管理员指南

CA Application Delivery Analysis

10.1 版

ca technologies

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

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

联系技术支持

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

目录

第 1 章： 欢迎使用 Application Delivery Analysis

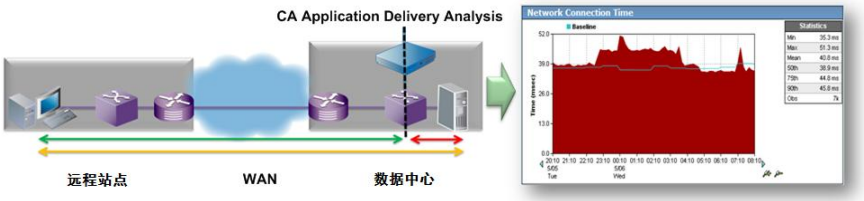
此部分包含以下主题：

了解 Application Delivery Analysis

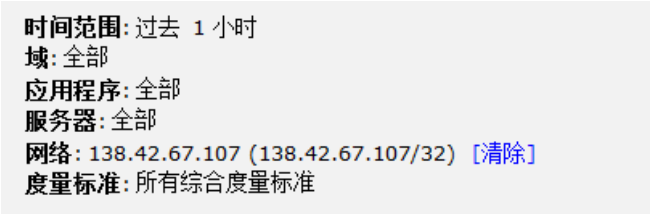
CA Application Delivery Analysis 是 CA Performance Center (CA PC) 和 CA NetQoS Performance Center (CA NPC) 的应用程序性能管理模块。CA Application Delivery Analysis 跟踪和测量最终用户响应时间 -- 无需桌面或服务器代理。CA Application Delivery Analysis 被动地监控遍历客户端和服务器之间的网络的基于 IPv4 的 TCP 数据包，从而提供所有关键应用程序的度量标准，如网络、服务器和应用程序延迟。

TCP 事务流经您的基础架构时，它基本上流过基础架构的三个主要组件 - 网络、服务器和应用程序。在上述任何组件上的性能降低时，它会对最终用户的事务时间造成不利影响。

CA Application Delivery Analysis 从服务器交换机测量每个 TCP 客户端和服务器上的应用程序端口之间的 TCP 事务时间。如下例所示，服务器交换机和客户端之间的响应时间是网络响应时间（由绿色箭头表示），服务器交换机和服务器之间的响应时间是服务器响应时间（由红色箭头表示）。网路和服务器的组合响应时间（由黄色箭头表示）反映最终用户的应用程序体验。



CA Application Delivery Analysis 报告时间范围、应用程序端口、服务器、网络和性能度量标准的唯一组合。例如，您可以报告过去 24 小时与 Development I 客户端网络通信的所有应用程序和服务器的平均网络连接时间。



CA Application Delivery Analysis 用于性能管理时，在 CA PC 或 CA NPC 上可以注册为数据源。CA Application Delivery Analysis 不用于性能管理时，应将其注册到 CA NPC。CA PC 或 CA NPC 安全功能 -- 包括用户、角色、产品权限和组 -- 允许您控制哪些用户可以在管理控制台中查看特定数据。

Application Delivery Analysis 的体系结构概述

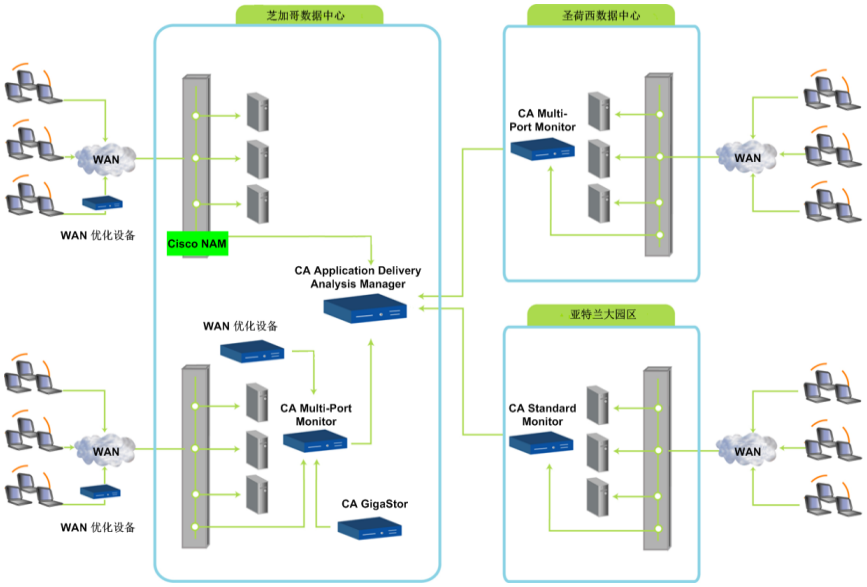
CA Application Delivery Analysis 包括 CA Application Delivery Analysis Manager 和一个或多个监视设备。CA Application Delivery Analysis Manager 是运行数据库引擎和报告控制台的设备。监视设备是监视 TCP 事务的设备。CA Application Delivery Analysis Manager 整合来自一个或多个监视设备的响应时间数据。

CA Application Delivery Analysis 提供多个监视选件：

- CA Multi-Port Monitor 是用于 SPAN 或 TAP 数据的最具伸缩性、功能最丰富的选件。它有 1 千兆位和 10 千兆位两种选择。
- CA Standard Monitor 可处理高达 1 千兆位的 SPAN 或 TAP 数据。
- CA Virtual Systems Monitor 监视同一“VMware ESX 主机”上虚拟服务器之间的传入/传出通信量。
- Cisco Network Analysis Module (NAM)。Cisco NAM 是 CA Application Delivery Analysis 的监视设备，使您可以进行深层次的故障排除。

CA Standard Monitor 或 CA Multi-Port Monitor 还处理来自以下设备的数据包摘要：

- WAN 优化设备，包括 Cisco WAAS 和 Riverbed Steelhead。
- CA GigaStor 连接器。CA GigaStor 是一个长期数据包获取设备，它将性能数据发送到 CA Application Delivery Analysis，并同时启用回顾性网络分析，以便往回追溯来进行数据包分析或重放会话数据。



在所有服务器通信量都可以从单个交换机端口镜像的环境中，可以使用单机 CA Application Delivery Analysis Manager，让 CA Application Delivery Analysis Manager 在其“监视器 NIC”上接收镜像的 TCP 包。

使用 Application Delivery Analysis 监控

CA Application Delivery Analysis 通过自动执行以下操作来监控端到端性能：

- 基于默认服务器子网和客户端网络以及您指定的服务器子网和客户端网络收集和计算应用程序的基于 IPv4 的 TCP 事务时间。
- 按指定的服务器分配，监视用户定义的应用程序。
- 生成应用程序性能基准，以了解什么情况属于正常。
- 设置可接受性能的阈值上限
- 超过阈值时创建突发事件。
- 显示 IPv4 事务的所有性能度量标准的 5 分钟摘要。

默认情况下，CA Application Delivery Analysis 被动监视端到端响应时间。您可以使用该产品更加主动，例如，通过启用用于响应网络突发事件的网络跟踪路由调查，或设置应用程序可用性的运行水平协议 (OLA)。

详细信息：

如何设置和维护 CA Application Delivery Analysis (p. 25)

Application Delivery Analysis 中的管理员角色

CA Application Delivery Analysis 管理员负责以下内容：

- 设置监视设备。
- 与网络管理员一起将监视设备放置在网络上的适当位置，并将适当的 TCP 通信镜像到每个监视设备。
- 指定要监视的服务器子网、应用程序和客户端网络定义。
- 管理管理控制台基于观测到的所有服务器通信量自动创建的应用程序，例如，分配突发事件响应，创建应用程序并分配特定服务器。
- 指定性能和可用性的服务水平。
- 管理安全性，例如，让用户登录管理控制台并管理特定的应用程序组、服务器组和客户端网络组。请注意，在 CA PC 或 CA NPC 上注册为数据源时，可以在 CA PC 或 CA NPC 管理控制台的“管理”选项卡中执行这些任务。

如何访问管理控制台

CA Application Delivery Analysis Manager 在企业网络中安装并且可用后，请打开 Web 浏览器，并键入托管 CA Application Delivery Analysis Manager 的服务器的 IP 地址。如果 DNS 配置为解析主机名，请输入服务器的主机名。

注意：有关安装和配置 CA Application Delivery Analysis 的信息，请参阅*《安装指南》*。

可提供相应的 URL 来访问 管理控制台 Web 接口：

如果 CA PC	指定此 URL
安装在管理控制台服务器上	http://*hostname/sa*
未安装在管理控制台服务器上	http://*hostname*

管理控制台 的设计适合在 Microsoft Internet Explorer 版本 8 或 9 以及 Mozilla Firefox 中显示，并且需要使用 Adobe Flash Player。不支持 Internet Explorer 版本 6 和 7。如果您在初次尝试访问 Web 接口时看到 Internet Explorer 增强的安全性发出的有关被阻止网站的安全提示，建议您调整浏览器设置。

如果您没有 CA Application Delivery Analysis 管理员帐户，请联系您的 CA PC 或 CA NPC 管理员。如果您是首次登录，可使用预定义的管理员帐户 admin 以及默认密码 admin。

在“登录”页面上，键入您的用户名和密码。请记住，登录凭据区分大小写。一旦您成功通过身份验证，将自动重定向到管理控制台。如果登录不正确，您将返回“登录”页面。

为了提高安全性，建议更改预定义用户帐户的默认密码。管理员可以通过登录并编辑用户帐户来执行此操作。

详细信息：

管理用户帐户权限 (p. 193)
推荐的浏览器设置 (p. 19)

推荐的浏览器设置

建议更新您的 Web 浏览器配置以禁用弹出窗口阻止功能，并且仅在 Internet Explorer 上将管理控制台添加到受信任 Internet 站点列表中。

通过 Internet Explorer 8 访问管理控制台时，页面顶端格式可能出现问题。

要避免这种情况，请在 Internet Explorer 中按 F12 ，然后设置“浏览模式”为 IE8，“文档模式” 为 Quirks。

禁用弹出窗口阻止程序

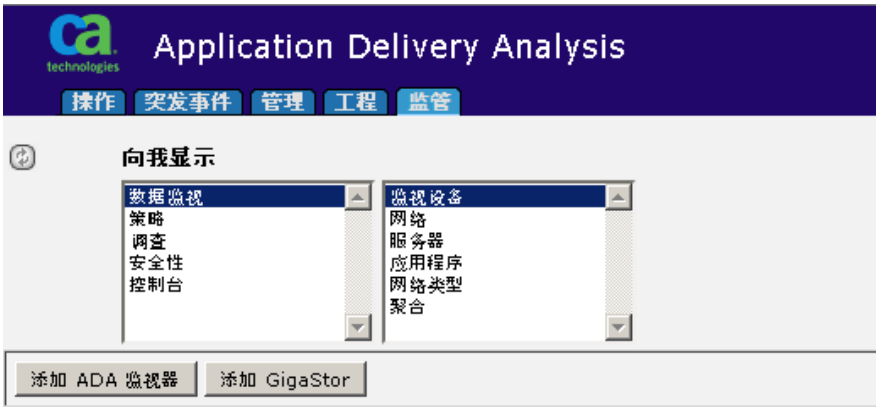
手动启动调查时，请在 Web 浏览器中禁用弹出窗口阻止程序，否则将阻止调查运行。您启动了一个调查，如果未看到显示调查运行状态的弹出消息，则很可能是弹出窗口阻止程序仍在运行，而您的调查并未运行。

更新受信任的 Internet 站点

建议在 Internet Explorer 浏览器实例中将 管理控制台 服务器的主机名添加到受信任 Internet 站点列表中，以改善用户界面性能。默认情况下，Internet Explorer 使用高安全性设置，从而限制您只能导航到受信任的站点，或在您导航到不在受信任站点列表中的站点时重复显示警告消息。此建议仅适用于 Internet Explorer。

如何导航“管理配置”页面

具有管理员权限的 CA Application Delivery Analysis 用户可以访问“管理配置”页面。



在“管理配置”页面上的“向我显示”菜单中，单击各菜单项以便管理 CA Application Delivery Analysis：

- 数据监视 - 指定从环境中的应用程序、服务器和网络收集应用程序响应时间数据的监视设备。
- 策略 - 指定应用程序、服务器和网络性能的阈值、对性能下降的响应以及性能和可用性的运行水平协议 (OLA)。
- 调查 - 指定用于轮询服务器或网络设备的 SNMP 配置文件。
- 安全性 - 指定用户权限。在 CA PC 或 CA NPC 上注册为数据源时，可以从 CA PC 或 CA NPC 管理用户权限。
- 控制台 - 管理 CA Application Delivery Analysis Manager 数据库、报告和监视设备突发事件。

监视的 TCP 会话

要使 管理控制台 能够跟踪和度量最终用户响应时间，监视设备必须观测客户端与服务器上的应用程序端口之间的基于 IPv4 的事务。使用您指定的服务器子网和客户端网络，管理控制台会自动为匹配的 TCP 事务计算性能度量标准。

通常，CA 技术代表可帮助您指定要监视的客户端网络、服务器和应用程序。

如果管理的 ISP 具有重叠的服务器或客户端 IP 地址，您将需要使用域来分隔 TCP 通信量。

CA ADA 包括“捕获所有”默认客户端网络的以下默认条目：

- 所有其他：0.0.0.0/0
- 所有其他 10 网络：10.0.0.0/8
- 所有其他 172.16 网络：172.16.0.0/12
- 所有其他 192.168 网络：192.168.0.0/16

详细信息：

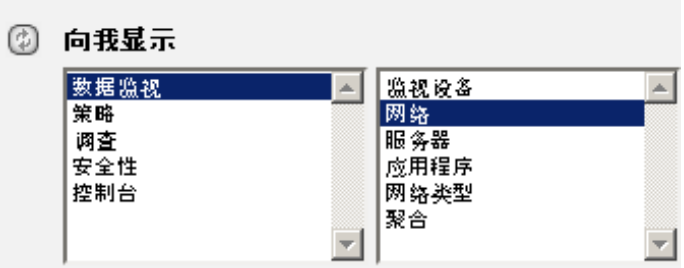
管理承租人 (p. 87)

查看客户端网络的列表

使用“网络列表”可以管理管理控制台监视的客户端网络的列表。每个监视设备会计算应用程序服务器与“网络列表”中指定的客户端网络之间的响应时间度量标准。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“网络”。



将显示“网络列表”。在以下示例中，定义了 2 个具有 /24 子网掩码的 IPv4 客户端网络。


网络 列表

定义如何将整个网络分成更细化的网络，以便分别用于每个子网的跟踪统计。

通过检查感兴趣的网络，并单击反色标题中的选项，同时修改多个网络。

网络	子网	地区	网络类型
(Test)Server	138.42.67.18/32	1	未分配
10.0.11.21	10.0.11.21/32	1	未分配
10.0.11.24	10.0.11.24/32	1	未分配
10.0.11.30	10.0.11.30/32	1	未分配
10.0.12.102	10.0.12.102/32	1	未分配
10.0.12.103	10.0.12.103/32	1	未分配
10.0.12.140	10.0.12.140/32	1	未分配
10.0.12.248	10.0.12.248/32	1	未分配
10.0.13.129	10.0.13.129/32	1	未分配
10.0.13.137	10.0.13.137/32	1	未分配

1 / 15

CA Application Delivery Analysis 包括“捕获所有”默认客户端网络的以下默认条目：

- 所有其他 0.0.0.0/0
- 所有其他 10 网络 10.0.0.0/8
- 所有其他 172.16 网络 172.16.0.0/12
- 所有其他 192.168 网络 192.168.0.0/16

详细信息：

管理客户端网络 (p. 27)

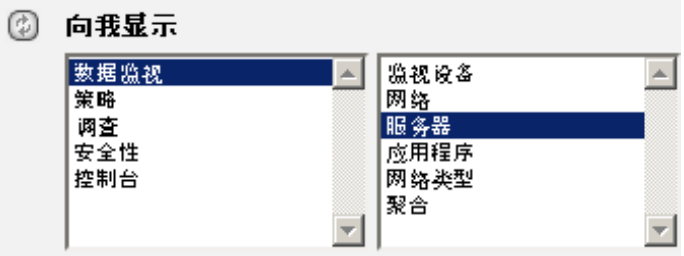
查看服务器列表

使用“服务器列表”可以查看和管理管理控制台监视的服务器的列表。

如果某服务器未显示在该列表中，请浏览“服务器子网列表”，以验证匹配的服务器子网是否存在。管理控制台在服务器上观测到匹配的应用程序端口通信量之后，会自动将该服务器添加到“服务器列表”中。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“服务器”。



将显示“服务器列表”。在以下示例中，“服务器列表”中的 IPv4 地址列表对应于“服务器子网列表”中的 IPv4 服务器子网。

注意：Application Delivery Analysis 包括称作“*Monitor All Servers* on subnet 0.0.0.0 mask 0”的默认服务器子网。添加新的监视器时，默认服务器子网使数据收集能够自动发生。

详细信息：

管理服务器 (p. 61)

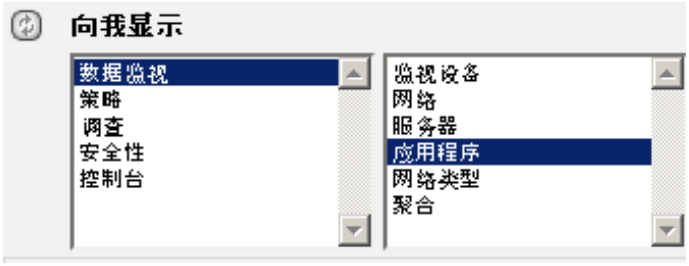
查看应用程序列表

使用“应用程序列表”可以管理管理控制台监视的应用程序。CA Application Delivery Analysis 会自动监视指定的服务器子网和客户端网络之间的所有应用程序通信量。

如果某应用程序未显示在该列表中，请确保已配置管理控制台来监视该应用程序。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。



将显示“应用程序列表”。在以下示例中，会自动对已知端口中的应用程序通信命名。

详细信息：

管理应用程序 (p. 93)

如何设置和维护 CA Application Delivery Analysis

现在您已熟悉 CA Application Delivery Analysis 的工作原理，因此您已准备好执行通常的管理员任务。

任务	详细信息
■ 添加或删除监视设备 ■ 管理监视设备性能 ■ 查看监视设备活动	监视设备管理 (p. 221)
■ 指定要监视的客户端网络 ■ 使用网络类型对网络分组	管理客户端网络 (p. 27)
■ 指定要监视的服务器 ■ 指定服务器维护的排定期间	管理服务器 (p. 61)
■ 指定要监视的应用程序	管理应用程序 (p. 93)
■ 将默认性能阈值添加到各组网络 ■ 针对跨某组网络的用户定义的应用程序自定义性能阈值 ■ 调整性能阈值以提高或降低 CA Application Delivery Analysis 对应用程序、服务器和网络响应时间更改的敏感度	管理性能阈值 (p. 125)
■ 使 CA Application Delivery Analysis 可以自动通知您并调查服务器或网络突发事件	管理突发事件响应 (p. 151)
■ 指定应用程序性能的运行水平	管理应用程序性能 OLA (p. 175)
■ 监视应用程序可用性并指定可用性的运行水平	管理应用程序可用性 (p. 185)
■ 添加或删除用户 ■ 管理用户权限	管理用户帐户权限 (p. 193)
■ 排定并执行每周数据库备份 ■ 指定系统首选项 ■ 管理 SNMP 配置文件	管理控制台 (p. 201)
■ 执行系统维护	执行系统维护 (p. 216)

第 2 章： 管理客户端网络

此部分包含以下主题：

客户端网络的工作方式

*客户端网络*指定要监视的客户端 IPv4 地址范围，它对应于环境中的物理位置或用户组。

建议根据客户端通信的来源（如远程站点、数据中心）创建客户端网络，或为对外的应用程序 (Internet) 创建客户端网络。例如，如果您在奥斯汀有一个客户端网络定义为 192.168.0.0/22，则可使用管理控制台创建一个具有相同网络地址和子网掩码的“奥斯汀”客户端网络。

为了使管理控制台用户能够快速分析和响应客户端网络中的性能问题，可以根据环境中的实际客户端网络创建对应的客户端网络。

将服务器添加到服务器列表时，管理控制台自动创建相应的 /32 客户端网络以监控多层应用程序中服务器之间的通信量。

正确指定相关客户端网络可优化可用的系统资源。

Application Delivery Analysis 包括“捕获所有”默认客户端网络的以下默认条目：

- 所有其他 0.0.0.0/0
- 所有其他 10 网络 10.0.0.0/8
- 所有其他 172.16 网络 172.16.0.0/12
- 所有其他 192.168 网络 192.168.0.0/16

注意：客户端网络重叠时，管理控制台报告更具体的客户端网络中的应用程序通信量。

详细信息：

网络列表的工作方式

使用“网络列表”可以查看和管理管理控制台监视的网络。“网络列表”包括您指定的客户端网络，以及 /32 客户端网络。

*/32 客户端网络*是具有单个 IPv4 地址的客户端网络。CA Application Delivery Analysis 使用 /32 客户端网络监控多层应用程序。在将服务器添加到“服务器列表”时，管理控制台会自动创建相应的 /32 客户端网络。

注意：要删除 /32 客户端网络，请从“服务器列表”中删除相应的服务器。不能删除管理控制台创建的 /32 客户端网络。

详细信息：

管理多层应用程序 (p. 119)

基于网络的报告的工作方式

为了监视整个网络的应用程序性能，管理控制台将报告整个客户端网络的平均应用程序响应时间，而不报告单个 TCP 会话的响应时间。在网络级别报告使管理控制台能够将性能问题隔离到特定网络。

监控至少使用 24 位子网掩码（24 位到 32 位）定义的客户端网络时，管理控制台会报告在指定时间间隔内与应用程序通信的实际客户端 IP 地址。例如，191.168.1.0/24 网络的报告会显示访问该应用程序的实际客户端 IP 地址。

由于管理控制台对整个网络的应用程序响应时间求平均值，因此该信息无法帮助您隔离哪些客户端计算机受到性能问题的影响。而该信息只显示了指定时段内与应用程序通信的客户端列表。将性能问题隔离到特定网络并不需要此级别的详细信息。

如果您创建子网掩码小于 24 位的客户端网络，管理控制台 将报告与应用程序通信的 C 类网络。例如，如果您创建子网掩码为 22 位的客户端网络（如 192.168.0.0/22），则管理控制台将报告 C 类客户端网络（191.168.0.0/24 至 191.168.3.0/24，而不是访问应用程序的实际客户端 IP）的度量标准。

注意：如果您对会话级报告感兴趣，请将 CA Multi-Port Monitor 用作监视设备。CA Standard Monitor 按 5 分钟粒度分析网络级别的 TCP 会话，与此不同，CA Multi-Port Monitor 按 1 分钟粒度分析服务器和特定客户端之间的 TCP 会话。此外，CA Multi-Port Monitor 允许您分析所有观测的网络通信（包括 TCP 和非 TCP 通信）的通信量。

网络区域的工作方式

为了使管理控制台用户能够快速分析和响应远程站点中的性能问题，可以根据环境中的实际客户端网络创建对应的客户端网络。

但是，如果还希望管理控制台能够报告与应用程序通信的基于 IPv4 的实际客户端 IP，则客户端网络必须至少有 24 位子网掩码。

如有必要，可将大型客户端网络转换为较小的网络区域，以使管理控制台能够按区域报告观测到的 TCP 通信量。*网络区域*是客户端网络的较小子网。例如，如果您具有 /22 客户端网络，可将其转换为四个 /24 网络区域。

如果网络定义为以下类型	创建如下数量的区域
/24	1
/23	2
/22	4
/21	8
/20	16
/19	32
/18	64
/17	128
/16	256

将客户端网络转换为区域后，管理控制台将按区域而非定义的客户端网络来报告观测到的 TCP 通信量。继续前一个示例，把 /22 客户端网络转换为 /24 网络区域后，/22 客户端网络将仅在“管理配置”页面中可见，而不会用于报告用途。在报告中，您将需要查找单个网络区域。

为了使管理控制台用户能够报告已定义客户端网络中的应用程序性能，而不是特定 /24 网络区域中观测的通信量，请使用 CA PC 或 CA NPC 创建一个由所有网络区域构成的组。

为了方便识别与客户端网络对应的网络区域，请遵循熟悉的命名约定。在以下示例中，“奥斯汀”组包括从 192.168.0.0/22 客户端网络转换的 /24 网络区域。

报告一组网络区域时，“工程”页面上的性能详细信息报告（如“响应时间组成: 平均”报告）会聚合所有 /24 网络区域的数据。但是，所有其他报告（如“操作”页面报告和“工程”页面性能图）会分别列出每个 /24 网络区域。有关报告一组网络的信息，请参阅*《用户指南》*。

下表显示具有网络区域的一些示例网络配置。

网络配置	**/24 网络区域**
名称：ABC 子网：10.10.1.0 掩码：24 区域：1 网络类型：128K	10.10.1.0
名称：DEF 子网：10.10.0.0 掩码：22 区域：4 网络类型：128K	10.10.0.0 10.10.1.0 10.10.2.0 10.10.3.0

网络配置	/24 网络区域
名称：XYZ 子网：10.10.0.0 掩码：16 区域：256 网络类型：128K	10.10.0.0 10.10.1.0 。 。 。 10.10.255.0

详细信息：

命名约定 (p. 32)

命名约定

下面是建议用于客户端网络的一些命名约定。切记，如果您已经使用区域定义客户端网络，您将不能报告客户端网络。因此，从报告的角度，客户端网络区域名称非常重要：

对于	使用	示例
客户端网络	*位置-说明*	Singapore-Backbone
客户端网络区域	*位置-区域-带宽*	奥斯汀-Subnet10-128K

查找客户端网络

搜索“网络列表”，以查找管理控制台当前监视的客户端网络。也可以使用“工程”页面上的“QoS 用户”报告，例如，在“捕获所有”默认客户端网络上查找与应用程序通信的客户端 IP。

详细信息：

默认客户端网络 (p. 35)

搜索“网络列表”

搜索“网络列表”，查找已定义的客户端网络。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“网络”。
3. （可选）选择要搜索的域。
4. 单击“网络列表”中的蓝色齿轮菜单 ( ) 并选择“查找网络”。
5. 在“网络列表”中单击“搜索”，以按“网络名称”或“子网”进行搜索。
6. 在“搜索对象”字段中，指定搜索字符串。可在搜索模式的开头或结尾指定一个模式匹配字符，包括：

   *****

   匹配所有字符。

   %

   匹配一个字符。
7. 单击“搜索”以查找匹配的网络。

   注意：单击超链接以编辑客户端网络的属性。

详细信息：

管理承租人 (p. 87)
编辑客户端网络 (p. 42)

查找具有 QoS 用户报告的未知客户端网络

随着时间的推移，扩展地址范围是很常见的事情。创建“捕获所有”网络可确保一旦进行扩展，CA Application Delivery Analysis 便对其进行计算。如果看到广泛的超集网络中显示客户端 IP 通信，则可使用“QoS 用户”报告查看显示通信的 /24 客户端网络，然后显式定义这些子集网络。

遵循这些步骤:

1. 单击“工程”页面。
2. 单击“QoS 用户”报告的蓝色齿轮菜单 ( ) 并单击“列出用户”，以将客户端网络中观测的通信筛选到更具体的更小 8 位子网中。例如，在 /16 网络（如 192.168.0.0/16“捕获所有”网络）中报告时，“用户”列表会显示相应的管理控制台已观测到客户端 IP 通信的 /24 网络。在以下示例中，预计 /24 网络在 30-39 范围内，但是管理控制台在 192.168.112.0/24 客户端网络中看到意外的客户端 IP。

   要查看 192.168.112.0/24 客户端网络中的实际客户端 IP，请创建一个 192.168.112.0/24 客户端网络并使用“QoS 用户”报告列出 /32 用户的 IP 地址。

CA Application Delivery Analysis 包括“捕获所有”默认客户端网络的以下默认条目：

- 所有其他 0.0.0.0/0
- 所有其他 10 网络 10.0.0.0/8
- 所有其他 172.16 网络 172.16.0.0/12
- 所有其他 192.168 网络 192.168.0.0/16

详细信息：

默认客户端网络 (p. 35)

管理客户端网络

通过指定要监控应用程序端口通信量的网络来管理客户端网络。

- 从 CSV 文件导入网络信息以加速配置。
- 添加客户端网络。
- 通过轮询路由器导入网络信息。

在将客户端网络添加到管理控制台中时，可计划按照用于报告用途和用于在网络中启动突发事件响应的网络类型对客户端网络分组。

详细信息：

按网络类型对客户端网络分组 (p. 45)

默认客户端网络

随着时间的推移，扩展地址范围是很常见的事情。“捕获所有”网络可确保一旦进行扩展，CA Application Delivery Analysis 便对其进行计算。如果客户端 IP 通信出现在一个大的默认客户端网络中，则请使用“QoS 用户”报告查看显示通信的 /24 客户端网络，然后显式定义这些子集网络。

CA Application Delivery Analysis 包括“捕获所有”默认客户端网络的以下默认条目：

- 所有其他 0.0.0.0/0
- 所有其他 10 网络 10.0.0.0/8
- 所有其他 172.16 网络 172.16.0.0/12
- 所有其他 192.168 网络 192.168.0.0/16

注意：客户端网络重叠时，管理控制台报告更具体的客户端网络中的应用程序通信。

在 DMZ 中面对 Internet 的应用程序可以使用子网 0.0.0.0 /掩码 0 的“所有其他”客户端网络进行监控，以监控您未显式定义的客户端网络的应用程序活动。不要使用此客户端网络来监视其他类型的应用程序。否则，“操作”和“工程”页面将显示许多超出阈值的异常客户端 IP 地址，原因它们没有正常的基准。

注意：“所有其他”客户端网络不允许您查看 TCP 会话，但允许管理控制台报告其他客户端网络的应用程序活动。

详细信息：

基于网络的报告的工作方式 (p. 29)
查找客户端网络 (p. 32)

从 CSV 文件导入客户端网络

从 CSV 文件导入 IPv4 客户端网络，以轻松地指定您想要的客户端网络。

首先，导出 IPv4 客户端网络的列表（例如，从 DHCP 管理工具），然后编辑该列表以描述 /24 客户端网络。

为了避免在导入后编辑客户端网络，建议您在 CSV 文件中为每个网络定义所有网络属性。请注意，在导入网络后，必须从管理控制台中编辑网络，并且无法通过重新导入现有网络来更新其属性。

在创建 CSV 文件时，不要忽略网络类型。网络类型在监视应用程序性能时发挥着重要作用。

注意：如果已在 CA PC 或 CA NPC 中定义域，则必须将客户端网络的列表导入相同的域中。支持的 CSV 文件语法不允许您为每个网络定义指定域。

详细信息：

编辑客户端网络 (p. 42)
按网络类型对客户端网络分组 (p. 45)

创建 CSV 文件

执行以下步骤来创建用于指定要监视的 IPv4 客户端网络的 CSV 文件。

创建 CSV 文件时：

- 用逗号分隔每个字段，并确保逗号后没有空格。
- 将嵌入的逗号或双引号括在双引号中。
- 将包含一个或多个空格的字符串括在双引号中；例如："Houston Office"。

遵循这些步骤:

1. 创建一个具有 .csv 文件扩展名的文件。
2. 在单独行中添加每个网络定义。
3. 对于每个网络定义，采用以下格式：

   网络名称,子网,掩码,区域,网络类型

   请注意，在以下示例中，“休斯顿办公室”条目未指定网络类型，因此它在管理控制台中默认为“未分配”：

   ```
   "亚特兰大实验室",192.168.100.0,24,1,LAN
   "休斯顿办公室",192.168.200.0,24,1
   ```

   network_name

   定义实际客户端网络的名称，最多包含 50 个字符。建议遵循命名约定，如*位置-说明*。

   如果您计划使用网络区域将网络子网转换为 /24 子网，则建议遵循命名约定，如*位置-区域-带宽*。

   子网

   以四部分、点分十进制表示法定义网络的 IPv4 地址，例如 192.168.100.0。

   mask

   为实际客户端网络指定子网掩码。

   请注意，管理控制台会自动为每个服务器创建一个 /32 网络，以监视即充当处理客户端请求的服务器又充当其他服务器的客户端的服务器。

   区域

   （可选）指定可以从范围更大的网络子网转换的 /24 子网的数目。例如，如果网络子网是 /22，则 4 个区域会将 /22 转换为四个 /24 子网。

   网络类型

（可选）指定您要分配给网络的网络类型及其网络区域（如果适用）。如果未指定网络类型，将设置为“未分配”。

4. 保存文件，然后将其导入管理控制台。

详细信息：

管理多层应用程序 (p. 119)
网络区域的工作方式 (p. 30)
按网络类型对客户端网络分组 (p. 45)

导入 CSV 文件

在创建 CSV 文件之后，将 IPv4 客户端网络定义导入管理控制台。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“网络”。
3. （可选）选择要将客户端网络导入的域。

   将打开“网络列表”。
4. 单击蓝色齿轮菜单 ( ) 并选择“从文件导入”。

   将打开“导入网络定义”。
5. 单击“浏览”选择 CSV 文件。
6. 单击“下一步”。

   将打开“网络属性”。
7. 解决您从 CSV 文件导入的定义与管理控制台中现有网络定义之间的任何重叠。任何重叠都将突出显示：

   红色

   表示该子网定义匹配已定义的一个子网定义。单击红色 X ( ) 以删除网络或修改其子网定义。

   您无法多次添加同一子网定义。例如，如果已定义了一个具有 256 个客户端区域的 11.2.0.0/16 网络，则您无法导入 11.2.3.0/24 客户端网络。

   黄色

   表示该子网定义与现有的一个更广的子网定义重叠。如果您不再需要那个更广的子网定义，请在完成导入之后将其删除。

   管理控制台虽然会导入相互重叠的网络定义，但始终针对更具体的网络报告客户端的活动。例如，如果您导入了一个 /26 网络，而该网络与 /24 网络重叠，则管理控制台将针对 /26 网络报告匹配的客户端通信量。

   绿色

   表示该子网定义与现有的一个更窄的子网定义重叠。如果您不再需要那个更窄的子网定义，请在完成导入之后将其删除。

   管理控制台虽然会导入相互重叠的网络定义，但始终针对更具体的网络报告客户端的活动。例如，如果您导入了一个 /26 网络，而该网络与 /24 网络重叠，则管理控制台将针对 /26 网络报告匹配的客户端通信量。
8. 单击“确定”。

9. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)

添加客户端网络

添加客户端网络，以使管理控制台能够监视整个客户端网络中所有应用程序服务器的性能。不将该客户端网络分配给特定应用程序服务器。

要快速、轻松地导入所有客户端网络，请从 CSV 文件导入网络定义。

要手动添加客户端网络，

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“网络”。
3. （可选）选择要在其中创建客户端网络的域。
4. 在“向我显示”菜单下，单击以添加 IPv4 客户端网络。
5. 填写“网络属性”中的字段，然后单击“确定”。

   有关网络属性的信息，请单击“帮助”。
6. 解决您从 CSV 文件导入的定义与管理控制台中现有网络定义之间的任何重叠。任何重叠都将突出显示：

   红色

   表示该子网定义与已定义的一个子网定义匹配。单击红色 X ( ) 来删除网络或修改其子网定义。

   您无法替换现有子网定义。例如，如果已定义了一个具有 256 个客户端区域的 11.2.0.0/16 网络，则您无法导入 11.2.3.0/24 客户端网络。

   黄色

   表示该子网定义与现有的一个更广的子网定义重叠。如果您不再需要那个更广的子网定义，请在完成导入之后将其删除。

   管理控制台虽然会导入相互重叠的网络定义，但始终针对更具体的网络报告客户端活动。例如，如果您导入了一个 /26 网络，而该网络与 /24 网络重叠，则管理控制台将针对 /26 网络报告匹配的客户端通信量。

   绿色

   表示该子网定义与现有的一个更窄的子网定义重叠。如果您不再需要那个更窄的子网定义，请在完成导入之后将其删除。

   管理控制台虽然会导入相互重叠的网络定义，但始终针对更具体的网络报告客户端的活动。例如，如果您导入了一个 /26 网络，而该网络与 /24 网络重叠，则管理控制台将针对 /26 网络报告匹配的客户端通信量。

7. 单击“确定”。
8. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
从 CSV 文件导入客户端网络 (p. 36)

编辑客户端网络

使用“网络列表”可编辑客户端网络或其区域之一。在管理控制台观测到网络中的通信后，不得更改 IP 地址或子网掩码。

请注意，不得更改将网络分配到的域。如有必要，可删除客户端网络，然后使用正确的域重新创建客户端网络。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“网络”。

   将显示“网络列表”。
3. （可选）选择要编辑的客户端网络所在的域。
4. 单击编辑图标 ( ) 以编辑网络。
5. 填写“网络属性”中的字段，然后单击“确定”。

   有关网络属性的信息，请单击“帮助”。
6. （可选）要编辑特定网络区域，请执行以下操作：
   a. 单击 + 展开客户端网络的区域列表。
   b. 在“网络列表”中，重命名网络区域或分配网络类型。
   c. 单击“确定”。
7. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)

删除客户端网络

删除客户端网络，以停止监视客户端网络中的 TCP 会话。现有网络数据将继续可用于报告用途。

删除客户端网络时，请切记您：

- 不能从客户端网络中删除某个网络区域。删除客户端网络时，将会删除其所有的网络区域。
- 不能删除管理控制台自动创建的 /32 或 /128 客户端网络。从“服务器列表”中删除相应的服务器。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“网络”。

   将打开“网络列表”。
3. （可选）选择要删除的客户端网络所在的域。
4. 在“网络列表”中，单击红色 X () 以删除网络。
5. 在“删除确认”提示中，单击“继续删除”。
6. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
/32 客户端网络的工作方式 (p. 64)

SNMP 为客户端网络轮询路由器

您可以通过 SNMP 轮询路由器以获取其 IPv4 网络定义，并将它们导入到管理控制台中。请注意，当管理控制台轮询路由器时，您无法在管理控制台中执行其他任务。

在路由器中查询网络信息时，请尝试导入路由成本为零的直连网络。例如，轮询远程站点中的单个路由器，并检索具有 LAN 类型成本的所有网络（例如，小于 5、10 或 18），而不轮询一个站点中的 6 到 7 个路由器。使用“最大成本”可将检索的网络限制在局域网，这样便可将它们与特定远程站点关联，例如，通过遵循标准命名约定并使用网络类型对网络分组。

要允许 SNMP 的管理控制台轮询路由器，请为具有分配的 SNMP 配置文件的路由器添加网络设备。如果不向设备分配 SNMP 配置文件，管理控制台将尝试从可用 SNMP 配置文件的列表中发现有效的 SNMP 配置文件。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“网络”。
3. （可选）选择要将客户端网络导入的域。
4. 在“网络列表”中，单击蓝色齿轮菜单 ( ) 并选择“从 SNMP 导入”。

   将打开“导入网络定义”。
5. 完成各个字段并单击“轮询”。

   有关网络定义属性的信息，请单击“帮助”。

   “轮询确认”消息会通知您，轮询可能需要几分钟的时间。请注意，当管理控制台轮询路由器时，您无法在管理控制台中执行其他任务。
6. 在“轮询确认”中单击“继续”。
7. 在管理控制台完成轮询后，单击“关闭状态窗口”以查看结果。
8. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
管理网络设备 (p. 211)

将客户端网络导出至 CSV 文件中

将管理控制台中的现有客户端网络导出至 CSV 文件中，例如，以生成格式化的网络列表，以便您可以编辑，然后导入到管理控制台中。请注意，管理控制台不允许导入现有客户端网络。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“网络”。

   将打开“网络列表”。
3. （可选）选择要从中导出客户端网络的域。
4. 单击蓝色齿轮菜单 ( ) 并选择“导出网络”。
5. 在“文件下载”对话框中选择选项：
   - 要在 Microsoft Excel 中打开文件，请单击“打开”。
   - 要保存文件，请单击“保存”。在“另存为”对话框中，为文件选择目录和文件名，然后单击“保存”。

详细信息：

管理承租人 (p. 87)

按网络类型对客户端网络分组

通过网络类型，可以将具有相似延迟特征的客户端网络进行组合管理。例如，可对 Cary 站点中的客户端网络分组，并对管理控制台如何管理该位置的性能进行自定义。

默认情况下，CA Application Delivery Analysis 包括预配置的 VPN 和无线网络类型。由于延迟增加，VPN 和无线网络类型的性能阈值将设置为其他网络类型敏感度的的二分之一。

网络类型的工作原理

*网络类型*本质上是一组网络。该组应反映客户端网络上的用户体验的延迟。

总体上，延迟的最大影响因素应是子网的地理位置和带宽。管理控制台包括用于表示带宽的默认网络类型，如 T1，但管理控制台无法假定网络相对于观测应用程序通信的监视设备的具体位置。因此，需要根据您的组织的布局自定义网络类型，因为 200 英里长的 T1 和 1500 英里长的 T1 之间存在很大的性能差异。

所需网络类型的数目取决于您的组织的规模。使用网络类型对必须跨相同网络路径进行对话并因此经历相同延迟的子网进行分组。重要原则是，网络类型应当是共享相同物理资源并因此由于距离、序列化和排队延迟而经历相同延迟的一组子网。准确的网络图非常有助于建立网络类型。

注意：默认情况下，CA Application Delivery Analysis 为延迟变化很大的网络的用户包含了预配置 VPN 和无线网络类型。VPN 和无线网络类型的性能阈值预配置为其他网络类型敏感度的二分之一。作为管理员，您希望管理控制台创建您的团队可以解决的突发事件。在此情况下，不太可能解决通过 Internet 访问网络的远程用户（如在伦敦或新加坡的宾馆里）的延迟问题。

详细信息：

编辑性能阈值 (p. 137)

为何网络类型很有用？

网络类型提供若干优点：

- 自动对客户端网络分组，以用于报告用途。在 CA PC 或 CA NPC 上注册为数据源时，您定义的每个网络类型都会创建一个“网络区域类型”系统组。

  如果未将网络类型分配给您的客户端网络，您可以在 CA PC 或 CA NPC 中创建组，以在管理控制台和 CA PC 或 CA NPC 中报告一组客户端网络。

  考虑在 CA PC 或 CA NPC 中实施基于规则的站点组以管理远程站点。

- 按网络类型调整性能阈值，使不同客户端网络对同一应用程序拥有松紧程度不同的阈值。

  管理控制台会为每个应用程序端口、服务器和客户端网络之间的所有 TCP 会话计算灵敏度阈值。但是，通过网络类型，您可以调整一组特定网络中的应用程序的敏感度。

  如果计划使用静态阈值，则通过网络类型可对一组特定网络设置静态阈值。

- 按照网络类型自定义网络突发事件响应。以下所列是一些示例：
  - 通过电子邮件或 SNMP 陷阱通知适当人员。
  - 为了响应一组特定网络的网络突发事件，启动跟踪路由调查。
- 按网络类型创建性能运行水平协议 (OLA)，以允许远程和本地网络具有不同的性能 OLA 阈值。使用网络类型来组合具有相似延迟的网络，使您能够按网络类型配置 OLA，从而确保您可以针对“网络往复传输时间”和“总事务时间”度量标准配置适当的 OLA。

详细信息：

管理性能阈值 (p. 125)
管理应用程序性能 OLA (p. 175)

添加网络类型

添加网络类型，以标识一组共享通常延迟特征的客户端网络，如远程站点中共享相同的域控制器物理路径的一组客户端网络。

使用与远程站点（包含您要分组的客户端网络）相同的名称对网络类型命名。在对网络类型命名时，请记住，管理控制台无法确定 TCP 数据包在客户端和服务器之间采用的网络路径。例如，如果要为位于奥斯汀（使用 128 Kbps 线路）的子网 10 和子网 50 网络创建网络类型，则可将该网络类型命名为“奥斯汀”。

默认情况下，管理控制台会向“未分配”网络类型分配一个客户端网络。如果您计划实施网络类型，请向客户端网络分配一个可表示一组网络的公共延迟特征的网络类型，而不是默认网络类型。

注意：创建客户端网络的最简单方法是创建网络和关联的网络类型信息的 Excel 图表，并将该列表作为 CSV 文件导入管理控制台中。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“网络类型”。
3. 在“向我显示”菜单下，单击“添加网络类型”。
4. 填写“网络类型属性”中的字段，然后单击“确定”。

   有关指定网络类型属性的信息，请单击“帮助”。

详细信息：

导入 CSV 文件 (p. 39)
向客户端网络分配网络类型 (p. 50)

编辑网络类型

编辑网络类型，以更改其名称或网络突发事件响应。对网络类型的更改适用于分配了网络类型的相应客户端网络。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“网络类型”。
3. 在“网络类型”中，单击编辑图标 ( ) 以编辑网络类型。
4. 填写“网络类型属性”中的字段，然后单击“确定”。

   有关网络类型属性的信息，请单击“帮助”。

详细信息：

管理突发事件响应 (p. 151)

删除网络类型

如果删除分配给网络的网络类型，管理控制台将自动为客户端网络重新分配默认网络类型“未分配”。请注意，可为“未分配”网络类型分配突发事件响应。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“网络类型”。
3. 单击红色 X ( ) 以删除网络类型。
4. 单击“继续删除”以确认您要删除网络类型。

   管理控制台会将“未分配”网络类型分配给以前分配给删除的网络类型的网络。

详细信息：

编辑网络类型 (p. 49)

向客户端网络分配网络类型

将网络类型分配给要在其中启动特定操作以响应网络突发事件的客户端网络。建议将网络类型分配给：

- 客户端网络。在向网络类型分配突发事件响应时，请记住，为了响应分配该网络类型的任何客户端网络上的网络突发事件，管理控制台均会启动指定的操作。

  在向管理控制台中添加客户端网络时，还务必要分配网络类型。默认情况下，管理控制台不向新客户端网络分配网络类型。如有必要，可以编辑一个或多个客户端网络，以分配网络类型。
- 服务器子网。管理控制台自动将指定的网络类型分配给其从相应服务器通信量创建的 /32 和 /128 客户端网络。

详细信息：

/32 客户端网络的工作方式 (p. 64)
编辑客户端网络 (p. 42)
编辑服务器子网 (p. 68)

使用 Web 服务方法管理客户端网络

在管理控制台的三个主要配置和报告元素（应用程序、网络和服务器）中，网络是数量最多、最难于维护的元素。

使用 Web 服务方法，以编程方式创建、读取、更新和删除网络定义，即使用网络配置服务应用程序编程接口 (API)，而不是通过管理控制台添加网络。

请参阅以下各节，了解有关使用 Web 服务方法配置网络的详细信息。

参数说明

以下各节讨论在整个所述 Web 服务方法中使用的参数：

ClientId

类型：4 字节无符号整数

定义：网络定义标识符（clients 表条目）。可能映射到多个网络（client_cache 表条目），具体取决于配置的子区域数。

在“管理配置”页面中，“网络列表”中的每个网络定义都有一个唯一的客户端 ID，但不显示。

ClientSetId

类型：4 字节无符号整数

定义：此定义所属的网络集。此字段不显示，并且始终默认为第一个活动的客户端集标识符。

说明

类型：不超过 50 个字符的字符串 (latin1)

定义：用户为要添加的网络定义指定的标签。

在“管理配置”页面中，“网络列表”中的“网络”列会列出每个网络定义的说明。

网络类型

类型：不超过 50 个字符的字符串 (latin1)

定义：标识定义的已分配类型，如果不需要指定类型，则可以留空或者指定空值/*不分配*。此参数在匹配时不区分大小写。如果找不到匹配项，则会添加新的网络类型。

在“管理配置”页面中，“网络列表”中的“网络类型”列显示与每个网络定义关联的网络类型。如果没有为定义分配网络类型，则会将其标记为“未分配”。

区域

类型：2 的整数幂，介于 1 和 256 之间。地区受子网掩码选择约束；例如，/31 只能扩展成 2 个子区域。

定义：此定义应扩展成的子区域的数量。

在“管理配置”页面中，“网络列表”中的“地区”列显示每个网络定义将扩展成的子区域的数量。显示的值设置为最小值；即每个定义一个区域。

子网

类型：x.x.x.x/m 格式的字符串，其中 x.x.x.x 是有效的 IP 地址，m 为介于 1 和 32 之间的整数子网掩码。

定义：此网络定义的子网的地址和掩码。

在“网络列表”中，“子网”列以预期的地址/掩码输入和输出格式显示网络定义的子网。

Web 服务方法

本节说明 web 服务方法。

详细信息：

错误报告的工作方式 (p. 56)

InsertNetworkDefinition

用途：允许您创建网络定义。

在“管理配置”页面中，“网络属性”中的每个提交的新条目等效于一个方法调用。

输入参数：

- 说明（可选）
- 子网（必需）
- 区域（必填）
- 网络类型（可选，空值等于*未分配*）

返回：具有根节点 *InsertNetworkDefinition* 和 *ClientId* 元素（包含已插入网络的新建 ClientId）的 XML 文档。如果不成功，ClientId 将为零。

返回的错误：提供标准错误报告。

UpdateNetworkDefinition

用途：允许您修改传递的客户端 ID 标识的网络定义，包括子网络说明、IP 地址和掩码。

在“管理配置”页面中，每个网络定义编辑等效于一个方法调用。

输入参数：

- ClientId（必需）
- 说明（可选，但空值会擦除原有说明）
- 区域（必填）
- NetworkType（可选；空值等于*未分配*，新值将创建新的 NetworkType）

返回：true 或 false，表示更新的成功或失败。

返回的错误：提供标准错误报告。

DeleteNetworkDefinition

用途：允许您删除传递的客户端 ID 标识的网络定义。在内部，客户端网络标记为*非活动*。删除已删除网络将导致 *false* 返回代码。

在“管理配置”页面中，从“网络列表”中删除网络等效于一个方法调用。

输入参数：ClientId（必需）

返回：具有根节点 *DeleteNetworkDefinition>* 和 *ClientId* 元素（包含已删除 ClientId）的 XML 文档。

返回的错误：提供标准错误报告。

NetworkDefinitionsList

用途：允许您通过客户端 ID 检索网络定义。

在“管理配置”页面中，“网络列表”包括“默认网络集”中的每个网络定义。

输入参数：无。

返回：每个网络定义对应一个条目的 XML 文档。每个条目包含以下参数：

- ClientId
- 说明
- 网络类型
- 子网
- 区域

返回的错误：提供标准错误报告。

ReloadCollectors

用途：触发所有监视设备重置，以选取配置数据，然后重新启动。

在“管理配置”页面的“向我显示”菜单中，单击“数据监视”，然后单击“监视设备”。在“ADA 监视设备列表”中，单击蓝色齿轮菜单 ( ) 并选择“同步监视器设备”。

输入参数：无

返回：具有根节点 *ReloadCollectors>* 和每个监视设备的状态报告的 *Collector* 元素的 XML 文档。“状态/消息”属性表示重新加载过程成功。分别检查每个监视设备，以查找同步的结果。

返回的错误：提供标准错误报告。

ShowVersion

用途：显示此 API 的字符串/数字版本号。此方法只适用于此 Web 服务 API。

输入参数：无。

返回：字符串形式的版本号。

返回的错误：提供标准错误报告。

如何测试 Web 服务 API

测试并访问网络配置服务 API，并以编程方式管理网络定义。

遵循这些步骤:

1. 导航到 http://localhost/SuperAgentWebService/NetworkConfigService.asmx。此站点提供方便的用户界面，用于访问 NetworkConfigService 和其服务说明。

   要从可以访问的远程计算机访问 NetworkConfigService 测试站点，请将 localhost 替换成 <ADA_Server_FQDN>。

2. 查看 SuperAgent NwkConfig WS 下的应用程序事件日志，以了解对故障的其他解释性消息。
3. 对于脚本操作，请查看示例 Perl 脚本 (p. 57)以练习 API。

详细信息：

示例 Perl 脚本 (p. 57)

错误报告的工作方式

除 ShowVersion() 以外的所有接口均返回 XmlDocument 对象。文档的根节点用方法的名字命名；例如，NetworkDefinitionsList 或 UpdateNetworkDefinition。以下属性会附加到此根节点中：

- 状态：字符串文字 True 或 False，指明执行是否成功。对于 ReloadCollectors()，True 状态不一定表示操作成功，因为当监控脱机或不可用时，重新加载在内部可能不报告任何异常。
- 消息：包含故障的特定错误消息的字符串。如果操作成功，消息将为空。具有堆栈跟踪的完整详细信息将出现在 Windows 事件日志中。

以下示例对这些对象和属性进行了说明：

```
<NetworkDefinitionsList Status="True" Message="">
  <Network>
  <ClientId>3</ClientId>
  <Description>192.168.0.2</Description>
  <SubnetMask>192.168.0.2/32</SubnetMask>
  <Regions>1<_/Regions>
  </Network>
</NetworkDefinitionsList>

<?xml version="1.0" encoding="utf-8" ?> <ReloadCollectors Status="False"
Message="Can't connect to MySQL server on 'localhost' (10061)" />
<?xml version="1.0" encoding="utf-8" ?> <UpdateNetworkDefinition Status="True"
Message=""><ClientId>7</ClientId></UpdateNetworkDefinition>
<?xml version="1.0" encoding="utf-8" ?> <InsertNetworkDefinition Status="True"
Message=""><ClientId>8</ClientId></InsertNetworkDefinition>
```

示例 Perl 脚本

```
#########################################################################
#################
#########################################################################
#
# 练习网络配置 API 的示例 Perl 脚本
# CA
#########################################################################
#
#
#########################################################################
#
# 注意：请修改 $url，以指向 ADA 控制台的承载位置
#########################################################################
#
#
#########################################################################
#
#!/usr/local/bin/perl
use Data::Dump qw(dump);
use SOAP::Lite (
#       +trace => all,
        maptype => {}
);
$SOAP::Constants::DO_NOT_USE_CHARSET = 1;
#
#
#########################################################################
#
my $uri = "http://www.netqos.com/networkconfig";
my $url = "http://localhost/SuperAgentWebService/NetworkConfigService.asmx";
#
my ($method, $result, $networks, @nodes, @params);
my ($clientId, $description, $subnetCidr, $regionCount, $networkType);
#
sub SOAP::Transport::HTTP::Client::get_basic_credentials {
   return $user => $pass;
}
#
#########################################################################
#
my $soap = SOAP::Lite
    -> uri($uri)
    -> on_action( sub { join '/', @_ } )
    -> proxy($url);
#
#
#########################################################################
#
# NetworkDefinitionsList
```

```
##############################################################################
#
$method = SOAP::Data->name('NetworkDefinitionsList')->attr({xmlns => $uri});
$networks = $soap->call($method);
print "\nNetworkDefinitionsList:\n";
if ($networks->fault) {
    print join ', ', $result->faultcode, $result->faultstring,
$result->faultdetail;
} else {
   if ($networks->dataof('//NetworkDefinitionsList')->{_attr}->{Status} eq
"False") {
        print $network->dataof('//NetworkDefinitionsList')->{_attr}->{Message},
"\n";
   } else {
    print "\n\nClientID\tDescription\tSubnet\t\tRegions\t\tNetworkType\n";
    @nodes = $networks->valueof('//Network');
    foreach $n (@nodes)
    {
       print $n->{'ClientId'}, "\t", $n->{'Description'},"\t\t",
       $n->{'Subnet'},"\t\t", $n->{'Regions'}, $n->{'NetworkType'},"\t", "\n";
    }
  }
}
#
##############################################################################
#
# UpdateNetworkDefinition
##############################################################################
#
print "\n\nUpdateNetworkDefinition:\n";
$method = SOAP::Data->name('UpdateNetworkDefinition')->attr({xmlns => $uri});
$clientId = $networks->valueof('//Network/ClientId');
$description = $networks->valueof('//Network/Description') . " UPDATED";
$description = substr($description, 0, 50);
$regionCount = $networks->valueof('//Network/Regions');
$networkType = "未分配";
@params = ( SOAP::Data->name(ClientId => $clientId),
        SOAP::Data->name(Description => $description),
        SOAP::Data->name(Regions => $regionCount),
        SOAP::Data->name(NetworkType => $networkType)
);
$result = $soap->call($method => @params);
if ($result->fault) {
    print join ', ', $result->faultcode, $result->faultstring,
$result->faultdetail;
} else {
   if ($result->dataof('//UpdateNetworkDefinition')->{_attr}->{Status} eq
"False") {
        print
$result->dataof('//UpdateNetworkDefinition')->{_attr}->{Message};
   } else {
       print "UpdateNetworkDefinition($clientId, $description, $regionCount,
$networkType):\n";
       print dump($result->result), "\n";
```

```
   }
}
#
################################################################################
#
# DeleteNetworkDefinition
################################################################################
#
print "\n\nDeleteNetworkDefinition:\n";
$method = SOAP::Data->name('DeleteNetworkDefinition')->attr({xmlns => $uri});
$clientId = $networks->valueof('//Network/ClientId');
$description = $networks->valueof('//Network/Description');
@params = (SOAP::Data->name(ClientId => $clientId)->attr({xmlns => $uri}));
$result = $soap->call($method => @params);
if ($result->fault) {
    print join ', ', $result->faultcode, $result->faultstring,
$result->faultdetail;
} else {
   if ($result->dataof('//DeleteNetworkDefinition')->{_attr}->{Status} eq
"False") {
        print
$result->dataof('//DeleteNetworkDefinition')->{_attr}->{Message};
   } else {
    print "DeleteNetworkDefinition($clientId, $description):\n";
    print dump($result->result), "\n";
   }
}
#
################################################################################
#
# InsertNetworkDefinition
################################################################################
#
print "\n\nInsertNetworkDefinition:\n";
$method = SOAP::Data->name('InsertNetworkDefinition')->attr({xmlns => $uri});
$description = $networks->valueof('//Network/Description');
$subnetCidr = $networks->valueof('//Network/Subnet');
$regionCount = $networks->valueof('//Network/Regions');
$networkType = "未分配";
@params = ( SOAP::Data->name(Description => $description),
        SOAP::Data->name(Subnet => $subnetCidr),
        SOAP::Data->name(Regions => $regionCount),
        SOAP::Data->name(NetworkType => $networkType)
);
$result = $soap->call($method => @params);
if ($result->fault) {
    print join ', ', $result->faultcode, $result->faultstring,
$result->faultdetail;
} else {
   if ($result->dataof('//InsertNetworkDefinition')->{_attr}->{Status} eq
"False") {
        print
$result->dataof('//InsertNetworkDefinition')->{_attr}->{Message};
   } else {
```

```
    print "InsertNetworkDefinition($description, $subnetCidr, $regionCount,
$networkType):\n";
    print dump($result->result), "\n";
   }
}
#
#
################################################################################
#
# ReloadCollectors
################################################################################
#
$method = SOAP::Data->name('ReloadCollectors')->attr({xmlns => $uri});
print "\n\nReloadCollectors():....\n";
$result = $soap->call($method);
if ($result->fault) {
    print join ', ', $result->faultcode, $result->faultstring,
$result->faultdetail;
} else {
   if ($result->dataof('//ReloadCollectors')->{_attr}->{Status} eq "False") {
        print $result->dataof('//ReloadCollectors')->{_attr}->{Message};
   } else {
      @nodes = $result->valueof('//Collector');
      foreach $node (@nodes)
      {
         print $node->{'Address'}, "\t", $node->{'Status'},
"\t",$node->{'Info'}, "\n";
      }
   }
}
#
#
################################################################################
#
# ShowVersion
################################################################################
#
$method = SOAP::Data->name('ShowVersion')->attr({xmlns => $uri});
print "\n\nShowVersion():\n";
$result = $soap->call($method);
if ($result->fault) {
    print join ', ', $result->faultcode, $result->faultstring,
$result->faultdetail;
} else {
    print $result->result, "\n";
}

#
```

第 3 章： 管理服务器

此部分包含以下主题：

服务器的工作方式

server 指定想要监控的服务器 IPv4 地址。配置管理控制台监控服务器子网时其运行最佳。服务器子网指定您希望管理控制台监视的服务器 IPv4 地址的范围，并使管理控制台可以自动监视匹配服务器上的应用程序通信。

默认情况下，管理控制台自动监控称作“*Monitor All Servers* on subnet 0.0.0.0 mask 0”的预定义服务器子网。在添加新监视器时，默认 *Monitor All Servers* 子网启用自动数据收集。

详细信息：

管理控制台如何管理数据库增长 (p. 228)

“服务器子网列表”的工作方式

使用“服务器子网列表”指定一个服务器子网，它标识管理控制台要监视的服务器 IP 地址的范围。当监视设备观测服务器与客户端网络间的匹配应用程序通信量时，根据您指定的服务器子网，管理控制台会将监视设备分配给该服务器，并将该服务器添加到“服务器列表”中。也可以手动将服务器添加到“服务器列表”中。

默认情况下，管理控制台自动监控称作“*Monitor All Servers* on subnet 0.0.0.0 mask 0”的预定义服务器子网。在添加新监视器时，默认 *Monitor All Servers* 子网启用自动数据收集。

“服务器列表”的工作方式

使用“服务器列表”可查看和管理管理控制台监视的服务器。管理控制台会自动监视“服务器列表”中每台服务器上的所有应用程序通信。

通常，用“服务器子网列表”中的指定 IP 地址范围所对应的服务器来填充“服务器列表”。如有必要，您可以添加希望管理控制台监视的特定服务器，管理控制台会立即将该服务器添加到“服务器列表”中。

在 CA PC 或 CA NPC 上注册为数据源时，CA PC 或 CA NPC 自动分组服务器进行报告。

详细信息：

管理服务器子网 (p. 65)
系统组 (p. 197)

/32 客户端网络的工作方式

在将服务器添加到“服务器列表”时，管理控制台会自动创建相应的 /32 客户端网络。/32 客户端网络是具有单个 IPv4 地址的客户端网络。

使用 /32 客户端网络来监视多层应用程序。多层应用程序是在多台服务器上运行的应用程序，服务器之间的通信由至少一台服务器执行 - 该服务器既充当客户端请求的服务器，又充当其他服务器的客户端。

