链滴

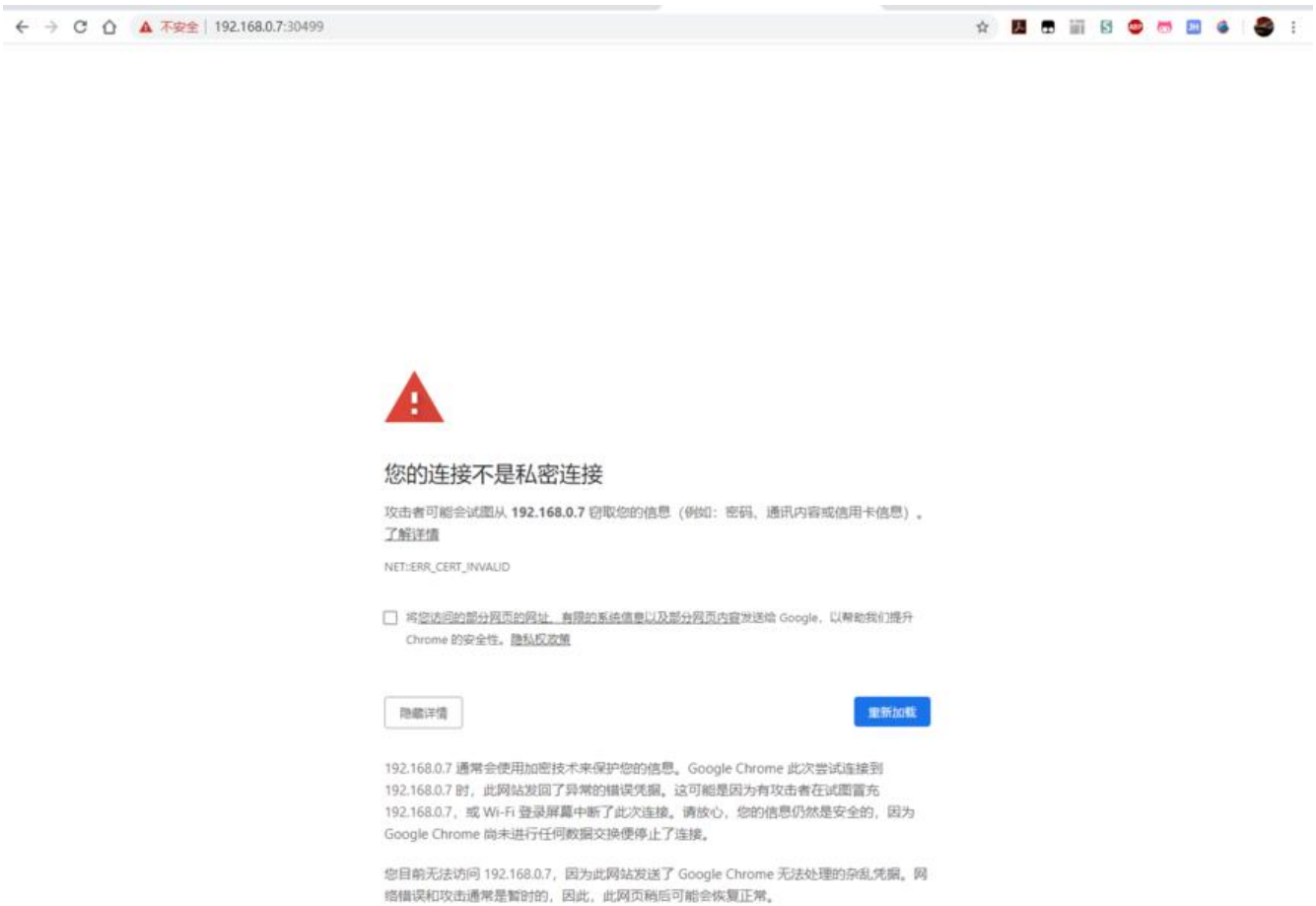
解决 Kubernetes-Dashboard 在 chrome 浏览器上无法打开（证书不可信任）的问题

