CA Application Delivery Analysis

用户指南

10.1

ca technologies

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA Application Delivery Analysis
- CA GigaStor
- CA GigaStor 连接器
- CA Multi-Port Monitor
- CA Performance Center
- CA NetQoS Performance Center
- CA Standard Monitor
- CA Virtual Systems Monitor

联系技术支持

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：http://www.ca.com/worldwide。

目录

第 1 章： 欢迎使用 Application Delivery Analysis

此部分包含以下主题：

简介

CA Application Delivery Analysis 是 CA Performance Center (CA PC) 和 CA NetQoS Performance Center (CA NPC) 中的端到端性能监视模块，可跟踪和度量应程序用响应时间，而无需桌面或服务器代理。端到端性能监视使您可以执行以下操作：

- 度量网络向最终用户交付服务的情况
- 获得对网络中发生情况的最佳了解

CA Application Delivery Analysis 可监视 TCP 应用程序数据包从网络传入和传出数据中心的过程，并允许您度量网络往复传输时间、服务器响应时间、数据传输时间等。

管理控制台将响应时间分割为应用程序、网络和服务器延迟这几个组成部分，以帮助您快速排除网络性能瓶颈并维护应用程序性能。自动进程可为所有 TCP/IP 用户事务度量和分析应用程序性能。然后，这些进程会将响应时间与阈值进行比较，并在问题发生时自动调查问题。现在，“网络”和“操作”组具有用于快速解决性能问题的关键诊断数据。

CA Application Delivery Analysis 还监视可用性和应用程序性能，这样即使未制定正式的运行水平协议 (OLA)，您也将具有一组一致的用于内部用户和外部服务提供商的服务质量度量标准。

度量性能

为了监视端到端性能，管理控制台使用：

- 管理控制台计算的*基准*或平均值，以使您能够查看历史上网络中的正常性能。使用基准将特定期间内的应用程序/服务器组合的性能与过去性能的历史平均值进行比较。超出基准不一定表示出现问题。
- *阈值*可在性能超过可接受限制时告知管理控制台。管理控制台包括默认阈值，管理控制台管理员可将这些阈值调整为基于百分位的值（敏感度因素）或毫秒值。当超出性能阈值时，管理控制台会创建一个突发事件。管理控制台管理员可为突发事件响应创建操作和通知，以帮助标识问题源。

通过将阈值与基准进行比较，可以查看阈值与历史平均值的比较情况，并将此信息用于容量计划。管理控制台使用阈值对数据分级。阈值违反表明现有问题或潜在问题。

基准

基准是性能的历史标准。管理控制台自动计算每小时基准，并针对一天中的特定时间、星期日期和每月中的特定日期进行调整。上周活动的加权系数最大，因此基准将正确适应系统性变化。这些基准高度细化，因此可以反映业务周期的影响。每个组合（度量标准、网络、服务器、应用程序）收到自己对一天中每小时的计算。基准允许您将实际性能与此时的预期性能进行对比，从而为“正常”定义提供上下文。

管理控制台会为 10 个基准度量标准中的每个度量标准计算特定网络-服务器-应用程序组合的基准。它不对基准求平均值；因此，报告不显示聚合的基准。管理控制台包括性能详细信息图表中的基准信息。它不使用基准来确定阈值。

要在图表中查看基准，请选择网络、服务器、应用程序和基准度量标准。摘要图表不包含基准。“操作”页面显示在性能图表中绘制的基准值，以帮助您将当前性能与正常值进行比较。“管理”页面上的性能记分卡以表格格式显示基准值。

当您在“图表设置”页面中启用基准时，管理控制台将在“操作: 度量标准详细信息”视图中显示基准。

阈值、突发事件和突发事件响应

*阈值*是可接受性能的上限。由于以下原因，阈值非常重要：

- 阈值使管理控制台可对数据分级。
- 阈值有助于突发事件创建和生成的突发事件响应及调查，通过这些响应和调查可以及时进行故障排除和解决问题。

默认情况下，每个应用程序都存在阈值。管理控制台管理员会为网络和服务器性能设置阈值。对于每个度量标准，您会定义一个“轻微”（黄色）阈值、一个“重大”（橙色）阈值以及显示性能下降所需的最小观测值数。

管理控制台会计算默认阈值。它不使用基准来计算阈值，而是从相同数据中分别计算阈值和基准。管理员可以更改阈值，以提高或降低对性能更改的敏感度。

当超出阈值时，管理控制台将创建突发事件并启动配置的突发事件响应。您可以为每个网络、服务器、应用程序或监视设备突发事件类型配置突发事件响应。管理控制台包括每种突发事件类型的默认突发事件响应。

管理控制台管理员可以设置操作和通知，以响应对指定时段满足或违反的每个阈值。对于给定的突发事件响应，管理员可以指定要在以下情况下发生的操作或通知：

- 当性能满足或超出“轻微”阈值时
- 当性能满足或超出“重大”阈值时

管理控制台会为每个条件打开一个突发事件。如果用于条件的操作存在，管理控制台将自动启动该操作。

请记住有关突发事件、突发事件响应和操作的以下详细信息：

- 当超出阈值时，管理控制台将创建突发事件。
- 除非满足以下条件，否则突发事件不会自动触发操作：
  - 相应的突发事件响应与网络、服务器、应用程序或监视设备关联。当创建突发事件响应时，您设置了关联。
  - 关联的突发事件响应具有关联的操作。默认的突发事件响应没有关联的操作。
  - 违反超过最小严重度和持续时间条件。
- 可能有的突发事件没有操作。
- 可能启动没有突发事件的操作。与突发事件关联的操作被称作调查，可以手动启动或排定调查。

就以下方式而言，突发事件和突发事件响应对于故障排除很有用：

- 当发生问题时，突发事件会维护一个条件记录。
- 突发事件响应会自动收集信息，这些信息可帮助您在发生问题时进行故障排除，从而缩短平均修复时间 (MTTR)。

突发事件响应是零个或多个操作的集合。操作可能是通知或自动调查。有关可以创建的突发事件响应的类型的信息，请参阅*《管理员指南》*。

调查

如果突发事件响应未搜集足够信息来帮助您解决问题，则可启动即时或排定的调查来搜集附加信息，以便进一步对该问题进行故障排除。调查是管理控制台执行的一项操作，用于收集有关阈值违反原因的诊断信息。管理控制台用户帐户必须具有允许您执行调查的关联角色。

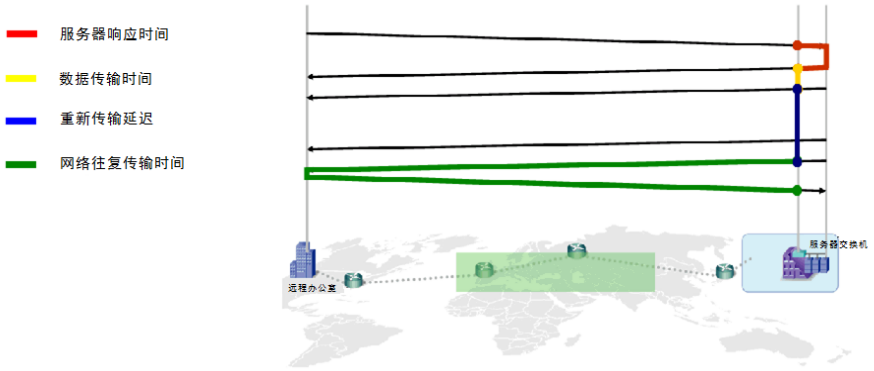
调查可以执行以下操作之一：

- 应用程序连接时间
- 数据包捕获
- Ping 响应时间
- SNMP 服务器查询
- SNMP 路由器查询
- ICMP 跟踪路由
- TCP 跟踪路由

请注意，管理控制台管理员必须配置能够调查的 SNMP 团体。有关详细信息，请参阅*《管理员指南》*。

响应时间

管理控制台包括响应时间的度量，以 5 分钟间隔（含）对这些度量求平均值。



注意： 对于 WAN 优化的事务，这些响应时间的定义会有所不同。

服务器响应时间

服务器发送对客户端请求的初始响应所需的时间，或初始服务器的“思考时间”。“服务器响应时间”的增加通常表示以下含义：

- 服务器资源（如 CPU、内存、磁盘或 I/O）不足
- 写入应用程序的性能不佳

数据传输时间

将度量的完整响应从初始数据包传送至最后一个数据包所需的时间。如果发送的数据比 TCP 窗口中填充的数据多，则数据传输时间不包括初始的服务器响应时间，而仅包含网络往复传输时间。

重传延迟

在原始数据包发送与最后一个重复数据包发送之间的已用时间。管理控制台报告的“重传延迟”是整个观测的平均值，而不仅仅是针对重传的数据包。如果一整套 10 个数据包需要 300 毫秒重传时间，则报告的重传延迟为 30 毫秒（300 毫秒/10 个数据包）。

网络往复传输时间

数据包在网络上的服务器和客户端之间双向经过所花的时间。

总事务时间

在永久 TCP 连接中完成 TCP 事务或数据请求所花的时间。

有效往复传输时间

网络往复传输时间加上重传引起的延迟。

关键概念

要了解并使用管理控制台收集和报告的数据，您必须熟悉一些重要的概念和术语。

本节中的主题解释了新用户不熟悉的大部分产品术语以及一些行业标准术语。

聚合

聚合是您为使比较报告变得有意义而创建的一组应用程序、服务器或网络。在“工程”页面上，管理控制台将聚合视为一个实体。“操作”和“突发事件”页面分别显示聚合中每个成员的数据。

一个聚合示例是远程办公室中的一组 IP 子网，其中管理控制台跨构成远程办公室的各个客户端子网分析性能度量标准。最好为每个远程办公室创建一个聚合，以允许进行比较。

可用性

如果用户在 5 分钟期间内可以访问某一应用程序或服务器，管理控制台会将该服务器或应用程序分类为可用。管理控制台会通过被动数据观测在服务器和应用程序端口级别跟踪可用性度量标准。当未观测到任何用户通信量时，管理控制台将通过每 5 分钟发出活动请求来验证可用性。

如果已启用可用性监视，管理控制台将跟踪服务器和应用程序组合，以了解其可用性。管理控制台不跟踪网络可用性。

冒泡

管理控制台会将最差的执行程序排序或“冒泡”到“操作”报告页面上列表的顶部。这些页面显示执行效果最差的网络、服务器和应用程序的性能度量标准。

监视设备

监视设备监视 TCP 会话的响应时间。管理控制台支持若干种类型的监视设备。

数据点

默认情况下，管理控制台会对预设间隔内的数据求平均值，以生成数据点。对于用于计算数据平均值的每个时间间隔，管理控制台将计算具有代表性的数据点，并在图表或表中显示此数据。每个图表和表将报告用于计算每个数据点的时段。

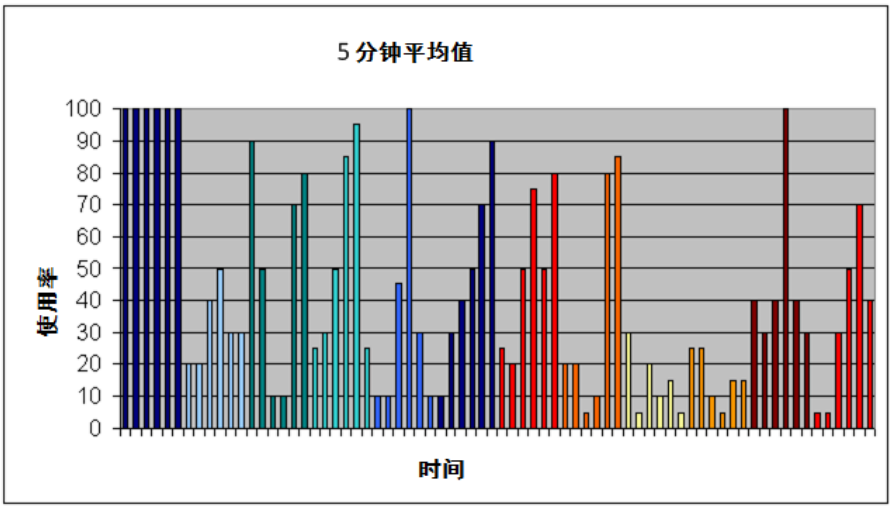
对于使用下表中时段的视图，管理控制台将使用以下间隔计算数据的平均值：

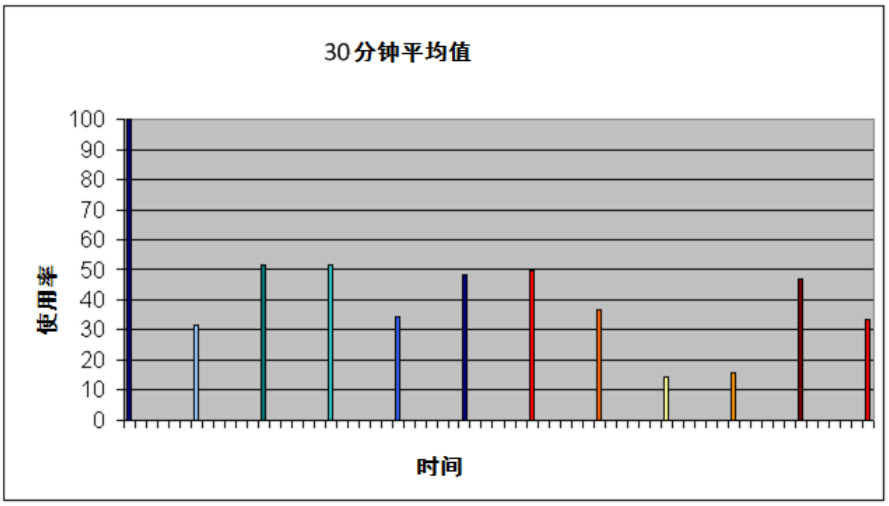
时段	间隔
过去 1 小时	5 分钟
过去 8 小时	5 分钟
最后一天	15 分钟
上周	1 小时
上月	6 小时

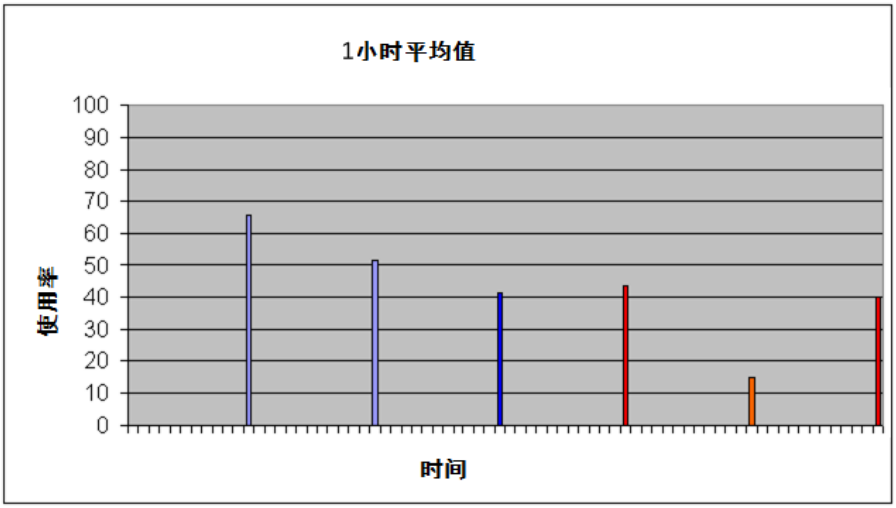
按如下所述配置数据点的报告：

- 使用更短的平均间隔来分析特定问题。
- 使用更长的平均间隔标识一段时间内的模式和趋势。

以下视图显示，当平均间隔从 5 分钟增至 1 小时时，粒状数据点到用于趋势和模式标识的曲线的转变。







突发事件

突发事件是管理控制台在检测到满足或超过已定义阈值的性能时创建的信息记录。您可能需要分析突发事件，以确定导致度量标准提高的事件。在“突发事件”页面中，管理控制台按分配的案例编号来报告突发事件。

如果在 CA PC 或 CA NPC 上注册了管理控制台，管理控制台会将其突发事件状态与 CA PC 或 CA NPC 中的事件保持同步。

管理控制台会根据您为 5 分钟数据配置的存储时间来存储突发事件记录。

突发事件响应

突发事件响应可帮助您在发生问题时进行故障排除，减少平均修复时间，将突发事件响应分配给业务关键型应用程序、服务器和网络。突发事件响应：

- 就性能下降向您的团队发送通知。
- 主动调查问题来收集其他信息，以帮助您识别导致性能下降的根本原因。

默认情况下，管理控制台不会自动启动突发事件响应。

调查

如需了解有关突发事件原因的详细信息，您可以手动启动或排定调查操作。

维护排定

可将维护排定与每个受监视的服务器相关联。以下规则适用于维护排定：

- 在维护期间，管理控制台将在数据库中标记用于该服务器的数据点和突发事件，并且不在报告中包括这些内容。
- 如果更改维护排定，该更改将不修改历史数据。
- 管理控制台在维护期间仍会报告服务器性能，但对于维护期间在 OLA 报告中出现的低性能或低观测计数不会打开突发事件。
- 当维护排定结束或开始时，管理控制台将关闭已打开的突发事件并创建新突发事件来反映当前的维护状态。

度量

度量标准是管理控制台在 5 分钟的报告期间内针对特定服务器和网络上的特定应用程序度量的参数。管理控制台还记录在 5 分钟期间内观测到的具有度量标准平均值的观测数。

管理控制台报告以下度量标准：

- 字节数据量
- 连接建立时间
- 数据速率(比特数/秒)（传入和传出服务器）；按数据包（传入和传出服务器）
- 数据量(以字节为单位)（传入和传出服务器）；按数据包（传入和传出服务器）
- 数据包数据量
- 百分位吞吐量
- 每用户综合速率
- 重传延迟
- TCP/IP 会话 - 完成
- TCP/IP 会话 - 打开
- TCP/IP 会话 - 已到期
- TCP/IP 会话时间
- 用户
- 用户正常输出

您不能为这些度量标准设置阈值，管理控制台不创建与这些度量标准相关的突发事件。您可以为其设置阈值的度量标准被称为*相关度量标准*。管理控制台还报告相关度量标准。

网络类型

网络类型是用于对具有相似特点和性能预期的网络进行分组的已配置网络的分类。使用网络类型可为报告、突发事件响应生成或服务水平监视组织企业；例如：

- 按带宽 - 128K、T1、LAN
- 按位置 - 中西部、HQ

可以使用默认网络类型或创建自定义类型。

通知

通知是与突发事件响应关联的操作类型。通知会提醒用户或计算机阈值已满足或超出指定时段。

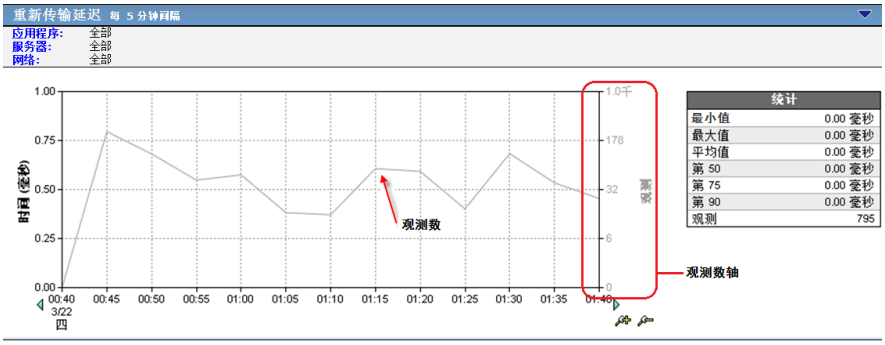
通知可为以下内容之一：

- 发送给特定人员的电子邮件
- 发送给接收器（如第三方监视平台）的 SNMP 陷阱

观测

观测是在指定的时间间隔内发生的受监视 TCP 事务的数量。观测是度量标准度量的机会。为每个度量标准指定如果未提供有意义的通信量，则用于触发调查并避免通知的最小观测数。

观测计数在管理控制台视图中显示为灰线。右侧的轴指明观测数，并且为指数，其中包括视图中的计数变化。



观测计数指明使用率。观测计数越高，则表示应用程序、服务器或网络的使用率越高。

使用观测计数可确定事件的重要性。如果观测数较多，则表示一个事件可能会影响许多用户、应用程序或服务器。如果服务器的观测数减少，同时“服务器连接时间”增加，则“服务器连接时间”的增加可能表示服务器中正在运行其他操作（如备份）。

百分位

*百分位*是从 5 分钟数据点的集合中执行的百分比计算。管理控制台存储百分位数据并在报告中使用该数据。

已分级的度量标准

在 5 分钟报告间隔期间，如果注意到足够的观测数，并且每个应用程序、服务器、网络和 5 分钟期间的组合都有可用阈值，则管理控制台会将度量标准分级为“正常”、“轻微”（黄色）或“重大”（橙色）。如果观测数不足或没有阈值可用，则管理控制台会将度量标准分类为“未分级”。

相关度量标准

*相关度量标准*具有管理控制台管理员可以配置的关联阈值。当超出阈值时，管理控制台将打开一个突发事件并计算 5 分钟期间内相关度量标准参数的平均度量，以报告基准。

在以下各部分中介绍的度量标准与其描述的项相关；例如，“网络往复传输时间”与网络相关。

网络度量标准

网络度量标准与网络性能相关。

度量	说明
网络往复传输时间	数据包遍历网络所需的时间。
网络连接时间	客户端确认服务器的连接确认所需的时间。延迟可能由网络延迟引起。
有效往复传输时间	网络往复传输时间加上重传引起的延迟。
数据包丢失百分比	重传数据占总数据的比率、被监视网络上丢失的数据所占的百分比，以及用“数据包数/秒”表示的丢失速率。QoS 视图的一部分。

服务器度量标准

服务器度量标准与服务器性能相关。

度量	说明
服务器响应时间	服务器开始响应请求所花的时间。

服务器连接时间	服务器确认初始客户端连接请求所花的时间。
拒绝的会话	服务器在三次握手期间显式拒绝的连接请求。“未实现的 TCP/IP 会话请求”视图的一部分。
无响应的会话	已发送连接请求、但服务器从未响应的会话。“未实现的 TCP/IP 会话请求”视图的一部分。

了解组合度量标准

综合度量标准与应用程序性能相关，由服务器和网络度量标准组成。

度量标准	说明
数据传输时间	传送所测的完整响应（从初始数据包到响应中的最终数据包）所花的时间。如果发送的数据比 TCP 窗口中填充的数据多，则数据传输时间不包括初始的服务器响应时间，而仅包含网络往复传输时间。
事务时间	从客户端发送请求（数据包级别或事务级别）开始到客户端接收响应中的最后一个数据包为止所用的时间。管理控制台在“工程”页面的摘要“响应时间组成: 平均”视图中显示此类型的响应时间数据。

可为相关度量标准设置阈值。管理控制台将计算 5 分钟期间的相关度量标准的平均度量，以报告基准。

注意：WAN 优化事务的度量标准定义有所不同。

报告分辨率

管理控制台报告的默认报告分辨率如下所示：

- 小于或等于 8 小时的报告的默认分辨率为 5 分钟
- 大于 8 小时且小于或等于 24 小时的报告的默认分辨率为 15 分钟
- 大于 1 天且小于或等于 7 天的报告的默认分辨率为 1 小时
- 大于 7 天且小于或等于 1 个月的报告的默认分辨率为 6 小时

当创建自定义时间范围时，请从以下值中选择报告分辨率：

- 5 分钟
- 15 分钟
- 30 分钟
- 1 小时
- 1 天

使用 5 分钟间隔来查看少于 8 小时的持续时间中的数据，以便用最高分辨率进行报告。当报告持续时间大于 1 个月时，则使用 1 天的间隔。

如果为较长的报告期间选择较短间隔，则由于数据点数的原因，视图可能难于读取和确定趋势，管理控制台生成可能需要较长时间。

样本分辨率

管理控制台报告的默认样本分辨率如下所示：

- 8 小时报告的默认样本分辨率为 5 分钟
- 每日报告的默认样本分辨率为 15 分钟
- 每周报告的默认样本分辨率为 1 小时
- 每月报告的默认样本分辨率为 6 小时

运行水平协议 (OLA)

运行水平管理 (OLM) 中包括的过程可确保，根据业务优先级并以可接受的成本向所有 IT 用户交付适当水平的服务。通过在管理控制台中设置和监视运行水平协议 (OLA)，您可以确定服务水平是否得到了满足。在“管理”页面中查看 OLA 报告。

您通常会对以下性能度量标准设置 OLA：

- 服务器响应时间，以量化数据中心的性能
- 网络往复传输时间，以量化网络基础架构的性能
- 事务时间，以捕获用户使用应用程序的体验

阈值类型

管理控制台通过使用百分位和敏感度设置对数据示例中的每个度量标准分类，可基于最新的过去性能自动计算阈值。

通过调整敏感度设置或通过设置百分比或毫秒值来更改阈值。

阈值类型	说明
无	（关闭）强制管理控制台将所有数据分级为“*未分级*”。管理控制台不为阈值为“无”的度量标准创建突发事件。
敏感度	（动态）通过使用百分比值设置此类型的阈值。管理控制台将此百分比值作为因素计入用于自动计算阈值的公式中。如果敏感度设置为 200，则会将在 75 百分位度量的通信量分级为“轻微”（黄色）或“重大”（橙色）。低敏感度设置会使得阈值较高，从而导致突发事件数量减少。
毫秒	（静态）将此类型的阈值设置为静态值（如 100）。

吞吐量

管理控制台通过将传输的字节数除以已用时间来计算吞吐量。管理控制台对每个 TCP 事务执行此计算。传输的字节来自服务器，而不是总字节数。吞吐量计算是仅用于大型事务的适当度量。

时间范围

使用通过报告页面上的“设置”提供的“时间范围”菜单可在管理控制台中配置视图。管理控制台显示在当前时间结束的时间间隔的数据。选择“自定义”，以指定结束日期不是今天的时间间隔。

登录管理控制台

要开始使用管理控制台，请使用服务器名称或 IP 地址访问承载控制台的服务器；例如：

`http://<IPAddress>`

管理控制台的设计适合在 Microsoft Internet Explorer 7 或 8 以及 Mozilla Firefox 3.6 中显示，并且需要使用 Adobe Flash Player。如需登录信息，请联系管理控制台管理员。

查看“关于”信息

要查看管理控制台版本和修订信息，请单击菜单栏上的“关于”。

- 版本：显示有关管理控制台的已安装版本、安装日期和时间、HASP 到期日期和时间以及配置的信息。其中还包括到产品文档的链接。
- 修订历史：列出已安装版本及其安装时间的历史记录。
- CA PC 和 CA NPC：如果已作为数据源连接到 CA PC 或 CA NPC，则表示 CA PC 或 CA NPC 服务器地址和产品版本号。

导航提示和技巧

当您熟悉管理控制台界面时，请记住以下提示。

- 当您在管理控制台中查看报告页面和视图时，通过单击网络、应用程序、度量标准、突发事件以及蓝色字体显示的其他列出项导航到报告，以获取详细信息。
- 查看并单击可看到以下符号的任何信息框中的链接： 。管理控制台使用信息框引导您完成整个过程，并向您提示附加信息。
- 在报告或视图中单击蓝色项并检查信息之后，单击“设置”区域中的 [清除] 并返回更高级别的数据或页面。

- 将鼠标放在控件或视图部分等项目上方，以查看有帮助的“工具提示”信息。将鼠标放在视图中表示界面的条上方，以获取有关该界面的详细信息，如其路由器、说明和速度。
- 通过打印、以电子邮件形式发送报告页面或视图，或者将报告页面或视图保存到电子表格中来共享信息。要打印、通过电子邮件发送或导出整个报告页面，请使用报告页面顶部的按钮。要打印、通过电子邮件发送或导出视图，请使用视图顶部的蓝色齿轮菜单 。
- 通过单击列标题来更改排序顺序，可按升序或降序来排列视图中的数据。
- 如果已在 CA Performance Center 或 CA NetQoS Performance Center 中将管理控制台添加为数据源，则可以通过单击管理控制台右上角的 NPC 链接来从管理控制台访问相连的 Performance Center。有关使用 CA Performance Center 或 CA NetQoS Performance Center 的信息，请参阅 CA Performance Center 或 CA NetQoS Performance Center 文档。

第 2 章： 使用管理控制台

AITempty

此部分包含以下主题：

单点登录

单点登录是 CA PC、CA NPC 及所有支持的数据源（包括 CA Application Delivery Analysis）使用的身份验证方案。用户通过 CA PC 或 CA NPC 的身份验证后，用户可以在 CA PC、CA NPC 和注册的数据源之间导航，而无需再次登录。

单点登录已自动安装。相连的 CA PC 或 CA NPC 的链接显示在管理控制台的右上角。

编辑您的用户配置文件

您可以编辑自己的用户配置文件，例如，指定您的本地时区。在 CA PC 或 CA NPC 中注册为数据源后，您的更改将在 5 分钟内自动同步。

遵循这些步骤:

1. 在菜单栏上单击您的用户名。

   将打开“用户配置文件”页面。

2. 输入以下信息：

   密码

   键入您的新密码。

   确认密码

   重新键入您的密码。

   电子邮件地址

   键入您的电子邮件地址。

   时区

   选择您的本地时区。管理控制台偏移报告数据到该时区。默认时区为 CST6CDT，也就是比 GMT 晚 6 小时的中部标准时间，或晚 5 小时的中部夏令时。可能的情况下尽量使用特定时区，而不要使用您所在时区的 Etc 时间，因为 Etc 时间不会考虑夏令时，且偏移量与您期待的恰好相反，即 Etc/GMT+4 是比 GMT 晚 4 小时，而不是早 4 小时。

   主页

   选择您访问管理控制台时要显示的默认页面。

3. 单击“应用”，然后单击“确定”。

收集的数据、报告页面和视图

使用管理控制台报告可确定某个性能问题是源于网络基础架构、服务器还是应用程序。管理控制台使用以下变量的组合生成报告：

- 网络
- 服务器
- 应用程序
- 时间范围
- 度量

如果您知道想要分析的数据，则可以轻松生成一份报告来显示所需的信息。

管理控制台可让您将性能问题隔离到下表中的某个元素或元素组合。

元素	性能问题的可能起因
网络基础架构	以下组件引起的延迟： ■ 线路 ■ 通信拥塞 ■ 路由器 ■ 交换机
服务器基础架构	以下组件引起的延迟： ■ CPU 处理 ■ 内存 I/O ■ 磁盘读取和写入
应用程序体系结构	许多要传输的小数据包中正写入大量数据请求

可以使用以下方法来查看和分析管理控制台数据，从而确定性能问题的起因：

1. 使用性能图和应用程序详细信息视图，识别存在性能问题的应用程序。
2. 隔离作为性能问题促成因素的响应时间组成。“响应时间组成”视图中的颜色标识出了构成总时间的每个组成部分。
3. 通过检查“通信量”、“会话”、“趋势”、“响应大小”、“QoS”和“统计”页面，可调查导致性能问题的因素。

   有关识别和解决性能问题的详细信息，请参阅故障排除 (p. 125)。

报告页面导航

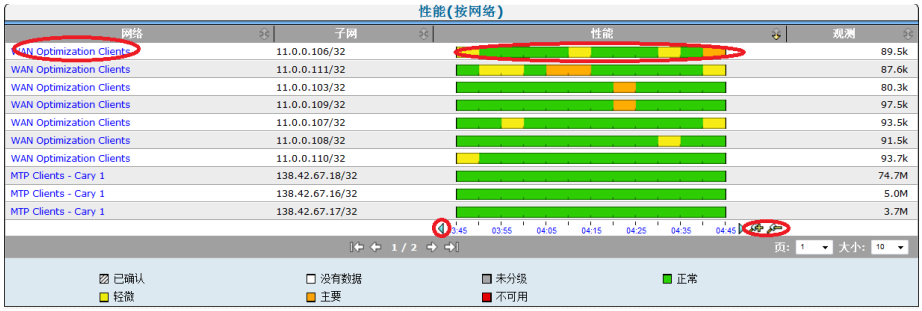
采用选项卡式页面，以对应 IT 部门的职能角色。例如，“工程”页面可让您快速访问包含网络工程师感兴趣的数据的报告，其中第一个页面就是“性能(按网络)”报告页面。每个选项卡式页面以不同的方式呈现数据，以帮助您进行故障排除、分析趋势以进行优化，或查看摘要报告。

您可以导航到所需报告，或者在“向我显示”菜单中选择一个视图。通过单击“操作”、“突发事件”、“管理”、“工程”或“优化”视图和报告页面上的“设置”，可以更改要在视图或报告中显示的时间范围、选定度量标准、应用程序、服务器和网络。

筛选报告页面上的数据	请参阅
从概览报告导航到详细信息。	导航到报告 (p. 32)
在“向我显示”菜单中选择一个视图。	“向我显示”菜单导航 (p. 33)
通过单击“设置”来更改视图的设置。	更改报告设置 (p. 34)

导航到报告

通过单击“操作”报告中的链接和用户界面中的其他元素（如以下“性能”示例报告中所示），可以访问详细信息。

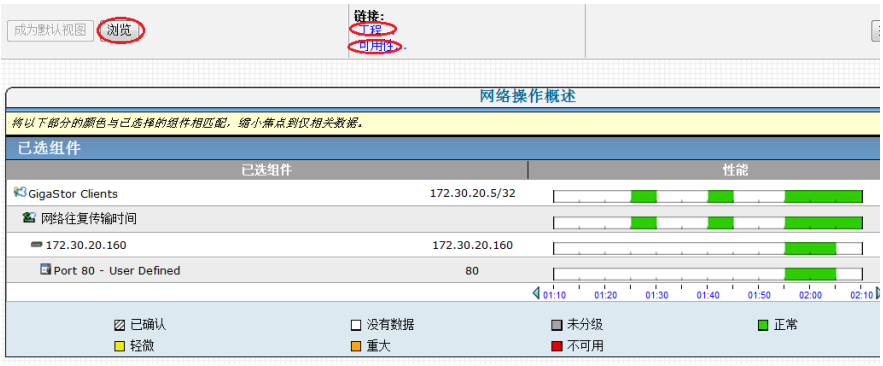


在“性能”报告中，通过执行以下操作来查看详细信息：

- 单击某个网络可查看该网络的选定组件。
- 单击时间设置上的箭头可前后移动时间设置。
- 单击放大镜可放大（缩小时间范围）或缩小（放大时间范围）。

还可以单击相关报告的链接。在以下示例中：

- 单击“浏览”，可显示关联的“度量标准详细信息”报告。
- 单击“工程”，可显示选定组件的“组件”报告。
- 单击“可用性”，可显示“可用性”报告。



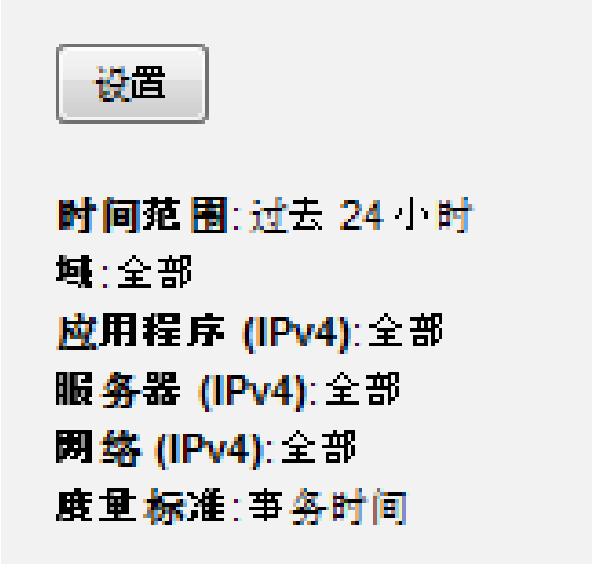
“向我显示”菜单导航

管理控制台顶部的六个选项卡对应于职能角色。每个选项卡以不同的方式呈现数据，以帮助您进行故障排除、分析趋势以进行优化，或查看摘要报告。

在每个选项卡上，使用“向我显示”菜单可更改页面上的数据视图。在“操作”页面上，使用“向我显示”菜单可查看网络、服务器或应用程序视图的数据概览。

更改报告设置

管理控制台在每个报告页面顶部的“设置”按钮下方显示当前页面和报告设置。在以下示例中，管理控制台在视图和报告中显示了 191.168.1.0 网络上所有应用程序、服务器和网络的最近一个小时数据，并包括了所有相关的度量标准。



