

知 iMC-TAM与CISCO设备对接偶尔认证失败问题的解决办法

Radius 罗孝晨 2016-07-28 发表

某局点使用iMC-TAM组件与CISCO交换机对接进行TAM认证，据现场反馈，使用TAM账号登录CISCO交换机偶尔可以成功，偶尔失败。

无

- 1、与CISCO设备对接使用的是TACACS+协议，该协议TYPE类型分为：认证、授权、计费三部分。根据故障现象，可以推断出问题出在认证过程中。首先查看iMC-TAM页面中，设备用户管理-日志管理-认证日志，发现问题出现时间段并没有认证失败日志。
- 2、将TAM日志级别修改为“调试”级别。然后复现问题，同步在iMC服务器上运行抓包。收集抓包和\$IMC/TAM/log下日志文件。

用户 > 设备用户策略管理 > 业务参数配置 > 系统配置 > 运行日志参数配置

运行日志参数配置

日志级别	调试
日志保留时长(天) *	30 ?

确定 取消

3、分析TAM日志

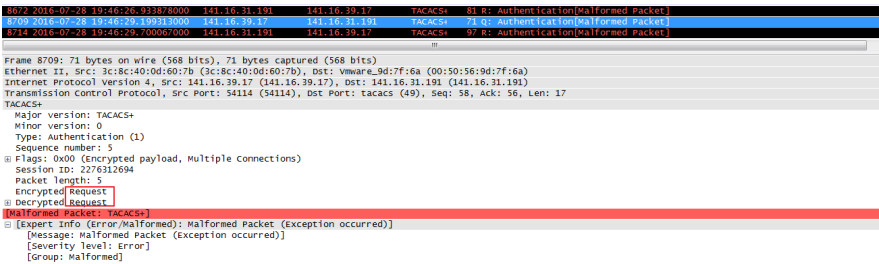
```
% 2016-07-28 19:06:12 ; [L_DEBUG (4)] ; [9568] ; TAM ; $SYS$ ; (NULL) ; (NULL) ; (NULL) ; CheckMsgBody(): Recv msg content is RT[0]: Receive message from 141.16.39.17:\\该地址为设备IP地址
PACKET_TYPE = AUTHEN.\\认证请求报文
AUTHEN_ACTION = AUTHEN.
AUTHEN_PRIV_LEVEL = 15.\\认证权限级别，0x0f即15为最高级别
AUTHEN_AUTHEN_TYPE = TAC_PLUS_AUTHEN_TYPE_ASCII.\\认证类型：ASCII值
AUTHEN_AUTHEN_SERVICE = TAC_PLUS_SVC_ENABLE .
AUTHEN_USER = 123.\\用户名为123
AUTHEN_PORT = tty1.
AUTHEN_REM_ADDR = 141.16.47.110.
AUTHEN_DATA = .
.
% 2016-07-28 19:06:12 ; [L_DEBUG (4)] ; [4064] ; MNG ; $SYS$ ; (NULL) ; (NULL) ; (NULL) ; Begin processAuthenItem().\\内部线程，开始认证过程
% 2016-07-28 19:06:12 ; [L_DEBUG (4)] ; [4064] ; MNG ; $SYS$ ; (NULL) ; (NULL) ; (NULL) ; Begin processAuthenEnable().\\使能TAM认证
% 2016-07-28 19:06:12 ; [L_DEBUG (4)] ; [4064] ; TAM ; $SYS$ ; (NULL) ; (NULL) ; (NULL) ; [send_authen_reply] Sent msg content is
PACKET_TYPE = AUTHEN_REPLY.\\iMC给设备的回应报文
AUTHEN_STATUS = TAC_PLUS_AUTHEN_STATUS_GETPASS.\\回应报文，需要获取密码
AUTHEN_FLAGS = 1.\\用来表示一些特殊条件，1为不加密
AUTHEN_SERVER_MSG = Password:.
AUTHEN_DATA= .
```

从上述日志看认证的第一过程是正常的，认证开始，客户端发送一个START报文给服务器，该报文描述了要执行的身份验证类型，可能还包括用户名和一些认证数据。其实数据包仅作为TACACS+会话开始或者会话充值后紧接着的第一个报文。开始数据包的序列号总是等于1。服务器发送一个REPLY包以响应START包。回复包表明认证是否结束或者继续。通过该报文可以指明下一个报文所需要的新的认证信息。从上述包可以分析出服务器需要获取设备发送密码。所以继续分析下面的报文。

