Rex Kubernetes 5G

Déployer un coeur de réseau 5G sur Kubernetes

Présenté par Modou DIOUF
Cloud & DevSecOps Engineer

Beopen IT®
<We love Tech>

Live Session
Vendredi 09 Décembre

Déployer un coeur de réseau 5G sur Kubernetes

Présenté par Modou DIOUF
Cloud & DevSecOps Engineer

> Rediffusion ici <

Beopen IT®

Conseils et développement de software.

- DevSecOps
- Cybersécurité
- Data, Ml & IA
- Formations K8S

kubernetes TRAINING PARTNER

THE LINUX FOUNDATION AUTHORIZED TRAINING PARTNER

Présenté par MODOU DIOUF
Cloud & DevSecOps engineer

Expériences
DevSecOps, DevOps

Technos & cloud
K8s, Golang, aws, gcp, azure

Déploiement d'un cœur de réseau 5G sur Kubernetes.

Introduction

1) Contexte

2) Du legacy au cloud Native

2.1) Virtualisation vs Conteneurisation
2.2) Architecture Monolithique vs Microservices

Les Grandes étapes

1) Networking

1.1) Architecture 5G Core
1.2) Choix CNI
1.3) Plateforme supporte SCTP Protocol
1.4) Gestion des Flux cluster (E/W et N/S)
1.5) Maillage de Service

2) Resources Management

3) Télémetrie

4) DevOps Stack

FAQ

1

Introduction

Cloud Native

Beopen IT <Formation K8S>

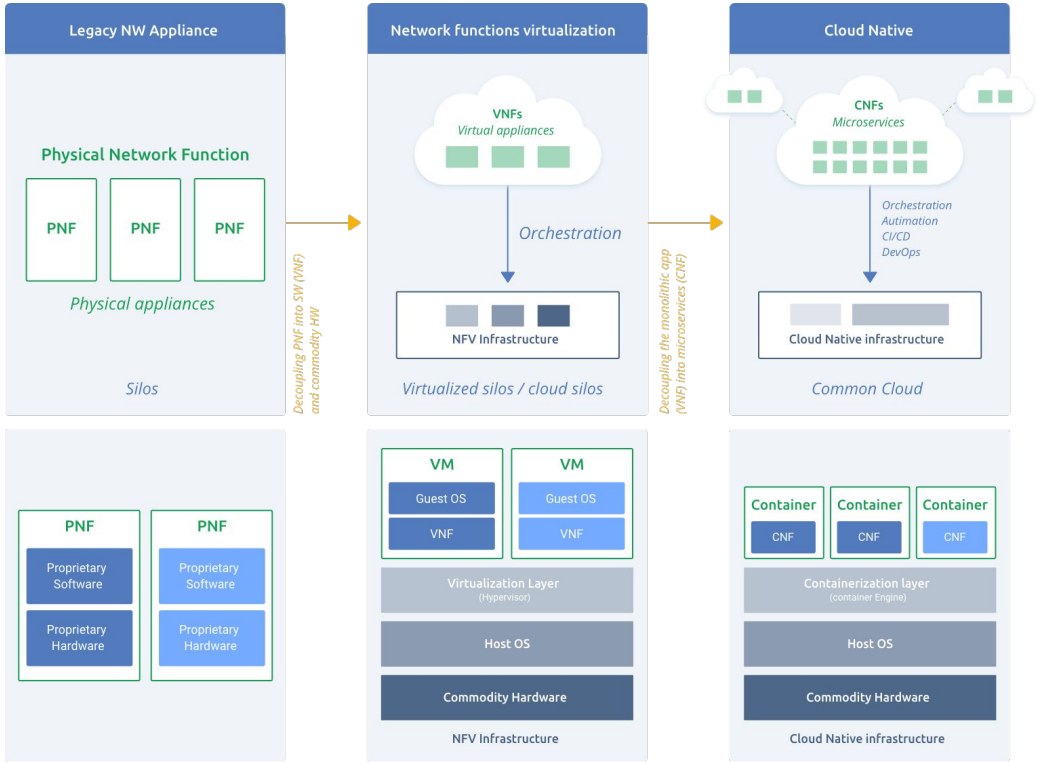
Déploiement d'un coeur de réseau 5G sur Kubernetes BeOpen IT©

Contexte et cas d'usage

Comment et pourquoi déployer un cœur de réseau 5G sur Kubernetes ?