要使管理控制台用户能够快速分析并响应多层应用程序中的网络问题，请为 /32 客户端网络分配网络类型。

在添加服务器子网时，可以分配默认网络类型，这样在管理控制台创建相应的 /32 客户端网络时，便会分配正确的网络类型。

不能删除管理控制台创建的 /32 客户端网络。在从“服务器列表”中删除相应的服务器时，管理控制台会自动删除 /32 客户端网络。

详细信息：

客户端网络的工作方式 (p. 27)
管理多层应用程序 (p. 119)

TCP 会话标识

要使管理控制台能够准确报告来自服务器的应用程序响应时间，监视设备必须能够标识客户端/服务器 TCP 会话的服务器端。监视设备使用以下条件确定 TCP 会话的两个端点中哪个端点表示服务器端：

- 新 TCP 会话。为了标识新 TCP 对话中的服务器端，将针对服务器子网定义检查作为 SYN 收件人的 IP 地址。SYN 收件人的 IP 地址必须在指定的服务器子网中的一个服务器子网中。SYN 和 SYN-ACK 都必须观测到。
- 现有 TCP 会话（看不到 TCP 连接设置的对话的通信）。如果两个端点 IP 均不在服务器子网之一包括的范围内，则忽略该对话。

  如果两个 IP 地址中只有一个在服务器子网的范围内，则假定该端点为服务器。

  如果两个 IP 地址都在一个或多个服务器子网的范围内，并且两者均未记录为已知应用程序，则监视设备假定最低的端口是服务器。

主机名解析

如果在 CA PC 或 CA NPC 上将管理控制台 注册为数据源，在管理控制台将服务器添加到“服务器列表”时，CA PC 或 CA NPC 将使用代理服务器自动查询 DNS。或者，管理控制台在默认端口 UDP-53 上向其 DNS 服务器发送查找请求。

当您执行以下操作时，管理控制台不会自动解析服务器的主机名：

- 手动添加服务器
- 导入服务器的列表

要手动解析服务器的主机名，请编辑服务器属性。

详细信息：

管理服务器 (p. 70)
管理控制台设置 (p. 205)

管理服务器子网

服务器子网可指定要监视的服务器 IP 地址的连续范围。当监视设备观测与指定服务器子网匹配的应用程序通信量时，管理控制台会：

- 将服务器添加到任何匹配的系统应用程序中。
- 将服务器添加到“服务器列表”中，在此可以查看和管理服务器的属性，例如，分配突发事件响应。
- 将服务器作为 /32 或 /128 客户端网络添加到“网络列表”中。

建议将服务器子网添加到与服务器 VLAN 定义完全一致的 CA Application Delivery Analysis 中。为了限制管理控制台在每个服务器子网中监视的 TCP 端口，请为服务器子网络分配端口排除。

Application Delivery Analysis 包括称作“*Monitor All Servers* on subnet 0.0.0.0 mask 0”的默认服务器子网。在添加新监视器时，默认服务器子网将启用自动数据收集。

详细信息：

/32 客户端网络的工作方式 (p. 64)
应用程序端口排除 (p. 96)
应用程序的工作方式 (p. 93)
管理控制台如何管理数据库增长 (p. 228)
管理服务器 (p. 70)

添加服务器子网

添加服务器子网，以自动监视匹配的服务器通信。当指定服务器子网时，请指定 IP 地址范围，该范围表示您希望管理控制台监视的应用程序服务器。通常，此范围与服务器 VLAN 定义几乎完全一致。

在添加服务器子网之后，编辑该服务器子网以添加排除，从而忽略来自指定的服务器 IP 地址范围中的特定服务器的通信。

指定要包括或排除服务器	指定子网掩码的范围
包括	■ IPv4：/16 和 /31。不能指定 /32 子网掩码。
排除	■ IPv4：/17 和 /32。

如有必要，可在监视设备观测其通信之前将服务器添加到管理控制台中。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“服务器”。
3. （可选）选择要添加服务器子网的域。
4. 滚动到“服务器子网列表”，然后单击以添加 IPv4 服务器子网。

   将打开“添加服务器子网”。
5. 完成“服务器子网”中的字段，然后单击“确定”。

   有关设置服务器子网属性的信息，请单击“帮助”。

   管理控制台验证服务器子网未与您已定义的任何现有服务器子网冲突，然后添加服务器子网。
6. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

   在 5-10 分钟之后，“服务器列表”会自动显示与指定的服务器子网匹配的服务器。

详细信息：

管理承租人 (p. 87)
添加服务器 (p. 72)

编辑服务器子网

编辑服务器子网，以更改其 IP 地址范围（例如排除特定服务器）或为管理控制台从匹配的服务器通信量自动创建的客户端网络指定默认网络类型。

在更新的 IP 范围之外的现有数据将继续可用于报告用途。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“服务器”。
3. （可选）选择带有要编辑的服务器子网的域。
4. 滚动到“服务器子网列表”，然后单击 以编辑服务器子网。

   将打开“服务器子网属性”。
5. 完成“服务器子网属性”中的字段，然后单击“应用”。

   有关设置服务器子网属性的信息，请单击“帮助”。

   管理控制台验证服务器子网不与您已定义的任何现有服务器子网冲突，然后添加服务器子网。
6. 单击“添加排除项”，以排除服务器子网所指定的 IP 地址范围内的特定 IP 地址。

   指定 /16（或更高的）子网掩码。
7. 单击“确定”。
8. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
/32 客户端网络的工作方式 (p. 64)

删除服务器子网

删除服务器子网，以防止管理控制台自动监视与服务器子网匹配的新服务器。管理控制台会继续监视与服务器子网匹配的现有服务器。

如有必要，可从“服务器列表”中删除服务器。现有数据将继续可用于报告用途。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“服务器”。

   将显示“服务器列表”。
3. （可选）选择带有要编辑的服务器子网的域。
4. 单击  以删除“服务器子网列表”中的服务器子网。
5. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)

管理服务器

使用“服务器列表”可以管理服务器属性，如：

- SNMP 配置文件。管理控制台需要具有有效 SNMP 用户凭据的 SNMP 配置文件，以在服务器上执行通过 SNMP 的性能调查。

  如果未指定有效的 SNMP 配置文件，管理控制台将尝试发现 SNMP 配置文件。

- 监视器源分配。您可以覆盖管理控制台自动维护的监视器源分配，以便向服务器分配特定监视器源，并选择永久覆盖该分配。

  如果您希望管理控制台监视来自多个监视器源的服务器通信量（例如，当网络故障切换到不同网络路径时或者服务器通信在 2 台交换机之间进行负载平衡时），则可向服务器的已分配监视器源分配备用的监视器源。

- TCP/IP 主机名解析。管理控制台会为匹配指定服务器子网的服务器自动解析 DNS 主机名。

  对于手动添加或导入的服务器，编辑服务器属性以输入主机名。

- 服务器维护排定。管理控制台向服务器分配默认的维护排定，但必须为维护分配排定的期间。

- 突发事件响应。默认情况下，管理控制台不启动操作来响应服务器突发事件。

  如果您计划启用通过 SNMP 的性能调查，则建议您还向服务器分配 SNMP 配置文件。

要限制管理控制台监视的 TCP 端口，请向端口排除中分配服务器或服务器子网。

详细信息：

将操作添加到网络或服务器突发事件响应中 (p. 163)
创建一对监视器源 (p. 225)
监视器源分配的工作方式 (p. 223)
管理 SNMP 配置文件 (p. 207)
排定服务器维护 (p. 79)

命名约定

下表列出了一些建议用于服务器的命名约定。

服务器类型	推荐的命名约定	示例
单一功能服务器	*DNS 名称-IP 地址*	Goliath-196.128.34.1
一个应用程序、场中的多个服务器	*应用程序名称-DNS 名称*	DocMgr-Zeus DocMgr-Athena DocMgr-Mercury
一个应用程序、多个服务器、多个位置	*应用程序名称-DNS 名称-位置*	DocMgr-Hamlet-NewYork DocMgr-Romeo-Milan DocMgr-Othello-London

查找服务器

搜索“服务器列表”，以查找当前监视的服务器。

在“服务器列表”中，单击放大镜 图标以查看管理控制台在服务器中正在监视的应用程序。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“服务器”。
3. （可选）选择带有要编辑的服务器子网的域。
4. 滚动到“服务器列表”，在字段中输入搜索字符串，然后单击“搜索”。

   不支持模式匹配字符，如 * 或 %。
5. 单击“清除”以重置该列表。

详细信息：

管理承租人 (p. 87)

添加服务器

管理控制台将用观测到的服务器自动填充“服务器列表”，这些服务器与指定的服务器子网匹配，并且其应用程序端口通信量不符合您定义的任何端口排除项。

如果要在管理控制台观测到其通信之前将服务器分配给应用程序，请添加该服务器，然后将该服务器分配给应用程序。

添加服务器时，请不要覆盖服务器的自动监视器源分配。而是允许管理控制台在必要时自动重新分配监视器源。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“服务器”。
3. （可选）选择要添加服务器的域。
4. 滚动到“服务器列表”，然后单击以添加 IPv4 服务器。

   将打开“服务器属性”。
5. 填写“服务器属性”中的字段，然后单击“确定”。

   有关设置服务器属性的信息，请单击“帮助”。
6. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)

编辑服务器

使用“服务器列表”可查看和管理管理控制台监视的服务器：

- 单击“应用程序”列中的放大镜 图标，以查看管理控制台在特定服务器中正在监视的应用程序。
- 例如，编辑服务器，以查看其监视器源统计信息或更改其属性。如果更改服务器的属性，其“用户已修改”状态将更改为“是”。监视器源统计信息包括：
  - 服务器通信量(按源)(最后 24 小时) - 按服务器报告每个监视器源上的通信量，这样您就可以验证监视器源分配对于自动分配和固定的监控分配是否都正确。
  - 分配监视器设备的卷统计(过去 7 天) - 描述过去 7 天内分配给服务器的监视设备观测到的通信量。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“服务器”。
3. （可选）选择所需服务器所在的域。
4. 滚动到“服务器列表”，然后单击 来编辑服务器。

   （可选）若要编辑不止一个服务器，请选择每个服务器，然后单击 来批量编辑选定的所有服务器。请注意，您所做的任何更改都将应用到选定的每台服务器。

   将打开“服务器属性”。
5. 填写“服务器属性”中的字段，然后单击“确定”。

   有关设置服务器属性的信息，请单击“帮助”。
6. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)

删除服务器

删除服务器，以停止监视其应用程序端口通信量。删除服务器之后，现有数据继续可用于报告用途。

删除匹配服务器子网的服务器只是暂时删除该服务器。当监视设备观测到与服务器子网匹配的服务器通信量时，管理控制台随后会将该服务器重新添加到列表中。如果要删除的服务器与服务器子网匹配，请编辑服务器子网并添加服务器排除，以防止管理控制台监视该服务器。

如果不需要服务器上的特定端口或端口范围，可添加端口排除。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“服务器”。
3. （可选）选择要删除的服务器所在的域。
4. 滚动到“服务器列表”并单击 来删除服务器。
5. 在提示中单击“继续删除”，以删除服务器。
6. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
应用程序端口排除 (p. 96)
编辑服务器子网 (p. 68)

从 CSV 文件中导入服务器定义

要快速地将新服务器添加到管理控制台中，请将服务器主机名和 IPv4 地址的逗号分隔列表添加到 CSV 文件中，然后将该文件导入管理控制台。您不能：

- 导入服务器子网络定义
- 重新导入现有 IPv4 地址

作为导入过程的一部分，您可以批量编辑服务器列表，例如，分配服务器维护排定。完成后，同步监视设备，以开始使用您指定的属性监视服务器。

创建 CSV 文件

为了快速配置好，可以将用逗号分隔的服务器名称和 IPv4 地址的列表添加到 CSV 文件中。

如果未同时包含服务器名称和 IP 地址，可以在完成导入之前编辑该定义列表。例如，您可以创建仅带有 IP 地址的 CSV 文件，然后可以在完成导入之前指定相应的服务器名称。管理控制台不会查询 DNS 来解析导入服务器的主机名。

执行以下步骤创建一个 CSV 文件，该文件指定希望管理控制台监视的服务器。在创建 CSV 文件时，用逗号分隔每个字段并且：

- 将嵌入的逗号或双引号引在双引号中。
- 在双引号中包含一个或多个空格的字符串；例如："Houston Office"。

下面显示 CSV 格式的服务器定义的示例。“奥斯汀 DNS 服务器”条目指定 ref-sa-coll (CA Standard Monitor) 在其数据包监视器源上查看 192.168.100.2 的服务器通信量，并且默认应使用名为“netqos”的 SNMP 配置文件来轮询服务器：

```
"奥斯汀 DNS 服务器", 192.168.100.2, "ref-sa-coll", "Packets",
"netqos"
```

遵循这些步骤:

1. 创建一个扩展名为 .CSV 的文本文件，例如，austin_servers.csv。
2. 在单独行中指定每个逗号分隔的服务器定义。
3. 对每个条目使用以下格式：
   Server_Name,Server_IP,Monitoring_Device,Monitor_Feed,SNMP_Profile

   Server_Name

   定义希望在管理控制台中显示的服务器名称，最多包含 50 个字符。

   请注意，在导入服务器列表时，管理控制台不自动解析 DNS 主机名。

   Server_IP

   采用由点分隔的四部分十进制符号格式定义服务器的 IPv4 地址。如果指定的地址格式不正确，导入将使用 IP 地址作为服务器名称。

   Monitoring_Device

   （可选）定义查看服务器通信量的监视设备。如果指定监视设备，那么还必须指定设备中的监视器源。导入服务器之后，如有必要，管理控制台会自动重新分配监视设备和监视器源。如果未指定监视器源，管理控制台将自动分配最佳监视器源。

Monitor_Feed

（可选）在查看服务器通信量的监视设备中定义监视器源。如果指定监视设备，还必须指定设备中的监视器源，数据包监视器源中的数据包。导入服务器之后，如有必要，管理控制台会自动重新分配监视设备和源。

如果未指定监视器源，管理控制台将自动分配最佳监视器源。

要浏览监视设备中的可用监视器源名称的列表，请编辑 CA Standard Monitor 或 CA Multi-Port Monitor。

SNMP_Profile

（可选）。定义希望管理控制台在轮询服务器时使用的 SNMP 配置文件名称，例如，作为通过 SNMP 的性能调查的一部分。如果您想要管理控制台发现有效的 SNMP 配置文件，请指定空值 ("")。

4. 保存文件，然后将其导入管理控制台。

详细信息：

监视设备的工作方式 (p. 221)
SNMP 配置文件发现的工作方式 (p. 208)

导入服务器定义

在导入服务器定义时，确保文本文件的文件扩展名为 .CSV。作为导入的一部分，您可以批量编辑服务器定义，例如，分配 SNMP 配置文件。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“服务器”。
3. （可选）选择要将服务器导入到的域。
4. 滚动到“服务器列表”，然后单击蓝色齿轮菜单 ( ) 并选择“从文件导入”。

   将打开“导入服务器定义”。
5. 复查有关 CSV 文件格式的信息，并在必要时将示例复制和粘贴到您的 CSV 文件中。
6. 单击“浏览”选择 CSV 文件，然后单击“下一步”。

   将打开“保存导入服务器定义”。
7. 复查导入的服务器定义的列表，并在必要时进行更改，然后单击“确定”。
8. 在管理控制台中解决您从 CSV 文件导入的定义以及现有服务器定义所具有的任何问题。

   保存导入的服务器定义将突出显示有冲突的服务器定义。
9. 编辑突出显示的服务器定义，以解决任何问题，然后单击“确定”。

   黄色

   表示指定的监视设备不存在，或服务器的 IP 地址无效。管理控制台允许您继续导入，但在继续之前，应先解决以上类型的问题。

   红色

   表示服务器 IP 地址重复。要继续导入，请单击 以删除任何重复的 IP 地址。
10. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

    监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)

将服务器定义导出到 CSV 文件中

将 IPv4 服务器定义导出到 .CSV 文件，以用作导入新服务器定义的模板。请注意，您无法重新导入现有的 IPv4 服务器地址。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“服务器”。
3. （可选）选择要从中导出服务器的域。
4. 滚动到“服务器列表”，然后单击蓝色齿轮菜单 ( ) 以选择“导出服务器”。

   将打开“导出服务器定义”。
5. 选择导出选项，然后单击“确定”。

   只有唯一 IP 地址

   指定您只想导出 IP 地址。

   所有导出字段

   指定您要导出服务器主机名和 IP 地址、分配的监视设备和监视器源，以及分配的 SNMP 配置文件名称。

   将打开“文件下载”对话框。
6. 单击“打开”以查看 CSV 文件内容，或单击“保存”以保存 CSV 文件。

详细信息：

管理承租人 (p. 87)

将监视器源固定到服务器

固定监视器源可以向服务器永久分配一个特定监视器源，例如，您知道希望管理控制台通过其监视该服务器的监视设备，并且不希望管理控制台更改它，那就可以这么做。

当删除某个监视设备时，将取消固定已固定到对应监视器源的所有服务器，并自动分配另一个监视器源。更新监视器源分配可能需要长达 10 分钟。

添加服务器后，可以选择固定某个监视器源。或者，编辑服务器属性，以便向服务器分配一个特定监视器源。

详细信息：

编辑服务器 (p. 73)

排定服务器维护

服务器维护排定指定预计服务器性能出现异常的时间，例如，由于备份或软件更新等排定的维护任务。

在排定的服务器维护期间，管理控制台将会：

- 执行以下操作：
  - 在维护期间开始时关闭现有服务器突发事件。

    如果服务器突发事件条件在维护期间结束后仍然存在，管理控制台将打开一个新服务器突发事件。
  - 继续收集有关应用程序、服务器和网络性能的数据，并将性能分级为“正常”、“轻微”（黄色）或“重大”（橙色）。此数据对于了解维护期间之前、之中和之后的性能很有帮助。
- 请不要：
  - 触发对维护期间创建的新服务器突发事件的响应。
  - 使用在维护期间收集的数据计算敏感度阈值。
  - 使用在维护期间收集的数据计算基准。
  - 计算性能 OLA 或可用性 OLA。

注意：管理控制台用户可以选择在维护期间是否报告下降的应用程序、服务器和网络性能。在报告的“设置”中，使用“包括排定维护”选项显示或隐藏在维护期间收集的性能数据。

维护排定的工作方式

使用“维护排定”列表可以：

- 确定维护排定是否至少有一个维护期间
- 查看将维护排定分配到的服务器的数量

管理控制台提供了“默认”和“周末”维护排定，但这些维护排定不包括任何维护期间。在下面的示例中，管理控制台管理员向每个维护排定至少分配了一个维护期间。

管理控制台自动向新观测的服务器分配“默认”维护排定。建议您向“默认”维护排定中添加一个维护期间，如有必要，还可向服务器分配自定义排定。

要查看分配给特定服务器的维护排定，请编辑服务器属性。

详细信息：

编辑服务器 (p. 73)
向维护排定中添加维护期间 (p. 83)

添加维护排定

通过添加具有适当维护期间的维护排定来覆盖默认维护排定，然后将维护排定分配给适当服务器。

重要说明！确保您为默认维护排定定义了维护期间。管理控制台会自动向新服务器分配默认维护排定。

在添加维护排定之后，向该排定分配维护期间。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“维护排定”。
3. 在“向我显示”菜单下，单击“添加维护排定”。

   将打开“排定属性”。
4. 键入排定名称，然后单击“应用”。

   您现在随时可向维护排定中添加维护期间。
5. 完成后，单击“确定”。

详细信息：

向维护排定中添加维护期间 (p. 83)

重命名服务器维护排定

将服务器维护排定重命名为与现有的服务器维护排定对应的名称。请注意，可对管理控制台提供的“默认”和“周末”维护排定进行重命名。

在重命名维护排定时，还可以修改其维护期间，例如，添加一个维护期间。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“维护排定”。

   将打开“维护排定”。
3. 单击  来编辑维护排定。
4. 在第三个“向我显示”菜单中，单击“编辑排定名称”，以便更改维护排定的名称。
5. 在“排定属性”中键入新名称，然后单击“确定”。

   在“维护排定”中，将显示重命名的维护排定。

详细信息：

向维护排定中添加维护期间 (p. 83)
删除维护期间 (p. 84)
编辑维护期间 (p. 84)

删除维护排定

如果删除正在使用的维护排定，管理控制台将自动为所有受影响的服务器分配“默认”维护排定。要确定是否已将某维护排定分配给服务器，可查看服务器属性。

如果您尚未执行此操作，则建议您向“默认”维护排定中添加维护期间。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“维护排定”。
3. 单击  以在“维护排定”中删除某一维护排定。
4. 在提示中单击“继续删除”，以删除维护排定。

详细信息：

编辑服务器 (p. 73)
向维护排定中添加维护期间 (p. 83)

向维护排定中添加维护期间

每天向维护排定中添加一个或多个维护期间。在向维护排定中添加维护期间后，便随时可将维护排定分配给服务器。

维护期间不能跨越午夜边界。例如，如果有一个每周维护期间从周六晚上 10 点持续到周日早上 4 点，则必须创建两个维护期间：

- 晚上 10 点到周六午夜
- 午夜到周日早上 4 点

建议至少为一个维护排定分配一个维护期间。在下面的示例中，“期间”列中的“警告”图标表示没有为默认维护排定定义维护期间。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“维护排定”。

   将打开“维护排定”列表。
3. 单击 以编辑维护排定。

   将打开“排定期间”列表。
4. 在“向我显示”菜单中，单击“添加期间”。

   将打开“排定期间属性”。
5. 指定排定期间设置，然后单击“确定”。

   有关指定排定期间设置的信息，请单击“帮助”。

详细信息：

向服务器分配维护排定 (p. 85)

编辑维护期间

编辑维护期间，以指定计划进行服务器维护的时间。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“维护排定”。

   将打开“维护排定”。
3. 单击 来编辑维护排定。

   将打开“排定期间”。
4. 单击 以编辑维护期间。

   将打开“排定期间属性”。
5. 指定排定期间设置，然后单击“确定”。

   有关指定排定期间设置的信息，请单击“帮助”。

删除维护期间

删除维护期间，以从服务器维护排定中将其删除。如果您已为服务器分配维护计划，排定应当至少包括一个有效的维护期间，不过，管理控制台不要求分配的维护排定具有维护期间。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“维护排定”。
3. 单击 以编辑“维护排定”列表中的维护排定。

   “排定期间”的列表将会打开。
4. 单击 以删除维护期间。
5. 在“删除确认”中，单击“继续删除”以删除维护期间。

   在“排定期间”内，将删除维护期间。

详细信息：

维护排定的工作方式 (p. 80)

向服务器分配维护排定

服务器维护排定标识服务器性能因排定维护活动而应不正常的一个或多个维护期间。将维护排定分配给一台或多台服务器，以指定计划进行服务器维护的时间。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“服务器”。
3. （可选）选择所需服务器所在的域。
4. 滚动到“服务器列表”，然后单击 来编辑服务器。

   将打开“服务器属性”。

   （可选）若要编辑不止一个服务器，请选择每个服务器，然后单击 来批量编辑选定的所有服务器。请注意，您所做的任何更改都将应用到选定的每台服务器。
5. 单击“维护排定”，从列表中选择排定，然后单击“确定”。

   有关服务器属性的详细信息，请单击“帮助”。

   在编辑多个服务器时，您进行的任何更改都将应用于所有服务器。“无更改”值表示将保留每台服务器中的现有值。
6. 单击“确定”。
7. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
向维护排定中添加维护期间 (p. 83)

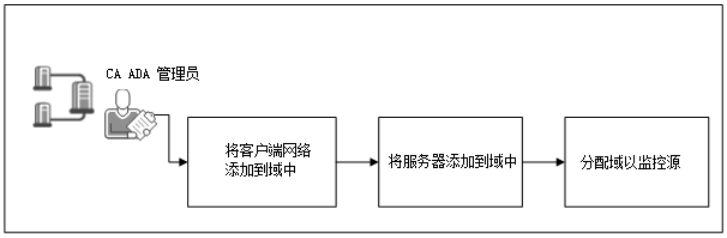
第 4 章： 管理承租人

在 CA Application Delivery Analysis 中使用域管理承租人数据。CA Application Delivery Analysis 无法识别承租人，但是您可以通过域分隔承租人通信。在非 ISP 环境中，域使用重叠（重复）的客户端网络 IP 地址分隔应用程序通信。

重要信息：在 CA Application Delivery Analysis 中，管理员角色对所有域数据和域配置有访问权限。在 CA Application Delivery Analysis 上不要将管理员角色提供给承租人用户。

租用简介

使用域可唯一标识监视器源上服务器和客户端网络之间的通信量。CA Application Delivery Analysis 就是通过按域分隔承租方数据来支持多承租方的。



请完成以下任务：

1. 将客户端网络添加到域 (p. 90)。
2. 将服务器添加到域 (p. 90)。
3. 为监视器源分配域 (p. 92)。

先决条件

要在 CA Application Delivery Analysis 中使用 CA PC 管理承租人，请确保：

- CA PC 满足以下要求：
  - CA Application Delivery Analysis 是注册的数据源。
  - 承租方用户有权访问相应的 IP 域组。不授予承租方用户访问来自其他承租方的域数据的权限。
  - 承租方用户在 CA Application Delivery Analysis 上没有“管理员”角色。“管理员”角色授予 CA Application Delivery Analysis 用户访问所有域中所有数据以及“管理”页面的权限。
  - CA Application Delivery Analysis 数据源已同步。
- CA Application Delivery Analysis 满足以下要求：
  - 监视设备上的监视器 NIC 可以从数据包标头读取 VLAN 标记信息。如果不需要按 VLAN 分隔通信量，这将不适用。

    注意：使用配置实用工具来确认 VLAN 标记信息可用，或从监视设备进行数据包捕获。
  - 管理控制台与 CA PC 或 CA NPC 的域列表同步。

    注意：在“管理”页面上依次单击“数据监视”、“域”，可显示可用域的列表。

要在 CA Application Delivery Analysis 中使用 CA NPC 管理承租人，请确保：

- CA NPC 满足以下要求：
  - CA Application Delivery Analysis 是注册的数据源。
  - 承租人用户有权访问适当的域组。不授予承租方用户访问来自其他承租方的域数据的权限。
  - 承租方用户在 CA Application Delivery Analysis 上没有“管理员”角色。“管理员”角色授予 CA Application Delivery Analysis 用户访问所有域组中所有数据以及“管理配置”页面的权限。
  - CA Application Delivery Analysis 数据源已同步。
- CA Application Delivery Analysis 满足以下要求：
  - 管理控制台与 CA NPC 中的域组列表同步。

域如何分隔通信

域在以下位置分隔通信：

- 监视器源
- 客户端网络
- 服务器子网或服务器

为服务器、网络和监视器源分配相同的域后，管理控制台从监视器源报告客户端和服务器之间的唯一应用程序通信。

基于 VLAN 标记定义，可以将 VLAN 标记的通信在监视器源分隔成不同域。将 VLAN 标记的通信分隔成域允许单个监视器源监控多个域。

应用程序独立于域。报告可以显示各个域的应用程序性能，无需多个应用程序定义，例如 Exchange Company A 和 Exchange Company B。

请注意，应用程序属性中不含域信息。例如，如果重命名某个应用程序，则该应用程序在不同域中的名称相同。然而，如果您想为应用程序性能、性能 OLA 及可用性 OLA 设置不同阈值，则必须为每个域都创建一个应用程序。

数据源同步

CA PC 和 CA NPC 与 CA Application Delivery Analysis 同步域列表。管理控制台最多花费 5 分钟来更新其域列表。

从 CA PC 删除域时，管理控制台：

- 删除与域关联的所有客户端网络、服务器子网、服务器及端口排除，并从用户定义的应用程序中删除关联的服务器分配。

  将继续提供现有的特定于域的数据，以便进行报告。

  请注意，用户定义的应用程序不与特定域相关联，因此，删除域后，如果管理控制台在属于任何剩余域的服务器和客户端网络之间观测到应用程序通信，管理控制台便会继续报告该应用程序。
- 将与域关联的所有监视器源重新分配给默认域。请注意，您无法删除默认域。

详细信息：

用户和组 (p. 197)

基于域的报告的工作方式

可以使用“设置”页面来报告与特定域相对应的服务器和网络情况。应用程序是独立于域的，因此，您不需要按域对应用程序进行筛选。

在 CA PC 和 CA NPC 中使用域组权限，以便为承租人用户提供访问其域的报告数据的权限。

深入到 CA MultiPort Monitor 时将会保留您选择的报告设置。

如果管理控制台中“向我显示”框不显示域列，则请检验管理承租人的先决条件。

详细信息：

先决条件 (p. 88)

将客户端网络添加到域

将客户端网络添加到域。为服务器、网络和监视器源分配相同的域后，管理控制台就可以针对客户端网络与服务器之间的独特应用程序通信量生成报告。

添加客户端网络时，请确保指定正确域。添加客户端网络之后，将无法更改其所在的域。必要时，删除客户端网络，然后将其添加到正确域。

详细信息：

添加客户端网络 (p. 41)

将服务器添加到域

将服务器添加到域。为服务器、网络和监视器源分配相同的域后，管理控制台就可以针对客户端网络与服务器之间的独特应用程序通信量生成报告。

添加服务器时，请确保指定正确域。添加服务器之后，将无法更改其所在的域。必要时，删除服务器，然后将其添加到正确域。

详细信息：

添加服务器子网 (p. 66)
添加服务器 (p. 72)

为监视器源分配域

分配域以指定管理控制台进行报告的位置：

- 未标记的通信量。所有未标记的通信量都将分配给监视器源的域。
- VLAN 标记的通信量。通过将 VLAN 分配给域来分隔监视器源上 VLAN 标记的通信量。

  您也可以将域分配给未分配的 VLAN 通信量。

默认情况下，会将监视器源上的所有通信量都分配给默认域。

重要说明！同时使用 Multi-Port Monitor 和 CA CEM TIM 时，请不要将 TIM 逻辑端口上的 VLAN 通信量分配给域。TIM 不支持基于 VLAN 的监视器源。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“ADA 监视设备列表”，然后单击编辑图标 ( ) 以编辑监视设备。

   将打开“监视器属性”。
4. 向下滚动至“监视器源”。
5. 单击编辑图标 ( ) 以编辑监视器源。

   将展开“监视器源”列表。

   a. 单击“域”以将域分配给未使用 VLAN 信息标记的通信量。

   b. 单击“应用”。
6. 单击“分配 VLAN”。

   在“分配 VLAN”中，编辑监视器源的 VLAN 分配：

   a. 指定要分配给每个域的 VLAN。

   b. 在“未分配 VLAN”列中，为未分配的 VLAN 通信量指定域。

      有关详细信息，请单击“帮助”。

   c. 单击“确定”。
7. 重复这些步骤，为每个监视器源分配域。

详细信息：

管理承租人 (p. 87)

第 5 章： 管理应用程序

此部分包含以下主题：

应用程序的工作方式

*应用程序*指定了您希望管理控制台跨一系列服务器 IP 地址监视的 TCP 端口或端口范围。例如，管理控制台可以监视跨 /29 服务器子网的 TCP-80 通信量。

默认情况下，管理控制台自动创建系统定义的应用程序，以监视跨越所有客户端网络的所有应用程序端口和服务器上的 TCP 会话。例如，如果管理控制台配置为监视若干个 /24 服务器子网，管理控制台将创建一个系统定义的 Microsoft SQL Server 应用程序，以监视所有服务器中的 TCP-1433 通信量。在供应具有匹配的 IP 地址的新服务器时，管理控制台会自动监视它们。

创建端口排除，以忽略所有服务器子网、特定服务器子网或特定服务器上的特定端口或端口范围中的 TCP 会话。

从系统定义的应用程序列表中，可以根据您的专业知识而不只是根据 TCP 标头中提供的信息创建用户定义的应用程序，以报告承载应用程序的实际服务器的情况。例如，要报告特定数据库应用程序的性能，请创建用户定义的 SQL Server 应用程序并分配用于标识承载应用程序的适当服务器的应用程序子网。

或者，如果您知道同一应用程序总是在同一端口上运行，则可让管理控制台自动监视所有服务器中的应用程序。

在 CA PC 或 CA NPC 上注册为数据源时，CA PC 或 CA NPC 自动分组所有应用程序以进行报告。

如果已在 CA PC 或 CA NPC 中定义域，则可选择一个域，来筛选观测的应用程序通信。

详细信息：

管理承租人 (p. 87)
应用程序端口排除 (p. 96)

优先应用程序的工作方式

为了管理数据库的增长，CA Application Delivery Analysis Manager 在必要时会针对低数据量的应用程序梳理 5 分钟数据。CA Application Delivery Analysis Manager 梳理数据后，应用程序的数据将仅在 5 分钟间隔内可用，“操作”页面中的响应时间数据会看起来像一个“棋盘”。

如果不希望 CA Application Delivery Analysis Manager 为系统或用户定义的应用程序梳理 5 分钟数据，请编辑“应用程序属性”并选中“优先级”复选框。CA Application Delivery Analysis Manager 不会对优先应用程序梳理数据。

详细信息：

管理控制台如何管理数据库增长 (p. 228)
编辑用户定义的应用程序 (p. 117)

查找应用程序

筛选“应用程序列表”，以查找所需应用程序：

显示子网 | 服务器

指定选项，以查看观测和分配的服务器信息：

- “*子网*”将显示承载应用程序通信的相应服务器子网。
- “*服务器*”将显示承载应用程序的实际服务器。

搜索

在“应用程序列表”中查找匹配条目。要清除搜索结果，请单击“清除搜索”。

重置列表

在“应用程序列表”中删除所有当前选择，包括当前不可见列表的页面。如果您不确定是否已选择某一对象，请在选择所需对象之前单击“重置列表”命令。

显示应用程序列表

筛选系统和用户定义的应用程序。

每页最多

指定每页的最多应用程序条目数。如果应用程序列表占据一页以上的位置，则列表会保留您在页面之间导航时所做的全部选择。

域

（可选）指定一个域，以筛选观测的应用程序服务器端口通信量。

详细信息：

管理承租人 (p. 87)
管理用户定义的应用程序 (p. 106)
管理系统定义的应用程序 (p. 103)

命名约定

下表列出了一些建议用于应用程序的命名约定。

应用程序类型	推荐的命名约定	示例
一个应用程序、单个端口	User-Defined-*端口号*	User-Defined-80

应用程序类型	推荐的命名约定	示例
一个应用程序、多个端口	User-Defined-*开始端口号-结束端口号*	User-Defined-1024-5000 User-Defined-135-145 User-Defined-110-120 User-Defined-25-50

应用程序端口排除

创建端口排除，以忽略所有服务器子网、特定服务器子网或特定服务器上的特定端口或端口范围中的 TCP 会话。默认情况下，管理控制台会创建系统定义的应用程序，以监视与指定的服务器子网匹配的所有服务器上的所有应用程序端口。

详细信息：

管理服务器子网 (p. 65)

端口排除的工作方式

*端口排除项*对监视设备上的应用程序端口通信量进行筛选，最大化管理控制台上的可用资源，同时可以使管理控制台用户将注意力集中放在要关注的应用程序上。监视设备会忽略与端口排除项匹配的 TCP 会话。例如，每次用户连接到远程共享（如 \\myserver\sharename）时，SMB（服务器消息块）协议将打开两个 TCP 会话，TCP-139 和 TCP-445。如果远程会话建立在 445（Windows 2000 后的任何基于 Windows 的系统）上，SMB 协议将重置 (RST) 139 会话，并使用在 TCP 端口 445 上建立的会话。SMB 将 TCP-139 用于 Windows 2000 之前的 Windows 计算机。要避免监视所有指定服务器子网上的短期 TCP-139 会话，请为端口 139 创建一个端口排除项，并在必要时将其分配给域。

端口排除的优先级高于系统和用户定义的应用程序。例如，如果要创建用户定义的应用程序，并且存在与所需端口范围匹配的现有端口排除，请编辑该端口排除以允许管理控制台监视端口范围，然后创建该应用程序。

还可以使用端口排除来忽略那些不想关注的应用程序服务器通信量；未设置排除时，管理控制台会自动对它们进行监视。例如，假定所有 Microsoft SharePoint 服务器都承载在 192.168.43.0/24 服务器子网中，但 192.168.43.14 和 192.168.43.15 是测试服务器，您不想对其进行监视。要让管理控制台自动监视所有生产 SharePoint 服务器，请执行以下操作：

- 创建名为 SharePoint-80 的应用程序，并为其分配 192.168.43.0/24 服务器子网。
- 要忽略测试 SharePoint 服务器，请在 TCP-80 上针对 192.168.43.14 和 192.168.43.15 创建端口排除。

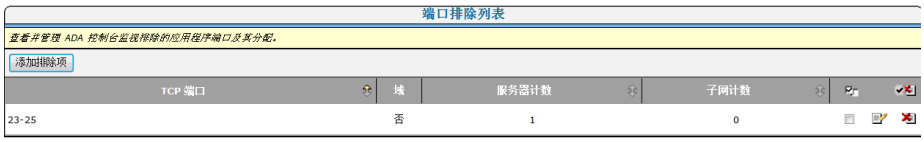
详细信息：

管理承租人 (p. 87)

端口排除列表的工作方式

使用“端口排除项列表”可以查看和管理用于指定忽略哪些应用程序端口的端口排除项。“服务器计数”和“子网计数”列指明端口排除应用到的服务器或子网的数目。

CA Application Delivery Analysis 不监视匹配端口排除项的应用程序通信。您不能创建端口范围与端口排除匹配的应用程序。



添加端口排除

添加端口排除，以指定您希望管理控制台忽略的端口范围：

- 域中的所有服务器。如果未定义域，则可配置管理控制台，以通过向默认域中添加端口排除来忽略所有服务器中的端口通信量。
- 服务器子网中的所有服务器。如有必要，可以创建自定义服务器子网，以忽略特定服务器 IP 地址范围中的应用程序端口通信量。
- 一台或多台服务器。管理控制台可以忽略特定的一台或多台服务器的端口通信量。如有必要，可将服务器添加到端口排除中。

在添加端口排除时，如果存在与端口排除匹配的现有应用程序，管理控制台将停止监视这些应用程序。

删除应用程序时，您可以选择创建一个端口排除项，以防止管理控制台以后自动监视该应用程序。

按照以下步骤添加端口排除项：

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. （可选）选择要将端口排除添加到的域。如果您未定义域来分离重复的 IP 通信量，此选项将排除默认域中所有监视设备中的端口通信量。
4. 滚动到页面底部的“端口排除列表”，并单击“添加排除项”。

   将打开“端口排除属性”。
5. 指定“开始端口”和“结束端口”，以排除特定的端口或端口范围。

   “开始端口”必须小于或等于“结束端口”。
6. （可选）要排除当前选定域中所有服务器上的端口范围，请选择“忽略域中所有服务器上的应用程序端口通信量”。请注意，如果未定义域，默认域将应用于所有服务器。

   在选择此选项时，管理控制台会提示您确认要忽略域中的端口通信量。
7. （可选）要排除某一服务器范围中的端口范围，请执行以下操作：

   a. 单击“分配子网”。

   b. 在“端口排除项子网”中，分配现有服务器子网或创建应用程序子网以排除某一服务器范围中的端口通信量。

      要创建应用程序子网，请指定 IP 地址和掩码，然后单击“添加应用程序子网”。

要分配现有服务器子网，请双击所需子网。可用子网列表包括管理控制台 用来在监控环境中的服务器的服务器子网络以及您已经创建的任何应用子网。

c. 单击“应用”。

8. （可选）要排除特定的一台或多台服务器中的端口范围，请执行以下操作：

   a. 单击“分配服务器”。

   b. 在“端口排除项服务器”中，双击可用服务器，以将其添加到端口排除项中。

   c. 单击“应用”。

9. 单击“确定”。

10. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

    监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理服务器 (p. 61)
管理承租人 (p. 87)
删除用户定义的应用程序 (p. 118)

编辑端口排除

编辑端口排除，以更新希望管理控制台忽略的端口和服务器的范围。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. （可选）选择要编辑端口排除项的域。
4. 滚动到页面底部的“端口排除项列表”，然后单击 以编辑端口排除项。

   将打开“端口排除属性”。
5. 指定端口排除属性，并单击“确定”。

   有关指定端口排除项属性的信息，请单击“帮助”。
6. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)

删除端口排除

删除端口排除项，可恢复对先前排除的端口通信的监视。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. （可选）选择要从中删除端口排除的域。
4. 滚动到页面底部的“端口排除列表”，并单击 以删除排除项。

   （可选）要删除多个应用程序排除项，请选择适当的排除项，并单击 以删除所有选定的排除项。
5. 在出现提示时单击“继续删除”，以允许管理控制台自动监视匹配的应用程序端口通信。

   排除项将被删除。
6. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)

管理系统定义的应用程序

管理控制台会基于您指定的客户端网络和服务器子网的列表创建系统定义的应用程序，以监视匹配的每台服务器上最繁忙的“标准”应用程序和主动 FTP（TCP-20 和 TCP-21）应用程序。

如果可能，请允许管理控制台自动监视所有服务器上的应用程序通信量。与用户定义的应用程序不同，不能将服务器分配给系统定义的应用程序。如果除了 TCP 数据包中提供的可用于监视应用程序的信息外，管理控制台还需要其他信息，请创建用户定义的应用程序。例如，可以创建一个用户定义的应用来监视：

- 在一系列端口上通信的应用程序
- 在 TCP-80 上通信的特定 Web 应用程序

您不能为系统定义的应用程序设置性能 OLA 或可用性 OLA。但如果您要将 OLA 应用于管理控制台监视的所有服务器，请创建用户定义的应用程序并将其分配给域中的所有服务器。

要减少管理控制台自动监视的应用程序端口的数目，请执行以下操作：

- 删除应用程序。
- 创建端口排除。

详细信息：

删除系统定义的应用程序 (p. 105)
应用程序端口排除 (p. 96)
向应用程序分配服务器 (p. 115)

编辑系统定义的应用程序

例如，编辑系统定义的应用程序，以便：

- 重命名应用程序。默认情况下，管理控制台会对熟知端口中的系统应用程序命名。
- 确定应用程序的优先级并阻止管理控制台梳理或筛选应用程序。
- 更改默认的突发事件响应。请注意，默认的应用程序突发事件响应不指定任何响应操作。

系统定义的应用程序的状态不会变化。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. 如果已在 CA PC 或 CA NPC 中定义了域，则您不需要选择域。您对系统定义的应用程序属性所做的任何更改将应用到所有域。
4. 浏览“应用程序列表”中的“配置者”列，以查找系统配置的应用程序。

   如有必要，单击“重置列表”来重新组织“应用程序列表”。

   要编辑多个系统定义的应用程序，请选择所需的应用程序。请注意，您不能将多个应用程序重命名为相同的名称。
5. 选择需要的应用程序，然后单击“编辑”。

   将打开“应用程序属性”。
6. 完成“应用程序属性”中的字段，然后单击“确定”。

   有关设置应用程序属性的信息，请单击“帮助”。
7. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
管理用户定义的应用程序 (p. 106)

删除系统定义的应用程序

删除系统定义的应用程序，以优化管理控制台及其监视设备中的可用系统资源。通过创建端口排除项来删除应用程序后，可以防止管理控制台自动监视它。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. 如果已在 CA PC 或 CA NPC 中定义了域，则您不需要选择域。您对应用程序所做的任何更改都将应用到整个域。
4. 浏览“应用程序列表”中的“配置者”列，以选择系统配置的应用程序并单击“删除”。

   如有必要，单击“重置列表”来重新组织“应用程序列表”。

   要删除多个系统定义的应用程序，请选择所需的应用程序。请注意，您不能将多个应用程序重命名为相同的名称。
5. 选择选项以删除应用程序：

   删除和添加端口排除

   删除选定的应用程序，并阻止管理控制台自动监视该应用程序。

   删除

   删除选定的应用程序，但允许管理控制台在看到匹配的应用程序通信量时自动监视该应用程序。
6. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
应用程序端口排除 (p. 96)

管理用户定义的应用程序

如果可能，请允许管理控制台自动监视所有服务器上的应用程序通信量。如果除了 TCP 数据包中提供的可用于监视应用程序的信息外，管理控制台还需要其他信息，请创建一个用户定义的应用程序并分配特定服务器或服务器 IP 地址的范围。例如，可以创建一个用户定义的应用来监视：

- 在一系列端口上通信的应用程序
- 特定的一台或多台服务器上的 TCP-80 通信量

使用系统定义的应用程序的列表标识最繁忙的应用程序端口，然后利用您的应用程序专业知识创建用户定义的应用程序，以监视通信量最大、对业务最关键和对时间最敏感的 TCP 应用程序。

在创建用户定义的应用程序以监视系统应用程序当前监视的应用程序服务器通信量时，请记住，在创建用户定义的应用程序之后：

- 系统应用程序将停止报告分配给用户定义的应用程序的匹配服务器的情况。如果管理控制台在用户应用程序的服务器分配未标识的服务器上观测到应用程序通信量，管理控制台将报告系统应用程序中的应用程序服务器响应时间。
- 管理控制台将收集新数据，以报告用户定义的应用程序的情况。管理控制台不报告用户应用程序中现有的系统应用程序数据。
- 端口排除的优先级高于系统和用户定义的应用程序。如有必要，可从任何端口排除中删除所需端口，然后创建用户定义的应用程序。

详细信息：

应用程序端口排除 (p. 96)
向应用程序分配服务器 (p. 115)

创建标准应用程序

*标准应用程序*是连接到服务器上某一端口的典型 TCP 应用程序。所有通信量都在该端口与客户端上的端口之间流动。任意类型的监视设备都可以监视标准应用程序。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. （可选）选择域来筛选可用服务器子网和服务器的列表。
4. 使用下列方法之一可创建用户定义的应用程序：

   创建新应用程序

   单击“创建新应用程序”。

   基于现有系统定义的应用程序创建新应用程序

   单击系统应用程序，然后单击“创建新应用程序”。要创建在一系列端口上通信的应用程序，请单击所需的系统应用程序。
5. 将“应用程序类型”设置为“标准”，然后完成“应用程序属性”中的字段：
   - 应用程序名称。
   - 使其成为优先应用程序。选择此选项可指定您不希望管理控制台梳理或筛选该应用程序。
   - 开始端口。端口范围的开始 TCP 端口号。
   - 结束端口。端口范围的结束 TCP 端口号。
   - 端口方。选择一个选项来指定标准应用程序如何响应客户端请求：
     - 应用程序在这些端口上侦听。当服务器侦听指定端口范围内的客户端请求时，请指定该选项。这是默认设置。
     - 应用程序与这些端口对话。当服务器响应客户端上指定端口范围内的客户端请求时，请选择该选项。通过 Cisco NAM 监视设备监视应用程序时，此选项不适用。
   - 突发事件响应。选择应用程序突发事件响应，以指定 Application Delivery Analysis 如何响应影响应用程序的网络或服务器突发事件。
   - 可用性监视。选择一个选项以启用或禁用对应用程序的可用性监视。启用时，管理控制台会被动地观测应用程序的可用性，必要时会主动检查其可用性。
   - 注意。（可选）有关应用程序的更多信息。

有关设置标准应用程序属性的信息，请单击“帮助”。

6. 单击“下一步”，为应用程序分配服务器子网和服务器，然后单击“确定”。

   有关为应用程序分配服务器的信息，请单击“帮助”。

7. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
向应用程序分配服务器 (p. 115)

创建 Web 应用程序

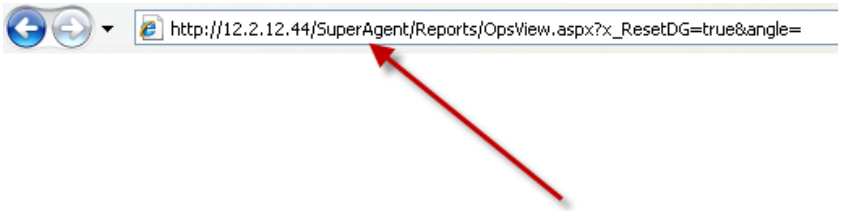
创建 Web 应用程序以报告 HTTP 通信量的 TCP 响应时间。要监视 HTTP 通信量，您必须使用 CA Standard Monitor。

指定希望监视的 Web 应用程序的资源路径。该资源路径必须与 HTTP 请求标头（GET，POST，HEAD 或 TRACE) 中的内容匹配。管理控制台使用该资源路径来标识 Web 服务器上的特定 HTTP 通信量。

重要说明！如果管理控制台仅报告 *appname*-其他应用程序，请根据数据包捕获确认您指定的资源路径匹配 HTTP 请求标头。在某些情况下（例如，当监视通过代理的 Web 通信量时），可能需要您指定完整的 URL，例如 http://*server/resource*，而不是以下示例中显示的资源路径：

/SuperAgent

标识到 CA Application Delivery Analysis 的所有 HTTP 通信量。例如：



/pc

标识到 CA NPC 的所有 HTTP 通信量。例如：

管理控制台会为您定义的每个资源路径创建单独的 Web 应用程序，并创建一个 *appname*-Other 应用程序来监视分配给该应用程序的所有服务器上的所有其他 HTTP 通信量。使用 *appname*-Other 应用程序可分析网站上的资源更改。例如，如果 *appname*-Other 应用程序经历性能下降，则会分析服务器上的 HTTP 通信量并在必要时添加资源路径。

如果您具有负载平衡的 Web 应用程序，则为该应用程序分配服务器子网可使 管理控制台 在配置服务器时自动监视每个资源路径的响应时间。

详细信息：

面向 Internet 的 Web 应用程序 (p. 111)

Web 应用程序注意事项

在创建 Web 应用程序时，请记住以下几点：

- 您必须使用数据包源 (一个 CA Standard Monitor) 才能监视 Web 应用程序。CA Standard Monitor 是监视 Web 应用程序的唯一监视设备。在创建 Web 应用程序之后，确认为属于该 Web 应用程序的每个服务器分配数据包监视器源。
- 不要创建 Web 应用程序来监视服务器上的所有 HTTP 通信量。如果您要监视服务器上的所有 TCP-80 或 8080 通信量，请创建标准应用程序。Web 应用程序是需要大量使用监视设备的过程，因为监控必须处理 HTTP 标头。
- 不要在 2 个以上非标准端口上监视 Web 应用程序。非标准端口是除 TCP-80 或 TCP-8080 之外的端口。例如，您可以在 TCP-80 和 TCP-8080 上以及其他 2 个端口上监视 Web 应用程序。处理非标准端口所需的其他资源会对管理控制台性能产生负面影响。
- 在用户通过代理服务器访问 Web 应用程序时，管理控制台将从代理服务器的客户端网络报告应用程序通信量。

  如果代理服务器使用 X-Forwarded-For (XFF)，管理控制台可以转换 XFF 标头，以报告实际客户端网络，而不是代理服务器的客户端网络。
- 管理控制台 不报告来自任何 Web 应用程序的 HTTP 会话。
- 由于 URL 已加密，因此管理控制台无法在 HTTPS (TCP-443) 上监视 Web 应用程序通信量。所有此类通信量都显示在“其他”应用程序中。

详细信息：

编辑服务器 (p. 73)
支持 XFF 转换 (p. 252)

面向 Internet 的 Web 应用程序

当进行响应时间计算时，管理控制台假定它位于应用程序服务器旁边。监视接近服务器的响应时间使管理控制台能够准确度量网络和服务器响应时间。

监控 Internet 上的网站将导致偏离的度量标准，因为管理控制台在客户端旁边，而不在服务器旁边。在客户端上测量的服务器响应时间将包括服务器的网络延迟。

在监控面向 Internet 的 Web 应用程序时，建议禁用网络性能度量标准的性能阈值，而仅监控服务器性能度量标准的性能阈值状态。设置网络度量标准的阈值对于针对特定网站并共享特定线路的客户端子网很有意义。对于有意义的网络性能阈值而言，Internet 是过于广泛的类别。

如果要监视第三方服务（如 google.com），则请使用 IPSLA 测试来记录响应时间，但由于 Internet 延迟、服务器响应或应用程序问题无法知道何时峰值出现。

详细信息：

编辑性能阈值 (p. 137)

创建 Web 应用程序

通过指定要监视的 Web 服务器上资源的路径创建 Web 应用程序。管理控制台会自动创建一个 Web 应用程序，以报告分配给该应用程序的所有服务器中匹配的 HTTP 通信量。

重要信息！要监控特定资源的 HTTP 通信，您必须在 CA Standard Monitor 上使用“数据包”监视器源。

您必须至少指定一个要监视的资源路径。

重要说明！如果希望监视某个服务器上的*所有* HTTP 通信，请创建监视 TCP-80 或 TCP-8080 通信的标准应用程序。

按照以下步骤创建 Web 应用程序：

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. （可选）选择域来筛选可用服务器子网和服务器的列表。
4. 滚动至“应用程序列表”，然后单击“创建新应用程序”。
5. 将“应用程序类型”设置为“Web”。
6. 填写“应用程序属性”中的字段。

   有关设置 Web 应用程序属性的信息，请单击“帮助”。
7. 单击“下一步”，为应用程序分配服务器子网和服务器，然后单击“确定”。

   有关为应用程序分配服务器的信息，请单击“帮助”。
8. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。
9. 编辑服务器属性，以确认分配给应用程序的每台服务器也分配给 CA Standard Monitor 上的数据包监视器源。监视 Web 应用程序需要数据包监视器源。

详细信息：

管理承租人 (p. 87)
编辑服务器 (p. 73)
向应用程序分配服务器 (p. 115)

创建 FTP 应用程序

创建 FTP 应用程序来监视特定服务器上的主动 FTP。管理控制台自动监视所有主动 FTP 会话。各种类型的监视设备都可以监视 FTP 应用程序。

在主动 FTP 中，由于请求和响应操作发生在不同的端口上，因此管理控制台监视命令和数据端口对来确定响应时间。

在主动 FTP 中：

TCP 端口	是
20	数据端口。FTP 服务器的本地数据端口，以向客户端传输数据。
21	命令端口。客户端连接到此端口，以发送 FTP 命令。

要监视使用不同端口的主动 FTP 应用程序，请创建控制端口应用程序。

请注意，管理控制台也会自动监视被动 FTP。但是，由于被动 FTP 会打开服务器上未授权的随机端口，以向客户端传输数据，因此应用程序活动数据量很低。因此，被动 FTP 应用程序无法冒泡到管理控制台的“操作”页面。

要创建主动 FTP 应用程序，请执行以下步骤：

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. （可选）选择域来筛选可用服务器子网和服务器的列表。
4. 滚动至“应用程序列表”，然后单击“创建新应用程序”。
5. 将“应用程序类型”设置为“FTP”。
6. 填写“应用程序属性”中的字段。

   有关设置 FTP 应用程序属性的信息，请单击“帮助”。
7. 单击“下一步”，为应用程序分配服务器子网和服务器，然后单击“确定”。

   有关为应用程序分配服务器的信息，请单击“帮助”。
8. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
创建控制端口应用程序 (p. 114)
向应用程序分配服务器 (p. 115)

创建控制端口应用程序

可以创建控制端口应用程序来监视应用程序，其中控制端口负责发送和接收请求信息，数据端口负责发送和接收实际数据。管理控制台必须监视这两个端口才能确定事务响应时间。各种类型的监视设备都可以监视控制端口应用程序。

遵循这些步骤:

1. 单击“监管”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. （可选）选择域来筛选可用服务器子网和服务器的列表。
4. 滚动至“应用程序列表”，然后单击“创建新应用程序”。
5. 将“应用程序类型”设置为“控制端口”。
6. 填写“应用程序属性”中的字段。

   有关设置控制端口应用程序属性的信息，请单击“帮助”。
7. 单击“下一步”，为应用程序分配服务器子网和服务器，然后单击“确定”。

   有关为应用程序分配服务器的信息，请单击“帮助”。
8. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
向应用程序分配服务器 (p. 115)

向应用程序分配服务器

使用“应用程序列表”可查看和管理承载应用程序的服务器。

如果承载应用程序的服务器具有连续范围的 IP 地址，则向应用程序分配服务器子网而不是特定服务器。指定服务器子网可优化管理控制台性能并启用自动服务器分配。

重复使用现有服务器子网，或创建与承载应用程序的实际服务器密切相关的应用程序子网。

*应用程序子网*收集某一服务器 IP 地址范围的数据，其子网掩码可能比现有服务器子网更宽或更窄。通过将应用程序子网分配给多个应用程序可以重复使用该应用程序子网。

建议将服务器子网或应用程序子网分配给应用程序。当您的服务器管理员使用连续 IP 范围配置应用程序服务器时，此方法的效果最好。请勿将服务器分配给应用程序。如果主机资源更改，则必须更新应用程序的服务器分配，以继续监视该应用程序。

分配：

- 域

  使管理控制台能够将域中的所有匹配服务器自动分配给应用程序，并使得应用程序服务器分配在服务器子网更改时保持最新。

  如果未创建域来分隔通信，则分配默认域将分配管理控制台监视的所有服务器。

- 现有服务器子网或应用程序子网指定的服务器 IP 地址的范围。

  例如，如果已将管理控制台配置为使用与服务器 VLAN 定义密切相关的服务器子网来监视服务器，则可将同一服务器子网分配给应用程序。

- 新应用程序子网。

  例如，如果您有一个现有 /22 服务器子网，但对于特定应用程序，您知道其 /26 服务器子网定义，则可创建 /26 应用程序子网并将其分配给该应用程序。

- 服务器。

  可从“服务器列表”中分配服务器，或添加新服务器。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. （可选）选择域来筛选可用服务器子网和服务器的列表。

4. 滚动到“应用程序列表”，选择应用程序，然后单击“编辑”。

   将打开“应用程序属性”。

5. 单击“分配”将服务器分配给应用程序。

   有关为应用程序分配服务器的信息，请单击“帮助”。

6. （可选）取消选择服务器子网、应用程序子网或服务器，以取消分配它。请注意，当应用程序子网未分配给任何应用程序时，控制台会自动删除该应用程序子网。

7. 如果已启用应用程序可用性监视，并且负载平衡器在服务器之间分布应用程序通信量，那么要使管理控制台检查服务器可用性，请指定必须可用的服务器的数目。

8. 单击“确定”。

   如果已禁用“确定”按钮，请确保已向该应用程序分配服务器或子网，然后单击“属性”确认已正确指定应用程序属性。

9. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
检查服务器可用性 (p. 190)

编辑用户定义的应用程序

编辑用户定义的应用程序的属性，例如，将 URL 添加到 Web 应用程序中。

如果同时编辑多个应用程序，则可指定通用应用程序属性，如可用性监视。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. （可选）选择域来筛选可用服务器子网和服务器的列表。
4. 滚动到“应用程序列表”，并选择要编辑的应用程序，然后单击“编辑”。

   如有必要，则单击“重置列表”从“应用程序列表”中删除任何选择。
5. 单击“属性”以编辑应用程序设置。

   有关应用程序属性的信息，请单击“帮助”。
6. 单击“分配”，以编辑应用程序的服务器分配，然后单击“确定”。

   有关为应用程序分配服务器的信息，请单击“帮助”。
7. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   如果您未收到提示，则对应用程序属性所做的更改不要求同步监视设备。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)

删除用户定义的应用程序

删除用户定义的应用程序，以将其从“应用程序列表”中删除，还可以创建端口排除，以防止管理控制台试图自动监视相应的应用程序端口。

在考虑要删除哪些应用程序时，请记住以下几点：

- 避免监视对时间不敏感的应用程序，如应用程序的响应时间不是那么关键的备份应用程序。
- 在监视设备和管理控制台上使用更多的系统资源来处理而不是筛选的且不是很关键的应用程序是可以删除的候选项。例如，备份应用程序可在环境中的所有客户端 IP 中生成通信，这会占用数据库中的很多行，并在每个监视设备上产生更高的负载。

在删除应用程序之后，根据数据库设置，现有数据将继续可用于报告用途。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. 如果已在 CA PC 或 CA NPC 中定义了域，则您不需要选择域。您对应用程序所做的任何更改都将应用到整个域。
4. 滚动到“应用程序列表”，从列表中选择应用程序，然后单击“删除”。

   管理控制台会提示您确认删除，并可以选择通过添加匹配端口排除来防止管理控制台自动监视应用程序。

   - 单击“删除”来删除应用程序，并允许管理控制台基于观测的应用程序通信量重新创建应用程序。
   - 单击“删除和添加端口排除”，以删除应用程序并创建端口排除规则，从而防止管理控制台基于观测的应用程序通信量重新创建应用程序。
5. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
编辑数据库存储首选项 (p. 203)

管理多层应用程序

使用管理控制台可查看多层应用程序中每层的网络、服务器和应用程序性能。*多层应用程序*是在多台服务器上运行的应用程序，服务器之间的通信由至少一台服务器执行 - 该服务器既充当客户端请求的服务器，又充当其他服务器的客户端。

详细信息：

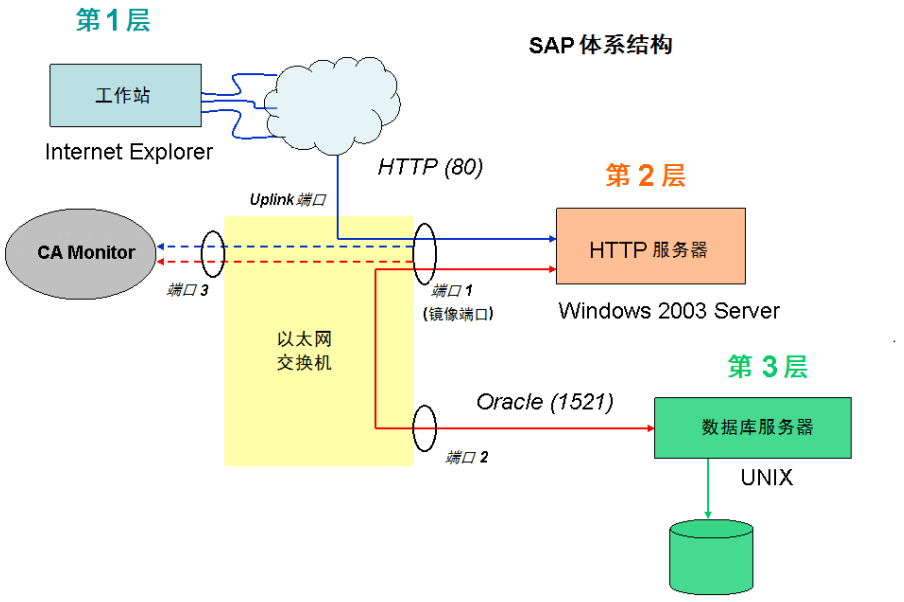
多层应用程序的工作方式 (p. 119)
如何监视多层应用程序 (p. 120)

