Bro + ELK

BroCon 2015

Michael Pananen

Vigilant Technology Solutions

www.vigilantnow.com

mpananen@vigilantnow.com

Twitter: @panaman13

https://github.com/panaman/brocon2015

ELK

- Elasticsearch
- Logstash
- Kibana

Elasticsearch

Recommended Hardware

- Medium size machines
- Dual 8 core CPU's
- 64G Memory
- Fastest hard drive on the planet

ELK Server Packages – CentOS 7

https://www.elastic.co/downloads

- elasticsearch
- logstash
- **java**-1.8.0-openjdk – needed by elasticsearch
- httpd – needed by Kibana
- mod_ssl – needed by Kibana
- GeoIP – needed by Logstash

Simple Install

1. Install Java

sudo yum install java-1.8.0-openjdk

2. Download and install Elasticsearch

curl -O https://download.elastic.co/elasticsearch/elasticsearch/elasticsearch-1.7.1.noarch.rpm

sudo yum install elasticsearch-1.7.1.noarch.rpm

3. Download and install Logstash

curl -O https://download.elastic.co/logstash/logstash/packages/centos/logstash-1.5.2-1.noarch.rpm

sudo yum install logstash-1.5.2-1.noarch.rpm

4. Install GeoIP and update it

sudo yum install GeoIP

sudo geoipupdate

5. Install Apache and mod_ssl

sudo yum install httpd

sudo yum install mod_ssl

Elasticsearch Config

/etc/elasticsearch/elasticsearch.yaml

```
cluster.name: panapad
node.name: deathstar
node.master: true
node.data: true
# This shard count is not recommended for production
index.number_of_shards: 1
index.number_of_replicas: 0
node.data.
path.data: /data/esdata
path.logs: /data/eslogs
```

Memory

In production environments it is recommended to disable swap

/dev/mapper/centos-swap swap swap defaults 0 0

/etc/sysconfig/elasticsearch

Set ES_HEAP_SIZE to 50% of available RAM, but no more than 31g

ES_HEAP_SIZE=31g

Shards & Indices

Shard = a single Lucene instance

Index = logstash-2015.08.05 = primary and replica shards if applicable

Multiple data nodes

- Multiple primary shards spread across multiple machines to scale the load
- Replica shards for redundancy and search speed

Elasticsearch - Four Data Node Cluster

Two Primary Shards and 1 replica

ESDATANODE1

Primary Shard

ESDATANODE2

Replica Shard

ESDATANODE3

Primary Shard

ESDATADATA4

Replica Shard

Elasticsearch - Four Data Node Cluster

Two Primary Shards and 1 replica

ESDATANODE1

Primary1 - Logstash-2015.08.05

Replica2 – Logstash-2015.08.04

ESDATANODE2

Replica1 - Logstash-2015.08.05

Primary2 – Logstash-2015.08.04

ESDATANODE3

Primary2 - Logstash-2015-08.05

Replica1 – Logstash-2015.08.04

ESDATADATA4

Replica2 - Logstash-2015.08.05

Primary1 – Logstash-2015.08.04

Reboot?

DISABLE

```
curl -XPUT http://localhost:9200/_cluster/settings -d '{ "transient" :
{ "cluster.routing.allocation.enable" : "none" }}’
```

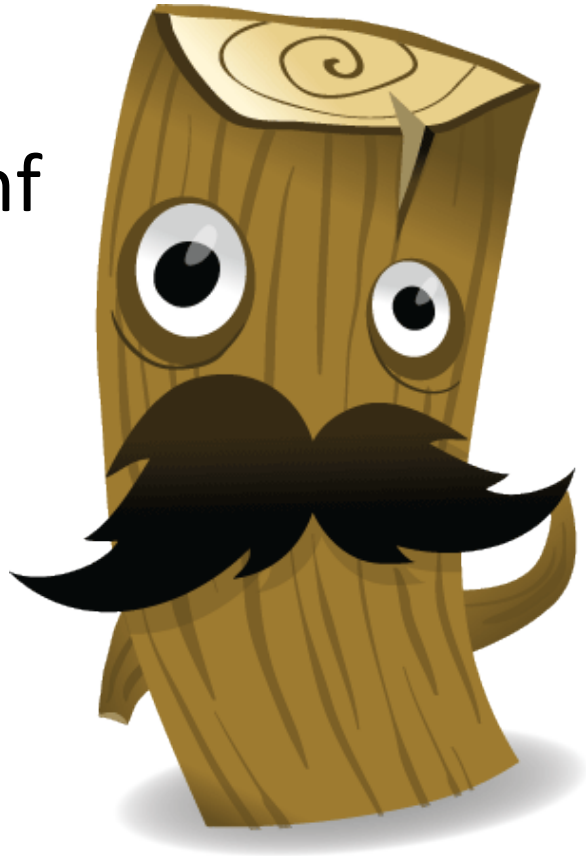
ENABLE

```
curl -XPUT http://localhost:9200/_cluster/settings -d '{ "transient" :
{ "cluster.routing.allocation.enable" : "all" }}'
```

