How to win skeptics to log aggregation using Vagrant and ELK

London DevOps, 16th December 2014

#londondevops

SKELTON THATCHER

EFFECTIVE SOFTWARE OPERATIONS

Ease of spinning up ELK box

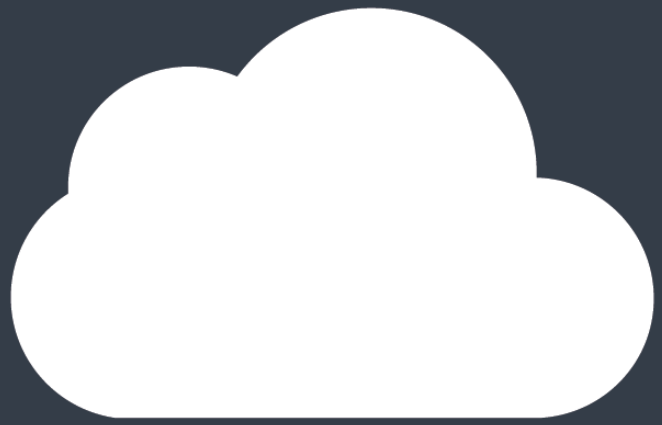
Assume you can install Virtualbox, Vagrant & Git

Use Canned / Artificial data feeding log entries

Rob Thatcher

@robtthatcher

- 16+ years' systems infrastructure & operations experience
- Systems, networks & operations
  - Finance tech
  - Saas Migrations
  - Team dynamics



‘Cloud’ changes the way we must
design, deliver, and operate
our software systems

