KUBERNETES
COMMUNITY DAYS DALIAN

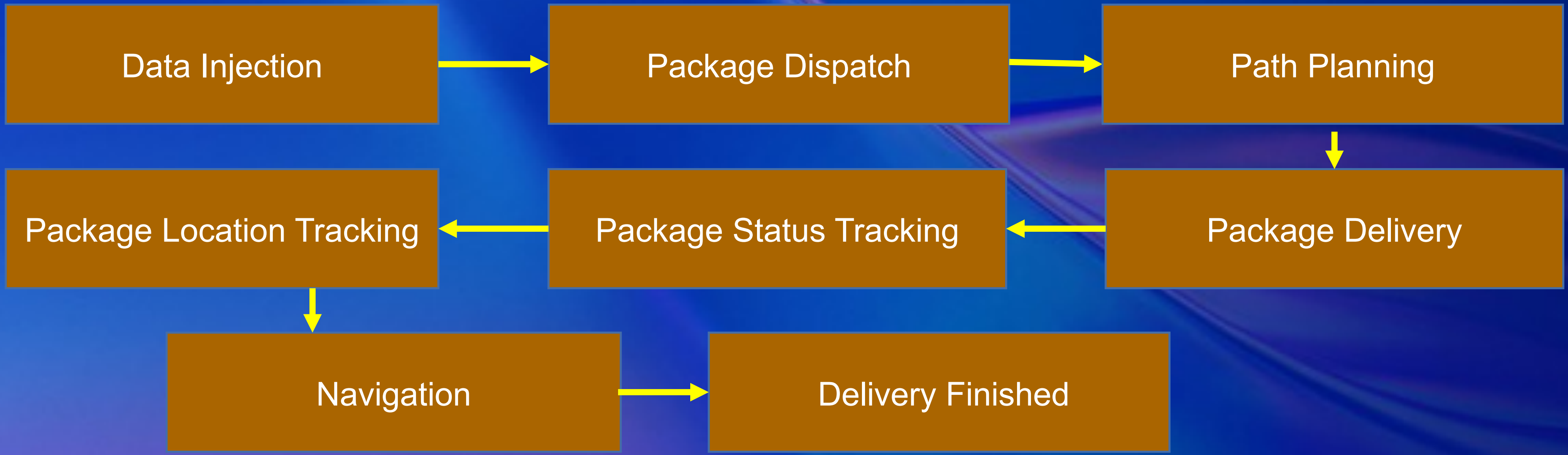
Kubernetes Practice In Rakuten Logistic System

Wang, Shuguang

Agenda

- Business Overview
- Systems Introduction
- Infrastructure
- Architecture
- Systems Security
- Summary
- Q/A(?)

