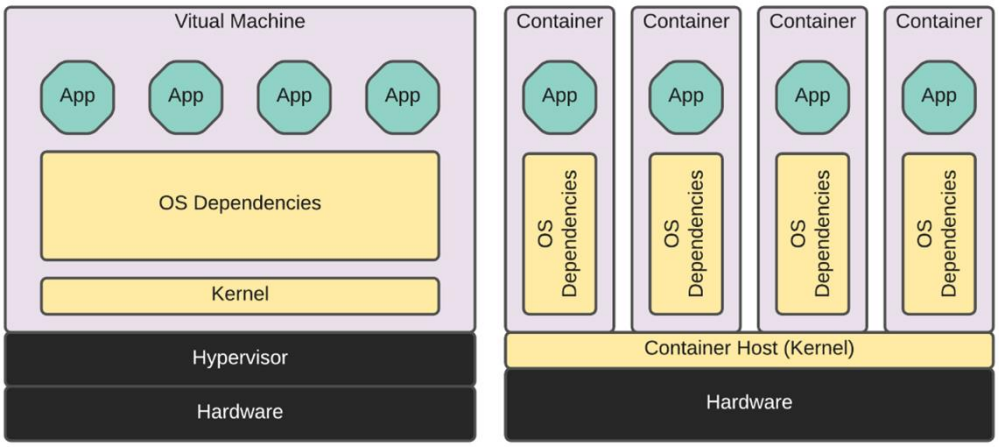
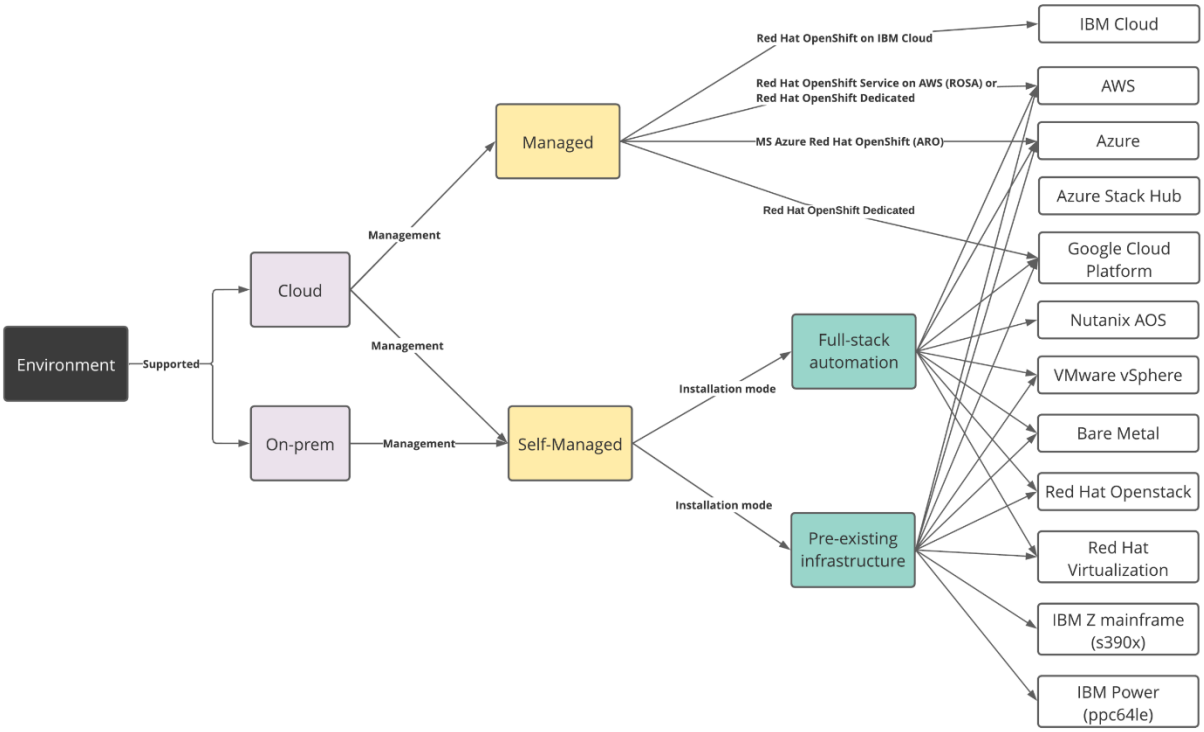
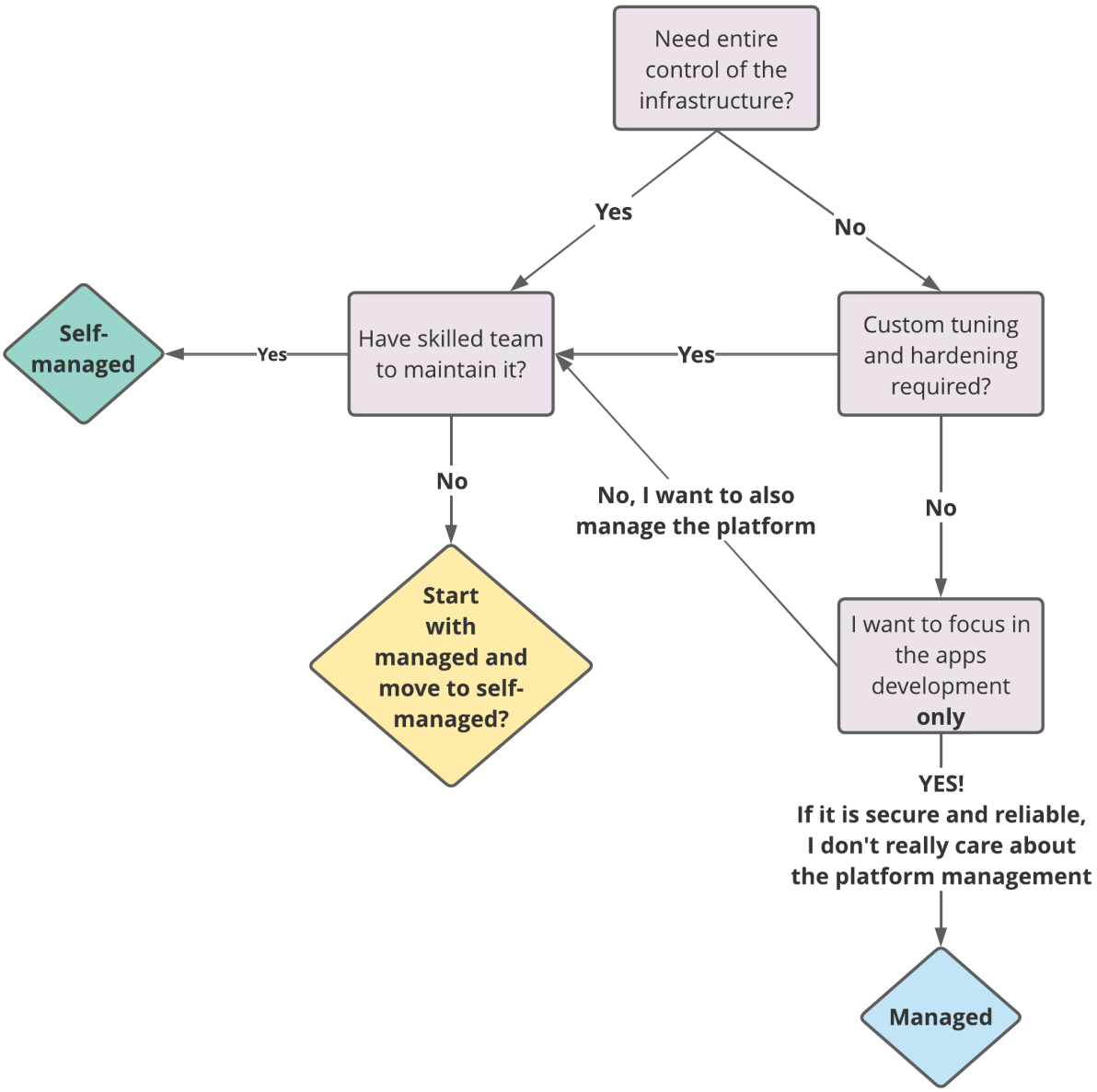
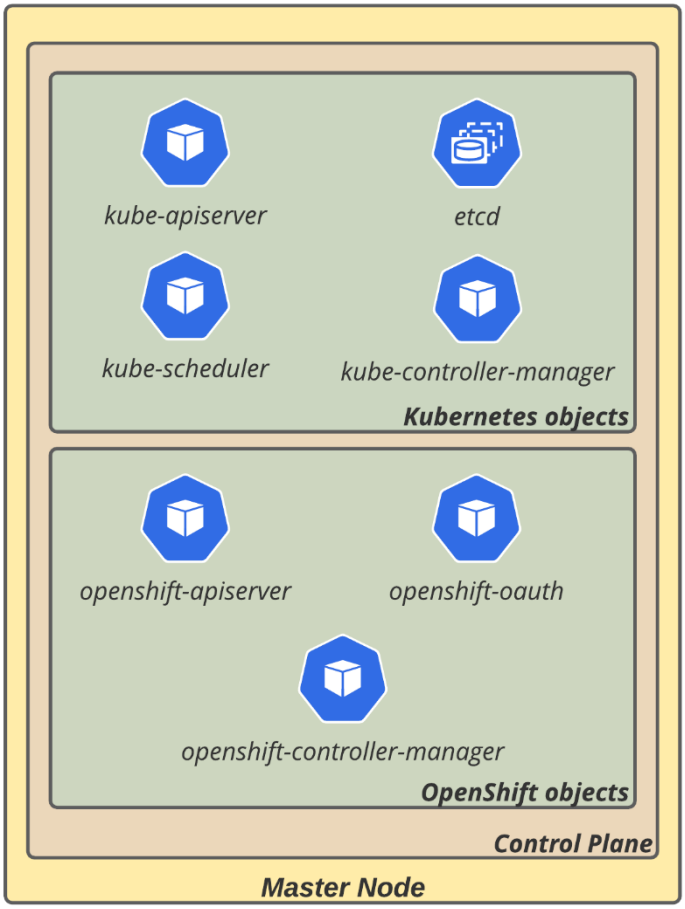
Chapter 1: Hybrid Cloud Journey and Strategies

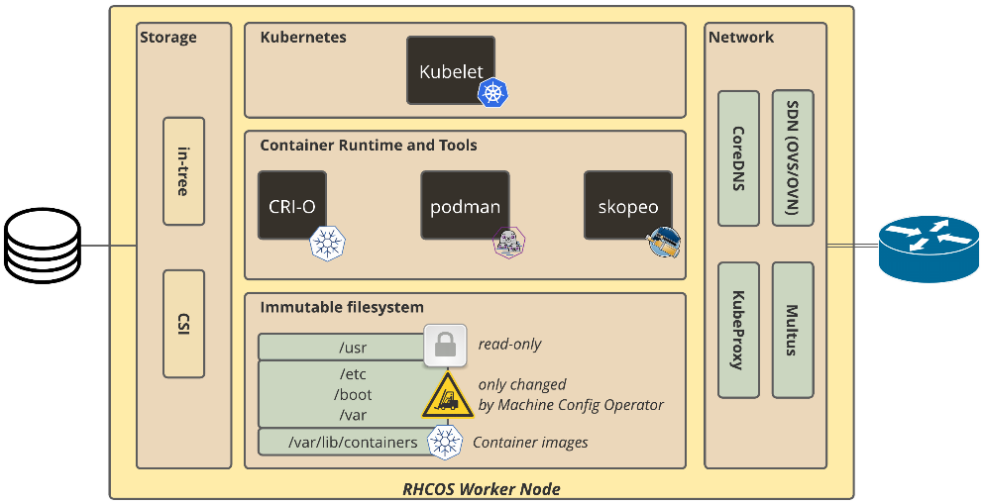


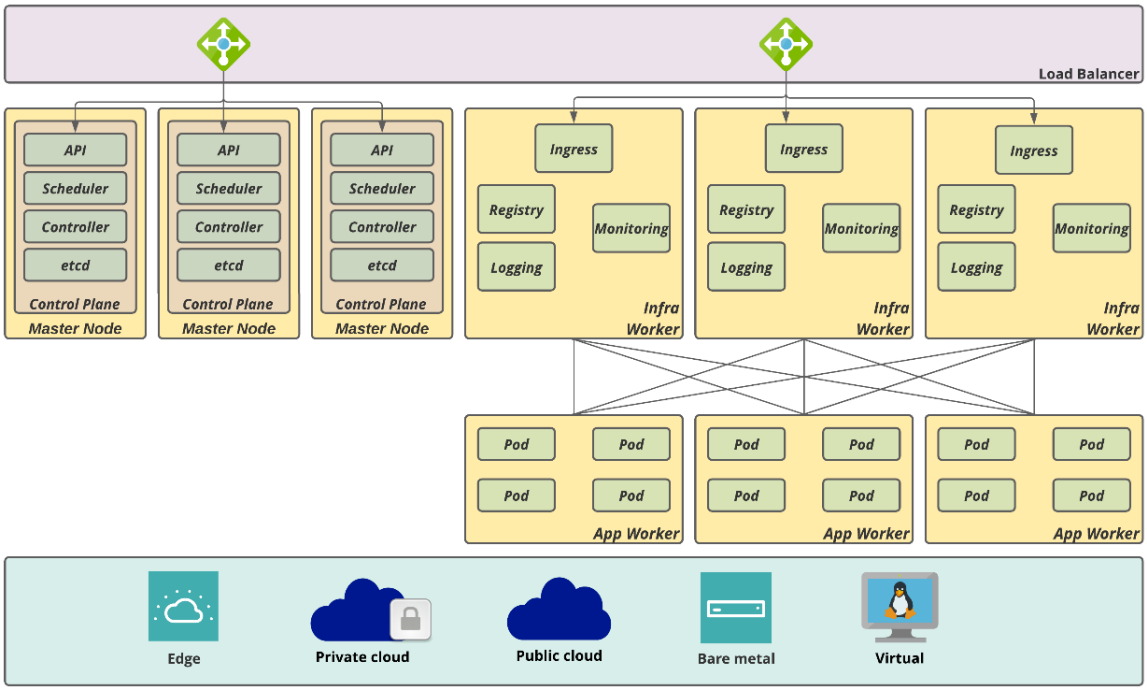


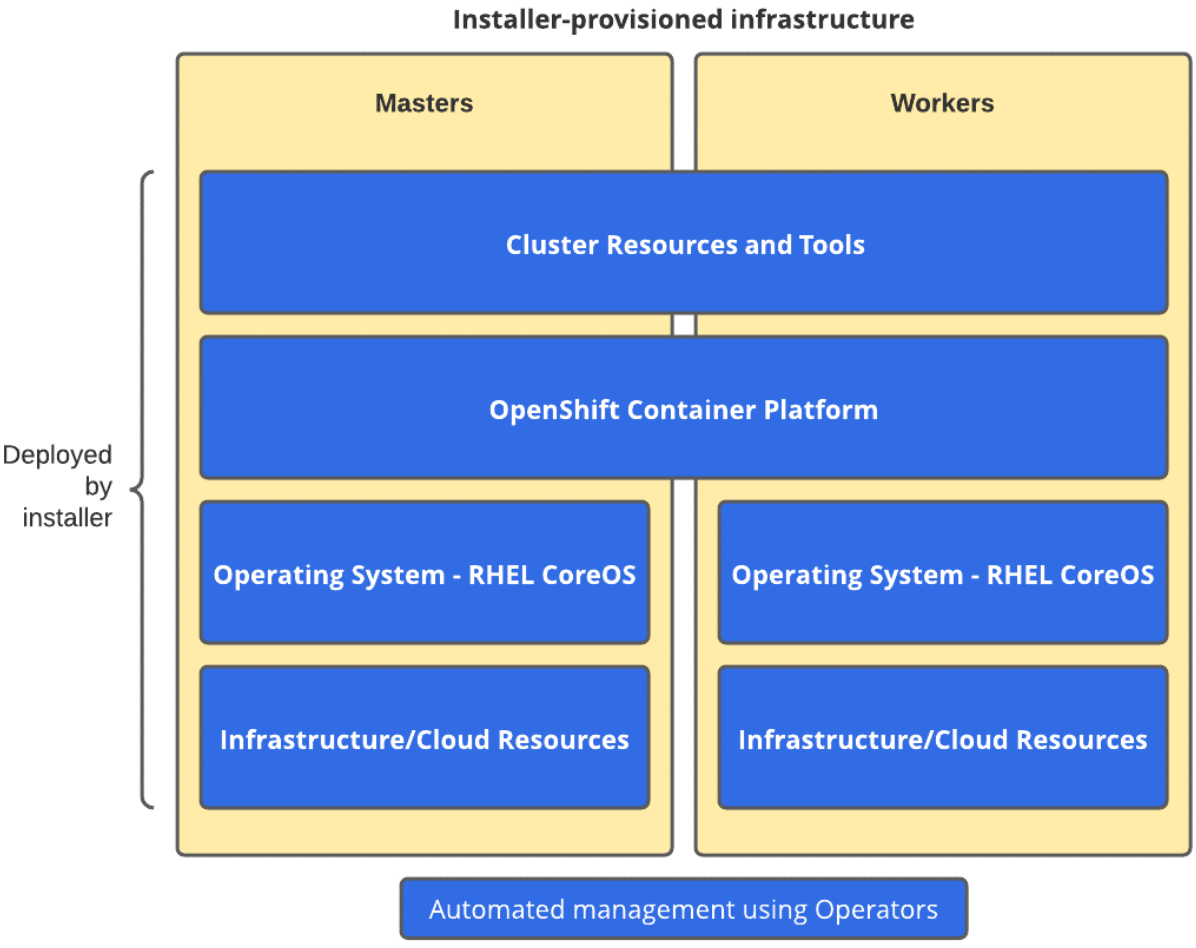

Need entire control of the infrastructure?
Yes
No
Have skilled team to maintain it?
Yes
Self-managed
Yes
Custom tuning and hardening required?
No
Start with managed and move to self-managed?
No, I want to also manage the platform
No
I want to focus in the apps development only
YES!
If it is secure and reliable, I don't really care about the platform management
Managed

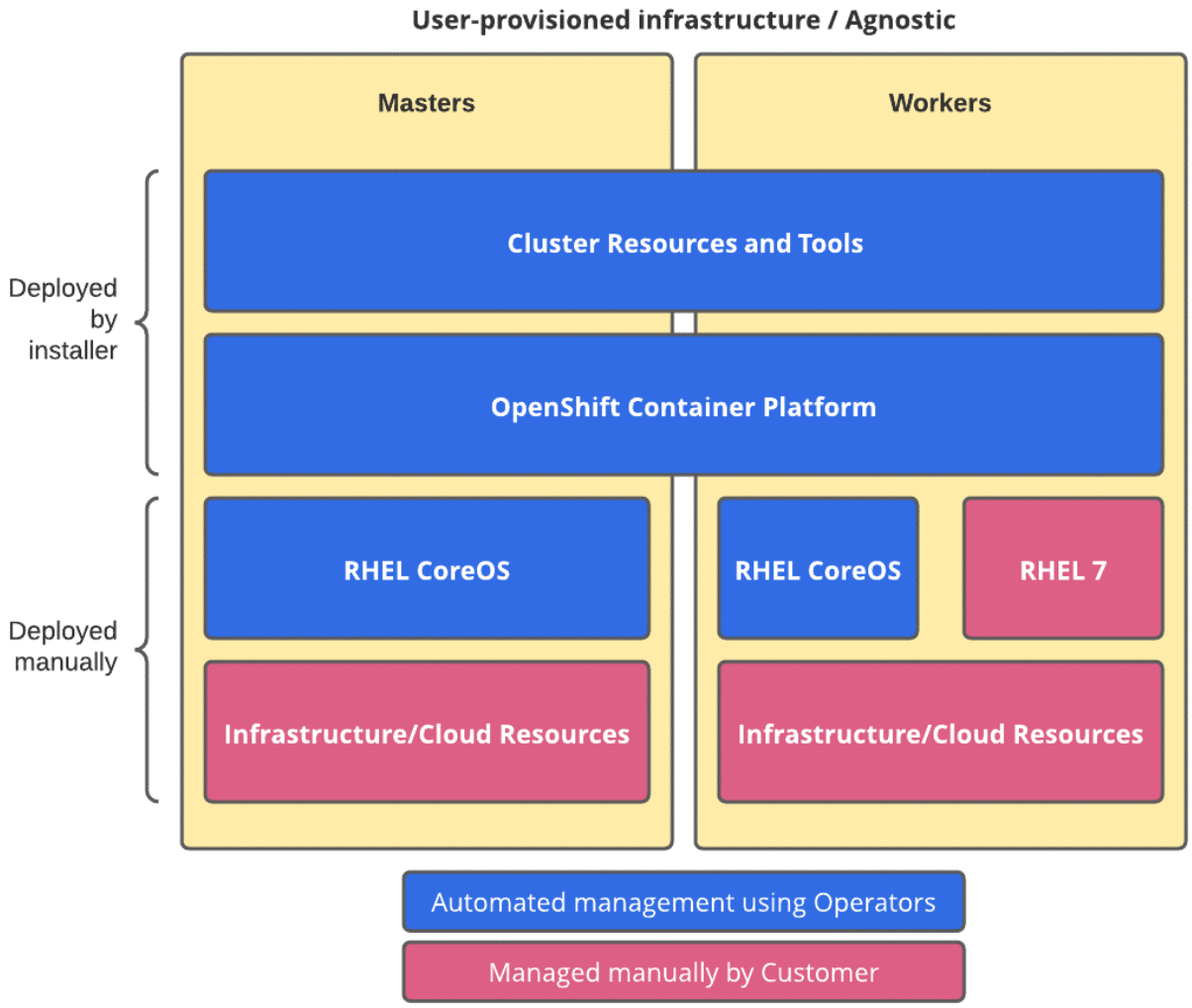
Chapter 2: Architecture Overview and Definitions

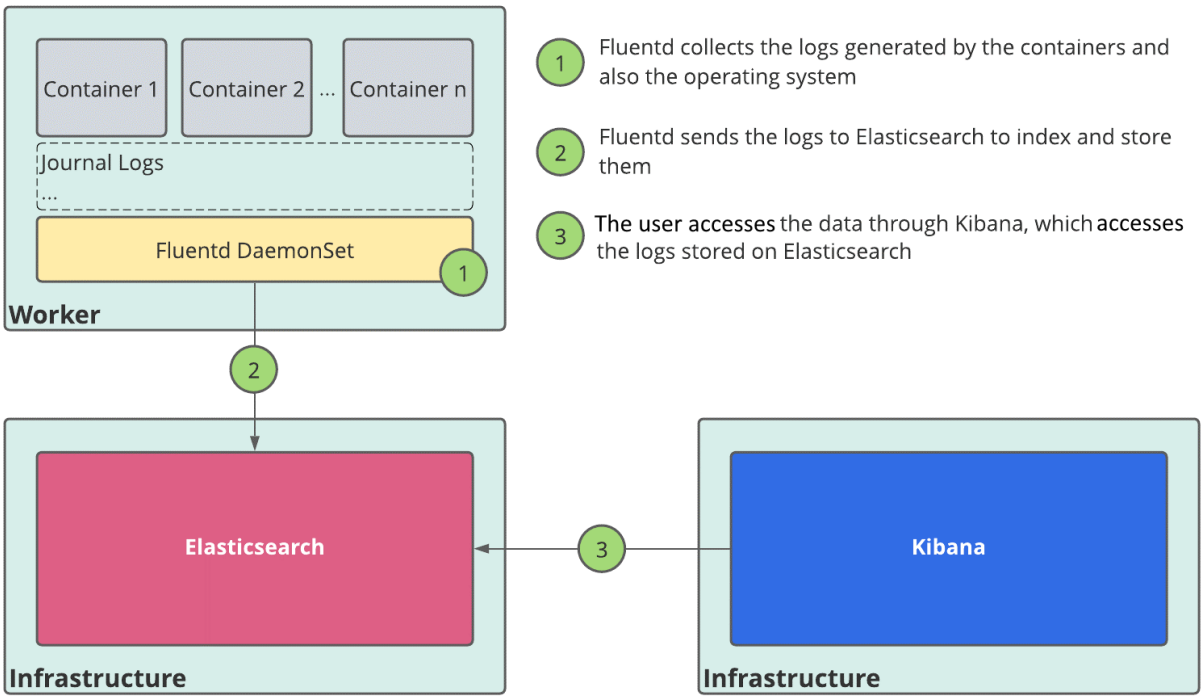


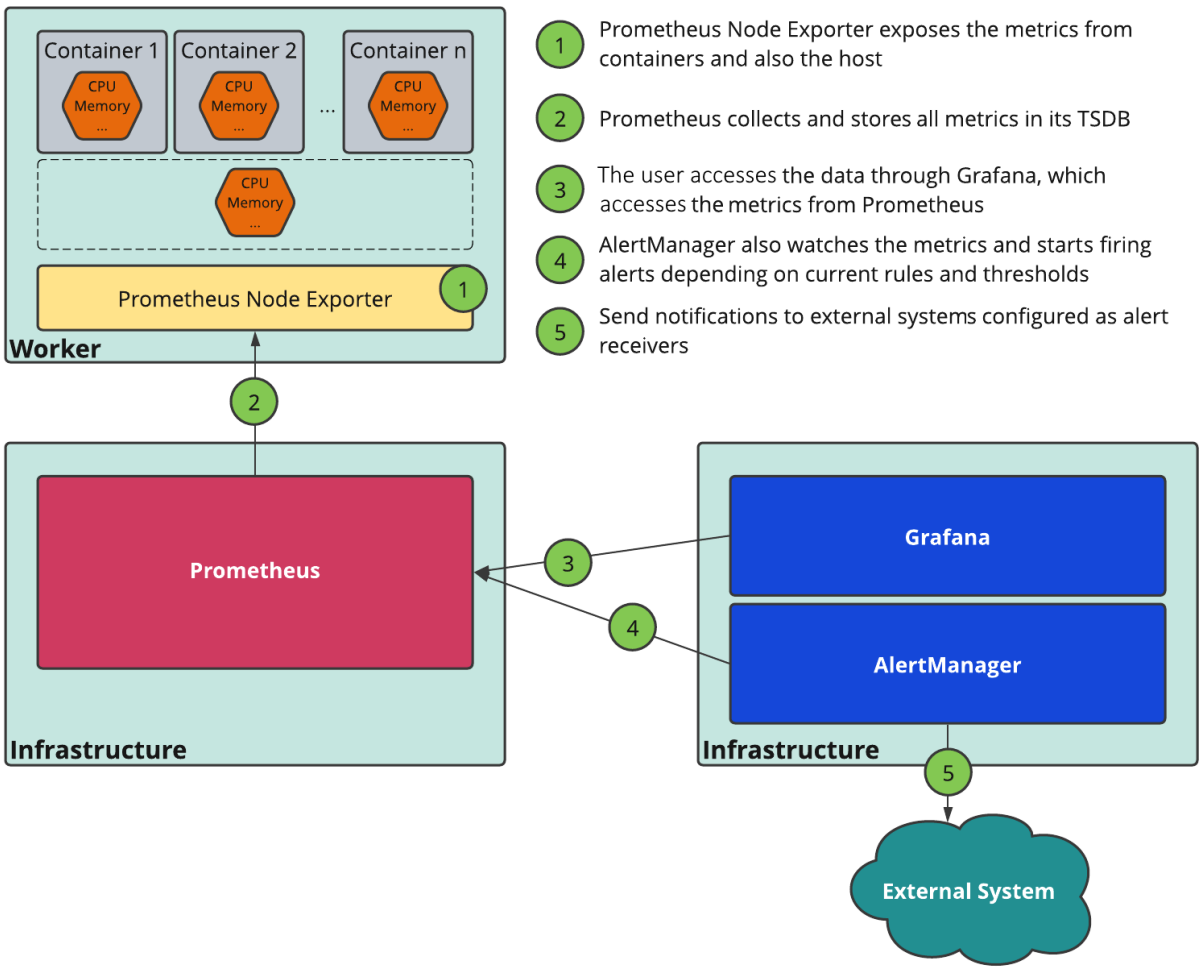



Load Balancer
API
Scheduler
Controller
etcd
Control Plane
Master Node
Ingress
Registry
Logging
Monitoring
Infra Worker
Pod
App Worker
Edge
Private cloud
Public cloud
Bare metal
Virtual

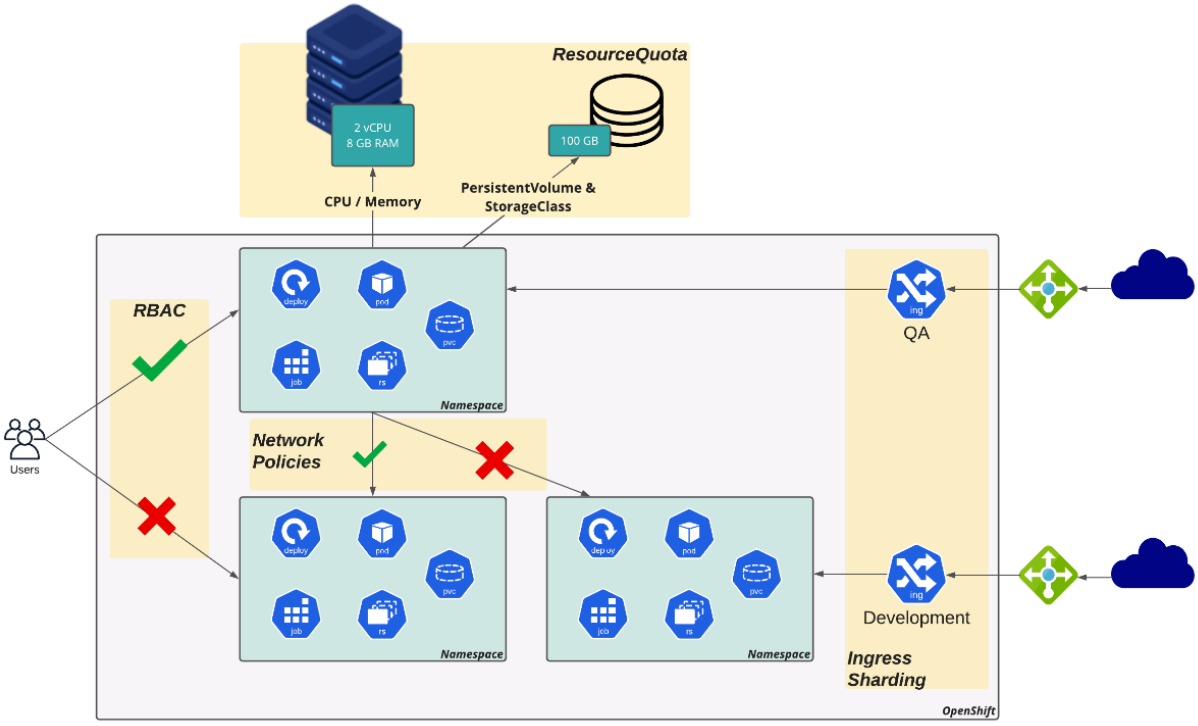

Installer-provisioned infrastructure
Masters
Workers
Cluster Resources and Tools
OpenShift Container Platform
Operating System - RHEL CoreOS
Infrastructure/Cloud Resources
Deployed by installer
Automated management using Operators

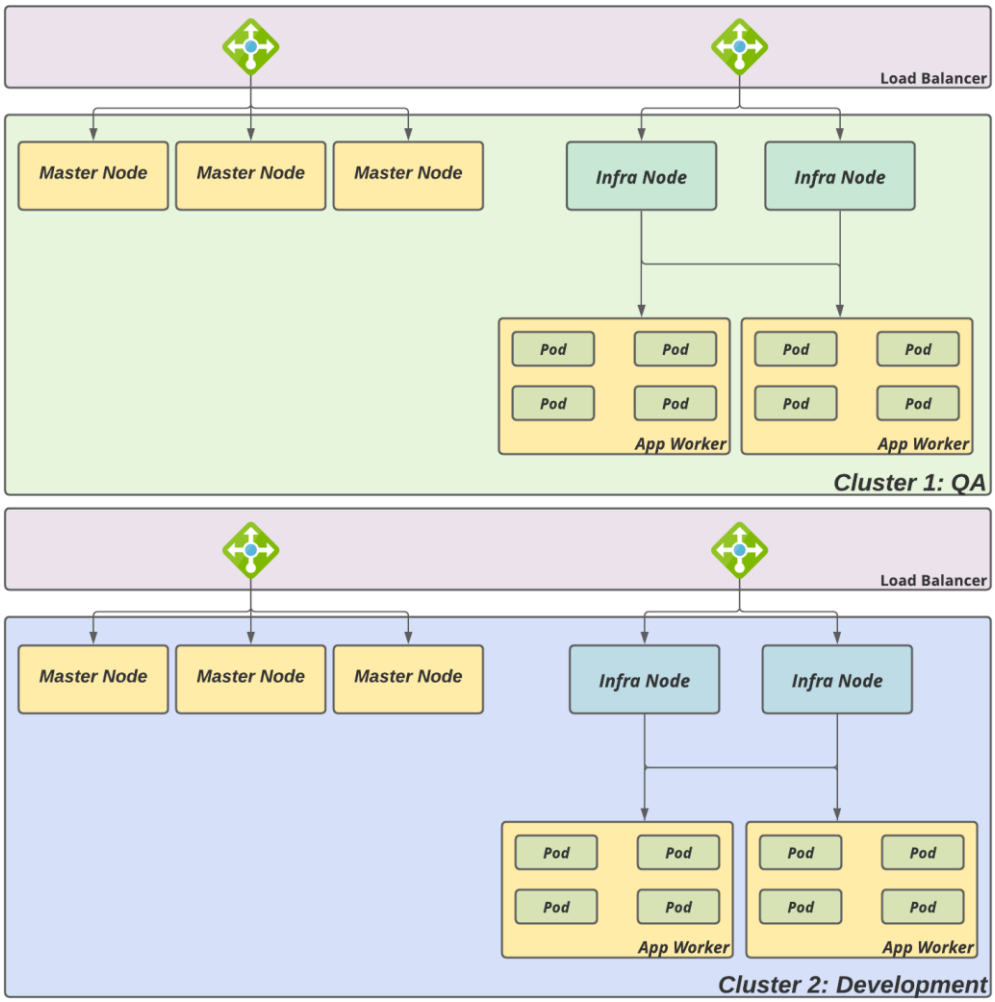

User-provisioned infrastructure / Agnostic
Masters
Workers
Deployed by installer
Deployed manually
Cluster Resources and Tools
OpenShift Container Platform
RHEL CoreOS
RHEL CoreOS
RHEL 7
Infrastructure/Cloud Resources
Infrastructure/Cloud Resources
Automated management using Operators
Managed manually by Customer

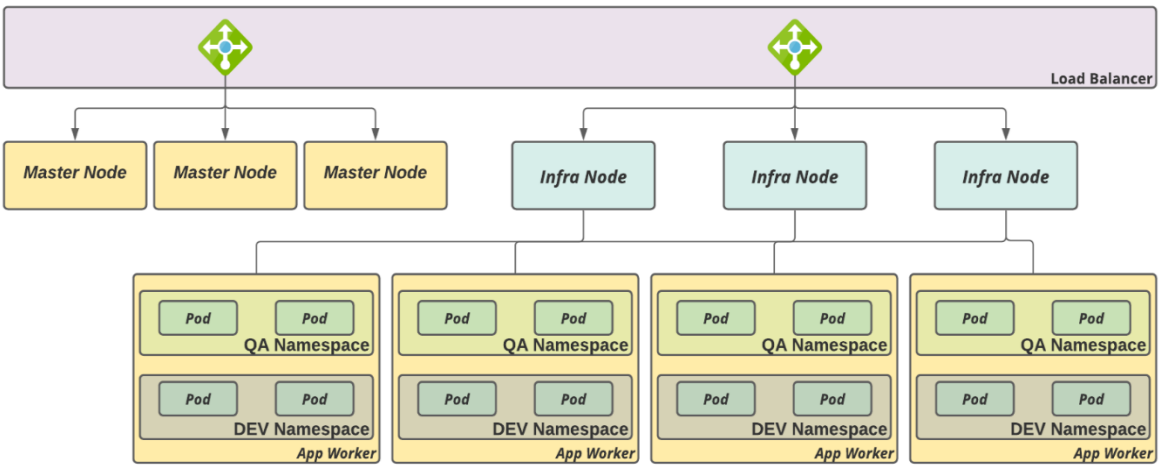

Container 1
Container 2
...
Container n
Journal Logs
...
Fluentd DaemonSet
1
Worker
2
Elasticsearch
3
Kibana
Infrastructure
Infrastructure
1 Fluentd collects the logs generated by the containers and also the operating system
2 Fluentd sends the logs to Elasticsearch to index and store them
3 The user accesses the data through Kibana, which accesses the logs stored on Elasticsearch

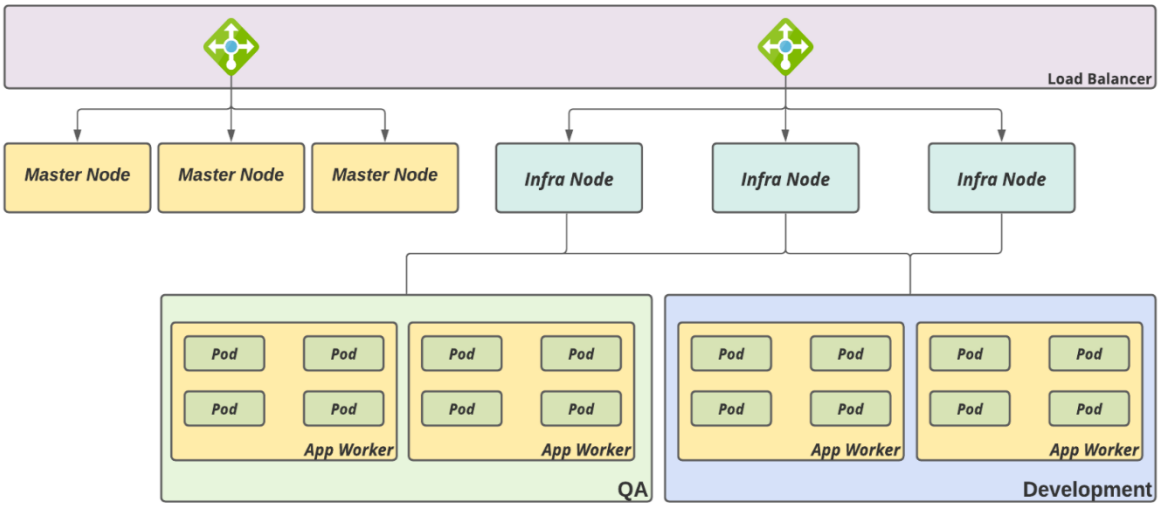

Container 1
CPU
Memory
...
Container 2
CPU
Memory
...
...
Container n
CPU
Memory
...
CPU
Memory
...
Prometheus Node Exporter
1
Worker
2
Prometheus
Infrastructure
3
4
Grafana
AlertManager
Infrastructure
5
External System
1 Prometheus Node Exporter exposes the metrics from containers and also the host
2 Prometheus collects and stores all metrics in its TSDB
3 The user accesses the data through Grafana, which accesses the metrics from Prometheus
4 AlertManager also watches the metrics and starts firing alerts depending on current rules and thresholds
5 Send notifications to external systems configured as alert receivers

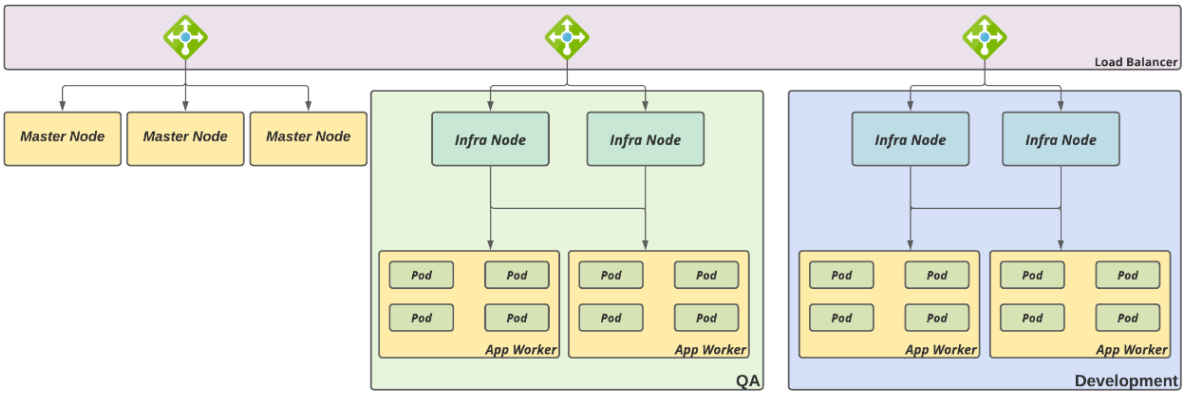
Chapter 3: Multi-Tenant Considerations



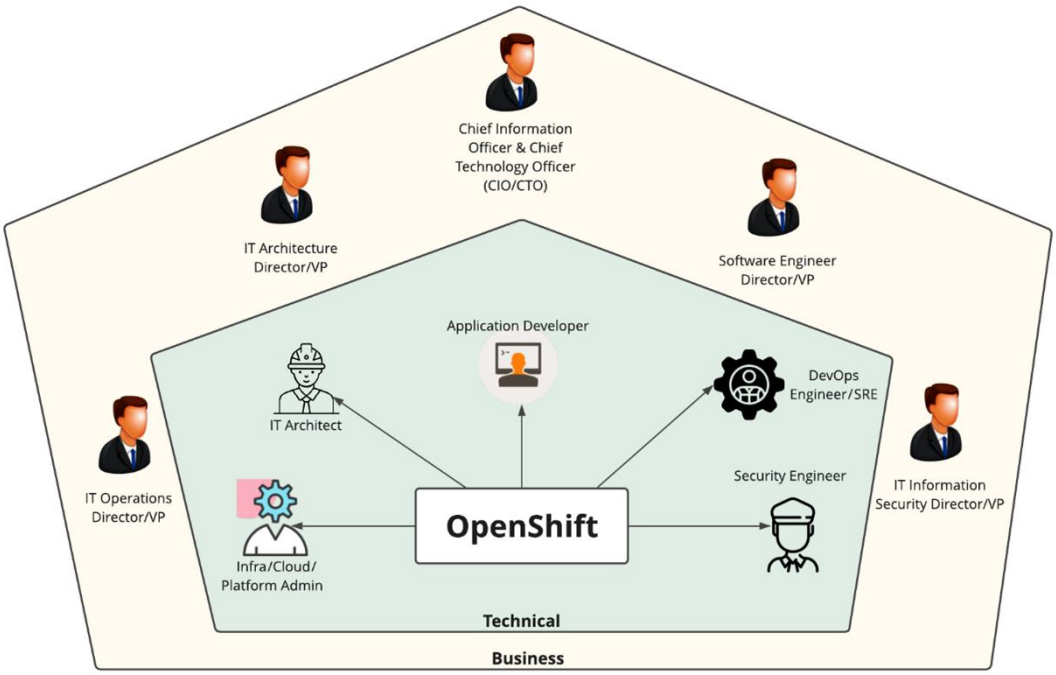

Load Balancer
Master Node
Master Node
Master Node
Infra Node
Infra Node
Pod
Pod
Pod
Pod
App Worker
Pod
Pod
Pod
Pod
App Worker
Cluster 1: QA
Load Balancer
Master Node
Master Node
Master Node
Infra Node
Infra Node
Pod
Pod
Pod
Pod
App Worker
Pod
Pod
Pod
Pod
App Worker
Cluster 2: Development


Load Balancer
Master Node
Master Node
Master Node
Infra Node
Infra Node
Infra Node
Pod
Pod
QA Namespace
Pod
Pod
DEV Namespace
App Worker
Pod
Pod
QA Namespace
Pod
Pod
DEV Namespace
App Worker
Pod
Pod
QA Namespace
Pod
Pod
DEV Namespace
App Worker
Pod
Pod
QA Namespace
Pod
Pod
DEV Namespace
App Worker

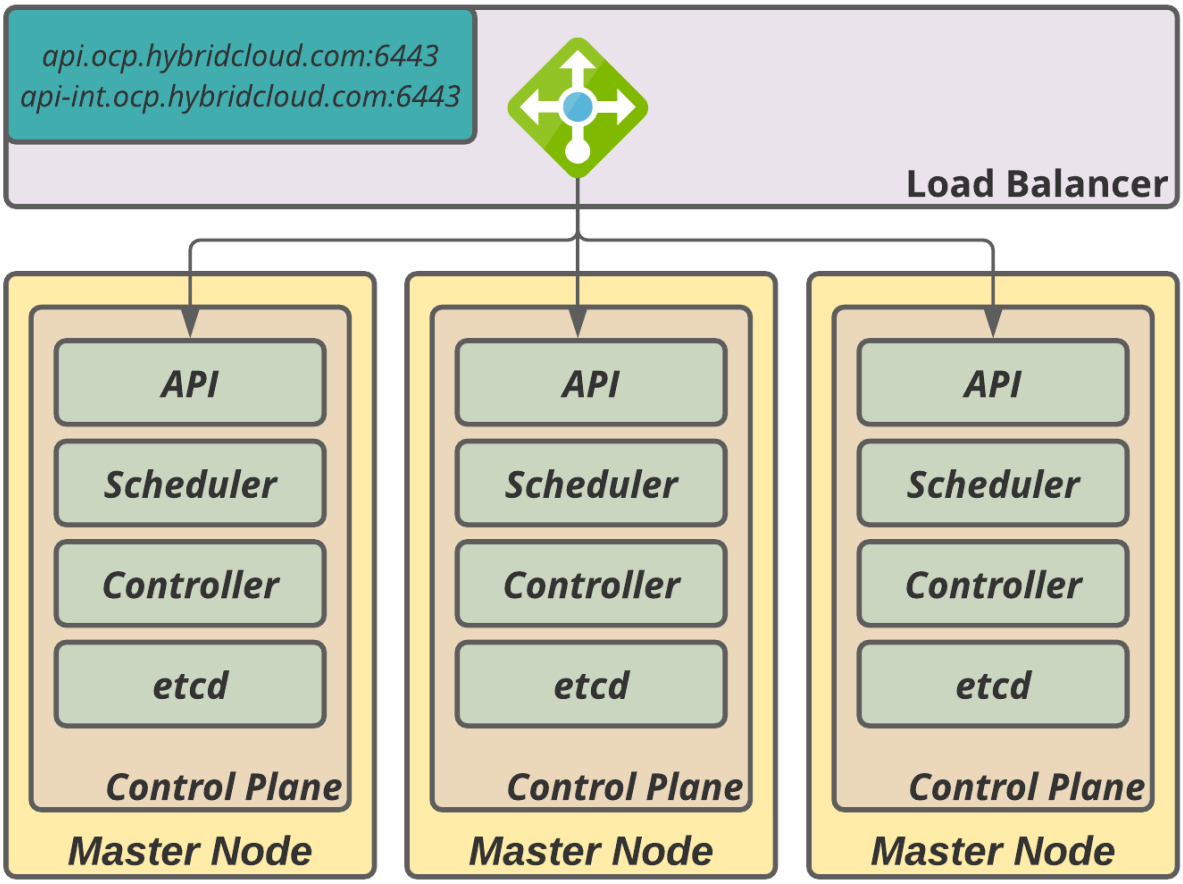

Load Balancer
Master Node
Master Node
Master Node
Infra Node
Infra Node
Infra Node
Pod
App Worker
QA
Development

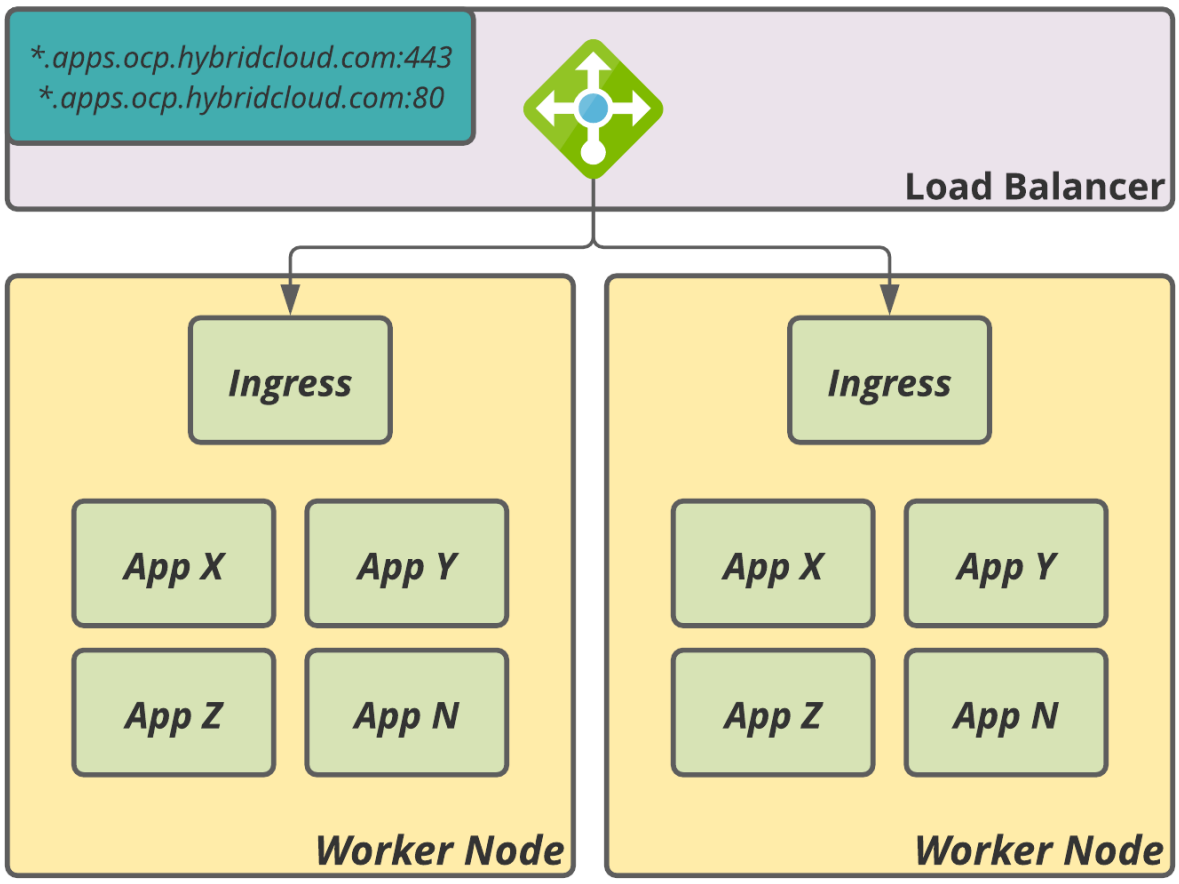

Load Balancer
Master Node
Master Node
Master Node
Infra Node
Infra Node
Infra Node
Infra Node
Pod
App Worker
QA
Development

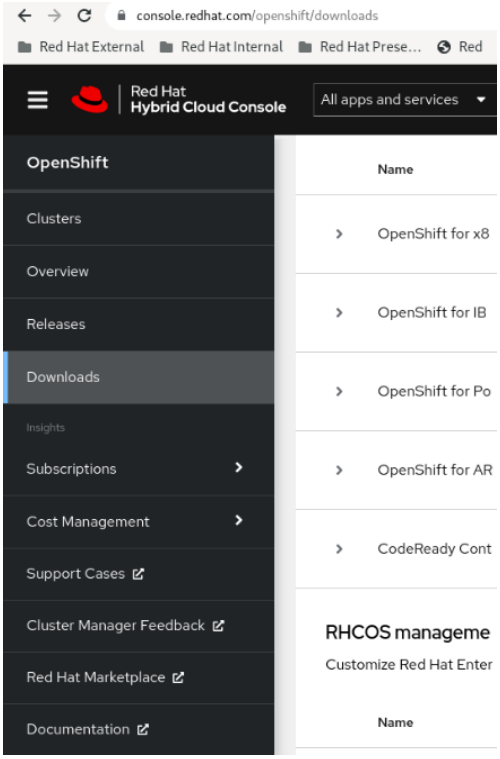
Chapter 4: OpenShift Personas and Skillsets



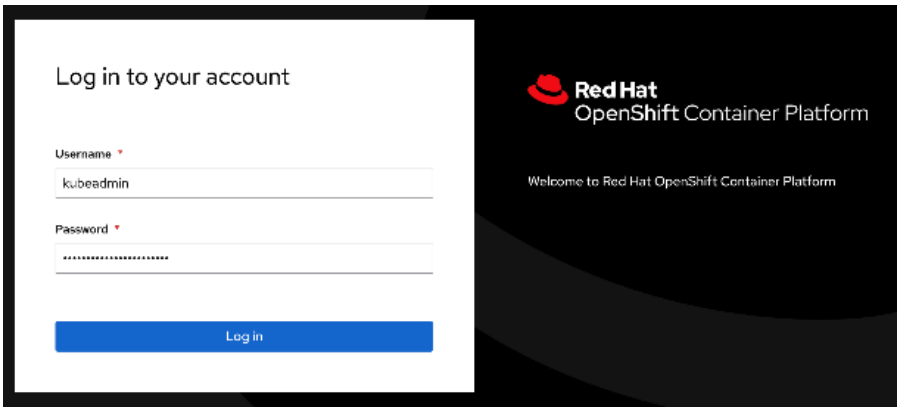
Chapter 5: OpenShift Deployment

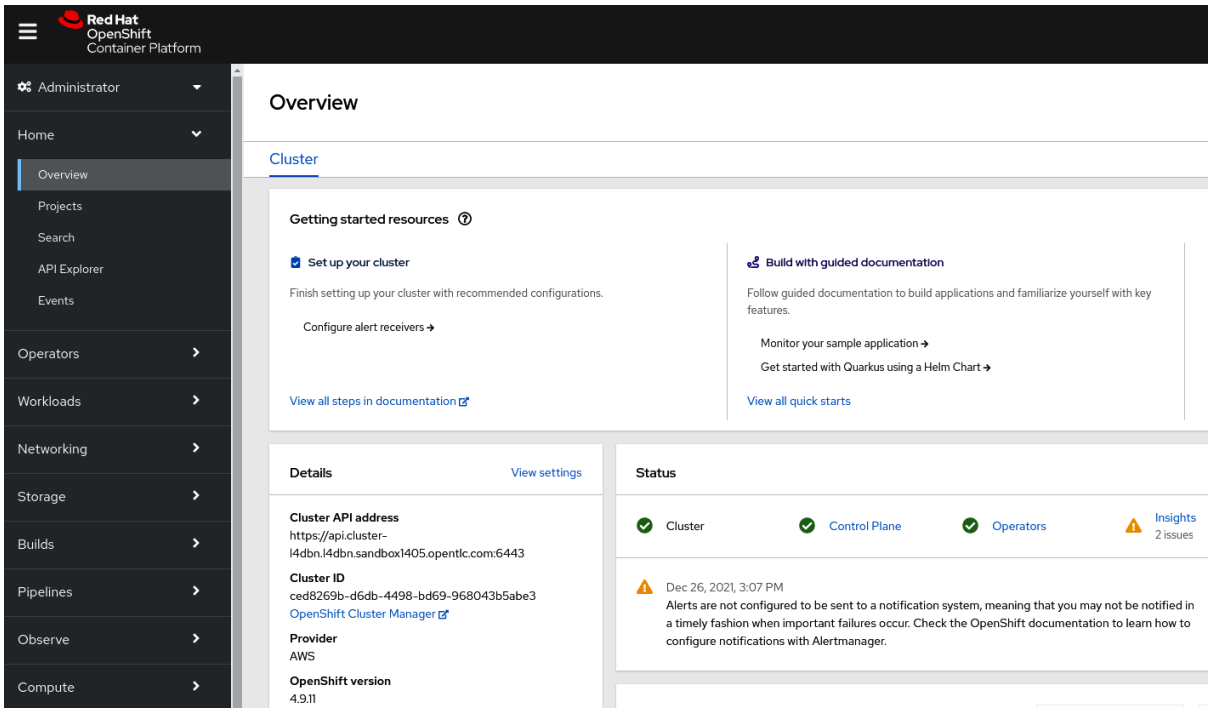



*.apps.ocp.hybridcloud.com:443
*.apps.ocp.hybridcloud.com:80
Load Balancer
Ingress
App X
App Y
App Z
App N
Worker Node
Ingress
App X
App Y
App Z
App N
Worker Node

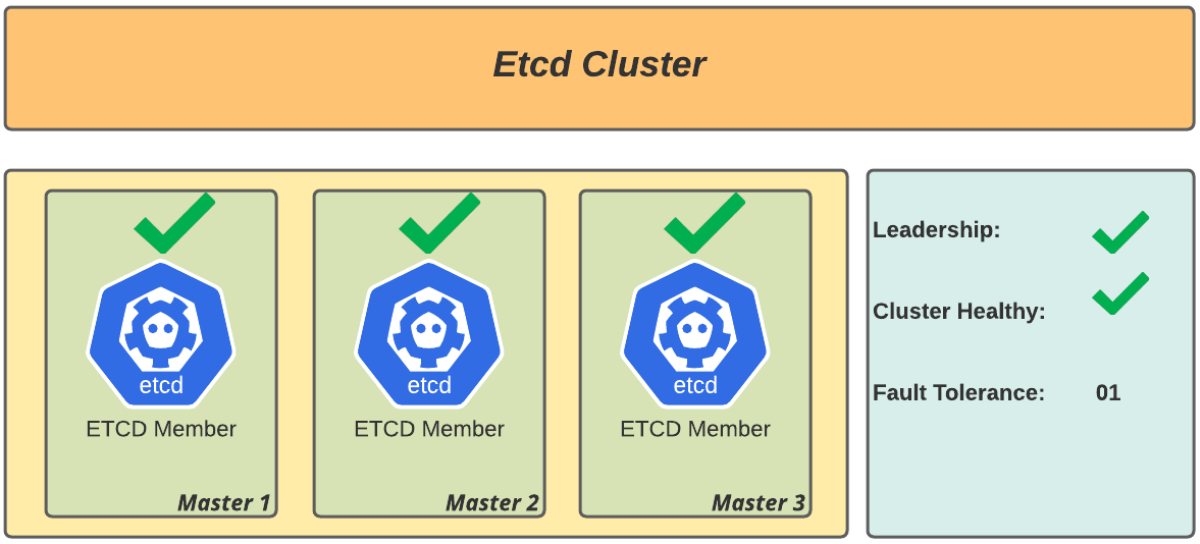

console.redhat.com/openshift/downloads
Red Hat External
Red Hat Internal
Red Hat Prese...
Red
Red Hat
Hybrid Cloud Console
All apps and services
OpenShift
Clusters
Overview
Releases
Downloads
Insights
Subscriptions
Cost Management
Support Cases
Cluster Manager Feedback
Red Hat Marketplace
Documentation
Name
OpenShift for x8
OpenShift for IB
OpenShift for Po
OpenShift for AR
CodeReady Cont
RHCOS manageme
Customize Red Hat Enter
Name

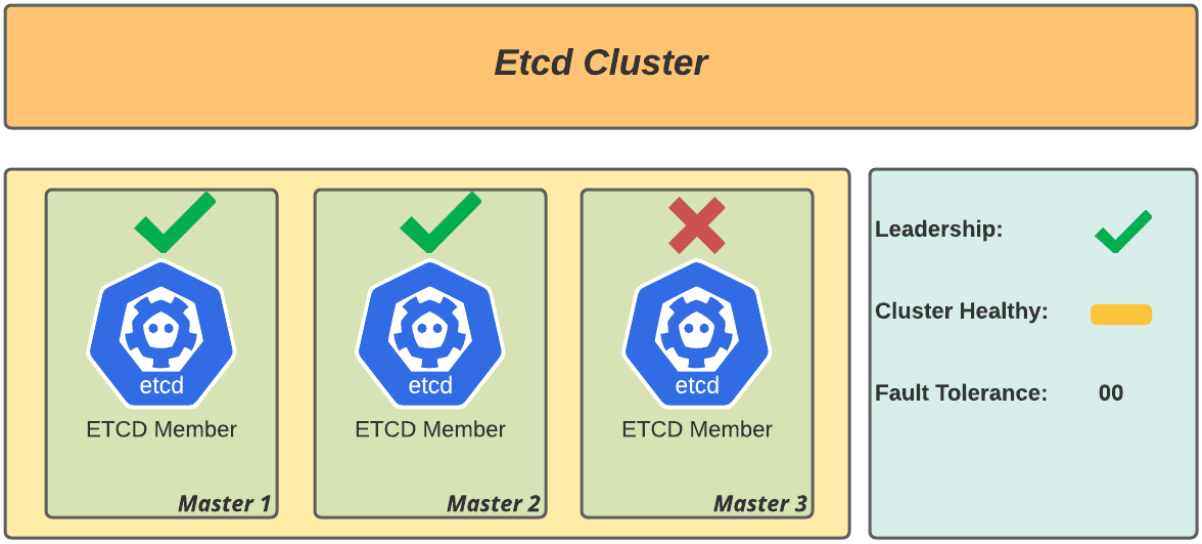
Tokens
Pull secret
Copy
Download

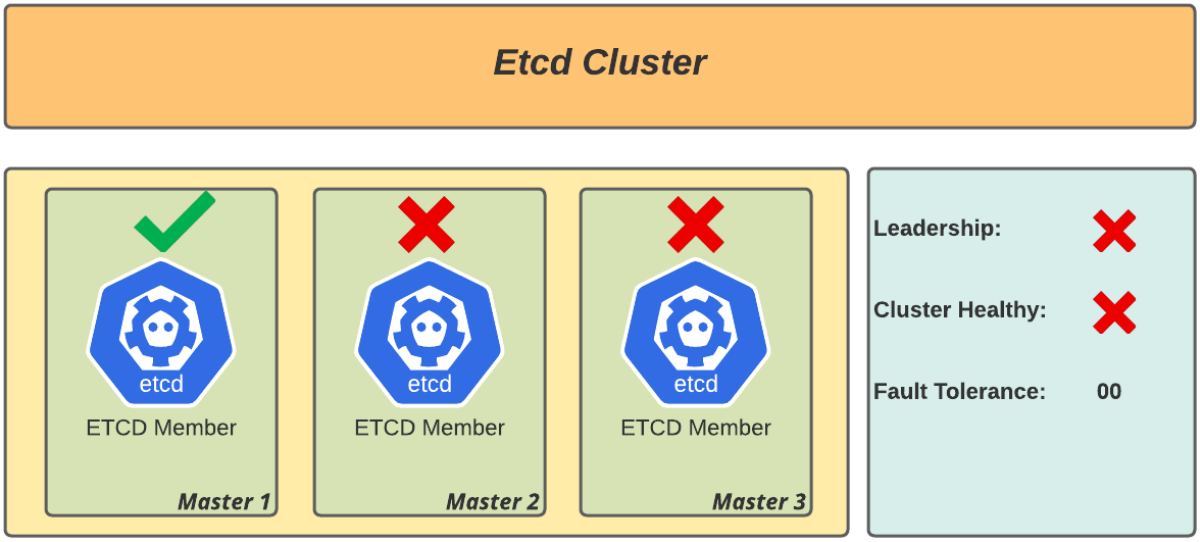

Log in to your account
Username *
kubeadmin
Password *
Log in
Red Hat
OpenShift Container Platform
Welcome to Red Hat OpenShift Container Platform

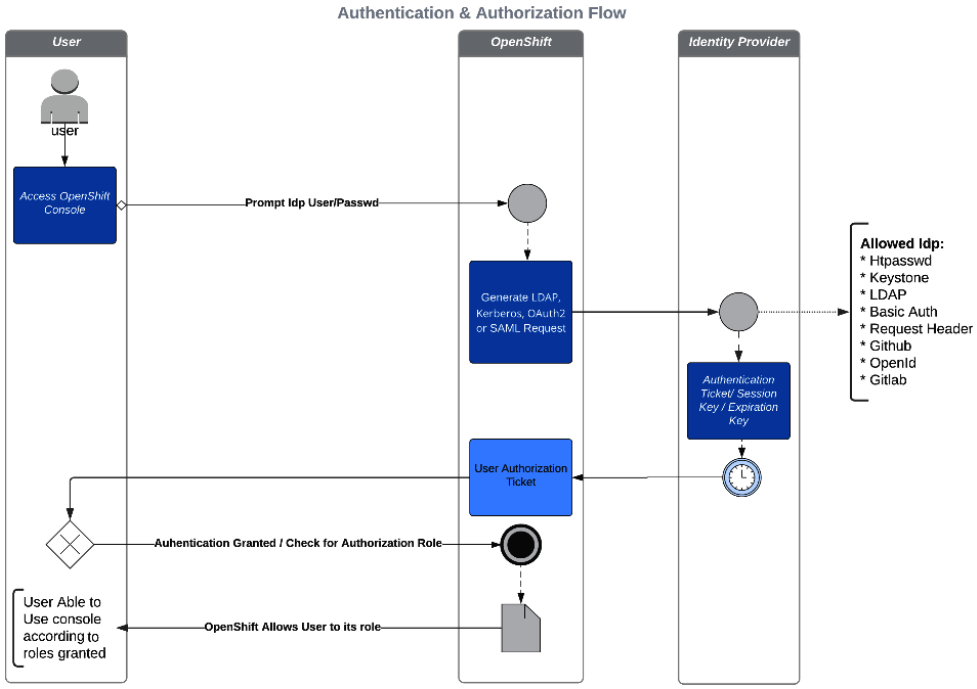

Red Hat
OpenShift
Container Platform
Administrator
Home
Overview
Projects
Search
API Explorer
Events
Operators
Workloads
Networking
Storage
Builds
Pipelines
Observe
Compute
Overview
Cluster
Getting started resources
Set up your cluster
Finish setting up your cluster with recommended configurations.
Configure alert receivers
View all steps in documentation
Build with guided documentation
Follow guided documentation to build applications and familiarize yourself with key features.
Monitor your sample application
Get started with Quarkus using a Helm Chart
View all quick starts
Details
View settings
Cluster API address
https://api.cluster-l4dbn.l4dbn.sandbox1405.opentlc.com:6443
Cluster ID
ced8269b-d6db-4498-bd69-968043b5abe3
OpenShift Cluster Manager
Provider
AWS
OpenShift version
4.9.11
Status
Cluster
Control Plane
Operators
Insights
2 issues
Dec 26, 2021, 3:07 PM
Alerts are not configured to be sent to a notification system, meaning that you may not be notified in a timely fashion when important failures occur. Check the OpenShift documentation to learn how to configure notifications with Alertmanager.