Recent Work

Education

UK legal

Charitable

Finance

Tourism

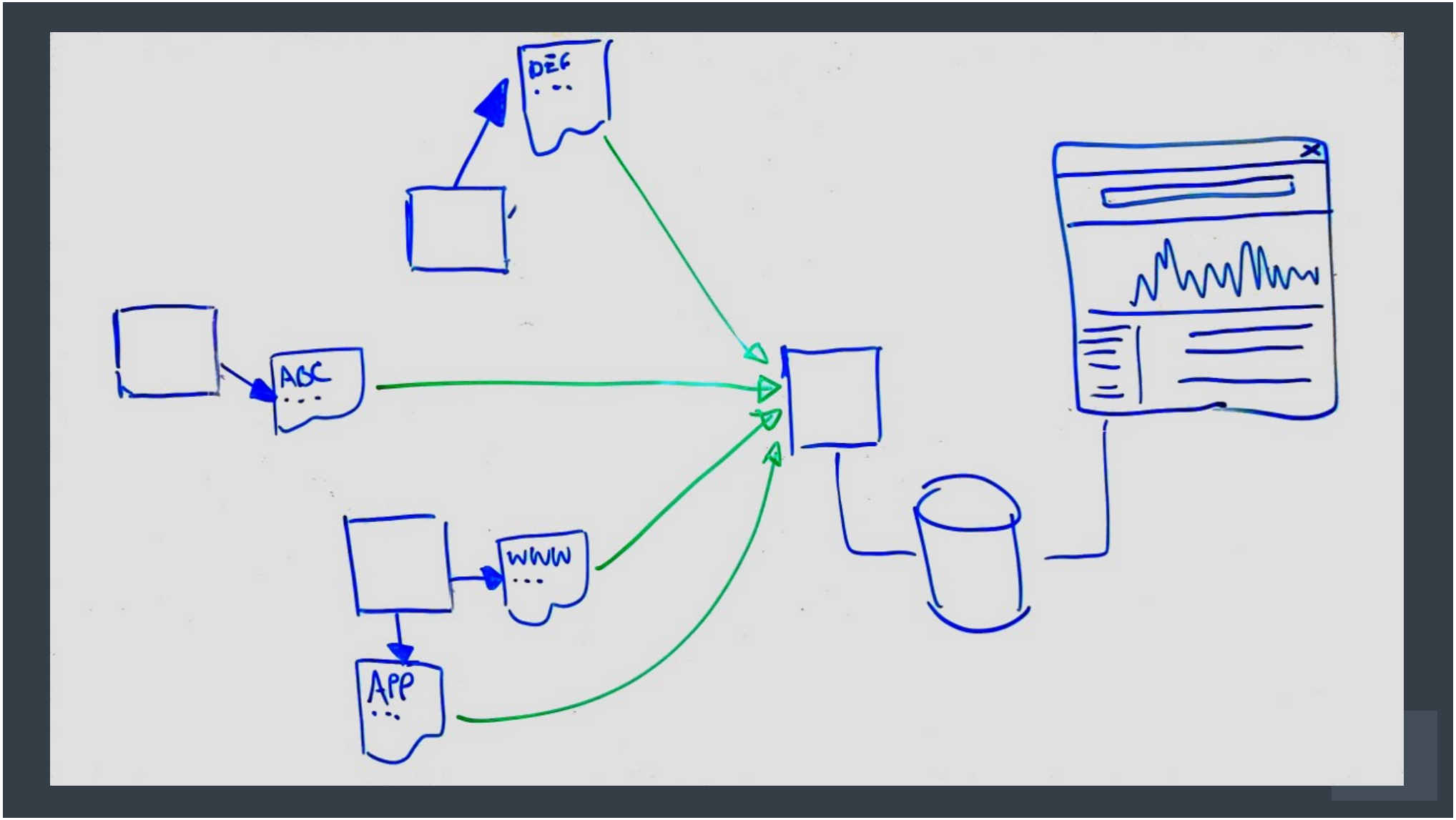
Online betting

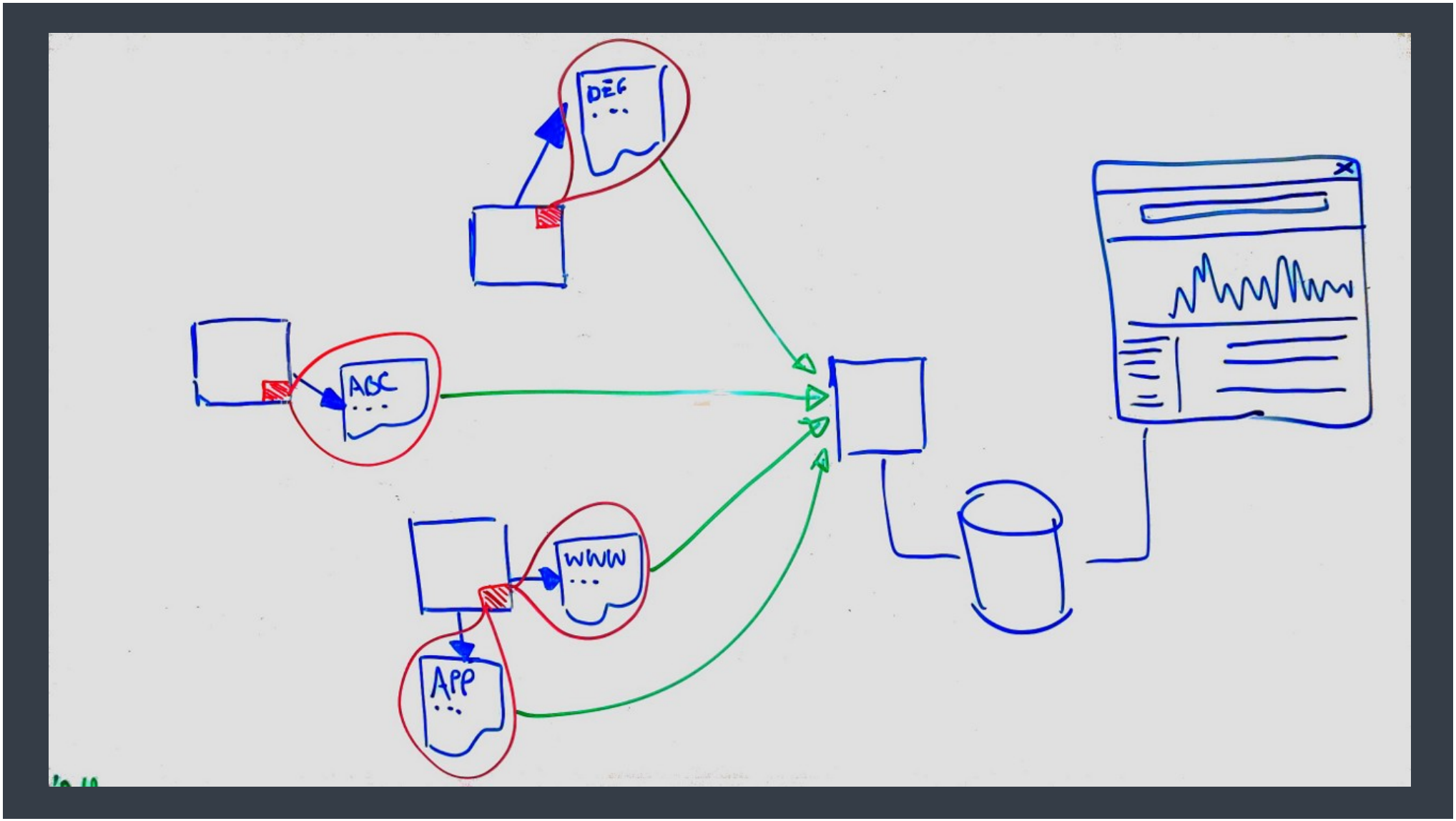
So why are we here?

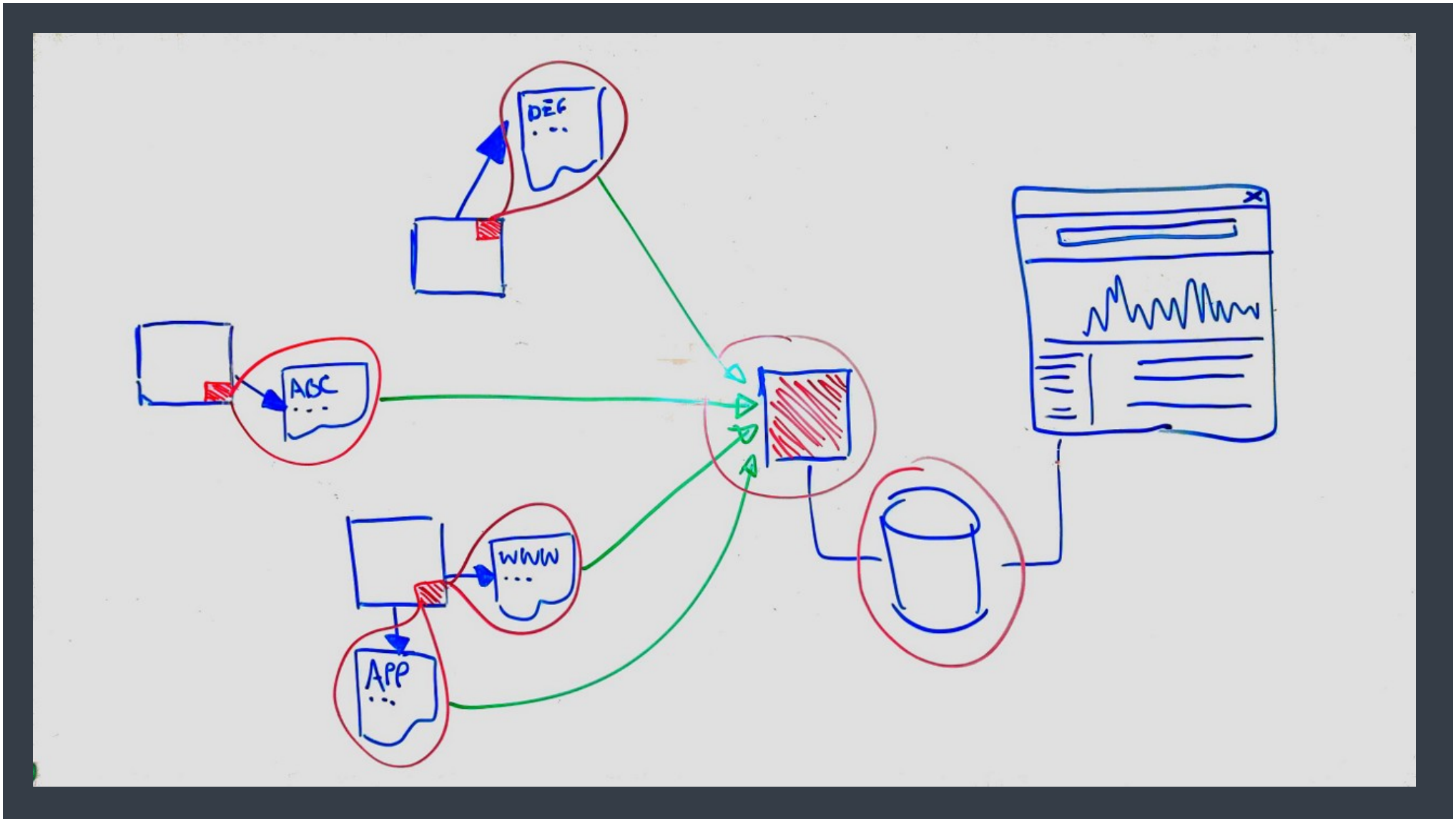
We believe… (in aggregated logging)
ELK with Vagrant rocks…

