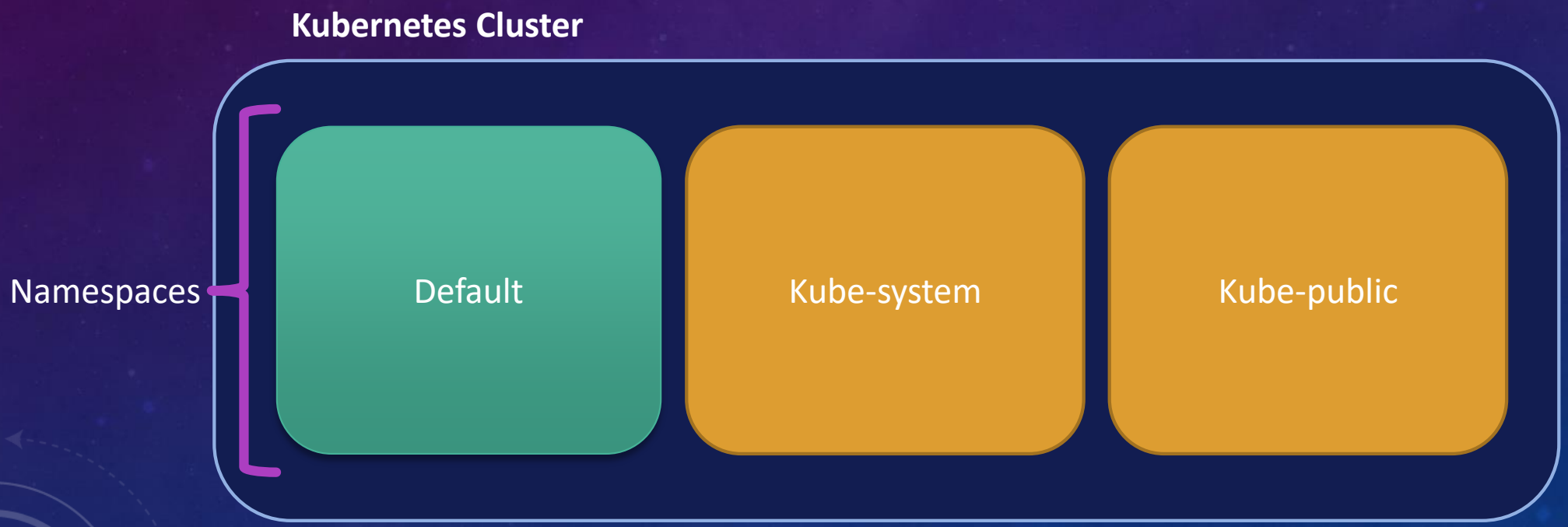
ROLES, USUARIOS Y SERVICE ACCOUNT KUBERNETES

Primeros pasos

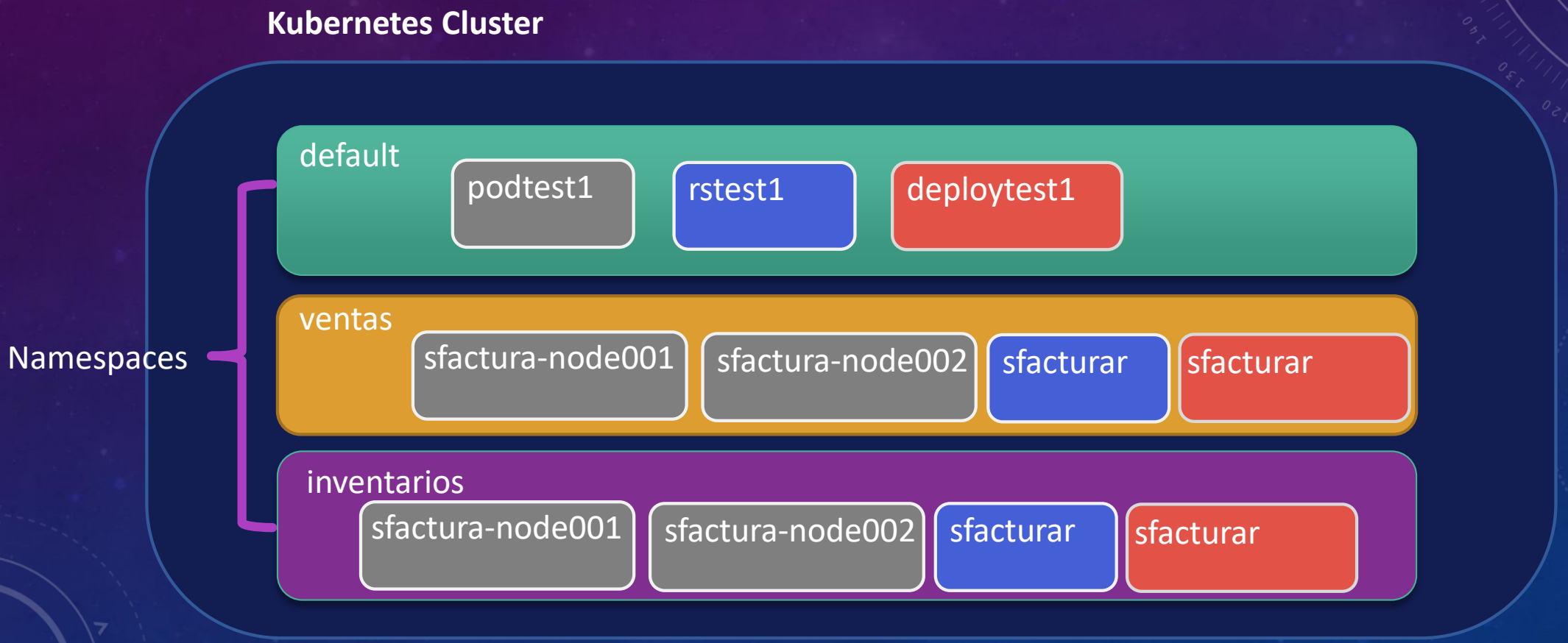
JHON EMMANUEL ZUÑIGA PAREDES
https://www.linkedin.com/in/jhonezp/

