



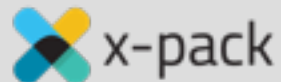
David Pilato
Developer | Evangelist
@dadoonet

And the beats go on!

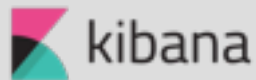


The Elastic Stack

Plugins



User Interface



Store, Index & Analyze



Ingest



Hosted Service





beats

**Beats are lightweight
shippers that collect and
ship all kinds of operational
data to Elasticsearch**

Examples of operational data



Diagram illustrating three types of operational data and the associated Elastic Beats:

- wire data** (Teal circle) associated with **Packetbeat** (light gray rectangle).
- system stats** (Yellow circle) associated with **Topbeat** (light gray rectangle).
- logs** (Pink circle) associated with **Filebeat** and **Winlogbeat** (light gray rectangle).

wire data

Packetbeat

system stats

Topbeat

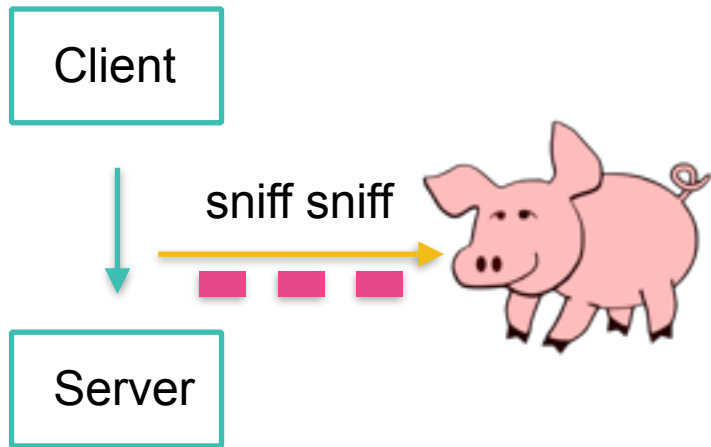
logs

Filebeat
Winlogbeat

Packetbeat

Captures insights from
network packets

Sniffing the network traffic



- Copy traffic at OS or hardware level
- Is completely passive
- ZERO latency overhead
- Not in the request/response path, cannot break your application

Packetbeat: Available decoders



HTTP



Thrift-RPC



DNS



MySQL



Memcache



AMQP



PostgreSQL



MongoDB



Add your own



Redis



ICMP

Processes: 367 total, 3 running, 6 stuck, 358 sleeping, 1833 threads
 Load Avg: 2.79, 2.69, 2.66 CPU usage: 35.77% user, 8.25% sys, 55.98% idle
 SharedLibs: 161M resident, 22M data, 10M linkedit. MemRegions: 132196 total, 5764M resident, 90M private
 PhysMem: 13G used (3762M wired), 2581M unused.
 VM: 2084G vsize, 527M framework vsize, 56231732(0) swaptins, 59291027(0) swapouts.
 Networks: pockets: 66492613/486 in, 57364574/316 out. Disks: 6744547/369G read, 34720560/883G written.

