Simplify Istio for your R&D

How all devs use Istio Security without knowing Istio

About

Isan Rivkin

- Production Engineer @ SimilarWeb
- K8s, Rust, Go & Distributed systems

isan-rivkin

isan_rivkin

About

Isan Rivkin

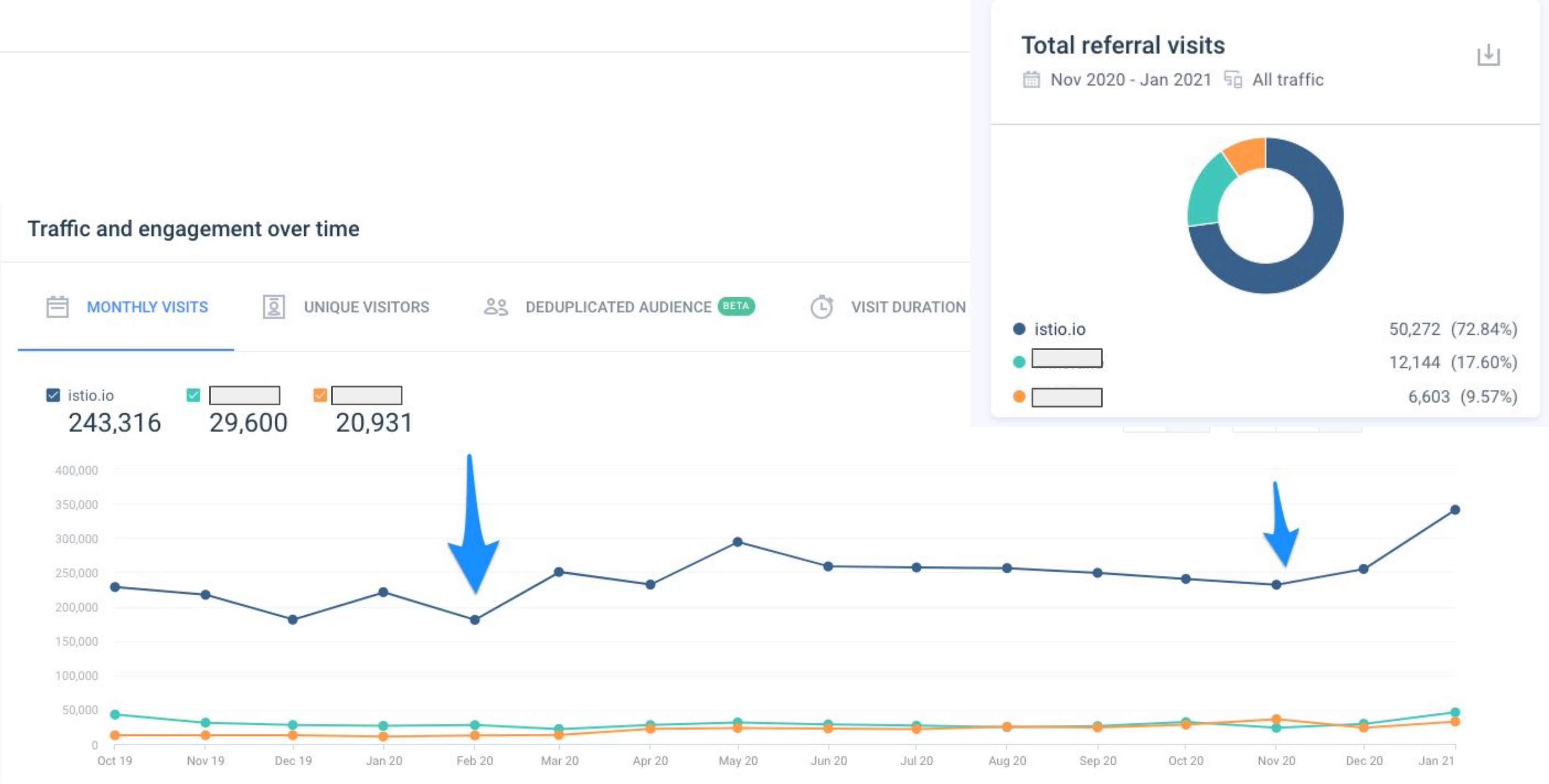
- Production Engineer @ SimilarWeb
- K8s, Rust, Go & Distributed systems

isan-rivkin

isan_rivkin

similarweb.com

- Data analytics
- Micro services
- Nomad -> AWS EKS
- Active-Active Multi cluster
- 100K ~ RP/s, 10 Petabyte
- similarweb



Total referral visits

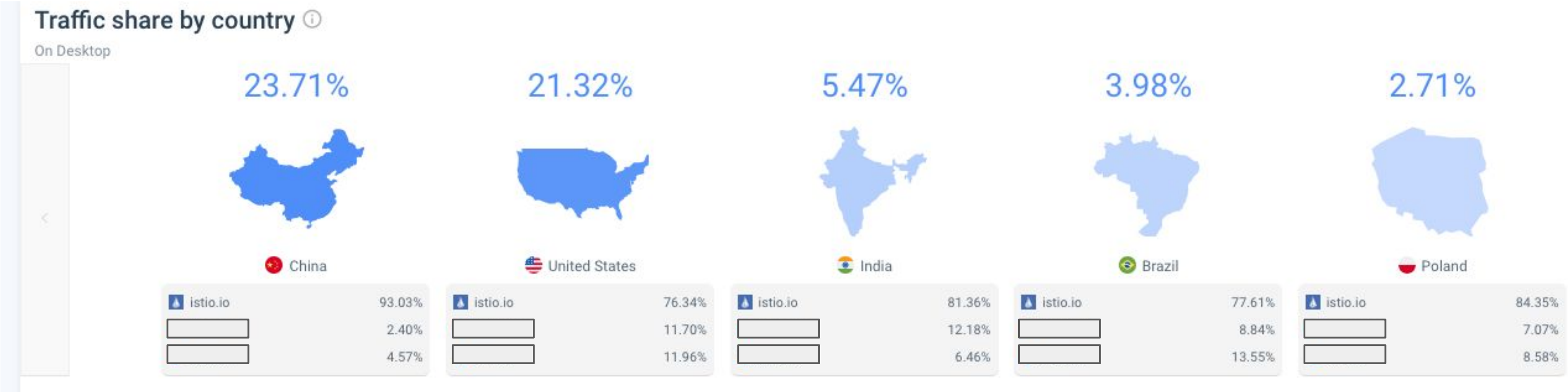
Nov 2020 - Jan 2021 All traffic

● istio.io	50,272	(72.84%)
● [redacted]	12,144	(17.60%)
● [redacted]	6,603	(9.57%)

Traffic and engagement over time

MONTHLY VISITS UNIQUE VISITORS DEDUPLICATED AUDIENCE BETA VISIT DURATION

☑ istio.io	☑ [redacted]	☑ [redacted]
243,316	29,600	20,931



Traffic share by country ⓘ

On Desktop

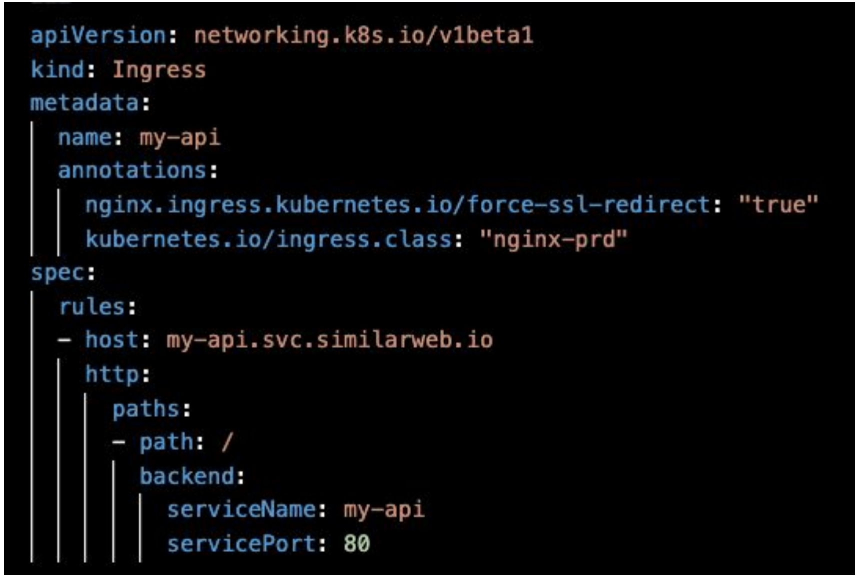
	China	United States	India	Brazil	Poland
	23.71%	21.32%	5.47%	3.98%	2.71%
istio.io	93.03%	76.34%	81.36%	77.61%	84.35%
	2.40%	11.70%	12.18%	8.84%	7.07%
	4.57%	11.96%	6.46%	13.55%	8.58%

Why Istio

- Traffic Access control for pods
- Network capabilities
- Visibility Distributed tracing
- All in one!

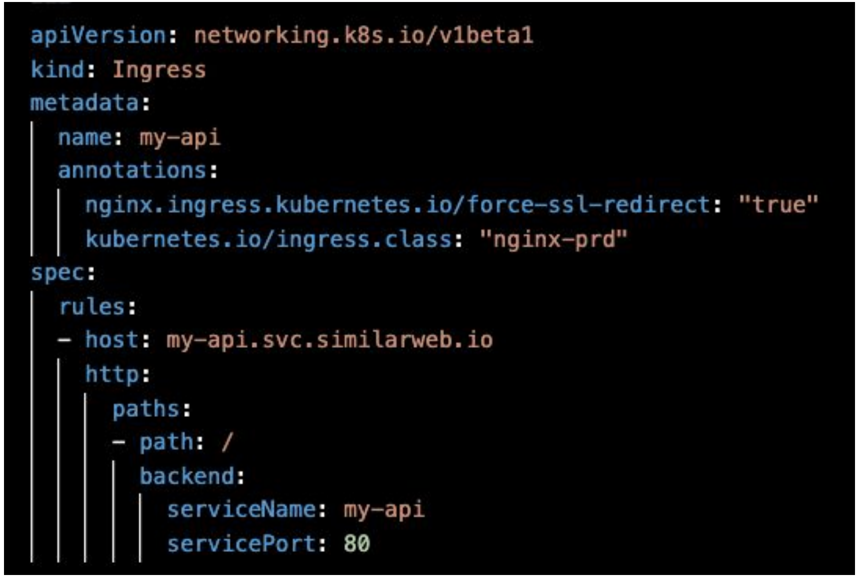
The Problem

Nginx was simple!



