

CA Application Performance Management

CA Infrastructure Management 集成指南
版本 9.5



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

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

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

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

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

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

本文档由 CA 制作。

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

版权所有 © 2013 CA。保留所有权利。此处涉及的所有商标、商品名称、服务标识和徽标均归其各自公司所有。

CA Technologies 产品引用

本文档涉及以下 CA Technologies 产品和功能：

- CA Application Performance Management (CA APM)
- CA Application Performance Management ChangeDetector (CA APM ChangeDetector)
- CA Application Performance Management ErrorDetector (CA APM ErrorDetector)
- CA Application Performance Management for CA Database Performance (CA APM for CA Database Performance)
- CA Application Performance Management for CA SiteMinder® (CA APM for CA SiteMinder®)
- CA Application Performance Management for CA SiteMinder® Application Server Agents (CA APM for CA SiteMinder® ASA)
- CA Application Performance Management for IBM CICS Transaction Gateway (CA APM for IBM CICS Transaction Gateway)
- CA Application Performance Management for IBM WebSphere Application Server (CA APM for IBM WebSphere Application Server)
- CA Application Performance Management for IBM WebSphere Distributed Environments (CA APM for IBM WebSphere Distributed Environments)
- CA Application Performance Management for IBM WebSphere MQ (CA APM for IBM WebSphere MQ)
- CA Application Performance Management for IBM WebSphere Portal (CA APM for IBM WebSphere Portal)
- CA Application Performance Management for IBM WebSphere Process Server (CA APM for IBM WebSphere Process Server)
- CA Application Performance Management for IBM z/OS® (CA APM for IBM z/OS®)
- CA Application Performance Management for Microsoft SharePoint (CA APM for Microsoft SharePoint)
- CA Application Performance Management for Oracle Databases (CA APM for Oracle Databases)
- CA Application Performance Management for Oracle Service Bus (CA APM for Oracle Service Bus)
- CA Application Performance Management for Oracle WebLogic Portal (CA APM for Oracle WebLogic Portal)

- CA Application Performance Management for Oracle WebLogic Server (CA APM for Oracle WebLogic Server)
- CA Application Performance Management for SOA (CA APM for SOA)
- CA Application Performance Management for TIBCO BusinessWorks (CA APM for TIBCO BusinessWorks)
- CA Application Performance Management for TIBCO Enterprise Message Service (CA APM for TIBCO Enterprise Message Service)
- CA Application Performance Management for Web Servers (CA APM for Web Servers)
- CA Application Performance Management for webMethods Broker (CA APM for webMethods Broker)
- CA Application Performance Management for webMethods Integration Server (CA APM for webMethods Integration Server)
- CA Application Performance Management Integration for CA CMDB (CA APM Integration for CA CMDB)
- CA Application Performance Management Integration for CA NSM (CA APM Integration for CA NSM)
- CA Application Performance Management LeakHunter (CA APM LeakHunter)
- CA Application Performance Management Transaction Generator (CA APM TG)
- CA Cross-Enterprise Application Performance Management
- CA Customer Experience Manager (CA CEM)
- CA Embedded Entitlements Manager (CA EEM)
- CA eHealth® Performance Manager (CA eHealth)
- CA Insight™ Database Performance Monitor for DB2 for z/OS®
- CA Introscope®
- CA SiteMinder®
- CA Spectrum® Infrastructure Manager (CA Spectrum)
- CA SYSVIEW® Performance Management (CA SYSVIEW)

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：简介	9
统一的最终用户体验监控.....	9
解决方案体系结构.....	10
部署注意事项.....	11
端口注意事项.....	13
单点登录.....	14
CA SiteMinder 支持.....	14
更多信息.....	15
第 2 章：组件概览	17
多端口监视器.....	17
聚合设备中的数据流.....	18
Application Delivery Analysis 管理器	18
NetQoS Performance Center/CA Performance Center	19
TIM	19
企业管理器.....	20
APM 数据库.....	21
CEM 控制台	22
Workstation.....	22
WebView	23
Java 代理.....	23
.NET 代理	24
第 3 章：集成方案	25
如何将 CA APM 连接到多端口监视器	25
先决条件.....	27
多端口监视器上的 TIM	27
独立 TIM 选项	28
在多端口监视器上安装 TIM.....	29
配置硬件筛选.....	30
在逻辑端口上配置 TIM 监控.....	33
多进程模式下的 TIM	34
配置多进程模式的 TIM	35
将 TIM 与企业管理器相关联.....	37
(可选) 配置 Web 服务器筛选	38
同步监视器.....	39
验证连接.....	40

如何将 CA APM 连接到 Application Delivery Analysis.....	40
先决条件.....	41
运行安装程序.....	42
启动 ADA-APM 服务.....	45
同步时间.....	45
验证连接.....	46
如何将 CA APM 连接到 CA Performance Center	47
先决条件.....	49
运行安装程序.....	49
启动 APM-CAPC 服务	51
在 APM WebView 上配置报警.....	51
将 APM 视图导入 NetQoS Performance Center	52
将 APM 注册为数据源	52
将 APM 菜单项添加到应用程序运行状况	54
启用 HTTPS 支持（可选）	54
验证连接.....	55
如何将 CA APM 连接到 NetQoS Performance Center	56
先决条件.....	58
运行安装程序.....	58
启动 APM-CAPC 服务	60
在 APM WebView 上配置报警.....	60
更新 NetQoS Performance Center 数据库.....	61
将 CA APM 注册为数据源.....	62
启用 HTTPS 支持（可选）	63
验证连接.....	64

第 4 章：分类方案	65
如何使用 CEM 控制台对应用程序和基础架构问题进行分类.....	65
确定分类方案。	66
继续使用多端口监视器进行分类.....	69
继续使用 APM WebView 进行分类.....	70
如何使用 APM WebView 对应用程序和基础架构问题进行分类	70
确定分类方案。	71
继续使用 APM WebView 进行分类.....	77
继续使用 NPC/CAPC 进行分类.....	78
网络数据时间延迟.....	78
工具提示数据.....	79
ADA 如何计算网络和服务器运行状况.....	79
如何使用 NPC 对应用程序问题进行分类.....	80
确定分类方案。	81
继续使用 APM WebView 进行分类.....	90
继续使用 NPC/CAPC 进行分类.....	90

附录 A：故障排除 93

CA APM 应用程序数据在 NPC 上不可用	93
CA APM 应用程序数据在 CAPC 上不可用	94
TIM 停止工作	94
基础架构数据在 CEM 控制台上不可用	96
Workstation 上的“更多信息”按钮不起作用	97

第 1 章：简介

此部分包含以下主题：

- [统一的最终用户体验监控 \(p. 9\)](#)
- [解决方案体系结构 \(p. 10\)](#)
- [部署注意事项 \(p. 11\)](#)
- [端口注意事项 \(p. 13\)](#)
- [单点登录 \(p. 14\)](#)
- [CA SiteMinder 支持 \(p. 14\)](#)
- [更多信息 \(p. 15\)](#)

统一的最终用户体验监控

统一的最终用户体验监控是 CA APM 和 CA Infrastructure Management 之间的集成。通过此集成，您可以查看与最终用户的应用程序使用情况相关的应用程序级数据。选择集成哪些组件决定了在各种控制台和用户界面显示哪些信息。

集成选项包括：

CA APM 到多端口监视器

通过此集成，可在 CEM 控制台上查看高级别网络性能信息。有关详细信息，请参阅“[如何将 CA APM 连接到多端口监视器 \(p. 25\)](#)”。

CA APM 到 NetQoS Performance Center/CA Performance Center

通过此集成，可在 NetQoS Performance Center 上查看 CA APM 应用程序数据。有关详细信息，请参阅“[如何将 CA APM 连接到 NetQoS Performance Center \(p. 56\)](#)”或“[如何将 CA APM 连接到 CA Performance Center \(p. 47\)](#)”。

CA APM 到 CA Application Delivery Analysis

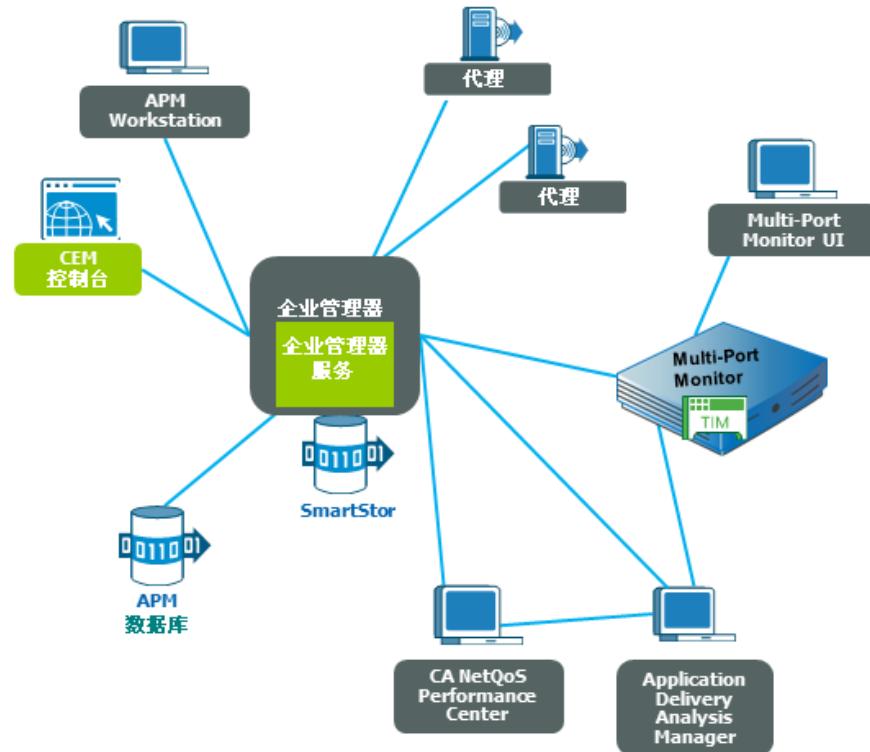
通过此集成，可在 APM WebView 上查看基础架构数据。有关详细信息，请参阅“[如何将 CA APM 连接到 CA Application Delivery Analysis \(p. 40\)](#)”。

解决方案体系结构

统一的最终用户体验监视解决方案提供许多部署选项，具体取决于网络的规模和复杂性。本节概述了两个可能的方案。

在单个多端口监视器就足够的较小环境中，部署体系结构可能看起来类似于下图。

图表1：带有单个多端口监视器的部署体系结构。

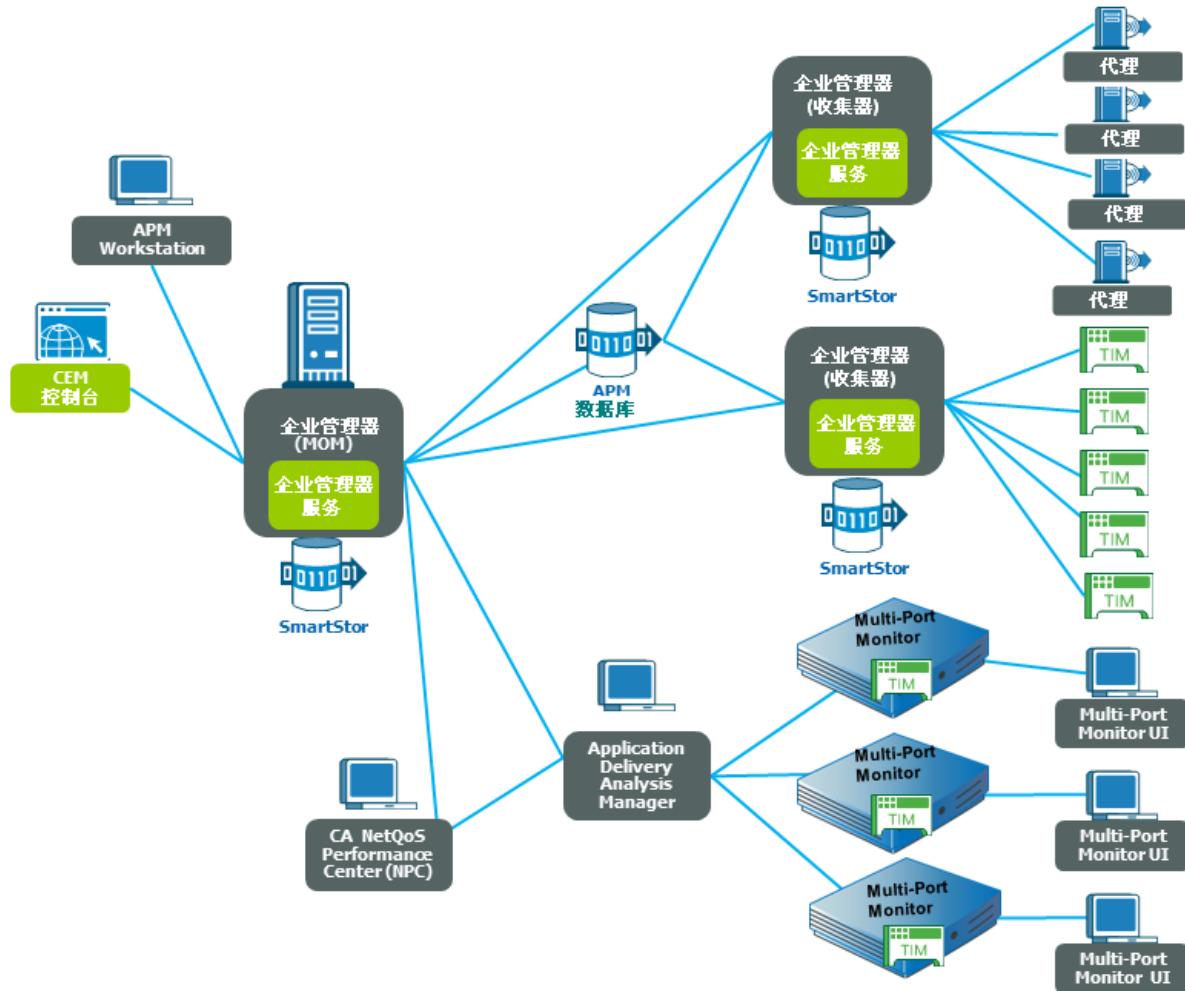


在需要多个多端口监视器的较为复杂的环境中，最多可以将规模扩大至：

- 10个企业管理器收集器
- 5个多端口监视器
- 5个独立TIM
- 3个ADA管理器、200个Java或.NET代理

较为复杂的环境通常需要包含多个多端口监视器的群集 CA APM 环境。在群集 CA APM 环境中，多个企业管理器（在群集时称为收集器）收集所有代理度量标准。您可以订阅来自所有企业管理器收集器和管理器的管理器 (MOM) 企业管理器的度量标准。此外，MOM 管理群集功能。例如，MOM 处理对数据的所有 Workstation 请求，并收集来自收集器的那些请求。您的部署体系结构可能看起来类似于下图。

图表 2：群集部署体系结构。



部署注意事项

在安装或升级之前，请仔细规划部署。以下列表概述了要考虑的一些重要步骤：

- 评估现有环境，并确定计划如何以及在何处部署必要的组件。
- 确定要监控的环境的特征。

- 了解并考虑聚合设备的 SPAN 或镜像端口选项。必须通过 SPAN 或镜像端口将多端口监视器连接到密钥交换机，该交换机承载到网络的应用程序通信。

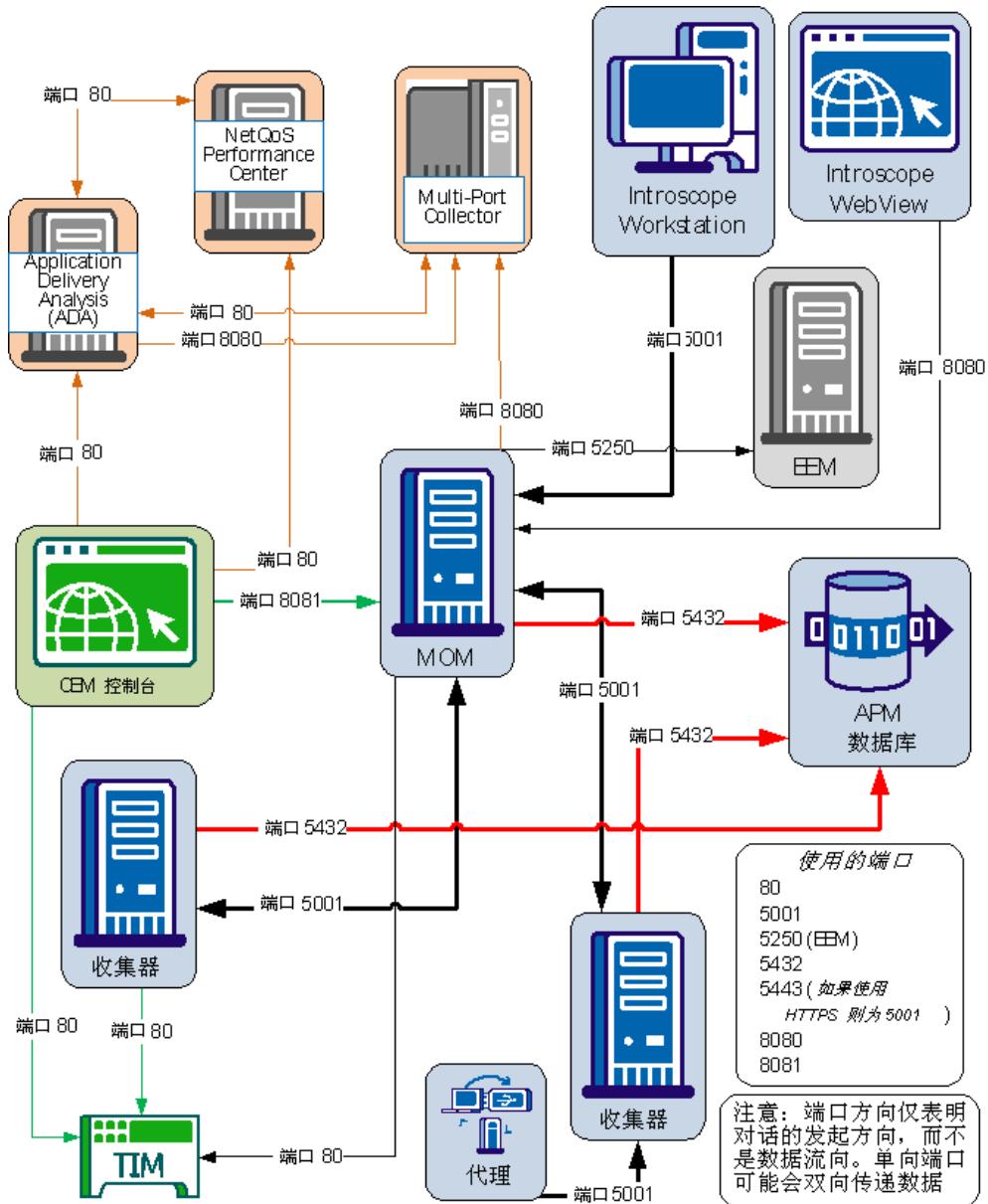
注意：有关与聚合设备相关的镜像端口的详细信息，请参阅《CA 多端口监视器用户指南》。
- 了解并考虑独立 TIM 的镜像端口选项。必须将独立 TIM 连接到镜像端口或网络分路。该配置确保 TIM 可以监控网络通信而不会干扰数据传输。

注意：有关与独立 TIM 相关的镜像端口和网络分路的详细信息，请参阅《CA APM 配置和管理指南》。
- 收集服务器 IP 地址和应用程序端口号。需要您想在企业网络中监控的 IP 地址和应用程序端口来配置交换机 SPAN 或镜像会话。
- 考虑可以阻止收集器设备与 ADA 管理器之间的通信的任何防火墙。

