

# CA Application Performance Management

配置和管理指南

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

---

<b>第 1 章： 《CAAPM 配置和管理指南》 简介</b>	<b>21</b>
关于 APM .....	21
<b>第 2 章： 启动和停止企业管理器</b>	<b>23</b>
在 Windows 上启动企业管理器 .....	23
将企业管理器作为 Windows 服务运行 .....	23
在 Windows 上手动启动企业管理器 .....	25
在 UNIX 上启动企业管理器 .....	25
在 UNIX 上手动启动企业管理器 .....	26
在 UNIX 上运行企业管理器控制脚本 .....	26
在 UNIX 上的 nohup 模式下运行企业管理器 .....	27
配置企业管理器以使用不同的 JVM .....	28
关于企业管理器日志文件 .....	28
按日期或大小轮转企业管理器日志 .....	29
配置企业管理器配置目录 .....	30
停止企业管理器 .....	31
从终端窗口停止企业管理器 .....	31
从工作站停止企业管理器 .....	31
企业管理器的自动关闭 .....	32
意外关闭后重新启动 .....	32
企业管理器 shell 和终端窗口命令 .....	33
<b>第 3 章： 配置企业管理器通信</b>	<b>35</b>
默认的企业管理器通信通道 .....	35
将通信通道重新绑定到正在使用中的端口 .....	36
配置 SSL .....	36
跨防火墙连接到企业管理器 .....	39
针对 HTTPS 配置企业管理器 Web 服务器 .....	39
了解 HTTPS 的工作原理 .....	39
默认的 Jetty 配置文件 .....	40
<b>第 4 章： 配置企业管理器数据库</b>	<b>45</b>
管理 APM 数据库 .....	45
备份或还原数据库 .....	45
导出或导入数据库配置 .....	51
将 APM 数据库移至其他操作系统 .....	57

---

将 PostgreSQL 数据库中的数据迁移到 Oracle 数据库 .....	57
数据库故障排除 .....	59
配置 SmartStor 数据存储 .....	59
有关 SmartStor 层如何工作的详细信息 .....	60
自动删除元数据 .....	61
确定 SmartStor 系统要求 .....	61
指定 SmartStor 数据层值 .....	61
配置事务事件数据库位置和老化 .....	62
配置基准存储的位置 .....	63
备份 SmartStor、基准和事务事件数据 .....	63
创建仅供查询的副本群集 .....	64
使用 SmartStor 工具调整 SmartStor 数据 .....	65
SmartStor 工具命令 .....	66
merge .....	66
remove_metrics .....	67
remove_agents .....	68
keep_agents .....	69
prune .....	69
test_regex .....	70
list_agents .....	71
清除 SmartStor 元数据 .....	71
清除 SmartStor 数据和元数据 .....	73
示例：使用 test_regex 命令查找 SmartStor 数据问题 .....	75
将 8.x 数据升级到 9.x .....	76
使用“升级”命令来升级 8.x 数据 .....	77

## **第 5 章：使用虚拟代理聚合度量标准** **79**

了解虚拟代理 .....	79
虚拟代理要求 .....	79
配置虚拟代理 .....	80

## **第 6 章：配置企业管理器和群集** **83**

配置独立的企业管理器 .....	83
了解企业管理器群集 .....	83
什么情况下构建企业管理器群集 .....	84
了解 MOM 如何管理收集器 .....	84
群集和企业管理器时钟同步 .....	85
群集和代理命名 .....	85
群集和管理模块 .....	86
使用企业管理器故障切换 .....	86
企业管理器故障切换规则 .....	88
将企业管理器故障切换配置为在单个主机上运行 .....	89

关于 MOM 故障切换和 CA CEM TIM.....	89
配置企业管理器群集.....	91
配置 MOM.....	92
配置收集器.....	92
关于 CDV.....	93
配置 CDV.....	94

## 第 7 章：配置 MOM 代理负载平衡 97

代理负载平衡概览.....	97
MOM 将代理分配给收集器的方式.....	98
MOM 如何重新平衡群集.....	99
设置代理负载平衡度量标准的加权因子.....	99
设置代理负载平衡度量标准的阈值.....	100
设置代理负载平衡时间间隔属性.....	101
代理负载平衡使用方案.....	101
将新收集器添加到群集时的代理负载平衡.....	102
添加具有代理的收集器时的代理负载平衡.....	102
收集器出现故障时的代理负载平衡.....	103
收集器重新启动时的代理负载平衡.....	103
具有权重的代理负载平衡.....	103
配置对收集器的代理分配.....	104
代理负载平衡配置示例.....	107

## 第 8 章：配置代理—企业管理器网络拓扑 113

代理—企业管理器网络拓扑概述.....	113
代理连接信息在 CA Introscope 中传播的方式.....	115
配置如何影响代理到企业管理器的连接.....	116
当代理与企业管理器断开连接时会发生什么情况.....	117
当代理连接请求被拒绝时会发生什么情况.....	117
配置代理的过程—企业管理器网络拓扑.....	118
规划代理—企业管理器网络拓扑.....	119
配置在没有 loadbalancing.xml 规则时是否允许新代理连接.....	121
配置代理重新连接等待时间.....	121
配置禁止连接的代理连接限定限值.....	122
配置代理连续重新连接到任何允许的企业管理器.....	122
为企业管理器允许和禁止的代理配置 loadbalancing.xml.....	124
对代理进行故障排除—企业管理器网络拓扑.....	124
企业管理器如何处理拒绝的代理.....	124
收集器使用 introscope.apm.agentcontrol.agent.allowed 属性时.....	125
代理未将 loadbalancing.xml 正则表达式匹配为允许或禁止.....	125
分配给代理的所有收集器不可用，其他收集器可用.....	126
收集器使用直接连接处理不允许的代理的方式.....	126

introscope.apm.agentcontrol.agent.allowed 属性缺失时的默认代理连接值.....	126
CA Introscope 确定没有 MOM 可用时代理连接位置的方式.....	127

## 第 9 章：使用命令行 Workstation 129

关于命令行工作站 (CLW).....	129
运行 CLW .....	130
JVM 要求.....	130
从何处运行 CLW 命令.....	130
使用 CLW 交互模式.....	130
调用 CLW .....	131
CLW 区分大小写。.....	131
CLW 命令输出.....	131
CLW 和正则表达式.....	132
CLW 命令中的反斜线和引号.....	132
在不同环境中使用 CLW .....	132
配置命令行 Workstation 日志.....	132
CLW 命令参考.....	133
企业管理器命令.....	133
Introscope 代理命令.....	135
APM 状态控制台命令.....	138
管理模块命令.....	142
操作命令.....	145
报警命令.....	147
报警停机时间日程表命令.....	149
计算器命令.....	150
显示板命令.....	152
度量标准和度量标准组命令.....	154
报告模板命令.....	156
SNMP 收集命令.....	160
配置事务跟踪选项.....	162
启动事务跟踪会话.....	162
应用程序分类视图命令.....	168
Loadbalancing.xml 命令.....	175
示例脚本.....	177
事务跟踪会话.....	177
由报警触发的事务跟踪会话.....	181

## 第 10 章：使用 WatchDog 命令行工具 183

关于 WatchDog.....	183
运行 WatchDog.....	184
在 SAP 上运行 WatchDog.....	185
WatchDog 命令.....	185



WatchDog start 命令 .....	186
WatchDog stop 命令 .....	187
WatchDog status 命令 .....	187
WatchDog 命令选项 .....	189
WatchDog -watch 命令选项 .....	189
WatchDog -port 命令选项 .....	190
WatchDog -startcmd 命令选项 .....	190
WatchDog -interval 命令选项 .....	191
WatchDog -startuptime 命令选项 .....	191
WatchDog -jre 命令选项 .....	192
WatchDog -emport 命令选项 .....	192
WatchDog -emuser 命令选项 .....	192
WatchDog -empwd 命令选项 .....	193
查看 WatchDog 日志文件 .....	193
示例脚本 .....	193

## **第 11 章：配置 WebView 选项** **195**

配置 WebView 应用程序上下文路径 .....	195
如何配置和监控 APM WebView 性能 .....	195
查看先决条件 .....	196
配置 APM UI Performance Monitor .....	197
验证配置 .....	199
监控 WebView UI 性能 .....	199
配置 WebView 度量标准组 .....	202
查看和解析显示板数据 .....	202

## **第 12 章：配置工作站** **207**

以详细模式运行工作站 .....	207
将工作站输出重定向到某个文件 .....	207
配置工作站以提供登录值 .....	208
配置工作站以使用亚洲语言报告 .....	208

## **第 13 章：系统配置** **209**

配置时钟偏移容差 .....	209
设置最大数据点检索属性 .....	210
限制查询返回的数据点 .....	212
增大返回的查询结果数 .....	213
配置 APM 状态控制台限定和重要事件 .....	213

---

<b>第 14 章：配置应用程序分类地图</b>	<b>215</b>
应用程序分类视图.....	215
事务采样.....	216
配置视图元素老化.....	216
应用程序分类地图数据限定.....	219
配置应用程序分类视图数据清除.....	220
在应用程序分类视图对象中配置过时时间.....	222
应用程序分类视图时间老化属性.....	223
配置应用程序分类视图时间老化属性.....	224
<b>第 15 章：配置 APM 以加载 Catalyst 数据</b>	<b>225</b>
配置 CA APM 以加载 CA Catalyst 数据.....	225
配置 CatalystPolicy.xml 文件.....	226
<b>第 16 章：CA CEM 简介</b>	<b>227</b>
访问 CEM 控制台和设置页面.....	227
访问 CEM 控制台.....	227
对登录到 CA CEM 进行故障排除.....	228
访问 TIM 系统设置页面.....	228
从 CEM 控制台访问 TIM.....	229
CA CEM 管理员职责.....	229
每日任务.....	230
每周任务.....	230
每月任务.....	231
每季度任务.....	231
<b>第 17 章：CA CEM 联网备选方案</b>	<b>233</b>
关于 CA CEM 网络选项.....	233
关于监控网络通信.....	233
使用网络分流器.....	234
使用镜像端口.....	234
关于 CA CEM 插入位置.....	235
位于 Internet 和 Internet 路由器之间.....	236
位于 Internet 路由器和防火墙之间.....	236
位于防火墙和聚合交换机之间.....	237
位于聚合交换机和网络负载均衡器之间.....	237
位于网络负载均衡器和 Web 服务器之间.....	238
从浏览器连接到企业管理器.....	238
IPv6 和 CA CEM.....	238
关于 IPv6.....	239

CA CEM 中的 IPv6.....	239
监控 IPv6 网络通信.....	239
在双协议栈（IPv6 和 IPv4）主机上运行 CA CEM.....	240
允许的 IPv6 地址格式.....	241

## 第 18 章：管理 CA CEM 243

CA CEM 管理过程.....	243
分发企业管理器服务.....	244
企业管理器服务的典型分布.....	246
在群集环境中分发企业管理器服务.....	247
选择参与实时事务度量标准的 TIM.....	248
选择用于自动事务发现的 TIM.....	249
修改企业管理器配置.....	249
删除企业管理器.....	251
企业管理器服务故障排除.....	251
定义 CA CEM 域.....	253
突发事件成本与业务影响.....	258
定义与突发事件相关的设置.....	259
配置突发事件管理设置.....	262
设置突发事件生成规则.....	263
为突发事件设置业务影响并收集证据.....	264
证据收集脚本中使用的参数.....	266
配置突发事件过期规则.....	266
在突发事件打开或更改重要级别时发送电子邮件.....	267
配置 SMTP 服务器设置.....	268
为新的业务服务设置安全组.....	270
启用监视器.....	273
同步监视器.....	273
查看自上次同步以来的配置更改.....	274

## 第 19 章：在 CA CEM 上管理用户和组 277

关于用户组.....	277
最大用户组数.....	279
按请求属性自动分配新用户.....	279
自动将新用户分配给子网用户组.....	280
为新用户创建子网用户组.....	280
标识代理服务器用户.....	281
管理新的用户组.....	282
手动将新用户分配给用户组.....	282
配置用户组.....	283
通过批量编辑配置用户设置.....	284
配置关联 SLA.....	285

查看关联 SLA.....	286
添加关联 SLA.....	286
更新现有的关联 SLA.....	287
删除关联 SLA.....	288
删除用户组.....	288
停用或删除用户.....	289
重新激活用户.....	289

## **第 20 章：在 CA CEM 上管理系统操作** **291**

关于 CA CEM 事件.....	291
重要级别.....	291
可能事件列表.....	292
查看 CA CEM 事件.....	294
管理 CA CEM 事件.....	294
接收事件的电子邮件通知.....	294
检查 TIM 计算机的运行状况.....	296
设备运行状况页面参考表.....	296
查看 CA CEM 审核路径.....	297

## **第 21 章：CA CEM 报告** **299**

捕获 CA CEM 报告.....	299
关于 CA CEM 报告聚合.....	299
报告交付.....	300
保护报告数据.....	300
报告格式.....	301
报告时限.....	302
浏览报告.....	303
PDF 报告.....	303
电子邮件报告.....	304
已保存或已排定的报告.....	304
排定报告.....	305
使用“我的报告”排定报告.....	305
生成和排定报告.....	307
导出 CA CEM 数据.....	308
导出数据.....	308
保存或排定报告.....	310
CSV 标头.....	311

## **第 22 章：使用 CA CEM 监控安全 Web 应用程序** **313**

导入和管理 SSL 私钥.....	313
保存基于 Apache 或 OpenSSL 的 Web 服务器私钥文件.....	313

导出并转换 Microsoft Internet Information Service (IIS) 私钥 .....	314
SunONE、iPlanet 或 Netscape 企业服务器.....	315
针对 SSL 配置 CA CEM.....	318
关于 HTTPS 服务器的多个密钥.....	318
验证使用 SSL 的 CA CEM 功能。 .....	318

## **第 23 章： 将 Napatech 适配器用于 CA CEM** **321**

关于将 Napatech 适配器用于 CA CEM.....	321
获得 Napatech 适配器和软件.....	321
安装 Napatech 适配器和 Napatech 软件 .....	322
启用 Napatech 适配器并监控.....	323
（可选）创建和启用 Napatech 筛选.....	323
创建高级筛选.....	325
其他 Napatech 适配器任务 .....	326
排除 Napatech 适配器故障 .....	328
Napatech 适配器没有接收流量 .....	328
Napatech 适配器作为以太网端口 .....	329
未看到预期流量.....	329
序列号和其他 Napatech 适配器详细信息.....	329

## **第 24 章： 配置 CA Introscope 以与 CA CEM 一起使用** **331**

CA APM 使用入门.....	331
CA APM 客户体验度量标准概述.....	332
CA APM 问题解决方案分类概述.....	332
配置 CA CEM 的清单.....	334
决定需要哪些集成功能.....	334
配置 Introscope 设置 .....	335
配置客户体验度量标准集成.....	338
验证 CA CEM 配置.....	344
配置 Introscope 的清单.....	344
决定需要哪些集成功能.....	345
配置企业管理器.....	345
与 Java 代理集成.....	347
与 .NET 代理集成 .....	349
验证 Introscope 配置 .....	351
CA Introscope 与 CA CEM 集成故障排除.....	352
验证 CA CEM 上的 CA Introscope 集成.....	352
症状和解决方案.....	353
升级注意事项.....	354
设置业务应用程序.....	354

---

<b>第 25 章：将 CA SiteMinder 与 CA CEM 集成</b>	<b>357</b>
CA SiteMinder 的清单.....	357
在 CA CEM 上配置 CA SiteMinder .....	358
创建自定义 CA SiteMinder 代理.....	359
在 CA SiteMinder 上为 CA CEM 创建自定义代理类型 .....	359
定义 CA CEM 上的策略服务器 .....	360
定义 CA CEM 上的代理 .....	360
查看 TIM SiteMinder 主机配置.....	361
启用 CA SiteMinder.....	361
CA SiteMinder 与 CA CEM 集成故障排除 .....	362
<b>第 26 章：将 CA Service Desk 与 CA CEM 集成</b>	<b>363</b>
关于 CA Service Desk 与 CA CEM.....	363
CA Service Desk 集成概述 .....	363
为 CA CEM 配置 CA Service Desk.....	364
配置 CA Service Desk 插件 .....	364
配置 CA Service Desk 请求区域 .....	367
同时使用 CA Service Desk 与 CA CEM.....	367
CA Service Desk 与 CA CEM 集成故障排除 .....	368
症状和解决方案.....	369
CA Service Desk 到 CA CEM 的集成术语.....	370
CA Service Desk 术语 .....	370
CA Service Desk 与 CA CEM 的术语对应关系.....	371
<b>第 27 章：将 CA APM Cloud Monitor 与 CA APM 相集成</b>	<b>373</b>
如何将 CA APM Cloud Monitor 与您的 CA APM 部署相集成.....	373
下载并安装 CA APM Cloud Monitor 代理 .....	374
验证 CA APM Cloud Monitor 代理连接 .....	374
如何限制数据.....	375
<b>附录 A：属性文件参考</b>	<b>379</b>
IntroscopeEnterpriseManager.properties .....	379
可用处理器.....	380
报警行为.....	381
通讯 .....	381
Workstation 登录参数自动填充部分 .....	386
EM Web 服务器设置.....	386
热配置服务.....	387
应用程序启发.....	388
日志记录.....	388

永久性集合—将数据记录到数据库.....	389
平面文件属性.....	391
事务事件数据库.....	391
事务跟踪采样.....	392
企业管理器度量标准限制.....	393
<b>SmartStor</b> .....	395
基准数据存储.....	400
SNMP 收集.....	400
WebView.....	401
<b>CA APM ChangeDetector</b> .....	401
管理模块引导.....	401
管理模块部署.....	402
群集设置.....	402
代理交互.....	406
企业管理器故障切换.....	410
配置目录.....	411
应用程序分类地图数据.....	411
位置视图数据.....	416
<b>Web Services</b> .....	416
传出消息队列.....	416
线程转储.....	418
用于 Web 服务性能处理的线程属性 .....	420
SNMP 分类视图报警操作 .....	421
应用程序视图对象.....	423
<b>APMEnterpriseManager.properties</b> .....	423
c3p0 属性.....	423
特定于 Hibernate 的属性.....	425
<b>apm-events-thresholds-config.xml</b> .....	427
Introscope 限定属性 .....	427
introscope.clw.max.users .....	428
introscope.enterprisemanager.agent.connection.limit .....	428
introscope.enterprisemanager.agent.error.limit .....	429
introscope.enterprisemanager.agent.metrics.limit .....	429
introscope.enterprisemanager.agent.trace.limit.....	430
introscope.cdv.max.users .....	430
introscope.enterprisemanager.disconnected.historical.agent.limit.....	431
introscope.enterprisemanager.events.limit .....	433
introscope.enterprisemanager.metrics.historical.limit .....	433
introscope.enterprisemanager.metrics.live.limit .....	433
introscope.enterprisemanager.transactionevents.storage.max.disk.usage.....	434
introscope.workstation.max.users.....	434
客户体验限定属性.....	435
设置重要事件阈值.....	437
<b>ResourceMetricMap.properties</b> .....	440

---

CPU 使用率 .....	441
在 GC 中耗费的时间 .....	442
使用中的线程 .....	442
使用中的 JDBC 连接 .....	442
Catalyst.properties .....	442
catalyst.host .....	443
catalyst.protocol .....	443
catalyst.port .....	444
catalyst.login .....	444
catalyst.password .....	444
catalyst.rest.entrypoint .....	444
catalyst.rest.alerts.pollingperiodsec .....	445
catalyst.rest.virtualhosts.pollingperiodsec .....	445
catalyst.product.url .....	445
catalyst.alert.filter.total .....	446
catalyst.alert.filter.time .....	446
catalyst.alert.filter.products .....	446
catalyst.alert.filter.types .....	447
catalyst.alert.filter.severities .....	448
catalyst.rest.maxFailures .....	448
catalyst.rest.maxAlertsPerPage .....	449
catalyst.rest.alerts.threads .....	449
catalyst.rest.virtualhosts.threads .....	449
catalyst.entity.cache.size .....	450
catalyst.entity.cache.expirationsec .....	450
catalyst.database.alerts.enabled .....	450
catalyst.database.map.name .....	451
EMservice.conf .....	451
wrapper.java.command .....	451
wrapper.java.mainclass .....	452
wrapper.java.classpath.x .....	452
wrapper.java.library.path.1 .....	452
wrapper.java.additional.x= .....	452
wrapper.java.initmemory .....	453
wrapper.java.maxmemory .....	453
wrapper.app.parameter.x .....	453
wrapper.startup.timeout .....	453
wrapper.console.format .....	454
wrapper.console.loglevel .....	454
wrapper.logfile .....	454
wrapper.logfile.format .....	454
wrapper.logfile.loglevel .....	454
wrapper.logfile.maxsize .....	455
wrapper.logfile.maxfiles .....	455
wrapper.syslog.loglevel .....	455



---

wrapper.ntservice.name .....	455
wrapper.ntservice.displayname.....	456
wrapper.ntservice.description .....	456
wrapper.ntservice.dependency.x.....	456
wrapper.ntservice.starttype .....	456
wrapper.ntservice.interactive .....	456
Introscope Enterprise Manager.lax .....	457
lax.application.name .....	457
lax.class.path .....	457
lax.command.line.args .....	457
lax.dir .....	458
lax.main.class .....	458
lax.main.method .....	458
lax.nl.current.vm .....	458
lax.nl.java.launcher.main.class.....	459
lax.nl.java.launcher.main.method .....	459
lax.nl.java.option.additional.....	460
lax.nl.message.vm.not.loaded .....	460
lax.nl.valid.vm.list.....	461
lax.nl.win32.microsoftvm.min.version.....	461
lax.root.install.dir .....	461
lax.stderr.redirect .....	461
lax.stdin.redirect .....	462
lax.stdout.redirect.....	462
lax.user.dir.....	463
lax.version .....	463
IntroscopeWorkstation.properties.....	463
log4j.logger.Workstation .....	464
log4j.appender.logfile.File.....	464
introscope.workstation.graph.antialiased .....	464
transport.http.proxy.host .....	465
transport.http.proxy.port.....	465
transport.http.proxy.username .....	465
transport.http.proxy.password .....	465
transport.tcp.truststore .....	466
transport.tcp.trustpassword .....	466
transport.tcp.truststore .....	466
transport.tcp.keystore .....	466
transport.tcp.keypassword .....	467
transport.tcp.ciphersuites.....	467
Introscope Workstation.lax.....	467
lax.application.name .....	468
lax.class.path .....	468
lax.command.line.args .....	468
lax.dir .....	468

---

lax.main.class .....	468
lax.main.method .....	469
lax.nl.current.vm .....	469
lax.nl.java.launcher.main.class .....	469
lax.nl.java.launcher.main.method .....	469
lax.nl.java.option.additional .....	470
lax.nl.message.vm.not.loaded .....	470
lax.nl.valid.vm.list .....	470
lax.nl.win32.microsoftvm.min.version .....	470
lax.root.install.dir .....	471
lax.stderr.redirect .....	471
lax.stdin.redirect .....	471
lax.stdout.redirect .....	472
lax.user.dir .....	472
lax.version .....	472
IntroscopeWebView.properties .....	472
introscope.webview.jetty.configurationFile .....	473
introscope.webview.tcp.ipaddress .....	473
introscope.webview.tcp.port .....	473
introscope.webview.context.path .....	474
introscope.webview.enterprisemanager.tcp.host .....	474
introscope.enterprisemanager.webview.disableLogin .....	474
introscope.webview.enterprisemanager.tcp.port .....	474
log4j.logger.WebView .....	475
log4j.logger.WebServer .....	475
log4j.logger .....	476
log4j.logger.com.wily .....	476
log4j.logger.org.apache.myfaces .....	476
log4j.logger.org.apache.jasper .....	477
log4j.logger.org.apache.struts .....	477
log4j.logger.org.mortbay .....	477
日志记录配置属性 .....	478
log4j.appender.console .....	478
log4j.appender.logfile .....	478
log4j.appender.logfile.File .....	479
Introscope WebView.lax .....	479
可执行文件的名称 .....	479
lax.class.path .....	479
lax.command.line.args .....	479
lax.dir .....	480
lax.main.class .....	480
lax.main.method .....	480
lax.nl.current.vm .....	480
lax.nl.java.launcher.main.class .....	481
lax.nl.java.launcher.main.method .....	481

lax.nl.java.option.additional.....	481
lax.nl.message.vm.not.loaded .....	482
lax.nl.valid.vm.list.....	482
lax.nl.win32.microsoftvm.min.version.....	482
lax.root.installation.dir.....	482
lax.stderr.redirect .....	483
lax.stdin.redirect .....	483
lax.stdout.redirect.....	483
lax.user.dir.....	484
lax.version .....	484
APMCloudMonitor.properties .....	484
apmcm.folders.include .....	484
apmcm.monitors.include .....	485
apmcm.checkpoints.include .....	485
apmcm.include.inactive.monitors.....	486
apmcm.folder.metrics.include .....	486
apmcm.monitor.psp.metrics.include.....	486
apmcm.monitor.checkpoint.metrics.include.....	487
apmcm.force.global.update.....	487
apmcm.log.adjustment.....	487

## 附录 B: JDBC API 489

配置 JDBC API.....	489
使用 JDBC API.....	489
度量标准查询.....	490
事务跟踪查询.....	491

## 附录 C: 配置 Introscope 扩展 493

配置 SNMP 适配器.....	493
SNMP 适配器限制.....	493
SNMP 适配器组件.....	493
报警 .....	494
配置通知和报警.....	495
配置 SNMP 功能.....	496
上传到 HP LoadRunner.....	498
上传到 HP OpenView .....	500
将 Introscope 度量标准转换为 SNMP 度量标准.....	501
配置 Introscope 报警 Web 服务扩展.....	502

## 附录 D: 默认 tess-default.properties 文件 505

修改 tess-default.properties 属性默认文件.....	505
设置用于证据收集的 Perl 或 Python 路径.....	506

---

perl.path.....	506
python.path.....	507
设置“其他缺陷信息”链接的目录路径.....	507
additionalDefectDetailFileLocation.....	508
改进缺陷处理性能.....	508
defects.affectedUserGroupUpdateInterval_Secs.....	509
defects.affectedUserGroupAgeoutInterval_Mins.....	510
更改损坏文件的目录位置.....	510
collectors.badDataDirectory.....	511
其他 CA CEM 默认属性.....	511
baseline.durationInDays.....	512
BTStatsMetricName.backwardCompatible.....	513
email.defaultFromAddress.....	513
invalid.importexport.filename.chars.....	514
timTessCommunication.useSsl.....	514

# 第 1 章： 《CA APM 配置和管理指南》 简介

---

要使用本指南，需了解 Web 服务器、浏览器、支持平台以及网络环境的运行知识。熟悉 CA CEM 监控的应用程序。此外，还应注意与 CA CEM 集成的其他产品。

本指南假定：

- 已根据《CA APM 安装和升级指南》中的信息安装 CA CEM。
- 您基本了解《CA APM 概述指南》中介绍的 CA Introscope、CA APM 和 CA CEM。

此部分包含以下主题：

[关于 APM](#) (p. 21)

## 关于 APM

CA Introscope 和 CA CEM 是 CA APM 解决方案的核心产品。

CA APM 会提供全面有效的应用程序性能管理策略，使您能够了解最终用户体验并衡量服务级别协议 (SLA)。您可以将所有事务映射到端到端基础架构，以及在完整的集成解决方案中执行突发事件分类和根源诊断。

通过 CA APM，您可以：

- 了解真实的用户体验。
- 设置和管理业务服务的 SLA。
- 获取 100% 事务可见性。
- 快速确定问题源。
- 执行分类，确定相关利益人，并且进行根源分析。
- 确定基于真实业务影响的突发事件的优先级。
- 提供主动和预测性的应用程序监控。
- 增加报告并不断改善。



## 第 2 章： 启动和停止企业管理器

---

本章提供了有关启动和停止企业管理器以及在受支持环境中自动启动的说明。

**注意：**有关属性的详细信息，请参阅“[属性文件参考](#) (p. 379)”。

此部分包含以下主题：

[在 Windows 上启动企业管理器](#) (p. 23)

[在 UNIX 上启动企业管理器](#) (p. 25)

[配置企业管理器以使用不同的 JVM](#) (p. 28)

[关于企业管理器日志文件](#) (p. 28)

[按日期或大小轮转企业管理器日志](#) (p. 29)

[配置企业管理器配置目录](#) (p. 30)

[停止企业管理器](#) (p. 31)

[意外关闭后重新启动](#) (p. 32)

[企业管理器 shell 和终端窗口命令](#) (p. 33)

### 在 Windows 上启动企业管理器

在 Windows 环境中运行企业管理器时，您可以手工启动企业管理器，也可以将其作为 Windows 服务运行。

#### 将企业管理器作为 Windows 服务运行

将企业管理器作为 Windows 服务安装可以提高其可用性。如果您将企业管理器配置为 Windows 服务，则运行企业管理器的计算机会自动启动；当该计算机关闭时，企业管理器也会关闭。

**注意：**Introscope 使用 Tanuki Software (<http://wrapper.tanukisoftware.org>) 提供的公共域 Java Service Wrapper 使企业管理器可以作为 Windows 服务运行。有关 Tanuki 包装器的信息，请参阅“[Configuration Property Overview](#)”（配置属性概述）(<http://wrapper.tanukisoftware.org>)。

这些说明假定您熟悉如何在 Windows 服务上配置应用程序，并且熟悉如何使用 Windows 服务控制台。

#### 将企业管理器作为 Windows 服务运行的先决条件

要将企业管理器作为 Windows 运行，请确保企业管理器已经安装，并在控制台模式下正常运行。

## 将企业管理器配置为 Windows 服务

本节介绍了如何在使用 Introscope-default JVM 系统参数运行的 Windows 计算机上注册单个企业管理器。

1. 停止企业管理器—请参阅[停止企业管理器](#) (p. 31)。
2. 在 `<EM_Home>/` 目录中的 `IntroscopeEnterpriseManager.lax` 文件中，将 `lax.stdin.redirect` 属性设置为空，然后保存文件。
3. 在 `IntroscopeEnterpriseManager.properties` 文件中（位于 `<EM_Home>/config` 目录下），将 `introscope.enterprisemanager.disableInteractiveMode` 属性设置为 `true`，然后保存文件。
4. 为企业管理器服务指定一个唯一的名称。默认情况下，服务名称是在 `<EM_Home>/bin` 目录下的 `EMService.conf` 中指定的。如果计算机上未配置其他服务，可以使用默认的服务名称。否则，请修改 `EMService.conf` 以使用以下属性为服务指定一个唯一的名称和显示名称：
  - `wrapper.ntservice.name=<unique Enterprise Manager name>`
  - `wrapper.ntservice.displayname=<Enterprise Manager display name>`
5. 将更改保存到文件中。
6. 要将企业管理器实例注册为服务，请运行 `<企业管理器主目录>/bin/EMCtrl32.bat` 注册脚本。

Windows 服务控制台显示企业管理器已配置为 Windows 服务。

为要作为服务运行的每个企业管理器重复这些步骤。

## 更改 Windows 服务属性

如果您必须在 `EMService.conf` 文件中更改配置属性，请先取消注册该服务，如以下部分中所述。要使更改生效，请更改和重新注册该服务。



## 取消注册企业管理器 Windows 服务

取消注册企业管理器服务：

- 在您更改 *EMService.conf* 属性文件之前。
- 以使企业管理器实例返回到控制台控件。
- 在卸载企业管理器实例之前。

取消注册企业管理器服务：

1. 停止企业管理器服务并关闭 Windows 服务 GUI。
2. 运行 `<EM_Home>/bin/EMCtrl32.bat unregister`。

**注意：**如果企业管理器服务或者 Windows 服务 GUI 处于活动状态，该服务仅标记为删除。这是标准的 Windows 服务行为，发生此情况的原因在于 Windows 注册表锁阻止删除服务。重新启动计算机后，服务将被删除。

## 停止并重新启动企业管理器 Windows 服务

要启动、停止和重新启动作为 Windows 服务运行的企业管理器，请使用 Windows 服务 GUI 中的标准控件。

## 在 Windows 上手动启动企业管理器

您可以通过以下任一方式启动企业管理器：

- 导航到“开始”、“程序”、“CA APM”、“管理”、“CA APM”、“企业管理器”。
- 运行位于 `<EM_Home>` 目录中的 *IntroscopeEnterpriseManager.exe*。

企业管理器将按照 `<EM_Home>/Introscope Enterprise Manager.lax` 中的属性设置进行启动，如 *Introscope Enterprise Manager.lax* 中所述。

## 在 UNIX 上启动企业管理器

在 UNIX 环境中运行企业管理器时，您可以手动启动企业管理器，也可以在 *nohup* 模式下运行它。

## 在 UNIX 上手动启动企业管理器

在 UNIX 上手工启动企业管理器：

- 要在 UNIX 上启动企业 管理器，请在命令提示符下键入以下命令来运行 `Introscope_Enterprise_Manager`：

```
'./Introscope Enterprise Manager'
```

企业管理器将按照 `<EM_Home>` 中的属性设置进行启动，如[属性文件参考](#) (p. 379)中所述。

企业管理器的输出显示在 UNIX shell 中。shell 不接受用户输入，除非您以 `nohup` 模式启动企业管理器，如以下部分中所述。

## 在 UNIX 上运行企业管理器控制脚本

通过运行用来启动、停止服务器应用程序及检查其状态的控制脚本，可以对企业 管理器进行管理。您可以使用 `EMCtrl.sh startup` 脚本启动和停止企业 管理器而无需直接使用 `'./Introscope Enterprise Manager'` 命令。

在 UNIX 上运行企业管理器控制脚本：

使用位于 `bin` 目录下的以下命令：

- `./EMCtrl.sh start`—这将启动企业 管理器。
- `./EMCtrl.sh stop`—这将停止企业 管理器。
- `./EMCtrl.sh status`—这将显示企业 管理器的状态。
- `./EMCtrl.sh help`—这将显示脚本支持的选项。

## 在 UNIX 上的 `nohup` 模式下运行企业管理器

UNIX `nohup` 命令运行一个命令，但不显示 `HUP`（挂起）信号的操作，这使得命令可以在发出该命令的用户注销后继续运行。在这种情况下，正常情况下应输出到终端的输出将输出到名为 `nohup.out` 的文件。

### 在 UNIX 上的 `nohup` 模式下运行企业管理器：

1. 在 `<EM_Home>/` 目录下的 `IntroscopeEnterpriseManager.lax` 文件中，将属性 `lax.stdin.redirect` 设置为空白，然后保存文件。
2. 在 `<EM_Home>/config` 目录下的 `IntroscopeEnterpriseManager.properties` 文件中，将 `introscope.enterprisemanager.disableInteractiveMode` 属性设置为 `true`，然后保存文件。
3. 使用以下命令启动企业 管理器：  

```
nohup Introscope_Enterprise_Manager&
```

**注意：**不要在未执行上述配置的情况下，以 `nohup` 模式运行企业 管理器。否则，企业 管理器可能无法启动，或者可以启动但会消耗过多的系统资源。

## 配置企业管理器以使用不同的 JVM

默认情况下，Introscope 组件使用与其绑定的 JVM。本节介绍了如何将企业管理器配置为使用不同的 JVM。

- 如果您使用 *Introscope Enterprise Manager.exe* 启动企业管理器，请编辑 *Introscope Enterprise Manager.lax* 中的 *lax.nl.current.vm* 属性，以指向所需的 JVM 可执行文件。
  - 可以使用可执行文件的绝对路径，也可以使用相对路径。
  - 在 Windows 上，必须对反斜线进行转义，并包括 JVM 可执行文件扩展名：*java.exe*（而非 *java*）。
- 如果将企业管理器作为 Windows 服务运行，请编辑 *EMService.conf* 中的 *wrapper.java.command* 属性以指向所需的 JVM 可执行文件。
  - 可以使用绝对路径；必须对反斜线进行转义。
  - 也可以使用相对路径；CA Technologies 建议您使用 UNIX 正斜线并以点斜线 (./) 开头。
  - 可执行文件是 *java*，而不是 *java.exe*。
- 如果您在 AS/400 上使用 *runem.sh* 脚本启动企业管理器，请编辑 *runem.sh* 中的 *JAVA\_HOME* 变量以指向所需的 JVM 根目录。
  - 请使用可执行文件的绝对路径而非相对路径。

## 关于企业管理器日志文件

企业管理器日志文件 *IntroscopeEnterpriseManager.log* 位于 <企业管理器主目录>/logs 目录下，用于记录有关 Introscope、CA CEM 以及 APM 数据库的运行情况和错误情况的信息：例如，关于启动和关闭的消息、某些类型的过度开销、第三方库、CA CEM 与企业管理器的通信以及有关特定 Introscope 和 CA CEM 属性的数据。

您可以配置企业管理器日志记录属性。有关更多信息，请参阅[日志记录](#) (p. 388)。

## 按日期或大小轮转企业管理器日志

您可以基于日期或大小轮转企业管理器日志，从而保留指定天数的信息并清除其余内容。

### 轮转企业管理器日志文件：

1. 打开 <企业管理器主目录>\config 目录中的 *IntroscopeEnterpriseManager.properties* 文件。
2. 找到 Logging Configuration 节。
3. 修改属性以实现所需的日志轮转。请参阅下面的详细说明。
4. 保存并关闭 *IntroscopeEnterpriseManager.properties* 文件。

根据所需的日志轮转行为，设置以下属性。

### 按日期或者每天轮转日志文件：

- 修改属性：
  - *log4j.appender.logfile=com.wily.org.apache.log4j.DailyRollingFileAppender*
  - *log4j.appender.logfile.DatePattern*

这些属性共同起作用，以基于日期轮转企业管理器日志文件。

*log4j.appender.logfile.DatePattern* 定义执行

*log4j.appender.logfile=com.wily.org.apache.log4j.DailyRollingFileAppender* 属性的日志轮转时间段。

例如，以下配置每天轮转日志文件：

```
log4j.appender.logfile=com.wily.org.apache.log4j.DailyRollingFileAppender
```

```
log4j.appender.logfile.DatePattern='yyyy-MM-dd
```

### 按时间间隔轮转日志文件：

- 修改属性 *log4j.appender.logfile.DatePattern*。此企业管理器属性决定了何时基于一天中的某时来轮转企业管理器日志文件。

下面是两个相关示例。

- 以下配置每小时轮转日志文件：

```
log4j.appender.logfile.DatePattern='yyyy-MM-dd-hh
```
- 以下配置每天午夜时轮转日志文件：

```
log4j.appender.logfile=com.wily.org.apache.log4j.DailyRollingFileAppender
```

```
log4j.appender.logfile.DatePattern='yyyy-MM-dd
```

按日志大小和数量轮转日志文件：

- 修改属性：
  - `log4j.appender.logfile.MaxBackupIndex`  
此属性决定企业管理器保存多少个备份日志文件。
  - `log4j.appender.logfile.MaxFileSize`  
此属性决定日志文件的最大大小。

例如，以下配置最多保留三个备份/轮转的企业管理器日志，每个日志的最大大小为 2 KB：

```
log4j.appender.logfile.MaxBackupIndex=3
log4j.appender.logfile.MaxFileSize=2KB
```

## 配置企业管理器配置目录

如果您有多个企业管理器，并且希望使用单个 Introscope 实例运行它们，可以为每个企业管理器创建一个单独的配置目录。对于每个企业管理器，创建 `config`、`logs`、`data` 和 `traces` 目录的副本。针对 `config` 目录的每个副本，在 `IntroscopeEnterpriseManager.properties` 文件中设置相应的属性以指向您的 `config`、`logs`、`data` 和 `traces` 的副本。

通过创建单独的配置目录，您可以将所有目录保留在一个 Introscope 实例中，同时为每个企业管理器维护单独的 `config`、`logs`、`data` 和 `traces` 目录。

为企业管理器指定一个不同的配置目录：

1. 打开 `IntroscopeEnterpriseManager.properties` 文件并修改以下属性：  
`introscope.enterprisemanager.directory.config=config`  
默认目录为 `config`，这是第一次安装 Introscope 时所创建的配置目录。更改此目录的位置，可以使用绝对路径（例如，`C:\\Introscope\\em1\\config`），也可以使用相对于 Introscope 安装目录的相对路径（例如，`config2`）。例如：  
`introscope.enterprisemanager.directory.config=C:\\Introscope\\em1\\config`  
**注意：**在 Windows 环境中，必须对反斜线进行转义（使用两个反斜线），这样路径才会有效。
2. 保存更改的 `IntroscopeEnterpriseManager.properties` 文件。

3. 打开 *Introscope Enterprise Manager.lax* 文件并修改以下属性：

```
lax.nl.java.option.additional
```

此属性修改 Java 命令行并且可以包含多个属性。使用您在步骤 1 中选择的 *config* 文件的位置。例如：

```
lax.nl.java.option.additional=-Xms512m -Xmx1024m -Djava.awt.headless=false  
-Dcom.wily.introscope.em.properties=C:\Introscope\em1\config
```

**注意：**此属性可以指向包含企业管理器属性文件的目录，也可以直接指向 *IntroscopeEnterpriseManager.properties* 文件。例如：

```
-Dcom.wily.introscope.em.properties=C:\Introscope\em1\config
```

或

```
-Dcom.wily.introscope.em.properties=  
C:\Introscope\em1\config\IntroscopeEnterpriseManager.properties
```

4. 将所做的更改保存到 *Introscope Enterprise Manager.lax* 文件中。
5. 重新启动企业 管理器。

## 停止企业管理器

停止企业 管理器后：

- 代理停止报告数据。
- SmartStor 不保存数据。
- 您从 Workstation 注销。
- 已连接到企业管理器的所有用户都被断开连接。

## 从终端窗口停止企业管理器

在企业 管理器终端窗口中输入：

```
iscopeshutdown
```

**注意：**必须启用交互模式才能使用此命令。在企业管理器属性文件中将 *introscope.enterprisemanager.disableInteractiveMode* 设置为 *false*。有关更多信息，请参阅[属性文件参考](#) (p. 379)。

## 从工作站停止企业管理器

如果您拥有关闭企业管理器的权限，可以在“管理模块编辑器”窗口中通过选择“管理器”、“关闭企业管理器”从 Workstation 停止企业 管理器。

## 企业管理器的自动关闭

如果企业管理器检测到写入磁盘时出错，且错误指示磁盘空间不足，它会自动关闭。如果已配置了故障切换，代理可以故障切换到其他企业管理器。有关详细信息，请参阅《CA APM Java 代理实施指南》或《CA APM .NET 代理实施指南》。

## 意外关闭后重新启动

**重要信息！** 本主题仅适用于 CA APM。如果您使用的是独立 CA Introscope（不含 TIM），请跳过本主题。

在大多数情况下，重新启动企业管理器与启动时的操作相同。但是，如果企业管理器是在错误状态下停止的（而非有计划地关闭），重新启动之前可能需要删除一些文件。

如果企业管理器因负载过重或文件处理错误而将自身关闭（崩溃），则 <企业管理器主目录>/cem/tess/badfiles 目录中可能会存在未处理的文件。如果在保留这些文件的情况下重新启动企业管理器，则重新启动时会处理它们。如果关闭是由这些文件中的错误或这些文件带来的负载导致的，则企业管理器在重新启动时开始再次处理这些文件时，可能会立即导致再次崩溃。

解决方案是在重新启动企业管理器之前删除该目录中的文件。

### 在崩溃后重新启动企业管理器：

**重要信息！** 按照此过程删除文件会丢失某些数据。您可能会丢失最近的缺陷详细信息、客户体验度量标准和统计信息。

1. 在运行 TIM 收集服务的企业管理器上，删除 <企业管理器主目录>/cem/tess/badfiles 目录中的文件。

这些文件是 xml 文件，并具有诸如  
*btstats-2010-01-05-23\_26\_13-172.16.252.20.xml* 和  
*defect-1262733968000057712-172.16.252.20.xml* 之类的名称

有关企业管理器服务（包括 TIM 收集服务）的信息，请参阅[分发企业管理器服务](#) (p. 244)。

2. 按照以下任一主题所述启动企业管理器：
  - [在 Windows 上启动企业管理器](#) (p. 23)
  - [在 UNIX 上启动企业管理器](#) (p. 25)
  - 在 OS/400 上启动企业管理器



**排除企业管理器上的多个崩溃问题:****症状:**

运行 TIM 收集服务的企业管理器崩溃并在重新启动时再次崩溃。

原因可能是与 TIM 相关的数据文件使企业管理器负载过重或文件中包含错误。

**解决方案:**

按[意外关闭后重新启动](#) (p. 32)中所述删除这些文件。

## 企业管理器 shell 和终端窗口命令

当企业管理器正在运行时，如果 *lax.stdin.redirect*（在“属性文件参考”中定义）设置为 *console*，则您可以在企业管理器终端窗口或 shell 中输入以下命令：

命令	结果
<code>iscopedebugpolling [true   false] [delay in seconds]</code>	定期将调试信息报告到日志中
<code>iscopehelp</code>	显示帮助屏幕
<code>iscopeshutdown</code>	关闭企业 管理器

**注意：**必须启用交互模式才能使用这些命令。在企业管理器属性文件中将 *introscope.enterprisemanager.disableInteractiveMode* 设置为 *false*。有关更多信息，请参阅[属性文件参考](#) (p. 379)。



## 第 3 章：配置企业管理器通信

---

本节中的信息包括企业管理器如何与 Introscope 环境中的其他组件通信、默认的通信行为以及用于配置企业管理器通信的选项。

此部分包含以下主题：

[默认的企业管理器通信通道](#) (p. 35)

[跨防火墙连接到企业管理器](#) (p. 39)

[针对 HTTPS 配置企业管理器 Web 服务器](#) (p. 39)

### 默认的企业管理器通信通道

默认情况下，企业管理器在端口 5001 与代理、Workstation、WebView 以及

企业管理器群集通信。

与企业管理器的所有套接字通信都进行了模糊处理，并且密码已加密。

企业管理器属性文件中的下列属性定义了通信通道及其用途：

- introscope.enterprisemanager.serversocketfactory.<ChannelName>
- introscope.enterprisemanager.port.<ChannelName>
- introscope.enterprisemanager.serversockets.reuseaddr
- introscope.enterprisemanager.enabled.channels

与企业管理器通信的每个代理都具有必须指定匹配值的类似属性。

同样，WebView 属性文件在

introscope.webview.enterprisemanager.tcp.port 属性中指定企业管理器端口。

**注意：**.NET 代理不支持与企业管理器的直接 SSL 连接。有关代理属性的信息，请针对您的环境根据需要参阅《CA APM Java 代理实施指南》或《CA APM .NET 代理实施指南》。

**详细信息：**

[了解企业管理器群集](#) (p. 83)

## 将通信通道重新绑定到正在使用中的端口

存在这样的套接字状态：套接字实际未被使用，但内存仍在使用中，从而使套接字不可使用。这些状态的示例有 `FIN_WAIT` 和 `TIME_WAIT`。

`introscope.enterprisemanager.serversockets.reuseaddr (p. 383)` 属性允许企业管理器通信通道重新绑定到正在使用中的本地端口。如果某个企业管理器套接字卡在了不可使用状态，但您仍希望启动企业管理器，则可以使用此功能。

**注意：**默认情况下不要启用此属性，仅当某个套接字处于不可使用状态时才使用此属性。在企业管理器启动后，您应当禁用该属性，因为系统可能存在端口正在使用的正当理由（例如，同一计算机上的某个收集器已经绑定到该端口）。

## 配置 SSL

针对 SSL 配置企业管理器是在 `IntroscopeEnterpriseManager.properties` 中进行的，这是通过启用安全的通信通道实现的。这可以作为默认的非安全通道的补充。

以下是同时启用了安全和非安全通信通道的示例。它在端口 `5001` 上设置了默认的非安全侦听程序，在端口 `5443` 上设置了安全的侦听程序：

```
# The enabled communication channels.
introscope.enterprisemanager.enabled.channels=channel1, channel2

# The default communication channel.
introscope.enterprisemanager.serversocketfactory.channel1=com.wily.isengard.postofficehub.link.net.server.DefaultServerSocketFactory
introscope.enterprisemanager.port.channel1=5001

# The secure communication channel.
introscope.enterprisemanager.serversocketfactory.channel2=com.wily.isengard.postofficehub.link.net.server.SSLServerSocketFactory
introscope.enterprisemanager.port.channel2=5443
# Location of a keystore containing certificates for authenticating the
Enterprise Manager to clients.
# Either an absolute path or a path relative to the config directory.
# On windows, backslashes must be escaped. 例如：
```

```
#
introscope.enterprisemanager.keystore.channel1=C:\\Introscope\\config\\in
ternal\\server\\keystore
introscope.enterprisemanager.keystore.channel2=internal/server/keystore
# The password for the keystore.
# Set this property to true to enable encryption of
introscope.enterprisemanager.keypassword.channel2
# Once introscope.enterprisemanager.keypassword.channel2 is encrypted,
# this property is automatically set to false.
#
# To change the existing password, enter the new password and set this property
to true.
# Note: If this property is set to true and the password is not changed, the
existing encrypted password will be encrypted again.
# If password field for a new channel is configured, add the corresponding
# plaintextpassword field and set it to true to enable encryption.
introscope.enterprisemanager.keypassword.channel2.plaintextpassword=true
introscope.enterprisemanager.keypassword.channel2=password
# Location of a truststore containing trusted client certificates.
# Either an absolute path or a path relative to the config directory.
# On windows, backslashes must be escaped. 例如:
#
introscope.enterprisemanager.truststore.channel1=C:\\Introscope\\config\\
internal\\server\\keystore
# A truststore is only needed if client authentication is required.
# Set this property to true to enable encryption of
introscope.enterprisemanager.trustpassword.channel2
# Once introscope.enterprisemanager.trustpassword.channel2 is encrypted,
# this property is automatically set to false.
#
# To change the existing password, enter the new password and set this property
to true.
# Note: If this property is set to true and the password is not changed, the
existing encrypted password will be encrypted again.
# If password field for a new channel is configured, add the corresponding
# plaintextpassword field and set it to true to enable encryption.
#
introscope.enterprisemanager.trustpassword.channel2.plaintextpassword=fal
se
# The password for the truststore
#introscope.enterprisemanager.trustpassword.channel2=password
# If no truststore is specified, the Enterprise Manager trusts all client
certificates.
```

## SSL 属性规则

必须在 *IntroscopeEnterpriseManager.properties* 中为企业管理器配置 SSL 服务器套接字，这是通过启用除默认通道之外的安全通道来实现的。

配置 SSL 属性时，请遵循以下规则：

- **keystore** 属性是 **keystore** 的位置。它应当包含企业管理器用来向客户端证明自己身份的一个证书。企业管器的默认密钥库包含一个自签署的证书，从本质上来讲，该证书不可靠。不过这没有关系，因为默认情况下，**Workstation** 和代理不会验证服务器证书。
- **keystore** 属性可以是绝对路径，也可以是相对于 *config* 目录的相对路径。
- 如果 *needclientauth* 属性设置为 *true*，则企业管理器要求客户端进行身份验证。
  - 必须为企业管理器配置一个 **truststore**。
  - 必须为代理和 **Workstation** 配置一个包含企业管理器信任的证书的 **keystore**。
  - 如果 *needclientauth = true*，且未配置 **truststore**，则企业管理器不会启动。
  - 这要求设置 **trustore** 属性。
- **truststore** 属性是 **truststore** 的位置。它包含信任的客户端的证书，并且仅在需要验证客户端时需要该属性。
  - 如果未指定 **truststore**，则信任所有客户端证书。
- *ciphersuites* 属性用来设置启用的密码套件。
  - 这可以用来启用匿名身份验证或避免数据加密。例如，对于匿名身份验证，请将密码套件设置为 **SSL\_DH\_anon\_WITH\_RC4\_128\_MD5**。例如：

```
introscope.enterprisemanager.ciphersuites.channel2=SSL_DH_anon_WITH_RC4_128_MD5
```
  - 一个特定的 JSSE 实现可以具有多个允许匿名身份验证的密码套件（它们都包含“*anon*”）。不过，密码套件对客户端和服务端是通用的，在这两者上都处于启用状态。
  - 指定不对数据进行加密的密码套件。例如：

```
introscope.enterprisemanager.ciphersuites.channel2=SSL_RSA_WITH_NULL_SHA
```

## 跨防火墙连接到企业管理器

默认情况下启用 HTTP 隧道。利用隧道技术，一个网络可以通过另一个网络的连接发送其数据。

要在 Workstation 上使用隧道传输，请连接到企业管理器的嵌入式 Web 服务器的端口。默认情况下，该端口为 8081。您可以在 *企业管理器属性* 文件中使用 *introscope.enterprisemanager.webserver.port* 属性配置该端口。有关更多信息，请参阅 [introscope.enterprisemanager.webserver.port](#) (p. 384)。

除了为企业管理器使用隧道技术外，您还可以将代理配置为使用隧道技术来发送信息。使用此功能，代理可以远程连接到企业管理器。有关代理 HTTP 隧道的详细信息，请参阅《CA APM Java 代理实施指南》。

## 针对 HTTPS 配置企业管理器 Web 服务器

您可以使用 Jetty 配置文件为企业管理器 Web 服务器配置 HTTPS。Jetty 文件是为进行高级配置而提供的，可以在 <企业管理器主目录>/config 目录中找到。

通过在 IntroscopeEnterpriseManager.properties 文件中取消对 introscope.enterprisemanager.webserver.jetty.configurationFile 属性的注释可以激活此文件。

有关配置的详细信息，请参阅以下主题：

- [默认的 Jetty 配置文件](#) (p. 40)和[修改 Jetty-config.xml 文件](#) (p. 40)。
- 有关详细信息，请访问 Jetty 网站，网址为：  
<http://docs.codehaus.org/display/JETTY/How+to+configure+SSL>。

## 了解 HTTPS 的工作原理

企业管理器 Web 服务器支持基于 SSL 的 HTTP 隧道。通过引入企业管理器中嵌入的 Jetty Web 服务器的可选 Jetty XML 配置文件，系统将实施此安全措施。

启动时，企业管理器加载 Jetty 配置文件，该文件在端口 8444 上设置安全的侦听程序。有了这个安全的侦听程序，Workstation 和代理可使用通向企业管理器 Web 服务器的 HTTPS 隧道，访问企业管理器。默认 Jetty 配置文件是 em-jetty-config.xml。

您可以使用 `IntroscopeEnterpriseManager.properties` 文件中的 [introscope.enterprisemanager.webserver.jetty.configurationFile](#) (p. 386) 属性，配置 Jetty 配置文件的名称和位置。

`introscope.enterprisemanager.webserver.port` 属性与 `IntroscopeEnterpriseManager.properties` 文件中的 `introscope.enterprisemanager.webserver.port` 属性一起使用。企业管理器在加载 Jetty 配置文件时，不会创建在 `introscope.enterprisemanager.webserver.port` 属性中定义的不安全的侦听程序。不过，您可以在 Jetty 配置文件中配置不安全的侦听程序。

**警告：** 如果您在 `em-jetty-config.xml` 文件中取消注释 `introscope.enterprisemanager.webserver.jetty.configurationFile` 属性和不安全的侦听程序端口，CA APM 的安全可能遭到危害。通知您的组织的应用程序安全人员，然后一起进行这些配置。

## 默认的 Jetty 配置文件

<企业管理器主目录>/config 目录中提供了默认的 `em-jetty-config.xml` 文件。

## 修改 em-jetty-config.xml 文件

您可以在 `em-Jetty-config.xml` 文件中修改 SSL 的许多组件。

有关 Jetty 的更多信息，请参阅

<http://docs.codehaus.org/display/JETTY/How+to+configure+SSL>。

- 通过更改 `port` 属性的值更改默认值为 8444 的 HTTPS 端口，例如在以下示例中：

```
<Set name="port">8444</Set>
```

- `introscope.config` 系统属性指定了 `config` 目录的位置。此位置是可配置的。企业管理器 Web 服务器可在启动时设置 `introscope.config` 系统属性。
- 默认情况下，SSL 侦听程序会配置为使用位于 `/internal/server/keystore`（相对于 `config` 目录的相对路径）的 `keystore`。此 `keystore` 包含一个不可靠的自签名证书。将您自己的 `keystore` 替换成一个包含由公认的证书颁发机构 (CA) 签署的证书的 `keystore`。
- 默认的 `keystore` 密码是 `password`。默认情况下，会对 `em-jetty-config.xml` 和 `webview-jetty-config.xml` 中的明文密码进行模糊处理。模糊化的密码以 `OBF` 开头。可以通过删除 `OBF` 来提供纯文本密码。有关详细信息，请参阅

<http://docs.codehaus.org/display/JETTY/How+to+configure+SSL>。



- 默认情况下，SSL 配置为接受自签名证书。SSL 不会验证客户端 URL 中的主机名是否与数字证书中的主机名匹配。此配置可确保 SSL 立即应用默认 keystore 中的不可信证书。如果您需要进行高度安全的身份验证，请创建一个包含可信证书的 keystore。然后，请在 XML 中设置以下属性，将默认 keystore 替换成您自己的 keystore：

```
<Set name="validateCertificates">true</Set>
<Set name="verifyHostnames">true</Set>
<Set name="keystore"><SystemProperty name="introscope.config"
default="./config" />/internal/server/keystore</Set>
<Set name="password">password</Set>
```

- 此外，若需要进行客户端身份验证，请创建一个包含客户端证书的 truststore，并在 XML 中设置以下属性，将默认 truststore 替换成您自己的 truststore：

```
<Set name="needClientAuth">true</Set>
<Set name="truststore"><SystemProperty name="introscope.config"
default="./config" />/internal/server/keystore</Set>
<Set name="trustPassword">password</Set>
```

- 如果需要进行客户端身份验证，必须为代理和 Workstation 配置一个包含企业管理器 Web 服务器信任的证书的 keystore。

要设置启用的密码套件，请将 *cipherSuites* 属性设置为一个密码套件列表：

```
<Set name="cipherSuites">
  <Array type="java.lang.String">
    <Item>SSL_DH_anon_WITH_RC4_128_MD5</Item>
  </Array>
</Set>
```

要使用 SSL，代理和 Workstation 必须具备与企业管理器相同的启用密码套件。您可以限定启用密码套件执行以下操作：

- 预防弱密码套件的漏洞
- 允许匿名连接
- 不对数据进行加密。
- 企业管理器使用 *maxThreads* 属性来限制企业管理器可为其提供服务的 HTTPS 代理连接的数量。如果线程不充足，企业管理器将无法从中识别连接的代理或进程度量标准。

使用 HTTPS 时，企业管理器仅服务于在 `maxThreads` 属性中配置的数量代理。允许的代理连接数是在 `apm-events-thresholds-config.xml` 文件中的 [introscope.enterprisemanager.agent.connection.limit property](#) (p. 428) 属性中配置的。请确保 `maxThreads` 值大于或等于 `introscope.enterprisemanager.agent.connection.limit` 值。当代理配置为通过 HTTPS 进行连接时，如果没有足够的线程，某些 HTTPS 代理可能不会显示在客户端中或报告任何度量标准。

**注意：**当 `maxThreads` 属性限制企业管理器服务的代理数时，企业管理器和代理日志将不包含有关非服务代理的错误、警告或消息。

### 修改 `em-Jetty-config.xml` 以重置默认标题大小

如果在访问 CEM 控制台时偶尔看到空白页，您可以重置默认请求标题大小限制 (4 KB)。在 `em-jetty-config.xml` 文件中重置标题大小限制。

请执行以下步骤：

1. 在 MOM 中浏览至 `em-jetty-config.xml` 文件，然后在文本编辑器中将其打开。

2. 通过下列行找到该部分：

```
<New class="com.wily.webserver.NonPESocketConnector">
```

3. 修改具有以下值的 "NonPESocketConnector"：

```
<set name="headerBufferSize">8192</set>
```

```
<Set name="RequestBufferSize">16384</Set>
```

修改后的部分将显示为以下代码段：

```
<Call name="addConnector">
```

```
<Arg>
```

```
<New class="com.wily.webserver.NonPESocketConnector">
```

```
<Set name="port">8081</Set>
```

```
<set name="headerBufferSize">8192</set>
```

```
<Set name="RequestBufferSize">16384</Set>
```

```
<Set name="ThreadPool">
```

```
<New class="org.mortbay.thread.BoundedThreadPool">
```

```
<Set name="minThreads">10</Set>
```

```
<Set name="maxThreads">100</Set>
```

```
<Set name="maxIdleTimeMs">60000</Set>
```

```
</New>
```

```
</Set>
```

```
</New>
```

```
</Arg>
```

```
</call>
```

4. 保存并关闭文件。

5. 浏览至每个 MOM 和收集器上的 `IntroscopeEnterpriseManager.properties` 文件。

6. 取消注释以下行：  
`introscope.enterprisemanager.webserver.jetty.configurationFile=em-jetty-config.xml`
7. 保存并关闭 IntroscopeEnterpriseManager.properties 文件。



# 第 4 章：配置企业管理器数据库

---

本节介绍 CA Introscope 内部数据库的配置选项。

有关 APM 数据库的信息，请参阅“[管理 APM 数据库 \(p. 45\)](#)”。

此部分包含以下主题：

[管理 APM 数据库 \(p. 45\)](#)

[配置 SmartStor 数据存储 \(p. 59\)](#)

[配置事务事件数据库位置和老化 \(p. 62\)](#)

[配置基准存储的位置 \(p. 63\)](#)

[备份 SmartStor、基准和事务事件数据 \(p. 63\)](#)

[使用 SmartStor 工具调整 SmartStor 数据 \(p. 65\)](#)

[清除 SmartStor 元数据 \(p. 71\)](#)

[清除 SmartStor 数据和元数据 \(p. 73\)](#)

[将 8.x 数据升级到 9.x \(p. 76\)](#)

## 管理 APM 数据库

本章包含与将数据导出和导入 APM 数据库有关的信息。您可以导入和导出整个数据库，也可以只导入和导出配置数据。

有关其他 CA Introscope 数据库（SmartStor 和事务事件数据库）的信息，请参阅[配置企业管理器数据库 \(p. 45\)](#)。

## 备份或还原数据库

备份和还原功能包括备份 APM 数据库和配置信息的功能。

例如，您可以在其他计算机上保留数据库的副本以达到保护数据的目的。为此，请先备份数据库，然后将数据库备份文件复制到其他计算机。

## APM 数据库的备份和还原过程

此列表显示了保护 CA CEM 数据所涉及的主要任务：

1. [了解先决条件](#) (p. 46)。
2. [定期备份数据库](#) (p. 47)。
3. [根据需要还原数据库](#) (p. 48)。

PostgreSQL 数据库的备份和还原实用工具以批处理文件（或 shell 脚本）的形式提供，可以在命令行中执行。

**注意：** APM 数据库包括 CA CEM 配置设置、用户和组、业务服务和事务定义，以及应用程序分类视图数据。

## 备份或还原前要求

**警告！** 如果在还原功能使用指定名称创建数据库之前已存在指定的数据库，则会破坏该数据库。

备份和还原要求：

- 您正在其上运行数据库脚本以用于备份或还原 PostgreSQL 数据库的计算机必须安装 PostgreSQL。如果需要，只要远程计算机也安装有 PostgreSQL，可以在该远程计算机上运行脚本。

在以下任何平台上还原 APM 数据库之前：

- OS/400 (IBM)
- Solaris x86

确定已在运行 dbrestore 脚本的计算机上设置 JAVA\_HOME 环境变量。

**适用于 JRE 1.6：** 设置 JAVA\_HOME 环境变量并使之指向 JRE 根文件夹。需要 JRE 1.6 或更高版本，路径不得包含空格。例如，如果 JRE 安装在 c:\program files\java\jre1.6.0 中，则将 JAVA\_HOME 设置为该路径的简短形式，可为 c:\progra~1\java\jre1.6.0。

## 备份数据库

备份实用工具创建 APM 数据库的 *.backup* 文件。可以自定义备份文件名。如果您没有指定文件名，脚本会使用数据库名称和文件名后缀 *backup* 创建备份文件。

### 备份 APM 数据库：

1. 导航到操作系统的 `database-scripts` 目录。
  - Linux: `<EM_Home>/install/database-scripts/unix/`
  - Windows: `<EM_Home>\install\database-scripts\windows\`
2. 打开命令行，根据您的操作系统运行以下脚本：
  - Windows: `dbbackup-postgres.bat`
  - Linux: `dbbackup-postgres.sh`

使用以下语法和参数：

```
[dbbackup-postgres.bat | sh dbbackup-postgres.sh] [dbserverhostip]  
[dbinstalldir] [dbname] [dbuser] [dbpassword] [dbport] [outputfile]
```

包括以下参数：

#### **dbserverhostIP**

承载数据库的计算机的 IP 地址。如果直接在此计算机上运行，可以指定 `localhost`。

#### **dbinstalldir**

APM 数据库的目录位置。

在 Linux 中，如果路径中有空格，则必须是转义或引号形式的路径。例如，对于 Linux，目录 `/root/Introscope Enterprise Manager` 可以显示为 `/root/Introscope\ Enterprise\ Manager`。