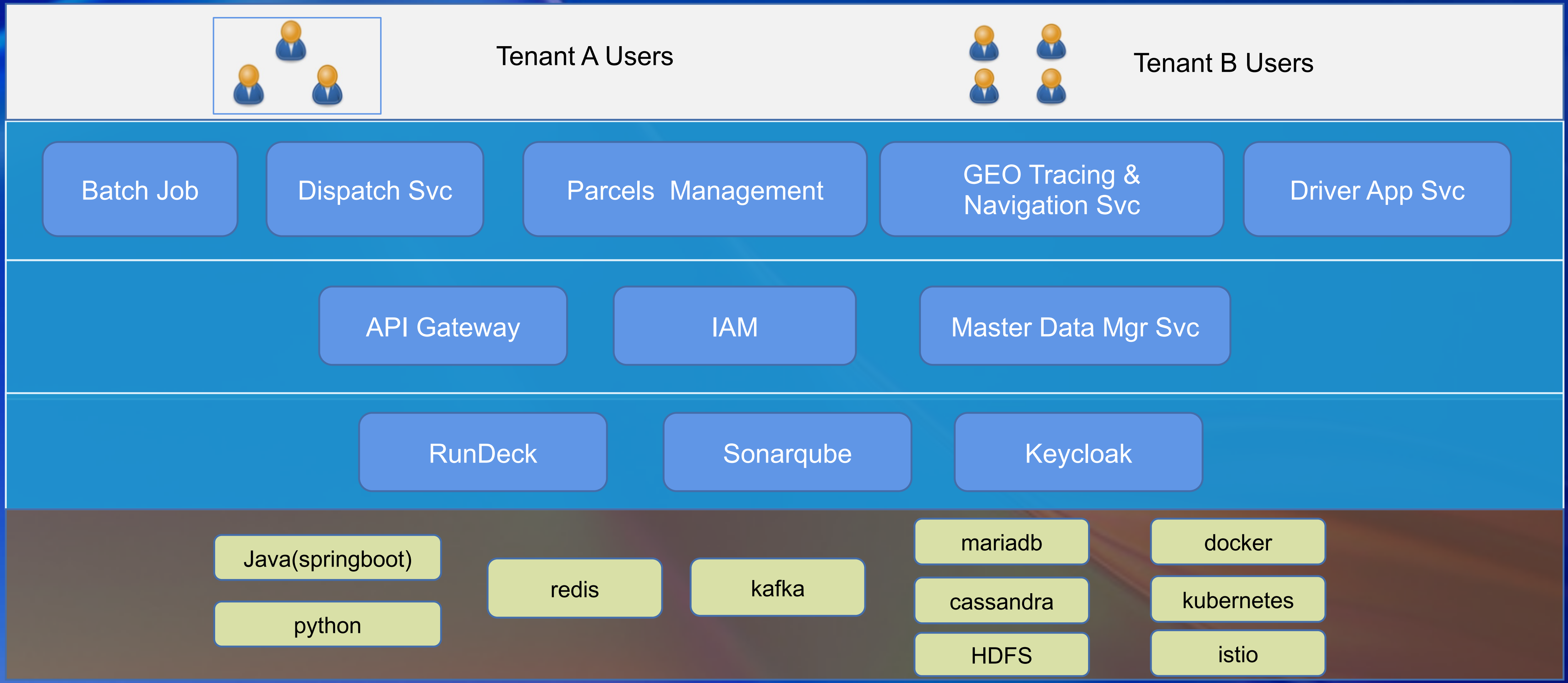
Business Introduction



Data Injection → Package Dispatch → Path Planning → Package Delivery → Package Status Tracking → Package Location Tracking → Navigation → Delivery Finished

System Overview

KUBERNETES
COMMUNITY DAYS DALIAN



Tenant A Users

Tenant B Users

Batch Job

Dispatch Svc

Parcels Management

GEO Tracing & Navigation Svc

Driver App Svc

API Gateway

IAM

Master Data Mgr Svc

RunDeck

Sonarqube

Keycloak

Java(springboot)

python

redis

kafka

mariadb

cassandra

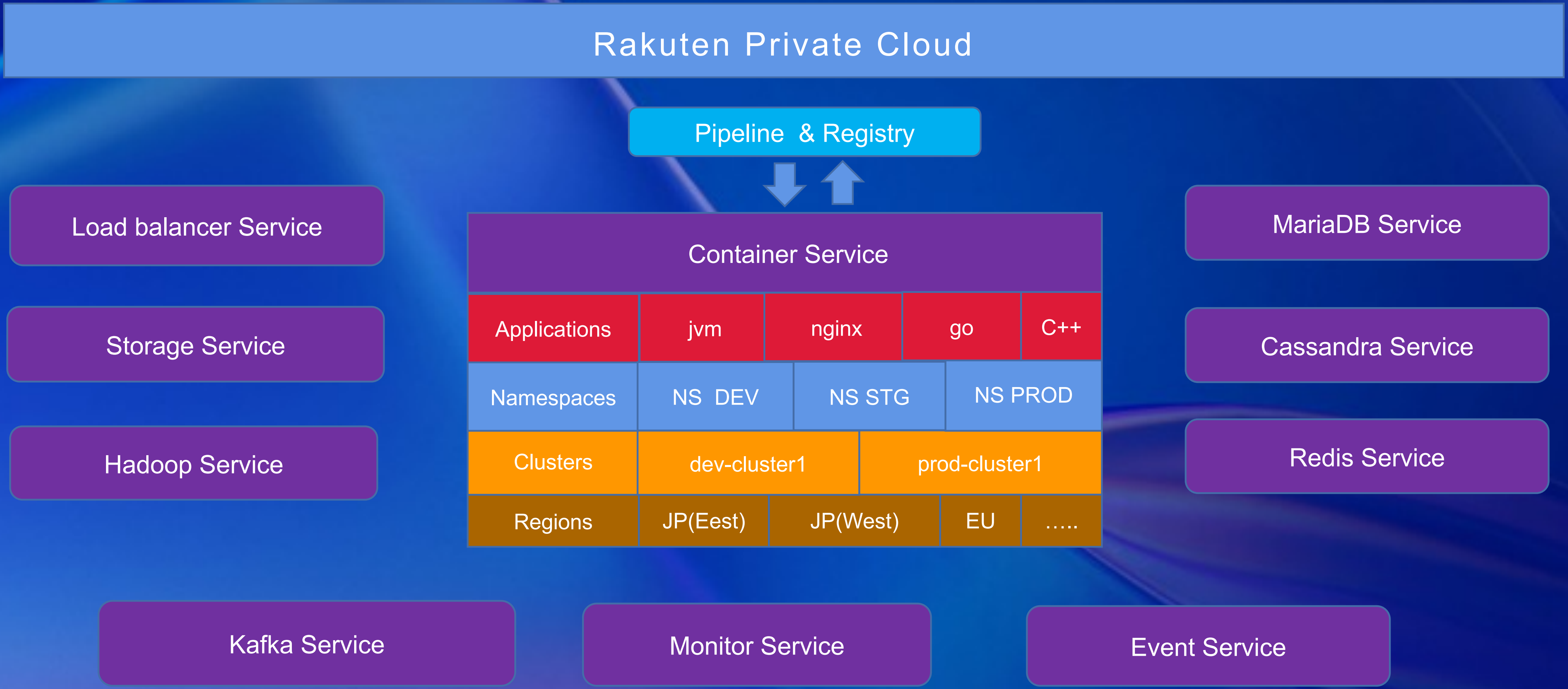
HDFS

docker

kubernetes

istio

Infrastructure



Rakuten Private Cloud

Pipeline & Registry

Load balancer Service

Storage Service

Hadoop Service

Container Service

Applications	jvm	nginx	go	C++
Namespaces	NS DEV	NS STG	NS PROD	
Clusters	dev-cluster1	prod-cluster1		
Regions	JP(Eest)	JP(West)	EU	…..

