分析指南

CA Application Delivery Analysis Multi-Port Monitor

版本 10.1

ca technologies

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： 什么是 Multi-Port Monitor？

CA Application Delivery Analysis Multi-Port Monitor 是一个功能强大的设备，可以从受监视数据中心捕获会话级数据包数据。该设备捕获的数据用于在 CA Application Delivery Analysis 和 CA Application Performance Management (CA APM) 中进行报告。

- TCP 数据包标头中的数据可帮助 CA Application Delivery Analysis 监视端到端的性能，以度量应用程序响应时间。
- 来自完全 HTTP 数据包的数据可以帮助 CA APM 映射您的环境中的事务，以便监视最终用户体验并度量服务水平协议。

Multi-Port Monitor 通过被动监视多个端口上数据中心的大量通信量，来帮助您维持恒定的端到端系统性能记录。

通过受监视镜像端口的所有通信量的数据包标头将被短期记录和存储在 Multi-Port Monitor 中。1 分钟报告间隔中的数据将保留数天，并提供给分析使用。度量标准将转发到 CA Application Delivery Analysis 以用于报告，或转发到 CA Transaction Impact Manager (CA TIM) 以用于在 CA APM 中报告。

Multi-Port Monitor 分析中的图表显示每个主机的活动和性能数据。分析将会基于会话数据、数据量统计和响应时间提供多个视图。分析还会提供工作流用于故障排除，提供多个选项用于导出数据，并提供筛选选项以帮助 IT 工作人员诊断问题并做出响应。

Multi-Port Monitor 提供相应的功能来监视自身的功能。

- 针对每个逻辑端口提供基于硬件的筛选和数据包捕获选项。
- 硬件筛选可用于校准性能，并只捕获所需的数据。
- 通过一个网页管理多个数据源。
- 对于可能会影响数据监视或捕获的错误，SNMP 陷阱将会发送自动通知。

Multi-Port Monitor 包括以下组件：

设备

用于监视流入和流出交换机的通信量的硬件和软件。执行以下功能：

- 捕获数据包并将其写入存储。
- 收集通信量统计并分析数据包以提供性能信息。

- 在高性能数据库中存储有关网络、服务器和应用程序性能的统计数据。
- 将统计数据发送到 CA TIM 或 CA Application Delivery Analysis 以进行报告和分析。

Web 界面

一个可从浏览器访问的管理界面，可让您：

- 查看设备统计，包括驱动器、CPU 和捕获卡状态。
- 配置系统设置（如端口定义、筛选选项和安全用户帐户）。
- 对基于捕获数据包并以特定格式图表呈现的性能数据进行查看、筛选和排序。
- 在“分析”选项卡上查看本地存储的会话级数据。

第 2 章： 如何登录到 Web 界面

登录到 Web 界面以分析数据。

请执行以下步骤：

1. 在 Web 浏览器中访问 Web 界面。在浏览器“地址”字段中使用以下语法：

   `http://<`*主机名或 IP 地址*`>/`

   此时将打开 Multi-Port Monitor 的“登录”页面。

2. 使用分配的区分大小写的用户名和密码登录。

   将打开 Web 界面。

第 3 章： 什么是分析？

分析是对通过深入查看 Multi-Port Monitor 设备中存储的数据包级会话数据以便采取故障排除步骤的说明。这种说明是以一系列分层组织的视图形式进行的。

Multi-Port Monitor 提供两种类型的分析。

预定义分析

提供对基于 IPv4 的 TCP 会话级信息的访问，在从 CA Application Delivery Analysis 报告或 CA APM 的“缺陷详细信息”页面进行深入查看时将使用这些信息。

例如，您可以检查 CA Application Delivery Analysis 组件报告，并缩小 192.94.5.6 网络的数据范围。当您单击“会话分析”按钮时，Multi-Port Monitor 的“分析”页面上会显示选定报告的分析。选定的网络和时间范围可筛选分析中的会话级数据。

自定义分析

提供用于筛选和查看会话级度量标准的选项，以加速故障排除过程。Multi-Port Monitor 用户可以创建、保存和重复使用自定义分析。

例如，从不适用于您的情况的预选上下文中的 CA Application Delivery Analysis 位置开始进行深入查看（或会话分析）。您可以创建一个分析，或打开保存的分析，以保存用于选择所需视图及其分层排列方式的某些步骤。关联的图表针对您要分析的数据，提供了足够细致的透视图。

所有分析都显示在“分析”页面的“显示”区域左侧的“分析”窗格中。

筛选将添加到视图级的分析，并将应用到同一分析中的所有从属视图。

新的分析不包含默认数据视图。请在应用新分析之前为数据添加视图。

此部分包含以下主题：

分析页面

Web 界面中的“分析”页面上显示了会话级网络数据的细化视图。“分析”页面包含两个窗格。

“显示”区域

右窗格，其中包含一个图表和一个数据表。选项卡式视图可让您轻松访问带有格式的性能度量标准。图表和表提供了多个选项让您查看数据、选择图表格式，以及排序度量标准以查找离群值。

注意：尽管 Multi-Port Monitor 以 1 分钟粒度报告数据，但出于性能方面的原因，它会每隔 2 分钟向数据库加载一次收集的度量标准。这种差异导致出现延迟，只有在经过此延迟后，您才能在“显示”区域查看最新的收集数据。

“分析”窗格

左窗格，其包含用于选择数据视图，以及筛选“显示”区域中显示的数据的选项。您可以针对数据视图创建分析筛选，并可以将这些筛选保存为可重复使用的故障排除工作流。“分析”窗格的顶部显示了活动筛选列表。主要筛选类型包括：

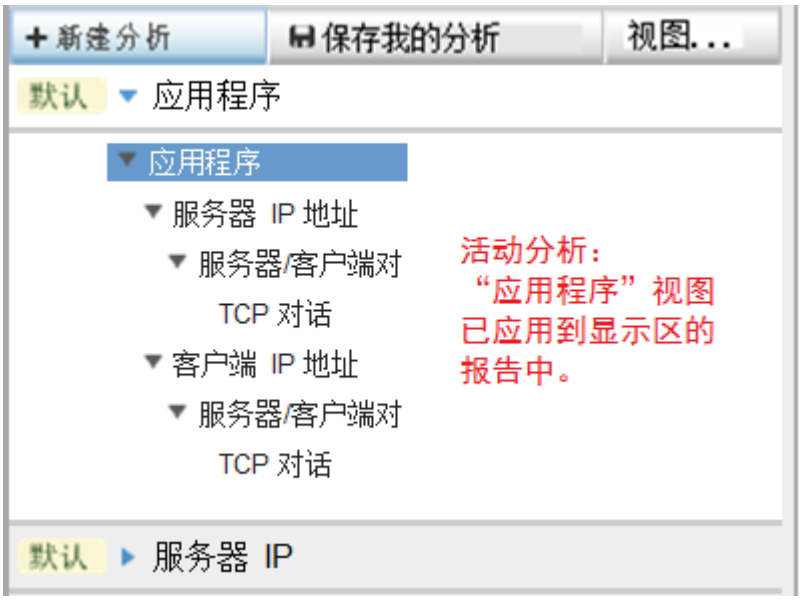
- 分析筛选 (p. 19)。当您单击“添加分析筛选”时，会将这些筛选显式应用到数据。双击“显示”区域中的某个项时，会隐式创建分析筛选。
- 全局筛选 (p. 26)。这些筛选将应用到所有分析，并基于 CA Application Delivery Analysis 中的深入查看上下文。

分析菜单

可使用“分析”菜单查看、创建和修改分析。默认情况下，该菜单在“分析”页面的“分析”窗格中可见。您可以将它隐藏，以展开图表的可用查看区域。

单击 **<<** 或 **>>** 符号（带有“分析菜单”标签）可隐藏或显示“分析”窗格。

在“分析”窗格中，活动的分析以白色文本、蓝色背景突出显示。活动的分析及其筛选将应用到“显示”区域中显示的报告。



活动分析的子视图可用于以更高的详细程度进行报告，在某些分析中，详细程度可达到 TCP 会话级别。这些分析的关联筛选可让您包含或排除“显示”区域中显示的度量标准内的特定会话。

展开某个分析可查看关联的视图。单击分析名称旁边的蓝色箭头可展开或折叠该分析。折叠或展开活动分析不会删除或添加筛选。

您可以将另一个视图应用到当前时间范围，以便在不同的上下文中查看数据。要应用另一个分析，请在“分析”窗格中将它展开，然后单击关联的视图。

预定义分析

预定义分析是可帮助您分析数据的排序和显示选项。在“分析”菜单中，这些分析的名称为“默认”。

您可以通过添加分析筛选，来暂时自定义预定义分析。您无法保存这些修改，它们只能保持到当前登录会话结束。

所有分析以更高的粒度级挖掘数据。每个数据视图都与某个预定义分析关联。当您选择一个分析时，该分析将会展开，在分层结构中显示视图列表。该结构基于监视的数据呈现您可以访问的更高详细程度的信息。这样，您便通过每个视图访问数据库中存储的、选定时间范围内的更详细度量标准。

