29.Ingress配置TLS

上一节中我们使用Ingress控制器转发HTTP流量，那如果是HTTPS流量呢？这一节我们来了解如何配置Ingress使其支持TLS。
在开始配置之前，先来了解一下什么是SSL终止。

什么是SSL终止

在将加密数据从客户端计算机发送到web服务器之前，安全套接字层（SSL）连接使用证书进行身份验证。「SSL终止」(SSL卸载的一种形式)将部分责任从web服务器转移到另一台机器上。
「SSL终止」的工作原理是拦截从SSL连接接收数据的服务器上的加密流量。它通过在一个不同的设备上解密和验证数据来分摊服务器的任务，这样服务器就不需要处理这个过程。
「SSL终止」充当SSL连接的行结束或终止点。该过程为服务器准备数据并组织传入的连接，以便web服务器集中处理其他任务，如加载web页面。
「SSL终止」允许使用SSL连接的服务器同时处理大量连接、会话和cookie。「SSL终止」还有助于通过提高服务器响应速度来提高站点和web应用程序的性能。它通过在单独的设备上执行解密来确保准确性。

配置Ingress处理TLS连接

当客户端与Ingress控制器建立TLS连接时，Ingress控制器会终止TLS连接。客户端与控制器之间的通信是加密的，而控制器与后端pod之间的通信不是加密的。
运行在pod中的应用程序不需要支持TLS。例如，如果pod中运行了一个web服务器，那么它可以只接收HTTP请求，而让Ingress控制器负责去处理与TLS相关的内容。要使控制器能够这样做，我们需要为Ingress资源附加一个证书和一个私钥。它们存储在一个被称为Secret的Kubernetes资源中，然后在Ingress的manifest文件中被引用。

准备证书

首先需要创建private key和certificate：

openssl genrsa -out tls.key 2048

```
[root@k8s-master test]# openssl genrsa -out tls.key 2048
Generating RSA private key, 2048 bit long modulus
..+++
.....................................................+++
e is 65537 (0x10001)
```

openssl req –new –x509 –key tls.key –out tls.cert –subj /C=CN/ST=Beijing/L=Beijing/O=DevOps/CN=test.pmx.com

```
[root@k8s-master test]# openssl req -new -x509 -key tls.key -out tls.cert -subj /C=CN/ST=Beijing/L=Beijing/O=DevOps/CN=test.pmx.com
[root@k8s-master test]# ll
total 68
-rw-r--r-- 1 root root 18391 Jan  7 03:14 deploy.yaml
-rw-r--r-- 1 root root   394 Jan 12 05:56 test-ingress-deployment.yaml
-rw-r--r-- 1 root root   140 Jan 12 05:46 test-ingress-svc.yaml
-rw-r--r-- 1 root root   296 Jan 12 06:32 test-nginx-ingress.yml
-rw-rw-r-- 1 root root   338 Jan  2 13:58 test-rc.yaml
-rw-r--r-- 1 root root   135 Jan  3 17:54 test-svc-loadbalancer.yaml
-rw-r--r-- 1 root root   174 Jan  2 17:44 test-svc-nodeport.yaml
-rw-rw-r-- 1 root root   132 Jan  2 14:15 test-svc.yaml
-rw-r--r-- 1 root root   357 Jan 12 11:03 test-tomcat-deployment.yaml
-rw-r--r-- 1 root root   304 Jan 12 11:10 test-tomcat-ingress-nginx.yml
-rw-r--r-- 1 root root   157 Jan 12 11:00 test-tomcat-svc.yaml
-rw-r--r-- 1 root root  1281 Jan 13 07:55 tls.cert
-rw-r--r-- 1 root root  1675 Jan 13 07:48 tls.key
[root@k8s-master test]#
```

