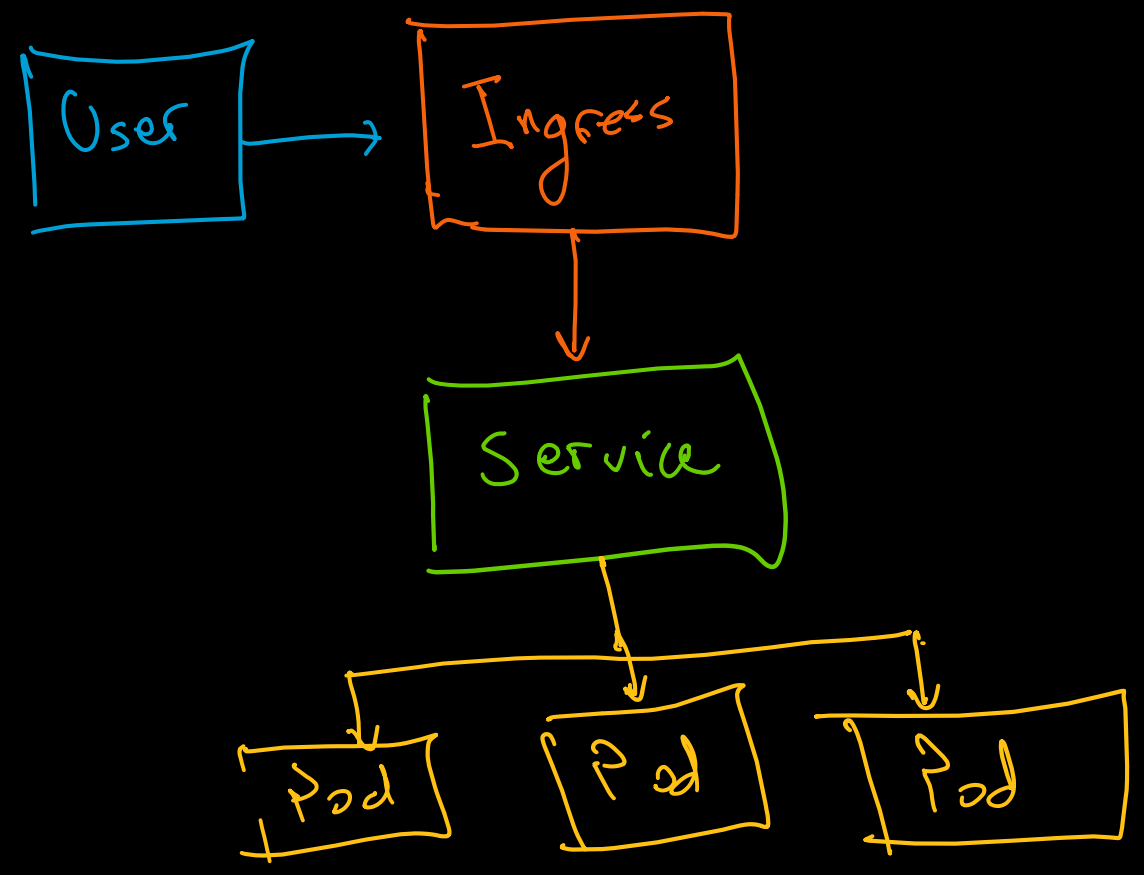
# Application Gateway for Containers

Houssem Dellai, CSA at Microsoft

# Kubernetes (old) Ingress




```yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: hello-world-ingress
  annotations:
    nginx.ingress.kubernetes.io/use-regex: "true"
spec:
  ingressClassName: nginx-app-02 # nginx
  tls:
  - hosts:
    - aks-app-02.westeurope.cloudapp.azure.com
    secretName: tls-ingress-app-02-secret
  rules:
  - host: aks-app-02.westeurope.cloudapp.azure.com
    http:
      paths:
      - path: /hello-world-one(/|$)(.*)
        pathType: Prefix
        backend:
          service:
            name: aks-helloworld-one
            port:
              number: 80
      - path: /hello-world-two(/|$)(.*)
        pathType: Prefix
        backend:
          service:
            name: aks-helloworld-two
            port:
              number: 80
```

