RED HAT SUMMIT

HYBRID CLOUD MONITORING

Hybrid Cloud Monitoring on AWS and Red Hat OpenShift

Tobias Denzler
Solution Architect
Helvetia Insurance

Mattia Mascia
Senior Consultant
Red Hat

Codrin Bucur
Principal Architect
Red Hat

Boston
May 9th 2019

CONTENT

- Helvetia Insurance
- OpenShift Adoption

- Metrics
- Visualization
- Applications
- Alerting

- Demo/Q&A

WHO WE ARE

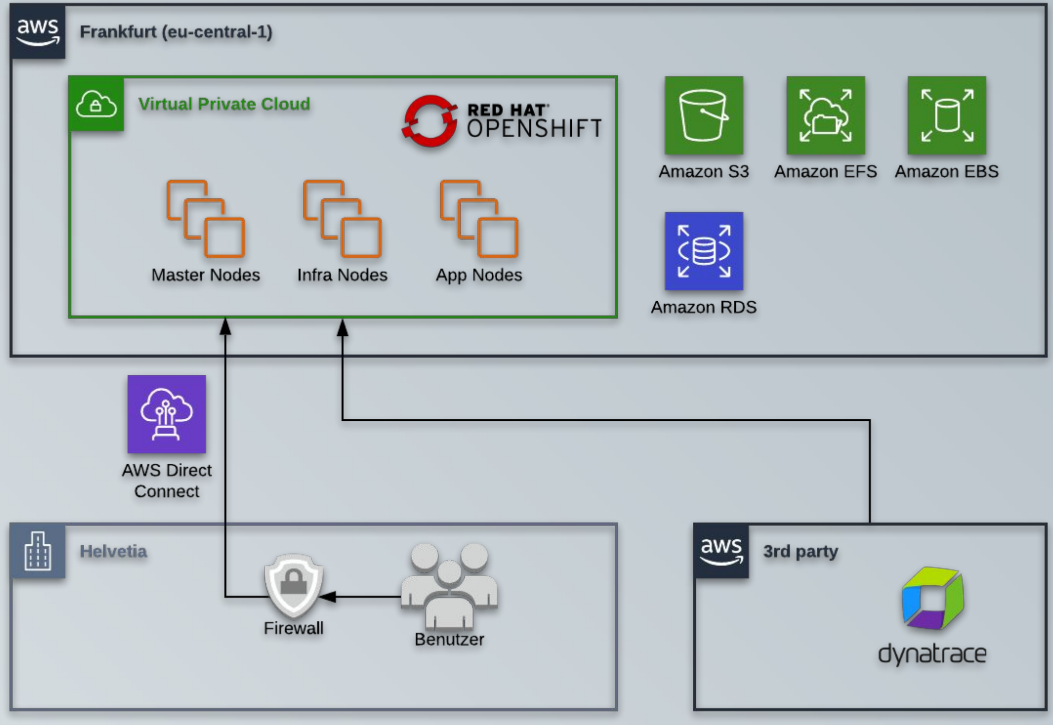
- Swiss insurance company
- Founded in 1858
- Operate in Switzerland + Europe
- 5 billion market capitalisation
- > 6’500 employees
- > 5’000’000 customers

- ~ 400 IT employees
- IT strategy focus on cloud and containers

helvetia

OPENSHIFT ADOPTION

SETUP



Frankfurt (eu-central-1)
Virtual Private Cloud
RED HAT OPENSHIFT
Master Nodes
Infra Nodes
App Nodes
Amazon S3
Amazon EFS
Amazon EBS
Amazon RDS
AWS Direct Connect
Helvetia
Firewall
Benutzer
3rd party
dynatrace

