Red Hat Insights

Processing OpenShift 4 health data at scale

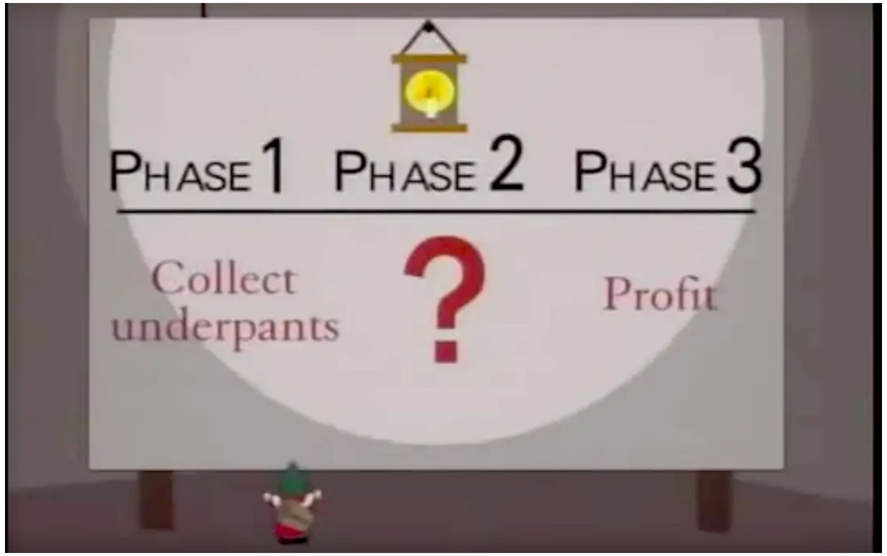
Pavel Tisnovsky
Principal Software Engineer
Red Hat Czech

Jose Luis Segura Lucas
Software Engineer
Red Hat Spain

Motivation

- **Phase 1:** Collect ~~underpants~~ cluster health data
- **Phase 2:** Process the data
- **Phase 3:** Profit

For more info please look at the presentation: Preventing catastrophes using OpenShift data

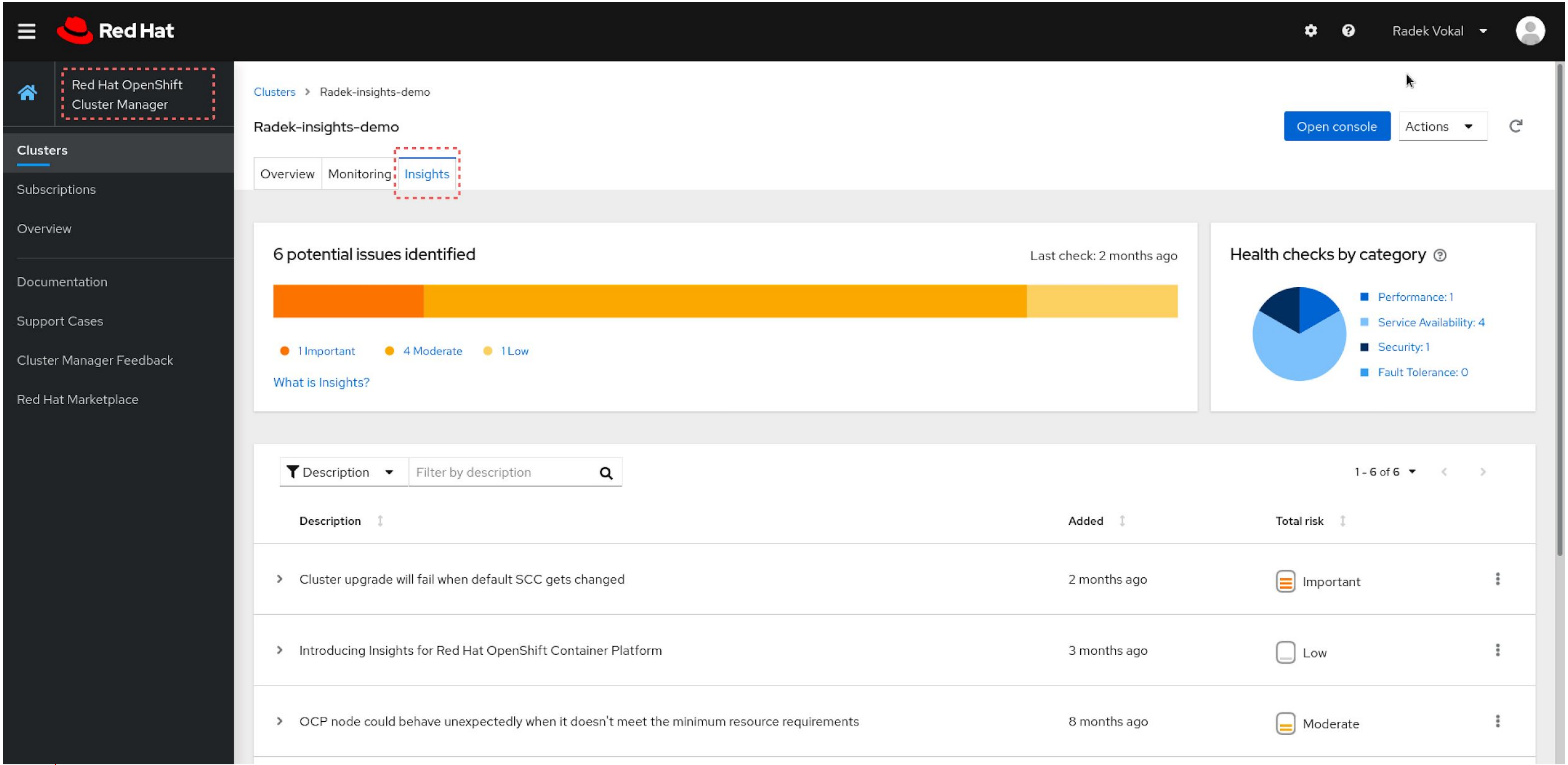


Source: South Park (Copyright ViacomCBS)

```
Software Failure.   Press left mouse button to continue.
          Guru Meditation #00000025.65045338
```

Designer
KEVIN RYAN
JEFF TUNNELL
Producer
Art Director
BRIAN HAHN
Music Director
CHRIS STEVENS
Artist
DENNIS CLEVENGER
Lead Tester
JEANNE RUBINSTEIN

OpenShift Cluster Manager - cloud.redhat.com/openshift



6 potential issues identified

Last check: 2 months ago

● 1 Important ● 4 Moderate ● 1 Low

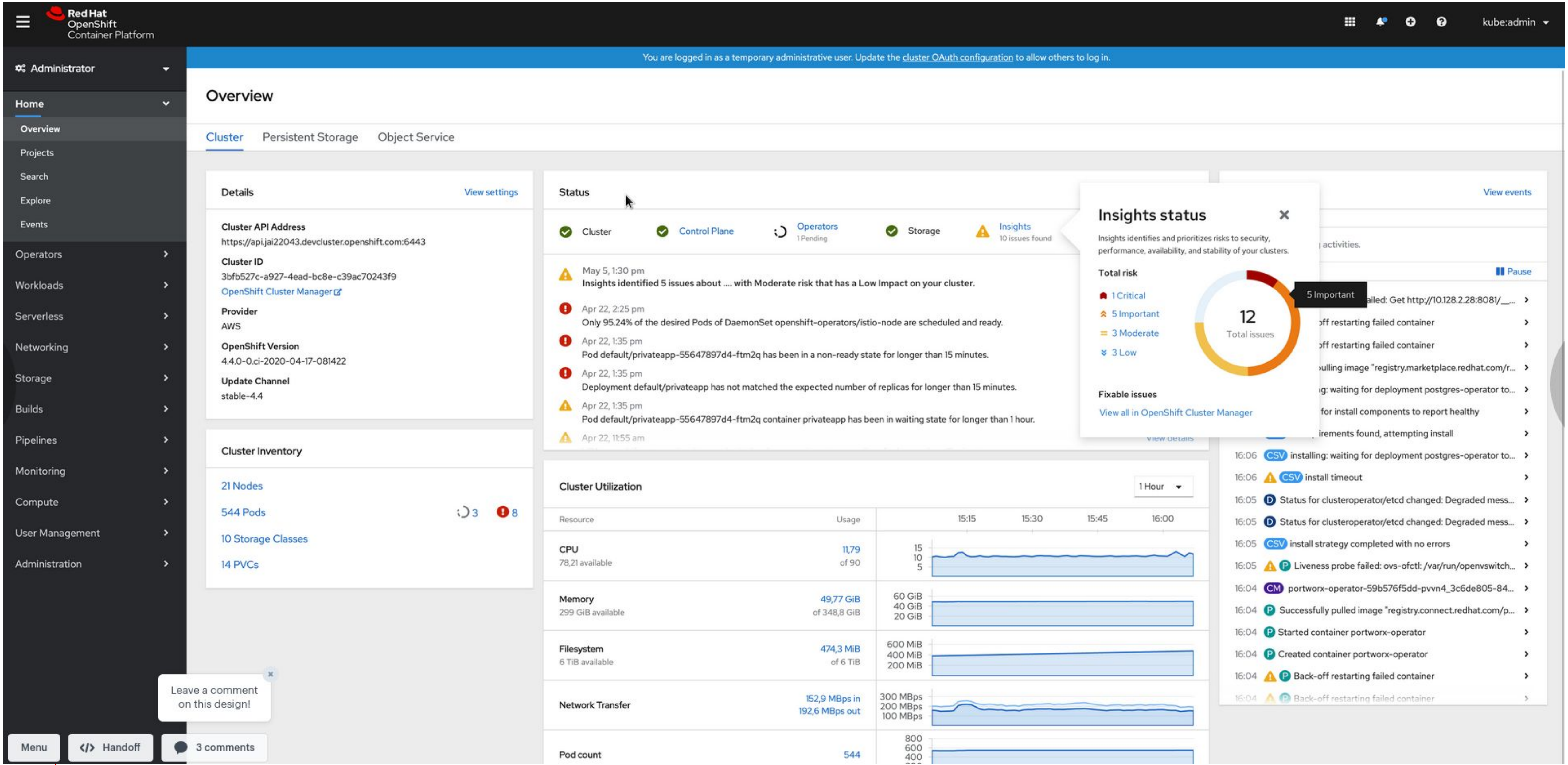
What is Insights?

Health checks by category

- Performance: 1
- Service Availability: 4
- Security: 1
- Fault Tolerance: 0

	Description	Added	Total risk
›	Cluster upgrade will fail when default SCC gets changed	2 months ago	Important
›	Introducing Insights for Red Hat OpenShift Container Platform	3 months ago	Low
›	OCP node could behave unexpectedly when it doesn't meet the minimum resource requirements	8 months ago	Moderate

OpenShift WebConsole



You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in.

Overview

Details

Cluster API Address
https://api.jai22043.devcluster.openshift.com:6443

Cluster ID
3bfb527c-a927-4ead-bc8e-c39ac70243f9
OpenShift Cluster Manager

Provider
AWS

OpenShift Version
4.4.0-0.ci-2020-04-17-081422

Update Channel
stable-4.4

Cluster Inventory

21 Nodes
544 Pods 3 8
10 Storage Classes
14 PVCs

Status

✓ Cluster ✓ Control Plane Operators 1 Pending ✓ Storage ⚠ Insights 10 issues found

⚠ May 5, 1:30 pm
Insights identified 5 issues about .... with Moderate risk that has a Low Impact on your cluster.

! Apr 22, 2:25 pm
Only 95.24% of the desired Pods of DaemonSet openshift-operators/istio-node are scheduled and ready.

! Apr 22, 1:35 pm
Pod default/privateapp-55647897d4-ftm2q has been in a non-ready state for longer than 15 minutes.

! Apr 22, 1:35 pm
Deployment default/privateapp has not matched the expected number of replicas for longer than 15 minutes.

⚠ Apr 22, 1:35 pm
Pod default/privateapp-55647897d4-ftm2q container privateapp has been in waiting state for longer than 1 hour.

⚠ Apr 22, 11:55 am

Insights status

Insights identifies and prioritizes risks to security, performance, availability, and stability of your clusters.

