

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

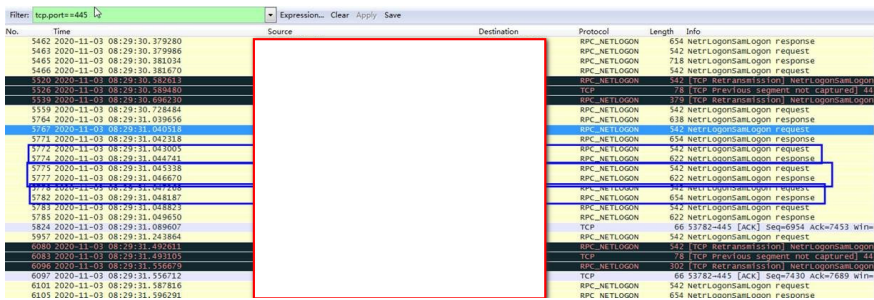
mschapV2server的日志中记录了大量的认证失败以及重建通道的信息

```
[Oct 30, 2020, 8:05:35 AM][Error]: Exception or unknwn 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\zho uly 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分时段域控响应很快，基本上2ms内响应。



8:30分时段响应耗时增加到200ms左右，如下图所示。

| | | | | | |
|-------|------------|-----------------|--------------|-----|-----------------------------------|
| 28287 | 2020-11-03 | 08:30:35.441278 | TCP | 66 | 53938-445 [ACK] Seq=4058 Ack=5083 |
| 28810 | 2020-11-03 | 08:30:36.494572 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 28946 | 2020-11-03 | 08:30:36.688955 | RPC_NETLOGON | 654 | NetrLogonSamLogon response |
| 28947 | 2020-11-03 | 08:30:36.688970 | TCP | 66 | 53938-445 [ACK] Seq=4934 Ack=5141 |
| 28950 | 2020-11-03 | 08:30:36.689822 | RPC_NETLOGON | 534 | NetrLogonSamLogon request |
| 29286 | 2020-11-03 | 08:30:36.858939 | RPC_NETLOGON | 638 | NetrLogonSamLogon response |
| 29288 | 2020-11-03 | 08:30:36.858958 | TCP | 66 | 53938-445 [ACK] Seq=5002 Ack=5198 |
| 29916 | 2020-11-03 | 08:30:37.186876 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 30013 | 2020-11-03 | 08:30:37.350390 | TCP | 66 | 53938-445 [ACK] Seq=5478 Ack=5254 |
| 30034 | 2020-11-03 | 08:30:37.393029 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 30121 | 2020-11-03 | 08:30:37.620984 | RPC_NETLOGON | 638 | NetrLogonSamLogon response |
| 30126 | 2020-11-03 | 08:30:37.620984 | TCP | 66 | 53938-445 [ACK] Seq=5951 Ack=5311 |
| 30237 | 2020-11-03 | 08:30:37.825445 | RPC_NETLOGON | 534 | NetrLogonSamLogon request |
| 30365 | 2020-11-03 | 08:30:38.041903 | RPC_NETLOGON | 622 | NetrLogonSamLogon response |
| 30346 | 2020-11-03 | 08:30:38.041923 | TCP | 66 | 53938-445 [ACK] Seq=6422 Ack=5367 |
| 30350 | 2020-11-03 | 08:30:38.042832 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 30441 | 2020-11-03 | 08:30:38.237169 | RPC_NETLOGON | 622 | NetrLogonSamLogon response |
| 30442 | 2020-11-03 | 08:30:38.238014 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 30509 | 2020-11-03 | 08:30:38.429854 | RPC_NETLOGON | 302 | NetrLogonSamLogon response |
| 30518 | 2020-11-03 | 08:30:38.460118 | RPC_NETLOGON | 530 | NetrLogonSamLogon request |
| 30587 | 2020-11-03 | 08:30:38.693932 | RPC_NETLOGON | 638 | NetrLogonSamLogon response |
| 30599 | 2020-11-03 | 08:30:38.733590 | TCP | 66 | 53938-445 [ACK] Seq=7858 Ack=5503 |
| 30645 | 2020-11-03 | 08:30:38.824982 | RPC_NETLOGON | 550 | NetrLogonSamLogon request |
| 30722 | 2020-11-03 | 08:30:39.023111 | RPC_NETLOGON | 654 | NetrLogonSamLogon response |
| 30723 | 2020-11-03 | 08:30:39.023128 | TCP | 66 | 53938-445 [ACK] Seq=8342 Ack=5562 |
| 31285 | 2020-11-03 | 08:30:40.444891 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 31351 | 2020-11-03 | 08:30:40.711567 | RPC_NETLOGON | 622 | NetrLogonSamLogon response |

32分时响应时间增加到400ms左右。

| | | | | | |
|-------|------------|-----------------|--------------|-----|---------------------------------------|
| 57374 | 2020-11-03 | 08:32:01.475085 | RPC_NETLOGON | 622 | NetrLogonSamLogon response |
| 57375 | 2020-11-03 | 08:32:01.475889 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 57484 | 2020-11-03 | 08:32:01.915795 | RPC_NETLOGON | 302 | NetrLogonSamLogon response |
| 57492 | 2020-11-03 | 08:32:01.959003 | TCP | 66 | 53938-445 [ACK] Seq=126414 Ack=139274 |
| 57706 | 2020-11-03 | 08:32:02.404483 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 57788 | 2020-11-03 | 08:32:03.225494 | RPC_NETLOGON | 622 | NetrLogonSamLogon response |
| 57789 | 2020-11-03 | 08:32:03.225518 | TCP | 66 | 53938-445 [ACK] Seq=126890 Ack=139830 |
| 57790 | 2020-11-03 | 08:32:03.226400 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 57883 | 2020-11-03 | 08:32:03.706446 | RPC_NETLOGON | 302 | NetrLogonSamLogon response |
