

# 与 CA Application Delivery Analysis 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

---

<b>第 1 章：对 CA Application Delivery Analysis 的支持</b>	<b>5</b>
数据包捕获调查.....	6
CA Application Delivery Analysis 支持的体系结构 .....	7
与 CA Application Delivery Analysis Standard Monitor 的比较.....	8
网络地址转换 (NAT).....	10
CA Application Delivery Analysis 数据概述 .....	11
端口要求.....	12
<b>第 2 章：将 Multi-Port Monitor 配置为监控设备</b>	<b>13</b>
添加监视设备.....	13
验证逻辑端口的状态.....	16
复查 TCP 会话信息.....	16
<b>第 3 章：监视设备的突发事件</b>	<b>19</b>
启用监视设备突发事件.....	20
响应非活动监视设备突发事件.....	21
<b>第 4 章：对特殊初始化 (.ini) 文件的支持</b>	<b>23</b>
消除重复数据包.....	24
筛选出保持连接消息.....	25
<b>第 5 章：在 WAN 优化的环境中进行监视</b>	<b>27</b>
CA Application Delivery Analysis 支持 Cisco WAAS .....	27
Multi-Port Monitor 如何与 WAN 优化设备集成.....	28
CA Application Delivery Analysis 优化报告 .....	28
共享来自 WAN 优化设备的数据.....	29



# 第 1 章：对 CA Application Delivery Analysis 的支持

---

Multi-Port Monitor 设备聚合基于 IPv4 的 TCP 度量标准，并将其导出到 CA Application Delivery Analysis。该设备比多个 Standard Monitor 收集数据的速度更快，收集的数据也更多。对于需要以更大的灵活性、更低的开销来监视大量数据的企业，该设备是一个不错的选择。

当监视基于 IPv4 的通信量时，该设备将存储数据包，让您在 CA Application Delivery Analysis 中执行增强的数据包捕获调查。通过 Standard Monitor，这些调查将只捕获启动调查后发送的数据包。相比之下，存储在该设备中的捕获文件可让您针对某个性能问题执行诊断分析。

当在 Multi-Port Monitor 和 CA Application Delivery Analysis 管理控制台中监视基于 IPv4 的通信量时，您可以执行下列任务：

- 处理网络吞吐率，其效果相当于多个 Single-Port Monitor。
- 以 1 分钟粒度查看数据，并从多个图表类型中进行选择。
- 在发生突发事件时生成数据包捕获调查文件，且将这些文件最多存储 90 天。
- 对网络、服务器和应用程序执行快速精确的检测。
- 跟踪多个交换机上的 TCP 会话，并从一个 CA Application Delivery Analysis 高度概括汇总报告深入查看多个详细的度量标准。
- 利用多种筛选和排序功能来分析可用数据，并快速隔离有问题的主机。
- 创建并保存分析，从而建立结合了常用筛选和报告选项的故障排除工作流。
- 以 PCAP 格式导出数据包捕获文件，并将其发送给 IT 工程人员以进一步分析。

- 监视 Cisco 广域应用服务 (WAAS) 环境，且无需安装单独的聚合器设备。
- 基于 CA GigaStor 提供的数据包摘要文件计算响应时间度量标准。

此部分包含以下主题：

[数据包捕获调查](#) (p. 6)

[CA Application Delivery Analysis 支持的体系结构](#) (p. 7)

[与 CA Application Delivery Analysis Standard Monitor 的比较](#) (p. 8)

[网络地址转换 \(NAT\)](#) (p. 10)

[CA Application Delivery Analysis 数据概述](#) (p. 11)

[端口要求](#) (p. 12)

## 数据包捕获调查

CA Application Delivery Analysis 可自动运行数据包捕获调查以响应网络或服务器性能突发事件。这些调查将自动记录可进一步分析的数据包级数据，从而增加了性能度量标准分析的粒度。

使用 CA Application Delivery Analysis Standard Monitor 执行数据包捕获调查时，捕获到的数据不总是包括所需的通信量。Multi-Port Monitor 执行的数据包捕获调查要全面得多。通过设备的短期数据包存储功能，可让数据包捕获调查提供发生突发事件时通信量的详细信息。

