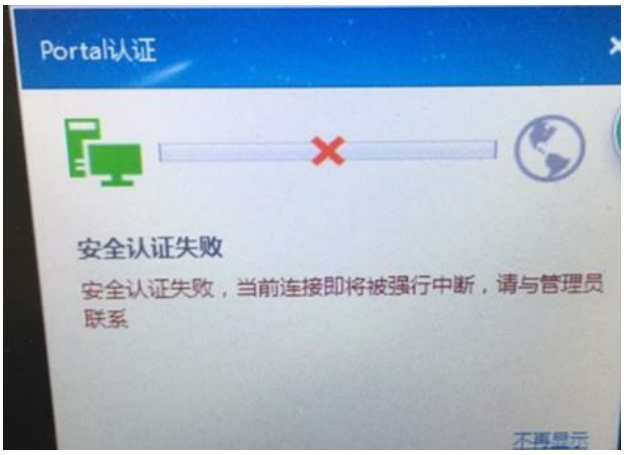
iNode Portal认证不带后缀时不定时提示安全认证失败的原因

寻尚岩 2017-05-30 发表

终端使用iNode进行Portal认证，服务器侧配置的服务带后缀，而iNode在认证时不选择后缀，此时会有一定概率提示安全认证失败，如下图所示。



iNode提示安全认证失败，随后断开连接。

本文同时分析安全认证通过和安全认证失败时的日志，通过两者的对比找出安全认证失败的原因。

首先说明下复现问题的时间点，因为服务器（5月13号）和终端PC时间（5月17号）不一致 所以iNode日志和服务器侧日志时间对不上。

操作时间点：

iMC侧时间	iNode时间	现象
17:01:16	18:29:55	iNode安全认证失败。
17:01:43	18:30:21	iNode安全检查通过。

查看策略服务器调试日志（imc/ead/log/policyserver），

认证不通过时的调试日志如下

2017-05-13 17:01:18 [策略服务器] [信息 (0)] [24] [ProxyRequestHandler::run] test ; EAD认证上线请求报文(1) ; 02:00:4C:4F:4F:50 ; 30.30.30.1 ; 报文解析成功

userName: test

hwAddr: 02:00:4C:4F:4F:50

clientPort: 10102

针对客户端请求报文，服务器侧有如下报错

2017-05-13 17:01:25 [策略服务器] [调试 (0)] [15] [CamsOnlineTable::synchronize] OnlineUser<test, 30.30.30.1, 02:00:4C:4F:4F:50, **null**>

2017-05-13 17:01:18 [策略服务器] [错误 (141584)] [17] [CamsOnlineTable::synchronize] 无法找到用户"OnlineUser<test, 30.30.30.1, 02:00:4C:4F:4F:50, null>"(userServiceId="null")在CAMS在线表的对应记录

2017-05-13 17:01:18 [策略服务器] [信息 (0)] [17] [RequestProcessor::procRequestLogon] 同步用户 test 上线请求处理时，获取在线信息失败

认证通过时的调试日志如下：

2017-05-13 17:01:44 [策略服务器] [信息 (0)] [24] [ProxyRequestHandler::run] test ; EAD认证上线请求报文(1) ; **6hZLPXTD** ; 02:00:4C:4F:4F:50 ; 30.30.30.1 ; 报文解析成功

userName: test

hwAddr: 02:00:4C:4F:4F:50

eventSeqID: 6hZLPXTD

clientPort: 10102

针对客户端请求报文，服务器侧回应如下

2017-05-13 17:01:44 [策略服务器] [调试 (0)] [17] [OnlineUserManager::manage] 用户 "OnlineUser<test@portal, 30.30.30.1, 02:00:4C:4F:4F:50, **6hZLPXTD**>" 被纳入服务器管理

2017-05-13 17:01:44 [策略服务器] [调试 (0)] [17] [RequestProcessor::addUserEvent] 成功地将事件 UserEvent<Least-TriggerTime=2017-05-13 17:01:44, TriggeredCount=0, test@portal, 30.30.30.1, 02:00:4C:4F:4F:50, UPDATE_OS_VERSION, ISOLATION,6hZLPXTD> 加入事件队列