分析可帮助您调查特定项，从而可为故障排除工作助上一臂之力。借助于任何分析，您可以将初始数据视图与对应的调查项结合考虑，这样可获得极大的便利。例如，“客户端 IP 地址”分析可帮助您找到某台 IP 地址已知的客户端计算机上出现问题的起因。首先，请应用“客户端”视图。双击一个客户端，以深入查看分析中的下一个视图，其中显示了与该客户端对话的所有服务器。

Multi-Port Monitor 提供以下预定义分析。

应用程序

使用此分析可识别有问题的应用程序。此分析将会识别运行该应用程序的服务器的 IP 地址，以及该应用程序使用的端口号。包含以下数据视图：

服务器 IP 地址 --> 服务器/客户端对 --> TCP 对话

客户端 IP 地址 --> 服务器/客户端对 --> TCP 对话

服务器 IP 或客户端 IP

使用该分析来识别存在问题的单个主机。包含以下数据视图：

服务器 IP 地址 --> 服务器/客户端对 --> TCP 对话

客户端 IP 地址 --> 服务器/客户端对 --> TCP 对话

网络

使用此分析可识别子网中多个主机出现的问题。包含以下数据视图：

服务器 IP 地址 --> 服务器/客户端对 --> TCP 对话

客户端 IP 地址 --> 服务器/客户端对 --> TCP 对话

IP 地址

使用该分析来识别存在问题的单个主机。包含以下数据视图，这些视图已根据捕获的数据组织成多个可能的筛选路径：

服务器 IP 地址 --> 服务器/客户端对 --> TCP 对话

客户端 IP 地址 --> 服务器/客户端对 --> TCP 对话

IP 地址对 --> IP 会话

Protocol

使用此分析可识别与使用单个协议的通信量相关的问题。包含以下数据视图：

IP 地址 --> IP 地址对 --> IP 会话

创建自定义分析

无法永久修改预定义分析。创建自定义分析来保持筛选或分析工作流。

遵循这些步骤:

1. 在“分析”窗格中单击“新建分析”。

   “分析”窗格中将显示一个新项。默认名称“我的分析 1”已突出显示。

   “分析”窗格的右侧将打开“视图”窗格。

2. 在突出显示的字段中键入新分析的名称。
3. 在“视图”窗格中选择要添加到自定义分析的视图。
4. 将此视图拖到“分析”窗格的“将视图拖放到此处”部分。
5. 重复步骤 3 至 4，将数据视图添加到您的分析中。建议在较高粒度的分层流中添加视图，并随着视图往下继续添加，以便筛选掉更多项。

6. （*可选*）添加高级筛选。右键单击一个视图并选择“添加分析筛选”。

   将打开“添加分析筛选”对话框。有关字段的说明，请参阅数据视图的筛选 (p. 19)。

7. 单击“保存我的分析”。

   自定义分析将保存。可同时保存多项更改。

   重要说明：如果您正在查看以电子邮件发送的分析，则单击“保存我的分析”将会覆盖以前保存的所有分析。

重复分析

您可以重复自定义和预定义的分析。使用重复功能，您可以保存对分析所做的修改。

遵循这些步骤:

1. 在“分析”窗格中，右键单击要复制的分析。
2. 选择“重复”。

   “分析”窗格中将显示一个新分析，其命名约定为“我的分析 #”。

3. 键入重复分析的新名称。

删除自定义分析

您可以删除自定义分析。但无法删除预定义分析。

遵循这些步骤:

1. 在“分析”窗格中，右键单击要删除的分析的名称。
2. 选择“删除分析”。
3. 在确认消息中单击“确定”。

   该分析随即从“分析”窗格中删除。

数据视图

数据视图可帮助您调查网络性能方面的问题。预定义分析包含数据视图。您可以使用自定义分析自身的视图集来创建和修改自定义分析。

当您创建分析时，“视图”菜单会自动打开。还可以通过单击“视图”按钮来查看可用数据视图的列表。

您可以使用以下项来自定义数据视图：

- 筛选 - 将重点放在所需的通信量上。
- 图表格式 - 以图形方式显示所需的性能度量标准。
- 数据表设置 - 有选择性地显示所需的度量标准 对于每个视图，将应用默认的排序方法。例如，在“协议”分析中，协议按最高字节速率到最低字节速率的顺序排序。

您可以自定义数据视图。某些更改（例如图表格式的更改）将自动在视图中保存。

应用程序

突出显示每个应用程序的响应时间（事务时间，以毫秒为单位）。应用程序名称源于 CA Application Delivery Analysis 配置或众所周知的端口使用。可用时，请提供应用程序名称。否则，将显示端口号。

默认图表显示响应时间及其组成的趋势。“事务时间”已细分为“网络往返传输时间”、“重传”、“数据传输时间”和“服务器响应时间”。

客户端 IP 地址

突出显示每个客户端的响应时间（事务时间，以毫秒为单位）。Multi-Port Monitor 基于启动 TCP 对话的三次握手识别客户端计算机。该图表显示响应时间及其组成部分的趋势。

IP 地址

（*“通信量”选项卡*）突出显示每个主机 IP 地址的吞吐量（字节速率，以比特数/秒为单位），按最高字节速率到最低字节速率的顺序排序。该图表显示*传入*及*传出*速率最高主机的定向字节速率。

IP 地址对

（*“通信量”选项卡*）突出显示主机 IP 地址的每个对话对的吞吐量（字节速率，以比特数/秒为单位），按最高字节速率到最低字节速率的顺序排序。该图表显示*传入*及*传出*速率最高主机对的定向字节速率。

IP 会话

（*“通信量”选项卡*）突出显示每个会话的吞吐量（字节速率，以比特数/秒为单位）。每个会话表示主机 IP 地址的一个对话对。会话按最高字节速率到最低字节速率的顺序排序。该图表显示*传入*及*传出*吞吐量排名前十的会话的字节速率组成。

逻辑端口

突出显示每个逻辑端口（即传入 Multi-Port Monitor 的每个交换机镜像端口会话）的响应时间。该图表显示响应时间的趋势（显示为“字节速率”）。

网络

突出显示每个网络的响应时间（事务时间，以毫秒为单位）。基于 CA Application Delivery Analysis 配置识别网络。该图表显示响应时间及其组成部分的趋势。

Protocol

（*“通信量”选项卡*）突出显示通过了硬件筛选的每个协议的吞吐量（字节速率，以比特数/秒为单位）。显示发送和收到的总字节数，以及 TCP 字节数。还显示了第 3 层协议。该图表显示一段时间内的吞吐量趋势（显示为“字节速率”）。

服务器 IP 地址

突出显示每台服务器的响应时间（服务器响应时间，以毫秒为单位）。该图表显示响应时间及其组成部分的趋势。

服务器/客户端对

突出显示每个主机对（客户端和服务器）的响应时间（事务时间，以毫秒为单位）。该图表显示响应时间及其组成部分的趋势。

TCP 对话

突出显示每个会话的响应时间（事务时间，以毫秒为单位）。每个会话包括一个服务器主机、一个客户端主机和端口。该图表显示响应时间及其组成部分的趋势。

详细信息：

创建分析筛选 (p. 19)
查看当前筛选条件 (p. 18)

第 4 章： 使用筛选自定义显示区域中的数据

Multi-Port Monitor 提供了多种方法用于缩小“分析”页面的“显示”区域中显示的会话级度量标准的范围。可对通过选定分析显示的数据应用以下选项。

数据视图

您可以选择不同的数据视图，以将重点放在对当前故障排除任务最为相关的网络方面。例如，如果某个应用程序的响应时间较长，请选择“服务器 IP”视图或“应用程序”视图，以查看关联的度量标准。

使用分析筛选 (p. 19)来筛选视图中的数据。

注意：分析筛选不同于应用到捕获数据的硬件筛选。硬件筛选会影响数据*捕获*。分析筛选会影响数据*显示*。

特定于上下文的筛选

- 在数据表中选择一行或一系列行。单击右键，然后选择“应用为筛选”，以缩小当前分析中的数据范围。要突出显示多个行，请按住 Ctrl 或 Shift 并单击。
- 使用鼠标指针选择图表的特定部分。松开鼠标指针，然后单击“设置”。图表将会刷新，以重点显示范围更小的段，例如，在线形图中显示一个尖峰，以指示背离基准度量标准的情况。

深入查看筛选

- 在数据表中双击一行可向下深入一级，进入分析中的下一个视图。
- 在“分析”页面上，从某个 APM 缺陷开始深入查看关联的数据。将会基于该缺陷的上下文自动创建一个分析筛选。
- 在 CA Application Delivery Analysis 报告中单击“会话分析”可在“分析”页面上查看关联的数据。“分析”页面上的全局筛选 (p. 26)基于 CA Application Delivery Analysis 报告的上下文。