| PID | COMMAND | %CPU | TIME | #TH | #WQ | #PORTS | MEM | PURG | OMPR | PGRP | PPID | STATE | BOOSTS |
|--------|--------------|------|----------|-------|-----|--------|--------|-------|-------|-------|-------|----------|-----------|
| 64667 | burn | 89.3 | 04:00.32 | 5/1 | 0 | 15 | 580K | 00 | 00 | 64667 | 63666 | running | *0[1] |
| 29105 | java | 21.0 | 92:05.82 | 74 | 0 | 186 | 369M | 00 | 63M | 29105 | 98883 | sleeping | *0[2] |
| 15112 | topbeat | 18.7 | 02:56:57 | 12 | 0 | 61 | 9900K | 00 | 1108K | 15111 | 15111 | sleeping | *0[1] |
| 325 | iTerm | 12.8 | 02:18:11 | 12 | 4 | 366 | 90M | 40960 | 40M | 325 | 1 | sleeping | *0[19740] |
| 65237 | top | 7.4 | 00:08.34 | 1/1 | 0 | 24 | 7012K | 00 | 00 | 65237 | 18734 | running | *0[1] |
| 0 | kernel_task | 4.6 | 23:39:40 | 220/4 | 0 | 2 | 1719M+ | 00 | 00 | 0 | 0 | running | 0[0] |
| 61 | mds | 3.3 | 01:48:47 | 10 | 6 | 329+ | 14M | 00 | 34M | 61 | 1 | stuck | *0[1] |
| 194 | mds_stores | 3.1 | 02:03:27 | 10 | 7 | 76 | 20M+ | 1184K | 41M | 194 | 1 | stuck | *0[1] |
| 186 | WindowServer | 1.8 | 14:39:27 | 5 | 2 | 1224 | 79M | 5324K | 267M | 186 | 1 | sleeping | *0[1] |
| 637- | Dropbox | 1.5 | 93:04.38 | 84 | 0 | 385 | 80M | 00 | 44M | 637 | 1 | sleeping | *0[51781] |
| 97 | hidd | 1.4 | 93:44.84 | 6 | 2 | 98- | 3300K- | 00 | 1400K | 97 | 1 | sleeping | *0[1] |
| 53155 | mdworker | 1.1 | 01:05.39 | 4 | 0 | 66 | 14M | 00 | 1268K | 53155 | 1 | sleeping | *0[1] |
| 53158 | mdworker | 1.0 | 01:06.41 | 4 | 0 | 62 | 12M | 00 | 1000K | 53158 | 1 | sleeping | *0[1] |
| 3431 | Slack | 0.9 | 03:36:09 | 19 | 1 | 456 | 613M- | 27M | 331M | 3431 | 1 | sleeping | *0[22918] |
| 75966 | python2.7 | 0.7 | 28:17.99 | 3 | 1 | 33 | 8240K | 00 | 13M | 75966 | 75959 | stuck | *0[1] |
| 53159 | mdworker | 0.7 | 01:04.20 | 4 | 0 | 62 | 17M | 00 | 1144K | 53159 | 1 | sleeping | *0[1] |
| 53157 | mdworker | 0.6 | 01:06.09 | 4 | 0 | 62 | 19M | 00 | 948K | 53157 | 1 | sleeping | *0[1] |
| 324- | zoom.us | 0.5 | 13:07:07 | 13 | 0 | 44995 | 124M | 00 | 179M | 324 | 1 | sleeping | *48[18] |
| 23794- | dbfseventsd | 0.4 | 01:45.43 | 1 | 0 | 7 | 4168K | 00 | 140K | 637 | 23793 | sleeping | *0[1] |