Total risk
1 Critical
5 Important
3 Moderate
3 Low

12 Total issues

5 Important

Fixable issues
View all in OpenShift Cluster Manager

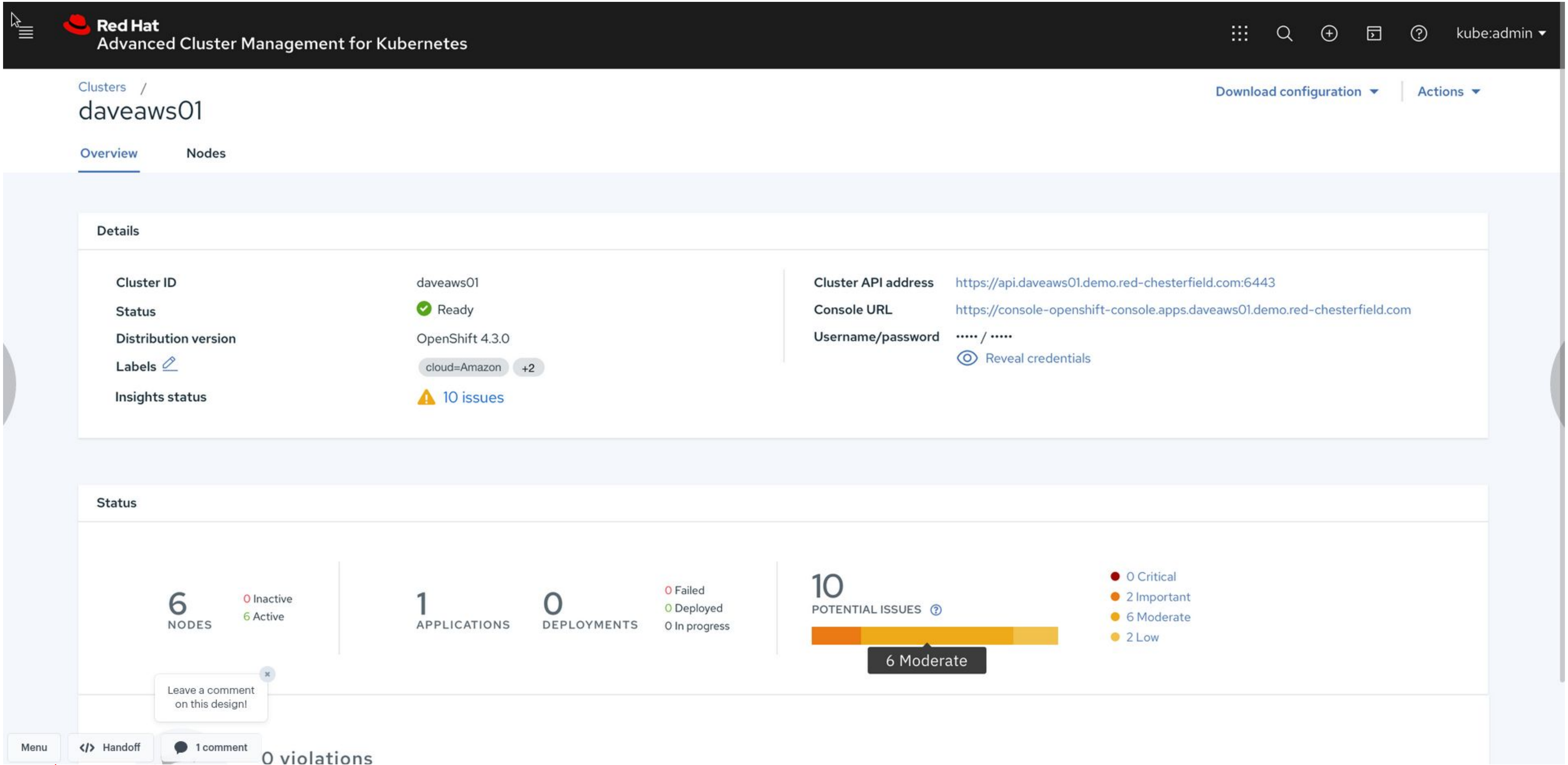
Cluster Utilization

Resource	Usage
CPU 78,21 available	11,79 of 90
Memory 299 GiB available	49,77 GiB of 348,8 GiB
Filesystem 6 TiB available	474,3 MiB of 6 TiB
Network Transfer	152,9 MBps in 192,6 MBps out
Pod count	544

activities.

ailed: Get http://10.128.2.28:8081/_...
off restarting failed container
off restarting failed container
pulling image "registry.marketplace.redhat.com/r...
g: waiting for deployment postgres-operator to...
for install components to report healthy
irements found, attempting install
16:06 CSV installing: waiting for deployment postgres-operator to...
16:06 ⚠ CSV install timeout
16:05 D Status for clusteroperator/etcd changed: Degraded mess...
16:05 D Status for clusteroperator/etcd changed: Degraded mess...
16:05 CSV install strategy completed with no errors
16:05 ⚠ P Liveness probe failed: ovs-ofctl: /var/run/openvswitch...
16:04 CM portworx-operator-59b576f5dd-pvvn4_3c6de805-84...
16:04 P Successfully pulled image "registry.connect.redhat.com/p...
16:04 P Started container portworx-operator
16:04 P Created container portworx-operator
16:04 ⚠ P Back-off restarting failed container
16:04 ⚠ P Back-off restarting failed container

Advanced Cluster Manager



Clusters /

daveaws01

Details

Cluster ID	daveaws01
Status	✓ Ready
Distribution version	OpenShift 4.3.0
Labels	cloud=Amazon +2
Insights status	⚠ 10 issues

Cluster API address	https://api.daveaws01.demo.red-chesterfield.com:6443
Console URL	https://console-openshift-console.apps.daveaws01.demo.red-chesterfield.com
Username/password	••••• / ••••• Reveal credentials

Status

6 NODES: 0 Inactive, 6 Active

1 APPLICATIONS

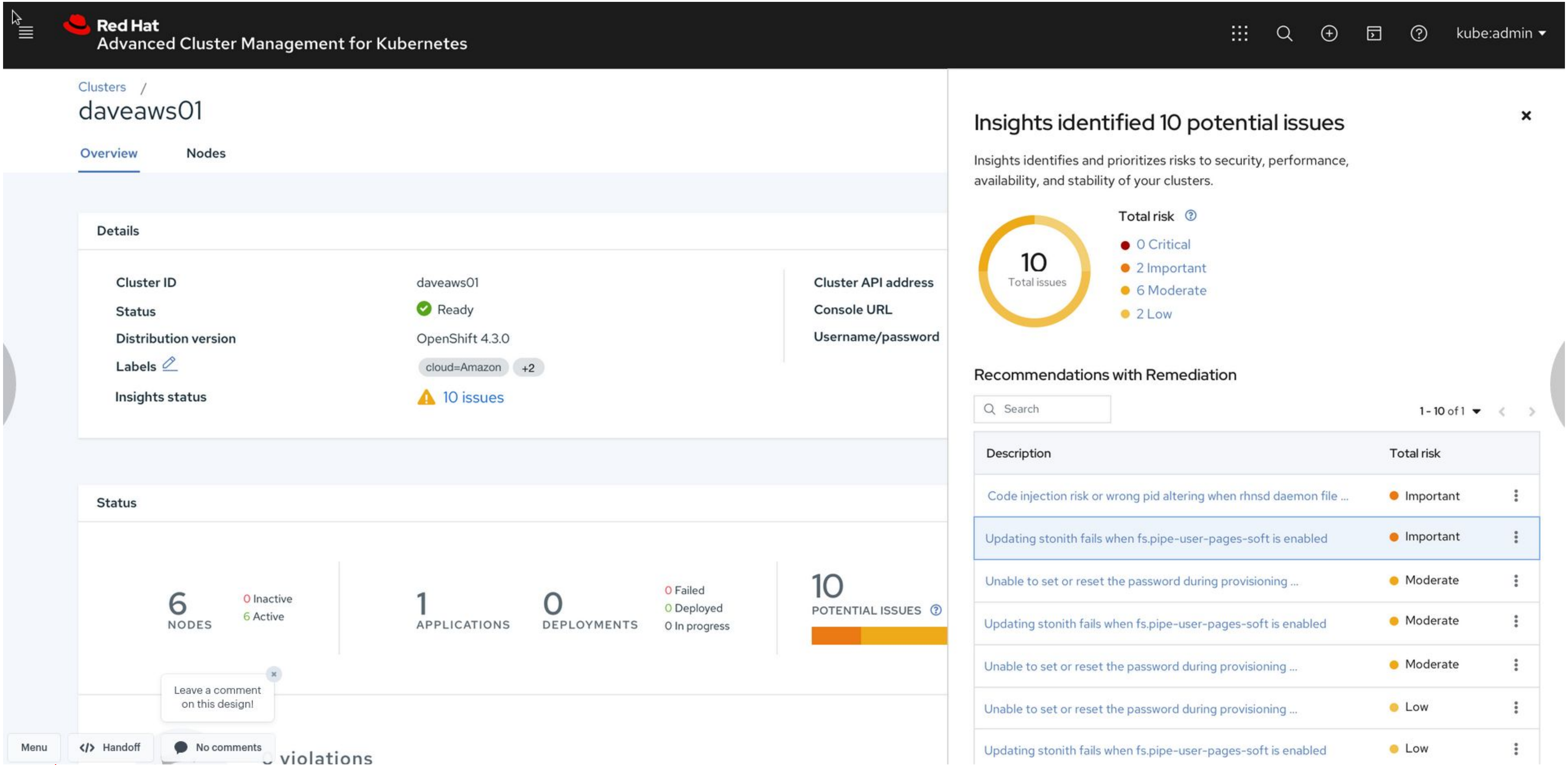
0 DEPLOYMENTS: 0 Failed, 0 Deployed, 0 In progress

10 POTENTIAL ISSUES

● 0 Critical
● 2 Important
● 6 Moderate
● 2 Low

0 violations

Advanced Cluster Manager



Red Hat
Advanced Cluster Management for Kubernetes

kube:admin

Clusters /

daveaws01

Overview | Nodes

Details

Cluster ID	daveaws01
Status	Ready
Distribution version	OpenShift 4.3.0
Labels	cloud=Amazon +2
Insights status	10 issues

Cluster API address
Console URL
Username/password

Status

6 NODES — 0 Inactive, 6 Active

1 APPLICATIONS

0 DEPLOYMENTS — 0 Failed, 0 Deployed, 0 In progress

10 POTENTIAL ISSUES

Leave a comment on this design!

Menu | Handoff | No comments

violations

Insights identified 10 potential issues

Insights identifies and prioritizes risks to security, performance, availability, and stability of your clusters.

10 Total issues

Total risk
- 0 Critical
- 2 Important
- 6 Moderate
- 2 Low

Recommendations with Remediation

Search

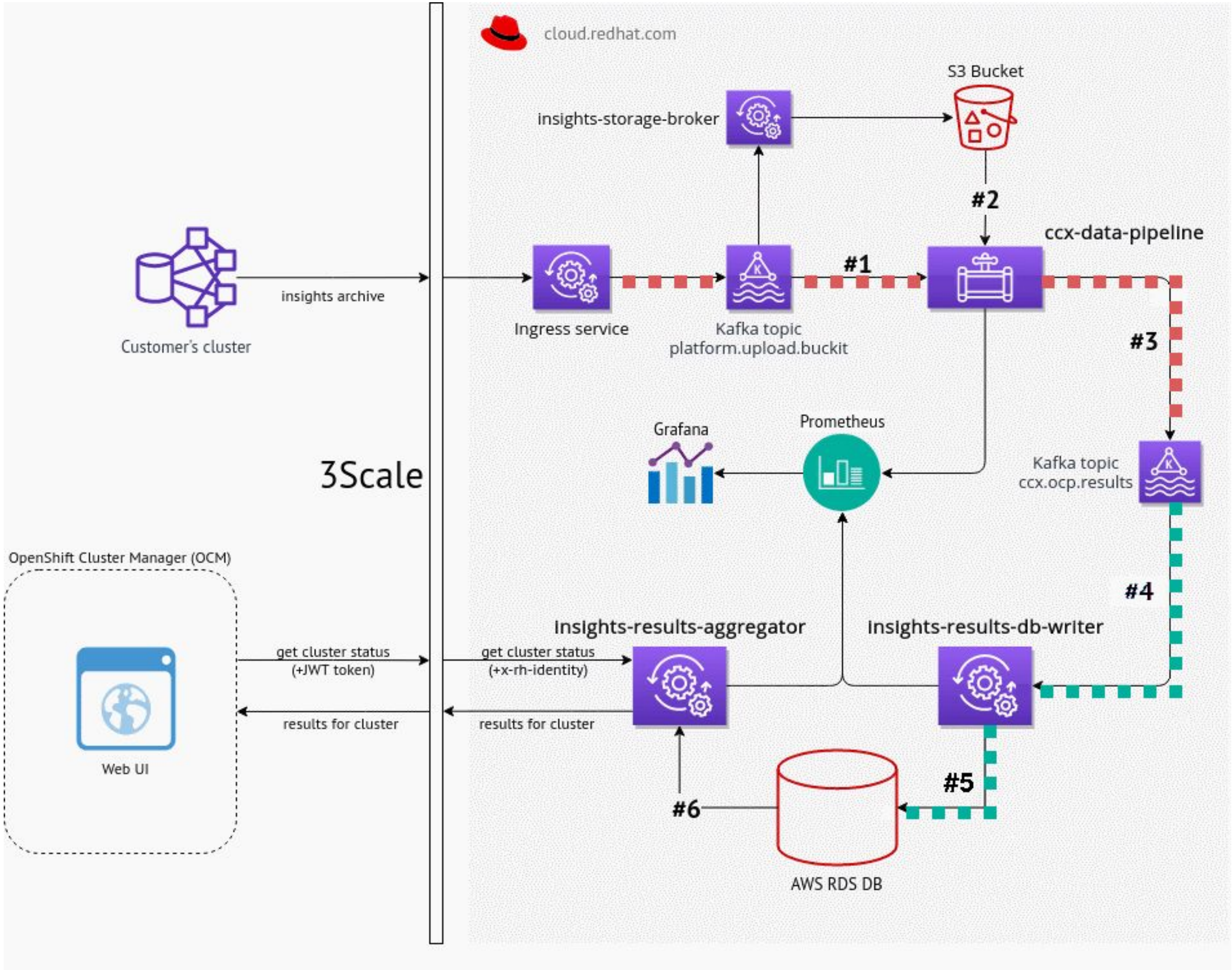
1 - 10 of 1

Description	Total risk
Code injection risk or wrong pid altering when rhnsd daemon file ...	Important
Updating stonith fails when fs.pipe-user-pages-soft is enabled	Important
Unable to set or reset the password during provisioning ...	Moderate
Updating stonith fails when fs.pipe-user-pages-soft is enabled	Moderate
Unable to set or reset the password during provisioning ...	Moderate
Unable to set or reset the password during provisioning ...	Low
Updating stonith fails when fs.pipe-user-pages-soft is enabled	Low