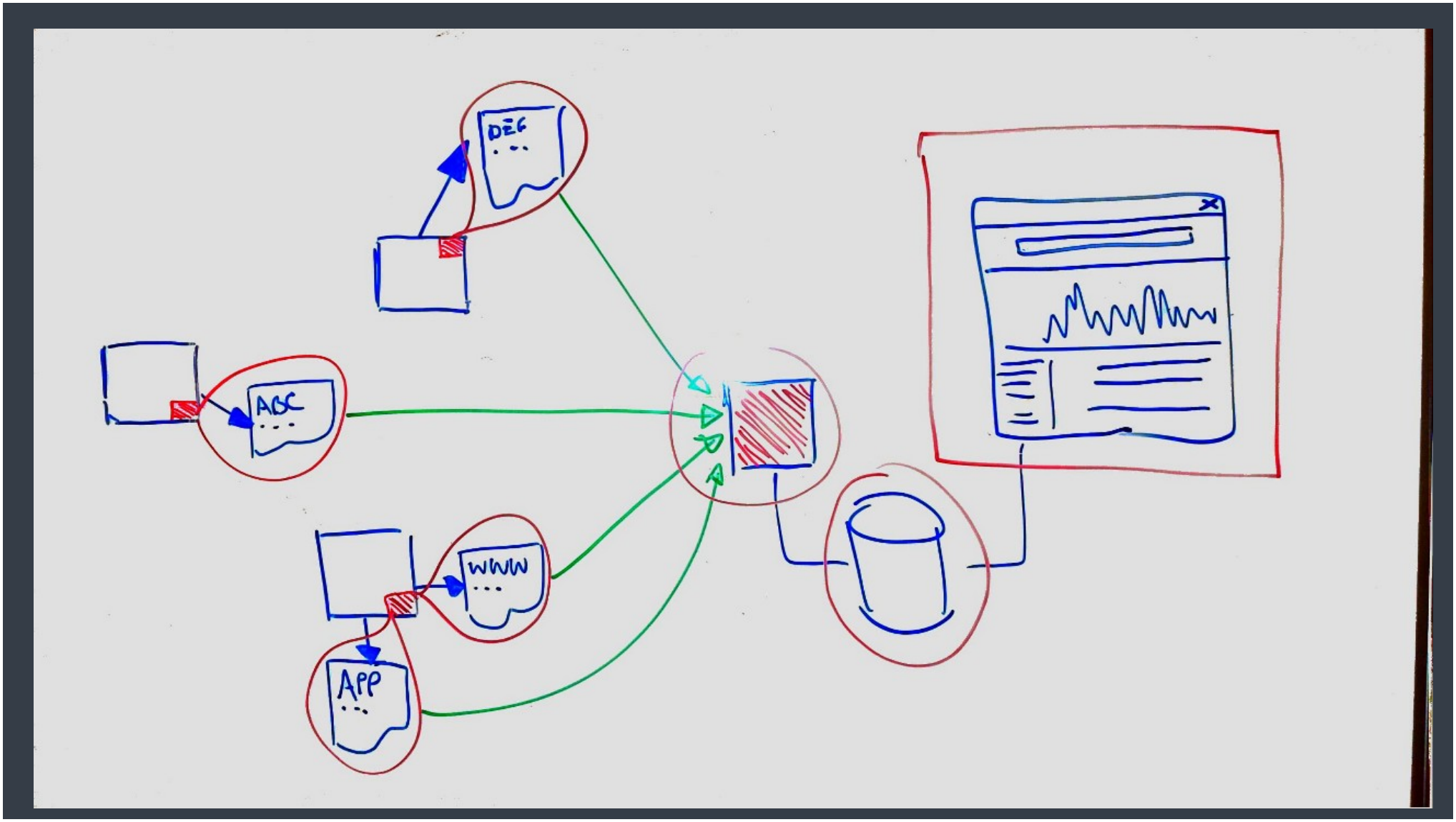
Winning skeptics to log aggregation...

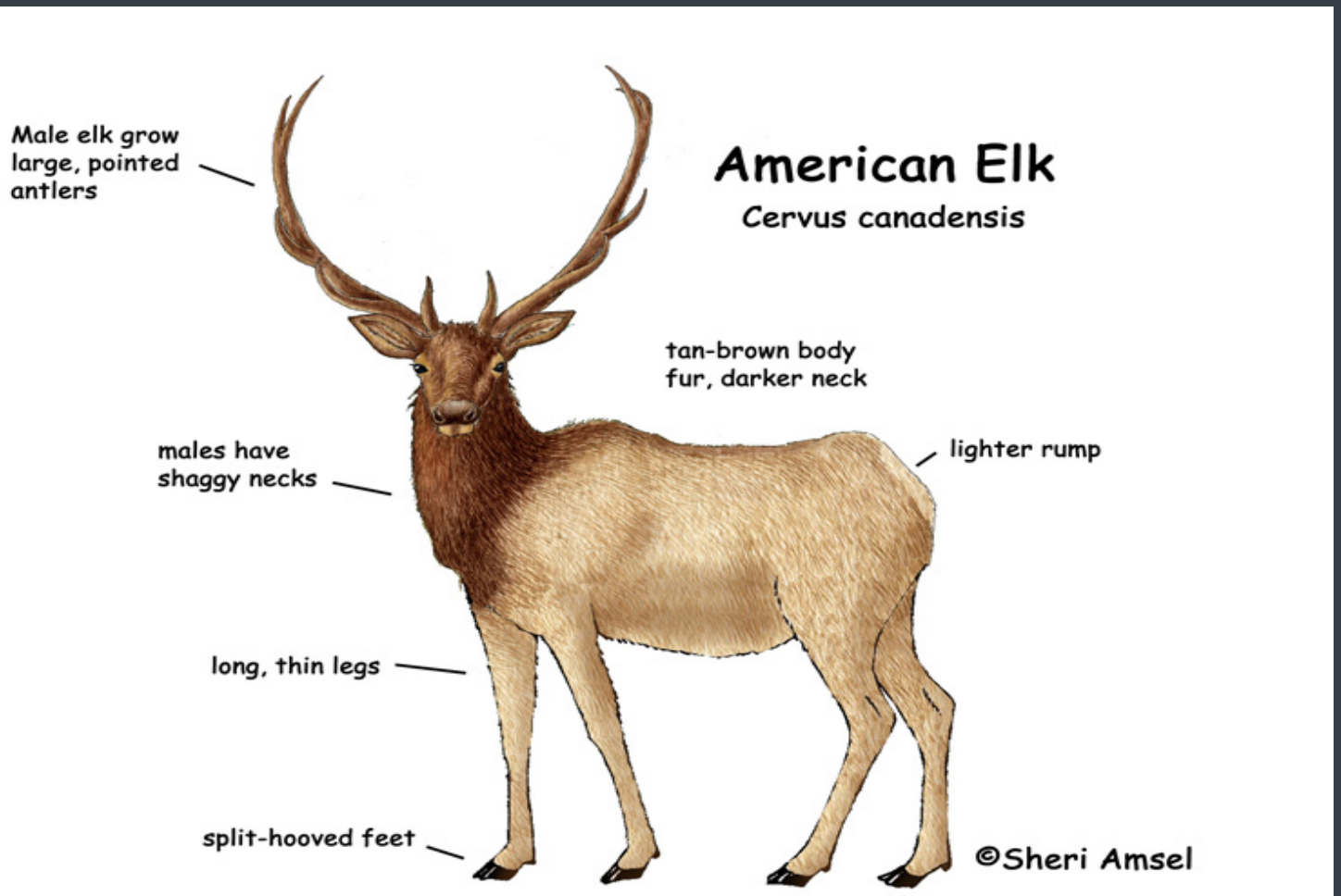
What is Log Aggregation?