Déploiement d'un coeur de réseau 5G sur Kubernetes BeOpen IT©

Du legacy au cloud Native



PNF

Physical Network Function

(routeur, firewall, appliance de sécurité...)

VNF

Virtual Network Function

(routeur, firewall, appliance de sécurité...)

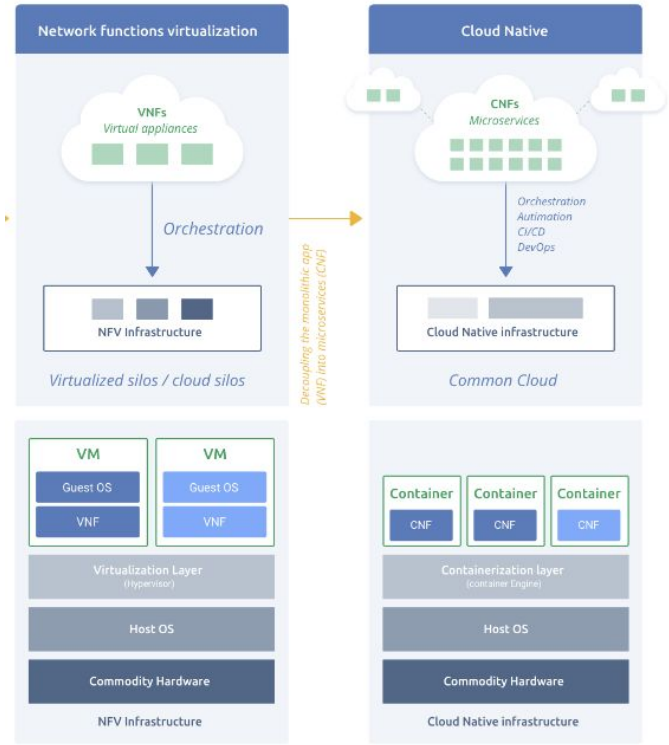
CNF

Container Network Function

(routeur, firewall, appliance de sécurité...)

Network Function

Du legacy au cloud Native: VM vs Containers



VNF

- Les VNFs sont implémentés sur de VMs et chacune a son propre OS.
- Les VMs partagent les ressources du cluster à travers l'hyperviseur.

CNF

- Les CNFs sont implémentés sur des architectures microservices, décomposé en petit bloc et emballé dans des conteneurs.
- Les conteneurs partages le noyau de la machine Hôte, ce qui réduit la surcharge au démarrage et les rends très légers

Architecture Applications Telco

Caracteristiques des CNF

CNF: Contaniers Network Functions

Couplage **Microservices**

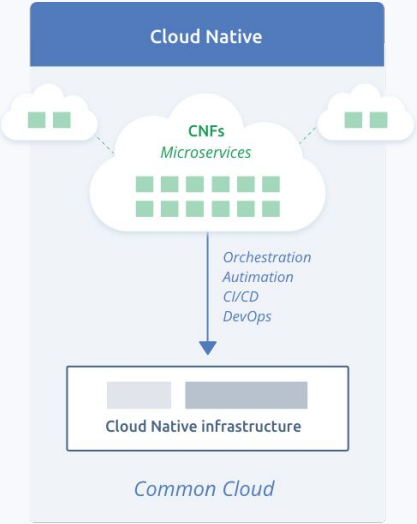
Une infrastructure élastique et une mise à l'échelle efficace.

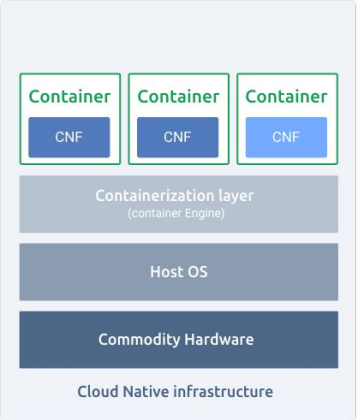
Emballage **Conteneurisé**

Les CNFs sont des conteneurs légers

Gestion **Agile** **DevOps**

Workflows CI/CD pour automatiser le déploiement





CNF Microservices: Avantages

Evolutivité

Ajouter de nouvelles fonctionnalités sans modifier tout le code

Rapidité

Agilité, accélérer le processus de déploiement des applications

Scalabilité

Adaptation automatique de l'offre à la demande.