OVERVIEW

MONITORING STACK

THORNTAIL

JBoss by Red Hat

spring boot

dynatrace

RED HAT OPENSHIFT

kubernetes

etcd

splunk>

HAPROXY

kafka

Prometheus

amazon web services

EC2

ELB

EBS

EFS

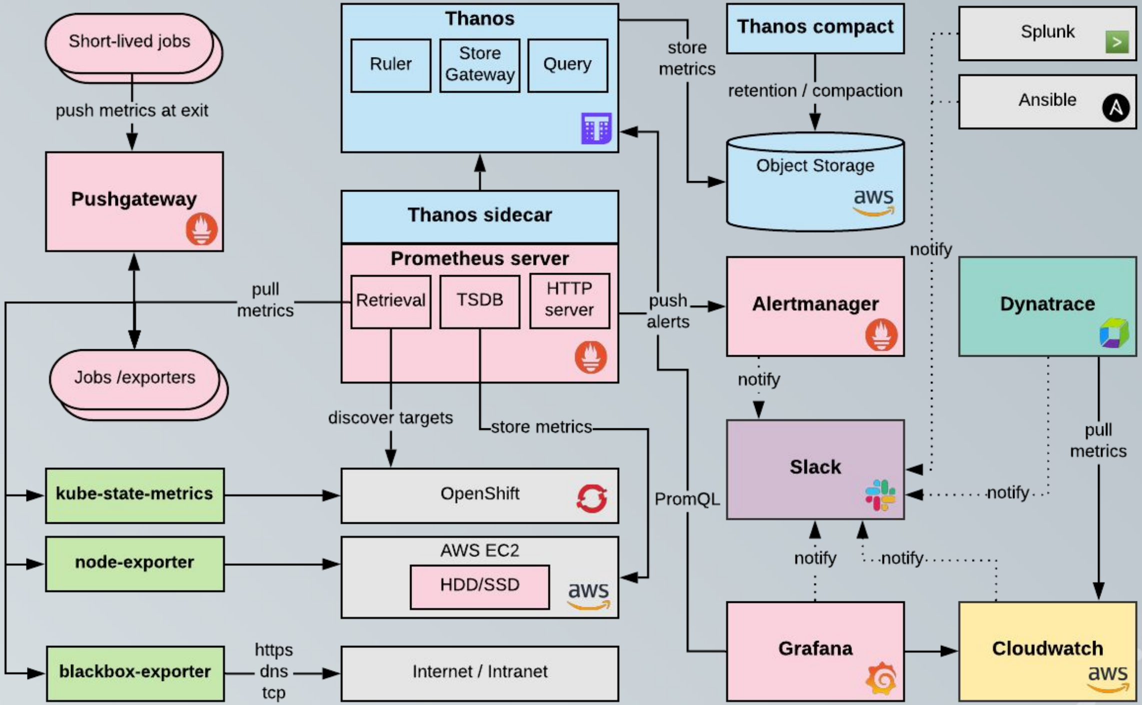
S3

VPC

RDS

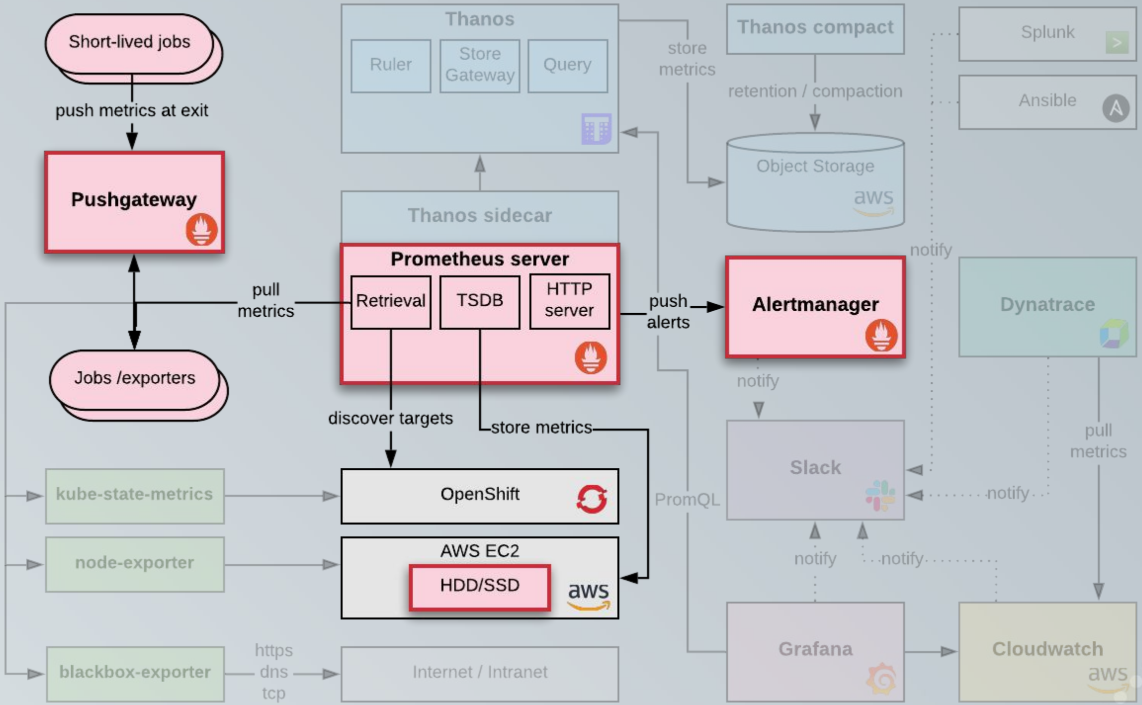
CloudWatch

HOW DO WE MONITOR



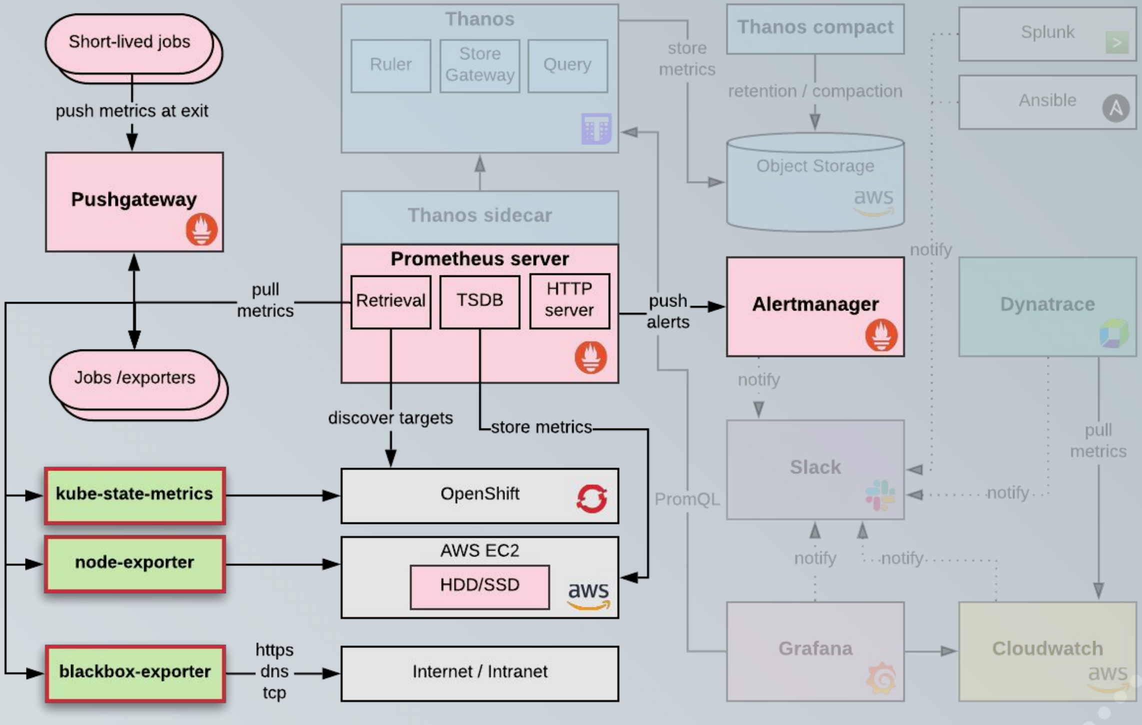
METRICS

PROMETHEUS

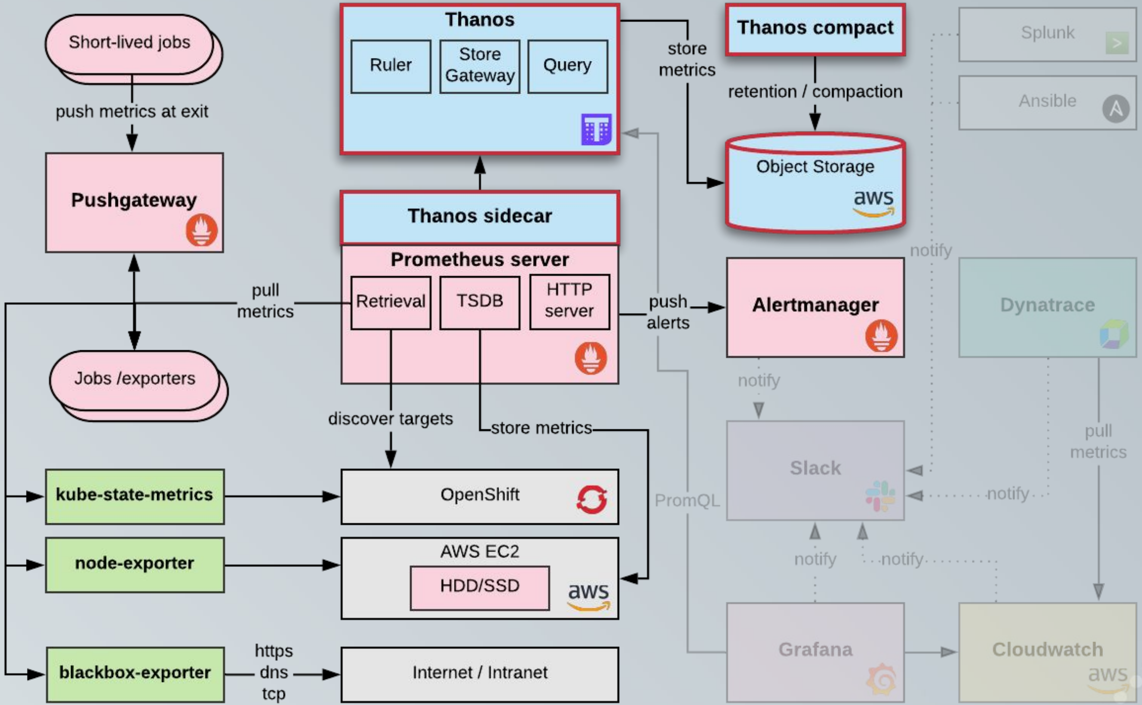


Short-lived jobs
push metrics at exit
Pushgateway
pull
metrics
Jobs /exporters
Thanos
Ruler
Store
Gateway
Query
Thanos sidecar
Prometheus server
Retrieval
TSDB
HTTP
server
discover targets
store metrics
store
metrics
Thanos compact
retention / compaction
Object Storage
aws
push
alerts
Alertmanager
notify
Splunk
Ansible
Dynatrace
notify
Slack
pull
metrics
notify
PromQL
notify
notify
kube-state-metrics
OpenShift
node-exporter
AWS EC2
HDD/SSD
aws
blackbox-exporter
https
dns
tcp
Internet / Intranet
Grafana
Cloudwatch
aws

EXPORTERS

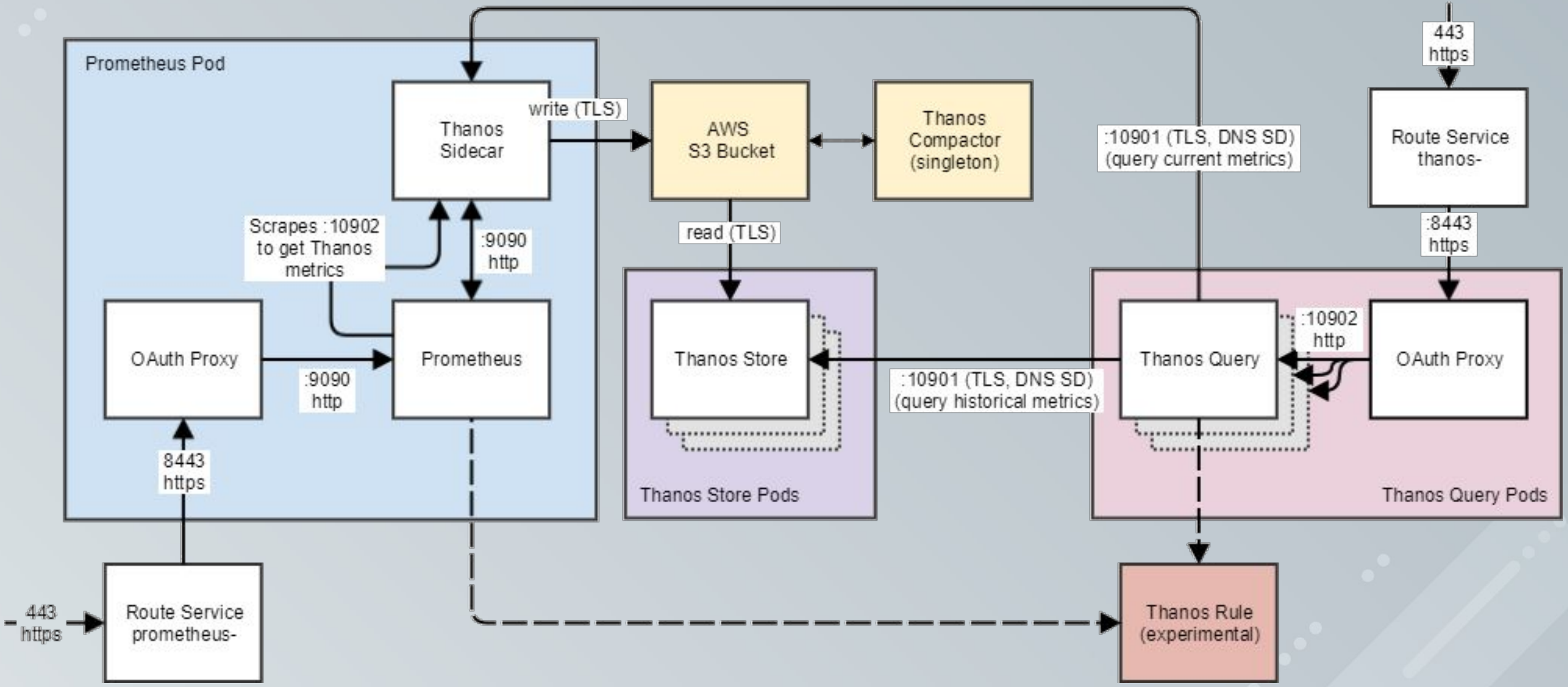

Short-lived jobs
push metrics at exit
Pushgateway
Jobs /exporters
pull
metrics
Thanos
Ruler
Store
Gateway
Query
Thanos sidecar
Prometheus server
Retrieval
TSDB
HTTP
server
discover targets
store metrics
kube-state-metrics
node-exporter
blackbox-exporter
https
dns
tcp
OpenShift
AWS EC2
HDD/SSD
aws
Internet / Intranet
store
metrics
Thanos compact
retention / compaction
Object Storage
aws
push
alerts
Alertmanager
notify
Slack
PromQL
notify
notify
Grafana
Cloudwatch
aws
Splunk
Ansible
notify
Dynatrace
notify
pull
metrics