注意：有关多端口监视器所使用的端口和协议，请参阅《CA 多端口监视器用户指南》。
- 检查《CA APM 安装和升级指南》以了解以下 CA APM 组件的要求：
 - APM 数据库
 - 企业管理器
 - CEM 控制台
 - Workstation
 - 独立 TIM
- 检查《CA APM .NET 代理实施指南》以了解 .NET 代理安装要求。
- 检查《CA APM Java 代理实施指南》以了解 Java 代理安装要求。

端口注意事项

CA APM 与 CA Infrastructure Management 组件需要一些端口以便能够进行通信。下图显示了这些组件和端口。



注意: 如果多端口监视器上安装了 TIM, 它将在端口 80 上通过多端口监视器与 MOM 企业管理器进行通信。端口 8080 由 MOM 企业管理器用于与多端口监视器进行通信。

单点登录

单点登录是由 NetQoS Performance Center (NPC)/CA Performance Center (CAPC) 和所有支持的数据源使用的身份验证方案。用户经身份验证有权访问 NPC/CAPC 之后，无需再次登录即可在控制台和已注册的数据源中导航。

通过支持在单独的产品界面中导航，单点登录为操作员提供了一种无缝的深入查看体验。例如，第一次从 CEM 控制台导航到 TIM 时，系统会要求您使用在 ADA 或 NPC/CAPC（如果将 ADA 绑定到 NPC/CAPC）上配置的凭据登录。初始登录之后，在这两个组件之间导航时，就不需要再次登录。

注意： CA APM Workstation 或 WebView 不支持单点登录。每次导航到 CA APM Workstation/WebView 时，都必须使用该产品的凭据登录。

NPC/CAPC 使用分布式体系结构。在已安装支持的数据源或 NPC/CAPC 的每个服务器上，会自动安装一个单点登录网站实例。如果在同一服务器上安装了两个数据源产品，那么它们使用同一个单点登录网站实例。使用分布式体系结构，用户可以通过登录到运行各个 CA 数据源产品的服务器来登录这些产品。

注意： 有关单点登录的详细信息，请参阅《*CA Performance Center 管理员和用户指南*》。

CA SiteMinder 支持

如果已在应用程序服务器上安装 SiteMinder，那么您必须正确配置 TIM 以便进行事务监控。如果未正确配置 TIM，那么它将忽略源于这些应用程序服务器的所有事务。

注意： 有关配置 TIM 以使用 SiteMinder 进行事务监控的详细信息，请参阅《*CA APM 配置和管理指南*》。

更多信息

您可以参阅以下文档和资源：

- **CA APM 安装和升级指南**

面向部署团队和系统管理员。本指南为以下组件提供了安装和升级信息：

- APM 数据库
- 企业管理器/MOM
- Workstation
- 独立 TIM

- **CA APM 配置和管理指南**

面向系统管理员。本指南为以下组件提供了配置和管理信息（不包括定义应用程序事务内容）：

- APM 数据库
- 企业管理器/MOM
- Workstation
- 独立 TIM

- **CA APM 事务定义指南**

面向系统管理员。本指南涵盖了与建立和维护业务应用程序、业务服务和事务定义相关的信息。

- **CA APM Java 代理实施指南**

面向系统管理员。本指南涵盖了与安装和配置 Java 代理相关的信息。

- **CA APM .NET 用户指南**

面向系统管理员。本指南涵盖了与安装和配置 .NET 代理相关的信息。

- **CA APM Workstation 用户指南**

面向系统管理员和系统分析人员。本指南涵盖了与使用 Workstation 对应用程序进行分类相关的信息。

- **CA APM WebView 方案**

面向系统管理和系统分析员、以任务为导向的方案。这些方案涵盖了有关使用 WebView 对应用程序分类的信息。

- **CA APM 规模调整和性能指南**

面向系统管理员。本指南涵盖了与基于您的规模调整决策的硬件规模调整和系统性能相关的信息。

- **CA 多端口监视器安装指南**

面向系统管理员。本指南涵盖了与安装多端口监视器软件相关的信息。

- **CA 多端口监视器升级指南**

面向系统管理员。本指南涵盖了与升级多端口监视器软件相关的信息。

- **CA 多端口监视器用户指南**

面向系统管理员和分析人员。本指南涵盖了与配置、管理和使用多端口监视器相关的信息。

- **CA CA Performance Center 安装指南**

面向系统管理员。本指南涵盖了与安装 NPC/CAPC 软件相关的信息。

- **CA CA Performance Center 管理员和用户指南**

面向系统管理员和分析人员。本指南涵盖了与管理和使用 NPC/CAPC 相关的信息。

- **CA Application Delivery Analysis 安装指南**

面向系统管理员。本指南涵盖了与安装 CA Application Delivery Analysis 软件相关的信息。

- **CA Application Delivery Analysis 管理员指南**

面向系统管理员。本指南涵盖了与配置和管理 CA Application Delivery Analysis 相关的信息。

- **CA Application Delivery Analysis 用户指南**

面向分析人员。本指南涵盖了与使用 CA Application Delivery Analysis 用户界面相关的信息。

第 2 章：组件概览

此部分包含以下主题：

[多端口监视器 \(p. 17\)](#)

[Application Delivery Analysis 管理器 \(p. 18\)](#)

[NetQoS Performance Center/CA Performance Center \(p. 19\)](#)

[TIM \(p. 19\)](#)

[企业管理器 \(p. 20\)](#)

[APM 数据库 \(p. 21\)](#)

[CEM 控制台 \(p. 22\)](#)

[Workstation \(p. 22\)](#)

[WebView \(p. 23\)](#)

[Java 代理 \(p. 23\)](#)

[.NET 代理 \(p. 24\)](#)

多端口监视器

多端口监视器是一款硬件设备，它具有下列组件：

- 高性能捕获卡
- 用于系统和数据库的 4 磁盘 RAID 阵列
- 用于存储数据包的 12 磁盘 RAID 阵列

多端口监视器是一个大容量收集器，可将多个数据包集合组合到一个设备中。多端口监视器包括硬件和软件组件。硬件组件是一个 16 磁盘服务器，用于捕获和处理流入和流出交换机的流量。软件组件是一个管理 Web 界面，用于执行维护任务，检查设备上的集合状态，以及构建自定义视图。

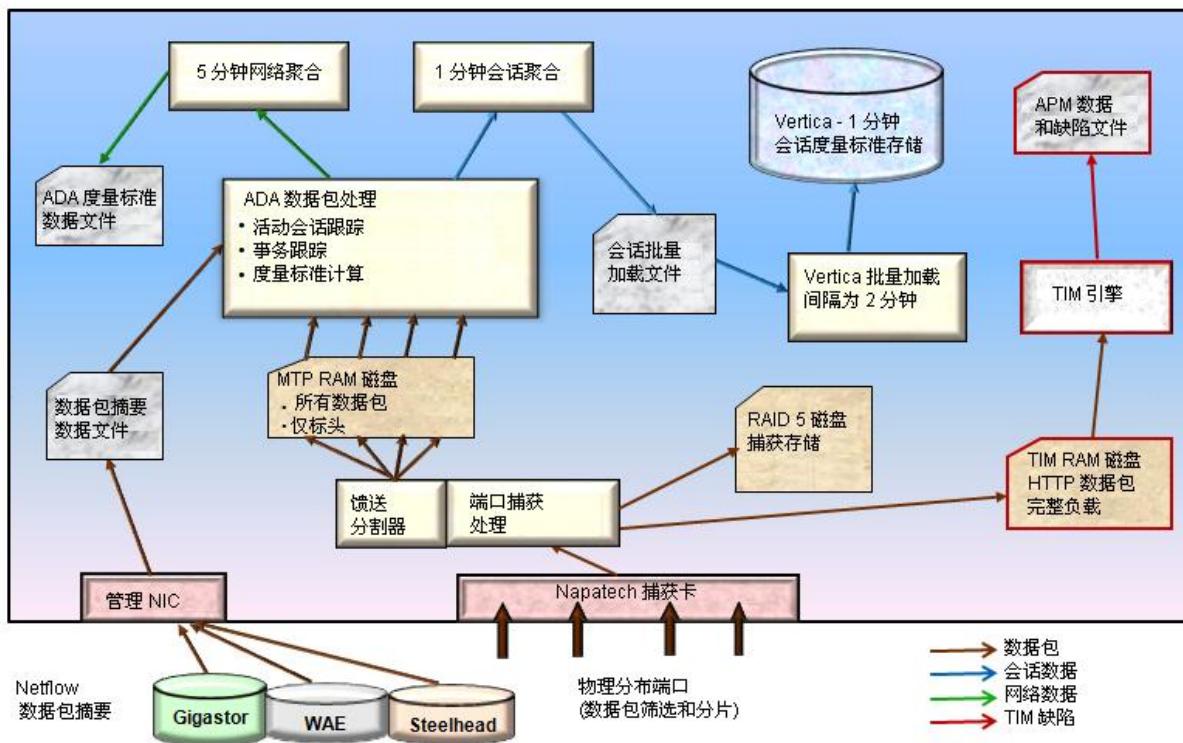
在多端口监视器上运行 TIM 时，该设备有时被称为聚合设备，以将其与没有 TIM 的多端口监视器进行区分。聚合设备支持 ADA 和 TIM 以执行网络、服务器和应用程序的非侵入式被动监控。它现在是 CA APM 和 ADA 的收集器设备。聚合设备连接到您的交换机，收集 SPAN 流量，并将该信息发送给 TIM 和 ADA。然后，这两个引擎将该信息发送到它们各自的控制台：CEM 控制台和 ADA 管理器。

重要信息！对于多端口监视器（未安装 TIM），您可以从网络上的不同点跨接到多端口监视器上的对应逻辑端口。对于聚合设备，您必须为 TIM 选择一个逻辑端口，并将 Web 通信从 WAN 跨接到该逻辑端口。为 TIM 以及 ADA 处理该通信。将其他逻辑端口用于其他跨接，最理想的是从最接近服务器的访问层交换机。仅为 ADA 处理非 TIM 逻辑端口。

注意：有关设备的详细信息，请参阅《多端口监视器用户指南》和《多端口监视器安装指南》。

聚合设备中的数据流

该图显示多端口监视器聚合设备内的数据包、会话数据、网络数据以及 TIM 缺陷的数据流。请注意，聚合设备有两个 RAM 磁盘。一个磁盘专门用于存储 TCP 数据包以进行 ADA 处理。第二个磁盘专门用于存储 HTTP 数据以进行 TIM 处理。



Application Delivery Analysis 管理器

ADA 是一个包含一个物理服务器和基于 Web 的用户界面（称为 ADA 管理器）的被动数据包收集器。ADA 可执行以下功能：

- 查看 TCP 数据，并专注于处于会话级别的网络级别度量标准
- 从集合设备中提取集合文件，并将这些文件导入到数据库中

- 将数据分类（通过按阈值评估）为正常、已降级或过度使用，并存储结果
- 维护突发事件列表和观察计数
- 每隔 5 分钟计算一次性能度量标准，并将其发送到 ADA 管理器
- 定义并关联服务器、网络和应用程序，并且将配置信息推送到集合设备
- 显示报告页面和视图上的已收集和已处理数据

NetQoS Performance Center/CA Performance Center

CA NetQoS Performance Center (NPC)/CA Performance Center (CAPC) 是基于 Web 的报告界面，显示来自 CA Performance Center 套件 CA APM 中的产品和受支持的第三方产品的性能数据。NPC/CAPC 报告提供各种格式的性能和设备数据视图，可帮助您有效地管理网络、应用程序和设备。

将 CA APM 与 NPC/CAPC 集成时，下列与应用程序相关的信息会显示在 NPC/CAPC 上：

- 在某个选定时间范围内由 CA APM 监控的应用程序、业务服务和业务事务的列表及其运行状况
- 选定时间范围的所有应用程序、业务事务组件 (BTC) 度量标准和客户体验度量标准（在 CA APM 用户界面显示为 RTTM）的趋势
- 选定业务事务的突发事件/缺陷的详细信息
- 到与某个缺陷相关联的特定客户端子网和服务器的链接（以进一步调查基础架构）

TIM

TIM 记录和观察 SPAN 端口上的 HTTP 和 HTTPS 数据包，识别用户登录和相关事务，并监控和报告缺陷和其他统计信息。TIM 计算所有这些度量标准，并将其发送到 CEM 控制台。

提供 **TIM** 的两个实例：独立 **TIM** 和在多端口监视器上安装的 **TIM**。这两个实例监控 **SPAN** 数据并收集有关基于 **Web** 的事务的度量标准。在多端口监视器上安装 **TIM** 之后，可以通过聚合设备查看应用程序和基础架构数据级别上的应用程序使用。下表概述了这两个 **TIM** 之间的关键差异。

多端口监视器上的 TIM	独立 TIM
在 64 位 CentOS Linux 5.5 上运行	在 64 位 Red Hat Linux 5.5 上运行
在多进程模式下运行可增加吞吐量	在单进程模式下运行
从由多端口监视器捕获层编写的文件读取数据包	直接从 NIC 读取数据包
时间源于数据包时间戳。 Napatech 卡（使用 Napatech 时钟）在数据包进入多端口监视器时为其打上时间戳。	时间源于系统时间（挂钟）
不需要 Napatech 卡或网卡，因为多端口监视器安装了自己的 Napatech 卡。	需要购买 Napatech 卡或网卡。
使用下列默认的登录凭据： 用户名: nqadmin 密码: nq	使用下列默认的登录凭据： 用户名: cemadmin 密码: quality

企业管理器

企业管理器运行分布在不同收集器上的服务。其中一些服务为 **TIM** 收集、统计聚合和数据库清除。使用单个企业管理器进行部署时，会将它称为独立环境。使用多个企业管理器进行部署时，会将它称为群集环境，在该环境中一个企业管理器作为 **MOM**。通过企业管理器群集，**MOM** 可以管理其他企业管理器。每个受管企业管理器（称为“收集器”）收集代理度量标准，并依次将这些度量标准传递到 **MOM**。

根据企业系统的规模和复杂性，可以使用不同的方式部署企业管理器。特定企业管理器的角色取决于其在独立或群集 **CA APM** 环境中的部署方式。

企业管理器/**MOM** 是使用 **CEM** 控制台和文本文件进行配置的。由企业管理器/**MOM** 所处理的一些数据可从 **CEM** 控制台进行查看，其他数据则可从 **CA APM Workstation/WebView** 进行查看。

有关 **CEM** 控制台的详细信息，请参阅

[CEM 控制台 \(p. 22\)](#)

有关 **CA APM Workstation** 的详细信息，请参阅

[Workstation \(p. 22\)](#)

APM 数据库

您可以选择 PostgreSQL 或 Oracle 作为您的 APM 数据库平台。多个因素可能会影响您的数据库平台选择。例如，PostgreSQL 数据库易于安装，只需很少的配置和日常管理。PostgreSQL 数据库还可以通过企业管理器安装程序自动安装。该数据库通常不需要单独的数据库管理员来安装或维护数据完整性和控制用户访问。然而，PostgreSQL 数据库也具有一些局限性，因而不适用于某些部署方案或组织。

通常，在决定 PostgreSQL 还是 Oracle 作为数据库平台时，请考虑下列因素。这些因素也可能会影响 APM 数据库从 PostgreSQL 到 Oracle 的规划迁移。

- 如果尚未安装数据库实例，可以使用企业管理器安装程序安装 PostgreSQL，而无需进行任何预先配置。
- 如果要最大程度地减少数据库维护，并尽可能地简化环境配置，可使用 PostgreSQL 数据库比使用 Oracle 数据库更为简单。
- 如果您要在没有数据库管理员组支持的情况下管理 APM 数据库，可使用 PostgreSQL 数据库，因为其所需的管理开销、专业知识以及数据库相关技能都较少。
- 如果您的组织基于某特定供应商的数据库进行了标准化，则可能需要使用该数据库平台。
- 如果已经拥有适用于特定数据库平台的数据库管理员资源和过程，您可以通过使用该数据库平台以最充分地利用这些资源。
- 如果您当前没有数据库管理员，与 PostgreSQL 数据库相比，则安装、配置和管理 Oracle 可能会比较困难。
- 如果您的组织具有复杂的数据库配置要求，可能需要比 PostgreSQL 所提供的更高级的配置和管理选件。
- 如果要监控大批量生产环境，可能需要比 PostgreSQL 所提供的更可靠的、可伸缩更强的数据库。

注意: 有关 APM 数据库的详细信息, 请参阅《CA APM 安装和升级指南》。

CEM 控制台

CEM 控制台是一个用户界面, 可用于:

- 记录和定义业务事务, 然后会使用业务事务创建事务定义
- 生成和查看与业务事务相关的报告
- 查看缺陷数据和事务定义, 将事务分组到服务中, 以及管理 CA APM 用户对企业管理器数据的访问

在统一的最终用户体验监控解决方案内, CEM 控制台的角色和责任不会显著地改变, 以下是一些例外:

- 网络运行状况数据可以从“缺陷详细信息”页面中获得
- 您可以使用缺陷和网络信息来识别潜在的性能问题, 并直接导航到多端口监视器

CEM 控制台是在企业管理器安装过程中安装的。

Workstation

使用 Workstation 以不同形式查看度量标准数据。授权用户可以执行管理和配置功能。Workstation 在以下窗口中提供信息:

控制台

显示包含数据查看器的显示板中的数据。

调查器

提供代理、应用程序、资源和度量标准的树和视图。

管理模块编辑器

提供管理模块和元素的树视图, 允许您创建和编辑管理模块。

显示板编辑器

允许对域 (或超级域) 具有写权限的用户创建和编辑数据查看器和其他显示板对象 (例如, 导入的图形、形状、线和文本)。

数据查看器

基于类型的数据的可视演示。

如果将 CA APM 与 CA Application Delivery Analysis 集成，基础架构运行状况数据会显示在 Workstation 调查器和控制台上。另外，从“网络状态信息”显示板可以直接访问 NetQoS Performance Center。

注意：有关 Workstation 的详细信息，请参阅《CA APM Workstation 用户指南》。

WebView

APM WebView 是 Workstation 的替代产品，但是没有管理功能。使用 APM WebView 以不同形式查看度量标准数据。APM WebView 在以下窗口中提供信息：

控制台

显示包含数据查看器的显示板中的数据。

调查器

提供代理、应用程序、资源和度量标准的树和视图。

管理

提供管理模块和元素的树视图，允许您创建和编辑管理模块。

如果将 CA APM 与 CA Application Delivery Analysis 集成，基础架构运行状况数据会显示在调查器和控制台上。另外，从“网络状态信息”显示板可以直接访问 NPC/CAPC。

Java 代理

Java 代理从在 Java 虚拟机 (JVM) 和应用程序服务器上运行的应用程序收集性能数据。Java 代理也从周围的计算环境中收集性能和可用性数据。Java 代理使用应用程序字节码中的探测器收集该数据，并将该数据发送到企业管理器。ProbeBuilder 指令 (PBD) 文件控制探测器监控哪些数据。可以更改 PBD 文件以适合环境的监控需求。在安装 Java 代理时会包含几个标准的 PBD，以及适用于应用程序服务器的特定 PBD。微调跟踪器和 PBD 文件中的指令，可以获得您希望在环境中监控的度量标准信息。

企业管理器负责处理和分析从 Java 代理接收的数据。可以从 CA APM Workstation 访问该信息。使用 Workstation，您可以检查信息，并基于接收到的数据设置操作和报警。

