



{KODE}{KLOUD



{KODE}{CLOUD

Service Mesh with Istio

Sevi Karakose

Instructor



Course Format

Course Video GIF

LAB GIF

Objectives

Monoliths &
Microservices

Service
Mesh

Istio

Install
Istio

Visualizing
with
Kiali

Objectives

Gateways

Virtual Services

Destination Rules

Subsets

Timeouts

Retries

Circuit Breaking

Fault Injection

Request Routing

A/B Testing

Objectives




Objectives



Viewing and
Collecting
Metrics



Kiali In
Detail



Distributed
Tracing



{KODE}{KLOUD

PRE-REQUISITES



Pre-Requisites



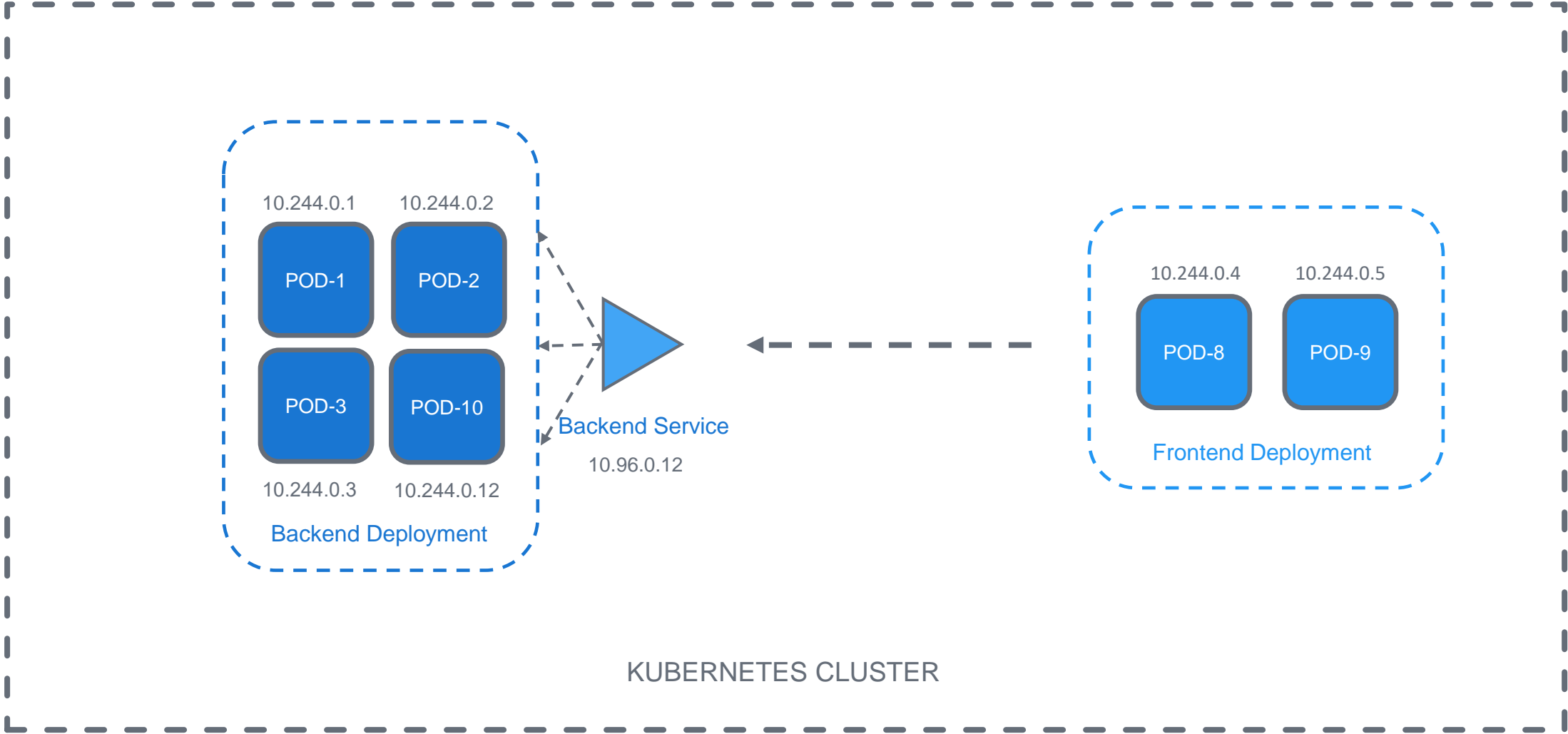


{KODE}{KLOUD

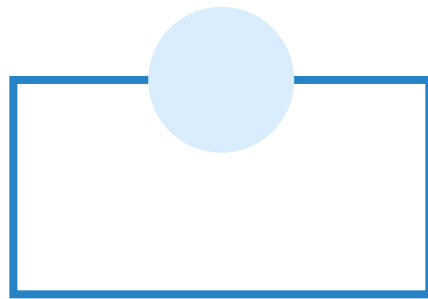
KUBERNETES SERVICES



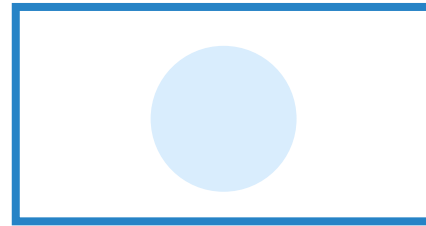
Kubernetes Services



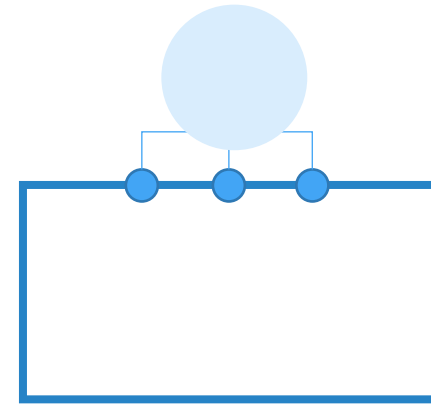
Kubernetes Services



NodePort



ClusterIP



LoadBalancer



{KODE}{KLOUD

KUBERNETES ON YOUR LOCAL MACHINES

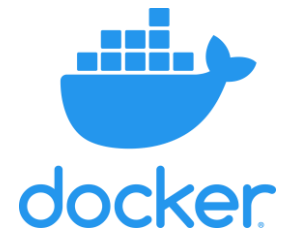


Two Popular Kubernetes Tools

kind



minikube



Hyperkit



podman

How to Install Minikube

The screenshot shows a web browser window with the URL `minikube.sigs.k8s.io/docs/start/`. The page title is "minikube start". The left sidebar contains a navigation menu with items like "Documentation", "Get Started!", "Handbook", "Basic controls", "Deploying apps", "Kubectl", "Accessing apps", "Addons", "Configuration", "Dashboard", "Pushing images", "Proxies and VPNs", "Registries", "Certificates", "Offline usage", "Host access", "Persistent Volumes", "Mounting filesystems", "File Sync", "Troubleshooting", "FAQ", "Presentations", "Tutorials", "Commands", "Drivers", "Contributing", and "Benchmarks".

minikube start

minikube is local Kubernetes, focusing on making it easy to learn and develop for Kubernetes.

All you need is Docker (or similarly compatible) container or a Virtual Machine environment, and Kubernetes is a single command away: `minikube start`

What you'll need

- 2 CPUs or more
- 2GB of free memory
- 20GB of free disk space
- Internet connection
- Container or virtual machine manager, such as: [Docker](#), [Hyperkit](#), [Hyper-V](#), [KVM](#), [Parallels](#), [Podman](#), [VirtualBox](#), or [VMWare](#)

1 Installation

Click on the buttons that describe your target platform. For other architectures, see [the release page](#) for a complete list of minikube binaries.

Operating system: [Linux](#) **[macOS](#)** [Windows](#)

Architecture: **[x86-64](#)** [ARM64](#)

Installer type: **[Binary download](#)** [Homebrew](#)

To install minikube on x86-64 macOS using binary download:

```
curl -L0 https://storage.googleapis.com/minikube/releases/latest/minikube-darwin-amd64
sudo install minikube-darwin-amd64 /usr/local/bin/minikube
```

2 Start your cluster

From a terminal with administrator access (but not logged in as root), run:

```
minikube start
```

Setting up Kubernetes Cluster with MiniKube

> _

```
$ minikube start
```

```
😊 minikube v1.16.0 on Darwin 10.15.5
```

```
📦 minikube 1.19.0 is available! Download it:
```

```
https://github.com/kubernetes/minikube/releases/tag/v1.19.0
```

```
💡 To disable this notice, run: 'minikube config set WantUpdateNotification false'
```

```
🌟 Automatically selected the docker driver
```

```
👍 Starting control plane node minikube in cluster minikube
```

```
📦 Pulling base image ...
```

```
🏠 Creating docker container (CPUs=2, Memory=4000MB) ...
```

```
! This container is having trouble accessing https://k8s.gcr.io
```

```
💡 To pull new external images, you may need to configure a proxy:
```

```
https://minikube.sigs.k8s.io/docs/reference/networking/proxy/
```

```
📦 Preparing Kubernetes v1.20.0 on Docker 20.10.0 ...
```

```
▪ Generating certificates and keys ...
```

```
▪ Booting up control plane ...
```

```
▪ Configuring RBAC rules ...
```

```
🔍 Verifying Kubernetes components...
```

```
🌟 Enabled addons: storage-provisioner, default-storageclass
```

```
🏠 Done! kubectl is now configured to use "minikube" cluster and "default" namespace by default
```

Setting up Kubernetes Cluster with MiniKube

```
>_
```

```
$ minikube addons enable ingress
```

```
Exiting due to MK_USAGE: Due to networking limitations of driver docker on darwin,  
ingress addon is not supported.
```

```
Alternatively to use this addon you can use a vm-based driver:
```

```
'minikube start --vm=true'
```

```
To track the update on this work in progress feature please check:  
https://github.com/kubernetes/minikube/issues/7332
```

Setting up Kubernetes Cluster with MiniKube

> _

```
$ minikube start --vm=true
```

```
😊 minikube v1.16.0 on Darwin 10.15.7
🌟 Automatically selected the hyperkit driver
👍 Starting control plane node minikube in cluster minikube
🔥 Creating hyperkit VM (CPUs=2, Memory=4000MB, Disk=20000MB) ...
📦 Preparing Kubernetes v1.20.0 on Docker 20.10.0 ...
  ▪ Generating certificates and keys ...
  ▪ Booting up control plane ...
  ▪ Configuring RBAC rules ...
🔍 Verifying Kubernetes components...
🌟 Enabled addons: storage-provisioner, default-storageclass

  ▪ Want kubectl v1.20.0? Try 'minikube kubectl -- get pods -A'
📦 Done! kubectl is now configured to use "minikube" cluster and "default" namespace
by default
```

```
$ minikube addons enable ingress
```

```
🔍 Verifying ingress addon...
🌟 The 'ingress' addon is enabled
```

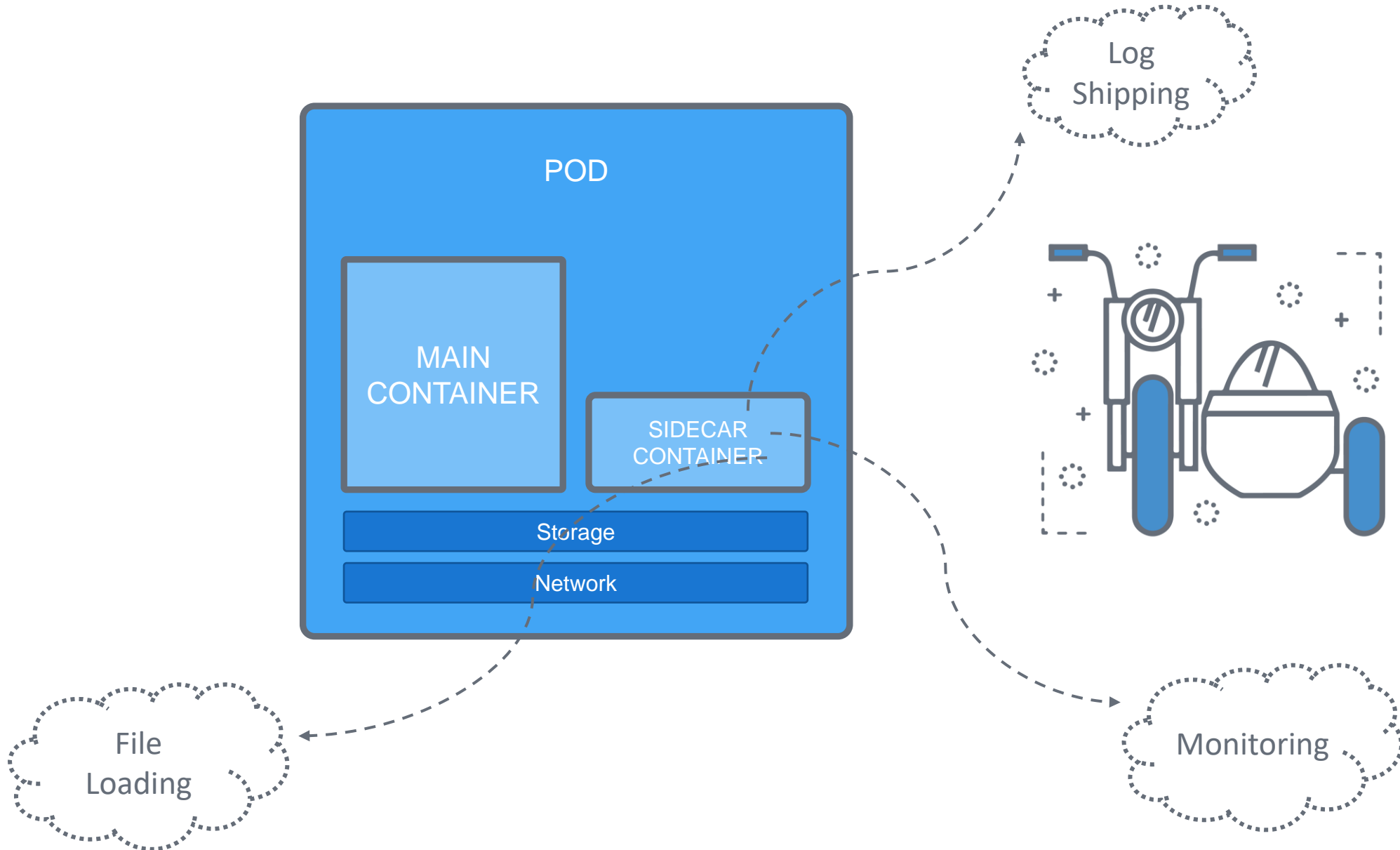


{KODE}{KLOUD

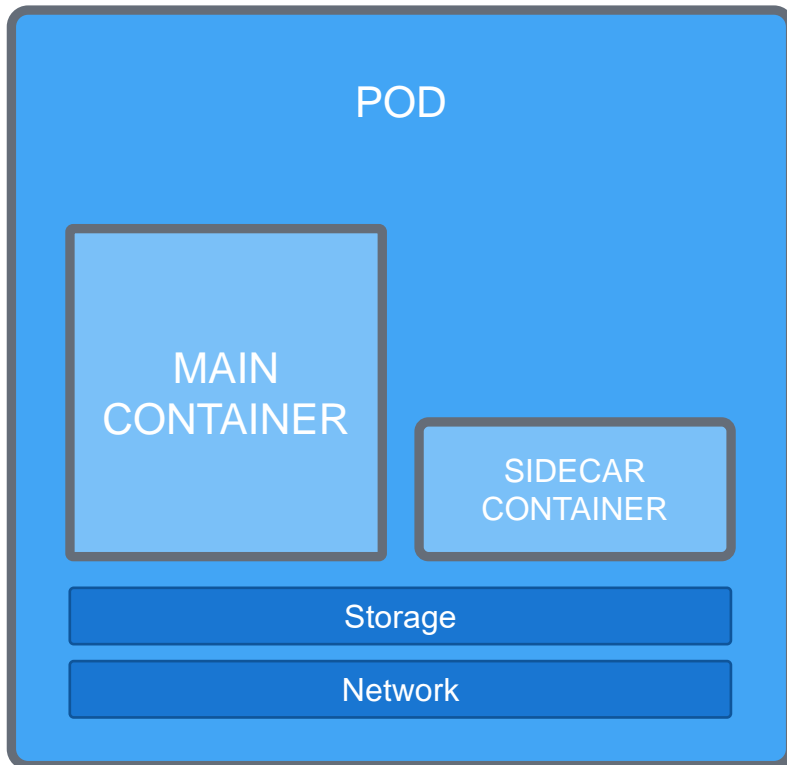
SIDECARS



Sidecars



Sidecars



```
pod.yaml

containers:
- name: nginx-container
  image: nginx
  volumeMounts:
  - name: shared-data
    mountPath: /usr/share/nginx/html
- name: sidecar-container
  image: fluent/fluentd
  volumeMounts:
  - name: shared-data
    mountPath: /pod-data
```

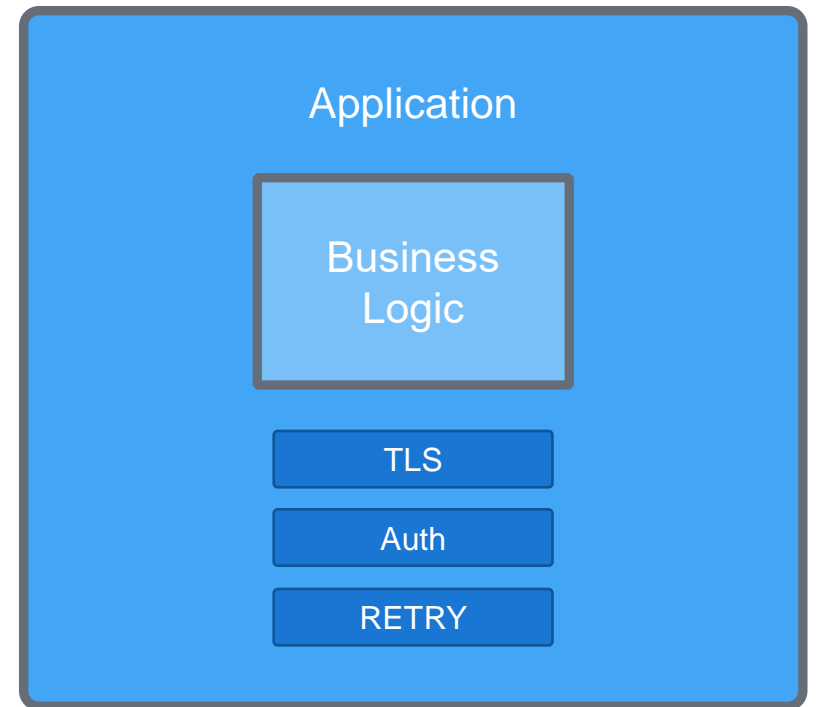


{KODE}{KLOUD

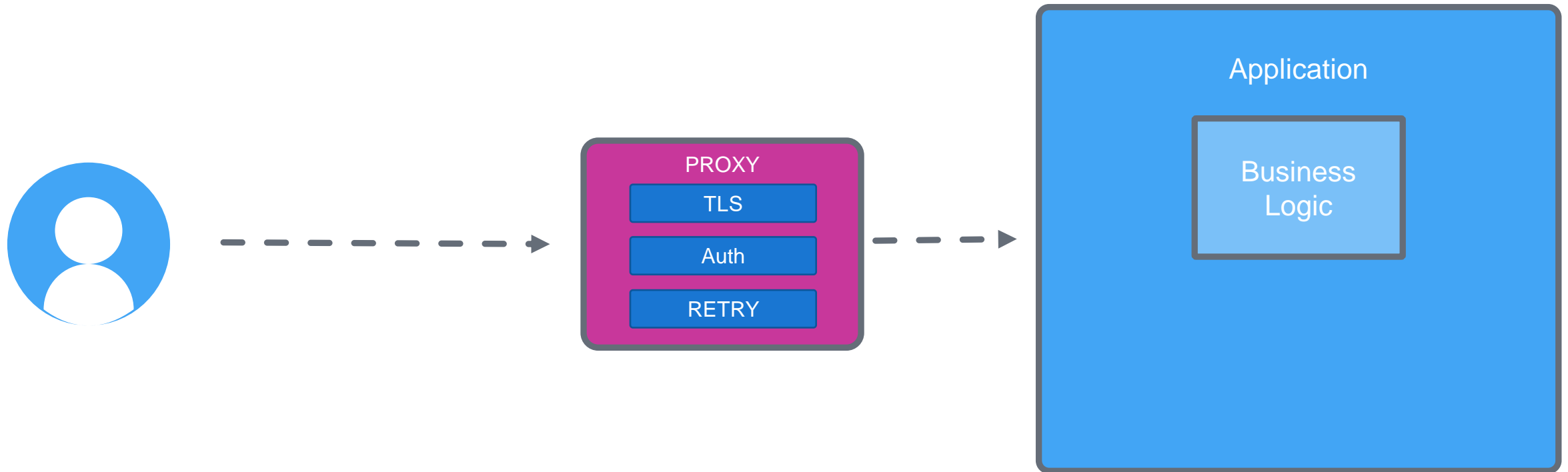
ENVOY

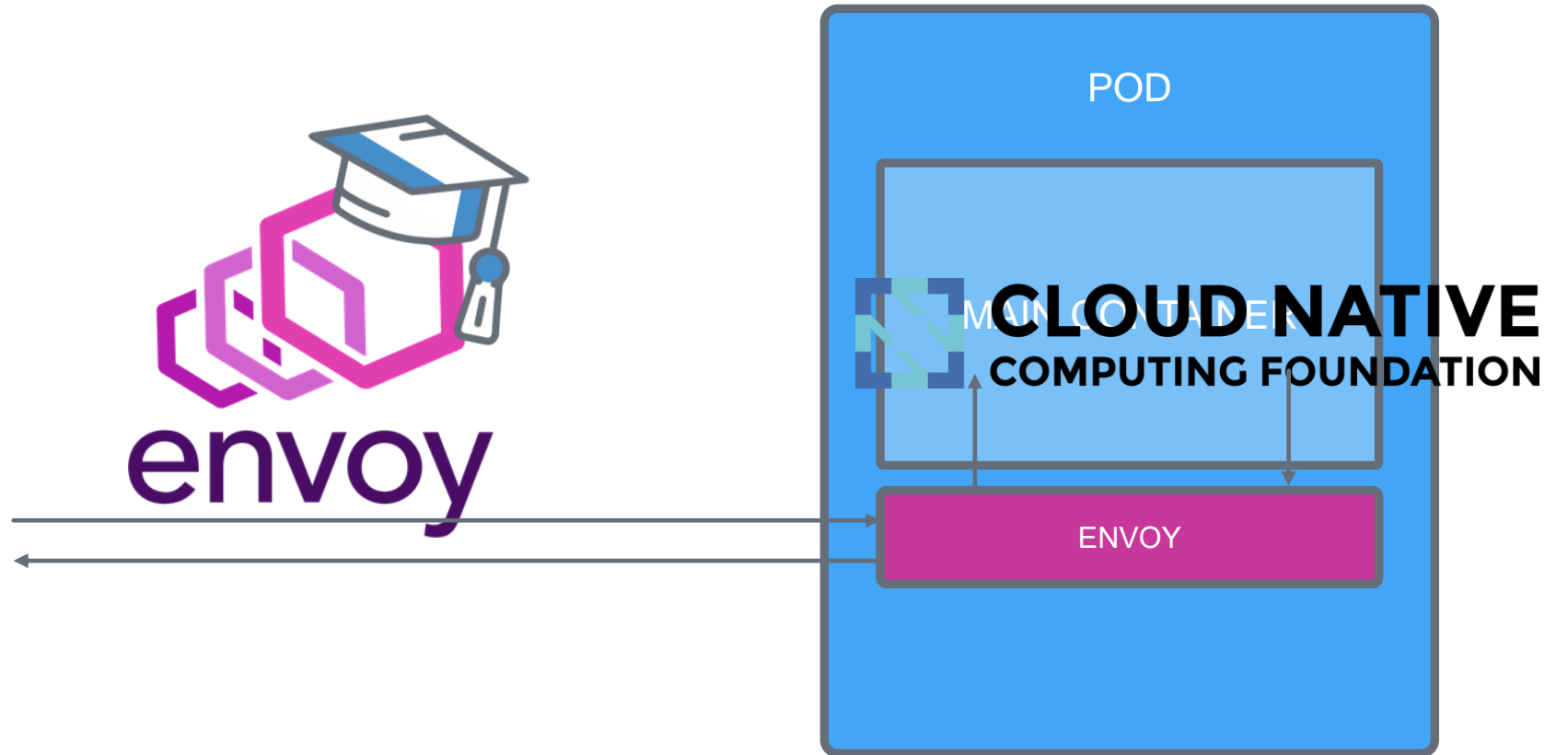


Proxy



Proxy







{KODE}{KLOUD

SECTION INTRODUCTION



Objectives

Monoliths &
Microservices

What is a
Service Mesh?

Istio

Installing
Istioctl

Installing Istio
on Your Cluster

Deploying Our
First App with
Istio

Visualizing
Service Mesh
with Kiali

Installing Kiali

Create Traffic
Into Your
Mesh



{KODE}{KLOUD

MONOLITHS & MICROSERVICES



Software Development until the 2000s



Agile Manifesto



Individuals & Interactions

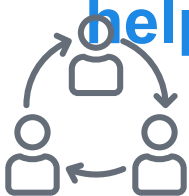
Processes and Tools



Working Software

Comprehensive Documentation

“We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:”



Customer Collaboration

Contract Negotiation

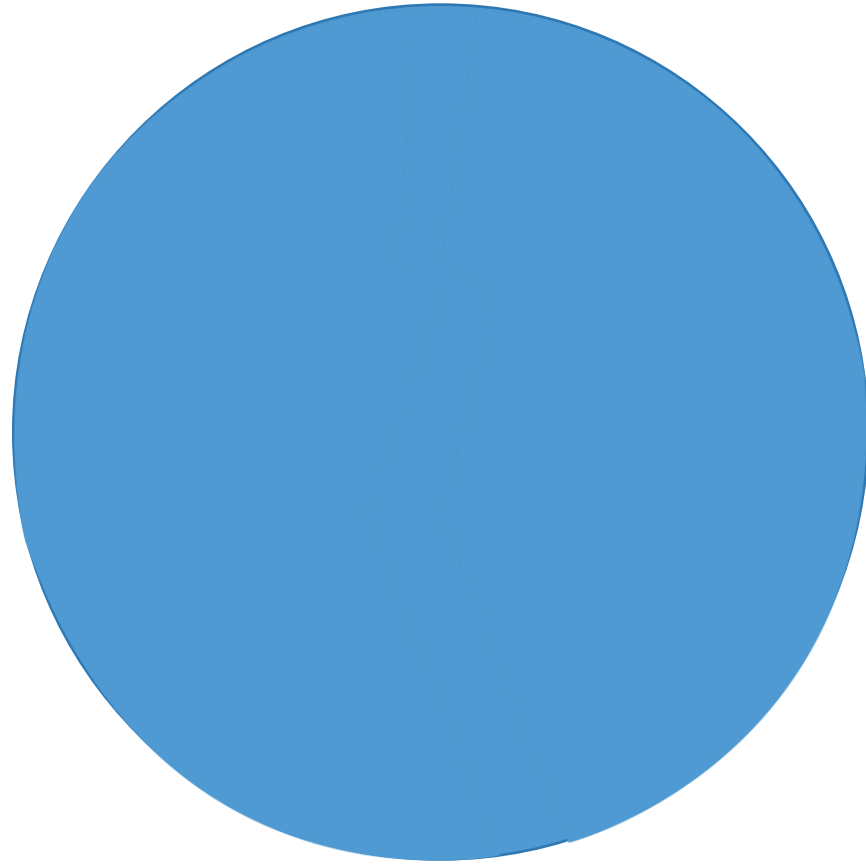


Responding to Change

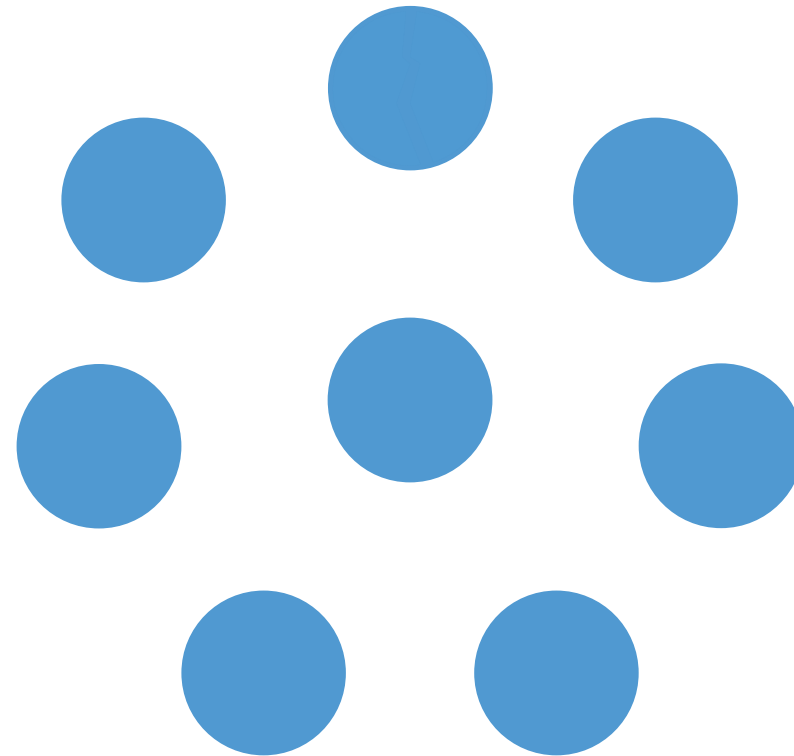
Following a plan

“That is, while there is value in the items on the right, we value the items on the left more.”

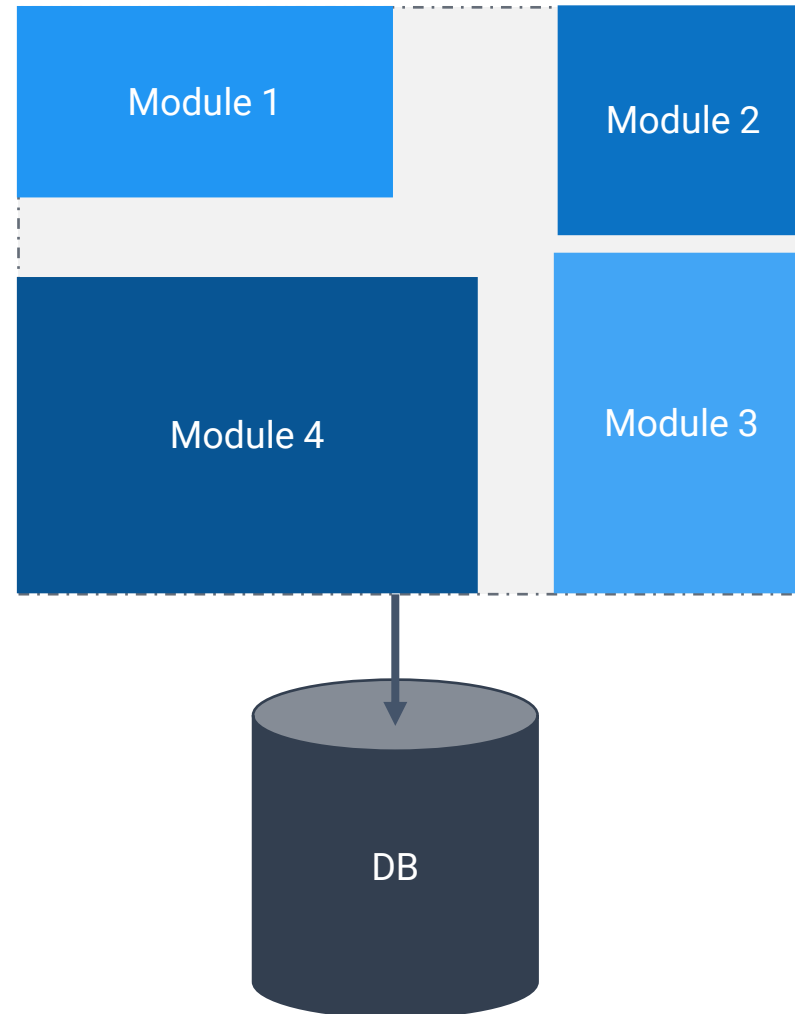
Agile Practices



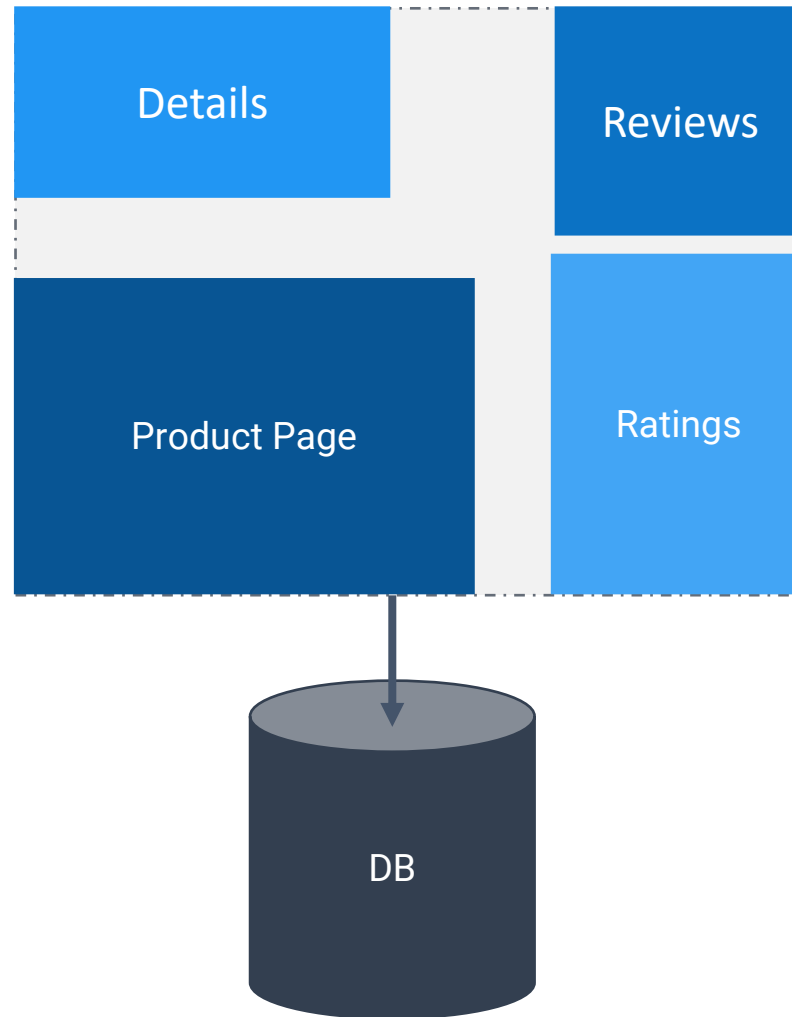
Agile Practices



Monolithic Applications



A Monolithic Book Info App



A Monolithic Book Info App

BookInfo Sample

Sign in

The Comedy of Errors

Summary: [Wikipedia Summary](#): The Comedy of Errors is one of **William Shakespeare's** early plays. It is his shortest and one of his most farcical comedies, with a major part of the humour coming from slapstick and mistaken identity, in addition to puns and word play.

