kubernetes+ cloud native

eastern canada meetup

Merci de valider votre présence

 |

Meetup Hosts

07 Février 2024

Sebastien / Prune

Lead Software Eng.

Cloud Native Ambassador (CNA)

Wunderkind

Mathieu Benoit

Customer Engineer

Cloud Native Ambassador (CNA)

humanitec

Agenda

- Introduction
- CNCF News
- Prochains Meetup
- KubeCon EU 2024 à Paris
- Présentations
  - Kubernetes et Sécurité par Franck Desert - 30 min
  - Comment Helm et ArgoCD nous ont évité la noyade par Dominique Laberge (L'Université du Québec) - 30 min
  - Test de Kubernetes Gateway API par Matthieu Evrin (UEAT) - 30 min
  - GitOps et Secrets par Sébastien Prune Thomas (Wunderkind) - 15 min
- Tirage de prix !

Un grand merci !

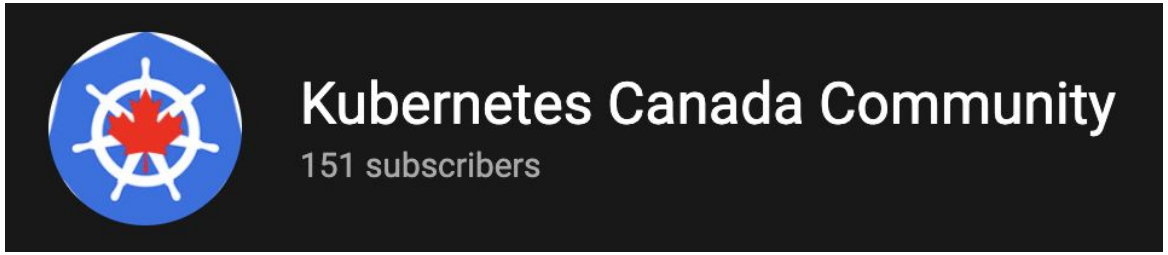
🍕 **Tickermaster** 🍕

🍻 **CNCF** 🍻

CLOUD NATIVE
COMPUTING FOUNDATION

Follow Us & Stay Connected!

@CloudNativeCA



Follow Us & Stay Connected!

linktr.ee/cloud.native.canada

Présentez lors de nos Meetups !

- **(Virtuel) Tech Talk**
  - **CFP link:** https://www.papercall.io/virtual-cncf-eastern-canada
  - **Who:** CNCF Ambassadors, CNCF Project Maintainers, community members, sponsors, etc.
  - **Focus:** cool projects, topics, tools: special guest speakers
  - **Durée:** 20 à 45 min + Q&A
- **In-Person Meetups**
  - **CFP link Montreal:** https://www.papercall.io/cncf-montreal
  - **CFP link Ottawa:** https://www.papercall.io/cncf-ottawa
  - **CFP link Toronto:** https://www.papercall.io/cncf-toronto
  - **CFP link Quebec City:** https://www.papercall.io/cncf-quebec

Become a Sponsor!

A venir

- **Next Meetup**
  - **Right after KubeCon Paris: 3 ou 10 avril ? Merci Vooban !**
- **Enregistrement et Livestream des prochaines sessions?**
  - **Enregistrement?**
  - **Livestream?**

CNCF News

CloudEvents is a specification for describing event data in common formats to provide interoperability across services, platforms and systems.

Event Formats specify how to serialize a CloudEvent with certain encoding formats.

Kubernetes 1.29 released

- ReadWriteOncePod PersistentVolume access mode
- Node volume expansion Secret support for CSI drivers
- KMS v2 encryption at rest generally available

kubernetes.io/blog

Posts in 2024

Image Filesystem: Configuring Kubernetes to store containers on a separate filesystem

Tuesday, January 23, 2024 in Blog

Author: Kevin Hannon (Red Hat) A common issue in running/operating Kubernetes clusters is running out of disk space. When the node is provisioned, you should aim to have a good amount of storage space for your container images and running containers. ...

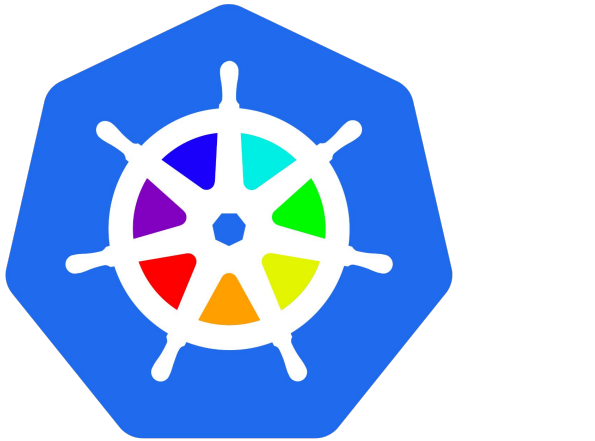
Read more

Spotlight on SIG Release (Release Team Subproject)

Monday, January 15, 2024 in Blog

Author: Nitish Kumar The Release Special Interest Group (SIG Release), where Kubernetes sharpens its blade with cutting-edge features and bug fixes every 4 months. Have you ever considered how such a big project like Kubernetes manages its timeline ...