Resilience

Si un service tombe en panne, l'application ne cesse pas de fonctionner.

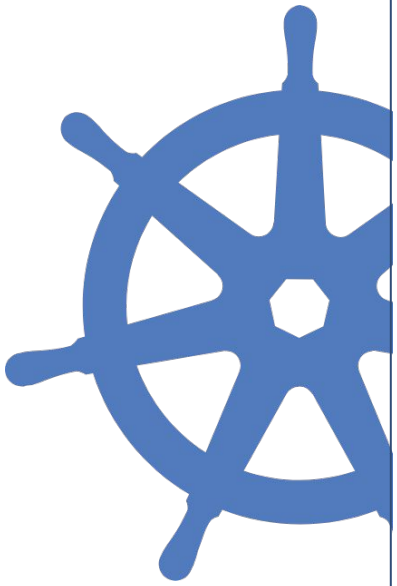
2

5G sur Kubernetes

Beopen IT <Formation K8S>

Déploiement d'un coeur de réseau 5G sur Kubernetes BeOpen IT©

Les grandes étapes



1) Kubernetes Networking

2) Resource Manager

3) DevOps Stack

4) Télemetry

Networking : 5G Core Architecture SBA

Control Plane Network Function

AMF: Acces & Mobility Management Function

SMF: Session Management Function

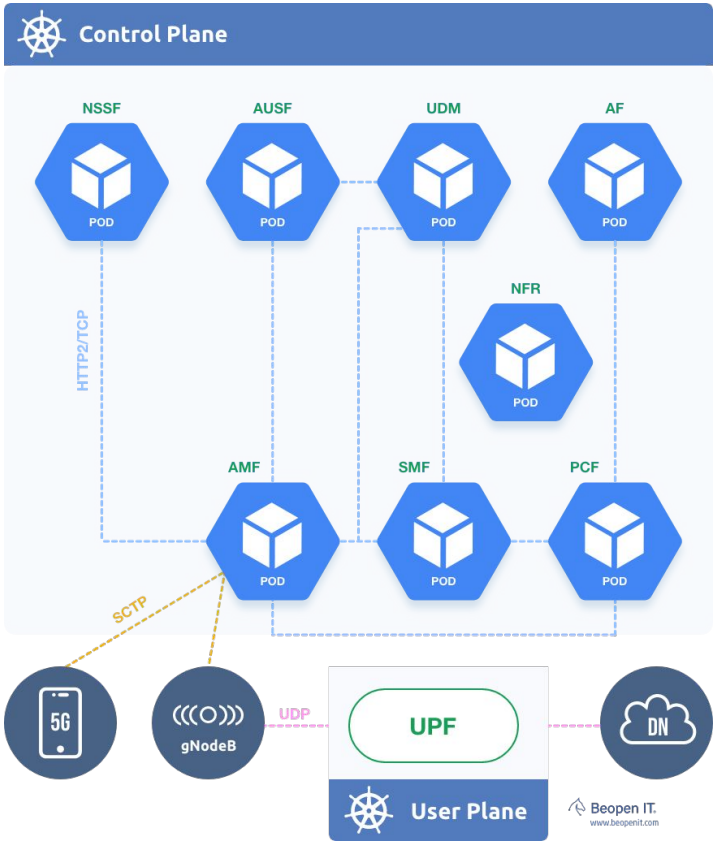
NRF: NF Repository Function

AUSF: Authentication Server Function

UDM: Unified Data Management

User Plane Network Function

UPF: User Plane Function



Networking : Plateforme support SCTP Protocol

SCTP avec Kubernetes (Bare Metal)

Supporte le protocol SCTP (stable 1.20)

