**K8S RBAC 用户鉴权认证**

Abstract:

Normal User:

Kubernetes does not have objects which represent normal user accounts. Normal users cannot be added to a cluster through an API call, any user that presents a valid certificate signed by the cluster's certificate authority (CA) is considered authenticated.

Kubernetes determines the username from the common name field in the 'subject' of the cert (e.g., "/CN=bob"). From there, the role based access control (RBAC) sub-system would determine whether the user is authorized to perform a specific operation on a resource

Service Account:

Service accounts are users managed by the Kubernetes API. They are bound to specific namespaces, and created automatically by the API server or manually through API calls. Service accounts are tied to a set of credentials stored as Secrets, which are mounted into pods allowing in-cluster processes to talk to the Kubernetes API.

1. 生成用户私钥

openssl genrsa -out eastech.key 2048

openssl req -new -key eastech.key -out eastech.csr(主要参数:CN & O)

cat eastech.csr | base64 | tr -d "\n"

1. 创建CSR(CertificateSigningRequest)

apiVersion: certificates.k8s.io/v1

kind: CertificateSigningRequest

metadata:

name: eastech

spec:

groups:

- system:authenticated

request: 

signerName: kubernetes.io/kube-apiserver-client

usages:

- client auth

1. 批准证书签名请求

kubectl certificate approve eastech

kubectl certificate deny <certificate-signing-request-name>

1. 从CSR导出颁发的证书

kubectl get csr/ eastech -o yaml

kubectl get csr eastech -o jsonpath='{.status.certificate}'| base64 -d > eastech.crt

1. 创建角色和角色绑定

kubectl create role developer --verb=create --verb=get --verb=list --verb=update --verb=delete --resource=pods

kubectl create rolebinding eastech --role=developer --user= eastech -n elk

1. 添加到kubeconfig

kubectl config set-credentials eastech --client-key= eastech.key --client-certificate= eastech.crt --embed-certs=true

kubectl config set-context eastech --cluster=kubernetes --user= eastech

kubectl config use-context eastech