Read more



- Version **v0.2.2** !
- Fix **`kubecolor get pod`** not showing **OOMKilled** with color
- Fix **`kubecolor describe pod`** not show **condition** with color
- Set **KUBECOLOR_LIGHT_BACKGROUND** to switch to light colors
- New feature for custom color coming soon !

https://github.com/kubecolor/kubecolor

- Version **v2.10** (2.10.1 soon, please wait) !
- Upgraded kubectl from 1.24 to 1.26
- Helm version upgraded from 3.13.2 to 3.14.0
- Advanced ApplicationSet templating using template patches
- Apps in Any Namespace & Notifications
- Argo CD Server-Side Diff (read the docs !!!)

https://argo-cd.readthedocs.io/en/latest/operator-manual/upgrading/2.9-2.10/

KubeCon Europe (Paris)

https://events.linuxfoundation.org/kubecon-cloudnativecon-europe/register/

15% avec le code KCEU24CNCFGMEET

Prochains KubeCon North America

Local community

Some contents from our local community

- Envoy Gateway in Production - Fabrice Aneche
- ArgoCD Appset-of-Appset Pattern - Prune
- Podcast | Kubernetes Security with Imad Bensisaid – Maxime Coquerel
- Score applies to become a CNCF sandbox project (TAG App Devliery (WG Platforms) Meeting)
- Dapr with Score and Humanitec — Improving the Developer Experience of your Platform, on steroids! - Mathieu Benoit (+ Dapr Community Call)
- Platform Engineering Maturity @ KubeCon NA 2023 - Mathieu Benoit

Présentations !

Kubernetes et Sécurité

Franck Desert

 |

Comment Helm et ArgoCD nous ont évité la noyade

Dominique Laberge

 |

Test de Kubernetes Gateway API

Matthieu Evrin

 |

K8S Gateway API

Test local avec Minikube

Agenda

- Présentation
- Exposition publique dans Kubernetes
- Gateway API
- Démo

Présentation

Matthieu EVRIN

Platform Engineer

Compagnie: UEAT

Exposition publique avec Kubernetes

Exposition publique:

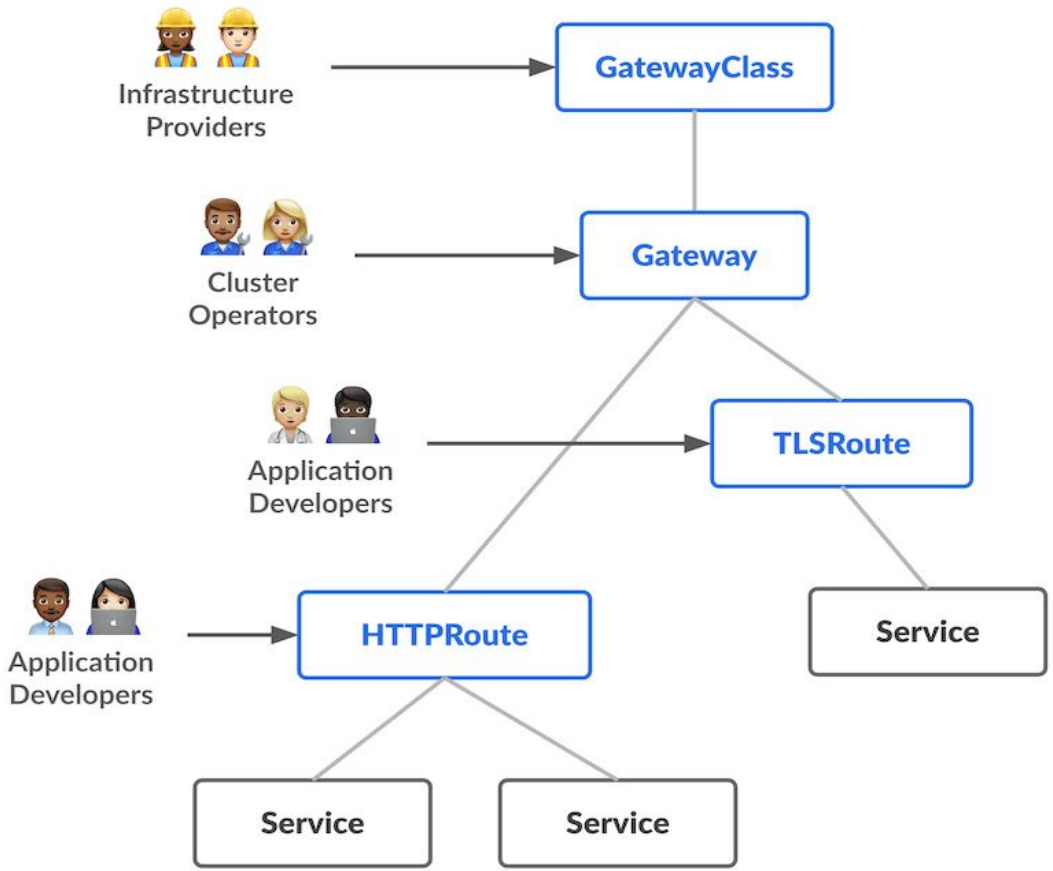
- Service (L4)
  - Node port
- Ingress (L7)
- Gateway API (L7)
  - Specification
  - Portabilité et Réutilisabilité