THANOS



Short-lived jobs
push metrics at exit
Pushgateway
pull metrics
Jobs /exporters
Thanos
Ruler
Store Gateway
Query
Thanos sidecar
Prometheus server
Retrieval
TSDB
HTTP server
store metrics
Thanos compact
retention / compaction
Object Storage
aws
push alerts
Alertmanager
discover targets
store metrics
kube-state-metrics
OpenShift
node-exporter
AWS EC2
HDD/SSD
aws
blackbox-exporter
https
dns
tcp
Internet / Intranet
Splunk
Ansible
notify
Dynatrace
notify
Slack
pull metrics
notify
PromQL
notify
notify
Grafana
Cloudwatch
aws

THANOS COMPONENTS



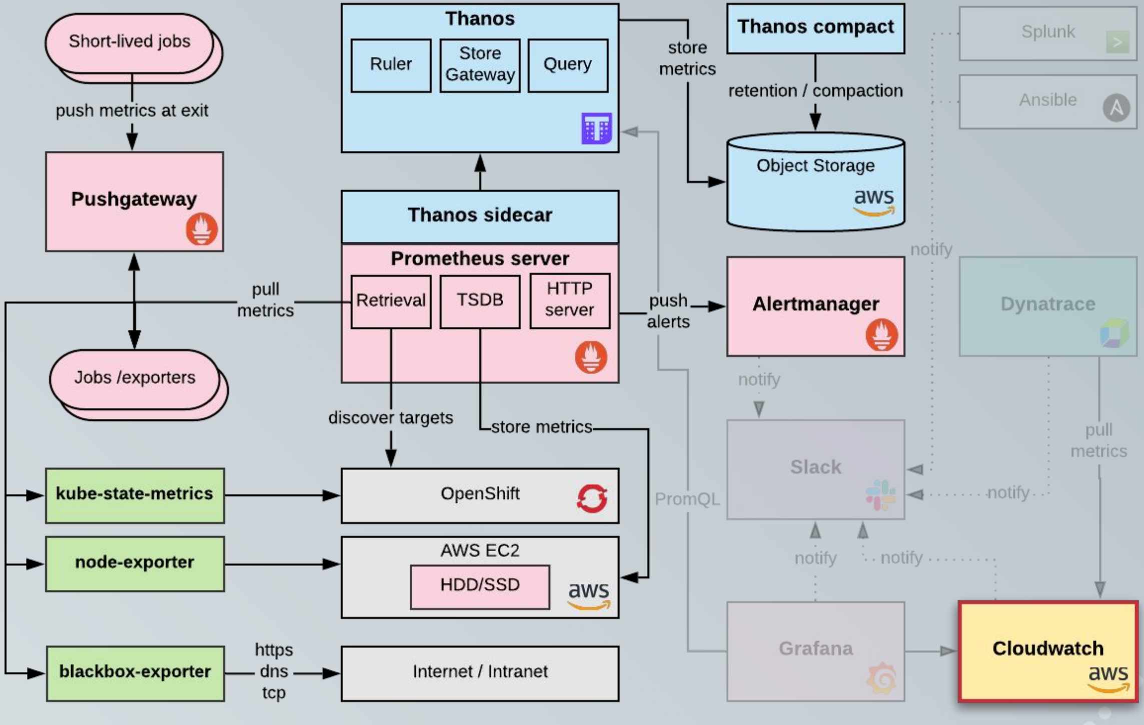
THANOS DATA RETENTION

Responsibility	Prometheus	Thanos		Thanos / AWS	
Retention	2 days	2 weeks	6 months		years
Granularity	full	full	reduced to 5 minutes		reduced to 1 hour
Storage	EBS 0.36 USD *	S3 Standard 0.0245 USD *		S3 Standard IA 0.0135 USD *	S3 Glacier 0.0045 USD *

* 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

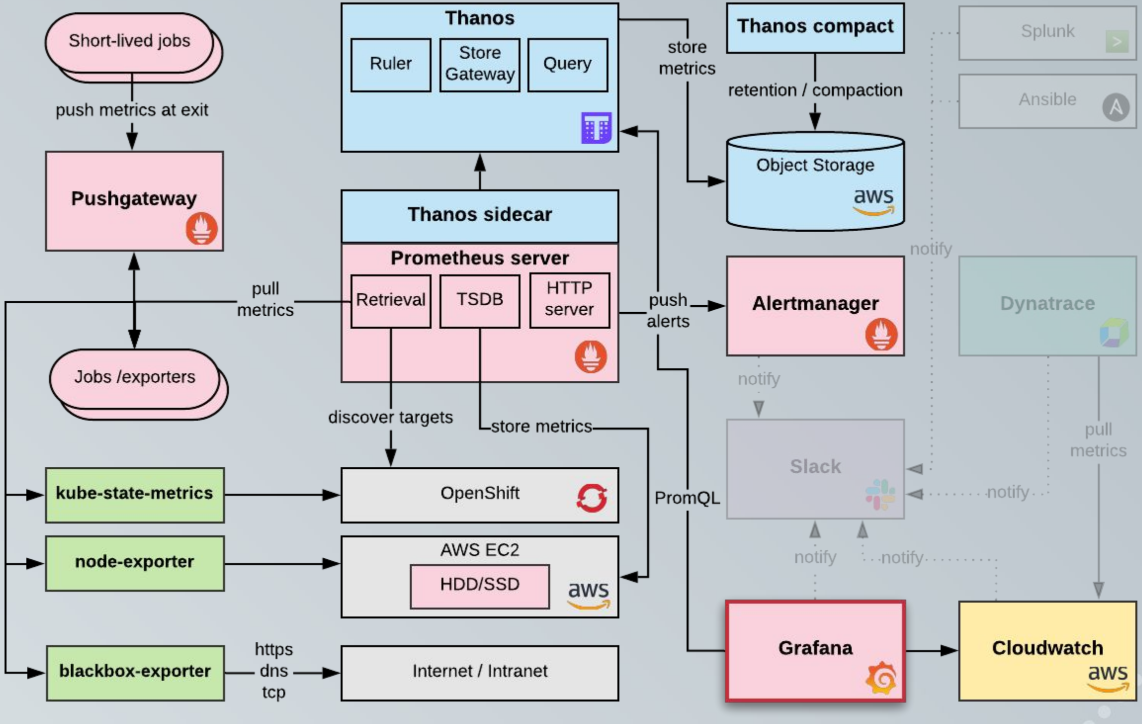
CLOUDWATCH



Short-lived jobs
push metrics at exit
Pushgateway
Jobs /exporters
pull metrics
Thanos
Ruler
Store Gateway
Query
Thanos sidecar
Prometheus server
Retrieval
TSDB
HTTP server
discover targets
store metrics
kube-state-metrics
node-exporter
blackbox-exporter
OpenShift
AWS EC2
HDD/SSD
aws
https
dns
tcp
Internet / Intranet
store metrics
Thanos compact
retention / compaction
Object Storage
aws
push alerts
Alertmanager
notify
Slack
PromQL
notify
notify
Grafana
Cloudwatch
aws
Splunk
Ansible
notify
Dynatrace
pull metrics
notify

