Sniffer Infinistream 分析案例

1、概述

用户业务的运行对网络的依赖性越来越强，网络特别是骨干网络的稳定健康运行直接关系到日常业务的正常运行。对骨干网络的流量分析；对潜在隐患提前预警；对各种发生的故障进行及时定位、分析、处理；在此基础上合理利用网络资源；根据应用现状和发展趋势进行网络规划；保障网络安全、高效、稳定的运行就变得日趋重要。

用户现有的网络管理系统在长期的网络流量分析方面存在不足。主要表现在如下方面：

长期的网络和应用问题分析能力不足

现有的网络管理系统无法长期的纪录网络和应用的运行状态，无法长期的保存网络流量信息，在出现网络或应用问题时，不能为网络技术人员提供有效的信息依据，问题往往是依靠网络技术人员通过推断来分析，这样网络问题的分析效率很低，同时很难得到确实的分析结论。

缺乏对网络和应用间歇性问题的分析能力

网络或应用可能出现间歇性故障，这种故障的出现一般很难判断，在出现后很难分析其产生原因，而再次出现的时间无法确定，因此难以解决，好像网络中存在一个不定时的炸弹，使用户网络和应用时刻处于危险之中。

对网络安全问题的分析能力不足

在发生网络安全问题时，缺乏有效的监控分析手段，导致网络的安全性降低，例如蠕虫病毒的爆发，应该能够对蠕虫病毒的传播情况进行有效的分析。

2、 Sniffer Infinistream 产品介绍

Sniffer Infinistream 是 Sniffer 企业网络管理系统的重要组成部分，Sniffer Infinistream 集成 Sniffer 业界领先的网络流量监控和解码分析能力以及专家系统，同时具备大容量的存储能力，为您提供了业界领先的的网络故障隔离和性能管理解决方案，Infinistream 具备如下技术特点：

千兆位网络流量数据捕获和存储

Infinistream 能够实现千兆网络流量的线速捕获，Infinistream 采用了 stream-to-disk 技术，实现高达 1800Mbps 的捕获存储性能，能够有效地捕获、检索和存储网络中的所有数据包，并提供全面、明确的分析数据。

大容量存储

Infinistream 的高达 4T 的磁盘空间可以支持长时间的网络流量的保存，按建行目前的网络流量情况，采用 Infinistream 能够存储长达两个多月的网络流量数据，从而为网络维护人员提供切实、科学的分析依据。

方便快速的数据检索

Infinistream 采用特殊设计的文件和索引系统，减少了需要检索和分析的数据的总量，这个智能化的数据采集过程可快速创建一个含有数据流图示的

Windows 界面，用户可以通过该界面迅速的检索到所需的数据，从而为您节省大量的时间。

历史统计分析

当用户进行问题诊断时，往往很难确定从何时开始。InfiniStream 解决方案中的历史信息统计功能提供大量的统计信息，能帮助用户快速找出何时出现网络异常。所有统计信息都会以数据包数和字节数、带宽大小和数据包大小来显示。可以得到基本的网络流量统计信息，从而用户能轻易的找出性能最好和性能最差时的网络流量，图形化的检索能帮用户快速的找到流量峰值或流量趋势。