Logstash

/etc/logstash/conf.d/logstash.conf

- input
- filter
- output



Logstash Input

```
input {
  lumberjack {
    port => 5555
    ssl_certificate => "/etc/ssl/logstash.crt”
    ssl_key => "/etc/ssl/logstash.key”
  }
}
```

Logstash Filter

```
if [type] =~ /^bro_/ {
  json {
    source => "message »
  }
  date {
    match => [ "ts", "UNIX" ]
  }
  if [type] == "bro_http" {
    mutate {
      rename => [ "host", "http_host" ]
    }
  }
```

Logstash Output

```
output {
  elasticsearch {
    cluster => "panapad"
    host => localhost
    protocol => transport
    index => "logstash-%{+YYYY.MM.dd}"
  }
}
```

Index Template

http://elasticsearch:9200/_template?pretty

Change field types

- String
- Integer
- Float
- boolean

index: analyzed

index: not_analyzed

Logstash Output – New template

```
output {
  elasticsearch {
    cluster => "panapad"
    host => localhost
    protocol => transport
    index => "logstash-%{+YYYY.MM.dd}"
    template => "/etc/logstash/bro_template.json"
    template_name => "logstash"
    template_overwrite => true
  }
}
```

Logstash Cert

- openssl req -subj '/CN=logstash.panapad.lan/' -x509 -batch -nodes -sha256 -newkey rsa:2048 -keyout logstash.key -out logstash.crt -days 365

1. Both the logstash server and the logstash-forwarder need the same certs
2. Common name must resolve

Turn Bro logs into json format

local.bro

@load policy/tuning/json-logs.bro

logstash-forwarder

AKA: Lumberjack

Light weight log forwarder designed to ship logs to a Logstash Server.

Download

curl –O https://download.elastic.co/logstash-forwarder/binaries/logstash-forwarder-0.4.0-1.x86_64.rpm

Install

sudo yum install logstash-forwarder

Bro – Logstash Forwarder Config

/etc/logstash-forwarder.conf

```
{
  "network": {
    "servers": [ "logstash.panapad.lan:5555" ],
    "ssl certificate": "/etc/ssl/logstash.crt",
    "ssl key": "/etc/ssl/logstash.key",
    "ssl ca": "/etc/ssl/logstash.crt"
  },
  "files": [
    {
      "paths": [ "/opt/bro/logs/current/conn.log" ],
      "codec" : "json",
      "fields": { "type": "bro_conn", "sensor": "dagobah" }
    },
    {
      "paths": [ "/opt/bro/logs/current/dns.log" ],
      "codec" : "json“,
      "fields": { "type": "bro_dns", "sensor": "dagobah" }
    },
```

Kibana

Open source browser based analytics and search dashboard for Elasticsearch

Kibana 3

Kibana 4

Kibana 3 Config

config.js

elasticsearch: "http://deathstar.panapad.lan:9200",

Kibana 3 Apache Config

```
<VirtualHost *:443>
  ServerName kibana3.panapad.lan

  ## Vhost docroot
  DocumentRoot "/var/www/kibana3"

  <Directory "/var/www/kibana3.panapad.lan">
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    Require all granted
  </Directory>

  ## Logging
  ErrorLog "/var/log/httpd/kibana3.error_ssl.log"
  ServerSignature Off
  CustomLog "/var/log/httpd/kibana3.access_ssl.log" combined

  ## SSL directives
  SSLEngine on
  SSLCertificateFile      "/etc/ssl/kibana3..crt"
  SSLCertificateKeyFile   "/etc/ssl/kibana3.key”
  SSLCACertificatePath    "/etc/pki/tls/certs"
  SSLProtocol             all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
</VirtualHost>
```

Kibana 4 Config

kibana.yml

elasticsearch_url: "http://localhost:9200"

Kibana 4 Systemd Service

/etc/systemd/system/kibana.service

```
[Unit]
Description=Kibana Service
After=network.target
[Service]
Type=simple
User=kibana
ExecStart=/var/www/kibana4/bin/kibana
Restart=on-abort
[Install]
WantedBy=multi-user.target
```

```
# systemctl start kibana
```

Demo

Questions?

https://github.com/panaman/brocon2015