如果未更改默认值，则位置如下所示：

Linux: `opt/database`

Windows: `<EM_Home>\database`

#### **database\_name**

指定数据库实例名称。如果使用的是 PostgreSQL 并且没有更改默认值，应将此参数设置为 `cemdb`。如果使用的是 Oracle，应将该参数设置为 Oracle 系统标识符 (SID)。

#### **dbuser**

指定与 APM 数据库关联的数据库用户的用户名。如果使用的是 PostgreSQL 并且没有更改默认值，应将此参数设置为 `admin`。如果使用的是 Oracle，应将该参数设置为 APM 数据库架构所有者。

**注意：**这不是 PostgreSQL 数据库管理员的用户名。

**password**

指定与 APM 数据库关联的数据库用户的密码。

**port\_number**

指定数据库用来与企业管理器和其他组件通信的端口号。如果使用的是 PostgreSQL 并且没有更改默认值，应将此参数设置为 5432。如果使用的是 Oracle 和默认侦听程序端口，则应将该参数设置为 1521。

**dbbackupdir**

您要保存数据库备份文件的现有目录位置。对于 Linux，如果路径中有空格，则必须是转义形式的路径。例如，对于 Linux，目录 `/root/Introscope Enterprise Manager` 可以显示为 `/root/Introscope\ Enterprise\ Manager`。

目录不能用引号引起来，并且不能有结束斜杠。

**outputfile**

(可选) 数据库备份文件的名称。如果没有指定该参数，脚本会使用提供的数据库名称生成名为 `dbname.backup` 的文件。按标准约定，备份文件名后缀是 `.backup`，但不是必需的。

以下是在 `/opt/database/backups` 目录中生成 `cemdb.backup` 文件的示例：

```
sh dbbackup-postgres.sh 127.0.0.1 /opt/database cemdb admin quality  
5432 ./backups
```

3. 在备份过程完成后，系统将显示一条确认消息。

如果脚本遇到错误，通常是由于以下原因所致：

- 数据库名称不正确。
- 未安装 PostgreSQL。
- APM 数据库的位置不正确。

## 还原数据库

还原实用工具允许您将先前备份的 APM 数据库备份文件还原到当前系统。例如，您可以在系统崩溃或硬盘发生故障之后通过还原数据库进行恢复。

**警告！** 如果在还原功能使用指定名称创建数据库之前已存在指定的数据库，则会破坏该数据库。

**注意：** 如果数据库在 UNIX 计算机上，还原过程也会升级数据库。



**注意：**还原数据库所需的时间与数据库大小直接相关。大型数据库还原时间更长，此外还原时间还取决于计算机性能和内存。例如，1 GB 数据库还原时间可能需要 1 到 2 个小时，具体取决于计算机资源。

#### 还原 APM 数据库：

1. 确保没有用户连接到数据库。如果有用户连接到数据库，则无法还原该数据库。
2. 导航到操作系统的 `database-scripts` 目录。
  - Linux: `<EM_Home>/install/database-scripts/unix/`
  - Windows: `<EM_Home>\install\database-scripts\windows\`
3. 打开命令行，根据您的操作系统运行以下脚本：
  - Windows: `dbrestore-postgres.bat`
  - Linux: `dbrestore-postgres.sh`

使用以下语法和参数：

```
[dbrestore-postgres.bat | sh dbrestore-postgres.sh][dbserverhostip]
[dbinstalldir] [dbserviceuser] [dbservicepassword] [dbname] [dbuser]
[dbpassword] [dbport] [backupfile]
```

包括以下参数：

#### **dbserverhostIP**

承载数据库的计算机的 IP 地址。如果直接在此计算机上运行，可以指定 `localhost`。

#### **dbinstalldir**

APM 数据库的目录位置。

在 Linux 中，如果路径中有空格，则必须是转义或引号形式的路径。例如，对于 Linux，目录 `/root/Introscope Enterprise Manager` 可以显示为 `/root/Introscope\ Enterprise\ Manager`。

如果未更改默认值，则位置如下所示：

Linux: `opt/database`

Windows: `<EM_Home>\database`

#### **dbserviceuser**

PostgreSQL 管理员用户名。默认情况下为 `postgres`。

#### **dbservicepassword**

与 `dbserviceuser` 关联的密码。（PostgreSQL 管理员密码。）

### **database\_name**

指定数据库实例名称。如果使用的是 PostgreSQL 并且没有更改默认值，应将此参数设置为 *cemdb*。如果使用的是 Oracle，应将此参数设置为 Oracle 系统标识符 (SID)。

### **dbuser**

指定与 APM 数据库关联的数据库用户的用户名。如果使用的是 PostgreSQL 并且没有更改默认值，应将此参数设置为 *admin*。如果使用的是 Oracle，应将此参数设置为 APM 数据库架构所有者。

**注意：**这不是 PostgreSQL 数据库管理员的用户名。

### **password**

指定与 APM 数据库关联的数据库用户的密码。

### **port\_number**

指定数据库用来与企业管理器和其他组件通信的端口号。如果使用的是 PostgreSQL 并且没有更改默认值，应将此参数设置为 5432。如果使用的是 Oracle 和默认侦听程序端口，则应将此参数设置为 1521。

### **backupfile**

数据库备份文件的目录位置和名称。

以下是从 */opt/database/backups* 目录还原 *cemdb.backup* 文件的示例：

```
sh dbrestore-postgres.sh 127.0.0.1 /opt/database postgres C@wilyapm90 cemdb
admin quality 5432 ./backups/cemdb.backup
```

4. 在还原过程完成后，系统将显示一条确认消息。

如果您遇到错误：

- 最常见的错误是仍有用户连接到数据库。您可以重新启动 PostgreSQL 服务器以断开引发错误的连接。
- 如果出现指明数据库不存在的错误，这是正常现象。这意味着在还原过程中系统正使用该脚本创建数据库。

## 导出或导入数据库配置

在某些情况下，不会在首次安装时将 CA CEM 系统置入生产环境中。例如，公司策略可能要求所有新硬件和软件在进入生产网络之前，应先在测试实验室中进行安装。

一旦在 QA 或测试环境中建立并测试了 CA CEM 配置，使用 CA CEM 导出和导入，即可将经验证的配置移到生产环境中。

配置信息包括用户、用户组、业务服务和事务。

### 数据库配置的导出和导入过程

此列表显示了导出 CA CEM 配置所涉及的主要任务：

1. [了解先决条件](#) (p. 51)。
2. [导出](#) (p. 52)CA CEM [配置](#) (p. 52)。
3. [导入](#) (p. 53)CA CEM [配置](#) (p. 53)。

导出和导入实用工具以批处理文件（或 shell 脚本）的形式提供，可以在命令行执行。

有关导入和导出业务事务定义的信息，请参阅《CA APM 事务定义指南》。

有关备份和还原 APM 数据库中所有信息（不仅仅是配置信息）的信息，请参阅[备份或还原数据库](#) (p. 45)。

### 导出或导入数据库配置数据之前要求

**警告！** 强烈建议您在尝试运行这两个实用工具之前先备份 APM 数据库（特别是导入实用工具，因为它在重建配置之前会破坏现有配置）。导入脚本会破坏数据库，从而生成一个仅包含旧数据库配置数据的数据库。有关详细信息，请参阅[备份或还原数据库](#) (p. 45)。

导出和导入要求：

- 您必须在安装有 APM 数据库的计算机上运行脚本。
- 您必须在企业管理器安装程序放置脚本的位置运行脚本，因为脚本所引用的文件是相对于这些位置的。
- 在运行这些脚本之前，请关闭到 APM 数据库的所有连接。关闭企业管理器，关闭任何数据库管理工具（例如，pgAdmin），以及确定所有用户均已注销或已关闭 CEM 控制台。尽管您不一定必须禁用 TIM，但请注意需要在导入之后重新启用它们。

- **适用于 JRE 1.6 或更高版本：** 设置 JAVA\_HOME 环境变量并使之指向 JRE 根文件夹。需要 JRE 1.6 或更高版本，路径不得包含空格。例如，如果 JRE 安装在 `c:\program files\java\jre1.6.0` 中，则将 JAVA\_HOME 设置为该路径的简短形式，可为 `c:\progra~1\java\jre1.6.0`。
- 如果要从 CA CEM 的早期版本导入配置，请注意，可以在 Linux 上导入任何早期版本，但在 Windows 上只能导入 5.0 版（或更高版本）。导入实用工具会自动将数据库架构从早期版本升级到当前版本。

## 导出 APM 数据库配置

`configexport.bat` 或 `configexport.sh` 脚本会创建包含所有 CA CEM 配置信息的 XML 文件。配置信息包括用户、用户组、业务服务和事务。导出配置信息使您能够移动测试或实验室系统的数据，以用作生产系统的基础。

### 导出 APM 数据库配置：

1. 设置 JAVA\_HOME 环境变量。
2. 导航到您操作系统的 `<EM_Home>/install/database-scripts` 目录。例如：

```
cd /home/Introscope9.0.5.0/install/database-scripts/unix
```

3. 打开命令窗口或终端窗口，在 Windows 上运行 `configexport.bat`，或在其他平台上运行带以下参数的 `configexport.sh`：

```
ConfigExport <dbhostIP> <database_name> <dbuser> <password> <port_number>  
<databasetype> <export-file>
```

#### dbhostIP

指定承载数据库的计算机的 IP 地址。不得在该命令中使用 localhost。

#### database\_name

指定数据库实例名称。如果使用的是 PostgreSQL 并且没有更改默认值，请将此参数设置为 `cemdb`。如果使用的是 Oracle，请将参数设置为 Oracle 系统标识符 (SID)。

#### dbuser

指定与 APM 数据库关联的数据库用户的用户名。如果使用的是 PostgreSQL 并且没有更改默认值，请将此参数设置为 `admin`。如果使用的是 Oracle，请将参数设置为 APM 数据库架构所有者。

**注意：**这不是 PostgreSQL 数据库管理员的用户名。

#### password

指定与 APM 数据库关联的数据库用户的密码。

**port\_number**

指定数据库用来与企业管理器和其他组件通信的端口号。如果使用的是 PostgreSQL 并且没有更改默认值，应将此参数设置为 5432。如果使用的是 Oracle 和默认侦听程序端口，则应将该参数设置为 1521。

**databasetype**

指定您要使用的数据库的类型。将此参数设置为 postgres 或 oracle。

**export-file**

指定包含导出数据的 xml 文件的绝对路径和文件名。

例如，要在 Linux 上运行 *configexport* 程序，将使用与以下内容类似的命令行：

```
./configexport.sh 197.168.144.10 arcade apmdba mypwd 1521 oracle  
/home/apmdba/export_oracle.xml
```

4. 在配置导出过程完成后，系统将显示一条确认消息。

## 导入 APM 数据库配置

您可以将配置设置从一个 APM 数据库导入另一个数据库。例如，您可以使用 *configimport.bat* 或 *configimport.sh* 程序将数据库配置从 QA 系统导入生产系统。导入的配置设置包括用户、用户组、业务服务和事务。

APM 数据库配置导入过程执行以下操作：

- 删除先前的数据库配置信息（关于操作员、用户、组、业务服务流程和事务定义），并且将它替换成已导入的配置数据。
- 删除缺陷、报告和统计数据并且不替换它。

**注意：**您可以导入 CA CEM 早期版本中的配置。例如，您可以下载并导出 CA CEM 4.1 中的配置，然后将其上载并导入 CA CEM 4.2（仅限 Linux）。

**请执行以下步骤：**

1. 导航到您操作系统的 `<EM_Home>/install/database-scripts` 目录。例如：

```
cd /home/Introscope9.0.5.0/install/database-scripts/unix
```

2. 打开命令窗口或终端窗口，在 Windows 上运行 `configimport.bat`，或在其他平台上运行带以下参数的 `configimport.sh`：

```
ConfigImport -dbhost <主机名> -dbname <数据库名称> -dbport <端口号>
-databasetype <数据库类型> -dbuser <数据库用户> -dbpassword <密码>
-dbscriptsdir <目录> -importfile <导入文件名> -targetRelease <目标版本>
-dbserviceuser <数据库服务用户> -dbservicepwd <数据库服务密码>
[-postgresinstalldir <PostgreSQL 安装目录>] [-nolog] [-jdbcbatchsize <jdbc 批
处理大小>] [-promptbeforeimport true|false] [-is64Bit true|false]
```

#### **dbhost**

指定用于承载数据库的计算机的主机名或 IP 地址。不得在该命令中使用 `localhost`。

#### **dbname**

指定数据库实例名称。如果使用的是 PostgreSQL 并且没有更改默认值，则将此参数设置为 `cemdb`。如果使用的是 Oracle，则将此参数设置为 Oracle 系统标识符 (SID)。

#### **dbport**

指定数据库用来与企业管理器和其他组件通信的端口。如果使用的是 PostgreSQL 并且没有更改默认值，则将此参数设置为 5432。如果使用的是 Oracle 和默认侦听程序端口，则将此参数设置为 1521。

#### **databasetype**

指定您要使用的数据库的类型。将此参数设置为 `postgres` 或 `oracle`。

#### **dbuser**

指定与 APM 数据库关联的数据库用户的用户名。如果使用的是 PostgreSQL 并且没有更改默认值，则将此参数设置为 `admin`。如果使用的是 Oracle，则将此参数设置为 APM 数据库架构所有者。

#### **dbpassword**

指定与 APM 数据库关联的数据库用户的密码。

**dbscriptsdir**

指定特定于数据库的 SQL 脚本的目录。例如，如果使用的是 Oracle 数据库架构，则使用 <企业管理器主目录>/install/oracle/database-scripts，或者如果使用的是 PostgreSQL 数据库，则使用 <企业管理器主目录>/install/database-scripts。

**importfile**

指定包含导入数据的 xml 文件的绝对路径和文件名。

**dbserviceuser**

指定 PostgreSQL 管理服务用户帐户。默认管理服务帐户为 *postgres*。该参数不适用于 Oracle。

**dbservicepwd**

指定 PostgreSQL 管理服务用户帐户的密码。

**postgresinstalldir**

(可选)指定使用 PostgreSQL 时 APM 数据库的目录位置。在 Linux 或 Solaris 上，必须将路径用引号引起来，或者如果路径包含空格，还必须包含转义字符。例如，如果该目录是 */root/Introscope Enterprise Manager*，您可以指定位置 *"/root/Introscope Enterprise Manager"* 或 */root/Introscope\ Enterprise\ Manager*。

如果没有更改默认值，则在 32 位 Linux 或 Solaris 上位置为 *opt/database*，在 64 位 Linux 或 Solaris 上位置为 *opt/database/postgres/8.3-community*，在 Windows 上位置为 <企业管理器主目录>\database。

该参数不适用于 Oracle。

**targetRelease**

指定要导入的目标版本。例如，您可以导入 9.0.5.1 配置文件，但可能希望数据库升级到 9.1.0.0。

**nolog**

(可选)指定您要关闭指向标准输出 (StdOut) 的记录。

**jdbcbatchsize**

(可选)指定可一次通过 Java 数据库连接 (JDBC) 传输的数据包的最大大小。默认值为 2500。

### **promptbeforeimport**

(可选) 指定您是否希望 *configimport* 程序在开始导入数据之前显示提示信息。如果要显示提示, 可将此参数设置为 *true*。默认值为 *false*。

### **is64Bit**

(可选) 指定 PostgreSQL 数据库是 32 位还是 64 位。如果要将数据导入 64 位 PostgreSQL 数据库, 可将此参数设置为 *true*。该参数不适用于 Oracle 数据库。

例如, 要在 Linux 和 PostgreSQL 数据库上运行 *configimport* 程序, 将使用与以下内容类似的命令行:

```
./configimport.sh -dbhost sfqa07 -dbname cemdb -dbport 5432 -databasetype postgres -dbuser admin -dbpassword mypassword -dbscriptsdir /apps/Introscope/install/database-scripts -importfile /tmp/apm_data.xml -dbserviceuser postgres -dbservicepwd %pas5w0rd -postgresinstalldir /opt/database -promptbeforeimport true
```

导入脚本会执行初始验证检查以确保 XML 格式正确。

导入脚本提供的该选项可用于更彻底地验证 XML 以确保正确处理 XML 内容。输入 Y 可执行验证, 或输入 N 可继续导入而不验证 XML 内容。

**注意:** 第二个验证可能需要一段时间, 具体取决于 XML 文件的大小。确保 XML 数据正确导入非常重要; 否则会发生错误。

该脚本显示进度消息, 并会在验证完成、导入开始和导入完成时显示消息。

如果任何一个验证检查失败, 都会显示错误消息, 而且不会继续进行配置导入。如果这两个验证检查都成功, 脚本导入指定的数据库配置数据。

**重要信息!** 配置导入不导入现有 HTTP 分析程序插件配置。要手工安装插件, 请使用 CEM 控制台。



## 将 APM 数据库移至其他操作系统

在某些情况下，在升级过程中需要将 APM 数据库从一台计算机移至另一台计算机或从一个平台移至另一个平台。例如，您可能需要将 APM 数据库从 Windows 或 Linux 上的 PostgreSQL 移至 Solaris 上的 PostgreSQL。要将数据库从一个平台移至另一个平台，需要从源数据库中导出业务事务和配置数据，然后将这些数据导入新平台上的目标数据库中。或者，您可以使用 *dbbackup-postgres* 和 *dbrestore-postgres* 实用工具创建现有 PostgreSQL 数据库的完整备份，然后在新计算机上还原该数据库。

有关从 PostgreSQL 数据库导出和导入数据或使用 *dbbackup-postgres* 和 *dbrestore-postgres* 实用工具的详细信息，请参阅《CA APM 配置和管理指南》。有关[将 PostgreSQL 数据库中的数据迁移到 Oracle 数据库](#) (p. 57) 的信息，请参阅《CA APM 安装和升级指南》。

## 将 PostgreSQL 数据库中的数据迁移到 Oracle 数据库

如果要升级数据库，并将数据从 PostgreSQL 迁移到 Oracle 数据库，请首先进行升级。例如，如果您的组织采用 Oracle 作为标准化数据库平台，需要将 APM 数据库迁移到 Oracle 以启用生产级别的监控。如果要将在 PostgreSQL 中源数据库内的现有数据移至 Oracle 中的目标数据库，可以使用 CA APM 迁移实用工具指定源数据库和目标数据库。

### 从 PostgreSQL 数据库迁移到 Oracle 数据库：

1. 通过查看升级方案和升级途径规划和准备升级。
2. 创建包含所有组件的备份副本。
3. 使用交互式或静默企业管理器安装程序升级企业管理器和 APM 数据库。
4. 导航到 `<EM_Home>/install/migration` 目录。
5. 使用以下参数，根据您的操作环境运行 *migration.bat* 或 *migration.sh* 脚本：

```
migration -srcDatabaseName <database_name> -srcDatabaseType <database_type>
-srcHost <hostname> -srcPort <port_number> -srcUser <username> -srcPassword
<password> -tgtDatabaseName <datatargetname> -tgtDatabaseType
<database_type> -tgtHost <hostname> -tgtPort <port_number> -tgtUser
<username> -tgtPassword <password>
```

#### srcDatabaseName

指定源数据库的名称。如果使用的是默认设置，则数据库名称为 *cemdb*。

#### srcDatabaseType

指定源数据库的类型。在本版本中，唯一的有效值为 *postgres*。

**srcHost**

指定源数据库所在数据库服务器的主机名或 IP 地址。

**srcPort**

指定连接到源数据库的端口号。如果使用的是默认设置，则端口为 5432。

**srcUser**

指定源数据库的数据库用户名。如果使用的是默认设置，则数据库用户名为 *admin*。

**srcPassword**

指定源数据库中数据库用户的密码。

**tgtDatabaseName**

指定目标数据库的名称或服务帐户标识符。对于 Oracle 数据库，目标数据库的名称是唯一系统标识符 (SID)。

**tgtDatabaseType**

指定目标数据库的类型。在本版本中，唯一的有效值为 *oracle*。

**tgtHost**

指定目标数据库的数据库服务器的主机名或 IP 地址。

**tgtPort**

指定用于连接到目标数据库的端口号。如果使用的是默认设置，则端口为 1521。

**tgtUser**

指定目标数据库的数据库用户名。

**tgtPassword**

指定目标数据库中数据库用户的密码。

**注意：**所有参数均区分大小写，在运行迁移工具时需要使用。

例如，要将 PostgreSQL 数据库 *cemdb* 中的数据迁移到 Linux 计算机上 SID 为 *orcl*、架构所有者为 *apmdb* 的 Oracle 数据库，命令行应类似于以下行：

```
./migration.sh -srcDatabaseName cemdb -srcDatabaseType postgres -srcHost nyc16 -srcPort 5432 -srcUser admin -srcPassword quality -tgtDatabaseName orcl -tgtDatabaseType oracle -tgtHost nyc23 -tgtPort 1521 -tgtUser apmdb -tgtPassword cent3R
```

- 查看 `logs` 目录中的 `migration.log` 文件，以确认已成功迁移该架构，或排除迁移发生的问题。例如，导航到 `<EM_Home>/install/migration/logs` 目录。

**注意：**您可以通过修改 `<EM_Home>/install/migration/log4j-migration.properties` 文件中的 `log4j.appender.logfile.File` 属性来修改 `migration.log` 文件的位置。有关自定义迁移和日志文件属性的详细信息，请参阅自定义迁移属性。

## 数据库故障排除

该主题提供一些提示，帮助您排除数据库的故障。

### 症状：

在运行我的 APM 数据库的计算机上，我看到许多数据库（PostgreSQL 或 Oracle）进程。是否正常？

### 解决方案：

数据库进程（PostgreSQL 或 Oracle）是为与 APM 数据库的每个客户端连接创建的。因此，看到许多单独的数据库进程同时运行是很正常的。

## 配置 SmartStor 数据存储

SmartStor 在处于生产状态时始终记录所有应用程序的性能数据（Introscope 度量标准），这不需要外部数据库。这使得您可以对历史数据进行分析，以便确定应用程序停机的根本原因或执行容量分析，这都不需要外部数据库。安装 Introscope 时将以默认设置启用 SmartStor。

每小时一次，SmartStor 会准点把 `.spool` 文件转化成 `.data` 文件，以优化查询处理。

每天一次，在午夜，SmartStor 会重新格式化基于企业管理器层设置的历史度量标准数据，并且删除过时的度量标准和元数据。

以下是 `IntroscopeEnterpriseManager.properties` 文件中的默认层设置：

```
introscope.enterprisemanager.smartstor.tier1.frequency=15
```

```
introscope.enterprisemanager.smartstor.tier1.age=7
```

```
introscope.enterprisemanager.smartstor.tier2.frequency=60
```

```
introscope.enterprisemanager.smartstor.tier2.age=30
```

introscope.enterprisemanager.smartstor.tier3.frequency=900

introscope.enterprisemanager.smartstor.tier3.age=365

在 SmartStor 使用的存储层次结构中，假定最近的数据访问最频繁并且拥有最高的解析度。下面是基于以前列出的默认属性设置的数据解析度：

将 1 周的数据存储在 15 秒块中（未压缩）

将 30 天的数据存储在 1 分钟（60 秒）块中（压缩）

将 1 年的数据存储在 15 分钟（900 秒）块中（压缩）

**重要信息！** 配置 SmartStor 以写入专用磁盘，以便避免严重影响企业管理器性能和响应速度。与运行在主机上的其他企业管理器活动或其他进程争夺磁盘可以导致性能不尽如人意。

当您为 SmartStor 数据设置专用磁盘时，将该属性设置为 true。在默认情况下企业管理器安装程序把此属性设为 false。请参阅 [introscope.enterprisemanager.smartstor.dedicatedcontroller](#) (p. 396)。

以下几部分提供了 SmartStor 规划和配置说明：

- [确定 SmartStor 系统要求](#) (p. 61)
- [指定 SmartStor 数据层值](#) (p. 61)

## 有关 SmartStor 层如何工作的详细信息

SmartStor 中的层定义存储度量标准数据的时间长度。您最多可拥有三层，每层均具有相同的或增加的频率周期。第 1 层是最短的老化期，由频率（秒）和期限（天）组成。基于第 1 层的频率配置来配置第 2 层。将第 2 层看作第 1 层的“摘要”，第 3 层则是第 2 层的“摘要”。

例如：

	频率 (15 秒的倍数)	期限 (天)
第 1 层	15	7
第 2 层	15	14
第 3 层	30	10

每晚会对 SmartStor 进行重新制定周期，并收集度量标准数据的存档文件（称为 A1）。新存档 A1 将进入第 1 层“时间段”，并停留 7 天。到第 8 天，A1 将被提升到第 2 层。存储频率不变。同样地，频率表示度量标准报告粒度。A1 在第 2 层中再存储 14 天。到第 15 天，A1 将被提升到第 3 层。数据频率转换为 30 秒。如果要查看度量标准数据，则其增量为 30 秒，而不是 15 秒。A1 将在第 3 层中停留 10 天，此后从 SmartStor 中删除。A1 会在 SmartStor 中存储总共 31 天。

## 自动删除元数据

在 SmartStor 再周期化期间，企业管理器会自动删除没有关联的度量标准数据点的元数据（度量标准和代理说明）。此进程释放磁盘和内存空间，以在 SmartStor 层化期间重新利用。在 `IntroscopeEnterpriseManager.properties` 文件中设置 SmartStor 层时间段。

企业管理器不删除手工安装在 Workstation 中的历史代理，包括 SmartStor 中没有度量标准数据的代理。

## 确定 SmartStor 系统要求

您可以使用 SmartStorSizing 电子表格来确定 SmartStor 系统要求。可以[从 CA Support 站点下载该电子表格](#)。

您可以为度量标准数目使用不同的值或者为数据层使用不同的时期和老化范围来进行试验。结果显示为 GB 大小使用情况。

SmartStor 性能受操作系统、JVM 和文件系统选择的影响。

确定适当的数据层频率和老化期后，在相应的 SmartStor 属性中配置规范。

## 指定 SmartStor 数据层值

指定三个数据层以配置 SmartStor 数据存储。每个数据层包含一个属性对：

- 存储频率（以秒为单位）
- 数据老化期（以天为单位）

以下是频率和老化值的规则：

- 存储频率必须是 15 秒的倍数。
- 频率不能大于 1800 秒（30 分钟）。

- 每个层的频率必须是前一个层频率的偶倍数。此倍数可以是一；每个层可以有同样的频率。
- 天数不能为零。
- 三个层都必须定义，您不能定义三个以上的层。

请执行以下步骤：

1. 打开 `IntroscopeEnterpriseManager.properties` 文件。
2. 对于 `introscope.enterprisemanager.smartstor.tier1.frequency` 属性，输入适当的值。
3. 对于属性 `introscope.enterprisemanager.smartstor.tier1.age`，请输入适当的值。
4. 对剩余的两个数据层属性对执行相同的步骤。
5. 重新启动企业管理器。

**注意：**如果您更改自己的数据层，然后重新启动企业管理器，SmartStor 会尝试根据新的配置调整数据。SmartStor 可能会最多丢失一天的数据。

## 配置事务事件数据库位置和老化

企业管理器将事务跟踪和其他事件数据存储存储在事务事件数据库中。

事务事件数据库的位置是在安装企业管理器期间配置的。除非您在安装期间指定了一个不同的位置，否则将在 `<企业管理器主目录>/traces` 目录中创建该数据库。在安装后，您可以通过 `IntroscopeEnterpriseManager.properties` 中的 `introscope.enterprisemanager.transactionevents.storage.dir` 属性选择一个不同位置。

Introscope 对事务事件数据的保留天数是在安装企业管理器期间配置的。默认值为 14，可以通过 `introscope.enterprisemanager.transactionevents.storage.max.data.age` 属性进行更改。

**注意：**增加 Introscope 对事件数据的保存时间会增加系统开销和磁盘存储空间要求。

## 配置基准存储的位置

默认情况下，Introscope 将度量标准基准信息存储在企业管理器计算机上的 `<EM_Home>/data/baselines.db` 中。

企业管理器安装程序没有提供用于为基准存储选择其他位置的选项。不过，您可以在企业管理器属性文件中的 `introscope.enterprisemanager.dbfile` 属性中为 `baselines.db` 定义一个不同的位置。

有关 Introscope 如何使用度量标准基准启用应用程序运行状况的高级别指示器的信息，请参阅《CA APM Workstation 用户指南》。

## 备份 SmartStor、基准和事务事件数据

停止企业管理器后，您可以备份和操作企业管理器 SmartStor、基准和事务事件数据文件。

默认情况下，企业管理器将所有 SmartStor 和基准数据存储在 `<EM_Home>/data` 目录中。

用于 SmartStor 的企业管理器数据文件包括：

- `metrics.metadata` 文件，它跟踪有关代理已报告的各种度量标准的信息。（最重要的是，`metrics.metadata` 跟踪度量标准的名称。）
- 以 `.spool` 结尾的文件（例如，`125122680000.spool`），用于保存自企业管理器上次执行“缓冲池到查询”转换后发送到 SmartStor 的 15 秒度量标准值。`.spool` 文件从不保存超过一小时的数据量。
- 以 `.data` 结尾的文件（例如，`125118360000.data`），用于以 SmartStor 的只读查询优化格式保存度量标准值。这些文件将数据点值保留 15 秒、1 分钟和 1 小时。

基准数据的企业管理器数据文件包括：

- `baselines.db`。

默认情况下，企业管理器将所有事务跟踪和事件数据保存在 `<EM_Home>/traces` 目录中。事务事件数据的企业管理器数据文件为：

- `traces_YYYYMMDD.db`。例如：`traces_20090923.db`。

当企业管理器运行时，它期望能够无错地创建和写入 `metrics.metadata`、`.spool` 和 `.data` 文件。因此，CA Technologies 强烈建议您在移动、复制和使用企业管理器数据之前停止企业管理器。

**警告！** 在企业管理器正在运行时复制或编辑企业管理器数据文件会导致数据丢失。

关闭企业管理器后，您可以执行以下所有操作来备份和操作企业管理器数据：

- 将数据保存到备份介质
- 使用 Smartstor 工具编辑 SmartStor 数据  
有关 SmartStor 工具的更多信息，请参阅[使用 SmartStor 工具调整 SmartStor 数据](#) (p. 65)。
- 压缩数据
- 还原数据
- 复制数据以便其他企业管理器脱机查看。

## 创建仅供查询的副本群集

您可以将 SmartStor 数据文件复制到副本群集计算机，以便用作仅供查询的源历史（非实时）数据。

**注意：** CA Technologies 建议，仅在生产环境中且服务需求大大超出运行群集的硬件的容量时创建副本群集。

**请执行以下步骤：**

1. 创建您的生产或测试群集的确切副本。  
将一台计算机用于 MOM，将另一台计算机用于群集中的每个收集器。
2. 关闭您的生产群集。
3. 将 SmartStor、基准和事务事件数据文件从生产或测试 MOM 复制到副本 MOM，并从每个生产或测试收集器复制到副本收集器。
4. 启动生产群集和仅供查询的副本群集。
5. 在仅供查询的副本群集上运行所需的任意查询。
6. 每天重复一次必要的步骤，以使仅供查询的副本群集上的数据保持最新。



## 使用 SmartStor 工具调整 SmartStor 数据

Introscope 提供了 SmartStor 命令行工具，可用于：

- 从度量标准遗漏和爆发中清除  
有关度量标准遗漏和爆发的信息，请参阅《CA APM 规模调整和性能指南》。
- 将单个企业管理器拆分成多个企业管理器
- 将多个企业管理器合并为单个企业管理器

SmartStor 工具启动脚本位于 `<EM_Home>/tools/` 目录中。使用 `SmartStorTools.bat` 启动脚本在 Windows 环境中运行 SmartStor 工具。使用 `SmartStorTools.sh` 启动脚本在 UNIX 环境中运行 SmartStor 工具。

从 `<EM_Home>` 命令行使用有效参数运行 SmartStor 工具命令时，工具会执行所请求的命令。如果使用无效参数运行 SmartStor 工具命令，脚本会显示一条帮助消息。

**警告！** 使用 SmartStor 工具时，源企业管理器必须关闭。CA Technologies 建议在运行 SmartStor 工具时关闭源企业管理器和目标企业管理器。如果使用 SmartStor 工具时企业管理器正在运行，会存在损坏 SmartStor 的风险。如果企业管理器向 SmartStor 写入数据时 SmartStor 工具也正在对 SmartStor 数据进行更改，就可能会发生该风险。

使用以下格式运行这些 SmartStor 工具命令：

```
<SmartStorTools start script> <command> <arguments>
```

- merge
- remove\_metrics
- remove\_agents
- keep\_agents
- prune
- list-agents
- test\_regex

**警告！** 请谨慎使用 `prune` 工具。由于此工具会删除数据，请特别注意不要误删重要数据。

## SmartStor 工具命令

使用 SmartStor 工具命令，您可以在 SmartStor 数据库上执行多个不同的维护和管理任务。

**重要信息！** 在这些命令中指定代理和度量标准的名称时，必须使用反斜线对特殊字符进行转义。特殊字符包括  $([\{\^-\$/\}])?*$ 。例如，度量标准名称 `SuperDomain /machineName /WebLogic /WebLogic` 将指定为 `SuperDomain \/machineName \/WebLogic \/WebLogic`。

### merge

将指定的 SmartStor 源目录合并到其他目标目录中。

参数：

- <destination SmartStor directory>
- -help 输出帮助消息
- <source SmartStor directory>

示例：

Windows：

```
SmartStorTools.bat merge <source directory> <destination directory>
```

例如：

```
SmartStorTools.bat merge <EM_Home>\data C:\data
```

成功执行该命令后，源目录中的所有 SmartStor 数据与目标目录中的数据合并。

UNIX：

```
SmartStorTools.sh merge <source directory> <destination directory>
```

## remove\_metrics

删除与给定的正则表达式相匹配的度量标准。使用此工具可以清除度量标准遗漏和爆发。

**警告！** 谨慎使用 `remove_metrics` 工具。由于此工具会删除数据，请特别注意不要误删重要数据。

参数:

- `-dest`—目标 SmartStor 目录。
- `-help`—输出一条帮助消息。
- `-metrics`—要删除的度量标准的正则表达式。
- `-src`—源 SmartStor 目录。

示例:

### Windows

```
SmartStorTools.bat remove_metrics -dest <destination directory> -metrics  
<metrics to be removed> -src <source directory>
```

例如:

```
<EM_Home>\tools\SmartStorTools.bat remove_metrics -dest C:\SWDump\destination  
-metrics ".*Socket.*" -src <EM_Home>\data
```

成功执行该命令后，除套接字度量标准以外的所有度量标准都出现在目标目录中，而源目录中的所有度量标准保持原样。

### UNIX

```
SmartStorTools.sh remove_metrics -dest < destination directory> -metrics  
<metrics to be removed> -src <source directory>
```

## remove\_agents

删除与给定的正则表达式匹配的代理。

**警告！** 请谨慎使用 `remove_agent` 工具。由于此工具会删除数据，请特别注意不要误删重要数据。

参数:

- `-agents`—要删除的代理的正则表达式。
- `-dest`—目标 SmartStor 目录。
- `-help`—输出一条帮助消息。
- `-src`—源 SmartStor 目录。

示例:

### Windows

```
SmartStorTools.bat remove_agents -agents <Agent name> -dest <destination directory> -src <source directory>
```

例如:

```
<EM_Home>\tools>SmartStorTools.bat remove_agents -agents ".*webSphere.*" -dest C:\SWDump\destination -src <EM_Home>\data
```

成功执行该命令后，与 WebSphere 代理相关的所有度量标准都将从目标目录中删除，而源目录中的所有度量标准则保持原样。

### UNIX

```
SmartStorTools.sh remove_agents -agents ".*webSphere.*" -dest <destination directory> -src <source directory>
```

## keep\_agents

保留与给定的正则表达式匹配的代理

参数:

- *-agents*—代理要保留的正则表达式
- *-dest*—目标 SmartStor 目录
- *-help*—输出一条帮助消息
- *-src*—源 SmartStor 目录

示例:

### Windows

```
SmartStorTools.bat keep_agents -agents <agent(s) name> -dest <destination directory> -src <source directory>
```

例如:

```
<EM_Home>\tools>SmartStorTools.bat keep_agents -agents ".*websphere.*" -dest C:\SWDump\destination\keepagents -src data
```

成功执行该命令后，与 Websphere 代理相关的所有度量标准都出现在目标目录中，而源目录中的内容则保持原样。

### UNIX

```
SmartStorTools.sh keep_agents -agents <Agent(s) name> -dest <destination directory> -src <source directory>
```

## prune

查找在 SmartStor 中没有历史数据的代理，并删除所有关联的度量标准元数据。使用此工具可以清除度量标准遗漏和爆发。

**警告！** 请谨慎使用 **prune** 工具。由于此工具会删除数据，请特别注意不要误删重要数据。

使用 **prune** 工具需要执行一些步骤。请参阅[清除 SmartStor 元数据](#) (p. 71)。

参数:

- *-dest*—包含已清理元数据文件以及 *src* 的未更改 \*.data 文件的目录。
- *-help*—输出一条帮助消息
- *-silent*—静默模式
- *-src*—源 SmartStor 目录

## 示例

### Windows

```
SmartStorTools.bat Prune -dest <destination directory> -src <source directory>
```

例如:

```
<EM_Home>\tools>SmartStorTools.bat Prune -dest C:\SWDump\destination\backup  
-src data
```

成功执行该命令后,元数据文件会使用名称 *metrics.metadata* 备份到 *dest* 目录。

### UNIX

```
SmartStorTools.sh prune -dest <destination directory> -src <source directory>
```

## test\_regex

将与给定正则表达式匹配的度量标准或代理输出到 Windows 或 UNIX 控制台。

参数:

- *-help*—输出一条帮助消息
- *-src*—源 SmartStor 目录
- *-agents*—代理要匹配的正则表达式
- *-metrics*—度量标准要匹配的正则表达式

示例:

### Windows

```
SmartStorTools.bat test_regex -agents <agent(s) name> -src <source directory>
```

例如:

```
<EM_Home>\tools>SmartStorTools.bat test_regex -agents ".*websphere.*" -src  
<EM_Home>\data
```

成功执行该命令后,将打印 WebSphere 代理的所有度量标准。

### UNIX

```
SmartStorTools.sh test_regex -agents <agent(s) name> -src <source directory>
```

## list\_agents

列出与给定正则表达式匹配的代理。

SmartStor 工具的 `list_agents` 工具列出与给定正则表达式匹配的代理。

参数:

- `-agents`—代理要匹配的正则表达式
- `-src`—源 SmartStor 目录
- `-help`—输出一条帮助消息

示例:

Windows

```
SmartStorTools.bat list_agents -agents <agent(s) name> -src <source directory>
```

例如:

```
<EM_Home>\tools>SmartStorTools.bat list_agents -agents ".*websphere.*" -src  
<EM_Home>\data
```

在该命令成功执行后，将列出与此正则表达式（此例中为“`.*WebSphere.*`”）匹配的所有代理名称及其最后报告的日期。

UNIX

```
SmartStorTools.sh list_agents -agents <代理名称> -src <源目录>
```

## 清除 SmartStor 元数据

要在 SmartStor 中找到没有历史数据的代理，并且清除度量标准遗漏和爆发，请使用 `prune SmartStor` 工具，然后删除所有关联的度量标准元数据。

**重要信息！** 因为企业管理器会在运行时创建 SmartStor 数据，所以 CA Technologies 建议在运行 SmartStor 工具时关闭企业管理器。在企业管理器正在运行时使用 SmartStor 工具会生成无法预测的结果。

请执行以下步骤:

1. 关闭企业管理器。
2. 从命令提示符中运行 `prune` 命令。

例如：

在 Windows 上：<EM\_Home>\tools>SmartStorTools.bat prune -src <path to data directory> -dest <path to dest backup directory>

在 UNIX 上：<EM\_Home>/tools>SmartStorTools.sh prune -src <path to data directory> -dest <path to dest backup directory>

成功执行该命令后：

- 元数据文件会使用名称 *metrics.metadata* 备份到 *dest* 目录。
- Windows 或 UNIX 控制台会显示在执行清除操作期间所清除的度量标准
- \*.data 文件会在无更改的情况下从 *src* 目录复制到 *dest*。

要将 Windows 或 UNIX 控制台中的已清除度量标准列表重定向到一个文本文件，请在命令中包含 >> 参数。

例如：<EM\_Home>\tools>SmartStorTools.bat prune -src <path to data directory> -dest D:\backup >>D:\console.txt

1. 重命名 <EM\_Home>/data 目录中的 *metrics.metadata* 文件。例如：*noprunemetrics.metadata*。
2. 对 <EM\_Home>/data 目录运行 *test\_regex* 命令。

Windows 或 UNIX 控制台会显示命令输出，根据您在命令中包含的正则表达式显示所有度量标准。注意，已清除的度量标准不会再显示。

例如，如果您要清除大量的套接字度量标准，可以运行此 *test\_regex* 命令：

Windows 系统中：

```
<EM_Home>\tools>SmartStorTools.bat test_regex -metrics ".*Socket.*" -src <path to data directory>
```

在 UNIX 上：

```
<EM_Home>/tools>SmartStorTools.sh test_regex -metrics ".*Socket.*" -src <path to data directory>
```

3. 重新启动企业管理器。



## 清除 SmartStor 数据和元数据

要清除过量的 SmartStor 数据和元数据，请使用 SmartStor 工具。

**重要信息！**请在运行 SmartStor 工具时关闭企业管理器。由于企业管理器在运行时创建 SmartStor 数据，因此如果此时使用 SmartStor 工具，结果将不可预测。

有关如何查找 SmartStor 数据问题的示例，请参阅[示例：使用 test\\_regex 命令查找 SmartStor 数据问题](#) (p. 75)。另请参阅《CA APM Java 代理实施指南》或《.NET 实施指南》中关于度量标准爆发的主题。

请执行以下步骤：

1. 关闭企业管理器。
2. 从命令提示符中，运行 `test_regex` 命令以输出当前的度量标准列表。

例如，如果 Introscope 安装在 <企业管理器主目录> 目录中，且 SmartStor 配置为将数据保存到 <企业管理器主目录>\data 目录中，请运行以下命令：

```
SmartStorTools.sh test_regex -metrics <agents regexp> -src ../data
```

```
le: SmartStorTools.sh test_regex -metrics ".*" -src ../data
```

结果是一列完全限定的度量标准名称，包括主机名称、代理名称、度量标准名称以及度量标准 ID。总行数指示度量标准的总数。但是，该行计数不像从调查器中的可支持性度量标准获得的度量标准计数那样准确。

通过根据与代理或度量标准名称相匹配的特定正则表达式进行行计数，您可以了解占据绝大部分空间的是哪些度量标准。这还可以帮助您识别哪些度量标准您不感兴趣，希望将其删除。

3. 从度量标准列表中，从特定代理中选择要删除的度量标准。
4. 运行 SmartStor 工具 `remove_metrics` 命令以删除一组过量的度量标准。

例如，如果您具有较高的 SQL 度量标准计数，可使用以下命令删除所有 SQL 度量标准：

```
<EM_Home>\tools>SmartStorTools.bat remove_metrics  
-dest c:\sql_metrics_removed -metrics ".*SQL.*" -src <EM_Home>\data
```

成功执行命令后，除 SQL 度量标准外的所有度量标准都将显示在目标目录中，而源目录中的所有度量标准保持原样。

**注意:** 此命令要求目标空间(虽然它会缩小几 GB)与原始数据(由 `-src` 选项指定)所占据的空间大小基本相同才能运行。在上面的示例中,没有 SQL 度量标准的新数据(由 `-dest` 选项指定)现在将位于 `c:\sql_metrics_removed` 目录中。

此命令是一个长时间运行的操作,可能会持续运行几个小时。

5. 如有需要,对另一组过量的度量标准重复 `remove_metrics` 命令。

套接字是遗漏的度量标准的另一常见源。在运行 `remove_metrics` 命令后,使用以下命令删除套接字度量标准:

```
<EM_Home>\tools>SmartStorTools.bat remove_metrics  
-dest c:\sql_and_sockets__metrics_removed -metrics ".*Sockets.*"  
-src c:\sql_metrics_removed
```

此命令将使用由删除 SQL 度量标准的第一个命令得到的数据作为源数据(`c:\sql_metrics_removed` 目录中的数据)。删除了 SQL 和套接字度量标准之后的数据则将位于由 `-dest` 选项指定的以下位置:`c:\sql_and_sockets__metrics_removed`。同样地,此命令要求额外空间与原始数据所占据的空间大小基本相同才能运行。

6. 在减少度量标准的数目之后,将任何备份元数据文件从 `<企业管理器主目录>\data` 目录转移到备份目录。

企业管理器自动使用最大的元数据文件,也就是具有最大数目的已定义度量标准的文件。减少度量标准可能导致备份元数据文件大于当前的数据文件。

7. 针对所清除的度量标准数据和元数据检查度量标准数据值。

- a. 打开 `<企业管理器主目录>\config` 目录中的 `apm-events-thresholds-config.xml` 文件。
- b. 记下当前的属性设置,然后设置属性 `introscope.enterprisemanager.metrics.historical.limit=500000`。
- c. 保存并关闭文件。
- d. 打开 `<企业管理器主目录>\config` 目录中的 `IntroscopeEnterpriseManager.properties` 文件。
- e. 记下当前的设置,然后将属性 `introscope.enterprisemanager.smartstor.directory=` 设置为指向度量标准删除操作的目标位置。  
  
例如,示例目标位置是 `c:\sql_and_sockets__metrics_removed`。因此,此属性设置将为 `introscope.enterprisemanager.smartstor.directory=c:\sql_and_sockets__metrics_removed`
- f. 保存并关闭文件。
- g. 重新启动企业管理器。



3. （可选）运行一个脚本对度量标准进行排序和分组。

例如，要确认 JMX 度量标准是度量标准的爆发源，您可以运行以下脚本：

```
grep '/!.*' / awk -F '/' '{print $1}' / sort / uniq -c
```

如果您使用的是 UNIX 系统，可以运行具有排序脚本的完整 `test_regex` 命令：

```
SmartStorTools.sh test_regex -metrics <agents regexp> -src ../data /  
grep '/!.*' / awk -F '/' '{print $1}' / sort / uniq -c  
le: SmartStorTools.sh test_regex -metrics ".*" -src ../data / grep '/!.*' /  
awk -F '/' '{print $1}' / sort / uniq -c
```

4. 查看排序结果。

例如，您可能会发现如下所示的度量标准计数和类型的列表：

```
1054327 JMX  
1564 JSP  
1051 OlamWebApp  
889 EJB  
569 CEF  
496 Struts  
173 Edocs  
167 Servlets  
36 CPU  
29 Sockets
```

在本例中，SmartStor 存储了超过一百万个度量标准，其中绝大部分是 JMX 度量标准。这表明存在 JMX 度量标准的爆发，可以使用 SmartStor 工具进行清除。有关度量标准爆发的详细信息，请参阅《CA APM Java 代理实施指南》或《.NET 代理实施指南》。

## 将 8.x 数据升级到 9.x

可以使用 SmartStor 工具命令将 8.x 代理中的 SmartStor 数据升级到 9.x。

此工具可将 8.x 前端和后端度量标准 ID 更新为 9.x 前端和后端度量标准 ID。执行此操作可防止在显示应用程序分类视图时出现重复的度量标准。

将企业管理器和代理升级到 9.x 后才可使用升级命令。

## 使用“升级”命令来升级 8.x 数据

请执行以下步骤：

1. 关闭企业管理器。
2. 从命令提示符浏览到 <企业管理器主目录>/tools 目录。
3. 备份 SmartStor 数据目录。
4. 提供源和目标目录路径，运行 *upgrade* 命令。

使用以下语法和参数：

语法：

```
upgrade <源目录> <目标目录>
```

参数：

- 源目录—包含 SmartStor 8.x 指标的现有目录的路径
- 目标目录—新目录的路径。

**注意：**实用工具会实时创建新的目录。不要预先创建目录。

示例：

```
C:\Program Files\CA APM\Introscope<新版本 (9.X)>\tools>SmartStorTools.bat upgrade C:\Program Files\CA APM\Introscope<新版本 (9.X)>\data C:\Program Files\CA APM\Introscope<新版本 (9.X)>\upgradeddata
```

5. 编辑 IntroscopeEnterpriseManager.properties 文件，以便将 SmartStor 目录设置为目标目录。
  - a. 打开 <企业管理器主目录>/config/IntroscopeEnterpriseManager.properties 进行编辑，并且找到“SmartStor Settings”部分。
  - b. 将 *introscope.enterprisemanager.smartstor.directory* 的值设置为目标目录。

默认值为 *data*，引用的是 <企业管理器主目录>/data/。
6. 重新启动企业管理器。



# 第 5 章：使用虚拟代理聚合度量标准

---

本节介绍了有关配置和使用虚拟代理的信息。

此部分包含以下主题：

[了解虚拟代理](#) (p. 79)

[虚拟代理要求](#) (p. 79)

[配置虚拟代理](#) (p. 80)

## 了解虚拟代理

您可以将多个物理代理配置到单个 *虚拟代理* 中。通过虚拟代理，可生成一个综合逻辑视图，其中包含由多个 Java 代理报告的度量标准。

如果您使用 Introscope 管理群集应用程序，虚拟代理将非常有用。

虚拟代理由多个监控同一群集应用程序的不同实例的代理组成，并作为单个代理显示在 Introscope Workstation 中。这样，多个群集应用程序实例中的度量标准将显示在一个逻辑的应用程序级别上，而不是单独显示在每个应用程序实例中。

您可以根据单个代理确定视图和交互的范围，从而查看特定应用程序实例的性能和可用性数据。

## 虚拟代理要求

如果您具有多个独立的企业管理器，则虚拟代理只能包含向同一企业管理器报告的代理。

在企业管理器群集中，向单个群集内的企业管理器报告的代理可以属于同一虚拟代理，无论这些代理向哪个收集器企业管理器报告。

配置虚拟代理时请考虑以下条件：

- 可将一个代理分配给多个虚拟代理。
- 如果定义了多个虚拟代理，它们必须具有唯一的名称（包括自定义度量标准代理），即群集中的所有代理都必须具有唯一的名称。
- 存在于 SuperDomain 下的虚拟度量标准能够发布到其他的自定义域。例如：

```
<agent-cluster name="Custom Metric Host" domain="SuperDomain"
tgtDomain="Production">
    <agent-specifier>(.*)\(.*\)Custom Metric Agent
    \(\Virtual\)(.*)</agent-specifier>

    <metric-specifier>Agents\(.*)ConnectionStatus</metric-specifier>
</agent-cluster>
```

设置此配置可以从“超级域.自定义度量标准主机（收集器）：代理列表”中的每个代理提取 **ConnectionStatus**（一个虚拟度量标准），并将其重新发布到生产域。

## 配置虚拟代理

可使用 *agentclusters.xml* 文件配置虚拟代理，该文件位于代理向其报告的企业管理器的 `<EM_Home>/config` 目录中。如果您运行群集企业管理器，请使用 MOM `<EM_Home>/config` 目录中的 *agentclusters.xml* 文件来配置虚拟代理。`<EM_Home>/config` 目录中提供了一个示例 *agentclusters.xml*。

示例 *agentclusters.xml* 定义了 Introscope SuperDomain 中名为 *BuyNowAppCluster* 的虚拟代理。该虚拟代理包括任意主机上的所有代理，其代理名称以 *BuyNow* 开头。

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<agent-clusters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="agentclusters0.1.xsd" version="0.1" >
  <agent-cluster name="BuyNowAppCluster" domain="SuperDomain" >
    <agent-specifier>.*\.*BuyNow.*</agent-specifier>
    <metric-specifier>Frontends\.*</metric-specifier>
  </agent-cluster>
</agent-clusters>
```



根元素 `<agent-clusters>` 是必需的元素。`<agent-cluster>` 元素定义了一个虚拟代理，该元素具有两个必需的属性：

- `name`—如果定义多个虚拟代理，则每个虚拟代理必须具有唯一的名称。
- `domain`—将虚拟代理分配给 Introscope 域。

如果代理-群集定义中没有定义任何域（如 `domain=""`），则虚拟代理默认为 SuperDomain。

如果定义多个虚拟代理，应为每个虚拟代理各定义一个 `<agent-cluster>` 元素。`<agent-cluster>` 元素需要具有两个子元素：

- `<agent-specifier>`—包含一个用于指定虚拟代理中的代理的正则表达式，它使用标准的完全限定代理名称：  
`<host> / <process> / <agentName>`
- `<metric-specifier>`—包含一个前缀，该前缀按照资源类型或资源类型实例的子集指定要从虚拟代理中的代理收集的度量标准。建议使用以下前缀：
  - Frontends
  - CPU
  - JMX
  - WebSpherePMI

**注意：**使用以上建议的前缀时，任何资源均可用作度量标准说明符。

`<agent-cluster>` 元素可以包含多个 `<metric-specifier>` 节。

**注意：**较高的匹配度量标准量会大大增加企业管理器的开销，并最终影响企业管理器的容量。

**重要信息！** 允许使用正则表达式和通配符度量标准说明符（如 `“.*”` 和 `“(.*)”`），但是如果确实需要，应当谨慎使用。使用通配符会生成大量度量标准并影响性能。

要在特定浏览树域节点下显示虚拟代理，请定义 `tgtDomain` 属性。

- `tgtDomain`—定义目标域，会在其中复制域属性中定义的虚拟代理度量标准以显示在浏览树中。
  - 如果没有定义 `tgtDomain`，域则命名为 `tgtDomain`。

- 如果 *tgtDomain* 值不是在 *domains.xml* 中定义的有效域，Introscope 则无法创建目标域浏览树节点。
- 要查看使用 *tgtDomain* 属性定义的域，用户必须在 *domains.xml* 中定义了权限。有关 *domains.xml* 权限的信息，请参阅《CA APM 安全指南》。

该示例 *agentclusters.xml* 定义了名为 *BuyNowAppCluster* 的虚拟代理，该代理在 Introscope SuperDomain 节点中有所定义并显示在 MyDomain 节点中。

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<agent-clusters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="agentclusters0.1.xsd" version="0.1" >
  <agent-cluster name="BuyNowAppCluster" domain="SuperDomain"
    tgtDomain="MyDomain"
    <agent-specifier>.*\|.*\|BuyNow.*</agent-specifier>
    <metric-specifier>Frontends\|.*</metric-specifier>
  </agent-cluster>
</agent-clusters>
```

在这种情况下，具有仅查看 MyDomain 域的权限的 CA APM 用户会看到以下“浏览”树：

```
自定义度量标准主机（虚拟）
  自定义度量标准进程（虚拟）
    BuyNowAppCluster
```

## 第 6 章：配置企业管理器和群集

---

本节介绍了企业管理器群集功能，并提供了有关配置企业管理器角色和群集功能的说明。

此部分包含以下主题：

[配置独立的企业管理器](#) (p. 83)

[了解企业管理器群集](#) (p. 83)

[使用企业管理器故障切换](#) (p. 86)

[配置企业管理器群集](#) (p. 91)

### 配置独立的企业管理器

您可以配置 `introscope.enterprisemanager.clustering.mode` 属性，以将某个企业管理器指定为独立的企业管理器。

请执行以下步骤：

1. 打开位于独立企业管理器 <企业管理器主目录>\config 目录中的 `IntroscopeEnterpriseManager.properties` 文件。
2. 设置 `introscope.enterprisemanager.clustering.mode=Standalone`
3. 保存并关闭文件。
4. 重新启动企业管理器以使该设置生效。

### 了解企业管理器群集

在群集环境中，一个企业管理器用作 *上级管理器 (MOM)*，管理着群集中的其他企业管理器。托管的企业管理器称为 *收集器*。

登录到 MOM 的 Workstation 用户可以执行以下操作：

- 查看和访问代理向 MOM 管理的每个收集器报告的数据。
- 对这些收集器执行所有常用的 Workstation 功能。

可选的企业管理器充当跨群集数据查看器 (CDV)，它可以跨群集连接到收集器。

登录到 CDV 的 Workstation 用户可以执行以下操作：

- 查看和访问显示板以及度量标准浏览器树中的代理和客户体验度量标准数据。这些数据将报告给 CDV 连接的每个收集器。
- 对这些收集器执行一部分常用 Workstation 功能，包括以下功能：
  - 使用管理模块编辑器创建显示板。
  - 运行事务跟踪。
  - 使用动态检测。
  - 您可以[配置企业管理器群集](#) (p. 91)。

## 什么情况下构建企业管理器群集

在由多个企业管理器和代理组成的大型 Introscope 环境中，构建群集很有用—群集配置可以降低管理多企业管理器环境的复杂性和成本。

## 了解 MOM 如何管理收集器

在您启动按[配置企业管理器群集](#) (p. 91)中所述配置的 MOM 时，它会尝试与自己管理的每个收集器建立连接。

调查器中的每个代理将自动拥有一个名为“企业管理器主机”的度量标准。运行群集时，此度量标准很有用，您可以通过它来判断代理连接到哪个收集器企业管理器。

MOM 使用一个内置的预配置用户帐户来连接到收集器。密码使用公钥/私钥加密加以保护。有关更多信息，请参阅《*CA APM 安全指南*》。

如果 MOM 初次尝试连接到一台收集器时导致了不可恢复的错误（如身份验证错误、未知的主机异常或 `java.rmi.ConnectIOException`），则该收集器将从群集中删除—MOM 会停止尝试连接到该收集器，直到 MOM 下次重新启动。

对于可恢复的错误（如连接断开，或 `java.rmi.ConnectionException`），MOM 会每隔 10 秒重复尝试连接。

连接状态的日志记录是以下述方式执行的：

- 如果日志记录级别是 **DEBUG**，则连接失败的堆栈跟踪将写入日志。
- 如果日志记录级别是 **VERBOSE**，则前 **10** 次连续失败尝试的消息将写入日志，在连续 **10** 次尝试失败后，会向日志中写入一条消息指出不再将失败尝试消息写入日志中。
- 当 **MOM** 连接或重新连接收集器时，总会有一条消息写入到日志中。

只要 **MOM** 保持运行状态，它就会轮询所管理的收集器。

## 群集和企业管理器时钟同步

在企业管理器群集中，收集器系统时钟与 **MOM** 时钟设置的差值不能超过三秒。如果启动时某个收集器的时钟与 **MOM** 的时钟不同步，则该收集器将无法加入群集。运行期间，如果先前同步的某个收集器的时钟偏移已超过三秒，则 **MOM** 将不再接受来自该收集器的数据。

**MOM** 与收集器企业管理器之间的时钟同步不会自动进行。

要使 **MOM** 和收集器企业管理器时钟保持同步，**CA Technologies** 建议所有企业管理器定期将其时钟同步到 **NTP** 服务器。如果某个收集器的时钟相对于 **MOM** 时钟的偏移已超过三秒，**MOM** 日志中的错误消息表明 **MOM** 不再接受来自该收集器的数据。如果发生此情况，请提高与 **NTP** 服务器进行同步的频率。时钟同步后不需要重新启动企业管理器。**MOM** 检测到时钟已同步后，会自动重新连接到收集器。

**注意：**有必要运行一个时间服务器软件，用以定期同步群集中所有计算机的时钟。

## 群集和代理命名

在企业管理器群集中，向收集器企业管理器进行报告的代理的名称必须是唯一的。

**MOM** 要求代理名称在整个群集中是唯一的。虽然每个企业管理器可以确保与其连接的代理都具有唯一的名称（如《*CA APM Java 代理实施指南*》或《*CA APM .NET 代理实施指南*》中有关解决代理命名冲突的讨论所述），但您还需要确保代理在群集中各收集器间都具有唯一的名称。如果群集中有多个代理具有相同的名称，则只有 **MOM** 最后遇到的代理会显示在 **Workstation** 视图中。将代理配置为从应用程序服务器获取其名称是一项分配唯一代理名称的技术。有关详细信息，请根据环境需要参阅《*CA APM Java 代理实施指南*》或《*CA APM .NET 代理实施指南*》中有关从应用程序服务器获取代理名称的讨论。

收集器自动重命名自定义的度量标准代理，向代理名称添加一个唯一的标识符以标识代理的收集器。默认标识符的格式为 (*host@port*)，其中 *host* 是收集器的主机名，*port* 是收集器的连接端口，如其 `introscope.enterprisemanager.port.<通道名称>` 属性中所定义。或者，可以使用 `introscope.enterprisemanager.clustering.collector.identifier` 属性设置标识符。标识符是唯一的。

例如，在端口 5001 上侦听连接的 *myhost* 上，某个收集器中超级域中的自定义度量标准代理的名称将是：

```
Custom Metric Agent (myhost@5001) (*SuperDomain*)
```

## 群集和管理模块

在企业管理器群集中，仅使用安装在 MOM 上的管理模块。出于性能方面的考虑，建议不要使管理模块位于收集器企业管理器上。

### 在群集环境中部署扩展文件

如果您已在 CA APM 部署中激活了扩展，则在群集环境中进行部署时，必须使用特定方式对扩展文件进行管理。

请执行以下步骤：

1. 在 `<EM_Home>/examples/<Extension_Home>` 中找到安装扩展文件的扩展文件夹，其中 `<Extension_Home>` 是扩展的名称。
2. 将此文件夹的整个内容复制到 MOM 中的 `<EM_Home>/` 位置。
3. 将此文件夹的整个内容（`<EM_Home>/examples/<Extension_Home>/config` 目录除外）复制到每个收集器企业管理器上的 `<EM_Home>/` 位置。

请勿复制 `<EM_Home>/examples/<Extension_Home>/config` 目录，因为管理模块 `.jar` 文件只能位于 MOM 上。

## 使用企业管理器故障切换

企业管理器故障切换的工作方式有以下两种：

- 一个企业管理器作为主企业管理器，另一个作为次要或备份企业管理器。
- 两台计算机都是主企业管理器。

次要企业管理器的职责是在主企业管理器失败后接管控制权，并在主企业管理器恢复后归还控制权。主企业管理器的职责是从次要企业管理器处接管控制权。

如果一对企业管理器共享一个 **Introscope** 安装，您可以配置企业管理器故障切换。通常，两个企业管理器在不同的计算机上。**Introscope** 安装必须位于网络文件系统上，因为两个企业管理器都需要对 **Introscope** 安装具有读取访问权限。但是每次只有一个企业管理器需要写入访问权限。例如，**Introscope** 安装可以使用网络连接存储 (NAS) 协议（如以下协议）共享：

- 网络文件系统 (NFS)
- 服务器消息块 (SMB)

要保持群集的稳定性和可用性，CA Technologies 建议为 MOM 企业管理器配置故障切换。此外，还可以为群集中的一个或多个收集器和 CDV，或为独立的企业管理器配置故障切换。如果要为群集中的 MOM、收集器和 CDV 配置故障切换，请单独配置每个企业管理器。

默认情况下，不会启用企业管理器故障切换。

请执行以下步骤：

1. 导航到 `<EM_Home>\config` 目录并打开 `IntroscopeEnterpriseManager.properties` 文件。
2. 找到 Hot Failover 节。
3. 设置[故障切换属性](#) (p. 410)。

当代理、TIM 和工作站尝试连接到企业管理器时，它们会尝试所有 IP 地址来获取主机名。如果您已使用主要和次要企业管理器的 IP 地址在 DNS 中定义了一个逻辑主机，则代理、TIM 和 Workstation 可以将它用作企业管理器主机名并连接到正在运行的任一企业管理器。

4. 确信次要的企业管理器计算机用户有对主企业管理器 SmartStor 数据目录的写权限。

在故障切换情况下，此权限允许次要的企业管理器对主企业管理器 SmartStor 数据库写入数据。

**注意：**在故障切换环境中，您可以使用 `EMCtrl` 脚本来启动主企业管理器。次要企业管理器不应使用控制脚本。例如，在 UNIX 平台上，使用控件脚本 `EMCtrl.sh` 启动主企业管理器。使用 `./Introscope Enterprise Manager` 命令启动次要企业管理器。

## 企业管理器故障切换规则

这些规则适用于企业管理器故障切换：

- 启用具有故障切换功能的企业管理器时，必须一次启动一个企业管理器。如果配置中有主次之分，必须首先启动主企业管理器。
- 如果两个企业管理器都是主企业管理器，则第二个主企业管理器会等待第一个企业管理器失败，并且在第一个主企业管理器恢复后不会归还控制权。
- 对于故障切换，主企业管理器、次要企业管理器和安装目录通常在不同的主机上。不过，Introscope 安装（Introscope 最初的安装位置）和企业管理器可以位于相同的主机上。有关更多信息，请参阅[将企业管理器故障切换配置为在单个主机上运转](#) (p. 89)。
- 如果一个企业管理器的主机匹配其中某个主主机，那么该企业管理器充当主企业管理器的角色。
- 如果一个企业管理器的主机匹配其中某个次要主机，那么该企业管理器充当次要企业管理器的角色。
- 如果一个企业管理器的主机不匹配主主机或次要主机，那么该企业管理器将会正常启动。但是会记录一条警告消息。
- 次要企业管理器每隔两分钟（可配置）检查主企业管理器是否在等待启动。如果是，次要企业管理器会向主企业管理器让步并关闭。  
[introscope.enterprisemanager.failover.interval](#) (p. 411) 属性控制正在运行的次要企业管理器检查主企业管理器是否在等待启动的频率。
- 主企业管理器不会向次要企业管理器或其他主企业管理器让步。
- 启动和关闭顺序如下所示：在启动故障切换对时，先启动主企业管理器，然后是次要企业管理器。关闭故障切换对时，首先然后停止次要企业管理器，然后再停止主企业管理器。

### 在向主企业管理器让步后重新启动次要企业管理器

次要企业管理器在向主企业管理器让步后，它会退出 JVM。是否重新启动次要企业管理器，取决于您。您可以使用脚本或通过将次要企业管理器作为 Windows 服务运行来执行重新启动。如果次要企业管理器因向主企业管理器让步而关闭，次要企业管理器将会退出，状态代码为 23 (`org.eclipse.equinox.app.IApplication.EXIT_RESTART`)。如果次要企业管理器是因为命令行中断或因工作站而正常关闭，则它会以状态代码 0 退出。



如果您在使用 Windows，可以使用如下命令：

```
:RESTART  
"Introscope Enterprise Manager"  
IF ERRORLEVEL 23 GOTO RESTART
```

## 将企业管理器故障切换配置为在单个主机上运行

您可以将企业管理器故障切换配置为在单个主机（而非共享的文件系统）上运行。您可以在单个主机上设置企业管理器故障切换，以便允许第二个企业管理器在第一个失败时进行接管。在您不想执行以下操作的时候，在单一主机上设置故障切换：

- 作为 Windows 服务运行企业管理器
- 使用 shell 脚本重新启动企业管理器。

**重要信息！** 如果在同一主机上配置两台故障切换企业管理器，会产生单点故障，无法在未造成明显中断的硬件平台故障中幸免。

请执行以下步骤：

1. 在 *IntroscopeEnterpriseManager.properties* 文件中设置以下企业管理器属性，如下所示：
  - *introscope.enterprisemanager.failover.enable=true*
  - *introscope.enterprisemanager.failover.primary=localhost*
2. 通过单击 Introscope Enterprise Manager.exe 来启动第一个主企业管理器。
3. 通过单击 Introscope Enterprise Manager.exe 启动第二个主企业管理器。

当第二个主企业管理器正常启动时，命令提示符（控制台）中将显示内容为 *acquiring primary lock* 的消息。如果此消息没有显示，则表明故障切换配置不正确，或者主企业管理器未在运行。

## 关于 MOM 故障切换和 CA CEM TIM

如果要在 CA APM 环境中部署 CA CEM，请配置 MOM 以便与每个 TIM 连接。启用 TIM 时，MOM 会为 TIM 提供两个 IP 地址：MOM IP 地址和运行 TIM 收集服务的收集器的 IP 地址。此收集器与 TIM 连接以收集 TIM 数据。

如果配置了 MOM 故障切换，当 TIM 已启用且正在运行时，主 MOM 会向 TIM 提供以下信息：

- 主 MOM IP 地址
- 在 `IntroscopeEnterpriseManager.properties` 文件中定义的次要 MOM IP 地址（如果已设置）。

TIM 存储这些 IP 地址，您可以在“Wily 系统设置” > “TIM” > “TIM 设置”页面中进行查看。

要将故障切换 MOM 连接至 TIM，必须满足下列条件：

- TIM 正在运行且已启用
- `IntroscopeEnterpriseManager.properties` 文件属性的设置正确：
  - `IntroscopeEnterpriseManager.failover.enable` 属性设置为 `true`
  - 在 `introscope.enterprisemanager.failover.primary` 属性中定义了一个或多个主 MOM IP 地址

**注意：**如果您定义了多个主 MOM IP 地址，则不必定义次要 IP 地址。

- 如果您仅定义了一个主 MOM IP 地址，必须在 `IntroscopeEnterpriseManager.properties` 文件的 `introscope.enterprisemanager.failover.secondary` 属性中定义一个或多个次要 MOM IP 地址。

**注意：**必要时您可以定义多个次要的 MOM。

- 如果故障切换 MOM 的地址发生更改，则禁用所有 TIM，然后再启用这些 TIM。启用 TIM 可让 TIM 获得新故障切换 MOM 的 IP 地址。您可以在 CEM 控制台中看到故障切换 MOM IP 地址。请参阅“TIM 设置”页面中的 `TessIpAddr` 字段。

如果满足了这些条件，则主 MOM 出现故障后，故障切换 MOM 会自动连接到 TIM。您可以配置故障切换到其他主 MOM 或次要 MOM。

如果没有满足这些条件，MOM 发生故障时会发生以下情况：

如果.....