Book Details

Type:
paperback
Pages:
200
Publisher:
PublisherA
Language:
English
ISBN-10:
1234567890
ISBN-13:
123-1234567890

Book Reviews

An extremely entertaining play by Shakespeare. The slapstick humour is refreshing!

— Reviewer1

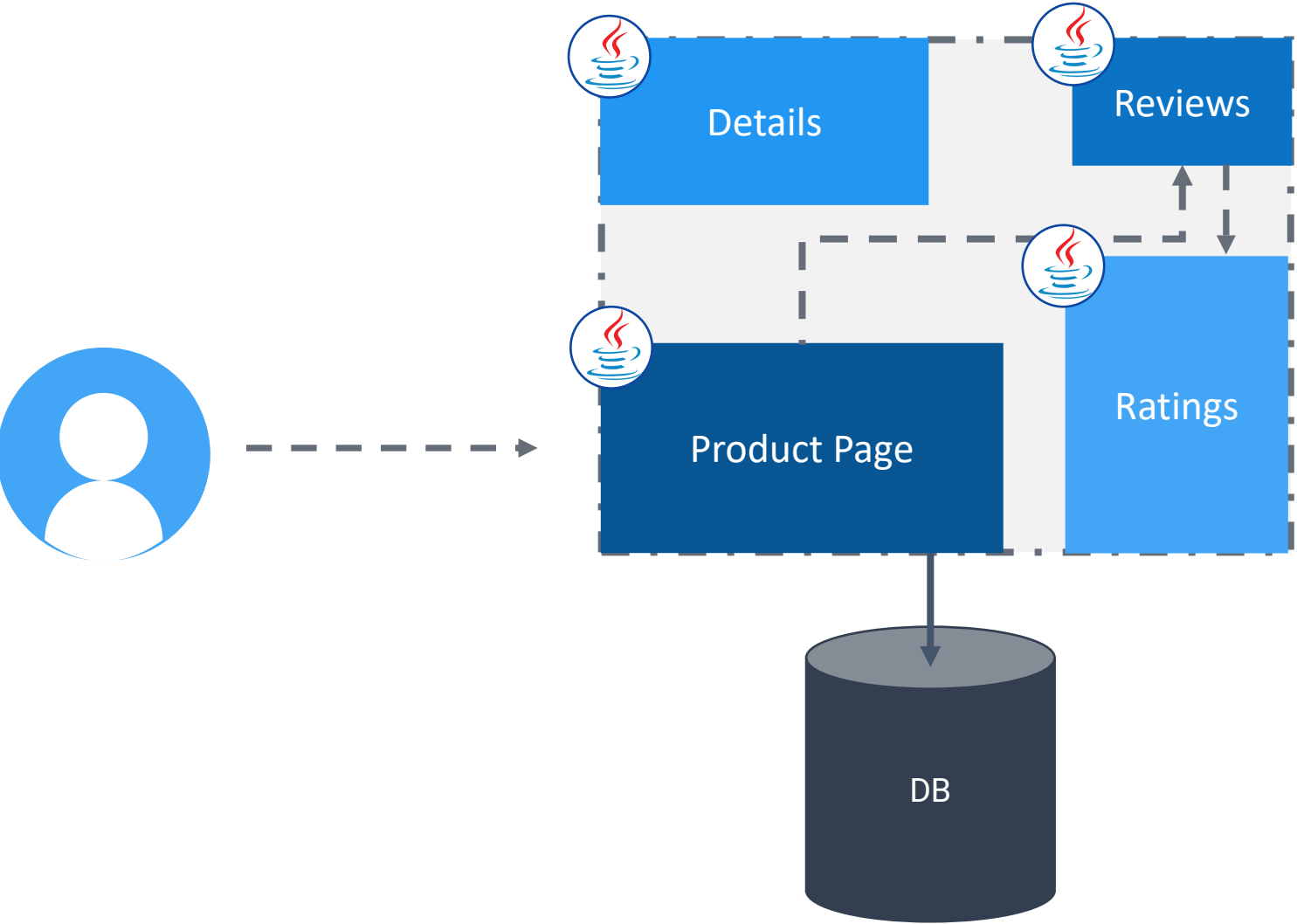


Absolutely fun and entertaining. The play lacks thematic depth when compared to other plays by Shakespeare.

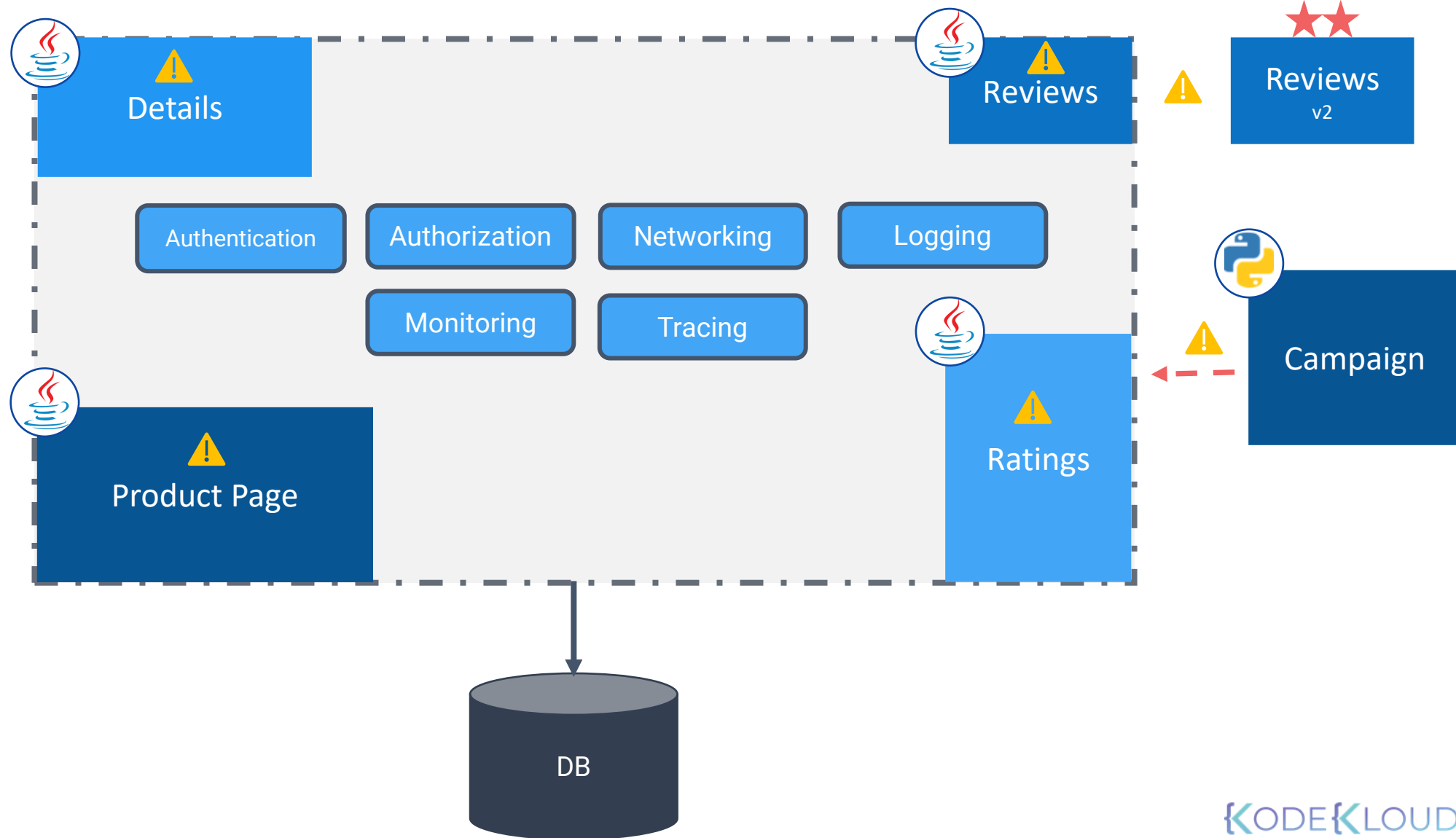
— Reviewer2



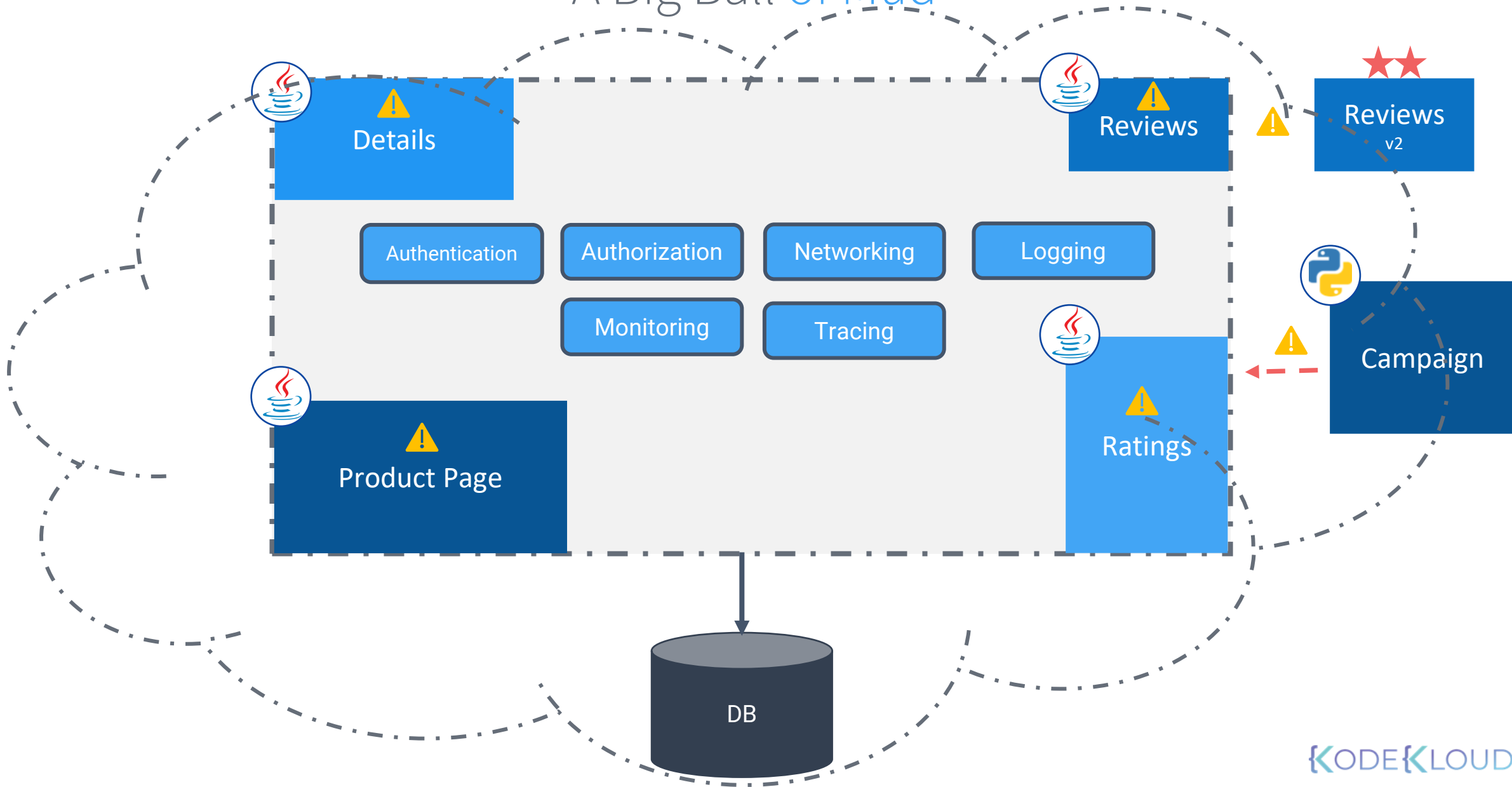
A Monolithic Book Info App



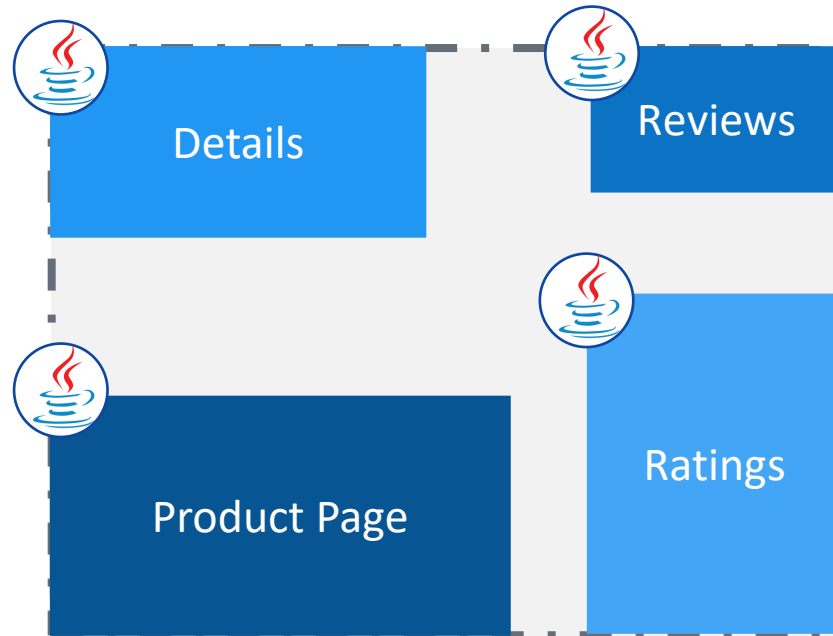
A Monolithic Book Info App



A Big Ball of Mud



A Monolithic Book Info App



A **Microservices** Book Info App



Product Page



Details

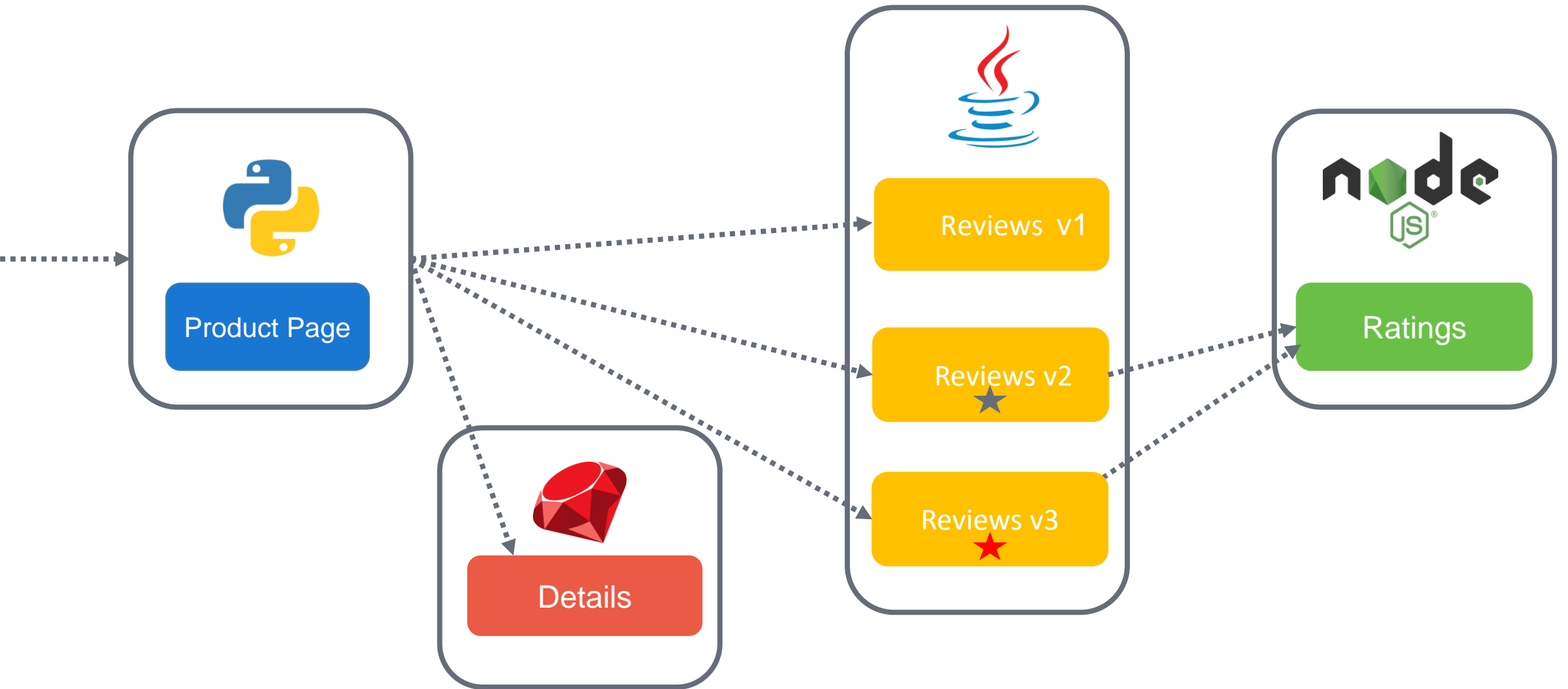


Reviews



Ratings

A Microservices Book Info App



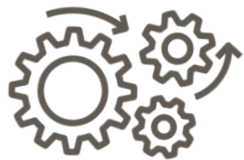
Pros of Microservices



 **Scalability**



 **Faster, smaller releases**



 **Technology and language agnostic
Development lifecycle**

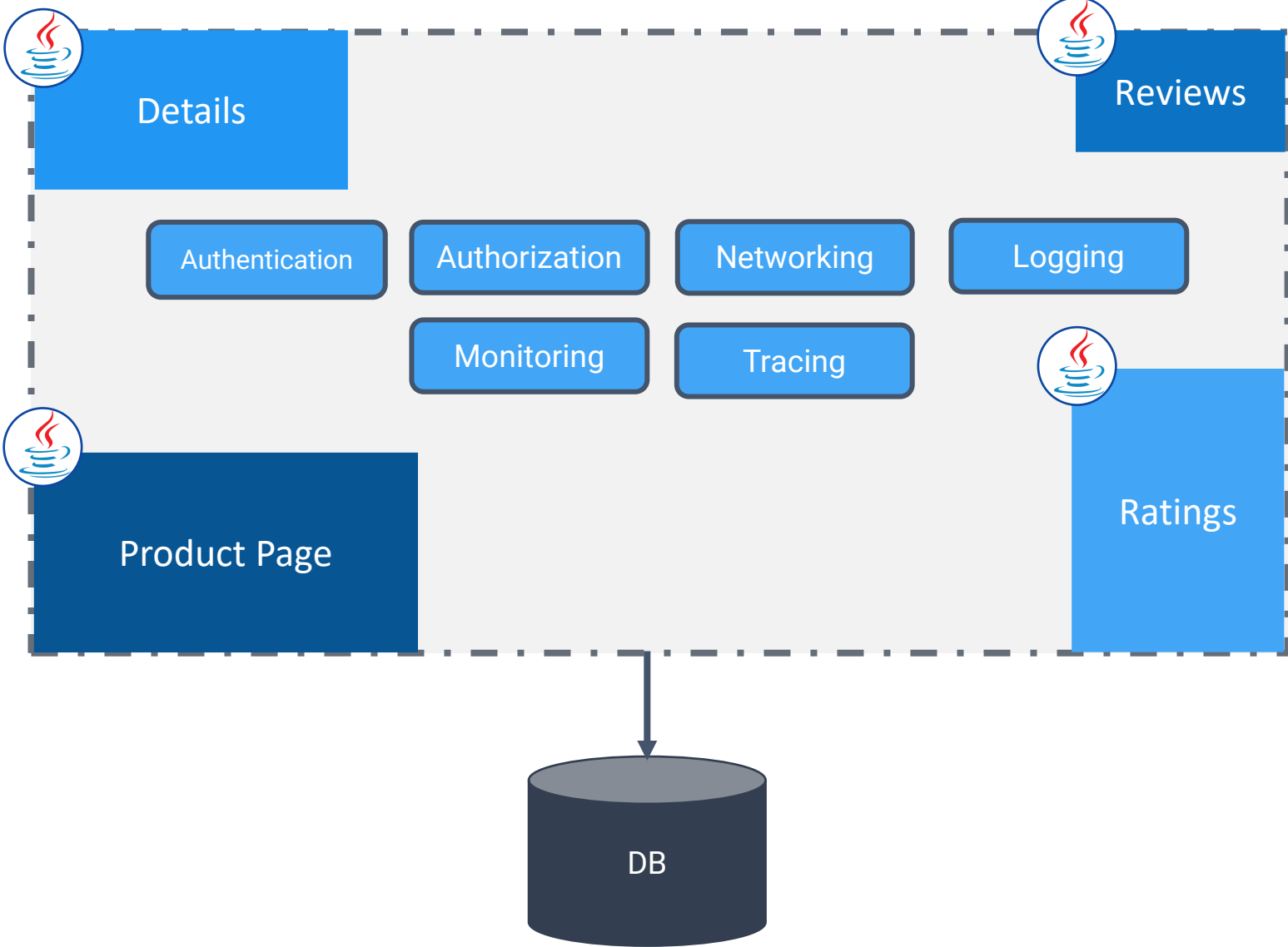


 **System resiliency and isolation**

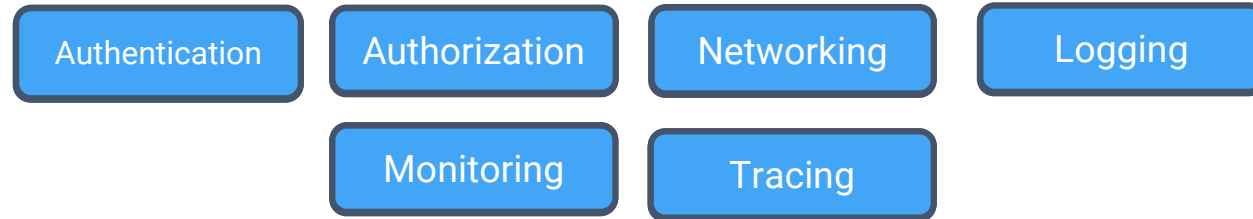


 **Independent and easy
to understand services**


A Monolithic Book Info App



A Microservices Book Info App



Product Page



Details

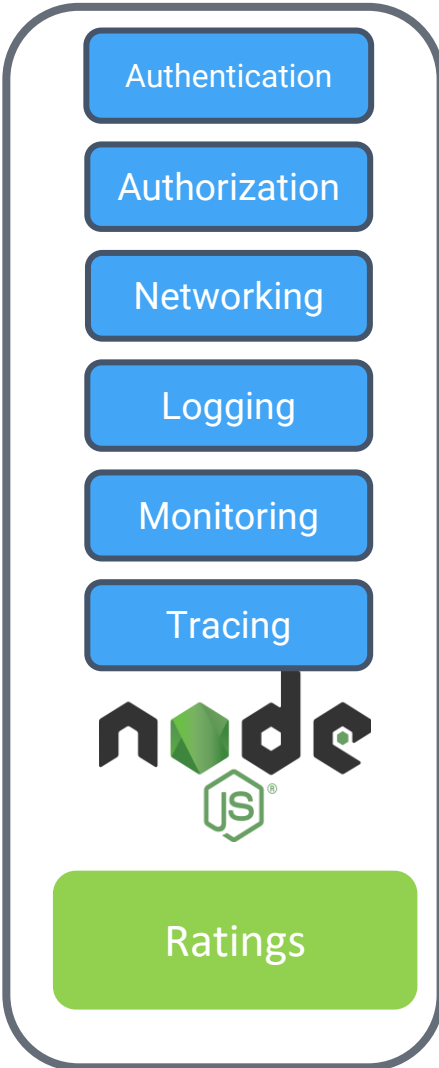
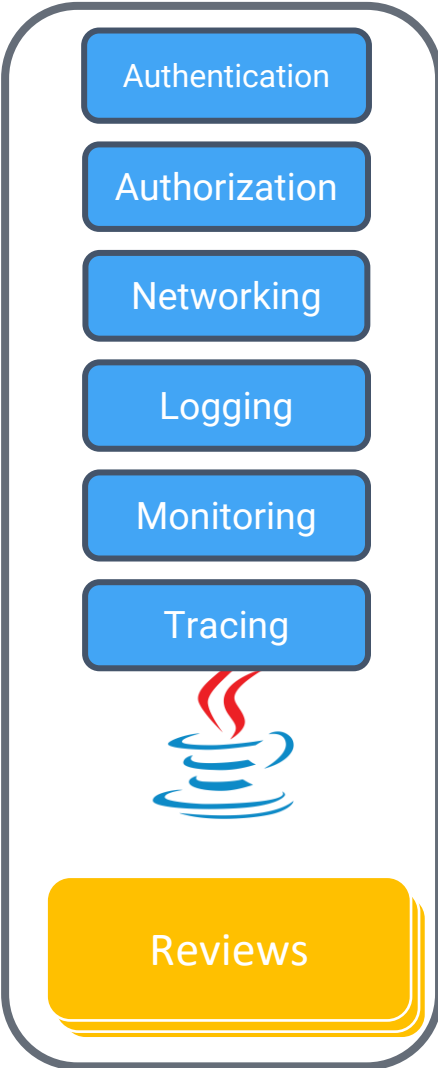
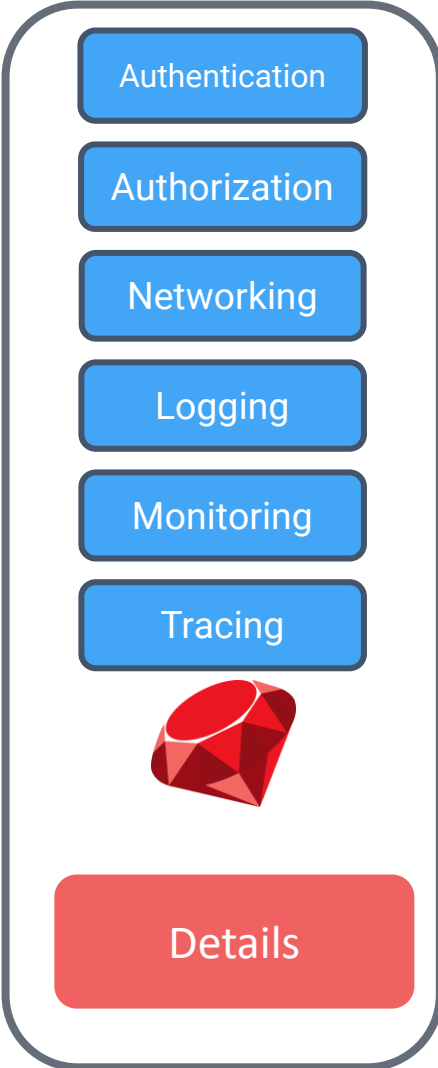
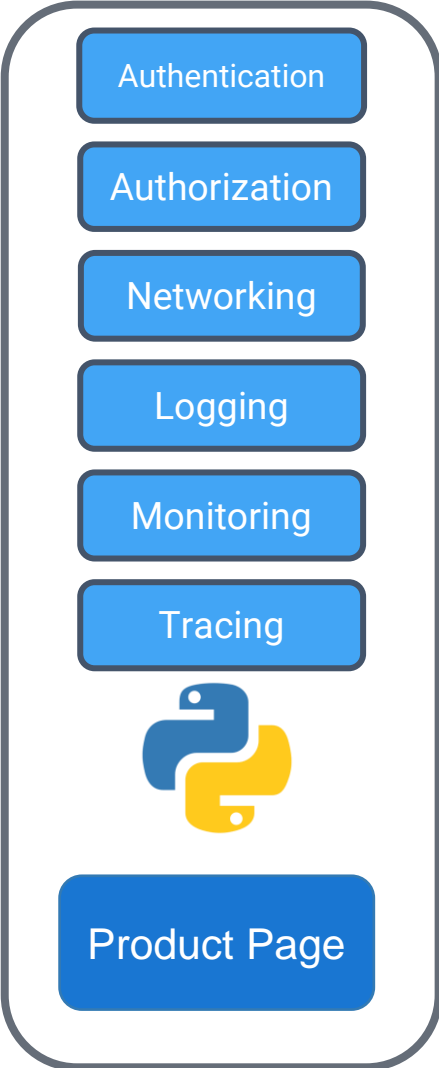


Reviews



Ratings

A Problem: Fat Microservices



Cons of **Microservices**



Complex Service Networking



Security



Observability



**Overload for
Traditional Operation Models**



{KODE}{KLOUD

SERVICE MESH



Authentication


Authorization

Networking

Logging

Monitoring

Tracing



Product Page

Authentication


Authorization

Networking

Logging

Monitoring

Tracing



Details

Authentication


Authorization

Networking

Logging

Monitoring

Tracing



Reviews

Authentication


Authorization

Networking

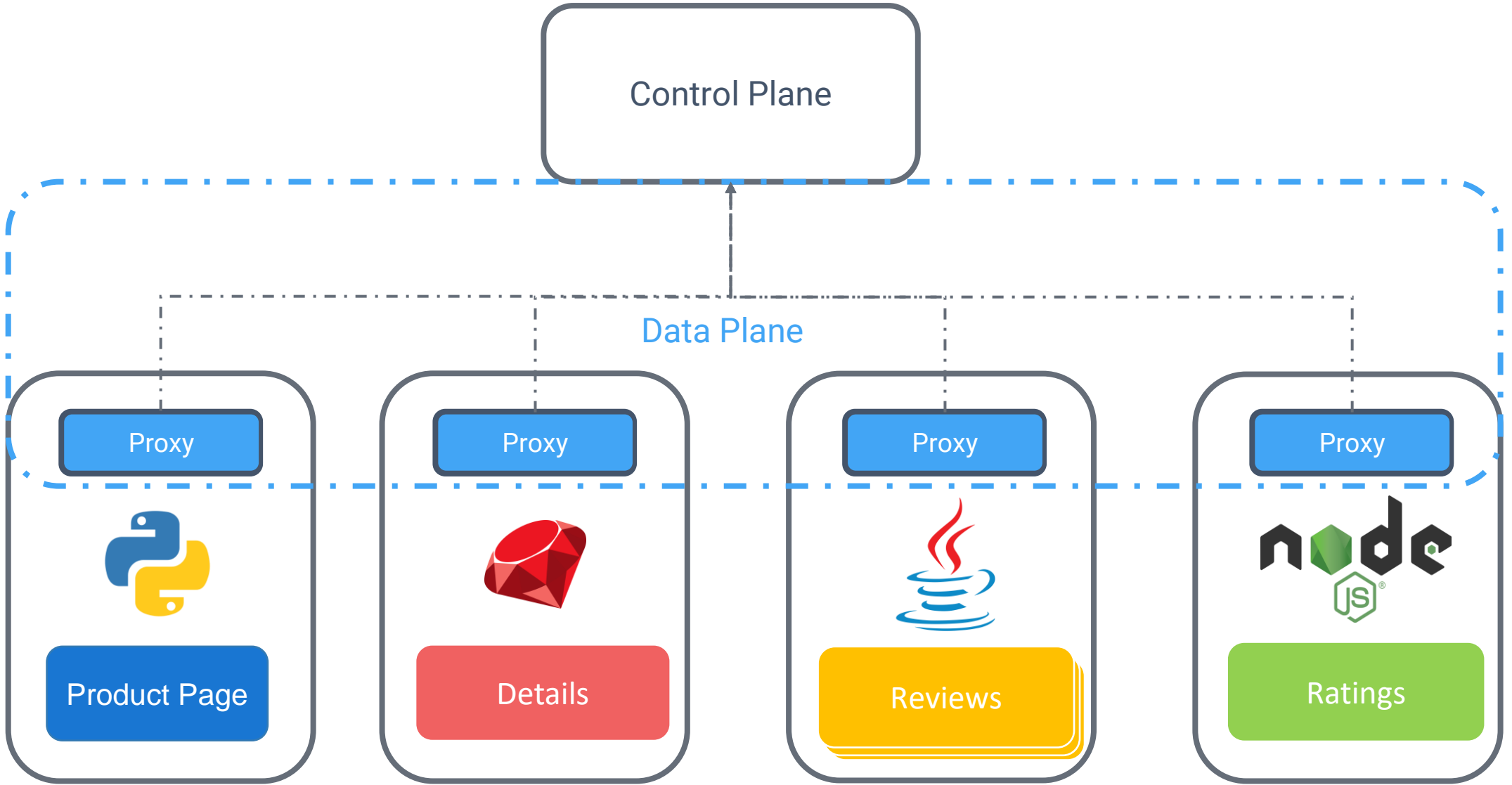
Logging

Monitoring

Tracing



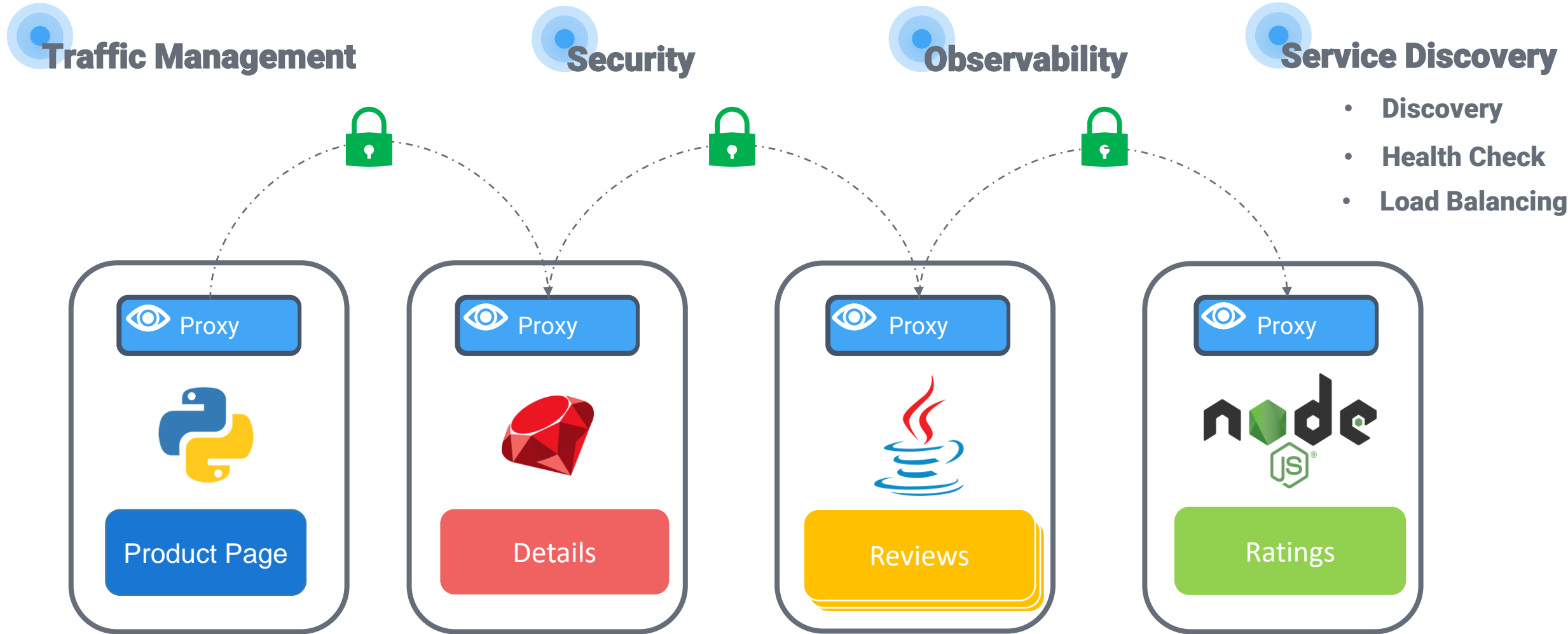
Ratings



What is Service Mesh?

