

知 某局点iMC EIA/iNode 认证成功后短时间内掉线并提示安全认证失败“未收到服务器回应，即将强制下线”

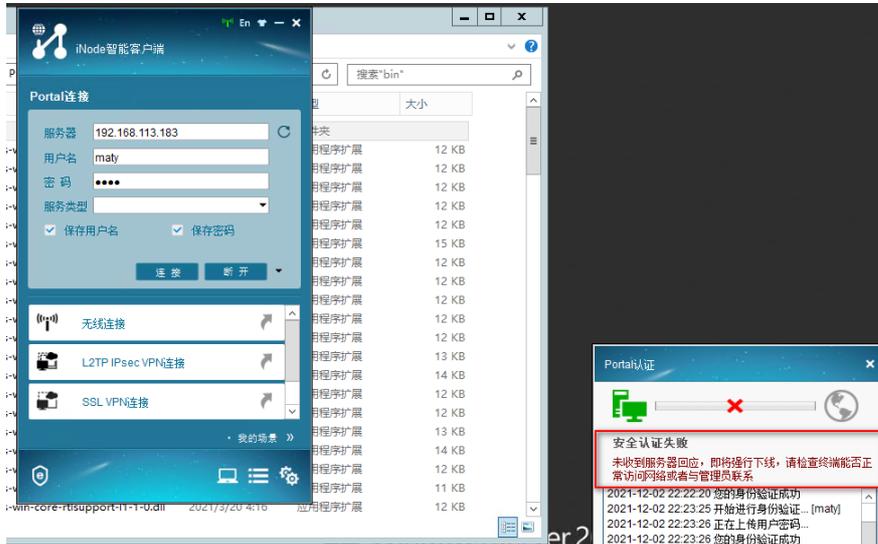
iNode iMC 栗鹏 2021-12-03 发表

组网及说明

8021.1x、portal认证组网都可能出现。

问题描述

iNode认证成功后，短时间内会出现掉线，iNode客户端提示安全认证失败，“未收到服务器回应，即将强制下线，请检查终端能否正常访问网络或者与管理员联系”



过程分析

认证逻辑:

iNode在定制了定制了EAD功能后,在认证成功后,iNode会与iMC EIA策略服务器进行安全检查报文交互。

即使没有配置任何安全检查项或者安全策略,也是要正常交互安全检查报文。iNode发起安全检查请求,策略服务器响应结果“不需要检查”。



排查思路:

- (1) 收集iNode详细级别日志、policy server的debug级别日志,客户端与iMC两侧抓包。
- (2) 分析iNode日志与策略服务器日志;

分析iNode日志 (iNodeSecPkt.xxxxx),记录已经发起了安全认证请求,但是没有收到服务器的回应

```
2021-11-09 15:03:15 [DtlCmn] [1294] SecPkt secPushInner: out-pkt (1)
<data>
  <i n="userName">lizv145</i>
  <i n="hwAddr">54:8D:5A:BB:B0:B6</i>
  <i n="eventSeqID">70BLS06</i>
  <i n="clientPort">10106</i>
  <i n="clientVersion">CH V7.30-0582</i>
  <i n="clientDisVersion">CH iNode PC 7.3 (E0582)</i>
  ...
  <i n="isSuppIacessid">false</i>
  <i n="vendor">LENOVO</i>
  <i n="model">20R83160R</i>
  <i n="serialNumber">WIKS0B513H5</i>
  <i n="osAuthCode">3V6E7</i>
  <i n="osSystemType">Unauthorized</i>
  <i n="licenseStatus">TRUE</i>
</data>
2021-11-09 15:03:15 [DtlCmn] [1294] SecPkt secPushInner: the state send before is 3
2021-11-09 15:03:20 [DtlCmn] [1294] SecPkt secPushInner: out-pkt (1) <data> <i n="userName">lizv145</i> <i n="hwAddr">54:8D:5A:BB:B0:B6</i> <i n="eventSeqID">70B
2021-11-09 15:03:24 [DtlCmn] [1294] SecPkt secPushInner: out-pkt (1) <data> <i n="userName">lizv145</i> <i n="hwAddr">54:8D:5A:BB:B0:B6</i> <i n="eventSeqID">70B
2021-11-09 15:03:31 [DtlCmn] [1294] SecPkt secPushInner: out-pkt (1) <data> <i n="userName">lizv145</i> <i n="hwAddr">54:8D:5A:BB:B0:B6</i> <i n="eventSeqID">70B
2021-11-09 15:03:37 [DtlCmn] [1294] SecPkt secPushInner: out-pkt (1) <data> <i n="userName">lizv145</i> <i n="hwAddr">54:8D:5A:BB:B0:B6</i> <i n="eventSeqID">70B
2021-11-09 15:03:42 [DtlCmn] [1294] SecPkt secPushInner: out-pkt (1) <data> <i n="userName">lizv145</i> <i n="hwAddr">54:8D:5A:BB:B0:B6</i> <i n="eventSeqID">70B
```