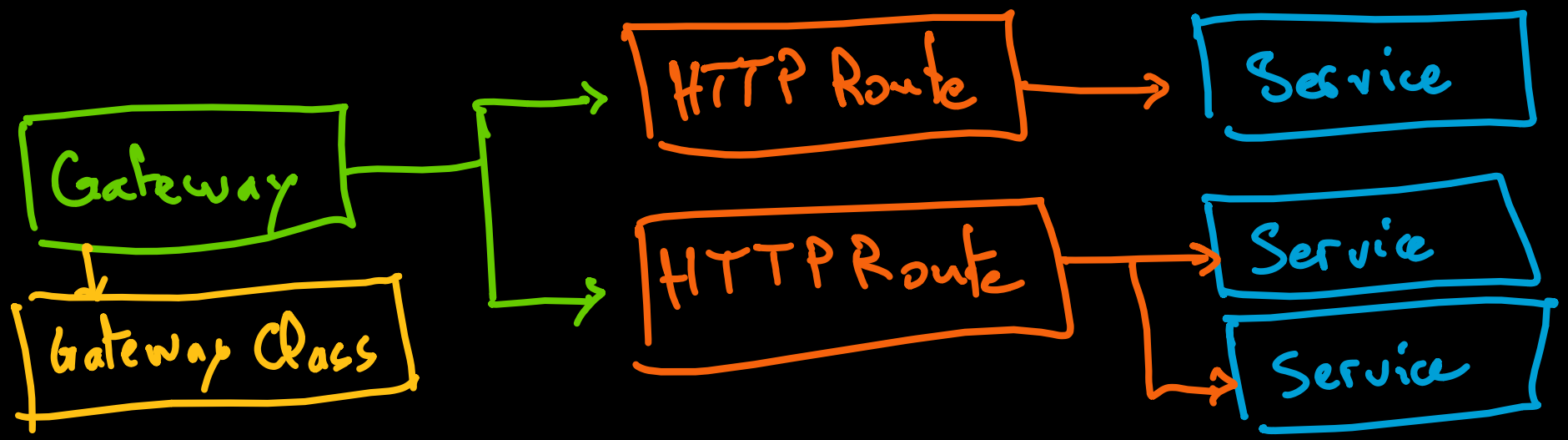
# What is Gateway API

An open-source project managed by the SIG-NETWORK community.

An API (collection of resources) that model service networking in Kubernetes.

These resources are **GatewayClass, Gateway, HTTPRoute, TCPRoute, Service**, etc.

Aim to evolve Kubernetes service networking through expressive, extensible, and role-oriented interfaces that are implemented by many vendors and have broad industry support.



# Gateway API project on Github

kubernetes-sigs / gateway-api

Type / to search

Code | Issues 124 | Pull requests 27 | Discussions | Actions | Projects 3 | Security | Insights

gateway-api Public

generated from kubernetes/kubernetes-template-project

Watch 61 | Fork 313 | Starred 1.1k

main | 5 branches | 26 tags | Go to file | Add file | Code

k8s-ci-robot Merge pull request #2255 from dprotaso/remove-routability-api ... f2b55c8 16 hours ago 2,949 commits

| | | |
|---|---|---|
| .github | docs: emphasis on GEP discussion process | 2 months ago |
| apis | remove routability from the go types | 19 hours ago |
| cmd/admission | Bump k8s.io to v0.27.1 (#1956) | 3 months ago |
| config | remove routability from the go types | 19 hours ago |
| conformance | remove routability from the go types | 19 hours ago |
| docker | Attempting to fix/understand broken presubmits | 2 months ago |
| docs | Linking from GitHub Pages to Netlify, removing generated docs from re... | 2 years ago |
| examples | drop routability examples | 16 hours ago |
| geps | Move GEP-1651 to Provisional | 19 hours ago |
| hack | drop routability examples | 16 hours ago |
| pkg | adding support for more than one mirror backends + adding clarificati... ( | last week |
| site-src | Merge pull request #2191 from david-martin/api-gateway-wording | last week |
| tools | Fix codegen script to work with Go modules. | 3 years ago |

**About**

Repository for the next iteration of composite service (e.g. Ingress) and load balancing APIs.