缩放筛选

折线图提供了更多筛选选项。使用“放大”和“缩小”链接可以更细致地重点查看较小的捕获数据段中的性能度量标准。

- “放大”会缩小当前时间范围，因此，绘制的数据段较小。
- “缩小”会还原时间范围以显示更广泛的数据段。

时间范围筛选

“汇总趋势”、“线形趋势”和“堆积趋势”图表格式在“显示”区域上方提供了一个时间导航组件。默认时间范围为 15 分钟。“时段选择器”可让您精确选择另一个时间范围。

- “后退”和“前进”按钮可让您向前或向后移动捕获数据的时间。通过这种类型的时间导航，您可以查看趋势数据，同时跟踪不断延续的每种趋势。
- 在日期、小时和分钟选择菜单中，您可以选择其他日期和时间参数。
- 日期在带有前进和后退导航控件的图形日历菜单中显示。
- 使用“时间范围”链接可以快速访问更大的时间段，例如，从“最后 15 分钟”改为“最后 180 分钟”。

此部分包含以下主题：

查看当前筛选条件 (p. 18)
分析筛选 (p. 19)
全局筛选 (p. 26)

查看当前筛选条件

您可以使用多个选项来查看已应用到分析的筛选的相关信息。

- 在“分析”窗格或“显示”区域中单击“显示筛选”链接可查看以下信息：
  - 从 CA Application Delivery Analysis 报告继承的所有全局筛选的列表。
  - 应用于当前数据视图的分析筛选的列表。
- 在分析中，将鼠标指针悬停在筛选的数据视图上。悬浮文本将描述相应筛选的条件和语法。
- 在分析中，右键单击一个数据视图并选择“编辑分析筛选”。“编辑分析筛选”对话框中的“条件”字段将显示相应筛选的条件和语法。
- 在分析中单击筛选图标。“条件”字段将显示相应筛选的条件和语法。

分析筛选

您可以向数据视图应用正则表达式，以限制“显示”区域中的数据。这种类型的筛选是*分析筛选*。

正则表达式筛选将直接应用到作为活动分析的组成部分的数据视图。只能将这些筛选保存为分析自定义的一部分。

创建分析筛选

您可以向数据视图应用正则表达式，以限制“显示”区域中的数据。这种类型的筛选是*分析筛选*。

正则表达式筛选将直接应用到作为活动分析的组成部分的数据视图。只能将这些筛选保存为分析自定义的一部分。

当您向某个数据视图添加分析筛选时，新的筛选和所有继承的筛选将应用到该视图。可以在“添加分析筛选”对话框中查看继承的筛选。

注意：新筛选不会修改继承的全局筛选。而是向通过了全局筛选的数据提供一个附加筛选。

遵循这些步骤:

1. 右键单击分析中的视图，并选择“添加分析筛选”。

   将打开“添加分析筛选”对话框。“继承的分析筛选”字段中显示了从同一分析中的另一个视图继承的筛选。

2. 从“参数”字段中选择筛选。当您单击每个项时，会显示“值”的帮助及相应的语法。

3. 选择运算符。

   - 等于号 (=)
   - 不等于 (!=)

4. 键入值完成该表达式。使用语法联机帮助获得指导。

   注意：在“值”字段中使用特定表达式可有效地禁用筛选。不要使用“保留的筛选表达式 (p. 20)”列表中的表达式。

5. 单击“添加到条件”。

   筛选语句显示在“条件”字段中。

   注意：要删除筛选语句，请单击“条件”字段上方的 [清除]。您也可以直接通过在“条件”字段中键入来编辑该语句。

6. （*可选*）选择一个布尔运算符并重复步骤 3 至 5，以添加与现有筛选语句相关的条件。
   - AND（串联）
   - OR（交替）
7. 单击“确定”。

   随后将验证筛选。如果该筛选有效，则会将它应用到“显示”区域中的数据表和图表。“分析”窗格中的视图名称旁边将显示一个筛选图标，用于指示已应用分析筛选。

详细信息：

创建自定义分析 (p. 13)

保留的筛选表达式

将保留以下筛选表达式。不要在“添加分析筛选”对话框的“值”字段中使用这些区分大小写的表达式。

```
ApplicationName, ApplicationTypeID, ApplicationNameTypeID
ClientNetworkName, ClientNetwork
HostName, Host
L4Port
LogicalPortName, LogicalPort
L3ProtocolName, L3ProtocolNumber, L4ProtocolName, L4ProtocolNumber,
L34ProtocolName, L34ProtocolNumber
MAC
NetworkName, Network
PairName, Pair
ServerName, Server
SessionID, ToS, or VLAN
```

如果参数包含一个保留表达式和“=”或“!=”，则分析筛选函数无法创建查询语法。如果您使用了保留表达式，请使用不同于列表中指定的表达式的大小写。

与“参数”字段关联的值

下表根据“参数”字段中选择的项描述了“值”字段的语法。

应用程序名称

应用程序名称的筛选。“显示”区域中的应用程序名称派生自 CA Application Delivery Analysis 配置或已知的端口使用。键入一个名称，或逗号分隔的名称列表。接受通配符。示例：

```
Secure HTTP*
Secure HTTP (443)
```

应用程序名称/类型/ID

表示应用程序名称、类型和 ID 编号的三个值的筛选。在“编辑列”对话框中启用“应用程序名称”、“应用程序类型”和“应用程序 ID”列后，即可看到这三个值。指定一个三段数组作为“名称/类型/ID”。示例：

```
MySQL (3306)/受监视/3
```

注意：“应用程序类型/ID”和“应用程序名称/类型/ID”参数要求使用内部分配的值。在数据表中使用右键单击菜单直接应用这些参数。

应用程序类型/ID

针对表示应用程序类型及其 ID 编号的两个值的筛选。在“编辑列”对话框中启用“应用程序类型”和“应用程序 ID”列后，即可看到这些值。指定一个对作为“类型/ID”。示例：

```
受监视/10
```

客户端网络

某个客户端网络子网 IP 地址或逗号分隔的子网列表的筛选。请使用斜线 (/) 来分隔掩码与地址。示例：

```
192.3.45.0/24
192.3.45.0/24,192.3.46.0/24,192.3.50.0/24
```

客户端网络名称

定义为要在 CA Application Delivery Analysis 中进行监视的某个客户端网络或以逗号分隔的网络列表的名称的筛选。

主机

IP 地址筛选。采取以下格式的任何组合的默认筛选参数：

- 一个 IP 地址
- IP 地址范围
- 逗号分隔 的 IP 地址列表
- 逗号分隔的地址范围列表

在地址范围中使用连字符且不要使用空格。示例：

```
198.168.0.1、198.165.0.1-198.165.1.255
```

主机名

客户端或服务器 DNS 主机名的筛选。键入一个 DNS 主机名，或逗号分隔的主机名列表。支持通配符 (*)。此参数是默认的。示例：

```
exchangeserver1、*noc*、database*
```

第 3 层协议名称

筛选网络层协议。键入一个第 3 层协议名称，或逗号分隔的名称列表。示例：

```
IP
```

第 3 层协议编号

筛选网络层协议。键入一个第 3 层协议的十进制注册编号，或逗号分隔的注册编号列表。

第 3/4 层协议名称

筛选来自第 3 层和第 4 层的协议对。键入一个协议名称对，或多个名称对列表。请使用斜杠 (/) 来分隔协议注册编号对。示例：

```
IP/TCP
```

第 3/4 层协议对

筛选来自第 3 层和第 4 层的协议对。键入一个协议注册编号对，或多个编号对列表。请使用斜杠 (/) 来分隔协议注册编号对。例如，对于 IP/TCP：

```
2048/6
```

第 4 层端口

传输层端口号的筛选。键入一个端口号，或逗号分隔的端口号列表。例如，对于 HTTPS：

```
443
```

第 4 层协议名称

筛选传输层协议。键入一个第 4 层协议名称，或逗号分隔的名称列表。

第 4 层协议编号

筛选传输层协议。键入一个第 4 层协议的十进制注册编号，或逗号分隔的注册编号列表。

逻辑端口

逻辑端口号的筛选。键入一个逻辑端口号，或逗号分隔的编号列表。使用此参数可以做到只查看从特定源镜像的数据。

逻辑端口名称

在 Multi-Port Monitor 设备上定义的逻辑端口名称筛选。键入一个逻辑端口名称，或逗号分隔的名称列表。

MAC 地址

某个媒体访问控制 (MAC) 地址或逗号分隔的 MAC 地址列表的筛选。示例：

```
00:19:2f:aa:bb:cc
```

网络名称

CA Application Delivery Analysis 网络名称的筛选。在 CA Application Delivery Analysis 的“管理”中配置网络时，可为每个网络提供一个名称。在该字段中键入一个网络名称，或逗号分隔的名称列表。

网络

针对网络子网的筛选。键入某个网络子网的 IP 地址，或逗号分隔的子网列表。请使用斜线 (/) 来分隔掩码与地址。示例：

```
192.3.45.0/24
192.3.45.0/24,192.3.46.0/24,192.3.50.0/24
```