Implementation

Processing pipeline architecture

- Hosted on cloud.redhat.com
- Based on OCP rules engine written in Python
- Processing parts written in Go
- Kafka used as a classic queue
    - “Replay” ability is not used (at the moment)
- RDS used as a storage
- Processed data exposed via HTTP API
    - Currently consumed by 3 internal clients


cloud.redhat.com
S3 Bucket
insights-storage-broker
#2
ccx-data-pipeline
#1
Customer's cluster
insights archive
Ingress service
Kafka topic
platform.upload.buckit
#3
Grafana
Prometheus
Kafka topic
ccx.ocp.results
3Scale
OpenShift Cluster Manager (OCM)
#4
insights-results-aggregator
insights-results-db-writer
get cluster status
(+JWT token)
get cluster status
(+x-rh-identity)
Web UI
results for cluster
results for cluster
#5
#6
AWS RDS DB

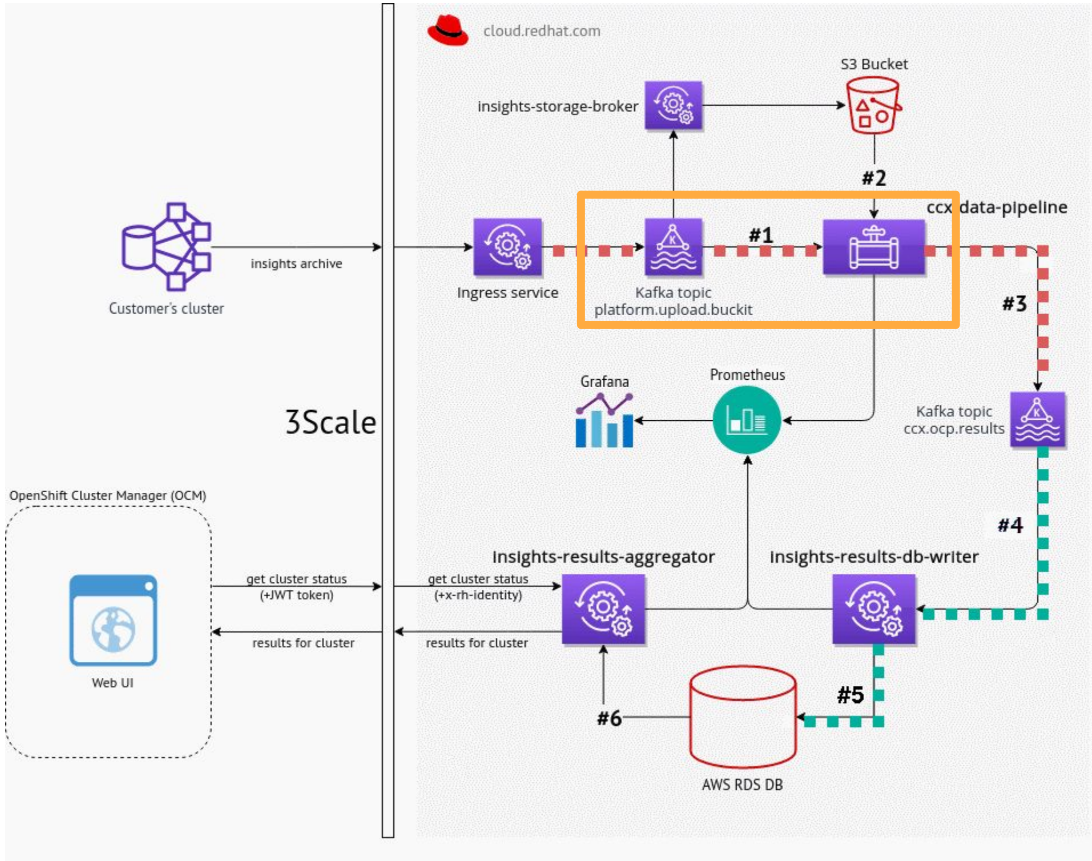
Technologies are cool

Technologies are cool

Data is everything

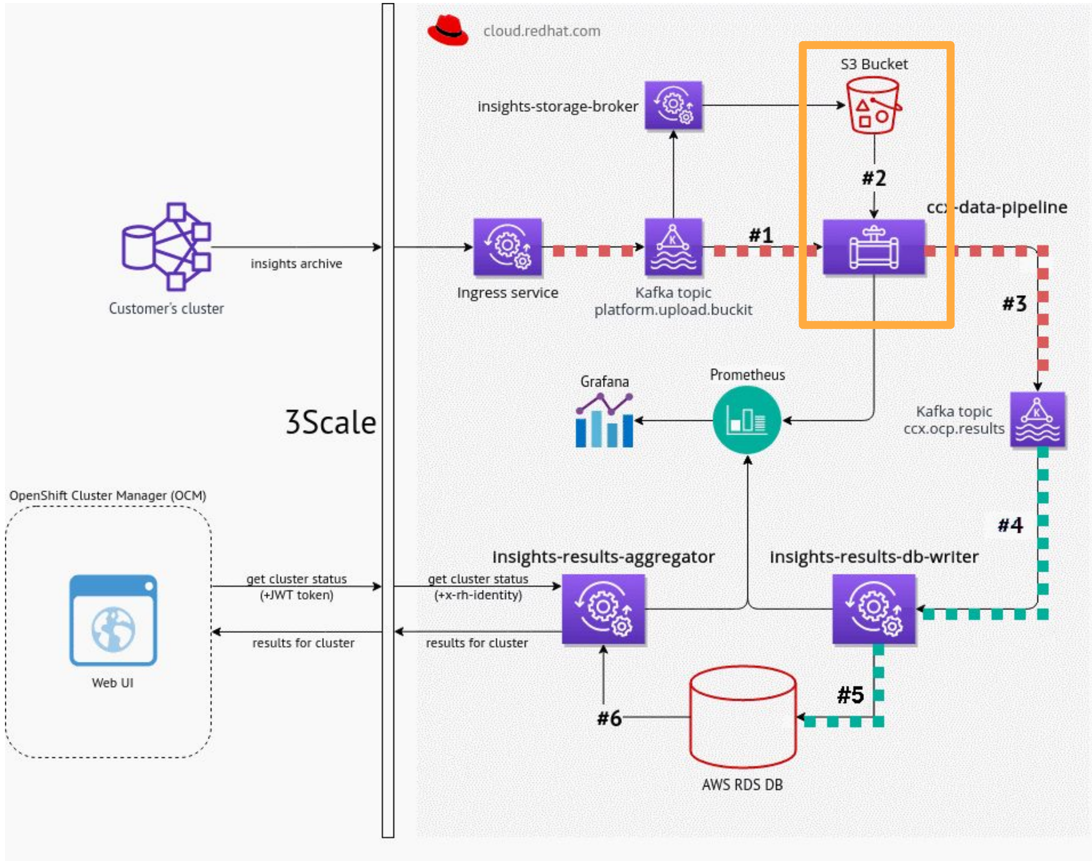
Processed data

- Event about new data from insights operator is consumed from Kafka. That event contains (among other things) URL to S3 Bucket



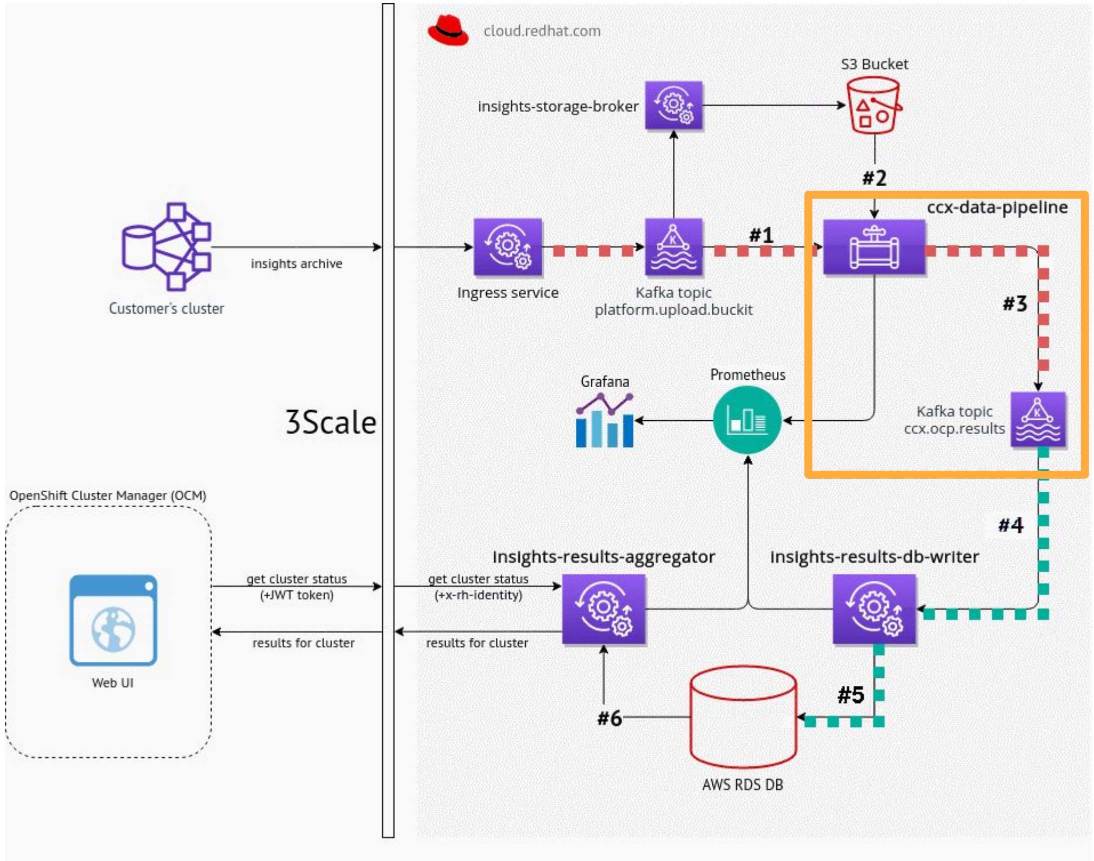
Processed data

- Event about new data from insights operator is consumed from Kafka. That event contains (among other things) URL to S3 Bucket
- Insights operator data is read from S3 Bucket and insights rules are applied to that data in ccx-data-pipeline



