科来

第 22 章
如何解决 SSO 单点登录跳转异常问题

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

应用出现访问异常，很大可能是由于网络设备出现故障或者设备关联验证过程中出现了问题造成的。但是在部分情况下，对系统程序的设置也会成为造成异常现象的原因所在。正如本案例所介绍的单点跳转异常情况。

22.1 问题描述

22.1.1 故障现象

某集团公司准备上线 SSO 单点登录 OA 业务，但在测试时发现 SSO 单点登录后，点击 OA 办公系统链接，不能跳转到正常业务页面，而是跳转到 oa.x.com 主页。由于此类故障频繁发生，导致单点登录 OA 业务无法及时上线，严重影响到该集团日常运作和管理。

22.1.2 基本环境描述

业务访问路径逻辑：

客户端（X.X.24.100）→OA 办公系统前端（X.X.39.31）→SP Token 验证接口机前端（X.X.24.50）。

SSO 单点登录 OA 业务系统具体认证流程：

1、用户在 SSO Portal 登录系统之后，根据“UserCode-登录名”获取 Token；

2、在 SSO Protal 中点击单点登录关联业务系统（如 OA 业务系统）的链接，通过 Request 参数传递 Token 到业务系统关联页面；

3、业务系统获取到 Token 之后，调用 SSO Portal 的 Token 验证接口机接口（提供 WebService 和 Rest 两种规格的接口）进行验证；

