Kubernetes

2021.11
v1.0

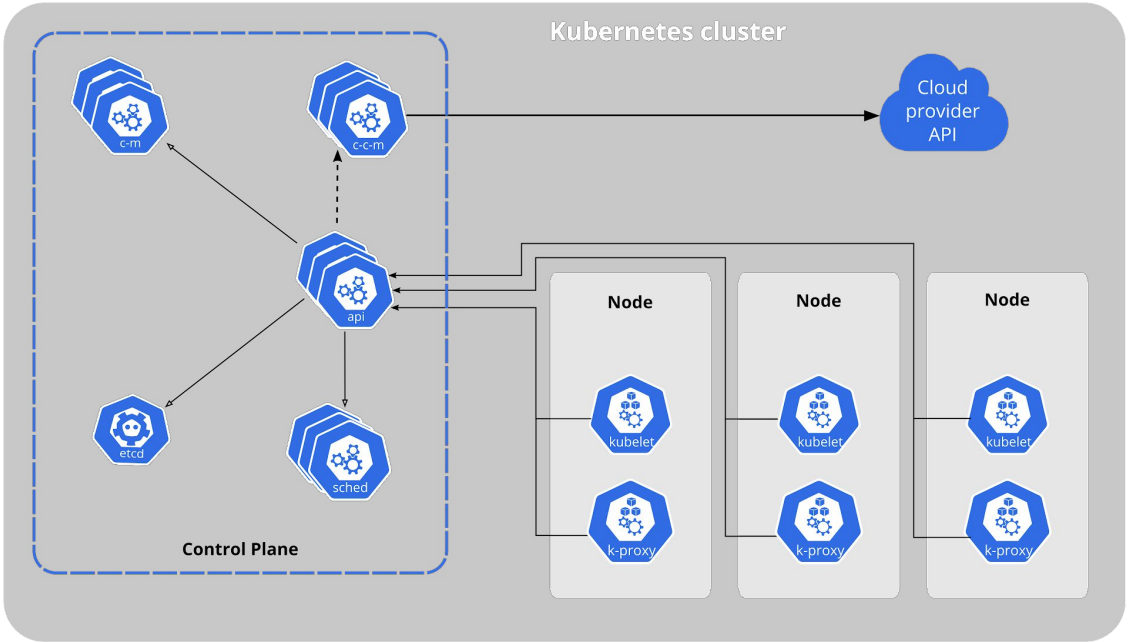
kubernetes

Présentation générale

Architecture

kubernetes

Control Plane



API server

Cloud controller manager *(optional)*

Controller manager

etcd (persistence store)

