

学习内容：

云原生公开课第二十四、二十五、二十六、二十七、二十八、二十九、三十章

收获：

- 主流的 operator framework 主要有两个：kubebuilder 和 operator-sdk。
- Service 其实是一种负载均衡 (Load Balance) 的机制，类型有：ClusterIP、NodePort、LoadBalancer、ExternalName。
- CNI 插件可以分为三种：Overlay、路由及 Underlay
 1. Overlay 模式的典型特征是容器独立于主机的 IP 段，这个 IP 段进行跨主机网络通信时是通过在主机之间创建隧道的方式，将整个容器网段的包全都封装成底层的物理网络中主机之间的包。该方式的好处在于它不依赖于底层网络。
 2. 路由模式中主机和容器也分属不同的网段，它与 Overlay 模式的主要区别在于它的跨主机通信是通过路由打通，无需在不同主机之间做一个隧道封包。但路由打通就需要部分依赖于底层网络，比如说要求底层网络有二层可达的一个能力。
 3. Underlay 模式中容器和宿主机位于同一层网络，两者拥有相同的地位。容器之间网络的打通主要依靠于底层网络。因此该模式是强依赖于底层能力的。
- RBAC 鉴权三要素：Subjects、API Resource、Verbs
- CRI 的出现是为了将容器运行时与 Kubernetes 解耦开
- 安全容器：Kata Containers、gVisor
- RuntimeClass 是 Kubernetes 一种内置的全局域资源，主要用来解决多个容器运行时混用的问题