从以上日志看出两者的区别就在于一个**eventSeqID，**iNode认证失败时是没有这个值的，而认证通过时包含该值。这个ID是用来唯一标识一个在线用户的，策略服务器首先根据该ID查询在线用户，如果获取不到该值，就会根据登录名查询，如果可以获取到该值就不再根据登录名查询。从上面日志看出，认证失败的时候iNode客户端请求报文是没有该值的，同时用户的登录名和UAM的在线表也不一致，所以导致认证失败；而认证通过的情况下iNode请求报文是包含该值的，所以即使登录名不一致，认证也不会出问题。

那么iNode又是如何获取这个eventSeqID值的呢。
继续分析iNode客户端在这两个时间点的调试日志：
认证失败时的调试日志如下：
55秒时收到认证通过报文
[2017-05-17 **18:29:55**] [DtlCmn] [73c] PortalPkt
Packet Type: [CODE_PP_LOGIN_RESPONSE] Client <--- Server/Bas
Head: Version = 0x2(Portal); HeadType = 0x65; AuthType = 0; Rsvd = 0; SeriOno= 2155; ReqId0 = 0
; ReqId1 = 0; UserIP = 30.30.30.1; UserPort = 0; ErrCode = 0; AttrNum = 12;
Attributes: EX_ATTR_HANDSHAKE_DELAY = 600000;
EX_ATTR_HANDSHAKE_OVERTIME = 1800000;
EX_ATTR_USER_STATUS = 99;
EX_ATTR_TIME_STAMP = 1494654382218;
EX_ATTR_DHCP_DELAY = 3000;
EX_ATTR_DHCP_TIMES = 3;
EX_ATTR_USER_PORT_NO = H3C-vlan-01-0030@vlan;
EX_ATTR_USER_ID = 2528892224761160283;
EX_ATTR_USER_SELF_SERVICE_URL =
http://100.100.100.100:8080/selfservice/modifyPasswordByURL.jsf?username=;
EX_ATTR_EAD_AGENT_IP = 100.100.100.100;
EX_ATTR_EAD_AGENT_PORT = 9019;
57秒时收到用户通知消息
[2017-05-17 **18:29:57**] [DtlCmn] [6c0] PortalPkt
Packet Type: [CODE_PP_NTF_USER_NOTIFY] Client <--- Server/Bas
Head: Version = 0x2(Portal); HeadType = 0x81; AuthType = 0; Rsvd = 0; SeriOno= 2155; ReqId0 = 0
; ReqId1 = 0; UserIP = 30.30.30.1; UserPort = 0; ErrCode = 0; AttrNum = 1;
Attributes: ATTR_RELAY_MESSAGE = =
ND9U9FJL>dddd?;#;
从上面日志可以看到iNode客户端在认证通过报文里面获取到策略服务器IP和端口号，在用户通知报文里面获取到eventSeqID。iNode收到认证通过报文和用户通知消息报文的时间间隔是2秒，也就是说iNode拿到策略服务器的IP地址和端口号后过了2秒才拿到eventSeqID，而这时iNode已经向策略服务器发起了上线请求，所以报文是不包含eventSeqID值的，iNode上线请求报文如下：
[2017-05-17 18:29:57] [DtlCmn] [12bc] SecPkt secPushInner: out-pkt [1] ---没有eventSeqID
<data>
  test
  02:00:4C:4F:4F:50
  10102
认证通过时的调试日志如下：
23秒时收到认证通过报文
[2017-05-17 **18:30:23**] [DtlCmn] [738] PortalPkt
Packet Type: [CODE_PP_LOGIN_RESPONSE] Client <--- Server/Bas
Head: Version = 0x2(Portal); HeadType = 0x65; AuthType = 0; Rsvd = 0; SeriOno= 27961; ReqId0 =
0; ReqId1 = 0; UserIP = 30.30.30.1; UserPort = 0; ErrCode = 0; AttrNum = 12;
Attributes: EX_ATTR_HANDSHAKE_DELAY = 600000;
EX_ATTR_HANDSHAKE_OVERTIME = 1800000;
EX_ATTR_USER_STATUS = 99;
EX_ATTR_TIME_STAMP = 1494654382218;
EX_ATTR_DHCP_DELAY = 3000;
EX_ATTR_DHCP_TIMES = 3;
EX_ATTR_USER_PORT_NO = H3C-vlan-01-0030@vlan;
EX_ATTR_USER_ID = 2528892224761160283;
EX_ATTR_USER_SELF_SERVICE_URL =
http://100.100.100.100:8080/selfservice/modifyPasswordByURL.jsf?username=;
EX_ATTR_EAD_AGENT_IP = 100.100.100.100;
EX_ATTR_EAD_AGENT_PORT = 9019;
23秒时收到用户通知消息报文
[2017-05-17 **18:30:23**] [DtlCmn] [6c0] PortalPkt
Packet Type: [CODE_PP_NTF_USER_NOTIFY] Client <--- Server/Bas
Head: Version = 0x2(Portal); HeadType = 0x81; AuthType = 0; Rsvd = 0; SeriOno= 27961; ReqId0 =
0; ReqId1 = 0; UserIP = 30.30.30.1; UserPort = 0; ErrCode = 0; AttrNum = 1;
Attributes: ATTR_RELAY_MESSAGE = =
6hZLPXTD>dddd?;#;
从上面日志看到iNode是在同一时间点收到认证通过报文和用户通知消息报文的，也就是说iNode拿到策略服务器的IP地址和端口号后也同时拿到了eventSeqID，所以iNode向策略服务器发起上线请求时，认证报文是包含eventSeqID值的，报文如下