kubelet

kube-proxy

Scheduler

Control plane

Node

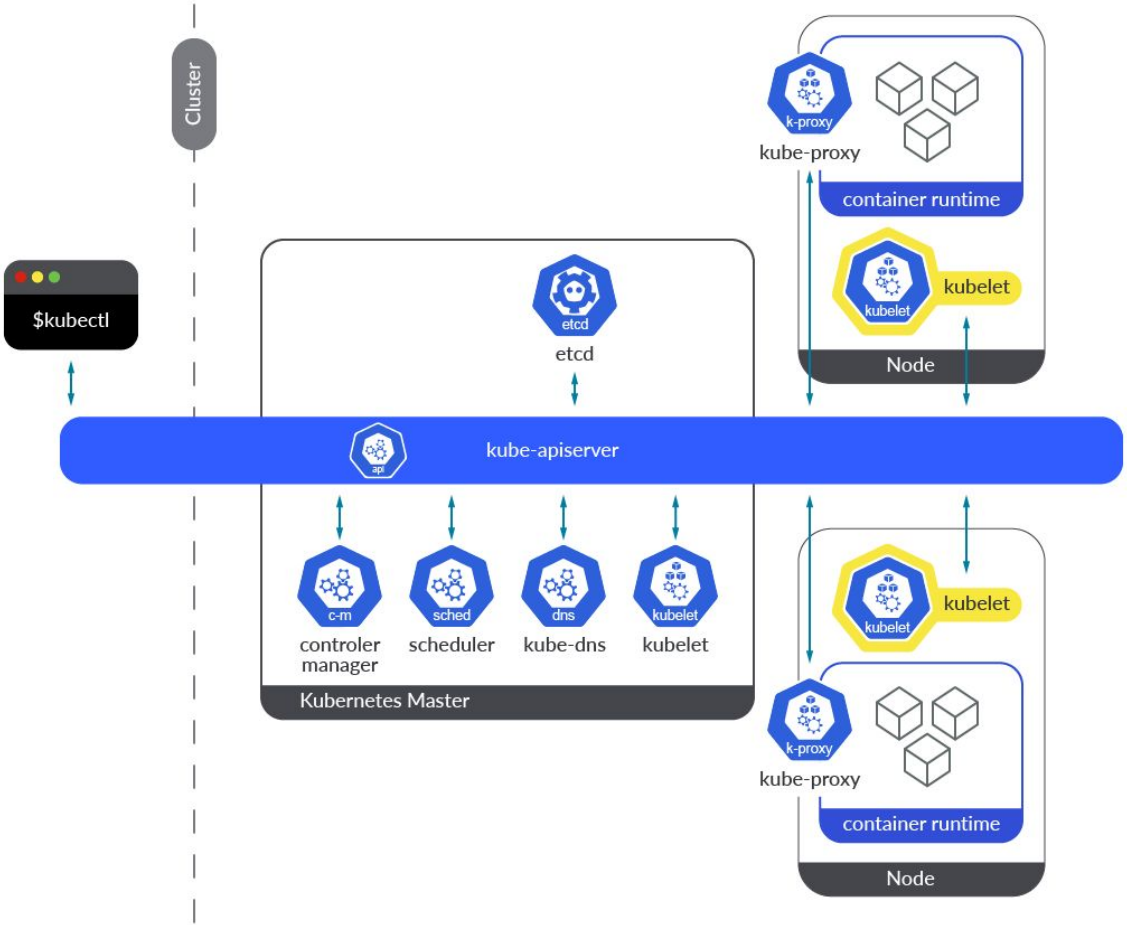
kubernetes

Control Plane

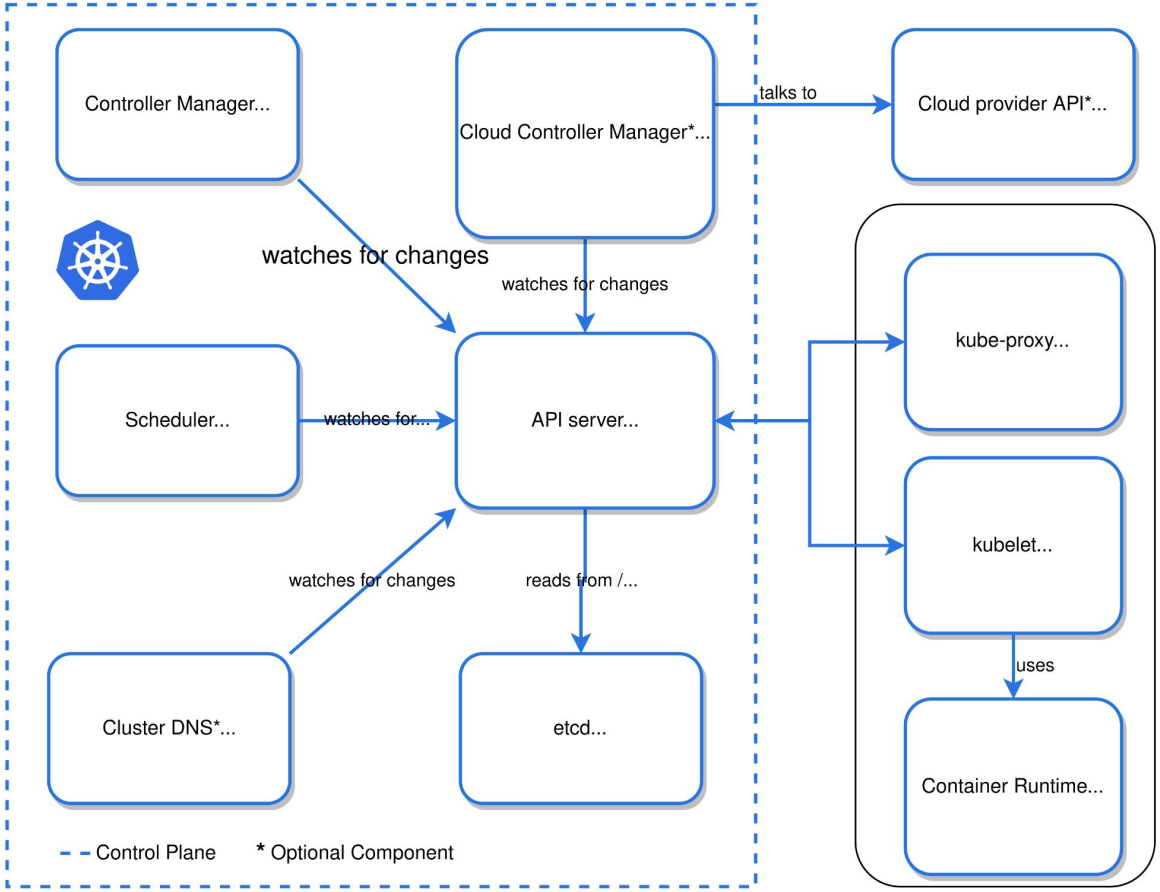
- Etcd
  - Persistence des données du cluster : clé/valeur distribuée, protocole RAFT
- APIServer
  - Serveur qui permet la configuration d'objet Kubernetes (Pods, Service, Replication Controller, ...)
  - Tous les communications du cluster passent par l'API Server
  - Gère l'authentification, l'autorisation, la validation de la demande, le contrôle d'admission
- Controller Manager
  - Gère les différents contrôleurs du cluster (NodeController, ReplicationController, EndpointController, ...
- Scheduler
  - S'occupe de trouver un noeud pour déployer un POD