4、返回对象的 Code 为 1，代表验证通过，加载关联页面（Data 对象为用户的编号、名称和登录名）；

5、返回对象的 Code 为 0 或者其他，即验证失败，直接跳转到 SSO Portal 的登录页面。

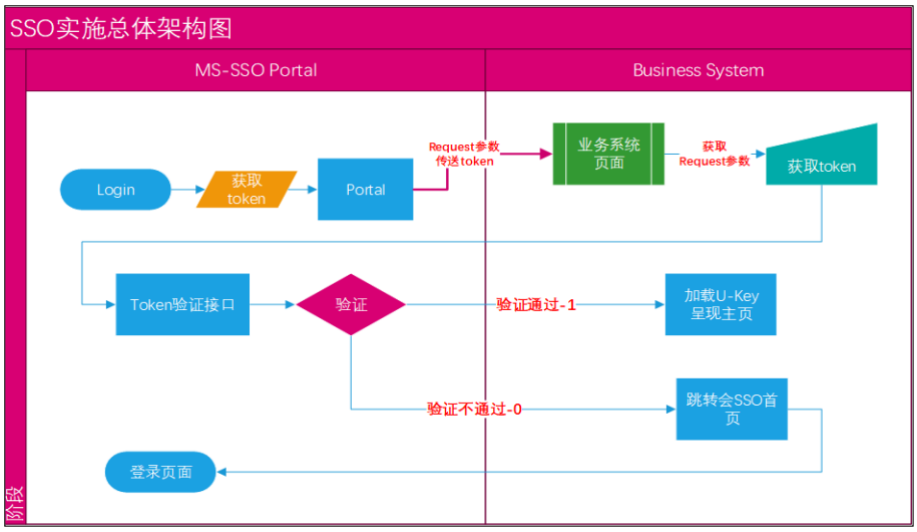

图　22-1

22.2　分析过程

点击 OA 办公系统链接，异常跳转到了 http://oa.x.com 系统登录页面，如下图所示。

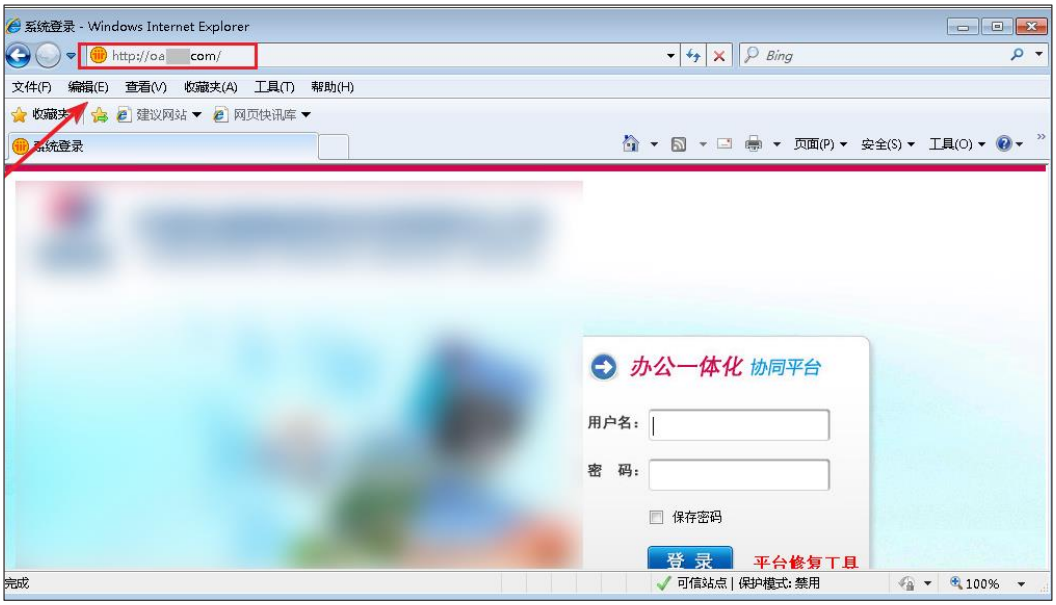

图　22-2

业务应正常跳转到登录页面，如下图所示。

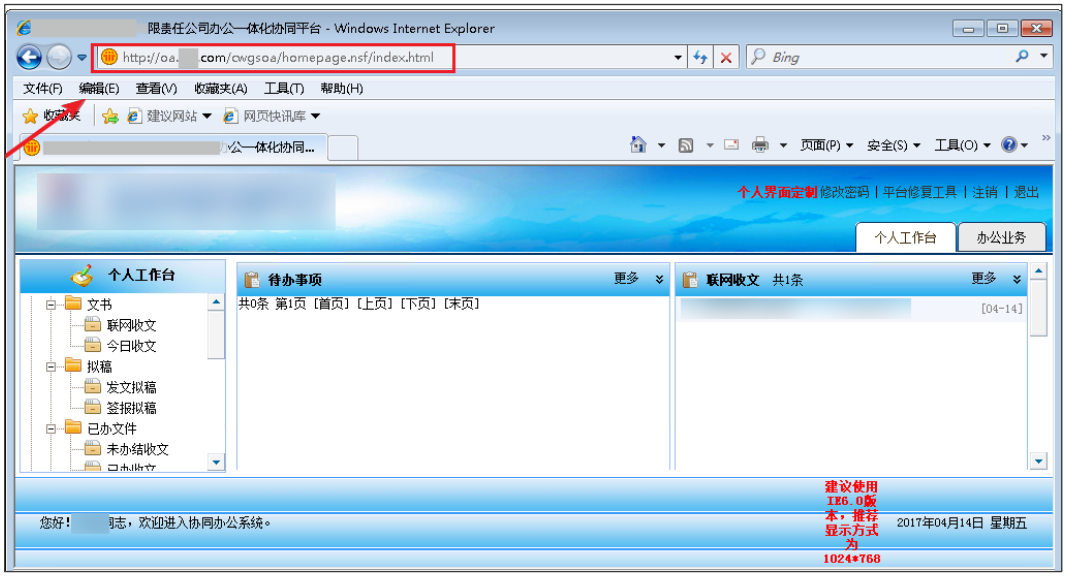

图　22-3

针对此异常跳转产生的时间段（14 点 13 分 03 秒-14 点 13 分 07 秒）回溯分析客户端至 OA 系统前端相应会话，可以看到产生了两条会话连接，如下图所示。