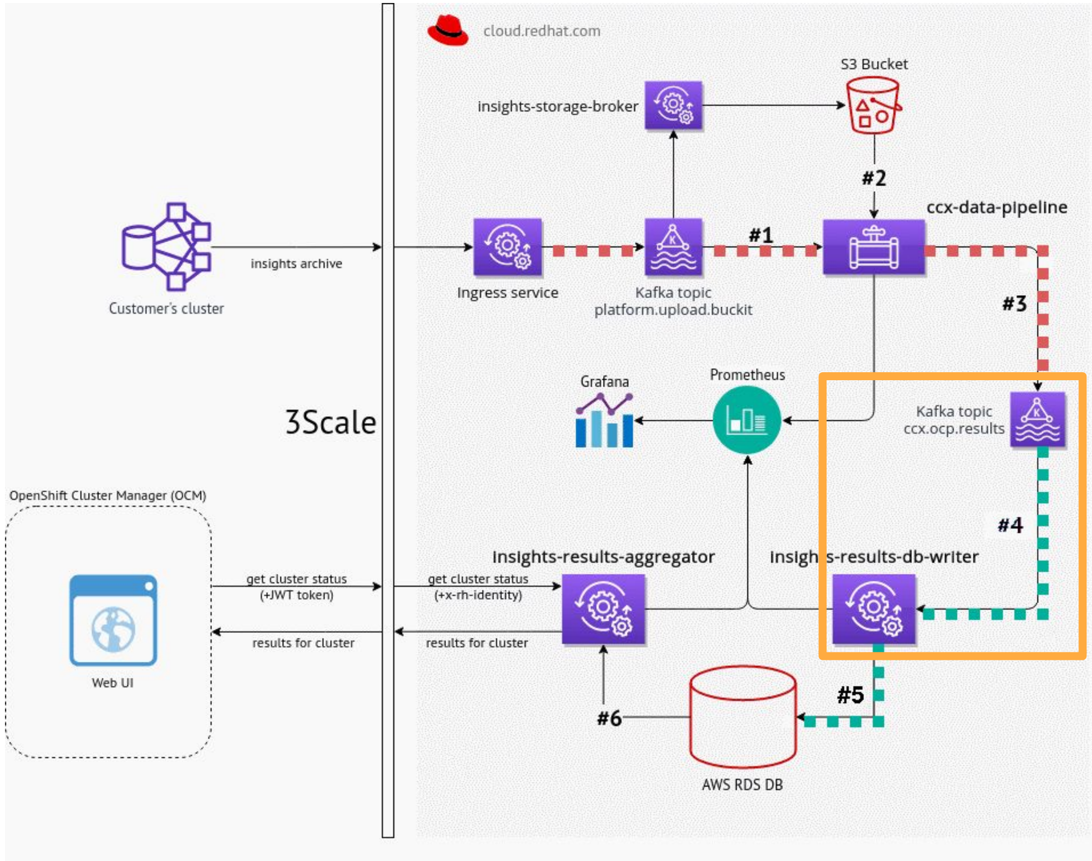
Processed data

- Event about new data from insights operator is consumed from Kafka. That event contains (among other things) URL to S3 Bucket
- Insights operator data is read from S3 Bucket and insights rules are applied to that data in ccx-data-pipeline
- Results (basically organization ID + cluster name + insights results JSON) are stored back into Kafka, but into different topic



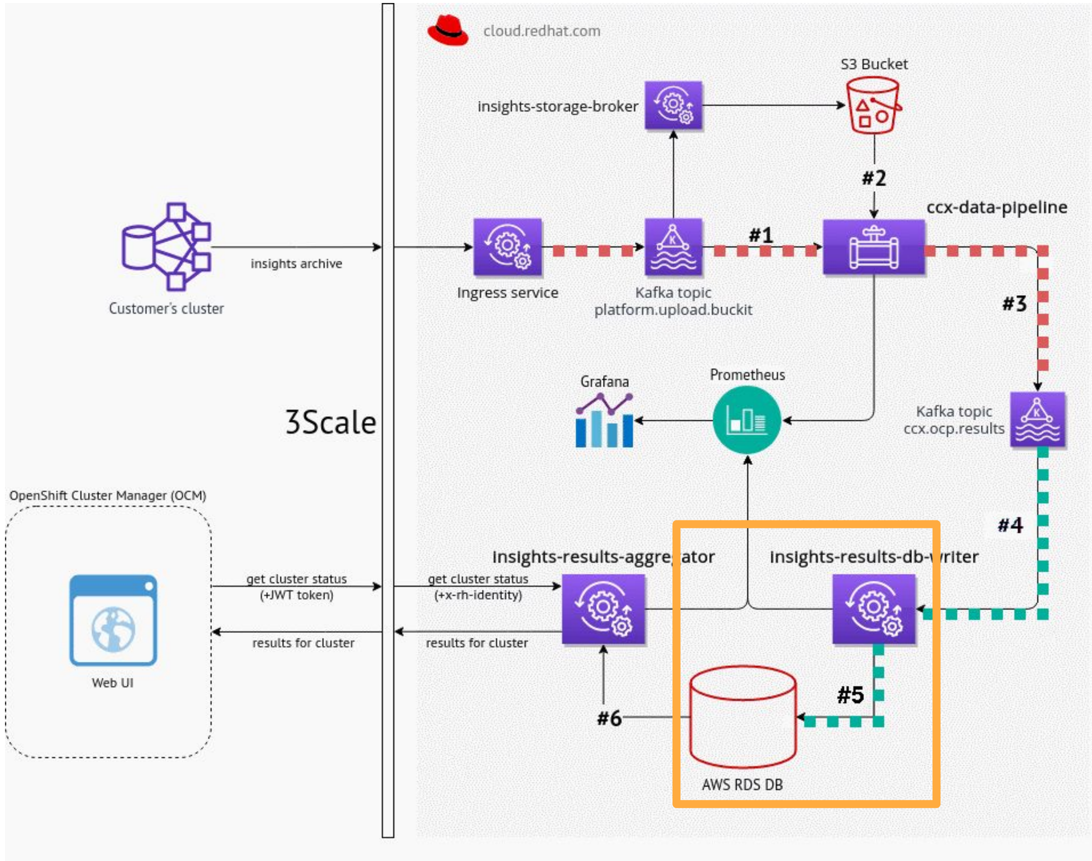
Processed data

- Event about new data from insights operator is consumed from Kafka. That event contains (among other things) URL to S3 Bucket
- Insights operator data is read from S3 Bucket and insights rules are applied to that data in ccx-data-pipeline
- Results (basically organization ID + cluster name + insights results JSON) are stored back into Kafka, but into different topic
- That results are consumed by insights-results-db-writer service



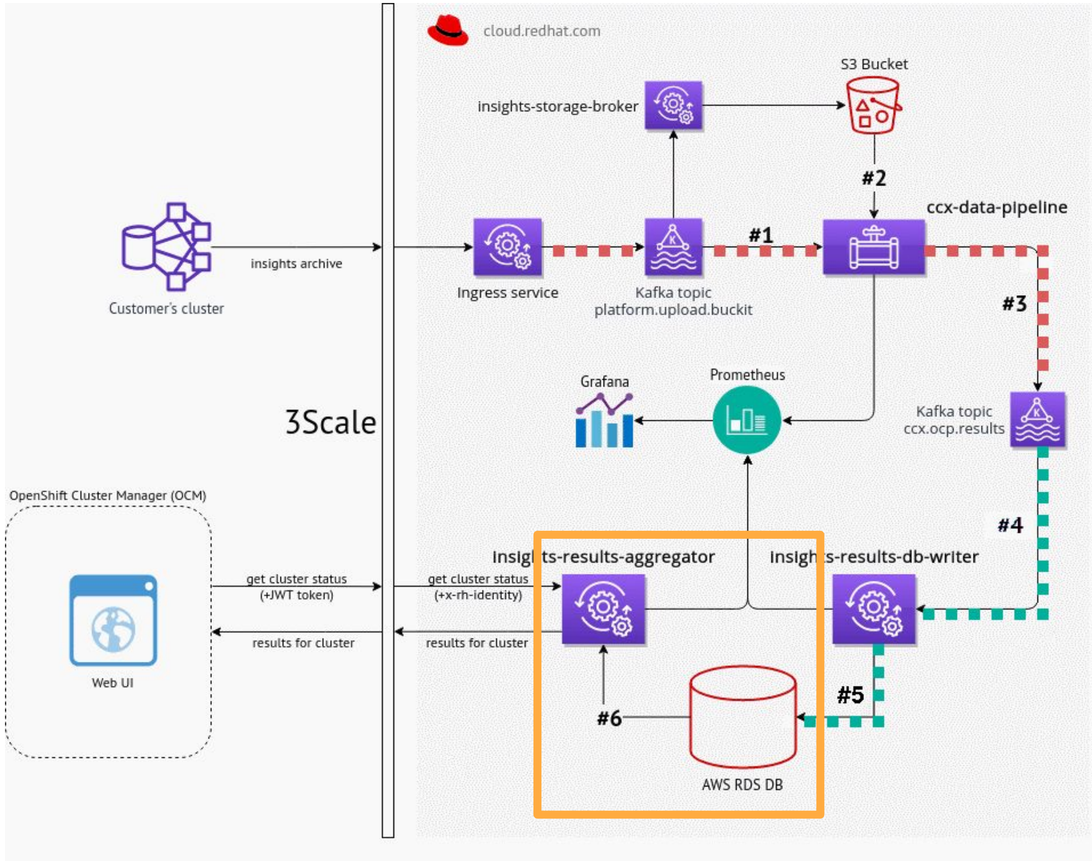
Processed data

- Event about new data from insights operator is consumed from Kafka. That event contains (among other things) URL to S3 Bucket
- Insights operator data is read from S3 Bucket and insights rules are applied to that data in ccx-data-pipeline
- Results (basically organization ID + cluster name + insights results JSON) are stored back into Kafka, but into different topic
- That results are consumed by insights-results-db-writer service
- insights-results-db-writer stores insights results into AWS RDS database



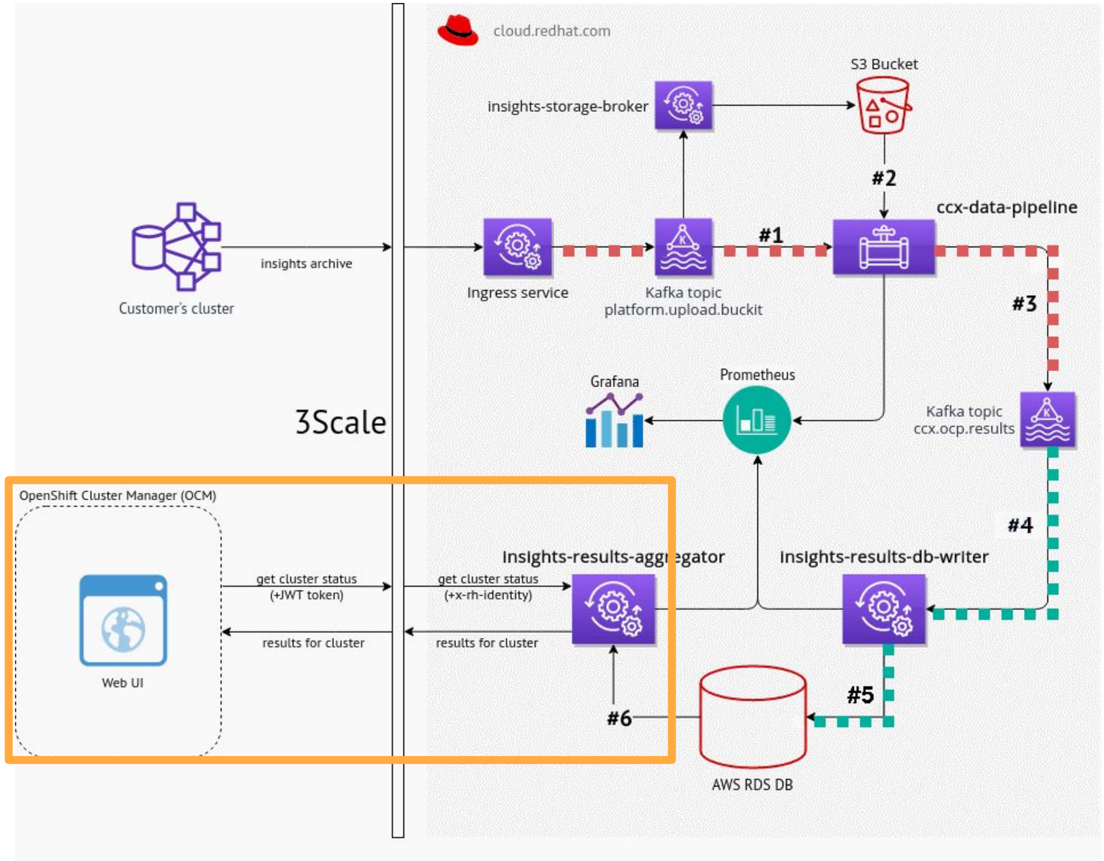
Processed data

- Event about new data from insights operator is consumed from Kafka. That event contains (among other things) URL to S3 Bucket
- Insights operator data is read from S3 Bucket and insights rules are applied to that data in ccx-data-pipeline
- Results (basically organization ID + cluster name + insights results JSON) are stored back into Kafka, but into different topic
- That results are consumed by insights-results-db-writer service
- insights-results-db-writer stores insights results into AWS RDS database
- insights-results-aggregator fetches insights results from AWS RDS database