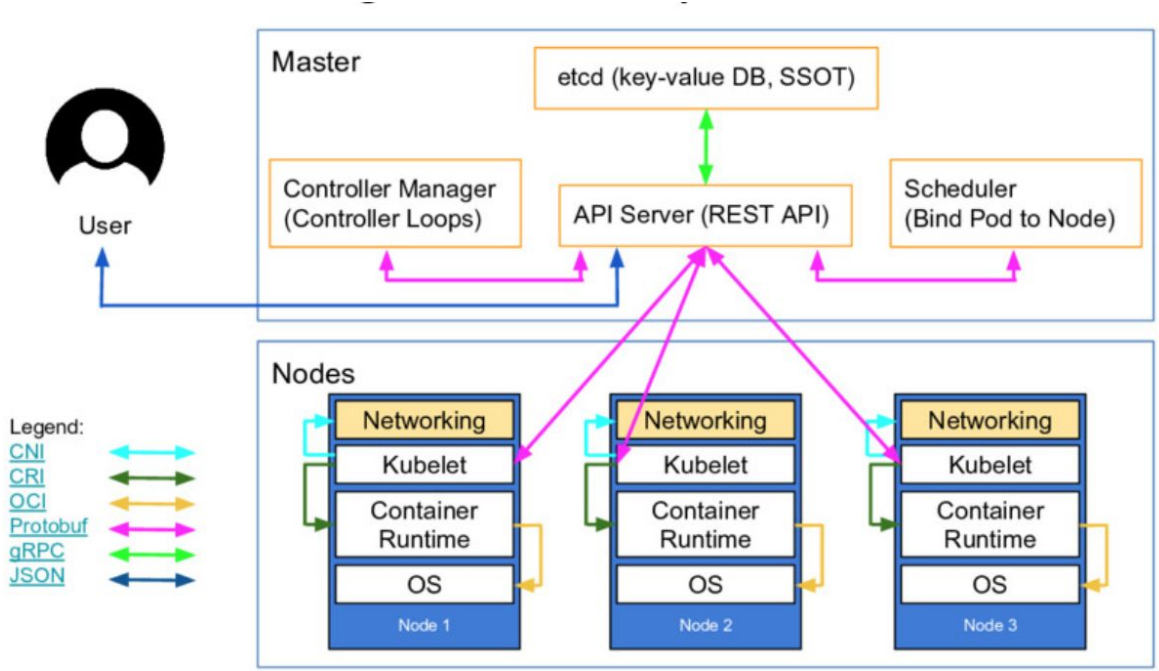
Composants des noeuds

- Kubelet
  - Crée et gère les conteneurs. Contacté par l'API Server
- Kube-proxy
  - Gère les règles réseaux sur chaque noeud
  - Forwarding TCP/UDP et Load balancing entre les services et les backend
- Container Runtime Interface (CRI)
  - Exécute les conteneurs :
  - Containerd (default), Cri-o, gVisor, Kata, Docker (Deprecated)
- Container Network Interface (CNI)
  - Allocation des adresses IP des conteneurs
  - Gestion de l'interface réseau qui va porter le conteneur
  - Cilium (GKE v2), Flannel, Weave, …
- Container Storage Interface (CSI)
  - Création, redimensionnement, attachement, montage […] des volumes
  - Secrets


Cluster
$kubectl
etcd
etcd
kube-apiserver
c-m
controler manager
sched
scheduler
dns
kube-dns
kubelet
kubelet
Kubernetes Master
k-proxy
kube-proxy
container runtime
kubelet
kubelet
Node
kubelet
kubelet
k-proxy
kube-proxy
container runtime
Node

Kubernetes Architecture




Master
etcd (key-value DB, SSOT)
Controller Manager
(Controller Loops)
API Server (REST API)
Scheduler
(Bind Pod to Node)
User
Nodes
Networking
Kubelet
Container
Runtime
OS
Node 1
Networking
Kubelet
Container
Runtime
OS
Node 2
Networking
Kubelet
Container
Runtime
OS
Node 3
Legend:
CNI
CRI
OCI
Protobuf
gRPC
JSON

