管理员指南

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 界面可以执行管理任务，如监视 Multi-Port Monitor 系统运行状况。

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。以下是默认值。

   - 用户名：admin
   - 密码：admin

   将打开 Web 界面。

详细信息

更改管理员帐户的密码 (p. 10)

第 3 章： 建议的配置

Multi-Port Monitor 的特有设置使其能够以最低配置运行。但是，管理员可以在安装硬件和 Multi-Port Monitor 软件后，对系统进行组织、保护和自定义。

注意：《*CA Application Delivery Analysis Multi-Port Monitor 安装指南*》中介绍了安装任务。

此部分包含以下主题：

配置受信任的 Internet 站点

要改善 Web 界面的性能，请将应用程序的主机名添加到受信任的 Internet 站点列表中。Microsoft Internet Explorer 使用高安全设置，会限制您导航到受信任站点。

在 Internet Explorer 中，可通过单击“工具”>“Internet 选项”>“安全”，来将主机名添加到“受信任站点”列表中。

更改管理员帐户的密码

Multi-Port Monitor 内置有预定义用户帐户，能够提供不同的产品权限。默认的管理员帐户提供对所有配置选项的访问。在以下情况下，请更改此帐户的密码：

- Multi-Port Monitor 将作为 CA Application Delivery Analysis 的监视设备，但尚未部署 CA Application Delivery Analysis。

  注意：在部署 CA Application Delivery Analysis 后，Multi-Port Monitor 将从 CA Application Delivery Analysis 检索包括密码在内的所有用户和角色信息。

- Multi-Port Monitor 仅在 CA APM 环境中与 CA TIM 一起部署。

请执行以下步骤：

1. 在 Web 界面上，依次单击“管理”、“用户”。

   将打开“用户帐户”页面。

2. 单击与管理员帐户对应的“编辑”链接。

   将打开“编辑用户”页面。

3. （*可选*）编辑“说明”字段中的默认文本，以指明更改了默认密码。尽管这是一项可选操作，但该步骤也属于最佳实践的一部分。

4. 在“密码”和“确认密码”字段中删除加密文本并键入新密码。

5. 选中“已启用”复选框。此设置可防止您意外禁用登录 Web 界面时所用的帐户。

6. 单击“保存”。

   新密码随即保存。

详细信息：

什么是用户和角色？ (p. 27)

验证通过端口的数据包流

验证数据包是否流经端口，以确定硬件和软件的安装是否成功。

请执行以下步骤：

1. 在 Web 界面中单击“系统状态”。
2. 查看“捕获卡物理端口状态”部分，了解以下信息：
   - 在适配器上连接的端口。
   - 通过每个端口接收的数据包数。

   如果端口处于活动状态，则表示配置成功。

确认 VLAN 标识符

将 CA Application Delivery Analysis 将逻辑端口上标记的 VLAN 通信分配给域时，我们建议您确认镜像到逻辑端口的通信量已正确标记。请确保：

- VLAN 通信在两个方向中都被标记。

  要正确计算 1 分钟的度量标准，逻辑端口必须接收服务器和客户端之间的标记 VLAN 通信量。对于仅在单向中标记的会话，“分析”页面不会报告 1 分钟度量标准。

  如果只有一个方向有 VLAN 标记：

  - 在 TCP 对话下，会话被列出，除了在“到”或“从”方向的一个数据包之外，不会包含任何度量标准。
  - 在“分析”页面上，通信量作为两个单独的单向会话来报告。
- VLAN 通信量通过单个 VLAN 标识符来标记。

  Multi-Port Monitor 通过数据包头中的第一个 VLAN 标识符来识别 VLAN 通信量。如果您的通信量通过多个 VLAN 标识符来标记，并且 VLAN 标识符的顺序不同，Multi-Port Monitor 将无法正常监控通信量。

配置逻辑端口

Multi-Port Monitor 设备有二个，四个或八个物理端口，它通过这些端口从网络中的交换机接收数据。连接到镜像端口后，将为每个物理端口分配一个逻辑端口定义，该定义与 Multi-Port Monitor 适配器上的 ID 编号相对应。

将名称与逻辑端口关联，以便轻松识别 CA Application Delivery Analysis 中用于 TIM 的监视器源。可以更改默认的逻辑端口定义。

CA CEM TIM 不支持基于 VLAN 的监视器源。不要将 TIM 逻辑端口上的 VLAN 通信量分配给域。

还可以使用逻辑端口设置来限制从每个镜像会话捕获和监视的数据量。端口筛选确定了要在捕获文件中包含或排除的受监视网段或主机以及数据类型。

CA Transaction Impact Monitor (CA TIM) 监视来自一个逻辑端口的多个镜像端口，而不管 Multi-Port Monitor 设备上是否有多个逻辑端口可用。要将多个物理端口映射到一个逻辑端口，请将 Web 通信从 WAN 镜像到该逻辑端口。为 CA TIM 和 CA CA Application Delivery Analysis 处理该通信量。将其他逻辑端口用于其他端口镜像，最理想的是从最接近服务器的访问层交换机。仅为 CA Application Delivery Analysis 处理非 TIM 逻辑端口。

遵循这些步骤:

1. 在 Web 界面上，依次单击“管理”、“逻辑端口”。将打开“逻辑端口”页面。
2. 在“名称”字段中指定端口的新名称。名称可帮助您识别想要监视的通信源，例如，核心交换机的名称或位置。
3. 选择“已启用”来启用要监视的端口。
4. （*可选*）选择“将数据包保存到磁盘”，将捕获的数据包保存在设备的硬盘驱动器上。

   注意：禁用此选项时，数据包将受到如下影响：

   - 不会保存数据包捕获文件。
   - 数据包捕获文件不可用于通过 CA Application Delivery Analysis 启动的数据包捕获调查。
   - 数据包捕获文件不可用于“导出到 PCAP”功能。

5. 选择“TIM”以标识您要配置为 CA TIM 端口的端口。仅当 Multi-Port Monitor 设备上安装了 CA TIM 时，才提供此复选框。您还可以使用此选项来启用或禁用到 TIM 的数据包。

   注意：禁用此选项时，数据包将受到如下影响：

   - 数据包将不会发送到 TIM。
   - TIM 的逻辑端口筛选设置将保留。

6. 单击“筛选”，为您配置的端口启用硬件筛选。有关详细信息，请参阅使用硬件筛选管理数据 (p. 14)。

   CA TIM 监视的 Web 通信量必须具有完整的数据包。

7. 选中相应的复选框，将物理端口分配（映射）到逻辑端口。可用端口数取决于购买的捕获卡配置。您可以将两个或更多个物理端口映射到一个逻辑端口。在使用非对称路由的环境中，此配置可提供更精确的监视，并可让您监视主要电路和故障转移电路。

   逻辑端口编号从 0 开始。捕获层将物理端口映射到逻辑端口。映射进程对于 CA TIM 是透明的。

8. 单击“保存”。
9. 对于要配置的每个端口，重复步骤 2 至 8。
10. 如果更改了除“名称”字段以外的任何参数，请重新启动 (p. 45) nqcapd 进程。
11. （*可选*）在“系统状态”页面上的“捕获卡逻辑端口状态”表中查看逻辑端口状态。

详细信息：

捕获卡逻辑端口状态 (p. 38)
什么是数据包切片？ (p. 14)
正则表达式语法 (p. 63)

使用硬件筛选管理数据

硬件筛选可进一步细化通过交换机处理的数据，因此可以优化 Multi-Port Monitor 的性能。例如：

- 如果网络中的数据量极大，您可以向选定的逻辑端口定义应用筛选或数据包切片。
- 您可以通过选择特定的 IP 地址或子网来细化数据捕获。

筛选选项包括优先顺序，以及按协议、VLAN、子网或 IP 地址以及端口包含或排除的数据包。通过数据包切片功能，您可以限制写入磁盘的数据包部分或大小。

作为逻辑端口定义的一部分，Multi-Port Monitor 筛选和数据包切片选项将基于每个端口进行应用。您可以设置筛选优先级，以确定应用筛选的顺序。

硬件筛选不同于分析筛选，后者可应用到捕获的数据。

- 硬件筛选会影响数据*捕获*。
- 分析筛选会影响数据*显示*。

当某个数据包与启用的筛选的条件匹配时，就会捕获通信量。包含重叠指令的筛选将根据其“优先级”设置按顺序应用。捕获卡提供了有限数目的硬件筛选资源。使用这些筛选可以细化针对镜像通信量的限制。

提示：您可以使用硬件筛选来细化捕获的数据。但是，不要使用硬件筛选来代替正确配置的镜像端口，后者在捕获数据之前就会筛选数据。

详细信息：

端口镜像 (p. 57)
配置逻辑端口 (p. 12)

什么是数据包切片？

Multi-Port Monitor 筛选包括一个数据包切片选项，可让您有选择性地丢弃所捕获帧的某些部分。

当数据量较大并且所需的数据位于数据包标头中时，通常会部署数据包切片。要进行 CA Application Delivery Analysis 监视，通常不需要数据包负载。数据包切片可降低 Multi-Port Monitor 负载，并使用较少的资源存储捕获文件。

“全部通信量 - 仅标头”筛选指定捕获所有类型的数据包并将其切片，以仅保留其标头。此筛选会将数据包切片为从帧到标头的大小，加上一个负载字节。除非您添加了一个筛选或编辑了此筛选，否则，将对新安装中的所有新逻辑端口定义应用数据包切片。此筛选可最大限度地提高 Multi-Port Monitor 性能，同时仍能捕获使用 CA Application Delivery Analysis 进行监视所需的全部数据。