对

对话主机的 IP 地址对的筛选。键入一个 IP 地址对，或逗号分隔的 IP 地址对列表。请在地址对之间使用斜杠 (/)。示例：

```
198.168.0.1/198.168.0.18
```

对名称

对话主机的 DNS 主机名对的筛选。为该值键入一个主机名对，或逗号分隔的对列表。请在主机名对之间使用斜杠 (/)。示例：

```
MyServer1/MyClient1
```

服务器

服务器 IP 地址的筛选。键入某个服务器的 IP 地址，或逗号分隔的地址列表。使用点分表示法。示例：

```
192.3.45.0
```

服务器名称

服务器主机名的筛选。键入一个主机名，或逗号分隔的主机名列表。

会话 ID

TCP 会话 ID 编号的筛选。键入一个会话 ID 编号，或逗号分隔的 ID 编号列表。

会话 ID 是在“编辑列”对话框中启用“会话 ID”列后提供的内部标识符。

ToS

“服务类型”位设置的筛选。键入一个十进制格式的 ToS 设置，或逗号分隔的设置列表。例如，要使用 0100 以最大化吞吐量，请键入：

```
4
```

VLAN 编号

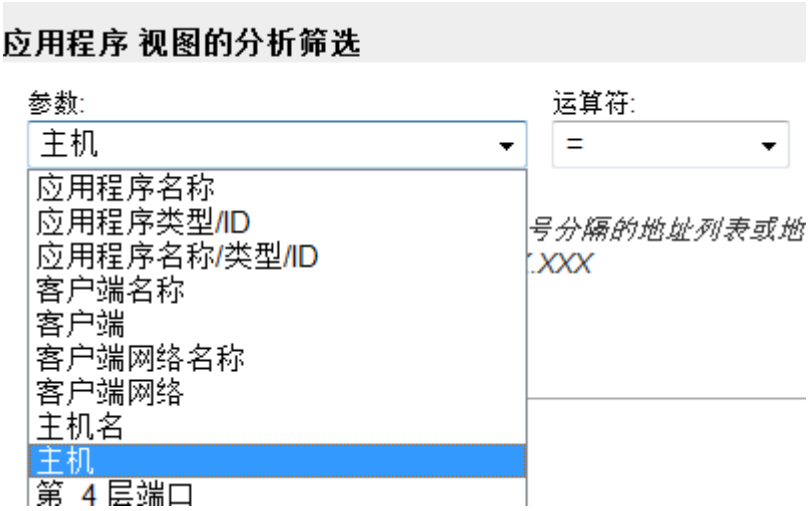
虚拟 LAN ID 编号的筛选。键入一个 VLAN ID 编号，或逗号分隔的编号列表。

详细信息：

在数据表中添加或删除列 (p. 42)

筛选如何查询数据库

在“添加分析筛选”对话框中，某些分析筛选是成对的集。例如，您可以按“主机”（IP 地址）或“主机名”进行筛选：



系统将以智能方式应用这些筛选参数，以创建有用的图表。例如，选择“主机”参数可筛选“客户端 IP 地址”视图的“TCP”选项卡上的数据。数据仅显示与筛选值匹配的客户端地址。然后将同一个“主机”筛选应用到“服务器 IP 地址”视图。数据仅显示与筛选值匹配的服务器地址。

某些数据视图不以这种方式限制显示。“协议”和“应用程序”视图按客户端和服务器进行筛选。一般而言，“通信量”选项卡较少应用筛选。

“网络”数据视图和“网络”分析筛选不总是搜索 CA Application Delivery Analysis 中定义的所有网络。CA Application Delivery Analysis 将网络分为客户端或服务器网络。该分类基于这些主机在捕获的事务中充当的角色。与网络地址或名称值匹配的“网络”和“网络名称”筛选，默认为对客户端网络进行匹配。但是，这些筛选也会根据选定的数据视图和选项卡发出不同的数据库查询。

- 当选择“网络”视图和“TCP”选项卡时，只会在客户端网络中查询匹配值。
- 当选择“服务器 IP”视图时，只有“网络”和“网络名称”分析筛选发送匹配服务器网络的查询。

更改分析筛选的属性

您可以修改已应用到数据视图的分析筛选。可以使用以下详细过程，通过“分析”菜单修改筛选。或者，可以在数据表中使用右键单击选项修改父筛选。对父筛选所做的更改将覆盖已应用到子视图的所有分析筛选。

遵循这些步骤:

1. 找到要更改的筛选。筛选图标 () 标识了活动筛选。
2. 右键单击该筛选，然后选择“编辑分析筛选”。

   “编辑筛选”对话框在“条件”字段中标识了活动筛选。“继承的分析筛选”字段中显示了从同一分析中的另一个视图继承的筛选。

   注意：在分析中，筛选继承将从前面的视图往下向同一分析中的所有后续视图持续进行。
3. 选择一个布尔运算符，以添加与现有筛选语句相关的条件。
   - AND（串联）
   - OR（交替）
4. 从“参数”字段中选择筛选。当您单击每个项时，会显示“值”字段的帮助及相应的语法。
5. 选择运算符。
   - 等于号 (=)
   - 不等于 (!=)
6. 键入值完成该表达式。使用语法联机帮助获得指导。

   注意：为“值”字段提供了某些表达式时，这些表达式会禁用筛选。不要使用“保留的筛选表达式 (p. 20)”列表中的表达式。
7. 单击“添加到条件”。

   筛选语句显示在“条件”字段中。

   注意：要删除该语句，请单击“条件”字段上方的 [清除]。您也可以直接通过在“条件”字段中键入来编辑该语句。
8. 单击“确定”。

   随后将验证修改的筛选。如果该筛选有效，则会将它应用到“显示”区域中的数据表和图表。

详细信息：

保留的筛选表达式 (p. 20)
与“参数”字段关联的值 (p. 20)

删除分析筛选

您可以删除已应用到数据视图的分析筛选。将鼠标指针悬停在某个筛选上可查看当前的筛选条件。您可以删除某个分析的一个筛选或所有筛选。

遵循这些步骤:

1. 找到您要删除的筛选。筛选图标 () 标识了筛选。
2. 右键单击筛选的视图，然后选择“删除分析筛选”以删除一个筛选。

   将刷新“显示”区域中的图表，以便包含筛选出的数据。
3. 右键单击分析的名称，然后选择“删除所有筛选”以删除所有筛选。

   将刷新“显示”区域中的图表，以便包含筛选出的数据。

全局筛选

全局筛选继承自您启动“会话分析”时生效的 CA Application Delivery Analysis 报告上下文。每个全局筛选设置都指定了上下文。

“分析”窗格的顶部显示了活动全局筛选列表。最先显示的是“域”、“应用程序”、“服务器”和“网络”全局筛选，其后为执行“会话分析”过程中选择的“逻辑端口”。

针对 Multi-Port Monitor 数据库的查询将会筛选数据。这些查询取决于筛选类型和选定的数据视图，选择这些查询可优化返回的数据。

- “域”全局筛选主要关注指定域。可用域列表基于 CA Performance Center 中为用户指定的域组。
- “服务器”全局筛选将重点放在指定的服务器上。
- “网络”全局筛选将重点放在该网络中的客户端上。

您可以修改全局筛选，以限制“显示”区域中显示的数据。您还可以清除某个全局筛选，使它还原为默认设置。

“全局筛选”对话框

“全局筛选”对话框提供以下信息。

“域”选项卡

- 名称。域的名称(如果定义了域)。可用域列表基于 CA Performance Center 中为用户指定的域组。

“应用程序”选项卡

- 名称。应用程序的名称（如果可用）。在括号中显示端口号。
- 应用程序类型/ID。应用程序标识符。通常是表示应用程序类型及其 ID 编号的两个值。每个对标识了 Multi-Port Monitor 数据库中的某个应用程序。

“服务器”选项卡

“服务器”选项卡包含主机列表。受监视事务中服务器的角色将其标识为主机。Multi-Port Monitor 可以在捕获的对话数据中区分服务器和客户端。

- 名称。CA Application Delivery Analysis 中配置的服务器名称，通常是 DNS 主机名。
- IP 地址。服务器的 IP 地址。

“网络”选项卡

“网络”选项卡标识了客户端网络。CA Application Delivery Analysis 的*网络*概念是在监视客户端区域，并通过这些区域观测客户端-服务器事务的基础上给出的。

- 名称。CA Application Delivery Analysis 中定义的网络名称。网络被视为客户端区域，其用途是为了执行 CA Application Delivery Analysis 性能监视。
- 子网。该客户端区域基于子网 IP 地址和掩码的组合。

“逻辑端口”选项卡

- 名称。Multi-Port Monitor 管理员定义的逻辑端口名称。默认名称与端口号相同。
- 逻辑端口。“逻辑端口”页面上显示的逻辑端口的编号。默认逻辑端口定义对应于适配器上的端口 ID 号。

修改全局筛选

您可以更改全局筛选，以限制分析中包含的数据。

注意：如果更改“逻辑端口”全局筛选，将会有效地更改选定分析的整个数据集。

遵循这些步骤:

1. 在“分析”窗格中，单击您要更改的全局筛选旁边的 [更改]。

   将打开“全局筛选”对话框。

2. 单击与您要更改的全局筛选对应的选项卡。例如，要根据受监视网络上运行的某个应用程序来筛选分析，请单击“应用程序”选项卡。

   该选项卡显示所有已知应用程序的列表，从您所查看的时间范围开始捕获的数据包中反映了这些应用程序的通信量。

3. 在列表中选择一个应用程序。例如，选择“简单邮件传输协议”。

   选定的应用程序将显示为“当前选定”。应用程序端口号显示在括号中。选择的应用程序还会筛选“全局筛选”对话框中其他选项卡上的项列表。

4. 单击另一个选项卡，以向分析中包含的数据应用更多限制。

   例如，单击“服务器”选项卡。列表中只显示正在运行选定应用程序（本示例中为 SMTP）的服务器。选择服务器。

5. 单击“确定”。

   随后将筛选当前分析的图表和表，以仅显示来自 SMTP 应用程序及其应用程序服务器的数据。

清除对全局筛选的修改

可以删除或清除您对某个全局筛选所做的更改。清除更改后，该全局筛选将还原为默认设置“全部”。

遵循这些步骤:

1. 在“分析”窗格中，单击您要清除的全局筛选旁边的 [更改]。

   将打开“全局筛选”对话框，其中的活动全局筛选显示为“当前选定”。

2. 单击选定筛选旁边的 [清除]。

3. 单击另一个选项卡以查看选择了哪些筛选，然后重复步骤 2。

4. 单击“确定”。

   数据表和图表将会刷新，以包含筛选掉的信息。

第 5 章： 了解显示区域中的数据

“显示”区域包含一个图表和一个数据表。以下项会影响图表和表中的数据：

- 域
- 时间范围
- 全局筛选
- 分析筛选
- 数据表中的活动选项卡：“TCP”或“通信量”选项卡

该图表沿着右侧提供了一系列格式按钮，让您将其他图表格式应用到相同的数据。您可以通过隐藏“分析”窗格来扩大“显示”区域的大小。单击“分析”窗格中的“隐藏”图标 (<<) 即可隐藏该窗格。

图表和表相互链接，因此，它们总是以互补格式显示数据。表显示的数据比图表多。但是，图表反映了应用到表的筛选，例如，更改了排序顺序及选择了新的页面。

数据表可呈现性能数据以进行故障排除和分析。您可以对每个列排序，以查看离群值和最小结果。有两个筛选始终会影响数据表：

- 当前时间范围
- 当前分析的筛选参数

预定义分析包含少量的筛选，并会应用某种逻辑，以便将数据限制为可控制的数量。此技术加速了数据库查询，同时还让普通用户看到一个更有条理的“显示”区域。

图表（“汇总趋势”图表除外）中呈现了前十个表行的数据。“汇总趋势”图表则反映了所有表行的数据。增大“每页最多”设置可显示更多表行。

此部分包含以下主题：

图表类型 (p. 30)
数据类型 (p. 33)

图表类型

在以下情况下，“显示”区域中的图表将会刷新：

- 从 CA Application Delivery Analysis 报告启动“会话分析”。
- 在“分析”窗格中单击某个数据视图。
- 在“显示”区域中的数据表内选择一列。
- 从某个 CA APM 缺陷开始深入查看。

图表和表提供了相辅相成的筛选选项。当您在数据表中单击一个列标题时，该表将会刷新，以按选定项为所有可用行进行排序。图表将会刷新以显示选定项。

当您单击“TCP”或“通信量”选项卡时，图表中的数据将相应地自动更改。大多数图表都限制为前十个条目。一个例外是“汇总趋势”图表，它符合 CA Application Delivery Analysis 约定，包含整个数据表中的数据。

每个趋势图允许您选择时间范围和缩放选项。

条形图

条形图格式呈现选定时段内的数据平均值。每个条形显示单个表行中的数据。Y 轴标识了每个表行。单个条形图最多可以包含十行。Y 轴标签指示用于标识行的列。例如，Y 轴显示“服务器 IP 地址”视图的每个相应服务器名称。X 轴通常显示度量标准值及其单位。

这种类型的图表格式最适合用于比较不同实体的性能度量标准。例如：

- 将一台服务器与另一台服务器的服务器响应时间进行比较。
- 比较排名前十个应用程序的“TCP 字节速率”。

条形的每个部分都提供了悬浮文本，用于标识度量标准及其值。要了解哪个构成度量标准是总计值的最大促成因素，使用此功能将十分有用。在图表中单击一个条形将会在数据表中突出显示相应的行。然后，您可以右键单击该表行并选择“应用为筛选”，以查看只与您选择的实体关联的数据。

重要说明：某些度量标准（例如“服务器响应时间”）以单一值显示。其他度量标准（例如“事务时间”）以综合格式显示。综合图表将某个选定度量标准显示为整个度量标准的一部分。综合条形图将单个值进行细分，以显示其单位。

线形趋势图

在线形趋势图格式中，每条线段代表数据表中每个行的数据。线段绘制了时段内的选定度量标准。每个图表最多绘制十个数据行。Y 轴标识了度量标准值（例如，以毫秒为单位的服务器响应时间 (SRT)）的散列单元。X 轴显示用于指示趋势的时间单位。

这种类型的图表格式提供了系统状态和趋势的快速概览。例如：

- 可以访问“服务器 IP 地址”视图，以比较服务器响应时间趋势并深入查看 SRT 中的峰值。
- 可以筛选单个 IP 地址，以找到事务时间逐渐增大的起因。

饼图

饼图格式以饼块的形式呈现选定度量标准的排名前十个条目。每个饼块表示一个整体的百分比。所有饼块值之和等于排名前 10 个表条目的选定度量标准总计值的 100%。每个饼块代表数据表中的一行。

注意：某些度量标准（如“TCP 字节丢失百分比”）不适合以饼图格式显示。

排名靠前的 10 个条目并不总是反映了选定时段内观测到的所有活动。您可以启用第 11 个饼块，以呈现余下的所有表行的合计（“其他”）。每个饼块的悬浮文本标识出了主机。单击一个饼块将会在数据表中突出显示关联的主机。然后，您可以按这些数据筛选。不支持深入查看“其他”饼块。

这种类型的图表格式最适合用于将主机的相对促成因素与选定的度量标准进行比较。例如，在特定服务器上筛选，并选择“服务器/客户端对”视图。然后选择“TCP 字节数”度量标准，并查看哪些客户端是服务器数据量的最大促成因素。

堆积趋势图

堆积趋势图的概念与饼图类似，不过，前者的数据是对应于时间绘制的。为每个表行显示一条使用不同颜色的线段。每个图表最多绘制十行。线条已被填充并已堆积，最高的表行绘制在图表的底部。每个线段下方的向下填充有助于查看每个数据区域如何与其他数据区域及更大的度量标准相关。

标有“总计”的粗线段标识了所绘制度量标准的 100% 坐落在 Y 轴上的哪个位置。要从图表中删除此线段，请单击图例旁边的“隐藏”链接。

这种类型的图表格式最适合用于将选定实体的相对促成因素与各时间内的性能度量标准进行比较。例如，在特定服务器上筛选，并选择“服务器/客户端对”视图。针对“TCP 字节数”度量标准的堆积趋势图指示了不同客户端的数据量是否随着时间的推移而变化。

积堆趋势图不适用于某些类型的度量标准，例如“TCP 字节丢失百分比”。

汇总趋势图

汇总趋势图使用积堆格式来显示数据表内所有表行和所有页面中的数据点。该图表显示选定度量标准值的分层视图。每个值等于度量标准上边界线和下边界线之间的垂直距离，而不是从 0 到上边界线之间的距离。

该图表格式类似于积堆趋势图，但两者存在以下差异：

- 积堆趋势图显示单个度量标准，该度量标准只代表数据表当前页面中的单个列。
- 汇总趋势图显示所有行和表列中的多个度量标准，并显示所有列的平均值。

要显示综合数据，使用积堆格式将十分有助。每个度量标准的值被视为整个度量标准的一部分。每个数据点将单个度量标准进行细分，以显示该度量标准的组成部分。

不同颜色的线段显示了构成一个总体值的数据点。例如，TCP 事务响应时间的组成部分包括：网络往返传输时间、服务器响应时间和数据传输时间。

为了呈现所绘制度量标准的趋势，该图表已对应于选定时段进行绘制，时间值显示在 X 轴上。

数据类型

数据表包括二个选项卡式视图，其中提供了从同一时间范围开始捕获的数据的不同透视图。每个视图提供不同的度量标准，并以不同的方式应用筛选。

TCP 选项卡

“TCP”选项卡包含的数据特定于 CA Application Delivery Analysis 报告中基于 TCP 的应用程序和度量标准。该选项卡还包含根据捕获的数据包计算的性能度量标准。“名称”列上的标签会发生变化，以指示显示的是客户端还是服务器。

