Monitoring All the Things! on your Linux system with the Elastic Stack

Joshua Rich
Principal Support Engineer, Elastic
linux.conf.au 2018 Sysadmin Miniconf
Agenda

What we will discuss today :) 

1. About the Elastic Stack
2. About Metricbeat
3. Elasticsearch for metrics?
4. Quick walkthrough of Metricbeat
5. Where to go from here...
What is the Elastic Stack?

Kibana gives shape to your data and is the extensible user interface for configuring and managing all aspects of the Elastic Stack.

Elasticsearch is a distributed, JSON-based search and analytics engine designed for horizontal scalability, maximum reliability, and easy management.

Beats is a platform for lightweight shippers (note: plural) that send data from edge machines to Logstash and Elasticsearch.

Logstash is a dynamic data collection pipeline with an extensible plugin ecosystem.
What is Metricbeat?

- One of many shippers built on the Beats platform
- Reads from local data sources
- Sends data to Elasticsearch or Logstash or Redis
- Deploy once per server, consume many local services
- Single binary and a few config files
- Docker ready!
What can Metricbeat monitor?
A lot of things...

<table>
<thead>
<tr>
<th></th>
<th>Apache</th>
<th>Ceph</th>
<th>Couchbase</th>
<th>Docker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Etcd</td>
<td>HAPerxy</td>
<td>Kafka</td>
<td>Memcached</td>
<td></td>
</tr>
<tr>
<td>MongoDB</td>
<td>MySQL</td>
<td>Nginx</td>
<td>PHP-FPM</td>
<td></td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>RabbitMQ</td>
<td>Redis</td>
<td>System*</td>
<td></td>
</tr>
</tbody>
</table>

This is just a sample of, full list here:

The Metricbeat System Module

What it monitors:

• CPU usage statistics totals and per core breakdown, system load
• Filesystem usage and statistics (no. of files, used/free)
• Disk IO totals and per device
• Memory usage (total and free/used)
• Network IO totals and per device breakdown
• Per process statistics (can be filtered)
• TCP sockets
• Uptime
I can use Elasticsearch for metrics?

Isn’t Elasticsearch for text search, not number search?

Everybody. All the time.
Elasticsearch Loves Numbers!

<table>
<thead>
<tr>
<th>Storage</th>
<th>Search</th>
<th>Management</th>
</tr>
</thead>
</table>
| • BKD-tree data structures for numeric types  
• Range data types for storing a value range  
• Half-float and scaled-float data types for confined numeric ranges  
• Sparse field storage improvements  
• Index sorting | • Per shard query and filter cache  
• Query rewriting to avoid shards that don't match | • Rollover API for ease of retention requirements  
• Shrink/Split APIs for helping with data growth  
• Reindex API and Ingest Node to help with data management |
TSVB In Kibana makes for lovely metric visualisations!
Walkthrough: Monitoring your Linux System Stats

with Elasticsearch, Kibana and Metricbeat
Start Elasticsearch and Kibana

Let’s use Docker containers for easy deploy:

# Start Elasticsearch:
docker run -p 9200:9200 -p 9300:9300 \
  -e "discovery.type=single-node" \
  --name elasticsearch \
  docker.elastic.co/elasticsearch/elasticsearch-oss:6.1.1

# Start Kibana:
docker run -p 5601:5601 \
  --name kibana --link elasticsearch \
  docker.elastic.co/kibana/kibana-oss:6.1.1
Start Metricbeat
Let’s use Docker containers for easy deploy:

```bash
# Start Metricbeat:
# docker run \
#  --volume="/proc:/hostfs/proc:ro" \n#  --volume="/sys/fs/cgroup:/hostfs/sys/fs/cgroup:ro" \n#  --volume="/:/hostfs:ro" \n#  --net=host --name metricbeat \n#  docker.elastic.co/beats/metricbeat:6.1.1 \n#  -system.hostfs=/hostfs -E \n#  output.elasticsearch.hosts="[http://localhost:9200]" \n#  -setup

# Note: no need to pass -setup on future runs...
```
Open http://localhost:5601 & view the pretty dashboards
Where do you go from here?
Listen to the beat of all your infrastructure...

Install
- Metricbeat on all your servers.
- Separate Elasticsearch and Kibana servers.

Configure
- Configure Metricbeat on each server according to the services it runs.
- Configure all Metricbeat instances to index to Elasticsearch.

Visualise
- Run Metricbeat setup to import the dashboards once only.
- Visualise, monitor and explore your servers and services in a central web UI.
But we can go further...
“Full Stack” Example

Dockerized Elastic+Web+DB Stack

- Elasticsearch, Kibana:
  - System stats
  - Docker stats (i.e., everything here)
- + Filebeat monitoring:
  - Apache/Nginx error/access logs
  - MySQL error/slow logs
  - System logs
- + Packetbeat monitoring:
  - ICMP, DNS, HTTP and MySQL traffic
  - TCP flows
- + Heartbeat monitoring:
  - ICMP
  - Apache, Nginx, MySQL, Kibana, Elasticsearch health checks
See what’s possible:

github.com/elastic/examples/tree/master/Miscellaneous/docker/full_stack_example
References

Explore the topics covered in this presentation!

- https://www.elastic.co/blog/minimize-index-storage-size-elasticsearch-6-0
- https://www.elastic.co/blog/index-sorting-elasticsearch-6-0
- https://www.elastic.co/guide/en/elasticsearch/reference/current/number.html#_which_type_should_i_use
- https://github.com/elastic/examples/tree/master/Miscellaneous/docker/full_stack_example

We ❤️ our open-source community: www.elastic.co/community

Contact me:

@devopswannabe

www.linkedin.com/in/joshuarichau