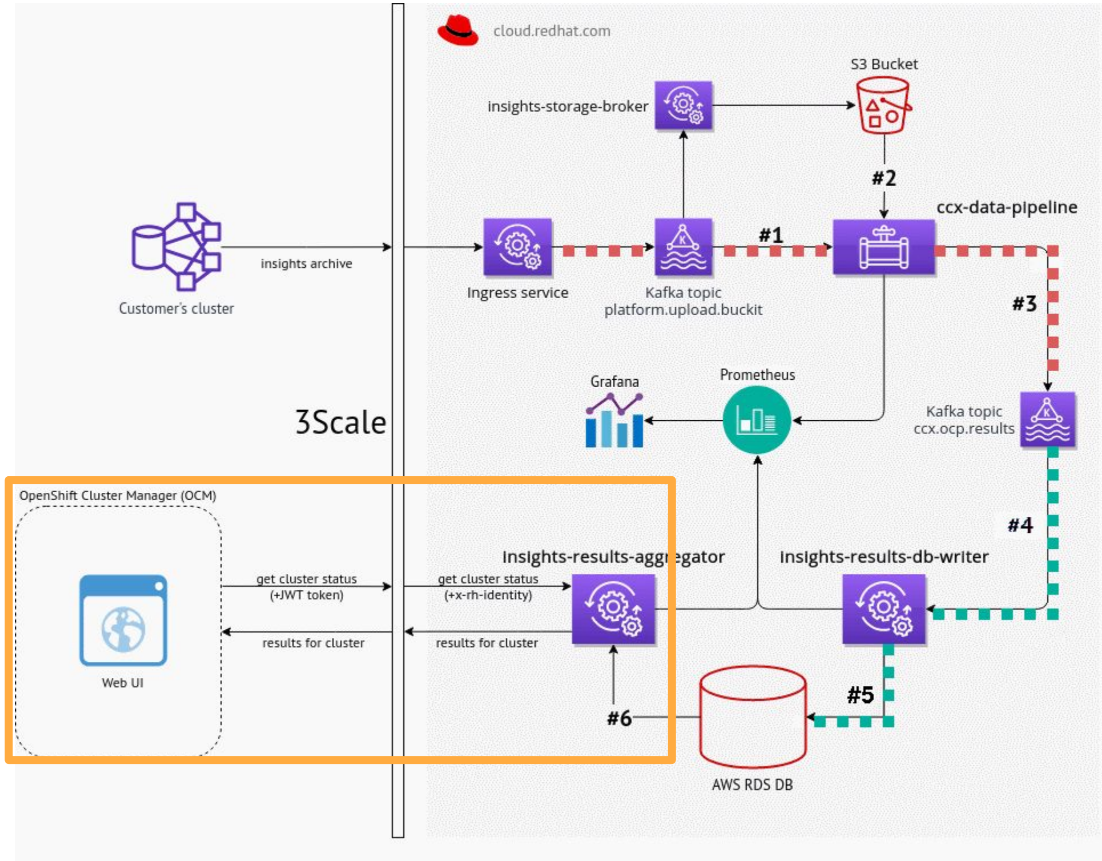
Processed data

- Event about new data from insights operator is consumed from Kafka. That event contains (among other things) URL to S3 Bucket
- Insights operator data is read from S3 Bucket and insights rules are applied to that data in ccx-data-pipeline
- Results (basically organization ID + cluster name + insights results JSON) are stored back into Kafka, but into different topic
- That results are consumed by insights-results-db-writer service
- insights-results-db-writer stores insights results into AWS RDS database
- insights-results-aggregator fetches insights results from AWS RDS database
- insights-results-aggregator provides insights results via ccx-smart-proxy



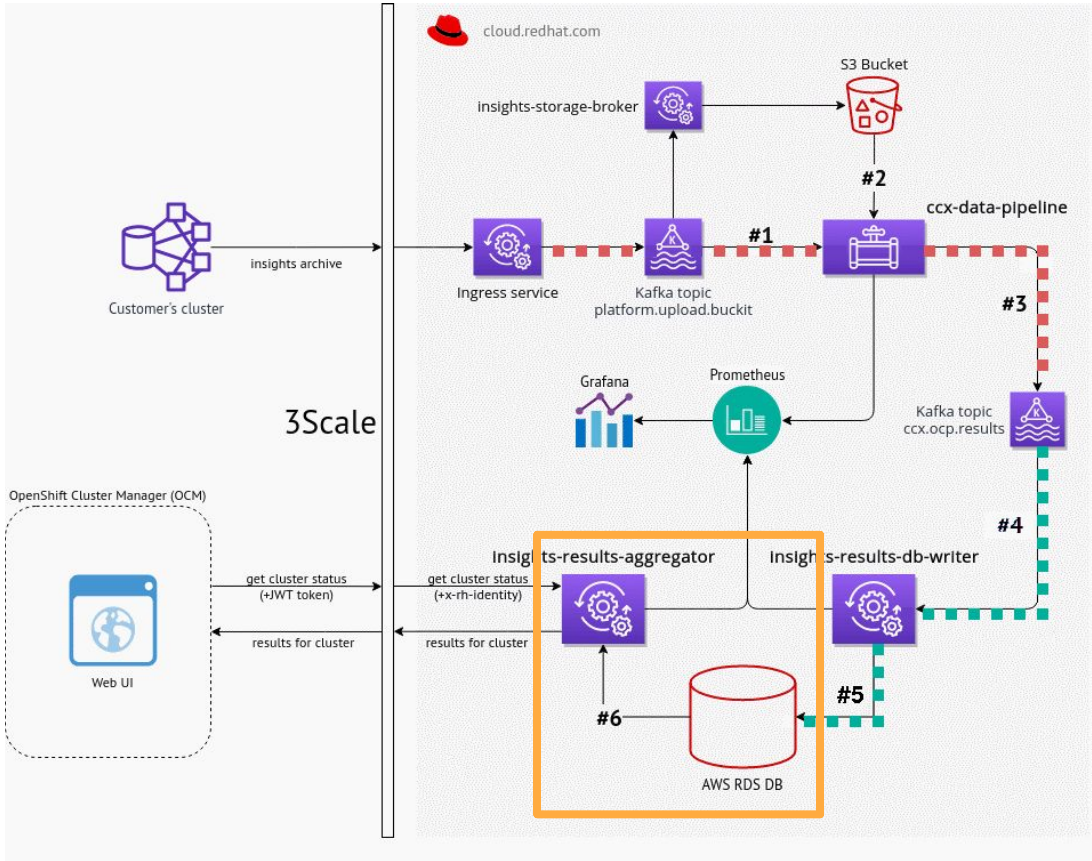
Processed data

- Event about new data from insights operator is consumed from Kafka. That event contains (among other things) URL to S3 Bucket
- Insights operator data is read from S3 Bucket and insights rules are applied to that data in ccx-data-pipeline
- Results (basically organization ID + cluster name + insights results JSON) are stored back into Kafka, but into different topic
- That results are consumed by insights-results-db-writer service
- insights-results-db-writer stores insights results into AWS RDS database
- insights-results-aggregator fetches insights results from AWS RDS database
- insights-results-aggregator provides insights results via ccx-smart-proxy
- POST and PUT requests which update the AWS RDS database go via ccx-smart-proxy, e.g.
  `PUT /clusters/{clusterId}/rules/{ruleId}/like`
- insights-results-aggregator updates the AWS RDS database



Processed data

- Event about new data from insights operator is consumed from Kafka. That event contains (among other things) URL to S3 Bucket
- Insights operator data is read from S3 Bucket and insights rules are applied to that data in ccx-data-pipeline
- Results (basically organization ID + cluster name + insights results JSON) are stored back into Kafka, but into different topic
- That results are consumed by insights-results-db-writer service
- insights-results-db-writer stores insights results into AWS RDS database
- insights-results-aggregator fetches insights results from AWS RDS database
- insights-results-aggregator provides insights results via ccx-smart-proxy
- POST and PUT requests which update the AWS RDS database go via ccx-smart-proxy, e.g.
  `PUT /clusters/{clusterId}/rules/{ruleId}/like`
- insights-results-aggregator updates the AWS RDS database



Some numbers

3633

250

768

6.4

10

64

3633 events per hour

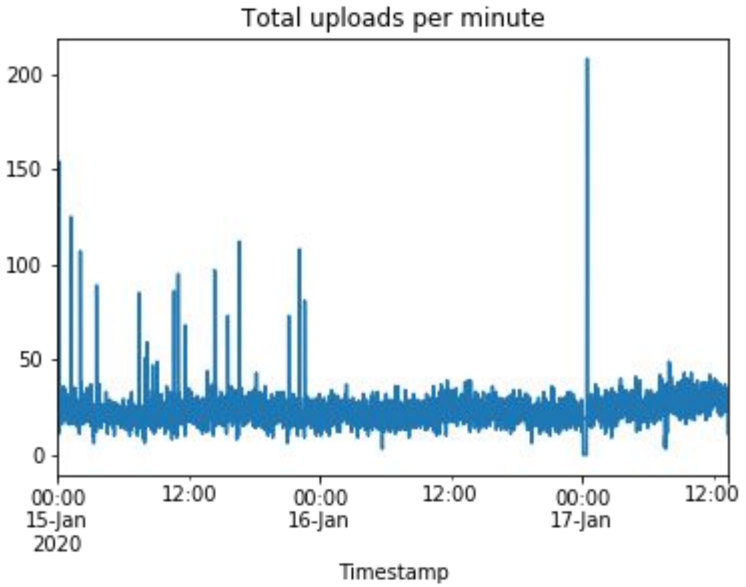
250

768

6.4

10

64



3633 events per hour

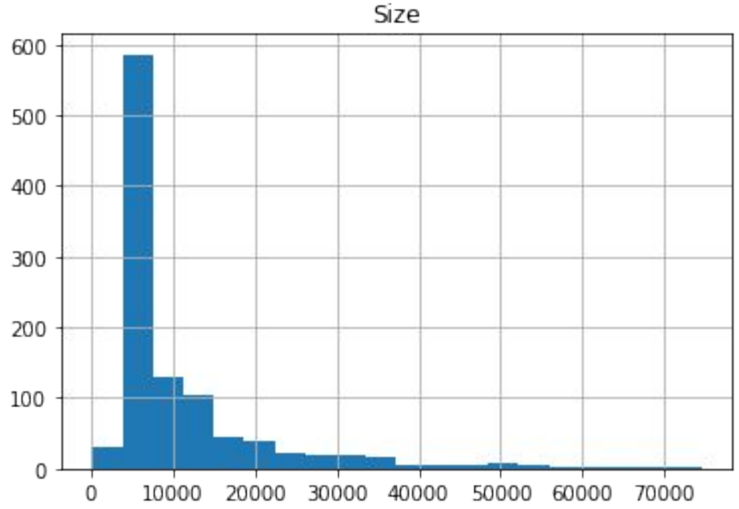
250 kB per event

768

6.4

10

64



3633 events per hour

250 kB per event

768 MB per hour

6.4

10

64

3633 events per hour

250 kB per event

768 MB per hour

6.4 TB per year

10

64

3633 events per hour

250 kB per event

768 MB per hour

6.4 TB per year

10 minimal required scale factor

64

3633 events per hour

250 kB per event

768 MB per hour

6.4 TB per year

10 minimal required scale factor

64 TB per year

64 TB per year = 47,000,000 floppies

64 TB per year = 47,000,000 floppies

actually not used

64 TB per year = 47,000,000 floppies

actually not used (yet)

