

与 CA Transaction Impact Monitor 集成

CA Application Delivery Analysis
Multi-Port Monitor

版本 10.1



本文档包括内嵌帮助系统和以电子形式分发的材料（以下简称“文档”），其仅供参考，CA 随时可对其进行更改或撤销。

未经 CA 事先书面同意，不得擅自复制、转让、翻印、透露、修改或转录本文档的全部或部分内容。本文档属于 CA 的机密和专有信息，不得擅自透露，或除以下协议中所允许的用途，不得用于其他任何用途：(i) 您与 CA 之间关于使用与本文档相关的 CA 软件的单独协议；或者 (ii) 您与 CA 之间单独的保密协议。

尽管有上述规定，但如果您为本文档中所指的软件产品的授权用户，则您可打印或提供合理数量的本文档副本，供您及您的雇员内部用于与该软件相关的用途，前提是所有 CA 版权声明和标识必须附在每一份副本上。

打印或提供本文档副本的权利仅限于此类软件所适用的许可协议的有效期内。如果该许可因任何原因而终止，您应负责向 CA 书面证明已将本文档的所有副本和部分副本已退还给 CA 或被销毁。

在所适用的法律允许的范围内，CA 按照“现状”提供本文档，不附带任何保证，包括但不限于商品适销性、适用于特定目的或不侵权的默示保证。CA 在任何情况下对您或其他第三方由于使用本文档所造成的直接或间接的损失或损害都不负任何责任，包括但不限于利润损失、投资受损、业务中断、信誉损失或数据丢失，即使 CA 已经被提前明确告知这种损失或损害的可能性。

本文档中涉及的任何软件产品的使用均应遵照有关许可协议的规定且根据本声明中的条款不得以任何方式修改此许可协议。

本文档由 CA 制作。

仅提供“有限权利”。美国政府使用、复制或透露本系统受 FAR Sections 12.212、52.227-14 和 52.227-19(c)(1) - (2) 以及 DFARS Section 252.227-7014(b)(3) 的相关条款或其后续条款的限制。

版权所有 © 2014 CA。保留所有权利。此处涉及的所有商标、商品名称、服务标识和徽标均归其各自公司所有。

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：对 CA TIM 的支持	5
端口要求.....	7
第 2 章：在 Multi-Port Monitor 设备上安装 CA TIM	9
停止或重新启动进程.....	10
配置逻辑端口.....	11
配置硬件筛选.....	12
使用正则表达式进行精确筛选.....	15
第 3 章：在 Multi-Port Monitor 设备上升级 CA TIM	19
第 4 章：故障排除	21
未配置 CA TIM 来使用 Napatech.....	21
CA TIM 停止工作.....	21

第 1 章：对 CA TIM 的支持

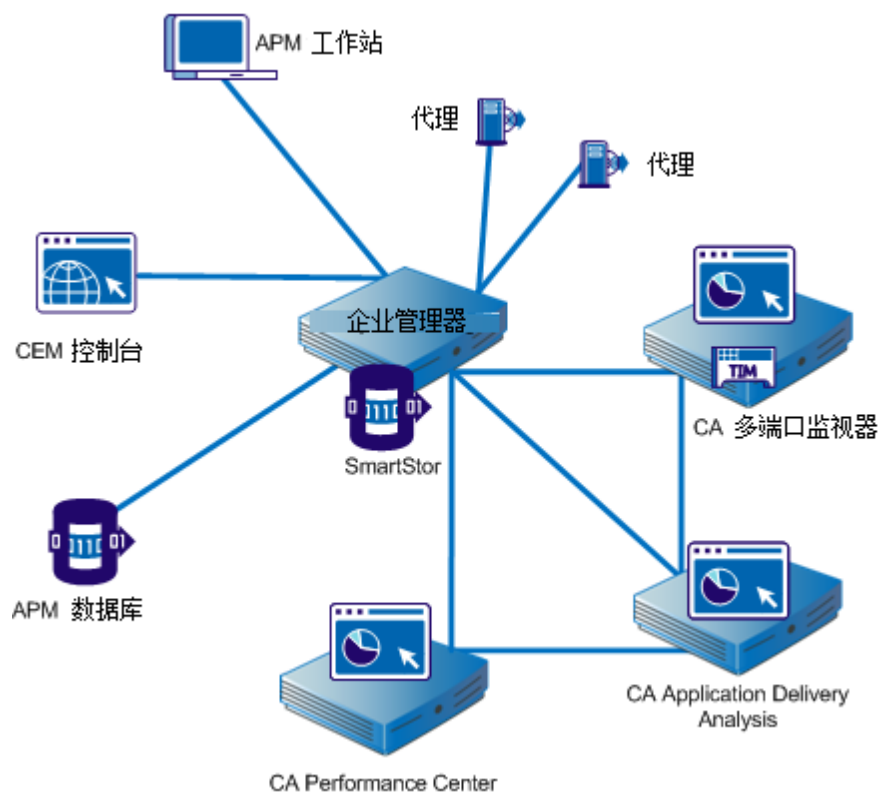
Multi-Port Monitor 捕获 CA Transaction Impact Manager (TIM) 的 HTTP 数据包。