gateway-api.sigs.k8s.io

**Releases** 24

v0.7.1 Latest
on Jun 1

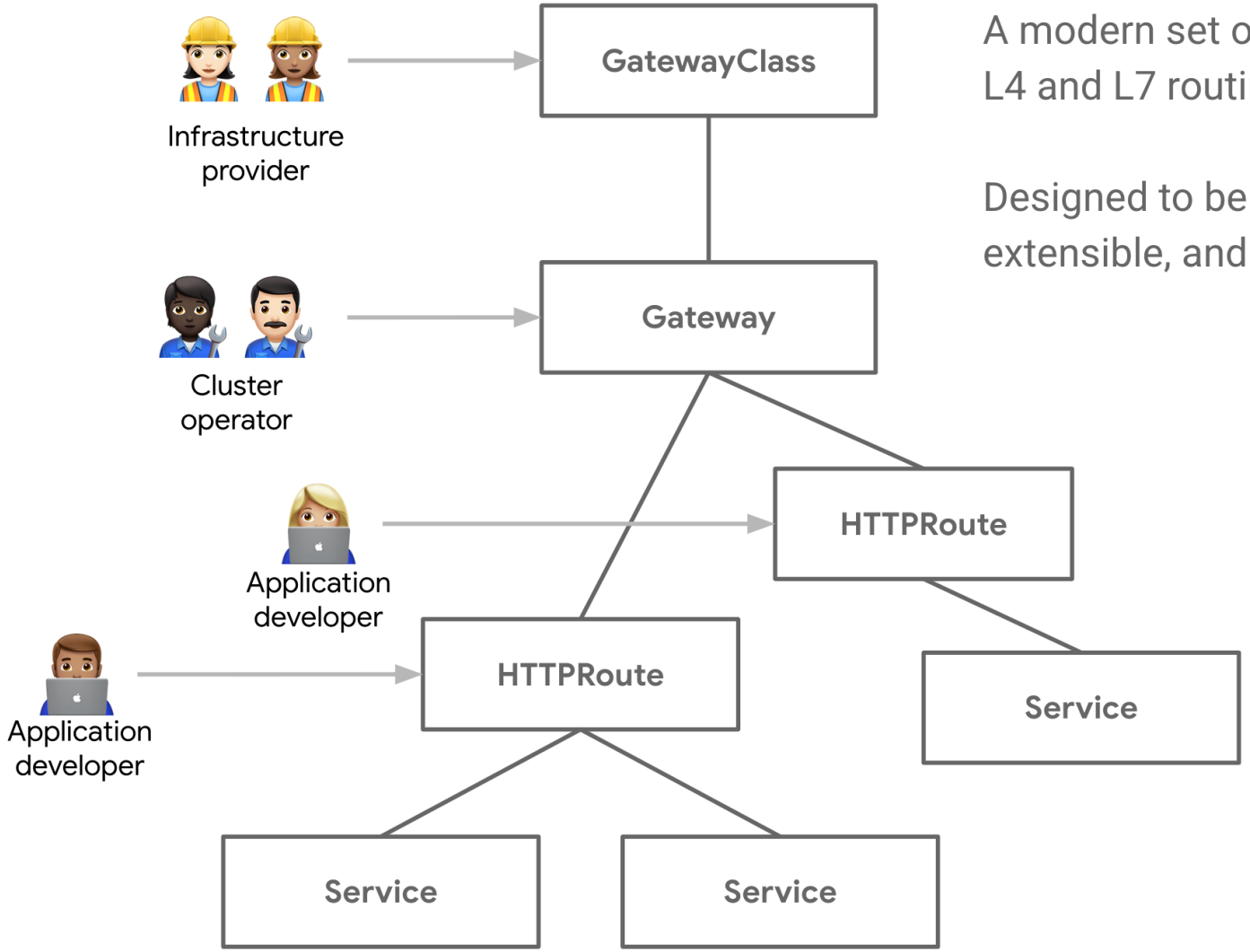
+ 23 releases

**Contributors** 160

+ 149 contributors

github.com/kubernetes-sigs/gateway-api

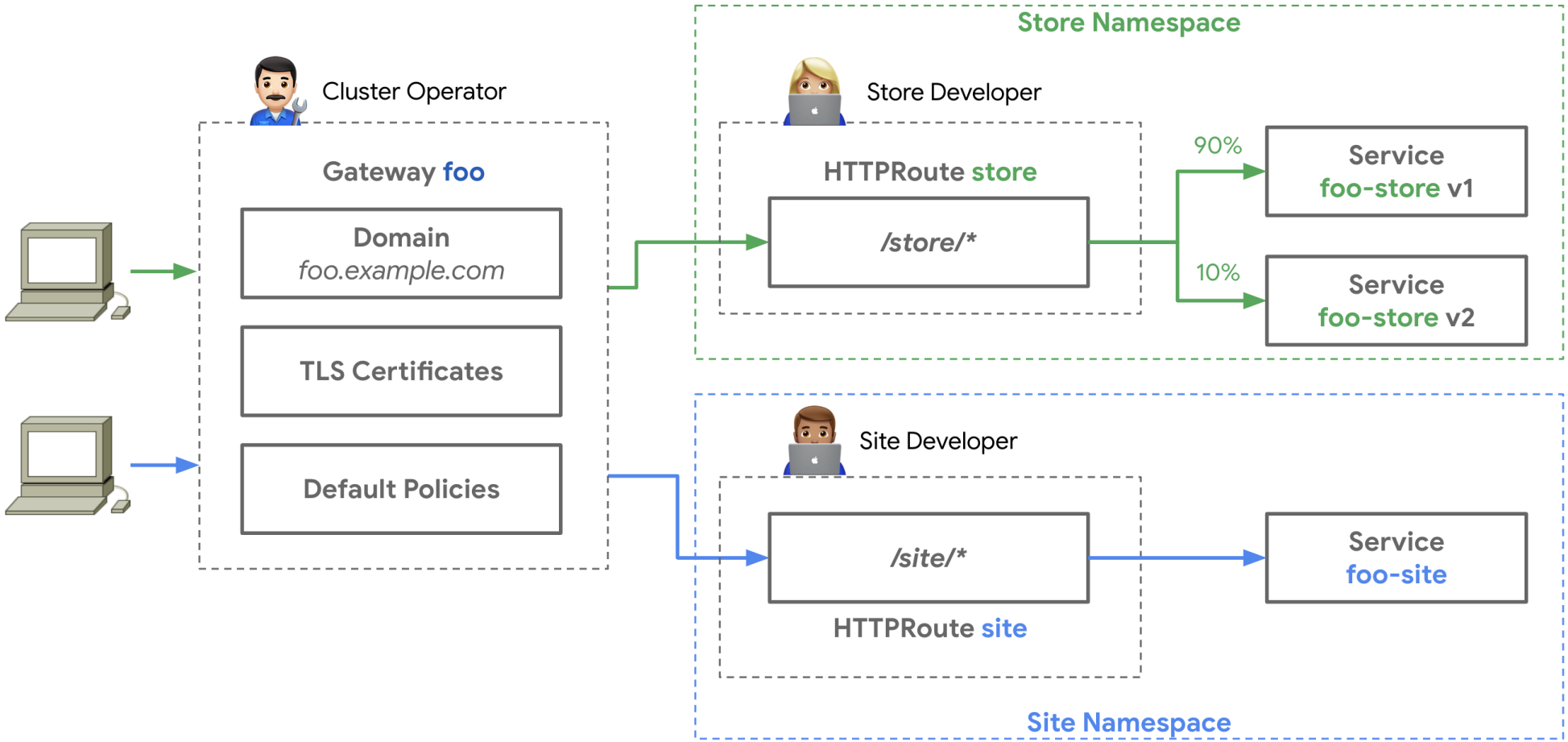
# Gateway API components and owners




A modern set of APIs for deploying L4 and L7 routing in Kubernetes

Designed to be generic, expressive, extensible, and role-oriented

# Gateway API role oriented (RBAC) model



# Gateway API implementations

**Azure Application Gateway for Containers (preview)**

Amazon Elastic Kubernetes Service (alpha)

Google Kubernetes Engine (GA)

NGINX Kubernetes Gateway

BIG-IP Kubernetes Gateway (beta)

Emissary-Ingress (Ambassador API Gateway) (alpha)

HAProxy Ingress (alpha)

