科来

第 31 章
如何解决业务应用访问失败的问题

科来官微
CSNA 公众号
400-6869-069
www.colasoft.com.cn
support@colasoft.com.cn

许多企事业单位对业务系统的性能、稳定性和扩展性有很高的要求。在业务网络环境中，负载均衡设备由于能对网络设备和服务器的带宽、吞吐量和数据处理能力进行扩容而备受青睐。然而负载均衡设备作为流量转发的一个环节，如果发生故障，也有可能导致业务访问失败，与正如本案例所示。

31.1 问题描述

31.1.1 基本环境描述

客户端通过 X.X.96.171 访问客服 web，负载均衡设备-1 的 IP 为 X.X.96.169，负载均衡设备-2 的 IP 为 X.X.96.170，负载均衡设备-1 和负载均衡设备-2 通过自身的 IP 与客服 Web 通讯，负载均衡设备一方面转发客户端的请求，另一方面将收到的响应转发给给客户端。

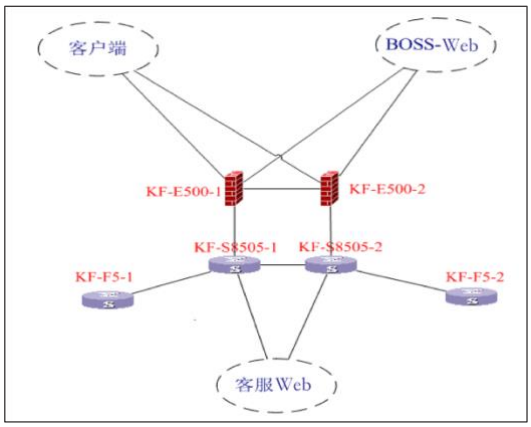

图 31-1

31.1.2 故障现象

客户端通过 X.X.96.171 访问 Web 服务器，会出现“404 Not Found”提示：

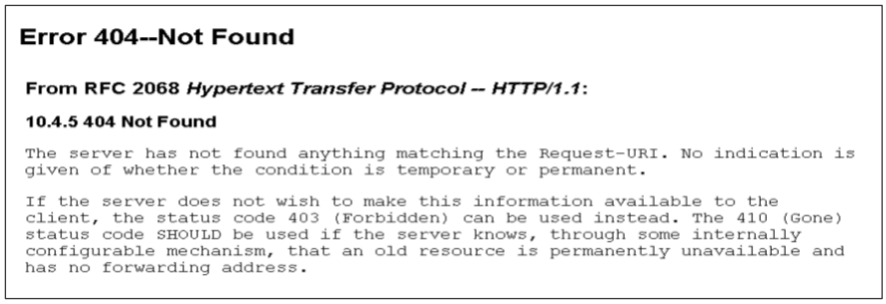

图　31-2

客户端直接访问客服 Web 的 IP 则不会出现问题，怀疑负载均衡设备转发存在问题，需要找到数据进行验证。

31.2　分析过程

本故障中出“404 Not Found”错误的可能性原因有两个：第一个是客户发起的请求不存在；第二个是负载均衡设备转发客户端的请求时发生异常。

针对第一个可能性原因进行分析：通过提取“404 Not Found”会话中的客户端请求并直接访问，就可以确定客户的请求是否有效，经验证，该客户端请求可以直接访问，因此排除了第一个原因。

针对第二个可能性原因进行分析：对比分析客户端的请求与负载均衡设备转发的请求，便可以确定负载均衡设备的转化是否存在问题。而这一环节这也是这次分析的重点。

通过客户反馈，科来网络分析工程师找出错误提示的会话并提取关键字：

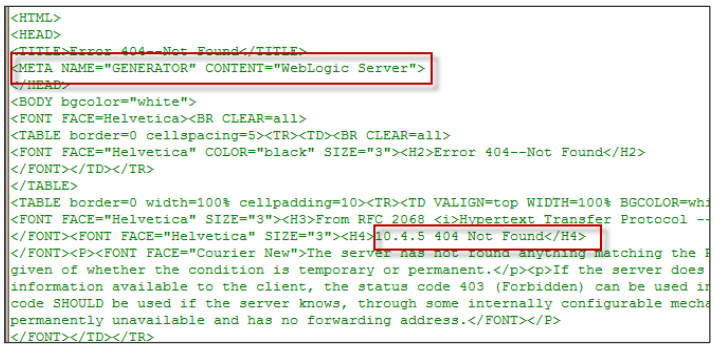

图　31-3

详细查看错误会话并与客户进行确认，判断错误提示具有以下特征：每个出

错页面的 content="WebLogic Server"；数据流信息包括客户端 IP、SessionID 等关键字。之后提取正常访问数据，为后期对比分析做准备。

