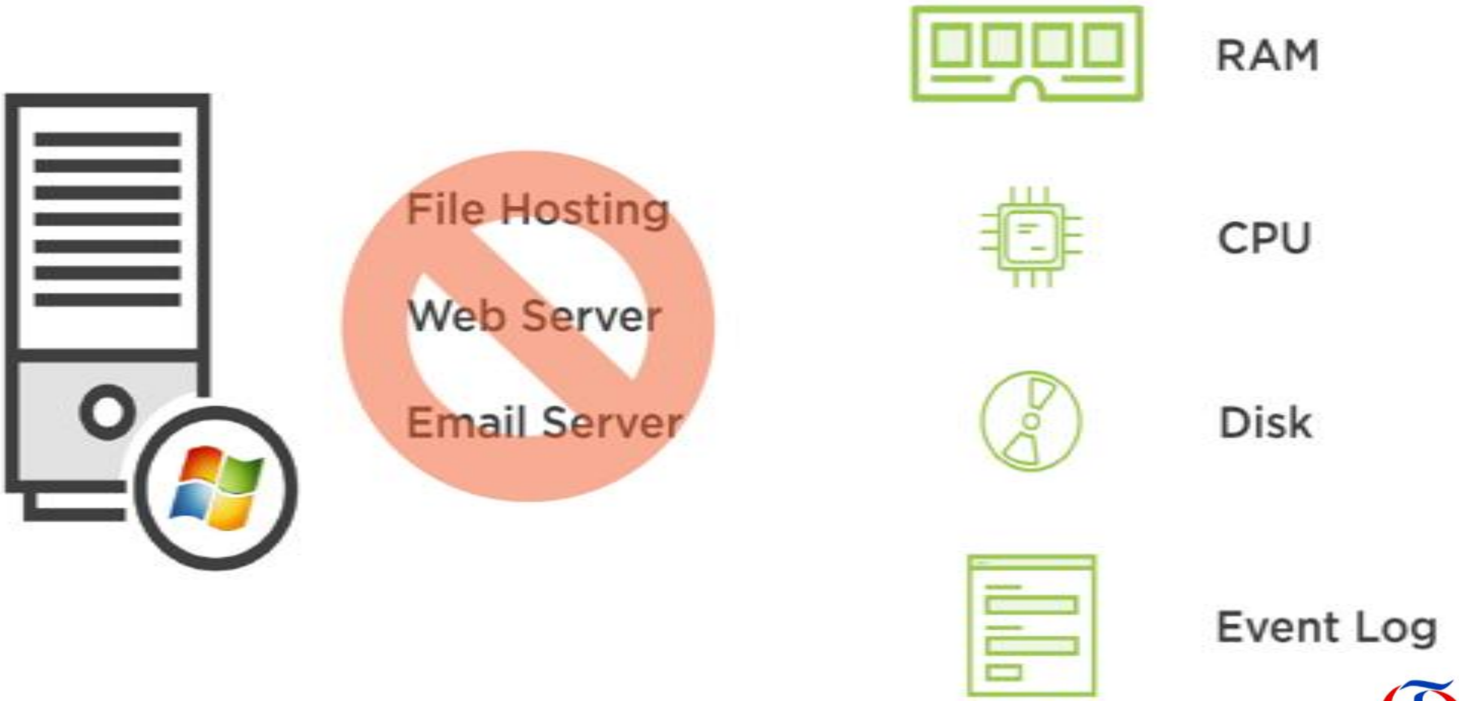
- Execute “apt-get update && apt-get install kibana”
- Make changes in configuration at /etc/kibana/kibana.yml as mentioned below

```
server.host:<ipaddress>

Server.name: <hostname>

Elasticsearch.url: <elasticsearchurl>
```