单击“设置”按钮可更改报告设置：

时间范围

在列表中单击所需的时间范围，然后选择是否要包含排定维护期间收集的数据。根据您选择的时间范围，当前时间和报告中的最新数据之间可能会存在一定的时间差。例如，如果时间范围设置为周，报告分辨率为 60 分钟，您可能会看到多达 55 分钟的时间差。

- 小于或等于 8 小时时，显示 5 分钟增量
- 小于或等于 16 小时时，显示 10 分钟增量
- 小于或等于 24 小时时，显示 15 分钟增量
- 小于或等于一周时，显示 60 分钟增量
- 小于或等于一个月时，显示 6 小时增量

度量标准

单击以选择需要的度量标准或度量标准组。例如，从“突发事件”页面，您可以选择“所有服务器度量标准”或特定服务器的度量标准。

应用程序/服务器/网络组合

选择需要的应用程序、服务器和网络组合：

- 单击“X”按钮清除选定的应用程序、服务器或网络，然后选择其他项。
- 单击“针对所有选择组”，对应用程序、服务器和网络应用来自 CA PC 或 CA NPC 的筛选。要覆盖组筛选，单击“X”按钮，然后单击需要的应用程序、服务器或网络。
- 要搜索应用程序、服务器或网络，请键入相应的名称，然后单击“搜索”。
- 如果您已创建域来分隔重复的 IP 通信量，请选择需要的域。该选项将筛选分配到相应域的服务器和网络列表。默认情况下，对所有服务器和网络应用“默认域”。

使用 CA Multi-Port Monitor 深入查看详细信息

管理控制台与 CA Multi-Port Monitor 集成，可让您查看会话级数据以及导出数据包以进行会话分析，例如在 CA Observer Expert 中。

在管理控制台的“操作”、“突发事件”或“工程”选项卡中，当前报告上下文（包括时间范围、网络、服务器和应用程序设置）已应用到 CA Multi-Port Monitor 中的深入查看视图。

CA Standard Monitor 以 5 分钟粒度在网络级分析 TCP 会话，与此不同，CA Multi-Port Monitor 能够以 1 分钟粒度分析服务器和特定客户端之间的 TCP 会话。此外，CA Multi-Port Monitor 可让您分析 CA Multi-Port Monitor 观测的所有通信的通信量，包括 TCP 和非 TCP 通信量。

为了遵循从管理控制台报告到 CA Multi-Port Monitor 中的默认分析这种故障排除路径，我们建议您首先在管理控制台报告设置中选择一个相对较窄的时间范围，例如一小时。在深入查看 CA Multi-Port Monitor 中的默认视图时，对报告应用的任何筛选（如精简为单个网络、服务器或应用程序的数据）仍然有效，并在您排除故障时可以帮助您定位到正确的网络区域。

遵循这些步骤:

1. 在“操作”、“突发事件”或“工程”选项卡中单击“设置”。

   将打开“设置”对话框。

2. 配置报告设置，然后单击“确定”。

   若要启用深入查看来自动选择观测服务器通信量的逻辑端口，那么必须在管理控制台中配置报告设置，以便选择特定的服务器。

3. 单击“会话分析”。

   如果“会话分析”按钮已禁用，请配置报告设置，以选择 CA Multi-Port Monitor 监视的服务器。

   CA Multi-Port Monitor 将打开“分析菜单”，其中显示了基于报告设置上下文的响应时间度量标准。

   有关使用“分析菜单”的详细信息，请参阅 CA Multi-Port Monitor 产品文档。

   提示：如果您将报告设置配置为显示“所有服务器”，并且为 CA Multi-Port Monitor 配置了多个逻辑端口，则“会话分析”对话框将提示您选择用于观测要分析的服务器通信量的逻辑端口。选择适当的逻辑端口，然后单击“确定”以打开 CA Multi-Port Monitor。

将报告格式从图表更改为表

您可以将报告格式从图表更改为表或详细表，或者将表更改为图表。还可以将某些报告页面从图表更改为大图。

遵循这些步骤:

1. 单击“工程”页面。
2. 单击图表右上角的蓝色齿轮菜单 ( )，然后单击“表”。

   注意：某些图表允许您选择“大图”作为显示格式。
3. 管理控制台以表格格式显示视图。要返回到图表视图，请单击蓝色齿轮菜单 ( )，然后单击“图表”。

解释报告页面和视图中的数据

如果您执行了足够多的观测，并且针对应用程序、服务器、网络和 5 分钟期间的每种组合设置了阈值，管理控制台将使用以下分级之一来分级度量标准：

Acknowledged

表示管理控制台用户确认了突发事件。发生此情况时，管理控制台会将突发事件涵盖的数据标记为“已确认”。管理控制台还会自动将已确认的突发事件将来涵盖的数据也标记为“已确认”。

没有数据

表示没有可用数据。

未分级

*“未分级”性能等级*在管理控制台的“操作”页面上以灰色严重度状态指示，表示以往数据不足（需要两个完整工作日的数据），无法建立阈值；或者观测数不够，未超出最小观测数阈值。

正常

表示度量标准值介于零和“轻微”阈值之间。

轻微

表示度量标准值超出了“轻微”阈值。

重大

表示度量标准值超出了“重大”阈值。

不可用

表示服务器上的应用程序未运行（不可用）。当您在“设置”中单击“所有服务器度量标准”时，会显示该分级。该分级仅适用于管理控制台管理员已向应用程序分配了服务器的用户定义的应用程序。

第 3 章： 使用“操作”页面

此部分包含以下主题：

使用“操作”报告页面

使用“操作”页面可以浏览和排除性能故障。*性能图*把表现最差的网络、服务器和应用程序冒泡到页面顶部。当您单击这些项时，报告焦点将会细化。

通常，最终用户会将以下性能问题报告给运营中心和支持团队：

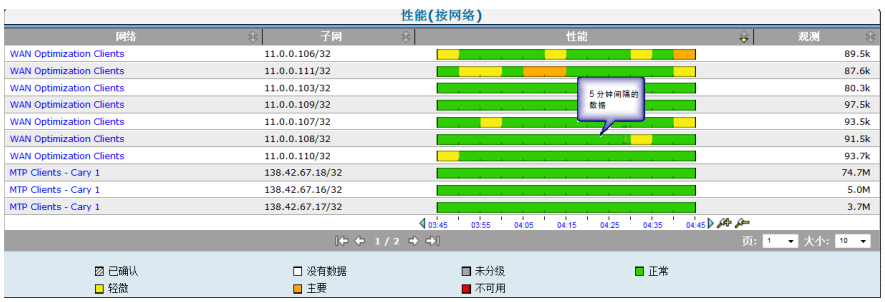
- 应用程序性能问题
- 网络性能问题
- 服务器性能问题

性能图收集有关性能问题的以下数据：

- 出现性能问题的应用程序和服务器的名称
- 用户、本地或远程办公地点的位置和 IP 地址（用于标识网络）
- 首次发生性能问题的时间
- 性能问题的历史记录，以及它是否反复发生
- 与该问题相关的其他性能问题

“操作”页面按网络、服务器或应用程序以彩色编码的水平条形图形式显示性能图，可根据定义的阈值比较各个性能要素。彩色编码对应于数据分级。

性能条上的增量表示五分钟期间的平均值。

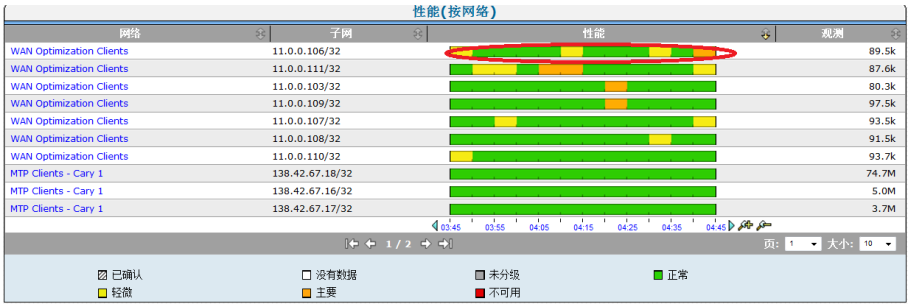


详细信息：

通过电子邮件发送报告页面 (p. 122)
打印报告页面 (p. 123)
更改报告设置 (p. 34)
将报告导出到文件 (p. 121)
导航到“操作”报告页面 (p. 40)

导航到“操作”报告页面

要查看与性能下降相关的网络、服务器和应用程序，请单击视图顶部某个表现最差的组件。



例如，如果单击与 NetQoS LAN 网络对应的性能条，管理控制台将显示网络度量标准以及受影响的服务器和应用程序。要查看未受轻微网络性能下降影响的服务器和应用程序，请单击“已无关”链接将其展开。“已无关”文件夹包括分级为“正常”的组件、“未分级”的组件或不包含任何数据的组件。

请注意，管理控制台在组件的前面显示一个图标，用于表示该组件的类型。以下图标不表示组件的状态：

图标	说明
	网络
	服务器
	应用程序

查看组件的详细信息

可通过查看组件的详细信息来调查性能问题。详细信息包括“相关度量标准”、“受影响度量标准”和“受影响用户”。

遵循这些步骤:

1. 单击“操作”页面。
2. 在“向我显示”菜单中，单击“浏览”。
3. 单击以下选项卡以调查性能并更改性能边界。

相关度量标准

该选项卡显示与问题相关的其他度量标准。使用该选项卡中的信息可帮助诊断问题。针对每个度量标准的图形包含以下内容：

- 相关统计或度量标准平均值。统计有最小值、最大值和平均值；第 50 百分位、第 75 百分位和第 90 百分位；观测数。平均是传入和传出服务器的字节数或数据包数。
- 基准性能，可用来与实际数据进行对比。

受影响度量标准

该选项卡显示受该问题影响的其他度量标准。针对每个度量标准的图形包含以下内容：

- 相关统计或度量标准平均值。统计有最小值、最大值和平均值；第 50 百分位、第 75 百分位和第 90 百分位；观测数。平均是传入和传出服务器的字节数或数据包数。
- 基准性能，可用来与实际数据进行对比。
- 向右箭头和向左箭头，可用于实时前后滚动。
- 网格，可用于使视图居中。

受影响用户

该选项卡显示性能问题影响的用户。对于每个用户，该选项卡显示 IP 地址、子网掩码和主机名。

编辑阈值

该选项卡可让您编辑用于定义性能分级的阈值。有关设置阈值的详细信息，请参阅*《管理员指南》*。

查看基准

基准可帮助您确定性能状态是否正常。管理控制台在基准计算中包括以下参数。可通过设置关联的数据库参数来配置这些参数。

参数	默认	数据库参数	说明
回溯天数系数	7	maxDaysBack	从其开始派生基准的最大回溯天数。默认值为上周。
回溯周数系数	12	maxWeeksBack	从其开始为星期日期派生基准的最大回溯周数。默认值为上一季度。
回溯月数系数	6	maxMonthsBack	从其开始为月份日期派生基准的最大回溯月数。

遵循这些步骤:

1. 单击“操作”页面。
2. 单击一个网络、服务器或应用程序。
3. 通过选择度量标准、网络、应用程序或服务器来缩小选择范围。
4. 在“向我显示”菜单中，单击“浏览”。

   将打开“操作: 度量标准详细信息”页面。
5. 单击“图表设置”。

将打开“图表设置”。

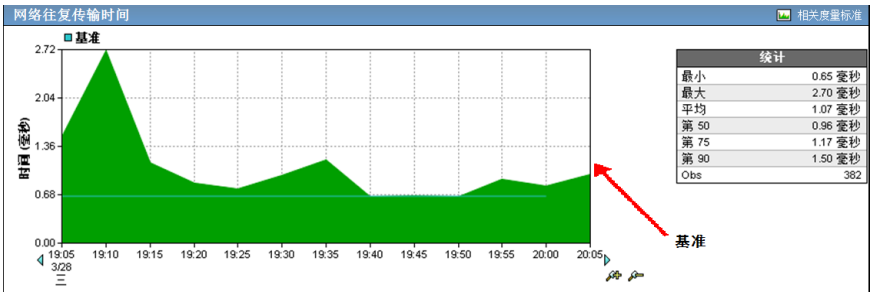
6. 配置“主轴”设置：

   a. 单击“度量标准和基准”

   b. 从“显示”框中选择基准。

   c. 单击“确定”。

   详细信息视图显示了选定的基准。



查看组件的突发事件

“突发事件”页面列出了突发事件的编号、目标、应用程序、严重度、时间和持续时间。

遵循这些步骤:

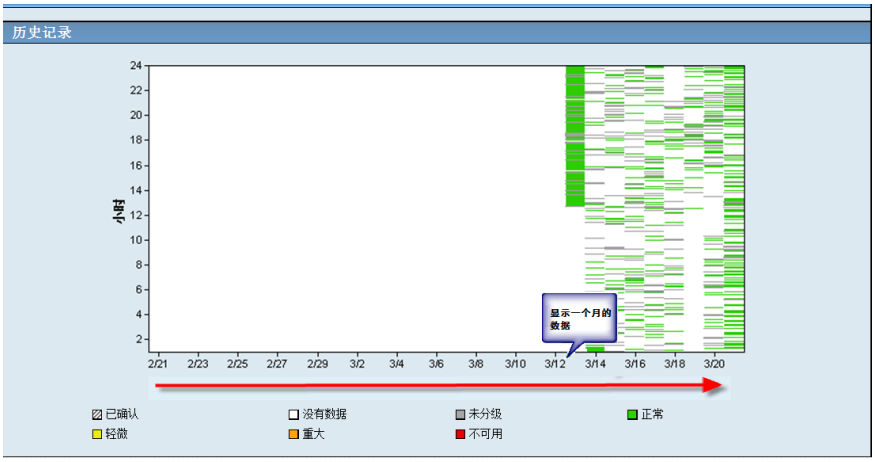
1. 单击“操作”页面。
2. 单击您要查看其突发事件的网络、服务器或应用程序的性能条。
3. 在“向我显示”菜单中单击“突发事件”，以查看选定组件的“突发事件”页面。

查看组件的历史数据

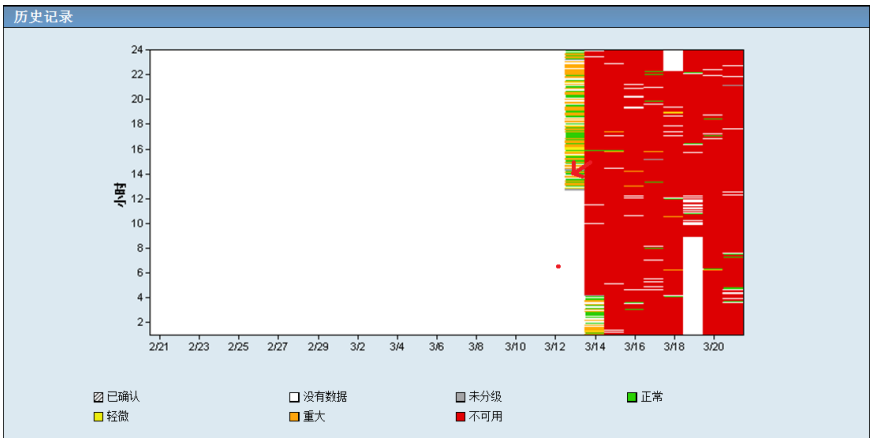
查看网络、服务器或应用程序的历史数据，以分析不同时间的性能行为。

遵循这些步骤:

1. 单击“操作”页面。
2. 单击您要查看其历史数据的网络、服务器或应用程序的性能条。
3. 在“向我显示”菜单中，单击“历史记录”。图表将显示选定项在上个月的数据。



4. 在图表中单击特定的数据点可显示该小时和日期的“已选组件”视图。



对应用程序性能问题进行故障排除

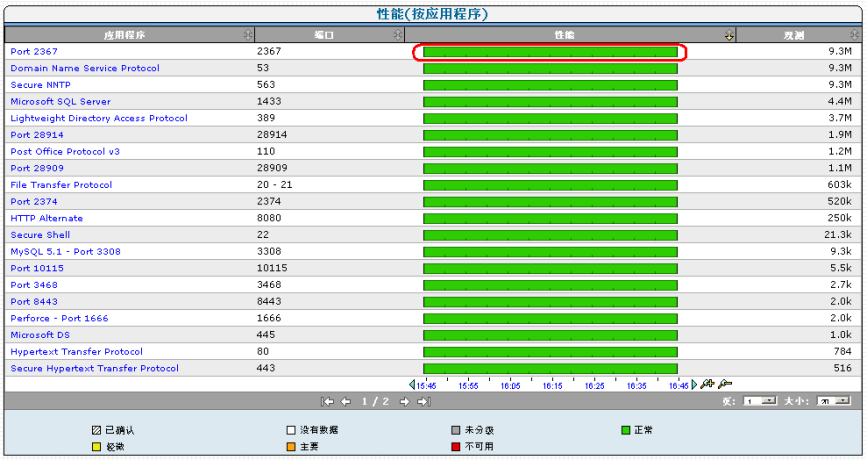
通过使用此过程，可以对某个应用程序出现的性能问题进行故障排除。您可以使用相同的过程来调查网络或服务器出现的问题，只需单击相应链接以按度量标准、网络或服务器缩小选择范围即可。

公司总部的某个用户报告了某个应用程序出现了性能问题。

遵循这些步骤:

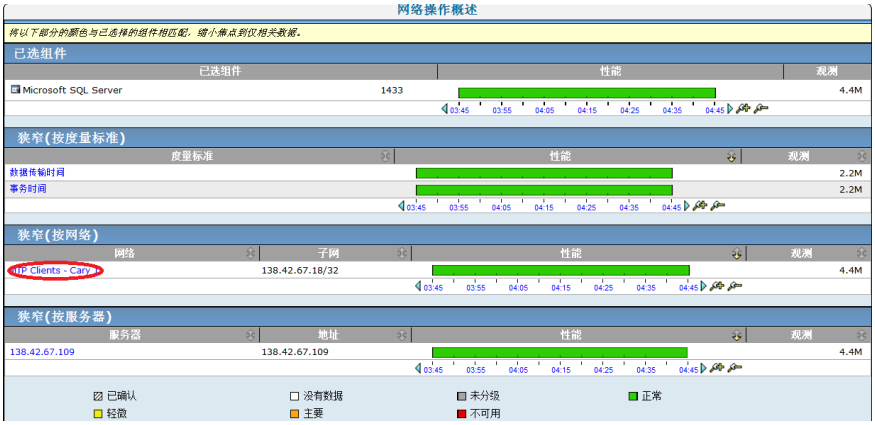
1. 单击“操作”页面。
2. 在“向我显示”菜单中，单击“应用程序”。
3. 确定出现问题的应用程序是否冒泡到了“性能(按应用程序)”列表的顶部。

   如果该应用程序未在列表顶部出现，请选择一个更大的“大小”设置。如果该应用程序未在列表中出现，管理控制台可能无法对它进行监视。
4. 单击应用程序名称旁边的性能条以显示有关该应用程序的详细信息。



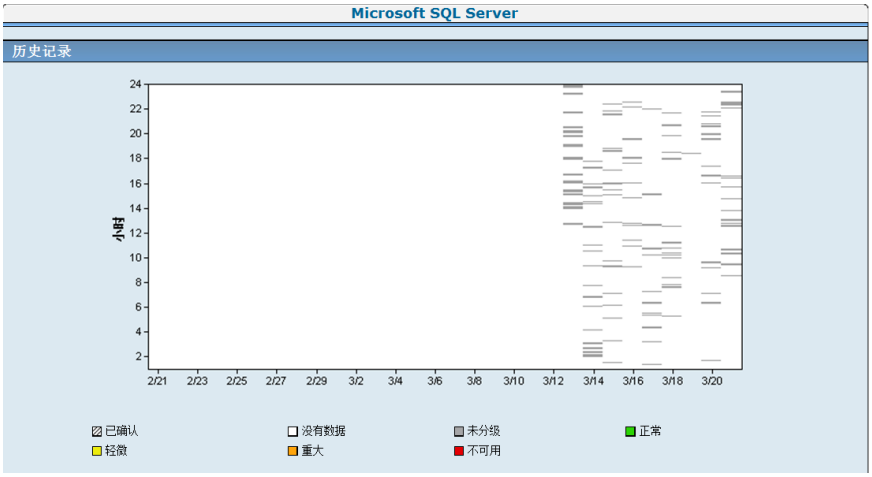
详细信息页面显示了相关的度量标准、网络和服务器，可用于导航到与问题相关的数据。

5. （可选）如果您知道承载应用程序的网络或服务器，请单击相应的性能条来缩小数据范围。



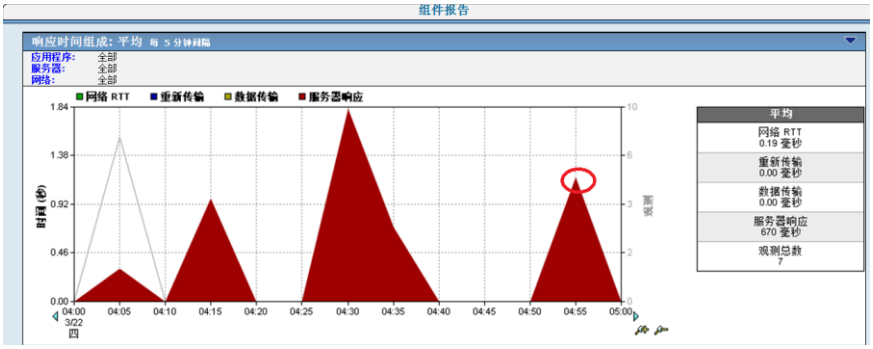
6. 在“向我显示”菜单中，单击“历史记录”。

7. 查看“历史记录”页面上的应用程序历史记录，以识别并记下不可用性能或受影响性能的系统化模式。



8. 在“向我显示”菜单中单击“性能”，然后单击“浏览”开始故障排除。
9. 可通过单击详细信息页面顶部的“工程”链接来执行更全面的故障排除。

10. 查看“组件报告”页面上的“响应时间组成: 平均”视图，以查明所报告问题的发生时间。



11. 识别哪个度量标准是该时间点的性能问题的主要促成因素。如果发生响应时间增大的度量标准是：
    - 服务器响应时间 (SRT)，请针对服务器响应时间增大 (p. 131)执行故障排除
    - 网络往复传输时间 (NRTT)，请针对网络往复传输时间 (NRTT) 增大 (p. 135)执行故障排除
    - 重传延迟，请针对网络往复传输时间 (NRTT) 增大 (p. 135)执行故障排除
    - 数据传输时间，请针对数据传输时间增大 (p. 139)执行故障排除

如果度量标准根据历史时间设置报告的性能可接受，则表示问题可能是用户的计算机造成的。

第 4 章： 使用突发事件页面

此部分包含以下主题：

使用突发事件页面

每当超出某个阈值或不符合运行水平协议 (OLA) 时，管理控制台就会创建突发事件或信息记录。如果管理控制台管理员配置了突发事件响应，管理控制台将自动启动操作来收集详细信息，或将性能问题通知给某人。如果突发事件响应不包括可帮助您解决问题的足够信息，您可以设置故障排除调查以收集更多数据。

“突发事件”页面列出了按顺序编号的突发事件。突发事件报告显示相关性能下降问题的详细信息，使用 24 小时的最大时间窗口，允许您改为包含所需的时间。由于突发事件是根据突发事件创建规则打开和关闭，因此，如果有一组连续发生的突发事件，则可能表示性能长时间都较差。

管理控制台存储历史突发事件记录的期限与存储 5 分钟数据的期限相同。有关更改 5 分钟数据保留期限的信息，请参阅 *《管理员指南》*。

突发事件、突发事件响应和调查

*突发事件*是超出某个性能阈值时创建的信息记录。*阈值*是可接受性能行为的边界，默认情况下，每个应用程序都存在这些边界。管理员可以更改阈值，以提高或降低对性能更改的敏感度。

当超出阈值时，管理控制台将使用分配的顺序案例编号创建突发事件，并在“突发事件”页面上报告这些突发事件。如果管理控制台管理员配置了突发事件响应并已将这些响应与违反的阈值进行关联，管理控制台将启动一个或多个自动响应。如果需要更多的信息来帮助解决问题，可以启动调查对该问题进行故障排除。

如果以下情况属实，管理控制台将关闭突发事件：

- 经过了整整一小时，性能可接受。
- 有问题的服务器进入了维护窗口。
- 突发事件超过了 24 小时。如果问题依然存在，管理控制台将打开新的突发事件。

将管理控制台注册到 CA PC 或 CA NPC 上后，管理控制台检测新的轻微或重大状况时，管理控制台会开出突发事件，CA PC 或 CA NPC 会开立相应的事件。

- 如果触发管理控制台突发事件的“轻微”或“重大”状况显示整整一小时内性能都正常，则管理控制台将关闭该突发事件，CA PC 或 CA NPC 将清除相应的事件。之后，如果又出现了“轻微”或“重大”突发事件状况，则管理控制台将开出新的突发事件，CA PC 或 CA NPC 也将开出相应的事件。
- 如果管理控制台突发事件打开了长达 24 小时，则不管情况如何，管理控制台都将自动关闭该突发事件。如果“轻微”或“重大”突发事件状态仍存在，则管理控制台将开出一个新的突发事件，CA PC 或 CA NPC 也将增加相应事件的计数。否则，在大约 10 分钟的同步延迟之后，CA PC 或 CA NPC 将清除事件。

为了使 CA PC 或 CA NPC 能够清除与服务器脱机的管理控制台突发事件关联的事件，如果管理控制台在整整一小时内对“轻微”或“重大”突发事件状况均报告“没有数据”，则 CA PC 或 CA NPC 将会清除相应的事件。如果管理控制台在服务器恢复联机后检测到新的“轻微”或“重大”状况，管理控制台将开出突发事件，CA PC 或 CA NPC 也将开出相应的事件。

在 CA PC 或 CA NPC 中，如果用户关闭与管理控制台突发事件对应的事件，管理控制台中的突发事件状态将更改为“已确认”。如果突发事件条件显示整整一小时内性能都正常，管理控制台将自动关闭该突发事件。

查看突发事件

管理控制台在“突发事件”页面上显示按顺序编号的网络、服务器和应用程序，并在“管理配置”页面上显示监视设备的突发事件。

突发事件报告显示相关性能下降问题的详细信息，使用 24 小时的最大时间窗口。您可以移动该窗口以包含相关时间。由于突发事件是根据突发事件创建规则来打开和关闭的，一组连续的突发事件可能表示一段较长的时间内性能都不佳。

在 CA PC 或 CA NPC 中注册后，管理控制台会将其突发事件与注册的 CA PC 或 CA NPC 保持同步：

- 如果您在管理控制台中确认了突发事件，相应突发事件的事件状态将在 CA PC 或 CA NPC 中自动更新。
- 如果您在事件管理器中确认了某个管理控制台突发事件导致的事件，则在管理控制台中，相应突发事件的状态将自动更新。

有关 CA PC 或 CA NPC 如何同步管理控制台突发事件的详细信息，请参阅 CA PC 或 CA NPC 产品文档。

注意： 历史突发事件记录的存储期限与 5 分钟数据的存储期限相同。可以在“管理配置”页面上配置保留期限。

按监视设备查看突发事件

监视设备突发事件显示在“管理”页面上。

注意：要查看监视设备突发事件，您的用户帐户必须拥有“管理员”产品权限。有关详细信息，请参阅*《管理员指南》*。

按网络、服务器或应用程序查看突发事件

如果在 5 分钟间隔内超出了网络、服务器或综合度量标准的相应阈值，管理控制台将打开网络或服务器突发事件。例如，如果超出了“数据传输时间”的阈值，管理控制台将为应用程序创建一个网络或服务器突发事件。

遵循这些步骤:

1. 单击“突发事件”页面以显示突发事件的列表。
2. 查看所关注的突发事件：
    1. 在“向我显示”菜单中选择一个选项来显示相应的突发事件。
    2. 单击“设置”以指定想要的突发事件的其他筛选条件，如特定的时间范围或网络。
    3. 通过从以下选项中选择来筛选突发事件列表：

        突发事件状态

        指定所需的一个或多个突发事件状态。

        最小严重度

        指定所需的最小突发事件严重度，以及突发事件状态必须持续的最短时间。请注意，“不可用”是最高严重度。

        查看方式

        指定突发事件列表的显示选项。

查看与突发事件相关的调查

遵循这些步骤:

1. 单击“突发事件”页面。
2. 在“向我显示”菜单中单击“概览”。

    将打开“突发事件列表”。
3. 在突发事件列表中单击一个链接以查看突发事件详细信息。

    将打开突发事件详细信息页面。
4. 在第二个“向我显示”菜单中单击“调查”。

    将显示与该突发事件相关的调查（如果有）。

查看突发事件详细信息

使用“突发事件”列表以深入查看网络或服务器突发事件详细信息。

遵循这些步骤:

1. 单击“突发事件”页面。
2. 如果该页面上的“查看方式”筛选已配置为显示突发事件计数，请单击“突发事件计数”列的性能条来查看突发事件的列表。

   突发事件的列表已根据您的选择进行筛选。
3. 单击一个突发事件编号以查看其突发事件详细信息。

   将打开突发事件详细信息页面。
4. 通过选择度量标准、服务器和应用程序来缩小显示的信息范围。

   管理控制台为突发事件列出以下信息：

   编号

   标识突发事件的唯一编号。

   网络

   如果这是网络相关的突发事件，则该选项表示突发事件的网络源。

   服务器

   如果这是服务器相关的突发事件，则该选项表示突发事件的服务器源。

   严重度

   突发事件的彩色编码分级 (p. 38)。

   时间范围

   突发事件的总持续时间。

   调查

   相关调查的链接。

   Status

   “打开”或“已关闭”。

   已选组件

   让您选择组件以缩小数据范围。

   性能条

   使用彩色编码段来显示发生问题的位置。

   观测

观测数。

浏览突发事件

使用“向我显示”菜单下的“浏览”按钮来查看相关度量标准、受影响度量标准、受影响用户，或者编辑阈值。

遵循这些步骤:

1. 单击“突发事件”页面。
2. 单击“概览”、“应用程序”、“服务器”或“网络”以查看选定组件的突发事件。
3. 单击选定组件以查看突发事件详细信息。

   “浏览”按钮不再是灰显状态。
4. 在“向我显示”菜单中，单击“浏览”。
5. 将显示“浏览”对话框。例如：

   “度量标准”选项卡

   显示相关度量标准

   受影响度量标准

   显示受影响度量标准。

   受影响用户

   显示在指定的时间范围内访问应用程序的客户端 IP 地址的列表。

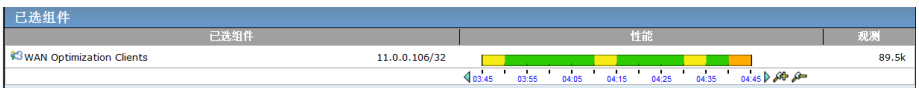
   编辑阈值

   为选定的度量标准编辑性能阈值。

确认突发事件

确认某个突发事件会降低它在报告中的优先级，并指明您已查看该突发事件。您也可以取消确认某个已确认的突发事件，以提高它在报告中的优先级。

当您确认突发事件时，相当于确认了该突发事件自始至终的整个生命周期。在以下示例中，突发事件详细信息页面在时间设置上显示哈希标志，用于表示突发事件从 14：00 到 16：00 为“已确认”状态。



遵循这些步骤:

1. 在突发事件的详细信息页面上单击“确认”。
2. 在“确认”页面上选择一个选项，然后单击“确定”：
   - 确认突发事件：选择该选项会将突发事件标记为已确认。
   - 取消确认突发事件：选择该选项会将突发事件标记为取消确认。

比较突发事件

使用“比较”页面查找可能与整个网络、服务器或应用程序相关的模式，如性能下降的迹象。单击特定网络、服务器或应用程序以浏览详细信息。还可以查看突发事件详细信息，了解是否存在相关的调查。

比较：

网络突发事件

根据类似网络比较与该突发事件有关的网络性能。

服务器突发事件

根据类似服务器比较与该突发事件有关的服务器性能。

遵循这些步骤:

1. 单击“突发事件”页面。
2. 如果该页面上的“查看方式”筛选已配置为显示突发事件计数，请单击“突发事件计数”列的性能条来查看突发事件的列表。

   突发事件的列表已根据您的选择进行筛选。
3. 单击一个突发事件编号以查看其突发事件详细信息。

   将打开突发事件详细信息页面。
4. 单击“向我显示”菜单中的“比较”，将指定时间范围内选定网络或服务器的性能与所有网络或服务器进行比较。

查看突发事件历史记录

查看在过去 30 天发生的、其目标与当前选定突发事件相同的突发事件。

遵循这些步骤:

1. 单击“突发事件”页面。
2. 如果该页面上的“查看方式”筛选已配置为显示突发事件计数，请单击“突发事件计数”列的性能条来查看突发事件的列表。

   突发事件的列表已根据您的选择进行筛选。
3. 单击一个突发事件编号以查看其突发事件详细信息。

   将打开突发事件详细信息页面。
4. 在“向我显示”菜单中，单击“历史记录”。

   将显示“突发事件历史记录”列表。
5. 单击某个突发事件编号以查看其详细信息。

按应用程序查看网络和服务器突发事件

“突发事件(按应用程序)”报告列出了某个应用程序的网络和服务器突发事件。

突发事件报告详细信息显示相关性能下降问题，并使用 24 小时的最大时间窗口。您可以移动该窗口以包含相关时间。由于突发事件是根据突发事件创建规则打开和关闭，因此，如果有一组连续发生的突发事件，则可能表示性能在一段较长的时间内都很差。

要导航到“突发事件(按应用程序)”报告，请在“突发事件”页面上单击“应用程序”。

查看服务器突发事件

“突发事件”页面按应用程序列出服务器突发事件。突发事件报告显示相关性能下降问题的详细信息，并使用 24 小时的最大时间窗口。您可以移动该窗口以包含相关时间。由于突发事件是根据突发事件创建规则打开和关闭的，因此，如果有一组连续发生的突发事件，则可能表示性能在一段较长的时间内都很差