VISUALIZATION

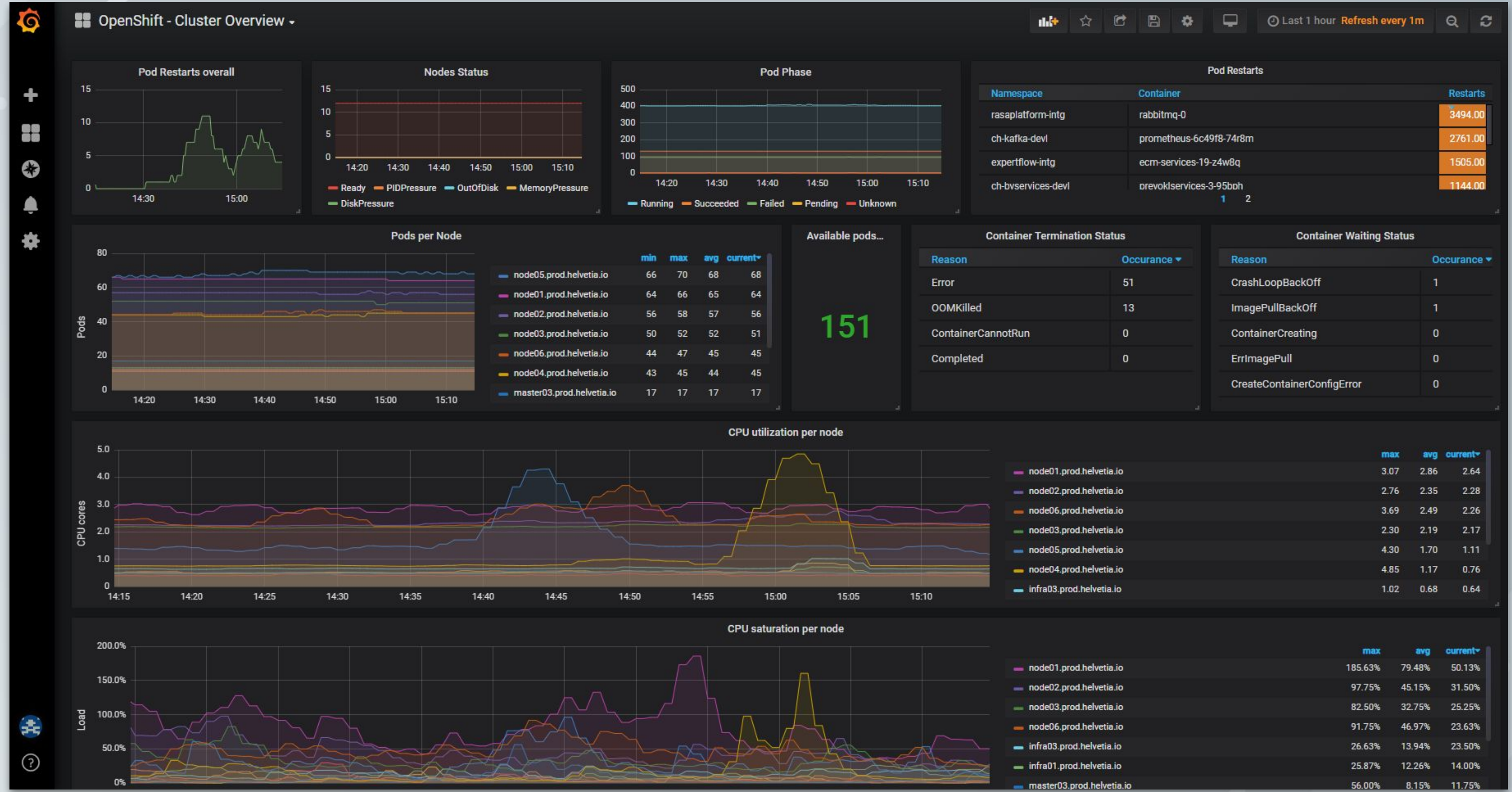
GRAFANA


Short-lived jobs
push metrics at exit
Pushgateway
pull
metrics
Jobs /exporters
Thanos
Ruler
Store Gateway
Query
store
metrics
Thanos compact
retention / compaction
Object Storage
aws
Thanos sidecar
Prometheus server
Retrieval
TSDB
HTTP server
push
alerts
Alertmanager
notify
Splunk
Ansible
Dynatrace
discover targets
store metrics
notify
Slack
pull
metrics
notify
kube-state-metrics
OpenShift
PromQL
node-exporter
AWS EC2
HDD/SSD
aws
notify
notify
blackbox-exporter
https
dns
tcp
Internet / Intranet
Grafana
Cloudwatch
aws

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



Pod Restarts

Namespace	Container	Restarts
rasaplatform-intg	rabbitmq-0	3494.00
ch-kafka-devl	prometheus-6c49f8-74r8m	2761.00
expertflow-intg	ecm-services-19-z4w8q	1505.00
ch-bvservices-devl	prevoklservices-3-95bph	1144.00

1 2

Pods per Node

	min	max	avg	current
node05.prod.helvetia.io	66	70	68	68
node01.prod.helvetia.io	64	66	65	64
node02.prod.helvetia.io	56	58	57	56
node03.prod.helvetia.io	50	52	52	51
node06.prod.helvetia.io	44	47	45	45
node04.prod.helvetia.io	43	45	44	45
master03.prod.helvetia.io	17	17	17	17

Container Termination Status

Reason	Occurance
Error	51
OOMKilled	13
ContainerCannotRun	0
Completed	0

Container Waiting Status

Reason	Occurance
CrashLoopBackOff	1
ImagePullBackOff	1
ContainerCreating	0
ErrImagePull	0
CreateContainerConfigError	0

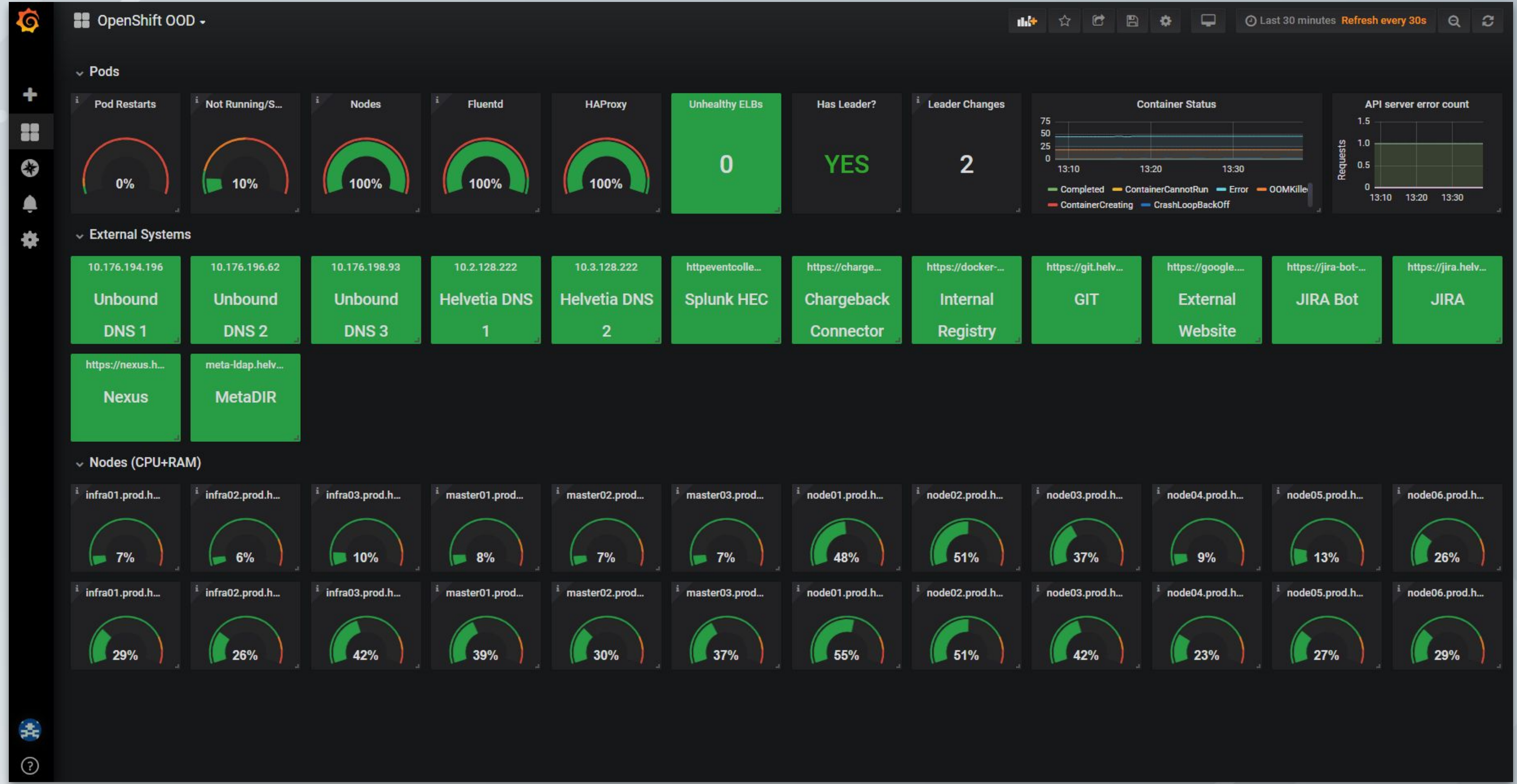
CPU utilization per node

	max	avg	current
node01.prod.helvetia.io	3.07	2.86	2.64
node02.prod.helvetia.io	2.76	2.35	2.28
node06.prod.helvetia.io	3.69	2.49	2.26
node03.prod.helvetia.io	2.30	2.19	2.17
node05.prod.helvetia.io	4.30	1.70	1.11
node04.prod.helvetia.io	4.85	1.17	0.76
infra03.prod.helvetia.io	1.02	0.68	0.64

CPU saturation per node

	max	avg	current
node01.prod.helvetia.io	185.63%	79.48%	50.13%
node02.prod.helvetia.io	97.75%	45.15%	31.50%
node03.prod.helvetia.io	82.50%	32.75%	25.25%
node06.prod.helvetia.io	91.75%	46.97%	23.63%
infra03.prod.helvetia.io	26.63%	13.94%	23.50%
infra01.prod.helvetia.io	25.87%	12.26%	14.00%
master03.prod.helvetia.io	56.00%	8.15%	11.75%