Cilium (beta)

Contour (beta)

HashiCorp Consul

Istio (beta)

Kong (beta)

Traefik (alpha)

Envoy Gateway (alpha)

HAProxy Ingress (alpha)

gateway-api.sigs.k8s.io/implementations/

# Load Balancing Portfolio

**Standard Load Balancer**

VM/VMSS/AKS workloads
L4 passthrough LB
Regional/Global

**Application Gateway**

VM/VMSS/Hybrid workloads
L7 regional LB
TCP/TLS proxy
WAF

**Front Door**

VM/VMSS/Hybrid workloads
L7 global LB
TCP/TLS proxy
WAF

**Application Gateway for Containers**

**AKS/container workloads**

Dynamic traffic shifting
L7 Ingress Controller
Regional/Global
WAF

# Application Gateway for Containers

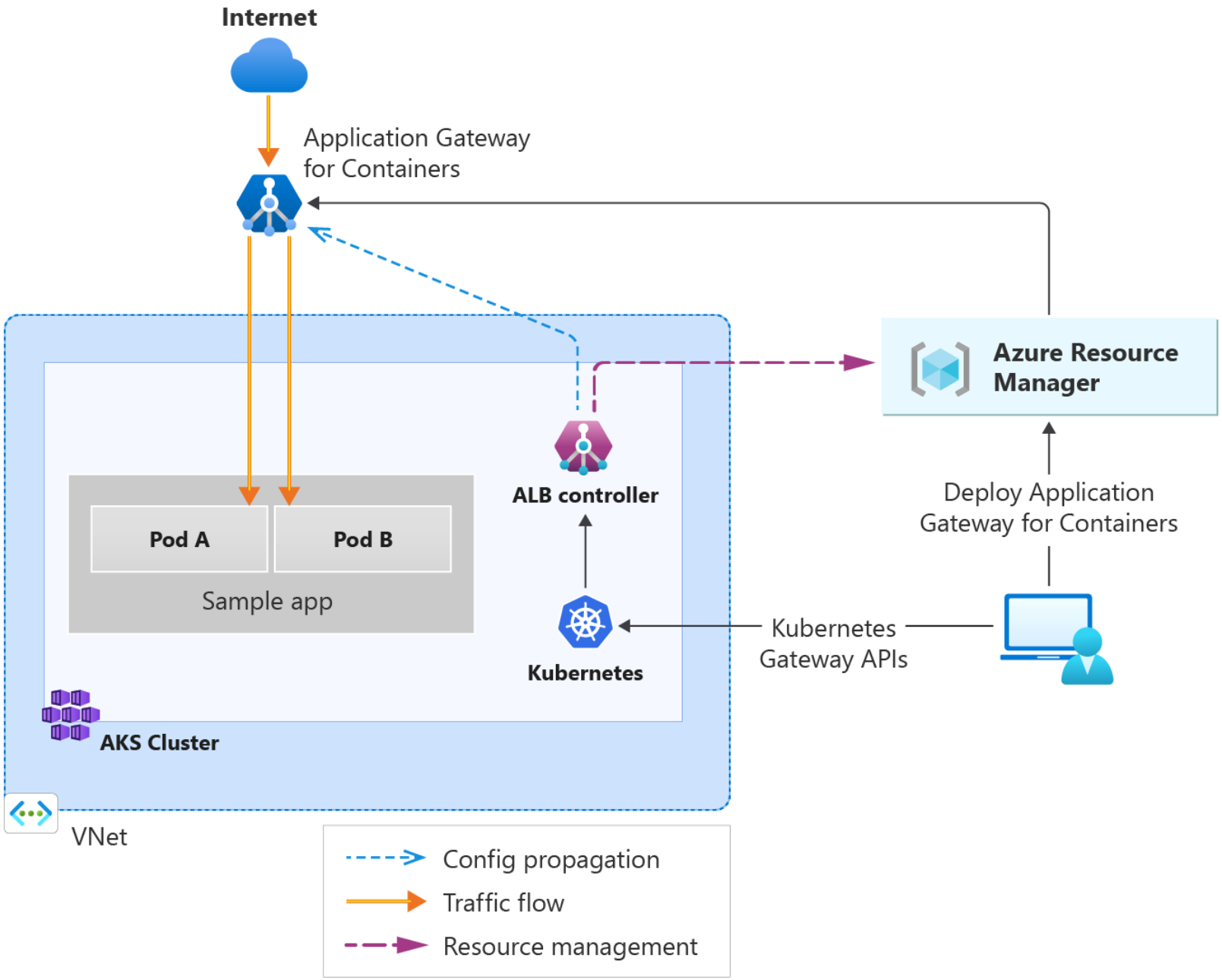
New **application load balancing (layer 7)** and dynamic traffic management for AKS.