注意：有关详细信息，请参阅《CA APM Java 代理实施指南》。

.NET 代理

.NET 代理是适用于受管企业 .NET 应用程序的应用程序管理解决方案，这些应用程序提供组件级别的可见性。.NET 代理监控 Microsoft 公共语言运行时 (CLR) 环境中运行的任务关键 .NET 应用程序。

代理收集应用程序和环境度量标准，并将其转发到企业管理器。向 Introscope 代理报告度量标准的应用程序称为“已检测应用程序”。在系统上安装和配置 .NET 代理后，此处运行的应用程序将在启动时自动检测。

默认情况下，仅检测系统中活动的 IIS ASP.NET 应用程序。可以检测任何 .NET 应用程序，包括 IIS ASP.NET 应用程序和独立的 .NET 可执行文件。还可以仅检测某个应用程序子集或特定应用程序。

检测过程是使用 ProbeBuilding 技术执行的。该技术使用在 ProbeBuilder 指令 (PBD) 文件中定义的跟踪器，以识别代理在运行时从应用程序和 CLR 收集的度量标准。随后，.NET 代理将此度量标准信息发送到企业管理器。

注意：有关详细信息，请参阅《CA APM .NET 代理指南》。

第 3 章：集成方案

此部分包含以下主题：

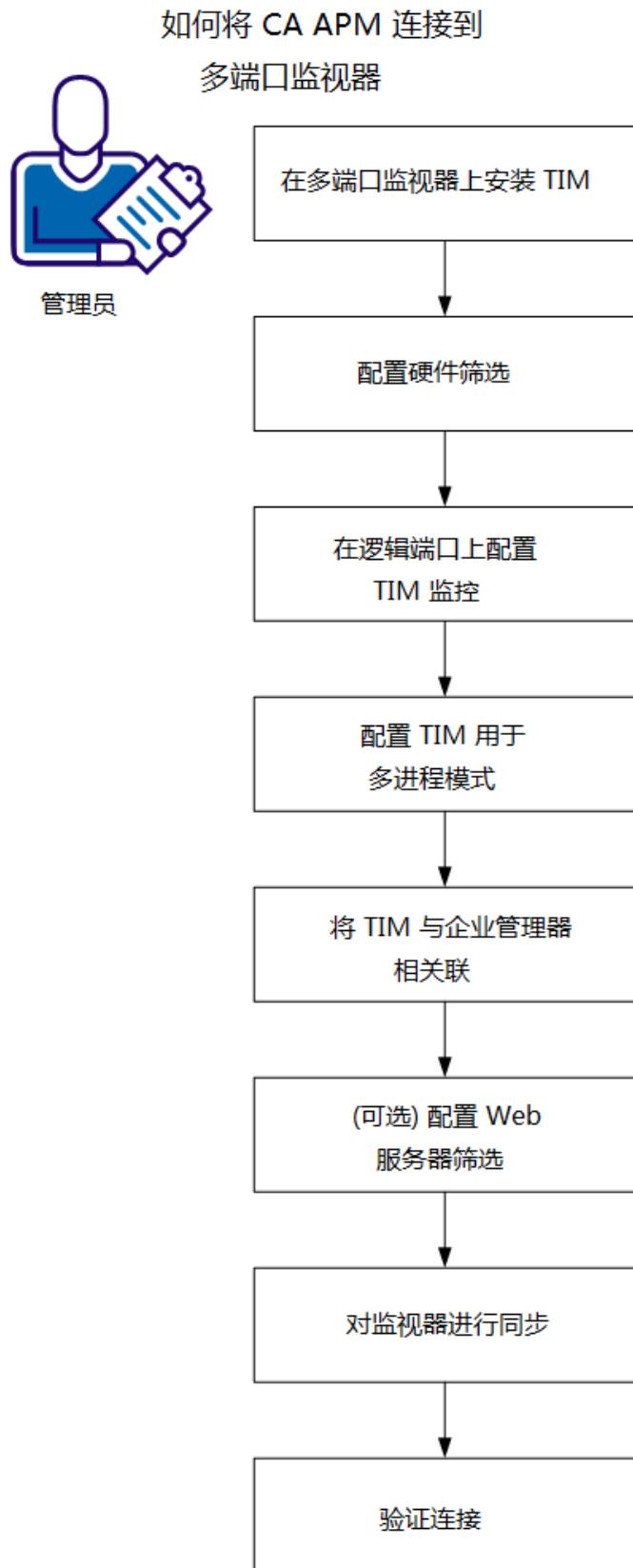
- [如何将 CA APM 连接到多端口监视器 \(p. 25\)](#)
- [如何将 CA APM 连接到 Application Delivery Analysis \(p. 40\)](#)
- [如何将 CA APM 连接到 CA Performance Center \(p. 47\)](#)
- [如何将 CA APM 连接到 NetQoS Performance Center \(p. 56\)](#)

如何将 CA APM 连接到多端口监视器

通过将 CA APM 连接到多端口监视器，可查看与被监控应用程序相关的高级别网络性能信息。对于正在查看的缺陷，将多端口监视器数据库中的网络数据导入到 CEM 控制台，并将其保存在 APM 数据库中。该数据会与 TIM 生成的缺陷一起呈现在“CEM 缺陷详细信息”页面中。您可以使用缺陷和网络信息确定潜在的性能问题，并直接导航到多端口监视器。

注意：生成缺陷与“CEM 缺陷详细信息”页面上显示网络数据之间可能会有短暂延迟(大约 4 到 5 分钟)。例如，如果缺陷在 2 分钟前生成，但“CEM 缺陷详细信息”页面上未显示网络运行状况信息，请等待几分钟，然后刷新视图。延迟是由于将网络数据定期加载到多端口监视器度量标准数据库造成的。

下图描述的是如何以管理员身份将 CA APM 连接到多端口监视器。



以管理员身份执行下列操作：

1. [在多端口监视器上安装 TIM \(p. 29\)](#)。
2. [配置硬件筛选 \(p. 30\)](#)。
3. [在逻辑端口上配置 TIM 监控 \(p. 33\)](#)。
4. [配置多进程模式的 TIM \(p. 35\)](#)。
5. [将 TIM 与企业管理器相关联 \(p. 37\)](#)。
6. [\(可选\) 配置 Web 服务器筛选 \(p. 38\)](#)。
7. [同步监视器 \(p. 39\)](#)。
8. [验证连接 \(p. 40\)](#)。

先决条件

在您开始之前，确认您已安装和配置：

- 多端口监视器 2.2
- APM 数据库 9.1 或更高版本
- 企业管理器 9.1 或更高版本
- CA APM Workstation 9.1 或更高版本
- CA APM WebView (可选)
- 下列各项之一：
 - CA APM .NET 代理 9.0 或更高版本
 - CA APM Java 代理 9.0 或更高版本

多端口监视器上的 TIM

使用 TIM，系统管理员可以配置多端口监视器设备来充当聚合设备。使用聚合设备可以收集 TCP 和 HTTP 数据，并将这些数据包传递至 TIM 和 CA Application Delivery Analysis（如果环境中配备了此产品）。通过多端口监视器聚合设备，您可以查看与最终用户的应用程序使用相关的应用程序和基础架构性能度量标准。

重要信息！对于多端口监视器（未安装 TIM），您可以从网络上的不同点跨接到多端口监视器上的对应逻辑端口。对于聚合设备，您必须为 TIM 选择一个逻辑端口，并将 Web 通信从 WAN 跨接到该逻辑端口。为 TIM 以及 ADA 处理该通信。将其他逻辑端口用于其他跨接，最理想的是从最接近服务器的访问层交换机。仅为 ADA 处理非 TIM 逻辑端口。

下表标识在多端口监视器上安装的 TIM 与独立 TIM 之间的差异。

多端口监视器上的 TIM	独立 TIM
在 64 位 CentOS Linux 5.5 上运行	在 64 位 Red Hat Linux 5.5 上运行
在多进程模式下运行可增加吞吐量	在单进程模式下运行
从由多端口监视器捕获层编写的文件读取数据包	直接从 NIC 读取数据包
时间源于数据包时间戳。 Napatech 卡（使用 Napatech 时钟）在数据包进入多端口监视器时为其打上时间戳。	时间源于系统时间（挂钟）
不需要 Napatech 卡或网卡，因为多端口监视器安装了自己的 Napatech 卡。	需要购买 Napatech 卡或网卡。
使用下列默认的登录凭据： 用户名: nqadmin 密码: nq	使用下列默认的登录凭据： 用户名: cemadmin 密码: quality

独立 TIM 选项

如果存在现有独立 TIM，则可以选择下列选项：

- 保留独立 TIM、将独立 TIM 升级到版本 9.1 或更高版本，以及重新配置每个 TIM（包括多端口监视器上的新 TIM）以监控特定网络通信并在 TIM 间平衡通信负载。

注意：独立 TIM 很少与 ADA 进行集成。由独立 TIM 和多端口监视器上的 TIM 所收集的数据生成在 CEM 控制台上显示的缺陷。但是，只能从多端口监视器上的 TIM 生成的缺陷链接到会话分析数据。多端口监视器必须为 CA APM 和 ADA 处理 SPAN 数据才能支持集成。

- 删除独立 TIM，并将独立 TIM 的 SPAN 移动到多端口监视器上的新 TIM。请参阅《CA 多端口监视器用户指南》。

有关配置 TIM 监控和负载平衡的详细信息，请参阅

[\(可选\) 配置 Web 服务器筛选 \(p. 38\)](#)

在多端口监视器上安装 TIM

在多端口监视器上安装 TIM，以便使它能够收集 TCP 和 HTTP 数据。下面的两个安装文件是多端口监视器所需的 CentOS 特定映像，并且必须按照以下顺序安装：

1. 第三方映像：APMCOSTRDPRTxxxx.img
2. TIM 映像：APM_COSTIMCMxxxx.img

[CA 支持](#)的 CA APM 软件下载区或 TIM 软件 DVD 捆绑中都提供这两个文件。

开始安装之前，请确认已配置多端口监视器并将其连接到网络。

遵循这些步骤：

1. 如果尚未更改默认值，请使用您的管理员凭据或以下凭据登录到多端口监视器：

用户名 = nqadmin

密码 = nq

2. 单击“系统设置”选项卡。

3. 单击“安装软件”选项卡。

此时将打开“安装软件”页面。

4. 安装第三方软件。

a. 单击“浏览”并导航到 TIM 安装文件。

b. 选择 APMCOSTRDPRTxxxx.img 文件。

c. 单击“上传并安装”。

d. 阅读并接受许可协议。

接受 EULA 以继续。

e. 此时将显示软件安装日志。如果看到错误，请与 CA 支持联系。

将安装第三方软件。

5. 安装 TIM 软件。
 - a. 单击“安装软件”选项卡。
 - b. 单击“浏览”并导航到 TIM 安装文件。
 - c. 选择 APM_COSTIMCMxxxx.img 文件。
 - d. 单击“上传并安装”。
 - e. 阅读并接受许可协议。
接受 EULA 以继续。
 - f. 此时将显示软件安装日志。如果看到错误，请与 CA 支持联系。
将安装 TIM 软件。
6. (可选) 单击“系统设置”选项卡以查看已安装的软件包列表，或单击“管理”选项卡以在多端口监视器逻辑端口上启用 TIM 监控。
7. 重新启动多端口监视器。

配置硬件筛选

对于 CA APM 到多端口监视器集成，由 TIM 监控的 Web 通信必须包含完整的数据包。通过从多端口监视器 Web UI 编辑“HTTP-完整数据包”默认筛选来定义完整数据包捕获。

您可以创建、启用、禁用和修改预定义筛选和您创建的筛选。

遵循这些步骤：

1. 在 Web 界面中单击“管理”、“逻辑端口”。
此时将打开“逻辑端口”页面。
2. 如果要筛选逻辑端口，单击“编辑筛选”列中的“筛选”链接。
此时将打开“逻辑端口：硬件筛选”页面。

3. 要创建筛选，单击“新建”。此时将打开“逻辑端口：新建硬件筛选”页面。

a. 填写下列字段：

- **启用的筛选**。在指明名称的逻辑端口上应用筛选。如果已选定，将在重新启动 nqcapd 进程之后应用筛选。
- **筛选名称**。正在创建或编辑的筛选的名称。该筛选名称将显示在已应用筛选的逻辑端口的“硬件筛选”页面上。
- **筛选优先级**。当筛选条件重叠时，优先级可决定筛选的优先顺序。当两个或多个重叠筛选具有相同优先级时，该优先顺序不确定。值介于 0（最高优先级）到 62（最低优先级）。默认优先级为 10。

筛选优先级设置可以用于数据包切割。例如，您希望为每个 HTTP 数据包保留更多字节。可以为 TCP 和端口 80 指定筛选，同时将切割设置为“TCP 标头 + 50 字节”，优先级设置为 1。然后为 TCP 指定其他筛选，同时将切割设置为“TCP 标头 + 1 字节”，优先级设置为 10。在这种情况下，为 HTTP 通信保留的负载字节数比为 TCP 通信保留的负载字节数多。

- **数据包切割模式**。用于仅捕获每个数据包选定部分的选项。通过硬件筛选可以捕获除 TCP/IP 之外的协议数据包。但是，多端口监视器仅收集 TCP 通信的性能度量标准。收集所有通信类型的卷度量标准。

捕获完整数据包：捕获经过筛选的每个数据包的所有信息。

捕获固定大小：从每个数据包捕获特定字节数。在“数据包切割大小”字段中，提供要捕获的字节数。

捕获标头及大小：捕获第 2 层、第 3 层和第 4 层的所有标头，以及“数据包切割大小”字段中的固定负载字节数。第 2 层标头包括 Ether II、LLC、SNAP 和原始标头以及 VLAN、ISL 和 MPLS 标记。第 3 层标头包括 IPv4（包括 IPv4 选项）、IPv6 和 IPX 标头。第 4 层标头包括 TCP、UDP 和 ICMP 标头。

- **仅包含协议**。限制要捕获和处理的协议。监控中仅包含选定的协议。如果未选中任何复选框，所有协议都将包含在内。

传输控制协议 **TCP** 是 CA Application Delivery Analysis 监控的主要协议。

用户数据报协议 **UDP** 用于传输实时或流应用程序发送的数据。

Internet 控制消息协议 **ICMP** 用于服务器之间错误消息传递以及 CA Application Delivery Analysis 跟踪路由调查。其限制要捕获和处理的协议。监控中仅包含选定的协议。如果未选中任何复选框，所有协议都将包含在内。

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

对于 IPv4 地址，使用以下格式：**x.x.x.x/n**，其中 **x.x.x.x** 是采用点分表示法的 IPv4 子网地址，**n** 是用于掩码的位数。

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

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

- **IP 地址**。需要进行监控或从监控中排除的各个主机的 IPv4 或 IPv6 地址或地址范围。用逗号分隔多个地址 (不含空格)。用连字符分隔范围 (不含空格)。不要组合使用列表中的单个地址和范围。不要组合使用同一列表中的 IPv4 和 IPv6 地址或地址范围。选择“排除”可放弃所列出地址的通信。

对 IPv4 地址使用点分表示法。例如，**10.9.7.7** 或 **10.9.8.5-10.9.8.7**。

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

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

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

- b. (可选) 单击“高级”以使用正则表达式创建更精确的筛选。有关详细信息，请参阅“使用正则表达式进行精确筛选”。
 - c. 单击“保存”。新筛选将显示在“逻辑端口：硬件筛选”页面上。
4. 要修改或启用筛选，请单击“编辑”。此时将打开“逻辑端口：编辑硬件筛选”页面。
- a. 填写步骤 3a 中所述的字段。
 - b. (可选) 单击“显示详细信息”以正则表达式查看您的选择。
 - c. 单击“保存”。筛选将显示在“逻辑端口：硬件筛选”页面上。
5. 在启用筛选后，重新启动 **nqcapd** 进程。

在逻辑端口上配置 TIM 监控

TIM 监视来自一个逻辑端口的镜像端口。要将多个物理端口映射到一个逻辑端口，请将 Web 通信从 WAN 镜像到该逻辑端口。系统会处理针对 TIM 和 CA Application Delivery Analysis（如果环境中配置了此产品）的通信。将其他逻辑端口用于其他端口镜像，最理想的是从最接近服务器的访问层交换机。仅为 CA Application Delivery Analysis 处理多端口监视器上的非 TIM 逻辑端口。

遵循这些步骤：

1. 打开浏览器窗口，并登录到多端口监视器 Web 界面。

此时将打开多端口监视器 Web 界面。

2. 单击“管理”选项卡。

此时将打开“逻辑端口”页面。将显示可用端口的默认设置。

1. 单击“编辑筛选”列中的“筛选”链接以将硬件筛选应用于端口。
2. 提供以下信息：

Name

指定需要 TIM 监控的逻辑端口的名称。

该名称有助于识别要监控的通信的源。例如，使用监控的交换机的名称或位置。

已启用

启用端口以进行监控。

确认已选中标签为“已启用”的复选框。

将数据包保存到磁盘

(可选) 将捕获的数据包保存在多端口监视器硬盘驱动器上。使用该选项，可以在“分析”页面上将数据导出到 PCAP。默认情况下，多端口监视器会将数据包保留六个小时。

TIM 监视器

与正在配置的逻辑端口相关联。

选中与正在配置的逻辑端口相关联的复选框。

物理端口

将一个或多个可用物理端口分配给逻辑端口。

可用的端口取决于从 CA Technologies 购买的捕获卡配置。

逻辑端口编号从 0 开始。捕获层执行物理端口到逻辑端口的映射。映射进程对于 TIM 是透明的。

3. 单击“保存”。

4. 重新启动 nqcapd 进程。

在“多端口监视器进程”页面上执行该任务。

5. (可选) 通过查看“系统状态”页面上的“捕获卡逻辑端口状态”表，检查逻辑端口的状态。

如果启动逻辑端口时出现问题（例如，在与该端口关联的硬件筛选中存在语法错误），“状态”列会显示一种错误状态。

多进程模式下的 TIM

在多端口监视器上安装了 TIM 之后，TIM 可以利用多个 CPU 并在多个进程间平衡通信负载。在多进程模式下运行会显著增加 TIM 吞吐量。具体的吞吐量数量基于许多因素（如，受监控通信、定义事务的方式等）而变化。

在多进程模式下，TIM 会在多个进程（称为工作进程）间拆分网络通信。要使 TIM 在多进程模式下高效地工作，请执行以下操作：

- 尽可能平均地在工作进程之间分布受监视通信。
- 确认同一工作进程监视属于同一业务事务实例的所有数据包。

在不同的网络配置中，可以通过不同的方式实现这些准则。CA Technologies 提供了几种在工作进程之间分布通信的灵活方式。选项包括：

客户端 IP 地址

网络通信基于客户端 IP 地址分配给工作进程。这是默认选项，也是 CA Technologies 建议的选项。如果您的网络配置使该选项不可行，请考虑其他选项。例如，如果所有通信看起来都来自同一客户端 IP 地址（比如，当 TIM 位于代理服务器后面时），请考虑其他配置选项。该示例的默认配置为 `shared=client`。使用该网络配置不可能平衡 TIM 上的负载，因此请考虑使用服务器 IP 地址选项。

服务器 IP 地址

网络通信基于服务器 IP 地址分配给工作进程，例如，`shared=server`。该选项要求单个服务器处理业务事务中的所有事务。

混合

可以基于客户端 IP 地址和服务器 IP 地址的组合，将通信分配给工作进程。如果服务器规则与客户端规则之间存在差异，则服务器规则优先。

使用负载平衡器配置文件来定义希望 TIM 如何对客户端或服务器进行负载平衡。

注意：独立 TIM 在单进程模式下运行。

有关编辑配置文件的信息，请参阅

[编辑负载平衡器配置文件 \(p. 35\)](#)

