iNode进行Portal认证提示“安全认证失败”故障经典案例

罗孝晨 2017-05-09 发表

PC使用iNode进行Portal认证，认证成功后很快iNode就会提示“安全认证失败，当前连接即将被强行终端，请联系管理员”。

一、首先收集UAM调试日志

% 2017-03-02 16:14:26.186 ; [L_DEBUG (4)] ; [13192] ; LAN ; guest@system ; 1 ;
20e34a6871164545b7bf1113481a3fe3 ; (NULL) ; RT[0]: Receive message from 10.240.129.1:
CODE = 1.\\认证开始报文
ID = 49.
ATTRIBUTES:
User-Name(1) = "..bTQLGB0BY3YvGB5nK1Mtf4Z6Zi0= guest@system".\\用户名
Password(2) = "$$$".
Service-Type(6) = 2.
NAS-Identifier(32) = "H3C".
NAS-Port(5) = 16785537.
Calling-Station-Id(31) = "70-5A-0F-D5-92-F8".\\终端MAC地址
Called-Station-Id(30) = "70-3D-15-4F-96-A4".\\接入设备MAC地址
Framed-IP-Address(8) = 183533924.\\用户IP地址
NAS-Port-Id(87) = "0100002000000129".
NAS-IP-Address(4) = 183533825.\\设备IP地址
设备发来认证开始报文后，iMC回应了认证成功报文，如下所示；
% 2017-03-02 16:14:26.197 ; [L_DEBUG (4)] ; [10688] ; LAN ; guest@system ; 2 ; 20e34a687116454
5b7bf1113481a3fe3 ; e9DVAKAk ; Send message attribut list:
Code = 2\\认证成功报文
ID = 49
ATTRIBUTES:
User-Name(1) = ..bTQLGB0BY3YvGB5nK1Mtf4Z6Zi0= guest@system
Service_Type(6) = 2
State(24) = e9DVAKAk
Termination-Action(29) = 0
Session-Timeout(27) = 86401
Acct-Interim-Interval(85) = 600
hw_User_Notify(61) =
IF_PROXY = 0
IF_DOUBLE_NETCARD = 0
IF_IE_PROXY = 0
FRAMED_IP_SET_MODE = 0
IF_CHECK_MODIFY_MAC = 0
IF_CHECK_SAME_MAC = 0
SERVER_VERSION = R003B03D004SP20
EAD_EVENT_SEQ_ID = e9DVAKAk
% 2017-03-02 16:14:26.209 ; [L_DEBUG (4)] ; [800] ; LAN ; guest@system ; 4 ;
756e38a5923b442294b10eb1762a3c07 ; (NULL) ; RT[1]: Receive message from 10.240.129.1:
CODE = 4.\\计费报文
ID = 22.
ATTRIBUTES:

User-Name(1) = "..bTQLGB0BY3YvGB5nK1Mtf4Z6Zi0= guest@system".
NAS-Identifier(32) = "H3C".
NAS-Port(5) = 16785537.
Calling-Station-Id(31) = "70-5A-0F-D5-92-F8".
Called-Station-Id(30) = "70-3D-15-4F-96-A4".
Framed-IP-Address(8) = 183533924.
Acct-Session-Id(44) = "000000072013-01-01:02:11:53-0000000e081".\\计费会话标识
Acct-Authentic(45) = 1.
NAS-IP-Address(4) = 183533825.
Acct-Status-Type(40) = 1.\\计费开始报文
Acct-Delay-Time(41) = 0.
Event-Timestamp(55) = 1357006313.
% 2017-03-02 16:14:26.218 ; [L_DEBUG (4)] ; [12032] ; LAN ; SYS ; (NULL) ; (NULL) ; (NULL) ; La
nAcctStartProcess: insert tbl_online done.\\7.1版本EIA根据计费报文插入在线表成功。
% 2017-03-02 16:14:26.219 ; [L_DEBUG (4)] ; [12032] ; LAN ; guest@system ; 5 ; 756e38a5923b442
294b10eb1762a3c07 ; e9DVAKAk ; Send message attribut list:
Code = 5\\计费回应报文
ID = 22
ATTRIBUTES:
hw_User_Notify(61) =
EAD_EVENT_SEQ_ID = e9DVAKAk
EAD_PROXY_IP = 184182067\\策略服务器地址
EAD_PROXY_PORT = 9019\\策略服务器端口
EAD_PROXY_IP_PREFERENCE = 0
从上述日志分析，用户guest@system完成了一次完成的认证过程。由于安全认证失败是策略服务器下发给iNode客户端的，因此需要进一步分析策略服务器日志。
二、策略服务器调试日志分析
2017-03-02 16:14:28 [策略服务器] [信息 (0)] [43] [ProxyRequestHandler::run] guest ; EAD认证上线请求报文(1) ; 70:5A:0F:D5:92:F8 ; 0 ; 10.240.129.100 ; 报文解析成功
userName: guest\\用户名guest
hwAddr: 70:5A:0F:D5:92:F8
clientPort: 10102
clientVersion: CH V7.20-0408
clientDisVersion: CH iNode PC 7.2 (E0408)
isIndependent: 1
patchStamp: hwRdNUwTWziuF+8wn1kFSA==
patchFailStamp: 2NDOXkXvVt8=
SupSoftRunCheckType: true
supBlackWhiteGroup: true
supPureWhiteGroup: true
supProcessCheckMD5: true
supBWGroupWithDtl: true
iSupCmp: true
ClientType: PC
ipv6Addr:
ipAddr: 10.240.129.100
hostname: nfw2588DC
BindToDomain: H3C
IsDomainUser: true
LogonDomain: H3C
DamClientId: 48F97BB25235E04598163905B81C58C1
iSupWanControl: false
iSupOnlineUnauthNetAudit: false
iSupACL: false
iSupURL: false
iSupRegHighOS: true
iSupAlias: true
OSInfo: Windows 7 Enterprise
CustomerizedTime: 2016-08-17 11:00:51
iSupOnlyWAV: true
iSupShareCheck: 1
iSupAntiServiceMonitor: true
diskDriveID: 57363242453950342020202020202020202020
baseboardID: 35434736313831444443202020202020202020