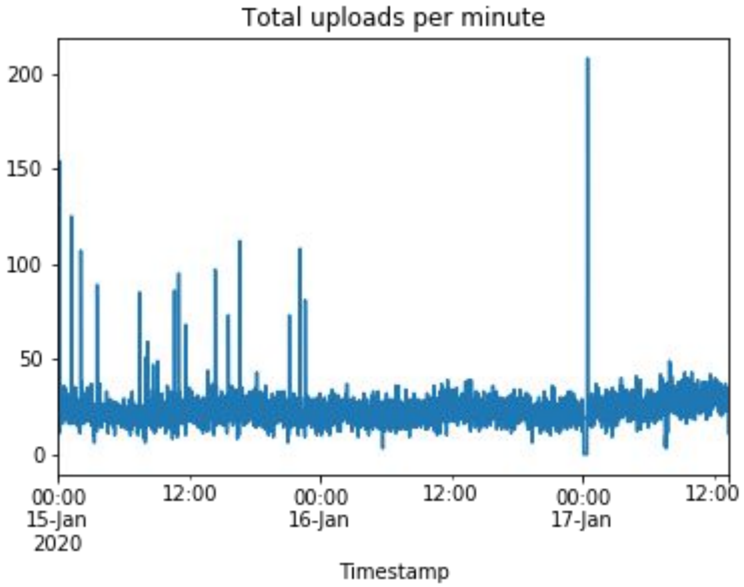
Throughput

Performance

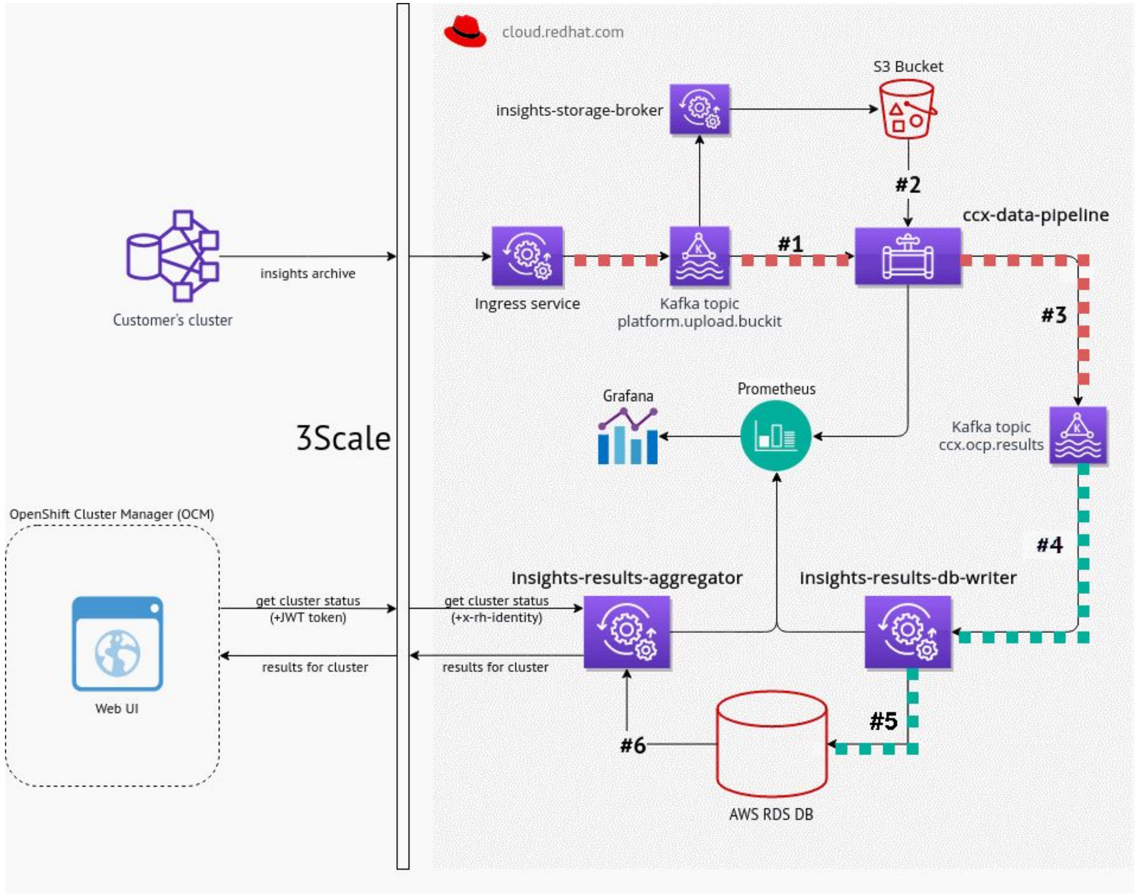
Scalability

Resilience

Flow of incoming data



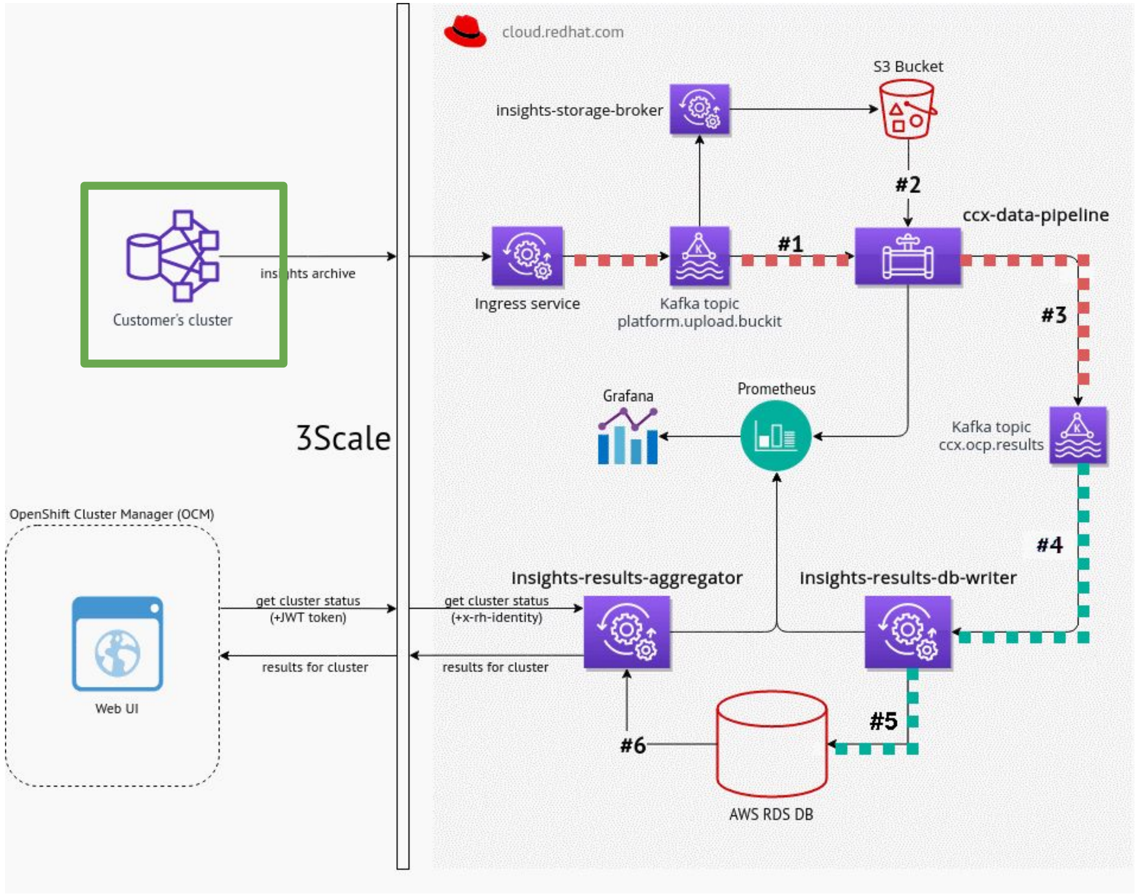
Throughput Performance Scalability Resilience



- Scalable parts
  - OCP rules engines
  - REST API service
- Parts that does not scale easily
  - Insights-results-db-writer
  - Fortunately just relatively small amount of time is spend by writes to DB

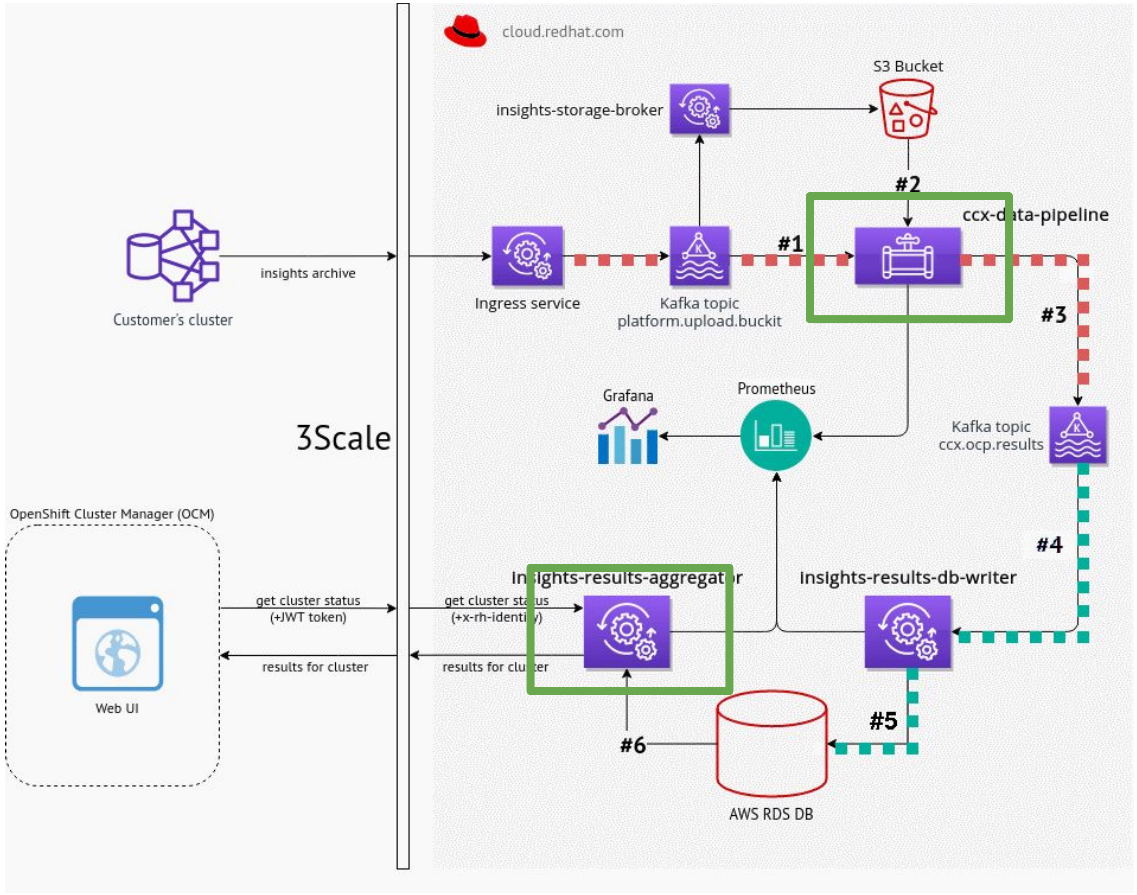
Throughput
Performance
Scalability
Resilience