[2017-05-17 18:30:23] [DtlCmn] [16ac] SecPkt secPushInner: out-pkt [1]
<data>
test
02:00:4C:4F:4F:50
6hZLPXTD
10102
由上面日志可以看出认证失败时有个2秒的延迟，那么这个2秒的延迟是Portal Server发送报文时延迟了2秒还是网络传输导致延迟了2秒呢，此时就需要继续分析Portal调试日志（imc/portal/log/portalserver），首先分析认证失败时的调试日志
服务器侧日志如下，可以看到服务器侧发送这两个报文时只差了0.02秒，所以可以断定是网络原因导致报文传输延迟了2秒。
2017-05-13 **17:01:16.011**[Portal服务器][调试(0)][ProxyResponseClientHandler::run]30.30.30.1 ; CODE_PP_LOGIN_RESPONSE(101) ; 2155 ; 30.30.30.1:55123 ; 报文处理成功(0)
<Content>
<Head>
Packet Type:CODE_PP_LOGIN_RESPONSE(101)
2017-05-13 **17:01:16.032**[Portal服务器][调试(0)][ProxyResponseDeviceHandler::run]30.30.30.1 ; AFF_NTF_USER_NOTIFY(20) ; 47 ; 30.30.30.254:2000 ; 报文处理成功
<Content>
<Head>
Packet Type:AFF_NTF_USER_NOTIFY(20)
认证通过时的调试日志如下：
2017-05-13 **17:01:43.916**[Portal服务器][调试(0)][ProxyResponseClientHandler::run]30.30.30.1 ; CODE_PP_LOGIN_RESPONSE(101) ; 27961 ; 30.30.30.1:57473 ; 报文处理成功(0)
<Content>
<Head>
Packet Type:CODE_PP_LOGIN_RESPONSE(101)
SerialNo:27961
2017-05-13 **17:01:44.016**[Portal服务器][调试(0)][ProxyResponseClientHandler::run]30.30.30.1 ; CODE_PP_NTF_USER_NOTIFY(-127) ; 27961 ; 30.30.30.1:61806 ; 报文处理成功
<Content>
<Head>
Packet Type:CODE_PP_NTF_USER_NOTIFY(-127)
SerialNo:27961

1：将服务后缀改成空，和iNode侧帐号形式保持一致；
2：在iMC侧配置默认服务类型标识，iNode在认证时会自动带上后缀。

1：8021x认证时，iNode侧账号名形式不用和服务器侧服务保持一致；
2：Portal认证时，iNode侧账号名形式必须和服务器侧服务保持一致。