要导航到“服务器突发事件”报告，请在“突发事件”页面上单击“服务器”。

按应用程序查看网络突发事件

“突发事件”页面按应用程序列出网络突发事件。突发事件报告显示相关性能下降问题的详细信息，并使用 24 小时的最大时间窗口。您可以移动该窗口以包含相关时间。由于突发事件是根据突发事件创建规则来打开和关闭的，一组连续的突发事件可能表示一段较长的时间内性能都不佳。

要导航到“网络突发事件”报告，请在“突发事件”页面上单击“网络”。

使用调查报告

*调查*是管理控制台作为突发事件响应的一部分自动启动的操作，或者是具有“管理员”产品权限的用户手动排定或启动的操作。调查可能使用以下类型之一：

调查类型	说明
应用程序连接时间	确定连接到 TCP/IP 应用程序端口所需的时间，这包括服务器使用连接确认作出响应所需的时间。
数据包捕获	对遇到了问题的特定服务器、应用程序端口和网络启用并调查筛选捕获。
通过 SNMP 的性能	调查使用简单网络管理协议 (SNMP) 收集的服务器或路由器的性能相关信息。
Ping 响应时间	度量发送 TCP ping 请求之后，收到 ping 回复所需的时间。
Ping 响应时间与数据包大小	度量收到不同大小的 TCP ping 请求（数据包）的 ping 回复所需的时间。帮助跟踪各种数据包大小时的过度延迟及缺少连接状况。
跟踪路由	记录管理控制台与端点之间的路径和每个跃点，以检测延迟和路由问题。

查看调查

使用“调查报告”可以查看有关某个调查的详细信息，更改报告设置，或删除调查。

遵循这些步骤:

1. 单击“突发事件”页面。
2. 单击“调查”。

   将显示“调查报告”页面。
3. 单击“设置”以筛选突发事件的列表。
4. 单击时间戳链接以查看有关调查结果的详细信息。

启动和排定调查

将调查设置为立即启动，或者在指定的日期和时间启动。

在手动启动调查时，您必须禁用弹出窗口阻止程序，否则调查将无法运行。您启动了一个调查，如果未看到显示调查运行状态的弹出消息，则很可能是弹出窗口阻止程序仍在运行，而您的调查并未运行。

遵循这些步骤:

1. 单击“突发事件”页面。

   在“向我显示”菜单中单击“调查”。
2. 将打开“调查报告”页面。
3. 在“向我显示”菜单中单击“启动”。

   将打开“调查类型”页面。
4. 通过执行以下任务之一来启动或排定调查：
   - 单击您要立即启动的调查类型旁边的“启动”。
   - 单击您要排定的调查类型旁边的“排定”。

   将打开适用于所选调查类型的“设置”页面。有关每个“设置”页面的信息，请参阅以下部分。

应用程序连接时间调查

*应用程序连接时间调查*确定连接到 TCP/IP 应用程序端口所需的时间，这包括服务器使用连接确认作出响应所需的时间。

排定该调查时，您为通知指定的时区也用于排定该调查。

指定以下设置，以启动或排定应用程序连接时间调查：

调查的目标

根据目标类型来指定您要调查的目标，例如服务器。要调查一组目标，请从“目标类型”列表中选择“服务器聚合”。

调查选项

指定以下选项：

调查源

指定要从中启动调查的监视设备。请选择可以与您要调查的服务器或设备进行通信的监视设备。

应用程序

指定要调查的应用程序。

样本

指定调查期间要观测的数据样本数（1 到 10）。一个样本是单个统计度量。

超时(秒)

指定调查记录应用程序超时之前必须经过的秒数（1 到 10）。

通知选项

向指定的电子邮件收件人通知调查结果。请注意，排定调查时使用的是为电子邮件通知指定的时区。

排定

只有在您选择排定该调查时才会显示排定选项。可以排定调查以便在特定日期的特定时间运行，或者排定调查按周或按月运行。

数据包捕获调查

*数据包捕获调查*对遇到问题的特定服务器、应用程序端口和网络执行筛选捕获。

排定该调查时，您为通知指定的时区也用于排定该调查。

指定以下设置，以启动或排定数据包捕获调查：

调查的目标

请指定要调查的服务器。

捕获筛选

指定以下选项：

应用程序

指定您要捕获的应用程序通信量。要捕获目标服务器上的所有应用程序通信量，请单击“全部”。要指定自定义端口范围，请单击“自定义应用程序”并指定开始与结束端口号。

网络

指定您要捕获其目标应用程序通信量的客户端网络。

单击“全部”指定所有客户端网络，或者单击“特定网络”指定某个特定网络，然后单击“网络”链接选择所需的网络。

调查选项

指定以下选项：

捕获期间

指定要捕获数据包的最大时段（30 秒到 30 分钟）。

最大文件大小

为数据包捕获文件指定最大大小（10 MB 到 100 MB）。

每数据包字节数

使用 CA Standard Monitor 捕获数据包时，请指定要捕获的每数据包字节数。选择“仅标头”或“8192 字节”。请注意，“仅标头”将捕获 MAC（第 2 层）、IP（第 3 层）和 TCP（第 4 层）的标头信息。

通过 CA GigaStor 或 CA Multi-Port Monitor 捕获数据包时，该选项不适用。

通知选项

向指定的电子邮件收件人通知调查结果。请注意，排定调查时使用的是为电子邮件通知指定的时区。

排定

只有在您选择排定该调查时才会显示排定选项。可以排定调查以便在特定日期的特定时间运行，或者排定调查按周或按月运行。

通过 SNMP 的性能调查

*通过 SNMP 的性能调查*使用“简单网络管理协议”(SNMP) 查询服务器或路由器以获得性能相关的信息。

排定该调查时，您为通知指定的时区也用于排定该调查。

指定以下设置，以启动或排定通过 SNMP 的性能调查：

调查的目标

根据目标类型来指定您要调查的目标，例如服务器。要调查一组目标，请从“目标类型”列表中选择“服务器聚合”。要对某个路由器进行 SNMP 轮询以获得性能信息，管理控制台管理员必须将该路由器添加为网络设备。有关详细信息，请参阅*《管理员指南》*。

调查选项

指定以下选项：

调查源

指定要从中启动调查的监视设备。请选择可以与您要调查的服务器或设备进行通信的监视设备。

样本期间(秒)

指定计算速率时等待样本的时间（5 到 300 秒）。

重试次数

指定获取响应的尝试次数（0 到 4）。

超时(秒)

指定管理控制台将服务器视为超时之前必须经过的时间（1 到 30 秒）。

通知选项

向指定的电子邮件收件人通知调查结果。请注意，排定调查时使用的是为电子邮件通知指定的时区。

排定

只有在您选择排定该调查时才会显示排定选项。可以排定调查以便在特定日期的特定时间运行，或者排定调查按周或按月运行。

ping 响应时间调查

*Ping 响应时间调查*度量发送一个 TCP ping 请求之后，收到 ping 回复所需的时间。

排定该调查时，您为通知指定的时区也用于排定该调查。

指定以下设置，以启动或排定 Ping 响应时间调查：

调查的目标

根据目标类型来指定您要调查的目标，例如服务器。要调查一组目标，请从“目标类型”列表中选择“服务器聚合”。

调查选项

指定以下选项：

调查源

指定要从中启动调查的监视设备。请选择可以与您要调查的服务器或设备进行通信的监视设备。

数据包大小

选择测试数据包的字节大小（32 到 8192）。

样本

选择调查期间要观测的数据样本数（1 到 10）。一个样本是单个统计度量。

超时(秒)

选择将服务器视为超时之前必须经过的秒数（1 到 10）。

通知选项

向指定的电子邮件收件人通知调查结果。请注意，排定调查时使用的是为电子邮件通知指定的时区。

排定

只有在您选择排定该调查时才会显示排定选项。可以排定调查以便在特定日期的特定时间运行，或者排定调查按周或按月运行。

Ping 响应时间与数据包大小调查

*Ping 响应与数据包大小调查*度量收到不同大小的 TCP ping 请求（数据包）的 ping 回复所需的时间。帮助跟踪各种数据包大小时的过度延迟及缺少连接状况。

Ping 响应时间与数据包大小调查将生成有关最小、最大和平均数据包往复传输时间的报告。与其他类型的调查不同，管理控制台不会自动启动此调查来响应某个突发事件。

排定该调查时，您为通知指定的时区也用于排定该调查。

指定以下设置，以启动或排定 Ping 响应与数据包大小调查：

调查的目标

根据目标类型来指定您要调查的目标，例如服务器。要调查一组目标，请从“目标类型”列表中选择“服务器聚合”。

调查选项

指定以下选项：

调查源

指定要从中启动调查的监视设备。请选择可以与您要调查的服务器或设备进行通信的监视设备。

最大数据包大小

选择要调查的最大数据包大小（512 到 8192 字节）。

样本类型

指定用于检查数据包大小的选项：

- 线性。检查不超过指定的最大数据包大小的每个数据包大小。使用该选项需要提供更多样本。
- 加倍。覆盖样本数较少的范围，以及数据包大小较少的范围。

每个大小的样本

选择每个大小的样本数（1 到 10）。

超时(秒)

选择将服务器视为超时之前必须经过的秒数（1 到 10）。

通知选项

向指定的电子邮件收件人通知调查结果。请注意，排定调查时使用的是为电子邮件通知指定的时区。

排定

只有在您选择排定该调查时才会显示排定选项。可以排定调查以便在特定日期的特定时间运行，或者排定调查按周或按月运行。

跟踪路由调查

*跟踪路由调查*记录管理控制台与端点之间的路径和每个跃点，以检测延迟和路由问题。

排定该调查时，您为通知指定的时区也用于排定该调查。

指定以下设置，以启动或排定跟踪路由调查：

调查的目标

根据目标类型来指定您要调查的目标，例如服务器。要调查一组目标，请从“目标类型”列表中选择“服务器聚合”。

调查选项

指定以下选项：

调查源

指定要从中启动调查的监视设备。请选择可以与您要调查的服务器或设备进行通信的监视设备。

协议

指定用于跟踪路由调查的协议（ICMP 或 TCP）。仅当 QoS 主动地为 ICMP 和给定的 TCP 端口中的某一个指定了更高优先级时，两者之间跟踪路由性能才有所不同。在这种情况下，TCP（如果它同时被网络路由器标记为实际应用程序通信）可能是首选方法。如果允许 ICMP 在给定的体系结构中通过（因为有时出于安全考虑而将它阻止），则通常会使用并接受 ICMP。

数据包大小

指定要调查的数据包大小（32 到 8192 字节）。

重试次数

指定获取响应的尝试次数（1 到 4）。

路由搜索

指定查找所选目标的其他路由的尝试次数（0 到 20）。

超时(秒)

指定将服务器视为超时之前必须经过的秒数（1 到 10）。

通过 SNMP 调查路由器

指定是否对每个网络设备执行 SNMP 查询以获得其性能详细信息。有关将网络设备添加到管理控制台的信息，请参阅*《管理员指南》*。

通知选项

向指定的电子邮件收件人通知调查结果。请注意，排定调查时使用的是为电子邮件通知指定的时区。

排定

只有在您选择排定该调查时才会显示排定选项。可以排定调查以便在特定日期的特定时间运行，或者排定调查按周或按月运行。

删除排定的调查

如果某个手动排定的调查不再有用，可将它删除。删除排定的调查不会删除其调查报告。

遵循这些步骤:

1. 单击“突发事件”页面。
2. 在“向我显示”菜单中单击“调查”>“启动”。

   将打开“调查类型”页面。
3. 展开调查类型以查看排定的调查。
4. 单击您要删除的排定调查旁边的 。

   该调查随即被删除。

第 5 章： 使用管理页面

此部分包含以下主题：

简介

可以在“管理”页面上查看“性能记分卡”和“运行水平协议”(OLA)，以确定应用程序在一段时间内的性能。

OLA 报告可帮助您将工作方向转移到性能改善上。只要在这些方面做出变动，就能看到 OLA 报告结果有所改善。

管理控制台包括两个级别的 OLA 报告。

- 执行报告，其中按应用程序汇总了 OLA 遵从性
- 详细信息报告，其中包括有关 OLA 阈值百分比、结果和观测数的信息

使用性能记分卡

“性能记分卡”显示企业中的应用程序每个月的性能。管理控制台使用以下彩色编码为性能分级：

- 未分级（灰色）
- 正常（绿色）
- 轻微（黄色）
- 重大（橙色）

管理控制台按观测数对性能等级进行排序。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，单击“性能记分卡”。

   将打开“应用程序列表”页面。
3. （可选）单击“设置”来更改报告设置，如筛选选项。
4. 在“应用程序列表”中单击带彩色编码的性能条或单击应用程序名称以按网络查看应用程序详细信息 (p. 69)。

详细信息：

通过电子邮件发送报告页面 (p. 122)
打印报告页面 (p. 123)
将报告导出到文件 (p. 121)

按时间查看应用程序详细信息

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，单击“性能记分卡”。

   将打开“应用程序列表”页面。
3. （可选）单击“设置”来更改报告设置，如筛选选项。
4. 单击应用程序名称或性能链接以查看性能详细信息。
5. 在第三个“向我显示”菜单中单击“时间”，以按时间查看应用程序详细信息。
6. 在“显示方式”列表中选择按“观测数”或按“百分比”显示。
7. 单击 [详细信息]，在“工程”页面上查看关联的“组件”报告。

按网络查看应用程序详细信息

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，单击“性能记分卡”。

   将打开“应用程序列表”页面。
3. （可选）单击“设置”更改报告设置。
4. 单击应用程序名称或性能链接，以获取性能与其对等方不同的网络的详细信息。
5. 在第三个“向我显示”菜单中单击“网络”，以按网络查看应用程序详细信息。
6. 在“显示方式”列表中单击某个选项来筛选列表：
   - 网络和性能
   - 网络和平均值
   - 网络类型和性能
   - 网络类型和平均值
7. 单击 [详细信息]，在“工程”页面上查看“性能(按网络)”报告。

按服务器查看应用程序详细信息

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，单击“性能记分卡”。
3. 在“应用程序列表”页面上，单击“设置”以根据需要更改报告设置。
4. 单击应用程序名称或性能链接，以获取性能与其对等方不同的服务器的详细信息。
5. 在第三个“向我显示”菜单中单击“服务器”，以按服务器查看详细信息。
6. 在“显示方式”列表中，选择显示“服务器和性能”或“服务器和平均值”。
7. 单击 [详细信息]，在“工程”页面上查看“性能(按服务器)”报告。

使用运行水平协议

“运行水平协议”(OLA) 报告可跟踪网络和应用程序最终用户接收的服务的性能，并告诉您达到 OLA 规范的频率。“性能 OLA”和“可用性 OLA”报告可帮助您确定和评估改进工作、优势以及您遇到的问题。

使用“管理”页面上配置的 OLA 定义可以跟踪数据并按时间、网络或服务器显示信息，以识别违反了 OLA 的哪些方面。您可以快速衡量网络是否遵从规范。如果它不遵从规范，请单击“工程”页面上的链接并查看组件视图、性能图或应用程序和服务器可用性时间设置报告，以隔离问题的发生位置。使用“突发事件”页面可以浏览性能问题的起因。

管理控制台管理员可针对性能和可用性设置 OLA。请遵循 OLA 的以下准则：

- 在设置性能 OLA 之前，管理控制台管理员必须定义您的网络类型，因为性能 OLA 按定义的网络类型应用。有关定义网络类型的信息，请参阅 *《管理员指南》*。
- 在设置可用性 OLA 之前，管理控制台管理员必须针对为其设置 OLA 阈值的应用程序和服务器启用可用性监视。有关详细信息，请参阅*《管理员指南》*。

了解运行水平管理

运行水平管理 (OLM) 包括一些约定俗成的主动性方法和过程，确保根据业务优先级，以可接受的成本向 IT 用户提供适当的服务水平。“运行水平协议”(OLA) 报告展示是否符合相应的服务水平。

针对以下度量标准设置 OLA：

- 用于量化数据中心性能的“服务器响应时间”
- 用于量化网络基础架构性能的网络往复传输时间
- 用于捕获应用程序端到端性能的“事务时间”

“管理”页面显示了以下类型的报告：

- “性能 OLA”报告，其中显示您的应用程序是否达到了 OLA 目标。
- “可用性 OLA”报告，其中显示应用程序可用性目标遵从性的大致形势。单击这些摘要报告中的链接可访问每日和每小时详细信息。

有效部署 OLA 涉及定义 OLA、监视遵从性、改善性能、在较低层面细化 OLA 以提高 OLA 遵从意识和性能改善力度的反复过程。

使用管理控制台可以根据静态阈值监视 OLA。在工作时间，您可以监视任务关键型应用程序是否达到了运行水平。在配置 OLA 时，管理控制台管理员应该将排定的维护和其他计划中的非典型使用时段排除在 OLA 监视之外。有关设置 OLA 的信息，请参阅 *《管理员指南》*。

在监视 OLA 时，请将数据中心度量标准和网络度量标准区分开来。每个度量标准并非对每个网络都有意义；例如，在后端应用程序上，您可能不想要看见“网络往复传输时间”。在选择 OLA 阈值时，对当前网络性能使用范围更宽的时间视图可以消除瞬时高峰或低谷。通过禁用某些网络类型来将它们从 OLA 中排除。

查看 OLA 报告

在查看 OLA 报告时，请指定一个有效的时间范围。建议指定以下时间范围：

时间范围	说明
按天	用于短期故障排除，以 IT 部门为重点的详细技术内容
按周	一份摘要，提供有关异常或趋势的附加详细信息；同样以 IT 为重点
按月	涉及业务单位和行政管理的摘要

时间范围	说明
每季度	广泛的运行水平信息及遵从性状态，可用作计划的输入

通常，OLA 违反可归因于以下方面之一：

- 时间；也就是说，一天中的某个特定时间，或一周中的某一天
- 用户组；例如 VPN 用户网络
- 服务器；例如 Web 服务器 2 和 5

使用性能详细描述 OLA 报告

“性能详细描述 OLA”报告包括应用程序名称、OLA 1 和 2 结果、OLA 1 和 2 百分比以及观测数目。在设置性能 OLA 之前，请添加网络类型。性能 OLA 适用于定义的网络类型。

使用性能 OLA 列表

“性能 OLA 列表”显示管理控制台监视的当前应用程序，并提供某个应用程序上个月的遵从性度量标准的特定视图。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，单击“性能详细描述 OLA”。

   将打开“性能 OLA 列表”。
3. 单击应用程序以查看其性能 OLA 详细信息。

   在 OLA 报告中， 表示应用程序达到了配置的性能 OLA， 表示未达到。
4. 如果应用程序达不到 OLA，将会显示红色感叹号。要查看附加信息，请执行以下操作：
   - 单击应用程序的时间链接，查看每小时的详细信息。
   - 单击 查看通过“工程”页面提供的详细信息报告。
5. 单击“显示方式”以按网络或网络类型筛选 OLA 遵从性详细信息。

使用性能详细描述 OLA (按时间) 报告

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，单击“性能详细描述 OLA”。

   将打开“性能 OLA 列表”。
3. 单击应用程序。

   “性能详细描述 OLA (按时间)”报告的默认视图是上个月的“每日视图”。该报告显示上个月每一天的结果，并根据 OLA 定义指定发生违反的日期。
4. （可选）在应用程序的“每日视图”中单击单个日期以导航到“每小时视图”，其中显示了报告的每个小时的特定违反和观测数据。
5. 单击页面顶部的“设置”以选择不同的度量标准来查看应用程序数据。
6. 单击  查看“组件报告”。

使用性能详细描述 OLA (按网络) 报告

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中单击“性能详细描述 OLA”。

   将打开“性能 OLA 列表”。
3. 单击应用程序。
4. 在“向我显示”菜单中单击“网络”。

   “性能详细描述 OLA (按网络)”报告可让您快速识别违反了为应用程序设置的阈值的客户端。该列表显示了按 IP 地址和子网掩码排序的客户端的逻辑组。

   在对应用程序进行故障排除时，可以使用该报告导航到遇到性能问题的客户端或客户端组。
5. 在“显示方式”框中选择“网络”或“网络类型”。

   报告将会刷新，以显示所有条目的违反数据。
6. 单击页面顶部的“设置”以选择不同的度量标准来查看网络数据。
7. 单击  查看“性能(按网络)”报告。

使用性能详细描述 OLA (按服务器) 报告

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，单击“性能详细描述 OLA”。

   将打开“性能 OLA 列表”。
3. 单击应用程序。
4. 在“向我显示”菜单中，单击“服务器”。

   “性能详细描述 OLA (按服务器)”报告显示违反应用程序 OLA 的服务器。使用该报告可以导航到遇到性能问题的一个或多个服务器。
5. 单击页面顶部的“设置”以选择不同的度量标准来查看服务器数据。
6. 单击  查看“性能(按服务器)”报告。

使用性能执行 OLA 报告

“性能执行 OLA”报告显示应用程序名称和指标，让您查看遵从或违反状态。

使用性能执行 OLA 列表

“性能执行 OLA”报告详细程度最低的高度概括性摘要报告。它根据您可以设置的 OLA 条件，着重显示您的 OLA 遵从状态。

遵循这些步骤:

1. 单击“管理”页面。
2. 单击“性能执行 OLA”。

   将打开“性能 OLA 执行列表”。

   在该报告中，  表示应用程序达到了配置的性能 OLA。  表示未达到配置的性能 OLA。
3. 单击一个应用程序以查看详细信息。

使用性能执行 OLA 摘要

“性能执行 OLA 摘要”报告是针对特定应用程序的、详细程度最低的高度概括性摘要报告。它根据您设置的 OLA 条件，着重显示您的 OLA 遵从状态。

遵循这些步骤:

1. 单击“管理”页面。
2. 单击“性能执行 OLA”。

   将打开“性能 OLA 执行列表”。

   在该报告中， ✔ 表示应用程序达到了配置的性能 OLA。 ! 表示未达到配置的性能 OLA。
3. 单击一个应用程序以查看摘要详细信息。
4. 要按时间、网络或服务器查看 OLA 结果的每日视图，请单击  。

使用可用详细信息 OLA 报告

在设置可用性 OLA 之前，请针对您在为其设置 OLA 阈值的应用程序和服务器启用可用性监视。

使用可用性 OLA 列表

“可用性 OLA 列表”显示有关 OLA 定义、正在运行的应用程序和服务器、这些应用程序和服务器是否符合 OLA 条件以及符合此条件的时间百分比的具体信息。在“可用性 OLA 列表”中，可以查看“可用性 OLA 定义每日视图”或“可用性 OLA 定义(按服务器)”报告，以及设置 OLA 条件。

要导航到“可用性 OLA”报告，请单击“管理”页面上的“可用细信息 OLA”。

在这些报告中， ✔ 表示应用程序达到了配置的可用性 OLA， ! 表示未达到。

查看可用性 OLA 定义每日视图

查看和管理用户定义的应用程序的可用性 OLA。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，单击“可用详细信息 OLA”。

   将打开“可用性 OLA 列表”。
3. 单击应用程序链接来查看“可用性 OLA 定义每日视图”。“每日视图”按小时显示应用程序的可用性百分比，并显示停机持续时间。
4. 单击应用程序的时间链接，查看每小时的详细信息。
5. 单击  查看应用程序的“可用性时间设置”报告。

查看可用性 OLA 定义(按服务器)

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，单击“可用详细信息 OLA”。

   将打开“可用性 OLA 列表”。
3. 单击应用程序链接来查看“可用性 OLA 定义每日视图”。
4. 在“向我显示”菜单中，单击“服务器”。

   “可用性 OLA 定义(按服务器)”报告按服务器显示应用程序可用性，包括停机持续时间。
5. 单击  查看“可用性时间设置”报告。

使用可用执行 OLA 报告

“可用性 OLA 执行”报告提供应用程序和服务器对 OLA 条件的遵从性的高度概括性摘要。

使用可用性 OLA 执行列表

“可用性 OLA 执行列表”是一份高度概括性摘要报告，告诉您运行的应用程序和服务器是否符合 OLA 条件。

要导航到“可用性 OLA 执行列表”，请在“管理”页面上单击“可用执行 OLA”。单击应用程序的链接以查看 OLA 定义的摘要报告。

查看可用执行 OLA 摘要

遵循这些步骤:

1. 单击“管理”页面。
2. 单击“可用执行 OLA”。

   将打开“可用性 OLA 执行列表”。
3. 单击服务器链接以查看“可用性 OLA 执行摘要”。

   “摘要”显示了服务器可用性百分比。
4. 单击  在“摘要”报告上查看“每日视图”。

第 6 章： 使用工程页面

使用“工程”页面可以深入查看和报告关于配置的网络、服务器和应用程序的性能度量标准。使用“工程”页面中的“性能”和“可用性”报告，您可以立即识别网络中最慢的应用程序。

此部分包含以下主题：

使用性能图

默认情况下，“性能”报告页面显示在“工程”页面上。性能图以水平条形图的形式显示最慢的网络、服务器和应用程序，显示的数据已按每个应用程序的“事务时间”排序。单击图表中的某个项可查看该项的详细报告。

导航性能报告

在“工程”页面上的“向我显示”菜单中，单击“性能”，然后单击一份性能报告：

网络

显示“性能(按网络)”图，性能最差的网络的详细信息显示在图的顶部。单击一个网络以查看性能详细信息报告。

服务器

显示“性能(按服务器)”图，性能最差的网络的详细信息显示在图的顶部。单击某个服务器以查看性能详细信息报告。

应用程序

显示“性能(按应用程序)”图，性能最差的应用程序的详细信息显示在图的顶部。单击某个应用程序以查看性能详细信息报告。

对于 WAN 优化的应用程序，您可以通过查找网段来查看每个优化的网段的性能。管理控制台将网段追加到应用程序名称上，如 SMTP [客户端]、SMTP [WAN] 和 SMTP [服务器]。

提示：在分析同一个应用程序的已优化和未优化性能数据时，请记住，未优化的应用程序响应时间更快，因为数据来自数据中心的本地用户。

详细信息：

通过电子邮件发送报告页面 (p. 122)
打印报告页面 (p. 123)
更改报告设置 (p. 34)
将报告格式从图表更改为表 (p. 37)
将报告页面导出到 CSV 文件 (p. 121)
将视图导出到 CSV 文件 (p. 121)
将视图导出到 XML 文件 (p. 122)
使用网络图 (p. 80)

使用网络图

网络图显示最慢的网络，显示的数据已按每个应用程序的“事务时间”排序。网络的性能图使用水平条形来显示最慢的网络。

要查看“性能(按网络)”图，请单击“工程”页面，然后依次单击“向我显示”菜单中的“性能”、“网络”。在“性能(按网络)”报告中，单击某个网络以查看详细报告。

网络由转发点和缓冲区组成，而这两者由距离不同的线路进行连接。转发点和缓冲区内部会发生拥塞。当应用程序明显加重了某个网络的负担时，用户就能察觉到性能下降。

网络延迟

使用以下等式量化网络延迟：
[序列化延迟] + [队列延迟] + [路由/交换延迟] + [距离延迟] + [协议延迟] = 网络延迟

其中：

序列化延迟

以一次一位的速率传输一帧所需的时间。

队列延迟

帧在通过网络接口传输之前在网络缓冲区内等待的时间。队列延迟是反映带宽/使用率的一个函数。

路由/交换延迟

网络节点确定帧/数据包的下一跃点并将该帧转发到出站接口所需的时间。可能会受交换路径、节点资源和策略（如 ACL）的影响。

距离延迟

光信号或电信号经过两个端点间的路径所需的时间。

协议延迟

网络相关的通信算法引起的延迟量，例如，载波侦听多址访问/冲突检测（CSMA/CD，属于传统以太网）、载波侦听多址访问/冲突规避 (CSMA/CA)、请求发送/清除待发 (RTS/CTS)（属于无线接入点）或长达 200 毫秒的延迟确认 (TCP)。

报告工作流

遵循这些步骤:

1. 单击“工程”页面。
2. 在“向我显示”菜单中，依次单击“性能”和“网络”。
3. 在“性能(按网络)”表中单击某个网络。
4. 通过单击“组件”并查看“网络往复传输时间”和“重传延迟”报告，可以查看主要指标。单击“会话”并查看“连接建立时间”报告。
5. 通过单击“通信量”并查看“数据量”和“数据速率”报告，可以查看辅助指标。单击“会话”，然后查看“TCP/IP 会话”报告。

使用服务器图

服务器图显示最慢的服务器，显示的数据已按每个应用程序的“事务时间”排序。服务器的性能图使用水平条形来显示最慢的服务器。

要查看“性能(按服务器)”图，请单击“工程”页面，然后依次单击“向我显示”菜单中的“性能”、“服务器”。在“性能(按服务器)”报告中，单击某个服务器以查看详细报告。

性能指标

服务器由以下子系统组成：

- CPU
- 内存
- I/O（网络和磁盘）

当应用程序明显加重了某个子系统的负担时，用户就能察觉到性能下降。

CPU 使用率增大可能表示存在许多事务、大量查询、其他与受监视的应用程序无关的进程、TCP、校验和计算，等等。

内存使用率增大可能表示内存中驻留了大型数据集、用户或会话数增加、进程数增加、无法取消分配内存（内存泄漏），等等。

I/O 增大表示向磁盘或网络的数据写入次数增加、用户或会话数增加、进出磁盘的内存页面数增加，等等。

报告工作流

遵循这些步骤：

1. 单击“工程”页面。
2. 在“向我显示”菜单中单击“性能”>“服务器”。
3. 在“性能(按服务器)”表中单击服务器。
4. 通过单击“组件”并查看“服务器响应时间”报告，可以查看主要指标。单击“会话”并查看“连接建立时间”报告。
5. 通过单击“通信量”并查看“数据量”和“数据速率”报告，可以查看辅助指标。单击“会话”并查看“未实现的 TCP/IP 会话请求”报告和“TCP/IP 会话”报告。

使用应用程序图

在“工程”页面上，“性能(按应用程序)”图使用水平条形显示最慢的应用程序。该报告还显示每个应用程序的观测数目。单击应用程序链接可查看选定应用程序的详细报告。

应用程序通常包含两个部分：

- 运行在一个或多个服务器上的后台程序
- 运行在用户计算机上的客户端

未针对网络传输优化的应用程序可能会导致性能下降；例如，它们可能会在网络中反复对传数据，可能打开多个连续的 TCP 会话而不是一个持久性的 TCP 会话，或者可能为高延迟的 WAN 链路使用较小的应用程序/TCP 窗口大小。

遵循这些步骤:

1. 单击“工程”页面。
2. 在“向我显示”菜单中单击“性能”>“应用程序”。
3. 在“性能(按应用程序)”表中单击某个应用程序。
4. 通过单击“组件”并查看“数据传输时间”报告，可以查看主要指标。单击“响应大小”并查看“数据传输时间(按响应大小)”报告。
5. 通过单击“通信量”并查看“数据量”和“数据速率”报告，可以查看辅助指标。单击“会话”，然后查看“TCP/IP 会话”报告。

查看性能详细信息报告

在“工程”页面上，管理控制台使用 5 分钟数据生成视图，并求这些数据的平均值以生成 15 分钟数据：

- 5 分钟数据可以报告最多 8 个小时。
- 5 分钟数据可以报告最多 24 个小时。

遵循这些步骤:

1. 单击“工程”页面。
2. 单击“向我显示”菜单中的“性能”，然后：
   - 单击“网络”以按网络显示性能图。
   - 单击“服务器”以按服务器显示性能图。
   - 单击“应用程序”以按应用程序显示性能图。

   将显示性能图。
3. 单击性能图中的某项以查看其详细信息报告。

   默认情况下，将显示组件报告。
4. 从第三个“向我显示”菜单中选择要查看的详细信息报告。
   - 组件报告 (p. 84)
   - 通信报告 (p. 91)
   - 会话报告
   - 响应大小报告 (p. 98)
   - QoS 报告 (p. 99)
   - 统计报告 (p. 103)
   - 趋势报告 (p. 105)

   每份性能详细信息报告显示了与该主题相关的视图的集合，该集合的下面显示了摘要报告和组件视图。有关详细信息，请参阅以下各节。

使用组件报告

“组件”详细信息报告显示每个选定应用程序、服务器和网络的度量标准详细信息。

提示：要按特定应用程序、服务器或网络筛选详细信息报告，请单击报告左上角的链接或单击“设置”按钮。

响应时间组成: 平均

“响应时间组成: 平均”报告显示端到端的响应时间，其中堆积了构成总时间的组件：

- 网络 RTT：网络往复传输时间
- 重传：重传时间
- 数据传输：数据传输时间
- 服务器响应：服务器响应时间

该报告显示在报告时段观测到的 TCP 事务的数目。

一个事务可能代表一个请求和一个服务器响应、数据传输的一个期间、一个或多个确认以及观测到的重传数据包引起的延迟。

查找	可能表示
所有值逐渐增大	网络通信量随着时间的推移正常增长
度量出现峰值	进一步调查时出现异常
响应时间的一个组件出现峰值，其他组件保持恒定	进一步调查时出现异常
观测数目增加，同时网络往复传输时间也增大	链路使用过度
数据传输时间较大，网络往复传输时间较小	服务器使用过度
重传延迟较大	数据包丢失
观测数不断增加	应用程序使用率增大
观测数不断增加，服务器响应时间也相应地增大	服务器过载

服务器响应时间

“服务器响应时间”报告显示服务器开始响应某个客户端发出的请求所需的时间。

提示：以表格格式查看“服务器响应时间”数据时，表中的最下面一行列出了每个列的平均/总计统计。但是，平均/总计统计是基于平均值来计算的。例如，“最小值”列的平均/总计值实际上是“平均值”列中的最小值 - 而不是“最小值”列的平均值。

服务器速度、应用程序设计和请求数量可能会影响该值。

查找	可能表示
服务器响应时间增大，同时观测数增加，然后，发现在同一时段以下度量标准增大： ■ 数据量 ■ 数据传输时间 ■ 打开的 TCP 会话	服务器过载的迹象明显。
服务器连接时间增大，同时观测数减少	检查此服务器上运行的其他应用程序是否受管理控制台的监视。如果是，请检查因这些应用程序的“服务器响应时间”增大而增加的观测，以标识服务器上造成问题的应用程序进程。
服务器上没有其他受监视的应用程序，观测数减少，同时服务器响应时间增大	另一个应用程序可能正在影响服务器响应时间；例如，服务器上运行的备份程序可能会增大并发运行的应用程序的响应时间。检查一段时间内服务器响应时间增大和观测数减少的模式，如有必要，请联系其他运营团队或使用网络协议分析器来确定是服务器上运行的哪个应用程序导致了服务器响应时间增大。

查找	可能表示
服务器响应时间较大	服务器存在以下问题之一： ■ 处理能力不足 ■ 可用内存不足 ■ 硬盘驱动器速度慢 ■ 进程挂起 ■ 错误地配置了 NIC 设置 ■ 存在写入性能较差的应用程序，例如，数据库查找使用了大型查询或不当的索引
服务器响应时间不断变化	较大的周期性数据量。
应用程序发送了一条响应，表示在收到请求后已立即开始工作，且服务器响应时间始终较小	用户体验到的实际延迟在数据传输速率组成中体现。