Infinistream 将给用户提供强大的网络流量数据存档分析能力，提供给用户事后分析的能力，大大地提高用户进行故障分析的能力和安全分析的能力。

3、Sniffer Infinistream 部分分析案例

现象描述

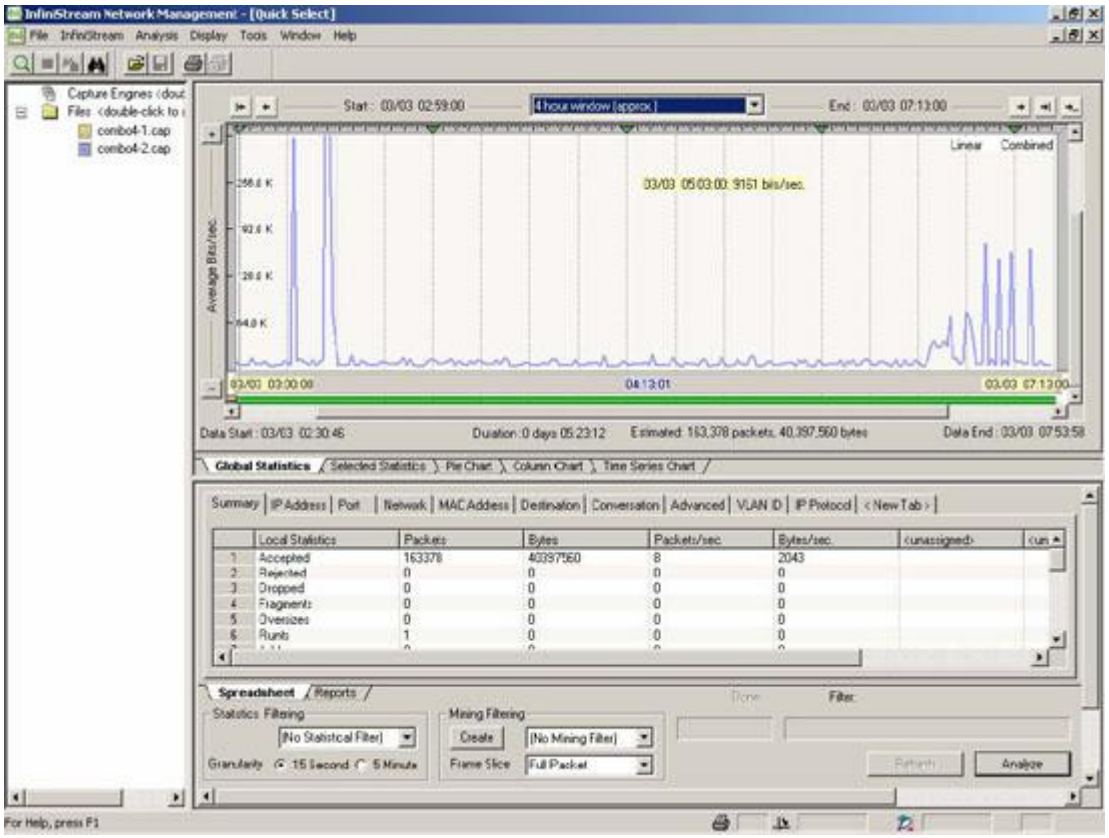
应用部门报告由于网络问题引起 SQL Server 无法正常访问，在凌晨 3:00 时数据库连接超时导致连接中断，数据库日志中没有发现错误报告，持续了一段时间后数据库访问恢复正常。