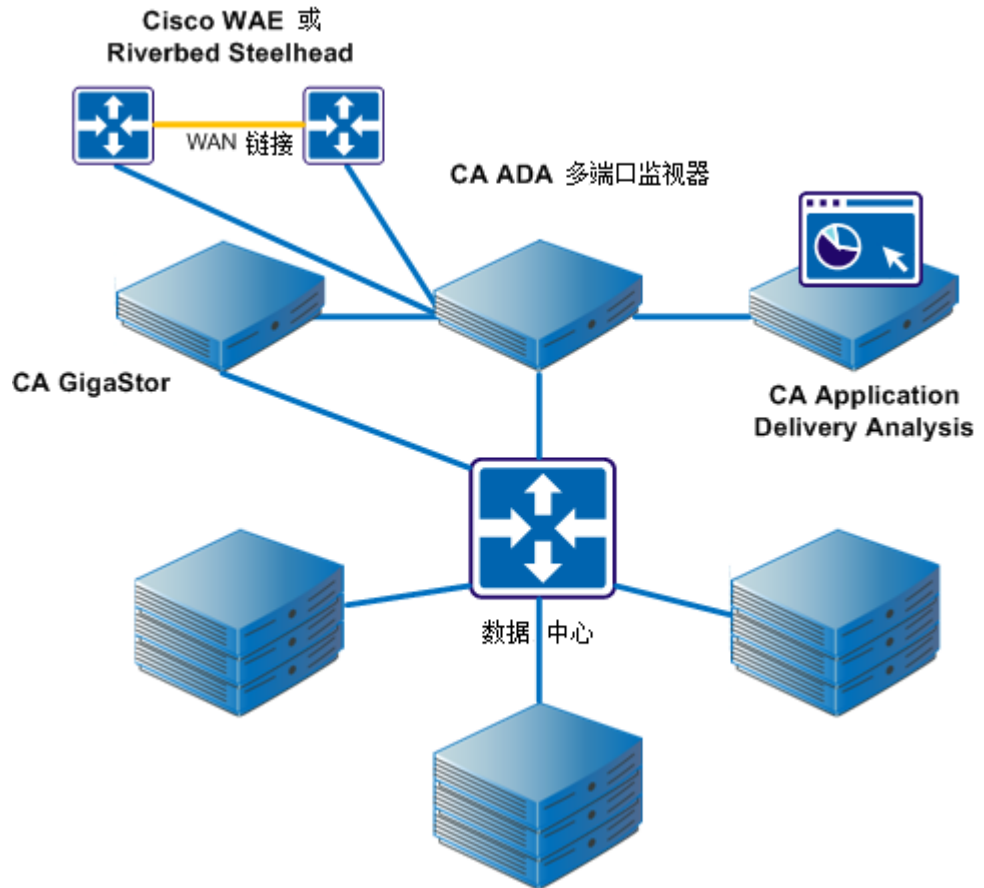
您可以使用捕获和监视的相关选项来检查数据包标头或整个数据包。默认情况下，设备将存储数据包捕获调查文件 90 天。要访问这些文件，请登录 CA Application Delivery Analysis 管理控制台，并导航到“数据包捕获调查”报告。单击“突发事件”选项卡以显示“调查报告”页面的链接。

将 CA GigaStor 作为监视设备分配给 CA Application Delivery Analysis 后，CA GigaStor 将向 CA Application Delivery Analysis 发送数据包摘要以进行聚合。CA Application Delivery Analysis 数据包捕获调查只基于 CA GigaStor 中存储的数据包。

## CA Application Delivery Analysis 支持的体系结构

以下插图描绘了为支持 CA Application Delivery Analysis 而使用的 Multi-Port Monitor 体系结构和配置。Multi-Port Monitor 在典型的 CA Application Delivery Analysis 分布式配置中工作，并与 CA Application Delivery Analysis 管理控制台建立了网络连接。

根据您的配置，一个设备可连接到多达八个独立交换机上的镜像端口。设备会将受监视交换机中的数据发送到管理控制台，而管理控制台会将这些数据包含在所有 CA Application Delivery Analysis 报告中。



## 与 CA Application Delivery Analysis Standard Monitor 的比较

Multi-Port Monitor 设备和 CA Standard Monitor 二者都可以聚合基于 IPv4 的 TCP 度量标准，并将其导出到 CA Application Delivery Analysis。下表汇总了监视基于 IPv4 的 TCP 通信量时，CA Application Delivery Analysis Single-Port Monitor 和 Multi-Port Monitor 之间的最显著差异：

功能	Standard Monitor	Multi-Port Monitor
监视多个镜像的交换机端口		是
对服务器、应用程序和网络进行可用性监视	是	是
提供自我监视和警报	是	是。支持 CA Application Delivery Analysis 非活动监视设备突发事件。SNMP 陷阱提供更多警报。
监视 URL	是	否
支持来自 CA Application Delivery Analysis 管理控制台的调查	是	是。支持增强的数据包捕获调查。
收集所有 CA Application Delivery Analysis 度量标准	是	是
支持自动配置服务器、应用程序和网络	是	是
忽略重复数据包（例如，来自镜像的 VLAN）	是，在提供附加配置后。	是，自动。
以 1 分钟粒度提供性能数据	否	是
筛选并显示指定主机、服务器或应用程序的捕获数据	否	是
从 Cisco WAE 设备接收数据包摘要数据	是	是



功能	Standard Monitor	Multi-Port Monitor
从 CA GigaStor 接收数据包摘要数据	是	是
支持 64 位操作系统上的 CA Application Delivery Analysis	是	是。CA Application Delivery Analysis 必须在 64 位操作系统上运行才能与 Multi-Port Monitor 兼容。

## 网络地址转换 (NAT)

Multi-Port Monitor 需要一些额外配置才能在 Multi-Port Monitor 和 ADA Manager 之间启用了网络地址转换的环境中正常运行。请确保：

1. 使用 `setNatInfo` 命令行实用程序来通过转换的 IP 地址更新 Multi-Port Monitor。
2. 指定将监视设备添加到 CA Application Delivery Analysis 时 Multi-Port Monitor 的转换 IP 地址。

