



邮箱故障说明及整改措施报告

北京二六三企业通信有限公司

2021年5月





一、关于 5.18 邮箱无法登陆的故障情况详细说明

尊敬的用户：

您好！

诚挚感谢您对 263 邮箱服务长期以来的关注与支持！

5 月 18 日凌晨电子邮件系统出现无法登陆、发送失败等故障，同时 400 客服热线也无法拨通，特就此故障情况说明如下：

1、故障现象

电子邮件系统无法登陆、电子邮件收发失败、客服热线无法拨通等故障。

2、故障原因

- 1) 由于光缆及机房配套设施遭遇意外损坏，导致电子邮件服务出现中断。
- 2) 应急预案机制不足，光缆及机房相关服务器虽有备机，但无法支撑核心机房中断后业务所需的 100%负载，同时备品备件库存不足，无法第一时间做到快速、全量备份。
- 3) 面对极端情况的应急管理不足，现场管理混乱，导致次生故障出现，影响故障的解决时间。
- 4) 故障爆发突然，涉及面广，复杂度高，超出以往实战经验，加上技术人员应急决策能力弱，致使故障恢复时间累积延长。

3、基础设施故障处理过程

- 1) 5 月 17 日 23:15，值班运维接到系统报警，发现所有核心出口意外中断。
- 2) 5 月 17 日 23:30，确认核心传输设备光缆中断，导致中断原因待查，

- 启动应急预案。
- 3) 5月18日00:00, 确认主备光缆均中断, 且短时间内均无法恢复, 召集相关技术人员现场处理。
 - 4) 5月18日00:00-01:00, 技术人员陆续抵达, 紧急讨论应急预案。
 - 5) 5月18日04:00, 确认新的应急预案。
 - ◇ 全力恢复核心机房光缆, 并重新搭建临时链路, 但该方案经讨论和评估后, 确认恢复时间过长。
 - ◇ 由于光缆恢复时间过长, 为尽快恢复邮件服务, 减少故障影响时间, 决定将前端应用及后端服务部署至异地机房。
 - ◇ 优先保证最新的邮件投递, 待核心机房恢复后, 再恢复历史数据, 直至故障彻底恢复。
 - 6) 5月18日4:30, 工程师开始按照此方案进行部署, 异地机房虽有备机, 但不足以支撑100%受理能力, 公司需协调其它备机资源, 部署新机器及前后端程序。
 - 7) 5月18日11:55, 异地备份机房增加前端100%服务模块, 依次为MX、SMTP、POP、IMAP等模块, 全部部署完毕。
 - 8) 5月18日15:55, 主要异地机房开始部署后端程序, 确保用户新收发的邮件数据可看, 历史邮件数据仍需等待主机房故障恢复。
 - 9) 5月18日17:00, 启动异地机房服务, 但未能成功恢复, 开始查询原因, 同步修复已知问题。
 - 10) 5月18日21:00, 大部分主机问题解决, 测试通过。
 - 11) 5月18日21:30, 所有数据清理工作完成, 开始恢复业务。
 - 12) 5月18日22:15, 邮件系统中断故障陆续恢复, 基本故障已解决。
 - 13) 5月19日03:00, 光缆恢复, 所有服务切换回核心机房(切换过程用户无感知)。



4、系统服务故障处理过程

由于基础设施服务中断 23 小时，大量外域投递给 263 的邮件在对方的 SMTP 服务器大量积压，故当 2021 年 5 月 18 日 22:15 邮件系统服务恢复后，海量邮件瞬间涌入，263MX 队列及负载过高，尤其海外邮件较为严重，故导致 5 月 19 日部分邮件出现延迟、退信等异常情况。整体情况如下：

■ 邮件投递

- ◇ 由于长时间中断服务，导致全国、全球的邮件服务器无法给 263 邮件服务器投递邮件，造成大量邮件堆积，随着光缆恢复，大量邮件瞬间涌入。
- ◇ 263 收信服务器压力越来越大、负载过高，造成服务器已经过载，同时在线备机配置高低不同，启动速度不一样，率先启动的备机承载大量压力，导致在线备机负载过高，整体收件服务处于响应缓慢状态。
- ◇ 同时也有部分用户出现客户端 IMAP 出现收信报错，POP 出现重复收信现象。
- ◇ 运维团队紧急扩容，增加带宽，压力得到缓解。
- ◇ 随着线下备机的逐步上线，收信服务器压力逐渐趋于正常。

■ 邮件存储

- ◇ 由于邮件数量过大，邮件存储系统处理异常，造成部分邮件功能报错，存储系统处理缓慢。
- ◇ 此时运维团队启动邮件存储备机，压力得到缓解，但由于邮件存储服务压力过大，处于高负载运行状态，造成用户使用部分功能出现异常，同时影响到邮件存储服务的邮件索引数据库。
- ◇ 由于短时间收信量过大，导致邮件存储到主节点和备份节点压力大，