SCTP avec OpenShift

SCTP est désactivé par defaut sur **Openshift**

SCTP avec les Cloud Provide

EKS support sctp protocol

Networking : Choix CNI

Critère n°1

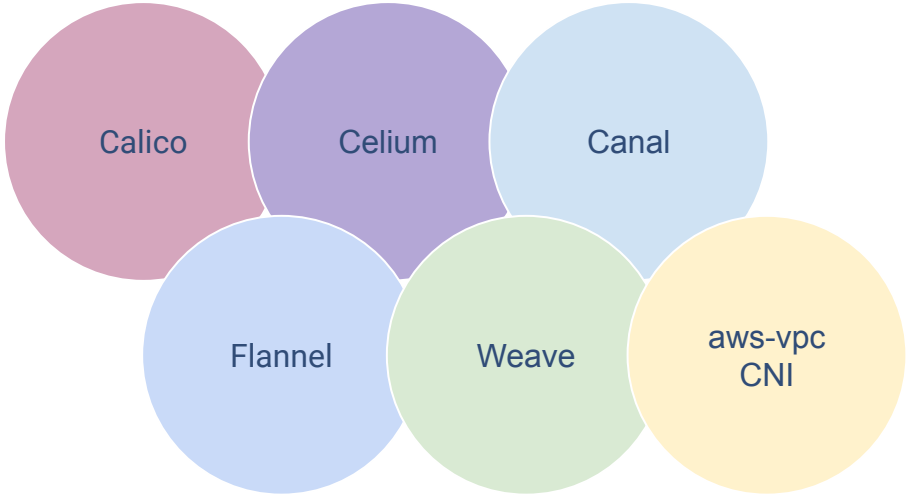
Est-ce que le CNI supporte Multus meta CNI?

Critère n°2

Le CNI supporte-il le protocol SCTP ?

Optionnel

Est-ce que le CNI supporte Network Policy ?



Networking : Packet Processing East-West(E-W) Traffic

E-W

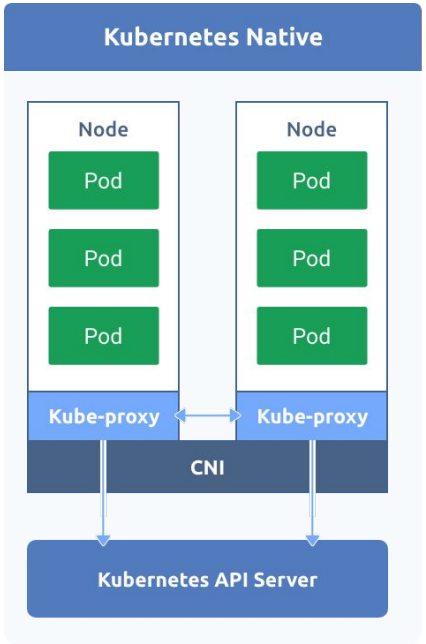
CNI Standard (Example Calico)

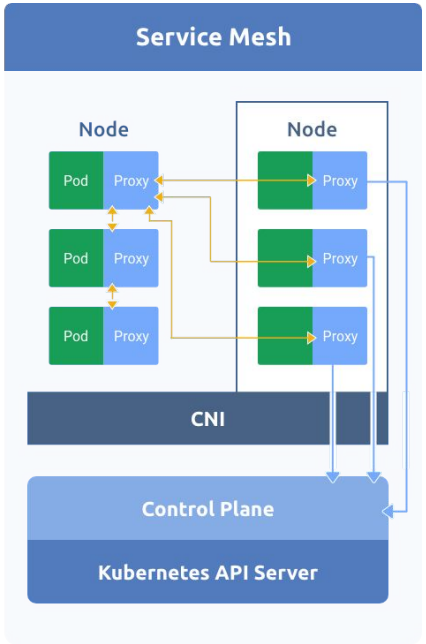
- Assure la communication Pod-to-Pod dans le Cluster
- Utilise l'interface par défaut eth0 pour la communication entre Pods

E-W

Service Mesh

Fournit une Observabilité et une meilleure sécurité sur le trafic échangé entre les microservices CNFs au sein du cluster.