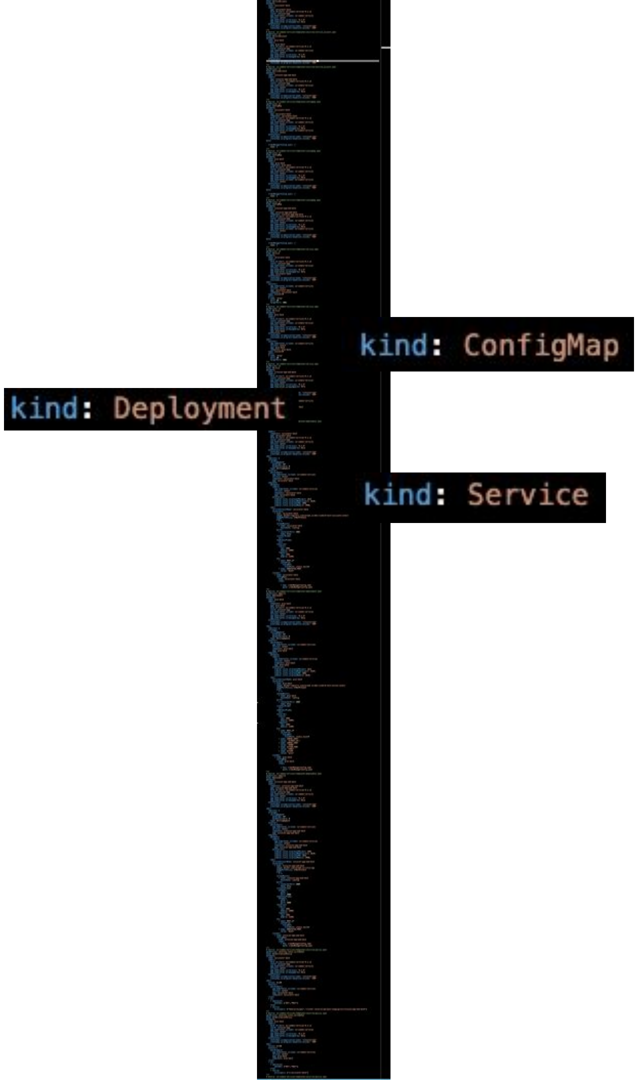
```yaml
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
  name: my-api
  annotations:
    nginx.ingress.kubernetes.io/force-ssl-redirect: "true"
    kubernetes.io/ingress.class: "nginx-prd"
spec:
  rules:
  - host: my-api.svc.similarweb.io
    http:
      paths:
      - path: /
        backend:
          serviceName: my-api
          servicePort: 80
```

Nginx was simple!



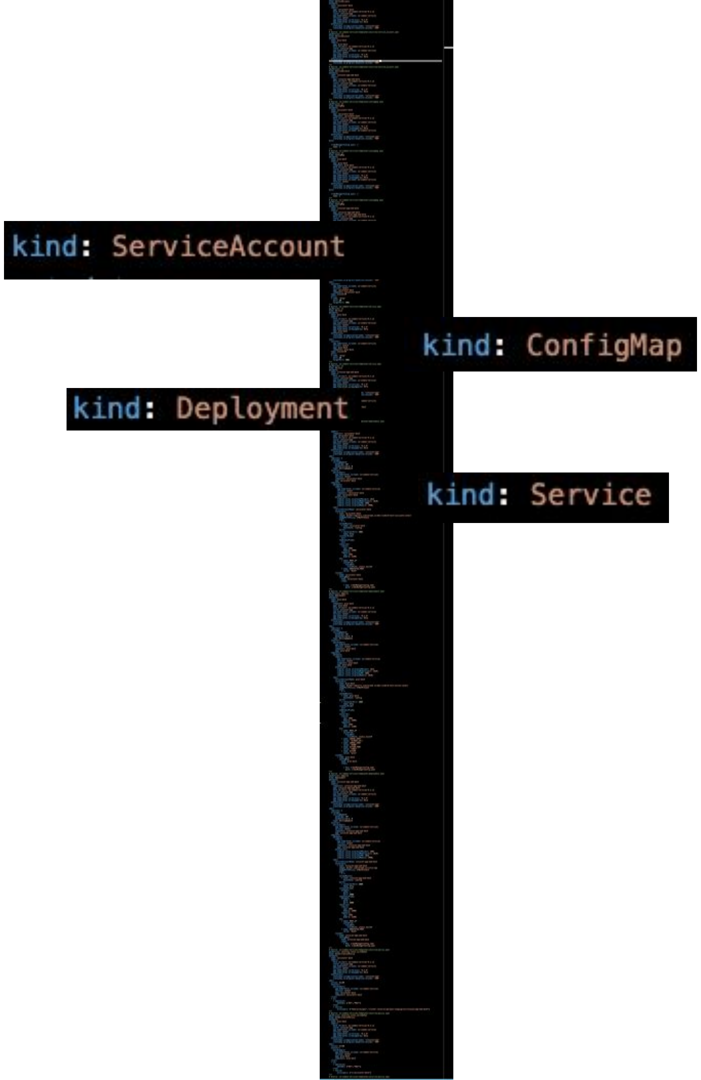
```yaml
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
  name: my-api
  annotations:
    nginx.ingress.kubernetes.io/force-ssl-redirect: "true"
    kubernetes.io/ingress.class: "nginx-prd"
spec:
  rules:
  - host: my-api.svc.similarweb.io
    http:
      paths:
      - path: /
        backend:
          serviceName: my-api
          servicePort: 80
```

Istio deployment



```
kind: ConfigMap
kind: Deployment
kind: Service
```

Istio deployment



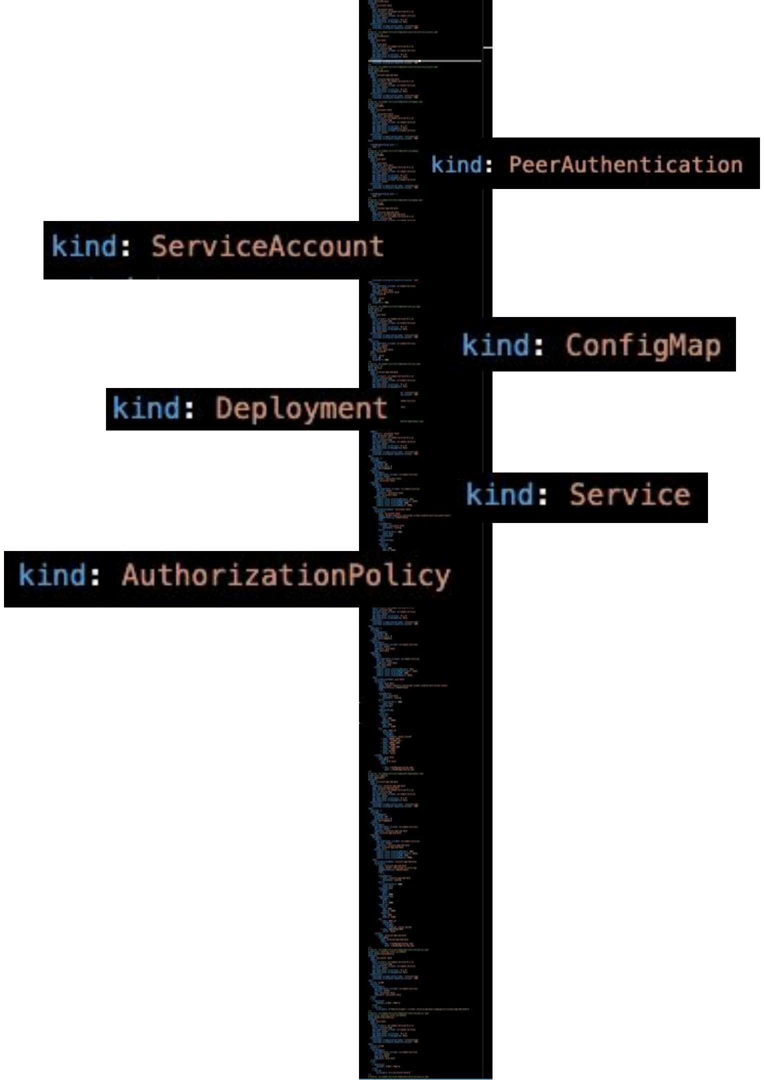
```
kind: ServiceAccount
```

```
kind: ConfigMap
```

```
kind: Deployment
```

