Callum Scott

FalkirkLUG 3rd Nov 2015

What is Elastic?

Elastic is a suite of applications

- Shield — Security for your ES Cluster
- Watcher — Alerting on Queries
- Marvel — Monitoring for your Cluster*
- Beats — Network Packet Analytics

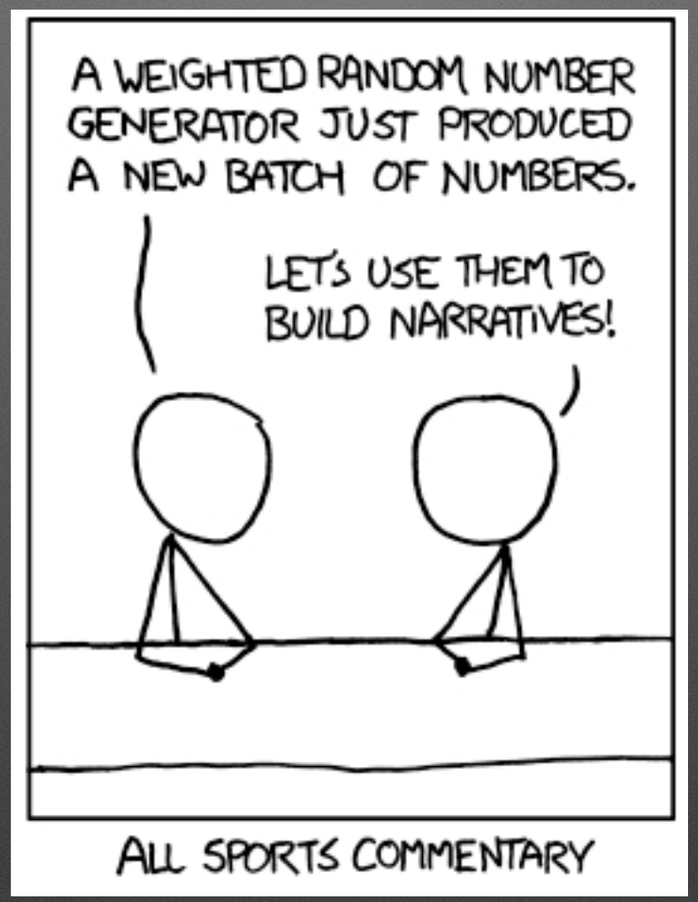
elasticsearch

{JSON}

Java

Lucene

But what is it for?



Getting It

Apt and RPM packages available
from http://elastic.co

OR

Tarball available, just unpack and run bin/elasticsearch

Puppet Module in the Forge is pretty good

GOTCHA!

Neither the RPM or the DEB pull in Java,
you need to install this yourself.

GOTCHA!

Java tries to bind to ipv6 addresses.
If you are not using ipv6 then you may need to disable it with sysctl or ES_JAVA_OPT

“No matter how slick the demo is in rehearsal, when you do it in front of a live audience, the probability of a flawless presentation is inversely proportional to the number of people watching, raised to the power of the amount of money involved.”

–Mark Gibbs

Pressing Wild Flowers

Logstash-forwarder
(aka lumberjack)

```
{
  "network": {
   "servers": [ "localhost:5043" ],
   "ssl certificate": "./logstash-forwarder.crt",
   "ssl key": "./logstash-forwarder.key",
   "ssl ca": "./logstash-forwarder.crt",
   "timeout": 15
  },

  "files": [
   {
      "paths": [
        # single paths are fine
        "/var/log/messages",
        # globs are fine too, they will be periodically evaluated
        # to see if any new files match the wildcard.
        “/var/log/apache2/*.log”
      ],
      "fields": { "type": "syslog" }
    #},
  ]
}
```

GOTCHA!

Default example of the log stash forwarder config file is heavily commented.