数据传输时间

“数据传输时间”报告显示将一个完整响应从初始数据包传输到最终数据包所需的度量时间。如果发送的数据比 TCP 窗口中填充的数据多，则数据传输时间不包括初始的服务器响应时间，而仅包含网络往复传输时间。

影响此时间的因素为响应大小、可用带宽、距离造成的网络延迟、某些服务器处理、往复传输次数等交互，以及应用程序和网络之间单个数据包大小。

“数据传输时间”与传送所有数据所需的网络往复传输次数以及每次往复传输的延迟有关。

查找	可能表示
数据传输时间增加	以下情况之一： ■ 应用程序写入性能较差 ■ TCP/IP 传输窗口设置得不够大，服务器无法发送连续的信息流 将“数据传输时间”的明显增大与数据量关联，以确定这种增大是由网络中传输的数据量增加造成的，还是另有其他问题。
不同子网的“数据传输时间”不同	区域可用的带宽不足、某些区域需要重传，以及应用程序的使用方式不同。

重传延迟

重传延迟是由需要重传的数据包导致的网络往复传输时间的额外延迟。

显示的数据是基于所有观测的平均值，而不是某个事务的实际重传时间。假设总共有五个事务，其中四个不需要重传，另一个存在 5 秒重传延迟，则视图将显示 1 秒重传延迟。

管理控制台通过从临近服务器的监视设备有利位置观测网络中的重复数据包来计算“重传延迟”。监视设备可以观测到由于网络路径中服务器->客户端方向上发生数据丢失而导致服务器重传的数据包。“重传延迟”中包括这些观测。但当客户端->服务器方向（如在到达服务器之前的网络路径）发生数据丢失时，监视设备无法观测到此类数据包丢失，因此该延迟不会包含在“重传延迟”度量标准中。管理控制台在包括服务器响应和客户端确认的“网络往复传输时间”度量标准中包含这种关联的重传延迟。未观测到的重传延迟造成的客户端确认延迟增大了 NRTT 值。该度量标准不能反映由于 TCP 拥塞而导致数据传输时间延长所带来的影响。

重传可能会导致指定会话的事务时间有所降低，但线路上的字节速度保持不变，除非路径发生了更改或拥塞有所增加。

查找	可能表示
“重传延迟”随着观测数的增加而增大	网络可能无法处理较高的负载。更改缓冲区分配或路由策略可能会缓解短期高峰。
“重传延迟”以一致的模式变化	区域链路出现问题。将较高的重传期间与其他信息源关联，以确定在那些时间网络中还发生了什么问题。如果特定子网的“重传延迟”占“网络往复传输时间”延迟的比率高于其他区域，则表示该区域的链路可能出现了问题。如果您怀疑特定网络由于重传而发生过度延迟，请查看有问题的网络的“重传延迟”，并将它与所有网络的平均“重传延迟”进行对比。
网络的“重传延迟”高于所有网络的平均值	在无线环境中这是正常行为。
“重传延迟”一贯较高	网络无法承载所需的负载，或者设备可能发生故障。

值较大	由网络拥塞、负载平衡配置不当、存在冗余路径或路由以及网络存在错误状态导致的已丢弃数据包。

网络往复传输时间

“网络往复传输时间”是指数据包在网络上的服务器和客户端之间往复传输所花的时间（不包括重传造成的延迟）。

计算该值时，不包括应用程序和服务器处理时间。管理控制台将通过查找所有应用程序通信量的 TCP 确认来连续细化“网络往复传输时间”（而不仅是连接建立时间），以构建最精确的模型。

使用“网络连接时间”作为载波延迟的基准，并与 NRTT 时间进行比较。

查找	可能表示
NRTT 随着观测数的增加而增大	客户端主机与服务器之间的带宽不足，无法处理应用程序传输的数据量。如果 NRTT 不随着观测数的增加而增大，则可能表示： ■ 另一个应用程序正在消耗远程客户端主机与应用程序服务器之间的可用带宽。 ■ 运营商网络已切换到受保护路径或备用路径。 ■ 网络中存在某种错误状况。
观测数随着 NRTT 的增大而增加	延迟增大的根源。查看“数据量”和 TCP 会话视图，以确定数据和/或 TCP 会话数是否相应地增加。
观测数随着 NRTT 的增大而减少	监视设备与远程客户端之间的其他受监视应用程序可能是带宽明显减少的原因。
在比较同一办公地点（例如同一栋建筑物）中的子网时，应该会观测到同一应用程序的 NRTT 存在最小差异	大于 10 ms 的差异可能是以下原因之一造成的： ■ LAN 体系结构出现了问题 ■ 不正确地配置了交换机或 NIC 端口设置 ■ 网络中存在错误状况 ■ LAN 中物理路径的使用率存在差异

查找	可能表示
远程办公室中与服务器之间距离不同，并通过不同服务器体验的 WAN 链路进行操作的用户遇到不同的延迟和 NRTT	已提供带宽、链路使用模式以及访问技术；例如，ATM 与 IP VPN。

有效网络往复传输时间

“有效往复传输时间”包括“网络往复传输时间”，以及单个事务重传导致的延迟。

该度量标准十分有用，因为它反映了用户实际遇到的延迟。“管理员”可为此度量标准设置一个突发事件阈值，以检测网络中由于重传而出现的性能下降。

与“网络往复传输时间”相比，“有效往复传输时间”更能体现最终用户的网络体验，，因为后者同时包括了“网络往复传输时间”和“重传延迟”。将它与“网络往复传输时间”和“重传延迟”进行比较，以了解每个组件如何相互影响。

通信报告

“工程”页面上网络、服务器和应用程序的“通信”详细信息报告包括以下度量标准：

- 响应时间组成: 平均
- 数据量(以字节为单位)
- 数据量(以数据包为单位)
- 数据速率(比特数/秒)
- 数据速率(数据包/秒)

提示：要按特定应用程序、服务器或网络筛选详细信息报告，请单击报告左上角的链接或单击“设置”按钮。

响应时间组成: 平均

“响应时间组成: 平均”报告显示端到端的响应时间，其中堆积了构成总时间的组件：

- 网络 RTT：网络往复传输时间
- 重传：重传时间
- 数据传输：数据传输时间
- 服务器响应：服务器响应时间

该报告显示在报告时段观测到的 TCP 事务的数目。

一个事务可能代表一个请求和一个服务器响应、数据传输的一个期间、一个或多个确认以及观测到的重传数据包引起的延迟。

查找	可能表示
所有值逐渐增大	网络通信量随着时间的推移正常增长
度量出现峰值	进一步调查时出现异常
响应时间的一个组件出现峰值，其他组件保持恒定	进一步调查时出现异常
观测数目增加，同时网络往复传输时间也增大	链路使用过度
数据传输时间较大，网络往复传输时间较小	服务器使用过度
重传延迟较大	数据包丢失
观测数不断增加	应用程序使用率增大
观测数不断增加，服务器响应时间也相应地增大	服务器过载

数据量(以字节为单位)

“数据量(以字节为单位)”表示在网络上观测到的应用程序层字节总数。

“数据量”报告可以显示高数据传输速率的影响。调查异乎寻常的高数据传输量是否为“网络往复传输时间”升高的原因。

使用该报告来实现以下目的：

- 标识过大的通信量在网络上造成的异常。
- 消除过大的通信量，从而排解这个可能导致性能问题的原因。
- 确定某个特定应用程序、应用程序组或网络的峰值使用情况，以进行容量计划。

数据量(以数据包为单位)

“数据量(以数据包为单位)”表示在受监视网络上观测到的数据包总数。该报告包括零字节数据包，例如 TCP 确认。

将该视图与“数据量”视图结合使用可以了解遍历网络的平均数据包大小。在标识问题区域或攻击时，此方法十分有用，因为出现许多的小数据包可能表示发生了拒绝服务攻击。

数据速率(比特数/秒)

“数据速率(比特数/秒)”显示在指定的时段内的数据速率（以比特数/秒为单位，即字节数/秒乘 8）。

由于该视图会比较传入和传出服务器的数据通信的速率，因此使用该视图可以计划服务器上的容量。

查找	可能表示
比特率较高	子网过载
比特率较低	网络或应用程序问题

数据速率(数据包/秒)

“数据速率(数据包/秒)”显示指定时段内的数据速率（以数据包/秒为单位）。

查找	可能表示
数据包速率较高	路由器、交换机和防火墙的压力较大，导致数据包丢弃数过大
数据包速率短期较高	可通过在受影响的设备中分配足够的缓冲区空间来缓解。在增大缓冲区容量时请保持谨慎，因为这可能会负面地影响延迟敏感型应用程序。丢弃语音包比在缓冲区中延迟语音包更好。
数据包速率持续偏高	可能需要升级设备容量。
与路由器、交换机和防火墙一样，监视设备可能会丢弃短期内数据包速率较高的数据包。	SPAN 端口可能在丢弃数据包。
数据包速率异常地低	网络问题。
数据包速率较高，同时比特率较低	安全攻击。

会话报告

使用“TCP/IP 会话报告”可以查找与无响应会话数和拒绝会话数相关的明显应用程序和服务器问题，以及唯一会话数和这些唯一会话长度的一般调查。该报告不包括来自任何 Web 应用程序的 HTTP 会话。

提示：要按特定应用程序、服务器或网络筛选详细信息报告，请单击报告左上角的链接或单击“设置”按钮。

响应时间组成: 平均

“响应时间组成: 平均”报告显示端到端的响应时间，其中堆积了构成总时间的组件：

- 网络 RTT：网络往复传输时间
- 重传：重传时间
- 数据传输：数据传输时间
- 服务器响应：服务器响应时间

该报告显示在报告时段观测到的 TCP 事务的数目。

一个事务可能代表一个请求和一个服务器响应、数据传输的一个期间、一个或多个确认以及观测到的重传数据包引起的延迟。

查找	可能表示
所有值逐渐增大	网络通信量随着时间的推移正常增长
度量出现峰值	进一步调查时出现异常
响应时间的一个组件出现峰值，其他组件保持恒定	进一步调查时出现异常
观测数目增加，同时网络往复传输时间也增大	链路使用过度
数据传输时间较大，网络往复传输时间较小	服务器使用过度
重传延迟较大	数据包丢失
观测数不断增加	应用程序使用率增大
观测数不断增加，服务器响应时间也相应地增大	服务器过载

连接建立时间

“连接建立时间”是在开始数据传输之前，先在客户端与服务器之间建立 TCP 会话所需的时间。该视图的网络组件应该大致与“有效往复传输时间”相同。

分别查看“连接建立时间”的两个组件：

- “服务器连接时间”(SCT) 是从收到客户端发出的初始 SYN 数据包，到服务器发出第一个 SYN/ACK 所需的时间。
- “网络连接时间”(NCT) 是从服务器发送 SYN/ACK，到收到完成三次握手的 ACK 所需的时间。

查找	可能表示
连接建立时间远远超过 SCT 和 NCT	可能是由服务器或 LAN 问题造成的。 ■ 将“连接建立时间”与“网络往复传输时间”、“重传”和“服务器设置时间”进行比较，以确定这些视图是否显示类似的模式。通常，“连接建立时间”和“网络往复传输时间”会同时增大，不过这种增大不是线性的。 ■ 如果 NRTT 和“数据传输时间”增大，而“连接建立时间”保持恒定，则可能表示服务器到客户端的方向出现了数据丢失。在客户端网络上使用探查器来查看重传，便可以证实是否存在数据丢失。
连接建立时间远远超过 SCT 和 NCT	■ 如果出现与“网络往复传输时间”峰值关联的“连接建立时间”峰值，则表示由于通信量增大、带宽不足、网络出错而使网络中发生了延迟，或者由于运营商切换到了备用路径而导致延迟增加。 ■ 如果仅仅是出现了“连接建立时间”峰值，则可能表示服务器由于 CPU 过载或超出了 TCP/IP 会话限制而面临着较大的压力。

TCP/IP 会话

“TCP/IP 会话报告”显示客户端与服务器之间的唯一连接数，并显示状态为“打开”、“完成”和“已到期”的 TCP/IP 会话。

管理控制台计算 5 分钟监视期间的状态为“已到期”和“完成”的 TCP/IP 会话。“打开的会话”是监视期间结束时仍处于打开状态的会话数。在后续的报告间隔期间，打开的会话的状态可能会变为“已到期”或“完成”。如果在 15 分钟内检测不到任何数据包，管理控制台就会将会话分类为“已到期”。

查找	可能表示
存在多个未完成的已到期的会话。	如果有过多的已到期的会话保持为打开状态，则可能会导致服务器挂起。服务器只能支持最大的同时连接数。

未实现的 TCP/IP 会话请求

“未实现的 TCP/IP 会话请求”表示客户端与服务器之间的未成功的唯一连接数，包括：

- 拒绝的会话。在三次握手期间，如果服务器显式拒绝了某个连接请求，则就会出现*拒绝的会话*。
- 无响应的会话。如果发出了连接请求，但服务器从未响应，则就会出现*无响应的会话*。

查找	可能表示
拒绝的会话数极多	启动的命令加重了一个或多个服务器的压力。 ■ 可能由于正常系统请求或恶意攻击的原因，使得服务器过于繁忙。 ■ 服务器上运行的应用程序许可可能超出了允许的最大用户或会话数。

TCP/IP 会话时间

“TCP/IP 会话时间”显示每个用户会话的持续时间。

查找	可能表示
相同的用户建立了许多短会话	连接池可能会给应用程序带来好处。
会话较长，并且通信量较少	应用程序可能在不必要地保持会话的打开状态。
一周中出现了服务器使用高峰，因此造成了问题	在过去数周，本已增加的打开会话数还在不断增加。检查下一部分介绍的“趋势”视图。

响应大小报告

“响应时间”是根据传输响应大小计算得出的“数据传输时间”的一个度量。不包括“连接建立时间”。

将传输不同大小的响应花费的时间进行比较，可让您了解性能问题是与应用程序还是网络相关。

提示：要按特定应用程序、服务器或网络筛选详细信息报告，请单击报告左上角的链接或单击“设置”按钮。

响应时间组成: 平均

如果您在此视图上观测到应用程序响应时间和“网络往复传输时间”较高，在“通信量”视图上观测到数据量和数据传输速率较高，则“响应大小”可能是性能较慢的促成因素。如果“服务器响应时间”的比率较高，则也非常有必要查看“响应大小”。

详细信息：

响应时间组成: 平均 (p. 85)

数据传输时间(按响应大小)

该报告按响应大小显示平均数据传输时间。通常，数据大小越大，传输时间就越长。

查找	可能表示
有限或特定的响应大小。	特定的事务类型正在导致端到端响应时间变慢。
较大响应的数据量。	使用“数据传输时间(按响应大小)”视图来确定较大响应的数据量，该数据量可能正在导致网络延迟。
该视图中与每个响应大小对应的灰色观测计数行表示每个大小的响应数目。	观测计数可能表示应用程序设计存在问题，例如，某个应用程序使用较小数据量的数据传输做出响应，而没有使用较大的数据传输。

平均数据传输时间(大)

“平均数据传输时间”报告按响应大小（小、中和大，以 KB 为单位）显示平均数据传输时间。

在这些视图中查找以下内容：

- 比较某个响应大小在一段时间内的响应时间，以指明应用程序响应时间的变化是否是由返回数据量的变化而引起的。如果每个响应大小的响应时间相当均衡，但是应用程序运行较慢，则问题可能是用户行为的变化造成的；例如，用户可能在请求更多的较大型对象。使用灰色观测行来确定有多少个事务属于每个大小类别。
- 相对响应时间表明应用程序是否正在等待分析请求或者传输响应。

QoS 报告

如果出现较大的通信量和较大的数据传输速率，并且给定响应大小的响应时间较慢，则表示您可能需要查阅“服务质量”报告。该报告还包括“用户”视图中应用程序的特定用户的详细信息。

提示：要按特定应用程序、服务器或网络筛选详细信息报告，请单击报告左上角的链接或单击“设置”按钮。

响应时间组成: 平均

“响应时间组成: 平均”报告显示端到端的响应时间，其中堆积了构成总时间的组件：

- 网络 RTT：网络往复传输时间
- 重传：重传时间
- 数据传输：数据传输时间
- 服务器响应：服务器响应时间

该报告显示在报告时段观测到的 TCP 事务的数目。

一个事务可能代表一个请求和一个服务器响应、数据传输的一个期间、一个或多个确认以及观测到的重传数据包引起的延迟。

查找	可能表示
所有值逐渐增大	网络通信量随着时间的推移正常增长
度量出现峰值	进一步调查时出现异常
响应时间的一个组件出现峰值，其他组件保持恒定	进一步调查时出现异常
观测数目增加，同时网络往复传输时间也增大	链路使用过度
数据传输时间较大，网络往复传输时间较小	服务器使用过度
重传延迟较大	数据包丢失
观测数不断增加	应用程序使用率增大
观测数不断增加，服务器响应时间也相应地增大	服务器过载

详细信息：

响应时间组成: 平均 (p. 85)

用户

“用户”视图显示给定的时段内，受监视网络中的唯一 IP 地址和/或子网的数目。

查找访问服务器的较大并发用户数。

数据包丢失百分比

“数据包丢失百分比”视图显示被监视网络上丢失的数据所占的百分比，以及用“数据包数/秒”表示的丢失速率。

监视设备通过从临近服务器的有利位置观测网络中的重传数据占总数据的比率来计算数据包丢失百分比。监视设备可以观测到由于网络路径中服务器->客户端方向上发生数据丢失而导致服务器重传的数据包。但当客户端->服务器方向（如到达服务器之前的网络路径上）发生数据丢失时，监视设备无法观测到此类数据包丢失，因此该延迟不会包含在“数据包丢失百分比”中。

在该视图中查找以下内容。

查找	可能表示
大于 1% 的并发值。	数据丢失较多。
该视图仅显示数据包丢失，而数据表同时显示数据包和字节丢失。	数据包丢失会导致数据重传，而这又会导致 TCP 减小窗口大小，从而使后续数据包的传输时间变慢。重传的数据包加大了网络基础架构的负载。重传的字节数表明重传的数据占用的带宽量。

用户正常输出

“用户正常输出”视图用于捕获客户体验信息。其中显示了传输的正常字节数（减去重传字节数）除以传输这些信息所需的时间后得到的值。

当您从 Web 下载数据时，浏览器通常会在您下载文件时计算吞吐量。吞吐量是将传输字节数除以活动期间得到的值。通常，您可以使用该吞吐量值来衡量网络连接的有效性，以及查看计算得出的“用户正常输出”，该值从吞吐量中减去了重传字节数，因为重传字节数会人为地提高吞吐量。

如果您有 100 kbps 的吞吐量度量，但一半的下载包括重传，用户正常输出为 50 kbps；因此，真正有效的只有一半吞吐量。

仅在活动传输期间计算用户正常输出和吞吐量。监视设备计算 5 分钟间隔内的平均通信量速率。大部分时间可能处于静态模式。用户正常输出/吞吐量和通信量速率间几乎没有关系。

为了说明这一点，可以考虑以下情形。如果 5 分钟间隔内的唯一传输为下载 50 KB 文档，在 1 秒内完成而且没有重传，则存在以下度量标准：

- 用户正常输出和吞吐量为 400 kbps，其按以下方式计算：

  50 KB * （8 比特数/字节）/1 秒 = 400 kbps
- 通信量速率为 1.3 kbps，其按以下方式计算：

  50 KB * （8 比特数/字节）/300 秒 = 1.3 kbps

仅在数据传输量比较大以及用于批量传输时，用户正常输出才有用，而对交互式事务没有意义。除包含重传数据包外，吞吐量的计算公式与用户正常输出的计算公式相同（字节数除以数据传输时间）。吞吐量总是大于或等于用户正常输出。

查找	可能表示
用户正常输出中的谷值	网络拥塞。仅在正在传输通信量时，才会将用户正常输出用作网络度量标准。一些字节（无论传输快慢）可能不起作用。
较差的正常输出	数据传输时间会受较差的服务器或应用程序性能限制。

详细信息：

吞吐量 (p. 26)

每用户综合速率

“每用户综合速率”视图显示传输的数据量除以时间间隔以及除以该间隔内唯一用户数所得到的结果。

“每用户综合速率”视图受网络上使用的地址空间影响。使用 A 或 B 类地址时，“每用户综合速率”视图可显示单个子网而不是单个客户端的结果。使用 C 类地址时则与此不同，“每用户综合速率”视图反映的是每个客户端的结果。

使用此视图可以：

- 帮助预测新用户对应用程序产生的影响。
- 通过部署前测试来确定不同网络链路上的预期应用程序负载。

统计报告

“统计”报告页面显示响应时间的变化。使用此报告页面可进行影响分析。“响应时间组成: 平均”视图显示总响应时间。“响应时间组成: 标准偏差”视图显示响应时间度量中存在的变化量。

提示：要按特定应用程序、服务器或网络筛选详细信息报告，请单击报告左上角的链接或单击“设置”按钮。

响应时间组成: 平均

“响应时间组成: 平均”报告显示端到端的响应时间，其中堆积了构成总时间的组件：

- 网络 RTT：网络往复传输时间
- 重传：重传时间
- 数据传输：数据传输时间
- 服务器响应：服务器响应时间

该报告显示在报告时段观测到的 TCP 事务的数目。

一个事务可能代表一个请求和一个服务器响应、数据传输的一个期间、一个或多个确认以及观测到的重传数据包引起的延迟。

查找	可能表示
所有值逐渐增大	网络通信量随着时间的推移正常增长
度量出现峰值	进一步调查时出现异常

响应时间的一个组件出现峰值，其他组件保持恒定	进一步调查时出现异常
观测数目增加，同时网络往复传输时间也增大	链路使用过度
数据传输时间较大，网络往复传输时间较小	服务器使用过度
重传延迟较大	数据包丢失
观测数不断增加	应用程序使用率增大
观测数不断增加，服务器响应时间也相应地增大	服务器过载

响应时间组成: 标准偏差

“响应时间组成: 标准偏差”度量标准量化响应时间度量中存在的变化量。

查找	可能表示
所有用户具有类似的行为（较低的标准偏差），且变化程度随着时间的推移发生变化。	平均响应时间不错但标准偏差较高的应用程序在存在大量用户时执行效果可能会不佳。
标准偏差中的常规模式。	随着时间的推移，应用程序的使用或客户端组合将发生改变。连接网络的链路中的变化可能会导致网络时间存在较高的标准偏差。只有几个样本可用时的变化会高于有大量数据点可用时的变化。
持续的高标准偏差。	值过于分散，很难进行有意义的分析；例如，比较既包括快速应用程序又包括慢速应用程序的数据时，得到的应用程序之间的用户体验偏差会很大。这种情况下，应按应用程序筛选数据，以便得到更有意义的结果。持续的高标准偏差也可能表示应用程序行为存在巨大变化。

百分位

使用“工程”页面上的“服务器响应时间百分位”、“数据传输时间百分位”、“重传延迟时间百分位”以及“网络往复传输时间百分位”视图，可以确定受特定问题影响的事务的百分比。如果网络问题仅出现在第 90 百分位视图中，则仅最慢的事务受该问题影响。如果该问题出现在第 75 或第 50 百分位视图中，则该问题影响较大部分的事务。

在大多数用户体验到正常的响应时间的同时，可能会有极少数用户抱怨应用程序响应慢。“网络往复传输时间百分位”视图也许能表明这种情况 - 第 90 百分位线远高于第 75 或第 50 百分位线。您可能会看到大约 10% 的事务性能较差，而余下的 90% 性能良好。位于远程站点的用户或执行特定类型事务的用户可能具有较差的体验。

如果第 90、75 和 50 百分位线彼此靠得非常近，则可以得出结论：无论位于何处、正在执行何种事务类型，大多数用户看到的结果都非常接近，没有太大的偏差。

趋势报告

“工程”页面上的“趋势”视图显示特定时段内端到端的平均响应时间数据。报告标题指明了间隔的粒度。

提示：要按特定应用程序、服务器或网络筛选详细信息报告，请单击报告左上角的链接或单击“设置”按钮。

趋势报告	间隔
一小时响应时间组成: 平均	5 分钟
八小时响应时间组成: 平均	5 分钟
每日响应时间组成: 平均	15 分钟
每周响应时间组成: 平均	1 小时
每月响应时间组成: 平均	6 小时

可以按如下所示使用这些视图：

- 在调查高数据传输速率和网络往复传输时间或端到端响应时间变化时，可以参考包含通信量峰值的“趋势报告”视图。
- 通过提升的响应时间识别拥塞模式。这是周期性、永久性还是突发性的拥塞？
- 检查与以前通信量趋势相比发生的显著变化。“趋势”视图对识别高网络使用率的时段很有帮助。
- 将每天的数据与一周内其他天的数据进行比较，或查看各天观测数目的比较情况。

使用可用性报告

管理控制台将应用程序可用性定义为一段时间内或响应服务器上应用程序端口请求期间观测到的成功 TCP 事务。管理控制台每 5 分钟收集一次应用程序端口级别的数据。

如果在 5 分钟观测间隔内出现以下情况之一，管理控制台就会质疑可用性：

- 观测数少于 10
- 被拒绝的会话超出 10%

如有必要，管理控制台会通过执行以下步骤来检查可用性：

1. 通过尝试连接已定义的应用程序端口来测试应用程序。对于按端口范围定义的应用程序，管理控制台将尝试连接到范围内的前八个端口。
2. 如果管理控制台未收到应用程序的响应，该应用程序将被分级为“不可用”。
3. 或者，管理控制台也可选择 ping 服务器来验证其状态。
   - 如果服务器确认了 ping 请求，管理控制台将认为服务器可用。
   - 如果服务器未确认 ping 请求，管理控制台将认为服务器不可用。
4. 如果应用程序或服务器不可用，管理控制台将打开一个服务器突发事件。

以下两种情形意味着不同的问题：

- 应用程序未运行，但承载它的服务器正在运行。
- TCP 端口专用于该应用程序（如端口 80 专用于 Web 应用程序）。

查看“应用程序可用性”和“服务器可用性”报告

遵循这些步骤:

1. 单击“工程”页面。
2. 在“向我显示”菜单中，单击“可用性”。

   将打开“应用程序可用性”或“服务器可用性”报告。
3. 单击彩色编码性能条，然后单击“时间”以查看可用性时间设置报告。
4. 单击箭头菜单并选择“聚合”，以便显示仅用于聚合的可用性报告。
5. 单击箭头菜单并选择“表”，以便按表格式显示可用性报告。

详细信息：

通过电子邮件发送报告页面 (p. 122)
打印报告页面 (p. 123)
更改报告设置 (p. 34)
将报告页面导出到 CSV 文件 (p. 121)
将视图导出到 CSV 文件 (p. 121)

查看可用性时间设置报告

遵循这些步骤:

1. 单击“工程”页面。
2. 在“向我显示”菜单中，单击“可用性”。

   将打开“应用程序可用性”或“服务器可用性”报告。
3. 单击应用程序或服务器对应的链接。
4. 在“向我显示”菜单中单击“时间”，以便查看“时间设置摘要”和“可用性时间设置”报告。

查看与可用性有关的突发事件

要查看指定时段内报告的突发事件，请单击“可用性”报告页面上的“相关突发事件”。突发事件报告列出了“可用性”报告时段内报告的突发事件。

详细信息：

使用突发事件页面 (p. 49)

使用“列表”报告

通过“工程”页面上的“列表”报告，可以查看由管理控制台监视的网络、服务器和应用程序。

了解“列表”报告

在“工程”页面上单击“列表”，可以查看网络、服务器和应用程序的列表。从这些列表可以导航到特定网络、服务器或应用程序的性能图。

查看网络、服务器和应用程序

在“工程”页面中，可以查看网络、服务器或应用程序的列表。从这些列表中，单击特定网络、服务器或应用程序的性能图中的链接，可以查看选中组件特定的度量标准。

在“工程”页面中单击“列表”，然后单击“网络”、“服务器”或“应用程序”即可查看相应报告。

在“网络列表”、“服务器列表”或“应用程序列表”中，单击图上的链接可以查看性能报告。

若您要	请执行
查看与应用程序或服务器相关的网络的“性能(按网络)”报告。	在“服务器列表”或“应用程序列表”页面上的“映射方式”列（如果可用）中单击“网络”链接。
查看与应用程序或网络相关的服务器的“性能(按服务器)”报告。	在“网络列表”或“应用程序列表”页面上的“映射方式”列中单击“服务器”链接。
查看与服务器相关的应用程序的“性能(按应用程序)”报告。	在“网络列表”或“服务器列表”页面上的“映射方式”列中单击“应用程序”链接。
显示聚合的列表报告。	单击箭头菜单并选择“聚合”。

详细信息：

通过电子邮件发送报告页面 (p. 122)
打印报告页面 (p. 123)
将报告页面导出到 CSV 文件 (p. 121)

第 7 章： 使用“优化”页面

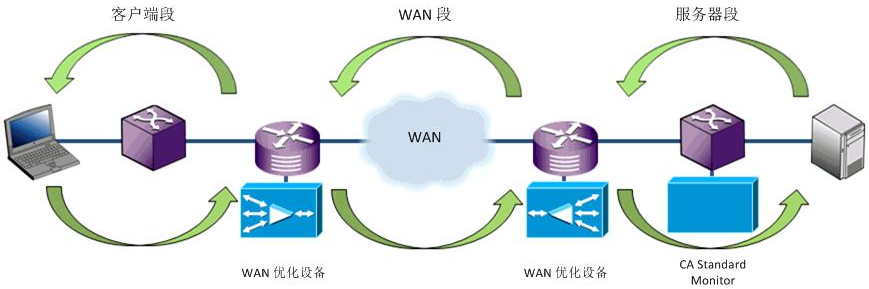
此部分包含以下主题：

了解优化事务

本节介绍了通过 Cisco WAAS 或 Riverbed Steelhead 传送的 WAN 优化事务，并帮助您理解“优化”页面上管理控制台报告中显示的优化事务数据。

WAN 优化解决方案在 WAN 两端均包括优化设备。WAN 优化设备通过将单个 TCP 连接拆分为以下三段，从而优化客户端和服务器间的 TCP 连接：

- 客户端到 WAN 优化边缘设备
- WAN 优化边缘设备到 WAN 优化核心设备
- WAN 优化核心设备到服务器



WAN 优化数据适用于由 WAN 优化解决方案创建的三个 TCP 网段。由于管理控制台从多个监视点对单个优化的应用程序-服务器-网络组合进行监视，它将为这三段分别生成一套度量标准，并将每套度量标准视为单独的应用程序。所有这三段的应用程序行为与三层应用程序的行为很类似，各层的源端口、目标端口和地址都相同。管理控制台的“优化”页面显示 WAN 优化事务的数据。

监视优化事务

通过为每个网段创建单独的应用程序，并将网段附加到应用程序名称上，“工程”页面可报告 WAN 优化应用程序。存在段时，管理控制台报告将对其进行标识。在每种视图中，管理控制台采用以下格式显示应用程序名称以及关联的段：
<*应用程序名称*> [<*段*>]

<*段*> 为“客户端”、“服务器”或“WAN”；例如：
HTTP [客户端]

如果未从分段应用程序收集通信量，[<*段*>] 标签将不显示。

查看“优化”页面

管理控制台监视 WAN 网段上的应用程序通信时，“优化”页面将打开。要查看“优化”页面，您必须拥有可以访问“工程”页面的角色。

“优化”页面从客户端的角度报告优化的应用程序体验。

“优化”页面上的“设置”参数与“工程”页面很类似，但以下内容除外：

- 服务器选择默认为“所有服务器”。服务器没有筛选选项。
- 可用应用程序仅包括 WAN 优化应用程序。
- 可用网络仅包括分段应用程序可从中观测客户端网段数据的网络。
- 您不能筛选特定度量标准或抽样间隔。

导航优化报告页面

使用“向我显示”菜单来导航优化报告页面。通过任何一个报告，您都可以深入到“组件”报告来查看特定应用程序的性能详细信息：

性能

显示每个客户端段应用程序的性能图。“优化事务的客户体验”视图反映真正的客户端体验。其中的度量来自远程 Cisco WAE 设备或监视远程 Steelhead 设备的远程 CA Standard Monitor。

带宽减少

显示每个 WAN 段应用程序的容量度量标准。“带宽减少”视图显示优化 WAN 段和数据中心服务器段或分支客户端段之间的总带宽减少量(字节)。您可以选择比较“总字节数”或“传出服务器字节”。

要报告 Steelhead 环境中的客户端段，CA Standard Monitor 必须监控分支 Steelhead 设备。

提示：默认情况下，单击“成为默认视图”可显示当前报告。

查看优化事务的性能详细信息报告

使用“组件”报告可查看优化事务的性能详细信息，并比较 WAN 优化的效果。从“优化”页面，深入到特定应用程序以显示“组件”报告。

下表概述了性能详细信息视图和这些视图源自的段：

视图	显示的应用程序段	参考
响应时间组成	客户端	响应时间组成: 平均 (p. 114)
服务器响应时间	服务器	服务器响应时间 (p. 115)
网络往复传输时间	WAN	网络往复传输时间 (p. 115)
重传延迟	WAN	重传延迟 (p. 89)
数据包丢失百分比	WAN	数据包丢失百分比 (p. 90)
数据速率(比特数/秒)	WAN	数据速率(比特数/秒) (p. 117)
数据速率(数据包/秒)	WAN	数据速率(数据包/秒) (p. 117)
数据量(以字节为单位)	WAN	数据量(以字节为单位) (p. 117)
数据量(以数据包为单位)	WAN	数据量(以数据包为单位) (p. 117)

在每种视图中，管理控制台采用以下格式显示应用程序名称以及关联的段：
<*应用程序名称*> [<*段*>]

<*段*> 为客户端、服务器或 WAN。

“组件”报告提供优化事务的性能详细资料视图。视图平均 5 分钟数据，以生成 15 分钟数据，并将：

- 5 分钟数据用于最多 8 小时的视图。
- 15 分钟数据用于最多 24 小时的视图。

详细信息：

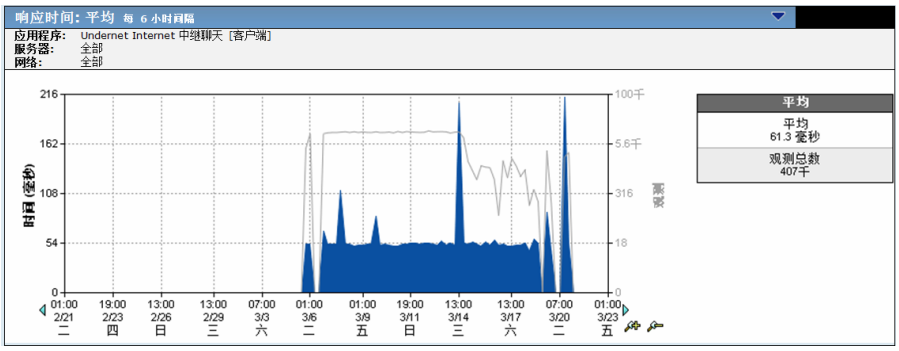
比较 WAN 优化的效果 (p. 118)

响应时间组成: 平均

“响应时间组成: 平均”视图显示客户端应用程序网段的事务时间。该视图反映了真实的客户体验。其中的度量来自：

- 远程 Cisco WAE 设备。
- 监视分支 Steelhead 设备的远程 CA Standard Monitor。如果 CA Standard Monitor 未监视分支位置上的客户端网段，则与该客户端网络对应的此视图为空。