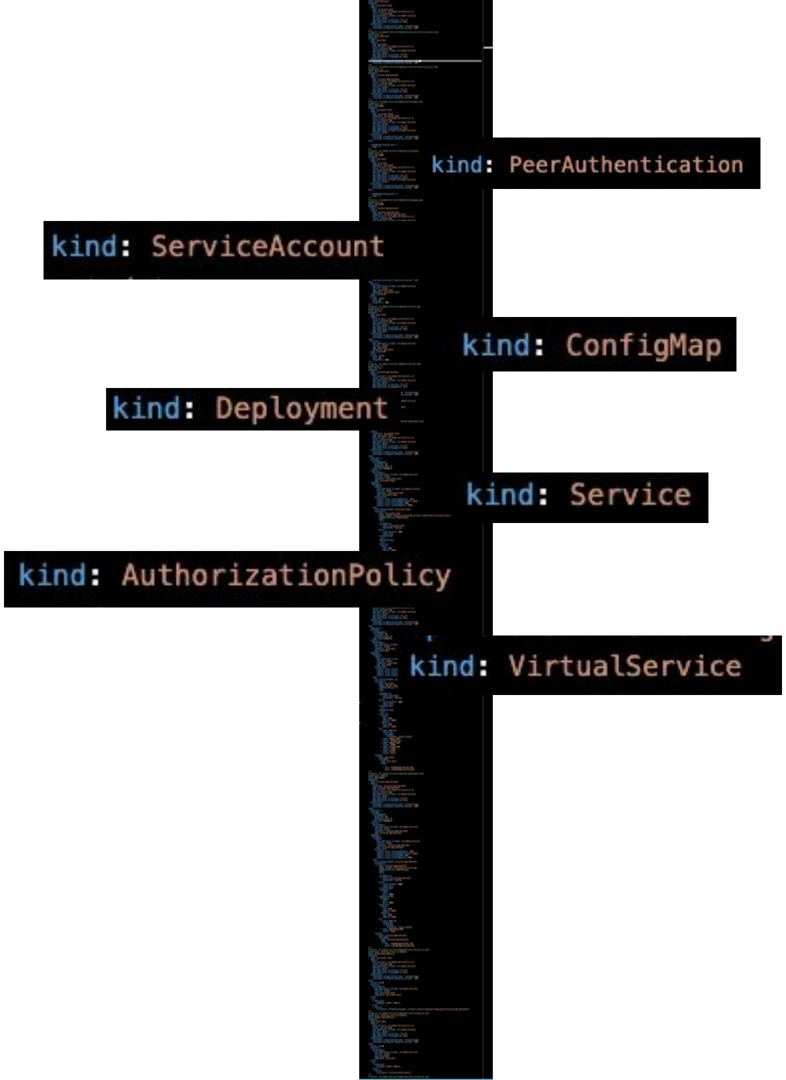
```
kind: Service
```

Istio deployment



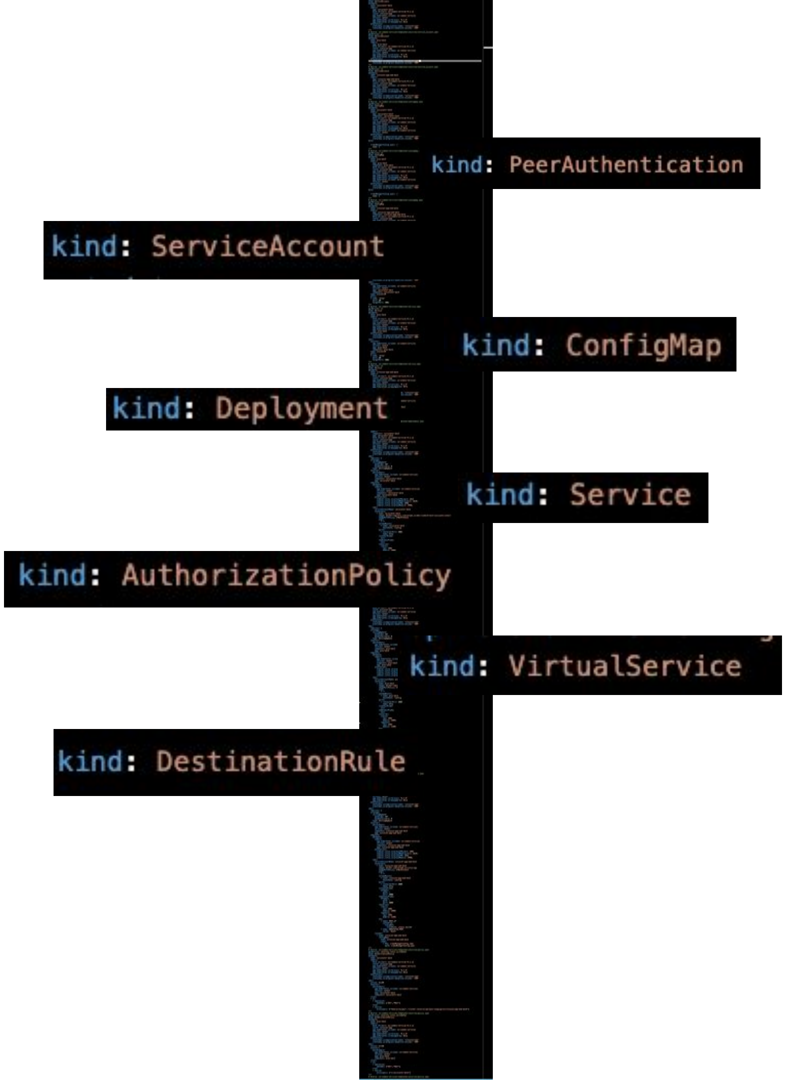
```
kind: PeerAuthentication
kind: ServiceAccount
kind: ConfigMap
kind: Deployment
kind: Service
kind: AuthorizationPolicy
```

Istio deployment



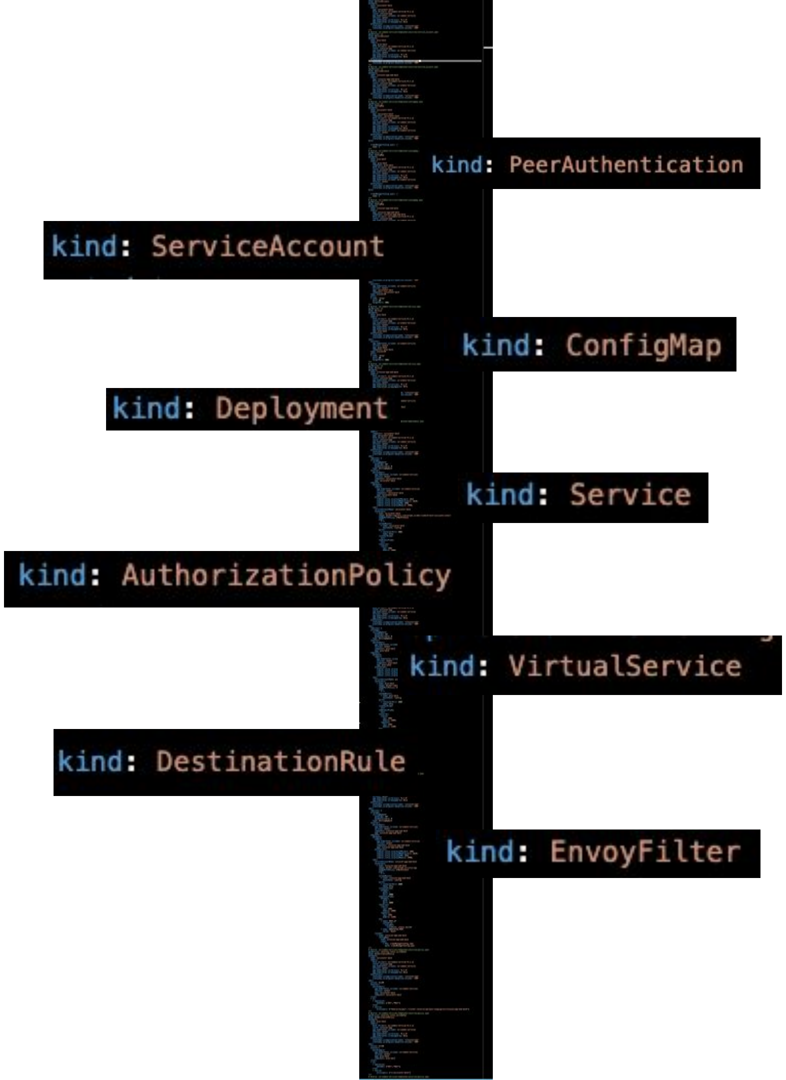
```
kind: PeerAuthentication
kind: ServiceAccount
kind: ConfigMap
kind: Deployment
kind: Service
kind: AuthorizationPolicy
kind: VirtualService
```

Istio deployment



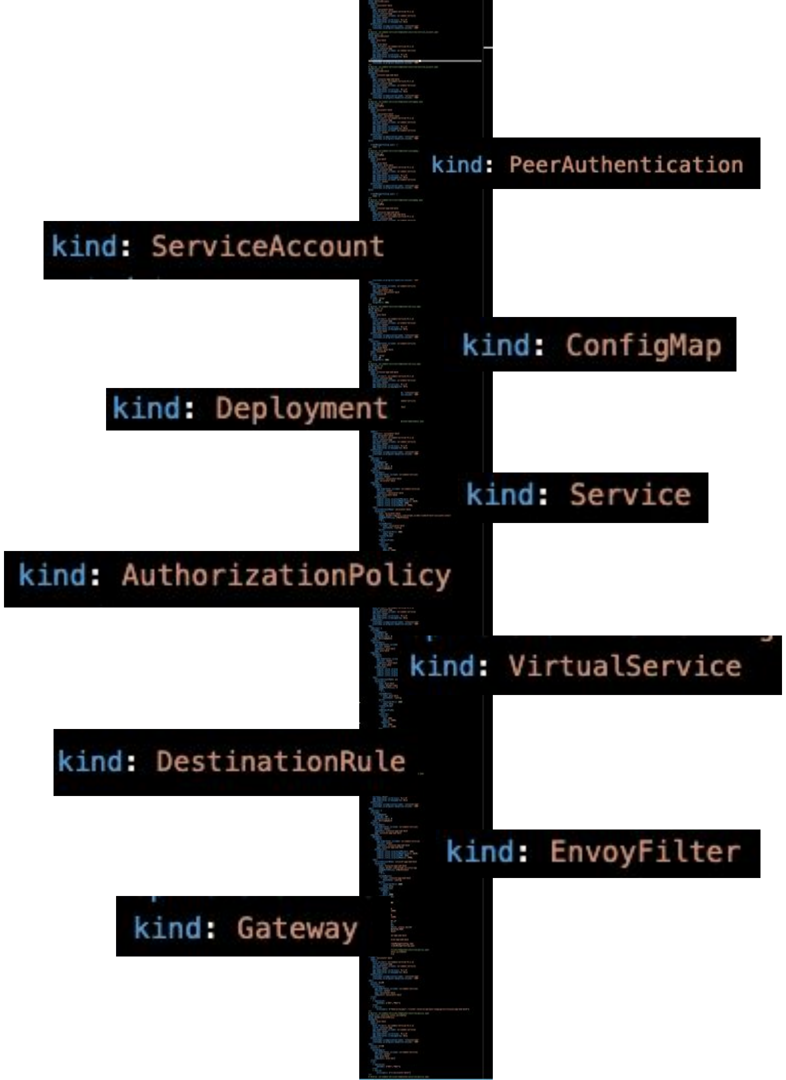
```
kind: PeerAuthentication
kind: ServiceAccount
kind: ConfigMap
kind: Deployment
kind: Service
kind: AuthorizationPolicy
kind: VirtualService
kind: DestinationRule
```