作者：Leif160519

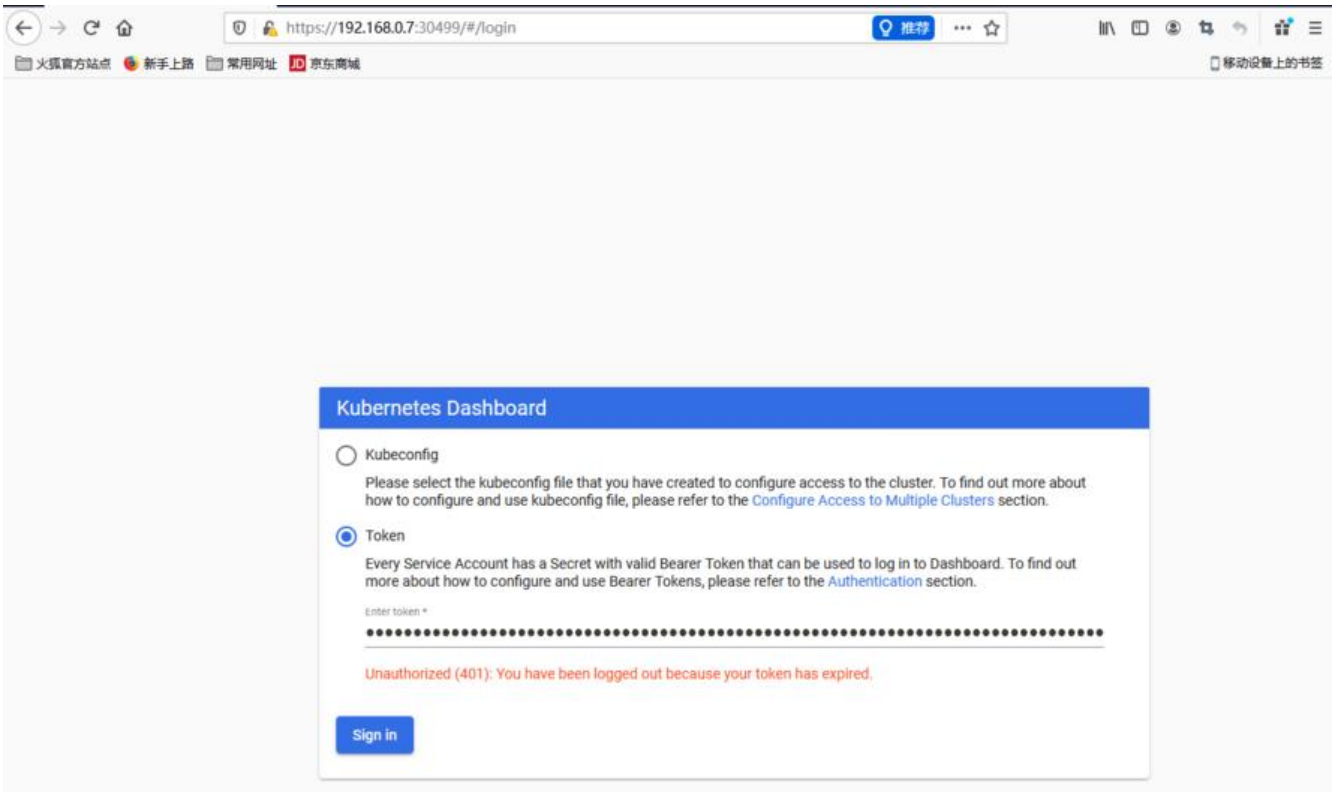
原文链接：https://ld246.com/article/1591598393945

来源网站：链滴

当我们搭建完一个k8s集群并且使用官方dashboard-yaml文件创建好k8s-dashboard之后发现，只火狐浏览器可以打开dashbaord界面，chrome和IE浏览器都无法访问



原文链接：解决 Kubernetes-Dashboard 在 chrome 浏览器上无法打开（证书不可信任）的问题



原因是部署UI的镜像中默认自带的证书是一个不可信任的证书

由此可以发现，该证书的很多信息都没有，并且证书的时间也都不正常，这就导致了大部分浏览器不这个证书，但是我们自己生成的证书大部分浏览器都是可以访问的，那是因为我们自己签发的证书是合校验字段的

下面介绍两种k8s集群搭建方式对应的解决方案(主要是将自带的证书替换成我们自己签发的证书)