Administration

kubernetes

Outillage

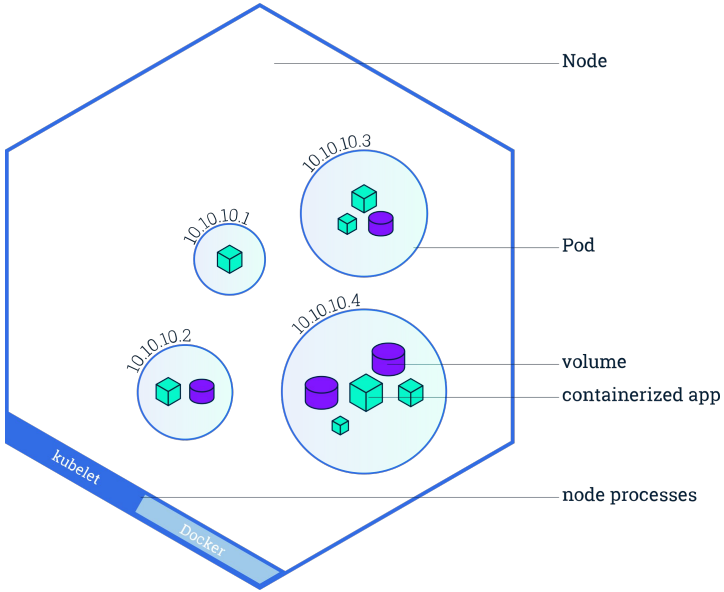
- Module Terraform par Google
- Kubectl - CLI officiel
- Kustomize / Helm
- Gcloud
- Krew - The package manager for kubectl plugins

kubernetes

Workloads

Pod

- C’est la plus petite unité schedulable
- Un pod est composé de 1 à N conteneurs
- Conteneurs:
  - Même namespace réseau (127.0.0.1)
  - Partage un espace de stockage commun
- Pod solitaire :
  - Aucun contrôle up/running
  - Il faut créer un Workload



kubernetes

Workload

- Deployment
  - Probablement le workload le plus utilisé dans Kubernetes
  - S’occupe du rolling update des pods lors d’un update (par un ReplicaSet)
- StatefulSet
  - Utilisé pour les applications avec état (cache, écriture disque, clustering, …)
  - Chaque pod a un identifiant persistant qu'il conserve lors de toute replanification
- DaemonSet
  - Place exactement 1 pod par node
  - Utile pour les agents de logging par exemple
- Cronjob / Job
  - Action ponctuelle ou répétitive

Requests / Limits

- Mécanismes utilisés pour contrôler les ressources processeur et la mémoire.

- Requests :
  - le conteneur est garanti d'obtenir.
  - le conteneur sera planifié que sur un nœud qui peut lui donner cette ressource.

- Limits :
  - le conteneur ne dépasse jamais une certaine valeur.
  - OOMKilled !

Probes

- Kubelet :
  - liveness : pour détecter si le pod est vivant
  - readiness : pour savoir si le pod est prêt à accepter le trafic
  - startup : démarrage des applications legacy

- Gèle le rolling update si l'application : ne démarre pas ou n'est pas prête

- Ne pas vérifier les éléments externes de l'application
  - Memcached, DB, etc …

ConfigMap

- Pour stocker et de gérer des informations
- Utilisation :
  - variables d'environnements
  - volumes