Istio deployment



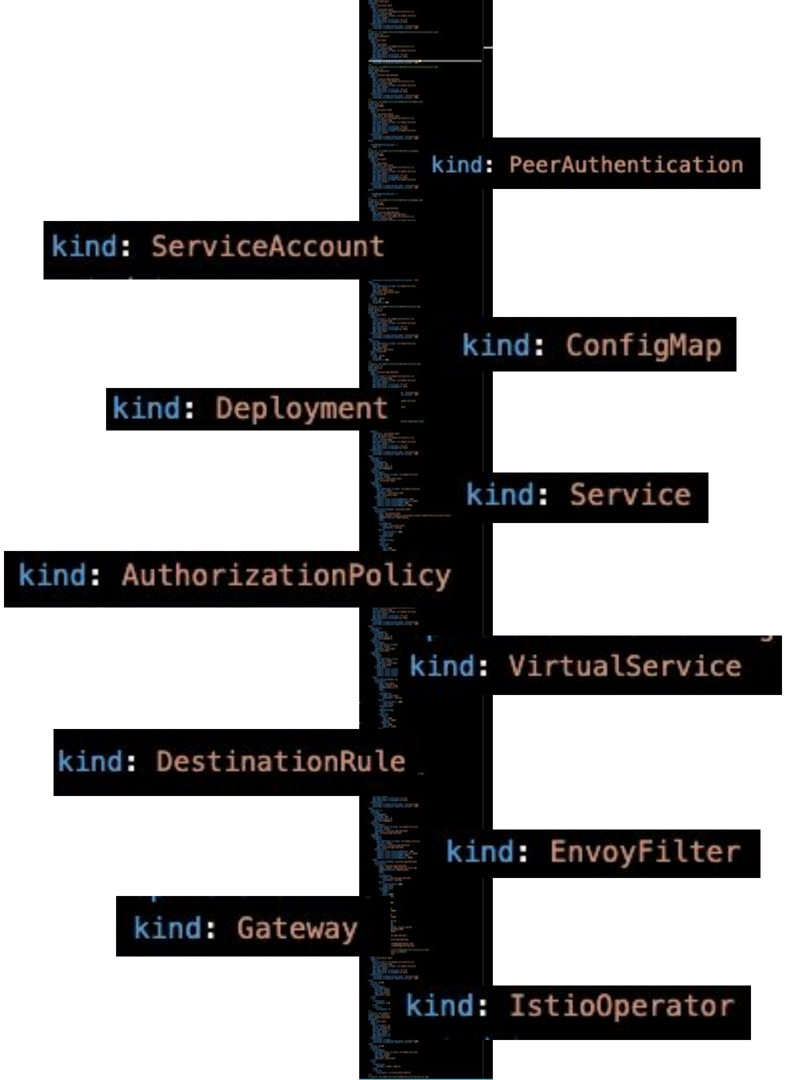
```
kind: PeerAuthentication
kind: ServiceAccount
kind: ConfigMap
kind: Deployment
kind: Service
kind: AuthorizationPolicy
kind: VirtualService
kind: DestinationRule
kind: EnvoyFilter
```

Istio deployment



```
kind: PeerAuthentication
kind: ServiceAccount
kind: ConfigMap
kind: Deployment
kind: Service
kind: AuthorizationPolicy
kind: VirtualService
kind: DestinationRule
kind: EnvoyFilter
kind: Gateway
```

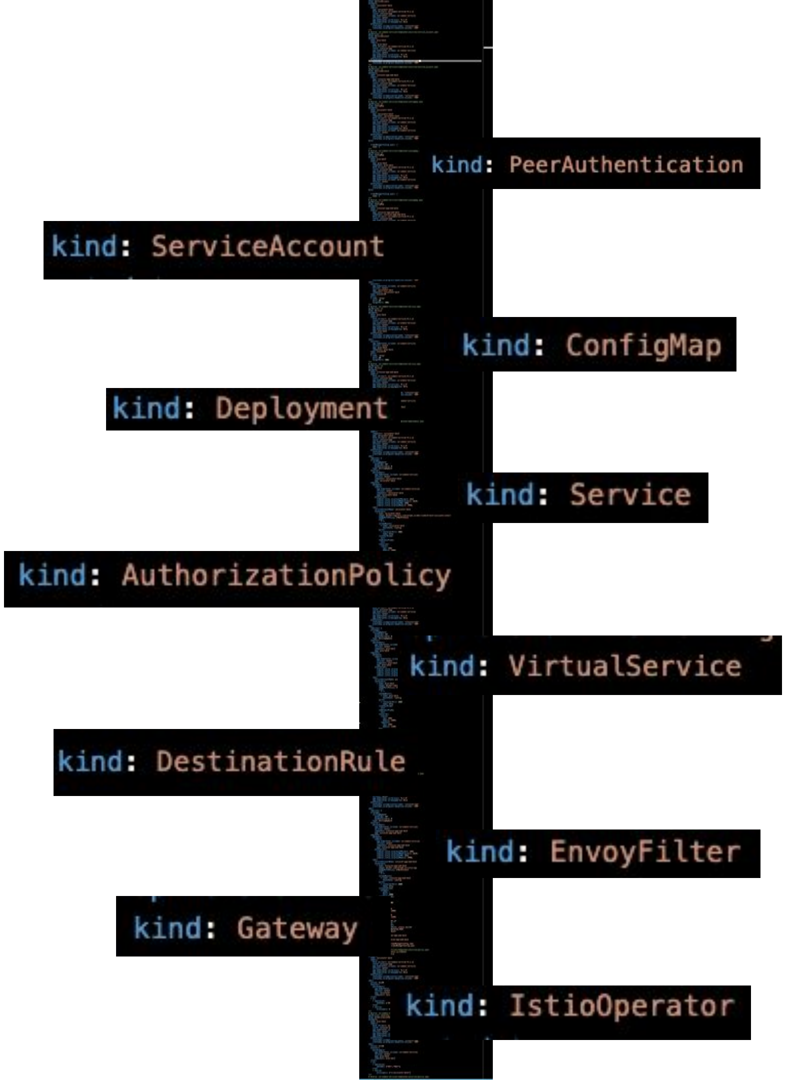
Istio deployment



```
kind: PeerAuthentication
kind: ServiceAccount
kind: ConfigMap
kind: Deployment
kind: Service
kind: AuthorizationPolicy
kind: VirtualService
kind: DestinationRule
kind: EnvoyFilter
kind: Gateway
kind: IstioOperator
```

Challenges

- Learning Curve
- Prevent Copy-Paste
- Security
- Ingress routing
- Visibility
- Rapid development



```
kind: PeerAuthentication
kind: ServiceAccount
kind: ConfigMap
kind: Deployment
kind: Service
kind: AuthorizationPolicy
kind: VirtualService
kind: DestinationRule
kind: EnvoyFilter
kind: Gateway
kind: IstioOperator
```

YOU SAID ALL I
NEEDED WAS A YAML FILE
imgflip.com

Abstractions

Istio @ similarweb - Architecture

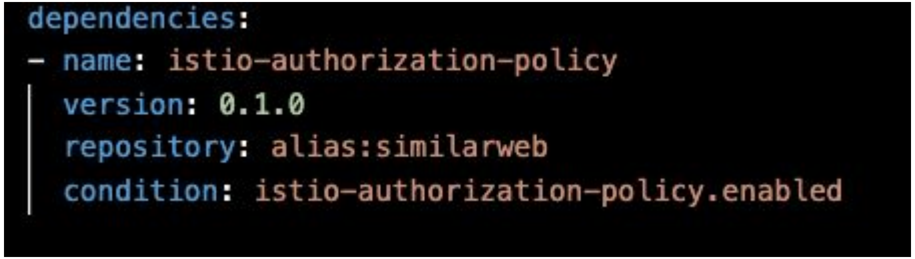
Istio @ similarweb - Architecture

Helm abstraction

- Building blocks - Helm dependencies
  - Istio Security Chart
  - Istio Ingress Network Chart

Helm abstraction

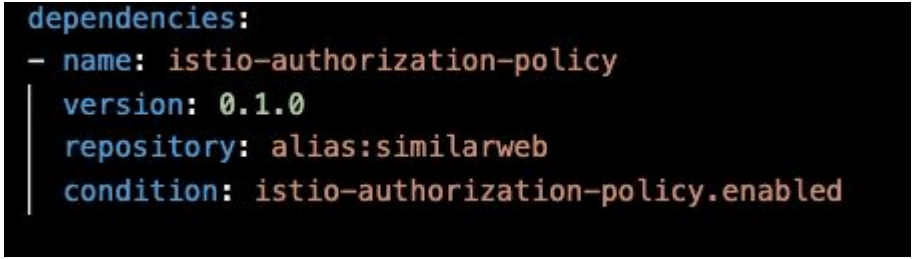
- Building blocks - Helm dependencies
  - Istio Security Chart
  - Istio Ingress Network Chart