原文链接：解决 Kubernetes-Dashboard 在 chrome 浏览器上无法打开（证书不可信任）的问题

对于自签证书，我们可以使用openssl或者cfssl工具生成证书，或者直接使用k8s证书(/etc/kubernete/pki)

kubeadm和二进制部署的k8s集群一般都有两套证书(2个ca签发)，一套是apiserver，一套是etcd，果想使用现成的证书，这两套都可以。

k8s-dashboard证书是存储在k8s中的：

```
[root@k8s-master k8s]# kubectl get secrets -n kubernetes-dashboard
NAME                         TYPE                                  DATA   AGE
default-token-gcw2j          kubernetes.io/service-account-token   3      50m
kubernetes-dashboard-certs   Opaque                                0      50m
kubernetes-dashboard-csrf    Opaque                                1      50m
kubernetes-dashboard-key-holder   Opaque                           2      50m
kubernetes-dashboard-token-l7k7m  kubernetes.io/service-account-token   3      50m
```

可以发现，certs后面的数据是空的，这就说明在这个secret中并没有存储任何东西，只不过有这个资创建了，证书在镜像中自带，那么我们需要做的就是需要在这个secret去签发证书，随后在重新创建dshboard的pod即可

二进制部署

注意你部署Dashboard的命名空间（之前部署默认是kube-system，新版是kubernetes-dashboard）

1、 删除默认的secret，用自签证书创建新的secret

```
kubectl delete secret kubernetes-dashboard-certs -n kubernetes-dashboard

kubectl create secret generic kubernetes-dashboard-certs \
--from-file=/opt/kubernetes/ssl/server-key.pem --from-file=/opt/kubernetes/ssl/server.pem
n kubernetes-dashboard
```

2、修改 dashboard.yaml 文件，在args下面增加证书两行

```
args:
      # PLATFORM-SPECIFIC ARGS HERE
      - --auto-generate-certificates
      - --tls-key-file=server-key.pem
      - --tls-cert-file=server.pem

kubectl apply -f kubernetes-dashboard.yaml
```

kubeadm部署

注意你部署Dashboard的命名空间（之前部署默认是kube-system，新版是kubernetes-dashboard）

1、删除默认的secret，用自签证书创建新的secret

```
kubectl delete secret kubernetes-dashboard-certs -n kubernetes-dashboard

kubectl create secret generic kubernetes-dashboard-certs \
--from-file=/etc/kubernetes/pki/apiserver.key --from-file=/etc/kubernetes/pki/apiserver.crt -
 kubernetes-dashboard
```

原文链接：解决 Kubernetes-Dashboard 在 chrome 浏览器上无法打开（证书不可信任）的问题

2、修改 dashboard.yaml 文件，在args下面增加证书两行

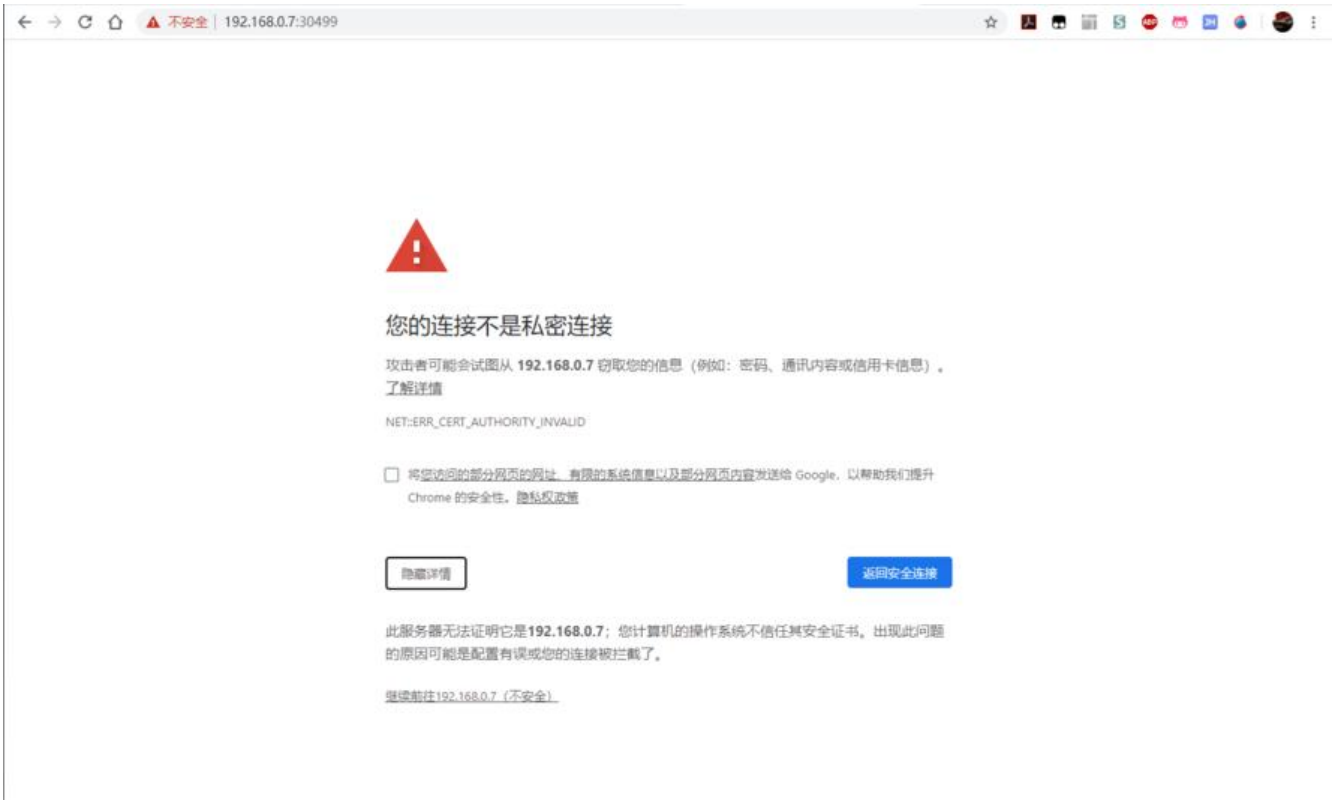
```
args:
        # PLATFORM-SPECIFIC ARGS HERE
        - --auto-generate-certificates
        - --tls-key-file=apiserver.key
        - --tls-cert-file=apiserver.crt
```

```
kubectl apply -f kubernetes-dashboard.yaml
```