**MOM 发生故障时将发生的情况.....**

---

TIM 没有运行且未启用

发生 MOM 故障前后没有到 TIM 的连接。TIM 必须正在运行且已启用才能被 MOM 识别并接收 MOM 连接。

---

IntroscopeEnterpriseManager.failover.enable 属性设置为 <i>false</i>	收集器继续从 TIM 提取数据，但是没有其他主 MOM 或次要 MOM 尝试连接到 TIM。 备用主 MOM 或次要 MOM 连接到收集器。
未定义 MOM 的其他主要或次要 IP 地址	收集器继续从 TIM 中提取数据，但没有任何备用的主要 MOM 或次要 MOM 尝试连接到 TIM。不会将任何 MOM 配置更改发送到 TIM。

## 配置企业管理器群集

您可以通过在属性文件中定义企业管理器角色和与群集相关的属性来配置企业管理器群集。

**重要信息！** 不要在 CA APM 群集内以及 CA APM 群集之间为 MOM、收集器和 CDV 使用不同的 `domains.xml` 文件。

MOM 可以在群集中为活动代理（正在向群集发送数据的代理）处理不同的域。但是，如果对 MOM 和收集器上的历史代理使用不同的域，会导致 MOM 的历史数据视图中出现不一致。在此类具有混合域的群集中，不会跟踪收集器上的历史代理，因此，历史代理的数据不会显示在通过 MOM 创建的 Workstation 图表中，除非显式装入历史代理。为避免以上情况，CA Technologies 强烈建议在一个群集中的 MOM 以及所有收集器上放置完全相同的 `domains.xml` 文件。这样，无需装入历史代理以查看 Workstation 上与特定收集器有关的历史数据，实时数据和历史代理数据会一直在 MOM Workstation 中可见。

如果要部署跨群集数据查看器 (CDV)，CDV `domains.xml` 文件必须包含以下域：

- CDV 连接到的所有收集器的所有域。
- 跨所有群集（包含 CDV 收集数据的收集器）的所有域。

如果某个域存在于收集器 `domains.xml` 文件中但在 CDV `domains.xml` 文件中缺失，将发生以下情况：

- CDV 不搜集缺失的收集器域的数据。
- CDV Workstation 不显示缺失的收集器域中的数据。

**注意：** 有关使用 `domains.xml` 的信息，请参阅《CA APM 安全指南》。

## 配置 MOM

您可以配置 `introscope.enterprisemanager.clustering.mode` 属性来指定企业管理器作为一组收集器的 MOM。

请执行以下步骤：

1. 打开位于 MOM <企业管理器主目录>\config 目录中的 `IntroscopeEnterpriseManager.properties` 文件。
2. 设置 `introscope.enterprisemanager.clustering.mode=MOM`。
3. 定义 MOM 管理的每个收集器的连接属性。对于每个收集器，在 MOM 属性文件中定义这些属性。在每个连接属性中，`<emName>` 都是收集器企业管理器的相同的任意标识符：
  - `introscope.enterprisemanager.clustering.login.<emName>.host`—指定收集器主机名或 IP 地址。
  - `introscope.enterprisemanager.clustering.login.<emName>.port`—指定收集器上的侦听程序端口。
  - `introscope.enterprisemanager.clustering.login.<emName>.publickey`—取消注释此属性以将其设置为默认值

*config/internal/server/EM.public*

如果独立设置连接属性，它们将使用热配置服务生效。

4. 保存并关闭文件。
5. 重新启动企业管理器以使这些属性设置生效。

`introscope.enterprisemanager.clustering.mode` 属性要求重新启动企业管理器。

## 配置收集器

可以配置属性以指定企业管理器作为收集器，并设置可以连接到收集器的最大 CDV 数目。

请执行以下步骤：

1. 打开位于收集器 <企业管理器主目录>\config 目录中的 `IntroscopeEnterpriseManager.properties` 文件。
2. 设置 `introscope.enterprisemanager.clustering.mode=Collector`。
3. （可选）如果希望该收集器有一个特殊标识符，可设置该属性：`introscope.enterprisemanager.clustering.collector.identifier`。

如果不为收集器指定特殊标识符，可使用默认值 `host@port`。`host` 是企业管理器主机名，`port` 是企业管理器连接端口。

4. 保存并关闭文件。
5. 重新启动企业管理器以使这些属性设置生效。
6. （可选）设置允许连接到收集器的最大 CDV 数目。

**重要信息！适用于收集器和 CDV 9.1：**所有收集器和 CDV 都必须至少为版本 9.1 且必须为相同版本。CDV 无法连接到包含混合版本的 CDV 或收集器的群集中的收集器。

如果要配置一个或多个 CDV 以连接到该收集器，请根据需要为您的环境设置该属性：

- a. 打开收集器 `<EM_Home>\config` 目录中的 `apm-events-thresholds-config.xml` 文件。
- b. 设置 `introscope.enterprisemanager.collector.cdv.max` 属性。
- c. 保存 `apm-events-thresholds-config.xml`。

在热部署期间（热部署大约每 60 秒执行一次），当企业管理器检查属性文件时会应用这些设置。

## 关于 CDV

跨群集数据查看器 (CDV) 是一个专用企业管理器，用于从多个群集中的多个收集器收集代理和客户体验度量标准数据。使用 CDV Workstation，可以创建和查看显示板，其中显示收集器提供的代理和客户体验度量标准的综合视图。收集器可以位于您组织的不同数据中心中。每个收集器都可连接多个 CDV，为您监控和查看报告到不同 CA APM 群集的应用程序方面提供了灵活性。

如果您组织中的多个大型 CA APM 部署分别具有其自己的群集，则 CDV Workstation 允许您监控不同群集中的应用程序。通过该功能，可以确定哪个群集中存在应用程序问题。

**注意：**代理不会连接到 CDV。

如果您要查看连接到 CDV 的收集器的图表，可以在 CDV Workstation APM 状态控制台中查看企业管理器视图。

**注意：**有关使用 APM 状态控制台的信息，请参阅《CA Introscope Workstation 用户指南》。

**重要信息！适用于收集器和 CDV 9.1：**所有收集器和 CDV 都必须至少为版本 9.1 且必须为相同版本。CDV 无法连接到包含混合版本的 CDV 或收集器的群集中的收集器。

每个收集器可以连接到不同数目的 CDV，这是在 `introscope.enterprisemanager.collector.cdv.max` 属性中设置的。这将使 CA APM 管理员或问题分类员能够创建提供多个应用程序监控视图的显示板。例如，CA APM 环境包括下列群集和企业管理器：

- 三个群集：A、B 和 C。
- 三个 CDV：1、2 和 3。
- 五个收集器：4、5、6、7 和 8。
  - 收集器 4 和 5 位于群集 A。
  - 收集器 6 和 7 位于群集 B。
  - 收集器 8 位于群集 C。

CA APM 管理员按照以下方式配置三个 CDV：

- CDV 1 连接到收集器 4 和 6，这两个收集器位于群集 A 和 B。
- CDV 2 连接到收集器 4 和 8，这两个收集器位于群集 A 和 C。
- CDV 3 连接到收集器 5 和 8，这两个收集器位于群集 A 和 C。

## 配置 CDV

您可以配置 CDV 来监控一组收集器。收集器可以位于不同的群集。

请执行以下步骤：

1. 转到 CDV `<EM_Home>\config` 目录并打开 `IntroscopeEnterpriseManager.properties` 文件。
2. 设置 `introscope.enterprisemanager.clustering.mode=CDV`。
3. 定义 CDV 连接的每个收集器的连接属性。

**重要信息！适用于收集器和 CDV 9.1：**所有收集器和 CDV 都必须至少为版本 9.1 且必须为相同版本。CDV 无法连接到包含混合版本的 CDV 或收集器的群集中的收集器。

对于每个收集器，请定义以下属性，其中每个属性中的 `<emName>` 都相同，是收集器的任意标识符：

- `introscope.enterprisemanager.clustering.login.<emName>.host`—指定收集器主机名或 IP 地址。

- `introscope.enterprisemanager.clustering.login.<emName>.port`—指定收集器上的侦听程序端口。
- `introscope.enterprisemanager.clustering.login.<emName>.publickey`—取消注释此属性以将其设置为 `config/internal/server/EM.public` 的默认值。

如果独立设置连接属性，它们将使用热配置服务生效。

4. 保存 `IntroscopeEnterpriseManager.properties` 文件。
5. 重新启动企业管理器以使这些属性设置生效。

`introscope.enterprisemanager.clustering.mode` 属性要求重新启动企业管理器。

CA APM 管理员和问题分类员可以在 CDV Workstation 显示板和调查器度量标准浏览器树中查看所有已配置收集器的代理度量标准数据。





# 第 7 章：配置 MOM 代理负载均衡

---

CA APM 群集环境支持代理负载均衡。MOM 根据度量标准负载和您的 CA Introscope 配置分发代理连接。代理会连接到可用的收集器。

此部分包含以下主题：

[代理负载均衡概览 \(p. 97\)](#)

[MOM 将代理分配给收集器的方式 \(p. 98\)](#)

[MOM 如何重新平衡群集 \(p. 99\)](#)

[设置代理负载均衡度量标准的加权因子 \(p. 99\)](#)

[设置代理负载均衡度量标准的阈值 \(p. 100\)](#)

[设置代理负载均衡时间间隔属性 \(p. 101\)](#)

[代理负载均衡使用方案 \(p. 101\)](#)

[配置对收集器的代理分配 \(p. 104\)](#)

## 代理负载均衡概览

通过将参与的代理从超载的收集器中逐出，MOM 使度量标准计数在收集器之间实现均衡。断开连接的代理将重新连接到 MOM，然后被重定向到欠载的收集器。负载均衡仅适用于代理度量标准负载；不适用于 CA CEM 数据负载。

**适用于 8.0 之前的代理：** 8.0 之前的代理无法连接到 MOM；它们必须直接连接到一个收集器。如果 8.0 之前的代理尝试连接到 MOM，则会发生以下情况：

- MOM 拒绝此连接。
- CA Introscope 将警告消息写入 MOM 日志和代理日志。

**注意：** 当对超载的收集器进行负载均衡时，在 CA APM 9.1 之前的版本中，MOM 不考虑已配置为直接连接到收集器的代理。从 CA APM v9.1 开始，MOM 考虑并可以断开 9.1 及其前后版本的代理。要保持 9.1 前后版本的代理连接到特定收集器且不进行负载均衡，请将“代理 - 收集器”元素添加到 loadbalancing.xml。

**注意：** 如果群集处理的是包括代理和 TIM 的满载，请对运行企业管理器服务的收集器使用[加权因子 \(p. 99\)](#)。企业管理器服务可以要求越来越多的资源，因此使用加权因子可以补偿可能减少的度量标准容量。

## MOM 将代理分配给收集器的方式

多个因素决定 MOM 将代理分配给收集器的方式。

- 代理没有与任何收集器的连接历史记录

如果代理是第一次启动或重新启动，则没有与任何收集器的连接历史记录。在这种情况下，MOM 根据负载分布配置将代理分配给允许的可用收集器。

- 连接类型

只将代理分配给支持该代理用来连接到 MOM 的相同连接类型的收集器。例如，如果代理使用 HTTP 连接到 MOM，则收集器必须已启用 HTTP 连接。有关设置连接类型的信息，请参阅《CA APM Java 代理实施指南》或《CA APM .NET 代理实施指南》。

- 在 loadbalancing.xml 文件中进行的配置

在 loadbalancing.xml 文件中进行这些配置：

- 设置 `<include>` 语句，以允许代理连接到一组特定的收集器。
- 设置 `<exclude>` 语句，以禁止代理连接到一组特定的收集器。
- 将 `latched` 属性设置为 `true`，以将代理连接到一组允许的收集器中的特定首选收集器。

- 代理与特定收集器的连接历史记录

当代理从群集中的一个收集器转移到另一个收集器时，CA Introscope 能够防止 SmartStor 数据爆发。如果代理先前已连接到某个收集器，则除非以下因素起作用，否则 MOM 支持该收集器用于未来的连接：

- 收集器在 loadbalancing.xml 中配置为禁止。
- 有欠载的备用收集器可用。
- 首选的收集器超载。

- 在 IntroscopeEnterpriseManager.properties 文件中进行的配置

在 IntroscopeEnterpriseManager.properties 文件中进行这些配置：

- 设置代理负载平衡度量标准的加权因子。
- 设置代理负载平衡度量标准的阈值。
- 对于[细粒度代理连接配置](#) (p. 113)，设置 `introscope.apm.agentcontrol.agent.allowed` 属性。这样可以向收集器提供针对 loadbalancing.xml 中未定义的代理的允许或禁止指令。

## MOM 如何重新平衡群集

如果 MOM 检测到群集度量标准负载变得不平衡，它可以断开代理与收集器之间的连接并将代理重定向到其他收集器。如果任何收集器的度量标准负载与加权调整的群集平均值之间的差额超过已配置的容差阈值，则认为该群集不平衡。

群集变得不平衡的原因有多种，如以下示例所示：

- 收集器进程已停止或与代理断开连接。
- 有新的收集器添加到群集中。
- 许多代理直接连接到一个收集器。

MOM 会定期检查群集不平衡现象。如果群集不平衡，MOM 会试图通过将代理与度量标准负载相对较重的收集器断开连接来恢复平衡。断开的代理将重新连接到 MOM，并且被重定向到负载相对较轻的收集器。目标是重新分配代理，在整个群集中平衡加权调整的度量标准负载。如果 MOM 确定代理将重新分配给同一个收集器，MOM 将不断开该代理。

## 设置代理负载平衡度量标准的加权因子

在配置代理负载平衡时，MOM 根据权重调整后的负载将代理分配给收集器。您可以调整群集中单个收集器的加权因子。收集器可以处理的度量标准数确定收集器在群集中的相对能力。很多因素会影响收集器可以处理的度量标准数，包括以下因素：

- 可用的 CPU 容量。
- 内存。
- Smartstor 磁盘 IO 性能。
- 收集器是否将运行处理 CA CEM 数据加载的任何已分配企业管理器服务。

在设置代理负载平衡时，您可以配置加权因子，以要求 MOM 将较少的度量标准分配给容量较小的收集器。您可以通过设置度量标准的权重负载来帮助避免群集性能问题，以便更为强大的收集器处理较大的度量标准负载。

`introscope.enterprisemanager.clustering.login.<emID>.weight` 属性的值是一个正数，用于控制收集器的相对负载。特定收集器上的权重值除以群集上的所有权重值总和，即可得出分配给该收集器的度量标准负载所占的百分比。确定 [MOM 将代理分配给收集器的方式](#) (p. 98) 的因素可以修改此行为。

**注意：**在 `introscope.enterprisemanager.clustering.login.<emID>.weight` 属性名称中，`<emID>` 是任意标识符。每个收集器都有唯一的标识符。请提供适用于您的环境的标识符。

然后，在将代理分配给收集器时和重新平衡代理度量标准负载时，MOM 将使用权重调整后的度量标准计数。

例如，MOM 连接到三个收集器，而这三个收集器当前均没有报告的度量标准。

这三个收集器有以下权重设置：

- 收集器 A 的权重为 150。
- 收集器 B 的权重为 100。
- 收集器 C 的权重为 50。

MOM 以大约 3:2:1 的比率将度量标准分配给收集器 A、B 和 C。

**请执行以下步骤：**

1. 打开位于 `<EM_Home>/config` 目录的 `IntroscopeEnterpriseManager.properties` 文件。
2. 设置该属性，以将加权负载因子分配给收集器。  
`introscope.enterprisemanager.clustering.login.<emID>.weight`
3. 保存并关闭 `IntroscopeEnterpriseManager.properties`。

## 设置代理负载平衡度量标准的阈值

`introscope.enterprisemanager.loadbalancing.threshold` 属性为度量标准的不平衡设置群集容差或阈值。

默认 `introscope.enterprisemanager.loadbalancing.threshold` 属性设置为 20,000 个度量标准，表示收集器失去平衡的度量标准数必须达到 20,000 个，MOM 才会重新平衡代理。如果收集器小于或大于权重调整后的群集平均数且两者之差超过阈值，则收集器会失去平衡。请参阅 [代理负载平衡使用方案](#) (p. 101) 以查看一些示例。

配置一个可避免频繁重新平衡的负载均衡阈值。代理度量标准负载往往是相当稳定的。如果阈值设置得太低，在问题调查期间生成的临时度量标准会触发重新平衡。

请执行以下步骤：

1. 打开位于 `<EM_Home>/config` 目录的 `IntroscopeEnterpriseManager.properties` 文件。
2. 设置该属性，为度量标准不平衡配置群集容差。  
`introscope.enterprisemanager.loadbalancing.threshold`
3. 保存并关闭 `IntroscopeEnterpriseManager.properties`。

## 设置代理负载均衡时间间隔属性

`introscope.enterprisemanager.loadbalancing.interval` 属性可指示 MOM 间隔多长时间检查一次群集中可能发生的重新平衡。默认时间间隔为 600 秒（10 分钟），最小时间间隔为 120 秒（2 分钟）。

在重新分配任何代理后，群集需要几分钟的时间进行重新调整。如果负载均衡时间间隔太短，在群集调整到以前的状态之前可能需要进行重新平衡。如果使用应用程序分类视图，这个风险会更大。在这种情况下，重新分配代理时，这些代理必须将应用程序分类视图数据重新发送给新的收集器（这会耗费更多时间）。如果您已执行了这些操作，请注意由于重新平衡太频繁而可能引起的不稳定迹象：

- 适用于 **CA Introscope 8.x**：已部署 CA Introscope 8.x 负载均衡。
- 设置的负载均衡时间间隔低于默认值。

请执行以下步骤：

1. 打开位于 `<EM_Home>/config` 目录的 `IntroscopeEnterpriseManager.properties` 文件。
2. 对此属性进行设置，配置 MOM 检查群集中负载均衡的频率。  
`introscope.enterprisemanager.loadbalancing.interval`
3. 保存并关闭 `IntroscopeEnterpriseManager.properties`。

## 代理负载均衡使用方案

以下是一些可帮助您了解代理负载均衡在群集环境中的工作方式方案。

## 将新收集器添加到群集时的代理负载均衡

确定包含三个收集器 A、B 和 C 的群集已超载。

通过将一组连接属性添加到 MOM 上的 `IntroscopeEnterpriseManager.properties` 文件来动态添加收集器 D。此外，您已将该群集中所有收集器的重新平衡阈值设置为 10,000 个度量标准。通过在 `IntroscopeEnterpriseManager.properties` 文件中配置 `introscope.enterprisemanager.loadbalancing.threshold` 属性执行了此操作。

度量标准平均负载是分别报告给收集器 A、B 和 C 的 30,000 个度量标准，而将零个度量标准报告给收集器 D。由于以下因素，MOM 将对群集进行重新平衡：

- 30,000 个度量标准的平均负载与 0 个度量标准之间的差额超过了 10,000 个度量标准的阈值。

MOM 会重新平衡分别来自收集器 A、B 和 C 的 7000 个度量标准，并将全部 21,000 个度量标准重定向为报告给收集器 D。重新平衡后，会将 23,000 个度量标准报告给收集器 A，将 23,000 个度量标准报告给收集器 B，将 23,000 个度量标准报告给收集器 C，将 21,000 个度量标准报告给收集器 D。

## 添加具有代理的收集器时的代理负载均衡

MOM 连接到收集器 A 和 B。36,000 个度量标准报告给收集器 A，30,000 个度量标准报告给收集器 B。使用 `IntroscopeEnterpriseManager.properties` 文件中的 `introscope.enterprisemanager.loadbalancing.threshold` 属性将度量标准阈值设置为 10,000 个度量标准。收集器 C（报告给它的度量标准有 24,000 个）添加到了该群集。

MOM 不对度量标准负载进行重新平衡，因为：

- 平均值是每个收集器 30,000 个度量标准。 $(36,000 + 30,000 + 24,000) = 90,000$  个度量标准 / 3 个收集器。
- 没有一个收集器的度量标准数与 30,000 的差额超过 10,000 个度量标准阈值。

## 收集器出现故障时的代理负载平衡

MOM 连接到收集器 A、B 和 C。报告给收集器 A 的度量标准有 36,000 个，报告给收集器 B 的度量标准有 30,000 个，报告给收集器 C 的度量标准有 24,000 个。收集器 A 出现故障，报告给收集器 A 的代理将重新连接到 MOM。MOM 将大约 15,000 个度量标准重定向到收集器 B，并将 21,000 个度量标准重定向到收集器 C。现在，报告给收集器 B 和 C 的度量标准各有 45,000 个。

## 收集器重新启动时的代理负载平衡

收集器 A 在出现故障后恢复时，群集是不平衡的。平均度量标准负载为 30,000 个度量标准  $[0 + 45,000 + 45,000]/3$ 。然而，报告给收集器 B 和 C 的度量标准各有 45,000 个，

- 这比平均值多 15,000 个度量标准。
- 这超过了 10,000 个度量标准阈值。

因此，MOM 将总共具有 15,000 个度量标准的代理分别从收集器 B 和 C 断开连接，然后将全部的 30,000 个度量标准重定向到收集器 A。这会导致将 30,000 个度量标准分别报告给收集器 A、B 和 C。

## 具有权重的代理负载平衡

MOM 连接到收集器 A、B 和 C。阈值设置为 10,000。报告给收集器 A 的度量标准有 24,000 个，报告给收集器 B 的度量标准有 30,000 个，报告给收集器 C 的度量标准有 36,000 个，总共有 90,000 个度量标准。群集的每个收集器平均有 30,000 个度量标准。您已经将收集器 A 的权重设置为 150，将收集器 B 的权重设置为 100，将收集器 C 的权重设置为 50。平均权重是 100（权重之和除以收集器数，或  $(150 + 100 + 50)/3$ ）。

理想情况下，每个收集器的度量标准负载应当与其相对权重成比例。由于收集器 A 的权重为 150，因此理想情况下它应当有 45,000 个度量标准。其权重比平均值高 50%，因此理想情况下其度量标准负载应当比平均值 30,000 个度量标准高 50%。收集器 B 的权重等于平均值，因此理想情况下其度量标准负载应为平均值，即 30,000 个度量标准。收集器 C 的权重是平均值的 50%，因此理想情况下其度量标准负载应为平均值的 50%，即 15,000 个度量标准。

基于这些相对权重和度量标准平均值，群集是不平衡的。收集器 A 欠载，因为它小于权重调整后的平均值，且两者之差大于阈值 (24,000 - 45,000 = -21,000)。收集器 B 完全平衡，因为其度量标准负载等于权重调整后的平均值，即 30,000 个度量标准。收集器 C 超载，因为它大于权重调整后的平均值，且两者之差大于 10,000 个度量标准的阈值 (36,000 - 15,000 = 21,000)。通过将具有 21,000 个度量标准的代理从收集器 C 中逐出，然后将其重定向到收集器 A，MOM 使群集重新平衡。

## 配置对收集器的代理分配

使用 MOM `loadbalancing.xml` 可以配置代理元素，这些元素将控制 MOM 负载均衡器如何将连接代理分配给收集器。您可以配置 `include` 和 `exclude` 元素，以允许和禁止代理连接到特定的企业管理器。

**注意：**当对超载的收集器进行负载平衡时，在 CA APM 9.1 之前的版本中，MOM 不考虑已配置为直接连接到收集器的代理。从 CA APM v9.1 开始，MOM 考虑并可以断开 9.1 及其前后版本的代理。要保持 9.1 前后版本的代理连接到特定收集器且不进行负载平衡，请将“代理 - 收集器”元素添加到 `loadbalancing.xml`。

请执行以下步骤：

1. 在 MOM 上导航到 `<企业管理器主目录>/config` 目录。
2. 打开 `loadbalancing.xml`。
3. 定义属性以满足您的环境的需求。

在定义这些属性时，使用下列准则和[代理负载平衡配置示例](#) (p. 107)：

- `<agent-collector name>` 属性是可选的。
- MOM 负载均衡器按顺序对 `<agent-collector>` 元素进行赋值。  
如果连接代理与某个 `<agent-specifier>` 正则表达式匹配，则将其分配给 `<include>` 列表中的一个收集器。优先选择 `loadbalancing.xml` 中第一个匹配的 `<agent-specifier>`。如果没有 `<include>` 列表，该代理将被分配给不在 `<exclude>` 列表中的一个收集器。如果没有满足这些限制的可用收集器，则代理对收集器连接的请求将被拒绝。
- 对于每个 `<agent-collector>` 元素，定义一个或多个 `<agent-specifier>` 元素以匹配一组代理。
- 确保 `<agent-specifier>` 的文本内容为 Perl5 正则表达式，例如 `.*\|.*\|EPAgent1</agent-specifier>`。



**注意：**代理说明符正则表达式必须包括代理路径名称的三个元素：<主机名称>|<自定义进程名称>|<代理名称>。例如，要包括名称以 EPAgent 开头的所有代理，可使用以下内容：

```
<agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
```

- 对于 <agent-collector> 元素，包含列表可以为空。包含列表还可以包含允许代理连接的收集器。

- 如果包含列表为空，则不允许代理连接到任何收集器。

```
<include>
</include>
```

- 在 <include> 和 </include> 元素内，可以添加允许代理连接的收集器。

在该示例中，仅允许在名为 localhost@5002 的收集器上使用代理。

```
<include>
  <collector host="localhost" port="5002"/>
</include>
```

- 对于 <agent-collector> 元素，排除列表可以为空。排除列表还可以包含不允许代理连接的收集器。

- 如果排除列表为空，将允许代理连接到所有收集器。

```
<exclude>
</exclude>
```

- 在 <exclude> 和 </exclude> 元素内，可以添加不允许代理连接的收集器。

在该示例中，仅不允许在名为 localhost@5002 的收集器上使用代理。

```
<exclude>
  <collector host="localhost" port="5002"/>
</exclude>
```

- 将 latched 属性设置为 true 以表示优先连接特定收集器（只要该收集器可用）。该收集器称为 **锁定收集器**。

在该示例中，代理锁定到了端口 6001 上名为 newCollector-ip 的收集器。当 newCollector-ip 不可用时，MOM 可以将代理分配给 Collector1-ip。

```
<include>
  <collector host="newCollector-ip" port="6001" latched=" true" />
  <collector host="Collector1-ip" port="6001" />
</include>
</agent-collector>
```

如果仅将一个收集器添加到包含列表，则不需要 latched 属性设置。

如果多个收集器的 latched 为 true，则连接首选项将应用于所有锁定的收集器。

当 `latched` 属性设置为 `true`，并且收集器超载时，MOM 不从收集器断开代理。如果锁定收集器关闭，则断开的代理将连接到另一个允许的可用锁定收集器。

如果没有可用的锁定收集器，代理将连接到允许的收集器。如果没有允许的可用收集器，[代理行为将取决于代理版本](#) (p. 117)。例如，如果您的环境中十个收集器，可以将代理配置为锁定到一个或多个收集器。如果锁定的收集器都变得不可用，MOM 可以将代理重定向到其他解锁的可用收集器。

如果未对某收集器设置 `latched` 属性，仅当所有锁定的收集器都不可用时，代理才会连接到该收集器。

`latched` 属性的默认值为 `false`。

- 如果部署了一个或多个跨群集数据查看器并且使用了负载平衡，请将所需的代理仅连接到 CDV 所连接的收集器。否则，MOM 可以从带有 CDV 连接的收集器到其他收集器之间对代理进行负载平衡。在这种情况下，会发生以下情况：
  - CDV 无法收集关于已移动代理的度量标准数据。
  - CDV Workstation 用户无法查看关于已移动代理的数据。
- 要对同一群集中承载的收集器代理进行负载平衡，请提供与默认通信通道关联的端口号。默认端口为 5001。

对于这些代理-企业管理器的任一通信协议，请提供正确的端口号：

- 直接套接字连接
  - HTTP 隧道连接或通过代理服务器的 HTTP 隧道
  - HTTPS 连接
  - SSL 连接
- 要对不同群集中承载的收集器代理进行负载平衡，请提供与特定安全通信通道关联的端口号。一个群集的 MOM 无法看到其他群集的收集器的属性。

对于这些代理-企业管理器的任一通信协议，请提供正确的特定安全通信通道端口号：

- 直接套接字连接。向默认通信通道提供端口（默认情况下是端口 5001）。
- HTTP 隧道连接或通过代理服务器的 HTTP 隧道。提供 HTTP 端口（默认情况下是 8081）。
- HTTPS 连接。提供 HTTPS 端口（默认情况下是 8444）。
- SSL 连接。提供 SSL 端口（默认情况下是 5443）。

#### 4. 保存并且关闭 loadbalancing.xml。

在热部署期间，当企业管理器检查属性文件时新值会自动生效。热部署大约每 60 秒执行一次。MOM 在下一个负载平衡时间间隔对群集进行负载平衡。

## 代理负载平衡配置示例

您可以通过各种方法配置 MOM 代理负载平衡属性。这些配置示例提供了代码示例：

- [将代理分配给特定的收集器或收集器组](#) (p. 107)
- [将代理排除在特定收集器或收集器组外](#) (p. 108)
- [将多个代理分配给多个收集器](#) (p. 109)
- [将代理分配给同一群集中的特定收集器](#) (p. 109)
- [将代理分配给不同群集中的特定收集器](#) (p. 110)

### 将代理分配给特定的收集器或收集器组

以下示例显示了如何配置将名为 MyAgent 的代理分配给端口 5001 上名为 “myhost” 的收集器。

```
<agent-collector name="Assign MyAgent to One Collector Example">
  <agent-specifier>.*\|.*\|MyAgent</agent-specifier>
  <include>
    <collector host="myhost" port="5001"/>
  </include>
</agent-collector>
```

以下示例显示了如何配置 latched 属性，其中：

- 代理被分配连接到端口 6001 上名为 “newCollector-ip” 的收集器。
- 在 newCollector-ip 不可用时，MOM 可以将名称中含有 “EPAgent” 的所有代理分配给 Collector1-ip 或 Collector2-ip。

```
<agent-collector name="Latch when Collector Unavailable Example">
  <agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
  <include>
    <collector host="newCollector-ip" port="6001" latched="true" />
    <collector host="Collector1-ip" port="6001" />
    <collector host="Collector2-ip" port="6001" />
  </include>
</agent-collector>
```

以下示例显示了如何分配代理，其中：

- 收集器在端口 5001 和 5002 上均称为 “localhost”。
- 收集器 localhost:5001 优先于 localhost:5002。

```
<agent-collector name="Allow EPAGents on Two Collectors and One is Preferred Example">
  <agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
  <include>
    <collector host="localhost" port="5001" latched="true"/>
    <collector host="localhost" port="5002"/>
  </include>
</agent-collector>
```

以下示例显示了如何分配代理，其中：

- 收集器在端口 5001、5002、5003 和 5004 上被命名为“localhost”。
- 收集器 localhost:5001 和 localhost:5003 优先于 localhost:5002 和 localhost:5004。

```
<agent-collector name="Allow EPAGents on Four Collectors and Two are Preferred Example">
  <agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
  <include>
    <collector host="localhost" port="5001" latched="true"/>
    <collector host="localhost" port="5002"/>
    <collector host="localhost" port="5003" latched="true"/>
    <collector host="localhost" port="5004"/>
  </include>
</agent-collector>
```

### 将代理排除在特定收集器或收集器组外

以下示例显示了如何从名为 MyHost 的收集器排除名为 MyAgent 的代理。

```
<agent-collector name="Exclude MyAgent from a Collector Example">
  <agent-specifier>.*\|.*\|MyAgent</agent-specifier>
  <exclude>
    <collector host="MyHost" port="5001"/>
  </exclude>
</agent-collector>
```

以下示例显示了如何从多个收集器排除多个代理。

```
<agent-collector name="Exclude Two Agents Assigned from Two Collectors Example">
  <agent-specifier>.*\|.*\|MyAgent.*</agent-specifier>
  <agent-specifier>.*\|.*\|MyOtherAgent.*</agent-specifier>
  <exclude>
    <collector host="MyHost" port="5001"/>
    <collector host="MyOtherHost" port="5001"/>
  </exclude>
</agent-collector>
```

## 将多个代理分配给多个收集器

以下示例显示了如何将多个代理分配给多个收集器。

```
<agent-collector name="Two Agents Assigned to Two Collectors Example">
  <agent-specifier>.*\|.*\|MyAgent.*</agent-specifier>
  <agent-specifier>.*\|.*\|MyOtherAgent.*</agent-specifier>
  <include>
    <collector host="MyHost" port="5001"/>
    <collector host="MyOtherHost" port="5001"/>
  </include>
</agent-collector>
```

## 将代理分配给同一群集中的特定收集器

下列示例显示了如何将名为 EPAgent 的代理分配给群集中的收集器，其中：

- 名为“host1”和“host2”的收集器处于同一群集。
- 连接到 host1 或 host2 的 EPAgent 可以使用这些连接中的任何一个：
  - 直接套接字
  - HTTP
  - HTTPS
  - SSL
- 收集器 host1 和 host2 都将端口 5001 用作默认通信通道端口。
- 在 host1 不可用时，MOM 可以将名字中带有“EPAgent”的所有代理分配到 host2。

注意，要将代理分配给 host1 和 host2，MOM 会使用默认通信信道端口，且 loadbalancing.xml 也有此要求。

```
<agent-collector name="Allow EPAGents on Two Collectors in the Same
Cluster Example">
  <agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
  <include>
    <collector host="host01" port="5001"/>
    <collector host="host02" port="5001"/>
  </include>
</agent-collector>
```

## 将代理分配给不同群集中的特定收集器

下列示例显示了如何将名为 EPAgent 的代理分配给不同群集中的收集器，其中：

- 名为“host1”和“host2”的收集器处于不同群集。
- 连接到 host1 或 host2 的 EPAgent 可以使用这些连接中的任何一个：
  - 直接套接字
  - HTTP
  - HTTPS
  - SSL
- 在 host1 不可用时，MOM 可以将名字中带有“EPAgent”的所有代理分配到 host2 的特定通信端口。

注意，要将代理分配给 host1 和 host2，MOM 会使用企业管理器通信信道端口的特定 EPAgent，且 loadbalancing.xml 也有此要求。

下列示例显示出，在代理使用直接套接字连接连接到收集器时，如何将 EPAgent 分配给在不同群集的收集器。

```
<agent-collector name="Allow EPAgents on Two Collectors in Different Clusters -
Direct Socket Connection Example">
  <agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
  <include>
    <collector host="host01" port="5001"/>
    <collector host="host02" port="5001"/>
  </include>
</agent-collector>
```

下列示例显示出，在代理使用 HTTP 连接到收集器时，如何将 EPAgent 分配给在不同群集的收集器。

```
<agent-collector name="Allow EPAgents on Two Collectors in Different Clusters -
HTTP Example">
  <agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
  <include>
    <collector host="host01" port="8081"/>
    <collector host="host02" port="8081"/>
  </include>
</agent-collector>
```

下列示例显示，在代理使用 HTTPS 连接到收集器时，如何将 EPAgent 分配给在不同群集的收集器。

```
<agent-collector name="Allow EPAgents on Two Collectors in Different Clusters -
HTTPS Example">
  <agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
  <include>
    <collector host="host01" port="8444"/>
    <collector host="host02" port="8444"/>
  </include>
</agent-collector>
```

下列示例显示，在代理使用 SSL 连接到收集器时，如何将 EPAgent 分配给在不同群集的收集器。

```
<agent-collector name="Allow EPAgents on Two Collectors in Different Clusters -
SSL Example">
  <agent-specifier>.*\|.*\|EPAgent.*</agent-specifier>
  <include>
    <collector host="host01" port="5443"/>
    <collector host="host02" port="5443"/>
  </include>
</agent-collector>
```





# 第 8 章：配置代理—企业管理器网络拓扑

---

您可以计划和配置哪些代理或者代理组可以连接这些计算机：

- 特定单机企业管理器。
- 收集器。
- 收集器组。

CA APM 将该过程命名为计划和配置 CA APM 代理—企业管理器网络拓扑（或结构）。

此部分包含以下主题：

[代理—企业管理器网络拓扑概述](#) (p. 113)

[代理连接信息在 CA Introscope 中传播的方式](#) (p. 115)

[配置如何影响代理到企业管理器的连接](#) (p. 116)

[当代理与企业管理器断开连接时会发生什么情况](#) (p. 117)

[当代理连接请求被拒绝时会发生什么情况](#) (p. 117)

[配置代理的过程—企业管理器网络拓扑](#) (p. 118)

[规划代理—企业管理器网络拓扑](#) (p. 119)

[配置在没有 loadbalancing.xml 规则时是否允许新代理连接](#) (p. 121)

[配置代理重新连接等待时间](#) (p. 121)

[配置禁止连接的代理连接限定限值](#) (p. 122)

[配置代理连续重新连接到任何允许的企业管理器](#) (p. 122)

[为企业管理器允许和禁止的代理配置 loadbalancing.xml](#) (p. 124)

[对代理进行故障排除—企业管理器网络拓扑](#) (p. 124)

## 代理—企业管理器网络拓扑概述

计划和配置代理 - 企业管理器网络拓扑的目的是防止或减少 CA APM 性能问题。如：

- 防止新代理被随机启动，并大量连接某个特定收集器。
- 防止测试环境中的代理连接生产环境。

您可以使用这些文件和属性来控制代理如何以及何时连接到特定的独立企业管理器或收集器：

- `loadbalancing.xml` 文件。
- `EnterpriseManager.properties` 文件中的 `introscope.apm.agentcontrol.agent.allowed` 属性。
- `introscopeAgent.profile` 文件的 `introscope.agent.enterprisemanager.failbackRetryIntervalInSeconds` 属性。

在 [loadbalancing.xml](#) 中配置 MOM 代理负载平衡 (p. 104) 时，请基于以下因素告知 MOM 移动代理的目标位置：

- 收集器容量。
- 生成的代理度量标准数量。
- 收集器容量加权因子。

### 示例

您的环境包括 MOM 和五个收集器。您想让代理 1 和代理 2 针对收集器 1 和收集器 2 进行负载平衡。您为这些代理配置 `loadbalancing.xml` 以便连接到企业管理器：

- 允许代理 1 和代理 2 连接到收集器 1 和 2。
- 不允许这些代理连接到收集器 3、4 和 5。

如果有超载，MOM 会按以下方式处理代理：

- 根据实时群集负载，分配收集器 1 和收集器 2 上的代理 1 和代理 2。
- 决不允许这些代理连接到收集器 3、4 或 5。

您还可以将细粒度代理的 `loadbalancing.xml` 文件用于企业管理器连接设置，然后 MOM 会在整个群集中执行它。此章描述您可以如何对企业管理器连接实施细粒度代理。

启动时以及每隔 10 分钟，MOM 都会在 `loadbalancing.xml` 中向每个收集器发送代理允许和禁止连接规则集。收集器使用这些规则了解当代理请求连接时，可以接受哪些代理。收集器将这些规则发送到每个代理，以便每个代理了解在这些操作发生时，它可以连接哪些收集器：

- MOM 停机。
- 收集器基于禁止配置设置拒绝代理连接请求。

如果[系统拒绝了代理与企业管理器的连接](#) (p. 117)，那么 APM 状态控制台“被拒绝的代理”列表会显示一个条目。如果代理是被动地连接到企业管理器，而不是在发送数据，APM 状态控制台“被拒绝的代理”列表也会显示一个条目。

您可以使用 APM 状态控制台“被拒绝的代理”列表，针对特定代理或代理组监视重复的遭到拒绝连接和被动连接。然后，可以配置 `loadbalancing.xml` 以便允许拒绝的或被动的代理连接到其他收集器。

## 代理连接信息在 CA Introscope 中传播的方式

CA Introscope 可以控制代理到企业管理器的连接信息，您可以在 MOM 中定义该信息。MOM 确保在群集中的各收集器和代理之间执行任何关联的配置。

MOM 定期将 `loadbalancing.xml` 发送到所有收集器，并在整个群集中同步 `loadbalancing.xml`。CA Introscope 忽略任何收集器或 CDV `loadbalancing.xml` 配置。

如果 MOM 在收集器接收到 `loadbalancing.xml` 之后关闭，收集器将使用从 MOM 接收到的 `loadbalancing.xml` 允许或禁止配置。如果收集器从未连接到 MOM，收集器将在其 `IntroscopeEnterprismanager.properties` 文件中使用其 `introscope.apm.agentcontrol.agent.allowed` 属性来允许代理连接。如果 MOM 首次连接到收集器，MOM 会将其 `introscope.apm.agentcontrol.agent.allowed` 属性值传输到收集器。MOM 值将覆盖收集器值。

收集器也会将 `introscope.apm.agentcontrol.agent.allowed` 属性用于针对 `loadbalancing.xml` 中未定义的代理的允许或禁止指令。

MOM 也向代理提供代理允许连接到且可用的企业管理器列表。该列表名为“允许的企业管理器”列表。“允许的企业管理器”列表基于企业管理器 IP 地址，因此可以包括不同群集中的企业管理器。

“允许的企业管理器”列表在以下任意计算机发生故障时指示代理连接到哪个企业管理器：

- MOM
- 独立企业管理器
- 代理连接到的初始收集器。

在存在以下两个因素时，企业管理器将基于 `loadbalancing.xml` 指令准备“允许的企业管理器”列表：

- 独立企业管理器关闭。
- 您的环境既包含独立企业管理器，又包含群集

“允许的企业管理器”列表指示代理连接到其他独立企业管理器或收集器。

代理重新启动时，会获得来自其 `IntroscopeAgent.profile` 文件中的 `introscope.agent.enterprisemanager.connectionorder` 属性的初始收集器连接信息。除定义的值之外，允许的收集器会自动提供给该属性。允许的可用收集器或独立企业管理器的列表仍然位于代理内存中，直到代理重新启动。代理重新启动后，会将允许的可用企业管理器列表从收集器发送到代理。

## 配置如何影响代理到企业管理器的连接

代理配置为在企业管理器上允许或禁止时，企业管理器可以在代理请求连接时采取各种操作。企业管理器可以接受连接或拒绝连接。企业管理器接受连接请求时，代理可以采用以下两种方式之一进行连接：

- 主动连接，且将度量标准数据发送到企业管理器。
- 被动连接，且不发送数据。

[企业管理器拒绝连接请求](#) (p. 117)时，代理的行为将根据其版本的不同而异。

基于代理版本以及允许和禁止配置，企业管理器可以采取三个操作。这些操作可以生成四种代理连接状态。其中两个状态使代理显示在 APM 状态控制台“拒绝的代理”列表中。

下表显示了企业管理器、代理和 APM 状态控制台在配置有允许和禁止的代理请求企业管理器连接时的行为方式。

代理版本	Allowed/Disallowed 配置	收到连接请求后的企业管理器操作	生成的代理连接状态	显示在 APM 状态控制台“拒绝的代理”列表中
9.1	允许	已接受主动连接	连接的代理主动发送数据	否
9.1 之前的版本	允许	已接受主动连接	连接的代理主动发送数据	否
9.1	禁止	连接被拒绝	已断开连接	是

代理版本	Allowed/Disallowed 配置	收到连接请求后的企业管理器操作	生成的代理连接状态	显示在 APM 状态控制台“拒绝的代理”列表中
9.1	禁止	已接受被动连接	连接的代理处于被动状态；不发送数据	是
9.1 之前的版本	禁止	连接被拒绝	断开的代理重试连接	是

## 当代理与企业管理器断开连接时会发生什么情况

当出现对代理进行负载平衡或企业管理器关闭等情况时，代理将与企业管理器断开连接。在特定情况下（当配置更改指示企业管理器禁止之前允许连接的代理时），代理也会与企业管理器断开连接。企业管理器通过断开现在配置为禁止的已连接代理来响应指示。

**适用于 9.1 以前的代理：**当以下操作发生时，这些代理将与企业管理器断开连接：

- 属性或 `loadbalancing.xml` 配置将代理与收集器的连接从允许更改为禁止。
- 代理连接到的企业管理器不再接受连接。

**适用于 9.1 代理：**当配置从允许连接更改为禁止连接且达到 `introscope.enterprisemanager.agent.disallowed.connection.limit` 限定值时，这些代理将与企业管理器断开连接。

## 当代理连接请求被拒绝时会发生什么情况

`loadbalancing.xml` 中设置的配置和 `introscope.apm.agentcontrol.agent.allowed` 属性将决定允许还是禁止代理与特定企业管理器连接。代理请求连接到企业管理器时，企业管理器可以接受或拒绝连接请求。

发生以下任一情况时，代理的连接请求会被拒绝：

- `introscope.apm.agentcontrol.agent.allowed` 属性已设置为 `true`，且 `loadbalancing.xml` 禁止代理进行连接。

- `introscope.apm.agentcontrol.agent.allowed` 属性已设置为 `false`，且 `loadbalancing.xml` 未明确允许代理进行连接。
- 达到或超过以下任何一个限定值：
  - `introscope.enterprisemanager.agent.disallowed.connection.limit`。
  - `introscope.enterprisemanager.agent.connection.limit`。

企业管理器拒绝代理连接请求时，可能会发生以下操作：

- 已连接到企业管理器的代理断开连接。
- 已断开连接的代理尝试连接到允许连接的其他企业管理器。

代理继续尝试连接到企业管理器，直到成功完成连接或尝试完所有企业管理器为止：

- 允许代理连接到的企业管理器。
- 可供连接的企业管理器。

如果代理被所有企业管理器拒绝，则代理的行为将因其 `introscopeagent.profile` 文件中的

`introscope.agent.enterprisemanager.failbackRetryIntervallInSecondsproperty` 设置而不同。如果属性配置按如下进行设置：

- 如果已取消注释并设置了持续时间，则代理会根据持续时间定期尝试与允许的企业管理器连接。
- 如果未设置（已注释掉）持续时间，则代理会根据 CA APM 代理版本执行以下操作：
  - **适用于 9.1 以前的代理：**断开与企业管理器的连接并继续尝试与其重新连接。
  - **适用于 9.1 代理：**被动与“允许的企业管理器”列表中最后允许的企业管理器连接。代理不会将任何度量标准数据发送给企业管理器。在等待通过企业管理器配置信息将代理的状态更改为允许连接时，代理会处于休眠状态。

## 配置代理的过程—企业管理器网络拓扑

将代理配置为企业管理器网络拓扑需要执行以下高级步骤。

1. [将代理规划到企业管理器或收集器拓扑](#) (p. 119)。
2. 如果适用，为您的部署配置 `introscopeopenenterprisemanager.properties` 文件。
  - a. （可选）[配置允许还是禁止不与 `loadbalancing.xml` 中的任何正则表达式匹配的代理与 MOM 或特定企业管理器建立连接](#) (p. 121)。

设置 `introscope.apm.agentcontrol.agent.allowed` 属性。

- b. (可选) [为代理尝试重新连接到企业管理器配置随机持续时间 \(p. 121\)](#)。

设置 `introscope.apm.agentcontrol.agent.reconnect.wait` 属性。

- c. (可选) [配置可以被动连接到企业管理器且不发送数据的 9.1 版本代理的数目 \(p. 122\)](#)。

设置

`introscope.enterprisemanager.agent.disallowed.connection.limit`。

3. 如果适用，为您的部署配置 `IntroscopeAgent.profile` 文件。

- (可选) [配置与企业管理器断开连接的代理是否不断尝试重新连接到任何允许的企业管理器 \(p. 122\)](#)。

设置

`introscope.agent.enterprisemanager.failbackRetryIntervalInSeconds` 属性。

4. [配置 `loadbalancing.xml` \(p. 124\)](#)。

- a. (可选) 配置锁定属性，以便特定代理始终连接到特定企业管理器。
- b. (可选) 配置 `include` 和 `exclude` 元素，以允许和禁止代理连接到特定的企业管理器。
- c. 保存 `loadbalancing.xml`。

在热部署期间（热部署大约每 60 秒执行一次），当企业管理器检查属性文件时新值会生效。MOM 在下一个负载平衡时间间隔将更新的 `loadbalancing.xml` 发送到群集中的收集器。

5. 根据需要执行系统监控并重新配置。

- a. 根据需要重新配置任何属性。
- b. 更新 `loadbalancing.xml`。

## 规划代理—企业管理器网络拓扑

在配置代理连接分配之前，可以将代理规划到企业管理器或收集器拓扑。在这些分配中，您可以配置允许或不允许哪些代理连接到特定的单个收集器或收集器组。

如果您的业务惯例需要，请将代理设置到子群集。您可以将代理分配给一组特定的收集器，然后配置 `loadbalancing.xml`，以便 MOM 仅该组收集器进行负载平衡。例如，您可以将监控特定业务部门的应用程序的代理连接到群集中十分之三的收集器。

在规划期间，会提出并回答下列问题，如：

- 群集或特定收集器上是否允许或禁止代理类或代理组或特定代理？
- 是否应对一些收集器提供超载保护？

例如，一些收集器是否需要防止配置错误的代理直接连接？如果所有代理都具备相同的代理配置文件并尝试进行连接，则它们将淹没单个 IP 地址。连接到收集器的代理过多会导致该收集器崩溃。

**请执行以下步骤：**

1. 对于每个代理组或代理类，确定您希望哪组收集器：

- a. 允许访问。
- b. 禁止访问。

2. 确定与 `loadbalancing.xml` 不匹配的代理的默认连接活动。

想要在特定企业管理器上允许或禁止连接与 `loadbalancing.xml` 不匹配的所有代理？

3. 是否将对任何代理进行负载平衡？如果是，在需要将其移至的所有收集器上是否允许这些代理？

请认真考虑代理连接限制的影响，因为它们会限制 MOM 的负载平衡选项。代理不允许连接到欠载的收集器时，执行负载平衡的 MOM 无法从超载的收集器删除代理。在这种情况下，MOM 必须将其他代理从超载收集器负载平衡到欠载收集器。

4. 确定与企业管理器断开连接的代理的行为。

是否希望代理不断尝试重新连接到任何允许的企业管理器？

或者，基于 CA APM 代理版本：

- **适用于 9.1 以前的代理：**是否断开与企业管理器的连接并继续尝试与其重新连接？
- **适用于 9.1 的代理：**是否保持被动与代理的“允许的企业管理器”列表中最后允许的企业管理器连接？

被动连接的代理有以下特点：

- 不将任何度量标准数据发送到企业管理器。
- 不尝试重新连接到可用的其他企业管理器。

5. 您的 CA APM 环境是否允许代理跨以下 CA APM 组件进行连接：

- 群集？
- 收集器和独立的企业管理器？
- 群集、收集器和独立企业管理器的任意组合？



## 配置在没有 loadbalancing.xml 规则时是否允许新代理连接

确定在代理与 loadbalancing.xml 中的任何正则表达式不匹配时，是允许还是禁止所有新代理连接。需要针对以下计算机做出以上决定：

- MOM。
- 每个收集器。
- 任何独立的企业管理器。

您可以将 introscope.apm.agentcontrol.agent.allowed 属性设置为性能度量标准。

**注意：**MOM 属性值总是覆盖收集器值。仅在 MOM 连接到收集器之前使用收集器值。此时，会将 MOM 属性值传输到收集器并由其使用。

您也可以在 loadbalancing.xml 中使用该属性设置和配置，以微调您环境中的代理到企业管理器的连接。

请执行以下步骤：

1. 转到 <EM\_Home>\config 目录并打开 IntroscopeEnterpriseManager.properties 文件。
2. 设置 introscope.apm.agentcontrol.agent.allowed=true。
3. 保存 IntroscopeEnterpriseManager.properties 文件。

在热部署期间当企业管理器检查属性文件时（该检查大约每 60 秒发生一次）会应用该设置。

## 配置代理重新连接等待时间

您可以更改[已断开连接的代理](#) (p. 117) 尝试重新连接到独立企业管理器或收集器之前必须等待的秒数。不同的等待时段有助于 CA APM 避免在许多代理同时尝试重新连接到企业管理器时发生性能问题。您可以配置 introscope.apm.agentcontrol.agent.reconnect.wait 属性来更改等待时间。

请执行以下步骤：

1. 转到 <EM\_Home>\config 目录，并打开 IntroscopeEnterpriseManager.properties 文件。
2. 设置 introscope.apm.agentcontrol.agent.reconnect.wait 属性。
3. 保存 IntroscopeEnterpriseManager.properties 文件。

在热部署期间当企业管理器检查属性文件时（该检查大约每 60 秒发生一次）会应用该设置。

与企业管理器断开连接后，代理基于企业管理器生成的重新连接时间尝试重新连接。连接时间基于默认值和随机的附加正值或负值。

## 配置禁止连接的代理连接限定限值

**适用于代理 9.1:** 您可以限制配置为禁止连接但可以被动连接到独立企业管理器或收集器的代理 9.1 的数目。被动连接的代理有以下特点：

- 不将任何度量标准数据发送到企业管理器。
- 不尝试重新连接到可用的其他企业管理器。

设置此限定限值是一种衡量性能的方法，因为它限制了与企业管理器的连接数。每个连接都需要一些资源，因此大量连接可能会降低企业管理器的性能。

**请执行以下步骤：**

1. 转到 `<EM_Home>\config` 目录并打开 `IntroscopeEnterpriseManager.properties` 文件。
2. 设置 `introscope.enterprisemanager.agent.disallowed.connection.limit` 属性。
3. 保存 `IntroscopeEnterpriseManager.properties` 文件。

在热部署期间当企业管理器检查属性文件时（该检查大约每 60 秒发生一次）会应用该设置。

在达到限定值且配置为禁止连接的代理尝试连接到企业管理器时，企业管理器会执行以下操作：

- 记录事件。
- 拒绝新的连接。

## 配置代理连续重新连接到任何允许的企业管理器

您可以配置在所有企业管理器上被拒绝连接的代理是否不断循环浏览“允许的企业管理器”列表以尝试重新连接。以下是允许的企业管理器：

- 在代理配置文件 `introscope.agent.enterprisemanager.connectionorder` 属性值中配置的企业管理器。
- 根据 `loadbalancing.xml` 配置允许连接的任何企业管理器。

如果被拒绝的代理无法连接到企业管理器，则会采用以下方式处理连接：

- 尝试连接到“允许的企业管理器”列表中下一个允许的企业管理器。
- 不连接到对其配置为禁止的任何企业管理器。

将拒绝的代理配置为继续尝试连接具有以下特点：

- 可用于允许代理跨以下 CA Introscope 组件连接的环境：
  - 群集。
  - 收集器和独立企业管理器。
  - 群集、收集器和独立企业管理器的任意组合。
- 在以下条件下强制已断开连接的代理继续尝试连接到允许的企业管理器：
  - 在企业管理器可供连接之前。
  - 即使企业管理器属于不同的群集。

否则，代理会采用以下方式处理连接：

- 被动连接到企业管理器且不发送度量标准数据。
- 不尝试连接到允许的企业管理器，其中包括在不可用后变为可用的任何企业管理器。

**请执行以下步骤：**

1. 打开 IntroscopeAgent.profile 文件。
2. 设置 `introscope.agent.enterprisemanager.failbackRetryIntervalInSeconds` 属性。
3. 保存 IntroscopeEnterpriseManager.properties 文件。
4. 重新启动托管应用程序。

如果发生以下事件：

- 拒绝代理连接到企业管理器
- 企业管理器关闭

则代理立即尝试连接到“允许的企业管理器”列表中的下一个允许的企业管理器。

如果代理无法连接到任何允许的企业管理器，则代理将执行以下操作：

- 等待一段时间，此时间与 `introscope.agent.enterprisemanager.failbackRetryIntervallInSeconds` 属性中设置的持续时间相等。
- 重试连接到允许的企业管理器，从其“允许的企业管理器”列表中的第一个企业管理器开始。

此循环会一直重复，直到代理连接到可以主动向其发送数据的企业管理器。

## 为企业管理器允许和禁止的代理配置 [loadbalancing.xml](#)

您可以在 MOM 或独立企业管理器上[配置 `loadbalancing.xml`](#) (p. 104)，以允许和禁止特定企业管理器上的代理连接。

MOM 会每 10 分钟向收集器发送一次 `loadbalancing.xml` 中的代理连接信息，然后收集器将允许的企业管理器信息发送到代理。MOM 根据最新的 `loadbalancing.xml` 文件允许和禁止特定企业管理器上的代理连接。

如果您的代理从不需要 MOM 对其进行负载平衡，也可以配置 `loadbalancing.xml`。在以下示例中，MOM 从不将名为 EPAgent 的代理从名为 Collector1-ip 的收集器负载平衡到任何其他收集器。

```
<agent-collector name="EPagent connects to only collector1-ip">
<agent-specifier>.*\|.*\|EPagent</agent-specifier>
  <include>
    <collector host="collector1-ip" port="6001" />
  </include>
</agent-collector>
```

## 对代理进行故障排除—企业管理器网络拓扑

### 企业管理器如何处理拒绝的代理

MOM 每 10 分钟向群集中的所有收集器发送一次 `loadbalancing.xml`。`loadbalancing.xml` 和 `introscope.apm.agentcontrol.agent.allowed` 属性告诉企业管理器允许和禁止哪些代理与其建立连接。根据允许和禁止配置，企业管理器可以接受或拒绝代理连接请求。

以下是当企业管理器拒绝代理连接时发生的情况。

### 适用于 9.1 以前的代理

如果代理已连接，企业管理器会断开与 9.1 版本之前的代理的连接。这些代理将使用其“允许的企业管理器”列表来尝试连接到其他允许的可用企业管理器。如果拒绝代理连接到与所有企业管理器，则这些代理会继续尝试连接到符合以下条件的最后一个企业管理器：

- 可用。
- 允许连接到代理。

### 适用于 9.1 代理

企业管理器断开与 9.1 版代理的连接，然后该代理尝试连接到其他允许的可用企业管理器。如果拒绝代理连接到所有企业管理器，则代理会与已连接到的最后一个企业管理器建立连接。代理仍然连接到企业管理器，但是不发送任何数据。

## 收集器使用 `introscope.apm.agentcontrol.agent.allowed` 属性时

在 MOM 连接到收集器时，MOM 会向收集器提供 `introscope.apm.agentcontrol.agent.allowed` 属性和 `loadbalancing.xml`。如果 MOM 关闭，收集器将使用 MOM 提供的以下信息来获知允许和禁止哪个代理连接：

- `IntroscopeEnterpriseManager.properties` 文件中的当前 `introscope.apm.agentcontrol.agent.allowed` 属性设置。
- `loadbalancing.xml`。

如果 MOM 从未连接到收集器，MOM 尚未将其 `introscope.apm.agentcontrol.agent.allowed` 属性和 `loadbalancing.xml` 文件传输到收集器。因此，收集器使用自己的 `introscope.apm.agentcontrol.agent.allowed` 属性来决定允许还是禁止特定代理连接。

## 代理未将 `loadbalancing.xml` 正则表达式匹配为允许或禁止

`IntroscopeEnterpriseManager.properties` 文件中 `introscope.apm.agentcontrol.agent.allowed` 属性的值确定与 `loadbalancing.xml` 中的正则表达式不匹配的代理是否可以连接到收集器。

如果属性值为 `true`，则允许与 `loadbalancing.xml` 中的任何正则表达式均不匹配的代理连接到收集器。

如果属性值为 `false`，则拒绝与 `loadbalancing.xml` 中的任何正则表达式均不匹配的代理连接到收集器。

## 分配给代理的所有收集器不可用，其他收集器可用

### 9.1 版本之前的代理

收集器断开与代理的连接，之后代理尝试连接到 MOM。允许代理连接到的收集器均不可用，MOM 拒绝每个代理连接尝试。代理继续尝试连接到 MOM，直到某个允许代理连接到的收集器可用。允许的收集器可用时，MOM 将代理重定向到该收集器。

### 9.1 版代理

收集器断开与代理的连接，之后代理连接到 MOM 但不发送任何数据。允许的收集器可用时，MOM 将代理重定向到该收集器。

## 收集器使用直接连接处理不允许的代理的方式

MOM 定期将 `loadbalancing.xml` 发送到群集中的所有收集器。`loadbalancing.xml` 文件使每个收集器了解允许连接的代理。如果发生以下操作：

- `loadbalancing.xml` 文件已更新，以便在特定收集器上不允许使用某个代理。
- 该代理尝试连接到该收集器。

会导致下列操作。

### 9.1 版本之前的代理

收集器拒绝代理连接，代理继续连接尝试。

### 9.1 版代理

收集器为代理提供最新的“允许的企业管理器”列表。基于禁止的配置设置，不允许在收集器上使用代理。如果 MOM 可用，则会将代理重定向到可用的允许的收集器。如果 MOM 不可用，则代理使用其“允许的企业管理器”列表浏览允许的可用收集器。

## `introscope.apm.agentcontrol.agent.allowed` 属性缺失时的默认代理连接值

`introscope.apm.agentcontrol.agent.allowed` 属性的默认值为 `allowed`。

## CA Introscope 确定没有 MOM 可用时代理连接位置的方式

代理尝试连接到的收集器决定是允许还是拒绝连接。收集器基于其 `loadbalancing.xml` 文件中当前的允许和禁止配置做出决定。





# 第 9 章：使用命令行 Workstation

---

本章介绍了 Introscope 命令行 Workstation (CLW)，一个针对企业管理器的命令行界面。

此部分包含以下主题：

[关于命令行工作站 \(CLW\)](#) (p. 129)