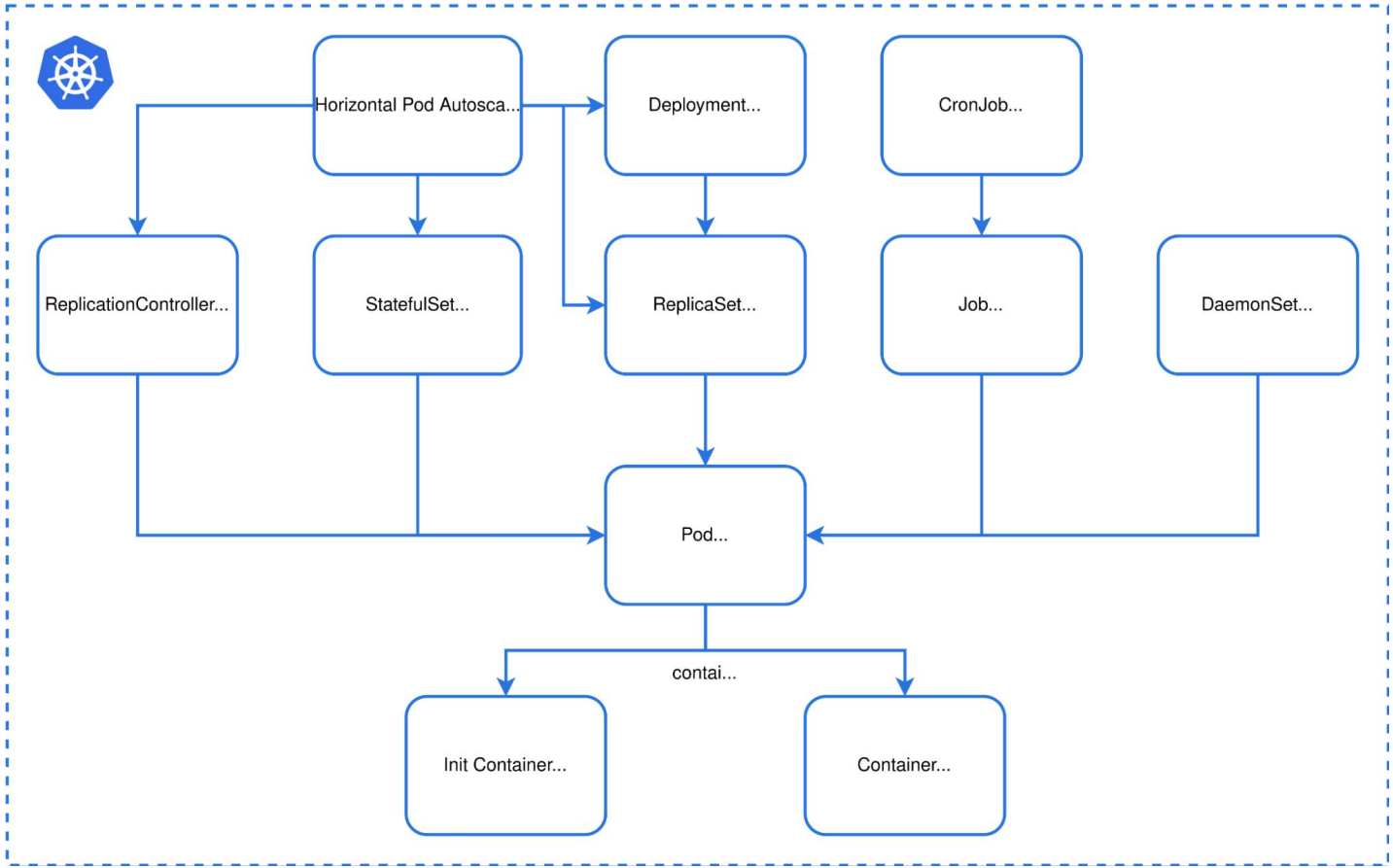
kubernetes

Secrets

- Pour stocker et de gérer des informations sensibles (Base 64 !!!)
  - Kubernetes Secrets Store CSI Driver
  - Outils externes : Sops, Sealed Secrets
- Types :
  - Opaque : secret définit par un utilisateur
  - kubernetes.io/service-account-token : service account token
  - kubernetes.io/dockercfg : fichier ~/.dockercfg sérialisé
  - kubernetes.io/dockerconfigjson : fichier ~/.docker/config.json sérialisé
  - kubernetes.io/basic-auth : basic authentication
  - kubernetes.io/ssh-auth : authentification SSH
  - kubernetes.io/tls : TLS pour un client ou serveur
  - bootstrap.kubernetes.io/token : bootstrap token
- Utilisation
  - variables d'environnements
  - volumes