MariaDB Service

Cassandra Service

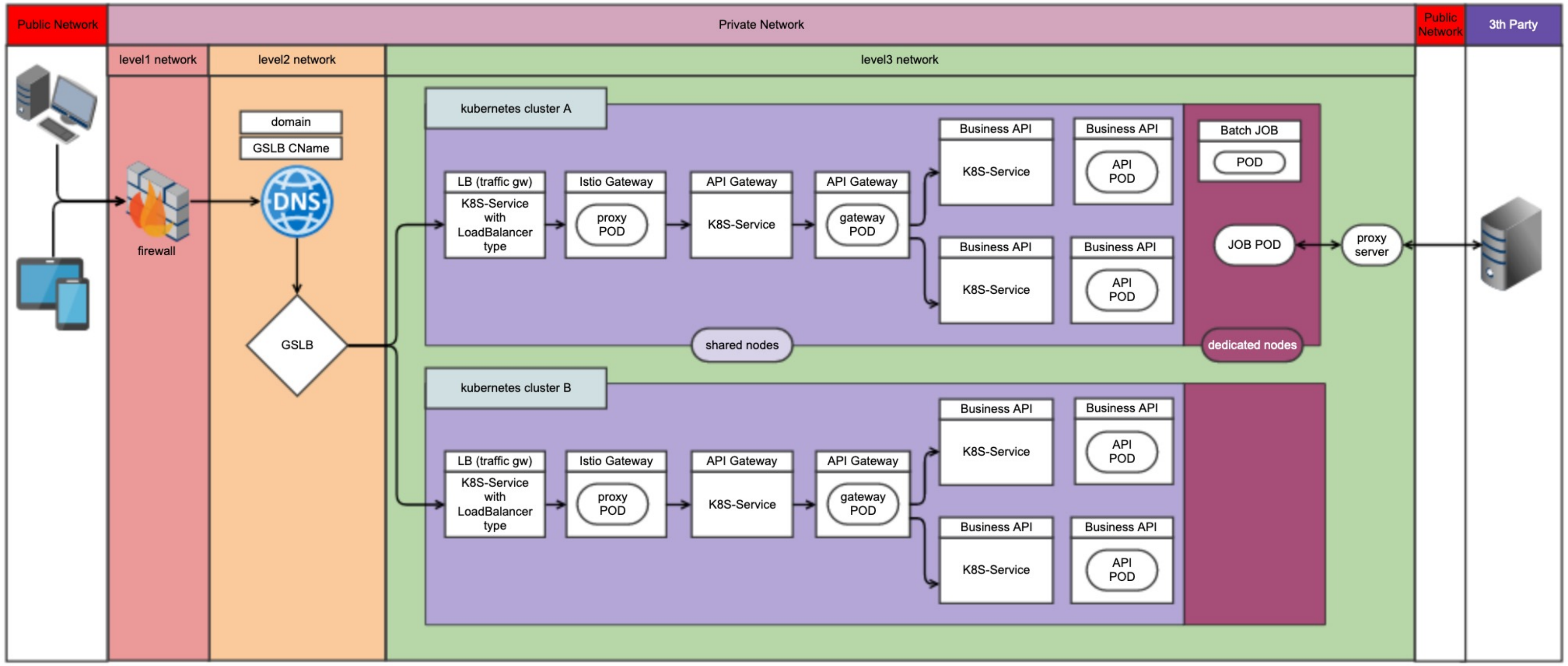
Redis Service

Kafka Service

Monitor Service

Event Service

Architecture



kubernetes | Deployment | Service | ConfigMap | Secret | PVC | HPA | Networkpolicy

istio | Gateway | Virtualservice | DestinationRule | AuthorizationPolicy | EnvoyFilter