Multi-Port Monitor 设备上安装的网络适配器提供了用于数据包切片的选项，包括固定长度的截断，以及按协议的动态截断。捕获卡执行两种类型的切片：

固定切片

帧大小将被截断为您可以设置的最大指定长度（以字节为单位）。

动态切片

帧大小将被截断为包含标头后的最大长度，例如，整个 TCP 标头加上 8 个负载字节。在计算丢弃的负载数据位置时，卡会考虑封装或 TCP 选项。

什么是默认硬件筛选？

硬件筛选指定由逻辑端口监视的协议、服务器和端口。捕获卡基于您指定的优先级应用多个硬件筛选。要进行更精细的捕获，可以筛选特定的 IP 地址或 TCP 端口。

在某一逻辑端口上创建多个硬件筛选时，它们将被视为 OR 元素。如果满足任意硬件筛选所指定的标准，则会捕获通信量。筛选优先级表示应用筛选的顺序。因此，如果筛选中存在重叠标准，则可使用优先级来确定其他选项（例如，切片）。

为了最大限度地提高可用系统资源，建议您筛选所需的通信量。您可以自己创建硬件筛选，也可以使用 CA Multi-Port Monitor 附带的硬件筛选：

全部通信量 - 仅标头

为所有协议捕获标头信息再加上一个负载字节。默认情况下，此筛选处于“已启用”状态。将此筛选用于：

- CA Multi-Port Monitor。包括非 TCP 通信的数据量度量标准
- CA Application Delivery Analysis。数据包捕获调查仅包括标头

HTTP - 完整数据包

在端口 80 和端口 443 上捕获具有完整负载的 HTTPS 数据包。默认情况下，该筛选处于“已禁用”状态。将此筛选用于：

- CA TIM
- CA Application Delivery Analysis。Web 应用程序的数据包捕获调查包括完整的数据包

TCP - 仅标头

为 TCP 协议捕获标头信息再加一个负载字节；来自其他所有协议的数据包将被丢弃。默认情况下，该筛选处于“已禁用”状态。将此筛选用于：

- CA Multi-Port Monitor。不包括非 TCP 通信的数据量度量标准
- CA Application Delivery Analysis。数据包捕获调查仅包括标头

配置硬件筛选

您可以创建、启用、禁用和修改预定义筛选以及您自己创建的筛选。例如，如果要临时禁用某个筛选，同时保留其筛选设置，可以禁用该筛选。

配置硬件筛选时，单个字段（例如，“IP 地址”）中所列的标准将视为 OR 元素。例如，如果您指定 IP 地址列表，则当数据包源地址或目标地址与该列表中的任意 IP 地址匹配时，数据包则符合该筛选。

如果使用多个字段，则每个字段的标准都将视为 AND 元素。因此，如果您既指定 IP 地址列表又指定端口号，则当源地址或目的地址匹配该列表中的任意 IP 地址且源端口或目标端口匹配指定端口时，数据包便符合该筛选。

如果单击硬件筛选的“显示详细信息”链接，则可查看组合不同字段时所用的逻辑。所用语法遵循 Napatech 指定硬件筛选时的相关要求；mIPSrcAddr、mIPDestAddr、mTCPSrcPort 和 mTCPDestPort 等关键字则为用于表示数据包字段的宏。

如果要创建更为复杂的筛选，则可通过“高级硬件筛选”页面来构建表达式。

遵循这些步骤:

1. 在 Web 界面上，依次单击“管理”、“逻辑端口”。将打开“逻辑端口”页面。
2. 在您要筛选的逻辑端口对应的“编辑筛选”列中，单击“筛选”链接。将打开“逻辑端口: 硬件筛选”页面。

3. *要创建筛选，请单击“新建”*。将打开“逻辑端口: 新建硬件筛选”页面。

   a. 完成以下字段：

   - **已启用筛选**。选择此选项以应用筛选。基于下面的选项分析通过筛选的数据包：

     将数据包发送到 ADA。筛选的数据包将根据网络级别度量标准进行分析，并显示在 Multi-Port Monitor Web 界面的“分析”选项卡中，然后根据控制台的配置发送到 Application Delivery Analysis 控制台中。此选项始终处于选中状态，无法关闭。

     将数据包发送到 TIM。筛选的数据包将根据应用程序级别度量标准和事件，由 Multi-Port Monitor 上的 CA APM Transaction Impact Manager (TIM) 进行分析。必须安装 TIM 才能显示此选项。

     筛选名称。您正创建或编辑的筛选的名称。筛选名称显示在应用筛选的逻辑端口的“硬件筛选”页面上。

   - **筛选优先级**。优先级确定了筛选条件重叠时优先执行哪个筛选。如果两个或更多个重叠的筛选具有相同的优先级，则这种优先权是不确定的。值的范围为 0（最高优先级）到 62（最低优先级）。默认优先级为 10。

     可以结合数据包切片使用筛选优先级设置。例如，您希望保留每个 HTTP 数据包的更多字节。可以为 TCP 和端口 80 指定筛选，同时将切割设置为“TCP 标头 + 50 字节”，优先级设置为 1。然后为 TCP 指定其他筛选，同时将切割设置为“TCP 标头 + 1 字节”，优先级设置为 10。在此方案中，为 HTTP 通信量保留的负载字节数比其他 TCP 通信量要多。

   - **数据包切片模式**。使用这些选项，可以只捕获每个数据包的选定部分。硬件筛选可让您捕获除 TCP/IP 以外的协议的数据包。但是，Multi-Port Monitor 只收集 TCP 通信量的性能度量标准。将收集所有通信类型的数据量度量标准。

     捕获完整数据包：捕获经过筛选的每个数据包的所有信息。

     捕获固定大小：从每个数据包捕获部分字节。在“数据包切片大小”字段中，指定要捕获的字节数。

     捕获标头及指定大小：捕获所有第 2 层、第 3 层和第 4 层标头，再加上“数据包切片大小”字段中指定的固定负载字节数。第 2 层标头包括 Ether II、LLC、SNAP 和原始标头以及 VLAN、ISL 和 MPLS 标记。第 3 层标头包括 IPv4（包括 IPv4 选项）和 IPX 标头。第 4 层标头包括 TCP、UDP 和 ICMP 标头。

- **仅包括协议**。限制要捕获和处理的协议。监视中只包括选定的协议。如果不选中任何复选框，则包括所有协议。传输控制协议 (TCP) 是 CA Application Delivery Analysis 监视的主要协议。用户数据报协议 (UDP) 用于传输实时或流应用程序发送的数据。Internet 控制消息协议 (ICMP) 用于服务器间的错误消息传递以及 CA Application Delivery Analysis 跟踪路由调查。
- **VLAN**。要监视的或要从监视中排除的虚拟局域网 (VLAN) 的标识符。列出其通信量将会通过指定逻辑端口的 VLAN 的标识符。使用逗号（不要加空格）分隔多个 VLAN。选择“排除”可丢弃来自所列 VLAN 的通信量。
- **子网**。要监视的或要从监视中排除的子网。提供有效的 IPv4 地址和子网掩码。选择“排除”可丢弃来自所列子网的通信量。

  对于 IPv4 地址，使用以下格式：x.x.x.x/*n*，其中 x.x.x.x 是采用点分表示法的 IPv4 子网地址，*n* 是用于掩码的位数。
- **IP 地址**。要监视或要从监视中排除的各个主机的 IPv4 地址或地址范围。用逗号分隔多个地址（不含空格）。用连字符分隔范围（不含空格）。选择“排除”可丢弃来自所列地址的通信量。

  对 IPv4 地址使用点分表示法。例如，10.9.7.7,10.9.8.5-10.9.8.7
- **端口**。要监视的或要从监视中排除的 TCP 端口或端口范围。使用逗号（不要加空格）分隔多个端口号。对于端口范围，请使用以下格式：2483-2484。选择“排除”可丢弃来自所列端口的通信量。

b. （*可选*）单击“高级”以使用正则表达式来创建更精确的筛选 (p. 20)。

c. 单击“保存”。新的筛选将显示在“逻辑端口: 编辑硬件筛选”页面上。

4. *要修改或启用筛选*，请单击“编辑”。将打开“逻辑端口: 编辑硬件筛选”页面。

   a. 填写步骤 3a 中所述的字段。

   b. （*可选*）单击“显示详细信息”，查看您用正则表达式表示的选择。

   c. 单击“保存”。修改后的筛选将显示在“逻辑端口: 硬件筛选”页面上。

5. 重新启动 (p. 45) nqcapd 进程以应用更改。

使用正则表达式进行精确筛选

“硬件”筛选可以包括正则表达式，用于精确控制捕获或丢弃的数据。在创建筛选时，可以应用正则表达式。

遵循这些步骤:

1. 创建硬件筛选。
2. 在“逻辑端口: 新硬件筛选”页面上单击“高级”。将打开“逻辑端口: 新高级硬件筛选”页面。
3. 完成以下字段：
   - **已启用筛选**。在指定了名称的逻辑端口上应用筛选。如果已选择，则会在重新启动 nqcapd 进程后应用筛选。
   - **筛选名称**。您正创建或编辑的筛选的名称。筛选名称显示在应用筛选的逻辑端口的“硬件筛选”页面上。
   - **筛选优先级**。优先级确定了筛选条件重叠时优先执行哪个筛选。如果两个或更多个重叠的筛选具有相同的优先级，则这种优先权是不确定的。值的范围为 0（最高优先级）到 62（最低优先级）。默认优先级为 10。