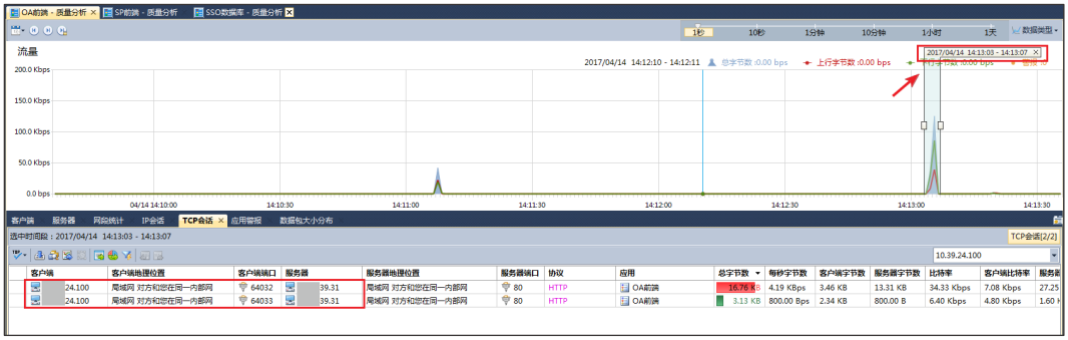

图　22-4

深度解码还原主请求会话（X.X.24.100:64032），可以看到传完 Token 参数及后续请求页面链接的情况，如下图所示。

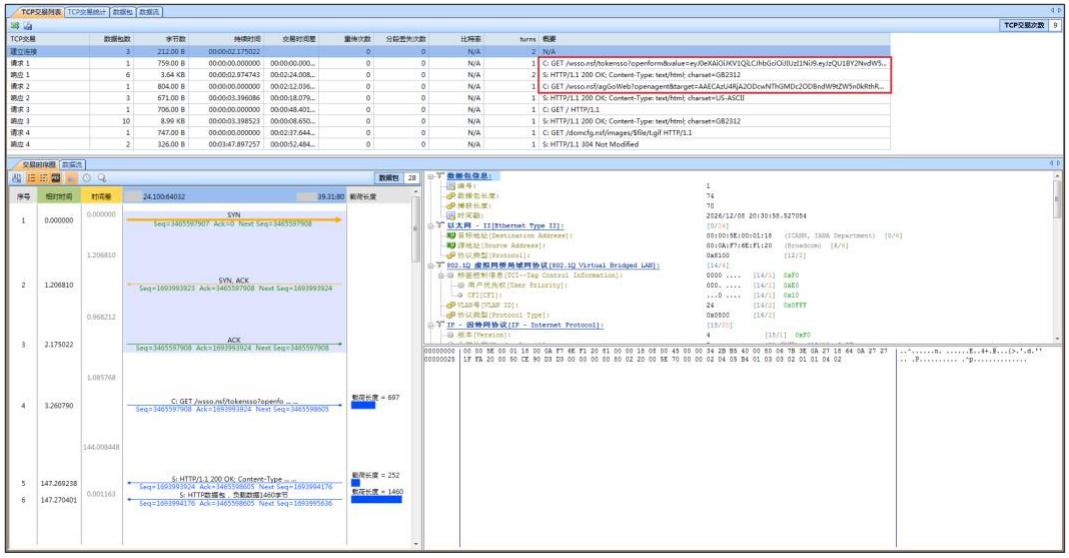

图　22-5

进一步观察分析，发现在 GET /HTTP/1.1 链接后，还出现了回复数据。查看回复数据的关键字，发现是异常跳转页面——“系统登录”页面的信息，如下图所示。

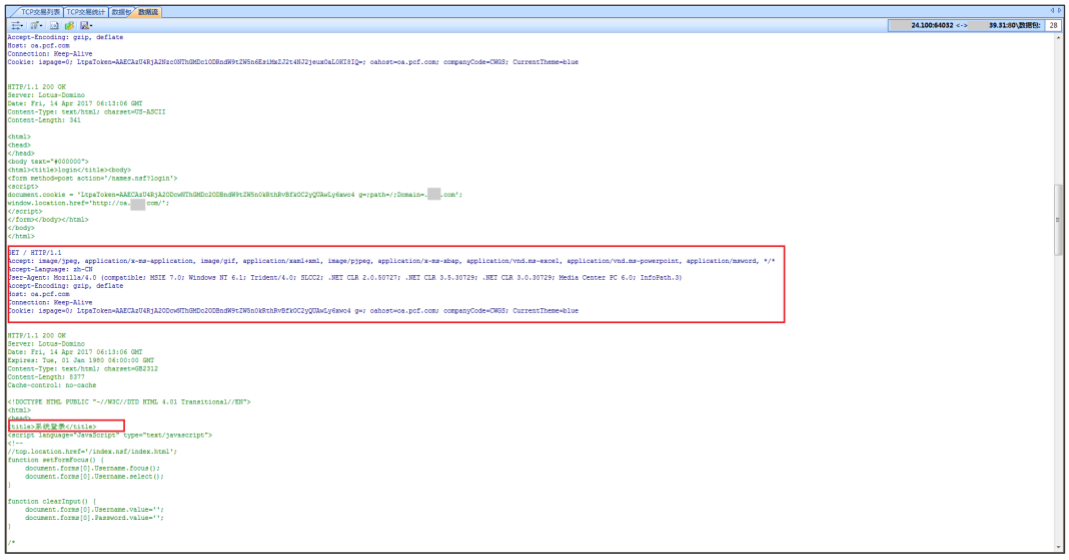