[运行 CLW](#) (p. 130)

[CLW 命令参考](#) (p. 133)

[示例脚本](#) (p. 177)

## 关于命令行工作站 (CLW)

Introscope 命令行工作站 (CLW) 可以用来执行一些 Introscope 工作站功能。

CLW 可用来自动执行或排定 Introscope 操作任务。例如，您可以执行重复性任务，例如禁用一些管理模块中的多个警报时，使用 CLW 比使用工作站接口速度更快。同样，CLW 可用来排定必须自动执行或定期执行的任务。

使用 CLW 命令，可以执行以下操作：

- **管理管理模块和元素**—您可以列出、复制、重命名和删除管理模块和要素，查看它们是否处于活动状态，以及更改它们的当前状态。

使用 CLW 复制和重命名命令，您可以基于现有的管理模块和元素来创建新的管理模块和元素。但是，您无法使用 CLW 从头创建管理模块和元素或修改它们的详细信息。

- **控制代理**—您可以远程启动、停止和恢复代理报告，以及将配置文件复制到远程代理。

- **启动事务跟踪会话**—您可以编写脚本，用以在出现报警时自动启动事务跟踪会话。
- **关闭企业管理器**—您可以编写脚本，用以定时关闭企业管理器。例如，您可能需要在非工作时间停止企业管理器，而那时可能不方便使用工作站。
- **如果 CLW 退出**—如果未发生错误，CLW 以值 0 退出。如果发生以下任一情况，它将以负的状态代码退出：
  - 企业管理器身份验证失败。
  - 企业管理器出现连接问题，例如网络连接断开，主机名无效。
  - 存在无效的 WS 和企业管理器。

## 运行 CLW

本节概述了如何运行 CLW。有关特定命令的信息，请参阅 [CLW 命令参考](#) (p. 133)。

### JVM 要求

CLW 需要 JVM 1.6 或更高版本。

### 从何处运行 CLW 命令

您可以将 CLW 命令包含在脚本或批处理文件中，也可以在命令行中输入它们。CLW .jar 文件安装在 `<EM_Home>/lib` 目录中。从该目录运行 CLW 命令，或将该目录的路径包含在命令中。

### 使用 CLW 交互模式

通过使用 `-i` 标志可以从默认模式更改为交互模式，如下例所示。如果您计划为 CLW 编写脚本，将无法使用此模式，因为它会破坏脚本。

```
java -Xmx128M <EM_logon> <TT_properties> -jar CLWorkstation.jar > usage  
/ -i / <command>
```

交互模式将读取命令的命令行参数，执行命令，然后退出。但是，如果未传递命令行参数（`-DHost=` 等 JVM 选项除外），则交互模式将读取并执行一行标准输入，直至到达文件结尾或您退出系统。如果未传递参数且未提供输入，将输出一个错误并退出系统。以 `#` 符号开头的行将被忽略。

## 调用 CLW

CLW 命令语法为：

```
java -Xmx128M <EM_logon> -jar CLWorkstation.jar <command>
```

其中：

- `-Xmx128M` 设置 Java 堆大小以防发生 `java.lang.OutOfMemoryError` 错误。
- `<EM_logon>` 是您的企业管理器登录信息：
  - `Duser=<user name>`
  - `Dpassword=<password>`
  - `Dhost=<Enterprise Manager host / ip address>`
  - `Dport=<Enterprise Manager port number>`
- `<command>` 是 [CLW 命令参考](#) (p. 133) 中介绍的命令之一。

例如：

```
java -Xmx128M -Duser=jdoe -Dpassword=mypassword -Dhost=jdoeDT  
-Dport=5001 -jar CLWorkstation.jar <command>
```

如果您调用 CLW 时未提供登录信息，则将使用用于访问企业管理器的默认登录值：

```
java -Xmx128M -jar CLWorkstation.jar <command>
```

您在命令行或脚本中输入的每个 CLW 命令必须以 CLW 调用开头：

```
java -Xmx128M -jar CLWorkstation.jar
```

**注意：** 为避免发生 `java.lang.OutOfMemoryError`，请设置 Java 堆大小。

## CLW 区分大小写。

CLW 命令接受指定您的 Introscope 部署中的代理、管理模块和其他已命名项目的参数。CLW 区分大小写—您必须输入 Introscope 对象的精确名称。例如，如果一个代理被命名为 `WebLogic1`，引用 `weblogic1` 的 CLW 命令无法针对该代理执行。

## CLW 命令输出

CLW 命令将其输出返回到命令窗口。您可以根据需要将命令输出定向到一个文件中。

## CLW 和正则表达式

您可以使用 **CLW** 命令来操纵 **Introscope** 环境的元素，例如代理、管理模块、显示板、操作以及报警。根据目标的类型，您可以执行复制、列出、重命名、激活和停用等操作。

可以使用精确的文本字符串或 **Perl** 正则表达式指定 **CLW** 命令的一个或多个目标。例如，以下 **CLW** 命令列出连接到企业管理器的所有代理：

```
list agents matching (.*)
```

以下命令仅列出名称中包含字符串 **weblogic** 的代理：

```
list agents matching .*weblogic.*
```

## CLW 命令中的反斜线和引号

提供包含空格的 **CLW** 命令参数时，请将参数用引号 (") 引起来，并在每个引号前使用一个反斜线，以防 **shell** 对引号进行解释。例如：

```
\ "2005/01/01 12:20:37"
```

## 在不同环境中使用 CLW

正则表达式语法因您的操作系统和命令 **shell** 而异，在某些情况下，还取决于您是在命令行中还是在脚本中输入表达式。本章中的示例命令是针对 **Windows** 环境编写的，反映的是在批处理文件中使用正则表达式时所需要的语法。

## 配置命令行 Workstation 日志

可以配置 **CA APM** 以将命令行 **Workstation (CLW)** 命令记录到企业管理器控制台和 **IntroscopeEnterpriseManager.log** 文件（位于 **<EM\_Home>/logs** 目录）。

### 配置命令行 Workstation 日志：

1. 打开位于 **<EM\_Home>\config** 目录中的 **IntroscopeEnterpriseManager.properties** 文件。
2. 配置 **IntroscopeEnterpriseManager.properties** 文件中的以下属性，以在日志文件和企业管理器控制台上记录 **CLW** 命令：
  - a. 设置 **log4j.additivity.Manager.CLW=true**。

**注意：** 该属性的默认值为 `false`。

b. 设置 `log4j.logger.Manager.CLW=DEBUG`。

该属性的默认值为 `INFO`。

## CLW 命令参考

本节包含有关 CLW 命令的详细信息。

**注意：** 为每个命令显示的语法未包括命令的调用部分。如[调用 CLW](#) (p. 131) 中所述，每个 CLW 命令的开头必须为：`java -jar CLWorkstation.jar`

### 企业管理器命令

企业管理器聚合来自代理的应用程序性能数据，运行所请求的计算，使性能数据可供授权的客户端使用，并存储性能数据。

#### 关闭企业管理器

此命令可关闭企业管理器。要运行该命令，您必须具有关闭权限或完全权限。关闭企业管理器时，连接到企业管理器的任何工作站用户都将注销。

#### 语法

```
shutdown
```

#### 示例

```
shutdown
```

#### 输出

无。

#### 从 SmartStor 提取永久性数据（在某个时间范围之内）

此命令可从 SmartStor 提取指定时段的历史数据。您提供一个用以指定代理的正则表达式、一个用以指定度量标准组的正则表达式，以及时段的开始和结束时间。日期-时间字符串的 `hh:mm:ss` 部分是可选的—如果未提供，默认为 `00:00:00`（午夜）。

## 语法

```
get historical data from agents matching [REGULAR EXPRESSION] and  
metrics matching [REGULAR EXPRESSION] between [EXACT MATCH] and  
[EXACT MATCH] with frequency of [EXACT MATCH]  
(second/seconds/sec/secs/s)
```

## 示例

```
get historical data from agents matching (*.weblogic.*) and metrics  
matching (Servlets:Responses Per Interval) between \"2011-10-12  
00:00:00\" and \"2011-10-12 00:10:00\" with frequency of 60 seconds
```

此命令为名称中包含字符串 `weblogic` 的所有代理提取“Servlets:每个时间间隔的响应数”度量标准组的永久性数据。提取数据的时间范围是从 2011 年 10 月 12 日 00:00:00（午夜）到 2011 年 10 月 12 日 00:10:00，频率为 60 秒。

## 输出

SmartStor 数据以逗号分隔值 (CSV) 格式返回。

## 从 SmartStor 提取永久性数据（以 N 秒的频率提取前 N 分钟的数据）

此命令提取在执行该命令之前指定分钟数内的历史数据。提取的数据以特定的频率（秒数）显示。您可以提供一个用于指定代理的正则表达式、一个用于指定度量标准组的正则表达式、要提取历史数据的分钟数以及数据的提取频率。

## 语法

```
get historical data from agents matching [REGULAR EXPRESSION] and  
metrics matching [REGULAR EXPRESSION] for past [EXACT MATCH]  
(minute/minutes) with frequency of [EXACT MATCH]  
(second/seconds/sec/secs/s)
```

## 示例

```
get historical data from agents matching (*.weblogic.*) and metrics  
matching (Servlets:Responses Per Interval) for past 1 minute with frequency  
of 60 seconds
```

此命令为名称中包含字符串 `weblogic` 的所有代理提取“Servlets:每个时间间隔的响应数”度量标准组的永久性数据。提取数据的时间段为过去 1 分钟，频率为 60 秒。

## 输出

SmartStor 数据以逗号分隔值 (CSV) 格式返回。

## 指定用于身份验证的路径名

指定在连接到企业管理器时要使用的公钥文件的完整路径名，而不是使用用户名/密码身份验证。所用的公钥与用于上级管理器/收集器身份验证的公钥是同一个。

有关配置公钥的详细信息，请参阅《CA APM 安全指南》。

## Introscope 代理命令

代理作为托管应用程序的一部分在 Java 应用程序计算机上运行。它收集并汇总探针报告的数据，并将其发送给企业管理器。

## 列出代理

“列出代理”命令可列出已连接到企业管理器的一个或多个代理。您应提供一个用于确定列出哪些代理的正则表达式。

## 语法

```
list agents matching <REGULAR EXPRESSION>
```

## 示例

```
list agents matching (.*)
```

此命令可列出已连接到企业管理器的所有代理。

## 输出

列出每个代理，以其主机和进程为前缀。虚拟代理包含在列表中。例如：

```
jdoe-dt /Weblogic /WebLogicAgent
```

自定义度量标准主机 (虚拟) / 自定义度量标准进程 (虚拟) / 自定义度量标准代理 (虚拟)

## 列出历史代理

“列出历史代理”命令列出在 SmartStor 中包含数据的所有代理，它们已经卸载，不会向企业管理器发送数据。

## 语法

*列出历史代理*

## 示例

*列出历史代理*

## 输出

每个已卸载的历史代理位于单独行，并使用主机名和进程作为前缀。例如：

```
jdoe-dt /Weblogic /WebLogicAgent
```

## 列出历史代理（某一时间范围内）

此命令列出在指定时间范围中 SmartStor 包含历史数据的所有已卸载代理。将自动安装发送数据的代理，因此不列出这些代理。

您需要提供时段的起始和结束时间。日期-时间字符串的 hh:mm:ss 部分是可选的—如果未提供，默认为 00:00:00（午夜）。

## 语法

*list historical agents between [TIME] and [TIME]*

## 示例

```
list historical agents between \"2013-04-22 00:00:00\" and \"2013-04-23 00:10:00\"
```

此命令列出从 2013 年 3 月 22 日 00:00:00（午夜）到 2013 年 3 月 23 日 00:10:00 期间内发送数据的所有已卸载代理。

## 输出

在指定时间范围中发送数据的每个已卸载历史代理会在单独一行中列出。代理名称使用主机名和进程作为前缀。例如：

```
jdoe-dt /Weblogic /WebLogicAgent
```



## 打开代理

此命令可启动或恢复来自一个或多个代理的度量标准报告。您应提供一个用于指定目标代理的正则表达式。

## 语法

```
turn on agents matching <REGULAR EXPRESSION>
```

## 示例

```
turn on agents matching (.*)
```

此命令可打开所有代理。

## 输出

无。

## 关闭代理

此命令可从一个或多个代理停止度量标准报告。您应提供一个用于指定目标代理的正则表达式。

## 发送配置文件

此命令可将指定的文件发送给一个或多个代理。您应提供文件名称、一个用以指定目标代理的正则表达式，以及源目录和目标目录。

必须在 *introscope.agent.remoteagentconfiguration.enabled* 属性中将目标代理配置为允许远程写入。位置和其默认值因情况而异。有关详细信息，请参阅《CA APM Java 代理实施指南》或《CA APM .NET 代理实施指南》。

您只能复制在代理的

*introscope.agent.remoteagentconfiguration.allowedfiles* 属性中明确指定的文件。

此属性的默认值是 *domainconfig.xml*，该文件包含 Introscope 识别 CA CEM 事务所需的所有信息。

## APM 状态控制台命令

本节提供与 APM 状态控制台相关的 CLW 命令。

**注意：**有关使用 APM 状态控制台的信息，请参阅《CA APM Workstation 用户指南》。

您必须具有 `apm_status_console_control` 权限才能运行 APM 状态控制台 CLW 命令。

**注意：**有关该权限的信息，请参阅《CA APM 安全指南》。

该 CLW 类别包括以下命令：

[Get Cluster Configuration](#) (p. 138)

[List Active Clamps](#) (p. 139)

[List Important Events](#) (p. 142)

### Get Cluster Configuration

该命令显示以下信息：

- MOM 的主机名和端口以及群集中的所有 CDV 和收集器。
- 独立企业管理器的主机和端口。

### 语法

```
get cluster configuration
```

### 示例

```
get cluster configuration
```

该命令列出 MOM 的主机名和端口以及群集中的所有收集器。

## 输出

列出 MOM 的主机名和端口以及群集中的所有收集器。首先列出 MOM，紧接着是收集器。

```
MOM:  
USERID04-w7@5001  
  
Collectors:  
Localhost@3001  
USERID04-@xyz_company.com@6001
```

对于独立企业管理器，列出企业管理器的主机和端口。

```
StandAlone:  
USERID05-w8@5001
```

## List Active Clamps

该命令列出 `apm-events-thresholds-config.xml` 中当前达到或超过阈值的限定属性。它们称为 *活动的* 限定。该命令提供这些活动的限定的列表：

- MOM 上和跨群集中的所有收集器。
- CDV 上和连接到 CDV 的所有收集器。
- 独立企业管理器上。

`apm-events-thresholds-config.xml` 限定值达到或超过其阈值时，企业管理器会通知 APM 状态控制台。

## 语法

```
list active clamps
```

## 示例

```
list active clamps
```

该命令列出以下 CA APM 组件中所有活动的限定，具体取决于您的环境：

- MOM 和群集中的所有收集器。
- CDV 及其附加的收集器和独立企业管理器。
- 独立企业管理器。

## 输出

列出以下 CA APM 组件中所有活动的限定的名称，具体取决于您的环境：

- MOM 和整个群集中的收集器。
- CDV、连接的收集器和独立企业管理器。
- 独立企业管理器。

对于每个限定，列出以下信息：

企业管理器名称、限定名称、限定说明、限定阈值、限定值、限定的时间

例如：

```
USERID04-w7@6001, introscope.enterprisemanager.metrics.live.limit, Per EM
Limit. Takes into account only live metrics (i.e. currently reporting from
Agents), 0, 40, 22:10:00 10/07/11
USERID04-w7@3001, introscope.enterprisemanager.agent.error.limit, Limits #
of Error Events Per Interval, 1, 1, 22:09:30 10/07/11
USERID04-w7@3001, introscope.enterprisemanager.metrics.live.limit, Per EM
Limit. Takes into account only live metrics (i.e. currently reporting from
Agents), 0, 219, 22:09:30 10/07/11
```

## 命令选项

本节说明了 *list active clamps* 命令选项。

### 列出特定和多个收集器的活动的限定

您可以将以下两个参数添加到 *list active clamps* 命令：

- of EM — 使用该参数可返回特定 MOM、收集器、CDV 或独立企业管理器上的活动的限定列表。

- 语法

```
list active clamps of EM <企业管理器主机@端口>
```

- 示例

```
list active clamps of EM localhost@3001
```

- 输出

企业管理器名称、限定名称、限定说明、限定阈值、限定值、限定的时间

```
localhost@3001, introscope.enterprisemanager.agent.error.limit, Limits
# of Error Events Per Interval, 1, 1, 22:09:30 10/07/11
localhost@3001, introscope.enterprisemanager.metrics.live.limit, Per
EM limit. Takes into account only live metrics (i.e. currently reporting
from Agents), 0, 219, 22:09:30 10/07/11
```

**注意：**如果您输入的企业管理器名称不正确，控制台会显示错误消息，其中列出包含活动的限定的收集器。要获得正确企业管理器的活动的限定列表，请使用错误消息中提供的企业管理器名称重试该命令。

- of EM  
EnterpriseManagerName1@port,EnterpriseManagerName2,@port  
EnterpriseManagerNameX@port—使用该参数返回多个特定企业管理器上活动的限定的列表。

- 语法

```
list active clamps of EM <EnterpriseManagerName1@port>,
<EnterpriseManagerName2@port>
```

- 示例

```
list active clamps of EM localhost@3001,USERID04-w7@5001
```

- 输出

对于指定的所有企业管理器：企业管理器名称、限定名称、限定说明、限定阈值、限定值、限定的时间

```
localhost@3001, introscope.enterprisemanager.agent.error.limit, Limits
# of Error Events Per Interval, 1, 1, 22:09:30 10/07/11
localhost@3001, introscope.enterprisemanager.metrics.live.limit, Per
EM limit. Takes into account only live metrics (i.e. currently reporting
from Agents), 0, 219, 22:09:30 10/07/11
USERID04-w7@3001, introscope.enterprisemanager.agent.error.limit,
Limits # of Error Events Per Interval, 1, 1, 22:09:30 10/07/11
USERID04-w7@3001, introscope.enterprisemanager.metrics.live.limit, Per
EM limit. Takes into account only live metrics (i.e. currently reporting
from Agents), 0, 219, 22:09:30 10/07/11
USERID04-w7@5001, introscope.enterprisemanager.metrics.live.limit, Per
EM limit. Takes into account only live metrics (i.e. currently reporting
from Agents), 200, 390, 22:22:55 10/07/11
```

**注意：**如果您输入的企业管理器名称不正确，控制台会显示错误消息，其中列出包含活动的限定的收集器。要获得正确企业管理器的活动的限定列表，请使用错误消息中提供的企业管理器名称重试该命令。

## List Important Events

该命令列出 `apm-events-thresholds-config.xml` 中当前达到或超过阈值的重要事件属性。该命令提供群集中所有 CDV 和收集器的列表或独立企业管理器。

`apm-events-thresholds-config.xml` 属性值达到或超过其阈值时，企业管理器会通知 APM 状态控制台。

### 语法

```
list important events
```

### 示例

```
list important events
```

该命令列出群集中或独立企业管理器上的所有重要事件。

### 输出

列出有关群集中或独立企业管理器上的所有重要事件的数据。

对于每个事件，显示以下信息：

企业管理器名称、事件重要级别、事件说明、事件时间

例如：

```
USERID04-w7@6001, Warning Event, The Smartstor duration on EM  
USERID04-w7@6001 is more than configured threshold [Actual value : 1,780/  
Threshold : 5]. The most likely cause would be slow disk., 22:10:02 10/07/11  
USERID04-w7@3001, Warning Event, The harvest duration of EM USERID04-w7@3001  
is more than configured threshold [Actual value : 169/ Threshold : 5], 22:09:30  
10/07/11  
USERID04-w7@3001, Warning Event, The Smartstor duration on EM  
USERID04-w7@3001 is more than configured threshold [Actual value : 1,255/  
Threshold : 5]. The most likely cause would be slow disk., 22:09:31 10/07/11  
USERID04-w7@5001, Warning Event, The Smartstor duration on EM  
USERID04-w7@5001 is more than configured threshold [Actual value : 95/  
Threshold : 50]. The most likely cause would be slow disk., 22:32:40 10/07/11
```

## 管理模块命令

管理模块组织 Workstation 中的元素，使其更便于查找和操纵。管理模块的 CLW 命令简化了将管理模块及其包含的元素从一个企业管理器移动到另一个企业管理器的流程。

## 列出管理模块

“列出管理模块”命令列出一个或多个管理模块。您提供可指定管理模块的正则表达式。

### 语法

```
list management modules matching <REGULAR EXPRESSION>
```

### 示例

```
list management modules matching (.*)
```

此命令可列出所有管理模块。

### 输出

列出每个管理模块的名称：

样本

```
sample13
```

```
sample11
```

## 查询管理模块

“查询管理模块”命令可列出管理模块及其当前状态：“活动”或“非活动”。您应提供用于指定目标管理模块的正则表达式。

### 语法

```
query state of management modules matching <REGULAR EXPRESSION>
```

### 示例

```
query state of management modules matching (.*)
```

此命令可返回所有管理模块的名称和状态。

### 输出

列出每个管理模块的名称和状态：

```
sample1:Active
```

```
sample2:Active
```

## 激活管理模块

“激活管理模块”命令可激活一个或多个管理模块。您应提供用于指定目标管理模块的正则表达式。

**注意：**“激活管理模块”命令无法激活分类视图配置管理模块。

## 停用管理模块

“停用管理模块”命令可停用一个或多个管理模块。您应提供用于指定目标管理模块的正则表达式。

**注意：**“停用管理模块”命令无法停用分类视图配置管理模块。

## 复制管理模块

“复制管理模块”命令可在 `<EM_Home>/config/modules` 目录中创建管理模块的副本。

此命令是基于现有管理模块创建一个或多个新管理模块的一种高效方式。例如，要创建一个与现有模块相同的新管理模块（其度量标准组除外），可以使用 CLW 复制它，然后在 GUI Workstation 中修改新管理模块的度量标准组。

在“复制管理模块”命令中，您标识要复制的管理模块、新管理模块的名称以及新管理模块的 `.jar` 文件的名称（不包括文件扩展名）。

**注意：**“停用管理模块”命令无法停用分类视图配置管理模块。

## 删除管理模块

“删除管理模块”命令可删除管理模块。您应提供要删除的管理模块的精确名称。



## 将管理模块设为只读

此命令可将与指定的正则表达式匹配的管理模块设置为只读。

**警告！** CA Technologies 建议您将可编辑的管理模块的一个版本保存到安全位置，以供将来使用。管理模块设置为只读后，您无法将其返回到可编辑状态。

请执行以下步骤：

1. 设置匹配 `<regular expression>` 的只读管理模块。
2. 登录到 Workstation，打开管理模块编辑器（注意，与正则表达式匹配的管理模块旁有一个锁图标）。
3. 取消选中不再允许的管理模块旁边的“可编辑”复选框。

**注意：**此功能供 CA Technologies 合作伙伴使用。在您的环境中使用此功能之前，请联系 CA Support。

## 操作命令

操作是可由报警触发的行为，例如通知。

### 列出操作

“列出操作”命令可列出一个或多个管理模块中的一个或多个操作。您应提供两个正则表达式，分别指定操作和管理模块。

### 语法

```
list actions matching <REGULAR EXPRESSION> in management modules  
matching <REGULAR EXPRESSION>
```

### 示例

```
list actions matching (.*) in management modules matching (.*)
```

此命令可列出所有管理模块中的所有操作。

## 输出

列出每个操作，以包含它的管理模块为前缀：

*Sample.SMTP Email Action*

*Sample10.Workstation Notification*

*Sample2.Workstation Notification*

## 激活操作

“激活操作”命令可激活一个或多个管理模块中的一项或多项操作。您应提供两个正则表达式，分别指定要激活的操作和要在其中激活操作的管理模块。

## 语法

*activate actions matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>*

## 示例

*activate actions matching (SMTP.\*) in management modules matching (.\*)*

此命令可激活所有管理模块中以字符串 *SMTP* 开头的操作。

## 输出

列出该命令激活的每个操作，以包含它的管理模块为前缀，以其激活状态为后缀：

*Sample.SMTP Email Action:Active*

*Sample10.Workstation Notification:Active*

*Sample2.Workstation Notification:Active*

## 停用操作

“停用操作”命令可停用一个或多个管理模块中的一项或多项操作。您应提供两个正则表达式，分别指定要停用的操作和要在其中停用操作的管理模块。

## 查询操作

“查询操作”命令可列出一个或多个管理模块中一个或多个操作的状态—“活动”或“非活动”。您应提供两个正则表达式，分别指定操作和管理模块。

## 重命名操作

“重命名操作”命令可对操作进行重命名。您应指定操作的名称、包含该操作的管理模块，以及操作的新名称。

## 删除操作

“删除操作”命令可从一个或多个管理模块中删除一个或多个操作。您应提供两个正则表达式，分别指定操作和要从中删除操作的管理模块。

**注意：**您无法删除由其他元素使用或引用的操作—例如，链接到报警的操作。

## 报警命令

报警通过将度量标准值与用户定义的阈值进行比较来指明受管理的 Java 应用程序中的潜在问题。

## 列出报警

“列出报警”命令可列出一个或多个管理模块中的一个或多个报警。您应提供两个正则表达式，分别指定报警和管理模块。

## 语法

```
list alerts matching <REGULAR EXPRESSION> in management modules  
matching <REGULAR EXPRESSION>
```

## 示例

```
list alerts matching (.*) in management modules matching Sample
```

此命令可列出名为 *Sample* 的管理模块中的报警。

## 输出

列出每个报警，前缀为包含该报警的管理模块：

```
Sample.Console Summary Alert  
Sample.All Servlet Response Time  
Sample.All EJB Response Times
```

## 激活报警

“激活报警”命令可激活一个或多个管理模块中的一个或多个报警。您应提供两个正则表达式，分别指定要激活的报警和要在其中激活这些报警的管理模块。

## 语法

```
activate alerts matching <REGULAR EXPRESSION> in management modules  
matching <REGULAR EXPRESSION>
```

## 示例

```
activate alerts matching (.*) in management modules matching Same2
```

此命令可激活名为 *Sample2* 的管理模块中的所有报警。

## 输出

列出该命令激活的每个报警，以包含它的管理模块为前缀，以其状态为后缀：

```
Sample2.Application Summary Alert:Active  
Sample2.SQL Average Processing Time #2 (ms):Active  
Sample2.CPUApp1:Active
```

## 停用报警

“停用报警”命令可停用一个或多个管理模块中的一个或多个报警。您应提供两个正则表达式，分别指定要停用的报警和要在其中停用这些报警的管理模块。

## 查询报警

“查询报警”命令可列出一个或多个管理模块中一个或多个报警的状态（活动或非活动）。您应提供两个正则表达式，分别指定报警和管理模块。

## 重命名报警

“重命名报警”命令可对报警进行重命名。您应指定报警名称、包含该报警的管理模块以及该报警的新名称。

## 删除报警

“删除报警”命令可从一个或多个管理模块中删除一个或多个报警。您应提供两个正则表达式，分别指定报警和要从中删除这些报警的管理模块。

**注意：**无法删除由其他元素使用或引用的报警—例如，在某个显示板上使用的报警。

## 报警停机时间日程表命令

报警停机时间日程表允许您通过 Introscope Workstation 管理模块编辑器来管理停机时间。

### 列出报警停机时间日程表

“列出报警停机时间日程表”命令可列出一个或多个管理模块中的一个或多个报警停机时间日程表。您应提供两个正则表达式，分别指定报警停机时间日程表和管理模块。

#### 语法

```
list alert downtime schedules matching [REGULAR EXPRESSION] in  
management modules matching [REGULAR EXPRESSION]
```

#### 示例

```
List alert downtime schedules matching (.*) in management modules  
matching Sample
```

#### 输出

```
Sample.Example Alert Downtime Schedule  
Sample.Another Alert Downtime Schedule
```

### 激活报警停机时间日程表

“激活报警停机时间日程表”命令可激活一个或多个管理模块中的一个或多个报警停机时间日程表。您应提供两个正则表达式，分别指定要激活的报警停机时间日程表和要在其中激活这些报警停机时间日程表的管理模块。

#### 语法

```
activate alert downtime schedules matching [REGULAR EXPRESSION] in  
management modules matching [REGULAR EXPRESSION]
```

#### 示例

```
activate alert downtime schedules matching (.*) in management modules  
matching Sample
```

## 输出

*Sample.Example Alert Downtime Schedule:Active*

*Sample.Another Alert Downtime Schedule:Active*

## 停用报警停机时间日程表

“停用报警停机时间日程表”命令可停用一个或多个管理模块中的一个或多个报警停机时间日程表。您应提供两个正则表达式，分别指定要停用的报警停机时间日程表和要在其中停用这些报警停机时间日程表的管理模块。

## 查询报警停机时间日程表

“查询报警停机时间日程表”命令可列出一个或多个管理模块中一个或多个报警停机时间日程表的状态—“活动”或“非活动”。您应提供两个正则表达式，分别指定报警停机时间日程表和管理模块。

## 重命名报警停机时间日程表

“重命名报警停机时间日程表”命令可对报警停机时间日程表进行重命名。您应指定报警停机时间日程表的名称、包含它的管理模块，以及报警停机时间日程表的新名称。

## 删除报警停机时间日程表

“删除报警停机时间日程表”命令可删除一个或多个管理模块中的一个或多个报警停机时间日程表。您应提供两个正则表达式，分别指定报警停机时间日程表和要从中删除这些报警停机时间日程表的管理模块。

## 计算器命令

计算器通过对度量标准数据求和或求平均值来创建自定义度量标准。

## 列出计算器

“列出计算器”命令可列出一个或多个管理模块中的一个或多个计算器。您应提供两个正则表达式，分别指定计算器和管理模块。

## 语法

```
list calculators matching <REGULAR EXPRESSION> in management modules  
matching <REGULAR EXPRESSION>
```

## 示例

```
list calculators matching (.*) in management modules matching (.*)
```

此命令列出所有管理模块中的所有计算器。

## 输出

列出每个计算器，前缀为包含该计算器的管理模块：

```
Sample.Average Servlet Response Time
```

## 激活计算器

“激活计算器”命令可激活一个或多个管理模块中的一个或多个计算器。您应提供两个正则表达式，分别指定要激活的计算器 and 要在其中激活这些计算器的管理模块。

## 语法

```
activate calculators matching <REGULAR EXPRESSION> in management  
modules matching <REGULAR EXPRESSION>
```

## 示例

```
activate calculators matching (.*) in management modules matching  
Sample2
```

此命令可激活名为 *Sample2* 的管理模块中的所有计算器。

## 输出

列出该命令激活的每个计算器，前缀为包含该计算器的管理模块，后缀为其状态：

```
Sample2.Average Servlet Response Time:Active
```

## 停用计算器

“停用计算器”命令可停用一个或多个管理模块中的一个或多个计算器。您应提供两个正则表达式，分别指定要停用的计算器和要在其中停用这些计算器的管理模块。

## 查询计算器

“查询计算器”命令可列出一个或多个管理模块中一个或多个计算器的状态（活动或非活动）。您应提供两个正则表达式，分别指定计算器和管理模块。

## 重命名计算器

“重命名计算器”命令可对计算器进行重命名。您应指定计算器名称、包含该计算器的管理模块以及该计算器的新名称。

## 删除计算器

“删除计算器”命令可从一个或多个管理模块中删除一个或多个计算器。您应提供两个正则表达式，分别指定计算器和要从中删除这些计算器的管理模块。

**注意：**您无法删除由其他元素使用或引用的计算器—例如，在显示板上使用的计算器。

## 显示板命令

显示板是工作站中的页面，包含数据查看器对象（如图表、条形图和报警状态指示器）以及图形对象和文本对象。

## 列出显示板

“列出显示板”命令可列出一个或多个管理模块中的一个或多个显示板。您应提供两个正则表达式，分别指定显示板和管理模块。

## 语法

```
list dashboards matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>
```

## 示例

```
list dashboards matching (. *Triage) in management modules matching (. *)
```

此命令可列出所有管理模块中名字以字符串 *Triage* 结尾的显示板。



## 输出

列出每个显示板，前缀为包含该显示板的管理模块：

*Sample10.3. Triage*

*Sample2.3. Triage*

*Sample.3. Triage*

## 激活显示板

“激活显示板”命令可激活一个或多个管理模块中的一个或多个显示板。您应提供两个正则表达式，分别指定要激活的显示板和要在其中激活这些显示板的管理模块。

## 语法

```
activate dashboards matching <REGULAR EXPRESSION> in management  
modules matching <REGULAR EXPRESSION>
```

## 示例

```
activate dashboards matching (.*) in management modules matching  
Sample2
```

此命令可激活名为 *Sample2* 的管理模块中的所有显示板。

## 输出

列出该命令激活的每个显示板，前缀为包含该显示板的管理模块，后缀为其状态：

*Sample2.4b. Database Detail:Active*

*Sample2.1. Introscope Console:Active*

*Sample2.2. Detection:Active*

## 停用显示板

“停用显示板”命令可停用一个或多个管理模块中的一个或多个显示板。您应提供两个正则表达式，分别指定要停用的显示板和要在其中停用这些显示板的管理模块。

## 查询显示板

“查询显示板”命令可列出一个或多个管理模块中一个或多个显示板的状态（活动或非活动）。您应提供两个正则表达式，分别指定显示板和管理模块。

## 重命名显示板

“重命名显示板”命令可对显示板进行重命名。应指定显示板的名称、包含它的管理模块，以及显示板的新名称。

## 删除显示板

“删除显示板”命令可从一个或多个管理模块中删除一个或多个显示板。您应提供两个正则表达式，分别指定显示板和要从中删除这些显示板的管理模块。

**注意：**您无法删除由其他元素使用或引用的显示板。例如，您无法删除其上包含的超链接指向其他显示板上的数据查看器的显示板。

## 度量标准和度量标准组命令

度量标准组命令指定要对哪些度量标准执行操作；它用作元素（例如报警和计算器）的构建块。

### 列出度量标准组

“列出度量标准组”命令可列出一个或多个管理模块中的一个或多个度量标准组。您应提供两个正则表达式，分别指定度量标准组和管理模块。

### 语法

```
list metric groups matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>
```

### 示例

```
list metric groups matching (. *Response. *) in management modules matching Sample
```

此命令可列出名为 *Sample* 的管理模块中名称中包含字符串 *Response* 的度量标准组。

## 输出

度量标准组按以下格式列出：

```
<Management Module>.<Metric Group>[Agent: "<Agent Expression>"  
Attribute: "<Metric Expression>"]
```

例如：

```
Sample.Servlet Average Response Time (ms) [Agent: "(.*) \/(.*) \/(.*)"  
Attribute: "\"Servlets:Average Response Time \\\(ms\\)\""]
```

以上示例提供了度量标准组的以下信息：

管理模块—*Sample*

度量标准组名称—*Servlet 平均响应时间(毫秒)*

代理表达式—*(.\*) \/(.\*) \/(.\*)*

度量标准表达式—*Servlets:平均响应时间\\(毫秒)*

## 打开精确度量标准

此命令要求代理打开特定度量标准。

## 语法

```
turn on exact metric <度量标准名称>
```

## 示例

```
turn on exact metric  
jdoe-dt /Weblogic /WebLogicAgent /Servlets /Servlet21 /Servlet21_1u2oj1_Im  
pl:Average Response Time (ms)
```

代理打开

“jdoe-dt | Weblogic | WebLogicAgent | Servlets | Servlet21 | Servlet21\_1u2oj1  
\_Impl:Average Response Time (ms)” 度量标准，开始发送数据。

## 输出

无

## 关闭精确度量标准

此命令要求代理关闭特定度量标准。

### 语法

```
turn off exact metric <度量标准名称>
```

### 示例

```
turn off exact metric  
jdoe-dt /Weblogic /WebLogicAgent /Servlets /Servlet21 /Servlet21_1u2oj1_Im  
pl:Average Response Time (ms)
```

代理关闭

“jdoe-dt | Weblogic | WebLogicAgent | Servlets | Servlet21 | Servlet21\_1u2oj1\_Impl:Average Response Time (ms)” 度量标准，停止发送数据。

### 输出

无

## 报告模板命令

本节定义了用于管理和生成报告的 CLW 命令。有关 Introscope 的报告功能的详细信息，请参阅《CA APM Workstation 用户指南》中的“报告”一章。

### 列出报告模板

“列出报告模板”命令可列出一个或多个管理模块中的一个或多个报告模板。您应提供两个正则表达式，分别指定报告模板和管理模块。

### 语法

```
list report templates matching <REGULAR EXPRESSION> in management  
modules matching <REGULAR EXPRESSION>
```

### 示例

```
list report templates matching (.*) in management modules matching  
Sample
```

此命令可列出名为 *Sample* 的管理模块中的所有报告模板。

## 输出

每个报告模板的前缀均为包含该报告模板的管理模块。

```
Sample.QA/Test Application Performance
Sample.System Availability
Sample.Application Capacity Planning
```

## 激活报告模板

“激活报告模板”命令可激活一个或多个管理模板中的一个或多个报告模板。您应提供两个正则表达式，分别指定要激活的报告模板和要在其中激活报告模板的管理模块。

## 语法

```
activate report templates matching <REGULAR EXPRESSION> in
management modules matching <REGULAR EXPRESSION>
```

## 示例

```
activate report templates matching (.*) in management modules matching
Sample2
```

此命令可激活名为 Sample2 的管理模块中的所有报告模板。

## 输出

列出该命令激活的每个报告模板，前缀为包含该报告模板的管理模块，后缀为其状态：

```
Sample2.Application Capacity Planning:Active
```

```
Sample2.Production Application Health:Active
```

```
Sample2.System Availability:Active
```

## 停用报告模板

“停用报告模板”命令可停用一个或多个管理模板中的一个或多个报告模板。您应提供两个正则表达式，分别指定要停用的报告模板和要在其中停用这些报告模板的管理模块。

## 查询报告模板

“查询报告模板”命令可列出一个或多个管理模块中一个或多个报告模板的状态—“活动”或“非活动”。您应提供两个正则表达式，分别指定报告模板和管理模块。

## 重命名报告模板

“重命名报告模板”命令可对报告模板进行重命名。您应指定报告模板的名称、包含它的管理模块，以及报告模板的新名称。

## 删除报告模板

“删除报告模板”命令可从一个或多个管理模块中删除一个或多个报告模板。您应提供两个正则表达式，分别指定报告模板和要从中删除这些报告模板的管理模块。

## 生成报告

使用“生成报告”命令可生成报告。您提供以下参数：

- 报告名称
- 开始时间
- 结束时间
- 管理模块名称
- 文件名—此文件将写入到当前工作目录中，除非指定了路径。该文件必须是以与下列文件扩展名之一关联的格式编写的：HTML、PDF、XLS、TEXT、XM 或 CSV。

## 命令

有三种“生成报告”命令：基本命令、扩展命令和代理覆盖命令：

*基本命令：*

*generate report named [EXACT MATCH] in management module named [EXACT MATCH] to [EXACT MATCH]*

*扩展命令：*

*generate report named [EXACT MATCH] in management module named [EXACT MATCH] starting at [EXACT MATCH] ending at [EXACT MATCH] to [EXACT MATCH]*

## 可选参数

可以为上面的基本命令和扩展命令使用可选参数：

```
{in agents matching [REGEX PATTERN]} {starting at [EXACT MATCH] ending at [EXACT MATCH]}
```

可选参数的语法为：

```
generate report named [EXACT MATCH] in management module named [EXACT MATCH] {in agents matching [REGEX PATTERN]} {starting at [EXACT MATCH] ending at [EXACT MATCH]} to [EXACT MATCH]
```

## 报告时间戳格式

报告时间戳有各种格式。下表标识了各种可能的格式。

时间戳格式：	示例
<i>M/d/yy h:mm a</i>	11/17/08 3:00 PM
<i>M/d/yy h:mm:ss a</i>	11/17/08 3:00:06 PM
<i>M/d/yy h:mm:ss a z</i>	11/17/08 3:00:06 PM PST
<i>M/d/yy</i>	11/17/08
<i>MMM d, yyyy h:mm a</i>	Nov 17, 2008 3:00 PM
<i>MMM d, yyyy h:mm:ss a</i>	Nov 17, 2008 3:00:06 PM
<i>MMM d, yyyy h:mm:ss a z</i>	Nov 17, 2008 3:00:06 PM PST
<i>MMM d, yyyy</i>	Nov 17, 2008
<i>MMMM d, yyyy h:mm a</i>	November 17, 2008 3:00 PM
<i>MMMM d, yyyy h:mm:ss a</i>	November 17, 2008 3:00:06 PM
<i>MMMM d, yyyy h:mm:ss a z</i>	November 17, 2008 3:00:06 PM PST
<i>MMMM d, yyyy</i>	November 17, 2008
<i>EEE MMM dd HH:mm:ss zzz yyyy</i>	Mon Nov 17 15:00:06 PST 2008
<i>MM/dd/yy HH:mm:ss</i>	11/17/08 15:00:06
<i>yyyy-MM-dd HH:mm:ss</i>	2008-11-17 15:00:06
<i>yyyy-MM-dd HH:mm:ss.SSSS</i>	2008-11-17 15:00:06.0840
<i>yyyy-MM-dd HH:mm</i>	2008-11-17 15:00
<i>yyyy-MM-dd hh:mm:ss a</i>	2008-11-17 03:00:06 PM
<i>yyyy-MM-dd hh:mm a</i>	2008-11-17 03:00 PM
<i>yyyy/MM/dd hh:mm:ss a</i>	2008/11/17 03:00:06 PM

<code>yyyy/MM/dd hh:mm a</code>	2008/11/17 03:00 PM
<code>yyyy/MM/dd HH:mm:ss</code>	2008/11/17 15:00:06
<code>yyyy/MM/dd HH:mm</code>	2008/11/17 15:00

## SNMP 收集命令

这些命令用于定义要将哪些已收集的度量标准包含在发布的 MIB 中。

### 列出 SNMP 收集

“列出 SNMP 收集”命令可列出一个或多个管理模块中的一个或多个 SNMP 收集。您应提供两个正则表达式，分别指定 SNMP 收集和管理模块。

#### 语法

```
list snmp collections matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>
```

#### 示例

```
list snmp collections matching (.*) in management modules matching (.*)
```

此命令可列出所有管理模块中的所有 SNMP 收集。

#### 输出

每个 SNMP 收集的前缀均为包含该收集的管理模块。例如：

```
Sample2.JDBC QueryUpdate
```

### 激活 SNMP 收集

“激活 SNMP 收集”命令可激活一个或多个管理模块中的一个或多个 SNMP 收集。您应提供两个正则表达式，分别指定要激活的 SNMP 收集和要在其中激活 SNMP 收集的管理模块。

#### 语法

```
activate snmp collections matching <REGULAR EXPRESSION> in management modules matching <REGULAR EXPRESSION>
```



## 示例

```
activate snmp collections matching (.*) in management modules matching  
Sample2
```

此命令可激活名为 *Sample2* 的管理模块中的所有 SNMP 收集。

## 输出

列出该命令激活的每个 SNMP 收集，前缀为包含该收集的管理模块，后缀为其状态。

```
Sample2.JDBC QueryUpdate:Active
```

## 停用 SNMP 收集

“停用 SNMP 收集”命令可停用一个或多个管理模块中的一个或多个 SNMP 收集。您应提供两个正则表达式，分别指定要停用的 SNMP 收集和要在其中停用这些 SNMP 收集的管理模块。

## 查询 SNMP 收集

“查询 SNMP 收集”命令可列出一个或多个管理模块中一个或多个 SNMP 收集的状态—“活动”或“非活动”。您应提供两个正则表达式，分别指定 SNMP 收集和管理模块。

## 重命名 SNMP 收集

“重命名 SNMP 收集”命令可对 SNMP 收集进行重命名。您应指定 SNMP 收集的名称、包含它的管理模块，以及 SNMP 收集的新名称。

## 删除 SNMP 收集

“删除 SNMP 收集”命令可从一个或多个管理模块中删除一个或多个 SNMP 收集。您应提供两个正则表达式，分别指定 SNMP 收集和要从中删除这些 SNMP 收集的管理模块。

## 配置事务跟踪选项

CLW 允许您使用以下系统属性来配置各种事务跟踪选项：

- `-Dintroscope.clw.tt.console` —如果设置为“true”，事务跟踪将输出到控制台。
- `-Dintroscope.clw.tt.dirname` —存储事务跟踪 XML 文件的本地目录。
- `-Dintroscope.clw.tt.filename` —用于存储事务跟踪的文件名。它不能包括目录名称。
- `-Dintroscope.clw.tt.encoding` —将 XML 文件写入到磁盘时所使用的编码。此属性的设置包括默认选项 *ISO-8859-1*，以及 *UTF-8*、*UTF-16* 和 *Windows-1252*

## 启动事务跟踪会话

各个事务流经单个 JVM 的边界时，事务跟踪器将跟踪它们的活动。

事务跟踪将自动保存到事务事件数据库中，默认情况下，还会将它们捕获到一个或多个 XML 文件中（您可以在 CA Introscope Workstation 的事务跟踪查看器中打开和分析这些文件）。有关 CA Introscope 事务跟踪器的信息，请参阅《*CA APM Workstation 用户指南*》。

## 命令语法

CLW 命令可以指定事务跟踪会话的许多方面。其中包括：

- 执行阈值 —要跟踪的事务的最短执行时间。对执行时间超过阈值的事务进行跟踪。阈值可以以秒为单位进行指定。
- 要跟踪的代理 —一个 Perl 正则表达式，用于指定要跟踪其事务的代理。
- 会话持续时间 —事务跟踪会话的持续时间（以秒为单位）。

下面是启动事务跟踪会话的语法（以秒为单位指定阈值）：

```
trace transactions exceeding <EXACT MATCH>  
(second/seconds/sec/secs/s) in agents matching <REGULAR  
EXPRESSION> for <EXACT MATCH> <second/seconds/sec/secs/s>
```

[下文中的命令选项](#) (p. 163)详细介绍了其他 CLW 命令选项。有关事务跟踪 CLW 命令的示例，请参阅[事务跟踪命令示例](#) (p. 164)。

## 指定事务跟踪输出文件

您可以指定事务跟踪输出文件的名称。

## 语法

```
Dintroscope.clw.tt.filename=<file name>
```

## 示例

指定事务跟踪输出文件的文件名（但不是完整路径）。与用来指定输出目录的一个属性配合使用。

## 输出

将事务跟踪输出发送到指定文件。

## 命令选项

本节介绍了事务跟踪命令选项。

## 跟踪模式

CLW 支持两种用于捕获事务跟踪会话结果的模式：

- 同步模式—默认情况下，CLW 在会话结束时将跟踪写入到事务事件数据库以及名为 *TransactionTraceData-yyyyMMddhhmmss.xml* 的单个 xml 文件，其中日期-时间字符串反映该会话的开始时间。
- 异步模式—在此模式下，将每个事务报告到事务事件数据库时，CLW 就立即将该事务跟踪写入到其自己的名为 *nnnn(sec)-TransactionTraceDatayyyyMMddhhmmss-<sequence number>.xml* 的 XML 文件中，其中 *nnnn* 是以秒为单位的事务持续时间，日期-时间字符串反映事务的开始时间。如果您提供自己的文件名，它会在最后的“.”之前添加一个序号。如果所提供的文件名不含“.”，它会在文件名末尾添加一个序号。

以同步模式记录的结果更容易查看—所有数据都在单个文件中。但是，必须等到会话结束后您才能查看数据，对于大容量或复杂的事务，同步捕获可能会消耗大量内存。

以异步模式记录事务数据占用较少内存，并且您在事务跟踪会话结束之前就可以查看事务数据。

```
-Dintroscope.clw.tt.mode=(Synch /Asynch)
```

## 仅输出到事务事件数据库

使用此选项运行事务跟踪并将输出仅保存到事务事件数据库（非 xml 文件输出）。可以通过某个 **Introscope** 报警触发此命令，该报警被触发后将触发该命令以自动启动跟踪事务。

如下所示，在命令前添加单词 *quietly*：

```
quietly trace transactions exceeding 2 seconds in agents matching "(.*)"
```

 for 60 seconds

## 仅返回标头数据

在某些情况下，通过 CLW 检索大量事务追踪数据时，*traces.db* 文件可能会无限增长，导致 CLW 花费很长时间才能返回数据。将此属性设为 **false**，可以减少企业管理器返回的数据量，从而解决上述问题。

CLW 将只返回标头跟踪数据。默认情况下，或在此属性设置为 **true** 时，通过 CLW 获取事务跟踪数据将同时返回标头和正文。

```
-Dwily.ps.workstation.clws.gettracebody
```

## 事务跟踪器限定

默认情况下，单个事务跟踪达到 5000 个跟踪组件时，会限制其大小。超出限制的事务跟踪将被丢弃在代理上，并在代理日志文件中记录如下警告消息：

```
2/23/07 05:33:18 PM PST [WARN] [IntroscopeAgent] Transaction trace component limit of 5000 reached, recording will cease for this transaction.
```

要更改一个事务跟踪中允许的最大组件数，请更改以下代理属性：

```
introscope.agent.transactiontrace.componentCountClamp=max_TT_components
```

（默认值是 5000）

例如，代理配置文件中的以下行：

```
introscope.agent.transactiontrace.componentCountClamp=30000
```

将事务跟踪中允许的最大组件数更改为 30,000。

**警告！**：如果增大此限制大小，事务跟踪可能会需要更多的内存，因此您有必要相应调整 JVM 的最大堆大小，否则企业管理器可能会内存不足。

## 事务跟踪命令示例

本节提供了启动事务跟踪会话的 CLW 命令示例。每个示例命令启动一个 600 秒长的会话。来自所有代理的超过 5 秒的事务将被跟踪。

**注意：**所有示例命令都使用默认登录设置连接到企业管理器。

有关用来运行事务跟踪会话的脚本示例，请参阅[示例脚本](#) (p. 177)。

## 使用默认选项值的事务跟踪

此 CLW 命令使用以下默认设置启动事务跟踪会话：

- 跟踪模式—同步捕获事务跟踪数据—所有结果都写入到单个 xml 文件中。
- 目录位置—未指定 `-Dintroscope.clw.tt.dirname` 时，跟踪结果将写入到当前工作目录中。

```
java -jar CLWorkstation.jar trace transactions exceeding 5 seconds in agents
matching "(.*)" for 600 seconds
```

## 使用异步捕获执行事务跟踪

此 CLW 命令启动事务跟踪会话并为会话输出使用默认目录位置：

```
java -Dintroscope.clw.tt.mode=Asynch -jar CLWorkstation.jar trace transactions
exceeding 5 seconds in agents matching "(.*)" for 600 seconds
```

数据以异步模式捕获—为每个事务创建单独的 xml 文件。

## 将事务跟踪结果写入用户定义的目录中

此 CLW 命令使用跟踪模式的默认设置启动事务跟踪会话—以同步模式捕获事务跟踪数据。所有结果都写入到单个 xml 文件中：

```
java -Dintroscope.clw.tt.dirname=C:\mytraces -jar CLWorkstation.jar trace
transactions exceeding 5 seconds in agents matching "(.*)" for 600 seconds
```

此命令为 xml 文件指定非默认位置—`C:\mytraces` 目录。

## 使用参数和错误筛选器的事务跟踪

您可以启动指定了运行秒数并使用与工作站中可用的筛选器相同的筛选器（用户 ID、URL、URL 查询、会话 ID、请求标头、请求参数、会话属性以及错误）的事务跟踪会话：

### 对用户 ID、URL、URL 查询或会话 ID 进行筛选

```
trace transactions where (userid|url|url query|sessionid) (equals|not
equals|contains|not contains|starts with|ends with) [EXACT MATCH] in agents
matching [REGULAR EXPRESSION] for [EXACT MATCH] (second|seconds|sec|secs|s)
trace transactions where (userid|url|url query|sessionid) (exists|not exists) in
agents matching [REGULAR EXPRESSION] for [EXACT MATCH]
(second|seconds|sec|secs|s)
quietly trace transactions where (userid|url|url query|sessionid) (equals|not
equals|contains|not contains|starts with|ends with) [EXACT MATCH] in agents
matching [REGULAR EXPRESSION] for [EXACT MATCH] (second|seconds|sec|secs|s)
quietly trace transactions where (userid|url|url query|sessionid) (exists|not
exists) in agents matching [REGULAR EXPRESSION] for [EXACT MATCH]
(second|seconds|sec|secs|s)
```

**对请求标头、请求参数或会话属性进行筛选**

```
trace transactions where (request header|request parameter|session attribute)
[EXACT MATCH] (equals|not equals|contains|not contains|starts with|ends with)
[EXACT MATCH] in agents matching [REGULAR EXPRESSION] for [EXACT MATCH]
(second|seconds|sec|secs|s)
```

```
trace transactions where (request header|request parameter|session attribute)
[EXACT MATCH] (exists|not exists) in agents matching [REGULAR EXPRESSION] for
[EXACT MATCH] (second|seconds|sec|secs|s)
```

```
quietly trace transactions where (request header|request parameter|session
attribute) [EXACT MATCH] (equals|not equals|contains|not contains|starts
with|ends with) [EXACT MATCH] in agents matching [REGULAR EXPRESSION] for [EXACT
MATCH] (second|seconds|sec|secs|s)
```

```
quietly trace transactions where (request header|request parameter|session
attribute) [EXACT MATCH] (exists|not exists) in agents matching [REGULAR
EXPRESSION] for [EXACT MATCH] (second|seconds|sec|secs|s)
```

**对错误进行筛选**

```
trace transactions with errors containing [EXACT MATCH] in agents matching [REGEX]
for [EXACT MATCH] (second|seconds|sec|secs|s)
```

```
quietly trace transactions with errors containing [EXACT MATCH] in agents matching
[REGEX] for [EXACT MATCH] (second|seconds|sec|secs|s)
```

**对事务事件数据库执行的事务跟踪查询**

事务跟踪结果自动存储在事务事件数据库中。可使用此处描述的 CLW 命令来检索该数据。

**Get Historical Events Matching <VALUE>**

此命令从事务事件数据库检索完整的事件 XML 输出文件。完整事件（与下文描述的摘要事件相对）是在事务事件查看器中靠下的部分中提供的完整数据。

```
java -Dintroscope.clw.tt.mode=Asynch -jar CLWorkstation.jar trace transactions
get historical events matching "localhost"
```

下面是一个输出示例：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TransactionTracerSession Duration="78" Version="0.1"
EndDate="2005-06-20T17:40:24.146-08:00"
StartDate="2005-06-20T17:40:24.068-08:00" User="Admin">
<TransactionTrace Domain="SuperDomain" Duration="78" Process="UnknownProcess"
Host="maddlemann-dt2" AgentName="Tomcat"
StartDate="2005-06-20T17:40:24.068-08:00"
EndDate="2005-06-20T17:40:24.146-08:00">
<CalledComponent RelativeTimestamp="0" Duration="78" ComponentType="Browser"
ComponentName="Browser" MetricPath="Browser">
<CalledComponents>
```

```
<CalledComponent RelativeTimestamp="0" Duration="0" ComponentType="JNDI"
ComponentName="ProxyDirContext" MetricPath="JNDI|Context|ProxyDirContext">
<Parameters>
<Parameter Value="lookup" Name="Method"/>
</Parameters>
</CalledComponent>
<CalledComponent RelativeTimestamp="0" Duration="0" ComponentType="JNDI"
ComponentName="ProxyDirContext" MetricPath="JNDI|Context|ProxyDirContext">
<Parameters>
<Parameter Value="lookup" Name="Method"/>
</Parameters>
</CalledComponent>
<CalledComponent RelativeTimestamp="0" Duration="62" ComponentType="Servlets"
ComponentName="HelloWorldExample" MetricPath="Servlets|HelloWorldExample">
<CalledComponents>
<CalledComponent RelativeTimestamp="0" Duration="0" ComponentType="JNDI"
ComponentName="ProxyDirContext" MetricPath="JNDI|Context|ProxyDirContext">
<Parameters>
<Parameter Value="lookup" Name="Method"/>
</Parameters>
</CalledComponent>
<CalledComponent RelativeTimestamp="0" Duration="0" ComponentType="JNDI"
ComponentName="ProxyDirContext" MetricPath="JNDI|Context|ProxyDirContext">
<Parameters>
<Parameter Value="lookup" Name="Method"/>
</Parameters>
</CalledComponent>
</CalledComponents>
</TransactionTrace>
</TransactionTracerSession>
```

## Get summaries matching <VALUE>

此命令从事务事件数据库仅检索事件摘要 XML 并输出一个 xml 文件。事件摘要是在事务事件查看器的顶部窗格中提供的信息。此命令可以用来导出事务事件数据库中的数据以便生成有关系统发生的错误数（例如每天发生的错误数）的报告。

```
get historical event summaries matching [REGULAR EXPRESSION]
```

下面是一个输出示例：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TransactionTracerSession Duration="78" Version="0.1"
EndDate="2005-06-20T17:40:24.146-08:00"
StartDate="2005-06-20T17:40:24.068-08:00" User="Admin">
<TransactionTrace Domain="SuperDomain" Duration="78" Process="UnknownProcess"
Host="maddlemann-dt2" AgentName="Tomcat"
StartDate="2005-06-20T17:40:24.068-08:00"
EndDate="2005-06-20T17:40:24.146-08:00">
<CalledComponent RelativeTimestamp="0" Duration="78" ComponentType="Browser"
ComponentName="Browser" MetricPath="Browser">
<Parameters>
<Parameter Value="" Name="URL"/>
<Parameter Value="Normal" Name="Trace Type"/>
<Parameter Value="\20050620\17\1119314425302" Name="Trace ID"/>
<Parameter Value="" Name="User ID"/>
</Parameters>
</CalledComponent>
</TransactionTrace>
</TransactionTracerSession>
```

## 应用程序分类视图命令

分类视图报警是与 AppMap 和 AppMap 实体关联的专用报警。分类视图报警位于 *TriageMapConfigurationsManagementModule.jar* 文件的分类视图配置管理模块中。

以下命令可供该管理模块使用：

[列出管理模块](#) (p. 168)

[查询管理模块的状态](#) (p. 169)

[列出分类视图报警](#) (p. 169)

[查询管理模块的状态](#) (p. 171)

[列出分类视图实体度量标准组](#) (p. 172)

[查询分类视图实体度量标准组的状态](#) (p. 173)

### 列出管理模块

此命令用于列出分类视图管理模块的名称。



## 语法

```
list management modules matching <REGULAR EXPRESSION>
```

## 示例

```
list management modules matching (Triage Map.*)
```

此命令将列出名称以 *Triage Map* 开头的管理模块。

## 输出

列出每个管理模块的名称和状态。在此示例中，分类视图配置管理模块会匹配正则表达式，并按如下方式列出：

```
Triage Map Configurations
```

## 查询管理模块的状态

此命令用于列出分类视图管理模块的状态。

## 语法

```
query state of management modules matching [REGULAR EXPRESSION]
```

## 示例

```
query state of management modules matching (.*)
```

此命令可返回所有管理模块的名称和状态。

## 输出

列出为您的系统配置的每个管理模块的名称和状态。例如：

```
Supportability:Active  
Trade Application Definitions:Active  
Triage Map Configurations:Active  
Browser Response Time Adapter:Active  
Sample:Active  
MOM Infrastructure Monitoring:Active  
Reports Unit Tests:Active  
Collector - 1:Active  
ChangeDetector:Active  
CEM BT Stats:Active
```

## 列出分类视图报警

此命令用于列出分类视图报警。

## 语法

*list triage map alerts matching [REGULAR EXPRESSION] in management modules matching [REGULAR EXPRESSION]*

## 示例

*list triage map alerts matching (.\*) in management modules matching (Triage Map .\*)*

此命令将尝试列出名称以 *Triage Map* 开头的管理模块中的所有分类视图报警。

## 输出

列出为您的系统配置的所有分类视图报警的名称。例如：

```

Triage Map Configurations.By Frontend/TradeService/Health:Average Response
Time (ms)_Summary_MetricAlert
Triage Map Configurations.By Business
Service/MedRecBS/loginAdmin.action/loginAdmin.action:Errors Per
Interval_Summary_MetricAlert
Triage Map Configurations.By Frontend/ReportingService/Backend
Calls/webServices:Average Response Time (ms)_Location_MetricAlert
Triage Map Configurations.By Business
Service/MedRecBS/viewNewlyRegisteredPatients.action/viewNewlyRegisteredPat
ients.action:Average Response Time (ms)_Location_MetricAlert
Triage Map Configurations.By Frontend/PatientFacadeServiceWebApp/Backend
Calls//localhost%9082/medrec(POINTBASE DB):Alert
Triage Map Configurations.By Frontend/ReportingEngine/Backend
Calls/jdbc%hsqldb%file%report-records:Stall Count_Summary_MetricAlert
Triage Map Configurations.By Business
Service/MedRecBS/viewNewlyRegisteredPatients.action/viewNewlyRegisteredPat
ients.action:Stall Count_Location_MetricAlert
Triage Map Configurations.Business Service/MedRecBS/Business
Transactions/home.action:Alert
Triage Map Configurations.By Frontend//medrec/Health:Errors Per
Interval_Location_MetricAlert
Triage Map Configurations.Business Service/Trading Service/Business
Transactions/View Orders:Total Defects Per Interval_Summary_MetricAlert
Triage Map Configurations.By Frontend/AuthenticationService/Health:Errors
Per Interval_Summary_MetricAlert
Triage Map Configurations.By Business Service/Trading Service/Options
Trading/Check Options:Concurrent Invocations_Summary_MetricAlert
Triage Map Configurations.By Business
Service/MedRecBS/index.action/index.action:Stall
Count_Location_MetricAlert
Triage Map Configurations.By Business
Service/MedRecBS/index.action/index.action:Concurrent
Invocations_Summary_MetricAlert
Triage Map Configurations.Business Service/MedRecBS/Business
Transactions/viewPatients.action:Total Defects Per
Interval_Summary_MetricAlert
Triage Map Configurations.By Business
Service/MedRecBS/index.action/index.action:Average Response Time
(ms)_Summary_MetricAlert

```

## 查询管理模块的状态

此命令用于列出分类视图报警的状态。

## 语法

```

query state of triage map alerts matching [REGULAR EXPRESSION] in
management modules matching [REGULAR EXPRESSION]

```

## 示例

```
query state of triage map alerts matching (.*) in management modules
matching (Triage Map .*)
```

此命令将列出名称以 *Triage Map* 开头的管理模块中的所有分类视图报警及其状态。

## 输出

列出为您的系统配置的所有分类视图报警的名称及其状态。例如：

```
Triage Map Configurations.By Frontend|TradeService|Health:Average Response
Time (ms)_Summary_MetricAlert:Active
Triage Map Configurations.By Business
Service|MedRecBS|loginAdmin.action|loginAdmin.action:Errors Per
Interval_Summary_MetricAlert:Active
Triage Map Configurations.By Frontend|ReportingService|Backend
Calls|WebServices:Average Response Time (ms)_Location_MetricAlert:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewNewlyRegisteredPatients.action|viewNewlyRegisteredPat
ients.action:Average Response Time (ms)_Location_MetricAlert:Active
Triage Map Configurations.By Frontend|PatientFacadeServiceWebApp|Backend
Calls|//localhost%9082/medrec(POINTBASE DB):Alert:Active
Triage Map Configurations.By Frontend|ReportingEngine|Backend
Calls|jdbc%hsqldb%file%report-records:Stall
Count_Summary_MetricAlert:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewNewlyRegisteredPatients.action|viewNewlyRegisteredPat
ients.action:Stall Count_Location_MetricAlert:Active
Triage Map Configurations.Business Service|MedRecBS|Business
Transactions|home.action:Alert:Active
Triage Map Configurations.By Frontend|/medrec|Health:Errors Per
Interval_Location_MetricAlert:Active
Triage Map Configurations.Business Service|Trading Service|Business
Transactions|View Orders:Total Defects Per
Interval_Summary_MetricAlert:Active
Triage Map Configurations.By Frontend|AuthenticationService|Health:Errors
Per Interval_Summary_MetricAlert:Active
Triage Map Configurations.By Business Service|Trading Service|Options
Trading|Check Options:Concurrent Invocations_Summary_MetricAlert:Active
Triage Map Configurations.By Business
Service|MedRecBS|index.action|index.action:Stall
Count_Location_MetricAlert:Active
```

## 列出分类视图实体度量标准组

此命令用于列出分类视图实体度量标准组的名称。

## 语法

```
list triage map entity metric groups matching [REGULAR EXPRESSION] in
management modules matching [REGULAR EXPRESSION]
```

## 示例

```
list triage map entity metric groups matching (.*) in management modules
matching (Triage Map .*)
```

此命令将列出管理模块中名称以 *Triage Map* 开头的所有分类视图实体组。

## 输出

列出为您的系统配置的所有分类视图实体组的名称和状态。例如：

```
Triage Map Configurations.By Frontend|/medrec|Health:Average Response Time
(ms)_Summary
Triage Map Configurations.By Frontend|AuthenticationEngine|Health:Average
Response Time (ms)_Summary
Triage Map Configurations.Business Service|MedRecBS|Business
Transactions|index.action:Total Defects Per Interval_Summary
Triage Map Configurations.By Business Service|Trading Service|View
Orders|View my order:Concurrent Invocations_Location
Triage Map Configurations.By
Frontend|PatientFacadeServiceWebApp|Health:Errors Per Interval_Summary
Triage Map Configurations.By Business Service|Trading Service|Transaction
Summary|Request Transaction Summary:Average Response Time (ms)_Summary
Triage Map Configurations.By Frontend|ReportingEngine|Health:Errors Per
Interval_Summary
Triage Map Configurations.By Business Service|Trading Service|Options
Trading|Check Options:Errors Per Interval_Summary
Triage Map Configurations.By Frontend|AuthenticationEngine|Backend
Calls|jdbc%hsqldb%file%customer-records:Average Response Time (ms)_Summary
Triage Map Configurations.By Frontend|OrderEngine|Health:Average Response
Time (ms)_Location
Triage Map Configurations.Business Service|MedRecBS|Business
Transactions|viewPatients.action:Total Transactions Per Interval_Summary
Triage Map Configurations.By Business Service|Trading Service|Options
Trading|Check Options:Stall Count_Summary
```

## 查询分类视图实体度量标准组的状态

此命令用于列出分类视图实体度量标准组的状态。

## 语法

*query state of triage map entities matching [REGULAR EXPRESSION] in management modules matching [REGULAR EXPRESSION]*

## 示例

`query state of triage map entities matching (.*) in management modules matching (Triage Map .*)`

此命令将尝试列出管理模块中名称以 *Triage Map* 开头的**所有**分类视图实体及其状态。

## 输出

列出为您的系统配置的所有分类视图实体的名称。例如：

```
Triage Map Configurations.By Frontend|OrderEngine|Backend Calls:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewRecordSummary.action|kmuernxjasdfghjwerhgiusadfoiuo
herg:Active
Triage Map Configurations.By Frontend|/medrec|Backend Calls|System localhost
on port 9082:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewPatient.action|viewPatient.action:Active
Triage Map Configurations.By Frontend|Apache-Axis:Active
Triage Map Configurations.By Business Service|Trading Service:Active
Triage Map Configurations.By Business Service|Trading
Service|Balances:Active
Triage Map Configurations.By Frontend|AuthenticationEngine:Active
Triage Map Configurations.By Frontend|AuthenticationService|Backend
Calls|webServices:Active
Triage Map Configurations.By Frontend|AuthenticationService|Health:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewRecordSummary.action:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewNewlyRegisteredPatients.action|kmuernxjasdfghjwerhg
iusadfoiuoherg:Active
Triage Map Configurations.By Business Service|Trading Service|Place
Order:Active
Triage Map Configurations.Business Service|Trading Service|Business
Transactions|Login:Active
Triage Map Configurations.Business Service|MedRecBS|Business
Transactions|index.action:Active
```

## Loadbalancing.xml 命令

MOM 使用 loadbalancing.xml 文件对整个群集的代理进行负载平衡，并且允许代理连接到特定收集器。这些命令更新 loadbalancing.xml 文件。

### Autoprepare Loadbalancing.xml

此命令可以在升级期间在 MOM 上运行。如果 8.x 和 9.0.x 代理有在 IntroscopeAgent.profile 中定义的收集器连接的代理，请使用此命令。

MOM 收集直接连接到收集器的所有 8.x 和 9.0.x 代理方面的运行时信息。MOM 填充 loadbalancing.xml 底部的连接信息。

**重要信息！** 在 MOM 和所有收集器升级到 9.1.2 或更高版本之后、代理升级之前运行此命令。如果您在代理升级之后运行此命令，MOM 无法搜集以前的代理与收集器连接的信息。

有关详细信息，请参阅《CA APM 安装和升级指南》。

### 语法

```
autoprepare loadbalancing.xml
```

### 示例

```
autoprepare loadbalancing.xml
```

代理 A、B、C、D、E 以及 F 都是版本 8.x 至 9.0.x。将这些代理在各自的 IntroscopeAgent.profile 文件中配置为连接到收集器 1、2、3，如下表所示：

代理名称	收集器名称
AgentA	Collector01
AgentB	Collector01
AgentC	Collector02
AgentD	Collector02
AgentE	Collector03
AgentF	Collector03

组织使用 loadbalancing.xml 对名为 EPAgent2 的代理进行负载平衡。

在所有 8.x 和 9.0.x 版本的代理启动并运行后，管理员可以运行 autoprepare loadbalancing.xml CLW 命令。loadbalancing.xml 文件由下列示例中以粗体显示的条目进行填充：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<loadbalancing xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="loadbalancing0.1.xsd">
  <agent-collector name="Example 1">
    <agent-specifier>.*\|.*\|EPAgent2</agent-specifier>
    <exclude>
      <collector latched="false" port="5001" host="collector02"/>
    </exclude>
  </agent-collector>
  <agent-collector name="Collector01@5001 auto-generated configuration">
    <agent-specifier>HostName|ProcessName|AgentA</agent-specifier>
    <agent-specifier>HostName|ProcessName|AgentB</agent-specifier>
    <include>
      <collector latched="false" port="5001" host="collector01"/>
    </include>
  </agent-collector>
  <agent-collector name="Collector02@5001 auto-generated configuration">
    <agent-specifier>HostName|ProcessName|AgentC</agent-specifier>
    <agent-specifier>HostName|ProcessName|AgentD</agent-specifier>
    <include>
      <collector latched="false" port="5001" host="collector02"/>
    </include>
  </agent-collector>
  <agent-collector name="Collector03@5001 auto-generated configuration">
    <agent-specifier>HostName|ProcessName|AgentE</agent-specifier>
    <agent-specifier>HostName|ProcessName|AgentF</agent-specifier>
    <include>
      <collector latched="false" port="5001" host="collector03"/>
    </include>
  </agent-collector>
</loadbalancing>
```

示例 1 是管理员运行命令之前的 loadbalancing.xml 条目。在示例 1 之后，MOM 添加了自动生成的条目。

## 输出

以代理对收集器的连接条目更新 Loadbalancing.xml。



## 示例脚本

本节包含使用 CLW 命令的示例脚本：

- [事务跟踪会话](#) (p. 177)
- [由报警触发的事务跟踪会话](#) (p. 181)

使用其他脚本的脚本（*setlscEnv.cmd* 和 *configureWily.cmd*）可在 <http://wilycommunity.ca.com/entry.jspa@externalID=2103&categoryID=492.html> 上找到。它们是名为 *Useful Introscope Scripts* 的社区开发工具的一部分，可以用来帮助进行启动、关闭和重新启动，还可用来帮助使用 CLW。下载相应的 ZIP 文件并按照说明来安装脚本：

1. 将相应的文件 *scriptsBin.unix.zip* 或 *scriptsBin.win.zip* 提取到您的企业管理器安装中。该软件包将创建 *bin* 子目录。
2. 转到 *bin* 子目录，并调用以下命令：

```
.\configureScriptsEnv.cmd
```

或

```
./configureScriptsEnv.sh
```

3. 这将创建文件 *setlscEnv.cmd* 或 *setlscEnv.sh*。此文件包含从中读取其他脚本的所有相关 Introscope 文件夹位置。

## 事务跟踪会话

此脚本启动针对所有代理的事务跟踪会话。在运行时，您提供两个参数：

- 执行阈值—要跟踪的事务的最短执行时间（以秒为单位）。
- 会话持续时间—事务跟踪会话的持续时间（以秒为单位）。

脚本将结果存储在以日期为导向的目录结构中。

### Name

```
clwTxnTracer
```

### 语法

```
clwTxnTracer <threshold> <duration>
```

其中：

*threshold* 是事务执行时间阈值（以秒为单位）

*duration* 是会话的持续时间（以秒为单位）

## 示例

```
clwTxnTracer 1 600
```

为执行时间超过 1 秒的事务运行持续时间为 600 秒的事务跟踪会话。

## 结果

将事务跟踪数据写入到单个文件中，该文件位于与当前日期对应的目录中：

```
<EM_Home>/traces\<year>\<month>\<day>\<agents>  
_<threshold>secs_for<duration>secs.<start_time>.xml
```

例如：

```
C:\introscope\traces\2004\11\11\AllAgents_1secs_for600secs.  
14091705.xml  
@ECHO OFF  
SETLOCAL  
TITLE Introscope -- Transaction Tracer Session
```

```
REM ****  
REM Sets the current working directory with quotes around it  
REM This enables this file to execute correctly if it is  
REM invoked somewhere other than its location.  
REM ****  
FOR /f "tokens=1 delims=" %%a in ('cd') DO SET PWD=%%a
```

```
REM ****
REM Set the command directory to the command argument itself,
REM namely the full path of this file or the relative path
REM to where the file was invoked.
SET CMD_DIR=%0
REM Now simply strip out the name of this file to get dir
REM !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
REM      Use current filename
SET CMD_DIR=%CMD_DIR:clwTxnTracer.cmd=%
REM !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
REM Strip the quotes
REM add quotes if they're not there
SET CMD_DIR="%CMD_DIR%"
REM if not add quotes, then this statement chokes
SET CMD_DIR=%CMD_DIR:="=%
REM if the current dir wasn't determined, just set it to working dir
IF NOT EXIST "%CMD_DIR%" SET CMD_DIR=.
IF "%CMD_DIR%" == %0 SET CMD_DIR=.
IF "%CMD_DIR%" == "%0" SET CMD_DIR=.