客户端与负载均衡设备正常的通讯数据：

图　31-4

客户端的请求里包括详细的 get 请求、客户端 IP、sna_cookie 和 login_cookie 信息。

负载均衡设备与服务器的正常通讯分析：

图　31-5

负载均衡设备（X.X.96.70）发起请求，包含的信息与客户端发出的请求信息一致。

由于此类现象不定期出现，想要完整抓取客户端到负载均衡设备和负载均衡设备到客服 Web 的所有数据，就需要部署科来网络回溯分析系统并镜像负载均衡设备端口进行数据采集，等业务故障重现后再提取数据包进行分析，拓扑图如下。

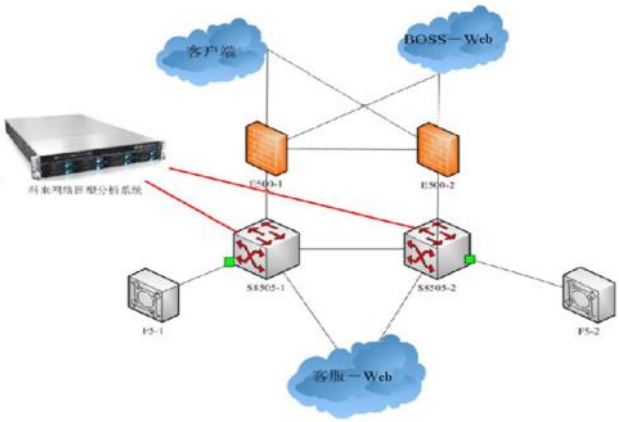

图　31-6

对客户端与负载均衡设备的通讯数据进行分析：

客户端（X.X.138.210）发起 GET 请求，请求数据大小为 1.601KB，内容包括客户端 IP、 sna_cookie 和 login_cookie 等信息，服务器 10.189.96.XXX 响应