多层应用程序的工作方式

考虑一个由以下层构成的 N 层 SAP 体系结构：

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

在多层应用程序中，至少有一个服务器同时充当其他应用程序服务器的服务器和客户端。在以上示例中，第 2 层是来自第 1 层的用户请求的服务器，同时是来自第 3 层服务器的请求的客户端。



将发生以下过程：

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

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

如何监视多层应用程序

通过完成以下步骤来配置管理控制台，以监视和报告 N 层应用程序体系结构：

- 将相关应用程序对话镜像到监视设备。
- 配置管理控制台以监视应用程序体系结构。

详细信息：

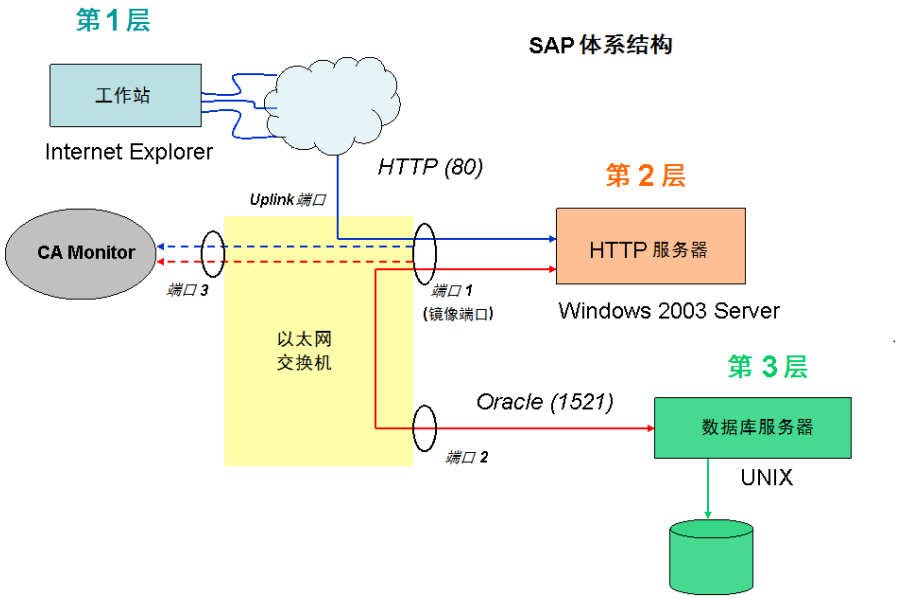
镜像应用程序对话的策略 (p. 121)

镜像应用程序对话的策略

要使管理控制台可以显示 N 层应用程序，必须将每层之间的主机对话镜像到监视设备。要启动此过程，请运行到服务器和监视设备连接的以太网交换机的镜像命令。镜像命令会使得进出各个主机的数据包被复制到监视设备。此复制功能对交换机的性能影响最小。

如果多层应用程序已被虚拟化，请考虑将“服务器到服务器”的通信量镜像到 ESX 主机上的虚拟交换机，并将前端服务器通信量镜像到物理监控。

下图描述了交换机端口镜像。



在具有两个以上服务器的复杂环境中，您可能需要镜像若干个端口，来捕获应用程序体系结构的所有层。请仔细选择此环境中要镜像的端口，以避免两次捕获同一对话。

详细信息：

监视设备推荐 (p. 232)

创建多层应用程序

要监视多层应用程序，请为每层创建一个应用程序，并遵循命名约定帮助您更轻松地标识并报告部分或全部层的情况。

遵循可促进管理、报告和分析的命名约定，以使管理控制台用户可以立即识别到每个应用程序层之间存在依赖关系。通常，标记为第 2 层的应用程序的性能依赖于标记为第 3 层的应用程序的性能。当分析第 2 层应用程序的性能时，请查看第 3 层应用程序的性能。

下表显示多层应用程序的示例。如果以此方式定义应用程序的每一层，则每个应用程序在管理控制台中将显示在一起。此方法显示应用程序体系结构的多个方面，并提醒您在应用程序和过程的各个元素之间存在依赖关系：

应用程序名称	开始端口	结束端口	端口方	关联服务器
SAP-HTTP-(80)-Tier 2	80	80	应用程序侦听这些端口	HTTP
SAP-Oracle-(1521)-Tier 3	1521	1521	应用程序侦听这些端口	Oracle

遵循这些步骤:

1. 将第 1 层客户端网络添加到“网络列表”中，并确保指定 24 位（或更高的）子网掩码。
2. 将参与应用程序层的所有服务器添加到“服务器列表”，并确认正确的监视器源与服务器关联。

   添加服务器时，会自动作为具有 32 位掩码的主机添加到“网络列表”中，这表示服务器像在 N 层体系结构中一样用作客户端。在前面的示例中，HTTP 服务器用作 Oracle 数据库服务器的客户端。
3. 将应用程序添加到管理控制台中。请遵循以下命名约定来命名 N 层应用程序：

   <ApplicationName>-<Protocol/Function>-(<TCPPort>)-<Tier#>

   其中变量定义如下：

   <ApplicationName>

   应用程序的名称。

   <Protocol/Function>

   在服务器上运行的应用程序后台进程。

   <TCPPort>

   后台进程端口号。

   <Tier#>

   层编号。
4. 重复这些步骤，以定义每个应用程序层。
5. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理客户端网络 (p. 27)
管理服务器 (p. 61)
管理用户定义的应用程序 (p. 106)

应用程序保持连接消息

在客户端和服务器之间交换的定期保持连接消息在 IP 网络中很常见，通过这些消息可以确定客户端是否仍处于活动状态或可访问状态。如果 TCP 保持连接符合 RFC 1122 中的标准，管理控制台通常会忽略这些消息并从字节计数和观测合计中排除任何关联的统计信息。

但是，某些应用程序的设计允许使用自定义的保持连接机制。如果来自客户端的响应是包含负载的确认，管理控制台会将客户端响应视为数据请求，并启动服务器响应时间 (SRT) 计时器。服务器通常会发出其他数据包，一旦保持连接计时器到期，便会导致 SRT 度量和 SRT 观测计数不准确。

使用保持连接的常见应用程序包括 Citrix 和 Microsoft Exchange。如果您怀疑其他应用程序正在发送保持连接消息，请在观测与 SRT 之间查找逆向关系，并在秒范围而非毫秒范围内查找 SRT 平均值。

CA Standard Monitor 或 CA Multi-Port Monitor 可以配置为按“服务器响应时间”筛选应用程序保持连接消息，以避免服务器度量标准出现偏差。

管理控制台使用 NRTT 观测来筛选使用应用程序保持连接的应用程序。如有必要，您可以调整 5 分钟间隔内最小 NRTT 观测数的阈值。

详细信息：

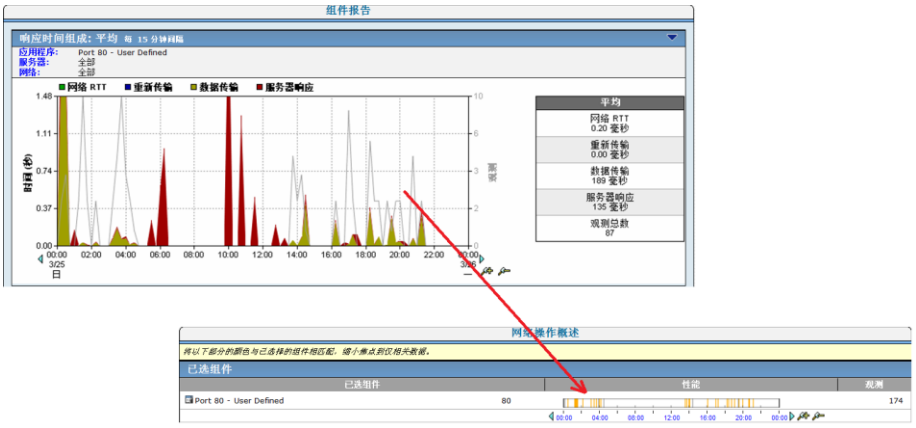
管理控制台设置 (p. 205)
筛选出保持连接消息 (p. 263)

第 6 章： 管理性能阈值

此部分包含以下主题：

性能阈值如何起作用

性能阈值可将“工程”页面上的高级趋势报告转换为“操作”页面上易于阅读的条形图报告。



性能阈值可帮助您识别性能问题，并允许管理控制台自动启动响应以便通知或调查问题。

阈值是每个系统和用户定义的应用程序存在的可接受的性能行为的边界。阈值的重要性在于：

- 使管理控制台能够分级数据。
- 参与突发事件创建和生成的突发事件响应及调查，从而可以及时排除故障和解决问题。

正确配置性能阈值后，会在条形图上显示相应的颜色来对应于真实的性能问题或度量标准下降。精确的阈值调整可使查明问题原因变成简单的颜色匹配。

黄色和橙色严重度指示符用于提醒用户注意“轻微”和“重大”程度的性能下降。建议校准阈值设置，以确保严重度指示符与导致网络用户提交帮助台票单的实际情况对应。

当管理控制台看到服务器或网络上的应用程序性能下降时，管理控制台会自动打开突发事件。*突发事件*包含在“突发事件”页面中，用于创建有关性能问题的信息记录。

在正确调整性能阈值设置后，选择管理控制台应如何响应网络和服务器突发事件，例如，通过在特定客户端网络上的应用程序性能下降时发送电子邮件通知。

详细信息：

管理突发事件响应 (p. 151)
突发事件的打开和关闭方式 (p. 134)

应用程序性能的分级方式

管理控制台通过观测应用程序的 TCP 事务和计算以下度量标准来分级应用程序的性能：

- 与应用程序通信的每个客户端网络的网络度量标准。如果网络度量标准的 5 分钟平均值超过阈值，并且管理控制台观测度量标准的次数为最小次数，则管理控制台会将客户端网络的相应 5 分钟间隔分级为“轻微”（黄色）或“重大”（橙色）并创建网络突发事件。
- 承载应用程序的每个服务器的服务器度量标准。如果服务器度量标准的 5 分钟平均值超过阈值，并且管理控制台观测度量标准的次数为最小次数，则管理控制台会将服务器的相应 5 分钟间隔分级为“轻微”（黄色）或“重大”（橙色）并创建服务器突发事件。
- 应用程序自身的综合度量标准，其中既包括网络度量标准又包括服务器度量标准。如果综合度量标准的 5 分钟平均值超过阈值，并且管理控制台观测度量标准的次数为最小次数，则管理控制台会将应用程序的相应 5 分钟间隔分级为“轻微”（黄色）或“重大”（橙色）。

  请注意，管理控制台不创建应用程序突发事件。然而，由于综合度量标准既包括网络度量标准，又包括服务器度量标准，所以管理控制台可以将服务器或网络分级为“轻微”（黄色）或“重大”（橙色），并分级对应用程序自身性能产生的相应影响。例如，如果服务器度量标准下降，管理控制台还可以将应用程序的综合度量标准分级为“轻微”。

要将性能数据分级为“正常”、“轻微”（黄色）或“重大”（橙色），管理控制台必须收集 2 个完整工作日的数据，从 GMT 午夜到下一个午夜计为一个工作日。例如，如果管理控制台在美国东部时间星期一下午 3:30 开始为服务器端口与客户端网络之间的 TCP 会话收集数据，则在美国东部时间星期三晚上 7:00 之前，管理控制台无法分级该网络上的应用程序性能。如果管理控制台未收集 2 个完整工作日的数据，则管理控制台会将服务器端口与客户端网络之间的 TCP 会话分级为“未分级”。

通过比较：

- 基准，通过“操作”页面上的“浏览”按钮提供，可为服务器上的应用程序端口与客户端网络之间的所有 TCP 会话报告历史准则。管理控制台在所有应用程序端口、服务器和客户端网络之间计算每小时基准，并跟踪一周中某天、月中某天和上周的活动。管理控制台使用基准来表示一天中该小时的性能条件何时为正常。管理控制台需要 2 个完整工作日的数据来计算基准。
- 运行水平协议 (OLA) 报告，从“管理”页面中提供，用于量化当前的性能和性能趋势。性能 OLA 通过按小时计算比特定阈值快的事务百分比来显示应用程序的执行情况。

详细信息：

管理应用程序性能 OLA (p. 175)
综合度量标准 (p. 130)
网络度量标准 (p. 129)
服务器度量标准 (p. 130)

性能度量标准的工作方式

以下各节介绍管理控制台用来分级应用程序性能的度量标准。如果应用程序由 Cisco WAAS 或 Riverbed Steelhead 进行 WAN 优化，则并非所有性能度量标准都适用于客户端、WAN 和服务器段。

管理控制台从标准 TCP 事务中计算以下度量标准：

- 网络度量标准
- 服务器度量标准
- 综合度量标准

网络度量标准

网络度量标准表示应用程序性能问题由与应用程序通信的网络引起。

网络往复传输时间

数据包在网络上的服务器和客户端之间经过所花的时间（不包括丢失）。不包括应用程序、服务器以及客户端处理时间。

网络连接时间

是服务器发送的 SYN-ACK 与接收的从客户端返回的 ACK 之间的时间量。在网络未被阻塞时，它是对网络延迟的一种度量，表示由于距离和序列化产生的最小延迟，也是网络体系结构中最佳的往复传输时间。

该值的突发峰值通常是由于网络拥塞引起的，而停滞（上升后停止不动）通常意味着路径更改。

有效网络往复传输时间

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

重传延迟

是原始数据包发送与上一个重复数据包发送之间所花的时间。管理控制台报告的“重传延迟”是整个观测的平均值，而不仅仅是针对重传的数据包。如果一整套 10 个数据包需要 300 毫秒重传时间，则报告的重传延迟为 30 毫秒（300 毫秒/10 个数据包）。

服务器度量标准

表示应用程序性能问题是由承载应用程序的服务器引起的。

服务器响应时间

表示服务器向客户端请求发送初始响应所需的时间，或初始服务器的“思考时间”。“服务器响应时间”增大通常意味着：

- 服务器资源（如 CPU、内存、磁盘或 I/O）不足
- 写入应用程序的性能不佳
- 多层应用程序中执行效果较差的层

服务器连接时间

表示服务器确认初始客户端连接请求所需的时间，确认方法是发送 Syn-Ack 来响应客户端的 SYN 数据包。

被拒绝会话百分比

表示服务器在三次握手 (请参阅本页中的定义 388)期间显式拒绝的连接请求的百分比。“未实现的 TCP/IP 会话请求”报告的一部分。

无响应会话百分比

表示发送连接请求但服务器从不响应的会话的百分比。“未实现的 TCP/IP 会话请求”报告的一部分。

综合度量标准

表示应用程序性能问题是由承载该应用程序的服务器以及与该应用程序通信的网络引起的。

事务处理时间

表示将从第一次响应（服务器响应时间结束）中测到的完整应用程序响应传送至该请求中的最后一个数据包所用的时间，应用程序的设计、服务器或网络的性能会影响此时间。

管理控制台在“工程”页面上的“响应时间组成: 平均”报告中显示这些类型的响应时间数据。当超出“事务时间”阈值时，管理控制台不会新开一个突发事件。

数据传输时间

表示在服务器开始响应与它完成发送数据之间所花的时间。响应大小、网络中的可用带宽以及应用程序和网络之间的交互等因素会影响该值。

当超出“数据传输时间”阈值时，管理控制台不会新开一个突发事件。

用于自定义性能阈值的选项

按照以下步骤指定性能阈值：

- 输入敏感度级别。管理控制台会根据敏感度级别动态生成阈值。
- 以毫秒为单位输入静态值或指定百分比
- 禁用度量标准阈值

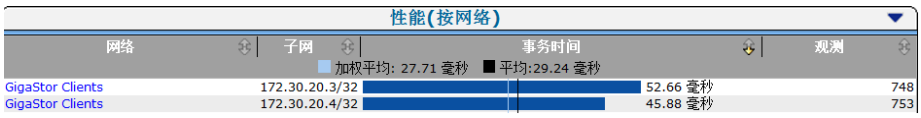
默认情况下，会启用“敏感度”选项。无论使用哪种方法，阈值总是包括最小观测数的值。*观测*是管理控制台通过 TCP 事务计算度量标准的机会。要将度量标准的性能分级为“正常”、“轻微”（黄色）或“重大”（橙色），监视设备必须看到最小数量的观测数。

当分级网络、服务器或应用程序的性能时，也可以选择不包括特定度量标准。

敏感度级别（动态值）

当指定敏感度级别时，管理控制台会在格林尼治标准时间的每个午夜自动为度量标准生成一个新阈值，同时使用过去 30 天的百分位统计信息确定适当设置。对于从每个客户端网络访问应用程序的用户，管理控制台会生成一组单独的阈值。

因此，管理控制台不对高延迟的远程链路中的用户与本地 LAN 中用户应用相同的阈值，并且从历史记录中来看阈值表示极端性能。例如，考虑位于迈阿密的数据中心的应用程序服务器，其用户有的从本地访问应用程序，有的通过德国慕尼黑的远程站点访问应用程序。



如果使用敏感度级别来设置此应用程序的性能阈值，管理控制台会为从每个客户端网络访问此应用程序的用户生成一组单独的阈值。指定敏感度级别还意味着，您不需要通过将同一应用程序定义两次（如慕尼黑的 Exchange 和迈阿密的 Exchange）来为远程位置的应用程序性能设置不同阈值。

当提高阈值的敏感度时，会降低阈值，以便根据性能级别接收更多突发事件。管理控制台敏感度阈值与疼痛敏感度相似。敏感度高的人的疼痛阈值较低，大声呼喊的频率较高。敏感度低的人可以忍受更多疼痛，大声呼喊的可能性大大降低。

敏感度的值可从 0（不敏感）调节为 200（非常敏感）。

- 敏感度设置为 200 时，会将超过第 75 个百分位的通信量度量分级为“轻微”（黄色）或“重大”（橙色）。
- 低敏感度设置会生成较高阈值，并导致突发事件较少。

在管理控制台重新计算阈值时，敏感度不会更改。要查看当天的敏感度级别值，请使用敏感度计算器。

详细信息：

从管理页面编辑阈值 (p. 138)

静态阈值（静态值）

通过选择“毫秒”或“百分比”阈值设置可为特定度量标准指定静态阈值。除非您更改它，否则此值不会更改。

静态阈值可用于为高度一致或具有与较差性能对应的已知值的度量标准定义目标值。例如，运行状况良好的服务器不应拒绝来自客户端的会话请求，因此为“轻微”（黄色）设置 1% 拒绝的静态阈值，为“重大”（橙色）设置 3% 拒绝的静态阈值，可防止管理控制台忽略频繁拒绝会话的服务器上的服务器问题。

适用于静态阈值的其他度量标准有：

- 无响应的会话。在运行状况良好的服务器上应为零。将低阈值 5 设置为 10%。
- 服务器连接时间。应为亚毫秒。只要管理控制台正在应用程序服务器所在的同一交换机上收集数据，便设置为在 2 到 5 毫秒时报警。

使用“毫秒”或“百分比”静态值设置还意味着，不再按网络或服务器自动分隔阈值。为了解决此问题，您必须按网络类型对具有相似延迟的网络分组，然后为每个网络类型分配一组自定义阈值。

在为给定应用程序配置静态阈值之前，可在“工程”页面中查看报告，并使用“设置”按钮选择相关度量标准。在未事先记录度量标准和更正任何基础问题之前，务必不要在永久下降的阈值水平设置任何服务器、网络或应用程序。

详细信息：

添加性能阈值 (p. 141)

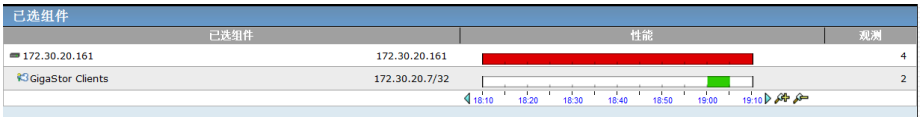
突发事件的打开和关闭方式

当网络或服务器度量标准的 5 分钟平均值超过阈值时，管理控制台将打开网络和服务器突发事件。

在以下情况下，管理控制台将自动关闭突发事件：

- 性能达到可接受程度已过 24 小时。
- 与网络或服务器突发事件关联的服务器进入维护周期。请注意，在排定的维护期间结束后，如果仍然存在性能问题，管理控制台可以打开新突发事件。
- 突发事件超过了 24 小时。请注意，如果性能问题仍然存在，管理控制台将打开新突发事件。

您也可以确认突发事件，以指明您已知道此问题。在下面的示例中，管理控制台在早上 7:05 打开 191.168.1.0/24 网络上的网络突发事件。在早上 7:20 之后，没有后续的网络阈值违反，因此管理控制台在上午 9:00 关闭该突发事件。请注意，由于管理控制台在整点关闭突发事件，因此当您确认突发事件时，报告也标记该突发事件之前的小时（整点，此示例中为早上 7:00），以显示突发事件的时间范围：



如果您已为可用性设置 OLA，管理控制台将在应用程序被分级为“不可用”时打开服务器突发事件。

详细信息：

管理应用程序可用性 (p. 185)
排定服务器维护 (p. 79)
应用程序性能的分级方式 (p. 127)

NetQoS Performance Center (CA NPC)

在 CA NPC 中将管理控制台注册为数据源后，管理控制台看到新的“轻微”（黄色）或“重大”（橙色）状况时，管理控制台将开出突发事件，CA NPC 也将开出相应的事件。

- 如果触发 CA Application Delivery Analysis 突发事件的“轻微”或“重大”情况显示整整一小时内性能都正常，管理控制台将关闭该突发事件，事件管理器也将清除相应的事件。之后，如果又出现了“轻微”或“重大”突发事件状况，管理控制台将*开出*一个新的突发事件，CA NPC 也将开出相应的事件。
- 如果管理控制台突发事件打开了长达 24 小时，则不管情况如何，管理控制台都将自动关闭该突发事件。如果“轻微”或“重大”突发事件状况仍存在，管理控制台将新开一个突发事件，CA NPC 也将增加相应事件的计数。否则，在大约 10 分钟的同步延迟之后，CA NPC 将清除该事件。

要使 CA NPC 能够清除与服务器脱机的 CA Application Delivery Analysis 突发事件关联的事件，管理控制台必须在整整一小时内对“轻微”或“重大”突发事件状况均报告“没有数据”，事件管理器才能清除相应的事件。如果管理控制台在服务器恢复联机后看到新的“轻微”或“重大”状况，管理控制台将开出突发事件，CA NPC 也将开出相应的事件。

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

CA Performance Center (CA PC)

在 CA PC 上将管理控制台注册为数据源后，CA Application Delivery Analysis 突发事件将显示在 CA PC 中，并由 CA Application Delivery Analysis 管理控制台进行管理。CA PC 不确认或关闭 CA Application Delivery Analysis 事件。

CA PC 的“性能事件”页面将列出 CA Application Delivery Analysis 突发事件，并按照服务器和网络显示突发事件计数。在该页面中，您可以单击某个 CA Application Delivery Analysis 突发事件，以深入到 CA Application Delivery Analysis 管理控制台查看突发事件详细信息并确认该突发事件：

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

要使 CA PC 能够清除服务器脱机的 CA Application Delivery Analysis 突发事件，CA Application Delivery Analysis 必须在整整一小时内对“轻微”或“重大”突发事件状况均报告“没有数据”。如果管理控制台在服务器恢复联机后看到新的“轻微”或“重大”状况，管理控制台将开出突发事件，并且 CA PC 将列出相应的突发事件并增加其突发事件计数。

编辑性能阈值

通过性能阈值，管理控制台能够对性能分级并生成突发事件。如有必要，可以针对跨某组客户端网络或所有客户端网络的应用程序设置更紧或更松的性能阈值。

通过按网络类型自定义性能阈值来自定义网络突发事件响应。

使用“性能阈值列表”管理每个网络的性能阈值列表。在下面的示例中，DCOM Service Control Manager 应用程序对分别属于“奥斯汀”和“圣地亚哥”网络类型的客户端网络就具有自定义阈值。管理控制台使用“默认”网络类型中的性能阈值来监视未分配有网络类型的任何客户端网络上的应用程序性能。

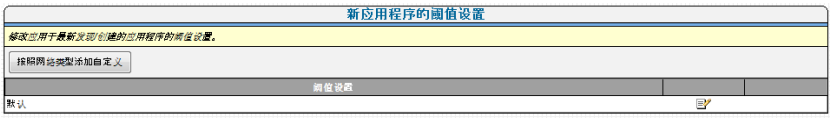

性能阈值列表

应用程序	TCP 端口	网络类型	数据段	
HTTP Alternate	8080	默认	否	
Microsoft SQL Monitor	1434	默认	否	
Microsoft SQL Server	1433	默认	是	
MySQL	3306	默认	否	
Port 80 - User Defined	80	默认	是	
Undernet Internet 中继聊天	6667	默认	是	
安全 NNTP	563	默认	否	
安全超文本传输协议	443	默认	否	
超文本传输协议	80	默认	是	
电子邮局协议 v3	110	默认	否	

1 / 3　　页: 1　大小: 10

使用“新应用程序的阈值设置”列表可管理对新应用程序所应用的性能阈值。

您还可以为特定网络类型创建阈值，以便在创建或发现应用程序时，自动对该网络上的应用程序应用自定义的阈值。例如，对于通过 VPN 访问的应用程序，可对网络响应时间脱敏或禁用性能阈值。默认情况下，所有新应用程序使用为该网络类型建立的性能阈值集。


新应用程序的阈值设置

修改应用于最新发现/创建的应用程序的阈值设置。

按照网络类型添加自定义

阈值设置		
默认		

从管理页面编辑阈值

编辑性能阈值，以便：

- 为所有关联的客户端网络设置公共阈值。例如，可以为所有客户端网络上的应用程序调整服务器度量标准。

  通常，服务器应以相同方式处理其所有客户端请求。

- 为与一组客户端网络通信的所有应用程序设置公共阈值。例如，可为与属于“奥斯汀”网络类型的客户端网络通信的所有应用程序调整网络度量标准。

如果在分级应用程序、服务器或网络时不希望管理控制台包括某一度量标准，则可禁用该度量标准。如果禁用某一度量标准，管理控制台将使用可用的度量标准来分级应用程序、服务器或网络。

要防止管理控制台分级应用程序的性能，请对应用程序禁用所有网络、服务器和综合度量标准。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“性能阈值”。
3. 滚动到“性能阈值列表”，找到所需应用程序的性能阈值，然后单击 进行编辑。所做的更改会应用到具有已分配网络类型的所有客户端网络。

   将打开“编辑应用程序阈值”。
4. 在要编辑的度量标准上单击“更改”。
5. 为“轻微”和“重大”突发事件自定义度量标准阈值：
   - 选择度量阈值的方法，然后指定阈值。
   - 在“最小观测数”下，指定 5 分钟间隔内的最小观测数或管理控制台必须计算度量标准的次数。例如，管理控制台可对每个 TCP 事务计算一次“服务器连接时间”，但每当客户端/服务器对交换数据包时，管理控制台都会计算 NRTT。如果管理控制台计算度量标准的次数未达到指定的最小次数，那么对该 5 分钟间隔而言，度量标准的状态将为“未分级”。

   有关设置阈值属性的信息，请单击“帮助”。
6. 单击“应用”。
7. 对其他度量标准重复这些步骤来编辑其“轻微”或“重大”阈值。
8. 单击“确定”。

详细信息：

性能度量标准的工作方式 (p. 128)

从操作页面编辑阈值

通过“操作”页面上的“浏览”按钮，管理控制台管理员或网络操作员可为特定的度量标准更改阈值。要从“操作”页面中更改阈值，可通过选择客户端网络、服务器、应用程序和度量标准来隔离问题。然后，单击“浏览”来编辑选定度量标准的阈值。

如果已为选定的网络分配网络类型，则对性能阈值所做的编辑会应用到属于该网络类型的所有客户端网络。例如，如果更改销售应用程序中的 NRTT 阈值，并且您已选择属于伦敦网络类型的客户端网络，则阈值更改将应用于分配给伦敦网络类型的所有客户端网络。

注意：有关“浏览”按钮的详细信息，请参阅*《用户指南》*。

遵循这些步骤:

1. 单击“操作”页面。
2. 单击“设置”。
3. 将打开“设置”对话框。
4. 选择所需的客户端网络、服务器、应用程序和度量标准。

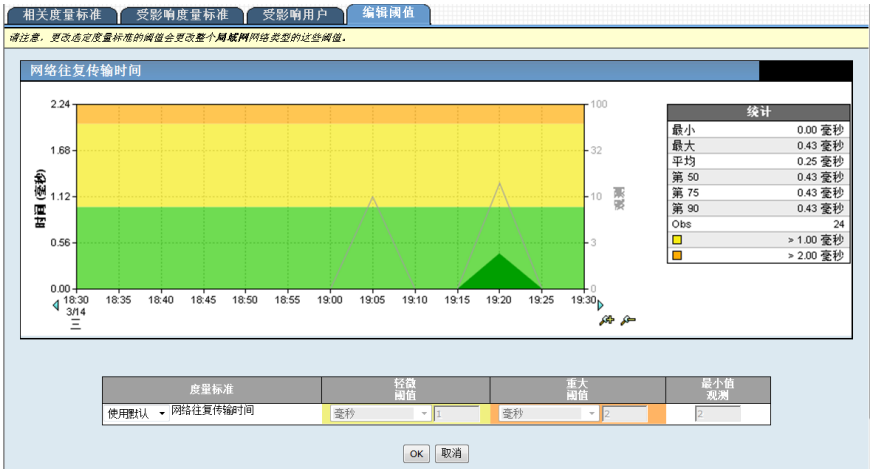
   有关指定报告设置的信息，请单击“帮助”。
5. 单击“浏览”。

   将打开“度量标准详细信息”。

6. 单击“编辑阈值”选项卡。

   如果已为选定的网络分配网络类型，则对性能阈值所做的编辑会应用到属于该网络类型的所有客户端网络。

   在以下示例中，将 NetQoS LAN 网络分配给了 T1 网络类型。对 NRTT 的 LDAP [客户端] 应用程序性能阈值所做的更改将应用到分配给 T1 网络类型的所有网络。



7. 编辑性能度量标准，以指定所需的“轻微”和“重大”阈值以及“最小观测数”。

8. 单击“确定”。

详细信息：

从管理页面编辑阈值 (p. 138)

添加性能阈值

为一组特定网络上的用户定义的应用程序设置更紧或更松的性能阈值。要执行此操作，请按网络类型自定义应用程序的性能阈值。

先决条件：分配网络类型以便定义网络组。通过网络类型，可以将默认性能阈值添加到一组网络。

要针对一组网络使用自定义的一组阈值来自动监视新应用程序，需为新应用程序创建性能阈值。

或者，您可以编辑应用程序的默认阈值设置。该默认阈值设置将应用到所有未分配网络类型的网络。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“性能阈值”。
3. 滚动到“性能阈值列表”。
4. 单击“按照网络类型添加自定义”。

   将打开“按网络类型自定义阈值”。
5. 指定要为其定义性能阈值的用户定义的应用程序和网络类型，然后单击“确定”。

   将打开“编辑应用程序阈值”。
6. 按网络类型为应用程序自定义性能阈值，然后单击“应用”。
7. 单击“确定”。

详细信息：

按网络类型对客户端网络分组 (p. 45)
编辑性能阈值 (p. 137)
为一组网络启用默认性能阈值 (p. 142)

为一组网络启用默认性能阈值

将默认性能阈值添加到一组网络，以便为该组网络上新发现的应用程序设置更紧或更松的性能阈值。该阈值会自动应用到新的系统或用户定义的应用程序。

启用默认阈值之后，仅会对新应用程序应用它们。现有应用程序会保留其性能阈值。使用“向我显示”菜单中“数据监视”、“应用程序”下的“应用程序列表”，可批量编辑现有应用程序的性能阈值。

先决条件：分配网络类型以便定义网络组。通过网络类型，可以将默认性能阈值添加到一组网络。

如果应用程序已存在，请针对一组网络为该应用程序添加性能阈值。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“性能阈值”。
3. 滚动到“新应用程序的阈值设置”列表。
4. 单击“按照网络类型添加自定义”。

   将打开“按网络类型自定义阈值”。
5. 选择所需网络类型，然后单击“确定”。

   将打开“编辑应用程序阈值”。
6. 按网络类型自定义应用程序的性能阈值。

   有关设置性能阈值的信息，请单击“帮助”。
7. 单击“应用”。

   指定的性能阈值会应用到已分配网络类型的客户端网络上新发现的所有应用程序。
8. 单击“确定”。

详细信息：

编辑用户定义的应用程序 (p. 117)
编辑系统定义的应用程序 (p. 104)

编辑 WAN 优化网段的性能阈值

管理控制台会创建不同的应用程序，来报告网络的优化客户端、WAN 和服务器段的应用程序性能。自定义每个网段的性能阈值，以提高或降低管理控制台对应用程序性能变化的敏感度。还要为非优化的应用程序通信量指定性能阈值。

为优化应用程序中的非优化通信量编辑阈值

编辑每个网段的性能阈值时，还可以编辑针对管理控制台观测到的未经优化的所有应用程序通信量的阈值。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“性能阈值”。
3. 滚动到“性能阈值列表”。
4. 单击 来编辑 WAN 优化应用程序。

   “数据段”列标识了 WAN 优化应用程序。如果管理控制台已按网段观测到了优化的应用程序通信量，“数据段”列状态为“是”。
5. 在第三个“向我显示”菜单中单击“阈值”。

   如果管理控制台未从非优化的应用程序通信量中计算响应时间度量标准，则不显示“阈值”命令。

   将打开“编辑应用程序阈值”。
6. 自定义“轻微”（黄色）和“重大”（橙色）突发事件的度量标准阈值：
   - 选择度量阈值的方法，然后指定阈值。
   - 在“最小观测数”下，指定 5 分钟间隔内的最小观测数或管理控制台必须计算度量标准的次数。如果管理控制台计算度量标准的次数未达到指定的最小次数，那么对该 5 分钟间隔而言，度量标准的状态将为“未分级”。

   有关设置阈值属性的信息，请单击“帮助”。
7. 单击“应用”。
8. 重复这些步骤，以便为其他度量标准设置阈值。
9. 单击“确定”。

详细信息：

从管理页面编辑阈值 (p. 138)

为优化的客户端段编辑阈值

对于 WAN 优化的应用程序，需针对每个网段编辑其性能阈值。

管理控制台从客户端段中计算以下度量标准：

网络往复传输时间

度量数据包在网络上的服务器和客户端之间经过所花的时间（不包括丢失）。不包括应用程序、服务器以及客户端处理时间。

重传延迟

度量“网络往复传输时间”中由于重传引起的其他延迟。显示的数据是跨整个观测的平均值，而不是每个事务的实际重新传输时间。

事务处理时间

度量从客户端发送请求（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之间经过的时间。

管理控制台在“工程”页面上的“响应时间组成: 平均”报告中显示这些类型的响应时间数据。当超出“事务时间”阈值时，管理控制台不会新开一个突发事件。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“性能阈值”。
3. 滚动到“性能阈值列表”。
4. 单击 来编辑 WAN 优化应用程序。“数据段”列标识了 WAN 优化应用程序。如果管理控制台已按网段观测到了优化的应用程序通信量，“数据段”列状态为“是”。
5. 在第三个“向我显示”菜单中单击“客户端段”。

   如果管理控制台未从“客户端段”计算响应时间度量标准，则不显示“客户端段”命令。

   将打开“客户端段阈值”。
6. 自定义每个响应时间度量标准的性能阈值，即（轻微（黄色）和重大（橙色）：
   - 选择度量阈值的方法，然后指定阈值。
   - 在“最小观测数”下，指定 5 分钟间隔内的最小观测数或管理控制台必须计算度量标准的次数。如果管理控制台计算度量标准的次数未达到指定的最小次数，那么对该 5 分钟间隔而言，度量标准的状态将为“未分级”。

   有关设置阈值属性的信息，请单击“帮助”。

7. 单击“应用”。
8. 对其他度量标准重复这些步骤来编辑其阈值。
9. 单击“确定”。

详细信息：

从管理页面编辑阈值 (p. 138)

为优化的 WAN 段编辑阈值

对于 WAN 优化的应用程序，需针对每个网段编辑其性能阈值。

管理控制台从 WAN 段中计算以下度量标准：

网络往复传输时间

度量数据包在网络上的服务器和客户端之间经过所花的时间（不包括丢失）。不包括应用程序、服务器以及客户端处理时间。

网络连接时间

度量客户端确认服务器的连接确认所需的时间。延迟可能由网络延迟引起。

有效往复传输时间

包括网络往复传输时间和由重传引起的延迟。为此度量标准设置阈值，以监视由于重传而引起的性能下降。

重传延迟

度量“网络往复传输时间”中由于重传而引起的其他延迟。显示的数据是跨整个观测的平均值，而不是每个事务的实际重新传输时间。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“性能阈值”。
3. 滚动到“性能阈值列表”。
4. 单击 来编辑 WAN 优化应用程序。“数据段”列标识了 WAN 优化应用程序。如果管理控制台已按网段观测到了优化的应用程序通信量，“数据段”列状态为“是”。
5. 在第三个“向我显示”菜单中单击“WAN 段”。

   如果管理控制台未从 WAN 网段中计算响应时间度量标准，则不显示“WAN 段”命令。

   将打开“WAN 段阈值”。
6. 自定义“轻微”（黄色）和“重大”（橙色）突发事件的度量标准阈值：
   - 选择度量阈值的方法，然后指定阈值。
   - 在“最小观测数”下，指定 5 分钟间隔内的最小观测数或管理控制台必须计算度量标准的次数。如果管理控制台计算度量标准的次数未达到指定的最小次数，那么对该 5 分钟间隔而言，度量标准的状态将为“未分级”。

   有关设置阈值属性的信息，请单击“帮助”。

7. 单击“应用”。
8. 对其他度量标准重复这些步骤来编辑其“轻微”或“重大”阈值。
9. 单击“确定”。

详细信息：

从管理页面编辑阈值 (p. 138)

为优化的服务器段编辑阈值

对于 WAN 优化的应用程序，需针对每个网段编辑其性能阈值。

管理控制台从服务器段中计算以下度量标准：

服务器响应时间

度量服务器开始响应客户端请求所花费的时间。此值受服务器速度、应用程序设计和请求数据量影响。

服务器连接时间

度量服务器确认初始客户端连接请求所需的时间。

被拒绝会话百分比

度量在三次握手期间被服务器显式拒绝的连接请求的百分比。“未实现的 TCP/IP 会话请求”报告的一部分。

无响应会话百分比

度量发送连接请求且客户端或服务器未响应的会话的百分比。“未实现的 TCP/IP 会话请求”报告的一部分。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“性能阈值”。
3. 滚动到“性能阈值列表”。
4. 单击 来编辑 WAN 优化应用程序。“数据段”列标识了 WAN 优化应用程序。如果管理控制台已按网段观测到了优化的应用程序通信量，“数据段”列状态为“是”。
5. 在第三个“向我显示”菜单中单击“服务器段”。

   如果管理控制台未从服务器网段中计算响应时间度量标准，则不显示“服务器段”命令。

   将打开“服务器段阈值”。
6. 自定义“轻微”（黄色）和“重大”（橙色）突发事件的度量标准阈值：
   - 选择度量阈值的方法，然后指定阈值。
   - 在“最小观测数”下，指定 5 分钟间隔内的最小观测数或管理控制台必须计算度量标准的次数。如果管理控制台计算度量标准的次数未达到指定的最小次数，那么对该 5 分钟间隔而言，度量标准的状态将为“未分级”。

   有关设置阈值属性的信息，请单击“帮助”。
7. 单击“应用”。

8. 对其他度量标准重复这些步骤来编辑其阈值。
9. 单击“确定”。

详细信息：

从管理页面编辑阈值 (p. 138)

第 7 章： 管理突发事件响应

此部分包含以下主题：

突发事件响应的工作方式

为帮助您在问题发生时排除问题并缩短平均修复时间，请将突发事件响应分配给关键业务应用程序、服务器和网络。突发事件响应：

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

默认情况下，管理控制台不会自动启动突发事件响应。

请注意，您还可以从“突发事件”页面中手动启动调查，以进一步排除突发事件故障。有关详细信息，请参阅*《用户指南》*。

突发事件响应的启动方式

当管理控制台查看网络或服务器度量标准的阈值违反时，管理控制台会自动打开网络或服务器突发事件。从“突发事件”页面中，可通过*突发事件*创建有关服务器或网络（包括受影响的应用程序）中的性能问题的信息记录。

当管理控制台打开以下对象的突发事件时：

- 对于服务器，管理控制台将评估服务器突发事件，并对受影响的服务器以及该服务器中运行的性能较差的应用程序启动一组操作。
- 对于网络，管理控制台将评估网络突发事件，并对该网络以及网络中运行的性能较差的应用程序启动一组操作。

虽然管理控制台使用综合度量标准分级应用程序的性能，但管理控制台不创建应用程序突发事件。但是，管理控制台允许您定义应用程序突发事件响应。*应用程序突发事件响应*是应用程序对网络或服务器突发事件的响应。例如，如果为 Exchange 应用程序配置了应用程序突发事件响应，则管理控制台将在以下情况下启动突发事件响应：

- 访问 Exchange 应用程序的客户端创建了一个网络突发事件
- 承载应用程序的服务器创建了一个服务器突发事件

超出某个综合度量标准（如数据传输时间）的阈值时，管理控制台不会启动应用程序突发事件响应。

默认情况下，管理控制台不会针对网络或服务器突发事件启动通知或调查。编辑默认突发事件响应，以添加一个或多个操作，并根据需要创建其他突发事件响应。

网络突发事件响应

为了响应网络突发事件而启动网络突发事件响应。对于网络突发事件，可以做出以下响应：

- 电子邮件通知 (p. 154)
- SNMP 陷阱通知 (p. 155)
- 跟踪路由调查 (p. 160)

服务器突发事件响应

为了响应服务器突发事件而启动服务器突发事件响应。以下响应可用于服务器突发事件：

- 电子邮件通知 (p. 154)
- SNMP 陷阱通知 (p. 155)
- ping 响应时间调查 (p. 159)
- 通过 SNMP 的性能调查 (p. 158)
- 数据包捕获调查 (p. 157)

应用程序突发事件响应

为了响应网络或服务器突发事件而启动应用程序突发事件响应。可提供以下应用程序响应：

- 电子邮件通知 (p. 154)
- SNMP 陷阱通知 (p. 155)
- 应用程序连接时间调查 (p. 156)

  请注意，管理控制台不会因为响应被分级为“不可用”的应用程序而启动此调查。
- 数据包捕获调查 (p. 157)

详细信息：

针对应用程序可用性的服务器突发事件的工作方式 (p. 187)

电子邮件通知

电子邮件通知可向用户更新受影响的应用程序、服务器或网络的状态。

管理控制台将电子邮件通知发送到 CA PC 指定的 SMTP 服务器。否则，管理控制台将电子邮件通知发送到 CA Application Delivery Analysis 控制台设置指定的 SMTP 服务器。CA NPC 电子邮件规范用于从 CA NPC 发送排定或特别报告。管理控制台不使用 CA NPC 中配置的 SMTP 服务器发送电子邮件通知。

要在同一电子邮件中包括多个应用程序、服务器或网络，请将相同的突发事件响应分配给多个应用程序、服务器或网络类型。

如果分配的服务器或网络满足突发事件的“持续时间”和“严重度”条件，管理控制台将在管理控制台每隔两小时发送的状态更新电子邮件中包含此信息。

编辑“持续时间”和“严重性”阈值，以发送有关以下内容的电子邮件通知：

- 偶尔短时间发生的轻微的性能下降。可能会发生某些状况，因此您应该监视。
- 持续 10 分钟的“重大”性能下降或持续 5 分钟的“不可用”条件。您应该立即调查这些类型的情况。

详细信息：

管理控制台设置 (p. 205)
应用程序可用性报告的工作方式 (p. 187)

SNMP 陷阱通知

使用 SNMP 陷阱通知可向 SNMP 管理器更新受影响的应用程序、服务器或网络的“未结”或“已关闭”突发事件状态。

您可以为任意突发事件响应分配 SNMP 陷阱。管理控制台从管理控制台计算机发送 SNMPv2 陷阱通知。

与电子邮件通知不同，管理控制台在管理控制台执行以下操作时发送 SNMP 陷阱：

- 打开和关闭服务器或网络突发事件
- （可选）服务器或网络突发事件的严重度发生更改，例如，从“轻微”更改为“重大”。

要在同一 SNMP 陷阱中包括多个应用程序、服务器或网络，请将相同的突发事件响应分配给多个应用程序、服务器或网络类型。如果不止一个应用程序、服务器或网络受影响，SNMP 陷阱将包含一个 URL，您可以通过它来查看详细信息。

默认情况下，管理控制台使用名为 *SuperAgent* 的 SNMPv2 团体发送 SNMP 陷阱。默认的 SNMP 配置文件仅适用于 SNMP 陷阱通知。

为了让 SNMP 管理器理解来自管理控制台的 SNMP 陷阱通知，可将管理控制台 MIB 编译到 SNMP 管理器上的陷阱接收器中。编译方法根据 SNMP 管理器的不同而有所不同。

管理控制台分发中不包括管理控制台 MIB。从 CA Support 网站 (http://support.ca.com) 下载 CA Application Delivery Analysis MIB。

CA Application Delivery Analysis 陷阱通知将以下缩写用于性能度量标准。

缩写	度量标准
ERTT	有效往复传输时间
NCT	网络连接时间
NRTT	网络往复传输时间
RS	拒绝的会话（百分比）
RTNS	重传延迟
SCT	服务器连接时间
SRT	服务器响应时间

缩写	度量标准
US	无响应的会话（百分比）

详细信息：

解释 SNMP 陷阱 (p. 173)

应用程序连接时间调查

使用应用程序连接时间调查可收集有关连接到 TCP/IP 应用程序端口所需时间的信息。这包括服务器通过连接确认来响应的时间。

可以将应用程序连接时间调查分配给应用程序突发事件响应。如果承载应用程序的服务器由 CA Standard Monitor 监视，管理控制台将从监视设备中启动该调查。否则，将从管理控制台中启动调查。

请注意，管理控制台不会因为响应“不可用”应用程序而启动此调查。

管理控制台管理员也可以从“突发事件”页面启动或排定该调查。有关详细信息，请参阅*《用户指南》*。

应用程序连接时间调查会生成有关成功和不成功尝试次数以及连接时间的报告。

详细信息：

针对应用程序可用性的服务器突发事件的工作方式 (p. 187)

数据包捕获调查

使用数据包捕获调查，可以有筛选地捕获那些遇到问题的特定服务器、应用程序端口和网络。

您可以将数据包捕获调查分配给应用程序来响应服务器突发事件，或者分配给服务器以及服务器上运行性能较差的应用程序。管理控制台将自动从适当的监视设备中进行数据包捕获。如果数据包捕获的执行者为：

- CA Standard Monitor，捕获文件将在 TCP-8080 上从监视设备复制到用户的计算机。确保用户的计算机可以访问监视设备。
- CA Multi-Port Monitor，捕获文件将不会复制到用户的计算机。用户可在监视设备上查看捕获文件。

以下监视设备不对 CA Application Delivery Analysis 进行数据包捕获调查：

- Cisco WAE 设备
- Cisco NAM 设备

管理控制台管理员也可以从“突发事件”页面启动或排定该调查。有关详细信息，请参阅*《用户指南》*。

数据包捕获调查报告包括有关服务器、应用程序和网络的信息，以及用于查看数据包捕获结果的链接。

通过 SNMP 的性能调查

使用通过 SNMP 的性能调查，可以对服务器进行 SNMP 轮询，以获取性能信息，例如内存和 CPU 使用率。

将通过 SNMP 的性能调查分配给服务器突发事件响应。如果服务器由 CA Standard Monitor 监视，管理控制台将从监视设备中启动该调查。否则，将从管理控制台中启动调查。

在“突发事件”页面中，管理控制台管理员还可以在服务器或路由器上启动或排定此调查。要对路由器执行 SNMP 轮询以获取性能信息，管理控制台管理员必须将路由器作为网络设备添加到管理控制台中。

- 如果没有将有效的 SNMP 配置文件分配给服务器或网络设备，管理控制台将尝试发现有效的 SNMP 配置文件。也可以使用其他 CA 产品对服务器和路由器执行 SNMP 轮询，以获取性能信息。
- 要使管理控制台能够对服务器或网络设备执行 SNMP 轮询，您必须将有效的 SNMP 配置文件添加到管理控制台中。

管理控制台使用以下条件来报告总体处理器，并处理 CPU 使用率值：

- 单个处理器百分比使用主机在最后 1 分钟（第一次轮询前的一分钟）维护的 HrProcessorTable (1.3.6.1.2.1.25.3.3.1.2) 来轮询。这是一个快照。
- 单个进程列表使用 HrSWRunPerfTable（1.3.6.1.2.1.25.5.1.1.1 和 .2，cpu 和内存）来轮询。CPU 值是原始时间；因此，将对此值执行两次轮询并将其减去。百分比是由所用的总 CPU 时间除以可用 CPU 时间所得。内存百分比是上次轮询除以可用内存所得。

对于下列 MIB，在调查期间，该调查将对服务器执行两次轮询 - 打开突发事件时执行一次，5 分钟后执行第二次：

- 系统 MIB (1.3.6.1.2.1.1.*.0)
- 接口 MIB (1.3.6.1.2.1.2.2.1)
- Cisco CPU MIB (1.3.6.1.4.1.9.2.1.*)
- 主机资源处理器 (1.3.6.1.2.1.25.3.3.1)
- 主机资源存储 (1.3.6.1.2.1.25.2.3.1)
- IP 地址表 (1.3.6.1.2.1.4.20.1)
- 运行软件 MIB 的主机资源 (1.3.6.1.2.1.25.4.2.1)
- 运行软件性能 MIB 的主机资源 (1.3.6.1.2.1.25.5.1.1)
- 主机资源内存 (1.3.6.1.2.1.25.2.2.0)

当在以下设备中启动或排定时：

- 对于服务器，通过 SNMP 的性能调查会生成有关服务器性能和接口统计信息的报告。
- 对于网络设备，通过 SNMP 的性能调查会生成有关设备性能和接口统计信息的报告。

详细信息：

管理 SNMP 配置文件 (p. 207)
添加网络设备 (p. 211)

Ping 响应时间调查

使用 ping 响应时间调查，可以确认服务器是否能响应 ping 请求，还可以度量接收响应的往复传输时间。

将 ping 响应时间调查分配给服务器突发事件响应。如果服务器由 CA Standard Monitor 监视，管理控制台将从监视设备中启动该调查。否则，将从管理控制台中启动调查。

用户也可以从“突发事件”页面启动或排定此调查。有关详细信息，请参阅 *《用户指南》*。

Ping 响应时间调查可生成关于数据包往复传输时间和响应时间的报告。

跟踪路由调查

使用跟踪路由调查来记录监视设备和端点之间的路径和每个跃点，以监视延迟和路由问题，并可选择性地对每个路由器进行 SNMP 轮询以获取其性能信息。

将跟踪路由调查分配给网络突发事件响应。如果承载应用程序的服务器由 CA Standard Monitor 监视，管理控制台将从监视设备中启动该调查。否则，将从管理控制台中启动调查。

在网络突发事件期间，管理控制台将从监视设备开始跟踪路由调查，并尝试到达有突发事件的网络子网上的设备。如果子网是 /24 或者更具体，该子网中的 IP 地址将用作目标；管理控制台 必须已为此地址收集了响应时间数据。如果子网比 /24 笼统，管理控制台将使用其他方法在子网范围中选取地址。如果在跟踪路由操作属性内，启用了选项“通过 SNMP 调查路由器”，则将首先执行跟踪路由，然后路由中的网络设备列表将用于 SNMP 调查。如果管理控制台发现有效的 SNMP 配置文件，管理控制台将查询设备的性能信息，这些信息将包含在调查结果中。

配置运行 TCP 跟踪路由时，TCP 跟踪路由将要监控的应用程序的 TCP 端口用于出站通信，将 ICMP TTL 到期消息用于沿着终止出站数据包的路径分隔路由器的返回。

管理控制台管理员也可以从“突发事件”页面启动或排定该调查。

跟踪路由调查可生成关于路径、跃点、延迟和使用情况的报告。

您也可以配置跟踪路由调查，以对路径中的每个设备的设备和性能接口统计信息启动通过 SNMP 的性能调查。

要对路径上的每个跃点进行 SNMP 轮询，您不需要将网络设备添加到管理控制台中。不过，要对服务器或网络设备进行 SNMP 轮询，您必须定义有效的 SNMP 配置文件。通过 SNMP 的性能调查可生成关于设备性能和接口统计信息的报告。

对路径上的每个跃点进行 SNMP 轮询时，如果您尚未在管理控制台中使用有效的 SNMP 配置文件定义网络设备，管理控制台会尝试发现每个网络设备上的有效 SNMP 配置文件。此外，您也可以使用其他 CA 产品对您的设备进行 SNMP 轮询以获取性能信息。

详细信息：

管理 SNMP 配置文件 (p. 207)
添加网络设备 (p. 211)

添加突发事件响应

要让管理控制台发送通知或启动调查以响应网络或服务器突发事件，请执行以下操作：

1. 添加网络、服务器或应用程序突发事件响应。
2. 将一个或多个操作添加到突发事件响应中。
3. 将突发事件响应分配给特定网络、服务器或应用程序。

此外，您也可以编辑默认网络、服务器和应用程序突发事件响应，以便添加响应操作。默认情况下，管理控制台不会针对网络或服务器突发事件启动通知或调查。

要让管理控制台启动通知，必须同时满足突发事件“持续时间”和“严重度”这两个条件。使用“持续时间”和“严重度”这两个条件来启动突发事件响应，以便应对以下情况：

- 偶尔短时间发生的轻微的性能下降。可能会发生某些状况，因此您应该监视。
- 性能出现重大下降，持续 1 小时，或“不可用”状态持续 10 分钟。您应该立即调查这些类型的情况。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“突发事件响应”。
3. 在“向我显示”菜单下，通过单击来添加操作。

   添加网络响应

   通知远程站点客户端网络的所有者，或运行跟踪路由调查。

   添加服务器响应

   通知服务器的所有者，或运行基于服务器的调查，如数据包捕获、Ping 响应时间或通过 SNMP 的性能调查。

   添加应用程序响应

   通知应用程序的所有者，或运行应用程序连接时间调查。
4. 单击“应用”。

   您已准备好将操作添加到突发事件响应中 (p. 163)。

详细信息：

管理应用程序可用性 (p. 185)
分配突发事件响应 (p. 165)
管理监视设备突发事件 (p. 234)

编辑突发事件响应

编辑突发事件响应，对其重命名。重命名突发事件响应时，也可以修改其响应操作，例如编辑或添加操作。

按照以下步骤重命名突发事件响应：

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“突发事件响应”。
3. 浏览突发事件列表，然后单击  以编辑网络、服务器或应用程序突发事件响应。

   确认为每个突发事件响应至少分配一个响应操作。
4. 在第三个“向我显示”菜单中单击“编辑突发事件响应”。
5. 在“突发事件响应名称”中键入新名称，然后单击“确定”。

详细信息：

将操作添加到网络或服务器突发事件响应中 (p. 163)
编辑响应操作 (p. 164)
删除响应操作。 (p. 164)

删除突发事件响应

删除突发事件响应将会删除突发事件响应及其响应操作。如果突发事件响应已分配，删除后，管理控制台将会为所有受影响的应用程序、服务器或网络重新分配默认突发事件响应。

您不能删除网络、服务器或应用程序的默认突发事件响应。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“突发事件响应”。
3. 浏览突发事件列表，然后单击 以删除网络、服务器或应用程序突发事件响应。请注意，您无法删除默认突发事件响应。
4. 在“删除确认”中，单击“继续删除”删除突发事件响应。

将操作添加到网络或服务器突发事件响应中

添加操作以启动用于响应网络或服务器突发事件的通知或调查。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“突发事件响应”。
3. 浏览突发事件响应列表，并单击 来编辑网络、服务器或应用程序突发事件响应。
4. 在第三个“向我显示”菜单中，单击“编辑操作”。
5. 在“向我显示”菜单中，单击“添加操作”。

   将打开“操作类型”。
6. 选择一个操作，然后单击“下一步”。

   将打开“操作属性”。
7. 指定响应操作设置，然后单击“确定”。有关详细信息，请单击“帮助”。

   新操作将显示在“突发事件响应操作”中。

编辑响应操作

编辑默认的网络、服务器和应用程序突发事件响应，以便添加一个或多个响应操作，并根据需要创建其他突发事件响应。默认情况下，管理控制台不会针对网络或服务器突发事件启动通知或调查。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“突发事件响应”。
3. 浏览突发事件响应列表，并单击 来编辑网络、服务器或应用程序突发事件响应。
4. 在第三个“向我显示”菜单中，单击“编辑操作”。

   将打开“突发事件响应操作”。
5. 单击 来编辑操作。

   将打开“操作属性”。
6. 指定响应操作设置，然后单击“确定”。有关详细信息，请单击“帮助”。

详细信息：

管理监视设备突发事件 (p. 234)

删除响应操作。

如果您不想继续让管理控制台启动特定响应操作，可将该操作从网络、服务器或应用程序突发事件响应中删除。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“突发事件响应”。
3. 浏览突发事件响应列表，并单击 来编辑网络、服务器或应用程序突发事件响应。
4. 在第三个“向我显示”菜单中，单击“编辑操作”。

   将打开“突发事件响应操作”。
5. 单击 来删除操作。
6. 系统提示您删除响应操作时，请单击“继续删除”。

分配突发事件响应

要让管理控制台响应网络或服务器突发事件，可以为应用程序、服务器或网络类型分配至少具有一个响应操作的突发事件响应。

请注意，默认突发事件响应不包括响应操作，但允许用户添加。

为以下类型分配突发事件响应	在以下对象上启动操作
应用程序	导致服务器或网络性能“轻微”（黄色）或“重大”（橙色）下降的应用程序。
服务器	性能“轻微”（黄色）或“重大”（橙色）下降的服务器。
网络类型	性能“轻微”（黄色）或“重大”（橙色）下降的网络。 请注意，当您将突发事件响应分配给某个网络类型时，突发事件响应会分配给具有相应网络类型的所有网络。

详细信息：

按网络类型对客户端网络分组 (p. 45)
编辑响应操作 (p. 164)

将突发事件响应分配给应用程序

将突发事件响应分配给应用程序，使得管理控制台能够调查应用程序，并将影响该应用程序的网络或服务器突发事件通知给您的团队。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. 滚动到“应用程序列表”，选择所需应用程序，然后单击“编辑”。

   将打开“应用程序属性”。
4. 单击“突发事件响应”，指定所需的突发事件响应，然后单击“确定”。

将突发事件响应分配给服务器

将突发事件响应分配给服务器，使得管理控制台能够调查服务器，并将相应的服务器突发事件通知给您的团队。管理控制台会将默认突发事件响应分配给所有服务器，不过，CA Application Delivery Analysis 是一种被动监视解决方案，默认情况下不会采取任何操作。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. 滚动到“应用程序列表”，然后单击 以编辑服务器。

   将打开“服务器属性”。

   （可选）要将同一突发事件响应分配给多个服务器，请选择相应的服务器，然后单击 以编辑所有选定的应用程序。
4. 在“服务器属性”中，单击“突发事件响应”以分配所需服务器突发事件响应，然后单击“确定”。

将突发事件响应分配给网络类型

将突发事件响应分配给网络类型，使得管理控制台能够调查网络，并将相应的网络突发事件通知给您的团队。

请注意，当您将突发事件响应分配给某个网络类型时，同一突发事件响应适用于具有相应网络类型的所有网络。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“网络类型”。

   将打开“网络类型”。
3. 单击 以编辑网络类型。

   将打开“网络类型属性”。
4. 单击“突发事件响应”，指定所需的突发事件响应，然后单击“确定”。

详细信息：

向客户端网络分配网络类型 (p. 50)

突发事件响应故障排除

如果管理控制台没有启动预期的响应操作，请确保：

- 相应的突发事件响应已分配给应用程序、服务器或网络类型。对于客户端网络，请确保相应的网络类型已分配给客户端网络。
- 分配给突发事件响应的响应操作已进行了适当的配置。通常情况下，请确保管理控制台创建的网络或服务器突发事件超过突发事件响应的“最小严重度”和“持续时间”这两个条件。复查响应操作属性并查看帮助以了解更多信息。

使用 Web 服务方法管理突发事件

将 SNMP 陷阱操作添加到突发事件响应中时，可使用 Web 服务来查询已发送数据之外的突发事件数据。可对突发事件响应陷阱使用“发送状态更新”选项。

对象标识符规范

- 突发事件 ID .1.3.6.1.4.1.4498.2.20.1.1.1
- 服务器名称 .1.3.6.1.4.1.4498.2.20.1.2.1
- 服务器 IP .1.3.6.1.4.1.4498.2.20.1.3.1
- 应用程序名称 .1.3.6.1.4.1.4498.2.20.1.4.1
- 网络名称 .1.3.6.1.4.1.4498.2.20.1.5.1
- 度量标准名称 .1.3.6.1.4.1.4498.2.20.1.6.1
- 突发事件时间 .1.3.6.1.4.1.4498.2.20.1.7.1
- 严重度 .1.3.6.1.4.1.4498.2.20.1.8.1
- 受影响百分比 .1.3.6.1.4.1.4498.2.20.1.9.1
- 持续时间 .1.3.6.1.4.1.4498.2.20.1.10.1
- 突发事件 URL .1.3.6.1.4.1.4498.2.20.1.11.1
- 响应类型 .1.3.6.1.4.1.4498.2.20.1.12.1 服务器 | 网络 | 应用程序
- 突发事件状态类型 .1.3.6.1.4.1.4498.2.20.1.13.1 打开 | 更新 | 关闭
- Web 服务 IP .1.3.6.1.4.1.4498.2.20.1.14.1