ENTENDIENDO LOS NAMESPACES

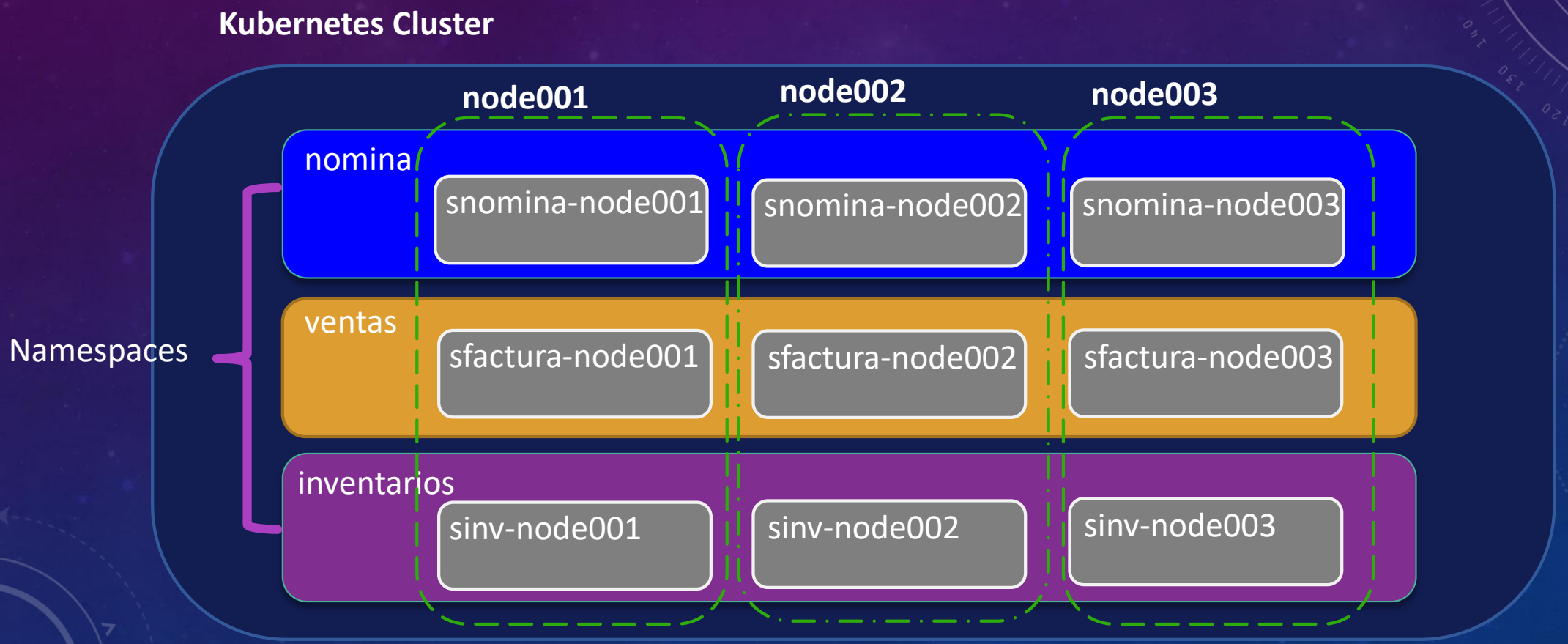
- Los namespaces permiten definir un Scope y hacer una separación lógica dentro de nuestro cluster de K8S.