示例：配置在多进程模式下运行的选项

以下示例显示在多进程模式下设置 TIM 的配置选项。在平衡器配置文件 balancer.conf（位于 /etc/wily/cem/tim/config/ 中）上进行这些配置更改。重新启动 TIM 以激活这些配置更改。

示例 1

如果拥有 HTTP 事务属于 138.42.123.*/24 子网的客户端，请使用以下配置将工作进程 0 分配给该子网：client=138.42.123.*/24 worker=0。

示例 2

如果您在 138.42 子网中有一个服务器，使用以下配置将工作进程 0 分配给该子网：server=138.42.0.0/16 worker=0。

配置多进程模式的 TIM

配置多进程模式的 TIM 可利用多个 CPU 并在多个进程中执行通信负载平衡。此配置过程包含两个步骤。

1. [编辑负载平衡器配置文件 \(p. 35\)](#)。
2. [启用多进程模式 \(p. 36\)](#)。

编辑负载平衡器配置文件

编辑负载平衡器配置文件来定义希望 TIM 如何对客户端或服务器进行负载平衡。该文件是纯文本文件，必须使用文本编辑器对其进行更改。

遵循这些步骤:

1. 使用连接的键盘和监视器登录到聚合设备（运行 TIM 的多端口监视器）。也可以使用在 Windows 上运行的安全 shell (SSH) 客户端（如 PuTTY）从远程系统登录。
 1. 如果使用连接的键盘和监视器，请在初始屏幕上按 Alt+F2。此时将打开 Linux 登录屏幕。
2. 使用以下凭据登录：
 - 用户名: netqos
 - 密码: 安装多端口监视器软件时创建的密码。“netqos”用户名和密码提供超级用户访问权限。Linux 命令行界面将打开。
2. 使用文本编辑器打开 balancer.cnf 文件。
该文件位于 /etc/wily/cem/tim/config/balancer.cnf。
不要使用 Word 处理器或其他添加格式化信息的程序。
3. 使用“sudo”前缀编辑文件。只能使用超级用户访问权限和“sudo”前缀编辑配置文件。
例如，如果正在使用 vi 编辑器，请使用以下命令：

```
$ sudo vi /etc/wily/cem/tim/config/balancer.cnf
```
4. 保存该文件。
5. 重新启动 TIM。
必须重新启动 TIM 才能应用编辑内容。

启用/禁用多进程模式

在 TIM 配置窗口中启用/禁用多进程模式。默认情况下会启用该模式。

遵循这些步骤:

1. 登录到多端口监视器用户界面，选择“系统设置”。
2. 选择“Tim x.x.x.x 内部版本 xx”。
此时将打开“Tim 设置”页面。
3. 选择“配置 TIM 设置”
此时将打开“Tim 设置”页面。
4. 选择“Parallel/UseWorker”。

5. 相应地更改“新值”字段。
1 表示已启用多进程模式。
0 表示已禁用多进程模式。
6. 重新启动 TIM。
您必须重新启动 TIM 以便该更改生效。

将 TIM 与企业管理器相关联

该任务与多端口监视器上的 TIM 以及独立 TIM（如果适用）都相关。

启用 TIM 以便 TIM 可以监控事务。企业管理器不从已禁用的 TIM 监视器接收数据。如果您有群集的企业管理器，请从 MOM 企业管理器启用 TIM。

下面列出了您需要启用 TIM 的一些情形：

- 设置 TIM 并且将其与企业管理器关联时。
- 在升级 TIM 和/或企业管理器之后。
- 在导入配置之后。

遵循这些步骤：

1. 打开 Web 浏览器，输入承载企业管理器的服务器的地址。如果使用的是群集环境，请指定 MOM 的地址：

`http://<IP 地址>:8081`

其中 `<IP 地址>` 是 MOM 或独立企业管理器的 IP 地址或 DNS 名称。例如：

`http://192.168.1.54:8081`

`http://cem.company.com:8081`

要使用 DNS 名称，您的 DNS 管理员必须已经配置了 DNS 名称。

注意：默认端口为 8081。它在 *IntroscopeEnterpriseManager.properties* 文件中定义为 *introscope.enterpriseManager.webserver.port=8081*，可以更改。

2. 输入用户名和密码。
此时将出现 CEM 控制台。
3. 选择“设置”、“监视器”。

4. 如果 TIM 没有出现在列表中：

- a. 单击“新建”。
- b. 输入 TIM 的名称和 IP 地址。
- c. 如果 TIM 正在侦听多端口监视器端口，请选中“多端口监视器已启用”复选框。

该任务仅在您部署多端口监视器时适用。

- d. 单击“保存”。

5. 选择每个所需 TIM 旁边的复选框，然后单击“启用”。

将启用企业管理器和 TIM 之间的通信。CA CEM 控制台中显示了其他选项卡。

(可选) 配置 Web 服务器筛选

该任务是可选的。如果在配置硬件筛选之后仍看到过多网络通信，请执行该任务。这种情况下，需要通过配置 Web 服务器筛选进一步将由 TIM 监控的通信限制到特定服务器。如果 TIM 超载，记录功能可能无法运行。

多端口监视器使用为在设备上运行的 TIM 配置的 Web 服务器筛选来定义将哪些数据转发到 TIM。

遵循这些步骤：

1. 登录到 CEM。
2. 选择“设置”>“Web 服务器过滤”。
3. 单击“新建”。
4. 键入一个名称来描述 TIM 监控的网络部分。例如，*WebFarmCorp1*。

Web 服务器筛选: Web
查看或修改分配给必须监控的网络部分的 TIM。
[保存] [删除]
Web 服务器筛选设置 [示例]
名称: Web Web 场 1xx
监视器: acceptanceMonitor
地址类型: IP 地址 MAC 地址

发件人 IP 地址: 0.0.0.0 [给我显示示例]
收件人 IP 地址: 255.255.255.255
端口: 443 443
0 匹配所有端口
[在没有检查重叠的 IP 地址的情况下保存]

5. 在“监视器”列表中，选择要用于监控此网络部分的 **TIM**。

默认情况下每个 **TIM** 监控一个 IP 地址范围。如果要改为使用特定 MAC 地址进行监控，请转到步骤 6。

a. 填充“起始 IP 地址”字段。

输入处于较低范围的 Web 服务器的 IP 地址。如果只有一个服务器需要监控，请输入特定的 IP 地址。

b. 填充“结束 IP 地址”字段。

输入处于较高范围的 Web 服务器的 IP 地址。如果只有一个服务器需要监控，请输入特定的 IP 地址。

c. 填充“端口”字段。

- 如果 **TIM** 仅用于监控特定端口上的事务，请输入该端口号。
- 如果 **TIM** 用于监控所有端口上的所有事务，请输入 0（默认值）。

d. 在大多数情况下，**TIM** 应监控网络中特定的服务器，而不是重叠的服务器。但在特殊情况下，您可以允许重叠 IP 地址。

如果要为某个 IP 地址或范围配置多个监视器，请选择“在没有检查重叠的 IP 地址的情况下保存”。

6. 如果您要监控某个特定的 MAC 地址而不是 IP 地址范围：

a. 单击“MAC 地址”作为地址类型。

b. 键入您要监控的设备的特定 MAC 地址。例如：12:eb:a0:32:51:4c。

7. 单击“保存”以按指定方式配置 **TIM** 监控器。

同步监视器

同步监视器以将当前域配置文件发送到所有已启用的 **TIM** 和代理。

遵循这些步骤：

1. 登录到 CEM 控制台。
2. 选择“设置”>“监视器”。
3. 如果禁用了任何所需的监视器，请将其启用。
4. 单击“同步所有监视器”。

将同步所有已启用的监视器，并在右上角显示关联图标。该任务将向网络中所有已启用的 **TIM** 发送更新的事务定义。**TIM** 立即开始监控已定义的事务。同步所有监视器还将导致 CEM 控制台向企业管理器发送事务和跟踪信息。

验证连接

针对正在查看的缺陷，根据需要将多端口监视器数据库中的网络数据导入到 CEM 控制台。该数据会与 TIM 生成的缺陷一起呈现在“CEM 缺陷详细信息”页面中。

查找“CEM 缺陷详细信息”页面上的网络数据，确认 CA APM 已连接到多端口监视器。

遵循这些步骤：

1. 登录到 CEM 控制台。
2. 依次选择“CEM”、“突发事件管理”、“缺陷”。
3. 执行以下操作之一：
 1. 从列表中选择一个缺陷。
 2. 搜索特定缺陷。
4. 复查与选定缺陷有关的网络运行状况度量标准。

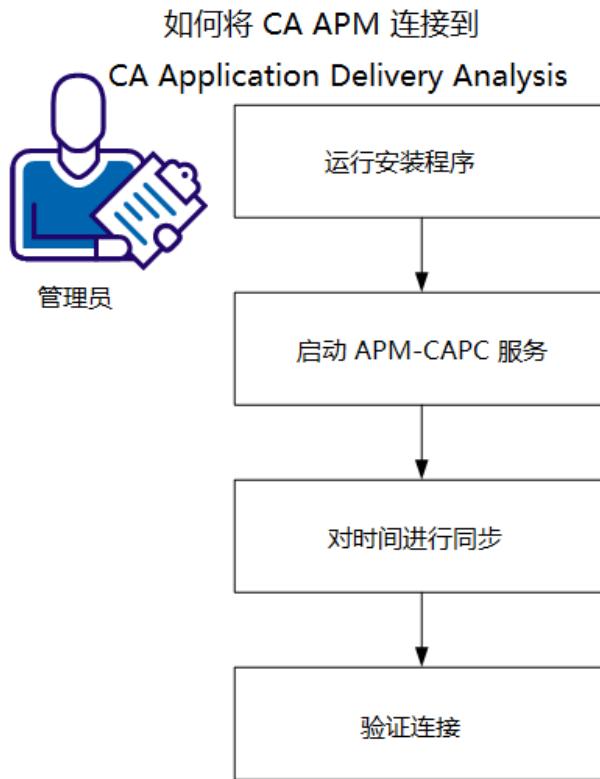
屏幕会显示 CT Observed、DTT、ENRTT、TCP 会话分析等网络度量标准，以及更多信息。“TCP 会话分析”字段中提供了指向多端口监视器的链接。

有关这些度量标准的信息，请参阅 [如何使用 CEM 控制台对应用程序和基础架构问题分类方案](#)。

如何将 CA APM 连接到 Application Delivery Analysis

通过将 CA APM 连接到 CA Application Delivery Analysis (ADA)，可在 APM WebView 上查看基础架构数据。企业管理器定期调用 ADA 管理器上的 Web 服务，以访问这些度量标准，并在 APM WebView 上呈现。企业管理器还将这些度量标准存储在历史报表的 SmartStor 中。

下图描述的是如何以管理员身份将 CA APM 连接到 CA Application Delivery Analysis。



以管理员身份执行下列操作：

1. [运行安装程序](#) (p. 42)。
2. [启动 ADA-APM 服务](#) (p. 45)。
3. [同步时间](#) (p. 45)。
4. [验证连接](#) (p. 46)。

先决条件

在您开始之前，确认您已安装和配置：

- CA Application Delivery Analysis 9.1 或更高版本
- NetQoS Performance Center 6.1/CA Performance Center 2.0
- APM 数据库 9.1 或更高版本
- 企业管理器 9.1 或更高版本
- CA APM Workstation 9.1 或更高版本
- CA APM WebView（可选）

- 下列各项之一：
 - CA APM .NET 代理 9.0 或更高版本
 - CA APM Java 代理 9.0 或更高版本

运行安装程序

CA APM Integration for CA Application Delivery Analysis 安装程序包含两个可安装的组件：“CAPC 集成包”和“适用于 APM 的 CA Application Delivery Analysis 扩展”。本部分介绍如何安装“适用于 APM 的 CA Application Delivery Analysis 扩展”。通过这一可安装组件，可实现 CA Application Delivery Analysis 和 CA APM 之间的通信。

在企业管理器或 MOM（如果具有群集 CA APM 环境）上安装这一可安装组件。

需要以下信息来完成安装：

- 企业管理器主机名
- 企业管理器端口号
- “适用于 APM 的 CA Application Delivery Analysis 扩展”可安装组件所连接的服务器的主机名或 IP 地址

遵循这些步骤：

1. 从 [CA 支持](#) 的 CA APM 软件下载区，下载 CA APM Integration for CA Application Delivery Analysis 安装程序。
2. 导航到 Integration Pack 安装程序的本地版本，并双击此版本。
此时将打开安装程序。
3. 在“欢迎”屏幕上单击“下一步”。
4. 阅读并接受最终用户许可协议。
接受协议以继续。
5. 指定希望集成包文件安装到的位置，然后单击“下一步”。
6. 选择“适用于 APM 的 CA Application Delivery Analysis 扩展”可安装组件。
7. 单击“下一步”。
8. 指定该可安装组件要连接的企业管理器的主机名和端口，然后单击“下一步”。
9. 指定该可安装组件要连接的所有 CA Application Delivery Analysis 控制台的主机名或 IP 地址，然后单击“下一步”。

10. 指定是否将“适用于 APM 的 CA Application Delivery Analysis 扩展”配置为 Windows 服务，然后单击“下一步”。

在 Windows OS 环境中，“适用于 APM 的 CA Application Delivery Analysis 扩展”可安装组件会安装 ADA-APM 服务。

11. 检查您的设置，然后单击“安装”。

CA Application Delivery Analysis 属性文件

安装“适用于 APM 的 CA Application Delivery Analysis 扩展”之后，ADAExtensionForAPM 文件夹会包含 ADAConnector 文件。使用这些文件，您可以验证配置设置，并在必要时更新默认设置。

以下配置设置是“适用于 APM 的 CA Application Delivery Analysis 扩展”可安装组件的一部分，但是您可以使用这些属性来验证和更新这些配置设置：

企业管理器主机名

`com.wily.apm.adaconnector.em.host=<EM host name>`

企业管理器端口号

`com.wily.apm.adaconnector.em.port=<EM port>`

主机名或 IP 地址

该信息反映了“适用于 APM 的 CA Application Delivery Analysis 扩展”可安装组件连接到的所有 ADA 管理器的值

`com.wily.apm.adaconnector.adawssoap_address_source1=<addr>`
`com.wily.apm.adaconnector.ada_hostName1=<host name>`

安装程序的名称

`com.wily.apm.adaconnector.ada_processName1=<ADAExtensionforAPM>`

ADAExtensionforAPM 值代表过程名称，就像在 Workstation 上看到的那样。

ADAConnector 文件使以下配置设置可用：

增强的度量标准

默认情况下会禁用这些基础架构度量标准的查询。如果需要使下列基础架构度量标准在 Workstation 上可用，请启用该查询：

- 数据传输时间
- 网络往返传输时间
- 重新传输延迟

■ 服务器响应时间

示例属性：

```
com.wily.apm.adaconector.ada_enhancedmetrics_enabled2=<true|false>
```

<enabled2> 是 ADA 管理器的一个索引。第一个 ADA 管理器与 <enabled1> 相对应，第二个管理控制台与 <enabled2> 相对应，依此类推。

CA Application Delivery Analysis Web 服务查询

ADA 数据时间 bin 和 Web 服务查询之间的等待时间。默认等待时间为 5 分钟。ADA 管理器可以连接到多个收集器，如多端口监视器和单端口 ADA 收集器。要聚合已收集数据，ADA 时间 bin 的范围为 5 分钟，并在 5 分钟边界处结束，例如 7:00、7:05 等。ADA 管理器每 5 分钟更新一次数据库。该属性中的等待时间值会按指定的时限从精确的 5 分钟边界移动该查询。例如，将等待时间定义为 2 分钟会将 ADA 时间 bin 移动到 7:02、7:07，以此类推。

CA Technologies 建议不更改默认值，除非 CA 支持指示您这样做。

注意：更新该属性不会更改 Web 服务调用频率。每隔 5 分钟会对该频率进行一次修复。

示例属性（以毫秒为单位）：

```
com.wily.apm.adaconector.adawebserice.wait=120000
```

SmartStor 数据馈送时间间隔

从 ADA 到企业管理器的数据馈送时间间隔。

默认时间间隔是 15 秒。CA Technologies 建议不更改默认值，除非 CA 支持指示您这样做。

示例属性（以毫秒为单位）：

```
com.wily.apm.adaconector.smartstorfeed.interval=15000
```

SmartStor 数据馈送等待时间

CA Application Delivery Analysis Web 服务查询与企业管理器开始其数据馈送之间的等待时间。

默认等待时间为 10 秒。CA Technologies 建议不更改默认值，除非 CA 支持指示您这样做。

示例属性（以毫秒为单位）：

```
com.wily.apm.adaconector.smartstorfeed.wait=10000
```

启动 ADA-APM 服务

安装“适用于 APM 的 CA Application Delivery Analysis 扩展”可安装组件之后，启动 ADA-APM 服务。

Windows OS

启动 Windows 服务中的 ADA-APM 服务。

此服务不会自动启动。您可以在安装之后手工启动它。

Linux/UNIX OS

使用以下命令启动“适用于 APM 的 CA Application Delivery Analysis 扩展”：

```
<INSTALL_HOME>\ADAExtensionForAPM$./ADAConector
```

同步时间

将以下计算机之间的时钟同步到某个公用的时间源：

- CA Application Delivery Analysis
- 企业管理器或 MOM

同步时钟有助于确保 NetQoS Performance Center/CA Performance Center 上的 CA APM 应用程序数据和 APM WebView 上的基础架构数据的完整性。如果未执行该任务，组件之间的时间可能会漂移，从而导致数据不准确或丢失。

CA Technologies 建议将整个网络同步到某个网络时间协议时间源或某个时间服务器。如果不可能做到，那么至少必须同步讨论的计算机。

验证连接

查找即用型显示板和特定网络度量标准，以便验证 CA APM 到 CA Application Delivery Analysis 的连接。

遵循这些步骤：

1. 登录到 APM WebView 或 Introscope Workstation。
2. 在控制台上查找“网络状态信息”显示板。
3. 在“调查器”、“度量标准浏览器”选项卡上，查找有关每个客户端子网和服务器的以下信息：
 - 网络运行状况状态
 - 服务器运行状况状态
 - 数据传输时间
 - 网络往返传输时间
 - 重新传输延迟
 - 服务器响应时间

默认情况下，禁用下列度量标准：

- 数据传输时间
- 网络往返传输时间
- 重新传输延迟
- 服务器响应时间

要启用这些度量标准，请使用 ADA 属性文件中的 `com.wily.apm.adaconector.ada_enhancedmetrics_enabled1=<true|false>` 属性。有关此属性文件的信息，请参阅“如何将 CA APM 连接到 Application Delivery Analysis”方案。

从“网络状态信息”显示板，您可以直接导航到 NetQoS Performance Center/CA Performance Center。除了此即用型显示板以外，您还可以使用基础架构度量标准来创建自定义显示板。

