

# Experiences from running Istio in a k8s production environment

Line Moseng  
@linemoseng

Johnny Horvi



Norwegian Labour and Welfare Administration





5,2 million







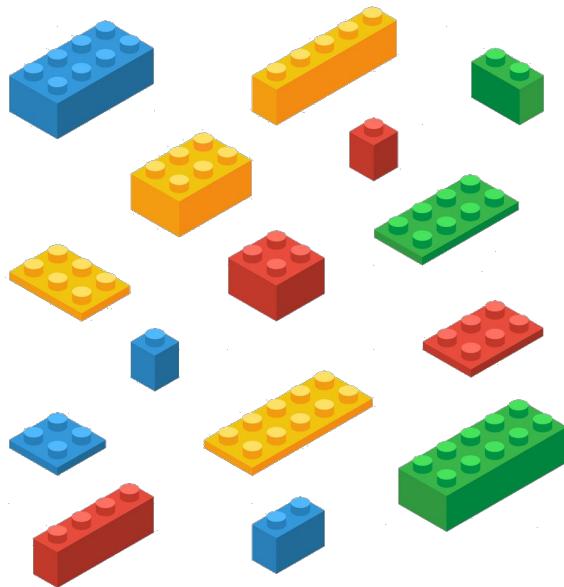




nais.io

github.com/nais

NAIS



logs



metrics



alerts



events



secrets



storage



 nerve // app

runtime



cache



deploy









internal

dev

prod

external

dev


prod

gke

dev

prod

on-prem 

public cloud 

internal

external

dev

dev

prod

prod

internal



external



DMZ

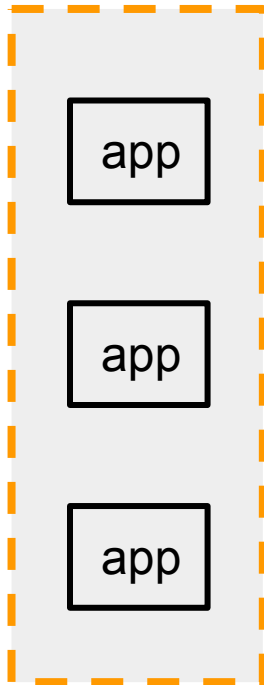


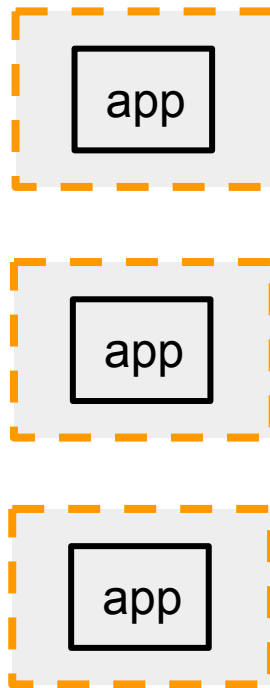
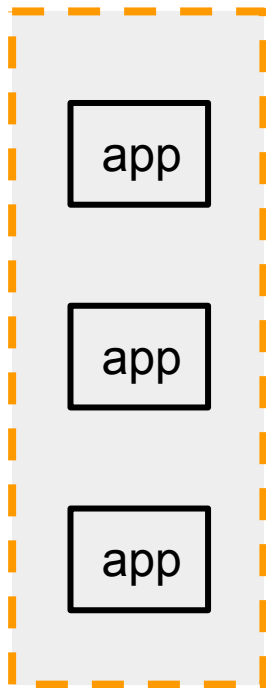
internet