- CA TIM 被动监视镜像端口中的通信量。
- CA TIM 记录 HTTP 和 HTTPS 数据包，以标识以下产品的用户登录及相关事务：
 - CA Customer Experience Manager (CA CEM)
 - CA Application Performance Management (CA APM)
- CA TIM 执行安全套接字层 (SSL) 解码。

在 Multi-Port Monitor 设备上安装 CA TIM 后，得到的聚合设备可让您按用户查看应用程序使用情况的应用程序级和网络级数据。作为独立设备，CA TIM 可实时监视 HTTP 事务，并在检测到异常时生成缺陷。Multi-Port Monitor 每隔 1 分钟提供会话级数据。借助聚合设备，可以使用这种更细致的数据粒度来调查 CA TIM 检测到的缺陷。使用 CA APM 控制台从缺陷深入查看 Multi-Port Monitor Web 界面中的相关数据。

通过 Web 界面，您可以执行 CA TIM 的管理和维护任务。

下图显示了安装有 Multi-Port Monitor、CA APM 和 CA Application Delivery Analysis 的网络中的组件。



如图所示，Multi-Port Monitor 可同时支持 CA TIM 和 CA Application Delivery Analysis。在此方案中，CA TIM 和 CA Application Delivery Analysis 的数据包被并行处理。独立的 RAM 磁盘可帮助缓存两个应用程序的数据包。

- 对于 CA Application Delivery Analysis，Multi-Port Monitor 只提供具有标头的所有数据包。
- 对于 CA TIM，Multi-Port Monitor 提供筛选过、具有完整负载的 HTTP 数据包。

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	<ul style="list-style-type: none"> ■ 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	<p>包含来自 WAE 设备的数据包摘要的 TCP 数据流。</p> <p>注意： 仅当 WAE 设备是监视器源时才需要。</p>
8080	从 CA Application Delivery Analysis 和 Enterprise Manager 入站	<ul style="list-style-type: none"> ■ 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	<p>包含来自 CA GigaStor 连接器的数据包摘要的 UDP 数据流。</p> <p>注意： 仅当 CA GigaStor 是监视器源时才需要。</p>

第 2 章：在 Multi-Port Monitor 设备上安装 CA TIM

Multi-Port Monitor 设备带有一张 CD，其中包含 CA Transaction Impact Manager (CA TIM) 软件。或者，您可以从 [CA 技术支持](#) 下载 CA TIM 软件。

注意：如果只是将 Multi-Port Monitor 与 CA Application Delivery Analysis 结合使用，则不需要安装 CA TIM 软件。

使用 Multi-Port Monitor Web 界面来安装以下文件：

- 第三方映像：third-party-update-xxxxxxxxx.image
- TIM 映像：tim-complete-xxxxxxxxxxxxx.image

遵循这些步骤：

1. 将安装文件下载到可通过 Web 浏览器访问 Multi-Port Monitor 设备的工作站。
2. 以具有管理权限的用户身份登录到 Multi-Port Monitor Web 界面。
将打开 Web 界面。
3. 在 Web 界面中单击“系统设置”>“安装软件”。
将打开“安装软件”页面。
4. 单击“浏览”并导航到下载安装文件的位置。
5. 选择 third-party-update-xxxxxxxxx.image 文件。
6. 单击“打开”。
该文件的名称将显示在“安装软件”页面上。
7. 单击“上传并安装”。
8. 阅读并接受许可协议。
此时将打开软件安装日志。如果日志中包含以红色文本显示的错误，请与 CA 技术支持人员联系。
9. 在“安装软件”页面上单击“浏览”，并导航到下载安装文件的位置。
10. 选择 tim-complete-xxxxxxxxxxxxx.image 文件，然后重复步骤 6 至 8。
11. 在 Web 界面中单击“系统设置”。
安装成功后，安装的文件名称将显示在“系统设置”页面上。