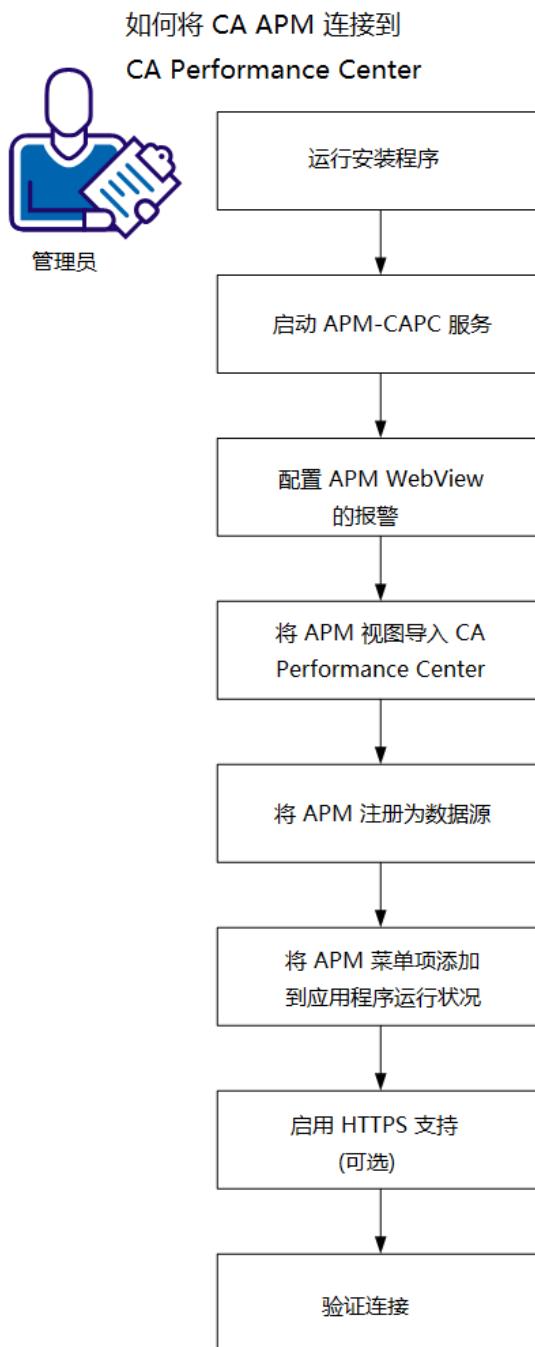
注意：有关创建显示板的详细信息，请参阅《CA APM Workstation 用户指南》。

如何将 CA APM 连接到 CA Performance Center

通过将 CA APM 连接到 CA Performance Center，可在 CA Performance Center 上查看 CA APM 应用程序数据。应用程序数据从企业管理器流到 CA Performance Center。

使用“CAPC 集成包”可安装组件将 CA APM 连接到 CA Performance Center。此可安装组件会安装 APM-CAPC 服务，并采用 CA Performance Center 可理解和显示的格式，提供 CA APM 数据。

下图描述的是如何以管理员身份将 CA APM 连接到 CA Performance Center。



以管理员身份执行下列操作：

1. [运行安装程序 \(p. 49\)](#)。
2. [启动 APM-CAPC 服务 \(p. 51\)](#)。
3. [在 APM WebView 上配置报警 \(p. 51\)](#)。
4. [将 APM 视图导入 CA Performance Center \(p. 52\)](#)。
5. [将 APM 注册为数据源 \(p. 52\)](#)。
6. [将 APM 菜单项添加到应用程序运行状况 \(p. 54\)](#)。
7. [启用 HTTP 支持（可选）\(p. 54\)](#)。
8. [验证连接 \(p. 55\)](#)。

先决条件

在您开始之前，确认您已安装和配置：

- CA Performance Center 2.0.00
- APM 数据库 9.1 或更高版本
- 企业管理器 9.1 或更高版本
- CA APM Workstation 9.1 或更高版本
- CA APM WebView（可选）
- 下列各项之一：
 - CA APM .NET 代理 9.0 或更高版本
 - CA APM Java 代理 9.0 或更高版本
- 有关 APM WebView 或 Workstation 应用程序分类视图元素的报警
- 要监视业务事务、业务服务和业务组件的代理

运行安装程序

CA APM Integration for CA Application Delivery Analysis 安装程序包含两个可安装的组件：“CA Performance Center 集成包”和“适用于 APM 的 CA Application Delivery Analysis 扩展”。本部分介绍如何安装“CA Performance Center 集成包”。通过这一可安装组件，可实现 CA Performance Center 和 CA APM 之间的通信。

在企业管理器或 MOM（如果具有群集 CA APM 环境）上安装这一可安装组件。

需要以下信息来完成安装：

- 企业管理器主机名
- 企业管理器 Web 服务器端口号
- CA APM Workstation 用户名
- CA APM Workstation 密码
- 企业管理器服务用户名和密码
- “CA Performance Center 集成包”可安装组件使用的 Web 服务器端口

遵循这些步骤：

1. 从 [CA 支持](#) 的 CA APM 软件下载区，下载 CA APM Integration for CA Application Delivery Analysis 安装程序。
2. 导航到 Integration Pack 安装程序的本地版本，并双击此版本。
此时将打开安装程序。
3. 在“欢迎”屏幕上单击“下一步”。
4. 阅读并接受最终用户许可协议。
接受协议以继续。
5. 指定希望集成包文件安装到的位置，然后单击“下一步”。
6. 选择“CA Performance Center 集成包”可安装组件。
7. 单击“下一步”。
8. 指定企业管理器主机名和 Web 服务器端口，然后单击“下一步”。
9. 指定企业管理器的 CA Introscope® 和 TESS 帐户，然后单击“下一步”。
10. 指定是否将“CA Performance Center 集成包”配置为 Windows 服务，然后单击“下一步”。
在 Windows OS 环境中，“CA Performance Center 集成包”可安装组件会安装 APM-CAPC 服务。
11. 指定供“CA Performance Center 集成包”使用的 Web 服务器端口，然后单击“下一步”。
12. 检查您的设置，然后单击“安装”。

安装“CA Performance Center 集成包”可安装组件之后，CAPCIIntegrationPack 文件夹将显示在第 5 步指定的目录中。该文件夹包含 webapps 文件夹，webapps 文件夹可提供解压缩的 Jetty Web Server 和 apm-capc-integration 文件夹。

启动 APM-CAPC 服务

安装“CA Performance Center 集成包”之后，启动 APM-CAPC 服务。

Windows OS

启动 Windows 服务中的 APM-CAPC 服务。

此服务不会自动启动。您可以在安装之后手工启动它。

Linux/UNIX OS

使用以下命令启动“CA Performance Center 集成包”：

```
<INSTALL_HOME>\CAPCIntegrationPack\bin$./jetty.sh start
```

在 APM WebView 上配置报警

使用 APM WebView 上的报警，可设置度量标准的阈值，并在度量标准超出阈值时执行操作。应用程序分类视图中的许多对象可以显示报警。这些报警反映那些对象的任何基准度量标准的最坏情况状态。

创建报警以使应用程序、业务服务和业务事务运行状况指示器在 CA Performance Center 上可用。

遵循这些步骤：

1. 在 WebView 中，依次单击“调查器”和“分类视图”。
2. 在树中导航到要编辑的报警，例如：
按前端|*Application_Name*|后端调用|file%customer-records
3. 右键单击组件，并从关联菜单中选择“编辑名称的报警”。
将显示“编辑名称的报警”对话框。
4. 在左侧窗格中，选择您希望构成报警状态的度量标准。
5. 从“问题”下拉列表中选择您想要触发报警的问题的类型：

值过高

度量标准值超过阈值时触发报警。

值过低

度量标准值下降到阈值以下时触发报警。

特定的错误值

度量标准值等于阈值时触发报警。然后，该阈值被视为错误值而不是阈值。

意外值

度量标准值不等于阈值时触发报警。然后，该值被视为期望值而不是阈值。

6. 单击“摘要度量标准”选项卡。为危险和警告报警设置阈值和敏感级别，然后单击“应用”。

危险

度量标准值超过阈值时触发报警。报警以红色显示。

警告

度量标准值接近阈值时触发报警。报警以黄色显示。

7. 单击“应用”。
8. 为每个度量标准重复第 4 步到第 7 步。
9. 单击“确定”。

将 APM 视图导入 NetQoS Performance Center

复制集成 XML 文件，并将 APM 视图定义导入 CA Performance Center 数据库。

遵循这些步骤：

1. 导航到以下位置：
`<CAPC Integration Pack Home>\CAPCIntegrationPack\CAPC_2_0`
2. 将 `apm` 目录从 `CAPC_2_0` 文件夹复制到以下位置的 `plugins` 文件夹：
`<CAPC-HOME>/PerformanceCenter/SQL/plugins`
3. 在命令提示符下，执行以下命令以将视图导入 CA Performance Center 数据库：
`<CAPC-HOME>/PerformanceCenter/Tools/bin/npcshell.sh dbmigrate - package com.ca.im.plugin.apm - path <CAPC-HOME>/PerformanceCenter/SQL/plugins/apm`

将 APM 注册为数据源

CA Performance Center 只能接收来自已注册数据源的信息。

遵循这些步骤：

1. 以具有管理权限的用户身份登录到 CA Performance Center。
2. 选择“管理”、“设置”，然后单击“数据源”。

此时将显示“数据源列表”页面。

3. 单击“添加”。

此时将显示“添加数据源”页面。

4. 从“源类型”列表中选择“应用程序性能管理”。

注意: “源类型”列表显示可以注册为 CA Performance Center 数据源的所有 CA Technologies 产品，包括未在环境中安装的产品和一些第三方集成。仅在完成需要的配置之后，才会列出来自其他公司的受支持数据源。应用程序性能管理数据源支持单个启用的数据源的定义。如果要添加其他数据源，请删除现有数据源。

5. 输入数据源的主机名。

该主机名是安装该数据源的数据库的服务器的 IP 地址或 DNS 主机名。对于 CA APM 数据源，输入安装了“CA Performance Center 集成包”安装程序的主机的 IP 地址。

6. 选择要用于联系数据源的协议。CA APM 数据源的默认协议为 HTTP。

如果您的网络使用 SSL 进行通信，请选择 https。确认在选择 https 选项之前已正确配置系统。

注意: 如果计划将 SSL 用于 CA Performance Center 与数据源产品之间的通信，请参阅《CA 单点登录指南》。特定于 CA APM 数据源的是，如果在此处选择 https 选项，则还必须支持企业管理器与集成 Web 服务之间的 SSL 通信。

7. 提供联系数据源时要使用的端口。端口取决于在上一步骤中选择的协议。对于应用程序性能管理器数据源，默认端口为 8082。

注意: 如果计划将 SSL 用于 CA Performance Center 和数据源产品之间的通信，请参阅《单点登录指南》以了解更多信息。

8. 为数据源输入一个显示名称。默认情况下，会将数据源类型和主机名组合在一起以创建数据源的名称。

示例: <datasourcename>@<hostname>

注意: Web 控制台地址不适用于 CA APM。

9. 如果已完成数据源注册，请单击“保存”。

CA Performance Center 列出了已经在“数据源列表”中注册的数据源。

将 APM 菜单项添加到应用程序运行状况

在 CA Performance Center 中，将以下 CA APM 显示板菜单项添加到“应用程序运行状况”菜单中：

- APM—应用程序状态
- APM—业务服务状态

可以为默认承租人或任何现有承租人添加菜单项。在为现有承租人设置菜单后，新承租人可以自动访问菜单，而无需这些步骤。

遵循这些步骤：

1. 以具有默认承租人或其他承租人管理员帐户的管理员身份登录。
2. 选择“管理”、“用户设置”，然后单击“菜单”。
“管理菜单”页面将显示当前的菜单列表。
3. 选择“应用程序运行状况”，然后单击“编辑”。
4. 在“可用”列表中，选择“APM – 应用程序摘要”和/或“APM – 业务服务摘要”显示板。要选择多个显示板，请按住 Shift 键并单击。
5. 单击向右箭头。
6. 显示板将移动到“选定”列表。
7. 单击“保存”。

菜单项已设置。

启用 HTTPS 支持（可选）

为了提高安全性，您可以使用安全套接字层 (SSL) 启用 HTTPS 协议，此协议支持 CA APM 和 CA Performance Center 之间的通信，如下所示：

- 获取服务器证书。为了提高安全性，某些管理员也可以选择使用客户端证书。将 IIS 中的网站配置为使用 SSL、服务器证书和客户端证书超出了本文档的讨论范围。但是，下面的 Microsoft 文章对这些 IIS 网站安全功能的使用进行了深入的讨论。

SSL and Certificates (IIS 6.0) (SSL 和证书 (IIS 6.0)) :

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/559bb9d5-0515-4397-83e0-c403c5ed86fe.mspx?mfr=true>

- 将 CA APM 数据源 (p. 52) 配置为包含 HTTPS 支持，以支持 CA Performance Center 和“CAPC 集成包”之间的 HTTPS 通信。
- 编辑 *apm-capc-integration.properties* 文件 (p. 55) 以支持企业管理器与 CAPC 集成包可安装组件之间的 HTTPS 通信。

编辑 `apm-capc-integration.properties` 文件

编辑 `apm-capc-integration.properties` 文件可支持企业管理器与 CAPC 集成包可安装组件之间的 HTTPS 通信。

遵循这些步骤：

1. 在文本编辑器中从以下位置打开 `apm-capc-integration.properties` 文件：
`<INSTALLATION_HOME>\CAPCIntegrationPack\resources`
2. 找到 `com.apm.npc.em.transport.protocol` 属性，并指定值 `<https>`。
3. 找到 `javax.net.ssl.keyStore` 属性，并指定值 `<KEYSTORE LOCATION FOR SSL CONNECTION>`。
4. 找到 `javax.net.ssl.keyStorePassword` 属性，并指定值 `<KEYSTORE PASSWORD FOR SSL CONNECTION>`。
5. 找到 `javax.net.ssl.trustStore` 属性，并指定值 `<TRUSTSTORE LOCATION>`。
6. 找到 `javax.net.ssl.trustStorePassword` 属性，并指定值 `<TRUSTSTORE PASSWORD>`。

属性已设置。

验证连接

CA Performance Center 在选定的时间段内以深入的方式显示应用程序运行状况和性能状态数据。CA APM 注册为 CA Performance Center 上的数据源时，您可以访问“应用程序摘要”报告或“业务服务摘要”报告中的应用程序数据。从这些报告中，可以深入查看事件和缺陷。

查找即用型报告中的数据，以便确认 CA APM 连接到 CA Performance Center。

遵循这些步骤：

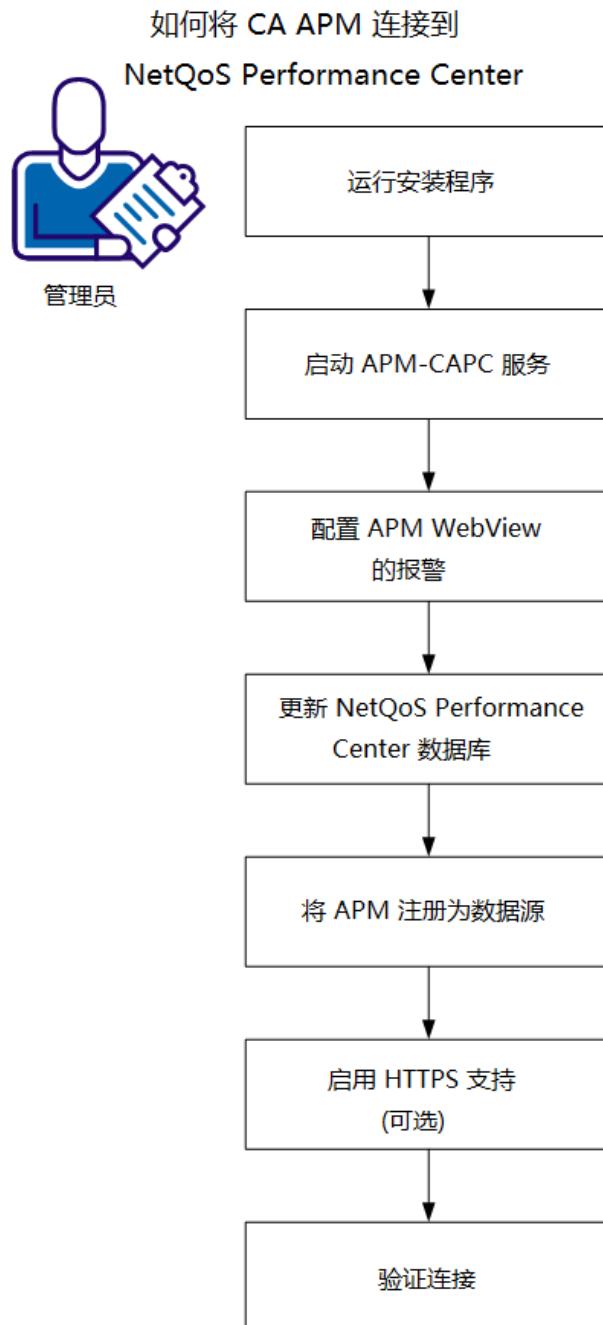
1. 登录到 CA Performance Center。
2. 在 CA Performance Center“报告”菜单中，可看到以下与 CA APM 相关的报告：
 - APM--应用程序摘要
 - APM--业务服务摘要
3. “应用程序摘要”报告中显示业务应用程序的运行状态。
4. “业务服务摘要”报告中显示选定应用程序的业务服务运行状态。

如何将 CA APM 连接到 NetQoS Performance Center

通过将 CA APM 连接到 NetQoS Performance Center (NPC)，可在 NPC 上查看 CA APM 应用程序数据。

使用“CAPC 集成包”可安装组件将 CA APM 连接到 NPC。此可安装组件会安装 APM-CAPC 服务，并采用 NPC 可理解和显示的格式，提供 CA APM 数据。

下图描述的是如何以管理员身份将 CA APM 连接到 NPC。



以管理员身份执行下列操作：

1. [运行安装程序 \(p. 58\)](#)。
2. [启动 APM-CAPC 服务 \(p. 51\)](#)。
3. [在 APM WebView 上配置报警 \(p. 60\)](#)。
4. [更新 NetQoS Performance Center 数据库 \(p. 61\)](#)。
5. [将 APM 注册为数据源 \(p. 62\)](#)。
6. [启用 HTTP 支持（可选）\(p. 63\)](#)。
7. [验证连接 \(p. 64\)](#)。

先决条件

在您开始之前，确认您已安装和配置：

- NetQoS Performance Center 6.1 或更高版本
- APM 数据库 9.1 或更高版本
- 企业管理器 9.1 或更高版本
- CA APM Workstation 9.1 或更高版本
- CA APM WebView（可选）
- 下列各项之一：
 - CA APM .NET 代理 9.0 或更高版本
 - CA APM Java 代理 9.0 或更高版本
- 有关 APM WebView 或 Workstation 应用程序分类视图元素的报警
- 要监视业务事务、业务服务和业务组件的代理

运行安装程序

CA APM Integration for CA Application Delivery Analysis 包含两个可安装的组件：“CA Performance Center 集成包”和“适用于 APM 的 CA Application Delivery Analysis 扩展”。本部分介绍如何安装“CA Performance Center 集成包”。通过这一可安装组件，可实现 NetQoS Performance Center 和 CA APM 之间的通信。

在企业管理器或 MOM（如果具有群集 CA APM 环境）上安装这一可安装组件。

需要以下信息来完成安装：

- 企业管理器主机名
- 企业管理器 Web 服务器端口号
- CA APM WebView 或 Workstation 用户名
- CA APM WebView 或 Workstation 密码
- 企业管理器服务用户名和密码
- “CAPC 集成包”可安装组件使用的 Web 服务器端口