注意：当您从 CA Application Delivery Analysis 深入查看时，会按默认选择“TCP”选项卡。一般而言，“TCP”选项卡中的数据格式与 CA Application Delivery Analysis 报告的数据格式非常相似。

“通信量”选项卡

“通信量”选项卡包含所有其他可用数据，而不局限于 TCP 应用程序。“通信量”选项卡不适用客户端或服务器的概念。因此，“名称”列既可以显示客户端的名称，也可以显示服务器的名称，具体取决于选定的视图。“通信量”选项卡还包含非 TCP 通信量，这可能会导致包含更多主机。

为了减小表的宽度，数据表中某些性能度量标准的名称采用了缩写。要查看度量标准的全名，请将鼠标指针定位在缩写的列名或其复选框上。悬浮文本将提供选定度量标准的全名。

“通信量”选项卡上的数据

数据表的“通信量”选项卡提供通过受监视镜像端口的数据包的综合视图。只有那些适用于选定视图的列才会显示在表中。以下列表描述了“通信量”选项卡所有可能的列。

应用程序

应用程序名称源于 CA Application Delivery Analysis 配置或众所周知的端口使用。可用时，请提供应用程序名称。否则，将在括号中显示端口号。

应用程序 ID

用于标识应用程序的一对值中的第二个值。内部标识符。

应用程序类型

标识 Multi-Port Monitor 数据库中的应用程序。大多数情况下，表示此应用程序的状态，因为它涉及到 CA Application Delivery Analysis。下列类型之一：

- **n/a**：未知协议。
- **受监视**：应用程序使用 TCP。CA Application Delivery Analysis 将会监视此应用程序。

  如果有多个收集设备要向一个 CA Application Delivery Analysis 管理控制台报告，则可能有一个不同的收集设备为 CA Application Delivery Analysis 监视此应用程序。指定的应用程序类型是指仅此 Multi-Port Monitor 主动监视的项。
- **UDP-未监视**：应用程序已在 CA Application Delivery Analysis 中定义，但使用了 UDP。CA Application Delivery Analysis 不监视 UDP。
- **TCP-未监视**：应用程序已在 CA Application Delivery Analysis 中定义并使用 TCP。但是，CA Application Delivery Analysis 未监视该应用程序。
- **TCP-未知**：应用程序使用 TCP，但未在 CA Application Delivery Analysis 中定义。“应用程序”列显示“端口 *X*”。
- **UDP-未知**：应用程序使用 UDP，而 CA Application Delivery Analysis 不监视 UDP。应用程序未在 CA Application Delivery Analysis 中定义，或未在已知 UDP 端口的 Multi-Port Monitor 列表中定义。“应用程序”列显示“端口 *X*”。

字节速率

以比特数/秒（每秒字节数 x 8）为单位度量的服务器处理效率。该吞吐量值对于容量计划来说非常重要，因为它提供了服务器负载或使用情况的相关信息。

字节速率从、字节速率到

选定主机所发送或接收数据的吞吐量（以比特数/秒（每秒字节数 x 8）为单位）。

字节数

数据量（以字节为单位）。在选定时段以及选定客户端-服务器会话期间发送和接收的应用程序层的总字节数。

字节数从、字节数到

数据量（以字节为单位）。在选定时段内选定主机发送或接收的应用程序层的总字节数。

IP 地址、IP 地址 1、IP 地址 2

主机的 IP 地址。指定的“1”或“2”针对成对的数据视图显示，表示主机之间数据流的方向。

第 3 层协议

网络层协议（IP 或 ARP）的名称，或数据包标头中“Ethertype”字段的 ID 编号。如果找到 IEEE 802 Ethertype 值，则表示“Ethertype=X”。

第 3 层协议编号

网络层协议的十进制注册编号，如 IPv4 的注册编号 2048。

第 4 层协议

传输层协议的名称，如 TCP。

第 4 层协议编号

传输层协议的十进制注册编号，如 TCP 的注册编号为 6。

逻辑端口、逻辑端口号

在表中作为数据源的 Multi-Port Monitor 设备上的逻辑端口和端口号。

MAC 地址、MAC 地址 1、MAC 地址 2、IP 地址 MAC

在选定会话期间指定所分配 IP 地址的服务器的媒体访问控制地址。指定的“1”或“2”针对成对的数据视图显示，表示主机之间数据流的方向。

名称、名称 1 或名称 2、服务器名称、客户端名称

主机（客户端或服务器）的名称。对于一些视图，指示客户端或服务器名称。对于其他视图，显示主机时未考虑其客户端或服务器角色。指定的“1”或“2”针对成对的数据视图显示，表示主机之间数据流的方向。

网络名称、网络名称 1、网络名称 2

定义为要在 ADA 中进行监视的网络的名称。指定的“1”或“2”针对成对的数据视图显示，表示网络之间数据流的方向。

网络子网、网络子网 1、网络子网 2

网络子网的 IP 地址。指定的“1”或“2”针对成对的数据视图显示，表示子网之间数据流的方向。

数据包速率

以数据包数/秒为单位度量的服务器处理效率。该吞吐量值对于容量计划来说非常重要，因为它提供了服务器负载或使用情况的相关信息。

数据包速率从、数据包速率到

选定主机所发送或接收数据的吞吐量（以数据包数/秒为单位）。

数据包

数据量（以数据包为单位）。在选定时段以及选定客户端-服务器会话期间发送和接收的数据包总数。

数据包从、数据包到

数据量。选定主机发送或接收的数据包总数。

端口 1、端口 2

发送或接收与对话或会话有关的数据的主机上的端口。

会话 ID

TCP 会话的 ID 号。内部标识符。

ToS

IPv4 标头中“服务类型”字段的位设置。

ToS 说明

TOS 设置的标准说明，如“默认流量”或“最大吞吐量”。

TCP 字节

TCP 数据量（以字节为单位）。在选定时间段内选定主机或主机对发送和接收的 TCP 总字节数。

TCP 数据包

TCP 数据量（以数据包为单位）。在选定时间段内选定主机（或主机对）发送和接收的 TCP 总数据包数。

VLAN

虚拟局域网的 ID 号。

“TCP”选项卡上的数据

数据表的“TCP”选项卡将排除非 TCP 数据包，并显示 CA Application Delivery Analysis 和 CA APM 通过所有 Multi-Port Monitor 逻辑端口监视的数据。只有那些适用于选定视图的列才会显示在表中。以下列表描述了“TCP”选项卡所有可能的列。

应用程序

应用程序名称源于 CA Application Delivery Analysis 配置或众所周知的端口使用。可用时，请提供应用程序名称。否则，将在括号中显示端口号。

应用程序 ID

用于标识应用程序的一对值中的第二个值。内部标识符。

应用程序类型

标识 Multi-Port Monitor 数据库中的应用程序。大多数情况下，表示此应用程序的状态，因为它涉及到 CA Application Delivery Analysis。下列类型之一：

- **n/a**：未知协议。
- **受监视**：应用程序使用 TCP。CA Application Delivery Analysis 将会监视此应用程序。

  如果有多个收集设备要向一个 CA Application Delivery Analysis 管理控制台报告，则可能有一个不同的收集设备为 CA Application Delivery Analysis 监视此应用程序。指定的应用程序类型是指仅此 Multi-Port Monitor 主动监视的项。
- **UDP-未监视**：应用程序已在 CA Application Delivery Analysis 中定义，但使用了 UDP。CA Application Delivery Analysis 不监视 UDP。
- **TCP-未监视**：应用程序已在 CA Application Delivery Analysis 中定义并使用 TCP。但是，CA Application Delivery Analysis 未监视该应用程序。
- **TCP-未知**：应用程序使用 TCP，但未在 CA Application Delivery Analysis 中定义。“应用程序”列显示“端口 *X*”。
- **UDP-未知**：应用程序使用 UDP，而 CA Application Delivery Analysis 不监视 UDP。应用程序未在 CA Application Delivery Analysis 中定义，或未在已知 UDP 端口的 Multi-Port Monitor 列表中定义。“应用程序”列显示“端口 *X*”。

客户端 IP 地址

客户端-服务器会话中客户端计算机的 IP 地址。

客户端名称

客户端-服务器会话（对话对）中客户端计算机的主机名。

客户端端口

发送或接收数据的客户端上的端口。

观测到的 CT

连接次数观测。在选定时间间隔内产生的受监控 TCP 连接数。它可以更好地体现使用级别以及衡量度量标准重要性。例如，许多观测可以表示影响用户的事件。

DTT

数据传输时间。服务器开始响应与完成发送数据之间的处理时间。影响该值的因素有多个，如响应大小、可用带宽以及应用程序和网络之间的交互。如果发送的数据比 TCP 窗口中所允许的最多数据多，则排除初始服务器响应时间，并且仅包括 NRTT。该值与交付所有数据所需的网络往返传输数以及每次往返传输产生的延迟有关。