服务器名称和 IP

- 对于所有服务器突发事件来说，“服务器名称“和”服务器 IP”字段均包含关联服务器的特定名称和 IP 地址。
- 对于只涉及一个相关服务器的网络突发事件来说，这些字段包含关联服务器的特定名称和 IP 地址。
- 对于涉及多个相关服务器的网络突发事件，这些字段包含 [n+ 服务器] 或 [n+ 地址] 来表示处于“严重度”状态的服务器的数目（n 或更多）。
- 对于因数据处于非活动状态（白色状态）而关闭的网络突发事件来说，这些字段为 [无]。

应用程序名称

- 对于仅涉及一个相关应用程序的服务器或网络突发事件来说，此字段包含该应用程序的特定名称。
- 对于服务器或网络突发事件的应用程序突发事件响应来说，此字段包含该应用程序的特定名称。
- 对于涉及多个相关应用程序的服务器或网络突发事件来说，此字段包含 [n 应用程序]，其中 n 表示处于“严重度”状态的应用程序的数目。
- 对于因数据处于非活动状态（白色状态）而关闭的服务器或网络突发事件来说，此字段为 [无]。
- 对于因服务器不可用而引发的服务器突发事件来说，此字段为 [全部]。

网络名称

- 对于所有网络突发事件来说，此字段均包含关联网络的特定名称和子网。
- 对于只涉及一个相关网络的服务器突发事件来说，此字段包含关联网络的特定名称和子网。
- 对于涉及多个相关网络的服务器突发事件来说，此字段包含 [n+ 网络]，表示处于“严重度”状态的网络的数目（n 或更多）。
- 对于因数据处于非活动状态（白色状态）而关闭的服务器突发事件来说，此字段为 [无]。

度量标准名称

- 对于因度量标准超过阈值而引发的突发事件来说，此字段为逗号分隔的缩略语列表。
  - NRTT 网络往复传输时间
  - RTNS 重传延迟
  - NCT 网络连接时间
  - ERTT 有效往复传输时间
  - SRT 服务器响应时间
  - SCT 服务器连接时间
  - RS 拒绝的会话（百分比）
  - US 无响应的会话（百分比）
- 对于因不可用而引发的突发事件来说，此字段为“可用性”。
- 对于因数据处于非活动状态（白色状态）而关闭的突发事件来说，此字段为“数据不足”。

Web 服务规范

请使用其中一个 Web 服务接口方式来获取数据。这些 Web 服务支持 XML 输出。

请通过以下网址访问 Web 服务：
`http://WebServiceIP/SuperAgentWebService/PublishedService.asmx`

输入

使用 FetchServersByIncident 或 FetchServersByIncidentSeverityDuration 检索服务器列表。

输入

- 突发事件 ID
- 最小严重度（可选）
- 最短持续时间（可选）

输出

- server_id，32 位未签名的标识符
- server_desc，最多可含 50 个字符的字符串名称
- address，32 位未签名的 IP 地址
- 无 - 突发事件期间未收集数据的时间的百分比，用浮点数表示
- 未分级 - 突发事件期间不存在阈值（尚未计算或已关闭）的时间的百分比，用浮点数表示
- 正常 - 突发事件期间收集正常（小于阈值）数据的时间的百分比，用浮点数表示
- 下降 - 突发事件期间收集已下降（但未过度）数据的时间的百分比，用浮点数表示
- 过度 - 突发事件期间收集过度数据的时间的百分比，用浮点数表示
- 不可用 - 突发事件期间服务器或应用程序不可用（仅服务器突发事件）的时间的百分比，用浮点数表示

输入

检索应用程序列表 FetchApplicationsByIncident 或 FetchApplicationsByIncidentSeverityDuration。

输入

- 突发事件 ID
- 最小严重度（可选）
- 最短持续时间（可选）

输出

- app_id，32 位未签名的标识符
- applications_desc，最多可含 50 个字符的字符串名称
- port_beg，范围内 16 位的未签名的第一个端口
- port_end，范围内 16 位的未签名的最后一个端口
- 无 - 突发事件期间未收集数据的时间的百分比，用浮点数表示
- 未分级 - 突发事件期间不存在阈值（尚未计算或已关闭）的时间的百分比，用浮点数表示
- 正常 - 突发事件期间收集正常（小于阈值）数据的时间的百分比，用浮点数表示
- 下降 - 突发事件期间收集已下降（但未过度）数据的时间的百分比，用浮点数表示
- 过度 - 突发事件期间收集过度数据的时间的百分比，用浮点数表示
- 不可用 - 突发事件期间服务器或应用程序不可用（仅服务器突发事件）的时间的百分比，用浮点数表示

输入

检索网络列表 FetchNetworksByIncident 或 FetchNetworksByIncidentSeverityDuration。

输入

- 突发事件 ID
- 最小严重度（可选）
- 最短持续时间（可选）

输出

- client_id，用于网络定义的 32 位未签名的标识符
- client_address，网络子网的 32 位未签名的地址部分
- client_mask，网络子网的 32 位未签名的掩码部分（扩展的 CIDR）
- client_desc，最多可含 50 个字符的字符串名称
- subnet，x.x.x.x/m 格式的子网规范
- 无 - 突发事件期间未收集数据的时间的百分比，用浮点数表示
- 未分级 - 突发事件期间不存在阈值（尚未计算或已关闭）的时间的百分比，用浮点数表示
- 正常 - 突发事件期间收集正常（小于阈值）数据的时间的百分比，用浮点数表示
- 下降 - 突发事件期间收集已下降（但未过度）数据的时间的百分比，用浮点数表示
- 过度 - 突发事件期间收集过度数据的时间的百分比，用浮点数表示
- 不可用 - 突发事件期间服务器或应用程序不可用（仅服务器突发事件）的时间的百分比，用浮点数表示

  注意：突发事件 Web 服务中的严重度百分比与“操作”和“突发事件”视图导出一致。

发送状态更新规范

应用程序、服务器和网络突发事件响应陷阱选项可发送增量严重度更新。不管持续时间如何，所有严重度更新都会发送。如果关闭该选项，则只在达到严重度/持续时间条件的情况下，才会发送打开和关闭的突发事件陷阱。

应用程序突发事件响应陷阱规范

应用程序突发事件响应陷阱以仅特定于该应用程序的网络和服务器突发事件响应方式进行发送。通常情况下，网络突发事件包含聚合应用程序和服务器数据。同样，服务器突发事件也包含聚合应用程序和网络数据。对于网络和服务器突发事件的应用程序突发事件响应来说，每个网络/应用程序和服务器/应用程序组合一超出阈值就会报警，并且都包含相应的聚合服务器和网络数据。

解释 SNMP 陷阱

下表列出了陷阱中的行，并对每个行进行了说明。

陷阱	说明
1.3.6.1.4.1.4498.2.20.1.1.1 netQoSIncident7Number **17841**	突发事件标识符。
1.3.6.1.4.1.4498.2.20.1.2.1 netQoSIncident7Server **dc1.netqos.local**	涉及的服务器的名称。
1.3.6.1.4.1.4498.2.20.1.3.1 netQoSIncident7ServerAddress **192.168.0.6**	涉及的服务器的地址。
1.3.6.1.4.1.4498.2.20.1.4.1 netQoSIncident7Application **Lightweight Directory Access Protocol**	涉及的应用程序。
1.3.6.1.4.1.4498.2.20.1.5.1 netQoSIncident7ClientRegion **SuperAgent LAN - 192.168.245.0/24**	涉及的网络。
1.3.6.1.4.1.4498.2.20.1.6.1 netQoSIncident7Regards **NRTT,ERTT**	涉及的度量标准。
1.3.6.1.4.1.4498.2.20.1.7.1 netQoSIncident7Time **07-2-20 20:40 GMT-4**	事件的结束时间戳。
1.3.6.1.4.1.4498.2.20.1.8.1 netQoSIncident7Severity **Excessive**	违反的阈值和严重度分级。

陷阱	说明
1.3.6.1.4.1.4498.2.20.1.9.1 netQoSIncident7Impact **91.5%**	受影响的观测的加权百分比。影响值表示前 netQoSIncident7Duration 分钟内 netQoSIncident7Severity 的影响。对于网络来说，它是指每个应用程序/度量标准对的服务器观测的百分比峰值。对于服务器来说，它是指每个应用程序/度量标准对的网络观测的百分比峰值。
1.3.6.1.4.1.4498.2.20.1.10.1 netQoSIncident7Duration **10.0 Minutes**	事件的持续时间。
1.3.6.1.4.1.4498.2.20.1.11.1 netQoSIncident7URL **http://192.168.100.131/SuperAgent/Investigator/Incidents/IncidentsViewFocus.aspx?Nav=13,0,0&Stack=T|M|N|A|S&I=1017841**	突发事件 UI 的 URL 链接。
1.3.6.1.4.1.4498.2.20.1.12.1 netQoSIncident7ResponseType **Network**	生成该陷阱的突发事件响应的类型。
1.3.6.1.4.1.4498.2.20.1.13.1 netQoSIncident7State **Open**	陷阱的“打开”、“更新”或“关闭”状态。
1.3.6.1.4.1.4498.2.20.1.14.1 netQoSIncident7WebServiceIP **192.168.100.131**	控制台的 IP 地址，可在其中找到 Web 服务以了解进一步的详细信息。

第 8 章： 管理应用程序性能 OLA

此部分包含以下主题：

性能 OLA 的工作方式

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

性能 OLA 通过跟踪一段时间表现最差的基于 IPv4 的事务的行为来增强报告。此跟踪会指出性能降低最严重的位置和时间。此跟踪还可以让用户了解性能与管理控制台中报告的平均数据点的偏差情况。

默认情况下，管理控制台不报告性能 OLA。可以为用户定义的应用程序而非为系统定义的应用程序创建 OLA。

考虑到管理控制台收集 OLA 数据和度量 OLA 遵从性的方式，建议您设置 OLA 以度量每个远程位置而非所有位置的遵从性。要在每个远程位置建立 OLA，请使用网络类型。

（可选）要为应用程序设置性能 OLA 并将 OLA 应用于管理控制台监视的所有服务器，请创建用户定义的应用程序并将其分配给域。服务器子网发生更改时，管理控制台会自动更新应用程序服务器分配。

详细信息：

按网络类型对客户端网络分组 (p. 45)

性能 OLA 报告的工作方式

性能 OLA 通过每小时计数一次快于给定阈值的基于 IPv 4 的事务的百分比，来显示用户定义的应用程序的性能情况。90% 的服务器响应时间必须少于 20 毫秒，这就是性能 OLA 的一个示例。性能 OLA 的结果显示在报告中，报告每小时指示一次应用程序是否满足运行水平协议。

管理控制台基于您指定的阈值度量每小时运行水平遵从性。您可以指定最多包含三位小数的的阈值，如 93.999。报告 OLA 遵从性违反可能会耗时长达一小时。

管理控制台收集 OLA 数据时，采用的方式与 5 分钟数据不同。对于性能 OLA 来说，监视设备可用于：

- 比较每个事务，了解该事务是否满足 OLA 阈值。
- 记录每小时通过的和失败的事务数。

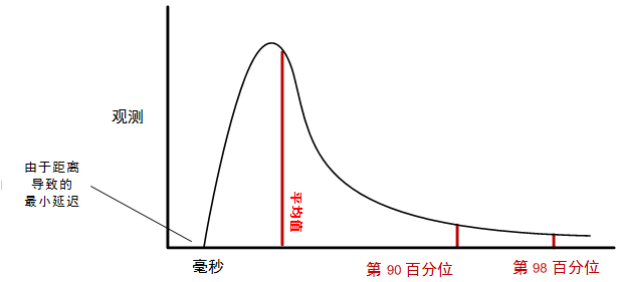
比如，管理控制台不会每五分钟记录一次州际公路上车辆的平均速度，而是对每辆车的车速是否超过 40 英里/小时进行记录，并每小时报告一次成功数和失败数。

与此相反，管理控制台每隔 5 分钟就会根据特定度量标准的平均响应时间，使用阈值来监视应用程序的性能。

性能 OLA 阈值的工作方式

由于可以通过性能 OLA 对执行速度最慢的事务进行更深入的了解，因此有必要了解典型的性能时间片的外观。多数人都熟悉标准分布曲线或钟形曲线，在谈到百分位时，通常会想到这种曲线。不过，TCP 事务不符合正态分布， 而是有一个因网络往复传输时间的距离因素以及服务器响应时间 (SRT) 中的 I/O 因素而造成的最小延迟。理想情况下，您应该尽可能让更多事务的处理时间符合此最小延迟时间。

以下示例显示了管理控制台在给定时段内看到的“网络往复传输时间”曲线的理想化版本。当性能下降时，整个曲线会右移，或者曲线的尾部会延伸。这种情况下，OLA 就很有用。



OLA 使用户能够为第 90 和 98 百分位指定阈值。请注意，用户可以指定任何百分位。报告显示这些值的哪个百分位实际达到了阈值。通过调整阈值，您可以监视后面部分的行为并根据目标来设置 OLA。

运行水平度量标准的工作方式

性能 OLA 使用下列关键度量标准来衡量运行水平遵从性。您可以选择在 OLA 中监视以下部分或全部运行水平：

运行水平度量标准	详细信息
网络往复传输时间	■ 按网络类型进行配置，特别是针对 WAN 链路进行配置。 ■ 确保已将具有类似延迟的网络分组到一起。 ■ 监视业务关键型应用程序，特别是针对 WAN 链路进行监视。 ■ 选择代表每个站点最大（或最恒定）通信量的应用程序，以便获取更多观测结果，并使结果更具统计意义。
服务器响应时间	■ 不要按网络类型来区分。 ■ 不管请求来自哪个网络，服务器都应独立对待这些请求。 ■ 监视多层应用程序中最具影响的层，并请牢记：前端服务器响应时间将包括后端服务器请求。 ■ 监视服务器中的业务关键型应用程序
总事务时间	■ 反映最终用户总体体验的最佳指标，因为它取决于服务器响应时间、网络往复传输时间和数据传输时间。 ■ 根据网络类型进行配置，因为它取决于网络往复传输时间。 ■ 监视业务关键型应用程序

性能 OLA 提示和技巧

我们建议为代表每个站点最大（或最恒定）通信量的用户定义的应用程序创建一个应用程序性能 OLA，以便获取更多观测结果，并使结果更具统计意义。您无法为系统定义的应用程序设置操作级别。

设置性能 OLA 时，请注意：

- 区分数据中心度量标准与网络度量标准。并非每个网络的每个度量标准都是有意义的。例如，在后端应用程序上，您可能不希望进行网络往复传输时间跟踪。
- 当确定 OLA 阈值时，有必要使用较长的时间表，以便消除瞬时峰值或峰谷。您也可以将特定度量标准从 OLA 排除。
- 最多可定义两个阈值来衡量应用程序是否遵从运行水平，例如，可以设置内部运行水平和外部运行水平。一般情况下，可以将运行水平定义在 90% 或更高，以便通过管理控制台对性能差异进行更深入的了解。此外，您也不需要设置 OLA 度量标准的性能阈值水平。

获得每个阈值水平的正确值以后，管理控制台将会有 5 分钟平均值以及每个远程位置的用户所经历的性能最差（最高百分位）的事务的历史趋势数据。

详细信息：

编辑应用程序性能 OLA (p. 183)

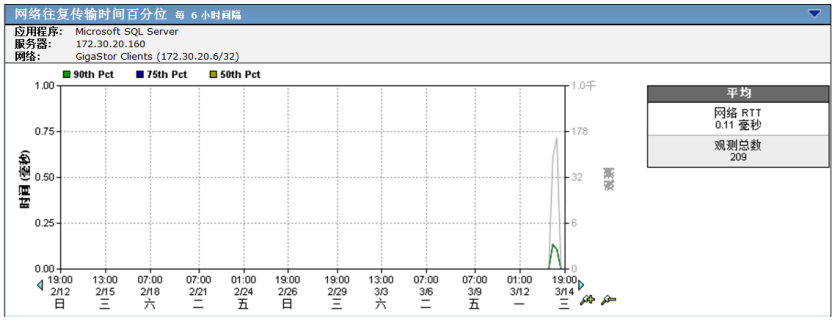
通过历史数据确定运行水平

使用历史报告数据作为起点来配置新的运行水平协议。我们建议您等待一个月，以允许管理控制台收集足够的数据来确定应用程序的正常行为。

遵循这些步骤:

1. 单击“工程”页面。
2. 在“向我显示”菜单中，单击“设置”。

   将打开“设置”对话框。
3. 选择应用程序。
4. 选择一台服务器。
5. 选择网络。
6. 设置时间范围以显示每月报告，然后单击“确定”。
7. 在组件报告（如网络往复传输时间报告，在下以下示例中，该报告包含洛杉矶网络和所有承载 Exchange 应用程序的服务器的响应时间数据）中找到所需的运行水平度量标准。



8. 在“统计信息”中，请记下第 90 个值和最大值。在以下示例中，第 90 个百分位为 12.4 毫秒，最大值为 41.7 毫秒。

统计	
最小值	3.97 毫秒
最大值	58.2 毫秒
平均值	8.72 毫秒
第 50	4.78 毫秒
第 75	6.36 毫秒
第 90	28.8 毫秒
观测	6千

注意：按月进行报告时，管理控制台会将报告统计信息聚合成 6 小时的增量。有关详细信息，请参阅*《用户指南》*。

9. 重复这些步骤以收集每个运行水平度量标准（包括网络往复传输时间和服务器响应时间）的第 90 个百分位和最大百分位。对于事务时间，请对网络往复传输时间、服务器响应时间、重传延迟和数据传输时间的第 90 个百分位和最大百分位求和和求平均值。
10. 要确定初始运行水平，可将每月第 90 个和第 98 个百分位的历史值加倍。根据上面的统计示例，第 90 个和第 98 个百分位加倍后，将等于网络往复传输时间 25 毫秒的第 90 个百分位以及 81 毫秒的第 98 个百分位。
11. 在 OLA 经历第一个报告期间时对其进行监视；如果一开始无法满足 OLA，不要气馁。进行调整之前，请等待整个报告期间结束。由于管理控制台每小时衡量一次运行水平遵从性，因此 OLA 显示遵从性违反可能会有长达一小时的滞后。
12. 完成一次报告期间之后，可对阈值进行调整，以便设置为可以实现的阈值。获得结果后，您就可以对阈值进行更有根据的评估。

详细信息：

为一组网络创建应用程序性能 OLA (p. 181)

为一组网络创建应用程序性能 OLA

创建性能 OLA，以定义某组客户端网络中由用户定义的、具有类似延迟特征的应用程序的预期服务级别。

管理控制台为每个用户定义的应用程序创建默认 OLA，以便度量跨所有未分配网络类型的网络的性能。一般来说，由于各个远程位置之间的网络延迟有所不同，因此不建议监视网络往复传输时间和总事务时间。

更新默认 OLA 中的阈值后，所做更改将动态应用到配置为使用默认 OLA 值的应用程序的所有新 OLA。例如，如果 POP3 应用程序的默认 OLA 要求在 1 小时间隔内网络往复传输时间观测的至少 90% 为 5 毫秒，而且您在“奥斯汀”网络类型中为 POP3 应用程序创建了 OLA，那么观测的默认百分比为 90%，网络往复传输时间阈值为 5 毫秒。如果您更改 POP3 为网络往复传输时间设置的默认 OLA 阈值，管理控制台会动态更新为 POP3 奥斯汀的 OLA 设置的网络往复传输时间阈值，使之能够使用新的默认值。

创建 OLA 时，您可以自定义阈值来覆盖动态的默认值。如果您更改了 OLA 度量标准的阈值数字或最小观测数但未自定义阈值，该更改即可应用到默认 OLA。

在创建 OLA 之前，建议您对应用程序监视一个月以确定其正常性能。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“性能 OLA”。
3. 浏览“性能 OLA 列表”中的 OLA 列表。如果列表中没有应用程序，则不存在用户定义的应用程序。

   默认情况下，管理控制台会为每个适用于网络且没有分配网络类型的用户定义应用程序创建“默认 OLA”。
4. 单击“按照网络类型添加自定义”为一组客户端网络创建应用程序 OLA。

   将打开“按网络类型自定义阈值”。
5. 选择与合适的远程位置相对应的应用程序和网络类型，然后单击“确定”。

   将打开“编辑 OLA 阈值”。
6. 为每个 OLA 度量标准编辑阈值设置，然后单击“确定”。

   有关编辑 OLA 阈值的信息，请单击“帮助”。
7. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

8. 耐心等待整个报告周期（长达一小时）结束，通过对照管理控制台观测到的实际响应时间来了解阈值是如何变化的。

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

   b. 必要时，可调整运行水平阈值百分比的值或增加阈值水平的值，使得应用程序能够满足远程站点的运行水平协议。

详细信息：

编辑应用程序性能 OLA (p. 183)
通过历史数据确定运行水平 (p. 179)

编辑应用程序性能 OLA

编辑性能 OLA，对一组按网络类型标识的网络上的用户定义应用程序的预期服务水平进行更改。

管理控制台为每个用户定义的应用程序创建默认 OLA，以便度量跨所有未分配网络类型的网络的性能。一般来说，由于各个远程位置之间的网络延迟有所不同，因此不建议监视网络往复传输时间和总事务时间。

更新默认 OLA 中的阈值后，所做更改将动态应用到配置为使用默认 OLA 值的应用程序的所有新 OLA。例如，如果 POP3 应用程序的默认 OLA 要求在 1 小时间隔内网络往复传输时间观测的至少 90% 为 5 毫秒，而且您在“奥斯汀”网络类型中为 POP3 应用程序创建了 OLA，那么观测的默认百分比为 90%，网络往复传输时间阈值为 5 毫秒。如果您更改 POP3 为网络往复传输时间设置的默认 OLA 阈值，管理控制台会动态更新为 POP3 奥斯汀的 OLA 设置的网络往复传输时间阈值，使之能够使用新的默认值。

如果您更改了 OLA 度量标准的阈值数字或最小观测数但未自定义阈值，该更改即可应用到默认 OLA。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. 滚动到“应用程序列表”，选择您想要的应用程序，然后单击“OLA”。

   将打开“编辑应用程序 OLA”，并按照网络类型列出选定应用程序的 OLA。
4. 单击  ，对一组客户端网络的性能 OLA 的相应网络类型进行编辑。

   （可选）要编辑多个远程位置的性能 OLA，请选择相应的网络类型，然后单击  对所选 OLA 进行编辑。

   将打开“编辑 OLA 阈值”。
5. 为每个 OLA 度量标准编辑阈值设置，然后单击“确定”。

   有关设置服务器属性的信息，请单击“帮助”。
6. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。
7. 耐心等待整个报告周期（长达一小时）结束，通过对照管理控制台观测到的实际响应时间来了解阈值是如何变化的。

a. 在“管理”页面上的“向我显示”菜单中，单击“性能详细描述 OLA”。

b. （可选）调整运行水平阈值的值。例如，如果网络往复传输时间的阈值在第 90 个百分位小于 11 毫秒，但仅仅 67.744% 的观测满足该阈值水平，则应调整阈值水平百分比或阈值水平，以便应用程序满足远程站点的运行水平协议。

详细信息：

为一组网络创建应用程序性能 OLA (p. 181)

删除应用程序性能 OLA

删除性能 OLA 以便为远程站点上的一个或多个应用程序删除任何预期服务水平。要删除远程位置客户端网络的应用程序性能 OLA，请标识分配给客户端子网的网络类型。

此外，您也可以从应用程序性能 OLA 中删除特定性能度量标准。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. 滚动到“应用程序列表”，选择您想要的应用程序，然后单击“OLA”。

   将打开“编辑应用程序 OLA”，并按照网络类型列出选定应用程序的 OLA。
4. 单击 删除 OLA。

   系统提示您删除指定 OLA 时，请单击“继续删除”。
5. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

按网络类型对客户端网络分组 (p. 45)
编辑应用程序性能 OLA (p. 183)

第 9 章： 管理应用程序可用性

此部分包含以下主题：

可用性监视的工作方式

CA Application Delivery Analysis 通过被动数据观测跟踪用户定义的应用程序的可用性。要确定应用程序可用性，监视设备将观测分配给应用程序的每个服务器上的基于 IPv4 的客户端活动。

可用性监控需要：

- CA Standard 或 Virtual Systems Monitor
- CA Multi-Port Monitor

如果监视设备在 5 分钟间隔内观测到服务器的应用程序端口的用户通信不足，监视设备会通过向应用程序提出主动请求来验证该应用程序的可用性。

可用性条件	含义
少于 10 个成功的 TCP 事务	如果在 5 分钟间隔内在应用程序端口上成功的 TCP 事务少于 10 个，监视设备将主动检查应用程序的可用性。
超过 10% 的被拒绝会话	如果应用程序端口在 5 分钟间隔期内拒绝 10%（或更多）的连接请求，监视设备会主动检查该应用程序的可用性。

监视设备通过向服务器上的应用程序端口发送 TCP SYN 数据包，主动检查应用程序可用性。对于由端口范围定义的应用程序，将会在该范围中的前八个端口每一个上尝试连接。

如果监视设备没有从应用程序服务器收到 SYN-ACK 数据包响应：

- 应用程序将被分级为“不可用”。
- 监视设备通过向承载应用程序的服务器发送 ping 请求来主动检查该服务器的可用性。除非应用程序被分级“不可用”，否则不会检查服务器可用性。如果服务器：
  - 响应 ping，即该服务器被分级为“可用”。
  - 不响应 ping，即该服务器被分级为“不可用”。

对于负载平衡的应用程序，您可以选择根据已分配服务器的最小数目来分级应用程序可用性，而不是在每个已分配服务器上检查应用程序的可用性。例如，如果负载平衡器将应用程序通信量分布到 2 至 5 台服务器之间，则正常情况下，该应用程序应至少在 2 台服务器上处于活动状态。要将该应用程序分级为“可用”，必须在 5 台服务器的至少 2 台上发生可接受的应用程序活动。如果将负荷平衡的应用程序分级为“不可用”，将检查每个已分配服务器的可用性 (p. 190)以确定哪些服务器可用。

详细信息：

检查服务器可用性 (p. 190)

为何要排除系统定义的应用程序

为了避免不正确地打开可用性突发事件，管理控制台不自动监视系统定义的应用程序的可用性。例如，首次观测到服务器端口 80 上的 TCP 通信量后，管理控制台将自动创建 HTTP 应用程序的实例。然而，在该应用程序上启用可用性监视可能会生成许多假的可用性突发事件，因为管理控制台会期望看到 HTTP 在域的每个服务器上运行，而不仅仅是在最初观测到通信量的服务器上运行。

（可选）要为应用程序设置可用性 OLA 并将 OLA 应用于受管理控制台监视的所有服务器，请创建用户定义的应用程序并为其分配域。服务器子网发生更改时，管理控制台会自动更新应用程序服务器分配。

针对应用程序可用性的服务器突发事件的工作方式

管理控制台会自动打开服务器突发事件，以响应处于“不可用”状态的应用程序。如果您已将突发事件响应分配给：

- 承载应用程序的服务器，并且应用程序不可用，则将启动分配的突发事件响应，如：
  - 电子邮件通知
  - SNMP 陷阱通知
  - ping 响应时间调查
  - 通过 SNMP 的性能调查
  - 数据包捕获调查
- 应用程序，并且应用程序不可用，则将启动分配的突发事件响应，如：
  - 电子邮件通知
  - SNMP 陷阱通知
  - 数据包捕获调查

  请注意，应用程序连接时间调查未启动来响应“不可用”应用程序，因为从调查结果中将查找不到任何有关应用程序状态的附加信息。

应用程序可用性报告的工作方式

单击“设置”中的“所有服务器度量标准”时，管理控制台将报告应用程序的可用性。默认情况下，“设置”显示不显示应用程序可用性状态的“所有相关度量标准”。

只有管理控制台管理员将服务器分配给用户定义的应用程序时，该分级才适用于该应用程序。管理控制台报告：

- 在 5 分钟间隔期间，服务器上的应用程序是否可用。
- 应用程序可用的时间百分比。

对于负载平衡的应用程序，应用程序可用性会被分级为该应用程序在最低数量的服务器上可用的时间百分比。

详细信息：

检查服务器可用性 (p. 190)

启用可用性监视

管理控制台可度量所有客户端网络的应用程序可用性。您无法监视特定网络上应用程序的可用性。

重要说明！使用域分隔承租人数据时，通过禁用可用性监控来避免误报可用性事件。在 ISP 环境中，监视设备不可能连接到应用程序服务器以主动地检查应用程序端口的可用性。

在应用程序上启用可用性监视，并选择性地在承载该应用程序的服务器上启用可用性监视。

监视应用程序可用性

要监视应用程序可用性，请编辑应用程序属性以启用可用性监视。默认情况下，可用性监视已禁用。

决定要监视哪些应用程序的可用性时，我们建议监视：

- 已分配服务器的用户定义的应用程序。应用程序在以下情况下时，管理控制台不监控应用程序可用性：
  - 自动受监视（系统定义）
  - 用户定义，具有一个已分配的服务器子网
  - 已分配给域中的所有服务器
- 优先应用程序。如果您在不属于优先应用程序的应用程序上设置可用性 OLA，且管理控制台对应用程序进行了梳理或对应用程序数据进行了筛选，则即使没有必要，管理控制台也会检查该应用程序的可用性。管理控制台不对优先应用程序进行梳理或筛选。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. 滚动到“应用程序列表”，选择您想要的用户定义的应用程序，然后单击“编辑”。

   将打开“应用程序属性”。

   要更轻松地查找用户定义的应用程序，请使用“显示”菜单隐藏系统定义的应用程序。
4. 单击“可用性监视”列表并选择“已启用”，然后单击“确定”。
5. 如果要使用负载平衡器在服务器之间分布应用程序的通信量，可编辑该应用程序的服务器分配情况，指定可用的服务器数目。
6. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

检查服务器可用性 (p. 190)
优先应用程序的工作方式 (p. 94)

检查服务器可用性

CA Application Delivery Analysis 监视设备主动确认服务器承载的应用程序不可用后，会检查服务器可用性。检查服务器可用性有助于确定应用程序可用性问题是否与应用程序或承载应用程序的服务器有关。

如果您不想主动检查承载应用程序的服务器的可用性，请在每个分配的服务器上禁用可用性监视。默认情况下，服务器可用性监视已启用。

要监视负载平衡的应用程序的可用性，除了检查服务器可用性，您还必须指定必须处于可用状态的服务器的最小数目。例如，针对一个负荷平衡的应用程序，负载平衡器可能不在其所有服务器之间共享应用程序负载，因此仅有必要确认有最少数量的服务器正在承载该应用程序。

注意：在应用程序的状态为“可用”时，将不会检查服务器可用性，因此，一个负荷平衡的应用程序中的所有已分配服务器都可能有“可用”状态，而实际上其中一些服务器并不可用。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“应用程序”。
3. 滚动到“应用程序列表”，选择您想要的用户定义的应用程序，然后单击“编辑”。

   将打开“应用程序属性”。
4. 单击“分配”。
5. （可选）如果承载应用程序的服务器是负载平衡场的一部分，请通过以下步骤指定必须处于可用状态的服务器的最小数目：
   a. 选择“服务器支持负载平衡场中的应用程序”。如果该选项不可选，请单击“属性”并启用应用程序可用性监视。
   b. 键入一个值以代表将应用程序视为“可用”所需的“最小”服务器数目。
6. 单击“确定”。
7. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

编辑服务器 (p. 73)

应用程序可用性 OLA 的工作方式

在可能会呈现给广大受众的报告中，可以使用可用性运行水平协议（可用性 OLA）来量化当前的应用程序和服务器可用性以及可用性趋势。了解服务器或应用程序是否没有运行是十分有用的信息。以下方案表明存在各种不同的问题：

- 应用程序未运行，但承载它的服务器正在运行。
- 仅针对该应用程序锁定 TCP 端口（如对 Web 应用程序锁定 TCP-80）。

可用性 OLA 报告为管理人员提供了一个切实的度量标准，可用于显示应用程序及其分配的服务器的可用性，而不仅仅是根据收到的停机数或投诉数目来监视性能。管理控制台不跟踪网络可用性。

可用性 OLA 报告的工作方式

可用性 OLA 可报告应用程序在所有网络中处于可用状态的时间百分比。例如，可用性 OLA 可能会指出，由特定服务器承载的某个应用程序在一个月内 95.999% 的时间处于可供所有网络使用的状态。管理控制台每 5 分钟更新一次可用性 OLA 报告，指出应用程序是否满足运行水平协议。

启用应用程序可用性 OLA

使用“可用性 OLA 列表”来启用应用程序的可用性 OLA 报告，并指定运行水平遵从性的阈值。在指定阈值时，请考虑好您计划用于报告的时段。例如，如果您希望进行为期 12 个月的可用性报告，则可设置一个与 1 个月的报告所用阈值不同的阈值。请注意，您不能为同一个应用程序创建多个可用性 OLA。

当您指定可用性 OLA 时，请确保也启用针对应用程序本身的可用性监视。指定可用性 OLA 不会自动对应用程序进行更新。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“可用性 OLA”。

   将打开“可用性 OLA 列表”。
3. 单击  以编辑 OLA。

   将打开“配置运行水平协议”。
4. 选择“启用可用性 OLA”，键入此应用程序应处于可用状态的最小时间百分比，然后单击“确定”。指定的阈值最多可包含三位小数，如 93.999。

   管理控制台会显示一个提醒，提醒用户启用对应用程序的可用性监视。

详细信息：

编辑用户定义的应用程序 (p. 117)

第 10 章： 管理用户帐户权限

此部分包含以下主题：

用户帐户权限的工作方式

用户帐户安全性基于登录访问权限，与 CA PC 和 CA NPC 的安全性完全兼容。管理控制台管理员可创建和管理在管理控制台、CA PC 和 CA NPC 中有效的安全用户帐户。这些帐户允许其他操作员访问管理控制台管理功能和报告数据。对报告数据的访问可以进一步基于 CA PC 或 CA NPC 组进行限制。

要创建安全的访问权限系统，授权用户必须按照与其用户帐户关联的角色和产品权限来获取产品功能的访问权限。在 CA PC 或 CA NPC 上注册管理控制台后，与创建和修改这些帐户关联的所有任务可在 CA PC 或 CA NPC“管理配置”页面中执行。

管理控制台管理员可能需要创建其他用户帐户来跟踪所选组件的性能。为了提高安全性，管理员还应计划好更改预配置管理员帐户和用户帐户的默认密码。

需要在 CA PC 或 CA NPC 上将管理控制台注册为数据源。管理控制台的“管理配置”页面中的相应管理任务会被禁用。您可以从 CA PC 或 CA NPC 管理用户、角色、产品权限和组。

在 CA PC 中设置管理控制台用户之前，请熟悉 CA PC 或 CA NPC 中的管理控制台用户角色、组和产品权限。CA PC 或 CA NPC 安全功能 -- 包括用户、角色、产品权限、组和域 -- 允许您控制哪些用户可以在管理控制台中查看特定数据。

如果您还没有这样操作，请在 CA PC 或 CA NPC 上将管理控制台注册为数据源。有关在 CA PC 或 CA NPC 上将管理控制台注册为数据源以及在 CA PC 或 CA NPC 中管理用户安全的信息，请参阅联机帮助。

在 CA PC 中将管理控制台注册为数据源后，管理控制台中的工具栏将显示 CA PC 超链接。在 CA NPC 中将管理控制台注册为数据源后，管理控制台中的工具栏将显示 CA NPC 超链接。

如果您已注册管理控制台数据源但看不到 CA PC 或 CA NPC 超链接，请注销，然后重新登录管理控制台。

集成安全性

*用户帐户*可指定：

- 用于登录管理控制台的数据库凭据和身份验证方法。在 CA PC 或 CA NPC 中注册为数据源后，用户帐户可以用于登录管理控制台和 CA PC 或 CA NPC。
- 管理控制台角色，用于定义可供用户访问的管理控制台的报告页面（如“突发事件”页面）。
- 权限组，用于定义可供用户访问的报告数据（如特定域的数据）。
- 产品权限，用于在管理控制台中定义管理员级权限（如访问“管理配置”页面的权限）。

  要在管理控制台数据源上管理用户安全性，您必须使用具有“管理员”产品权限的用户帐户登录管理控制台。

默认管理员帐户 admin 已锁定，防止更改产品权限。必须拥有该帐户才能拥有针对所有已注册数据源的管理员权限。如果选择一组包括 admin 帐户的帐户，您将无法编辑任何选定帐户的产品权限。

请使用下列默认用户帐户或自行创建一个帐户。建议您尽快更改默认密码：

用户帐户	默认属性	默认密码
用户	权限：用户 角色：网络操作员 权限组：所有组 允许生成 URL：否	用户
admin	权限：管理员 角色：网络管理员 权限组：所有组 允许生成 URL：是 使用此帐户管理管理控制台用户。	admin
inv	权限：超级用户 角色：网络工程师 权限组：所有组 允许生成 URL：是	inv

产品权限

用户必须具有针对 CA Application Delivery Analysis 数据源的产品权限才能登录管理控制台。产品权限还指定对于“管理配置”页面的访问权限：

用户

提供对于管理控制台所有页面的访问权限，“管理配置”页面除外。

管理员

提供对于管理控制台所有页面的访问权限，包括“管理配置”页面。

超级用户

提供用户级产品权限，以及对于“SNMP 配置文件”、“网络设备”和“设备组”的“向我显示”菜单访问权限。

提示：如果用户无法登录管理控制台用户界面，请验证是否已授予该用户 CA Application Delivery Analysis 数据源的产品权限。

角色

基于角色的安全使得 CA Application Delivery Analysis 用户能够：

- 访问管理控制台的多个部分。
- 从 CA PC 或 CA NPC 视图深入查看管理控制台中的报告。

详细信息：

“深入查看数据源”权限 (p. 196)
角色权限 (p. 195)

角色权限

下表总结了适用于 CA Application Delivery Analysis（以前是 NetQoS SuperAgent）管理控制台的角色权限：

角色权限的名称	说明
工程	导航“工程”部分；创建“工程”报告
操作	导航“运行”部分；创建“运行”报告
管理	导航“管理”部分；创建“管理”报告
突发事件	导航“事件”部分；查看“事件”报告
调查	启动“调查”；深入查看“调查”中的数据

角色权限不会为 CA Application Delivery Analysis 用户提供：

- 访问 CA Application Delivery Analysis 管理控制台“管理配置”页面的权限。

  要为用户提供访问“管理配置”页面的权限，请为该用户提供对于 CA Application Delivery Analysis 数据源的管理员或超级用户产品权限。

- CA Application Delivery Analysis 管理控制台中报告数据的访问权限。

  要使得用户能够查看报告数据，请将相应的组分配给该用户。

详细信息：

产品权限 (p. 195)
用户和组 (p. 197)

“深入查看数据源”权限

“深入查看数据源”角色权限使用户能够从 CA PC 或 CA NPC 下钻到支持的数据源，包括 CA Application Delivery Analysis。此访问权限适用于分配给用户角色的所有数据源。

配置了 CA MultiPort Monitor 后，此角色权限还使用户能够从 CA Application Delivery Analysis 深入查看 CA MultiPort Monitor。

重要说明！ Multi-Port Monitor 不强制实施来自 CA PC 或 CA NPC 的权限集。例如，如果用户对特定的一组服务器有权限，并且 Multi-Port Monitor 可以至少监控该组中的一个服务器，则 Multi-Port Monitor 会显示域中所有服务器的性能数据。

详细信息：

角色 (p. 195)

用户和组

CA PC 和 CA NPC 中基于组的安全模型允许您授予对管理控制台中的报告数据的访问权限。默认情况下，CA PC 或 CA NPC 角色未向用户授予访问管理控制台数据源中的报告数据的权限。

创建组，以向用户授予访问管理控制台数据源中的部分应用程序、服务器和网络（而非所有应用程序、服务器和网络）的权限。要让用户对管理控制台中的某个组进行报告，您必须授予用户该组的访问权限。

系统组允许您授予用户管理控制台数据的访问权限。必要时，可以创建自定义组来指定您想让用户访问的数据。例如，要让用户对系统定义的应用程序进行报告，可创建包括服务器的服务器组，让这些服务器承载所需应用程序端口。

系统组

创建系统组，以报告来自多个管理控制台或域的数据：

所有应用程序

包括每个管理控制台数据源报告的所有应用程序。

所有域

包括每个域的组成员身份。

域

包括域的组成员身份。默认情况下，将显示“默认域”。

所有服务器

包括每个管理控制台数据源报告的所有服务器，以及在其他数据源中定义的服务器。

Application Delivery Analysis 网络

包括来自所有管理控制台数据源的网络。

数据源

包括将配置信息报告给 CA PC 或 CA NPC 的管理控制台数据源。管理控制台数据源包括自己的系统组。

如果您将 CA PC 用户帐户分配给包括所有系统组的“所有组”组，则用户将能够看到其角色选择中包括的所有报告中的所有管理控制台数据。

数据源系统组

数据源系统组由 CA PC 和 CA NPC 自动生成，从 CA Application Delivery Analysis 管理控制台和 CA PC 或 CA NPC 管理控制台都可启用特定 CA Application Delivery Analysis 数据源的基于组的报告。将生成以下数据源系统组：

所有应用程序

包括数据源报告的所有应用程序，并按以下类型对应用程序进行组织：

- 控制端口应用程序。
- FTP 应用程序。
- 标准应用程序。
- Web 应用程序。

所有网络

包括数据源报告的所有客户端子网，并按以下类型对网络进行组织：

- 域。如果您尚未实施域来分隔重复的 IP 通信量，则所有通信量都将包括在“默认域”中。
- 网络区域类型。

所有服务器

包括数据源报告的所有服务器，并按以下类型对服务器进行组织：

- 监视设备。显示分配给监视设备的服务器。
- 未分配。显示未分配给监视设备的服务器。

关联关系

包括按以下关系组织的服务器和应用程序：

- 应用程序到服务器。包括分配给某个应用程序的所有服务器。
- 服务器到应用程序。包括分配给服务器的所有应用程序。

详细信息：

管理承租人 (p. 87)
管理服务器 (p. 70)
按网络类型对客户端网络分组 (p. 45)
创建控制端口应用程序 (p. 114)
创建 FTP 应用程序 (p. 113)
创建标准应用程序 (p. 107)
创建 Web 应用程序 (p. 112)

针对组的提示

当您因报告目的对应用程序、网络和服务器进行分组时，请考虑以下问题：

- 应用程序。在单个组中仅包括同一应用程序的多个层。试图对可能是不同层中多个应用程序一部分的应用程序通信量进行分组，可能会产生不可预知的后果。例如，就整个企业来说，Telnet 应用程序可能会在属于多个多层应用程序一部分的服务器上运行。将某个报告的所有 Telnet 应用程序通信量分组到一起会产生误导性，使得管理控制台数据难以解释。
- 网络。我们建议创建自定义网络组。在报告中比较类似网络或查看所有具有特定带宽的网络时，这些组将很有用。您可以将具有类似网络往复传输时间的网络分组到一起，因为这些网络通常具有类似的带宽，或者您也可以按职能部门（如财务部门、测试部门和开发部门）对网络进行分组，以便比较各自的运行水平。
- 服务器。对特定应用程序进行故障排除时，服务器组将很有用。您可以创建一个包括该应用程序使用的所有服务器的组，以查找反常性能。

常见问题

- 为何用户无法登录管理控制台？

  如果用户无法登录管理控制台，请确保用户在 CA PC 或 CA NPC (p. 195)中对管理控制台数据源有产品权限。

- 用户登录管理控制台之后，为何某些页面会缺失？

  如果用户无法查看“操作”页面、“突发事件”页面、“管理”页面或“工程”页面，请确保该用户的角色 (p. 195)是正确的，且该角色的各项选择是适当的。对每个报告页面的访问权限受用户已分配角色中的选择项控制。

- 如果用户无法查看“管理配置”页面，请确保用户在 CA PC 或 CA NPC (p. 195)中对管理控制台数据源有产品权限。

- 为何管理控制台中没有报告数据？

  如果管理控制台中的页面未显示适当的数据，请确保用户在 CA PC 或 CA NPC (p. 195) 中对管理控制台数据源有产品权限。

- 我为什么不能从 CA PC 或 CA NPC 深入查看管理控制台？

  您的角色必须有“深入查看数据源 (p. 196)”角色权限，以及对管理控制台 数据源的适当页面的角色权限。

第 11 章： 系统管理

此部分包含以下主题：

Windows 管理员凭据

CA 设备附带了下列默认管理员帐户：

Windows 2008 操作系统

netqos/Changepassword1

Windows 2003 操作系统

netqos/changeme

nqadmin/qosisking

管理数据库

管理控制台承载用于数据存储和报告的 MySQL 数据库。

所需服务

正常运行时，管理控制台会自动启动下面列出的服务。

警告：为了避免数据丢失，请不要尝试手动停止或重新启动这些服务。要寻求帮助，请联系 CA Support：http://support.ca.com。

- **CA ADA Availability Poller。**如果承载应用程序的服务器受 CA Standard Monitor 监视，监控上的 CA ADA Availability Poller 服务会检查该应用程序的可用性。否则，将由 CA Standard Monitor 上的 CA ADA Availability Poller 服务检查该应用程序的可用性。
- **CA ADA Data Transfer Manager。**同步 Cisco WAE 设备，以便基于管理控制台上定义的应用程序、服务器和客户端网络来监视应用程序性能。
- **CA ADA Inspector。**将 5 分钟的由 CA ADA Master Batch 服务处理的 .dat 文件加载到数据库中，并与 CA ADA Inspector Agent 服务通信以启动调查。
- **CA ADA Inspector Agent。**如果承载应用程序的服务器由 CA Standard Monitor 监视，监控上的 CA ADA Inspector Agent 将对应用程序、服务器和相关网络启动调查。否则，将由 CA Standard Monitor 上的 CA ADA Inspector Agent 服务启动调查。
- **CA ADA Messenger。**同步监视 CA Standard Monitor、CA Multi-Port Monitor 和 CA GigaStor 监视设备，以便根据管理控制台中定义的应用程序、服务器和客户端网络来监视应用程序性能。
- **NetQoS MySql51 服务。**启动并停止承载管理控制台数据库的 MySql 服务器。
- **CA ADA Monitor。**CA ADA Monitor Service 位于管理控制台或 CA Standard Monitor 上，会从 CA GigaStor、Cisco WAE 或 Cisco NAM 设备接收镜像的 TCP 数据包和摘要文件。
- **CA ADA Data Pump。**对管理控制台数据库执行每周维护。
- **CA ADA Master Batch 服务。**在 CA Standard Monitor 上接收来自 CA ADA Batch 服务的数据文件，以便将其处理成 5 分钟的 .dat 文件。

数据库的状态

“数据库状态”页面概述了可用磁盘空间的容量、当前受监视的服务器、应用程序和网络的数目，以及数据库增长速度。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“控制台”、“数据库”、“状态”。

   将打开“数据库状态”。
3. 查看关于数据库增长的摘要统计信息。

   有关数据库摘要统计的信息，请单击“帮助”。

详细信息：

管理控制台如何管理数据库增长 (p. 228)

编辑数据库存储首选项

编辑数据库存储首选项，以便指定以下内容：

- 报告数据在数据库中保存多长时间
- 何时运行每周数据库维护
- 当可用磁盘空间降到指定阈值以下时，谁应该接收电子邮件或 SNMP 陷阱通知

硬盘驱动器全满或几乎全满会影响对现有数据进行的报告以及对新数据的收集。可以使用多个选项来设置数据存储时间以及要保留的数据类型。有关详细信息，请参阅下面的内容。默认情况下，管理控制台在存储以下类型的数据时，存储时间如下：

数据类型	存储以下时间内的数据	存储时间
历史突发事件记录	与 5 分钟数据存储时间一样长	1 到 12 个月
5 分钟数据	1 个月	1 到 12 个月
每小时数据	6 个月	1 到 12 个月
OLA 数据	13 个月	1 到 25 个月

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“控制台”、“数据库”、“维护”。

   将打开“数据库维护”。
3. 编辑数据库存储首选项
4. 指定在可用磁盘空间降到阈值以下时，管理控制台应如何通知您。

   有关设置数据库存储首选项的信息，请单击“帮助”。
5. 单击“确定”。

清除数据库中的数据

管理控制台会自动根据您指定的应用程序、服务器和网络定义来维护响应时间数据，因此通常不需要清除数据。如有必要，您可以清除所有数据及定义，或清除某特定类型的数据，如特定时段的 5 分钟数据。

数据一旦被清除，将无法恢复。建议您仅在 CA Support 请求清除数据的情况下才清除数据。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“控制台”、“数据库”、“清除数据”。

   将打开“清除数据”对话框。
3. 选择一个可清除数据库中所有数据的选项，或者指定要清除特定类型数据的时间范围，然后单击“确定”。

   如果管理控制台已在 CA PC 或 CA NPC 中注册为数据源，那么在从管理控制台数据库中清除所有数据前，请先注销管理控制台。清除完成后，在 CA PC 或 CA NPC 中将管理控制台重新注册为数据源。有关注销管理控制台的信息，请参阅 CA PC 或 CA NPC 联机帮助。
4. 系统提示您删除指定数据时，请单击“继续删除”。

备份和还原数据库

第一次安装管理控制台时，管理控制台不会在每周数据库维护过程中自动执行数据库备份。

由于各种情况都可能会导致数据库无法恢复，因此我们建议您每周排定和执行一次数据库备份。有关详细信息，请访问 CA Support 网站：http://support.ca.com。

管理控制台设置

将管理控制台设置用于：

- 查看管理控制台的名称。
- 管理电子邮件设置。

  在 CA PC 或 CA NPC 中注册为数据源后，电子邮件设置将由 CA PC 或 CA NPC 管理。如果未将管理控制台注册为数据源，请指定以下设置：

  - SMTP 服务器的 IPv4 地址。
  - 从管理控制台到指定 SMTP 服务器的出站 TCP-25 访问。
  - “回复”电子邮件地址。指定有效的回复电子邮件地址，防止垃圾邮件程序将电子邮件通知从管理控制台中筛选掉。
  - 电子邮件报告的首选图像格式：PNG 或 JPEG。
- 设置 NRTT 阈值以筛选使用“保持连接”消息的应用程序。
- 验证 NIC 的管理 IP 地址和顺序，并将管理控制台的管理 IP 地址发送到监视设备。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“控制台”、“设置”。

   将打开“控制台设置”。
3. 编辑控制台设置，然后单击“确定”。

   有关控制台设置的信息，请单击“帮助”。

详细信息：

应用程序保持连接消息 (p. 124)
更改 IP 地址 (p. 206)

更改 IP 地址

更改管理控制台的 IP 地址以满足您的需求。您必须以四部分、点分十进制表示法指定 IPv4 地址。

当您更改 IP 地址时，管理控制台会先提示您，然后才会对其监视设备进行自动更新以使用新的 IP 地址。重新启动与管理控制台相关的服务时，监视会暂时中断。

如果监视器 NIC 的 IP 地址不可路由，则不需更改它。

遵循这些步骤:

1. 在开始之前，请注销管理控制台。
2. 在管理控制台计算机上登录 Windows 并完成以下任务：
   a. 更新管理 NIC 属性，以便以四部分、点分十进制表示法指定 IPv4 地址。
   b. 在“服务”控制面板中，重新启动与 CA ADA 相关的服务。
   c. 注销。
3. 在 Web 浏览器中登录管理控制台。

   管理控制台会通知您管理控制台的 IP 地址已更改，并且会提示您选择要使用的 IP 地址：
   a. 选择新的 IP 地址，并选择相应的选项将新的 IP 地址通知给所有监视设备。
   b. 单击“确定”。
4. 确认监视设备正与控制台的已更新 IP 地址进行通信：
   a. 单击“管理配置”页面。
   b. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
   c. 滚动到“ADA 监视设备列表”，并确认每个监控的状态均为“运行”。

   必要时，可依次单击蓝色齿轮菜单 、“设置控制台”和“同步监视器设备”以更新所有监视设备上的管理控制台的 IP 地址。

管理 SNMP 配置文件

SNMP 配置文件可存储管理控制台进行以下操作所需的 SNMP 用户凭据：

- 查询以下设备上的 SNMP 代理：
  - 服务器或网络设备：目的是获取性能数据，以便响应服务器或网络设备上的突发事件，或者用作调查。
  - 路由器：目的是收集网络定义，或在跟踪路由调查过程中收集性能信息。

    您可以编辑 SNMP 配置文件，以便指定一个允许管理控制台在其上查询 SNMP 代理的端口。默认情况下，管理控制台通过 UDP-161 查询 SNMP 代理。
- 发送 SNMP 陷阱消息以响应服务器、应用程序、网络或监视设备上的突发事件。

  请注意，您无法更改通过管理控制台在其上发送 SNMP 陷阱的端口。管理控制台始终将 SNMP 陷阱发送到 UDP-162。

管理控制台支持使用 SNMPv1、SNMPv2 和 SNMPv3 对设备进行身份验证，并要求“只读”权限。

在 CA Performance Center 或 CA NetQoS Performance Center 中注册后，CA Performance Center 或 CA NetQoS Performance Center 会在管理控制台和任何其他已注册到该 CA Performance Center 或 CA NetQoS Performance Center 实例的 CA 产品之间同步 SNMP 配置文件更改。有关 CA Performance Center 和 CA NetQoS Performance Center 如何同步 SNMP 配置文件的详细信息，请参阅联机帮助。

SNMP 配置文件发现的工作方式

当管理控制台执行 SNMP 轮询请求时，如果没有为服务器或路由器分配有效的 SNMP 配置文件，管理控制台会尝试使用提供的 SNMP 配置文件列表与 SNMP 代理通信，以发现有效的 SNMP 配置文件。

CA Application Delivery Analysis 在 CA PC 或 CA NPC 中注册为数据源后，CA Application Delivery Analysis Manager 会使用从 CA PC 或 CA NPC 同步而且也已配置为包含在发现中的 SNMP 配置文件来发现有效的 SNMP 配置文件。

当管理控制台发现有效的 SNMP 配置文件时，管理控制台会将该 SNMP 配置文件分配给服务器或网络设备。如果管理控制台无法发现有效的 SNMP 配置文件，SNMP 轮询请求将超时。

管理控制台 SNMP 会对服务器或网络设备进行轮询以实现以下目的：

- 执行通过 SNMP 的性能调查
- 作为跟踪路由调查的一部分
- 从路由器导入网络定义

请注意，您可以将 SNMP 配置文件配置为不包括在发现过程中。建议您对可供发现的 SNMP 配置文件的数目进行限制。

添加 SNMP 配置文件

添加 SNMP 配置文件，使得管理控制台能够查询服务器或网络设备，并使用指定的 SNMP 用户凭据集发送 SNMP 陷阱。

当管理控制台在 CA PC 或 CA NPC 中注册为数据源时，请在 CA PC 或 CA NPC 中管理 SNMP 配置文件。CA PC 和 CA NPC 通过允许您指定您希望管理控制台及任何其他已注册数据源发现有效配置文件的顺序，来改善 SNMP 配置文件发现。

我们建议您对包括在管理控制台发现过程中的 SNMP 配置文件的数目进行限制。有关从 CA PC 或 CA NPC 配置 SNMP 配置文件的信息，请参阅联机帮助。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“调查”、“SNMP 配置文件”。

   将打开“SNMP 配置文件”。
3. 单击“添加 SNMP 配置文件”。

   将打开“SNMP 配置文件属性”。
4. 指定 SNMP 配置文件，然后单击“确定”。

   有关设置 SNMP 配置文件属性的信息，请单击“帮助”。

详细信息：

管理承租人 (p. 87)
SNMP 配置文件发现的工作方式 (p. 208)

编辑 SNMP 配置文件

使用“SNMP 配置文件”列表查看和管理管理控制台和 CA PC 或 CA NPC 之间的 SNMP 配置文件的列表。

如果您在 CA PC 或 CA NPC 中注册了管理控制台，并且 CA PC 或 CA NPC 更改了一个 SNMP 配置文件，更改会自动与管理控制台同步。有关对管理控制台中的 SNMP 配置文件所做的更改如何影响也在 CA PC 或 CA NPC 中注册的其他数据源的信息，请参阅联机帮助。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“调查”、“SNMP 配置文件”。

   将打开“SNMP 配置文件”。
3. 单击  以编辑 SNMP 配置文件。

   将打开“SNMP 配置文件属性”。
4. 编辑 SNMP 配置文件属性，然后单击“确定”。

   有关设置 SNMP 配置文件属性的详细信息，请单击“帮助”。

删除 SNMP 配置文件

删除 SNMP 配置文件，将其从管理控制台中删除。如果您已在 CA PC 或 CA NPC 中注册了管理控制台，CA PC 或 CA NPC 会将更改同步到任何其他已注册数据源。

如果将删除的 SNMP 配置文件分配给服务器或网络设备，管理控制台会取消对 SNMP 配置文件的分配。当管理控制台需要执行 SNMP 轮询请求时，如果服务器或路由器没有分配的 SNMP 配置文件，管理控制台会尝试发现一个。

如果您删除分配给 SNMP 陷阱通知的 SNMP 配置文件，管理控制台会自动更新 SNMP 陷阱通知，以便使用保留给 SNMP 陷阱的特殊 SNMPv2 配置文件 *SuperAgent*。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“调查”、“SNMP 配置文件”。

   将打开“SNMP 配置文件”。
3. 单击  以删除 SNMP 配置文件。
4. 系统提示您要删除 SNMP 配置文件时，请单击“继续删除”。

详细信息：

SNMP 配置文件发现的工作方式 (p. 208)

管理网络设备

如果您计划使管理控制台在某个网络设备上执行 SNMP 查询（例如，对路由器进行 SNMP 轮询以获取其性能信息），我们建议您将该网络设备添加到管理控制台中。

如果您没有向网络设备分配 SNMP 配置文件，管理控制台会尝试发现有效的 SNMP 配置文件。

管理控制台在遇到以下情况时会执行 SNMP 查询：

- 对路由器进行 SNMP 轮询 (p. 44)以获取网络信息。
- 启动通过 SNMP 的性能调查 (p. 158)。
- 启动跟踪路由调查 (p. 160)。

详细信息：

SNMP 配置文件发现的工作方式 (p. 208)

添加网络设备

添加任意类型的网络设备，以便对该设备进行调查。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“调查”、“网络设备”。
3. 在“向我显示”菜单下单击“添加网络设备”。

   将打开“设备属性”。
4. 指定网络设备属性，然后单击“确定”，或单击“保存并添加另一个”来添加另一个设备。

   有关设置网络设备属性的信息，请单击“帮助”。

查看网络设备调查

使用“网络设备列表”来查看任意网络设备调查的结果。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“调查”、“网络设备”。

   将打开“网络设备”。
3. 单击设备旁边的  以打开“调查报告”页面。
4. 在“调查报告”中指定搜索条件，然后单击“搜索”以筛选调查列表。

   “调查报告”内容将根据您选择的筛选相应更改。

   有关设置搜索条件的信息，请单击“帮助”。

编辑网络设备

编辑网络设备以更新其属性，例如，通过分配 SNMP 配置文件来编辑网络设备。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“调查”、“网络设备”。
3. 将打开“网络设备”。
4. 单击  来编辑设备。

   将打开“设备属性”。
5. 指定网络设备属性，然后单击“确定”，或单击“保存并添加另一个”来添加另一个设备。

   有关设置网络设备属性的信息，请单击“帮助”。

删除网络设备

删除网络设备，防止管理控制台对该设备进行调查。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“调查”、“网络设备”。
3. 将打开“网络设备”。
4. 单击 以删除网络设备。
5. 系统提示您要删除网络设备时，请单击“继续删除”。

用于调查的组网络设备

创建网络设备组，使管理控制台管理员能够针对一组网络设备排定或启动调查。例如，您可以对一组路由器进行 SNMP 轮询以获取性能信息。

添加网络设备组

要想让管理控制台管理员针对一组网络设备排定或启动调查，请添加网络设备组：

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“调查”、“设备组”。

   将打开“网络设备组”。
3. 单击“添加设备组”。

   将打开“设备组属性”。
4. 在“设备组名称”框中键入名称，然后单击“确定”。
5. 将设备添加到组，方法是：在“可用设备”列表中选择设备，然后单击右箭头将其移至“包括的设备”列表中。

   从组中移除设备，方法是：在“包括的设备”列表中选择设备，然后单击左箭头将其移至“可用设备”列表中。

查看针对网络设备组的调查

使用“网络设备组”列表来查看由管理控制台管理员运行的针对一组网络设备的调查。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“调查”、“设备组”。

   将打开“网络设备组”。
3. 单击设备组旁边的  查看其调查。
4. 将打开“调查报告”。
5. （可选）指定用来筛选调查列表的条件：

   调查类型

   要查看的调查的类型。单击“所有调查”或特定调查类型。

   目标类型

   要查看的调查目标的类型。单击“所有目标”或特定目标类型（设备、组，等等）。

   目标

   要查看的调查目标。按名称或 IP 地址选择特定目标。

   “调查报告”内容将根据您选择的筛选相应更改。

编辑网络设备组

编辑网络设备组，以便更改属于该组的网络设备的列表。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“调查”、“设备组”。
3. 将打开“网络设备组”。
4. 单击  来编辑设备。

   将打开“设备属性”。
5. 指定网络设备属性，然后单击“确定”，或单击“保存并添加另一个”来添加另一个设备。

   有关设置网络设备属性的信息，请单击“帮助”。

删除设备组

删除网络设备组，防止管理控制台对设备组进行调查。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“调查”、“设备组”。

   将打开“网络设备组”。
3. 单击 以删除设备组。
4. 系统提示您要删除设备组时，请单击“继续删除”。

管理排定电子邮件

管理控制台用户的产品权限决定了用户可以对报告执行哪些操作，例如：

- 具有查看报告权限的用户可以创建一个排定，以便通过电子邮件发送报告。
- 具有“管理员”产品权限的用户可以调整电子邮件报告的排定或电子邮件设置，并排定和发送有关监视设备的报告。

编辑电子邮件报告的排定

例如，在查看和管理排定电子邮件报告的列表时，可以更改电子邮件和排定选项。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“控制台”、“排定电子邮件”。
3. 将打开“排定电子邮件”。
4. 单击 以编辑排定电子邮件。