分析策略服务器日志 (polycserver),策略服务器并没有收到请求报文。

```
line 898: 2021-11-09 15:03:06 [DEBUG] [Uam Response Processor Manager] [UamMsgUtil::sendSyncMsg]sendSyncMsg:response{ -- SEQUEN
line 1089: 2021-11-09 15:03:06 [DEBUG] [pool-6-thread-6] [MobileTerminalProcessor::proMdmEvent]mac:12:CD:87:16:42:80
line 1090: 2021-11-09 15:03:06 [DEBUG] [pool-6-thread-6] [MobileTerminalProcessor::proMdmEvent]没有找到安全策略
line 1091: 2021-11-09 15:03:07 [DEBUG] [Uam Fkt Receive Handler] [UamPktReceiveHandler::run]接收UAM后台发送的响应报文成功
line 1103: 2021-11-09 15:03:07 [DEBUG] [Uam Message Send Handler] [UamPktSendHandler::run]从请求队列中获取向UAM后台发送的请求报
line 1104: 2021-11-09 15:03:07 [DEBUG] [Uam Response Processor Manager] [UamMsgUtil::sendSyncMsg]sendSyncMsg:request{ -- SEQUEN
line 1112: 2021-11-09 15:03:07 [DEBUG] [Uam Message Send Handler] [UamPktSendHandler::run]向UAM后台发送请求报文成功
line 1121: 2021-11-09 15:03:07 [DEBUG] [Uam Response Processor Manager] [UamMsgUtil::sendSyncMsg]sendSyncMsg:response{ -- SEQUEN
line 1312: 2021-11-09 15:03:07 [DEBUG] [pool-6-thread-7] [MobileTerminalProcessor::proMdmEvent]mac:24:DA:33:48:FB:61
line 1313: 2021-11-09 15:03:07 [DEBUG] [pool-6-thread-7] [MobileTerminalProcessor::proMdmEvent]没有找到安全策略
line 1314: 2021-11-09 15:03:28 [DEBUG] [Uam Fkt Receive Handler] [UamPktReceiveHandler::run]接收UAM后台发送的响应报文成功
line 1326: 2021-11-09 15:03:28 [DEBUG] [Uam Message Send Handler] [UamPktSendHandler::run]从请求队列中获取向UAM后台发送的请求报
line 1327: 2021-11-09 15:03:28 [DEBUG] [Uam Response Processor Manager] [UamMsgUtil::sendSyncMsg]sendSyncMsg:request{ -- SEQUEN
line 1335: 2021-11-09 15:03:28 [DEBUG] [Uam Message Send Handler] [UamPktSendHandler::run]向UAM后台发送请求报文成功
line 1344: 2021-11-09 15:03:28 [DEBUG] [Uam Response Processor Manager] [UamMsgUtil::sendSyncMsg]sendSyncMsg:response{ -- SEQUEN
line 1535: 2021-11-09 15:03:28 [DEBUG] [pool-6-thread-8] [MobileTerminalProcessor::proMdmEvent]mac:70:F0:87:74:FD:36
line 1536: 2021-11-09 15:03:28 [DEBUG] [pool-6-thread-8] [MobileTerminalProcessor::proMdmEvent]没有找到安全策略
```