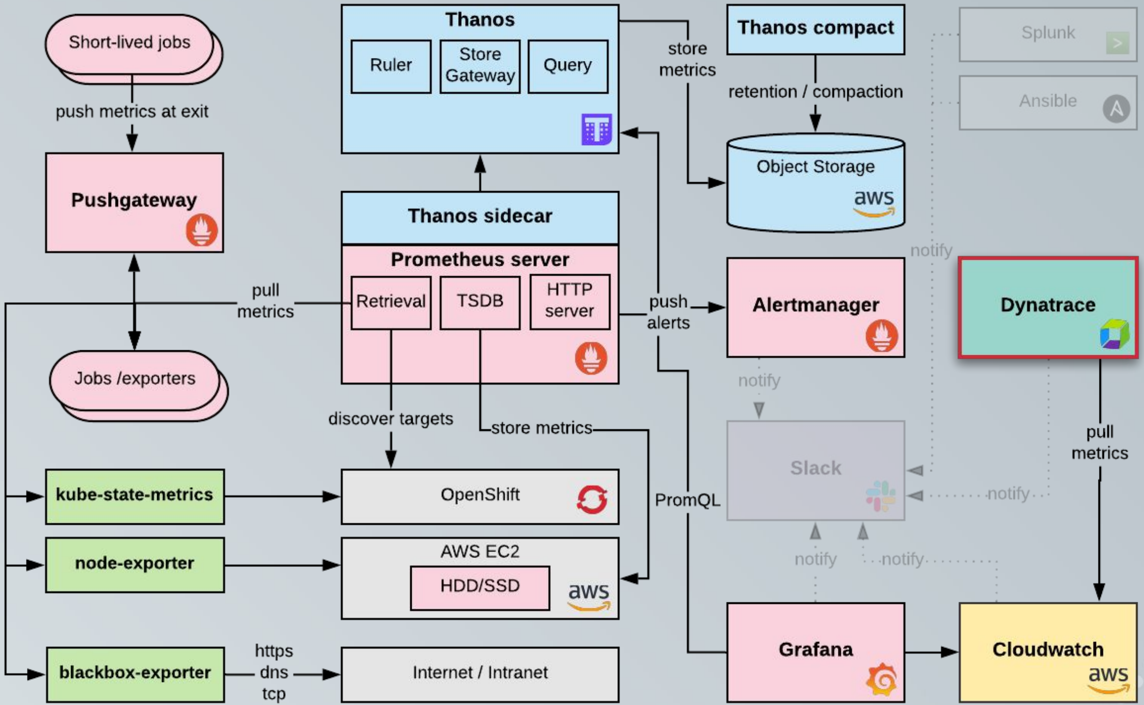
DASHBOARDS



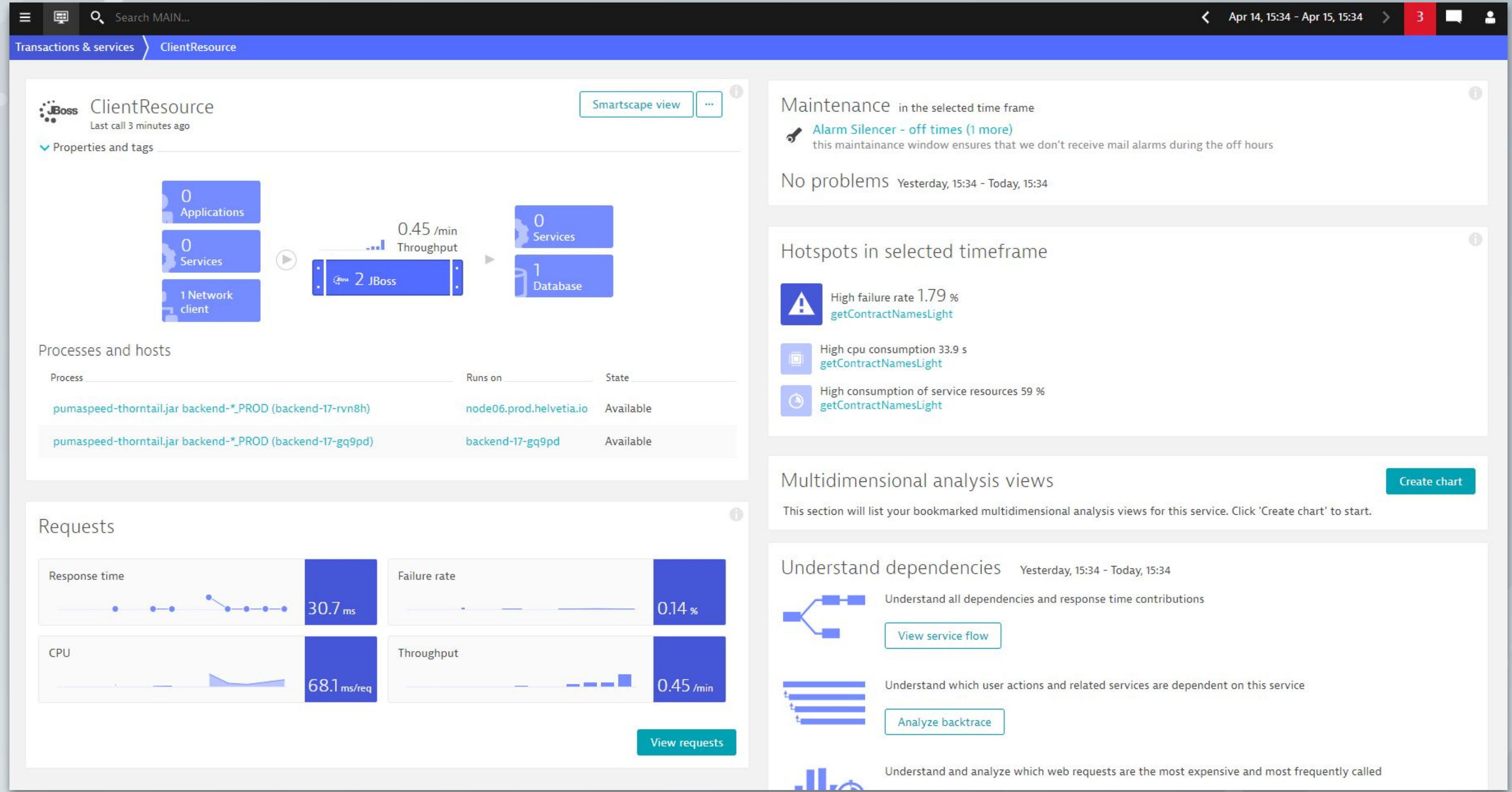
OpenShift OOD
Last 30 minutes Refresh every 30s
Pods
Pod Restarts 0%
Not Running/S... 10%
Nodes 100%
Fluentd 100%
HAProxy 100%
Unhealthy ELBs 0
Has Leader? YES
Leader Changes 2
Container Status
75
50
25
0
13:10
13:20
13:30
Completed
ContainerCannotRun
Error
OOMKille
ContainerCreating
CrashLoopBackOff
API server error count
Requests
1.5
1.0
0.5
0
13:10
13:20
13:30
External Systems
10.176.194.196 Unbound DNS 1
10.176.196.62 Unbound DNS 2
10.176.198.93 Unbound DNS 3
10.2.128.222 Helvetia DNS 1
10.3.128.222 Helvetia DNS 2
httpeventcolle... Splunk HEC
https://charge... Chargeback Connector
https://docker-... Internal Registry
https://git.helv... GIT
https://google.... External Website
https://jira-bot-... JIRA Bot
https://jira.helv... JIRA
https://nexus.h... Nexus
meta-ldap.helv... MetaDIR
Nodes (CPU+RAM)
infra01.prod.h... 7%
infra02.prod.h... 6%
infra03.prod.h... 10%
master01.prod... 8%
master02.prod... 7%
master03.prod... 7%
node01.prod.h... 48%
node02.prod.h... 51%
node03.prod.h... 37%
node04.prod.h... 9%
node05.prod.h... 13%
node06.prod.h... 26%
infra01.prod.h... 29%
infra02.prod.h... 26%
infra03.prod.h... 42%
master01.prod... 39%
master02.prod... 30%
master03.prod... 37%
node01.prod.h... 55%
node02.prod.h... 51%
node03.prod.h... 42%
node04.prod.h... 23%
node05.prod.h... 27%
node06.prod.h... 29%

APPLICATIONS

DYNATRACE


Thanos
Ruler
Store Gateway
Query
Thanos compact
Splunk
Ansible
Short-lived jobs
push metrics at exit
store metrics
retention / compaction
Object Storage
aws
Pushgateway
Thanos sidecar
Prometheus server
Retrieval
TSDB
HTTP server
notify
pull metrics
push alerts
Alertmanager
Dynatrace
Jobs /exporters
notify
discover targets
store metrics
pull metrics
Slack
kube-state-metrics
OpenShift
PromQL
notify
node-exporter
AWS EC2
HDD/SSD
aws
notify
notify
blackbox-exporter
https
dns
tcp
Internet / Intranet
Grafana
Cloudwatch
aws

DYNATRACE



ClientResource

Last call 3 minutes ago

Processes and hosts

Process	Runs on	State
pumaspeed-thorntail.jar backend-*_PROD (backend-17-rvn8h)	node06.prod.helvetia.io	Available
pumaspeed-thorntail.jar backend-*_PROD (backend-17-gq9pd)	backend-17-gq9pd	Available

Requests

Response time	30.7 ms
Failure rate	0.14 %
CPU	68.1 ms/req
Throughput	0.45 /min

Maintenance in the selected time frame

Alarm Silencer - off times (1 more)

this maintainance window ensures that we don't receive mail alarms during the off hours

No problems Yesterday, 15:34 - Today, 15:34

Hotspots in selected timeframe

High failure rate 1.79 %
getContractNamesLight

High cpu consumption 33.9 s
getContractNamesLight

High consumption of service resources 59 %
getContractNamesLight

Multidimensional analysis views

This section will list your bookmarked multidimensional analysis views for this service. Click 'Create chart' to start.