   将打开“排定电子邮件属性”。
5. 指定排定电子邮件属性，然后单击“确定”。

   有关设置排定电子邮件属性的信息，请单击“帮助”。

删除排定报告

要取消排定报告，请删除排定电子邮件。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“控制台”、“排定电子邮件”。
3. 将打开“排定电子邮件”。
4. 单击 以删除排定报告。
5. 在“删除确认”中，单击“继续删除”删除排定电子邮件。

执行系统维护

本节为系统管理员提供有关如何设置和维护 CA Application Delivery Analysis 的信息。

如何维护硬盘驱动器

管理控制台包含多个可持续访问以进行读/写操作的表。这些表占据了已安装管理控制台的驱动器上的大部分磁盘空间。随着时间的推移，这些 I/O 操作可能会形成磁盘碎片。

要维护硬盘驱动器，请执行以下任务：

- 对于 10 GB 以上的数据库，可每月对 D: 驱动器或安装了管理控制台的驱动器进行一次磁盘碎片整理。
  - 开始碎片整理过程之前，请确保该驱动器至少包含 20% 的可用磁盘空间。
  - 进行碎片整理之前，请停止所有与 CA ADA 相关的服务，包括 NetQoS MySql51 服务。
  - 碎片整理完成后，请重新启动这些进程。
- CA 产品经常对磁盘执行写入操作。在查找数据进行报告编译期间，驱动器头同时也在进行读写操作。这种随着时间的推移而累积的压力可能会导致故障，任何磁盘驱动器都是如此。要在尽量不丢失数据的情况下快速恢复，请排定一个固定的数据库备份时间。

详细信息：

备份和还原数据库 (p. 205)

如何更新系统安全并安装 Windows 更新

管理控制台在发送给用户时，已包含最新发布的 Windows 更新。请安装 Windows 更新和最新防病毒软件，以便持续对系统进行维护。考虑到安全和管理策略的多变性，我们禁用了 Microsoft 的自动更新功能。请按以下步骤启用自动更新：

1. 通过 Windows 控制面板启用自动更新。
2. 选择“有更新时通知我，但不自动下载或安装该更新”选项。此选项可防止导致系统不稳定的更新自动安装。
3. 安装重要 Microsoft 更新。不要安装推荐更新或驱动程序更新。
4. 应用某项更新后，请重新启动服务器。如果由第三方管理系统管理您的更新，请在应用更新之后确保该系统自动重启。

警告：CA Application Delivery Analysis 需要 Microsoft .NET Framework 版本 3.5。CA Application Delivery Analysis 与 Microsoft .NET 版本 4 或更高版本不兼容。如果 Windows 更新安装了 .NET Framework 版本 4 或更高版本，CA Application Delivery Analysis 可能停止工作。要纠正此问题，请在必要时卸载 .NET 版本 4 或更高版本，然后重新安装 .NET 版本 3.5。Microsoft 已经发布关于如何卸载 NET Framework 4 的知识库文章。

确保数据完整性并使用防病毒软件

请遵循下列准则以确保数据完整性：

- 如果您已在管理控制台设备上安装了防病毒软件，所有 NetQoS 目录均不得进行实时扫描和排定扫描以免数据库损坏。
- 如果您已将环境配置为从集中式防病毒系统推送规则，请增加一条规则以避免对下述目录进行扫描：
  - C:\Windows\Temp
  - D:\NETQOS（或安装 CA Application Delivery Analysis 的目录）和所有子目录。
- 如果自动备份在数据写入操作期间锁定数据库，则备份可能会损坏数据库。如果发生这种情况，请手动还原该数据库。
- 管理控制台不支持驱动器空间压缩。扩大驱动器空间虽然有很多优点，但可能会导致数据库损失或系统性能下降，因此并不值得。有关详细信息，请参阅 Microsoft 知识库文章：压缩卷上不支持 SQL Server 数据库。在该文中讨论的与压缩相关的问题也适用于 MySql 数据库。

详细信息：

备份和还原数据库 (p. 205)

第三方软件的问题

除防病毒软件、系统管理软件和时间同步软件以外，请不要在单机管理控制台或 CA Standard Monitor 上安装第三方软件，尤其是第三方网络监视软件（如 *Wireshark*）。第三方数据包驱动程序可能会干扰数据包监视并可能导致保修无效。

如果您在单机管理控制台或 CA Standard Monitor 上安装第三方软件，CA Support 可能会在进行故障排除之前要求您卸载该软件。

域组策略的问题

管理控制台和 CA Standard Monitor 设备运行 Windows 操作系统，因此可将其添加到 Windows 域中。可能会将安全策略和第三方软件推送到 CA Application Delivery Analysis 设备，具体取决于您的环境。安全策略和第三方软件可能会导致正常运行的设备出现问题。在向 Windows 域添加 CA Application Delivery Analysis 设备之前，请不要将安全策略和/或软件推送到服务器。

产品升级支持

如果您运行的是早期版本的 CA Application Delivery Analysis 且已购买了维护计划，请从 CA Support 网站 (http://ca.com/support) 下载最新版本

提示：在安装软件升级或内部版本之前，请重新启动服务器以确保 Windows 更新生效。不重新启动可能导致系统故障，并可能需要进行操作系统重建。

请求更换硬件

如果 CA Application Delivery Analysis 设备出现硬件故障（如硬盘、网络接口卡或 RAID 控制器故障），请联系 CA Support 请求进行更换。CA Support 会确认您什么时候需要更换硬件，并需要您提供以下信息：

- 服务器序列号
- 发生故障的硬件组件
- 加载到服务器上的 CA Application Delivery Analysis 软件和版本
- 加载到服务器上的操作系统版本
- 送货地址和收货人

当您的更换部件或服务器到达时，您会发现其中包括一个返回运输标签。请将故障部件或服务器重新包装好，然后将返回运输标签贴在包装盒上。

第 12 章： 监视设备管理

此部分包含以下主题：

监视设备的工作方式

管理控制台允许您混搭使用任何嵌入式仪器组合，不管该仪器是 Cisco 交换机基础架构、专用监视设备和数据包捕获设备还是 WAN 优化设备。这种用途广泛的监视体系结构在没有远程探测器或代理的情况下也可以工作，为网络组提供了一种经济有效的实现其应用程序交付目标的方法。

管理控制台整合了下列各类监视设备提供的响应时间数据：

监视设备	获取详细信息的位置
CA Multi-Port Monitor	*CA Multi-Port Monitor 用户指南*
CA Standard Monitor	使用 CA Standard Monitor 监视 (p. 247)
CA Virtual Systems Monitor	使用 CA Virtual Systems Monitor 监视 (p. 281)
CA GigaStor	使用 CA GigaStor 监视 (p. 301)
Cisco WAAS	使用 Cisco WAAS 监视 (p. 319)
Cisco NAM	使用 Cisco NAM 监视 (p. 349)
Riverbed Steelhead	使用 Riverbed Steelhead 监视 (p. 361)

监视器源的工作方式

监视设备可根据一个或多个监视器源计算响应时间度量标准。*监视器源*是响应时间数据源。例如：

- CA Standard Monitor 上的数据包监视器源接收镜像的 TCP 数据包。
- CA Multi-Port Monitor 上的多端口监视器源接收镜像的 TCP 数据包。
- CA Standard Monitor 或 CA Multi-Port Monitor 上的 WAN 优化监视器源从 Cisco WAE 设备接收数据包摘要文件。
- CA Standard Monitor 上的 Steelhead 监视器源接收 Steelhead 优化的数据包。
- CA Standard Monitor 或 CA Multi-Port Monitor 上的 GigaStor 监视器源从 CA GigaStor 接收数据包摘要文件。
- CA Application Delivery Analysis Manager 上的 NAM 监视器源从 Cisco NAM 接收度量标准摘要文件。

如果使用多个监视设备观测同一个服务器的通信量，管理控制台会自动将具有最佳响应时间数据源的监视器源分配给服务器。

如有必要，您可以通过编辑监视器源来分配：

- 备用监视器源。管理控制台会自动将最佳监视器源分配给服务器。如果您想让管理控制台自动监视其他监视器源的服务器（例如，当服务器迁移到其他位置时），请将备用监视器源分配给监视器源。
- 域。将域分配给监视器源可以让 CA Application Delivery Analysis 唯一标识服务器通信量。如果您想要监视重复的 IP 通信量，请将域分配给每一个监视器源。

详细信息：

创建一对监视器源 (p. 225)
监视器源分配的工作方式 (p. 223)
为监视器源分配域 (p. 92)

监视器源分配的工作方式

管理控制台可自动评估每个监视器源的服务器通信量，然后将最合适的监视器源分配给服务器。

当监视设备首次观测 TCP 会话时，管理控制台会将观测到最高入站数据包数据量的监视器源分配给服务器。在第一个小时内，分配每 5 分钟可能会变化一次，具体取决于哪一个监视器源具有最高数据包数据量。一小时后，监视器源上的数据包数据量必须明显增加才能让管理控制台自动更改监视器源分配。

如果数据包数据量类似，管理控制台会为监视器源分配较快的服务器连接时间 (SCT)。请注意，您可以覆盖自动监视器源分配，将特定监视器源永久分配给某个服务器。

在 WAN 优化的环境中，管理控制台会分配最优的数据包监视器源来监视服务器网段，并自动计算来自所有 WAN 优化设备的响应时间度量标准。

如果将服务器移至网络上的其他位置，自动分配的监视器源会自动变成能够观测服务器通信量的监视器源。管理控制台可能需要长达 1 小时的时间才能更改监视器源分配。

例如，为了在负载平衡配置过程中或进行灾难恢复和故障转移的时候让管理控制台从多个监视器源即时观测通信量，您可以将备用监视器源分配给监视器源。

详细信息：

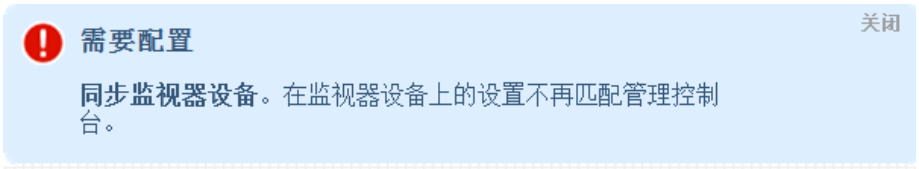
创建一对监视器源 (p. 225)
编辑服务器 (p. 73)

监视设备同步的工作方式

同步监视设备是为了让监视设备能根据管理控制台上当前的客户端网络、服务器子网和应用程序定义来同步监视应用程序性能。

为了确保同步期间最小化对监视的临时中断，请在同步监视设备之前完成所有更改。

如果监视设备尚未同步，系统会提示您进行同步操作：



此外，您也可以同步 (p. 233)特定 CA Standard Monitor 或 CA Multi-Port Monitor，或者 CA GigaStor。

详细信息：

执行基本操作 (p. 233)

创建一对监视器源

如果您已在 2 台交换机之间对服务器通信量进行了负载平衡，或者您拥有一台主交换机和一台用于故障转移的辅助交换机，则可创建一对监视器源，使得管理控制台能够自动监视两个监视器源中的已分配服务器。有了一对监视器源，就可以通过管理控制台即时报告任意一个监视器源中的应用程序通信量。

警告：如果一对监视器源观测到了相同的通信量，则会生成重复数据。

在故障转移的情况下，如果您没有创建一对监视器源且服务器已移至其他位置，则可能需要长达 1 小时的时间才能让管理控制台分配新的监视器源，并恢复对服务器承载的应用程序的监视。

例如，如果您有两台在负载平衡配置中充当对等方的交换机，则客户端网络和服务器之间的通信量可能会存在于任意一台交换机上，且每一台交换机的 SPAN 数据都会发送给不同的监视设备。如果某服务器与上述任意一个成对的监视器源关联，系统将从两个监视器源中收集该服务器的响应时间数据；实际上，该服务器有两个“最佳”监视器源。

就 WAN 优化的环境而言，管理控制台会自动计算所有 WAN 优化设备的响应时间，因此不需将 WAN 优化监视器源分配给服务器。

如果您创建了一对监视器源，请记住，主要和备用监视器源观测到的响应时间会存在差异。导致这种差异的因素很多，例如，监视设备的位置和该位置的可用服务器通信量，以及监视设备与服务器通信量之间距离的变化。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动至“ADA 监视设备列表”，并单击 来编辑 CA Standard Monitor 或 CA Multi-Port Monitor。

   将打开“监视器属性”。
4. 向下滚动至“监视器源”。
5. 单击 来编辑监视器源。
6. 单击“备用源”列表将备用监视器源分配给：
   - CA Standard Monitor 上的数据包监视器源。
   - CA Standard Monitor 或 CA Multi-Port Monitor 上的 WAN 优化或 GigaStor 监视器源
   - CA Multi-Port Monitor 上的多端口监视器源。

7. 单击“更新”应用您所做的更改。

详细信息：

管理承租人 (p. 87)
监视设备的工作方式 (p. 221)

查看会话信息

管理控制台显示存在于监视器源、监视设备或所有监视设备上的基于 IPv4 的 TCP 会话活动量的相关信息。

请使用活动会话信息来确认监视器源正在监视 TCP 会话。管理控制台会报告由服务器上的监控根据应用程序端口观测到的活动 TCP 会话的数目。子应用程序在该报告中会被视为父级的实例；例如，同一 Web 应用程序服务器的两个 URL 都将计为该 Web 服务器的活动。它不是服务器上已配置应用程序的计数。

在监视器源上查看活动会话

请使用“活动会话”页面查看在最后 5 分钟报告间隔期间监视器源报告的基于 IPv4 的活动 TCP 会话数目。

此外，您也可以查看最近一小时内由监控或管理控制台报告的活动会话信息。

请注意，NAM 监视器源不报告活动会话信息，因为 Cisco NAM Metric Agent 会计算自己的响应时间度量标准，因此不包括计算会话信息所需的 TCP 标头。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“ADA 监视设备列表”，然后单击 使用您所需的监视器源来编辑 CA Standard Monitor 或 CA Multi-Port Monitor。

   将打开“监视器属性”。

   请使用“已分配”列查找已分配 Cisco WAE 或 CA GigaStor 的 CA Standard Monitor 或 CA Multi-Port Monitor。
4. 单击“监视器源”下的“查看活动会话”。请注意，活动会话信息不适用于 Cisco NAM 监视器源。

   将打开“活动会话”。
5. 单击展开某个服务器，然后查看其活动会话信息。
6. （可选）单击“电子邮件”以电子邮件方式发送活动会话信息。有关指定电子邮件属性的信息，请单击“帮助”。

   要发送电子邮件，必须对管理控制台上的电子邮件设置 (p. 205)进行适当的配置。
7. （可选）单击蓝色齿轮菜单 ，然后选择“重新加载会话”以使用最近 5 分钟报告间隔的活动会话信息刷新列表。
8. （可选）单击“查看源的活动会话”，然后选择您要为同一监视设备上的另一个监视器源查看活动会话信息的监视器源。

详细信息：

查看会话计数的每小时摘要 (p. 228)

查看会话计数的每小时摘要

使用每小时摘要信息以按应用程序、服务器和监控查看基于 IPv4 的 TCP 会话计数，例如：

- 查看每个监控上的会话总数，并查看每个服务器上由特定监控观测到的会话计数。
- 按应用程序查看会话总数，并查看每个承载该应用程序的服务器上的会话计数。
- 按服务器查看会话总数，并查看每个由服务器承载的应用程序上的会话计数。

管理控制台会使用最后 5 分钟间隔期间观测到的基于 IPv4 的 TCP 会话自动更新会话信息。请注意，Cisco NAM 监视设备不提供会话信息。

重置每小时摘要信息即可开始报告最新会话信息。或者，您可以查看特定监视器源最近 5 分钟间隔内的会话信息。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“控制台”、“会话列表”。

   将打开“会话列表”。
3. 通过“监视设备”、“应用程序”和“服务器”浏览会话列表，然后展开一个列表查找您要的信息。
4. （可选）单击“重新加载会话”来重置每小时摘要。
5. （可选）通过单击蓝色齿轮菜单 ，来发送以列表形式列出摘要信息的电子邮件。

详细信息：

在监视器源上查看活动会话 (p. 227)

管理控制台如何管理数据库增长

管理控制台根据您所指定的服务器子网、客户端网络和端口排除来监视每台服务器上最繁忙的应用程序。管理控制台会尝试最大化其数据库资源，但请务必确保数据库不会不受管理。

数据库容量

管理控制台自动限制数据库的增长不超过 1.2 亿行。*行*包含 5 分钟间隔内服务器上承载的应用程序和客户端网络之间 TCP 会话的性能度量标准。请注意，组合的网络部分可能是实际的客户端 IP 地址，也可能是子网中所有客户端 IP 地址的聚合（前提是您已为网络定义了 /23 或更低的掩码。

管理控制台可以监视更多或更少的组合，具体取决于您希望管理控制台保存 5 分钟行数据的天数。默认情况下，管理控制台会将 5 分钟数据保留 1 个月，平均起来，这相当于每天要将大约 4 百万新行存储到数据库中。

为了更好地理解管理控制台是如何控制数据库增长的，请考虑以下示例：

- 一组 254 名会计全都在同一个 /24 网络上访问单个服务器上承载的同一个应用程序。
- 会计每天工作 8 小时，但考虑到午餐和休息因素，实际上一名会计每天访问会计应用程序的时间大约在 6 小时左右。
- 这种情况下，管理控制台每天会在数据库中创建约 18000 行的数据。[254 名会计 x 1 个应用程序 x 1 个服务器 x 6 小时 x 12 行/小时（每 5 分钟一次） = 18,288 行]

仍以上述示例为例，管理控制台可以监视大约 220 组会计人员，超过这个数目就必须对数据库的大小进行管理。

数据库增长控制

要管理最多 1.2 亿行数据，管理控制台可执行以下操作：

- 使用“网络往复传输响应时间”(NRTT) 的最小阈值筛选每个组合，以便限制周期性客户端和服务器消息（如保持连接消息）对监视报告中统计信息的影响，并控制数据库增长。

  如果 5 分钟间隔期间的 NRTT 观测数目达不到最小阈值，管理控制台就不会在数据库中为该组合创建行。

  从报告的角度来说，筛选后的组合会阻止管理控制台报告筛选出的 5 分钟间隔的会话级统计信息，但跨网络的应用程序的响应时间度量标准仍然有效。

  如果您不希望管理控制台筛选或梳理某个应用程序，可以对该应用程序提高优先级 (p. 94)。

  默认情况下，管理控制台会筛选在 5 分钟间隔期间少于10 个 NRTT 观测数 (p. 205)的非优先应用程序的组合。

- 如果行创建速率的移动平均值过高，管理控制台会通过梳理具有最小数目应用程序/服务器/网络组合的低数据量应用程序，来限制传入行的数目。当管理控制台*梳理*某个应用程序时，就不会在数据库中为应用程序/服务器/网络组合创建行。管理控制台不会梳理服务器上的优先应用程序或最繁忙的应用程序。

  通过梳理，可以帮助管理控制台将数据库的行数限制在最多不超过 1.2 亿，同时还可以让您根据需要的月度时段来报告最想关注、具有最高应用程序/服务器/网络组合数目的应用程序。当行创建的移动平均值回到某个可以接受的速率时，管理控制台会禁用梳理。

  从报告的角度看，管理控制台会将已梳理的应用程序数据分级为“没有数据”（白色）。

  如果您不希望管理控制台筛选或梳理某个应用程序，可以对该应用程序提高优先级 (p. 94)。

- 如果梳理不能成功降低行创建速率的移动平均值，管理控制台将不会为具有最小数据包数据量的非优先应用程序组合创建行。当行创建的移动平均值回到可接受的速率时，管理控制台会恢复对非优先应用程序的常规监视。

  从报告的角度来说，筛选后的组合会阻止管理控制台报告筛选出的 5 分钟间隔的会话级统计信息，但跨网络的应用程序的响应时间度量标准仍然有效。

  如果您不希望管理控制台筛选或梳理某个应用程序，可以对该应用程序提高优先级 (p. 94)。

监视设备比率

监视设备比率视环境而定，并取决于您将管理控制台配置为监视何种对象。尤其是，客户端网络数目往往会对生成的数据量产生很大影响。

如果您正在评估管理控制台，请使用评估的每日数据库增长速率 (p. 203)来预计用于生产的每日数据库行增长的情况。

切记，如果使用默认数据保留设置，则平均起来管理控制台可以每天创建多达 400 万行的数据。某些情况下，尤其是在客户端网络数目较大的情况下，CA Multi-Port Monitor 可以每天生成 400 万行的数据。如果每日数据库行增长速率超过阈值，管理控制台会自动管理数据库的大小。

将监视设备添加到管理控制台中时生成的处理负载可表示为一个*监视单位*。例如，一个 CA Standard Monitor 使用一个监视单位。管理控制台最多可支持 15 个监视单位。

以下列表概述了采用监视单位表示的每类监视设备的等效处理负载：

监视设备	监视单位
CA Multi-Port Monitor	5
CA Standard Monitor	1
CA Virtual Systems Monitor	.5（ESX 主机上层之间的通信量）
CA GigaStor	每 1 Gbps SPAN 1 个监视单位
Cisco WAE（多达 5 万个优化连接）	1
Cisco NAM-2 Blade（最高 1 Gbps）	1
Cisco NAM 2204 设备（最高 2 Gbps）	2
Cisco NAM 2220 设备（最高 5 Gbps）	5

无需任何有关每日数据库增长的信息，您就能预计到管理控制台可以支持以下监视设备配置之一：

- 30 个 CA Virtual Systems Monitor 监视设备，用于监视 ESX 主机上服务器间的通信量
- 3 个 CA Multi-Port Monitor 设备
- 10 个 Cisco NAM-2 Blade 和 1 个 CA Multi-Port Monitor
- 5 个 CA GigaStor 设备

监视设备推荐

要优化管理控制台数据库资源，请遵循下列准则：

- 如果可能，请使用物理监控通过物理交换机进行监视，而不要使用 CA Virtual Systems Monitor 通过虚拟交换机进行监视。例如，通过物理“分布”层交换机来监视客户端-服务器通信量，而不要使用具有 Web 服务器层的 ESX 主机上的 CA Virtual Systems Monitor 进行监视。

  物理交换机具有最佳 SPAN/VACL 功能，而且在您运行该功能时，物理交换机的性能不受影响。CA Virtual Systems Monitor 是 ESX 主机上的访客，因此会消耗系统资源。此外，Web 层是最难以监视的一层，因为该层涉及到客户端网络。因此，如果您从物理领域有更好的选择，就不要把 ESX 性能弄得太复杂。

- 使用物理监控通过物理交换机进行监视时，请尽可能靠近服务器进行监视。当监视设备接近服务器时，服务器度量标准的检测将更为准确，可以让管理控制台清楚地区分到底是网络还是服务器突发事件。

- 如果安装了 CA Multi-Port Monitor，您可以充分利用具有基于硬件筛选功能的监控上的 SPAN 聚合，从而大大提高工作效率。

  或者，您也可以在镜像交换机端口和监控之间放置一个矩阵交换机。这种投资在大环境中可以获得巨大回报。使用矩阵交换机或网络工具优化器来筛选不需要的线速通信量，并将精心处理过的数据包流发送到 CA Multi-Port Monitor 或 CA Standard Monitor 的每个端口。该方法具有以下优势：

  - 在变更窗口期间，通常您可以调整矩阵交换机数据（而不必与交换机管理员协调）来配置物理交换机。
  - 基于硬件的线速筛选不影响系统 CPU 或内存。
  - CA Standard Monitor 或 CA Virtual Systems Monitor 上提供的基于软件的筛选，会消耗大量 CPU 并降低监控吞吐量。
  - 前期成本和总拥有成本均较低。
  - 考虑到效率，比较实际的做法通常是在“接入”层（更靠近服务器）进行收集，而不是仅在“分布”层进行收集。

- 调整准则是通用的， 但每个环境的具体情况有所不同。拇指规则虽然有用，但实际容量取决于应用程序通信量的性质以及配置。

  管理控制台不会限制受监视的应用程序、服务器、CPU 或客户端网络的数目。在每个特定环境的独特特征所决定的最大容量范围内，管理控制台管理员可以自由使用管理控制台和监视设备。

- 请仔细定义下述项目，以便对管理控制台尝试监视的内容进行限制：

  - 应用程序端口排除。
  - 服务器子网。

  - 客户端网络。
- 删除不太重要的应用程序（如备份应用程序）。
- 将 24 位客户端网络聚合成更广的子网（如 /22 网络）。该方法可限制管理控制台确定哪些 TCP 客户端受性能下降影响的能力，但同时也会减少在数据库中创建的行的数目。

详细信息：

客户端网络的工作方式 (p. 27)
删除系统定义的应用程序 (p. 105)
删除用户定义的应用程序 (p. 118)
端口排除的工作方式 (p. 97)
服务器的工作方式 (p. 61)

执行基本操作

使用蓝色齿轮菜单 对列表中的所有监视设备执行基本操作。切记：

- “ADA 监视设备列表”包括 CA Standard Monitor、CA Virtual Systems Monitor 和 CA Multi-Port Monitor
- “WAN 优化设备列表”包括 Cisco WAE 设备
- “CA GigaStor 设备列表”包括 CA GigaStor 设备

在 Cisco NAM 上没有要执行的基本操作。

管理监视设备突发事件

管理监视设备突发事件，确保您的监视设备工作正常。如果出现以下情况，管理控制台将默认打开监视设备突发事件：

- 管理控制台不接收来自监视设备的数据，时间长达 15 分钟。例如，如果将 Cisco WAE 分配给 CA Multi-Port Monitor，且 Cisco WAE 停止生成响应时间数据，则在 15 分钟后，管理控制台将会为 Cisco WAE 创建监视设备突发事件。假定 CA Multi-Port Monitor 继续在至少一个逻辑端口上处理响应时间数据，那么管理控制台就不会为 CA Multi-Port Monitor 创建监视设备突发事件。
- CA Standard Monitor 或 CA GigaStor 无法处理超过 5% 的已接收数据包。
- 管理控制台无法访问 CA Standard Monitor 或 CA Multi-Port Monitor，时间长达 5 分钟。

要将突发事件通知给监视设备的所有者，请为监视设备分配突发事件响应。

当触发监视设备突发事件的条件不再存在时，管理控制台将自动关闭监视设备突发事件。因此，您不需要确认监视设备突发事件。

请注意，CA Multi-Port Monitor 会执行某些自我监视操作并通过发送 SNMP 陷阱通知，提醒您存在可能会影响其性能的条件。

详细信息：

分配监视设备突发事件响应 (p. 242)

查看监视设备突发事件

使用“监视器设备突发事件”列表来查看监视设备突发事件的摘要，并显示特定突发事件的报告详细信息。筛选列表以选择您要的突发事件状态和监视设备。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“控制台”、“监视设备突发事件”。
3. 复查“监视器设备突发事件”列表中的突发事件历史记录。

   有关突发事件状态的信息，请单击“帮助”。
4. 选择下面的某个选项来筛选需要的突发事件列表：

   设备

   从该列表中选择监视设备，或使用默认值“全部”来查看每个 CA Standard Monitor 的所有突发事件。

   突发事件状态

   选择需要的突发事件状态：“打开”、“已关闭”或“打开和已关闭”。

   最小严重度

   选择“重大”或“不可用”来筛选突发事件列表。与其他阈值不同，监视设备突发事件阈值的严重度级别为“重大”或“不可用”。
5. 单击列上的“突发事件”中的时间戳条目，来查看突发事件报告详细信息。

详细信息：

编辑监视设备突发事件阈值 (p. 236)
启用和禁用可用性监视 (p. 237)

编辑监视设备突发事件阈值

设置监视设备突发事件阈值，确保您的所有监视设备正在向管理控制台发送数据。根据监视设备的类型，您可以为已丢弃或已分段数据包配置一些其他的阈值。

请注意，您无法调整监视设备可用性的突发事件阈值。

指定以下项目的监视设备阈值：

- 数据非活动状态。如果管理控制台停止从任何类型的监视设备接收数据，管理控制台就会创建一个“重大”（橙色）监视设备突发事件。

  如果管理控制台停止从监视设备接收性能数据，它会认为监视设备处于*非活动状态*。发生以下情形时，可能会出现这种情况：

  - 网络故障；没有数据生成。
  - 监视设备故障；虽然生成了数据，但监视设备处于非活动状态。
  - SPAN 丢失；虽然生成了数据，但 SPAN 处于非活动状态。
- 数据包被监控丢弃。如果 CA Standard Monitor 或 CA GigaStor 过于繁忙无法处理所有接收到的数据包，且数据包捕获驱动程序丢弃过多数据包，则管理控制台会创建“重大”（橙色）监视设备突发事件。管理控制台不在交换机端口或监控上的监视器 NIC 上监视数据包丢失情况。该阈值仅适用于 CA Standard Monitor 或 CA GigaStor。

  如果 CA Standard Monitor 或 CA GigaStor 持续丢弃数据包，请排除已丢弃数据包故障 (p. 279)。
- 已分段数据包。如果 CA Standard Monitor 或 CA GigaStor 收到已分段数据包，管理控制台将会创建“重大”（橙色）监视设备突发事件。默认情况下，该阈值处于禁用状态。该阈值仅适用于 CA Standard Monitor 或 CA GigaStor。

  如果持续出现已分段数据包，则可能是因为存在以下某个条件：

  - 网络上发生恶意攻击。
  - 网络上设备（如路由器或服务器）的最大传输单位 (MTU) 设置可能不正确。确认您已在整个网络上应用了一致的 MTU 设置，防止出现数据包分段。如果 MTU 太大，则当数据包碰到无法处理该大小的数据包的路由器时，可能会出现重传的情况。如果 MTU 太小，则标头开销和需要发送和处理的确认的数目会增加。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“性能阈值”。

   将打开“监视设备阈值列表”。

3. 单击 编辑监视设备阈值，然后单击“确定”。

   将打开“监视设备阈值”。

   有关设置监视设备突发事件阈值的信息，请单击“帮助”。

启用和禁用可用性监视

默认情况下，当管理控制台无法访问 CA Standard Monitor、CA Virtual Systems Monitor 或 CA Multi-Port Monitor 时间长达 5 分钟时，管理控制台将打开“不可用”突发事件。要防止管理控制台在监视设备上打开“不可用”监视设备突发事件，请在设备上禁用可用性监视。

可用性监视不适用于其他类型的监视设备。请注意，您无法为可用性指定监视设备阈值。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动至“ADA 监视设备列表”，然后单击 来编辑 CA Standard Monitor 或 CA Multi-Port Monitor。

   将打开“监视器属性”。
4. 单击“可用性监视”启用可用性监视，然后单击“确定”。

为监视设备添加突发事件响应

添加突发事件响应，让管理控制台可以启动通知以响应监视设备突发事件。与针对应用程序、服务器和网络的突发事件响应不同，监视设备突发事件响应可按严重度（“重大”或“不可用”）来筛选，但不能按持续时间来筛选。

默认情况下，管理控制台不会针对监视设备突发事件启动通知。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“突发事件响应”。
3. 在“向我显示”菜单下，单击“添加监视设备响应”。

   将打开“监视器设备突发事件响应属性”。
4. 键入突发事件响应名称，然后单击“应用”。
5. 在第三个“向我显示”菜单中，单击“编辑操作”。
6. 在“向我显示”菜单中，单击“添加操作”。

   将打开“监视设备操作类型”。
7. 单击某个操作，然后单击“下一步”。

   将打开“监视器设备操作属性”。
8. 填写“监视器设备操作属性”中的字段，然后单击“确定”。

   有关设置监视设备操作属性的信息，请单击“帮助”。

   所做的更改将自动应用到带有分配的突发事件响应的监视设备。

详细信息：

将操作添加到监视设备突发发事件响应 (p. 240)

编辑监视设备突发事件响应名称

可以编辑监视设备突发事件响应并对它进行重命名。监视设备突发事件响应被重命名后，系统会将对名称的更改应用到带有该突发事件响应的所有监视设备。

编辑监视设备突发事件响应时，也可以修改其响应操作，例如编辑或添加某个操作。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“突发事件响应”。

   将打开“监视设备突发事件响应”。
3. 单击 来编辑监视设备突发事件响应。

   确认已为每个突发事件响应分配至少一个响应操作，并且已为每个监视设备分配突发事件响应。
4. 在第三个“向我显示”菜单中，单击“编辑突发事件响应”。

   将打开“突发事件响应名称”。
5. 键入突发事件响应名称，然后单击“确定”。

详细信息：

将操作添加到监视设备突发发事件响应 (p. 240)
删除响应操作。 (p. 241)
编辑响应操作 (p. 241)

删除监视设备突发事件响应

删除突发事件响应将会删除突发事件响应及其响应操作。如果突发事件响应已分配，删除后，管理控制台将会为所有受影响的应用程序、服务器或网络重新分配默认突发事件响应。

在删除突发事件响应之前，请确保已对默认突发事件响应进行了正确的设置，或者向受影响的应用程序、服务器或网络分配新的突发事件响应。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“突发事件响应”。

   将打开“监视设备列表”。
3. 单击 删除监视设备突发事件响应。请注意，您无法删除网络、服务器或应用程序的“默认”突发事件响应。

   管理控制台会自动将监视设备恢复为“默认”突发事件响应。

将操作添加到监视设备突发发事件响应

可以为突发事件响应添加操作，以便管理控制台能够启动一个或多个通知或调查来响应监视设备突发事件。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“突发事件响应”。

   将打开“监视设备突发事件响应”。
3. 单击 编辑突发事件响应。
4. 在第三个“向我显示”菜单中，单击“编辑操作”。
5. 在“向我显示”菜单中，单击“添加操作”。

   将打开“操作类型”。
6. 选择一个操作，然后单击“下一步”。

   将打开“操作属性”。
7. 填写“操作属性”中的字段，然后单击“确定”。

   有关设置操作属性的信息，请单击“帮助”。

   新操作将显示在“突发事件响应操作”中。

编辑响应操作

编辑响应操作，修改对监视设备突发事件的响应。默认情况下，管理控制台不会针对监视设备突发事件启动通知或调查。

编辑默认的突发事件响应，以便添加一个或多个响应操作，并根据需要创建其他突发事件响应。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“突发事件响应”。

   将打开“突发事件响应”。
3. 单击 来编辑监视设备突发事件响应。
4. 在第三个“向我显示”菜单中，单击“编辑操作”。

   将打开“突发事件响应操作”。
5. 单击 来编辑操作。

   将打开“操作属性”。
6. 编辑响应操作设置，然后单击“确定”。有关详细信息，请单击“帮助”。

删除响应操作。

如果您不希望继续让管理控制台启动特定的响应操作，可将该操作从监视设备突发事件响应中删除。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“策略”、“突发事件响应”。

   将打开“突发事件响应”。
3. 单击 来编辑监视设备突发事件响应。
4. 在第三个“向我显示”菜单中，单击“编辑操作”。

   将打开“突发事件响应操作”。
5. 单击 来删除操作。
6. 在“删除确认”中，单击“继续删除”来删除该响应操作。

详细信息：

为监视设备添加突发事件响应 (p. 238)

分配监视设备突发事件响应

响应监视设备突发事件时，管理控制台可以发送：

- 电子邮件通知
- SNMP 陷阱通知

创建带有您要的响应操作的突发事件响应，或者将操作分配给默认的监视设备突发事件响应。默认突发事件响应不包括操作。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。

   将打开监视设备列表。
3. 浏览到某个监视设备列表，然后单击 对监视设备进行编辑。

   将打开“监视器属性”。
4. 单击“突发事件响应”，从列表中选择一个突发事件响应，然后单击“确定”。

排除监视故障

此部分描述您在监视 TCP 通信量的过程中可能会碰到的问题，以及纠正这些问题的步骤。

详细信息：

监视设备的工作方式 (p. 221)

查看监视设备状态

CA Standard Monitor、CA Virtual Systems Monitor 和 CA Multi-Port Monitor 可以处理管理控制台的传入响应时间数据。使用“ADA 监视设备列表”来查看 CA Standard Monitor、CA Virtual Systems Monitor 或 CA Multi-Port Monitor 的状态，并验证监控最近已处理来自其监视器源的传入数据。

如果监控的状态不是“正在运行”，请先排除监控以及任何分配的监视设备（如 CA GigaStor）的故障。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。

   将打开“ADA 监视设备列表”。
3. 使用“状态”列来确定监控状态：

   正在运行

   监控正在从监视器源接收性能数据。

   已停止

   表示管理控制台目前未从监控接收性能数据，但可以连接到监控的 IP 地址。

   无法连接

   表示管理控制台无法连接到监控的管理 IP 地址。

   从未连接

   表示管理控制台从未连接到监控，您需要同步监控，以便基于管理控制台上目前定义的客户端网络、服务器子网和应用程序来收集性能数据。如有必要，可使用“设置控制台”命令更新监控，以便与管理控制台进行通信。

   已停止 - 没有数据

   表示数据包监视已被禁用，监控不会从 Cisco WAE 设备、Cisco NAM 设备或 CA GigaStor 接收摘要文件。
4. 使用“上次监视”列验证监控是否已在过去的 5 分钟内处理来自其监视器源的传入数据。
5. 要立即刷新状态信息，请单击蓝色齿轮菜单 ，然后单击“更新状态”。

详细信息：

监视设备操作 (p. 261)

排除通信故障

要报告应用程序响应时间，ADA 管理器及其监视设备必须能够相互进行通信。

验证	可以
ADA Manager	■ 在 TCP-3308 上与本地 mySQL 数据库通信 ■ 在 TCP-1000、TCP-1001 和 TCP-7878 上与 Standard Monitor 或 Virtual Systems Monitor 通信 ■ 在 TCP-80 和 TCP-8080 上与 Multi-Port Monitor 通信 ■ 在 TCP-8381 上与 SSO 通信
Standard Monitor 或 Virtual Systems Monitor	■ 在 TCP-80 和 TCP-8080 上与 ADA 管理器通信
Multi-Port Monitor	■ 在 TCP-80 和 TCP-8080 上与 ADA 管理器通信
与 Cisco NAM 上的 Cisco NAM Metric Agent 通信	■ 在 TCP-9996 上与 ADA 管理器通信
与 Cisco WAE 设备上的 Cisco WAAS Flow Agent 通信	■ 在 TCP-7878 上与 Standard Monitor 通信 ■ 在 TCP-7878 上与 Multi-Port Monitor 通信 ■ 在 TCP-7878 上与 ADA 管理器通信
与 GigaStor 上的 GigaStor 连接器通信	■ 在 UDP-9995 上与 Standard Monitor 通信 ■ 在 UDP-9995 上与 Multi-Port Monitor 通信 ■ 在 TCP-1001 上与 ADA 管理器通信

排除缺少数据故障

如果管理控制台不报告应用程序、服务器或网络的情况，请验证 (p. 226)控制台能够查看应用程序和服务器的 TCP 会话。

如果控制台未检测到 TCP 会话，请验证以下内容：

- 端口排除没有将应用程序数据筛选掉。有关详细信息，请参阅应用程序端口排除 (p. 96)。
- 对服务器子网进行定义 (p. 65)时，要求至少有一个承载应用程序通信量的服务器。
- 对客户端网络进行定义 (p. 35)时，要求可以通过客户端 IP 与应用程序通信。
- 监视设备经过同步 (p. 224)后，可以监视在管理控制台上定义的应用程序、服务器和网络。
- 如果您已经实施域，确认您已经将正确的域分配给监视设备、服务器和客户端网络。

第 13 章：使用 CA Standard Monitor 监视

此部分包含以下主题：

CA Standard Monitor 作为监视设备的工作方式

CA Standard Monitor 可以作为 CA Application Delivery Analysis 的一种监视设备来运行。CA Standard Monitor 最多从 2 个端口被动监控数据中心通信，并帮助保留端对端系统性能的连续记录。CA Standard Monitor 与管理控制台驻留在同一台服务器上，因此，管理控制台了解监控。您可以部署其他监视设备对服务器交换机端口的镜像 TCP 通信量进行被动监视。此外，CA Standard Monitor 还可以为其他类型的监视设备（如 CA GigaStor）计算响应时间度量标准。

注意：有关安装 CA Standard Monitor 的信息，请参阅 *《安装指南》*。

CA Standard Monitor 的工作方式

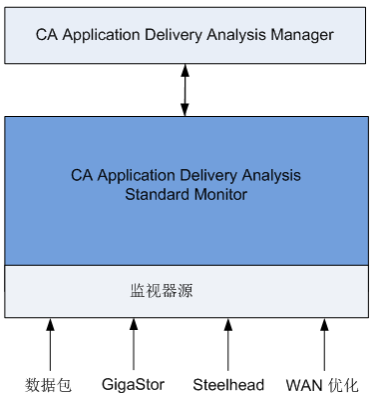
如下图所示，CA Standard Monitor 可以接收和处理来自多个源的性能数据，这些源包括：

- 数据包监视器源，其在监视器 NIC 上从 SPAN 端口或镜像端口或网络分流器接收基于 IPv4 的 TCP 数据包，通过 CA Standard Monitor 处理数据，计算响应时间统计信息并将其发送到管理控制台以显示在报告中。要获得最佳结果，我们建议您使用主交换机提供的本地 SPAN。
- GigaStor 监视器源，其在管理 NIC 上从 CA GigaStor 接收数据包摘要文件，处理基于 IPv4 的 TCP 标头信息，并将响应时间统计信息发送到管理控制台，以显示在报告中。
- Steelhead 监视器源，其从 Steelhead 设备接收基于 IPv4 的 Steelhead 优化数据包。
- WAN 优化监视器源，其从 IPv4 Cisco WAE 设备接收数据包摘要文件。

根据您所指定的应用程序端口、服务器和客户端网络的列表，监控可为其观测到的所有匹配的服务器-应用程序-网络通信创建响应时间统计信息。管理控制台使用该信息自动监视每个服务器上最忙的 TCP 应用程序。您也可以定义要监视的应用程序，然后将该配置加载到 CA Standard Monitor 上。

管理控制台评估来自所有监视设备的响应时间度量标准，以便为每个服务器分配最佳监视器源，并监视每个服务器上最繁忙的 TCP 应用程序。

如果要配置 CA Standard Monitor 从 CA GigaStor 接收数据包摘要，建议您不要配置监控同时接收镜像的数据包。



请注意，单机管理控制台在其数据包监视器源上接收镜像 TCP 数据包。

详细信息：

管理应用程序 (p. 93)
监视器源分配的工作方式 (p. 250)

所需服务

CA Standard Monitor 会自动启动下面列出的服务。

警告：为了避免数据丢失，请不要尝试手动停止或重新启动这些服务。要寻求帮助，请联系 CA Support：http://support.ca.com。

- CA ADA Monitor 管理。响应管理控制台的请求，将 .dat 文件从监控传输到管理控制台。
- CA ADA Data Transfer Manager。根据在 CA Standard Monitor 上定义的应用程序、服务器和客户端网络，将监视与 Cisco WAE 设备保持同步。
- CA ADA Inspector Agent。如果承载应用程序的服务器由 CA Standard Monitor 监视，监控上的 CA ADA Inspector Agent 将对应用程序、服务器和相关网络启动调查。否则，将由管理控制台上的 CA ADA Inspector Agent 服务启动调查。
- CA ADA Messenger 服务。将监视与 CA Standard Monitor 上定义的应用程序、服务器和客户端网络保持同步。
- CA ADA Monitor。位于管理控制台或 CA Standard Monitor 上，该服务可通过其分配的监视设备（如 CA GigaStor）接收镜像 TCP 数据包和摘要文件。
- CA ADA Batch。可将 .dat 数据文件暂存在 CA Standard Monitor 上，供管理控制台上的 CA ADA Master Batch 服务处理。

监视器源的工作方式

*监视器源*是响应时间数据的源，例如：

- 数据包监视器源可以在监视器 NIC 上接收镜像 TCP 数据包。
- Riverbed WAN 监视器源可以从 Riverbed Steelhead 设备接收 WAN 优化数据包。
- GigaStor 监视器源可以在 CA GigaStor 的管理 NIC 上接收数据包摘要文件。
- WAN 优化监视器源可以在管理 NIC 上从 Cisco WAE 设备接收数据包摘要文件。

管理控制台可以自动将最靠近服务器的监视器源作为监视服务器上 TCP 通信量的源进行分配。

针对以下目的编辑监视器源：

- 分配一个特定的域。默认情况下，新的监视器源会分配到默认域。如果您没有使用域来分隔重复的 IP 通信量，这将不适用。
- 与备用监视器源配对，以便进行冗余数据监视。
- 查看活动会话。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。

详细信息：

管理承租人 (p. 87)
创建一对监视器源 (p. 225)

监视器源分配的工作方式

如果 CA Standard Monitor 上的某个监视器源是监视服务器上 TCP 通信量的最佳源，管理控制台会自动将监视器源分配给服务器。

详细信息：

监视器源分配的工作方式 (p. 223)

数据包捕获调查的工作方式

将数据包监视器源分配给服务器时，管理控制台会在服务器上通过相应的可查看数据包的 CA Standard Monitor 执行数据包捕获调查。

与 CA GigaStor 或 CA Multi-Port Monitor 不同，CA Standard Monitor 可执行以下操作：

- 在管理控制台创建突发事件之后启动数据包捕获调查。
- 一次运行一个数据包捕获调查。
- 将数据包捕获文件从监控复制到用户的本地计算机，以便查看数据包捕获调查。可能要花很长时间才能打开数据包捕获调查，具体取决于数据包捕获文件的大小。
- CA Standard Monitor 不支持对数据包进行长期存储。

要使管理控制台用户能够打开由 CA Standard Monitor 创建的数据包捕获调查，需要使用网络数据包分析程序。

监视设备注意事项

将 CA Standard Monitor 用作监视设备时，请记住：

- 通常，CA 技术代表会帮助您将 TCP 通信量镜像到监视设备。有关镜像 TCP 通信的详细信息，请参阅 《*Best Practices for Data Acquisition Guide*》（数据采集最佳实践指南）。
- PacketMon 是唯一一个经过认证、可在 CA Standard Monitor 或单机管理控制台上安装的数据包探查器。为了避免与数据包捕获驱动程序冲突，请**不要**在 CA Standard Monitor 或单机管理控制台上安装任何其他数据包探查器（包括 *Wireshark*）。
- 当配置数据包捕获调查时，请记住 CA Standard Monitor 不支持对捕获的数据包进行长期存储。要优化可用资源，请对数据包捕获进行配置，以便限制：
  - 最大文件大小。
  - 每个数据包的字节数。
- 要限制对数据包捕获中可能存在的敏感内容的访问，您可以在 CA Standard Monitor 上禁用数据包捕获 (p. 257)。
- CA Standard Monitor 可以根据管理控制台上定义的客户端网络、服务器子网和端口排除，自动监视匹配的应用程序通信量。
- CA Standard Monitor 可以监视所有类型的应用程序。

支持 XFF 转换

当用户通过某种工具（例如代理服务器）访问 Web 应用程序时，如果该代理服务器与所代理的客户端属于不同的子网，管理控制台会错误地报告代理服务器的相应客户端网络的 Web 应用程序通信量，而不是实际客户端网络的 Web 应用程序通信量。

如果代理服务器使用 XFF，您可以在 CA Application Delivery Analysis Manager 中启用 XFF 转换，以扩展对 Web 应用程序的监视支持，并报告实际客户端网络的 Web 应用程序通信量，而不是代理服务器的相应客户端网络的 Web 应用程序通信量。

启用 XFF 转换会消耗每个 CA Standard Monitor 上的额外资源。默认情况下，CA Application Delivery Analysis Manager 不执行 XFF 转换。

详细信息：

创建 Web 应用程序 (p. 112)
启用 XFF 转换 (p. 253)

XFF 转换的工作方式

当客户端通过使用 XFF 的 HTTP 代理服务器连接到 Web 应用程序时，管理控制台使用 X-Forwarded-For (XFF) HTTP 标头来标识客户端的原始 IP 地址。典型的 XFF HTTP 标头格式如下：

```
TCP Source IP: proxy3
X-Forwarded-For: client1, proxy1, proxy2
```

IP 地址列表包括下游最远端的客户端、每个传递过请求的连续代理，以及从其接收过请求的代理。在示例中，请求通过了 proxy1、proxy2 和 proxy3（离服务器最近的代理）。

使用 XFF 转换，管理控制台就可以正确地报告每个客户端的 Web 通信量，将其归到相应的子网。在管理控制台中，您将可以看到正确的进出客户端的 Web 应用程序通信量。您还将看到代理服务器上的少量通信量。通信量由代理服务器发送到 Web 服务器的确认而非事务通信量组成。

提示：如果将代理服务器定义为其在代理环境中的网络，则可对 Web 服务器到代理服务器链路上的性能与 Web 服务器到客户端子网这个完整路径上的性能进行区分。在代理服务器与客户端不在同一位置的情况下，这是很有用的信息。

启用 XFF 转换

启用 XFF 转换时，必须在管理控制台数据库上运行 MySQL 命令。要运行所需的 MySQL 命令，请执行以下步骤：

1. 使用 Windows 管理员帐户登录到管理控制台服务器。
2. 使用正确的数据库名称和端口访问管理控制台数据库：

   数据库名称

   默认管理控制台数据库名称为 super。

   数据库端口

   管理控制台数据库的默认端口为 TCP-3308。

有关使用 MySQL 命令的详细信息，请参阅 www.mysql.com 上提供的 MySQL 文档。

遵循这些步骤:

1. 使用 Windows 管理员帐户登录管理控制台计算机。
2. 打开命令提示符。
3. 通过运行以下命令登录到 MySQL：
   ```
   mysql -P3308
   ```
4. MySQL 显示以下提示。
   ```
   mysql>
   ```
5. 在 MySQL 提示符下运行以下命令以转到管理控制台数据库：
   ```
   use super;
   ```
   MySQL 显示以下响应：
   ```
   Database changed
   ```
6. 在 MySQL 提示符下运行以下命令以启用 XFF 转换：
   ```
   INSERT IGNORE INTO parameter_descriptions (Parameter, Level,
   Type, DefaultValue, Description) VALUES ('XFFEnabled',
   'System', 'boolean', '1', 'Non-zero to enable XFF endpoint
   extraction in URL monitoring.');
   ```
   MySQL 显示以下响应：
   ```
   Query OK, 1 row affected (0.00 sec)
   ```
7. （可选）若要在启用 XFF 转换后要再禁用它，请运行下列命令：
   ```
   UPDATE parameter_descriptions SET DefaultValue='0' WHERE
   parameter='XFFEnabled';
   ```
   MySQL 显示以下响应：
   ```
   Query OK, 1 row affected (0.02 sec)
   Rows matched: 1  Changed: 1  Warnings: 0
   ```
8. 关闭命令提示符。
9. 要应用所做的更改，请同步 (p. 261)监视设备。

详细信息：

Windows 管理员凭据 (p. 201)

添加 CA Standard Monitor

添加 CA Standard Monitor 以便执行下述操作：

- 从 SPAN 交换机端口接收 TCP 数据包。
- 从 CA GigaStor (p. 301) 接收数据包摘要。
- 从 Cisco WAE (p. 319) 设备接收数据包摘要。

先决条件

在添加 CA Standard Monitor 之前，请确保：

- 监视设备比率 (p. 231)大小设置正确。
- 管理控制台可以在 TCP-80、TCP-1000 和 TCP-1001 上与 CA Standard Monitor 通信。
- 出站 UDP-161 可以使用，例如，可用来对服务器或网络设备进行 SNMP 轮询。
- 出站 UDP-162 可用，例如，用于发送 SNMP 陷阱。
- 出站和入站 ICMP 可用，例如，用于确认服务器可以响应 ping 请求以及用于度量往复传输时间。
- 您可以使用 Windows 终端服务 (RDP) 在 TCP-3389 上远程访问 CA Standard Monitor。

添加 CA Standard Monitor

当您添加 CA Standard Monitor 时，管理控制台会尝试使用您指定的管理 IP 地址与监控通信。如果您想要添加目前在网络上不可用的监控，管理控制台会立即轮询管理 IP 地址，然后您就可以指定其余监控属性。当监控在网络上可用时，请对监视设备执行同步 (p. 224)操作，以便在监控和管理控制台之间建立通信。

通过禁用 TCP 数据包监视，在监控上对可用资源进行优化。例如，如果您计划添加专用监控从 CA GigaStor 接收数据包摘要文件，而且您不想让监控监视其监视器 NIC 上的 TCP 通信量，则可禁用数据包监视。

监控在添加后会显示在“ADA 监视设备列表”中。如果您已在 CA PC 或 CA NPC 中定义了域 (p. 87)，则请将一个域分配给 CA Standard Monitor 上的数据包监视器源。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 在“向我显示”菜单下单击“添加 ADA 监视器”。

   将打开“Standard Monitor 属性”。
4. 填写“Standard Monitor 属性”中的字段，然后单击“确定”。

   有关设置监视设备属性的信息，请单击“帮助”。
5. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

NAT 防火墙通信

要让 CA Standard Monitor 与 NAT 防火墙后面的管理控制台通信，请通过 LockConsoleAddress 实用工具使用分配的控制台的 NAT 地址来更新监控配置。

此程序在很多情况下（例如，当管理控制台位于 NAT 防火墙后面的专用网络上时）是必需的。在该环境中，可能会出现在防火墙另一侧的 CA Standard Monitor 可以通过其 NAT 地址 ping 管理控制台，但管理控制台却收不到监控的任何报告数据。

在运行该实用工具之前，请确保您知道要向其分配监控的管理控制台的 IPv4 NAT 地址。

遵循这些步骤:

1. 在 CA Standard Monitor 上，打开命令提示符。
2. 在命令提示符下，将目录更改为 <ADA 主目录>\bin 目录，例如 D:\NetQoS\bin。
3. 键入以下命令，然后按 Enter 键：
   `LockConsoleAddress <NAT_IP>`

   其中，NAT_IP 是管理控制台的 IPv4 NAT 地址。实用工具使用您指定的 IPv4 NAT 地址更新以下注册表项：
   `HKEY_LOCAL_MACHINE\SOFTWARE\NetQos\SACollector\Parameters\NAT_MasterDB`
4. （可选）要确认监控用来与管理控制台通信的 IPv4 NAT 地址，请键入以下命令并按 Enter 键：
   `LockConsoleAddress`

   结果表示在 NAT 防火墙后面的控制台的当前 IP 地址。
5. （可选）要从监控中删除管理控制台的 NAT 地址删除，请键入以下命令并按 Enter 键：
   `LockConsoleAddress -d`

   实用工具更新以下注册表项来删除 IPv4 NAT 地址：
   `HKEY_LOCAL_MACHINE\SOFTWARE\NetQos\SACollector\Parameters\NAT_MasterDB`

保护数据包捕获调查文件

CA Standard Monitor 以未加密格式存储其数据包捕获调查文件。默认情况下，数据包捕获调查仅收集标头信息，这大大减少了加密需求。

要提升数据包捕获调查文件的安全，请执行以下操作：

- 您可以将数据包捕获调查配置为仅捕获标头信息。
- 在监控上禁用数据包捕获调查。请注意，升级 CA Standard Monitor 时，将启用数据包捕获调查。升级以后，必须手动修改监控配置才能禁用数据包捕获。

如果选择启用数据包捕获调查，则也应对角色 (p. 195)进行配置，以便限制能够创建并查看数据包捕获调查的人员。

遵循这些步骤:

1. 在 CA Standard Monitor 上，打开 Windows 资源管理器并浏览到 <ADA 主目录>\SuperAgent\dotnet\InspectorAgent。
2. 在 InspectorAgent.exe.config 文件中，取消对以下条目的注释：
   `<add key="Capture.CaptureTcp" value="disable" />`
3. 在监控上重新启动 NetQoS Inspector Agent 服务，以便应用所做的更改。
4. 要手动删除监控上的现有数据包捕获调查文件，请导航到 <ADA 主目录>\SuperAgent\Web\batch\snifferfiles，然后删除现有数据包捕获调查 (.enc) 文件。请注意，在数据库维护过程中清除 5 分钟数据时，与该 5 分钟数据关联的数据包捕获调查文件也将自动清除。

编辑 CA Standard Monitor

编辑 CA Standard Monitor 的属性，以便执行以下操作：

- 分配突发事件响应或启用可用性监视。
- 查看每个监视器源的活动会话信息。
- 查看 CA Standard Monitor 的监视设备突发事件。
- 编辑 CA Standard Monitor 上任何监视器源的属性。
- 在 CA Standard Monitor 上执行基本操作，如同步监视设备、停止和开始、重新启动及关闭监控。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“ADA 监视设备列表”，然后单击  以编辑 CA Standard Monitor。

   将打开“Standard Monitor 属性”。

   注意： “Standard Monitor”类型包括 CA Standard Monitor 和 CA Virtual Systems Monitor。如果无法确定监控是否在虚拟计算机上运行，请验证其 IP 地址。
4. 填写“Standard Monitor 属性”中的字段，然后单击“确定”。

   有关设置监视设备属性的信息，请单击“帮助”。
5. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

编辑数据包监视器源

*数据包*监视器源从 CA Standard Monitor 上的监视器 NIC 接收镜像 TCP 数据包。编辑数据包监视器源，以便执行以下操作：

- 更改监视器源的默认名称。
- 分配一个特定的域。默认情况下，新的监视器源会分配到默认域。如果您没有使用域来分隔重复的 IP 通信量，这将不适用。
- 创建一对监视器源 (p. 225)，使管理控制台能够自动从两个监视器源上收集已分配服务器的数据。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。

   将打开“ADA 监视设备列表”。
3. 单击 ，使用数据包监视器源来编辑 CA Standard Monitor。

   将打开“Standard Monitor 属性”。

   注意：“Standard Monitor”类型包括 CA Standard Monitor 和 CA Virtual Systems Monitor。如有必要，可验证监控 IP 地址。
4. 在“监视器源”下单击 ，对数据包监视器源进行编辑。
5. 编辑数据包监视器源属性，以便分配备用源或域。
6. 单击“更新”。
7. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
监视设备的工作方式 (p. 221)

管理监视设备性能

如果 CA Standard Monitor 出现以下情况，管理控制台将自动创建重大监视设备突发事件：

- 停止向管理控制台发送数据超过 1 小时
- 处理的数据包未达到所接收数据包的 5%

详细信息：

编辑监视设备突发事件阈值 (p. 236)

监视设备操作

在部分或全部监视设备上执行基本操作，例如同步监视设备之后，即可根据目前在管理控制台上定义的客户端网络、服务器子网和应用程序来收集性能数据。在“ADA 监视设备列表”中，使用蓝色齿轮菜单 执行基本操作。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“ADA 监视设备列表”，然后单击蓝色齿轮菜单 以对列表中的所有监视设备执行基本操作。
4. （可选）要对特定监视设备执行基本操作，请浏览该列表，然后单击编辑图标 。在“Standard Monitor 属性”页面上，单击蓝色齿轮菜单 ，然后选择一个命令。

   开始

   在状态为“已停止”的监控上开始数据监视。监控停止时，监控不会处理来自监视器源的任何响应时间度量标准。

   如果管理控制台无法与监控通信，请登录到 CA Standard Monitor，以便启动 CA ADA Monitor 服务。

   停止

   在状态为“正在运行”的监控上开始数据监视。监控停止时，监控不会处理来自监视器源的任何响应时间度量标准。

   同步监视器设备

   在监控上更新数据监视配置，以便根据当前已定义的客户端网络、服务器子网和应用程序收集性能数据。

   重新启动

   重新启动 CA Standard Monitor 或 CA Virtual Systems Monitor。该命令不适用于 CA Multi-Port Monitor。

   如果管理控制台无法与监控通信，请登录到监控重新启动它。

   关闭

   关闭 CA Standard Monitor 或 CA Virtual Systems Monitor 的电源。要在关闭 CA Standard Monitor 或 CA Virtual Systems Monitor 后又重新启动，必须通过监控进行操作。该命令不适用于 CA Multi-Port Monitor。

   如果管理控制台无法与监控通信，请登录到 CA Standard Monitor 将其关闭。

详细信息：

监视设备同步的工作方式 (p. 224)
执行基本操作 (p. 233)

筛选出保持连接消息

CA Standard Monitor 提供了一个选项来限制应用程序保持连接消息对报告中监视统计信息的影响。技术涉及到限制选定应用程序的服务器响应时间 (SRT) 或数据传输时间 (DTT)，为其设置一个最大值，这样系统就会忽略不必要的 SRT 或 DTT 观测。您可以将值设置为若干秒，使其恰好低于保持连接频率。

如果您怀疑应用程序正在发送保持连接消息，请在观测与 SRT 之间查找逆向关系，并在秒范围而非毫秒范围内查找 SRT 平均值。配置 CA Standard Monitor 以限制应用程序的最大 SRT。

如果确定应用程序使用了保持连接消息，从而导致数据传输时间 (DTT) 大大延长，您也可以应用类似限制来筛选 DTT。

通过控制台的内置 NRTT 筛选 (p. 205)，在 CA Standard Monitor 上使用 SRT 和 DTT 筛选。通常情况下，当客户端空闲时，应用程序保持连接消息会偏离 SRT 数据。当所有客户端空闲时（如非工作时间），NRTT 筛选有时会很有用。然而在白天，您可能很容易就会发现：客户端网络有 30 个连接是活动的，有 10 个连接却是空闲的。您可能会超过 NRTT 阈值，但考虑到该组合内仍有 10 个空闲连接，因此您实际得到的仍是偏离的数据。

如果不确定所选应用程序的保持连接频率，我们建议您一开始使用 10 秒，这样比较稳妥。服务器需要花 10 秒以上的时间才开始响应用户请求是十分罕见的。多数（并非所有）情况下，保持连接频率会大于 10 秒。

如果是使用随机端口的应用程序（如 Microsoft Exchange 2007），则最容易识别端口的方法是打开 Outlook，在计算机上运行 netstat 命令，然后记录 Outlook 连接到的动态端口。

CA Multi-Port Monitor 上也提供了必需设置。然而，更改默认设置所需采取的步骤并不相同。有关详细信息，请参阅 CA Multi-Port Monitor 产品文档。

遵循这些步骤:

1. 使用 Microsoft 远程桌面访问 CA Standard Monitor。
2. 浏览安装目录，例如：C:\CA\Bin。
3. 为要筛选的每个端口指定一个 SRT 阈值：
   a. 复制 LimitServerResponseParams.ini.sav 文件并将其重命名为 LimitServerResponseParams.ini。
   b. 在记事本中编辑 .ini 文件，为要筛选的每个端口指定 SRT 阈值。

