Transparent Check_MK history using Elasticsearch

Fabian Binder & Rika Denia, comNET GmbH
Fabian Binder
At comNET since 2013
Check_MK since 2015
IT-Services, Reporting, Development, Boxenluder
Rika Denia
At comNET since 2015
Expert for open source technologies
Elasticsearch, Big Data, OTRS, Linux
1. What is Elasticsearch?

2. How do we use Elasticsearch?

3. How do we monitor Elasticsearch?
1. What is Elasticsearch?

Data store & search engine
- NoSQL
- Document-based
- RESTful access

Data collection
- Syslog, SNMP, RMQ, XMPP, …
- Flexible matching and filtering

Frontend
- Web based analysis tool
- The main frontend
- Very powerful, still easy to use
What is Elasticsearch?
How do we use Elasticsearch?

Hi! Users report that some applications are slow! Can you get me a top 10 list of the hosts that had the highest CPU utilization recently?

(Hint: Yes we can!)
What is Elasticsearch?

Filebeat
Log-Dateien

Metricbeat
Metriken

Packetbeat
Netzwerkdaten

Winlogbeat
Windows-Ereignisanzeige

Auditbeat
Audit Data

Heartbeat
Uptime Monitoring
The solution: CMKBeat
CMKBeat

- [https://github.com/comnetgmbh/cmkbeat](https://github.com/comnetgmbh/cmkbeat)
- Written in GO
- Retrieves information via livestatus queries
- Forwards results to Elasticsearch
Check Results

Check_MK

Livestatus request (6557)

CMKBeat & Elasticsearch
CMKBeat Configuration

• Configuration via yml File

cmkbeat:
  # How often to query livestatus for data. The default is 30s.
  period: 30s

  # The host and port where livestatus is listening.
  cmkHost: "10.0.0.10:6557"

  # Which livestatus table to query
  query: "services"
Running CMKBeat

cmkbeat start running.

-----Config------
Host: 10.0.0.10:6557
Query: services
Columns: [host_name display_name state plugin_output ...]
Filter: []
Metrics: true

-------------
73 events submitted in 20.451469ms.
Demo!
ELK / „Anwendung“

„Datenbank“

virt1

cmkbeat
Monitoring Elasticsearch

- [https://github.com/comnetgmbh/check_elasticsearch](https://github.com/comnetgmbh/check_elasticsearch)
- Collect Elasticsearch stats via REST API
- Availability of shards and clusters
- Performance (latency / timeouts)
- Size and growth of indices
Check via REST API

Check_MK

Elasticsearch
Live demo!
Questions?