图　22-6

为进一步分析异常点，选择一次正常会话的数据做对比分析。选取 13 点 55 分 23 秒-13 点 55 分 32 秒时间段的一次正常业务跳转会话，可以看到正常会话时产生的多线程连接数（17 条）明显多于异常会话时的连接数（2 条），如下图所示。

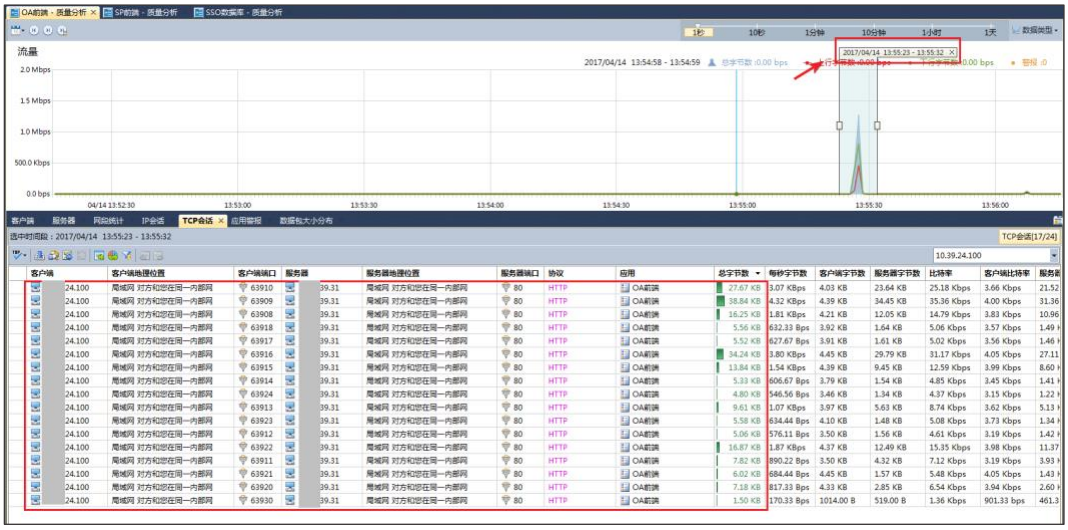

图　22-7

解码还原会话信息发现：传完 Token 参数、后续请求页面链接及 GET /HTTP/1.1 连接后，存在新的请求链接：GET /homepage.nsf/RedirectTO HTTP/1.1，如下图所示。