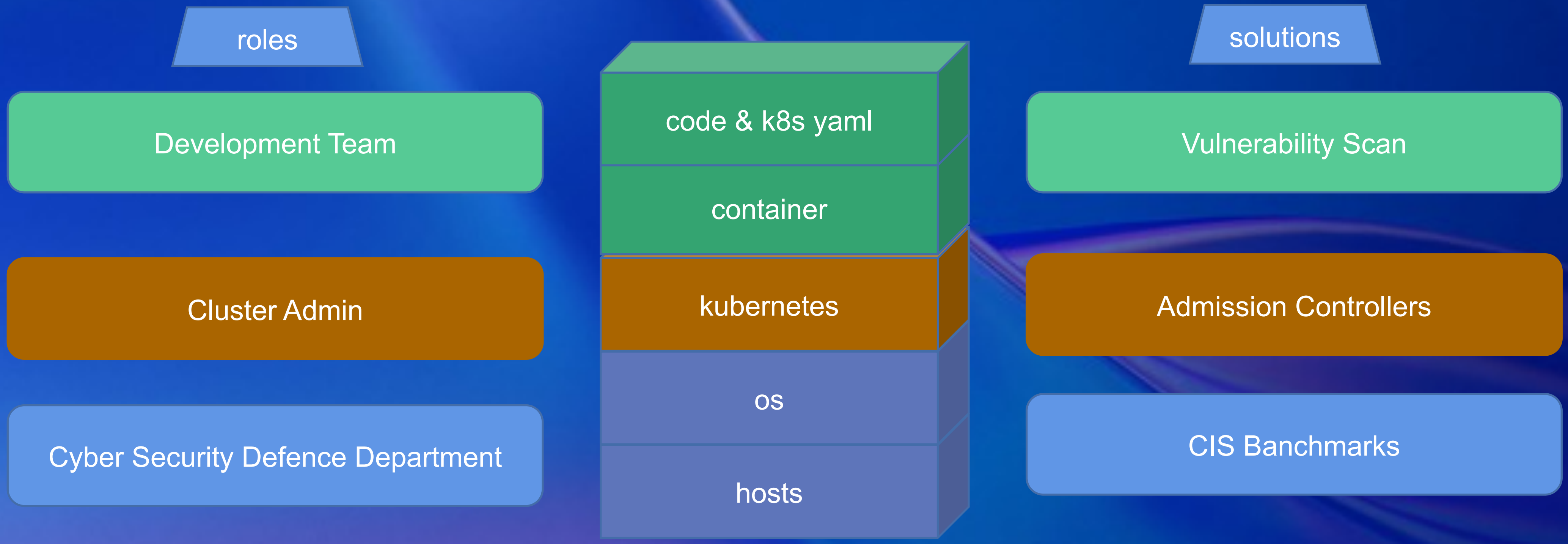
KUBERNETES
COMMUNITY DAYS DALIAN

Tech Stack

CI & CD	Application Runtime(K8S)	Image Registry	Log Shipping	Metric Collection	Tracing	Alert
Bitbucket	POD	HARBOR	Stack	prometheus	kiali	Elastic-alert
Jenkins	envoy istio-proxy				kiali	pagerduty
base library + Multi-Branch pipeline	Java app				jeager	
	file-beat					

Security

- **Purpose**
  - Shift Left, find & fix security issues early, save time & cost.
- **Roles and Solutions**



roles

Development Team

Cluster Admin

Cyber Security Defence Department

code & k8s yaml

container

kubernetes

os

hosts

solutions

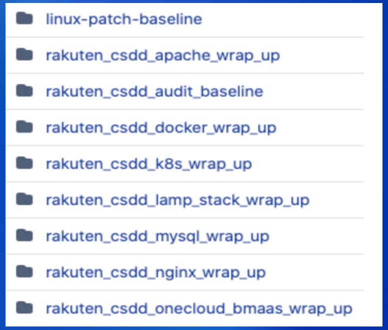
Vulnerability Scan

Admission Controllers

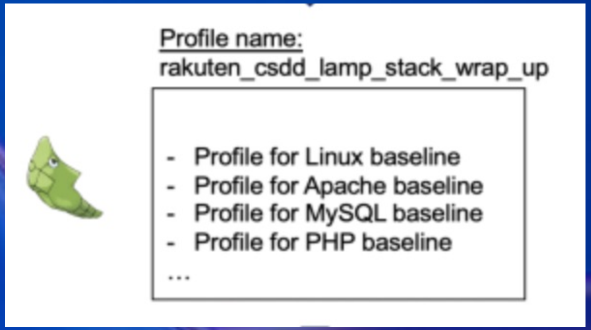
CIS Banchmarks

Security – Infra Misconfiguration

- Standard
  - CIS Benchmark compliance
    - Linux Baseline |Linux Patch Baseline | CIS Kubernetes Benchmark | CIS Docker Benchmark | …
  - Rakuten CSDD OS configuration compliance



linux-patch-baseline
rakuten_csdd_apache_wrap_up
rakuten_csdd_audit_baseline
rakuten_csdd_docker_wrap_up
rakuten_csdd_k8s_wrap_up
rakuten_csdd_lamp_stack_wrap_up
rakuten_csdd_mysql_wrap_up
rakuten_csdd_nginx_wrap_up
rakuten_csdd_onecloud_bmaas_wrap_up



Profile name:
rakuten_csdd_lamp_stack_wrap_up

- Profile for Linux baseline
- Profile for Apache baseline
- Profile for MySQL baseline
- Profile for PHP baseline