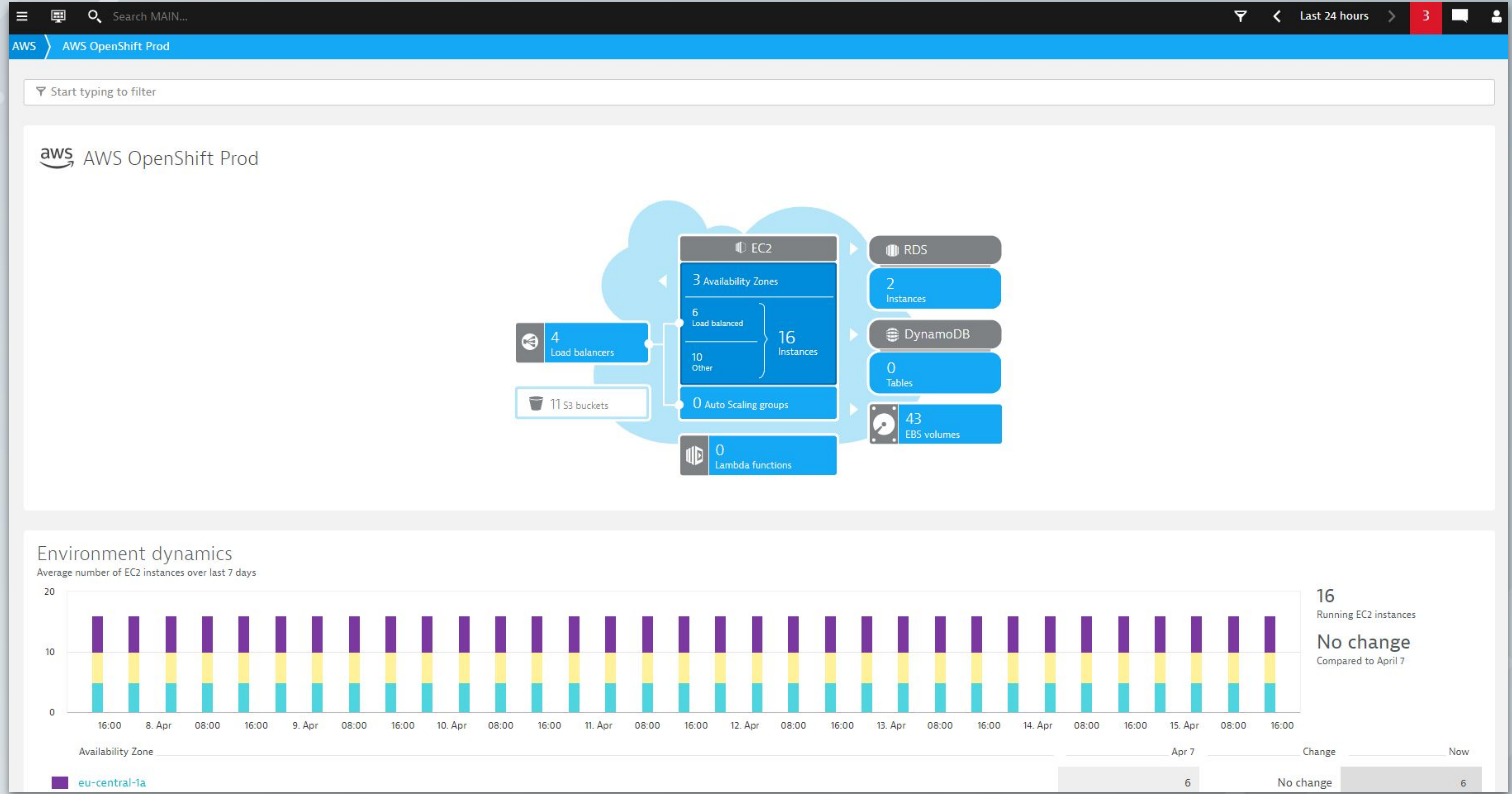
Understand dependencies Yesterday, 15:34 - Today, 15:34

Understand all dependencies and response time contributions

Understand which user actions and related services are dependent on this service

Understand and analyze which web requests are the most expensive and most frequently called