- Execute “service kibana start”
- Test the kibana by accessing

Instrumenting Windows Servers

Instrumenting Windows Servers



File Hosting

Web Server

Email Server

RAM

CPU

Disk

Event Log

A Complete Picture

Winlogbeat

Windows Event Log

- Reading
- Filtering
- Enhancing
- Forwarding

Metricbeat

All-purpose system & statistics

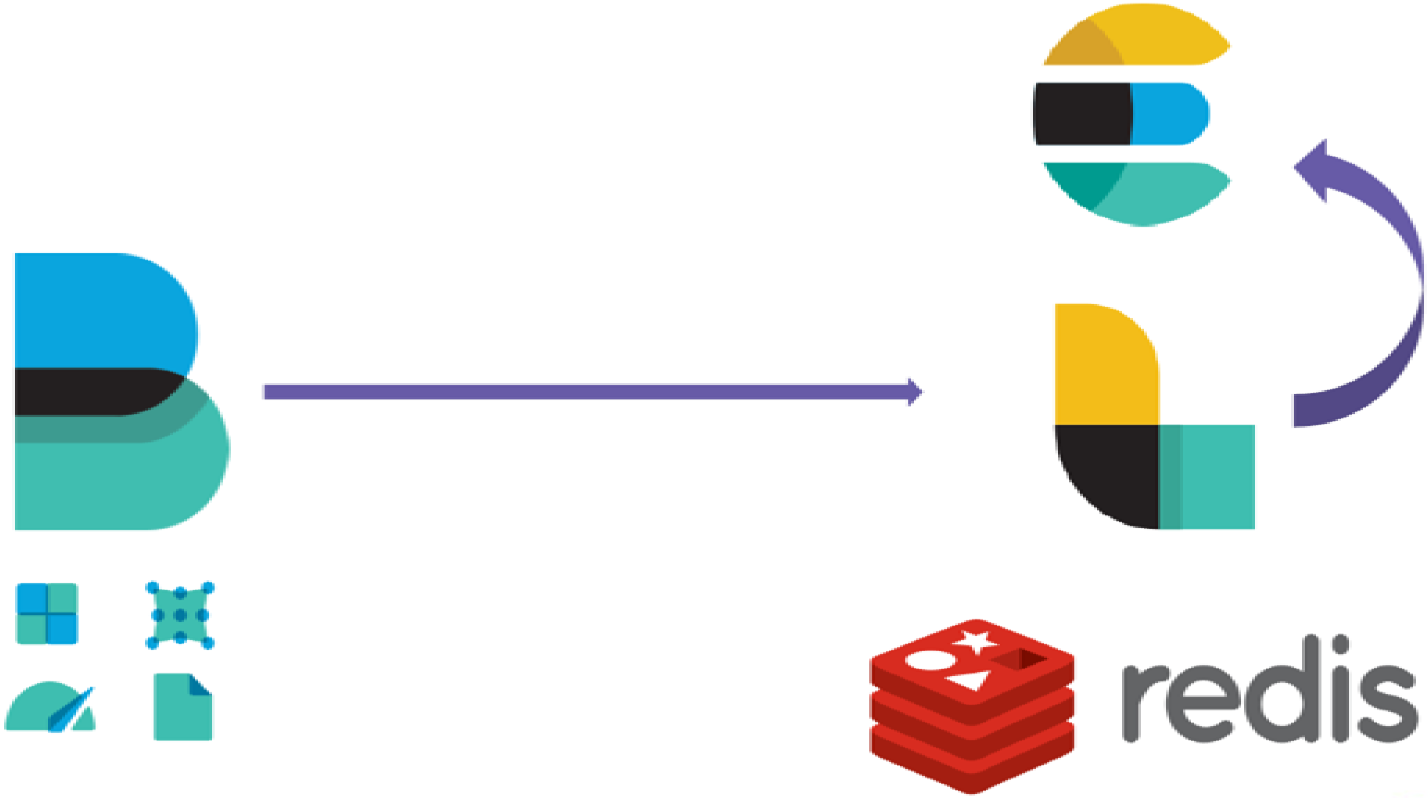
Broken into modules

- Apache
- HAProxy
- MongoDB
- MySQL
- NginX
- PostgreSQL
- Redis
- Zookeeper
- System logs

Go programs are static binaries, no need for JVM or other runtimes

Can be “cross-compiled” to work on Windows, Linux, macOS, and BSD

Usually pretty small and lightweight – great for system utilities


redis

Usually large companies have dozens, hundreds, or even thousands of servers

For our purposes, we’re going to use two Windows web servers and one Windows file server

Will keep the data diverse enough for our demonstrations

Demo

Download and unpack Winlogbeat

Configure it to use logstash and add some custom fields and data

Set it up to run as a Windows service

INSTALLING WINLOGBEAT

- Download winlogbeat file from elastic site
- Extract zip file and change the following in winlogbeat.yml

```
tags: ["us-east-1"]

fields:

  globo_environment: production
```

Enable logstash configuration.