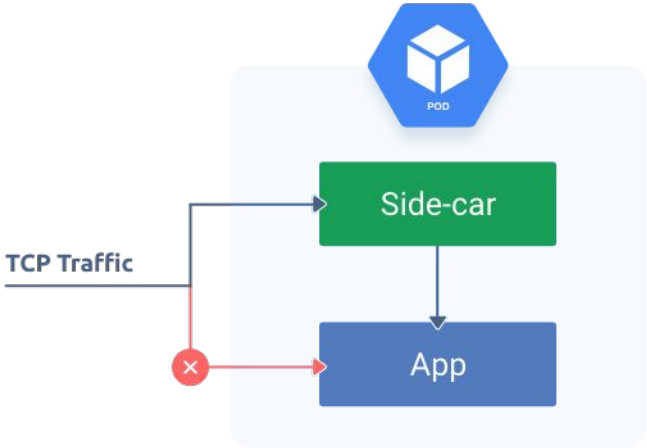


Trafic inside cluster

Networking : Service Mesh dans 5G core

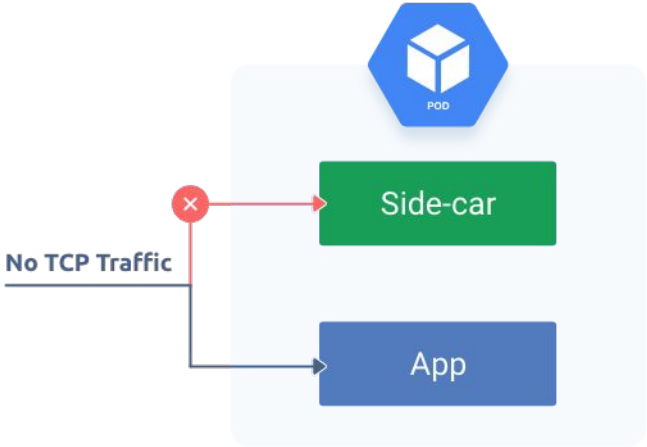
1

Tout trafic entrant provenant de n'importe quelle interface basée sur du TCP est dirigé vers le container side-car du service mesh. Il revient et va dans le container d'application, en suivant le même chemin au retour.



2

Tout trafic provenant de n'importe quelle interface utilisant un protocol non-tcp (SCTP ou UDP) sera directement envoyé vers le conteneur d'application



Networking : Packet Processing North-South(N-S) Taffic

Objectif

Attribuer plusieurs interfaces réseau a un Pod exécutant un CNF.

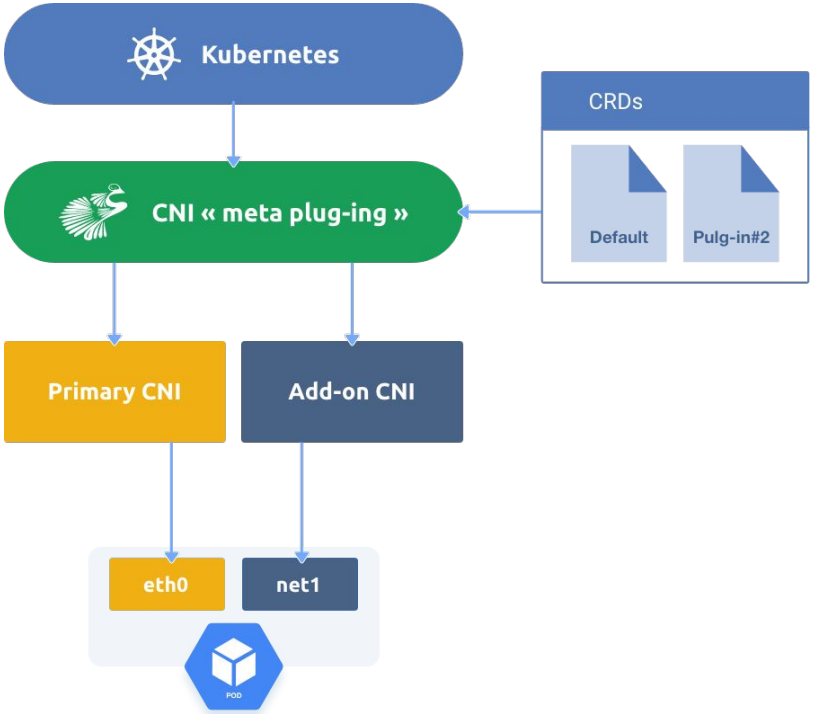
Problème

La norme 3GPP exige plusieurs interfaces réseaux pour chaque pod.