REM ****
REM Now set the home directory for Introscope, and others
IF NOT EXIST "%CMD_DIR%\setIscEnv.cmd" goto noSetEnvFile
call "%CMD_DIR%\setIscEnv.cmd"

SET TT_THRESHOLD_IN_SECS=%1
SET TT_DURATION_IN_SECS=%2
IF "X%TT_THRESHOLD_IN_SECS%" == "X" SET TT_THRESHOLD_IN_SECS=10000
IF "X%TT_DURATION_IN_SECS%" == "X" SET TT_DURATION_IN_SECS=600
IF %TT_THRESHOLD_IN_SECS% LEQ 0 GOTO badArg
IF %TT_DURATION_IN_SECS% LEQ 0 GOTO badArg
SET TT_AGENTS=(.*)

REM Java Settings (e.g. increase Max heap size )
SET JAVA_OPTS=-Xms64m -Xmx512m
SET
JAVA_OPTS=%JAVA_OPTS% %CLW_USER_OPT% %CLW_PASSWORD_OPT% %CLW_EM_HOST_OPT% %CLW_EM_PORT_OPT%
```

```

SET COMMAND=trace transactions exceeding %TT_THRESHOLD_IN_SECS% seconds in
agents matching \"%TT_AGENTS%\" for %TT_DURATION_IN_SECS% seconds

SET AGENT_STR=%TT_AGENTS%
REM Remove the spaces, parentheses
SET AGENT_STR=%AGENT_STR:(=%
SET AGENT_STR=%AGENT_STR:)=%
SET AGENT_STR=%AGENT_STR:=%
SET AGENT_STR=%AGENT_STR:=%
if "%TT_AGENTS%" == "X(.*)" SET AGENT_STR=AllAgents
FOR /f "tokens=1-4 delims=:" %%a in ("%time%") DO SET SECS_STR=%%a%%b%%c%%d
FOR /f "tokens=1-4 delims=/ " %%a in ("%date%") DO SET
TRACES_DIR=%ISC_TRACES%\%%d\%%b\%%c

REM Create the traces dir, if not exist
IF NOT EXIST "%TRACES_DIR%" MKDIR "%TRACES_DIR%"
SET
TT_FILE=%TRACES_DIR%\%AGENT_STR%\%TT_THRESHOLD_IN_SECS%secs_for%TT_DURATION_I
N_SECS%secs.%SECS_STR%.xml

TITLE Introscope -- Transaction Tracer for %TT_DURATION_IN_SECS% secs with
threshold %TT_THRESHOLD_IN_SECS% secs
REM send stderr to null b/c there are meaningless disconnect excepts that might
be *scary-looking*
ECHO Saving session output to %TT_FILE%
"%ISC_JAVA_HOME%\bin\java" %JAVA_OPTS% -jar "%CLW_JAR%" %COMMAND% > "%TT_FILE%"
2>NUL
goto finish

:badArg
ECHO Arguments should be greater than zero.
ECHO Syntax: $0 "threshold in secs" "duration in secs"
goto finish

:noSetEnvFile
ECHO There is no environment setup file: setIscEnv.cmd
ECHO Please re-run configurewily.cmd in installation directory!
goto finish

:finish
ENDLOCAL

```

## 由报警触发的事务跟踪会话

触发某个报警后，此脚本启动事务跟踪会话。您可以使用 Shell 命令操作来调用该会话，以将报警消息文本作为参数传递给它。

该脚本对报警消息文本进行解析以确定是哪个代理所报告的数据触发了报警，以及所超出的危险级别值，然后将其作为用于事务跟踪会话的代理和阈值。会话结果存储在以日期为导向的目录结构中。

### Name

*alert2TxnTracer*

### 语法

有关创建 shell 命令操作的详细信息，请参阅《CA APM Workstation 用户指南》。

### 结果

将事务跟踪数据写入到单个文件中，该文件位于与当前日期对应的目录中：

```
<EM_Home>/traces\<<year>\<month>\<day>\<agents>  
_<threshold>secs_for<duration>secs.<start_time>.xml
```

例如：

```
C:\introscope\traces\2004\11\11\AllAgents_1secs_for600secs.14091705.xml
```



## 第 10 章：使用 WatchDog 命令行工具

---

为保证可靠性和安全性，可以使用一个单独的 WatchDog 进程来启动和监控企业管理器服务器。您可以使用跨平台的 WatchDog 命令行工具来启动、停止和管理企业管理器服务器，以及重新启动失败的企业管理器服务器。

此部分包含以下主题：

[关于 WatchDog](#) (p. 183)

[运行 WatchDog](#) (p. 184)

[WatchDog 命令](#) (p. 185)

[WatchDog 命令选项](#) (p. 189)

[查看 WatchDog 日志文件](#) (p. 193)

[示例脚本](#) (p. 193)

### 关于 WatchDog

WatchDog 是用来启动、停止和管理企业管理器进程的跨平台命令行工具。本工具还能重新启动失败的企业管理器，以支持现有的企业管理器故障切换功能。

WatchDog 命令行工具位于 `<EM_Home>/bin` 目录中。您可以使用以下方法之一调用这些命令：

- 使用 `WatchDog.bat` 或 `WatchDog.sh` 帮手
- 直接从 `WatchDog.jar` 运行 Java 应用程序。此方式允许您指定更多也是更复杂的选项。例如，要通过 `watch` 模式的 WatchDog 进程启动企业管理器，请从 `bin` 目录键入 `WatchDog watch`。

**注意：**使用 WatchDog 需要安装 JRE 1.6。

每个 WatchDog 命令将控制权返还给命令窗口或 shell，同时返回一个结果代码。WatchDog 实际上是两个进程：

- **WatchDog 管理器**

接受来自命令行的行，执行各种操作，并返回结果。

- **WatchDog 服务器进程**

监控企业管理器的运行状况，并且自动地重新启动停止的企业管理器。

**注意：**因为您可以使用 WatchDog 之外的机制启动企业管理器，所以 *start* 命令不是始终能够知道企业管理器是否处于启动过程中。因此，如果在一个企业管理器启动后且 WatchDog 还不知道这一情况时立即调用了 WatchDog，则 WatchDog 会试图启动第二个企业管理器实例。第二次启动企业管理器的尝试将失败，且不会返回错误结果，因为发出的唯一命令是 *start*。会在 *<企业管理器主目录>/logs* 中的企业管理器日志文件中记录一个错误。

最后，第一个 WatchDog *start* 命令尝试成功，WatchDog 返回 *running* 命令。

## 运行 WatchDog

可使用 Windows 命令提示符或 UNIX shell 查看 WatchDog 结果代码。

### 使用 WatchDog.bat 或 WatchDog.sh 运行 WatchDog

1. 打开 Windows 命令提示符或 UNIX shell。
2. 转到 *<EM\_Home>\bin*（对于 Windows）或 *<EM\_Home>/bin*（对于 UNIX）。
3. 键入 *WatchDog <command>*，其中 *<command>* 为：*start*、*watch*、*stop*、*status* 或 *help*。有关命令的更多信息，请参阅 [WatchDog 命令](#) (p. 133)。

### 通过直接调用 WatchDog.jar 来运行 WatchDog:

1. 打开 Windows 命令提示符或 UNIX shell。
2. 转到 *<EM\_Home>\bin*（对于 Windows）或 *<EM\_Home>/bin*（对于 UNIX）。
3. 根据您的操作系统，键入以下命令：
  - Windows:  

```
..\jre\bin\java -jar WatchDog.jar command [-options]
```
  - UNIX:  

```
../jre/bin/java -jar WatchDog.jar command [-options]
```有关命令的更多信息，请参阅 [WatchDog 命令](#) (p. 133)。



## 在 SAP 上运行 WatchDog

在 SAP 环境中运行的企业管理器上使用 WatchDog 时，用户必须具有管理员凭据才能使用 WatchDog。

在 SAP 环境中的企业管理器上运行 WatchDog 命令：

- 提供您的企业管理器管理用户 ID 和密码以继续。

## WatchDog 命令

WatchDog 命令对应于其四个基本功能：

- 启动和重新启动企业管理器进程—请参阅 [WatchDog start 命令](#) (p. 186)
- 停止企业管理器进程—请参阅 [WatchDog stop 命令](#) (p. 187)
- 检查企业管理器的状态—请参阅 [WatchDog status 命令](#) (p. 187)

输入命令时使用以下两种语法之一：

- 基本语法，这是通过使用 *WatchDog.bat*（对于 Windows）或 *WatchDog.sh*（对于 UNIX）帮助程序脚本而得以简化的语法。
- 完整语法，直接调用 *WatchDog.jar* Java 应用程序并允许所有 WatchDog 选项。

WatchdDog 是通过在命令行上使用 `java -jar WatchDog.jar command [-options]` 进行控制的。

所有命令都将返回两个结果代码：

- 一个针对企业管理器。
- 另一个针对 WatchDog 的自动重新启动功能。

WatchDog 结果代码的前缀为 *wd*。

## WatchDog start 命令

*start* 命令用于启动企业管理器进程，但依赖于用以启动企业管理器进程的现有命令。

在使用 WatchDog 启动企业管理器时，您可以使用 WatchDog 的自动重新启动功能，也可以使用基本语法。如果您使用基本语法，则不必指定 *start* 命令，因为它默认为 *Introscope Enterprise Manager.exe*（对于 Windows）或 *Introscope\_Enterprise\_Manager*（对于 UNIX）。如果您使用 *watch* 命令，则该命令会将 WatchDog 服务器置于 *watch* 模式，在该模式下，WatchDog 服务器会定期检查企业管理器是否已停止运行，并在必要时重新启动企业管理器。

使用完整语法随 *start* 命令一起键入 *-watch* 命令选项，这会将 WatchDog 置于 *watch* 模式。

**注意：**因为 WatchDog 是一个同步进程（也就是说，它无需等待其他内容即可返回结果），所以，*startcommandissued* 和 *stopcommandissued* 是输入 *start* 或 *stop* 命令后唯一可能得到的结果。这些结果仅表示命令已发出，并不表示企业管理器实际上已启动或停止。要进行确认，可以检查企业管理器日志或检查操作系统进程。

### start 命令语法

本节介绍了 WatchDog *start* 命令的语法。

#### 基本语法

```
WatchDog start
```

```
WatchDog watch
```

#### 完整语法

```
..\jre\bin\java -jar WatchDog.jar start -startcmd <cmd>
```

```
..\jre\bin\java -jar WatchDog.jar start -watch -startcmd <cmd>
```

#### 企业管理器返回值

*startcommandissued*—企业管理器没有在运行。

*alreadyrunning*—企业管理器已在运行。

*starting*—企业管理器正在启动。

*starterror*—尝试启动企业管理器时出错。

## WatchDog 返回值

*wdstartedwatching*—WatchDog 已进入监控模式。

*wdalreadywatching*—WatchDog 已在运行。

*wdstartedsleeping*—WatchDog 服务器进程正在运行，但未处于监控模式。

*wdalreadysleeping*—WatchDog 已处于睡眠模式。

## WatchDog stop 命令

WatchDog stop 命令向企业管理器和 WatchDog 的服务器进程发出 *stop* 命令。因为 WatchDog 可能在 *watch* 模式下运行，因此该命令是确保企业管理器停止或保持停止状态的最好方式。

### stop 命令语法

本节介绍了 WatchDog stop 命令的语法。

### 基本语法

```
WatchDog stop
```

### 完整语法

```
..\jre\bin\java -jar WatchDog.jar stop
```

## 企业管理器返回值

*stopcommandissued*—企业管理器正在运行。

*alreadystopped*—企业管理器未运行。

*stoperror*—尝试停止企业管理器时出错。

## WatchDog 返回值

*wdstopped*—WatchDog 已停止。

*wdstopcommandissued*—WatchDog 正在运行。

## WatchDog status 命令

*status* 命令可报告企业管理器和 WatchDog 的状态。

### status 命令语法

本节介绍了 WatchDog status 命令的语法。

#### 基本语法

*WatchDog 状态*

#### 完整语法

```
..\jre\bin\java -jar WatchDog.jar status
```

#### 企业管理器返回值

*running*—企业管理器正在运行。

*stopped*—企业管理器未运行。

*starting*—企业管理器正在启动。

*statusunknown*—企业管理器的状态未知。

#### WatchDog 返回值

*wdwatching*—WatchDog 正在运行。

*wdsleeping*—WatchDog 服务器进程正在运行（与 WatchDog 启动企业管理器时一样），但未处于监控模式。

*wdstopped*—WatchDog 未在运行。

## WatchDog 命令选项

WatchDog 提供了高级选项，在使用基本语法时这些选项不可用。如果使用基本语法，这些选项将采用其默认值。

命令选项仅适用于 *start* 命令，但 *-port* 命令选项除外，该选项可以用于所有命令。

命令选项包括：

- [WatchDog -watch 命令选项](#) (p. 189)
- [WatchDog -port 命令选项](#) (p. 190)
- [WatchDog -startcmd 命令选项](#) (p. 190)
- [WatchDog -interval 命令选项](#) (p. 191)
- [WatchDog -startuptime 命令选项](#) (p. 191)
- [WatchDog -jre 命令选项](#) (p. 192)

### WatchDog -watch 命令选项

*-watch* 命令选项仅可以与 *start* 命令一起使用（请参阅 [WatchDog start 命令](#) (p. 186)）。这是在企业管理器中启用自动重新启动功能的唯一方法。

您可以在企业管理器已启动后打开或关闭 *watch* 功能。例如，如果企业管理器正在运行，但 WatchDog 未处于 *watch* 模式，您可以使用带 *-watch* 选项的 *start* 命令来将 WatchDog 服务器置于 *watch* 模式。同样，即使企业管理器已在运行，使用不带 *-watch* 选项的 *start* 命令可以使 WatchDog 脱离 *watch* 模式。

将 *-watch* 选项与 *start* 命令一起使用时，该命令会返回以下值：

- *startedwatching*—输入该命令之前，WatchDog 未在进行监控。它现在正在监控。
- *alreadywatching*—输入该命令之前，WatchDog 已在进行监控。WatchDog 将继续执行监控。

如果未将 `-watch` 选项与 `start` 命令结合使用，则会返回以下值：

- `startedsleeping`—输入该命令之后，WatchDog 才会进入睡眠状态。它已停止监控。
- `alreadysleeping`—输入该命令之前，WatchDog 已进入睡眠状态。WatchDog 将继续不执行监控。

### **-watch 命令选项示例：**

```
<EM_Home>\bin>..\jre\bin\java -jar watchDog.jar start -watch -startcmd
"..\Introscope Enterprise Manager.exe"
watchMgr: iPort = 4321; watch = true; startcmd = ..\Introscope Enterprise
Manager.exe;
startcommandissued & wdstartedwatching
```

## WatchDog -port 命令选项

使用 `-port` 选项为 WatchDog 的服务器端口指定值。如果不输入值，将使用默认值 4321。

为第一个 WatchDog `start` 命令指定 `-port` 值时，随后的所有命令将使用相同的值。

**注意：**另外，您还可以通过修改 `WatchDog.bat` 文件或创建新的批处理文件，在非默认端口上运行 WatchDog 服务器。这将确保正确的端口随每个命令传递到 WatchDog 管理器。

### **-port 命令选项示例：**

```
<EM_Home>\bin>..\jre\bin\java -jar watchDog.jar
start -port 5555 -startcmd "..\Introscope Enterprise Manager.exe"
watchMgr: iPort = 5555; watch = false; startcmd = ..\Introscope Enterprise
Manager.exe;
alreadyrunning & wdalreadysleeping
```

## WatchDog -startcmd 命令选项

使用此选项来指定启动企业管理器的命令。

**注意：**此命令选项仅适用于 `start` 命令。有关更多信息，请参阅 [WatchDog start 命令](#) (p. 186)。

## WatchDog -interval 命令选项

使用 *interval* 选项以秒为单位指定企业管理器状态检查发生的时间，从而查看企业管理器是否已停止。如果未指定此选项，将使用默认值 10 秒。

当 WatchDog 的状态为 *watching* 时，此选项适用。

**注意：**此命令选项仅适用于 *start* 命令。有关更多信息，请参阅 [WatchDog start 命令](#) (p. 186)。

### -interval 命令选项示例：

```
C:\Program Files\CA Wily\Introscope9.0d140\bin>..\jre\bin\java -jar
watchDog.jar start -watch -interval 300 -startcmd "..\Introscope Enterprise
Manager.exe"
watchMgr: iPort = 4321; watch = true; startcmd = ..\Introscope Enterprise
Manager.exe;
startcommandissued & wdstartedwatching
```

## WatchDog -startuptime 命令选项

使用此选项以秒为单位指定 WatchDog 允许企业管理器启动的时间。在 WatchDog 启动企业管理器后，会传递为此选项指定的时间量，且企业管理器的状态将更改为 *starting*。然后，所配置的用来确定企业管理器状态的正常机制将就位。

企业管理器状态检查是在企业管理器启动之后立即完成的，因此不会为它分配 *running* 状态。相反，在 WatchDog 启动企业管理器后的数秒内，WatchDog 的 *status* 命令会返回 *starting* 状态。此功能可防止 WatchDog 意外启动两个企业管理器实例。文件 *-startuptime* 选项允许将此延迟配置为默认值（30 秒）之外的值。

**注意：**此命令选项仅适用于 *start* 命令。有关更多信息，请参阅 [WatchDog start 命令](#) (p. 186)。

### -startuptime 命令选项示例：

```
<EM_Home>\bin>..\jre\bin\java -jar watchDog.jar start -watch -startuptime 60
-startcmd "..\Introscope Enterprise Manager.exe"
watchMgr: iPort = 4321; watch = true; startcmd = ..\Introscope Enterprise
Manager.exe;
startcommandissued & wdstartedwatching
```

## WatchDog -jre 命令选项

如果 JRE 不位于默认目录 `jre/bin/java` 中，则使用此选项来指定 JRE 路径。

### -jre 命令选项示例:

```
C:\Program Files\Java\jre1.6.0_07\bin\java" -jar watchDog.jar start -watch -jre
"C:\Program Files\Java\jre1.6.0_07\bin\java" -startcmd "..\Introscope
Enterprise Manager.exe"
startcommandissued & wdstartedwatching
```

## WatchDog -emport 命令选项

如果企业管理器在默认端口 5001 之外的端口号上运行，请使用 `-emport` 选项来指定企业管理器的服务器端口的值。如果企业管理器在默认端口 5001 之外的端口号上运行，需要使用此命令。

### -emport 命令选项示例:

```
C:\Program Files\CA wily\Introscope9.0\bin>..\jre\bin\java -jar watchDog.jar
start -emport 5003 -startcmd "..\Introscope Enterprise Manager.exe"
watchMgr: iPort = 5555; watch = false; startcmd = ..\Introscope Enterprise
Manager.exe;
alreadyrunning & wdalreadysleeping
```

## WatchDog -emuser 命令选项

如果已经为企业管理器配置了默认用户名 `Admin` 之外的用户名，请使用 `-emuser` 选项。

当为企业管理器配置了默认用户名 `Admin` 之外的用户名时，需要使用此命令。

此外，请将 `-emuser` 选项与 `-empwd` 选项结合使用。

### -emuser 命令选项示例:

```
<EM_Home>\bin>..\jre\bin\java -jar watchDog.jar
start -emuser EMUserName -empwd EMPassWord -startcmd "..\Introscope Enterprise
Manager.exe"
watchMgr: iPort = 5555; watch = false; startcmd = ..\Introscope Enterprise
Manager.exe;
alreadyrunning & wdalreadysleeping
```



## WatchDog -empwd 命令选项

如果已经为企业管理器配置了默认密码 "" 之外的密码时，请使用 `-empwd` 选项。

当为企业管理器配置了默认密码 "" 之外的密码时，需要使用此命令。

此外，请将 `-empwd` 选项与 `-emuser` 选项结合使用。

### **-empwd 命令选项示例：**

```
<EM_Home>\bin>..\jre\bin\java -jar WatchDog.jar
  start -emuser EMUserName -empwd EMPassWord -startcmd "..\Introscope Enterprise
Manager.exe"
watchMgr: iPort = 5555; watch = false; startcmd = ..\Introscope Enterprise
Manager.exe;
alreadyrunning & wdaalreadysleeping
```

## 查看 WatchDog 日志文件

`WatchDogServer` 进程日志文件写入到 `WatchDog.log` 文件中。

### **查看 WatchDog 日志文件：**

1. 转到 `<EM_Home>/logs`。
2. 打开 `WatchDog.log` 文件。

## 示例脚本

`WatchDog.bat` 和 `WatchDog.sh` 实现了针对 Windows 平台和 UNIX 平台的基本语法。还可以使用这些脚本作为起点，开发简化了 WatchDog 完全语法的自定义脚本。使用位于 Windows 和 UNIX 安装的 `<EM_Home>/bin` 目录中的 `WatchDog.bat` 和 `WatchDog.sh`。



# 第 11 章：配置 WebView 选项

---

此部分包含以下主题：

[配置 WebView 应用程序上下文路径](#) (p. 195)

[如何配置和监控 APM WebView 性能](#) (p. 195)

## 配置 WebView 应用程序上下文路径

您还可以为 WebView 安装配置应用程序上下文路径。此路径将附加到 WebView 的完全限定主机名和端口号之后，以形成用于访问 WebView 的 URL。此功能允许用户为 WebView 定义“应用程序名称”。

**在没有上下文路径的情况下访问 WebView：**

- 使用以下 URL：

`http://<Server_name>:<Port_number>`

**在配置了上下文路径时访问 WebView：**

- 使用以下 URL：

`http://<Server_name>:<Port_number>/<Context_path>/`

例如，如果 `Context_path` 定义为 `webview`，且 `introscope.webview.tcp.port` 属性设置为默认值 `8080`，则通过以下 URL 访问 WebView：

`http://<Server_name>:8080/webview/`

您可在 WebView 属性文件中使用 `introscope.webview.context.path` 属性配置 WebView 上下文路径。有关详细信息，请参阅 [introscope.webview.context.path](#) (p. 474)。在定义上下文路径属性后重新启动 WebView。

## 如何配置和监控 APM WebView 性能

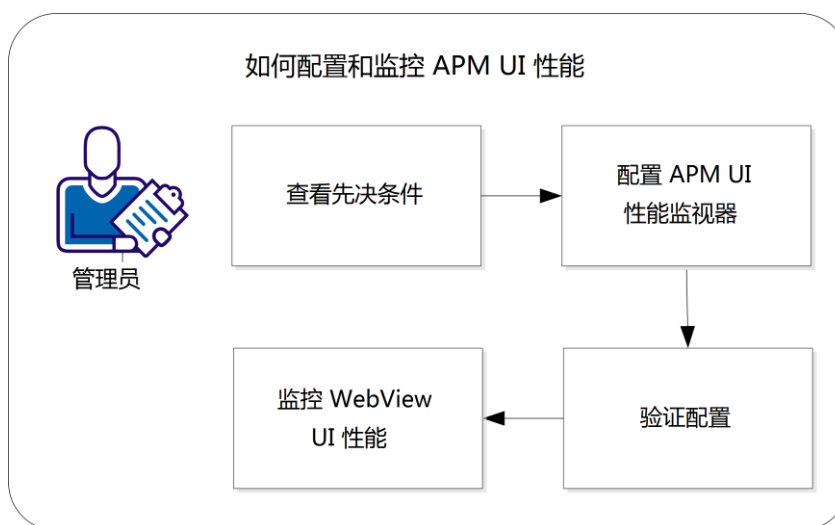
**注意：** APM UI Performance Monitor 对 SAP WebView 用户不可用。

APM UI Performance Monitor 为 WebView 应用程序收集和报告性能度量标准。您可以以管理员身份使用这些信息在潜在的 WebView 性能问题影响用户之前，检测并隔离这些问题。例如，在硬件资源不足或使用太多并行会话时，尤其在使用大数据视图时，可能会发生性能问题。

WebView 服务器安装可部署 Java 代理。启用后，嵌入式 Java 代理会监控服务器组件和硬件资源，并且收集的度量标准会报告给企业管理器。然后，企业管理器会处理和存储用于实时和历史报告的数据。收集的数据会显示在 WebView 中的以下示例显示板中：

- [WebView - 概览](#) (p. 200)
- [WebView - 视图和小组件](#) (p. 201)
- [WebView - 资源](#) (p. 201)

下图介绍了如何以管理员身份配置和使用 APM UI Performance Monitor：



- [查看先决条件](#) (p. 196)。
- [配置 APM UI Performance Monitor](#) (p. 197)。
- [验证配置](#) (p. 199)。
- [监控 WebView UI 性能](#) (p. 199)。
- (可选) [配置 WebView 度量标准组](#) (p. 202)。
- (可选) [查看和解析显示板数据](#) (p. 202)。

## 查看先决条件

前提条件如下所示：

1. 确保针对该配置显示以下组件及其目录（及文件）：
  - Java 代理。  
<WEBVIEW\_HOME>/products/webview/agent
  - 用于控制代理操作、度量标准数据收集和检测过程的 WebView Probuilder 指令文件 (WebView.pbd)。  
<WEBVIEW\_HOME>/products/webview/agent/wily/core/config

2. 为 Java 代理配置 *IntroscopeAgent.profile* 文件，如下所示：
  - a. 导航到 `<INSTALL_HOME>/product/webview/agent/wily/core/config`，然后在文本编辑器中打开 *IntroscopeAgent.profile*。
  - b. 搜索 *introscope.autoprobe.directivesFile*，并确认 *WebView.pbd* 附加在属性值末尾。
  - c. 搜索 *introscope.agent.defaultProcessName*，并确认属性值是 *APM WebView*。不要更改或删除此值。
  - d. 搜索 *introscope.agent.agentName*，并确认属性值是 *APM.WebView*。

配置已设置。

## 配置 APM UI Performance Monitor

在 Java 代理上配置 APM UI Performance Monitor 组件。使用以下两个安装选项之一：

- 企业管理器： `<EM_HOME>/product/webview`
- 独立的 WebView 服务器： `<WEBVIEW_HOME>/product/webview`

以下步骤适用于两种安装。

**请执行以下步骤：**

1. 在文本编辑器中打开 `<INSTALL_HOME>` 目录中的 *Introscope\_WebView.lax* 文件。
2. 搜索以下属性：

```
tax.n1.java.option.additional
```

此属性的注释行如以下示例所示：

```
# webview 监控器的 Introscope Java 代理参数
# -XX:PermSize=128m -XX:MaxPermSize=256m
-javaagent:./product/webview/agent/wily/Agent.jar
-Dcom.wily.introscope.agentProfile=./product/webview/agent/wily/core/config/IntroscopeAgent.profile
-Dcom.wily.introscope.wilyForwilyPrefix=com.wily
-Djetty.home=./
```

3. 从不包括“#”的行复制参数，并将它附加到 *lax.nl.java.option.additional* 属性值。

结果如以下示例所示：

```
lax.nl.java.option.additional=-Xms256m -Xmx1024m
-Djava.awt.headless=false
-Dorg.owasp.esapi.resources=./config/esapi
-Dsun.java2d.noddraw=true
-Dintroscope.webview.testpanel.enable=false
-Dintroscope.webview.saas.enable=false
-XX:PermSize=128m
-XX:MaxPermSize=256m
-javaagent:./product/webview/agent/wily/Agent.jar
-Dcom.wily.introscope.agentProfile=./product/webview/agent/wily/core/config/IntroscopeAgent.profile
-Dcom.wily.introscope.wilyForWilyPrefix=com.wily
-Djetty.home=.
```

**注意：**文件中的值可能不同于此示例。

保存您的更改。

4. 部署 WebView 监控器管理模块，方法是将 *WebView.jar* 文件从 *modules* 文件夹复制到：

```
<EM_HOME>/examples/webviewMonitor/config/modules
```

*deploy* 文件夹：

```
<INSTALL_HOME>/deploy
```

重新启动 WebView 服务器以完成配置。

5. （可选）仅针对 Windows：如果您创建了启动 WebView 应用程序的 Windows 服务，如下所示，您可以配置为：在该服务启动时启动 APM UI Performance Monitor：

- a. 导航至 <安装主目录>/bin 目录，并在文本编辑器中打开 *WVService.conf* 文件。

- b. 找到 *# Java Additional Parameters* 下的以下部分：

```
#wrapper.java.additional.4=-XX:PermSize=128m -XX:MaxPermSize=256m
-javaagent:./product/webview/agent/wily/Agent.jar
-Dcom.wily.introscope.agentProfile=./product/webview/agent/wily/core/config/IntroscopeAgent.profile
-Dcom.wily.introscope.wilyForWilyPrefix=com.wily -Djetty.home=.
```

- c. 删除此字符串开始处的“#”，以便在这些参数中进行注释。

保存您的更改。

重新启动 Windows 服务以完成配置。

## 验证配置

验证配置是否正确。

请执行以下步骤：

1. 在 WebView 中，依次单击“调查器”和“度量标准浏览器”。
2. 导航到 APM.WebView，如下所示：  
`<DomainName>|<webViewHostName>|APM Introscope webView|APM.webview`
3. 查看标准度量标准，并验证它们是否在将数据报告给企业管理器。
4. 单击“控制台”选项卡，验证以下示例显示板是否显示在显示板下拉列表中：
  - WebView - 概览
  - WebView - 视图和小组件
  - WebView - 资源
5. 打开“WebView - 概览”示例显示板，然后执行以下任务：
  - 右键单击数据查看器中的图形或图表。从“链接”下拉列表导航到管理模块中的相应度量标准。
  - 从图表或图形中打开工具提示，然后单击链接导航到度量标准浏览器树中相应的度量标准。

配置已验证。

## 监控 WebView UI 性能

APM UI Performance Monitor 示例显示板为 WebView 应用程序提供运行状况监控和问题解决功能。性能问题可以显示为可视化通知。例如，显示板显示具有以下信息的条形图：

- 黄线表示 3000 毫秒的警告阈值
- 红线表示 4000 毫秒的危险阈值

请执行以下步骤：

1. 在 WebView 中的“控制台”选项卡上，从下拉列表中选择 WebView 监控示例显示板。
  - [WebView - 概览](#) (p. 200)
  - [WebView - 视图和小组件](#) (p. 201)
  - [WebView - 资源](#) (p. 201)

此显示板将会打开并显示当前的性能状态。条形图以横条显示当前数据值。

2. 分析[标准度量标准](#) (p. 204)。
3. 如需有关显示板上数据的更多信息，请使用以下快捷方式：
  - 将鼠标悬停在具有超链接的显示板对象上。指针将变成手形。单击对象可跟随链接转到其默认目标。
  - 右键单击数据查看器中的显示板对象。指针将变成手形。从“链接”下拉列表导航到管理模块中的相应对象。数据查看器会自动链接到它所基于的度量标准组。
  - 将鼠标悬停在元素上打开工具提示。工具提示在分类视图选项卡和度量标准浏览器选项卡中都找到的分层树和查看器窗格中标识度量标准路径和值。要查看树内的度量标准，请单击工具提示内的超链接。
4. 通过选择时间范围[查看不同时间点的数据](#) (p. 203)。
5. [利用平均响应时间的趋势](#) (p. 204)以及其他度量标准中的变化来识别和诊断问题。

**注意：**您可以查看 **WebView** 控制台显示板中的所有信息，但不能编辑这些信息。要创建和编辑显示板，请使用 **Workstation**。

## “WebView - 概览” 显示板

“WebView - 概览”显示板专供管理员监控整个环境中 **WebView** 应用程序的性能。

这些图表提供 **WebView** 应用程序的高级信息，以及客户端和服务端之间交互的高级信息。

此显示板包括以下图表：

### WebView 前端

显示 **WebView** 监控的应用程序的前端运行状况度量标准。利用平均响应时间的趋势以及其他度量标准中的变化来识别和诊断性能问题。

### 活动浏览器

显示已连接到服务器的浏览器。

### 活动服务

显示已连接到订阅管理器的服务。

### 每个时间间隔（15 秒）的客户端请求数

显示每个时间间隔内来自客户端的请求数。



## “WebView - 视图和小组件” 显示板

“WebView - 视图和小组件” 显示板专供管理员监控分类视图和 SOA 依存关系视图性能以及 WebView 运行状况度量标准。

这些图表显示这些视图和小组件的总体运行状况和性能。

**注意：**直到导航到“调查器”->“分类视图”中的业务服务和前端，数据才会显示在分类视图图表中。

此显示板包括以下图表：

### 分类视图和 SOA 依存关系视图运行状况

在 APM Introscope WebView 代理的 JSP 节点下显示业务服务和前端的运行状况度量标准。

### 活动小组件计数

显示活动小组件的数量。

### 每个时间间隔的活动小组件数

显示每个时间间隔的活动小组件数。

### 分类视图加载时间（毫秒）

显示加载分类视图所用的毫秒数。

## “WebView - 资源” 显示板

“WebView - 资源” 显示板专供管理员监控前端 I/O 和主机资源。

这些图表显示 WebView 资源的总体运行状况和性能。

此显示板包括以下图表：

### 前端 I/O

显示前端套接字 I/O（每秒字节数）和前端套接字 I/O 并发的输入和输出带宽。

### 主机资源

显示进程 CPU 与主机 CPU 使用率，以及服务器内存使用率与分配情况。

## 配置 WebView 度量标准组

在“WebView - 资源”显示板中，WebView 度量标准组是保存以下信息的管理模块对象：

- 代理表达式-Perl 5 中的正则表达式，通过指定数据和代理名称来筛选度量标准的输入内容。
- 度量标准表达式-Perl 5 中的正则表达式，用于指定资源（引导到度量标准的文件夹链）和度量标准。

如果要在代理表达式中重命名默认代理进程名称或默认代理名称，则需要执行其他一些步骤。

请执行以下步骤：

1. 在 WebView 中，单击“管理”选项卡并找到 WebView 监控度量标准组。
  2. 找到要更新的“WebView - 资源”显示板度量标准组。例如，前端 I/O、进程和主机 CPU、前端 I/O 并发、堆大小和分配。
  3. 编辑代理表达式中的进程名称值 (APM Introscope WebView) 或代理名称值 (APM.WebView)。
  4. 保存您的更改。
  5. 在 Java 代理中，在文本编辑器中打开 *IntroscopeAgent.profile*。
  6. 搜索 *introscope.agent.defaultProcessName* 或 *introscope.agent.agentName* 属性。
  7. 输入在第 3 步中提供的相同名称值。
  8. 保存您的更改。
- 配置已设置。

## 查看和解析显示板数据

可以通过不同的方式查看和解释显示板数据：

- [在不同时间点查看数据](#) (p. 203)。
- [查看标准度量标准](#) (p. 204)。
- [解析平均响应时间趋势](#) (p. 204)。

## 在不同时间点查看数据

可以查看实时数据，也可以选择一个时间范围，在不同时间点查看数据。数据的默认视图是实时的。

可以通过查看浏览器顶部的“时段”来查看 WebView 是否处于实时模式。

要在不同时间点查看显示板，请执行以下任务：

- [查看历史数据](#) (p. 203)。
- [定义自定义时间范围](#) (p. 203)。

## 查看历史数据

监控应用程序时，实时数据视图将不断变化，显示最新数据。实时数据是默认视图。您也可以选择一个时间范围来查看历史数据，确定问题发生的时间。

**请执行以下步骤：**

1. 在 WebView 中的“控制台”选项卡上，从“显示板”下拉列表中选择要查看其历史数据的显示板。
2. 从“时段”下拉列表中选择历史视图的时间范围，例如 24 小时。  
显示板会使用您选定的持续时间（例如 24 小时）显示该范围内的数据。结束时间设置为当前时间。
3. 如果您想更改开始时间，请单击“时段”旁边的向前和向后箭头。
4. 如果要将范围的结束时间重置为当前时间，请单击“立即结束”。

## 定义自定义时间范围

可以定义在控制台中查看数据的自定义时间范围。

**请执行以下步骤：**

1. 选择您要查看其历史数据的度量标准或显示板。
2. 从“时段”下拉列表中选择“自定义范围”。
3. 将打开“自定义范围”窗口，显示以轮廓线突出显示的当前日期（今天）。
4. 使用日历控件选择开始和结束日期。
5. 单击“确定”。  
自定义范围的数据已设置。

## 标准度量标准

WebView 显示代理从远程和本地系统收集的、作为度量标准的应用程序性能数据。对于监控的前端和后端应用程序组件，以及许多其他应用程序组件，会显示以下标准度量标准：

- **平均响应时间 (毫秒)**—应用程序响应速度的度量。
- **并发调用**—在指定时间处理的请求数。
- **每个时间间隔的错误**—指定时间片内发生的错误数。
- **每个时间间隔的响应数**—指定时间片内完成的请求数。
- **停顿计数**—停顿数。停顿是在指定的时间阈值前未完成的请求。

## 平均响应时间趋势

您可以利用平均响应时间的趋势以及对其他度量标准的更改来识别和诊断问题。下表提供更多信息：

| 平均响应时间的趋势 | 定义  |
|-----------|---|
| 连续存在的问题   | <p>采用较低的可用线程计数时，一直很高的平均响应时间可能会指示出现以下问题：</p> <ul style="list-style-type: none"><li>■ 代码效率低</li><li>■ 过度使用外部系统</li><li>■ 后端速度较慢</li><li>■ 层次过多</li></ul> <p>一致的问题始终存在，不会变得更好或更坏。</p>  |
| 周期性问题的    | <p>周期性变高的平均响应时间，此时间在图表中会周期性突增，然后回归正常。</p> <p>采用较低的可用线程计数时，周期性变高的平均响应时间可能会指示出现以下问题：</p> <ul style="list-style-type: none"><li>■ 经常发生 GC 泄露</li><li>■ 与负荷相关的后端存在瓶颈</li></ul> <p>采用较低的 CPU 使用率读数时，周期性变高的平均响应时间可能会指示出现以下问题：</p> <ul style="list-style-type: none"><li>■ 内部阻塞点</li></ul> <p>周期性问题的在固定时间间隔内发生和消退。</p> |

---

渐进式问题

采用较低的每个时间间隔的响应数读数时, 在较长的时间段内平均响应时间稳定增加可能指示出现以下问题:

- 内存泄漏

渐进式问题随着时间的推移降级。

---



## 第 12 章：配置工作站

---

本节介绍了如何为 Introscope 工作站配置可选行为。

此部分包含以下主题：

[以详细模式运行工作站](#) (p. 207)

[将工作站输出重定向到某个文件](#) (p. 207)

[配置工作站以提供登录值](#) (p. 208)

[配置工作站以使用亚洲语言报告](#) (p. 208)

### 以详细模式运行工作站

以详细模式运行工作站时会创建详细的日志消息，这对于调试或故障排除很有帮助。

以详细模式运行工作站：

1. 打开 `<EM_Home>/config` 中的文件 `IntroscopeWorkstation.properties`。
2. 在属性 `log4j.logger.Workstation` 中，将 `"INFO"` 替换为以下内容：  
`VERBOSE#com.wily.util.feedback.Log4JSeverityLevel`
3. 保存更改。

### 将工作站输出重定向到某个文件

将工作站输出重定向到某个文件：

1. 打开 `<EM_Home>/config` 中的 `IntroscopeWorkstation.properties` 文件。
2. 在 `log4j.logger.Workstation` 属性中，将 `"console"` 替换为 `"logfile"`。例如，以下属性设置会导致工作站将详细消息记录到日志文件：  
`log4j.logger.workstation=VERBOSE#com.wily.util.feedback.Log4JSeverityLevel,logfile`
3. 您可以使用 `log4j.appender.logfile.File` 属性更改工作站日志文件的名称和位置。

## 配置工作站以提供登录值

您可以修改 *Introscope Workstation.lax* 文件以提供登录值并绕过登录屏幕。

**设置命令行参数以绕过工作站登录屏幕：**

1. 打开文件 `<EM_Home>/Introscope Workstation.lax`。
2. 在 `lax.command.line.args` 属性中，对要为其提供值的每个登录命令添加 `-login` 命令。例如，使用本地身份验证时，此属性可能会如下所示：  

```
lax.command.line.args=$CMD_LINE_ARGUMENTS$ -loginimmediate  
-loginhost foos -loginport 4503 -loginresponse sanderson,45tst87
```

**注意：** 请不要从设置中删除默认值 `$CMD_LINE_ARGUMENTS$`。

如果登录成功（使用正确的语法在命令中提供了正确的信息），则您会登录到工作站，然后控制台打开。

如果登录失败，则工作站不会启动，且会记录错误消息。

## 配置工作站以使用亚洲语言报告

如果您计划生成使用多字节字符集（如汉语和日语）语言的 Introscope 报告，请按照此处的说明将组件添加到您的工作站安装中。

**以 RTF 和 HTML 格式生成亚洲语言报告：**

- 在 Windows 中安装对东亚语言的补充语言支持。请参阅 <http://www.microsoft.com/globaldev/handson/user/xpintl supp.msp>。

**以 PDF 格式生成亚洲语言的报告：**

- 从 <http://www.adobe.com/products/acrobat/acrrasianfontpack.html> 下载并安装 Acrobat Reader 亚洲字体包。



# 第 13 章： 系统配置

---

本节介绍了 CA APM 的整个系统配置。

此部分包含以下主题：

[配置时钟偏移容差](#) (p. 209)

[设置最大数据点检索属性](#) (p. 210)

[限制查询返回的数据点](#) (p. 212)

[增大返回的查询结果数](#) (p. 213)

[配置 APM 状态控制台限定和重要事件](#) (p. 213)

## 配置时钟偏移容差

时钟偏移容差是通常以小幅增量进行的时钟设置调整的变差。例如，将运行稍快的计算机时钟向后调慢几秒钟，以解决您在日志中看到的小差异。此延迟的变差导致时钟为同一度量标准标记不同的时间戳，这将导致系统为重叠时段得到两个度量标准值。

将时间后调可以显式发生（操作员更改时钟时间），也可以通过自动时钟同步隐式发生（在大型安装中可能会发生此情况）。

企业管理器使用以下两种方法之一处理时钟偏移容差：

- 对于大的时钟调整，系统会发出错误并退出。
- 对于小的后向时钟调整，会发出一条警告并且收集周期停止，直至时间戳到达调整前的时间。

此阈值的值默认设置为 60 秒，但您可以配置该值。小于数秒的负值时钟调整会导致发生警告并且收集会临时中止，而较大的调整则会导致系统退出。

如果企业管理器检测您的系统时钟已向后调整（这在网络时间服务重置较快的 CPU 时钟时常会发生），则企业管理器会延迟搜集周期，直到时钟赶上它以前的时间。此延迟通常会伴随有警告消息。如果要禁止警告消息，您可以设置可选的

`introscope.enterprisemanager.clock.skewsuppresswarn` 属性。此属性的值是允许将度量标准收集延迟的毫秒数，如果超过该值，则认为延迟足够严重，需将其记录。

### 配置时钟偏移容差阈值：

1. 停止企业管理器。
2. 转到 `<EM_Home>\config` 目录，并打开 `IntroscopeEnterpriseManager.properties` 文件。
3. 添加以下属性，其中 `<XXX>` 是一个数字（秒数）：  
`introscope.enterprisemanager.clock.skewtoleranceseconds=<XXX>`
4. 可选：设置 `introscope.enterprisemanager.clock.skewsuppresswarn` 属性。默认值（以毫秒为单位）为 `0`。

**注意：**不能将此值设置为大于

`introscope.enterprisemanager.clock.skewtoleranceseconds` 属性，否则将会完全禁止警告并导致系统退出。

5. 启动企业管理器，这将应用新设置。

## 设置最大数据点检索属性

可以将最大数据点检索属性设置为 JDBC、CLW 和前 N 个（CLW 和 Workstation）查询的性能度量标准。数据点是一个度量标准在一个时间段内的值。

此企业管理器限定属性将限制任何企业管理器针对任意单个查询从 SmartStor 检索的最大度量标准数据点数目。不过，企业管理器始终会为至少一个度量标准返回完整数据。该属性适用于群集的收集器或独立的企业管理器。

如果未设置该属性，可能会导致以下情况发生：

- 企业管理器超载，导致 CA APM 系统性能降低并可能导致内存不足错误。
- 该属性会提示命令行 Workstation 或 Workstation 提取太多数据。这些操作可能会导致企业管理器停止响应。

请执行以下步骤：

1. 转到 <EM\_Home>\config 目录，并打开 *IntroscopeEnterpriseManager.properties* 文件。

2. 添加以下属性：

*introscope.enterprisemanager.query.datapointlimit=100000*

其中 100000 可将每次查询从 SmartStor 检索到的数据点限制在 100,000 左右。如果没有输入数值，则不会应用任何限制。

3. 保存 *IntroscopeEnterpriseManager.properties* 文件。

在热部署期间当企业管理器检查属性文件时（该检查大约每 60 秒发生一次）会应用该设置。

## 限制查询返回的数据点

您可以将 `introscope.enterprisemanager.query.returneddatapointlimit` 属性设置为 JDBC、CLW 和前 N 个（CLW 和 Workstation）查询性能度量指标。此企业管理器限制属性限制查询返回的数据点数目。数据点是一个度量标准在一个时间段内的值。

查询返回的数据点数目取决于以下因素：

- 匹配的度量标准数。
- 正在请求的时间范围。
- SmartStor 数据的解析度，取决于 SmartStor 数据层的配置。

例如，假定您以 1 分钟的解析度查询单个度量标准 1 小时的数据。如果数据以 15 秒的解析度存放在 SmartStor 中，则查询将匹配 240 个数据点。但是，因为您要求 1 分钟的解析度，所以 15 秒数据点将聚合为 1 分钟数据点。因此，查询仅返回 60 个数据点。

对于给定的度量标准，查询要么返回所请求的完整数据集，要么不返回任何数据。您从不会只看到度量标准的部分数据；您要么会看到所有数据，要么看不到任何数据。此限制的效果是减少了为其返回数据的度量标准数。

如果您的环境中内存比较缺乏，并且未设置此属性，则大型数据查询可能会导致发生企业管理器内存不足的情况。

**请执行以下步骤：**

1. 转到 `<EM_Home>\config` 目录，并打开 `IntroscopeEnterpriseManager.properties` 文件。
2. 添加以下属性：  

```
introscope.enterprisemanager.query.returneddatapointlimit= 100000
```

其中 100000 可将每次查询从 SmartStor 检索到的数据点限制在 100000 左右。如果没有输入数值，则不会应用任何限制。
3. 保存 `IntroscopeEnterpriseManager.properties` 文件。  
在热部署期间当企业管理器检查属性文件时（该检查大约每 60 秒发生一次）会应用该设置。

## 增大返回的查询结果数

执行 *RangeQuery*、*PrefixQuery*、*WildcardQuery* 或 *FuzzyQuery* 查询时，在执行搜索前将扩展这些查询。例如，如果索引的文档包含术语“car”和“cars”，则在执行搜索前，查询“ca\*”将扩展为“car OR cars”。如果该数目超过了术语阈值的默认值 (2048)，这可能会导致系统错误。如果发生此情况，则将返回 *TooManyClauses* 异常。

增加返回的查询结果数：

1. 转到 `<EM_Home>\config` 目录，并打开 `IntroscopeEnterpriseManager.properties` 文件。
2. 添加以下属性，并为其指定一个高于默认值 2048 的值：  
`introscope.enterprisemanager.lucene.search.BooleanQuery.SetMaxClauseCount`

在热部署期间当企业管理器检查属性文件时（该检查大约每 60 秒发生一次）会应用该设置。

## 配置 APM 状态控制台限定和重要事件

您可以在 `apm-events-thresholds-config.xml` 文件中为 CA Introscope 限定、CA CEM 限定和重要事件属性配置阈值。当达到或超过这些属性阈值时，企业管理器会通知 APM 状态控制台。限定信息显示在“活动的限定”选项卡中。重要事件信息显示在“重要事件”表视图中。

请执行以下步骤：

1. 转到 `<EM_Home>/config` 目录，并备份 `apm-events-thresholds-config.xml` 文件。

**重要信息！** 请勿忽视备份文件。如果配置的文件损坏，属性值将恢复为默认值，您的所有配置都将丢失。

2. 根据您的环境需要配置属性。

**注意：** 请仅配置 `阈值` 字段中的值。不要更改其他任何字段，如限定 ID、重要事件 ID 和说明，因为 CA Introscope 使用这些字段进行系统监控。

- a. 打开 `apm-events-thresholds-config.xml` 文件。
- b. 修改限定和重要事件阈值。

例如，`<threshold value="500000"/>`，其中 500000 是修改的值。

3. 保存并关闭 `apm-events-thresholds-config.xml`。

在热部署期间（热部署大约每 60 秒执行一次），企业管理器会应用您的配置设置。

如果企业管理器在 `apm-events-thresholds-config.xml` 文件中找到语法错误，则采取以下操作：

- 通知 APM 状态控制台在“重要事件”表视图中显示 `apm.events.thresholds.config.error` 重要事件。
  - 将所有限定和重要事件属性值恢复为默认值。
4. 如有必要，排除 `apm-events-thresholds-config.xml` 文件的问题。
    - a. 打开 `apm-events-thresholds-config.xml` 文件。
    - b. 检查文件中的语法错误并进行任何必要的更正。
    - c. 保存并关闭文件。
    - d. 如果您无法找到或修复 `apm-events-thresholds-config.xml` 文件错误，请用步骤 1 中保存的备份文件替换损坏的 `apm-events-thresholds-config.xml` 文件。
    - e. 重复步骤 2 和 3。
  5. 如果您在整个群集中配置企业管理器，请在所有收集器、MOM 和 CDV（如果已部署）上执行步骤 1 到 4。

所有企业管理器都配置有 CA Introscope 和 CA CEM 限定和重要事件属性。当达到或超过属性阈值级别时，会部署 `apm-events-thresholds-config.xml` 文件并激活限定和重要事件限定。

# 第 14 章：配置应用程序分类地图

---

本章介绍了如何为应用程序分类地图配置可选行为。

此部分包含以下主题：

[应用程序分类视图](#) (p. 215)

[应用程序分类地图数据限定](#) (p. 219)

[配置应用程序分类视图数据清除](#) (p. 220)

[在应用程序分类视图对象中配置过时时间](#) (p. 222)

## 应用程序分类视图

应用程序分类视图提供构成应用程序的组件的图形可视化表示，可显示应用程序的运行状况和错误。该视图是根据性能以及对 Introscope 度量标准、错误和事件的分析自动生成的。它会以已定义的、以业务为中心的术语呈现应用程序。通过应用程序分类视图，您可以直观地立刻掌握环境中应用程序的结构以及应用程序之间的关系，有助于识别当前存在的问题以及将要出现的问题，并对这些问题进行分类。

有关应用程序分类视图的外观和用法的详细信息，请参阅《*CA APM Workstation 用户指南*》。

Introscope 代理检测业务事务和前端，并检测它们的依赖关系。然后，代理将此信息作为数据报告给企业管理器，企业管理器将数据存储在 APM 数据库中，并且将数据发送到 Workstation。Workstation 将数据显示为“视图”选项卡中的应用程序分类视图。

您可以配置：

- 代理是否收集应用程序分类视图数据。
- 为了绘制视图，Introscope 对前端或业务服务数据进行采样的速率。请参阅[事务采样](#) (p. 216)。
- 应用程序分类视图数据存储在 APM 数据库中的时间。请参阅[视图元素老化](#) (p. 216)。
- 是否从 APM 数据库中清除应用程序分类视图数据，以及以何频率进行清除。请参阅[应用程序分类视图数据清除](#) (p. 220)。

## 事务采样

Introscope 使用称为 *事务采样* 的技术来为应用程序分类视图显示提供数据。在某个代理启动后，默认情况下，Introscope 采用前一百个事务来绘制前端或业务事务及其依赖关系的初始视图。随后，它逐渐减少采样的事务数目，直至达到仅使用每第十个事务为视图提供持续的数据支持这样一个级别。此模式针对每一万个事务重复一次。

您可以通过在 *IntroscopeAgent.profile* 中编辑以下属性来调整采样率：

- `introscope.agent.tracer.sampling.maxrate`
- `introscope.agent.tracer.sampling.initial.period`
- `introscope.agent.tracer.sampling.reset.period`

有关在 *IntroscopeAgent.profile* 中编辑属性的信息，请参阅《CA APM Java 代理实施指南》或《CA APM .NET 代理实施指南》（具体取决于您的环境）。

注意，调整这些属性来增大支持视图显示的事务数可能会影响开销。

## 配置视图元素老化

在连接的数据老化或从 APM 数据库被清除时，代理将重新发现前端和业务服务及其依存关系。Workstation 在应用程序分类视图上显示此数据。

在允许代理收集应用程序分类视图数据后，您可以配置代理执行此数据收集的频率。例如，您可以配置代理以收集应用程序分类视图数据：

- 如果环境频繁变动，则每 24 小时一次。
- 如果环境变动没那么频繁，则每星期一次。

您还可以配置企业管理器在视图中提供数据的时间段。例如，由代理发现的数据可以按星期或月显示。时间段基于两个分类视图时间范围属性：“老化时间”和“窗口时间”。

老化是应用程序分类视图元素的一个特征。当 CA Introscope 不再接收前端或业务事务的数据时，视图元素就会老化。老化时间是 Workstation 继续在应用程序分类视图中显示该元素的时间。此时间过期后，元素将会从代理缓存中删除，且元素在应用程序分类视图中显示为已老化状态。老化时间在 `introscope.apm.data.agingTime` 属性中进行设置。默认值为一天。

时段是在正在老化的元素从视图中完全消失之前，Workstation 显示该元素的时间量。该选项是在 `introscope.apm.data.timeWindow` 属性中设置的。默认值为三天。



例如，在使用上述默认设置的情况下：

ApplicationA 是应用程序分类视图中的前端以及与 ApplicationB 的依存关系。代理继续报告 ApplicationB 的数据，ApplicationB 正常显示在视图中。当停止从 ApplicationB 报告数据时，时钟同时对老化时间和窗口时间开始计时。一天后，ApplicationB 的图节点将显示为老化状态。三天后，ApplicationB 视图节点从视图中消失。

注意事项：

- timeWindow 包括 agingTime 时段。
- 如果将 timeWindow 和 agingTime 设置为同样的持续时间，则视图元素不会显示为老化状态。timeWindow 时段结束时，它们会消失。
- 如果您将 timeWindow 设置为大于 agingTime 的值，则已老化的视图元素将在 agingTime 时段结束时消失。
- 请根据您的组织添加和修改应用程序的频率为 agingTime 和 timeWindow 选择合适的值。该值可以增加或减少代理和企业经理的开销。如果您设置了较低的值，那么分类视图将实时地显示应用程序的依存关系。如果您设置了较高的值，那么分类视图将显示实时性稍差的应用程序依存关系。

**重要信息！** 在群集环境中，对 agingTime 或 timeWindow 默认属性值所做的任何更改也必须应用于 MOM，以及所有收集器。

请执行以下步骤：

1. 打开 <企业经理主目录>/config 目录中的 IntroscopeEnterpriseManager.properties 文件。
2. 如果您要更改 introscope.apm.data.agingTime 的值：
  - a. 停止代理。
  - b. 关闭企业经理。

**重要信息！** 如果您更改 introscope.apm.data.agingTime 属性的值，请参阅 [“减小应用程序分类视图老化时间设置带来的影响 \(p. 218\)”](#)。

3. 配置 introscope.apm.data.agingTime 属性。默认值为一天。该值不能少于 1 分钟。
4. 配置属性 introscope.apm.data.timeWindow。默认值为三天。该值不能少于 1 分钟。
5. 保存并关闭 IntroscopeEnterpriseManager.properties 文件。

6. 如果您更改了 `introscope.apm.data.agingTime` 属性，请重新启动代理。
7. 重新启动企业管理器。
8. 在 `<企业管理器主目录>/logs` 目录中查看分类视图数据老化属性的企业管理器日志文件消息。例如：

