

知 某局点portal认证接入场景匹配不准确

iMC

范中鹏 2019-12-08 发表

组网及说明

该局点移动终端连接WIFI为GDZY，接入服务为：***员工无线网络接入服务，缺省策略为：***员工笔记本无线能访问内外网接入策略，策略中认证方式为账号密码 + 动态密码。正常情况下，用户持移动终端接入该网络，应该匹配的接入场景为：***员工GDZY手持终端（操作系统分组）、***员工GDZY手持终端（终端类型分组）。分别以设备类型（smart phone）、操作系统（Android、IOS）等识别终端，接入策略均是***员工手持终端动态密码只能访问外网接入策略，策略中认证方式为账号密码。

问题描述

某局点portal认证接入场景匹配不准确，用户移动终端进行Portal认证，部分用户认证失败，提示原因为“动态密码不能为空,请输入动态密码”

认证失败日志列表							
定制认证失败原因							
账号名	登录名	服务名称	认证失败原因	认证失败时间	用户IP地址	用户MAC地址	详细信息
xionghm	xionghm	广州广无线网络接入服务2	E63637: 动态密码不能为空, 请输入动态密码。	2019-10-11 10:39:59	192.168.20.101	94:87:e0:51:7e:82	查看详情
xionghm	xionghm	广州广无线网络接入服务2	E63637: 动态密码不能为空, 请输入动态密码。	2019-10-11 10:39:45	192.168.20.101	94:87:e0:51:7e:82	查看详情
xionghm	xionghm	广州广无线网络接入服务2	E63637: 动态密码不能为空, 请输入动态密码。	2019-10-11 10:39:31	192.168.20.101	94:87:e0:51:7e:82	查看详情
xionghm	xionghm	广州广无线网络接入服务2	E63637: 动态密码不能为空, 请输入动态密码。	2019-10-11 10:38:40	192.168.20.101	94:87:e0:51:7e:82	查看详情
广州广无线网络接入服务2							

过程分析

分析诊断日志，结合抓包文件并对比同一用户认证成功与认证失败时的后台信息，发现认证失败时，iMC没有正确判断用户的接入场景而使用户进入缺省接入策略导致用户认证失败。

认证失败时，接入设备上传到iMC的Radius报文，缺少了30（SSID）和208（option55，客户端一个属性）号属性，使得iMC无法识别用户SSID和设备类型，故而无法匹配由SSID + 设备类型做为判断条件的接入场景。

抓包文件中也记录，即使AC上配置了Portal重定向报文中携带SSID参数，认证时也没有携带该参数。正常日志如下

```
CODE = 1.
ID = 51.
ATTRIBUTES:
  User-Name(1) = "...xionghm".
  Password(2) = "$$$".
  NAS-IP-Address(4) = 3232260631.
  NAS-Identifier(32) = "GZC-Wireless-Master-98.21".
  NAS-Port(5) = 16781532.
  NAS-Port-Id(87) = "0100001000000220".
  NAS-Port-Type(61) = 19.
  Service-Type(6) = 2.
  Framed-Protocol(7) = 255.
  Calling-Station-Id(31) = "94-87-E0-51-7E-82".
  Called-Station-Id(30) = "74-1F-4A-D5-49-40:GDZY".
  Acct-Session-Id(44) = "1191011104933128250046d".
  Framed-IP-Address(8) = 3232240741.
  hw_Connect_ID(26) = 1153.
  hw_Product_ID(255) = "H3C WX5540E".
  hw_IP_Host_Addr(60) = "192.168.20.101 94:87:e0:51:7e:82".
  H3C_DHCP_Option55(208) = "0103060f1a1c333a3b2b".
  hw_Nas_Startup_Timetamp(59) = 1570148654.
```

现场异常日志如下：

```
CODE = 1.
ID = 210.
ATTRIBUTES:
  User-Name(1) = "...xionghm".
  Password(2) = "$$$".
  NAS-IP-Address(4) = 3232260631.
  NAS-Identifier(32) = "GZC-Wireless-Master-98.21".
  NAS-Port(5) = 16781532.
  NAS-Port-Id(87) = "0100001000000220".
  NAS-Port-Type(61) = 15.
  Service-Type(6) = 2.
  Framed-Protocol(7) = 255.
  Calling-Station-Id(31) = "94-87-E0-51-7E-82".
  Acct-Session-Id(44) = "11910111036001282500455".
  Framed-IP-Address(8) = 3232240741.
  hw_Connect_ID(26) = 1129.
  hw_Product_ID(255) = "H3C WX5540E".
  hw_IP_Host_Addr(60) = "192.168.20.101 94:87:e0:51:7e:82".
  hw_Nas_Startup_Timetamp(59) = 1570148654.
```