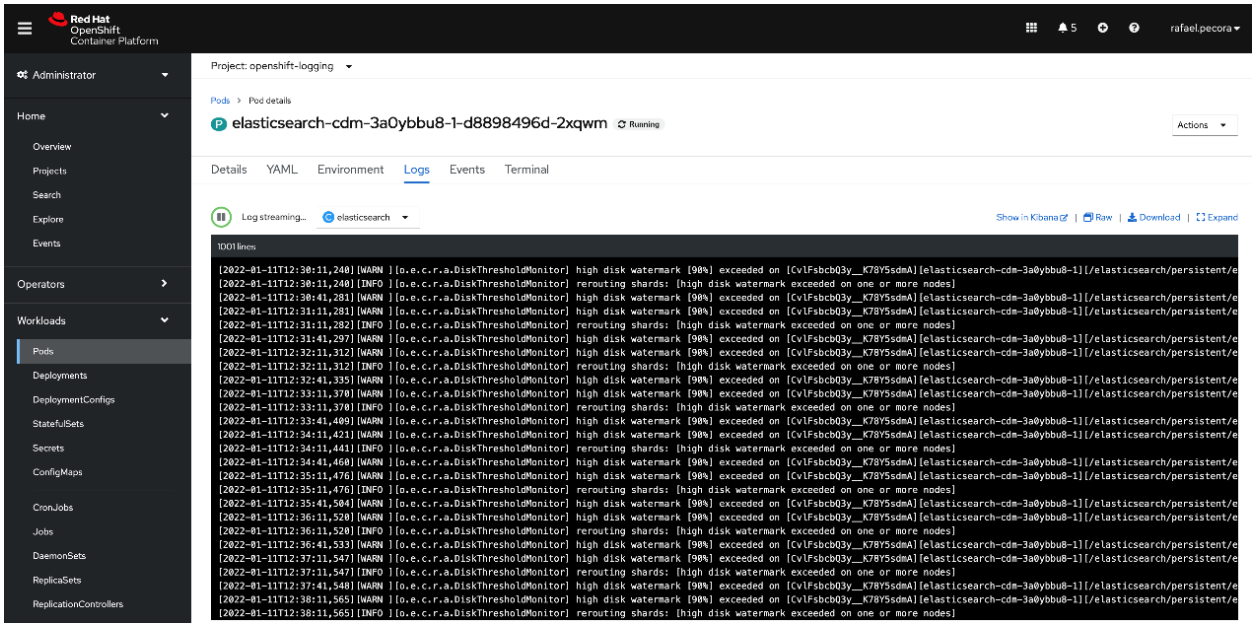
Chapter 6: OpenShift Troubleshooting, Performance, and Best Practices



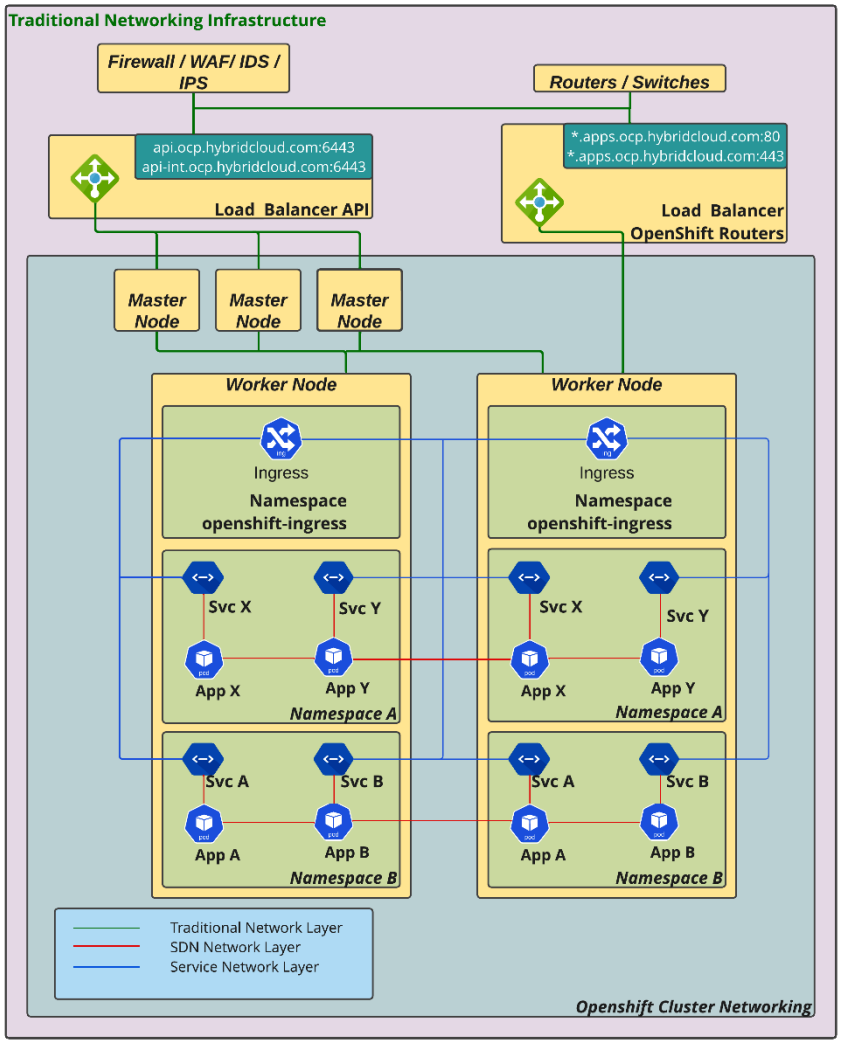


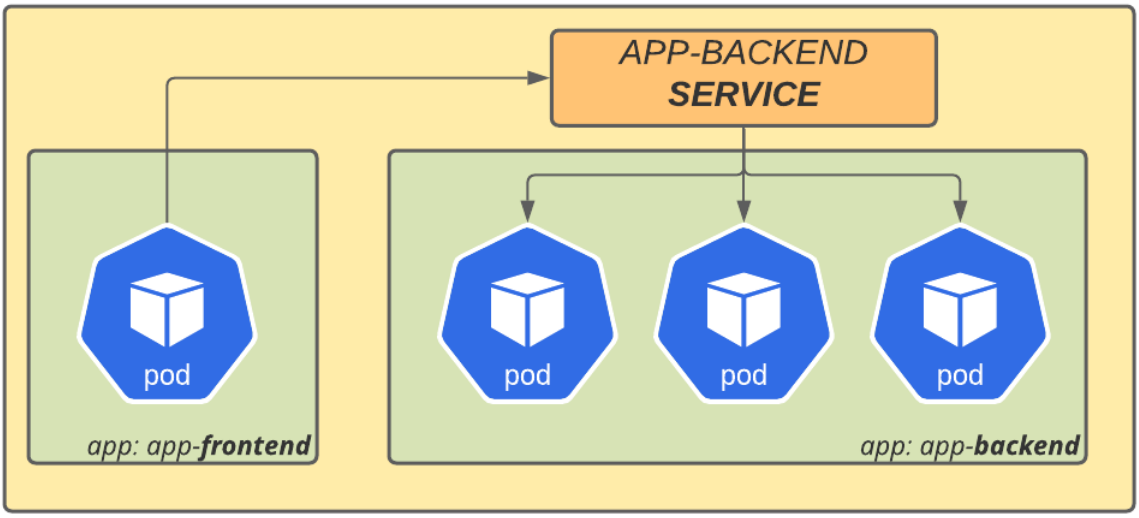

Etcd Cluster
etcd
ETCD Member
Master 1
etcd
ETCD Member
Master 2
etcd
ETCD Member
Master 3
Leadership:
Cluster Healthy:
Fault Tolerance:
00

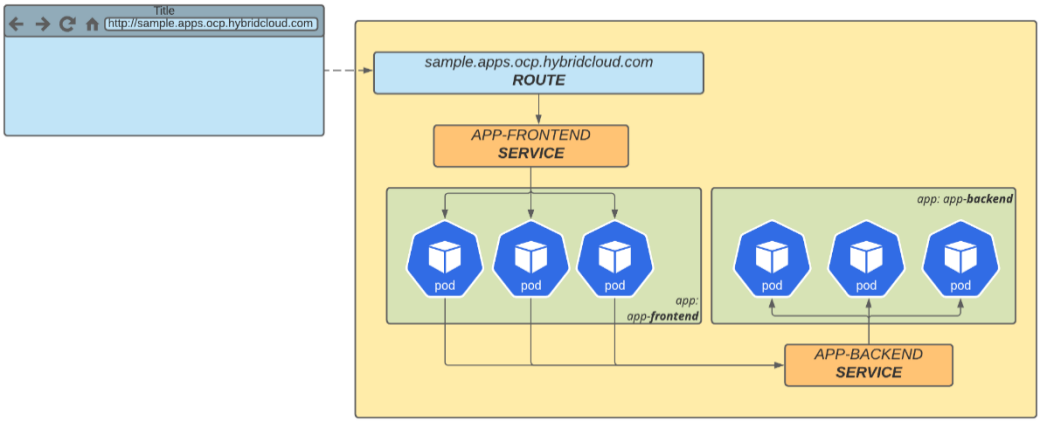

Authentication & Authorization Flow
User
OpenShift
Identity Provider
user
Access OpenShift Console
Prompt Idp User/Passwd
Generate LDAP, Kerberos, OAuth2 or SAML Request
Allowed Idp:
* Htpasswd
* Keystone
* LDAP
* Basic Auth
* Request Header
* Github
* OpenId
* Gitlab
Authentication Ticket/ Session Key / Expiration Key
User Authorization Ticket
Auhentication Granted / Check for Authorization Role
User Able to Use console according to roles granted
OpenShift Allows User to its role

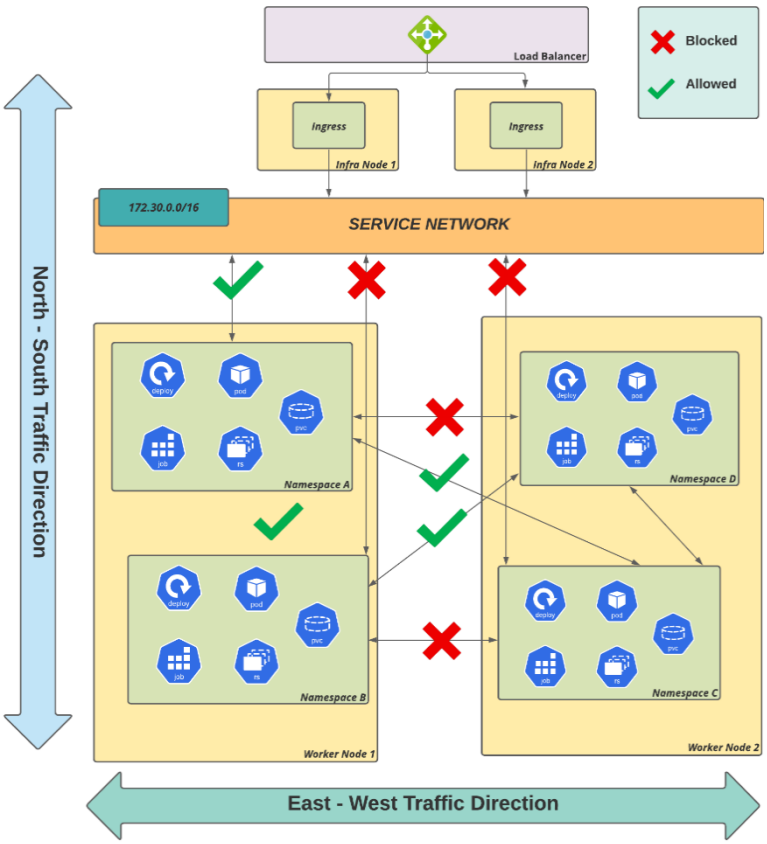

Red Hat
OpenShift
Container Platform
5
rafael.pecora
Administrator
Project: openshift-logging
Home
Overview
Projects
Search
Explore
Events
Operators
Workloads
Pods
Deployments
DeploymentConfigs
StatefulSets
Secrets
ConfigMaps
CronJobs
Jobs
DaemonSets
ReplicaSets
ReplicationControllers
Pods > Pod details
elasticsearch-cdm-3a0ybbu8-1-d8898496d-2xqwm
Running
Actions
Details
YAML
Environment
Logs
Events
Terminal
Log streaming...
elasticsearch
Show in Kibana
Raw
Download
Expand
1001 lines
[2022-01-11T12:30:11,240][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:30:11,240][INFO][o.e.c.r.a.DiskThresholdMonitor] rerouting shards: [high disk watermark exceeded on one or more nodes]
[2022-01-11T12:30:41,281][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:31:11,281][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:31:11,282][INFO][o.e.c.r.a.DiskThresholdMonitor] rerouting shards: [high disk watermark exceeded on one or more nodes]
[2022-01-11T12:31:41,297][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:32:11,312][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:32:11,312][INFO][o.e.c.r.a.DiskThresholdMonitor] rerouting shards: [high disk watermark exceeded on one or more nodes]
[2022-01-11T12:32:41,335][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:33:11,370][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:33:11,370][INFO][o.e.c.r.a.DiskThresholdMonitor] rerouting shards: [high disk watermark exceeded on one or more nodes]
[2022-01-11T12:33:41,409][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:34:11,421][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:34:11,441][INFO][o.e.c.r.a.DiskThresholdMonitor] rerouting shards: [high disk watermark exceeded on one or more nodes]
[2022-01-11T12:34:41,460][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:35:11,476][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:35:11,476][INFO][o.e.c.r.a.DiskThresholdMonitor] rerouting shards: [high disk watermark exceeded on one or more nodes]
[2022-01-11T12:35:41,504][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:36:11,520][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:36:11,520][INFO][o.e.c.r.a.DiskThresholdMonitor] rerouting shards: [high disk watermark exceeded on one or more nodes]
[2022-01-11T12:36:41,533][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:37:11,547][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:37:11,547][INFO][o.e.c.r.a.DiskThresholdMonitor] rerouting shards: [high disk watermark exceeded on one or more nodes]
[2022-01-11T12:37:41,548][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:38:11,565][WARN][o.e.c.r.a.DiskThresholdMonitor] high disk watermark [90%] exceeded on [CvlFsbcbQ3y__K78Y5sdmA][elasticsearch-cdm-3a0ybbu8-1][/elasticsearch/persistent/e
[2022-01-11T12:38:11,565][INFO][o.e.c.r.a.DiskThresholdMonitor] rerouting shards: [high disk watermark exceeded on one or more nodes]

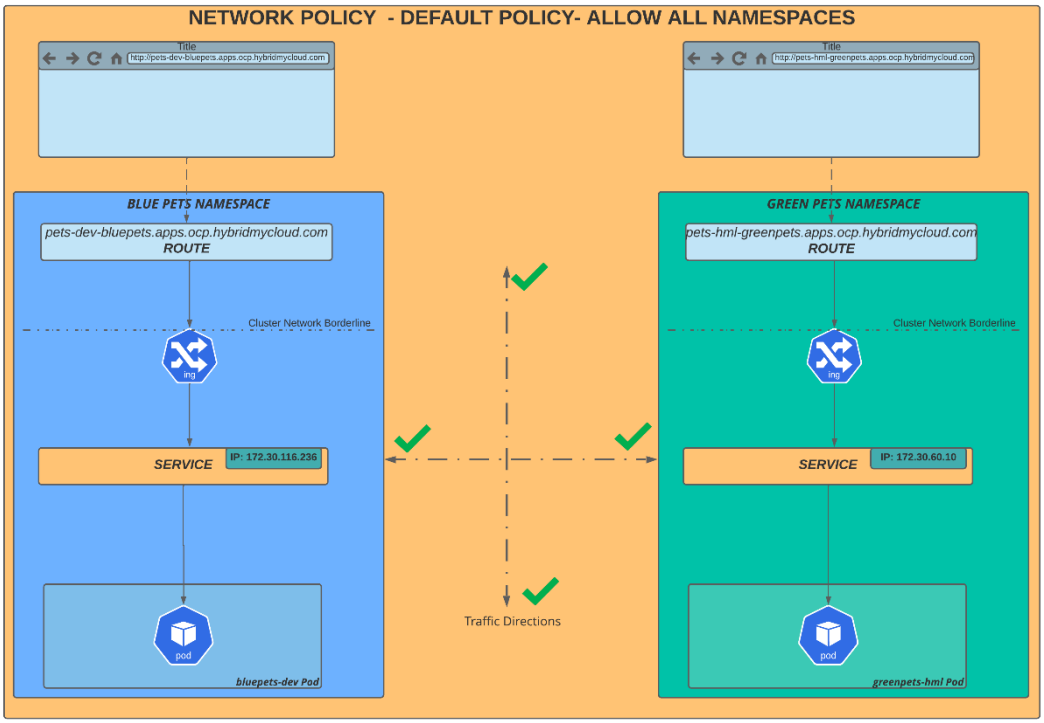
Chapter 7: OpenShift Network



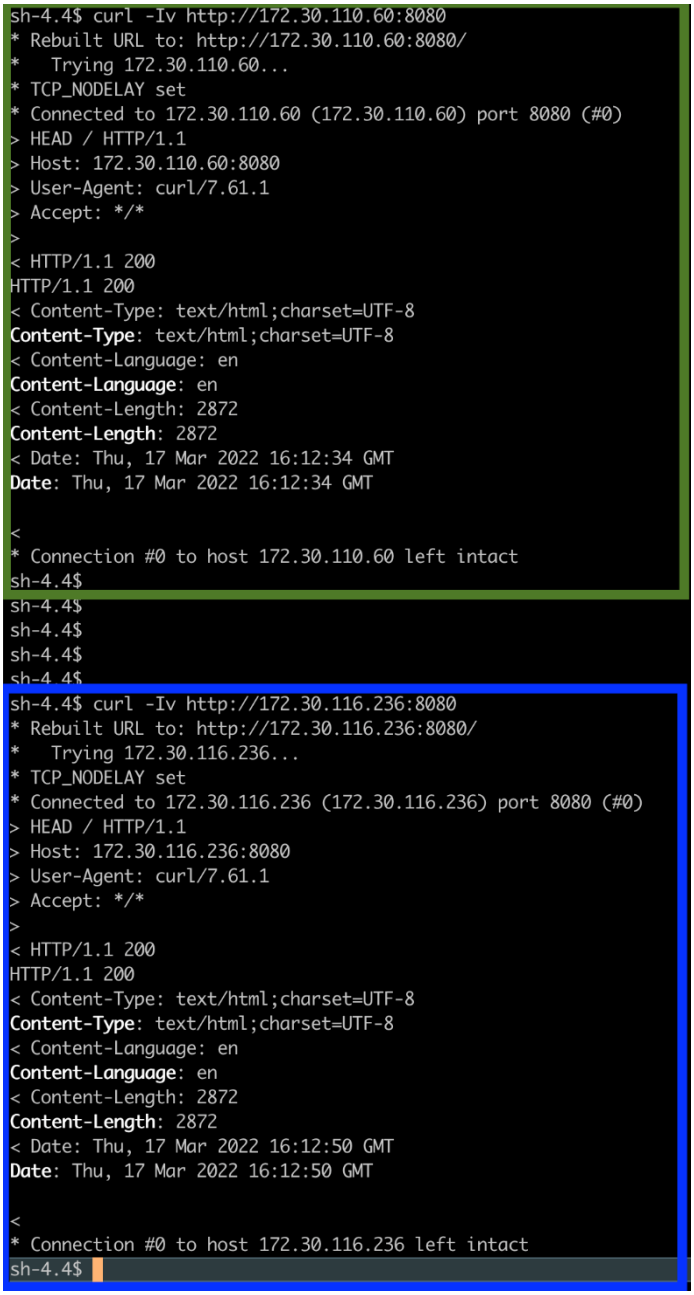


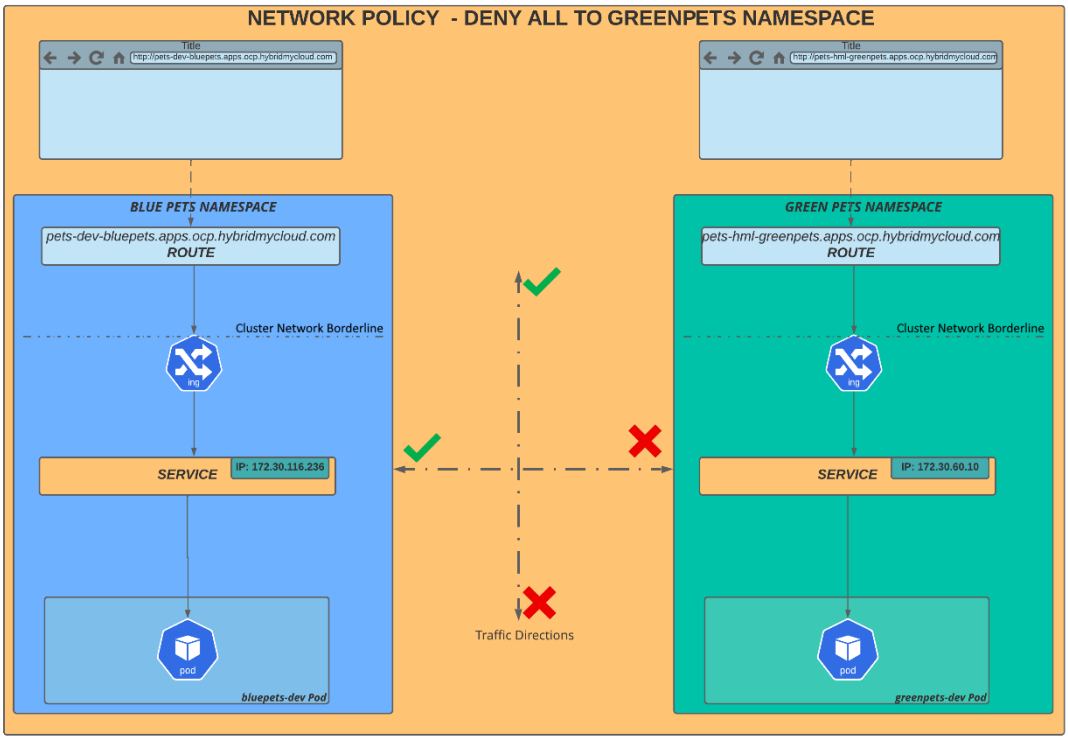

Title
http://sample.apps.ocp.hybridcloud.com
sample.apps.ocp.hybridcloud.com
ROUTE
APP-FRONTEND
SERVICE
pod
pod
pod
app:
app-frontend
app: app-backend
pod
pod
pod
APP-BACKEND
SERVICE


Load Balancer
Blocked
Allowed
Ingress
Infra Node 1
Ingress
Infra Node 2
172.30.0.0/16
SERVICE NETWORK
North - South Traffic Direction
Namespace A
Namespace B
Worker Node 1
Namespace D
Namespace C
Worker Node 2
East - West Traffic Direction



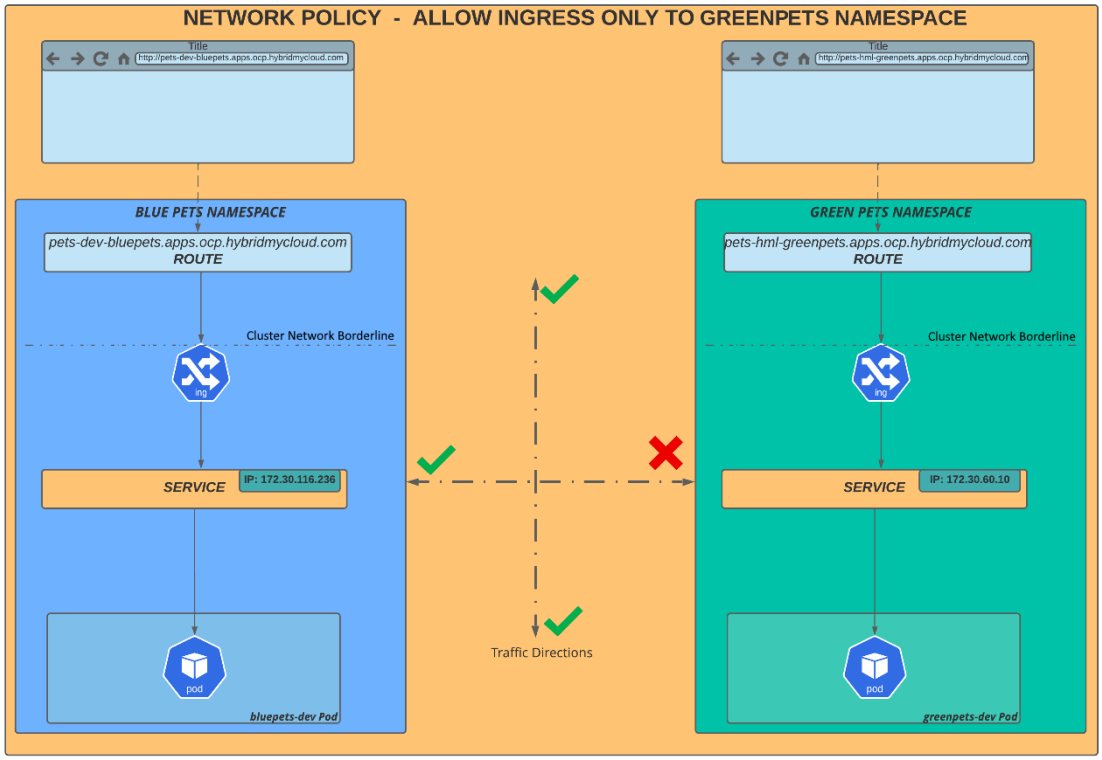

```
% oc get svc -n bluepets
NAME       TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)                      AGE
pets-dev   ClusterIP   172.30.116.236   <none>        8080/TCP,8443/TCP,8778/TCP   16m
                                                                                  /pecs-cluster ~ (greenpets) - 0:25:21]
% oc get svc -n greenpets
NAME       TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)                      AGE
pets-hml   ClusterIP   172.30.110.60   <none>        8080/TCP,8443/TCP,8778/TCP   12m
                                                                                  /pecs-cluster ~ (greenpets) - 0:26:06]
% oc get networkpolicy -n bluepets
No resources found in bluepets namespace.
                                                                                  pecs-cluster ~ (greenpets) - 0:26:34]
% oc get networkpolicy -n greenpets
No resources found in greenpets namespace.
```


sh-4.4$ curl -Iv http://172.30.110.60:8080
* Rebuilt URL to: http://172.30.110.60:8080/
*   Trying 172.30.110.60...
* TCP_NODELAY set
* Connected to 172.30.110.60 (172.30.110.60) port 8080 (#0)
> HEAD / HTTP/1.1
> Host: 172.30.110.60:8080
> User-Agent: curl/7.61.1
> Accept: */*
>
< HTTP/1.1 200
HTTP/1.1 200
< Content-Type: text/html;charset=UTF-8
Content-Type: text/html;charset=UTF-8
< Content-Language: en
Content-Language: en
< Content-Length: 2872
Content-Length: 2872
< Date: Thu, 17 Mar 2022 16:12:34 GMT
Date: Thu, 17 Mar 2022 16:12:34 GMT
<
* Connection #0 to host 172.30.110.60 left intact
sh-4.4$
sh-4.4$
sh-4.4$
sh-4.4$
sh-4.4$ curl -Iv http://172.30.116.236:8080
* Rebuilt URL to: http://172.30.116.236:8080/
*   Trying 172.30.116.236...
* TCP_NODELAY set
* Connected to 172.30.116.236 (172.30.116.236) port 8080 (#0)
> HEAD / HTTP/1.1
> Host: 172.30.116.236:8080
> User-Agent: curl/7.61.1
> Accept: */*
>
< HTTP/1.1 200
HTTP/1.1 200
< Content-Type: text/html;charset=UTF-8
Content-Type: text/html;charset=UTF-8
< Content-Language: en
Content-Language: en
< Content-Length: 2872
Content-Length: 2872
< Date: Thu, 17 Mar 2022 16:12:50 GMT
Date: Thu, 17 Mar 2022 16:12:50 GMT
<
* Connection #0 to host 172.30.116.236 left intact
sh-4.4$




```
sh-4.4$ curl -Iv http://pets-hml-greenpets.apps.ozb125e9.eastus.aroapp.io/
*   Trying 104.45.195.215...
* TCP_NODELAY set
* Connected to pets-hml-greenpets.apps.ozb125e9.eastus.aroapp.io (104.45.195.215) port 80 (#0)
> HEAD / HTTP/1.1
> Host: pets-hml-greenpets.apps.ozb125e9.eastus.aroapp.io
> User-Agent: curl/7.61.1
> Accept: */*
>
* HTTP 1.0, assume close after body
< HTTP/1.0 503 Service Unavailable
HTTP/1.0 503 Service Unavailable
< pragma: no-cache
pragma: no-cache
< cache-control: private, max-age=0, no-cache, no-store
cache-control: private, max-age=0, no-cache, no-store
< content-type: text/html
content-type: text/html

<
* Closing connection 0
sh-4.4$
```

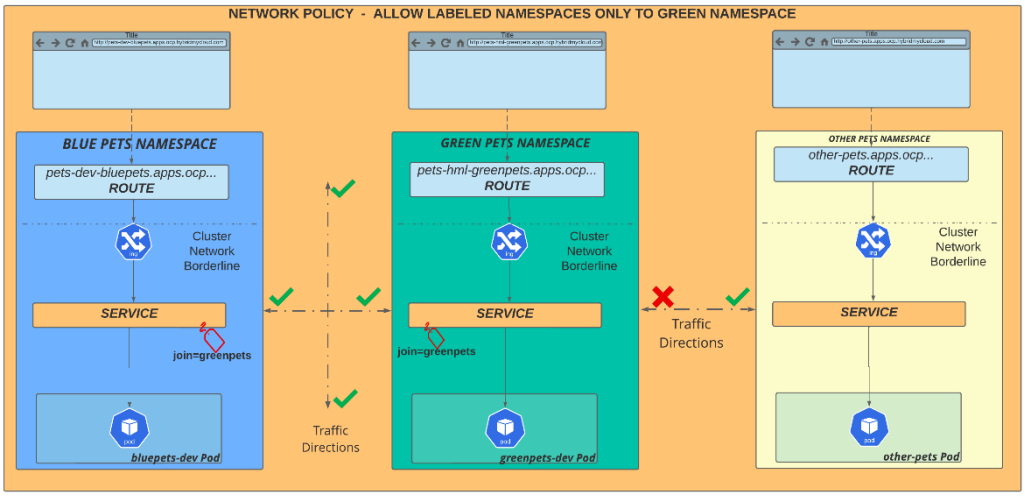
From Pod to Route in same namespace –> Connection Refused


NETWORK POLICY - ALLOW INGRESS ONLY TO GREENPETS NAMESPACE
Title
http://pets-dev-bluepets.apps.ocp.hybridmycloud.com
Title
http://pets-hml-greenpets.apps.ocp.hybridmycloud.com
BLUE PETS NAMESPACE
pets-dev-bluepets.apps.ocp.hybridmycloud.com
ROUTE
Cluster Network Borderline
ing
SERVICE
IP: 172.30.116.236
pod
bluepets-dev Pod
Traffic Directions
GREEN PETS NAMESPACE
pets-hml-greenpets.apps.ocp.hybridmycloud.com
ROUTE
Cluster Network Borderline
ing
SERVICE
IP: 172.30.60.10
pod
greenpets-dev Pod

```
% oc -n bluepets rsh pets-dev-7846d7d75-sdkc8
sh-4.4$
sh-4.4$
sh-4.4$ curl -Iv http://172.30.110.60:8080
* Rebuilt URL to: http://172.30.110.60:8080/
*   Trying 172.30.110.60...
* TCP_NODELAY set
* connect to 172.30.110.60 port 8080 failed: Connection timed out
* Failed to connect to 172.30.110.60 port 8080: Connection timed out
* Closing connection 0
curl: (7) Failed to connect to 172.30.110.60 port 8080: Connection timed out
sh-4.4$ curl -Iv http://pets-hml-greenpets.apps.[redacted]
*   Trying 104.45.195.215...
* TCP_NODELAY set
* Connected to pets-hml-greenpets.apps.[redacted] (104.45.195.215) port 80 (#0)
> HEAD / HTTP/1.1
> Host: pets-hml-greenpets.apps.[redacted]
> User-Agent: curl/7.61.1
> Accept: */*
>
< HTTP/1.1 200
HTTP/1.1 200
< content-type: text/html;charset=UTF-8
content-type: text/html;charset=UTF-8
< content-language: en
content-language: en
< content-length: 2872
content-length: 2872
< date: Thu, 17 Mar 2022 19:31:04 GMT
date: Thu, 17 Mar 2022 19:31:04 GMT
< set-cookie: 78fbf668d708c59275ac7bedf6c54540=d77151b1491f732de74affaec80db50d; path=/; HttpOnly
set-cookie: 78fbf668d708c59275ac7bedf6c54540=d77151b1491f732de74affaec80db50d; path=/; HttpOnly
< cache-control: private
cache-control: private

<
* Connection #0 to host pets-hml-greenpets.apps.[redacted] left intact
sh-4.4$
```

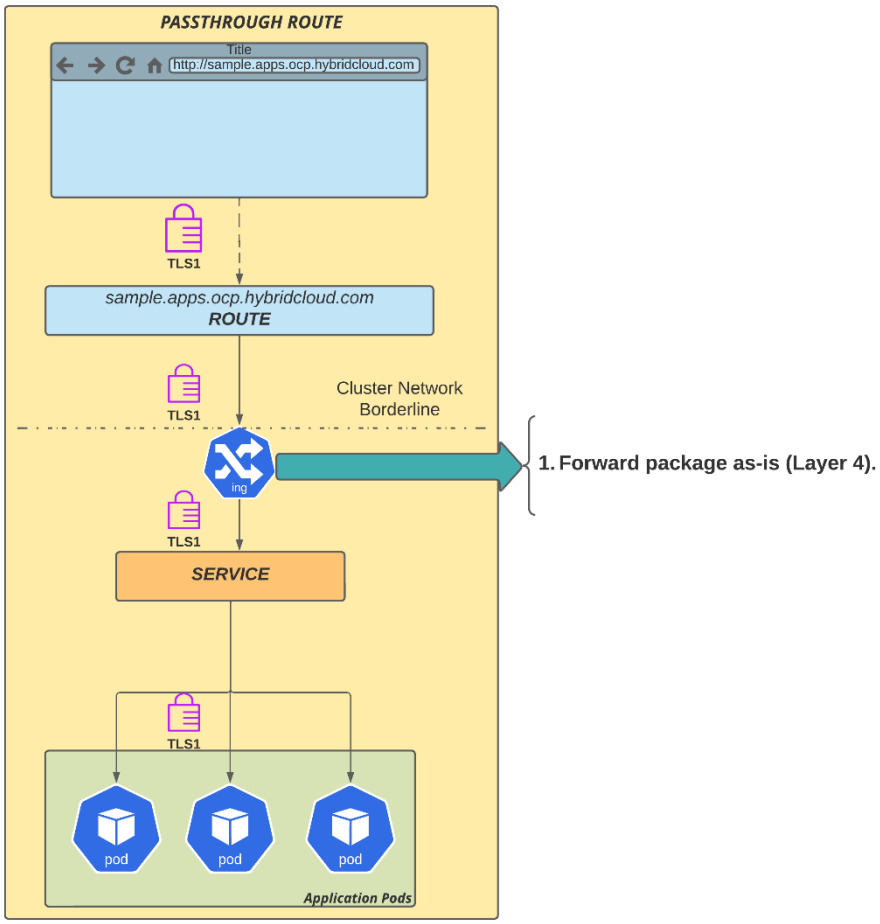
1

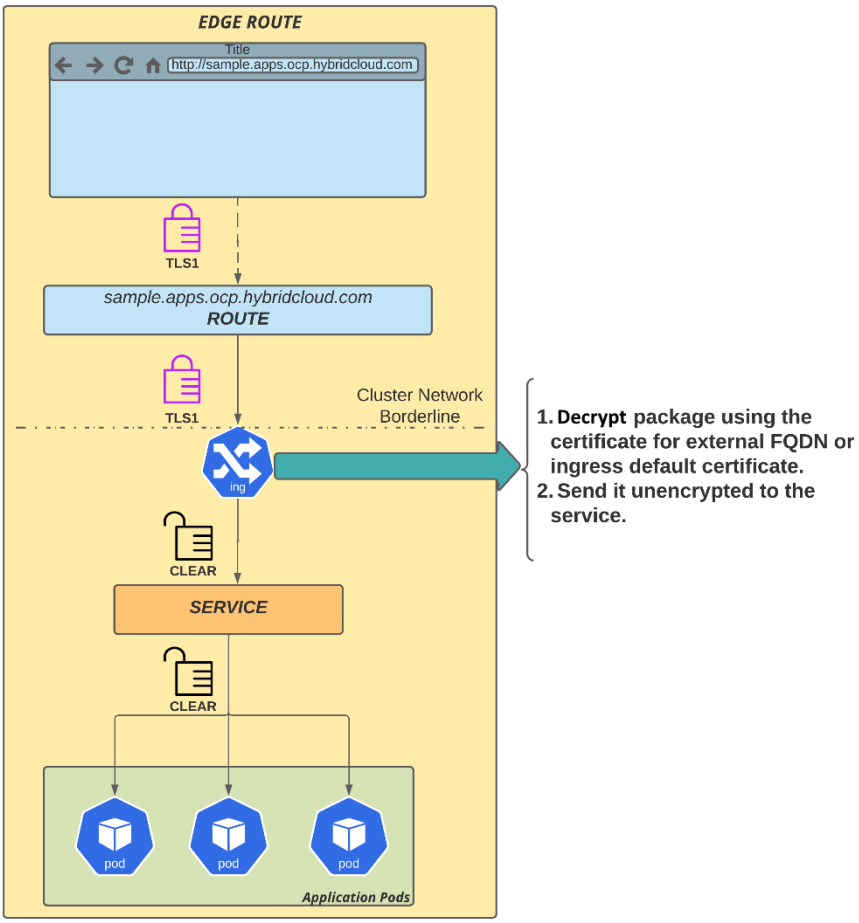
2

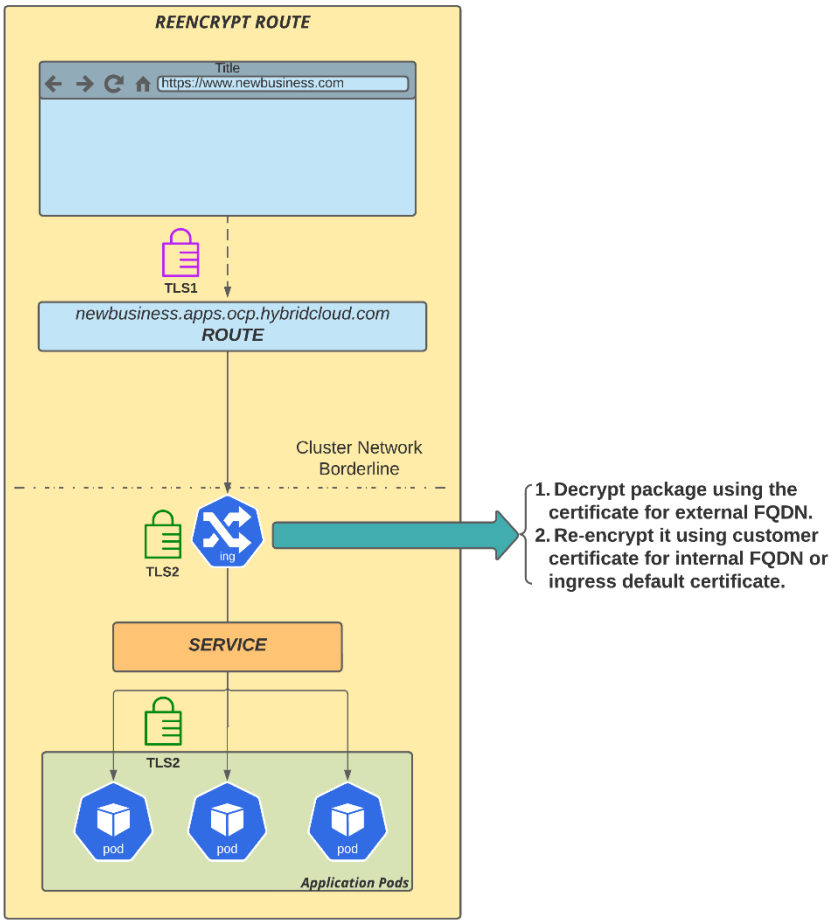


```
<
* Connection #0 to host 172.30.116.236 left intact
sh-4.4$
sh-4.4$
sh-4.4$ curl -Iv http://172.30.110.60:8080
* Rebuilt URL to: http://172.30.110.60:8080/
*   Trying 172.30.110.60...
* TCP_NODELAY set
* Connected to 172.30.110.60 (172.30.110.60) port 8080 (#0)
> HEAD / HTTP/1.1
> Host: 172.30.110.60:8080
> User-Agent: curl/7.61.1
> Accept: */*
>
< HTTP/1.1 200
HTTP/1.1 200
< Content-Type: text/html;charset=UTF-8
Content-Type: text/html;charset=UTF-8
< Content-Language: en
Content-Language: en
< Content-Length: 2872
Content-Length: 2872
< Date: Thu, 17 Mar 2022 22:27:12 GMT
Date: Thu, 17 Mar 2022 22:27:12 GMT

<
```

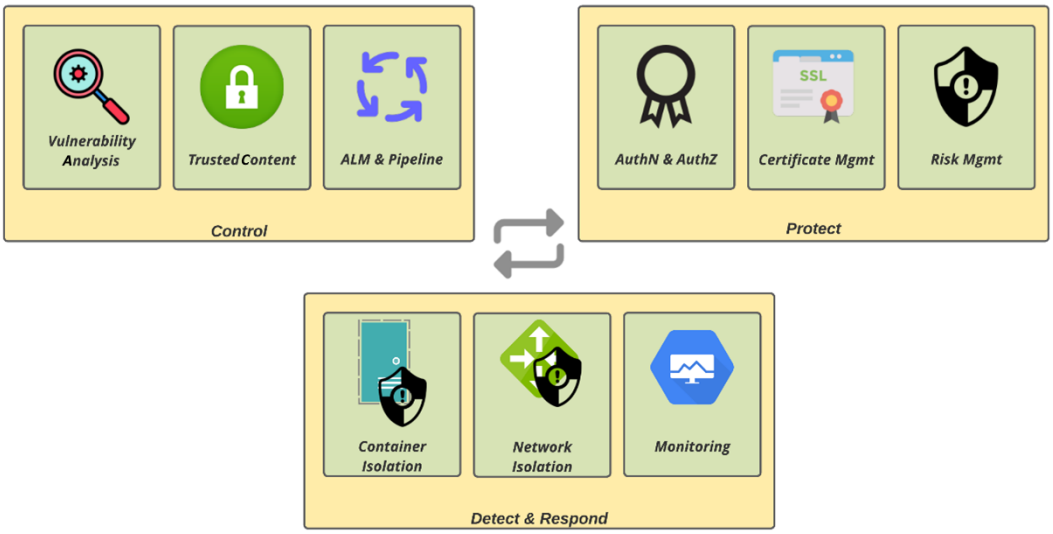
```
sh-4.4$ curl -Iv http://172.30.110.60:8080
* Rebuilt URL to: http://172.30.110.60:8080/
*   Trying 172.30.110.60...
* TCP_NODELAY set
* connect to 172.30.110.60 port 8080 failed: Connection timed out
* Failed to connect to 172.30.110.60 port 8080: Connection timed out
* Closing connection 0
curl: (7) Failed to connect to 172.30.110.60 port 8080: Connection timed out
sh-4.4$
```

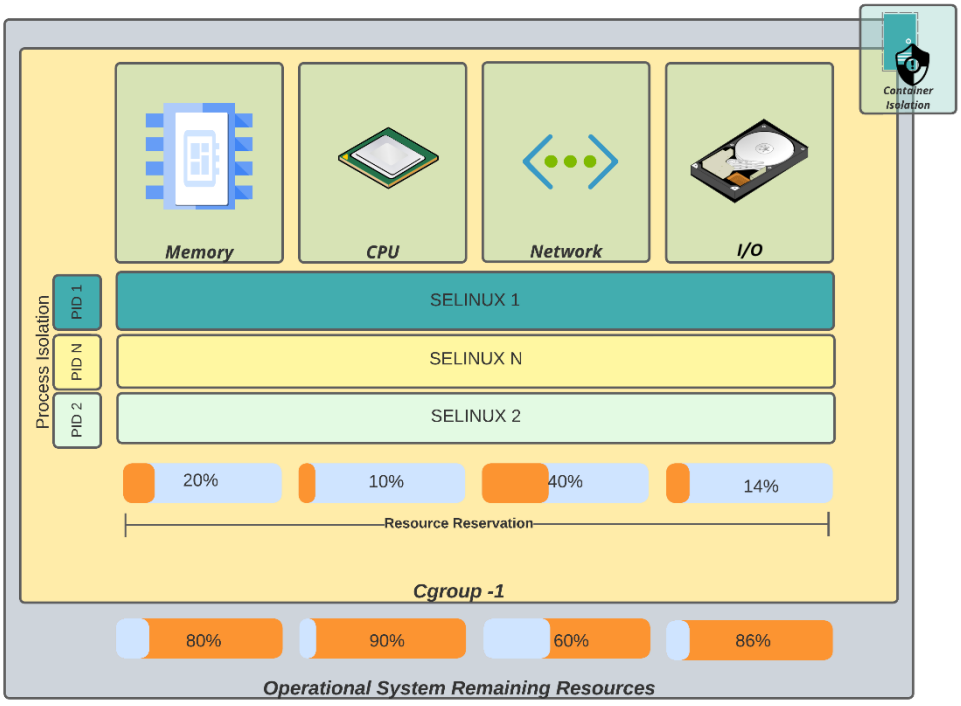

PASSTHROUGH ROUTE
Title
http://sample.apps.ocp.hybridcloud.com
TLS1
sample.apps.ocp.hybridcloud.com
ROUTE
TLS1
Cluster Network
Borderline
ing
1. Forward package as-is (Layer 4).
TLS1
SERVICE
TLS1
pod
pod
pod
Application Pods


EDGE ROUTE
Title
http://sample.apps.ocp.hybridcloud.com
TLS1
sample.apps.ocp.hybridcloud.com
ROUTE
TLS1
Cluster Network
Borderline
ing
CLEAR
SERVICE
CLEAR
pod
pod
pod
Application Pods
1. Decrypt package using the certificate for external FQDN or ingress default certificate.
2. Send it unencrypted to the service.


REENCRYPT ROUTE
Title
https://www.newbusiness.com
TLS1
newbusiness.apps.ocp.hybridcloud.com
ROUTE
Cluster Network
Borderline
ing
TLS2
1. Decrypt package using the certificate for external FQDN.
2. Re-encrypt it using customer certificate for internal FQDN or ingress default certificate.
SERVICE
TLS2
pod
pod
pod
Application Pods

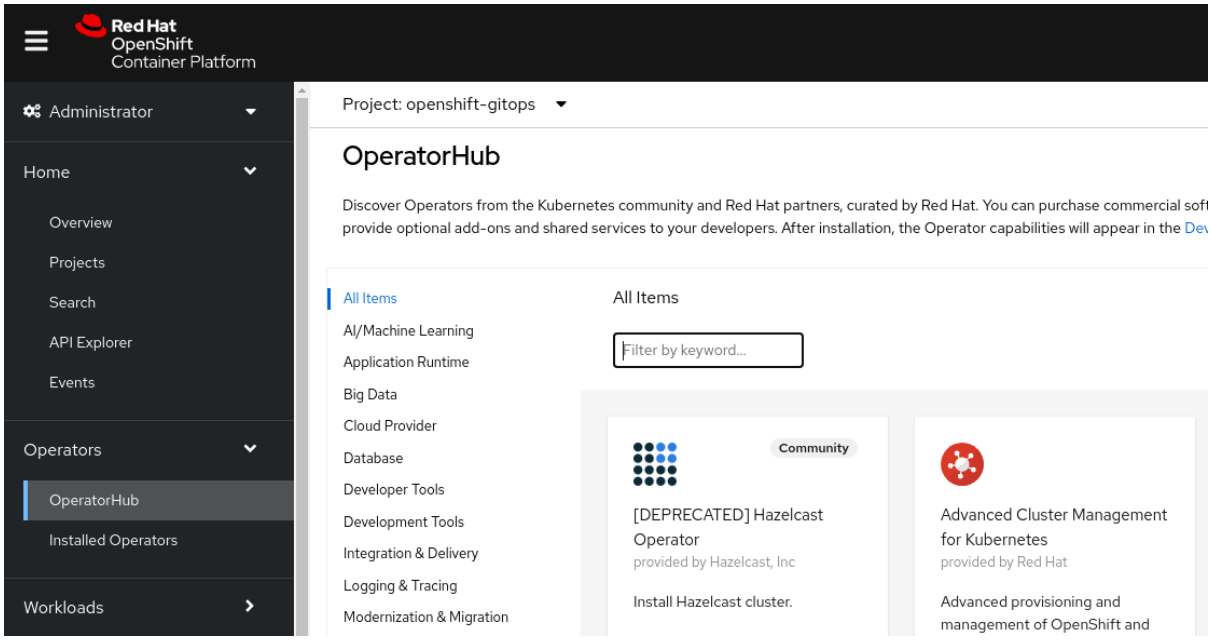
Chapter 8: OpenShift Security

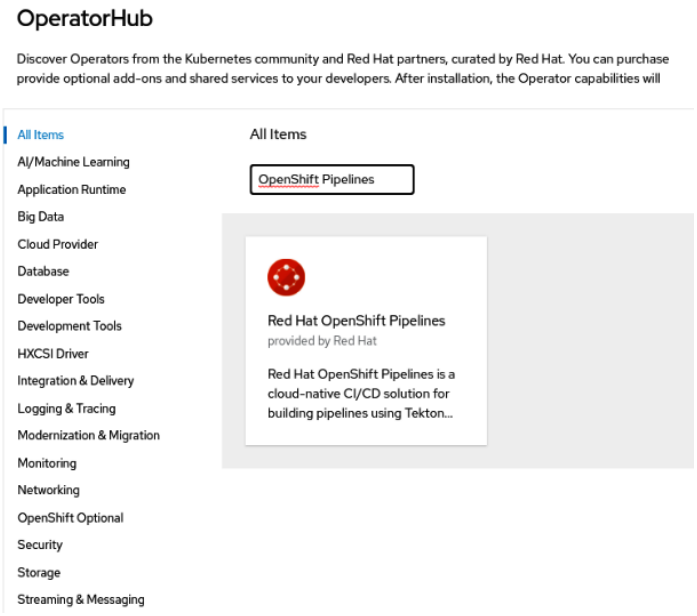




Chapter 9: OpenShift Pipelines – Tekton

```
INFO Operator openshift-controller-manager is progressing
INFO 2 operators are progressing: kube-apiserver, openshift-controller-manager
INFO All operators are available. Ensuring stability...
INFO Operators are stable (2/3)...
INFO Operators are stable (3/3)...
INFO Adding crc-admin and crc-developer contexts to kubeconfig...
Started the OpenShift cluster.

The server is accessible via web console at:
  https://console-openshift-console.apps-crc.testing

Log in as administrator:
  Username: kubeadmin
  Password: wdTe2-vKuFw-tBq6F-T6dro

Log in as user:
  Username: developer
  Password: developer

Use the 'oc' command line interface:
  $ eval $(crc oc-env)
  $ oc login -u developer https://api.crc.testing:6443
```




OperatorHub
Discover Operators from the Kubernetes community and Red Hat partners, curated by Red Hat. You can purchase
provide optional add-ons and shared services to your developers. After installation, the Operator capabilities will
All Items
AI/Machine Learning
Application Runtime
Big Data
Cloud Provider
Database
Developer Tools
Development Tools
HXCSI Driver
Integration & Delivery
Logging & Tracing
Modernization & Migration
Monitoring
Networking
OpenShift Optional
Security
Storage
Streaming & Messaging
All Items
OpenShift Pipelines
Red Hat OpenShift Pipelines
provided by Red Hat
Red Hat OpenShift Pipelines is a
cloud-native CI/CD solution for
building pipelines using Tekton...

Red Hat OpenShift Pipelines

1.5.2 provided by Red Hat

Install

Latest version

1.5.2

Capability level

- Basic Install
- Seamless Upgrades
- Full Lifecycle
- Deep Insights
- Auto Pilot

Source

Red Hat

Provider

Red Hat

Infrastructure features

Disconnected
Proxy-aware

Repository

https://github.com/openshift/tektoncd-operator

Container image

registry.redhat.io/openshif

Red Hat OpenShift Pipelines is a cloud-native continuous integration and delivery (CI/CD) solution for building pipelines using Tekton. Tekton is a flexible Kubernetes-native open-source CI/CD framework, which enables automating deployments across multiple platforms (Kubernetes, serverless, VMs, etc) by abstracting away the underlying details.

Features

- Standard CI/CD pipelines definition
- Build images with Kubernetes tools such as S2I, Buildah, Buildpacks, Kaniko, etc
- Deploy applications to multiple platforms such as Kubernetes, serverless and VMs
- Easy to extend and integrate with existing tools
- Scale pipelines on-demand
- Portable across any Kubernetes platform
- Designed for microservices and decentralized team
- Integrated with OpenShift Developer Console

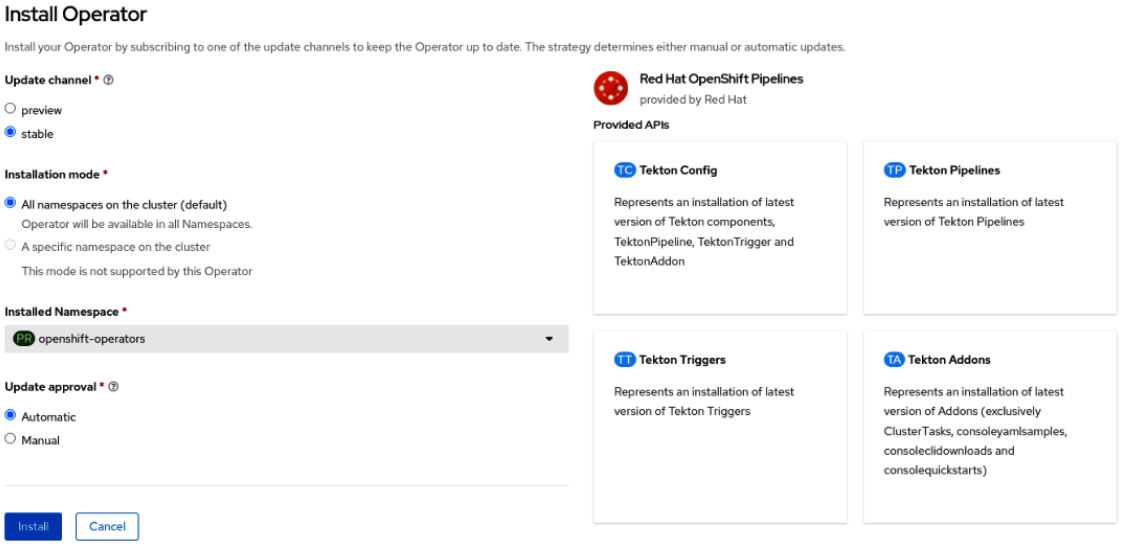
Installation

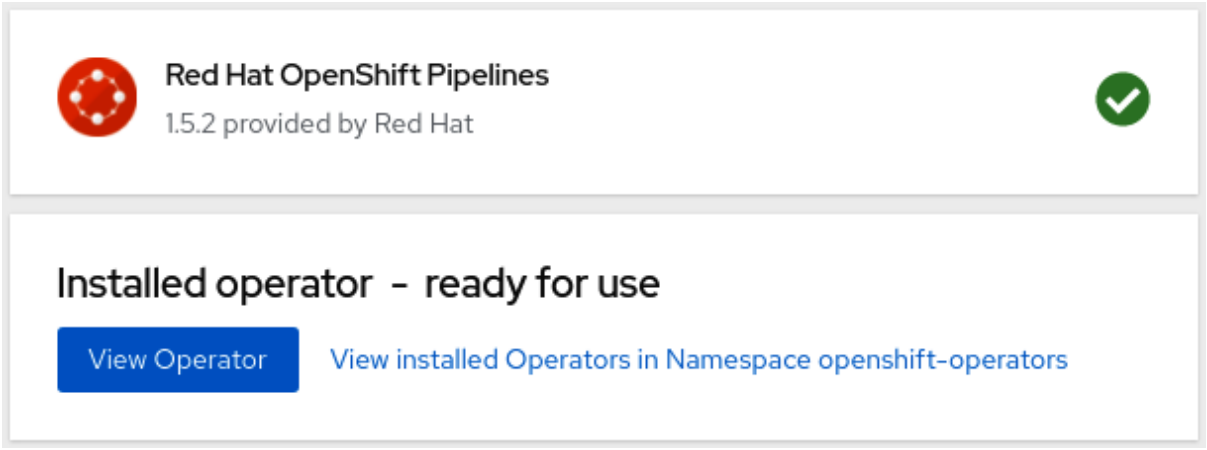
Red Hat OpenShift Pipelines Operator gets installed into a single namespace (openshift-operators) which would then install *Red Hat OpenShift Pipelines* into the openshift-pipelines namespace. *Red Hat OpenShift Pipelines* is however cluster-wide and can run pipelines created in any namespace.

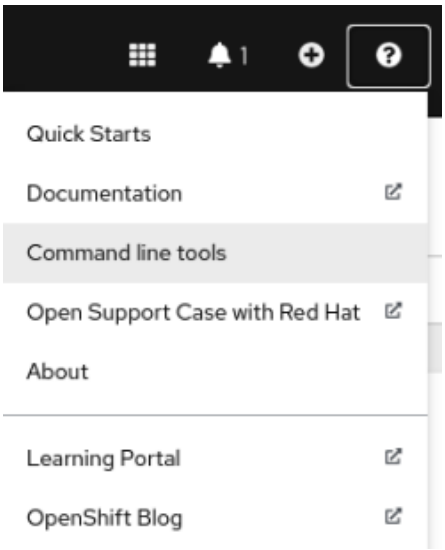
Components

- Tekton Pipelines: v0.24.3
- Tekton Triggers: v0.14.2
- ClusterTasks based on Tekton Catalog 0.24

Getting Started



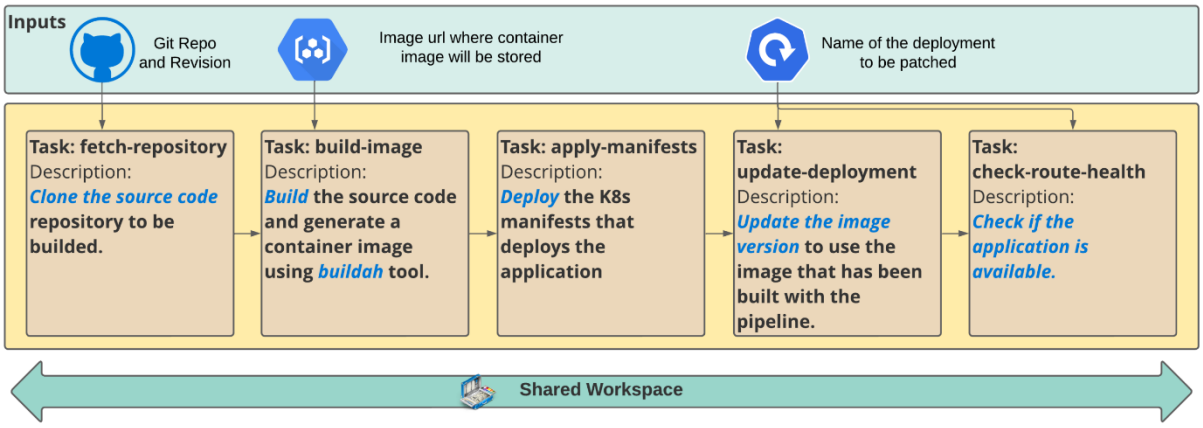


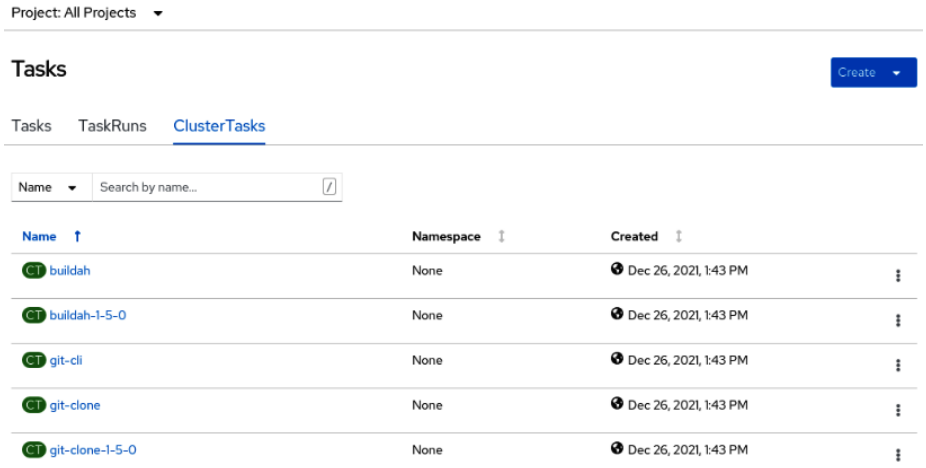


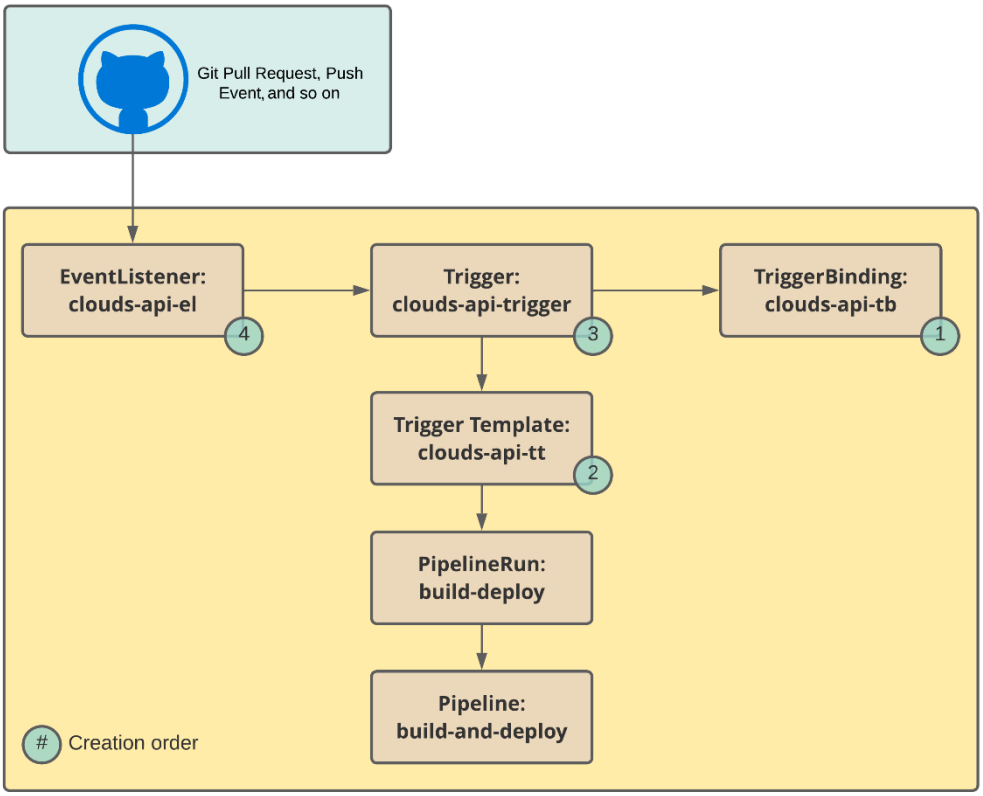
tkn - OpenShift Pipeline Command Line Interface (CLI)

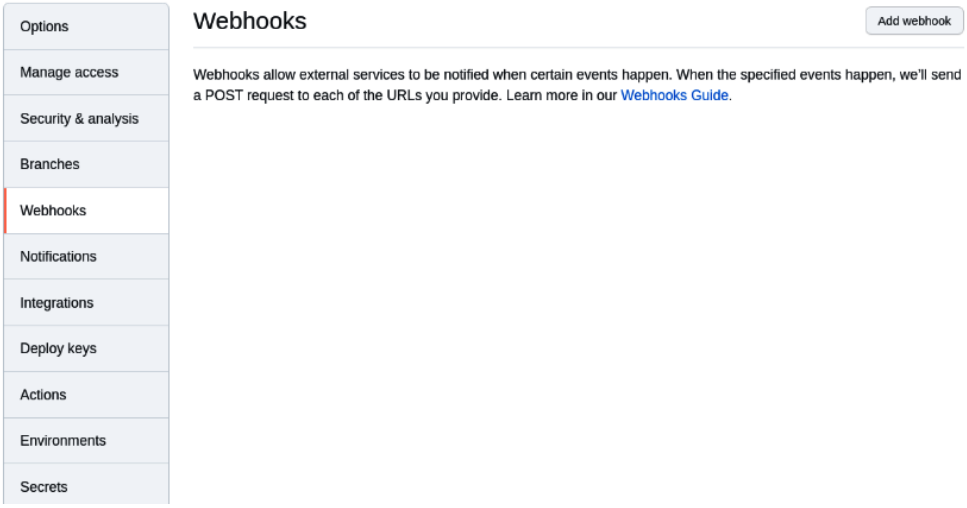
The OpenShift Pipeline client `tkn` is a CLI tool that allows you to manage OpenShift Pipeline resources.

- Download tkn for Linux
- Download tkn for Mac
- Download tkn for Windows
- Download tkn for IBM Power
- Download tkn for IBM Z


Inputs
Git Repo and Revision
Image url where container image will be stored
Name of the deployment to be patched
Task: fetch-repository
Description:
Clone the source code repository to be builded.
Task: build-image
Description:
Build the source code and generate a container image using buildah tool.
Task: apply-manifests
Description:
Deploy the K8s manifests that deploys the application
Task: update-deployment
Description:
Update the image version to use the image that has been built with the pipeline.
Task: check-route-health
Description:
Check if the application is available.
Shared Workspace


Project: All Projects
Tasks
Create
Tasks
TaskRuns
ClusterTasks
Name
Search by name...
Name
Namespace
Created
buildah
None
Dec 26, 2021, 1:43 PM
buildah-1-5-0
None
Dec 26, 2021, 1:43 PM
git-cli
None
Dec 26, 2021, 1:43 PM
git-clone
None
Dec 26, 2021, 1:43 PM
git-clone-1-5-0
None
Dec 26, 2021, 1:43 PM


Git Pull Request, Push Event, and so on
EventListener: clouds-api-el
4
Trigger: clouds-api-trigger
3
TriggerBinding: clouds-api-tb
1
Trigger Template: clouds-api-tt
2
PipelineRun: build-deploy
Pipeline: build-and-deploy
Creation order


Options
Manage access
Security & analysis
Branches
Webhooks
Notifications
Integrations
Deploy keys
Actions
Environments
Secrets
Webhooks
Add webhook
Webhooks allow external services to be notified when certain events happen. When the specified events happen, we'll send a POST request to each of the URLs you provide. Learn more in our Webhooks Guide.

Webhooks / Add webhook

We'll send a `POST` request to the URL below with details of any subscribed events. You can also specify which data format you'd like to receive (JSON, `x-www-form-urlencoded`, *etc*). More information can be found in our developer documentation.

Payload URL *

http://el-clouds-api-el-pipelines-sample.apps.cluster-zzkwx.zzkwx.s

Content type

application/json

Secret

tekton

Which events would you like to trigger this webhook?

- (•) Just the `push` event.
- ( ) Send me **everything**.
- ( ) Let me select individual events.

[x] **Active**
We will deliver event details when this hook is triggered.

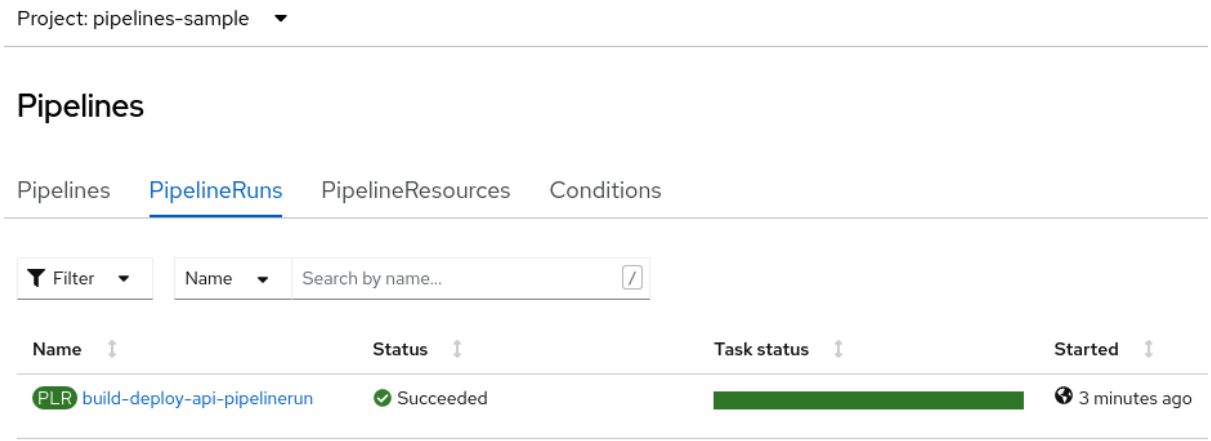
Add webhook

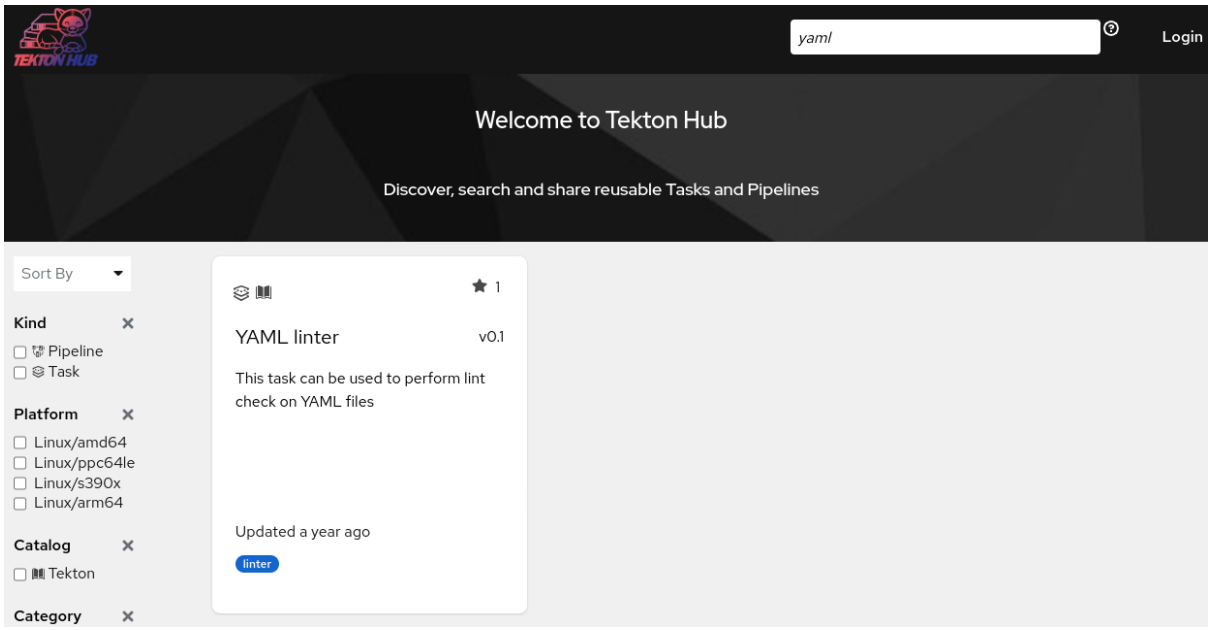
Webhooks

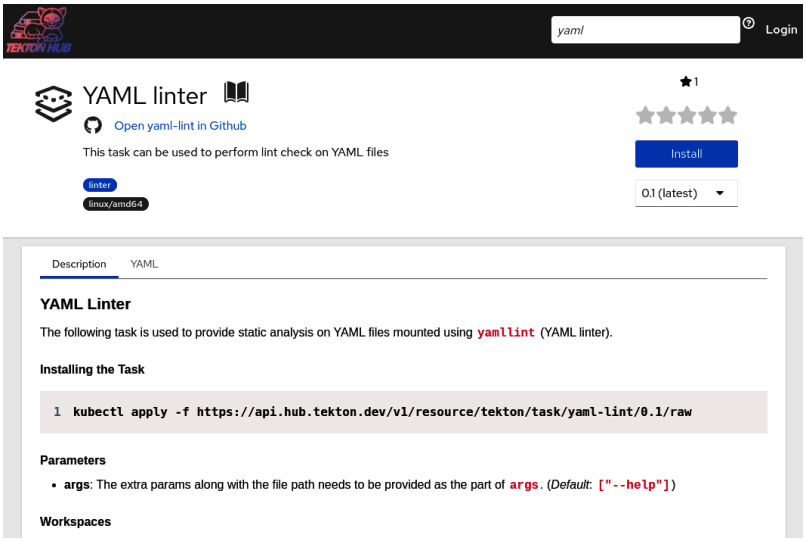
Add webhook

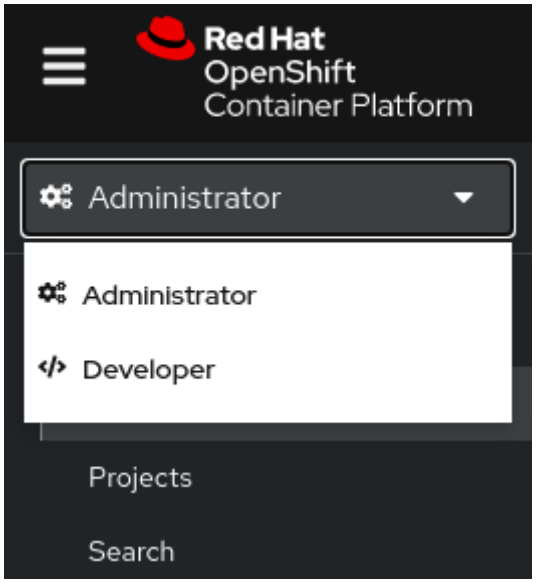
Webhooks allow external services to be notified when certain events happen. When the specified events happen, we'll send a POST request to each of the URLs you provide. Learn more in our Webhooks Guide.

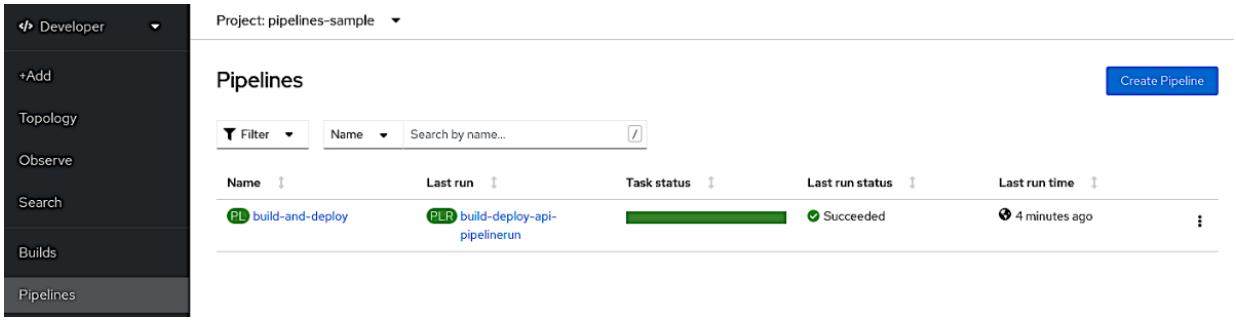
✓ http://el-clouds-api-el-default.ap… *(push)* Edit Delete

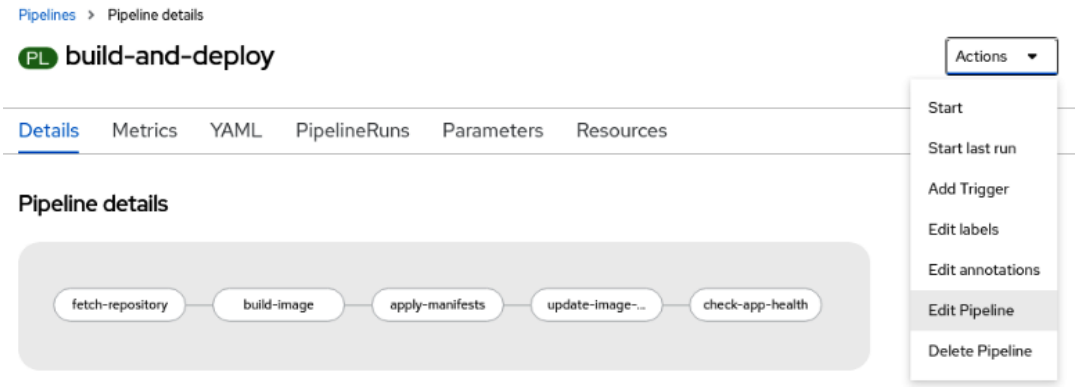

Project: pipelines-sample
Pipelines
Pipelines
PipelineRuns
PipelineResources
Conditions
Filter
Name
Search by name...
/
Name
Status
Task status
Started
PLR
build-deploy-api-pipelinerun
Succeeded
3 minutes ago

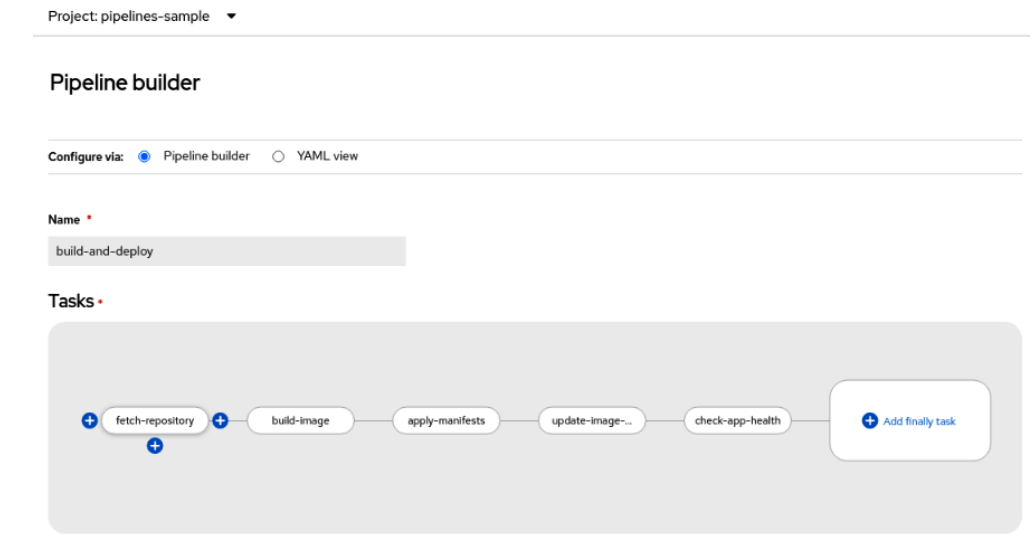

TEKTON HUB
yaml
Login
Welcome to Tekton Hub
Discover, search and share reusable Tasks and Pipelines
Sort By
Kind
Pipeline
Task
Platform
Linux/amd64
Linux/ppc64le
Linux/s390x
Linux/arm64
Catalog
Tekton
Category
1
YAML linter
v0.1
This task can be used to perform lint check on YAML files
Updated a year ago
linter

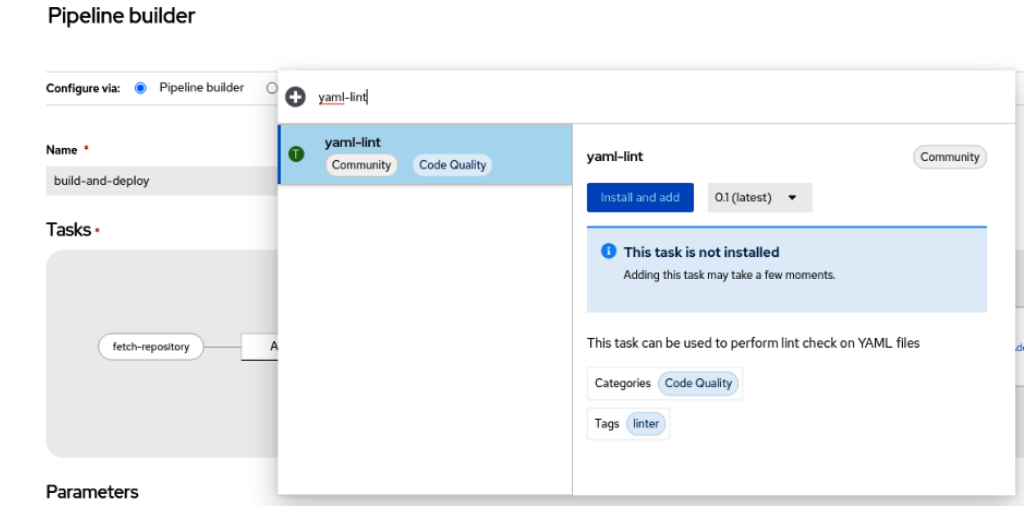

TEKTON HUB
yaml
Login
YAML linter
Open yaml-lint in Github
This task can be used to perform lint check on YAML files
linter
linux/amd64
1
Install
0.1 (latest)
Description
YAML
YAML Linter
The following task is used to provide static analysis on YAML files mounted using yamllint (YAML linter).
Installing the Task
1 kubectl apply -f https://api.hub.tekton.dev/v1/resource/tekton/task/yaml-lint/0.1/raw
Parameters
args: The extra params along with the file path needs to be provided as the part of args. (Default: ["--help"])
Workspaces

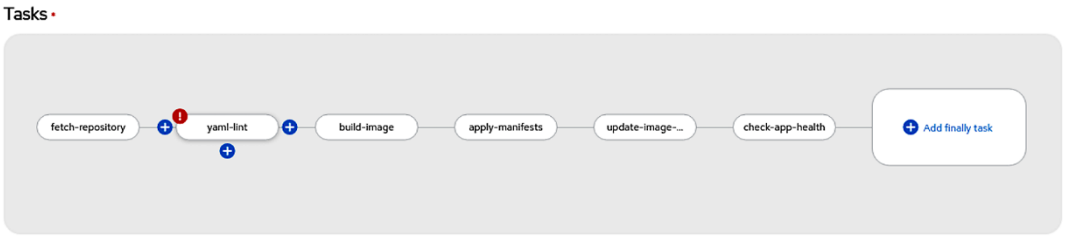

Red Hat
OpenShift
Container Platform
Administrator
Administrator
Developer
Projects
Search


Developer
+Add
Topology
Observe
Search
Builds
Pipelines
Project: pipelines-sample
Pipelines
Create Pipeline
Filter
Name
Search by name...
Name
Last run
Task status
Last run status
Last run time
PL build-and-deploy
PLR build-deploy-api-pipelinerun
Succeeded
4 minutes ago


Pipelines > Pipeline details
PL build-and-deploy
Actions
Details
Metrics
YAML
PipelineRuns
Parameters
Resources
Pipeline details
fetch-repository
build-image
apply-manifests
update-image-...
check-app-health
Start
Start last run
Add Trigger
Edit labels
Edit annotations
Edit Pipeline
Delete Pipeline


Project: pipelines-sample
Pipeline builder
Configure via:
Pipeline builder
YAML view
Name *
build-and-deploy
Tasks *
fetch-repository
build-image
apply-manifests
update-image-...
check-app-health
Add finally task


Pipeline builder
Configure via:
Pipeline builder
Name *
build-and-deploy
Tasks *
fetch-repository
yaml-lint
yaml-lint
Community
Code Quality
yaml-lint
Community
Install and add
0.1 (latest)
This task is not installed
Adding this task may take a few moments.
This task can be used to perform lint check on YAML files
Categories
Code Quality
Tags
linter
Parameters


Tasks *
fetch-repository
yaml-lint
build-image
apply-manifests
update-image-...
check-app-health
Add finally task

yaml-lint

Actions

View shortcuts

Display name *

yaml-lint

Parameters

Use this format when you reference variables in this form: `$(`

args

./sample-go-app/clouds-api/k8s

Add values

Workspaces

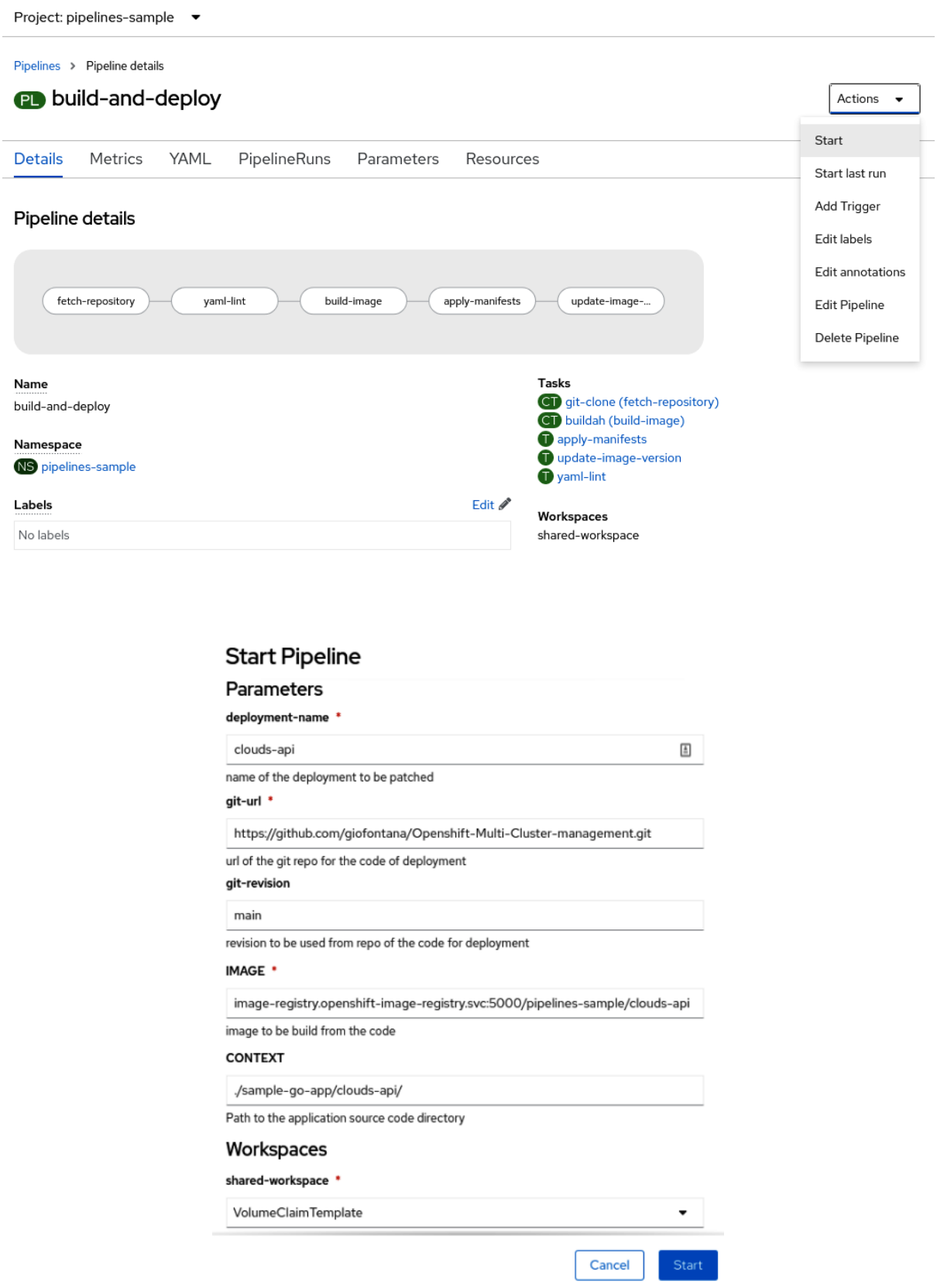
shared-workspace *

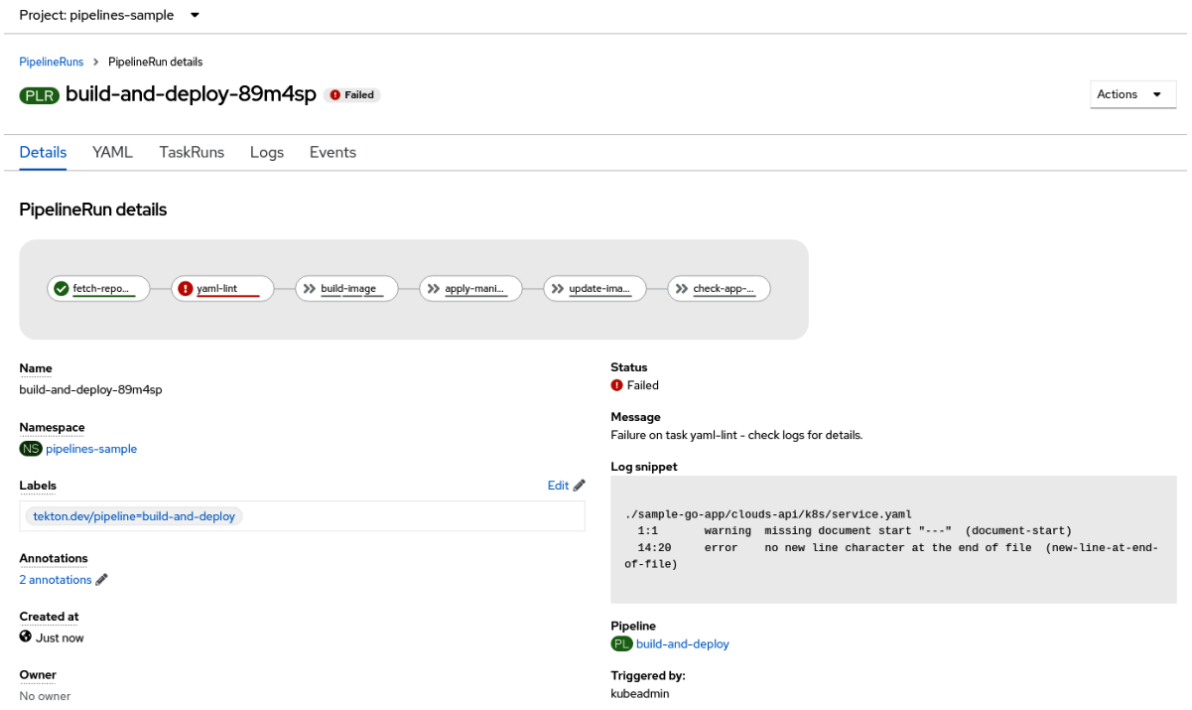
shared-workspace

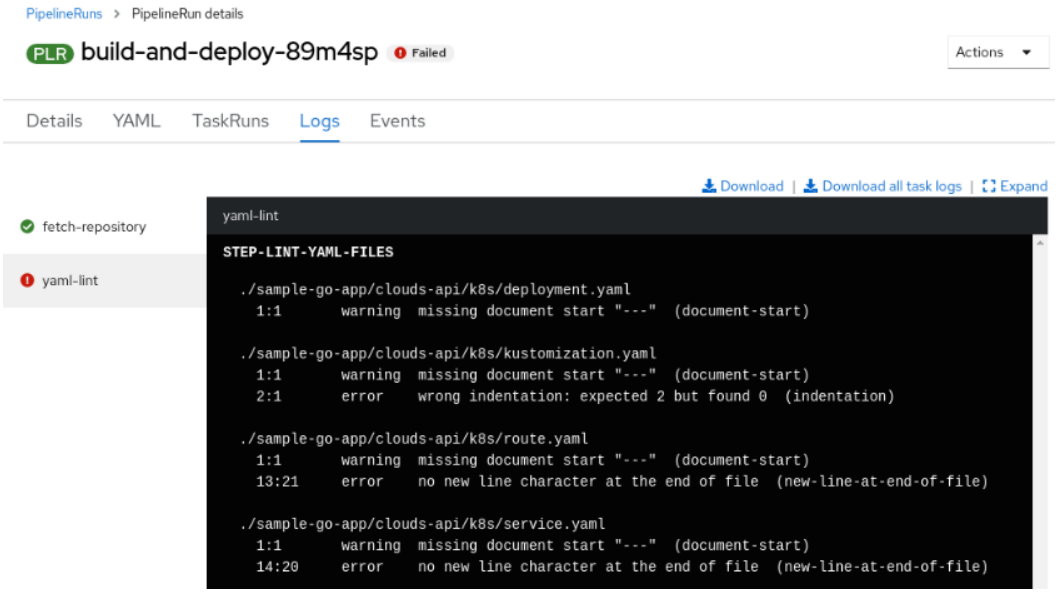
When expressions

No when expressions are associated with this task.