该示例视图显示 WAN 优化前后对 HTTP 应用程序的影响。该子网中的用户将体验到事务数提高了 50 倍，而响应时间降低到了 1/25。

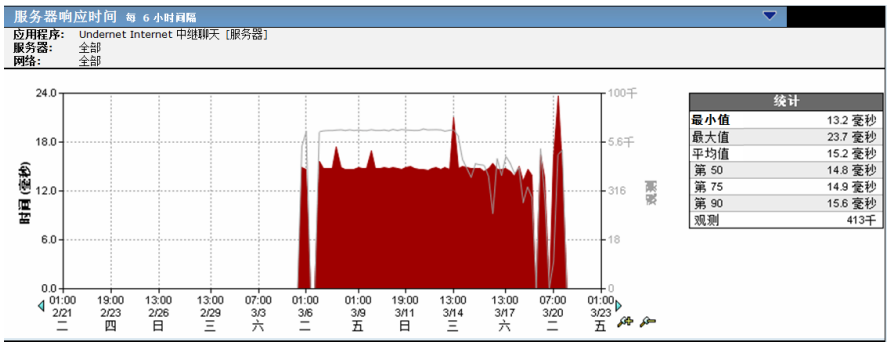


一个事务可能代表一个请求和一个服务器响应、数据传输的一个期间、一个或多个确认以及观测到的重传数据包引起的延迟。

服务器响应时间

“服务器响应时间”视图显示服务器响应应用程序请求所花费的时间。该视图还显示服务器段中应用程序的信息。在存在 SPAN 数据的位置，管理控制台使用这些数据来填充此段；否则，管理控制台使用数据中心 WAN 优化设备的服务器端的 FlowAgent 数据来填充此段。

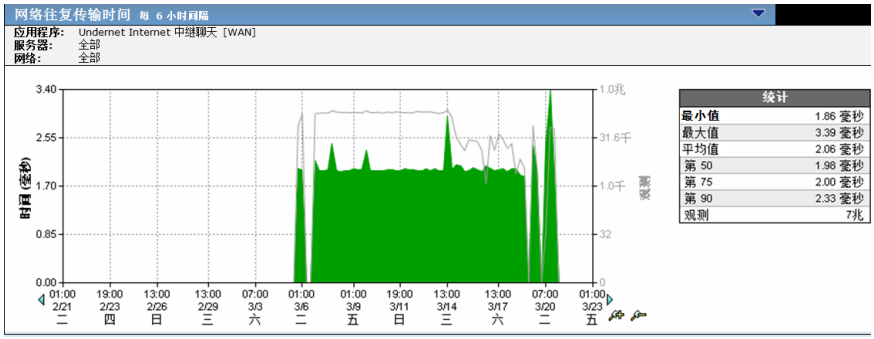
以下与“响应时间: 平均”视图一起生成的示例视图同样显示了该 HTTP 应用程序的事务数提高了 50 倍，而服务器响应时间无明显变化。



“响应时间: 平均”视图显示数据中心效率有了显著改进。每当客户端缓存处于活动状态时，“服务器响应时间”视图就能定量显示数据中心卸除负载所带来的好处。服务器响应时间值可能会受服务器速度、应用程序设计和请求数量的影响。

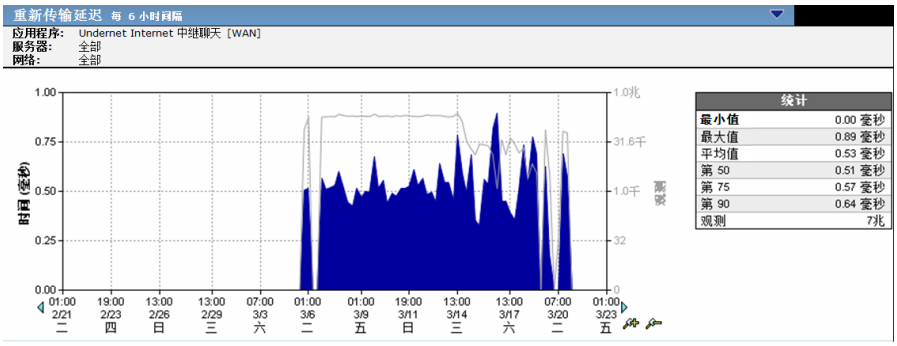
网络往复传输时间

“网络往复传输时间”视图显示数据包在网络上的本地和远程 WAN 优化设备之间往复传输所花的时间，但不包括重传导致的延迟。以下示例视图显示在激活 WAN 优化后，由于排队延迟减少或完全消除所带来的 WAN 上网络往复传输时间方面的显著改进。



重传延迟

重传延迟是由需要重传的数据包导致的网络往复传输时间的额外延迟。以下示例视图显示 WAN 上针对该 HTTP 应用程序的重传在 WAN 优化处于活动状态时停止。



该数据是所有观测的平均值，而不是某一个事务的实际重传时间。如果总共有 5 个事务，其中 4 个不存在重传，1 个具有 5 秒的重传延迟，则该视图显示 1 秒的重传延迟。

通过从临近服务器的有利位置观测网络中的重复数据包来计算重传延迟。监视设备可以观测到由于网络路径中服务器->客户端方向上发生数据丢失而导致服务器重传的数据包。这些观测包含在重传延迟中。但当客户端->服务器方向（如到达服务器之前的网络路径上）发生数据丢失时，监视设备无法观测到此类数据包丢失，因此该延迟不会包含在“重传延迟”度量标准中。

管理控制台将该重传延迟包含在“网络往复传输时间”度量标准（包括服务器响应和客户端确认）中；因此，这是客户端确认中由未观测的重传延迟引起的延迟，它将增大网络往复传输时间值。该度量标准不能反映由于 TCP 拥塞而导致数据传输时间延长所带来的影响。

重传可能会导致指定会话的事务时间有所降低，但线路上的字节速度保持不变，除非路径发生了更改或拥塞有所增加。

数据包丢失百分比

“数据包丢失百分比”视图显示被监视网络上丢失的数据所占的百分比，以及用“数据包数/秒”表示的丢失速率。

监视设备通过从临近服务器的有利位置观测网络中的重传数据占总数据的比率来计算数据包丢失百分比。监视设备可以观测到由于网络路径中服务器->客户端方向上发生数据丢失而导致服务器重传的数据包。但当客户端->服务器方向（如到达服务器之前的网络路径上）发生数据丢失时，监视设备无法观测到此类数据包丢失，因此该延迟不会包含在“数据包丢失百分比”中。

数据速率(比特数/秒)

“数据速率(比特数/秒)”视图以比特数/秒（字节数/秒乘以 8）为单位显示指定时段内 WAN 上的数据速率。

数据速率(数据包/秒)

“数据速率(数据包/秒)”视图以数据包/秒为单位显示指定时段内 WAN 上应用程序的数据速率。

数据量(以字节为单位)

“数据量(以字节为单位)”视图显示在网络上观测到的应用程序层的总字节数。

数据量(以数据包为单位)

“数据量(以数据包为单位)”视图显示在监视的网络上观测到的数据包总数。零字节数据包（如 TCP 确认）会计到该视图中。

比较 WAN 优化的效果

使用“组件”报告来比较 WAN 优化对响应时间和容量度量标准的影响。管理控制台不会自动为您选择时段。浏览到 WAN 优化启动或停止的相应时段，以比较响应时间差异。

要比较 WAN 优化的效果，请将“组件”报告筛选到特定网络上的应用程序。

遵循这些步骤:

1. 从“优化”页面，单击“向我显示”菜单中的“性能”。
2. 单击“设置”以指定所需的应用程序和网络。
3. 单击“确定”。

   “优化事务的客户体验”显示该应用程序。
4. 在“向我显示”菜单中单击“性能”、“应用程序”。
5. 单击“显示优化之前和之后”选项。

   组件报告现在即可提供来自服务器 SPAN 的未优化应用程序性能数据，也可提供 WAN 优化性能数据。
6. 单击左右箭头浏览 WAN 优化启动或停止的相应时段，以便比较响应时间差异。管理控制台不会自动为您选择时段。

检测外溢通信量

如果某个组合存在需要完全优化的外溢（即，需要优化的会话由于 WAN 优化设备在那一刻无法进行另一个会话而导致未得到优化），那么外溢会话的 SPAN 度量将转换到 [服务器] 段。

外溢会话度量不会影响 [客户端] 段或 [WAN] 段。“服务器响应时间 [服务器]”虽然包含外溢和优化会话的度量，但它是准确的。“优化”页面上的所有度量标准均是准确的。“网络往复传输时间 [服务器]”会显示增量，因为它不再能获得 100% 本地 ACK。外溢度量显示传出到客户端的实际网络往复传输时间。“RetransDelay [服务器]”和“PacketLossPct [服务器]”也可能会显示增量。

在规模适当的 WAN 优化部署中，应该极少情况下会没有外溢。如果发现网络往复传输时间 [服务器] 的空闲时间和高负载时间之间一直存在差异，则可能存在外溢。该解决方案用于增加 WAN 优化部署的容量。如果所有网络都显示增量，则说明数据中心 WAN 优化设备可能容量不足。如果仅少数几个网络显示增量，则说明那些分支 WAN 优化设备可能容量不足。

另一个外溢线索是 [服务器] 段上报告的会话比 [客户端] 段上多。对于至少具有一些优化的组合，如果在 [服务器] 段而不是所属的父级应用程序中报告非优化会话，就会发生这种情况。

第 8 章： 共享报告页面和视图中的信息

此部分包含以下主题：

将报告导出到文件

将报告数据导出到 CSV 文件。您可以将报告页面上的特定视图或所有视图的数据导出到 CSV 文件或 XML 文件。

将报告页面导出到 CSV 文件

将管理控制台页面上的所有视图数据导出到 CSV 文件。例如，您可以将“操作”页面中的所有视图数据导出到 CSV 文件。

遵循这些步骤:

1. 单击报告页面。
2. 单击“导出”。

   将打开“文件下载”对话框。
3. 单击“保存”将报告保存为 CSV 文件，或单击“打开”以查看 CSV 文件。

将视图导出到 CSV 文件

将“工程”页面上的视图数据导出到 CSV 文件。

遵循这些步骤:

1. 单击“工程”页面。
2. 单击所需视图上的蓝色箭头 菜单，然后选择“导出到 CSV”。

   将打开“文件下载”对话框。
3. 单击“保存”将视图保存为 CSV 文件，或单击“打开”以打开 CSV 文件。

将视图导出到 XML 文件

将“工程”页面上的视图数据导出到 XML 文件。

遵循这些步骤:

1. 单击“工程”页面。
2. 单击所需视图上的蓝色箭头 菜单，然后选择“导出到 XML”。

   将显示 XML 格式的数据。

通过电子邮件发送报告页面

采用 HTML 格式通过电子邮件将报告页面发送给指定的收件人。通过电子邮件发送报告页面时，可以立即发送该报告，也可以进行排定以便以后发送。

遵循这些步骤:

1. 单击报告页面。
2. 单击“电子邮件”。

   将打开“发送电子邮件属性”。
3. 指定以下设置，然后单击“确定”：

   电子邮件属性

   通知指定的电子邮件收件人。请注意，电子邮件通知使用指定时区进行排定。

   排定选项

   只有在您选择排定通知时才会显示排定选项。可以排定通知以便在特定日期的特定时间运行，也可以排定通知按周或按月运行。

打印报告页面

使用“打印预览”按钮格式化报告页面以便打印，然后使用 Web 浏览器来打印该报告。

遵循这些步骤:

1. 单击报告页面。
2. 单击“打印预览”。

   管理控制台将在浏览器窗口中显示报告页面。
3. 使用 Web 浏览器打印报告页面。

第 9 章： 故障排除

此部分包含以下主题：

概述

通过管理控制台执行以下操作：

- 使用操作级别报告量化企业网络上达到的应用程序性能
- 使用前后分析验证计划内和计划外的变更所产生的影响
- 发生突发事件时，自动标识最终用户问题、隔离原因并收集诊断数据，从而更快速地解决性能问题

性能问题的根源可能是以下三个实施元素中的任何一个或组合：

- 网络基础架构（例如，由线路、通信拥塞、路由器及交换机引起的延迟）。
- 服务器基础架构（例如，由 CPU 处理、内存 I/O 或磁盘读写引起的延迟）。
- 应用程序体系结构（例如，将大量数据请求写入传输的大量小型数据包）。

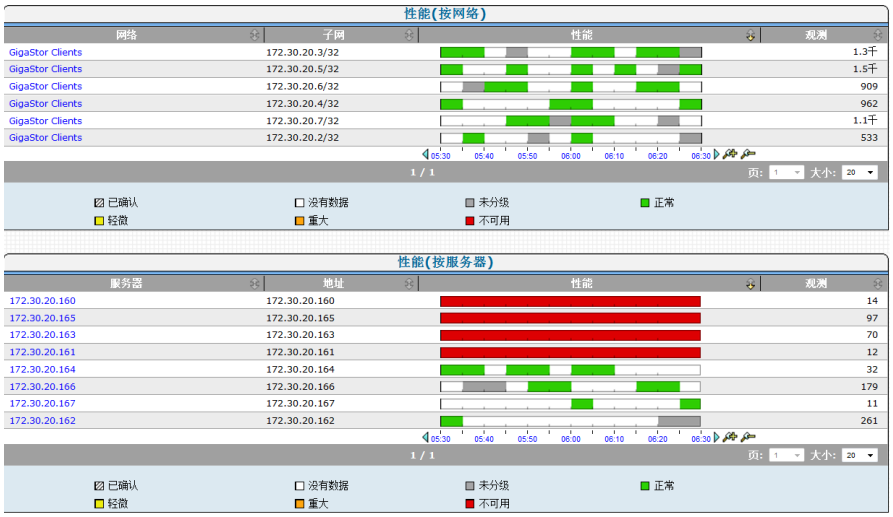
使用以下方法检查并分析管理控制台数据，可以确定性能问题的起因：

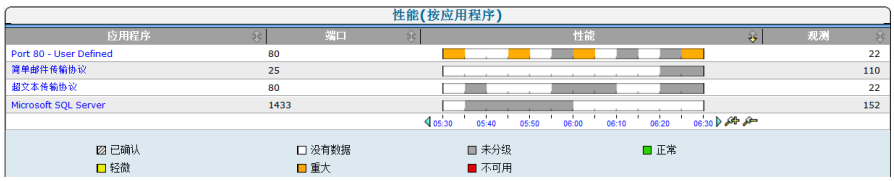
1. 使用性能图和应用程序详细信息视图，识别存在性能问题的应用程序。
2. 隔离导致性能问题的时间组成。“响应时间组成”视图中的颜色标识出了构成总时间的每个组成部分。
3. 通过检查“通信量”、“会话”、“趋势”、“响应大小”、“QoS”和“统计”页面，可调查导致性能问题的因素。

使用“操作”页面

“操作”页面显示水平条形图，用于对总体性能元素与阈值进行对比。被监视的性能最差的网络、服务器和应用程序按降序列在每个视图中。

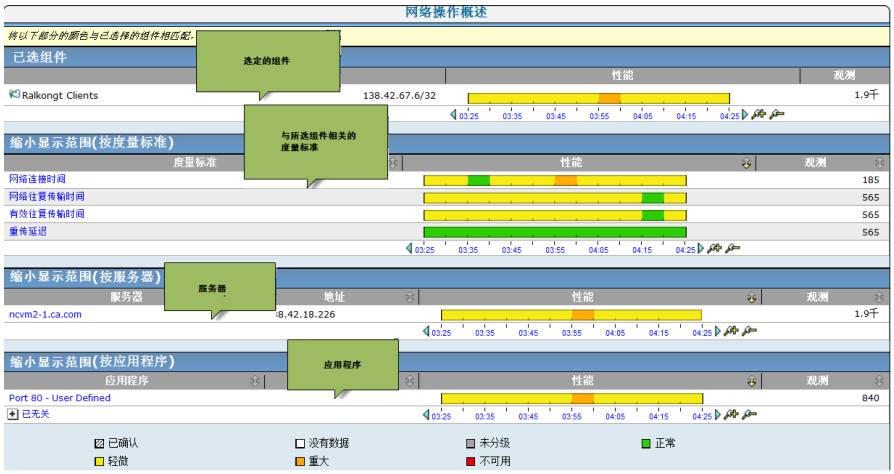
这样，您可以快速看出企业中哪些区域应该引起您的关注。





要隔离导致性能问题的组成部分和度量标准，请单击视图顶端性能最差的某个项。

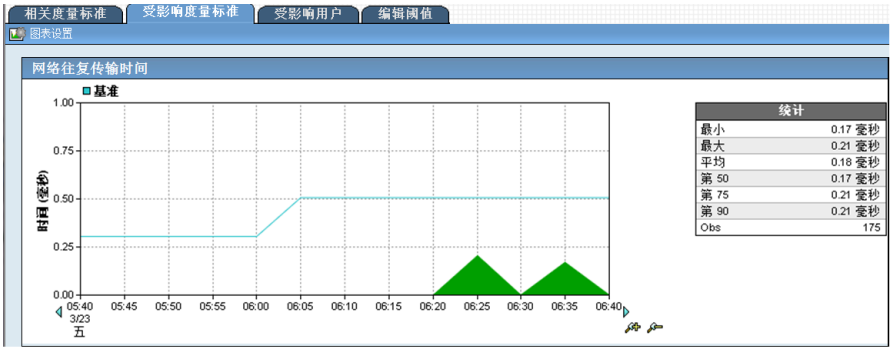
在以下示例中，选中的是“性能(按网络)”视图顶端的 Singapore 网络。刷新页面后，将显示与我们选择的项相关的信息：



在该页面上，您可以看到：

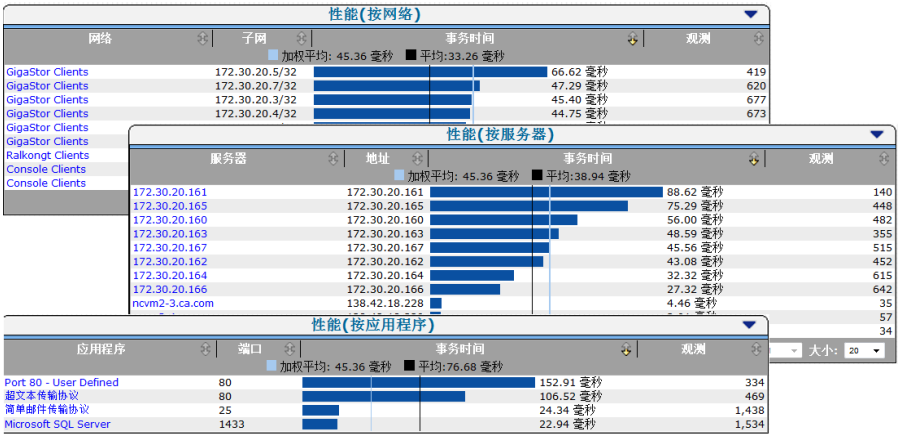
- 所需的度量标准和相关组成
- 指明受影响项的基于阈值的颜色模式
- 匹配选定组件的性能模式

要进一步调查性能，请选择匹配的性能配置文件，然后单击“浏览”查看更多详细信息：



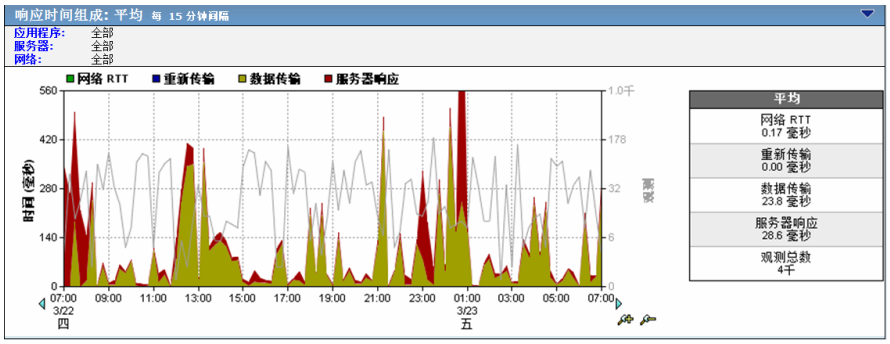
使用“工程”页面

“性能图”显示在“工程”页面中。格式为可以比较各个元素的水平条形图 - 每个已配置应用程序的“总事务时间”（最长时间也就是最慢应用程序排在最上面）、每个已配置网络的“网络往复传输时间”（最长时间也就是最慢网络排在最上面）以及每个已配置服务器的“服务器响应时间”（最长响应时间也就是最慢服务器排在最上面）。

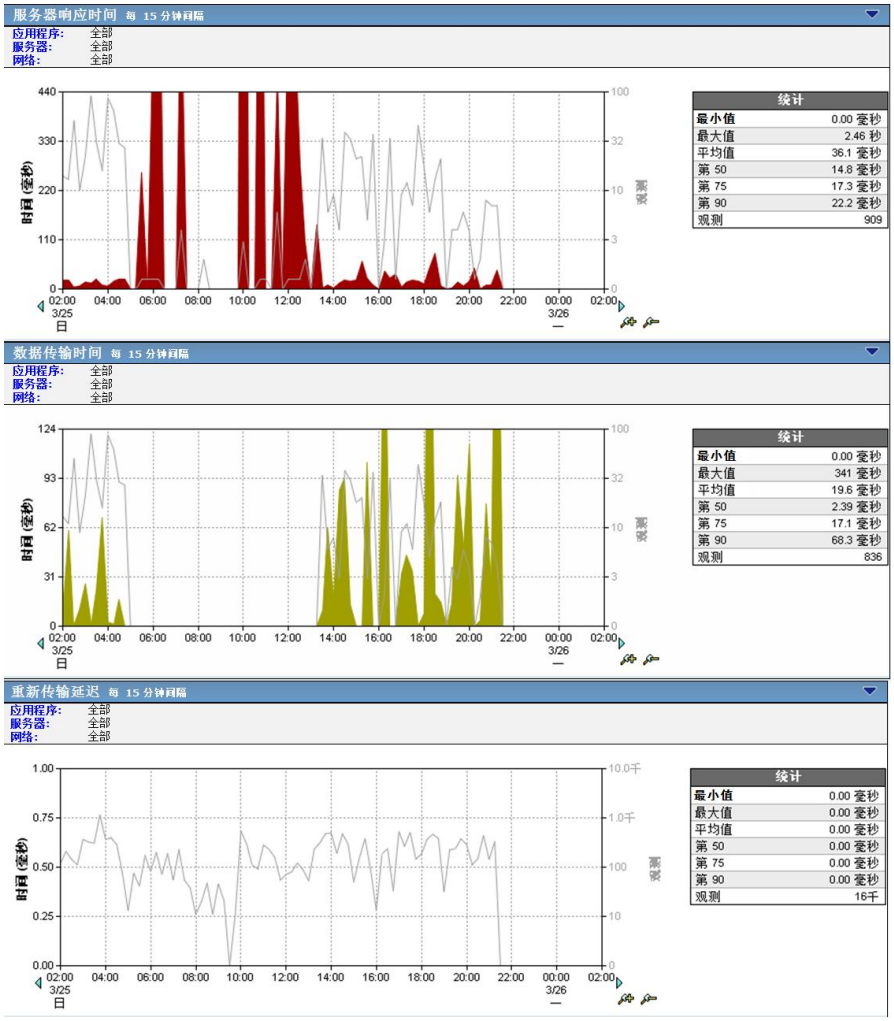


单击视图上列出的项目之一，可以隔离导致性能问题的组成时间。刷新页面后，将显示与您选择的项相关的信息。

以下示例显示“响应时间组成: 平均”视图：



“响应时间组成: 平均”视图的各个组成部分堆积在其下面，如下图中所示的部分：



查看堆积的组成视图时，整体颜色最多或处于任何峰值的组成就是那一刻导致应用程序性能不佳的主要因素。

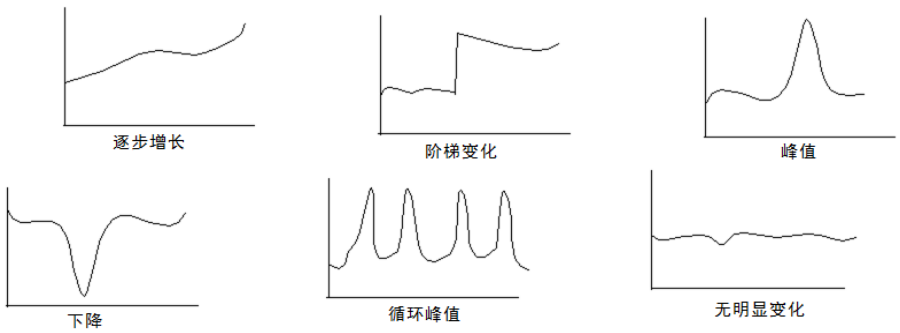
识别导致影响应用程序总体性能的最大延迟的组成部分，然后向下滚动到单个组成视图，以便开始调查性能问题的范围。

遵照以下一些通用准则调查性能问题的范围：

1. 首先分析总事务时间。
2. 深入查看堆积视图 - 使用基于 15 分钟间隔数据点创建的“每日”视图。如果按 15 分钟间隔无法看出性能事件，请将间隔降低到 5 分钟。
3. 查看按 5 分钟间隔显示的过去 1 小时或 8 小时视图中的峰值事件，以实现高数据分辨率。
4. 将在某个图表中观测到的峰值或颜色模式与同一时刻另一度量标准类似的峰值、谷值或颜色模式相关联。
5. 打开多个 Web 会话以便于进行比较。也可以使用放大或缩小功能来查找发生问题的日期中的特定时间、周或月份中的特定日期的大规模模式。

常规故障排除

使用管理控制台可将问题的根源范围缩小到网络、服务器或应用程序问题。本节中建议的方法可以帮助您理解在各种报告中看到的数据。请注意度量标准视图中遵循以下指示模式的一些更改：



调查以找出度量标准的哪些组成部分导致了变化。

确定问题的原因

1. 单击“操作”页面，选择一个或多个组件（相关网络、服务器、应用程序），然后单击“链接: 工程”，以便查看“工程”页面上反映的您所做的选择。
2. 在“向我显示”菜单中，单击“组件”。
3. 使用组件报告开始进行调查。该报告由各种响应时间视图组成，这些视图顶部彼此堆积在一起，显示了每个部分占总体响应时间的比例。“组件”报告中包括：
   - 响应时间组成: 平均
   - 服务器响应时间
   - 数据传输时间
   - 重传延迟
   - 网络往复传输时间
   - 有效网络往复传输时间

   根据视图上的时间点，主宰该视图的组成颜色指明了导致应用程序整体响应时间延迟最长的组件。

   单独考虑以下因素：
   - 较高的服务器响应时间值表示服务器可能存在问题
   - 较高的数据传输时间值通常表示应用程序是问题的根源
   - 较高的 NRTT 或重传时间值通常表示网络中存在问题
4. 识别导致组件报告中最长延迟的响应时间组成后，通过向下滚动图表页面，可查看该组成的单独视图。
5. 在单独组成视图中，请注意问题发生时记录的观测数。观测数有助于确定问题根源到底是服务器还是网络或应用程序。

   与“正常”内容相关的观测数将帮助您了解：
   - 事件的重要性 - 观测计数较大通常表示对所分析应用程序的用户影响重大，而此值较小表示对最终用户的影响有限和/或不存在足够的数据点来分析问题。
   - 相关应用程序的相关影响 - 观测计数较小可能表示性能事件不是由正在分析的应用程序导致的。
6. 遵循相关流程来确认这些结果，并将源问题区域标识为服务器、网络或应用程序。在极少情况下，性能问题可能源于多个潜在因素，但这种情况并不常见。

请考虑以下可能性：

- 发现 1：正面发现表明问题源是特定的服务器、网络或应用程序。例如，数据显示该服务器就是问题所在。
- 发现 2：负面发现表明问题源不是特定的网络、服务器或应用程序。例如，数据清晰地显示该网络不是问题所在。
- 发现 3：负面发现表明问题源不是最后的其他网络、服务器或应用程序。例如，数据进一步显示该应用程序不是问题所在。

综合以上发现，就可将服务器判定为问题源，同时可以排除网络和应用程序是问题源的可能性。通过这三方面的发现，就可以很有把握地确定问题的根本原因并继续采取补救措施。

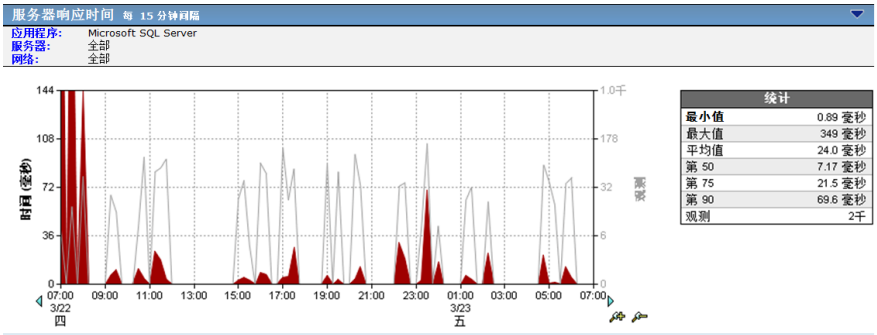
注意：可以将鼠标光标停留在“响应时间组成”视图中的某点或感兴趣的位置，并使用向下箭头键向下滚动页面，使下面的视图进入鼠标光标下的视图中。当您使用箭头键向下移动页面时，鼠标指针将停留在屏幕上的精确位置，这样您能方便地将“组成”视图中的给定点对准该页面下方的视图。

服务器响应时间增加

服务器响应时间增加与观测计数有关 - 以下分析中既考虑了增加的情况，又考虑了减少的情况。

服务器响应时间和观测计数增加

服务器响应时间和观测数增加，强有力地说明了性能问题与服务器有关。通过将其与其他相关数据关联，可以更好地说明这一点。



与服务器有关的性能问题应当在所有网络集和聚合中均可见 - 既包括本地网络集（包括与数据中心在同一构建中的用户），又包括远程网络集（包括跨 WAN 连接的用户）。

如果服务器响应时间和观测数在观测到性能问题的同一时间点达到峰值，请查看此同一时间点的数据集：

- 通信量 - [数据量、数据速率]

  检查数据量/速率是否有所增加。向网络写入的数据量越高，服务器的工作强度越大。服务器响应时间增加的同时伴有数据量的异常增加表示服务器很难满足需求。

- 会话 - [连接建立时间，TCP/IP 会话，未实现的 TCP/IP 会话请求，TCP/IP 会话时间]

  检查服务器连接建立时间是否同时增加，这可能表明操作系统内核增加了响应新会话请求所需的时间。

  检查 TCP/IP 会话数是否显著增加，例如大于 10%。其他 TCP 会话和随之产生的应用程序请求将需要来自服务器的更多资源并会增加其负担。

  检查未实现的 TCP/IP 请求数是否出现异常增加。如果显著增加，则强有力地说明了服务器的硬件资源存在过载。

- QoS - [用户、数据包丢失百分比、用户正常输出、每用户综合速率]

  检查用户数是否有显著增加。用户数量增加会增大对服务器资源的需求。可将特定数量的用户导致服务器响应时间降低的点解释为升级服务器或对配置相似的服务器之间的应用程序进行负载平衡的未来前瞻性点。

- 统计 - [响应时间组成: 标准偏差，服务器响应时间百分位，数据传输时间百分位，重传延迟时间百分位，网络往复传输时间百分位]

  检查服务器响应时间和/或百分位的标准偏差是否增加。这可能表明服务器性能的不一致性和偶发性（如与平均距离显著不同距离处的更多“无关”数据点中所示），同时也强有力地说明存在基于服务器的问题。

服务器响应时间增加和观测计数减少

服务器响应时间增加的同时观测数减少，可能表明存在两个完全不同的事件：

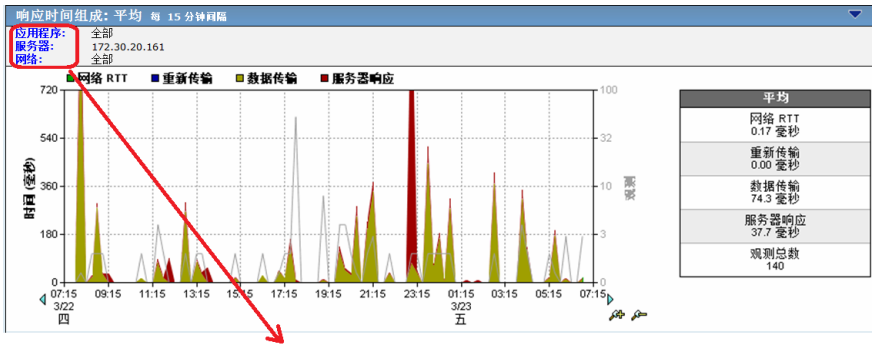
- 服务器上的其他应用程序导致服务器响应时间增加。此应用程序可能由管理控制台监视，也可能不由其监视。
- 由于服务器中的 CPU、内存或 NIC 不稳定，因此应用程序服务不可靠。这可能会导致服务偶尔中断，或最终导致服务完全停机。

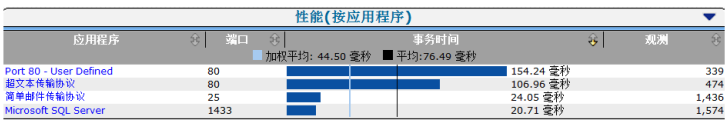
当观测数在观测到性能问题的同时出现谷值时，如果服务器响应时间达到峰值，请完成以下步骤，以确定哪个事件导致了性能的下降：

确定 SRT 出现峰值和观测计数出现谷值的原因

首先确定服务器中是否有其他应用程序处于活动状态。

1. 单击“工程”页面。
2. 从任意“响应时间”视图中选择以下设置：
   - 应用程序 - 全部
   - 服务器 - 选择服务器的名称
   - 网络集 - 全部
3. 单击“响应时间组成”视图标题中的蓝色超文本“应用程序”，以查看服务器上正在监视的所有应用程序：





如果生成的性能图中显示其他应用程序，请重复这些步骤以确定它是否是性能问题的问题源。

关键是在报告性能问题的同时特定应用程序的观测数增加。

4. 如果生成的性能图中未显示其他应用程序，则可使用后退箭头返回到“工程”页面。单击水平菜单中的“趋势”，并检查此性能事件在过去数周和月份中是否呈现某种模式。如果呈现某种模式，则可在预测的重复时间和日期内出现问题的特定时间使用协议分析器来确定问题源应用程序。

   给服务器上的主应用程序造成问题的应用程序示例有：

   - 在夜间执行的备份
   - 防病毒软件的升级
   - 其他团队用来度量服务器容量或性能的代理

   备份进程通常通过用于重复时段的备份软件代理来排定。因此，“趋势”视图上应有一个可见模式，它显示每 24 小时时段、每隔 24 小时时段内服务器响应时间的循环峰值，或备份排定指示的任何内容。

   防病毒定义的升级通常每周执行一次，或在紧急情况下“按需”执行。请向您的防病毒软件供应商和/或桌面/安全团队咨询，以确定自动更新版本排定。有时，应用程序开发团队可能会安装第三方代理或将性能代理编码到软件中。查看更改通知，以确定在性能问题开始出现之前是否对服务器上的软件进行了任何更改。