默认情况下，Multi-Port Monitor 和 ADA Manager 使用其管理 IP 地址与彼此通信。

要查看 Multi-Port Monitor 和 ADA Manager 当前用于与彼此通信的 IP 地址，请单击“系统状态”页面。“系统信息”部分显示管理 IP 地址，如果已指定则显示转换的 IP 地址。

使用命令行实用程序 `/opt/NetQoS/scripts/setNATInfo.php` 指定转换的 IP 地址。用法如下所示：

```
/opt/NetQoS/scripts/setNATInfo.php [--console d.d.d.d] [--probe d.d.d.d]
```

其中：

**--console**

是 ADA Manager 的转换 IP 地址。Multi-Port Monitor 通过此地址访问 ADA Manager。

**--probe**

是 Multi-Port Manager 的转换 IP 地址。ADA Manager 通过此地址访问 Multi-Port Monitor。

使用命令行实用程序执行以下任务：

**查看使用声明**

运行不含参数的实用程序：`/opt/NetQoS/scripts/setNATInfo.php`

**指定 ADA Manager 的转换 IP 地址。**

运行含有以下参数的实用程序：`/opt/NetQoS/scripts/setNATInfo.php --console d.d.d.d`

**指定 Multi-Port Manager 的转换 IP 地址。**

运行含有以下参数的实用程序：`/opt/NetQoS/scripts/setNATInfo.php --probe d.d.d.d`

**指定 ADA Manager 和 Multi-Port Monitor 的转换 IP 地址**

运行含有以下参数的实用程序：`/opt/NetQoS/scripts/setNATInfo.php --console d.d.d.d --probe d.d.d.d`

### 重置（清除）数据库中的 NAT 信息

运行含有 NULL 关键字的实用程序：`/opt/NetQoS/scripts/setNATInfo.php --console NULL --probe NULL`

## CA Application Delivery Analysis 数据概述

CA Application Delivery Analysis 产品文档提供的相关信息可以帮助解释报告数据以及诊断源自受监视网络、服务器或应用程序的问题。

无论您排除什么故障，都可以从事务时间（“响应时间”的另一种叫法）这一度量标准入手。一个事务由以下部分组成：

- 一个请求和一个服务器响应
- 一个数据传输期间
- 一条或多条确认
- 观测到的数据包重传引起的延迟

CA Application Delivery Analysis 数据从网络角度标识性能。分析中的相应数据使用 TCP 会话、数据量统计和响应时间的多个视图突出显示活动和性能数据。在调查性能问题时，请考虑事务时间和相关度量标准（如吞吐量）。

**注意：**会话级性能数据仅适用于 Multi-Port Monitor 逻辑端口上接收到的基于 IPv4 的端口镜像数据。会话级数据不能用于来自 CA GigaStor 或 WAE 设备的数据包摘要数据。

过程如下：

- 在 CA Application Delivery Analysis 报告中单击“会话分析”。
- CA Application Delivery Analysis 向 Multi-Port Monitor 传递信息，以识别选定网络、服务器或应用程序的数据的上下文和时间范围。
- 在单独的浏览器窗口中，Multi-Port Monitor Web 界面将会打开并显示“分析”页面。筛选数据，以显示选定上下文的相关性能数据。分析中的图形在外观上不同于 CA Application Delivery Analysis 中显示的图表，原因是 Multi-Port Monitor 数据以 1 分钟增量提供。最小的 CA Application Delivery Analysis 报告间隔为 5 分钟。

由于报告间隔长度不同，因此度量标准的平均值也有所不同。您的配置确定了分析中显示的数据是否出现在管理控制台中。例如，来自未在 CA Application Delivery Analysis 中定义的网络的数据仅出现在分析中。

- 您可以应用更多筛选，选择不同的图表格式，更改时间范围，并保存自定义分析。

## 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"><li>■ 用于 Web 界面访问的 HTTP</li><li>■ Enterprise Manager 与 CA TIM 的通信</li></ul>
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。 <b>注意：</b> 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	<ul style="list-style-type: none"><li>■ CA Application Delivery Analysis Web 服务对数据的请求</li><li>■ 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。</li></ul>
9995	入站	包含来自 CA GigaStor 连接器的数据包摘要的 UDP 数据流。 <b>注意：</b> 仅当 CA GigaStor 是监视器源时才需要。

## 第 2 章： 将 Multi-Port Monitor 配置为监控设备

---

Multi-Port Monitor 设备是 CA Application Delivery Analysis 的监视设备。

在 Multi-Port Monitor 和 ADA Manager 之间启用了网络地址转换 (NAT) 的环境中，请确保：

1. 使用 `setNatInfo` 命令行实用程序来通过转换的 IP 地址更新 Multi-Port Monitor。
2. 指定将监视设备添加到 CA Application Delivery Analysis 时 Multi-Port Monitor 的转换 IP 地址。

**提示：** 将该设备配置为监视设备之前，请执行以下可选步骤。

- 配置硬件筛选，以控制发送给 CA Application Delivery Analysis 的数据。
- 为每个逻辑端口分配有意义的标签，以便更轻松地标识每个数据源。

此部分包含以下主题：

[添加监视设备](#) (p. 13)