Kubernetes n'est pas conçu dans l'optique d'attribuer plusieurs interfaces à un Pod

Solution : Utilisation Multus CNI

- Créer plusieurs interfaces dans les pods Kubernetes avec Multus CNI et la spécification : NetworkAttachementDefinition
- Multus nécessite un CNI standard (calico, celuim ...)



Networking : Multus Meta CNI

Multus avec les Containers Network Plugin

- mcvlan: Crée une nouvelle adresse MAC et transfert tous le trafic vers cette adresse au conteneur
- bridge: Crée un pont et y ajoute l'hôte et le conteneur
- host device

Utilisation Multus avec SR-IO

- Conditions à remplir pour quel le noeud soit compatibleavec SR-IOV
- La carte réseau physique doit prendre en charge SR-IOV
- L'OS hôte comprend des pilotes capables de faire du SR-IOV

Configuration Multus CNI

```
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: macvlan-conf
spec:
  config: '{
      "cniVersion": "0.3.0",
      "type": "macvlan",
      "master": "eth0",
      "mode": "bridge",
      "ipam": {
        "type": "host-local",
        "subnet": "192.168.1.0/24",
        "rangeStart": "192.168.1.200",
        "rangeEnd": "192.168.1.216",
        "routes": [
          { "dst": "0.0.0.0/0" }
        ],
        "gateway": "192.168.1.1"
      }
    }'
```

Is a custom resource, and uses NetworkAttachmentDefinitions as defined by the Network Plumbing Working Group

Annotations refer to this name

Contains a CNI configuration packaged in the spec.config field.

Resources Manager : Performances elevée, faible latence et HA

CPU / MEMORY

- Bien dimensionner les ressources du cluster
- Les Applications Telco ont besoins d'une performance élevée et d'une faible latence

Auto Scaling

- Auto scaling Horizontal/Vertical des Pods Applications
- Auto scaling Cluster (cloud provider)

Resources Manager 5G Core

DevOps Stack : automatiser le déploiement

Intégration Continue

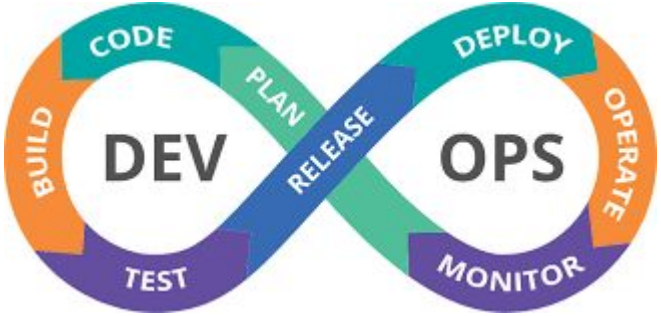
- Synchronise avec le Repository de code source
- Build et Push images docker vers le registre

Automatiser les tests de sécurité

- Teste de sécurité code source
- Analyse de vulnérabilités de l'image docker

Déploiement Continue

- Automatiser le déploiement



DevOps Stack : automatiser le déploiement

Packaging

Packager les manifestes dans un template Helm.

Automatisation

Automatiser le processus de déploiement

Sécurisation

Mettre en place et sécuriser la chaîne CI/CD.

Beopen IT

Une équipe DevSecOps efficace

Telemetry : Logging, Tracing, Metric consommation

Logging

Visualiser les logs des micro-services dans une plateforme dédiée.

Grafana loki

Tracing

Remonter les communications entre les différents micro-services.

JAEGER

Metrics

Afficher les metrics de consommations de chaque micro-service.

Prometheus

FAQ

Du partage naît l'apprentissage
et de l'apprentissage naît le partage.

Beopen IT®

Conseils DevSecOps, cybersécurité et Data
et formations linux K8s

www.beopenit.com
Join us on linkedin !