- (3) 分析抓包文件,过滤udp.port==9019端口查看,目的端口不可达。进一步排查iMC侧进程情况。

No.	Time	Source	Destination	Protocol	Length	Info
2157	2021-11-09 16:45:44.656979	10.118.250.65	10.116.1.163	UDP	1511	ezproxy-2(10102) → 9019 Len=1469
2158	2021-11-09 16:45:44.657025	10.116.1.163	10.118.250.65	ICMP	590	Destination unreachable (Port unreachable)
2209	2021-11-09 16:45:51.486917	10.118.250.65	10.116.1.163	UDP	1511	ezproxy-2(10102) → 9019 Len=1469
2211	2021-11-09 16:45:51.486950	10.116.1.163	10.118.250.65	ICMP	590	Destination unreachable (Port unreachable)
2212	2021-11-09 16:45:51.486960	10.118.250.65	10.116.1.163	UDP	1511	ezproxy-2(10102) → 9019 Len=1469
2213	2021-11-09 16:45:56.106705	10.116.1.163	10.118.250.65	ICMP	590	Destination unreachable (Port unreachable)
11549	2021-11-09 16:47:29.493060	10.118.250.65	10.116.1.163	UDP	1511	ezproxy-2(10102) → 9019 Len=1469
11550	2021-11-09 16:47:29.493090	10.116.1.163	10.118.250.65	ICMP	590	Destination unreachable (Port unreachable)
12696	2021-11-09 16:47:36.387076	10.118.250.65	10.116.1.163	UDP	1511	ezproxy-2(10102) → 9019 Len=1469
12697	2021-11-09 16:47:36.387099	10.116.1.163	10.118.250.65	ICMP	590	Destination unreachable (Port unreachable)
13131	2021-11-09 16:47:40.501071	10.118.250.65	10.116.1.163	UDP	1511	ezproxy-2(10102) → 9019 Len=1469
13132	2021-11-09 16:47:40.501100	10.116.1.163	10.118.250.65	ICMP	590	Destination unreachable (Port unreachable)
14026	2021-11-09 16:47:47.235968	10.118.250.65	10.116.1.163	UDP	1511	ezproxy-2(10102) → 9019 Len=1469

(4) 检查下IMC策略服务器配置的IP检查imc/common/conf/server_addr.xml文件，策略服务器的IP是否是IMC 正确的IP地址，如果地址不正确，请修改为正确的IP地址并重启对应的进程生效。

```

<db-config address="127.0.0.1" dbname="icc_db" password="-105-61-35-7-31-241-241-1:
</component>
<component address="127.0.0.1" id="imc-INODE-MC"/>
<component address="127.0.0.1" id="imc-ISP">
  <custom-addr name="EAD_PROXY_IP" value="192.168.113.182"/>
  <custom-addr name="EAD_PROXY_IPV6" value=""/>
  <custom-addr name="EAD_PROXY_SERVER_IP" value="192.168.113.182"/>
</component>
<component address="127.0.0.1" id="imc-ITSM">
<db-config address="127.0.0.1" dbname="servicedesk_db" password="-105-61-35-5-31-1:

```

(5) 检查policy server、ispserver进程是否正常运行？以及9019端口是否被正常监听？如图所示，正常情况，监听udp 9019端口进程是IP地址为192.168.113.183的java进程，该java进程对应IMC监控代理中ispserver（策略代理服务器）

```

[root@imc conf]#
[root@imc conf]#
[root@imc conf]# netstat -anlp | grep 9019
udp6      0      0 192.168.113.183:9019  :::*
          44184/java
[root@imc conf]#
[root@imc conf]#
[root@imc conf]# ps -ef | grep 44184
root      26078 11280  0 06:09 pts/3    00:00:00 grep --color=auto 44184
root      44184      1  0 Nov08 ?        00:02:00 /opt/IMC/common/jre/bin/java -server -Xmx512m -Xrs -XX:PermSize=64m -XX:MaxPermSize=512m -Dimc:/opt/IMC/isp -Duser.language=-Duser.country=-Djava.awt.headless=true -Dcom.sun.management.jmxremote.port=9189 -Dcom.sun.management.jmxremote.authenticate=false -Dorg.jboss.netty.epollBugWorkaround=true -Djavax.net.ssl.keyStores=/opt/IMC/isp/security/newks -Djavax.net.ssl.keyStorePwd=IMCVS00R00 -Djava.io.tmpdir=/opt/IMC/tmp -jar /opt/IMC/isp/bin/bootstrap.jar start -port 8033

```

(6) 如果进程监听都正常，则进一步排查网络情况是否存在丢包、防火墙拦截等情况。