| 75965 | python2.7 | 0.4 | 22:28.90 | 2 | 0 | 15 | 6860K | 00 | 11M | 75965 | 75959 | sleeping | *0[1] |
| 58424 | Google Chrom | 0.3 | 01:23.17 | 12 | 0 | 111 | 117M- | 00 | 37M | 316 | 316 | sleeping | *0[2] |
| 46 | fseventsd | 0.3 | 30:30.91 | 13 | 0 | 306 | 4796K | 00 | 4104K | 46 | 1 | sleeping | *0[1] |
| 23795- | dbfseventsd | 0.2 | 01:07.97 | 1 | 0 | 7 | 32K | 00 | 152K | 637 | 23794 | sleeping | *0[1] |
| 48135 | Google Chrom | 0.2 | 00:38.73 | 15 | 0 | 60 | 43M | 00 | 18M | 316 | 316 | sleeping | *0[1] |
| 65300 | screencaptur | 0.2 | 00:00.14 | 2 | 0 | 52 | 2220K | 20K | 00 | 336 | 336 | sleeping | *0[1] |
| 89 | mDNSResponse | 0.2 | 46:50.49 | 7 | 2 | 88 | 2096K | 00 | 1124K | 89 | 1 | sleeping | *0[1] |
| 316 | Google Chrom | 0.1 | 20:08:22 | 48 | 1 | 1998 | 943M | 736K | 1245M | 316 | 1 | sleeping | *0[18133] |
| 39271 | inkscape-bin | 0.1 | 03:05.45 | 7 | 0 | 39 | 7844K | 00 | 168M | 39268 | 39268 | sleeping | *0[1] |
| 60240 | Google Chrom | 0.1 | 01:33.59 | 9 | 0 | 110 | 39M- | 00 | 34M | 316 | 316 | sleeping | *0[2] |
| 212 | symptomsd | 0.1 | 16:32.42 | 4 | 2 | 102 | 2184K | 00 | 2112K | 212 | 1 | sleeping | 0[66876] |
| 23793- | dbfseventsd | 0.0 | 00:23.07 | 1 | 0 | 12 | 36K | 00 | 180K | 637 | 637 | sleeping | *0[1] |
| 61533 | Google Chrom | 0.0 | 00:07.55 | 13 | 0 | 123 | 90M | 00 | 00 | 316 | 316 | sleeping | *0[2] |
| 16578 | Google Chrom | 0.0 | 06:12.31 | 13 | 0 | 155 | 150M+ | 00 | 50M | 316 | 316 | sleeping | *0[2] |
| 639- | Google Photo | 0.0 | 15:39.98 | 14 | 0 | 262 | 4648K | 00 | 34M | 639 | 1 | sleeping | *0[27260] |
| 13660 | Finder | 0.0 | 16:11.28 | 9 | 2 | 423 | 119M | 00 | 239M | 13660 | 1 | sleeping | *0[2627] |
| 58571 | com.apple.op | 0.0 | 00:13.14 | 4 | 1 | 263 | 20M | 512K | 19M | 58571 | 1 | sleeping | *0[297] |
| 54793 | Google Chrom | 0.0 | 00:18.73 | 13 | 0 | 121 | 80M | 00 | 10M | 316 | 316 | sleeping | *0[2] |
| 54832 | com.apple.op | 0.0 | 01:02.49 | 4 | 1 | 263 | 9248K | 00 | 20M | 54832 | 1 | sleeping | *0[1856] |
| 62861 | Google Chrom | 0.0 | 00:01.85 | 12 | 0 | 112 | 70M | 00 | 00 | 316 | 316 | sleeping | *0[2] |
| 3391 | com.apple.op | 0.0 | 02:43.68 | 4 | 1 | 256 | 4992K | 00 | 10M | 3391 | 1 | sleeping | *0[1361] |