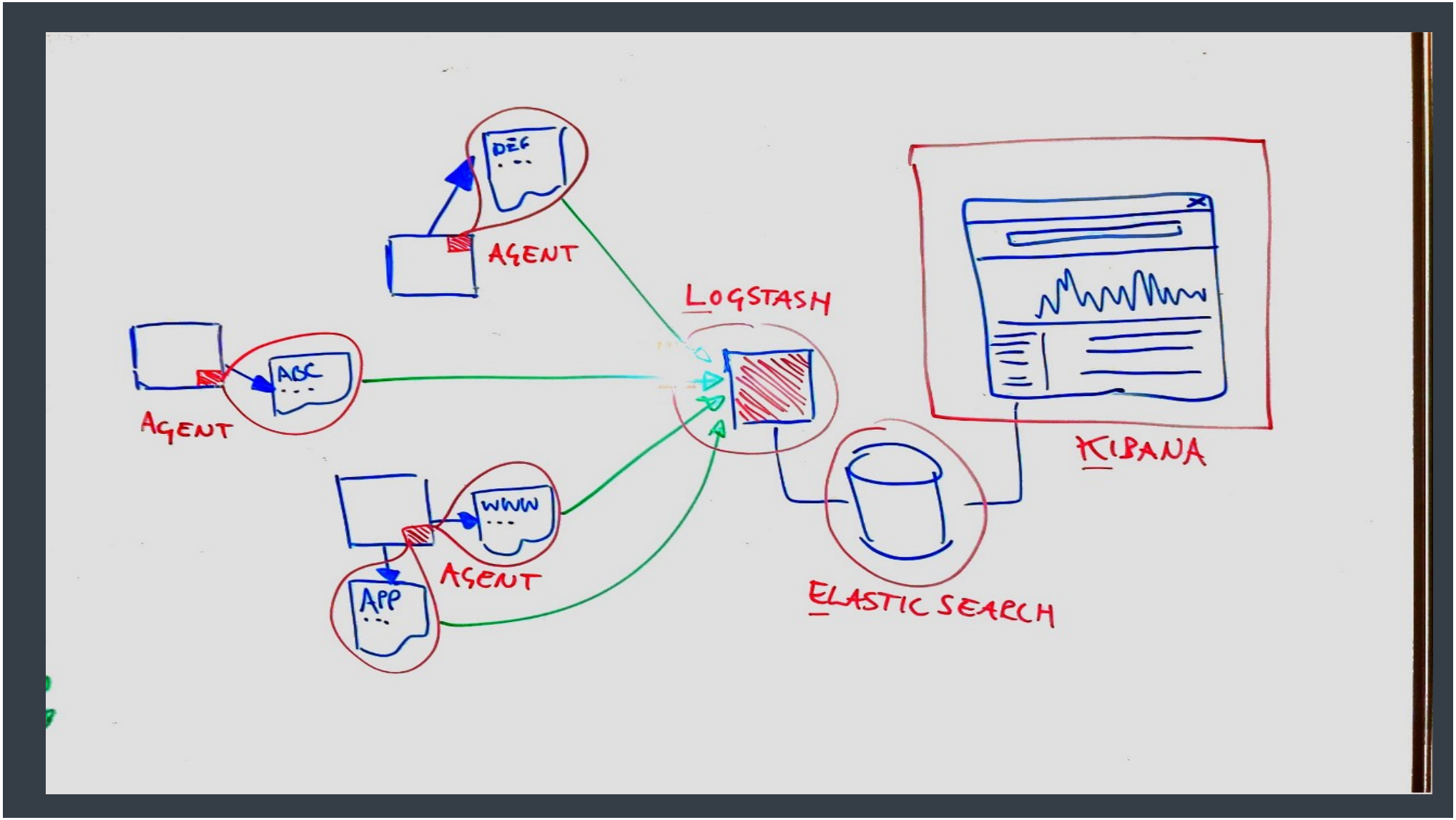

DEF
ABC
WWW
APP


DEF
ABC
WWW
APP


DEF
ABC
WWW
APP


DEF
ABC
WWW
APP


Male elk grow large, pointed antlers
American Elk
Cervus canadensis
tan-brown body fur, darker neck
males have shaggy necks
lighter rump
long, thin legs
split-hooved feet
©Sheri Amsel


DEG
AGENT
LOGSTASH
KIBANA
ABC
AGENT
WWW
APP
AGENT
ELASTIC SEARCH

Elasticsearch, Logstash, Kibana

Why?
How?
What?

Why do log aggregation?

Collaboration
Visibility
CSI

A software fairy tale…

There was a company of developers brave and true,
built their product and shipped when due (just)..

Of their product they were proud, but they soon saw it wouldn't work in the cloud..

The long march to Saas well underway, quite soon, they asked 'Why does deployment take more than a day?'

Manual installs, no puppet, chef, or dependency tree, a giant tarball was all the Ops guy could see…

Many components interacting like free, no combined logging allowed any to see...

Not a fairy tale...

Born from experience, helping Organisations fix Ops and Software Infrastructure.

Multi-layer Architecture

Multiple live / production versions

No Ops team

No shared tools

No application logs

Single deployment took around 1 week, sometimes more.
Less than 1 release per month

Why?
How?
What?

Why? - Dev

Application components
Messaging events
Streams
Etc..

Why? - Dev

Logging to same location can help with...

Why? - Dev

Improve debugging
Look into performance analysis
Understanding Interop of components

Why? - Ops

Routers, Firewalls
Web servers
Hypervisors

Why? - Ops

All logging to same location helps...

Why? - Ops

Faster event correlation
Better unified view across components
Visibility of events over time

Why? - Shared!