遵循这些步骤：

1. 从 [CA 支持](#) 的 CA APM 软件下载区，下载 CA APM Integration for CA Application Delivery Analysis 安装程序。
2. 导航到 Integration Pack 安装程序的本地版本，并双击此版本。
此时将打开安装程序。
3. 在“欢迎”屏幕上单击“下一步”。
4. 阅读并接受最终用户许可协议。
接受协议以继续。
5. 指定希望集成包文件安装到的位置，然后单击“下一步”。
6. 选择“CA Performance Center 集成包”可安装组件。
7. 单击“下一步”。
8. 指定企业管理器主机名和 Web 服务器端口，然后单击“下一步”。
9. 指定企业管理器的 CA Introscope® 和 TESS 帐户，然后单击“下一步”。
10. 指定是否将“CA Performance Center 集成包”配置为 Windows 服务，然后单击“下一步”。
在 Windows OS 环境中，“CA Performance Center 集成包”可安装组件会安装 APM-CAPC 服务。
11. 指定供“CA Performance Center 集成包”使用的 Web 服务器端口，然后单击“下一步”。
12. 检查您的设置，然后单击“安装”。

安装“CA Performance Center 集成包”可安装组件之后，
CAPCIIntegrationPack 文件夹将显示在第 5 步指定的目录中。该文件夹包含 webapps 文件夹，webapps 文件夹可提供解压缩的 Jetty Web Server 和 apm-capc-integration 文件夹。

启动 APM-CAPC 服务

安装“CA Performance Center 集成包”之后，启动 APM-CAPC 服务。

Windows OS

启动 Windows 服务中的 APM-CAPC 服务。

此服务不会自动启动。您可以在安装之后手工启动它。

Linux/UNIX OS

使用以下命令启动“CA Performance Center 集成包”：

```
<INSTALL_HOME>\CAPCIntegrationPack\bin$./jetty.sh start
```

在 APM WebView 上配置报警

使用 Workstation 上的报警，可设置度量标准的阈值，并在度量标准超出阈值时执行操作。应用程序分类视图中的许多对象可以显示报警。这些报警反映那些对象的任何基准度量标准的最坏情况状态。

创建报警以使应用程序、业务服务和业务事务运行状况指示器在 NetQoS Performance Center 上可用。

遵循这些步骤：

1. 在 WebView 中，依次单击“调查器”和“分类视图”。
2. 在树中导航到要编辑的报警，例如：
按前端|*Application_Name*|后端调用|file%customer-records
3. 右键单击组件，并从关联菜单中选择“编辑名称的报警”。
将显示“编辑名称的报警”对话框。
4. 在左侧窗格中，选择您希望构成报警状态的度量标准。
5. 从“问题”下拉列表中选择您想要触发报警的问题的类型：

值过高

度量标准值超过阈值时触发报警。

值过低

度量标准值下降到阈值以下时触发报警。

特定的错误值

度量标准值等于阈值时触发报警。然后，该阈值被视为错误值而不是阈值。

意外值

度量标准值不等于阈值时触发报警。然后，该值被视为期望值而不是阈值。

6. 单击“摘要度量标准”选项卡。为危险和警告报警设置阈值和敏感级别，然后单击“应用”。

危险

度量标准值超过阈值时触发报警。报警以红色显示。

警告

度量标准值接近阈值时触发报警。报警以黄色显示。

7. 单击“应用”。
8. 为每个度量标准重复第 4 步到第 7 步。
9. 单击“确定”。

更新 NetQoS Performance Center 数据库

该任务使用 `apm_integration.sql` 脚本更新 NetQoS Performance Center 数据库。该脚本将 CA APM 数据源添加到可用数据源列表中。另外，该脚本会将其他 CA APM 特定信息添加到数据库中，在 NetQoS Performance Center 上显示应用程序数据需要这些信息。

运行 SQL 脚本：

1. 将 `apm_integration.sql` 文件从 CAPCIIntegrationPack 文件夹复制到 NetQoS Performance Center 计算机。

该文件夹是在安装 CA APM Integration Pack for CA Application Delivery Analysis 安装程序时创建的。

2. 打开 Windows 命令提示符。
3. 执行：`cd <location of the apm_integration.sql>`
4. 执行：`mysql`
5. 执行：`source <path>\apm_integration.sql`

将更新 NetQoS Performance Center 数据库。

将 CA APM 注册为数据源

NetQoS Performance Center 只能接收来自已注册数据源的数据。

注意: 有关管理数据源和单个 NetQoS Performance Center 实例可以支持的数据源数量的详细信息, 请参阅《CA Performance Center 管理员和用户指南》。

遵循这些步骤:

1. 以具有管理权限的用户身份登录到 NetQoS Performance Center。
2. 选择“管理”、“CA 设置”, 然后单击“数据源”。
此时将打开“数据源列表”页面。
3. 单击“新建”。
此时将打开“添加新数据源”页面。
4. 选择需要从“源类型”列表添加的数据源的类型。

注意: “源类型”列表显示可以注册为 NetQoS Performance Center 数据源的所有 CA Technologies 产品, 包括那些未在环境中安装的产品和一些第三方集成。仅在完成需要的配置之后, 才会列出来自其他公司的受支持数据源。如果未列出某个数据源类型, 请检查以确认是否已为该类型注册了最大数量的数据源。

5. 输入数据源的主机名。
该主机名是安装该数据源的数据库的服务器的 IP 地址或 DNS 主机名。对于 CA APM 数据源, 输入安装了“CAPC 集成包”可安装组件的主机的 IP 地址。
6. 选择要用于联系数据源的协议。CA APM 数据源的默认协议为 HTTP。
如果您的网络使用 SSL 进行通信, 请选择 https。确认在选择 https 选项之前已正确配置系统。

注意: 如果计划将 SSL 用于 NetQoS Performance Center 与数据源产品之间的通信, 请参阅《CA 单点登录指南》。CA APM 数据源的特殊之处在于, 如果选择 https 选项, 还必须在企业管理器与集成 Web 服务之间支持 SSL (p. 63) 通信。

7. 提供联系数据源时要使用的端口。端口号取决于您在上一步骤中选择的协议。默认 CA APM 端口为 8082。
如果计划将 SSL 用于 NetQoS Performance Center 和数据源产品之间的通信, 请参阅《单点登录指南》以了解更多信息。
8. 确认 Web 控制台地址。如果该地址与主机名不同, 请清除“同上”复选框, 并提供 Web 控制台信息:

9. (可选) 为数据源输入一个显示名称。

默认情况下，会将数据源类型和主机名组合在一起以创建数据源的名称。可以在此处提供另一个名称。

例如，可以将数据源命名为 *APM_SantaFe*，而不是 *APM@xxx.x.x.xx*。

10. 如果已完成数据源注册，请单击“保存”。

NetQoS Performance Center 列出了已经在“数据源列表”中注册的数据源。

启用 HTTPS 支持 (可选)

您可以使用安全套接字层 (SSL) 启用 HTTPS 协议，提高安全性。要使用安全套接字层 (SSL) 在 CA APM 和 NetQoS Performance Center 之间进行通信，请执行以下操作：

- 获取服务器证书。为了提高安全性，某些管理员也可能会选择使用客户端证书。将 IIS 中的网站配置为使用 SSL、服务器证书和客户端证书超出了本文档的讨论范围。但是，下面的 Microsoft 文章对这些 IIS 网站安全功能的使用进行了深入的讨论。

SSL and Certificates (IIS 6.0) (SSL 和证书 (IIS 6.0)) :

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/559bb9d5-0515-4397-83e0-c403c5ed86fe.mspx?mfr=true>

- 将 CA APM 数据源 (p. 62) 配置为包含 HTTPS 支持，以支持 NetQoS Performance Center 与 NetQoS Performance Center Integration Pack 之间的 HTTPS 通信。
- 编辑 *apm-capc-integration.properties* 文件 (p. 55) 以支持企业管理器与 CAPC 集成包可安装组件之间的 HTTPS 通信。

编辑 *apm-capc-integration.properties* 文件

编辑 *apm-capc-integration.properties* 文件可支持企业管理器与 CAPC 集成包可安装组件之间的 HTTPS 通信。

遵循这些步骤：

1. 在文本编辑器中从以下位置打开 *apm-capc-integration.properties* 文件：
`<INSTALLATION_HOME>\CAPCIntegrationPack\resources`
2. 找到 `com.apm.npc.em.transport.protocol` 属性，并指定值 `<https>`。
3. 找到 `javax.net.ssl.keyStore` 属性，并指定值 `<KEYSTORE LOCATION FOR SSL CONNECTION>`。

4. 找到 javax.net.ssl.keyStorePassword 属性，并指定值 <KEYSTORE PASSWORD FOR SSL CONNECTION>。
5. 找到 javax.net.ssl.trustStore 属性，并指定值 <TRUSTSTORE LOCATION>。
6. 找到 javax.net.ssl.trustStorePassword 属性，并指定值 <TRUSTSTORE PASSWORD>。
属性已设置。

验证连接

NetQoS Performance Center 在选定的时间段内以深入查看的方式显示应用程序运行状况和性能状态数据。CA APM 注册为 NetQoS Performance Center 上的数据源时，可以访问“应用程序摘要”报表或“业务服务摘要”报表中的应用程序数据。从这些报告中，可以深入查看事件和缺陷。

查找即用型报告中的数据，以便确认 CA APM 连接到 NetQoS Performance Center。

遵循这些步骤：

1. 登录到 NetQoS Performance Center。
2. NetQoS Performance Center“报告”菜单中应显示下列与 CA APM 相关的报告：
 - APM--应用程序摘要
 - APM--业务服务摘要
3. “应用程序摘要”报告中显示业务应用程序的运行状态。
4. “业务服务摘要”报告中显示选定应用程序的业务服务运行状态。

第4章：分类方案

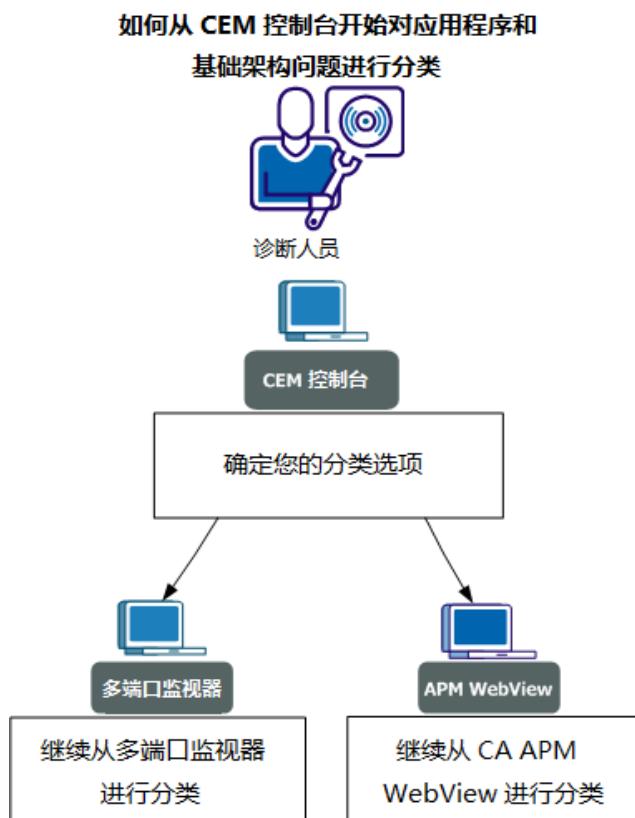
此部分包含以下主题：

- [如何使用 CEM 控制台对应用程序和基础架构问题进行分类 \(p. 65\)](#)
- [如何使用 APM WebView 对应用程序和基础架构问题进行分类 \(p. 70\)](#)
- [如何使用 NPC 对应用程序问题进行分类 \(p. 80\)](#)

如何使用 CEM 控制台对应用程序和基础架构问题进行分类

CEM 控制台上的网络数据为诊断人员提供与受监视的应用程序相关的高级别网络性能信息。然后，您可以确定网络问题是否为促成被分类问题的因素，并深入查看多端口监视器以了解会话级别数据。如果度量标准表明网络没有问题，则可以连接到 APM WebView 对应用程序进行调查和分类。

下图显示可能的分类方案。



作为诊断人员，请执行下列操作：

1. [确定分类选项 \(p. 66\)](#)。
2. [继续使用多端口监视器进行分类 \(p. 69\)](#)。
3. [继续使用 APM WebView 进行分类 \(p. 70\)](#)。

确定分类方案。

发现与应用程序有关的基础架构问题时，确定一些分类方案能够为您的后续操作提供指导。

遵循这些步骤：

1. 登录到 CEM 控制台。
2. 依次选择“CEM”、“突发事件管理”、“缺陷”。
3. 执行以下操作之一：
 1. 从列表中选择一个缺陷。
 2. 搜索特定缺陷。
4. 复查与选定缺陷有关的网络运行状况度量标准。

如果发现高网络往返传输时间或包丢失，您可能会选择连接到多端口监视器。在这里，您可以更详细地调查网络基础架构。

有关网络运行状况度量标准的详细信息，请参阅[“缺陷详细信息”页面上的网络度量标准 \(p. 66\)](#)。

“缺陷详细信息”页面上的网络度量标准

CEM 识别缺陷后，会在多端口监视器中查询会话级 TCP 信息并将其保存在缺陷详细信息中。挖掘到缺陷后，此 TCP 信息会在 CEM 控制台显示。

每个字段均显示 Web 服务器和客户端 IP 之间的应用程序在缺陷时间之前 15 分钟的所有 TCP 会话的平均值。使用“TCP 会话分析”字段上的链接可查看各个 TCP 会话的度量标准。

“缺陷详细信息”页面上显示以下网络信息：

观测到的 NCT

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

DTT

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

ENRTT

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

NCT

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

NRTT

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

观测到的 NRTT

网络往返传输时间观测。选定的时间间隔期间网络上的服务器和客户端之间的往返传输次数。它可以更好地体现使用率级别，以及衡量度量标准的重要性。例如，大量观测表明事件可能会影响许多用户。

重新传输

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

SCT

服务器连接时间。从服务器接收来自客户端的 SYN 数据包到服务器发送第一个 SYN/ACK 数据包的时间。

打开 TCP 连接涉及交换以下三个数据包：SYN、SYN/ACK 和 ACK。TCP 标头具有 SYN（同步）和 ACK（确认）位。第一个数据包设置了 SYN 位。第二个数据包设置了这两个位。第三个数据包只设置了 ACK 位。此交换可建立连接的初始序号。

SCT 和 NCT 都包含“连接设置时间”度量标准。有关详细信息，请参阅“ADA 会话”报告。

SRT

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

TCP 字节

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

TCP 字节，从

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

TCP 字节损失百分比

数据丢失，表示为发送和接收的 TCP 字节百分比。

TCP 字节速率

TCP 数据量（以字节为单位）。选定时间段的数据速率（以每秒字节数为单位）。

TCP 字节速率，从

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

重新传输的 TCP 字节速率

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

TCP 会话分析

“分析”选项卡上指向多端口监视器 TCP 会话报表的链接。与多端口监视器有关的客户端网络信息与 CEM 控制台请求的会话的客户端网络 ID 相对应。TCP 会话报表的初始视图按“事务处理时间”进行排序。通过该报告，可以访问“服务器/客户端对”视图，以便查看与给定服务器通信的客户端 IP 地址所属相同子网的所有客户端。

数据包丢失百分比

数据丢失，表示为发送和接收的 TCP 数据包百分比。

TCP 数据包速率

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

TCP 数据包速率，从

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

重新传输的 TCP 数据包速率

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

TCP 数据包

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

重新传输的 TCP 字节数

因数据丢失而重新传输的 TCP 字节数。

重新传输的 TCP 数据包数

因数据丢失而重新传输的 TCP 数据包数。

事务处理时间

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

观测到的事务处理时间

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

继续使用多端口监视器进行分类

如果缺陷的网络度量标准表明网络/服务器性能下降（例如高网络往返传输时间或包丢失），可选的一种方案是通过“TCP 会话分析”链接连接到多端口监视器。在多端口监视器中，您可以更详细地调查网络基础架构。执行以下操作之一访问多端口监视器。

遵循这些步骤:

1. 在 CEM 的“缺陷详细信息”页中，选择与“TCP 会话分析”字段有关的链接。

此链接会将您带至多端口监视器的 TCP 会话报告。TCP 会话报表的初始视图按“事务处理时间”进行排序。通过该报告，可以访问“服务器/客户端对”视图，以便查看与给定服务器通信的客户端 IP 地址所属相同子网的所有客户端。

有关详细信息，请参阅《[多端口监视器用户指南](#)》。

遵循这些步骤:

1. 登录到多端口监视器。
2. 选择“分析”选项卡。
3. 导航到相关的 TCP 会话报告。

有关详细信息，请参阅《[多端口监视器用户指南](#)》。

继续使用 APM WebView 进行分类

如果缺陷的网络度量标准在业务的预期范围之内，可选的一种方案是继续使用 APM WebView 进行分类。

遵循这些步骤:

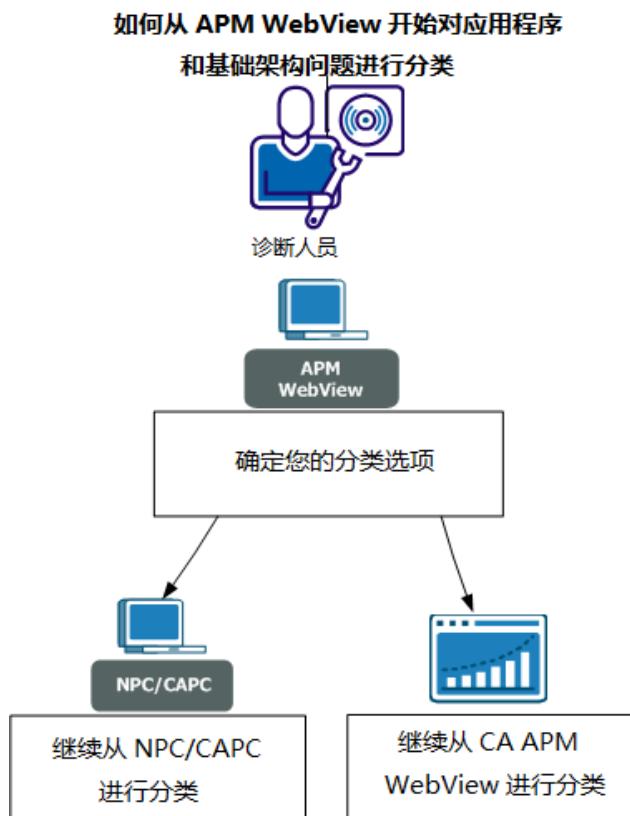
1. 登录到 APM WebView。
2. 使用控制台或调查器对问题分类。

如何使用 APM WebView 对应用程序和基础架构问题进行分类

使用 APM WebView 上的基础架构数据，支持工程师可执行以下操作：

- 查看高级别客户端网络和服务器运行状况状态，然后确定是否需要对基础架构立即进行深入调查。
- 如果需要，您可以直接连接到 NetQoS Performance Center (NPC)/CA Performance Center (CAPC) 以调查特定客户端网络或服务器。
- 如果基础架构数据表明性能在可接受的范围内，但应用程序的性能仍在降低，可使用 APM WebView 进一步调查应用程序

下图显示可能的分类方案。



作为诊断人员，请执行下列操作：

1. [确定分类选项](#) (p. 71)。
2. [继续使用 NPC/CAPC 进行分类](#) (p. 78)。
3. [继续使用 APM WebView 进行分类](#) (p. 77)。

确定分类方案。

发现与应用程序有关的基础架构问题时，确定一些分类方案能够为您的后续操作提供指导。

遵循这些步骤：

1. 登录到 APM WebView。

2. 导航到以下其中一个显示板或概览页：

1. 从“控制台”、“显示板”下拉列表中选择“网络状态信息”显示板。

根据客户端子网和服务器的运行状况状态，确定后续的操作。例如，如果关键客户端网络或服务器运行不正常，可选择关联“更多信息”按钮，访问 NetQoS Performance Center (NPC)/CA Performance Center (CAPC) 中的客户端子网/服务器概览报告。