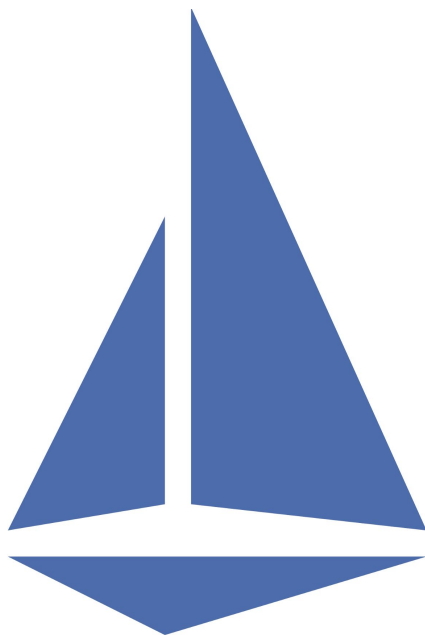




Zone







mTLS as a service

Telemetry





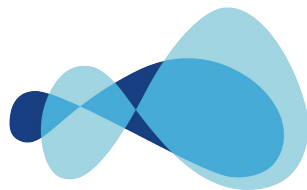


0.5



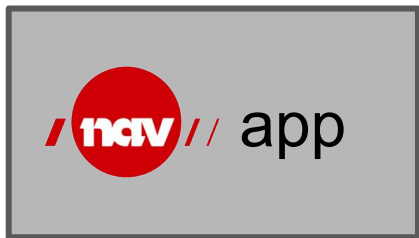


0.8



Tetrade

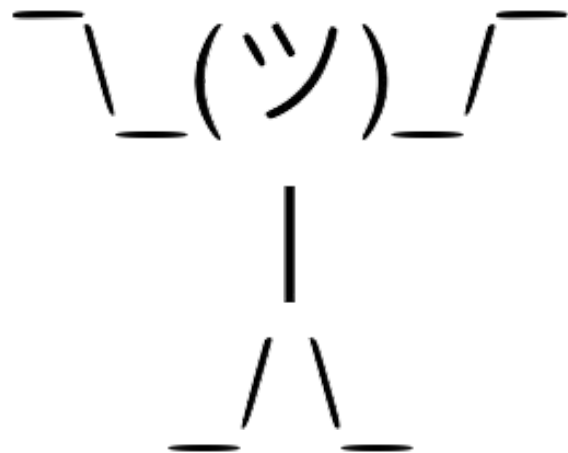


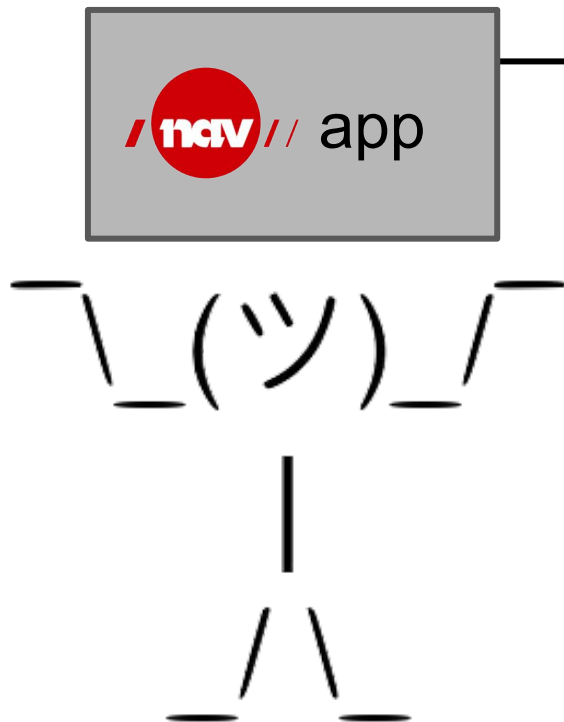












```
apiVersion: "nais.io/v1alpha1"
kind: "Application"
```

```
metadata:
```

```
  name: app
```

```
  labels:
```

```
    team: pension
```

```
spec:
```

```
  image: navikt/app:1
```

```
  port: 8080
```

```
  replicas: { min: 2, max: 4 }
```

```
  probes: { liveness: ... }
```

```
  ingresses:
```

```
    - app.dev-gke.nais.io
```

```
  egresses:
```