[验证逻辑端口的状态](#) (p. 16)

[复查 TCP 会话信息](#) (p. 16) 详细信息：

[网络地址转换 \(NAT\)](#) (p. 10)

### 添加监视设备

添加 Multi-Port Monitor 作为 CA Application Delivery Analysis 的监视设备

在 Multi-Port Monitor 和 ADA Manager 之间启用了网络地址转换 (NAT) 的环境中，请确保：

1. 使用 `setNatInfo` 命令行实用程序来通过转换的 IP 地址更新 Multi-Port Monitor。
2. 指定将监视设备添加到 CA Application Delivery Analysis 时 Multi-Port Monitor 的转换 IP 地址。

默认情况下，Multi-Port Monitor 和 ADA Manager 使用其管理 IP 地址与彼此通信。

**请执行以下步骤：**

1. 在 Web 浏览器中禁用弹出窗口阻止功能。当添加监视设备时，CA Application Delivery Analysis 会使用弹出窗口。
  2. 以具有管理权限的用户身份登录到 CA Application Delivery Analysis 管理控制台。
  3. 依次单击“管理配置”、“数据监视”、“监视设备”。  
将打开“ADA 监视设备列表”。
  4. 单击“添加 ADA 监视器”。  
将打开“Standard Monitor 属性”页面。
  5. 完成以下字段：
    - **服务器名称**。键入设备的服务器名称。如果不知道服务器名称，请在“管理地址”字段中键入一个 IP 地址，然后单击“DNS”。CA Application Delivery Analysis 将尝试解析该 IP 地址。
    - **管理地址**。键入 Multi-Port Monitor 管理 NIC 的 IP 地址。如果不知道 IP 地址，请在“服务器名称”字段中键入 DNS 名称，然后单击“IP”。CA Application Delivery Analysis 将尝试解析该 DNS 名称。
    - **突发事件响应**。为监视设备突发事件选择响应。
    - **可用性监视**。（*可选*）选择“已启用”，让 CA Application Delivery Analysis 每隔 5 分钟监视一次设备的可用性。
    - **是 Multi-Port Monitor**。选择此选项以添加 CA Multi-Port Monitor。当管理控制台无法通过主机名或 IP 地址与监视设备联系时，将显示此选项。
- 注意：**以下字段不适用于 Multi-Port Monitor：
- 启用多个监视器 NIC
  - 监视地址
  - 禁用数据包监视
6. 单击“确定”。  
“ADA 监视设备列表”将刷新，以显示该设备是可用的。

7. (可选) 如果域是在 CA Performance Center 中实施的, 则会为每个监视器源分配正确的域。默认情况下, 会将所有监视器源分配给“默认域”。
  - a. 单击以编辑 CA Multi-Port Monitor 监视设备。
  - b. 在 Multi-Port Monitor 属性中, 监视器源的列表对应于 CA Multi-Port Monitor 上的逻辑端口。管理每个监视器源, 包括:
    - 要在其中进行报告的域:
      - VLAN 标记的通信量。单击“分配 VLAN”, 把特定的 VLAN 通信分配给域, 并且为未分配的 VLAN 通信指定域。
      - 未标记的通信量。单击编辑图标 (✎), 为监视器源上未标记的通信量指定域。

如果您没有使用域来分隔重复的 IP 通信量, 这将不适用。

    - 进行冗余数据监视的监视器源 (例如, 当相同通信量故障转移到不同网络时)。

要与备用监视器源配对, 请单击编辑图标 (✎), 然后单击“备用源”列。可通过仅分配观测到的通信量与该监视器源相同的备用监视器源来避免数据重复。
    - 活动会话信息。

要查看活动会话信息, 请单击“活动会话”。活动会话信息可以帮助您了解监视器源是否正在监视活动 TCP 会话。
8. 单击蓝色齿轮菜单 (⚙), 然后单击“同步监视器设备”。

CA Application Delivery Analysis 将向设备发送监视指令。
9. 配置您要监视的网络、服务器和应用程序。《CA Application Delivery Analysis 管理员指南》中提供了完整说明。
10. 导航到“ADA 监视设备列表”, 并再次同步。
11. 查看“ADA 监视设备列表”, 确认设备能向 CA Application Delivery Analysis 发送数据。

**注意:** 在至少配置了一个有效服务器子网和一个网络后, “上次监视”和“状态”字段将会更新。可能需要等待 10 分钟, 设备才会向 CA Application Delivery Analysis 发送数据。

## 验证逻辑端口的状态


通过 CA Application Delivery Analysis 来验证 Multi-Port Monitor 的逻辑端口状态。逻辑端口是 TCP 响应时间数据的源。您可以查看 CA Application Delivery Analysis 管理控制台中标识为监视器源的逻辑端口的状态。