It is a dedicated and configurable infrastructure layer that handles the communication between services without having to change the code in a microservice architecture.

What is Service Mesh Responsible For?



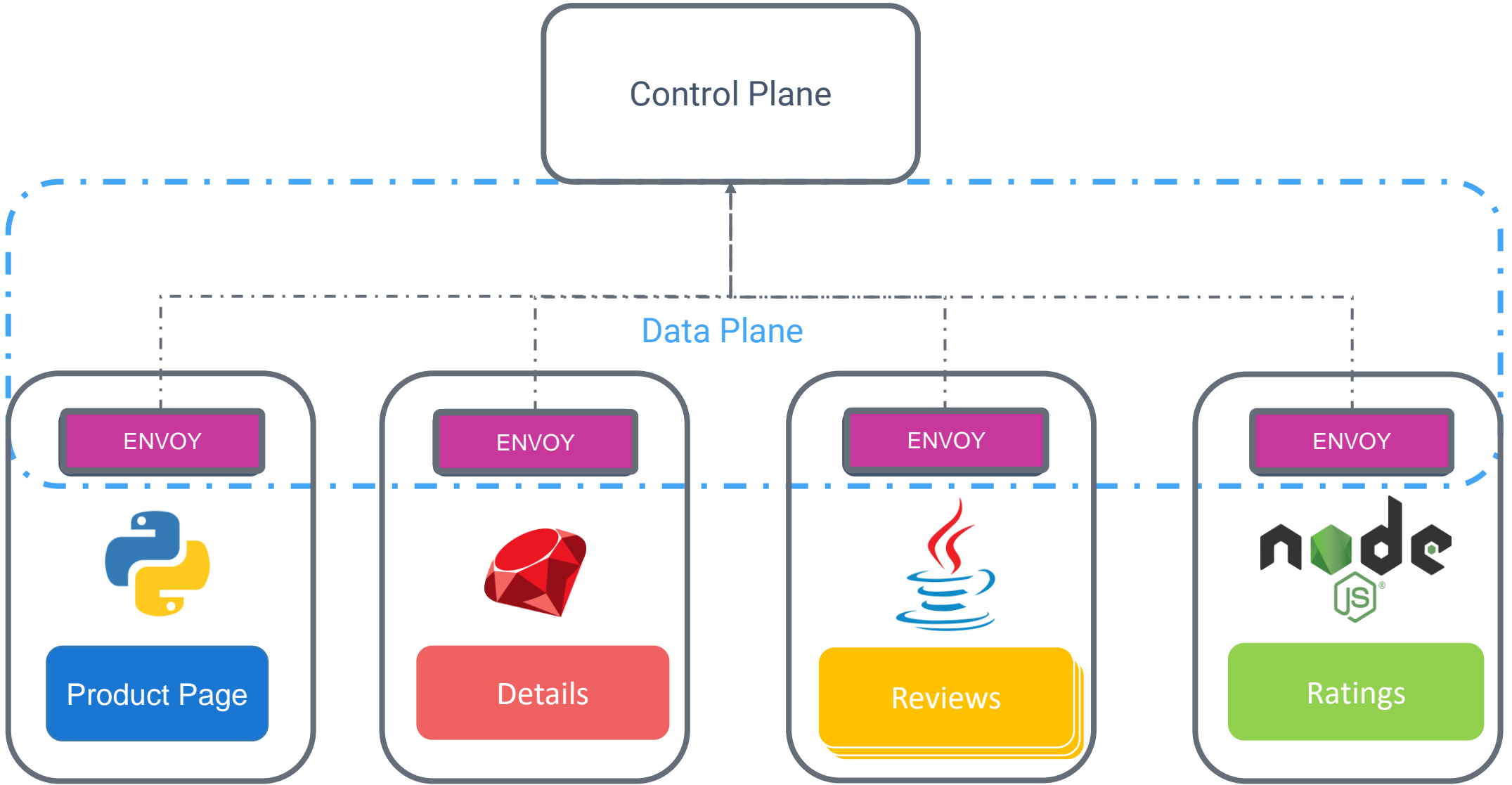


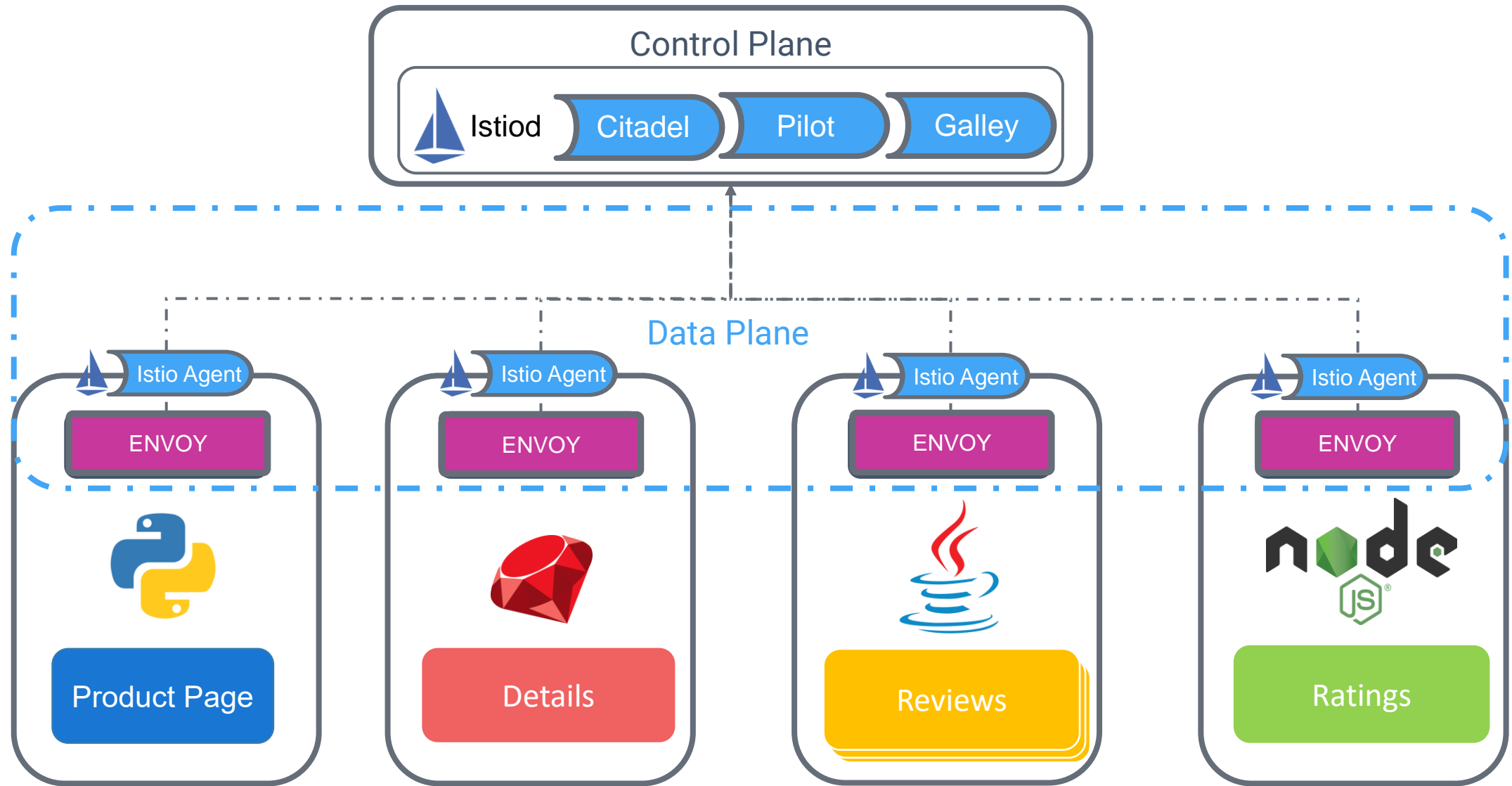
{KODE}{KLOUD

ISTIO











{KODE}{KLOUD

INSTALLING ISTIOCTL



Installing istioctl

```
>_
$ curl -L https://istio.io/downloadIstio | sh -
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
 100   102    100   102     0     0    123     0  --:--:-- --:--:-- --:--:--   123
 100  4573    100  4573     0     0   3606     0  0:00:01 0:00:01 --:--:--  3606

Downloading istio-1.9.4 from
https://github.com/istio/istio/releases/download/1.9.4/istio-1.9.4-osx.tar.gz ...
Istio 1.9.4 Download Complete!

Istio has been successfully downloaded into the istio-1.9.4 folder on your system.

Next Steps:
See https://istio.io/latest/docs/setup/install/ to add Istio to your Kubernetes
cluster.

To configure the istioctl client tool for your workstation,
add the /Users/sevikarakose/Downloads/istio-1.9.4/bin directory to your environment
path variable with:
    export PATH="$PATH:/Users/sevikarakose/Downloads/istio-1.9.4/bin"

Begin the Istio pre-installation check by running:
    istioctl x precheck

Need more information? Visit https://istio.io/latest/docs/setup/install/
```

Installing istioctl


```
>_  
$ cd istio-1.10.0  
$ ls  
LICENSE          README.md        bin              manifest.yaml    manifests  
samples          tools  
$ export PATH=$PWD/bin:$PATH  
$ istioctl verify-install  
0 Istio control planes detected, checking --revision "default" only  
0 Istio injectors detected  
Error: could not load IstioOperator from cluster: the server could not find the  
requested resource. Use --filename
```



{KODE}{KLOUD

INSTALLING ISTIO ON YOUR CLUSTER





Install with
Istioctl

Istio Operator
Install

Install with
Helm



```
> _
```

```
$ istioctl install --set profile=demo -y
```

```
Detected that your cluster does not support third party JWT authentication. Falling  
back to less secure first party JWT. See https://istio.io/v1.9/docs/ops/best-practices/security/#configure-third-party-service-account-tokens for details.
```

```
Istio core installed
```

- ✓ Istiod installed
- ✓ Ingress gateways installed
- ✓ Egress gateways installed
- ✓ Installation complete

istio-ingressgateway

Istiod

istio-egressgateway



istio-system

```
> _  
$ istioctl verify-install
```

```
1 Istio control planes detected, checking --revision "default" only  
✓ Deployment: istio-ingressgateway.istio-system checked successfully  
✓ PodDisruptionBudget: istio-ingressgateway.istio-system checked successfully  
✓ Role: istio-ingressgateway-sds.istio-system checked successfully  
✓ RoleBinding: istio-ingressgateway-sds.istio-system checked successfully  
✓ Service: istio-ingressgateway.istio-system checked successfully  
✓ ServiceAccount: istio-ingressgateway-service-account.istio-system checked successfully  
✓ Deployment: istio-egressgateway.istio-system checked successfully  
✓ PodDisruptionBudget: istio-egressgateway.istio-system checked successfully  
✓ Role: istio-egressgateway-sds.istio-system checked successfully  
✓ RoleBinding: istio-egressgateway-sds.istio-system checked successfully  
✓ Service: istio-egressgateway.istio-system checked successfully  
✓ ServiceAccount: istio-egressgateway-service-account.istio-system checked successfully  
✓ ClusterRole: istiod-istio-system.istio-system checked successfully  
  
✓ EnvoyFilter: tcp-stats-filter-1.9.istio-system checked successfully  
Checked 12 custom resource definitions  
Checked 3 Istio Deployments  
✓ Istio is installed and verified successfully
```



{KODE}{KLOUD

DEPLOYING OUR FIRST APPLICATION WITH ISTIO



```
> _  
$ kubectl apply -f samples/bookinfo/platform/kube/bookinfo.yaml  
deployment.apps/details-v1 created  
deployment.apps/ratings-v1 created  
deployment.apps/reviews-v1 created  
deployment.apps/reviews-v2 created  
deployment.apps/reviews-v3 created  
deployment.apps/productpage-v1 created  
...
```

Product Page

Details

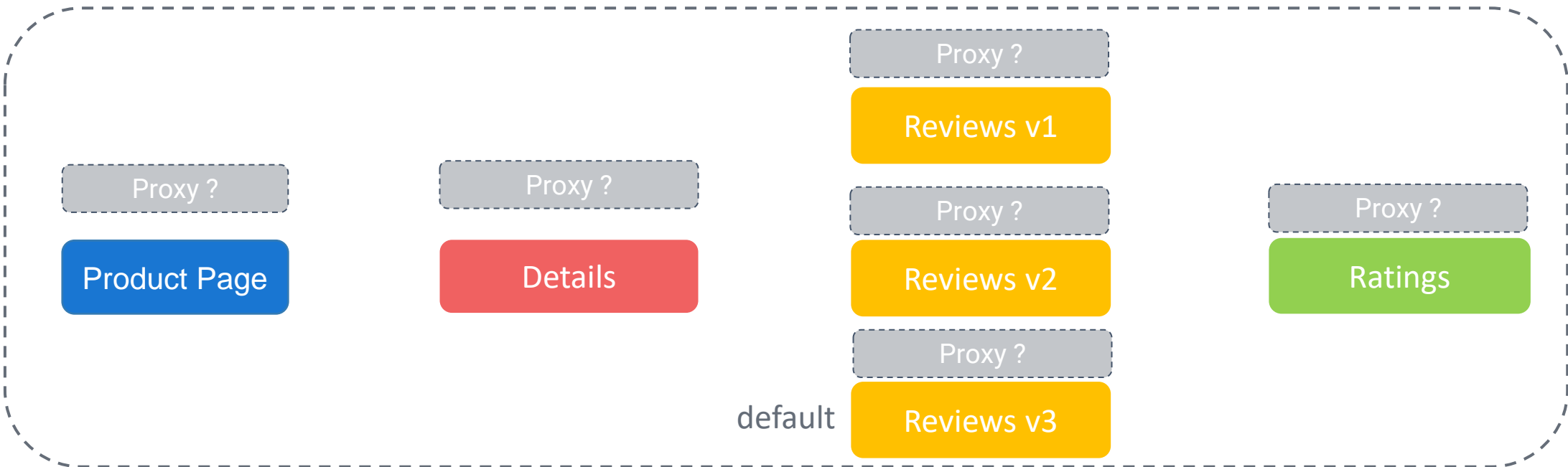
Reviews v1

Reviews v2

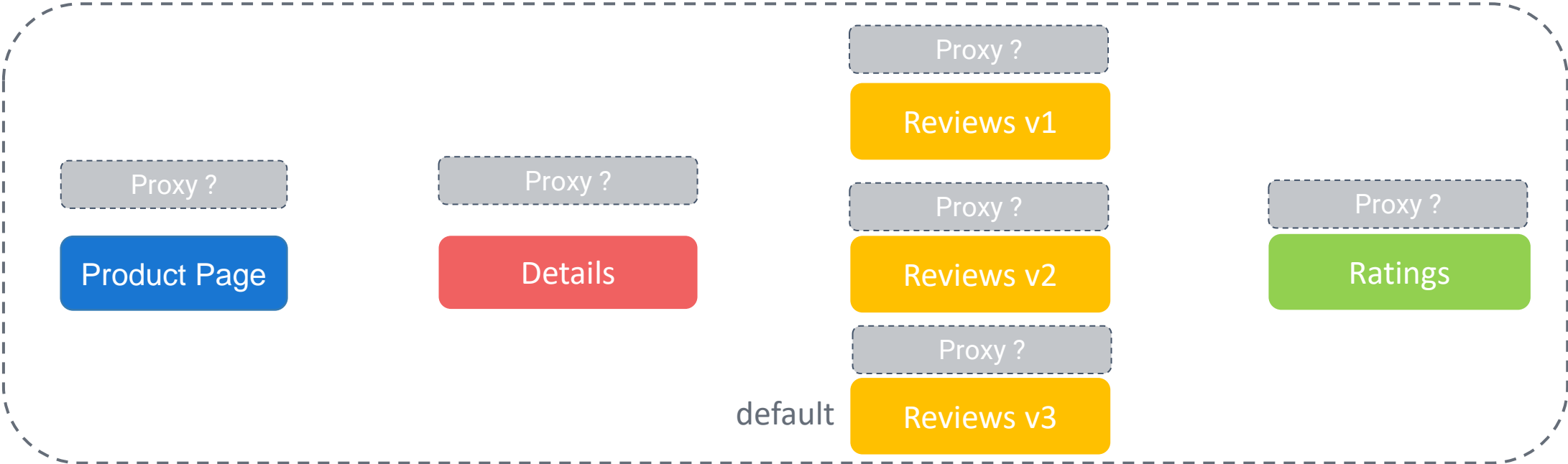
Reviews v3

Ratings

```
> _
$ kubectl get pods -A
NAMESPACE      NAME                                     READY   STATUS    RESTARTS   AGE
default        details-v1-66b6955995-zgrd8            1/1     Running   0           6m57s
default        productpage-v1-5d9b4c9849-dckrt        1/1     Running   0           6m57s
default        ratings-v1-fd78f799f-s94cc             1/1     Running   0           6m58s
default        reviews-v1-6549ddccc5-bxv4n           1/1     Running   0           6m58s
default        reviews-v2-76c4865449-2qmhj           1/1     Running   0           6m58s
default        reviews-v3-6b554c875-vbf8v            1/1     Running   0           6m58s
```



```
> _  
$ istioctl analyze  
Info [IST0102] (Namespace default) The namespace is not enabled for Istio injection.  
Run 'kubectl label namespace default istio-injection=enabled' to enable it, or  
'kubectl label namespace default istio-injection=disabled' to explicitly mark it as  
not needing injection.
```



> _

```
$ istioctl analyze
```

```
Info [IST0102] (Namespace default) The namespace is not enabled for Istio injection.  
Run 'kubectl label namespace default istio-injection=enabled' to enable it, or  
'kubectl label namespace default istio-injection=disabled' to explicitly mark it as  
not needing injection.
```

kube-system

Product Page

Details

Reviews v1

Reviews v2

Reviews v3

Ratings

default

hr

payroll

> _

```
$ kubectl delete -f samples/bookinfo/platform/kube/bookinfo.yaml
```

```
service "details" deleted  
serviceaccount "bookinfo-details" deleted  
service "ratings" deleted  
serviceaccount "bookinfo-ratings" deleted  
serviceaccount "bookinfo-reviews" deleted  
service "productpage" deleted  
serviceaccount "bookinfo-productpage" deleted
```



> _

```
$ kubectl label namespace default istio-injection=enabled
```

```
namespace/default labeled
```

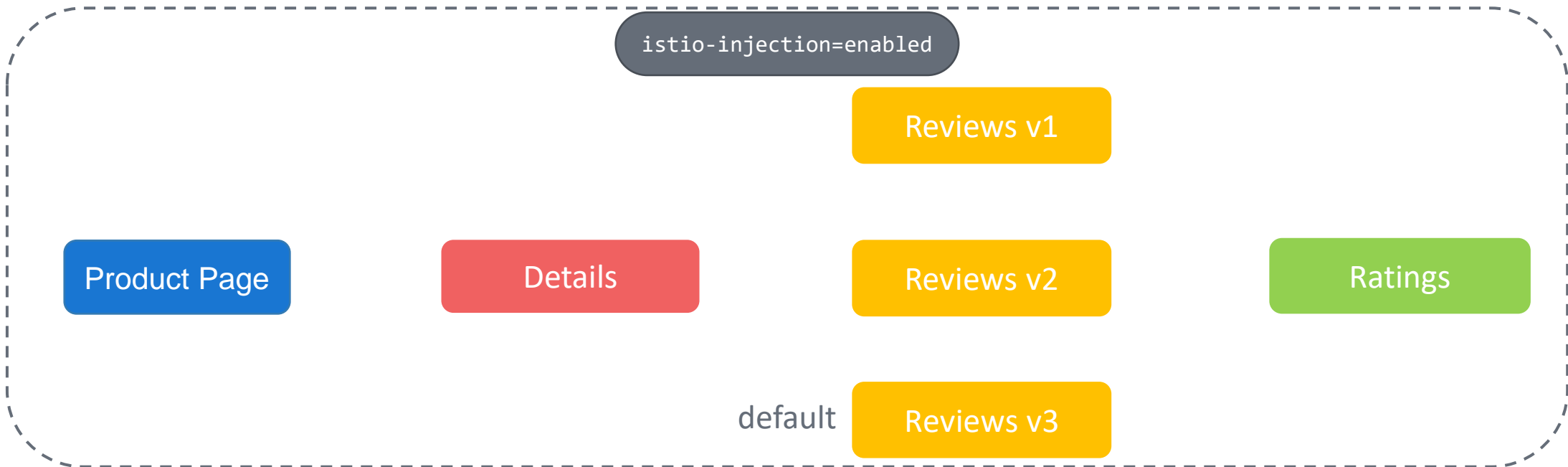


istio-injection=enabled

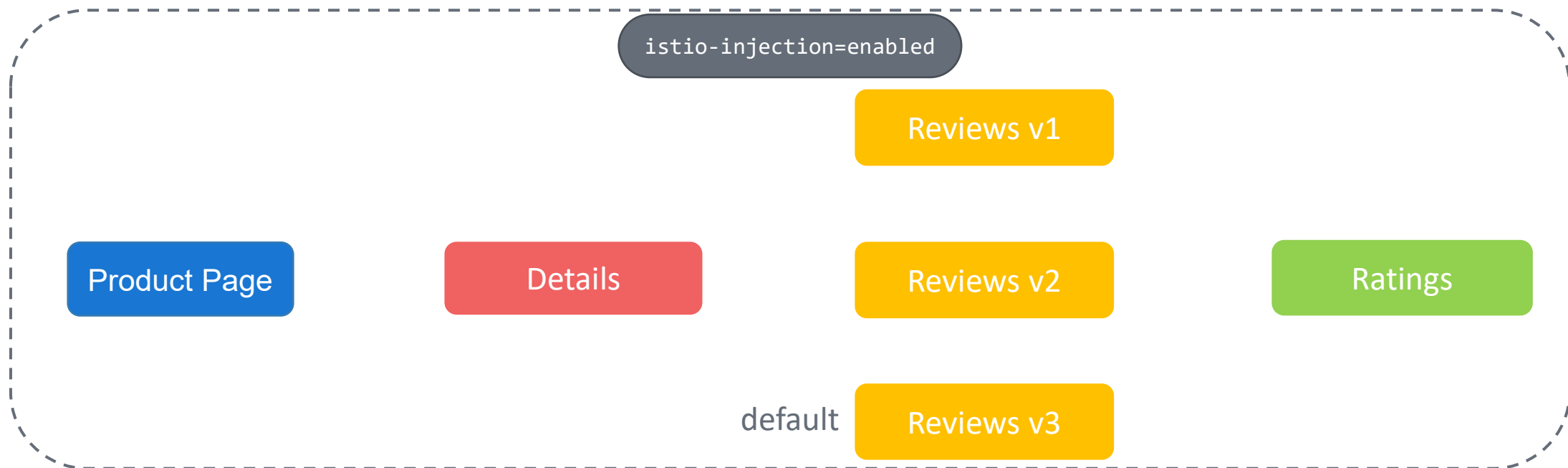
The diagram consists of a dashed-line rounded rectangle. At the top, a dark grey rounded rectangle contains the text 'istio-injection=enabled'. At the bottom center of the dashed rectangle is the text 'default'.

default

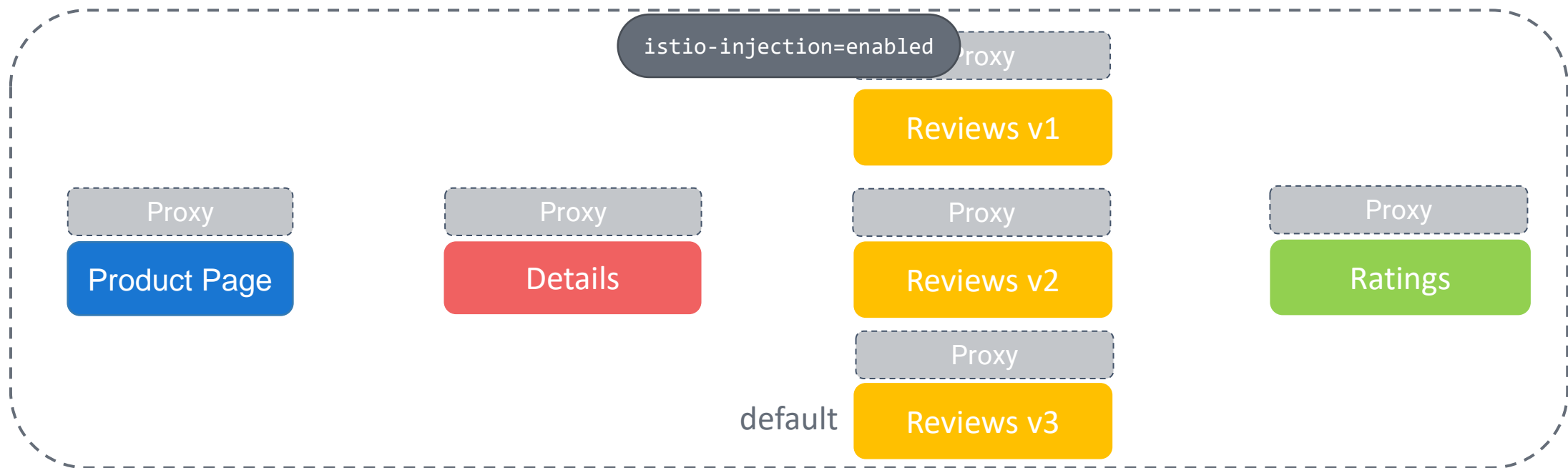
```
> _  
$ kubectl apply -f samples/bookinfo/platform/kube/bookinfo.yaml  
deployment.apps/details-v1 created  
deployment.apps/ratings-v1 created  
deployment.apps/reviews-v1 created  
deployment.apps/reviews-v2 created  
deployment.apps/reviews-v3 created  
service/productpage created  
deployment.apps/productpage-v1 created  
...
```



```
> _  
$ istioctl analyze  
✓ No validation issues found when analyzing namespace: default.
```



```
> _
$ kubectl get pods
NAME                                READY   STATUS    RESTARTS   AGE
details-v1-5f449bdbb9-vrgzh         2/2     Running   0           26s
productpage-v1-6f9df695b7-cx259     2/2     Running   0           26s
ratings-v1-857bb87c57-hmpfd        2/2     Running   0           26s
reviews-v1-68f9c47f69-cbj7c        2/2     Running   0           26s
reviews-v2-5d56c488f5-wb4v7        2/2     Running   0           26s
reviews-v3-869ff44845-h5fpf        2/2     Running   0           26s
```





{KODE}{KLOUD

VISUALIZING SERVICE MESH WITH KIALI





Define

Validate

Observe

The screenshot displays the Kiali web interface. On the left is a navigation sidebar with options: Overview, Graph (selected), Applications, Workloads, Services, and Istio Config. The main area shows a service graph for the namespace 'default' and 'Versioned app graph'. The graph includes nodes for 'istio-ingressgateway latest (istio-system)', 'productpage v1', 'reviews v1, v2, v3', 'ratings v1', and 'details v1'. A 'Current Graph' summary on the right shows 5 apps (7 versions), 4 services, and 11 edges. Below this is an HTTP performance table and a bar chart.

HTTP (requests per second):		
Total	%Success	%Error
0.01	100.00	0.00

Legend: OK (green), 3xx (blue), 4xx (red), 5xx (black), NR (grey)



{KODE}{KLOUD

INSTALLING KIALI



> _

```
$ kubectl apply -f samples/addons
```

```
$ kubectl rollout status deployment/kiali -n istio-system
```

```
monitoringdashboard.monitoring.kiali.io/springboot-jvm created
```

```
monitoringdashboard.monitoring.kiali.io/springboot-tomcat created
```

```
monitoringdashboard.monitoring.kiali.io/thorntail created
```

```
monitoringdashboard.monitoring.kiali.io/tomcat created
```

```
monitoringdashboard.monitoring.kiali.io/vertx-client created
```

```
monitoringdashboard.monitoring.kiali.io/vertx-eventbus created
```

```
monitoringdashboard.monitoring.kiali.io/vertx-jvm created
```

```
monitoringdashboard.monitoring.kiali.io/vertx-pool created
```

```
monitoringdashboard.monitoring.kiali.io/vertx-server created
```

```
serviceaccount/prometheus created
```

```
configmap/prometheus created
```

```
clusterrole.authorization.k8s.io/prometheus created
```

```
clusterrolebinding.authorization.k8s.io/prometheus created
```

```
service/prometheus created
```

```
deployment.apps/prometheus created
```

```
Waiting for deployment "kiali" rollout to finish: 0 of 1 updated replicas are available...
```

```
deployment "kiali" successfully rolled out
```

> _

```
$ kubectl -n istio-system get svc kiali
```

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
kiali	ClusterIP	10.96.6.123	<none>	20001/TCP,9090/TCP	3m42s

> _

```
$ istioctl dashboard kiali
```


```
http://localhost:20001/kiali
```




Overview

- Graph
- Applications
- Workloads
- Services
- Istio Config

Namespace ▾ Filter by Namespace Name ▾ ↓↕

Last 1m ▾ Every 10s ▾ 

Health for Apps ▾ 

Namespace	Health	Labels	Resources
default		1 Label	Istio Config N/A
istio-system		1 Label	Istio Config N/A
local-path-storage		No labels	Istio Config N/A



{KODE}{KLOUD

CREATE TRAFFIC INTO YOUR MESH



```
> _
```

```
$ istioctl analyze
```

```
✓ No validation issues found when analyzing namespace: default.
```

> _

```
$ minikube ip
```

```
192.168.64.6
```

> _

```
$ export INGRESS_HOST=$(minikube ip)
```

> _

```
$ export INGRESS_PORT=$(kubectl -n istio-system get service istio-  
ingressgateway -o jsonpath='{.spec.ports[?(@.name=="http2")].nodePort}')  
$ export SECURE_INGRESS_PORT=$(kubectl -n istio-system get service istio-  
ingressgateway -o jsonpath='{.spec.ports[?(@.name=="https")].nodePort}')  
$ export TCP_INGRESS_PORT=$(kubectl -n istio-system get service istio-  
ingressgateway -o jsonpath='{.spec.ports[?(@.name=="tcp")].nodePort}')
```

> _

```
$ curl "http://$INGRESS_HOST:$INGRESS_PORT/productpage"
```

```
<!DOCTYPE html>  
<html>  
  <head>  
    <title>Simple Bookstore App</title>  
    <meta charset="utf-8">  
    <meta http-equiv="X-UA-Compatible" content="IE=edge">  
    <meta name="viewport" content="width=device-width, initial-scale=1.0">  
  
    <!-- Latest compiled and minified CSS -->  
    <link rel="stylesheet" href="static/bootstrap/css/bootstrap.min.css">  
  
    <!-- Optional theme -->  
    <link rel="stylesheet" href="static/bootstrap/css/bootstrap-theme.min.css">  
  
  </head>  
  <body>
```

>_

```
$ while sleep 0.01;do curl -sS  
'http://'"$INGRESS_HOST"' : '"$INGRESS_PORT"' /productpage'\ &>  
/dev/null ; done
```

Namespace: default

Versioned app graph

Last 5m

Every 15s

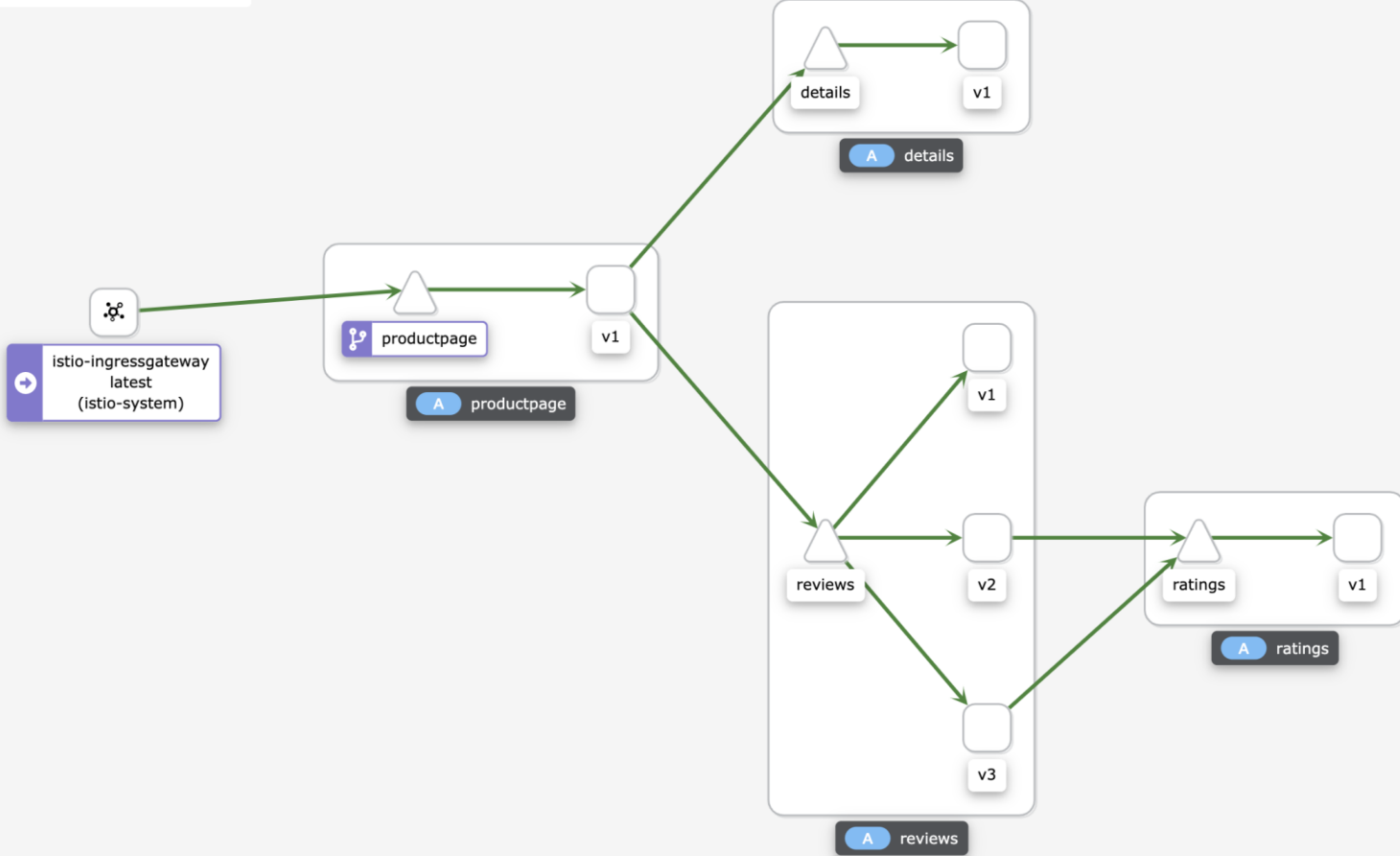
Display

Find...