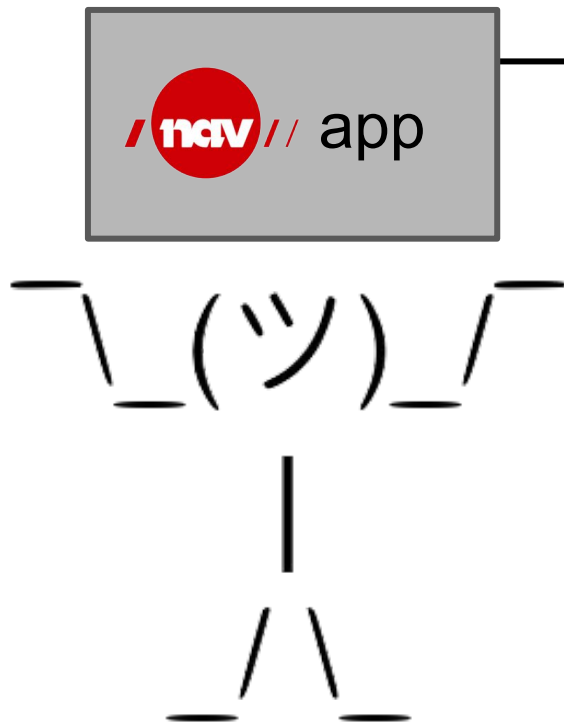
```
    - svc-not-in-mesh.nav.local
```

```
  secrets: true
```

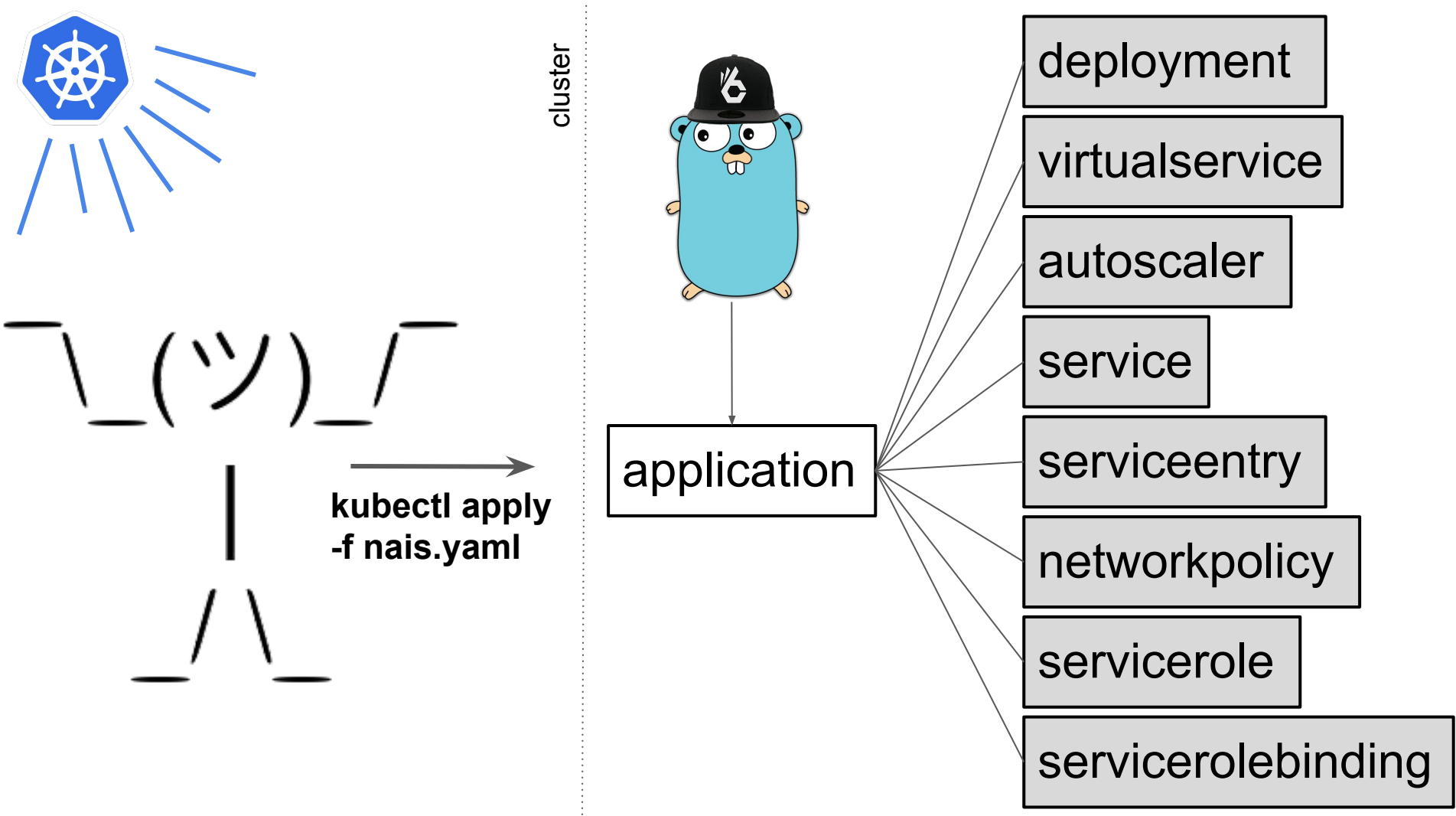
```
  accessPolicy:
```

```
    inbound:
```

