# AC对接虚拟化部署的认证服务器不成功

Portal 谭奇伟 2024-01-10 发表

## 组网及说明

AC旁挂核心，本地转发。

由于认证服务器分为主备，地址分别是72和73，为了接入设备的配置方便，设计为虚拟化后采用统一的地址74与外界通信。

因此AC上配置的radius scheme和portal web-server以及portal server下相关的配置都使用74地址进行对接：

```
#
radius scheme portal-server
 primary authentication 10.1.6.74
 primary accounting 10.1.6.74
 user-name-format without-domain
 nas-ip 10.10.0.5
#
portal web-server portal-server
 url http://10.1.6.74/a79.htm
#
portal server portal-server
 ip 10.1.6.74 key cipher $c$3$iMo798Y0l9XnCW7GlzehLgthnee7uefCektWfQ==
 server-type cmcc
#
```

## 告警信息

无

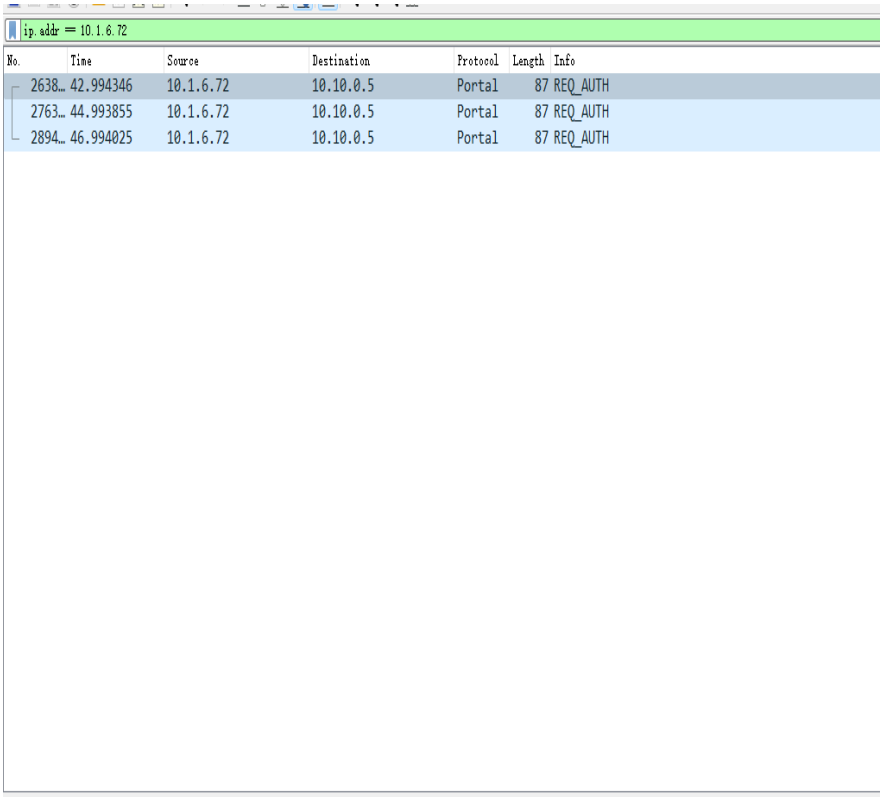
## 问题描述

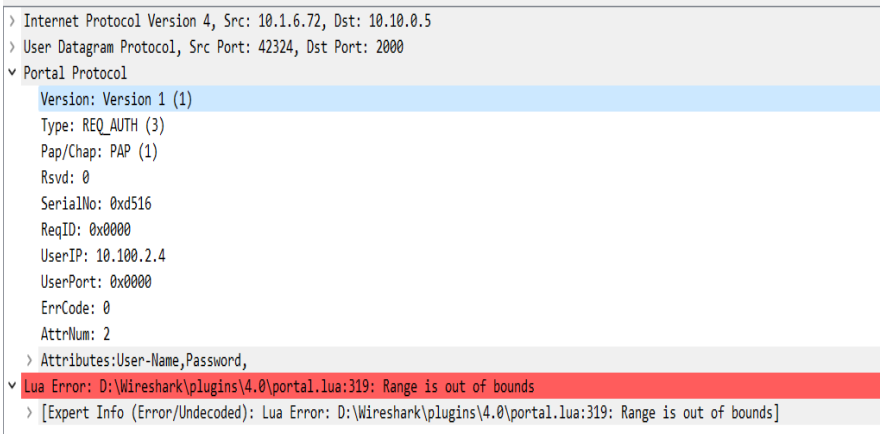
终端连接wifi后弹出的认证页面正常，但是认证失败，终端上认证页面报错如下：


过程分析

通过AC和服务器之间抓包发现，服务器给AC发送了req_auth报文，但并未收到AC发起的access requ

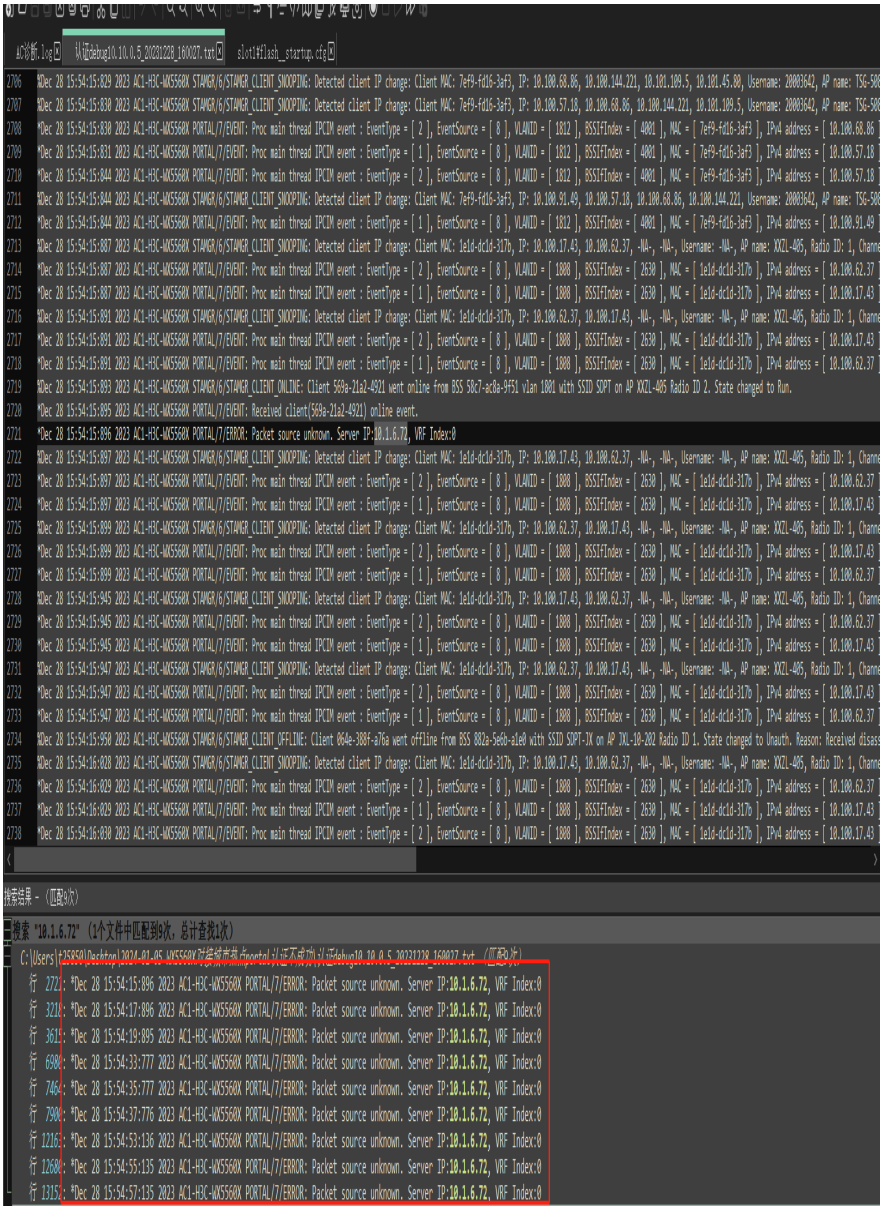
est（radius）报文，也未收到AC发送给服务器的ack_auth报文：




通过在AC上debug portal all和debug radius all发现，虽然服务器设计为虚拟化后采用统一的地址74与外界通信，但实际服务器采用72的地址向AC发送了req_auth报文。