     可以结合数据包切片使用筛选优先级设置。例如，您希望保留每个 HTTP 数据包的更多字节。可以为 TCP 和端口 80 指定筛选，同时将切割设置为“TCP 标头 + 50 字节”，优先级设置为 1。然后为 TCP 指定其他筛选，同时将切割设置为“TCP 标头 + 1 字节”，优先级设置为 10。在此方案中，为 HTTP 通信量保留的负载字节数比其他 TCP 通信量要多。
   - **数据包切片模式**。使用这些选项，可以只捕获每个数据包的选定部分。硬件筛选可让您捕获除 TCP/IP 以外的协议的数据包。但是，Multi-Port Monitor 只收集 TCP 通信量的性能度量标准。将收集所有通信类型的数据量度量标准。
     - 捕获完整数据包：捕获经过筛选的每个数据包的所有信息。
     - 捕获固定大小：从每个数据包捕获部分字节。在“数据包切片大小”字段中，指定要捕获的字节数。
     - 捕获标头及指定大小：捕获所有第 2 层、第 3 层和第 4 层标头，再加上“数据包切片大小”字段中指定的固定负载字节数。第 2 层标头包括 Ether II、LLC、SNAP 和原始标头以及 VLAN、ISL 和 MPLS 标记。第 3 层标头包括 IPv4（包括 IPv4 选项）和 IPX 标头。第 4 层标头包括 TCP、UDP 和 ICMP 标头。

4. 在字段列表和空白字段中构建您的表达式。将捕获与筛选语法*匹配*的所有数据包。不接受通配符。

   a. 从第一个列表中，选择您要筛选的数据包标头中的字段。默认情况下，该筛选*包括*通信量。请选择与应用该筛选的逻辑端口上的通信数据对应的项。要创建一个筛选来*排除*通信量，请指定*除*您要排除的通信量以外的全部通信量。

      - **VLAN ID**：要包括其数据的虚拟 LAN (VLAN) 的标识符。指定要在所提供空字段中以逗号分隔的列表形式包括的 VLAN ID。例如，要包括来自 VLAN 165 和 140 的通信量，请输入 165,140。如果您尚未向该逻辑端口添加筛选，则将捕获具有其中任何一个 VLAN 标识符的数据包。您还可以指定一定范围的 VLAN，如 140-165。此类筛选包含范围较广。
      - **封装**：应用到某个数据包的封装。为通过捕获文件包含的封装类型提供一个值。有效值如下：

        VLAN：筛选类别，指定在筛选操作中包含带有 VLAN 标头的所有数据包。

        MPLS：多协议标签交换网络体系结构。MPLS 将为包含标签的每个数据包附加一个标头，以控制数据包路由（包括服务质量和 TTL 信息）。

        ISL：适用于高性能链接的专有 Cisco VLAN 封装方法。
      - **第 3 层协议**：要在筛选操作中包含的第 3 层协议。如果选择该选项，那么请指定一个协议或用逗号分隔的协议列表。有效值为 IP 和 IPv4。
      - **第 4 层协议**：要在筛选操作中包含的第 4 层协议。指定一个协议或用逗号分隔的协议列表。有效值为 TCP、UDP 和 ICMP。
      - **IPv4 源子网**、**IPv4 目标子网**：要包含在筛选操作中的子网的 IP 地址。选择“IPv4 源子网”或“IPv4 目标子网”，或者单击 AND 或 OR 按钮以将它们添加到正则表达式中。该筛选将应用到数据包标头中的“源”或“目标”字段。提供 IP 地址和子网掩码的位数。使用以下语法：123.45.67.0/24。
      - **IPv4 源 IP 地址**、**IPv4 目标 IP 地址**：要在筛选操作中包含的主机的完整 IPv4 地址。该筛选将应用到数据包标头中的“源”或“目标”字段。您可以输入一个 IPv4 地址、逗号分隔列表或范围。使用标准语法，如 123.45.67.89，或 123.45.67.8,123.45.67.15，或 123.45.67.8-123.45.67.15。
      - **TCP 源端口**、**TCP 目标端口**：单个端口号、逗号分隔的端口号列表或要在筛选操作中包含的连字符连接的端口号范围。该筛选将应用到数据包标头中的“源”或“目标”端口字段。

   b. 从第二个列表中选择条件：“等于”(==) 或“不等于”(!=)。

c. 在空白字段中，键入与您在步骤 a 中所做选择关联的值。

d. （*可选*）要向筛选添加更多条件，请单击布尔运算符按钮之一（AND 或 OR），然后重复步骤 a 至 d。

筛选语法将显示在“条件”字段中。

5. 单击“保存”。该筛选将显示在“逻辑端口: 硬件筛选”页面上。

6. 在启用筛选后，重新启动 (p. 45) nqcapd 进程。

设置全局首选项

您可以配置影响自动收集、存储和转发数据方式的全局设置，例如以下设置：

- 数据包捕获文件的保留小时数。
- 自动数据库维护的频率。
- 是否启用消除重复数据包。

在多数情况下，默认设置能够满足您的需要。但是，您可以更改这些设置，以确保系统以最佳状态运行。

遵循这些步骤:

1. 在 Web 界面中，依次单击“管理”>“应用程序设置”。将打开“应用程序设置”页面。

2. 完成以下字段：

   - **执行自动文件维护间隔**。每两次执行自动文件维护操作相隔的分钟数。在维护期间，将根据需要删除最旧的原始数据包捕获文件。此设置确定了删除捕获文件的频率。默认值为 5。如果您更改了该设置，请重新启动 nqmaintd 进程。删除原始数据包的阈值也会影响删除文件的频率。

   - **当磁盘空间占用正常时，保留原始数据包捕获文件**。在自动删除原始数据包捕获文件之前，这些文件的存储时间长度。在正常监视期间，会不断地生成这些文件。默认值为 6。如果您更改了该设置，请重新启动 nqmaintd 进程。

   - **自动删除达到磁盘利用率之前超过一小时的原始数据包捕获文件**。在自动清除一小时前的原始数据包捕获文件之前，可以使用的最大磁盘空间百分比。自动文件维护间隔也会影响删除文件的频率。默认值为 80%。此阈值不会应用到数据包捕获调查文件。如果您更改了该设置，请重新启动 nqmaintd 进程。

- **保留 Application Delivery Analysis 数据包捕获调查文件**。在自动删除数据包捕获调查文件之前，这些文件的存储天数。这些文件是在响应 CA Application Delivery Analysis 发出的数据包捕获调查请求时生成的。数据包捕获调查文件与原始捕获文件分开存储。此阈值不会应用到原始数据包捕获文件。默认值为 90。如果您更改了该设置，请重新启动 nqmaintd 进程。
- **保留一分钟会话度量标准。**基于捕获的数据包生成的度量标准数据在 Multi-Port Monitor 数据库中的保留天数。默认值为 7。将向此数据库应用一个内部最大阈值。当数据库中的行数超过 120 亿行时，将保留未超过所选天数的数据。如果超出了阈值，则首先会丢弃最旧的数据。
- **执行消除重复数据包**。启用此设置后，Multi-Port Monitor 会尝试筛选掉可能从镜像端口收到的重复数据包。默认情况下，会启用消除重复。“系统状态”页面将跟踪捕获卡丢弃的数据包数。如果您更改了该设置，请重新启动 nqcapd 进程。
- **加密磁盘上的原始数据包捕获文件**。启用此设置后，原始数据包捕获文件将以加密格式保存在 Multi-Port Monitor 硬盘上。默认情况下，这些文件只包含捕获的所有通信量的标头信息。但是，如果更改了数据包切片选项以保留更多数据包，则这些文件可能包含负载数据。经筛选后包含来自单个服务器信息的数据包捕获调查文件不会加密。加密属于处理器资源密集型功能。启用此选项可能会降低监视设备保存数据包捕获文件的能力。您可以在首次启动 Multi-Port Monitor 时创建一个用于加密的唯一密钥。该密钥以后不可更改。如果您更改了该设置，请重新启动 nqcapd 进程。

3. 单击“保存”。“应用程序设置”页面将会刷新以反映您所做的更改。
4. 如有必要，请重新启动 (p. 45) nqmaintd 进程或 nqcapd 进程。

详细信息：

消除重复数据包 (p. 59)
捕获卡物理端口统计 (p. 39)
停止或重新启动进程 (p. 45)
什么是数据包切片？ (p. 14)
清除数据库中的数据 (p. 48)

创建 SNMP 陷阱

SNMP 报警功能在 CA Application Delivery Analysis 突发事件功能的基础上增加了一层错误报告功能。借助 SNMP 报警功能，Multi-Port Monitor 可执行一些自我监视任务，并发送陷阱通知以警告您出现了可能会影响性能的状况。

nqsnmptrap_[Date].log 文件中标识了触发 SNMP 陷阱的状况。有关详细信息，请参阅查看系统日志 (p. 45)。

当检测到错误状况时，系统会自动将 SNMP 陷阱发送到第三方监视应用程序。您可以修改 SNMP 陷阱设置，以更改发送陷阱的原因。陷阱在“管理信息库”(MIB) 中定义，并作为 SNMP v2 通知发出。

Multi-Port Monitor 包括一个含有唯一 OID 的 MIB 文件：CA-MULTI-PORT-MONITOR-MIB。您可以在 Web 界面中，进入“管理”>“SNMP 陷阱”来查看该 MIB 文件的内容。

先决条件：

- 配置要与 Multi-Port Monitor 通信的陷阱接收器。
- 将 CA-MULTI-PORT-MONITOR-MIB 导入该陷阱接收器。导入 MIB 文件的进程取决于特定的陷阱接收器。

遵循这些步骤:

1. 在 Web 界面上，依次单击“管理”、“SNMP 陷阱”。

   将打开“SNMP 陷阱”页面。

2. 键入装有 SNMP 陷阱接收器的计算机的 IP 地址或主机名。
3. 单击“保存”。

   默认情况下，会启用表中显示的所有陷阱，其严重度级别为“警告”。使用此设置意味着不会按默认发送“信息”陷阱。但是，在响应符合“警告”条件或“错误”条件的状况时将会发送陷阱。

详细信息：

复查系统日志 (p. 45)