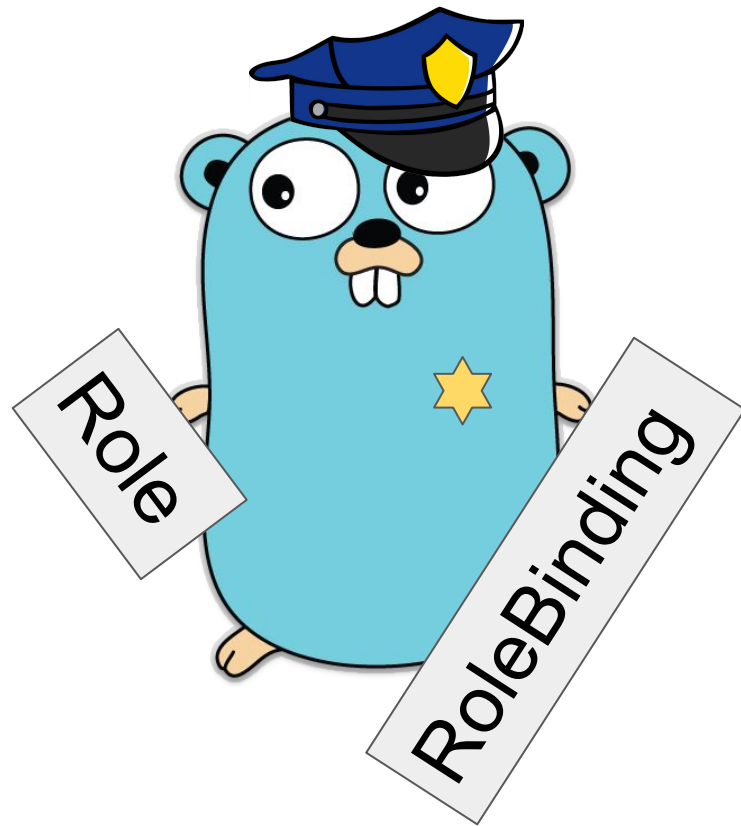
```
      - name: consumer-a
```



```
apiVersion: "nais.io/v1alpha1"
kind: "Application"
metadata:
  name: app
  labels:
    team: pension
spec:
  image: navikt/app:1
  port: 8080
  replicas: { min: 2, max: 4 }
  probes: { liveness: ... }
  ingresses:
    - app.dev-gke.nais.io
  egresses:
    - svc-not-in-mesh.nav.local
  secrets: true
  accessPolicy:
    inbound:
      - name: consumer-a
```