IN, Filter, Out

```
input {
  lumberjack {{
     port => 5000
     ssl_certificate => /path/to/certificate
     ssl_key => /path/to/key
  }
  }
```

```
filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}" }
  }
  date {
    match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]
  }
}

output {
  elasticsearch { host => localhost }
  stdout { codec => rubydebug }
}
```

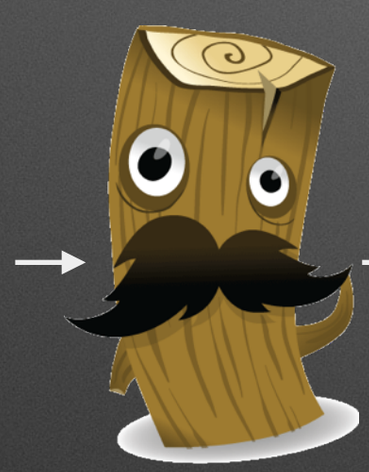
Pressing Wild Flowers

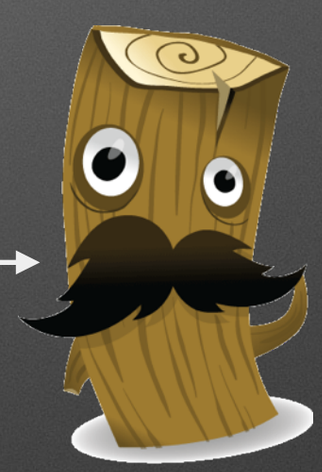
Transvestism and loitering in public houses