确定服务器/应用程序服务是否已经变得不可靠。

1. 在管理控制台中设置阈值，以便在服务器响应时间超过接受值时启动调查。管理控制台会自动收集 CPU 和内存使用率等相关信息。
2. 查看服务器系统日志能够发现可能正在影响应用程序稳定性的错误和其他事件。
3. 检查面向服务器和服务器 NIC 的交换机端口，以确保针对下表中的正确双工和速度设置设置了该端口，并且该端口没有错误。

服务器	Switch	结果
自动	自动	全双工、自动速度
自动	手工	半双工、手动速度
手工	自动	半双工、手动速度
手动 - 完全	手动 - 完全	全双工，手动速度（假定两端设置了相同速度，10 Mbps、100 Mbps、1000 Mbps）

网络往复传输时间 (NRTT) 增加

网络往复传输时间可根据以下等式来定义：

```
NRTT = S_Delay + Q_Delay + R/SW_Delay + D_Delay + P_Delay
```

其中：

S_Delay

序列化延迟 - [(帧大小 * 8)/(访问速率)]

Q_Delay

队列延迟 - 取决于使用率和 S_Delay

R/SW_Delay

路由/交换机延迟 - 通常每个跃点不大于 1 毫秒

D_Delay

距离延迟 - 由于传输距离导致的传播延迟。通常光纤为 5ìs/km，铜缆为 5.56ìs/km，卫星为 3.3ìs/km

P_Delay

协议延迟 - 通过传输或较高级别的协议添加的延迟

例如：用于共享以太网的 CSMA/CD

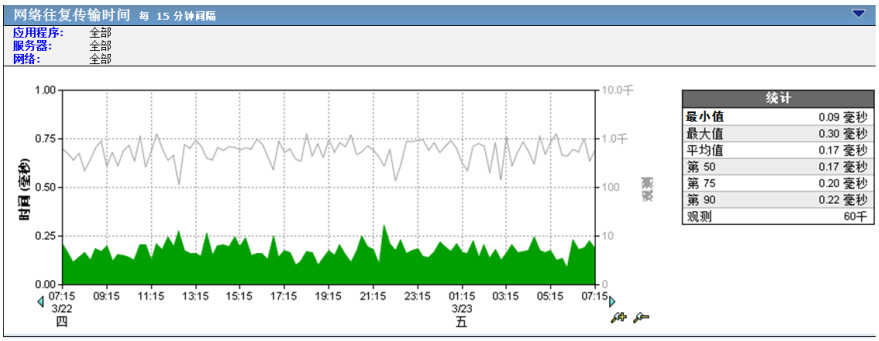
通常，与应用程序关联的 NRTT 的增加是由上面所列任意变量的增加导致的。但是，NRTT 增加的典型原因按通常的发生顺序列出：

- 由于线路使用率增加（从而加深网络队列）而导致的 Q_Delay 增加
- 由于运送者或企业故障转移到距离较长的受保护/冗余路径而导致的 D_Delay 增加
- 由于网络错误而导致的 R/SW_Delay 增加
- 由于企业故障转移到具有较低带宽的冗余路径而导致的 S_Delay 增加

要确定网络问题是否局限于单个远程站点，可将受影响远程站点的 NRTT 中的峰值与其他站点（在与服务器的距离、带宽和用户计数方面可比较）进行对比和比较。如果 NRTT 在多个站点中同时增加或达到峰值，问题可能与运送者相关，或由路由协议的不稳定性导致。

NRTT 和观测计数增加

NRTT 和观测计数增加强有力地说明了性能问题与网络的应用程序使用率有关。通过将此指标与其他相应数据点关联，可以更有力地说明网络就是问题源。



如果 NRTT 和观测数在观测到性能问题的同一时间点达到峰值，请查看此同一时间点的数据集：

- 组件 - [重传延迟]

  检查重传的长度是否增加。重传表明网络队列正以比清空速度更快的速度进行填充，从而引起数据包丢弃和相关的 TCP 重传

- 会话 - [连接建立时间，TCP/IP 会话]

  检查网络连接建立时间是否同时增加。此增加表明由于网络中其他已建立会话增加了队列深度，导致网络中的三向 TCP 握手发生延迟。

  检查 TCP/IP 会话数目是否存在显著增加（大于 10%）。其他 TCP 会话和伴随的应用程序数据需要更多带宽。

- 通信量 - [数据量、数据速率]

  检查数据量/速率是否有所增加。如果网络中的数据量较大，则会增加队列深度和相关延迟。NRTT 增加的同时伴有数据量的异常增加表示网络很难满足需求。

- QoS -- [用户]

  检查用户数是否有显著增加。网络使用率增加通常与用户数的增加一致。可将特定数量的用户导致 NRTT 降低的点解释为升级其他类似站点的网络带宽的未来前瞻性点。

- 统计 - [响应时间组成: 标准偏差，网络往复传输时间百分位]

  检查 NRTT 和/或百分位的标准偏差是否增加。此增加表明网络性能的不一致性和偶发性（如与平均距离显著不同距离处的更多“无关”数据点中所示），同时也强有力地说明存在基于网络的问题。

NRTT 增加和观测计数减少

观测计数减少的同时 NRTT 增加，可能表明存在两个完全不同的事件：

- 网络上的其他应用程序对 NRTT 增加负责。此应用程序可能由管理控制台监视，也可能不由其监视。
- 由于网络不稳定（链路失败、路由发散、STP 发散、运送者故障转移以及其他错误），应用程序服务已变得不可靠。这可能会导致服务偶尔中断，或最终导致服务完全停机。

当观测计数在观测到性能问题的同时出现谷值时，如果 NRTT 达到峰值，请完成以下操作，以确定上面提及的哪个事件导致了性能下降。

确定性能下降的原因

确定网络中是否有其他应用程序处于活动状态：

1. 单击“工程”页面。
2. 从任意“响应时间”视图中选择以下设置：
   - 应用程序 - 全部
   - 服务器 - 全部
   - 网络集 - 相关聚合，如下面所示的远程站点聚合
3. 在“响应时间组成”视图中，单击蓝色超文本“应用程序”链接，以查看此服务器上正由管理控制台监视的所有应用程序。

   如果生成的性能图中显示其他应用程序，请为此应用程序重复这些步骤以确定它是否是性能问题的问题源。

   关键是在报告性能问题的同时观测数增加。
4. 如果生成的性能图中未显示其他应用程序，则可使用后退箭头返回到主“工程”页面。从水平菜单中选择“趋势”，并检查此性能事件在过去数周和月份中是否呈现某种模式。如果呈现某种模式，则需使用历史 NetFlow 数据、IP 记帐或协议分析器数据来确定在出现问题的时间内应用程序是否使网络饱和。如果没有可用的历史数据，则可在预测的重复时间和日期内手动查看出现问题的时间，以确定问题源应用程序。

   给网络上的主应用程序造成问题的应用程序示例有：
   - 远程站点之间的复制或备份数据
   - 服务器之间的大型文件传输
   - 在亚速率 WAN 链路中 (< T1) 流动大量数据的用户
   - 跨亚速率 WAN 链路的防病毒升级

确定网络是否已经变得不可靠：

1. 检查面向服务器和服务器 NIC 的交换机端口，以确保针对正确的双工和速度设置（请参阅下表）设置了该端口，并且该端口没有错误。

服务器	Switch	结果
自动	自动	全双工、自动速度
自动	手工	半双工、手动速度
手工	自动	半双工、手动速度

服务器	Switch	结果
手动 - 完全	手动 - 完全	全双工、手动速度（假定在两端设置了相同速度）

2. 通过在管理控制台中设置阈值以在 NRTT 超过接受值时启动调查，来确定网络是否因配置问题或网络错误已变得不可靠。管理控制台会自动收集来自路由器和交换机的相关信息。
3. 查看路由器和交换机日志、接口错误和更改记录，以发现可能会影响网络稳定性的任何事件，如路由分散和线路错误。

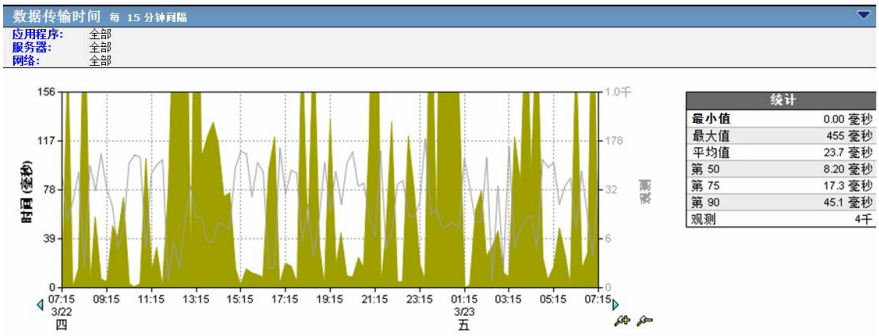
数据传输时间增加

数据传输时间增加与观测计数有关 - 以下分析中同时考虑了增加和减少这两种情况。

数据传输时间和观测计数增加

数据传输时间和观测计数增加很好地说明了性能问题与应用程序有关。

通过将此指标与相应数据点关联，可以更有力地说明应用程序就是问题源。



与应用程序关联的性能问题会因站点而异，具体取决于可用带宽和因距离引起的延迟。位于相同站点的应用程序用户的子集抱怨应用程序性能的情况并不常见。您可以跨应用程序查询，以查看“数据传输时间”中的峰值是否可与跨越相同网络路径或源自同一服务器的应用程序关联。如果是这样，则问题可能在网络或服务器中。

如果确定数据传输时间增加与单个服务器上的单个应用程序相关，并且数据传输时间和观测数在观测到性能问题的同一时间点达到峰值，请查看该时间的以下数据集：

- 通信量 - [数据量、数据速率]

  检查数据量/速率是否有所增加。应用程序可能无法有效地跨慢速 WAN 链路写入，或者无法写入距离很远的站点。

- 组件 - [网络往复传输时间、重传延迟、服务器响应时间]

  检查 NRTT 和重传延迟是否随着数据量的增加而保持不变。恒定的、可接受的网络往复传输时间加上少量数据包丢弃表明存在应用程序问题。

  检查服务器响应时间是否增加。如果服务器响应时间增加，而会话或用户计数、未实现的 TCP 会话请求和 NRTT 不增加，则表明应用程序存在问题。

- 会话 - [连接建立时间，TCP/IP 会话，未实现的 TCP/IP 会话]

  检查服务器连接建立时间是否同时增加。此类增加表明操作系统内核增加了响应新会话请求所需的时间。

  检查 TCP/IP 会话数目是否存在显著增加（大于 10%）。其他 TCP 会话和随之产生的应用程序请求将需要来自服务器的更多资源并会增加其负担。

  检查未实现的 TCP/IP 请求是否保持不变（最佳时为零）。在活动会话建立期间缺少未实现的 TCP 请求表明服务器资源可供用户使用，并且可进一步减轻服务器对性能问题的责任。

- QoS -- [用户]

  检查在性能事件之前、之中和之后是否存在恒定数量的用户。如果服务器在发生性能事件时缺少新用户，通常会将服务器负载从因素中排除。

- 统计 - [响应时间组成: 标准偏差，数据传输时间百分位]

  检查“数据传输时间”和/或“百分位”的标准偏差是否增加 - NRTT 没有伴随的增加，服务器响应时间的增加也不显著。此类增加表明了应用程序性能的不一致性和偶发性（如与平均距离显著不同距离处的更多“无关”数据点中所示），同时很好地说明了存在基于应用程序的问题。

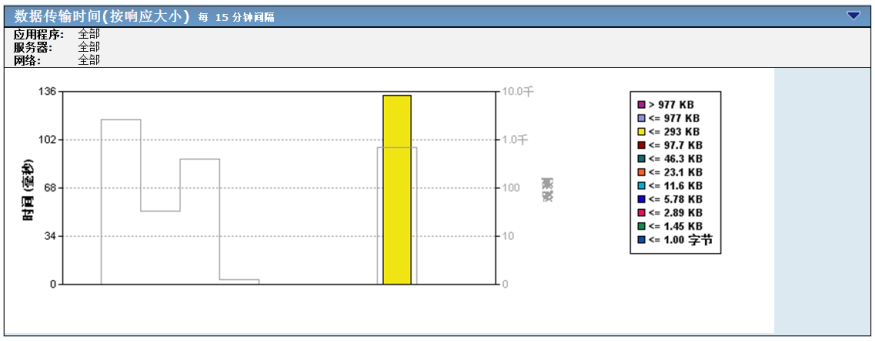
数据传输时间 = 0（Ping-Pong 应用程序）

“Ping-Pong”应用程序将单个数据包响应发送给大多数或所有请求；这是一个应用程序问题。管理控制台计算“数据传输时间”的方法是，从与客户端数据请求的第一个应用程序响应关联的时间戳中减去与客户端数据请求的最后一个应用程序响应关联的时间戳。如果两个时间戳相等，则结果为 0，因为应用程序只发送一个数据包来响应客户端请求，并且必须在应用程序层确认此数据包后，客户端才能请求下一个数据包。

如果完成总事务数所需的数据量达到数万或数十万字节，则会导致应用程序出现较大的吞吐量问题，因为客户端必须等待每个数据包的一个 NRTT+ 被传递并由应用程序确认。如果客户端在单个请求中请求所有数据，应用程序的响应方式是一次在多个数据包中尽量发送 TCP 活动窗口允许发送的字节数。这会显著减少传输数据所需的往复传输数，并且会提高应用程序的性能。

在“数据传输时间”等于零时验证此方案：

1. 在“向我显示”菜单中，单击“响应大小”。
2. 滚动到“数据传输时间(按响应大小)”视图，并确定小于 1.45 KB 的数据传输数、基于以太网框架的一个段或数据包是否是以下视图中最重要的条。此图表明大部分数据包都包含最少数据：



数据传输时间增加和观测计数减少

数据传输时间增加的同时观测计数减少，通常表明问题与服务器或网络有关。如果“服务器响应时间”随着“数据传输时间”的增加而增加，请查看服务器资源和应用程序代码。

如果 NRTT 和“重传延迟”随着“数据传输时间”的增加而增加 - 请在确定问题网段之后查看网络路径和关联设备。

操作

通常，最终用户和业务管理通过以下三种方式之一向操作中心和支持团队报告性能问题：

- 应用程序存在性能问题。
- 网络存在性能问题。
- 服务器存在性能问题。

“操作”页面使用简单、直接的方法直接处理性能问题的报告。在报告性能问题时，从报告问题的人员那里收集以下问题信息非常重要：

- 出现性能问题的应用程序和服务器的名称
- 最终用户、本地或远程办公室的位置和/或 IP 地址，以便于标识它们所在的网络
- 首先注意到时间性能问题，如果问题仍然存在
- 性能问题的历史记录 - 问题是否重复出现 - 一天几次、在不同天的同一时间、总是在月末？
- 用户认为可能关联的其他任何性能问题 - 其他应用程序或服务器速度慢

示例 1：应用程序的性能问题

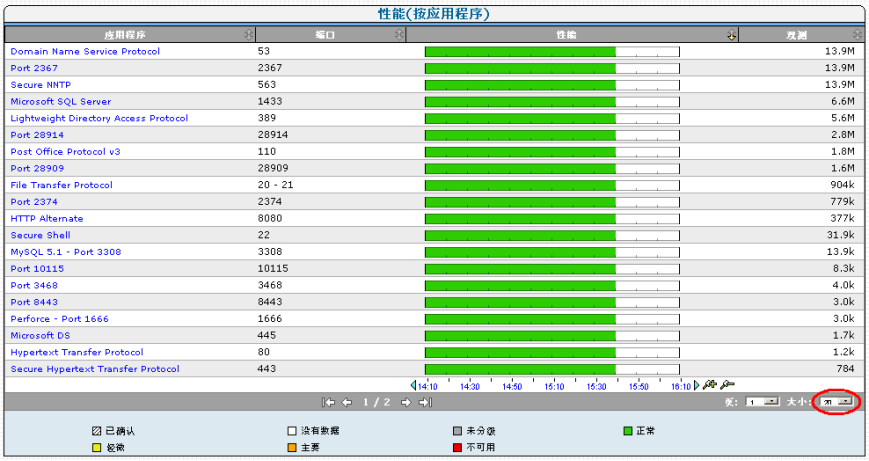
来自公司总部的用户报告，他们的应用程序出现问题。

方法

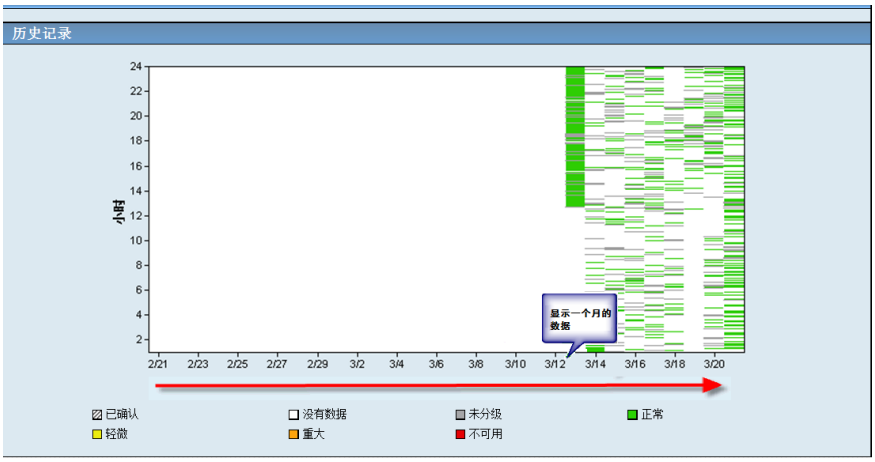
从用户搜集问题信息并创建故障单。

1. 单击“操作”页面。
2. 在“向我显示”菜单中，单击“应用程序”。

   将打开“性能(按应用程序)”页面。
3. 确定报告的应用程序是否已在列表中向上冒泡到顶部。通常它排在前十位之内。如果应用程序未出现在前 10 个位置，请将“大小”设置更改为更大的值，直到该应用程序出现在列表中。如果应用程序不在列表中，它可能不是由 CA Application Delivery Analysis 来监视。



4. 单击应用程序名称右侧的性能条，以显示详细信息页。从详细信息页中，可通过单击网络或服务器度量标准来缩小数据的范围。
5. 如果网络或服务器为已知，则可选择适当的性能条来进一步缩小范围。
6. 在“向我显示”菜单中，单击“历史记录”。
7. 查看应用程序的历史记录，以标识并指出任何不可用或性能降低的系统模式。



8. 在“向我显示”菜单中，您还可以单击“性能”，然后单击“浏览”开始进行故障排除。您也可以通过以下方法以便更彻底地排除故障：单击页面顶部的“工程”来显示“响应时间组成延迟”页面。请注意在页面顶部的查询选择框中选定的应用程序名称和服务器或网络名称。
9. 查看“响应时间组成: 平均”视图，并查明所报告问题的发生时间。识别哪个组成部分是那一刻最关键的因素。
   - 如果服务器响应时间 (SRT) 主宰这一刻，请参阅服务器响应时间增加 (p. 131)。
   - 如果网络往复传输时间 (NRTT) 和/或重传延迟主宰这一刻，请参阅网络往复传输时间 (NRTT) 增加 (p. 135)。
   - 如果数据传输时间主宰这一刻，请参阅数据传输时间增加 (p. 139)。
   - 如果与历史时间设置相关的所有组成部分均正常，那么问题可能存在于用户计算机上。

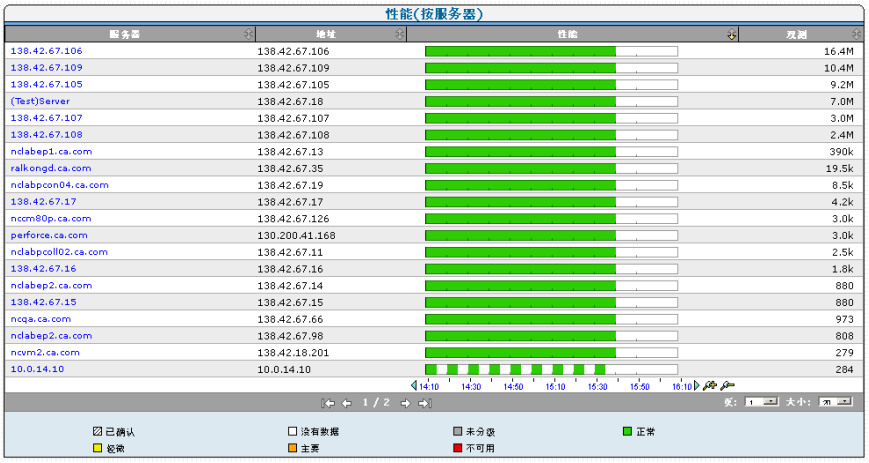
示例 2：服务器的性能问题

来自公司总部的最终用户报告，他们的服务器出现问题。

方法

从用户搜集问题信息并创建故障单。

1. 单击“操作”页面。
2. 向下滚动到页面中间，并查看“性能(按服务器)”视图。
3. 确定报告的服务器是否已在列表中向上冒泡到顶部。通常它排在前十位之内。如果服务器未出现在前 10 个位置，请单击“设置”并从“服务器列表”中选择该服务器。



4. 选择服务器名称右侧的性能条，以显示详细信息页。
5. 如果网络或应用程序为已知，则可选择适当的性能条来缩小范围。
6. 在“向我显示”菜单中，单击“历史记录”。
7. 查看服务器的历史记录，以标识并指明任何系统模式。
8. 在“向我显示”菜单中，您还可以单击“性能”，然后单击“浏览”开始进行故障排除。您也可以通过以下方法以便更彻底地排除故障：单击页面顶部的“工程”来显示“响应时间组成延迟”页面。请注意在页面顶部的查询选择框中选定的服务器名称和/或应用程序或网络名称。
9. 查看第一个视图“响应时间组成: 平均”视图，并查明在视图中报告发生问题的时间。识别哪个组成部分是那一刻最关键的因素。
   - 如果服务器响应时间 (SRT) 主宰这一刻，请参阅服务器响应时间增加 (p. 131)。
   - 如果网络往复传输时间 (NRTT) 和/或重传延迟主宰这一刻，请参阅网络往复传输时间 (NRTT) 增加 (p. 135)。
   - 如果数据传输时间主宰这一刻，请参阅数据传输时间增加 (p. 139)。
   - 如果与历史时间设置相关的所有组成部分均正常，那么问题可能存在于用户计算机上。

示例 3：网络的性能问题

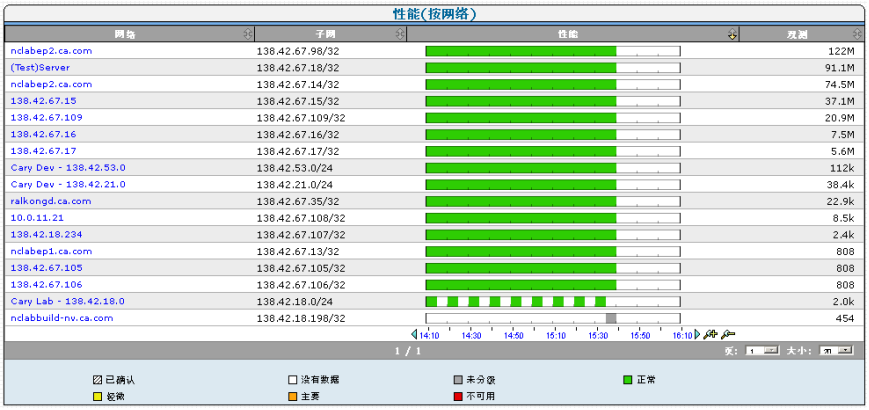
来自公司总部的最终用户报告，他们的特定网络出现问题。

方法

从用户搜集问题信息并创建故障单。

1. 单击“操作”页面。
2. 在“向我显示”菜单中，单击“网络”。

   将打开“性能(按网络)”视图。
3. 确定报告的网络是否已在列表中向上冒泡到前 N 个位置。如果网络未出现在前 N 个位置，请将“大小:”设置更改为更大的值，直到该网络出现在列表中。如果网络未出现在列表中，它可能不是由 CA Application Delivery Analysis 来监视。



4. 选择网络名称右侧的性能条，以显示详细信息页。从详细信息页中，可通过单击应用程序或服务器度量标准来缩小数据的范围。
5. 如果应用程序或服务器为已知，则可选择适当的性能条来进一步缩小范围。
6. 在“向我显示”菜单中，单击“历史记录”。
7. 查看网络的历史记录，以标识并指明任何系统模式或趋势。
8. 选择页面顶部的“链接: 工程”，以显示“响应时间组成延迟”页面。您应注意在页面顶部的查询选择框中选定的网络名称和/或服务器或应用程序名称。
9. 查看第一个视图“响应时间组成: 平均”视图，并查明在视图中报告发生问题的时间。识别哪个组成部分是那一刻最关键的因素。
   - 如果服务器响应时间 (SRT) 主宰这一刻，请参阅服务器响应时间和观测计数增加 (p. 131)。
   - 如果网络往复传输时间 (NRTT) 和/或重传延迟主宰这一刻，请参阅 NRTT 和观测计数增加 (p. 136)。
   - 如果数据传输时间主宰这一刻，请参阅数据传输时间和观测计数增加 (p. 139)。
   - 如果与历史时间设置相关的所有组成部分均正常，那么问题可能存在于用户计算机上。

调查

可以通过以下方式启动调查：

- 手动启动调查
- 排定调查
- 使用调查操作创建突发事件响应；在为与突发事件响应关联的项目打开突发事件时，会自动启动此类型的调查

要手动调查路由器、交换机或其他已启用 SNMP 的设备，可要求 CA Application Delivery Analysis 管理员将其添加为网络设备。

通过数据中心分析来自用户的数据流

为了帮助具有较差性能的用户进行诊断，可能要通过数据中心从用户设备中启动跟踪路由调查，以突出显示问题区域。

方法之一是导航到用户设备并从那里启动跟踪路由。使用管理控制台，可将用户设备添加到 CA Application Delivery Analysis 中，然后对该设备执行跟踪路由。

通过数据中心生成来自用户的数据流的报告

使用“操作”页面在性能较差的网络中查找用户。

1. 单击“操作”页面。
2. 在“向我显示”菜单中，单击“网络”。

   将打开“性能(按网络)”页面。
3. 单击网络名称，然后单击“浏览”。

   将打开“操作度量标准详细信息”页面。
4. 单击“受影响用户”选项卡。

   将显示用户报告。
5. 请注意包括 /24 或 /32 子网掩码的“IP 地址/掩码”字段。
6. 使用管理控制台的“管理”页面将相应的网络设备添加到 CA Application Delivery Analysis 中。
7. 使用管理控制台的“突发事件”页面启动跟踪路由调查。

标识受影响网络

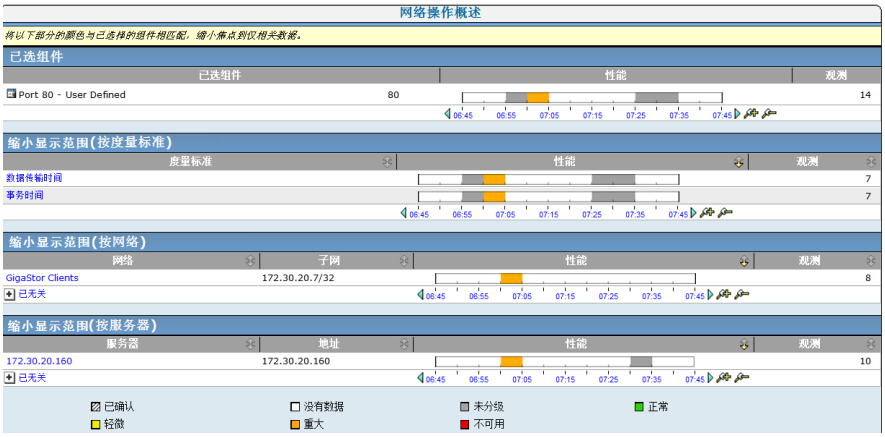
应用程序的性能可能会下降，并且会影响访问该应用程序的多个网络。

应用程序性能

在“操作”页面上，“性能(按应用程序)”报告会显示向管理控制台报告的性能最差的应用程序。要显示受性能下降影响的所有网络，请单击列表顶部的应用程序名称。

在向下浏览服务器和网络的图表时，您可以选择分级与“已选组件”页中的分级匹配的服务器和网络。例如，如果这是应用程序性能的视图：

单击此性能条，并在后续页面中查看“狭窄(按网络)”页面：



您可以轻松查看涉及的网络。

从服务器突发事件中标识受影响的网络

在发生服务器突发事件时，“突发事件”页面将显示该突发事件。要了解突发事件导致的影响，您可能需要知道：

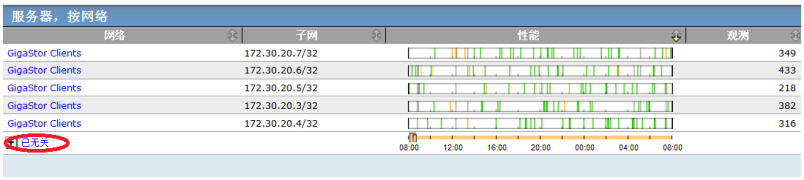
- 哪些网络和用户组受到了影响？
- 哪些特定用户受到了影响？
- 当突发事件发生时，系统的用户数有何变化？
- 对于特定站点，哪些用户受到了影响？

标识受突发事件影响的用户和网络

要查看受影响的网络和用户组，请执行以下过程：

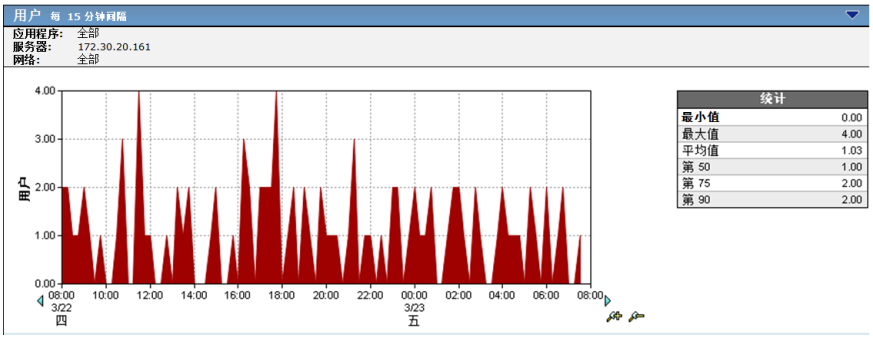
1. 在“服务器突发事件”页面上单击突发事件的链接，以显示有关该突发事件的更多详细信息：

2. 单击“已无关”链接旁的加号图标，以查看未受影响的网络：



3. 要了解受突发事件影响的特定用户，请单击“浏览”。
4. 单击“受影响用户”选项卡，以查看在发生突发事件时正在访问应用程序/服务器的所有用户的 IP 地址和主机名（如果可用）。
5. 关闭“受影响用户”报告并单击“链接: 工程”，以查看发生突发事件时的用户总数以及问题对用户量有何影响。

   将打开“组件报告”页面。
6. 在“向我显示”菜单中，单击“QoS”。
7. 向下滚动到“用户”视图，以查看一段时间内的用户数的可视表示。



8. 单击“设置”并选择网络，以查看特定网络上的用户。

确定网络对较差应用程序性能的影响

遵循这些步骤:

1. 单击“操作”页面。
2. 在“向我显示”菜单中，单击“应用程序”。

   将打开“性能(按应用程序)”报告。
3. 单击性能不佳的应用程序。该应用程序性能配置文件显示在下一页面的“已选组件”部分中。
4. 单击“设置”。在“设置”页面上的“度量标准”下，选择“所有网络度量标准”。
5. 从上往下浏览页面一直到“按网络精简”部分，查看运行该应用程序的网络。如果这些网络显示与应用程序类似的降级配置文件，那么说明网络也是关键因素之一。如果应用程序运行缓慢时网络显示性能正常，那么该网络则不是关键因素。
6. 或者，可以直接查看“操作概览”页面上的“网络(按性能)”报告，找出性能最差的那些网络。如果这些网络之一正在运行相关应用程序（单击网络时可以看到应用程序），则说明该网络是导致“按应用程序精简”列表中显示的性能不佳问题的关键因素之一。

确定导致应用程序性能下降的网络组件

请完成以下步骤：

1. 单击“操作”页面。
2. 在“向我显示”菜单中，单击“应用程序”。

   将打开“性能(按应用程序)”报告。
3. 单击性能不佳的应用程序。该应用程序性能配置文件显示在下一页面的“已选组件”部分中。
4. 单击“设置”。在“设置”页面上的“度量标准”下，选择“所有网络度量标准”。
5. 从上往下浏览页面一直到“按网络精简”部分，查看运行该应用程序的网络。如果这些网络显示与应用程序类似的降级配置文件，那么说明网络也是关键因素之一。如果应用程序运行缓慢时网络显示性能正常，那么该网络则不是关键因素。
6. 或者，可以直接查看“操作概览”页面上的“网络(按性能)”报告，找出性能最差的那些网络。如果这些网络之一正在运行相关应用程序（单击网络时可以看到应用程序），则说明该网络是导致“按应用程序精简”列表中显示的性能不佳问题的关键因素之一。

确定有性能问题的服务器的位置

在“操作”页面的“性能(按服务器)”视图中可以快速查看服务器性能问题。使用管理控制台进行排除故障有助于将问题源缩小到单个服务器。您可以：

- 根据视图的时间轴确定问题的*时间*
- 根据彩色段的宽度确定问题的*持续时间*
- 根据段的颜色确定问题的*严重度*
- 根据在相应的“性能(按网络)”视图中有多少网络显示类似的降级配置文件，确定问题的*普遍性*。

根据调查可以很明显地看出根本原因。管理控制台主要强调调查工作，以便您可以使用其他专门工具来快速找出根本原因。

为了帮助在企业网络中查找服务器，最佳做法是在管理控制台中以有意义的方式命名设备，如第三银行服务器、南部建筑服务器 C 等等。服务器场中的服务器可以包含公用标识符，Web 服务器应类似地进行命名，等等。

使用调查的 SNMP 查询

本节说明如何在“突发事件”页中使用 SNMP 性能调查。

情况 1 - 服务器突发事件

“服务器突发事件”在“突发事件”页的“概览”页中进行标识。

概述

确定突发事件已经打开的时间长度是非常重要的。“突发事件”持续的时间越长，可能受该问题影响的用户越多。在“突发事件”页面上，单击突发事件以显示其突发事件详细信息。查看“持续时间”字段中的数据。

还需检查“严重度”字段，以了解突发事件的最新状态。应尽快检查分级为“重大”的突发事件。如果突发事件已关闭，则性能下降不再发生，并且在一个重要时段已达到以前的正常性能级别。

单击突发事件编号以查看“详细信息”页面。

突发事件详细信息

对于分析，首先通过检查“服务器(按度量标准)”部分确定哪个度量标准导致了突发事件。在验证“服务器响应时间”度量标准（包括无响应和拒绝的会话）的下降时，SNMP 性能查询非常有用。