New offering under the **Application Gateway** product family.

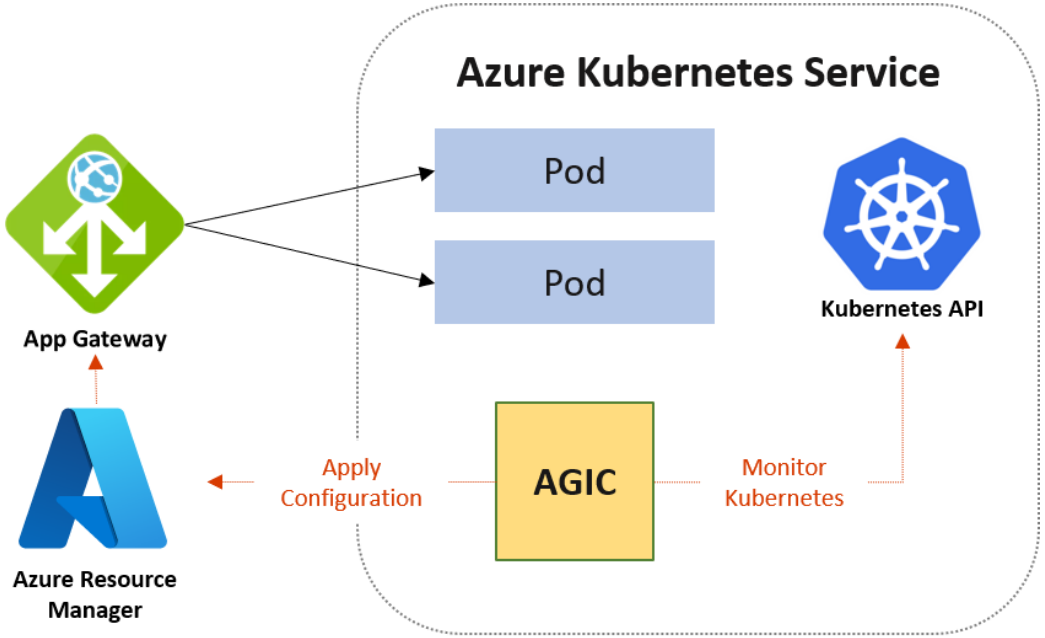
The evolution of the **Application Gateway Ingress Controller (AGIC).**

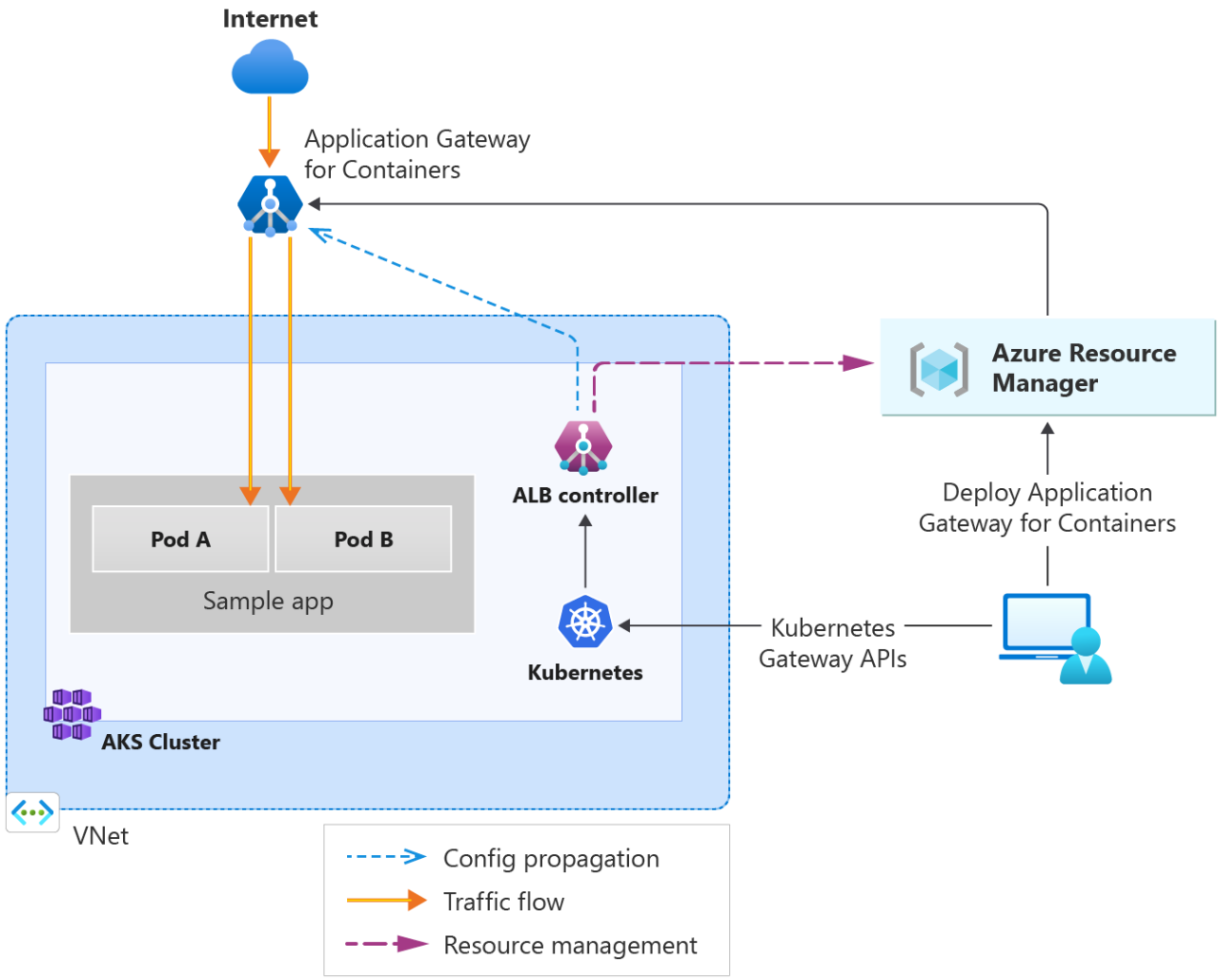
| Name | Type | Location |
|---|---|---|
| agwc-alb | Application Gateway for Containers | West Europe |
| aks-cluster | Kubernetes service | West Europe |
| identity-azure-alb | Managed Identity | West Europe |