See problems in system, and app context

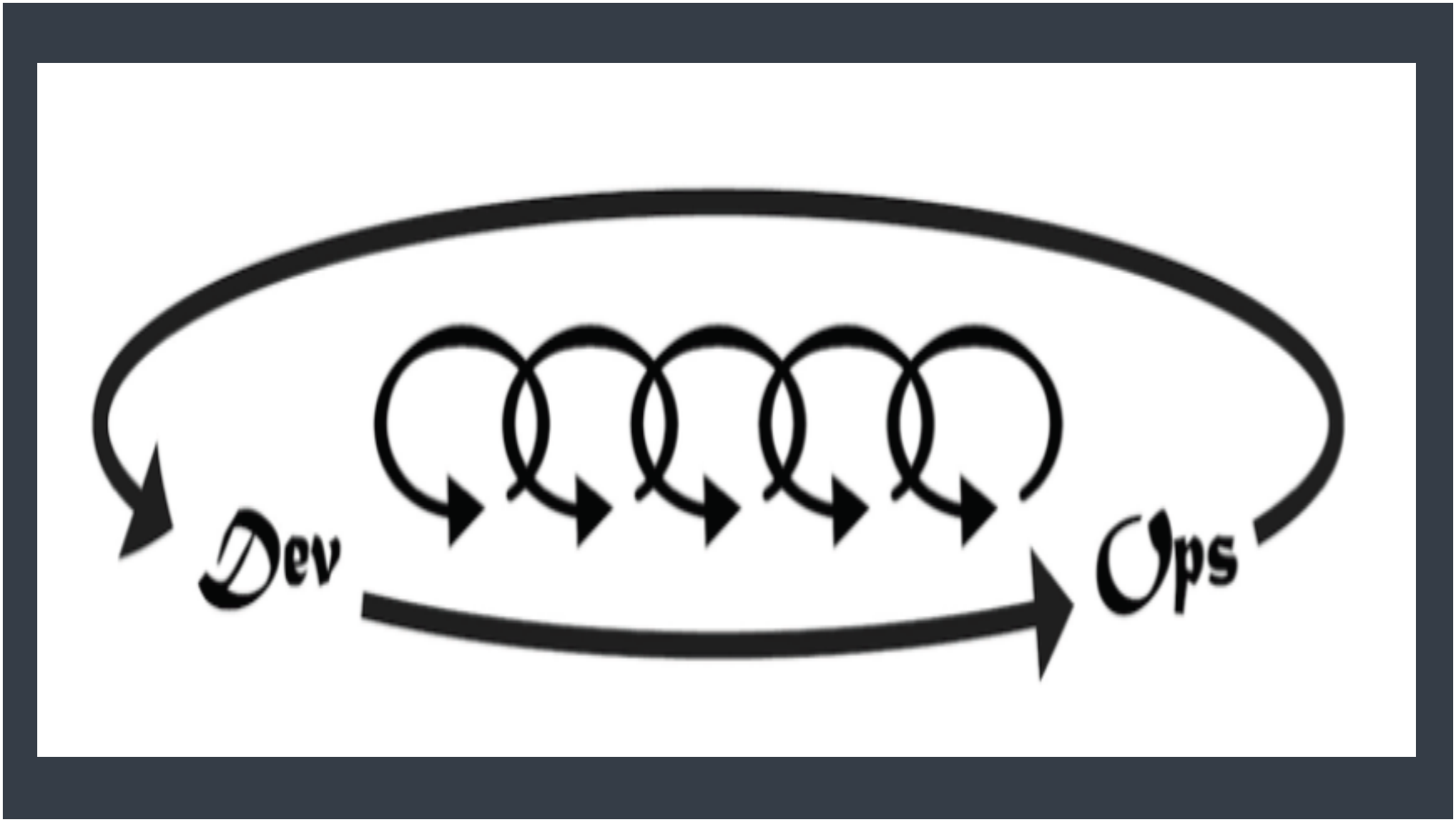
Operations gain insight into application behaviour

Common Tools across Dev and Ops

Why? - Shared!

ENABLE Collaboration
ENABLE Visibility
ENABLE CSI

ENABLE CONTINUAL SERVICE IMPROVEMENT


Dev
Ops

How .....?

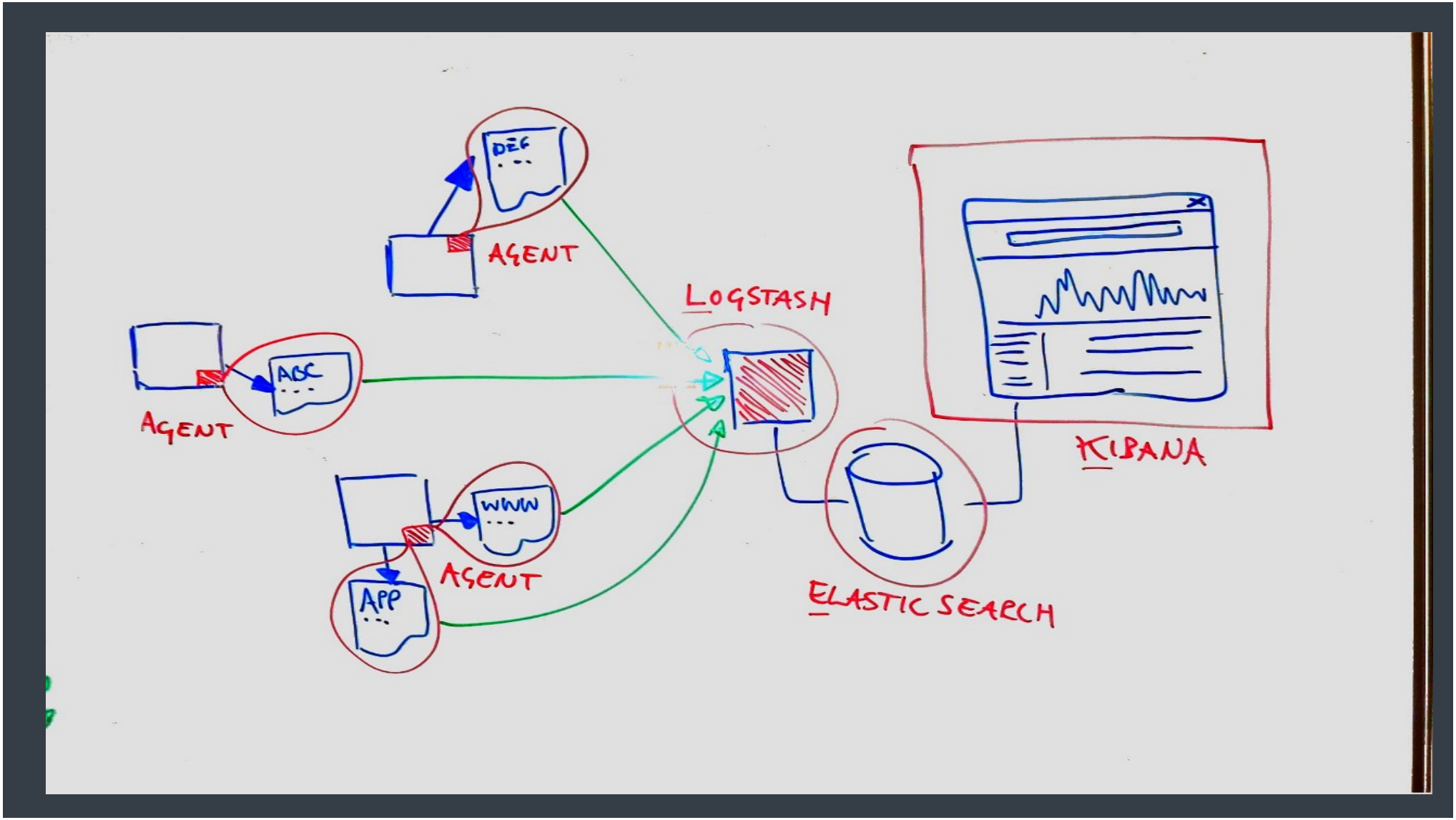
How - Components

Vagrant – As Box provisioner with Virtualbox

Elasticsearch – Search engine

Logstash – Log Database

Kibana – Make it pretty & UI


DEG
AGENT
LOGSTASH
KIBANA
ABC
AGENT
WWW
APP
AGENT
ELASTIC SEARCH

Vagrant

Create & configure lightweight, reproducible, portable environments

Manage start and stop of VM + 'provisioning layer'

Hooks into AWS and Azure
Lightweight for Linux boxes

ELK (Elasticsearch, Logstash, Kibana)

Elasticsearch provides powerful query interface

Logstash for storing incoming log messages

Kibana makes the whole thing pretty

Simple searches powered by good regex

Built for Simplicity and Ease of use

What – The Demonstrator

Fully installed ELK machine

Configured to listen to its own nginx logs, and bundled with a trivial log generator script.

Using the ELK interface adds more logs entries.