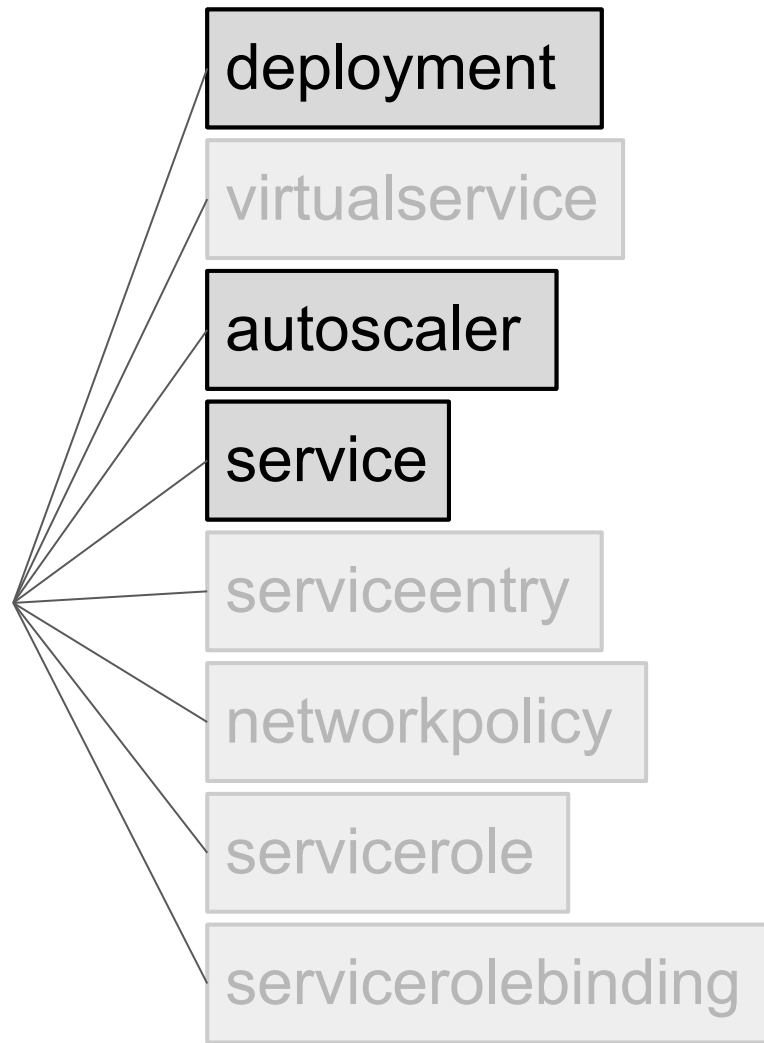


```
apiVersion: "nais.io/v1alpha1"
kind: "Application"
metadata:
  name: app
  labels:
    team: pension
spec:
  image: navikt/app:1
  port: 8080
  replicas: { min: 2, max: 4 }
  probes: { liveness: ... }
  ingresses:
    - app.dev-gke.nais.io
  egresses:
    - svc-not-in-mesh.nav.local
  secrets: true
  accessPolicy:
    inbound:
      - name: consumer-a
```