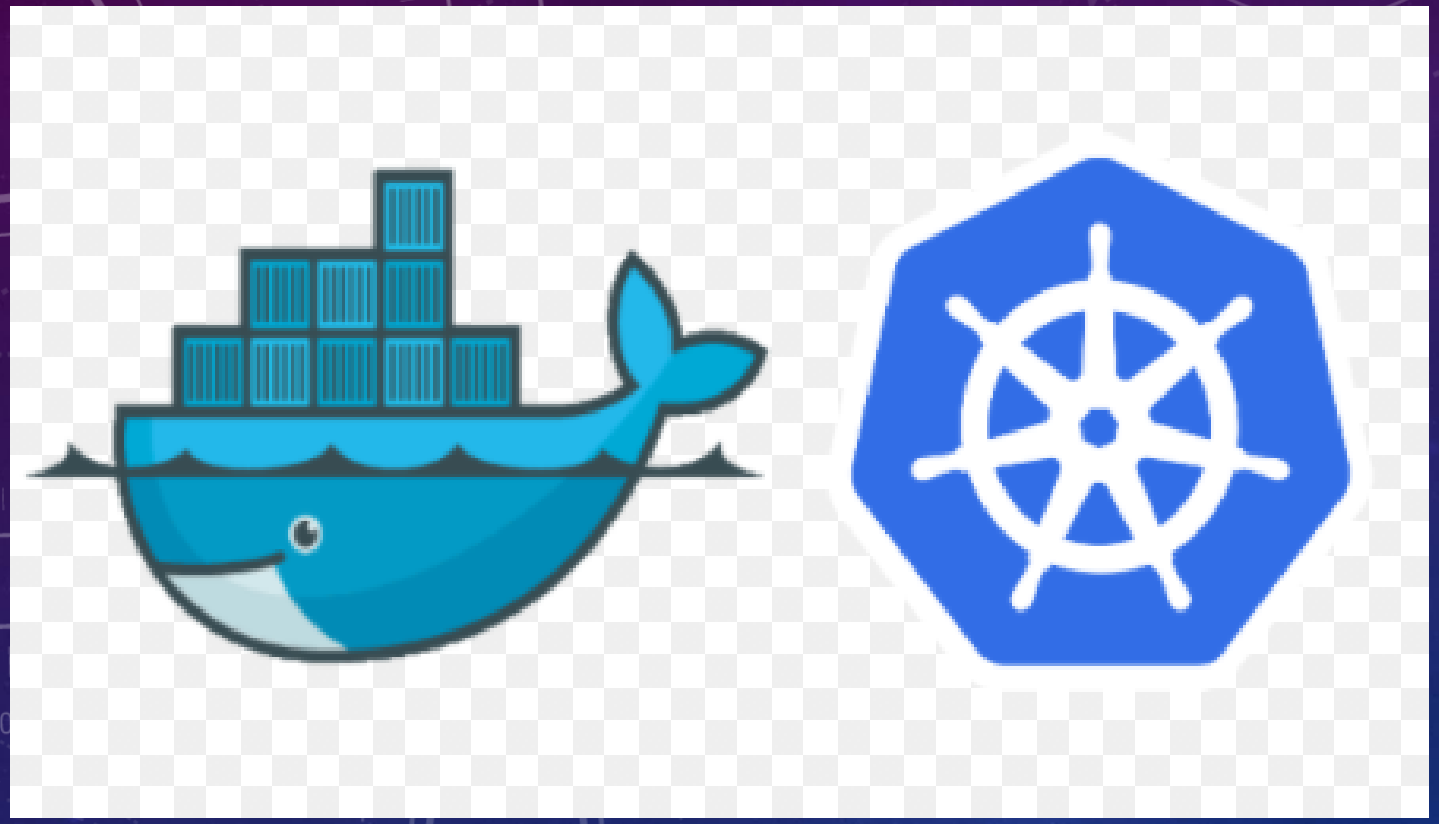


ENTENDIENDO LOS NAMESPACES



ENTENDIENDO LOS NAMESPACES