Hide...

Graph tour

Jun 12, 05:51:55 PM ... 05:56:55 PM



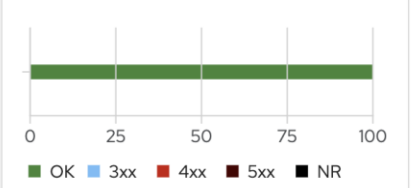
Current Graph:

- NS default ✓
- 5 apps (7 versions)
- 4 services
- 11 edges

Inbound	Outbound	Total
---------	----------	-------

HTTP (requests per second):

Total	%Success	%Error
0.11	100.00	0.00



> _

```
$ kubectl delete deployments/productpage-v1  
deployment.apps "productpage-v1" deleted
```

Namespace: default

Workload graph

Last 1m

Every 15s



Display

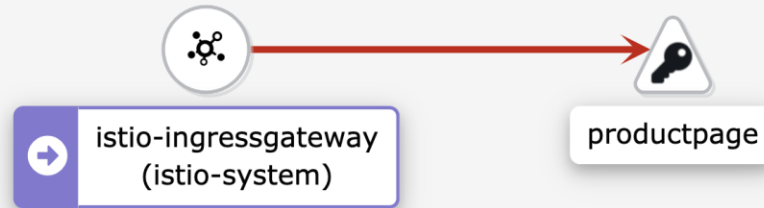
Find...

Hide...



Graph tour

Jun 12, 06:10:27 PM ... 06:11:27 PM



Hide

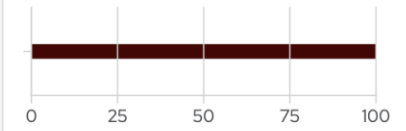
Current Graph:

- NS default
- 1 service
- 1 workload
- 1 edge

Inbound | Outbound | Total

HTTP (requests per second):

Total	%Success	%Error
0.98	0.00	100.00



OK 3xx 4xx 5xx NR

Legend

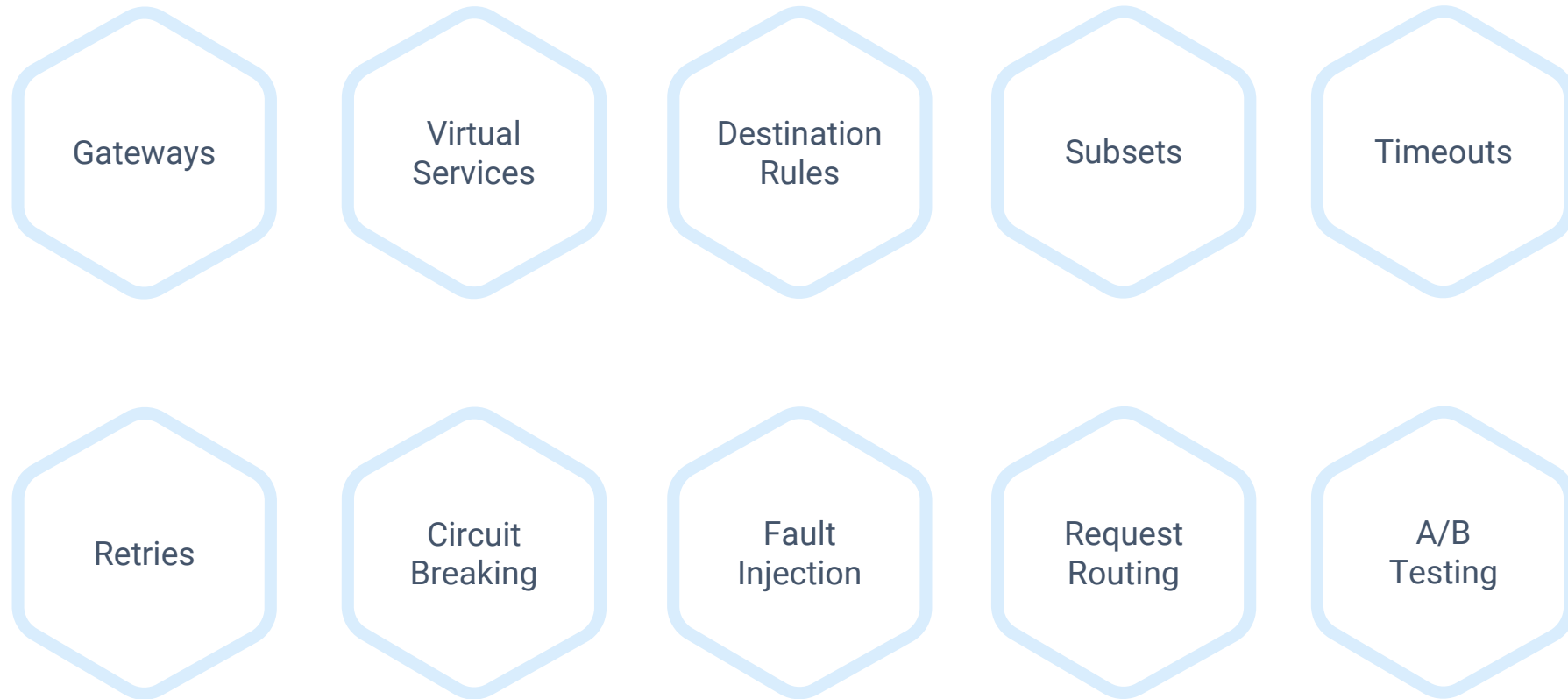


{KODE}{KLOUD

TRAFFIC MANAGEMENT



Traffic Management



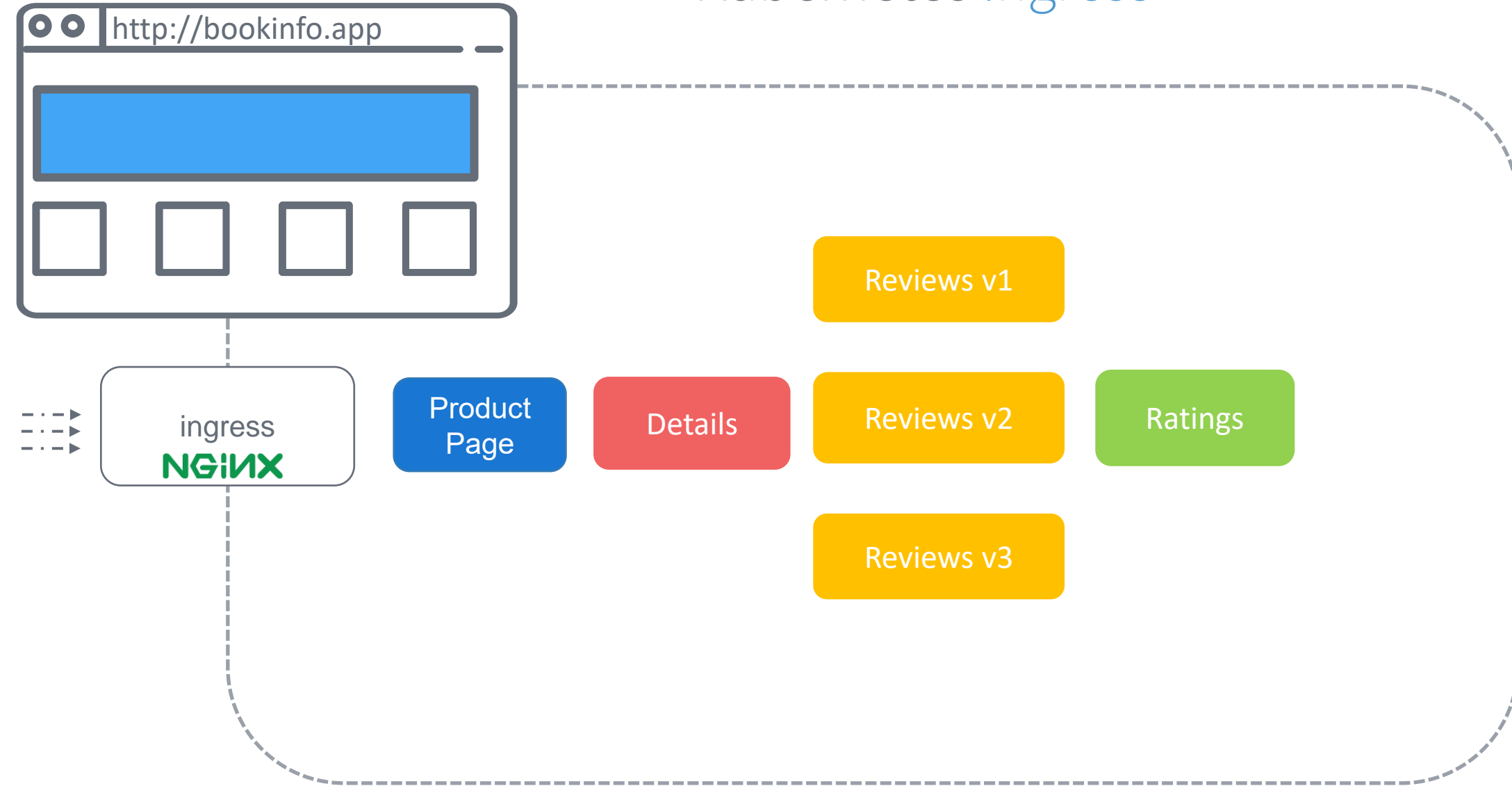


{KODE}{KLOUD

GATEWAYS



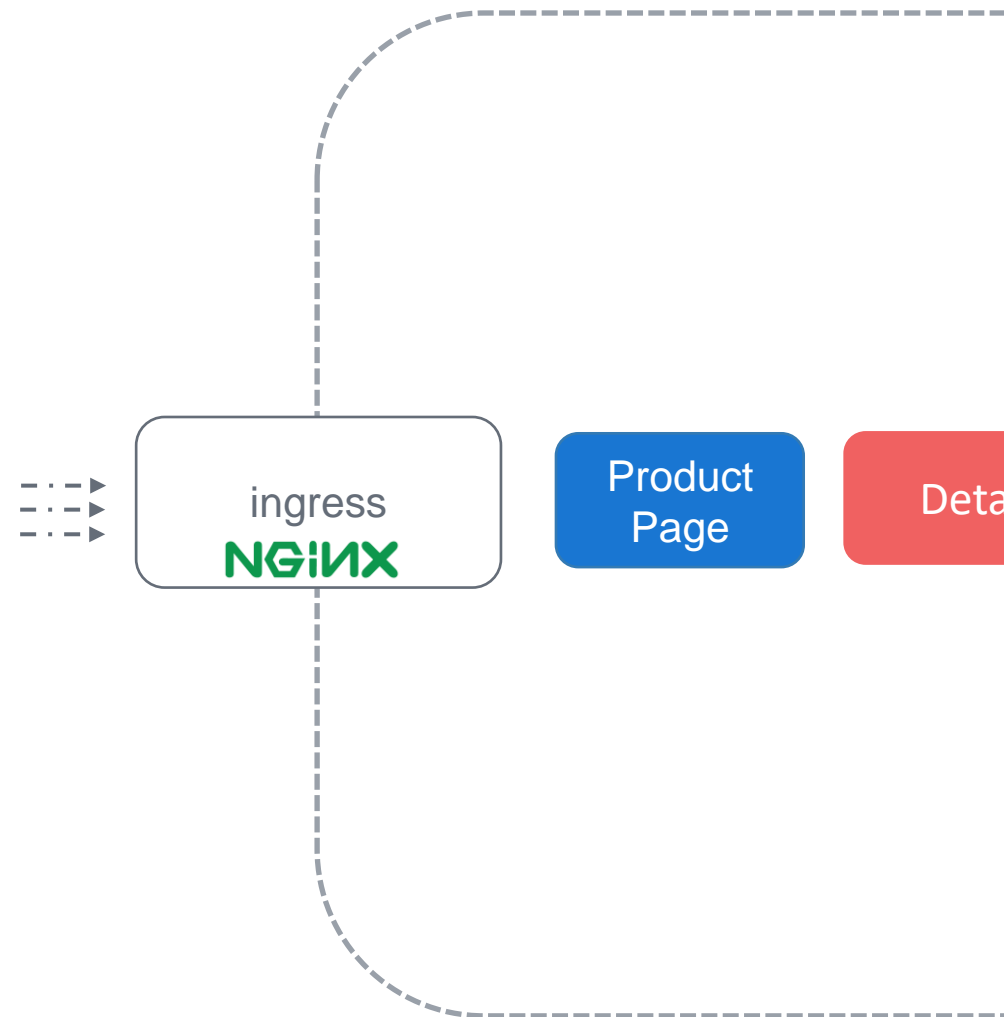
Kubernetes Ingress



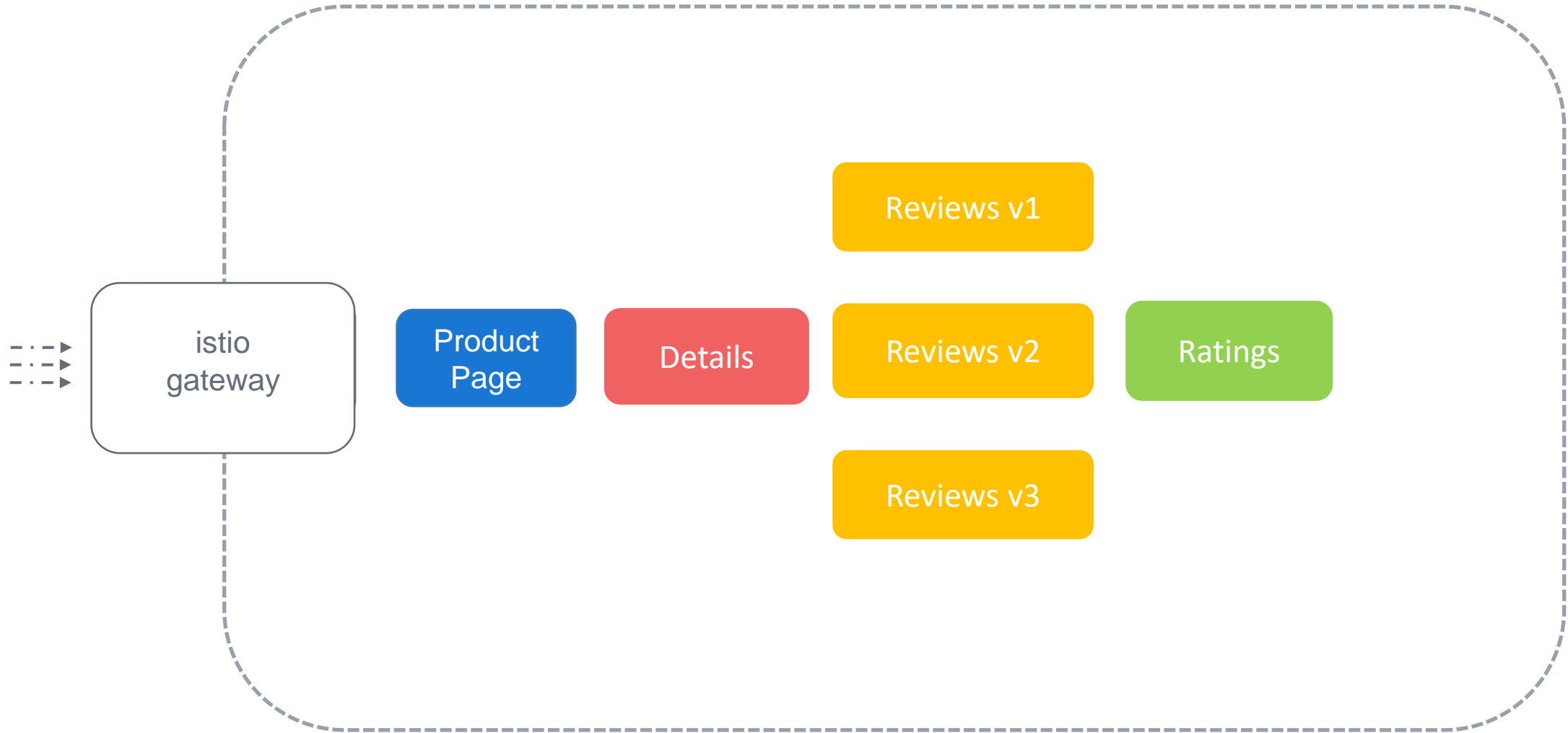
Kubernetes Ingress

bookinfo-ingress.yaml

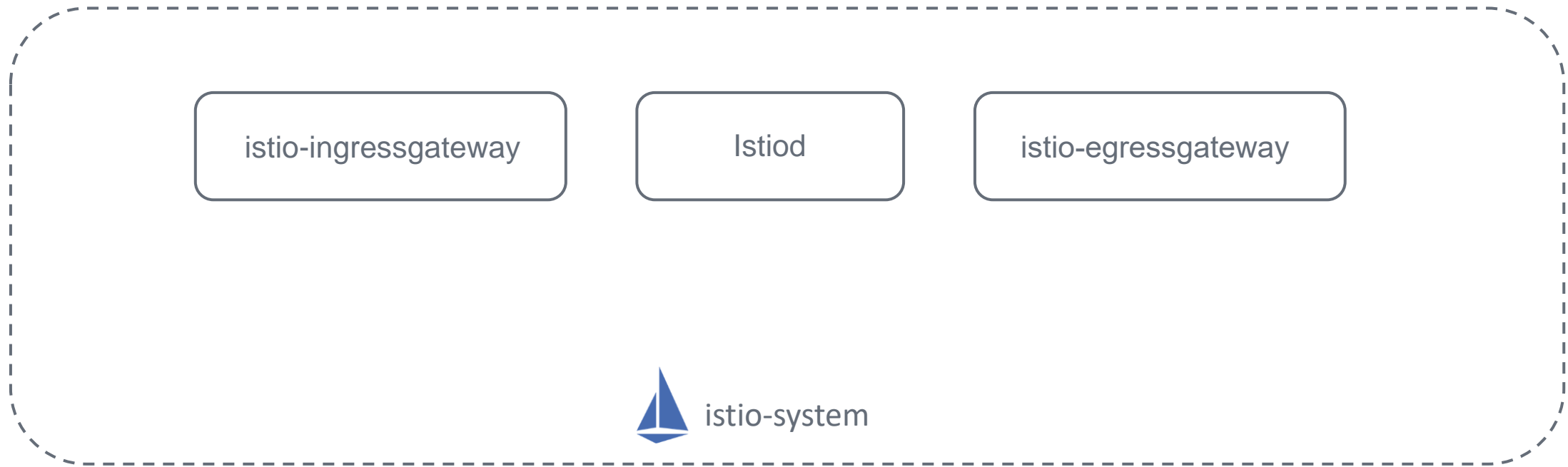
```
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
  name: ingress
spec:
  rules:
  - host: bookinfo.app
    http:
      paths:
      - path: /
        backend:
          serviceName: productpage
          servicePort: 8000
```



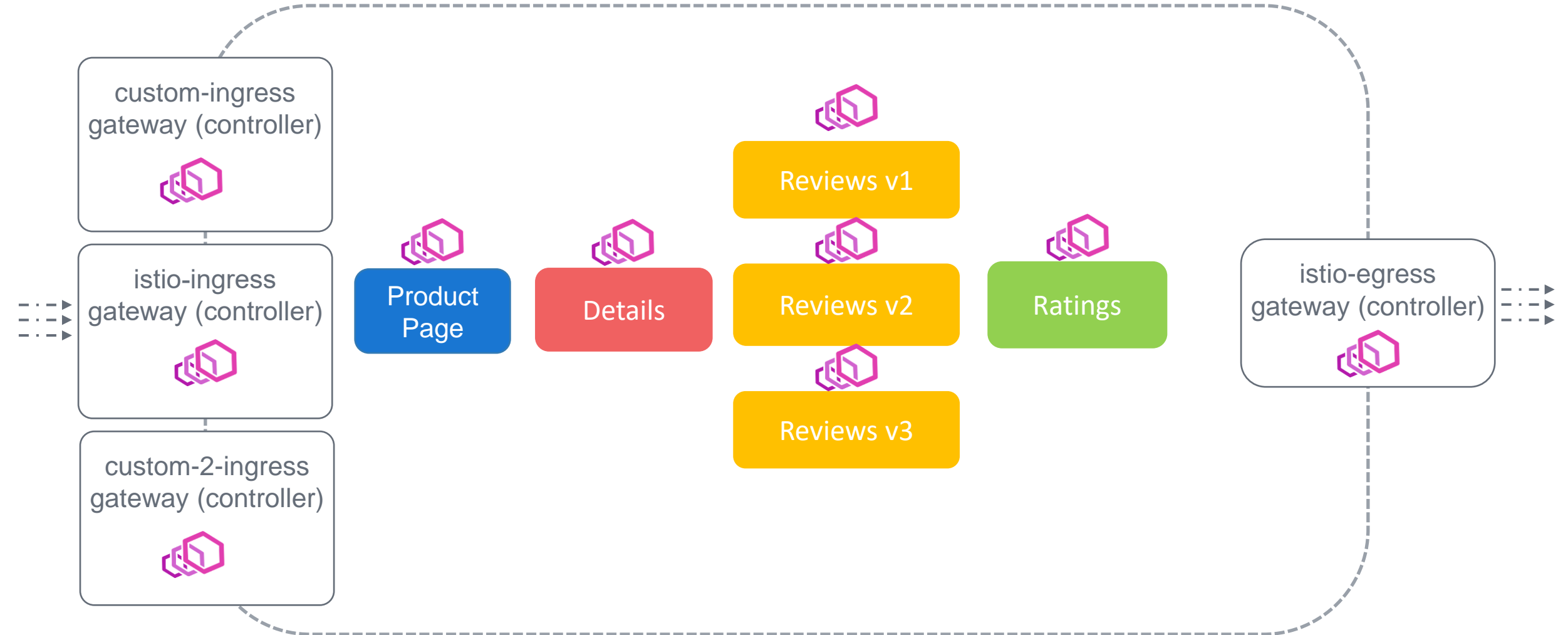
Istio Gateway



Istio Gateway



Istio Gateway



Istio Gateway

bookinfo-gateway.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: Gateway
metadata:
  name: bookinfo-gateway
spec:
  selector:
    istio: ingressgateway
  servers:
  - port:
      number: 80
      name: http
      protocol: HTTP
    hosts:
    - "bookinfo.app"
```

>_

```
$ kubectl apply -f bookinfo-gateway.yaml
```

```
gateway.networking.istio.io/bookinfo-gateway created
```

bookinfo-gateway



custom-ingress
gateway (controller)



istio-ingress
gateway (controller)



custom-2-ingress
gateway (controller)



Product
Page

Istio Gateway

```
bookinfo-gateway.yaml
```

```
apiVersion: networking.istio.io/v1alpha3
kind: Gateway
metadata:
  name: bookinfo-gateway
spec:
  selector:
    istio: ingressgateway
  servers:
  - port:
      number: 80
      name: http
      protocol: HTTP
    hosts:
    - "bookinfo.app"
```

```
>_
```

```
$ kubectl apply -f bookinfo-gateway.yaml
```

```
gateway.networking.istio.io/bookinfo-gateway created
```

```
>_
```

```
$ kubectl get gateway
```

```
NAME          AGE
bookinfo-gateway 9d
```

```
$ kubectl describe gateway bookinfo-gateway
```

```
Name:          bookinfo-gateway
Namespace:     default
Labels:        <none>
Annotations:   API Version: networking.istio.io/v1beta1
Kind:          Gateway
...
Spec:
  Selector:
    Istio: ingressgateway
  Servers:
    Hosts:
      *
    Port:
      Name:  http
      Number: 80
      Protocol: HTTP
  Events:   <none>
```

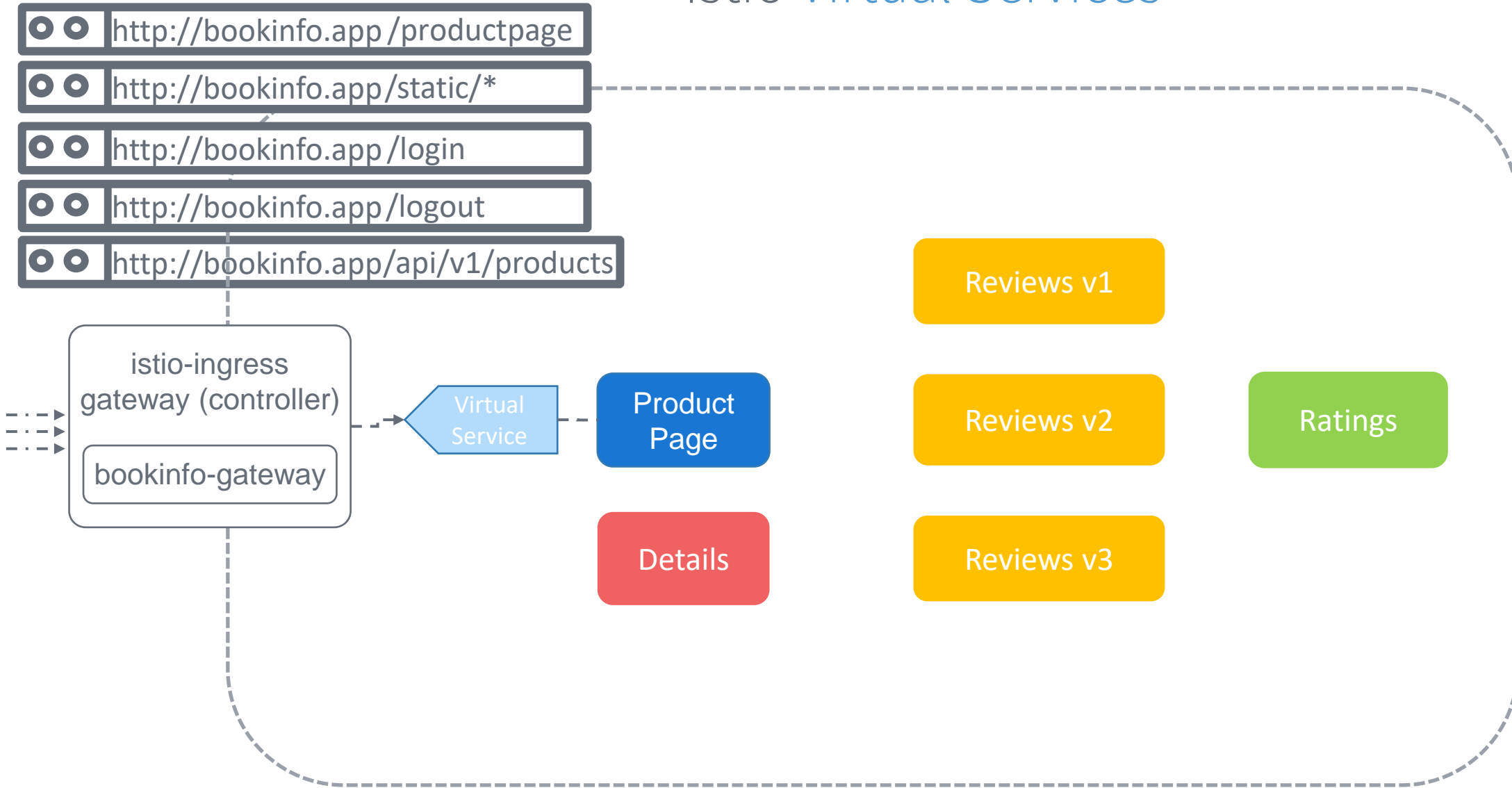


{KODE}{KLOUD

VIRTUAL SERVICES



Istio Virtual Services



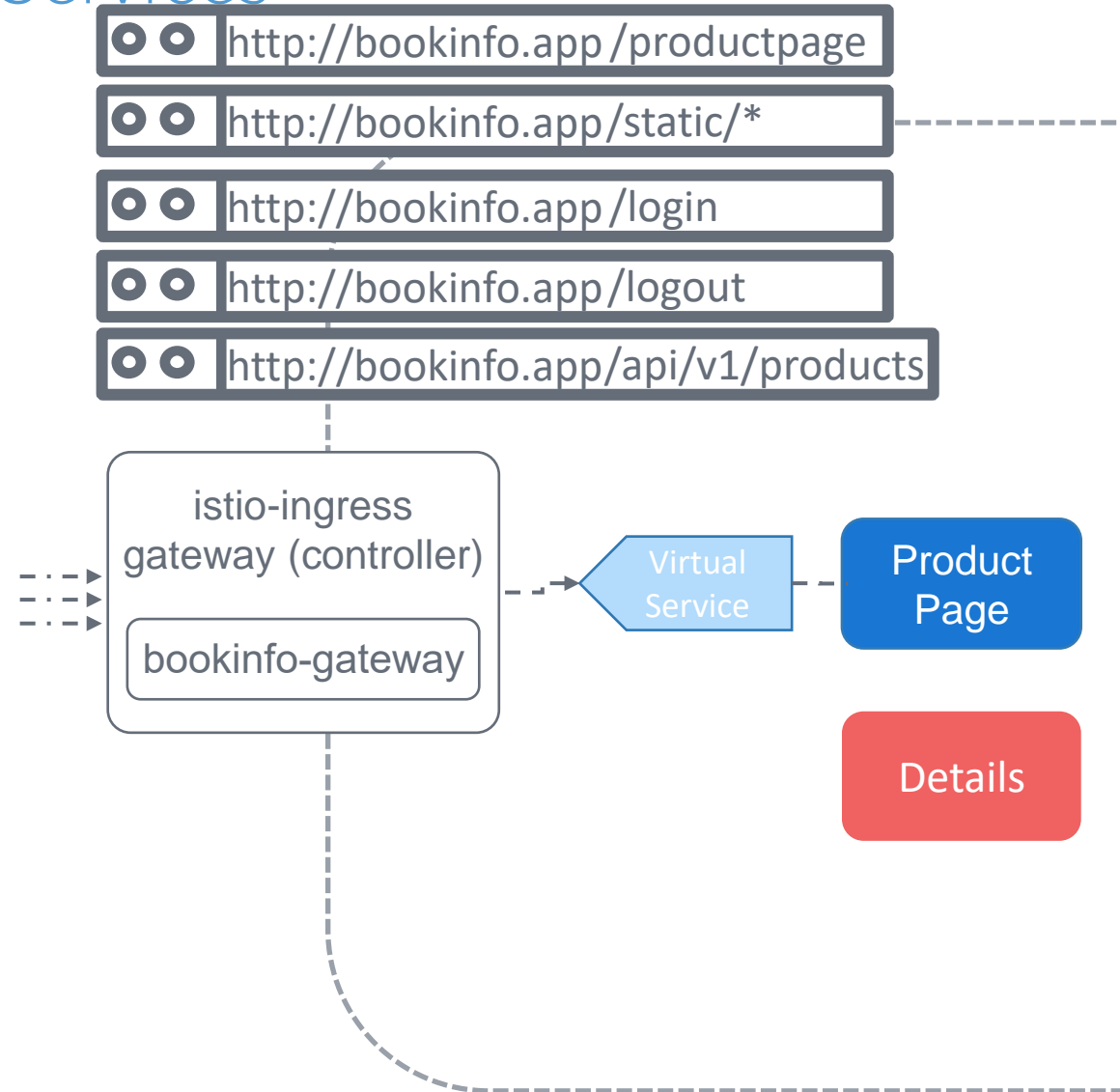
Istio Virtual Services

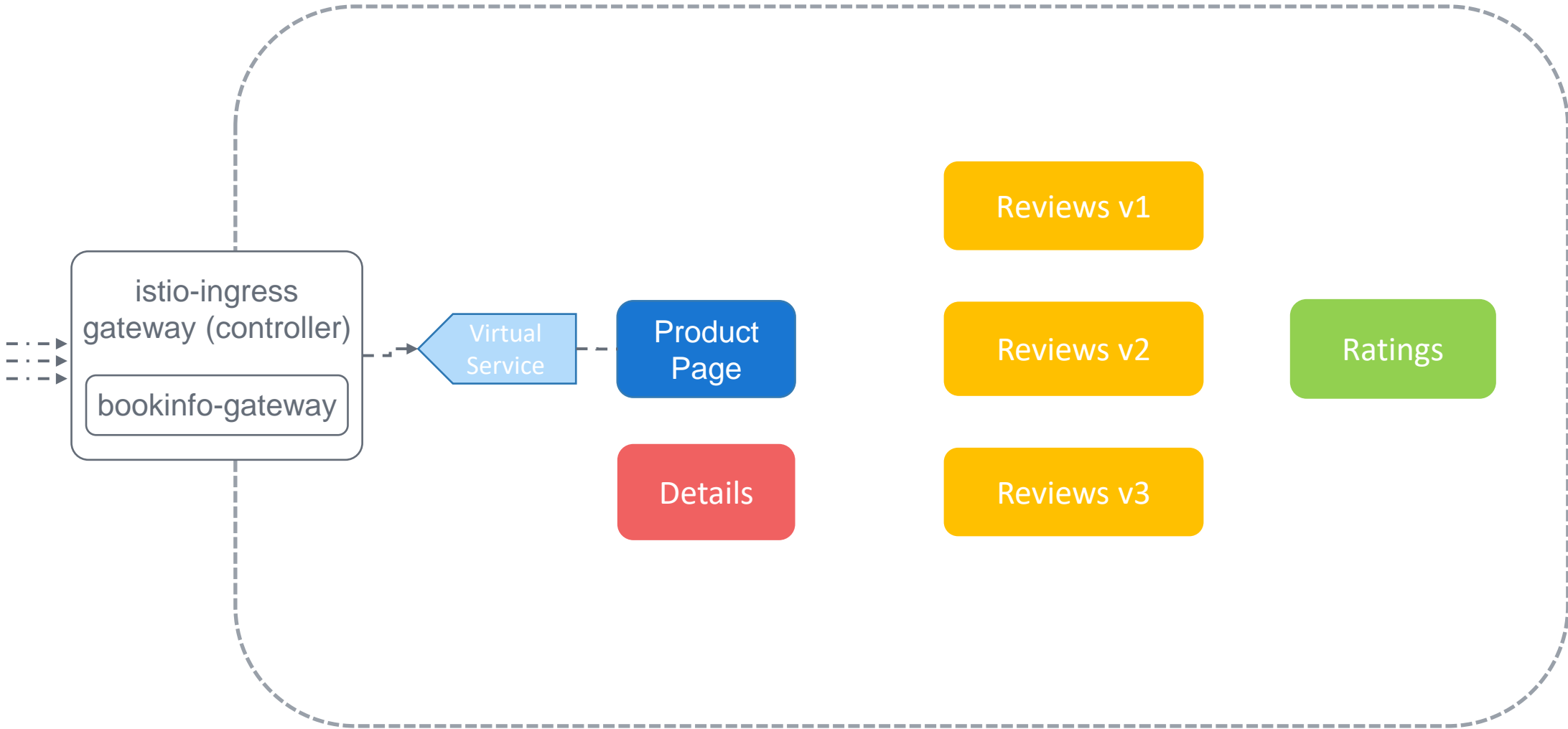
virtual-service1.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: bookinfo
spec:
  hosts:
  - "bookinfo.app"

  gateways:
  - bookinfo-gateway

  http:
  - match:
    - uri:
        exact: /productpage
    - uri:
        prefix: /static
    - uri:
        exact: /login
    - uri:
        exact: /logout
    - uri:
        prefix: /api/v1/products
    route:
    - destination:
        host: productpage
        port:
            number: 9080
```





