

Disseny i implementació d'un clúster de K8s en AWS

Una guia pràctica enfocada en l'automatització i l'IaC per a empreses tecnològiques

ALBERT JUBANY JUAREZ

TREBALL FINAL DE GRAU

GRAU D'ENGINYERIA INFORMÀTICA



ÍNDEX

1. Introducció
2. Kubernetes
3. Amazon EKS
4. La infraestructura AWS
5. La infraestructura com a codi
6. Estudi de components
 1. Components de xarxa
 2. L'escalat de pods
 3. L'escalat de nodes
 4. La confidencialitat del clúster
7. Conclusions i treballs futurs

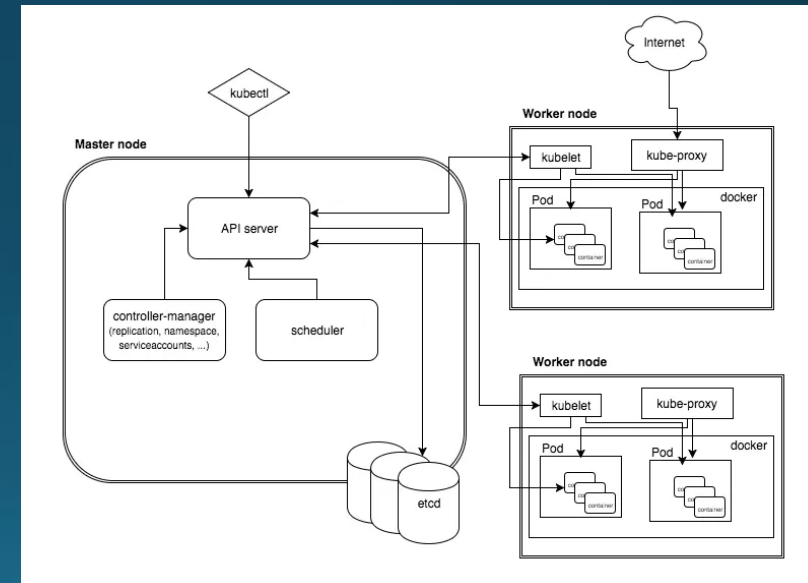
Introducció

- Estat actual de la infraestructura
 - AWS EC₂
 - AWS ASG
- Objectius del projecte:
 - Aprofundir en el coneixement de K8s i EKS
 - Utilitzar IaC per a tot
 - Analitzar i seleccionar objectivament components de K8s

Kubernetes



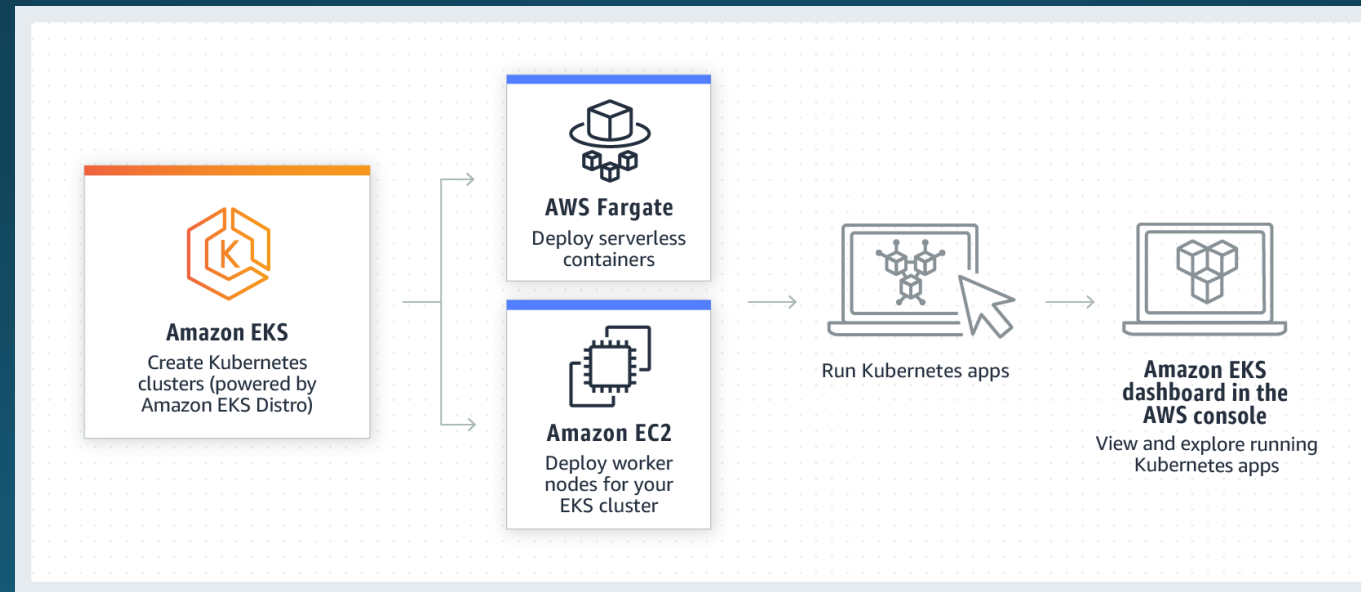
- Què és Kubernetes?
- Què NO és Kubernetes?
- L'arquitectura de Kubernetes