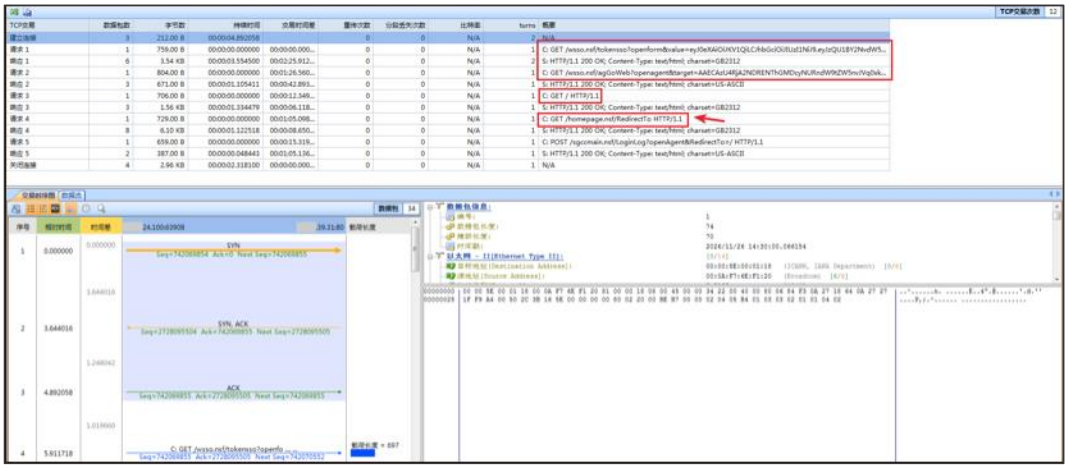

图　22-8

经查看，发现 GET /HTTP/1.1 链接后，出现的数据和异常情况时不一致，如下图所示。

图　22-9

正常情况下，GET /homepage.nsf/RedirectTO HTTP/1.1 后，返回的数据如下图所示。

图　22-10

通过对比分析，查看到从客户端至 OA 前端在异常跳转情况下的 url 请求有较大不同：异常跳转情况下的请求缺少 GET /homepage.nsf/RedirectTO HTTP/1.1 链接，并且多线程连接会话仅为 2 条，远低于正常情况时的连接会话。

因业务存在 Token 关联验证流程，因此需关联分析 OA 前端与 SP Token 接口机前端的通信会话。

检索异常跳转时同一时间段 14 点 13 分 03 秒-14 点 13 分 07 秒 OA 前端与 SP Token 接口机前端的通信会话，如下图所示。

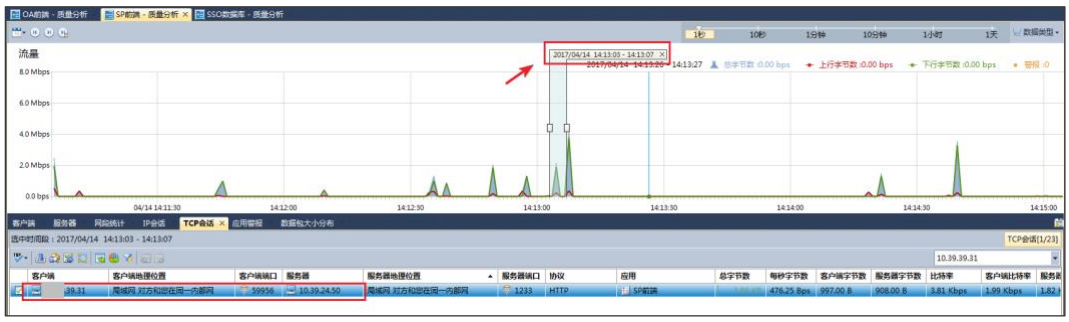

图　22-11

深度解码还原此会话，发现通过 Token 验证接口的验证后，SP Token 接口机前端返回的 Code 值是“1”，而默认认证失败返回的 Code 值应该是“0”，如下图所示。

