logstash

> “logstash is a tool for managing events and logs. You can use it to **collect logs**, **parse them**, and **store them** for later use (like, for searching).”
>
> \- http://logstash.net

collect logs

37 inputs

amqp, drupal_dblog, elasticsearch, eventlog, exec, file, ganglia, gelf, gemfire, generator, graphite, heroku, imap, irc, log4j, lumberjack, pipe, rabbitmq, redis, relp, s3, snmptrap, sqlite, sqs, stdin, stomp, syslog, tcp, twitter, udp, unix, varnishlog, websocket, wmi, xmpp, zenoss, zeromq,

37 inputs

amqp, drupal_dblog, elasticsearch, eventlog, exec, file, ganglia, gelf, gemfire, generator, graphite, heroku, imap, irc, log4j, lumberjack, pipe, rabbitmq, redis, relp, s3, snmptrap, sqlite, sqs, **stdin**, stomp, syslog, tcp, twitter, udp, unix, varnishlog, websocket, wmi, xmpp, zenoss, zeromq,

Demo…

(or how to slip on a banana)

Use redis as input…

```
input {
  redis {
    data_type => 'list'
    host => '127.0.0.1'
    threads => 2
    db => 6
    key => 'logstash:bunyan'
    type => 'bunyan'
  }
}
```

Demo

(or how to juggle chainsaws)

parse logs

39 filters

advisor, alter, anonymize, checksum, cidr, cipher, clone, csv, date, dns, drop, environment, extractnumbers, gelfify, geoip, grep, grok, grokdiscovery, json, json_encode, kv, metaevent, metrics, multiline, mutate, noop, prune, railsparallelrequest, range, ruby, sleep, split, syslog_pri, translate, urldecode, useragent, uuid, xml, zeromq

39 filters

advisor, alter, anonymize, checksum, cidr, cipher, clone, csv, date, dns, drop, environment, extractnumbers, gelfify, geoip, grep, grok, grokdiscovery, json, json_encode, kv, metaevent, metrics, multiline, **mutate**, noop, prune, railsparallelrequest, range, ruby, sleep, split, syslog_pri, translate, urldecode, useragent, uuid, xml, zeromq

```
filter {
  if [response][a] =~ /Linux/ {
    mutate {
      add_field => ['os', 'Linux']
    }
  }
}
```

39 filters

advisor, alter, anonymize, checksum, cidr, cipher, clone, csv, date, dns, drop, environment, extractnumbers, gelfify, geoip, grep, **grok**, grokdiscovery, json, json_encode, kv, metaevent, metrics, multiline, mutate, noop, prune, railsparallelrequest, range, ruby, sleep, split, syslog_pri, translate, urldecode, useragent, uuid, xml, zeromq

```
input {
  redis {
    data_type => 'list'
    host => '127.0.0.1'
    threads => 2
    db => 6
    key => 'logstash:bunyan'
    type => 'bunyan'
  }
}
```

```
filter {
  grok {
    type => "nginx-access"
    pattern => "%{COMBINEDAPACHELOG}"
  }
}
```

```
filter {
  grok {
    type => "couchdb"
    match => "\[%{DAY:day_of_week}, %{MONTHDAY:day} %
{MONTH:month} %{YEAR:year} %{TIME} %{WORD:timezone}\]
\[%{WORD:level}\] \[\<%{INT:process}\.%{INT:pid}\.%
{INT:pid2}\>\] %{IP:client} - - %{WORD:method} %
{URIPATHPARAM:request} %{WORD:http_status_code}"
  }
}
```

39 filters

advisor, alter, anonymize, checksum, cidr, cipher, clone, csv, date, dns, drop, environment, extractnumbers, gelfify, geoip, grep, grok, grokdiscovery, json, json_encode, kv, metaevent, metrics, multiline, mutate, noop, prune, railsparallelrequest, range, ruby, sleep, split, syslog_pri, translate, urldecode, useragent, uuid, xml, zeromq

store logs

51 outputs

amqp, boundary, circonus, cloudwatch, datadog, datadog_metrics, elasticsearch, elasticsearch_http, elasticsearch_river, email, exec, file, ganglia, gelf, gemfire, google_cloud_storage, graphite, graphtastic, hipchat, http, irc, jira, juggernaut, librato, loggly, lumberjack, metriccatcher, mongodb, nagios, nagios_nsca, null, opentsdb, pagerduty, pipe, rabbitmq, redis, riak, riemann, s3, sns, sqs, statsd, stdout, stomp, syslog, tcp, udp, websocket, xmpp, zabbix, zeromq