Amazon EKS



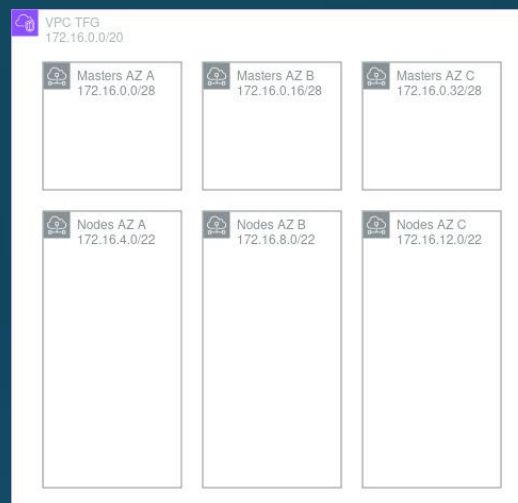
- Què és Amazon EKS?
- Quines són les principals diferències amb K8s?



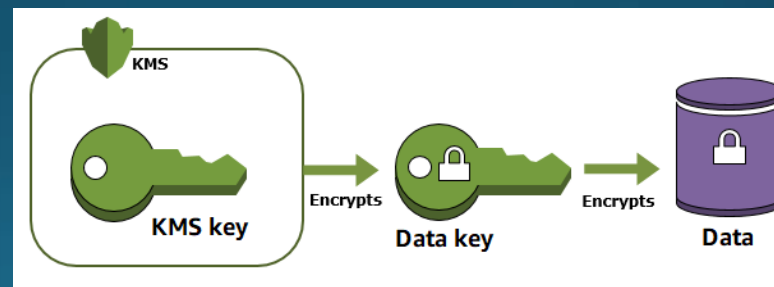


La infraestructura AWS

- VPC i subnets
 - CIDR
 - Nodes mestres
 - Nodes treballadors
 - Alta disponibilitat



- Seguretat i compliance
 - Security groups
 - Amazon KMS



La infraestructura com a codi

- *L'IaC a AWS*
 - CloudFormation
 - Sceptre
 - Terraform
- *L'IaC a Kubernetes*
 - Eksctl
 - Terraform



AWS CloudFormation

La infraestructura a EKS amb eksctl

- YAML com a origen de tot
 - VPC
 - Subnets
 - Nodegroups
 - Famílies d'instàncies
 - AMI
 - KMS
 - Versió de Kubernetes



Estudi de components de K8s

- Tecnologies de xarxa
- L'escalabilitat dels pods
- L'escalabilitat dels nodes
- La confidencialitat del clúster

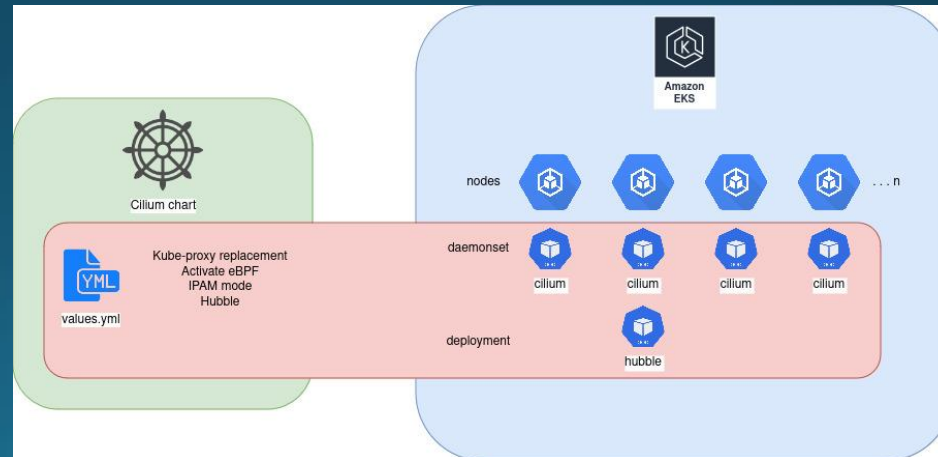
Els components de xarxa a K8s

- Kube-proxy i AWS VPC CNI
- Cilium
- Calico

	Kube-proxy + VPC CNI	Cilium	Calico
IPs	VPC	IPAM propi	IPAM propi
Gestió del tràfic	IpTables, IPVS	eBPF	IPVS o eBPF
Monitoratge de paquets	No n'inclou per defecte	Hubble	No n'inclou per defecte (es pot integrar fàcilment amb Prometheus)