仅当设备已配置为 CA Application Delivery Analysis 的监视设备时，此过程才有效。

### 遵循这些步骤:

1. 在 CA Application Delivery Analysis 管理控制台中，依次单击“管理配置”、“数据监视”、“监视设备”。

设备的名称将显示在“ADA 监视设备列表”中。

2. 在“选项”列中，单击“编辑”图标 (  )。

将打开“Multi-Port Monitor 属性”页面。“监视器源”表提供了每个逻辑端口的状态信息。

3. 单击“帮助”可获得表中信息的说明。


## 复查 TCP 会话信息

在 CA Application Delivery Analysis 中查看 Multi-Port Monitor 的 TCP 会话信息。对于 Multi-Port Monitor 上的每个逻辑端口，CA Application Delivery Analysis 均会报告基于 IPv4 的活动 TCP 会话数，并附带用于标识流量的服务器名称、地址、VLAN 标识符和端口号。在 CA Application Delivery Analysis 管理控制台中，逻辑端口将标识为监视器源。如果某一监视器源将标记 VLAN 流量拆分为多个域，CA Application Delivery Analysis 则会报告该监视器源中的所有会话。

### 遵循这些步骤:

1. 在 CA Application Delivery Analysis 管理控制台中，依次单击“管理配置”、“数据监视”、“监视设备”。

设备的名称将显示在“ADA 监视设备列表”中。

2. 在“选项”列中，单击“编辑”图标 (  )。

将打开“Multi-Port Monitor 属性”页面。



3. 在第三个“向我显示”列表中单击“活动会话”。  
将打开“活动会话”页面。
4. 选择某一监视器源以查看其会话信息。  
“活动会话”页面提供有关受监视服务器及其相应源的信息。“活动会话”数据有助于验证设备和镜像端口的设置,并有助于解决网络或服务器问题。
5. 单击“帮助”可了解“活动会话”页面上字段的相关信息。



## 第 3 章： 监视设备的突发事件

---

在 CA Application Delivery Analysis 管理控制台中，管理员可以指定当 Multi-Port Monitor 或监视器源变为非活动状态时，是否要创建监视设备突发事件。

当 CA Application Delivery Analysis 停止从 Single-Port Monitor、Multi-Port Monitor 或监视源接收数据时，将会引发“非活动监视器”突发事件。所有监视设备突发事件的严重度均为“过度”。CA Application Delivery Analysis 不会创建“下降”监视设备突发事件。

在响应与以下事件关联的问题时，Multi-Port Monitor 还会发送 SNMP 陷阱：

- “严重”进程状态
- 数据包捕获功能
- 磁盘用量级别
- RAID 阵列和磁盘驱动器失败

当 CA Application Delivery Analysis 停止从某个监视设备接收性能数据时，该设备将被视为非活动。例如：

- 网络故障。未生成数据。
- 监视设备停机。镜像端口上存在数据，但监视设备不活动。
- 分配给监视设备的源是非活动的。例如，某个 WAN 优化设备不可用。
- 镜像端口连接断开。数据已生成，但端口不活动。

即使当某些逻辑端口仍在向 CA Application Delivery Analysis 发送数据，也可能会创建该突发事件。例如，分配给 Multi-Port Monitor 的监视器源停止发送数据包摘要，但其他端口保持活动状态。因此，该突发事件不一定表示 Multi-Port Monitor 处于完全非活动状态。

此部分包含以下主题：

[启用监视设备突发事件](#) (p. 20)

[响应非活动监视设备突发事件](#) (p. 21)

## 启用监视设备突发事件

为每个监视设备分配了默认的“监视设备”突发事件响应。默认响应未与操作关联。您可以在 CA Application Delivery Analysis 中的“Multi-Port Monitor 属性”页面上，为突发事件响应关联一个操作。典型 CA Application Delivery Analysis 工作流程如下：

- 创建“监视设备”突发事件响应。
- 将某个操作（如电子邮件通知）添加到该响应中。
- 在设备属性中选择新的突发事件响应。

“Multi-Port Monitor 属性”页面上的“可用性监视”设置确定了 CA Application Delivery Analysis 是否针对 Multi-Port Monitor 引发“非活动监视设备”突发事件。默认情况下，在所有新监视设备上已启用该设置。要防止 CA Application Delivery Analysis 创建“非活动监视设备”突发事件，请在设备上禁用可用性监视。

CA Application Delivery Analysis 联机帮助包含有关创建突发事件响应的指导。但是，以下过程概述可帮助您入门。

### 遵循这些步骤：

1. 在 CA Application Delivery Analysis 管理控制台中，依次单击“管理配置”、“策略”、“突发事件响应”。
2. 单击“添加监视设备响应”。  
将打开“监视设备突发事件响应属性”页面。
3. 键入新突发事件响应的名称，然后单击“确定”。  
新的突发事件响应将显示在“监视设备突发事件响应”列表中。
4. 单击新响应的对应“编辑”图标。  
将打开“监视设备突发事件响应操作”页面。
5. 单击“添加操作”。  
将打开“监视设备操作类型”页面。
6. 选择“发送电子邮件”或“发送 SNMP 陷阱”，然后单击“下一步”。
7. 完成必填字段，这些字段根据所选操作的不同而异。
8. 单击“确定”。  
“监视设备突发事件响应操作”页面中将显示该操作的说明。

