iNode 认证提示安全检查失败案例

802.1X iNode Portal 张月鹏 2019-03-30 发表

组网及说明

无

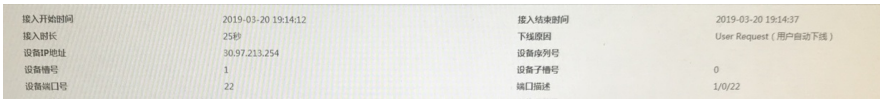
问题描述

在使用iNode认证，并且iMC服务器侧启用了策略服务器的场景中。iNode输入用户名密码，在认证成功后，很快提示“安全认证失败，当前连接即将被强行中断，请与管理员联系”。

过程分析

场景一：

排查imc侧用户上线信息，用户正常上线，上线后立即下线，下线原因user request。由此判断，认证上线流程没有问题，iMC默认启用策略服务器，用iNode认证时，认证完成后，终端会与策略服务器交互EAD报文。排查策略服务器状态。



接入开始时间	2019-03-20 19:14:12	接入结束时间	2019-03-20 19:14:37
接入时长	25秒	下线原因	User Request（用户自动下线）
设备IP地址	30.97.213.254	设备序列号	
设备槽号	1	设备子槽号	0
设备端口号	22	端口描述	1/0/22

1、如通过排查iNode日志\CollectInfo20190322211434\Log\iNodeClient报错如下，应该是终端与策略服务器通信异常导致。

[2019-03-20 18:49:20] [Dbg] [10b8] x1Widget::HandleLog old id and strLog 2019-03-20 18:49:20 您的身份验证成功

[2019-03-20 18:49:20] [Dbg] [10b8] BaseWidget::HandleLog :ConnId is 8022 您的身份验证成功

[2019-03-20 18:49:22] [Dbg] [1584] x1Widget::HandleLog old id and strLog 2019-03-20 18:49:22 自动获取IP地址...

[2019-03-20 18:49:22] [Dbg] [1584] BaseWidget::HandleLog :ConnId is 8022 自动获取IP地址...

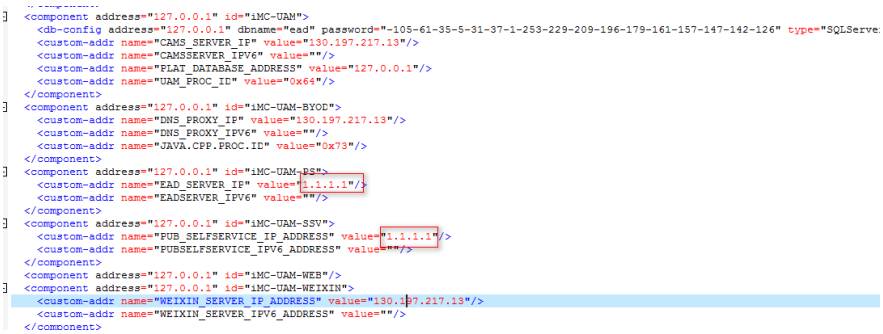
[2019-03-20 18:49:44] [Dbg] [147c] BaseWidget::HandleCmnLog :ConnId is 8022 未收到服务器回应，即将强行下线，请检查终端能否正常访问网络或者与管理员联系 notifycode "0d08"H --

[2019-03-20 18:49:44] [Dbg] [147c] x1Widget::HandleLog old id and strLog 2019-03-20 18:49:44 未收到服务器回应，即将强行下线，请检查终端能否正常访问网络或者与管理员联系

由日志判断，下线原因为与策略服务器通信超时导致。

2、排查客户端 PC 上的软件防火墙，网络中及 UAM服务器上的软件防火墙均已关闭。

3、排查server-addr.xml文件，如发现地址填写不一致，修改后，重启imc解决，文件路径iMC安装路径\common\conf\server-addr.xml。



```
<component address="127.0.0.1" id="iMC-UAM">
  <db-config address="127.0.0.1" dbname="ead" password="-105-61-35-5-31-37-1-253-229-209-196-179-161-157-147-142-126" type="SQLServe
  <custom-addr name="CAMS_SERVER_IP" value="130.197.217.13"/>
  <custom-addr name="CAMSSERVER_IPV6" value=""/>
  <custom-addr name="PLAT_DATABASE_ADDRESS" value="127.0.0.1"/>
  <custom-addr name="UAM_PROC_ID" value="0x64"/>
</component>
<component address="127.0.0.1" id="iMC-UAM-BYOD">
  <custom-addr name="DNS_PROXY_IP" value="130.197.217.13"/>
  <custom-addr name="DNS_PROXY_IPV6" value=""/>
  <custom-addr name="JAVA.CPP.PROC.ID" value="0x73"/>
</component>
<component address="127.0.0.1" id="iMC-UAM-RS">
  <custom-addr name="EAD_SERVER_IP" value="1.1.1.1"/>
  <custom-addr name="EADSERVER_IPV6" value=""/>
</component>
<component address="127.0.0.1" id="iMC-UAM-SSV">
  <custom-addr name="PUB_SELFSERVICE_IP_ADDRESS" value="1.1.1.1"/>
  <custom-addr name="PUBSELFSERVICE_IPV6_ADDRESS" value=""/>
</component>
<component address="127.0.0.1" id="iMC-UAM-WEB"/>
<component address="127.0.0.1" id="iMC-UAM-WEIXIN">
  <custom-addr name="WEIXIN_SERVER_IP_ADDRESS" value="130.197.217.13"/>
  <custom-addr name="WEIXIN_SERVER_IPV6_ADDRESS" value=""/>
</component>
```