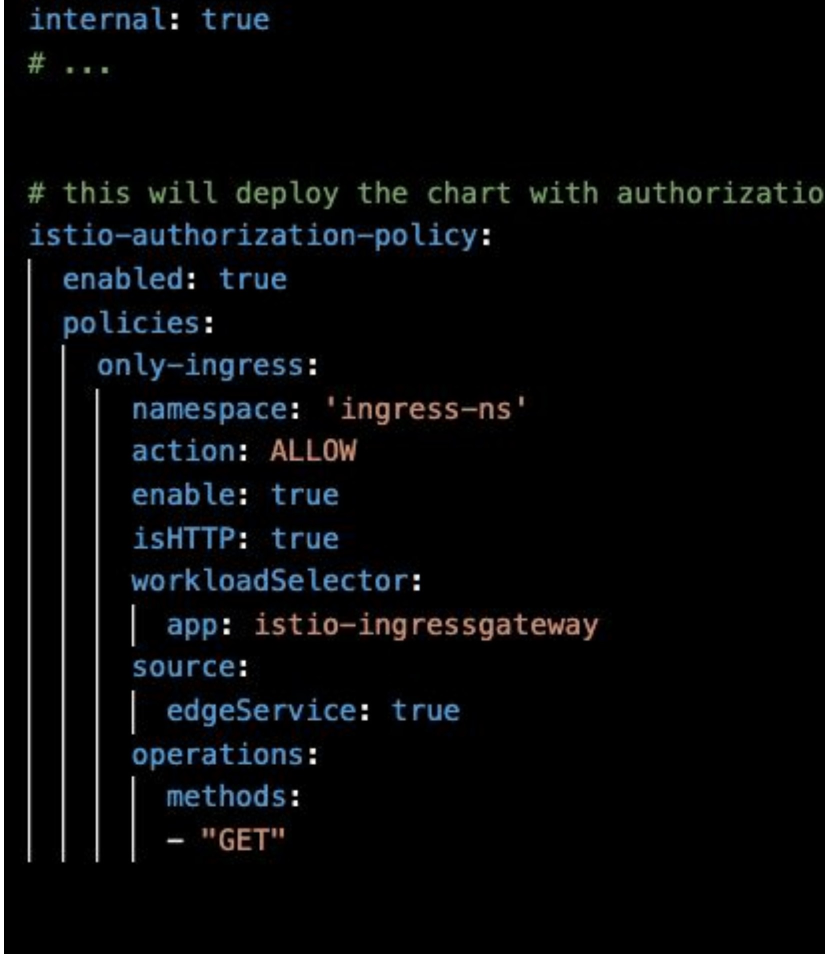
```yaml
dependencies:
- name: istio-authorization-policy
  version: 0.1.0
  repository: alias:similarweb
  condition: istio-authorization-policy.enabled
```

Helm abstraction

- Building blocks - Helm dependencies
  - Istio Security Chart
  - Istio Ingress Network Chart



```yaml
dependencies:
- name: istio-authorization-policy
  version: 0.1.0
  repository: alias:similarweb
  condition: istio-authorization-policy.enabled
```



```yaml
internal: true
# ...


# this will deploy the chart with authorizatio
istio-authorization-policy:
  enabled: true
  policies:
    only-ingress:
      namespace: 'ingress-ns'
      action: ALLOW
      enable: true
      isHTTP: true
      workloadSelector:
        app: istio-ingressgateway
      source:
        edgeService: true
      operations:
        methods:
        - "GET"
```

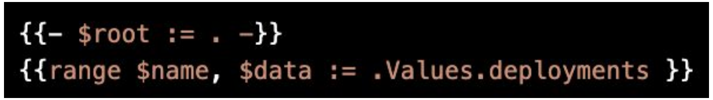
Helm abstraction

- Applicative Charts

Helm abstraction

- Application Charts
- sw-common-services
  - List of deployments

templates/deployment.yaml

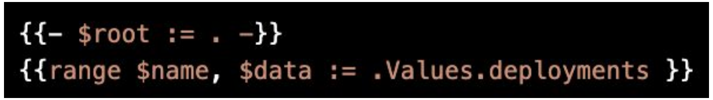


```
{{- $root := . -}}
{{range $name, $data := .Values.deployments }}
```

Helm abstraction

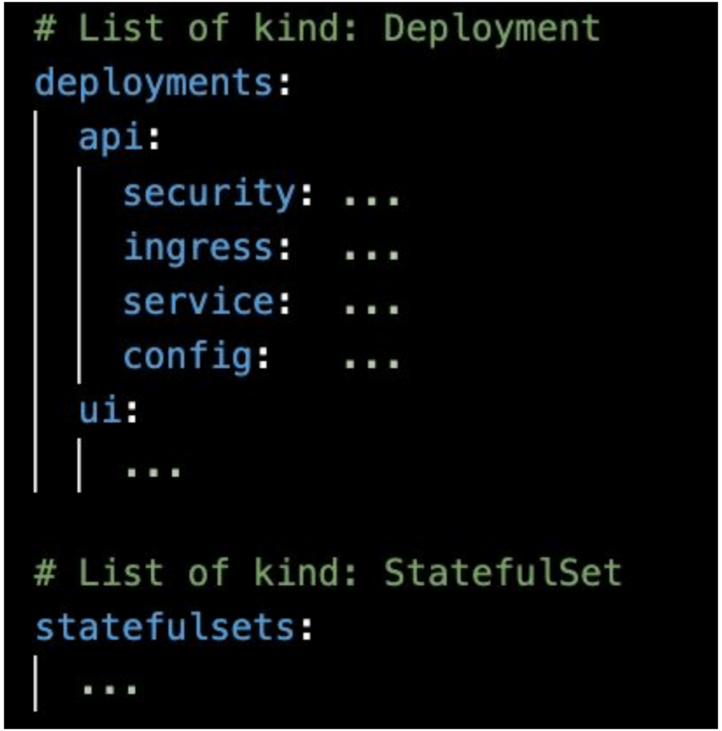
- Application Charts
- sw-common-services
    - List of deployments
    - Networking
    - Security
    - Upgrade strategy
    - Encapsulation

templates/deployment.yaml



```
{{- $root := . -}}
{{range $name, $data := .Values.deployments }}
```

values.yaml

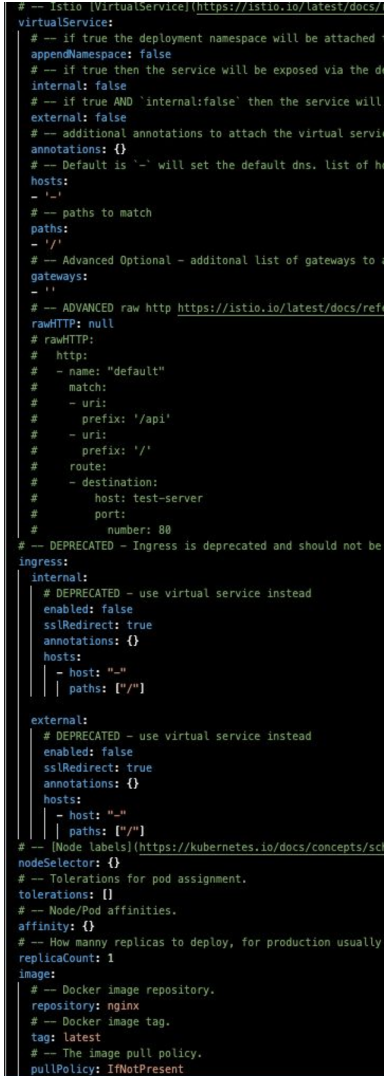


```
# List of kind: Deployment
deployments:
  api:
    security: ...
    ingress:  ...
    service:  ...
    config:   ...
  ui:
    ...

# List of kind: StatefulSet
statefulsets:
  ...
```

Helm abstraction

- Application Charts
- sw-common-services
  - List of deployments
  - Networking
  - Security
  - Upgrade strategy
  - Encapsulation
- values.yaml big and complex!