9. 启用突发事件响应：
  - a. 在管理控制台中，依次单击“管理配置”、“数据监视”、“监视设备”。  
将打开“ADA 监视设备列表”。
  - b. 单击 Multi-Port Monitor 的对应“编辑”图标。  
将打开“Multi-Port Monitor 属性”页面。
  - c. 从“突发事件响应”字段中选择新的突发事件响应。
  - d. 单击“确定”。当创建“非活动监视设备”突发事件时，将会执行所选操作。

## 响应非活动监视设备突发事件

如果收到“非活动监视设备”突发事件，请执行以下一项或多项任务：

- 单击 CA Application Delivery Analysis “突发事件”页面上的日期链接以查看详细信息。
- 查看陷阱接收器中收到的警报。对于可能影响数据监视和捕获的问题，Multi-Port Monitor 会发送 SNMP 陷阱。
- 查看 Multi-Port Monitor Web 界面中的“系统状态”页面。该页面可让您评估突发事件的起因：
  - 硬件或软件问题。查看已停止进程的“流程信息”表。
  - 网络问题。查看“捕获卡物理端口状态”表，了解哪些链路未建立连接或出现了故障。
  - 监视器源问题。查看“捕获卡逻辑端口状态”表，了解处于非活动状态的源。该表中不报告非活动 WAN 优化设备或 CA GigaStor。
  - 配置问题。查看“捕获卡逻辑端口状态”表，了解哪些逻辑端口的状态为“已禁用”。验证这些端口是否在“已处理数据包数”列中显示了数据包计数。
  - 数据包捕获问题。查看“捕获卡物理端口统计”表，了解“数据包”或“已接收字节数”列中的异常错误计数和“0”值。
  - RAID 驱动器问题。查看 RAID 表，了解 RAID 状态和发生故障的驱动器。



# 第 4 章：对特殊初始化 (.ini) 文件的支持

---

Multi-Port Monitor 支持的方案需要使用更多参数来指示监视设备以忽略不相关的数据。以下支持的初始化 (.ini) 文件可将这些参数分发到监视设备。

## **DataTransferManager.ini**

设置 sadatransfermanager 进程侦听客户端连接所在的 TCP 端口号。请勿更改此端口号。

## **DTMDistributedConsoles.ini.sav**

控制接收共享数据包摘要数据的 IP 地址。有关详细信息，请参阅 Multi-Port Monitor 设备上的 /opt/NetQoS/bin 目录中的 DTMDistributedConsoles.ini.readme 文件。

## **LimitDTTPParams.ini.sav**

控制“数据传输时间”阈值。

## **LimitServerResponseParams.ini.sav**

控制“服务器响应时间”阈值。

## **RetransPacketDefs.ini.sav**

控制软件是否消除重复。

## **saCollectorOptions.ini**

包含 nqmetricd 服务使用的默认调试跟踪日志记录标志。[CA 技术支持](#) 人员可以告诉您在要提高日志记录级别时需启用哪些标志。

## **saLinuxCollectorDirectives.ini**

定义日志文件的命名格式，以及用于访问本地 MySQL 数据库的参数。请勿更改此信息。

## **saMetricEngine.ini.sav**

控制“活动会话”报告的大小。有关详细信息，请参阅 Multi-Port Monitor 设备上的 /opt/NetQoS/bin 目录中的 saMetricEngine.ini.readme 文件。

《CA Application Delivery Analysis 管理员指南》中介绍了其他初始化文件。

此部分包含以下主题：

[消除重复数据包](#) (p. 24)

[筛选出保持连接消息](#) (p. 25)

## 消除重复数据包

使用多种镜像端口配置可能会导致 Multi-Port Monitor 源上发生数据包重复。本节介绍在典型硬件筛选选项无法满足需要的环境下，将 TCP 通信量镜像到 Multi-Port Monitor 的最佳实践。

SuperAgentErrors.log 文件中丢弃的数据包在此处不是考虑因素。CA Application Delivery Analysis Single-Port Monitor 将会丢弃与 CA Application Delivery Analysis 配置不匹配的数据包。相反，由于 CA Application Delivery Analysis 不分析已丢弃数据包，因此已丢弃数据包可能会造成问题。

当您将 VLAN 镜像到 CA Application Delivery Analysis 监视设备时，CA Application Delivery Analysis 将会接收每个 VLAN 数据包的两个副本。要更正这种数据包重复的情况，您可以将更多的配置参数传递给 Multi-Port Monitor。由于修改此目录中的文件需要超级用户权限，因此请使用“sudo”命令前缀。

### 遵循这些步骤:

1. 导航到 Multi-Port Monitor 设备上的 /opt/NetQoS/bin/ 目录。

```
cd /opt/NetQoS/bin
```

2. 复制 RetransPacketDefs.ini.sav 文件以删除扩展名。

```
sudo cp RetransPacketDefs.ini.sav RetransPacketDefs.ini
```

在监视器下一次同步期间或重新启动 nqmetricd 进程后，将激活 .ini 文件。

3. 将以下代码行添加到 RetransPacketDefs.ini 文件:

```
<nologging>
50 1000
10 20 30 40 50 60
```

第一行指示 CA Application Delivery Analysis 不要记录有关重复数据包的信息。Single-Port Monitor 支持这种类型的日志记录。但 Multi-Port Monitor 不支持。