SNMP 陷阱严重度级别

Multi-Port Monitor SNMP 陷阱与检测影响性能的错误状况的关键进程相关联。对应于以下重要级别的错误状况会触发每个陷阱：

- Info（最低严重度的状况）
- Warning（中等严重度的状况）
- Error（最高严重度的状况）

您可以选择希望 Multi-Port Monitor 发送的最小严重度的陷阱。这样，当任何条件达到或超过最小严重度的条件时，就会发送陷阱。默认情况下，为“Warning”或“Error”严重度启用所有陷阱，但没有为“Info”严重度启用陷阱。

提供以下 SNMP 陷阱：

mtpProcessTrap

当某个 Multi-Port Monitor 进程失败或重新启动时，将发送此陷阱。陷阱文本提供了重新启动的进程的名称。默认情况下，将会针对以下状况发送此陷阱：

- 当 watchdog 进程重新启动了另一个进程时发送“Warning”。
- 当 watchdog 进程重新启动同一进程最大次数时发送“Error”。

mtpCaptureTrap

在响应来自网络适配器（捕获卡）的错误或警告消息时，将发送此陷阱。在适用的情况下，陷阱文本将提供信息用于识别受影响的适配器。

- 当不再连接某个物理端口时发送“Warning”。
- 当 nqcapd 进程在捕获数据包期间遇到问题时发送“Error”。

mtpDiskUsageTrap

当某个文件系统超出了磁盘用量阈值时，将发送此陷阱。

- 当磁盘用量达到 80% 时发送“Warning”。
- 当磁盘用量达到 95% 时发送“Error”。

提示：

- mtpDiskUsageTrap 将监视 /nqtmp/headers 文件系统（一种 RAM 磁盘文件系统）。当 nqmetricd 进程无法充分处理标头文件时，/nqtmp/headers 文件系统超出了阈值。可能的原因包括：
  - nqmetricd 进程无法在 CA Application Delivery Analysis 管理控制台中查询配置信息。请查看 nqMetricReader.log 文件，以获得 SQL 错误的指示。
  - Multi-Port Monitor 设备可能出现了影响 nqmetricd 进程的资源问题。重新启动设备。如果问题持续存在或反复发生，请与 CA 技术支持人员联系。
- mtpDiskUsageTrap 还会监视 /nqtmp/tim 文件系统（一种 RAM 磁盘文件系统）。当 TIM 进程无法充分处理数据包文件时，/nqtmp/tim 文件系统超出了阈值。

mtpRAIDTrap

在响应 RAID 阵列或磁盘驱动器故障时，将发送此陷阱。

- 在正在重建的 RAID 阵列返回“Optimal”状态时发送“Info”。
- 当磁盘 RAID 阵列由于重建磁盘驱动器而下降时发送“Warning”。
- 当发生磁盘 RAID 阵列故障，或者磁盘 RAID 阵列由于检测到磁盘驱动器故障而下降时发送“Error”。

注意：仅当已安装 Adaptec Storage Manager (arcconf) 实用工具时，此陷阱才可用。有关详细信息，请参阅 *《CA ADA Multi-Port Monitor 安装指南》*。

详细信息：

进程信息 (p. 36)
登录到设备 (p. 50)
复查系统日志 (p. 45)

更改陷阱行为

可为每种类型的陷阱更改严重度。对于 mtpDiskUsageTrap，您还可以更改用量阈值。每种类型的陷阱都包括若干个严重度参数。您可以选择会触发陷阱通知的最小严重度级别。严重度级别范围为最低的“Info”到最高的“Error”。

遵循这些步骤:

1. 在 Web 界面上，依次单击“Administration”、“SNMP Traps”。

   “SNMP Traps”页面显示了所配置陷阱接收器的 IP 地址或主机名，以及用于描述 SNMP 陷阱的表。

2. 针对您要禁用或更改的陷阱单击“Edit”。

   将打开“Edit SNMP Trap Settings”页面。

3. 在“Setting”字段中选择该陷阱的严重度级别。

4. 更改“Send Warning trap when disk utilization reaches”字段中的值。默认值为 80。

   注意：该字段适用于 mtpDiskUsageTrap。

5. 更改“Send Error trap when disk utilization reaches”字段中的值。默认值为 95。

   注意：该字段适用于 mtpDiskUsageTrap。

6. 单击“Save”。

   将打开“SNMP Traps”页面。对陷阱设置所做的更改将显示在表中。

什么是用户和角色？

在将 Multi-Port Monitor 配置为 CA Application Delivery Analysis 的监视设备之前，可以使用以下两个默认用户帐户：admin 和 user。

将 Multi-Port Monitor 配置为监视设备之后，它将从 CA Application Delivery Analysis 获取有关用户和角色的信息。CA Application Delivery Analysis 管理员可以创建和管理对 CA Application Delivery Analysis 和 Multi-Port Monitor 有效的安全用户帐户。操作员可以使用这些帐户来访问“系统状态”页面、“分析”页面、“系统设置”页面或“管理”页面。此外，这些帐户将会同步并显示在 Web 界面中的“用户帐户”页面上。

重要说明：Multi-Port Monitor 不会从 CA TIM 或 CA APM 获取有关用户和角色的信息。如果 CA TIM 安装在设备上，*且*该设备不是 CA Application Delivery Analysis 的监视设备，则只有默认的用户帐户适用。

Multi-Port Monitor 安全性与 CA Application Delivery Analysis 完全兼容，并基于登录访问权限。

- 具有 CA Application Delivery Analysis 用户权限以及至少一个角色权限的用户可以查看“系统状态”选项卡中的数据。具有用户产品权限但没有角色权限的用户将被拒绝访问“系统状态”页面。
- 具有 CA Application Delivery Analysis 管理员权限的用户可以访问 Multi-Port Monitor 的“管理”选项卡。

与用户帐户角色关联的权限进一步确定了访问权限。

- 具有 CA Application Delivery Analysis 工程角色的用户可以查看“分析”页面。
- 具有 CA Application Delivery Analysis 调查角色的用户可以查看“分析”页面，并可以使用“导出到 PCAP”功能。

CA Application Delivery Analysis 管理员可以创建更多用户帐户来跟踪 Multi-Port Monitor 状态并配置数据监视。为提高安全性，请更改管理员和用户帐户的默认密码。

详细信息：

更改管理员帐户的密码 (p. 10)

用户帐户信息

Multi-Port Monitor 提供了具有不同产品权限和不同角色的默认用户帐户。使用默认帐户的产品权限可对 Web 界面进行两个不同级别的访问。

用户权限级别

对“系统状态”和“分析”页面进行“仅查看”访问。

管理员权限级别

访问所有产品功能。

分配给每个用户帐户的角色确定了用户可以访问的网页和产品功能。

如果 Multi-Port Monitor 是 CA Application Delivery Analysis 的监视设备，则管理员可以在管理控制台或 CA Performance Center 中创建和修改帐户。这些帐户将被同步并显示在 Multi-Port Monitor Web 界面中。您可以在“管理”>“用户”中查看有关用户帐户的详细信息。

名称

该帐户的用户名和登录 ID。标识用户帐户。标识默认帐户的产品权限级别。

角色

确定用户对产品功能的访问级别。

权限

对产品配置的访问级别，即管理员或用户。只有具有管理员权限的用户才能更改产品配置，例如，设置捕获筛选或更改数据库保留设置。

状态

用户帐户的状态（“已启用”或“已禁用”）。

时区

最有可能使用该用户帐户的操作员的本地时区。

更改用户帐户的属性

用户帐户为有权操作 Multi-Port Monitor 及执行特定任务的人员建立了凭据。可以在 Web 界面的“用户帐户”页面上查看有关默认用户帐户（admin 和 user）的信息。

在将 Multi-Port Monitor 添加为 CA Application Delivery Analysis 的监视设备之前，可以使用 Web 界面来修改默认用户帐户。例如，您可以更改帐户密码、更新关联的时区，或分配其他角色。

注意：在将 Multi-Port Monitor 添加为监视设备并使其同步后，将使用 CA Application Delivery Analysis 中的设置更新这些帐户的设置。在将 Multi-Port Monitor 添加为监视设备后，可使用 CA Application Delivery Analysis 管理控制台或 CA Performance Center 来创建和更改用户帐户。

遵循这些步骤:

1. 在 Web 界面上，依次单击“管理”、“用户”。

   “用户帐户”页面显示预定义的用户帐户以及您创建的自定义帐户。

2. 单击您要编辑的帐户对应的“编辑”链接。

   将打开“编辑用户”页面。

3. 完成以下字段：
   - **说明**。描述帐户或最近的更改。例如，可以指明更改了密码。该可选步骤属于最佳实践的一部分。
   - **密码**、**确认密码**。在每个字段中删除加密文本，然后在每个字段中输入新密码。
   - **产品权限**。选择一个权限级别，用于确定用户是否可以执行管理任务。
   - **角色**。选择一个角色，以确定用户查看报告数据和访问产品功能所具有的权限。
   - **时区**。选择最有可能使用该用户帐户的操作员的本地时区。
   - **已启用**。选中该复选框可防止您意外禁用登录 Web 界面时所用的帐户。要禁用 admin 帐户，请创建另一个具有管理员产品权限的用户，并以该用户的身份登录。然后，您就可以禁用 admin 帐户。
4. 单击“保存”。

角色信息

角色控制对产品菜单和数据源的访问权限。可以通过分配角色来限制用户对产品功能的访问。例如，限制用户对 Multi-Port Monitor 中“系统状态”页面的访问。当角色限制用户的访问权限时，用户将无法查看受限的产品部分。

与用户帐户关联的角色确定了以下限制：

- 用户可访问的菜单和报告页面。
- 用户自定义数据以及深入查看详细信息的能力。

在 CA Application Delivery Analysis 中，每个角色都有一个“区域访问”参数，该参数确定了对 CA Application Delivery Analysis 报告和其他功能（如按需调查）的页面级访问。在注册 CA Application Delivery Analysis 数据源后，相同的角色在 CA Performance Center 中也将起作用。