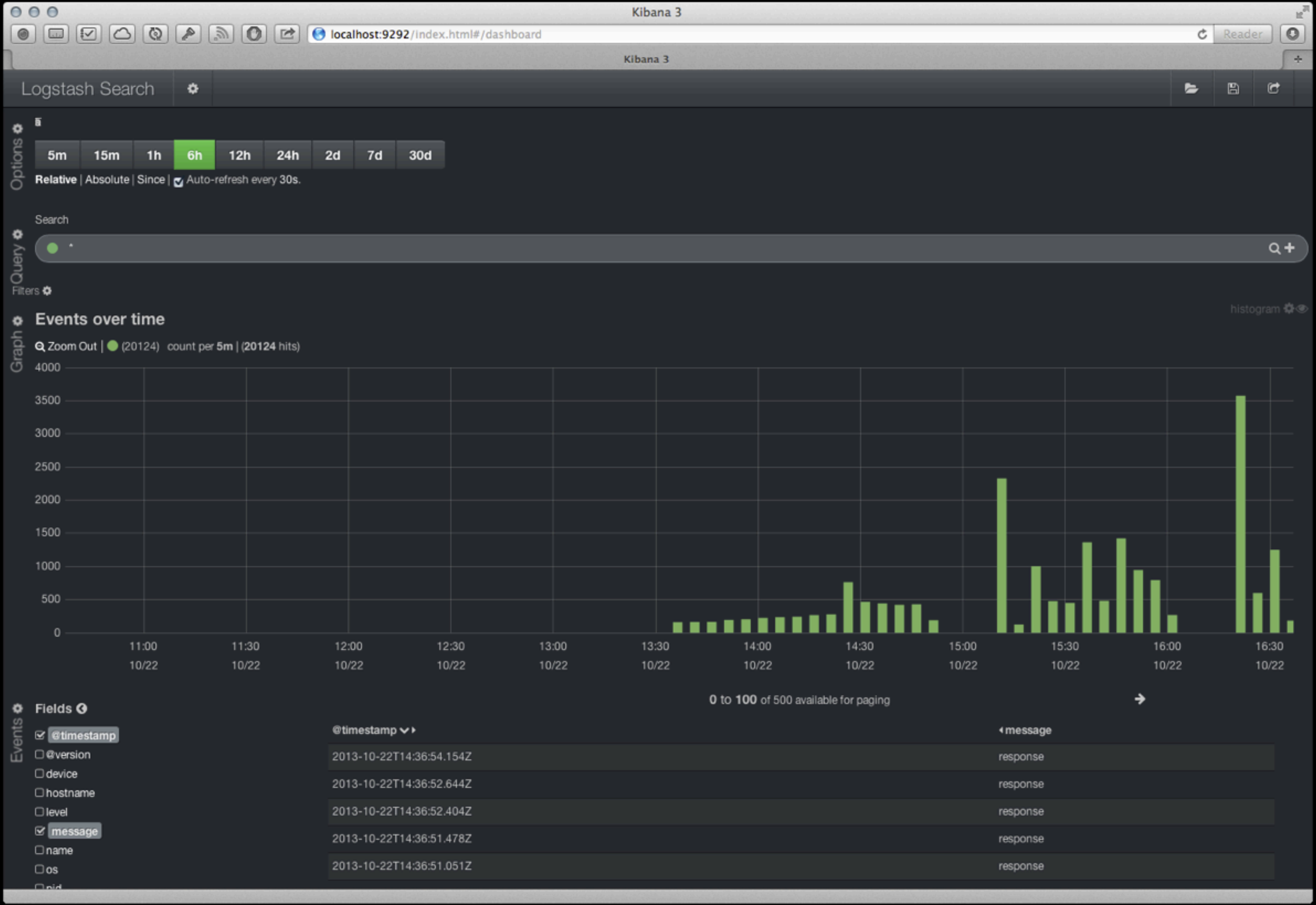
Fully searchable

Build your own Dashboards

All Open Source

51 outputs

amqp, boundary, circonus, cloudwatch, datadog, datadog_metrics, **elasticsearch**, elasticsearch_http, elasticsearch_river, email, exec, file, ganglia, gelf, gemfire, google_cloud_storage, graphite, graphtastic, hipchat, http, irc, jira, juggernaut, librato, loggly, lumberjack, metriccatcher, mongodb, nagios, nagios_nsca, null, opentsdb, pagerduty, pipe, rabbitmq, redis, riak, riemann, s3, sns, sqs, statsd, stdout, stomp, syslog, tcp, udp, websocket, xmpp, zabbix, zeromq



Events over time

Zoom Out | ● (20124) count per 5m | (20124 hits)

- ☑ @timestamp
- □ @version
- □ device
- □ hostname
- □ level
- ☑ message
- □ name
- □ os
- □ pid

0 to 100 of 500 available for paging

@timestamp	message
2013-10-22T14:36:54.154Z	response
2013-10-22T14:36:52.644Z	response
2013-10-22T14:36:52.404Z	response
2013-10-22T14:36:51.478Z	response
2013-10-22T14:36:51.051Z	response

Demo

(or how to catch a liger)

Mechanics

Written in ruby.

Bundled in Java.

WTF!?

It just works.

Author

Jordan Sissel

(former Czar of Logging at DreamHost)

Watch one of his talks!

http://www.youtube.com/watch?v=RuUFnog29M4

Use logstash!

Image Credits:

Banana designed by 42 from The Noun Project

Lion designed by m. turan ercan from The Noun Project