LimitServerResponseParms.ini 文本文件可接受多个由换行符分隔的条目。通过提供端口号和允许的最大 SRT 数量，对每个应用程序的 SRT 进行限制。将最大 SRT 设置为略小于保持活动状态频率的值。例如，要忽略以 60 秒频率发生的 Citrix 保持连接消息，请提供以下条目：

```
/port=1494 /max seconds=59
```

c. 要筛选端口范围，请使用以下语法：

```
/min port=<lowerPort> /max port=<higherPort> /max
seconds=59
```

如果不指定任何端口，或指定为 0，则指定的限制将应用于所有端口。如果将 0 指定为端口范围的下限也会具有同样的效果，无论端口上限指定为什么内容都是如此。

在文件中较早出现的条目优先级高于后面显示的条目。因此，如果多个规则对端口范围的规定具有重叠，则必须首先列出更为具体的规则，否则它们会被不那么具体的规则所掩盖。例如：

```
/port=23 /max seconds=15
```

```
/min port=100 /max port=200 /max seconds=50
```

```
/max seconds=120
```

此文件将端口 23 的 SRT 或 DTT 限制为 15 秒，将端口 [100-200] 的上述内容限制为 50 秒，将所有其他端口的上述内容限制为 120 秒。

d. 保存文件。

4. 如有必要，为要筛选的每个端口指定一个 DTT 阈值：

a. 复制 LimitDTTParams.ini.sav 文件并将其重命名为 LimitDTTParams.ini。

b. 指定 DTT 筛选条件，如前一步所述。

c. 保存文件。

5. 打开管理控制台，然后同步监视设备以应用所做的更改：

a. 单击“管理配置”页面。

b. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。

c. 滚动到“ADA 监视设备列表”，并单击蓝色齿轮菜单 ，然后选择“同步监视器设备”。

删除 CA Standard Monitor

删除 CA 标准监视设备，以将其作为响应时间数据的源删除。删除监视设备时：

- 取消连接已连接到对应监视器源的所有服务器，并自动分配另一个监视器源。更新监视器源分配可能需要长达 10 分钟。
- 现有数据将保留，用于报告目的。

如果您已将服务器连接到监视器源，并且您想在监视设备暂时脱机时继续监控服务器通信，则考虑下列选项：

- 将监视设备脱机之前，将服务器连接到其他监视器源。使监视设备重新联机时，将适当的服务器连接到监视器源。
- 删除监视设备。另一个监视器源将自动被分配，但是更新监视器源分配所使用的时间高达 10 分钟。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 单击 以从“ADA 监视设备列表”中删除 CA Standard Monitor。

   注意：“Standard Monitor”类型包括 CA Standard Monitor 和 CA Virtual Systems Monitor。如有必要，请验证监控的 IP 地址。
4. 在“删除监视设备确认”中，单击“继续删除”删除监视设备。

详细信息：

将监视器源固定到服务器 (p. 78)

禁用数据包监视器源

要优化可用 CA Standard Monitor 资源以处理来自 Cisco NAM、Cisco WAE、Riverbed Steelhead 或 CA GigaStor 的传入摘要文件，请在 CA Standard Monitor 上禁用数据包监视。禁用数据包监视将删除数据包监视器源。

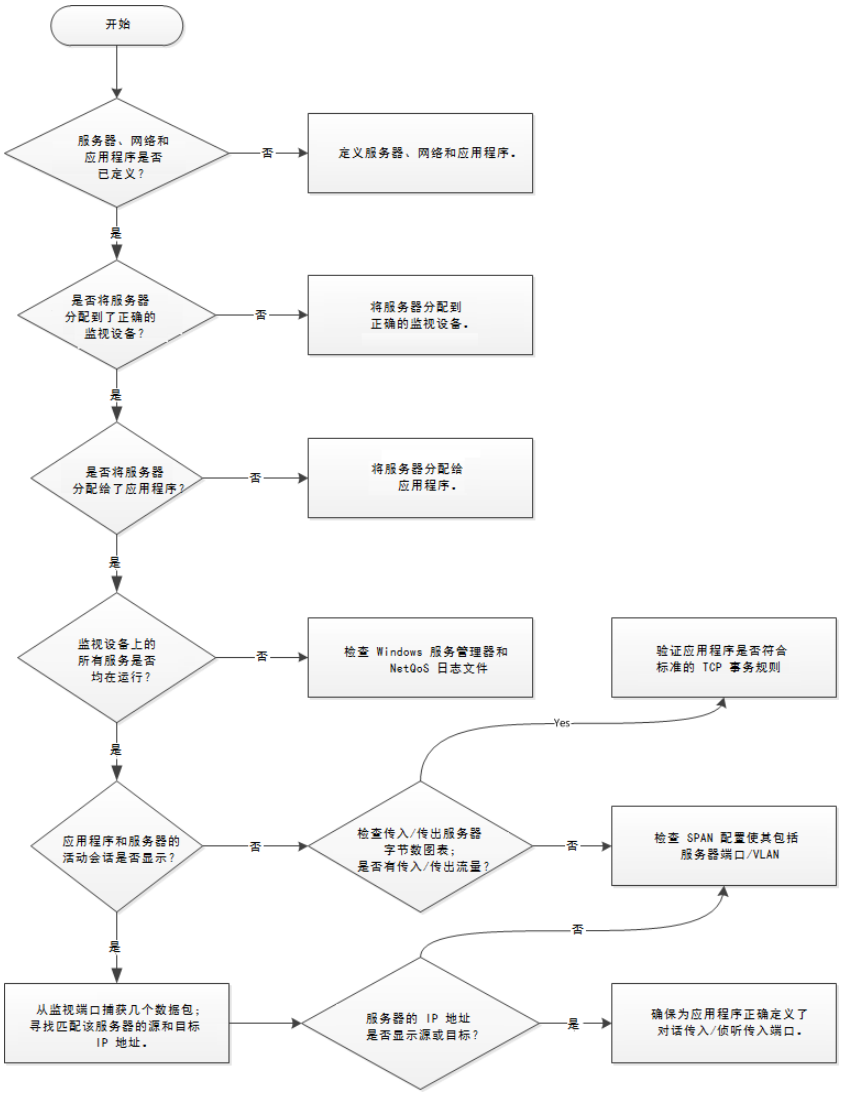
添加 CA Standard Monitor 时，您可以选择禁用数据包监视。添加 CA Standard Monitor 之后，您无法选择禁用数据包监视。如有必要，可先删除 CA Standard Monitor，然后再添加禁用了数据包监视功能的 CA Standard Monitor。如果已将某个监视设备分配给了 CA Standard Monitor，则在添加 CA Standard Monitor 之后，将需要重新分配。

详细信息：

添加 CA Standard Monitor (p. 254)

CA Standard Monitor 故障排除

对 CA Standard Monitor 进行故障排除，识别本应由 CA Standard Monitor 监视的报告数据的缺失原因。如果您在对 Cisco WAE 或 CA GigaStor 的数据监视问题进行故障排除，请确保 CA Standard Monitor 正在接收和处理相应的摘要文件。



验证活动会话

使用“活动会话”页面，可以报告最后 5 分钟报告间隔内由 CA Standard Monitor 或 CA Virtual Systems Monitor 上的每个监视器源报告的活动 IPv4 TCP 会话数目。请记住，CA Virtual Systems Monitor 只接收数据包监视器源。

如果监视器源没有服务器或应用程序的任何活动会话，请确保：

- 数据包监视器源正在查看 TCP 通信量。
- CA ADA Monitor 服务正在运行。

详细信息：

在监视器源上查看活动会话 (p. 227)
排除 CA ADA 监视器服务故障 (p. 271)
查看监视器源统计 (p. 268)

查看监视器源统计

在 CA Standard Monitor 上，CA ADA Monitor 服务负责根据从每个监视器源接收到的传入数据计算 5 分钟平均值。

使用监视器源计数器可以更好地了解该服务的功能：

数据包接收器

镜像到 CA Standard Monitor 的数据包数据。

GigaStor 接收器

从 CA GigaStor 接收的数据包摘要文件。要显示该计数器，必须将 CA GigaStor 分配给 CA Standard Monitor。

Steelhead 接收器

从 Riverbed Steelhead 设备接收的数据包摘要文件。

WAN 优化接收器

从 Cisco WAE 设备接收的数据包摘要文件。为了显示此计数器，必须将 Cisco WAE 设备分配给 CA Standard Monitor。

重要提示：开始之前，请同步监视设备。直到同步数据监视之后，才会显示计数器窗口。

要查看监视器源计数器，您必须登录到 CA Standard Monitor 计算机。

遵循这些步骤:

1. 登录到 CA Standard Monitor 计算机或使用 Microsoft 远程桌面连接 (RDC) 客户端远程连接到 CA Standard Monitor 计算机。

   使用远程桌面来连接基于 Windows Server 2003 的服务器时，请使用 /admin 开关连接到物理控制台会话。必须连接到物理控制台会话才能查看源接收器计数器。有关 /admin 开关的信息，请参阅 Microsoft KB 947723。

   查看下述项目的统计信息：

   数据包数据

   登录到接收镜像 TCP 数据包的 CA Standard Monitor 或管理控制台。

   WAN 优化设备或 CA GigaStor 提供的数据包摘要文件

   登录到接收数据包摘要文件的 CA Standard Monitor。

2. 承载 CA Standard Monitor 的操作系统版本不同，查看监视器源统计信息所需执行的步骤会有所不同。如果 CA Standard Monitor 运行在：

- Windows Server 2003 上，将自动显示源接收器计数器。如果未显示，请确保您已连接到物理控制台会话。
- Windows Server 2008 上，双击桌面上的“ADA 监视器活动”快捷方式即可显示源接收器计数器。

3. 如果未正确显示计数器说明，请关闭计数器窗口，然后双击桌面上的“ADA 监视器活动”快捷方式来重新打开它。
4. 如果任何一个源接收器计数器都没有显示，请确保：
   - CA ADA Monitor 服务正在运行。
   - 监控已与管理控制台同步

详细信息：

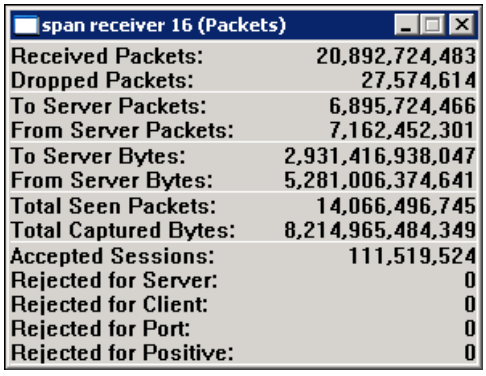
监视设备同步的工作方式 (p. 224)
监视设备操作 (p. 261)
查看 GigaStor 计数器统计信息 (p. 317)
查看 SPAN 接收器统计 (p. 269)

查看 SPAN 接收器统计

有关 CA Standard Monitor 在特定监视器 NIC 上接收的未优化 TCP 数据包数据的信息，请查看数据包计数器统计。

重要提示：开始之前，请同步监视设备。必须同步监视设备才能显示其计数器窗口。

数据包计数器会显示以下信息：



接收的数据包

标识 CA Standard Monitor 上由监视器 NIC 接收但未检查的数据包总数。

注意：通过检查数据包标头，您可以使用这些数据包来计算应用程序响应时间度量标准。有关详细信息，请参阅“可见数据包总计”。

已丢弃数据包

标识已到达监视器 NIC 但其数据包标头未经检查的数据包总数。如果 CA Standard Monitor 忙于处理其他数据包且数据包捕获驱动程序缓冲区已满，数据包会被丢弃。

到服务器数据包

标识从客户端发送到服务器的数据包总数。

来自服务器数据包

标识从服务器发送到客户端的数据包总数。

到服务器字节

标识从客户端发送到服务器的字节总数。

来自服务器字节

标识从服务器发送到客户端的字节总数。

可见数据包总计

标识与指定的应用程序端口、客户端网络和服务器子网相匹配的数据包总数。

注意：如果监控正常运行，则“可见数据包总计”数目与“接收的数据包”数目一致。如果 监控 无法检查它接收的所有数据包，则“可见数据包总计”数目将小于“接收的数据包”数目，且“已丢弃数据包”数目会增加。有关详细信息，请参阅“已丢弃数据包”。

捕获的字节总计

表示与指定的应用程序端口、客户端网络和服务器子网相匹配的数据包的总字节数。

注意：CA Standard Monitor 会检查每个数据包标头，以便确定数据包是否与指定的应用程序端口、客户端网络和服务器子网相匹配。有关详细信息，请参阅“可见数据包总计”。

已接受的会话

表示匹配管理控制台上的有效应用程序/服务器/网络组合的 TCP 会话数目。

服务器被拒绝

标识其中的服务器 IP 与服务器子网不匹配的 TCP 会话数。

客户端被拒绝

标识其中的客户端 IP 与客户端网络不匹配的 TCP 会话数。

端口被拒绝

标识其中的服务器端口与管理控制台忽略的端口列表相匹配的 TCP 会话数。

正当拒绝

保留给将来使用。

详细信息：

客户端网络的工作方式 (p. 27)
应用程序的工作方式 (p. 93)
服务器的工作方式 (p. 61)
编辑 CA Standard Monitor (p. 258)

排除 CA ADA 监视器服务故障

CA ADA Monitor 服务处理传入的监视器源数据。它：

- 加载、初始化并控制数据包驱动程序，这些数据包驱动程序读取通过 CA Standard Monitor 或管理控制台上的监视器 NIC 的每个 TCP 数据包。
- 处理来自管理 NIC 的数据包摘要文件，例如，来自分配的 CA GigaStor。
- 在管理控制台上，它处理来自 Cisco NAM 的度量标准摘要文件。
- 报告每个监视器源观测到的 TCP 通信。

如果 CA ADA Monitor 服务已停止，您可以尝试重新启动它。如果无法启动 CA ADA Monitor 服务，请参阅以下几部分来了解更多的故障排除信息。该信息适用于 CA Standard Monitor，以及在其监视器 NIC 上接收 TCP 数据包或处理来自另一类型的监视设备（如 CA GigaStor）的数据包摘要文件的管理控制台。

遵循这些步骤:

1. 在 Windows 桌面上，单击“开始”菜单，然后单击“控制面板”。
2. 在“控制面板”中，双击“管理工具”。
3. 双击“服务”。
4. 右键单击 CA ADA Monitor 服务，然后单击“启动”。

检查管理控制台日志文件

如果 CA ADA Monitor 服务没有启动，请打开该日志文件，以查找可以帮助您确定根本原因的错误消息。默认情况下，日志文件保存在 <ADA 主目录>\Logs\SACollectorErrors[日期].log 中。

验证 NIC 的状态和优先级

如果 CA ADA Monitor 服务没有启动，请验证是否仅启用了两个 NIC 并且管理 NIC 具有最高优先级。

遵循这些步骤:

1. 在 Windows 桌面上，单击“开始”菜单，然后单击“控制面板”。
2. 在“控制面板”中，双击“网络连接”。
3. 在“网络连接”窗口中，确保：
   - 管理 NIC 和监视器 NIC 的状态为“已启用”。
   - 所有其他 NIC 的状态为“已禁用”。

   注意：“网络电缆被拔出”状态也会导致 CA ADA Monitor 服务无法启动。
4. 要禁用某个 NIC，请右键单击该 NIC，然后单击“禁用”。
5. 在“网络连接”窗口中，单击“高级”菜单上的“高级设置”。确认管理 NIC 显示在最前面，之后紧接着是监视器 NIC，然后是其他未使用的连接。
6. 启动 CA ADA Monitor 服务。如果该服务未启动，请按下一部分中所述执行故障排除步骤。

验证网络适配器的注册表设置

如果 CA ADA Monitor 服务没有启动，请验证网络适配器的注册表设置。

遵循这些步骤:

1. 在 Windows 桌面上，单击“开始”菜单，然后单击“运行”。
2. 在“打开”框中，键入 regedit。
3. 导航到以下注册表表项：
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}

   其下应当有几个子项，从 0000 开始直到 0008。每个子项代表 Windows 中加载的一个网络适配器。
4. 展开每个子项来确保它具有一个 Linkage 子文件夹。如果某个子项没有 Linkage 子文件夹，请导出该子项并将其删除。
5. 导出某个子项：
   a. 选择该子项。
   b. 在注册表编辑器菜单上，单击“文件”，然后单击“导出”。
   c. 选择目标位置和文件名。
   d. 单击“保存”。
6. 删除该子项，右键单击该子项，然后单击“删除”。
7. 针对没有 Linkage 子文件夹的所有子项，重复步骤 5 和 6。
8. 启动 CA ADA Monitor 服务。如果该服务未启动，请按下一部分中所述执行故障排除步骤。

验证 NIC 设置

如果 CA ADA Monitor 服务未启动，请使用 statstconsole.exe 程序来验证 NIC 设置。

遵循这些步骤:

1. 在 Windows 资源管理器中，浏览到 <ADA 主目录>\bin。
2. 双击 statstconsole.exe。
3. 在“Super Agent 控制台”对话框中，记下“适配器”字段中的监视器 IP 地址。这是管理控制台要寻找的 IP 地址。
4. 在“适配器”字段中，键入当前分配给监视器 NIC 的 IP 地址。
5. 使用 Microsoft Windows“网络连接”窗口，验证是否已为管理 NIC 分配了静态 IP 地址。

   注意：如果您为管理 NIC 使用 DHCP 地址，会出现问题。
6. 在管理控制台上，单击“启动”。
7. 启动 CA ADA Monitor 服务。如果该服务未启动，请按下一部分中所述执行故障排除步骤。

检验监视器服务的注册表设置

如果 CA ADA Monitor 服务没有启动，请检查 Windows 注册表。

遵循这些步骤:

1. 在 Windows 桌面上，单击“开始”菜单，然后单击“运行”。
2. 在“打开”框中，键入 regedit。
3. 导航到以下注册表表项：
   HKEY_LOCAL_MACHINE\SOFTWARE\NetQoS\SuperAgent\Parameters
4. 验证 MasterDB 注册表项是否已设置为管理控制台或 CA Standard Monitor 的 IP 地址。
5. 验证 Role 注册表项是否设置为以下内容之一：
   - CA Standard Monitor：Slave
   - 单机管理控制台：Standalone
6. 验证 LastManagementAddress 是否已设置为 CA Standard Monitor 或管理控制台的管理 NIC IP 地址的 UNIX 等效项。
7. 要查找 UNIX 等效 IP 地址，请登录到安装 MySQL 的服务器。运行以下查询：
   `SELECT INET_ATON('x.x.x.x');`

   其中，*x.x.x.x* 是 CA Standard Monitor 或管理控制台上的管理 NIC 的 IP 地址；例如：
   `mysql> SELECT INET_ATON('209.207.224.40');`
8. 启动 CA ADA Monitor 服务。如果该服务未启动，请按下一部分中所述执行故障排除步骤。

验证与管理控制台的通信

如果 CA ADA Monitor 服务未启动，请确认 CA Standard Monitor 可以通过 TCP-80 与 CA Application Delivery Analysis Manager 进行通信。

以下过程适用于在管理控制台上的 CA Standard Monitor。

遵循这些步骤:

1. 在 CA Standard Monitor 上打开一个命令提示符并键入以下命令：
   `telnet <host> <port>`

   其中：

   <host>

   是管理控制台的 IP 地址

   <port>

   是 80

   如果您收到“连接失败”错误，则表明端口被阻止并且需要打开。如果您看见空白的黑色屏幕，则表明连接成功。
2. 启动 CA ADA Monitor 服务。如果该服务未启动，请按下一部分中所述执行故障排除步骤。

验证是否至少有一个监视器源处于活动状态

如果 CA ADA Monitor 服务未启动，请确认“Standard Monitor 属性”*未*配置为禁用数据包监视。

如果您在添加 CA Standard Monitor 时选择了“禁用数据包监视”选项，则必须向监控分配一个监视设备（如 CA GigaStor），以便 CA ADA Monitor 服务可以启动。

执行数据包捕获

使用 PacketMon 来对 CA Standard Monitor 上的监视器端口接收的 TCP 数据包执行数据包捕获，然后观察数据包标头和内容。

PacketMon 是唯一一个经过认证、可在 CA Standard Monitor 或单机管理控制台上安装的数据包探查器。为了避免与数据包捕获驱动程序冲突，请**不要**在监控上安装任何其他数据包探查器，包括 *Wireshark*。

遵循这些步骤:

1. 在监控上安装 PacketMon。
2. 在安装完成后，启动 PacketMon。
3. 在 PacketMon 中，单击“开始”来开始数据包捕获。

   如果没有结果出现，或者如果出现了“UDP/未知”数据包类型，则说明 SPAN 的配置错误，或网络分流器没有正确安装。验证 SPAN 配置或网络分流器，并再执行一次数据包捕获。
4. 当返回了有效的 TCP 数据包时，启动 CA ADA Monitor 服务。

检查重复的客户端网络

如果您配置了服务器、应用程序和客户端网络，请确保您没有重复的客户端网络。

如果您有大型配置（几百万组合），则 CA ADA Monitor 服务需要花费几分钟的时间才能启动，而不是立即启动。如果定义了数百台服务器，并且您不想监视所有服务器，请将其从配置中删除。最佳做法是减小管理控制台配置，以便仅剩下所需的服务器、应用程序和客户端区域。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“网络”。

   将打开“网络列表”。
3. 检查网络列表以确保您没有将同一客户端区域配置两次。

排除缺少数据故障

如果 CA Standard Monitor 正在监视通信量，但是管理控制台没有显示数据或者数据不是当前的，则表明管理控制台与监控之间的通信可能存在问题。

遵循这些步骤:

1. 验证是否可以从管理控制台通过 TCP-8080 建立到 CA Standard Monitor 的 Telnet 连接。
2. 如果无法连接，请确认没有防火墙或 ACL 在阻止通信。管理控制台使用 TCP-8080 从 CA Standard Monitor 获取数据文件。
3. 验证是否所有 CA ADA 相关服务都已在管理控制台和 CA Standard Monitor 上启动。
4. 确认管理控制台上的 <ADA 主目录>\Datafiles 目录未充满着跨越几小时或几天的文件。

排除已丢弃数据包故障

有时 CA Standard Monitor 会在短暂的时段（或较长的时段）内报告“已丢弃数据包”。该情况持续存在的时间长度取决于可以通过执行下列故障排除步骤识别的几个因素。

遵循这些步骤:

1. 评估在 SPAN 到监控的过程中聚合通信量的总量。入站数据速率（而不是监控监视的活动会话数）可能会导致数据被丢弃。这是该端口的百分比使用率统计数据。

   如果进入到监视设备中的数据通信量的绝对值太高，请减少 SPAN 到监控上监视器端口的数据量。如果配置管理控制台监视所有通信，则您可能需要添加一个监控并在监视设备之间对服务器 SPAN 进行负载平衡。

2. 评估“数据包”监视器源中的活动会话的总数。监控会区分并计算每个活动会话的响应时间数据，因此，活动会话越多，对新传入数据的处理的影响就越大。

   当监控观测到与您在管理控制台中定义的应用程序端口、服务器和客户端网络匹配的 SPAN 通信量时，它会创建一个*活动会话*。

   如果您可以更新管理控制台来优化所监视的应用程序端口、服务器和客户端网络的列表，则您可以优化监控上的处理资源。如果管理控制台在监视恰当的应用程序、服务器和网络，则您可能需要添加一个监控并在监视设备之间对服务器 SPAN 进行负载平衡。

3. 评估后台进程，如病毒扫描、间谍软件扫描和删除程序，以及系统备份进程。在监控上运行的每个额外应用程序都会影响总的处理器使用率，并且会降低监控处理入站数据通信量的能力。这些进程对内存、CPU、处理器或磁盘 IO 总线的使用越密集，监控在将数据包丢弃之前可以实际处理的数据包就越少。

   要优化可用的监控资源，请从监控中删除这些应用程序。

第 14 章： 使用 CA Virtual Systems Monitor 监视

此部分包含以下主题：

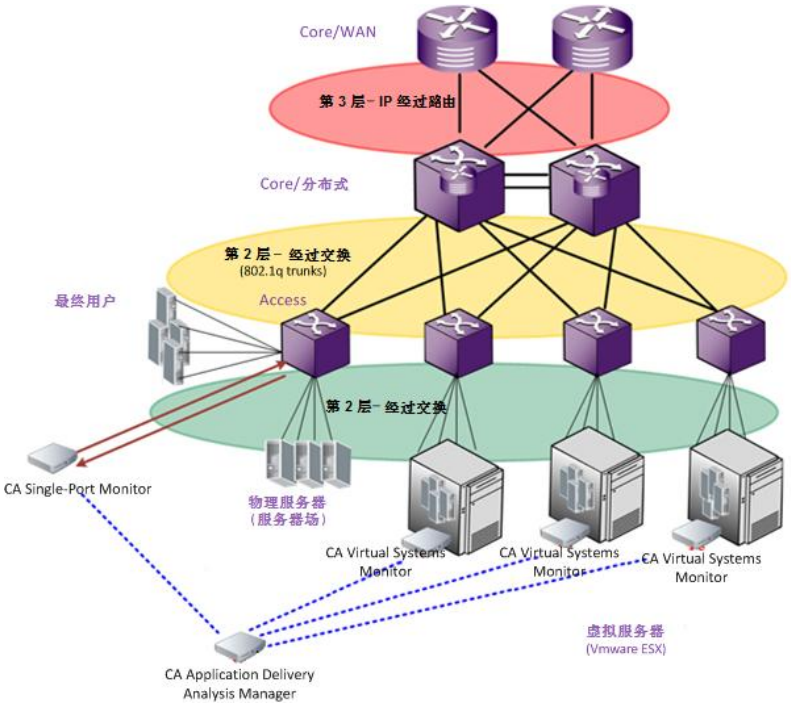
CA Virtual Systems Monitor 作为监视设备的工作方式

Response Time CA Virtual Systems Monitor (CA Virtual Systems Monitor) 可以作为 CA Application Delivery Analysis 的一种监视设备来运行。使用 CA Virtual Systems Monitor 监视同一 VMware ESX 主机上各个虚拟服务器之间的 IPv4 TCP 通信。CA Virtual Systems Monitor 监视同一 ESX 主机上各个 VM 之间的“服务器到服务器”通信量，尽量减少 CA Virtual Systems Monitor 上的负载，并通过扩展最大程度地利用 ESX 主机上的可用资源。

要监视来自虚拟环境外的通信量（例如，来自另一 ESX 主机的通信量，或来自与同一 ESX 主机内的虚拟服务器通信的远程子网的通信量），请将来自物理服务器交换机的服务器通信量镜像到一个物理监视设备，如 CA Multi-Port Monitor。

CA Virtual Systems Monitor 的设计目的只是用来监视 VMware ESX 主机内的“虚拟服务器到虚拟服务器”通信。不要使用 CA Virtual Systems Monitor 来监视物理(外部)设备与虚拟服务器之间的通信量。要监视“物理到物理”和“物理到虚拟”通信，请使用物理监视设备，如 CA Multi-Port Monitor。

如下例中所示，CA Virtual Systems Monitor 监视同一 ESX 主机上各个 VM 之间的“服务器到服务器”通信量，而物理监视设备则获取来自物理交换机的 SPAN 数据。



CA Virtual Systems Monitor 类似于 CA Standard Monitor，但是您将它安装在 VMware 虚拟机上而不是安装在物理设备上。与 CA Standard Monitor 一样，CA Virtual Systems Monitor 被动收集来自镜像端口的数据，检查数据包标头以获取性能相关信息，并将相关的性能度量标准传递到管理控制台，以便进行报告和显示。

与 CA Standard Monitor 不同，CA Virtual Systems Monitor 不从 Cisco WAE 设备或 CA GigaStor 接收摘要文件。

CA Virtual Systems Monitor 通过 Cisco Nexus 1000V 支持 SPAN（端口镜像）。如果您使用的是 VMware vSwitch，则 CA Virtual Systems Monitor 需要一个混合端口组才能看到虚拟交换机上的镜像通信量。

详细信息：

使用 CA Standard Monitor 监视 (p. 247)

部署计划

CA Virtual Systems Monitor 必须能够“看见” ESX 主机上的“虚拟服务器到虚拟服务器”通信量，并且还要无法看见 ESX 主机外的任何外部通信量。在计划您的安装时，请考虑以下注意事项：

- 我们需要监视哪些多层应用程序？
- ESX 主机上的哪些服务器会产生“服务器到服务器”通信量？请使 CA Virtual Systems Monitor 能够看见此“虚拟服务器到虚拟服务器”通信的网络通信量。
- 哪些服务器与外部设备（如另一 ESX 主机上的虚拟服务器或一台物理服务器）进行通信？不要让 CA Virtual Systems Monitor 看见该通信，而是要将该通信量镜像到一个物理监视设备，如 CA Multi-Port Monitor。

  注意：在监视设备上分隔外部通信可让管理控制台自动分配 CA Virtual Systems Monitor 来监视虚拟服务器到虚拟服务器的通信，以及自动分配一个物理监控来监视物理到虚拟的通信。
- 如果您计划监视的虚拟机被分配给多个虚拟 NIC，则该虚拟机的管理 IP 地址必须分配给属于 ESX 主机上的最后一个物理 NIC 的网络适配器（虚拟 NIC）。这是一个 VMware 问题 - 当选中某个网络适配器时，只有当网络适配器分配给最后一个虚拟 NIC 时，VMware 才会显示其 IP 地址。例如，对于具有 3 个虚拟 NIC（VMNIC1、VMNIC2 和 VMNIC3）的虚拟机，将报告分配给 VMNIC3 的网络适配器的 IP 地址，而不会报告分配给 VMNIC1 和 VMNIC2 的此类信息。

详细信息：

监视设备推荐 (p. 232)

端口使用和防火墙

在设置 CA Virtual Systems Monitor 并准备将其添加为监视设备时，您需要考虑可能会阻止 CA Virtual Systems Monitor（驻留在虚拟机上）与管理控制台（驻留在物理计算机上）之间的通信的任何防火墙。您必须确定：

- 已打开了哪些防火墙端口？
- 这些端口上允许什么类型的通信量？

CA Virtual Systems Monitor 包括一个与管理控制台进行通信的 Web 服务。管理控制台需要定期将监视指令发送到其监视设备，并且 CA Virtual Systems Monitor 需要将包含 5 分钟聚合数据的文件发送到管理控制台。因为 5 分钟数据文件包含的是聚合数据，所以在上行端口上消耗的网络带宽最小。

下表汇总了要允许管理控制台与 CA Virtual Systems Monitor 之间的通信所必须打开的防火墙端口：

端口	方向	说明
TCP-1000	入站（从管理控制台到 CA Virtual Systems Monitor）	用于管理控制台访问的 HTTP
TCP-80	入站	针对数据的 Web 服务请求
TCP-161	入站	SNMP MIB 查询
UDP-162	出站	SNMP 警报陷阱

系统要求

CA Virtual Systems Monitor 必须安装在 Microsoft® Windows 操作系统上。安装 Windows 操作系统的已许可版本是您的职责。CA 不提供与 CA Virtual Systems Monitor 一起使用的 Windows 操作系统的许可。

要成功部署 CA Virtual Systems Monitor，您的虚拟机应当满足以下要求：

要求	说明
虚拟交换机	■ 带有 VMware vSwitch 的 VMware ESX® 和 VMware ESXi® 3.5 或 4.1。 ■ 带有 Cisco Nexus® 1000V 的 VMware ESX 和 ESXi 4.1。
用于承载 CA Virtual Systems Monitor 的虚拟机	处理器：1 个虚拟处理器（*最少*）。 内存：1 GB（*最少*）。 虚拟磁盘： ■ Windows Server 2003：16 GB ■ Windows Server 2008 R2：30 GB 网络：2 个虚拟网络适配器（最小 1 Gbit）。要使 CA Virtual Systems Monitor 能够与相应的管理控制台进行通信，需要一个上行端口（离开 ESX 主机的物理端口）。
访客操作系统	CA Virtual Systems Monitor 也要求： ■ Microsoft Windows Server 2003 Standard Edition SP2（x64 或 32 位） ■ Microsoft Windows Server 2008 R2 Standard Edition（仅限 x64）。

如果您已在 CA PC 或 CA NPC 上注册了管理控制台，CA PC 或 CA NPC 将报告来自 VMware 的虚拟机相关性能统计信息以及来自 CA Virtual Systems Monitor 的性能数据。

要使 CA PC 或 CA NPC 能够显示来自 VMware 的虚拟机相关性能统计信息：

- 必须在您计划监视的 VM 上安装 VMware 工具。
- 如果您计划监视的虚拟机被分配给多个虚拟 NIC，则该虚拟机的管理 IP 地址必须分配给属于 ESX 主机上的最后一个物理 NIC 的网络适配器（虚拟 NIC）。这是一个 VMware 问题 - 当选中某个网络适配器时，只有当网络适配器分配给最后一个虚拟 NIC 时，VMware 才会显示其 IP 地址。例如，对于具有 3 个虚拟 NIC（VMNIC1、VMNIC2 和 VMNIC3）的虚拟机，将报告分配给 VMNIC3 的网络适配器的 IP 地址，而不会报告分配给 VMNIC1 和 VMNIC2 的此类信息。

添加 CA Virtual Systems Monitor

要配置 CA Virtual Systems Monitor，请完成以下任务：

1. 配置虚拟交换机 (p. 286)。
2. 创建虚拟机 (p. 292)。
3. 配置网络连接 (p. 294)。
4. 运行 CA Application Delivery Analysis 安装程序 (p. 298)。
5. 完成设置 (p. 299)。
6. 如何管理 CA Virtual Systems Monitor (p. 300)。

配置虚拟交换机

CA Virtual Systems Monitor 与 VMware vSwitch 或 Cisco Nexus 1000V 配合使用。

如何配置 VMware vSwitch

要监视 VMware vSwitch 上的虚拟机内通信量，可创建一个启用了混杂模式的专用监视器端口组，并将 CA Virtual Systems Monitor 上的监视器 NIC 分配给该监视器端口组。

CA Virtual Systems Monitor 旨在监视虚拟环境“内”虚拟服务器之间的通信。如果：

- 前端和后端服务器使用单独的 vSwitches：
  - 在后端 vSwitch 上启用混杂模式。
  - 将前端服务器通信量镜像到物理监视设备。
- 前端和后端服务器不使用单独的 vSwitches：
  - 在 vSwitch 上启用混杂模式。
  - 将前端服务器通信量镜像到物理监视设备，并将前端服务器“固定”到物理监视设备。

为了让 CA Virtual Systems Monitor 上的管理网络适配器与位于 ESX 主机外部的管理控制台进行通信，可以配置 CA Virtual Systems Monitor 使用现有的虚拟网络适配器，或创建一个新的管理端口组。不必在管理端口组上启用混杂模式。有关混杂模式的详细信息，请参阅您的 VMware 产品文档。

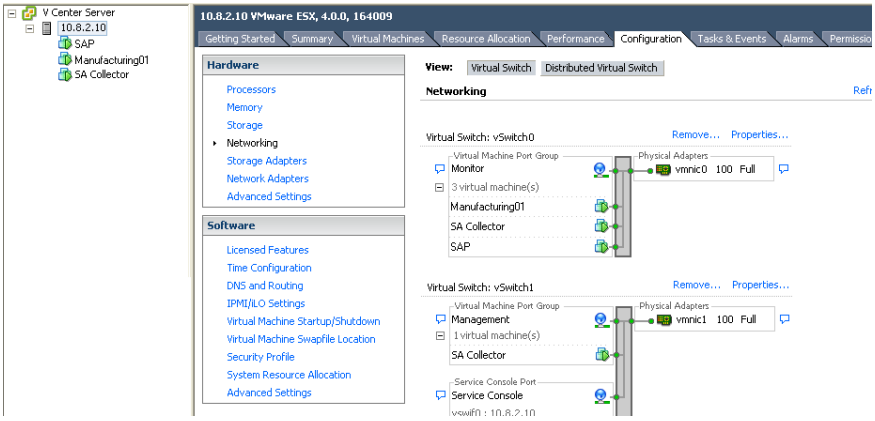
在以下示例中，将配置管理控制台虚拟机 (SA Collector) 使用监视器和管理网络。ESX 主机 10.8.2.10 配置有：

- vSwitch0。该虚拟交换机被分配给 vmnic0 设备，且其安全策略配置为在虚拟交换机和监视器端口组上接受混杂模式。使用混杂模式，CA Virtual Systems Monitor 可以针对连接到监视器网络的虚拟机（包括 Manufacturing01 和 SAP 虚拟机）观测服务器到服务器的通信量。

  vmnic0 网络适配器是上行链路端口，通过该端口，来自虚拟交换机外的客户端通信量可与虚拟交换机上的服务器（如将客户端请求发送到后端 SAP 服务器上 SAP 应用程序的面向外部的 Web 服务器）进行通信。

  要监视前端 Web 服务器到外部物理客户端（未显示）的通信量，请使用物理监控（如 CA Multi-Port Monitor）监视来自物理交换机的镜像服务器通信量。

- vSwitch1。该虚拟交换机被分配给 vmnic1 网络适配器，且其安全策略以及其上的管理端口组均配置为拒绝混杂模式。vmnic1 网络适配器是上行链路端口，通过该端口，CA Virtual Systems Monitor 可与不是由 ESX 主机承载的管理控制台进行通信。



遵循这些步骤:

1. 在 VMware vSwitch 上，创建启用混杂模式的专用端口组：
   a. 标识用于观测您要监视的应用程序通信量的 VMware vSwitch。
   b. 在 VMware vSwitch 上，使用以下设置创建专用监视器端口组：

   网络标签

   命名网络监视器。稍后，在配置虚拟机时，可通过镜像的应用程序通信量轻松标识网络适配器。

   VLAN ID

   指定您希望监视其应用程序通信量的 VLAN ID 或选择“全部”。如果未在使用 VLAN 标记，请保留该字段为空。

   如果您在 ESX 3.5 Server 上而且希望监视所有 VLAN，请将 VLAN ID 指定为 4095。

   如果虚拟机具有 AMD 适配器，您必须配置访客操作系统使用 Intel E1000 驱动程序。有关详细信息，请访问 http://kb.vmware.com/kb/1004252。

   混杂模式

   将安全策略配置为接受混杂模式，从而允许监视器端口组观测 VMware vSwitch 上的所有通信量。

2. 要在监视器端口组上启用混杂模式，VMware vSwitch 和监视器端口组必须配置为接受混杂模式。

   如果未在 VMware vSwitch 上启用混杂模式，需要将 VMware vSwitch 上的安全策略配置为接受混杂模式。

3. 如果 vSwitch 已有针对管理数据的端口组，请使用该端口组以便让 CA Virtual Systems Monitor 能够与管理控制台进行通信。

   如有必要，创建名为“管理”的端口组，以便标识未接收镜像的交换机通信量的网络适配器。

如何配置 Cisco Nexus 1000V

为了让 CA Virtual Systems Monitor 监视 Cisco Nexus 1000v 上的通信量，请为 CA Virtual Systems Monitor 创建一个专用端口配置文件，以便观测相应的 VLAN 通信量。配置好虚拟机后，您可以将 VLAN 通信量 SPAN 至该虚拟机上的监视器接口。有关镜像 VLAN 通信量的信息，请参阅您的 Cisco 产品文档。

选择要监视的 VLAN 时，如果：

- 前端服务器（来自 ESX 外部的通信量）和后端服务器（ESX 内部的内部通信量）使用单独的 VLAN，可将前端服务器通信量镜像到物理监视设备。
- 前端和后端服务器不使用单独的 VLAN，可将 ESX 中的所有通信量和进入 ESX 的外部通信量镜像到物理收集器，然后将前端服务器“固定”到物理监视设备。

遵循这些步骤:

1. 在 Cisco 虚拟监管模块 (VSM) 中，创建并启用专用监视器端口配置文件，CA Virtual Systems Monitor 可使用该配置文件来观测适当 VLAN 的 SPAN 通信量。有关创建端口配置文件的信息，请参阅您的 Cisco 产品文档。

   如果已存在用于管理数据的端口组或端口配置文件，请使用它以便让 CA Virtual Systems Monitor 与管理控制台进行通信。如有必要，创建一个名为“管理”的端口配置文件，以便在 CA Virtual Systems Monitor 上配置网络连接时，可以轻松标识缺少镜像的交换机通信量的网络适配器。

2. 创建 (p. 292)将承载 CA Virtual Systems Monitor 上的虚拟机，并配置该虚拟机使用监视器和管理网络适配器。
3. 将虚拟服务器到虚拟服务器的 VLAN 通信量 SPAN 至该 CA Virtual Systems Monitor 虚拟机上的监视器接口 (p. 294)。

与 SPAN 相关的其他注意事项

在配置 SPAN 时，切记：

- 源端口可以是以太网端口、虚拟以太网端口或 VLAN 接口。标准 SPAN 会话将仅 SPAN 同一物理 (ESX) 主机上的源和目标。
- 目标端口可以是任何物理或虚拟以太网端口，但不可以是端口通道。
- SPAN 会话的所有目标必须在同一主机上。例如，您不能在一个 SPAN 会话中使用 VLAN 作为源（在一台主机上），同时具有两个位于不同物理主机上的目标。
- 在 Cisco Nexus 1000V 上，最多只允许 16 个 SPAN 会话，但最多只允许 4 个会话具有同一源（如 VLAN）。在以下示例中，两个监视器会话都引用 VLAN 152 作为源，因此，仅 2 个以上的监视器会话可配置为使用 VLAN 152 作为源。

```
monitor session 1
  source vlan 152 both
  destination interface Vethernet6
  no shut
monitor session 2
  source vlan 152 both
  destination interface Vethernet9
  no shut
```

消除 VLAN 上的重复数据包

CA Virtual Systems Monitor 在接收数据包的两个副本（如将 VLAN SPAN 至 CA Virtual Systems Monitor）时，“工程”页面上的“数据包丢失百分比”报告将会错误地报告一个极高的丢失数据包百分比。

本节讨论如何使 CA Virtual Systems Monitor 消除重复的 TCP 数据包。

遵循这些步骤:

1. 在 C:\CA\bin 目录中找到 RetransPacketDefs.ini.sav 文件。
2. 从文件名中删除 .sav 扩展名。
3. 编辑 RetransPacketDefs.ini 文件。默认情况下，该文件包含以下条目：

   ```
   <no logging>
   50 1000
   10 20 30 40 50 60
   ```

   第一行告知 CA Virtual Systems Monitor 在何处记录有关重复数据包的信息。如果您将短语 <no logging> 替换为日志记录文件的路径（如 C:\CA\bin\duppkts.txt），CA Virtual Systems Monitor 将记录该信息。启用日志文件是一种不错的实践，可帮助您确定缓冲区大小是否合适。

   在第二行上，第一个数字 50 用于指定 CA Virtual Systems Monitor 维护可容纳 50 个数据包的缓冲区来查找重复项。如果您减少该参数，CA Virtual Systems Monitor 将使用较少的 CPU 周期来查找重复项。这将改善 CA Virtual Systems Monitor 的性能，但可能只能找到较少的重复项。请注意，将不使用第二个数字 1000。

   文件的最后一行说明重复项的直方图区间，它将显示在第一个行指定的日志文件中。该直方图显示了每个重复项距离原始位置有多远。该信息可帮助您调整缓冲区大小参数。理想情况下，重复项丢失主要发生在前几个直方图区间中，远程区间的计数会下降或消失。如果大编号区间的计数仍然很大，可能是由于缓冲区太小导致的。
4. 要应用您的更改，请重新启动 CA ADA Monitor 服务，等待 10 分钟以便管理控制台报告消除重复的数据，然后检查“数据包丢失百分比”报告以验证数据包丢失百分比是否降低。

   如有必要，请增加缓冲区大小，以便使 CA Virtual Systems Monitor 跨大量数据包搜索重复项。

创建虚拟机

创建虚拟机来承载 CA Virtual Systems Monitor。使用 CA Virtual Systems Monitor 来监视同一 VMware ESX 主机上各虚拟服务器之间的应用程序性能。

如果您的虚拟交换基础架构使用的是 Cisco 1000v，请确保记得将相应的 VLAN 通信量 SPAN 至监视器 NIC。

确保虚拟机满足以下要求。

设置	说明
虚拟机名称	指定虚拟机的名称（例如“CA Virtual Systems Monitor”）
数据存储	选择具有可用空间的数据存储。您应该计划为虚拟机分配 10 GB 存储空间。

设置	说明
访客操作系统	CA Virtual Systems Monitor 也要求： ■ Microsoft Windows Server 2003 Standard Edition SP2（64 位或 32 位） ■ Microsoft Windows Server 2008 R2 Standard（仅 64 位）。 安装操作系统之后，请执行以下操作： ■ 在 Windows Server 2003 上安装 Microsoft .NET Framework 3.5 SP1。Windows Server 2008 R2 已包含 Microsoft .NET Framework 3.5 SP1。 ■ 安装 SNMP，并确保 public 是接受的团体名称。 ■ 安装 ASP.NET，包括网络 COM+ 访问和 IIS。在为安装配置 IIS 时，单击以安装 SMTP 服务，并安装默认的 IIS 组件（公共文件、Internet 信息服务管理器、万维网服务）和 IIS 6 元数据库兼容性组件。 ■ 安装任何关键或重要更新。 ■ 不要安装推荐更新（同时列为 *“软件，可选”*）。 ■ 不要安装驱动程序更新（同时列为 *“硬件，可选”*）。 ■ 应当清除建议更新和驱动程序更新，应选择“不显示...”复选框以从未来扫描中隐藏该项。要寻求帮助，请联系 CA Support：http://support.ca.com。 ■ 在 Windows Server 2003 上卸载 Internet Explorer 增强的安全配置。 ■ 安装 VMware Tools（必需）。
虚拟 CPU	分配 1 个虚拟 CPU。
内存	分配 1 GB（1024 MB）
NIC	为管理 NIC 和监视器 NIC 创建 2 个网络连接。 ■ 网络适配器 1 上，选择“管理”网络。 ■ 网络适配器 2 上，选择“监视器”网络。

设置	说明
虚拟磁盘	■ 在 Windows Server 2003 上，创建一个新的虚拟磁盘，并分配 16 GB 的虚拟磁盘空间。请务必选择相关选项以便立即分配所有空间。在“高级”选项下，选中“独立”，然后选择“永久”。 ■ 在 Windows Server 2008 R2 上，创建一个新的虚拟磁盘，并分配 30 GB 的虚拟磁盘空间 。请务必选择相关选项以便立即分配所有空间。在“高级”选项下，选中“独立”，然后选择“永久”。
管理员帐户	■ 指定管理员帐户的密码并选择“密码永不过期”。 ■ 在本地 Administrators 组中创建一个名为 *netqos* 的用户，密码设为 *changeme*，然后选择“密码永不过期”。

详细信息：

如何配置 Cisco Nexus 1000V (p. 289)

配置网络连接

完成以下步骤，以便在访客操作系统上配置网络连接：

1. 重命名网络连接 (p. 295)。
2. 为网络连接配置高级设置 (p. 296)。
3. 为网络连接分配 IP 地址 (p. 297)。

重命名网络连接

为了更方便识别和配置您在配置虚拟交换机时创建的网络连接，请在访客操作系统中重命名网络连接，以便与绑定到虚拟机的“监视器”和“管理”网络适配器相对应。

遵循这些步骤:

1. 在 VMware vSphere 客户端中，标识“管理”和“监视器”网络适配器的 MAC 地址：
   a. 右键单击虚拟机，然后单击“编辑设置”。
   b. 在“虚拟机属性”中，记下监视器和管理网络适配器的 MAC 地址。
2. 在访客操作系统中，标识每个网络连接的 MAC 地址：
   a. 在 Windows 桌面上，单击“开始”菜单，然后右键单击“网上邻居”，并单击“属性”。或者依次单击“开始”、“控制面板”。右键单击“网络连接”，然后单击“打开”。
   b. 在 Windows 网络连接中，右键单击某个连接，然后单击“属性”。在“属性”对话框中，单击“支持”选项卡，然后单击“详细信息”。物理地址对应于“监视器”和“管理”网络适配器的 MAC 地址。

   提示：在命令提示窗口中，您可以运行 ipconfig /all 命令来验证 MAC 地址。
3. 单击“取消”。
4. 在“网络连接”窗口中，编辑与相应接口对应的默认名称，如下所示：
   a. 管理
   b. 监视器

详细信息：

配置虚拟交换机 (p. 286)

为网络连接配置高级设置

在访客操作系统中，配置高级网络连接设置，以指定正确的连接顺序和绑定。

遵循这些步骤:

1. 在“网络连接”中的“高级”菜单上，单击“高级设置”。
2. 在“适配器和绑定”选项卡上，使用右侧的向上箭头将“管理 NIC”移至顶部。该操作将设置优先级，且必须执行该操作，CA Virtual Systems Monitor 才能正确运行。
3. 在“绑定”框中，清除以下绑定上所有 NIC 对应的“Internet 协议 (TCP/IP)”选项。
   - Microsoft 网络的文件和打印机共享
   - Microsoft 网络客户端
4. 单击“确定”。

为网络连接分配 IP 地址

在访客操作系统中，为管理网络连接分配 IPv4 地址、子网掩码和默认网关。

如果您使用的是 VMware vSwitch，请为监视器网络连接配置一个非路由 IP 地址。使用非路由 IP 地址时，不必分配默认网关。

记下您分配给 NIC 的 IP 地址。您在将 CA Virtual Systems Monitor 添加到管理控制台时将需要该信息。

遵循这些步骤:

1. 在 Windows 桌面上，单击“开始”菜单，然后单击“控制面板”。
2. 在“控制面板”中，单击“网络连接”。
3. 右键单击“管理”，然后单击“属性”。
4. 在“常规”选项卡上，单击“Internet 协议 (TCP/IP)”，然后单击“属性”。
5. 选择“使用下面的 IP 地址”，并键入 IP 地址、子网掩码和默认网关。单击“确定”。
6. 对“监视器”网络连接重复这些步骤，但指定非路由 IP 地址和子网掩码，不要指定默认网关。我们建议以下值：

   监视器 1

   IP 地址：1.1.0.1

   子网掩码：255.0.0.0

详细信息：

如何配置 VMware vSwitch (p. 287)

运行 CA Application Delivery Analysis 安装程序

运行 CA Application Delivery Analysis 安装程序，以便在虚拟机上安装 CA Virtual Systems Monitor。在您运行安装程序之前，确保您可以通过“远程桌面”访问虚拟机。

CA Application Delivery Analysis 安装程序包含在 CA Application Delivery Analysis .iso 下载文件中。如有必要，请从 CA Support 网站 (http://ca.com/support) 下载 CA Application Delivery Analysis .iso。

在运行 CA Application Delivery Analysis 安装程序之前，请创建虚拟机快照，以便在必要时卸载 CA Virtual Systems Monitor。CA Application Delivery Analysis 安装程序不会卸载 CA Virtual Systems Monitor；您必须恢复到以前（安装前）的快照将其删除。有关获取虚拟机快照的信息，请参阅您的 VMware 文档。

遵循这些步骤:

1. 以具有管理员权限的用户身份登录到虚拟机。
2. 验证 CA Application Delivery Analysis 安装程序是否有权限运行。要完成该步骤，请右键单击安装程序可执行文件，然后单击“属性”。从该对话框中，单击“解除阻止”按钮（如果可用），然后单击“确定”。
3. 运行 CA Application Delivery Analysis 安装程序。安装程序将提示您输入以下信息：

   最终用户许可协议

   接受许可协议以继续安装。

   安装路径

   将 CA Virtual Systems Monitor 安装到 C:\CA 下。

   选择安装类型

   单击“虚拟系统监视器”以安装 CA Virtual Systems Monitor。
4. 在安装程序完成后，您必须重新启动访客操作系统。
5. 重新登录访客操作系统，并验证 (p. 269) CA Virtual Systems Monitor 是否正在观测 SPAN 通信量。

与时间服务器同步时间

如果您在不同的时区有监视设备，请将每个 CA Virtual Systems Monitor 设置为其本地时区，并使用时间服务器（如 NTP）来确保系统时间准确。时间将转换为格林尼治标准时间 (GMT)。

遵循这些步骤:

1. 打开命令提示窗口并运行以下命令：
   `net time /querysntp`

   记下 SNTP 服务器的名称。
2. 将以下命令中的 *<NTPServer>* 替换为查询中返回的 SNTP 服务器的名称：
   `net time /setsntp:<NTPServer>`
3. 将 Windows 时间服务配置为自动启动。
4. 重新启动计算机。

完成安装

执行以下安装后任务：

1. 检查 CA 支持网站 (http://support.ca.com) 上是否有 CA Virtual Systems Monitor 软件更新。
2. （可选）配置 CA Virtual Systems Monitor 筛选重复数据包 (p. 291)。
3. 安装防病毒软件，但将以下目录从扫描中排除：
   - C:\Windows\Temp
   - 安装目录（默认为 C:\CA）和所有子目录。
4. 验证系统时间和时区。如果您更改了这些值，请重新启动计算机。

安装后步骤

完成安装后，就可以将 CA Virtual Systems Monitor 添加到管理控制台中。记住以下几点：

- 使用与添加 CA Standard Monitor 相同的方式添加 CA Virtual Systems Monitor。添加 CA Virtual Systems Monitor 时，为 CA Virtual Systems Monitor 上的管理 NIC 和监视器 NIC 提供 IP 地址。
- 管理 CA Virtual Systems Monitor 的方式与管理 CA Standard Monitor 类似。使用 ADA 监视设备列表查看和管理您的 CA Virtual Systems Monitor 监视设备。

  请注意，在 ADA 监视设备列表中，CA Virtual Systems Monitor 具有与 CA Standard Monitor 相同的类型 - Standard Monitor。要将 CA Virtual Systems Monitor 与 CA Standard Monitor 区分开来，您需要了解 CA Virtual Systems Monitor 上管理 NIC 的主机名或 IP 地址。
- 不要将 Cisco WAE 设备或 CA GigaStor 分配给 CA Virtual Systems Monitor。

第 15 章： 使用 CA GigaStor 监视

此部分包含以下主题：

CA GigaStor 作为监视设备的工作方式

CA GigaStor 设备 (CA GigaStor) 可以作为 CA Application Delivery Analysis 的一种监视设备来运行。CA Application Delivery Analysis 负责识别性能问题的发生时间和源，CA GigaStor 负责对问题进行详细的根本原因分析。CA GigaStor：

- 是用于捕获所有 IPv4 TCP 数据包的固定捕获设备。有多个目标接口的单个 SPAN 会话使 CA GigaStor 和 CA Standard Monitor 能够共享 SPAN。无需分流。
- 与 CA Standard Monitor 不同，CA GigaStor 专用于捕获纯数据包，且可接收来自多个 SPAN 端口的多个接口（八个或更多）上的 TCP 数据包。
- 捕获整个数据包，以完成对话分析和重建。
- 将来自多个接口的 TCP 标头组合到单个 GigaStor 监视器源中。

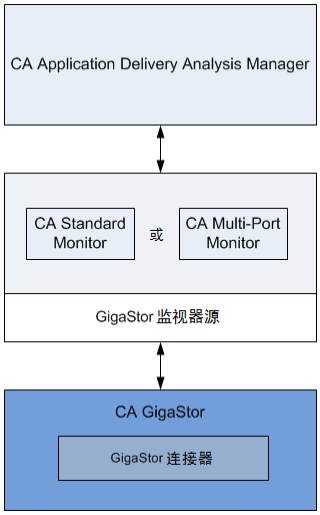
通过 CA GigaStor 连接器，管理控制台用户可快速轻松地分析已捕获并存储在 CA GigaStor 设备上的大量 IPv4 数据包数据，这样，网络工程师就能够在管理控制台中的网络、服务器和应用程序性能视图以及 CA Observer Expert 中的深度包检测之间无缝切换，从而轻松快速地排除故障。

CA GigaStor 连接器的工作方式

CA GigaStor 捕获被动复制（如从 SPAN、镜像端口或网络分流器复制）的所有数据包，并捕获整个数据包以便进行完整的对话分析和重建。

CA GigaStor 上的 CA GigaStor 连接器轮询管理控制台上的服务器子网、客户端网络和端口排除项列表。当数据包位于 CA GigaStor 上的内存中时，在被写入磁盘之前，CA GigaStor 连接器会将匹配的 TCP 标头数据复制到数据包摘要文件，并将摘要文件发送到其分配的监视设备。如有必要，可以将 CA GigaStor 分配给多个监视设备。CA 不建议将 CA GigaStor 分配给 CA Application Delivery Analysis Manager。

CA GigaStor 连接器将数据包摘要文件发送到为其分配的 CA Standard Monitor 或 CA Multi-Port Monitor，用于处理和计算每个应用程序/服务器/网络组合的响应时间度量标准。CA GigaStor 连接器不计算响应时间度量标准。



监视设备上的 GigaStor 监视器源将接收数据包摘要文件 。然后，管理控制台评估来自所有监视设备的响应时间度量标准，以便为每个服务器分配最佳监视器源，并监视每个服务器上最繁忙的 TCP 应用程序。

您还可以定义希望管理控制台监视的应用程序，然后在 CA GigaStor 上加载该配置。

详细信息：

管理应用程序 (p. 93)

监视器源分配的工作方式

如果 CA GigaStor 是针对给定服务器的最佳监视点，那么管理控制台会自动将相应的 GigaStor 监视器源分配给该服务器。

如果出于负载平衡的考虑已将 CA GigaStor 分配给多个 CA Standard Monitor 或 CA Multi-Port Monitor，则管理控制台在进行服务器分配时会将 GigaStor 监视器源视为单个“逻辑”源。手动分配 GigaStor 监视器源时，您可以将任何一个 GigaStor 监视器源分配给服务器。

详细信息：

监视器源分配的工作方式 (p. 223)

数据包捕获调查的工作方式

为服务器分配 CA GigaStor 监视器源后，管理控制台会通过观测数据包的相应 CA GigaStor 在该服务器上执行数据包捕获调查。

管理控制台在 CA GigaStor 上启动数据包捕获调查时，管理控制台将会无缝深入到 CA Observer Expert。CA Observer Expert 提供数据包级别详细信息和专家分析，以确定该性能问题的根本原因。

您可以在 CA GigaStor 上启动或排定数据包捕获调查，正如您在其他类型的监视设备上执行的操作一样。在数据包捕获调查报告中，单击数据包捕获调查报告中的链接可创建 CA Observer Expert 筛选器，以便在 CA Observer Expert 中显示 CA GigaStor 上需要的数据包。与 CA Standard Monitor 上的数据包捕获调查不同，不会有数据包捕获文件复制到您的本地计算机。

推荐大小

CA GigaStor 将数据包摘要文件发送到分配的监视设备上的管理 NIC 中进行处理。根据 CA GigaStor 的加载方式，您应将一个 CA GigaStor 至少分配给一个监视设备。您无法将多个 CA GigaStor 分配给同一个监视设备。

为了避免所分配的监视设备上的管理 NIC 过载，请勿将 CA GigaStor 分配给同时从另一个监视设备（如 Cisco WAE 设备）接收数据包摘要的监视设备。

监视设备注意事项

将 CA GigaStor 用作监视设备时，请记住：

- 通常，CA 技术代表会帮助您将 TCP 通信量镜像到监视设备。

  注意：有关数据获取最佳实践的信息，请参阅*《安装指南》*。

- 配置管理控制台在 CA GigaStor 上执行数据包捕获调查时，不必指定：
  - 最大文件大小。最大文件大小不适用，因为 CA GigaStor 捕获和存储所有数据包，因此不存在捕获文件。数据包捕获调查会创建 CA Observer Expert 筛选以显示您需要的数据包。
  - 每个数据包的字节数。CA GigaStor 捕获整个数据包。
- 要限制对所捕获的潜在敏感内容的访问，请针对 CA GigaStor 上的被动探测器实例授予用户权限 (p. 305)。
- CA GigaStor 可以根据管理控制台上定义的客户端网络、服务器子网和端口排除，自动监视匹配的应用程序通信量。
- CA GigaStor 连接器不存储数据包摘要文件，因此，如果 CA GigaStor 连接器无法与分配的 CA Standard Monitor 或 CA Multi-Port Monitor 进行通信，管理控制台将报告缺少数据。但是，CA GigaStor 会不断捕获 TCP 数据包，您可以在 CA GigaStor 上使用 Observer 查看数据。
- 管理控制台无法使用来自 CA GigaStor 连接器的基于 TCP 的性能数据来监视 Web 应用程序的性能。CA GigaStor 连接器中的性能数据不包括确定 Web 应用程序的关联 URL 所需的 HTTP 标头信息。

  要使管理控制台能够通过 CA GigaStor 设备监视 Web 应用程序，请定义标准应用程序来监视所有 TCP-80 通信，或者使用 CA Observer Expert 监视该 Web 应用程序。

添加 CA GigaStor 监视设备

要将 CA GigaStor 添加为 CA Application Delivery Analysis 的监视设备，请执行以下任务：

1. 验证先决条件 (p. 305)，包括所需的端口访问。
2. 在 CA GigaStor 设备上安装并配置所需的软件 (p. 305)。
3. 添加 CA GigaStor 监视设备 (p. 306)。
4. 将 CA GigaStor 分配给监视设备 (p. 307)。
5. 在用户的客户端计算机上安装所需的 CA Observer 软件 (p. 305)。
6. 授予用户 (p. 310)访问 CA GigaStor 上被动探测器实例的权限。

先决条件

下面列出了添加 CA GigaStor 监视设备的先决条件：

- 已在 CA GigaStor 安装 CA Observer 软件。如果您要升级连接器，那么可以从 CA Support 网站 (http://ca.com/support) 下载 CA Observer 升级程序。
- 配置 CA GigaStor 上的时间和日期，以匹配为其分配的 CA Standard Monitor 或 CA Multi-Port Monitor 上的时间和日期。