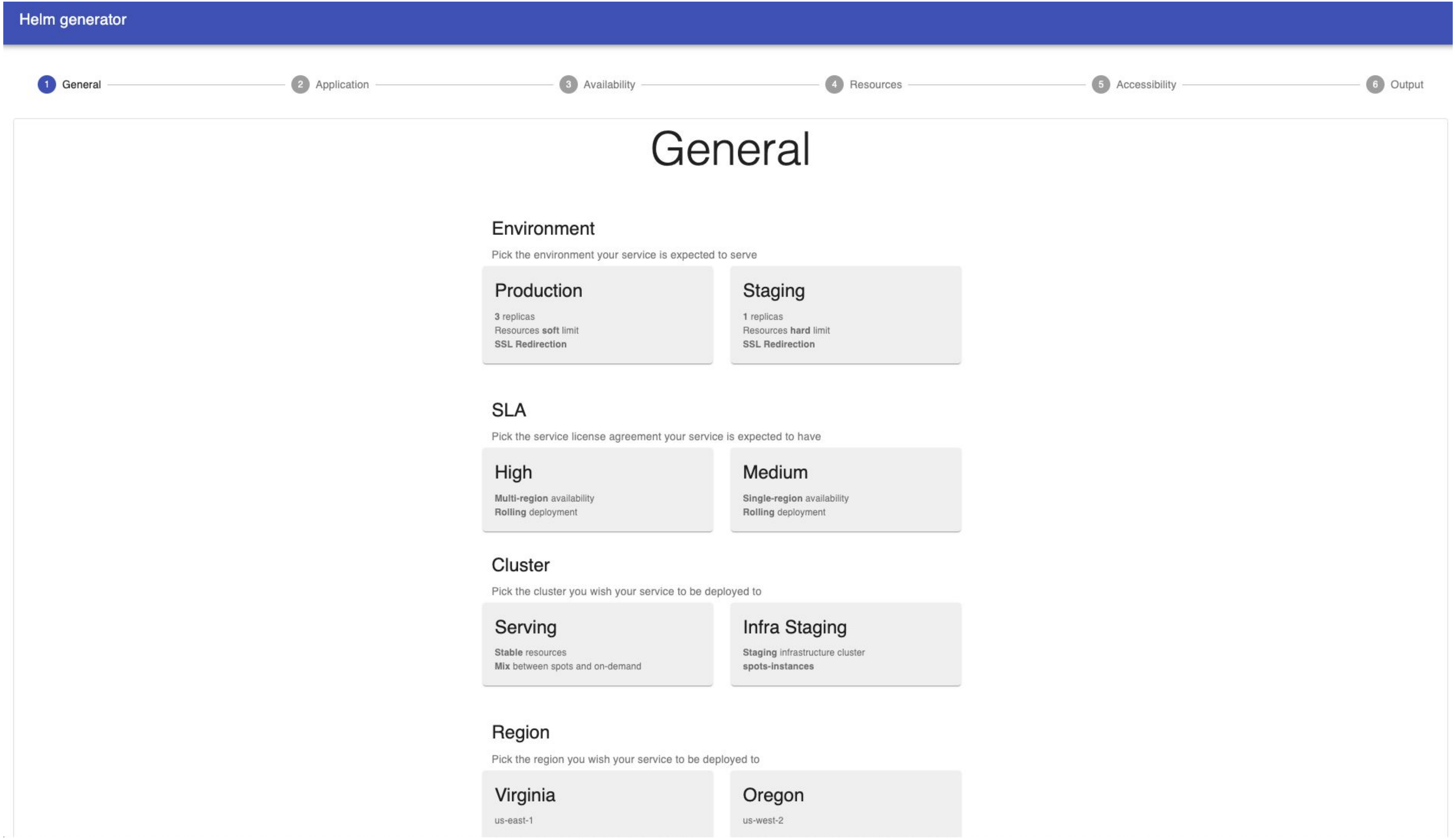
```
# -- Istio [VirtualService](https://istio.io/latest/docs/
virtualService:
  # -- if true the deployment namespace will be attached
  appendNamespace: false
  # -- if true then the service will be exposed via the de
  internal: false
  # -- if true AND `internal:false` then the service will
  external: false
  # -- additional annotations to attach the virtual servic
  annotations: {}
  # -- Default is `-` will set the default dns. list of ho
  hosts:
  - '-'
  # -- paths to match
  paths:
  - '/'
  # -- Advanced Optional - additonal list of gateways to a
  gateways:
  - ''
  # -- ADVANCED raw http https://istio.io/latest/docs/refe
  rawHTTP: null
  # rawHTTP:
  #   http:
  #   - name: "default"
  #     match:
  #     - uri:
  #         prefix: '/api'
  #     - uri:
  #         prefix: '/'
  #     route:
  #     - destination:
  #         host: test-server
  #         port:
  #           number: 80
# -- DEPRECATED - Ingress is deprecated and should not be
ingress:
  internal:
    # DEPRECATED - use virtual service instead
    enabled: false
    sslRedirect: true
    annotations: {}
    hosts:
      - host: "-"
        paths: ["/"]

  external:
    # DEPRECATED - use virtual service instead
    enabled: false
    sslRedirect: true
    annotations: {}
    hosts:
      - host: "-"
        paths: ["/"]
# -- [Node labels](https://kubernetes.io/docs/concepts/sch
nodeSelector: {}
# -- Tolerations for pod assignment.
tolerations: []
# -- Node/Pod affinities.
affinity: {}
# -- How manny replicas to deploy, for production usually
replicaCount: 1
image:
  # -- Docker image repository.
  repository: nginx
  # -- Docker image tag.
  tag: latest
  # -- The image pull policy.
  pullPolicy: IfNotPresent
```

Helm Generator

Helm Generator

- Prevent Copy-Paste
- Precise configuration
- Zero to very little knowledge
- Generate config based on questionnaire!



General

Environment

Pick the environment your service is expected to serve

Production

3 replicas
Resources **soft** limit
SSL Redirection

Staging

1 replicas
Resources **hard** limit
SSL Redirection

SLA

Pick the service license agreement your service is expected to have

High

Multi-region availability
Rolling deployment

Medium

Single-region availability
Rolling deployment

Cluster

Pick the cluster you wish your service to be deployed to

Serving

Stable resources
Mix between spots and on-demand

Infra Staging

Staging infrastructure cluster
spots-instances

Region

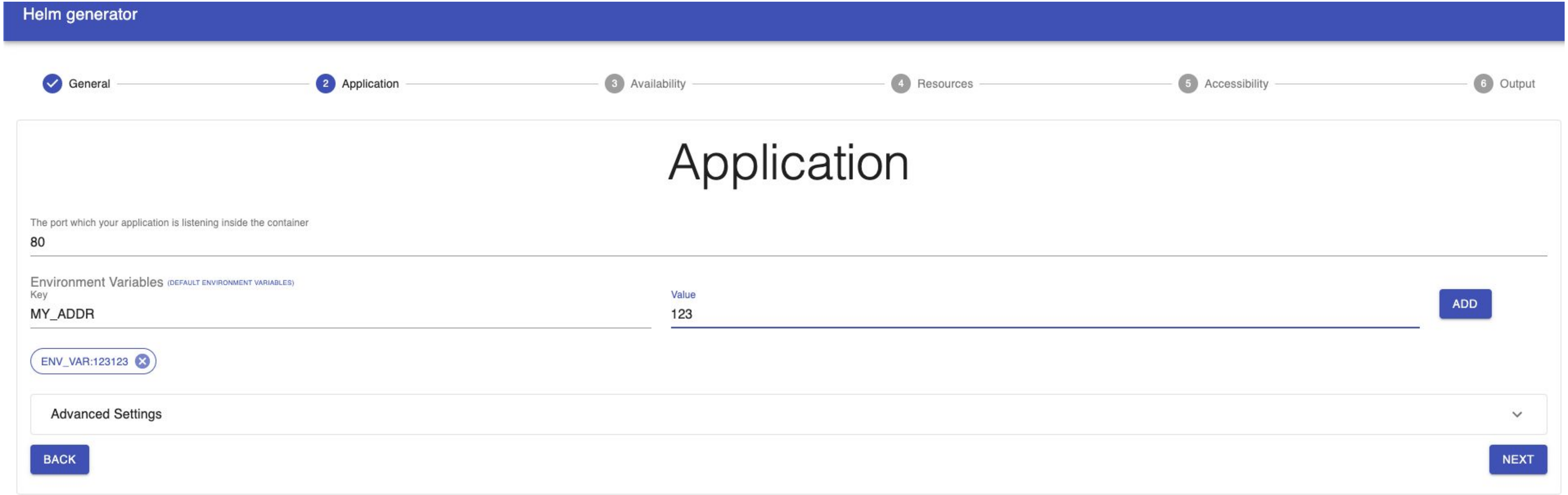
Pick the region you wish your service to be deployed to

Virginia

us-east-1

Oregon

us-west-2



Application

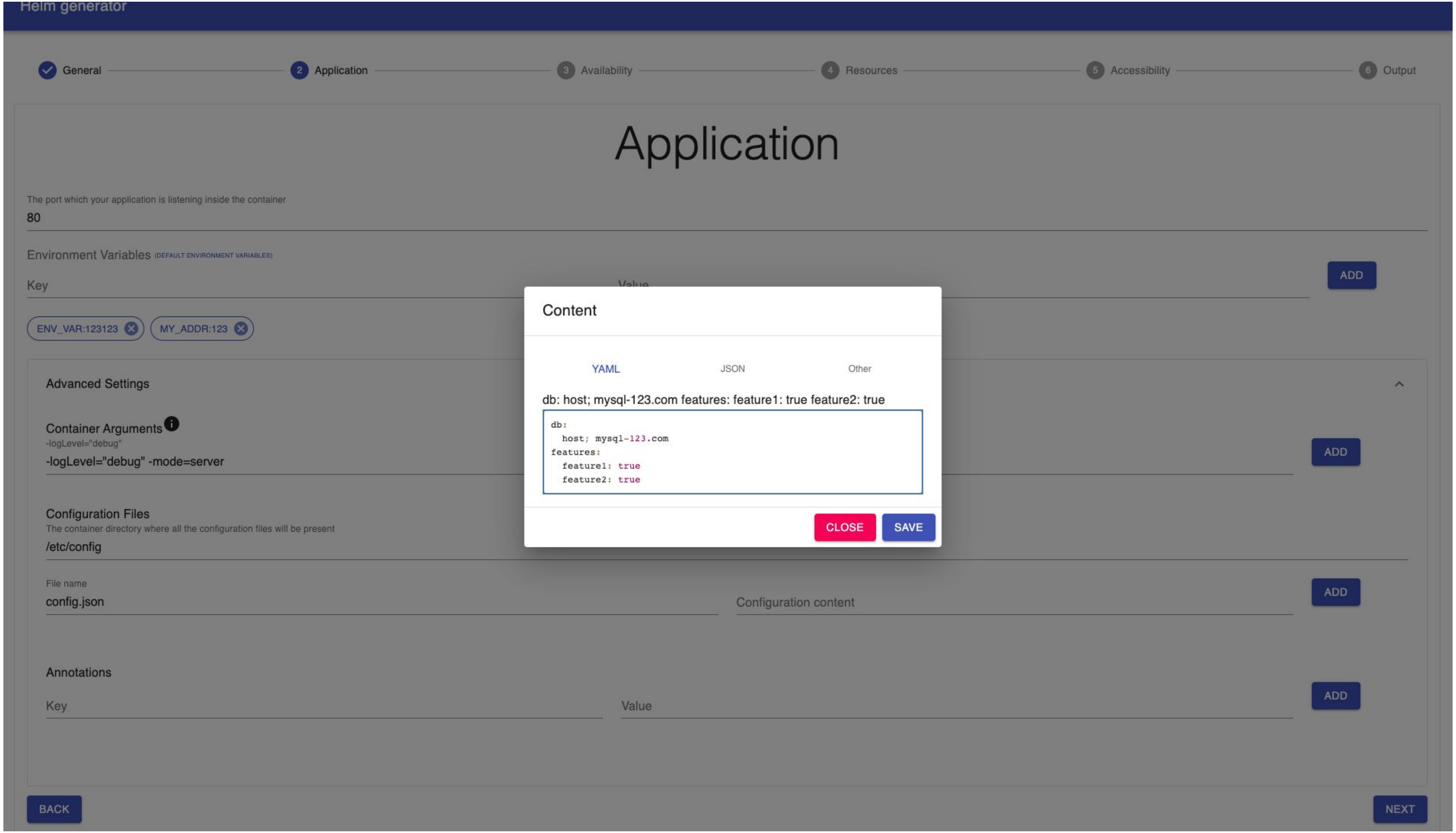
The port which your application is listening inside the container
80