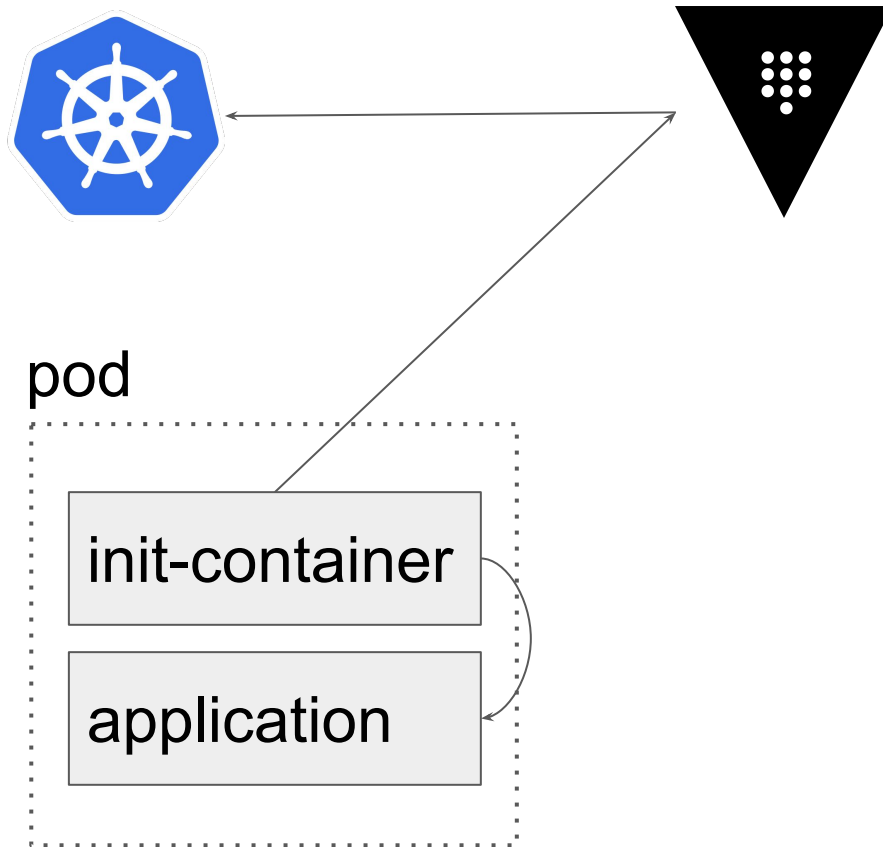
```
apiVersion: "nais.io/v1alpha1"
kind: "Application"
metadata:
  name: app
  labels:
    team: pension
spec:
  image: navikt/app:1
  port: 8080
  replicas: { min: 2, max: 4 }
  probes: { liveness: ... }
  ingresses:
    - app.dev-gke.nais.io
  egresses:
    - svc-not-in-mesh.nav.local
  secrets: true
  accessPolicy:
    inbound:
      - name: consumer-a
```



```
apiVersion: "nais.io/v1alpha1"
kind: "Application"
metadata:
  name: app
  labels:
    team: pension
spec:
  image: navikt/app:1
  port: 8080
  replicas: { min: 2, max: 4 }
  probes: { liveness: ... }
  ingresses:
    - app.dev-gke.nais.io
  egresses:
    - svc-not-in-mesh.nav.local
  secrets: true
  accessPolicy:
    inbound:
      - name: consumer-a
```

```
apiVersion: "nais.io/v1alpha1"
kind: "Application"
metadata:
  name: app
  labels:
    team: pension
spec:
  image: navikt/app:1
  port: 8080
  replicas: { min: 2, max: 4 }
  probes: { liveness: ... }
  ingresses:
    - app.dev-gke.nais.io
  egresses:
    - svc-not-in-mesh.nav.local
  secrets: true
  accessPolicy:
    inbound:
      - name: consumer-a
```

```
apiVersion: "nais.io/v1alpha1"
kind: "Application"
metadata:
  name: app
  labels:
    team: pension
spec:
  image: navikt/app:1
  port: 8080
  replicas: { min: 2, max: 4 }
  probes: { liveness: ... }
  ingresses:
    - app.dev-gke.nais.io
  egresses:
    - svc-not-in-mesh.nav.local
  secrets: true
  accessPolicy:
    inbound:
      - name: consumer-a
```