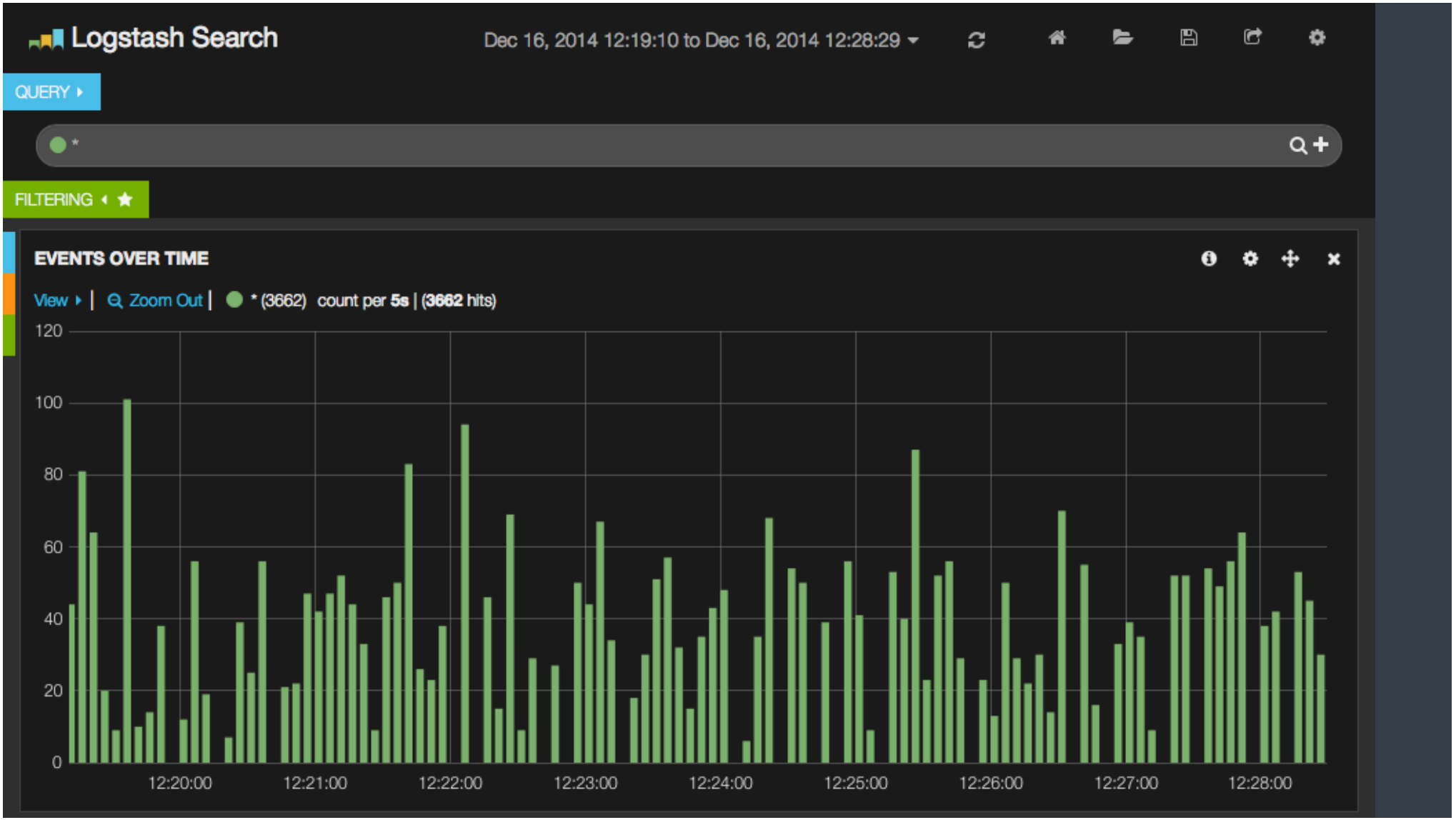
Can be used “Pre-canned” to allow offline demo (packages are cached are first run)

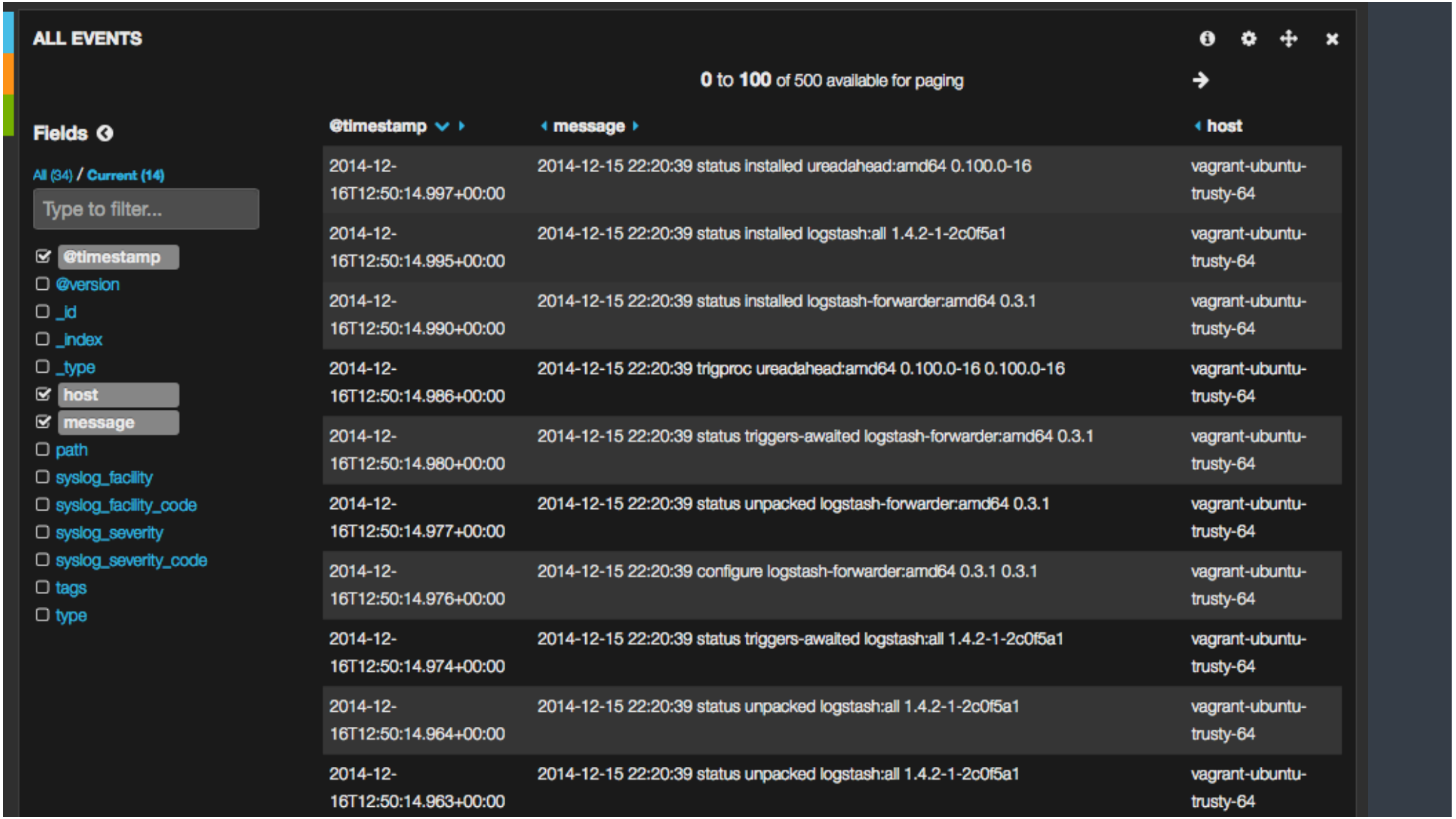
Live from the net, takes about 5 minutes