Gateway API

Documentation: https://gateway-api.sigs.k8s.io/

- Architecture
  - Diagramme
  - Composantes
  - Securité
- Comparaison avec Ingress

Gateway API - Architecture



Gateway API - Composantes

GatewayClass: https://gateway-api.sigs.k8s.io/concepts/api-overview/#gatewayclass

Gateway: https://gateway-api.sigs.k8s.io/concepts/api-overview/#gateway

Route: https://gateway-api.sigs.k8s.io/concepts/api-overview/#route-resources

- HTTPRoute (L7)
- TLSRoute (experimental) (L4 et L7)
- TCPRoute/UDPRoute (experimental) (L4)
- GRPCRoute (experimental) (L7)

Policy

- BackendTLSPolicy: https://gateway-api.sigs.k8s.io/api-types/backendtlspolicy/

ReferenceGrant: https://gateway-api.sigs.k8s.io/api-types/referencegrant/

Gateway API - Composantes (Suite)

GatewayClass

Ressources créées par le fournisseur de l'infrastructure.
Exemple de classe dans GCP *gke-l7-global-external-managed, gke-l7-rilb*

Gateway API - Composantes (Suite)

Gateway

Passerelle de configuration de l'infrastructure

Specifications:

- gatewayClassName
- listeners
- addresses

```yaml
apiVersion: gateway.networking.k8s.io/v1beta1
kind: Gateway
metadata:
  name: my-gateway
spec:
  gatewayClassName: gke-l7-rilb
  listeners:
  - name: http
    protocol: HTTP
    port: 80
    allowedRoutes:
      kinds:
      - kind: HTTPRoute
```

Gateway API - Composantes (Suite)

Route

HTTPRoute: Routage des requêtes HTTP

TLSRoute: Similaire TCP route avec le support TLS

UDPRoute / TCPRoute: Routage de requêtes TCP et UDP

GRPCRoute: Routage des requêtes gRPC

Specifications

- parentRefs (Gateway)
- hostnames (Liste de domaines supportés, IP non autorisé)
- rules
  - matches
  - filters
  - backendRefs
- status

Gateway API - Composantes (Suite)

```yaml
apiVersion: gateway.networking.k8s.io/v1beta1
kind: HTTPRoute
metadata:
  name: my-route
spec:
  parentRefs:
  - name: my-gateway
  hostnames:
  - "example.com"
  rules:
  - matches:
    - path:
        value: /
    backendRefs:
    - name: site
      port: 80
  - matches:
    - path:
        value: /shop
    backendRefs:
    - name: store
      port: 80
```

```yaml
apiVersion: gateway.networking.k8s.io/v1alpha2
kind: GRPCRoute
metadata:
  name: grpc-app-1
spec:
  parentRefs:
  - name: my-gateway
  hostnames:
  - "example.com"
  rules:
  - matches:
    - method:
        service: com.example.User
        method: Login
    backendRefs:
    - name: my-service1
      port: 50051
  - matches:
    - headers:
      - type: Exact
        name: magic
        value: foo
      method:
        service: com.example.Things
        method: DoThing
    backendRefs:
    - name: my-service2
      port: 50051
```

Gateway API - Composantes (Suite)

Policy

BackendTLSPolicy: Traitement de la configuration TLS pour acheminer les requetes HTTPS au backend

Specifications

- targetRef
- tls
  - caCertRefs
  - wellKnownCACerts
  - hostname
- status

Gateway API - Composantes (Suite)