redis

elasticsearch

Transvestism and loitering in public houses

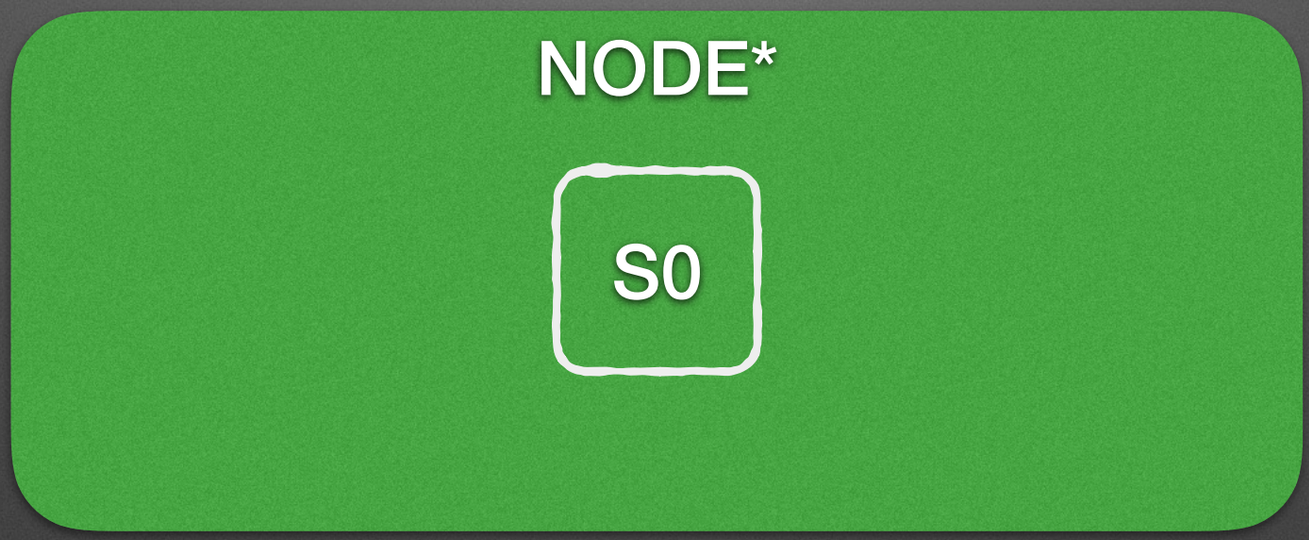




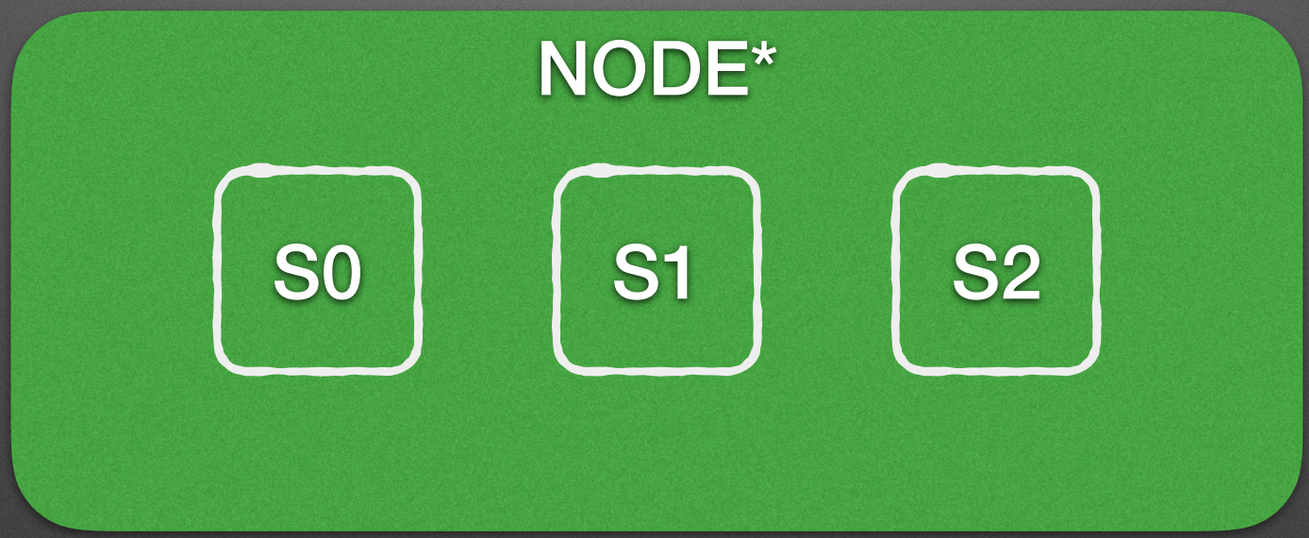
Where does it all go

NODE*
(Master)