DYNATRACE



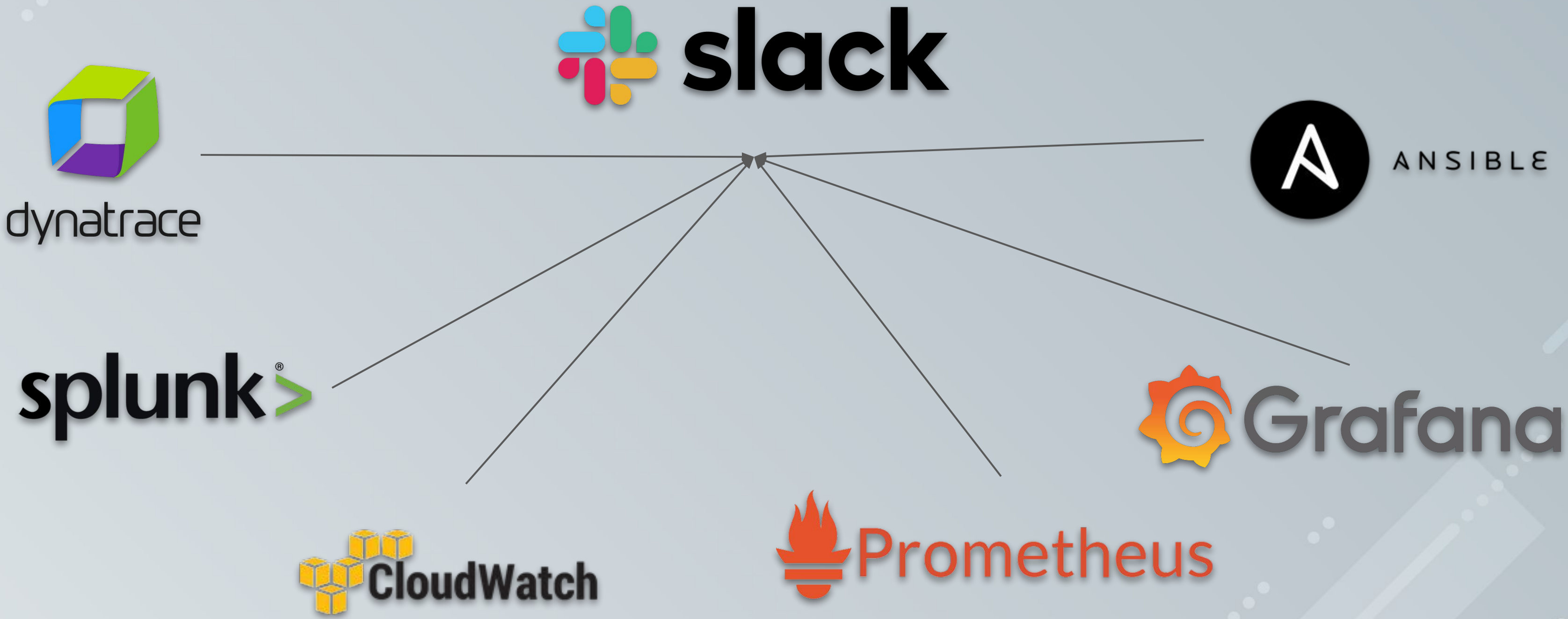
16
Running EC2 instances

No change
Compared to April 7

Availability Zone	Apr 7	Change	Now
▇ eu-central-1a	6	No change	6

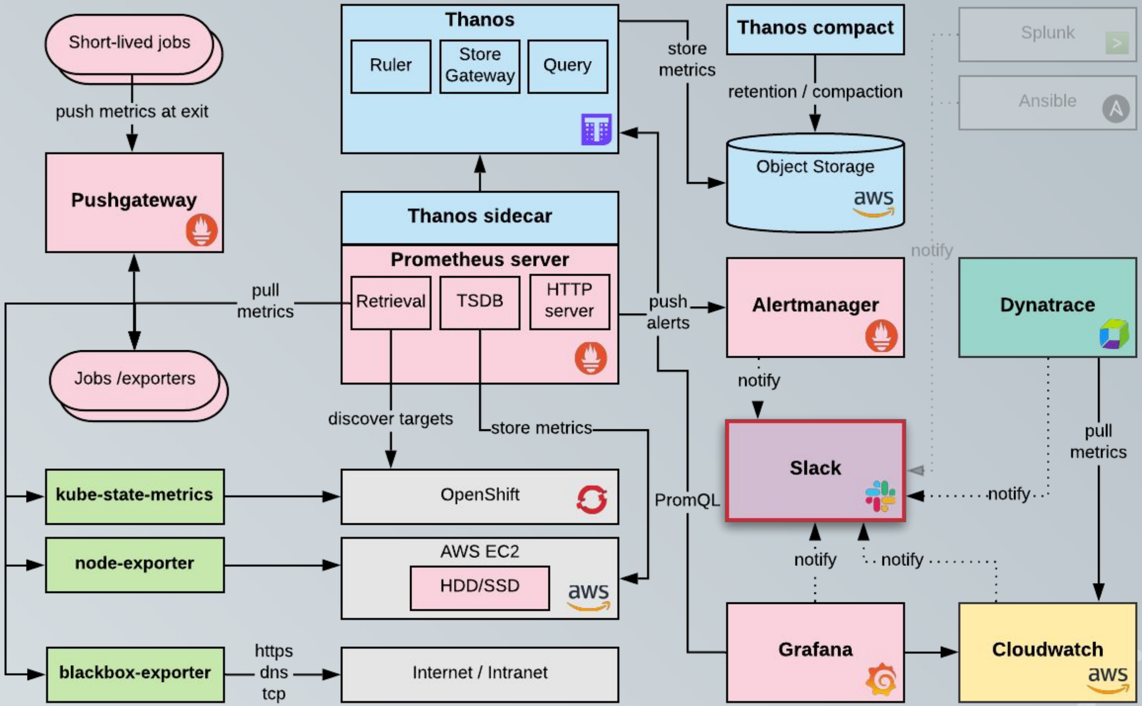
ALERTING

SLACK


slack
dynatrace
ANSIBLE
splunk>
Grafana
CloudWatch
Prometheus

SLACK

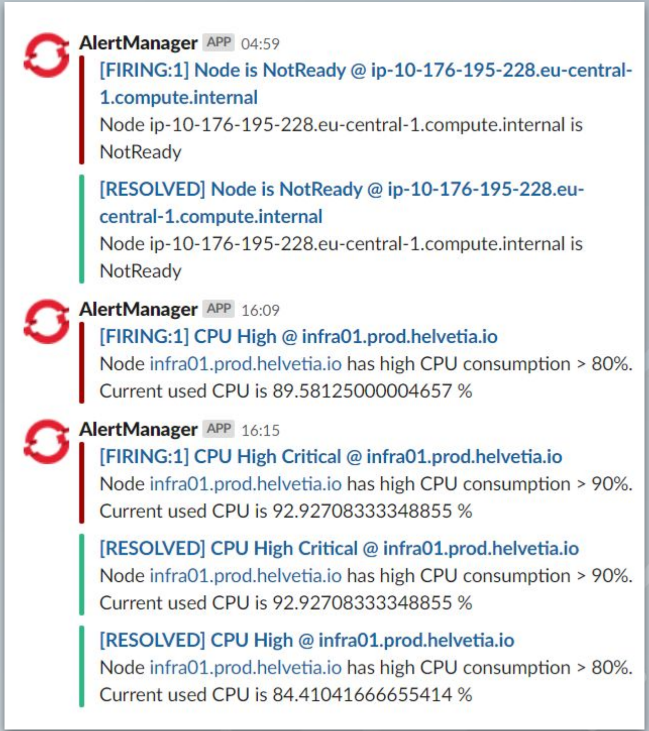
slack



Short-lived jobs
push metrics at exit
Pushgateway
pull metrics
Jobs /exporters
Thanos
Ruler
Store Gateway
Query
Thanos sidecar
Prometheus server
Retrieval
TSDB
HTTP server
discover targets
store metrics
store metrics
Thanos compact
retention / compaction
Object Storage
aws
push alerts
Alertmanager
notify
Slack
PromQL
Splunk
Ansible
notify
Dynatrace
pull metrics
notify
notify
notify
kube-state-metrics
OpenShift
node-exporter
AWS EC2
HDD/SSD
aws
blackbox-exporter
https
dns
tcp
Internet / Intranet
Grafana
Cloudwatch
aws

ALERTMANAGER RULES

```
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 }}
%"
```



AlertManager APP 04:59

[FIRING:1] Node is NotReady @ ip-10-176-195-228.eu-central-1.compute.internal

Node ip-10-176-195-228.eu-central-1.compute.internal is NotReady

[RESOLVED] Node is NotReady @ ip-10-176-195-228.eu-central-1.compute.internal

Node ip-10-176-195-228.eu-central-1.compute.internal is NotReady

AlertManager APP 16:09

[FIRING:1] CPU High @ infra01.prod.helvetia.io

Node infra01.prod.helvetia.io has high CPU consumption > 80%. Current used CPU is 89.58125000004657 %

AlertManager APP 16:15

[FIRING:1] CPU High Critical @ infra01.prod.helvetia.io

Node infra01.prod.helvetia.io has high CPU consumption > 90%. Current used CPU is 92.92708333348855 %

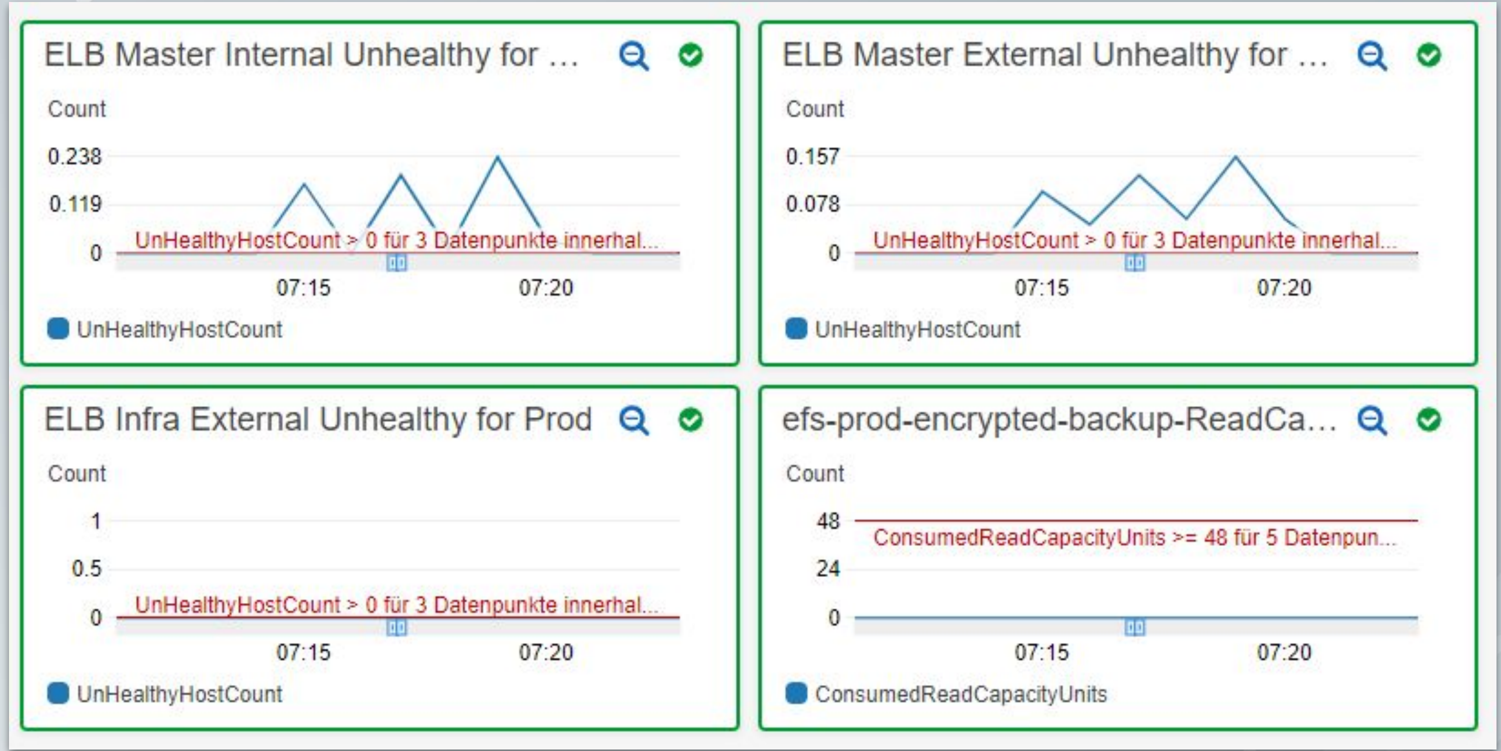
[RESOLVED] CPU High Critical @ infra01.prod.helvetia.io

Node infra01.prod.helvetia.io has high CPU consumption > 90%. Current used CPU is 92.92708333348855 %

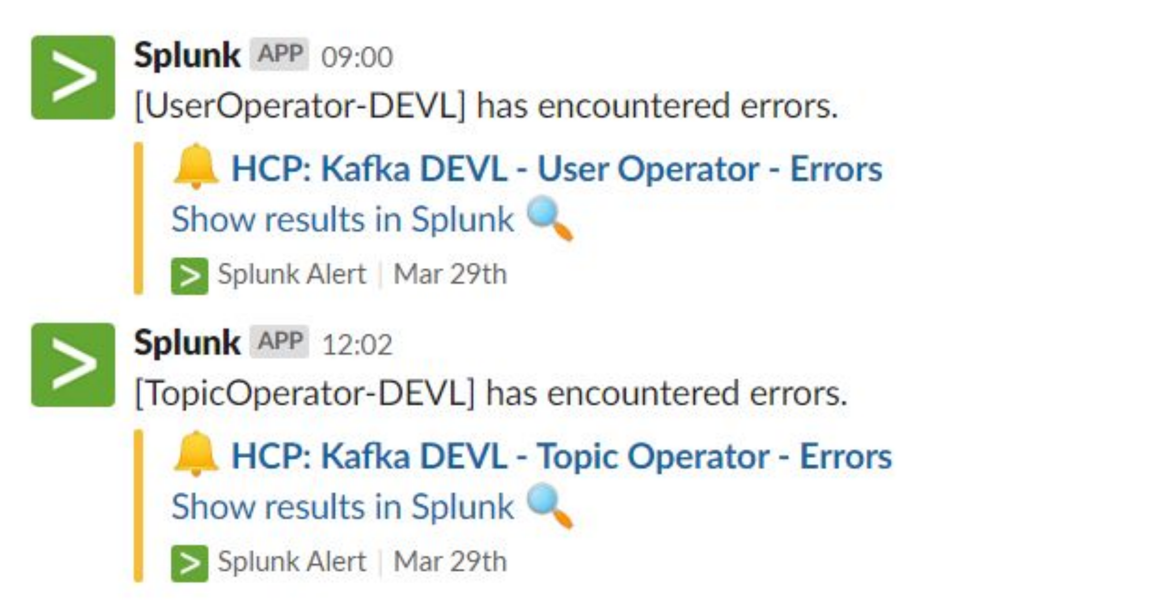
[RESOLVED] CPU High @ infra01.prod.helvetia.io