ReferenceGrant

Permet

- cross reference entre namespace

  Ex: HttpRoute A dans namespace A redirige vers service B dans le namespace B

- Gateway peut référencer un secret dans un namespace différent

Specifications

- from
- to

```yaml
kind: HTTPRoute
metadata:
  name: foo
  namespace: foo
spec:
  rules:
  - matches:
    - path: /bar
    backendRefs:
      - name: bar
        namespace: bar
---
kind: ReferenceGrant
metadata:
  name: bar
  namespace: bar
spec:
  from:
  - group: gateway.networking.k8s.io
    kind: HTTPRoute
    namespace: foo
  to:
  - group: ""
    kind: Service
```

Gateway API - Composantes (Suite)

Status

<- HTTPRoute

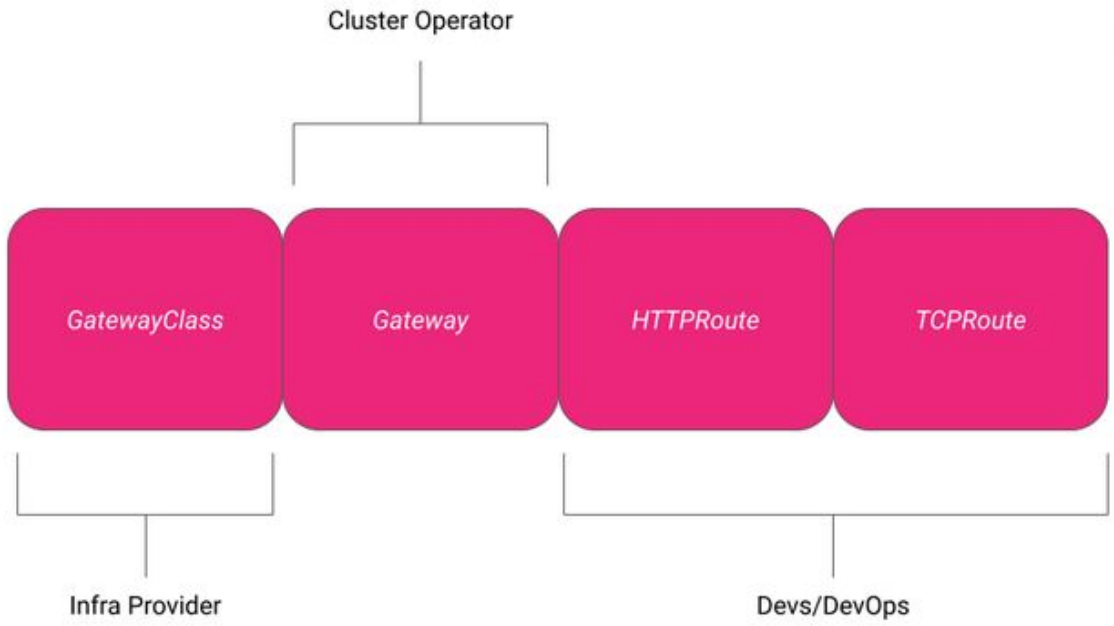
Gateway ->

```
      Value:  /
Status:
  Parents:
    Conditions:
      Last Transition Time:  2024-02-06T02:37:00Z
      Message:               Route is accepted
      Observed Generation:   1
      Reason:                Accepted
      Status:                True
      Type:                  Accepted
      Last Transition Time:  2024-02-06T02:37:00Z
      Message:               Resolved all the Object references for the Route
      Observed Generation:   1
      Reason:                ResolvedRefs
      Status:                True
      Type:                  ResolvedRefs
    Controller Name:         gateway.envoyproxy.io/gatewayclass-controller
    Parent Ref:
      Group:      gateway.networking.k8s.io
      Kind:       Gateway
      Name:       envoy-gateway
      Namespace:  gateway-non-prod
    Conditions:
      Last Transition Time:  2024-02-06T02:37:00Z
      Message:               Route is accepted
      Observed Generation:   1
      Reason:                Accepted
      Status:                True
      Type:                  Accepted
      Last Transition Time:  2024-02-06T02:37:00Z
      Message:               Resolved all the Object references for the Route
      Observed Generation:   1
      Reason:                ResolvedRefs
      Status:                True
      Type:                  ResolvedRefs
    Controller Name:         gateway.envoyproxy.io/gatewayclass-controller
    Parent Ref:
      Group:      gateway.networking.k8s.io
      Kind:       Gateway
      Name:       envoy-gateway
      Namespace:  gateway-common
Events:           <none>
```

```
Status:
  Conditions:
    Last Transition Time:  2024-02-06T02:37:00Z
    Message:               The Gateway has been scheduled by Envoy Gateway
    Observed Generation:   1
    Reason:                Accepted
    Status:                True
    Type:                  Accepted
    Last Transition Time:  2024-02-06T02:37:00Z
    Message:               No addresses have been assigned to the Gateway
    Observed Generation:   1
    Reason:                AddressNotAssigned
    Status:                False
    Type:                  Programmed
  Listeners:
    Attached Routes:  4
    Conditions:
      Last Transition Time:  2024-02-06T02:37:00Z
      Message:               Sending translated listener configuration to the data plane
      Observed Generation:   1
      Reason:                Programmed
      Status:                True
      Type:                  Programmed
      Last Transition Time:  2024-02-06T02:37:00Z
      Message:               Listener has been successfully translated
      Observed Generation:   1
      Reason:                Accepted
      Status:                True
      Type:                  Accepted
      Last Transition Time:  2024-02-06T02:37:00Z
      Message:               Listener references have been resolved
      Observed Generation:   1
      Reason:                ResolvedRefs
      Status:                True
      Type:                  ResolvedRefs
    Name:                    http
    Supported Kinds:
      Group:  gateway.networking.k8s.io
      Kind:   HTTPRoute
      Group:  gateway.networking.k8s.io
      Kind:   GRPCRoute
Events:       <none>
```