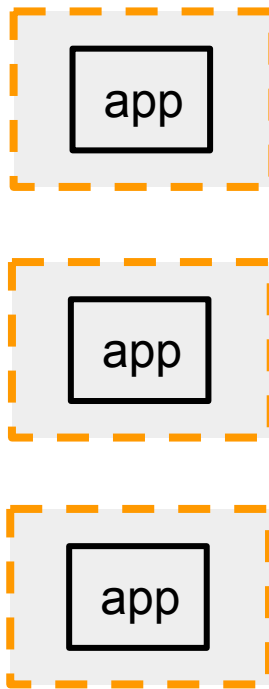
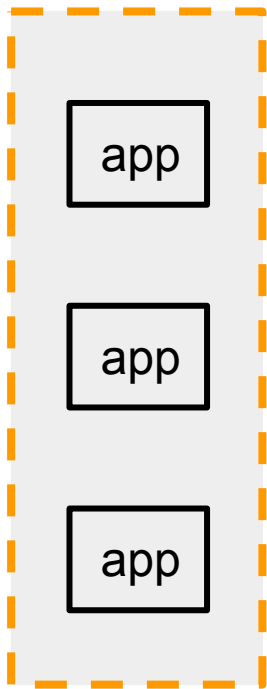


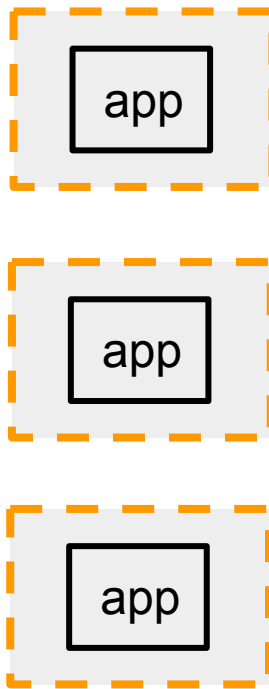
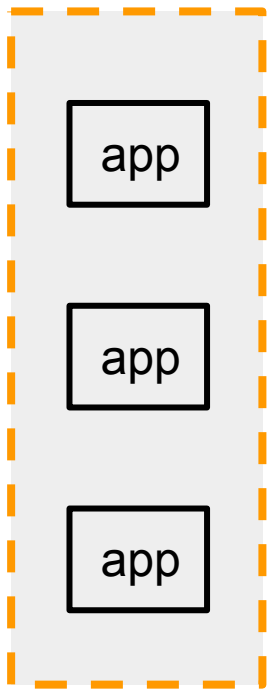
```
apiVersion: "nais.io/v1alpha1"
kind: "Application"
metadata:
  name: app
  labels:
    team: pension
spec:
  image: navikt/app:1
  port: 8080
  replicas: { min: 2, max: 4 }
  probes: { liveness: ... }
  ingresses:
    - app.dev-gke.nais.io
  egresses:
    - svc-not-in-mesh.nav.local
  secrets: true
  accessPolicy:
    inbound:
      - name: consumer-a
```

NetworkPolicy

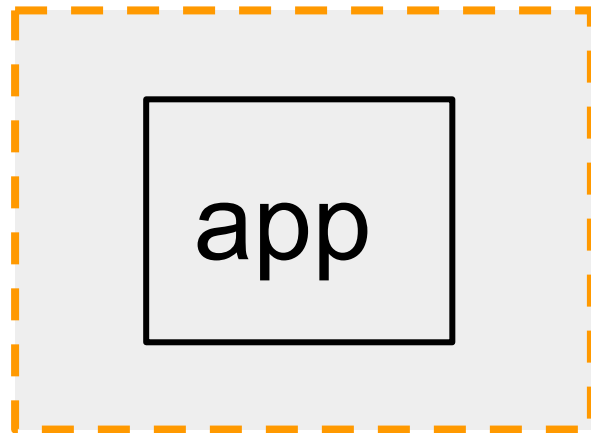
ServiceRoleBinding

Zero trust











Istio RBAC



Kubernetes  
Network Policy

naiscar

Lessons learned

What's next?



@nais\_io

@linemoseng

@j\_hrv