查看secret：

```
[root@k8s-master k8s]# kubectl get secrets -n kubernetes-dashboard
NAME                         TYPE                                  DATA   AGE
default-token-gcw2j          kubernetes.io/service-account-token   3      57m
kubernetes-dashboard-certs   Opaque                                2      2m51s
kubernetes-dashboard-csrf    Opaque                                1      57m
kubernetes-dashboard-key-holder   Opaque                           2      57m
kubernetes-dashboard-token-l7k7m  kubernetes.io/service-account-token   3      57m
[root@k8s-master k8s]# kubectl get pod -n kubernetes-dashboard
NAME                                         READY   STATUS    RESTARTS   AGE
dashboard-metrics-scraper-694557449d-dvqqp   1/1     Running   0          57m
kubernetes-dashboard-5d8766c7cc-6q7rp        1/1     Running   0          35s
```

效果：



证书信息：

原文链接：解决 Kubernetes-Dashboard 在 chrome 浏览器上无法打开（证书不可信任）的问题

证书

kube-apiserver

主题名称
通用名称 kube-apiserver

颁发者名称
通用名称 kubernetes

有效性
起始时间 2020/6/1 上午8:41:16 (Asia/Shanghai)
终止时间 2021/6/1 上午8:41:16 (Asia/Shanghai)

主题替代名称
DNS 名称 k8s-master
DNS 名称 kubernetes
DNS 名称 kubernetes.default
DNS 名称 kubernetes.default.svc
DNS 名称 kubernetes.default.svc.cluster.local
IP 地址 10.96.0.1
IP 地址 192.168.0.7

公钥信息
算法 RSA
密钥大小 2048
指数 65537
模块 AE:67:F2:A3:DF:32:3F:62:70:75:1B:7A:57:E3:92:0D:FD:E4:51:57:BB:48:50:25:EE:64:AF:6F:57:BF:5B:3B:DB:B5:...

杂项
序列号 14:8A:59:BD:79:86:C5:AC
签名算法 SHA-256 with RSA Encryption
版本 3
下载 PEM（证书） PEM（证书链）

指纹
SHA-256 70:19:9F:FE:C7:18:C9:E2:10:4A:11:13:CA:D5:C8:98:6B:37:74:B4:21:9C:0B:B9:90:03:0C:FD:FA:28:08:FC
SHA-1 8A:A8:AA:19:FF:1B:B2:88:0C:4A:9C:A9:36:53:5A:B6:D3:1A:C3:30

密钥用途
用途 Digital Signature, Key Encipherment

扩展密钥用途
用途 Server Authentication

原文链接：解决 Kubernetes-Dashboard 在 chrome 浏览器上无法打开（证书不可信任）的问题