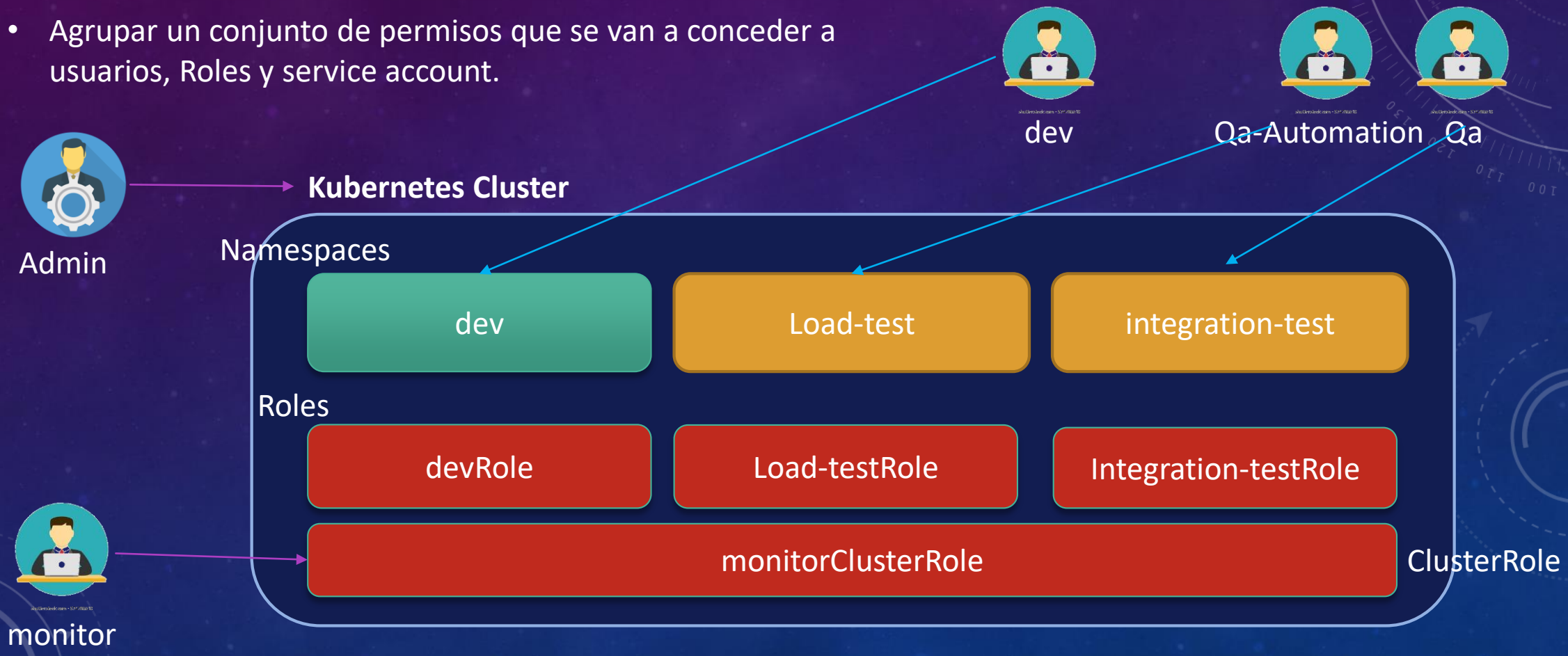




TALLER 1
NAMESPACES

RBAC (ROLE BASED ACCESS CONTROL)