12. 标识要用于 CA TIM 监视的逻辑端口。有关详细信息，请参阅[配置逻辑端口](#) (p. 11)。
13. 启用“HTTP - 完整数据包”硬件筛选以捕获完整数据包：
 - a. 在 Web 界面上，依次单击“管理”、“逻辑端口”。
 - b. 单击与 CA TIM 监视关联的逻辑端口对应的“筛选”链接。
将打开“逻辑端口: 硬件筛选”页面。
 - c. 单击“HTTP - 完整数据包”筛选对应的“编辑”链接。
将打开“逻辑端口: 编辑硬件筛选”页面。
 - d. 选中“已启用筛选”复选框。
 - e. 重新启动 nqcapd 进程。

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。

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 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。

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. 10) 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。

配置硬件筛选

您可以创建、启用、禁用和修改预定义筛选和您创建的筛选。

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**。在指明名称的逻辑端口上应用筛选。如果已选定，将在重新启动 `nqcapd` 进程之后应用筛选。
- **筛选名称**。正在创建或编辑的筛选的名称。该筛选名称将显示在已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）、IPv6 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 监控的主要协议。

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** 用于服务器之间错误消息传递以及 CA Application Delivery Analysis 跟踪路由调查。其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。

- **VLAN。**需要进行监控或从监控中排除的虚拟局域网 (VLAN) 的标识符。列出其流量通过指定逻辑端口的 VLAN 的标识符。用逗号分隔多个 VLAN (不含空格)。选择“排除”可放弃所列出 VLAN 的通信。
- **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，或有效的 IPv6 地址和前缀位。不要组合使用列表中的 IPv4 和 IPv6 地址。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。

对于 IPv6 地址，使用以下格式：**x:x:x:x/n**，其中 **x:x:x:x** 是以冒号分隔的 IPv6 子网地址，**n** 是前缀位数。您可以使用标准缩写的 IPv6 地址。例如，**2001:ba0:1a0::/48**

提示：要对 IPv4 和 IPv6 子网进行筛选，请分别对 IPv4 子网和 IPv6 子网创建一个硬件筛选。

- **IP 地址。**需要进行监控或从监控中排除的各个主机的 IPv4 或 IPv6 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)。不要组合使用列表中的单个地址和范围。不要组合使用同一列表中的 IPv4 和 IPv6 地址或地址范围。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** 或 **10.9.8.5-10.9.8.7**。

使用冒号分隔的 IPv6 地址。您可以使用标准缩写的 IPv6 地址。例如，**2001:f0d0:1002:51::4**

提示：要对 IPv4 和 IPv6 地址进行筛选，请分别对 IPv4 地址和 IPv6 地址创建一个硬件筛选。

端口。需要进行监控或从监控中排除的 TCP 端口或端口范围。用逗号分隔多个端口号 (不含空格)。对于一系列端口，请使用以下格式：**2483-2484**。选择“排除”可放弃所列出端口的通信。

- b. (可选) 单击“高级”以使用正则表达式来创建更精确的筛选。
 - c. 单击“保存”。新的筛选将显示在“逻辑端口: 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”以正则表达式查看您的选择。
 - c. 单击“保存”。该筛选将显示在“逻辑端口: 硬件筛选”页面上。
 5. 在启用筛选后, [重新启动](#) (p. 10) nqcapd 进程。

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](#) (p. 12)。
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. 10) nqcapd 进程。

第 3 章：在 Multi-Port Monitor 设备上升级 CA TIM

当有新版本可用时，管理员可以升级 CA TIM 软件。产品升级文件可以从 [CA 技术支持网站](#) 下载。

使用 Multi-Port Monitor Web 界面来安装以下文件：

- 第三方映像：third-party-update-xxxxxxxxx.image
- TIM 映像：tim-complete-xxxxxxxxxxxxx.image

遵循这些步骤：

1. 将安装文件下载到可通过 Web 浏览器访问 Multi-Port Monitor 设备的工作站。
2. 以具有管理权限的用户身份登录到 Multi-Port Monitor Web 界面。
将打开 Web 界面。
3. 在 Web 界面上，依次单击“管理”、“升级”页面。
将打开“升级软件”页面。
4. 单击“浏览”并导航到下载安装文件的位置。
5. 选择 third-party-update-xxxxxxxxx.image 文件。
6. 单击“打开”。
该文件的名称将显示在“升级软件”页面上。
7. 单击“上传并安装”。
8. 阅读并接受许可协议。
此时将打开软件安装日志。如果日志中包含以红色文本显示的错误，请与 CA 技术支持人员联系。
9. 在“升级软件”页面上单击“浏览”，并导航到下载安装文件的位置。
10. 选择 tim-complete-xxxxxxxxxxxxx.image 文件，然后重复步骤 6 至 8。
11. 在 Web 界面中单击“系统设置”。
如果升级成功，则您安装的文件名称将显示在“系统设置”页面上。