SQL Server IP 地址：130.214.90.94

客户端 IP 地址：130.214.90.63

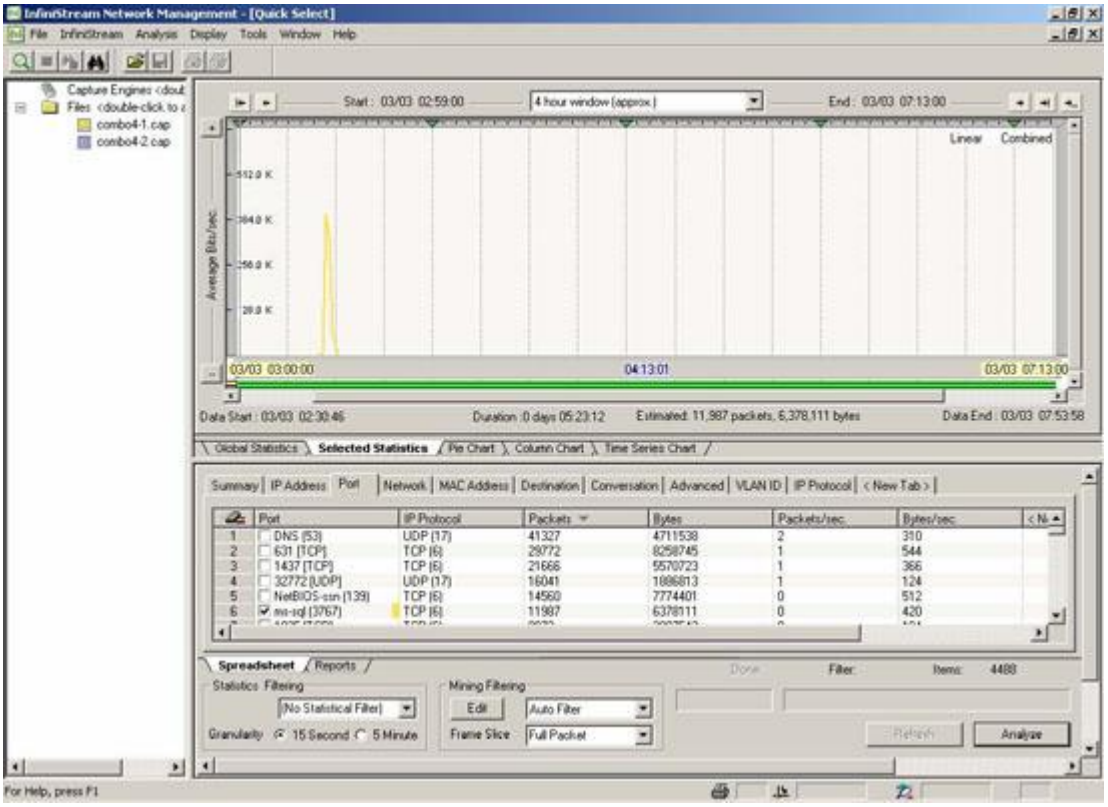
SQL Server 服务端口：3767

利用 Infinitream 进行分析



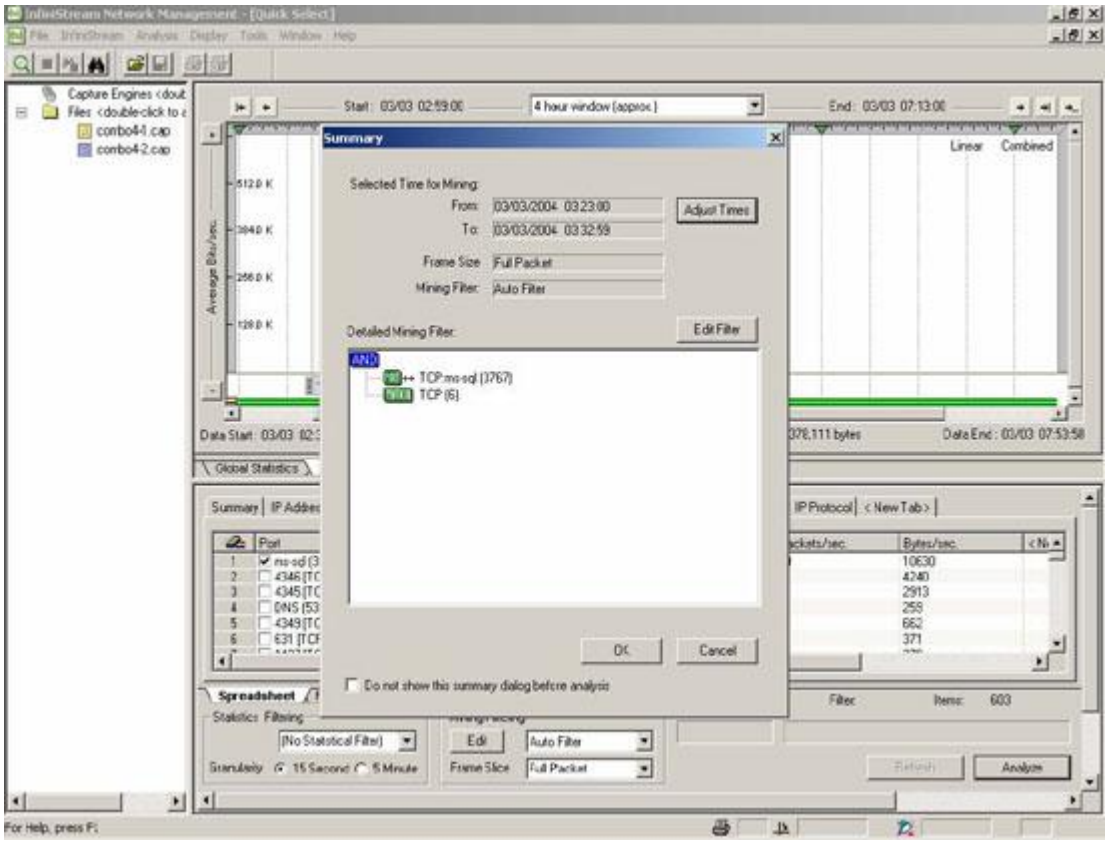
部署了 Infinitream 后，我们保存了所有的网络流量，使我们得以分析发生问题时的网络流量从而找到问题产生的原因。