Topbeat

Like the Unix **top** command but sends the output periodically to Elasticsearch. Also works on Windows.

Topbeat: Exported data

System wide

- system load
- total CPU usage
- CPU usage per core
- Swap, memory usage

Per process

- state
- name
- command line
- pid
- CPU usage
- memory usage

Disk usage

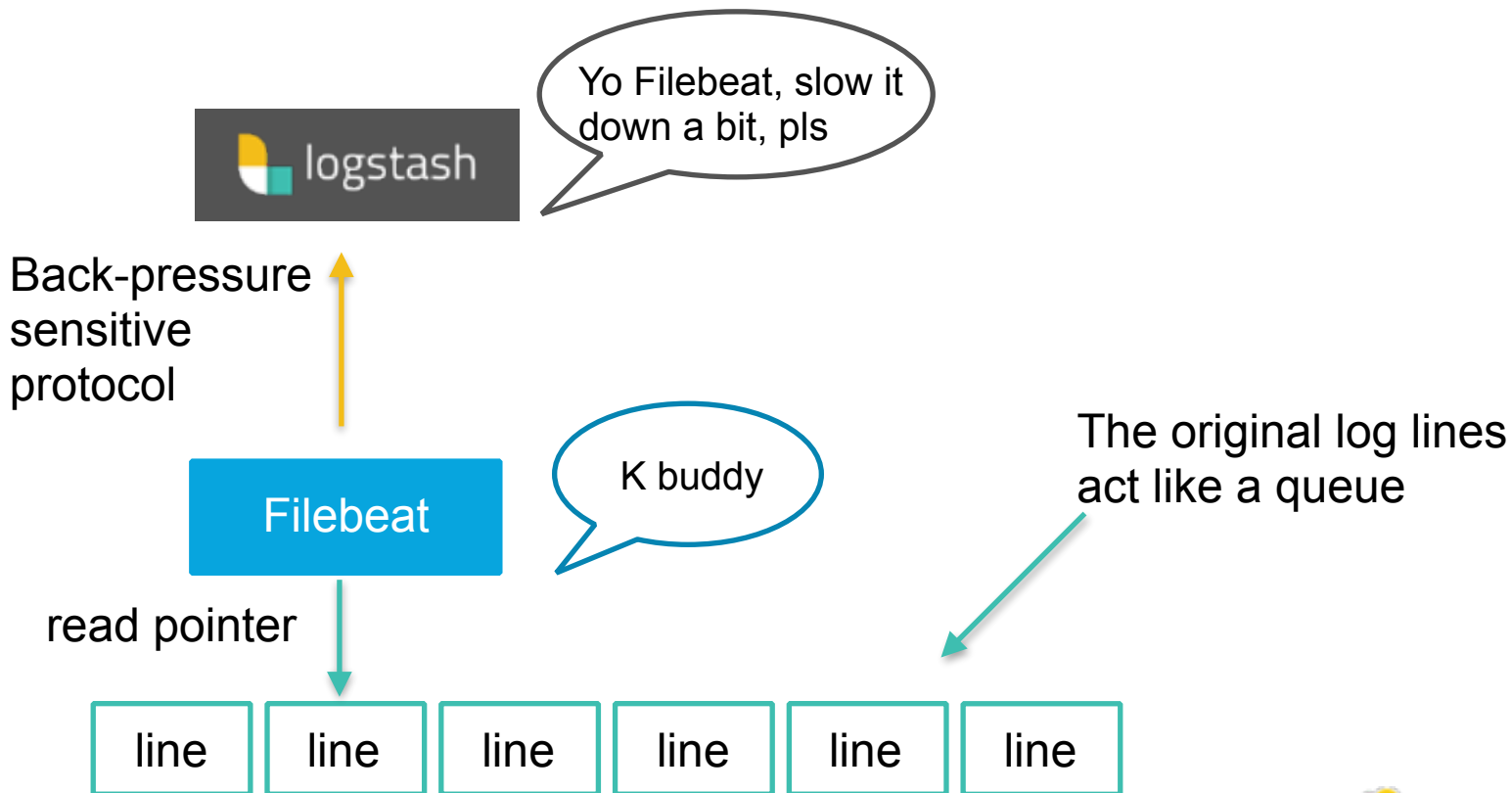
- available disks
- used, free space
- mounted points