场景二：
如通过iNode日志排查报错如下
[2019-03-22 16:27:00] [Dbg] [2314] BaseWidget::HandleConTime :ConnId is 5021 conntime: 2019-3-22 16:27:00
[2019-03-22 16:27:08] [Dbg] [252c] BaseWidget::HandleLog :ConnId is 5021 开始进行身份验证... [lwj1]
[2019-03-22 16:27:08] [Dbg] [8dc] BaseWidget::HandleLog :ConnId is 5021 正在上传用户密码...
[2019-03-22 16:27:17] [Dbg] [2314] BaseWidget::HandleLog :ConnId is 5021 Portal认证失败，网络故障或Portal服务器没有回应，请联系管理员。
[2019-03-22 16:27:17] [Dbg] [252c] BaseWidget::HandleLog :ConnId is 5021 报文发送错误
此时与上述情况不同，需排查策略服务器日志policyserver，如日志报错如下
2019-03-22 23:20:59 [策略服务器] [调试 (0)] [23] [RequestProcessor::initialize] 报文不完整，缺少必须的属性: "ipv6Addr"
2019-03-22 23:20:59 [策略服务器] [调试 (0)] [23] [RequestProcessor::processRequest] Begin processRequest()
2019-03-22 23:20:59 [策略服务器] [调试 (0)] [23] [RequestProcessor::procReqLogon] Begin procReqLogon()
2019-03-22 23:20:59 [策略服务器] [调试 (0)] [23] [RequestProcessor::procRequestLogon] Begin procRequestLogon()
2019-03-22 23:20:59 [策略服务器] [调试 (0)] [23] [RequestProcessor::procRequestLogon] Patch Check interval time is null from data,and the time is set with 0
2019-03-22 23:20:59 [策略服务器] [警告 (141001)] [23] [DataCacheManager::queryUserServiceInfo] 无法从数据库中查询到用户业务信息（userServiceName=lwj1）
2019-03-22 23:20:59 [策略服务器] [调试 (0)] [23] [RequestProcessor::procRequestLogon] Create a new online user
2019-03-22 23:20:59 [策略服务器] [信息 (0)] [23] [RequestProcessor::procRequestLogon] 同步用户 lwj1 上线请求处理时，获取在线信息失败
2019-03-22 23:20:59 [策略服务器] [调试 (0)] [23] [RequestProcessor::procRequestLogon] null
2019-03-22 23:20:59 [策略服务器] [调试 (0)] [23] [RequestProcessor::procReqLogon] End procReqLogon()
2019-03-22 23:20:59 [策略服务器] [信息 (0)] [23] [RequestProcessor::processRequest] End processRequest() successfully
失败日志中记录“无法从数据库中查询到用户业务信息”可知，用户在iMC侧不存在导致用户无法认证上线，此种情况，一般是用户未携带域名而在接入服务中配置服务后缀导致，配置参考如下

表1 iMC 中服务后缀的选择

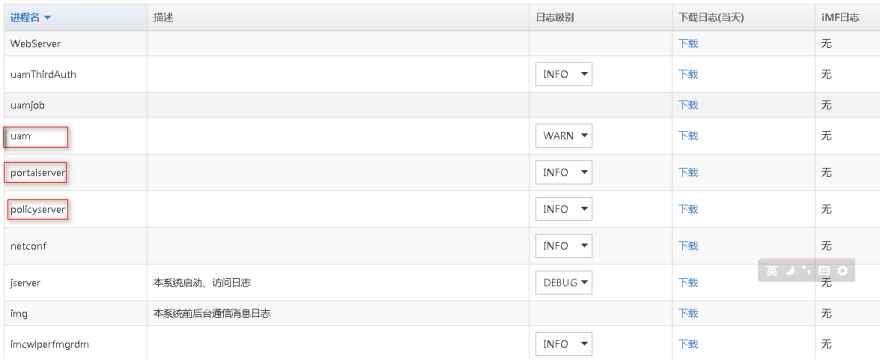
认证连接用户名	设备用于认证的 Domain	设备 Radius scheme 中的命令	iMC 中服务的后缀
X@Y	Y	user-name-format with-domain	Y
		user-name-format without-domain	无后缀
X	[Default Domain] 设备上指定的缺省域	user-name-format with-domain	[Default Domain]
		user-name-format without-domain	无后缀

解决方法

iNode 客户端安全认证失败问题排查思路相对清晰：
1. 在启用策略服务器的情况下， iNode客户端与策略服务器不通造成iNode与策略 服务器的心跳超时后主动下线。这种情况下一般iNode会给出类似“代理服务器没有回应，即将强行下线”之类 的提示。这时请检查iNode与策略服务器（UAM服务器）是否路由可达，通地ping，tracert等命令来进行排查。 等命令来进行排查。
2. 如果 iNode与策略服务器路由可达请检查是否iNode与策略服务器通信的端口 与策略服务器通信的端口（udp 9019）被防火墙过滤,包括客户端 PC 上的软件防火墙，网络中及 UAM服务器上的软件防火墙。
3. 如上述方法未解决问题，收集iNode日志，收集方法如下。

选择iNode右下角齿轮标志，将日志级别调成调试，复现问题2—3次，收集相关日志反馈。

4.收集uam，portal，policyserver日志，在系统管理-系统配置-日志配置页签下，将日志级别修改为调试，复现问题，收集日志反馈。



进程名	描述	日志级别	下载日志(当天)	iMF日志
WebServer			下载	无
uamThirdAuth		INFO	下载	无
uamJob			下载	无
uam		WARN	下载	无
portalserver		INFO	下载	无
policyserver		INFO	下载	无
netconf		INFO	下载	无
jserver	本系统启动、访问日志	DEBUG	下载	无
img	本系统前后台通信消息日志		下载	无
imcwlperfmgrdm		INFO	下载	无

附件下载：iNode 认证提示安全检查失败案例.pdf