iSupblackssid: false
vendor: Hewlett-Packard
model: HP EliteBook 820 G2
Proxy IP: 10.250.101.51
attr:ipType: 0
Address: 10.240.129.100
Port: 10102
MsgId: 1793
MsgType: 1
2017-03-02 16:14:28 [策略服务器] [错误 (141584)] [22] [CamsOnlineTable::synchronize] 无法找到用户"OnlineUser<guest, 10.240.129.100, null, 70:5A:0F:D5:92:F8, null>"(userServiceId="null")在CAMS在线表的对应记录
2017-03-02 16:14:28 [策略服务器] [信息 (0)] [22] [RequestProcessor::procRequestLogon] 同步用户 guest 上线请求处理时，获取在线信息失败\\策略服务器无法获取用户的在线信息
2017-03-02 16:14:28 [策略服务器] [警告 (141001)] [22] [DataCacheManager::queryUserServiceInfo] 无法从数据库中查询到用户业务信息（userServiceName=guest）\\此记录说明从tbl_online无法找到对应guest用户
2017-03-02 16:14:28 [策略服务器] [调试 (0)] [22] [RequestProcessor::procRequestLogon] get service info of the user failed.
2017-03-02 16:14:28 [策略服务器] [调试 (0)] [22] [RequestProcessor::procRequestLogon] null
2017-03-02 16:14:28 [策略服务器] [调试 (0)] [22] [RequestProcessor::procReqLogon] End procReqLogon()
2017-03-02 16:14:28 [策略服务器] [信息 (0)] [22] [RequestProcessor::processRequest] End processRequest() successfully
2017-03-02 16:14:28 [策略服务器] [信息 (0)] [22] [RequestProcessor::processRequest] guest ; EAD认证上线回应报文(2) ; null ; 70:5A:0F:D5:92:F8 ; 10.240.129.100 ; 回应报文属性列表:
MsgId: 1793
MsgType: 2
attr:ipType: 0
Address: 10.240.129.100
Proxy IP: 10.250.101.51
attr:encrypt: true
syncUserError: true\\同步用户失败标识
从策略服务器日志可以看出，iNode与策略服务器交互安全认证报文时，策略服务器无法从在线表中找到对应的guest用户的在线信息，因此匹配在线用户失败，策略服务器通知iNode下线。
为何会匹配在线用户失败，从UAM调试日志看用户在线表已经成功创建了。但是有一点需要注意UAM创建的在线表用户名为guest@system，而策略服务器匹配的在线用户是guest，两者差了一个后缀system。为何两这的用户名不一致呢？需要进一步分析。
而现场iMC接入服务配置了服务后缀system，设备上RADIUS方案下配置的user-name-format with-domain，同时指定了domain default enable system，用户在iNode侧输入的用户名是guest，根据上述配置，设备在给iMC发送认证及计费报文时，会携带上服务后缀的。而iNode上报给策略服务器的用户名则不会携带服务后缀。因此才会出现两者的用户名不一致的问题。
根据下面对接入服务后缀的配置要求表格，针对现场的情况有两种结局办法

表1 iMC 中服务后缀的选择

认证连接用户名	设备用于认证的 Domain	设备 Radius scheme 中的命令	iMC 中服务的后缀
X@Y	Y	user-name-format with-domain	Y
		user-name-format without-domain	无后缀
X	[Default Domain] 设备上指定的缺省域	user-name-format with-domain	[Default Domain]
		user-name-format without-domain	无后缀

1、接入服务后缀配置与设备上的dmoain名称一致，RADIUS SCHEME配置user-name-format with-domain,认证用户名采用X@Y的形式
2、接入服务不配置服务后缀，RADIUS SCHEME配置user-name-format without-domain，设备上指定default domain xx，认证用户名采用X的形式。
以上两种方法均可以保证设备上传的RADIUS报文的USERNAME属性值与iNode上传给策略服务器的格式保持一致。策略服务器则可以正确匹配到在线用户。
1、学会分析策略服务器日志及UAM调试日志
2、仔细检查配置是否合理正确。