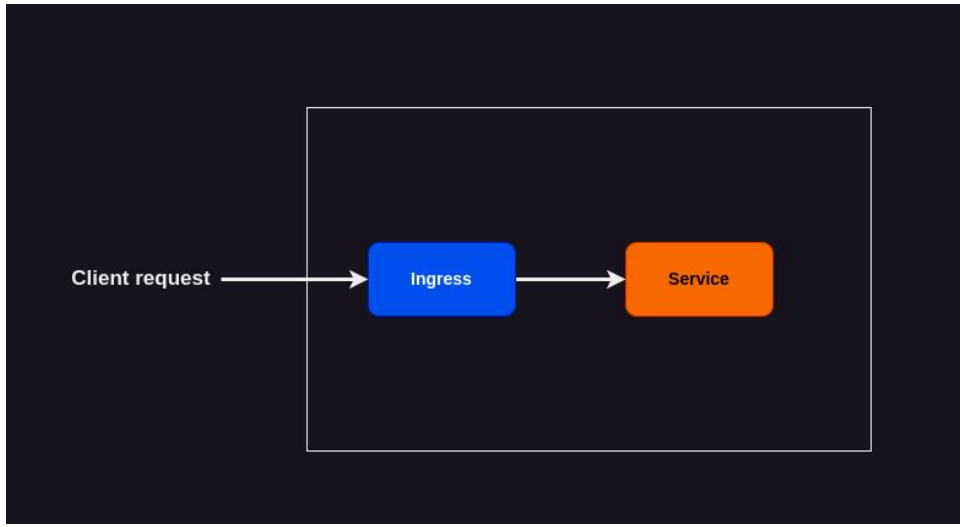
Gateway API - Securité

Baser sur RBAC

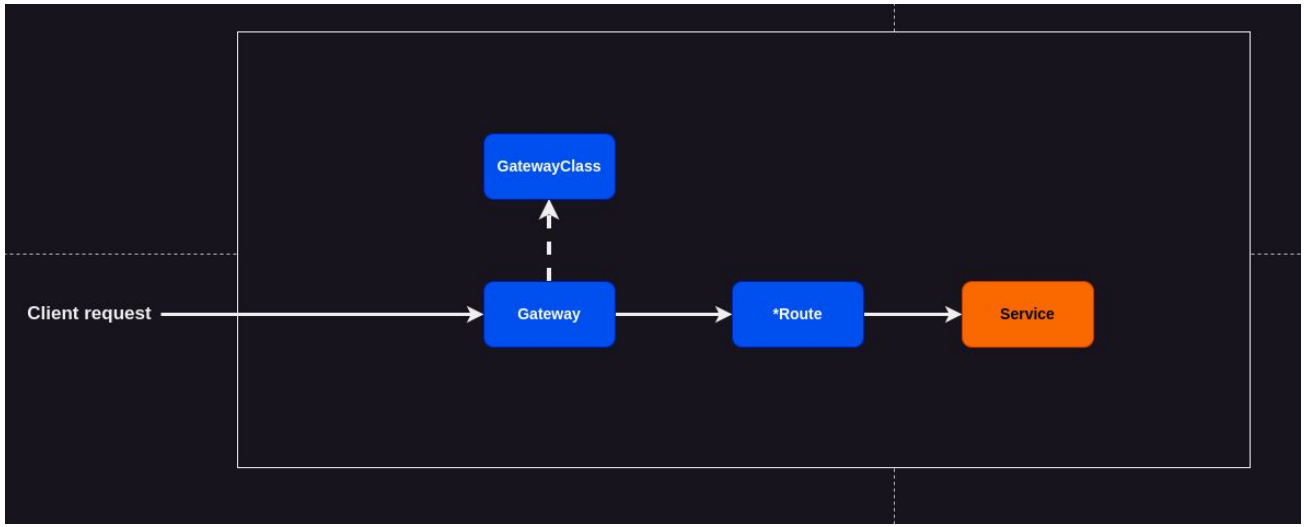


Gateway API - Ingress (Nginx) Comparaison

Ingress



Gateway API



Gateway API - Ingress (Nginx) Comparaison

Ex: Routage basée sur les Headers

```yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: header-ingress
  namespace: default
  annotations:
    nginx.ingress.kubernetes.io/server-snippet: |
      if ($http_custom_header = "value1") {
          proxy_pass http://service-1;
      }
      if ($http_custom_header = "value2") {
          proxy_pass http://service-2;
      }
spec:
  ingressClassName: nginx
  rules:
    - host: your-domain.com
      http:
        paths:
          - path: /
            pathType: Prefix
            backend:
              service:
                name: default-backend
                port:
                  number: 80
```

```yaml
apiVersion: gateway.networking.k8s.io/v1beta1
kind: HTTPRoute
metadata:
 name: bar-route
spec:
 parentRefs:
   - name: gateway
 hostnames:
   - foo.example.com
 rules:
 - backendRefs:
   - name: default
    port: 8080
 - matches:
   - headers:
    - name: http_custom_header
    value: value1
   backendRefs:
   - name: service1
    port: 8080
 - matches:
   - headers:
    - name: http_custom_header
    value: value2
   backendRefs:
   - name: service2
    port: 8080
```

Gateway API - Ingress (Nginx) Comparaison

```yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: canary-ingress-v1
  namespace: default
  annotations:
    nginx.ingress.kubernetes.io/rewrite-target: /