Node infra01.prod.helvetia.io has high CPU consumption > 80%. Current used CPU is 84.41041666655414 %

CLOUDWATCH ALERTS


ELB Master Internal Unhealthy for …
Count
0.238
0.119
0
UnHealthyHostCount > 0 für 3 Datenpunkte innerhal...
07:15
07:20
UnHealthyHostCount
ELB Master External Unhealthy for …
Count
0.157
0.078
0
UnHealthyHostCount > 0 für 3 Datenpunkte innerhal...
07:15
07:20
UnHealthyHostCount
ELB Infra External Unhealthy for Prod
Count
1
0.5
0
UnHealthyHostCount > 0 für 3 Datenpunkte innerhal...
07:15
07:20
UnHealthyHostCount
efs-prod-encrypted-backup-ReadCa…
Count
48
24
0
ConsumedReadCapacityUnits >= 48 für 5 Datenpun...
07:15
07:20
ConsumedReadCapacityUnits

LOG-BASED ALERTS



Splunk APP 09:00

[UserOperator-DEVL] has encountered errors.

🔔 HCP: Kafka DEVL - User Operator - Errors

Show results in Splunk 🔍

Splunk Alert | Mar 29th

Splunk APP 12:02

[TopicOperator-DEVL] has encountered errors.

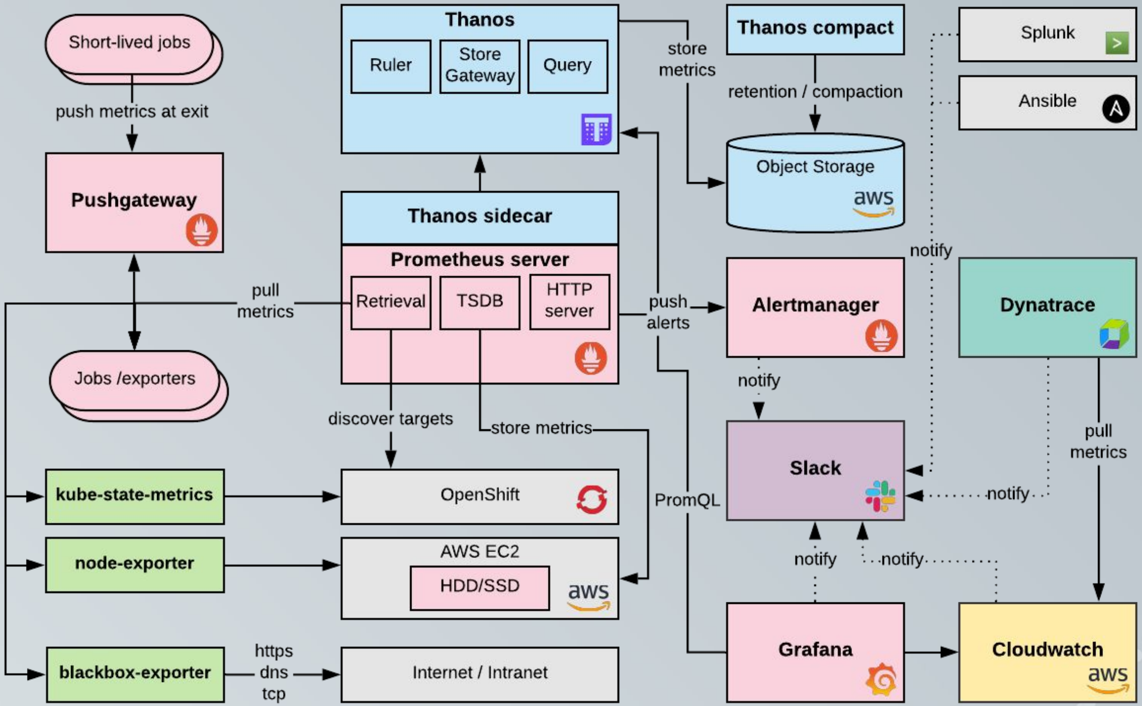
🔔 HCP: Kafka DEVL - Topic Operator - Errors

Show results in Splunk 🔍

Splunk Alert | Mar 29th

SUMMARY

FINAL SOLUTION



FUTURE PLANS

- Upgrade to OpenShift 3.11
- Using Prometheus Cluster Operator
- Using Dynatrace Operator
- Using Grafana alerts
- Integrate custom solutions

DEMO/Q&A

RED HAT
SUMMIT

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

BLACKBOX EXPORTER

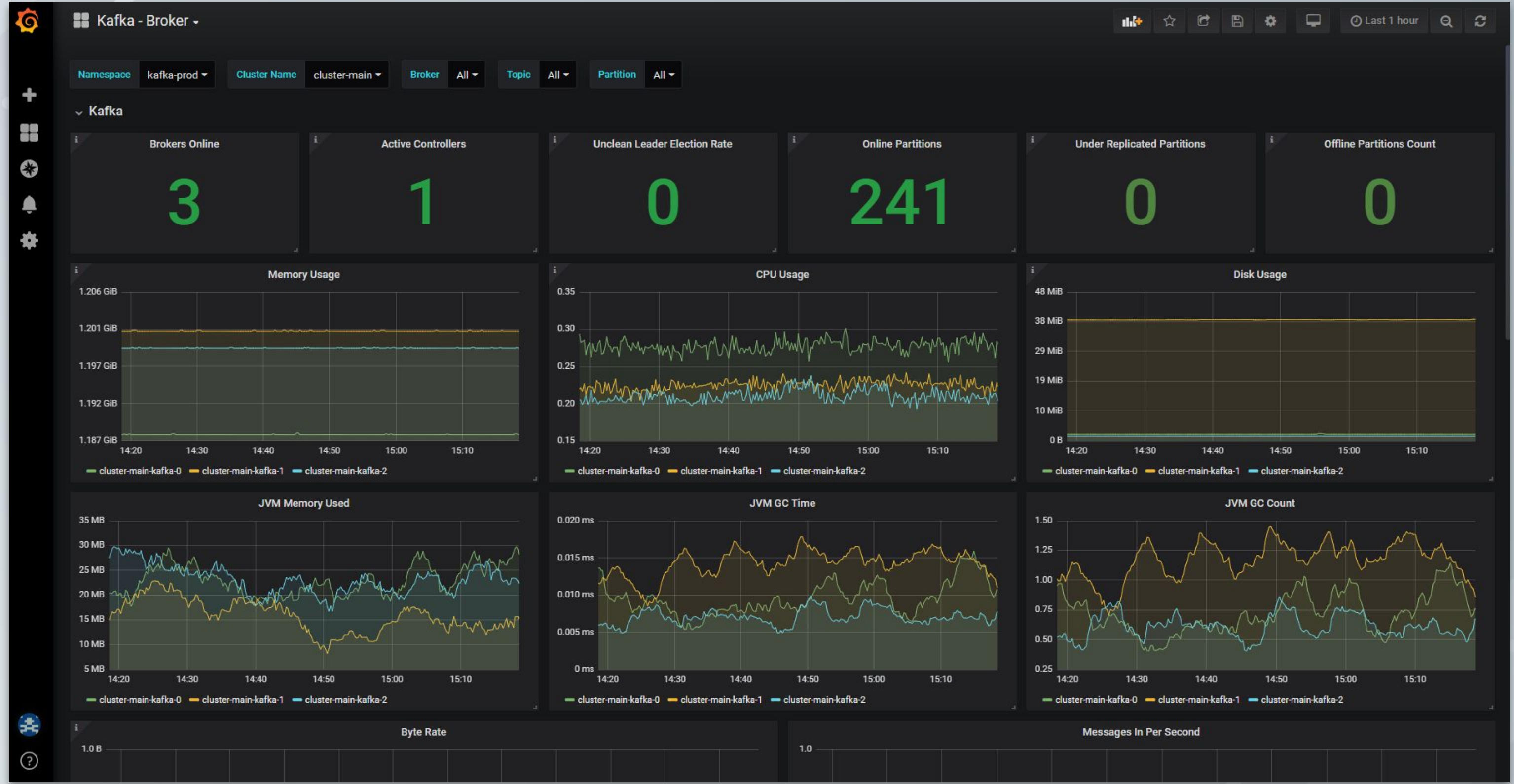
config.yml

```
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
```

dns_udp.target.yml

```
- labels:
    module: dns_udp
  targets:
  - 11.2.888.999
  - 11.3.888.999
```

DASHBOARDS



Kafka - Broker

Namespace: kafka-prod
Cluster Name: cluster-main
Broker: All
Topic: All
Partition: All

Kafka

Brokers Online: 3
Active Controllers: 1
Unclean Leader Election Rate: 0
Online Partitions: 241
Under Replicated Partitions: 0
Offline Partitions Count: 0

ALERTMANAGER RECEIVER

```
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
```