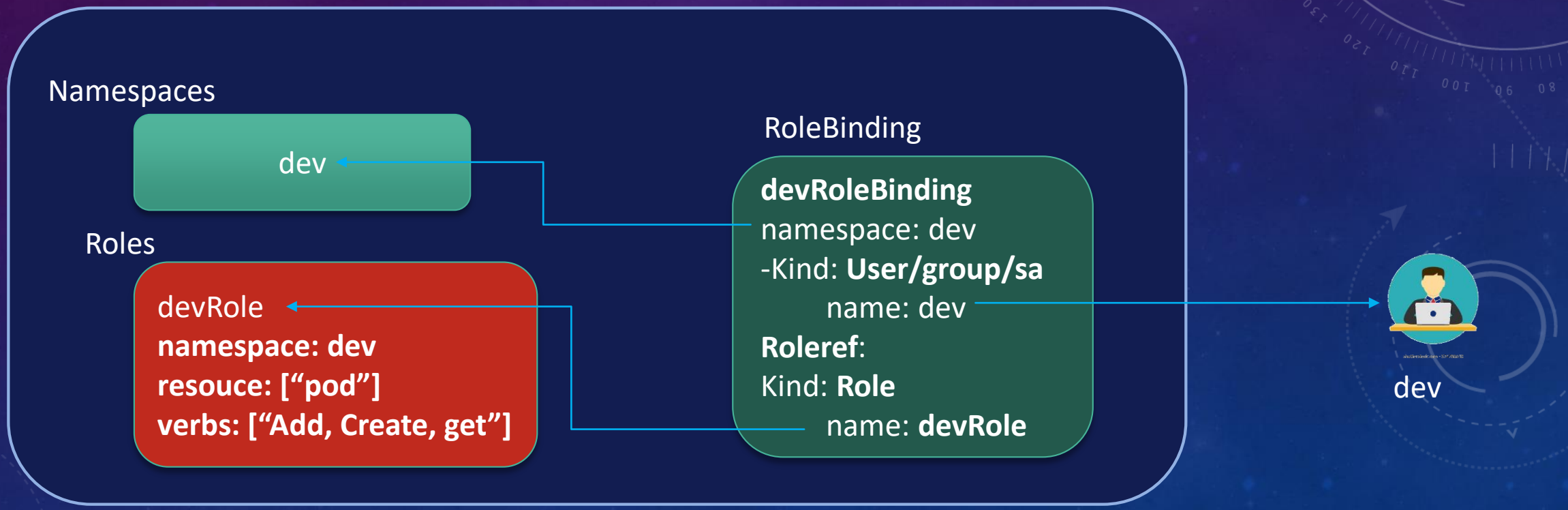
- Agrupar un conjunto de permisos que se van a conceder a usuarios, Roles y service account.



RBAC (ROLE BASED ACCESS CONTROL)

RoleBinding

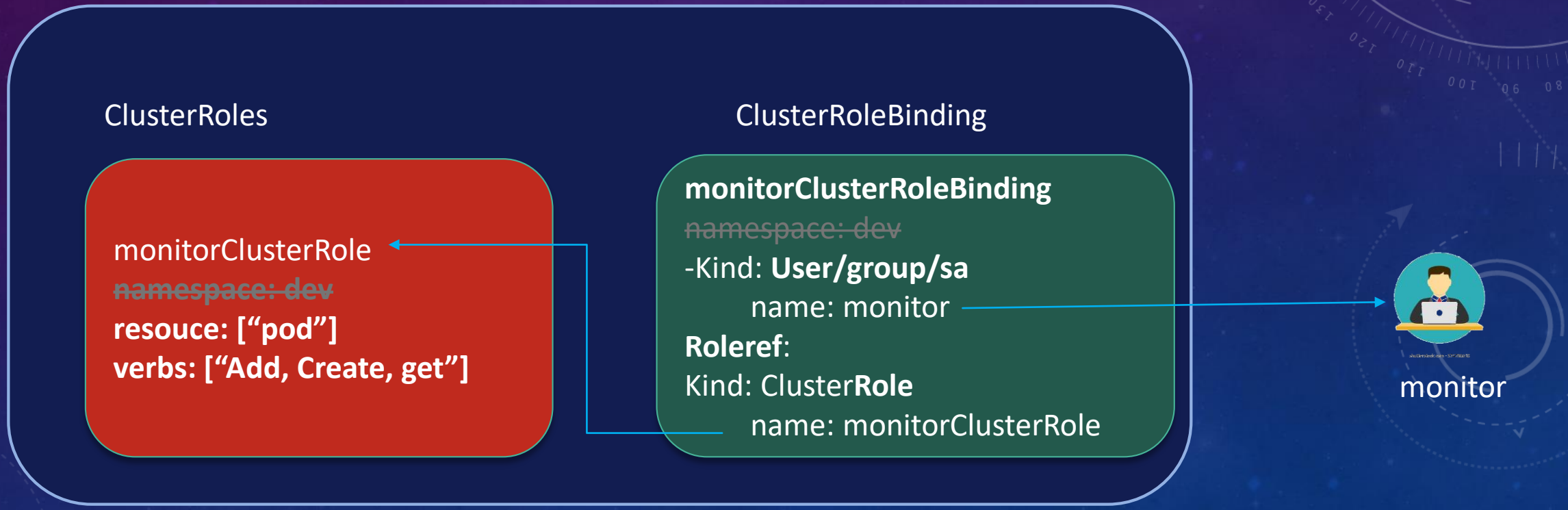
Scope: Tiene los permisos aplicados sobre el namespace específico.