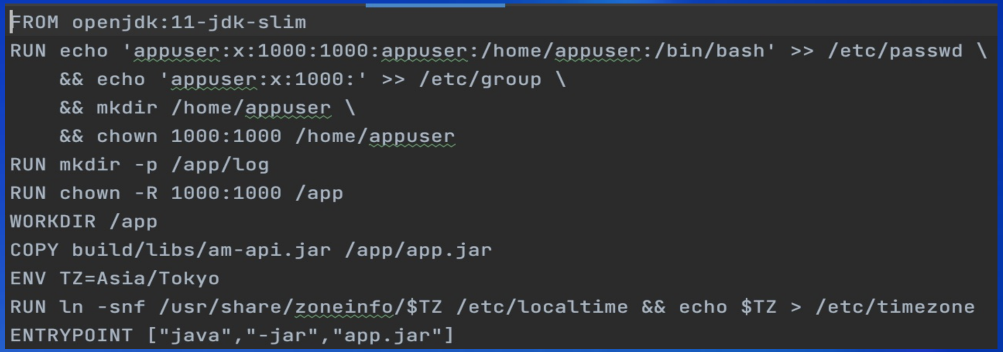
…

- Tool - MetaPod

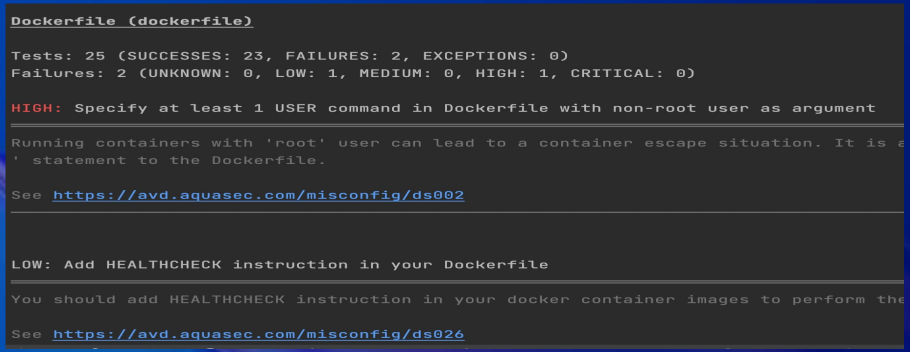
MetaPod is an operating system hardening/configuration audit (self-service compliance as code) project uses Chef InSpec (https://github.com/inspec/inspec) profiles to perform several controls on hosts.

Security – Image Vulnerability (1)

- Tool - Trivy :
  - Local scan for configuration files Dockerfile, k8s-resources.yaml
    - trivy fs --scanners config,vuln ./Dockerfile
    - trivy fs --scanners config,vuln ./deployment.yaml



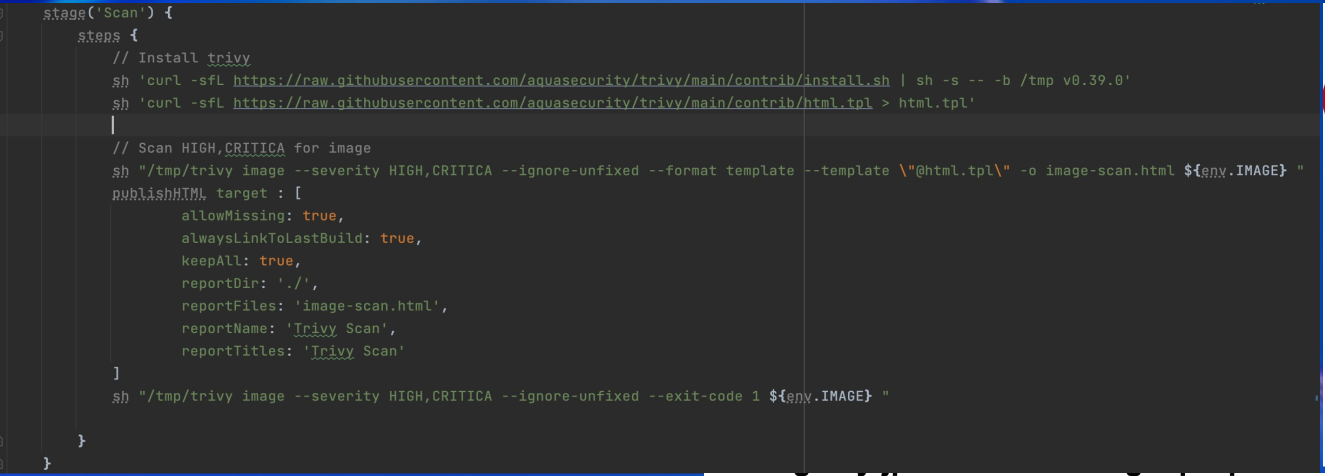
```
FROM openjdk:11-jdk-slim
RUN echo 'appuser:x:1000:1000:appuser:/home/appuser:/bin/bash' >> /etc/passwd \
    && echo 'appuser:x:1000:' >> /etc/group \
    && mkdir /home/appuser \
    && chown 1000:1000 /home/appuser
RUN mkdir -p /app/log
RUN chown -R 1000:1000 /app
WORKDIR /app
COPY build/libs/am-api.jar /app/app.jar
ENV TZ=Asia/Tokyo
RUN ln -snf /usr/share/zoneinfo/$TZ /etc/localtime && echo $TZ > /etc/timezone
ENTRYPOINT ["java","-jar","app.jar"]
```