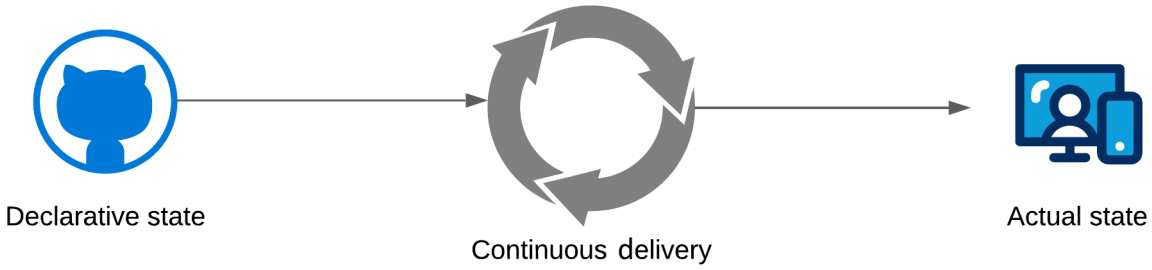
Add when expression

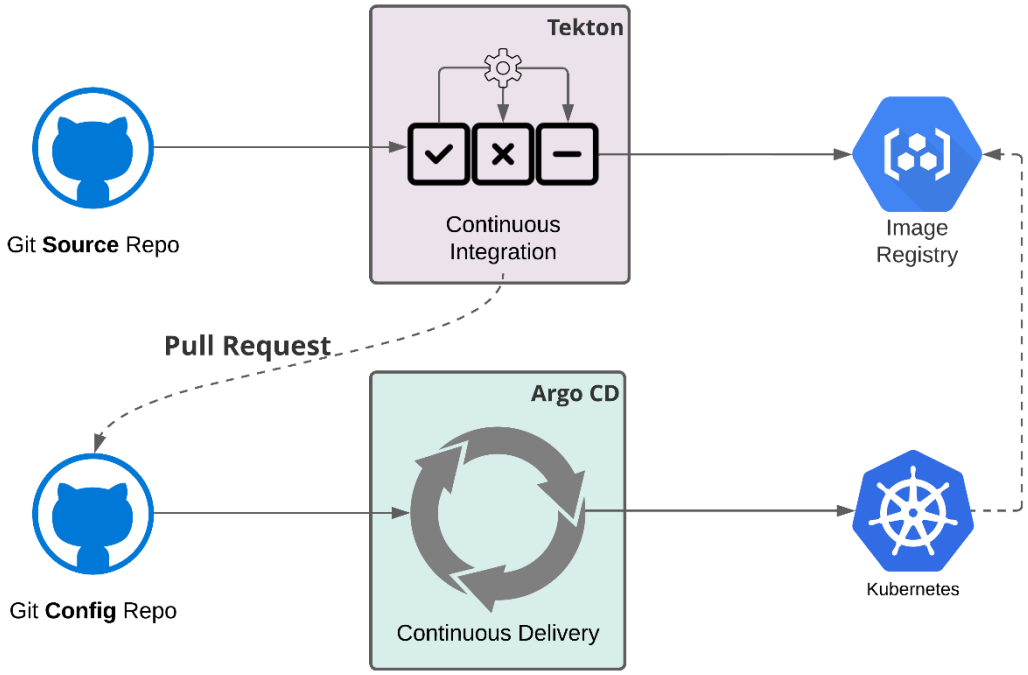

Project: pipelines-sample
Pipelines > Pipeline details
PL build-and-deploy
Actions
Start
Start last run
Add Trigger
Edit labels
Edit annotations
Edit Pipeline
Delete Pipeline
Details
Metrics
YAML
PipelineRuns
Parameters
Resources
Pipeline details
fetch-repository
yaml-lint
build-image
apply-manifests
update-image-...
Name
build-and-deploy
Namespace
NS pipelines-sample
Labels
Edit
No labels
Tasks
CT git-clone (fetch-repository)
CT buildah (build-image)
T apply-manifests
T update-image-version
T yaml-lint
Workspaces
shared-workspace
Start Pipeline
Parameters
deployment-name *
clouds-api
name of the deployment to be patched
git-url *
https://github.com/giofontana/Openshift-Multi-Cluster-management.git
url of the git repo for the code of deployment
git-revision
main
revision to be used from repo of the code for deployment
IMAGE *
image-registry.openshift-image-registry.svc:5000/pipelines-sample/clouds-api
image to be build from the code
CONTEXT
./sample-go-app/clouds-api/
Path to the application source code directory
Workspaces
shared-workspace *
VolumeClaimTemplate
Cancel
Start

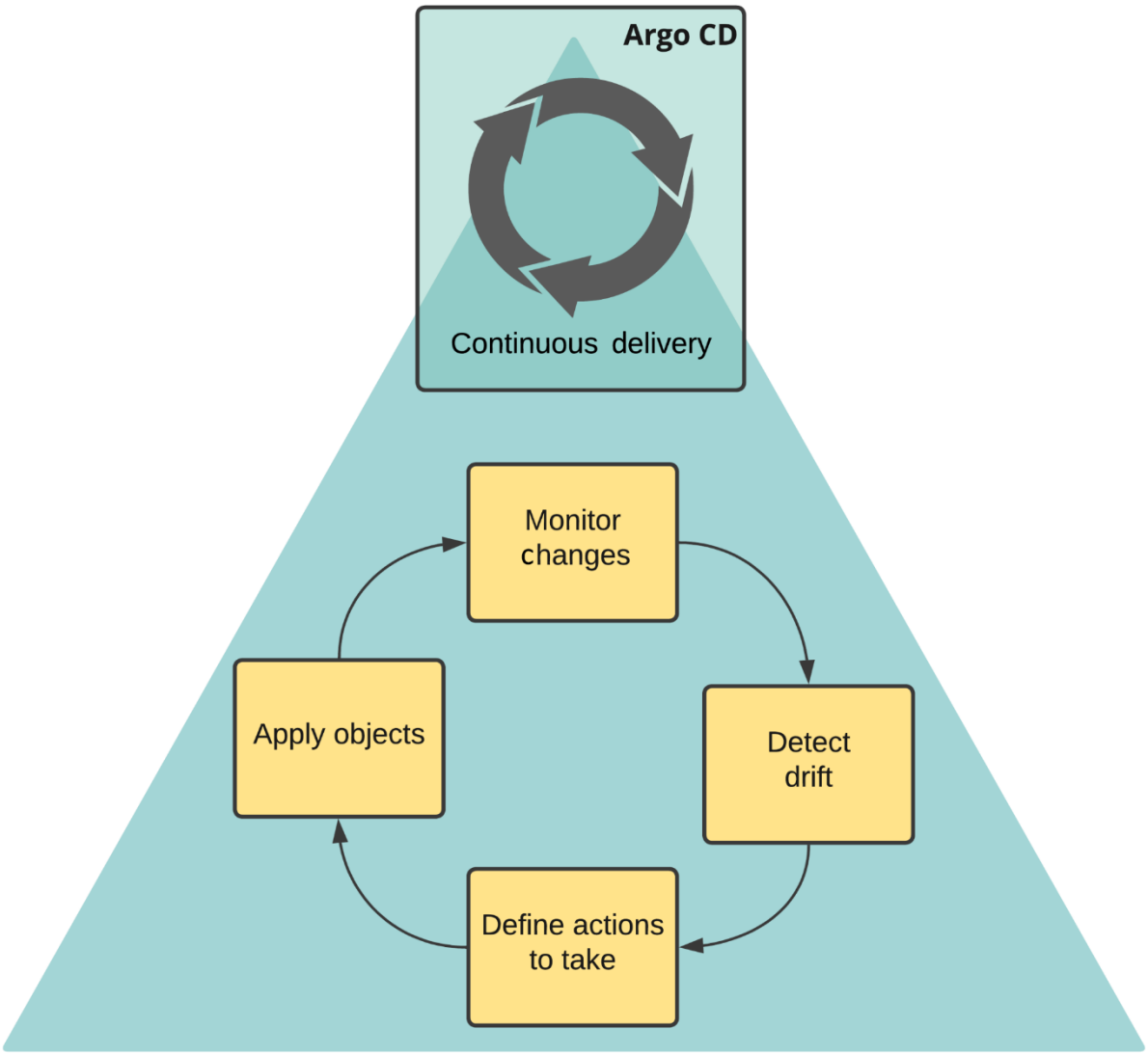

Project: pipelines-sample
PipelineRuns > PipelineRun details
PLR build-and-deploy-89m4sp Failed
Actions
Details YAML TaskRuns Logs Events
PipelineRun details
fetch-repo...
yaml-lint
build-image
apply-mani...
update-ima...
check-app-...
Name
build-and-deploy-89m4sp
Namespace
NS pipelines-sample
Labels
Edit
tekton.dev/pipeline=build-and-deploy
Annotations
2 annotations
Created at
Just now
Owner
No owner
Status
Failed
Message
Failure on task yaml-lint - check logs for details.
Log snippet
./sample-go-app/clouds-api/k8s/service.yaml
1:1 warning missing document start "---" (document-start)
14:20 error no new line character at the end of file (new-line-at-end-of-file)
Pipeline
PL build-and-deploy
Triggered by:
kubeadmin

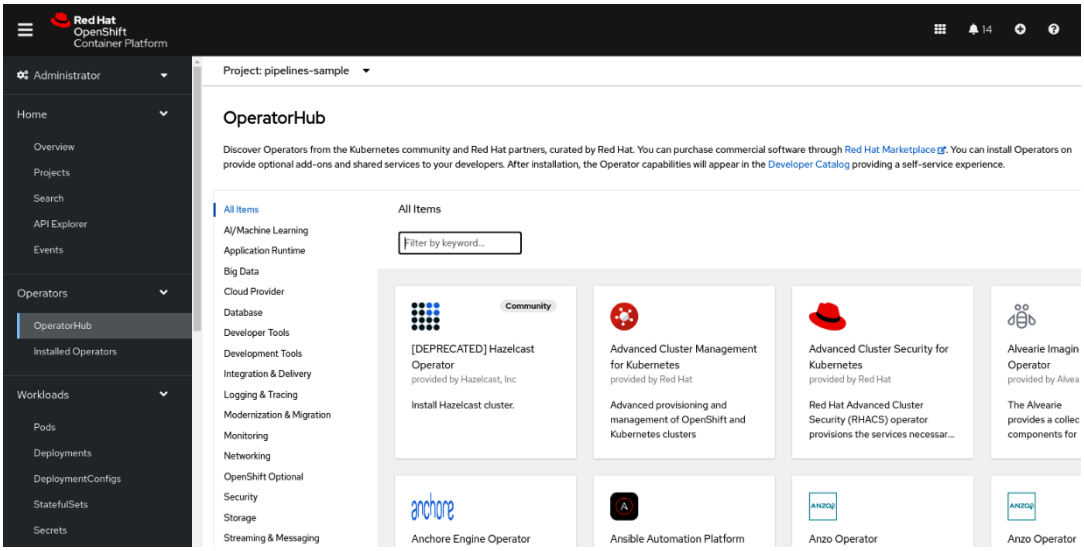

PipelineRuns > PipelineRun details
PLR build-and-deploy-89m4sp Failed
Actions
Details YAML TaskRuns Logs Events
Download | Download all task logs | Expand
fetch-repository
yaml-lint
yaml-lint
STEP-LINT-YAML-FILES
./sample-go-app/clouds-api/k8s/deployment.yaml
1:1 warning missing document start "---" (document-start)
./sample-go-app/clouds-api/k8s/kustomization.yaml
1:1 warning missing document start "---" (document-start)
2:1 error wrong indentation: expected 2 but found 0 (indentation)
./sample-go-app/clouds-api/k8s/route.yaml
1:1 warning missing document start "---" (document-start)
13:21 error no new line character at the end of file (new-line-at-end-of-file)
./sample-go-app/clouds-api/k8s/service.yaml
1:1 warning missing document start "---" (document-start)
14:20 error no new line character at the end of file (new-line-at-end-of-file)

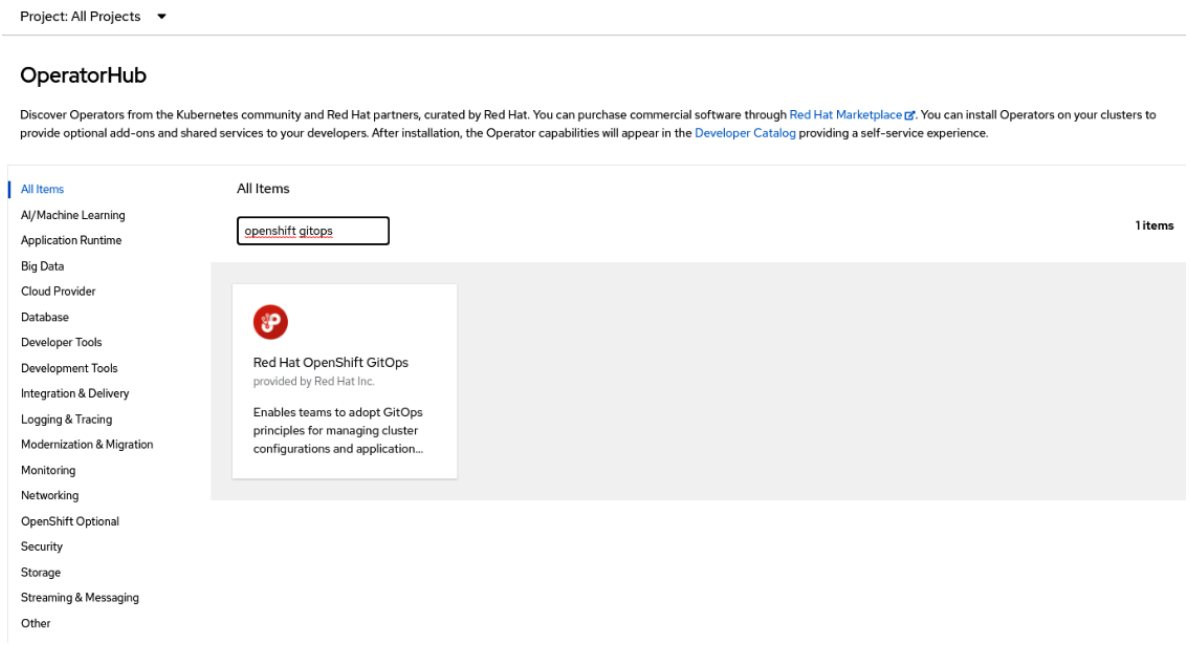
Chapter 10: OpenShift GitOps – Argo CD






Argo CD
Continuous delivery
Monitor changes
Detect drift
Define actions to take
Apply objects


Red Hat OpenShift Container Platform
Administrator
Home
Overview
Projects
Search
API Explorer
Events
Operators
OperatorHub
Installed Operators
Workloads
Pods
Deployments
DeploymentConfigs
StatefulSets
Secrets
Project: pipelines-sample
OperatorHub
Discover Operators from the Kubernetes community and Red Hat partners, curated by Red Hat. You can purchase commercial software through Red Hat Marketplace. You can install Operators on provide optional add-ons and shared services to your developers. After installation, the Operator capabilities will appear in the Developer Catalog providing a self-service experience.
All Items
AI/Machine Learning
Application Runtime
Big Data
Cloud Provider
Database
Developer Tools
Development Tools
Integration & Delivery
Logging & Tracing
Modernization & Migration
Monitoring
Networking
OpenShift Optional
Security
Storage
Streaming & Messaging
All Items
Filter by keyword...
Community
[DEPRECATED] Hazelcast Operator
provided by Hazelcast, Inc
Install Hazelcast cluster.
Advanced Cluster Management for Kubernetes
provided by Red Hat
Advanced provisioning and management of OpenShift and Kubernetes clusters
Advanced Cluster Security for Kubernetes
provided by Red Hat
Red Hat Advanced Cluster Security (RHACS) operator provisions the services necessar...
Alvearie Imagin Operator
provided by Alvea
The Alvearie provides a collec components for
anchore
Anchore Engine Operator
Ansible Automation Platform
Anzo Operator
Anzo Operator


Project: All Projects
OperatorHub
Discover Operators from the Kubernetes community and Red Hat partners, curated by Red Hat. You can purchase commercial software through Red Hat Marketplace. You can install Operators on your clusters to provide optional add-ons and shared services to your developers. After installation, the Operator capabilities will appear in the Developer Catalog providing a self-service experience.
All Items
AI/Machine Learning
Application Runtime
Big Data
Cloud Provider
Database
Developer Tools
Development Tools
Integration & Delivery
Logging & Tracing
Modernization & Migration
Monitoring
Networking
OpenShift Optional
Security
Storage
Streaming & Messaging
Other
All Items
openshift gitops
1 items
Red Hat OpenShift GitOps
provided by Red Hat Inc.
Enables teams to adopt GitOps principles for managing cluster configurations and application...

Red Hat OpenShift GitOps

1.3.2 provided by Red Hat Inc.

Install

Latest version

1.3.2

Capability level

- Basic Install
- Seamless Upgrades
- Full Lifecycle
- Deep Insights
- Auto Pilot

Source

Red Hat

Provider

Red Hat Inc.

Infrastructure features

Disconnected

Repository

N/A

Container image

registry.redhat.io/openshift-gitops-1/gitops-rhel8-operator@sha256:67cd9f0b3c969fda1a62a732be1f7ca356c32c4d4913eefe689674408cabbb8c

Red Hat OpenShift GitOps is a declarative continuous delivery platform based on Argo CD. It enables teams to adopt GitOps principles for managing cluster configurations and automating secure and repeatable application delivery across hybrid multi-cluster Kubernetes environments. Following GitOps and infrastructure as code principles, you can store the configuration of clusters and applications in Git repositories and use Git workflows to roll them out to the target clusters.

Features

- Automated install and upgrades of Argo CD
- Manual and automated configuration sync from Git repositories to target OpenShift and Kubernetes clusters
- Support for the Helm and Kustomize templating tools
- Configuration drift detection and visualization on live clusters
- Audit trails of rollouts to the clusters
- Monitoring and logging integration with OpenShift
- Automated GitOps bootstrapping using Tekton and Argo CD with GitOps Application Manager CLI

Components

- Argo CD v2.1.8
- GitOps Application Manager CLI (download)

How to Install

After installing the OpenShift GitOps operator, an instance of Argo CD is installed in the `openshift-gitops` namespace which has sufficent privileges for managing cluster configurations. You can create additional Argo CD instances using the `ArgoCD` custom resource within the desired namespaces.

```
apiVersion: argoproj.io/v1alpha1
kind: ArgoCD
metadata:
  name: argocd
spec:
  server:
```

Install Operator

Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.

Update channel *

- preview
- stable

Installation mode *

- All namespaces on the cluster (default)
  Operator will be available in all Namespaces.
- A specific namespace on the cluster
  This mode is not supported by this Operator

Installed Namespace *

PR openshift-operators

Update approval *

- Automatic
- Manual

Install Cancel

Red Hat OpenShift GitOps
provided by Red Hat Inc.

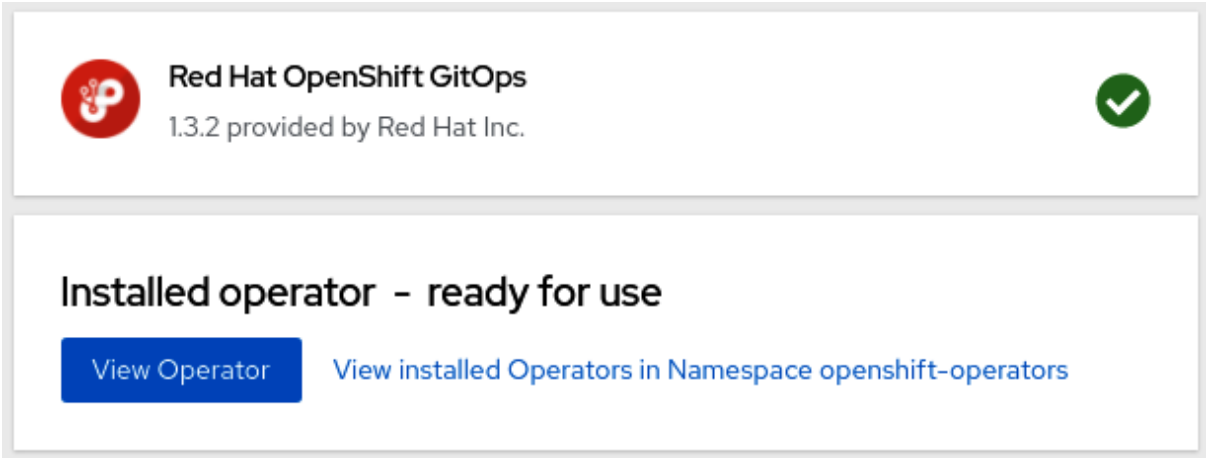
Provided APIs

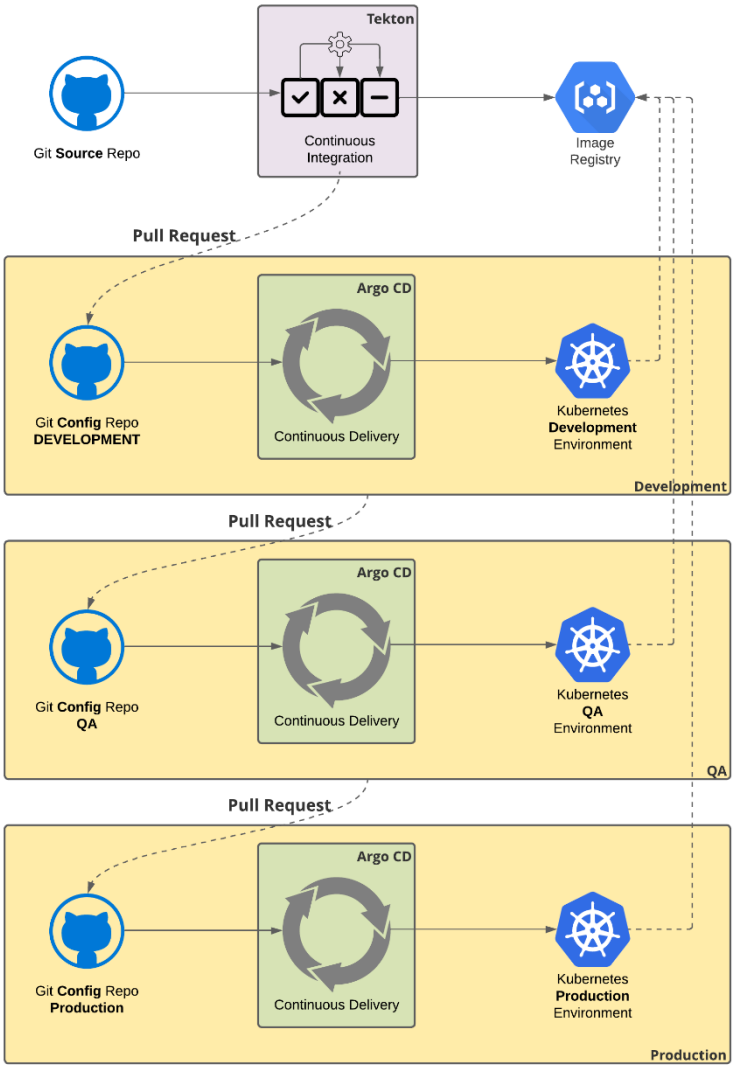
A Application
An Application is a group of Kubernetes resources as defined by a manifest.

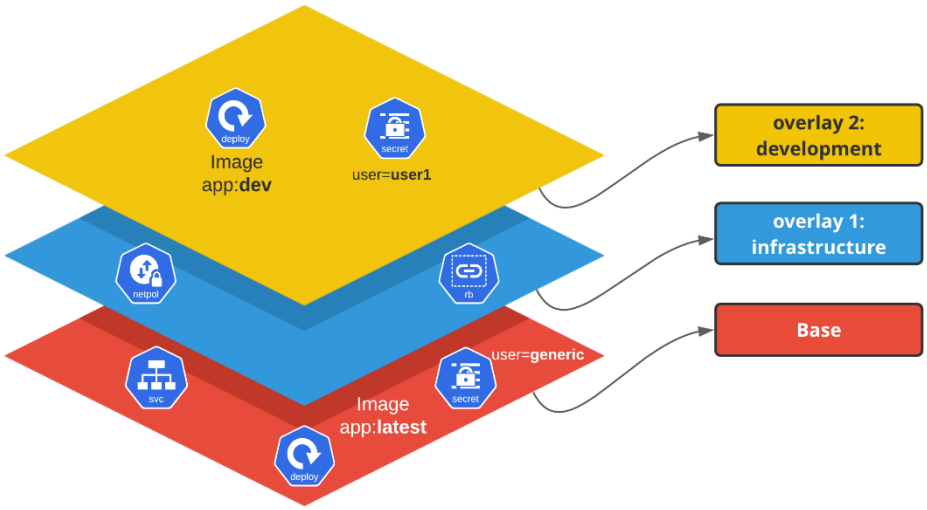
AS ApplicationSet
ApplicationSet is the representation of an ApplicationSet controller deployment.

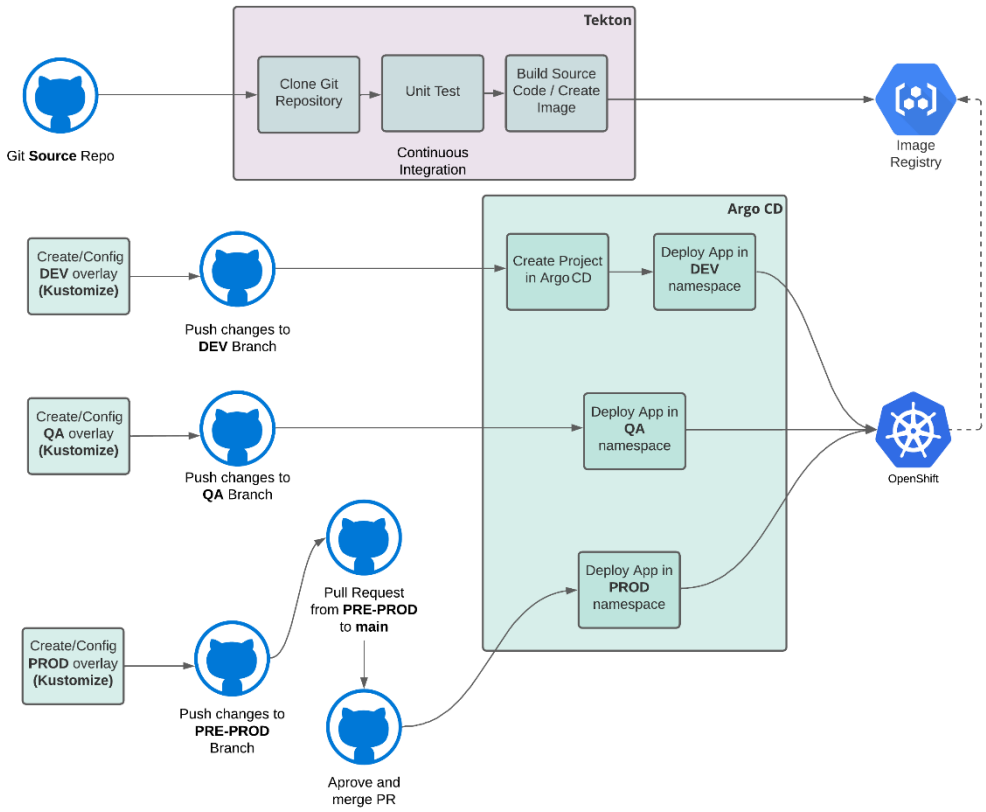
AP AppProject
An AppProject is a logical grouping of Argo CD Applications.

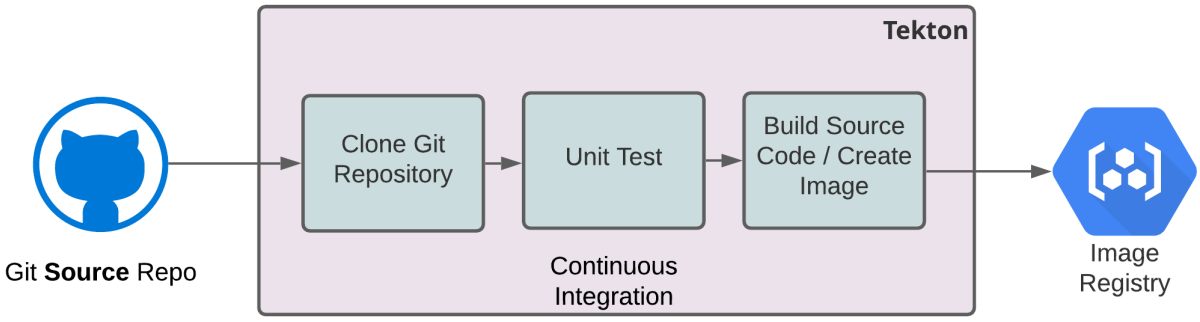
ACD Argo CD
Argo CD is the representation of an Argo CD deployment.


Red Hat OpenShift GitOps
1.3.2 provided by Red Hat Inc.
Installed operator - ready for use
View Operator
View installed Operators in Namespace openshift-operators


Tekton
Git Source Repo
Continuous Integration
Image Registry
Pull Request
Argo CD
Git Config Repo DEVELOPMENT
Continuous Delivery
Kubernetes Development Environment
Development
Pull Request
Argo CD
Git Config Repo QA
Continuous Delivery
Kubernetes QA Environment
QA
Pull Request
Argo CD
Git Config Repo Production
Continuous Delivery
Kubernetes Production Environment
Production


deploy
Image
app:dev
secret
user=user1
overlay 2:
development
overlay 1:
infrastructure
Base
netpol
rb
svc
secret
user=generic
Image
app:latest
deploy


Tekton
Clone Git
Repository
Unit Test
Build Source
Code / Create
Image
Continuous
Integration
Git Source Repo
Image
Registry
Argo CD
Create/Config
DEV overlay
(Kustomize)
Push changes to
DEV Branch
Create Project
in Argo CD
Deploy App in
DEV
namespace
Create/Config
QA overlay
(Kustomize)
Push changes to
QA Branch
Deploy App in
QA
namespace
OpenShift
Pull Request
from PRE-PROD
to main
Deploy App in
PROD
namespace
Create/Config
PROD overlay
(Kustomize)
Push changes to
PRE-PROD
Branch
Aprove and
merge PR


Tekton
Clone Git Repository
Unit Test
Build Source Code / Create Image
Git **Source** Repo
Continuous Integration
Image Registry

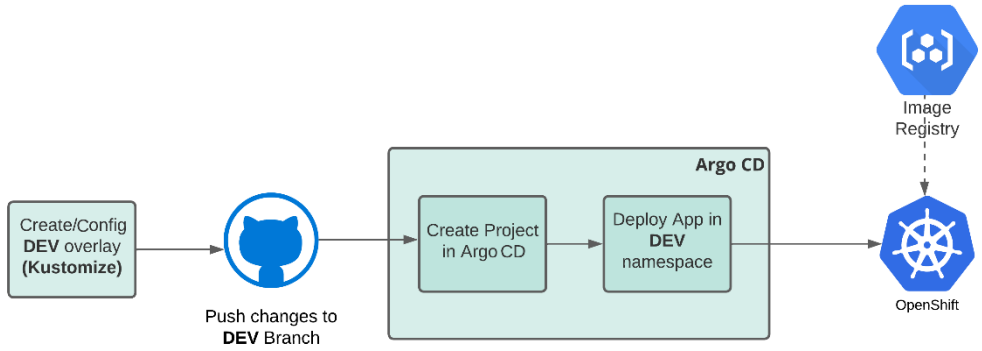
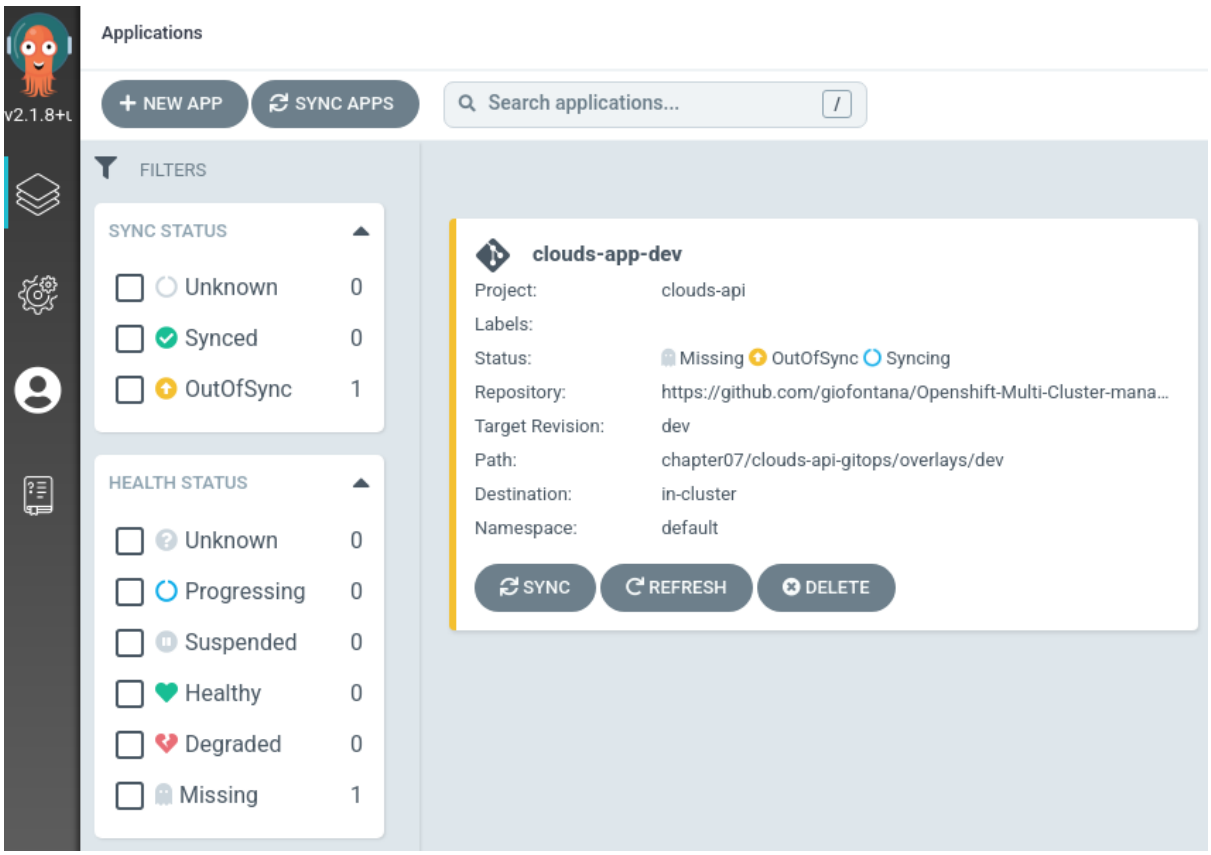
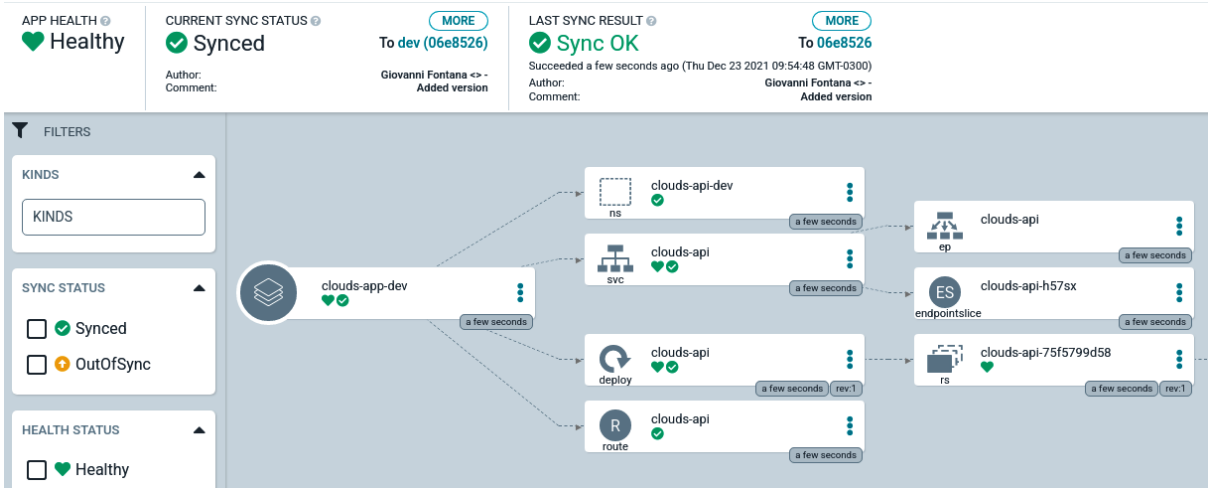


Image Registry
Argo CD
Create/Config **DEV** overlay **(Kustomize)**
Push changes to **DEV** Branch
Create Project in Argo CD
Deploy App in **DEV** namespace
OpenShift


Applications
v2.1.8+1
+ NEW APP
SYNC APPS
Search applications...
/
FILTERS
SYNC STATUS
Unknown 0
Synced 0
OutOfSync 1
HEALTH STATUS
Unknown 0
Progressing 0
Suspended 0
Healthy 0
Degraded 0
Missing 1
clouds-app-dev
Project: clouds-api
Labels:
Status: Missing OutOfSync Syncing
Repository: https://github.com/giofontana/Openshift-Multi-Cluster-mana...
Target Revision: dev
Path: chapter07/clouds-api-gitops/overlays/dev
Destination: in-cluster
Namespace: default
SYNC
REFRESH
DELETE


APP HEALTH
Healthy
CURRENT SYNC STATUS
Synced
MORE
To dev (06e8526)
Author:
Comment:
Giovanni Fontana <> -
Added version
LAST SYNC RESULT
Sync OK
MORE
To 06e8526
Succeeded a few seconds ago (Thu Dec 23 2021 09:54:48 GMT-0300)
Author:
Comment:
Giovanni Fontana <> -
Added version
FILTERS
KINDS
KINDS
SYNC STATUS
Synced
OutOfSync
HEALTH STATUS
Healthy
clouds-app-dev
clouds-api-dev
ns
clouds-api
svc
clouds-api
deploy
clouds-api
route
clouds-api
ep
clouds-api-h57sx
endpointslice
clouds-api-75f5799d58
rs
a few seconds
rev:1

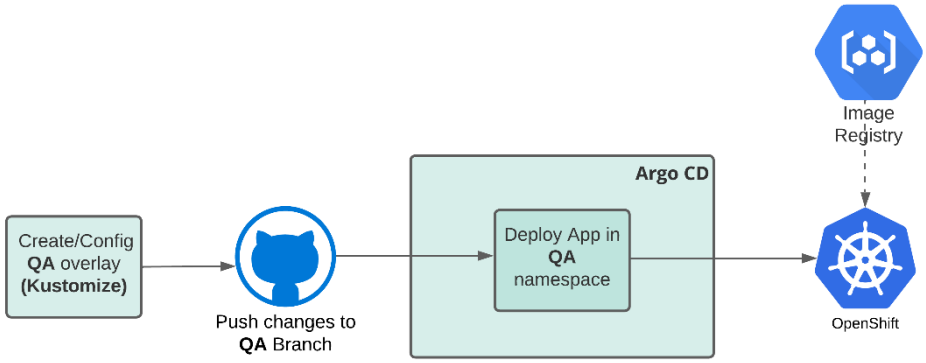
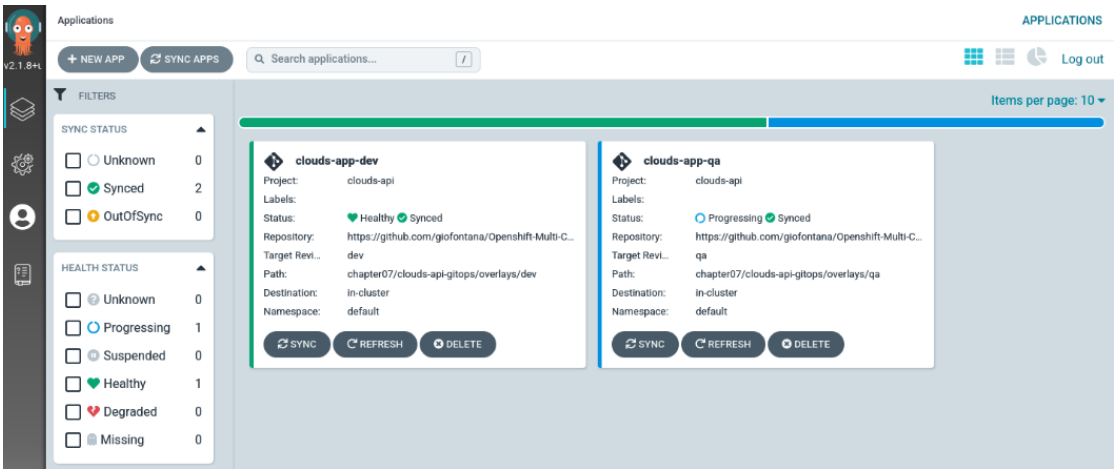


Image Registry
Argo CD
Create/Config QA overlay (Kustomize)
Push changes to QA Branch
Deploy App in QA namespace
OpenShift


Applications
APPLICATIONS
+ NEW APP
SYNC APPS
Search applications...
Log out
FILTERS
Items per page: 10
SYNC STATUS
Unknown 0
Synced 2
OutOfSync 0
HEALTH STATUS
Unknown 0
Progressing 1
Suspended 0
Healthy 1
Degraded 0
Missing 0
clouds-app-dev
Project: clouds-api
Labels:
Status: Healthy Synced
Repository: https://github.com/giofontana/Openshift-Multi-C...
Target Revi... dev
Path: chapter07/clouds-api-gitops/overlays/dev
Destination: in-cluster
Namespace: default
SYNC
REFRESH
DELETE
clouds-app-qa
Project: clouds-api
Labels:
Status: Progressing Synced
Repository: https://github.com/giofontana/Openshift-Multi-C...
Target Revi... qa
Path: chapter07/clouds-api-gitops/overlays/qa
Destination: in-cluster
Namespace: default
SYNC
REFRESH
DELETE

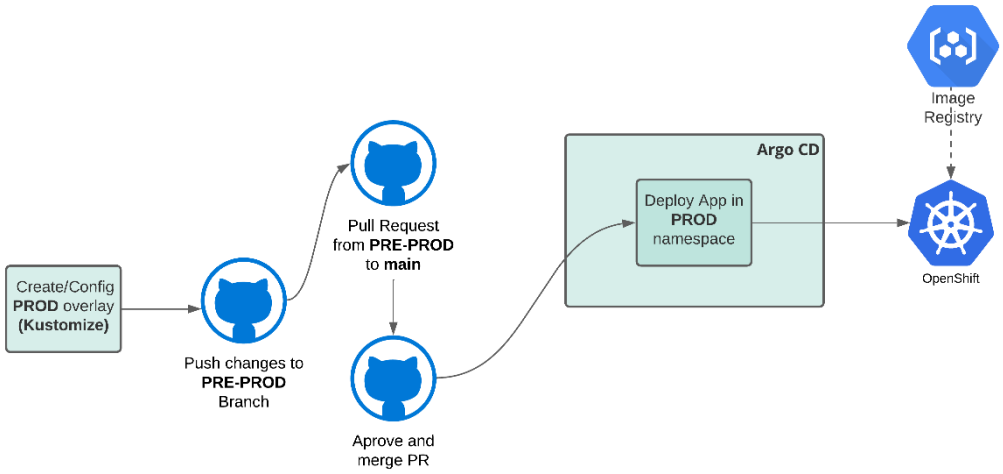
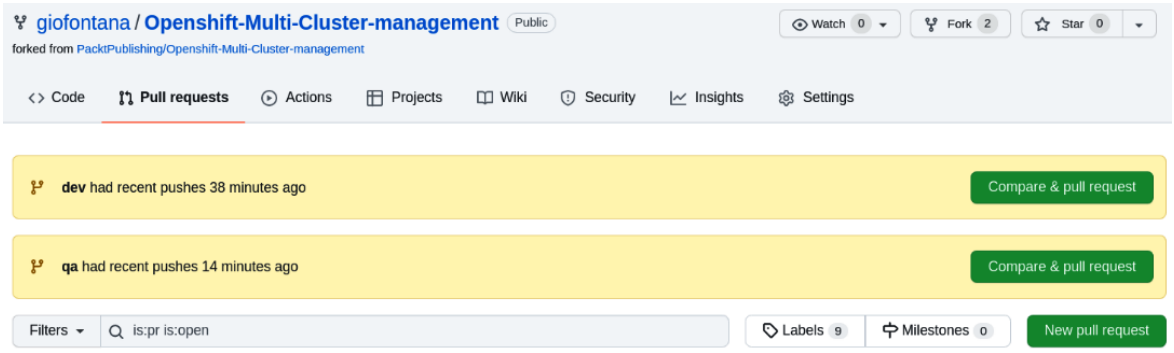
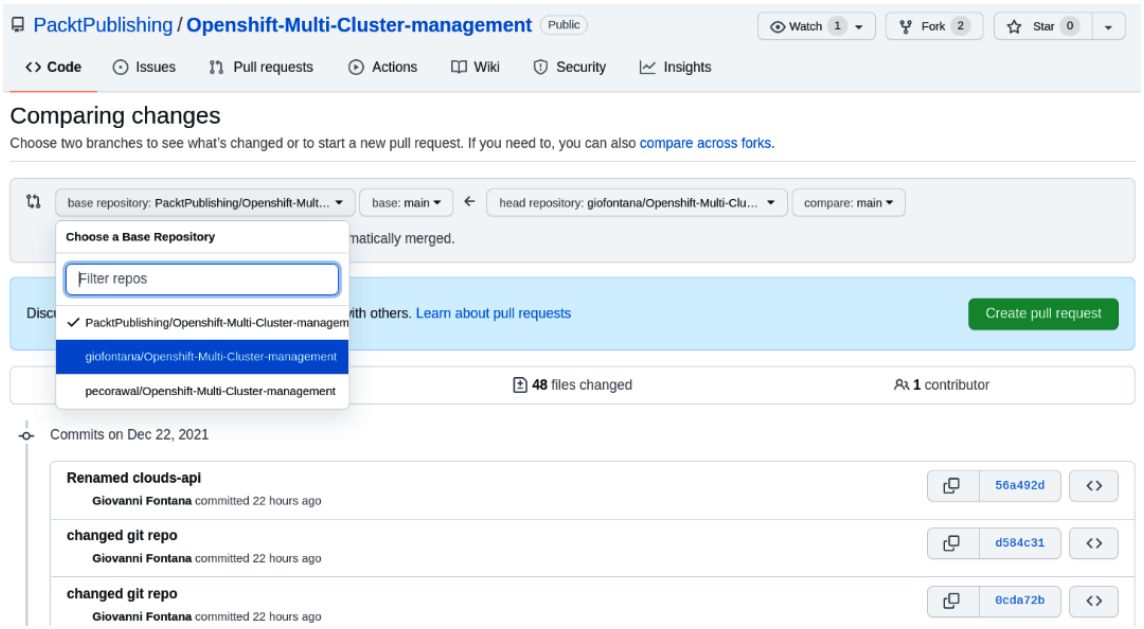


Image Registry
Argo CD
Deploy App in PROD namespace
OpenShift
Pull Request from PRE-PROD to main
Create/Config PROD overlay (Kustomize)
Push changes to PRE-PROD Branch
Aprove and merge PR


giofontana / Openshift-Multi-Cluster-management
Public
forked from PacktPublishing/Openshift-Multi-Cluster-management
Watch 0
Fork 2
Star 0
Code
Pull requests
Actions
Projects
Wiki
Security
Insights
Settings
dev had recent pushes 38 minutes ago
Compare & pull request
qa had recent pushes 14 minutes ago
Compare & pull request
Filters
is:pr is:open
Labels 9
Milestones 0
New pull request


PacktPublishing / Openshift-Multi-Cluster-management
Public
Watch 1
Fork 2
Star 0
Code
Issues
Pull requests
Actions
Wiki
Security
Insights
Comparing changes
Choose two branches to see what's changed or to start a new pull request. If you need to, you can also compare across forks.
base repository: PacktPublishing/Openshift-Mult...
base: main
head repository: giofontana/Openshift-Multi-Clu...
compare: main
Choose a Base Repository
Filter repos
PacktPublishing/Openshift-Multi-Cluster-managem
giofontana/Openshift-Multi-Cluster-management
pecorawal/Openshift-Multi-Cluster-management
matically merged.
ith others. Learn about pull requests
Create pull request
48 files changed
1 contributor
Commits on Dec 22, 2021
Renamed clouds-api
Giovanni Fontana committed 22 hours ago
56a492d
changed git repo
Giovanni Fontana committed 22 hours ago
d584c31
changed git repo
Giovanni Fontana committed 22 hours ago
0cda72b

Comparing changes

Choose two branches to see what's changed or to start a new pull request. If you need to, you can also compare across forks.

base: main ← compare: pre-prod ✓ **Able to merge.** These branches can be automatically merged.

Discuss and review the changes in this comparison with others. Learn about pull requests

Create pull request

giofontana / **Openshift-Multi-Cluster-management** Public

forked from PacktPublishing/Openshift-Multi-Cluster-management

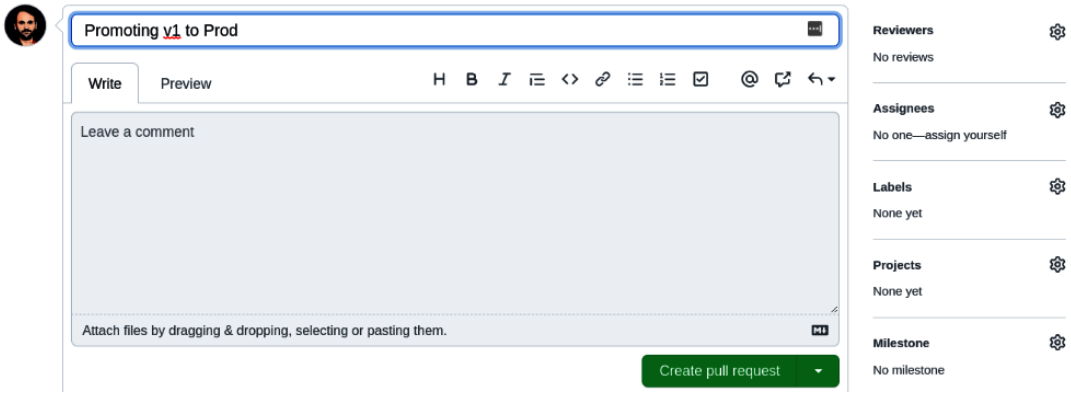
Watch 0 Fork 2 Star 0

<> Code Pull requests Actions Projects Wiki Security Insights Settings

Open a pull request

Create a new pull request by comparing changes across two branches. If you need to, you can also compare across forks.

base: main ← compare: pre-prod ✓ **Able to merge.** These branches can be automatically merged.



Add more commits by pushing to the `pre-prod` branch on **giofontana/Openshift-Multi-Cluster-management**.

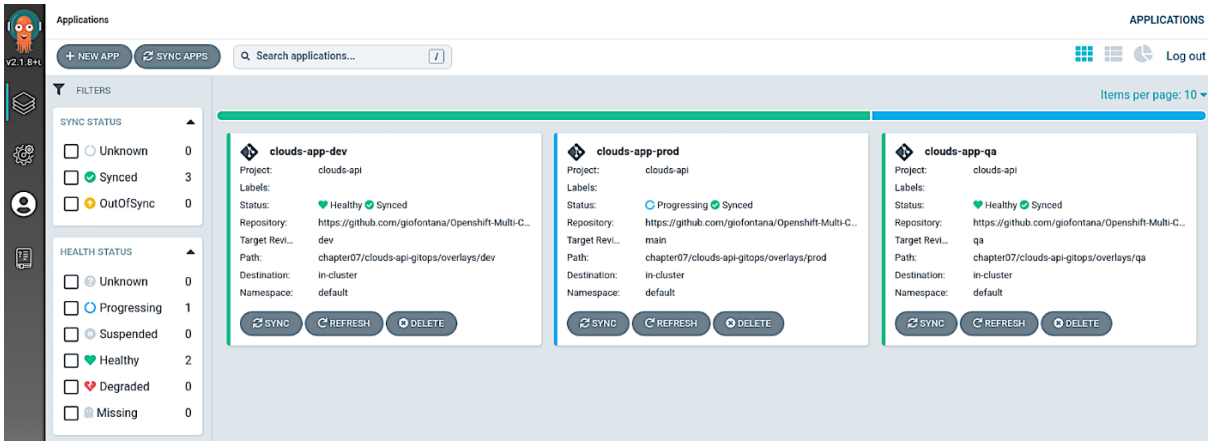
Continuous integration has not been set up

GitHub Actions and several other apps can be used to automatically catch bugs and enforce style.

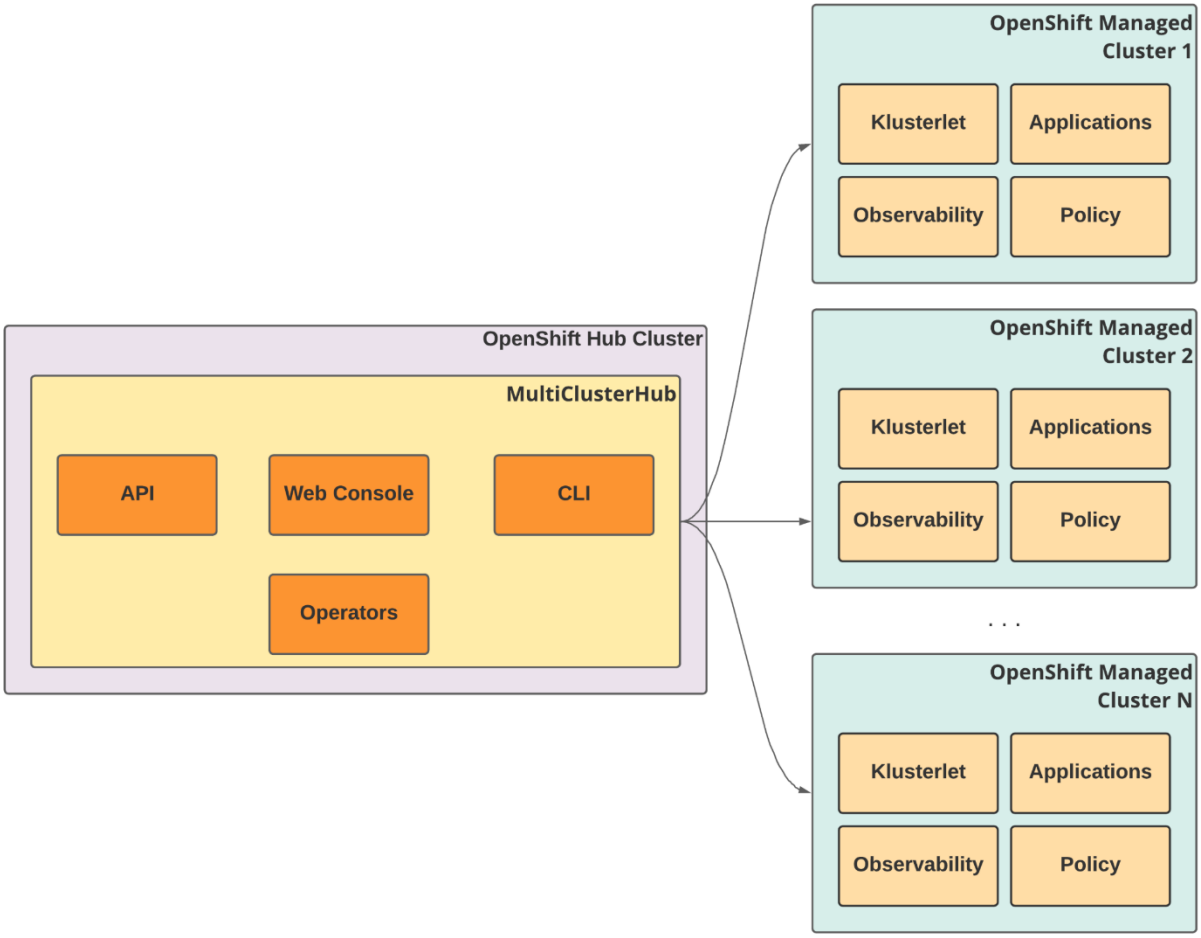
This branch has no conflicts with the base branch

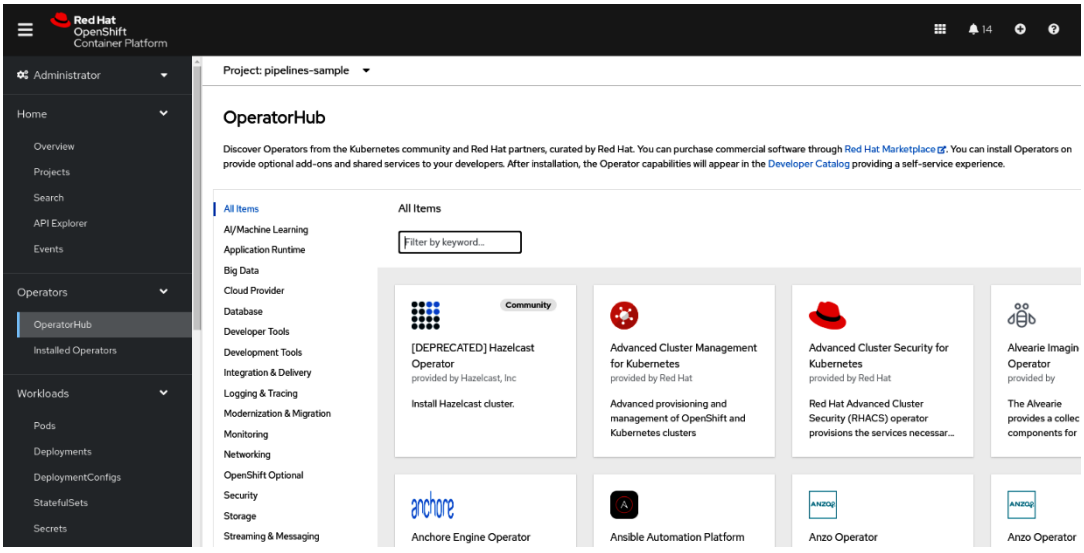
Merging can be performed automatically.

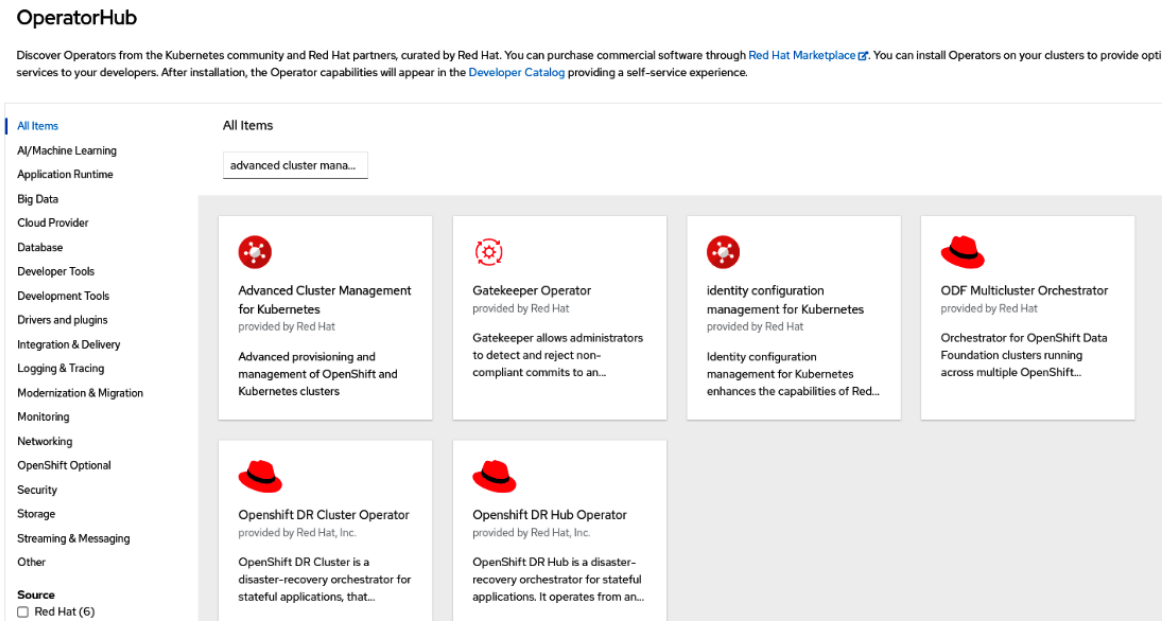
Merge pull request or view command line instructions.


Applications
APPLICATIONS
v2.1.8+t
+ NEW APP
SYNC APPS
Search applications...
/
Log out
FILTERS
Items per page: 10
SYNC STATUS
Unknown 0
Synced 3
OutOfSync 0
HEALTH STATUS
Unknown 0
Progressing 1
Suspended 0
Healthy 2
Degraded 0
Missing 0
clouds-app-dev
Project: clouds-api
Labels:
Status: Healthy Synced
Repository: https://github.com/giofontana/Openshift-Multi-C...
Target Revi... dev
Path: chapter07/clouds-api-gitops/overlays/dev
Destination: in-cluster
Namespace: default
SYNC
REFRESH
DELETE
clouds-app-prod
Project: clouds-api
Labels:
Status: Progressing Synced
Repository: https://github.com/giofontana/Openshift-Multi-C...
Target Revi... main
Path: chapter07/clouds-api-gitops/overlays/prod
Destination: in-cluster
Namespace: default
SYNC
REFRESH
DELETE
clouds-app-qa
Project: clouds-api
Labels:
Status: Healthy Synced
Repository: https://github.com/giofontana/Openshift-Multi-C...
Target Revi... qa
Path: chapter07/clouds-api-gitops/overlays/qa
Destination: in-cluster
Namespace: default
SYNC
REFRESH
DELETE

Chapter 11: OpenShift Multi-Cluster GitOps and Management







Advanced Cluster Management for Kubernetes

2.5.0 provided by Red Hat

Install

Latest version

2.5.0

Capability level

- Basic Install
- Seamless Upgrades
- Full Lifecycle
- Deep Insights
- Auto Pilot

Source

Red Hat

Provider

Red Hat

Infrastructure features

Disconnected
Proxy-aware
FIPS Mode

Valid Subscriptions

OpenShift Platform Plus
Red Hat Advanced Cluster Management for Kubernetes

Red Hat Advanced Cluster Management for Kubernetes provides the multicluster hub, a central management console for managing multiple Kubernetes-based clusters across data centers, public clouds, and private clouds. You can use the hub to create Red Hat OpenShift Container Platform clusters on selected providers, or import existing Kubernetes-based clusters. After the clusters are managed, you can set compliance requirements to ensure that the clusters maintain the specified security requirements. You can also deploy business applications across your clusters.

Red Hat Advanced Cluster Management for Kubernetes also provides the following operators:

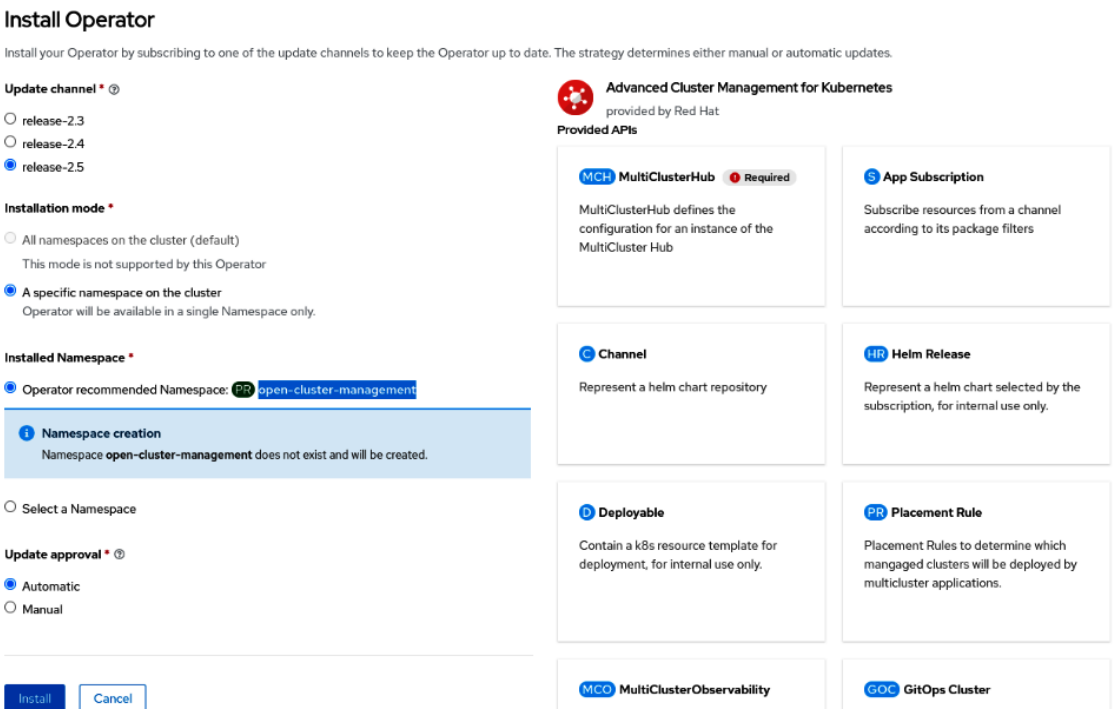
- Multicluster subscriptions: An operator that provides application management capabilties including subscribing to resources from a channel and deploying those resources on MCH-managed Kubernetes clusters based on placement rules.
- Hive for Red Hat OpenShift: An operator that provides APIs for provisioning and performing initial configuration of OpenShift clusters. These operators are used by the multicluster hub to provide its provisioning and application-management capabilities.

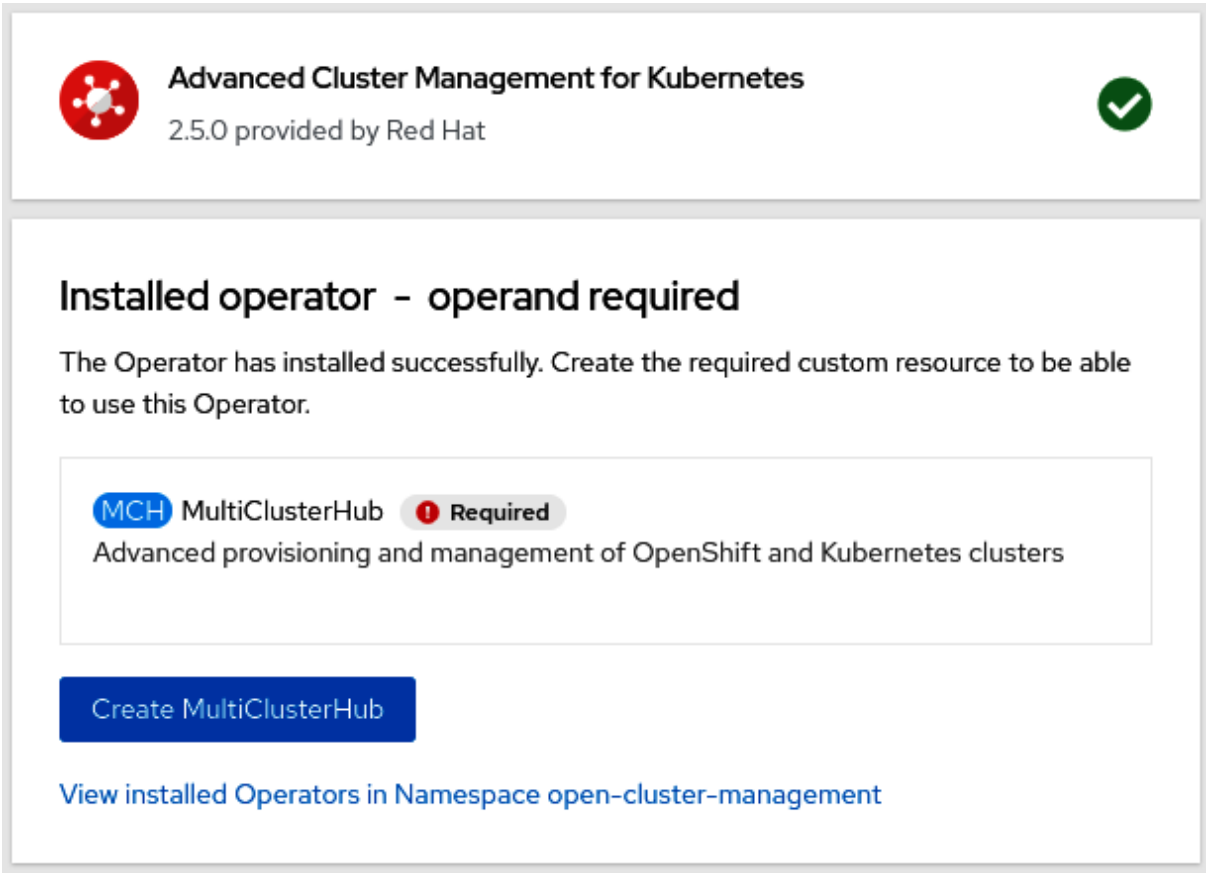
How to Install

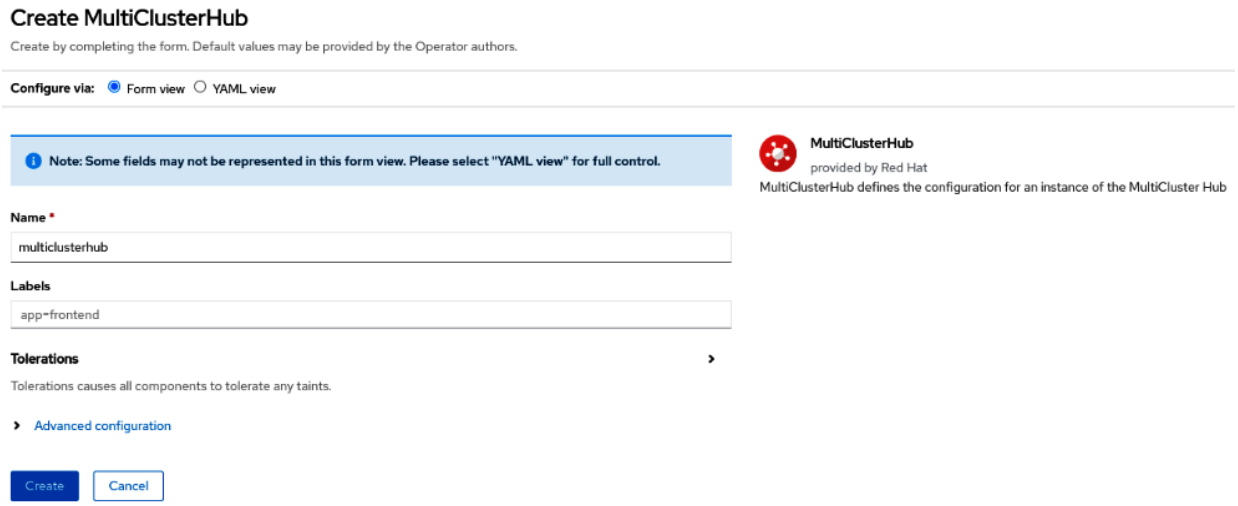
Use of this Red Hat product requires a licensing and subscription agreement.