ENRTT

有效的网络往返传输时间。包括 NRTT 和重新传输延迟（重新传输对事务造成的延迟）。反映用户实际体验的延迟，并且充当重新传输造成性能下降的指示器。

第 3 层协议

网络层协议（IP 或 ARP）的名称，或数据包标头中“Ethertype”字段的 ID 编号。如果找到 IEEE 802 Ethertype 值，则表示“Ethertype=X”。

第 3 层协议编号

网络层协议的十进制注册编号，如 IPv4 的注册编号 2048。

第 4 层协议

传输层协议的名称，如 TCP。

第 4 层协议编号

传输层协议的十进制注册编号，如 TCP 的注册编号为 6。

逻辑端口、逻辑端口号

在表中作为数据源的 Multi-Port Monitor 设备上的逻辑端口和端口号。

NCT

网络连接时间。客户端确认服务器连接情况所用的时间。通常，网络延迟会造成连接时间延迟。NCT 充当载体延迟的基准并与 NRTT 值进行比较。

NRTT

网络往返传输时间。数据包在网络上的服务器和客户端之间往返传输所用的时间（不包括重新传输产生的延迟）。该值不包括应用程序和服务器处理时间。与 NCT 值相比，该值通常更有用。

重新传输

重新传输延迟。重新传输造成的其他 NRTT 延迟。重新传输是指数据丢失之后重新传输的数据包。数据表示为所有观测的平均值，而不是每个事务的实际重新传输时间。重新传输延迟造成客户端确认延迟时，NRTT 值将增大。该度量标准不会显示因 TCP 拥塞造成的 DTT 丢失影响。该度量标准仅反映从服务器到客户端的数据丢失，而不反映从客户端到服务器的数据丢失。

SCT

服务器连接时间。从服务器接收客户端发出的 SYN 数据包，到服务器发送第一个 SYN/ACK 所用的时间。

打开一个 TCP 连接需要交换三个数据包：SYN、SYN/ACK 和 ACK。TCP 标头具有 SYN（表示同步）和 ACK（表示确认）位。第一个数据包设置了 SYN 位。第二个数据包设置了这两个位。第三个数据包只设置了 ACK 位。此交换将会建立连接的初始序号。

SCT 和 NCT 构成了“连接建立时间”度量标准。

服务器 IP 地址

客户端-服务器会话中服务器的 IP 地址。

服务器 MAC、客户端 MAC

用于标识主机的唯一媒体访问控制地址。

服务器名称

客户端-服务器会话（对话对）中服务器的主机名。

服务器网络名称、客户端网络名称

定义为要在 CA Application Delivery Analysis 中进行监视的网络的名称。指定的“客户端”或“服务器”针对成对的数据视图显示，并且表示网络之间数据流的方向。

服务器网络子网、客户端网络子网

网络子网的 IP 地址。指定的“客户端”或“服务器”针对成对的数据视图显示，并且表示子网之间数据流的方向。

服务器端口

发送或接收数据的服务器上的端口。

SRT

服务器响应时间。服务器响应客户端请求所用的时间。服务器速度、应用程序设计和请求量都会影响 SRT。

TCP 字节丢失

数据丢失，表示为发送和接收的 TCP 字节百分比。

TCP 字节速率从、TCP 字节速率到

TCP 吞吐量（以位为单位）。在选定时段内选定服务器和客户端之间的数据速率（以位/秒为单位，每秒字节数 x 8）。

重新传输的 TCP 字节速率

重新传输的数据和总数据的比率，受监控网络上丢失的数据百分比，以及以位/秒为单位的丢失率。

TCP 字节

TCP 数据量（以字节为单位）。在选定时段内的网络上观测到的应用程序层的总字节数。

TCP 字节从、TCP 字节到

TCP 数据量（以字节为单位）。在选定时段内选定服务器发送至客户端或从客户端接收的应用程序层总字节数。

TCP 数据包丢失

数据丢失，表示为发送和接收的 TCP 数据包百分比。

TCP 数据包速率

TCP 吞吐量（以数据包为单位）。在选定时间段内的数据速率（以每秒数据包数为单位）。ADA 报告使用术语“数据速率”。

TCP 数据包速率从、TCP 数据包速率到

TCP 吞吐量（以数据包为单位）。在选定时段内从选定服务器到客户端或从客户端到服务器的数据速率（以每秒数据包数为单位）。

重新传输的 TCP 数据包速率

重新传输的数据和总数据的比率，受监控网络上丢失的数据百分比，以及以每秒数据包数为单位的丢失率。

TCP 数据包

TCP 数据量（以数据包为单位）。在选定时段内网络上数据包的总数。包括零字节数据包，如 TCP 确认。

TCP 数据包从、TCP 数据包到

TCP 吞吐量（以比特数为单位）。选定时段内的数据速率（字节数/秒 x 8）。CA Application Delivery Analysis 报告使用术语“数据速率”。

重新传输的 TCP 字节数

因数据丢失而重新传输的 TCP 字节数。

重新传输的 TCP 数据包数

因数据丢失而重新传输的 TCP 数据包数。

ToS

IPv4 标头中“服务类型”字段的位设置。

ToS 说明

TOS 设置的标准说明，如“默认流量”或“最大吞吐量”。

事务时间

从客户端发送请求（数据包级别或事务级别）到客户端接收响应中的最后一个数据包所用的时间。

事务时间 Obs

事务发生次数观测。在选定时间间隔内产生的受监控 TCP 事务数。它可以更好地体现使用级别以及衡量度量标准重要性。例如，许多观测可以表示影响多个用户的事件。

VLAN

虚拟局域网的 ID 号。

网络和主机的字节计数

“TCP”选项卡从客户端网络的角度显示活动。“通信量”选项卡显示常规网络活动，而不考虑哪个对话主机是客户端，哪个对话主机是服务器。如果同一子网中的一对主机交换了数据，则在每个选项卡中，同一对话的字节计数可能不同。

在“通信量”选项卡中，同一子网中对话的字节总计看起来可能是“TCP”选项卡中显示的总计的两倍。当他们退出网络时*以及*当他们再进去时，在两个位置显示的*两个主机*之间交换的总字节数会匹配上。总计中包含了两个方向交换的数据量，而不按主机区分统计。

在反映客户端透视图的“TCP”选项卡中，由*一台主机*在同一时段内发送和接收的字节数相匹配。结果是一个总字节数值，该值小于“通信量”选项卡中的总字节数值。

在数据表中添加或删除列

默认情况下，某些数据已从“通信量”和“TCP”选项卡上的数据表中排除。您可以包含更多数据列。

遵循这些步骤:

1. 单击“编辑列”。

   将打开“编辑列”对话框。

2. 选中您要添加到数据表中的度量标准对应的复选框。
3. 清除您要从数据表中删除的度量标准对应的复选框。
4. 单击“默认”还原默认的列设置。
5. 单击“保存”。

   刷新数据表后，数据表中将反映所做的更改。

第 6 章： 导出数据

此部分包含以下主题：

导出数据到 PDF 文件

可以使用 PDF 格式共享分析中的图表，不过存在以下限制：

- 不会导出数据表。
- 不会导出用于解释图表中的颜色的图例。因此，对于线形趋势图和积堆趋势图格式，请通过电子邮件以链接形式发送视图。

应用到当前图表的所有筛选将在导出的分析中保留。

遵循这些步骤:

1. 显示要导出的数据：
   a. 在“分析”窗格中单击数据视图。
   b. 应用更多筛选，或按选定列排序数据表。
2. 单击“导出”>“到 PDF”。
   将打开“文件下载”对话框。
3. 选择是要打开还是保存文件。
   - 如果单击“打开”，则 PDF 显示在 Acrobat Reader 应用程序中。
   - 如果单击“保存”，请使用“另存为”对话框浏览到文件保存位置，然后单击“保存”。

   当前图表将导出到一个扩展名为 .pdf 的文件中。标签标识了数据视图、活动筛选、数据的时间范围和生成 PDF 的时间。

导出数据到 CSV 文件

可以将分析中的数据表导出到按逗号分隔值 (.csv) 格式的电子表格。应用到数据表的所有筛选将在导出的分析中保留。

作为最佳实践，请选择精确的数据段以限制电子表格的大小：

- 向定义的逻辑端口应用硬件筛选。
- 向选择的数据视图应用筛选。
- 使用“时段”选择器选择一个相对较小的时段。

遵循这些步骤:

1. 显示要导出的数据：
   a. 在“分析”窗格中单击数据视图。
   b. 应用更多筛选，或按选定列排序数据表。
2. 单击“导出”>“到 CSV”。
   将打开“导出到 CSV”对话框。
3. （*可选*）在“导出行限制”字段中键入要导出的最大数据表行数。或者选择“没有限制”导出数据表中从选定时段开始的所有行。
4. 单击“确定”。
   将打开“文件下载”对话框。
5. 要最大程度地缩短下载时间，请单击“保存”。
   注意：不建议使用打开文件的选项。如果在尝试导出大量数据时选择该选项，下载将花费更长的时间。
6. 输入或浏览到文件保存位置，然后单击“确定”。
   选择的详细信息将导出到扩展名为 .csv 的文件中。此过程可能需要数分钟才能完成，具体取决于数据库中可用的数据量以及您提供的行限制。

