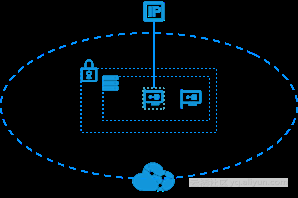
# ECS 8080端口连接拒绝问题排查

**摘要：** 如果遇到ECS部署的web服务无法访问，可以参考这个case进行排查

## 用户ECS网络设置

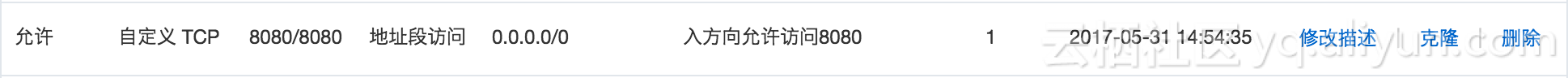
[](https://yq.aliyun.com/articles/javascript:;)

* 上图是用户ECS的网络示意图：
  1. ecs处于vpc网络下
  2. ecs加入了一个安全组，该安全组出入方向均开放8080端口
  3. ecs有两个网卡，一个私网主网卡（有虚线的网卡），一个私网normal网卡
  4. ecs绑定了一个EIP（弹性公网IP）实现与公网互通

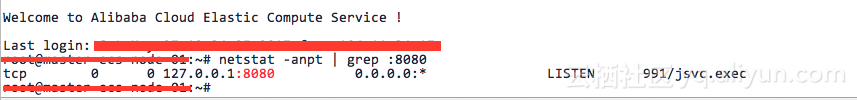
## 问题现象

* 8080端口无法连接

## 排查过程

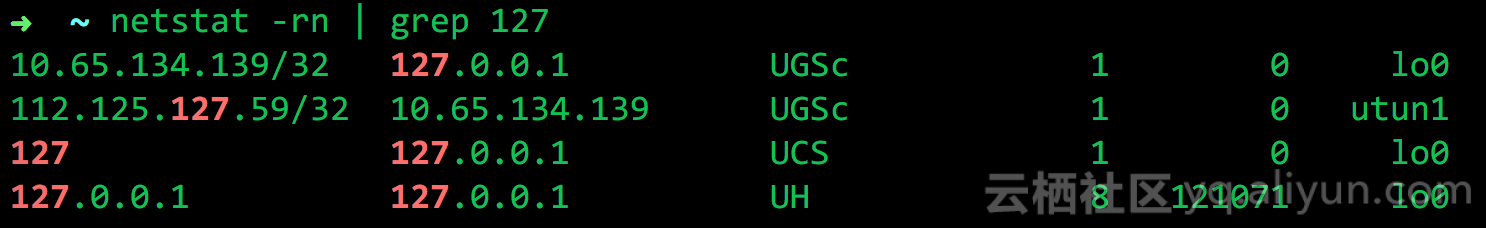
首先确认安全组规则中，的确开放了入和出的8080端口，说明安全组配置没有问题：  
[](https://yq.aliyun.com/articles/javascript:;)  
[](https://yq.aliyun.com/articles/javascript:;)

****注意：经典网络不允许在安全组规则中设置 0.0.0.0/0 的地址段，vpc网络由于网络之间是隔离的，所以这样设置问题不大。****

安全组设置没有问题，那重点怀疑用户的8080监听服务没有启动，用户反馈说本地curl 8080服务能够正确返回，说明服务已经启动. 要求用户反馈8080在监听的截图如下：  
[](https://yq.aliyun.com/articles/javascript:;)

从上图能够看出用户的web服务被绑定在127.0.0.1的8080端口上了，而这会导致公网无法访问该web服务，解释如下：

* 1. 127.0.0.1是一个回送（loopback）地址，指本地机，一般用来测试使用
  2. 127.0.0.1是通过网卡传输，依赖网卡，并受到网络防火墙和网卡相关的限制,这也是跟localhost重要区别之一，localhost是不走网卡的，因此防火墙设置对localhost是无效的。
  3. 正常的网络包都是从ip层进入链路层，然后发送到网络上，而发向127.0.0.1的包，直接在IP层短路了，也就是发到IP层的包直接被IP层接收了，不再向下发送。这也就决定了web应用绑定在127.0.0.1上是不可能被公网访问到的。

为了印证发向127.0.0.1无法被传输到网络上，可以使用netstat -r命令来看一下本机路由表的设置：  
[](https://yq.aliyun.com/articles/javascript:;)

稍微解释一下上面的表格：

* + 第一列：Destination，目标网段或者主机
  + 第二列：Gateway，网关地址，”\*” 表示目标是本主机所属的网络，不需要路由
  + 第三列：Flags，标记。一些可能的标记如下：
    - U ：路由是活动的
    - H ： 目标是一个主机
    - G ：路由指向网关
  + R ：恢复动态路由产生的表项
    - D ：由路由的后台程序动态地安装
    - M ：由路由的后台程序修改
    - ! ：拒绝路由
  + 第四列：Ref，路由项引用次数
  + 第五列：Use，此路由项被路由软件查找的次数
  + 第六列：Iface，该路由表项对应的输出接口

从截图可以看出，目标是127的数据包，网关地址仍然是127，这就印证了127是回送（loopback）地址。

解决方案：

* 1. 修改web容器配置，把web应用绑定在ecs主网卡上。ECS bind EIP，实际上相当于EIP与ECS私有主网卡建立了映射关系，因此通过EIP:8080来访问web服务，最终就会\*请求到私网主网卡:8080上。
  2. 更好的做法是把web服务绑定在0.0.0.0这个特殊IP上，关于0.0.0.0，这个IP并不是真实存在的，我们ping不通它，它只是一个符号，代表当前设备的IP。绑定在0.0.0.0上后无论是通过127.0.0.1还是本机ip去访问web服务，都是可以的。

## 总结

* 127.0.0.1是一个回送（loopback）地址，只能用于本机测试，web应用绑定在127.0.0.1上是不可能被公网访问到的。
* 把web应用绑定在ECS私网主网卡上就可以实现用EIP从公网来访问web服务，因为EIP与ECS私有主网卡建立了映射关系。
* 0.0.0.0是个特殊的IP，绑定在0.0.0.0上后无论是通过127.0.0.1还是本机ip去访问web服务，都是可以的。