# Application Gateway for Containers architecture



# Application Gateway for Containers vs App Gateway/AGIC



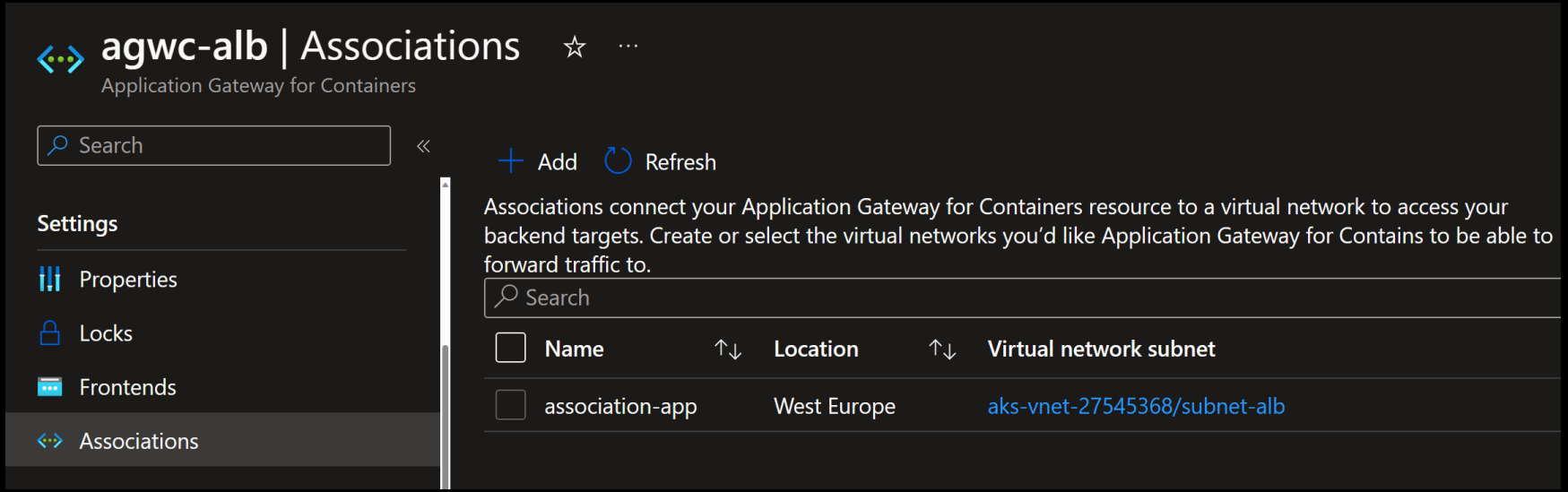



# Application Gateway for Containers components

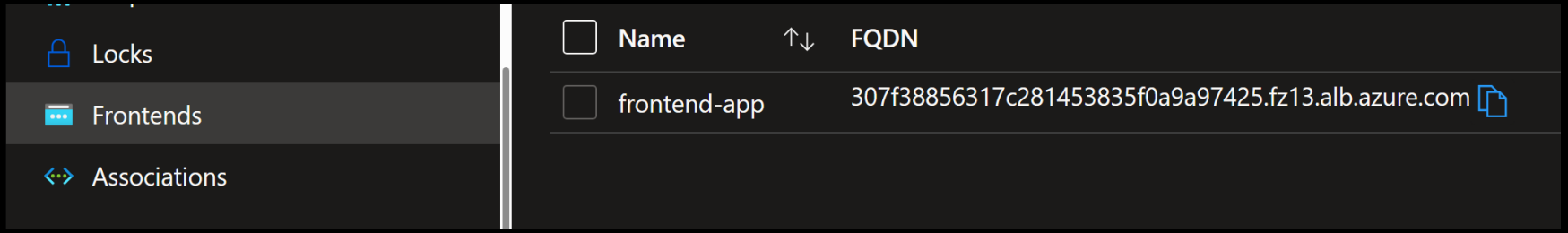
## ALB Controller

```
$
$ kubectl get all -n azure-alb-system
NAME                                          READY   STATUS    RESTARTS   AGE
pod/alb-controller-764cf9ccdf-hf8v6           1/1     Running   0          31h
pod/alb-controller-bootstrap-5c6c59c7b8-cspg7 1/1     Running   0          31h
```