  使用为 CA GigaStor 分配的监控的时间戳为其收集的性能数据加上时间戳。如果您已配置监控使用网络时间协议 (NTP)，则在 CA GigaStor 上配置 NTP。
- 监视设备比率 (p. 231)大小设置正确。
- CA Standard Monitor 或 CA Multi-Port Monitor 可用于将来自 CA GigaStor 连接器的摘要文件处理成响应时间数据。要在 CA Standard Monitor 上最大化可用资源，请在添加 CA Standard Monitor (p. 254) 时禁用数据包监视。
- 管理控制台可通过 TCP-1001 与 CA GigaStor 进行通信。
- CA GigaStor 可通过 UDP-9995 与分配的 CA Standard Monitor 或 CA Multi-Port Monitor 进行通信。
- 要在 CA GigaStor 上打开数据包捕获调查的管理控制台用户可在 TCP-25901 - 25903 上与 CA GigaStor 进行通信。
- 您可以通过“远程桌面”使用 Windows 终端服务 (RDP) 在 TCP-3389 上访问 CA GigaStor。

在 GigaStor 设备上安装并配置软件

请按下列步骤安装所需软件：

- 在 CA GigaStor 设备上安装 CA GigaStor 连接器。
- 针对每个管理控制台用户，在 CA GigaStor 上创建一个被动探测器实例。

安装 CA GigaStor 连接器

在 GigaStor 设备上安装 CA GigaStor 连接器，以将您的 CA GigaStor 设备用作 CA Application Delivery Analysis 的监视设备。连接器的版本号应与 CA Observer 的版本匹配。联系 CA Support 以下载正确的版本。

要安装 GigaStor 连接器，请在 GigaStor 桌面上运行连接器安装程序。安装完成时，请重新启动系统。

为每位用户创建一个被动探测器实例

要允许管理控制台用户打开 CA GigaStor 上的数据包捕获调查，请为您希望访问 CA GigaStor 的每个管理控制台用户创建被动探测器实例。

为了避免管理控制台用户与 CA Observer Expert 的连接意外断开，请不要在管理控制台用户之间共享被动探测器实例。如果管理控制台用户使用一个已被占用的 CA GigaStor 探测器实例打开 CA GigaStor 数据包捕获调查，则现有用户与 CA GigaStor 的连接将被断开。

有关在 CA GigaStor 上创建被动探测器实例的信息，请参阅 CA GigaStor 产品文档。

添加 CA GigaStor 监视设备

将 CA GigaStor 监视设备添加为管理控制台中的数据源。如果您需要按域分隔重复的 IP 通信量，请在添加 CA GigaStor 后，编辑 GigaStor 监视器源 (p. 313)，并将 GigaStor 监视器源分配给需要的域。

添加 CA GigaStor 后，将 CA GigaStor 分配给监视设备 (p. 307)。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 在“向我显示”菜单中，单击“添加 GigaStor”。

   将打开“GigaStor 属性”。
4. 完成“GigaStor 属性”中的字段，然后单击“确定”。
5. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

将 CA GigaStor 分配给监视设备

将 CA GigaStor 添加到管理控制台后，可将其分配给 CA Standard Monitor 或 CA Multi-Port Monitor，以便将来自 CA GigaStor 连接器的摘要文件处理成响应时间数据。不要将 CA GigaStor 分配给 CA Virtual Systems Monitor。

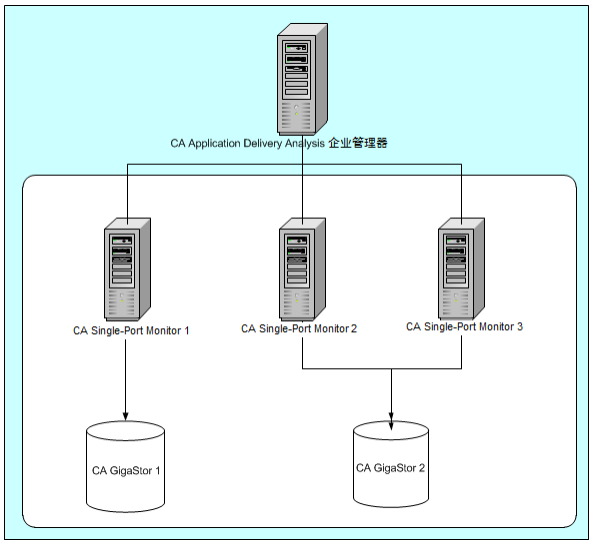
要在 CA Standard Monitor 上最大化可用资源，请在添加 CA Standard Monitor (p. 254) 时禁用数据包监视。

如果出于可伸缩性考虑而希望对来自单个 CA GigaStor 的监视器源进行负载平衡，那么可将 CA GigaStor 分配给多个 CA Standard Monitor 或 CA Multi-Port Monitor。如果在两个监视设备之间对 CA GigaStor 进行负载平衡，CA GigaStor 连接器会基于以下端点之一的 IP 地址自动将通信量分发给每个监视设备：

- 服务器 IP 地址（如果为客户端-服务器连接）
- 最小的 IP 地址（如果为多层应用程序的服务器-服务器连接）

CA GigaStor 连接器将来自具有偶数 IP 地址的服务器的通信量的数据包摘要文件发送给一个监视设备，而将来自具有奇数 IP 地址的服务器的通信量发送给另一个。

如以下示例所示，您可以将 CA GigaStor 分配给多个 CA Standard Monitor 或 CA Multi-Port Monitor。



如果您的部署包含单个管理控制台和 CA GigaStor，则将 CA GigaStor 分配给管理控制台上的监控。

遵循这些步骤:

1. 单击“监管”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“ADA 监视设备列表”，然后单击 以编辑您希望将 CA GigaStor 分配到的 CA Standard Monitor 或 CA Multi-Port Monitor。使用“活动源”列确定是否将 CA GigaStor 分配给了监控。
4. 在第三个“向我显示”菜单中，单击“监视器设备”。

   将打开“监视器设备”。
5. 从“GigaStor 设备”列表单击 CA GigaStor，然后单击“确定”。
6. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

使用 CA Standard Monitor 监视 (p. 247)
在 GigaStor 设备上安装并配置软件 (p. 305)

在用户计算机上安装 CA Observer

要允许管理控制台用户打开 CA GigaStor 上的数据包捕获调查，必须在用户的计算机上安装下列软件组件：

- CA Observer Expert。CA Observer Expert with CA GigaStor 扩展了 CA Application Delivery Analysis 的全局应用程序响应时间监视，以便深入查看数据包级别的数据来进行根本原因分析。

  CA Observer Expert 必须能够通过 TCP-25901 - 25903 与 CA GigaStor 进行通信。有关在管理控制台计算机上安装和授权 CA Observer Expert 的详细信息，请联系您的 CA GigaStor 管理员。与 CA Observer Expert 连接器不同，用户无法从管理控制台安装 CA Observer Expert。

- CA Observer Expert 连接器。在管理控制台用户首次尝试打开 CA GigaStor 上的数据包捕获调查时，“数据包捕获调查”报告会显示一个提示您安装 CA Observer Expert 连接器的链接。

  在“必需的软件”下，单击箭头链接以运行连接器安装程序。

授予用户访问被动探测器实例的权限

要允许管理控制台用户打开 CA Observer 中 CA GigaStor 上的数据包捕获调查，请授予 CA Application Delivery Analysis 用户访问 CA GigaStor 上的被动探测器实例的权限。

如果 CA GigaStor 具有多个主动探测器实例，则授予用户访问与活动探测器实例对应的被动探测器实例的权限。您不能将管理控制台用户权限授予给同一 CA GigaStor 上的多个被动探测器实例。默认情况下，管理控制台连接到 CA GigaStor 上的第一个主动探测器实例。有关允许管理控制台连接到 CA GigaStor 上另一主动实例的信息，请联系 CA Support。

有关探测器实例管理的信息，请参阅 CA GigaStor 产品文档。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“安全”、“GigaStor 实例”。

   将打开“GigaStor 实例(按用户)”。

   如果未显示“GigaStor 实例”命令，则确认至少已将一个 CA GigaStor 添加 (p. 306)到了管理控制台。
3. 单击  以编辑管理控制台用户。

   将打开“*<user>* 的 GigaStor 实例”。
4. 键入您希望管理控制台用户在 CA GigaStor 上访问的被动实例名称，然后单击“确定”。

   “GigaStor 实例(按用户)”将刷新“GigaStor 设备 [实例名]”列，以便显示 GigaStor 上该被动实例的名称。

阻止 CA GigaStor 输入端口

如果您注意到观测数比预期多了一倍，NRTT 翻番，则可能需要排除来自 CA GigaStor 设备上选定监视器端口的所有数据包。端口阻止功能是在多层环境中进行监视的有效方式。如果您已配置 CA GigaStor，使不同端口从不同的有利位置（如接入交换机和分布式交换机）报告同一服务器的通信量，则可以排除来自分布式交换机的数据，这样，那些数据包就不会被视为从接入交换机收集的数据包的重复项。

遵循这些步骤:

1. 登录到 CA GigaStor。
2. 将目录更改为 C:\NetQoS\GigaStorReader，然后创建名为 BlockedGigaStorPorts.ini 的文件。
3. 打开 BlockedGigaStorPorts.ini 并使用以下格式添加条目：
   `/exclude port=`*`port`*

   其中，*port* 是介于 0 到 7 的端口值，该值将映射到 CA GigaStor 接口 1 到 8 。要指定 CA GigaStor 上的多个输入端口，请使用逗号分隔每个条目。

编辑 CA GigaStor 监视设备

例如，编辑 CA GigaStor 监视设备，以便：

- 查看 CA GigaStor 设备上 CA GigaStor 连接器和 CA Observer Expert 软件的版本信息。
- 查看 CA GigaStor 上负责将数据包摘要文件发送到分配的监控的进程的状态。
- 为监视设备分配突发事件响应
- 在特定 CA GigaStor 上执行基本操作（如启动和停止 CA GigaStor 连接器）。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 单击 以编辑“GigaStor 设备列表”中的 CA GigaStor。

   将打开“GigaStor 属性”。
4. 查看状态信息，对指定设置进行更改，然后单击“确定”。

   有关设置 CA GigaStor 属性的信息，请单击“帮助”。

   要查看 CA GigaStor 的监视设备突发事件，请在第三个“向我显示”菜单中单击“突发事件”。

详细信息：

查看监视设备突发事件 (p. 235)

编辑 GigaStor 监视器源

*GigaStor 监视器源*从 CA GigaStor 监视设备接收数据包摘要文件。编辑 GigaStor 监视器源，以便：

- 分配一个特定的域。默认情况下，新的监视器源会分配到默认域。如果您没有使用域来分隔重复的 IP 通信量，这将不适用。
- 创建一对监视器源，使管理控制台能够自动从两个监视器源上收集已分配服务器的数据。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 浏览“ADA 监视设备列表”中的“活动源”列，以查找具有活动 GigaStor 监视器源的监视设备。
4. 单击 以编辑监视设备。

   如果您不确定要编辑哪个监视设备，可使用“GigaStor 设备列表”中的“已分配”列查找 CA GigaStor 分配到的监视设备。
5. 在监视设备的属性对话框中，向下滚动到“监视器源”。
6. 单击 以编辑 GigaStor 监视器源。
7. 对 GigaStor 监视器源设置进行更改，然后单击“更新”。

   有关设置 GigaStor 监视器源属性的信息，请单击“帮助”。
8. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
创建一对监视器源 (p. 225)
监视设备的工作方式 (p. 221)

取消分配 CA GigaStor

取消分配 CA GigaStor，以将其作为响应时间数据源删除。取消分配监视设备时，将取消连接已连接到对应监视器源的所有服务器，并自动分配另一个监视器源。更新监视器源分配可能需要长达 10 分钟。

如果您已将服务器连接到 GigaStor 监视器源，并且您想在临时取消分配 GigaStor 时继续监控服务器通信，则请考虑下列选项：

- 取消分配 GigaStor 之前，将服务器连接到其他监视器源。重新分配 GigaStor 时，将适当的服务器连接到该 GigaStor 监视器源。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“ADA 监视设备列表”，然后单击 以编辑分配 CA GigaStor 的 CA Standard Monitor 或 CA Multi-Port Monitor。
4. 在第三个“向我显示”菜单中，单击“监视器设备”。
5. 在“已分配设备列表”中单击 以取消分配 CA GigaStor。
6. 当系统提示时，单击“继续取消分配”以继续。

   管理控制台将更新“已分配设备列表”。
7. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

GigaStor Incidents

如果 CA GigaStor 出现以下情况，管理控制台将自动创建“重大”监视设备突发事件：

- 停止向管理控制台发送数据超过 1 小时
- 处理的数据包未达到所接收数据包的 5%

详细信息：

编辑监视设备突发事件阈值 (p. 236)

执行基本操作

在“CA GigaStor 设备”列表中，使用蓝色齿轮菜单 可以在您的所有 CA GigaStor 设备上执行基本操作，包括启动和停止 CA GigaStor 连接器以及同步监视。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 在“GigaStor 设备”列表中单击蓝色齿轮菜单 ，可在您的所有 CA GigaStor 设备上执行基本操作。要执行基本操作，请浏览列表，单击编辑图标 ，然后单击蓝色齿轮菜单 ：

   开始

   启动连接器。当连接器的状态为“正在运行”时，将向分配的监控发送数据包摘要文件以便生成管理控制台报告。

   停止

   停止连接器。当连接器的状态为“已停止”时，CA GigaStor 会继续将数据包写入磁盘，但连接器不会向分配的监控发送数据包摘要文件。管理控制台报告中的数据缺口可使用 CA Observer Expert 查看 CA GigaStor 上的实际数据来解决。

   同步监视器设备

   同步 CA GigaStor，以针对控制台中当前定义的客户端网络、服务器子网和应用程序收集性能数据。

详细信息：

监视设备同步的工作方式 (p. 224)

删除 CA GigaStor 监视设备

可以删除 CA GigaStor 监视设备，不再将其作为管理控制台的响应时间数据源。如果您不再希望将 CA GigaStor 用作监视设备，可以从已分配的监控取消分配 CA GigaStor，然后删除 CA GigaStor。

或者，您可以将 CA GigaStor 分配 (p. 307)给其他 CA Standard Monitor 或 CA Multi-Port Monitor。

详细信息：

将 CA GigaStor 分配给监视设备 (p. 307)

删除 CA GigaStor

可以删除 CA GigaStor，不再将其作为管理控制台的响应时间数据源。

若要删除某个 CA GigaStor，它不能已被分配给 CA Standard Monitor 或 CA Multi-Port Monitor。请先取消分配 CA GigaStor，然后从管理控制台删除 CA GigaStor (p. 314)。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 单击 以从“GigaStor 设备”列表中删除 CA GigaStor。
4. 当系统提示时，单击“继续删除”以删除 CA GigaStor。

   该 CA GigaStor 将从“GigaStor 设备”列表中删除。
5. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

排除 CA GigaStor 监视设备故障

对 CA GigaStor 进行故障排除，识别本应由 CA GigaStor 监视的报告数据的缺失原因。添加 CA GigaStor 监视设备后，管理控制台可能需要花费长达 10 分钟才能报告性能数据。

查看 GigaStor 监视器源上的活动会话

使用“活动会话”页面，可以报告最后 5 分钟报告间隔内由 GigaStor 监视器源报告的活动 IPv4 TCP 会话的数目。GigaStor 监视器源包括来自分配给监视设备的任何 CA GigaStor 设备的会话信息。

查看活动会话信息 (p. 227)，以确认监视器源正在监视 TCP 会话。管理控制台按应用程序端口报告服务器上的活动 TCP 会话的数目。如果监视器源没有服务器或应用程序的任何活动会话，则表示 CA GigaStor 配置存在问题。

查看 GigaStor 计数器统计信息

GigaStor 计数器显示它从所分配的 CA GigaStor 连接器接收的数据包摘要的相关信息，包括有关传输数据包摘要的 Netflow 数据包的信息。

要查看 GigaStor 计数器，请登录 CA Standard Monitor (p. 268)（CA GigaStor 被分配到的监视器）。

重要提示：开始之前，请同步监视设备。直到同步数据监视之后，才会显示计数器窗口。

GigaStor 计数器显示以下统计信息：

正常数据流

表示已按发送顺序正常接收的 Netflow 数据包的数目。

丢弃的数据流

表示未经 CA ADA Monitor 服务处理的 Netflow 数据包的数目。来自丢弃的 Netflow 数据包中所包含的数据包摘要的任何响应时间数据都不会包含在管理控制台报告中。

无序数据流

表示已被监控接收但未按照发送顺序接收的 Netflow 数据包的数目。

到服务器数据包

表示从客户端发往服务器的数据包的数目。

来自服务器数据包

表示从服务器发往客户端的数据包的数目。

到服务器字节

表示从客户端发往服务器的字节数。

来自服务器字节

表示从服务器发往客户端的字节数。

可见数据包总计

表示 CA GigaStor 连接器在确定数据包标头是否与指定应用程序端口、客户端网络和服务器子网相匹配时检查的数据包的数目。

捕获的字节总计

表示匹配指定应用程序端口、客户端网络和服务器子网的数据包的总字节数。

注意：监控检查每个数据包标头，以便确定该数据包是否与指定应用程序端口、客户端网络和服务器子网相匹配。有关详细信息，请参阅“可见数据包总计”。

已接受的会话

表示匹配管理控制台上有效的应用程序/服务器/网络组合的 TCP 会话的数目。

服务器被拒绝

表示服务器 IP 与管理控制台监视的服务器子网不匹配。

客户端被拒绝

表示客户端 IP 与管理控制台要监视的客户端网络的列表不匹配。

端口被拒绝

表示服务器端口与管理控制台应忽略的端口的列表相匹配。

正当拒绝

保留给将来使用。

详细信息：

客户端网络的工作方式 (p. 27)
应用程序的工作方式 (p. 93)
服务器的工作方式 (p. 61)

第 16 章： 使用 Cisco WAAS 监视

此部分包含以下主题：

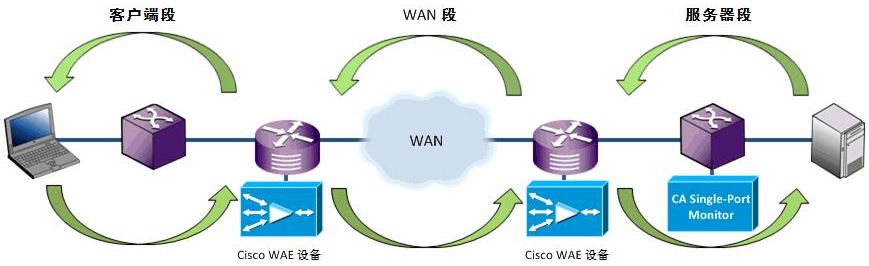
Cisco WAAS 作为监视设备的工作方式

Cisco WAE 设备 (Cisco WAE) 可以作为 CA Application Delivery Analysis 的一种监视设备来运行。使用 Cisco WAE 设备可了解优化。与监视服务器 SPAN 的监视设备不同，Cisco WAE 设备跨网络分布。

通过监视 Cisco WAE 设备之间的 WAN 优化，您可了解 Cisco WAAS 优化对每个网段上的各个应用程序响应时间有什么样的影响。

在以下示例中，位于分支和数据中心位置的 Cisco WAE 设备将优化的应用程序性能数据发送到同时监视服务器 SPAN 的 CA Standard Monitor。CA Standard Monitor 将执行以下操作：

- 计算客户端和 WAN 段上优化通信量的性能度量标准。
- 将来自数据中心 WAE 的服务器段性能数据替换为由 CA Standard Monitor 从服务器的镜像交换机端口收集的更准确的性能数据。
- 自动监视服务器 SPAN 中的应用程序通信量，并使用要由所有监视设备监视的服务器列表更新管理控制台。



监视 Cisco WAAS 环境时，不需要监视服务器的镜像交换机端口。

详细信息：

监视设备注意事项 (p. 326)

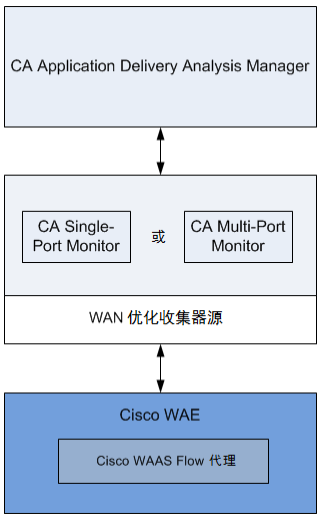
Cisco WAAS 的工作方式

Cisco WAE 设备上的 Cisco WAAS Flow Agent 每 5 分钟轮询一次管理控制台，以获取要监视的服务器 IP 地址的列表。Cisco WAAS Flow Agent 将带有已优化通信量的匹配 TCP 标头的数据包摘要文件发送给分配的 CA Standard Monitor 或 CA Multi-Port Monitor。要求分布式的管理控制台。

数据包摘要文件由 CA Standard Monitor 或 CA Multi-Port Monitor 上的 WAN 优化监视器源接收，并处理成观测的每个应用程序/服务器/网络组合的响应时间度量标准。

Cisco WAAS Flow Agent 基于管理控制台上存储的服务器的列表监视应用程序通信量。若要让 Cisco WAAS Flow Agent 自动监视新服务器通信量，则需要使用其他监视设备监视服务器 SPAN。

Cisco WAAS Flow Agent 不为未优化通信量发送 TCP 标头，也不计算响应时间度量标准。



与 Cisco NAM Metric Agent 不同，Cisco NAM Metric Agent：

- 发送包括 TCP 标头（而不是计算的响应时间度量标准）的数据包摘要文件。
- 为与服务器列表匹配的已优化通信量（而不是所有已优化通信量）发送 TCP 标头。

监视器源分配的工作方式

管理控制台自动组合来自所有 Cisco WAE 设备的响应时间度量标准，以便计算每个网段上的应用程序响应时间。如果有一个监控正在监视服务器 SPAN，而且该监控与服务器离得最近，则管理控制台会分配该监视器源来监视服务器段。否则，管理控制台将把 WAN 优化监视器源分配给服务器。

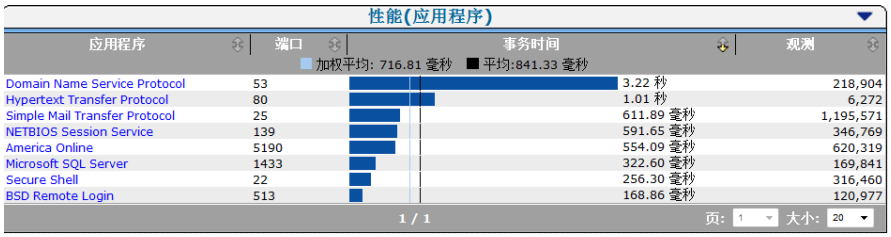
网段的工作方式

由于管理控制台是从网络上的多个点来监视应用程序-服务器-网络的单一组合，因为管理控制台会为三个网段中的每一个生成一组单独的度量标准，并将每个网段视为一个单独的应用程序。管理控制台为下面的每一个段生成一组单独的度量标准：

- 客户端段，即分支位置中的客户端 IP 与分支 WAE 设备之间的网段。为了报告该网段，管理控制台需要分支 WAE 设备导出响应时间数据。
- WAN 段，即分支 WAE 设备与数据中心 WAE 设备之间的网段。为了报告该网段，管理控制台需要数据中心 WAE 设备导出响应时间数据。
- 服务器段，即数据中心 WAE 设备与数据中心服务器之间的网段。为了报告该网段，管理控制台需要数据中心 WAE 设备导出响应时间数据。

  使用监视设备监视服务器 SPAN 时，管理控制台将来自数据中心 Cisco WAE 的服务器段数据替换为更准确的服务器 SPAN 数据。由于服务器的 SPAN 源更接近实际服务器，因此它更准确。如果管理控制台在服务器 SPAN 中观测到 未优化的应用程序通信量，它将为未优化的应用程序（如 SMTP）另外生成一组单独的度量标准。

管理控制台将网段追加到应用程序名称上，如 SMTP [客户端]、SMTP [WAN] 和 SMTP [服务器]。在下面的示例中，SMTP 应用程序代表未优化的应用程序性能。请注意，由于数据来自数据中心的本地用户，因此未优化应用程序的响应时间更短。



性能阈值如何对 WAN 优化的网段发挥作用

管理控制台创建独立的应用程序，以便跨网络的客户端段、WAN 段以及服务器段报告应用程序性能。自定义每个网段的应用程序性能阈值，以提高或降低管理控制台对性能变化的敏感度。

详细信息：

编辑 WAN 优化网段的性能阈值 (p. 143)

优化停止时如何监视

根据优化中断的时间长度，管理控制台会对受影响的通信量使用不同的报告方式。如有必要，您可以重置管理控制台来忽略优化中的最新更改，并基于当前可用的优化信息来报告优化和未优化的通信量。有关详细信息，请参阅下面的内容。

临时中断

如果管理控制台暂时停止了从 Cisco WAE 接收分段的应用程序性能数据，管理控制台将使用来自未优化的服务器 SPAN 的数据报告服务器段中的应用程序情况。管理控制台使用几个条件来确定中断是临时性还是永久性的，但临时中断通常不超过 20 分钟。

当管理控制台针对来自服务器段中服务器镜像交换机端口的未优化应用程序数据临时报告时：

- 虽然“优化”页面上的度量标准并未全部得到填充，但这些度量标准都是正确的。
- 未优化会话的度量不影响客户端或 WAN 段。
- 由于管理控制台总是使用来自服务器镜像交换机端口的更准确数据，因此服务器段是准确的。
- 在“工程”页面上显示的“网络往复传输时间 [服务器]”会显示增量，因为它不再能获得 100% 本地 ACK。外溢度量显示传出到客户端的实际网络往复传输时间。
- “RetransDelay [服务器]”和“PacketLossPct [服务器]”也可能会显示增量。

恢复优化数据时，管理控制台会自动报告应用程序的客户端、WAN 和服务器段的分段应用程序数据。

优化监视可能会出现临时中断，例如在以下情况下：

- 优化停止。当 Cisco WAE 没有资源来优化其他会话时，可能会发生此情况。未优化的会话称为 *“外溢”*。
- 监视停止。当 CA Standard Monitor 或 CA Multi-Port Monitor 停止从分配的 Cisco WAE 设备接收数据包摘要时（例如，Cisco WAE 与分配的监视设备之间的链路出现中断，或者 Cisco WAE 未配置为导出响应时间数据），就可能会发生这种情况。

永久更改

管理控制台使用几个条件来确定中断是临时性还是永久性的；如果 Cisco WAE 停止发送分段的应用程序性能数据超过 20 分钟，管理控制台通常认为这是永久性中断。在这种情况下，管理控制台将停止报告来自应用程序的服务器段中的服务器镜像交换机端口的未优化通信量（如 HTTP [服务器]），而改为报告未优化应用程序 HTTP 中的 SPAN 数据。优化恢复后，管理控制台将自动恢复到按网段监视优化的应用程序。

例如，如果您正在设置 WAAS 优化，若要度量优化不同应用程序的优点，而且您希望管理控制台立即报告优化中的更改，则可以重置 (p. 324, p. 334)管理控制台。

推荐大小

Cisco WAE 设备将数据包摘要文件发送到分配的 CA Standard Monitor 或 CA Multi-Port Monitor 上的管理 NIC 进行处理。

CA Standard Monitor 或 CA Multi-Port Monitor 可以针对至少 50,000 个优化连接处理来自全部三个数据段（客户端、WAN 和服务器）的数据包摘要文件。如果可能，请不要将多个数据中心 WAE 分配给同一个监控。在可用 CA Standard Monitor 或 CA Multi-Port Monitor 中对分支 Cisco WAE 设备进行负载平衡。

为了避免 CA Standard Monitor 或 CA Multi-Port Monitor 上的管理 NIC 过载，请不要将 Cisco WAE 设备分配给同时从 CA GigaStor 接收数据包摘要的监控。

监视设备注意事项

使用 Cisco WAE 作为监视设备时，请记住：

- 管理控制台需要分支 WAE 设备在客户端网段上导出应用程序响应时间。如有必要，您可以直接启用数据中心 WAE 设备来跨 WAN 和服务器段将应用程序性能报告给管理控制台。
- 管理控制台无法按网段报告以下应用程序的性能：
  - FTP 应用程序（因为 Cisco WAAS 不会优化 FTP）。
  - Web 应用程序（按 URL）。或者，您可以定义标准应用程序来跨客户端段、WAN 段和服务器段监视所有 TCP-80 通信量。
- 如果在 Cisco WAE 设备与其已分配的 CA Standard Monitor 或 CA Multi-Port Monitor 之间的通信中断，Cisco WAAS Flow Agent 会暂时存储其数据包摘要文件，以避免报告数据丢失。
- Cisco WAAS Flow Agent 每 5 分钟轮询一次管理控制台，以获取要监视的服务器 IP 地址的列表。

  要允许 Cisco WAE 设备监视与服务器子网匹配的新服务器通信量，请配置监视设备监视服务器 SPAN（如 CA Multi-Port Monitor）。如果您仅使用 Cisco WAE 设备收集响应时间数据，请手动更新控制台，以添加希望监视的服务器的 IP 地址。

  要查看管理控制台监视的服务器的列表，请在“向我显示”列表中，依次单击“数据监视”、“服务器”。
- Cisco WAE 设备不捕获有关未优化的通过通信量的性能信息。要监视“通过”应用程序的应用程序性能，请配置监视设备来监视服务器 SPAN，如 CA Multi-Port Monitor。
- Cisco WAE 设备可识别和消除重复数据，因此，不必通过配置 CA Standard Monitor 或 CA Multi-Port Monitor 来消除来自 WAN 优化监视器源的重复数据包。
- 但是，数据包捕获调查无法从 Cisco WAE 设备执行，例如，如果您使用 CA Multi-Port Monitor 监视服务器 SPAN，管理控制台将使用此设备执行数据包捕获。

添加 Cisco WAE 监视设备

要将 Cisco WAE 监视设备添加到管理控制台中，请执行以下任务：

1. 配置 Cisco WAE (p. 328) 设备导出应用程序响应时间数据。
2. 分配 Cisco WAE (p. 329) 给 CA Standard Monitor 或 CA Multi-Port Monitor。
3. 等待至多 10 分钟，让 Cisco WAE 设备轮询 CA Application Delivery Analysis Manager 以获取要监视的服务器的列表，并让管理控制台显示优化应用程序的数据。

   必要时，排除 Cisco WAE 设备的故障 (p. 335)，以确认 Cisco WAE 设备正在监视优化的应用程序。

先决条件

要添加 Cisco WAE 监视设备，您必须满足以下先决条件：

- Cisco WAE 运行受支持版本的 Cisco WAAS 软件。管理控制台支持 Cisco WAAS 4.0.17 到 4.4.3a，并将数据包摘要文件发送到：
  - CA Standard Monitor
  - CA Multi-Port Monitor
- 在每个 Cisco WAE 以及分配的 CA Standard Monitor 或 CA Multi-Port Monitor 上的时间和日期相同。Cisco WAE 收集的性能数据的时间戳使用设备的时间戳。如果将管理控制台配置为使用网络时间协议 (NTP)，请使用 WAAS Central Manager 在 Cisco WAE 设备上配置 NTP。有关详细信息，请参阅《*Cisco Wide Area Application Services Configuration Guide*》(Cisco Wide Area Application Services 配置指南)。
- 监视设备比率 (p. 231)大小设置正确。
- Cisco WAE 可通过 TCP-7878 与分配的 CA Standard Monitor 或 CA Multi-Port Monitor 以及管理控制台进行通信。

配置 Cisco WAE 导出响应时间数据

从 Cisco WAE CLI 或 Central Manager GUI 中，配置 Cisco WAE 设备导出应用程序响应时间数据。

遵循这些步骤:

1. 在 Cisco WAE 上，运行以下命令来更改配置模式：
   `config`
2. 命令行提示符将变为：
   `WAE<config>#`
3. 运行以下命令，在 Cisco WAE 上禁用数据流监视：
   `no flow monitor tcpstat-v1 enable`
4. 通过运行以下命令，使用管理控制台的 IP 地址注册 Cisco WAE：
   `flow monitor tcpstat-v1 host <MCAddress>`

   其中，*<MCAddress>* 是管理控制台的 IP 地址。
5. 通过运行以下命令，在 Cisco WAE 上启用数据流监视：
   `flow monitor tcpstat-v1 enable`
6. 运行以下命令，返回权限模式：
   `exit`
7. 命令行提示符将变为：
   `WAE#`
8. 为了确认 Cisco WAAS Flow Agent 已连接到 CA Application Delivery Analysis Manager，请运行以下命令：
   `show statistics flow monitor tcpstat-v1`

   结果应指明配置的主机地址是 CA Application Delivery Analysis Manager 的 IP 地址。请注意，对于主机连接状态为“等待轮询”（Cisco WAE 轮询 CA Application Delivery Analysis Manager 时除外）的情况，这很正常。
9. 确认 Cisco WAE 显示在管理控制台上的 WAN 优化设备列表中：
   a. 打开管理控制台。
   b. 单击“管理配置”页面。
   c. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
   d. 滚动至“WAN 优化设备列表”。如果显示 Cisco WAE，则可将 Cisco WAE 分配 (p. 329)给 CA Standard Monitor 或 CA Multi-Port Monitor。

将 Cisco WAE 分配给监视设备

在配置 Cisco WAE 设备导出响应时间数据之后，便可以将 Cisco WAE 分配给 CA Standard Monitor 或 CA Multi-Port Monitor。不要将 Cisco WAE 分配给 CA Virtual Systems Monitor。

要使可用的监视设备资源实现最大化，请在添加 CA Standard Monitor (p. 254)时禁用数据包监视。

当确定 Cisco WAE 的分配位置时，仅在 CA Standard Monitor 与 CA Multi-Port Monitor 监视设备之间实现负载平衡。如果可能，请尽量避免将多个数据中心 WAE 分配给同一监控，然后对分支 Cisco WAE 设备实现负载平衡。

Cisco WAE：

- 每 5 分钟轮询它已分配的监视设备，以查看要监视的服务器列表
- 将数据包摘要文件发送至它已分配的监视设备

将 Cisco WAE 分配给正在监视服务器 SPAN 的监视设备或专用于从 Cisco WAE 设备接收数据包摘要文件的监视设备。为避免 CA Standard Monitor 上的管理端口过载，请勿将 Cisco WAE 分配给同时从 CA GigaStor 接收数据包摘要文件的 CA Standard Monitor。

如果要使用域分隔重复的 IP 通信，请编辑 WAN 优化监视器源 (p. 331)并将其分配给域。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 在“ADA 监视设备列表”中，单击 以编辑 CA Standard Monitor 或 CA Multi-Port Monitor。

   请注意，在“活动源”列，WAN 优化会指明 WAN 优化设备（如 Cisco WAE 设备）已分配到监控。
4. 在第三个“向我显示”菜单中，单击“监视器设备”。
5. 在“监视器设备”中，滚动到“WAN 优化”，然后单击“可用”列中的设备。单击向右箭头以将其移到“已分配”列。“已分配”列中的 Cisco WAE 设备当前已分配给监控。

   如果未列出所需的 Cisco WAE，请确认已将 Cisco WAE 配置为与管理控制台进行通信 (p. 328)。
6. 重复上述步骤以分配其他 Cisco WAE 或单击“确定”以完成。

7. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

8. 在 5-10 分钟之后，管理控制台的“优化”页面应显示已优化网段的应用程序性能数据。在管理控制台的“优化”页面中，按“过去 1 小时”进行筛选，以便在接收性能数据时查看该数据。

   如果看不到您的应用程序的数据，请对 Cisco WAE 监视设备进行故障排除 (p. 335)。

详细信息：

添加 CA Standard Monitor (p. 254)
编辑 WAN 优化监视器源 (p. 331)

编辑 Cisco WAE 监视设备

编辑 Cisco WAE 监视设备来更新其属性，例如，分配突发事件响应。当编辑 Cisco WAE 时，您还可以查看任何监视设备突发事件。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动至“WAN 优化设备列表”。
4. （可选）从“选择源集”列表中单击一个源集，以查看相应的 Cisco WAE 设备组。
5. 单击  以编辑 Cisco WAE 监视设备。

   将打开“WAN 优化属性”。

6. 单击“突发事件响应”以选择突发事件响应，然后单击“确定”。

   要查看监视设备的突发事件，请在第三个“向我显示”菜单中单击“突发事件”。

详细信息：

监视具有一组 Cisco WAE 设备的服务器 (p. 339)
查看监视设备突发事件 (p. 235)

编辑 WAN 优化监视器源

编辑 WAN 优化监视器源，以将特定域分配给一组 Cisco WAE 设备。默认情况下，新的监视器源会分配到默认域。CA Standard Monitor 或 CA Multi-Port Monitor 中提供的 *WAN 优化*监视器源可从 WAN 优化设备（如 Cisco WAE 设备）中接收数据包摘要文件。

注意：在 WAAS 环境中，无需创建一对 WAN 优化监视器源。如果位置有一个附加的 Cisco WAE 用于冗余，只需将其分配给 CA Standard Monitor 或 CA Multi-Port Monitor。要为 WAAS 环境中的冗余启用支持，请创建一对 (p. 225)用于监视服务器 SPAN 的监视器源。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动至“ADA 监视设备列表”，并单击 来编辑 CA Standard Monitor 或 CA Multi-Port Monitor。

   请注意，在“活动源”列，WAN 优化会指明 WAN 优化设备（如 Cisco WAE 设备）已分配到监控。

   如果您不确定要编辑哪个监控，可使用“WAN 优化设备列表”中的“已分配”列查找它已分配的监控。

   将打开“监视器属性”。
4. 滚动到“监视器源”部分，并单击 以编辑 WAN 优化监视器源，然后指定 WAN 优化监视器源设置。

   请注意，WAN 优化监视器源的监视器源设置不允许您配置备用源。备用监视器源不适用于 WAN 优化设备。
5. 单击“更新”。
6. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)

取消分配 Cisco WAE

从已分配的监控中取消分配 Cisco WAE。如果从监控中取消分配所有 WAN 优化设备，管理控制台将自动删除其 WAN 优化监视器源。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“ADA 监视设备列表”并单击  ，以编辑将 Cisco WAE 分配到的 CA Standard Monitor 或 CA Multi-Port Monitor。

   请注意，在“活动源”列，WAN 优化会指明 WAN 优化设备（如 Cisco WAE 设备）已分配到监控。
4. 在第三个“向我显示”菜单中，单击“监视设备”。

   将打开“监视器设备”。
5. 单击  以取消分配 Cisco WAE。
6. 在提示时单击“继续取消分配”，以取消分配 Cisco WAE。

   管理控制台将更新“已分配设备列表”。
7. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

WAAS Incidents

如果 Cisco WAE 设备停止向管理控制台发送数据的时间超过 15 分钟，管理控制台将自动创建重大监视设备突发事件。

有关更多信息：

编辑监视设备突发事件阈值 (p. 236)

删除 Cisco WAE 监视设备

可以删除 Cisco WAE，不再将其作为管理控制台的响应时间数据源。删除 Cisco WAE 监视设备时，管理控制台会自动为已分配该 WAN 优化监视器源的每台服务器分配另一个监视器源。管理控制台可能需要花费长达 10 分钟才能完成监视器源分配更新。

删除 Cisco WAE 监视设备会自动从其 CA Standard Monitor 或 CA Multi-Port Monitor 中取消分配 Cisco WAE。

遵循这些步骤:

1. 从它已分配的 CA Standard Monitor 或 CA Multi-Port Monitor 监视设备中取消分配 Cisco WAE (p. 332)。您也可以将 Cisco WAE 设备重新分配 (p. 329)给其他监视设备。
2. 在 Cisco WAE 中禁用数据流监视 (p. 333)，以从管理控制台中的未分配 Cisco WAE 监视设备的列表中删除 Cisco WAE。
3. 从管理控制台中删除 Cisco WAE (p. 334)。

在 Cisco WAE 中禁用数据流监视

要从未分配 Cisco WAE 监视设备的列表中删除 Cisco WAE，必须先在 Cisco WAE 上禁用数据流监视。

遵循这些步骤:

1. 在 Cisco WAE 上，运行以下命令来更改配置模式：
   `config`
2. 命令行提示符将变为：
   `WAE<config>#`
3. 运行以下命令，在 Cisco WAE 上禁用数据流监视：
   `no flow monitor tcpstat-v1 enable`
4. 运行以下命令，返回权限模式：
   `exit`
5. 命令行提示符将变为：
   `WAE#`
6. 要确认已禁用数据流监视，请运行以下命令：
   `show statistics flow monitor tcpstat-v1`
7. 该命令若返回以下结果，说明数据流监视已禁用：
   数据流应用程序未启用或不可用。

删除 Cisco WAE 监视设备

在删除 Cisco WAE 监视设备之前，请配置 Cisco WAE 以 禁用响应时间数据导出。如果您从管理控制台删除 Cisco WAE 监视设备，并配置 Cisco WAE 设备导出响应时间数据，则 Cisco WAE 将继续可用作监视设备。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“WAN 优化设备列表”，并单击 以删除 Cisco WAE 监视设备。
4. 在提示时单击“继续删除”，以删除 Cisco WAE。

   将从“WAN 优化设备列表”中删除 Cisco WAE。

重置优化的应用程序

重置所有优化的应用程序，以使管理控制台能够根据管理控制台当前接收的分段应用程序数据来报告应用程序性能。通常 (p. 323)，无需重置优化，因为如果优化中断，管理控制台会继续报告应用程序的情况。

如果您计划使用管理控制台来证实可优化不同应用程序的优点，则通过重置优化可以快速比较 WAAS 优化中的更改。例如，如果您停止优化，则管理控制台将在最长 20 分钟的时间内报告应用程序的服务器段中未优化的服务器 SPAN，然后再报告未优化应用程序中的未优化通信量。

在重置优化之后，在服务器段中报告的任何未优化的应用程序通信量此时都会在未优化的应用程序中报告，并且当前优化的应用程序由网段报告。但是，管理控制台最多可能需要 10 分钟将服务器 SPAN 度量标准替代到应用程序的服务器段中。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“WAN 优化设备列表”，单击 并选择“重置已优化”。
4. 等待 10 分钟，在“优化”页面中查看更新的报告数据。

详细信息：

优化停止时如何监视 (p. 323)

对 Cisco WAE 监视设备进行故障排除

对 Cisco WAE 进行故障排除以确定报告数据缺失的原因。在添加 Cisco WAE 监视设备之后，管理控制台可能需要 10 分钟按网段来报告已优化的应用程序性能。

如果管理控制台不显示某一分支位置或所有分支位置的分段应用程序数据，请确认相应的 Cisco WAE 设备具有活动会话，并且 Cisco WAE 设备正在导出所需应用程序通信量的响应时间数据。

如果以下段的网段数据缺失：

客户端段

检验分支 WAE 设备。

WAN 段

检验数据中心 WAE 设备。

服务器段

检验监控数据中心 WAE 设备和数据中心服务器之间的通信的监视设备。如果未配置监视设备监控服务器 SPAN，请检验数据中心 WAE 设备。

查看活动会话

使用“活动会话”页面，可以报告前 5 分钟报告间隔内由 WAN 优化监控报告的活动会话的数目。

通过活动会话信息，可以验证 WAN 优化监视器源是否正在监视 TCP 会话 (p. 227)。管理控制台按应用程序端口报告服务器上的活动 TCP 会话的数目。如果监视器源没有任何用于服务器或应用程序的活动会话，则会出现 WAE 配置问题。

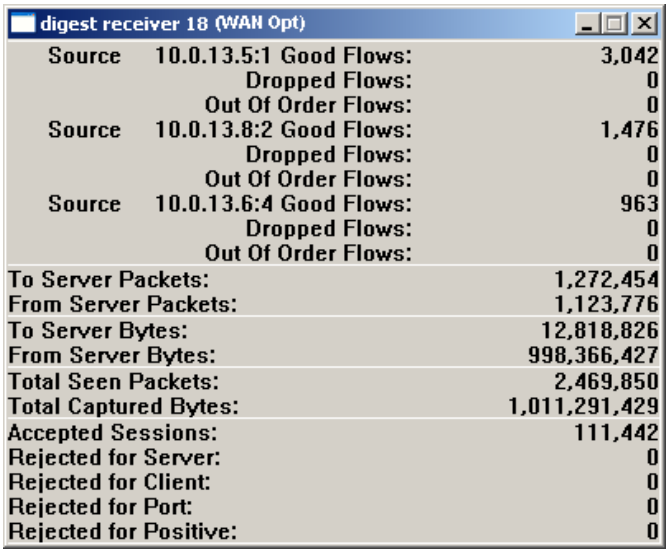
查看 WAN 优化计数器统计

查看 WAN 优化计数器，以便显示有关它从已分配的 Cisco WAE 设备接收的数据包摘要的信息，包括有关传输数据包摘要的 Netflow 数据包的信息。

要查看 WAN 优化计数器窗口，您必须登录到 (p. 268)将 Cisco WAE 分配到的 CA Standard Monitor。

重要提示：开始之前，请同步监视设备。直到同步数据监视之后，才会显示计数器窗口。

WAE 优化计数器会显示来自分配给监控的 Cisco WAE 设备的统计：



正常数据流

表示已按发送顺序正常接收的 Netflow 数据包的数目。

丢弃的数据流

表示未经 CA ADA Monitor 服务处理的 Netflow 数据包的数目。来自丢弃的 Netflow 数据包中所包含的数据包摘要的任何响应时间数据都不会包含在管理控制台报告中。

无序数据流

表示已被监控接收但未按照发送顺序接收的 Netflow 数据包的数目。

到服务器数据包

表示从客户端发送到服务器的数据包的数目。

来自服务器数据包

表示从服务器发送到客户端的数据包的数目。

到服务器字节

表示从客户端发送到服务器的字节数。

来自服务器字节

标识从服务器发送到客户端的字节数。

可见数据包总计

表示为了确定数据包标头是否与指定的应用程序端口、客户端网络和服务器子网匹配而检查的数据包的数目。

捕获的字节总计

表示与指定的应用程序端口、客户端网络和服务器子网相匹配的数据包的总字节数。

注意：Cisco WAAS Flow Agent 会检查每个数据包标头，以便确定数据包是否与指定的应用程序端口、客户端网络和服务器子网相匹配。有关详细信息，请参阅“可见数据包总计”。

已接受的会话

表示与管理控制台中有效的应用程序/服务器/网络组合匹配的 TCP 会话的数目。

服务器被拒绝

表示服务器 IP 与管理控制台监视的服务器子网不匹配。

客户端被拒绝

表示客户端 IP 与管理控制台要监视的客户端网络的列表不匹配。

端口被拒绝

表示服务器端口与管理控制台应忽略的端口的列表相匹配。

正当拒绝

保留给将来使用。

详细信息：

客户端网络的工作方式 (p. 27)
应用程序的工作方式 (p. 93)
服务器的工作方式 (p. 61)

验证 Cisco WAE 配置

验证 Cisco WAE 配置以确保：

- Cisco WAE 正在优化要监视的服务器。
- Cisco WAAS Flow Agent 正在导出所优化服务器的响应时间数据。

遵循这些步骤:

1. 在 Cisco WAE 上，运行以下命令来显示其优化的通信量：

   WAAS/WAE 版本 4.1.x

   show statistics connection all

   WAAS/WAE 版本 4.0.x

   show tfo connection summary

2. 复查服务器 IP 地址和端口的列表，以确保 Cisco WAE 正在优化相关的应用程序通信量。
3. 运行以下命令，以查看 Cisco WAAS Flow Agent 正为其导出响应时间数据的服务器的列表：
   `show statistics flow filters`

   如果服务器列表与上一步中的优化服务器列表不匹配：

   a. 验证管理控制台是否正在监视服务器。

   b. 验证是否已将服务器分配给应用程序。
4. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。
5. 等待 5 分钟，然后通过运行以下命令来验证 Cisco WAE 正在监视的服务器列表是否与管理控制台中的服务器列表相对应：
   `show statistics flow filters`

   您应该会看到，服务器现在已添加，而且数据流命中数大于 0。

详细信息：

管理服务器 (p. 70)
向应用程序分配服务器 (p. 115)

监视具有一组 Cisco WAE 设备的服务器

通常允许所有 Cisco WAE 设备监视所有服务器是比较好的做法，因为 Cisco WAE 设备分布在整个网络范围内，并且单个 Cisco WAE 设备可能会看到以下内容：

- 传入和传出特定服务器的全部通信量
- 看不到传入和传出特定服务器的任何通信量
- 传入和传出特定服务器的部分通信量

源集的工作方式

*源集*是一组 Cisco WAE 设备。由于管理控制台会将所有服务器和 Cisco WAE 设备分配给同一源集，这样所有 Cisco WAE 设备都可以监视所有服务器，因此大部分时间内，您无需配置源集。如有必要，您可以创建一个源集，以指定要用于监视特定服务器的一组 Cisco 设备。

源集不能确保由那些设备报告的通信量的唯一性。如有必要，可使用域分隔重复通信量 (p. 87)。

要使用一组 Cisco WAE 设备监视服务器，请执行以下任务：

- 向相应的 Cisco WAE 设备分配一个源集 (p. 340)。
- 将源集分配到适当的服务器 (p. 341)。

向 Cisco WAE 设备分配一个源集

向 Cisco WAE 设备分配一个源集，以创建一组 Cisco WAE 设备。为报告所用，将该源集分配给一台服务器，以确保只有源集中的 Cisco WAE 设备监视该服务器上的 WAN 优化的应用程序通信量。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动至“WAN 优化设备列表”，然后单击“选择源集”来筛选 WAE 设备列表。

   如果未显示“选择源集”列表，则未定义其他源集。

   默认情况下，管理控制台会向名为“默认部署”的默认源集分配一个新 WAE 设备。选择“默认部署”，以查看当前分配给默认源集的 WAE 设备的列表。
4. 单击 编辑 Cisco WAE 监视设备。

   将打开“WAN 优化设备属性”。
5. 单击“选择源集”，以选择要将 Cisco WAE 分配到的源集，或单击“添加”以添加新源集，并键入源集名称，然后单击“确定”。

   管理控制台将更新属于当前选定源集的 Cisco WAE 设备的列表。

   如果未显示“源集”列表，说明未定义额外的源集。
6. 重复这些步骤，以向每个 Cisco WAE 监视设备分配一个源集。

为服务器分配源集

由于管理控制台会自动使用所有 Cisco WAE 设备来监视所有服务器，因此大部分时间内，您无需向服务器分配源集。

如有必要，可指定一组 Cisco WAE 设备 (p. 340)，以通过向服务器分配源集来监视服务器。

如果您创建了一个或多个源集，“服务器属性”页面将显示“源集”选项，您可以通过它为服务器分配特定的源。

遵循这些步骤:

1. 单击“管理”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动至“服务器列表”，并单击  来编辑服务器。

   将打开“服务器属性”。
4. 单击“源集”以选择不同的源集，然后单击“确定”。

   如果未显示“源集”列表，说明未定义额外的源集。

重命名源集

编辑源集，更改其名称。如果要更改将 Cisco WAE 监视设备分配到的源集，请编辑 Cisco WAE 监视设备 (p. 330)。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动至“WAN 优化设备列表”，然后单击“选择源集”来筛选 WAE 设备列表。
4. 单击  ，然后单击“编辑源集”。
5. 在“源集”中，为源集键入新名称，然后单击“确定”。

删除源集

当删除源集时，管理控制台会将分配给已删除源集的相应 Cisco WAE 设备和任何服务器均重新分配给“默认部署”源集。

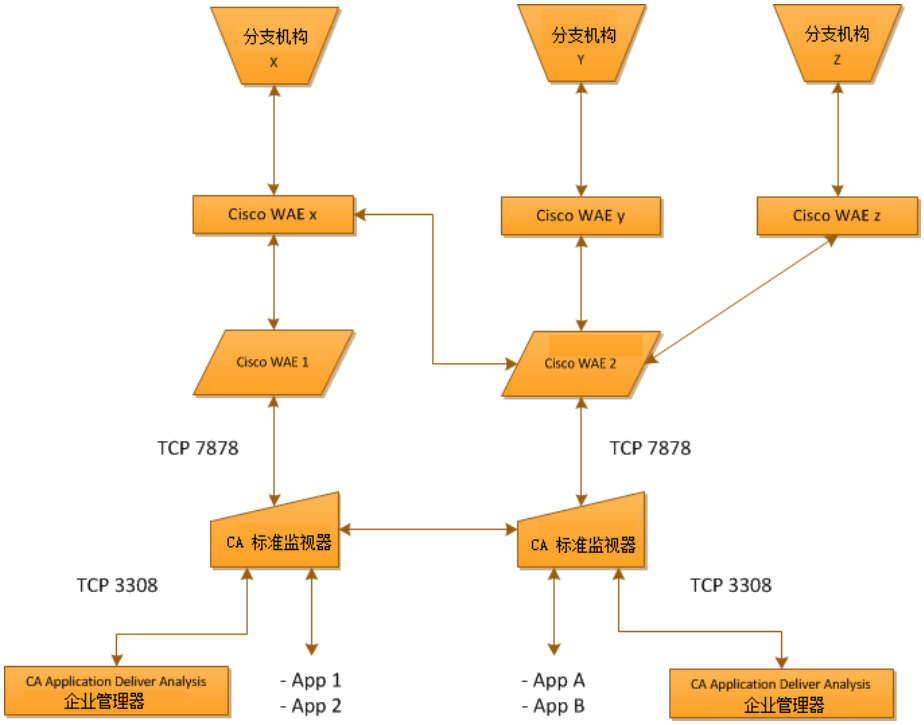
遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“WAN 优化设备列表”，然后单击“选择源集”以选择要删除的源集。
4. 单击 ，然后单击“删除源集”。
5. 在“删除源集”中，会提示您确认删除。

在管理控制台之间共享优化数据

管理控制台通常支持环境中的所有 Cisco WAE 设备。但是，如果您的 WAAS 部署优化的应用程序需要部署的 Cisco WAE 监视设备比单个管理控制台可以支持的 数量多，请为多个管理控制台之间的远程站点共享客户端、WAN 和服务器段应用程序性能数据。

在以下示例中，共享 WAN 优化的应用程序性能数据使右侧的管理控制台能够为分支 X 和 WAE x 之间的 App A 和 App B 段通信量报告客户端段。如果不使用共享，右侧的管理控制台将只为分支 X 中的 App A 和 App B 报告 WAN 和服务器段。



或者，如果您配置左侧的管理控制台，来监视跨远程分支的 APP A 和 APP B 的性能，则共享 WAN 优化应用程序性能数据将使控制台能够为分支 X 中的 APP A 和 App B 报告 WAN 和服务器段，并为分支 Y 和分支 Z 中的 App A 和 App B 报告客户端、WAN 和服务器段。如果不使用共享，则左侧的管理控制台不会为分支 X 或分支 Y 和分支 Z 中的 App A 和 App B 报告 WAN 和服务器段。

通过轮询每个管理控制台的 CA Standard Monitor 和 CA Multi-Port Monitor 监视设备的列表，然后与属于共享控制台的监控共享数据包摘要文件，管理控制台可以在多个管理控制台之间共享 Cisco WAE 设备中的数据包摘要文件。例如，如果 CA Standard Monitor 收到它不应监视的服务器的数据包摘要文件，监控将与属于一个共享管理控制台的监控共享数据包摘要文件。要最大程度地减少共享的数据量，可从与应用程序距离最近的监控所属的管理控制台中监视该应用程序。

共享 WAN 优化的性能数据

共享 WAN 优化的应用程序性能数据需要您执行以下操作：

- 将所有 Cisco WAE 设备和服务器分配给同一源集。如果未配置源集，则只需使用“默认部署”源集。
- 配置接收数据包摘要文件的监视设备，以共享应用程序性能数据。
- 确保所有共享的监视设备都可与以下对象通信：
  - 每个管理控制台（通过端口 TCP-3308）。从 Cisco WAE 接收数据包摘要文件的所有监视设备都必须能够通过 TCP-3308 与每个管理控制台通信。
  - 所有 Cisco WAE 设备（通过端口 TCP-7878）。管理控制台会自动在监视设备之间配置共享。

在所有监视设备上启用共享之后，Cisco WAE 可能需要花费长达 25 分钟的时间来轮询分配的监控，以获取更新的服务器列表并开始报告共享数据。

如果监控无法共享 WAN 优化的应用程序性能数据，它将存储数据，直到还原共享为止。但是，一个监控最多只能存储 1 GB 的共享数据。在监控中无法存储的任何共享数据都将丢失，并且无法恢复。

遵循这些步骤:

1. 确保从 Cisco WAE 接收数据包摘要文件的 CA Standard Monitor 和 CA Multi-Port Monitor 监视设备可通过 TP-3308 与每个管理控制台通信。所有监视设备均必须能通过 TCP-3308 与管理控制台通信。
2. 确保所有监视设备均可通过 TCP-7878 彼此通信。
3. 配置所有监视设备，以共享 WAN 优化的应用程序性能数据：
   a. 创建一个名为 DTMDistributedConsoles.ini 的配置文件。
   b. 在 DTMDistributedConsoles.ini 中，输入要共享的每个管理控制台的 IP 地址。确保包括分配给监控的管理控制台的 IP 地址。当指定 IP 地址时，使用十进制点符号在新行中分隔每个 IP 地址。
   c. 将同一 DTMDistributedConsoles.ini 文件复制到全部监视设备中。对于：
      - CA Standard Monitor：将文件复制到 <ADA 主目录>\bin 文件夹
      - CA Multi-Port Monitor：复制文件到 /opt/NetQoS/bin 文件夹
   d. 要根据 .ini 文件配置开始共享：
      - 在每个 CA Standard Monitor 上，从 Windows 控制面板中打开“服务”，然后重新启动 CA ADA Data Transfer Manager 服务。

- 在每个 CA Multi-Port Monitor 上，从 Web 界面，打开“进程状态”页面，然后重新启动 caperformancecenter_devicemanager 进程。

管理控制台报告共享的 WAN 优化客户端段数据，最多可能需要 25 分钟。

更新共享配置

更新共享的管理控制台配置，以添加或删除共享的管理控制台。

遵循这些步骤:

1. 编辑 DTMDistributedConsoles.ini 文件。
2. 更新 IP 地址的列表，以包括所需的每个管理控制台，同时在新行中分隔每个 IP 地址。使用十进制点符号指定每个 IP 地址。
3. 将更新的 DTMDistributedConsoles.ini 文件复制到所有监视设备中。对于：
   - CA Standard Monitor：将文件复制到 <ADA 主目录>\bin 文件夹
   - CA Multi-Port Monitor：复制文件到 /opt/NetQoS/bin 文件夹

   如果您从配置文件中删除管理控制台，请确保从关联的监视设备中删除配置文件。
4. 根据更新的 .ini 文件配置开始共享：
   - 在每个 CA Standard Monitor 上，从 Windows 控制面板中打开“服务”，然后重新启动 CA ADA Data Transfer Manager 服务。
   - 在每个 CA Multi-Port Monitor 上，从 Web 界面，打开“进程状态”页面，然后重新启动 caperformancecenter_devicemanager 进程。

   开始在每个管理控制台之间共享 WAN 优化的客户端段数据，最多可能需要 25 分钟。

删除监视设备

当删除共享 WAE 性能数据的 CA Standard Monitor 或 CA Multi-Port Monitor 时，请务必尽快在其他共享监视设备中重置配置，以便仅在它们之间共享数据。

删除共享监控不会在其他共享监视设备上自动重置配置。管理控制台将继续在监视设备之间共享数据，与已删除的监控共享的数据将会丢失。

遵循这些步骤:

1. 取消分配 (p. 329)要删除的已分配给 CA Standard Monitor 或 CA Multi-Port Monitor 的 Cisco WAE 设备。
2. 删除 CA Standard Monitor (p. 265)。
3. 在所有其余的监视设备上重新启动数据传输管理器服务。更新共享配置可能需要长达 25 分钟。
4. 通过在每个 Cisco WAE 上重新启动数据流监视，更新 Cisco WAE 设备以便与可用的监视设备共享性能数据。

   使用 CLI 重新启动数据流监视：

   a. 在 Cisco WAE 上，运行以下命令来更改配置模式：

      ```
      config
      ```

   b. 命令行提示符将变为：

      ```
      WAE<config>#
      ```

   c. 通过运行以下命令来禁用数据流监视：

      ```
      no flow monitor tcpstat-v1 enable
      ```

   d. 通过运行以下命令来启用数据流监视：

      ```
      flow monitor tcpstat-v1 enable
      ```

   e. 运行以下命令，返回权限模式：

      ```
      exit
      ```

   f. 命令行提示符将变为：

      ```
      WAE#
      ```

   g. 通过运行以下命令来检查数据流监视状态：

      ```
      show statistics flow monitor tcpstat-v1
      ```

故障排除提示

如果管理控制台无法正确显示共享数据，请验证以下内容：

- 在一个源集内，同一服务器 IP 不得由多个管理控制台来管理。在此情况下，有些应用程序数据可能会出现在多个管理控制台中，或者所有数据可能都意外出现在不与距离应用程序服务器最近的 Cisco WAE 通信的管理控制台中。
- Cisco WAE 设备上的数据流筛选是最新的。在配置监控以共享数据后，监控最多可能需要 25 分钟来与每个共享的管理控制台通信，并更新 Cisco WAE 设备上的数据流筛选。数据流筛选中的服务器列表应在所有 Cisco WAE 设备上都相同。
- 从 Cisco WAE 设备接收数据包摘要的所有监视设备均可通过 TCP-7878 彼此通信。
- 从 Cisco WAE 设备接收数据包摘要的所有监视设备均可通过 TCP-7878 与每个管理控制台通信。
- 同一配置文件位于每个监控上。

第 17 章： 使用 Cisco NAM 监视

此部分包含以下主题：

Cisco NAM 作为监视设备的工作方式

Cisco NAM 刀片或设备 (Cisco NAM) 可以作为 CA Application Delivery Analysis 的一种监视设备来运行，并允许您在 IP 地址级别（分辨率最高为 30 秒）进行故障排除。使用 Cisco NAM 作为监视设备可减少 CA Application Delivery Analysis 的服务器需求量。此外，Cisco NAM 还可以：