出现数据不同步现象，邮件索引数据在主备数据库之间同步出现异常，导致部分用户出现邮件不能搜索，或搜索报错情况。

◇ 随着线下备机的逐步上线，邮件存储服务器压力趋于正常。

- 随着邮件投递服务、邮件存储服务恢复正常，整体邮件系统运行逐渐恢复正常，趋于平稳。

二、落实整改措施

1、全面整改

针对本次故障，公司高度重视，决定将 5.18 定为公司“质量警示日”，每年举办质量专题活动，强化全员质量意识，警钟长鸣。

重新梳理、制定运维管理整体机制，落实管理规范、管理制度、管理流程，再次明确树立监管与考核制度，责任落实到人。

2、整改原则

- 1) 贯彻我司关于网络的各项规章制度，担负网络维护、监控工作，掌握网络运行状况，及时处理网络故障。
- 2) 保证各种网络、主机系统设备的技术性能和各项质量指标达到 SLA 标准。
- 3) 保证用户设备的正常运行，提高服务水平和客户的满意度。
- 4) 面向网络，以用户满意为目标，以技术支持为保证，强化资源的有效利用，全面提高网络运行维护质量和服务水平。

3、体系制度整改

- 1) 按季度提升运营维护团队的整体素质，强化运营人员的知识/技能/

- 经验/运营意识等专业方面的培训和管理。
- 2) 强化运营维护的储备计划和机制,确保有足够的专业人员,在服务客户、应对突发事件等方面能发挥及时的作用。
 - 3) 完善运营维护相关的培训机制,制定定期定向的培训计划,并完善相应的考核和奖惩制度。
 - 4) 建立起科学的运营维护日常操作规范,日常维护管理、记录、监督、评估规范,让运营维护人员在实际工作中有章可循,按规执行。
 - 5) 完善运营维护的监控管理,尤其是对邮件系统进行必要的数据采集和监控,评估可能导致的运营维护故障因素。
 - 6) 完善备件库存核查管理,确保运营维护必要的备件充足,并定期对备件状态进行检测,不可放过任何一个细小的问题。
 - 7) 完善应急预案,定期进行应急演练,针对演练中发现的不足,及时进行修订和完善应急预案,切实提升应急水平。
 - 8) 进一步加大督促检查力度,定期邀请政府及上级监管部门进行监督检查。

4、维护管理整改

(1) 设备维护管理整改

- ◇ 全面检查所有设备,更新设备长期使用(已超过设计使用年限),性能严重下降的设备。
- ◇ 配套设备同步更新。
- ◇ 相关配件补充齐全。
- ◇ 加强设备巡检。
- ◇ 新设备严禁直接进入机房运行,必须做好上线检测后才可上线。

(2) 数据维护管理整改

- ◇ 数据备份与恢复策略改进与优化。
- ◇ 认真做好数据备份与恢复的测试与演练。
- ◇ 每日进行数据健康度的巡检。
- ◇ 加强定期对运行日志和审计数据进行分析，以便及时发现异常行为。

(3) 网络安全管理整改

- ◇ 保证数据中心设备的安全性和保密性，以保证网络的持续、稳定的运行。
- ◇ 监测到链路或设备故障时，尤其是骨干线路延迟、重要设备宕机等，发出故障告警信。
- ◇ 监测到网络设备、服务器的端口流量、丢包率、ping 延时和丢包、CPU 利用率、内存利用率、硬盘利用率等运行参数超过预设阈值时，发出故障预警信息。
- ◇ 执行监控脚本并进行监控数据采集，并定期提供各系统监控报告。
- ◇ 定期检查网络系统设备是否正常运行，检测网络系统性能，包括数据传输的稳定性、可靠性、传输速率。

(4) 系统安全管理整改

- ◇ 加强每周通过系统性能分析软件，对主机系统进行运行性能分析，并做详细记录，根据分析情况对主机系统进行系统优化，包括磁盘碎片整理、系统日志文件清理，系统升级等。
- ◇ 加强下载安装最新版的系统补丁的及时性，对系统主机进行升级。
- ◇ 在系统主机发生故障时应及时通知用户，用最短的时间解决故障。
- ◇ 每月对系统主机运行情况进行总结、并写出系统主机运行维护报告。

(5) 备份与恢复管理整改

- ◇ 对关键通讯线路必须采用双通讯线路；网络的运行线路和备份线路必须采用不同的网络服务供应商，重要网络设备必须有冗余备份。
- ◇ 核心服务器需采用热备份方式，确保在运行出现故障的时候备机能够自动接管；重要服务器可根据要求采用热备份方式或双机备份及其他冗余、容错措施。
- ◇ 应用系统、程序和数据做到双备份，一份保存到本地由系统管理员管理，方便及时安装，一份做灾难备份。
- ◇ 确保所有的备机系统处于可用状态。

(6) 故障应急机制整改

- ◇ 重新梳理制定应急方案。
- ◇ 加快应急响应处理速度，故障发生 3 分钟内通知相关岗位负责人。
- ◇ 故障发生时客服每 30 分钟会跟踪处理进度。
- ◇ 对于故障应急方案定期演练。
- ◇ 故障处理结束后 4 小时内给出故障报告。

最后，请允许我们再次向您郑重道歉，请相信，我们必将以此为鉴，直面问题，正本清源，用更为严谨认真的实际行动，回报所有给予理解和支持的用户朋友。

真诚希望能得到您的谅解！

北京二六三企业通信有限公司

2021年5月24日