Cilium

- Mode IPAM
- eBPF
- Funcions de CNI i kube-proxy
- Hubble



L'escalat de pods

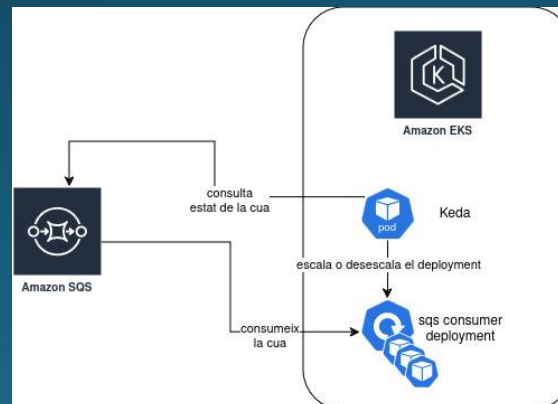
- Horitzontal pod autoscaler



- Vertical pod autoscaler

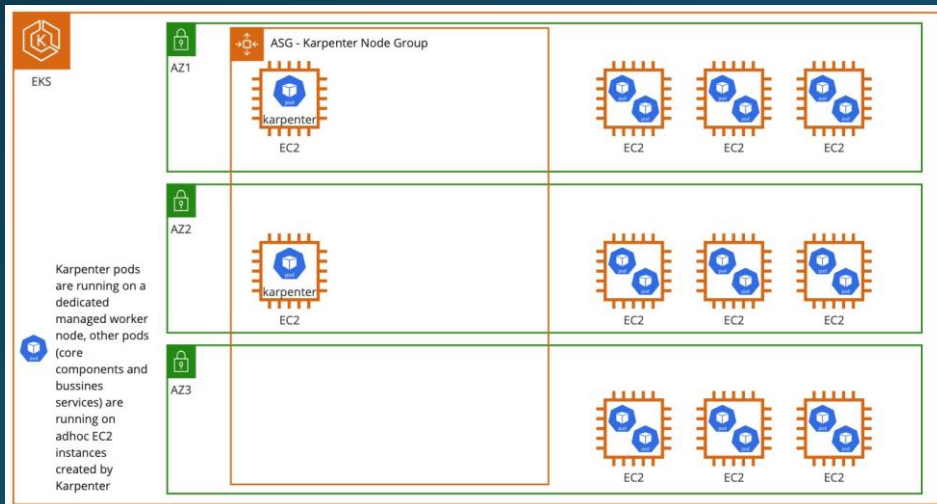
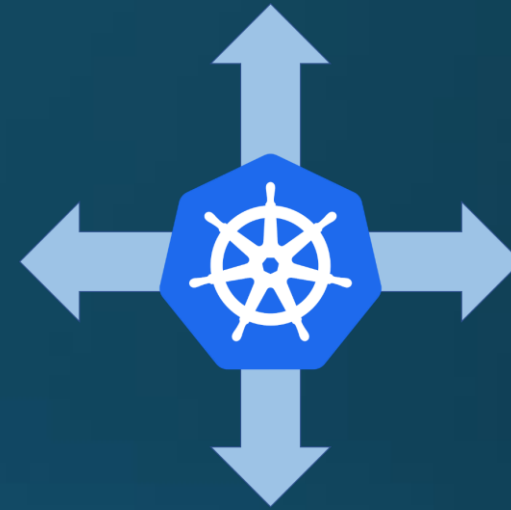


- Keda



L'escalat de nodes

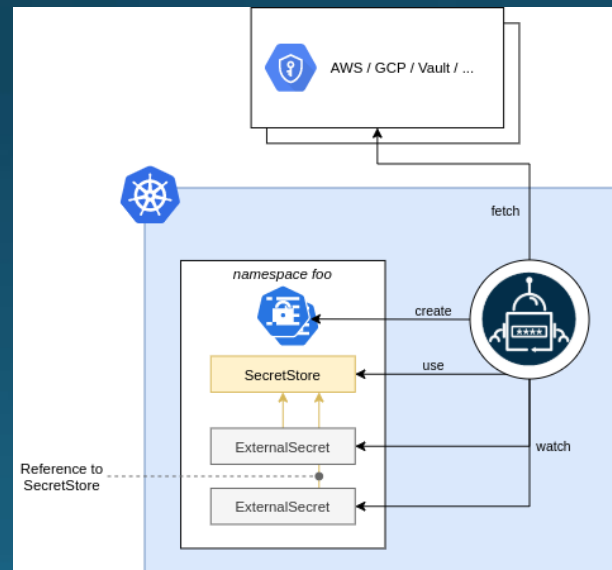
- Cluster autoscaler (CAS)
- Karpenter



Karpenter

La confidencialitat al clúster

- External-secrets
 - Com funciona?
 - Com garantitzem la confidencialitat de les dades?



Conclusions

- Investigació dels components
- Experiència amb AWS
- Facilitat de instal·lació
- Desafiaments en la personalització



Treballs futurs

- Monitorització i observabilitat
- Optimització contínua de l'escalabilitat
- Integració de noves tecnologies



MOLTES MERCÈS PER LA VOSTRA ATENCIÓ

ALBERT JUBANY JUAREZ
TREBALL FINAL DE GRAU
GRAU D'ENGINYERIA INFORMÀTICA