第二行指示如何应用重传数据筛选。数字 50 和 1000 指示 CA Application Delivery Analysis 维护一个能容纳 50 个数据包的缓冲区，以便查找重复。如果您减小该参数，则 Multi-Port Monitor 在查找重复时使用的 CPU 周期较少。因此，Multi-Port Monitor 的性能将得到改善，但找到的重复的数目也会更少。建议使用这些默认值。

第三行描述了出现重复的直方图区间。Single-Port Monitor 支持使用直方图作为日志记录选项的一部分。但 Multi-Port Monitor 不支持。

4. 从 Multi-Port Monitor Web 界面重新启动 nqmetricd 进程。



## 筛选出保持连接消息

您可以限制应用程序保持连接消息对报告中的监视统计的影响。将“服务器响应时间”(SRT)或“数据传输时间”(DTT)限制为最大值，以忽略不必要的 SRT 或 DTT 观测。可以将该值设置为低于保持连接频率的秒数。

如果您怀疑某个应用程序会发送保持连接消息，请查找观测与 SRT 之间的相反关系。同时，在秒范围（而不是毫秒范围）中查找 SRT 平均值。当您确认该应用程序会发送保持连接消息时，则可以向 SRT 应用阈值。

如果应用程序使用了导致 DTT 偏高的保持连接消息，可以应用类似的限制来筛选 DTT。

如果您不确定所选应用程序的保持连接频率，请使用 10 秒作为起点。一般而言，服务器不太可能在超过 10 秒后才开始响应用户请求。在多数情况下，保持连接频率大于 10 秒。

**注意:**您也可以在 CA Application Delivery Analysis Single-Port Monitor 上应用 SRT 和 DTT 筛选。有关详细信息，请参阅《CA Application Delivery Analysis 管理员指南》。

### 遵循这些步骤:

1. 导航到 Multi-Port Monitor 设备上的 /opt/NetQoS/bin 目录。

```
cd /opt/NetQoS/bin
```

**注意:**要修改 /opt/NetQoS/bin 目录中的文件，需要具有超级用户权限。因此，对于本过程中所述的所有命令，请使用“sudo”前缀。

2. 指定 SRT 阈值。

- a. 复制 LimitServerResponseParams.ini.sav 文件以删除扩展名:

```
sudo cp LimitServerResponseParams.ini.sav LimitServerResponseParams.ini
```

在下一次同步期间或重新启动 nqmetricd 进程后，将激活 .ini 文件。

- b. 验证新文件是否可写:

```
sudo chmod u+w LimitServerResponseParams.ini
```

- c. 编辑 .ini 文件，以更改要筛选的每个端口的 SRT 阈值。

对于每个应用程序，键入端口号以及 SRT 的最大可接受量。将最大 SRT 设置为略小于保持连接频率的值。例如，要忽略以 60 秒频率发生的 Citrix 保持连接消息，请输入以下值:

```
-port=1494 -max seconds=59
```

**注意:**在本示例中，max seconds 是包含空格的单个参数名。

- d. 保存文件。

3. 指定要筛选的每个端口的 DTT 阈值。
  - a. 复制 `LimitDTTParams.ini.sav` 文件以删除扩展名：

```
sudo cp LimitSDTTParams.ini.sav LimitDTTParams.ini
```
  - b. 将新文件配置为可写：

```
sudo chmod u+w LimitDTTParams.ini
```
  - c. 编辑 `.ini` 文件，以更改步骤 2 所述的 DTT 阈值。
  - d. 保存文件。
4. 在 `Multi-Port Monitor Web` 界面中重新启动 `nqmetricd` 进程。

## 第 5 章：在 WAN 优化的环境中进行监视

---

CA Application Delivery Analysis 与 WAN 优化解决方案（如 Cisco 广域应用程序服务 (WAAS)）集成，以监视应用程序的性能。在 WAN 优化环境中，应用程序数据对监视系统不可见。数据看上去像是来自 WAAS 设备，而不是来自实际主机。CA Application Delivery Analysis 与 WAN 优化设备集成，让用户深入了解 WAN 优化如何影响单个应用程序响应时间。

Cisco WAAS 要求在网络中的关键点（如数据中心和分公司）部署多个 Cisco 广域应用引擎 (WAE) 设备。Cisco WAE 设备和 WAN 优化设备可向 CA Application Delivery Analysis 监视设备发送性能数据。通过这些数据，可以深入了解 WAN 优化如何在网络的各个段影响应用程序响应时间。

当 WAN 优化设备通过受监视的镜像端口发送性能数据时，Multi-Port Monitor 将从该设备接收性能数据。可以在配置 Multi-Port Monitor 期间手动激活 WAN 优化支持。《CA Application Delivery Analysis 管理员指南》中介绍了相关过程。

此部分包含以下主题：

[CA Application Delivery Analysis 支持 Cisco WAAS](#) (p. 27)

[Multi-Port Monitor 如何与 WAN 优化设备集成](#) (p. 28)

[CA Application Delivery Analysis 优化报告](#) (p. 28)

[共享来自 WAN 优化设备的数据](#) (p. 29)