```
11/23/09 12:02:13 PM PST [INFO] [Manager] [ The APM Data property :
introscope.apm.data.agingTime set to value : [ PropertywithTimeunit : 1 Min]]
```

### 减小应用程序分类视图老化时间设置带来的影响

如果您打算在 `IntroscopeEnterpriseManager.properties` 文件中减小属性 `introscope.apm.data.agingTime` 的值，CA Technologies 建议您清除应用程序分类视图数据，以避免对历史数据造成意外影响。减小老化时间意味着较小的数据示例将显示在视图显示中，并且可能会因代理将数据报告给企业管理器的方式而基于 APM 数据库中的数据出现误导性显示。从数据库清除数据可防止此问题。

要清除数据，您必须使用 PostgreSQL 客户端。可以从 PostgreSQL 网站 <http://www.pgadmin.org> 下载此类客户端。

#### 使用 PostgreSQL 客户端来清除数据库：

- 执行以下 SQL 语句：

```
truncate apm_edge;
```

增大属性 `introscope.apm.data.agingTime` 的值没有此类意外影响。仅当您希望减小该属性的值时才需要清除数据库。

## 会老化的属性如何影响历史视图

通过应用程序分类地图查看历史数据时，请记住以下概念：

- 不管您如何设置历史时段的起点和终点，显示在应用程序分类地图上的数据的时间跨度始终至少是在 *introscope.apm.data.timeWindow* 属性中设置的跨度。例如：
  - 如果您将历史时段的开始和结束日期设置为 10 天的跨度，但 *introscope.apm.data.timeWindow* 设置为 3 天，则分类地图将显示整个 10 天时间跨度的数据。
  - 如果您将历史时段的开始和结束日期设置为 2 天的跨度，但 *introscope.apm.data.timeWindow* 设置为 3 天，则地图将仍然显示 3 天的数据，为期 3 天的时段与为期 2 天的时段结束时间相同。*introscope.apm.data.timeWindow* 属性设置的时段始终是分类地图显示的最短时段，即使手动设置了更短的历史时段也是如此。
- 地图元素的老化行为将遵循 *introscope.apm.data.agingTime* 属性中设置的时段，好像老化时间是发生在历史时间窗口的末尾一样。例如：
  - 如果 *introscope.apm.data.agingTime* 设置为 1 天，并且您的历史时段设置为 10 天，则如果在该时段的最后一 (1) 天没有代理报告该元素，则该地图元素将显示为老化状态。

## 应用程序分类地图数据限定

为了控制应用程序分类地图的数据流以确保良好的性能，Introscope 使用 *introscope.apm.query.max.results* 属性（可在 *APMEnterpriseManager.properties* 中找到）设置的阈值来限制工作站尝试在地图中显示的数据量。在选择一个树节点或试图展开将超过该阈值的地图元素时，将出现一条消息，指出“地图太大而不能显示”。您可以通过调整属性值来调整该阈值。

**注意：**调整 *introscope.apm.query.max.results* 属性的值可能会影响工作站性能。

有关此属性的更多信息，请参阅 [introscope.apm.query.max.results](#) (p. 426)。

### 编辑应用程序分类地图显示阈值：

1. 打开 *<EM\_Home>/config* 目录中的 *APMEnterpriseManager.properties* 文件。
2. 关闭企业管理器。
3. 查找 *introscope.apm.query.max.results* 属性并调整其值。

4. 保存并关闭 *APMEnterpriseManager.properties* 文件。
5. 重新启动企业管理器。

## 配置应用程序分类视图数据清除

APM 数据库中的应用程序分类视图数据会随着时间的推移而增长。APM 数据库中的数据过多可能会影响企业管理器对应用程序分类视图数据的检索，以及 Workstation 和企业管理器的性能。您可以清除应用程序分类视图数据，以避免在 APM 数据库中收集过多的分类视图数据。

**重要信息！** 如果在 APM 数据库上启用应用程序分类视图数据清理，仅为群集中的一个企业管理器配置该设置。然而，建议在 MOM 上启用应用程序分类视图数据清理。

您可以配置在将视图数据清除之前它在数据库中保留的时间，以及您希望清除操作发生的频率。视图数据清除是由一个排定程序控制的，该排定程序可以配置为每日、每周或每月清除一次数据。

**重要信息！** 无法为应用程序分类数据清除操作配置收集器。如果将收集器的 *introscope.apm.pruning.enabled* 属性设置为 *true*，则会返回错误。

如果清除应用程序分类视图数据时用户正在查看视图，则清除的数据仍保留在视图上，直至用户更改视图时间范围（这将导致视图重绘）。

如果您允许多个企业管理器清理数据库，多个清理进程会争用数据库访问并导致数据库死锁。

**请执行以下步骤：**

1. 打开 <企业管理器主目录>/config 目录中的 *IntroscopeEnterpriseManager.properties* 文件。
2. 关闭企业管理器。
3. 验证 *introscope.apm.pruning.enabled* 属性是否设置为 *true*。

此属性使代理能够清理应用程序分类视图数据。

如果将 *introscope.apm.pruning.enabled* 从 *false* 重置为 *true*，请重新启动企业管理器以使此属性生效。

## 4. (可选) 配置以下属性:

**注意:** 要管理您的环境中应用程序分类视图数据的卷, 请适当降低 `introscope.apm.data.preserving.time` 属性的值, 否则会显示异常。要防止出现异常, 请确认在安装 APM SOI 连接器之前, 您的环境符合应用程序使用情况。如果您仍然看到异常, 请增加 `APMEnterpriseManager.properties` 文件的 `introscope.apm.query.max.results` 属性的值。

- `introscope.apm.data.preserving.time`
- `introscope.apm.pruning.cron.trigger.expression`

- a. 配置 `introscope.apm.data.preserving.time` 属性, 它控制应用程序分类视图数据存储在 APM 数据库中的时间。比保留时间值久的分类视图数据将被视为已老化, 可以进行清理。默认值为 365 天。

清理期间, 将删除比 `introscope.apm.data.preserving.time` 与 `Introscope.apm.data.agingTime` 值的总和早的分类视图数据。例如, 如果 `introscope.apm.data.preserving.time` 值为 30 天, `introscope.apm.data.agingTime` 值为 1 天, 则会删除  $30 + 1 = 31$  天前的视图数据。

根据您的组织添加和修改应用程序的频率来更新值, 添加和修改应用程序会将应用程序分类视图数据添加到 APM 数据库中。有关详细信息, 请参阅 [introscope.apm.data.preserving.time](#) (p. 414)。默认值为 365 天。

- b. 配置 `introscope.apm.pruning.cron.trigger.expression` 属性, 此属性排定从 APM 数据库中清理已老化的应用程序分类视图数据的频率。默认值为每天上午 6 点。

根据您的组织添加和修改应用程序的频率来更新值, 添加和修改应用程序会将应用程序分类视图数据添加到 APM 数据库中。有关详细信息, 请参阅 [introscope.apm.pruning.cron.trigger.expression](#) (p. 415)。

5. 保存并关闭 `IntroscopeEnterpriseManager.properties` 文件。

## 6. 重新启动企业管理器。

企业管理器启动时, 您可以转到 `<EM_Home>/logs`, 查看与视图数据清理属性有关的企业管理器日志文件消息。例如:

```
11/23/09 12:02:13 PM PST [INFO] [Manager] [ The APM Data property :
introscope.apm.pruning.enabled set to value : true]
11/23/09 12:02:13 PM PST [INFO] [Manager] [ The APM Data property :
introscope.apm.pruning.cron.trigger.expression set to value : 0 0 6 * * ?]
```

## 在应用程序分类视图对象中配置过时时间

CA APM 使用术语 *边线* 和 *顶点* 指代应用程序分类视图对象以及这些对象之间的关系。APM 数据库存储有关这些对象的数据。

随着时间的推移，当企业管理器与监控的应用程序之间的连接丢失时，边线对象会根据两个因素被标记为“过时”：

- 属性 `introscope.apm.data.obsolete.time` 的值
- 如下表所述的规则

如果边线对象过时，所有未应用于任何其他的活动边线对象的关联对象将归类为 *过时*。应用程序分类视图将与这些过时的对象有关的元素显示为“灰色”，以清楚表明他们代表非最新的旧数据。

这些“过时”对象仍存在于 APM 数据库中，不会自动删除。这些对象仅在发生“应用程序分类视图清理”进程时，基于为清理设置的属性而被删除。“清理”存储过程会根据清理规则实际删除对象，这一点不同于“过时”规则。有关清理的详细信息，请参阅“[Pruning SmartStor Metadata](#) (p. 71)”。

### 应用程序分类视图对象老化的规则

| 对象                                  | 条件   |
|-------------------------------------|--|
| 边线<br>(数据库表 <code>apm_edge</code> ) | 当边线的更新日期比 <code>introscope.apm.data.obsolete.time</code> 属性的值旧时，边线被认为是过时的。 |
| 顶点 (数据库表 <code>apm_vertex</code> )  | 如果应用程序分类视图中只有过时边线（而没有其他边线）参考某顶点，该顶点就被认为是过时的。                               |
| 所有者 (数据库表 <code>apm_owner</code> )  | 如果应用程序分类视图中只有过时边线（而没有其他边线）参考某所有者，该所有者就被认为是过时的。                             |
| 代理 (数据库表 <code>apm_agent</code> )   | 如果应用程序分类视图中只有过时顶点参考某代理，该代理就被认为是过时的。  |

## 应用程序分类视图时间老化属性

您可以通过为应用程序分类视图配置“时间老化”属性，从数据库返回对过时对象的请求。如果未配置时间，那么任何指向时期 (`introscope.apm.data.preserving.time + introscope.apm.data.agingTime - introscope.apm.data.obsolete.time`) 之内某时间点的请求可以将对象指定为过时。

### 默认值为：

- `introscope.apm.data.preserving.time`  
默认值：365 DAYS
- `introscope.apm.data.agingTime`  
默认值：1 DAY
- `introscope.apm.data.obsolete.time`  
默认：300 DAYS

**重要信息！** 在群集环境中，对 `agingTime` 或 `timeWindow` 默认属性值所做的任何更改也必须应用于 MOM，以及所有收集器。

### 示例

要检索关于过时对象的信息，请在 11 月 1 日 0800h 和 1500h 以及 11 月 2 日 1000h 运行查询 Web 服务 API。此查询对每个请求提供以下结果：

#### 获取 11 月 1 日 8:00 的过时对象

确定比 11 月 1 日 8:00 早 300 天的过时对象。不会返回早于 `introscope.apm.data.preserving.time + introscope.apm.data.agingTime` 的任何对象。

#### 获取从 11 月 1 日 8:00 至 11 月 1 日 15:00 的过时对象

从 11 月 1 日 8:00 和 11 月 1 日 15:00 这两个值中减去 300 DAYS 的 `introscope.apm.data.obsolete.time` 值，确定 11 月 1 日 8:00 到 11 月 1 日 15:00 之间的过时对象。不会返回早于 `introscope.apm.data.preserving.time + introscope.apm.data.agingTime` 的对象。

#### 获取从 11 月 1 日 15:00 至 11 月 2 日 10:00 的过时对象

从 11 月 1 日 15:00 和 11 月 2 日 10:00 这两个值中减去 300 DAYS 的 `introscope.apm.data.obsolete.time` 值，确定 11 月 1 日 15:00 到 11 月 2 日 10:00 之间的过时对象。不会返回早于 `introscope.apm.data.preserving.time + introscope.apm.data.agingTime` 的对象。

## 配置应用程序分类视图时间老化属性

系统会基于 `introscope.apm.data.obsolete.time` 属性将应用程序分类视图对象标记为过时。如果 `introscope.apm.data.obsolete.time` 使用 300 DAYS 的默认值，那么早于 300 天的对象会过时。

请执行以下步骤：

1. 关闭 CA 企业管理器。
2. 打开 `<企业管理器主目录>/config` 目录中的 `IntroscopeEnterpriseManager.properties` 文件。
3. 确认 `introscope.apm.data.obsolete.time` 属性已取消注释，并且设置了不同于 300 天默认值的其他值。

指定 HOURS 或 DAYS；最低值是 24 小时或 1 天。

4. 保存并关闭 `IntroscopeEnterpriseManager.properties` 文件。
5. 重新启动企业管理器。

配置过时时间属性。

6. 在 `<企业管理器主目录>/logs` 目录中查看消息日志。例如：

```
10/19/12 12:02:13 PM EST [INFO] [Manager] [ The APM Data property:
introscope.apm.data.obsolete.timeset to value : 2 DAYS]
```

**注意：**比该值集旧的对象无法报告，因为它们已从 APM 数据库被实际删除。



# 第 15 章：配置 APM 以加载 Catalyst 数据

---

本章介绍了如何配置 CA APM 以加载来自 CA Catalyst 的数据。

此部分包含以下主题：

[配置 CA APM 以加载 CA Catalyst 数据](#) (p. 225)

[配置 CatalystPolicy.xml 文件](#) (p. 226)

## 配置 CA APM 以加载 CA Catalyst 数据

如果要配置 *Catalyst.properties* 文件，可以将数据从 CA Catalyst 加载到 CA APM 中，对其进行处理，然后在 Workstation 中进行查看。

请执行以下步骤：

1. 打开位于 `<EM_Home>/config` 目录中的 *Catalyst.properties* 文件。
2. 关闭企业管理器。
3. 编辑以下必需属性：

- *catalyst.host*=<输入 CA Catalyst 闲置 API 位置>
- *catalyst.protocol* = <输入 http 或 http 连接>
- *catalyst.port* = <输入 CA Catalyst 端口号>
- *catalyst.login* =<输入 CA Catalyst 用户名>
- *catalyst.password* =<输入 CA Catalyst 密码>

**注意：**设置 *catalyst.login* 和 *catalyst.password* 属性可允许企业管理器登录到 CA Catalyst。重新启动（请参阅此过程中的最后一步）后，企业管理器会使用基于密码的加密 (PBE) 通过 MD5 和数据加密标准 (DES) 算法来加密 Catalyst 密码。

- *catalyst.rest.entrypoint* = /ssaweb/search
4. （可选）设置 CA Catalyst 报警筛选属性。
  5. 保存并关闭 *Catalyst.properties* 文件。
  6. （可选）打开 `<EM_Home>/config` 目录中的 *Catalyst.Policy.xml* 文件，并配置实体报警关联的规则。
  7. 保存并关闭 *Catalyst.Policy.xml* 文件。
  8. 重新启动企业管理器。

详细信息:

[配置 CatalystPolicy.xml 文件](#) (p. 226)

[Catalyst.properties](#) (p. 442)

## 配置 CatalystPolicy.xml 文件

*CatalystPolicy.xml* 文件是可选配置, 通过连接器为基于策略的配置提供了最大的灵活性。*CatalystPolicy.xml* 文件可用于定义规则, 如 USM 实体、关联的实体列表和关联的关系列表。这些配置可根据定义的规则来限定任何给定实体上的报警搜索。

下面是 XML 文件结构的一个示例:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<policy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="policy0.1.xsd">
  <entity name="ComputerSystem" alertable="true">
    <include_entities>Processor Memory File Port</include_entities>
    <include_relations>IsComposedOf HasMember</include_relations>
  </entity>
  <entity name="Database" alertable="true">
    <include_entities>Tablespace</include_entities>
    <include_relations>IsManagerFor</include_relations>
  </entity>
  <entity name="DatabaseInstance" alertable="true">
    <include_entities>Tablespace</include_entities>
    <include_relations>IsManagerFor</include_relations>
  </entity>
  <entity name="Group" alertable="false">
    <include_entities>ComputerSystem VirtualSystem</include_entities>
    <include_relations>HasMember</include_relations>
  </entity>
</policy>
```

详细信息:

[配置 CA APM 以加载 CA Catalyst 数据](#) (p. 225)

[Catalyst.properties](#) (p. 442)

## 第 16 章： CA CEM 简介

---

CA CEM 监控您用户的事务，以便在数据中心隔离问题的原因。CA CEM 度量事务的性能和质量、标识缺陷和差异，并且量化对用户和业务的影响。通过主动检测降级事务响应时间的趋势并提供各种可操作的报告，CA CEM 使您能够在问题发生之前或不遵从服务级别协议 (SLA) 之前采取措施。

此部分包含以下主题：

[访问 CEM 控制台和设置页面](#) (p. 227)

[CA CEM 管理员职责](#) (p. 229)

### 访问 CEM 控制台和设置页面

可以从任何安装有 Web 浏览器的计算机设置和管理 CA CEM。

本主题介绍了 CA CEM 的界面及其访问方式：

- [访问 CEM 控制台](#) (p. 227)
- [访问 TIM 的 Wily 系统设置页面](#) (p. 228)
- [从 CEM 控制台访问 TIM](#) (p. 229)

### 访问 CEM 控制台

可以通过任何安装有 Web 浏览器的计算机来设置和管理业务应用程序、业务服务以及事务定义。

CEM 控制台是 CA CEM 的主用户界面。管理员可以使用该控制台设置和配置 CA CEM，包括事务记录和创建事务定义。分析人员可以使用该控制台生成和查看报告。

如果您是管理员，CEM 控制台将提供其他菜单选项。此外，如果未启用任何 TIM，将不会显示某些 CA CEM 链接。

（如果未启用任何 TIM，将不会显示“工具”和“CA CEM”链接。）

除非另有说明，否则本指南假设您正在以管理员身份使用 CEM 控制台。

在群集环境中，CEM 控制台位于管理器的管理器 (MOM) 上。

### 请执行以下步骤：

1. 打开 Web 浏览器并键入以下地址：

`http://<IP 地址>:8081/wily`

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/wily`

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

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`，可以进行更改。

2. 输入用户名和密码。

CA CEM 管理员的默认用户名为 *cemadmin*。

此时将出现 CEM 控制台。

有关安全性和登录的信息，请参阅《CA APM 安全指南》。

## 对登录到 CA CEM 进行故障排除

### 症状：

如果无法登录到 CA CEM，请验证是否在浏览器上启用了活动脚本。

如果禁用活动脚本，在 CA CEM 登录页面单击“登录”时，您将重定向到“CEM 控制台”/“上一步”页面中。即使已正确输入用户名和密码，仍会发生该问题。

### 解决方案：

要启用活动脚本，请参阅浏览器的用户文档。例如，在 Internet Explorer 8 中，设置位于“Internet 选项”>“安全”>“自定义级别”>“脚本”>“活动脚本”下。

## 访问 TIM 系统设置页面

通过 TIM 的“系统设置”页面，可以访问各种配置和状态页面。管理员通常使用这些页面来查看状态信息或进行故障排除。

请执行以下步骤：

1. 打开 Web 浏览器，然后输入以下地址，其中 *<IP\_Address>* 是 TIM IP 地址或 DNS 名称：

```
http://<IP_Address>/cgi-bin/wily/system/index
```

例如：

```
http://192.168.1.54/cgi-bin/wily/system/index
```

```
http://cem.company.com/cgi-bin/wily/system/index
```

要使用 DNS 名称，您的 DNS 管理员必须已经配置了 DNS 名称。

2. 输入用户名和密码。  
“系统设置”页面的默认用户名为 *admin*。  
此时将显示“系统设置”页面。

## 从 CEM 控制台访问 TIM

如果您知道 TIM 的 IP 地址和路径，可以通过“系统设置”页面访问“TIM 设置”页面。但如果已打开 CEM 控制台，则可以通过控制台访问“TIM 设置”页面。

请执行以下步骤：

1. 在管理员控制台中，选择“设置” > “监视器”。
2. 单击 TIM 的 IP 地址（最右列）。
3. 在“系统设置”页面上输入用户名 *admin* 和密码。  
此时将显示“TIM 设置”页面。

## CA CEM 管理员职责

每个站点 CA CEM 管理员的职责都不相同，具体取决于环境复杂性、集成类型、用户数量、支持资源，以及 CA CEM 监控的应用程序的增长率。

- [每日任务](#) (p. 230)
- [每周任务](#) (p. 230)
- [每月任务](#) (p. 231)
- [每季度任务](#) (p. 231)

## 每日任务

以下是 CA CEM 管理员的典型每日任务：

- 执行和验证每日备份。
- 检查突发事件和缺陷（若有）。使用 Introscope 解决问题。
- 将发现的 CA CEM 问题报告给相应的组。
- 检查 TIM 和 IntroscopeEnterpriseManager 日志。
- 在线或接收电子邮件通知后，检查系统事件。例如，已丢弃缺陷。（请参阅[查看](#) (p. 294)CA CEM [事件](#) (p. 294)和[接收事件的电子邮件通知](#) (p. 294)。）
- 检查 TIM 的运行状况。（请参阅[检查 TIM 计算机的运行状况](#) (p. 296)。）
- 使用 Introscope Workstation 检查 CA CEM 在企业管理器中的运行状况。

## 每周任务

以下是 CA CEM 管理员的典型每周任务：

- 测试备份和还原过程。
- 测试与 CA SiteMinder、CA NSM、CA Service Desk 等的集成是否如预期一样工作。例如，是否可在 SiteMinder Web 代理上使用单点登录？
- 在站外保存 CA CEM 配置和备份文件的副本。
- 检查 Embedded Entitlements Manager 中的 CA CEM 管理员列表，找出不需要的管理员。
- 检查 CA CEM 审核日志，找出意外或未授权的更改。
- 检查 CA CEM CPU、磁盘和系统使用率。（请参阅[检查 TIM 计算机的运行状况](#) (p. 296)。）
- 适当关闭已解决的或旧的突发事件。
- 检查报告的准确性和趋势。
- 检查是否将如预期一样创建和分发电子邮件报告。
- 在 Introscope 中检查实时业务事务度量标准和自定义显示板。
- 检查集成日志，如 CA Service Desk 和 CA SiteMinder 的日志。
- 检查证据收集日志。（请参阅[为突发事件设置业务影响并收集证据](#) (p. 264)。）

## 每月任务

以下是 CA CEM 管理员的典型每月任务：

- 检查故障切换过程（如果已安装）。
- 清除旧的/不需要的用户和用户组。
- 检查是否需要定义新的业务服务/事务等。
- 检查是否需要修改业务规范设置。
- 检查是否需要调整基准或 SLA 设置。
- 检查每月报告的准确性和趋势。
- 检查已启用的事务和业务事务统计信息；禁用不再需要监控的事务的定义。（有关管理事务定义的信息，请参阅《CA APM 事务定义指南》。）
- 如果已启用 HTTP 分析程序插件，请检查其操作。插件是否满足预期需求？是否还有其他需要满足的要求？自上次 JAR 文件更新以来，性能是否有所降低？（请参阅《CA APM 事务定义指南》。）

## 每季度任务

以下是 CA CEM 管理员的典型每季度或每年任务：

- 检查 CA CEM 体系结构的性能、可扩展性、故障切换、地理分布以及其他因素。
- 确定 CA CEM 自定义或集成是否需要 CA CEM 专业服务。
- 对下一版本的 CA CEM 进行 Beta 测试（如果适用），找出潜在问题和新增功能。
- 检查用户组定义。（例如，IP 子网用户组规则是否需要修改？）





# 第 17 章： CA CEM 联网备选方案

---

此部分包含以下主题：

[关于 CA CEM 网络选项](#) (p. 233)

[关于监控网络通信](#) (p. 233)

[关于 CA CEM 插入位置](#) (p. 235)

[从浏览器连接到企业管理器](#) (p. 238)

[IPv6 和 CA CEM](#) (p. 238)

## 关于 CA CEM 网络选项

您的网络中有多个位置可用于放置 CA CEM，并有多种将系统连接到网络的备选方式。本章描述这些选项。

TIM 和企业管理器驻留在单独的硬件上。主要注意事项是与向企业管理器（收集器和管理器的管理器 (MOM)）报告的 TIM 的连接。

有多种供您放置 TIM 的位置选项，在[关于 CA CEM 插入位置](#) (p. 235)中对这些选项进行了介绍。TIM 的位置确定可以收集的信息。

TIM 的首选插入点逻辑上位于网络负载均衡器与 Web 服务器聚合交换机之间；如果未使用聚合交换机，则在负载均衡器与 Web 服务器之间。有关详细信息，请参阅[位于聚合交换机与网络负载均衡器之间](#) (p. 237)。

在所选位置安装 TIM 时，还必须选择一种将其连接到您的网络的方法。

## 关于监控网络通信

TIM 通过监控接口读取网络中的流量，这些监控接口可以连接到镜像端口或网络分流器。

以下部分描述使用镜像端口向 TIM 转发数据包与使用网络分流器向 TIM 转发数据包之间的权衡。

- [使用网络分流器](#) (p. 234)
- [使用镜像端口](#) (p. 234)

## 使用网络分流器

网络分流器是直接于基础架构电缆相连的硬件设备，用于创建数据包副本并将其转发至一个或多个目标。分流器在物理层与基础架构捆绑，不使用路由器或交换机上的资源。为了插入分流器，分流器要求暂时挂起连接。

分流器对网络延迟没有任何影响。许多分流器在两个物理接口上分别转发传输的和接收的流量，这要求 TIM 中存在两个物理接口。这些数据流必须由 TIM 合并。以这种方式合并数据流会对 TIM 的性能造成轻微影响。一些分流器是全双工的，不需要其他接口或者在 TIM 上合并。

分流器是纯传输设备，因此可能比镜像端口更安全。分流器的另一个优点是配置相对简单。因为分流器是内嵌设备，所以出现故障会干扰网络操作，或需要停机来替换有缺陷的分流器（无源分流器除外）。分流器的先进技术大大减少了出现故障的概率。

## 使用镜像端口

镜像端口（在 Cisco 术语中为 SPAN 端口）是网络路由器和交换机的软件功能。在现代交换机（如 Cisco 的 6500 系列交换机）中，启用 SPAN 端口不会对交换机性能造成影响。镜像端口通常用来附加网络故障排除设备，如协议分析程序。交换机支持的镜像端口的数目有限，因此在某些情况下网络工程师反对将设备永久附加到这些维护端口。

因为镜像端口是路由器或交换机的软件功能，所以它们不需要更改基础架构，并且破坏性比分流器小。与需要额外花费资金的分流器不同，已经部署的交换机通常支持镜像端口，无需额外开销。

镜像端口对网络延迟没有任何影响。镜像端口通常在转发之前组合发送与接收的流量，以便减少 TIM 上所需的接口。TIM 不需要合并多个接口的数据流，因此使用该配置性能有所提高。

虽然错误的配置更改可能将镜像端口配置成双向交换机端口，但是镜像端口在大多数情况下是纯传输端口。因此，有时认为镜像端口不如分流器安全。根据 TIM 软件的设计，它不会在监控端口上传输数据，从而确保 TIM 不会引入任何安全风险。

**注意：**如果最终用户流量通过两台不同的交换机进入应用程序，那么来自两台交换机的流量有可能被镜像到同一个 TIM。您需要购买和部署网卡（多端口 NIC）来执行此操作。有关网卡支持的信息，请参阅《CA APM 兼容性指南》。

## 关于 CA CEM 插入位置

TIM 在基础架构中的插入位置影响所收集的信息。

TIM 通过监控接口读取网络通信。正如在上一部分中所述，监控接口可以连接到镜像端口或网络分路。在这两种情况中，TIM 接收所需数据包的副本，进行分析，然后丢弃。TIM 不在监控端口上传输数据。流量单向传入 TIM，并且将 TIM 配置为仅从监控端口中接收数据包。

在典型的大型企业网络基础架构中，有多个位置可以插入 TIM 监控端口。该图说明了不同的插入位置。

**注意：**大多数环境使用冗余的基础架构。然而为简单起见，仅在该图中显示一条路径。



（从左向右读图）数据包通过 Internet 路由器进入企业。插入位置 A 位于路由器外，介于 Internet 和路由器之间。

该路由器通常将流量转发至防火墙，插入位置 B 位于路由器和该防火墙之间。防火墙可以检测入站和出站的流量，并且根据企业的安全策略阻止或接受流量。防火墙还能执行网络地址转换 (NAT)，以防企业的网络连接设备直接连接到 Internet。

**注意：**在某些情况下，聚合交换机和网络负载均衡器位于相同的设备中。

插入位置 C 位于防火墙和聚合交换机/网络负载均衡器之间。可接受的流量从防火墙转发至聚合交换机/网络负载均衡器。在许多情况下，聚合交换机/网络负载均衡器可以终止 SSL 会话，并实例化虚拟 IP 地址 (VIP) 供客户连接。许多聚合交换机/网络负载均衡器充当代理，终止客户端的连接并代表客户端建立到 Web 服务器的连接。一些聚合交换机/网络负载均衡器建立并使用到 Web 服务器的永久性连接，以减轻 Web 服务器上的负载。

在许多情况下，聚合交换机将数据包转发至网络负载均衡器。插入位置 D 位于聚合交换机和网络负载均衡器之间。

最后，Web 服务器连接到聚合交换机，或直接连接到网络负载均衡器。插入位置 E 位于 Web 服务器前面，要么介于聚合交换机和 Web 服务器之间，要么介于网络负载均衡器和 Web 服务器之间。

数据包按反向路径离开企业，以相反顺序通过每个插入位置。（数据包也可能经由一条路径进入，再经由另一条路径退出（即采用三角形路径）。或者数据包可以离开 Web 服务器，直接进入 Internet。

## 位于 Internet 和 Internet 路由器之间

插入位置 A 位于 Internet 和 Internet 路由器之间，总能提供客户端 IP 地址的可见性。



插入位置 A 几乎从不提供服务器的 IP 地址或服务器的 MAC 地址的可见性。CA CEM 在基于排除的关系发现机制中使用 Web 服务器 IP 或 MAC 地址限制收集的证据集，以便提高故障排除速度。没有此信息，将继续收集证据，但是证据集并未减少，而且技术人员必须比在不使用基于排除的发现机制时分析更多信息。

因为 TIM 不使用客户端 IP 地址标识用户，所以使用插入位置 A 的优点非常有限，而且还存在不少缺点。

## 位于 Internet 路由器和防火墙之间

插入位置 B 位于 Internet 路由器和防火墙之间，几乎总能提供客户端 IP 地址的可见性。



插入位置 B 几乎从不提供服务器的 IP 地址或服务器的 MAC 地址的可见性。CA CEM 在基于排除的关系发现机制中使用 Web 服务器 IP 或 MAC 地址限制收集的证据集，以便提高故障排除速度。没有此信息，将继续收集证据，但是证据集并未减少，而且技术人员必须比在不使用基于排除的发现机制时分析更多信息。

因为 TIM 不使用客户端 IP 地址标识用户，所以使用插入位置 B 的优点非常有限，而且还存在不少缺点。

## 位于防火墙和聚合交换机之间

插入位置 C 位于防火墙和聚合交换机之间，几乎总能提供客户端 IP 地址的可见性。插入位置 C 几乎从不提供服务器的 IP 地址的可见性。



因为 TIM 不使用客户端 IP 地址标识用户，所以使用插入位置 C 的优点非常有限，而且还存在不少缺点。在某些环境中，插入位置 C 与插入位置 A 和 B 相比具有一些无足轻重的优点。

## 位于聚合交换机和网络负载均衡器之间

插入位置 D 位于聚合交换机和网络负载均衡器之间，通常提供客户端 IP 地址的可见性。为了执行此操作，如果将网络负载均衡器充当代理，则必须在其中启用“保留源地址”。插入位置 D 几乎总能提供服务器的 IP 地址的可见性。



如果网络负载均衡器使用永久性连接，当 TIM 位于此处时，其中的负载将减少。减少打开的连接能减少负载，该功能很有意义。如果网络负载均衡器代表客户端终止 SSL，并且不重新加密流量，那么几乎在所有情况下都将大量减少 TIM 上的负载。

在某些负载平衡环境中（如 Resonate），可能根据 MAC 地址标识服务器。然而，在许多环境中，返回的服务器 IP 地址和 MAC 地址是网络负载均衡器虚拟 IP 地址 (VIP) 的地址。

因为 TIM 使用服务器 IP 地址收集证据，所以使用插入位置 D 的优点最多，而且几乎没有缺点。插入位置 D 是 TIM 的首选插入位置。

## 位于网络负载均衡器和 Web 服务器之间

插入位置 E 位于网络负载均衡器和 Web 服务器（或服务器）之间，通常提供客户端 IP 地址的可见性。为了执行此操作，如果将网络负载均衡器充当代理，则必须在其中启用“保留源地址”。插入位置 E 几乎总能提供服务器的 IP 地址的可见性。



如果网络负载均衡器使用永久性连接，当 TIM 位于此处时，其中的负载将减少。减少打开的连接能减少负载，该功能很有意义。如果网络负载均衡器代表客户端终止 SSL，并且不重新加密流量，那么几乎在所有情况下都将大量减少 TIM 上的负载。

因为 TIM 使用服务器 IP 地址收集证据，所以使用插入位置 E 有很多优点。然而，插入位置 E 有插入位置 D 没有的一些缺点。因为可能有许多 Web 服务器，所以可能有许多插入位置。这可能导致无法在插入位置 E 使用分流器。

使用端口镜像时，插入位置 D 和插入位置 E 的功能相同。在许多情况下，使用插入位置 E 只需跨接虚拟局域网 (VLAN)。对于插入位置 D，简单的端口镜像可能就足够了。

## 从浏览器连接到企业管理器

默认情况下，允许在浏览器和企业管理器之间进行 HTTP 访问。

然而，可以将对企业管理器的访问限制为只允许 SSL 连接。请参阅《CA APM 安全指南》。

## IPv6 和 CA CEM

本部分简要讨论了 Internet 协议版本 6 (IPv6)、IPv6 网络中的 CA CEM 的计算机设置页面以及 CA CEM 中的 IPv6 地址格式。

- [关于 IPv6](#) (p. 239)
- [CA CEM 中的 IPv6](#) (p. 239)
- [监控 IPv6 网络通信](#) (p. 239)

- [在双协议栈（IPv6 和 IPv4）主机上运行 CA CEM](#) (p. 240)
- [允许的 IPv6 地址格式](#) (p. 241)

## 关于 IPv6

Internet 协议版本 4 (IPv4) 地址预计将在几年内用尽。IPv6 增加了可用的 Internet 地址的数目。

IPv6 地址有 128 位（16 字节）。通常按十六进制编写，用冒号 (:) 分隔每个 16 位组。例如，2001:0db8:30d2:55c9:06ff:e579:5aa4。

相比之下，IPv4 地址有 32 位（4 字节）。通常按十进制编写，用点 (.) 分隔每个字节。例如，172.24.131.197。

## CA CEM 中的 IPv6

CA CEM 中的 IPv6 支持包括两方面：

- 监控 IPv6 网络通信
- 在 IPv6 网络中配置 CA CEM

这二方面彼此独立。例如，可以将 CA CEM 计算机置于 IPv4 网络中，然后监控 IPv6 和 IPv4 网络通信。同样，可以将 CA CEM 计算机置于 IPv6（或双协议栈）网络中，然后监控 IPv6 和 IPv4 网络通信。

## 监控 IPv6 网络通信

CA CEM 支持 IPv4 和 IPv6 地址。在字段中输入 IP 地址或子网掩码时，可以输入 IPv4 或 IPv6 地址。

**监控 IPv6 网络通信：**

- 以监控 IPv4 通信的相同方式设置 CA CEM。根据需要输入 IPv6 地址（和主机名），而非 IPv4 地址（和主机名）。

请参阅[允许的 IPv6 地址格式](#) (p. 241)。

## 在双协议栈（IPv6 和 IPv4）主机上运行 CA CEM

当设置和安装 CA CEM 时，请遵循由 SE 或支持人员提供的说明，或《CA CEM 安装和升级指南》中提供的说明。作为双协议栈主机，IPv4 和 IPv6 地址分配给企业管理器和 TIM 计算机。

**重要信息！** 如果为 TIM 分配了 IPv6 地址，则还必须为运行 TIM 收集服务的企业管理器分配 IPv6 地址。同样，如果 TIM 使用 IPv4 地址，那么运行 TIM 收集服务的企业管理器也必须使用 IPv4 地址。

在 CA CEM 控制台中实施这一重要约束，例如：

- 如果启用的 TIM 使用 IPv6 地址，则无法在使用 IPv4 地址的企业管理器上运行 TIM 收集服务（反之亦然）。
- 如果启用的 TIM 使用 IPv6 地址，则无法使用 IPv4 地址启用 TIM（反之亦然）。
- 如果 TIM 收集服务将导致企业管理器和启用的 TIM 之间的地址类型不匹配，则无法更改运行 TIM 收集服务的企业管理器的 IP 地址。
- 如果 TIM 收集服务将导致企业管理器和启用的 TIM 之间的地址类型不匹配，则无法将 TIM 收集服务移动至其他企业管理器。

如果需要确认、修改，或排除配置故障，请遵循这些过程。

### 在 TIM 上检查或修改 CA CEM 的 IPv6 设置：

1. 访问 TIM 的 Wily 系统设置页面。（[访问 TIM 的 Wily 系统设置页面。](#) (p. 228)）
2. 在“Wily 系统设置”页面中，选择“计算机设置” > “配置 IPv6”。确认已正确分配 IPv6 地址，并且已启用 IPv6。

IPv6 设置页面的注意事项如下：

- 全局范围的 IPv6 地址类似 IPv4 地址。
  - RADV 和 DHCPv6 可将多个全局 IPv6 地址分配给计算机。然而，只能手动分配一个地址。
  - 如果手动分配 IPv6 地址，请使用斜杠符号表示网络前缀的长度。（这类似于为 IPv4 网络指定子网掩码。）
  - “单击禁用”按钮专供故障排除使用。例如，如果无法通过 IPv6 网络与 CA CEM 计算机进行通信，请验证在系统范围内和连接到管理网络 (ethn) 的接口上都启用了 IPv6。
3. 验证是否已正确分配 IPv4 设置：返回“计算机设置”，然后选择“网络设置”。



**更改双协议栈企业管理器的 IP 地址:**

- 请参阅[编辑企业管理器的 IP 地址](#) (p. 249)。

**将浏览器指向 CA CEM 控制台:**

- 如果在控制台的 URL 中使用文本 IP 地址，请使用 [] 符号（方括号）表示 IPv6 地址。

请参阅[允许的 IPv6 地址格式](#) (p. 241)中的路径示例。

## 允许的 IPv6 地址格式

用于 IPv6 地址的格式根据您是在 CEM 控制台中还是在 Wily 系统设置页面中而有所不同:

- CEM 控制台—在 CEM 控制台中输入 IPv6 地址时，无法使用压缩格式，除非用于指定：
  - 子网掩码，其中允许使用压缩格式和斜杠符号
  - “管理” > “记录会话” 页面中的客户端 IP 地址，其中可以使用压缩格式和混合格式。

确保遵循 UI 中给出的示例。

- Wily 系统设置页面—在 Wily 系统设置页面（如 IPv6 设置页面）中，可以使用压缩格式和更长的格式来指定 IPv6 地址。

在 IPv6 设置页面中，必须使用前缀长度（用斜杠与地址分开），而不是子网掩码。

此表列出了 CA CEM 中可接受的 IPv6 地址格式示例。

| IPv6 地址示例  | 格式和说明  |
|--|--|
| <code>3fff:ffff:0ed5:0000:0000:0000:2448:78eb</code> | 标准格式：<br>可在 CA CEM 中的任何位置使用。                               |
| <code>3fff:ffff:ed5:0:0:0:2448:78eb</code>           | 在 16 位组中删除了前导 0：<br>可在 CA CEM 中的任何位置使用。                    |
| <code>3fff:ffff:fed5::2448:78eb</code>               | 压缩格式：<br>不要在 CEM 控制台 UI 中使用斜杠符号，在子网掩码和“管理” > “记录会话” 页面中除外。 |

| IPv6 地址示例                                     | 格式和说明  |
|---|--|
| <i>3fff:ffff:fed5:0::/64</i>                  | 斜杠符号：<br>用于子网掩码（“设置” > “域” > “子网掩码和管理” > “用户组”）和手动 IPv6 地址（“Wily 系统设置” > “计算机设置” > “配置 IPv6”）。 |
| <i>ffff:ffff:ffff:ffff:0:0:0:0</i>            | 子网掩码：<br>用于子网掩码（“设置” > “域” > “子网掩码和管理” > “用户组”）。   |
| <i>2001:0db8:85a3:08d3:0:0:172.31.124.132</i> | IPv4 和 IPv6 混合格式：<br>不要在 CA CEM 中使用，在“管理” > “记录会话”页面中除外。                                       |

此表列出了 CA CEM 中可接受的 IPv6 路径格式示例。

| IPv6 路径示例  | 格式和说明                                 |
|--|---------------------------------------|
| <i>http://cemhost_ipv6:8081/wily</i>                     | CEM 控制台的示例路径，其中主机名定义为 cemhost_ipv6。   |
| <i>http://[2001:db8:85a3:8d3:0:0:370:7348]:8081/wily</i> | CEM 控制台的示例路径，其中企业管理器的 IP 地址是 IPv6 格式。 |

# 第 18 章：管理 CA CEM

---

此部分包含以下主题：

- [CA CEM 管理过程](#) (p. 243)
- [分发企业管理器服务](#) (p. 244)
- [定义 CA CEM 域](#) (p. 253)
- [突发事件成本与业务影响](#) (p. 258)
- [定义与突发事件相关的设置](#) (p. 259)
- [配置 SMTP 服务器设置](#) (p. 268)
- [为新的业务服务设置安全组](#) (p. 270)
- [启用监视器](#) (p. 273)
- [同步监视器](#) (p. 273)
- [查看自上次同步以来的配置更改](#) (p. 274)

## CA CEM 管理过程

列表显示了管理 CA CEM 所涉及的主要任务：

1. 在多个企业管理器之间分发企业管理器服务。请参阅[分发企业管理器服务](#) (p. 244)
2. 定义域，包括用户识别、用户组、事务以及数据保留的设置。请参阅[定义 CA CEM 域](#) (p. 253)
3. 为突发事件生成、业务影响和证据收集、突发事件过期规则以及突发事件电子邮件设置突发事件设置。请参阅[定义与突发事件相关的设置](#) (p. 259)
4. 定义报告和事件通知的电子邮件设置。请参阅[配置 SMTP 服务器设置](#) (p. 268)
5. 为新的业务服务设置默认安全组。请参阅[为新的业务服务设置安全组](#) (p. 270)
6. 启用 TIM— 在设置和禁用 TIM 时需要执行此任务。这将启用收集器和 TIM 之间的通信。请参阅[启用监视器](#) (p. 273)
7. 同步监视器— 将事务和缺陷配置信息发送给 TIM 时，以及让 TIM 开始使用更新的配置监控时，需要执行此任务。  
还需要将与业务服务和事务相关的配置更改发送到 Introscope 代理。请参阅[同步监视器](#) (p. 273)

## 分发企业管理器服务

如果有多个企业管理器 (EM)，即收集器和 MOM，则可以在企业管理器之间分发企业管理器服务。如果不分发服务，所有企业管理器服务将在一个企业管理器上运行；在某些情况下，将无法获得最佳性能。

**注意：**如果系统中只有一个（独立）企业管理器，可以跳过此主题。在只有一个企业管理器的情况下，所有企业管理器服务必须在一个企业管理器上运行。

在多企业管理器环境中启动 CA APM 时，所有企业管理器服务都在第一个收集器上启动。启动所有收集器后，可以将企业管理器服务分配给适合的企业管理器。

下表指明执行企业管理器服务任务的时间。

**注意：**TESS 服务在收集器上而不是 MOM 上运行。

| 如果...              | 请执行这些任务...  |
|--------------------|---|
| 首次设置 CA APM        | <a href="#">分发企业管理器服务</a> (p. 244)<br><a href="#">修改企业管理器配置</a> (p. 249)                            |
| 将企业管理器添加到环境中       | <a href="#">分发企业管理器服务</a> (p. 244)<br><a href="#">修改企业管理器配置</a> (p. 249)                            |
| 在环境中更改企业管理器的 IP 地址 | <a href="#">修改企业管理器配置</a> (p. 249)  |
| 删除环境中的企业管理器        | <a href="#">分发企业管理器服务</a> (p. 244)（要在关闭企业管理器之前从企业管理器中移除企业管理器服务）<br><a href="#">删除企业管理器</a> (p. 251) |

您可以分发以下企业管理器服务：

**注意：**可以在群集中运行每种服务的一个（且只有一个）实例。例如，永远不会同时在两个企业管理器上运行 TIM 收集服务。

#### **数据库清除服务**

删除数据库中的旧数据。

#### **统计聚合服务**

每天聚合一次数据库中的统计信息。默认情况下，聚合在午夜前后进行。有关详细信息，请参阅[关于 CA APM 报告聚合](#) (p. 299)。

#### **TIM 收集服务**

如果没有任何 TIM（即，如果运行的是 Introscope 而不是 CA APM），则该服务的位置无关紧要。

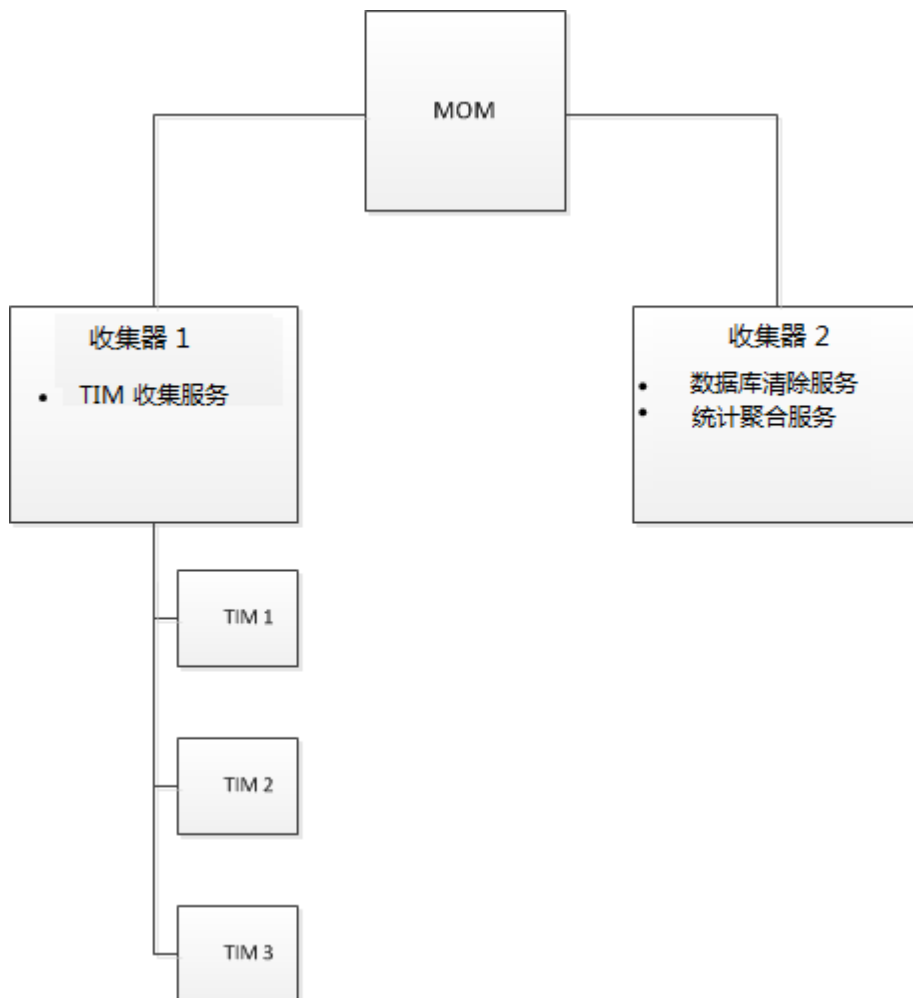
由用于处理 TIM 收集的数据的一组服务组成。包括用于处理登录、缺陷、记录、CA CEM 事件、每小时统计信息、客户体验度量标准以及事务发现的服务。

**注意：** TIM 收集服务是计算密集程度最高的企业管理器服务。

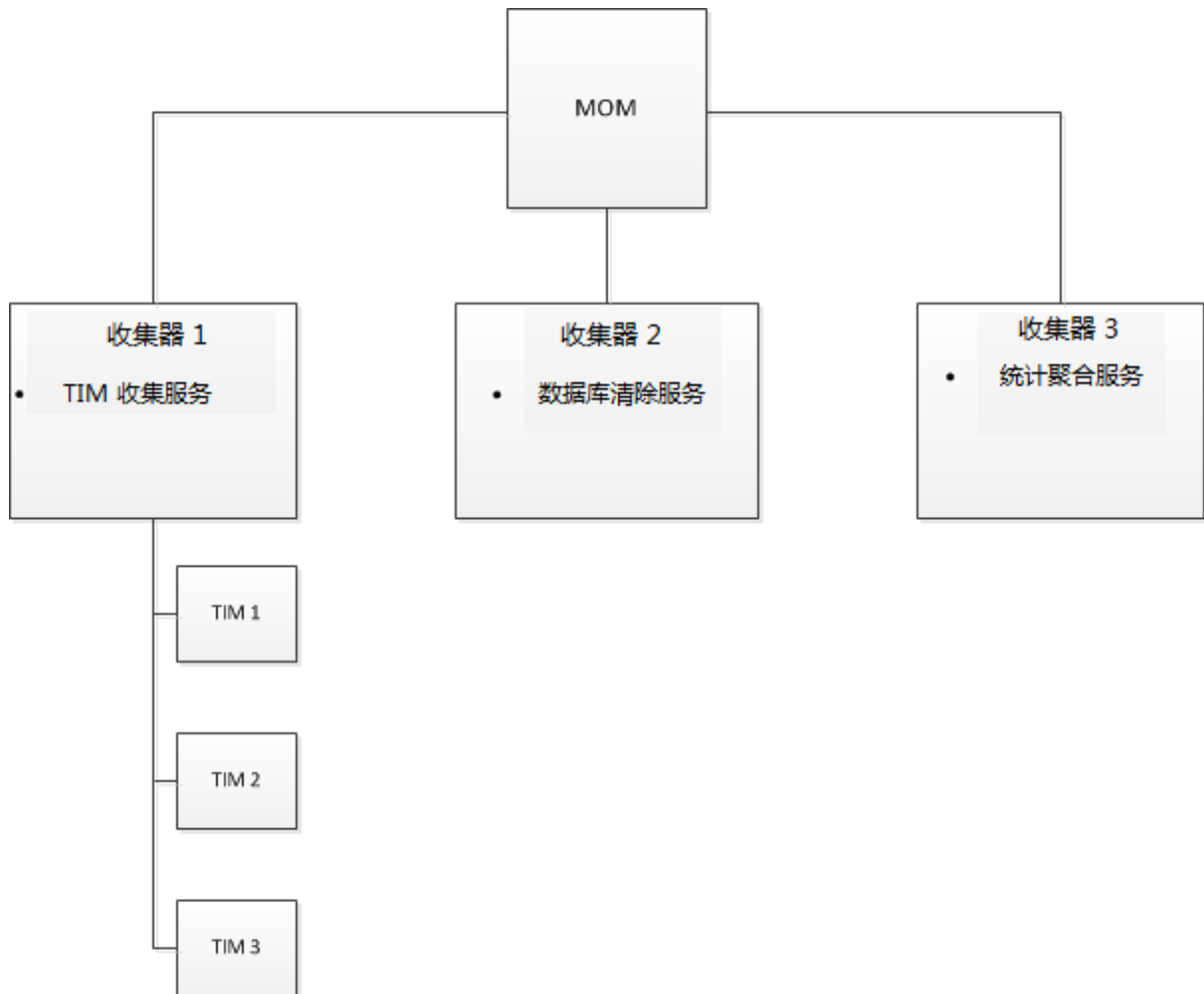
其他企业管理器服务分配给所有企业管理器。因为这些服务无法分发，所以未显示在“服务”页面中。

## 企业管理器服务的典型分布

下图显示了在包含两个收集器的环境中的典型企业管理器服务分布：



下图显示了在包含三个收集器的环境中的典型企业管理器服务分布：



## 在群集环境中分发企业管理器服务

这是在企业管理器之间重新分发企业管理器服务的过程。例如，在第一次启动 CA APM 时以及从系统中添加或删除企业管理器时执行此操作。

**重要信息！** 在关闭企业管理器之前，从企业管理器中删除企业管理器服务。

该过程的目的是在企业管理器之间分配工作负荷。

**注意：** 当 TIM 收集服务移至其他企业管理器时，系统不会处理原始企业管理器上余留的任何未处理数据文件（除非该服务又移回到原始企业管理器）。有关详细信息，请参阅[更改损坏文件的目录位置](#) (p. 510)。

CA Technologies 建议选择非高峰时段重新分发企业管理器服务。在高峰时段关闭和移动服务可能导致处理延迟。

### 在群集环境中分发企业管理器服务：

1. 选择“设置”、“服务”、“服务配置”。

“服务配置”页面显示当前正在运行每种服务的企业管理器的概述。

2. 单击想要分配给不同企业管理器的服务（如数据库清除服务）。
3. 从企业管理器的列表中，选择要分配服务的企业管理器，然后单击“保存”。

群集中的所有企业管理器都显示在列表中。您可以确定企业管理器是在运行还是已关闭。

**注意：** MOM 不显示在列表中。

CA Technologies 建议不要在正在运行 TIM 收集服务的企业管理器中运行防病毒软件，因为防病毒软件会大大降低该服务的运行速度。

4. 重复步骤 2 和 3，直到每个企业管理器服务都在预期的企业管理器上运行为止。
5. 单击“保存”。

## 选择参与实时事务度量标准的 TIM

默认情况下，从所有 TIM 中收集实时事务度量标准数据。但是，可以指定为仅从环境中的某些 TIM 中收集数据。在测试或排除故障时，可能需要执行此操作。

### 请执行以下步骤：

1. 选择“设置”、“服务”。
2. 单击“TIM 收集服务”。
3. 在“TIM 收集服务”菜单中，选择“RTTM 收集服务”（如果尚未选择）。

参与实时事务度量标准的 TIM 在 TIM 列表中标记为已启用。

4. 根据需要在列表选择或清除 TIM。
5. 单击“保存”。



## 选择用于自动事务发现的 TIM

默认情况下，自动事务发现功能运行时，将扫描所有 TIM 的 HTTP 流量。但是，您可以指定只有环境中的某些 TIM 可参与自动事务发现。

当您知道感兴趣的事务仅由某个特定 TIM 访问时，可能会想执行此操作。将事务发现限制到此 TIM，意味着不会在其他 TIM 上产生任何与发现相关的开销。

### 查看或指定哪些 TIM 参与自动事务发现：

1. 选择“设置” > “服务”。
2. 单击“TIM 收集服务”。
3. 在“TIM 收集服务”菜单中，选择“事务发现收集服务”。  
参与事务发现的 TIM 在 TIM 列表中标记为已启用。
4. 根据需要在列表选择或清除 TIM。
5. 单击“保存”。

## 修改企业管理器配置

如果要修改企业管理器的说明或 IP 地址，请遵循这些过程。

### 编辑说明

默认情况下，将说明设置为包括企业管理器的主机名和端口号。

例如，可以对说明进行编辑，在其中添加计算机的资产标签或位置 ID，帮助标识计算机。

### 修改企业管理器的说明：

1. 选择“设置” > “服务” > “EM 配置”。
2. 选择“企业管理器”。
3. 编辑“说明”，然后单击“保存”。

### 编辑企业管理器的 IP 地址

在大多数情况下，将自动在“EM IP 地址”字段中填充企业管理器的正确 IP 地址。

在以下示例中，可能需要编辑企业管理器的 IP 地址：

- 企业管理器计算机包括两个 IP 地址，这是因为它位于两个网络中。“EM 配置”页面显示一个 IP 地址，“TIM 设置”页面显示 TessCollectorIpAddr 或 TessIpAddr 值的另一个地址。要查看“TIM 设置”页面，请参阅可选步骤 6。
- 企业管理器是具有 IPv6 和 IPv4 地址的双协议栈主机。如果启用的 TIM 具有 IPv6 地址，那么运行 TIM 收集服务的企业管理器需要在“EM IP 地址”字段中显示 IPv6 地址。

### 修改企业管理器的 IP 地址：

1. 选择“设置”、“服务”、“EM 配置”。
2. 选择“企业管理器”。
3. 选择备用企业管理器 IP 地址，然后单击“保存”。  
编辑该地址一次之后，如果该 IP 地址再次更改，则必须手工更新。（企业管理器重新启动时，该字段不再自动更新。）
4. 选择“设置”、“监视器”。
5. 禁用和启用所有 TIM：
  - a. 选择 TIM。
  - b. 单击“禁用”。
  - c. 单击“启用”。
6. （可选）如果企业管理器正在运行 TIM 收集服务，请确认启用的 TIM 已经接收到更新的 IP 地址：
  - a. 单击 TIM 的 IP 地址。  
此时将显示“TIM 系统设置”页面。
  - b. 单击“配置 TIM 设置”。
  - c. 确认 TessCollectorIpAddr 和 TessIpAddr 设置正确。不要直接编辑这些设置。

## 删除企业管理器

该过程说明如何从“服务”页面中删除企业管理器。

企业管理器启动后自动显示在“服务”页面中。不过，不会从“服务”页面中自动删除企业管理器的名称。该过程的目的是从“服务”页面中删除未使用的企业管理器的名称。

### 删除企业管理器：

1. 如果企业管理器正在运行任何企业管理器服务，请将服务移动至其他企业管理器。请参阅[分发企业管理器服务](#) (p. 244)。
2. 关闭企业管理器。请参阅《CA APM 管理配置指南》中的“停止企业管理器”主题。
3. 选择“设置” > “服务” > “EM 配置”。
4. 选择“企业管理器”。
5. 单击“删除”。

该企业管理器不再显示在“服务”页面中。

如果以后重新启动该企业管理器，它将再次显示在“服务”页面中。

## 企业管理器服务故障排除

该表提供一些可能有助于解决企业管理器服务中出现的问题的提示。

### 症状：

与服务相关的 CA CEM 事件显示在“事件”页面中：

- TIM 收集服务已停止
- 统计聚合服务已停止
- 数据库清除服务已停止

### 解决方案：

一种企业管理器服务已停止并且需要立即重新启动。

重新启动运行该服务的企业管理器。

### 症状：

似乎没有聚合每日统计信息。

报告未显示每日数据。

**解决方案:**

可能是由于统计聚合服务未正常运行。

检查位于运行统计聚合服务的企业管理器上的 IntroscopeEnterpriseManager 日志文件。

**症状:**

似乎企业管理器未能及时从 TIM 接收数据。

**解决方案:**

可能是由于 TIM 收集服务未正常运行。

检查位于运行 TIM 收集服务的企业管理器上的 IntroscopeEnterpriseManager 日志文件。

**症状:**

收集器未从 TIM 接收信息。

例如，在 TIM 日志中存在如下错误消息：

`ERROR` 表明该 TIM 没有收集器服务

**解决方案:**

收集器或 MOM 的 IP 地址可能已更改，“企业管理器配置”页面未反映该更改。

重新启动企业管理器，或遵循《CA APM 配置和管理指南》中的[编辑企业管理器的 IP 地址](#) (p. 249)过程。

**症状:**

与上一症状相同。（收集器未从 TIM 接收信息。）

例如，在 TIM 日志中存在如下错误消息：

`ERROR` 表明该 TIM 没有收集器服务

**解决方案:**

收集器或 MOM 可能有两个 IP 地址，一个 IP 地址显示在“企业管理器配置”页面中，另一个显示在“TIM 设置”页面中。

查找“EM 配置”页面和“TIM 设置”页面中不匹配的地址。

如果地址不同，请遵循《CA APM 配置和管理指南》中的[编辑企业管理器的 IP 地址](#) (p. 249)过程。

**症状:**

收集器的运行状态在“服务配置”页面中显示为“关闭”，即使收集器处于运行状态也是如此。

**解决方案:**

MOM 和收集器之间的时间不同步。

同步 MOM 和收集器之间的时间。

有关详细信息，请参阅《CA APM 配置和管理指南》中的[企业管理器时钟同步](#) (p. 85)。

**症状:**

收集器的运行状态显示为“未知”。

**解决方案:**

验证收集器的主机名和 IP 地址是否正确。如果不正确，请编辑 `<EM_Home>\config` 目录中 `IntroscopeEnterpriseManager.properties` 文件中的 `introscope.enterprisemanager.clustering.login.em1.host` 属性。验证 IP 地址是否可解析。请不要使用 localhost。

## 定义 CA CEM 域

CA CEM 域为管理员提供了一种建立 CA CEM 范围内的默认值和设置的方式，从而可以获得预期的事务行为、用户和业务影响以及 CA CEM 范围内的数据保留。

公司必须为 CA CEM 定义一个域。业务服务、业务事务和业务应用程序在域级别下创建。默认域名是 Local Domain。

在创建用户组、业务服务和事务时，可以使用继承 CA CEM 域默认值或创建特定值（例如，用户的 SLA 设置）的选项。

### 定义 CA CEM 域:

1. 选择“设置”、“域”。
2. 定义域设置:

#### 域名

为 CA CEM 域提供一个有意义的名称。域名不区分大小写。

#### 捕获全面缺陷详细信息

如果选择该选项，“CEM” > “突发事件管理” > “缺陷详细信息” 页面将显示关于 Query 和 POST 参数的更多数据以及请求和响应正文。有关详细信息，请参阅《CA APM 安全指南》。

#### 通过 IP 子网排除缺陷

如果选择该选项，突发事件故障排除图网络层将按照源子网显示缺陷分布。（不会按 IP 地址重新分组用户。）

#### 子网掩码

使用此功能和“通过 IP 子网排除缺陷”来定义子网。

掩码通常设置为 255.255.255.0。不过，对于大型网络，设置为 255.255.0.0 可能更合适。

3. 定义“用户组”设置:

#### 通过 IP 子网创建用户组

该功能用于根据新用户的客户端 IP 子网自动创建新用户组。

**重要信息！** 如果在大型电子商务站点（拥有数十万或数百万用户）上执行安装，请不要使用此功能。创建的用户组数将难以管理。有关详细信息，请参阅[管理用户和组 \(p. 277\)](#)。

#### 子网掩码

使用此功能和“通过 IP 子网创建用户组”定义子网以创建用户组。

掩码通常设置为 255.255.255.0。不过，对于大型网络，设置为 255.255.0.0 可能更合适。通过基于特定 IP 地址和限制性更强的子网掩码创建用户组，可以进一步优化用户组。请参阅[管理新的用户组 \(p. 282\)](#)。

## 4. 定义标识设置：

**在用户识别中忽略应用程序**

如果未选择该选项，那么用户对于每个业务应用程序都是唯一的，并且会针对每个用户 ID（业务应用程序 + 登录名）对统计信息历史计数。例如：

- ApplicationOne\_MyLoginName = 用户 ID
- ApplicationTwo\_MyLoginName = 另一个用户 ID
- ApplicationThree\_MyLoginName = 第三个用户 ID
- eCommApplication\_MyLoginName = 第四个用户 ID，但是因为它 是电子商务业务应用程序，缺陷会被保留；统计信息会归入未指定的用户历史。