Filebeat

Forwards log lines to
Elasticsearch

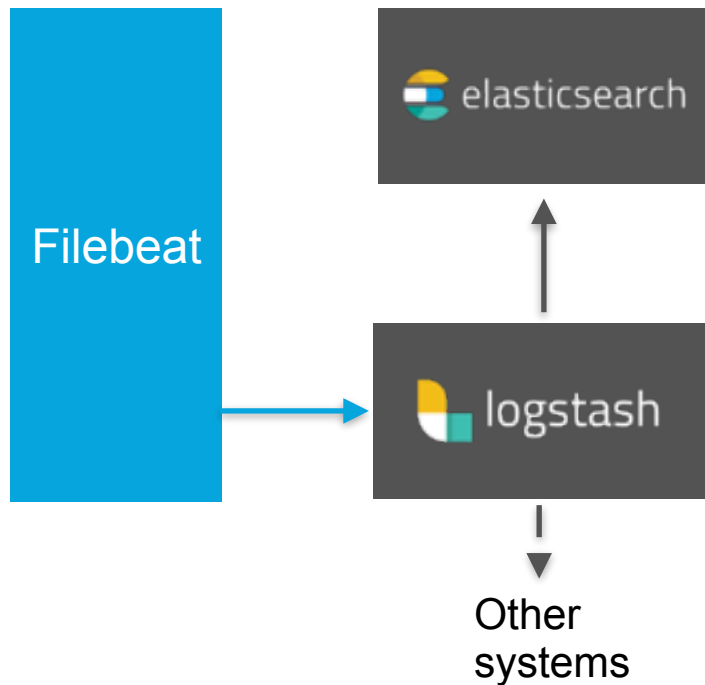
```
2016/02/09 21:20:42.414572 client.go:257: WARN Can not index event (status=400):
2 105 110 103 95 101 120 99 101 112 116 105 111 110 34 44 34 114 101 97 115 111 1
16 104 32 102 97 105 108 117 114 101 115 32 123 91 109 97 112 112 101 114 32 91 1
2 32 100 105 102 102 101 114 101 110 116 32 116 121 112 101 44 32 99 117 114 114
114 103 101 100 95 116 121 112 101 32 91 100 111 117 98 108 101 93 93 125 34 125]
2016/02/09 21:20:42.414805 single.go:135: DBG send completed
2016/02/09 21:20:42.414833 output.go:87: DBG output worker: publish 50 events
2016/02/09 21:20:42.416692 bulkapi.go:131: DBG Sending bulk request to http://lo
2016/02/09 21:20:42.427488 single.go:135: DBG send completed
2016/02/09 21:20:42.427526 output.go:87: DBG output worker: publish 50 events
2016/02/09 21:20:42.429343 bulkapi.go:131: DBG Sending bulk request to http://lo
2016/02/09 21:20:42.472419 client.go:257: WARN Can not index event (status=400):
2 105 110 103 95 101 120 99 101 112 116 105 111 110 34 44 34 114 101 97 115 111 1
16 104 32 102 97 105 108 117 114 101 115 32 123 91 109 97 112 112 101 114 32 91 1
114 101 110 116 32 116 121 112 101 44 32 99 117 114 114 101 110 116 95 116 121 1
121 112 101 32 91 100 111 117 98 108 101 93 93 125 34 125]
2016/02/09 21:20:42.472656 single.go:135: DBG send completed
2016/02/09 21:20:42.472679 output.go:87: DBG output worker: publish 50 events
2016/02/09 21:20:42.474100 bulkapi.go:131: DBG Sending bulk request to http://lo
2016/02/09 21:20:42.482476 single.go:135: DBG send completed
2016/02/09 21:20:42.482513 output.go:87: DBG output worker: publish 50 events
2016/02/09 21:20:42.484328 bulkapi.go:131: DBG Sending bulk request to http://lo
2016/02/09 21:20:42.499058 single.go:135: DBG send completed
2016/02/09 21:20:42.499152 output.go:87: DBG output worker: publish 50 events
2016/02/09 21:20:42.503488 bulkapi.go:131: DBG Sending bulk request to http://lo
2016/02/09 21:20:42.520429 single.go:135: DBG send completed
2016/02/09 21:20:42.520605 output.go:87: DBG output worker: publish 50 events
2016/02/09 21:20:42.522417 bulkapi.go:131: DBG Sending bulk request to http://lo
2016/02/09 21:20:42.537352 single.go:135: DBG send completed
2016/02/09 21:20:42.885891 output.go:87: DBG output worker: publish 22 events
2016/02/09 21:20:42.886780 bulkapi.go:131: DBG Sending bulk request to http://lo
2016/02/09 21:20:42.894049 single.go:135: DBG send completed
^C2016/02/09 21:20:47.311827 service.go:30: DBG Received sigterm/sigint, stoppin
2016/02/09 21:20:47.311844 beat.go:300: INFO Start exiting beat
2016/02/09 21:20:47.311852 beat.go:275: INFO Stopping Beat
2016/02/09 21:20:47.311862 beat.go:283: INFO Cleaning up topbeat before shutting
2016/02/09 21:20:47.311868 beat.go:139: INFO Exit beat completed
```