角色控制的权限不能扩展到管理权限。管理权限是在创建用户帐户时分配给用户的。

Multi-Port Monitor 的“角色”页面是预定义角色名称和说明的只读列表。

IT 经理

适用于 Multi-Port Monitor 和 CA Application Delivery Analysis 的此管理员角色提供对以下 CA Application Delivery Analysis 报告的访问：

- 调查
- 工程
- 操作
- 突发事件
- 管理

IT 工程师

此角色：

- 包括专用于解决所报告问题的用户权限，并提供对下列 CA Application Delivery Analysis 报告的访问权限：
  - 调查
  - 工程
  - 操作
  - 突发事件
  - 管理
- 授予“深入查看数据源”角色权限。该角色权限允许用户从 Performance Center 深入查看数据源（包括 CA Application Delivery Analysis 管理控制台）以及从 CA Application Delivery Analysis 管理控制台深入查看 Multi-Port Monitor。

  重要说明！ Multi-Port Monitor 不会强制实施来自 CA Performance Center 的权限集。例如，如果为用户分配了特定的服务器组，则 Multi-Port Monitor 将显示域中所有服务器的性能数据。

IT 操作员

此角色：

- 包括专用于解决所报告问题的用户权限，并提供对下列 CA Application Delivery Analysis 报告的访问权限：
  - 工程
  - 操作
  - 突发事件
  - 管理
- 不授予“深入查看数据源”角色权限，但是，该角色不会阻止用户登录 CA Application Delivery Analysis 管理控制台以及从该管理控制台深入查看 Multi-Port Monitor。

  重要说明！ Multi-Port Monitor 不会强制实施来自 CA Performance Center 的权限集。例如，如果为用户分配了特定的服务器组，则 Multi-Port Monitor 将显示域中所有服务器的性能数据。

产品权限

*产品权限*是用户帐户的一个方面，用于授予或限制对管理功能的访问权限。

每个产品权限级别都对应于一个预定义角色。CA Application Delivery Analysis 管理员可以向用户帐户分配不同的角色和权限，还可以自定义角色以授予对不同产品区域的访问权限。

Multi-Port Monitor 中不存在“超级用户”产品权限。但是，有权访问 CA Application Delivery Analysis 工程产品区域的“超级用户”可以访问除“管理”页面上功能之外的所有 Multi-Port Monitor 功能。

CA Performance Center 支持 CA Application Delivery Analysis 和 Multi-Port Monitor 中使用的产品权限，但这些权限采用的级别不同。使用产品权限，同一个用户帐户可以在不同的 CA 数据源产品中拥有不同的访问级别。例如，某人可能是 CA Application Delivery Analysis 的用户，他（她）可以查看 CA Performance Center 中的选定项。这同一个人在从 CA Performance Center 视图导航时，还可能是某个 CA Application Delivery Analysis 特定实例的管理员。

所有 Multi-Port Monitor 操作员都有权访问“系统状态”页面。但是，“用户”权限要求至少被授予一个角色权限，才能访问“系统状态”页面。

操作员要访问“管理”页面，必须获得“管理员”产品权限。但是，用户帐户的角色确定了对“分析”区域的访问权限。而另一个区域访问参数又进一步限制了将分析导出为 PCAP 格式的功能。

对 Multi-Port Monitor 中“分析”页面的访问权限与对 CA Application Delivery Analysis“工程”选项卡的访问权限是关联的。用户帐户角色的“区域访问”参数确定了此访问权限。但是，即使获得该访问权限，也不足以允许用户导出 PCAP 文件，因为这需要访问“调查”区域。

在 CA Performance Center 中，产品权限设置与数据源级别的角色设置重叠。要执行以下任务，用户必须拥有对数据源的访问权限，以及最起码的“用户”产品权限：

- 查看报告。
- 深入查看视图。
- 从 CA Performance Center 导航到该数据源。

Multi-Port Monitor Web 界面中保留了 CA Performance Center 中适用的权限以及角色确定的访问权限。

以下列表汇总了 CA Application Delivery Analysis 和 Multi-Port Monitor 中提供的产品权限类型，并说明了其默认访问区域：

管理员级别

此级别通常与“IT 经理”角色关联，提供对以下功能的访问权限：

- “分析”页面
- “系统状态”页面
- 管理页面
- 导出分析到 PCAP 功能

超级用户或调查员级别

Multi-Port Monitor 中未提供预定义的“超级用户”帐户。此级别是“网络工程师”角色的默认级别，并提供对以下功能的访问权限：

- “分析”页面
- “系统状态”页面
- 导出分析到 PCAP 功能

用户级别

此级别是“IT 操作员”角色的默认级别，提供对以下功能的访问权限：

- “分析”页面
- “系统状态”页面

默认的“IT 操作员”角色不允许关联用户将数据导出为 PCAP 格式，其中可能包含敏感数据。要向具有此角色的用户授予必要的区域访问权限，CA Application Delivery Analysis 管理员可将“调查”区域添加到“IT 操作员”角色。

第 4 章： 系统运行状况和维护

Multi-Port Monitor 可执行自我监视，以让系统保持最佳运行状态。此外，管理员还可以执行以下任务：

- 查看系统状态。
- 自定义系统维护选项。
- 停止或重新启动进程。
- 向设备应用软件升级。
- 查看系统日志以进行故障排除。

此部分包含以下主题：

系统状态

“系统状态”页面显示所有活动 Multi-Port Monitor 进程的状态，包括以下度量标准：

- 捕获卡和磁盘性能
- 文件系统状态
- 内存和 CPU 使用情况

用户和管理员都有权访问“系统状态”页面。

系统信息

“系统信息”部分提供有关 Multi-Port Monitor 设备的详细信息。

主机名（IP 地址）

设备的 DNS 主机名和 IPv4 地址。

CA Application Delivery Analysis Manager

CA Application Delivery Analysis 管理控制台的 IPv4 地址，以及指向 CA Application Delivery Analysis 登录页面的链接。

只有设备已配置为 CA Application Delivery Analysis 的监视设备时，才提供这些信息。

Multi-Port Monitor 版本

软件的版本和内部版本编号。

进程信息

Multi-Port Monitor 包括用于捕获数据包、计算度量标准、检查数据包和执行自动系统维护的多个进程或后台程序。“进程信息”部分提供以下进程的经常更新的状态信息：

nqcapd

数据包捕获后台程序。它的日志文件名为 nqnapacapd.log。

提示：要重置端口统计，请重新启动 nqcapd 进程。

nqmetricd

度量标准计算引擎大致相当于 CA Application Delivery Analysis Single-Port Monitor 上的度量标准计算模块。它的日志文件名为 nqMetricReader.log。

nqinspectoragentd

Inspector 后台程序大致相当于 Single-Port Monitor 上的 SA Monitor 服务。它的日志文件名为 nqInspectorAgentd.log。

nqwatchdog

watchdog 进程可监视其他进程的状态并在必要时重新启动这些进程。它的日志文件名为 nqwatchdog.log。

nqmaintd

系统维护后台程序。它的日志文件名为 nqmaintd.log。

sadatatransfermanager

数据传输管理器进程从 Cisco 广域应用程序服务部署中接收和传输数据。当 Multi-Port Monitor 未配置为 CA Application Delivery Analysis 监视设备时，此进程的状态为“已停止”。在您配置监视设备后，此进程将一直运行，即使它未被使用，也是如此。日志文件名为 saDataTransferManager.log。

提示：您还可以通过单击“管理”>“进程”进入“进程状态”页面来查看这些进程的状态。

详细信息：

停止或重新启动进程 (p. 45)

数据库状态

“数据库状态”部分标识 Multi-Port Monitor 设备中高性能数据库的状态。此部分显示本地数据库的名称以及下列状态级别之一：

- 运行
- 停止
- 正在关闭
- 正在初始化

时间戳指示状态更新的时间。

详细信息：

数据库状态和使用情况 (p. 47)

捕获卡物理端口状态

“捕获卡物理端口状态”部分提供有关流过每个端口的通信量的信息，并描述了每条链路。大多数值都是动态更新的，并且浏览器每 5 秒刷新一次。

物理端口

Multi-Port Monitor 设备上的物理端口。

类型

用于连接的电缆类型。

链路状态

到该端口的链路是连接还是未连接。

链路质量

该连接的质量，基于来自网络适配器的信息。指示链路是否已关闭。

链路速度

该链路的正常速度。

详细信息：

捕获卡时钟与系统时钟存在偏差 (p. 56)

捕获卡逻辑端口状态

“捕获卡逻辑端口状态”部分提供每个逻辑端口的状态，以及已处理和已丢弃数据包数。在如下所述的情况下，可将多个物理端口或数据源分配到一个逻辑端口定义：

- 围绕主要电路和故障转移电路组织您的报告。
- 在非对称路由环境中更准确地进行监视。

逻辑端口

“逻辑端口”页面中定义的逻辑端口。捕获卡上的每个物理端口都与一个逻辑端口定义关联。这种关联可帮助您识别数据源 (feed)，并让您聚合数据源 (source)，以便对这些源统一进行监视。逻辑端口定义包括一个端口号、一个名称，以及让您确定所捕获通信量的硬件筛选设置。

逻辑名称

逻辑端口名称。如果未向端口分配名称，将使用默认值：“端口 0”、“端口 1”等等。

状态

该端口所在链路的状态：“已启用”或“已禁用”。

状态

当前端口状态：“正在运行”、“已停止”或“错误”。如果状态为“错误”，将鼠标指针悬停在错误图标上可显示错误原因。

已处理数据包数

指示在应用硬件筛选后由捕获卡传送的数据包总数。在启动或重新启动 nqcapd 进程时，该统计数据将重置。

丢弃数

从该逻辑端口传入的、捕获卡丢弃的以及未处理的数据包数。丢弃数提供了捕获卡负载指数。在正常的性能条件下，丢弃数为零。

详细信息：

配置逻辑端口 (p. 12)