图　22-12

同样，对比分析正常业务 13 点 55 分 23 秒-13 点 55 分 32 秒时间段的通信会话，如下图所示。

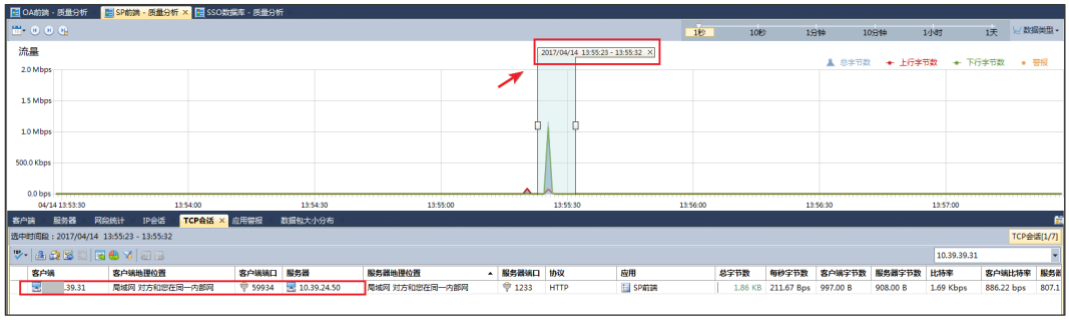

图　22-13

解码还原会话后发现 SP Token 接口机前端返回的 Code 值是“1”。表明验证通过，符合业务程序正常设定，如下图所示。

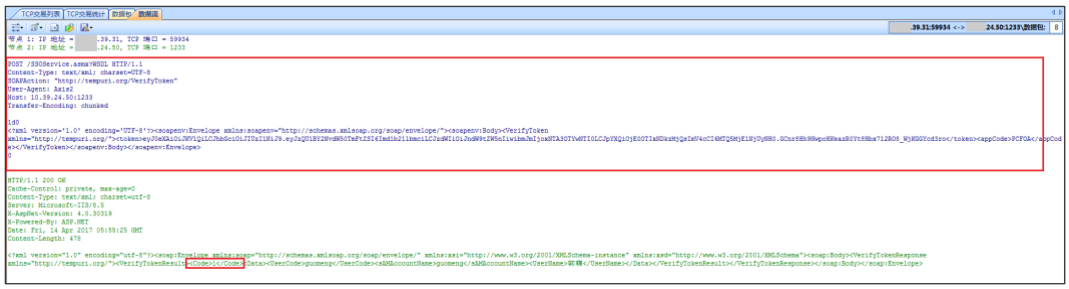

图　22-14

通过上述分析可以判断，异常跳转出现时，OA 前端发送至 SP Token 接口机前端的 Token 的验证返回是正常通过的，也就是说 SP Token 接口机前端正常返回了成功验证消息（Code=1）。OA 前端在收到 Token 的正常验证后，内部程序存在异常，导致无法生成正常 OA 系统主页链接请求，最终跳转到异常页面。

22.3　分析总结及问题处理

异常跳转发生时从客户端至 OA 前端系统请求链接与正常业务时出现的请求链接存在很大不同，正常会话时产生的多线程连接（17 条）明显多于异常会话时的连接数（2 条）。并且异常跳转发生时，OA 前端与 SP Token 接口机前端的 Token 关联验证阶段，明显看到验证是成功的。因此可以排除是 SP Token 接口机前端的问题，OA 前端系统程序存在较大可疑。

开发人员在听取分析结论后，修改 OA 前端系统代码，成功解决了 Token 正常验证后生成跳转链接的不稳定问题。

22.4　价值

运用网络回溯分析技术对数据流进行精准分析，可迅速排除干扰因素，精准定位 SSO 单点登录跳转异常的发生节点，确定故障根因。避免业务损失，优化运维工作。

科来网络流量分析解决方案

科来业务性能解决方案

- 科来业务性能管理系统(UPM)
- 科来网络回溯分析系统(RAS)
- 科来网络分析系统(CSNAS)

科来网络安全分析解决方案

- 科来大数据安全态势感知平台(BAP)
- 科来网络全流量安全分析系统(TSA)
- 科来APT攻击检测系统(APT)

CSNA 网络分析认证培训

课程介绍

培训报名

科来网络流量分析技术资料

网络攻击与防范图谱

科来网络通讯协议图

科来网络故障诊断图

CSNA 网络分析经典实战案例

数据包样本

网络分析过滤器

术语表

科来网络流量分析产品下载(免费版)

科来网络分析系统

科来 MAC 地址扫描器

科来 Ping 工具

科来数据包播放器

科来数据包生成器

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