RBAC (ROLE BASED ACCESS CONTROL)

ClusterRoleBinding

Scope: Tiene los permisos aplicados sobre todos los Namespaces



RBAC (ROLE BASED ACCESS CONTROL)

- Grupos y Usuarios


dev


dev2


dev1


monitor1


qa


qa1


qa2


API

Kubernetes Cluster

Certificate authority (CA)

RoleBinding

ClusterRoleBinding

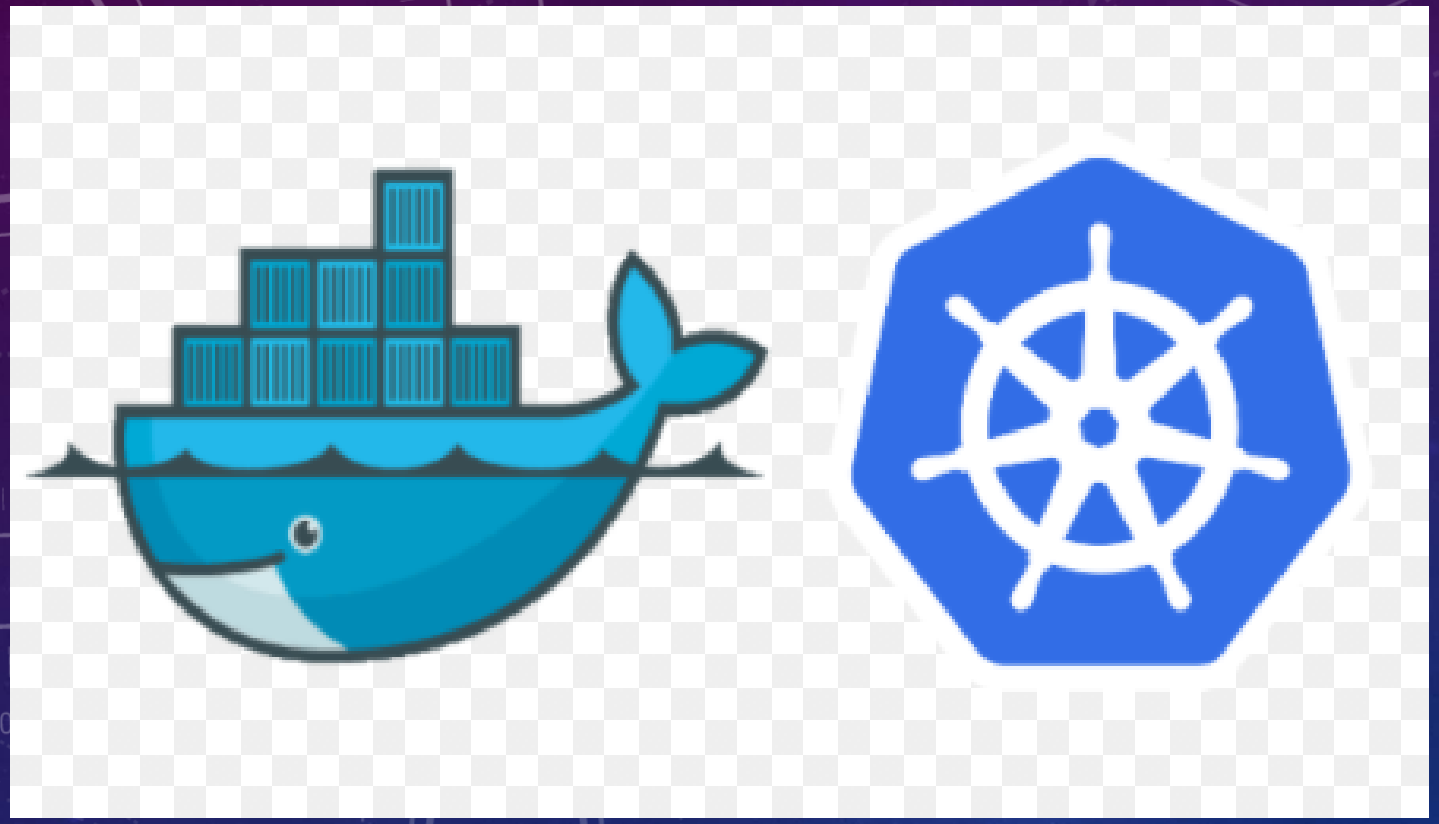
Namespaces

Resources


Admin

RBAC (ROLE BASED ACCESS CONTROL)