    nginx.ingress.kubernetes.io/canary: "true"
    nginx.ingress.kubernetes.io/canary-weight: "10"
spec:
  ingressClassName: nginx
  rules:
    - host: your-domain.com
      http:
        paths:
          - path: /
            pathType: Prefix
            backend:
              service:
                name: service-1
                port:
                  number: 80
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: canary-ingress-v2
  namespace: default
  annotations:
    nginx.ingress.kubernetes.io/rewrite-target: /
spec:
  ingressClassName: nginx
  rules:
    - host: your-domain.com
      http:
        paths:
          - path: /
            pathType: Prefix
            backend:
              service:
                name: service-2
                port:
                  number: 80
```

Ex: Traffic pondéré

```yaml
apiVersion: gateway.networking.k8s.io/v1beta1
kind: HTTPRoute
metadata:
  name: canary-gw-api
spec:
  parentRefs:
    - name: gateway
  rules:
    - matches:
        - path:
            type: PathPrefix
            value: /
      backendRefs:
        - name: foo-v1
          port: 8080
          weight: 90
        - name: foo-v2
          port: 8080
          weight: 10
```

Gateway API - Démo

https://github.com/lekaf974/kubernetes-learning

Gateway API - Démo

Sources

- https://gateway-api.sigs.k8s.io/
  - https://gateway-api.sigs.k8s.io/implementations/
- https://cloud.google.com/kubernetes-engine/docs/concepts/gateway-api
- https://dzone.com/articles/kubernetes-gateway-api-vs-ingress
- https://imesh.ai/blog/kubernetes-gateway-api/