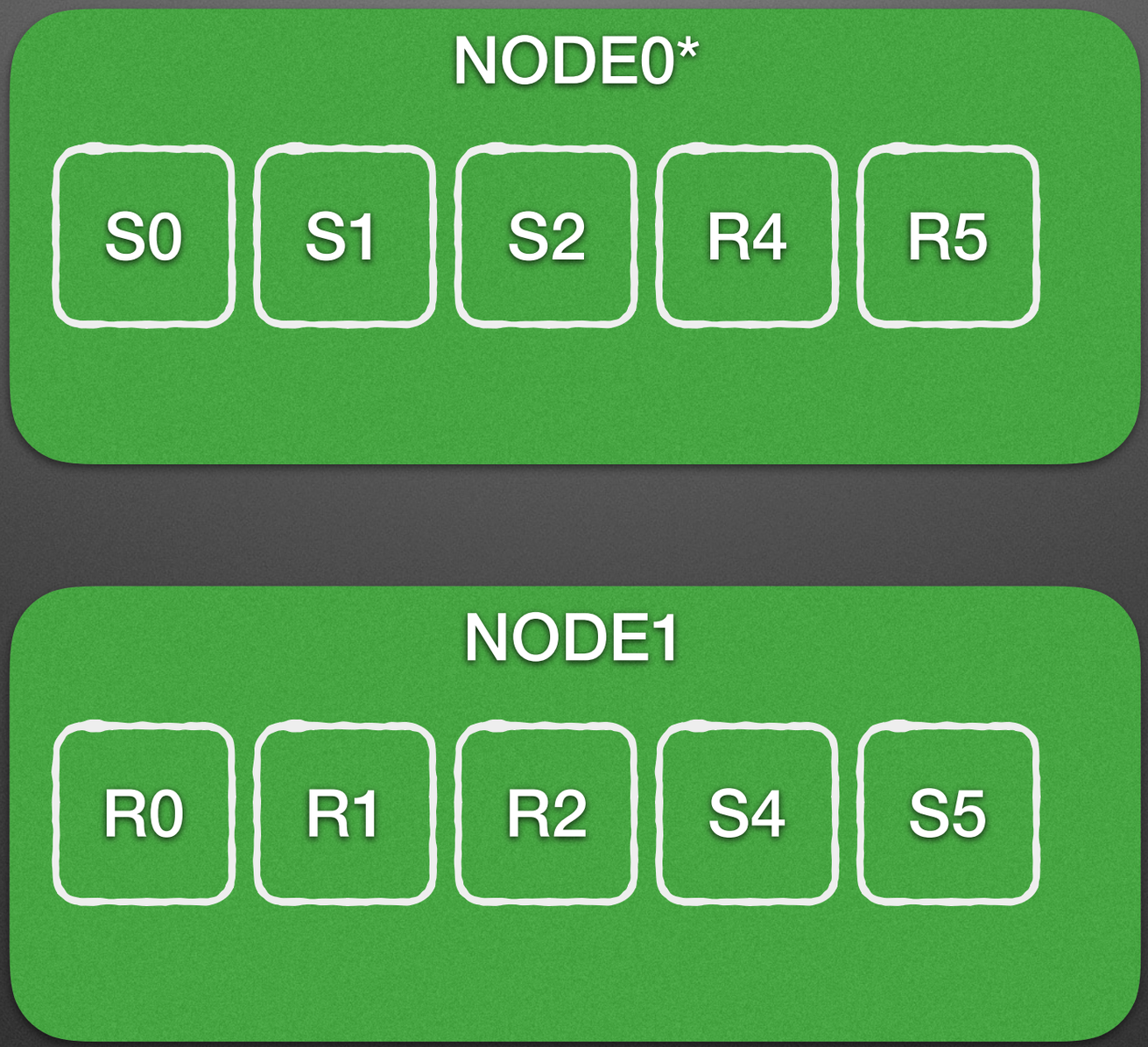
Where does it all go



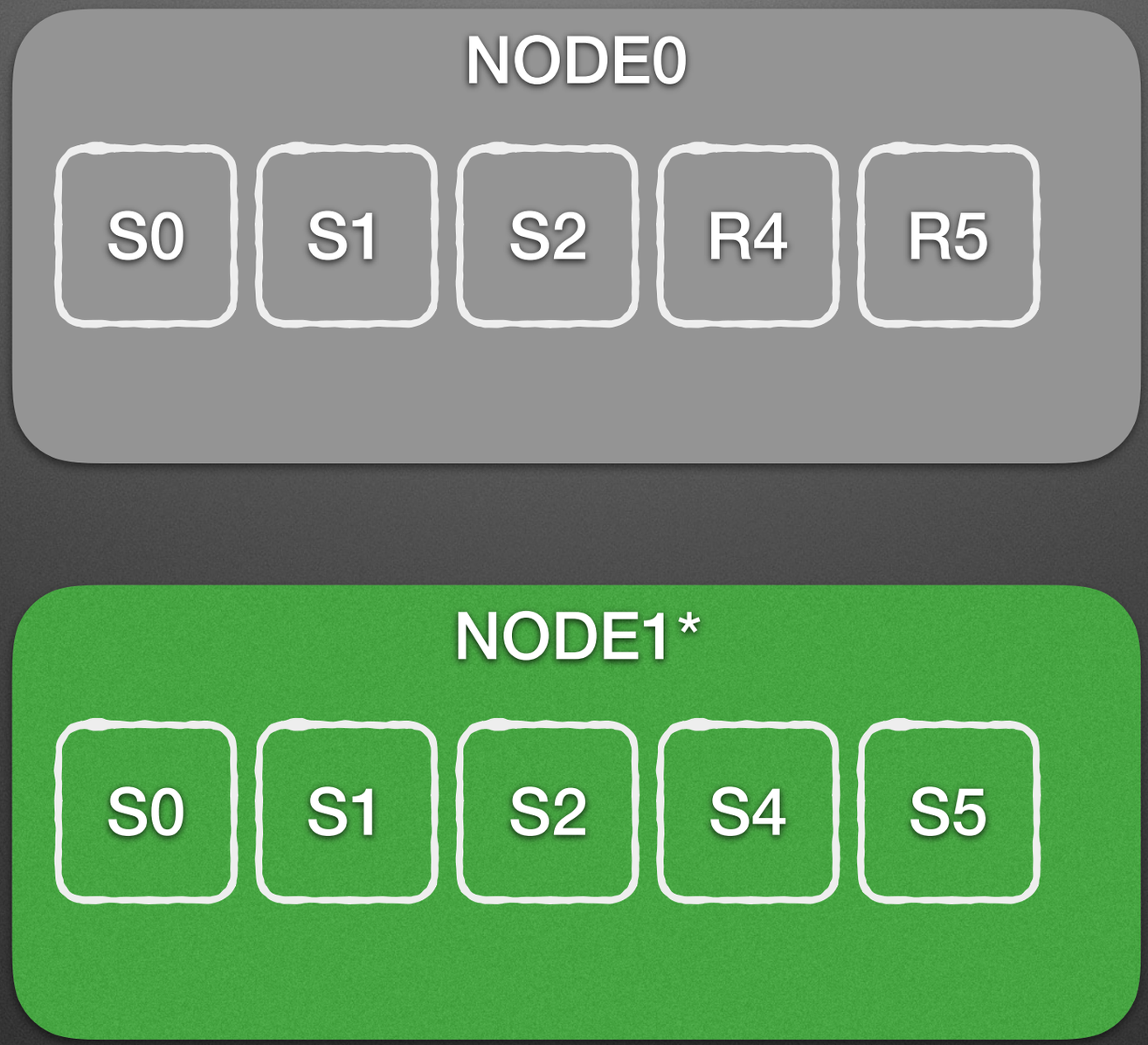
Where does it all go



Where does it all go



Where does it all go



Filtering

```
filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}" }
  }
  date {
    match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]
  }
}

COMMONAPACHELOG %{IPORHOST:clientip} %{USER:ident} %{USER:auth}
\[%{HTTPDATE:timestamp}\] "(?:%{WORD:verb} %{NOTSPACE:request}(?: HTTP/%
{NUMBER:httpversion})?|%{DATA:rawrequest})" %{NUMBER:response} (?:%
{NUMBER:bytes}|-)

COMBINEDAPACHELOG %{COMMONAPACHELOG} %{QS:referrer} %{QS:agent}
```

Filtering

```
input {
  file {
    path => "/tmp/*_log"
  }
}

filter {
  if [path] =~ "access" {
    mutate { replace => { type => "apache_access" } }
    grok {
      match => { "message" => "%{COMBINEDAPACHELOG}" }
    }
    date {
      match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]
    }
  } else if [path] =~ "error" {
    mutate { replace => { type => "apache_error" } }
  } else {
    mutate { replace => { type => "random_logs" } }
  }
}
```

Honourable Mention

graylog

An Open-Source
Community Site

www.elastic.co

www.digitalocean.com

https://github.com/bhaskarvk/vagrant-elk-cluster

http://grokdebug.herokuapp.com

http://grokconstructor.appspot.com

IRC: moncky
#falkirklug
#scotlug
Twitter: @moncky