**AWS动手实验网络ACL**

**实验目的**

定义一条网络ACL

**实验要求**

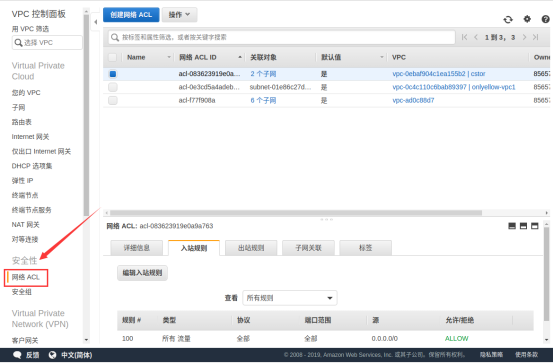
了解网络ACL的基本知识

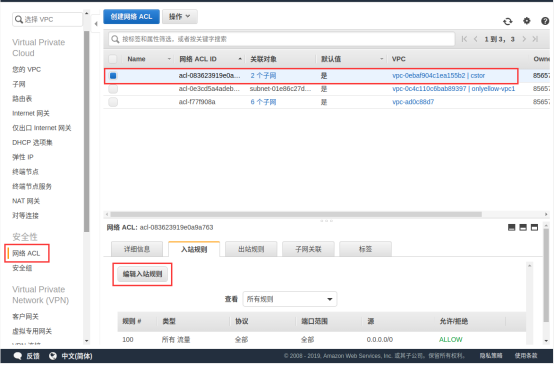
**实验原理**

网络安全访问控制列表（ACL）是VPC的一个可选安全层，可用作防火墙来控制进出一个或多个子网的流量。您可以设置网络ACL，使其规则与您的安全组相似，以便您的VPC添加额外的安全层。

**注意：网络ACL包含规则的编号列表，以供网络ACL按顺序评估（从编号最小的规则开始），以判断流量是否被允许进入或离开任何与网络ACL关联的子网。您可以使用最高规则编号为32766。建议您开始以增量方式创建规则（例如，以10或100的增量增加），这样您就可以在稍后需要时插入新的规则。**

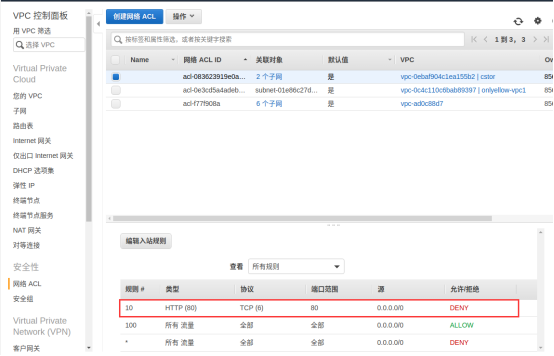
**实验步骤**

1、在VPC左侧导航窗格，点击【网络ACL】，如下：  


2、选择现有的网络ACL【 VPC-×××××××× | cstor】，每个VPC默认自动创建一个网络ACL，点击页面下半部分【入站规则】，如下：  
注意：默认ACL配置为允许所有网络流入和流出与其关联的子网。每个网络ACL还包括规则为星号（\*）的规则，此规则可确保如果数据包与任何其他编号规则不匹配，则会被拒绝。我们无法修改或删除此规则。  


3、在“编辑入站规则”中，新增一条规则，配置如下：  
规则：10  
类型：自定义TCP规则  
协议：TCP（6）  
端口范围：80  
源：0.0.0.0/0  
允许/拒绝：DENY

完成以上配置后，点击【保存】，如下：  


4、现在与此ACL关联的两个子网中的所有实例的80端口将都不能被访问。  


**实验结果**

新增一条网络ACL，限制所有人访问80端口  