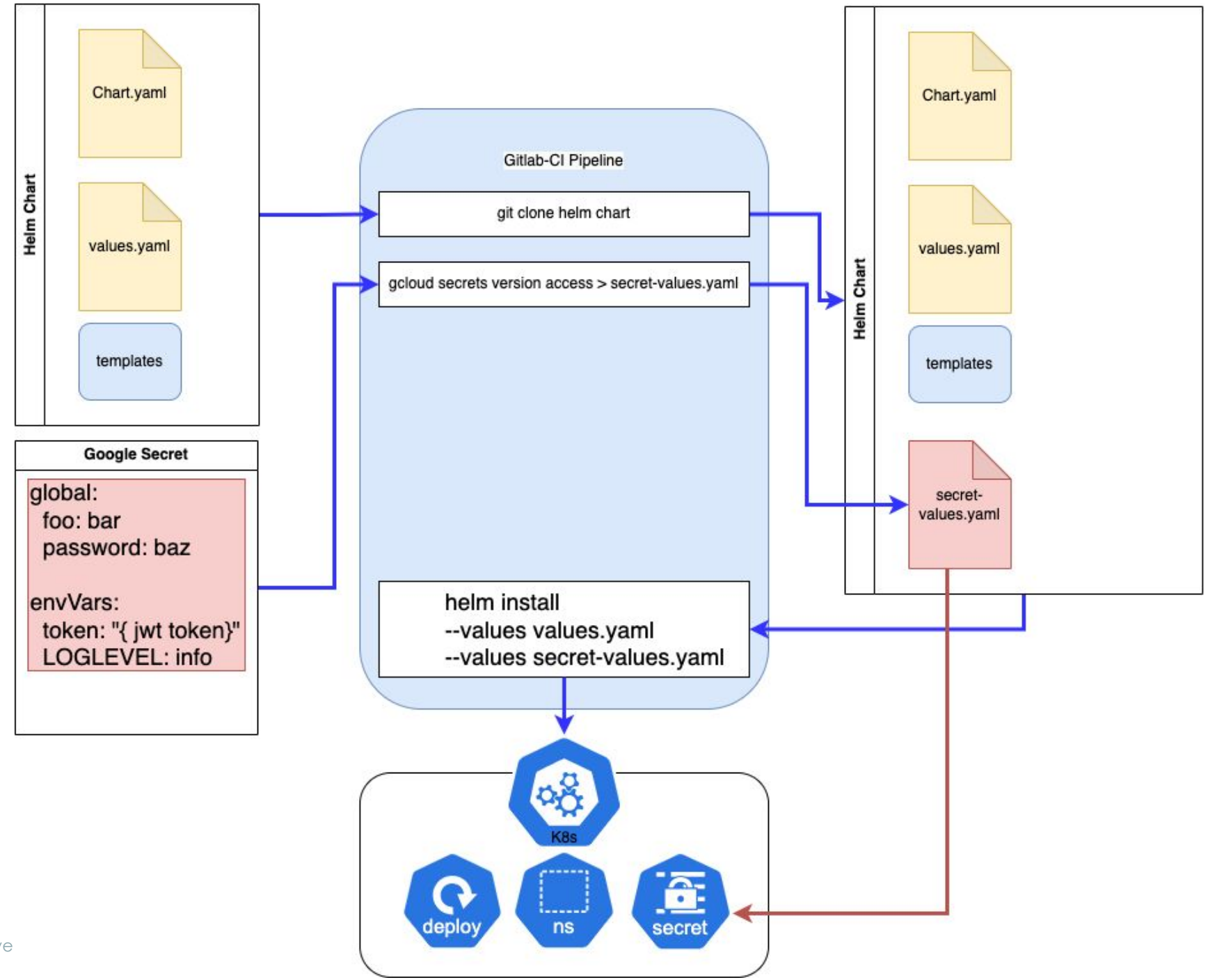
Kubernetes Gateway API

Merci

ArgoCD et les Secrets

Sébastien Prune Thomas

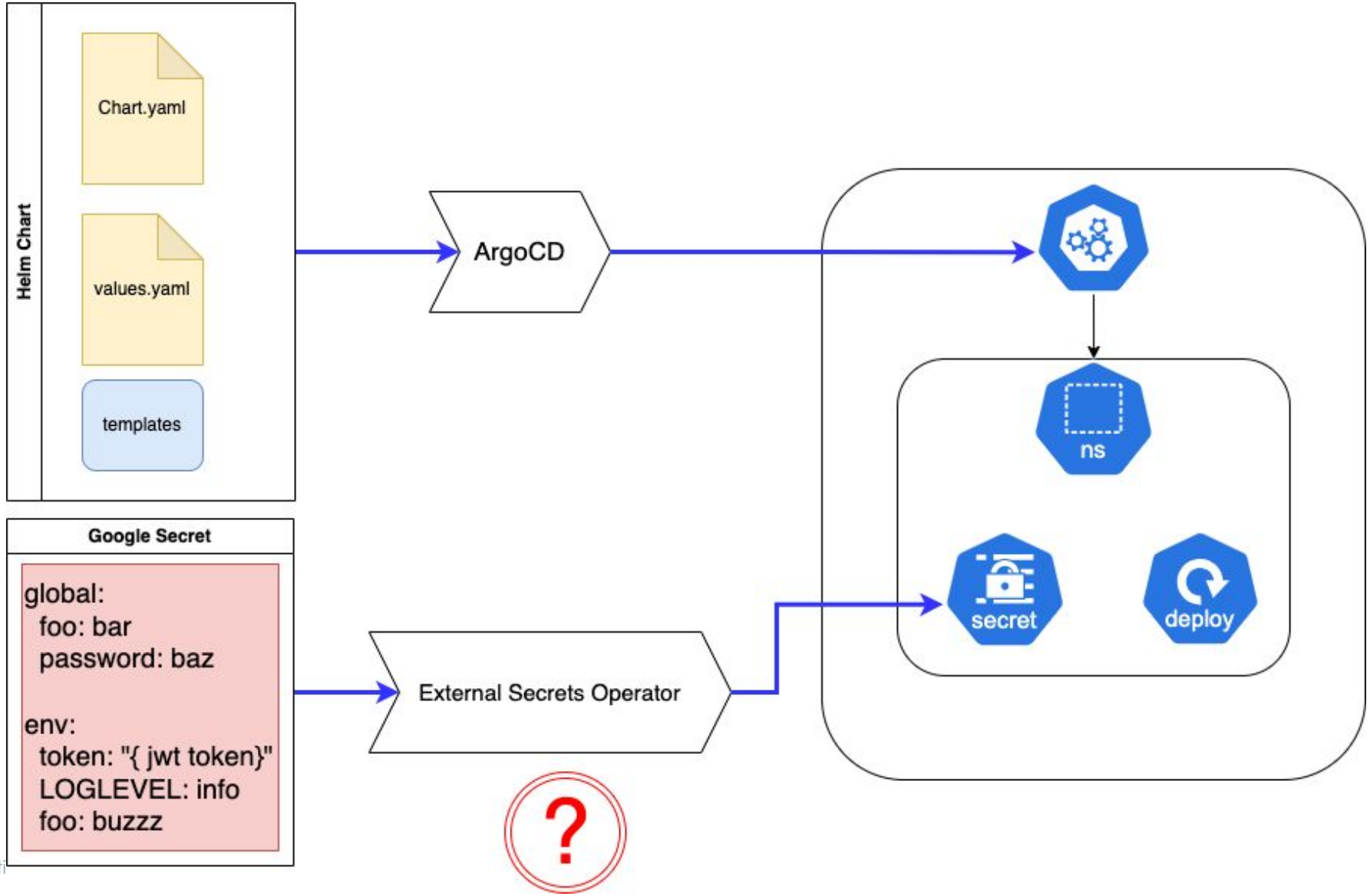
 |



Problems

- Not GitOps
- Secret format in Google Secret Manager not compatible with K8s secrets
- Helm Template merges some values from other part of the chart into the final K8s secret

GitOps, ArgoCD and Secrets



Problems

- Secret format in *Google Secret Manager* not compatible with *External Secrets Operator*
- No CI to copy some secret's values into deployment **env**

Solutions

- Use External Secrets Operator **templates** !
- Update deployments to use **valueFrom** secret

ESO templates

```yaml
apiVersion: external-secrets.io/v1beta1

kind: ExternalSecret

metadata:
  name: my-secret
  namespace: my-app-ns

spec:
  refreshInterval: 1h                    # rate SecretManager pulls GCPSM
  secretStoreRef:
    kind: SecretStore
    name: my-namespace-secret-store      # name of the SecretStore

  target:
    name: my-secret                      # name of the k8s Secret to be created
    creationPolicy: Owner
```


ESO templates

```
  template:
    templateFrom:
      - target: Data
        literal: |

