**多租户环境下的安全加固**

1. **背景**

Kubernetes是Google内部使用的私有云模型：Node节点是所有namespace可以共享的，而且所有node节点跟master节点的通信使用同一个证书，API server在授权的同时并不区分namespace。这个在公有云场景下会有产生一些安全问题：如果某个恶意用户攻破linux的cgroup和namesapce的限制，拿到node的节点上的证书，就可以拿到整个集群的数据。

解决方案：不同的namesapce使用不同的证书，API server在授权时区分namespace，不允许一个namespace访问另外一个namespace的数据。

1. **实现原理**
2. 使用API server的插件机制，当API server接收到的是一个创建namesapce的请求的时候，为这个namespace创建一个证书，并打包上传到NOS
3. Node节点在初始化的时候，会从NOS下载证书。然后kubelet用这个证书去访问API server
4. API server根据证书区分namespace，不允许跨namesapce的访问

Note：我主要负责第1部分（生成证书并上传）

1. **证书生成&上传**

给API server加一个CertificateGeneration的插件。实现代码在plugin/admission/namespace/certgeneratoa里。基本原理是：

1. 判断请求类型，如果是个创建namespace的请求，就跑一个生成证书的脚本，生成证书。
2. 将生成的证书上传NOS即可。