第 4 章：故障排除

此部分包含以下主题：

[未配置 CA TIM 来使用 Napatech](#) (p. 21)

[CA TIM 停止工作](#) (p. 21)

未配置 CA TIM 来使用 Napatech

症状：

我在 CA TIM 错误日志中看到以下消息：

安装了 Napatech 软件，但 TIM 未配置为使用 Napatech。

解决方案：

此消息是在 Multi-Port Monitor 设备上安装 CA TIM 时出现的。由于 Multi-Port Monitor 已配置为管理 Napatech 卡，因此您可以放心地忽略此消息。

CA TIM 停止工作

症状：

安装在 Multi-Port Monitor 上的 TIM 停止功能的运行。例如，它已经停止记录和生成统计信息。另外，我在 TIM 日志中看到“跳过旧数据包”消息。

解决方案：

如果 Multi-Port Monitor 上安装了 Tim，则 Multi-Port Monitor 上的 NapaTech 卡将使用该卡上的时间来标记数据包到达时间。如果 Multi-Port Monitor 的系统时间和 NapaTech 卡的时间不同，那么 TIM 可能会无法正常运行。

存在两种可能情况。请确定哪种情况适用于您。

1. TIM 处理有时可能落后于 Multi-Port Monitor 中的数据包文件。例如，如果 TIM 停止然后重新启动，或 Multi-Port Monitor 生成数据包文件的速度比 TIM 使用的速度快。通过执行以下任务来确认 TIM 滞后时间：
 - a. 确认 NapaTech 卡的时间已与 Multi-Port Monitor 的系统时间同步。
 - b. 查看 Multi-Port Monitor 系统状态页面并验证该页面上未显示警告消息。

如果您已经确认上述两种情况，则表示 TIM 没有错误。TIM 不会处理 15 分钟以前的数据包文件（该默认值可以更改）。忽略这些旧数据包文件之后，TIM 将恢复正常处理。TIM 只是需要时间来赶上 Multi-Port Monitor 生成的文件。

2. 比较 NapaTech 卡的时间与 Multi-Port Monitor 的系统时间。在终端上使用以下命令以查看 NapaTech 卡的时间：

```
/opt/napatech/bin/TimeConfig -cmd time_get
```

在终端上使用以下命令可查看 Multi-Port Monitor 系统时间：

```
date
```

如果这两个时间不同，且 Multi-Port Monitor 的“系统状态”页面显示一条警告消息，则查看 NapaTech 卡的时间以及网络时间协议 (NTP) 服务器上的时间。

在下列网站选择时区可获取 NTP 时间：

```
http://www.time.gov/
```

考虑以下情况并确定哪一种适用于您。

情况 1

条件

- Napattech 卡的时间与 NTP 时间差异较大（超过 15 分钟）。
- Multi-Port Monitor 的系统时间与 NTP 时间存在很小的差别（不到 5 秒）。

操作

- 运行以下命令，将 NapaTech 时间与系统时钟同步：

```
/opt/NetQoS/scripts/syncNapattechClock
```
- 如果 NapaTech 时间与 Multi-Port Monitor 的系统时间的差异不到 5 分钟，则 NapaTech 驱动程序操作系统同步将逐渐调整 NapaTech 时钟。如果 NapaTech 时间与 Multi-Port Monitor 的系统时间的差异超过 5 分钟，则 NapaTech 时间将立即与 Multi-Port Monitor 的系统时间同步。

情况 2

条件

- NapaTech 卡的时间与 NTP 时间略有不同。
- Multi-Port Monitor 的系统时间和 CEM 控制台时间与 NTP 时间存在很大差异。

操作

- 调整 CEM 控制台时间，以便与 NTP 时间同步。
- 等待并确认 Multi-Port Monitor 的系统时间已设置并已与 NTP 时间同步。
- 确认 Multi-Port Monitor 的 ntpd 进程正在运行。如果未运行，则启动该进程。

Multi-Port Monitor 的系统时间与 NTP 时间的差异超过 1000 秒时，ntpd 进程可能自动停止。

情况 3

条件

- NapaTech 卡的时间与 NTP 时间差异**较大**。
- Multi-Port Monitor 的系统时间和 CEM 控制台时间与 NTP 时间存在**很大**差异。

操作

- 调整 CEM 控制台时间，以便与 NTP 时间同步。
- 等待并确认 Multi-Port Monitor 的系统时间已设置并已与 NTP 时间同步。
- 确认 Multi-Port Monitor 的 ntpd 进程正在运行。如果未运行，则启动该进程。
- 运行以下命令，将 NapaTech 时间与系统时钟同步：
`/opt/NetQoS/scripts/syncNapatechClock`