Filebeat: Never lose a log line



Filebeat: Parse logs with Logstash

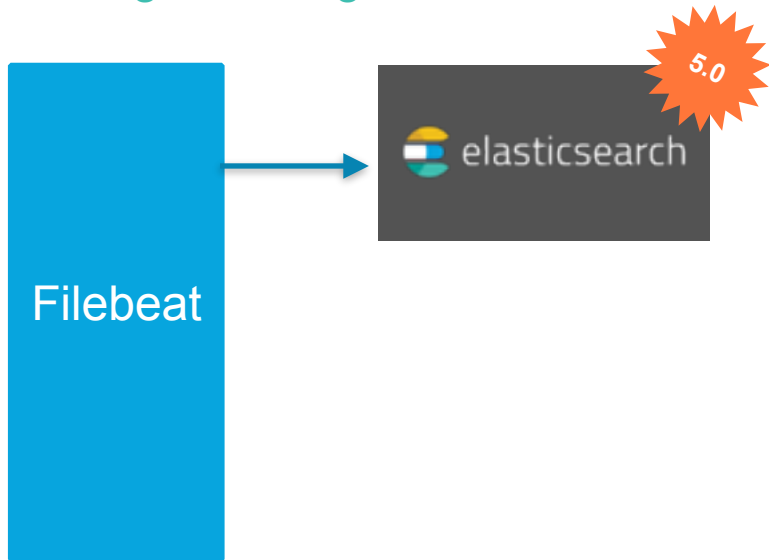
Parse logs with Logstash



- Filebeat sends out unparsed log lines
- Use filters from Logstash to parse the log lines
- Flexible, with conditionals & custom filters
- Forward data to other systems using the Logstash output plugins

Filebeat: Parse logs with Ingest Node

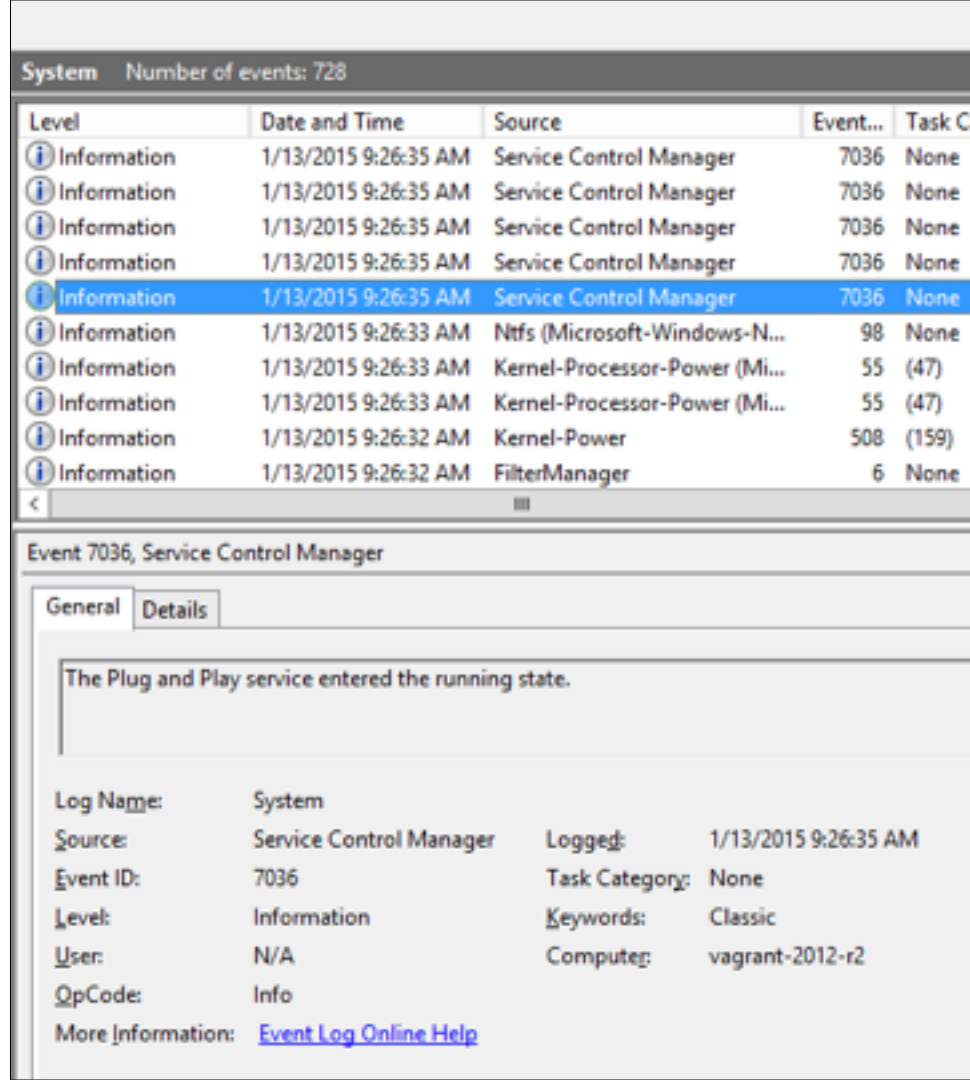
Parse logs with Ingest node in Elasticsearch