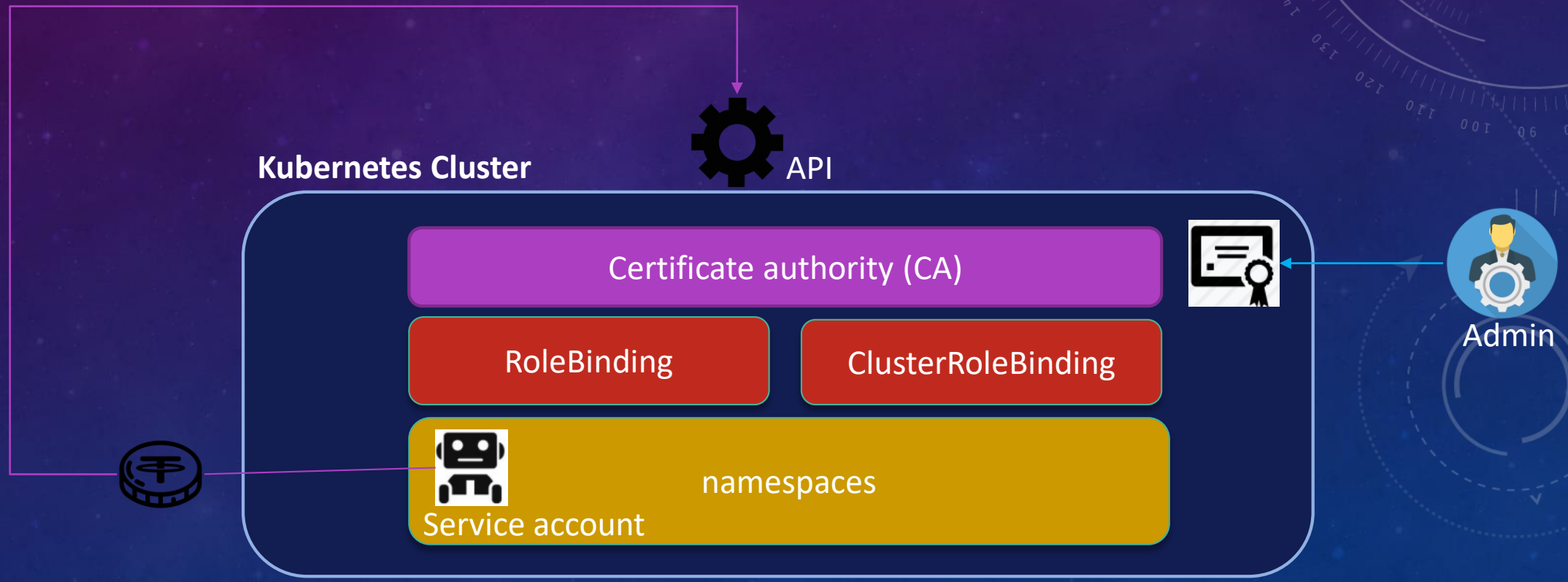
- Generando el certificado
- Del lado del Usuario (dev1)
  - Generar el key con Openssl
  - Generamos el csr (certificate signing request)
    - “/CN=usuario/O=dev” ej. “/CN=dev1/O=dev” ej. “/CN=qa/O=qa”
- Del lado del ADMIN del Cluster
  - Generar el crt del usuario dev1, utilizando el ca.crt del cluster.
- Del lado del Usuario (dev1)
  - Configurar el certificado en su ambiente de K8S en sus context.