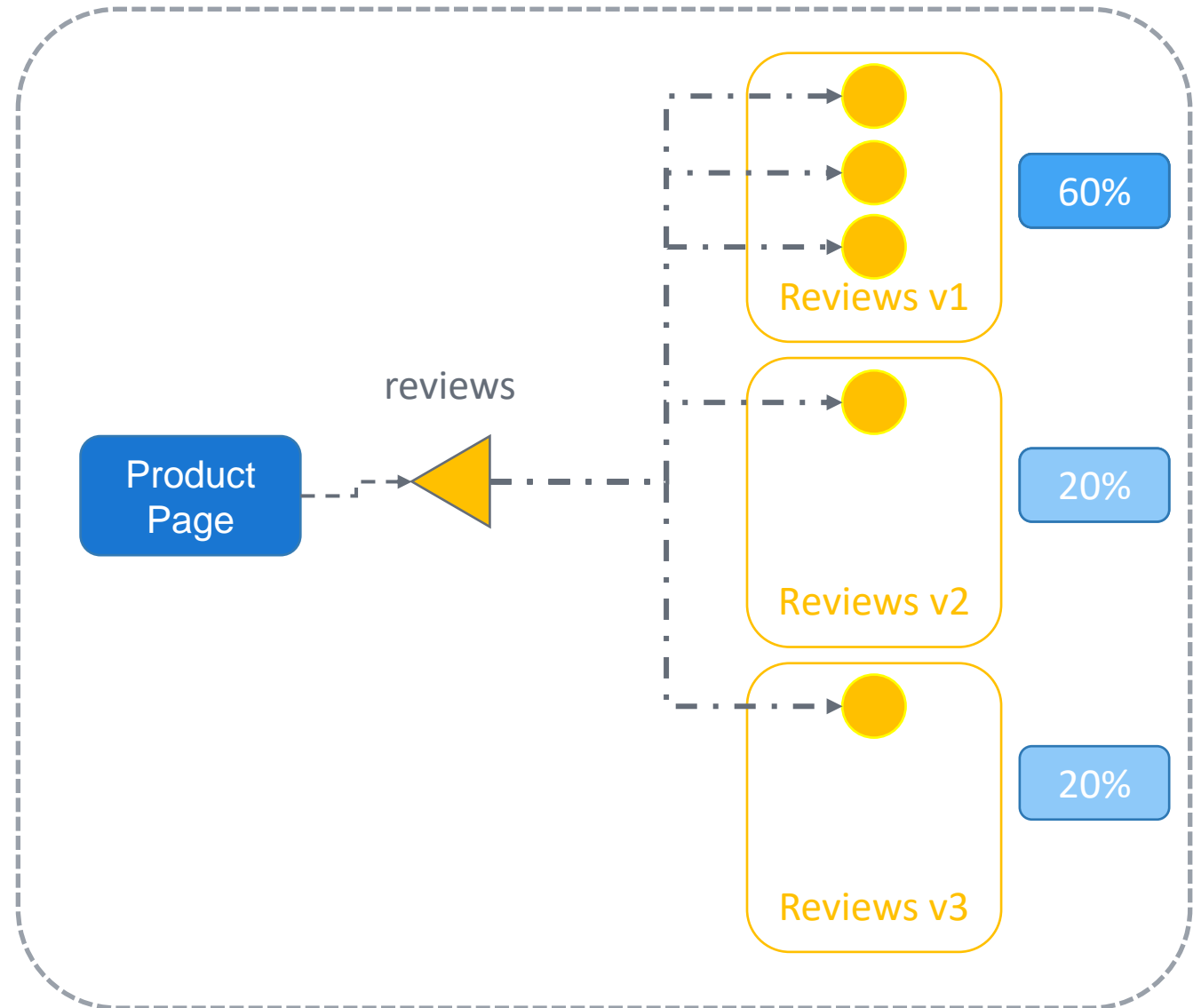


review-v3-deployment.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: reviews-v3
spec:
  replicas: 1
  <...>
  template:
    metadata:
      labels:
        app: reviews
        version: v1
```

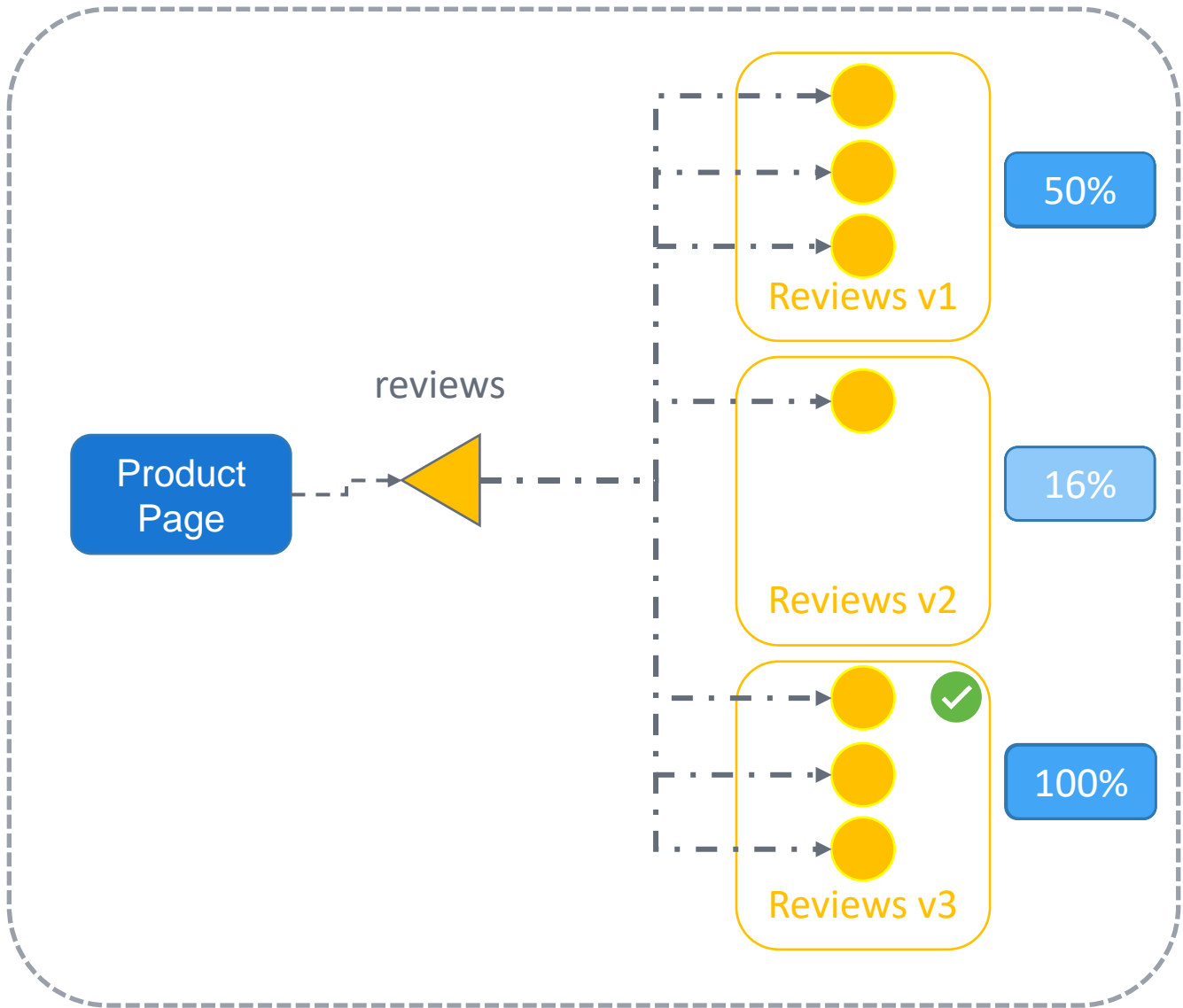
review-service.yaml

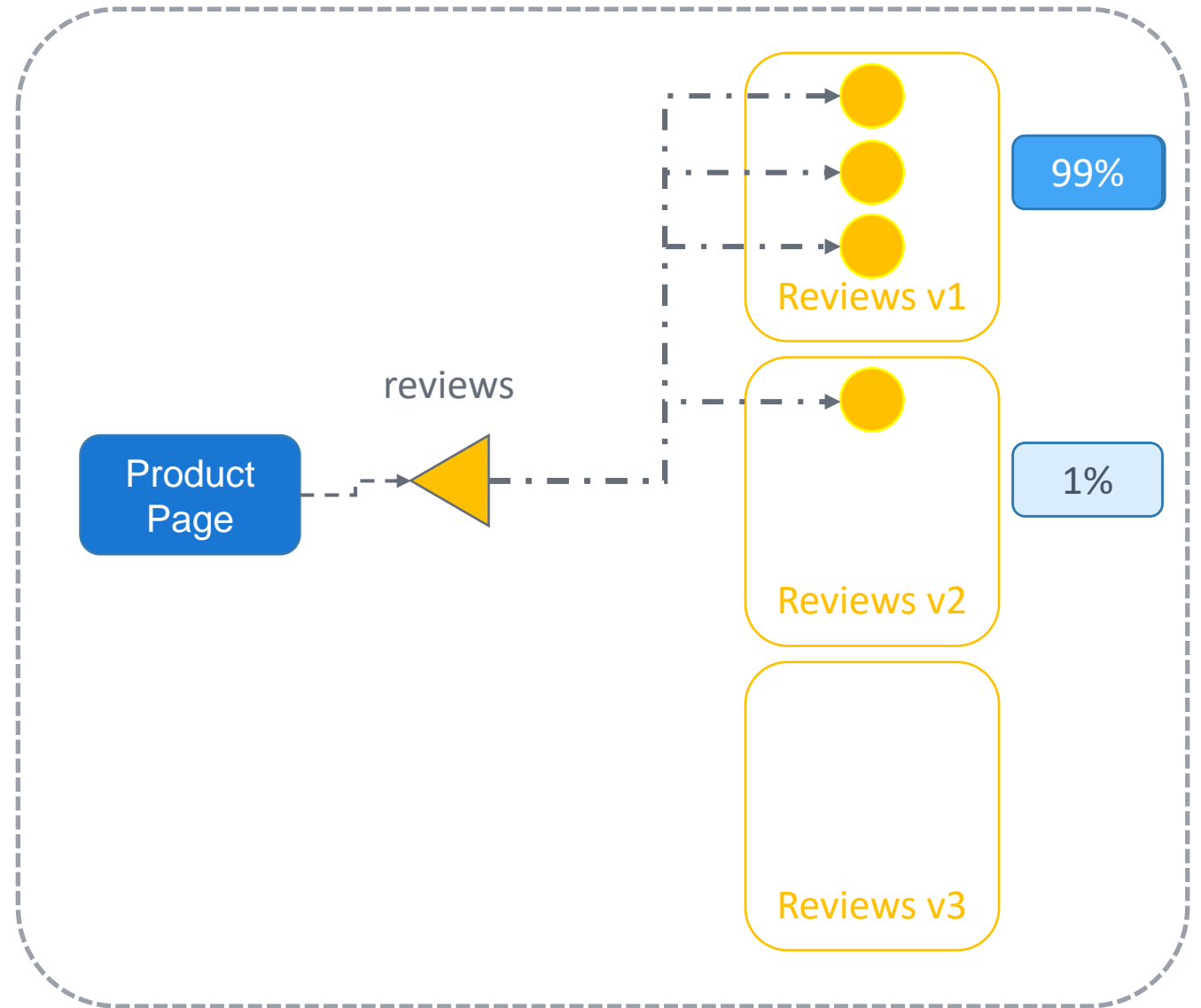
```
apiVersion: v1
kind: Service
metadata:
  name: reviews
spec:
  ports:
    - port: 9080
      name: http
  selector:
    app: reviews
```



```
> _  
$ kubectl scale deployment reviews-v3 --replicas=3  
deployment.apps/reviews-v3 scaled  
$ kubectl scale deployment reviews-v2 --replicas=0  
deployment.apps/reviews-v2 scaled  
$ kubectl scale deployment reviews-v1 --replicas=0  
deployment.apps/reviews-v1 scaled
```

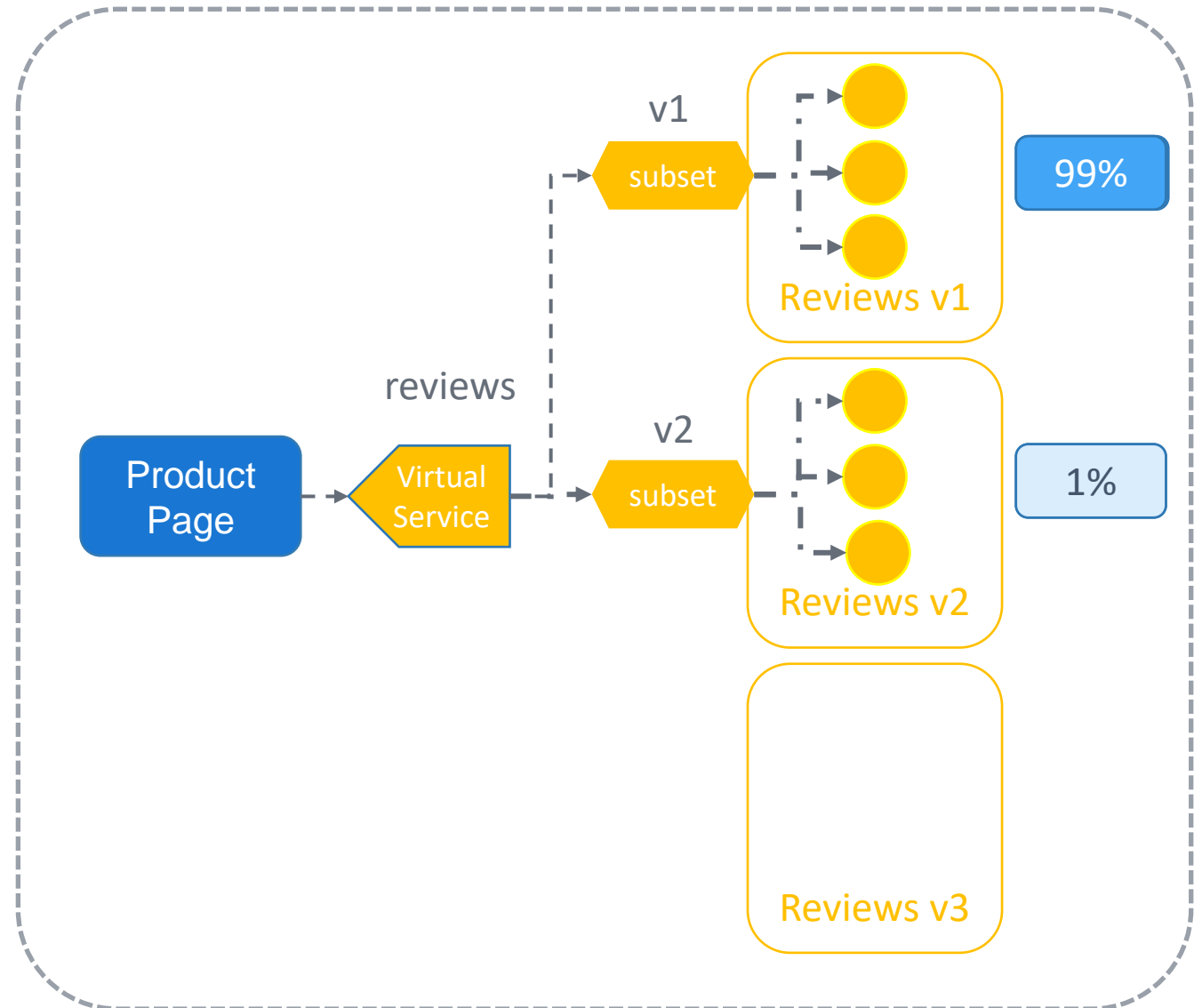
```
review-service.yaml  
apiVersion: v1  
kind: Service  
metadata:  
  name: reviews  
spec:  
  ports:  
  - port: 9080  
    name: http  
  selector:  
    app: reviews
```





review-service.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: reviews
spec:
  hosts:
  - reviews
  http:
  - route:
    - destination:
        host: reviews
        subset: v1
      weight: 99
    - destination:
        host: reviews
        subset: v2
      weight: 1
```





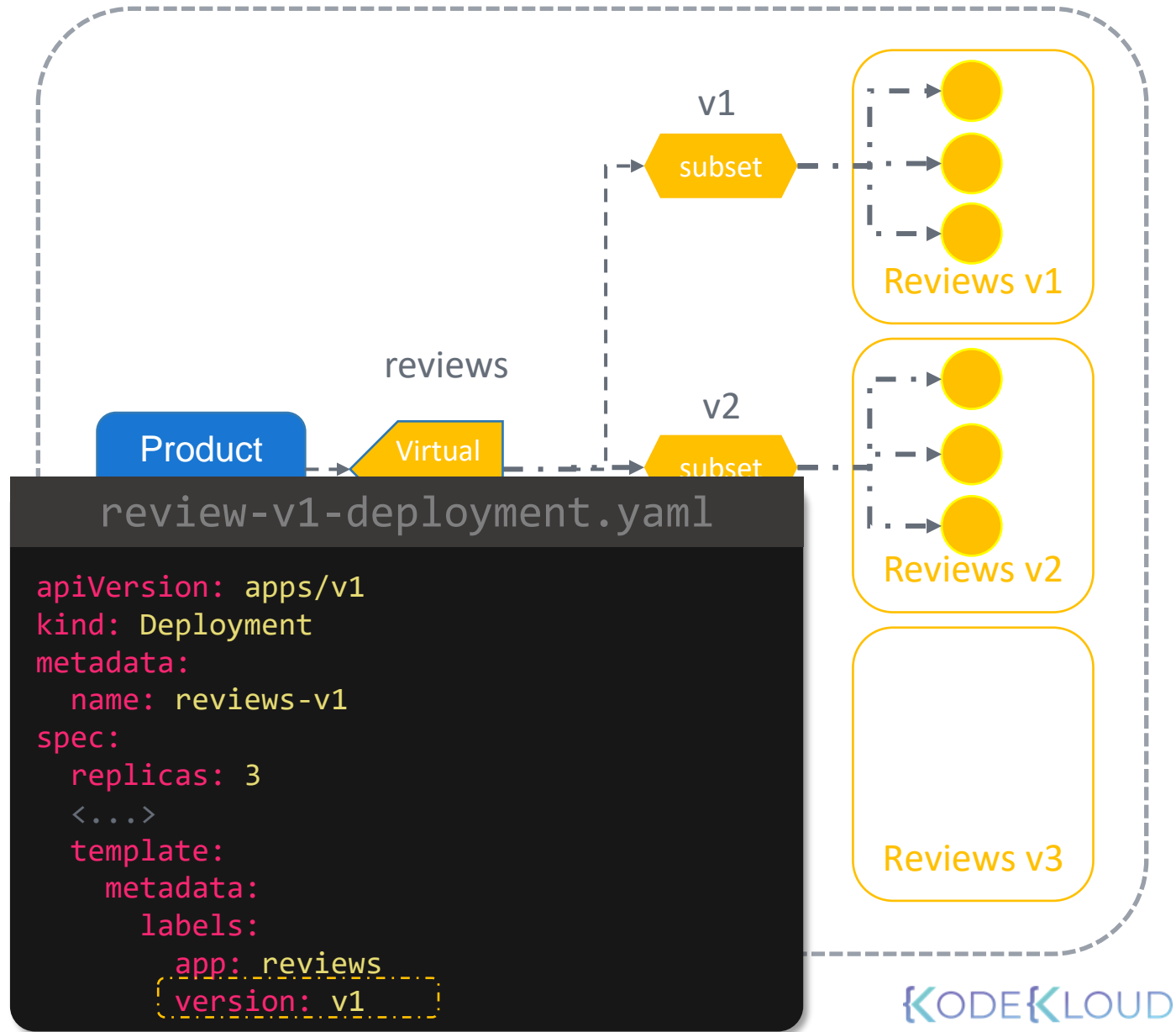
{KODE}{KLOUD

DESTINATION RULES



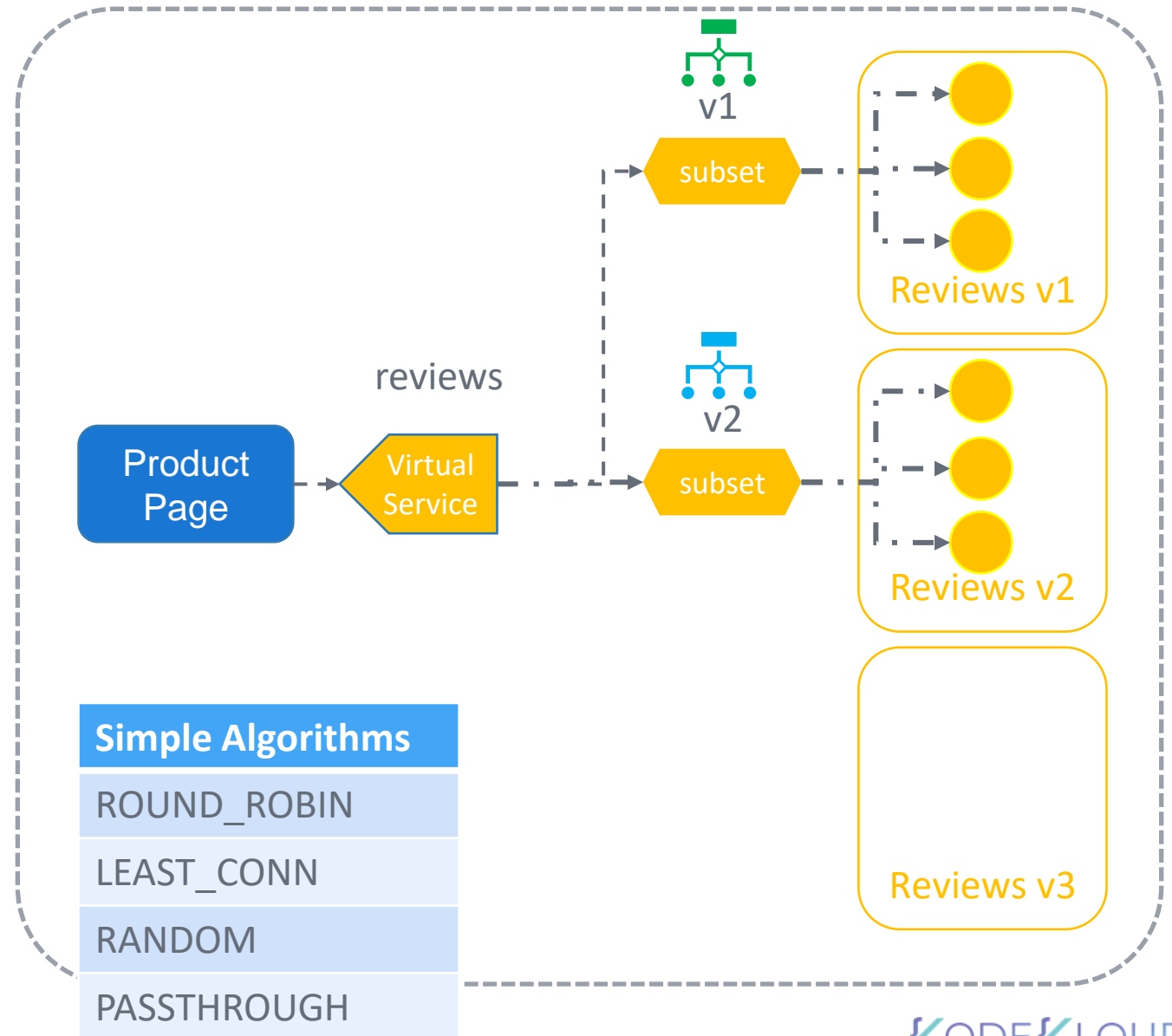
review-destination.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: reviews-destination
spec:
  host: reviews
  subsets:
  - name: v1
    labels:
      version: v1
  - name: v2
    labels:
      version: v2
```



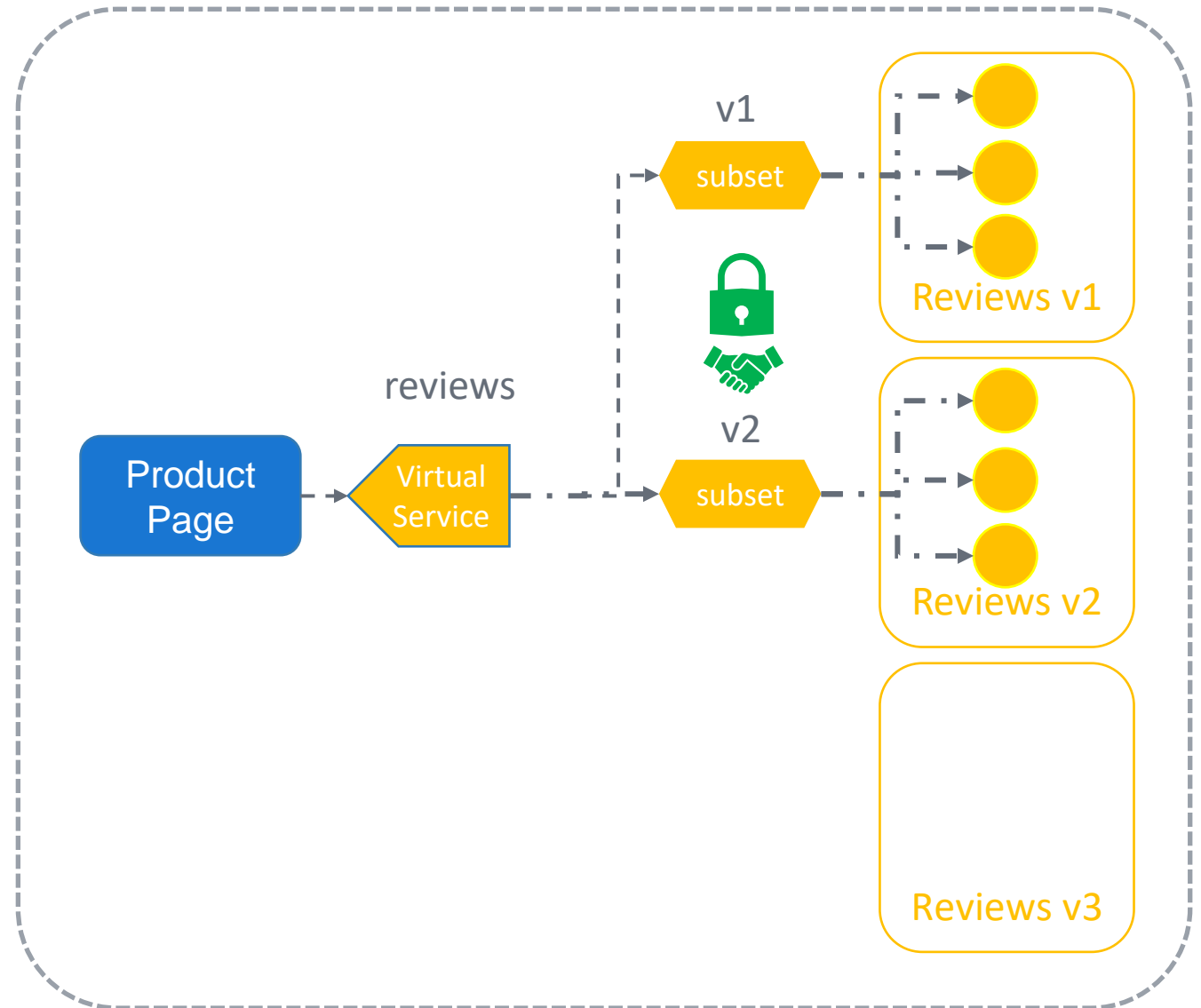
review-destination.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: reviews-destination
spec:
  host: reviews
  trafficPolicy:
    loadBalancer:
      simple: PASSTHROUGH
  subsets:
  - name: v1
    labels:
      version: v1
  - name: v2
    labels:
      version: v2
    trafficPolicy:
      loadBalancer:
        simple: RANDOM
```



review-destination.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: reviews-destination
spec:
  host: reviews.default.svc.cluster.local
  trafficPolicy:
    tls:
      mode: MUTUAL
      clientCertificate: /myclientcert.pem
      privateKey: /client_private_key.pem
      caCertificates: /rootcacerts.pem
```



An Example With Fully Qualified Domain Names

virtual-service.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: productpage
  namespace: default
spec:
  hosts:
  - productpage.prod.svc.cluster.local
  http:
  - timeout: 5s
    route:
    - destination:
        host: productpage.prod.svc.cluster.local
```