kubernetes

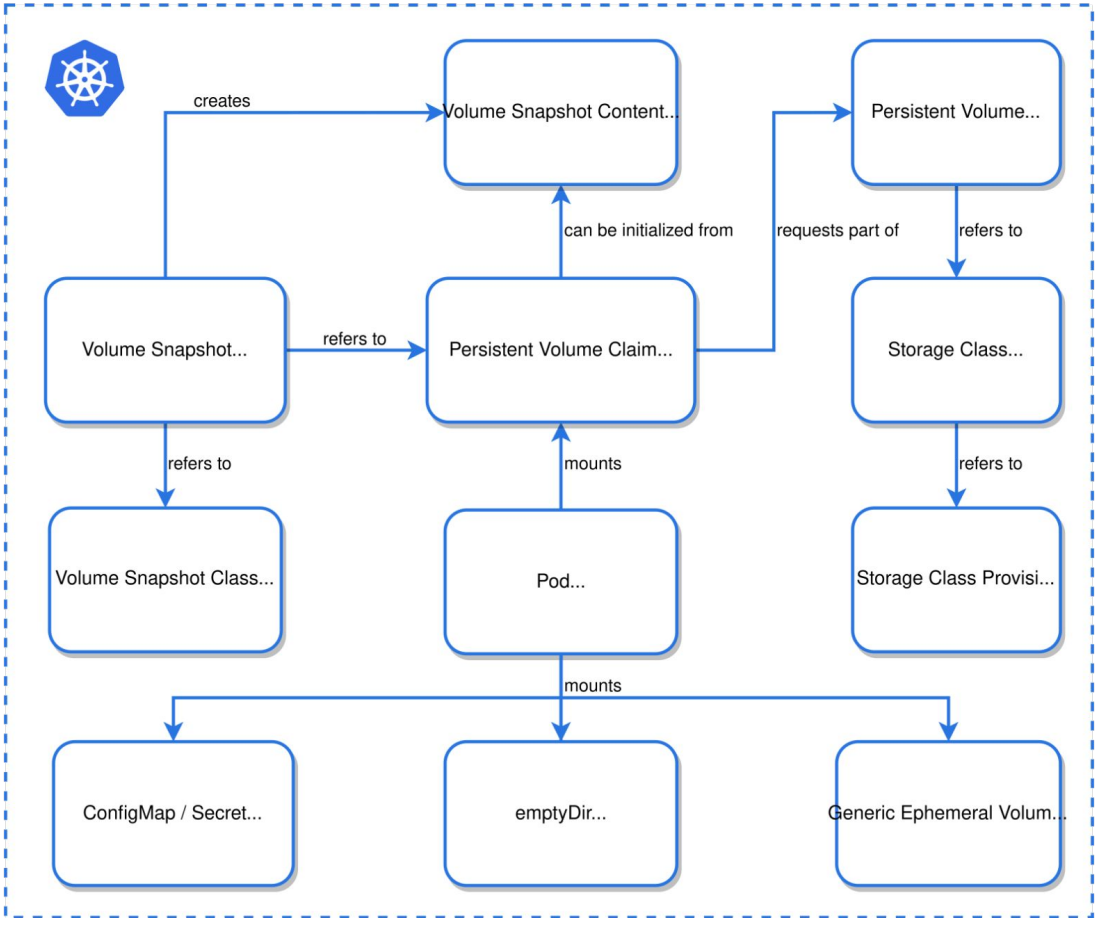
Kubernetes Workload Objects



Stockage

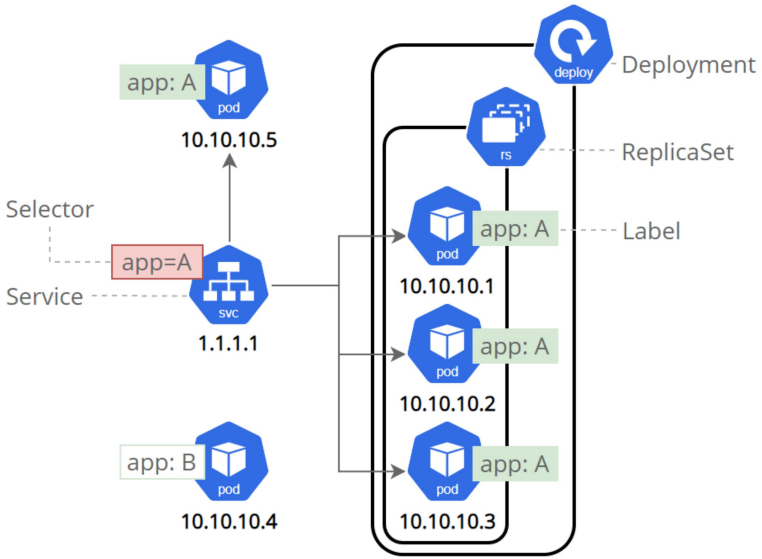
- StorageClass : définit plusieurs offre de stockage
  - des niveaux de qualité de service
  - des politiques de sauvegarde
- PersistentVolume :
  - élément de stockage dans le cluster
  - provisionné par un administrateur ou provisionné dynamiquement à l'aide de Storage Classes
- PersistentVolumeClaim : est une demande de stockage par un utilisateur
  - une taille
  - des modes d'accès spécifiques

Kubernetes Storage Objects



Service

- Définit un ensemble logique de pods
- Stratégie permettant d'y accéder
- Types de Service
  - None
  - ClusterIP
  - NodePort
  - LoadBalancer