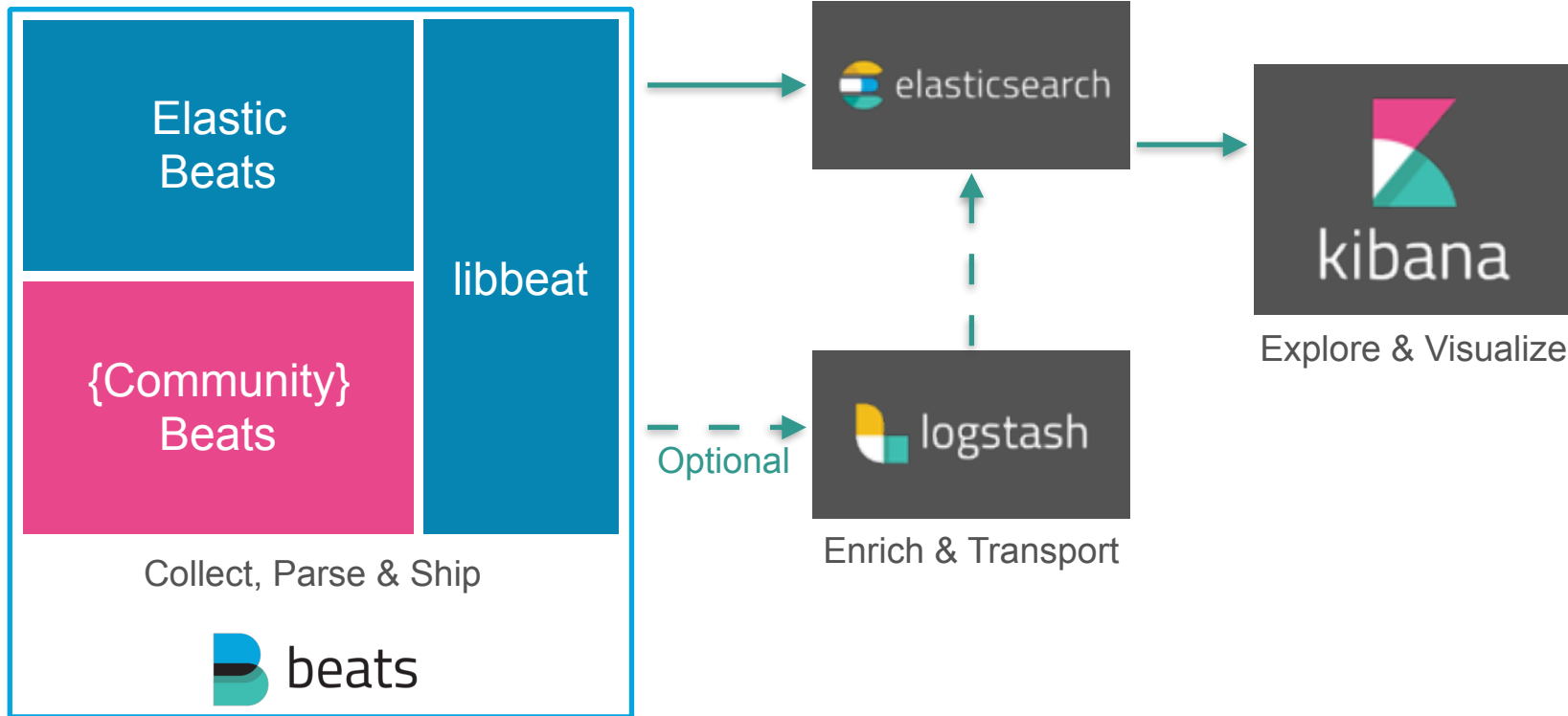
- Filebeat sends out unparsed log lines directly to Elasticsearch
- Use Ingest Node processors (grok, geoip...) to parse the log lines
- Easier to setup