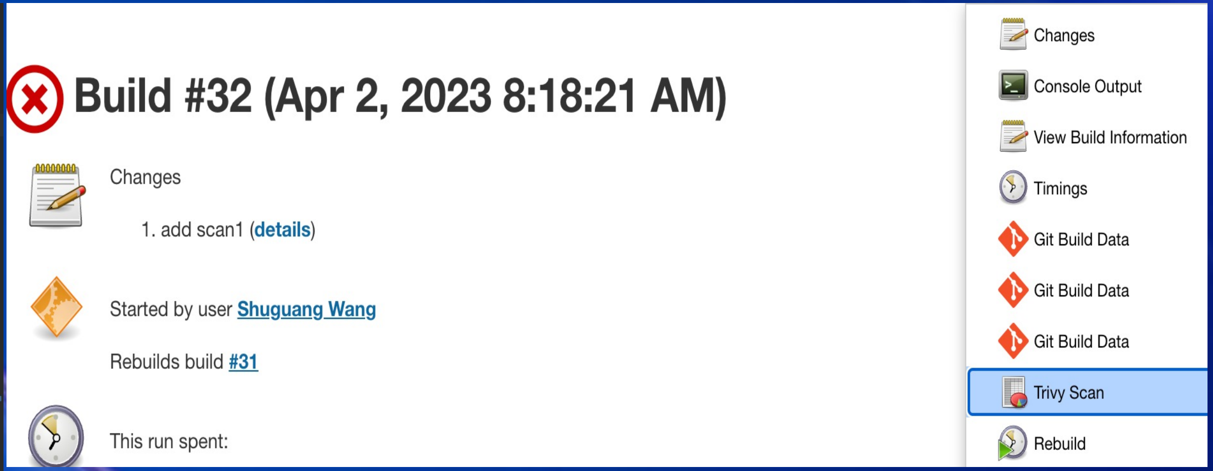
```
Dockerfile (dockerfile)

Tests: 25 (SUCCESSES: 23, FAILURES: 2, EXCEPTIONS: 0)
Failures: 2 (UNKNOWN: 0, LOW: 1, MEDIUM: 0, HIGH: 1, CRITICAL: 0)

HIGH: Specify at least 1 USER command in Dockerfile with non-root user as argument
══════════════════════════════════════════════════════════════════════
Running containers with 'root' user can lead to a container escape situation. It is a
' statement to the Dockerfile.

See https://avd.aquasec.com/misconfig/ds002
──────────────────────────────────────────────────────────────────────


LOW: Add HEALTHCHECK instruction in your Dockerfile
══════════════════════════════════════════════════════════════════════
You should add HEALTHCHECK instruction in your docker container images to perform the

See https://avd.aquasec.com/misconfig/ds026
```

Security - Image Vulnerability (2)

- Trivy : Integrate with Jenkins Pipeline and Harbor



```
stage('Scan') {
    steps {
        // Install trivy
        sh 'curl -sfL https://raw.githubusercontent.com/aquasecurity/trivy/main/contrib/install.sh | sh -s -- -b /tmp v0.39.0'
        sh 'curl -sfL https://raw.githubusercontent.com/aquasecurity/trivy/main/contrib/html.tpl > html.tpl'

        // Scan HIGH,CRITICA for image
        sh "/tmp/trivy image --severity HIGH,CRITICA --ignore-unfixed --format template --template \"@html.tpl\" -o image-scan.html ${env.IMAGE} "
        publishHTML target : [
                allowMissing: true,
                alwaysLinkToLastBuild: true,
                keepAll: true,
                reportDir: './',
                reportFiles: 'image-scan.html',
                reportName: 'Trivy Scan',
                reportTitles: 'Trivy Scan'
        ]
        sh "/tmp/trivy image --severity HIGH,CRITICA --ignore-unfixed --exit-code 1 ${env.IMAGE} "

    }
}
```



Build #32 (Apr 2, 2023 8:18:21 AM)

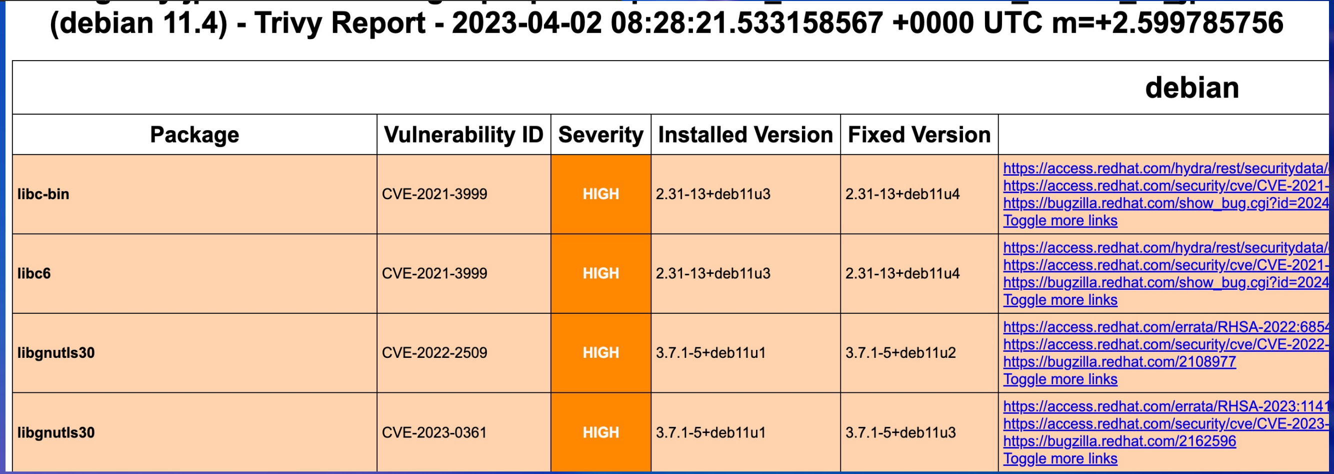
Changes

1. add scan1 (details)

Started by user Shuguang Wang

Rebuilds build #31

This run spent:



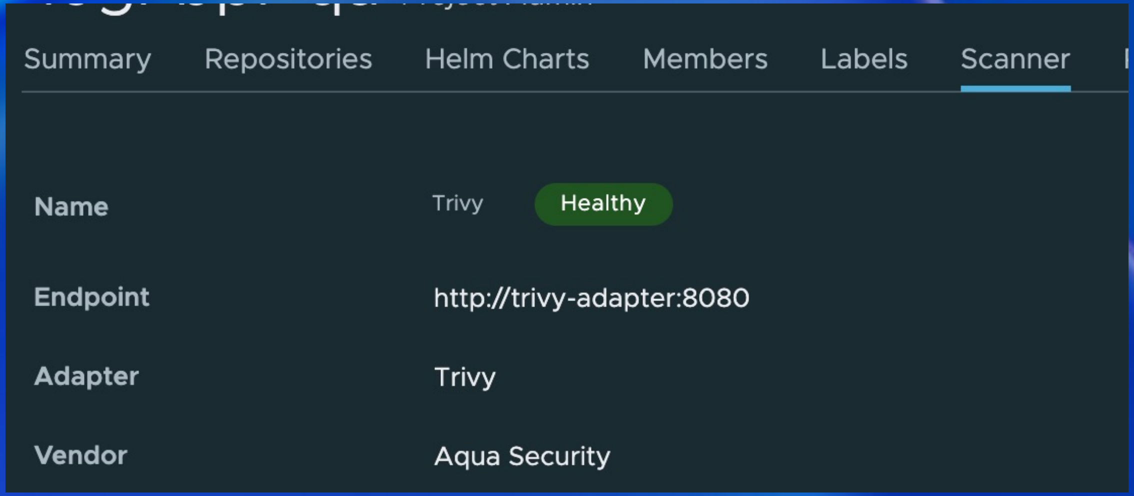
(debian 11.4) - Trivy Report - 2023-04-02 08:28:21.533158567 +0000 UTC m=+2.599785756

debian

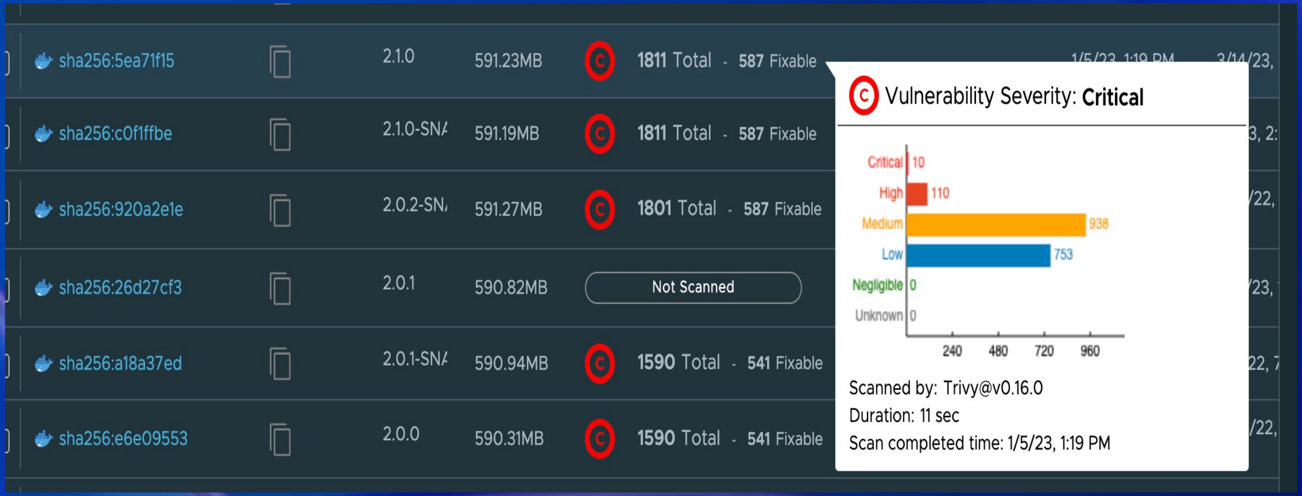
Package	Vulnerability ID	Severity	Installed Version	Fixed Version	
libc-bin	CVE-2021-3999	HIGH	2.31-13+deb11u3	2.31-13+deb11u4	https://access.redhat.com/hydra/rest/securitydata/ https://access.redhat.com/security/cve/CVE-2021- https://bugzilla.redhat.com/show_bug.cgi?id=2024 Toggle more links
libc6	CVE-2021-3999	HIGH	2.31-13+deb11u3	2.31-13+deb11u4	https://access.redhat.com/hydra/rest/securitydata/ https://access.redhat.com/security/cve/CVE-2021- https://bugzilla.redhat.com/show_bug.cgi?id=2024 Toggle more links
libgnutls30	CVE-2022-2509	HIGH	3.7.1-5+deb11u1	3.7.1-5+deb11u2	https://access.redhat.com/errata/RHSA-2022:6854 https://access.redhat.com/security/cve/CVE-2022- https://bugzilla.redhat.com/2108977 Toggle more links
libgnutls30	CVE-2023-0361	HIGH	3.7.1-5+deb11u1	3.7.1-5+deb11u3	https://access.redhat.com/errata/RHSA-2023:1141 https://access.redhat.com/security/cve/CVE-2023- https://bugzilla.redhat.com/2162596 Toggle more links