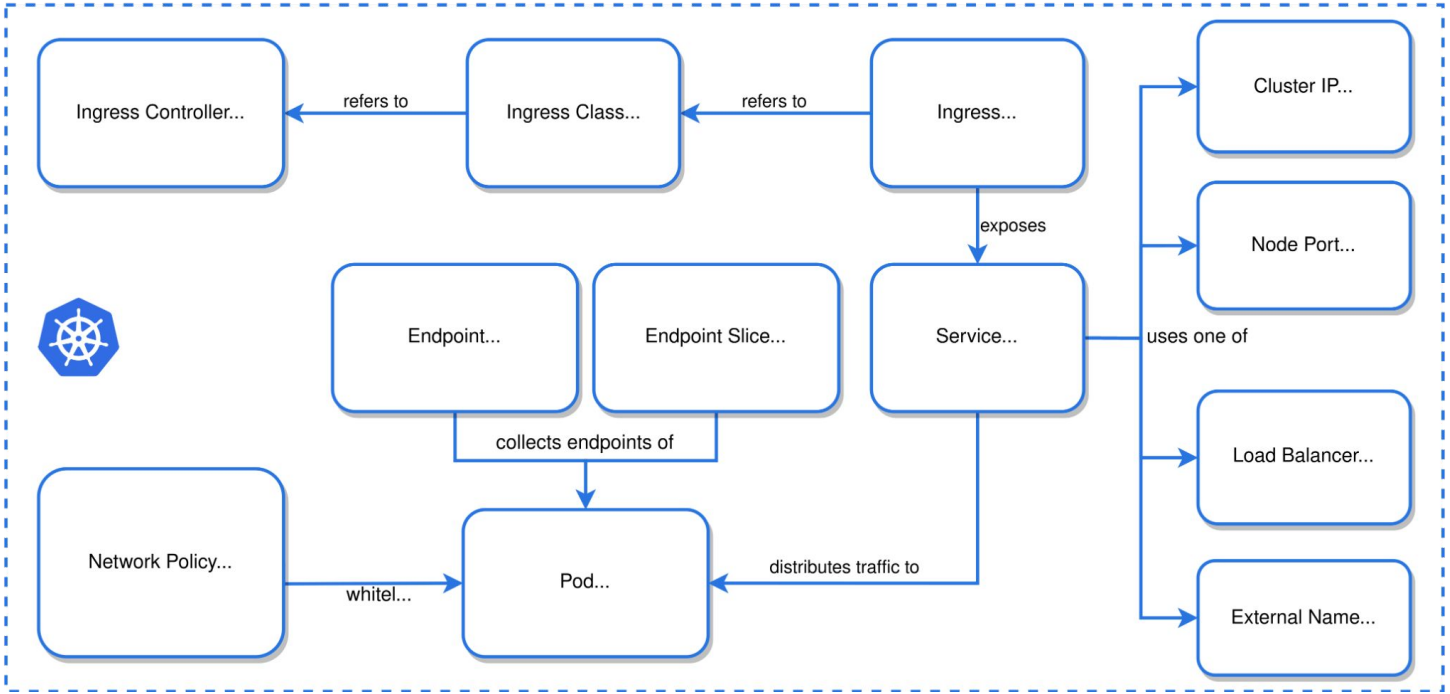
kubernetes

Ingress

- Expose les routes HTTP et HTTPS de l'extérieur du cluster à des services au sein du cluster
- Routage du trafic est contrôlé par des règles définies sur la ressource Ingress.
- Ingress Controller : Nginx, Traefik, Contour, HAProxy Ingress

kubernetes

Kubernetes Networking Objects



Namespace

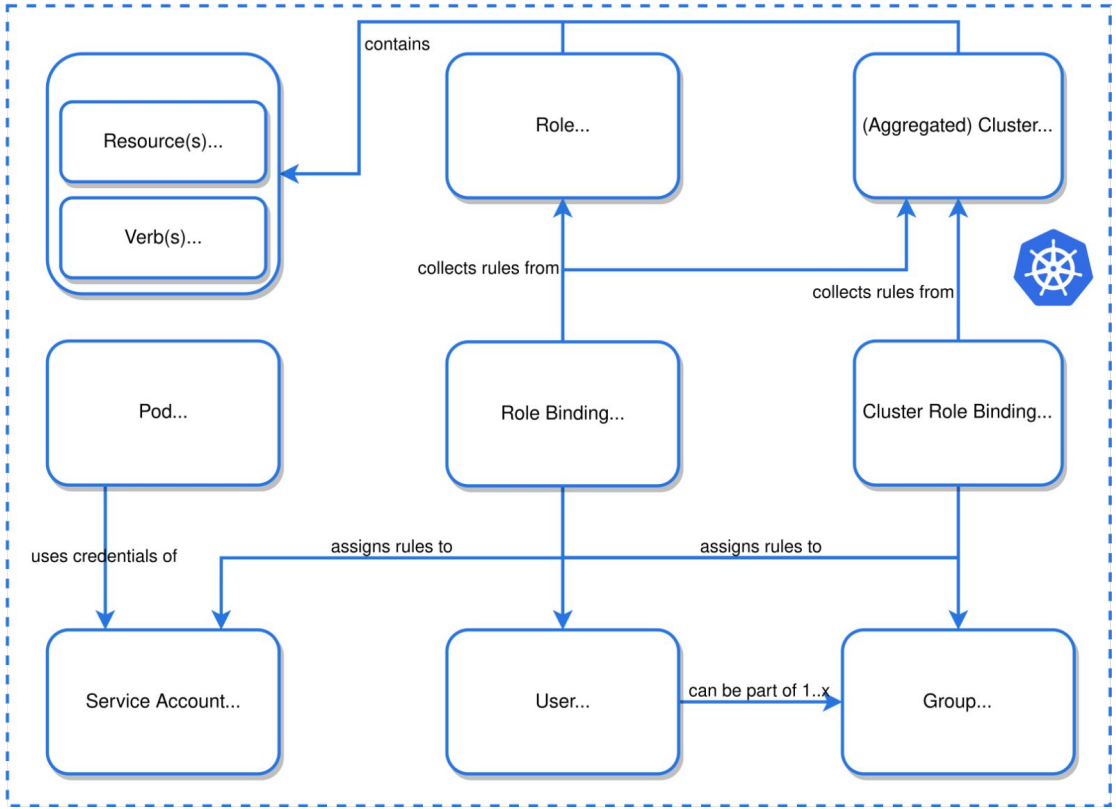
- Isolation logique des objets kubernetes
  - Par défaut les namespaces :
    - default
    - kube-system
      - kube-dns
      - kube-proxy
- On peut :
  - Limiter les ressources allouées (CPU / Memory / Pods..)
  - “Isoler” des groupes de pods / domaines métiers
- Bonne pratique :
  - Ne pas mettre les objets K8S dans le namespace default