如果选择“在用户识别中忽略应用程序”选项，那么用户将仅被计算一次，即使用户登录多个业务应用程序也如此。

**重要信息！** 如果已经有原始方案（即一个用户使用多个用户 ID 收集统计信息），并选择此选项以忽略业务应用程序，则将创建其他用户 ID：

- MyLoginName = 用户 ID（用于该用户将来所有的登录，不受业务应用程序的限制）

在本示例中，将显示一个用户的统计信息历史，并且分成五个时间段保存。统计信息历史将根据数据保留规则的配置保留在数据库中。

**路径参数分隔符**

如果使用路径参数标识用户、会话、用户组或事务，请在此处指定分隔符。有关路径参数的详细信息，请参阅《CA APM 事务定义指南》。

## 5. 定义默认事务设置：

- a. 定义影响级别，该级别确定事务的缺陷类型的业务优先级。

在大多数情况下，默认值“中”已足够。默认情况下，该值由 CA CEM 域中的业务服务继承，但可以在事务级别进行编辑。

- b. 定义事务服务级别协议 (SLA) 的级别。

默认情况下，这些值由 CA CEM 域中的业务服务继承，但可以在事务级别进行编辑。该表描述了 CA CEM 域级别的 SLA 选项。

**成功率 SLA**

成功率服务级别协议（百分比）。默认值是 95% 无缺陷事务。

### Sigma SLA

**Sigma** 服务级别协议（数值）。**Sigma** 分数是根据每百万次采样数的缺陷率 (DPMO) 进行计算的度量方式。默认值是 4.00，接近完美的分数为 6.00，完美（零个事务缺陷）的分数为无穷大。

### 事务处理时间 SLA

事务处理时间服务级别协议（秒）。默认值是 8 秒总处理时间。

**提示：** CA CEM 中的时间可以指定为 1/1000 秒 (0.001)。如果您指定的值小于该值（例如 0.0001），CA CEM 会将该值设置为 0.000。

#### 6. 定义默认用户设置：

- a. 定义影响级别，该级别确定缺陷类型的业务优先级。

在大多数情况下，默认值“中”已足够。默认情况下，该值由 CA CEM 域中的业务服务继承，但可以在用户组级别进行编辑。

- b. 定义默认用户服务级别协议 (SLA) 级别。

默认情况下，这些值由 CA CEM 域中的业务服务继承，但可以在用户组级别进行编辑。

#### 7. 定义值设置：

性能报告（业务服务和业务事务页面）可以显示（或不显示）IT 价值列，该列的计算方式如下：

IT 价值 = （每个业务事务的 IT 价值） \* （业务事务的数量）

例如，观测到每个正常业务事务盈利 2.00 美元，这意味着每个成功的事务可以为业务获利 2.00 美元。

- a. 要显示 IT 价值：选中“计算 IT 价值”复选框，然后按相应币种键入“每个业务事务的 IT 价值”。

如果不选中该复选框，IT 价值列不会显示在“性能”报告中。

- b. 有关设置“计算突发事件成本”复选框的信息，请参阅[突发事件成本与业务影响](#) (p. 258)。

#### 8. 定义数据保留设置：

##### 取消用户活动状态晚于

只要用户在网络上生成事务，就会处于活动状态。默认为当在过去的 730 天内未观测到用户的事务时，即将该用户置于非活动状态。

**提示：** 请考虑像休假或请假长度之类的因素与终止相比，哪些因素可以帮助您确定适当的天数。



## 统计信息聚合

可以按每个用户每小时、每个用户组和所有用户聚合统计信息。可以选择保持用户和用户组统计信息的时间长度。

### 保持每小时用户统计信息时间

默认值是将每小时用户统计信息保持 3 天。3 天后，您可以看到每日或每周用户统计信息，但看不到 3 天前的每小时统计信息。

### 保持每日用户统计信息时间

默认值是将每日用户统计信息保持 15 天。15 天后，您仍可以看到每周用户统计信息，但看不到 15 天前的每日统计信息。

### 保持每周用户统计信息时间

默认值是将每周用户统计信息保持 27 周。将丢弃早于约 6 个月的每周用户统计信息。

### 保持每小时用户组统计信息时间

默认值是将每小时用户组统计信息保持 3 天。3 天后，您可以看到每日或每周用户组统计信息，但看不到 3 天前的每小时统计信息。

### 保持每日用户组统计信息时间

默认值是将每日用户组统计信息保持 15 天。15 天后，您仍可以看到每周用户组统计信息，但看不到 15 天前的每日统计信息。

### 保持每周用户组统计信息时间

默认值是将每周用户组统计信息保持 27 周。将丢弃早于约 6 个月的每周用户组统计信息。

**警告！** 如果设置的这些数据保留设置太高，则每日聚合可能会滞后。如果 `IntroscopeEnterpriseManager` 日志文件显示企业管理器正在处理几天前不是昨天的统计信息记录，则说明每日聚合延迟。

9. 单击“保存”保存所有设置。

## 突发事件成本与业务影响

该主题说明在“域”页面（“设置”>“域”）中选中“计算突发事件成本”复选框的效果。

“突发事件管理”>“突发事件”报告可以显示“突发事件成本”列或者“业务影响”列。CA CEM 将突发事件成本定义如下：

$$\text{突发事件成本} = (\text{每个用户每分钟的成本}) * (\text{用户人数}) * (\text{分钟数})$$

—其中，分钟数是突发事件的持续时间（分钟），用户数是唯一用户的数量，不包括归类为未指定用户的任何用户。

**注意：**在用户登录前发生的企业事务以及所有电子商务事务都计入未指定的用户组。CA CEM 事务仅由未指定用户执行时，CA CEM 在“用户”列中显示一个符号，突发事件成本是 0.00 美元（每个用户每分钟的成本 \* 0 \* 分钟数）。

### 显示突发事件成本：

1. 选中“计算突发事件成本”复选框。

如果选中该复选框，突发事件报告中将不显示“业务影响”列，而显示“突发事件成本”列。

2. 按相应币种键入“每个用户每分钟的突发事件成本”。

例如，0.50 美元；这意味着如果业务突发事件为 5 个用户打开了 10 分钟，对业务成本是 25.00 美元。

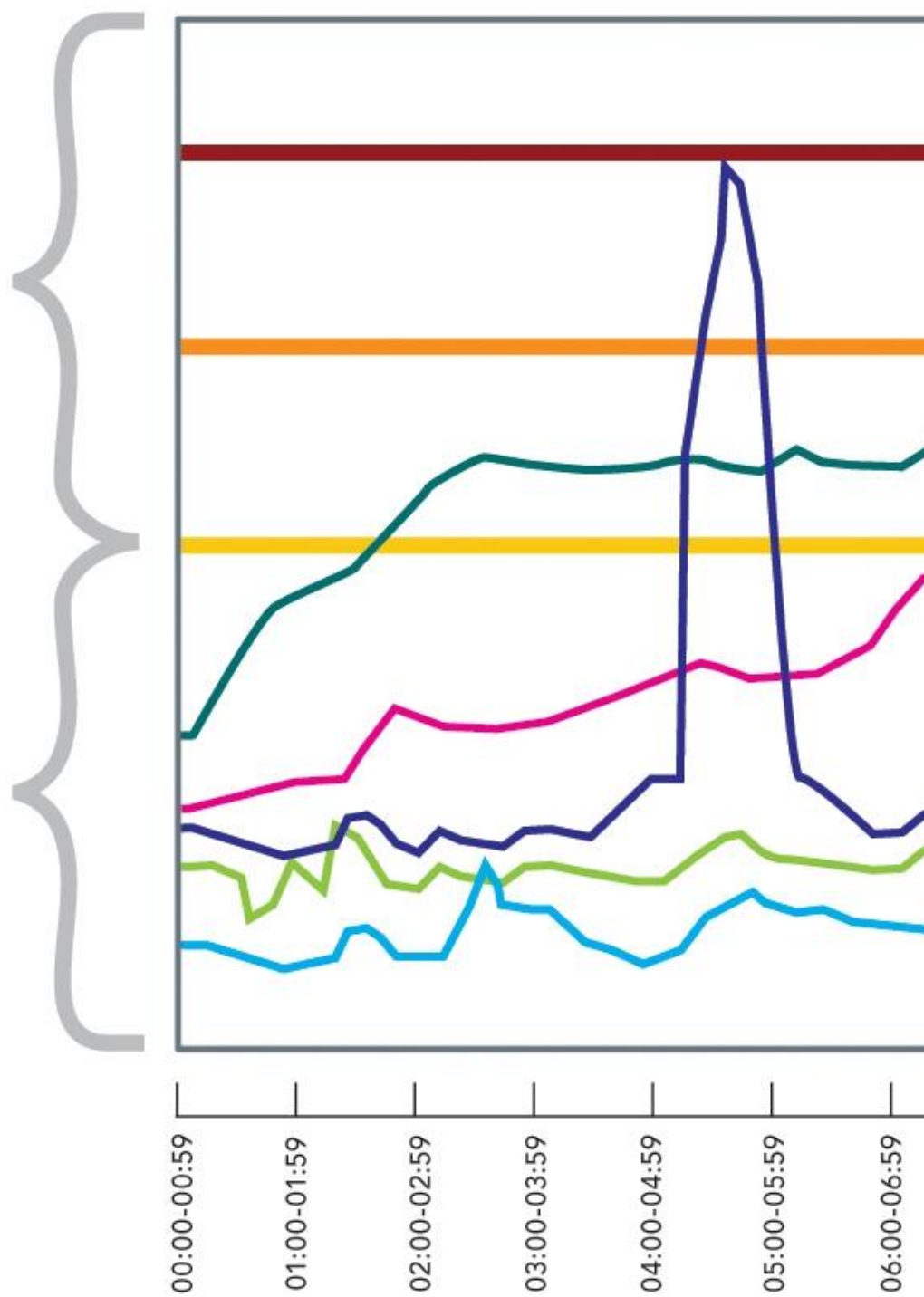
### 显示业务影响：

- 清除“计算突发事件成本”复选框。
  - 如果在“设置”>“域”页面中选中了“计算突发事件成本”复选框，突发事件报告中将显示“突发事件成本”，而不显示“业务影响”。
  - 如果不选中该复选框，突发事件报告中将不显示“突发事件成本”列，而显示“业务影响”列。
  - 不需要在“每个用户每分钟的突发事件成本”文本框中输入值。

**注意：**有关业务影响限制的信息，请参阅[定义与突发事件相关的设置](#) (p. 259)。

## 定义与突发事件相关的设置

在许多环境中，出现一些缺陷是正常的。但当偏离正常值时，您需要及时了解。



当偏离正常值时，可以使用突发事件管理设置、突发事件生成规则和影响设置来生成突发事件。

### 缺陷业务影响

CA CEM 基于缺陷的业务事务、缺陷类型和用户，将业务影响分配给每个传入缺陷。

缺陷的业务影响的计算方式如下所示：

$$\text{业务事务权重} * \text{缺陷类型权重} * \text{用户权重}$$

影响级别分配给每个：

- 业务事务
- 缺陷类型
- 用户

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

### 突发事件业务影响

CA CEM 将传入的缺陷聚合到突发事件中。按照业务事务和缺陷类型聚合突发事件。突发事件的业务影响是指其所有聚合缺陷的业务影响总和。业务影响显示在“突发事件管理”报告中。

如果业务事务、缺陷类型和用户影响的影响级别都是中等 (4)，那么缺陷影响为  $4 * 4 * 4 = 64$ 。这是默认值，显示在[突发事件报告](#) (p. 258)的图形中。如果使用这些默认业务影响，那么：

- 1000 为中等 = 16 个缺陷可以打开中等突发事件
- 2500 为严重 = 40 个缺陷升级为严重突发事件
- 5000 为关键 = 79 个缺陷升级为关键突发事件

### 如何生成突发事件

有两种创建突发事件的方式：

- 通过达到业务影响阈值（这是默认方法）

通过触发已启用的突发事件生成规则

### 主要影响因素报告

“主要影响因素”报告对前五个重要影响进行了概述，包括业务服务、业务事务、用户/组以及突发事件。

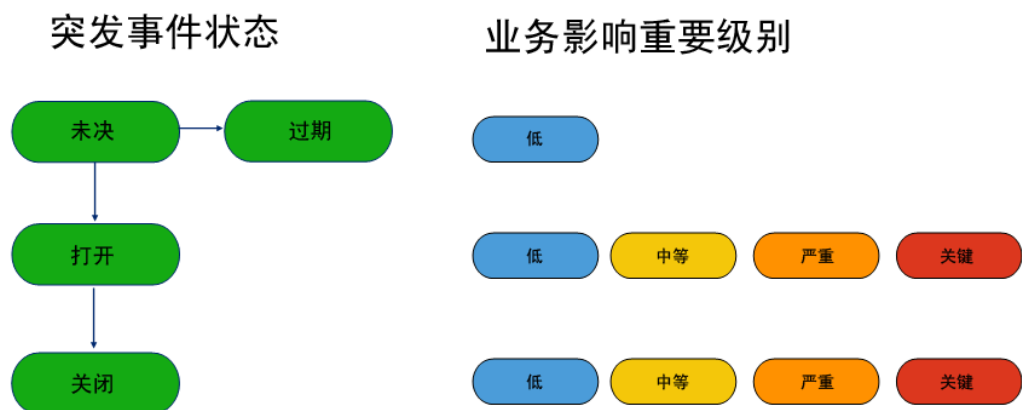
### 缺陷报告

缺陷报告显示每个缺陷的业务影响。

### 突发事件状态与业务影响的重要级别

突发事件可以遍历多个状态，具体取决于其业务影响价值。任何 CA CEM 用户都可以关闭突发事件。可以使用中等、严重和关键重要级别设置，在“设置”>“突发事件设置”页面中定义每个状态之间的临界值。

该图将突发事件状态与业务影响重要级别进行比较。



### 配置突发事件管理设置

突发事件管理配置直接影响突发事件生成规则和过期规则及其逻辑。

要配置突发事件管理设置，请执行以下操作：

1. 选择“设置” > “突发事件设置”。
2. 以分钟为单位键入“评估时间间隔” — 默认值是 5 分钟。  
该值用于突发事件的生成和过期规则。例如，如果设置为 5 分钟，则每隔 5 分钟将复查一次每个活动（启用的）规则，以确定是否应生成突发事件，或未决突发事件是否过期。
3. 在“删除缺陷晚于”中键入天数 — 默认为在 7 天后删除缺陷。
4. 单击“保存”保存所有设置。

## 设置突发事件生成规则

可以配置自定义规则，以便在业务的相应时刻生成突发事件。

当达到在“影响设置”中设置的重要级别阈值时，CA CEM 也会生成突发事件；请参阅[为突发事件设置业务影响并收集证据](#) (p. 264)。

**配置突发事件生成规则：**

1. 选择“设置” > “突发事件设置”。
2. 键入要求生成突发事件的缺陷数。该数表示在很短的时间内迅速增加的缺陷数。  
例如，可以针对 5 分钟（示例评估期）内生成 1000 个缺陷配置一条规则，因为在该时间段内生成该数目的缺陷将对业务产生巨大影响。
3. 键入要求生成突发事件的缺陷增加百分比。该百分比表示在很短的时间内迅速增加的缺陷百分比。
4. 键入组合规则：
  - 要求生成突发事件的缺陷数。
  - 一个评估时间间隔数，例如（3 个中的）2 个，如上所述。
  - 另一个评估时间间隔数，例如 3 个（中的 2 个），如上所示。

在本示例中，您可能针对在 3 个评估时间间隔的后 2 个时间间隔内（如果评估时间间隔为 5 分钟，即在 15 分钟的后 10 分钟内）生成 500 个缺陷配置一条规则。

5. 选中要激活的每个规则旁边的“启用”复选框。

CA CEM 基于评估时间间隔（例如，每隔 5 分钟）检查每个启用的规则。

**注意：**突发事件生成规则使用 AND 逻辑。换句话说，在 CA CEM 生成突发事件之前，每个启用的规则必须为 true。

6. 单击“保存”保存所有设置。

## 为突发事件设置业务影响并收集证据

影响设置允许您设置生成突发事件并确定突发事件重要级别的阈值。证据收集设置允许您部署高级证据收集脚本。

CA CEM 可以配置为每次更改突发事件重要级别时执行证据收集脚本。

| 该脚本...      | 在下列情况下执行...           |
|-------------|-----------------------|
| 打开时收集证据     | 突发事件打开时。              |
| 中等重要级别时收集证据 | 突发事件重要级别从“低”更改为“中等”。  |
| 严重重要级别时收集证据 | 突发事件重要级别从“中等”更改为“严重”。 |
| 关键重要级别时收集证据 | 突发事件重要级别从“严重”更改为“关键”。 |

在 CA CEM 中收集证据之前，需在系统中安装 Python 或 Perl。然后，可以修改 CA CEM 属性 `python.path` 或 `perl.path`，以指定 Python 或 Perl 的安装位置。

**注意：**该主题描述收集突发事件证据。CA Technologies Professional Services 允许您收集和显示各个缺陷的证据。有关详细信息，请参阅[设置“其他缺陷信息”链接的目录路径](#) (p. 507)。



**请执行以下步骤：**

1. 在运行 TIM 收集服务的企业管理器上安装 Python 或 Perl。
2. 编辑 *tess-customer.properties* 文件，并修改 `python.path` 或 `perl.path` 属性。

例如，`python.path=/usr/bin/python` 或 `perl.path=C:\\perl\\bin\\perl.exe`

如果为 Windows 平台使用反斜线，则需要使用双斜线 (\\)，因为单斜线 (\) 将解析为转义字符。

**注意：** 如果还没有 *tess-customer.properties* 文件，请创建一个。

有关详细信息，请参阅 [CA CEM 默认属性](#) (p. 505)。

设置 Python 或 Perl 之后，在打开突发事件或更改突发事件状态时，可以创建和启用要运行的证据收集脚本。

**定义突发事件的业务影响级别并设置证据收集脚本：**

1. 选择“设置” > “突发事件设置”。

此时将显示默认设置。

2. 确定中等、严重或关键突发事件的影响设置。

这些设置确定突发事件创建的时间和突发事件重要级别更改的时间。

默认为中等 1000，严重 2500，关键 5000。请参阅[定义与突发事件相关的设置](#) (p. 259)。

3. 确定证据收集设置。如果要在打开突发事件时或在生成中等、严重、关键突发事件时收集证据，请选中一个复选框。例如，检测到中等突发事件时，可以运行下列脚本：

```
%PYTHON%
C:\Introscope\cem\customer\evidencecollectors\evidence.py %ACTION% %SEVERITY% %DEFECTID% %TRANID% %TRANDEFID% %SERVER% %CLIENTIP% %OUTPUT%
%PERL%
cem/customer/evidencecollectors/evidence.pl %ACTION% %SEVERITY% %DEFECTID% %TRANID% %TRANDEFID% %SERVER% %CLIENTIP% %OUTPUT%
```

有关这些参数的信息，请参阅[证据收集脚本中使用的参数](#) (p. 266)。

为 `python.path` 属性（上述“要设置与脚本一起使用的 Python 或 Perl”中的第 2 步）指定的位置将取代 `%PYTHON%`。如果已经安装 Perl，在命令行中使用 `%PERL%`，而非 `%PYTHON%`。

4. 单击“保存”保存对影响级别和证据收集设置所做的更改。

## 证据收集脚本中使用的参数

这些是可以用于证据收集脚本的参数。上述“要设置与脚本一起使用的 Python 或 Perl”的第 3 步中显示了一个示例。

### **ACTION**

为 OPEN 或 CLOSE，具体取决于突发事件处于打开还是关闭状态。

### **SEVERITY**

业务影响（低、中等、严重或关键）。

### **DEFECTID**

突发事件的数据库 ID。

### **TRANID**

业务事务的数据库 ID。

### **TRANDEFID**

业务服务的数据库 ID。

### **SERVER**

从中检测到最新缺陷的服务器的 IP 地址。（缺陷可能发生在多个服务器中。但是，此参数仅捕获最新的服务器 IP 地址。）

### **CLIENTIP**

从中检测到最新缺陷的客户端（例如，用户的 PC）的 IP 地址。（缺陷可能发生在多个客户端中。但是，此参数仅捕获最新的客户端 IP 地址。）

### **OUTPUT**

放置证据收集脚本输出的位置。

证据收集的一个示例脚本文件随该产品安装在以下位置：

*cem/customer/evidencecollectors/evidence-example.py*

该脚本说明参数的用法。

## 配置突发事件过期规则

突发事件过期规则让您可以去掉影响程度低的未决突发事件。

可以配置自定义规则来确定未决突发事件过期的时间。

未决突发事件是指已发生但未达到影响阈值，因而未在 CA CEM 中报告为突发事件的缺陷事件。例如，如果业务影响阈值为 1000，并且观测到业务影响值仅为 999，则该突发事件为未决突发事件。

**配置未决突发事件过期规则：**

1. 选择“设置” > “突发事件设置”。
2. 键入在未决突发事件过期之前，不能出现相关缺陷的分钟数。例如，要设置一天，则键入 1440 分钟（60 分钟 \* 24 个小时 = 1440）。
3. 键入在未决突发事件过期之前，突发事件必须处于未决状态的分钟数。
4. 键入组合规则：
  - 未决突发事件尚未达到的缺陷数。
  - 一个评估时间间隔数，例如（10 个中的）9 个。
  - 另一个评估时间间隔数，例如 10 个（中的 9 个）。

在本示例中，您可能针对在 10 个评估时间间隔的后 9 个时间间隔内（如果评估时间间隔为 5 分钟，即在 50 分钟的后 45 分钟内）生成 500 个缺陷配置一条规则。

5. 选中要激活的每个规则旁边的“启用”复选框。

CA CEM 基于评估时间间隔（例如，每隔 5 分钟）检查每个启用的规则。

**注意：**突发事件过期规则使用 OR 逻辑。换句话说，任何启用的规则都可能导致 CA CEM 使突发事件过期。

6. 单击“保存”保存所有设置。

## 在突发事件打开或更改重要级别时发送电子邮件

可以将 CA CEM 配置为在突发事件打开或其重要级别更改时发送电子邮件。例如，可以将 CA CEM 配置为当突发事件重要级别变为关键时向突发事件分析人员发送电子邮件。

**注意：**系统不会为打开的重要级别为低的事件生成电子邮件。

请执行以下步骤：

1. 选择“设置”、“突发事件设置”。
2. 在“突发事件电子邮件设置”部分，根据需要编辑字段。  
如果要向多个地址发送电子邮件，请使用逗号 (,) 分隔电子邮件地址。
3. 单击“保存”保存所有设置。
4. 确保 CA CEM 已配置为发送电子邮件。请参阅[配置 SMTP 服务器设置](#) (p. 268)。

CA CEM 向 CEM 管理员发送的电子邮件通知包含以下信息：

- 突发事件 ID
- 受影响的业务应用程序
- 受影响的业务服务
- 受影响的业务事务
- 受影响的组数
- 受影响的用户数
- 缺陷数
- 缺陷名称
- 首先发生的缺陷
- 最后发生的缺陷

## 配置 SMTP 服务器设置

必须提供 SMTP 服务器的名称和端口号，以便 CA CEM 可以通过电子邮件发送报告。还可以为随附报告的电子邮件配置主题和消息文本。有关报告的信息，请参阅 [CA CEM 报告](#) (p. 299)。

这些 SMTP 设置也可用于 CA CEM 事件和突发事件的电子邮件通知。（请参阅[接收事件的电子邮件通知](#) (p. 294)和[在突发事件打开或更改重要级别时发送电子邮件](#) (p. 267)。）

保存电子邮件连接之前必须先对其进行测试。

请执行以下步骤：

1. 选择“系统”>“电子邮件设置”。
2. 定义 SMTP 服务器设置：

#### 主机名

输入 SMTP 服务器的主机名称。

#### 端口

输入 SMTP 服务器上的端口号。

#### 发件人地址

这是测试连接电子邮件的发件人地址。

#### 收件人

这是测试连接电子邮件的收件人地址。默认情况下，该地址和“发件人地址”取自 Embedded Entitlements Manager 中的 CA CEM 用户（操作员）的详细信息。如果该地址缺失，将使用 `tess-default.properties` 文件中的 `email.defaultFromAddress` 属性；有关更改此默认值的详细信息，请参阅 [email.defaultFromAddress](#) (p. 513)。

#### 需要身份验证

如果 SMTP 服务器需要用户名和密码，请选中此复选框。

#### 用户名

如果需要身份验证，请输入用户名。

#### 密码

如果需要身份验证，请输入密码。

3. 定义电子邮件设置：

#### 主题

输入通过电子邮件发送报告时使用的标准主题行。

#### 消息

输入通过电子邮件发送报告时使用的标准消息。

#### 页脚文本

输入显示在通过电子邮件发送的报告底部的标准文本。

4. 单击“测试连接”。将发生以下三件事情之一：
  - 如果显示确认消息并且收到指示测试成功的电子邮件，则表示 SMTP 设置和“收件人”电子邮件地址均正确。
  - 如果显示确认消息，但是未接收到电子邮件，则表示 SMTP 设置正确，但“收件人”电子邮件地址不正确。
  - 如果显示错误消息，则表示 SMTP 设置不正确。（如果必须等待 SMTP 服务器超时，可能需要一段时间才会显示消息。）
5. 单击“保存”。

**注意：**如果没有为报告设置电子邮件，CA CEM 用户在尝试创建报告时将接收到错误消息。

有关报告类型以及配置和排定报告的 CA CEM 用户选项的详细信息，请参阅 [CA CEM 报告](#) (p. 299)。

## 为新的业务服务设置安全组

如果您的组织已部署 Embedded Entitlements Manager，则可以使用访问策略来控制哪些安全组具有访问业务服务及其关联数据的权限。

安全组是为 Embedded Entitlements Manager APM 应用程序创建的用户组。在 Embedded Entitlements Manager 中，安全组称为应用程序组。

管理员配置哪些安全组可以自动访问所有新创建的业务服务。

默认情况下，已设置四个访问策略：

### 业务服务—所有权限

CEM 系统管理员组具有所有业务服务的所有权限。

### 业务服务—读写

CEM 配置管理员组具有所有业务服务的读取和写入权限。

### 业务服务—读取敏感数据

CEM 突发事件分析人员组具有读取所有业务服务的敏感数据的权限。

### 业务服务—读取

CEM 分析人员组和 CEM 突发事件分析人员组具有所有业务服务的读取权限。

如果使用的是标准安全组（CEM 系统管理员、CEM 配置管理员、CEM 突发事件分析人员以及 CEM 分析人员），那么这些访问策略可能已足够。但是，如果已经创建其他安全组，并且希望这些组的成员能够访问所有业务服务，则需要创建或修改访问策略以包括这些组。

**注意：**该主题的过程描述如何为*所有*业务服务修改或创建访问策略。如果需要为*特定*业务服务修改或创建访问策略，请参阅《CA APM 事务定义指南》中有关访问策略的主题。

#### 查看或编辑所有业务服务的现有访问策略：

1. 选择“安全”>“访问策略”。

如果自安装 CA CEM 以来未添加过访问策略，将看到在上表中列出的访问策略。

2. 单击策略名称进行查看或编辑。

此时将显示“更新访问策略”页面。

3. 修改“更新访问策略”页面中的字段，然后单击“保存”。

将在下面的列表中对字段进行描述。

确保为“业务服务”选择“全部”。这意味着所选的安全组与所有后续创建的业务服务关联，并且适用于所有现有的业务服务。

#### 为所有业务服务创建新访问策略：

1. 选择“安全”>“访问策略”。

2. 单击“新建”。

3. 完成“新访问策略”页面上的字段，然后单击“保存”。

将在下面的列表中对字段进行描述。

**注意：**确保为“业务服务”选择“全部”并为“安全组”选择“选择”。这意味着所选的安全组与所有业务服务（现有的和将来的）关联。

此处描述“新访问策略”页面中的字段。

#### 访问策略名称

为该策略提供一个有意义的名称。

#### 说明

添加描述性备注。

#### 策略选项

选择创建策略以明确同意或拒绝对业务服务的操作。

如果在同意和拒绝之间有冲突，将优先选择拒绝策略。

### 已启用

如果要让策略生效，则启用该策略。

如果现在不想使用策略，但是将来可能要使用该策略，则禁用该策略。删除不再使用的策略。

### 写

选择此选项将允许安全组成员在“业务服务”选项卡中查看、编辑和删除业务服务及其所有子对象（业务事务、事务、组件等）。

用户至少要对一个业务服务具有访问权限，才能看到“业务服务”选项卡。

### 读

选择此选项将允许安全组成员在“CEM”选项卡中查看与该业务服务关联的图表和报告。

**注意：**确保 Embedded Entitlements Manager 是配置的唯一领域。如果配置了本地领域（除 Embedded Entitlements Manager 领域之外），那么所有用户均可以访问排定报告中的所有数据。有关领域的信息，请参阅《CA APM 安全指南》。

### 读取敏感数据

选择此选项将允许安全组成员查看与缺陷有关的主机、URL 路径、TCP 端口、Cookie 以及 HTTP 头。这些内容显示在“CEM”>“突发事件管理”>“缺陷详细信息”页面中。

如果选中“捕获全面缺陷详细信息”复选框（在“设置”>“域”页面中），那么“缺陷详细信息”页面中还会显示缺陷的 Query 和 Post 参数以及请求和响应的正文信息。有关详细信息，请参阅《CA APM 安全指南》中有关 CA CEM 的章节。

将此选项与读取复选框一起使用。访问缺陷详细信息页面需要执行读取操作。

### 业务服务

全选。这会将访问策略应用于所有业务服务和所有新业务服务（在创建新服务时应用）。

**注意：**要修改特定业务服务的访问策略，请参阅《CA APM 事务定义指南》以获取详细信息。例如，如果需要通过下面方式拒绝分析人员对某个特定业务服务进行访问：为 CEM 分析人员和 CEM 突发事件分析人员安全组设置对该业务服务的明确拒绝。



## 安全组

选择“选择”并将策略的安全组移动至“已选择”列。

此处显示的安全组对应于 Embedded Entitlements Manager 中特定于 APM 应用程序的用户组。无法在 CA CEM 中选择 Embedded Entitlements Manager 全局用户组。

使用 Embedded Entitlements Manager 查看或修改安全组。有关使用 Embedded Entitlements Manager 的信息，请参阅《CA APM 安全指南》。无法从 CEM 控制台中管理安全组。

## 启用监视器

需要确保 TIM 已启用，以便监控事务。企业管理器不从已禁用的 TIM 监视器接收数据。

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。（请参阅《CA APM 安装和升级指南》。）
- 在升级 TIM 和/或企业管理器之后。（请参阅《CA APM 安装和升级指南》。）
- 在导入配置之后。（请参阅[导入 APM 数据库配置](#) (p. 53)。）

### 启用 TIM 与企业管理器之间的通信：

1. 选择“设置”>“监视器”。
2. 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。

## 同步监视器

同步监视器会将当前域配置文件发送到所有已启用的 TIM 和代理。域配置文件包括事务定义、缺陷规范和 Introscope 事务跟踪参数。

下面列出了您需要同步监视器的一些情形：

- 在 CA CEM 中创建或更新业务服务之后。在同步监视器并生成更改的业务服务的某些度量标准之前，在 CA CEM 中对业务服务和事务所做的更改不会显示在 Workstation 或 WebView 调查器树中。
- 设置 TIM 并且将其与企业管理器关联时。（请参阅《CA APM 安装和升级指南》。）

- 在升级 TIM 和/或企业管理器之后。（请参阅《CA APM 安装和升级指南》。）
- 在创建或修改事务定义之后，要将更新的定义发送给代理和已启用的 TIM。（请参阅《CA APM 事务定义指南》。）
- 导入配置文件之后，要将导入的定义发送给代理和已启用的 TIM。（请参阅[导入 APM 数据库配置](#) (p. 53)。）

### 在网络中同步监视器：

1. 选择“设置” > “监视器”。
2. 如果禁用了任何所需的监视器，请将其启用。（请参阅[启用监视器](#) (p. 273)。）
3. 如果要检查自上次同步以来对配置所做的更改，请参阅[查看自上次同步以来的配置更改](#) (p. 274)。
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。这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 CA CEM 向企业管理器发送事务和跟踪信息。

## 查看自上次同步以来的配置更改

在同步之前，可以列出对配置所做的更改。这允许您在同步之前复查更改。

自从上次同步以来对这些属性所做的任何更改均显示在“域配置更改历史”表中：

- 业务应用程序定义
- 业务服务定义
- 缺陷定义
- 业务事务定义
- 缺陷重要性定义
- 事务定义
- 缺陷影响级别
- 用户标识参数
- 事务参数定义

- 会话标识参数
- 临时会话标识参数
- 事务重要性定义
- 用户组标识参数
- 事务组件定义
- 私有参数

如果您删除特定类型的参数（如私有参数），则对象名称显示为空白，属性更改显示为“没有显示任何内容”。这是因为已将对象名称和更改从数据库中删除。

**要查看自上次同步以来所做的配置更改，请执行以下操作：**

1. 确认未同步监控器。
2. 选择“设置” > “监视器”。
3. 单击“查看自上次同步以来的更改”。

此时显示更改历史表。

**注意：**更改历史表列出自上次同步以来所做的配置更改。这与列出上次同步和当前配置之间的差异不同。例如，如果将一个值从 5 改为 2，然后改回 5；这会在表中生成两行，而不是像您所期望的那样一行都不生成。

默认情况下，“域配置更改历史”表中的最大行数为 1000。要更改该值，请参阅[限制自上次同步以来列出的更改数](#) (p. 435)。

并非所有列出的属性值都对您有用。例如，在创建参数时显示的配置管理器值显示对象的内部类名。



# 第 19 章：在 CA CEM 上管理用户和组

---

该列表显示管理用户和组所涉及到的主要任务：

1. [了解 CA CEM 中可用的用户组类型](#) (p. 277)。
2. [了解通过事务中的信息自动创建用户组](#) (p. 279)。
3. [了解通过 IP 子网自动创建用户组](#) (p. 280)。
4. [将用户从新用户组重新分配给其他组](#) (p. 282)。
5. [配置用户组和 SLA（服务级别协议）设置](#) (p. 283)。
6. [通过批量编辑管理用户和用户组](#) (p. 284)。
7. [将用户组 SLA 与业务事务关联起来](#) (p. 285)。
8. [删除用户组](#) (p. 288)，或者[停用或删除单个用户](#) (p. 289)。

**注意：**本章讨论的*用户*是受监控应用程序的用户。例如，在银行业应用程序中，用户是银行的客户，可通过登录查看和管理其帐户。可能会根据这些用户的帐户类型对其分组。

不过，举例来说，如果您要寻找将 CA CEM 用户分成 *安全用户组*，以便配置 CA CEM 用户可以在 CEM 控制台上访问的选项卡、菜单项和业务服务的相关信息，请参阅《CA APM 安全指南》。

## 关于用户组

使用用户组可以方便地为的一组用户配置设置，而不必分别为各个用户配置设置。可以定义用户组，以便轻松确定可能遇到问题的用户群体。

可以手工创建新用户组，并且可以手工将用户移到用户组中。CA CEM 还提供自动创建用户组的方法。一个用户只属于一个 CA CEM 用户组。

有多种类型的用户组：

### 请求属性用户组

按用户发出的请求中的内容进行分组的用户。

### 子网用户组

按用户子网自动分配新用户的组。

### 手工创建的用户组

必须手工将用户从“新用户”组（或其他用户组）移到此类型的用户组中。

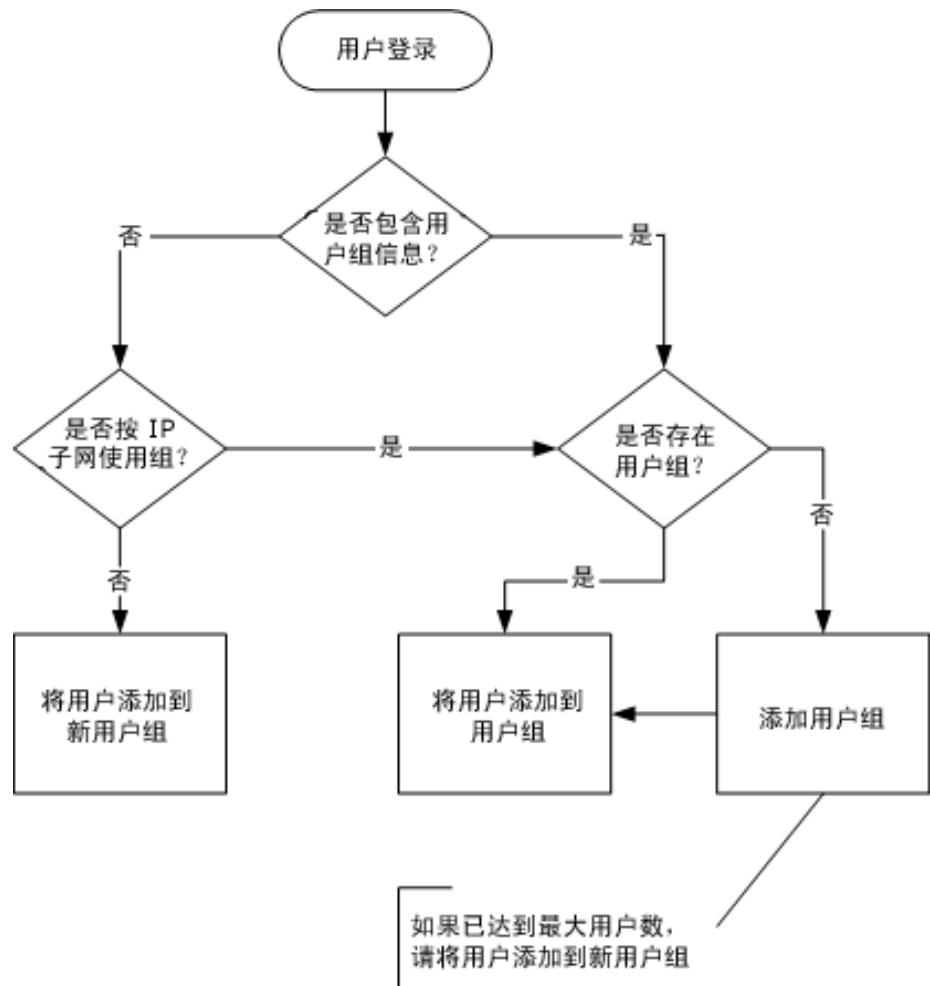
### 新用户

如果没有选择自动生成用户组的方法，所有新用户登录都会分配到新用户组中。

### 未指定的用户

所有电子商务事务都分配到未指定的用户组中。此外，用户登录之前发生的企业事务也会分配到未指定的用户组中。

以下流程图阐释了自动创建和分配用户组背后的逻辑。



## 最大用户组数

CA CEM 允许您控制自动创建的用户组的数目。在不可预料的情况下（如在 CEM 管理员察觉之前，组的数量可能会急剧增长），此控制功能很有用。

默认情况下，自动创建的用户组的最大数为 5000。在 [apm-events-thresholds-config.xml](#) (p. 427) 文件中，配置 [introscope.enterprisemanager.max.transaction.user.groups](#) (p. 436) 属性，以便调整默认值。

## 按请求属性自动分配新用户

可以按用户发出的请求中的内容对用户分组。最常见的情况是：

- URL 字符串—例如，查询字符串中的属性代码或客户代码
- HTTP 头—例如，不同电话类型或不同网关的用户
- CA APM TG 头—例如，使用 CA APM TG (x-wtg-info) 头的合成用户

使用该方法，CA CEM 可以按用户位置或公司报告性能信息。例如，这可以帮助您按受影响群体管理中断情况。用户组统计信息可供电子商务业务应用程序使用。

**注意：**按用户组参数所进行的分组优先于按子网进行的自动用户组分类。

**重要信息！**如果在大型电子商务站点（拥有数十万或数百万用户）上进行安装，请慎用此功能。创建的用户组数将难以管理。

**重要信息！**如果您按客户端 IP 地址而非用户名标识用户，请不要按请求属性分配用户。有关使用客户端 IP 地址标识用户的信息，请参阅《CA APM 事务定义指南》。

**按请求属性分配新用户：**

1. 选择“管理”>“业务应用程序”。
2. 选择要按请求属性标识用户的业务应用程序。
3. 选择“用户组标识”。  
此时显示所有现有用户组参数的列表。
4. 单击“新建”创建新用户组参数。
5. 选择相应的参数类型。

- 键入参数名称。
- 单击“保存”。

例如，`x-wtg-info` 类型将 CA APM TG 用户归到名为 `Synthetic` 的组中。这有助于将实际通信与 CA APM TG 通信区分开来。

## 自动将新用户分配给子网用户组

可以通过用户的 IP 子网对用户分组。CA CEM 会自动将新用户的 IP 地址与现有用户组的子网进行比较。首先检查限制最为严格的子网掩码。例如，定义了以下用户组：

```
SubGroup—255.255.255.0 掩码/192.168.2.0 起始 IP  
BigGroup—255.255.0.0 掩码/192.168.0.0 起始 IP
```

传入 IP 流量首先与 `SubGroup` 用户组进行比较，因为其子网掩码更为严格。例如，IP 地址 `192.168.2.4` 将分配给 `SubGroup` 组，IP 地址 `192.168.9.9` 将分配给 `BigGroup` 组。

如果检测到的 IP 地址不在 `SubGroup` 组中，也不在 `BigGroup` 组中，系统会根据您的配置选择分配用户。例如，IP 地址 `192.1.9.9` 的子网掩码为 `255.255.255.0`，但该 IP 地址不适合任何一个组的 IP 地址范围。

**注意：**按用户组参数所进行的分组优先于按子网进行的自动用户组分类。有关详细信息，请参阅[按请求属性自动分配新用户](#) (p. 279)。

## 为新用户创建子网用户组

子网用户组由“设置”>“域”选项卡上的“根据 IP 子网创建用户组”选项确定。

如果您在“设置”>“域”页面上选择了“按 IP 子网创建用户组”选项，则新 IP 地址会触发创建新用户组操作，而不是分配给名为“新用户”的组。

**重要信息！**如果在大型电子商务站点（拥有数十万或数百万用户）上执行安装，请不要使用此功能。创建的用户组数将难以管理。

默认情况下，自动创建的用户组的最大数为 5000。如果想要调整默认值，请参阅[默认 tess-default.properties 文件](#) (p. 505)。

新用户组名称是检测到的 IP 地址的起始编号。在我们的示例中，新用户组将命名为：

```
Usergroup-192.1.9.0—255.255.255.0 掩码/192.1.9.0 地址
```



### 查看新建的用户组：

1. 选择“管理” > “用户组”。
2. 单击“Usergroup-192.1.9.0”查看列出的新用户。

**注意：**已使用一个 IP 地址放入子网用户组中的用户即使其 IP 地址以后发生变化，也会保留在该用户组中。如果需要，您可以手工移动原始用户条目。

## 标识代理服务器用户

在[自动将新用户分配给子网用户组](#) (p. 280)所述的方案中，代理服务器用户将根据代理服务器子网而非其客户端计算机进行分组。这可能并不能满足您业务需求的要求。您可能希望根据客户端子网创建用户组。

同样，对于缺陷列表（“突发事件管理” > “缺陷”页面），您可能希望客户端 IP 地址显示源计算机 IP 地址而非代理服务器的 IP 地址。

如果请求的通信包含 HTTP 头，而该头包含客户端 IP 地址，您可以将 CA CEM 配置为*针对登录和缺陷报告客户端 IP 地址，而不是报告连接 IP 地址*。X-Forwarded-For、Forwarded-For 和 iv-remote-address 都是用于标识客户端 IP 地址的头的示例。也可以使用包含采用点分十进制表示法的 IP 地址（或采用标准表示法的 IPv6 地址）的其他头。例如：

```
X-Forwarded-For: 172.24.192.4
```

名为 ProxyForwardHeader 的 TIM 设置用于指定头的名称。

**注意：**如果缺少头或头的值未采用 IP 地址形式，请使用连接 IP 地址。也就是说，该行为与未指定 ProxyForwardHeader 设置时的默认行为相同。

对于每个 TIM，将 ProxyForwardHeader 的值设置为包含客户端 IP 地址的头。

### 基于头的值标识代理服务器的客户端：

1. 访问 TIM 系统设置页面。（从[CEM 控制台访问 TIM](#) (p. 229)。）
2. 单击“配置 TIM 设置”。  
此时将显示“TIM 设置”页面。
3. 单击 ProxyForwardHeader。
4. 在“新值”字段中，输入头名称（不带冒号），然后单击“更改”。  
此字段不区分大小写。
5. 如果您有多个 TIM，对每个 TIM 重复上述步骤。该设置影响为其定义的每个 TIM 所监控的所有服务器和应用程序。

### 基于头的值创建用户组：

1. 如上述“要基于头的值标识代理服务器的客户端”中所述设置 ProxyForwardHeader。
2. 在 CEM 控制台上，确保选中了通过 IP 子网创建用户组的选项：
  - a. 选择“设置”>“域”。
  - b. 选择“通过 IP 子网创建用户组”。

这意味着，系统会基于头中提供的客户端子网而不是连接子网创建新用户组，并且将报告来自客户端 IP 地址而不是来自连接 IP 地址的缺陷。

3. （可选）通过从代理服务器的客户端创建缺陷来测试配置。如果与缺陷关联的 IP 地址是客户端的 IP 地址而不是代理服务器的 IP 地址，则配置是正确的。

## 管理新的用户组

如果您没有设置自动创建和分配用户组方法之一，则与现有子网用户组不匹配的任何新用户都会自动分配给“新用户”组。

### 要查看新用户，请执行以下操作：

1. 选择“管理”>“用户组”。
2. 单击“新用户”组查看列出的新用户。

此时显示已检测到但尚未分配给用户组的新用户。

**注意：** 在开始监控事务之前，检测不到任何新用户。

## 手动将新用户分配给用户组

新用户自动放入子网用户组或“新用户”组中。

### 要将用户移出当前组，请执行以下操作：

1. 选择“管理”>“用户组”。
2. 单击“新建”定义新用户组。
  - a. 为该用户组指定有意义的名称（如伦敦）。用户组名不区分大小写。
  - b. 键入组的说明。

- c. 目前保留其他参数不变，或参阅[配置用户组 \(p. 283\)](#)了解详细信息。
  - d. 单击“保存”保存新的组。
3. 单击刚创建的用户组。在开始监控事务或将用户移至该组之前，系统检测不到任何新用户。
  4. 返回“用户组”页面，然后单击“新用户”组。
  5. 要将一个或多个用户移到新用户组，请选中“登录名称”左侧的一个或多个复选框。
  6. 从“移至”列表中选择您的新用户组（如伦敦）。
  7. 单击“移动”将用户移至新用户组。
  8. 如果要将当前用户组中的每个用户都移至列表中选定的用户组，请单击“移动全部”。（您不必单击每个“登录名称”左侧的复选框。）
  9. 当您返回“用户组”页面时，单击新用户组（如伦敦）可查看已移动的用户。

## 配置用户组

### 在您的网络上编辑用户组并定义 SLA:

1. 选择“管理” > “用户组”。
- 此时显示当前用户组。
2. 单击“用户组”的名称修改该组的设置。
  3. 单击“常规”选项卡。
  4. 如果需要，更改用户组名称。用户组名不区分大小写。
  5. 键入或修改该组的说明。
  6. 选择“影响级别”，该级别确定该组事务的缺陷类型的业务优先级。在大多数情况下，默认值“中”已足够。
- 默认情况下继承 CA CEM 域的影响级别。如果要更改此值，请清除该复选框并从列表中选择“影响级别”。
- 注意：**要更改 CA CEM 域默认值，请按[定义 CA CEM 域 \(p. 253\)](#)中所述选择“设置” > “域”。
7. 选择在业务服务级别定义 SLA 的服务级别协议 (SLA) 值。
- 默认情况下继承 CA CEM 域的 SLA 值。如果要更改此值，请清除该复选框并从列表中选择一个新值。
- 这些值还用于定义可由业务服务中的用户组事务继承的 SLA 默认值。

### 成功率 SLA

成功率服务级别协议（百分比）。默认值为 95%。

### Sigma SLA

Sigma 服务级别协议（数值）。Sigma 分数是根据每百万次采样数的缺陷率 (DPMO) 进行计算的度量方式。默认值是 4.00，接近完美的分数为 6.00，完美（零个事务缺陷）的分数为无穷大。

### 事务处理时间 SLA

事务处理时间服务级别协议（秒）。没有默认值。

8. 如果要自动将按登录 ID 检测到的新用户添加到按子网名称标识的新用户组中，请选中“按 IP 子网对新用户进行分组”复选框。
  - a. 键入用户组的 IP 地址（如 192.168.1.0）。
  - b. 键入默认子网掩码（如 255.255.255.0）。

在本例中，使用 192.168.1.1 到 192.168.1.254 地址范围中的 IP 地址登录的任何新用户都会自动分配给该用户组而不是“新用户”组。

**提示：**如果您要使用 IP 地址方法将用户分配给组，则在组名中包含 IP 信息是个很好的方法。

9. 单击“保存”保存新的用户组。它出现在“用户组”列表中。

## 通过批量编辑配置用户设置

在某些情况下，您可能需要对您的用户设置进行大范围更改。例如，您可能希望找出几名用户，而不是整个用户组，并将“Sigma SLA”设置从 4.00 修改为 5.00。

使用批量编辑可以对以下各项进行大范围更改：

- 业务服务和事务设置
- 事务和组件缺陷条件
- 用户设置

如果您要大规模修改与事务相关的设置，请参阅《CA APM 事务定义指南》。

使用“用户搜索”页面可以大规模修改用户设置。

### 通过批量编辑配置用户设置：

1. 选择“管理”>“用户组”>“用户搜索”。

此时将显示搜索选项。

2. 选择用户组的名称（如公司）。
3. 选择影响级别（如“全部”）。
4. 如果您要搜索特定的用户，则可以有针对性地键入“登录名称”、“名字”或“姓氏”。
5. 单击“搜索”。  
此时会显示您的搜索结果。
6. 选中您要更改的用户左侧的复选框。或者，如果您要更改整个列表，请单击最上面的复选框。
7. 从“设置值”列表中选择一项：
  - 继承 Sigma SLA
  - Sigma SLA
  - 继承成功率 SLA
  - 成功率 SLA
  - 继承事务处理时间 SLA
  - 事务处理时间 SLA
 此时会显示值文本框或“是/否”列表，具体取决于您的选择。
8. 键入值，或选择“是”或“否”，然后单击“设置”。

## 配置关联 SLA

在某些情况下，您可能希望按业务服务或业务事务设置用户组的 SLA，而不是对整个用户组使用同一个 SLA 或对某个事务（独立于用户组）使用同一个 SLA。

下表是基于事务和用户位置的不同可接受响应时间的示例。

| 用户组/业务事务可接受的响应时间 | 本地  | 远程  | 海外   |
|------------------|-----|-----|------|
| 登录               | 3 秒 | 6 秒 | 9 秒  |
| 购买               | 5 秒 | 7 秒 | 10 秒 |

使用关联 SLA 可按用户组、业务服务或业务事务的组合设置 SLA。关联 SLA 可被视为业务事务或用户组的单维 SLA 集的多维替代。

**注意：**关联 SLA 不会替换域、业务事务或用户组的 SLA。关联 SLA 并非继承自这些 SLA，CEM 管理员必须专门设置关联 SLA。

配置关联 SLA 的过程如下所示：

- [查看关联 SLA](#) (p. 286)
- [添加关联 SLA](#) (p. 286)
- [更新现有的关联 SLA](#) (p. 287)
- [删除关联 SLA](#) (p. 288)

## 查看关联 SLA

按照此过程可复查已创建的关联 SLA，或者查找并选择要删除的 SLA。

您不能在一个表中查看所有关联 SLA。这是因为，在典型的生产系统中，所有用户组、业务服务和业务事务的矩阵非常大。不过，您可以查看给定业务服务或给定用户组的关联 SLA。

**要按用户组和业务事务查看关联 SLA，请执行以下操作：**

1. 选择“管理”、“关联 SLA”。
2. 在“显示”字段中，选择“按用户组”或“按业务服务”。
3. 在第二个字段中，选择组或服务。
4. 在第三个字段中，选择“全部”或者选择组或服务。
5. 单击“刷新”。

此时显示指定用户组或业务服务的关联 SLA。

## 添加关联 SLA

以下过程介绍如何为用户组/业务服务/业务事务集创建新的关联 SLA。

**要添加关联 SLA，请执行以下操作：**

1. 选择“管理”、“关联 SLA”。
2. 确保您要创建的关联 SLA 不存在。如果存在，并且您希望对其进行更改，请参阅“[更新现有的关联 SLA](#) (p. 287)”。
3. 单击“新建”。

4. 按用户组/业务服务/业务事务定义关联设置：
  - a. 用户组—选择用户组的名称或选择“全部”。
  - b. 选择“区域”。
  - c. 业务服务—选择业务服务的名称或选择“全部”。
  - d. 业务事务—选择业务事务的名称或选择“全部”。
  - e. 设置 SLA 值。

#### 成功率 SLA

成功率服务级别协议（百分比）。没有默认值。

#### Sigma SLA

Sigma 服务级别协议（数值）。Sigma 分数是根据每百万次采样数的缺陷率 (DPMO) 进行计算的度量方式。可接受的 Sigma 分数可能为 4.00，接近完美的分数为 6.00，完美（零个事务缺陷）的分数为无穷大。没有默认值。

#### 事务处理时间 SLA

事务处理时间服务级别协议（秒）。没有默认值。

5. 单击“保存”。

此时新的关联 SLA 显示在列表中。

**注意：**在创建新的关联 SLA 时，现有的关联 SLA 不会更改。例如，如果您已经拥有用户组 A (UG-A)、业务服务 X (BP-x) 和业务事务 3 (BT-3) 的关联 SLA，则为 UG-A、PB-x 和所有业务事务创建新业务服务不会更改先前定义的 SLA（针对 UG-A/BT-x/BT-3）。

**注意：**如果您先为业务服务中的所有业务事务创建关联 SLA，此后添加另外一个业务事务，请记住为该添加的业务事务创建新 SLA。（系统不会自动为该业务事务添加 SLA。）

## 更新现有的关联 SLA

要更改现有的关联 SLA，请使用“更新”按钮。

**要更改现有的关联 SLA，请执行以下操作：**

1. 选择“管理”、“关联 SLA”。
2. 选择要修改的关联 SLA。（使用“显示”、“业务服务”、“用户组”列表和“刷新”可显示您要更改的关联 SLA。）
3. 单击“更新”。
4. 设置字段以指定要更改的关联 SLA。

5. 设置 SLA 值。
6. 单击“更新”。

此时更新的关联 SLA 显示在列表中。

## 删除关联 SLA

如果您不再需要某个关联 SLA，可将其删除。

### 删除关联 SLA:

**警告!** 单击“删除”会立即删除 SLA。删除时不会显示“确定?”对话框。

1. 选择“管理”、“关联 SLA”。
2. 选择要删除的关联 SLA。
3. 单击“删除”。

## 删除用户组

您可以删除用户组及其所有相关事务统计信息。在发生以下情况时，您可能需要执行上述操作：

- 办事处关闭并且您不再需要该组的事务信息时
- 您要合并组时：将用户从一个组移到另外一个组，然后删除空组
- 自动创建用户组过程所创建的用户组超过您需要的数量时

**重要信息!** 删除不需要的用户组，包括不含用户的用户组。用户组太多可能对性能产生负面影响。

### 删除用户组:

1. 选择“管理”>“用户组”。
2. 在“用户组”选项卡上，选中要删除的用户组对应的复选框。
3. 单击“删除”。



## 停用或删除用户

如果您知道用户在较长的一段时间内不会被 CA CEM 监控,则可以暂时停用这些用户。在这种情况下,事务历史和用户记录都予以保留。如果 CA CEM 观测到任何已停用用户的新事务,会自动重新激活该用户。

在您删除用户时,仅保留用户的事务历史。管理页面上不会显示已删除的用户。用户的历史在报告中灰显。如果 CA CEM 观测到任何已删除用户的新事务,会创建一个新用户。只有当您确信用户不会再次使用您正在监控的应用程序时,才应删除这些用户。

### 停用或删除用户:

1. 选择“管理”>“用户组”。
2. 单击“用户搜索”,搜索您需要停用或删除的特定用户。
3. 检查您要停用或删除的用户。
4. 单击“停用”或“删除”。

## 重新激活用户

如果您以前停用了某个用户,现在要重新激活该用户:

### 要激活用户,请执行以下操作:

1. 选择“管理”>“用户组”。
2. 单击“用户搜索”,搜索您需要激活的特定用户。
3. 选中您要激活的用户。
4. 单击“激活”。



# 第 20 章：在 CA CEM 上管理系统操作

---

本章介绍了为确保 CA CEM 正常工作（如检查错误报告以及检查磁盘空间和内存）管理员需要执行的任务。

以下列表显示了您需要了解的有关 CA CEM 监控事件和查看 CA CEM 审核路径的内容：

1. [了解 CA CEM 事件](#) (p. 291)。
2. [检查 CA CEM 事件](#) (p. 294)。
3. [维护必需的 CA CEM 事件](#) (p. 294)。
4. [将 CA CEM 配置为发送电子邮件通知事件，如错误和警告](#) (p. 294)。
5. [检查信息，例如 TIM 计算机的内存使用情况和磁盘空间](#) (p. 296)。
6. [检查 CA CEM 审核路径](#) (p. 297)。

## 关于 CA CEM 事件

CA CEM 会捕获并记录事件，因此您可以即时了解可能影响系统运行和性能的事件。建议您定期复查事件日志。

### 重要级别

事件有三个重要级别：

- 信息
- 警告
- 错误

## 可能事件列表

CA CEM 捕获并记录以下系统事件：

| 事件            | 重要级别 | 类别        | 详细信息  |
|---------------|------|-----------|---|
| 业务应用程序名称无效    | 错误   | CA APM TG | CA APM TG 脚本中的业务应用程序名称包含无效字符，例如 < 或 >。在 CA APM TG 中，更正 CA CEM 应用程序名称并再次迁移脚本。  |
| 数据库清除服务已启动    | 参考性  | 正在处理      | 数据库清除服务已启动。运行服务的企业管理器的 IP 地址在事件列表中提供。   |
| 数据库清除服务已停止    | 参考性  | 正在处理      | 数据库清除服务已停止。运行服务的企业管理器的 IP 地址在事件列表中提供。   |
| 缺陷已丢弃         | 警告   | 正在处理      | 突发事件报告性能处理超载，因而一个或多个缺陷被丢弃。  |
| 检测到重复会话 ID    | 警告   | 监控        | 可能原因：<br>两个或多个 TIM 正在监控同一流量。<br>多个登录拥有相同的会话 ID。（可表示用于会话标识的参数有问题。）   |
| 企业管理器无法访问 TIM | 错误   | 通讯        | 企业管理器无法访问 TIM 以检索数据。  |
| 企业管理器已重新启动    | 参考性  | 管理        | 重新启动企业管理器的日期和时间。  |
| HTTP 分析程序插件错误 | 错误   | 正在处理      | HTTP 分析程序插件出现故障。  |
| 已超过添加新组件的限制   | 警告   | 正在处理      | 仅当选中“发现新的非标识组件”时才发生此事件。<br>当超过非标识组件的最大数时，新组件会替换最旧的组件。每次发生此情况时，系统都会记录“已超过添加新组件的限制”事件。<br>有关自动发现组件的信息，请参阅《CA APM 事务定义指南》。 |
| 登录已丢弃         | 警告   | 正在处理      | 由于性能处理超载，一次或多次登录被丢弃。  |

| 事件                       | 重要级别 | 类别        | 详细信息  |
|--------------------------|------|-----------|---|
| 无网络数据                    | 警告   | 通讯        | TIM 在一段时间内没有通过网络收到任何数据。例如，可能移动了电缆，未正确配置网络交换机或网络拓扑已经更改，因而不符合 CA CEM 配置。  |
| 统计聚合服务已启动                | 参考性  | 正在处理      | 统计聚合服务已启动。运行服务的企业管理器的 IP 地址在事件列表中提供。  |
| 统计聚合服务已停止                | 参考性  | 正在处理      | 统计聚合服务已停止。运行服务的企业管理器的 IP 地址在事件列表中提供。  |
| TIM 收集服务已启动              | 参考性  | 正在处理      | TIM 收集服务已启动。运行服务的企业管理器的 IP 地址在事件列表中提供。  |
| TIM 收集服务已停止              | 参考性  | 正在处理      | TIM 收集服务已停止。运行服务的企业管理器的 IP 地址在事件列表中提供。  |
| TIM 删除了它的一些数据文件，因为磁盘空间不足 | 参考性  | 管理        | TIM 删除了它的一些数据文件以保护磁盘空间。默认情况下，当磁盘的已用空间达到全部磁盘空间的 75% 时，将删除文件。该行为由“TIM 设置”页面上的 DiskSpace/MinFreeDataSpaceInPercent 确定。 |
| TIM 已重新启动                | 参考性  | 管理        | 重新启动 TIM 的日期和时间。  |
| 事务定义已丢弃                  | 参考性  | 正在处理      | 该事件仅在自动事务发现处于开启状态时才发生。此事件意味着，某些自动发现的事务定义会因性能处理超载而被丢弃。如果您看到该事件，请考虑关闭自动事务发现，然后在其他时间运行。                                |
| 已达用户组限制                  | 警告   | 正在处理      | 用户组报告，已达到按 IP 子网自动创建的用户组的最大数量。  |
| WTG 代理关闭                 | 警告   | CA APM TG | CA APM TG 代理不可用。  |
| WTG 代理运行                 | 参考性  | CA APM TG | CA APM TG 代理可用。   |

## 查看 CA CEM 事件

您可以定期监控 CA CEM 事件，查找网络问题、系统或备份故障以及 HTTP 分析程序插件错误的征兆。

**请执行以下步骤：**

1. 选择“系统”>“事件”。  
此时将显示 CA CEM 事件列表。
2. 单击事件名称查看更多信息。  
此时将显示事件详细信息页面。
3. 选择“系统”>“事件”返回事件列表。

## 管理 CA CEM 事件

您可以指定保留事件的天数。

**请执行以下步骤：**

1. 选择“系统”>“事件”，然后单击“事件管理器”选项卡。  
此时将显示 CA CEM 事件的当前设置。

2. 定义事件设置：

### 删除事件晚于

CA CEM 事件可从事件日志中删除之前需经过的天数。

3. 单击“保存”。

## 接收事件的电子邮件通知

您可以将 CA CEM 配置为在发生事件时发送电子邮件通知。

您至少应将事件电子邮件通知设置为 CA CEM 管理员接收错误事件的电子邮件通知。

可以指定以下内容：

- 用于接收通知的电子邮件地址。
- 通知的事件。
- 邮件的主题和正文。

**将 CA CEM 配置为发送事件的电子邮件通知:**

1. 选择“系统” > “事件”，然后单击“事件管理器”选项卡。

此时将显示 CA CEM 事件的当前设置。

2. 选中“事件电子邮件通知”复选框。

此时将显示“事件通知设置”。

3. 选中您要启用（或禁用）电子邮件通知的每个事件旁边的复选框。

该复选框是一个切换选项。如果状态当前为“已禁用”，选中该复选框并单击“保存”将为该事件启动电子邮件通知（并且状态变为“已启用”）。如果状态当前为“已启用”，选中该复选框并单击“保存”将为该事件停用电子邮件通知（并且状态变为“已禁用”）。

**注意：**状态字段指示事件的 *电子邮件* 通知是启用还是禁用。所有事件（无论其电子邮件通知状态为何）都会显示在“事件”页面上。

4. （可选）如果您只想从企业管理器和 TIM 的子集接收电子邮件通知，请指定 IP 地址范围。

例如，如果您要查看有关企业管理器而非 TIM 的电子邮件通知，请指定包含企业管理器地址但不包含 TIM 地址的 IP 地址范围。

5. 编辑电子邮件的“发件人”地址和“收件人”地址（如果需要）。

6. （可选）编辑“消息”字段。使用以下变量可创建自定义说明：

- <id>
- <name>
- <severity>
- <category>
- <源>
- <ipaddress>
- <desc>
- <time>

您可以重新排列变量来创建自己的消息。每个变量都被发送电子邮件通知时的实际事件值取代。

**提示：**您可以将示例区域中的变量和文本复制并粘贴到消息字段。

7. 单击“保存”。
8. 确保 SMTP 服务器设置正确。请参阅[配置 SMTP 服务器设置](#) (p. 268)。

## 检查TIM 计算机的运行状况

在例行维护和排除故障时，您应检查 TIM 计算机的运行状况。这包括检查计算机上的磁盘和内存使用情况以及正在运行的进程。

**注意：**您需要访问 Wily 的系统设置页面才能查看这些运行状况报告。

### 查看 TIM 计算机的运行状况快照：

1. 选择“设置” > “监视器”。
2. 单击“获取报告”（在最右侧的“TIM 运行状况”列中）。
3. 如果显示登录对话框，请使用您的用户名和密码登录 Wily 系统设置页面；此登录的默认用户名是 `admin`。  
此时将显示“设备运行状况”页面。
4. 单击“完整的设备运行状况”链接。  
或者，单击其他链接之一查看运行状况报告的其中一部分。  
有关每个链接的详细信息，请参阅[设备运行状况页面参考表](#) (p. 296)。
5. 为每个 TIM 计算机，重复上述步骤。

## 设备运行状况页面参考表

该表描述“设备运行状况”页面上每个链接所提供的信息。

| 链接   | 信息  | 等效的 Linux 命令         |
|------|---|----------------------|
| 磁盘信息 | 显示文件系统磁盘空间使用情况（以 MB 为单位）。<br>如果磁盘使用率太高，超过 80%，请通过删除 TIM 日志文件来降低磁盘空间使用率。                           | <code>df -m</code>   |
| 内存信息 | 显示系统中可用和已用的内存量（以 MB 为单位）。<br>如果可用内存量变低，则留意过度内存交换（抖动）。<br>在 TIM 上，插件最有可能引起抖动。您可能需要修改插件代码才能改善内存使用率。 | <code>free -m</code> |



|           |  |                  |
|-----------|--|------------------|
| 登录用户      | 显示登录到计算机本身的任何用户。通常，您不应看到任何用户。然而，您可能会看到已登录到计算机的 <b>root</b> 用户，例如，通过安全 shell (ssh) 登录的用户。如果您看到任何您无法识别的用户，请立即进行调查。 | who              |
| 当前正在运行的进程 | 显示每个正在运行的进程。(使用标准语法和 <b>CMD</b> 列表中的 <b>ASCII</b> 字符显示可指示进程路径。) 在该列表中，查找异常高的 <b>CPU</b> 使用率和意外的进程。               | ps -efl --forest |
| 完整的设备运行状况 | 显示所有上述信息。  | 见上文              |

## 查看 CA CEM 审核路径

CEM 管理员可以查看 CA CEM 活动的审核路径。

您可以在管理详细信息页面上查看 CA CEM 活动。列表页面上不提供审核信息。

### 查看审核路径信息：

- 选择要审核的管理页面之一。
  - “管理” > “业务服务”
  - “设置” > “域”
  - “系统” > “电子邮件设置”
- 在地址中，将 **&showHistory=true** 或 **?showHistory=true** 添加到 URL 的末尾。（使用与号 (&) 或问号 (?)。）
  - 如果 URL 末尾的内容与 **.html?pid=600001** 类似，应使用和号：

```
http://<IP_Address>:8081/wily/cem/tess/app/admin/transDefGroupList.html?pid=1&showHistory=true
```

```
http://<IP_Address>:8081/wily/cem/tess/app/admin/domainDetail.html?pid=1&showHistory=true
```
  - 如果 URL 以 **.html** 结尾，请使用问号：

```
http://<IP_Address>:8081/wily/cem/tess/app/system/emailSettings.html?showHistory=true
```