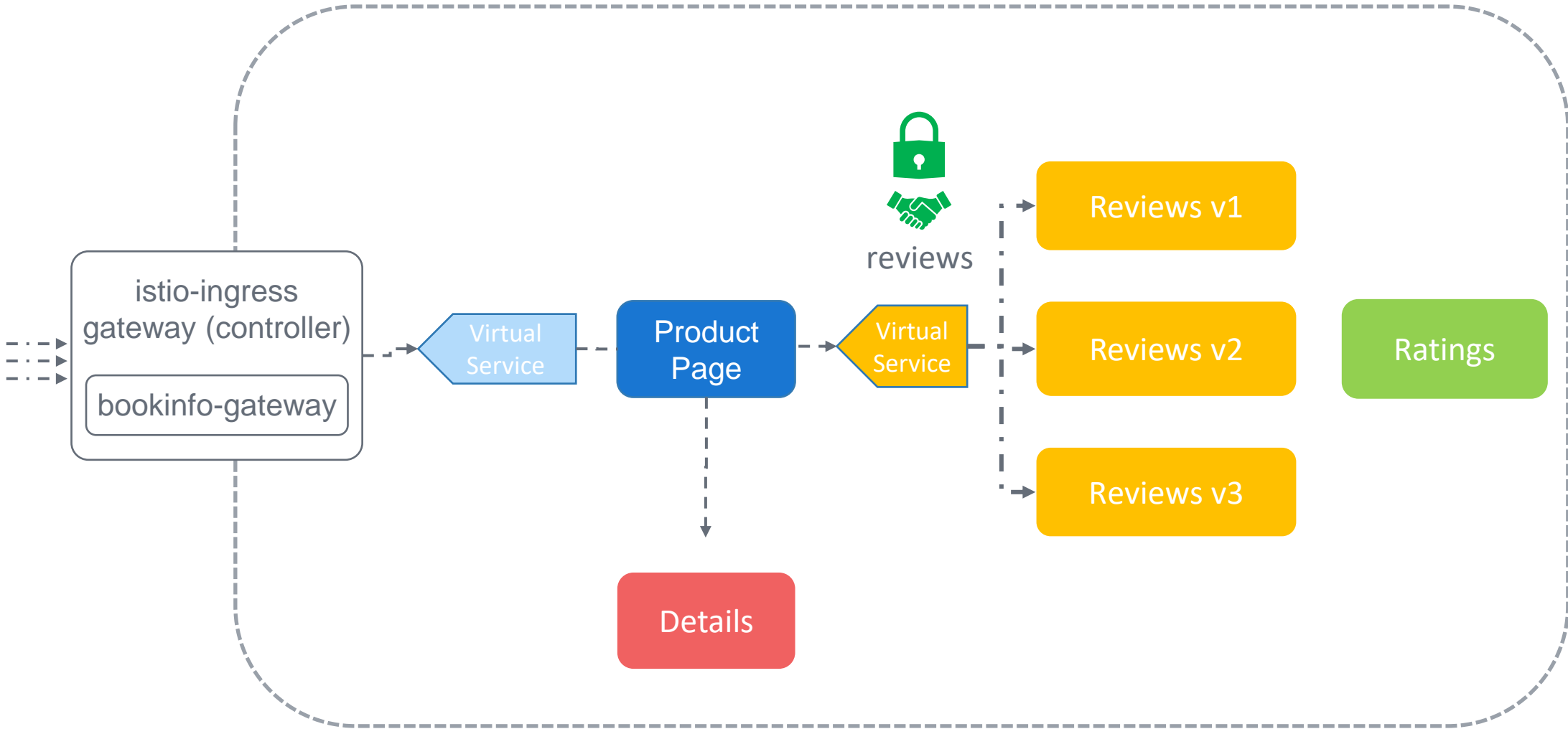


{KODE}{KLOUD

FAULT INJECTION



Istio Virtual Services



fault-injection.yaml

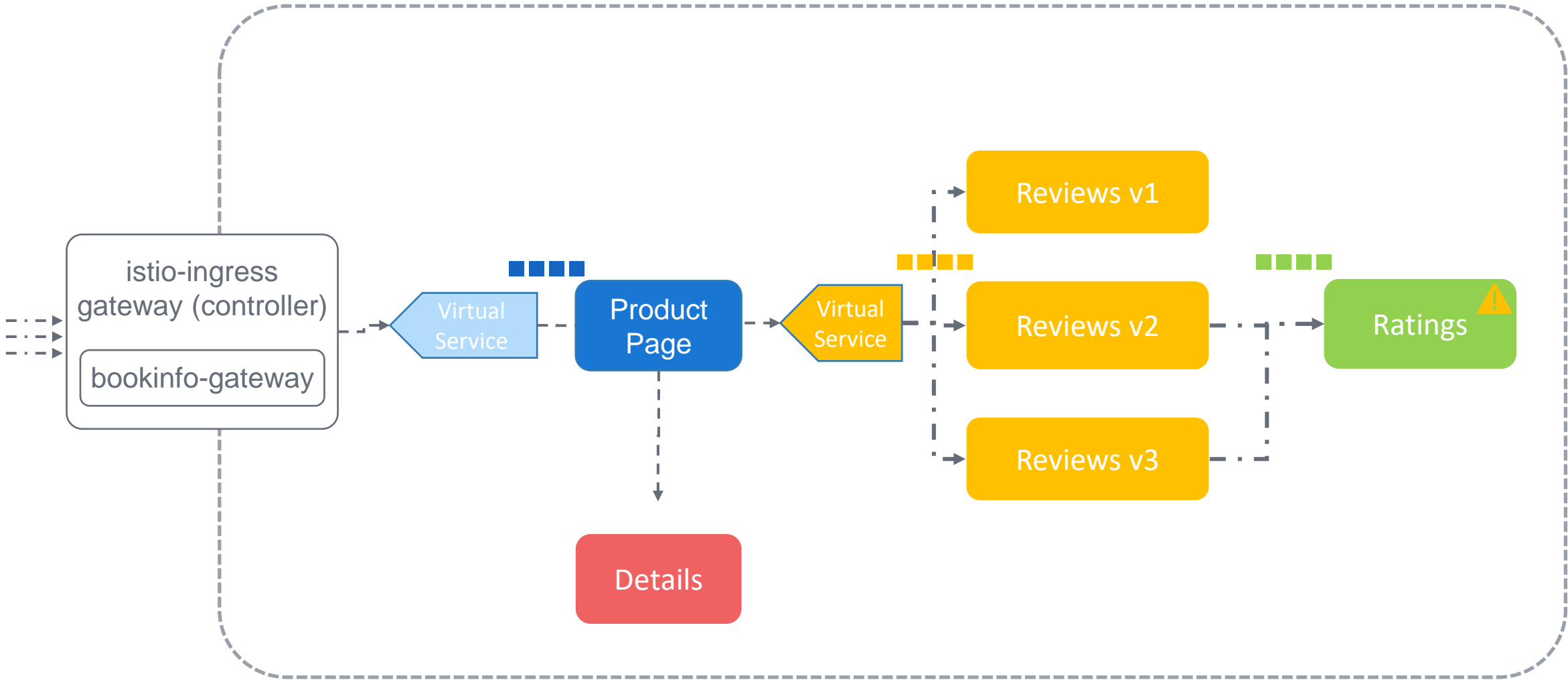
```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: my-service
spec:
  hosts:
  - my-service
  http:
  - fault:
      delay:
      percentage:
        value: 0.1
        fixedDelay: 5s
      abort:
        percentage:
          value: 0.1
          httpStatus: 400
  route:
  - destination:
      host: my-service
      subset: v1
```



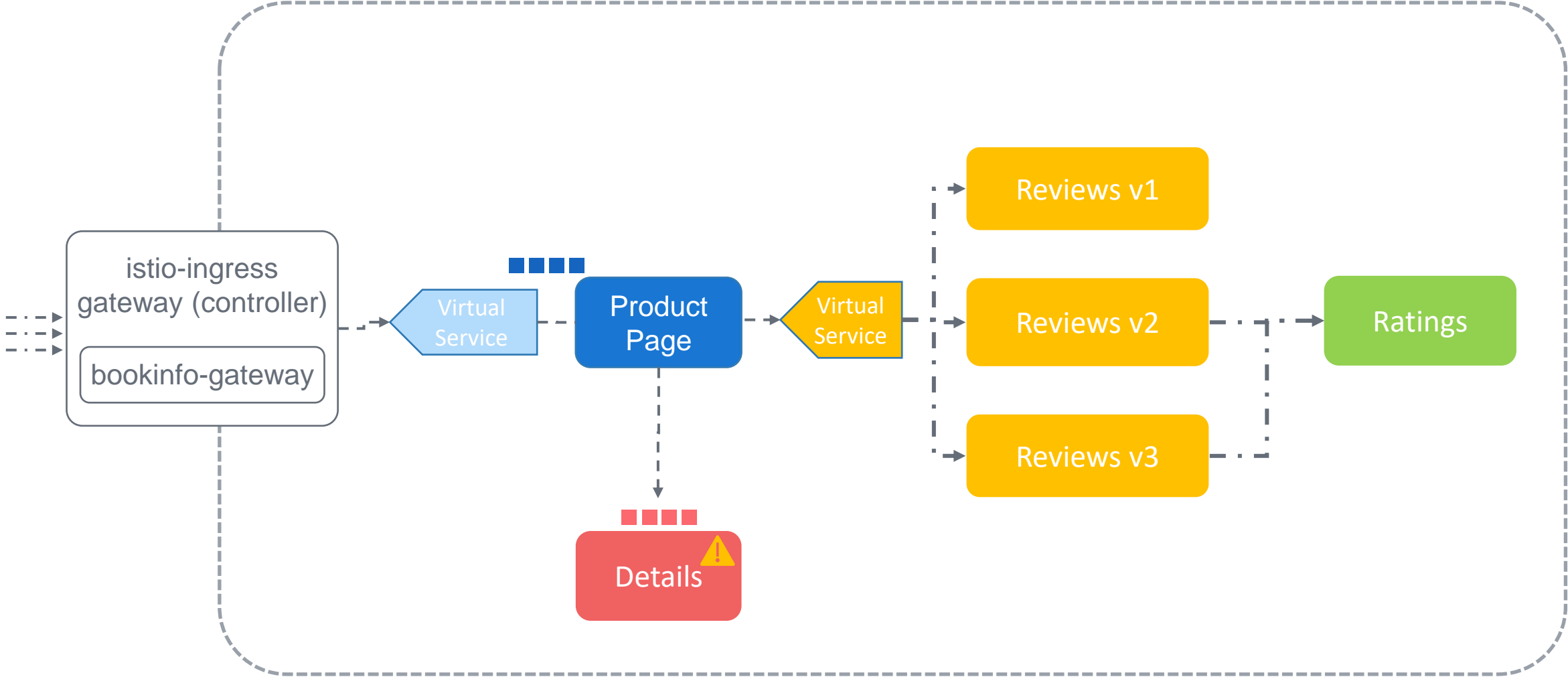
{KODE}{KLOUD

TIMEOUTS





Timeouts



book-info.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: bookinfo
spec:
  hosts:
  - "bookinfo.app"

  gateways:
  - bookinfo-gateway

  http:
  - match:
    - uri:
        exact: /productpage
    - uri:
        prefix: /static
    <code hidden>

    route:
    - destination:
        host: productpage
        port:
          number: 9080
    timeout: 3s
```

details-service.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: details
spec:
  hosts:
  - details

  http:
  - route:
    - destination:
        host: details
        subset: v1

    fault:
      delay:
        fixedDelay: 5s
        percent: 50
```

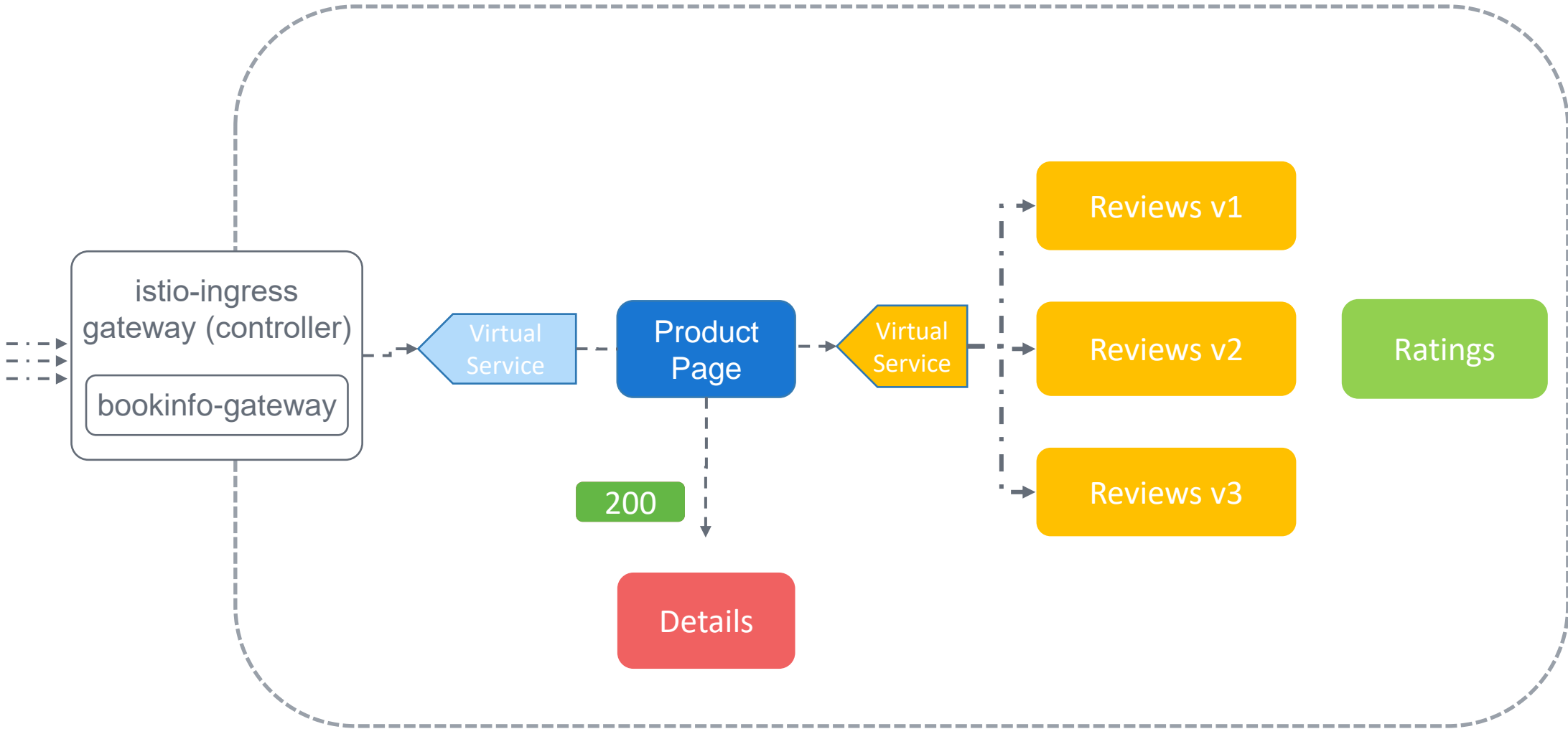


{KODE}{KLOUD

RETRIES



Istio Virtual Services



Virtual-service-timeout.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: my-service
spec:
  hosts:
  - my-service
  http:
  - route:
    - destination:
        host: my-service
        subset: v1
    retries:
      attempts: 3
      perTryTimeout: 2s
```

ISTIO DEFAULTS

25ms+ intervals after 1st fail
2 retries before returning an error

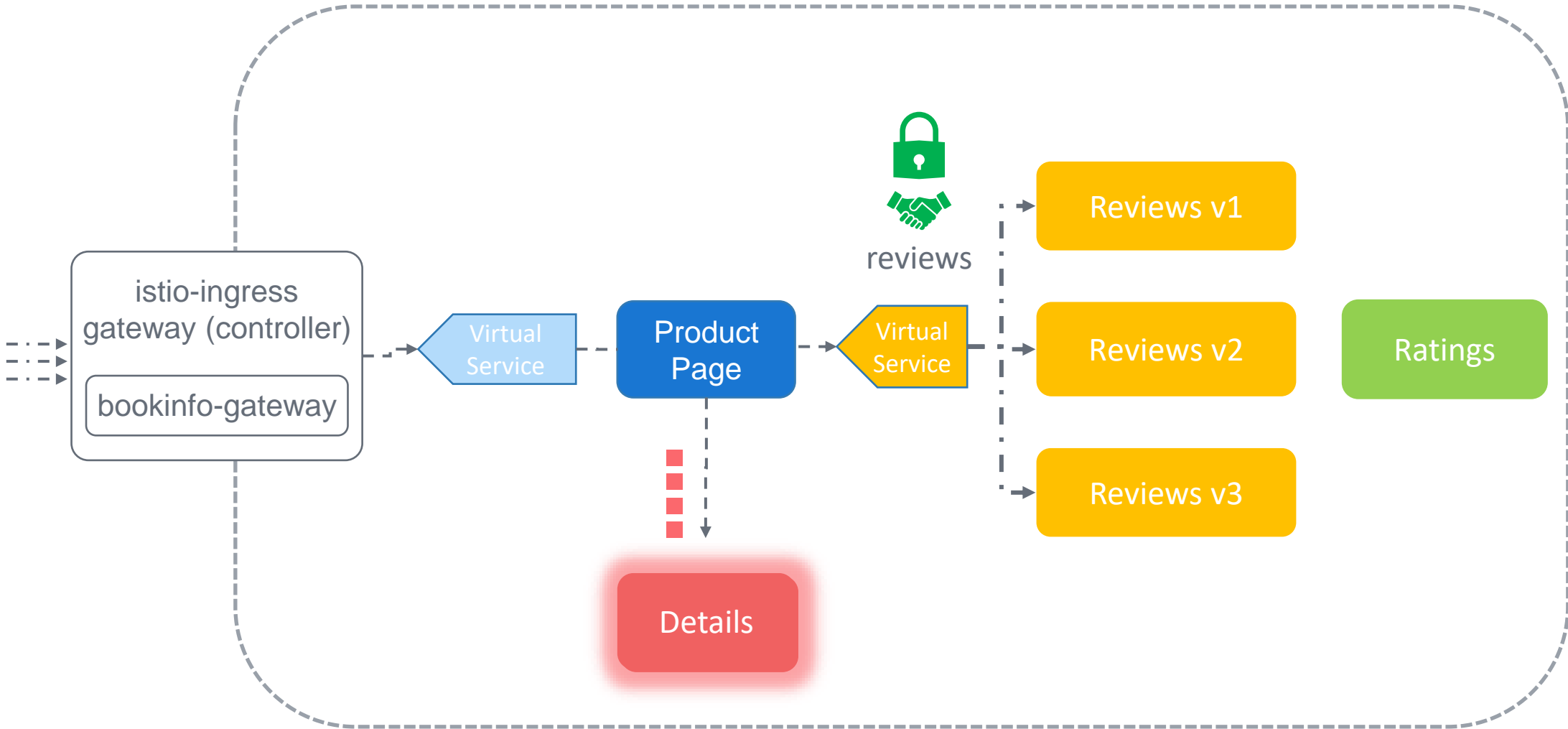


{KODE}{KLOUD

CIRCUIT BREAKING



Istio Circuit Breaking



Circuit Breaking

circuit-breaking.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: productpage
spec:
  host: productpage
  subsets:
  - name: v1
    labels:
      version: v1
    trafficPolicy:
      connectionPool:
        tcp:
          maxConnections: 3
```

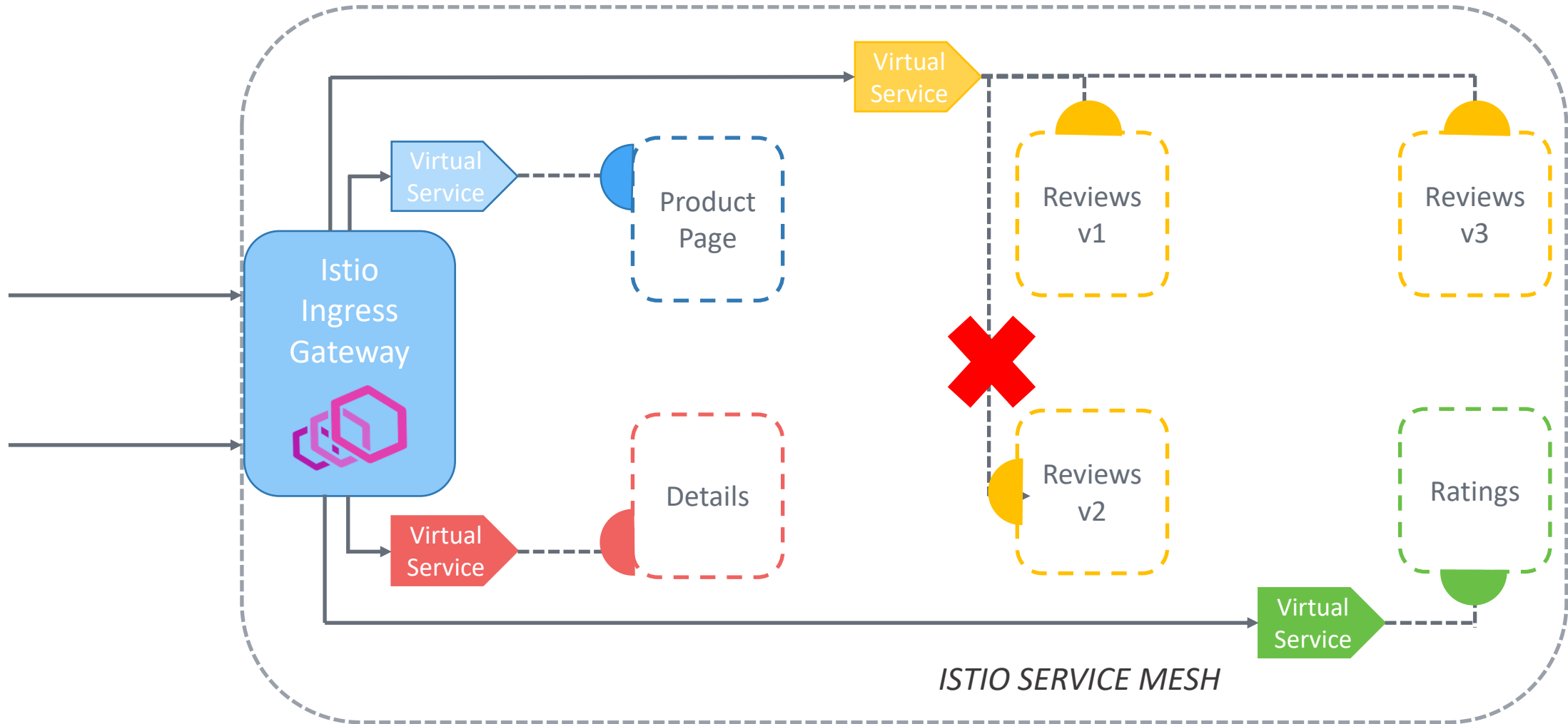


{KODE}{KLOUD

REQUEST ROUTING



Request Routing



Request Routing

request-routing.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: reviews
spec:
  hosts:
  - reviews
  http:
  - route:
    - destination:
      host: reviews
      subset: v1
```

Request Routing

request-routing.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: reviews
spec:
  hosts:
  - reviews
  http:
  - route:
    - destination:
      host: reviews
      subset: v1
```

Request Routing

request-routing.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: reviews
spec:
  hosts:
  - reviews
  http:
  - route:
    - destination:
      host: reviews
      subset: v1
```



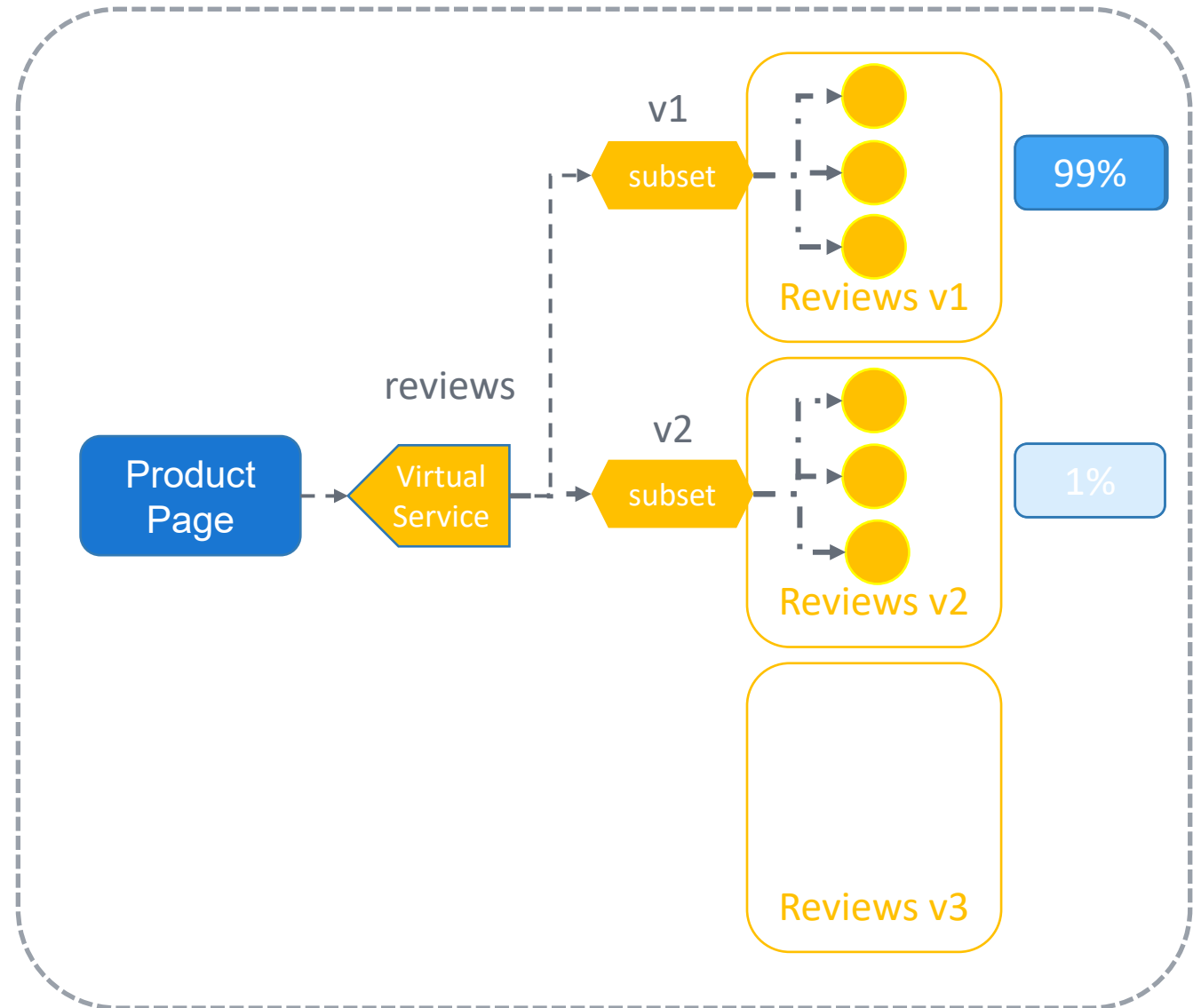
{KODE}{KLOUD

A/B TESTING



review-service.yaml

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: reviews
spec:
  hosts:
  - reviews
  http:
  - route:
    - destination:
        host: reviews
        subset: v1
      weight: 99
    - destination:
        host: reviews
        subset: v2
      weight: 1
```