捕获卡物理端口统计

“捕获卡物理端口统计”部分提供流过 Multi-Port Monitor 设备上每个物理端口的数据量的信息。该统计数据是在应用任何硬件筛选之前计算的，因此，该统计数据指示从交换机传入的实际线速。

此部分还列出当前错误数。通过这些信息可验证镜像端口配置，以确保镜像会话不会超载。

在启动或重新启动 nqcapd 进程时，这些统计将会重置为零。

物理端口

数据流向 Multi-Port Monitor 时所经过的物理端口。值为“全部”（基于所有通道的总计）或某个物理端口的标识符。物理端口数取决于使用的捕获卡类型。

逻辑名称

与该物理端口关联的逻辑端口的名称。

已接收数据包数

重置统计数据后接收到的离散数据包数。

已接收字节数

重置统计数据后接收到的字节数。

CRC/对齐错误

具有循环冗余校验 (CRC) 错误或对齐错误的帧数。

已丢弃重复

捕获卡根据其“消除重复”逻辑丢弃的数据包的数目（原因是这些数据包与已收到的数据包重复）。可以在“应用程序设置”页面上启用或禁用自动消除重复。

该值指示镜像端口是否已正确配置。如果较大百分比的捕获通信量包括重复的数据包，请验证端口镜像配置。

接收速率

每秒通过该通道接收的数据包数。

详细信息：

设置全局首选项 (p. 22)
停止或重新启动进程 (p. 45)

RAID 状态信息

“RAID”部分提供 Multi-Port Monitor 设备上 RAID 阵列中的磁盘性能的信息。

注意：仅当已安装 Adaptec Storage Manager (arcconf) 实用工具时，才提供 RAID 信息。有关详细信息，请参阅*《CA ADA Multi-Port Monitor 安装指南》*。

数组

RAID 阵列的标识符。指示信息是适用于“系统”阵列还是“数据”阵列。

状态

阵列的状态：

- 最佳：以最高级别运行
- 下降：不是以最高级别运行
- 失败：未运行；显示错误状态。将指示错误类型以及受影响驱动器的 ID 和序列号。
- 正在重建：正在重新联机。在 RAID 控制器检测到某个正在重建的驱动器后，状态将更改为“Optimal”。同时，阵列仍以“下降”状态运行。仍会收集所有度量标准。

注意：当数据阵列显示某个驱动器的状态为“失败”时，度量标准处理不会中断，但是无法执行数据包捕获调查。您可以在不中断度量标准处理的情况下更换掉失败的驱动器。

类型

RAID 阵列的类型。

- CA6000 Multi-Port Monitor RAID 阵列已配置为 RAID 5。
- CA6300 RAID 阵列：
  - 系统阵列：RAID 1
  - 数据阵列：RAID 6

驱动器数

阵列控制的磁盘驱动器的数目。

失败驱动器

指示已失败的驱动器，即发生错误或正在重建的驱动器。包括驱动器编号、ID 号和序列号。系统阵列驱动器的 ID 号为 1 至 4。数据阵列驱动器的 ID 号为 5 至 16。

文件系统

“文件系统”部分提供 Multi-Port Monitor 设备上的文件系统的使用情况统计。

文件系统

显示了其统计的文件系统的名称。

大小

该文件系统的总容量（以字节数表示）。

已使用

正在使用的文件系统中的字节数。

可用性

该文件系统中可供使用的字节数。

使用百分比

文件系统中已用容量的百分比。

已安装

文件系统在操作系统目录中的安装点。

内存

“内存”部分提供有关内存大小、已用和可用字节的信息以及缓冲统计。

当仍有足够的内存供进程使用时，Linux 可能会显示高内存利用率。原因是，该操作系统将可用内存用于磁盘缓存（已缓存），但在需要时放弃此内存以供进程使用。这是 Linux 操作系统的标准行为，这样做是为了提高性能。

解释内存信息时，请考虑以下情况：

- 如果“可用内存”列的值很低，而“已缓存”数值很高，“使用的交换内存”很低或为零，则表示 Multi-Port Monitor 运行正常。
- 如果“可用内存”列的值很低，“已缓存”数值也很低，而“使用的交换内存”很高（指示 Multi-Port Monitor 正在交换内存），则这可能表示某些进程正在使用大量内存并且可能会影响性能。

Multi-Port Monitor 设备在 64 位 CentOS Linux 上运行。可使用 Linux 的“free –o”命令获取内存信息。将显示以下列：

总计

指示物理内存或交换空间的字节总数。

已使用

指示正在使用的物理内存或交换空间的字节数。请注意，对于物理内存，此数字包括已缓存的字节数。

可用

指示可用的物理内存或交换空间的字节数。

缓冲区

指示内核缓冲区使用的物理内存的字节数。

已缓存

指示内核用于磁盘缓存的物理内存的字节数。

有关 Linux 内存管理的详细信息，请参阅以下文章：

- http://www.linuxhowtos.org/System/Linux%20Memory%20Management.htm
- http://www.itworld.com/it-managementstrategy/280695/making-sense-memory-usage-linux
- http://www.linuxintheshell.org/2012/06/05/episode-008-free-understanding-linux-memory-usage/

CPU

CPU 部分提供有关 CPU 使用情况的信息以及性能统计数据，用于说明 Multi-Port Monitor 性能和负载。

CPU

标识与统计数据对应的设备上的 CPU。以下值之一：

- 全部：所有处理器的平均统计。
- 0 至 15：CPU 标识符 0 至 15。Multi-Port Monitor 平台配有一个支持超线程的四核双 CPU，犹如拥有 16 个 CPU。

用户

在用户级执行的进程使用的 CPU 时间百分比。

Nice

在优先级为 nice 的用户级执行的进程使用的 CPU 时间百分比。内核确定了优先级。

系统

可归因于内核本身的 CPU 用量百分比。

IO 等待

CPU 处于空闲状态，但系统具有未处理的磁盘 I/O 请求的时间百分比。

IRQ

花费在处理中断请求上的 CPU 时间百分比。

Soft

花费在软中断状态上的 CPU 时间百分比。

Steal

当虚拟机监控程序为另一个虚拟处理器服务时，虚拟 CPU 等待实际 CPU 的 CPU 时间百分比。

空闲

CPU 处于空闲状态，并且系统没有未处理的磁盘 I/O 请求的时间百分比。

中断数/秒

CPU 每秒收到的中断总数。

维护任务

一些系统维护会自动执行。另一些任务（如重新启动后台程序或进程）需手动执行。

极少需要登录 Multi-Port Monitor 设备，即使是执行数据库维护。您可以使用 Web 界面来执行以下任务：

- 升级软件。
- 停止和启动进程。
- 打开系统日志并将其保存到文件。
- 生成支持文件。
- 清除数据库中的数据。

升级软件

当提供了新版本或修补程序时，管理员可以升级 Multi-Port Monitor 软件、操作系统和 CA TIM 软件。产品升级文件可以从 CA 技术支持网站下载。

在 Web 界面上，通过“管理”、“升级”页面来升级 Multi-Port Monitor 软件，其中包括先决文件、Multi-Port Monitor 软件和操作系统。通过“系统设置”、“安装软件”页面来升级 CA TIM 软件。

升级 Multi-Port Collector 软件和操作系统

《*CA ADA Multi-Port Monitor 升级指南*》包含有关升级 Multi-Port Monitor 和升级 CentOS 操作系统的完整说明（如果适用）。

升级 CA TIM 软件

升级 CA TIM 的过程与安装 CA TIM 的过程相同。有关详细信息，请参阅安装 TIM 软件。

一般而言，升级过程如下所述：

1. 浏览到保存升级文件的位置。
2. 选择该文件并单击“打开”。
3. 单击“升级”开始升级过程。

   将会出现用于指示修补或升级进度的消息。在出现指示完成的消息之前，请不要从该页面导航到其他位置。

停止或重新启动进程

当出现特定的错误状态，或者您更改了系统范围的设置时，请停止或重新启动 Multi-Port Monitor 进程。

注意：您可以通过 Web 界面重新启动 nqmaintd 进程。但是，您无法通过 Web 界面停止或启动该进程。如果停止了 nqmaintd 进程，请直接登录设备将它启动。

遵循这些步骤:

1. 在 Web 界面中，依次单击“管理”、“进程”。

   将打开“进程状态”页面。“进程”列列出了进程的名称。

2. 在“启动/停止”列中单击用于启动、停止或重新启动进程的链接。

提示：要重置端口统计，请重新启动 nqcapd 进程。

详细信息：

进程信息 (p. 36)

复查系统日志

在 Multi-Port Monitor 进程的日志文件中，可以查看最后 200 个记录的活动行。除了 Multi-Port Monitor 进程的日志外，还可以查看以下日志中的最新条目：

SAService.log

包含 CA Application Delivery Analysis 到 Multi-Port Monitor 之间通信的条目，其中包括检测信号和源状态更新。

此外，还包含对 APM 控制台中的“缺陷详细信息”页面上显示的网络运行状况信息的请求。

SAInvestigations.log

包含 CA Application Delivery Analysis 发出的记录数据包捕获调查请求的条目。

nqsnmptrap.log

包含触发 SNMP 陷阱的每个条件的条目。

遵循这些步骤:

1. 在 Web 界面中，依次单击“管理”、“系统日志”。

   将打开“系统日志”页面。

2. 从“日志文件”字段中选择一个日志文件。

   “系统日志”页面将会刷新以显示选定日志的大小。例如：

   文件 nqInspectorAgentd_20110228.log 的大小为 300160 字节。

3. 单击“查看”。

   “系统日志”页面将会刷新，最多显示选定日志的最后 200 行。

详细信息：

进程信息 (p. 36)

生成支持文件

您可以生成一个支持文件，其中包含对于 CA 技术支持人员来说十分有用的故障排除信息。该支持文件汇编了所有进程的所有最新日志，并以压缩的 tar 格式 (.tgz) 保存数据。