## Associations




## Frontends



# Application Load Balancer (ALB) Controller

ALB is a Kubernetes deployment installed via Helm chart.

**Creates the App Gateway for Containers** if using the BYO (managed) mode when an ApplicationLoadBalancer custom resource is defined on the cluster.

The service lifecycle is based on the lifecycle of the custom resource.

Supports **Workload Identity** and Managed Identity (UMI).

Watches CRD resources like **Ingress, Gateway & ApplicationLoadBalancer**.

**Propagates configuration** to the App Gateway for Containers.

# Application Load Balancer (ALB) Controller

Two running pods inside **azure-alb-system** namespace.

1. **alb-controller pod** propagates configuration to Application Gateway for Containers
2. **alb-controller-bootstrap pod** is responsible for management of CRDs.

```
 $
 $ kubectl get all -n azure-alb-system
NAME                                          READY   STATUS    RESTARTS   AGE
pod/alb-controller-764cf9ccdf-hf8v6           1/1     Running   0          31h
pod/alb-controller-bootstrap-5c6c59c7b8-cspg7 1/1     Running   0          31h

NAME                                 TYPE        CLUSTER-IP     EXTERNAL-IP   PORT(S)    AGE
service/alb-controller               ClusterIP   10.0.126.102   <none>        8000/TCP   31h
service/alb-controller-bootstrap     ClusterIP   10.0.91.170    <none>        9005/TCP   31h

NAME                                       READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/alb-controller             1/1     1            1           31h
deployment.apps/alb-controller-bootstrap   1/1     1            1           31h
```

# Application Load Balancer (ALB) Controller logs

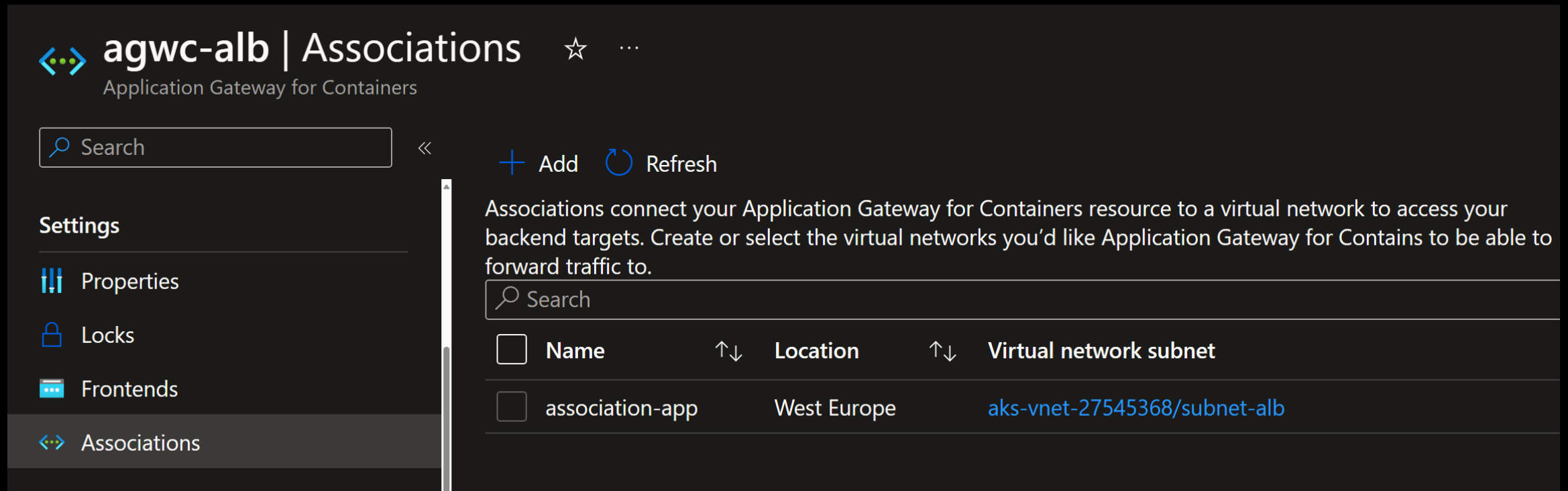
```
kubectl logs pod/alb-controller-764cf9ccdf-hf8v6 -n azure-alb-system
```


```
{"level":"info","component":"lb-resources-reconciler","Timestamp":"2023-08-
03T19:12:41.47807995Z","caller":"/__w/1/s/alb-
controller/k8s/reconcilers/reconcile.go:142","message":"Successfully processed object test-
infra/gateway-01"}
{"level":"info","component":"armclient-logger","Timestamp":"2023-08-
03T19:12:41.508898212Z","caller":"/__w/1/s/pkg/armclient/armclient
.go:161","message":"Creating Application Gateway for Containers resource alb-eed2f86a from CRD alb-
infra/alb-appgw-containers in RG mc_rg-aks_aks-cluster_westeurope"}
{"level":"info","component":"armclient-logger","Timestamp":"2023-08-
03T19:13:53.094882916Z","caller":"/__w/1/s/pkg/armclient/armclient
.go:271","message":"Getting association as-25e7ea3b for Application Gateway for Containers resource
/subscriptions/xxxx/resourceGroups/mc_rg-aks_aks-
cluster_westeurope/providers/Microsoft.ServiceNetworking/trafficControllers/alb-eed2f86a"}
{"level":"info","component":"lb-resources-reconciler","Timestamp":"2023-08-
03T19:31:05.834265509Z","caller":"/__w/1/s/alb-
controller/k8s/reconcilers/reconcile.go:142","message":"Successfully processed object ns-app/httproute-
app"}
```