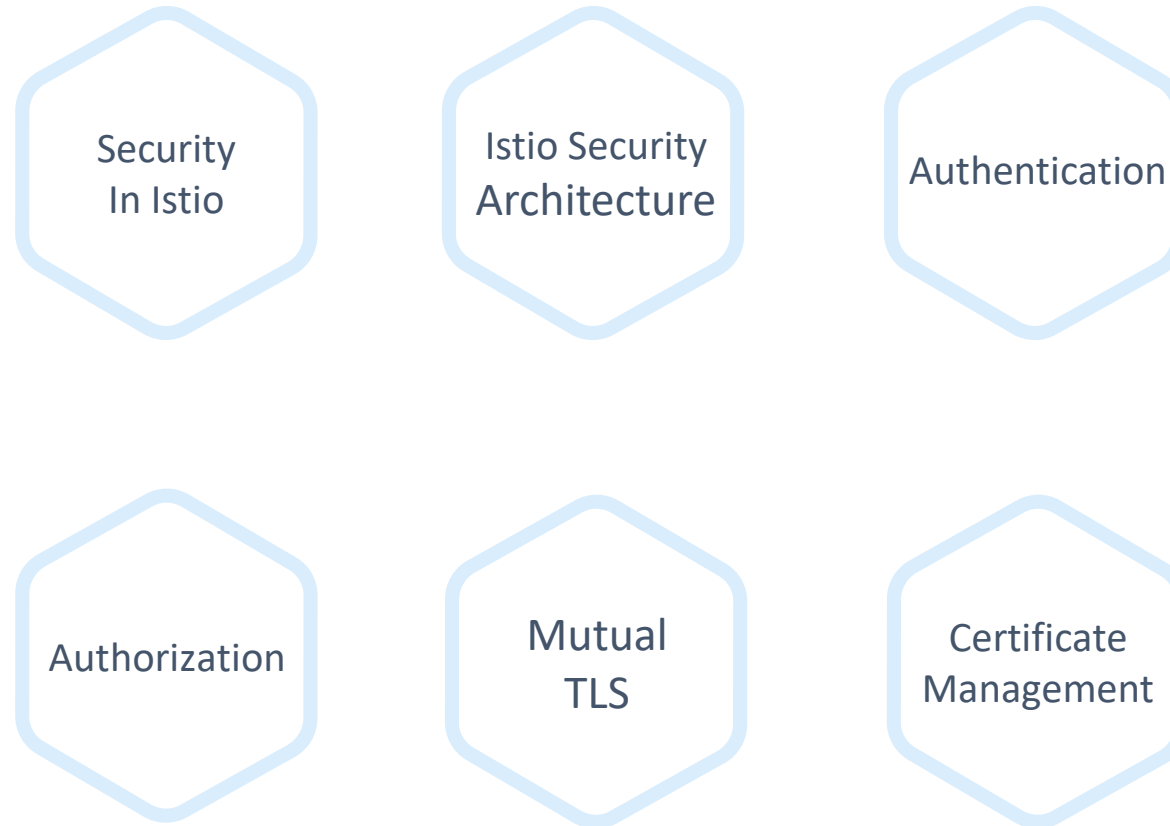


{KODE}{KLOUD

SECTION INTRODUCTION



Security

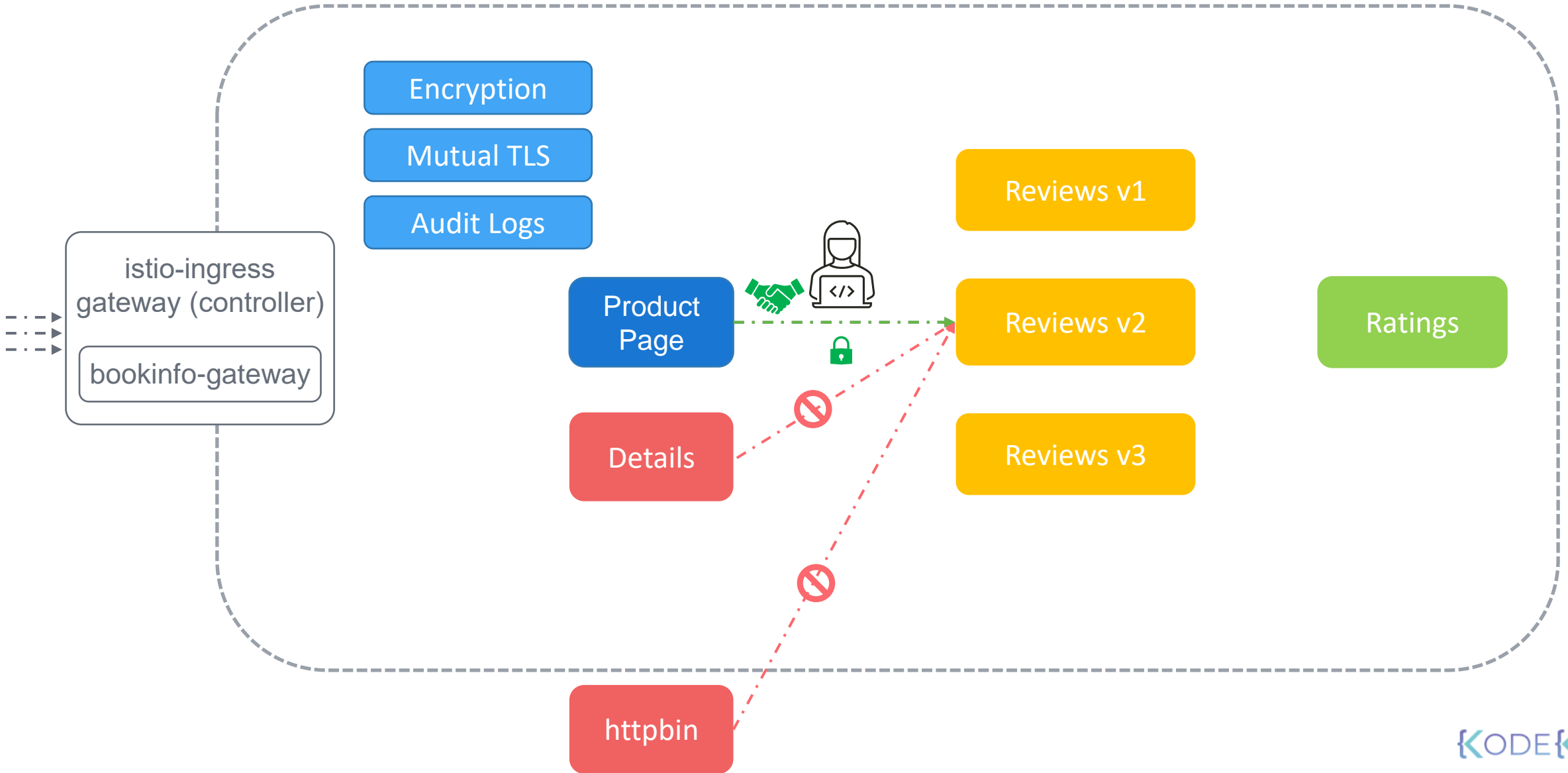




{KODE}{KLOUD

SECURITY IN ISTIO





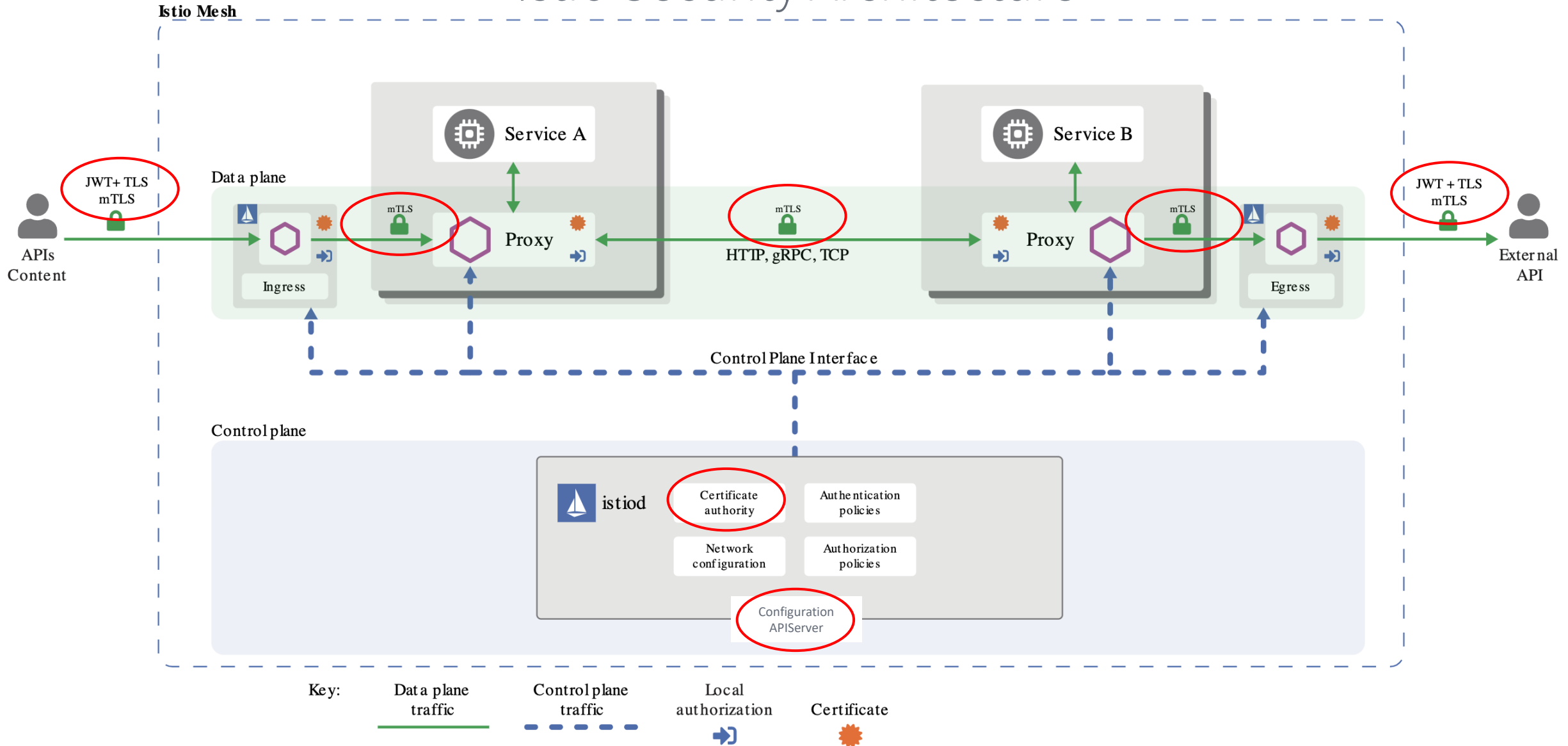


{KODE}{KLOUD

ISTIO SECURITY ARCHITECTURE



Istio Security Architecture



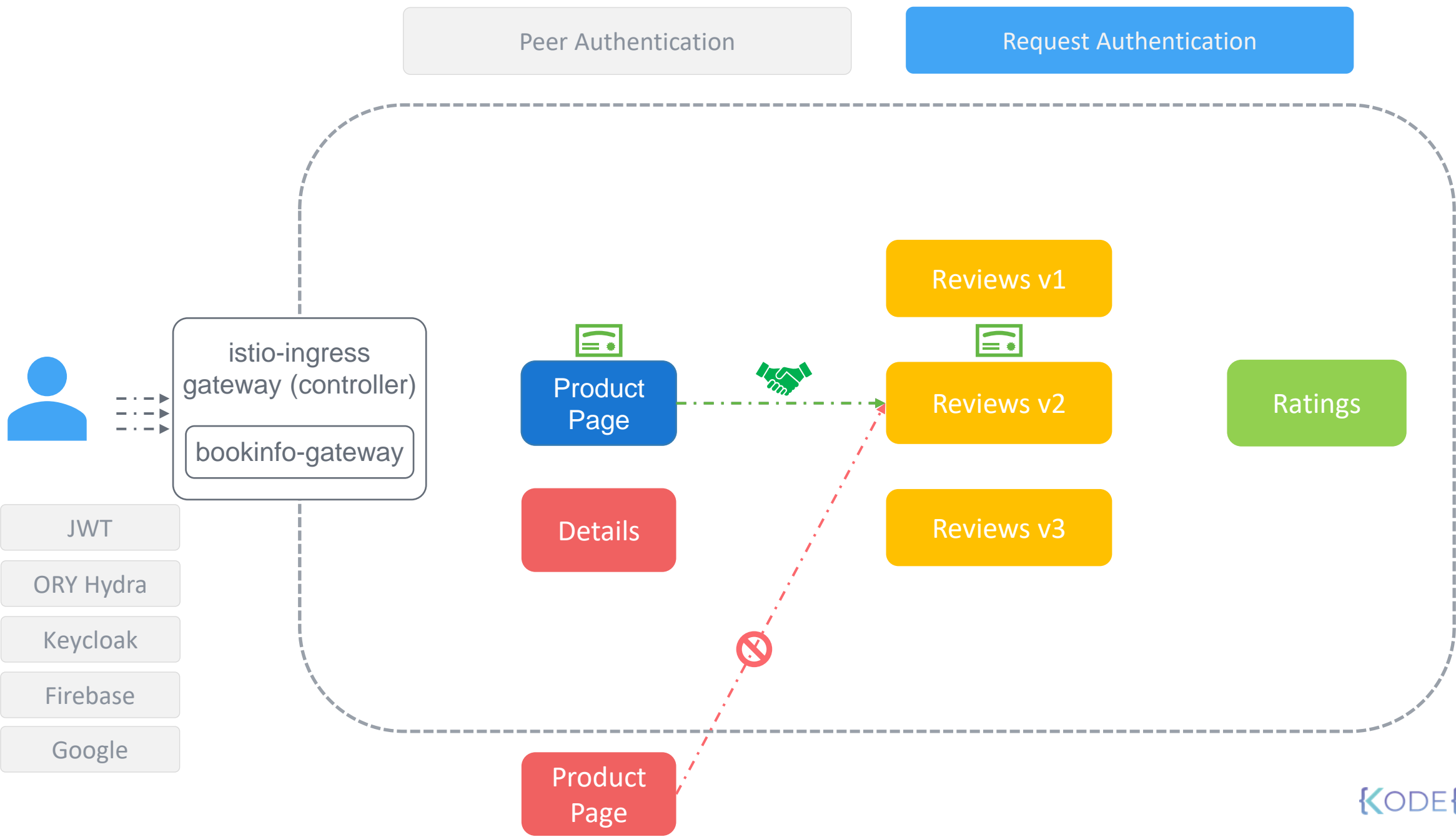
Security Architecture



{KODE{KLOUD

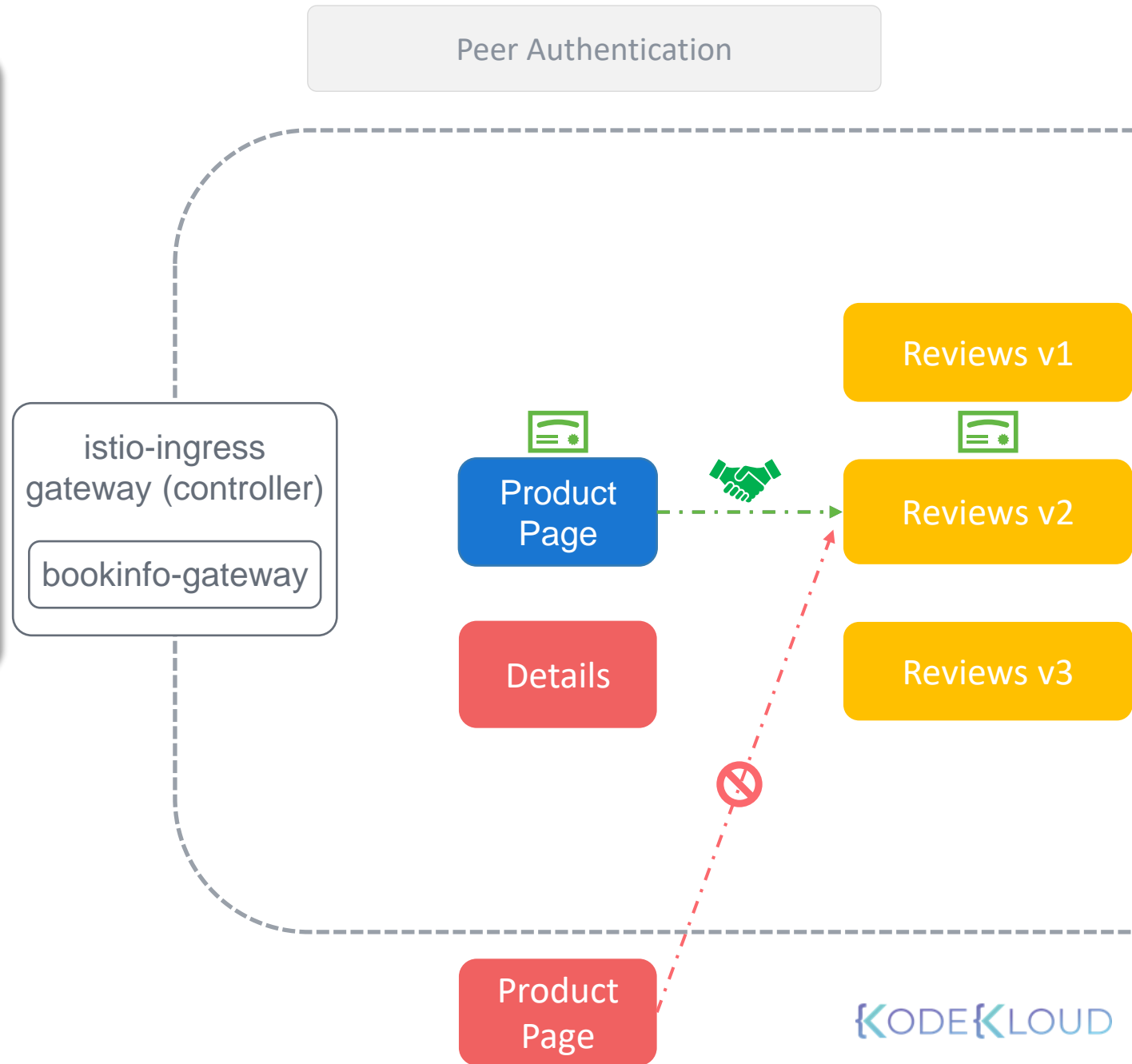
AUTHENTICATION





```
example-peer-authentication.yaml
```

```
apiVersion: security.istio.io/v1beta1
kind: PeerAuthentication
metadata:
  name: "example-peer-policy"
  namespace: "book-info"
spec:
  selector:
    matchLabels:
      app: reviews
  mtls:
    mode: STRICT
```



```
example-peer-authentication.yaml
```

```
apiVersion: security.istio.io/v1beta1  
kind: PeerAuthentication  
metadata:  
  name: "example-peer-policy"  
  namespace: "istio-system"  
spec:
```

```
mtls:  
  mode: STRICT
```

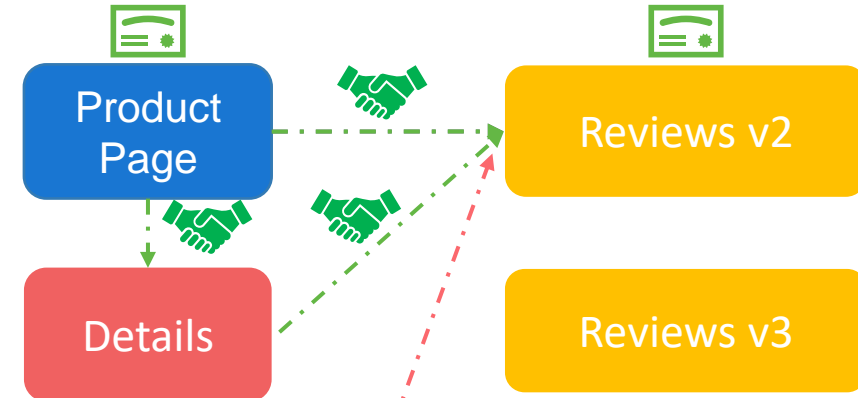
Workload-specific policy

Namespace-wide policy

Mesh-wide policy

Peer Authentication

istio-ingress
gateway (controller)
bookinfo-gateway



Product
Page

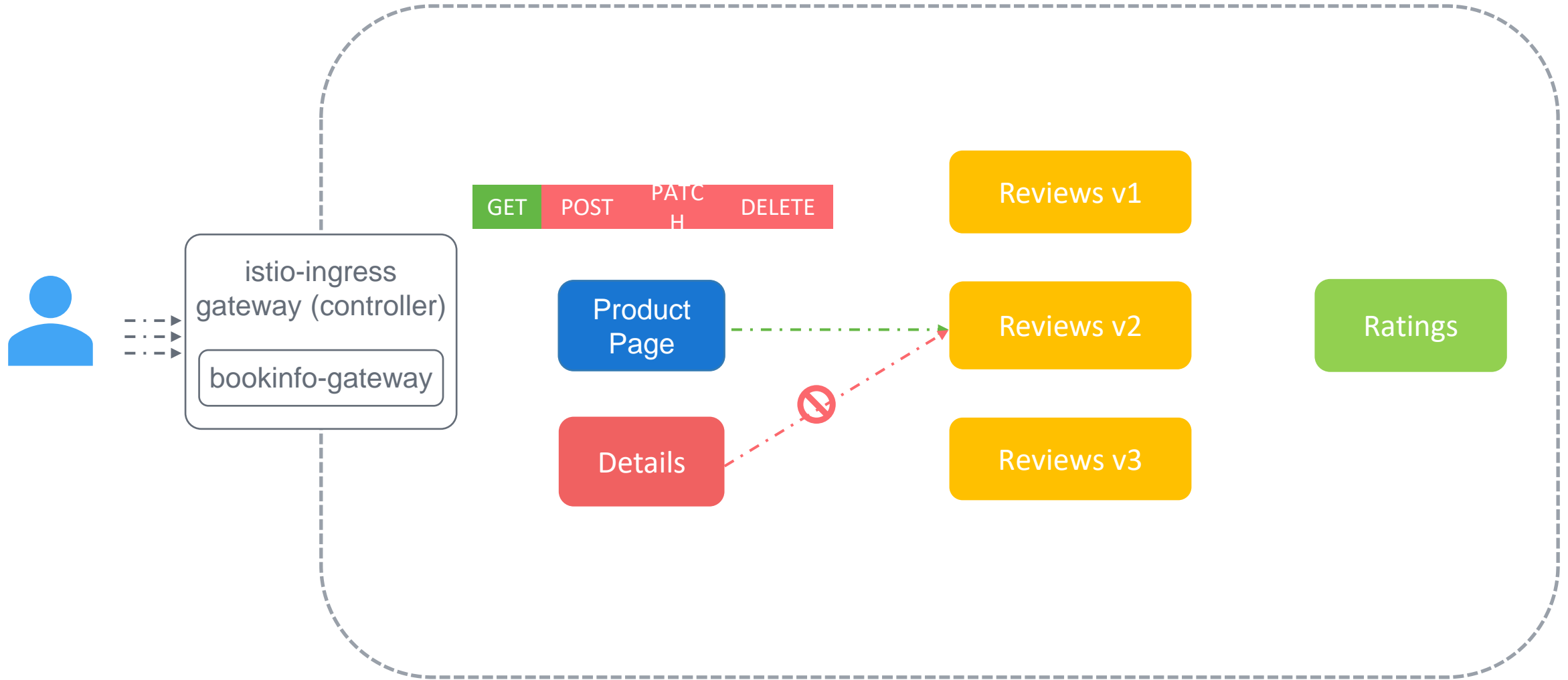


{KODE}{KLOUD

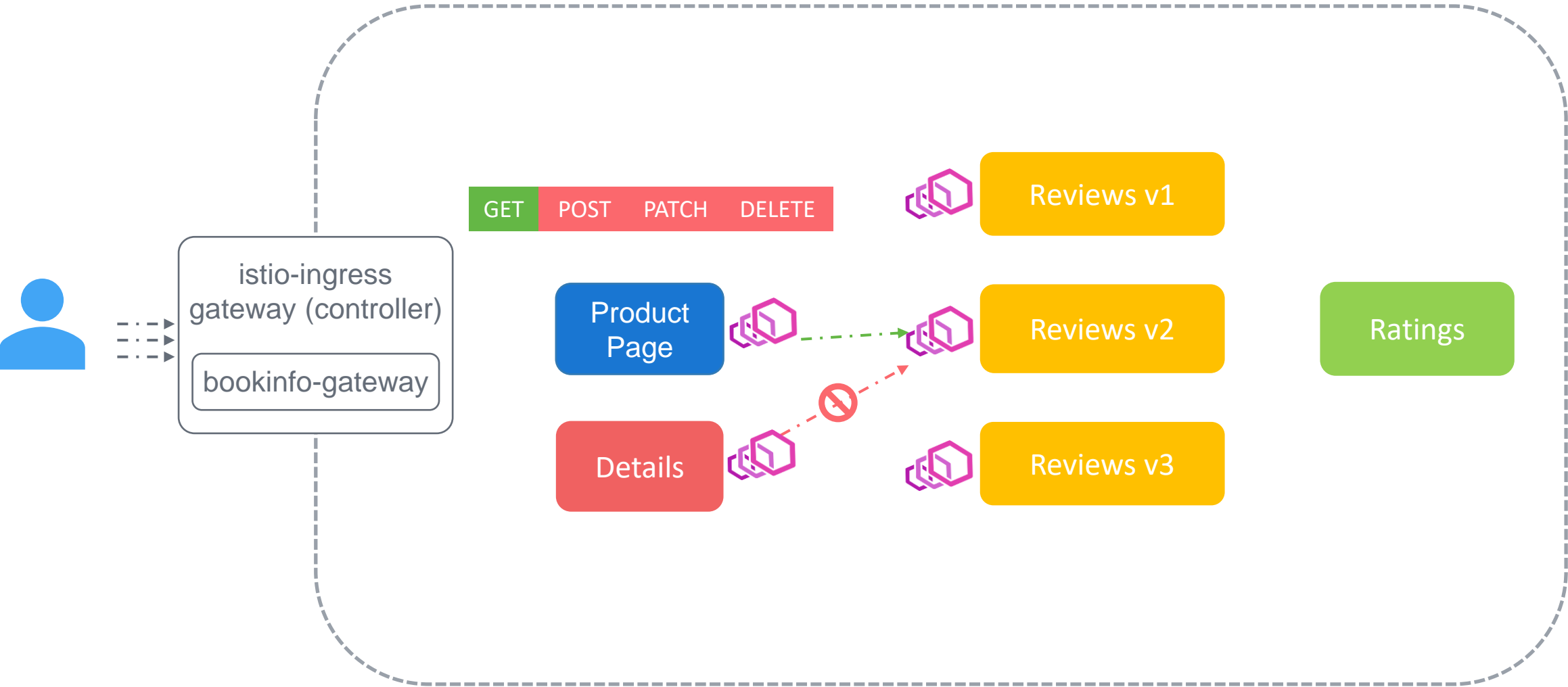
AUTHORIZATION



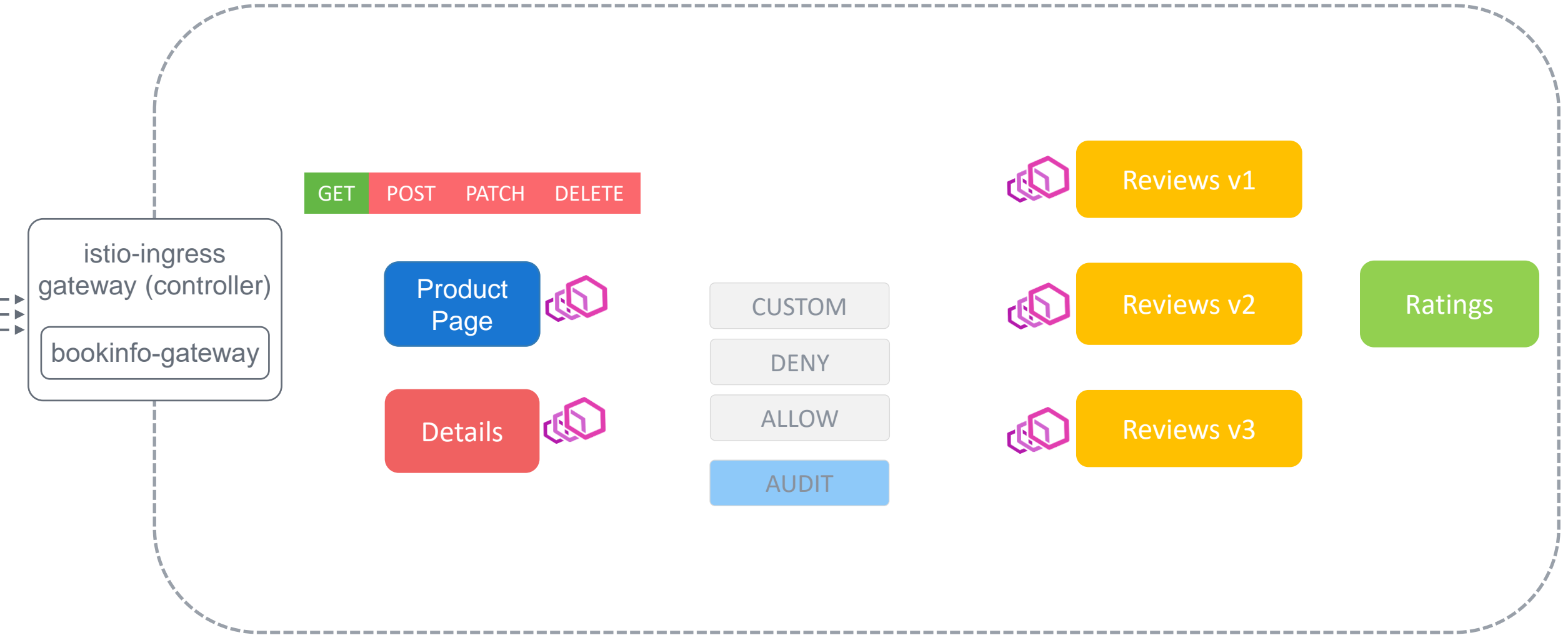
Authorization



Authorization Actions

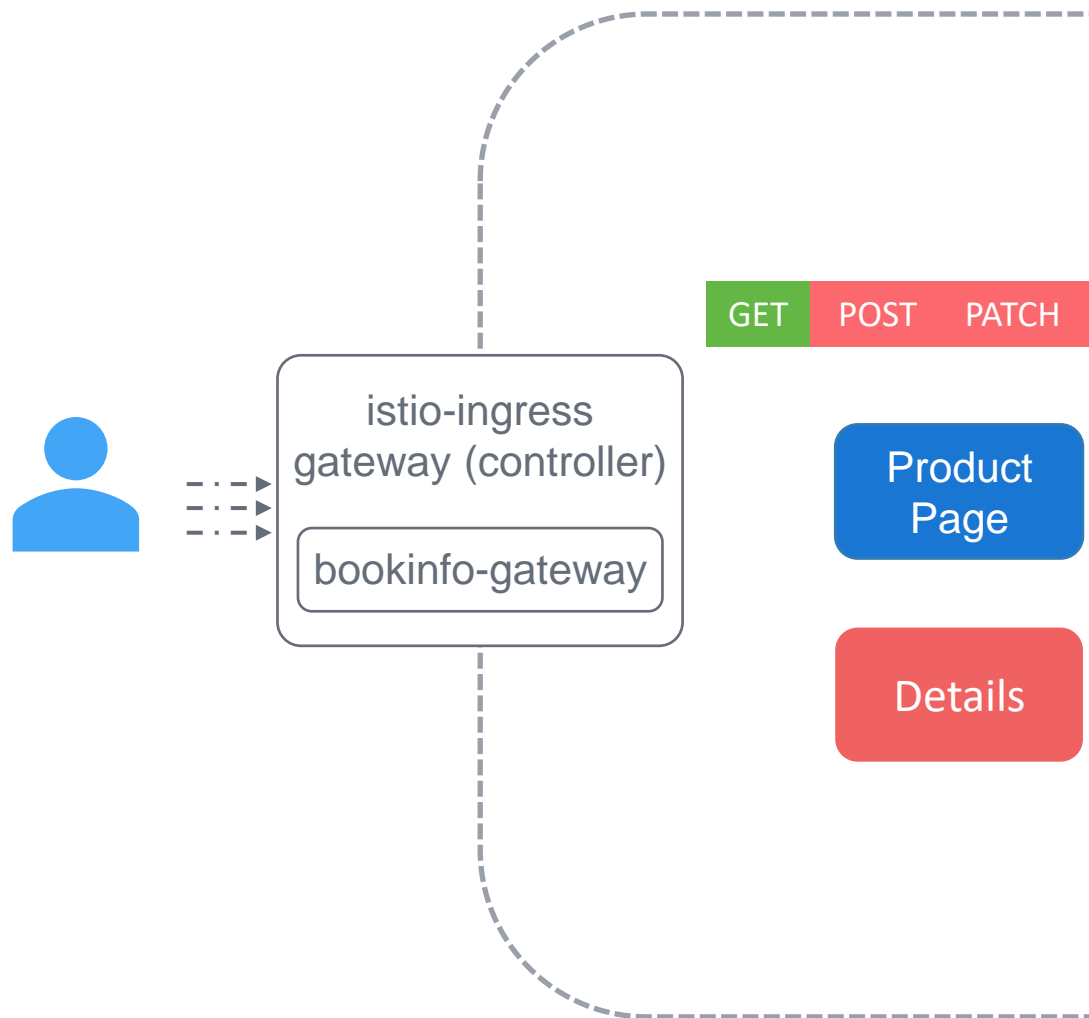


Authorization



auth-policy.yaml

```
apiVersion: security.istio.io/v1beta1
kind: AuthorizationPolicy
metadata:
  name: authdenypolicy
  namespace: bookinfo
spec:
  action: DENY
  rules:
  - from:
    - source:
      namespaces: ["bar"]
    to:
    - operation:
      methods: ["POST"]
```



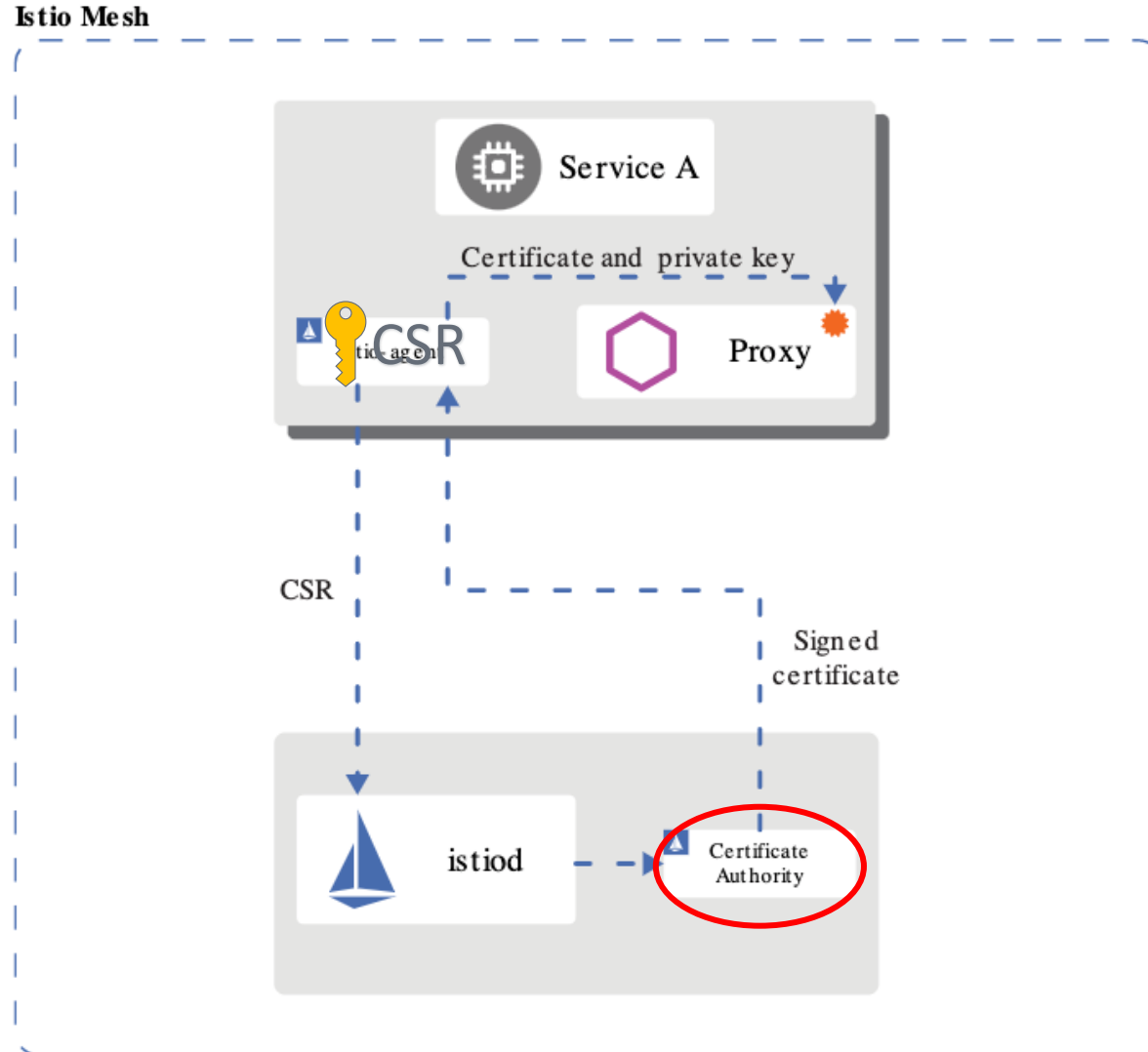


{KODE}{KLOUD

CERTIFICATE MANAGEMENT

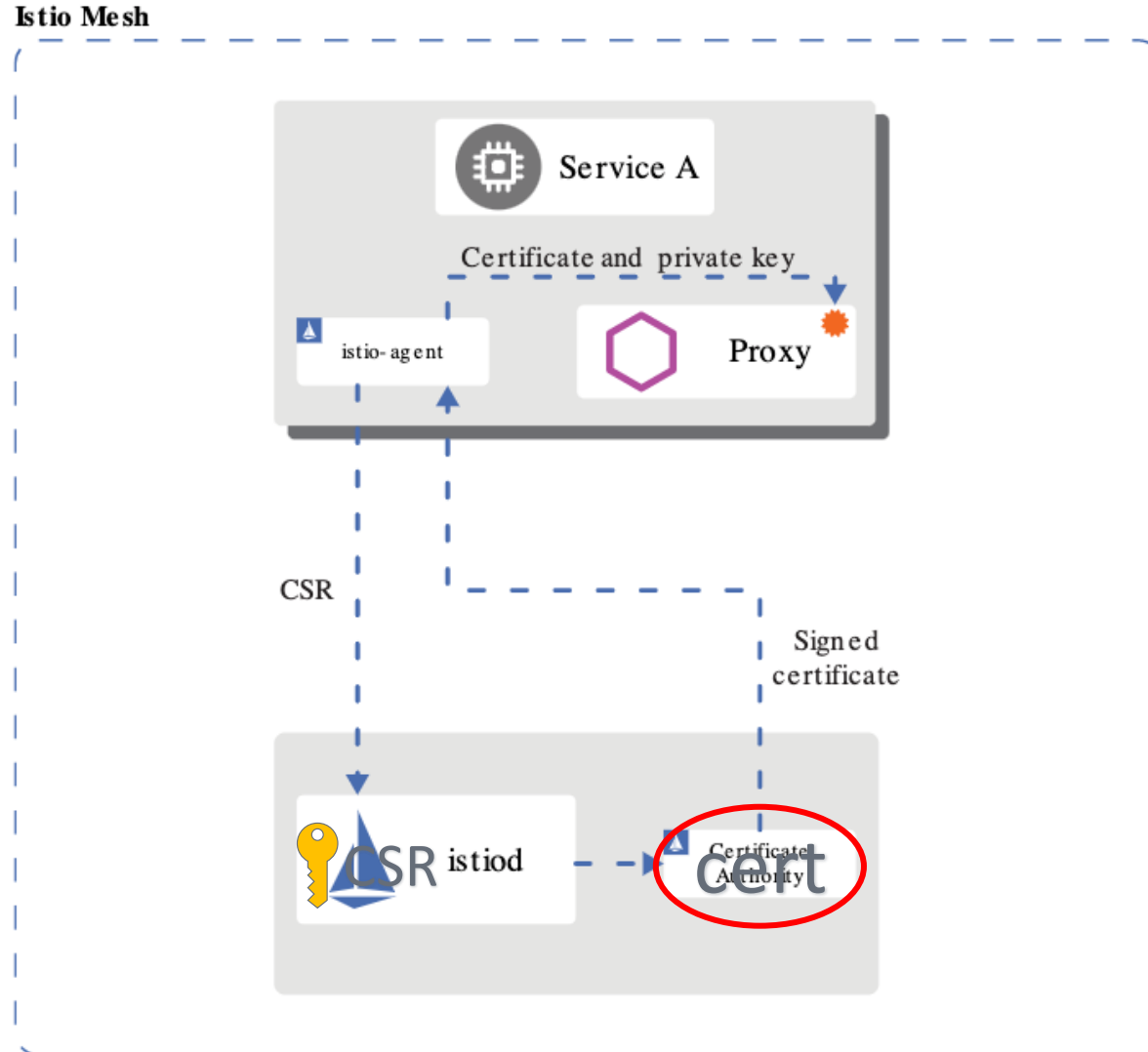


Certificate Management



Identity Provisioning Workflow

Certificate Management



Identity Provisioning Workflow

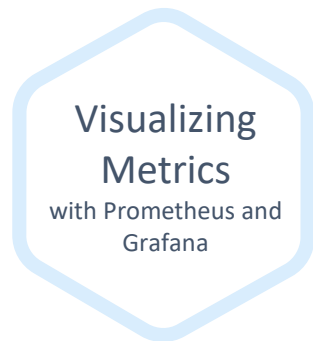


{KODE}{KLOUD

OBSERVABILITY



Observability





{KODE}{KLOUD

VISUALIZING METRICS

WITH PROMETHEUS AND GRAFANA







{KODE}{KLOUD

DISTRIBUTED TRACING WITH JAEGER





Lightstep



Search JSON File

Service (1)
istio-ingressgateway

Operation (1)
productpage.default.svc.cluster.local:9080/produ..