- 监视来自交换机或路由器的网络
- 报告通信量使用情况
- 捕获数据包并对数据包解码
- 跟踪响应时间，以查明网络或服务器的应用程序问题

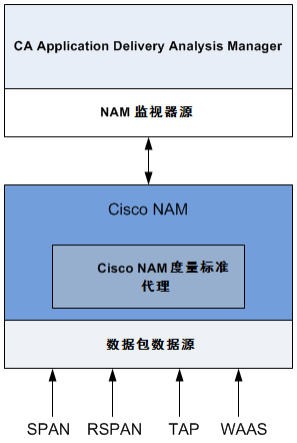
Cisco NAM 的工作方式

Cisco NAM Metric Agent 会创建度量标准摘要文件，其中包括镜像到 Cisco NAM 的所有通信量的计算响应时间度量标准。

CA Application Delivery Analysis Manager 的 NAM 监视器源在其管理 NIC 上从 Cisco NAM 中接收度量标准摘要文件并处理响应时间统计信息，以自动监视最繁忙的应用程序和任何用户定义的应用程序。

要求分布式的 CA Application Delivery Analysis Manager。

如下图所示，您可以从 SPAN 、镜像端口、网络分流器以及 Cisco WAE 设备收集数据包。数据通过 Cisco NAM Metric Agent 进行处理，计算的响应时间统计信息发送给 CA Application Delivery Analysis Manager。



CA Application Delivery Analysis Manager 在其 NAM 监视器源中接收数据包摘要文件。

监视器源分配的工作方式

如果 Cisco NAM 是最佳监视点，管理控制台会自动将 NAM 监视器源分配给服务器。

详细信息：

监视器源分配的工作方式 (p. 223)

监视设备注意事项

将 Cisco NAM 用作监控时，请考虑以下事项：

- Cisco NAM Metric Agent 会为它观测的所有应用程序-服务器-网络组合计算响应时间统计信息。CA Application Delivery Analysis Manager 会丢弃 Cisco NAM 中与 CA Application Delivery Analysis Manager 中的服务器子网、客户端网络和应用程序定义不匹配的应用程序-服务器-网络组合。
- SPAN 至 Cisco NAM Metric Agent 的数据可能会多于 Cisco NAM Metric Agent 可以处理的数据。小心执行 SPAN，以尽量减少 CPU 资源消耗，并使 Cisco NAM Metric Agent 尽其所能达到更精确的度量，而避免丢弃它无法处理的数据包。
- 您无法使用域来分隔 Cisco NAM 监视设备之间的数据收集。所有 Cisco NAM 监视设备属于 CA Application Delivery Analysis Manager 上的同一 NAM 监视器源。
- 如果配置 Cisco NAM 以使用 Cisco WAE 设备作为数据源，则 Cisco NAM Metric Agent 可从 Cisco WAE 设备发送的 TCP 标头中计算响应时间统计信息。
- Cisco NAM 不临时存储数据包摘要文件。如果 Cisco NAM 无法与为其分配的管理控制台通信，管理控制台报告将缺少数据。
- 来自 Cisco NAM 的度量标准摘要文件不包含会话级别信息，因此，“活动会话”报告对于 NAM 监视器源不可用。可改用“度量标准接收器计数器”窗口查看有关 Cisco NAM 向 CA Application Delivery Analysis Manager 发送的内容的摘要统计信息。
- 应用程序通过响应客户端上指定端口范围内的客户端请求来与客户端进行对话时，Cisco NAM 将无法监控该应用程序。Cisco Metric Agent 根据来自服务器端口（而不是服务器将 TCP 数据包发送到的客户端中的端口）的 SYN-ACK 响应来标识承载应用程序的服务器。在管理控制台中定义应用程序时，如果要用 Cisco NAM 监视该应用程序，则必须将该应用程序的端口方设置为应用程序侦听这些端口。
- 管理控制台无法从 Cisco NAM 中启动数据包捕获调查，但 Cisco NAM 支持触发的数据包捕获调查。
- 当 Cisco NAM 用作监控时，在 Cisco NAM Traffic Analyzer 控制台而不是管理控制台中支持 URL 报告。

详细信息：

管理用户定义的应用程序 (p. 106)
对 Cisco NAM 监视设备进行故障排除 (p. 359)

添加 Cisco NAM 监视设备

下面总结了配置 Cisco NAM 监视设备所需的步骤。有关详细信息，请参阅以下各节。

1. 配置 Cisco NAM 以将计算的响应时间统计导出至管理控制台。 (p. 353)
2. 配置 Cisco NAM 以将计算的响应时间统计信息导出至 CA Application Delivery Analysis Manager。
3. 确认 Cisco NAM (p. 354) 已连接到 CA Application Delivery Analysis Manager 并且正在接收来自 Cisco NAM Metric Agent 的响应时间统计信息。
4. 在管理控制台上启用 NAM 监视器源 (p. 355)。
5. *（可选）*要优化 Cisco NAM 中的可用资源，请在 Cisco NAM 上手动配置 SPAN 数据源，以便与管理控制台监视相同的网络、服务器和应用程序。Cisco NAM Metric Agent 将自动为 SPAN 数据源中的所有应用程序通信量计算响应时间度量标准。
6. *（可选）*为非活动状态编辑监视设备突发事件阈值 (p. 236)。

先决条件

下面列出了添加 Cisco NAM 监视设备的先决条件：

- Cisco NAM 软件版本 4.2.x 或 5.1(2)。

  如果管理控制台只为分支本地的服务器和应用程序处理数据，则它可以支持 Cisco Branch Router Series NME-NAM。除非您确定只有 SPAN 至该分支 NAM 的数据用于该分支本地的服务器，否则请勿将分支 NAM 数据导出至管理控制台。
- 监视设备比率 (p. 231)大小设置正确。
- Cisco NAM 可通过 TCP-9996 与管理控制台通信。

配置 Cisco NAM 导出响应时间数据

配置 Cisco NAM Metric Agent 以将响应时间数据从 SPAN、远程 SPAN、网络分流器或 Cisco WAE 导出至 CA Application Delivery Analysis Manager。与 Cisco WAE 不同，Cisco NAM 计算响应时间度量标准并将其直接发送至 CA Application Delivery Analysis Manager，并且 Cisco NAM 会为它接收的所有网络通信量计算响应时间数据。

当使用 SPAN 数据时，最好从主机交换机中配置 SPAN。建议您使用 SPAN 数据，以便监视层与层的通信量。在 Cisco NAM 中进行处理之前，RSPAN 数据会经历延迟，但有些情况需要使用它。

配置 Cisco NAM Metric Agent 以将计算的响应时间统计信息导出至 CA Application Delivery Analysis Manager 后，管理控制台会自动将 Cisco NAM 添加到可用监视设备列表中。

使用 Cisco NAM Traffic Analyzer 控制台可以：

- 启用计算响应时间度量标准导出。
- 在正在运行的配置中验证所需的活动 SPAN 会话并将其保存到启动配置中（用于仅运行 Cisco IOS 软件的交换机）。
- 查看 Cisco NAM 中的 SPAN 数据。

遵循这些步骤:

1. 在 Cisco NAM 中启用响应时间数据导出：
   a. 打开 NAM Traffic Analyzer 控制台。
   b. 单击“Admin”选项卡。
      将打开“Admin”选项卡。
   c. 单击“System”。
      将打开“System Overview”。
   d. 单击“Response Time Export”。
      将打开“External Response Time Reporting Console Export”。
   e. 选择“Enable Export”，然后单击“Apply”。
   f. 通过单击“Admin”选项卡上的“Diagnostics”来确认 Cisco NAM 正在更新其将数据导出至管理控制台的配置。
      “System Alerts”页面会显示 Cisco NAM 日志记录消息。
2. 在正在运行的配置中验证活动 SPAN 会话，并将其保存到启动配置中：
   a. 在 NAM Traffic Analyzer 用户界面中，单击“Setup”，然后单击“NAM Data Sources”。

b. 从列表中选择 SPAN 会话，然后单击“Save”以将运行配置中的活动 SPAN 会话保存到启动配置（适用于仅运行 Cisco IOS 软件的交换机）。

c. 对于要在管理控制台中查看的每个 SPAN 会话重复上一步。

3. 查看 SPAN 数据：

a. 在 NAM Traffic Analyzer 用户界面中，单击“Monitor”，然后单击“Server”、“Response Time”。通过排序查找客户端数最多的服务器。

b. 要查看详细信息，请选择服务器并单击“Details”。

确认 Cisco NAM 已连接到管理控制台

使用管理控制台确认 Cisco NAM 正将响应时间数据导出至管理控制台。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“NAM 设备列表”，以查看每个 Cisco NAM 联系管理控制台的最后时间。

启用 NAM 监视器源

默认情况下，会禁用 NAM 监视器源。

管理控制台将创建单个 NAM 监视器源，以从环境的 Cisco NAM 设备中处理度量标准摘要文件。要处理度量标准摘要文件，请启用 NAM 监视器源。

如果不再打算使用 Cisco NAM 作为管理控制台的监视设备，则可通过禁用 NAM 监视器源来优化可用的系统资源。要禁用 NAM 监视器源，请删除 (p. 265)驻留在管理控制台中的 CA Standard Monitor。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“ADA 监视设备列表”并浏览该列表，以查找与管理控制台具有相同的管理 IP 地址的 CA Standard Monitor。

   使用“地址”列标识监控的管理 IP 地址。CA Standard Monitor 和控制台共享相同的管理 IP 地址。
4. 单击 以编辑与管理控制台具有相同的管理 IP 地址的 CA Standard Monitor。如有必要，单击“添加 ADA 监视器”，以添加与管理控制台具有相同的管理 IP 地址的 CA Standard Monitor。

   将打开“Standard Monitor 属性”。
5. 选择一个选项以启用或禁用 NAM 监视，然后单击“确定”：
   - 启用 NAM 监视
   - 禁用数据包监视

   “NAM 设备列表”将显示正将响应时间数据导出至管理控制台的所有 Cisco NAM 刀片或设备。

详细信息：

管理控制台设置 (p. 205)
添加 CA Standard Monitor (p. 255)
编辑 CA Standard Monitor (p. 258)

编辑 Cisco NAM 监视设备

编辑 Cisco NAM 监视设备，以更改其监视设备突发事件响应并查看其他详细信息。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“NAM 设备列表”，并单击 以编辑 Cisco NAM。

   将打开“NAM 属性”。
4. 单击“突发事件响应”选择一个监视设备突发事件响应，然后单击“确定”。

编辑 NAM 监视器源

管理控制台创建一个 NAM 监视器源，以接收来自 Cisco NAM 的响应时间数据。编辑 NAM 监视器源，以便：

- 分配一个特定的域。默认情况下，新的监视器源会分配到默认域。如果您没有使用域来分隔重复的 IP 通信量，这将不适用。
- 创建一对监视器源。默认情况下，一台服务器由单个监视器源来监视。

Cisco NAM Metric Agent 会计算自己的 5 分钟响应时间度量标准，因此管理控制台不显示 Cisco NAM 监视器源的活动会话信息。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“ADA 监视设备列表”，然后单击  ，以编辑与管理控制台具有相同管理 IP 地址的 CA Standard Monitor。请注意，所有 Cisco NAM 设备都将自动分配给管理控制台中的 NAM 监视器源。

   将打开“Standard Monitor 属性”。
4. 滚动到“监视器源”，并单击  以编辑 NAM 监视器源。
5. 分配备用源或域，然后单击“更新”。

   有关设置服务器属性的信息，请单击“帮助”。
6. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
创建一对监视器源 (p. 225)

NAM Incidents

如果 Cisco NAM 停止向管理控制台发送数据的时间超过 15 分钟，管理控制台将自动创建重大监视设备突发事件。编辑监视设备突发事件阈值 (p. 236)，以指定所需阈值。

删除 Cisco NAM 监视设备

删除 Cisco NAM 监视设备，以将其作为响应时间数据的源删除。当删除 Cisco NAM 监视设备时，将取消连接已连接到 NAM 监视器源的所有服务器，并自动分配另一个监视器源。更新监视器源分配可能需要长达 10 分钟。

如果您已将服务器连接到 NAM 监视器源，并且您想在监视设备暂时脱机时继续监控服务器通信，则请考虑下列选项：

- 删除监视设备之前，将服务器连接到其他监视器源。使监视设备重新联机时，将适当的服务器连接到 NAM 监视器源。
- 删除 Cisco NAM 监视设备 另一个监视器源将自动被分配，但是更新监视器源分配所使用的时间高达 10 分钟。

如果您删除一个 Cisco NAM 监视设备，并已配置该 Cisco NAM 导出响应时间数据，则该 Cisco NAM 将继续可用作监视设备。

遵循这些步骤:

1. 在 Cisco NAM 中禁用 Cisco NAM Metric Agent 数据导出：
   a. 打开 NAM Traffic Analyzer 控制台。
   b. 单击“Admin”选项卡。

      将打开“Admin”选项卡。
   c. 单击“System”。

      将打开“System Overview”。
   d. 单击“Response Time Export”。

      将打开“External Response Time Reporting Console Export”。
   e. 取消选择“Enable Export”，然后单击“Apply”。
   f. 通过单击“Admin”选项卡的“Diagnostics”来确认 Cisco NAM 正在更新其禁止将数据导出至管理控制台的配置。

      “System Alerts”页面会显示 Cisco NAM 日志记录消息。
2. 在管理控制台中，从“NAM 设备列表”删除 Cisco NAM：
   a. 单击“管理配置”页面。
   b. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
   c. 滚动到“NAM 设备列表”，并单击 以删除 Cisco NAM。
   d. 在“删除监视设备确认”中，单击“继续删除”以删除 NAM 监视设备。

      将从“NAM 设备”列表中删除 Cisco NAM。

对 Cisco NAM 监视设备进行故障排除

查看 NAM 计数器以显示有关其接收的 Netflow 的信息。

要查看 NAM 计数器窗口，您必须登录到 (p. 268)管理控制台。

重要提示：开始之前，请同步监视设备。直到同步数据监视之后，才会显示计数器窗口。

对 Cisco NAM 进行故障排除，以标识缺少本应由 CA Standard Monitor 收集的报告数据的原因。切记，在将 Cisco NAM 添加到管理控制台之后，管理控制台最多可能需要 10 分钟时间来报告来自 Cisco NAM 的应用程序性能数据。

与其他监视设备不同，Cisco NAM 不生成会话级别的统计信息，因此，管理控制台不对其进行报告。要查看有关 Cisco NAM 发送给管理控制台的内容的摘要统计信息，请在管理控制台中查看 NAM 计数器统计信息。

遵循这些步骤:

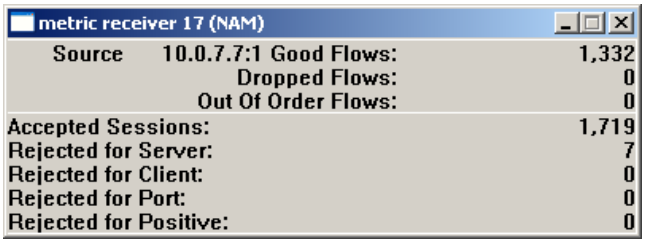
1. 登录管理控制台计算机或使用 Microsoft Remote Desktop Connection (RDC) 客户端进行远程连接。

   使用远程桌面来连接基于 Windows Server 2003 的服务器时，请使用 /admin 开关连接到物理控制台会话。通过物理控制台会话可以查看源接收器计数器。有关 /admin 开关的信息，请参阅 Microsoft KB 947723。

2. 在不同的操作系统上，查看 NAM 监视器源统计信息所需执行的步骤会有所不同：

   - 如果管理控制台正在 Windows Server 2003 中运行，将自动显示源接收器计数器。如果未显示，请确保您已连接到物理控制台会话。
   - 如果管理控制台正在 Windows Server 2008 中运行，则双击桌面上的“ADA 监视器活动”快捷方式可显示源接收器计数器。

   NAM 计数器将显示来自所有 Cisco NAM 设备的统计信息：



如果未正确显示计数器说明，请关闭计数器窗口，然后双击桌面上的“ADA Monitor Activity”快捷方式来重新打开它们。

如果未显示任何源接收器计数器，请验证 CA ADA Monitor 服务是否正在运行并验证监控是否与管理控制台同步。

3. 解释 NAM 计数器统计信息以标识问题：

正常数据流

表示已按发送顺序正常接收的 Netflow 数据包的数目。

丢弃的数据流

表示未经 CA ADA Monitor 服务处理的 Netflow 数据包的数目。管理控制台报告中不包括已丢弃 Netflow 数据包中包括的任何度量标准摘要中的响应时间数据。

无序数据流

表示已被监控接收但未按照发送顺序接收的 Netflow 数据包的数目。

已接受的会话

表示与管理控制台上的有效应用程序/服务器/网络组合相匹配的 TCP 会话的数目。

服务器被拒绝

标识与管理控制台监视的服务器子网不匹配的服务器 IP。

客户端被拒绝

表示与管理控制台要监视的客户端网络的列表不匹配的客户端 IP。

端口被拒绝

表示服务器端口与管理控制台应忽略的端口的列表相匹配。

正当拒绝

保留给将来使用。

详细信息：

客户端网络的工作方式 (p. 27)
应用程序的工作方式 (p. 93)
服务器的工作方式 (p. 61)
执行基本操作 (p. 315)

第 18 章： 使用 Riverbed Steelhead 监视

此部分包含以下主题：

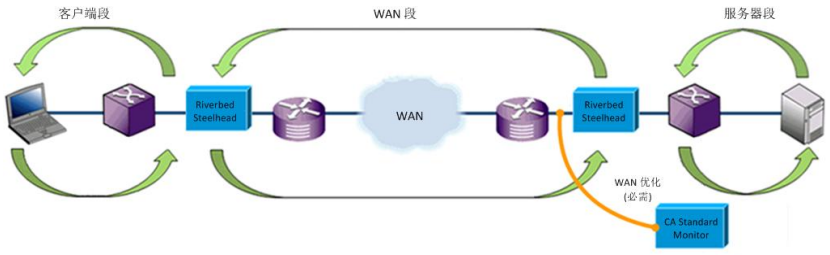
概念

本节讨论了 CA Application Delivery Analysis 如何监视 Steelhead 优化的网络。

简介

CA Standard Monitor 充当基于 IPv4 的 Steelhead 优化通信的 一种监视设备类型。CA Standard Monitor 被动监视 WAN 优化的通信量，并且帮助您持续记录端到端的系统性能。

在下面的 Steelhead 物理径内配置中，位于数据中心的监视设备监视跨 WAN 网段的优化 WAN 通信量。



数据中心中的 CA Standard Monitor 可同时监视 WAN 段上的优化通信和服务器段上的未优化通信。

对优化通信量和未优化通信量需要使用单独的监视器 NIC。

体系结构

在数据中心，CA Standard Monitor 使用不同的监视器源来同时监视优化和未优化的通信。

Stealhead 监视器源

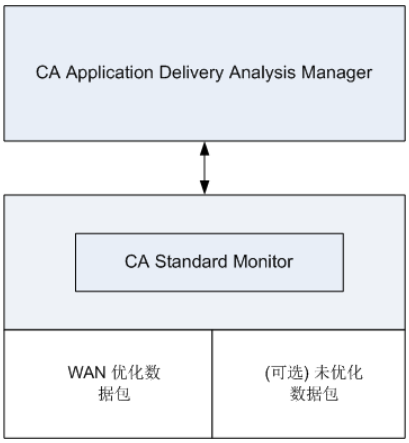
从数据中心接收 WAN 优化数据包，并计算观测的每个应用程序/服务器/网络组合的 WAN 段的响应时间度量标准。

数据包镜像监视器源

从服务器交换机接收未优化的数据包，并计算观测的每个应用程序/服务器/网络组合的服务器段的响应时间度量标准。CA Application Delivery Analysis 必须监视未优化的服务器通信量以报告服务器网段。

需要单独的监视器 NIC 来监视 Steelhead 优化的 WAN 通信量和未优化的服务器通信量。

管理控制台会自动报告与管理控制台上定义的客户端网络、服务器子网相匹配的新应用程序通信量。



要在分支位置报告 WAN 优化应用程序的响应时间，则在该分支位置将需要 CA Standard Monitor。Riverbed 客户端段监视器源接收客户端计算机和分支 Steelhead 设备之间的未优化通信，并计算客户端段的响应时间度量标准。如果分支位置未部署监视设备，CA Application Delivery Analysis 仍然可以深入了解 WAN 性能。

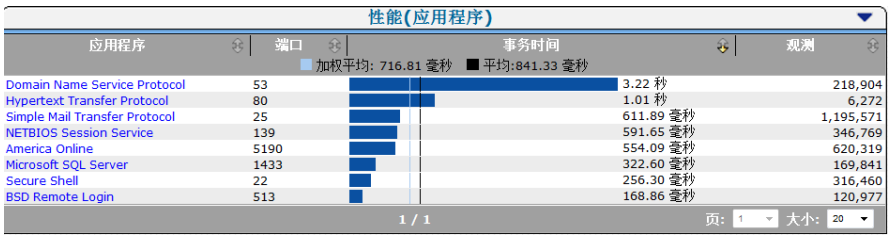
网段

管理控制台为三个网段中的每一个生成一组单独的度量标准，并将每个网段视为一个单独的应用程序。管理控制台为下面的每一个段生成一组单独的度量标准：

- **客户端段**，这是分支位置的客户端和分支 Steelhead 设备之间的网段。在分支位置部署 CA Standard Monitor，以便监视未优化的客户端网段。
- **WAN 段**，这是分支 Steelhead 设备与数据中心 Steelhead 设备之间的网段。在数据中心部署 CA Standard Monitor，以便监视 Steelhead 优化的 WAN 网段。
- **服务器段**，这是数据中心 Steelhead 设备与数据中心服务器之间的网段。在数据中心部署 CA Standard Monitor，以便监视未优化的服务器网段。

  如有必要，请使用数据中心中的 CA Standard Monitor 同时监视 Steelhead 优化 WAN 网段和未优化服务器网段。

管理控制台将网段追加到应用程序名称上，如 SMTP [客户端]、SMTP [WAN] 和 SMTP [服务器]。在下面的示例中，SMTP 应用程序代表未优化的应用程序性能。未优化应用程序的响应时间更短，因为数据来自数据中心中的本地用户。



监视器源分配

如果 CA Standard Monitor 上的监视器源是监视某服务器上未优化的 TCP 通信量的最佳源，管理控制台会自动将监视器源分配给该服务器。

网段的突发事件阈值

管理控制台会为 WAN 优化网络的每个段设置不同性能阈值。要提高或降低管理控制台对性能变化的敏感度，请编辑每个网段上的性能阈值 (p. 143)。

监视 Steelhead 优化的通信量时，为客户端网段设置的突发事件阈值将用于部署了监视设备的分支。监视设备必须观测客户端计算机与分支 Steelhead 设备之间的通信量，以便对应用程序性能进行分级并创建突发事件。

数据包捕获调查

监视未优化服务器通信的监视设备还执行数据包捕获调查。

如果在使用 CA Standard Monitor 监视未优化的服务器通信量，则监视设备会：

- 在管理控制台创建突发事件之后启动数据包捕获调查。
- 一次运行一个数据包捕获调查。
- 捕获未优化的服务器网段。如果另一个监视设备离服务器 SPAN 更近，相应的监视器源将分配给该服务器。
- 将数据包捕获文件从监视设备复制到用户的本地计算机。可能要花很长时间才能打开数据包捕获调查，具体取决于数据包捕获文件的大小。
- CA Standard Monitor 不提供长期的数据包存储。

优化停止时监视

根据优化中断的时间长度，管理控制台会对受影响的通信量使用不同的报告方式。必要时，重置 管理控制台 以忽略优化中的最新更改，并报告为优化。

临时中断

如果监视器源临时停止接收 Steelhead 优化的数据包，管理控制台会使用来自未优化的服务器 SPAN 的数据来报告服务器段中的应用程序。几个条件用于确定中断是临时性还是永久性的，但临时中断通常不超过 20 分钟。

当管理控制台临时报告来自服务器网段中镜像的交换机端口的未优化应用程序数据时：

- 虽然“优化”页面上的度量标准并未全部填充，但所有这些度量标准都是准确的。
- 未优化会话的度量不影响客户端或 WAN 段。
- 由于管理控制台使用的是来自离服务器最近的镜像交换机端口的更准确的数据，因此服务器网段是准确的。
- “工程”页面上的“网络往复传输时间 [服务器]”会显示增加，因为它不再获取 100% 的本地 ACK。直通度量显示传出到客户端的实际网络往复传输时间。
- “重传延迟 [服务器]”和“数据包丢失百分比 [服务器]”的值会增加。

恢复优化数据时，管理控制台会自动报告客户端、WAN 和服务器网段中分段的应用程序数据。

优化监视可能会出现临时中断，例如在以下情况下：

- 优化停止。当 Steelhead 设备没有资源来优化更多会话时，就会出现这种中断。
- 监视停止。当 Steelhead 设备和监视设备之间的链路出现中断时，就会出现这种中断。如果监视设备停止在其监视器 NIC 上接收数据包，则监视将停止。

永久更改

当监视设备停止接收优化数据包数据的时间超过 20 分钟时，管理控制台通常会将该中断视为永久性的。这种情况下，管理控制台会停止报告应用程序（如 HTTP [服务器]）的服务器网段中的未优化通信量。相反，管理控制台会报告未优化应用程序 HTTP 中的服务器 SPAN 数据。优化恢复后，管理控制台将自动恢复到按网段监视优化的应用程序。

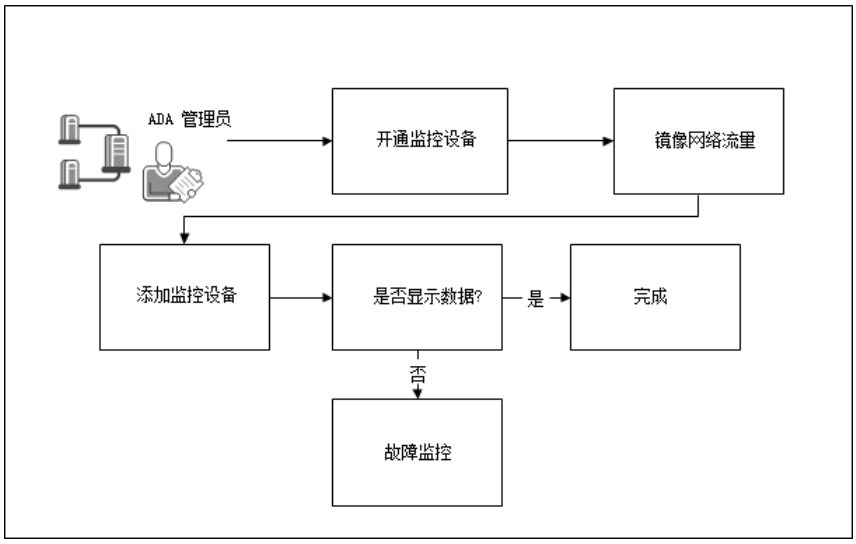
例如，设置 WAN 优化时，您无需等待便可度量优化不同应用程序的优点。要立即报告优化的更改，可以在管理控制台上重置优化的应用程序 (p. 324, p. 334)。

详细信息：

重置优化的应用程序 (p. 334)

添加监视设备

添加监视设备，可以深入了解数据中心和分支机构 Steelhead 设备之间的 WAN 优化。通过监视 Steelhead 设备之间的 WAN 优化，可显示 WAN 优化对各个应用程序在每个网段上的响应时间会产生怎样的影响。



遵循这些步骤:

1. 配置监视设备 (p. 368)。
2. 镜像网络通信量 (p. 368)。
3. 添加监视设备 (p. 373)。
4. （可选）排除监视故障 (p. 377)。

监视设备注意事项

监视 Steelhead 优化的通信量时，请记住：

- CA Standard Monitor 会监视以下 Steelhead 配置：
  - 物理径内
  - 带 WCCP（GRE 或第二层重定向）的虚拟径内配置
- CA Standard Monitor 自动支持以下 Steelhead WAN 可见性模式：
  - *正确寻址*，该模式在 WAN 上使用 Steelhead 设备地址和端口。
  - *完全透明度*，该模式保留数据包标头字段中的客户端和服务器 IP 地址以及端口号。
- 要报告 WAN 段，数据中心中需要部署 CA Standard Monitor 来监视 WAN 网段上 Steelhead 优化的通信量。如果配置了两个 NIC，每个 CA Standard Monitor 将最多可以监视两个 Steelhead 设备。
- 要报告服务器网段，监视设备必须监视数据中心中未优化的服务器通信量。如有必要，可使用数据中心中的 CA Standard Monitor 来监视未优化的服务器通信量。需要单独的监视器 NIC 来分别监视 Steelhead 优化的 WAN 通信量和未优化的服务器网段通信量。
- 要报告客户端网段，需在分支位置部署 CA Standard Monitor 来监视分支客户端计算机和分支 Steelhead 之间的通信量。
- CA Application Delivery Analysis 不能按照 URL 来监视 Web 应用程序，但可以监视所有 HTTP 通信量，例如，端口 80 上的通信量。

配置监视设备

配置 CA Standard Monitor 在数据中心监视 Steelhead 优化通信量，也可以选择在分支位置对其进行监视。

基于监视设备的位置分配内存：

- 数据中心（*建议*）：2 GB (2048 MB)
- 分支机构（*建议*）：1 GB (1024 MB)

监视 Steelhead 优化的通信量时，数据中心中的 CA Standard Monitor 还可以监视数据中心 LAN 上的未优化通信量。需要使用单独的监视器 NIC 来使用同一台监视设备同时监视 WAN 优化和未优化的通信量。

配置监视设备时，请记住：

- 使用 CA Application Delivery Analysis 安装程序来安装 CA Standard Monitor。可从 CA 支持网站 (support.ca.com) 下载 CA Application Delivery Analysis .iso。
- 如果 管理控制台 使用网络时间协议 (NTP)，请在监视设备上配置 NTP。
- 监视设备可以在 TCP-7878 上与分配的管理控制台进行通信。

注意：有关配置 CA Standard Monitor 的详细信息，请参阅 CA Application Delivery Analysis 的*《安装指南》*。

镜像网络通信量

使用网络分流器，或者将网络通信量镜像到 CA Standard Monitor。数据包镜像需求因所需的网段而异。

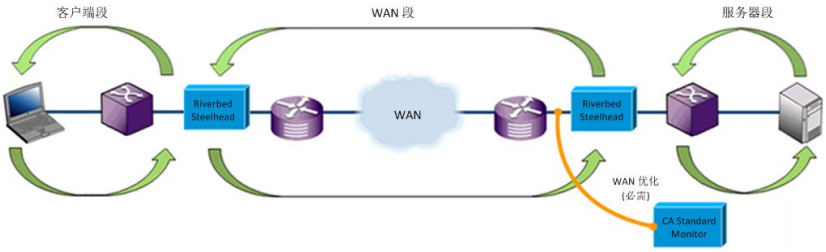
WAN 网段 - 物理径内

要报告 WAN 网段，数据中心中的 CA Standard Monitor 必须接收 Riverbed Steelhead 设备之间的优化 TCP 通信量。

CA Application Delivery Analysis 支持 Steelhead 物理径内配置。使用网络分流器或将通信量从数据中心 Steelhead 设备镜像到监视设备上的监视器 NIC。

如果 CA Application Delivery Analysis 尚未监视数据中心未优化的服务器网段，可使用 CA Standard Monitor 来同时监视 WAN 优化和未优化的服务器通信量。

在下面的 Steelhead 物理径内配置中，CA Standard Monitor 接收 WAN 网段上已优化通信量的镜像副本。



详细信息：

服务器网段 (p. 372)

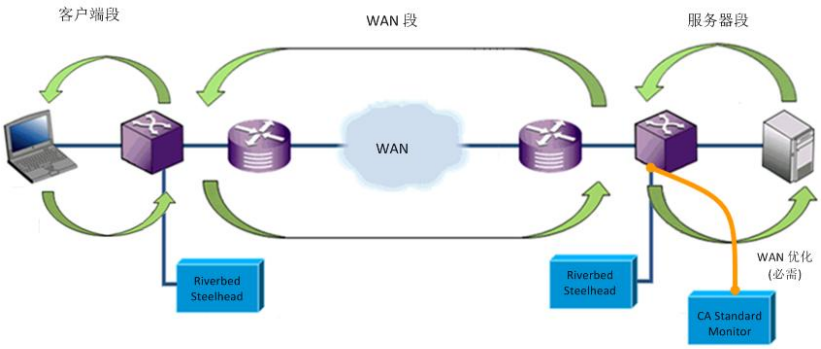
WAN 网段 - 虚拟径内

要报告 WAN 网段，数据中心中的 CA Standard Monitor 必须接收 Riverbed Steelhead 设备之间的优化 TCP 通信量。

CA Application Delivery Analysis 支持带 WCCP（GRE 或第二层重定向）的 Steelhead 虚拟径内配置。使用网络分流器或将通信量从数据中心 Steelhead 设备镜像到监视设备上的监视器 NIC。

如果 CA Application Delivery Analysis 尚未监视数据中心中的未优化服务器通信量，可使用 CA Standard Monitor 来同时监视 WAN 优化和未优化的服务器通信量。

在下面的 Steelhead 虚拟径内配置中，CA Standard Monitor 接收 WAN 网段上已优化通信量的镜像副本。



详细信息：

服务器网段 (p. 372)

客户端网段

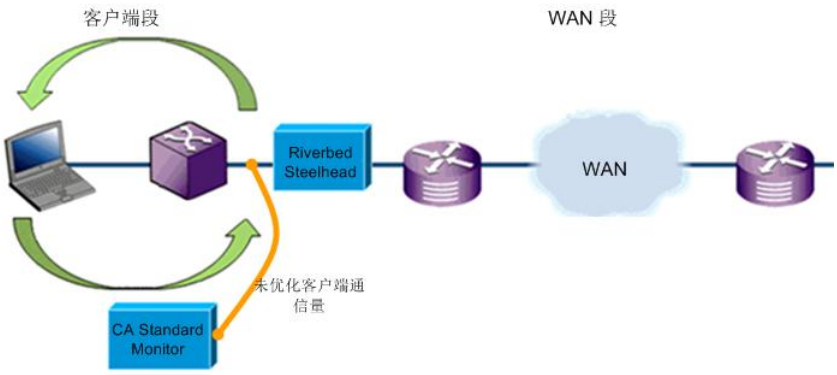
要报告客户端网段，分支机构中的 CA Standard Monitor 必须接收客户端计算机和分支 Riverbed Steelhead 设备之间的未优化 TCP 通信量。

可以使用网络分流器，也可以将来自分支交换机的通信量镜像到监视设备上的监视器 NIC。

建议您将分支监视设备部署到需要深入了解分支位置的优化应用程序列表的远程位置。如果不监视分支位置的客户端网段，CA Application Delivery Analysis 用户仍然可以查看 WAN 网段上所有应用程序的列表。通过此列表，用户可以深入查看有关 WAN 和服务器网段的性能详细信息报告。

或者，在 CA PC 或 CA NPC 中，创建一个包含具有“WAN”或“服务器”的任何应用程序的组，然后筛选关于该组和特定客户端网络的“工程”页面报告。

将客户端计算机与分支 Steelhead 设备间的未优化通信镜像到监视设备上的监视 NIC。在下面的 Steelhead 物理径内配置中，客户端计算机和分支 Steelhead 设备之间的客户端通信被镜像到 CA Standard Monitor。



服务器网段

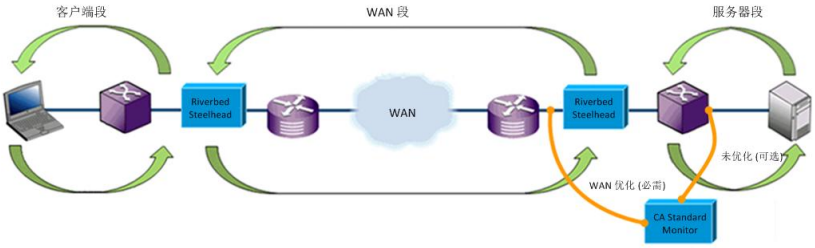
要报告服务器网段，数据中心中的 CA Standard Monitor 必须接收数据中心服务器和数据中心服务器交换机之间的未优化 TCP 通信量。

可以使用网络分流器，也可以将来自服务器交换机的通信量镜像到监视设备上的单独监视器 NIC。

CA Application Delivery Analysis 需要在数据中心部署 CA Standard Monitor 来监视服务器网段上的未优化通信量。

如果 CA Application Delivery Analysis 尚未监视数据中心中的未优化服务器通信量，可使用 CA Standard Monitor 来同时监视 WAN 优化和未优化的服务器通信量。

将服务器和数据中心交换机之间的未优化数据包镜像到监视设备上的单独监视器 NIC。在下面的 Steelhead 物理径内配置中，CA Standard Monitor 同时监视 WAN 网段中的优化通信量和服务器网段中的未优化通信量。



添加监视设备

将 CA Standard Monitor 添加到管理控制台以开始报告。

如果添加的监视设备当前在网络上不可用，那么在监控在网络中可用之后，需同步 (p. 224)监视设备，以便在监控和管理控制台之间建立通信。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 在“向我显示”菜单下单击“添加 ADA 监视器”。

   将打开“Standard Monitor 属性”。
4. 填写“Standard Monitor 属性”中的字段。有关指定监视设备属性的信息，请单击帮助。

   指定监视器 NIC 时，请确保已指定数据包源。例如，如果数据包源自 Steelhead 物理径内配置，请选择“Riverbed WAN 物理径内”选项。
5. 单击“确定”。

   监控将显示在“ADA 监视设备列表”中。
6. 单击相应链接，让监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步期间会暂时停止监视应用程序性能。为了最大程度地减少监视中断，请在同步监视设备之前完成所有更改。

   5-10 分钟之后，将显示“优化”页面。
7. 单击“优化”页面上的“帮助”，以获取如何报告 WAN 优化应用程序的详细信息。

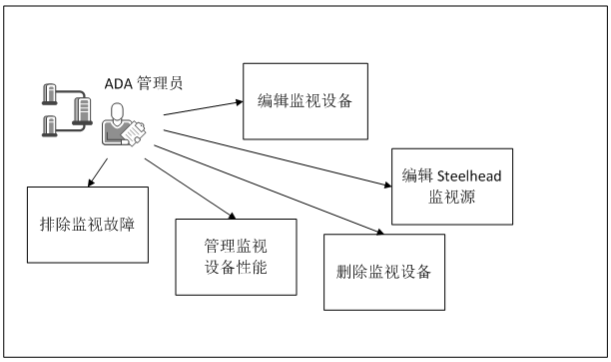
   如果未看到与您的应用程序相关的数据，请对监视设备进行故障排除。
8. 如果使用了域来分隔重复的 IP 通信量，请编辑 Steelhead 监视器源以分配域。

详细信息：

编辑监视器源 (p. 375)

管理监视设备

通过执行以下任务来管理监视设备：



任务
编辑监视设备 (p. 374)
编辑 Steelhead 监视器源 (p. 375)
管理监视设备性能 (p. 376)
删除监视设备 (p. 374)
排除监视故障 (p. 377)

编辑监视设备

例如，编辑监视设备以分配突发事件响应。编辑监视设备时，还可以查看任意监视设备突发事件。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“ADA 监视设备列表”，然后单击 进行编辑。
4. 在第三个“向我显示”菜单中单击“属性”。

   将打开“Standard Monitor 属性”。

   要查看监视设备的突发事件，请在第三个“向我显示”菜单中单击“突发事件”。
5. 单击“突发事件响应”，然后单击“确定”。此步骤将选择突发事件响应。

详细信息：

查看监视设备突发事件 (p. 235)

编辑监视器源

要将特定域分配给监视设备，请编辑监视器源。默认情况下，新的监视器源会分配到默认域。

管理控制台按照其数据包源来命名监视器源：

***IP 地址*物理 Riverbed 或 *IP 地址*虚拟 Riverbed**

指监视器源接收来自 WAN 网段并经过 Steelhead 优化的数据包。例如，IP 为 1.1.6.44 且使用 Steelhead 物理径内配置的监视器 NIC 被命名为“1.1.6.44 物理 Riverbed”。

***IP 地址*数据包**

指监视器源接收来自服务器网段未经优化的数据包。例如，IP 为 1.1.5.43 的监视器 NIC 将命名为 1.1.5.43 数据包。

***IP 地址*客户端网段**

指监视器源接收来自客户端网段未经优化的数据包。例如，IP 为 1.1.6.44 的监视器 NIC 将命名为 1.1.6.44 客户端网段。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。

   滚动到“ADA 监视设备列表”，找到包含所需数据包或 Steelhead 监视器源的 Standard Monitor，然后单击 。
3. 滚动到“监视器源”部分，并单击 以编辑 监视器源。有关详细信息，请单击“帮助”。
4. 单击“更新”。
5. 单击相应链接，将监视设备与管理控制台上当前的客户端网络、服务器子网和应用程序定义同步。

   监视设备在同步过程中暂时停止监视应用程序性能。为了尽量减少监视中断，请在同步监视设备前完成所有更改。

详细信息：

管理承租人 (p. 87)
创建一对监视器源 (p. 225)

管理监视器性能

如果监视设备停止向管理控制台发送数据的时间超过 15 分钟，管理控制台会自动创建一个“重大”监视设备突发事件。

详细信息：

编辑监视设备突发事件阈值 (p. 236)

删除监视设备

删除 CA 标准监视设备，以将其作为响应时间数据的源删除。当删除某个监视设备时，将取消固定已固定到对应监视器源的所有服务器，并自动分配另一个监视器源。更新监视器源分配可能需要长达 10 分钟。

如果您已将服务器连接到监视器源，并且您想在监视设备暂时脱机时继续监控服务器通信，则考虑下列选项：

- 删除监视设备之前，将服务器连接到其他监视器源。使监视设备重新联机时，将适当的服务器连接到监视器源。
- 删除监视设备。另一个监视器源将自动被分配，但是更新监视器源分配所使用的时间高达 10 分钟。

遵循这些步骤:

1. 单击“管理配置”页面。
2. 在“向我显示”菜单中，依次单击“数据监视”、“监视设备”。
3. 滚动到“ADA 监视设备列表”，然后单击 以删除监视设备。
4. 出现提示时单击“继续删除”。此步骤将删除监视设备。

   监视设备将从“ADA 监视设备列表”中删除。

排除监视设备故障

检修监视设备，以解决特定网段丢失报告数据的问题。

添加监视设备时，请同步 (p. 224) 监视设备 以建立 监控 和 管理控制台 间的通信。添加监视设备之后，可能需要花费最多 10 分钟的时间，报告网段上经过优化的应用程序性能。

如果管理控制台未显示分段的应用程序数据，请对以下每个段进行故障排除：

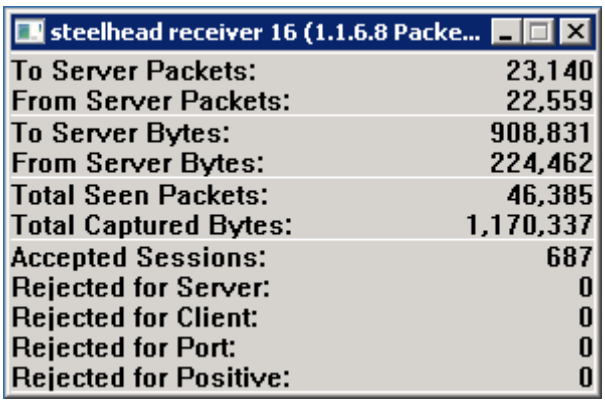
- WAN 网段：
  - 查看 Steelhead 接收器统计，检验监视设备在 Steelhead 监视器源存在活动会话。
  - 打开 Standard Monitor 属性，检查接收 Steelhead 优化通信的监视器 NIC 是否拥有数据中心内 Steelhead 设备的内径 IP 地址。
  - 从监视设备的监视端口实施数据包捕获，检查其是否包含 Steelhead 设备的 MAC 地址。
- 服务器网段。
  - 查看 SPAN 接收器统计，检查数据中心内的监视设备在数据包镜像监视器源是否存在活动会话。
  - 打开 Standard Monitor 属性，检查接收未优化服务器通信的监视器 NIC 是否为数据包镜像数据源。
- 客户端网段。
  - 查看 SPAN 接收器统计，检查分支机构的监视设备在数据包镜像监视器源是否存在活动会话。
  - 打开 Standard Monitor 属性，检查接收未优化客户端通信的监视器 NIC 是否为客户端网段镜像数据源。

查看 Steelhead 接收器统计

查看数据包计数器统计，可以获取有关 CA Standard Monitor 在特定监视器 NIC 上接收的 Steelhead 优化 TCP 数据包数据的信息。

重要提示：开始之前，请同步监视设备。必须同步监视设备才能显示其计数器窗口。

数据包计数器会显示以下信息：



到服务器数据包

标识从客户端发送到服务器的数据包总数。

来自服务器数据包

标识从服务器发送到客户端的数据包总数。

到服务器字节

标识从客户端发送到服务器的字节总数。

来自服务器字节

标识从服务器发送到客户端的字节总数。

可见数据包总计

标识与指定的应用程序端口、客户端网络和服务器子网相匹配的数据包总数。

注意：如果监控正常运行，则“可见数据包总计”数目与“接收的数据包”数目一致。如果监控无法检查其接收到的所有数据包，则“可见数据包总计”数目会低于“接收的数据包”数目。在此情况下，“已丢弃数据包”数目也将增加。有关详细信息，请参阅“已丢弃数据包”。

捕获的字节总计

表示与指定的应用程序端口、客户端网络和服务器子网相匹配的数据包的总字节数。

注意：CA Standard Monitor 会检查每个数据包标头，以便确定数据包是否与指定的应用程序端口、客户端网络和服务器子网相匹配。有关详细信息，请参阅“可见数据包总计”。

已接受的会话

表示与管理控制台上的有效应用程序/服务器/网络组合相匹配的 TCP 会话的数目。

服务器被拒绝

标识其中的服务器 IP 与服务器子网不匹配的 TCP 会话数。

客户端被拒绝

标识其中的客户端 IP 与客户端网络不匹配的 TCP 会话数。

端口被拒绝

标识其中的服务器端口与管理控制台忽略的端口列表相匹配的 TCP 会话数。

正当拒绝

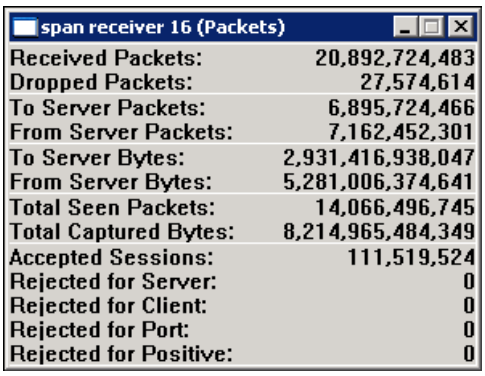
保留给将来使用。

查看 SPAN 接收器统计

有关 CA Standard Monitor 在特定监视器 NIC 上接收的未优化 TCP 数据包数据的信息，请查看数据包计数器统计。

重要提示：开始之前，请同步监视设备。必须同步监视设备才能显示其计数器窗口。

数据包计数器会显示以下信息：



接收的数据包

标识 CA Standard Monitor 上由监视器 NIC 接收但未检查的数据包总数。

注意：通过检查数据包标头，您可以使用这些数据包来计算应用程序响应时间度量标准。有关详细信息，请参阅“可见数据包总计”。

已丢弃数据包

标识已到达监视器 NIC 但其数据包标头未经检查的数据包总数。如果 CA Standard Monitor 忙于处理其他数据包且数据包捕获驱动程序缓冲区已满，数据包会被丢弃。

到服务器数据包

标识从客户端发送到服务器的数据包总数。

来自服务器数据包

标识从服务器发送到客户端的数据包总数。

到服务器字节

标识从客户端发送到服务器的字节总数。

来自服务器字节

标识从服务器发送到客户端的字节总数。

可见数据包总计

标识与指定的应用程序端口、客户端网络和服务器子网相匹配的数据包总数。

注意：如果监控正常运行，则“可见数据包总计”数目与“接收的数据包”数目一致。如果 监控 无法检查它接收的所有数据包，则“可见数据包总计”数目将小于“接收的数据包”数目，且“已丢弃数据包”数目会增加。有关详细信息，请参阅“已丢弃数据包”。

捕获的字节总计

表示与指定的应用程序端口、客户端网络和服务器子网相匹配的数据包的总字节数。

注意：CA Standard Monitor 会检查每个数据包标头，以便确定数据包是否与指定的应用程序端口、客户端网络和服务器子网相匹配。有关详细信息，请参阅“可见数据包总计”。

已接受的会话

表示匹配管理控制台上的有效应用程序/服务器/网络组合的 TCP 会话数目。

服务器被拒绝

标识其中的服务器 IP 与服务器子网不匹配的 TCP 会话数。

客户端被拒绝

标识其中的客户端 IP 与客户端网络不匹配的 TCP 会话数。

端口被拒绝

标识其中的服务器端口与管理控制台忽略的端口列表相匹配的 TCP 会话数。

正当拒绝

保留给将来使用。

详细信息：

客户端网络的工作方式 (p. 27)
应用程序的工作方式 (p. 93)
服务器的工作方式 (p. 61)
编辑 CA Standard Monitor (p. 258)

查看活动会话

要查看在最后 5 分钟报告间隔内报告的活动 IPv4 TCP 会话数，请使用“活动会话”页面。

活动会话信息确认 CA Application Delivery Analysis 正在监视 TCP 会话。管理控制台按应用程序端口和网段报告服务器上的活动 TCP 会话数。例如，端口 9088 [WAN] 显示的是 WAN 网段上端口 9088 应用程序通信量的会话信息。

详细信息：

在监视器源上查看活动会话 (p. 227)

词汇表

“未分级”性能等级

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

“轻微”性能分级

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

“重大”性能分级

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

5 分钟摘要文件

CA Application Delivery Analysis Standard Monitor、Multi-Port Monitor、Virtual Systems Monitor、CA GigaStor 或 Cisco NAM 创建的 *5 分钟摘要文件*包括每个性能度量标准/应用程序/服务器/网络组合 (p. 394)的 5 分钟平均值。

ACK 数据包

在 TCP 连接设置期间，客户端会向服务器发送 *ACK 数据包*，确认收到来自服务器的 SYN-ACK 数据包 (p. 387)。

CA ADA Availability Poller 服务

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

CA ADA Batch 服务

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

CA ADA Data Pump 服务

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

CA ADA Data Transfer Manager 服务

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

CA ADA Inspector Agent 服务

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

CA ADA Inspector 服务

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

CA ADA Master Batch 服务

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

CA ADA Messenger 服务

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

CA ADA Monitor Management 服务

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

CA ADA Monitor 服务

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

CA ADA Reader 服务

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

CA Application Delivery Analysis Manager (CA ADA Manager)

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

CA Observer Expert

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

FIN 数据包

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

NetQoS MySql51 服务

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

OLA

*请参见*性能运行水平协议（性能 OLA） (p. 393)和可用性运行水平协议（可用性 OLA） (p. 388)。

Ping 响应时间与数据包大小调查

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

Ping 响应时间调查

*Ping 响应时间调查*是一项服务器突发事件响应 (p. 394)，用于度量在发送 ping 请求之后收到 ping 回复所需的时间，并采用“数据包往复传输时间”进行报告。CA Application Delivery Analysis 管理员也可以启动或排定该调查。

role

*角色*指定 CA ADA 管理控制台中显示给 CA ADA 用户的页面。

RST 数据包

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

SNMP 配置文件

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

SNMP 陷阱通知

*SNMP 陷阱通知*是一种应用程序突发事件响应 (p. 392)、网络突发事件响应 (p. 391)或服务器突发事件响应 (p. 394)，用于向 SNMP 管理器通知受影响的应用程序、服务器或网络的“打开”或“已关闭”突发事件状态。

SPAN

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

SYN 数据包

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

SYN-ACK 数据包

在 TCP 连接设置期间，服务器会向客户端发送 *SYN-ACK 数据包*，确认收到来自客户端的 SYN 数据包 (p. 387)。监视设备使用 SYN-ACK 数据包对网络中的受监视连接进行计时和分析。

WAN

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

WAN 优化设备

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

三次握手

在 TCP 协议中，使用*三次握手*来建立客户端与服务器之间的连接。客户端会向服务器发送 SYN 数据包 (p. 387)来启动连接设置。服务器向客户端发送一个 SYN-ACK 数据包 (p. 387)来确认收到来自客户端的 SYN。最后，客户端向服务器发送一个 ACK 数据包 (p. 384)来确认收到来自服务器的 SYN-ACK 并建立 TCP 连接。监视设备使用三次握手对网络中的受监视连接进行计时和分析。

已分段数据包

*已分段数据包*是遍历网络时被拆分成多个数据包的数据包。

已丢弃数据包

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

分流器

请参阅网络分流器 (p. 390)。

分配层

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

无响应会话百分比

*无响应会话百分比*是一个服务器度量标准 (p. 394)，用于度量连接请求已发送但服务器未响应的会话的百分比。该度量标准是“未实现的 TCP/IP 会话请求”视图的一部分。

可用性运行水平协议（可用性 OLA）

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

电子邮件通知

*电子邮件通知*是应用程序突发事件响应 (p. 392)、服务器突发事件响应 (p. 394)或网络突发事件响应 (p. 391)，用于通知收件人有关受影响的应用程序、服务器或网络的阈值违反的信息。

丢弃的数据包

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

产品权限

*产品权限*确定用户在“管理配置”页面上可以执行的操作。

同步监视设备

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

多层应用程序

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

有效网络往复传输时间

*有效网络往复传输时间*是包括网络往复传输时间 (p. 391)和重传延迟 (p. 395)的网络度量标准 (p. 391)。请注意，重传延迟并不是由于重新传输导致的延迟，而是每次往复传输的平均重传延迟量。尤其值得注意的是，管理控制台增加了两个平均值，实际上是将两个度量标准组合在了一起。

权限集

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

网络分流器

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

网络区域

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

网络连接时间

网络连接时间 (*NCT*) 是一个网络度量标准 (p. 391)，用于度量从服务器发出 Syn-Ack 到从客户端再收到 Ack 所需的时间。在网络未被阻塞时，它是对网络延迟的一种度量，表示由于距离和序列化产生的最小延迟，也是网络体系结构中最佳的往复传输时间。该值的突发峰值通常是由于网络拥塞引起的，而停滞（上升后停止不动）通常意味着路径更改。

网络往复传输时间

*网络往复传输时间*是一个网络度量标准 (p. 391)，用于度量数据包在网络上的服务器和客户端之间双向传输所花的时间，不包括丢失的数据包。不包括应用程序、服务器以及客户端处理时间。

网络度量标准

*网络度量标准*表示某个应用程序性能问题是由当时与该应用程序通信的网络导致的。使用 CA Application Delivery Analysis 管理控制台，可以为以下每个网络度量标准自定义性能阈值：网络往复传输时间 (p. 391)、网络连接时间 (p. 390)、有效网络往复传输时间 (p. 390)和重传延迟 (p. 395)。

网络突发事件

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

网络突发事件响应

*网络突发事件响应*是 CA ADA 对网络突发事件 (p. 391)做出的响应。CA ADA 管理员可以将电子邮件通知 (p. 389)、SNMP 陷阱通知 (p. 387)和跟踪路由调查 (p. 399)分配给网络突发事件。

网络类型

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

观测计数

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

设备

*设备*可以是连接到受监视网络的任何 TCP/IP 系统。

严重度

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

应用程序

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

应用程序连接时间调查（术语）

*应用程序连接时间调查*是一种应用程序突发事件响应 (p. 392)，它向 IT 工作人员提供所需的信息来确定连接到某个 TCP/IP 应用程序端口需要多长时间。这包括服务器通过连接确认来响应的时间。CA ADA 管理员还可以启动或排定此调查。

应用程序突发事件

当网络事件或服务器事件影响应用程序的性能时，应用程序突发事件就会发生。

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

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

应用程序突发事件响应

*应用程序突发事件响应*是对网络突发事件 (p. 391)或服务器突发事件 (p. 394)的应用程序响应。例如，如果您为 Exchange 应用程序配置了应用程序突发事件响应，则当访问该 Exchange 应用程序的客户端创建了网络突发事件，或者承载该应用程序的服务器创建了服务器突发事件时，管理控制台就会启动该突发事件响应。超出某个综合度量标准 (p. 398)（如数据传输时间）的阈值时，管理控制台不会启动应用程序突发事件响应。管理控制台允许您向应用程序分配以下响应：电子邮件通知 (p. 389)、SNMP 陷阱通知 (p. 387)和应用程序连接时间调查 (p. 392)。

报告页面

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

事务

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

事务处理时间

*事务时间*是一个综合度量标准 (p. 398)，用于度量从客户端发送请求到收到响应中最后一个数据包的使用时间。“事务时间”是服务器响应时间 (p. 393)、网络往复传输时间 (p. 391)、重传延迟 (p. 395)和数据传输时间 (p. 399)之和。当超出“数据传输时间”阈值时，管理控制台不会打开一个突发事件。

到期的会话

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

性能运行水平协议（性能 OLA）

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

性能阈值

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

服务器子网

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

服务器连接时间

服务器连接时间 (SCT) 是一个服务器度量标准 (p. 394)，用于度量服务器通过发送 Syn-Ack 来响应客户端的 SYN 数据包，从而确认初始客户端连接请求所需的时间。

服务器响应时间

*服务器响应时间*是服务器度量标准 (p. 394)，用于测量服务器发送对客户端请求的初始响应或发送初始服务器思考时间所花费的时间。服务器响应时间增加通常表示缺乏服务器资源（如 CPU、内存、磁盘 I/O）、应用程序编写的糟糕或多层应用程序中某层性能不佳。

服务器度量标准

*服务器度量标准*将指明应用程序性能问题是由承载应用程序的服务器所导致的。使用 CA ADA 管理控制台，可以为以下每个服务器度量标准自定义性能阈值：服务器响应时间 (p. 393)、服务器连接时间 (p. 393)、被拒绝会话百分比 (p. 396)和无响应会话百分比 (p. 388)。

服务器突发事件

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

服务器突发事件响应

*服务器突发事件响应*是管理控制台对服务器突发事件 (p. 394)做出的响应。管理控制台允许您向服务器突发事件分配以下响应：电子邮件通知 (p. 389)、SNMP 陷阱通知 (p. 387)、Ping 响应时间调查 (p. 386)、通过 SNMP 的性能调查 (p. 396)和数据包捕获调查 (p. 398)。

组合

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

保持连接消息

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

响应操作

响应操作（如发送通知或启动调查）是对性能阈值违反做出的响应。

度量标准摘要文件

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

突发事件

当应用程序、服务器或客户端网络在某段时间出现异常行为时，管理控制台将会打开一个*突发事件*以提醒用户注意。请参阅响应操作 (p. 394)。

突发事件响应

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

重传延迟

*重传延迟*是一个网络度量标准 (p. 391)，用于度量从发送原始数据包到发送最后一个重复数据包使用的时间。管理控制台报告的“重传延迟”是整个观测的平均值，而不仅仅是针对重传的数据包。例如，如果一整套 10 个数据包需要 300 毫秒重传时间，则报告的重传延迟为 30 毫秒（300 毫秒/10 个数据包）。

核心层

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

监视设备

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

监视设备突发事件

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

监视单位

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

监视器源

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

被拒绝会话百分比

*被拒绝会话百分比*是一个服务器度量标准 (p. 394)，用于度量在报告间隔期间，服务器显式拒绝的连接请求的百分比。该度量标准是 CA ADA 管理控制台中“未实现的 TCP/IP 会话请求”报告的一部分。

调查

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

通过 SNMP 的性能调查

*通过 SNMP 的性能调查*是一种服务器突发事件响应 (p. 394)，其使用 SNMP 轮询服务器以获得性能信息，例如 CPU 和内存使用率。CA ADA 管理员还可以启动或排定此调查。

预计跃点延迟

*预计跃点延迟*是两个节点之间存在的延迟时间的预计值。管理控制台通过使用所有样本的平均值来确定此预计值（例如，在跟踪路由调查 (p. 399) 期间）。

域

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

基准

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

接入层

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

控制端口应用程序

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

敏感度级别

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

综合度量标准

*综合度量标准*将指明应用程序性能问题是由承载应用程序的服务器还是当前与该应用程序通信的网络再或是二者共同所导致的。CA ADA 管理控制台将为以下每个综合度量标准设置性能阈值：数据传输时间 (p. 399)和事务时间 (p. 393)。请注意，管理控制台不会创建应用程序突发事件。但是，由于综合度量标准既包括网络度量标准，又包括服务器度量标准，因此管理控制台可以将服务器或网络分级为“轻微”（黄色）或“重大”（橙色），并分级对应用程序自身性能产生的相应影响。例如，如果服务器度量标准分级为“轻微”，则管理控制台还可将应用程序的综合度量标准分级为“轻微”。

跃点

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

阈值

请参阅性能阈值 (p. 393)。

数据包丢失百分比

*数据包丢失百分比*是一个网络度量标准 (p. 391)，从临近服务器的监视设备有利位置度量重传数据占网络中总数据的比率。监视设备可以观测到由于网络路径中服务器到客户端方向上发生数据丢失而导致服务器重传的数据包。到达服务器之前客户端到服务器方向发生数据丢失时，监视设备将无法观测到数据包丢失，且“数据包丢失百分比”中不会包括该丢失。在管理控制台的“工程”页面上，“数据包丢失百分比”是 QoS 报告的一部分。

数据包捕获调查

*数据包捕获调查*是一种应用程序突发事件响应 (p. 392)或服务器突发事件响应 (p. 394)，用于对遇到问题的特定服务器、应用程序端口和网络执行筛选捕获。CA ADA 管理员还可以启动或排定此调查。

数据包摘要文件

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

数据传输时间

*数据传输时间*是一个综合度量标准 (p. 398)，用于度量传输完整的应用程序响应所花费的时间，从首次响应（服务器响应时间 (p. 393)结束）到该请求中发送完最后一个数据包。

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

当超出“数据传输时间”阈值时，管理控制台不会打开一个突发事件。

跟踪路由

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

跟踪路由调查

*跟踪路由调查*是一种网络突发事件响应 (p. 391)，可记录监视设备与端点之间的路径和每个跃点，以监视延迟和路由问题；在某些情况下，SNMP 会轮询每个路由器以获得其性能信息。CA ADA 管理员还可以启动或排定此调查。

端口排除项

*端口排除项*对监视设备上的应用程序端口通信量进行筛选，最大化管理控制台上的可用资源，同时可以使管理控制台用户将注意力集中放在要关注的应用程序上。监视设备会忽略与端口排除项匹配的 TCP 会话。

操作

*请参阅*响应操作 (p. 394)。