生成secret

基于上面生成的两个文件创建Secret：

kubectl create secret tls tomcat–ingress–secret ––cert=tls.cert ––key=tls.key

```
[root@k8s-master test]# kubectl create secret tls tomcat-ingress-secret --cert=tls.cert --key=tls.key
secret/tomcat-ingress-secret created
[root@k8s-master test]#
```

kubectl get secret

```
[root@k8s-master test]# kubectl get secret
NAME                  TYPE                                  DATA   AGE
default-token-vh7qq   kubernetes.io/service-account-token   3      10d
tomcat-ingress-secret   kubernetes.io/tls                   2      39s
[root@k8s-master test]#
```

private key和certificate存储在名为tomcat–ingress–secret的Secret资源中：

kubectl describe secret tomcat–ingress–secret

```
[root@k8s-master test]# kubectl describe secret tomcat-ingress-secret
Name:         tomcat-ingress-secret
Namespace:    default
Labels:       <none>
Annotations:  <none>

Type:  kubernetes.io/tls

Data
====
tls.crt:  1281 bytes
tls.key:  1675 bytes
[root@k8s-master test]#
```

创建Ingress

修改上一节中创建的Ingress YAML文件：

vim test-tomcat-ingress-nginx.yml

apiVersion: extensions/v1beta1

kind: Ingress

metadata:

  name: test-tomcat-ingress-nginx

  annotations:

    kubernetes.io/ingress.class: "nginx"

spec:

  tls:

  - hosts:

    - test.pmx.com

    secretName: tomcat-ingress-secret

  rules:

  - host: test.pmx.com

    http:

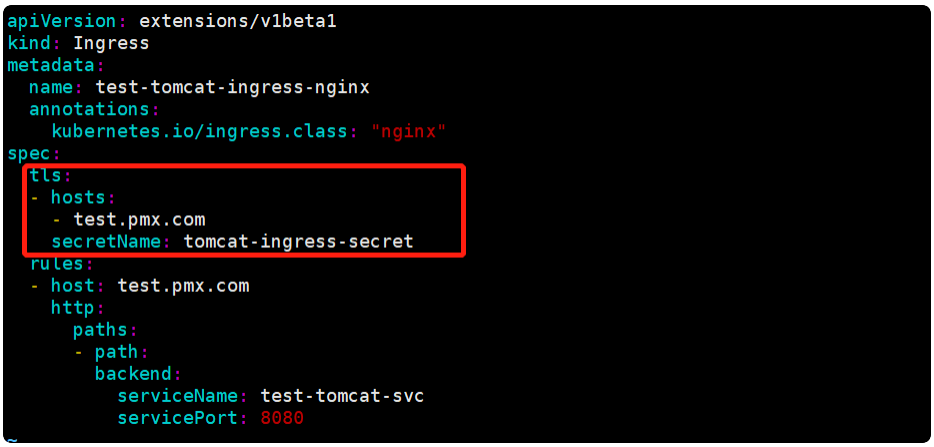
      paths:

      - path:

        backend:

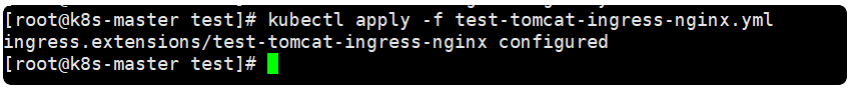
          serviceName: test-tomcat-svc

          servicePort: 8080



使用如下命令更新Ingress对象：

kubectl apply -f test-tomcat-ingress-nginx.yml



kubectl get ingress

```
[root@k8s-master test]# kubectl get ingress
NAME                        CLASS    HOSTS          ADDRESS           PORTS     AGE
test-tomcat-ingress-nginx   <none>   test.pmx.com   192.168.188.132   80, 443   20h
[root@k8s-master test]#
```

可以看到PORT列中出现了443端口。

kubectl describe ingress test-tomcat-ingress-nginx

```
[root@k8s-master test]# kubectl describe ingress test-tomcat-ingress-nginx
Name:             test-tomcat-ingress-nginx
Namespace:        default
Address:          192.168.188.132
Default backend:  default-http-backend:80 (<error: endpoints "default-http-backend" not found>)
TLS:
  tomcat-ingress-secret terminates test.pmx.com
Rules:
  Host          Path  Backends
  ----          ----  --------
  test.pmx.com
                      test-tomcat-svc:8080 (10.244.1.20:8080,10.244.1.21:8080,10.244.1.22:8080)
Annotations:    kubernetes.io/ingress.class: nginx
Events:
  Type    Reason  Age                  From                      Message
  ----    ------  ----                 ----                      -------
  Normal  Sync    2d2h (x5 over 2d23h)  nginx-ingress-controller  Scheduled for sync
[root@k8s-master test]#
```

访问测试

访问地址：https://test.pmx.com:32443/