| 57893 | 2020-11-03 | 08:32:03.743660 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 57996 | 2020-11-03 | 08:32:04.144134 | RPC_NETLOGON | 302 | NetrLogonSamLogon response |
| 58001 | 2020-11-03 | 08:32:04.178844 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 58118 | 2020-11-03 | 08:32:04.599962 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 58288 | 2020-11-03 | 08:32:05.038619 | RPC_NETLOGON | 622 | NetrLogonSamLogon response |
| 58389 | 2020-11-03 | 08:32:05.039377 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 58418 | 2020-11-03 | 08:32:05.490451 | RPC_NETLOGON | 302 | NetrLogonSamLogon response |
| 58508 | 2020-11-03 | 08:32:05.954632 | RPC_NETLOGON | 622 | NetrLogonSamLogon response |
| 58532 | 2020-11-03 | 08:32:05.994590 | TCP | 66 | 53938-445 [ACK] Seq=129738 Ack=142222 |
| 58578 | 2020-11-03 | 08:32:06.129598 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 58703 | 2020-11-03 | 08:32:06.548909 | RPC_NETLOGON | 302 | NetrLogonSamLogon response |
| 58704 | 2020-11-03 | 08:32:06.548939 | TCP | 66 | 53938-445 [ACK] Seq=130214 Ack=142458 |
| 58746 | 2020-11-03 | 08:32:06.667203 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 58884 | 2020-11-03 | 08:32:07.133550 | RPC_NETLOGON | 634 | NetrLogonSamLogon response |
| 58885 | 2020-11-03 | 08:32:07.133576 | TCP | 66 | 53938-445 [ACK] Seq=130690 Ack=143046 |

42分时响应时间维持在400ms左右。

| | | | | | |
|--------|------------|-----------------|--------------|-----|----------------------------|
| 285832 | 2020-11-03 | 08:41:59.396468 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 285937 | 2020-11-03 | 08:41:59.809690 | RPC_NETLOGON | 622 | NetrLogonSamLogon response |
| 285938 | 2020-11-03 | 08:41:59.810100 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 286049 | 2020-11-03 | 08:42:00.163773 | RPC_NETLOGON | 622 | NetrLogonSamLogon response |
| 286050 | 2020-11-03 | 08:42:00.166395 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 286239 | 2020-11-03 | 08:42:00.500150 | RPC_NETLOGON | 622 | NetrLogonSamLogon response |
| 286240 | 2020-11-03 | 08:42:00.500775 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 286335 | 2020-11-03 | 08:42:00.875031 | RPC_NETLOGON | 638 | NetrLogonSamLogon response |
| 286376 | 2020-11-03 | 08:42:00.876822 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 286410 | 2020-11-03 | 08:42:01.250295 | RPC_NETLOGON | 302 | NetrLogonSamLogon response |
| 286441 | 2020-11-03 | 08:42:01.285828 | RPC_NETLOGON | 550 | NetrLogonSamLogon request |
| 286507 | 2020-11-03 | 08:42:01.730213 | RPC_NETLOGON | 638 | NetrLogonSamLogon response |
| 286511 | 2020-11-03 | 08:42:01.731531 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 286700 | 2020-11-03 | 08:42:02.104765 | RPC_NETLOGON | 670 | NetrLogonSamLogon response |
| 286701 | 2020-11-03 | 08:42:02.105938 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 286863 | 2020-11-03 | 08:42:02.479112 | RPC_NETLOGON | 654 | NetrLogonSamLogon response |
| 286864 | 2020-11-03 | 08:42:02.479753 | RPC_NETLOGON | 534 | NetrLogonSamLogon request |
| 287025 | 2020-11-03 | 08:42:02.900440 | RPC_NETLOGON | 622 | NetrLogonSamLogon response |
| 287026 | 2020-11-03 | 08:42:02.901088 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 287321 | 2020-11-03 | 08:42:03.335914 | RPC_NETLOGON | 622 | NetrLogonSamLogon response |
| 287323 | 2020-11-03 | 08:42:03.336785 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 287409 | 2020-11-03 | 08:42:03.770883 | RPC_NETLOGON | 622 | NetrLogonSamLogon response |
| 287410 | 2020-11-03 | 08:42:03.771494 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 287504 | 2020-11-03 | 08:42:04.159767 | RPC_NETLOGON | 302 | NetrLogonSamLogon response |
| 287510 | 2020-11-03 | 08:42:04.189904 | RPC_NETLOGON | 542 | NetrLogonSamLogon request |
| 287511 | 2020-11-03 | 08:42:04.189929 | RPC_NETLOGON | 638 | NetrLogonSamLogon response |

解决方法

- 1、排查是否是域控性能不足
- 2、排查现场网络