导出数据到 PCAP 文件

您可以将当前视图的数据包捕获数据导出到 PCAP 格式的数据包捕获文件。数据包捕获文件是基于原始捕获文件构建的，它显示当前分析中包含的所有会话的数据包。

PCAP 格式广泛应用于网络跟踪文件，以及其他用于检查和交换数据包级数据的方法。PCAP 与 WinPcap (Windows) 和 libpcap (UNIX) 兼容。使用这些应用程序编程接口的应用程序可轻松读取和显示 PCAP。

管理员以及具有 CA Application Delivery Analysis 调查角色权限的用户可以使用“导出到 PCAP”功能。默认情况下，只有“IT 工程师”和“IT 经理”角色允许访问该功能。

提示：

- PCAP 文件导出可以需要一段时间才能完成。打开“文件下载”对话框所需的时间取决于导出的数据量。
- 缩小分析的时间范围可以改善“导出到 PCAP”功能的性能。缩小时间范围可以减少在其中搜索相关数据包的原始捕获文件的数目。使用“时段”选择器或图表时间控件可放大所需的时间范围。
- 删除含有所需数据的原始捕获文件后，“导出到 PCAP”功能将不可用。捕获文件的保留时间短于度量标准数据库中度量标准数据的保留时间。
- 对于 IPv4（TCP 和 UDP）标头（包括扩展标头），“每数据包最大字节数”参数的“仅标头”选项适用。如果在导出非 IP 通信量时选择“仅标头”，则仅会接收第 2 层 MAC 标头。此时，应选择一个字节值（例如 128），以查看每个帧的更多信息。
- 会话级性能数据仅适用于 Multi-Port Monitor 逻辑端口上接收的基于 IPv4 的端口镜像数据。
- 可以在协议分析器（又称*数据包探查器*，如免费工具 Wireshark）中查看 PCAP 文件。协议分析器将观测通过网络的数据流，并检查每个数据包的副本。它们在图形用户界面中显示数据包标头中每个字段的内容，而用户可以在图形用户界面中筛选、排序和分析数据。
- 协议分析器是一个非常有用的工具，可帮助诊断与分析 Multi-Port Monitor 捕获到的数据。使用协议分析器需要了解以太网、IP 和第 4 层协议数据包的结构。

请执行以下步骤：

1. 显示要导出的数据：
   a. 在“分析”窗格中单击数据视图。
   b. 应用更多筛选，或按选定列排序数据表。
2. 单击“导出”>“到 PCAP”。
   “导出到 PCAP”对话框显示了要导出的数据包跟踪的时间范围。
3. 在“逻辑端口”字段中选择收到了您要导出的数据的端口。显示了每个可用端口的会话数和通信量（以字节为单位）。这些统计数据基于当前筛选（如时间范围和视图）。它们不指示您要导出的文件大小。
   对于每个导出的 PCAP 文件只选择一个端口。
4. 在“每数据包最大字节数”字段中选择要从每个数据包包含的最大字节数。默认选项是只在 PCAP 文件中包含标头。
5. 单击“确定”。
   将打开“另存为”对话框。
6. 选择一个位置用于保存导出的 PCAP 文件。
7. 单击“保存”。

通过电子邮件共享数据

发送分析的链接通常是最快的数据共享方法。“电子邮件”选项将基于分析构建一个 URL，并使用默认邮件客户端来创建电子邮件。

限制

- 必须安装电子邮件客户端。要使用电子邮件功能，请在用户访问 Web 界面时所用的计算机上安装电子邮件客户端并配置 SMTP 服务器。
- 收件人必须拥有一个有权查看“分析”页面的用户帐户。
- 收件人必须在数天内查看分析，超过这些天数后，基础数据将从数据库中清除。

遵循这些步骤:

1. 显示要导出的数据：
   a. 在“分析”窗格中单击数据视图。
   b. 应用更多筛选，或按选定列排序数据表。

2. 单击“电子邮件”。

   您的消息传送应用程序中将打开一条空白消息。消息正文中显示了 URL。“主题”行中显示了日期和时间。该日期和时间表示生成电子邮件的时刻，而不是分析的时间范围。分析的时间范围显示在“分析”页面的“显示”区域中。

3. 键入收件人地址并单击“发送”。

   发送给收件人的电子邮件包含分析 URL 的链接。

附录 A： 命令行语法

Multi-Port Monitor 设备的默认用户名和密码提供超级用户访问权限。您可以在 Linux 命令行界面上使用“sudo”前缀（用于标识超级用户命令）执行以下操作。

sudo /sbin/service nqmaintd status

验证维护后台程序 (nqmaintd) 的状态。

sudo /sbin/service nqmaintd restart

重新启动维护后台程序。仅当状态消息指示该进程正在运行时才使用。

sudo /sbin/service nqmaintd start

启动维护后台程序。仅当状态消息指示该进程已停止时才使用。

sudo /opt/NetQoS/scripts/stopprocs.sh

停止所有后台程序（进程）。

sudo /opt/NetQoS/scripts/startprocs.sh

启动所有后台程序（进程）。

sudo /sbin/shutdown -h now

立即停止设备。在停止该设备前，请先停止 Multi-Port Monitor 数据库。

sudo reboot

立即停止并重新启动设备。在停止该设备前，请先停止 Multi-Port Monitor 数据库。

sudo /opt/NetQoS/scripts/doVerticaCmd.sh --shutdown

停止 Vertica 度量标准数据库。也可以从 Web 界面停止数据库。

sudo /opt/NetQoS/scripts/doVerticaCmd.sh --start

启动 Vertica 度量标准数据库。

sudo /opt/NetQoS/scripts/doVerticaCmd.sh --status

验证 Vertica 度量标准数据库的状态。也可以从 Web 界面验证状态。

sudo /opt/NetQoS/tui/tui-setup.php

在设备上调用网络设置实用工具。

sudo /opt/NetQoS/scripts/syncNapatechClock --force

将 Multi-Port Monitor 捕获卡上的时钟与系统时钟立即同步。该命令会暂时停止 nqcapd 和 nqmetricd 进程，且不中断监视。同步时钟后，将重新启动这两个进程。

附录 B： 正则表达式语法

对于高级筛选，写入“条件”字段的语法将自动遵循捕获卡兼容性的供应商规范。查看生成的表达式（尤其是用于表达式分组的括号的位置），以确认是否会按正确的顺序评估这些表达式。例如，以下分组：

```
(A OR B) AND C
```

与以下分组的结果不同:

```
A OR (B AND C)
```

可以在“条件”字段中编辑语法。

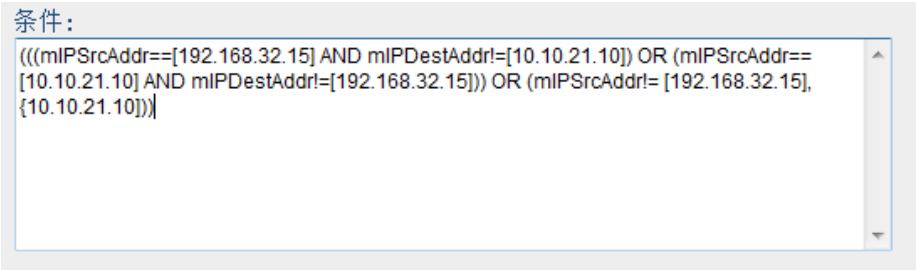
Multi-Port Monitor 筛选包括与条件匹配的数据包。在创建用于将数据包从特定主机或子网中*排除*的筛选时请特别小心。请与 CA 技术支持人员讨论与表达式语法相关的任何问题。

示例

您想要忽略主机 A (192.168.32.15) 和主机 B (10.10.21.10) 之间的某个对话。该对话代表一个自动备份进程，该进程每周运行一次，并且每次都会偏离基准。您想要针对“所有其他通信量”生成报告。您还想要保留传入除已排除对以外的主机的通信量中的所有数据包。因此，您可以创建一个保留以下数据包的筛选：

- 主机 A 是源，但目标不等于主机 B 的所有数据包，OR
- 主机 B 是源，但目标不等于主机 A 的所有数据包，OR
- 源地址不等于主机 A 和主机 B 的 IP 地址的所有数据包（所有其他通信量）。

在“条件”字段中，正确的语法类似于以下：



如果以英语书写，您创建的表达式大致如下所示：

```
(IP Source Address EQUALS 192.168.32.15 AND IP Destination Address does NOT EQUAL 10.10.21.10) OR (IP Source Address EQUALS 10.10.21.10 AND IP Destination Address does NOT EQUAL 192.168.32.15) OR (IP Source Address does NOT EQUAL 192.168.32.15, 10.10.21.10)
```

在创建包含正则表达式的高级筛选时，选择“Equals”会插入“==”，选择“Not Equals”会插入“!=”。