遵循这些步骤:

1. 在 Web 界面中，依次单击“管理”、“系统日志”。

   将打开“系统日志”页面。

2. （*可选*）选择“包括度量标准数据库诊断”，以便包括来自 Multi-Port Monitor 度量标准数据库中诊断实用工具的信息。

   注意：如果选择该选项，则生成支持文件可能需要较长的时间。仅当 CA 技术支持人员指示您这样操作时，才选择该选项。

3. 单击“生成”。

   “系统日志”页面将显示新的支持日志文件的名称。

4. 从“选择要下载的支持文件”字段中选择日志文件。

5. 单击“下载”。

   将打开“文件下载”对话框。

6. 单击“保存”并导航到要保存该文件的位置。

数据库状态和使用情况

“数据库状态”页面上的统计描述了数据库的状态和使用情况。当在“应用程序设置”页面上选择清除（“文件保留”）设置时，将使用这些信息作为指南。“数据库使用情况”部分中的信息特别适用于确定何时清除包含 1 分钟间隔中的度量标准的较旧数据库条目。

“数据库状态”页面提供以下信息：

数据库

Multi-Port Monitor 设备上本地数据库的名称。

状态

数据库的状态：“运行”、“停止”、“正在关闭”或“正在初始化”。

启动/停止

让您启动/停止某个数据库的链路。在关闭或重新启动设备之前，请停止数据库。

Date of oldest data

数据库中数据的最早时间戳。

Date of newest data

数据库中数据的最新时间戳。

Rows in database

数据库中已使用的总行数。最大行数为 120 亿。如果超出了最大阈值，则夜间维护例程会将行数裁剪到 120 亿以下。

Rows for past day

在过去 24 小时内使用的数据库行数。

Rows for past 7 days

在过去一周内使用的数据库行数。

提示：

- “Database Usage”部分提供了用于显示最早和最新数据插入时间的一系列日期，以及多个数据库行计数。这些信息可帮助您衡量数据累积的速度。基于这些信息，您可以调整信息在数据库中的保留天数。
- 要减少添加到数据库的行数，请调整应用到每个逻辑端口的筛选。例如，您可以只捕获 TCP 数据包，而不必使用捕获所有协议通信量的默认筛选。

- 数据库的状态每 60 秒自动更新一次。仅当您导航到“Database Status”页面时，或在刷新浏览器时，行计数才会更新。
- 没有“管理员”产品权限的用户可以在“系统状态”页面上查看数据库状态。所有 Multi-Port Monitor 用户都可以访问“System Status”页面。

详细信息：

设置全局首选项 (p. 22)
命令行语法 (p. 61)
系统状态 (p. 35)
使用硬件筛选管理数据 (p. 14)

清除数据库中的数据

在正常运行期间，Multi-Port Monitor 将对数据库和文件系统执行日常维护。日常维护包括清除各种类型的数据和文件。通常，原始数据包捕获文件在保留六小时后将被清除。包含 1 分钟间隔中性能度量标准的文件在保留一周后将被清除。

您可以出于如下原因手动清除 Multi-Port Monitor 数据库：

- “数据库状态”页面揭露了某个问题。
- “系统状态”页面上的统计指示文件系统几乎已满。
- 您收到了 mpcDiskUsage SNMP 陷阱，指示磁盘用量超出了阈值。

重要说明：已清除的数据将从数据库中永久删除。无法恢复清除的数据。

遵循这些步骤:

1. 在 Web 界面中依次单击“Administration”、“Purge Data”。

   将打开“Purge Data”页面。

2. 选择“Purge all data and metric database tables”可删除所有数据和数据库表。

   该选项将停止收集数据的进程。在重新启动这些进程之前，不收集任何新数据。

   如果选择该选项，页面上的所有其他选项均不可用。

3. 至少选择下列选项中的一个，以便只删除选定的数据。进程将继续运行，并且仍会收集新数据。

   - **Purge one-minute session metrics**。从度量标准数据库中删除 1 分钟会话度量标准。
   - **Purge raw capture files**。删除数据包捕获文件。在正常监视期间，这些文件将不断生成，并用于派生性能统计。默认值为 6。
   - **Purge packet capture investigations**。从数据包捕获调查中删除文件。调查文件与原始捕获文件分开存储。默认值为 90。
   - **Purge log files**。删除 Multi-Port Monitor 创建的日志文件。

4. 选择时间范围，以删除您在步骤 3 中选择的数据。

   - **Purge across all dates**。删除选定类型的数据，不管时间范围如何。
   - **Purge prior to this date**。删除在指定日期之前收集的数据。

     注意: 数据以自协调通用时间 (UTC) 存储。该选项将删除在 UTC 午夜之前收集的数据。当您使用本地时间查看数据时，似乎仍然存在前一天的某些数据。

5. 单击“确定”。
6. 如果按步骤 2 所述清除了所有数据，请重新启动已停止的进程。

详细信息：

设置全局首选项 (p. 22)
数据库状态 (p. 37)
系统状态 (p. 35)
创建 SNMP 陷阱 (p. 24)

登录到设备

通常，在安装硬件和软件之后，无需登录 Multi-Port Monitor 设备。大多数管理任务可以从 Web 界面执行。但是，对于以下任务，您需要直接访问设备：

启动已停止的维护后台程序 (nqmaintd)

要启动或重新启动其他进程，需要启动后台程序。无法从 Web 界面启动或停止后台程序。

关闭或重新启动设备

不需要关闭或重新启动，即使在完成升级后也是如此。但是，要使计算机脱机，请使用登录进程和命令来正确地将它关闭。

在加载或合并操作期间关闭设备可能会损坏本地数据库。在关闭设备前请停止数据库。

使用连接的键盘和监视器直接登录设备。也可以使用 Microsoft Windows 上运行的安全 Shell (SSH) 客户端（如 PuTTY）从远程系统登录。

遵循这些步骤:

1. 在出现初始屏幕时按 Alt+F2。

   将打开 Linux 登录屏幕。

2. 使用以下凭据登录：
   - 用户名：netqos
   - 密码：在您安装 Multi-Port Monitor 软件时创建的密码。

   将打开 Linux 命令行界面。

3. 运行必要的命令。

详细信息：

数据库状态 (p. 37)
命令行语法 (p. 61)

系统设置

“系统设置”页面列出了 Multi-Port Monitor 设备上安装的组件。通常，组件名称显示为超链接，您可以通过该链接查看详细信息。

计算机设置

内部版本编号，以及指向“Machine Settings”页面的链接。使用“Machine Settings”页面可查看网络设置，设置时区，以及关闭或重新启动设备。

Multi-Port Monitor

内部版本编号，以及指向“Administration”页面的链接。使用“Administration”页面可配置数据监视、系统设置和身份验证，以及执行维护。

Multi-Port Monitor Prerequisites

最近下载的先决程序包的内部版本编号。

System Health

内部版本编号，以及指向 Customer Experience Manager (CEM) 控制台上“设备运行状况”页面的链接。使用“Appliance Health”页面可查看有关磁盘和内存用量、登录的用户和正在运行的进程的信息。仅当在设备上安装了 CA TIM 时，该项才可用。

Third-party

设备上安装的 CA TIM 第三方应用程序的版本和内部版本编号。仅当在设备上安装了 CA TIM 时，该项才可用。

TIM

内部版本编号，以及指向 CEM 控制台上“TIM 设置”页面的链接。使用“TIM 设置”页面可停止和启动 CA TIM，以便查看状态和统计数据以及配置 Watchdog 设置。仅当在设备上安装了 CA TIM 时，该项才可用。

详细信息：

计算机设置 (p. 52)

计算机设置

“Machine Settings”页面提供以下页面的链接：

- Network Setup (p. 52)
- Set Time Zone (p. 53)
- System Shutdown/Restart (p. 54)

网络设置

“Network Setup”页面标识了您在安装 Multi-Port Monitor 软件和启用网络访问时创建的网络配置。有关详细信息，请参阅设备随附的*《CA ADA Multi-Port Monitor 安装指南》*。

您可以使用此页面上的字段来更改网络配置。

Select which interface to configure

在该字段中所做的选择确定了该页面上其他字段的内容。选择一个接口并单击“Set”，然后更改其余字段中的信息。页面将会刷新，并指示该接口是否使用了 IPv4 地址。

Automatically obtain IP address settings with DHCP

选择该选项可使用 DHCP（动态主机配置协议）来获取管理 NIC 的 IP 地址。您可以提供管理 NIC 的 DHCP 主机名。

Manual IP Address Settings

选择该选项可键入管理 NIC 的 IP 地址、子网掩码和默认网关地址。

注意：管理 NIC 的 IP 地址必须与 CA Application Delivery Analysis 管理控制台中分配给 Multi-Port Monitor 的 IP 地址一致。

Manual DNS Settings

在“DNS 服务器 1”字段中键入本地 DNS 服务器的 IP 地址。

（*可选*）在“DNS 服务器 2”和“DNS 服务器 3”字段中键入备用 DNS 服务器的 IP 地址。

Submit

单击此项可保留您对网络设置所做的更改。

选择时区

您可以更改 Multi-Port Monitor 设备的时区。

遵循这些步骤:

1. 在 Web 界面中，依次单击“System Setup”、“Machine Settings”。
   将打开“Machine Settings”页面。
2. 单击“Set Time Zone”。
   将打开“Set Time Zone”页面。
3. 选择设备的时区。
4. 在出现确认提示时单击“Set Time Zone”。
   随后将出现一条确认消息。