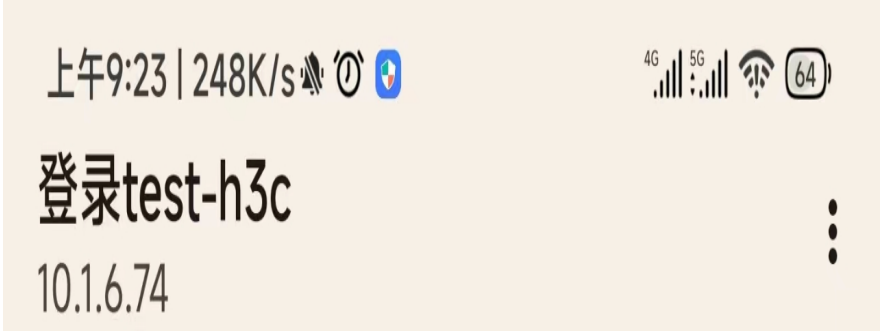
此时由于AC上是按照设计要求配置74的地址与服务器对接，因此在radius scheme，portal server和portal web-server下相关的配置都使用74地址进行对接，因此将源地址为72的服务器发送过来的portal报文识别为无效报文直接丢弃。



进一步地，将AC上portal server和portal web-server，radius scheme下的地址改为72：

```
#
portal web-server portal-server
 url http://10.1.6.72/a79.htm
#
portal server portal-server
 ip 10.1.6.72 key cipher $c$3$iMo798Y0l9XnCW7GlzehLgthnee7uefCektWfQ==
 server-type cmcc
#
radius scheme portal-server
 primary authentication 10.1.6.72
 primary accounting 10.1.6.72
 user-name-format without-domain
 nas-ip 10.10.0.5
#
```