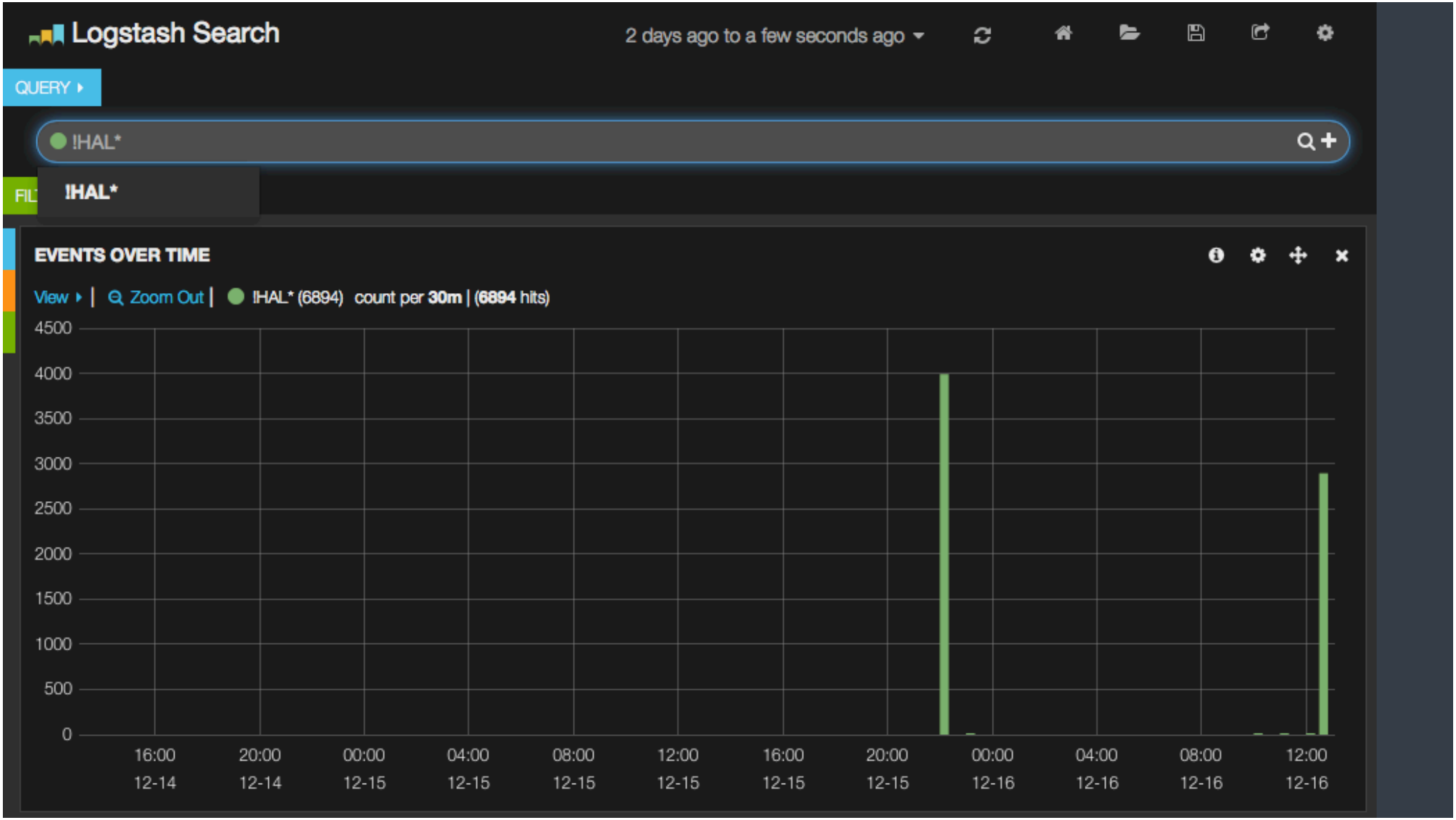
Config and scripts available via Github

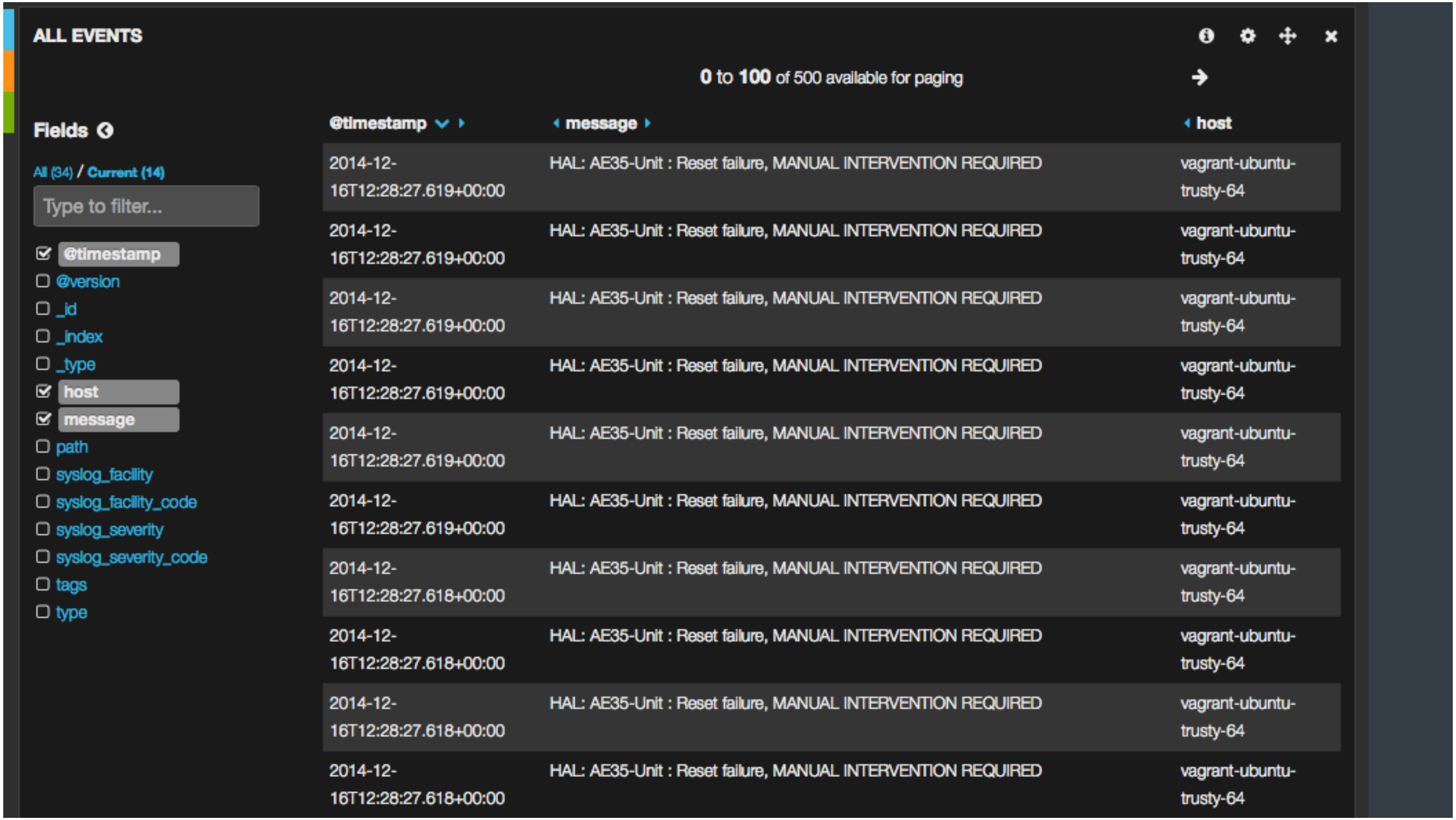
https://github.com/SkeltonThatcher/velk-demo