关闭或重新启动设备

适用于 CA6000 和 CA6300 设备

在关闭或重新启动设备之前，请始终先关闭 Vertica 度量标准数据库。通过以下方式关闭或重新启动设备：

Multi-Port Monitor Web 界面

1. 关闭 Vertica 度量标准数据库：
   a. 单击“管理”以打开“管理”页面。
   b. 单击“数据库状态”以打开“数据库状态”页面。
   c. 单击“停止”以停止“度量标准”数据库。
2. 关闭或重新启动设备：
   a. 单击“系统设置”以打开“系统设置”页面。
   b. 单击“计算机设置”以打开“计算机设置”页面。
   c. 单击“系统关闭/重新启动”。
   d. 单击以下某个选项：
      - **关闭计算机**。选择该选项将会关闭设备。要使设备重新开机，您必须对设备具有物理访问权限。
      - **重新启动计算机**。选择该选项将会关闭设备，然后将其重新启动。在重新启动设备时，Vertica 度量标准数据库会自动启动。

命令行

运行以下命令：

1. 停止 Vertica 度量标准数据库。
   ```
   sudo /opt/NetQoS/scripts/doVerticaCmd.sh --shutdown
   ```
2. 关闭或重新启动设备。

   要关闭设备：
   ```
   sudo /sbin/shutdown -h now
   ```
   要重新启动设备：
   ```
   sudo /sbin/shutdown –r now
   ```

详细信息：

登录到设备 (p. 50)

第 5 章： 故障排除

此部分包含以下主题：

不能正确捕获 IPv6 通信量

症状：

在我尝试捕获 IPv6 通信量时，发生以下错误：

- 切片为“仅标头”的通信量包括 IPv6 标头，但不包括 TCP 标头。
- 基于第 4 层标头信息（如 TCP 端口号）的筛选不会捕获 IPv6 通信量。

解决方案：

您可能需要更新 Napatech 卡上的 FPGA（固件）。下表列出了捕获 IPv6 通信量所需的 FPGA 版本：

Napatech 卡型号	**FPGA 版本**
NT4E (4x1Gb)	200-9015-**42**-08
NTPORT4（4x1Gb 扩充卡）	200-9019-**42**-05
NT20E (2x10Gb)	200-9014-**42**-07

FPGA 版本号中采用粗体文本的部分是决定性因素。该数字小于 42 的 FPGA 不完全支持 IPv6 数据包标头的解码。

可使用以下方法之一来验证 FPGA 的版本：

- 在 Multi-Port Monitor Web 界面中单击“关于”。“关于”页面列出了活动 Napatech FPGA 的版本号。
- 从 Linux 命令行运行以下命令。

  ```
  sudo  /opt/napatech/bin/AdapterInfo
  ```

  输出包括指示活动 FPGA 映像的行。

在升级 Multi-Port Monitor 软件时，不会更新 Napatech FPGA。有关说明与 FPGA 映像，请与 CA 技术支持联系。

捕获卡时钟与系统时钟存在偏差

症状：

我在“系统状态”页面上的“捕获卡物理端口状态”部分看到以下消息：

“捕获卡时钟与系统时钟存在 *N* 秒的偏差”。

解决方案：

捕获卡有一个独立时钟，用于对传入的数据包进行时间戳记。在正常工作状态下，该时钟与 Multi-Port Monitor 系统时钟同步。如果 Multi-Port Monitor 系统时钟与捕获卡上的时钟存在偏差，将会显示该错误消息。例如，当某人手动更改了系统时钟的时间时，就可能发生偏差。

使用以下方法同步时钟：

- **立即同步时钟**。在设备上从 Linux 命令行界面运行以下命令。该命令将会停止 nqcapd 和 nqmetricd 进程，从而中断监视。同步时钟后，这些进程将重新启动。

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

- **维持同步**。运行网络时间协议 (NTP) 来维持时钟之间的同步。可以在设备上使用网络设置实用工具来配置 NTP。要打开该实用工具，请从 Linux 命令行界面运行以下命令：

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

  在该实用工具上的“NTP 服务器”字段中键入 NTP 服务器的主机名或 IP 地址。默认值为 pool.ntp.org。

时间范围超出了原始数据包保留时间

症状：

当尝试以 PCAP 格式导出数据时，我收到了以下警告消息：

时间范围超过了原始数据包捕获保留时间。

解决方案：

Web 界面中的应用程序设置 (p. 22)页面包括一个会影响导出到 PCAP 功能的“文件保留”设置。当要导出的数据来自小于“原始数据包捕获文件的保留时长”设置的时间范围时，就会发生此错误。

使用“系统状态”页面可评估“文件系统”部分中数据的磁盘用量。如果您有足够的可用空间，请增大“原始数据包捕获文件的保留时长”设置的值。将来执行的 PCAP 导出将会包括过去更早日期的数据。

附录 A： 部署最佳实践

此部分包含以下主题：

设备放置

Multi-Port Monitor 设备需要连接到处理要监视通信量的每个网络交换机上的 SPAN 或镜像端口。连接通常在访问层发生。

设备必须能够*观测*到尽可能多的相关网络通信量。请考虑以下问题：

- 要监视哪些应用程序？
- 哪些服务器承载这些应用程序？
- 这些服务器连接到哪些交换机？
- 用户从哪些子网访问监视的应用程序？

如果您的网络或通信量异常地大，您可以购买附加设备来平衡处理负载。

端口镜像

在网络交换机上，*端口镜像*功能用于将来自一个端口的网络数据包的副本发送到另一个交换机或端口以供分析。端口镜像是将通信量镜像到 CA Application Delivery Analysis 监视设备的安全且有效的方式。某些交换机不提供各种 TCP 数据包镜像功能。如果不能对通信量进行最佳镜像，请使用其他方式，例如光纤分流器。

注意：Cisco 交换机上的端口镜像功能被命名为 Switched Port Analyzer (SPAN)。

将用于在受监视服务器上传入或传出通信量的交换机端口镜像到 Multi-Port Monitor 所连接到的端口。正确配置镜像端口后，CA Application Delivery Analysis 就可以监视客户端和服务器之间的应用程序流，而无需使用桌面或服务器代理。

有关详细信息，请参阅*《CA 数据获取最佳实践指南》*。

端口要求

Multi-Port Monitor 设备需要打开多个端口才能支持以下通信路径：

- CA Application Delivery Analysis 与该设备之间。
- Enterprise Manager 与该设备（如果已安装 CA TIM）之间。
- 允许通过 Web 界面访问 Multi-Port Monitor 管理。

端口	方向	说明
80	从 CA Application Delivery Analysis 和 Enterprise Manager 入站	■ 用于 Web 界面访问的 HTTP ■ Enterprise Manager 与 CA TIM 的通信
80	出站到 CA Application Delivery Analysis	Multi-Port Monitor Web 服务对配置数据的请求
161	入站	SNMP MIB 查询
162	出站	SNMP 陷阱
7878	入站	包含来自 WAE 设备的数据包摘要的 TCP 数据流。 **注意**：仅当 WAE 设备是监视器源时才需要。
8080	从 CA Application Delivery Analysis 和 Enterprise Manager 入站	■ CA Application Delivery Analysis Web 服务对数据的请求 ■ Enterprise Manager 对 CA APM 控制台中“缺陷详细信息”页面上显示的网络运行状况数据的请求。
9995	入站	包含来自 CA GigaStor 连接器的数据包摘要的 UDP 数据流。 **注意**：仅当 CA GigaStor 是监视器源时才需要。

消除重复数据包

术语*数据包重复*是指同一通信量通过交换机上的多个接口时会多次进行报告。使用多种端口镜像配置可能会导致重复，因为所有端口的通信量都会转发到 Multi-Port Monitor。

如果存在重复数据包，则可能会偏离收集的度量标准。数据包丢失统计会受到影响，因为重复数据包被视为重传。

作为最佳实践，请配置镜像端口来减少或消除重复数据包。Multi-Port Monitor 提供适用于捕获卡的数据包消除重复设置，并且在默认情况下处于启用状态。该设置会丢弃看似是已处理的数据包重复项的数据包。

在初始端口镜像配置期间，您可以暂时禁用全局设置以消除重复数据包。禁用该设置后，您可以查看重复数据包，从而帮助您消除镜像会话中的重复。

消除重复逻辑适用于在给定逻辑端口上接收的所有数据包。因此，如果在其他逻辑端口上接收到同一 VLAN 中的重复数据包，则不会将其丢弃。如果您将两个物理端口组合到一个逻辑端口定义中，在下列情况下将会丢弃重复项：

- 如果原始数据包到达一个物理端口后，它随即到达另一个物理端口。
- 如果它到达第二个交换机。

如果未将两个物理端口组合到一个逻辑端口中，则这两个数据包都将保留。

附录 B： 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。

详细信息：

登录到设备 (p. 50)
数据库状态 (p. 37)
数据库状态和使用情况 (p. 47)
捕获卡时钟与系统时钟存在偏差 (p. 56)

附录 C： 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。

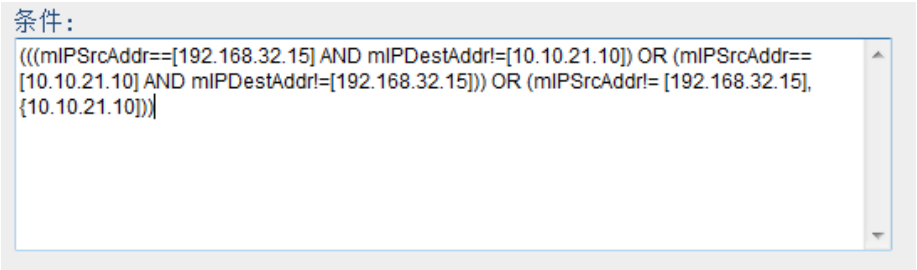
Multi-Port Monitor 筛选包括与条件匹配的数据包。在创建用于将数据包从特定主机或子网中*排除*的筛选时请特别小心。请与 CA 技术支持人员讨论与表达式语法相关的任何问题。

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“!=”。

详细信息：

使用正则表达式进行精确筛选 (p. 20)