

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
- 许可协议: 署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)



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

← → C ① ▲ 不安全 | 192.168.0.7:30499

* 🖪 🖬 🖬 🗟 😂 🛅 🚳 🥞 🗄



您的连接不是私密连接

攻击者可能会试图从 192.168.0.7 窃取您的信息(例如:密码、通讯内容或信用卡信息)。 了解详情

NET::ERR_CERT_INVALID

□ 将您访问的部分阅页的网址 育房的系统信息以及部分阅页内容发送给 Google, 以帮助我们提升 Chrome 的安全性。融私权改集

隐藏详情



192.168.0.7 通常会使用加密技术来保护您的信息。Google Chrome 此次尝试连接到 192.168.0.7 时,此网站发回了异常的错误凭握。这可能是因为有攻击者在试图言充 192.168.0.7,或 Wi-Fi 登录屏幕中断了此次连接。请放心,您的信息仍然是安全的,因为 Google Chrome 尚未进行任何数据交换便停止了连接。

您目前无法访问 192.168.0.7,因为此网站发送了 Google Chrome 无法处理的杂乱先偏。网络借误和攻击通常是暂时的,因此,此网页稍后可能会恢复正常。



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

	证书
右边性	
起始时间	1901/1/1 上午8:00:00 (Asia/Shanghai)
终止时间	1901/1/1 上午8:00:00 (Asia/Shanghai)
公钥信息	
算法	Elliptic Curve
密钥大小	256
曲线	P-256
公开值	04:15:FC:25:D1:8B:93:FB:E8:86:42:3D:D0:DD:50:12:BD:AD:69:A3:55:F6:F7:BB:80:EC:B8:3A:20:71:84:74:91
杂项	
序列号	00:81:83:88:04:8A:F5:0E:7A:86:32:7D:46:CA:DC:4A:CF
签名算法	ECDSA with SHA-256
版本	3
下载	
指纹	
SHA-256	20:10:75:38:97:F0:71:AB:C5:67:3C:4F:BD:A9:CF:26:28:47:49:45:5C:09:62:21:28:1A:D0:45:2D:8A:B6:54
SHA-1	E0:77:15:3A:F7:50:78:09:B1:2E:7F:A4:F9:39:F4:D0:EC:A6:24:BA

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)

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-17k7m	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d shboard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
```

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	kubernet	es-dashboar	d			
NAME	TYPE				DATA	AGE	
default-token-gcw2j	kubernetes.io/service-account-token				3	57m	
kubernetes-dashboard-certs	Opaque				2	2m51s	
kupernetes-dasnpoard-csri	opaque				1	5/m	
kubernetes-dashboard-key-holder	Opaque				2	57m	
kubernetes-dashboard-token-17k7m	kubernetes.io/service-account-token				3	57m	
[root@k8s-master k8s]# kubectl ge	et pod -n ku	ubernetes	s-dashboar	i			
NAME		READY	STATUS	RESTAR	RTS	AGE	
dashboard-metrics-scraper-694557449d-dvqqp		1/1	Running	0		57m	
kubernetes-dashboard-5d8766c7cc-6q7rp		1/1	Running	0		35s	

效果:

← → C 合 ▲ 不安全 192.168.0.7:30499		\$ Л	iii	8	•	8	6	9	:
	A								
	您的连接不是私密连接								
	攻击者可能会试图从 192.168.0.7 窃取您的信息(例如:密码、通讯内容或信用卡信息)。 了解详情								
	NET:ERR_CERT_AUTHORITY_INVALID								
	将您访问的部分网页的网址,有限的系统值意以及部分网页内容发送给 Google,以帮助我们提升 Chrome 的安全性。 <u>隐私权支援</u>								
	隐意详情								
	此服务器无法证明它是192.168.0.7;您计算机的操作系统不信任其安全证书。出现此问题 的原因可能是配置有误成您的连接被拦截了。								
	·登读前注192.168.0.7(不安全)								
证书信息:									

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 一
    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
```