Environment Variables (DEFAULT ENVIRONMENT VARIABLES)

Key
MY_ADDR

Value
123

ENV_VAR:123123



Application

The port which your application is listening inside the container
80

Environment Variables (DEFAULT ENVIRONMENT VARIABLES)

Key

Value

ENV_VAR:123123 ⊗ MY_ADDR:123 ⊗

Advanced Settings

Container Arguments
-logLevel="debug"
-logLevel="debug" -mode=server

Configuration Files
The container directory where all the configuration files will be present
/etc/config

File name
config.json

Configuration content

Annotations

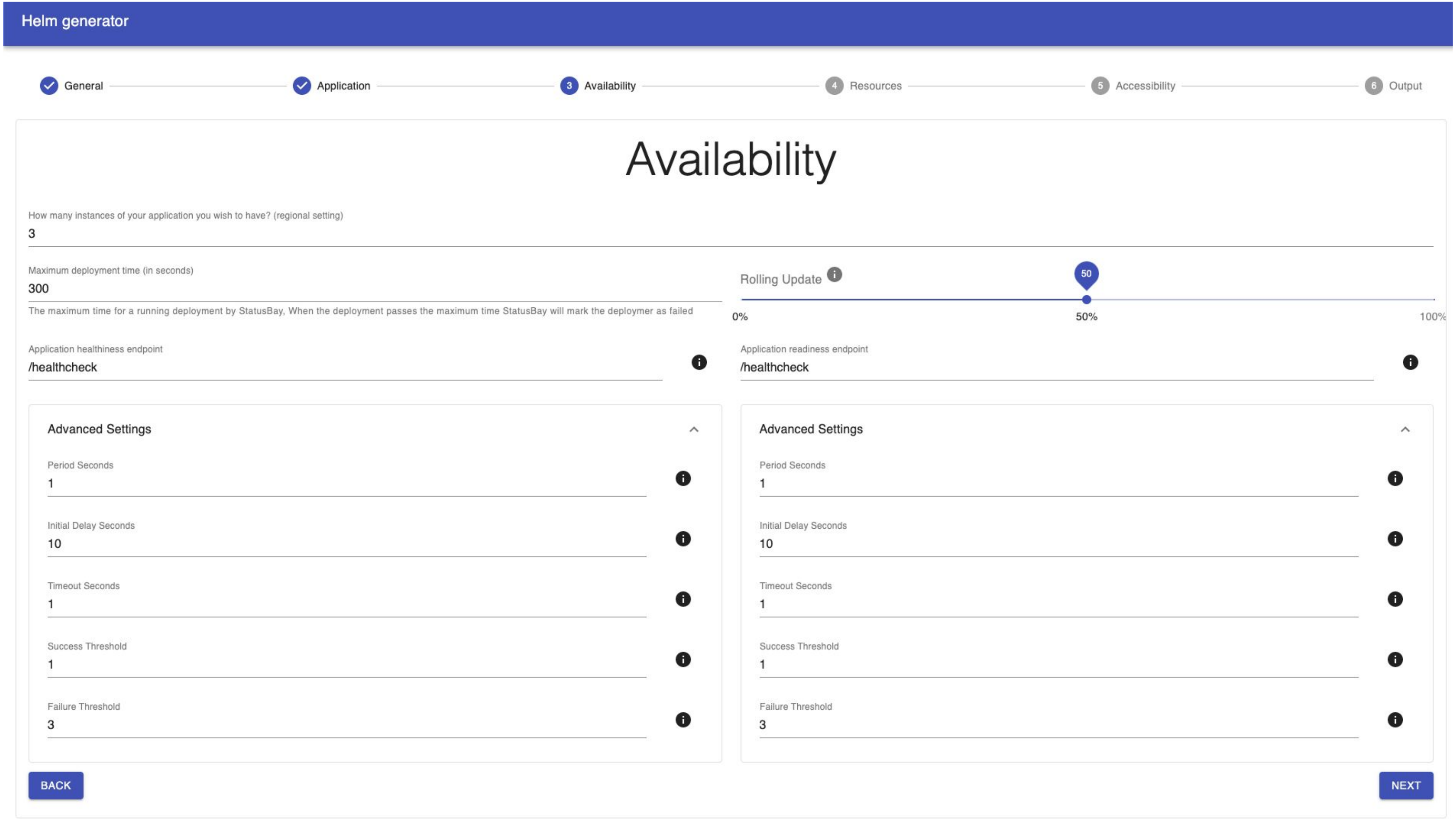
Key

Value

Content

db: host; mysql-123.com features: feature1: true feature2: true

```
db:
  host; mysql-123.com
features:
  feature1: true
  feature2: true
```



Availability

How many instances of your application you wish to have? (regional setting)
3

Maximum deployment time (in seconds)
300
The maximum time for a running deployment by StatusBay, When the deployment passes the maximum time StatusBay will mark the deploymer as failed

Rolling Update
50
0% 50% 100%

Application healthiness endpoint
/healthcheck

Application readiness endpoint
/healthcheck

Advanced Settings

Period Seconds
1

Initial Delay Seconds
10

Timeout Seconds
1

Success Threshold
1

Failure Threshold
3

Advanced Settings

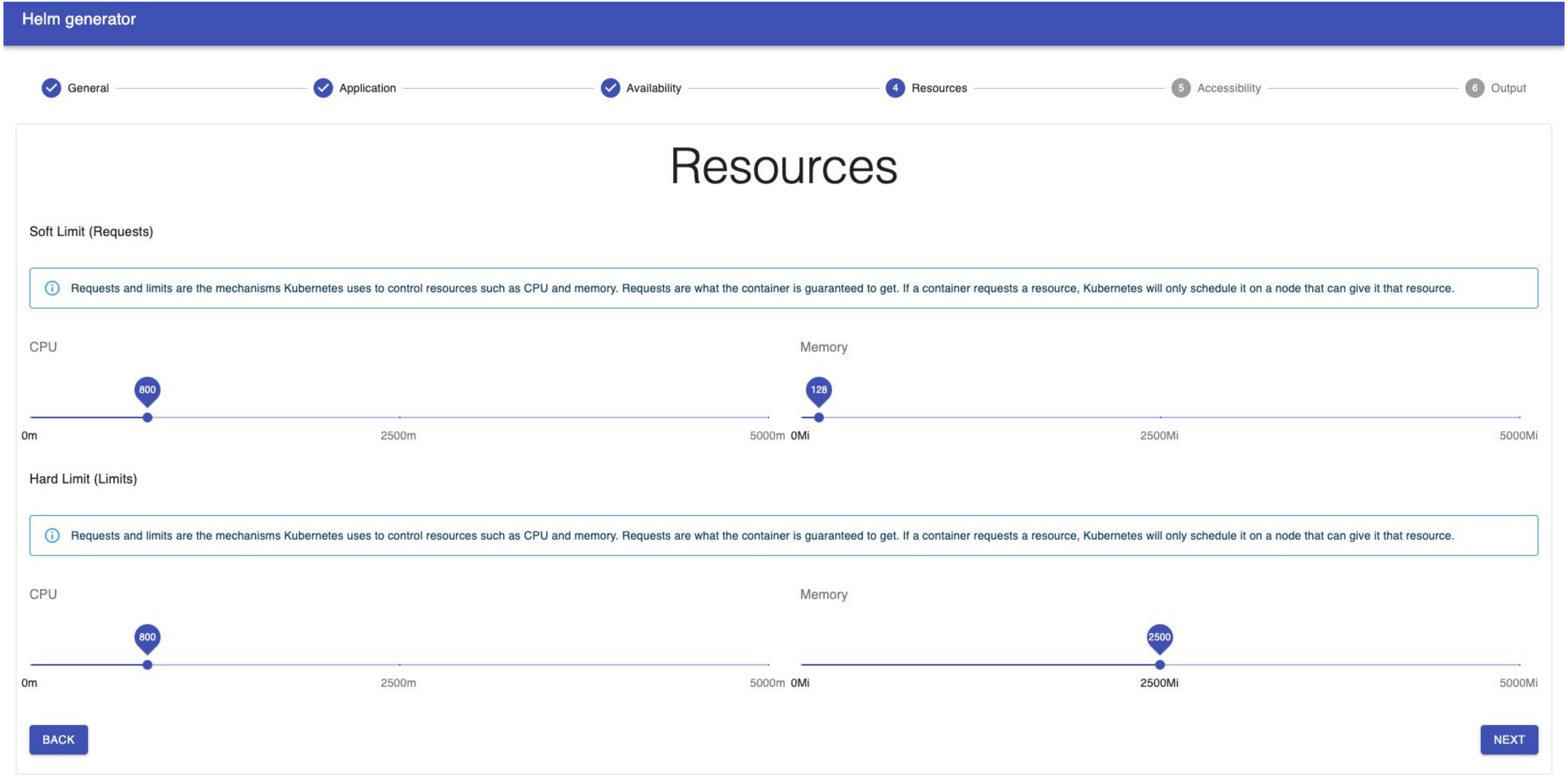
Period Seconds
1

Initial Delay Seconds
10

Timeout Seconds
1

Success Threshold
1

Failure Threshold
3



Resources

Soft Limit (Requests)

Requests and limits are the mechanisms Kubernetes uses to control resources such as CPU and memory. Requests are what the container is guaranteed to get. If a container requests a resource, Kubernetes will only schedule it on a node that can give it that resource.