          {{- $payload := .key | fromYaml }}
          {{- $envVars := deepCopy $payload.global |
                    mergeOverwrite (deepCopy $payload.env) -}}
          {{- range $k, $v := $envVars }}
            {{ $k }}: '{{ $v }}'
          {{- end }}

data:
- secretKey: key
  remoteRef:
    key: my-app-google-secret # name of the GCPSM secret key
```


example secret

```
global:
  key1: foo
  loglevel: info
env:
  key1: bar
  key2: other
```

```
apiVersion: v1
kind: Secret
metadata:
  name: my-secret
  namespace: my-app-ns
type: Opaque
data:
  key1: dFHJhwbGFsYQ==  (bar)
  key2: drGdd90bw==     (other)
  loglevel: aW5mbwo=    (info)
```


Chart update

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: my-app
  namespace: my-app-ns
spec:
  template:
    spec:
      containers:
      - env:
        - name: SECRET_KEY1
          valueFrom:
            secretKeyRef:
              key: key1
              name: my-secret
        - name: SECRET_KEY2
          valueFrom:
            secretKeyRef:
              key: key2
              name: my-secret
```


Prix pour les bonnes questions !

CLOUD NATIVE
COMPUTING FOUNDATION

Québec Meetup

kubernetes+ cloud native

eastern canada meetup