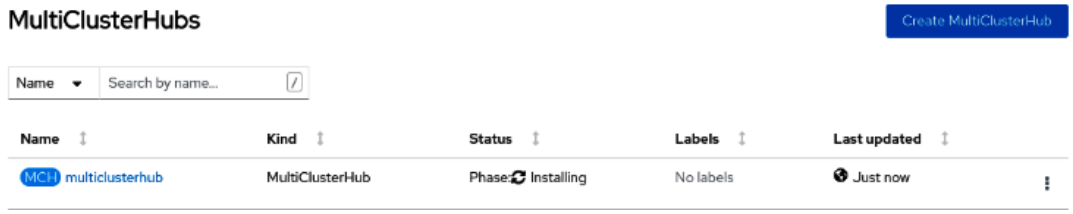
Install the Red Hat Advanced Cluster Management for Kubernetes operator by following instructions presented when you click the `Install` button. After installing the operator, create an instance of the `MultiClusterHub` resource to install the hub. Note that if you will be using the hub to manage non-OpenShift 4.x clusters, you will need to create a Kubernetes `Secret` resource containing your OpenShift pull secret and specify this `Secret` in the `MultiClusterHub` resource, as described in the install documentation.

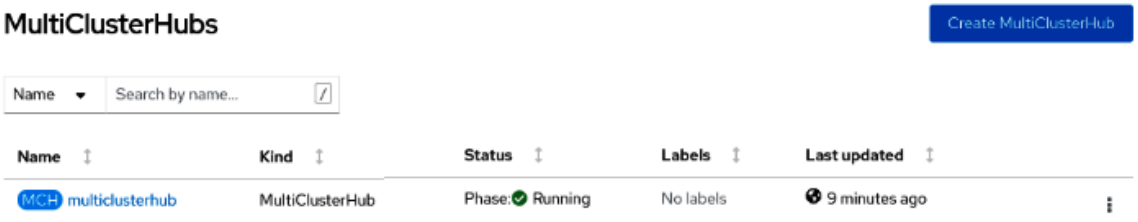
You can find additional installation guidance in the install documentation.

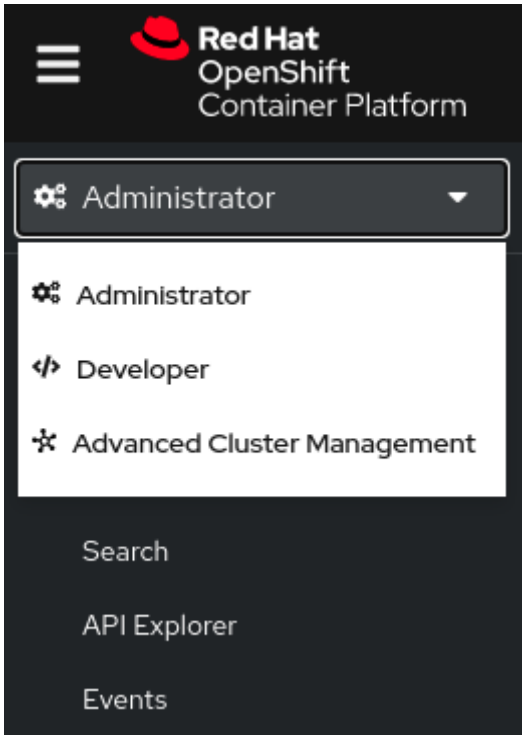

Install Operator
Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.
Update channel *
release-2.3
release-2.4
release-2.5
Installation mode *
All namespaces on the cluster (default)
This mode is not supported by this Operator
A specific namespace on the cluster
Operator will be available in a single Namespace only.
Installed Namespace *
Operator recommended Namespace: PR open-cluster-management
Namespace creation
Namespace open-cluster-management does not exist and will be created.
Select a Namespace
Update approval *
Automatic
Manual
Install
Cancel
Advanced Cluster Management for Kubernetes
provided by Red Hat
Provided APIs
MCH MultiClusterHub Required
MultiClusterHub defines the configuration for an instance of the MultiCluster Hub
S App Subscription
Subscribe resources from a channel according to its package filters
C Channel
Represent a helm chart repository
HR Helm Release
Represent a helm chart selected by the subscription, for internal use only.
D Deployable
Contain a k8s resource template for deployment, for internal use only.
PR Placement Rule
Placement Rules to determine which mangaged clusters will be deployed by multicluster applications.
MCO MultiClusterObservability
GOC GitOps Cluster

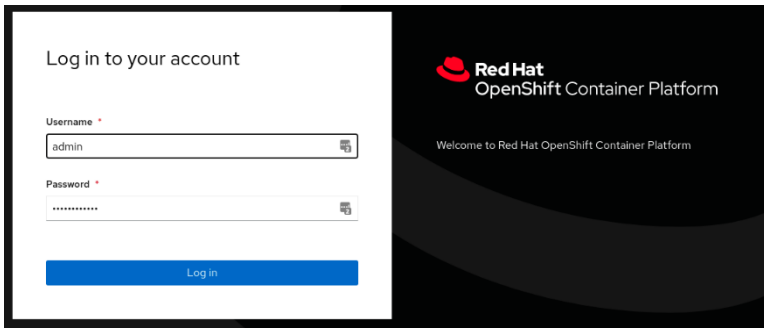

Advanced Cluster Management for Kubernetes
2.5.0 provided by Red Hat
Installed operator - operand required
The Operator has installed successfully. Create the required custom resource to be able to use this Operator.
MCH MultiClusterHub Required
Advanced provisioning and management of OpenShift and Kubernetes clusters
Create MultiClusterHub
View installed Operators in Namespace open-cluster-management

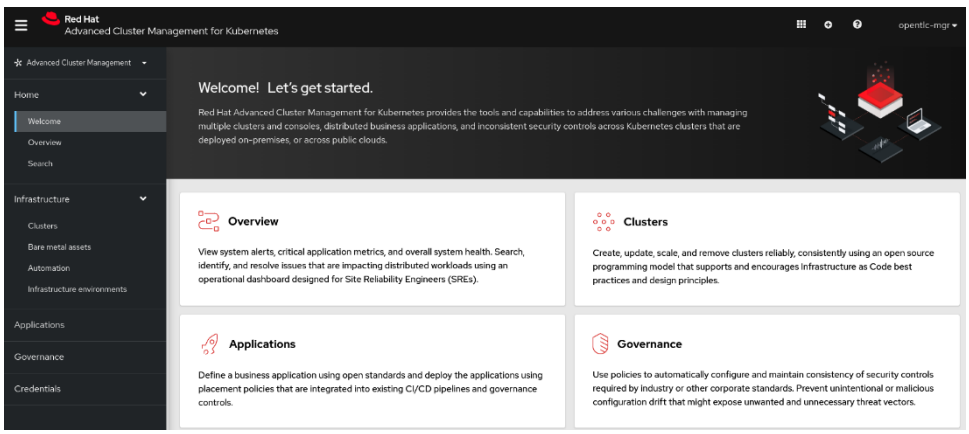

Create MultiClusterHub
Create by completing the form. Default values may be provided by the Operator authors.
Configure via: Form view YAML view
Note: Some fields may not be represented in this form view. Please select "YAML view" for full control.
Name *
multiclusterhub
Labels
app=frontend
Tolerations
Tolerations causes all components to tolerate any taints.
Advanced configuration
Create
Cancel
MultiClusterHub
provided by Red Hat
MultiClusterHub defines the configuration for an instance of the MultiCluster Hub

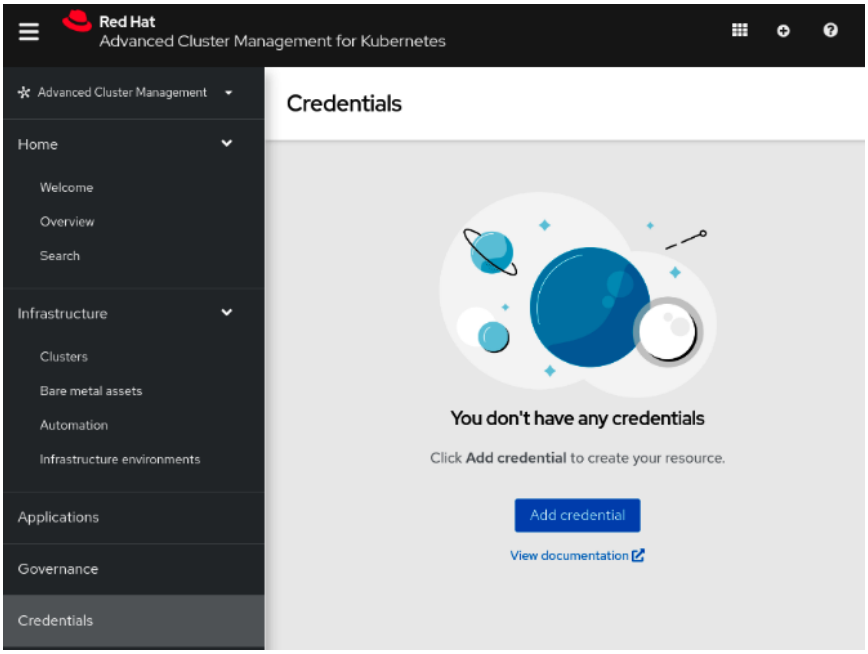

MultiClusterHubs
Create MultiClusterHub
Name
Search by name...
Name
Kind
Status
Labels
Last updated
MCH multiclusterhub
MultiClusterHub
Phase: Installing
No labels
Just now

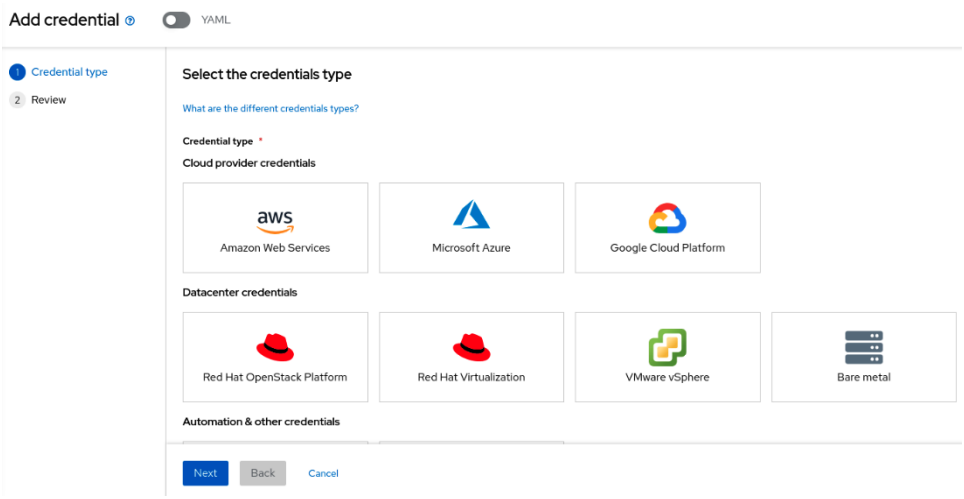

MultiClusterHubs
Create MultiClusterHub
Name
Search by name...
Name
Kind
Status
Labels
Last updated
MCH multiclusterhub
MultiClusterHub
Phase: Running
No labels
9 minutes ago

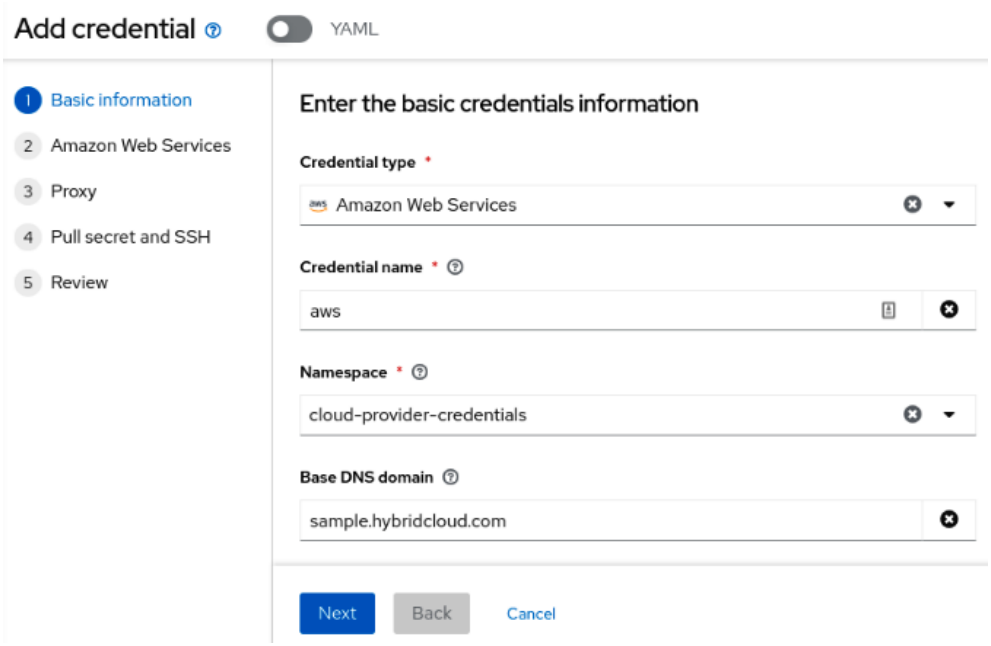

Red Hat
OpenShift
Container Platform
Administrator
Administrator
Developer
Advanced Cluster Management
Search
API Explorer
Events

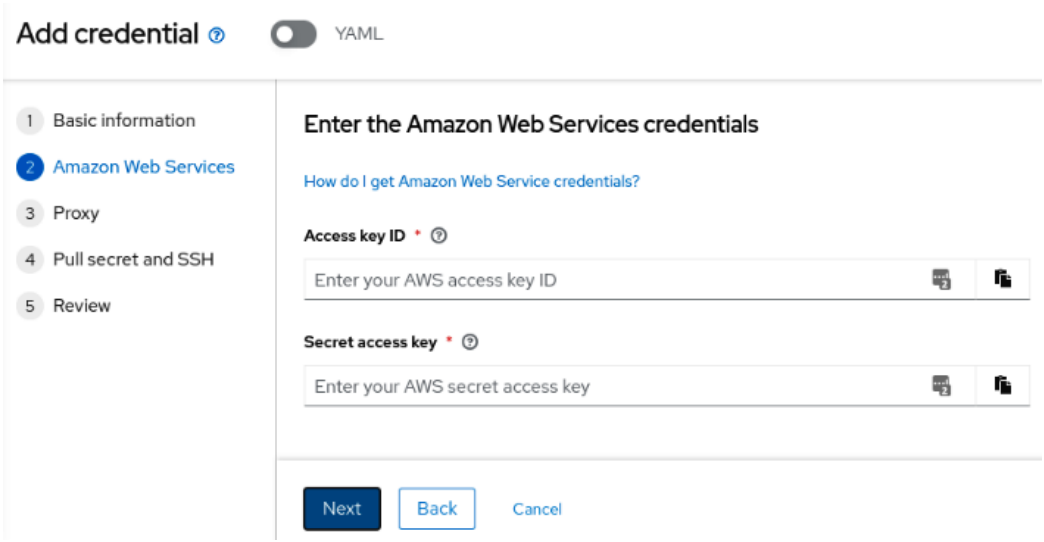

Log in to your account
Username *
admin
Password *
Log in
Red Hat
OpenShift Container Platform
Welcome to Red Hat OpenShift Container Platform

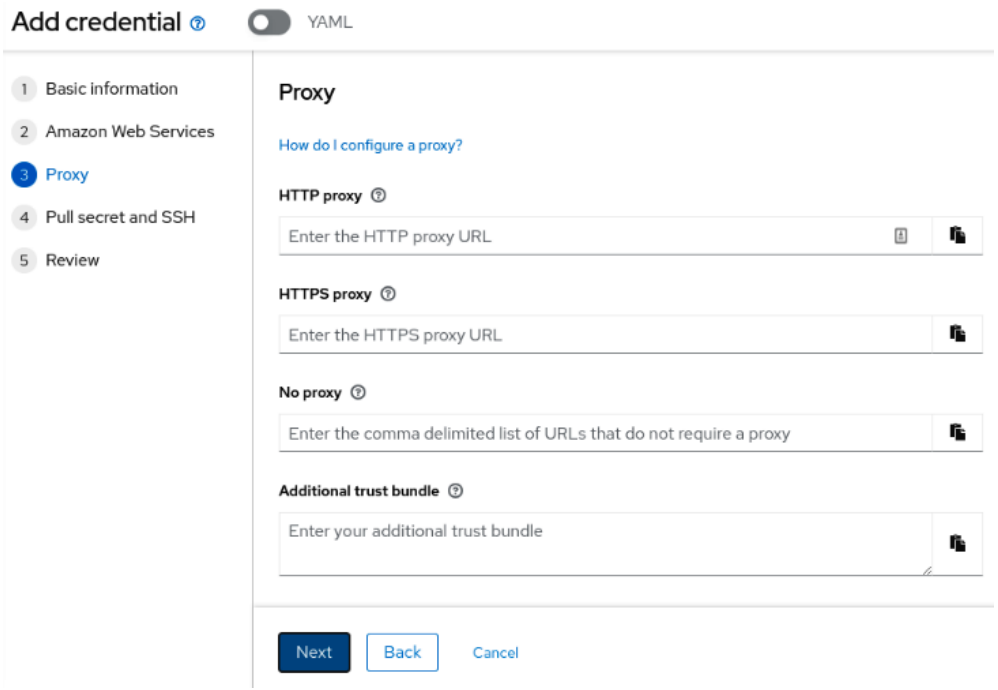

Red Hat
Advanced Cluster Management for Kubernetes
opentlc-mgr
Advanced Cluster Management
Home
Welcome
Overview
Search
Infrastructure
Clusters
Bare metal assets
Automation
Infrastructure environments
Applications
Governance
Credentials
Welcome! Let's get started.
Red Hat Advanced Cluster Management for Kubernetes provides the tools and capabilities to address various challenges with managing multiple clusters and consoles, distributed business applications, and inconsistent security controls across Kubernetes clusters that are deployed on-premises, or across public clouds.
Overview
View system alerts, critical application metrics, and overall system health. Search, identify, and resolve issues that are impacting distributed workloads using an operational dashboard designed for Site Reliability Engineers (SREs).
Clusters
Create, update, scale, and remove clusters reliably, consistently using an open source programming model that supports and encourages Infrastructure as Code best practices and design principles.
Applications
Define a business application using open standards and deploy the applications using placement policies that are integrated into existing CI/CD pipelines and governance controls.
Governance
Use policies to automatically configure and maintain consistency of security controls required by industry or other corporate standards. Prevent unintentional or malicious configuration drift that might expose unwanted and unnecessary threat vectors.

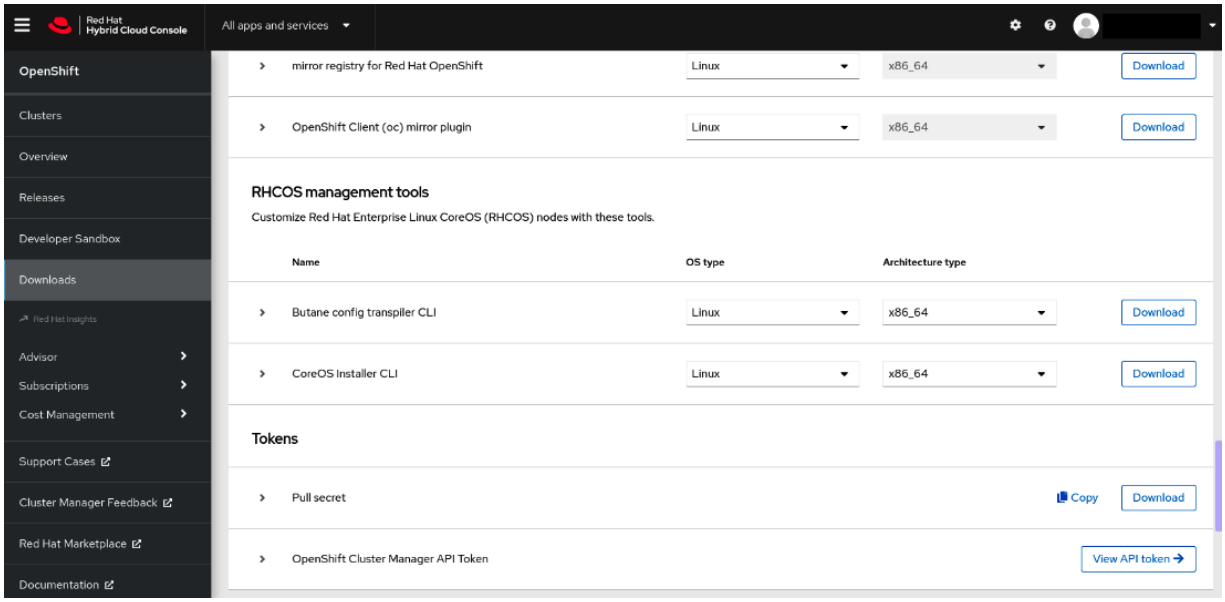

Red Hat
Advanced Cluster Management for Kubernetes
Advanced Cluster Management
Home
Welcome
Overview
Search
Infrastructure
Clusters
Bare metal assets
Automation
Infrastructure environments
Applications
Governance
Credentials
Credentials
You don't have any credentials
Click Add credential to create your resource.
Add credential
View documentation

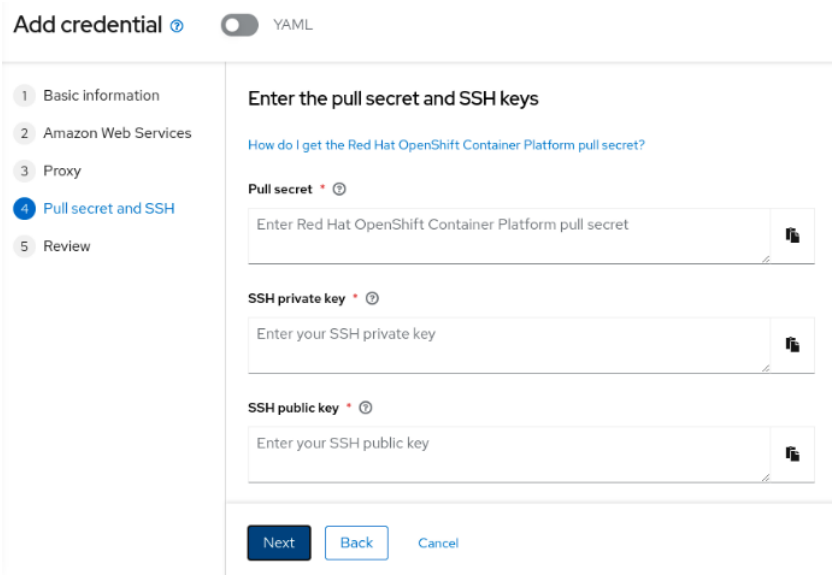

Add credential
YAML
1 Credential type
2 Review
Select the credentials type
What are the different credentials types?
Credential type *
Cloud provider credentials
aws
Amazon Web Services
Microsoft Azure
Google Cloud Platform
Datacenter credentials
Red Hat OpenStack Platform
Red Hat Virtualization
VMware vSphere
Bare metal
Automation & other credentials
Next
Back
Cancel


Add credential
YAML
1 Basic information
2 Amazon Web Services
3 Proxy
4 Pull secret and SSH
5 Review
Enter the basic credentials information
Credential type *
Amazon Web Services
Credential name *
aws
Namespace *
cloud-provider-credentials
Base DNS domain
sample.hybridcloud.com
Next
Back
Cancel

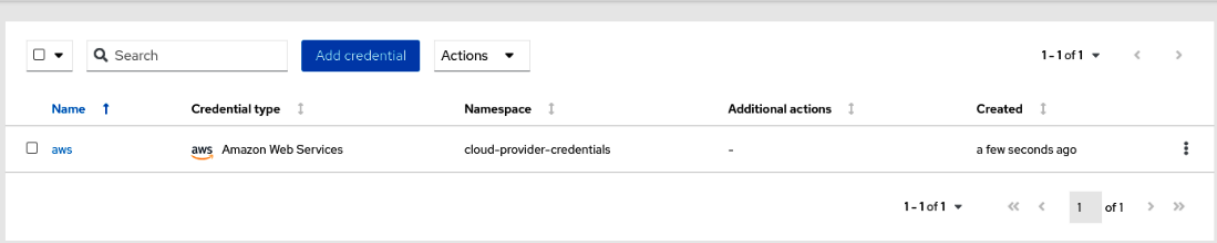

Add credential
YAML
1 Basic information
2 Amazon Web Services
3 Proxy
4 Pull secret and SSH
5 Review
Enter the Amazon Web Services credentials
How do I get Amazon Web Service credentials?
Access key ID *
Enter your AWS access key ID
Secret access key *
Enter your AWS secret access key
Next
Back
Cancel

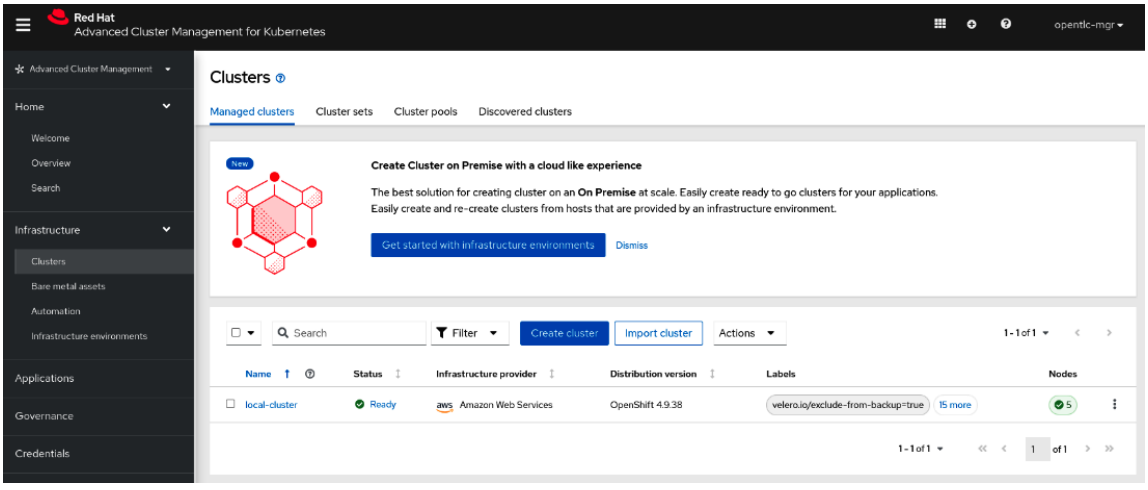

Add credential
YAML
1 Basic information
2 Amazon Web Services
3 Proxy
4 Pull secret and SSH
5 Review
Proxy
How do I configure a proxy?
HTTP proxy
Enter the HTTP proxy URL
HTTPS proxy
Enter the HTTPS proxy URL
No proxy
Enter the comma delimited list of URLs that do not require a proxy
Additional trust bundle
Enter your additional trust bundle
Next
Back
Cancel

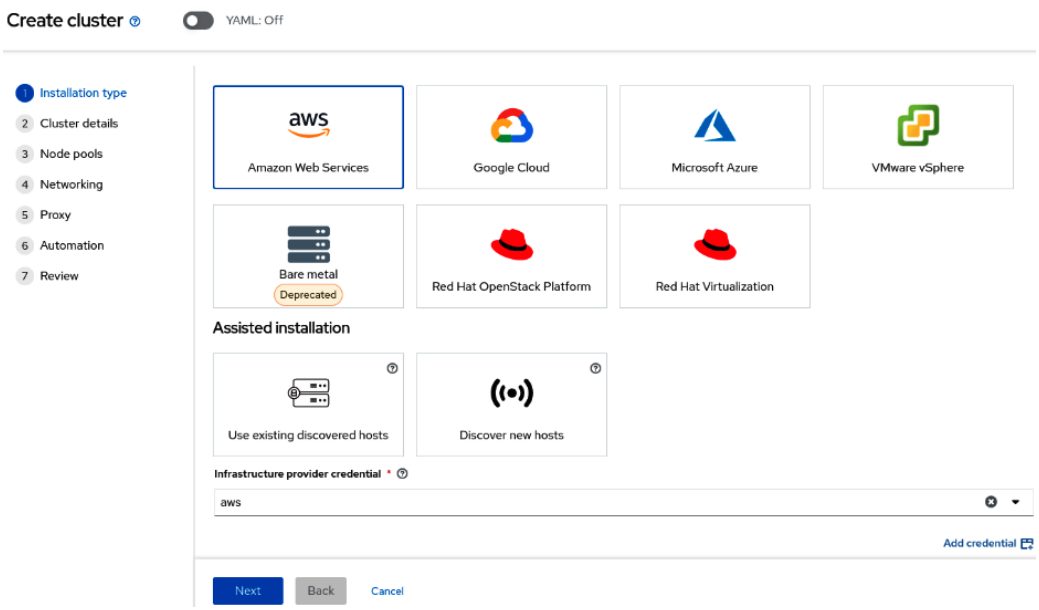

Red Hat Hybrid Cloud Console
All apps and services
OpenShift
Clusters
Overview
Releases
Developer Sandbox
Downloads
Advisor
Subscriptions
Cost Management
Support Cases
Cluster Manager Feedback
Red Hat Marketplace
Documentation
mirror registry for Red Hat OpenShift
Linux
x86_64
Download
OpenShift Client (oc) mirror plugin
Linux
x86_64
Download
RHCOS management tools
Customize Red Hat Enterprise Linux CoreOS (RHCOS) nodes with these tools.
Name
OS type
Architecture type
Butane config transpiler CLI
Linux
x86_64
Download
CoreOS Installer CLI
Linux
x86_64
Download
Tokens
Pull secret
Copy
Download
OpenShift Cluster Manager API Token
View API token

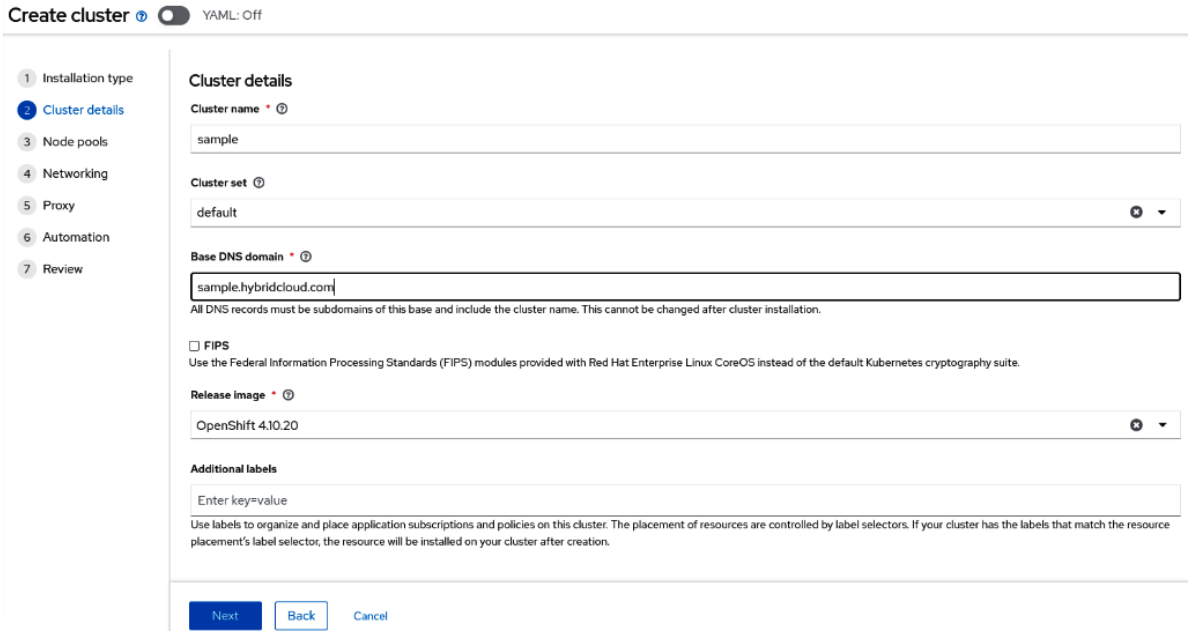


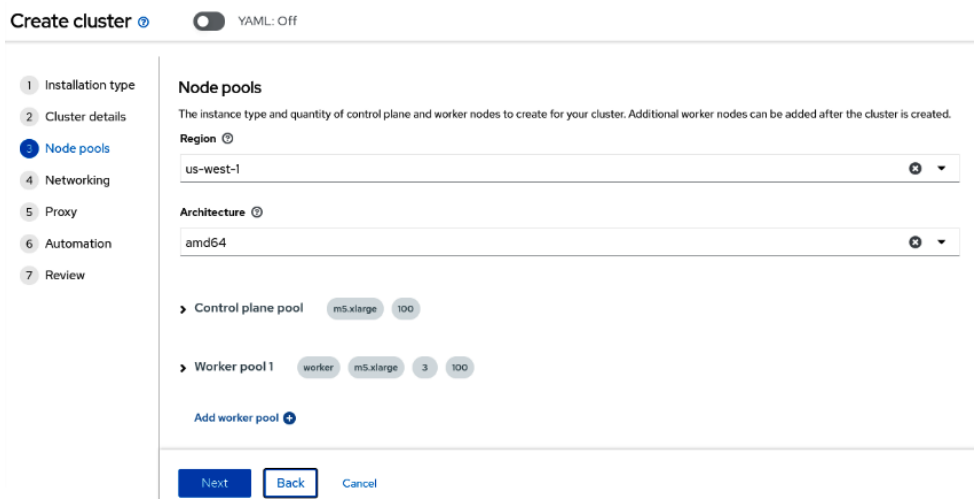
Credentials

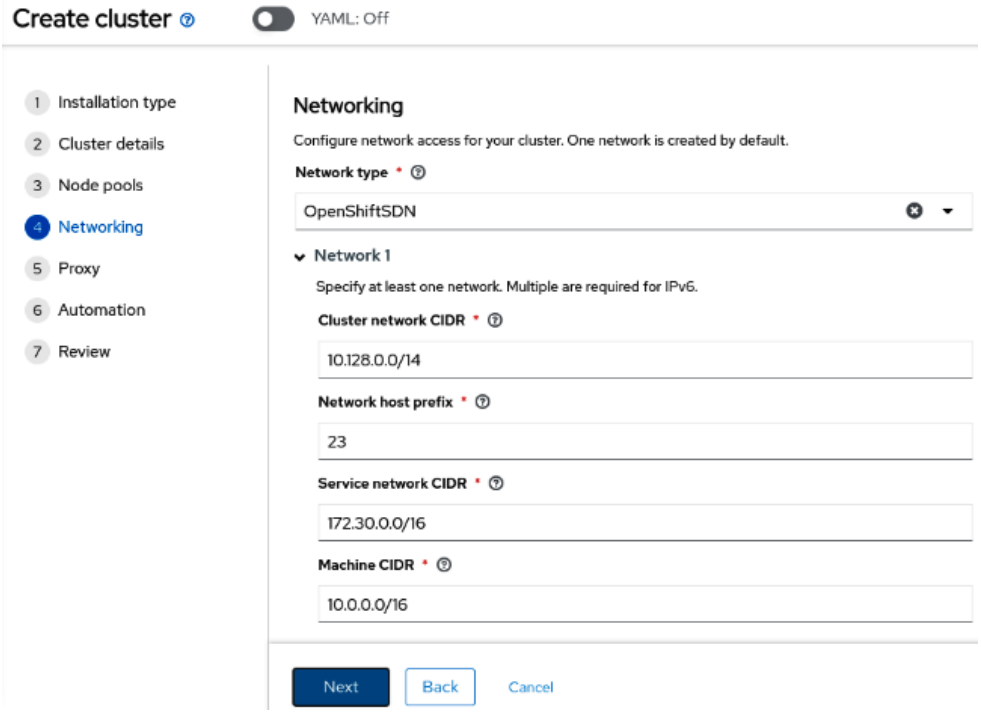


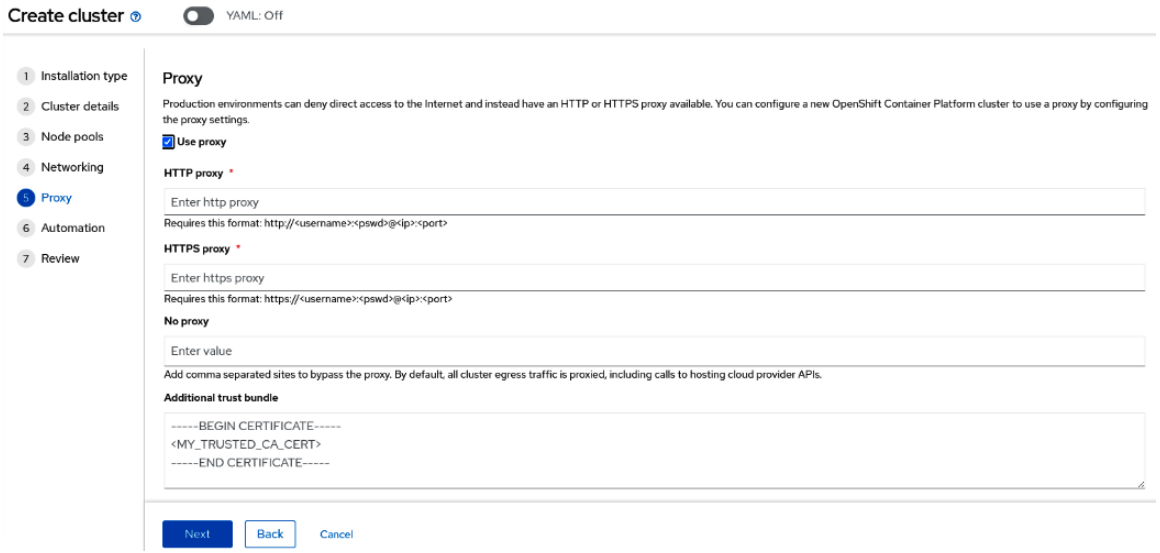


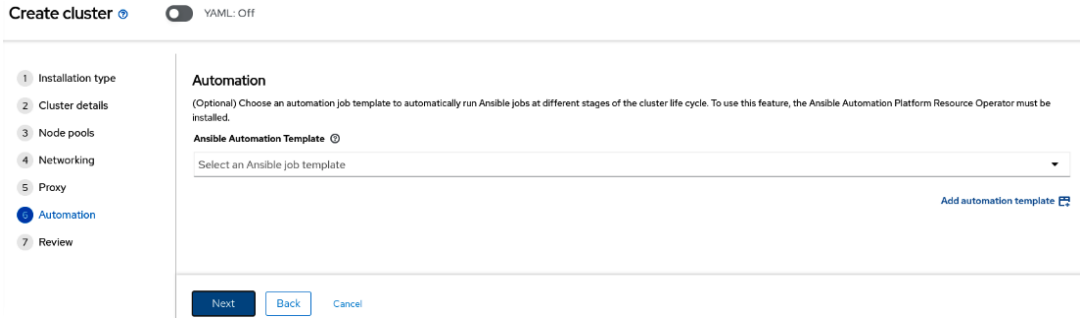

Create cluster
YAML: Off
1 Installation type
2 Cluster details
3 Node pools
4 Networking
5 Proxy
6 Automation
7 Review
Amazon Web Services
Google Cloud
Microsoft Azure
VMware vSphere
Bare metal
Deprecated
Red Hat OpenStack Platform
Red Hat Virtualization
Assisted installation
Use existing discovered hosts
Discover new hosts
Infrastructure provider credential *
aws
Add credential
Next
Back
Cancel

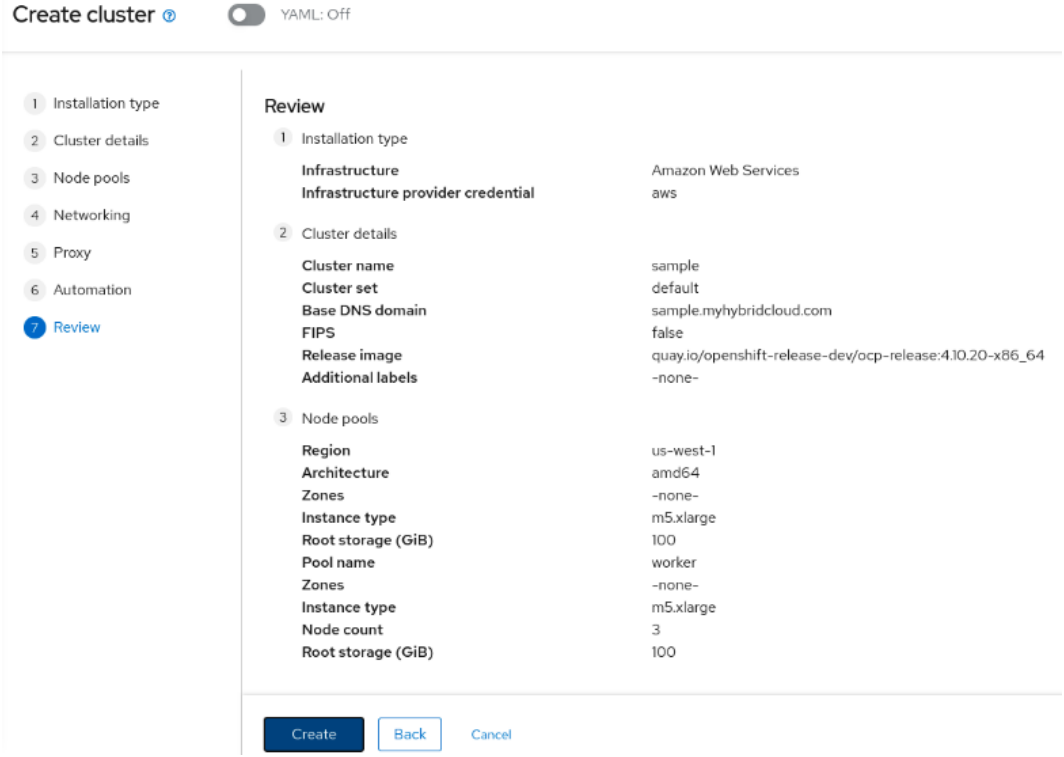

Create cluster
YAML: Off
1 Installation type
2 Cluster details
3 Node pools
4 Networking
5 Proxy
6 Automation
7 Review
Cluster details
Cluster name *
sample
Cluster set
default
Base DNS domain *
sample.hybridcloud.com
All DNS records must be subdomains of this base and include the cluster name. This cannot be changed after cluster installation.
FIPS
Use the Federal Information Processing Standards (FIPS) modules provided with Red Hat Enterprise Linux CoreOS instead of the default Kubernetes cryptography suite.
Release image *
OpenShift 4.10.20
Additional labels
Enter key=value
Use labels to organize and place application subscriptions and policies on this cluster. The placement of resources are controlled by label selectors. If your cluster has the labels that match the resource placement's label selector, the resource will be installed on your cluster after creation.
Next
Back
Cancel

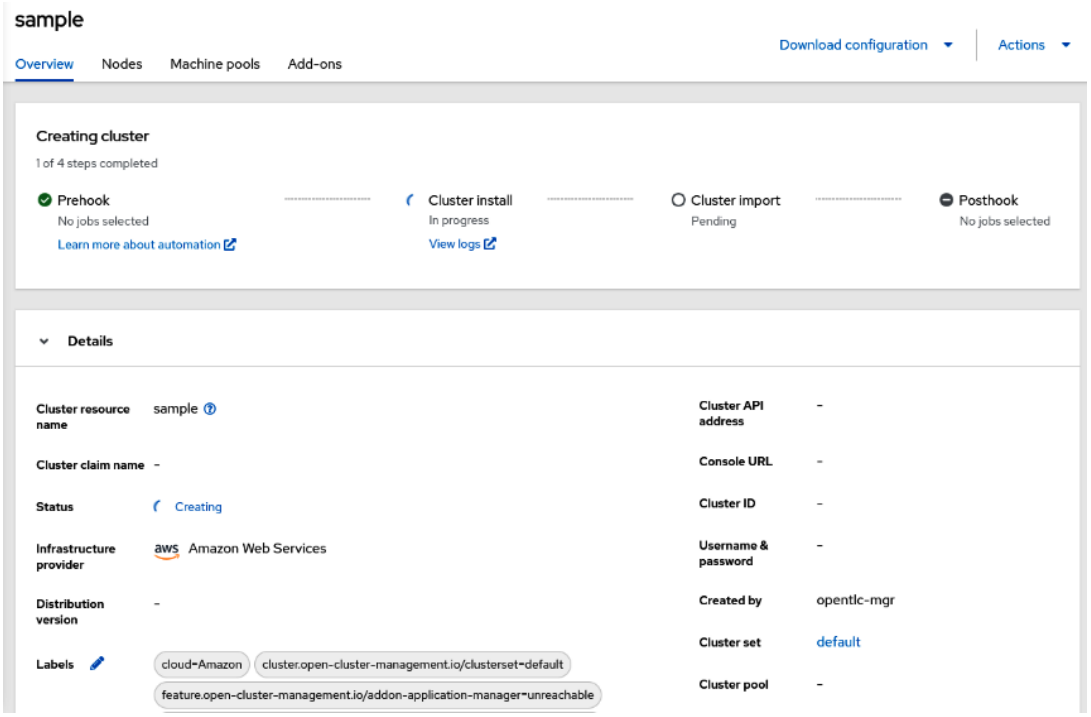

Create cluster
YAML: Off
1 Installation type
2 Cluster details
3 Node pools
4 Networking
5 Proxy
6 Automation
7 Review
Node pools
The instance type and quantity of control plane and worker nodes to create for your cluster. Additional worker nodes can be added after the cluster is created.
Region
us-west-1
Architecture
amd64
Control plane pool
m5.xlarge
100
Worker pool 1
worker
m5.xlarge
3
100
Add worker pool
Next
Back
Cancel


Create cluster
YAML: Off
1 Installation type
2 Cluster details
3 Node pools
4 Networking
5 Proxy
6 Automation
7 Review
Networking
Configure network access for your cluster. One network is created by default.
Network type *
OpenShiftSDN
Network 1
Specify at least one network. Multiple are required for IPv6.
Cluster network CIDR *
10.128.0.0/14
Network host prefix *
23
Service network CIDR *
172.30.0.0/16
Machine CIDR *
10.0.0.0/16
Next
Back
Cancel


Create cluster
YAML: Off
1 Installation type
2 Cluster details
3 Node pools
4 Networking
5 Proxy
6 Automation
7 Review
Proxy
Production environments can deny direct access to the Internet and instead have an HTTP or HTTPS proxy available. You can configure a new OpenShift Container Platform cluster to use a proxy by configuring the proxy settings.
Use proxy
HTTP proxy *
Enter http proxy
Requires this format: http://<username>:<pswd>@<ip>:<port>
HTTPS proxy *
Enter https proxy
Requires this format: https://<username>:<pswd>@<ip>:<port>
No proxy
Enter value
Add comma separated sites to bypass the proxy. By default, all cluster egress traffic is proxied, including calls to hosting cloud provider APIs.
Additional trust bundle
-----BEGIN CERTIFICATE-----
<MY_TRUSTED_CA_CERT>
-----END CERTIFICATE-----
Next
Back
Cancel


Create cluster
YAML: Off
1 Installation type
2 Cluster details
3 Node pools
4 Networking
5 Proxy
6 Automation
7 Review
Automation
(Optional) Choose an automation job template to automatically run Ansible jobs at different stages of the cluster life cycle. To use this feature, the Ansible Automation Platform Resource Operator must be installed.
Ansible Automation Template
Select an Ansible job template
Add automation template
Next
Back
Cancel


Create cluster
YAML: Off
1 Installation type
2 Cluster details
3 Node pools
4 Networking
5 Proxy
6 Automation
7 Review
Review
1 Installation type
Infrastructure Amazon Web Services
Infrastructure provider credential aws
2 Cluster details
Cluster name sample
Cluster set default
Base DNS domain sample.myhybridcloud.com
FIPS false
Release image quay.io/openshift-release-dev/ocp-release:4.10.20-x86_64
Additional labels -none-
3 Node pools
Region us-west-1
Architecture amd64
Zones -none-
Instance type m5.xlarge
Root storage (GiB) 100
Pool name worker
Zones -none-
Instance type m5.xlarge
Node count 3
Root storage (GiB) 100
Create
Back
Cancel


sample
Download configuration
Actions
Overview
Nodes
Machine pools
Add-ons
Creating cluster
1 of 4 steps completed
Prehook
No jobs selected
Learn more about automation
Cluster install
In progress
View logs
Cluster import
Pending
Posthook
No jobs selected
Details
Cluster resource name
sample
Cluster claim name
-
Status
Creating
Infrastructure provider
Amazon Web Services
Distribution version
-
Labels
cloud=Amazon
cluster.open-cluster-management.io/clusterset=default
feature.open-cluster-management.io/addon-application-manager=unreachable
Cluster API address
-
Console URL
-
Cluster ID
-
Username & password
-
Created by
opentlc-mgr
Cluster set
default
Cluster pool
-

sample

Overview | Nodes | Machine pools | Add-ons

Cluster resource name	sample
Cluster claim name	-
Status	Ready
Infrastructure provider	aws Amazon Web Services
Distribution version	OpenShift 4.10.20
Channel	stable-4.10
Labels	cloud=Amazon cluster.open-cluster-management.io/clusterset=default clusterID=e974c5ae-3747-46bd-ac9a-82d51fbbdb1a feature.open-cluster-management.io/addon-application-manager=available feature.open-cluster-management.io/addon-cert-policy-controller=available feature.open-cluster-management.io/addon-config-policy-controller=available feature.open-cluster-management.io/addon-governance-policy-framework=available feature.open-cluster-management.io/addon-iam-policy-controller=available feature.open-cluster-management.io/addon-search-collector=available feature.open-cluster-management.io/addon-work-manager=available name=sample openshiftVersion=4.10.20 region=us-east-1 vendor=OpenShift

Edit labels

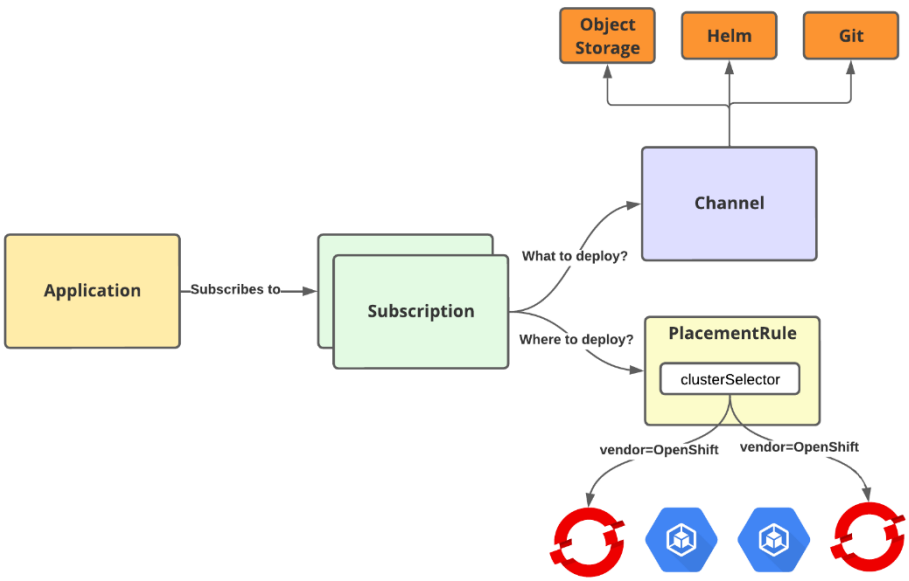
Labels help you organize and select resources. Adding labels allows you to query for objects by using the labels. Selecting labels during policy and application creation allows you to distribute your resources to different clusters that share common labels.

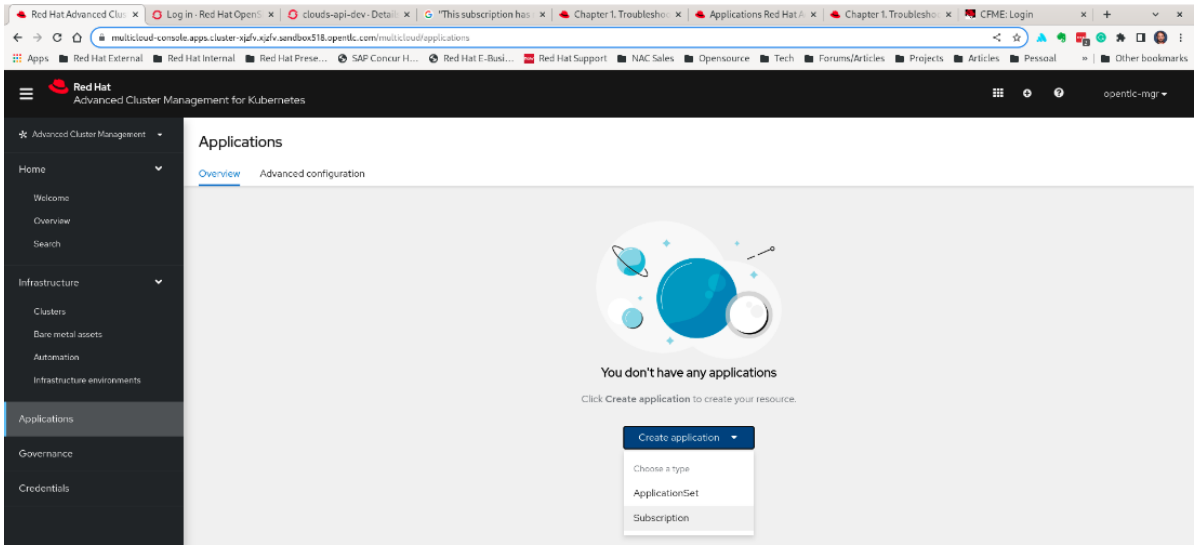
sample labels

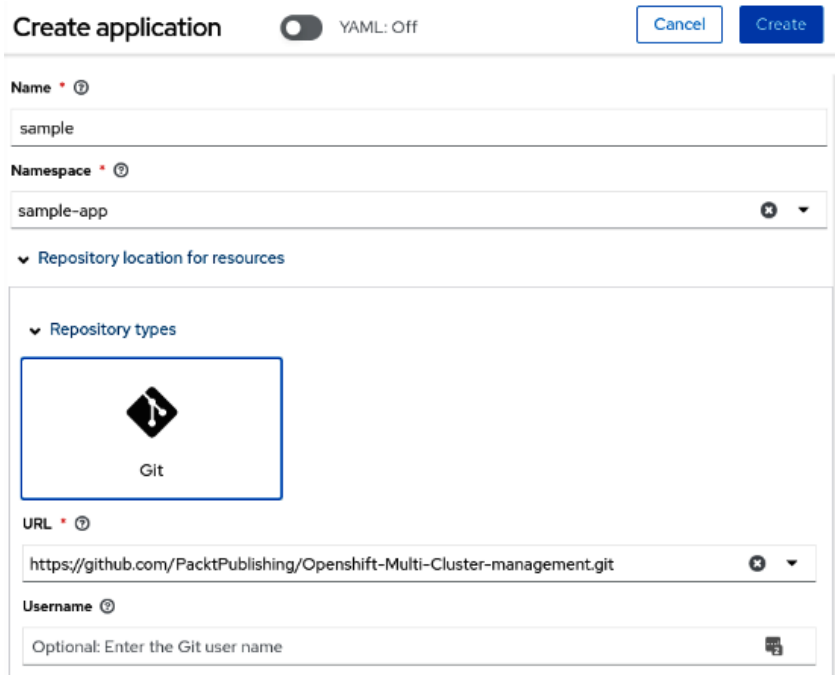
cloud=Amazon ×
cluster.open-cluster-management.io/clusterset=default ×
clusterID=e974c5ae-3747-46bd-ac9a-82d51fbbdb1a ×
feature.open-cluster-management.io/addon-application-manager=available ×
feature.open-cluster-management.io/addon-cert-policy-controller=available ×
feature.open-cluster-management.io/addon-config-policy-controller=available ×
feature.open-cluster-management.io/addon-governance-policy-framework=available ×
feature.open-cluster-management.io/addon-iam-policy-controller=available ×
feature.open-cluster-management.io/addon-search-collector=available ×
feature.open-cluster-management.io/addon-work-manager=available ×
name=sample ×
openshiftVersion=4.10.20 ×
region=us-east-1 ×
vendor=OpenShift ×

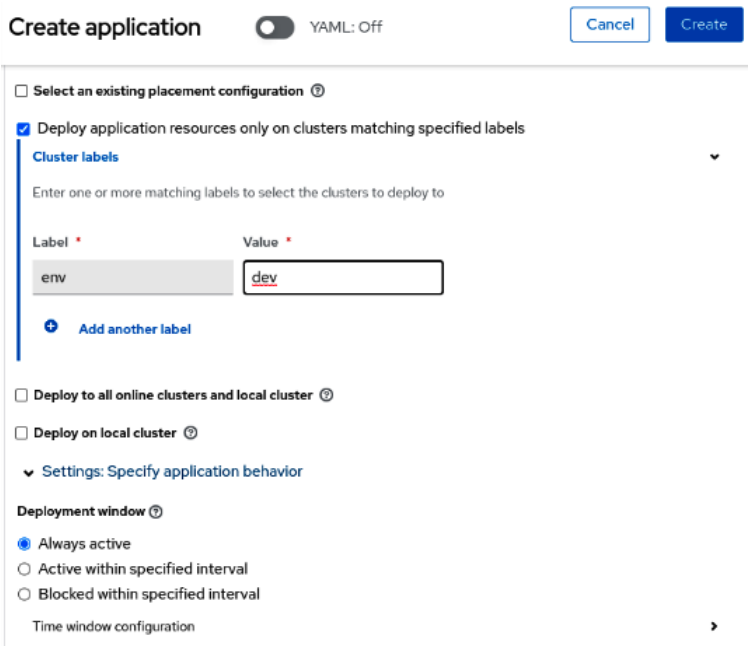
env=dev

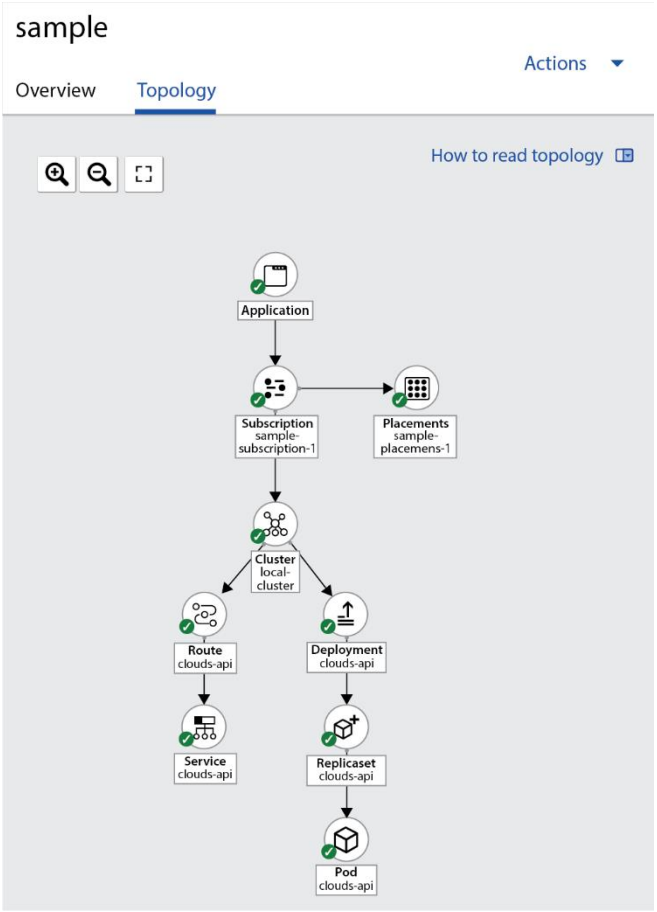
Save Cancel




Red Hat
Advanced Cluster Management for Kubernetes
opentlc-mgr
Advanced Cluster Management
Home
Welcome
Overview
Search
Infrastructure
Clusters
Bare metal assets
Automation
Infrastructure environments
Applications
Governance
Credentials
Applications
Overview
Advanced configuration
You don't have any applications
Click Create application to create your resource.
Create application
Choose a type
ApplicationSet
Subscription


Create application
YAML: Off
Cancel
Create
Name *
sample
Namespace *
sample-app
Repository location for resources
Repository types
Git
URL *
https://github.com/PacktPublishing/Openshift-Multi-Cluster-management.git
Username
Optional: Enter the Git user name


Create application
YAML: Off
Cancel
Create
Select an existing placement configuration
Deploy application resources only on clusters matching specified labels
Cluster labels
Enter one or more matching labels to select the clusters to deploy to
Label *
Value *
env
dev
Add another label
Deploy to all online clusters and local cluster
Deploy on local cluster
Settings: Specify application behavior
Deployment window
Always active
Active within specified interval
Blocked within specified interval
Time window configuration


sample
Actions
Overview
Topology
How to read topology
Application
Subscription
sample-
subscription-1
Placements
sample-
placemens-1
Cluster
local-
cluster
Route
clouds-api
Deployment
clouds-api
Service
clouds-api
Replicaset
clouds-api
Pod
clouds-api

Manage resource assignments

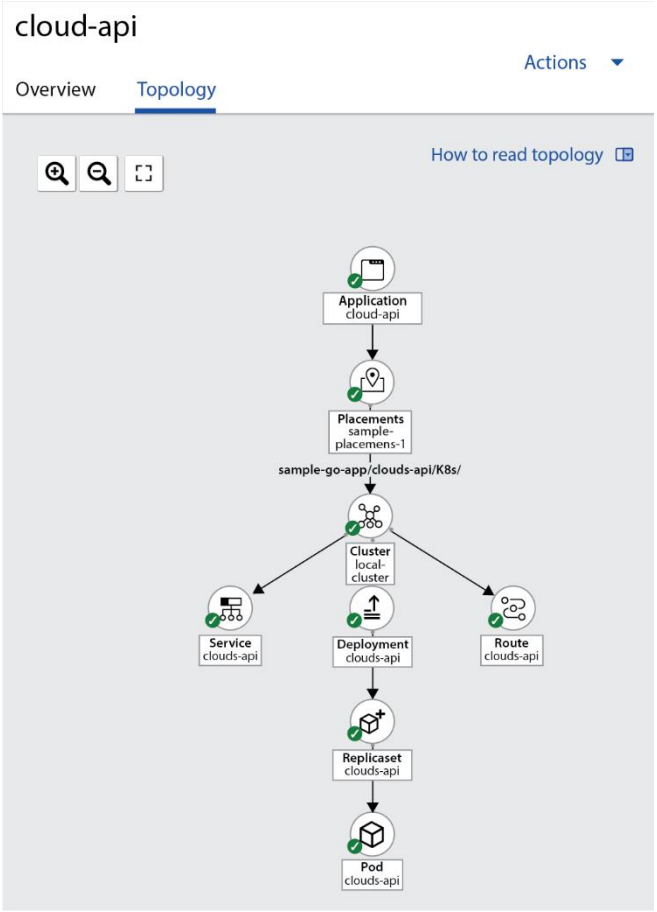
Select resources to toggle their assignments to the cluster set

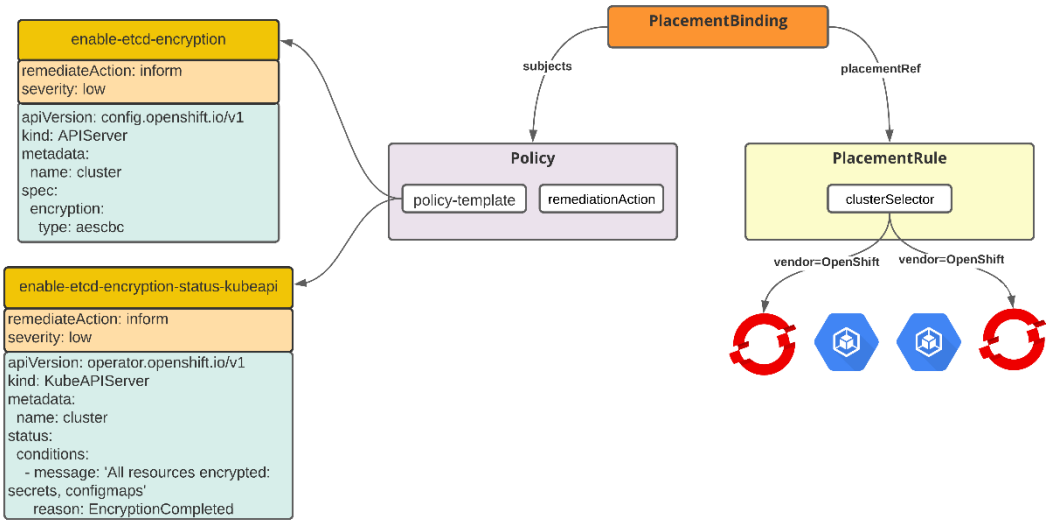
Resources can be added, removed, and transferred from other cluster sets (if you have permissions to remove from them from their assigned set).

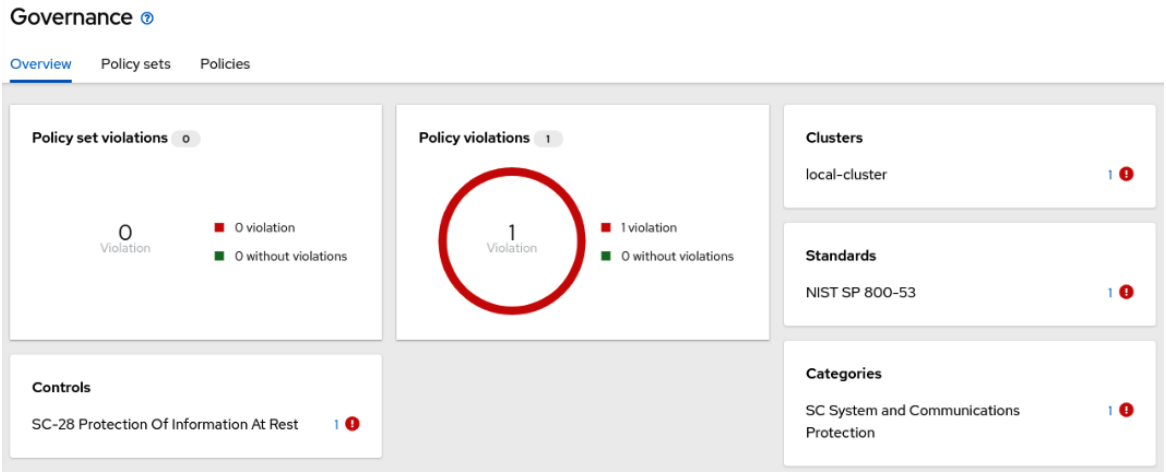
Important: assigning a resource to the cluster set will give all cluster set users permissions to the resource's namespace.