“更多信息”按钮要求一次性完成配置。使用 APM Workstation 配置这些按钮。请参阅[在“网络状态信息”显示板上配置“更多信息”\(p. 74\)](#)。

有关此显示板的详细信息，请参阅[“网络状态信息”显示板 \(p. 73\)](#)。

2. 导航到您正在监控的所有网络/服务器的概览数据：“调查器”、“度量标准浏览器”选项卡、“网络”或“服务器”节点、“概览”选项卡。

根据每个客户端子网/服务器的运行状况状态，确定后续的操作。例如，如果关键客户端子网或服务器的运行状况状态为 2(降级)，您可以登录到 NPC/CAPC 以获得更多详细信息。

有关运行状况状态的详细信息，请参阅[概览—所有网络/服务器 \(p. 75\)](#)。

3. 导航到您正在监控的特定客户子网/服务器的概述数据：“调查器”、“度量标准浏览器”选项卡、“网络”或“服务器”节点、客户端子网或特定服务器、“概览”选项卡。

根据运行状况状态信息或其他度量标准，确定是否需要进一步调查客户端子网或服务器。例如，如果数据表明托管问题应用程序的服务器能够按照预期的方式运行，那么您可以选择使用 APM WebView 更详细地调查应用程序。

默认情况下，禁用下列度量标准：

- 数据传输时间
- 网络往返传输时间
- 重新传输延迟
- 服务器响应时间

要启用这些度量标准，请使用 ADA 属性文件中的 `com.wily.apm.adaconnector.ada_enhancedmetrics_enabled1=<true/false>` 属性。有关此属性文件的信息，请参阅[“如何将 CA APM 连接到 Application Delivery Analysis”方案](#)。

有关此概览数据的详细信息，请参阅[概览—特定网络/服务器 \(p. 76\)](#)。

“网络状态信息”显示板

可从 WebView 控制台访问“网络状态信息”显示板。其显示 10 个性能最差的客户端子网和服务器，并显示相关的运行状况。关键客户端网络或服务器是否运行不正常将一目了然，并且您可链接到 NetQoS Performance Center (NPC)/CA Performance Center (CAPC) 以获取更多信息。使用 APM Workstation 配置“更多信息”按钮之后，双击这些按钮可转到 NPC/CAPC 中的客户端子网/服务器概览报告。每个按钮均需要一次性配置。

Y 轴表示：

由 CA Application Delivery Analysis 计算的指定时限的每个客户端子网/服务器的运行状况（默认视图为实时数据）。企业管理器/MOM 接受 CA Application Delivery Analysis 运行状况数据，并在 Workstation 中显示相应的数值。有关两个系统之间的数据映像的信息，请参阅下表。

CA Application Delivery Analysis 状态	WebView 状态值
不可用	4
过度使用	3
已降级	2
正常	1
未分级	0
无	-1(相应的客户端子网/服务器没有向企业管理器报告)

有关配置“更多信息”按钮的详细信息，请参阅

[配置“网络状态信息”显示板上的“更多信息” \(p. 74\)](#)

有关 **Application Delivery Analysis** 如何计算网络和服务器运行状况的信息，请参阅

[ADA 如何计算网络和服务器运行状况 \(p. 79\)](#)

配置“网络状态信息”显示板上的“更多信息”

通过“更多信息”按钮可转到 NetQoS Performance Center (NPC)/CA Performance Center (CAPC)，具体是指“网络概览”和“服务器概览”报告。这些报表的链接需要对每个按钮进行一次性配置。在 APM Workstation 上配置这些按钮。

遵循这些步骤：

1. 登录到 APM Workstation
2. 在“Workstation 控制台”窗口上，选择“显示板”和“编辑显示板”。
此时将显示“网络状态信息”显示板的“编辑器”的视图。
3. 右键单击“更多信息”按钮，并选择“取消分组”。
4. 直接右键单击“更多信息”文本并选择“对象链接...”
此时将显示“对象链接”窗口。
5. 单击“编辑”。
此时将打开“编辑对象链接”窗口。
6. 确认已选中“Web 链接”单选按钮。
7. 在“URL”文本框中，将 <主机名> 替换为 NPC/CAPC 服务器的名称。
注意： URL 默认访问 NPC。要访问 CAPC，请更改默认值，以便其中包含您的 CAPC 端口号（通常为 8181）和新地址。
要访问 CAPC 中的其他网络信息，请将
`http://<hostname>/npc/default.aspx?pg=6001&mn=6001`
替换为
`http://<hostname>:CA Portal/pc/desktop/?pg=2000009&mn=3`
要访问 CAPC 中的其他服务器信息，请将
`http://<hostname>/npc/default.aspx?pg=7006&mn=6003`
替换为
`http://<hostname>:CA Portal/pc/desktop/?pg=2000010&mn=3`
8. 在“编辑对象链接”和“对象链接”窗口上单击“确定”
9. 在报告的“编辑器”视图上，依次选择“文件”、“保存”。
10. 关闭“编辑器”视图。
您和“网络状态信息”显示板的所有随后用户现在即可直接访问 NPC/CAPC 中关联的概览报告。

概览—所有网络/服务器

与正在监控的所有网络/服务器关联的概览数据可从 APM WebView、“调查器”、“度量标准浏览器”选项卡、“网络”或“服务器”节点、“概览”选项卡进行访问。“概览”页面显示以下信息，且默认情况下按“状态”度量标准值的降序排序：

网络/服务器名称

显示在树层次结构中的网络/服务器的名称。

状态

由 CA Application Delivery Analysis 计算的指定时限的每个客户端子网/服务器的运行状况（默认视图为实时数据）。企业管理器/MOM 接受 CA Application Delivery Analysis 运行状况数据，并在 Workstation 中显示相应的数值。有关两个系统之间的数据映像的信息，请参阅下表。

CA Application Delivery Analysis 状态	WebView 状态值
不可用	4
过度使用	3
已降级	2
正常	1
未分级	0
无	-1(相应的客户端子网/服务器没有向企业管理器报告)

已为两个“状态”度量标准值定义默认阈值。“警告”与状态值 2 相对应。“危险”与状态值 3 相对应。度量标准值超过警告阈值时，“状态”单元格的背景色会显示黄色。超过危险阈值时，“状态”单元格的背景色会显示红色。您可以通过编辑 ADAExtensionforAPM.tv.xml 文件来自定义这些阈值。该文件位于 CA Application Delivery Analysis Extension for APM 安装程序的 <EM_HOME>\ext\xmltv 文件夹中。

有关 **Application Delivery Analysis** 如何计算网络和服务器运行状况的信息，请参阅

[ADA 如何计算网络和服务器运行状况 \(p. 79\)](#)

概览—每个网络/服务器

此“概览”页面显示与客户端子网或特定服务器关联的数据。此信息可从 APM WebView、“调查器”、“度量标准浏览器”选项卡、“网络”或“服务器”节点，客户端子网或特定服务器、“概览”选项卡进行访问。

默认情况下，禁用下列度量标准：

- 数据传输时间
- 网络往返传输时间
- 重新传输延迟
- 服务器响应时间

要启用这些度量标准，请使用 ADA 属性文件中的 `com.wily.apm.adaconnector.ada_enhancedmetrics_enabled1=<true/false>` 属性。有关此属性文件的信息，请参阅“如何将 CA APM 连接到 Application Delivery Analysis”方案。

“概览”页面显示以下信息：

状态

由 CA Application Delivery Analysis 计算的指定时限的每个客户端子网/服务器的运行状况（默认视图为实时数据）。企业管理器/MOM 接受 CA Application Delivery Analysis 运行状况数据，并在 Workstation 中显示相应的数值。有关两个系统之间的数据映像的信息，请参阅下表。

CA Application Delivery Analysis 状态	WebView 状态值
不可用	4
过度使用	3
已降级	2
正常	1
未分级	0
无	-1(相应的客户端子网/服务器没有向企业管理器报告)

数据传输时间 (毫秒)

数据传输时间测量传输完整的应用程序响应所用的时间，从该请求中发送的第一个响应（服务器响应时间结束）到最后一个数据包。响应时间可受应用程序设计、服务器的性能或网络的影响。如果发送的数据比 TCP 窗口中所允许的最多数据多，则排除初始服务器响应时间，并且仅包括网络往返传输时间。

网络往返传输时间 (毫秒)

网络往返传输时间测量数据包在网络上的服务器和客户端之间传输所用的时间（不包括丢失的时间）。不包括应用程序、服务器和客户端的处理时间。

重新传输延迟 (毫秒)

重新传输延迟测量发送的原始数据包和发送的最后重复数据包之间的处理时间。重新传输延迟报告为所有观测的平均值，而不是仅针对重新传输的数据包。如果 10 个数据包中有一个需要 300 毫秒的重新传输时间，则重新传输延迟将报告为 30 毫秒（300 毫秒/10 个数据包）。

服务器响应时间 (毫秒)

服务器响应时间测量服务器发送针对客户端请求的初始响应所用的时间或初始服务器“思考时间”。服务器响应时间的增加通常表示缺乏服务器资源（如 CPU、内存、磁盘或 I/O）、应用程序编写欠佳或多层应用程序中的某个层性能不佳。

有关 **Application Delivery Analysis** 如何计算网络和服务器运行状况的信息，请参阅

[ADA 如何计算网络和服务器运行状况 \(p. 79\)](#)

继续使用 APM WebView 进行分类

如果状态或度量标准数据表明网络/服务器正常，但是关联应用程序的性能仍然未达到标准，可选的一种方案是继续使用 APM WebView 对应用程序分类。

遵循这些步骤：

1. 登录到 APM WebView。

使用控制台或调查器对问题分类。

继续使用 NPC/CAPC 进行分类

如果运行状况状态或度量标准数据表明网络/服务器不正常，可选的一种方案是使用 NetQoS Performance Center (NPC)/CA Performance Center (CAPC) 更详细地调查基础架构问题。使用下列步骤之一访问 NPC/CAPC。

遵循这些步骤：

1. 在“网络状态信息”显示板中，选择关联的“更多信息”按钮，以便在 NPC/CAPC 中访问客户端子网/服务器概述报告。
2. 登录到 NPC/CAPC，并使用搜索功能查找有关网络/服务器的更多信息。

有关使用 NPC/CAPC 的详细信息，请参阅《*CA Performance Center 管理员和用户指南*》。

网络数据时间延迟

APM WebView 上的网络和服务器数据在 CA Application Delivery Analysis 管理控制台上大约有 5 分钟的时间延迟。管理控制台可以连接到多个收集器，如多端口监视器和单端口 CA Application Delivery Analysis 收集器。为了聚合收集的数据，CA Application Delivery Analysis 时间仓库的宽度为 5 分钟，以 5 分钟为结束界限，例如 7:00 和 7:05 等。CA Application Delivery Analysis 管理控制台每 5 分钟更新一次其数据库。因此，CA Application Delivery Analysis 管理控制台与 CA APM 之间的 Web 服务网桥会检索网络运行状况数据，5 分钟的时间范围内最多有 5 分钟延迟。例如，如果当前时间是下午 6:22，那么数据请求的时间将从下午 6:15 到下午 6:20 结束。APM WebView 上这两个时间之间的数据点将显示相同的结果。

以下内容是来自 Web 服务的示例日志消息：

```
6/15/11 06:22:00.175 PM IST [INFO] [pool-1-thread-2] [ADAConector] Calling
ADA web service...
6/15/11 06:22:00.175 PM IST [INFO] [pool-1-thread-2] [ADAConector]
utcStartTime: 2011-06-15T18:15:00.000+0530
6/15/11 06:22:00.175 PM IST [INFO] [pool-1-thread-2] [ADAConector]
utcEndTime: 2011-06-15T18:20:00.000+0530
```

工具提示数据

APM WebView 图表上提供了工具提示，如“网络状态信息”显示板和“概览”页面上的提示。将您的鼠标悬停在图表的数据点上可从工具提示中获取更多信息。请注意，以下工具提示字段值对应于选定时间片的 Y 轴上的运行状况状态数据值：

- 度量标准的值
- 度量标准的最小值和最大值

CA Application Delivery Analysis 每隔 5 分钟收集一次数据，但 CA Application Delivery Analysis 与 CA APM 之间的集成网桥每隔 15 秒只发送一个数据点。因此，Workstation 将显示相同的数据值，直到从 CA Application Delivery Analysis 获取一个新数据值为止。这会导致所选时间片内报告的数据点数的计数始终显示为 1。CA APM 代理发送数据时，它们会每隔 15 秒发送多个数据点。这样，APM WebView 可以使数据得到平衡，并显示应用程序度量标准的值、最小值和最大值的不同值。

ADA 如何计算网络和服务器运行状况

CA Application Delivery Analysis 通过观测其 TCP 事务并计算以下值来评估网络/服务器的运行状况：

- 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 5 分钟的平均值超过了阈值，且 CA Application Delivery Analysis 观测到最小次数的度量标准，则 CA Application Delivery Analysis 会将客户端网络相应的 5 分钟时间间隔评估为“已降级”或“过度使用”，并创建网络突发事件。
- 托管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 5 分钟的平均值超过了阈值，且 CA Application Delivery Analysis 观测到最小次数的度量标准，则 CA Application Delivery Analysis 会将服务器相应的 5 分钟时间间隔评估为“已降级”或“过度使用”，并创建服务器突发事件。

要评估性能数据，CA Application Delivery Analysis 管理控制台必须收集整整 2 个工作日的数据。工作日从 GMT 午夜到午夜进行计算。例如，如果 CA Application Delivery Analysis 管理控制台在美国东部时间星期一下午 3:30 开始收集服务器端口和客户端网络之间 TCP 会话的数据，则在美国东部时间星期三晚上 7:00（午夜 GMT）之前，CA Application Delivery Analysis 无法评估该网络上应用程序的性能。如果 CA Application Delivery Analysis 管理控制台未收集整整 2 个工作日的数据，则 CA Application Delivery Analysis 会将服务器端口和客户端网络之间的 TCP 会话分为“未评估”。

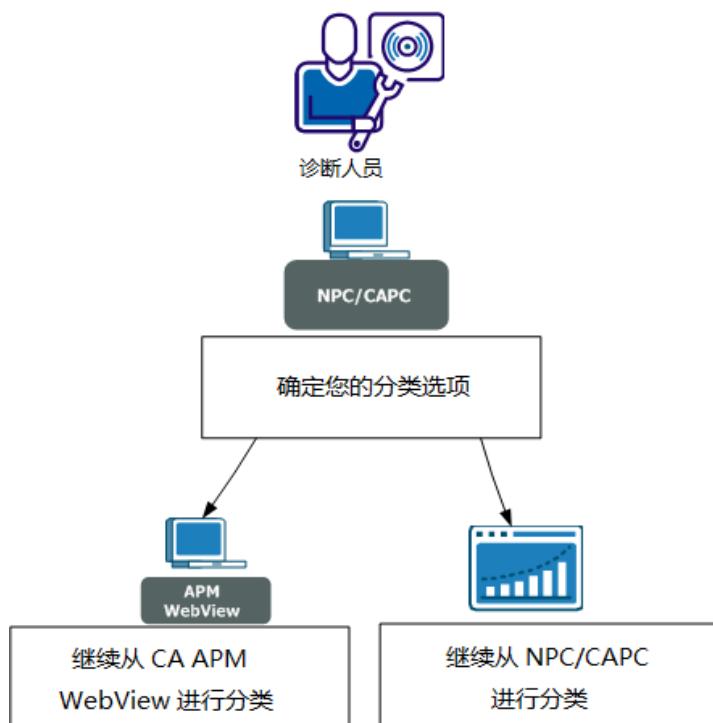
如何使用 NPC 对应用程序问题进行分类

利用 NetQoS Performance Center (NPC)/CA Performance Center (CAPC) 上的应用程序数据，诊断人员可在 NPC/CAPC 用户界面中执行下列操作：

- 查看应用程序和业务服务的运行状况状态。
- 深入查看缺陷和更多的详细度量标准。
- 如果应用程序度量标准显示业务的预期性能，则您可以查看与正在分类的缺陷关联的 Web 服务器或客户端。

下图描述的是诊断人员如何使用 NPC/CAPC 对应用程序问题进行分类的一些方案。

如何从 NPC/CAPC 开始对应用程序问题进行分类



诊断人员请执行下列步骤（步骤 2 和 3 取决于应用程序的度量标准和您的分类决策）：

1. [确定分类选项](#) (p. 81)。
2. [继续使用 APM WebView 进行分类](#) (p. 90)。
3. [继续使用 NPC/CAPC 进行分类](#) (p. 90)。

确定分类方案。

NPC/CAPC 用户界面上显示应用程序性能问题时，请确定一些分类方案为您的后续操作提供指导。

遵循这些步骤：

1. 登录到 NPC/CAPC。

2. 从“应用程序运行状况”菜单打开下列显示板之一：“APM - 应用程序摘要”或“APM - 业务服务摘要”。

使用“状态”字段中的运行状况状态信息，判断需要进一步调查哪个应用程序或业务服务。

有关此显示板的详细信息，请参阅[“APM - 应用程序摘要”显示板 \(p. 83\)](#)。

有关此显示板的详细信息，请参阅[“APM - 业务服务摘要”显示板 \(p. 84\)](#)。

3. 通过挖掘“APM - 应用程序摘要”或“APM - 业务服务摘要”显示板，查看“APM - 业务事务摘要”报告。

“业务事务摘要”报告显示选定业务服务的业务事务运行状况。使用“状态”字段中的运行状况状态信息，判断需要进一步调查哪个业务事务。

有关此报告的详细信息，请参阅[“APM - 业务事务摘要”报告 \(p. 84\)](#)。

4. 通过挖掘“APM - 业务事务摘要”报告查看“APM - 度量标准和突发事件摘要”报告。

“APM - 度量标准和突发事件摘要”报告显示选定业务事务的业务事务组件 (BTC) 度量标准和客户体验度量标准（在用户界面上显示为 RTTM）。

使用业务事务度量标准组件和客户体验度量标准 (RTTM) 来确定后续工作的开展方式。例如，如果 RTTM 和 BTC 度量标准显示高平均响应时间、高每间隔错误和/或停顿计数，您可能选择通过登录到 Workstation 更详细地调查应用程序。如果 RTTM 和 BTC 度量标准在业务的预期范围之内，您可以选择与缺陷有关的客户端 IP 地址或 Web 服务器地址。通过此方案，可调查与缺陷有关的网络问题。

有关此报告的详细信息，请参阅[“APM - 度量标准和突发事件摘要”报告 \(p. 85\)](#)。

5. 通过挖掘“APM - 度量标准和突发事件摘要”报告查看“APM - 缺陷摘要”报告。

“APM - 缺陷摘要”报表显示选定突发事件的最后十个缺陷及其相关详细信息。

有关此报告的详细信息，请参阅[“APM - 缺陷摘要”报告 \(p. 88\)](#)。

NPC/CAPC 显示应用程序数据的方式

NetQoS Performance Center (NPC)/CA Performance Center (CAPC) 上的应用程序数据表示 CA APM 收集的应用程序运行状况数据。Web 服务集成网桥使该数据可供 NPC/CAPC 使用。CA APM 通过对各个应用程序组件执行的各个方法的性能进行测量来监控应用程序运行状况。插入到应用程序组件字节码中的探测器会向代理报告数据，代理又向企业管理器报告数据。诸如 JMX 和 PMI 的其他子系统也报告由代理收集的数据。企业管理器将该数据编译成度量标准（即在应用程序子系统中的许多点经过测量得到的应用程序性能）。根据与应用程序有关的观察事务，CA APM 在应用程序、业务服务和业务事务之间建立关联。