# Application Gateway for Containers associations

Defines a connection point into a virtual network.

1:1 mapping of an association resource to a delegated Azure Subnet.

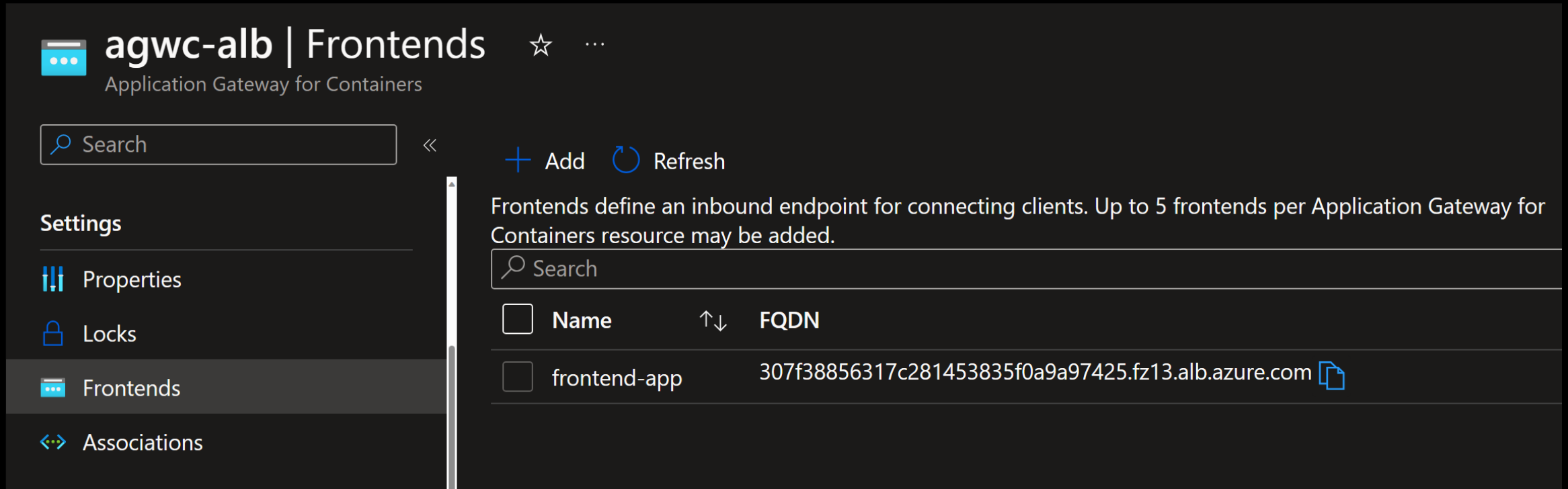


# Application Gateway for Containers frontends

Defines the entry point client traffic should be received by a given AppGwC.

Each frontend provides a unique FQDN.

A single AppGwC support multiple frontends.



# Azure Application Gateway for Containers benefits

- **Traffic splitting** / Weighted round robin
- Mutual authentication (**mTLS**) to the backend target
- Kubernetes **support for Ingress and Gateway API**
  - AGIC only supports Ingress
- Better RBAC model for **separation of concerns**
- **Near real-time updates** to add or move pods, routes, and probes

# Sample resources

```yaml
apiVersion: gateway.networking.k8s.io/v1beta1
kind: Gateway
metadata:
  name: gateway-app
  namespace: ns-gateway
  annotations:
    alb.networking.azure.io/alb-id: appgwc_resId
spec:
  gatewayClassName: azure-alb-external
  listeners:
  - name: http-listener
    port: 80
    protocol: HTTP
    allowedRoutes:
      namespaces:
        from: All # Same
  addresses:
  - type: alb.networking.azure.io/alb-frontend
    value: frontend-app
```

```yaml
apiVersion: gateway.networking.k8s.io/v1beta1
kind: HTTPRoute
metadata:
  name: httproute-app
  namespace: ns-app
spec:
  parentRefs:
  - kind: Gateway
    name: gateway-app
    namespace: ns-gateway
  rules:
  - backendRefs:
    - name: svc-app
      port: 80
```