CPU: 800

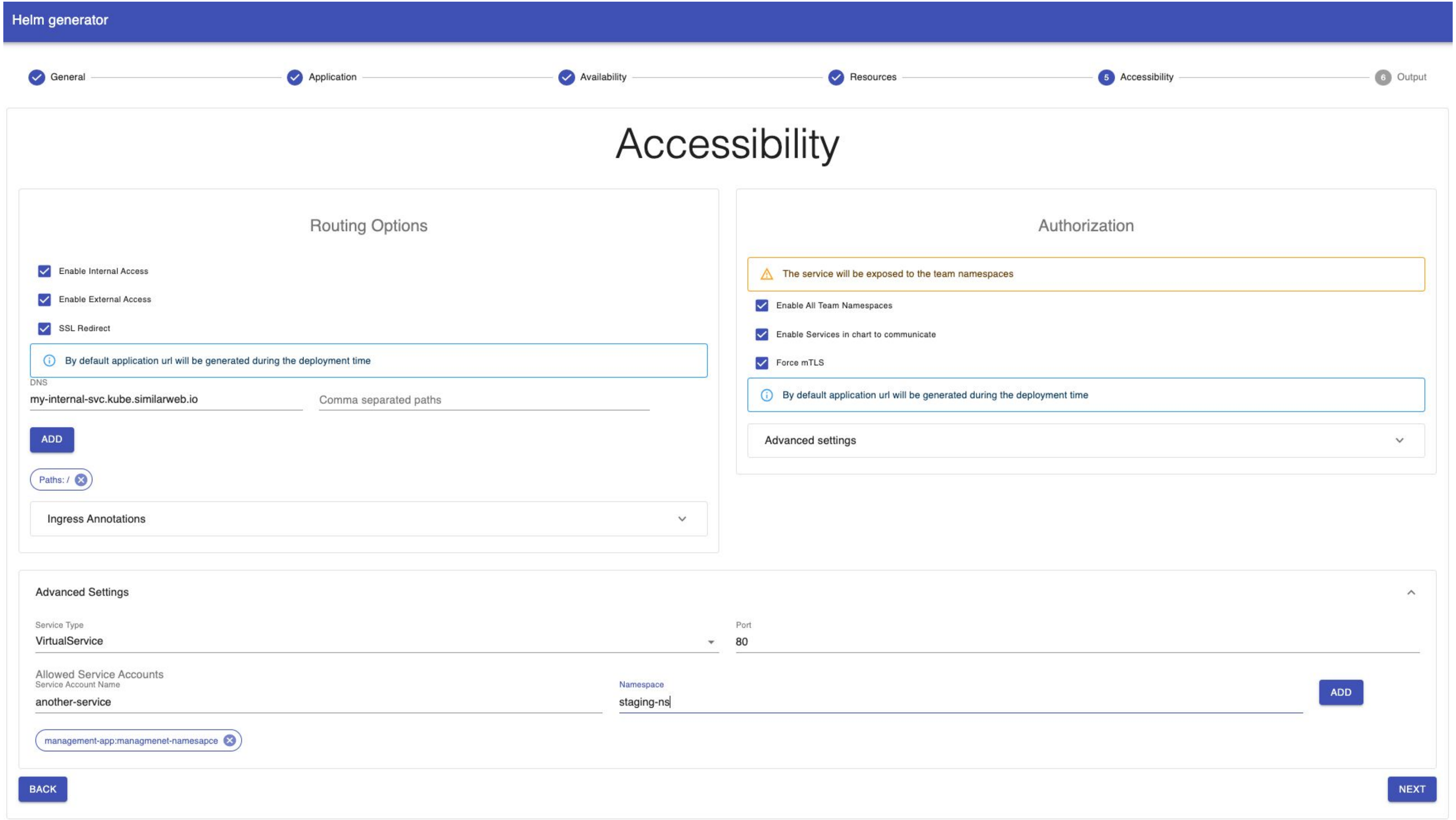
Memory: 128

Hard Limit (Limits)

Requests and limits are the mechanisms Kubernetes uses to control resources such as CPU and memory. Requests are what the container is guaranteed to get. If a container requests a resource, Kubernetes will only schedule it on a node that can give it that resource.

CPU: 800

Memory: 2500



Accessibility

Routing Options

☑ Enable Internal Access

☑ Enable External Access

☑ SSL Redirect

ⓘ By default application url will be generated during the deployment time

DNS: my-internal-svc.kube.similarweb.io

Comma separated paths

Paths: / ⊗

Ingress Annotations

Authorization

⚠ The service will be exposed to the team namespaces

☑ Enable All Team Namespaces

☑ Enable Services in chart to communicate

☑ Force mTLS

ⓘ By default application url will be generated during the deployment time

Advanced settings

Advanced Settings

Service Type: VirtualService

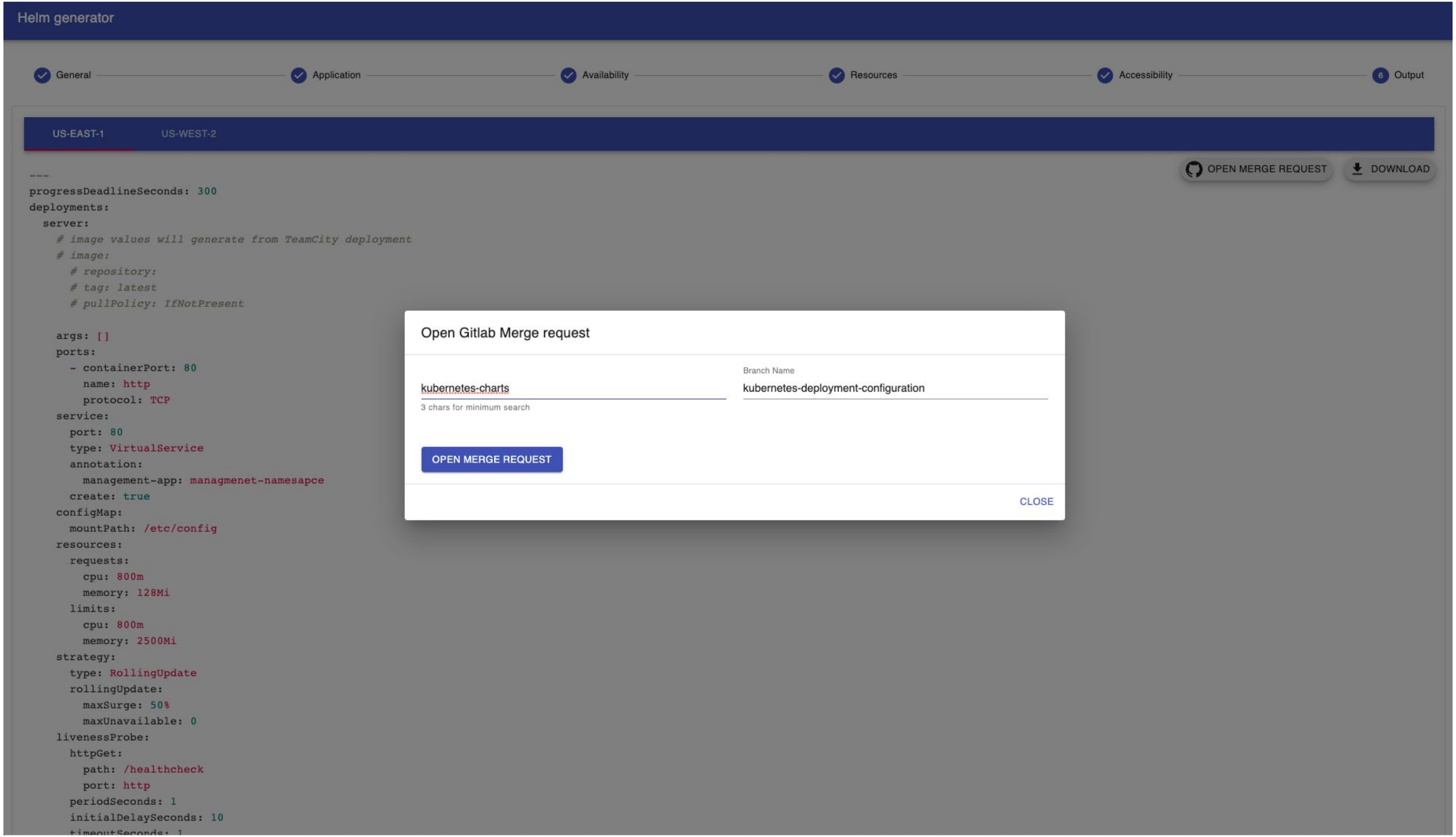
Port: 80

Allowed Service Accounts

Service Account Name: another-service

Namespace: staging-ns

management-app:managmenet-namesapce ⊗



```
---
progressDeadlineSeconds: 300
deployments:
  server:
    # image values will generate from TeamCity deployment
    # image:
      # repository:
      # tag: latest
      # pullPolicy: IfNotPresent

    args: []
    ports:
      - containerPort: 80
        name: http
        protocol: TCP
    service:
      port: 80
      type: VirtualService
      annotation:
        management-app: managmenet-namesapce
      create: true
    configMap:
      mountPath: /etc/config
    resources:
      requests:
        cpu: 800m
        memory: 128Mi
      limits:
        cpu: 800m
        memory: 2500Mi
    strategy:
      type: RollingUpdate
      rollingUpdate:
        maxSurge: 50%
        maxUnavailable: 0
    livenessProbe:
      httpGet:
        path: /healthcheck
        port: http
      periodSeconds: 1
      initialDelaySeconds: 10
      timeoutSeconds: 1
```

Open Gitlab Merge request

kubernetes-charts

3 chars for minimum search

Branch Name: kubernetes-deployment-configuration

Summary

- Building blocks
  - Security, Traffic management
- Application Charts
  - Construct full stack
- Helm generator

Thank You

🙏