Security - Image Vulnerability (3)

- Trivy : Integrate with Harbor



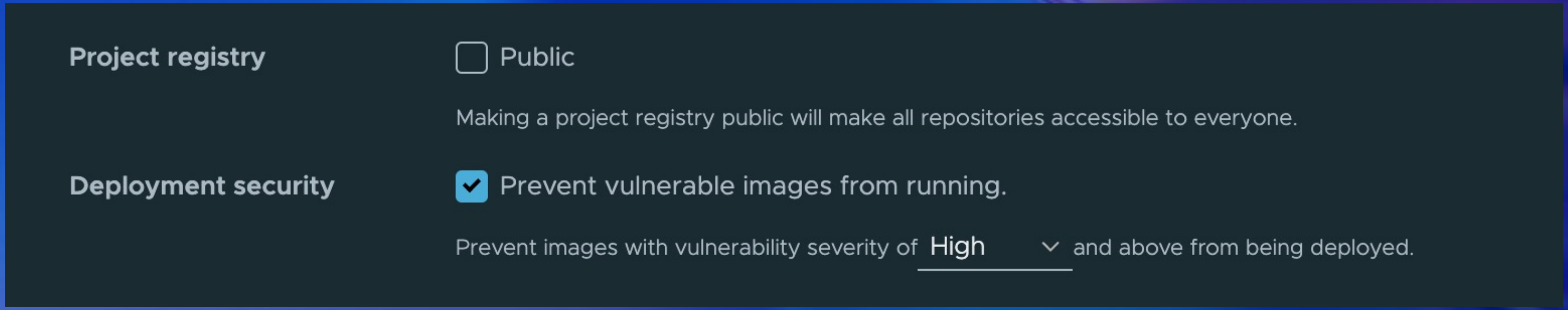
Name	Trivy Healthy
Endpoint	http://trivy-adapter:8080
Adapter	Trivy
Vendor	Aqua Security



sha256:5ea71f15	2.1.0	591.23MB	1811 Total - 587 Fixable	1/5/23, 1:19 PM	3/14/23,
sha256:c0f1ffbe	2.1.0-SN/	591.19MB	1811 Total - 587 Fixable		3, 2:
sha256:920a2e1e	2.0.2-SN/	591.27MB	1801 Total - 587 Fixable		/22,
sha256:26d27cf3	2.0.1	590.82MB	Not Scanned		/23,
sha256:a18a37ed	2.0.1-SN/	590.94MB	1590 Total - 541 Fixable		22, 7
sha256:e6e09553	2.0.0	590.31MB	1590 Total - 541 Fixable		/22,

Vulnerability Severity: **Critical**

Scanned by: Trivy@v0.16.0
Duration: 11 sec
Scan completed time: 1/5/23, 1:19 PM



Project registry ☐ Public

Making a project registry public will make all repositories accessible to everyone.

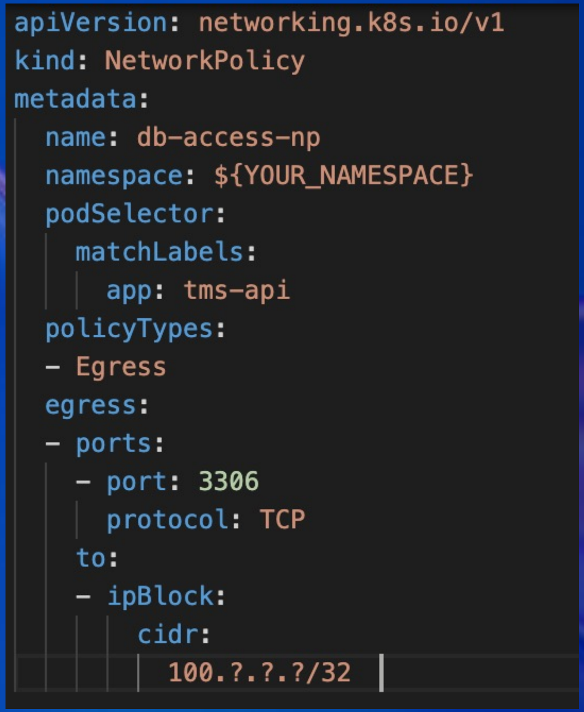
Deployment security ☑ Prevent vulnerable images from running.

Prevent images with vulnerability severity of High ⌄ and above from being deployed.

Security - POD Access Control

Solution

- Globalnetworkpolicies (cluster scope)
  - your pod can use GlobalNetworkPolicy to access to or be accessed from kube-apiserver
- networkpolicies (namespace scope)
  - Default Settings
    - to/from the same namespace.
    - to/from istio-system namespace.
    - to coredns (kubernetes dns).
  - User Settings



```yaml
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: db-access-np
  namespace: ${YOUR_NAMESPACE}
  podSelector:
    matchLabels:
      app: tms-api
  policyTypes:
  - Egress
  egress:
  - ports:
    - port: 3306
      protocol: TCP
    to:
    - ipBlock:
        cidr:
          100.?.?.?/32
```

Summary

- Kubernetes, prometheus, elk ,kiali - High avaiability, scalability , observability and pod level access control.
- Istio – service governance, traffic control ,fault injection and servicel level access control.
- Trivy – configuration files and container vulnerability scan.

Thanks