CONTENT

● Helvetia Insurance
● OpenShift Adoption

● Metrics
● Visualization
● Applications
● Alerting

● Demo/Q&A
WHO WE ARE

- Swiss insurance company
- Founded in 1858
- Operate in Switzerland + Europe
- 5 billion market capitalisation
- > 6’500 employees
- > 5’000’000 customers

- ~ 400 IT employees
- IT strategy focus on cloud and containers
OPENSHEET ADOPTION
SETUP

Frankfurt (eu-central-1)

Virtual Private Cloud

Master Nodes
Infra Nodes
App Nodes

RED HAT OPENSHIFT

Amazon S3
Amazon EFS
Amazon EBS
Amazon RDS

AWS Direct Connect

Helvetia

Firewall
Benutzer

3rd party
dynatrace
MONITORING STACK
METRICS
EXPORTERS
**THANOS DATA RETENTION**

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>Prometheus</th>
<th>Thanos</th>
<th>Thanos / AWS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retention</td>
<td>2 days</td>
<td>2 weeks</td>
<td>6 months</td>
</tr>
<tr>
<td>Granularity</td>
<td>full</td>
<td>full</td>
<td>reduced to 5 minutes</td>
</tr>
<tr>
<td>Storage</td>
<td>EBS 0.36 USD *</td>
<td>S3 Standard 0.0245 USD *</td>
<td>S3 Standard IA 0.0135 USD *</td>
</tr>
</tbody>
</table>

* current AWS pricing for GB/month (Frankfurt)

- Compactor: Define retention and downsampling of metrics data
- AWS S3: Move older downsampled metrics data to cold storage
DASHBOARDS

- **OpenShift**
  - Cluster and node health
  - Etcd health
  - HAProxy metrics
  - Endpoint probes
  - Capacity overview

- **AWS**
  - EC2, ELB, EBS, EFS, RDS, ..

- **Others**
  - Kafka Broker/Zookeeper
DASHBOARDS
APPLICATIONS
DYNATRACE
ALERTING
SLACK

- Slack
- Dynatrace
- Splunk
- Ansible
- Grafana
- CloudWatch
- Prometheus

#redhat #rhsummit
rules:
- alert: "CPU High"
  expr: (100 - (avg by (instance, descriptiveinstance)
  (irate(node_cpu{job="kubernetes-nodes-exporter",mode=
  "idle"}[5m])) * 100)) > 80
  for: 5m
  annotations:
    miqTarget: "ContainerNode"
    severity: "WARN"
    identifier: "{{ $labels.descriptiveinstance }}"
  description: "Node
  {{labels.descriptiveinstance}} has high CPU consumption > 80%. Current used CPU is {{ $value }}
  ""
CLOUDWATCH ALERTS

ELB Master Internal Unhealthy for Prod

ELB Master External Unhealthy for Prod

ELB Infra External Unhealthy for Prod

efs-prod-encrypted-backup-ReadCapacityUnits

UnHealthyHostCount > 0 für 3 Datenpunkte innerhalb einer Minute

ConsumedReadCapacityUnits >= 48 für 5 Datenpunkte innerhalb einer Minute

#redhat #rhsummit
LOG-BASED ALERTS

[Splunk APP 09:00]
[UserOperator-DEVL] has encountered errors.

[HCP: Kafka DEVL - User Operator - Errors]
Show results in Splunk

[Splunk APP 12:02]
[TopicOperator-DEVL] has encountered errors.

[HCP: Kafka DEVL - Topic Operator - Errors]
Show results in Splunk
SUMMARY
FUTURE PLANS

- Upgrade to OpenShift 3.11
- Using Prometheus Cluster Operator
- Using Dynatrace Operator
- Using Grafana alerts
- Integrate custom solutions
DEMO/Q&A
THANK YOU

linkedin.com/company/Red-Hat
youtube.com/user/RedHatVideos
facebook.com/RedHatinc
twitter.com/RedHat
BACKUP
EXPORTERS

● node-exporter
  ○ Prometheus exporter for hardware and OS metrics exposed by *NIX kernels
  ○ https://github.com/prometheus/node_exporter

● kube-state-metrics
  ○ Listen to Kubernetes API server and generate metrics about state of objects
  ○ https://github.com/kubernetes/kube-state-metrics

● blackbox-exporter
  ○ Allows blackbox probing of endpoints over HTTP, HTTPS, DNS, TCP and ICMP
  ○ https://github.com/prometheus/blackbox_exporter
config.yml

modules:
dns_udp:
dns:
    preferred_ip_protocol: ip4
    query_name: www.helvetia.ch
    query_type: A
    valid_rcodes:
    - NOERROR
    validate_answer_rrs:
        fail_if_not_matches_regexp:
        - "www.helvetia.ch.t900.tIN.tA\111.22.333.444"
    prober: dns
    timeout: 5s

#redhat #rhsummit
DASHBOARDS
global:
    slack_api_url: 'https://hooks.slack.com/services/token'

route:
    receiver: default-receiver

receivers:
- name: default-receiver
  slack_configs:
    - title: '{{ template "custom_title" . }}'
      text: '{{ template "custom_slack_message" . }}'
      title_link: 'https://yourdomain.com/alerts?receiver=default-receiver'
      send_resolved: true

templates:
- /alertmanager/templates/slack.tmpl