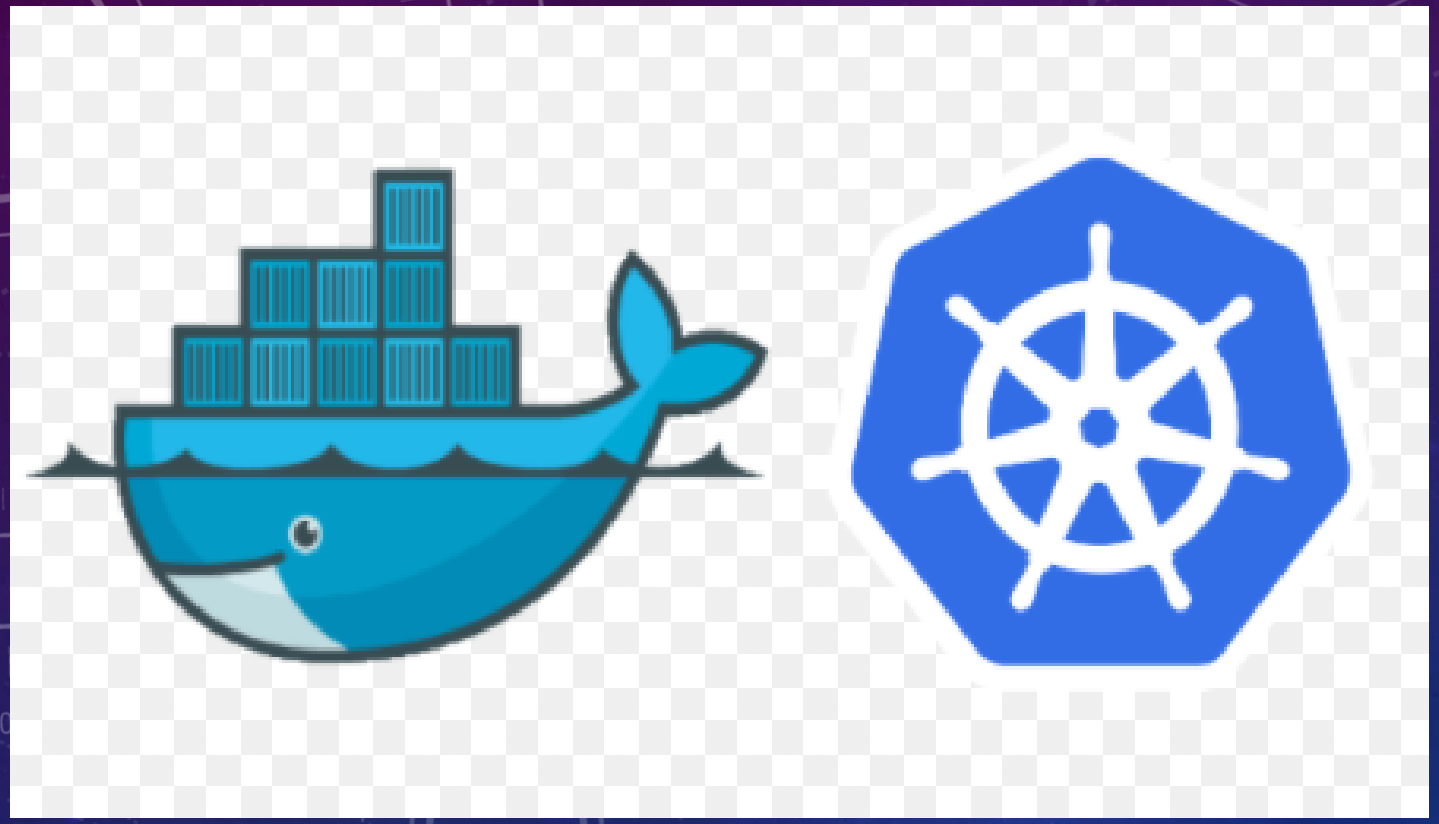


TALLER 2
RBAC
USUARIOS
GRUPOS

RBAC (ROLE BASED ACCESS CONTROL)

- Service Account





TALLER 2
RBAC
SERVICE ACCOUNT