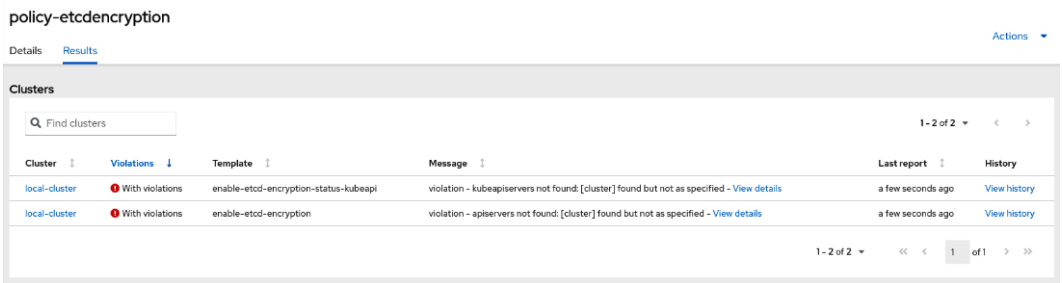
2 selected | Search

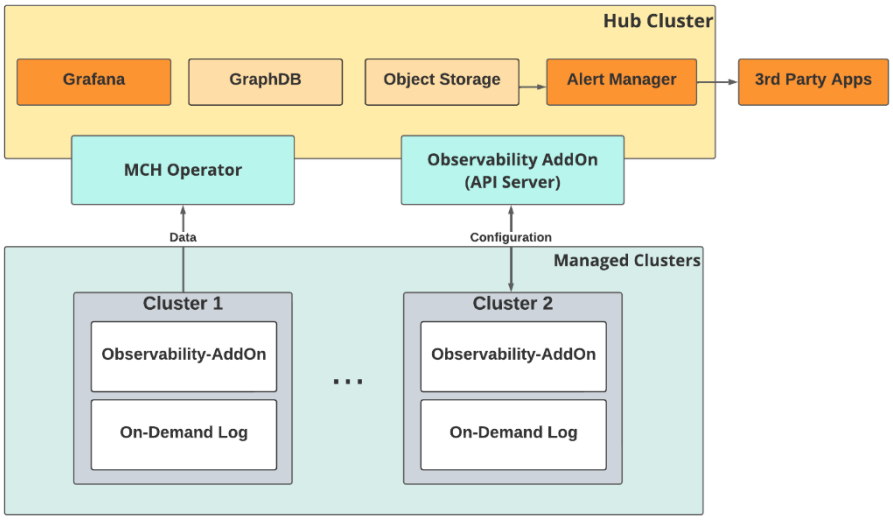
Name	Kind	Current cluster set
local-cluster	ManagedCluster	default
sample	ManagedCluster	default

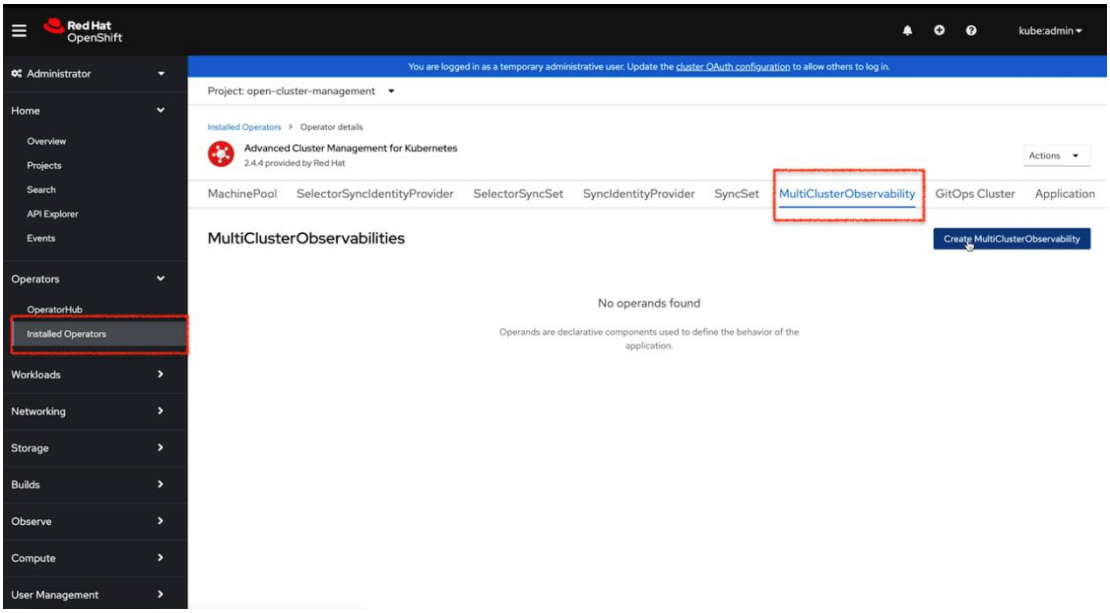


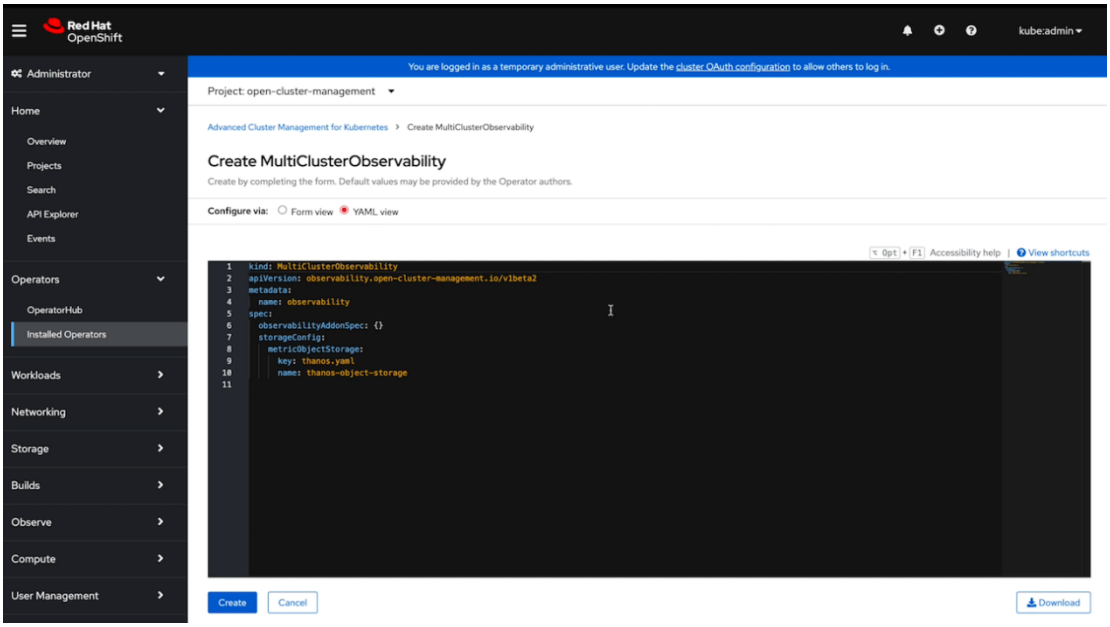

PlacementBinding
subjects
placementRef
enable-etcd-encryption
remediateAction: inform
severity: low
apiVersion: config.openshift.io/v1
kind: APIServer
metadata:
name: cluster
spec:
encryption:
type: aescbc
Policy
policy-template
remediationAction
PlacementRule
clusterSelector
vendor=OpenShift
vendor=OpenShift
enable-etcd-encryption-status-kubeapi
remediateAction: inform
severity: low
apiVersion: operator.openshift.io/v1
kind: KubeAPIServer
metadata:
name: cluster
status:
conditions:
- message: 'All resources encrypted:
secrets, configmaps'
reason: EncryptionCompleted

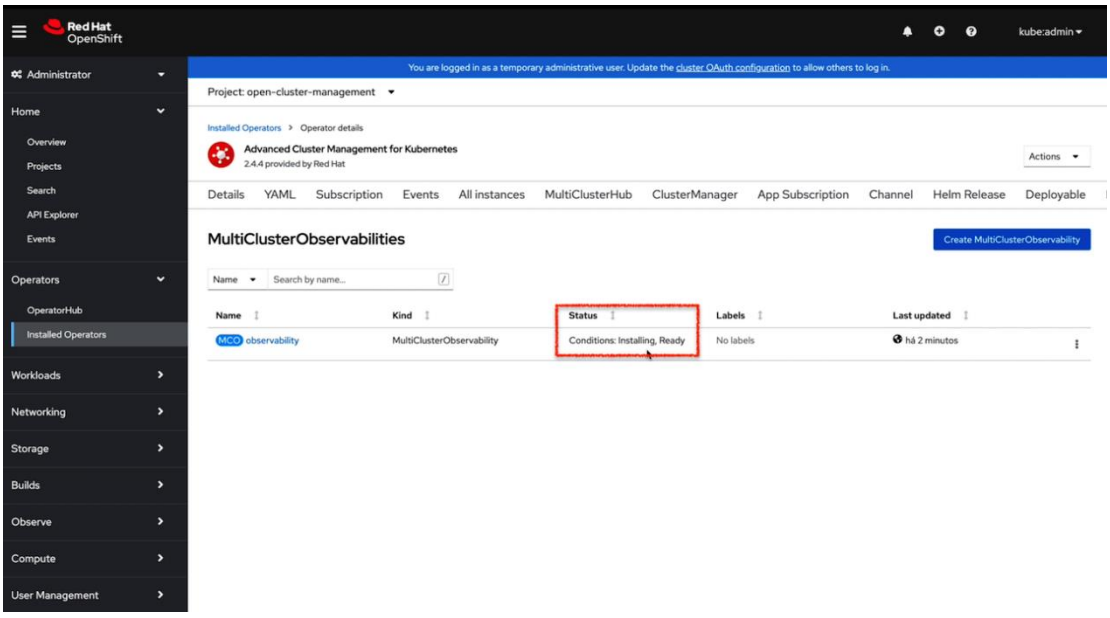

Governance
Overview
Policy sets
Policies
Policy set violations 0
0
Violation
0 violation
0 without violations
Policy violations 1
1
Violation
1 violation
0 without violations
Clusters
local-cluster 1
Standards
NIST SP 800-53 1
Controls
SC-28 Protection Of Information At Rest 1
Categories
SC System and Communications Protection 1

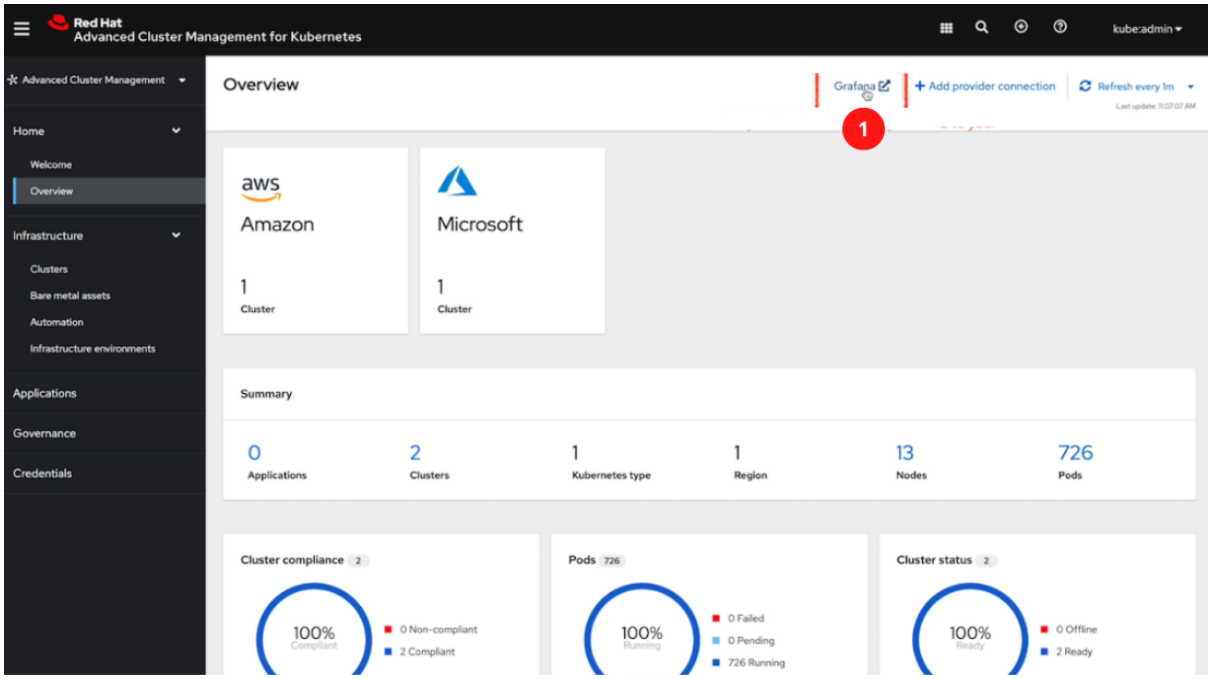

policy-etcdencryption
Details
Results
Actions
Clusters
Find clusters
1 - 2 of 2
Cluster
Violations
Template
Message
Last report
History
local-cluster
With violations
enable-etcd-encryption-status-kubeapi
violation - kubeapiservers not found: [cluster] found but not as specified - View details
a few seconds ago
View history
local-cluster
With violations
enable-etcd-encryption
violation - apiservers not found: [cluster] found but not as specified - View details
a few seconds ago
View history
1 - 2 of 2
1
of 1

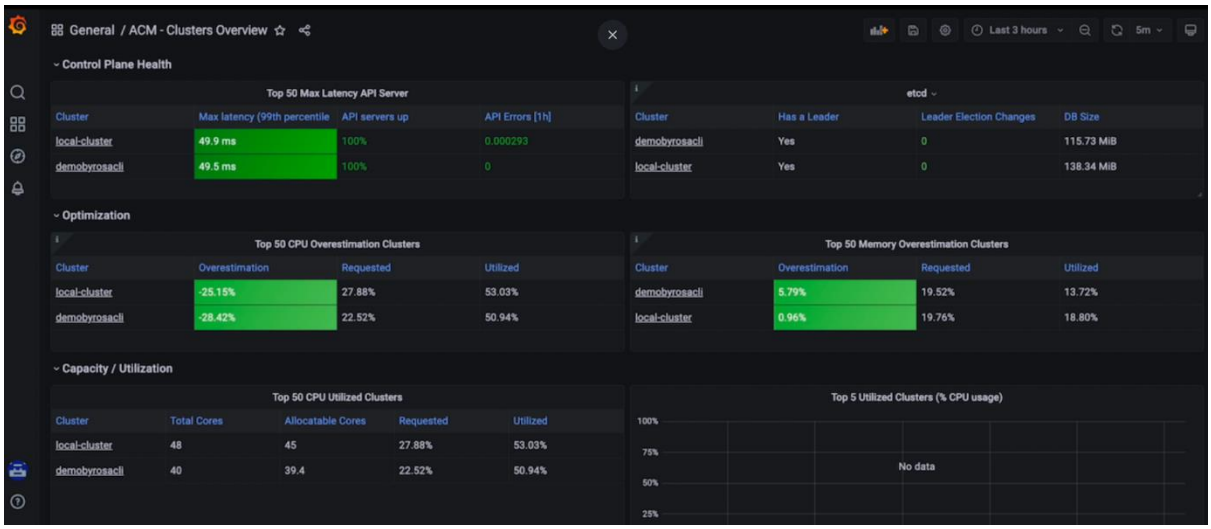

Hub Cluster
Grafana
GraphDB
Object Storage
Alert Manager
3rd Party Apps
MCH Operator
Observability AddOn
(API Server)
Data
Configuration
Managed Clusters
Cluster 1
Observability-AddOn
On-Demand Log
Cluster 2
Observability-AddOn
On-Demand Log

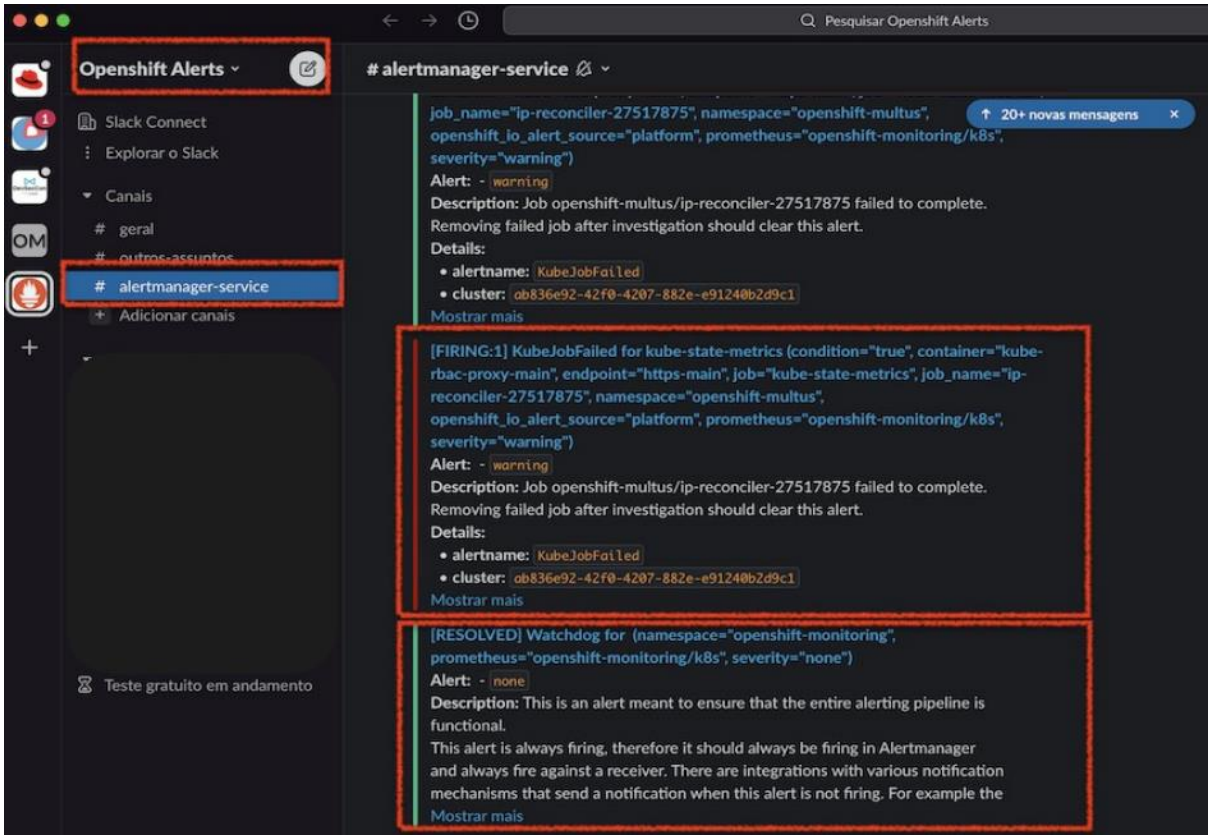

Red Hat OpenShift
kube:admin
Administrator
Home
Overview
Projects
Search
API Explorer
Events
Operators
OperatorHub
Installed Operators
Workloads
Networking
Storage
Builds
Observe
Compute
User Management
You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in.
Project: open-cluster-management
Installed Operators > Operator details
Advanced Cluster Management for Kubernetes
2.4.4 provided by Red Hat
Actions
MachinePool
SelectorSyncIdentityProvider
SelectorSyncSet
SyncIdentityProvider
SyncSet
MultiClusterObservability
GitOps Cluster
Application
MultiClusterObservabilities
Create MultiClusterObservability
No operands found
Operands are declarative components used to define the behavior of the application.


Red Hat OpenShift
kube:admin
Administrator
You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in.
Project: open-cluster-management
Home
Overview
Projects
Search
API Explorer
Events
Operators
OperatorHub
Installed Operators
Workloads
Networking
Storage
Builds
Observe
Compute
User Management
Advanced Cluster Management for Kubernetes > Create MultiClusterObservability
Create MultiClusterObservability
Create by completing the form. Default values may be provided by the Operator authors.
Configure via: Form view YAML view
Accessibility help
View shortcuts
kind: MultiClusterObservability
apiVersion: observability.open-cluster-management.io/v1beta2
metadata:
name: observability
spec:
observabilityAddonSpec: {}
storageConfig:
metricObjectStorage:
key: thanos.yaml
name: thanos-object-storage
Create
Cancel
Download

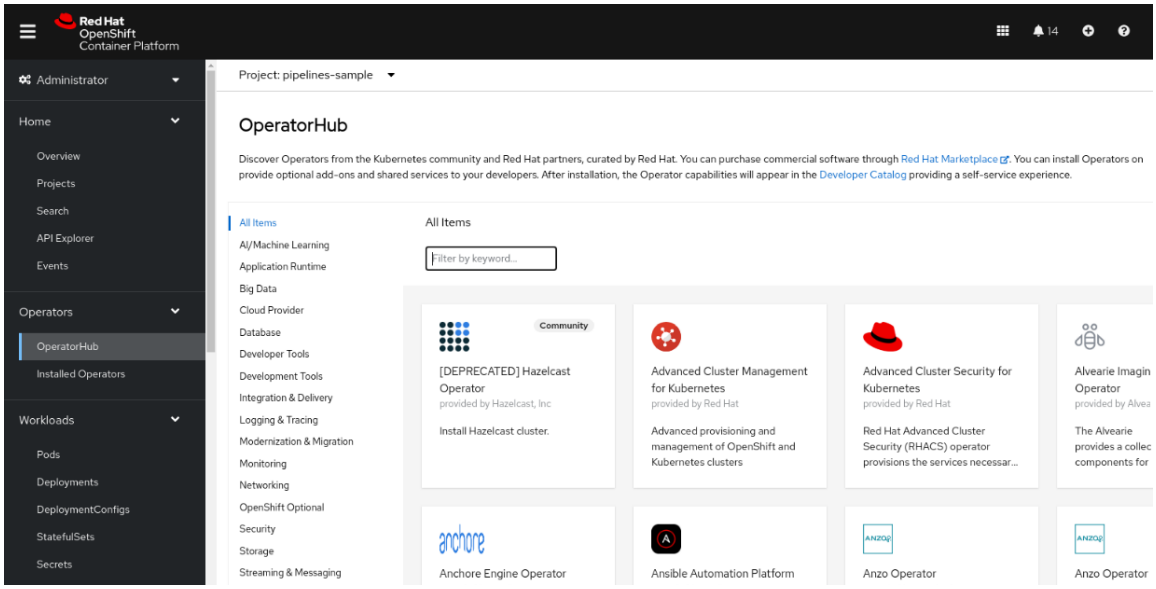

Red Hat OpenShift
kube:admin
Administrator
You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in.
Project: open-cluster-management
Home
Overview
Projects
Search
API Explorer
Events
Operators
OperatorHub
Installed Operators
Workloads
Networking
Storage
Builds
Observe
Compute
User Management
Installed Operators > Operator details
Advanced Cluster Management for Kubernetes
2.4.4 provided by Red Hat
Actions
Details YAML Subscription Events All instances MultiClusterHub ClusterManager App Subscription Channel Helm Release Deployable
MultiClusterObservabilities
Create MultiClusterObservability
Name
Search by name...
Name
Kind
Status
Labels
Last updated
MCO observability
MultiClusterObservability
Conditions: Installing, Ready
No labels
há 2 minutos

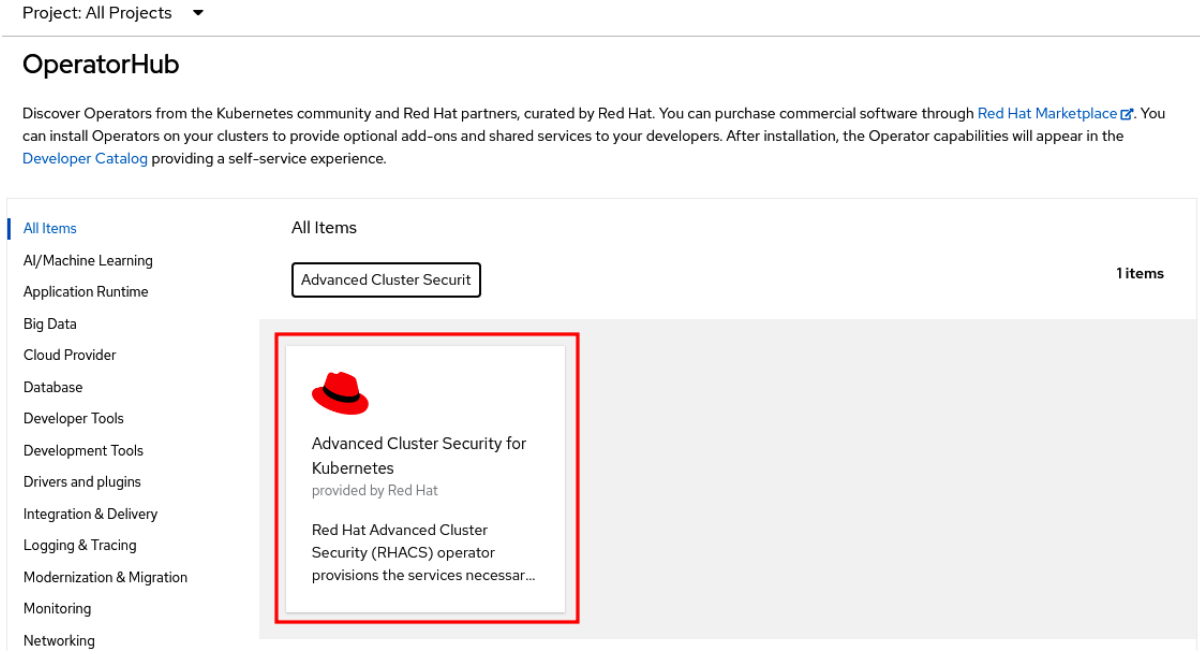

Red Hat
Advanced Cluster Management for Kubernetes
kube:admin
Advanced Cluster Management
Home
Welcome
Overview
Infrastructure
Clusters
Bare metal assets
Automation
Infrastructure environments
Applications
Governance
Credentials
Overview
Grafana
Add provider connection
Refresh every 1m
1
aws
Amazon
1
Cluster
Microsoft
1
Cluster
Summary
0
Applications
2
Clusters
1
Kubernetes type
1
Region
13
Nodes
726
Pods
Cluster compliance 2
100%
Compliant
0 Non-compliant
2 Compliant
Pods 726
100%
Running
0 Failed
0 Pending
726 Running
Cluster status 2
100%
Ready
0 Offline
2 Ready


General / ACM - Clusters Overview
Last 3 hours
5m
Control Plane Health
Top 50 Max Latency API Server
Cluster
Max latency (99th percentile
API servers up
API Errors [1h]
local-cluster
49.9 ms
100%
0.000293
demobyrosacli
49.5 ms
100%
0
etcd
Cluster
Has a Leader
Leader Election Changes
DB Size
demobyrosacli
Yes
0
115.73 MiB
local-cluster
Yes
0
138.34 MiB
Optimization
Top 50 CPU Overestimation Clusters
Cluster
Overestimation
Requested
Utilized
local-cluster
-25.15%
27.88%
53.03%
demobyrosacli
-28.42%
22.52%
50.94%
Top 50 Memory Overestimation Clusters
Cluster
Overestimation
Requested
Utilized
demobyrosacli
5.79%
19.52%
13.72%
local-cluster
0.96%
19.76%
18.80%
Capacity / Utilization
Top 50 CPU Utilized Clusters
Cluster
Total Cores
Allocatable Cores
Requested
Utilized
local-cluster
48
45
27.88%
53.03%
demobyrosacli
40
39.4
22.52%
50.94%
Top 5 Utilized Clusters (% CPU usage)
100%
75%
50%
25%
No data


Pesquisar Openshift Alerts
Openshift Alerts
alertmanager-service
Slack Connect
Explorar o Slack
Canais
geral
outros-assuntos
alertmanager-service
Adicionar canais
Teste gratuito em andamento
20+ novas mensagens
job_name="ip-reconciler-27517875", namespace="openshift-multus", openshift_io_alert_source="platform", prometheus="openshift-monitoring/k8s", severity="warning")
Alert: - warning
Description: Job openshift-multus/ip-reconciler-27517875 failed to complete. Removing failed job after investigation should clear this alert.
Details:
• alertname: KubeJobFailed
• cluster: ab836e92-42f0-4207-882e-e91240b2d9c1
Mostrar mais
[FIRING:1] KubeJobFailed for kube-state-metrics (condition="true", container="kube-rbac-proxy-main", endpoint="https-main", job="kube-state-metrics", job_name="ip-reconciler-27517875", namespace="openshift-multus", openshift_io_alert_source="platform", prometheus="openshift-monitoring/k8s", severity="warning")
Alert: - warning
Description: Job openshift-multus/ip-reconciler-27517875 failed to complete. Removing failed job after investigation should clear this alert.
Details:
• alertname: KubeJobFailed
• cluster: ab836e92-42f0-4207-882e-e91240b2d9c1
Mostrar mais
[RESOLVED] Watchdog for (namespace="openshift-monitoring", prometheus="openshift-monitoring/k8s", severity="none")
Alert: - none
Description: This is an alert meant to ensure that the entire alerting pipeline is functional.
This alert is always firing, therefore it should always be firing in Alertmanager and always fire against a receiver. There are integrations with various notification mechanisms that send a notification when this alert is not firing. For example the
Mostrar mais

Chapter 12: OpenShift Multi-Cluster Security





Advanced Cluster Security for Kubernetes

3.70.1 provided by Red Hat

Install

Latest version

3.70.1

Capability level

- Basic Install
- Seamless Upgrades
- Full Lifecycle
- Deep Insights
- Auto Pilot

Source

Red Hat

Provider

Red Hat

Infrastructure features

Disconnected
Proxy-aware

Repository

N/A

Container image

registry.redhat.io/advanced-cluster-security/rhacs-rhel8-operator@sha256:fb903bf9e110ba03e9c63977ebaf707e6884dd8fd413

Why use Red Hat Advanced Cluster Security for Kubernetes?

Protecting cloud-native applications requires significant changes in how we approach security—we must apply controls earlier in the application development life cycle, use the infrastructure itself to apply controls, and keep up with increasingly rapid release schedules.

Red Hat® Advanced Cluster Security for Kubernetes, powered by StackRox technology, protects your vital applications across build, deploy, and runtime. Our software deploys in your infrastructure and integrates with your DevOps tooling and workflows to deliver better security and compliance. The policy engine includes hundreds of built-in controls to enforce DevOps and security best practices, industry standards such as CIS Benchmarks and National Institute of Standards Technology (NIST) guidelines, configuration management of both containers and Kubernetes, and runtime security.

Red Hat Advanced Cluster Security for Kubernetes provides a Kubernetes-native architecture for container security, enabling DevOps and InfoSec teams to operationalize security.

Features and Benefits

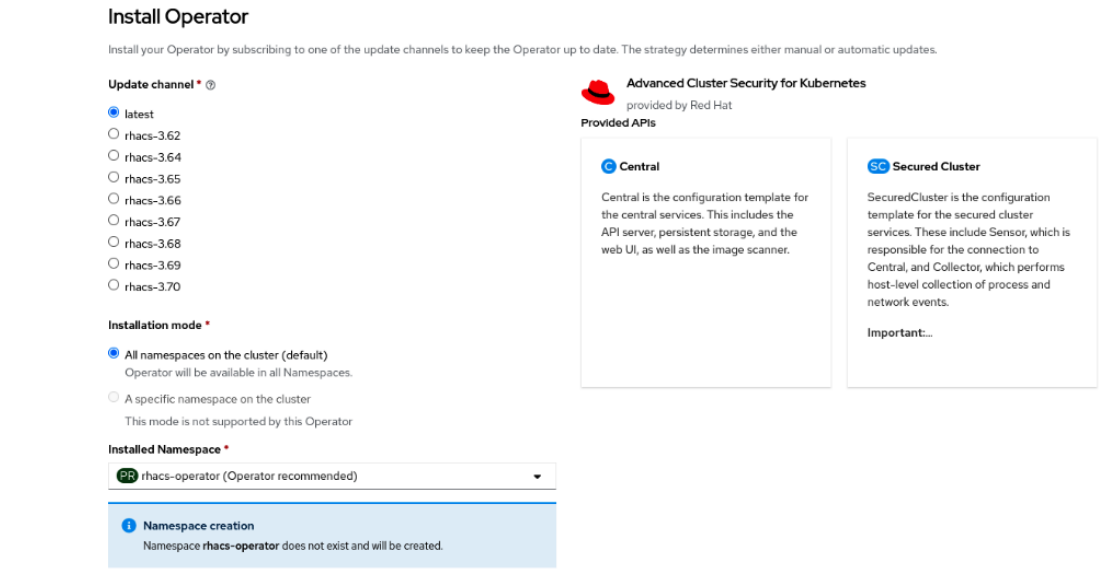
Kubernetes-native security:

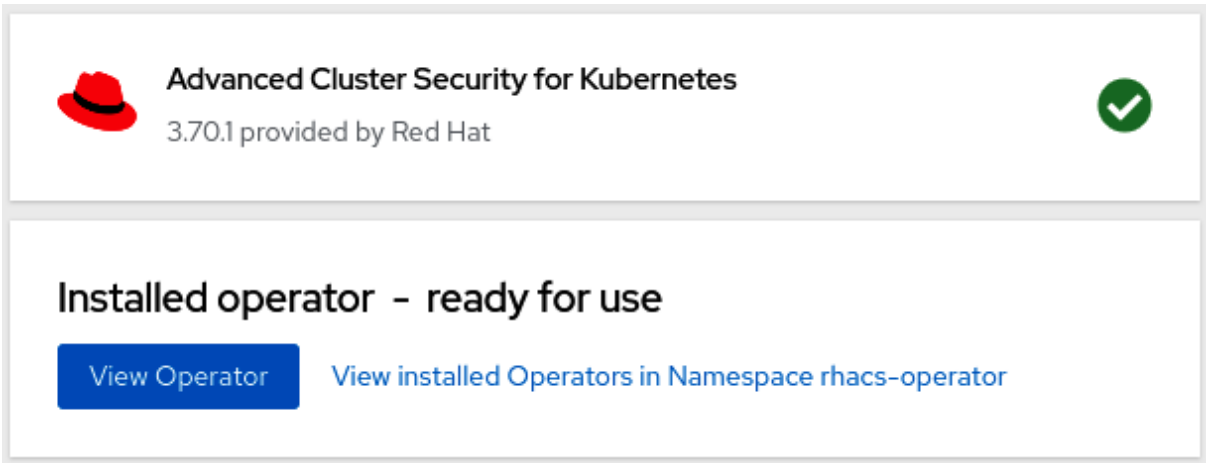
1. Increases protection.
2. Eliminates blind spots, providing staff with insights into critical vulnerabilities and threat vectors.
3. Reduces time and costs.
4. Reduces the time and effort needed to implement security and streamlines security analysis, investigation, and remediation using the rich context Kubernetes provides.
5. Increases scalability and portability.
6. Provides scalability and resiliency native to Kubernetes, avoiding operational conflict and complexity that can result from out-of-band security controls.

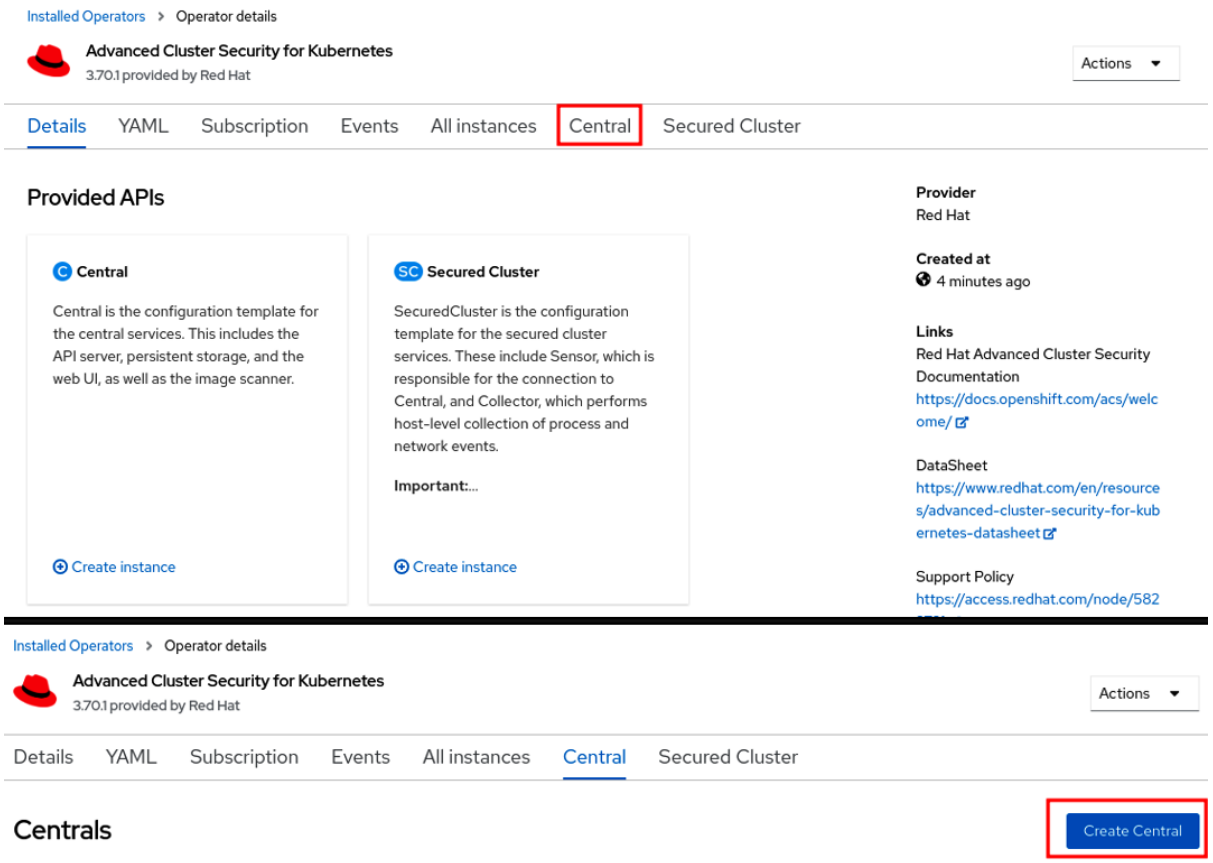
Using the RHACS Operator

RHACS comes with two custom resources:

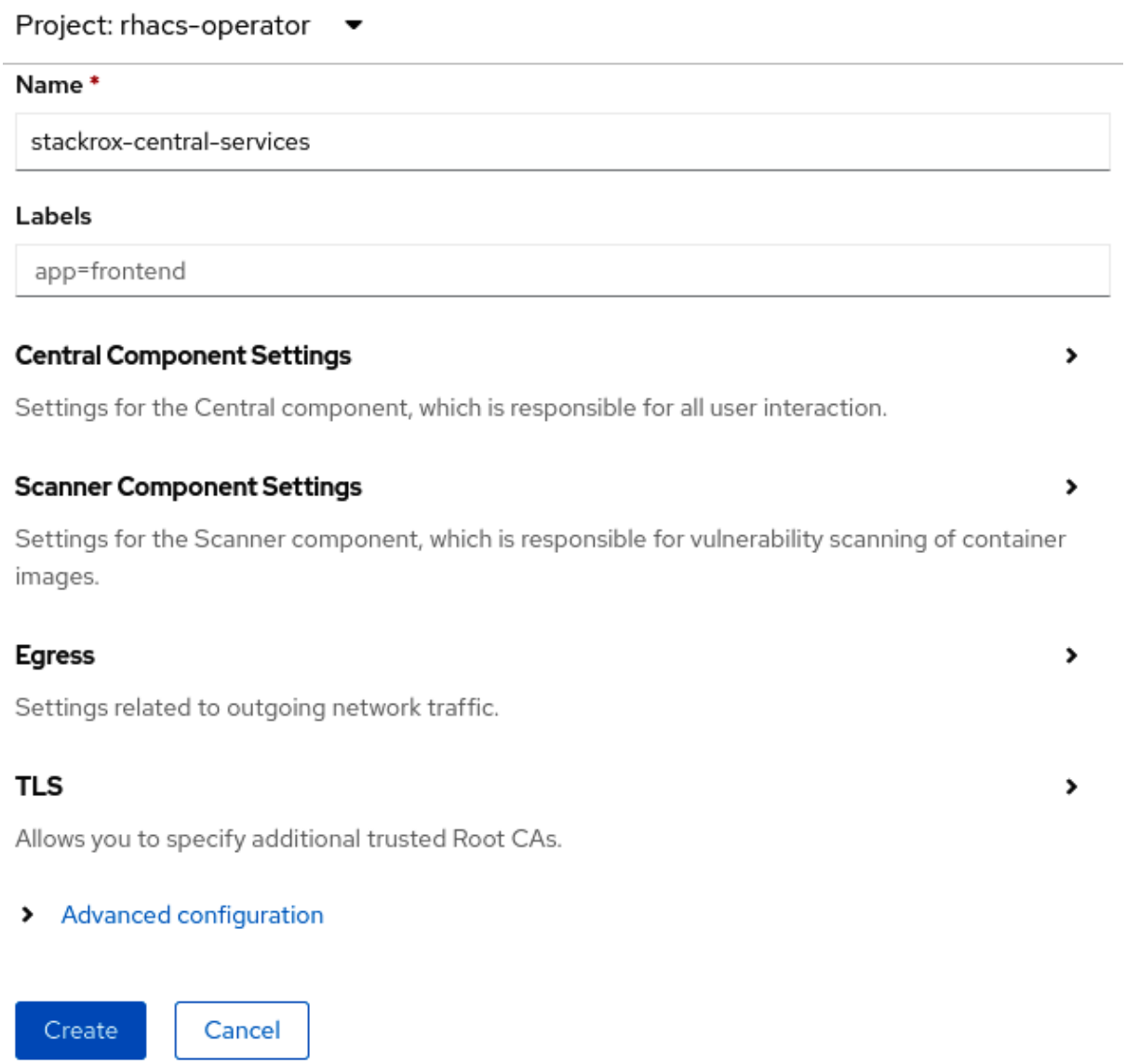
1. **Central Services** - Central is a deployment required on only one cluster in your environment. Users interact with RHACS via the user interface or APIs on Central. Central also sends notifications for

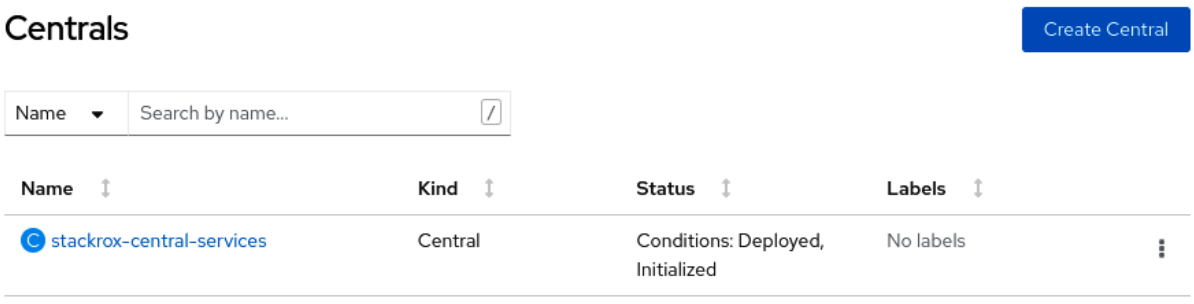

Install Operator
Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.
Update channel *
latest
rhacs-3.62
rhacs-3.64
rhacs-3.65
rhacs-3.66
rhacs-3.67
rhacs-3.68
rhacs-3.69
rhacs-3.70
Installation mode *
All namespaces on the cluster (default)
Operator will be available in all Namespaces.
A specific namespace on the cluster
This mode is not supported by this Operator
Installed Namespace *
PR rhacs-operator (Operator recommended)
Namespace creation
Namespace rhacs-operator does not exist and will be created.
Advanced Cluster Security for Kubernetes
provided by Red Hat
Provided APIs
C Central
Central is the configuration template for the central services. This includes the API server, persistent storage, and the web UI, as well as the image scanner.
SC Secured Cluster
SecuredCluster is the configuration template for the secured cluster services. These include Sensor, which is responsible for the connection to Central, and Collector, which performs host-level collection of process and network events.
Important:...

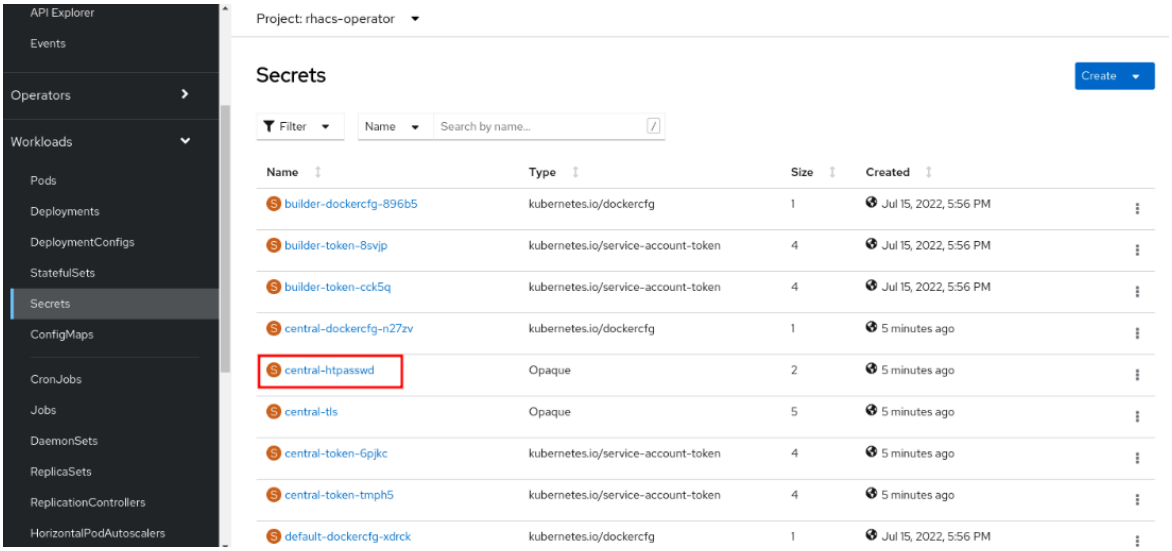

Advanced Cluster Security for Kubernetes
3.70.1 provided by Red Hat
Installed operator - ready for use
View Operator
View installed Operators in Namespace rhacs-operator


Installed Operators > Operator details
Advanced Cluster Security for Kubernetes
3.70.1 provided by Red Hat
Actions
Details
YAML
Subscription
Events
All instances
Central
Secured Cluster
Provided APIs
Central
Central is the configuration template for the central services. This includes the API server, persistent storage, and the web UI, as well as the image scanner.
Create instance
Secured Cluster
SecuredCluster is the configuration template for the secured cluster services. These include Sensor, which is responsible for the connection to Central, and Collector, which performs host-level collection of process and network events.
Important:...
Create instance
Provider
Red Hat
Created at
4 minutes ago
Links
Red Hat Advanced Cluster Security Documentation
https://docs.openshift.com/acs/welcome/
DataSheet
https://www.redhat.com/en/resources/advanced-cluster-security-for-kubernetes-datasheet
Support Policy
https://access.redhat.com/node/582

Installed Operators > Operator details
Advanced Cluster Security for Kubernetes
3.70.1 provided by Red Hat
Actions
Details
YAML
Subscription
Events
All instances
Central
Secured Cluster
Centrals
Create Central
No operands found
Operands are declarative components used to define the behavior of the application.


Project: rhacs-operator
Name *
stackrox-central-services
Labels
app=frontend
Central Component Settings
Settings for the Central component, which is responsible for all user interaction.
Scanner Component Settings
Settings for the Scanner component, which is responsible for vulnerability scanning of container images.
Egress
Settings related to outgoing network traffic.
TLS
Allows you to specify additional trusted Root CAs.
Advanced configuration
Create
Cancel


Centrals
Create Central
Name
Search by name...
/
Name
Kind
Status
Labels
stackrox-central-services
Central
Conditions: Deployed, Initialized
No labels



Project: rhacs-operator

Labels Edit

No labels

Annotations

0 annotations

Created at

6 minutes ago

Owner

stackrox-central-services

Data

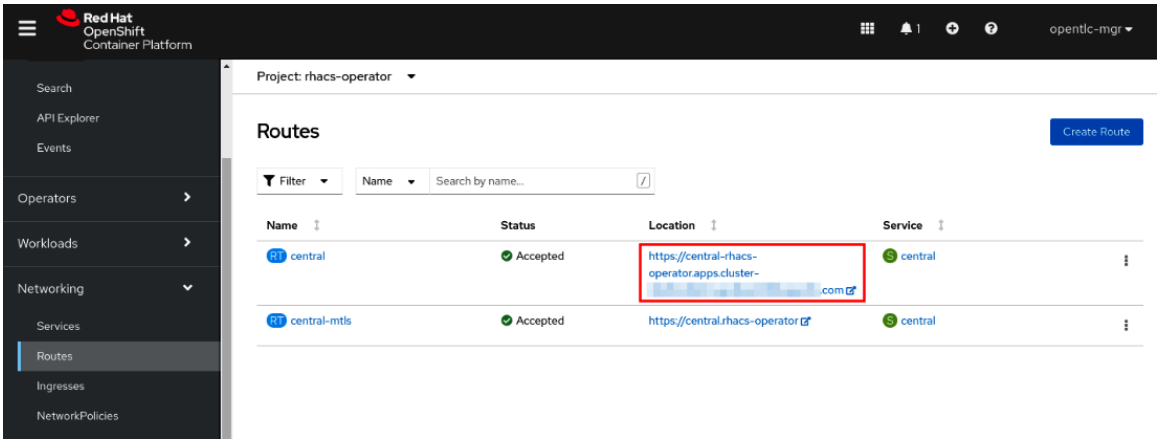
Hide values

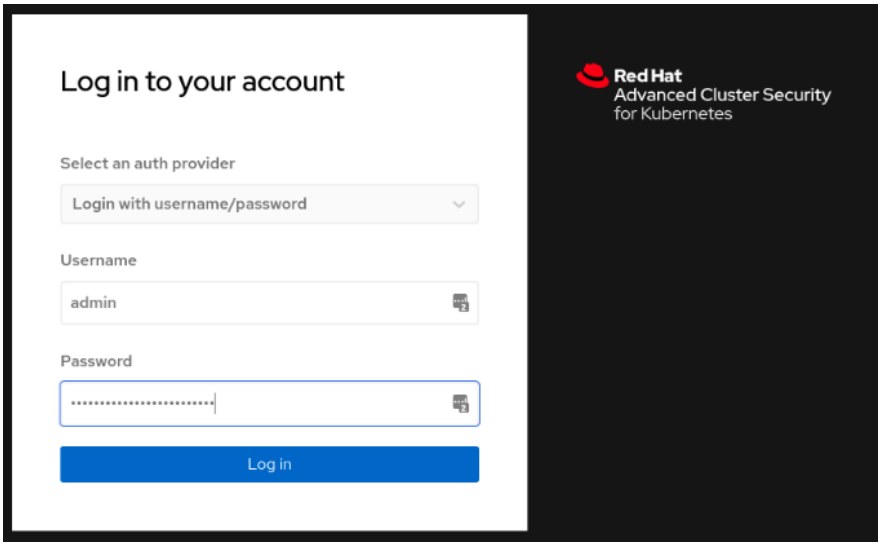
htpasswd

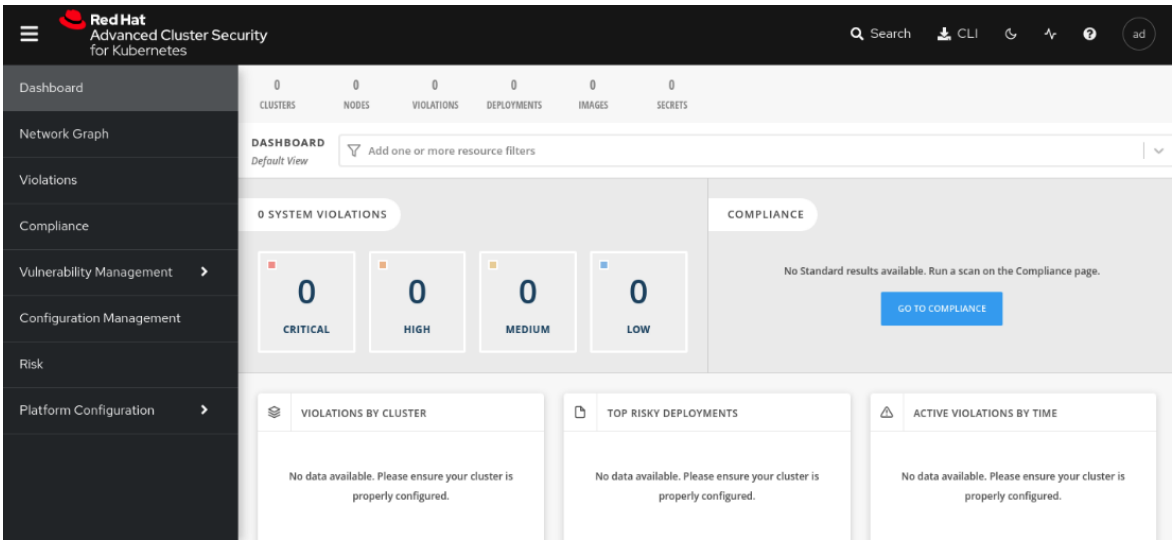
admin:$2a$05$n8QNch[redacted]

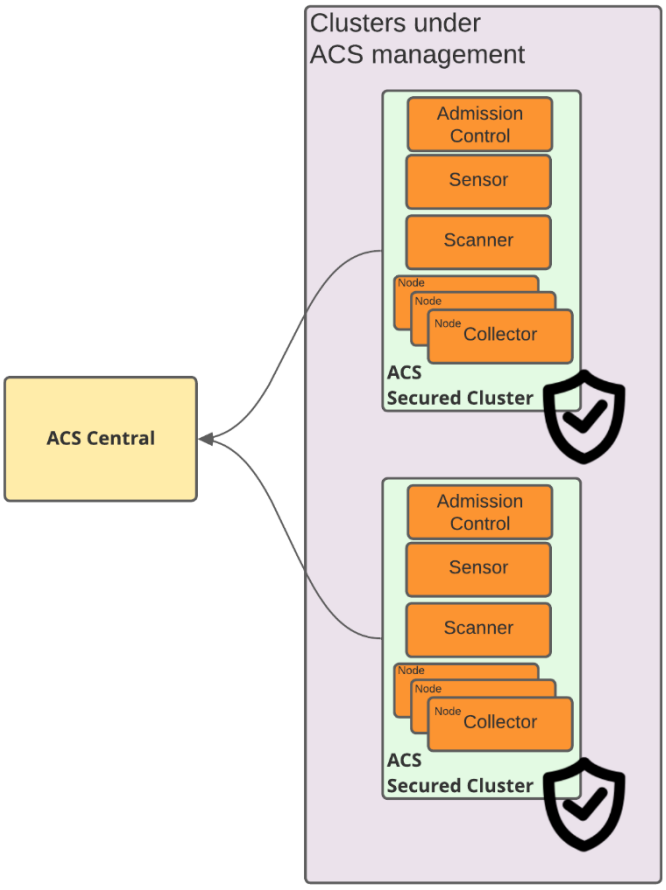
password

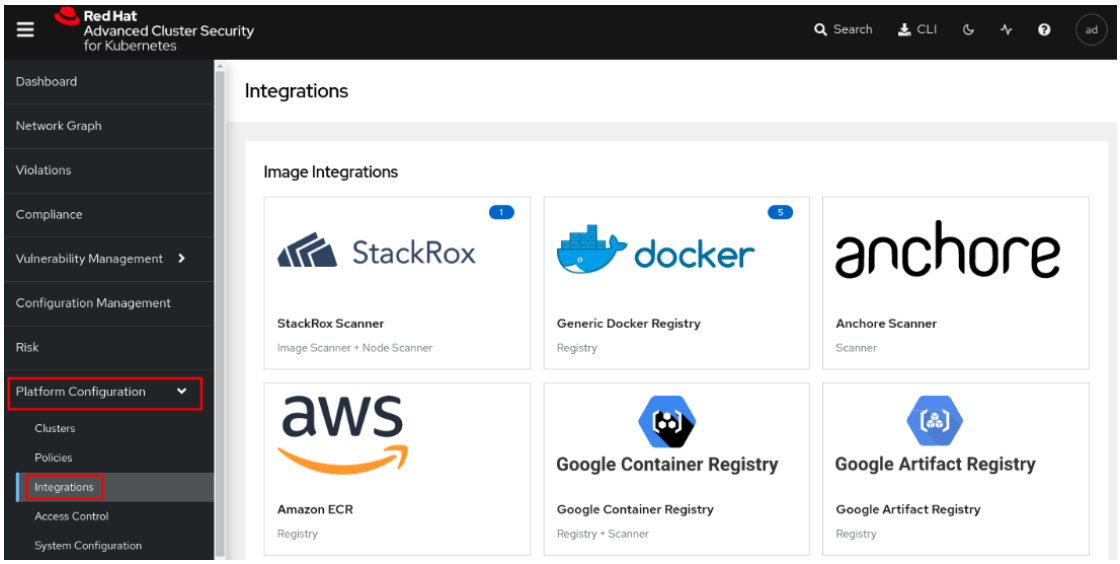
voAA05u[redacted]


Red Hat
OpenShift
Container Platform
opentlc-mgr
Search
API Explorer
Events
Operators
Workloads
Networking
Services
Routes
Ingresses
NetworkPolicies
Project: rhacs-operator
Routes
Create Route
Filter
Name
Search by name...
Name
Status
Location
Service
central
Accepted
https://central-rhacs-operator.apps.cluster-
.com
central
central-mtls
Accepted
https://central.rhacs-operator
central


Log in to your account
Select an auth provider
Login with username/password
Username
admin
Password
Log in
Red Hat
Advanced Cluster Security
for Kubernetes


Red Hat
Advanced Cluster Security
for Kubernetes
Search
CLI
ad
Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Configuration Management
Risk
Platform Configuration
0 CLUSTERS
0 NODES
0 VIOLATIONS
0 DEPLOYMENTS
0 IMAGES
0 SECRETS
DASHBOARD
Default View
Add one or more resource filters
0 SYSTEM VIOLATIONS
0 CRITICAL
0 HIGH
0 MEDIUM
0 LOW
COMPLIANCE
No Standard results available. Run a scan on the Compliance page.
GO TO COMPLIANCE
VIOLATIONS BY CLUSTER
No data available. Please ensure your cluster is properly configured.
TOP RISKY DEPLOYMENTS
No data available. Please ensure your cluster is properly configured.
ACTIVE VIOLATIONS BY TIME
No data available. Please ensure your cluster is properly configured.


Clusters under
ACS management
Admission Control
Sensor
Scanner
Node
Node
Node
Collector
ACS
Secured Cluster
ACS Central
Admission Control
Sensor
Scanner
Node
Node
Node
Collector
ACS
Secured Cluster


Red Hat
Advanced Cluster Security
for Kubernetes
Search
CLI
ad
Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Configuration Management
Risk
Platform Configuration
Clusters
Policies
Integrations
Access Control
System Configuration
Integrations
Image Integrations
StackRox
StackRox Scanner
Image Scanner + Node Scanner
docker
Generic Docker Registry
Registry
anchore
Anchore Scanner
Scanner
aws
Amazon ECR
Registry
Google Container Registry
Google Container Registry
Registry + Scanner
Google Artifact Registry
Google Artifact Registry
Registry

Authentication Tokens

Integrations > Cluster Init Bundle > Create Integration

Configure Cluster Init Bundle Integration

Integration was saved successfully

Please copy the generated cluster init bundle YAML file and store it safely. You will not be able to access it again after you close this window.

Download Helm values file

Use the following file if you do not want your secrets to be managed by Helm. Most users should use the Helm values file above instead.

Download Kubernetes secrets file

Name	local-cluster
Issued	07/15/2022 | 6:36:21PM
Expiration	07/15/2023 | 6:36:00PM
Created By	sso:4df1b98c-24ed-4073-a9ad-356aec6bb62d:admin

Back

Project: rhacs-operator

Installed Operators > Operator details

Advanced Cluster Security for Kubernetes
3.70.1 provided by Red Hat

Actions

Details | YAML | Subscription | Events | All instances | Central | Secured Cluster

Provided APIs

Central

Central is the configuration template for the central services. This includes the API server, persistent storage, and the web UI, as well as the image scanner.

Create instance

Secured Cluster

SecuredCluster is the configuration template for the secured cluster services. These include Sensor, which is responsible for the connection to Central, and Collector, which performs host-level collection of process and network events.

Important:...

Create instance

Provider
Red Hat

Created at
Jul 23, 2022, 12:00 PM

Links
Red Hat Advanced Cluster Security Documentation
https://docs.openshift.com/acs/welcome/

DataSheet
https://www.redhat.com/en/resources/advanced-cluster-security-for-kubernetes-datasheet

Support Policy
https://access.redhat.com/node/5822721

Community Site
https://www.stackrox.io/

Maintainers
Advanced Cluster Security product team
rhacs-pm@redhat.com

Description

Why use Red Hat Advanced Cluster Security for Kubernetes?

Protecting cloud-native applications requires significant changes in how we approach security—we must apply controls earlier in the application development life cycle, use the infrastructure itself to apply controls, and keep up with increasingly rapid release schedules.

Project: rhacs-operator

Installed Operators > Operator details

Advanced Cluster Security for Kubernetes
3.70.1 provided by Red Hat

Actions

Details | YAML | Subscription | Events | All instances | Central | Secured Cluster

Provided APIs

Central

Central is the configuration template for the central services. This includes the API server, persistent storage, and the web UI, as well as the image scanner.

Create instance

Secured Cluster

SecuredCluster is the configuration template for the secured cluster services. These include Sensor, which is responsible for the connection to Central, and Collector, which performs host-level collection of process and network events.

Important:...

Create instance

Provider
Red Hat

Created at
Jul 15, 2022, 5:57 PM

Links
Red Hat Advanced Cluster Security Documentation
https://docs.openshift.com/acs/welcome/

DataSheet
https://www.redhat.com/en/resources/advanced-cluster-security-for-kubernetes-datasheet

Support Policy
https://access.redhat.com/node/5822721

Project: rhacs-operator

Note: Some fields may not be represented in this form view. Please select "YAML view" for full control.

Name *

stackrox-secured-cluster-services

Labels

app=frontend

Cluster Name *

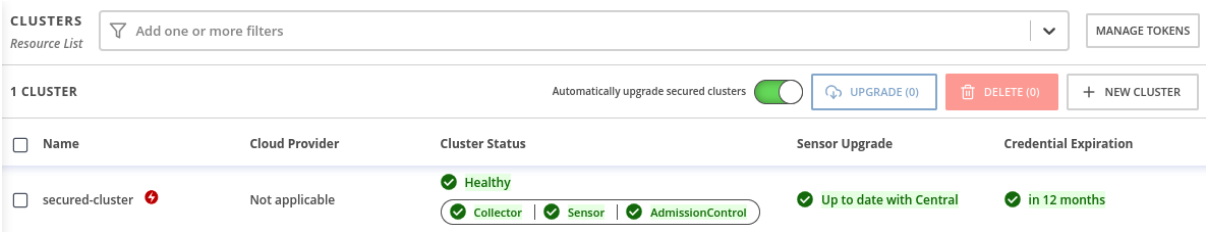
local-cluster

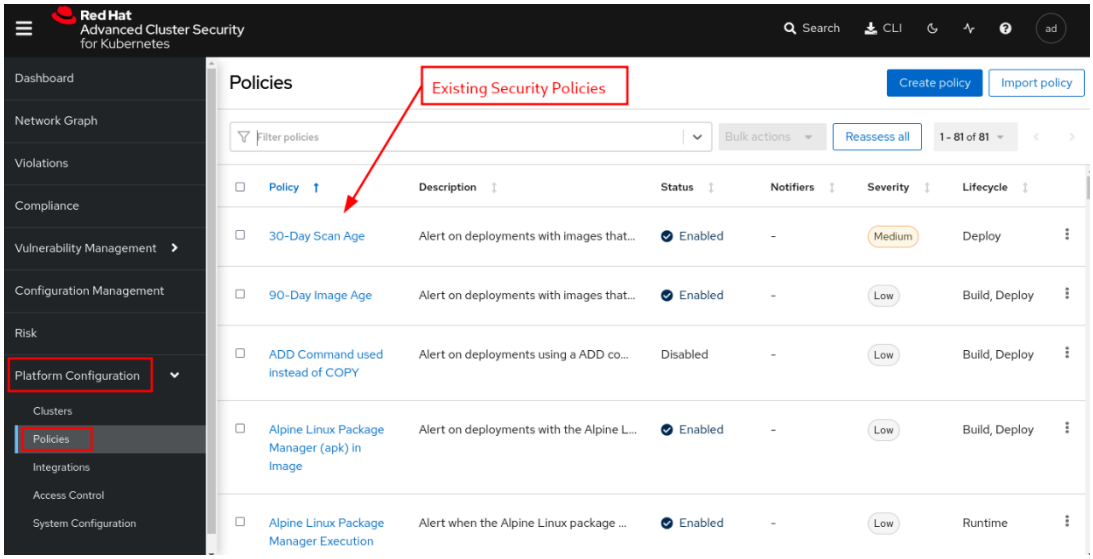
The unique name of this cluster, as it will be shown in the Red Hat Advanced Cluster Security UI. Note: Once a name is set here, you will not be able to change it again. You will need to delete and re-create this object in order to register a cluster with a new name.

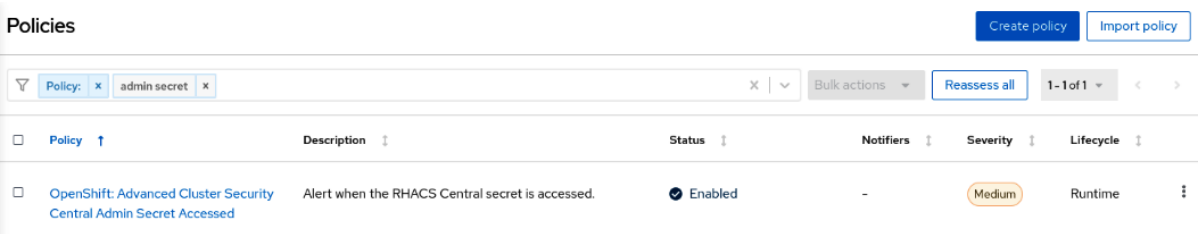
Central Endpoint

central-rhacs-operator.apps.[redacted]m:443

The endpoint of the Red Hat Advanced Cluster Security Central instance to connect to, including the port number. If using a non-gRPC capable load balancer, use the WebSocket protocol by prefixing the endpoint address with wss://. Note: when leaving this blank, Sensor will attempt to connect to a Central instance running in the same namespace.







OpenShift: Advanced Cluster Security Central Admin Secret Accessed

Enabled

Actions

Policy details

Severity	Medium
Categories	Anomalous Activity, Kubernetes Events
Type	System default
Description	Alert when the RHACS Central secret is accessed.
Rationale	The Central secret can be used to login to the Central user interface as the admin user. This secret is generally salted and hashe d by default in the data.htpasswd field, but may contain a base64 encoded password in the field data.password (if deployed with an Operator). This field may be safely removed. This secret should only be accessed for break glass troubleshooting and initial c onfiguration. An update or access of this secret may indicate that it will be used to administer and configure security controls.
Guidance	Ensure that the Central admin secret was accessed for valid buiness purposes.

MITRE ATT&CK

Credential Access TA0006

The adversary is trying to steal account names and passwords. Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

OpenShift: Advanced Cluster Security Central Admin Secret Accessed

Design custom security policies for your environment

1. Policy details
2. Policy behavior
3. Policy criteria
4. Policy scope
5. Review policy

Policy details

Describe general information about your policy.

Name *

OpenShift: Advanced Cluster Security Central Admin Secret Accessed

Provide a descriptive and unique policy name

Severity *

○ Low ◉ Medium ○ High ○ Critical

Select a severity level for this policy

Categories *

Anomalous Activity × Kubernetes Events ×

Select policy categories you want to apply to this policy

Description

Alert when the RHACS Central secret is accessed.

Attach notifiers

Forward policy violations to external tooling by selecting one or more notifiers from existing integrations.

No notifiers found. Add notifiers in the Integrations Page to add them to this policy.

Add a notifier

Next Back Cancel

OpenShift: Advanced Cluster Security Central Admin Secret Accessed

Design custom security policies for your environment

1. Policy details
2. Policy behavior
3. Policy criteria
4. Policy scope
5. Review policy

Policy behavior

Select which stage of a container lifecycle this policy applies. Event sources can only be chosen for policies that apply at runtime.

Info

Build-time policies apply to image fields such as CVEs and Dockerfile instructions.

Deploy-time policies can include all build-time policy criteria but they can also include data form your cluster configurations, such as running in privileged mode or mounting the Docker socket.

Runtime policies can include all build-time and deploy-time policy criteria but they can also include data about process executions during runtime.

Lifecycle stages *

☐ Build ☐ Deploy ☑ Runtime

Ch 1 fecycle 2 to which 3 olicy is applicable. You can select more than one stage.

Event sources (Runtime lifecycle only)

○ Deployment ◉ Audit logs

Response method

Next Back Cancel

OpenShift: Advanced Cluster Security Central Admin Secret Accessed

Design custom security policies for your environment

1. Policy details
2. Policy behavior
3. Policy criteria
4. Policy scope
5. Review policy

Policy criteria

Chain criteria with boolean logic.

Editing policy criteria is disabled for system default policies

If you need to edit policy criteria, clone this policy or create a new policy.

1

Kubernetes resource:

Kubernetes resource

Secrets

– and –

Kubernetes API verb:

Kubernetes API verb

GET

Next Back Cancel

OpenShift: Advanced Cluster Security Central Admin Secret Accessed

Design custom security policies for your environment

1. Policy details
2. Policy behavior
3. Policy criteria
4. Policy scope
5. Review policy

Policy scope

Create scopes to restrict or exclude your policy from entities within your environment.

Restrict by scope 1

Use Restrict by scope to enable this policy only for a specific cluster, namespace, or label. You can add multiple scope and also use regular expressions (RE2 syntax) for namespaces and labels.

Add inclusion scope

Exclude by scope 2

Use Exclude by scope to exclude entities from your policy. This function is only available for Deploy and Runtime lifecycle stages. You can add multiple scopes and also use regular expressions (RE2 syntax) for namespaces and labels.

Add exclusion scope

Exclude images 3

The exclude images setting only applies when you check images in a continuous integration system (the Build lifecycle stage). It won't have any effect if you use this policy to check running deployments (the Deploy lifecycle stage) or

Next Back Cancel

Violations

Filter violations

110 results found | Row Actions | 1 - 50 of 110 | 1 of 3

Policy	Entity	Type	Enforced	Severity	Categories	Lifecycle	Time
OpenShift: Advanced Cluster Security Central Admin Secret Accessed	central-htpasswd in "local-cluster/rhacs-operator"	secrets	No	Medium	Multiple	Runtime	07/18/2022 | 7:23:33PM
Pod Service Account Token Automatically Mounted	kube-apiserver-ip-10-0-170-36.us-east-2.compute.internal in "local-cluster/openshift-kube-apiserver"	deployment	No	Medium	Multiple	Deploy	07/16/2022 | 3:12:25PM
Pod Service Account Token Automatically Mounted	kube-apiserver-ip-10-0-209-35.us-east-2.compute.internal in "local-cluster/openshift-kube-apiserver"	deployment	No	Medium	Multiple	Deploy	07/16/2022 | 3:07:36PM
Pod Service Account Token	kube-apiserver-ip-10-0-137-27.us-east-	deployment	No	Medium	Multiple	Deploy	07/16/2022 | 3:02:47PM

Red Hat Package Manager Execution

in "scanner" deployment

Violation | Deployment | Policy

Violation events

Binary '/usr/bin/rpm' executed with 19 different arguments under user ID 65534

First occurrence
07/15/2022 | 7:04:19PM

Last occurrence
07/15/2022 | 7:05:25PM

/usr/bin/rpm

0 | 0

Container ID
73dfa3157aae

Time
07/15/2022 | 7:04:19PM

User ID
65534

Arguments
--dbpath /tmp/rpm1964258894 --query --all --queryformat %{name}\n%{evr}\n%{ARCH}\n%{RPMTAG_MODULARITYLABEL}\n[%{FILENAMES}\n].\n

Add violation metadata

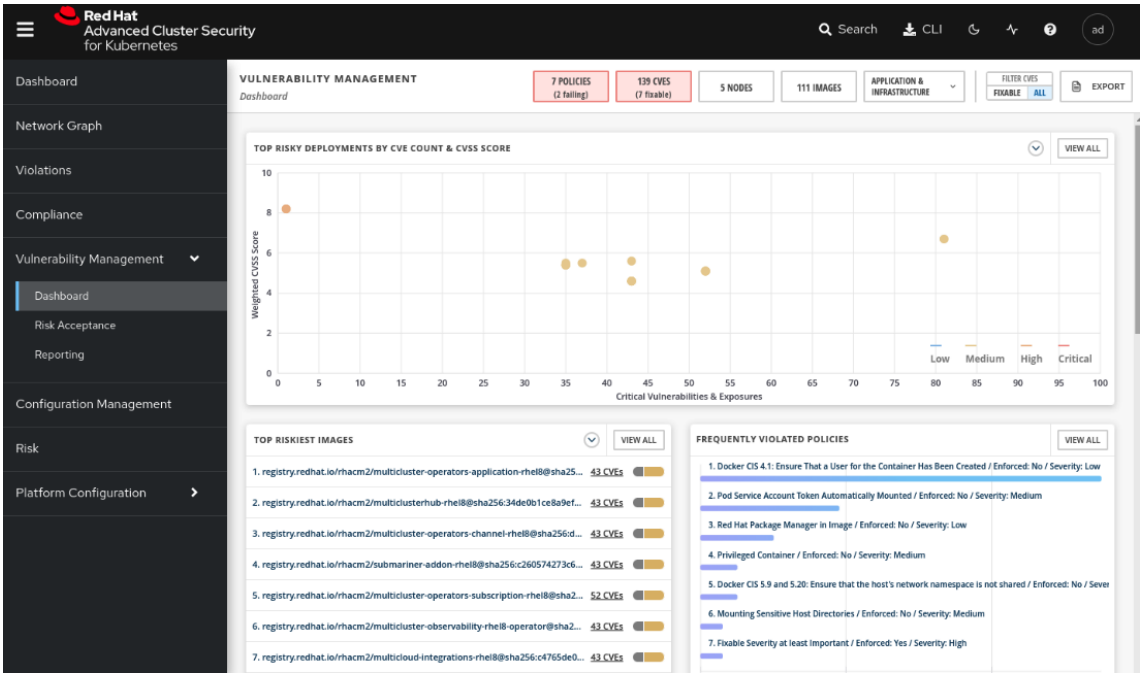
0 Violation Tags

Select or create new tags.