IMC没有正确判断用户的接入场景而使用户进入缺省接入策，日志记录。

```
(NULL) ; (NULL) ; prsRawPkt: chk-sum 671832723.
.L) ; prsMixedUsr: in [NAK(S)D(xionghm), out [xionghm].
(NULL) ; setPxyType: No domain name.
(NULL) ; getLanAuthAttrFromItem: no attribute of DEVICE-SN.
(NULL) ; getLanAuthAttrFromItem: no attribute of DEVICE-IMSI.
.) ; lanAuthMsgProc.Init: a"th-type 1, state , pxy , sequence .
(NULL) ; parseVer: invalid ver .
(NULL) ; lanAuthMsgProc.exec: begin...
(NULL) ; lanAuth.exec: Begin...
.) ; onlineLicChk: UAM LicChk OK[1441 3800].
(NULL) ; c.getUsrSrvInfo: [SrvName:xionghm: MAC:94:87:a0:51:7a:82: UserIp:{c0a81
NULL) ; matchSvcStragy: matching default rule(41) under srvc-templ 62.
(NULL) ; c.getUsrSrvInfo: fail 0W.
(NULL) ; lanAuth.exec: before dealstate with evntSeq .
(NULL) ; lanAuth.authByBlacklist: user xionghm, eventSeqID: KpcjenMY.
NULL) ; chAndGetPasswd: fail to call chkDynamicPwd.
NULL) ; lanAuth.authByBlacklist: fail to call chkAndGetPasswd.
NULL) ; lanAuth.exec: failed to be authenticated by the black list, retCode: 63637.
NULL) ; lanAuthMsgProc.finsh: fail to authenticate the request message. retCode: 63
```

Radius报文中缺少两个重要属性，说明做为接入设备的AC无法获取终端SSID信息，很可能是终端连接的AP没有注册到该AC上。通过检查AC配置，发现两台AC做VRRP备份，AP本地转发，开启认证的VLAN接口对外发布虚地址，所有用户认证接口都是主AC的接口。部分AP在主备AC上配置的优先级相同（都是priority level 7），使得这些AP部分注册到备AC，当这些AP关联的用户在主AC进行认证时，主AC就无法从AP中获取用户接入的SSID和终端信息。

部分AP注册到备AC：

```
<GZC-wireless-master-98.21>dis w1
<GZC-wireless-master-98.21>dis wlan ap all
Total Number of APs configured      : 52
Total Number of configured APs connected : 52
Total Number of auto APs connected   : 0
Total Number of APs connected       : 52
Maximum AP capacity                  : 64
Remaining AP capacity                 : 12
AP Profiles
State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad
       C = Config, R = Run, KU = KeyUpdate, KC = KeyCfm
       M = Master, B = Backup
-----
AP Name      State Model      Serial-ID
-----
iap-j31f-a01 R/M WA4620i-ACN 210235A1B5C158000661
iap-j31f-a02 R/M WA4620i-ACN 210235A1B5C158000704
iap-j31f-a03 R/M WA4620i-ACN 210235A1B5C158000854
iap-j31f-a04 R/M WA4620i-ACN 210235A1B5C158000438
iap-j31f-a05 R/M WA4620i-ACN 210235A1B5C158000827
iap-j31f-b01 R/M WA4620i-ACN 210235A1B5C158000797
iap-j31f-c01 R/M WA4620i-ACN 210235A1B5C158000840
iap-j31f-c02 R/M WA4620i-ACN 210235A1B5C158000447
iap-j31f-d01 R/M WA4620i-ACN 210235A1B5C158000782
iap-j31f-d02 R/M WA4620i-ACN 210235A1B5C158000658
iap-j32f-a01 R/M WA4620i-ACN 210235A1B5C158000242
iap-j32f-a02 R/M WA4620i-ACN 210235A1B5C158000171
iap-j32f-a03 R/M WA4620i-ACN 210235A1B5C158000921
iap-j32f-a04 R/M WA4620i-ACN 210235A1B5C158000693
iap-j32f-b01 R/M WA4620i-ACN 210235A1B5C158000015
iap-j32f-b02 R/M WA4620i-ACN 210235A1B5C158000756
iap-j32f-d03 R/M WA4620i-ACN 210235A1B5C158000173
iap-j32f-d04 R/M WA4620i-ACN 210235A1B5C158000016
iap-j32f-d05 R/M WA4620i-ACN 210235A1B5C158001046
iap-j33f-a01 R/M WA4620i-ACN 210235A1B5C158000859
iap-j33f-a02 R/M WA4620i-ACN 210235A1B5C158000445
iap-j33f-a03 R/M WA4620i-ACN 210235A1B5C158000829
iap-j33f-a04 R/M WA4620i-ACN 210235A1B5C158000872
iap-j33f-b01 R/B WA4620i-ACN 210235A1B5C158000857
iap-j33f-b02 R/M WA4620i-ACN 210235A1B5C158000838
iap-j33f-c01 R/M WA4620i-ACN 210235A1B5C158000007
iap-j33f-c02 R/B WA4620i-ACN 210235A1B5C158000032
iap-j33f-c03 R/M WA4620i-ACN 210235A1B5C158000499
iap-j33f-c04 R/M WA4620i-ACN 210235A1B5C158000282
iap-j33f-c05 R/B WA4620i-ACN 210235A1B5C158000863
iap-j34f-a01 R/B WA4620i-ACN 210235A1B5C158000885
iap-j34f-a02 R/B WA4620i-ACN 210235A1B5C158000917
iap-j34f-a03 R/B WA4620i-ACN 210235A1B5C158000861
iap-j34f-a04 R/B WA4620i-ACN 210235A1B5C158000013
iap-j34f-a05 R/B WA4620i-ACN 210235A1B5C158000812
iap-j34f-a06 R/M WA4620i-ACN 210235A1B5C158000725
```

解决方法

AC配置问题导致部分认证报文无法上传用户SSID信息。建议调整配置，将AC2上所有AP配置的优先级调低，使AP都注册到主AC，用户认证也都在主AC进行