在“向我显示”列表中，单击“调查”以查看服务器或服务器组的关联的 SNMP 性能调查。

将列出与此突发事件关联的调查。SNMP 轮询调查类型使用主机资源 MIB 在服务器中查询 SNMP 性能度量标准。单击“查看”按钮以查看 SNMP 轮询数据。如果列表中没有 SNMP 轮询调查，请通过完成以下步骤启动一个。

SNMP 性能调查

在以下情况下，手动启动调查可能会很有帮助：

- 没有用于服务器突发事件的 SNMP 轮询
- 调查日期已过期（早于某一天）
- 分析中需要包括其他服务器

详细信息：

通过 SNMP 的性能调查 (p. 61)

分析 SNMP 性能数据

在显示服务器的 SNMP 性能报告之后，找到与发生的服务器突发事件类型对应的故障排除部分。

“服务器响应时间”或“服务器连接时间”突发事件分析

对于“服务器响应时间”或“服务器连接时间”突发事件，服务器对客户端请求的响应速度比正常情况慢。

CPU

查看服务器的 CPU 使用率。如果此值较高（接近 70% 到 100%），则检查占用 CPU 的进程。如果有某个进程占用了所有 CPU，则响应速度会变慢。这可能是因为并发用户太多或进程产生的 CPU 负载较大。要减少 CPU 使用率，可以重新启动该进程。这将终止用户执行的任何工作。如果这是一个非关键进程，请停止该进程。如果 CPU 使用率较低，则 CPU 不是导致此突发事件的问题。

内存

查看服务器的内存使用率；如果此值超过 70%，请检查占用内存的进程。响应速度慢可能是因为并发用户太多或进程存在内存泄漏。要减少内存使用率，请重新启动该进程。如果这是一个非关键进程，请停止该进程。如果 CPU 和内存的使用率都较低，那么典型的硬件约束不是问题所在。

接口统计

如果服务器的内存和 CPU 使用率都正常，那么可能是 NIC 出现问题，使得服务器响应变慢。检查接口统计。首先确保所有接口均已正确列出并已连接。确认 NIC 的接口速度和 IP 地址均已正确报告。双工不匹配错误将使接口无法发送和接收数据。双工不匹配错误、电缆问题或 CRC 错误将通过丢弃和错误字段指示 NIC 及其连接出现问题。

磁盘空间

检查驱动器的容量。由于用于存储数据的容量有限，服务器的速度会变慢。如果服务器的磁盘空间不足，则其处理数据的能力将下降。其他注意事项需要访问服务器，以检查错误段的分段或 I/O 错误。如果任何给定驱动器的可用空间少于 10-15%，则可能是使用大型工作数据集的应用程序存在问题。

“服务器被拒绝”或“无响应的会话”突发事件分析

如果您看到无响应或被拒绝的会话（服务器用完可用线程）以及到期的会话，则表示应用程序尚未发布这些资源。

对于“服务器被拒绝”或“无响应的会话”突发事件，表示服务器不会及时响应对新会话的请求。

排名靠前 CPU 进程或内存进程

在分析 CPU 资源时，请确保负责承载应用程序的进程正在运行。例如，在 SQL Server 的进程列表中，应在 CPU 或内存的进程中列出 sqlserver.exe。进程应当正在运行并且未消耗所有 CPU。如果 CPU 使用率较高（接近 70% 或 100%），请标识正在消耗 CPU 的进程。如果这是一个非关键进程，请停止该进程或重新启动它。该进程可能会被锁定或处于较差状态，这样会不必要地在对关键应用程序提供服务时占用处理能力。

如果内存使用率超过 80%，请标识正在消耗内存的进程。如果此进程不是关键性的，请停止该进程或重新启动它。该进程可能会被锁定或处于较差状态，这样会不必要地占用关键进程中的关键内存资源。如果正在消耗内存的进程很关键，则重新启动该进程应清除其内存缓存并使其正常重新启动。

磁盘空间

如果未列出预期进程，则可能由于磁盘空间限制而导致其失败。检查驱动器，以确保服务器有足够磁盘空间来启动应用程序。然后登录服务器，以确定进程是否正在运行并且能够启动。可能需要通过重新启动服务或进程来恢复连接。

接口统计

如果进程运行正常，则可能是 NIC 遇到问题，使得服务器速度变慢或不可用。检查接口统计。确保所有接口均已正确列出并已连接。

当 SNMP 数据看起来正常时，可以启动操作调查，其中包括：

- 查看活动会话的数目、Time_Wait 和服务器上的其他 TCP/IP 参数，以确保它们没有用尽 TCP 端口可用性。
- 将服务器连接时间与在远程办公室和服务器之间运行的其他应用程序进行比较，以查看增加是否全面。

情况 2 - 网络突发事件

您还可以为基础架构中的路由器和第 3 层交换机启动 SNMP 调查。对于此情况，会使用 TCP 跟踪路由调查启动 SNMP 性能调查。

在配置跟踪路由调查时，在“调查选项”下，务必将“通过 SNMP 调查路由器”设置为“是”，并为路径中的每个路由器添加网络设备。

详细信息：

跟踪路由调查 (p. 65)

分析 SNMP 跟踪路由数据

该报告会提供一个具有多个跃点的路由。对于详细分析，请选择具有最大延迟的跃点的性能统计。单击最右列中的“报告”图标。将在新窗口中打开路由器的 SNMP 性能报告。对于网络突发事件，按照清单所列内容确定网络问题的根本原因。

1. 检查设备的 CPU 和内存使用率。如果内存或 CPU 使用率较高，则可能是大型配置使路由器过载，或者过量的数据包处理使路由器负担过重。通常，当设备中充满错误数据包时，如果病毒爆发或 DDOS 攻击该设备，CPU 使用率将会提高。

   针对设备类型执行故障排除过程，以减少 CPU 或内存使用率，从而使性能级别恢复正常状态。

2. 确保所有接口均已正确列出，并且状态为“运行”。如果出现问题的接口已经故障转移到备用接口，请确保其速度相同。如果备用接口的速度较低，则网络延迟会增加，直到主接口恢复正常运行。

3. 确认接口未观测到任何丢弃或错误。如果报告发生了丢弃或错误，请登录路由器，并对接口连接进行故障排除，以便解决与接口的介质类型有关的问题。丢弃和错误通常表明接口与所连接的路由器或设备之间的连接存在问题。

4. 确保接口使用率未超过容量。每秒的接口进入位数必须小于线路分级。如果线路的使用率出现问题，请查看接口上的通信流，以确定导致突然拥塞的原因。

5. 如果设备按预期运行，则通过执行相同工作流来检查通过 SNMP 调查的其余跃点，以标识并解决受网络突发事件影响的最终用户与服务器之间的网络延迟的任何潜在问题。

性能和可用性 OLA 跟踪

运行水平管理 (OLM) 是受限制的主动式方法和过程，用于确保根据业务优先级以可接受成本向所有 IT 用户交付足够的运行水平。管理控制台中的运行水平协议 (OLA) 报告可以揭示是否满足运行水平。设置 OLA 所基于的公用性能度量标准包括：

- 服务器响应时间，用于量化数据中心的性能
- 网络往复传输时间，用于量化网络基础架构的性能
- 事务时间，用于捕获应用程序的端到端性能

因为经理需要高度概括性摘要报告来回答包括“我们是否满足目标？”在内的各种问题，因此性能执行 OLA 报告是可为每个应用程序快速回答该问题的冒泡式报告。可用性执行 OLA 报告整体显示对应用程序可用性目标的遵从性。通过单击这些摘要报告可以访问每日或每小时详细信息。

以有意义的频率生成 OLA 报告：

频率	说明
按天	非常详细，短期故障排除，关注 IT 部门，技术内容
按周	包含异常或趋势的其他详细信息的摘要，也关注 IT
按月	业务部门和执行管理的摘要；通常作为报告卡提供
每季度	使用合规性量化各种运行水平，并用作计划输入

在以下区域之一中通常可看到 OLA 违反：

- 时间，如一天中某一时刻或一周中某一天
- 用户组，如 VPN 用户网络
- 服务器；例如，Web 服务器 #2 和 #5

OLA 报告驱动器操作，以便改进性能。在这些区域中进行更改时，您可以看到 OLA 报告得到改进。

第 10 章： 分析

此部分包含以下主题：

影响分析

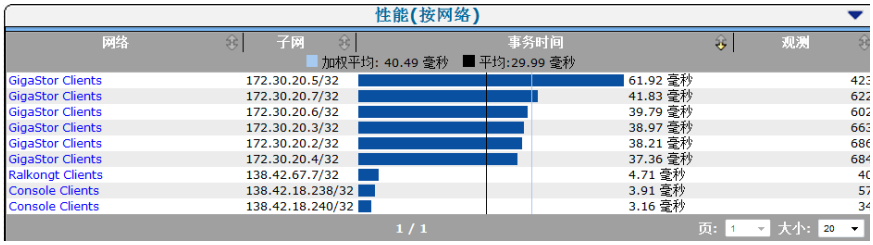
管理控制台使 IT 员工能够度量和验证基础架构更改的影响。下面提供了该分析方法的两个示例。

验证 QoS 策略实施

QoS 策略可以通过优先考虑关键应用程序通信量来改进远程用户的响应时间。此示例显示如何验证它的实际操作。在此示例中，策略是在昨天下午午餐之后实施的。

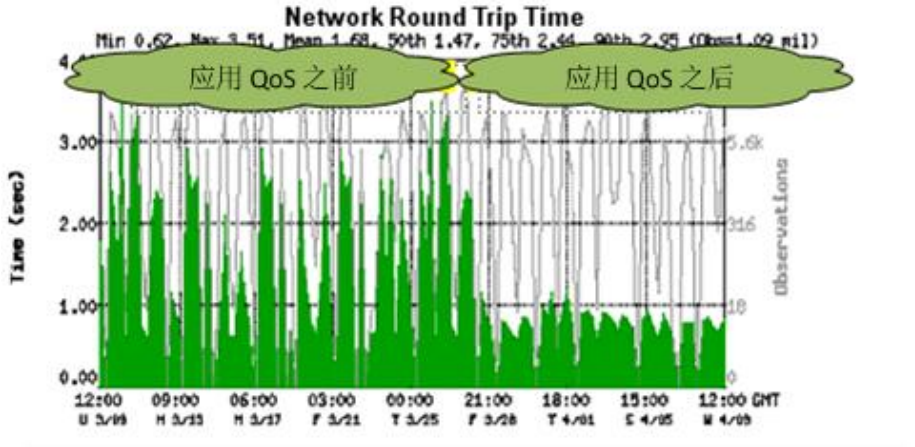
1. 单击“工程”页面
2. 在“向我显示”菜单中，依次单击“性能”和“网络”。
3. 单击“设置”并进行以下选择：
   - 时间范围：过去 24 小时
   - 度量标准：网络往复传输时间
   - 应用程序、服务器和网络：无选择
4. 单击“确定”。

   将显示以下报告：



每日“网络往复传输时间”的这一视图显示具有最高延迟的网络。56 K 和 VPN 连接通常表现为响应最慢。

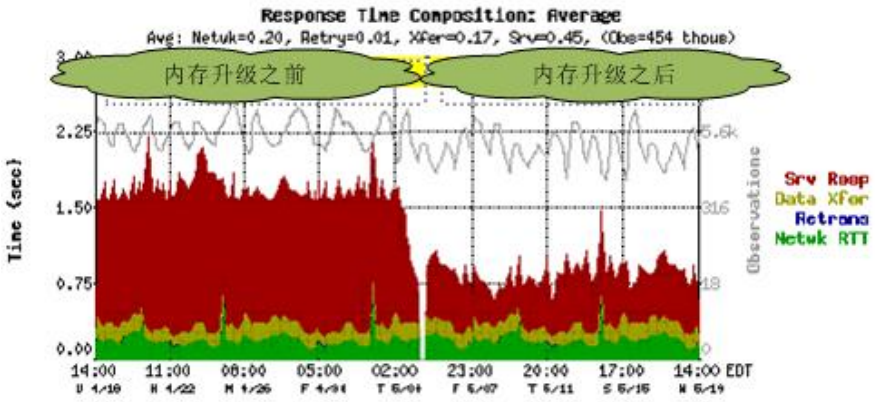
QoS 策略通过匹兹堡的 PA 链路来实施。“网络往复传输时间”视图中显示了 QoS 策略更改的效果。



在应用 QoS 策略之前的时间与实施策略之后的快速时间形成了鲜明的对比。

验证服务器内存升级

关于哪些元素需要升级，多层应用程序的响应迟缓会引起混乱。可能原因有后端数据库服务器过载或应用程序服务器的内存不足。使用管理控制台确定有效的解决方案。此示例介绍了升级应用程序服务器内存对总响应时间的结果。



趋势服务器响应时间

服务器响应时间 (SRT) 是服务器的“思考时间”，即在服务器接收客户端请求数据包的时刻与服务器将第一个响应数据包放在网络上的时刻之间经过的时间。SRT 受以下因素影响：

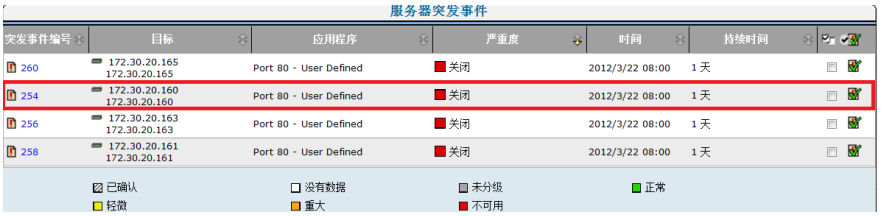
- 服务器硬件，例如 CPU 功率、可用内存、磁盘 I/O 以及 NIC I/O
- 应用程序行为，例如查询和索引优化以及应用程序算法
- 挂起或出故障的进程
- 使用率，或应用程序需要的处理能力

通常服务器硬件的速度越快、应用程序编写的越好、服务器使用率越低 - SRT 越低。SRT 值因服务器平台和应用程序而异。

下表中显示了“服务器响应时间”值的常规分级。除非指明，否则应用程序是单层的。

应用程序	极好	好	差
Citrix	50 毫秒	75 毫秒	200 毫秒
Citrix（2 层）	90 毫秒	125 毫秒	200 毫秒
CRM（2 层）	70ms	90 毫秒	200 毫秒
HTTP（Java，2 层）	120 毫秒	150 毫秒	250ms
HTTP（无 Java）	75 毫秒	90 毫秒	200 毫秒
Lotus Notes	50 毫秒	75 毫秒	200 毫秒
MS Exchange	50 毫秒	75 毫秒	200 毫秒
MS SQL	60ms	90 毫秒	150 毫秒
MS 终端服务	50 毫秒	75 毫秒	200 毫秒
MS 终端服务（2 层）	90 毫秒	125 毫秒	200 毫秒
Oracle	50 毫秒	75 毫秒	200 毫秒
其他	75 毫秒	90 毫秒	200 毫秒
其他（2 层）	90 毫秒	120 毫秒	200 毫秒

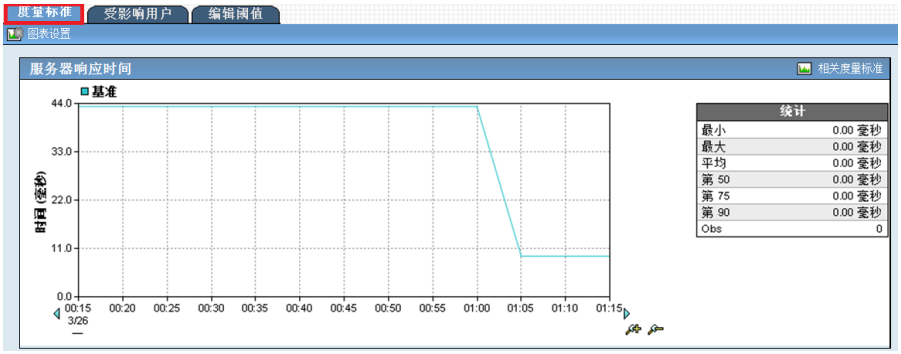
您可以确定“服务器响应时间”在一段时间内的趋势，以确定长期问题。诱发事件可能预示着进一步分析的机会。考虑“突发事件”页面中的以下服务器突发事件：



单击此突发事件的链接，以显示跨越阈值并启动该突发事件的度量标准的详细信息：

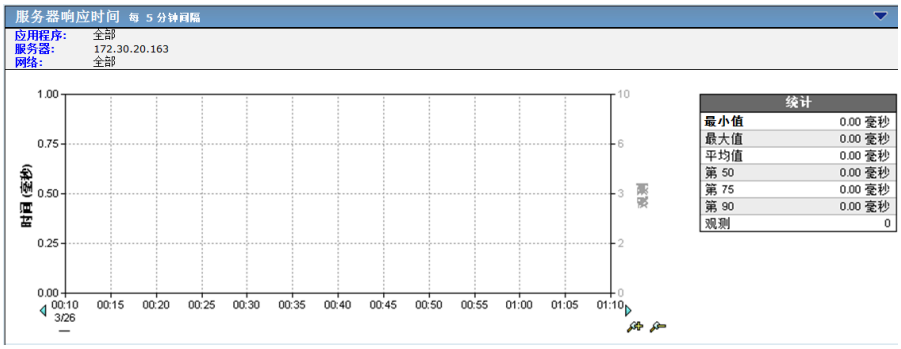
打开突发事件时的 5 分钟期间易于查看，引起它的度量标准是“服务器响应时间”。

单击标题中的“浏览”，以查看以下详细信息视图。此视图中显示的时间范围与上一页中相同。您可能想要查看，在此服务器和度量标准的长期视图中是否存在任何模式。在“工程”页面中提供了更长期限的视图。可将此窗口保持打开状态，以供参考。



单击标题中的“工程”链接，以显示以下视图。此视图与“突发事件”页面中的视图属于同一时间范围，因此看上去也相同。

要将时间范围更改为更长的期限，请单击页面顶部的“设置”。



还可以从“工程”页面的任何报告页中调查与该突发事件相关的其他度量标准。高度量标准（如拒绝的会话）指示服务器可运行，但太忙无法回答请求。

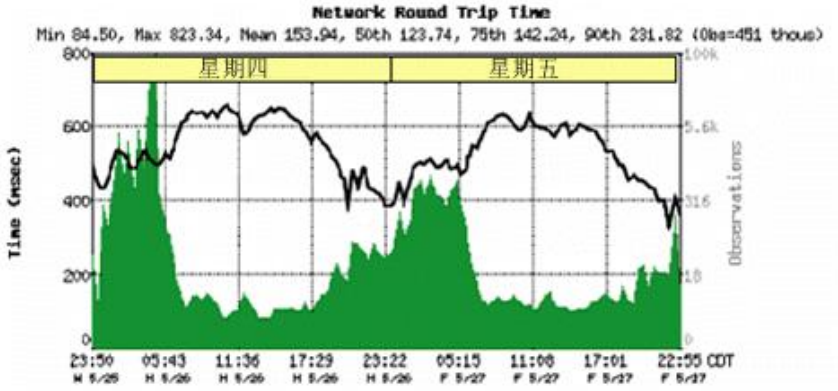
应用程序性能和数据量趋势

性能视图显示观测计数和度量标准度量。响应时间视图在左侧使用线性时间刻度，在右侧的 y 轴中使用对数观测计数刻度。甚至，观测计数略微增加或减少都会产生重要影响，因为它在对数刻度上。

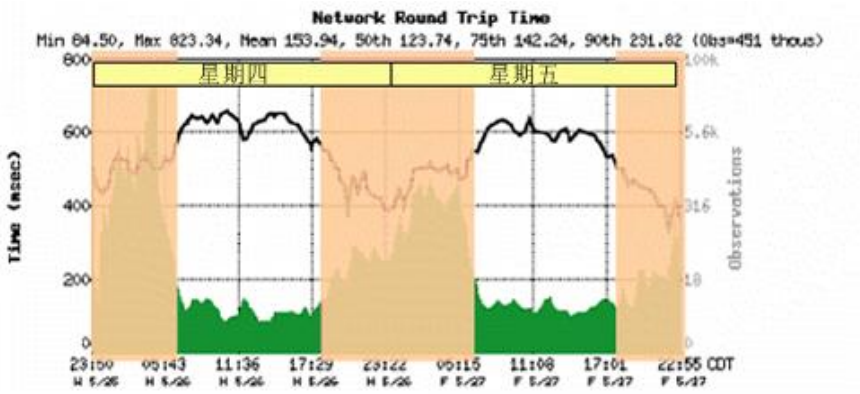
本节的性能视图中显示了随着网络往复传输时间 (NRTT) 和数据量的变化，用户所经历的性能。要查看度量标准中的趋势，请改变视图的时段。本节讨论对性能度量标准和数据量趋势的分析。

短期视图中的趋势

在以下性能视图中，可以看出工作日期间的运营模式很相似：

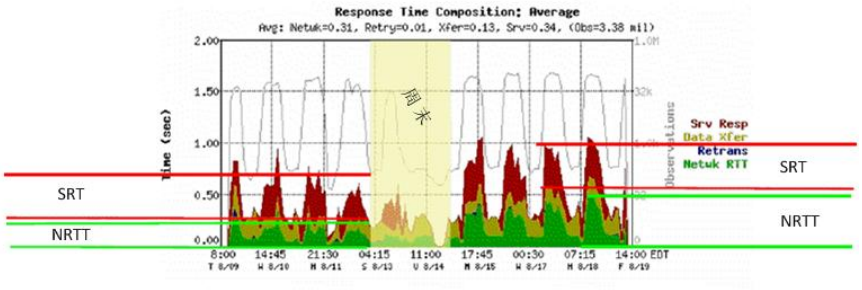


在高峰期间，高观测计数对应于低 NRTT，如图所示：



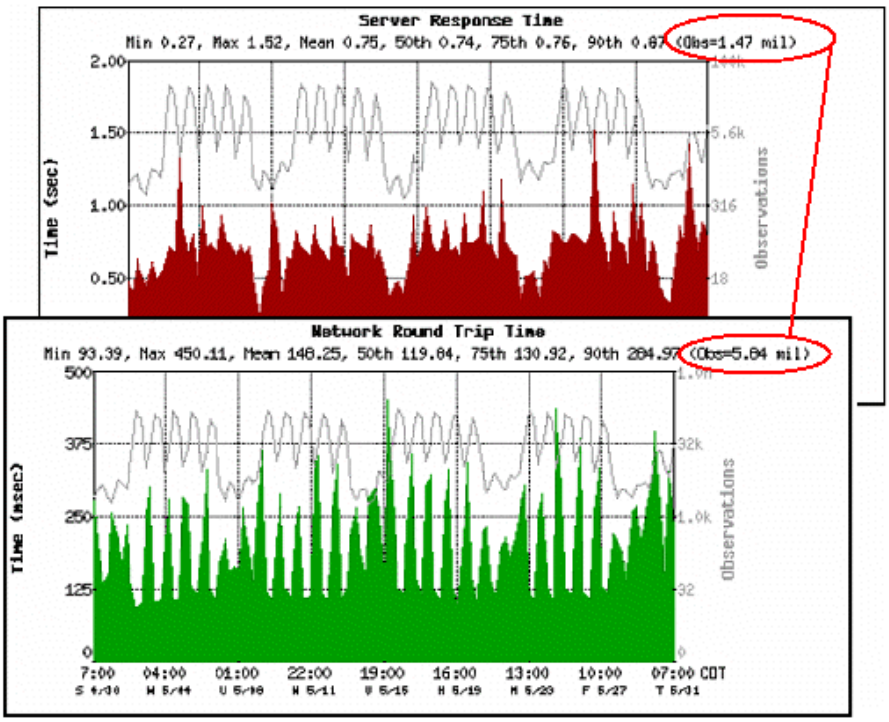
在非工作时间内，会出现相反的模式。原因为，海外用户在夜间访问应用程序，并且这些线路经历高延迟的 WAN 访问。针对每天的特定时刻或每周中的特定天计算的基准反映了这些常规模式。

还可以在下面的 10 天视图中查看每周模式。高峰期间高数据量导致 NRTT 和 SRT 更长。NRTT（绿色）部分在第二周比第一周大，而 SRT 部分则保持稳定。在整个时段内，此应用程序还有一个非常一致的观测模式。第二周中响应时间增加可能是因为网络更改或其他应用程序的使用发生了变化。

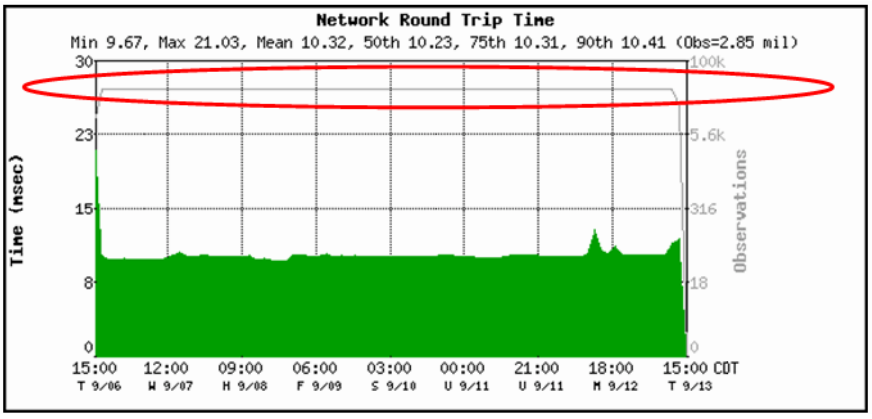


查看每月模式，您可以了解那些会影响容量规划的趋势。在下面的示例中，您可以看到，NRTT 观测数与 SRT 观测数的比约为 4:1。

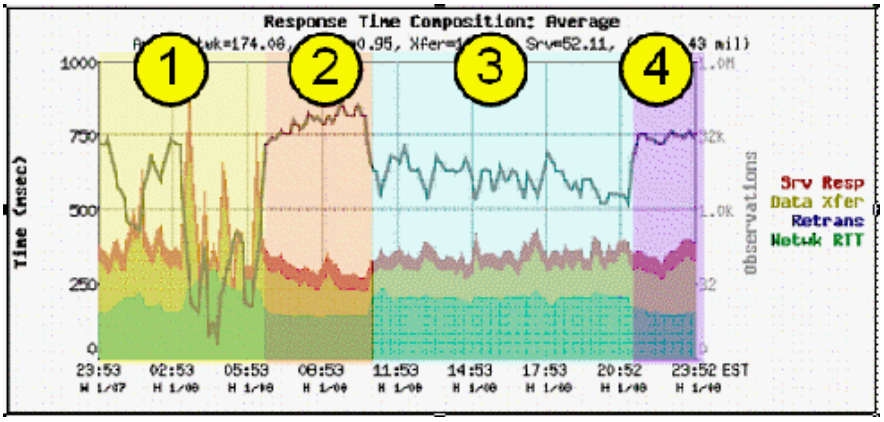
对于每个 TCP 事务，此应用程序平均需要往复传输约四次。跟数据往返量低的应用程序相比，那些数据往返量高的应用程序受网络性能下降的影响更大。



性能视图中平直的观测计数表明存在批处理进程或活动代理：



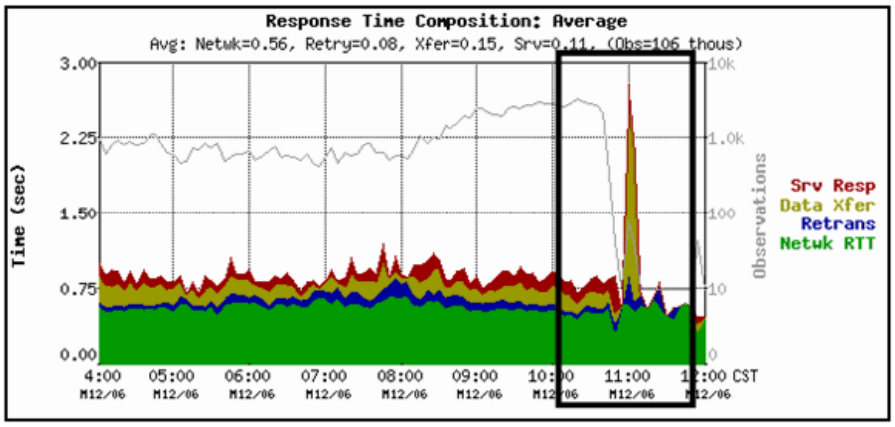
以下视图显示的是货运公司的包裹跟踪应用程序的每日模式。



该模式根据每日工作流形成：

1. 在深夜与清晨之间，会进行成批窗口脱机处理和备份。
2. 在早上装车时，会对包裹进行扫描。这会在模式的这一部分中产生高观测计数。
3. 送货操作发生变化，并显示稳定的系统响应。
4. 最后一部分反映卡车卸货活动。

下面的视图是一个反应应用程序故障的示例。观测计数显著减少。



不可用状态：分析可用性度量标准和突发事件

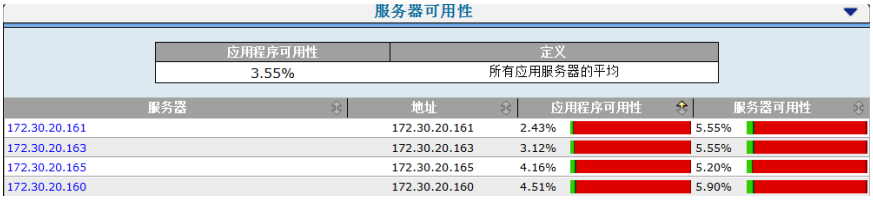
如果已启用可用性监视，管理控制台将同时监视应用程序和服务器的可用性。当服务出现中断时，可能是由这两者中的任何一方引起的。本节讨论浏览数据的方法。

1. 单击“工程”页面。
2. 在“向我显示”菜单中，单击“可用性”。

   将打开“应用程序可用性”报告。

3. 单击某个应用程序可看到承载该应用程序的主机。

   此时将打开“服务器可用性”报告。



4. 单击“应用程序可用性”列中的性能条可看到“可用性时间设置”报告。

   注意：应用程序可用性为 100%（绿色）时，“服务器可用性”视图可能会显示一些服务器不是 100% 可用的。要使应用程序可用，并不需要场中的每个服务器都可用。CA Application Delivery Analysis 管理员可以指定场中必须有多少台服务器可用应用程序服务器才会被视为可用。

5. 单击“相关突发事件”链接，可以从该视图中查看关联的突发事件。

使用性能记分卡

在“管理”页面上，单击“性能记分卡”。生成的“应用程序列表”页面将显示每月企业中应用程序的执行情况。“应用程序列表”页面使用以下彩色编码对性能分级：

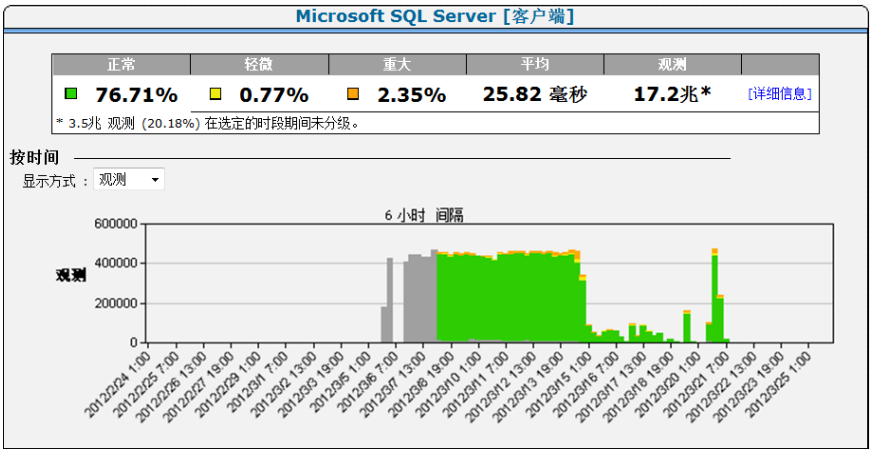
- 未分级（灰色）
- 正常（绿色）
- 轻微（黄色）
- 重大（橙色）

“应用程序列表”按观测数对每个应用程序的性能分级进行排序。

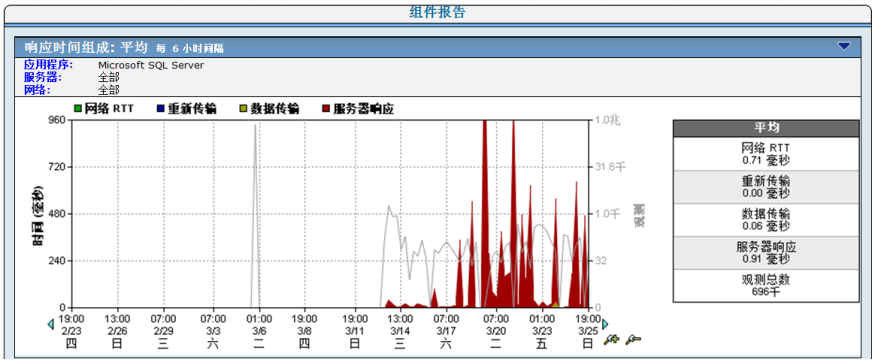
遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，单击“性能记分卡”。
3. 滚动到“应用程序列表”，并单击一个应用程序。
4. 单击“设置”，以更改报告设置。
5. 单击彩色编码的性能条或单击应用程序名称，可以获取有关哪些服务器和网络未与其对等方以相同方式执行的详细信息。

   应用程序的详细视图按时间间隔显示数据。选择按“观测数”还是“百分比”查看数据。
6. 在“向我显示”菜单中，依次单击“性能记分卡”、“网络”，可以按网络查看应用程序详细信息。
7. 在“向我显示”菜单中，依次单击“性能记分卡”、“服务器”，可以按服务器查看应用程序详细信息。
8. 单击“详细信息”，可以查看应用程序的“组件报告”。



将显示“组件报告”页面。



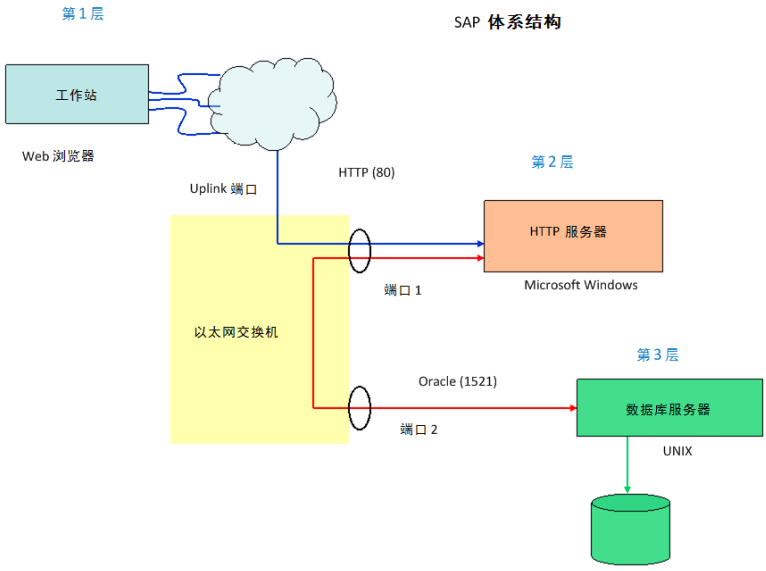
多层应用程序的性能

使用管理控制台查看多层应用程序中每层的网络、服务器和应用程序性能。监视多层应用程序并获取必要数据，以便将应用程序性能问题隔离到特定层以及每层中服务器、网络或应用程序的特定问题源。