Tags [?]
http.status_code=200 error=true

Lookback
Last Hour

Min Duration
e.g. 1.2s, 100ms, 500us

Max Duration
e.g. 1.2s, 100ms, 500us

Limit Results
20

[Find Traces](#)



20 Traces Sort: Most Recent Deep Dependency Graph

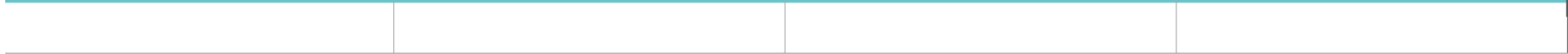
Compare traces by selecting result items

- istio-ingressgateway: productpage.default.svc.cluster.local:9080/productpage** df78a37 42.09ms
1 Span 1 Error istio-ingressgateway (1) Today | 7:53:33 am
a few seconds ago
- istio-ingressgateway: productpage.default.svc.cluster.local:9080/productpage** ac0bf53 63.29ms
1 Span 1 Error istio-ingressgateway (1) Today | 7:53:32 am
a few seconds ago
- istio-ingressgateway: productpage.default.svc.cluster.local:9080/productpage** 152acf4 64.47ms
1 Span 1 Error istio-ingressgateway (1) Today | 7:53:32 am
a few seconds ago
- istio-ingressgateway: productpage.default.svc.cluster.local:9080/productpage** 033ca82 57.72ms
1 Span 1 Error istio-ingressgateway (1) Today | 7:53:32 am

istio-ingressgateway: productpage.default.svc.cluster.local:9080/ productpage df78a37

Find... Trace Timeline

Trace Start June 29 2021, 07:53:33.068 Duration 42.09ms Services 1 Depth 1 Total Spans 1



Service & Operation	0ms	10.52ms	21.04ms	31.57ms	42.09ms
istio-ingressgateway productpage.default.svc.cluster.local:908...					

productpage.default.svc.cluster.local:9080/productpage

Service: istio-ingressgateway | Duration: 42.09ms | Start Time: 0ms

Tags

- component: proxy
- downstream_cluster: -
- error: true
- guid:x-request-id: b6420793-5e13-98fb-9b64-77a39402e761
- http.method: GET
- http.protocol: HTTP/1.1
- http.status_code: 503
- http.url: http://192.168.64.17:30421/productpage
- internal.span.format: zipkin
- istio.canonical_revision: latest
- istio.canonical_service: istio-ingressgateway
- istio.mesh_id: cluster.local
- istio.namespace: istio-system
- node_id: router-172.17.0.4-istio-ingressgateway-8657768d87-fgc2z.istio-system-istio-system.svc.cluster.local
- peer.address: 172.17.0.1

Process

- ip: 172.17.0.4

SpanID: 5baf9352b9dc8891



{KODE}{KLOUD

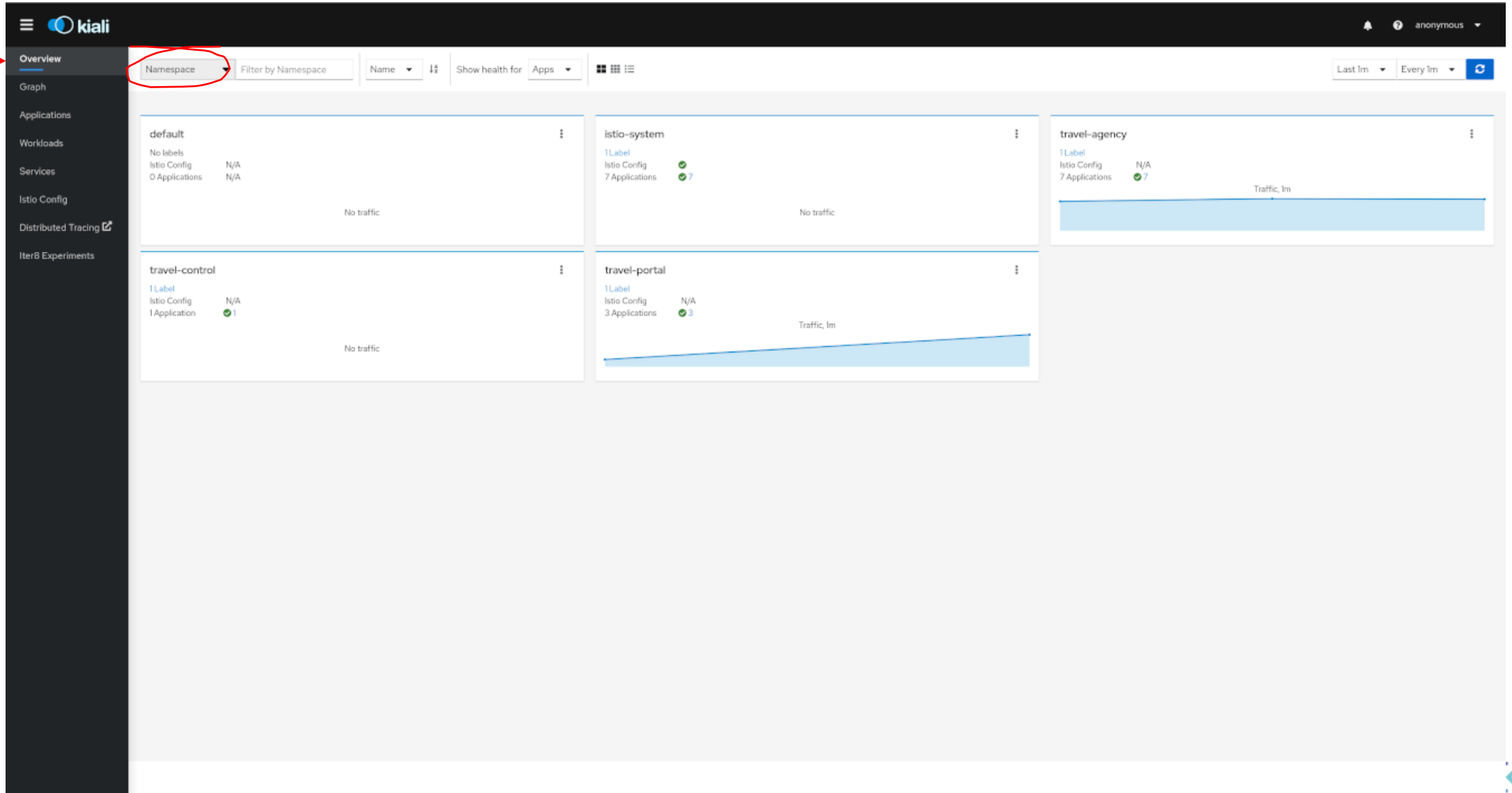
KIALI IN DETAIL



Kiali in Detail



Overview



The screenshot shows the Kiali Overview page. On the left is a dark sidebar with navigation options: Overview, Graph, Applications, Workloads, Services, Istio Config, Distributed Tracing, and Iter8 Experiments. A red arrow points to the 'Overview' menu item. The main content area has a top navigation bar with a 'Namespace' dropdown menu (circled in red), a 'Filter by Namespace' input, a 'Name' dropdown, a 'Show health for' dropdown set to 'Apps', and view toggles for 'Last 1m' and 'Every 1m'. Below this are five namespace cards: 'default', 'istio-system', 'travel-agency', 'travel-control', and 'travel-portal'. Each card displays metrics for labels, Istio Config, and Applications, along with a traffic graph. The 'travel-agency' and 'travel-portal' cards show traffic graphs with a blue area under a line, while the others show 'No traffic'.

Namespace	Labels	Istio Config	Applications	Traffic
default	No labels	N/A	0 Applications	No traffic
istio-system	1 Label	✓	7 Applications	No traffic
travel-agency	1 Label	N/A	7 Applications	Traffic, 1m
travel-control	1 Label	N/A	1 Application	No traffic
travel-portal	1 Label	N/A	3 Applications	Traffic, 1m

Graph

Jul 29, 05:58:24 PM .. 05:59:24 PM

istio-ingressgateway latest (istio-system)

productpage

details

reviews

ratings

mysql

Namespace: default | Versioned app graph

Display Find... Hide...

Last 1m Every 1m

NS default

Current Graph:
6 apps (9 versions)
5 services
14 edges

Incoming	Outgoing	Total
HTTP (requests per second):		
Total	%Success	%Error
0.09	100.00	0.00

0 25 50 75 100

OK 3xx 4xx 5xx

Legend

>_

```
$ kubectl delete service/details
```

```
service "details" deleted
```

Graph

The screenshot displays the Kiali Graph interface. On the left, a sidebar menu has the 'Graph' option highlighted with a red arrow. The main area shows a service mesh topology with nodes for 'istio-ingressgateway latest (istio-system)', 'productpage v1', 'reviews v1, v2, v3', 'ratings v1, v2-mysql', and 'mysql v1'. A red circle highlights the 'productpage v1' node and its connection to 'details.default.svc.cluster.local'. Another red circle highlights the 'details.default.svc.cluster.local' node. A third red circle highlights the 'health' status indicator in the right-hand panel. The right-hand panel shows a 'Degraded' status for 'productpage-v1: 1/1' with an 'Error Rate over 1m' of 18.89% for outbound traffic. Below this, there is a table for HTTP requests per second and a bar chart showing traffic distribution.

Namespace: default | Versioned app graph

Display Find... Hide...

Jul 29, 06:14:48 PM ... 06:15:48 PM

istio-ingressgateway latest (istio-system)

productpage v1

reviews v1 v2 v3

ratings v1 v2-mysql

mysql v1

details.default.svc.cluster.local

Degraded

Pod Status

productpage-v1: 1/1

health

Error Rate over 1m

Inbound: 0.00%

Outbound: 18.89%

Last 1m Every 1m

HTTP (requests per second):

	Total	%Success	%Error
In	0.13	100.00	0.00
Out	0.22	68.18	31.82

Out In

0 25 50 75 100

OK 3x 4xx 5xx

HTTP - Inbound Request Traffic min / max: RPS: 0.13 / 0.13, %Error 0.00 / 0.00

HTTP - Outbound Request Traffic min / max: RPS: 0.20 / 0.27, %Error 0.00 / 0.00

No gRPC traffic logged.

```
> _
```

```
$ kubectl apply -f  
samples/bookinfo/platform/kube/bookinfo.yaml
```

```
service/details created  
serviceaccount/bookinfo-details unchanged  
deployment.apps/details-v1 unchanged  
service/ratings unchanged  
serviceaccount/bookinfo-ratings unchanged  
deployment.apps/ratings-v1 unchanged  
service/reviews unchanged  
serviceaccount/bookinfo-reviews unchanged  
deployment.apps/reviews-v1 unchanged  
deployment.apps/reviews-v2 unchanged  
deployment.apps/reviews-v3 unchanged  
service/productpage unchanged  
serviceaccount/bookinfo-productpage unchanged  
deployment.apps/productpage-v1 unchanged
```

Graph

Namespace: default | Versioned app graph

Display Find... Hide...

Jul 29, 06:14:48 PM ... 06:15:48 PM

istio-ingressgateway latest (istio-system)

productpage v1

reviews v1 v2 v3

ratings v1 v2-mysql

mysql v1

details v1

details.default.svc.cluster.local

Degraded

Pod Status

productpage-v1: 1 / 1

health

Error Rate over 1m

Inbound: 0.00%

Outbound: 18.89%

Last 1m Every 1m

HTTP (requests per second):

	Total	%Success	%Error
In	0.13	100.00	0.00
Out	0.22	68.18	31.82

Out: In: 0 25 50 75 100

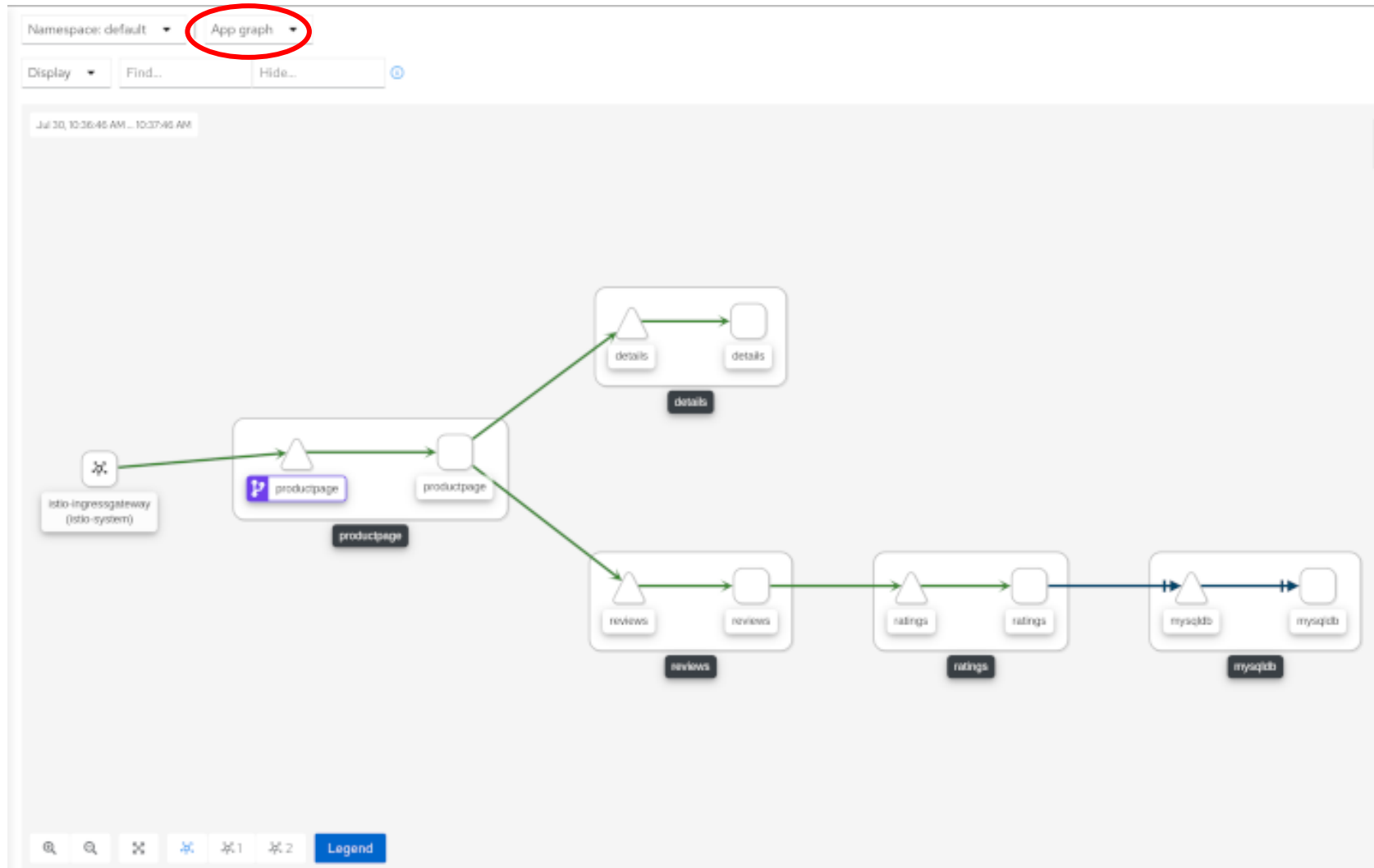
OK 3x 4xx 5xx

HTTP - Inbound Request Traffic min / max: RPS: 0.13 / 0.13, %Error 0.00 / 0.00

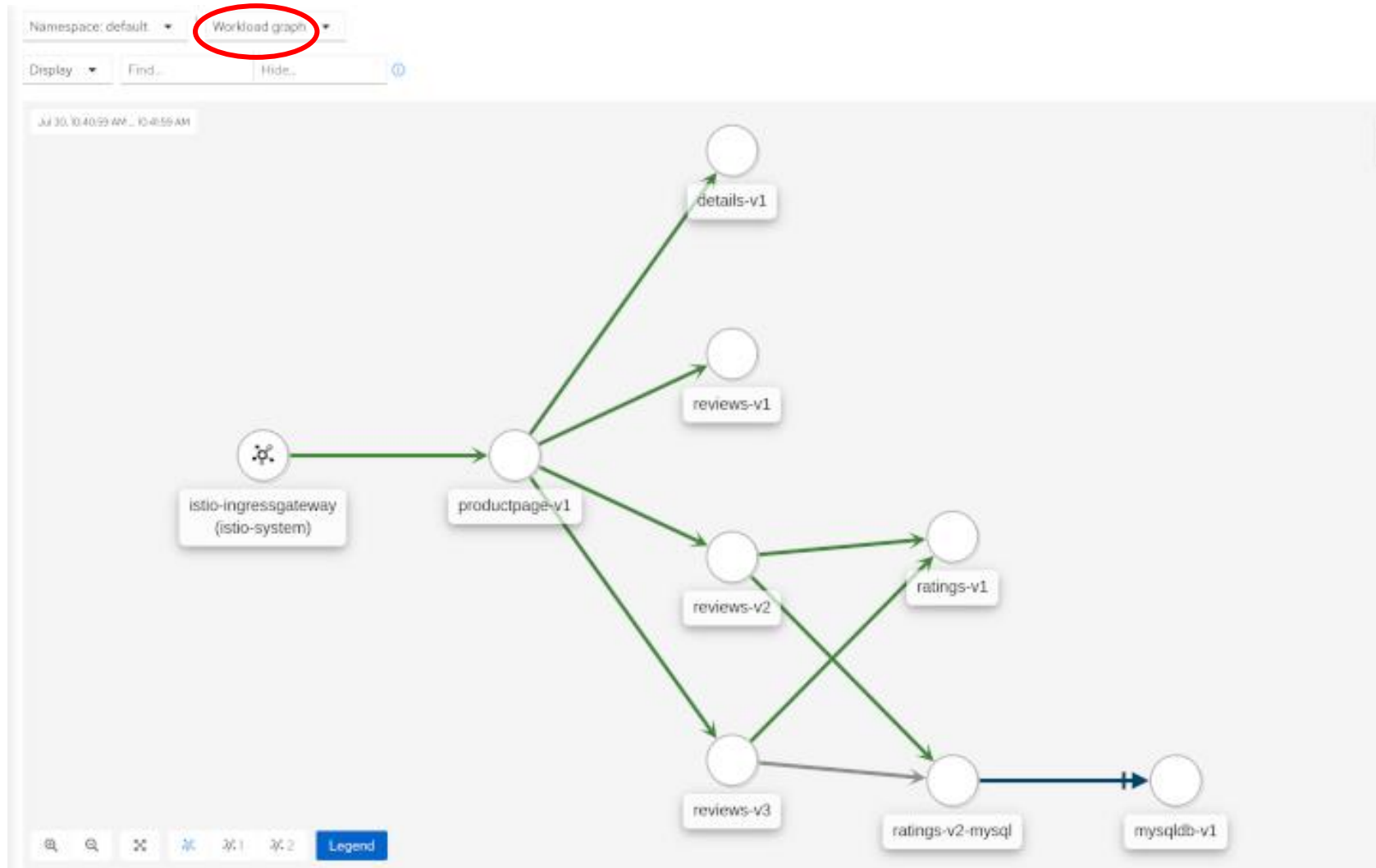
HTTP - Outbound Request Traffic min / max: RPS: 0.20 / 0.27, %Error 0.00 / 0.00

No gRPC traffic logged.

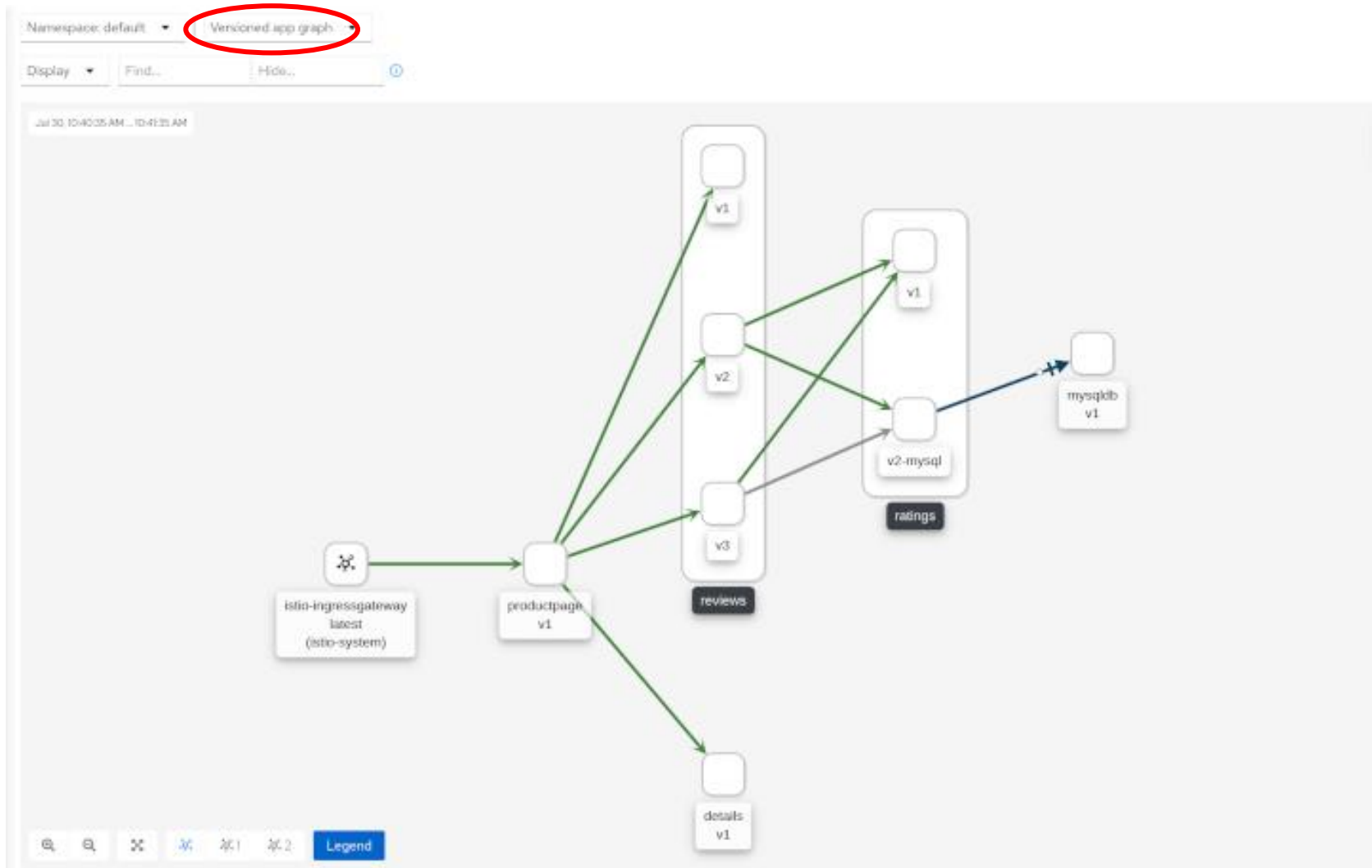
The App Graph



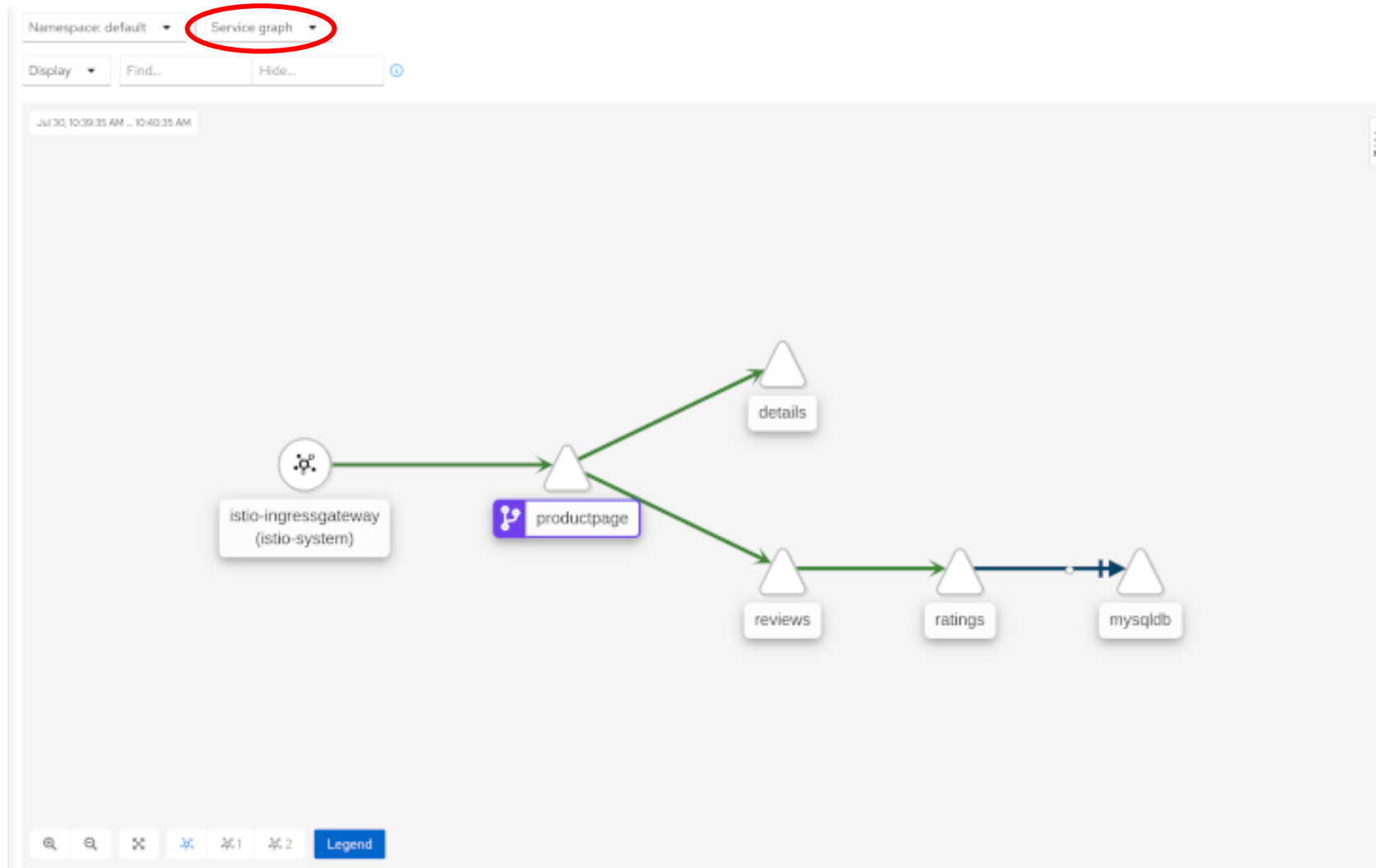
The Workload Graph



The Versioned App Graph



The Service Graph



Replay An Issue Back in Time

The screenshot displays the Kiali application interface. On the left, a navigation sidebar is visible with the 'Graph' option selected and highlighted by a red arrow. The main area shows a service graph for the namespace 'default'. The graph includes components like 'istio-ingressgateway', 'productpage', 'reviews', 'ratings', and 'mysqldb', each with its own versioned sub-graph. A red circle highlights the 'List 1m' button in the top right corner of the sidebar, which is used for replaying issues.

Namespace: default | Versioned app graph

Display | Find... | Hide...

Jul 29, 05:58:24 PM .. 05:59:24 PM

istio-ingressgateway latest (istio-system)

productpage

reviews

ratings

mysqldb

Legend

Graph tour

List 1m | Every 1m

NS default

Current Graph:
6 apps (9 versions)
5 services
14 edges

Incoming	Outgoing	Total
HTTP (requests per second):		
Total	%Success	%Error
0.09	100.00	0.00

0 25 50 75 100

OK 3xx 4xx 5xx

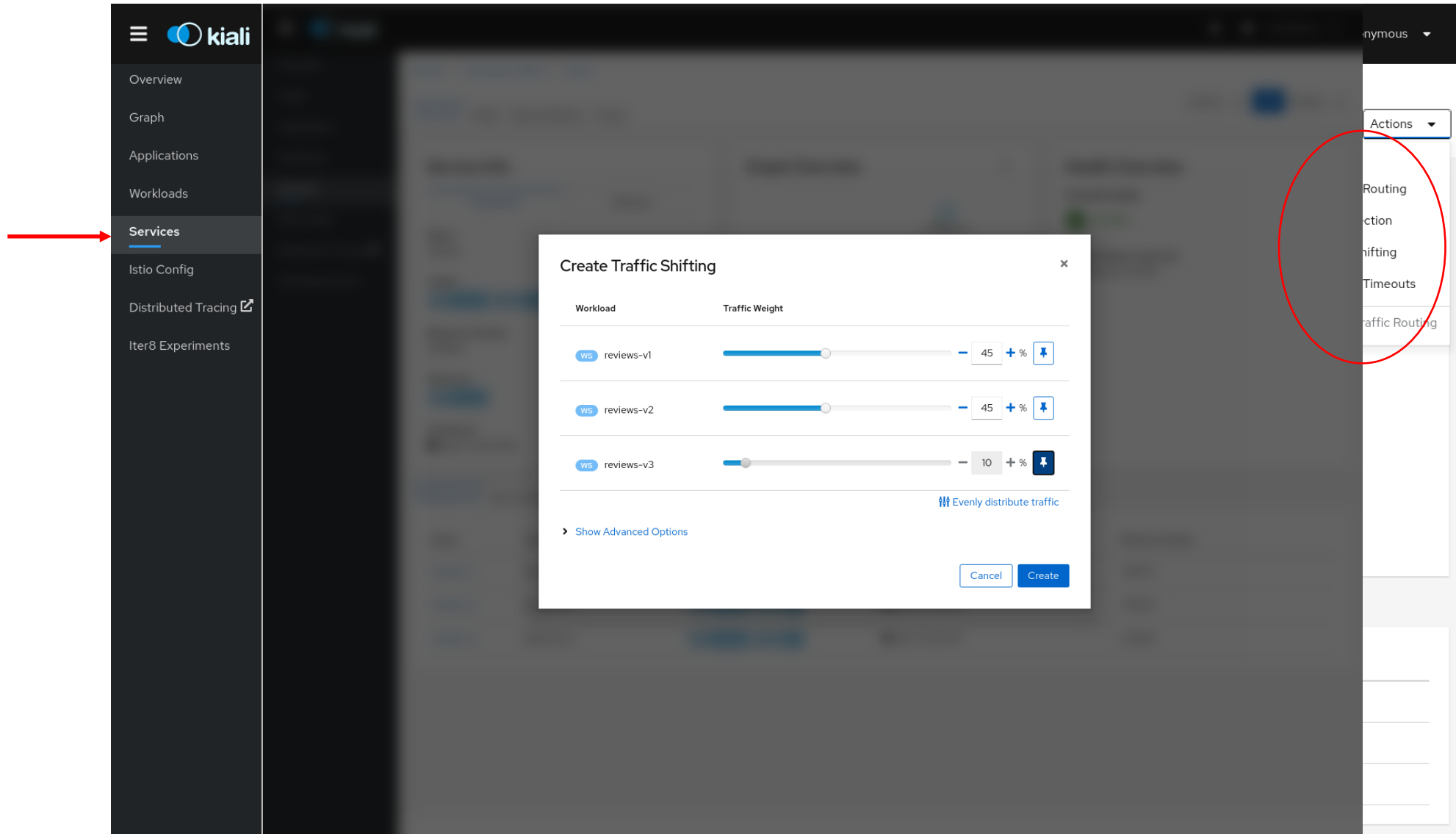
Applications & Workloads & Services

The screenshot displays the Kiali web interface. On the left is a navigation sidebar with options: Overview, Graph, Applications, Workloads (selected), Services, Istio Config, Distributed Tracing, and Istio Experiments. The main content area shows the 'Workloads' view for the 'default' namespace, specifically for the 'productpage-v1' workload. The interface includes tabs for Overview, Traffic, Logs, Inbound Metrics, and Outbound Metrics. The 'Logs' tab is active, showing a list of log entries for the pod 'productpage-v1-7f4cc988c6-8hm98' in the 'productpage-v1' container. The logs are displayed in two columns: 'productpage-v1' and 'Istio proxy (sidecar)'. The logs show a sequence of HTTP requests and responses, including headers like 'content-type: application/json', 'date: Thu, 30 Jul 2020 11:16:32 GMT', and 'x-envoy-upstream-service-time: 3'. The 'Istio proxy' logs show the corresponding proxy actions, such as 'GET /productpage HTTP/1.1' and 'GET /reviews/0 HTTP/1.1'. The interface also features a 'Side by Side' toggle, a 'Last 500 lines' dropdown, and a search bar.

The screenshot shows the Kiali web interface for configuring Istio. The left sidebar has a red arrow pointing to the 'Istio Config' menu item. The main content area displays the configuration for a VirtualService named 'reviews' in the 'default' namespace. The configuration is shown in a code editor with line numbers 1 through 30. The configuration includes metadata, a selflink, and a spec with three destinations. The first destination is highlighted in orange and has a warning icon. The second destination is also highlighted in orange and has a warning icon. The third destination is not highlighted. The right sidebar shows 'Validation references' with a link to 'default/bookinfo'. At the bottom of the code editor are 'Save', 'Reload', and 'Cancel' buttons.

```
1 kind: VirtualService
2 apiVersion: networking.istio.io/v1alpha3
3 metadata:
4   name: reviews
5   namespace: default
6   selfLink: >-
7     /apis/networking.istio.io/v1alpha3/namespaces/default/virtualservices/reviews
8   uid: ac58e595-9bd6-44ef-971e-2ade2d3bc323
9   resourceVersion: '4325'
10  generation: 2
11  creationTimestamp: '2020-07-31T08:03:20Z'
12  labels:
13    kiali_wizard: weighted_routing
14  spec:
15    hosts:
16      - reviews.default.svc.cluster.local
17    http:
18      - route:
19          - destination:
20              host: reviews.default.svc.cluster.local
21              subset: v1
22              weight: 72
23          - destination:
24              host: reviews.default.svc.cluster.local
25              subset: v22
26              weight: 28
27          - destination:
28              host: reviews.default.svc.cluster.local
29              subset: v3
30
```

Istio Wizards



The screenshot displays the Kiali web interface. On the left, a dark sidebar contains a navigation menu with the following items: Overview, Graph, Applications, Workloads, **Services** (highlighted with a red arrow), Istio Config, Distributed Tracing, and Iter8 Experiments. The main content area is dimmed, showing a 'Create Traffic Shifting' wizard dialog box. The dialog has a title bar with a close button (X) and contains the following elements:

Workload	Traffic Weight
ws reviews-v1	45 %
ws reviews-v2	45 %
ws reviews-v3	10 %

Below the table, there is a checkbox labeled 'Evenly distribute traffic' which is currently checked. At the bottom of the dialog are 'Cancel' and 'Create' buttons. On the right side of the interface, a dropdown menu is open, showing options: Routing, Action, **Traffic Shifting** (circled in red), Timeouts, and Traffic Routing. The user's name 'Anonymous' is visible in the top right corner.



{KODE}{KLOUD

A QUICK NOTE ON SERVICE MESH INTERFACE



Service Mesh Interface

Service
Mesh
Interface

[Specification](#) [Ecosystem](#) [Blog](#) [Slack](#) [Twitter](#) [GitHub](#)



A standard interface for service meshes on Kubernetes.

Service Mesh Interface provides:

- A standard interface for service meshes on Kubernetes
- A basic feature set for the most common service mesh use cases
- Flexibility to support new service mesh capabilities over time
- Space for the ecosystem to innovate with service mesh technology

[View the Spec](#)

Service Mesh Interface



NGINX Service Mesh

In partnership with



<https://github.com/servicemeshinterface/smi-spec>



{KODE}{KLOUD

CONCLUSION





Thank You!



{KODE}{KLOUD