Rbac

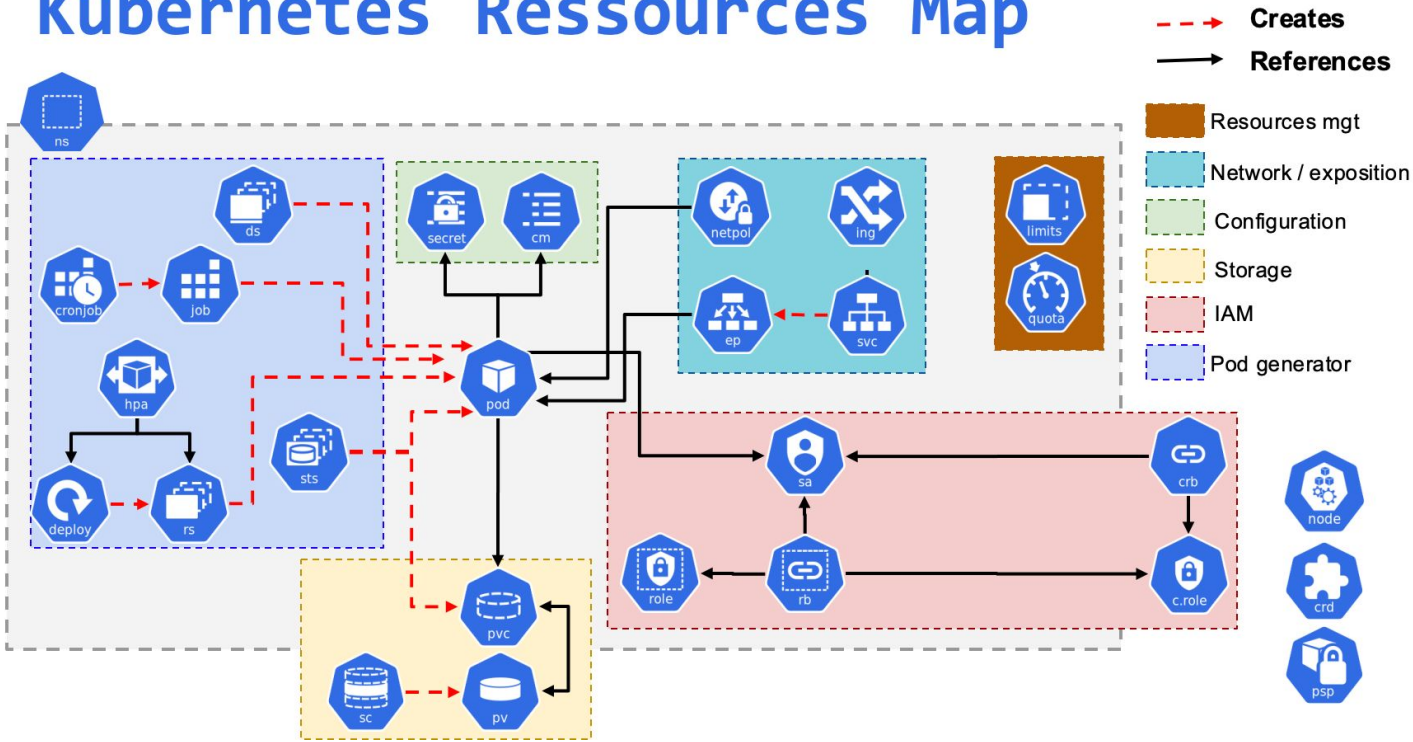
- Role :
  - gère l'accès à des ressources dans des namespaces.
- ClusterRole :
  - idem rôle
  - pour octroyer un accès à des ressources à l'échelle du cluster
- Subjects :
  - entité qui effectuera les opérations dans le cluster
  - ServiceAccount
  - User
- RoleBinding et ClusterRoleBinding :
  - liaison entre un sujet et un Role ou un ClusterRole.

kubernetes

Kubernetes RBAC Objects



Kubernetes Ressources Map



Questions