### CA Application Delivery Analysis 支持 Cisco WAAS

在 CA Application Delivery Analysis 配置为监视 Cisco WAAS 环境时，WAE 设备将向 CA 数据源导出 FlowAgent 数据。Cisco WAAS 可有效地为网络创建三个不同的 TCP 段。将从每个段收集事务性能数据并为数据建立关联。CA Application Delivery Analysis 通过一个应用程序-服务器-网络优化组合的多个监视点进行监视。因此，CA Application Delivery Analysis 将为每个 TCP 段生成一个独立的度量标准集，并将每个集视为独立的应用程序。

为了让用户完全深入了解 Cisco WAAS 的有效性，CA Application Delivery Analysis 将按段报告应用程序性能，如下所述：

- [客户端] 段：分支位置中的客户端与该分支位置的 WAE 设备之间的网段
- [WAN] 段：分支 WAE 设备与在数据中心运行的 WAE 设备之间的网段
- [服务器] 段：数据中心的 WAE 设备与服务器之间的网段

所有三个段上的应用程序行为类似于三层应用程序上的应用程序行为。源和目标端口与地址在所有层上保持相同。一个新的 CA Application Delivery Analysis 应用程序属性将会监视 WAN 优化的应用程序并标识每个段。

CA Application Delivery Analysis 报告在应用程序名称后面附加一个段标识符。例如，HTTP 应用程序通信量可能标识为三个独立的项：HTTP [客户端]、HTTP [WAN] 和 HTTP [服务器]。附加报告 - CA Application Delivery Analysis “优化” 页面 - 显示了优化事务的数据。默认视图 “优化事务的客户体验” 使用分段数据提供应用程序客户端段的性能图。

## Multi-Port Monitor 如何与 WAN 优化设备集成

sadatransfermanager 进程聚合它从 WAN 优化设备接收的 TCP 标头中的数据。该进程总在运行，即使它未主动传输或聚合数据。您可以将它停止或重新启动。

WAN 优化设备每 5 分钟轮询一次 Multi-Port Monitor 设备，以获取要监视的服务器的列表。优化设备将向本设备发送数据包摘要文件。这些文件包含与 WAN 优化设备上的服务器列表匹配的优化通信量的 TCP 标头。优化设备不发送未优化通信量的 TCP 标头。

本设备将通过它从 WAN 优化设备接收的数据包标头执行以下任务：

- 为 “客户端” 和 “WAN” 段上已优化的通信量计算性能度量标准。
- 将从 WAN 优化设备发送的 “服务器” 段性能数据替换为本设备从镜像端口发送的更精确数据。
- 自动检测端口镜像中的应用程序通信量，并提供更新的服务器列表。CA Application Delivery Analysis 会将此列表传播到所有 WAN 优化设备，以验证是否监视了所有服务器。

sadatransfermanager 进程在端口 7878 上侦听 WAN 优化设备发送的传入数据包标头。

## CA Application Delivery Analysis 优化报告

Multi-Port Monitor 将处理数据包摘要的内容，并向 CA Application Delivery Analysis 发送性能度量标准。这些度量标准显示在管理控制台中的 “优化” 页面上。

“优化” 页面上的默认视图是 “优化事务的客户体验”，它是事务时间和观测的性能图。事务时间（响应时间）最长的应用程序列在最前面。

您无法在“优化”页面上导航到 Multi-Port Monitor 中的“会话分析”。但是，每个应用程序的名称都与该应用程序的“组件”报告相链接。该报告将事务时间细分为以下几个部分：

- 服务器响应时间
- 网络往复传输时间
- 重传延迟
- 数据速率和数据量

“组件”报告页面提供了一些链接，可定向到相关突发事件和可用性的信息。

## 共享来自 WAN 优化设备的数据

一个 CA Application Delivery Analysis 管理控制台通常能够支持您环境中的所有 WAN 优化设备。但是，如果您的 WAN 优化部署要求的监视设备的数目超出了管理控制台可以支持的数目，则您可以分散负载。以下过程描述了如何在多个 Multi-Port Monitor 之间共享 [客户端]、[WAN] 和 [服务器] 段性能数据。

### 遵循这些步骤：

1. 创建一个名为 DTMDistributedConsoles.ini 的配置文件。
2. 打开该 .ini 文件。
3. 键入分配给 Multi-Port Monitor 的管理控制台的 IP 地址。管理控制台将指示 Multi-Port Monitor 如何查找其他监视设备以接收共享数据。

**注意：**提供了一个示例文件。该示例包含无效的 IP 地址，因此无法演示正确的文件格式。可在 /opt/NetQoS/bin 文件夹中找到该示例。

4. 使用点分隔的十进制符号，将每个 IP 地址分隔到一个新行。
5. 将 DTMDistributedConsoles.ini 文件复制到所有监视设备。对于 Multi-Port Monitor，请将该文件复制到 /opt/NetQoS/bin 文件夹。
6. 重新启动 sadatatransfermanager 进程。

最多 25 分钟后，WAN 优化的客户端段数据将在监视设备之间共享。

7. 要与更多监视设备共享数据，请重复步骤 2 至 5。

**注意：**《CA Application Delivery Analysis 管理员指南》中提供了有关共享来自 WAN 优化设备的数据的详细信息。

