某局点mschapV2进程异常重启导致认证失败

802.1X　iMC　**龚文文**　2020-12-22 发表

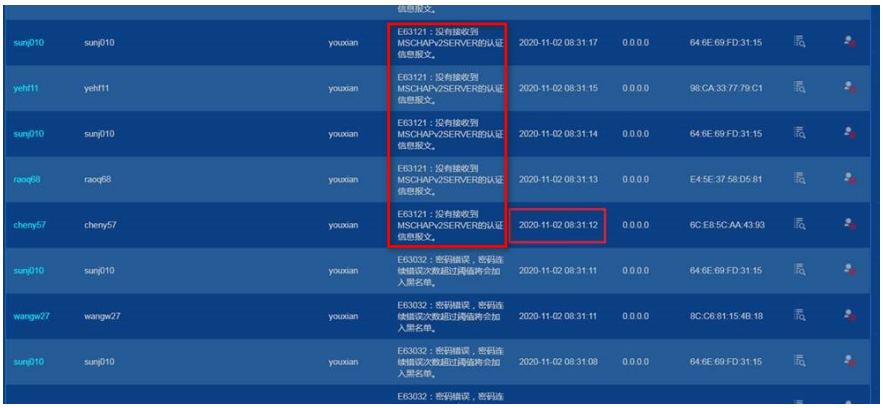
组网及说明

无特殊组网

问题描述

现场iMC前台收到了 mschapv2server进程意外停止的告警，由于正值刚上班期间，出现大批量用户无法上线的问题

认证失败日志提示没有接收到mschapv2server的认证信息报文



过程分析

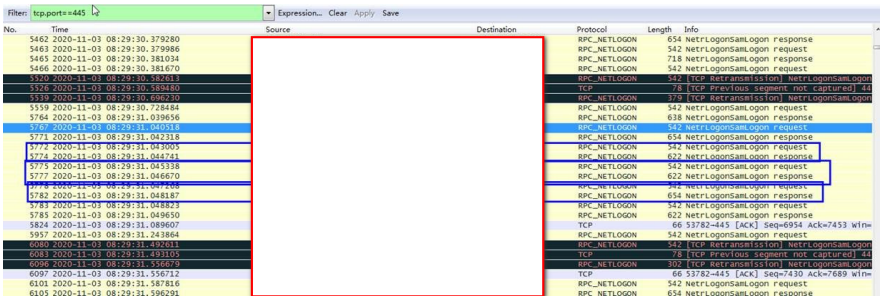
mschapV2server的日志中记录了大量的认证失败以及重建通道的信息

[Oct 30, 2020, 8:05:35 AM][Error]: Exception or unkown exception, **create new channel connect with error code=1** [2020-10-30 08:05:48.972] [Error] [MSChapAuthProvider::authenticate] authenticate Exception. mscv2js.security.SecurityProviderException: The supplied credentials are invalid: null\zhouly at mscv2js.mschap.MSChapAuth.mschapv2Validate(Unknown Source) at mscv2js.mschap.MSChapAuthProvider.authenticate(Unknown Source) at mscv2js.server.MsChapAuthHandler.run(Unknown Source) at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1128) at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:628) at java.base/java.lang.Thread.run(Thread.java:834)

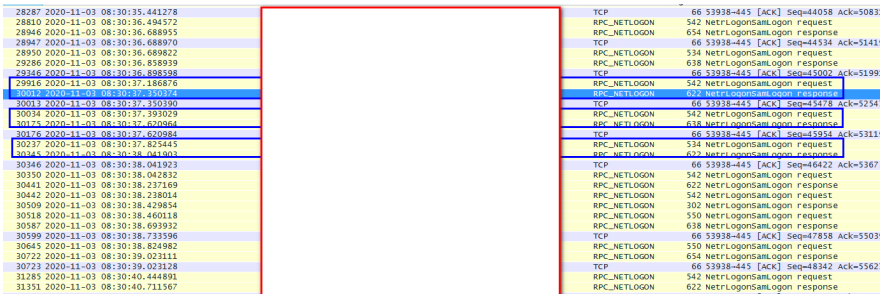
从抓包中分析，发现域控服务器响应时间越来越长，最终维持在400ms左右，即1s内只能认证两三个用户，当队列中的数据越来越多时，如果一个请求放到队列中2s后无法及时处理的就会提示超时，大量的认证失败，会触发mschapV2进程的保护机制而重启

具体抓包分析过程：

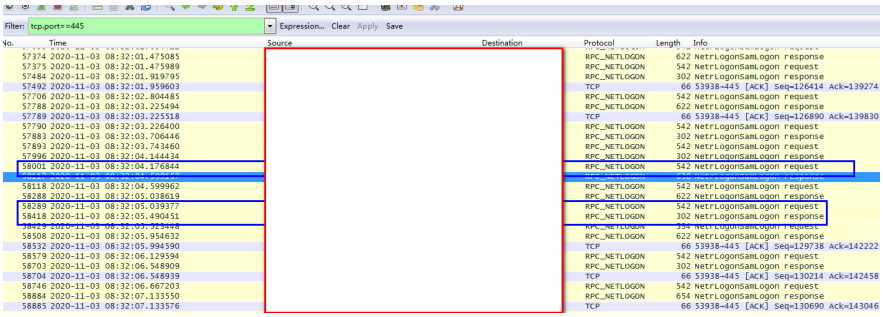
如下图所示，8:29分时域控响应很快，基本上2ms内响应。



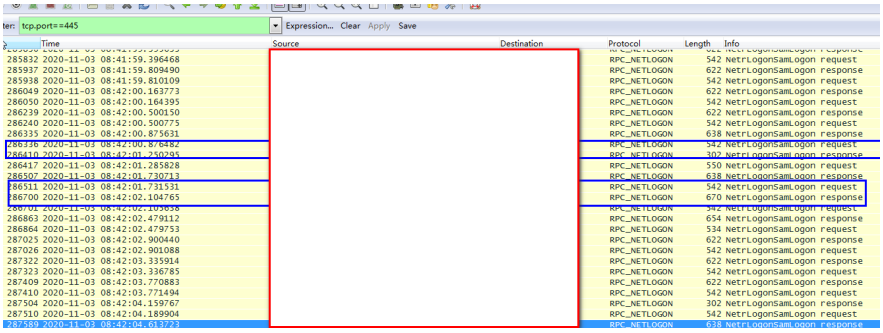
8:30分时响应耗时增加到200ms左右，如下图所示。



32分时响应时间增加到400ms左右。



42分时响应时间维持在400ms左右。



解决方法

1、排查是否是域控性能不足

2、排查现场网络