NPC/CAPC 在选定的时间段内以深入的方式显示应用程序运行状况和性能状态数据。CA APM 注册为 NPC/CAPC 上的数据源时，您可以访问“应用程序摘要”报告或“业务服务摘要”报告中的应用程序数据。从这些报表中，可以深入查看缺陷。

应用程序运行状况和性能状态数据分为以下类别：

应用程序

指示 CA APM 监控的应用程序的运行状况状态。选择某个应用程序显示业务服务受监控。

业务服务

指示选定应用程序的业务服务的运行状况状态。选择某个业务服务显示 CA APM 监控的业务事务。

业务事务

指示选定业务服务的业务事务的运行状况状态。选择某个业务事务显示客户体验度量标准（在 UI 上显示为 RTTM）以及业务事务组件 (BTC) 度量标准和突发事件。

突发事件

表示相关联的缺陷组（具体取决于事务类型和缺陷类型）。选择某个突发事件显示最后 N（其中 N = 10 最大）个缺陷。

缺陷

显示特定于每个缺陷的信息。通过选择与每个缺陷关联的 Web 服务器 IP 地址或客户端 IP 地址，可导航至各自服务器或客户端地址的搜索结果页面。

注意：有关 NetQoS Performance Center/CA Performance Center 及其用户界面组件的信息，请参阅《CA Performance Center 管理员和用户指南》。

“APM - 应用程序摘要”显示板

“APM - 应用程序摘要”显示板页面显示业务应用程序的运行状况。从“应用程序运行状况”菜单访问此显示板。

CA APM 监控 Java、J2EE 和 .NET 应用程序的性能和运行状况。前端称为应用程序。

业务应用程序是一个软件程序，可使业务服务实现自动化。CA APM 监控 Web 事务，这些事务是 Web 应用程序的产品。业务应用程序是事务层次结构的一部分。

此显示板上的“应用程序状态”视图显示以下信息：

应用程序

列出 CA APM 监控的应用程序。此报表中仅显示具有已定义的业务事务组件的应用程序。选择一个应用程序可查看关联的业务服务。

状态

指定的时间范围内应用程序的运行状况状态。 使用此信息来确定哪个应用程序需要进一步调查。 颜色表示：

- 白色—无数据，因为企业管理器没响应（无度量标准值）
- 灰色—无数据（度量标准值：0）
- 绿色—正常（度量标准值：1）
- 黄色—警告（度量标准值：2）
- 红色—危险（度量标准值：3）

APM - 业务服务摘要

“APM - 业务服务摘要”显示板页面显示选定应用程序的业务服务的运行状况。 从某个应用程序深入访问此显示板，或从“应用程序运行状况”菜单直接导航以访问此显示板。

CA APM 业务服务是一组业务事务。 度量将聚合到事务层次结构的此级别。

此显示板上的“业务服务状态”视图显示以下信息：

业务服务

列出选定应用程序的业务服务。 选择一个业务服务可查看关联的业务事务。

状态

指定的时间范围内业务服务的运行状况状态。 使用此信息来确定哪个业务服务需要进一步调查。 颜色表示：

- 白色—无数据，因为企业管理器没响应（无度量标准值）
- 灰色—无数据（度量标准值：0）
- 绿色—正常（度量标准值：1）
- 黄色—警告（度量标准值：2）
- 红色—危险（度量标准值：3）

APM - 业务事务摘要

“业务事务摘要”报告显示选定业务服务的业务事务运行状况。 从“APM - 应用程序摘要”或“APM - 业务服务摘要”深入查看此报表。

术语“业务事务”用于描述一系列后端到后端、计算机生成事务。不包含可向事务添加不同客户端行为（思考时间）的用户生成事务。业务事务包括标识事务和一系列可按顺序执行的其他相关事务。可将事务指定为“已包括”、“可缓存”或这两种状态。业务事务在 CEM 控制台中有所定义。

注意：有关定义和创建业务事务的详细信息，请参阅《CA APM 事务定义指南》。

此报表上的“业务事务状态”视图显示以下信息：

业务事务

列出选定服务的业务事务。选择一个业务事务可显示关联的客户体验度量标准（在 UI 上显示为 RTTM）以及业务事务组件 (BTC) 度量标准和突发事件。

状态

指定的时间范围内业务事务的运行状况状态。使用此信息来确定哪个业务事务需要进一步调查。颜色表示：

- 白色—无数据，因为企业管理器没响应（无度量标准值）
- 灰色—无数据（度量标准值：0）
- 绿色—正常（度量标准值：1）
- 黄色—警告（度量标准值：2）
- 红色—危险（度量标准值：3）

APM—度量标准和突发事件摘要

“APM - 度量标准和突发事件摘要”报表显示选定业务事务的业务事务组件度量标准和客户体验度量标准（在 UI 上显示为 RTTM）。CA APM 代理会针对每个业务事务报告业务事务组件度量标准。这些度量标准有时称为 BLAME 度量标准。TIM 会针对每个业务事务收集客户体验度量标准，并将这些度量标准发送到企业管理器。

有关详细信息，请参阅[业务事务组件度量标准 \(p. 86\)](#)。

有关详细信息，请参阅[客户体验度量标准 \(p. 87\)](#)。

业务事务组件度量标准

CA APM 代理会针对每个业务事务报告五个业务事务组件度量标准。这五个度量标准有时称为 **BLAME** 度量标准。BTC 视图包含以下度量标准：

平均响应时间 (毫秒)

响应时间是指完成请求花费的时间。此时间是测量应用程序响应速度的一种基本方式。因此：

- 希望响应时间短些。
- 响应时间较长表明存在问题。

“平均响应时间”度量标准计算在时间间隔内完成的所有请求的平均响应时间。

注意：“平均响应时间”的计数与“每个时间间隔的响应数”的值相等。

每个时间间隔的响应数

每个时间间隔的响应数反映该时间间隔内完成的调用数。这是测量数据吞吐量的一种方式，因此可反映应用程序性能。通常：

- 希数目较大。
- 不希望数目较小。
- 响应数突然激增可能表示使用过度外部系统，例如，网站上拒绝服务攻击。

并发调用

调用指由应用程序及其各种组成部分处理的请求。并发调用指在指定时间处理的请求。

CA APM 通过计算特定时间间隔结束时仍在处理的请求数，来计算并发调用度量标准。

- 希获得较低的并发调用值。
- “并发调用”值较高表明存在问题。

每个时间间隔的错误

错误指由 **JVM** 和 **HTTP** 错误代码报告的异常的数量。错误示例包括：

- 由 **HTTP** 服务器报告的“404 找不到页面”状态
- **SQL** 异常
- **Java** 异常

低错误计数较理想。

停顿计数

停顿请求是指在指定时间阈值内尚未完成的请求。如果某个请求被计为停顿，这并不表示该请求已挂起并永远不能完成，而是表示该请求的执行超过停顿阈值。

- 低计数较理想。
- 不希望计数较高。

默认停顿阈值是 30 秒。

有关停顿事件的信息存储在事务事件数据库中。

客户体验度量标准

TIM 会针对每个业务事务收集客户体验度量标准（在 UI 上显示为 RTTM），并将这些度量标准发送到企业管理器。如果多个 TIM 监控同一业务事务，则将在企业管理器上聚合这些度量标准。

客户体验包括以下度量标准：

平均响应时间 (毫秒)

对于每个时间间隔，执行业务事务所花费的平均时间（以毫秒为单位）。

Total Defects Per Interval

业务事务的所有缺陷类型的缺陷数，聚合所有 TIM。

Total Transactions Per Interval

每个时间间隔中业务事务的事务总数，聚合所有 TIM。

缺陷类型

客户体验度量标准（有时在产品 UI 上显示为 RTTM）被分为几种缺陷类型。这些度量标准可以出现在任何这些类型之中，在用户自定义之前，这些类型就是缺陷的默认名称。

将为与业务事务相关的每种缺陷类型收集缺陷度量标准，包括用户命名的事务 — 如“*<BT_Name>* 的 Slow Time”。

以下是每种缺陷类型的默认值，其中 s = 秒。

慢速

事务处理时间 > 5.000 秒

快速

事务处理时间 < 0.005 秒

高吞吐量

吞吐量 > 100.0 KB/秒

低吞吐量

吞吐量 < 1.0 KB/秒

大

事务大小 > 100.0 KB

小

事务大小 < 0.1KB

缺少事务

组件超时 = 10.000 秒

如何计算客户体验度量标准

使用企业管理器中的 Javascript 计算器计算客户体验事务度量标准。

注意: 只在具有正在运行的 TIM 收集服务和 BTstats 处理器的收集器企业管理器中计算聚合的度量标准。不会在 MOM 企业管理器中运行这些计算。

缺陷摘要报表

“APM - 缺陷摘要”报表显示选定突发事件的最后十个缺陷及其相关详细信息。

缺陷代表事务未能符合客户期望和事务规范。缺陷分为两类：行为缺陷和响应缺陷。如果事务不满足多个规范，则会生成多个缺陷（例如，时间缓慢和缺少组件）。

“缺陷摘要”报表显示以下信息：

缺陷 ID

每个缺陷的标识号

缺陷名称

与缺陷关联的名称

业务服务

与缺陷关联的业务服务

业务事务

与缺陷关联的业务事务

日期和时间

缺陷发生的日期和时间

值

如果大于或等于该基准值，CA APM 则认为事务有缺陷。使用下列 CEM 控制台页面，配置触发缺陷的基准吞吐量值：

管理、业务服务（业务服务）、（业务事务）、业务事务规范

业务影响

业务影响是缺陷或突发事件在业务上的衡量。

CEM 控制台基于与业务事务、缺陷类型和用户关联的缺陷，将业务影响分配给每个传入缺陷。

缺陷的业务影响按如下方式进行计算：

业务事务权重 * 缺陷类型权重 * 用户权重

例如，如果给每个值分配了以下影响级别：

业务事务权重 = 4

缺陷类型权重 = 4

用户权重 = 4

然后， $4 * 4 * 4 = 64$

业务影响是 64。

该影响级别 ...	分配该权重 ...
最低要求	1
很低	2
低	3
中	4
高	5
紧急	6
立即触发	7

登录名称

与缺陷关联的最终用户的登录名称

用户组

受缺陷影响的用户组的名称

在 CA APM 中，用户组允许您为一组（受监控）用户配置设置。而无需为每位用户分别配置设置。可以定义用户组，以便能够轻松确定可能遇到问题的（受监控）用户群体。一个用户只属于一个用户组。

客户端 IP 地址

受缺陷影响的最终用户的客户端 IP 地址。

单击可访问有关客户端的更多详细信息。您将进入此客户端 IP 地址的 NPC/CAPC 上的搜索结果页面。

Web 服务器 IP 地址

与缺陷关联的请求 Web 服务器的 IP 地址。

单击可访问有关 Web 服务器的更多详细信息。您将进入此 Web 服务器 IP 地址的 NPC/CAPC 上的搜索结果页面。

Web 服务器 MAC 地址

与缺陷关联的服务器所对应网卡的硬件地址。

继续使用 APM WebView 进行分类

如果 NPC/CAPC 中的 RTTM 和 BTC 度量标准显示业务的高平均响应时间，高每间隔错误或停顿计数，可选的一种方案是使用 APM WebView 进行分类。使用 APM WebView 查找有关应用程序的详细信息。

遵循这些步骤：

1. 登录到 APM WebView。

使用控制台或调查器对问题分类。

继续使用 NPC/CAPC 进行分类

如果 NetQoS Performance Center (NPC)/CA Performance Center (CAPC) 的 RTTM 和 BTC 度量标准在业务的预期范围之内（但是“应用程序”或“业务服务”显示板仍显示性能问题），可选的一种方案是调查与缺陷有关的网络问题。您可以使用 NPC/CAPC 来执行此调查。

遵循这些步骤:

1. 在“APM - 缺陷摘要”报告中, 请执行下列操作之一:
 1. 选择客户端 IP 地址链接以连接到 NPC/CAPC, 并查找客户端方面的更多详细信息。
 2. 选择 Web 服务器 IP 地址链接以连接到 NPC/CAPC, 并查找 Web 服务器方面的更多详细信息。
2. 使用详细的客户端或 Web 服务器信息, 对与应用程序有关的网络问题进行分类。

有关网络度量标准的详细信息, 请参阅《*CA Performance Center 管理员和用户指南*》。

附录 A：故障排除

此部分包含以下主题：

[CA APM 应用程序数据在 NPC 上不可用 \(p. 93\)](#)

[CA APM 应用程序数据在 CAPC 上不可用 \(p. 94\)](#)

[TIM 停止工作 \(p. 94\)](#)

[基础架构数据在 CEM 控制台上不可用 \(p. 96\)](#)

[Workstation 上的“更多信息”按钮不起作用 \(p. 97\)](#)

CA APM 应用程序数据在 NPC 上不可用

症状：

选择应用程序相关的报表（业务服务摘要或应用程序摘要）之后，看不到 NetQoS Performance Center 中的任何 CA APM 数据。

解决方案：

验证以下方面：

- 您已经在企业管理器或 MOM 上[安装“CA Performance Center 集成包” \(p. 58\)](#)。
- 您已[启动 APM-CAPC 服务 \(p. 51\)](#)。
- 您已[更新 NetQoS Performance Center 数据库 \(p. 61\)](#)。
- 您已在 NetQoS Performance Center 中[将 APM 注册为数据源 \(p. 62\)](#)。
- 您已[创建应用程序分类视图报警 \(p. 60\)](#)。

有关注册数据源的说明，请参阅

[将 CA APM 注册为数据源 \(p. 62\)](#)

有关配置应用程序视图报警的信息，请参阅

[在 APM WebView 上配置报警 \(p. 60\)](#)

CA APM 应用程序数据在 **CAPC** 上不可用

症状:

选择应用程序相关的报告（业务服务摘要或应用程序摘要）之后，看不到 CA Performance Center 中的任何 CA APM 数据。

解决方案:

验证以下方面：

- 您已经在企业管理器或 MOM 上[安装“CA Performance Center 集成包”](#) (p. 49)。
- 您已[启动 APM-CAPC 服务](#) (p. 51)。
- 您已在 CA Performance Center 中[导入 APM 视图](#) (p. 52)。
- 您已在 CA Performance Center 中[将 APM 注册为数据源](#) (p. 52)。
- 您已在 CA Performance Center 中向“应用程序运行状况”菜单[添加 APM 显示板](#) (p. 54)。
- 您已[创建应用程序分类视图报警](#) (p. 51)。

有关注册数据源的说明，请参阅

[将 CA APM 注册为数据源](#) (p. 62)

有关配置应用程序视图报警的信息，请参阅

[在 APM WebView 上配置报警](#) (p. 60)

TIM 停止工作

症状:

安装在多端口监视器上的 TIM 停止功能的运行。例如，它已经停止记录和生成统计信息。另外，我在 TIM 日志中看到“skip old packets”消息。

解决方案:

多端口监视器上安装了 Tim 的情况下，多端口监视器上的 NapaTech 卡将使用该卡上的时间标记数据包到达时间。如果多端口监视器的系统时间和 NapaTech 卡的时间存在明显不同，TIM 则会停止功能的运行。

存在两种可能情况。请确定哪种情况适用于您。

1. TIM 处理有时可能落后于多端口监视器生成的数据包文件。例如，如果 TIM 停止然后重新启动，或多端口监视器生成数据包文件的速度比 TIM 使用的速度快。请通过以下操作来确认 TIM 延迟时间：
 - a. 确认 NapaTech 卡时间已经与多端口监视器的系统时间进行同步。
 - b. 查看多端口监视器系统状态页面并验证该页面上未显示警告消息。

如果您已经确认上述二种情况，则表示 TIM 上可能没什么错误。TIM 不会处理 15 分钟以前的数据包文件（该默认值可以更改）。忽略这些旧数据包文件之后，TIM 将恢复正常处理。TIM 只是需要时间来赶上多端口监视器生成的文件。

2. 将 NapaTech 卡时间与您的多端口监视器系统时间进行比较。在终端上使用以下命令可查看 NapaTech 卡时间：

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

在终端上使用以下命令可查看多端口监视器系统时间：

```
date
```

如果两个时间不同，且多端口监视器系统状态页面显示警告消息，则查看 NapaTech 卡的时间以及网络时间协议 (NTP) 服务器上的时间。

在下列网站选择时区可获取 NTP 时间：

<http://www.time.gov/>

考虑以下情况并确定哪一种适用于您。

情况 1

条件

- Napattech 卡时间与 NTP 时间存在较大不同（超过 15 分钟）
- 多端口监视器的系统时间与 NTP 时间存在很小的差别（不到 5 秒）

操作

- 通过运行以下命令将 NapaTech 时间与系统时钟进行同步：

```
/opt/NetQoS/scripts/syncNapattechClock
```
- 如果 Napattech 时间与多端口监视器上的系统时间差异不到 5 分钟，Napattech 驱动器操作系统同步将逐渐校准 Napattech 时钟。如果 Napattech 时间与多端口监视器上的系统时间差异超过 5 分钟，Napattech 时间将立即与多端口监视器上的系统时间进行同步。

情况 2

条件

- NapaTech 卡时间与 NTP 时间存在细微差异。
- 多端口监视器的系统时间和 CEM 控制台时间与 NTP 时间存在很大差异。

操作

- 调整 CEM 控制台时间，以便与 NTP 时间同步。
- 等待并确认多端口监视器的系统时间是由 CEM 设置的，并同时与 NTP 时间进行了同步。
- 确认多端口监视器的 ntpd 进程正在运行。如果未运行，则启动该进程。

多端口监视器的系统时间与 NTP 时间的差异超过 1000 秒时，
ntpd 进程可能自动停止。

情况 3

条件

- NapaTech 卡时间与 NTP 时间存在很大差异。
- 多端口监视器的系统时间和 CEM 控制台时间与 NTP 时间存在很大差异。

操作

- 调整 CEM 控制台时间，以便与 NTP 时间同步。
- 等待并确认多端口监视器的系统时间是由 CEM 设置的，并同时与 NTP 时间进行了同步。
- 确认多端口监视器的 ntpd 进程正在运行。如果未运行，则启动该进程。
- 通过运行以下命令将 NapaTech 时间与系统时钟进行同步：
`/opt/NetQoS/scripts/syncNapatechClock`

基础架构数据在 CEM 控制台上不可用

症状:

缺陷详细信息应配有关联的网络基础架构信息，但查看缺陷详细信息时看不到关联的网络基础架构信息。

解决方案:

确认已正确配置以下项:

- 已选中 CEM 控制台 UI (“监视器”, 多端口监视器计算机) 上的“多端口监视器已启用”复选框来启动对多端口监视器的 Web 服务调用, 从而获得 TCP 数据。
- 生成该缺陷已超过 5 分钟。在多端口监视器数据库中提供网络运行状况数据之前, 可能会存在最多 5 分钟的延迟。如果生成该缺陷的时间还不到 5 分钟, 请等待几分钟, 然后刷新浏览器页面。

Workstation 上的“更多信息”按钮不起作用

症状:

无法从 CA APM Workstation/WebView 上的“网络状态信息”显示板直接连接到 NetQoS Performance Center (NPC)/CA Performance Center (CAPC)。该显示板上的“更多信息”按钮不起作用。

解决方案:

通过“更多信息”按钮可转到 NPC/CAPC (具体为网络概览和服务器概览报告)。这些报表的链接需要对每个按钮进行一次性配置。请参阅[在“网络状态信息”显示板上配置“更多信息” \(p. 74\)](#)。

有关配置“更多信息”按钮的说明, 请参阅

[配置“网络状态信息”显示板上的“更多信息” \(p. 74\)](#)