- Thousands of connected clusters
- At least 10x in the future

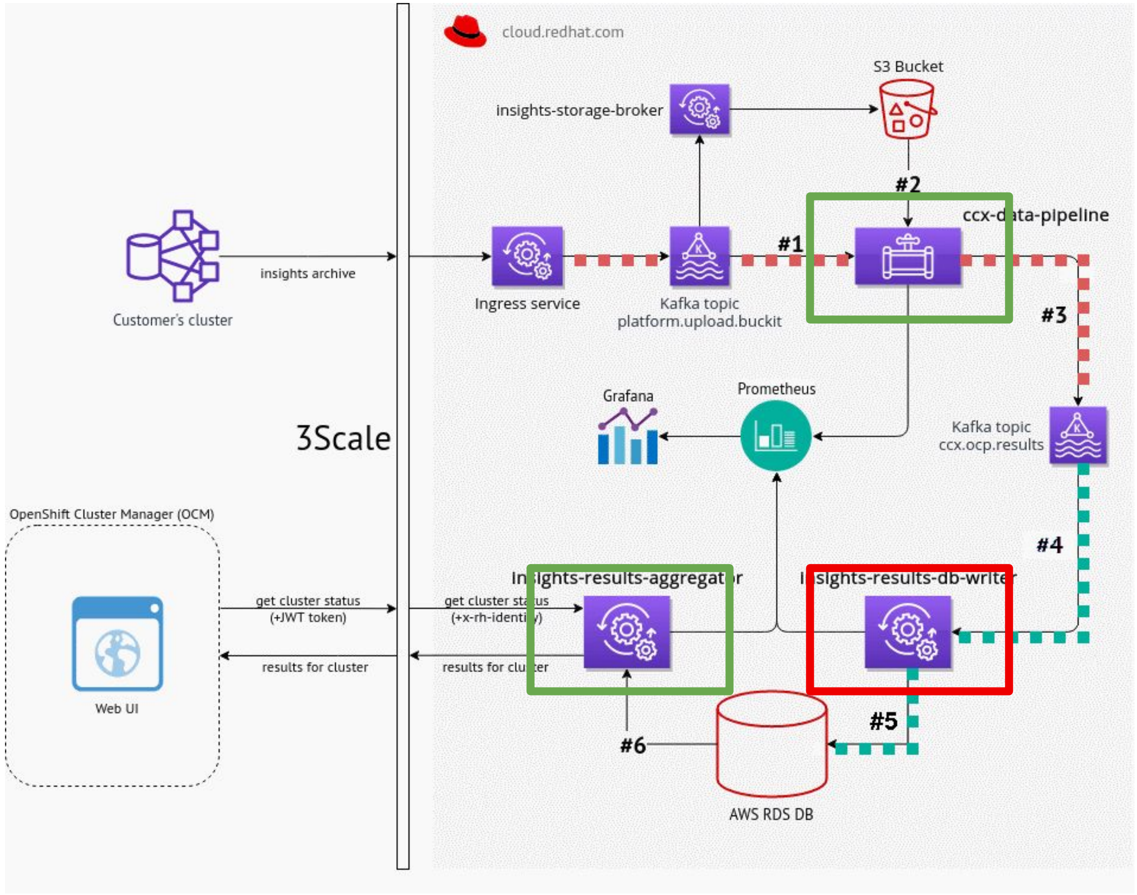


Throughput
Performance
Scalability
Resilience

- Scalable parts
  - OCP rules engines
  - REST API service

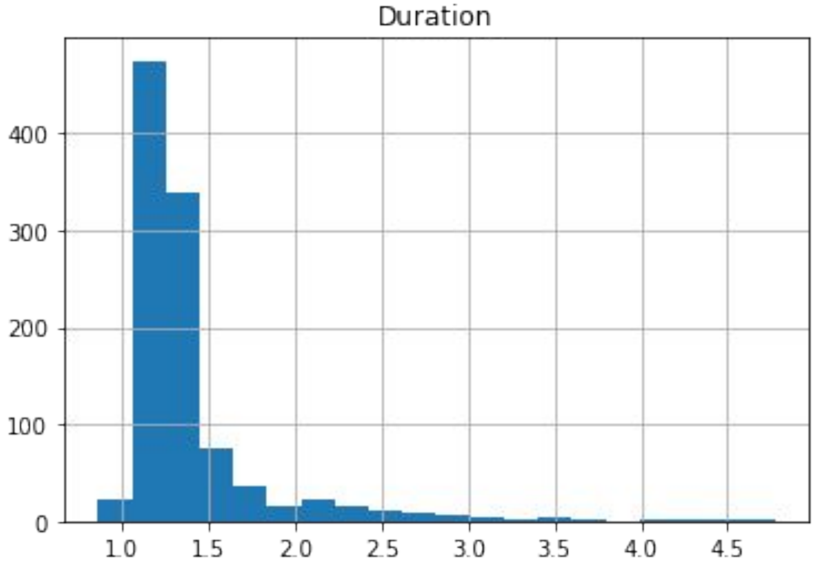


Throughput
Performance
Scalability
Resilience



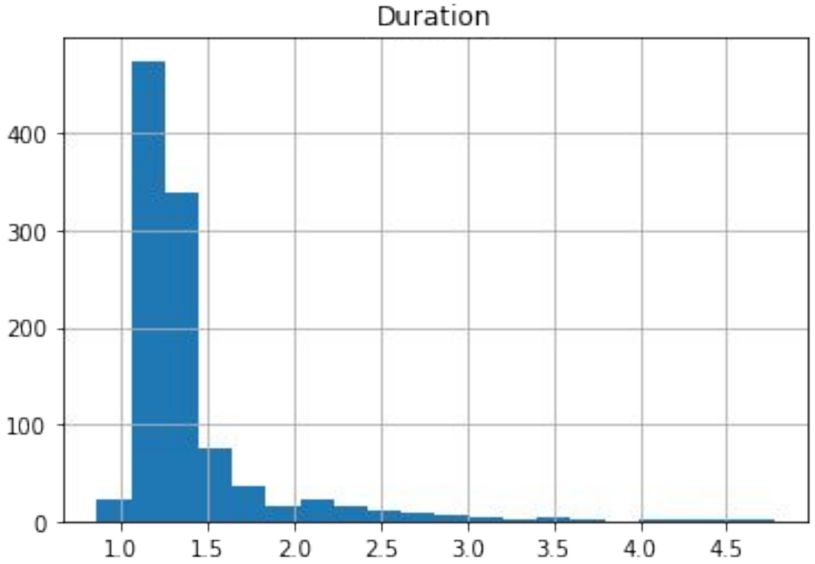
- Scalable parts
  - OCP rules engines
  - REST API service
- Parts that does not scale easily
  - Insights-results-db-writer
  - Fortunately just relatively small amount of time is spend by writes to DB
  - Horizontal splitting possible!

Processing part duration - OCP rules engine (in seconds)

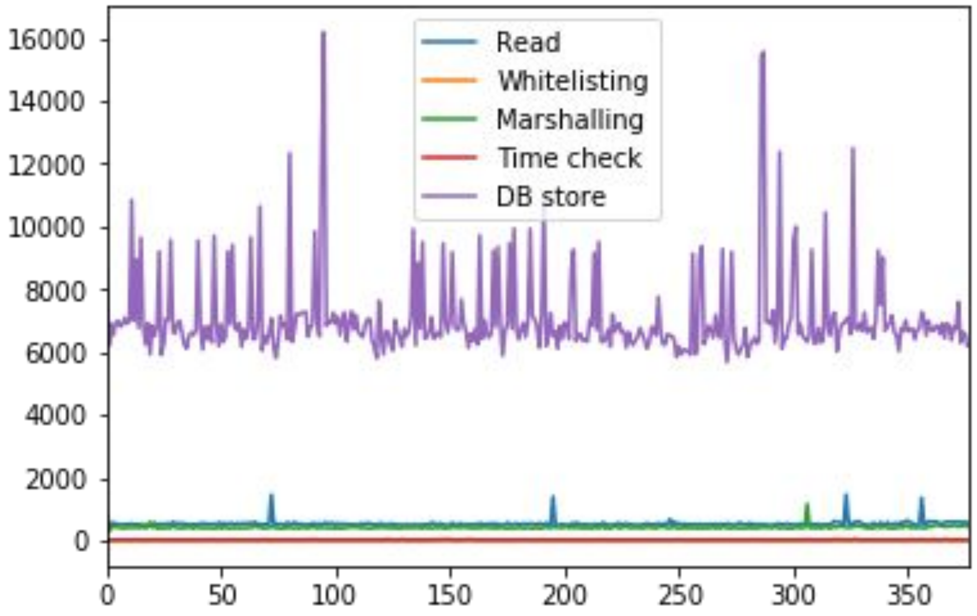


Processing part duration - OCP rules engine (in seconds)

- ~ 40 messages/second processed by one pod
- 5 pods enough for current message flow
- More pods can be created on demand