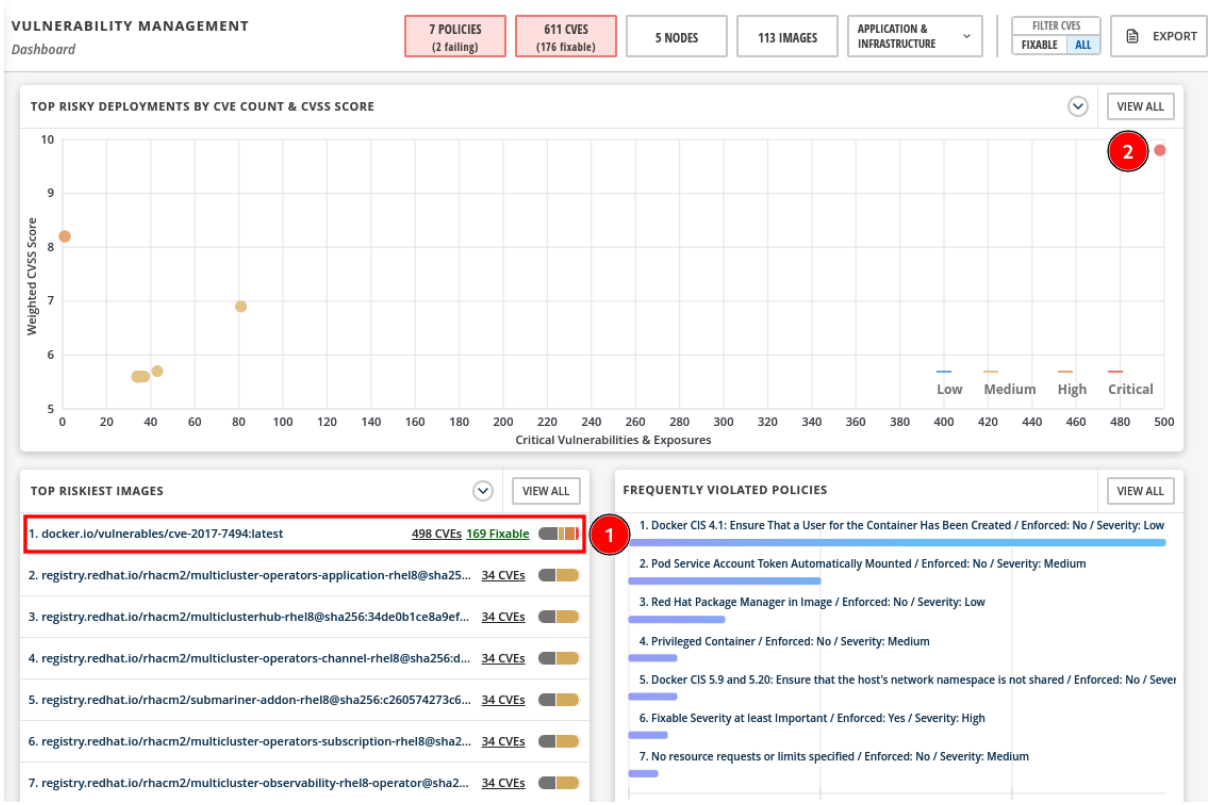
0 Violation Comments

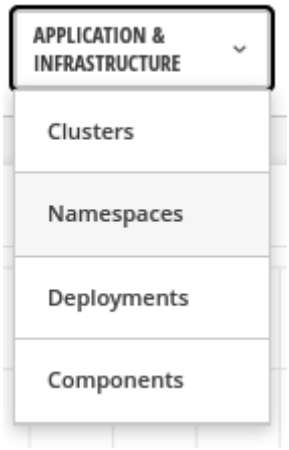
New

No Comments


Red Hat
Advanced Cluster Security
for Kubernetes
Search
CLI
ad
Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Dashboard
Risk Acceptance
Reporting
Configuration Management
Risk
Platform Configuration
VULNERABILITY MANAGEMENT
Dashboard
7 POLICIES (2 failing)
139 CVES (7 fixable)
5 NODES
111 IMAGES
APPLICATION & INFRASTRUCTURE
FILTER CVES
FIXABLE ALL
EXPORT
TOP RISKY DEPLOYMENTS BY CVE COUNT & CVSS SCORE
VIEW ALL
Weighted CVSS Score
Critical Vulnerabilities & Exposures
Low
Medium
High
Critical
TOP RISKIEST IMAGES
1. registry.redhat.io/rhacm2/multicluster-operators-application-rhel8@sha25... 43 CVEs
2. registry.redhat.io/rhacm2/multiclusterhub-rhel8@sha256:34de0b1ce8a9ef... 43 CVEs
3. registry.redhat.io/rhacm2/multicluster-operators-channel-rhel8@sha256:d... 43 CVEs
4. registry.redhat.io/rhacm2/submariner-addon-rhel8@sha256:c260574273c6... 43 CVEs
5. registry.redhat.io/rhacm2/multicluster-operators-subscription-rhel8@sha2... 52 CVEs
6. registry.redhat.io/rhacm2/multicluster-observability-rhel8-operator@sha2... 43 CVEs
7. registry.redhat.io/rhacm2/multicloud-integrations-rhel8@sha256:c4765de0... 43 CVEs
FREQUENTLY VIOLATED POLICIES
1. Docker CIS 4.1: Ensure That a User for the Container Has Been Created / Enforced: No / Severity: Low
2. Pod Service Account Token Automatically Mounted / Enforced: No / Severity: Medium
3. Red Hat Package Manager in Image / Enforced: No / Severity: Low
4. Privileged Container / Enforced: No / Severity: Medium
5. Docker CIS 5.9 and 5.20: Ensure that the host's network namespace is not shared / Enforced: No / Sever
6. Mounting Sensitive Host Directories / Enforced: No / Severity: Medium
7. Fixable Severity at least Important / Enforced: Yes / Severity: High

7 POLICIES (2 failing)
27 CVES (1 fixable)
5 NODES
111 IMAGES
APPLICATION & INFRASTRUCTURE


VULNERABILITY MANAGEMENT
Dashboard
7 POLICIES (2 failing)
611 CVES (176 fixable)
5 NODES
113 IMAGES
APPLICATION & INFRASTRUCTURE
FILTER CVES
FIXABLE ALL
EXPORT
TOP RISKY DEPLOYMENTS BY CVE COUNT & CVSS SCORE
VIEW ALL
2
Weighted CVSS Score
Critical Vulnerabilities & Exposures
Low
Medium
High
Critical
TOP RISKIEST IMAGES
1. docker.io/vulnerables/cve-2017-7494:latest 498 CVEs 169 Fixable
2. registry.redhat.io/rhacm2/multicluster-operators-application-rhel8@sha25... 34 CVEs
3. registry.redhat.io/rhacm2/multiclusterhub-rhel8@sha256:34de0b1ce8a9ef... 34 CVEs
4. registry.redhat.io/rhacm2/multicluster-operators-channel-rhel8@sha256:d... 34 CVEs
5. registry.redhat.io/rhacm2/submariner-addon-rhel8@sha256:c260574273c6... 34 CVEs
6. registry.redhat.io/rhacm2/multicluster-operators-subscription-rhel8@sha2... 34 CVEs
7. registry.redhat.io/rhacm2/multicluster-observability-rhel8-operator@sha2... 34 CVEs
1
FREQUENTLY VIOLATED POLICIES
1. Docker CIS 4.1: Ensure That a User for the Container Has Been Created / Enforced: No / Severity: Low
2. Pod Service Account Token Automatically Mounted / Enforced: No / Severity: Medium
3. Red Hat Package Manager in Image / Enforced: No / Severity: Low
4. Privileged Container / Enforced: No / Severity: Medium
5. Docker CIS 5.9 and 5.20: Ensure that the host's network namespace is not shared / Enforced: No / Sever
6. Fixable Severity at least Important / Enforced: Yes / Severity: High
7. No resource requests or limits specified / Enforced: No / Severity: Medium

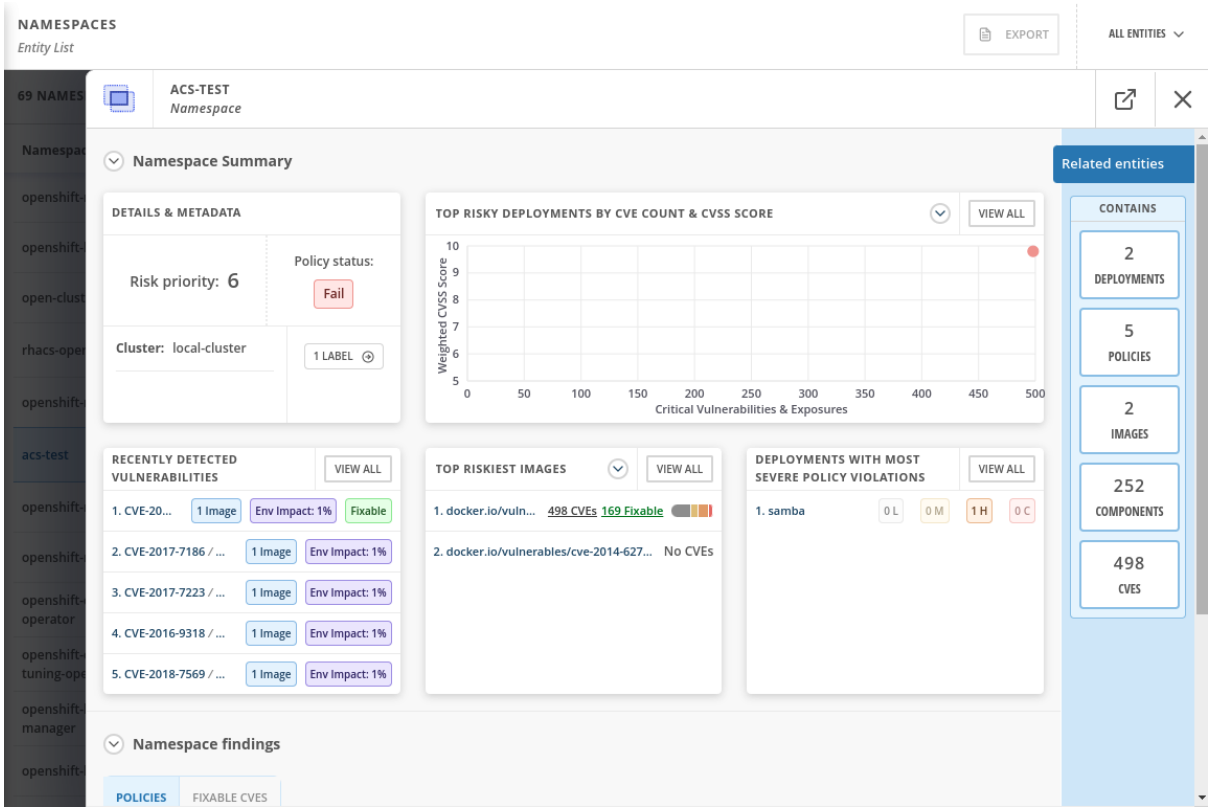


NAMESPACES
Entity List

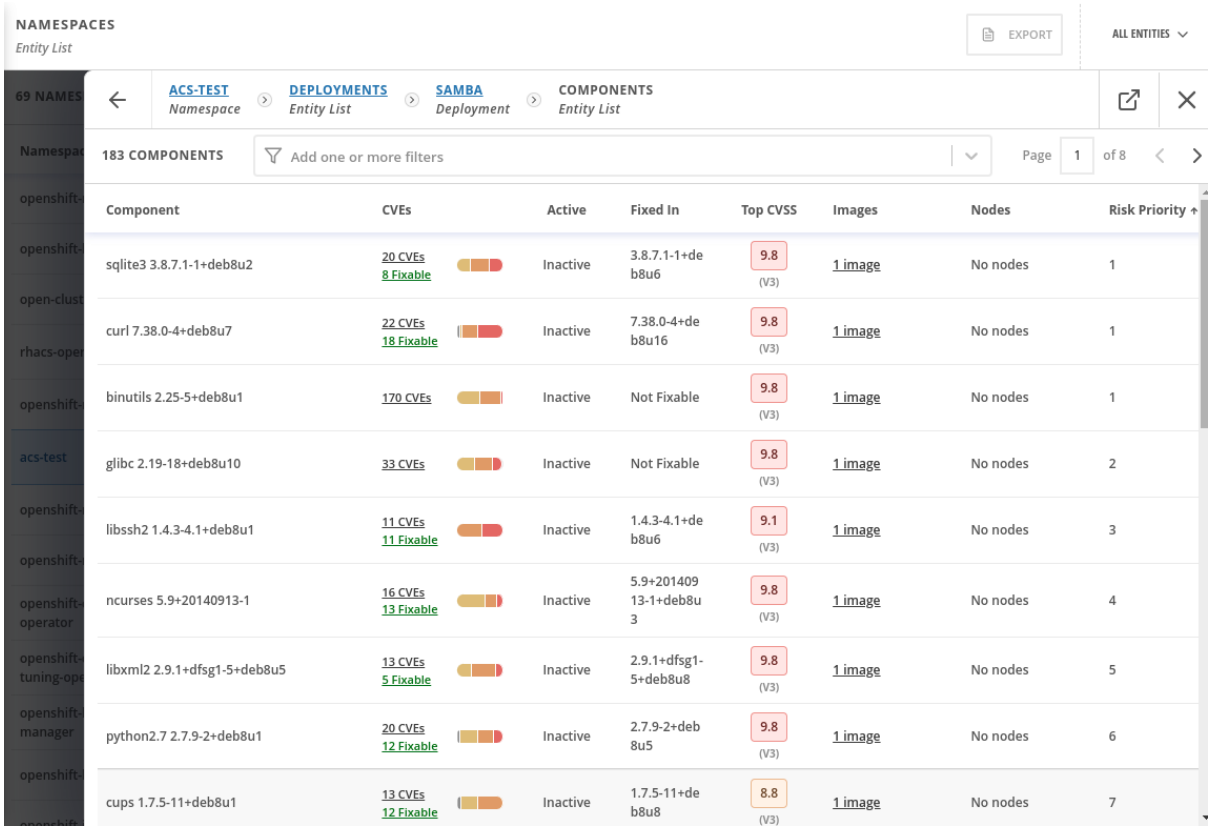
EXPORT | ALL ENTITIES

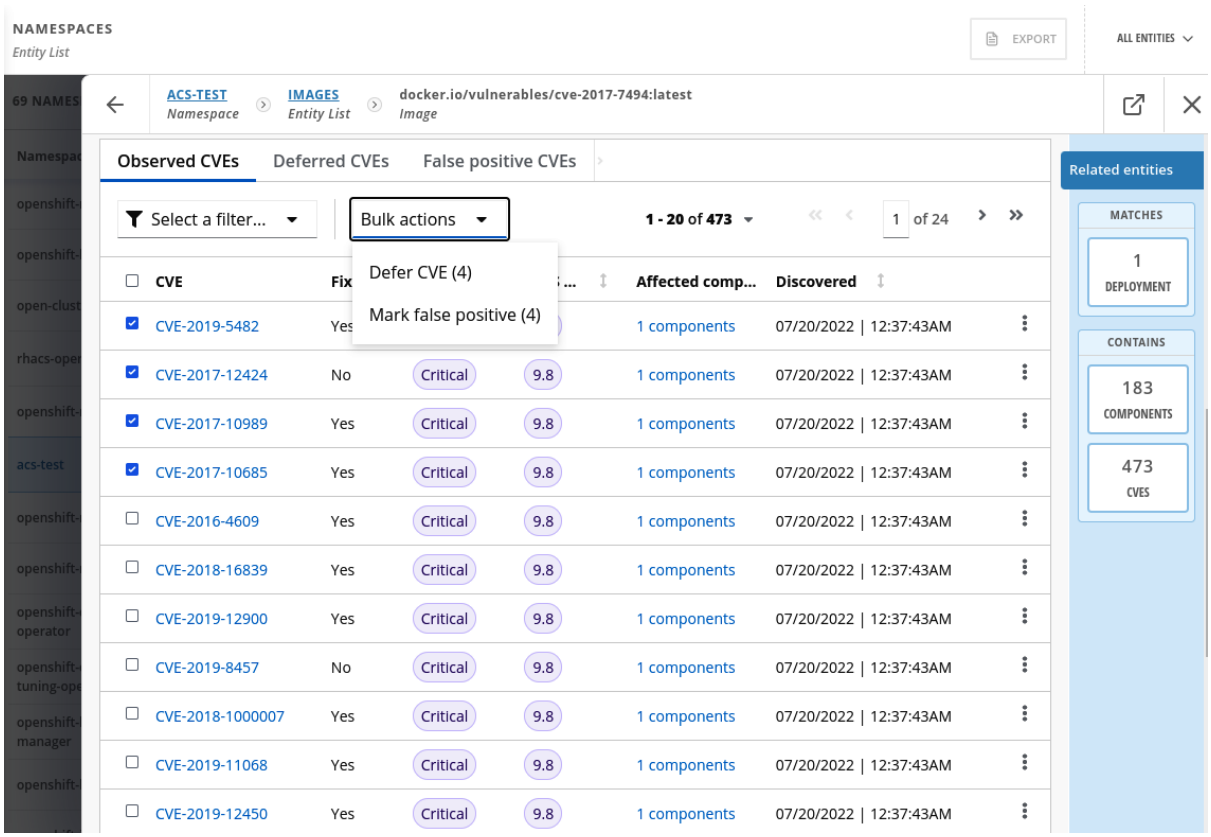
69 NAMESPACES | Add one or more filters | Page 1 of 3

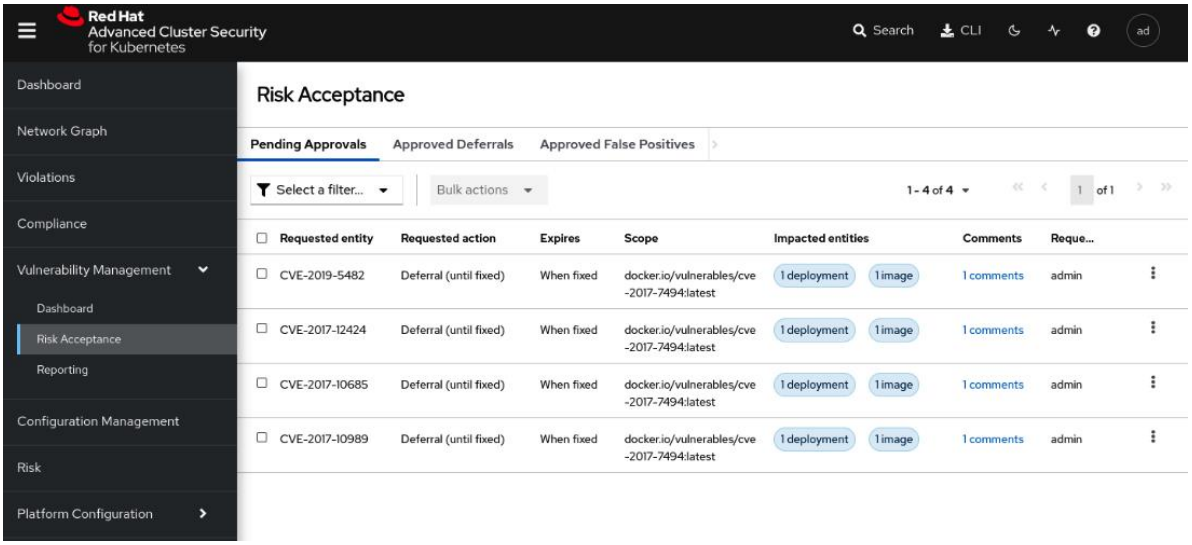
Namespace	CVEs	Cluster	Deployments	Images	Policy Status	Latest Violation	Risk Priority
openshift-marketplace	No CVEs	local-cluster	5 deployments	5 images	Pass	—	1
openshift-kube-apiserver	No CVEs	local-cluster	3 deployments	2 images	Pass	—	2
open-cluster-management	34 CVEs	local-cluster	8 deployments	7 images	Pass	—	3
rhacs-operator	94 CVEs 6 Fixable	local-cluster	7 deployments	6 images	Fail	07/20/2022 12:32:44AM	4
openshift-monitoring	No CVEs	local-cluster	11 deployments	15 images	Pass	—	5
acs-test	498 CVEs 169 Fixable	local-cluster	1 deployment	1 image	Fail	07/20/2022 12:41:39AM	6
openshift-machine-api	No CVEs	local-cluster	5 deployments	5 images	Pass	—	7
openshift-multus	No CVEs	local-cluster	5 deployments	5 images	Pass	—	8
openshift-cluster-storage-operator	No CVEs	local-cluster	4 deployments	4 images	Pass	—	9

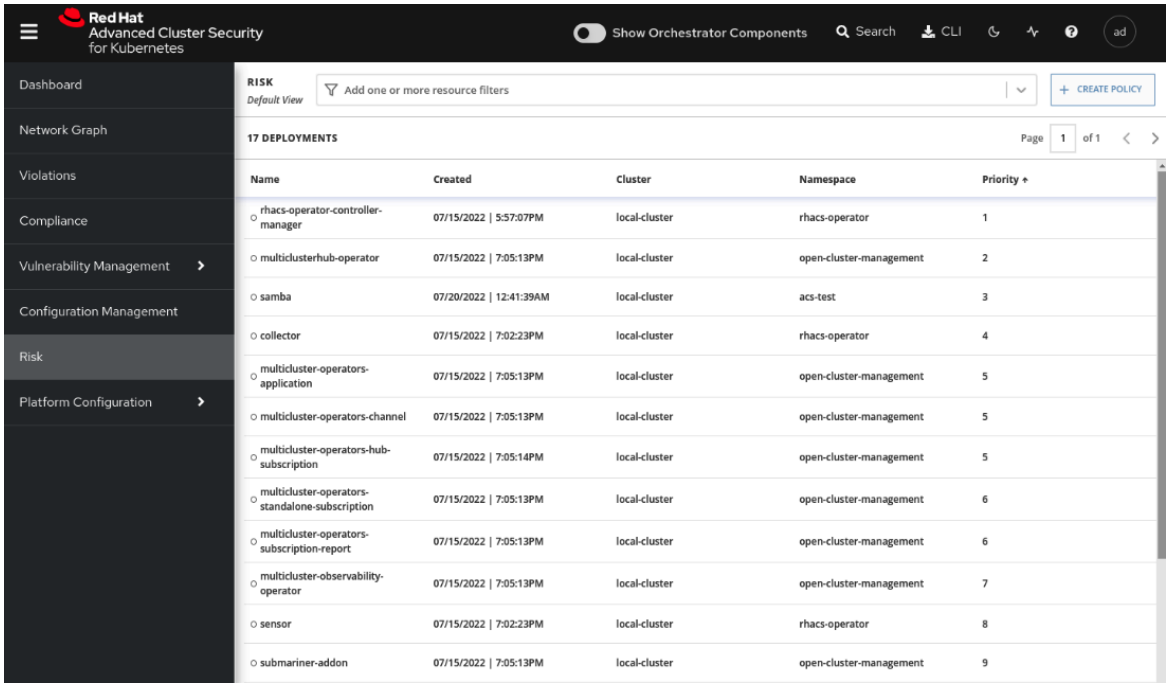


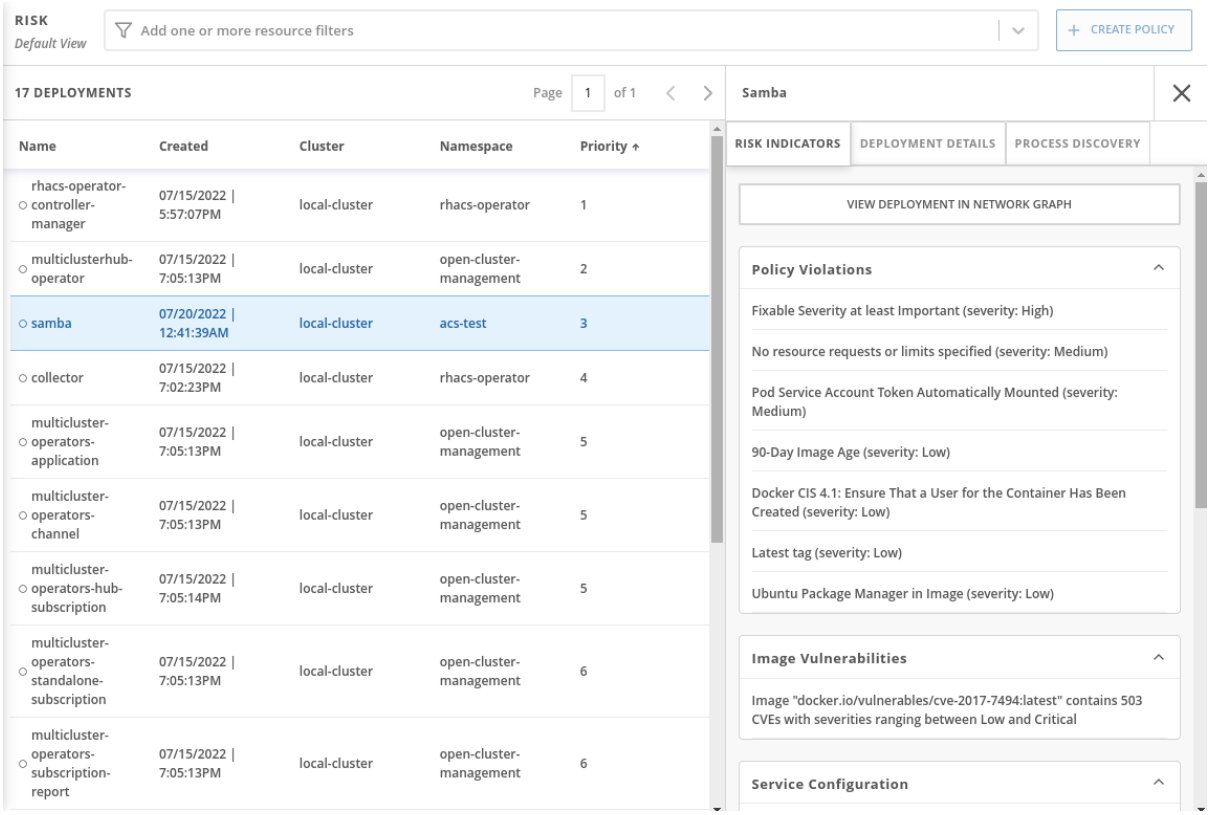
Deployment	CVEs	Latest Violation	Policy Status	Images	Risk Priority ↑
samba	498 CVEs 169 Fixable	07/20/2022 12:41:39AM	Fail	1 image	3
shell	No CVEs	—	Pass	1 image	23

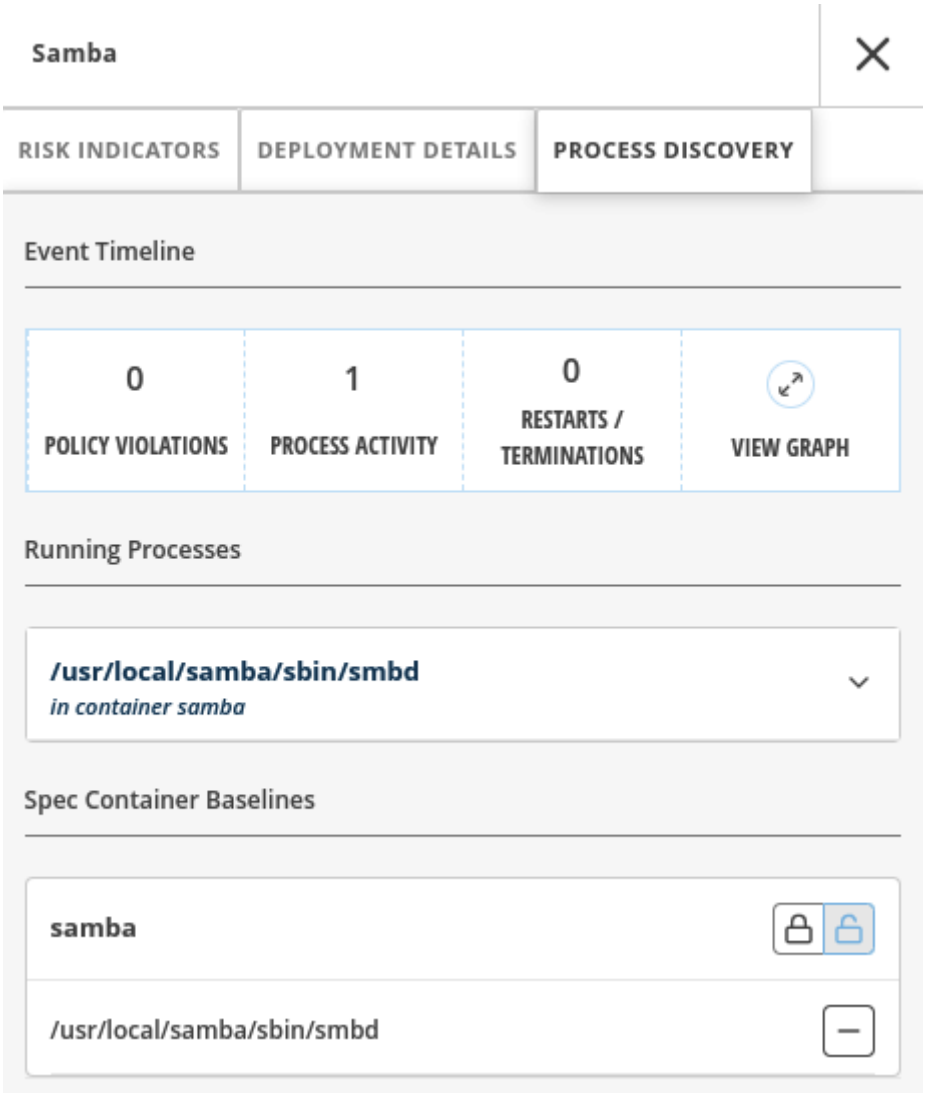

NAMESPACES
Entity List
EXPORT
ALL ENTITIES
ACS-TEST
Namespace
DEPLOYMENTS
Entity List
SAMBA
Deployment
COMPONENTS
Entity List
183 COMPONENTS
Add one or more filters
Page 1 of 8
Component
CVEs
Active
Fixed In
Top CVSS
Images
Nodes
Risk Priority
sqlite3 3.8.7.1-1+deb8u2
20 CVEs
8 Fixable
Inactive
3.8.7.1-1+deb8u6
9.8 (V3)
1 image
No nodes
1
curl 7.38.0-4+deb8u7
22 CVEs
18 Fixable
Inactive
7.38.0-4+deb8u16
9.8 (V3)
1 image
No nodes
1
binutils 2.25-5+deb8u1
170 CVEs
Inactive
Not Fixable
9.8 (V3)
1 image
No nodes
1
glibc 2.19-18+deb8u10
33 CVEs
Inactive
Not Fixable
9.8 (V3)
1 image
No nodes
2
libssh2 1.4.3-4.1+deb8u1
11 CVEs
11 Fixable
Inactive
1.4.3-4.1+deb8u6
9.1 (V3)
1 image
No nodes
3
ncurses 5.9+20140913-1
16 CVEs
13 Fixable
Inactive
5.9+20140913-1+deb8u3
9.8 (V3)
1 image
No nodes
4
libxml2 2.9.1+dfsg1-5+deb8u5
13 CVEs
5 Fixable
Inactive
2.9.1+dfsg1-5+deb8u8
9.8 (V3)
1 image
No nodes
5
python2.7 2.7.9-2+deb8u1
20 CVEs
12 Fixable
Inactive
2.7.9-2+deb8u5
9.8 (V3)
1 image
No nodes
6
cups 1.7.5-11+deb8u1
13 CVEs
12 Fixable
Inactive
1.7.5-11+deb8u8
8.8 (V3)
1 image
No nodes
7

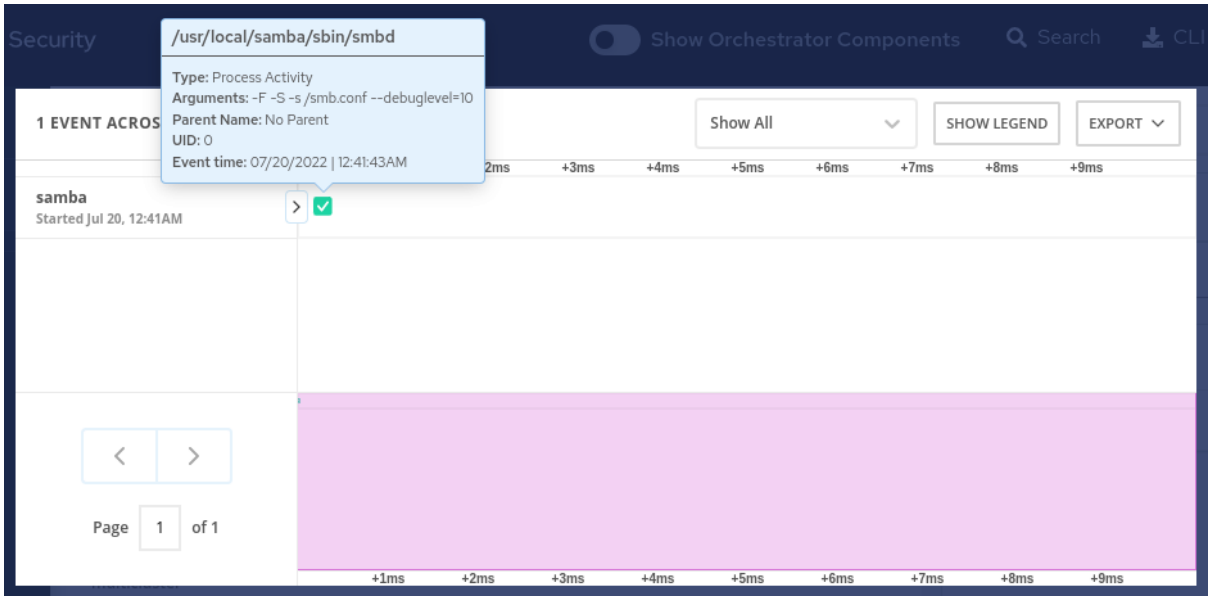

NAMESPACES
Entity List
EXPORT
ALL ENTITIES
ACS-TEST
Namespace
IMAGES
Entity List
docker.io/vulnerables/cve-2017-7494:latest
Image
Observed CVEs
Deferred CVEs
False positive CVEs
Related entities
Select a filter...
Bulk actions
Defer CVE (4)
Mark false positive (4)
1 - 20 of 473
1 of 24
MATCHES
1
DEPLOYMENT
CONTAINS
183
COMPONENTS
473
CVES
CVE
Affected comp...
Discovered
CVE-2019-5482
1 components
07/20/2022 | 12:37:43AM
CVE-2017-12424
No
Critical
9.8
1 components
07/20/2022 | 12:37:43AM
CVE-2017-10989
Yes
Critical
9.8
1 components
07/20/2022 | 12:37:43AM
CVE-2017-10685
Yes
Critical
9.8
1 components
07/20/2022 | 12:37:43AM
CVE-2016-4609
Yes
Critical
9.8
1 components
07/20/2022 | 12:37:43AM
CVE-2018-16839
Yes
Critical
9.8
1 components
07/20/2022 | 12:37:43AM
CVE-2019-12900
Yes
Critical
9.8
1 components
07/20/2022 | 12:37:43AM
CVE-2019-8457
No
Critical
9.8
1 components
07/20/2022 | 12:37:43AM
CVE-2018-1000007
Yes
Critical
9.8
1 components
07/20/2022 | 12:37:43AM
CVE-2019-11068
Yes
Critical
9.8
1 components
07/20/2022 | 12:37:43AM
CVE-2019-12450
Yes
Critical
9.8
1 components
07/20/2022 | 12:37:43AM

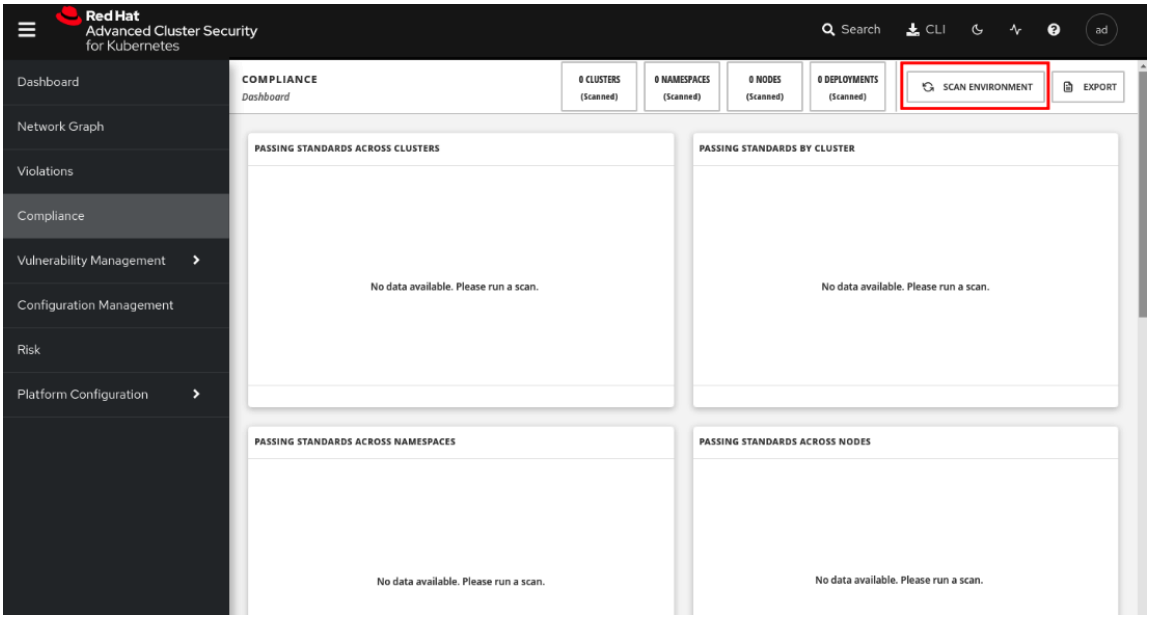

Red Hat
Advanced Cluster Security
for Kubernetes
Search
CLI
ad
Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Dashboard
Risk Acceptance
Reporting
Configuration Management
Risk
Platform Configuration
Risk Acceptance
Pending Approvals
Approved Deferrals
Approved False Positives
Select a filter...
Bulk actions
1 - 4 of 4
1 of 1
Requested entity
Requested action
Expires
Scope
Impacted entities
Comments
Reque...
CVE-2019-5482
Deferral (until fixed)
When fixed
docker.io/vulnerables/cve-2017-7494:latest
1 deployment
1 image
1 comments
admin
CVE-2017-12424
Deferral (until fixed)
When fixed
docker.io/vulnerables/cve-2017-7494:latest
1 deployment
1 image
1 comments
admin
CVE-2017-10685
Deferral (until fixed)
When fixed
docker.io/vulnerables/cve-2017-7494:latest
1 deployment
1 image
1 comments
admin
CVE-2017-10989
Deferral (until fixed)
When fixed
docker.io/vulnerables/cve-2017-7494:latest
1 deployment
1 image
1 comments
admin

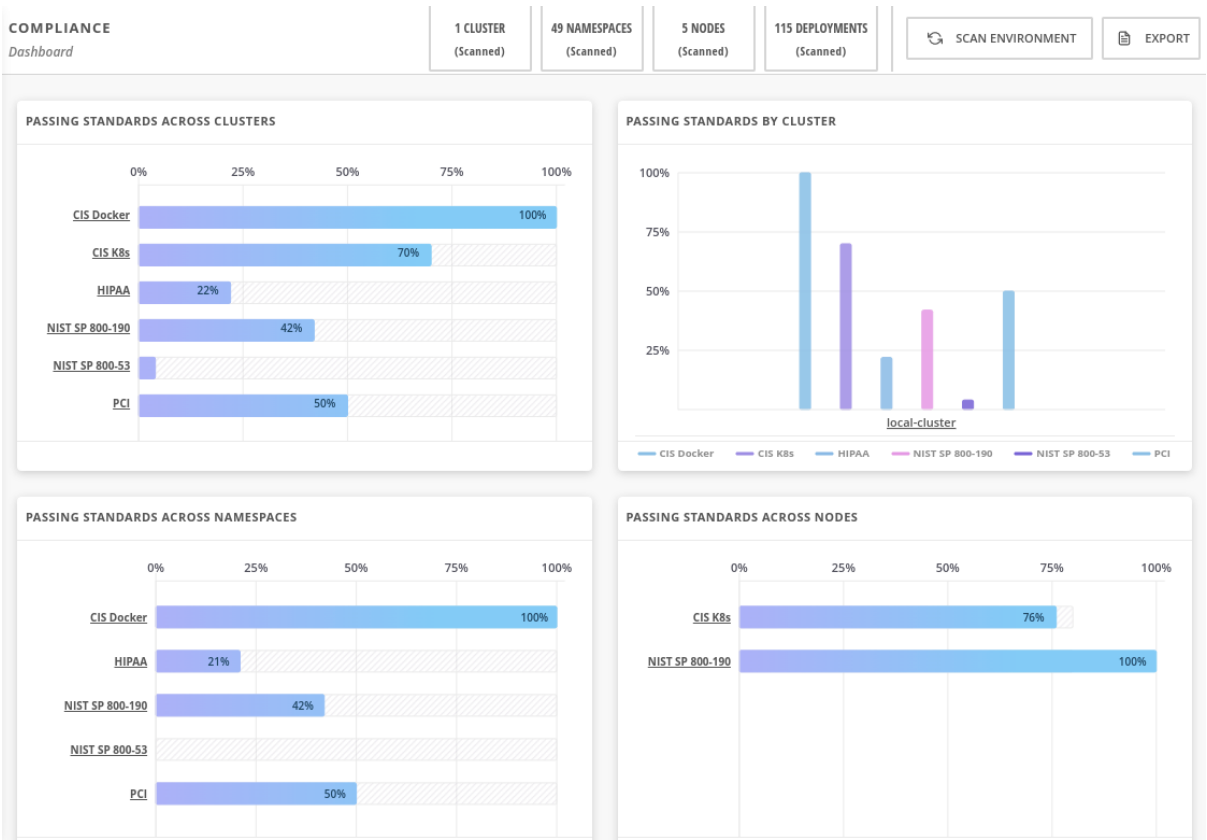

Red Hat
Advanced Cluster Security
for Kubernetes
Show Orchestrator Components
Search
CLI
ad
Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Configuration Management
Risk
Platform Configuration
RISK
Default View
Add one or more resource filters
CREATE POLICY
17 DEPLOYMENTS
Page 1 of 1
Name
Created
Cluster
Namespace
Priority
rhacs-operator-controller-manager
07/15/2022 | 5:57:07PM
local-cluster
rhacs-operator
1
multiclusterhub-operator
07/15/2022 | 7:05:13PM
local-cluster
open-cluster-management
2
samba
07/20/2022 | 12:41:39AM
local-cluster
acs-test
3
collector
07/15/2022 | 7:02:23PM
local-cluster
rhacs-operator
4
multicluster-operators-application
07/15/2022 | 7:05:13PM
local-cluster
open-cluster-management
5
multicluster-operators-channel
07/15/2022 | 7:05:13PM
local-cluster
open-cluster-management
5
multicluster-operators-hub-subscription
07/15/2022 | 7:05:14PM
local-cluster
open-cluster-management
5
multicluster-operators-standalone-subscription
07/15/2022 | 7:05:13PM
local-cluster
open-cluster-management
6
multicluster-operators-subscription-report
07/15/2022 | 7:05:13PM
local-cluster
open-cluster-management
6
multicluster-observability-operator
07/15/2022 | 7:05:13PM
local-cluster
open-cluster-management
7
sensor
07/15/2022 | 7:02:23PM
local-cluster
rhacs-operator
8
submariner-addon
07/15/2022 | 7:05:13PM
local-cluster
open-cluster-management
9

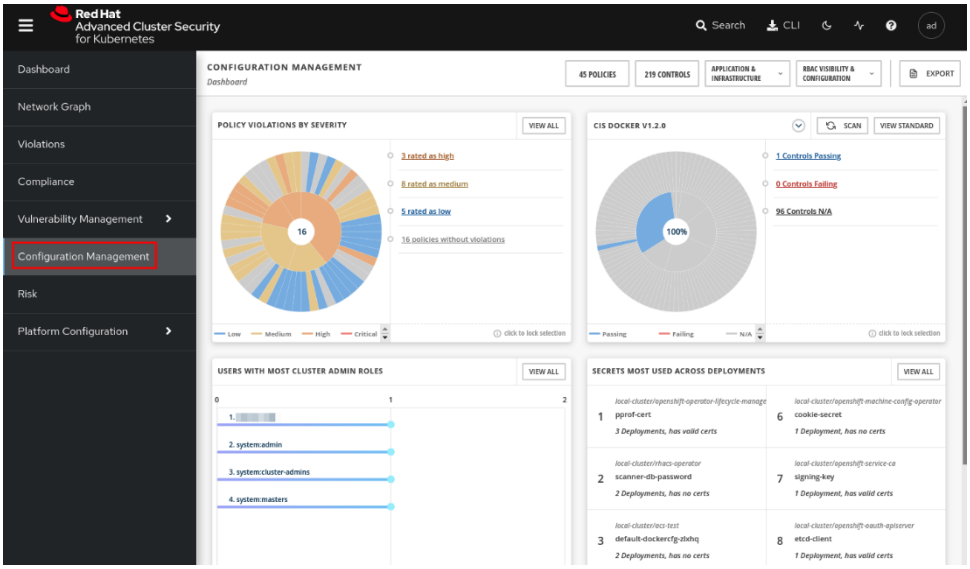

RISK
Default View
Add one or more resource filters
CREATE POLICY
17 DEPLOYMENTS
Page 1 of 1
Name
Created
Cluster
Namespace
Priority
rhacs-operator-controller-manager
07/15/2022 | 5:57:07PM
local-cluster
rhacs-operator
1
multiclusterhub-operator
07/15/2022 | 7:05:13PM
local-cluster
open-cluster-management
2
samba
07/20/2022 | 12:41:39AM
local-cluster
acs-test
3
collector
07/15/2022 | 7:02:23PM
local-cluster
rhacs-operator
4
multicluster-operators-application
07/15/2022 | 7:05:13PM
local-cluster
open-cluster-management
5
multicluster-operators-channel
07/15/2022 | 7:05:13PM
local-cluster
open-cluster-management
5
multicluster-operators-hub-subscription
07/15/2022 | 7:05:14PM
local-cluster
open-cluster-management
5
multicluster-operators-standalone-subscription
07/15/2022 | 7:05:13PM
local-cluster
open-cluster-management
6
multicluster-operators-subscription-report
07/15/2022 | 7:05:13PM
local-cluster
open-cluster-management
6
Samba
RISK INDICATORS
DEPLOYMENT DETAILS
PROCESS DISCOVERY
VIEW DEPLOYMENT IN NETWORK GRAPH
Policy Violations
Fixable Severity at least Important (severity: High)
No resource requests or limits specified (severity: Medium)
Pod Service Account Token Automatically Mounted (severity: Medium)
90-Day Image Age (severity: Low)
Docker CIS 4.1: Ensure That a User for the Container Has Been Created (severity: Low)
Latest tag (severity: Low)
Ubuntu Package Manager in Image (severity: Low)
Image Vulnerabilities
Image "docker.io/vulnerables/cve-2017-7494:latest" contains 503 CVEs with severities ranging between Low and Critical
Service Configuration

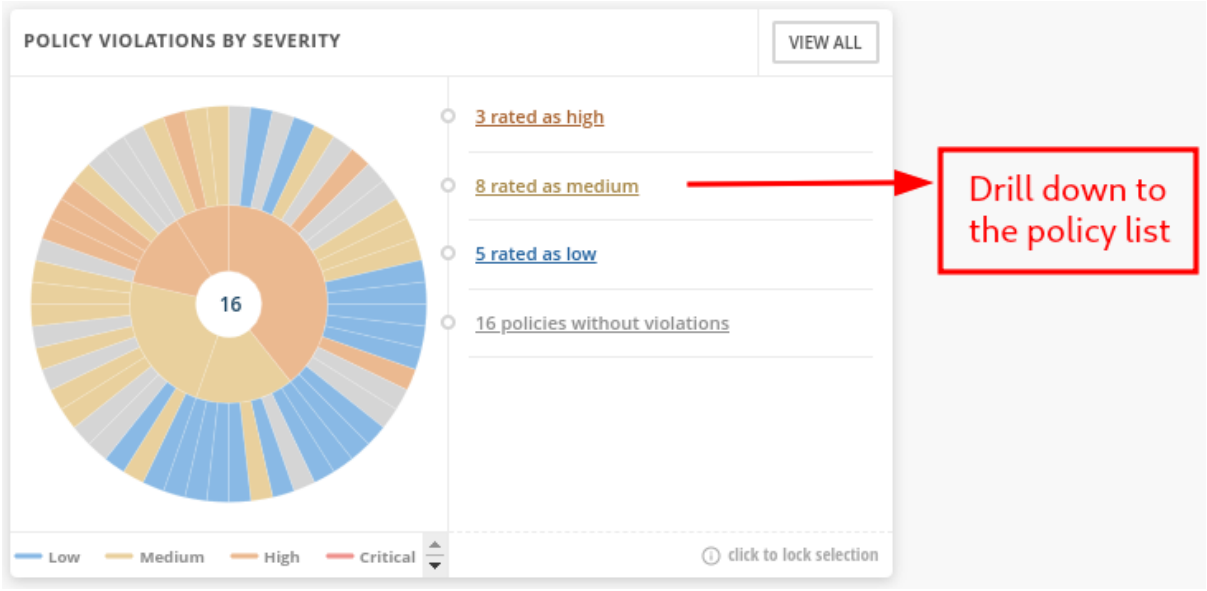

Samba
RISK INDICATORS
DEPLOYMENT DETAILS
PROCESS DISCOVERY
Event Timeline
0
POLICY VIOLATIONS
1
PROCESS ACTIVITY
0
RESTARTS / TERMINATIONS
VIEW GRAPH
Running Processes
/usr/local/samba/sbin/smbd
in container samba
Spec Container Baselines
samba
/usr/local/samba/sbin/smbd

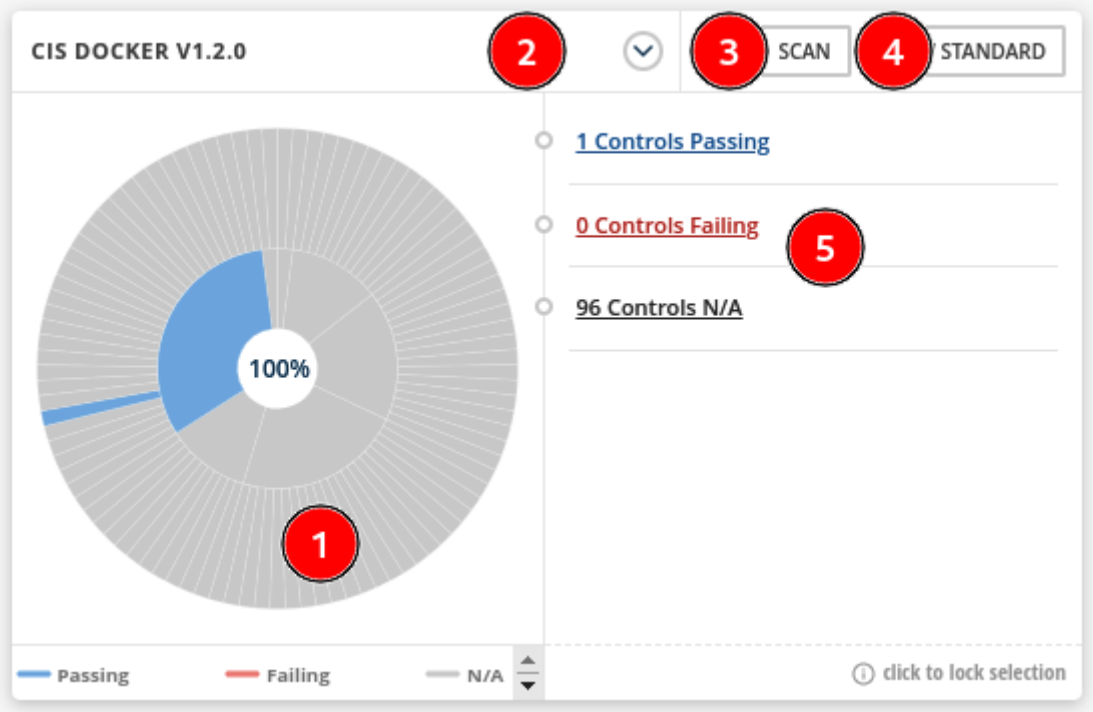

Security
/usr/local/samba/sbin/smbd
Type: Process Activity
Arguments: -F -S -s /smb.conf --debuglevel=10
Parent Name: No Parent
UID: 0
Event time: 07/20/2022 | 12:41:43AM
Show Orchestrator Components
Search
1 EVENT ACROS
Show All
SHOW LEGEND
EXPORT
+2ms
+3ms
+4ms
+5ms
+6ms
+7ms
+8ms
+9ms
samba
Started Jul 20, 12:41AM
Page 1 of 1
+1ms
+2ms
+3ms
+4ms
+5ms
+6ms
+7ms
+8ms
+9ms

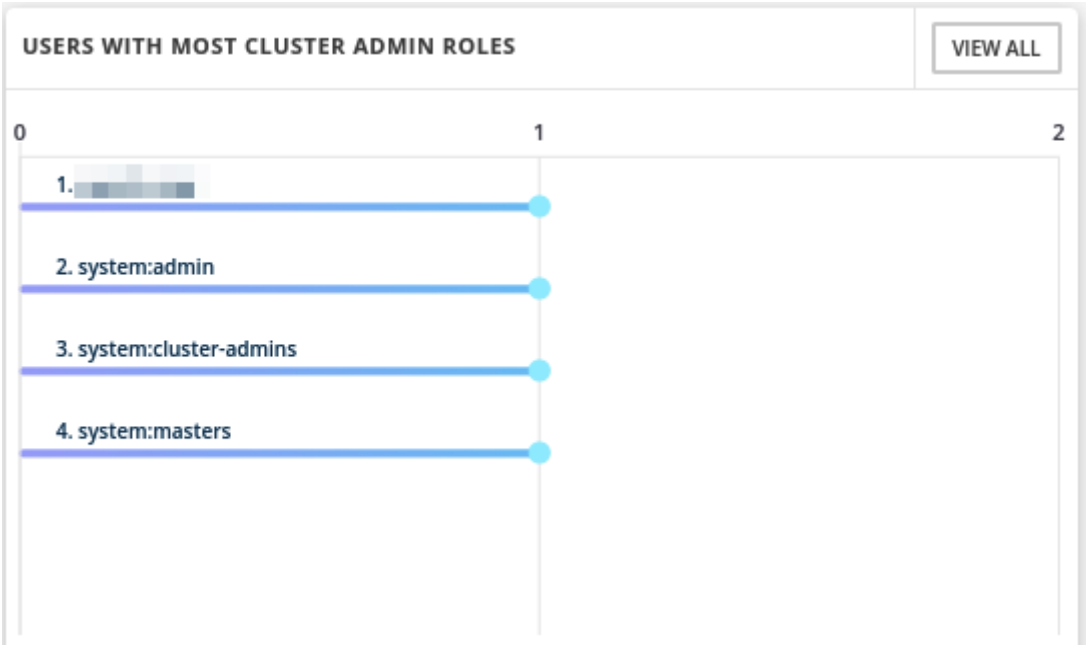

Red Hat
Advanced Cluster Security
for Kubernetes
Search
CLI
ad
Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Configuration Management
Risk
Platform Configuration
COMPLIANCE
Dashboard
0 CLUSTERS (Scanned)
0 NAMESPACES (Scanned)
0 NODES (Scanned)
0 DEPLOYMENTS (Scanned)
SCAN ENVIRONMENT
EXPORT
PASSING STANDARDS ACROSS CLUSTERS
No data available. Please run a scan.
PASSING STANDARDS BY CLUSTER
No data available. Please run a scan.
PASSING STANDARDS ACROSS NAMESPACES
No data available. Please run a scan.
PASSING STANDARDS ACROSS NODES
No data available. Please run a scan.

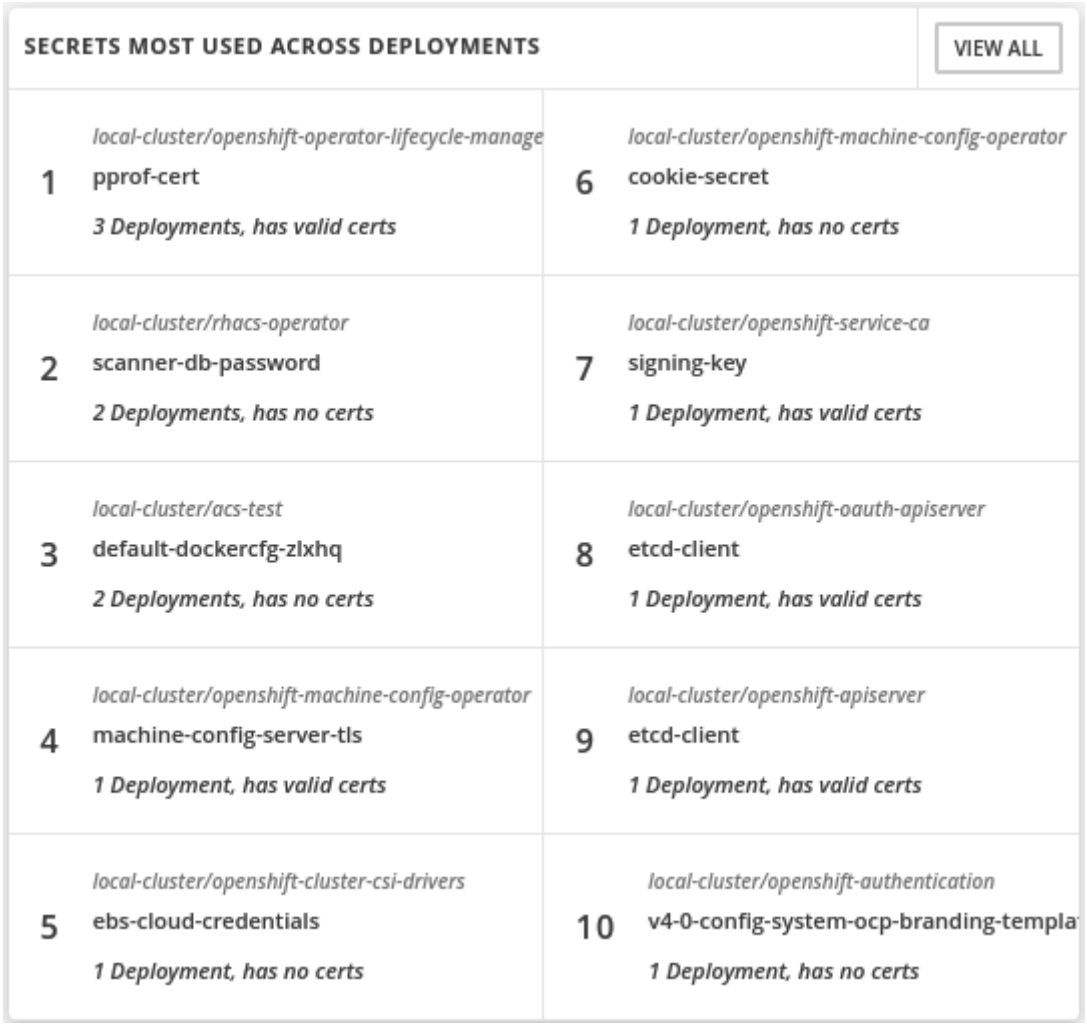

COMPLIANCE
Dashboard
1 CLUSTER (Scanned)
49 NAMESPACES (Scanned)
5 NODES (Scanned)
115 DEPLOYMENTS (Scanned)
SCAN ENVIRONMENT
EXPORT
PASSING STANDARDS ACROSS CLUSTERS
0%
25%
50%
75%
100%
CIS Docker
100%
CIS K8s
70%
HIPAA
22%
NIST SP 800-190
42%
NIST SP 800-53
PCI
50%
PASSING STANDARDS BY CLUSTER
100%
75%
50%
25%
local-cluster
CIS Docker
CIS K8s
HIPAA
NIST SP 800-190
NIST SP 800-53
PCI
PASSING STANDARDS ACROSS NAMESPACES
0%
25%
50%
75%
100%
CIS Docker
100%
HIPAA
21%
NIST SP 800-190
42%
NIST SP 800-53
PCI
50%
PASSING STANDARDS ACROSS NODES
0%
25%
50%
75%
100%
CIS K8s
76%
NIST SP 800-190
100%

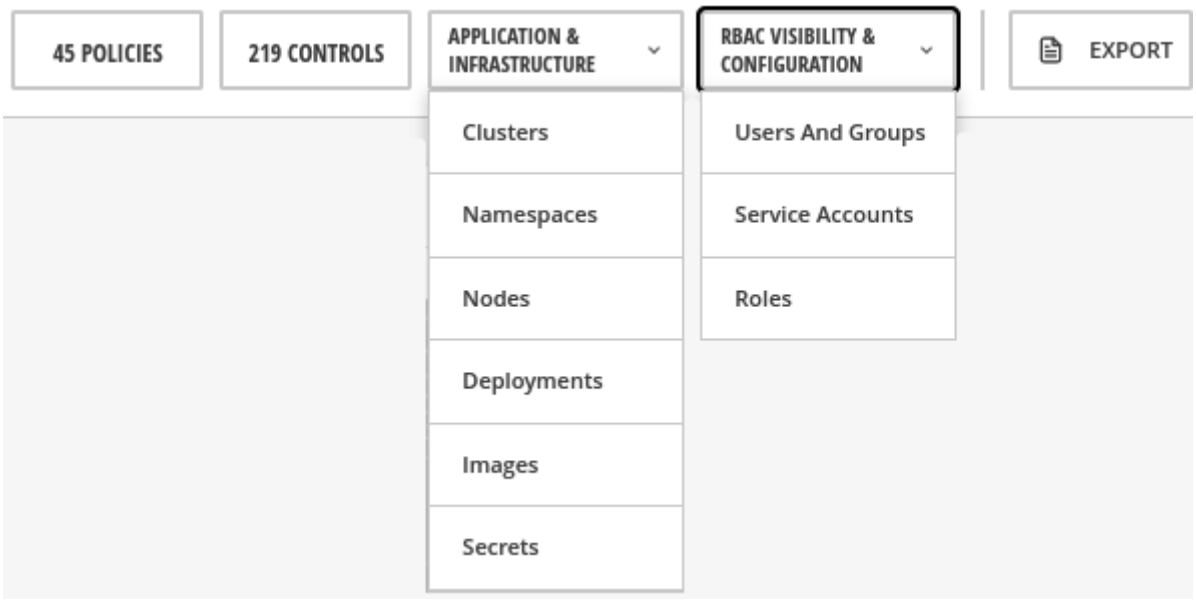

Red Hat
Advanced Cluster Security
for Kubernetes
Search
CLI
Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Configuration Management
Risk
Platform Configuration
CONFIGURATION MANAGEMENT
Dashboard
45 POLICIES
219 CONTROLS
APPLICATION & INFRASTRUCTURE
RBAC VISIBILITY & CONFIGURATION
EXPORT
POLICY VIOLATIONS BY SEVERITY
VIEW ALL
3 rated as high
8 rated as medium
5 rated as low
16 policies without violations
16
CIS DOCKER V1.2.0
SCAN
VIEW STANDARD
1 Controls Passing
0 Controls Failing
96 Controls N/A
100%
USERS WITH MOST CLUSTER ADMIN ROLES
1.
2. system:admin
3. system:cluster-admins
4. system:masters
SECRETS MOST USED ACROSS DEPLOYMENTS
1 pprof-cert
3 Deployments, has valid certs
2 scanner-db-password
2 Deployments, has no certs
3 default-dockercfg-zlxhq
2 Deployments, has no certs
6 cookie-secret
1 Deployment, has no certs
7 signing-key
1 Deployment, has valid certs
8 etcd-client
1 Deployment, has valid certs

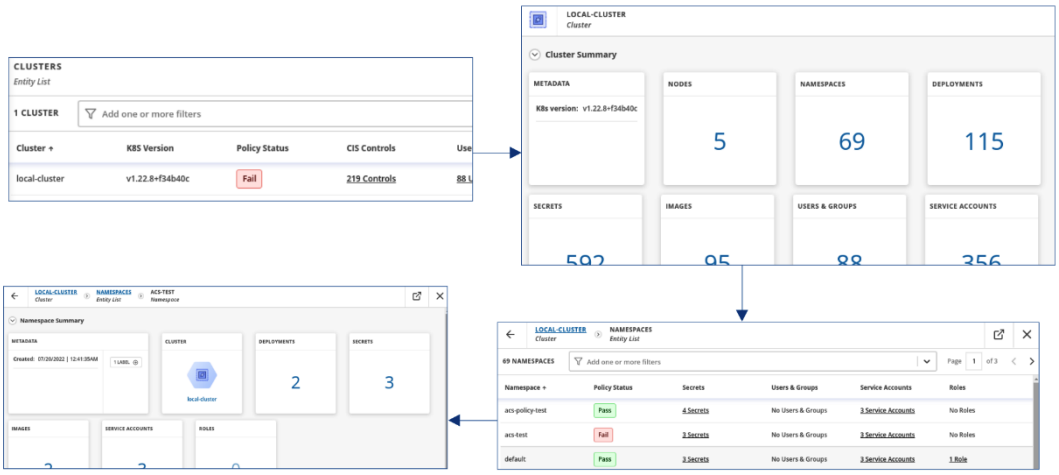

POLICY VIOLATIONS BY SEVERITY
VIEW ALL
3 rated as high
8 rated as medium
5 rated as low
16 policies without violations
16
Low
Medium
High
Critical
click to lock selection
Drill down to the policy list

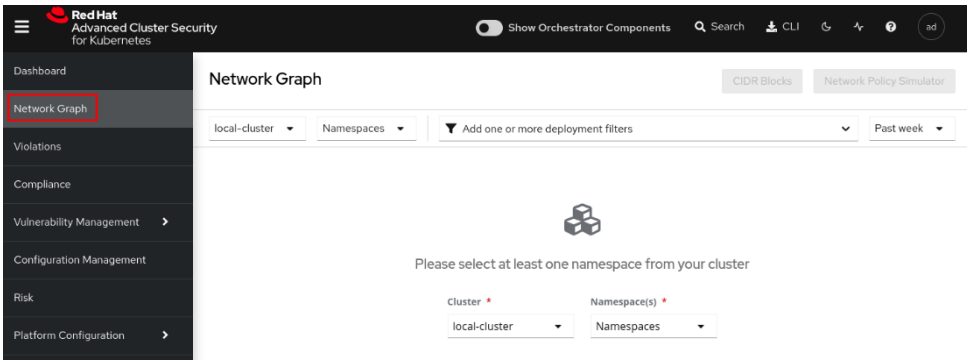

CIS DOCKER V1.2.0
2
3
SCAN
4
STANDARD
1 Controls Passing
0 Controls Failing
5
96 Controls N/A
100%
1
Passing
Failing
N/A
click to lock selection

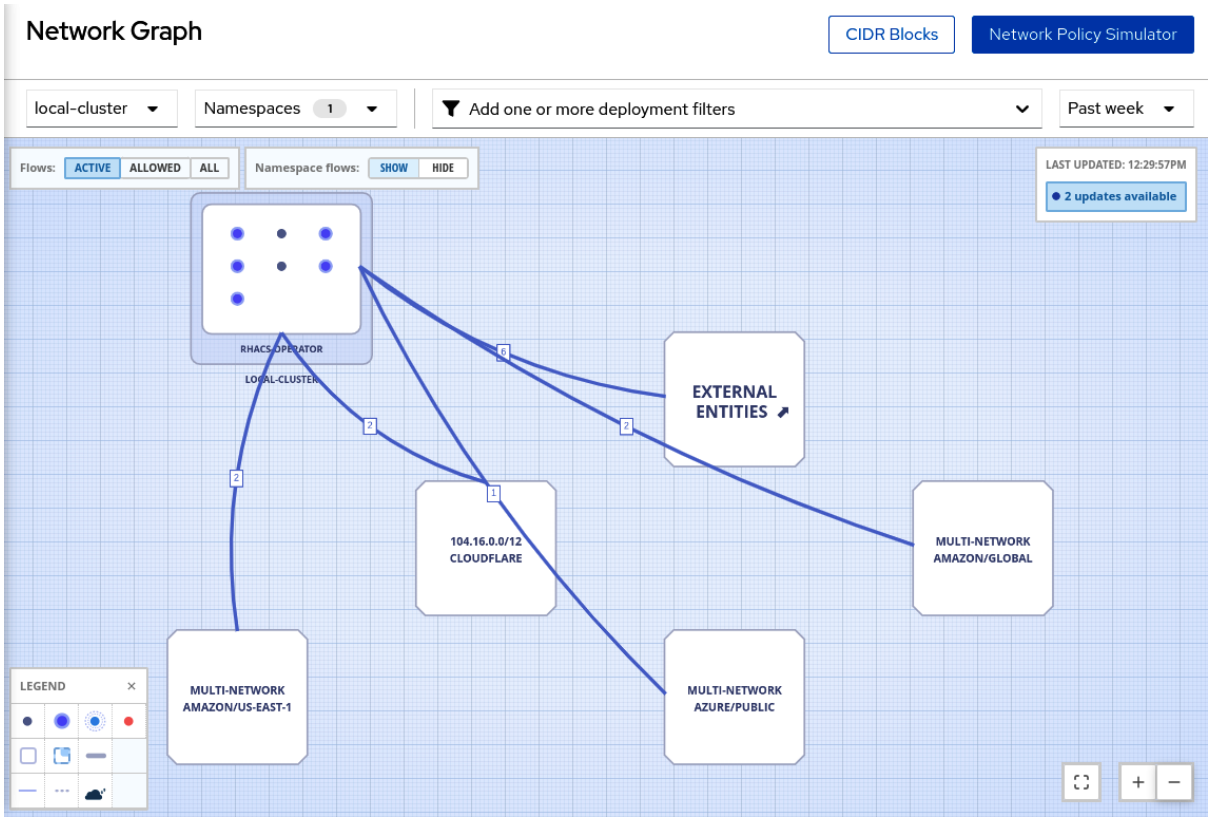

USERS WITH MOST CLUSTER ADMIN ROLES
VIEW ALL
0
1
2
1.
2. system:admin
3. system:cluster-admins
4. system:masters

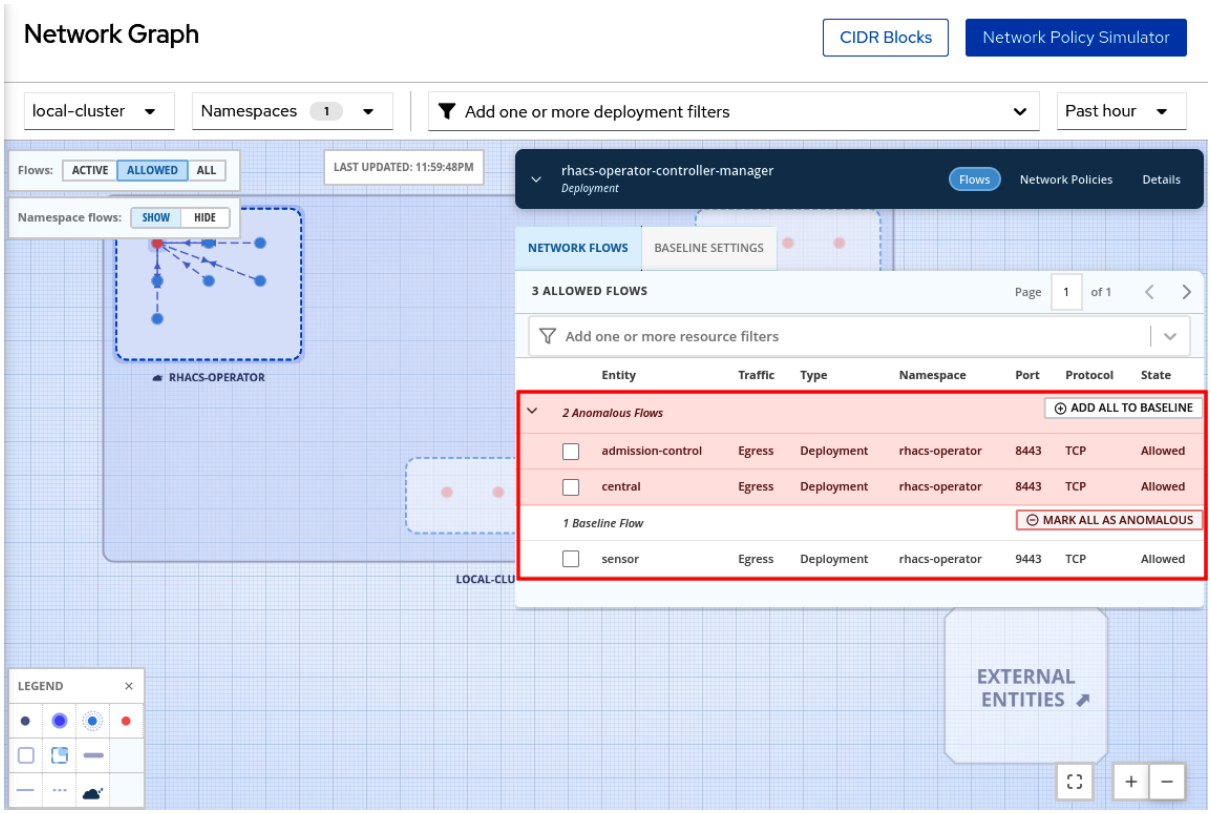

SECRETS MOST USED ACROSS DEPLOYMENTS
VIEW ALL
1
local-cluster/openshift-operator-lifecycle-manage
pprof-cert
3 Deployments, has valid certs
2
local-cluster/rhacs-operator
scanner-db-password
2 Deployments, has no certs
3
local-cluster/acs-test
default-dockercfg-zlxhq
2 Deployments, has no certs
4
local-cluster/openshift-machine-config-operator
machine-config-server-tls
1 Deployment, has valid certs
5
local-cluster/openshift-cluster-csi-drivers
ebs-cloud-credentials
1 Deployment, has no certs
6
local-cluster/openshift-machine-config-operator
cookie-secret
1 Deployment, has no certs
7
local-cluster/openshift-service-ca
signing-key
1 Deployment, has valid certs
8
local-cluster/openshift-oauth-apiserver
etcd-client
1 Deployment, has valid certs
9
local-cluster/openshift-apiserver
etcd-client
1 Deployment, has valid certs
10
local-cluster/openshift-authentication
v4-0-config-system-ocp-branding-templa
1 Deployment, has no certs

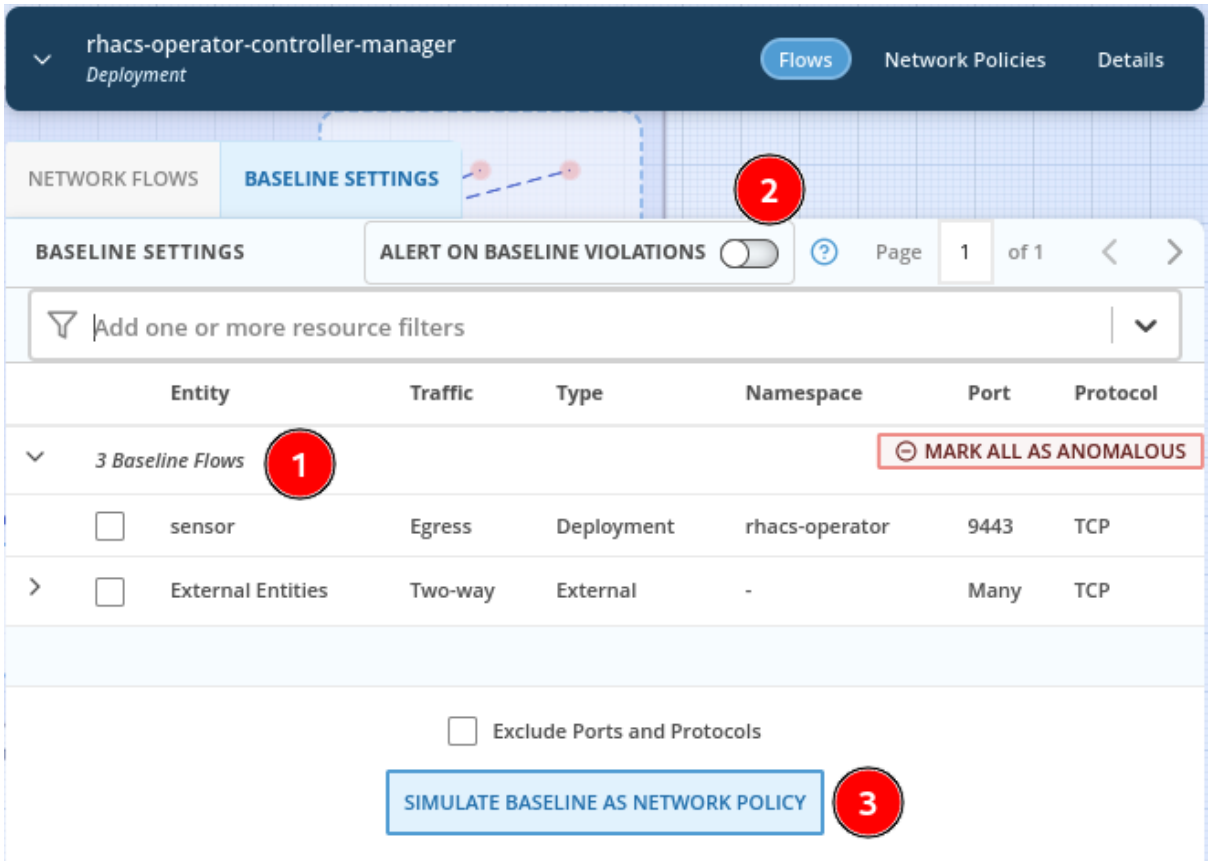

45 POLICIES
219 CONTROLS
APPLICATION & INFRASTRUCTURE
RBAC VISIBILITY & CONFIGURATION
EXPORT
Clusters
Namespaces
Nodes
Deployments
Images
Secrets
Users And Groups
Service Accounts
Roles

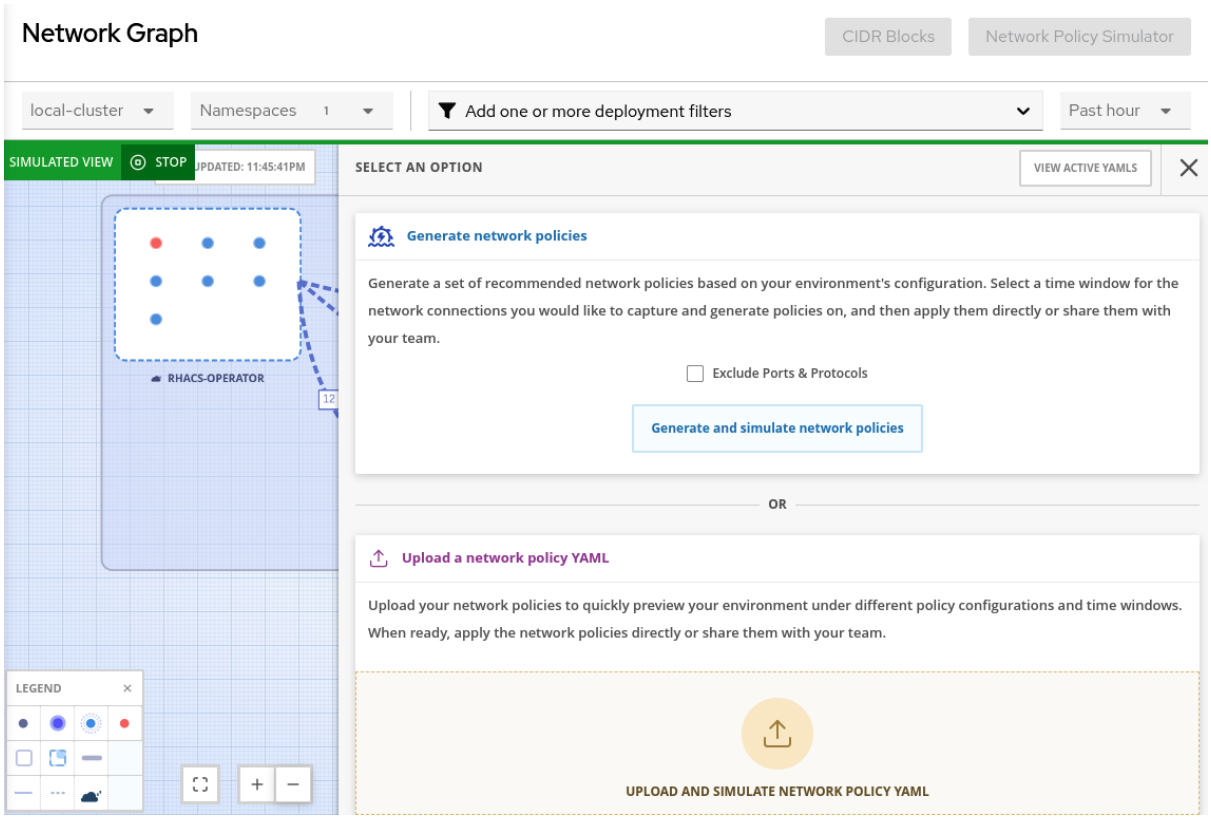

CLUSTERS
Entity List
1 CLUSTER
Add one or more filters
Cluster
K8S Version
Policy Status
CIS Controls
local-cluster
v1.22.8+f34b40c
Fail
219 Controls
LOCAL-CLUSTER
Cluster
Cluster Summary
METADATA
NODES
NAMESPACES
DEPLOYMENTS
5
69
115
SECRETS
IMAGES
USERS & GROUPS
SERVICE ACCOUNTS
592
95
88
356
Namespace Summary
CLUSTER
DEPLOYMENTS
SECRETS
2
3
NAMESPACES
69 NAMESPACES
Add one or more filters
Namespace
Policy Status
Secrets
Users & Groups
Service Accounts
Roles
acs-policy-test
Pass
4 Secrets
No Users & Groups
3 Service Accounts
No Roles
acs-test
Fail
3 Secrets
No Users & Groups
3 Service Accounts
No Roles
default
Pass
3 Secrets
No Users & Groups
3 Service Accounts
1 Role

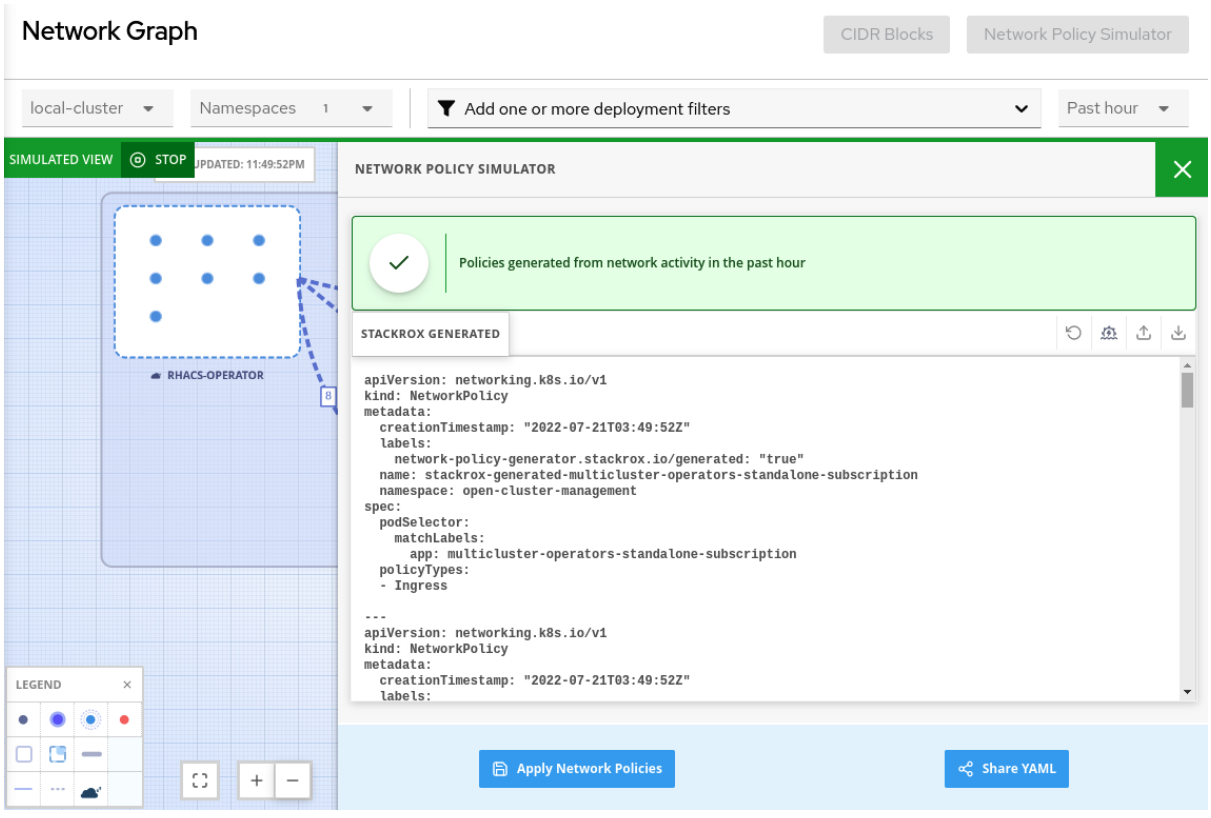

Red Hat
Advanced Cluster Security
for Kubernetes
Show Orchestrator Components
Search
CLI
Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Configuration Management
Risk
Platform Configuration
Network Graph
CIDR Blocks
Network Policy Simulator
local-cluster
Namespaces
Add one or more deployment filters
Past week
Please select at least one namespace from your cluster
Cluster *
Namespace(s) *
local-cluster
Namespaces


Network Graph
CIDR Blocks
Network Policy Simulator
local-cluster
Namespaces 1
Add one or more deployment filters
Past week
Flows: ACTIVE ALLOWED ALL
Namespace flows: SHOW HIDE
LAST UPDATED: 12:29:57PM
2 updates available
RHACS-OPERATOR
LOCAL-CLUSTER
EXTERNAL ENTITIES
104.16.0.0/12
CLOUDFLARE
MULTI-NETWORK
AMAZON/GLOBAL
MULTI-NETWORK
AMAZON/US-EAST-1
MULTI-NETWORK
AZURE/PUBLIC
LEGEND