Winlogbeat

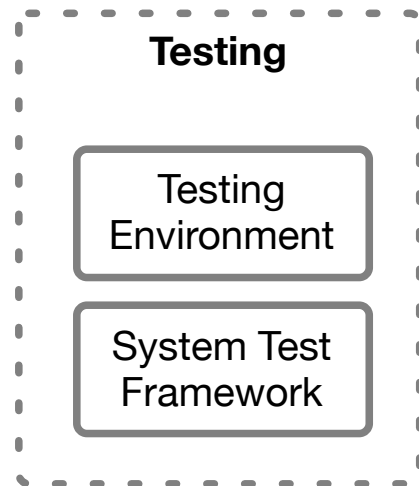
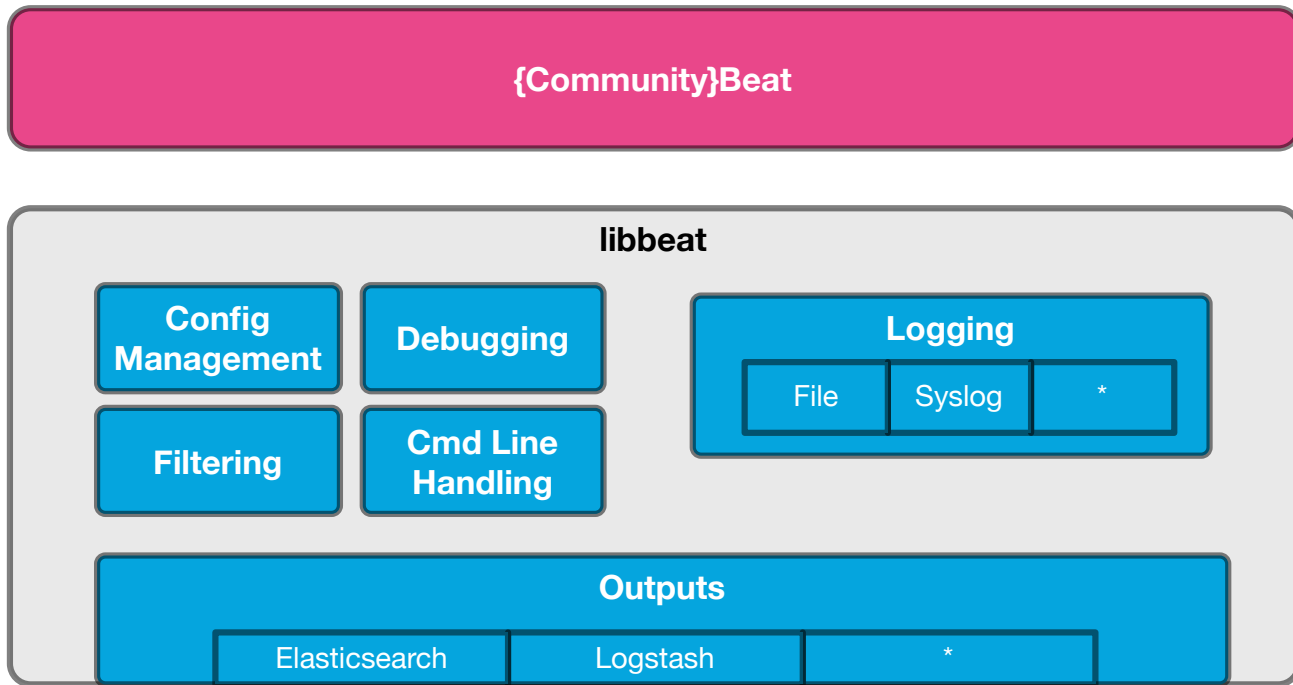
Forwards Windows Event logs
to Elasticsearch



Beats Platform



Architecture Overview - libbeat



Beats Packer

Produces RPMs, DEBs, ...

<https://github.com/elastic/beats-packer>



Super-Sound-Single **45** rpm

**Disco-
Remix**

THE WHISPERS

RCA

And The Beat Goes On 7:30
Side 1

Can You Do The Boogie 6:07
Side 2

FC 1895





topbeat, packetbeat and soundbeat

<https://github.com/dadoonet/soundbeat>





thanks!

<https://github.com/dadoonet/soundbeat>