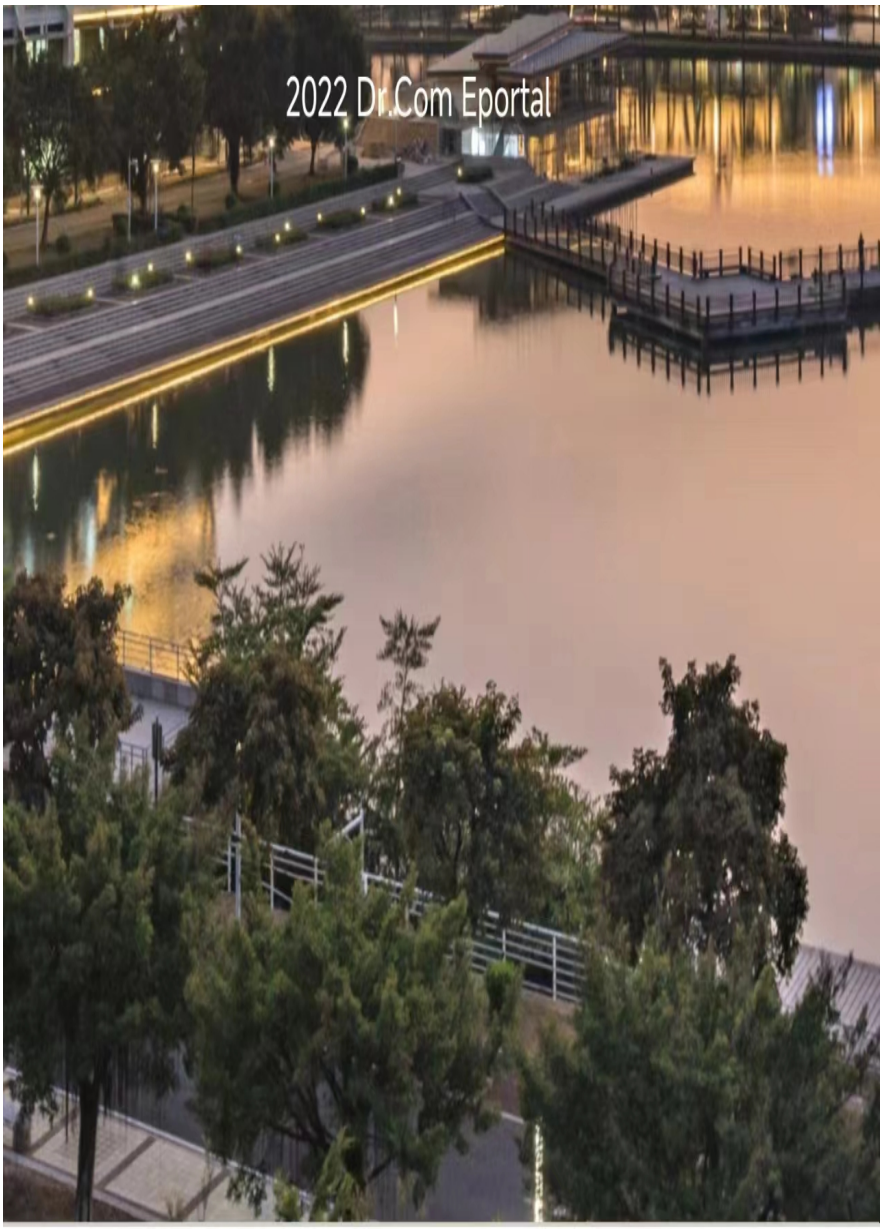
修改之后，认证还是出现了异常，报错为AC999



AC999

返回

其他




再次在AC和服务器之间抓包发现，这次AC收到服务器来自72发来的req_auth报文后，向服务器发起了access request（radius）认证请求，但是却未收到服务器的radius应答报文，导致认证失败。
在服务器侧查看日志发现，服务器上radius模块却按照74地址与外界交互认证报文，因此又将AC上radius下之前改为72的地址又再次修改为74，然后认证成功。

```
#
radius scheme portal-server
 primary authentication 10.1.6.74
 primary accounting 10.1.6.74
 user-name-format without-domain
 nas-ip 10.10.0.5
#
```

## 解决方法

最后，现场决定将虚拟化的服务器重新使用主备模式部署，并分别使用72和73的主备地址与AC及其它接入设备进行portal认证对接，但是这涉及到AC与主备服务器对接，那么这样的情况应当怎么配置呢？
这里选取了一个AC和主备IMC认证对接的配置方法，现场照此配置后对接成功，以下列出关键配置段：

```
#
radius scheme portal
 primary authentication 1.1.1.1
 primary accounting 1.1.1.1
 secondary authentication 1.1.1.2
 secondary accounting 1.1.1.2
 key authentication cipher $c$3$IFFvw9uzrY2iITN2kc4MkGbVUKggZO5Bjg==
```

```
 key accounting cipher $c$3$dAwxH6y9twc3OLYCQU1LhhV11DtUfCKd7g==
 user-name-format without-domain
 nas-ip X.X.X.X
#
radius dynamic-author server
 client ip 1.1.1.1 key cipher $c$3$FSEMTlq5J/hpeilD+glsezD63pzzecqM4Q==
 client ip 1.1.1.2 key cipher $c$3$wVL+0kiodpYq9MjLhBx+dfuheB0nmrptDA==
#
domain portal
 authorization-attribute idle-cut 10 10240
 authentication portal radius-scheme portal
 authorization portal radius-scheme portal
 accounting portal radius-scheme portal
#
portal web-server portal
 url http://1.1.1.1:80/portal
 server-detect interval 20 log trap
 server-detect url http://1.1.1.1:80/portal
 url-parameter nasip value X.X.X.X
 url-parameter wlanacname value AC
 url-parameter wlanuserip source-address
#
portal web-server portal_backup
 url http://1.1.1.2:80/portal
 server-detect interval 20 log trap
 server-detect url http://1.1.1.2:80/portal
 url-parameter nasip value X.X.X.X
 url-parameter wlanacname value AC
 url-parameter wlanuserip source-address
#
portal server portal
 ip 1.1.1.1 key cipher $c$3$s1xfsy28vDTowpGtlNgmOdik0kKDjlhfhQ==
 server-detect log
#
portal server portal_backup
 ip 1.1.1.2 key cipher $c$3$HNCyD85qNPMzTSQEzqZopxFaXzXpOvM1JA==
 server-detect log
#
portal mac-trigger-server portal
 ip 1.1.1.1
#
portal mac-trigger-server portal_backup
 ip 1.1.1.2
#
wlan service-template portal
 ssid test
 client forwarding-location ap
 portal enable method direct
 portal domain portal
 portal bas-ip X.X.X.X
 portal apply web-server portal
 portal apply web-server portal_backup secondary
 service-template enable
#
```