Demo the thing.....


Logstash Search
Dec 16, 2014 12:19:10 to Dec 16, 2014 12:28:29
QUERY
*
FILTERING
EVENTS OVER TIME
View | Zoom Out | * (3662) count per 5s | (3662 hits)
120
100
80
60
40
20
0
12:20:00
12:21:00
12:22:00
12:23:00
12:24:00
12:25:00
12:26:00
12:27:00
12:28:00


ALL EVENTS
0 to 100 of 500 available for paging
Fields
All (34) / Current (14)
Type to filter...
@timestamp
@version
_id
_index
_type
host
message
path
syslog_facility
syslog_facility_code
syslog_severity
syslog_severity_code
tags
type
@timestamp
message
host
2014-12-16T12:50:14.997+00:00
2014-12-15 22:20:39 status installed ureadahead:amd64 0.100.0-16
vagrant-ubuntu-trusty-64
2014-12-16T12:50:14.995+00:00
2014-12-15 22:20:39 status installed logstash:all 1.4.2-1-2c0f5a1
vagrant-ubuntu-trusty-64
2014-12-16T12:50:14.990+00:00
2014-12-15 22:20:39 status installed logstash-forwarder:amd64 0.3.1
vagrant-ubuntu-trusty-64
2014-12-16T12:50:14.986+00:00
2014-12-15 22:20:39 trigproc ureadahead:amd64 0.100.0-16 0.100.0-16
vagrant-ubuntu-trusty-64
2014-12-16T12:50:14.980+00:00
2014-12-15 22:20:39 status triggers-awaited logstash-forwarder:amd64 0.3.1
vagrant-ubuntu-trusty-64
2014-12-16T12:50:14.977+00:00
2014-12-15 22:20:39 status unpacked logstash-forwarder:amd64 0.3.1
vagrant-ubuntu-trusty-64
2014-12-16T12:50:14.976+00:00
2014-12-15 22:20:39 configure logstash-forwarder:amd64 0.3.1 0.3.1
vagrant-ubuntu-trusty-64
2014-12-16T12:50:14.974+00:00
2014-12-15 22:20:39 status triggers-awaited logstash:all 1.4.2-1-2c0f5a1
vagrant-ubuntu-trusty-64
2014-12-16T12:50:14.964+00:00
2014-12-15 22:20:39 status unpacked logstash:all 1.4.2-1-2c0f5a1
vagrant-ubuntu-trusty-64
2014-12-16T12:50:14.963+00:00
2014-12-15 22:20:39 status unpacked logstash:all 1.4.2-1-2c0f5a1
vagrant-ubuntu-trusty-64


Logstash Search
2 days ago to a few seconds ago
QUERY
!HAL*
!HAL*
EVENTS OVER TIME
View | Zoom Out | !HAL* (6894) count per 30m | (6894 hits)
4500
4000
3500
3000
2500
2000
1500
1000
500
0
16:00 12-14
20:00 12-14
00:00 12-15
04:00 12-15
08:00 12-15
12:00 12-15
16:00 12-15
20:00 12-15
00:00 12-16
04:00 12-16
08:00 12-16
12:00 12-16


ALL EVENTS
0 to 100 of 500 available for paging
Fields
All (34) / Current (14)
Type to filter...
@timestamp
@version
_id
_index
_type
host
message
path
syslog_facility
syslog_facility_code
syslog_severity
syslog_severity_code
tags
type
@timestamp
message
host
2014-12-16T12:28:27.619+00:00
HAL: AE35-Unit : Reset failure, MANUAL INTERVENTION REQUIRED
vagrant-ubuntu-trusty-64
2014-12-16T12:28:27.619+00:00
HAL: AE35-Unit : Reset failure, MANUAL INTERVENTION REQUIRED
vagrant-ubuntu-trusty-64
2014-12-16T12:28:27.619+00:00
HAL: AE35-Unit : Reset failure, MANUAL INTERVENTION REQUIRED
vagrant-ubuntu-trusty-64
2014-12-16T12:28:27.619+00:00
HAL: AE35-Unit : Reset failure, MANUAL INTERVENTION REQUIRED
vagrant-ubuntu-trusty-64
2014-12-16T12:28:27.619+00:00
HAL: AE35-Unit : Reset failure, MANUAL INTERVENTION REQUIRED
vagrant-ubuntu-trusty-64
2014-12-16T12:28:27.619+00:00
HAL: AE35-Unit : Reset failure, MANUAL INTERVENTION REQUIRED
vagrant-ubuntu-trusty-64
2014-12-16T12:28:27.618+00:00
HAL: AE35-Unit : Reset failure, MANUAL INTERVENTION REQUIRED
vagrant-ubuntu-trusty-64
2014-12-16T12:28:27.618+00:00
HAL: AE35-Unit : Reset failure, MANUAL INTERVENTION REQUIRED
vagrant-ubuntu-trusty-64
2014-12-16T12:28:27.618+00:00
HAL: AE35-Unit : Reset failure, MANUAL INTERVENTION REQUIRED
vagrant-ubuntu-trusty-64
2014-12-16T12:28:27.618+00:00
HAL: AE35-Unit : Reset failure, MANUAL INTERVENTION REQUIRED
vagrant-ubuntu-trusty-64

What?

Very fast ELK deployment
PoC demonstrator
A tool which Supports a collaborative approach
A powerful searchable archive of logging

Proven persuasion power (of Dev and managers)

As simple as

$git clone https://github.com/SkeltonThatcher/velk-demo.git

$cd velk-demo

$vagrant up

Why do Log Aggregation?

ENABLE & INCREASE

Collaboration
Visibility
Continual Service Improvement

SKELTON THATCHER

EFFECTIVE SOFTWARE OPERATIONS

http://skeltonthatcher.com/

enquiries@skeltonthatcher.com

@SkeltonThatcher

+44 (0)20 8242 4103