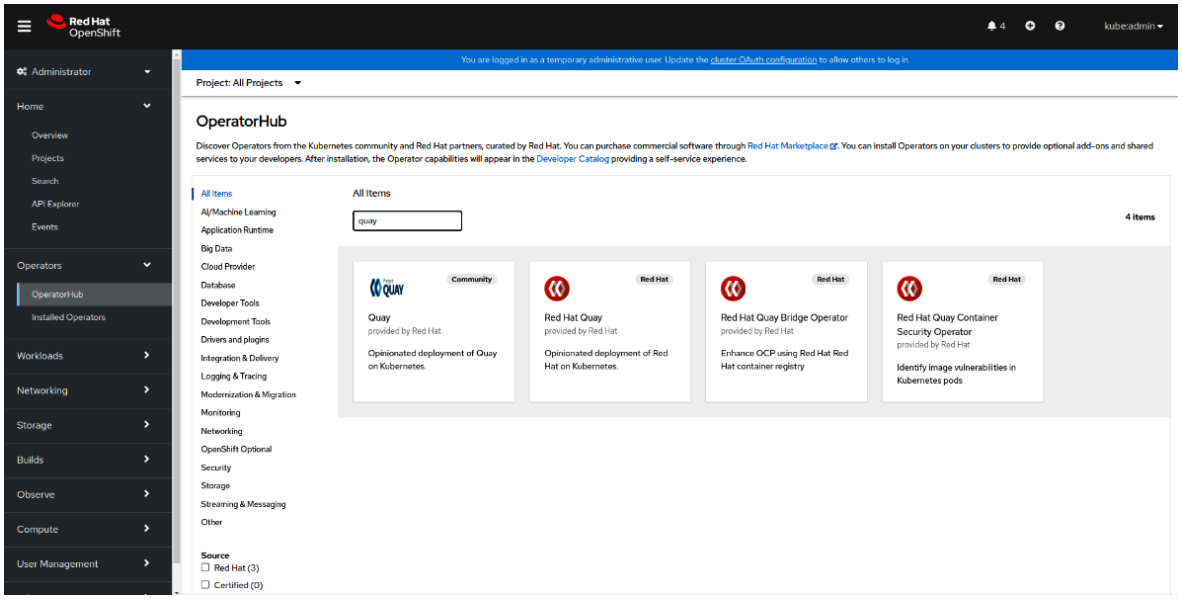

Network Graph
CIDR Blocks
Network Policy Simulator
local-cluster
Namespaces 1
Add one or more deployment filters
Past hour
Flows: ACTIVE ALLOWED ALL
LAST UPDATED: 11:59:48PM
Namespace flows: SHOW HIDE
RHACS-OPERATOR
rhacs-operator-controller-manager
Deployment
Flows
Network Policies
Details
NETWORK FLOWS
BASELINE SETTINGS
3 ALLOWED FLOWS
Page 1 of 1
Add one or more resource filters
Entity
Traffic
Type
Namespace
Port
Protocol
State
2 Anomalous Flows
ADD ALL TO BASELINE
admission-control Egress Deployment rhacs-operator 8443 TCP Allowed
central Egress Deployment rhacs-operator 8443 TCP Allowed
1 Baseline Flow
MARK ALL AS ANOMALOUS
sensor Egress Deployment rhacs-operator 9443 TCP Allowed
LEGEND
EXTERNAL ENTITIES

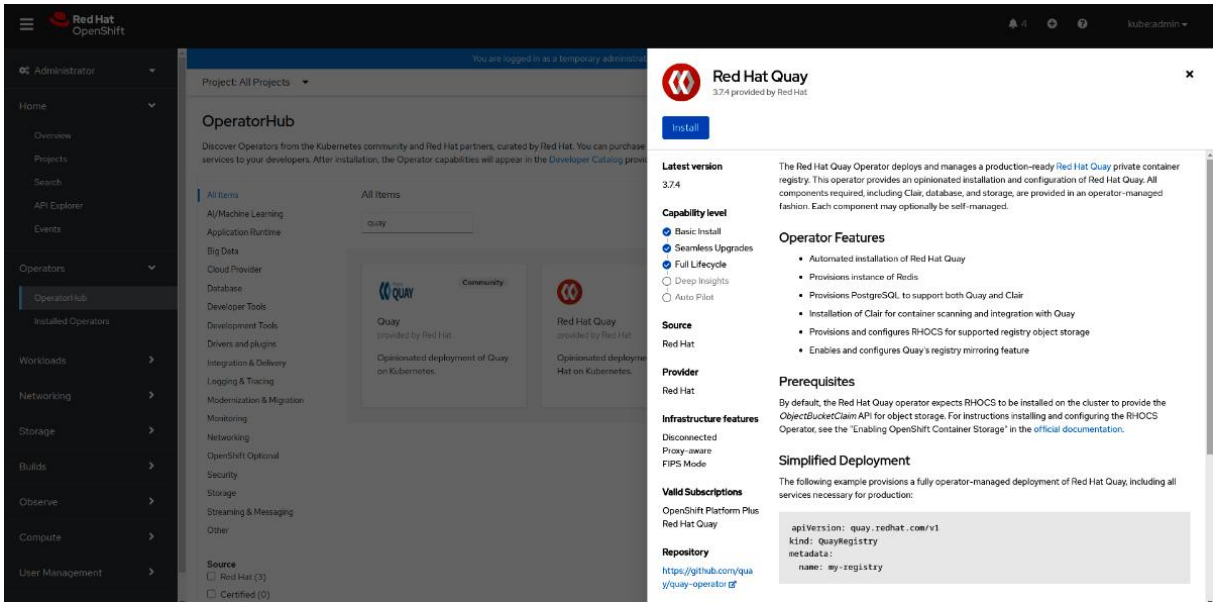

rhacs-operator-controller-manager
Deployment
Flows
Network Policies
Details
NETWORK FLOWS
BASELINE SETTINGS
2
BASELINE SETTINGS
ALERT ON BASELINE VIOLATIONS
Page 1 of 1
Add one or more resource filters
Entity
Traffic
Type
Namespace
Port
Protocol
3 Baseline Flows
1
MARK ALL AS ANOMALOUS
sensor Egress Deployment rhacs-operator 9443 TCP
External Entities Two-way External - Many TCP
Exclude Ports and Protocols
SIMULATE BASELINE AS NETWORK POLICY
3

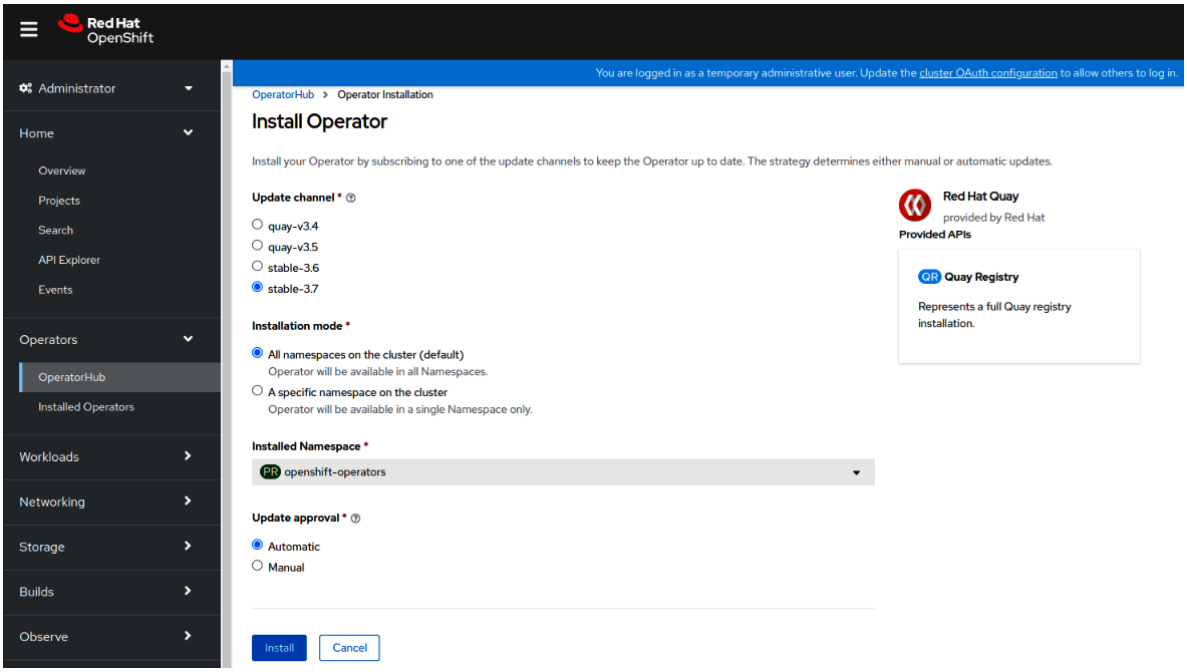

Network Graph
CIDR Blocks
Network Policy Simulator
local-cluster
Namespaces 1
Add one or more deployment filters
Past hour
SIMULATED VIEW
STOP
UPDATED: 11:45:41PM
SELECT AN OPTION
VIEW ACTIVE YAMLS
Generate network policies
Generate a set of recommended network policies based on your environment's configuration. Select a time window for the network connections you would like to capture and generate policies on, and then apply them directly or share them with your team.
Exclude Ports & Protocols
Generate and simulate network policies
OR
Upload a network policy YAML
Upload your network policies to quickly preview your environment under different policy configurations and time windows. When ready, apply the network policies directly or share them with your team.
UPLOAD AND SIMULATE NETWORK POLICY YAML
RHACS-OPERATOR
LEGEND

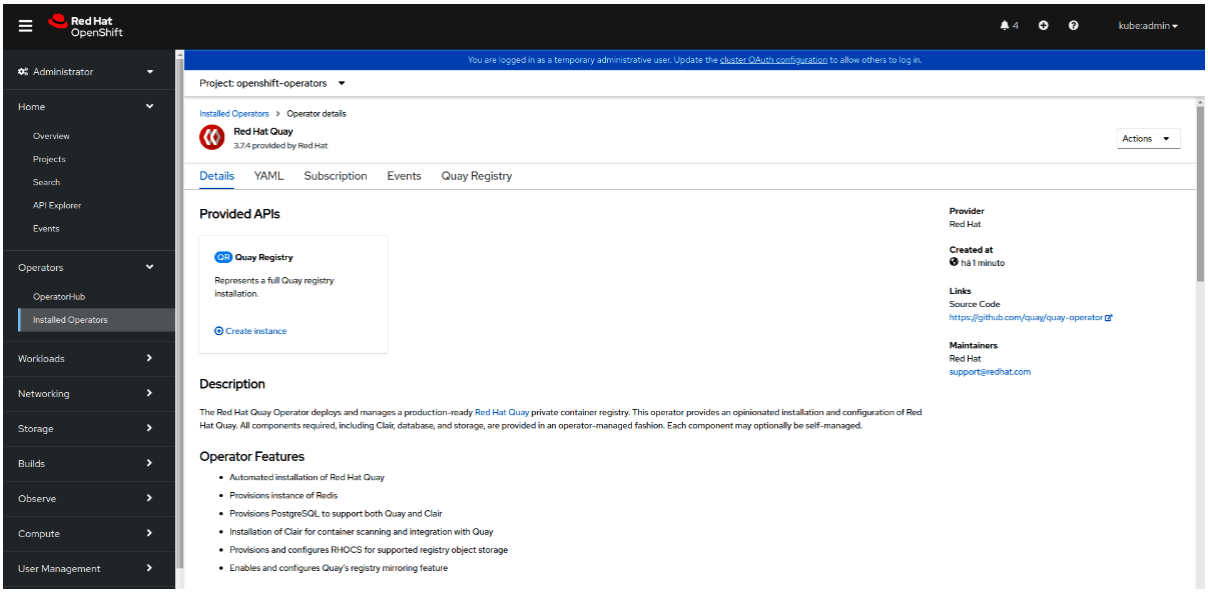

Network Graph
CIDR Blocks
Network Policy Simulator
local-cluster
Namespaces 1
Add one or more deployment filters
Past hour
SIMULATED VIEW
STOP
UPDATED: 11:49:52PM
NETWORK POLICY SIMULATOR
Policies generated from network activity in the past hour
STACKROX GENERATED
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
creationTimestamp: "2022-07-21T03:49:52Z"
labels:
network-policy-generator.stackrox.io/generated: "true"
name: stackrox-generated-multicluster-operators-standalone-subscription
namespace: open-cluster-management
spec:
podSelector:
matchLabels:
app: multicluster-operators-standalone-subscription
policyTypes:
- Ingress
---
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
creationTimestamp: "2022-07-21T03:49:52Z"
labels:
Apply Network Policies
Share YAML
RHACS-OPERATOR
LEGEND

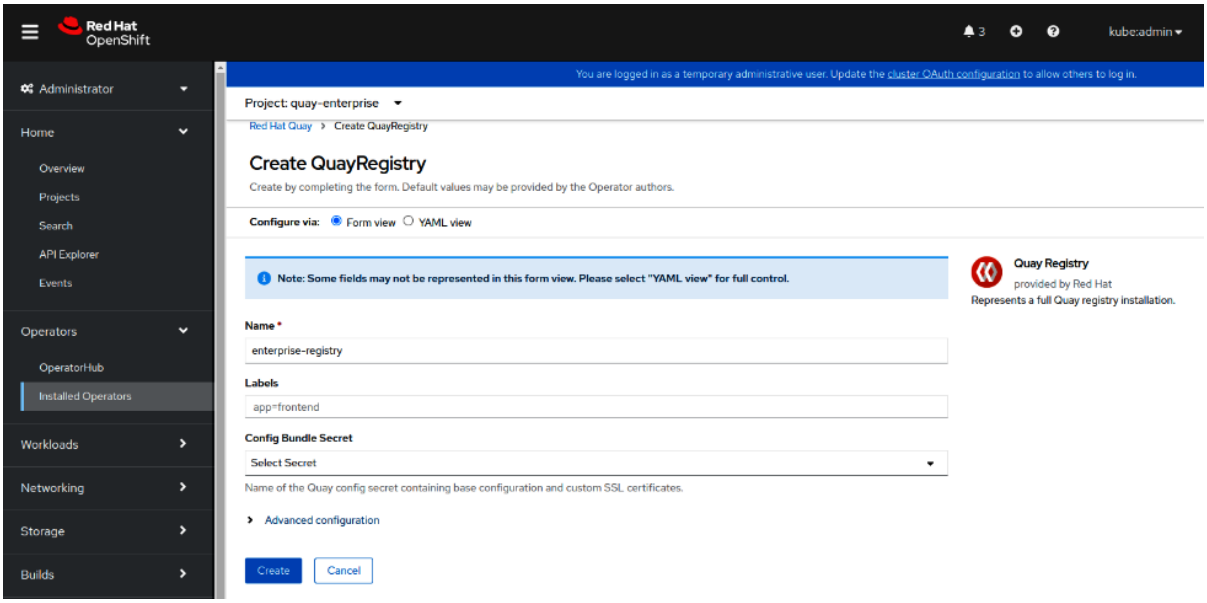
Chapter 13: OpenShift Plus – a Multi-Cluster Enterprise Ready Solution

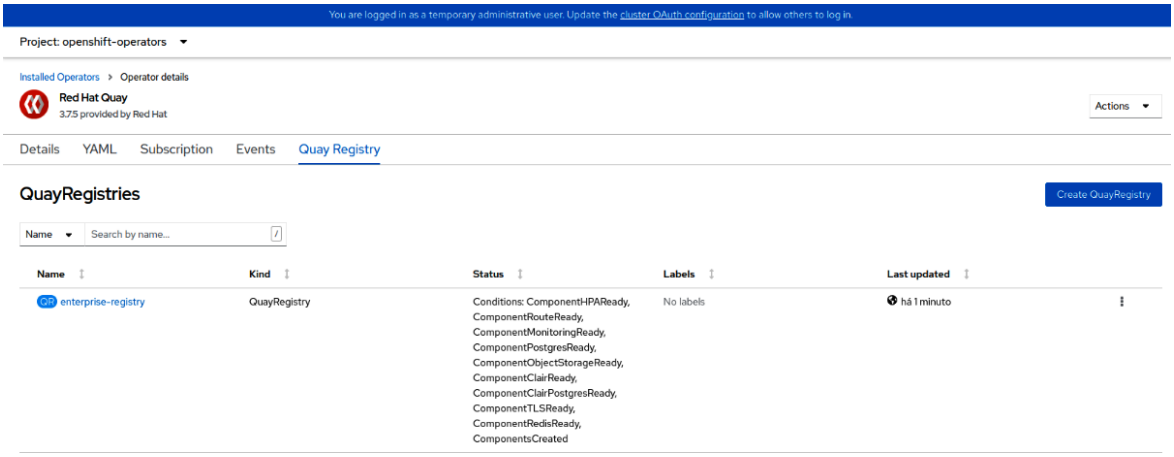


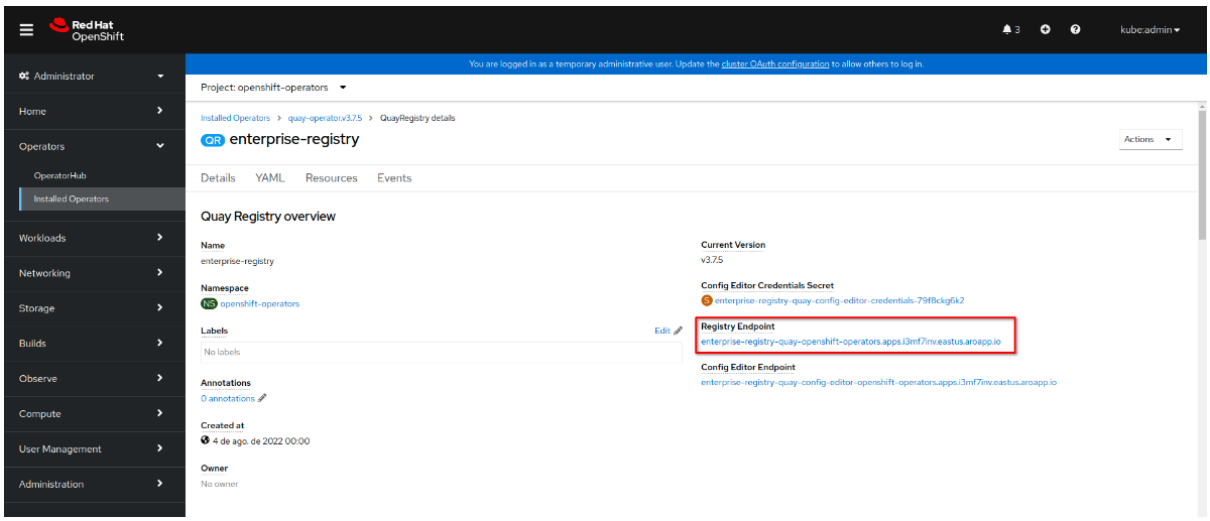


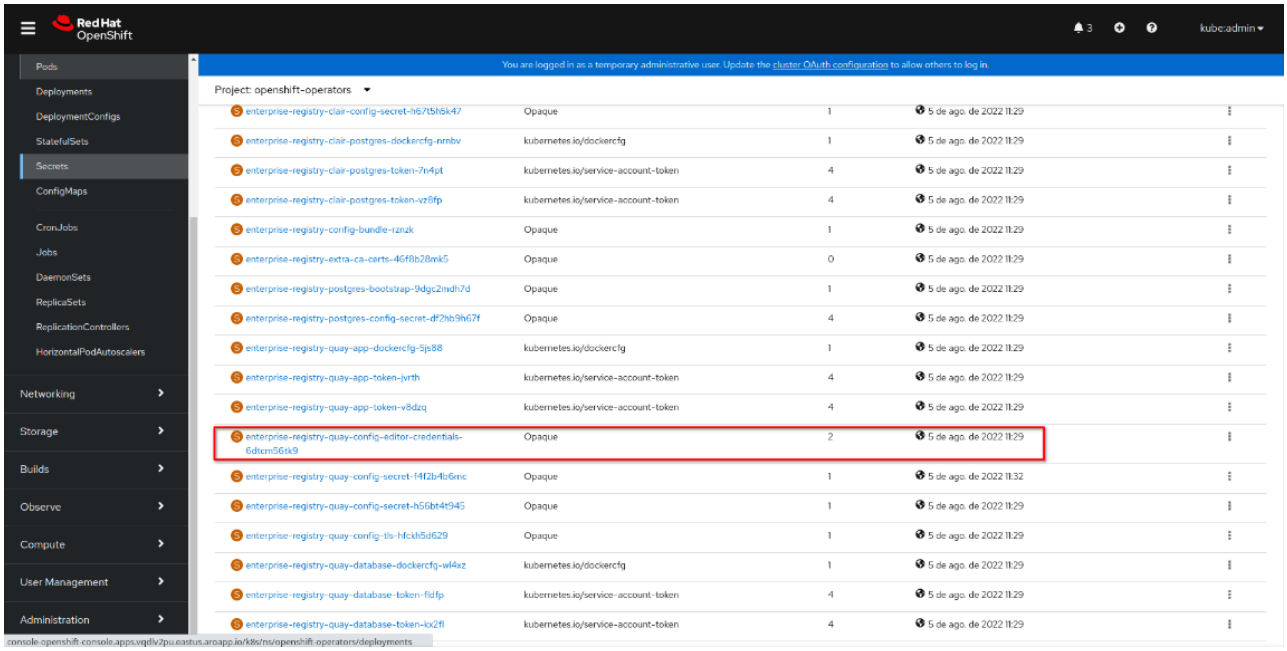

Red Hat OpenShift
Administrator
Home
Overview
Projects
Search
API Explorer
Events
Operators
OperatorHub
Installed Operators
Workloads
Networking
Storage
Builds
Observe
You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in.
OperatorHub > Operator Installation
Install Operator
Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.
Update channel *
quay-v3.4
quay-v3.5
stable-3.6
stable-3.7
Installation mode *
All namespaces on the cluster (default)
Operator will be available in all Namespaces.
A specific namespace on the cluster
Operator will be available in a single Namespace only.
Installed Namespace *
openshift-operators
Update approval *
Automatic
Manual
Install
Cancel
Red Hat Quay
provided by Red Hat
Provided APIs
Quay Registry
Represents a full Quay registry installation.

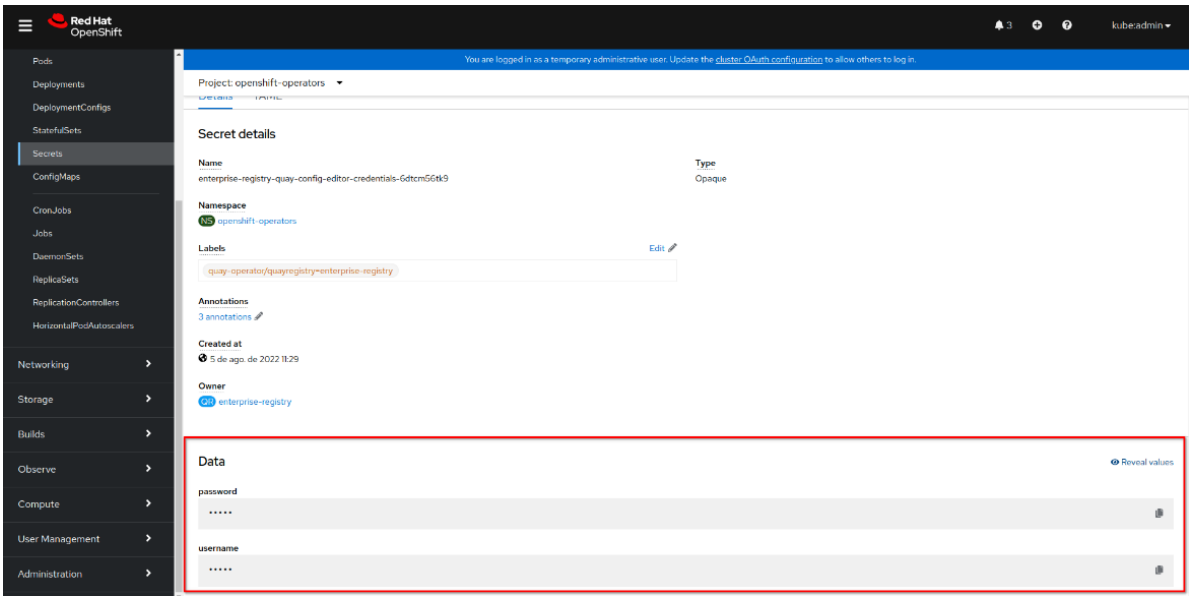

Red Hat OpenShift
kube:admin
Administrator
Home
Overview
Projects
Search
API Explorer
Events
Operators
OperatorHub
Installed Operators
Workloads
Networking
Storage
Builds
Observe
Compute
User Management
You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in.
Project: openshift-operators
Installed Operators > Operator details
Red Hat Quay
3.7.4 provided by Red Hat
Actions
Details
YAML
Subscription
Events
Quay Registry
Provided APIs
Quay Registry
Represents a full Quay registry installation.
Create instance
Provider
Red Hat
Created at
há 1 minuto
Links
Source Code
https://github.com/quay/quay-operator
Maintainers
Red Hat
support@redhat.com
Description
The Red Hat Quay Operator deploys and manages a production-ready Red Hat Quay private container registry. This operator provides an opinionated installation and configuration of Red Hat Quay. All components required, including Clair, database, and storage, are provided in an operator-managed fashion. Each component may optionally be self-managed.
Operator Features
Automated installation of Red Hat Quay
Provisions instance of Redis
Provisions PostgreSQL to support both Quay and Clair
Installation of Clair for container scanning and integration with Quay
Provisions and configures RHOCS for supported registry object storage
Enables and configures Quay's registry mirroring feature

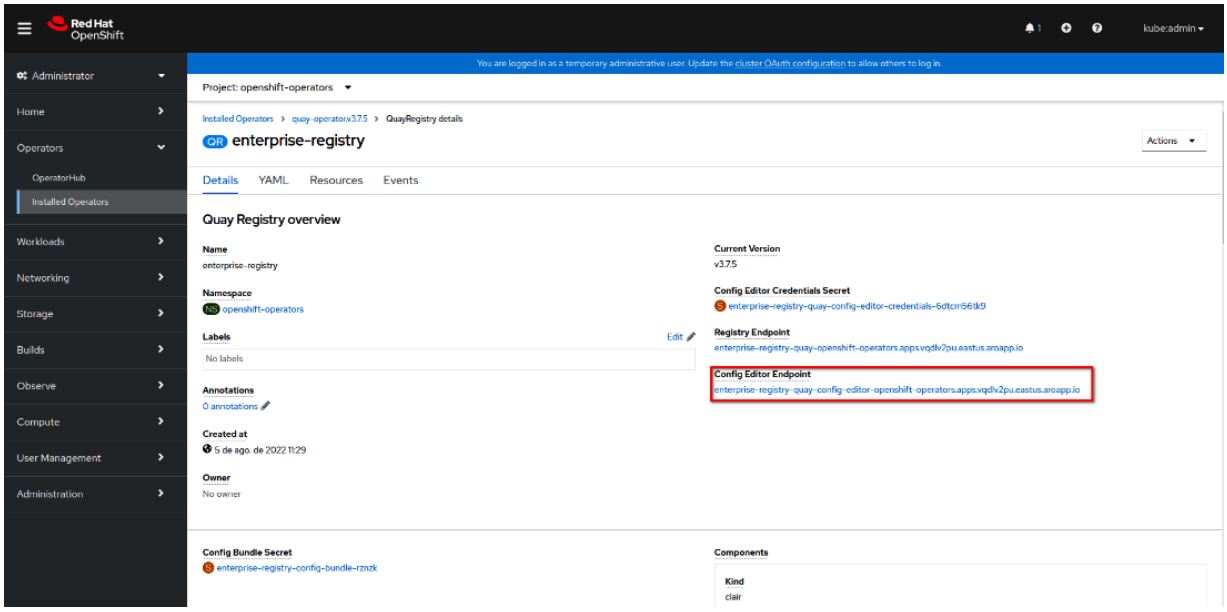

Red Hat OpenShift
kube:admin
You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in.
Administrator
Home
Overview
Projects
Search
API Explorer
Events
Operators
OperatorHub
Installed Operators
Workloads
Networking
Storage
Builds
Project: quay-enterprise
Red Hat Quay > Create QuayRegistry
Create QuayRegistry
Create by completing the form. Default values may be provided by the Operator authors.
Configure via: Form view YAML view
Note: Some fields may not be represented in this form view. Please select "YAML view" for full control.
Quay Registry
provided by Red Hat
Represents a full Quay registry installation.
Name *
enterprise-registry
Labels
app=frontend
Config Bundle Secret
Select Secret
Name of the Quay config secret containing base configuration and custom SSL certificates.
Advanced configuration
Create
Cancel

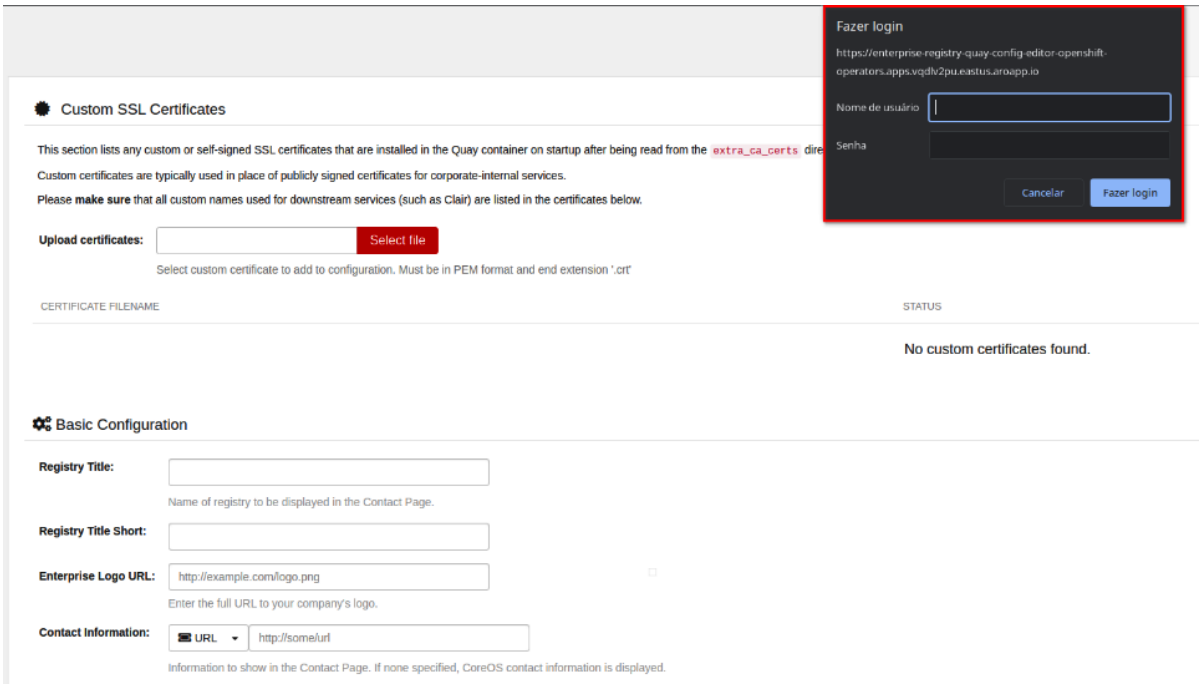

You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in.
Project: openshift-operators
Installed Operators > Operator details
Red Hat Quay
3.7.5 provided by Red Hat
Actions
Details
YAML
Subscription
Events
Quay Registry
QuayRegistries
Create QuayRegistry
Name
Search by name...
Name
Kind
Status
Labels
Last updated
enterprise-registry
QuayRegistry
Conditions: ComponentHPAReady, ComponentRouteReady, ComponentMonitoringReady, ComponentPostgresReady, ComponentObjectStorageReady, ComponentClairReady, ComponentClairPostgresReady, ComponentTLSReady, ComponentRedisReady, ComponentsCreated
No labels
há 1 minuto

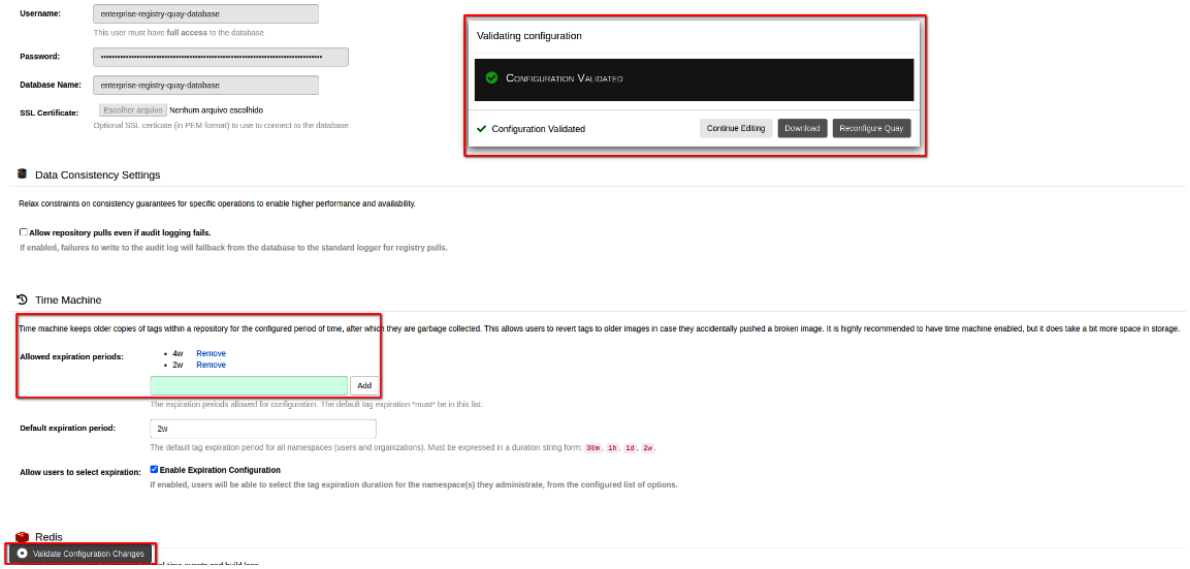

Red Hat OpenShift
kube:admin
You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in.
Administrator
Home
Operators
OperatorHub
Installed Operators
Workloads
Networking
Storage
Builds
Observe
Compute
User Management
Administration
Project: openshift-operators
Installed Operators > quay-operator.v3.7.5 > QuayRegistry details
enterprise-registry
Actions
Details
YAML
Resources
Events
Quay Registry overview
Name
enterprise-registry
Namespace
openshift-operators
Labels
Edit
No labels
Annotations
0 annotations
Created at
4 de ago. de 2022 00:00
Owner
No owner
Current Version
v3.7.5
Config Editor Credentials Secret
enterprise-registry-quay-config-editor-credentials-79f8ckg6k2
Registry Endpoint
enterprise-registry-quay-openshift-operators.apps.i3mf7inv.eastus.aroapp.io
Config Editor Endpoint
enterprise-registry-quay-config-editor-openshift-operators.apps.i3mf7inv.eastus.aroapp.io

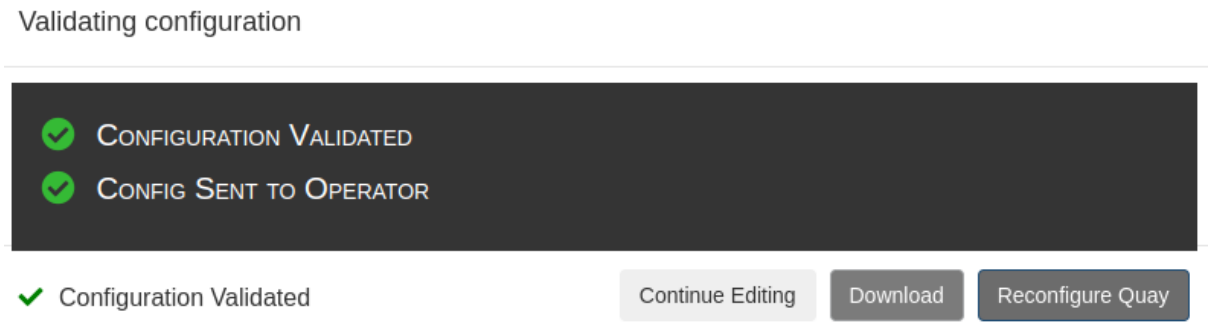

Red Hat OpenShift
kube:admin
You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in.
Project: openshift-operators
Pods
Deployments
DeploymentConfigs
StatefulSets
Secrets
ConfigMaps
CronJobs
Jobs
DaemonSets
ReplicaSets
ReplicationControllers
HorizontalPodAutoscalers
Networking
Storage
Builds
Observe
Compute
User Management
Administration
enterprise-registry-clair-config-secret-h67t5h5k47 Opaque 1 5 de ago. de 2022 11:29
enterprise-registry-clair-postgres-dockercfg-nrnbv kubernetes.io/dockercfg 1 5 de ago. de 2022 11:29
enterprise-registry-clair-postgres-token-7n4pt kubernetes.io/service-account-token 4 5 de ago. de 2022 11:29
enterprise-registry-clair-postgres-token-vz8fp kubernetes.io/service-account-token 4 5 de ago. de 2022 11:29
enterprise-registry-config-bundle-rznzk Opaque 1 5 de ago. de 2022 11:29
enterprise-registry-extra-ca-certs-46f8b28mk5 Opaque 0 5 de ago. de 2022 11:29
enterprise-registry-postgres-bootstrap-9dgc2mdh7d Opaque 1 5 de ago. de 2022 11:29
enterprise-registry-postgres-config-secret-df2hb9h67f Opaque 4 5 de ago. de 2022 11:29
enterprise-registry-quay-app-dockercfg-5js88 kubernetes.io/dockercfg 1 5 de ago. de 2022 11:29
enterprise-registry-quay-app-token-jvrth kubernetes.io/service-account-token 4 5 de ago. de 2022 11:29
enterprise-registry-quay-app-token-v8dzq kubernetes.io/service-account-token 4 5 de ago. de 2022 11:29
enterprise-registry-quay-config-editor-credentials-6dtcm56tk9 Opaque 2 5 de ago. de 2022 11:29
enterprise-registry-quay-config-secret-f4f2b4b6mc Opaque 1 5 de ago. de 2022 11:32
enterprise-registry-quay-config-secret-h56bt4t945 Opaque 1 5 de ago. de 2022 11:29
enterprise-registry-quay-config-tls-hfckh5d629 Opaque 1 5 de ago. de 2022 11:29
enterprise-registry-quay-database-dockercfg-wl4xz kubernetes.io/dockercfg 1 5 de ago. de 2022 11:29
enterprise-registry-quay-database-token-fldfp kubernetes.io/service-account-token 4 5 de ago. de 2022 11:29
enterprise-registry-quay-database-token-kx2fl kubernetes.io/service-account-token 4 5 de ago. de 2022 11:29
console-openshift-console.apps.vqdlv2pu.eastus.aroapp.io/k8s/ns/openshift-operators/deployments

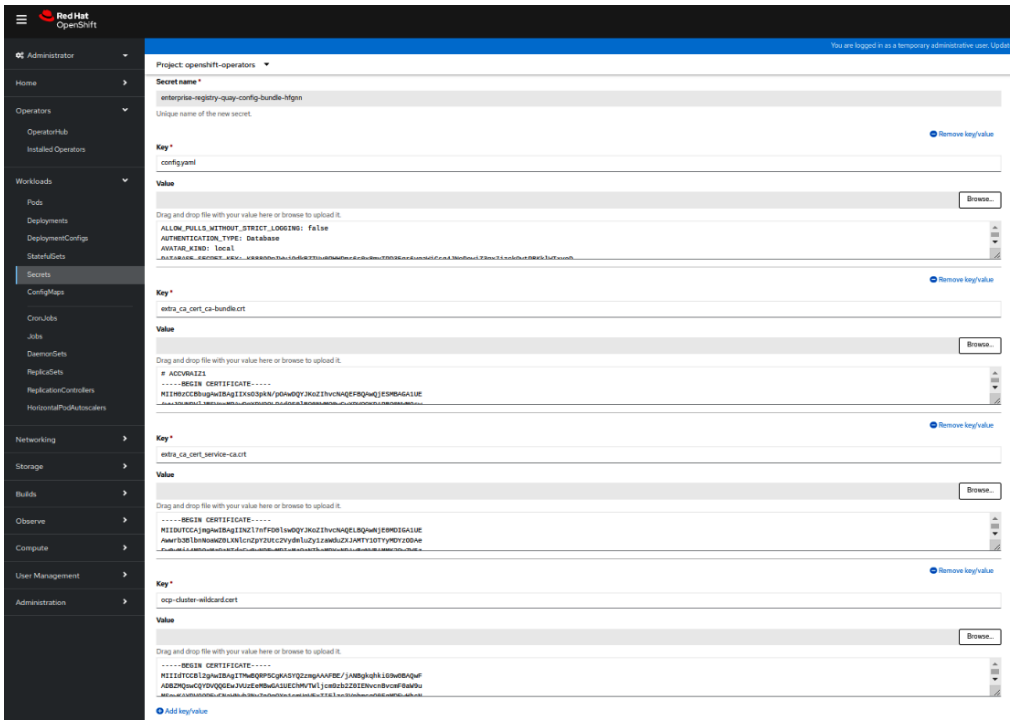

Red Hat OpenShift
kube:admin
You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in.
Project: openshift-operators
Pods
Deployments
DeploymentConfigs
StatefulSets
Secrets
ConfigMaps
CronJobs
Jobs
DaemonSets
ReplicaSets
ReplicationControllers
HorizontalPodAutoscalers
Networking
Storage
Builds
Observe
Compute
User Management
Administration
Secret details
Name
enterprise-registry-quay-config-editor-credentials-6dtcm56tk9
Type
Opaque
Namespace
NS openshift-operators
Labels
Edit
quay-operator/quayregistry=enterprise-registry
Annotations
3 annotations
Created at
5 de ago. de 2022 11:29
Owner
OW enterprise-registry
Data
Reveal values
password
*****
username
*****

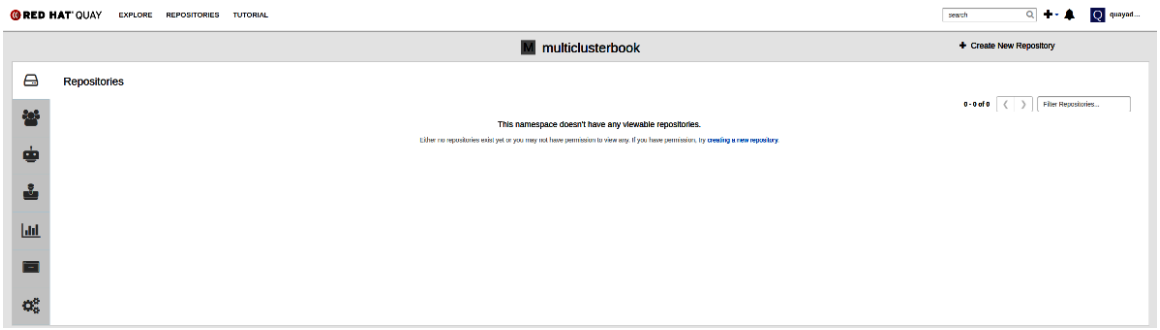

Red Hat OpenShift
kube:admin
You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in.
Administrator
Home
Operators
OperatorHub
Installed Operators
Workloads
Networking
Storage
Builds
Observe
Compute
User Management
Administration
Project: openshift-operators
Installed Operators > quay-operator.v3.7.5 > QuayRegistry details
QR enterprise-registry
Actions
Details
YAML
Resources
Events
Quay Registry overview
Name
enterprise-registry
Namespace
NS openshift-operators
Labels
Edit
No labels
Annotations
0 annotations
Created at
5 de ago. de 2022 11:29
Owner
No owner
Current Version
v3.7.5
Config Editor Credentials Secret
enterprise-registry-quay-config-editor-credentials-6dtcm561k9
Registry Endpoint
enterprise-registry-quay-openshift-operators.apps.vqdlv2pu.eastus.aroapp.io
Config Editor Endpoint
enterprise-registry-quay-config-editor-openshift-operators.apps.vqdlv2pu.eastus.aroapp.io
Config Bundle Secret
enterprise-registry-config-bundle-rznzk
Components
Kind
clair

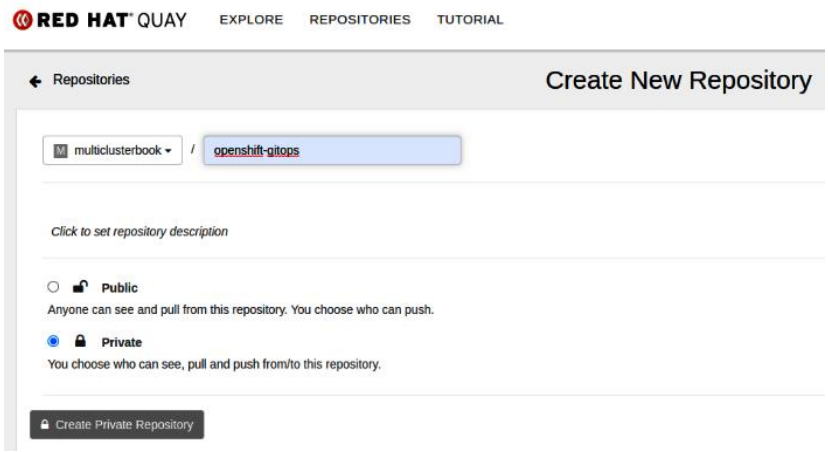

Fazer login
https://enterprise-registry-quay-config-editor-openshift-operators.apps.vqdlv2pu.eastus.aroapp.io
Nome de usuário
Senha
Cancelar
Fazer login
Custom SSL Certificates
This section lists any custom or self-signed SSL certificates that are installed in the Quay container on startup after being read from the extra_ca_certs dire
Custom certificates are typically used in place of publicly signed certificates for corporate-internal services.
Please make sure that all custom names used for downstream services (such as Clair) are listed in the certificates below.
Upload certificates:
Select file
Select custom certificate to add to configuration. Must be in PEM format and end extension '.crt'
CERTIFICATE FILENAME
STATUS
No custom certificates found.
Basic Configuration
Registry Title:
Name of registry to be displayed in the Contact Page.
Registry Title Short:
Enterprise Logo URL:
http://example.com/logo.png
Enter the full URL to your company's logo.
Contact Information:
URL
http://some/url
Information to show in the Contact Page. If none specified, CoreOS contact information is displayed.


Username:
enterprise-registry-quay-database
This user must have full access to the database
Password:
Database Name:
enterprise-registry-quay-database
SSL Certificate:
Escolher arquivo
Nenhum arquivo escolhido
Optional SSL certificate (in PEM format) to use to connect to the database
Validating configuration
Configuration Validated
Configuration Validated
Continue Editing
Download
Reconfigure Quay
Data Consistency Settings
Relax constraints on consistency guarantees for specific operations to enable higher performance and availability.
Allow repository pulls even if audit logging fails.
If enabled, failures to write to the audit log will fallback from the database to the standard logger for registry pulls.
Time Machine
Time machine keeps older copies of tags within a repository for the configured period of time, after which they are garbage collected. This allows users to revert tags to older images in case they accidentally pushed a broken image. It is highly recommended to have time machine enabled, but it does take a bit more space in storage.
Allowed expiration periods:
4w Remove
2w Remove
Add
The expiration periods allowed for configuration. The default tag expiration *must* be in this list.
Default expiration period:
2w
The default tag expiration period for all namespaces (users and organizations). Must be expressed in a duration string form: 30m, 1h, 1d, 2w.
Allow users to select expiration:
Enable Expiration Configuration
If enabled, users will be able to select the tag expiration duration for the namespace(s) they administrate, from the configured list of options.
Redis
Validate Configuration Changes


Validating configuration
Configuration Validated
Config Sent to Operator
Configuration Validated
Continue Editing
Download
Reconfigure Quay


Red Hat OpenShift
Administrator
Home
Operators
OperatorHub
Installed Operators
Workloads
Pods
Deployments
DeploymentConfigs
StatefulSets
Secrets
ConfigMaps
CronJobs
Jobs
DaemonSets
ReplicaSets
ReplicationControllers
HorizontalPodAutoscalers
Networking
Storage
Builds
Observe
Compute
User Management
Administration
Project: openshift-operators
Secret name *
enterprise-registry-quay-config-bundle-hfgnn
Unique name of the new secret.
Remove key/value
Key *
config.yaml
Value
Browse...
Drag and drop file with your value here or browse to upload it.
ALLOW_PULLS_WITHOUT_STRICT_LOGGING: false
AUTHENTICATION_TYPE: Database
AVATAR_KIND: local
Remove key/value
Key *
extra_ca_cert_ca-bundle.crt
Value
Browse...
Drag and drop file with your value here or browse to upload it.
ACCVBAIZ1
-----BEGIN CERTIFICATE-----
MIIHBzCCBbugAwIBAgIIXsO3pkN/pOAwDQYJKoZIhvcNAQEFBQAwQjESMBAGA1UE
Remove key/value
Key *
extra_ca_cert_service-ca.crt
Value
Browse...
Drag and drop file with your value here or browse to upload it.
-----BEGIN CERTIFICATE-----
MIIDUTCCAjmgAwIBAgIINZl7nfFD0lswDQYJKoZIhvcNAQELBQAwNjE0MDIGA1UE
Remove key/value
Key *
ocp-cluster-wildcard.cert
Value
Browse...
Drag and drop file with your value here or browse to upload it.
-----BEGIN CERTIFICATE-----
MIIIdTCCB12gAwIBAgITMwQQPSCgKASYQZzmgAAAPBE/jANBgkqhkiG9w0BAQwF
ADBZMQswCQYDVQQGEwJVUzEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmF0aW9u
Add key/value


RED HAT QUAY
EXPLORE
REPOSITORIES
TUTORIAL
search
quayad...
multiclusterbook
Create New Repository
Repositories
0 - 0 of 0
Filter Repositories...
This namespace doesn't have any viewable repositories.


RED HAT QUAY
EXPLORE
REPOSITORIES
TUTORIAL
Repositories
Create New Repository
multiclusterbook
/
openshift-gitops
Click to set repository description
Public
Anyone can see and pull from this repository. You choose who can push.
Private
You choose who can see, pull and push from/to this repository.
Create Private Repository

RED HAT® QUAY EXPLORE REPOSITORIES TUTORIAL

Step 2: Create a new container

The first step to creating an image is to create a container and fill it with some data.

First we'll create a container with a single new file based off of the `busybox` base image:

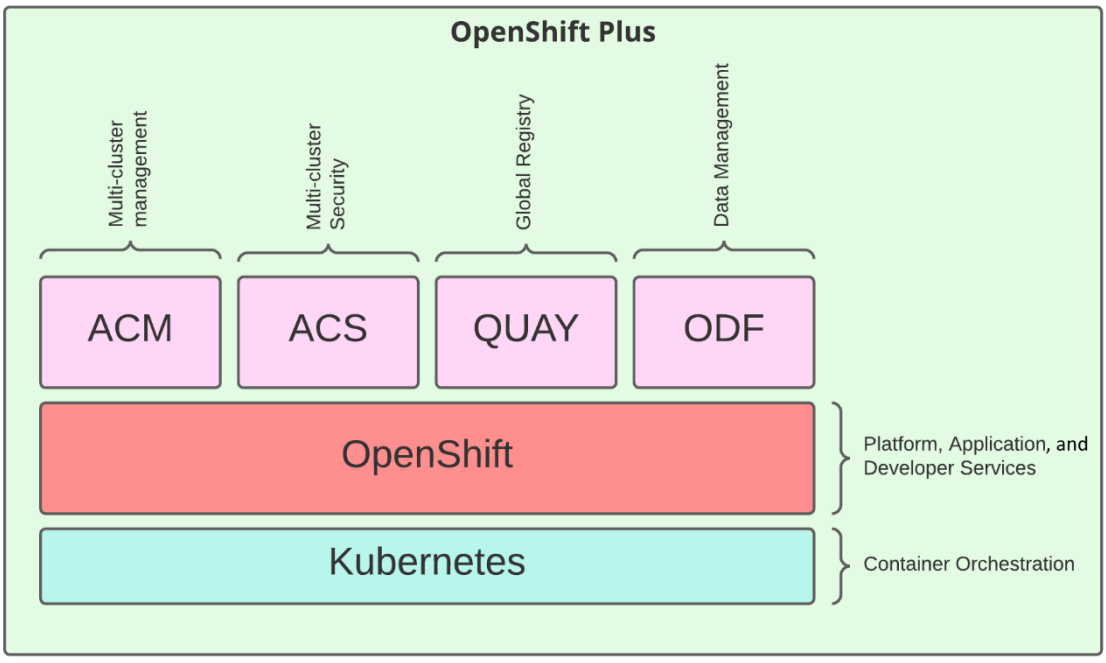
```
>_ docker run busybox echo "fun" > newfile
```

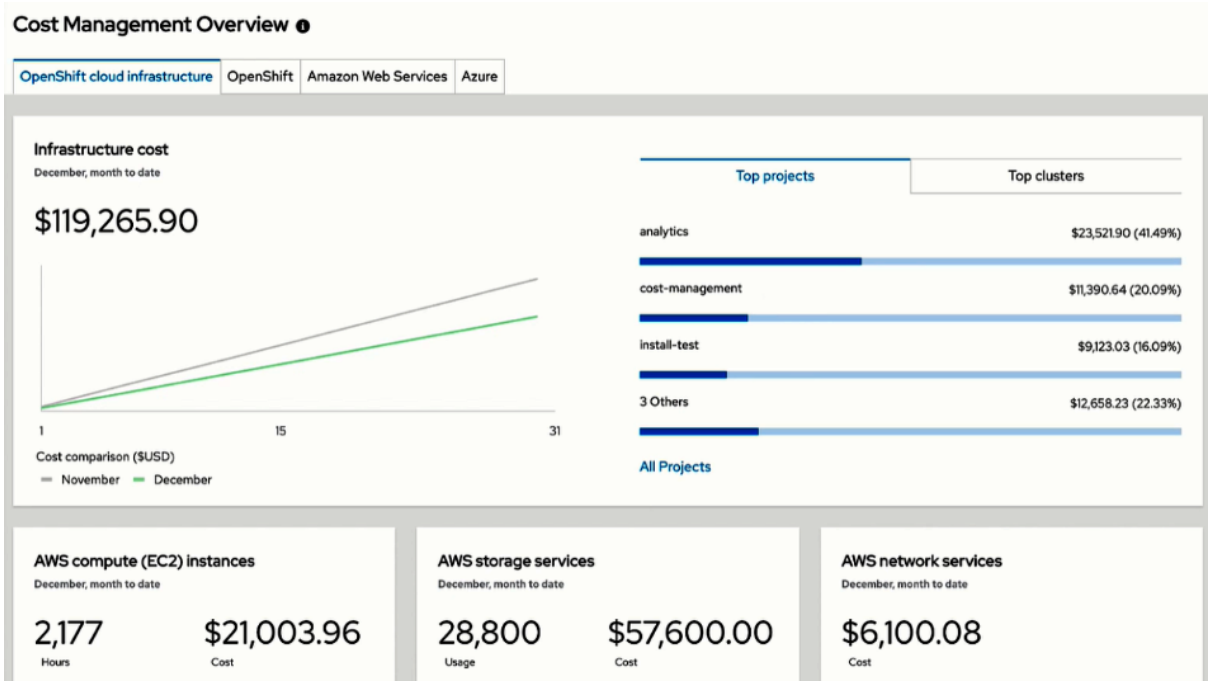
The container will immediately terminate (because its one command is `echo`), so we'll use `docker ps -l` to list it:

```
>_ docker ps -l
CONTAINER ID        IMAGE               COMMAND             CREATED
07f2065197ef        busybox:latest        echo fun          31 seconds ago
```

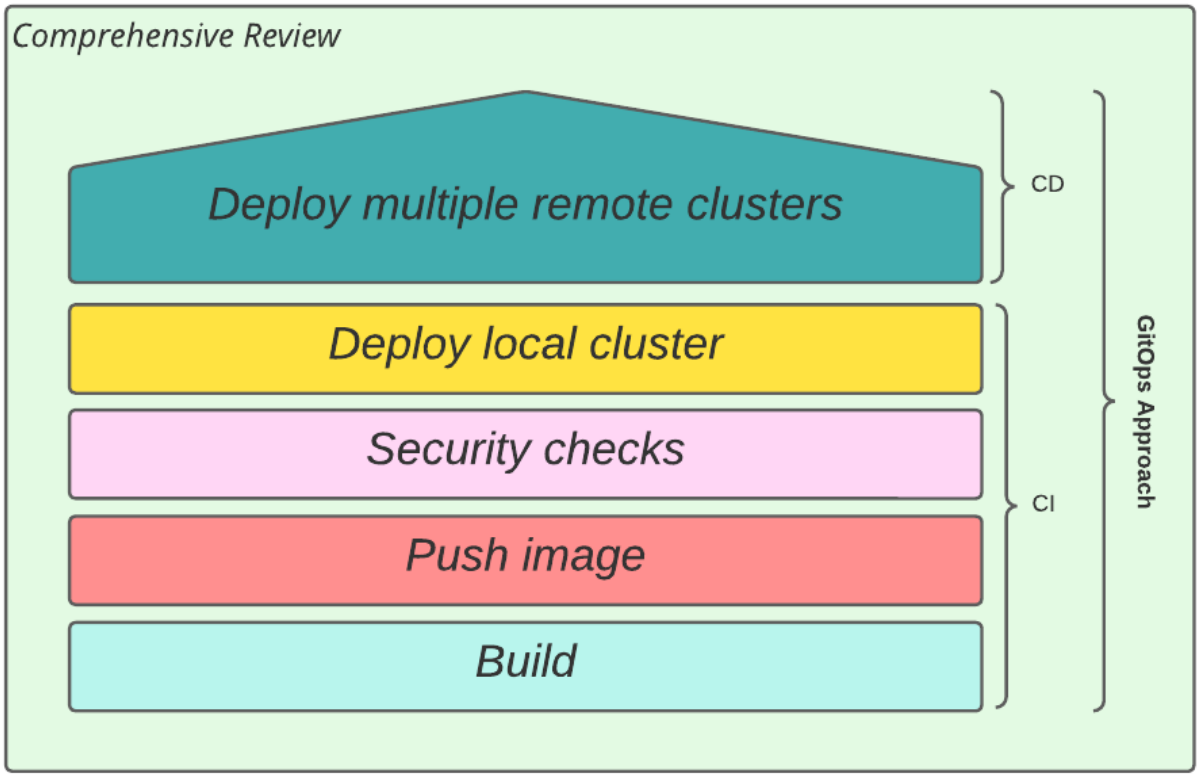
Enter the container ID returned: containerId

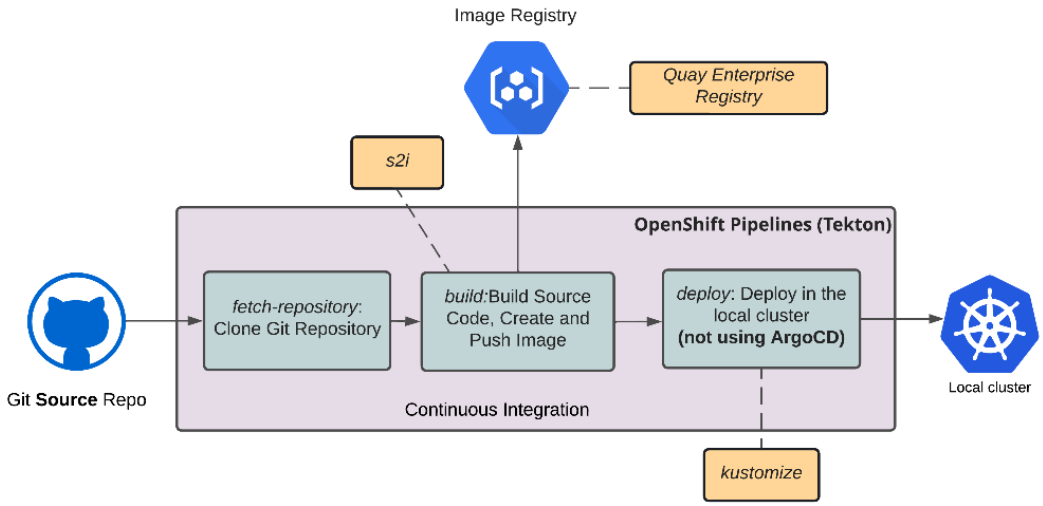
Continue Tutorial

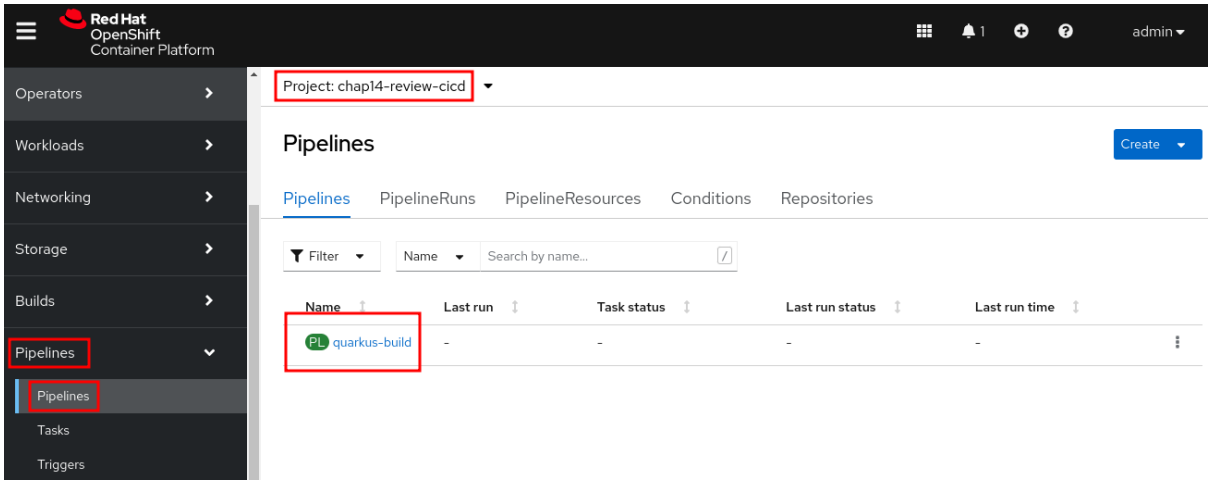


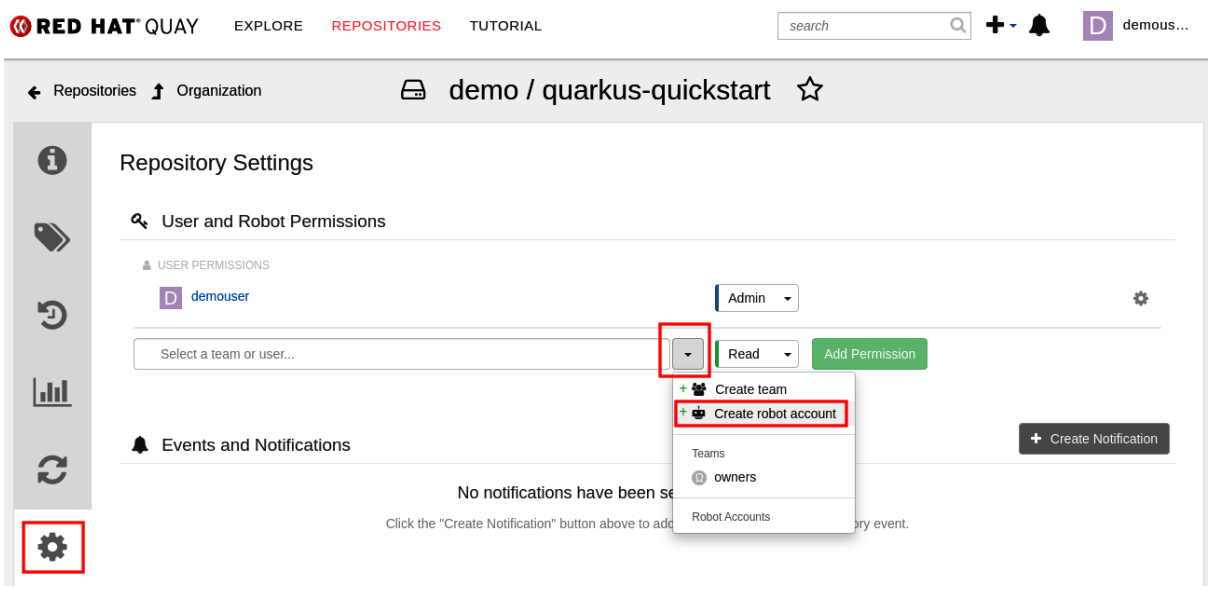

Cost Management Overview
OpenShift cloud infrastructure
OpenShift
Amazon Web Services
Azure
Infrastructure cost
December, month to date
$119,265.90
1
15
31
Cost comparison ($USD)
November
December
Top projects
Top clusters
analytics
$23,521.90 (41.49%)
cost-management
$11,390.64 (20.09%)
install-test
$9,123.03 (16.09%)
3 Others
$12,658.23 (22.33%)
All Projects
AWS compute (EC2) instances
December, month to date
2,177
Hours
$21,003.96
Cost
AWS storage services
December, month to date
28,800
Usage
$57,600.00
Cost
AWS network services
December, month to date
$6,100.08
Cost

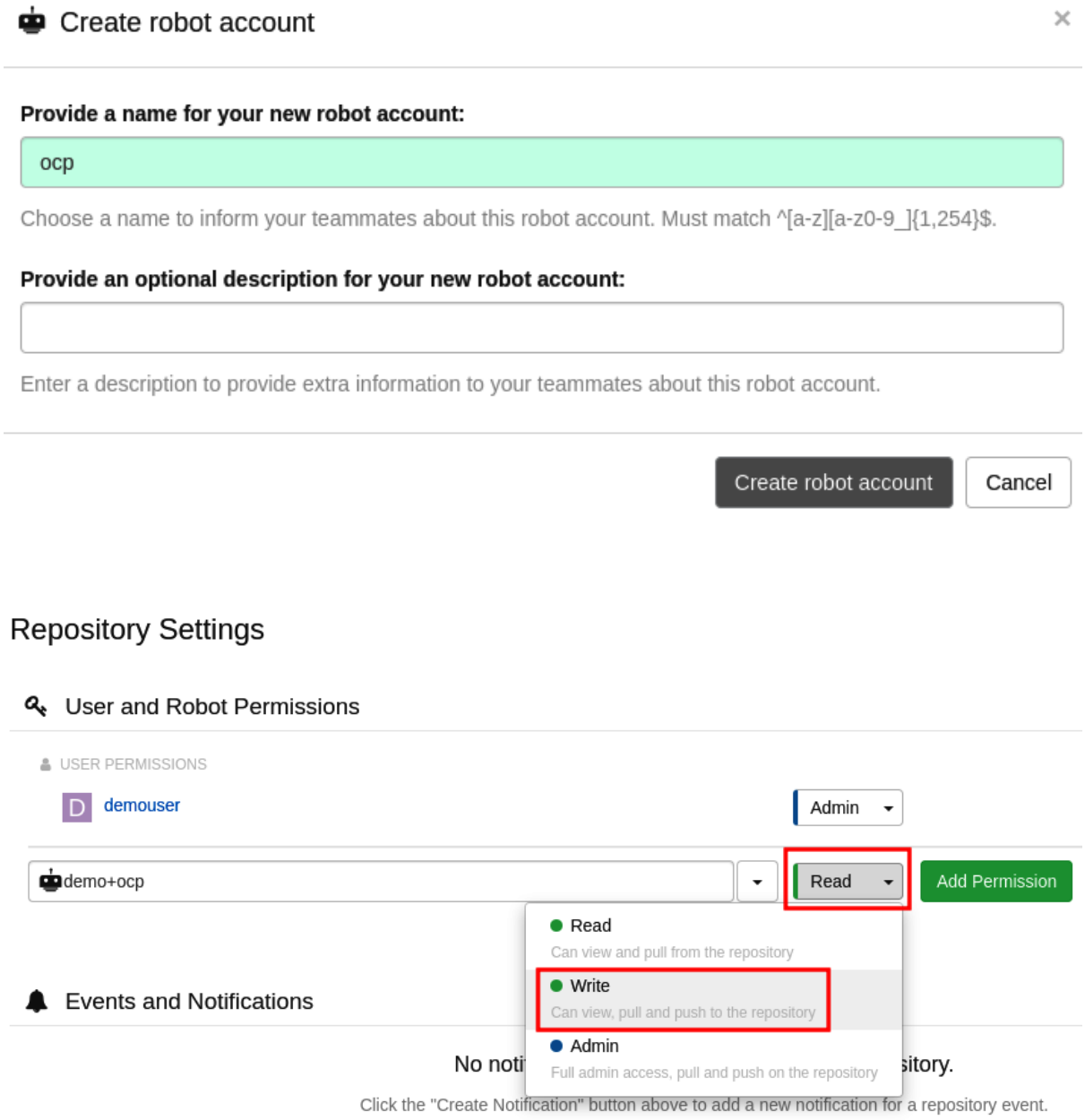
Chapter 14: Building a Cloud-Native Use Case in a Hybrid Cloud Environment

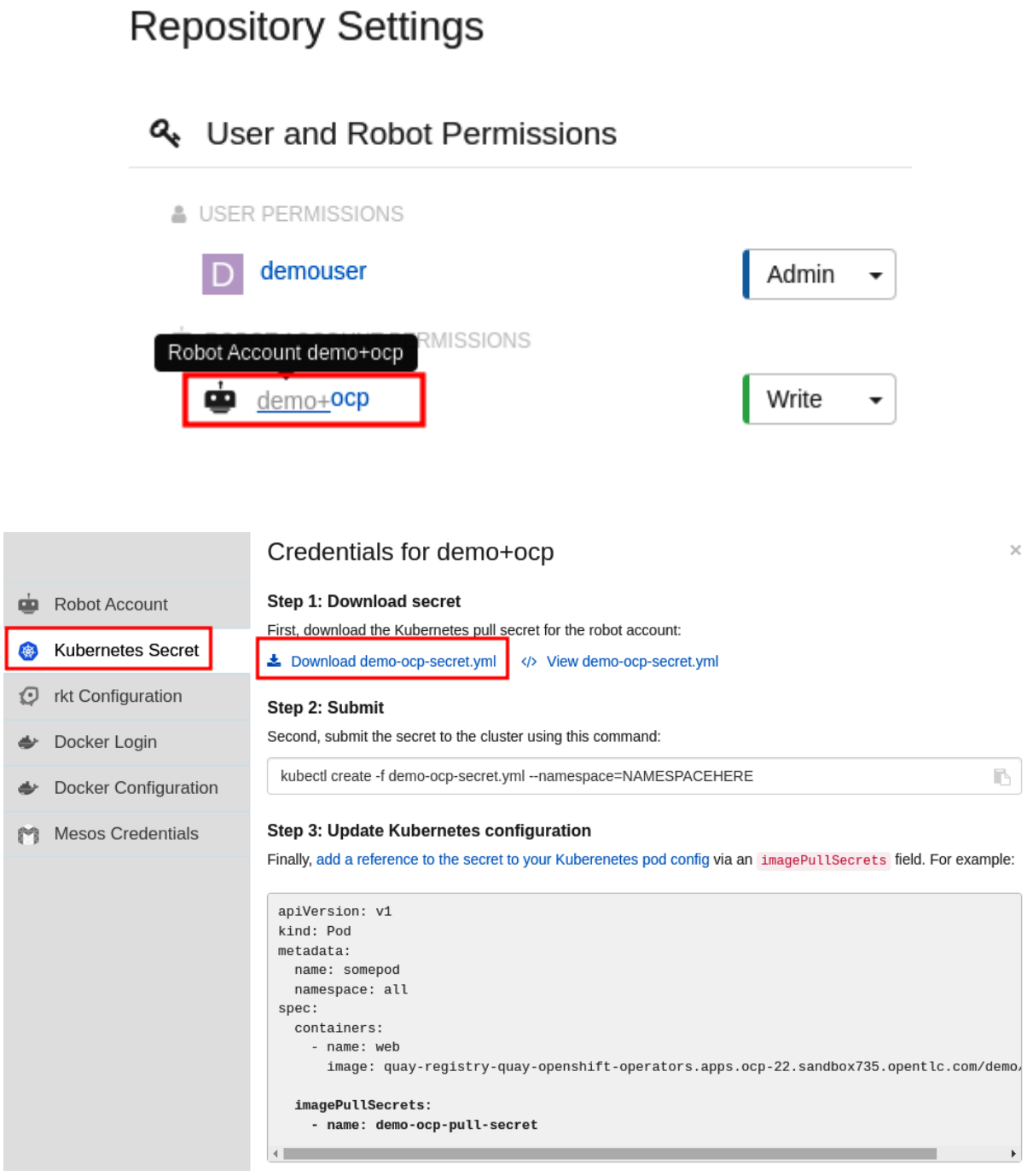


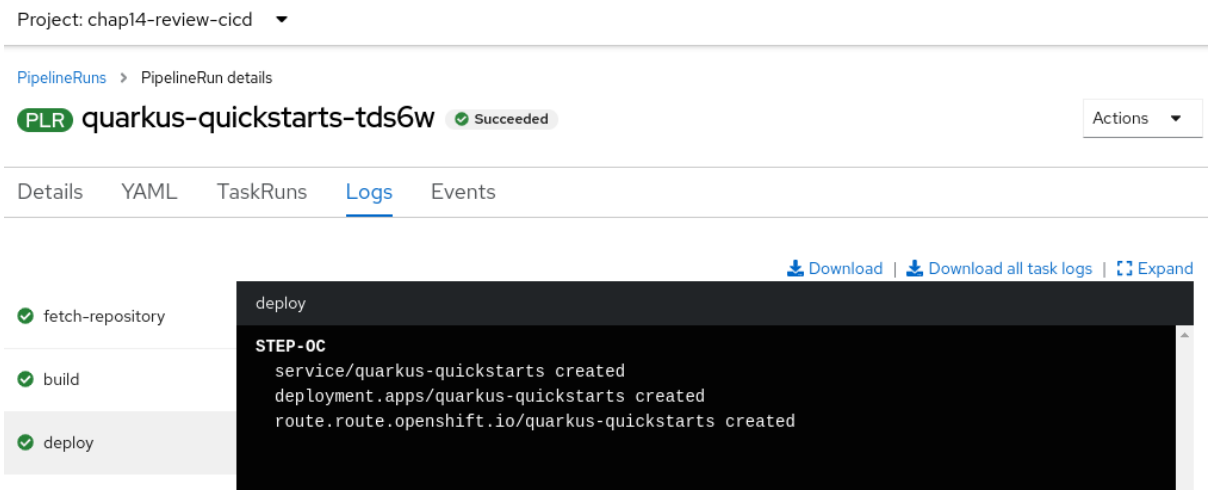


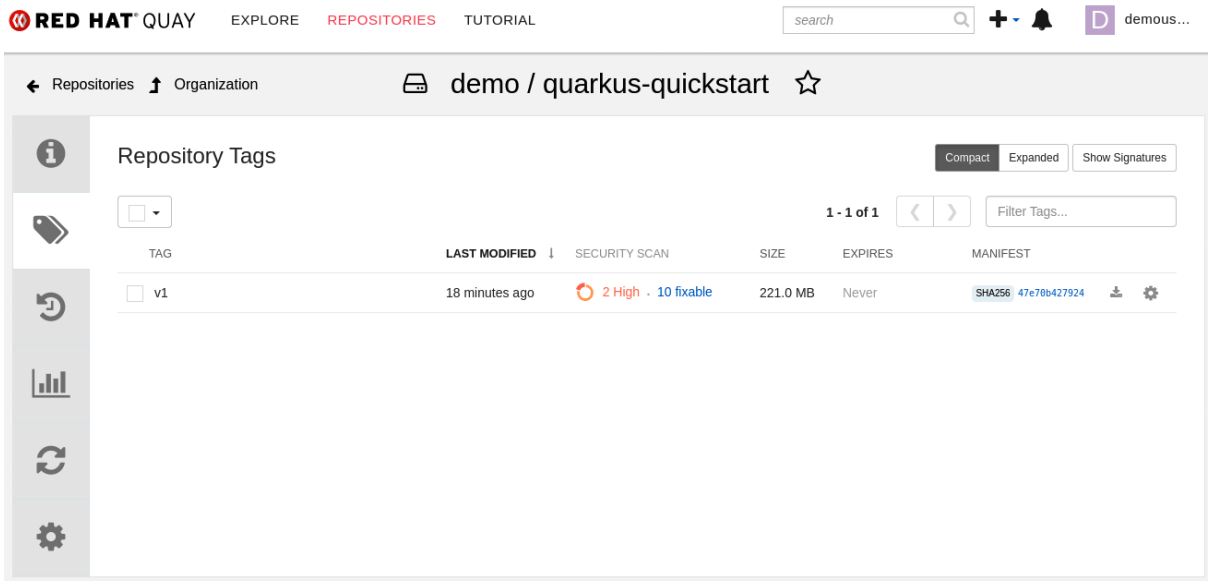

Red Hat OpenShift Container Platform
admin
Operators
Workloads
Networking
Storage
Builds
Pipelines
Pipelines
Tasks
Triggers
Project: chap14-review-cicd
Pipelines
Create
Pipelines
PipelineRuns
PipelineResources
Conditions
Repositories
Filter
Name
Search by name...
Name
Last run
Task status
Last run status
Last run time
PL quarkus-build
-
-
-
-


RED HAT QUAY
EXPLORE
REPOSITORIES
TUTORIAL
search
demous...
Repositories
Organization
demo / quarkus-quickstart
Repository Settings
User and Robot Permissions
USER PERMISSIONS
demouser
Admin
Select a team or user...
Read
Add Permission
Create team
Create robot account
Teams
owners
Robot Accounts
Events and Notifications
Create Notification
No notifications have been se
Click the "Create Notification" button above to add
ory event.