选取当时的 SQL Server 访问流量



通过 Sniffer Infinitream 强大的检索分析功能，我们能快速的将发生问题当时的 SQL Server 流量找到并选取出来。

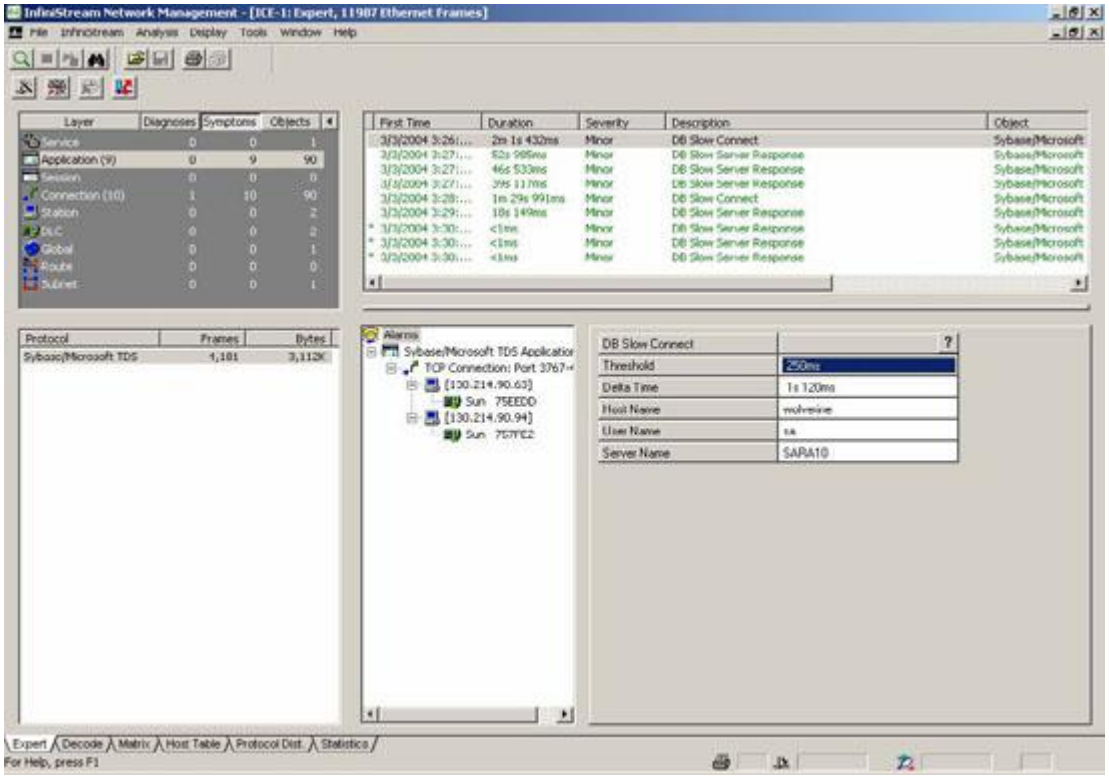
对相关流量进行过滤



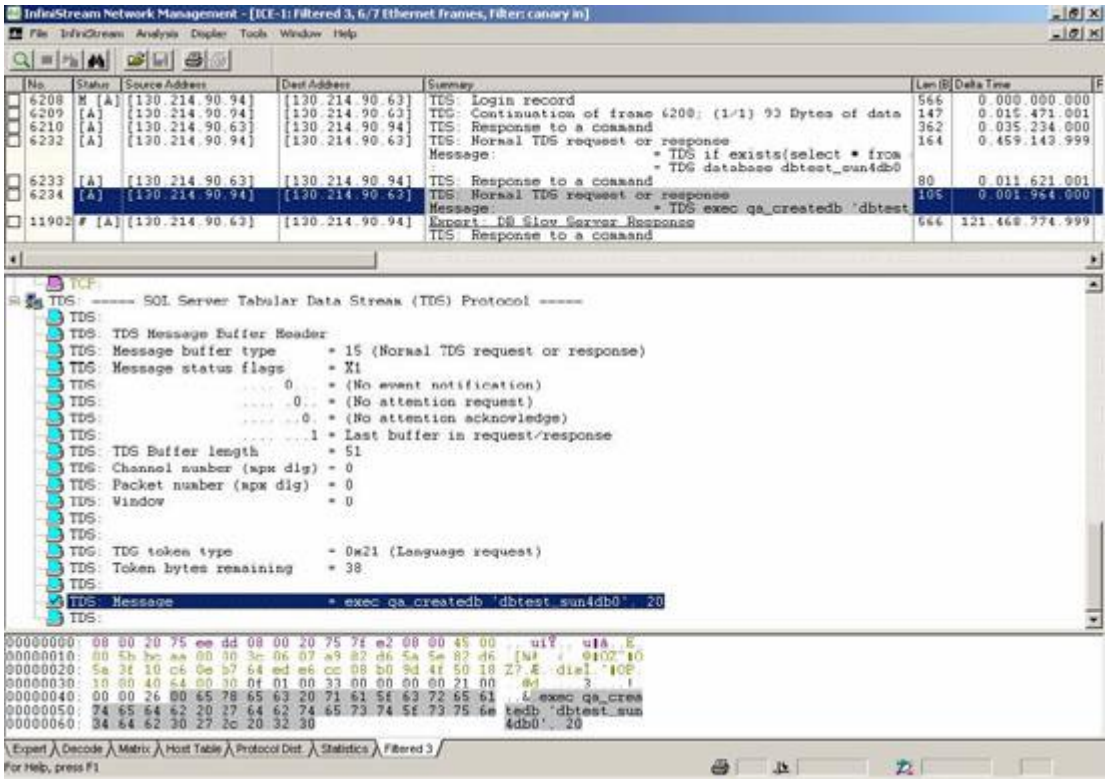
将当时的 SQL Server 流量(端口号为 3767)的流量快速过滤出来进行分析。

Sniffer 业界最强大的流量分析能力帮你分析问题产生的原因

强大的专家系统帮你迅速找到问题流量。



强大的协议解码可以分析当时数据库访问请求的内容。



通过协议解码我们发现在 SQL Server 响应变慢前客户端正在执行 qa_createdb 脚本，该操作造成数据库响应缓慢。

利用 Sniffer Infinitream 我们可以回现问题发生时的网络流量并进行分析，从而有效地分析问题发生的原因。

4、结论

Sniffer Infinistream 的高性能长期网络流量捕获存贮能力、快速网络流量检索能力、流量的高级统计分析能力以及其强大的协议解码能力和专家分析能力能够有效地帮助网络管理人员纪录关键网络链路上的网络流量信息，从而有助于进行网络的日常流量分析，一旦出现网络异常能够迅速发现。并能够迅速取得网络和应用故障时的网络流量数据，从而能够极大地提高网络和应用问题的分析能力并加快解决问题的速度，为提高网络管理水平提供了有效的技术手段