“404 Not Found”，客户端的端口为 1359。

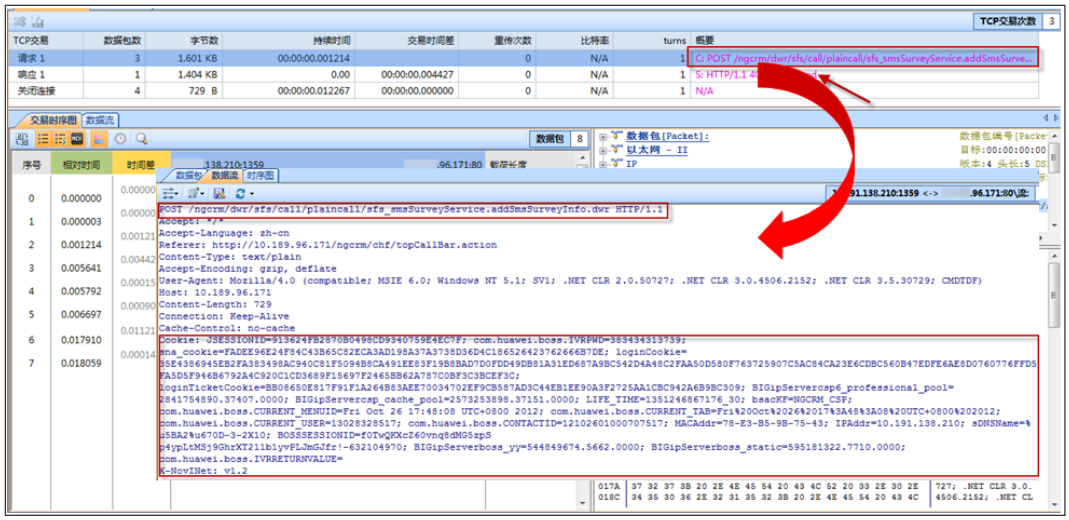

图　31-7

对客户端与负载均衡设备的数据流信息验证：

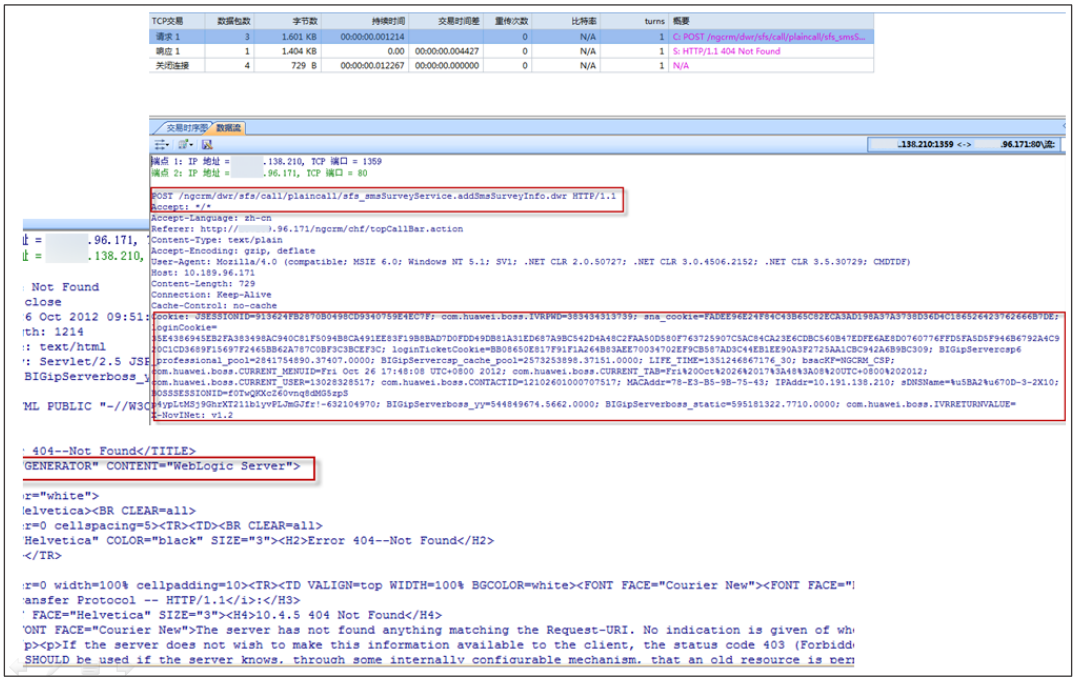

图　31-8

客户端的请求里包括详细的 get 请求，客户端 IP、sna_cookie 和 login_cookie 信息，且服务器的错误响应包含 content=“WebLogic Server”。

负载均衡设备与服务器的通讯分析

提取负载均衡设备与服务器的通讯，设置高级过滤器：（请求里的 cookie 有客户端的 IP 信息，数据流包括 WebLogic Server，还可以通过 SessionID 等）。