Create robot account
Provide a name for your new robot account:
ocp
Choose a name to inform your teammates about this robot account. Must match ^[a-z][a-z0-9_]{1,254}$.
Provide an optional description for your new robot account:
Enter a description to provide extra information to your teammates about this robot account.
Create robot account
Cancel
Repository Settings
User and Robot Permissions
USER PERMISSIONS
demouser
Admin
demo+ocp
Read
Add Permission
Read
Can view and pull from the repository
Write
Can view, pull and push to the repository
Admin
Full admin access, pull and push on the repository
Events and Notifications
Click the "Create Notification" button above to add a new notification for a repository event.


Repository Settings
User and Robot Permissions
USER PERMISSIONS
demouser
Admin
Robot Account demo+ocp
demo+ocp
Write
Credentials for demo+ocp
Robot Account
Kubernetes Secret
rkt Configuration
Docker Login
Docker Configuration
Mesos Credentials
Step 1: Download secret
First, download the Kubernetes pull secret for the robot account:
Download demo-ocp-secret.yml
View demo-ocp-secret.yml
Step 2: Submit
Second, submit the secret to the cluster using this command:
kubectl create -f demo-ocp-secret.yml --namespace=NAMESPACEHERE
Step 3: Update Kubernetes configuration
Finally, add a reference to the secret to your Kuberenetes pod config via an imagePullSecrets field. For example:
apiVersion: v1
kind: Pod
metadata:
name: somepod
namespace: all
spec:
containers:
- name: web
image: quay-registry-quay-openshift-operators.apps.ocp-22.sandbox735.opentlc.com/demo
imagePullSecrets:
- name: demo-ocp-pull-secret


Project: chap14-review-cicd
PipelineRuns
PipelineRun details
PLR
quarkus-quickstarts-tds6w
Succeeded
Actions
Details
YAML
TaskRuns
Logs
Events
Download
Download all task logs
Expand
fetch-repository
build
deploy
deploy
STEP-OC
service/quarkus-quickstarts created
deployment.apps/quarkus-quickstarts created
route.route.openshift.io/quarkus-quickstarts created


RED HAT QUAY
EXPLORE
REPOSITORIES
TUTORIAL
search
demous...
Repositories
Organization
demo / quarkus-quickstart
Repository Tags
Compact
Expanded
Show Signatures
1 - 1 of 1
Filter Tags...
TAG
LAST MODIFIED
SECURITY SCAN
SIZE
EXPIRES
MANIFEST
v1
18 minutes ago
2 High . 10 fixable
221.0 MB
Never
SHA256 47e70b427924

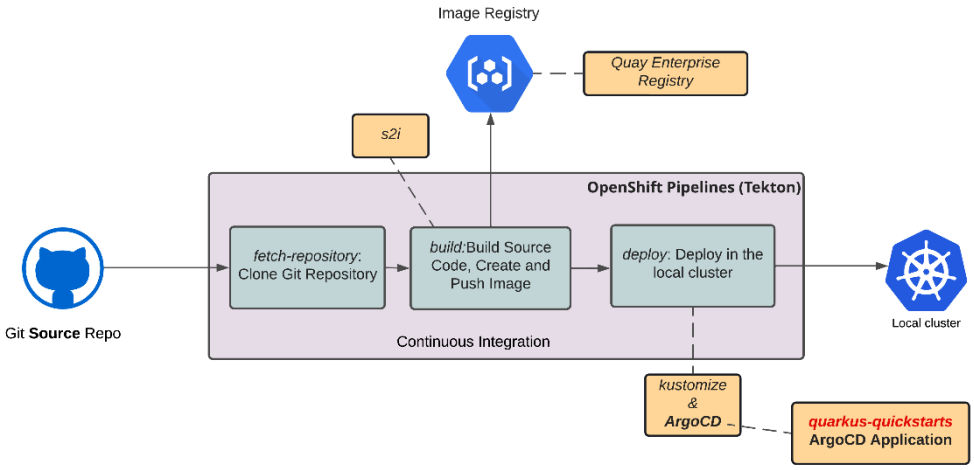
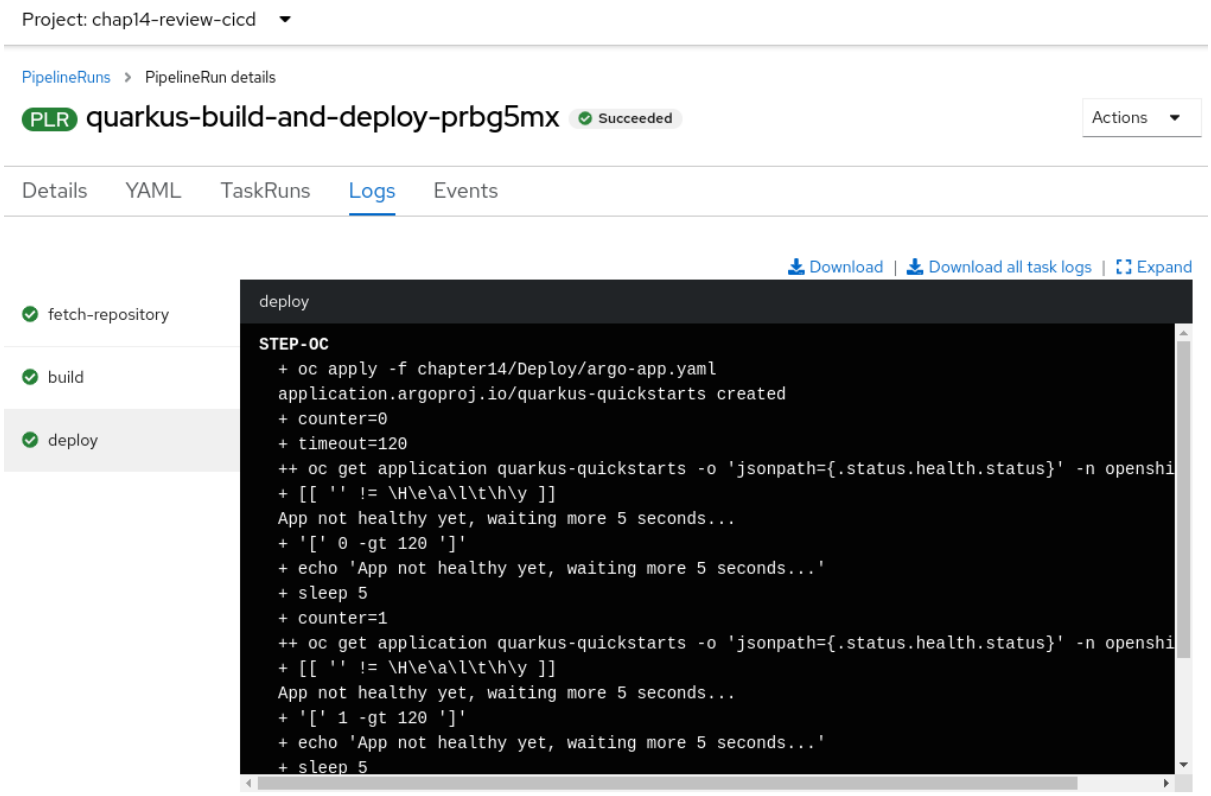
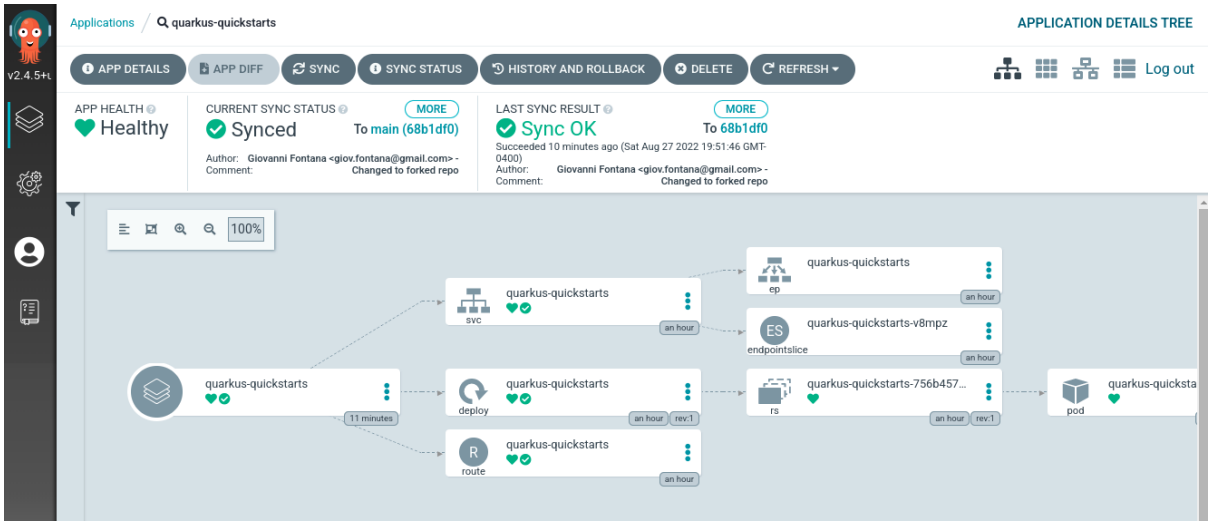


Image Registry
Quay Enterprise Registry
s2i
OpenShift Pipelines (Tekton)
fetch-repository: Clone Git Repository
build:Build Source Code, Create and Push Image
deploy: Deploy in the local cluster
Git Source Repo
Local cluster
Continuous Integration
kustomize & ArgoCD
quarkus-quickstarts ArgoCD Application


Project: chap14-review-cicd
PipelineRuns > PipelineRun details
PLR quarkus-build-and-deploy-prbg5mx Succeeded
Actions
Details YAML TaskRuns Logs Events
Download | Download all task logs | Expand
fetch-repository
build
deploy
deploy
STEP-OC
+ oc apply -f chapter14/Deploy/argo-app.yaml
application.argoproj.io/quarkus-quickstarts created
+ counter=0
+ timeout=120
++ oc get application quarkus-quickstarts -o 'jsonpath={.status.health.status}' -n openshi
+ [['' != \H\e\a\l\t\h\y]]
App not healthy yet, waiting more 5 seconds...
+ '[' 0 -gt 120 ']'
+ echo 'App not healthy yet, waiting more 5 seconds...'
+ sleep 5
+ counter=1
++ oc get application quarkus-quickstarts -o 'jsonpath={.status.health.status}' -n openshi
+ [['' != \H\e\a\l\t\h\y]]
App not healthy yet, waiting more 5 seconds...
+ '[' 1 -gt 120 ']'
+ echo 'App not healthy yet, waiting more 5 seconds...'
+ sleep 5


Applications / quarkus-quickstarts
APPLICATION DETAILS TREE
APP DETAILS APP DIFF SYNC SYNC STATUS HISTORY AND ROLLBACK DELETE REFRESH
Log out
APP HEALTH
Healthy
CURRENT SYNC STATUS
Synced
To main (68b1df0)
MORE
Author: Giovanni Fontana <giov.fontana@gmail.com> -
Comment: Changed to forked repo
LAST SYNC RESULT
Sync OK
To 68b1df0
MORE
Succeeded 10 minutes ago (Sat Aug 27 2022 19:51:46 GMT-0400)
Author: Giovanni Fontana <giov.fontana@gmail.com> -
Comment: Changed to forked repo
100%
quarkus-quickstarts
11 minutes
svc
quarkus-quickstarts
an hour
ep
quarkus-quickstarts
an hour
endpointslice
quarkus-quickstarts-v8mpz
an hour
deploy
quarkus-quickstarts
an hour rev:1
rs
quarkus-quickstarts-756b457...
an hour rev:1
pod
quarkus-quicksta
route
quarkus-quickstarts
an hour

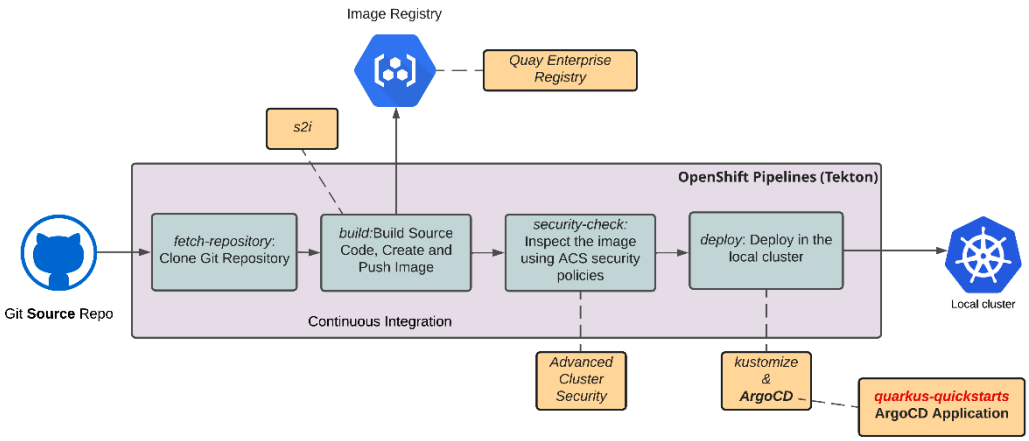
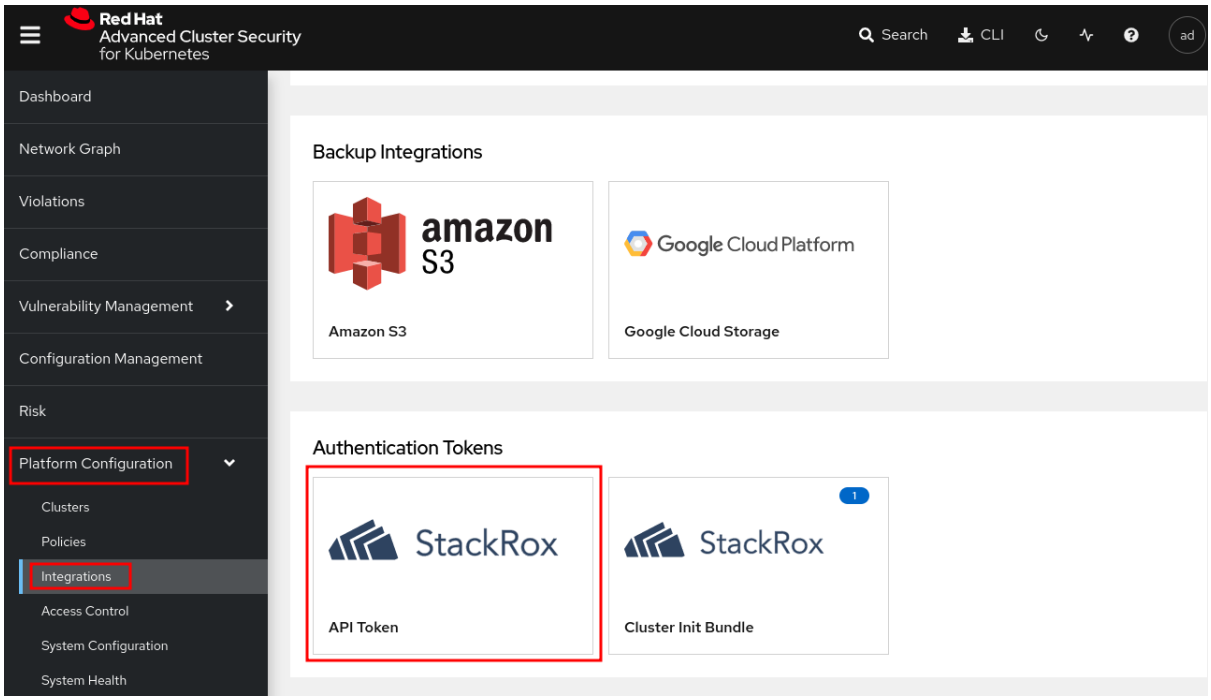
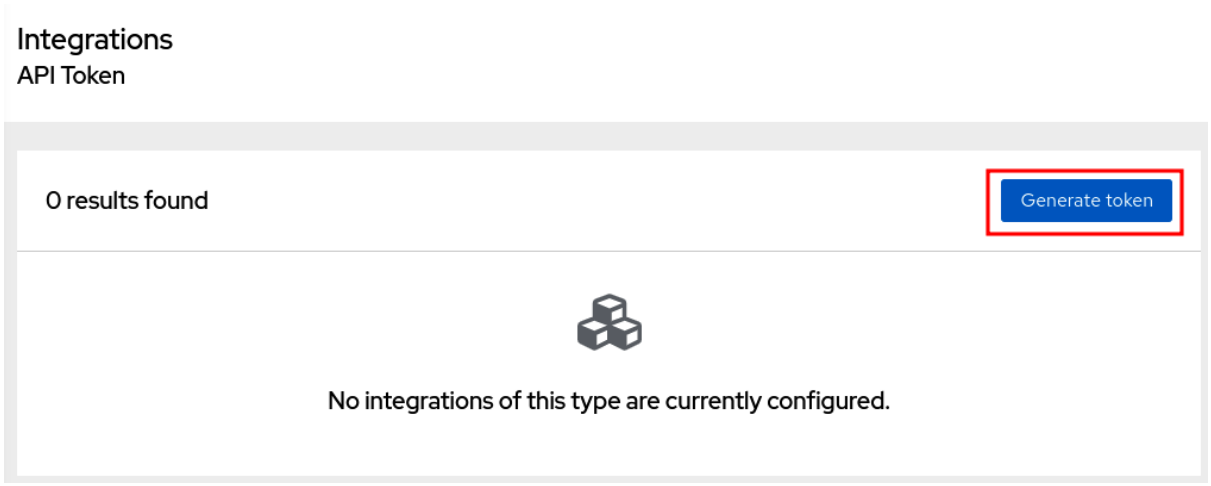
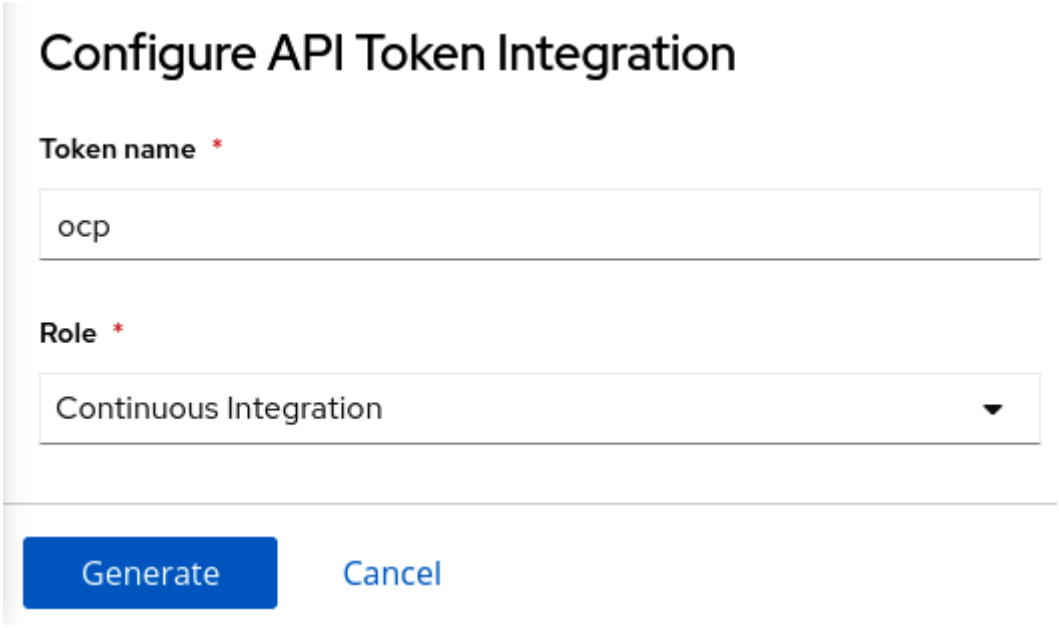
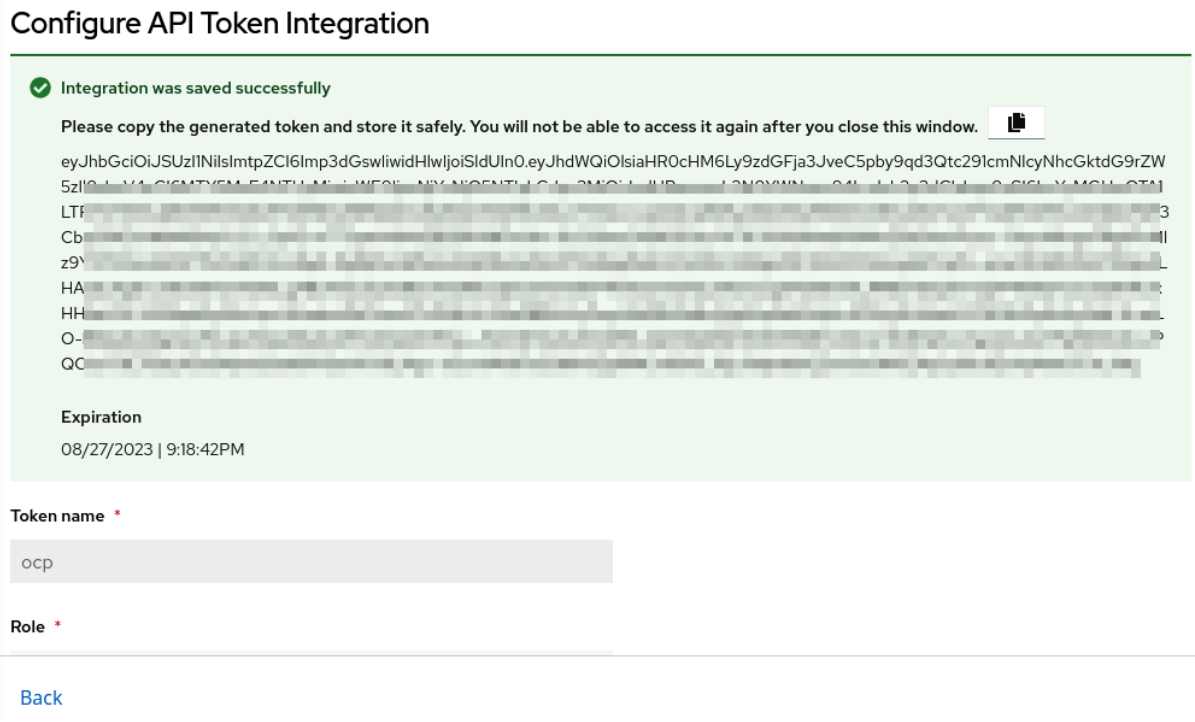


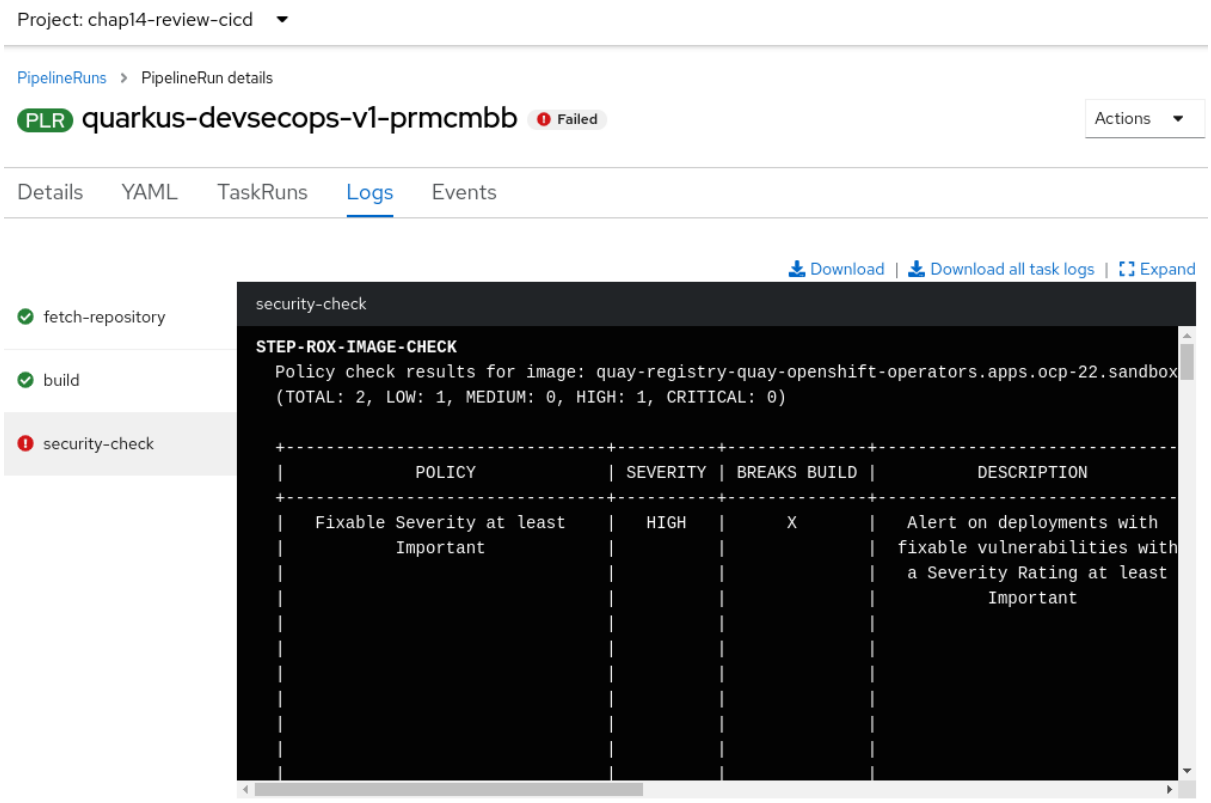
Image Registry
Quay Enterprise Registry
s2i
OpenShift Pipelines (Tekton)
Git Source Repo
fetch-repository: Clone Git Repository
build:Build Source Code, Create and Push Image
security-check: Inspect the image using ACS security policies
deploy: Deploy in the local cluster
Local cluster
Continuous Integration
Advanced Cluster Security
kustomize & ArgoCD
quarkus-quickstarts ArgoCD Application

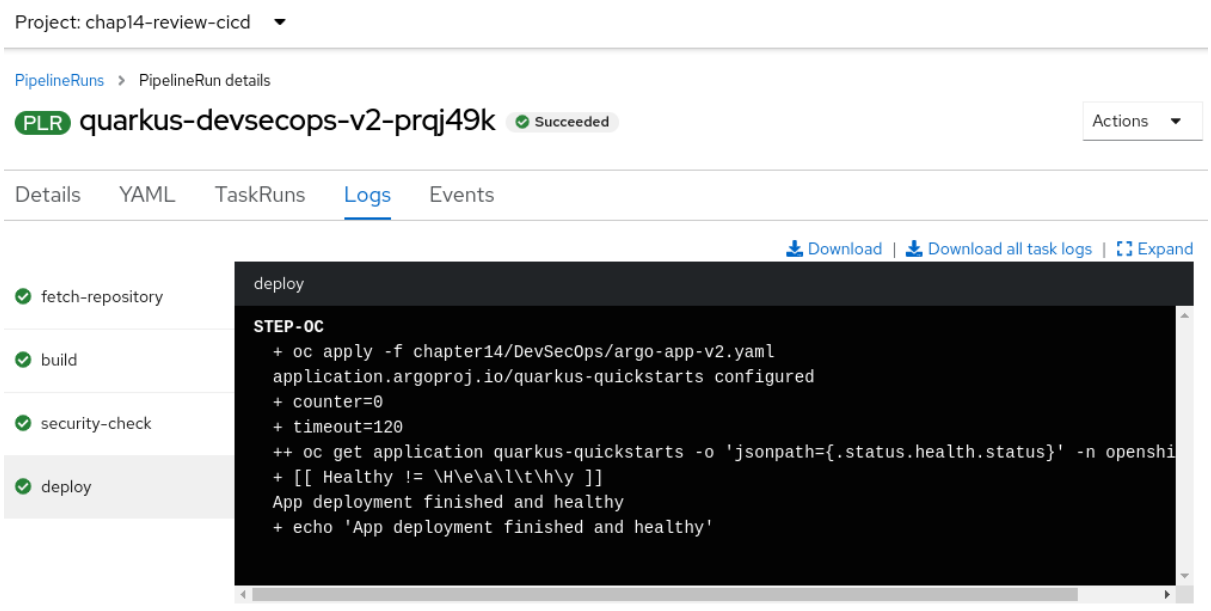

Red Hat
Advanced Cluster Security
for Kubernetes
Search
CLI
ad
Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Configuration Management
Risk
Platform Configuration
Clusters
Policies
Integrations
Access Control
System Configuration
System Health
Backup Integrations
amazon S3
Amazon S3
Google Cloud Platform
Google Cloud Storage
Authentication Tokens
StackRox
API Token
StackRox
Cluster Init Bundle

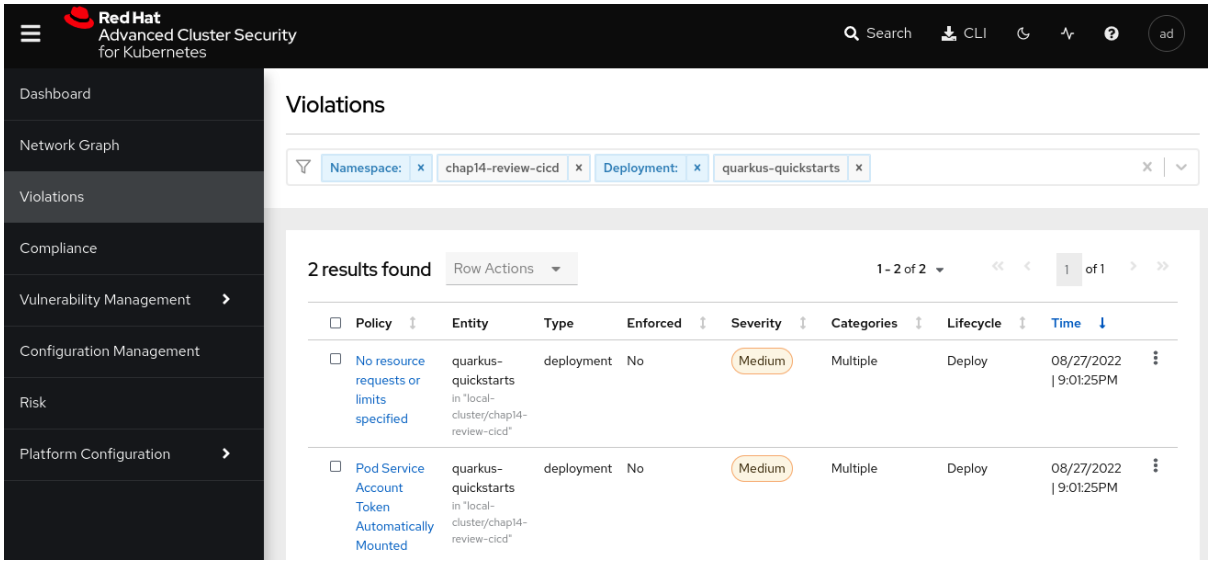

Integrations
API Token
0 results found
Generate token
No integrations of this type are currently configured.

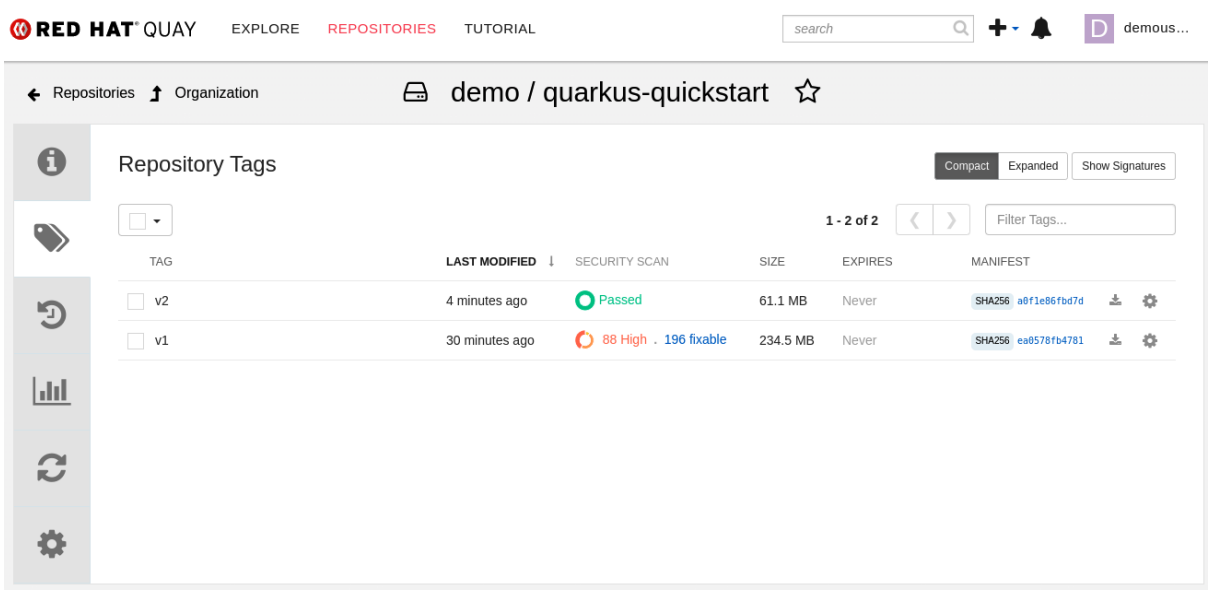

Configure API Token Integration
Token name *
ocp
Role *
Continuous Integration
Generate
Cancel

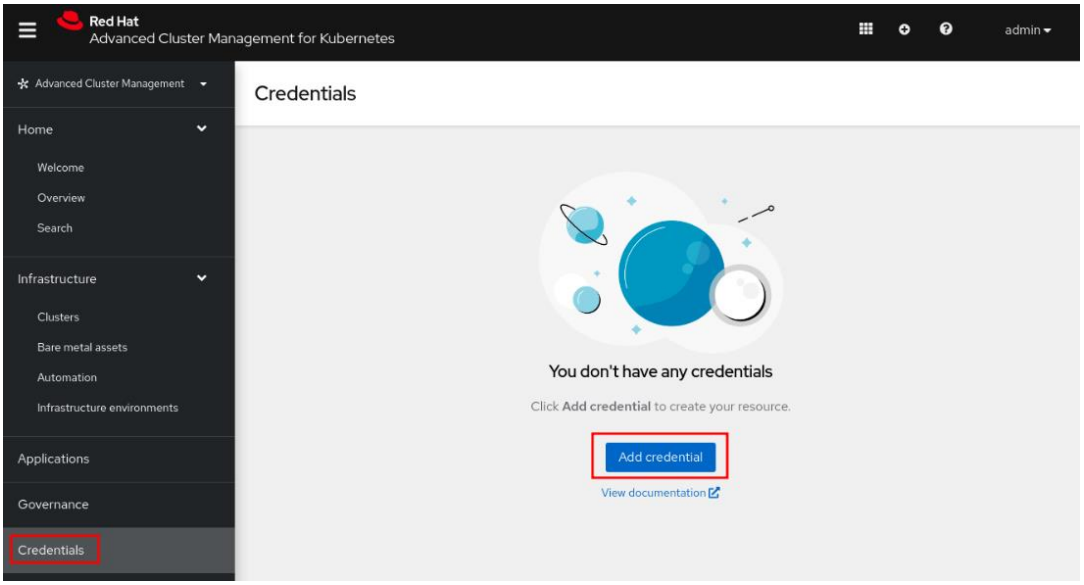

Configure API Token Integration
Integration was saved successfully
Please copy the generated token and store it safely. You will not be able to access it again after you close this window.
eyJhbGciOiJSUzI1NiIsImtpZCI6Imp3dGswIiwidHlwIjoiSldUIn0.eyJhdWQiOlsiaHR0cHM6Ly9zdGFja3JveC5pby9qd3Qtc291cmNlcyNhcGktdG9rZW
Expiration
08/27/2023 | 9:18:42PM
Token name *
ocp
Role *
Back

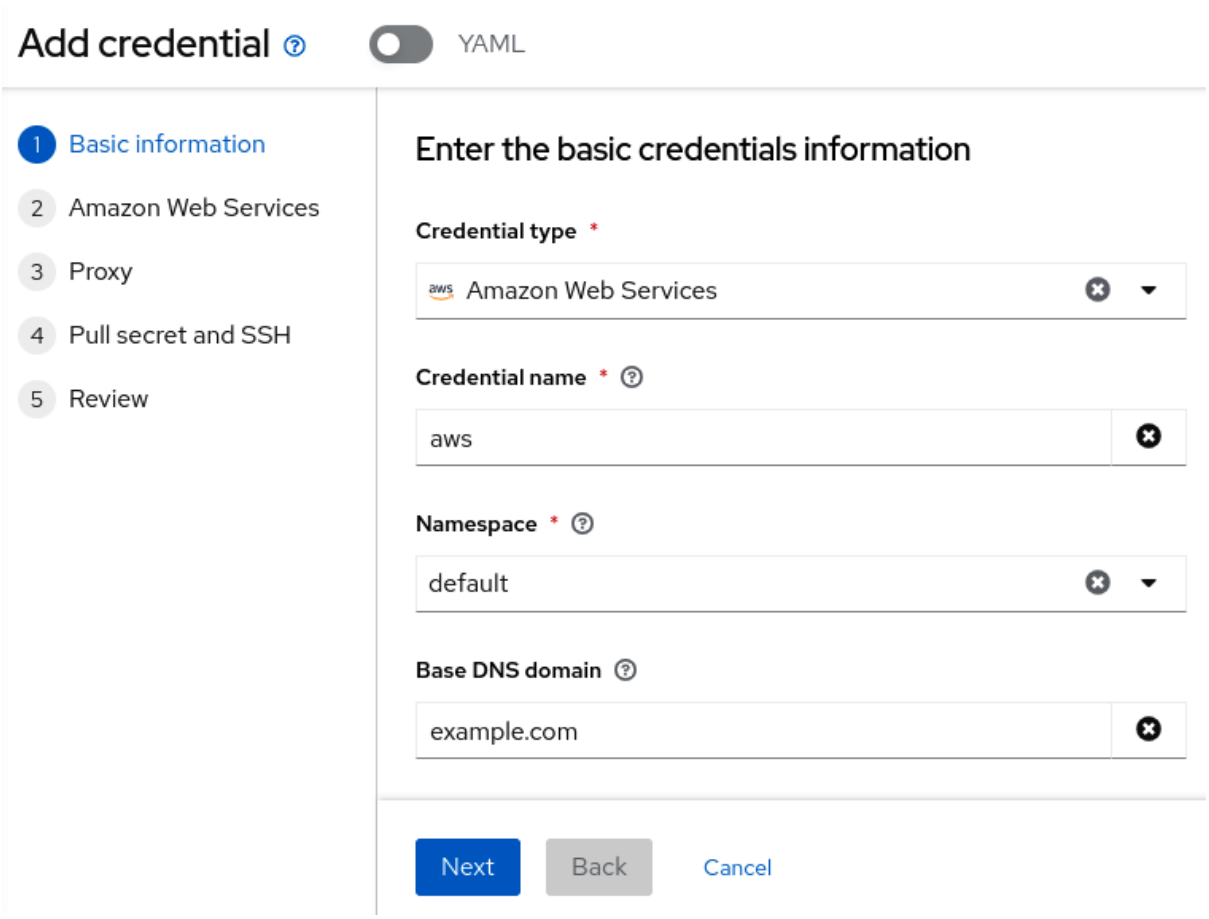

Project: chap14-review-cicd
PipelineRuns > PipelineRun details
PLR quarkus-devsecops-v1-prmcmbb Failed
Actions
Details YAML TaskRuns Logs Events
Download | Download all task logs | Expand
fetch-repository
build
security-check
security-check
STEP-ROX-IMAGE-CHECK
Policy check results for image: quay-registry-quay-openshift-operators.apps.ocp-22.sandbox
(TOTAL: 2, LOW: 1, MEDIUM: 0, HIGH: 1, CRITICAL: 0)
POLICY
SEVERITY
BREAKS BUILD
DESCRIPTION
Fixable Severity at least Important
HIGH
X
Alert on deployments with fixable vulnerabilities with a Severity Rating at least Important

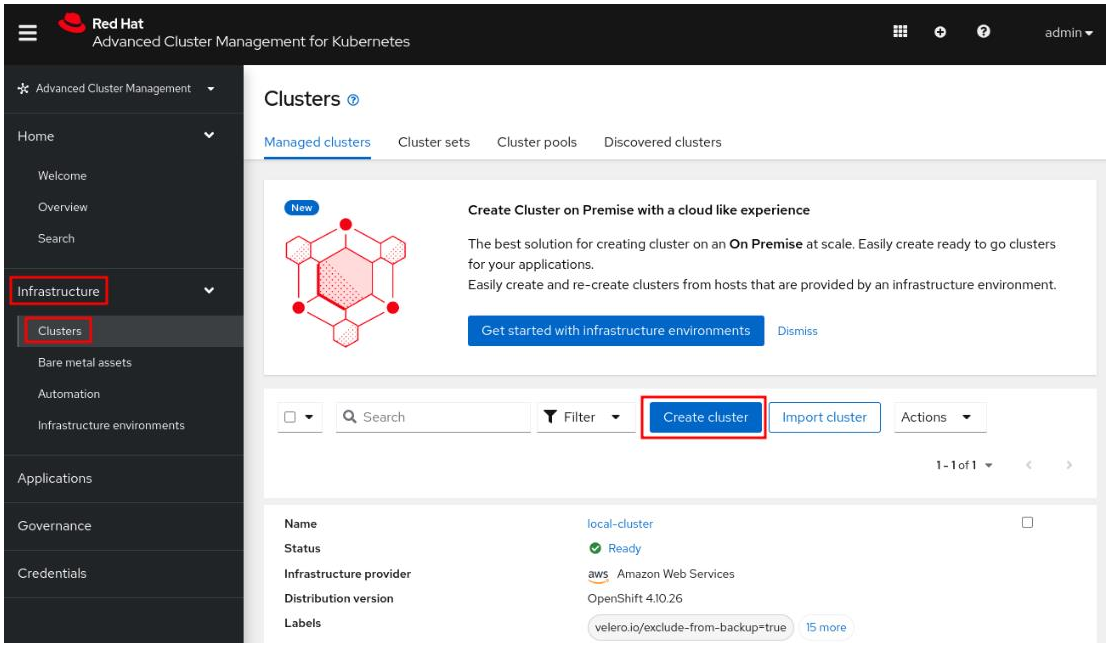

Project: chap14-review-cicd
PipelineRuns > PipelineRun details
PLR quarkus-devsecops-v2-prqj49k Succeeded
Actions
Details YAML TaskRuns Logs Events
Download | Download all task logs | Expand
fetch-repository
build
security-check
deploy
deploy
STEP-OC
+ oc apply -f chapter14/DevSecOps/argo-app-v2.yaml
application.argoproj.io/quarkus-quickstarts configured
+ counter=0
+ timeout=120
++ oc get application quarkus-quickstarts -o 'jsonpath={.status.health.status}' -n openshi
+ [[Healthy != \H\e\a\l\t\h\y]]
App deployment finished and healthy
+ echo 'App deployment finished and healthy'

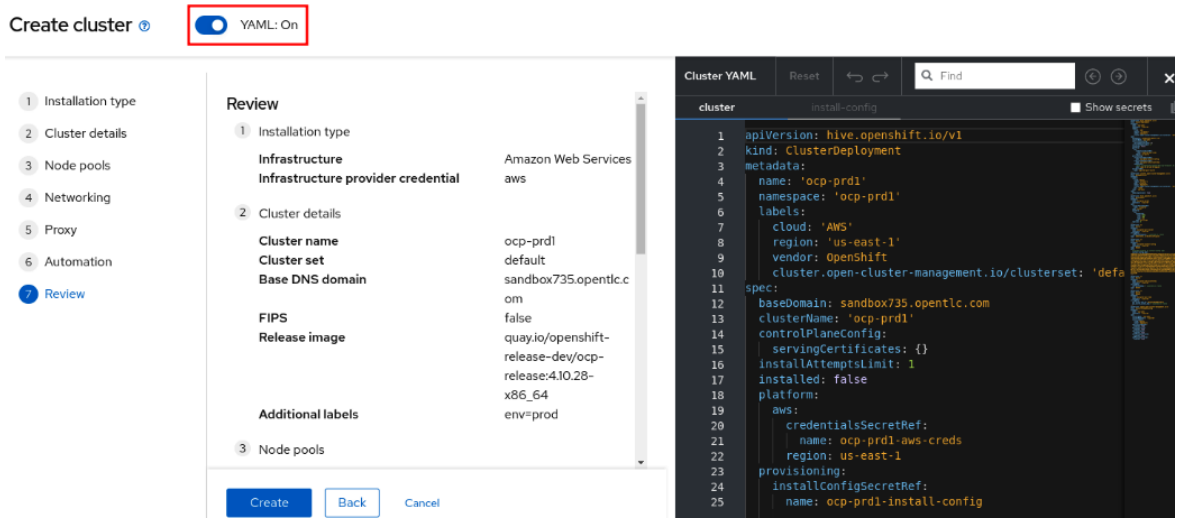

Red Hat
Advanced Cluster Security
for Kubernetes
Search
CLI
ad
Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Configuration Management
Risk
Platform Configuration
Violations
Namespace:
chap14-review-cicd
Deployment:
quarkus-quickstarts
2 results found
Row Actions
1 - 2 of 2
1 of 1
Policy
Entity
Type
Enforced
Severity
Categories
Lifecycle
Time
No resource requests or limits specified
quarkus-quickstarts
in "local-cluster/chap14-review-cicd"
deployment
No
Medium
Multiple
Deploy
08/27/2022 | 9:01:25PM
Pod Service Account Token Automatically Mounted
quarkus-quickstarts
in "local-cluster/chap14-review-cicd"
deployment
No
Medium
Multiple
Deploy
08/27/2022 | 9:01:25PM

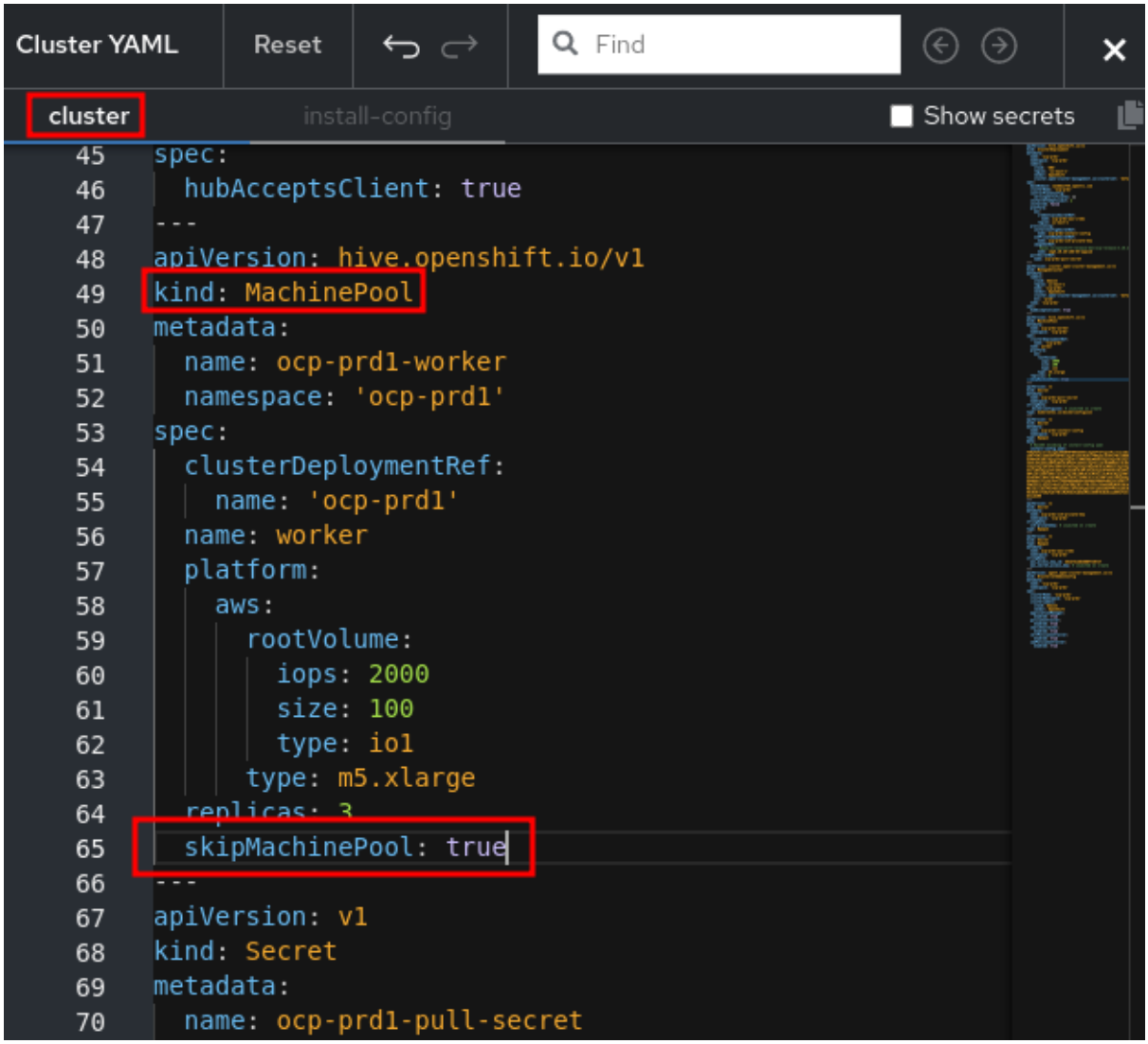

RED HAT QUAY
EXPLORE
REPOSITORIES
TUTORIAL
search
demous...
Repositories
Organization
demo / quarkus-quickstart
Repository Tags
Compact
Expanded
Show Signatures
1 - 2 of 2
Filter Tags...
TAG
LAST MODIFIED
SECURITY SCAN
SIZE
EXPIRES
MANIFEST
v2
4 minutes ago
Passed
61.1 MB
Never
SHA256 a0f1e86fbd7d
v1
30 minutes ago
88 High . 196 fixable
234.5 MB
Never
SHA256 ea0578fb4781

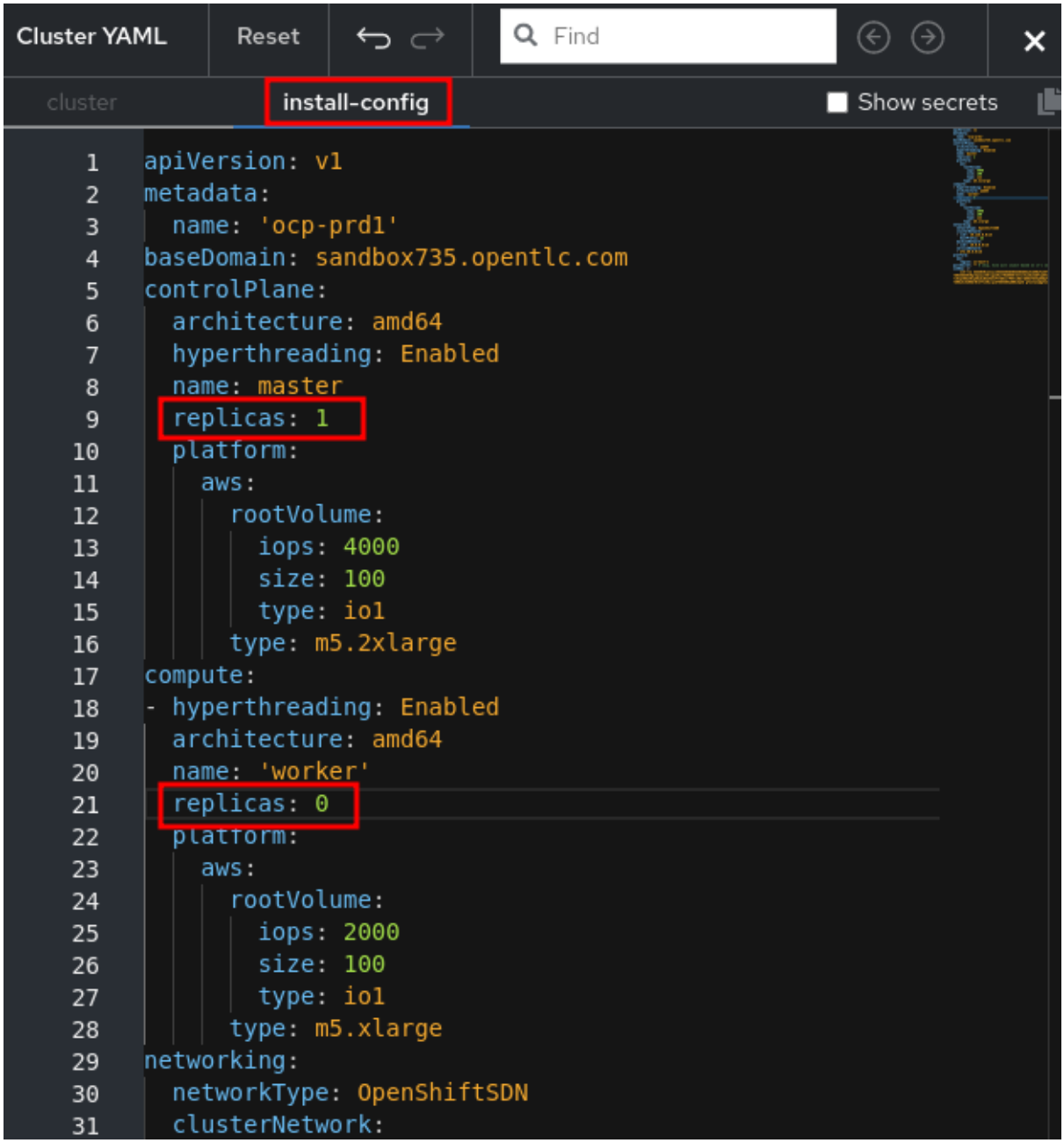

Red Hat
Advanced Cluster Management for Kubernetes
admin
Advanced Cluster Management
Home
Welcome
Overview
Search
Infrastructure
Clusters
Bare metal assets
Automation
Infrastructure environments
Applications
Governance
Credentials
Credentials
You don't have any credentials
Click Add credential to create your resource.
Add credential
View documentation

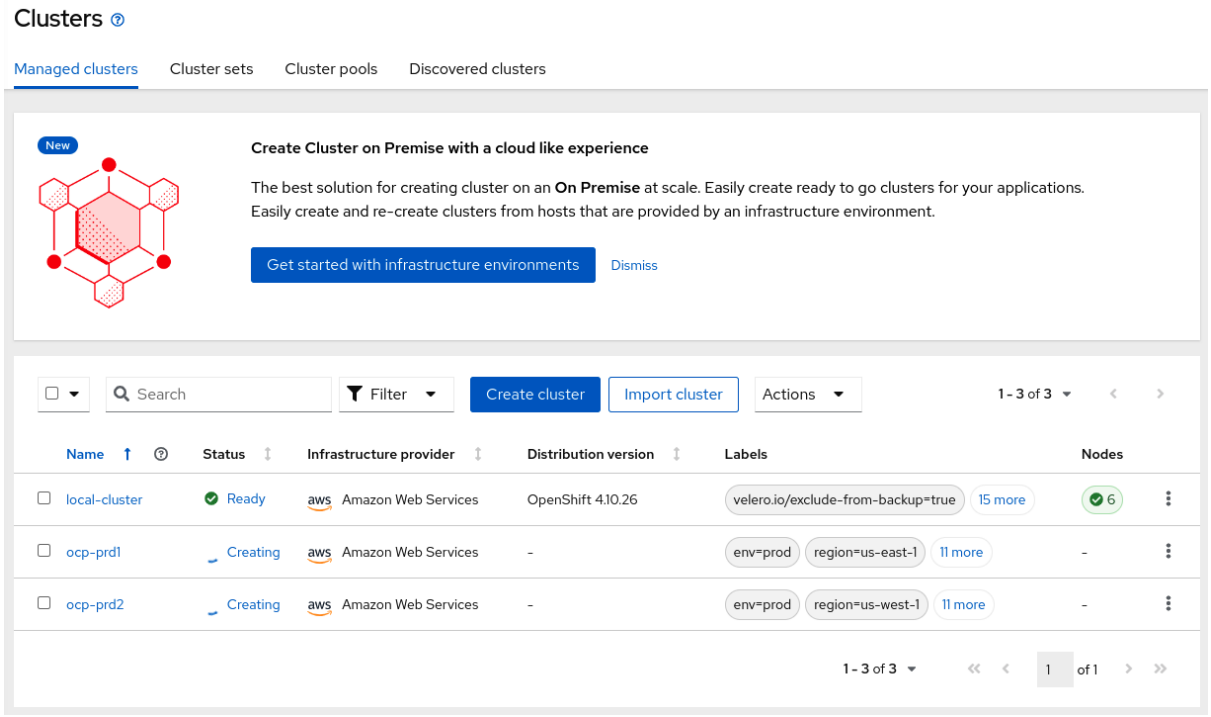

Add credential
YAML
1 Basic information
2 Amazon Web Services
3 Proxy
4 Pull secret and SSH
5 Review
Enter the basic credentials information
Credential type *
Amazon Web Services
Credential name *
aws
Namespace *
default
Base DNS domain
example.com
Next
Back
Cancel

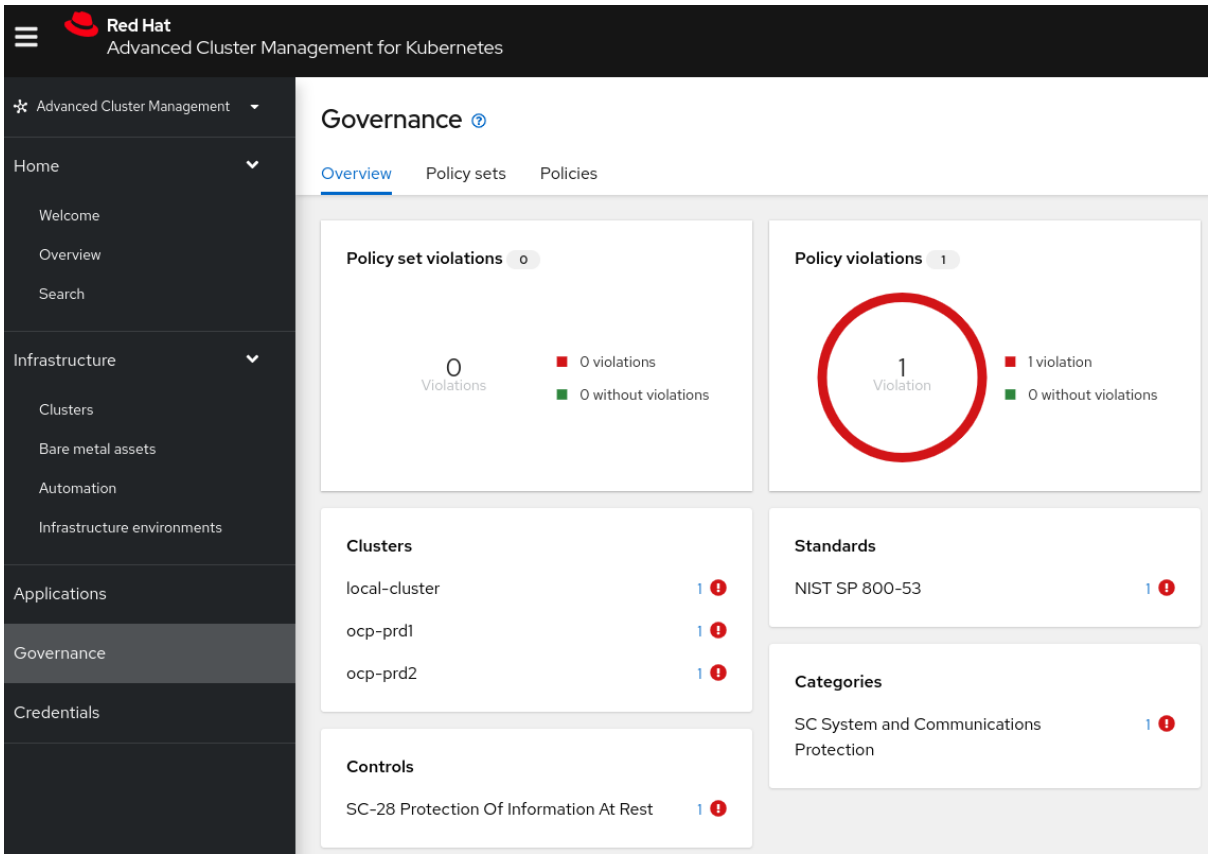

Red Hat
Advanced Cluster Management for Kubernetes
admin
Advanced Cluster Management
Home
Welcome
Overview
Search
Infrastructure
Clusters
Bare metal assets
Automation
Infrastructure environments
Applications
Governance
Credentials
Clusters
Managed clusters
Cluster sets
Cluster pools
Discovered clusters
New
Create Cluster on Premise with a cloud like experience
The best solution for creating cluster on an On Premise at scale. Easily create ready to go clusters for your applications.
Easily create and re-create clusters from hosts that are provided by an infrastructure environment.
Get started with infrastructure environments
Dismiss
Search
Filter
Create cluster
Import cluster
Actions
1 - 1 of 1
Name
local-cluster
Status
Ready
Infrastructure provider
Amazon Web Services
Distribution version
OpenShift 4.10.26
Labels
velero.io/exclude-from-backup=true
15 more


Create cluster
YAML: On
1 Installation type
2 Cluster details
3 Node pools
4 Networking
5 Proxy
6 Automation
7 Review
Review
1 Installation type
Infrastructure
Amazon Web Services
Infrastructure provider credential
aws
2 Cluster details
Cluster name
ocp-prd1
Cluster set
default
Base DNS domain
sandbox735.opentlc.com
FIPS
false
Release image
quay.io/openshift-release-dev/ocp-release:4.10.28-x86_64
Additional labels
env=prod
3 Node pools
Create
Back
Cancel
Cluster YAML
Reset
Find
cluster
install-config
Show secrets
apiVersion: hive.openshift.io/v1
kind: ClusterDeployment
metadata:
name: 'ocp-prd1'
namespace: 'ocp-prd1'
labels:
cloud: 'AWS'
region: 'us-east-1'
vendor: OpenShift
cluster.open-cluster-management.io/clusterset: 'defa
spec:
baseDomain: sandbox735.opentlc.com
clusterName: 'ocp-prd1'
controlPlaneConfig:
servingCertificates: {}
installAttemptsLimit: 1
installed: false
platform:
aws:
credentialsSecretRef:
name: ocp-prd1-aws-creds
region: us-east-1
provisioning:
installConfigSecretRef:
name: ocp-prd1-install-config


Cluster YAML
Reset
Find
cluster
install-config
Show secrets
45 spec:
46 hubAcceptsClient: true
47 ---
48 apiVersion: hive.openshift.io/v1
49 kind: MachinePool
50 metadata:
51 name: ocp-prd1-worker
52 namespace: 'ocp-prd1'
53 spec:
54 clusterDeploymentRef:
55 name: 'ocp-prd1'
56 name: worker
57 platform:
58 aws:
59 rootVolume:
60 iops: 2000
61 size: 100
62 type: io1
63 type: m5.xlarge
64 replicas: 3
65 skipMachinePool: true
66 ---
67 apiVersion: v1
68 kind: Secret
69 metadata:
70 name: ocp-prd1-pull-secret


Cluster YAML
Reset
Find
cluster
install-config
Show secrets
1 apiVersion: v1
2 metadata:
3 name: 'ocp-prd1'
4 baseDomain: sandbox735.opentlc.com
5 controlPlane:
6 architecture: amd64
7 hyperthreading: Enabled
8 name: master
9 replicas: 1
10 platform:
11 aws:
12 rootVolume:
13 iops: 4000
14 size: 100
15 type: io1
16 type: m5.2xlarge
17 compute:
18 - hyperthreading: Enabled
19 architecture: amd64
20 name: 'worker'
21 replicas: 0
22 platform:
23 aws:
24 rootVolume:
25 iops: 2000
26 size: 100
27 type: io1
28 type: m5.xlarge
29 networking:
30 networkType: OpenShiftSDN
31 clusterNetwork:


Clusters
Managed clusters
Cluster sets
Cluster pools
Discovered clusters
New
Create Cluster on Premise with a cloud like experience
The best solution for creating cluster on an On Premise at scale. Easily create ready to go clusters for your applications.
Easily create and re-create clusters from hosts that are provided by an infrastructure environment.
Get started with infrastructure environments
Dismiss
Search
Filter
Create cluster
Import cluster
Actions
1 - 3 of 3
Name
Status
Infrastructure provider
Distribution version
Labels
Nodes
local-cluster
Ready
Amazon Web Services
OpenShift 4.10.26
velero.io/exclude-from-backup=true
15 more
6
ocp-prd1
Creating
Amazon Web Services
-
env=prod
region=us-east-1
11 more
-
ocp-prd2
Creating
Amazon Web Services
-
env=prod
region=us-west-1
11 more
-
1 - 3 of 3
1
of 1


Red Hat
Advanced Cluster Management for Kubernetes
Advanced Cluster Management
Home
Welcome
Overview
Search
Infrastructure
Clusters
Bare metal assets
Automation
Infrastructure environments
Applications
Governance
Credentials
Governance
Overview
Policy sets
Policies
Policy set violations 0
0
Violations
0 violations
0 without violations
Policy violations 1
1
Violation
1 violation
0 without violations
Clusters
local-cluster 1
ocp-prd1 1
ocp-prd2 1
Standards
NIST SP 800-53 1
Categories
SC System and Communications Protection 1
Controls
SC-28 Protection Of Information At Rest 1

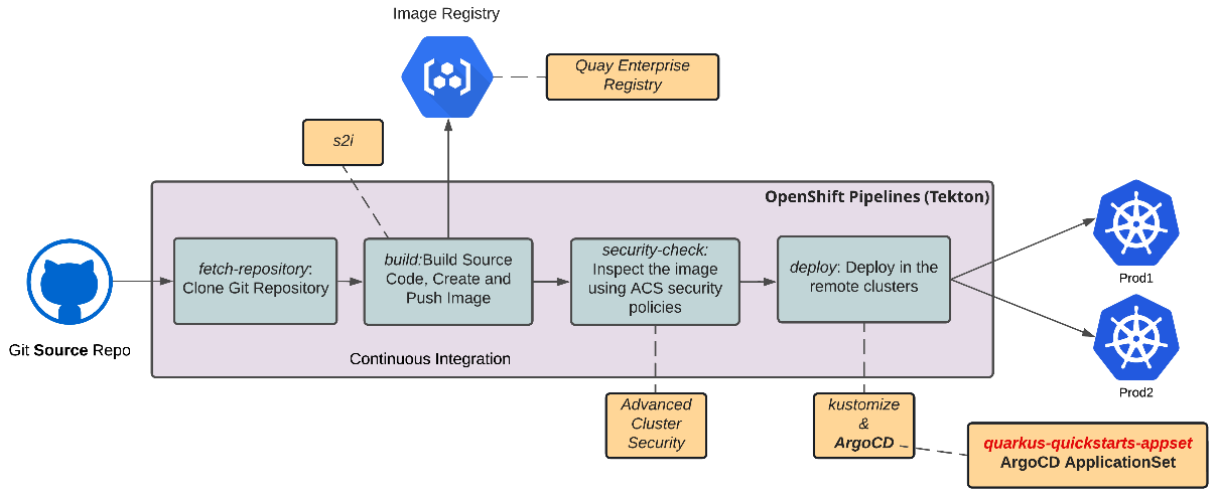
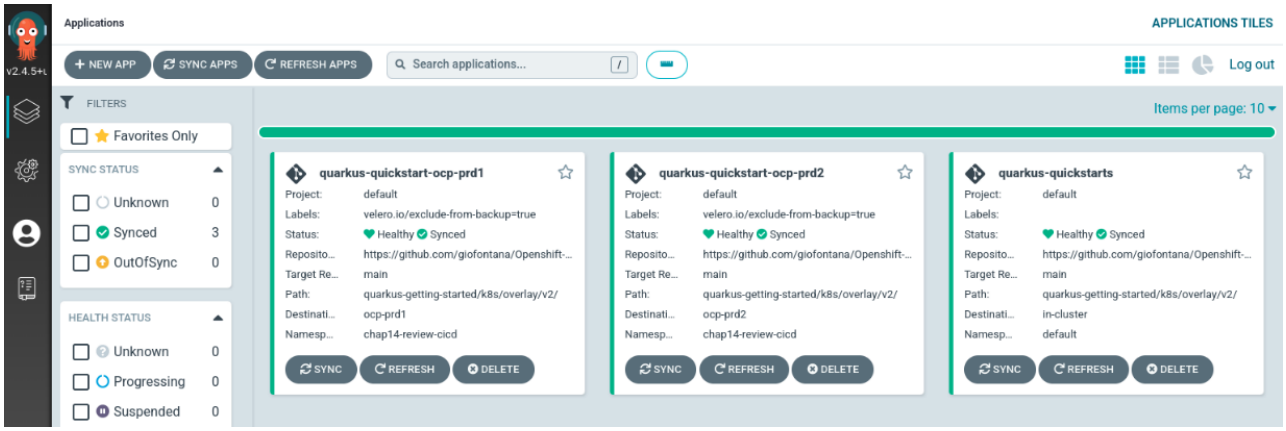
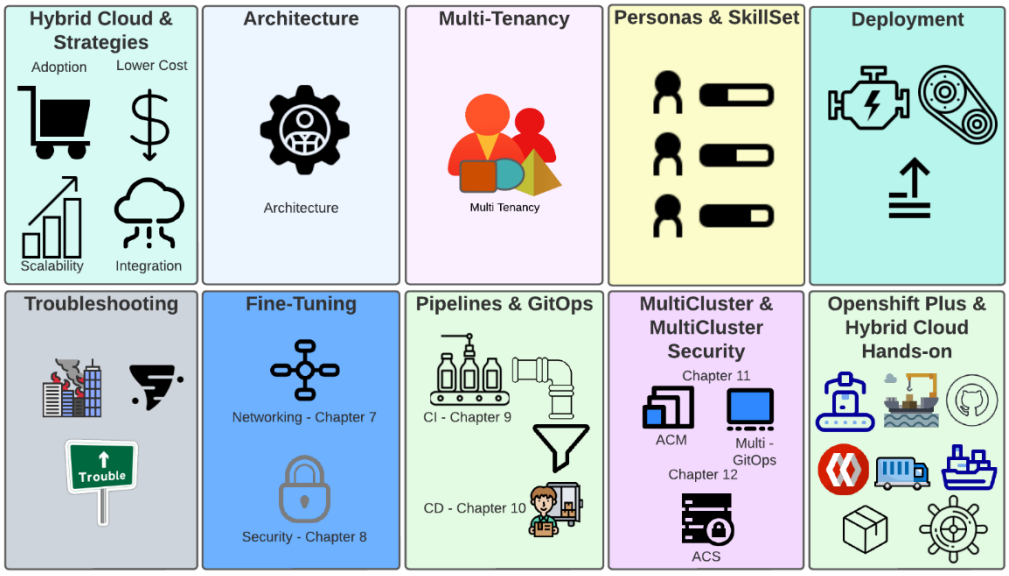
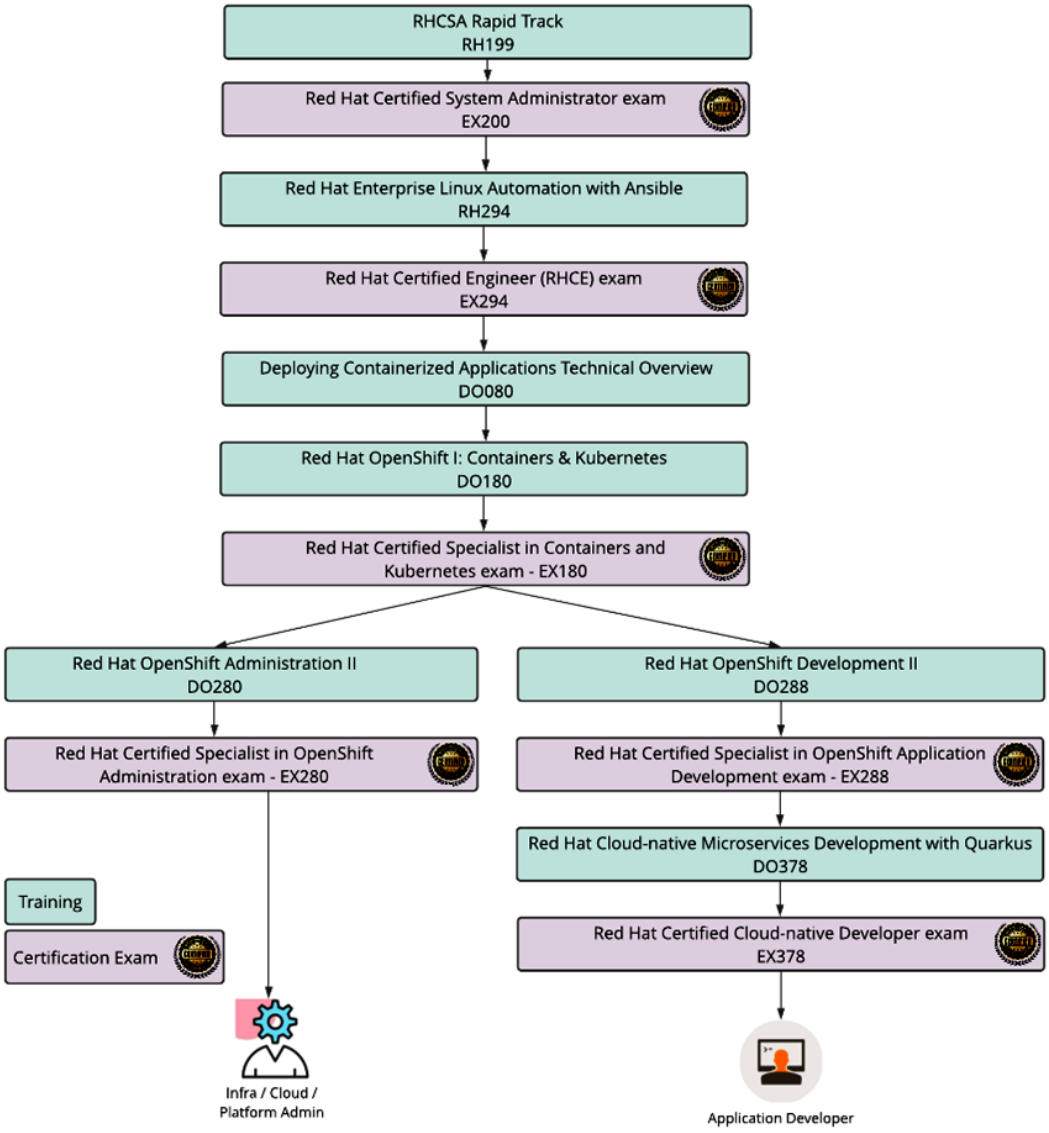


Image Registry
Quay Enterprise Registry
s2i
OpenShift Pipelines (Tekton)
Git Source Repo
fetch-repository: Clone Git Repository
build:Build Source Code, Create and Push Image
security-check: Inspect the image using ACS security policies
deploy: Deploy in the remote clusters
Prod1
Prod2
Continuous Integration
Advanced Cluster Security
kustomize & ArgoCD
quarkus-quickstarts-appset
ArgoCD ApplicationSet


Applications
APPLICATIONS TILES
NEW APP
SYNC APPS
REFRESH APPS
Search applications...
Log out
FILTERS
Favorites Only
SYNC STATUS
Unknown 0
Synced 3
OutOfSync 0
HEALTH STATUS
Unknown 0
Progressing 0
Suspended 0
Items per page: 10
quarkus-quickstart-ocp-prd1
quarkus-quickstart-ocp-prd2
quarkus-quickstarts
SYNC
REFRESH
DELETE


Hybrid Cloud & Strategies
Adoption
Lower Cost
Scalability
Integration
Architecture
Architecture
Multi-Tenancy
Multi Tenancy
Personas & SkillSet
Deployment
Troubleshooting
Trouble
Fine-Tuning
Networking - Chapter 7
Security - Chapter 8
Pipelines & GitOps
CI - Chapter 9
CD - Chapter 10
MultiCluster & MultiCluster Security
Chapter 11
ACM
Multi - GitOps
Chapter 12
ACS
Openshift Plus & Hybrid Cloud Hands-on

Chapter 15: What's Next