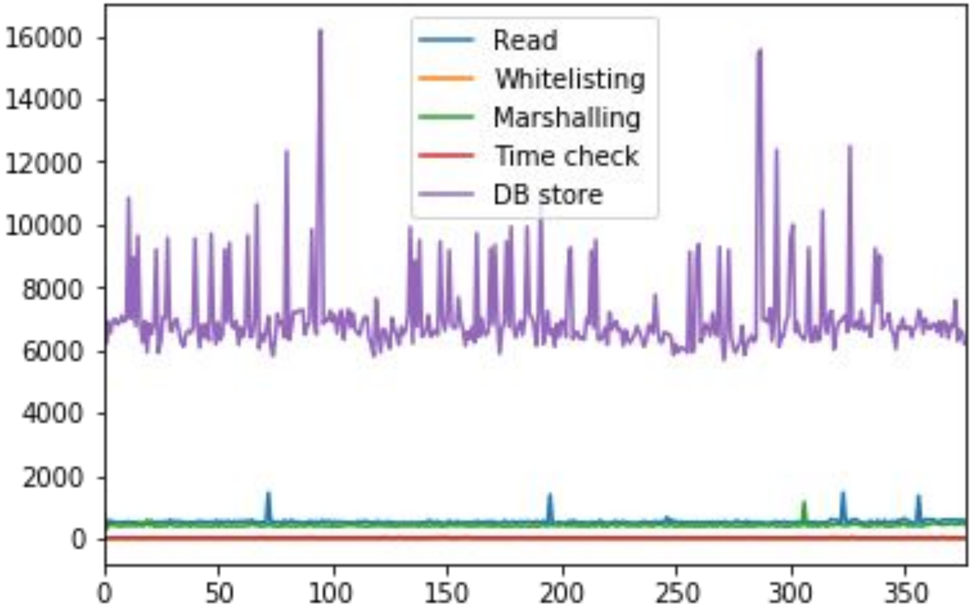


Writing into DB



Writing into DB

- DB store operation is the most time consuming
- It is the real bottleneck



Possible speedup

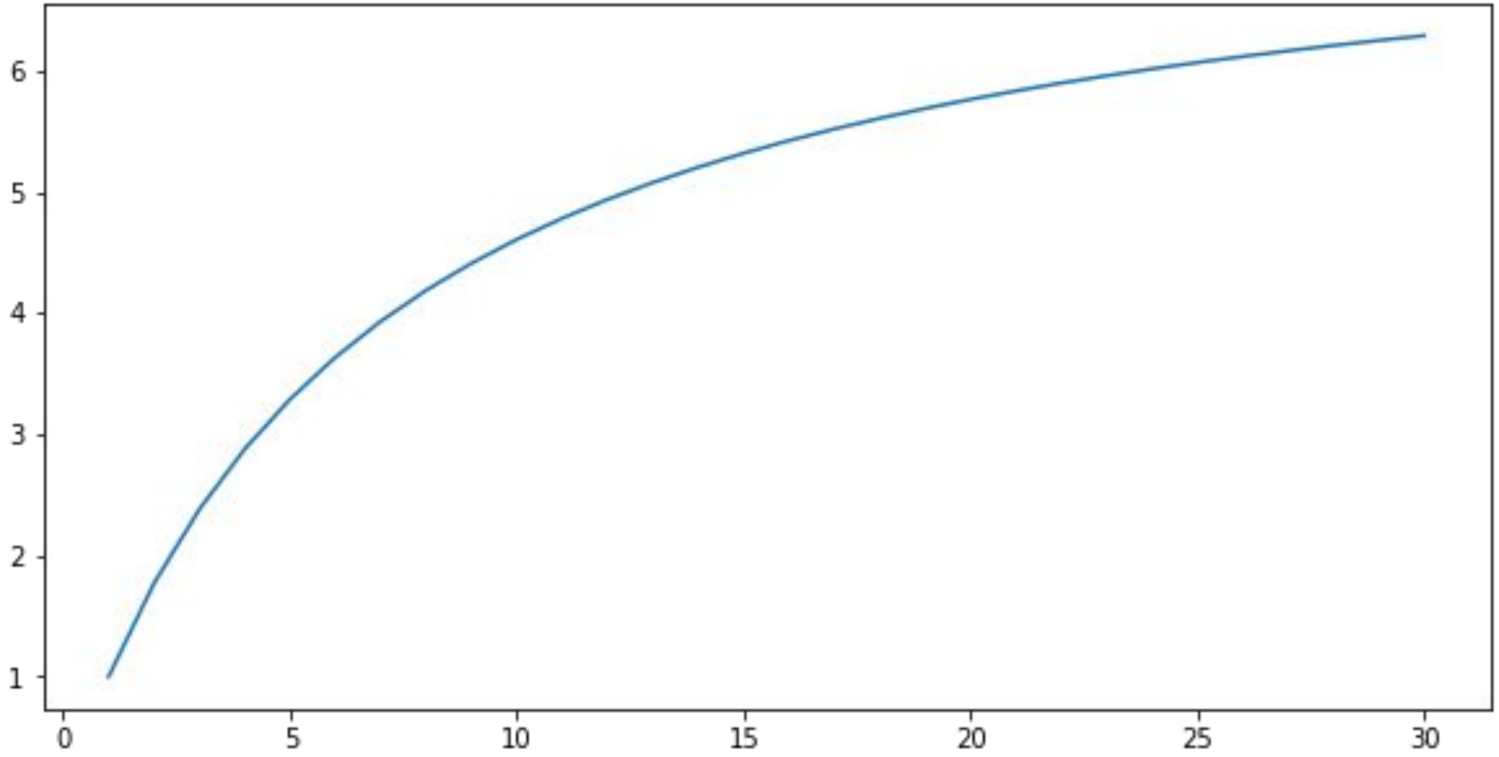
DB writer is THE bottleneck

 * 32 pods -> 6x throughput

The rest of pipeline scale well

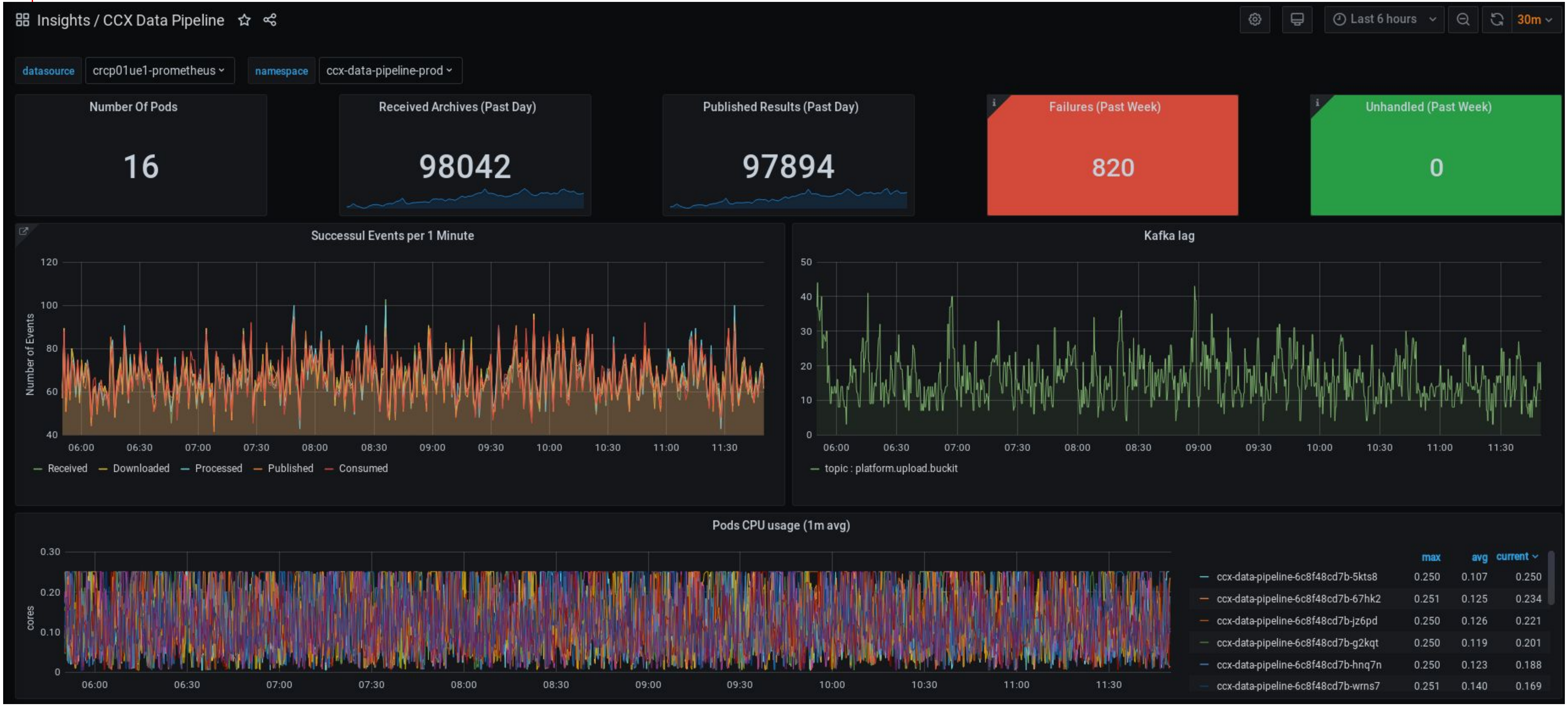
 * almost linearly

Amdahl’s law



Monitoring

Service monitoring



Insights / CCX Data Pipeline

Last 6 hours

30m

datasource: crcp01ue1-prometheus

namespace: ccx-data-pipeline-prod

Number Of Pods: 16

Received Archives (Past Day): 98042

Published Results (Past Day): 97894

Failures (Past Week): 820

Unhandled (Past Week): 0

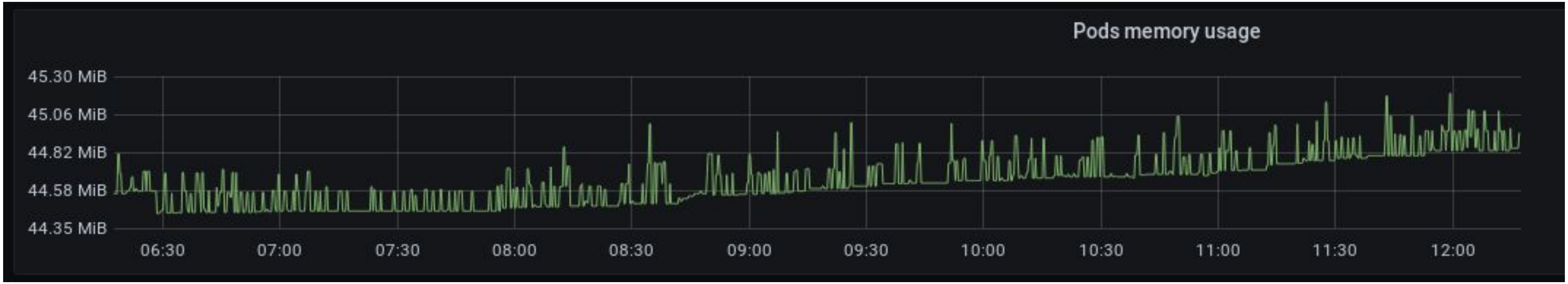
Successul Events per 1 Minute

Kafka lag

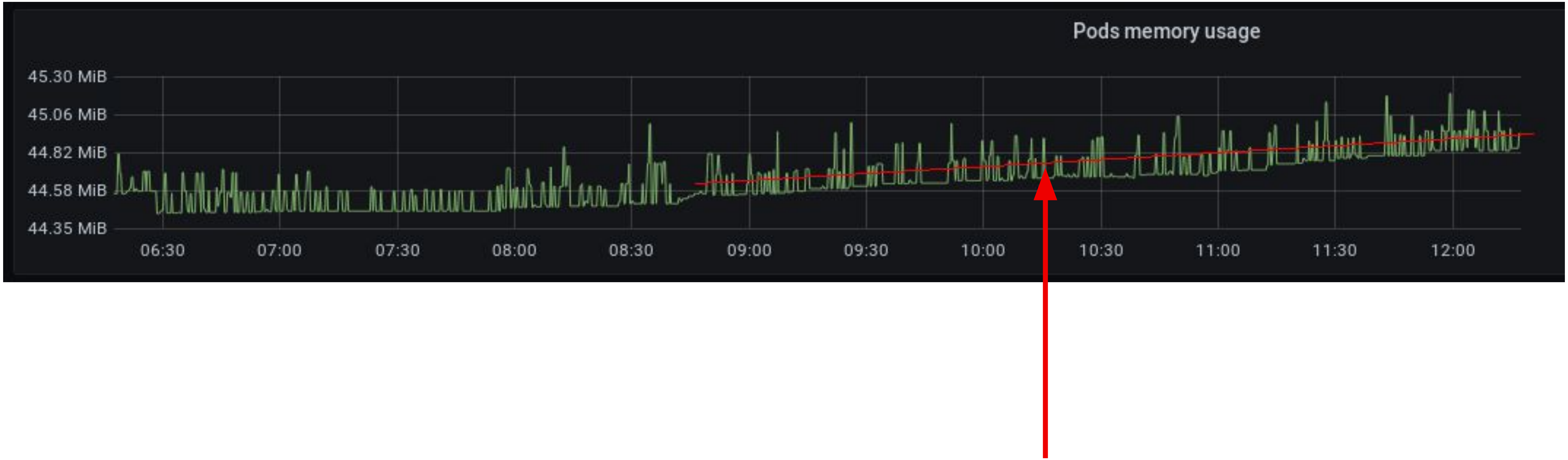
Pods CPU usage (1m avg)

	max	avg	current
ccx-data-pipeline-6c8f48cd7b-5kts8	0.250	0.107	0.250
ccx-data-pipeline-6c8f48cd7b-67hk2	0.251	0.125	0.234
ccx-data-pipeline-6c8f48cd7b-jz6pd	0.250	0.126	0.221
ccx-data-pipeline-6c8f48cd7b-g2kqt	0.250	0.119	0.201
ccx-data-pipeline-6c8f48cd7b-hnq7n	0.250	0.123	0.188
ccx-data-pipeline-6c8f48cd7b-wrns7	0.251	0.140	0.169

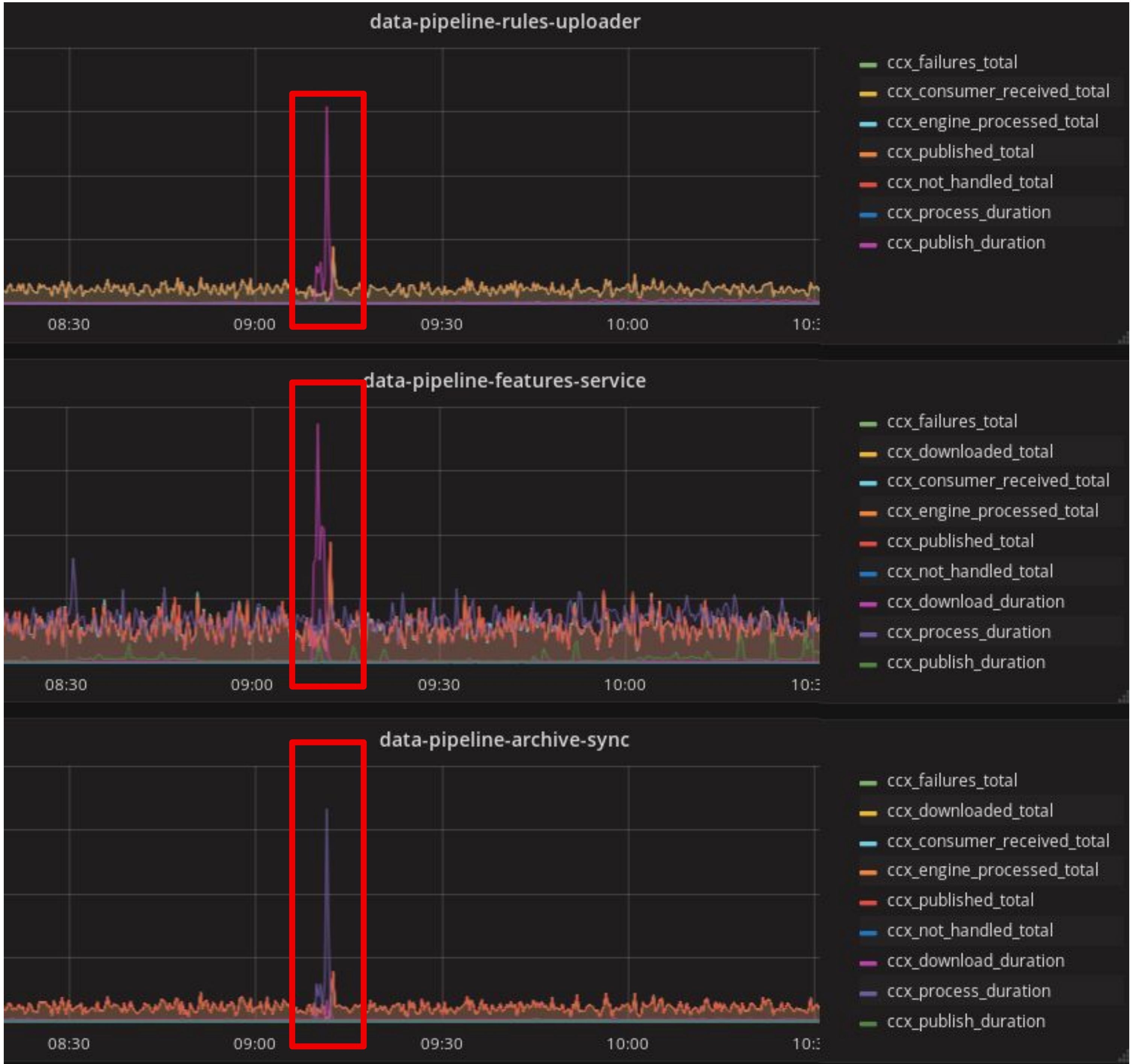
Detecting GC issues



Detecting GC issues



Storage-related issues



Alerts

- Some situations could lead into an outage of the health checks
  - Stop receiving archives from customer clusters due to some connectivity problem
  - Problems in the used infrastructure, like Kafka
  - BUGS in the code (not very much, we are good)
- The status of the whole system is being monitored 24/7
- Define thresholds which will trigger alerts

But...

Alerts

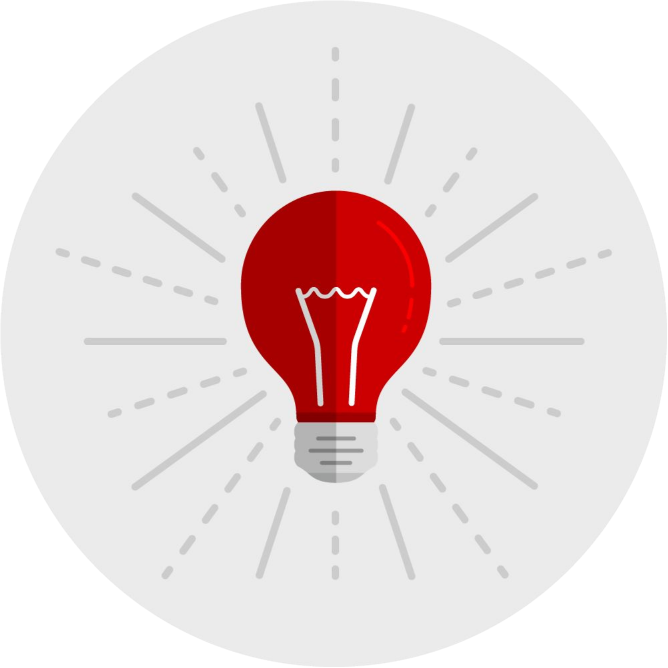
Who is watching the watcher?

Alerts

- If we only trigger alerts when something bad happens, we cannot know what is happening when there is no alerts
- “Continuous testing” mechanism
  - An end-to-end test is triggered every 30 minutes
  - Both possible results are notified
- Lack of notification IS an alert

Wrap-up

Wrap up



Scalable technologies based on OpenShift and Kafka

DB writer is the bottleneck

Monitoring is essential part of the whole pipeline

Lack of notification in alerting mechanisms is an alert

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

in linkedin.com/company/red-hat

▶ youtube.com/user/RedHatVideos

f facebook.com/redhatinc

twitter.com/RedHat