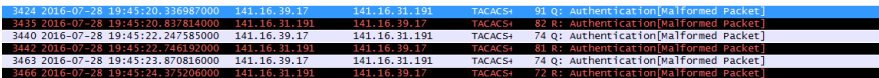
```
% 2016-07-28 19:06:15 ; [WARNING (2)] ; [4064] ; MNG ; $SYS$ ; (NULL) ; (NULL) ; (NULL) ; [read_packet] Read head of packet fail, return NULL.\\读取报文头失败，返回空值
% 2016-07-28 19:06:15 ; [WARNING (2)] ; [4064] ; MNG ; $SYS$ ; (NULL) ; (NULL) ; (NULL) ; [get_authen_continue] Read continue packet fail.\\读取continue报文失败
% 2016-07-28 19:06:15 ; [WARNING (2)] ; [4064] ; MNG ; $SYS$ ; (NULL) ; (NULL) ; (NULL) ; [getInfoFromNAS] Null reply packet, expecting CONTINUE.\\空的回应报文
% 2016-07-28 19:06:15 ; [L_DEBUG (4)] ; [4064] ; MNG ; $SYS$ ; (NULL) ; (NULL) ; (NULL) ; [processAuthenEnable] Get password fail.\\获取密码失败
% 2016-07-28 19:06:15 ; [L_DEBUG (4)] ; [4064] ; MNG ; $SYS$ ; (NULL) ; (NULL) ; (NULL) ; Send no authen reply due to invalid socket or client abort.\\终止该次认证
```

从上述日志可以分析出，服务器没有准确的获取到设备发送的含有密码的continue报文，所以无法给设备回应REPLY报文，从而导致该次认证失败。而通过现场的故障描述，发现设备只是偶尔出现该问题。所以判断基本的认证配置不会出现问题，否则不会有认证成功。判断有可能是设备回应的时间超过了iMC服务器的设定某个时间导致的认证失败。

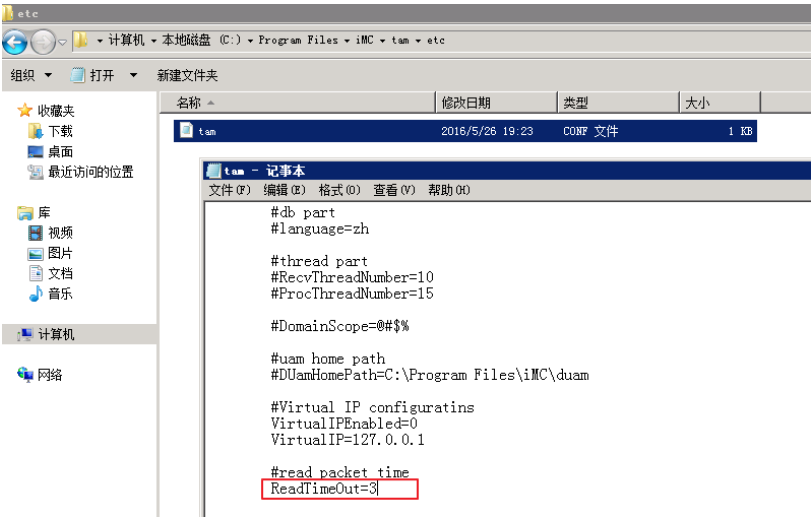
4、为了验证该分析是否正确，进一步分析iMC服务器的抓包。如下图所示：



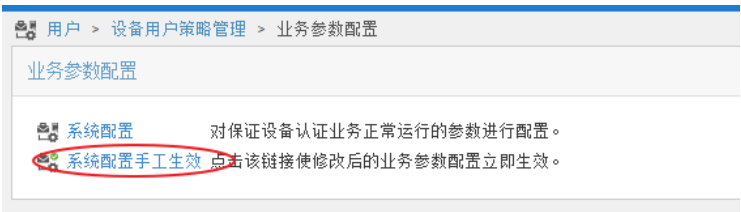
从上述抓包可以明确看出，当iMC服务器在19:46:26给设备发了REPLY报文后，设备等了超过3s的时间才给服务器发送的REQUEST报文。而在正常认证的抓包中，并没有发现设备给iMC发送报文超过3s的，所以判断3s为一个临界值。正常的认证抓包如下图所示：



1、修改iMC安装目录/TAM/etc/tam.conf文件，使用记事本打开该文件。



发现现场的超时时间为3，与分析的结论一致，修改为180，点击系统配置手工生效即可。



1、对于TACACS+协议，要充分理解认证、授权、计费三个过程的区别和报文交互流程，这样才能快速定位问题。