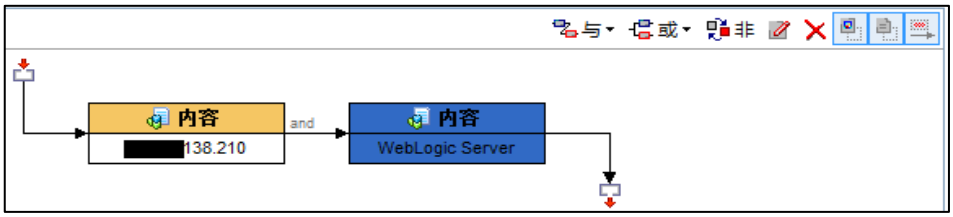

图　31-9

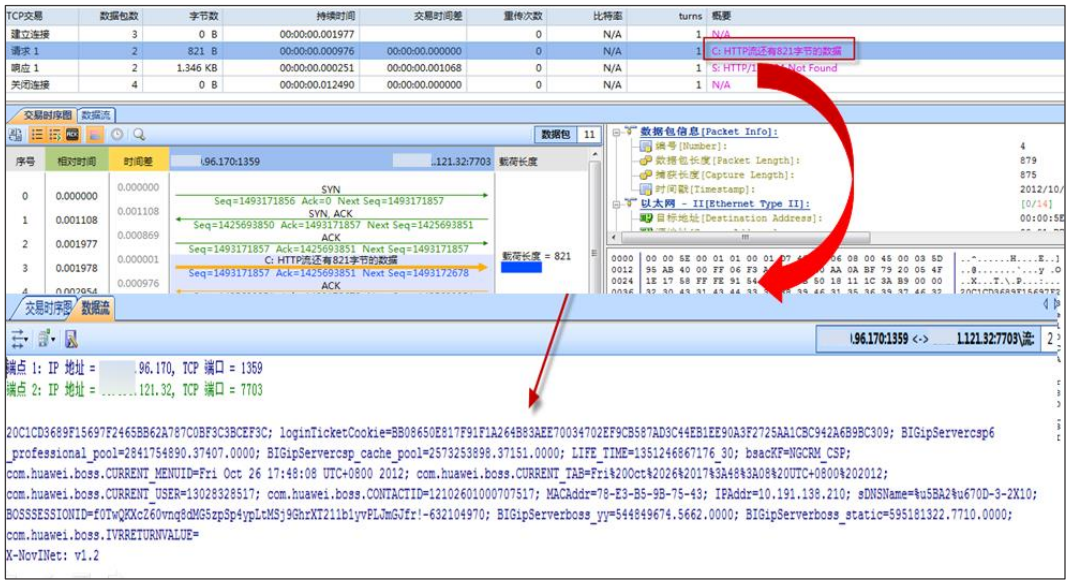

图　31-10

负载均衡设备（X.X.96.70）发起请求，请求数据 826B，小于客户端的请求数据（未见 get 请求），服务器响应“404 Not Found”，负载均衡设备的端口为 1359，与客户端的端口一样。

与客户端的请求综合对比分析可知，负载均衡设备与服务器端通讯的请求不完整，未见 sna_cookie 信息，但通过 login_cookie，客户端 IP，SessionID 等信息可以确定这是与客户端请求负载均衡设备的同一会话，且服务器的错误响应包含 content=“WebLogic Server”。

图　31-11

31.3　分析结论与建议

负载均衡设备转发的请求与客户端发出的请求不一致，导致客户端访问客服 Web 出现“404 Not Found”提示，该问题与客户端和服务器无关，应是负载均衡设备的转发存在 Bug。

31.4　价值

当应用出现不能访问时，我们通常会怀疑是某个网络设备或端点设备的问题，比如本案例我们怀疑是应用负载均衡的问题，但如果缺乏有效的手段和工具，排查问题将会耗费大量的时间。

通过网络分析技术能够帮助用户进行数据包级的精细分析，可以看出数据包在传输中是否存在异常，迅速定位异常节点，从而进行快速排障。

科来介绍

科来成立于 2003 年，是专注于网络流量分析技术研究与产品开发的高新技术企业，在这一领域有着几十项专利技术和完全独立的自主知识产权。科来研发的产品广泛应用于国内外用户的网络安全分析及网络智能运维等关键领域。科来连续入围 GartnerNPMD 魔力象限，并

荣获“远见者”称号，是唯一入选“远见者”象限的中国企业。科来产品还曾被美国权威评测机构 PC Magazine 评选为《全球最佳科技产品》。

科来专业的技术服务在用户的业务保障上起到关键作用，已经成为对网络时效性高要求的企业的最佳选择，得到了社会各界的广泛认可。同时，科来创办的《CSNA 网络分析认证培训》是我国广具影响力的网络分析认证体系，为国家培养了大量的网络分析技术高级人才。

由于科来公司在网络安全领域的技术优势，受邀为青岛“上合峰会”、多届“两会”、“十九大”、杭州“G20 峰会”、“九三”阅兵、“世界田径锦标赛”、多届“数博会”等重大国家级活动做网络安保工作，做出突出贡献。

- 100 余家世界 500 强企业选择科来
- 为全球 10000 余家商业客户提供网络分析解决方案
- 全球 90 余万用户正在使用科来的产品
- 科来的技术服务于世界 110 个国家和地区