INSTALLING WINLOGBEAT (CONTD..)

- From powershell install winlogbeat template by using following command

```
“Invoke-WebRequest -Method PUT -InFile
.\winlogbeat.template.json -Uri
http://<elasticsearchserver>:9200/_template/winlogbeat”
```

- From Powershell install winlogbeat service using following command “.\install-service-winlogbeat.ps1”

- Start service using start-service winlogbeat

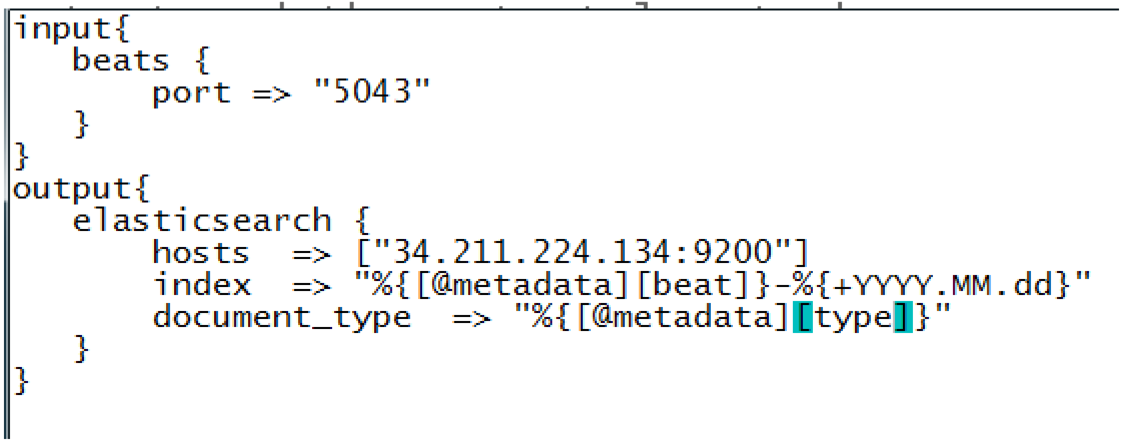
Demo

Configure Logstash to read Beats data and forward it to Elasticsearch

Configure Logstash server for winlogbeat

- Login into logstash server and navigate to /etc/logstash/conf.d

- Create a file with name “beats.conf” and following c



```
input{
   beats {
        port => "5043"
   }
}
output{
   elasticsearch {
        hosts   => ["34.211.224.134:9200"]
        index   => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"
        document_type   => "%{[@metadata][type]}"
   }
}
```

Instrumenting Linux Servers

Beats for Linux

Metricbeat

RAM

CPU

Disk

Filebeat

Filebeat

Built for consuming and shipping text-based logs and data

Outputs to Elasticsearch or Logstash

Most Linux logs are text-based so it’s a good fit for monitoring

Demo

Download, install, and configure Filebeat

Setup Filebeat to read syslog files and forward to Logstash

Add a filter configuration to Logstash for syslog

Installing File BEAT

- Create the ubuntu instance

```
Curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-5.4.1-amd64.deb
```

- dpkg -i filebeat-5.4.1-amd64.deb
- We will now configure filebeat to read syslog from /var/log/syslog
- Upload template by curl -XPUT ‘http://<elasticsearch>:9200/_template/filebeat’ -d /etc/filebeat/filebeat.template.json

Installing File Beat (ContD..)

- Configure Logstash from configuration @ https://s3-us-west-2.amazonaws.com/qt-elastic-softwares/Configuration/LinuxSyslogfilebeat/beats.conf in /etc/logstash/conf.d and restart logstash
- Create visualization in kibana

For Rest of configurations

https://s3-us-west-2.amazonaws.com/qt-elastic-softwares/Configuration/centralized-logging-elastic-stack.zip