了解多层应用程序操作

考虑一个由以下层构成的 N 层 SAP 体系结构：

- 第 1 层 - 在用户工作站上运行的 Internet Explorer
- 第 2 层 - 在 Windows Server 2003 上运行的基于 HTTP 的应用程序
- 第 3 层 - 在 UNIX 上运行的 Oracle 数据库服务器



此图演示了以下过程：

1. 用户使用 Internet Explorer 启动与第 2 层 HTTP 服务器的连接 - 在图中用蓝线标注。
2. 建立连接之后，用户请求应用程序数据。
3. HTTP 服务器将该请求转发至第 3 层 Oracle 数据库服务器 - 在图中用红线标注。
4. Oracle 服务器运行用户查询，并将结果返回到第 2 层 HTTP 服务器。
5. HTTP 服务器将数据发送回第 1 层客户端。

当 N 层应用程序出现性能问题时，由于在应用程序的各层之间进行了多次转接，因此将难以识别问题来源。从操作上看，当第 2 层等待第 3 层响应时，其性能取决于第 3 层性能。

分析多层应用程序的性能

使用管理控制台可以按照分析单层应用程序的相同方式来分析多层应用程序，但有两点不同：

- 低层应用程序的性能通常取决于高层应用程序的性能。
- 在报告每个层时，将上面的层设置为网络，将下面的层设置为服务器和应用程序。

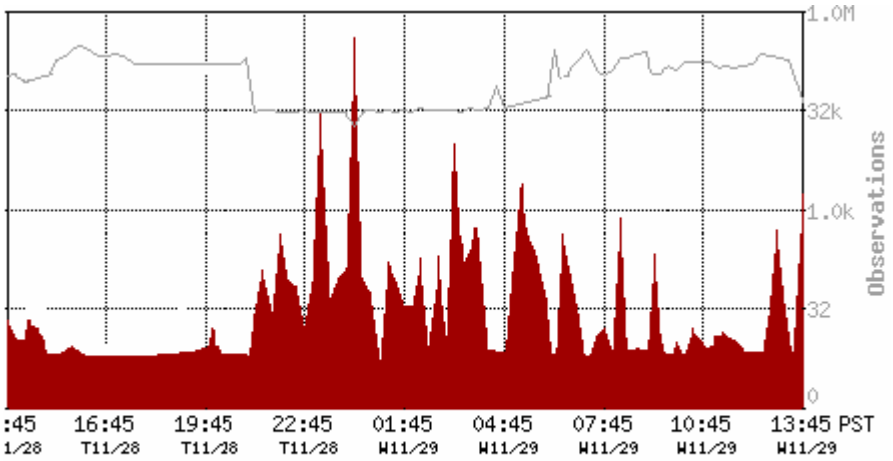
在前一部分的示例中，第 2 层 HTTP Web 应用程序的性能是第 3 层 Oracle 数据库服务器性能的函数。由此得出，第 N 层 HTTP Web 服务器在报告中显示为客户端，而第 N+1 层主机显示为服务器/应用程序。

在分析 N 层应用程序时，从最高层（距离最终用户最远的层）开始并向用户的方向前进。请注意相关层上的相关性能点的影响。各层之间的公共相关性能遵循可能的发生次序。

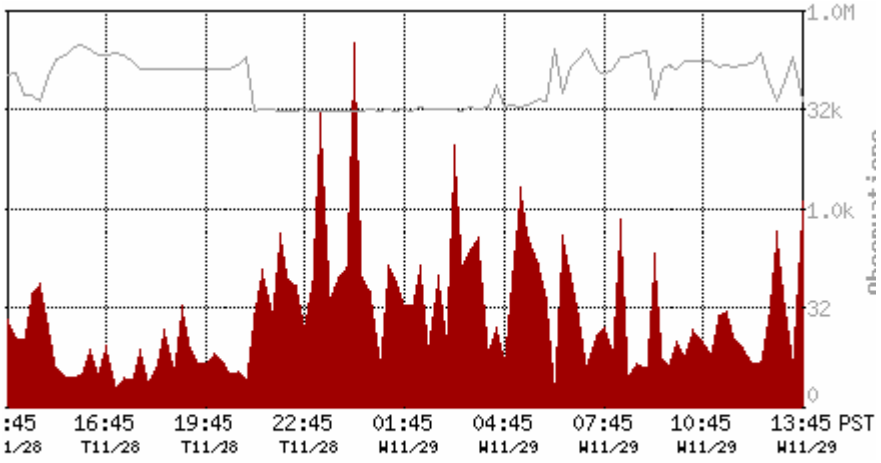
1. 第 N+1 层的服务器响应时间 (SRT) 会影响第 N 层的 SRT。
   - SRT 是服务器资源使用率的函数。该值较高表示，服务器可能没有足够的内存、CPU 或磁盘 I/O 资源来为给定负载的应用程序提供服务。
   - 查看会话和 QoS 视图，以确定哪些会话或用户在慢速 SRT 的实例期间对服务器施加了过多负载。
2. 第 N 层和第 N+1 层之间的网络往复传输时间 (NRTT) 很高，并且会影响数据吞吐量。
   - LAN 环境中的 NRTT 是交换机背板速度和交换机之间共享上行链路上带宽争用的函数。最佳实践是始终将 N 层应用程序的主 NIC 放在同一交换机上并在同一 VLAN 之内，以消除上行链路带宽争用问题，并取消服务器之间的两个额外的交换机跃点。这可以显著提高 N 层应用程序的性能。
   - 查看“通信量”和“数据量”视图，以确定 NRTT 是否随着数据量的增加而增加。如果是这样，则可能是两个服务器之间没有足够带宽用于应用程序。
3. 第 N 层和第 N+1 层之间的数据传输时间 (DTT) 恰好为零或趋向于零。查看“响应大小”和“数据传输时间(按响应大小)”视图，了解应用程序是否使用了大于 1.45 KB（适合一个数据包的数据量）的各种响应大小。DTT 为零或接近于零通常表示，后端办公室服务器正为每个用户请求发送单个数据包。对于数据库服务器，通常的形式是一次查询请求一行数据并执行多次，而不是在单次查询中请求所有行。可以重写查询以优化性能。
4. 第 N 层和第 N+1 层之间的重传时间表示显著的数据包丢失。
   - 查看“通信量”和“数据量”视图，以确定在高重传期间是否正在传输大量数据。

- 查看“会话”和“网络连接时间”视图，以确定 TCP 会话启动经历的延迟量。值较高表示这两层之间存在拥塞。

下图说明了应用程序体系结构中的第 2 层和第 3 层之间的“服务器响应时间”依存关系。在高响应时间期间，第 2 层服务器的 SRT 在第 3 层服务器的 SRT 之后。



Server Response Time - Tier 2



Server Response Time - Tier 3

这两层之间的尾部数据点表示第 3 层服务器性能会影响第 2 层服务器性能。第 3 层服务器是此应用程序体系结构中的瓶颈。

当第 N 层应用程序延迟与第 N+1 层应用程序延迟在高峰延迟期间具有相同的常规曲线时，第 N+1 层应用程序很可能对第 N 层应用程序产生了不利影响。

找出 N+1 层应用程序中的性能瓶颈（高 SRT 表示服务器存在问题；高 NRTT 和重传次数表示网络存在问题；以及 SRT 和 NRTT 偏低时零次或很多次数据传输通常表示应用程序存在问题）并更正相关问题后，请重复分析过程以找出其他次要瓶颈。

词汇表

“未分级”性能等级

*“未分级”性能等级*在管理控制台的“操作”页面上以灰色严重度状态指示，表示以往数据不足（需要两个完整工作日的数据），无法建立阈值；或者观测数不够，未超出最小观测数阈值。

“轻微”性能分级

*“轻微”性能分级*是在管理控制台中表示的一种严重度状态（黄色），用于表示度量标准值超出了“轻微”阈值。通过管理控制台可为“轻微”和“重大”性能降低设置阈值。

“重大”性能分级

*“重大”性能分级*是在管理控制台中表示的一种严重度状态（橙色），用于表示度量标准值超出了“重大”阈值。通过管理控制台可为“轻微”和“重大”性能降低设置阈值。

5 分钟摘要文件

CA Application Delivery Analysis Standard Monitor、Multi-Port Monitor、Virtual Systems Monitor、CA GigaStor 或 Cisco NAM 创建的 *5 分钟摘要文件*包括每个性能度量标准/应用程序/服务器/网络组合 (p. 185)的 5 分钟平均值。

ACK 数据包

在 TCP 连接设置期间，客户端会向服务器发送 *ACK 数据包*，确认收到来自服务器的 SYN-ACK 数据包 (p. 179)。

CA ADA Availability Poller 服务

*CA ADA Availability Poller 服务*检查应用程序的可用性。如果承载应用程序的服务器受 CA Standard Monitor 监视，则由该监视设备执行检查。否则，CA ADA Manager 上的 CA ADA Availability Poller 服务将检查该应用程序的可用性。

CA ADA Batch 服务

*CA ADA Batch 服务*可暂存 .dat 数据文件，以便通过 CA ADA Manager 上的 CA ADA Master Batch 服务进行处理。该服务在 CA Standard Monitor 上运行。

CA ADA Data Pump 服务

*CA ADA Data Pump 服务*在 CA ADA Manager 上执行每周数据库维护。

CA ADA Data Transfer Manager 服务

*CA ADA Data Transfer Manager 服务*基于 CA ADA Manager 上定义的应用程序、服务器和客户端网络同步 Cisco WAE 设备监视。此服务运行在 CA ADA Manager 上。

CA ADA Inspector Agent 服务

*CA ADA Inspector Agent 服务*针对应用程序、服务器及其相关网络启动调查。如果承载应用程序的服务器受 CA Standard Monitor 的监视，将从该监视设备启动调查。否则，CA ADA Manager 上的 CA ADA Inspector Agent 服务将启动调查。

CA ADA Inspector 服务

*CA ADA Inspector 服务*将 CA ADA Master Batch 服务处理的 5 分钟 .dat 文件加载到 CA ADA Manager 数据库中，并与 CA ADA Inspector Agent 服务进行通信以启动调查。此服务运行在 CA ADA Manager 上。

CA ADA Master Batch 服务

*CA ADA Master Batch 服务*在管理控制台上运行，可接收来自 CA Standard Monitor 上的 CA ADA Batch 服务的数据文件，用于处理成 5 分钟 .dat 文件。此服务运行在 CA ADA Manager 上。

CA ADA Messenger 服务

*CA ADA Messenger 服务*基于在 CA ADA Manager 上定义的应用程序、服务器和客户端网络同步任何分配的 CA Standard Monitor、CA Multi-Port Monitor 和 CA GigaStor 监视设备上的监视。此服务运行在 CA ADA Manager 上。

CA ADA Monitor Management 服务

*CA ADA Monitor Management 服务*响应 CA ADA Manager 的请求以传输 .dat 文件。该服务在 CA Standard Monitor 上运行。

CA ADA Monitor 服务

*CA ADA Monitor 服务*接收来自 CA ADA 监视设备的镜像 TCP 数据包和数据包摘要文件。该服务运行在 CA Standard Monitor 和 CA ADA Manager 上。

CA ADA Reader 服务

CA ADA Reader 服务在 CA GigaStor 上运行，可将由 TCP 标头构成的数据包摘要文件发送到分配的 CA ADA Standard Monitor 或 Multi-Port Monitor 以进行度量标准计算。

CA Application Delivery Analysis Manager (CA ADA Manager)

CA Application Delivery Analysis Manager (CA ADA Manager) 是 ADA 体系结构的组件，跨多个监视设备提供集中的配置、分析、管理和报告。CA ADA Manager 从分配的任何监视设备（包括 CA ADA Standard Monitor、Multi-Port Monitor、Virtual Systems Monitor、CA GigaStor 或 Cisco NAM）接收响应时间度量标准。

CA Observer Expert

CA Observer Expert 与 CA GigaStor 捆绑在一起。它融合了 CA ADA 的应用程序响应时间监视功能，还能够下钻到数据包级别数据以进行根本原因分析。

FIN 数据包

在 TCP 协议中，客户端使用 SYN 数据包与服务器建立 TCP 连接。同样，*FIN 数据包*用于开始销毁或终止 TCP 连接。监视设备在接收 FIN 或 RST 数据包时，便能确定某个 TCP 对话正在被终止。

NetQoS MySql51 服务

启动和停止承载 CA ADA Manager 数据库的 MySql 服务器。

OLA

*请参见*性能运行水平协议（性能 OLA） (p. 184)和可用性运行水平协议（可用性 OLA） (p. 180)。

Ping 响应时间与数据包大小调查

*Ping 响应时间与数据包大小*调查度量收到不同大小的 ping 请求（数据包）的 ping 回复所需的时间。该调查帮助跟踪各种数据包大小的过度延迟及缺少连接状况。CA ADA 管理员可以手动启动或排定此调查。

Ping 响应时间调查

*Ping 响应时间调查*是一项服务器突发事件响应 (p. 185)，用于度量在发送 ping 请求之后收到 ping 回复所需的时间，并采用“数据包往复传输时间”进行报告。CA Application Delivery Analysis 管理员也可以启动或排定该调查。

role

*角色*指定 CA ADA 管理控制台中显示给 CA ADA 用户的页面。

RST 数据包

RST 数据包是结束 TCP 会话的正常方式。Web 浏览器通常使用 RST 而不是 FIN 来结束会话。在连接握手期间，管理控制台将一个 RST 数据包计数为一个未实现的会话请求。如果监视设备在 TCP 三次握手完成之前看到 RST，则管理控制台会将会话视为被拒绝。

SNMP 配置文件

管理控制台使用 *SNMP 配置文件*来管理 SNMPv3 用户凭据以及 SNMPv1 和 SNMPv2 团体名称。SNMP 配置文件用于维护 SNMP 用户凭据，管理控制台需要使用这些凭据查询服务器或网络设备上的 SNMP 代理，并发送 SNMP 陷阱消息。

SNMP 陷阱通知

*SNMP 陷阱通知*是一种应用程序突发事件响应 (p. 183)、网络突发事件响应 (p. 182)或服务器突发事件响应 (p. 185)，用于向 SNMP 管理器通知受影响的应用程序、服务器或网络的“打开”或“已关闭”突发事件状态。

SPAN

Switched Port Analyzer (SPAN) 又称端口镜像，在 Cisco 网络交换机上用于将一个交换机端口上观测到的所有网络数据包的副本发送到另一个交换机端口上的网络监视连接。网络设备通常使用该技术来监视网络通信量。SPAN 使监视设备能够在一个或多个交换机端口上查看多个广播域中发生的通信。SPAN 的功能根据机箱的不同而异。

SYN 数据包

在 TCP 协议中，客户端与服务器之间的对话（连接）是通过三次握手建立的。客户端会向服务器发送 *SYN 数据包*来启动连接设置。监视设备使用 SYN 数据包对网络中的受监视连接进行计时和分析。

SYN-ACK 数据包

在 TCP 连接设置期间，服务器会向客户端发送 *SYN-ACK 数据包*，确认收到来自客户端的 SYN 数据包 (p. 179)。监视设备使用 SYN-ACK 数据包对网络中的受监视连接进行计时和分析。

WAN

广域网 (WAN) 是通常覆盖了大型多样化区域的网络，该区域由多个局域网 (LAN) 组成。WAN 可以是专用的，由单个企业的不同办公室使用；也可以是公共的（如 Internet）。

WAN 优化设备

*WAN 优化设备*可通过压缩或其他算法，减少数据中心与远程办公室之间传输的通信量。例如，Cisco WAE 设备和 Riverbed Steelhead 设备就是 WAN 优化设备。

三次握手

在 TCP 协议中，使用*三次握手*来建立客户端与服务器之间的连接。客户端会向服务器发送 SYN 数据包 (p. 179)来启动连接设置。服务器向客户端发送一个 SYN-ACK 数据包 (p. 179)来确认收到来自客户端的 SYN。最后，客户端向服务器发送一个 ACK 数据包 (p. 176)来确认收到来自服务器的 SYN-ACK 并建立 TCP 连接。监视设备使用三次握手对网络中的受监视连接进行计时和分析。

已分段数据包

*已分段数据包*是遍历网络时被拆分成多个数据包的数据包。

已丢弃数据包

*已丢弃数据包*是 CA Standard Monitor 上的数据包捕获驱动程序或 CA GigaStor 上的 GigaStor 连接器未分析的数据包，这是因为监视设备过于繁忙而无法处理其接收的所有数据包。如果监视设备丢弃太多数据包，管理控制台将创建“重大”监视设备突发事件。管理控制台不监视服务器交换机端口或监视设备中监视器 NIC 上的数据包丢失。

分流器

请参阅网络分流器 (p. 181)。

分配层

在典型的 3 层 LAN 网络（接入、分配、核心）中，*分配层*是路由、筛选和策略管理发生的位置。该层通常包括路由器和第 3 层交换机。当接入交换机向分配层发送数据时，就会收集数据。可以在该层看到一些服务器间的通信，只要这些服务器位于不同的交换机上。

无响应会话百分比

*无响应会话百分比*是一个服务器度量标准 (p. 185)，用于度量连接请求已发送但服务器未响应的会话的百分比。该度量标准是“未实现的 TCP/IP 会话请求”视图的一部分。

可用性运行水平协议（可用性 OLA）

*可用性运行水平协议（可用性 OLA）*报告应用程序可用的时间百分比。例如，应用程序一个月期间在服务器上必须有 99% 时间可用。

电子邮件通知

*电子邮件通知*是应用程序突发事件响应 (p. 183)、服务器突发事件响应 (p. 185)或网络突发事件响应 (p. 182)，用于通知收件人有关受影响的应用程序、服务器或网络的阈值违反的信息。

丢弃的数据包

*丢弃的数据包*是监视设备有意丢弃的数据包，丢弃的原因是该数据包与管理控制台中指定的应用程序、服务器和客户端网络的列表不匹配。

同步监视设备

*同步监视设备*可以根据管理控制台中的当前客户端网络、服务器子网和应用程序定义监视 TCP 会话。为了确保同步期间最小化对监视的临时中断，请在同步监视设备之前完成所有更改。

多层应用程序

*多层应用程序*是在多台服务器上运行的应用程序，服务器之间的通信由至少一台服务器执行 - 该服务器既充当客户端请求的服务器，又充当其他服务器的客户端。

有效网络往复传输时间

*有效网络往复传输时间*是包括网络往复传输时间 (p. 182)和重传延迟 (p. 186)的网络度量标准 (p. 182)。请注意，重传延迟并不是由于重新传输导致的延迟，而是每次往复传输的平均重传延迟量。尤其值得注意的是，管理控制台增加了两个平均值，实际上是将两个度量标准组合在了一起。

权限集

用户有权查看的应用程序、服务器和网络聚合的已定义列表。一个聚合可以是一个或多个权限集的成员。

网络分流器

*网络分流器*是一种硬件设备，可让您访问流经计算机网络的数据。部署分流器后，您可以将监视设备连接到分流器，而不会影响受监视的网络。使用分流器，可查看两个方向（上游和下游）发生的通信量，不过仅限于交换网络中的一个广播域。

网络区域

*网络区域*是一种管理控制台工具，用于将一个广泛的子网定义自动扩展成若干个更窄的子网。您可以定义一个最多包含 256 个区域的网络，例如，可以定义一个包含 256 个区域的 /16 网络，这就相当于定义了 256 个 /24 网络。如果您使用网络区域，管理控制台将报告更窄的网络区域子网定义而不是更广的网络定义。

网络连接时间

网络连接时间 (*NCT*) 是一个网络度量标准 (p. 182)，用于度量从服务器发出 Syn-Ack 到从客户端再收到 Ack 所需的时间。在网络未被阻塞时，它是对网络延迟的一种度量，表示由于距离和序列化产生的最小延迟，也是网络体系结构中最佳的往复传输时间。该值的突发峰值通常是由于网络拥塞引起的，而停滞（上升后停止不动）通常意味着路径更改。

网络往复传输时间

*网络往复传输时间*是一个网络度量标准 (p. 182)，用于度量数据包在网络上的服务器和客户端之间双向传输所花的时间，不包括丢失的数据包。不包括应用程序、服务器以及客户端处理时间。

网络度量标准

*网络度量标准*表示某个应用程序性能问题是由当时与该应用程序通信的网络导致的。使用 CA Application Delivery Analysis 管理控制台，可以为以下每个网络度量标准自定义性能阈值：网络往复传输时间 (p. 182)、网络连接时间 (p. 182)、有效网络往复传输时间 (p. 181)和重传延迟 (p. 186)。

网络突发事件

如果在 5 分钟间隔内，应用程序/服务器/网络的特定组合超出了某个网络度量标准的阈值（如“网络往复传输时间”、“网络连接时间”、“有效往复传输时间”或“重传延迟”），管理控制台将创建一个*网络突发事件*。

网络突发事件响应

*网络突发事件响应*是 CA ADA 对网络突发事件 (p. 182)做出的响应。CA ADA 管理员可以将电子邮件通知 (p. 181)、SNMP 陷阱通知 (p. 179)和跟踪路由调查 (p. 190)分配给网络突发事件。

网络类型

共享相同的应用程序物理访问权限的一组网络。例如，远程站点内的所有子网都共享同一 WAN 链路来访问数据中心。

观测计数

观测计数度量监视设备在 5 分钟监视间隔期间计算特定应用程序/服务器/网络组合的性能度量标准的次数。在 TCP 事务内，对于不同的度量标准，可以有不同的观测数。例如，与服务器响应时间相比，网络往复传输时间可能有更多观测计数。其他度量标准是一些链接，它们始终具有相同的观测数。例如，每个 TCP 事务有一个服务器响应时间观测和一个数据传输时间观测。要将度量标准分级为“正常”、“轻微”（黄色）或“重大”（橙色），该度量标准必须具有最小的观测数。

设备

*设备*可以是连接到受监视网络的任何 TCP/IP 系统。

严重度

严重度在某个时段内根据建立的阈值将性能数据分级为“无”、“未分级”、“轻微”、“重大”和“不可用”。

应用程序

*应用程序*指定了要跨一系列服务器 IP 地址监视的 TCP 端口或端口范围，如跨 /29 服务器子网的 TCP-80 通信量。

应用程序连接时间调查（术语）

*应用程序连接时间调查*是一种应用程序突发事件响应 (p. 183)，它向 IT 工作人员提供所需的信息来确定连接到某个 TCP/IP 应用程序端口需要多长时间。这包括服务器通过连接确认来响应的时间。CA ADA 管理员还可以启动或排定此调查。

应用程序突发事件

当网络事件或服务器事件影响应用程序的性能时，应用程序突发事件就会发生。

主要的网络突发事件或服务器突发事件导致应用程序的组合度量标准超过性能阈值时，组合度量标准的阈值便会被超过。

组合度量标准超过阈值时，管理控制台将对应用程序的性能影响分级为“重大”（橙色）或“轻微”（黄色），但不会创建应用程序突发事件响应。您必须定义应用程序的主要网络或服务器突发事件发生时要启动的应用程序突发事件响应。

应用程序突发事件响应

*应用程序突发事件响应*是对网络突发事件 (p. 182)或服务器突发事件 (p. 185)的应用程序响应。例如，如果您为 Exchange 应用程序配置了应用程序突发事件响应，则当访问该 Exchange 应用程序的客户端创建了网络突发事件，或者承载该应用程序的服务器创建了服务器突发事件时，管理控制台就会启动该突发事件响应。超出某个综合度量标准 (p. 189)（如数据传输时间）的阈值时，管理控制台不会启动应用程序突发事件响应。管理控制台允许您向应用程序分配以下响应：电子邮件通知 (p. 181)、SNMP 陷阱通知 (p. 179)和应用程序连接时间调查 (p. 183)。

报告页面

管理控制台在针对特定类型的用户（如操作人员、主管和工程师）设计的标准*报告页面*下组织报告数据。

事务

*事务*是某个 TCP 请求和所有后续响应。一个应用程序事务（如加载 Web 页面）可以包括多个 TCP 事务。

事务处理时间

*事务时间*是一个综合度量标准 (p. 189)，用于度量从客户端发送请求到收到响应中最后一个数据包的使用时间。“事务时间”是服务器响应时间 (p. 185)、网络往复传输时间 (p. 182)、重传延迟 (p. 186)和数据传输时间 (p. 190)之和。当超出“数据传输时间”阈值时，管理控制台不会打开一个突发事件。

到期的会话

*到期的会话*度量 CA ADA Monitor 服务在其中看不到 TCP 会话关闭 (teardown) 指令（FIN 或 RST 数据包）的 TCP 会话的数目。在一段时间内不活动的会话将从内存中清除，并标记为“已到期”。如果在 15 分钟时段内观测不到任何数据包，管理控制台就会将会话分类为“已到期”。如果有过多的已到期的会话保持为打开状态，则可能会导致服务器无响应。

性能运行水平协议（性能 OLA）

性能运行水平协议（性能 OLA）用于评估对远程站点上的应用程序性能目标的遵从性。默认情况下，管理控制台没有针对应用程序性能定义运行水平。

性能阈值

性能阈值是默认情况下每个应用程序都存在的可接受性能行为的边界。阈值使管理控制台能够对数据分级。它们会促进突发事件创建、突发事件响应和调查。

服务器子网

服务器子网标识每个监视设备监视的一系列连续服务器 IP 地址。在定义应用程序时，您可以向应用程序分配特定的服务器子网，使管理控制台能够自动监视一系列连续服务器 IP 地址中的应用程序性能。

服务器连接时间

服务器连接时间 (SCT) 是一个服务器度量标准 (p. 185)，用于度量服务器通过发送 Syn-Ack 来响应客户端的 SYN 数据包，从而确认初始客户端连接请求所需的时间。

服务器响应时间

*服务器响应时间*是服务器度量标准 (p. 185)，用于测量服务器发送对客户端请求的初始响应或发送初始服务器思考时间所花费的时间。服务器响应时间增加通常表示缺乏服务器资源（如 CPU、内存、磁盘 I/O）、应用程序编写的糟糕或多层应用程序中某层性能不佳。

服务器度量标准

*服务器度量标准*将指明应用程序性能问题是由承载应用程序的服务器所导致的。使用 CA ADA 管理控制台，可以为以下每个服务器度量标准自定义性能阈值：服务器响应时间 (p. 185)、服务器连接时间 (p. 185)、被拒绝会话百分比 (p. 187)和无响应会话百分比 (p. 180)。

服务器突发事件

如果在 5 分钟间隔内，应用程序/服务器/网络的特定组合超出了某个服务器度量标准（如“服务器响应时间”、“服务器连接时间”、“被拒绝会话百分比”或“无响应会话百分比”）的阈值，管理控制台将创建一个服务器突发事件。

服务器突发事件响应

*服务器突发事件响应*是管理控制台对服务器突发事件 (p. 185)做出的响应。管理控制台允许您向服务器突发事件分配以下响应：电子邮件通知 (p. 181)、SNMP 陷阱通知 (p. 179)、Ping 响应时间调查 (p. 178)、通过 SNMP 的性能调查 (p. 187)和数据包捕获调查 (p. 189)。

组合

*组合*标识 CA ADA 用于计算响应时间度量标准的时间范围、应用程序端口、服务器、网络和性能度量标准。例如，管理控制台可以报告过去 24 小时与开发客户端网络进行通信的所有应用程序和服务器的平均“网络连接时间”。

保持连接消息

持久建立 TCP 连接并使其保持活动状态，而不是为每个请求/响应都建立新的 TCP 连接的一种方法。TCP *保持连接消息*使用已知的格式，且不会偏离响应时间度量标准。递增序号并包含负载的应用程序保持连接可能会偏离某些服务器度量标准（例如服务器响应时间 (SRT)）的度量。

响应操作

响应操作（如发送通知或启动调查）是对性能阈值违反做出的响应。

度量标准摘要文件

*度量标准摘要文件*包含 Cisco NAM 提供的预先计算的响应时间度量标准。CA ADA Manager 从 Cisco NAM 接收度量标准摘要文件。

突发事件

当应用程序、服务器或客户端网络在某段时间出现异常行为时，管理控制台将会打开一个*突发事件*以提醒用户注意。请参阅响应操作 (p. 186)。

突发事件响应

在发生问题时，*突发事件响应*可帮助您对问题进行故障排除，并有助于减少平均修复时间。向关键业务应用程序、服务器和网络分配突发事件响应。突发事件响应会通知您的团队出现了性能下降的情况，并让他们积极调查问题，以收集更多信息来帮助标识性能下降的根本原因。

重传延迟

*重传延迟*是一个网络度量标准 (p. 182)，用于度量从发送原始数据包到发送最后一个重复数据包使用的时间。管理控制台报告的“重传延迟”是整个观测的平均值，而不仅仅是针对重传的数据包。例如，如果一整套 10 个数据包需要 300 毫秒重传时间，则报告的重传延迟为 30 毫秒（300 毫秒/10 个数据包）。

核心层

在典型的 3 层 LAN 网络（接入、分配、核心）中，*核心层*可以实现分配层设备的高速互连。核心层通常拥有最高的互连速度，并拥有网络中功能最为强大的路由器和交换机。一般而言，只能在该层看到客户端与服务器之间发生的事务。

监视设备

*监视设备*可监视 TCP 事务并计算应用程序、服务器和网络响应时间度量标准。

监视设备突发事件

如果违反了监视设备的性能和可用性阈值，管理控制台将创建*监视设备突发事件*。例如，当某个设备不可访问、设备检测不到数据或者设备丢弃了数据包时。

监视单位

*监视单位*是通过添加监视设备而在 CA ADA Manager 上创建的处理负载。例如，一个 CA Standard Monitor 使用一个监视单位。CA ADA Manager 最多可支持 15 个监视单位。

监视器源

*监视器源*是响应时间信息的源，如 CA Standard Monitor。

被拒绝会话百分比

*被拒绝会话百分比*是一个服务器度量标准 (p. 185)，用于度量在报告间隔期间，服务器显式拒绝的连接请求的百分比。该度量标准是 CA ADA 管理控制台中“未实现的 TCP/IP 会话请求”报告的一部分。

调查

*调查*是指主动地深入查询应用程序、网络和服务器上特定的性能数据。管理控制台可自动启动调查来响应某个突发事件。CA ADA 管理员还可以启动或排定调查。

通过 SNMP 的性能调查

*通过 SNMP 的性能调查*是一种服务器突发事件响应 (p. 185)，其使用 SNMP 轮询服务器以获得性能信息，例如 CPU 和内存使用率。CA ADA 管理员还可以启动或排定此调查。

预计跃点延迟

*预计跃点延迟*是两个节点之间存在的延迟时间的预计值。管理控制台通过使用所有样本的平均值来确定此预计值（例如，在跟踪路由调查 (p. 190) 期间）。

域

*域*分隔客户端 IP 通信以进行报告，并标识管理控制台用于解析服务器主机名的 DNS 服务器。

基准

使用*基准*可以查看网络中正常性能的历史记录。管理控制台会自动报告服务器上应用程序端口与客户端网络之间的所有 TCP 会话的基准。使用基准可将应用程序的当前性能与以往性能的历史平均值进行比较。超出基准不一定表示出现了问题。基准按小时计算，并考虑一天中的小时、星期日期和月份日期。

接入层

在典型的 3 层 LAN 网络（接入、分配、核心）中，*接入层*是最靠近服务器的层，它将服务器连接到网络。交换机和集线器通常属于接入层。通常，可以在该层看到所有服务器通信，但这需要最多的监视点。

控制端口应用程序

控制端口应用程序使用两个 TCP 端口。控制端口负责发送和接收请求信息，数据端口负责发送和接收实际数据。同一监视设备必须同时监视控制端口和数据端口通信量，才能确定事务响应时间。任何类型的监视设备均可监视控制端口应用程序。

敏感度级别

*敏感度级别*是一个无单位度量值，值的范围是 0-200，应用于一个专用公式，该公式基于历史数据计算每个客户端、服务器和应用程序组合的新阈值。管理控制台使用过去 30 天的百分位统计，在每个午夜 (GMT) 自动生成度量标准的新阈值。对于从每个客户端网络访问应用程序的用户，管理控制台会自动生成一组单独的阈值。

综合度量标准

*综合度量标准*将指明应用程序性能问题是由承载应用程序的服务器还是当前与该应用程序通信的网络再或是二者共同所导致的。CA ADA 管理控制台将为以下每个综合度量标准设置性能阈值：数据传输时间 (p. 190)和事务时间 (p. 184)。请注意，管理控制台不会创建应用程序突发事件。但是，由于综合度量标准既包括网络度量标准，又包括服务器度量标准，因此管理控制台可以将服务器或网络分级为“轻微”（黄色）或“重大”（橙色），并分级对应用程序自身性能产生的相应影响。例如，如果服务器度量标准分级为“轻微”，则管理控制台还可将应用程序的综合度量标准分级为“轻微”。

跃点

*跃点*是网络中两个网关之间的逻辑链路。通常，当数据包遍历网络时，将通过一个或多个路由器或网关。任何两个逻辑邻接的网关之间的路径被视为“*跃点*”。

阈值

请参阅性能阈值 (p. 184)。

数据包丢失百分比

*数据包丢失百分比*是一个网络度量标准 (p. 182)，从临近服务器的监视设备有利位置度量重传数据占网络中总数据的比率。监视设备可以观测到由于网络路径中服务器到客户端方向上发生数据丢失而导致服务器重传的数据包。到达服务器之前客户端到服务器方向发生数据丢失时，监视设备将无法观测到数据包丢失，且“数据包丢失百分比”中不会包括该丢失。在管理控制台的“工程”页面上，“数据包丢失百分比”是 QoS 报告的一部分。

数据包捕获调查

*数据包捕获调查*是一种应用程序突发事件响应 (p. 183)或服务器突发事件响应 (p. 185)，用于对遇到问题的特定服务器、应用程序端口和网络执行筛选捕获。CA ADA 管理员还可以启动或排定此调查。

数据包摘要文件

*数据包摘要文件*包含来自 Cisco WAE 设备或 CA GigaStor 连接器的 TCP 标头。

数据传输时间

*数据传输时间*是一个综合度量标准 (p. 189)，用于度量传输完整的应用程序响应所花费的时间，从首次响应（服务器响应时间 (p. 185)结束）到该请求中发送完最后一个数据包。

如果没有更多适合 TCP 窗口的数据要发送，则数据传输时间将排除初始服务器响应时间，并包括网络往复传输时间。响应时间可能会受应用程序的设计以及服务器或网络的性能影响。

当超出“数据传输时间”阈值时，管理控制台不会打开一个突发事件。

跟踪路由

*跟踪路由*是指突发事件分析中使用的两个类型诊断工具中的任何一个类型：ICMP 或 TCP。

跟踪路由调查

*跟踪路由调查*是一种网络突发事件响应 (p. 182)，可记录监视设备与端点之间的路径和每个跃点，以监视延迟和路由问题；在某些情况下，SNMP 会轮询每个路由器以获得其性能信息。CA ADA 管理员还可以启动或排定此调查。

操作

*请参阅*响应操作 (p. 186)。