3. 单击“执行”或按 Enter 以查看审核路径。  
审核路径显示在页面的底部。
4. 向下滚动页面以查看 Wily CEM 审核信息。系统会显示最新的 200 条更改。
5. 如果要覆盖显示 200 条记录的默认值，可以将 `&maxResults=nnn` 添加到查询字符串的末尾。

例如：

```
http://<IP_Address>:8081/wily/cem/tess/app/system/emailSettings.html?showHistory=true&maxResults=500
```

# 第 21 章： CA CEM 报告

---

以下列表显示了需要了解的有关 CA CEM 报告的内容：

1. [了解 CA CEM 报告以及当您在系统中导航时如何捕获这些报告](#) (p. 299)。
2. [定期排定所需的 CA CEM 报告](#) (p. 305)。

## 捕获 CA CEM 报告

可以通过多种方式分析 CA CEM 数据。您可以在 CA CEM 菜单中导航，并且基于业务服务、业务事务、用户组以及按突发事件和缺陷执行查询。

报告选项因您所选择的报告类型而异。例如，如果选择趋势报告，则需要指定主次时限以在趋势分析中比较。

有关报告输出供选方案的信息，请参阅[报告交付](#) (p. 300)。

有关可用报告的信息，请参阅[报告格式](#) (p. 301)。

您的 CA CEM 系统数据保留选项和统计信息聚合日程表可能影响报告输出。有关详细信息，请参阅[报告时限](#) (p. 302)。

## 关于 CA CEM 报告聚合

CA CEM 聚合会影响报告中显示的数据。了解 CA CEM 如何聚合每日、每周、每月和每年的统计信息。

CA CEM 报告基于已聚合的业务事务统计信息。CA CEM 每小时运行一次包含每小时聚合的统计信息处理。

CA CEM 每天运行一次（午夜，每小时统计信息聚合过程完成之后）：

- 每日聚合处理
- 每周聚合过程
- 每月聚合过程

出于性能原因，每天聚合一次是最佳方法，不过需要注意对报告的影响。例如：

- 如果您在今天下午 5 点运行每周报告或每月报告，则报告统计信息包含截至午夜的数据。该报告不包含今天的统计信息。
- 如果运行“统计聚合服务”的企业管理器在午夜未运行，则聚合处理不运行（直到下次企业管理器在午夜运行时才运行）。因此，如果您要查找昨天的统计信息，则它们未包含在每日（昨天时限）、每周、每月或每年报告中。
- 从“今日”时限报告生成报告统计信息花费的时间比从每日聚合数据生成报告统计信息花费的时间稍长。
- 每年报告基于每月聚合数据。

## 报告交付

CA CEM 允许您通过多种方法捕获和管理 CA CEM 报告：

- 在您查询 CA CEM 数据时在线查看报告
- 查看“我的报告”列表中预定义的报告
- 创建 PDF 文件，您可以保存或打印该文件
- 通过电子邮件将 PDF 文件发送给一个用户或一组用户
- 保存报告，以后可以运行和查看该报告
- 排定报告，以便定期（每日、每周或每月）运行或通过电子邮件发送报告

## 保护报告数据

如果使用安全组来限制 CA CEM 用户对业务服务和关联数据的访问，则验证您是否仅具有 **Embedded Entitlements Manager** 安全领域。

如果存在多个领域（例如，本地领域和 **Embedded Entitlements Manager** 领域），则 CA CEM 用户能够在没有访问权限的已排定报告中看到数据。

有关配置领域的信息，请参阅《*CA APM 安全指南*》。

## 报告格式

当您在 CEM 选项卡的以下页面上导航时，可以捕获 CA CEM 报告：

- 服务级别管理
  - 事务 SLA—性能和质量
  - 用户 SLA—性能和质量
  - 关联 SLAs
  - 事务趋势—性能和质量
  - 用户趋势—性能和质量
  - 业务价值
- 事件管理
  - 突发事件
  - 主要影响因素
  - 缺陷
  - 事务跟踪会话
- 性能报告
  - 业务服务
  - 用户组
- 质量报告
  - 业务服务
  - 用户组
- 分析图
  - 成功率
  - time
  - 吞吐量
  - 大小
  - 量
  - 计数
  - 产出率
  - 缺陷—频率
  - 会话使用情况

## 报告时限

CA CEM 允许您通过多种方式指定报告视图时限：

| 时限 | 当前  | 上一页  | 自定义   |
|----|-----|------|-------|
| 小时 | N/A | 前一小时 | 自定义小时 |
| 日  | 今天  | 昨天   | 自定义日  |
| 周  | 本周  | 上周   | 自定义周  |
| 月  | 本月  | 上个月  | 自定义月  |
| 年  | 本年  | 上一年  | N/A   |

**注意：**当您选择报告时限和指定排定的报告时，请考虑 CA CEM 系统聚合和数据保留设置，这非常重要。如果统计信息尚未聚合、数据已被清除或突发事件设置已被更改，则您的报告将不是您所期望的报告。

CA CEM 管理员可将系统配置为保留生成报告所需的数据。不过，为获得最佳的系统性能，必须定期清除 CA CEM 统计信息。有关数据保留设置的详细信息，请参阅[定义 CA CEM 域](#) (p. 253)。

CA CEM 系统聚合数据，保留每小时、每天、每周和每月的统计信息。聚合也是用于性能和可伸缩性的工具。有关 CA CEM 聚合的详细信息，请参阅[关于 CA CEM 报告聚合](#) (p. 299)。

## 浏览报告

在提供报告的 CEM 页面上，您可以使用多种选项。

### PDF

PDF 链接将提供 PDF 格式的报告。您可以将报告保存为文件或打印 PDF。

### 通过电子邮件发送 PDF

“通过电子邮件发送 PDF” 链接会打开一个新页面，您可在此发送附有 PDF 报告的电子邮件。

### 保存或排定报告

“保存或排定报告” 链接指向“我的报告” 页面，您可在此保存或排定报告。

您必须先使用有效数据查询和刷新报告页面，然后才能单击这些报告选项之一。

**注意：**如果您在另外一个 CEM 报告页面打开后（例如，使用浏览器的“在新窗口中打开” 选项），单击 CEM 报告页面上的 PDF 链接，将出现错误。返回第一个 CEM 报告页面，单击“刷新”，然后再次单击 PDF 链接。

## PDF 报告

PDF 链接会打开 Adobe Acrobat PDF 格式的报告，您可以将其保存为文件或进行打印。

### 要打印该报告，请执行以下操作：

1. 在 Internet Explorer 中，单击“文件” > “打印” 打印 PDF 格式的报告。
2. 单击“后退” 按钮，返回到上一页面。

### 要将报告保存为文件，请执行以下操作：

1. 在 Internet Explorer 中，单击“文件” > “另存为”。
2. 浏览您要保存报告的位置。为报告键入适当的“文件名”。单击“保存” 将报告保存至文件。

**注意：**如果未更改该名称，则名称为 *Wily CEMReport.pdf*。

3. 单击“后退” 按钮，返回到上一页面。

要在 PDF 报告上使用自己的徽标，请执行以下操作：

- 替换 APM 数据库 ts\_settings 表中的 reports.userImage。

**注意：**您不得在通过电子邮件发送的报告中使用您的徽标。

## 电子邮件报告

电子邮件链接允许您发送 PDF 格式的报告。系统会打开一个包含电子邮件表单的新窗口。

**通过电子邮件发送报告：**

1. 完成该电子邮件表单。

### 发件人

这是已登录用户的电子邮件地址。如果未提供电子邮件地址，则使用可能从 tess-default.properties 文件中的 email.defaultFromAddress 填充的地址（[默认 tess-default.properties 文件](#) (p. 513)）。

### 收件人

输入逗号分隔的列表：电子邮件地址或分发列表。

**注意：**请勿使用分号分隔电子邮件地址。

### 主题

为附加的报告输入有意义的主题行。

### 消息

将适当的信息添加到报告的标准消息中。

2. 单击“发送”。

**注意：**如果您要通过电子邮件发送报告，CEM 系统管理员需要配置邮件 SMTP 服务器。

## 已保存或已排定的报告

“保存或排定报告”和“我的报告”功能允许您将报告设置为定期（每日、每周或每月）运行。CA CEM 系统会在指定的时间生成并通过电子邮件发送报告。

有关详细信息，请参阅[排定报告](#) (p. 305)。



## 排定报告

在 CA CEM 中可通过两种方式排定报告：

- [在“我的报告”中定义和排定您的报告](#) (p. 305)。
- [生成所需的报告，然后排定该报告](#) (p. 307)。

### 使用“我的报告”排定报告

本节介绍了如何通过“我的报告”手工排定报告。

**请执行以下步骤：**

1. 选择“CEM” > “我的报告”，然后单击“新建”。
2. 从列表中选择“报告格式”。每个报告格式都需要附加信息，这些信息因您的选择而异。

有关详细信息，请参阅[报告格式](#) (p. 301)。

“业务价值”报告需要：

#### **业务应用程序**

选择特定的业务应用程序或选择“全部”。

#### **业务服务**

选择特定的业务服务或选择“全部”。

#### **时限**

指定小时、天、周、月或年。

#### **安排该报告的 PDF 版本通过电子邮件发送**

(可选) 选择该选项可排定通过电子邮件发送此报告。

有关详细信息，请参阅[报告时限](#) (p. 302)。

“用户趋势质量”报告需要：

#### **业务应用程序**

选择特定的业务应用程序或选择“全部”。

#### **业务服务**

选择特定的业务服务或选择“全部”。

#### **业务事务**

您的选择因选定的业务服务而异。选择特定的业务事务或选择“全部”。

### 用户组

选择特定的用户组或选择“全部”。

### 主要时限

指定小时、天、周、月或年。这通常是当前时限，例如本周。

### 次要时限

指定小时、天、周、月或年。这通常是先前的时限。例如，您可以比较今天与昨天；或比较本周与上周，或比较上个月、去年。

### 安排该报告的 PDF 版本通过电子邮件发送

(可选) 选择该选项可排定通过电子邮件发送此报告。

## 3. 确定所需的报告运行频率。

### 每日

选择每日要运行报告的时间。

### 每周

选择每周要运行报告的日期和时间。

### 藩竣

选择每月要运行报告的日期和时间。

**重要信息!** 如果您选择的日期在给定的月份中不存在，则该月不发送报告。例如，如果您选择 31 号，则在小于 31 天的月份内不发送报告。

## 4. 确定希望运行报告的时间；设置重复周期时间。

**提示:** 如果您希望报告包含上一小时的数据，则将报告排定为推迟一小时是个好方法，这便为完成统计信息处理留出时间。

有关 CA CEM 聚合的详细信息，请参阅[关于 CA CEM 报告聚合](#) (p. 299)。

## 5. 定义电子邮件设置。

**提示:** 为了防止客户对报告存在疑问，建议通过主题行和消息让报告收件人知道报告的类型、报告的运行频率和联系人姓名。

### 发件人地址

输入发送报告的发件人电子邮件地址。您可以更改该地址，例如，您希望报告收件人回复到其他电子邮件地址。

### 发件人名称

输入与电子邮件地址关联的姓名；这通常是您的姓名，或 CA CEM 负责用户的姓名。

### 收件人

输入逗号分隔的列表：电子邮件地址或分发列表。

### 主题

为该报告输入有意义的主题行。

### 消息

为该报告输入有用的消息。

6. 单击“保存”。您的新报告显示在报告的列表中。

所有 CA CEM 用户都能看到他们自己创建的报告；只有 CA CEM 系统管理员才能看到其他 CA CEM 用户创建的报告。

**提示：**如果您以一致的方式对您的所有报告命名，便可轻松地找到您需要的报告。例如，所有报告名称可能包括：

- 包括业务应用程序、服务和事务
- 包括用户组
- 频率

## 生成和排定报告

本节提供一个示例，介绍在使用您所需的选项生成报告后如何排定该报告。

### 要生成和排定报告，请执行以下操作：

1. 转至所需的页面，然后以所需的方式生成报告视图。例如：
  - a. 选择“CEM” > “服务级别管理” > “用户趋势”。
  - b. 选择要在报告中查看的“用户组”、“业务应用程序”、“业务服务”以及“业务事务”。
  - c. 选择主次时限。
  - d. 单击“质量”查看用户组的质量报告。
  - e. 单击“刷新”更新质量报告页面。
  - f. 单击“保存或排定报告”。此时显示“我的报告”页面，您刚查看的“用户趋势质量”报告预填充了所有“报告设置”。
2. 根据需要修改预填充的报告设置。
3. 选中复选框“将该报告的 PDF 版本排定为通过电子邮件发送”。此时显示“重复周期”和“电子邮件设置”选项。
4. 根据需要定义重复周期设置。

5. 根据需要定义电子邮件设置。
6. 单击“保存”排定该报告。

有关报告排定选项的详细信息，请参阅[使用“我的报告”排定报告](#) (p. 305)。

## 导出 CA CEM 数据

可以从“导出数据”选项卡中导出 CA CEM 数据。通过该选项卡，您可以检索业务统计信息、缺陷和突发事件数据。

您可以导出以下内容的 CA CEM 数据：

- 指定时间范围内的合计业务统计信息和非合计业务统计信息。
- 指定时间范围内的缺陷、最后  $N$  个缺陷或最后  $X$  分钟的缺陷。
- 指定时间范围内的突发事件。

**注意：**在电子商务模式下，无法导出统计数据中的用户信息。

## 导出数据

本节提供了如何导出 CA CEM 数据的示例。

**请执行以下步骤：**

1. 单击“CEM”、“导出数据”，然后单击“统计数据”。  
此时将显示“统计数据”视图。
2. 指定下列选项的组合：
  - a. 选择要在数据中查看的“报告类型”、“业务应用程序”、“业务服务”和“业务事务”。

- b. 选择“用户组”或“用户”。

**注意：**如果您选择“非聚合”报告类型，则只能选择“用户组”。

- c. 指定“开始日期”和“结束日期”。

**注意：**默认情况下，显示当前的系统日期和时间。

- d. 选择一个“时间间隔”，例如，对于“非聚合”报告类型，选择“每小时”、“每天”、“每周”或“每月”。

- e. （可选）指定事务的“吞吐量”、“大小”和“时间”的百分比值。

“吞吐量”、“大小”和“时间”字段表示事务的百分位值。分号用于分隔多个百分位值。例如，吞吐量 = 25; 50; 75。也可以在这些字段中指定“全部”，以包含从 5 到 95（以 5 递增）的百分位值。

**注意：**默认情况下，事务的“吞吐量”、“大小”和“时间”为 50%。

- f. 单击“保存到 CSV”。

“文件下载”对话框将打开包含统计数据的 CSV 文件。

3. 单击“CEM”、“导出数据”，然后单击“缺陷数据”。

此时将显示“缺陷数据”视图。

4. 指定下列选项的某种组合：

- a. 选择要在导出的数据中查看的“业务应用程序”、“业务服务”和“业务事务”。

- b. 选择“用户组”和“缺陷类型”。

如果选择“内容错误”缺陷类型，则可以指定要在缺陷数据中导出的内容字符串值。

- c. 指定“起始日期”和“结束日期”，或者指定“最后 N 个缺陷”（N 介于 0-1000 之间）或“最后 X 分钟”（X 介于 0-1440 之间）。

- d. （可选）指定要作为缺陷的一部分进行检索的 Meta 键。

Meta 键是在缺陷的“HTTP 响应和请求标头”中指定的值。

**注意：**使用分号分隔多个 Meta 键。Meta 键区分大小写。

- e. (可选) 对于某个缺陷业务事务, 针对“包括组件计时信息”选择“是”。
  - f. 单击“保存到 CSV”。
- “文件下载”对话框将打开包含缺陷数据的 CSV 文件。
5. 单击“CEM”、“导出数据”, 然后单击“突发事件数据”。  
此时将显示“突发事件数据”视图。
  6. 指定“开始日期”和“结束日期”。
  7. 单击“保存到 CSV”。
- “文件下载”对话框将打开包含突发事件数据的 CSV 文件。

## 保存或排定报告

您可以通过在“我的报告”选项卡中选择“缺陷数据”、“突发事件数据”或“统计数据”报告格式来保存或排定报告的 CA CEM 数据。

**注意:** CA CEM 数据的排定报告会作为 .zip 附件以电子邮件的形式发送给您。大于 800 KB 大小的 CSV 报告会分为几等份, 并且作为 .zip 附件以电子邮件的形式发送。

有关报告排定选项的详细信息, 请参阅[使用“我的报告”排定报告](#) (p. 305)。

## CSV 标头

以下部分中解释了部分 CSV 标头：

- **TransactionThroughputPercentile(Bytes/s)** - <百分位请求> 列数取决于请求的百分比数。例如，吞吐量 = 25、40、75 会为指定的每个请求百分比生成三列。如果没有指定百分比请求，那么默认情况下使用列“**TransactionThroughputPercentile - 50%**”。
- **DefectValue** 是针对特定事务产生缺陷必须满足的条件。
- 只针对缺陷类型 9 生成 **MissingID** 和 **MissingName**。**MissingID** 和 **MissingName** 表示缺少的事务组件或事务单元的 ID 和名称。
- **Cause** 表示关闭突发事件时所提供的理由。在系统关闭突发事件时，例如，在删除 BT 时，原因显示“**Business transaction was deleted**”（已删除业务事务）。
- **CloseBy** 表示关闭突发事件的用户名。
- **Evidence1**、**Evidence2** 和 **Evidence3** 表示证据收集文件的名称，当影响阈值为中等、严重和关键时会分别生成这些文件。
- 在“状态”列中，1 表示已关闭，2 表示打开，3 表示未决，4 表示过时。
- **TriggerDate** 表示突发事件的创建时间。
- 有关 **DefectType** 的详细信息，请参阅《*CA APM API 参考指南*》的“缺陷命令参数和语法”部分。
- 有关 **UserImportance**、**DefectImportance** 和 **TransactionImportance** 的详细信息，请参阅“[定义与突发事件相关的设置](#) (p. 259)”





# 第 22 章：使用 CA CEM 监控安全 Web 应用程序

---

该列表显示了设置 CA CEM 以监控使用基于 SSL 的安全机制的 Web 应用程序所涉及的主要任务：

1. [获取您的 Web 服务器的 SSL 私钥](#) (p. 313)。
2. [确保 SSL 私钥位于 PEM 文件中](#) (p. 313)。  
如果需要，转换私钥。
3. [针对 SSL 配置 CA CEM 并将 PEM 文件上传到 CA CEM](#) (p. 318)。
4. [验证使用 SSL 的 CA CEM](#) (p. 318)。

## 导入和管理 SSL 私钥

CA CEM 支持多个私钥，这样便可使用不同私钥分析各种 HTTPS 服务器的 SSL 流量。CA CEM 支持 PEM 私钥格式（基于 Apache 和 OpenSSL 的服务器使用该格式）。Microsoft IIS、SunONE、iPlanet 和 Netscape 使用专用格式，但您可以将这些密钥转换为 CA CEM 所使用的 PEM 文件。CA CEM 会自动识别对其所捕获的数据进行解密所需的密钥。

用于执行转换的系统上必须提供一个 OpenSSL 版本。可从 <http://www.openssl.org> 获得 OpenSSL。

有关如何获取受支持的 Web 服务器的 SSL 私钥的详细信息，请参阅：

- [基于 Apache 或 OpenSSL 的 Web 服务器](#) (p. 313)。
- [Microsoft Internet Information Service \(IIS\)](#) (p. 314)。
- [SunONE、iPlanet 或 Netscape 企业服务器](#) (p. 315)。

## 保存基于 Apache 或 OpenSSL 的 Web 服务器私钥文件

您可以保存基于 Apache 或 OpenSSL 的 Web 服务器私钥文件，以便可与 CA CEM 一起使用。

请执行以下步骤：

1. 找到服务器的配置文件。例如：

```
/etc/httpd/conf.d/ssl.conf
```

2. 查找 SSL 证书密钥文件，其指向私钥文件。例如：

```
SSLCertificateKeyFile=/etc/httpd/conf/ssl.key/server.key
```

3. 复制并将该文件重命名为 `output.pem`。

有关详细信息，请参阅：<http://httpd.apache.org/> 和 <http://www.openssl.org/>

## 导出并转换 Microsoft Internet Information Service (IIS) 私钥

Microsoft Internet Information Service (IIS) 私钥必须导出为 CA CEM 可读的格式。此格式为 PFX。用于执行转换的系统上必须提供一个 OpenSSL 版本。您可以从 <http://www.openssl.org/> 获取 OpenSSL。

首先，从 IIS 服务器导出私钥，然后将输出文件转换为 PEM 格式。

### 以 PFX 格式导出密钥：

1. 在运行 IIS 的基于 Windows 的系统上，单击“开始”，然后单击“运行”。
2. 键入 `MMC.exe` 并单击“确定”。
3. 单击“控制台”菜单，然后单击“添加/删除管理单元”。
4. 单击“添加”。选择“证书”管理单元，然后单击“添加”。
5. 选择“计算机帐户”并单击“下一步”。
6. 选择“本地计算机”并单击“确定”。
7. 单击“关闭”，然后单击“确定”。
8. 展开“证书”菜单，然后单击“个人”文件夹。右键单击要导出的证书并选择“所有任务” > “导出”。

此时将显示向导。

9. 要包含私钥并继续完成向导直到获得 PFX 文件为止，请选择该框。

**将 PFX 文件转换为 PEM 密钥文件:**

1. 在运行 OpenSSL 软件的系统上执行以下命令。

```
openssl pkcs12 -in filename.pfx -nocerts -out output.pem
```

2. 将 *filename.pfx* 替换为您创建的文件名称。
3. 将 *output.pem* 替换为您正在创建的输出文件的名称。
4. 执行该命令。

在创建该 PEM 文件时指定的密码是您将该文件上传至 TIM 时所用的密码短语。

## SunONE、iPlanet 或 Netscape 企业服务器

Sun、SunONE、iPlanet 和 Netscape Web 服务器全都基于相同的核心技术。它们的私钥必须导出为 CA CEM 可读取的格式。

用于执行转换的系统上必须提供以下实用工具:

- OpenSSL
- Network Security Services (NSS)
- Netscape Portable Runtime (NSPR)

以下步骤假定某个 Windows 系统将用于转换。

**创建私钥文件:**

1. 下载并解压密钥管理实用工具:
  - 可从 <http://www.openssl.org> 获得 OpenSSL
  - Network Security Services (NSS) 可从 <http://www.mozilla.org/projects/security/pki/nss/> 获得
  - Netscape Portable Runtime (NSPR) 可从 <http://www.mozilla.org/projects/nspr/> 获得
2. 提取文件。
  - 将 ZIP 文件提取到临时目录中。
  - 将 nss-3.9.zip 提取到 c:\。
  - 将 nspr-4.4.1 提取到 c:\。
3. 适用于 **Win32-OpenSSL-v0.9.7c**: 运行 Win32-OpenSSL-v0.9.7c 并且安装在 C:\OpenSSL 目录中。

4. 修改 PATH 变量，以便它包括下列行：

```
c:\nss-3.9\lib;c:\nspr-4.4.1\lib
```

SunONE/iPlanet/Netscape 证书和密钥存储在扩展名为 `.db` 的文件中。

5. 将 `*.db` 文件复制到可写目录（在本例中，该目录为 `c:\dbfiles`）。
6. 打开命令提示符并键入：

```
cd c:\nss-3.9\bin
```

默认情况下，NSS 工具查找名为 `key3.db` 和 `cert7.db` 的文件。如果您的数据库文件命名为 `key3.db` 和 `cert7.db` 之外的其他名称，请不要重命名这些文件。为了让 `certutil` 和 `pk12util` 查找不合命名惯例的文件，请提供 `-P`（前缀）开关。

例如，如果您的文件命名为 `prodSite-cert.db` 和 `prodSite-key.db`，请使用 `certutil` 命令创建文件 `prodSite-cert7.db` 和 `prodSite-key3.db`。该命令的输出显示已包含的证书名称：

```
certutil -P prodSite- -K -d C:\dbfiles\
```

7. 输入 NSS 证书数据库的密码或 PIN：（输入数据库密码）。  
创建了文件 `prodSite-cert7.db` 和 `prodSite-key3.db`。

#### 执行导出和转换：

1. 在提示符下，键入：

```
pk12util -P prodSite- -d C:\dbfiles\ -o C:\dbfiles\output.p12 -n Server-Cert
```

2. 输入 NSS 证书数据库的密码或 PIN：（输入数据库密码）。
3. 输入 PKCS12 文件的密码：（输入输出密码）。
4. 重新输入密码：（重新输入输出密码）。

现在 `C:\dbfiles` 目录中包含文件名 `output.p12`。

输出密码是将该文件上传至企业管理器时所需的密码短语。

5. 在 `OpenSSL\bin` 目录中，运行以下命令：

```
openssl pkcs12 -in C:\dbfiles\output.p12 -nodes -out  
C:\dbfiles\pkcs12out.txt
```

该命令将 `pkcs12` 结构转换为包含 MAC 和包信息的文本文件。它还创建私钥和证书的 PEM 文件。

`pkcs12out.txt` 文件的内容与下面的示例类似：

```

Enter Import Password:
MAC verified OK
Bag Attributes
localKeyID: 01 00 00 00
1.3.6.1.4.1.311.17.1: Microsoft Enhanced Cryptographic Provider v1.0
friendlyName: 98849c683ad0e90810a77235bd728b12_668b93c6-0795-
4ba7-9da8-78737a299d3f
Key Attributes
X509v3 Key Usage: 10
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDLIwhdY7ngYk/A1omX9rqnaZfb8PdJ+Mc6msuRWBUDHeIH2ev1
yiL7ID/0vkUN6qGnnqvumQ3kuy7mnN/qSPz37/FKTbwF10QOP2LCZVuhU6SI/90Q
1rTINqQEpi1hyPV10lDv8Fjevvhv80jMD1gvjaCmP84FzcRi fyDgHonh4nQIDAQAB
AoGAUXaJIjjeDjge15MHNuQBUqXr+o4V/ZpA+2wcgXsbyhax0KI3FRdFFASI4XN0
Zdpo1P7oY/cdF6w5EFsvC64t7dIpD+AineQpGeYJ4whmBstyV1BShNb9drcCQDFg
vvcyfmi3tT13Mfecv3whENU6889iGogbg1MMQvqmtOCFDPY7fPM3I38FbEwO3Yu+
gWEZ/f7DLdSt7GDKf0CQQDSAqXWTmabqGB6bwxqy6M51pwBw8YAQAXpKhLILRqb
C/Jxfd63KTN90pegkhEOBn50dqTqfs4kodv45bHeHYxn
-----END RSA PRIVATE KEY-----
Bag Attributes
localKeyID: 01 00 00 00
subject=/C=US/ST=Utah/L=SLC/O=MooseCo./OU=Moose
Land/CN=www.megamoose.com
issuer=/C=US/ST=Utah/L=SLC/O=MooseCo./OU=Moose
Land/CN=www.megamoose.com
-----BEGIN CERTIFICATE-----
MIICgDCCAemgAwIBAgIDBJ3ZMA0GCSqGSIb3DQEBAUAMIGSMQswCQYDVQGEWJa
QTEVMBMGA1UECBMV2vdGvbyBiBDYXB1MRlWAEYDVQQHEW1DYXB1IFRvd24xdZAN
BgnVBAoTB1RoYXd0ZTEdMBSGA1UECxMUQ2Vydg1mawNhdGUGU2Vydm1jZXMxKDAM
BgnVBAMTH1B1cnNvbWFsIEZyZWVtYW1sIFJTSAYMDAwLjguMzAwHhcnMDEwNDE3
MDAZNzU5whcNMDIwNDE3MDAZNzU5wjbFMR8wHQYDVQQDEXZUAaG3dGUGRnJ1ZW1h
awwgTWVtYmVYMSIwIAYJKoZIhvcNAQKBFnqBGV2eUBzb25pY3dhbGwuy29tMIGf
MA0GCSqGSIb3DQEBAQUAA4Ger3DBiQKBgQDLIwhdY7ngYk/A1omX9rqnaZfb8PdJ
Y29tMAwGA1UdEwEB/wCMAAwDQYJKoZIhvcNAQEEBQADgYEACHF7eiQDoC08sna
izV22+7FwiEksR0PLcoFTyTyOUJoQ0RLt7SPqKPJ2NswyC0A2nHgnOFL7ImFGiAi
5Xg91EAtscgC7ceo0C3GBKorPE8hiqGcuVc1YKLws7YGRWRPTzQp7TemCoAMocv
io/6K6qiCsZupej7eYqCbogmEYU=
-----END CERTIFICATE-----

```

- 复制密钥结构并将其粘贴到扩展名为 PEM 的单独文件（例如，output.pem）中，如该示例所示。

```

-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDLIwhdY7ngYk/A1omX9rqnaZfb8PdJ+Mc6msuRWBUDHeIH2ev1
yiL7ID/0vkUN6qGnnqvumQ3kuy7mnN/qSPz37/FKTbwF10QOP2LCZVuhU6SI/90Q
1rTINqQEpi1hyPV10lDv8Fjevvhv80jMD1gvjaCmP84FzcRi fyDgHonh4nQIDAQAB
AoGAUXaJIjjeDjge15MHNuQBUqXr+o4V/ZpA+2wcgXsbyhax0KI3FRdFFASI4XN0
Zdpo1P7oY/cdF6w5EFsvC64t7dIpD+AineQpGeYJ4whmBstyV1BShNb9drcCQDFg
vvcyfmi3tT13Mfecv3whENU6889iGogbg1MMQvqmtOCFDPY7fPM3I38FbEwO3Yu+
gWEZ/f7DLdSt7GDKf0CQQDSAqXWTmabqGB6bwxqy6M51pwBw8YAQAXpKhLILRqb
C/Jxfd63KTN90pegkhEOBn50dqTqfs4kodv45bHeHYxn
-----END RSA PRIVATE KEY-----

```

## 针对 SSL 配置 CA CEM

请执行以下步骤：

1. 选择“设置” > “HTTPS 设置”。
2. 选择地址类型。
3. 根据您选择的地址类型指定以太网或 Web 服务器 IP。  
对于 Web 服务器 IP，输入单个地址或地址范围。  
范围输入示例，172.16.10.2-172.16.10.15  
通过不带空格的一个连字符分隔两个地址。
4. 指定 Web 服务器端口号。
5. 浏览 output.pem 文件的位置（在您的客户端计算机上）并选择它。  
要将私钥文件转换成 PEM 格式，请参阅[导入和管理 SSL 私钥](#) (p. 313)。
6. 将您用来创建 PEM 文件的密码输入到“密钥文件密码短语”字段。  
如果您没有使用密码创建 PEM 文件，请将此字段保留为空。
7. 单击“保存”上传 PEM 文件。  
如果每个 Web 服务器都有不同的 output.pem 文件，请对每个 Web 服务器重复这些步骤。

## 关于 HTTPS 服务器的多个密钥

一个 HTTPS 服务器或一组 HTTPS 服务器可以支持多个私钥，前提是每个密钥都有不同的端口或地址。例如，您可以有一个 HTTPS 服务器，一个密钥用于内部用户，另一个密钥用于外部用户。在这种情况下，您可以将一个端口用于内部密钥，另一个端口用于外部密钥。

如果您对同一个地址（或地址范围）/端口对再输入一个密钥，第一个密钥就会被覆盖。如果您的地址范围出现重叠，那么密钥会被单独保留。但是，TIM 仅使用一个密钥，即其发现的第一个包含实际 IP 地址和端口的密钥。

## 验证使用 SSL 的 CA CEM 功能。

请执行以下步骤：

1. [通过 CEM 控制台](#) (p. 229) 访问“TIM 系统设置”页面。
2. 单击“查看 TIM 事务检查”。

3. 输入 TIM 要监控的计算机的 IP 地址。
4. 单击“开始”开始监控定义为 SSL 的事务。
5. 执行简单的 HTTPS 事务（您之前定义的事务）。  
几秒钟后，事务检查数据显示在页面上。
6. 事务检查完成后，单击“停止”。

**注意：**如果您不单击“停止”，系统会继续收集检查数据。





# 第 23 章：将 Napatech 适配器用于 CA CEM

---

安装 Napatech 适配器可以改善一些高流量环境的 TIM 性能。

此部分包含以下主题：

[关于将 Napatech 适配器用于 CA CEM](#) (p. 321)

[获得 Napatech 适配器和软件](#) (p. 321)

[安装 Napatech 适配器和 Napatech 软件](#) (p. 322)

[启用 Napatech 适配器并监控](#) (p. 323)

[\(可选\) 创建和启用 Napatech 筛选](#) (p. 323)

[其他 Napatech 适配器任务](#) (p. 326)

[排除 Napatech 适配器故障](#) (p. 328)

## 关于将 Napatech 适配器用于 CA CEM

在 TIM 计算机中安装适配器可以防止 TIM 丢弃数据包。工作原理如下：

- 适配器缓冲区存储数据包，直到 TIM 可以处理它们为止。
- 适配器可以筛选流量，以便 TIM 分析更少的流量。
- CPU 从 Napatech 适配器读取数据的时间比从大多数其他以太网适配器读取数据的时间要短，从而留给 TIM 更多的 CPU 时间。

适配器可以删除重复数据包—这个功能在 SPAN 端口多次发现相同的数据包时很有用。

将 Napatech 适配器用于 TIM 的过程如下所示：

1. [获得正确的适配器和软件。](#) (p. 321)
2. [安装适配器和软件。](#) (p. 322)
3. [配置 TIM 以使用适配器。](#) (p. 323)
4. [\(可选\) 为适配器创建和启用筛选。](#) (p. 323)

## 获得 Napatech 适配器和软件

Napatech NT4E-4T PCIe 适配器包含四个千兆位电子接口，它是唯一为 TIM 支持的适配器。该适配器无法与光缆一起使用。

Network Allies, LLC 是唯一一家可以提供您需要的正确适配器和 Napatech 软件的经销商。此 Napatech 软件仅仅适用于 NT4E-4T PCIe 适配器。

**注意：**运行在多端口监视器设备上的 TIM 支持不同的 Napatech 适配器。有关支持的适配器的详细信息，请参阅《CA APM 兼容性指南》（从 CA Support 中获得）。

要获得 Napatech 适配器和 Napatech 软件，请执行以下操作：

- 从 Network Allies 购买 NT4E-4T PCIe 适配器，部件号为 801-0075-0800CA。  
包装中包含 DVD 和 USB 闪存驱动器以及相应的软件和安装说明。

## 安装 Napatech 适配器和 Napatech 软件

DVD 和 USB 闪存驱动器包含：

- Napatech 硬件安装说明
- 在 TIM 上安装的软件映像
- 示例筛选文件

### 安装适配器

1. 按照 DVD 和 USB 闪存驱动器上提供的《NT4E-4T 硬件安装指南》中的说明执行操作。将适配器安装到 TIM 计算机的 PCI Express 插槽。
2. 将流量监控电缆从监控端口（通常是 eth1）移到适配器中的任何其他端口。

**注意：**您还可以在[启用 Napatech 适配器并监控](#) (p. 323) 之后执行该步骤。稍后执行会减少数据丢失。但是，现在这样做，意味着少到服务器机房去一次。

### 安装软件

1. 创建可在网络上使用的 Napatech 软件映像 (napatech-<version>.image)。
2. 从 TIM Wily 系统设置页面安装 napatech-<version>.image。有关安装 TIM 软件的一般信息，请参阅《CA APM 安装和升级指南》。
3. （可选）通过导航到 Wily 系统设置页面，确认已安装 Napatech 软件。  
如果已安装软件，页面上会显示带项目符号的行“Napatech <installation timestamp>”。（它不是链接。）
4. （可选）检查 Napatech 驱动程序日志。
  - a. 在“TIM 系统设置”页面上，单击“配置 Napatech”。
  - b. 单击“查看 Napatech 驱动程序日志”。

c. 检查日志。

例如，如果您在此页面上的日志中看到与以下内容类似的行：

```
4B85587F.00030BC4 | #WARN | 注意：适配器的吞吐量有限。
```

```
4B85587F.00030D15 | #WARN | 链接协商为 4 通道。适配器支持 8 通道，
```

而您在四通道插槽而非八通道插槽中安装了 Napatech 适配器。这会影响 Napatech 主板的性能，但不会让其停止工作。

## 启用 Napatech 适配器并监控

在安装 Napatech 适配器和 Napatech 软件之后，请按照以下步骤启用 Napatech 适配器并配置 TIM 以监控 ntxc0:0 端口。

### 启用适配器

1. 在“TIM 系统设置”页面上，单击“配置 Napatech”。

此时将显示“TIM Napatech 配置”页面。

2. 单击“启用 Napatech”并且重新启动 TIM。

如果 TIM 未运行，单击“启用 Napatech”。启动 TIM 开始监控。

### 配置 TIM 网络监控接口以使用适配器

1. 在 TIM 系统设置页面上，单击“配置 TIM 网络接口”。

有关配置 TIM 网络监控接口的一般信息，请参阅《CA APM 安装和升级指南》。

2. 选择 ntxc0:0 接口并单击“设置”。

如果已将或计划将流量监控电缆从另一个接口移至 ntxc0:0，请清除不使用的接口对应的复选框。TIM 可以从 ntxc0:0 接口或其他接口（如 eth1）进行监控；也可以仅从 ntxc0:0 接口进行监控。

3. 如果尚未将流量监控电缆连接到适配器端口之一，请立即连接：将流量监控电缆从监控端口（通常是 eth1）移到适配器中的任何其他端口。

## （可选）创建和启用 Napatech 筛选

Napatech 适配器提供筛选硬件中数据包的方法。

筛选需使用 Napatech 编程语言 (NTPL) 编写并上传到 TIM。使用示例筛选文件。示例筛选文件位于 USB 闪存驱动器上

TIM 本身可以按 Web 服务器 IP 地址筛选流量。(有关使用此方法配置 TIM 监控的信息, 请参阅《CA APM 安装和升级指南》。)但是, 最佳做法是只使用 Napatech 适配器筛选。硬件筛选速度更快。

如果已经为 TIM 设置 Web 服务器筛选和 Napatech 筛选, 则会对这些筛选执行“与”逻辑。也就是说, 将获得筛选的交集。

### 为 Napatech 适配器创建和启用筛选

1. 从 DVD 或 USB 闪存驱动器复制示例筛选文件 (sample\_filter.ntpl) 并根据您的环境进行编辑 (使用简单的文本编辑器, 如记事本或 vi)。

**注意:** 确认 DeleteFilter=all 命令位于文件开头。

2. 在“TIM 系统设置”页面上, 单击“配置 Napatech”。

此时将显示“TIM Napatech 配置”页面。

3. 单击“上传 Napatech 硬件筛选配置文件”。

此时将显示“TIM Napatech 硬件筛选配置”页面。

4. 浏览文件, 然后上传并安装该文件。

5. (可选) 确认已安装筛选。

- a. 在“TIM 系统设置”页面上, 单击“配置 Napatech”。

- b. 单击“查看 Napatech 硬件筛选配置文件”(在“TIM Napatech 配置”页面上)。或者, 有关更多详细信息, 请单击“查看 Napatech 硬件筛选配置日志”。

**重要信息!** 当上传新文件时, 来自旧文件的信息不再显示在 Napatech 硬件筛选配置日志或文件页面上。但是, 仅当在新筛选文件的开头包含 DeleteFilter=all 命令时, 才会删除早期筛选本身。

## 创建高级筛选

您可以基于本节的示例创建高级筛选。

### 根据 IP 地址范围进行筛选：

下列示例显示如何使用 10.11.28.23 – 10.11.28.32 的 IP 地址进行筛选：

```
([10.11.28.23]..[10.11.28.32]).
```

**注意：**在只更改 1 个字节时，此范围效果最好。如果更改量多于 1 个字节，您可能会用尽资源。

### 使用子网掩码筛选：

- 下列示例显示如何使用子网掩码进行筛选。例如，如果您想筛选 192.168.1.x 地址（这里的 x 是多少不重要），请使用此筛选：

```
mIPv4SrcAddr={ [FF.FF.FF.00]:[192.168.1.0]}
```

- 下列示例仅比较掩码为 1 的比特位。例如，如果子网是 10.20.30.0 – 10.20.33.255，使用此筛选：

```
{[FF:FF:FA:00]:[10.20.30.0]}
```

最后一个字节以及前一字节中的 2 位被掩。

### 对多个端口进行筛选：

下列示例显示出如何对两个端口进行筛选：

```
mTcpSrcPort = 43,80
```

**注意：**您可以指定多达 8 项，并且只要仅更改 1 个字节，就只使用 1 个筛选资源。

## 消除重复帧

只要重复现象发生在彼此的八个帧之内并且达到超时条件（其值最多为下列命令中指定的值，单位为毫秒），Napatech 适配器即会删除重复帧：

```
Deduplication [Timeout = 100] = Channel == 0,1,2,3
```

重复数据消除机制会合并所有四个端口的流量，并且在检测重复帧时会应用 100 毫秒窗口。高级重复数据消除可以排除帧的几个部分，仅仅检查帧的 IP 部分。它排除了 IP 标头以及 16 字节的额外固定偏移：

```
Deduplication [DynOffset = Layer2And3HeaderSize; Offset = 16; Timeout = 10] =  
Channel == 0,1,2,3
```

## 其他 Napatech 适配器任务

以下是您可能需要执行的其他一些 Napatech 适配器任务：

- 从 Napatech 适配器中删除筛选
- 删除 Napatech 适配器
- 查看 Napatech 适配器特定的日志

### 从 Napatech 适配器中删除筛选

在排除故障或者不再需要筛选流量时，可以从 Napatech 适配器中删除筛选。

#### 从 Napatech 适配器中删除筛选

1. 在“TIM 系统设置”页面上，单击“配置 Napatech”。  
此时将显示“TIM Napatech 配置”页面。
2. 单击“上传 Napatech 硬件筛选配置文件”。  
此时将显示“TIM Napatech 硬件筛选配置”页面。

- 单击“删除所有 Napatech 硬件筛选”。

此删除操作会将捕获所有筛选功能应用到 Napatech 适配器，以便将所有流量都发送到 TIM。

- (可选) 确认已删除筛选。
  - 在“TIM 系统设置”页面上，单击“配置 Napatech”。
  - 单击“查看 Napatech 硬件筛选配置文件”(在“TIM Napatech 配置”页面上)。

确认页面显示以下内容：

```
Capture=A11
```

### 删除 Napatech 适配器

您可能要从 TIM 中删除 Napatech 适配器；例如，在其他 TIM 计算机上尝试适配器。

### 删除 Napatech 适配器

- 清除 ntxc0:0 接口复选框。( [配置 TIM 网络监控接口以使用适配器](#) (p. 323) )。
- 禁用 Napatech 适配器：
  - 在“TIM 系统设置”页面上，单击“配置 Napatech”。
  - 此时将显示“TIM Napatech 配置”页面。
  - 单击“禁用 Napatech”并且重新启动 TIM。或者，如果 TIM 未运行，单击“禁用 Napatech”。
- 从 TIM 计算机中删除 Napatech 适配器硬件。

### 查看 Napatech 适配器特定的日志

有两个日志文件是 Napatech 适配器所特有的：

- 在应用或删除筛选时，系统会更新 TIM Napatech 硬件筛选配置日志。
- Napatech 驱动程序日志会在每次加载 Napatech 驱动程序时更新。(只要 TIM 重新启动就会加载该驱动程序。)

### 查看 TIM Napatech 硬件筛选配置日志

- 在“TIM 系统设置”页面上，单击“配置 Napatech”。
- 此时将显示“TIM Napatech 配置”页面。
- 单击“查看 Napatech 硬件筛选配置日志”。
- 此时将显示“TIM Napatech 硬件筛选配置日志”。

### 查看 Napatech 驱动程序日志

1. 在“TIM 系统设置”页面上，单击“配置 Napatech”。  
此时将显示“TIM Napatech 配置”页面。
2. 单击“查看 Napatech 驱动程序日志”。  
此时显示 Napatech 驱动程序日志。

## 排除 Napatech 适配器故障

### 关于 Napatech 适配器和 TIM 日志

在 TIM 日志中，与网络接口有关的所有消息前面都会添加 AdapterManager。例如，与 Napatech 适配器相关的消息引用 ntxc0:0 接口。例如：

```
AdapterManager: "ntxc0:0": thread starting
```

### 故障排除主题

本页包括以下故障排除主题：

- [Napatech 适配器没有接收流量](#) (p. 328)
- [Napatech 适配器作为以太网端口](#) (p. 329)
- [未看到预期流量](#) (p. 329)
- [序列号和其他 Napatech 适配器详细信息](#) (p. 329)

## Napatech 适配器没有接收流量

### 症状：

TIM 没有接收数据包。我复查“TIM 数据包统计信息”页面，发现系统没有捕获数据包。

确认有要显示的流量。将电缆从 ntxc0:0 端口移到 eth1 端口，并且打开 eth1 端口。如果立即看到数据包，则是适配器有问题。

### 解决方案：

确认已启用接口。请参阅[配置 TIM 网络监控接口以使用适配器](#) (p. 323)。

验证是否已配置该软件。请参阅[安装软件](#) (p. 322)。

复查日志。请参阅[查看 Napatech 适配器特定的日志](#) (p. 326)。



在日志中查找问题。请参阅[查看 Napatech 适配器特定的日志](#) (p. 326)和[关于 Napatech 适配器和 TIM 日志](#) (p. 328)。

删除筛选。请参阅[从 Napatech 适配器中删除筛选](#) (p. 326)。

如果您认为是 Napatech 适配器本身有问题，请致电 Network Allies；否则，请致电 CA Support。

## Napatech 适配器作为以太网端口

### 症状：

当我在 TIM 的 Linux 提示符下键入 `ifconfig` 命令时，`ntxc0:0` 端口不显示。操作系统未将 Napatech 适配器识别为以太网端口。

### 解决方案：

无需执行任何操作。Napatech 适配器在该应用程序中表现正常。

## 未看到预期流量

### 症状：

我看到一些流量，但不是预期的流量。

### 症状：

如果您已经启用多个接口进行监控，请关闭其他接口，确认您正在从 `ntxc0:0` 接口获取流量。如果您没有从 `ntxc0:0` 接口获取任何流量，请参阅[Napatech 适配器没有接收流量](#) (p. 328)。

复查筛选。删除筛选。是否看到预期的流量？如果看到，请复查并编辑筛选，然后重新应用它。确认筛选文件的开头已包含 `DeleteFilter=all` 命令。

## 序列号和其他 Napatech 适配器详细信息

### 症状：

我想找到我的 Napatech 适配器的序列号。

（与 Network Allies 支持人员联系时可能需要序列号。）

### 解决方案：

您可以在 Napatech 状态页面上查看有关 Napatech 适配器的信息。

**打开 Napatech 状态页面**

1. 在“TIM 系统设置”页面上，单击“配置 Napatech”。  
此时将显示“TIM Napatech 配置”页面。
2. 查看 Napatech 状态。  
Napatech AdapterInfo 程序运行，并显示输出。

# 第 24 章：配置 CA Introscope 以与 CA CEM 一起使用

---

CA CEM 可满足两种不同用户的需求：负责 Web 业务的用户可获取趋势、服务级别和成功率报告；负责响应突发事件的用户可实时洞察事务缺陷的详细信息。Introscope 在应用程序服务器级别提供行业领先的问题隔离解决方案。客户集成 CA CEM 和 CA Introscope 时，可在操作中获取其 Web 应用程序的完整端到端视图。此解决方案是 CA APM。

整个端到端客户体验的实时知识提供了新的见解，可以显著改善服务交付，提高客户忠诚度，增强客户的总体在线体验。CA APM 报告中提供的事务分类信息提供了可同时满足 IT 和业务利益相关者需求的公共语言。

CA CEM 增强了 IT 的业务管理合作伙伴角色，团队一起努力，可确保为客户提供高质量的联机服务。

本章介绍了如何安装和配置 Introscope 以与 CA CEM 进行集成。有关如何一起使用这些产品的详细信息，请参阅“将 Introscope 与 CA CEM 结合使用”。有关 Introscope 代理记录功能的信息，请参阅《CA APM 事务定义指南》。

此部分包含以下主题：

[CA APM 使用入门](#) (p. 331)

[CA APM 客户体验度量标准概述](#) (p. 332)

[CA APM 问题解决方案分类概述](#) (p. 332)

[配置 CA CEM 的清单](#) (p. 334)

[配置 Introscope 的清单](#) (p. 344)

[CA Introscope 与 CA CEM 集成故障排除](#) (p. 352)

[升级注意事项](#) (p. 354)

[设置业务应用程序](#) (p. 354)

## CA APM 使用入门

CA APM 需要集成 CA Introscope 和 CA CEM。

该列表显示了如何开始使用 CA APM：

1. 了解具有 CA Introscope 的 CA CEM 如何为企业所需的客户体验信息。请参阅 [CA APM 客户体验度量标准概述](#) (p. 332)。

2. 了解具有 CA Introscope 的 CA CEM 如何帮助进行 IT 分类并解决问题。请参阅 [CA APM 问题解决方案分类概述](#) (p. 332)。
3. 配置集成的 CA CEM 端。请参阅[配置 CA CEM 的清单](#) (p. 334)。
4. 配置集成的 CA Introscope 端。请参阅[配置 CA Introscope 的清单](#) (p. 344)。
5. 验证集成功能是否正常工作。请参阅 [CA Introscope 到 CA CEM 的集成故障排除](#) (p. 352)。
6. 如果要将 CA CEM/CA Introscope 环境升级到 CA APM，请检查升级注意事项。请参阅[升级注意事项](#) (p. 354)。

## CA APM 客户体验度量标准概述

CA CEM 和 CA Introscope 客户体验度量标准集成由企业管理器和每个 TIM 上的配置参数控制。

1. 每隔 7 秒或根据定义的时间间隔，TIM 将所有客户体验度量标准写入 XML 文件，直到这些度量标准被删除或者已达到或超出过期期限。
2. 企业管理器 TIM 收集服务检索客户体验度量标准文件并指示 TIM 将其删除。
3. 企业管理器 TIM 收集服务解析客户体验度量标准数据，但不会将这些数据存储在 APM 数据库中，也不会对数据执行任何聚合。
4. 客户体验度量标准通过原始 TIM 进行分组；企业管理器将客户体验度量标准存储在 SmartStor 数据库中。
5. CA Introscope Workstation 显示默认的业务显示板，使用类型视图和计算器来提供聚合和缺陷百分比。
6. 您可以使用相同的客户体验度量标准数据根据需要创建自己的自定义业务显示板。请参阅将 CA Introscope 与 CA CEM 结合使用。

有关 TIM 收集服务的详细信息，请参阅[分发企业管理器服务](#) (p. 244)。

## CA APM 问题解决方案分类概述

CA CEM 和 CA Introscope 问题解决方案分类集成由 CA Introscope 配置设置控制。配置信息包含在域配置信息中，其中包括事务定义、缺陷规范和事务跟踪参数。

1. 单击“设置”>“监视器”>“同步所有监视器”时，CA CEM 会通知 CA Introscope 对域配置信息所做的更改。（单击“同步所有监视器”时，CA CEM 还会将域配置信息发送到 TIM。）
2. CA Introscope 代理侦听域配置信息的任何更新。（适用于 9.0 之前的代理：CEMDefinitionHandler 会将解析的域配置信息发送到所有已注册的代理。）
3. 随后，每个已注册代理都会创建稍后可启用事务跟踪的规则集。该规则集包括可标识 CA CEM 事务的参数名/值的正则表达式模式。
4. 安装有 ServletHeaderDecorator 的 Java 代理将额外信息添加到每个 HTTP 响应头。标头信息包括 GUID，稍后会使用它将 CA Introscope 事务跟踪与 CA CEM 缺陷相关联。.NET 代理需要安装 HTTPHeaderDecorator 才能提供相同的功能。
5. CA CEM TIM 解析 HTTP 响应标头，并包括其发送给企业管理器的任何已报告缺陷中的信息。
6. CA CEM 将缺陷和 GUID 信息保存在 APM 数据库中。
7. CA CEM 生成一个慢速突发事件，并将事务跟踪会话启动请求发送到企业管理器。（CA CEM 通过“设置”>“突发事件设置”将突发事件状态从“未决”更改为“打开”，从而生成一个慢速突发事件。）  
事务跟踪会话启动请求包括业务事务名称和事务跟踪时间阈值，该阈值是慢速缺陷规范的百分比。事务跟踪继续运行，直到突发事件关闭或达到配置的事务跟踪会话持续时间。
8. 安装有 BizTrxHttpTracer 的代理按代理规则集中指定的业务事务名称查找事务定义。这些代理使用参数匹配来标识 CA CEM 事务。
9. 当某个代理标识事务且事务处理时间大于事务跟踪时间阈值时，该代理会向企业管理器发送事务跟踪。
10. CA CEM 将收到事务跟踪，并根据 APM 数据库中存储的 GUID 匹配这些跟踪。找到 GUID 匹配时，CA CEM 将事务跟踪信息保存在 APM 数据库中。

企业管理器事务跟踪信息以及其他 CA CEM 缺陷信息用于帮助将突发事件分发到适当的团队进行解决。请参阅将 CA Introscope 与 CA CEM 结合使用。

## 配置 CA CEM 的清单

该列表显示了需要了解的有关配置 CA CEM 以与 CA Introscope 集成的内容。

### 配置 CA CEM 以与 CA Introscope 集成:

1. 决定要使用哪些集成功能。请参阅[决定需要哪些集成功能](#) (p. 345)。
2. 配置 CA Introscope 工作站。请参阅[配置 CA Introscope 工作站](#) (p. 335)。
3. 配置 CA Introscope 事务跟踪。请参阅[配置事务跟踪](#) (p. 336)。
4. 配置实时事务度量标准。请参阅[配置实时事务度量标准集成](#) (p. 338)。
5. 验证集成功能是否正常工作。请参阅[验证 CA CEM 配置](#) (p. 344)。

## 决定需要哪些集成功能

有两种类型的 CA APM 集成:

- 问题解决方案分类—允许您使用相关的事务信息来分析问题的根本原因。
- 客户体验度量标准—为业务事务提供量、错误和平均响应时间方面的常规更新。

如果要使用问题解决方案分类,则需要配置 Introscope 设置。这允许您配置工作站和事务跟踪。

如果要使用客户体验度量标准,则需要配置 TIM 收集服务。这允许您配置收集器并在每个 TIM 上启用度量标准收集。

您可以选择同时使用这两种集成功能或者仅使用其中一种,具体取决于您在业务环境中的需求。

**注意:** 如果要使用 CA Introscope 代理记录功能,请参阅《CA APM 事务定义指南》。

### 详细信息:

[配置 Introscope 设置](#) (p. 335)

[配置客户体验度量标准集成](#) (p. 338)

[验证 CA CEM 配置](#) (p. 344)

## 配置 Introscope 设置

要启用 CA APM 集成，您需要收集基本信息来设置 CA Introscope。

本部分包括以下主题：

[配置 CA Introscope 工作站](#) (p. 335)

[配置事务跟踪](#) (p. 336)

[查看事务跟踪会话信息](#) (p. 337)

### 配置 CA Introscope 工作站

您需要设置 Workstation Web Start 和 WebView 应用程序的连接参数。

#### 配置 CA CEM 以与 CA Introscope 工作站通信：

1. 选择“设置” > “Introscope 设置”。  
此时将显示“Introscope 设置”页面。
2. 启用 Workstation Web Start 链接—如果要使 CA CEM 在突发事件和缺陷页面上显示 Workstation Web Start 链接，请选中该复选框。如果不选中该框，则不会在突发事件和缺陷页面上显示该链接。
3. 输入 Introscope WebView 信息：
  - a. 启用 WebView 链接—如果要使 CA CEM 在突发事件和缺陷页面上显示 WebView 链接，请选中该复选框。如果不选中该框，则不会在突发事件和缺陷页面上显示该链接。
  - b. 主机名—键入承载 CA CEM 的 WebView 的 CA Introscope 系统的主机名或 IP 地址。
  - c. 端口—键入企业管理器侦听与 WebView 的连接端口。WebView 的默认端口号为 8080。
  - d. 上下文路径—键入指定 CA Introscope 的应用程序上下文路径的 *introscope.webview.context.path* 属性值。  
**注意：** *introscope.webview.context.path* 的默认值为 “/”（在文本框中无引号）。该属性在承载企业管理器的计算机上 `<EM_Home>\config\` 目录中的 *IntroscopeWebView.properties* 文件中定义。
4. 单击“保存设置”。  
CA CEM 将保存 Introscope 工作站配置信息。
5. 继续[配置事务跟踪](#) (p. 336)。

## 配置事务跟踪

当突发事件生成并基于这些规则时，CA APM 集成将启动事务跟踪。您还可以通过“CEM” > “突发事件概览”页手工启动事务跟踪。

**注意：**仅在应用程序服务器时间阈值为 15 毫秒或更长时间时，CA CEM 缺陷的事务跟踪信息才会显示在 CA CEM “缺陷详细信息”页面上。

您可以配置事务跟踪设置或将其设置为默认值。

**重要信息！** 事务跟踪可能会导致被检测应用程序的性能降低。（如果相关慢速缺陷规范过低，则可能会降低被检测应用程序的性能。）请注意，这些设置是全局设置，并非针对每个业务事务。

### 配置 CA Introscope 事务跟踪：

1. 输入“事务跟踪会话最长持续时间 (分钟)”。

默认情况下，事务跟踪在 30 分钟之后停止。

只有在业务事务具有打开的突发事件时，CA CEM 才会启动与 CA Introscope 的事务跟踪会话。CA CEM 有权使用特殊的事务跟踪方法，通过业务事务的时间阈值进行跟踪。例如，跟踪超过 1000 毫秒（即 1 秒）的所有更新配置文件 Web 请求。

这允许代理优化性能，因为一旦识别出某个请求不是更新配置文件，便无需执行其他操作。虽然可能有多个事务跟踪会话正在运行，开销仍然控制到最低。

2. 输入“事务跟踪时间阈值”（慢速缺陷规范的百分比）。

默认值为 50%。

事务跟踪时间阈值是事务的执行时间限制。当事务跟踪正在运行时，将会跟踪阈值内未完成的所有事务。

事务跟踪时间阈值是慢速缺陷规范的百分比。例如，如果慢速缺陷指定设置为 5.00 秒，事务跟踪时间阈值设置为 50%，则将跟踪完成时间超过 2.50 秒（在 CA Introscope 中，即在应用程序服务器上）的所有事务。



如果上述示例使用默认值 30 分钟和 50%，则将在符合下列条件时跟踪事务：

- 业务事务存在打开的突发事件。
- 事务完成时间为 2.50 秒以上。
- 事务跟踪运行的时间少于 30 分钟。

**重要信息！** 在某些情况下，您可能需要将 CA CEM 慢速缺陷指定设置为非常短的时间，如 1 毫秒（即千分之一秒）。例如，您可能需要为仅在出现错误时发生的事务执行此项设置。但是，如果 CA Introscope 事务跟踪中涉及到该相同的事务，那么 1 毫秒设置可能会导致企业管理器 MOM、企业管理器收集器和代理出现性能问题。

3. 输入后端组件。在 CA Introscope 中，与给定模式相匹配的任何组件均被视为后端组件。

使用星号（“\*”）作为通配符，并且总在模式的末尾使用。

例如：Backends /\*, JDBC /\*

各个模式之间使用逗号分隔。因此，上述示例具有两种模式：Backends /\* 和 JDBC /\*

如果事务跟踪中的任一组件均以 Backends /\* 或 JDBC /\* 开头，则将该组件识别为后端组件。

4. 单击“保存设置”。

CA CEM 将保存事务跟踪配置信息。

**注意：** 如果要了解有关监控事务跟踪会话的信息，请参阅查看事务跟踪会话信息。

## 查看事务跟踪会话信息

可以查看当前正在运行的事务跟踪会话列表。也可以选择特定的突发事件，以了解有关该突发事件的详细信息。

### 查看所有正在运行的事务跟踪：

1. 选择“CEM” > “突发事件管理”。  
此时将显示“突发事件”页面。
2. 选择“事务跟踪会话”链接。  
此时将显示当前正在运行的事务跟踪的列表。
3. 单击特定的突发事件编号，以直接转至该突发事件的“CEM” > “突发事件概览”页面。

## 配置客户体验度量标准集成

本节提供了有关升级客户体验度量标准、如何启动/停止服务以及可选故障排除方面的信息。

本部分包括以下主题：

[升级客户体验度量标准](#) (p. 338)

[启动客户体验度量标准收集服务](#) (p. 338)

[停止 RTTM 收集服务](#) (p. 339)

[在 TIM 上对客户体验度量标准进行故障排除](#) (p. 339)

[客户体验度量标准的 TIM 设置](#) (p. 341)

### 升级客户体验度量标准

**注意：**如果您在早期版本的 CA CEM 中使用过客户体验度量标准，则将术语“业务流程”更改为“业务服务”可能会对您产生一定的影响。

如果您在升级之后不执行任何操作，新术语“业务服务”将显示在显示板度量标准中。

**适用于 CA CEM 4.5：**要保留度量标准中的度量标准名称“业务流程”，需要设置 `tess-customer.properties` 以及继续使用 CA CEM 4.5 Javascript 计算器。

针对客户体验度量标准保留“业务流程”度量标准名称：

1. 设置 `tess-customer.properties`，并更改属性：  
`BTStatsMetricName.backwardCompatible`  
有关如何编辑 `tess-customer` 属性文件的信息，请参阅[修改 tess-customer.properties 文件](#) (p. 505)。
2. 将企业管理器上的 Javascript 计算器替换成 CA CEM 4.5 中的计算器。  
替换 `CEM-AggregatedTree.js` 和 `CEM-DefectPercent.js`。
  - a. 获取 `CEM_BT_Stats_package.zip` 文件。
  - b. 将 `CEM-AggregatedTree.js` 提取到 `<EM_Home>\scripts` 目录中。
  - c. 将 `CEM-DefectPercent.js` 提取到 `<EM_Home>\scripts` 目录中。
  - d. 重新启动企业管理器以重新加载 Javascript 计算器。

### 启动客户体验度量标准收集服务

通过 TIM 收集服务，可以收集客户体验度量标准。通常，作为最初安装和设置的一部分，您将分发企业管理器服务，其中包括 TIM 收集服务。

有关企业管理器服务的详细信息，请参阅[分发企业管理器服务](#) (p. 244)。

必须首先配置 TIM 收集服务并启动 RTTM 收集服务，才能显示客户体验度量标准数据。

#### 启动客户体验度量标准收集服务：

1. 选择“设置”>“服务”>“服务配置”。
2. 选择“TIM 收集服务”。
3. 在“TIM 收集服务”列表中，选择“RTTM 收集服务”（如果尚未选择）。
4. 单击“启动”以启动客户体验度量标准收集服务。
5. 验证“服务状态”是否从“已停止”更改为“正在运行”。

### 停止 RTTM 收集服务

有时，您可能要停止客户体验度量标准功能。

#### 停止 RTTM 收集服务：

1. 选择“设置”>“服务”>“服务配置”。
2. 选择“TIM 收集服务”。
3. 在“TIM 收集服务”列表中，选择“RTTM 收集服务”（如果尚未选择）。
4. 单击“停止”以停止客户体验度量标准收集服务。
5. 验证“服务状态”是否从“正在运行”更改为“已停止”。

### 在 TIM 上对客户体验度量标准进行故障排除

**注意：**以下配置过程对于 TIM 是*可选的*。在大多数情况下，应当通过“设置”>“服务”>“服务配置”来配置 TIM 收集服务。有关 TIM 收集服务的详细信息，请参阅[分发企业管理器服务](#) (p. 244)。

可以在 TIM 上临时禁用客户体验度量标准收集，也可以将其永久禁用。可以更改收集频率和文件老化，并修改其他设置以排除环境中的故障。

#### 在 TIM 上临时禁用客户体验度量标准：

1. 在“Wily 系统设置”页面中，选择“TIM”>“配置 TIM 设置”。（有关如何进入“Wily 系统设置”页面的信息，请参阅[访问 TIM 的 Wily 系统设置页面](#) (p. 228)。）

此时将显示“TIM 设置”页面。

2. 单击“定义”以定义新值。
3. 键入名称：*BtStats/Enabled*
4. 键入新值：*0*
5. 单击“变更”。

这样便会在此 TIM 上临时禁用客户体验度量标准收集。下次重新启动企业管理器时，将恢复收集功能。

**注意：**上述过程假设之前已启用客户体验度量标准收集。

#### 在 TIM 上永久禁用客户体验度量标准：

1. 在“Wily 系统设置”页面中，选择“TIM” > “配置 TIM 设置”。  
此时将显示“TIM 设置”页面。
2. 单击“定义”以定义新值。
3. 键入名称：*BtStats/ForceDisabled*
4. 键入新值：*1*  
这将不允许 CA CEM 控制此 TIM 上的客户体验度量标准。
5. 单击“变更”。

这样便会在此 TIM 上禁用客户体验度量标准收集。下次重新启动企业管理器时，不会在此 TIM 上恢复客户体验度量标准收集。

**注意：**您可以通过将值更改回默认值 *0* 使 CA CEM 可以重新控制此 TIM 上的客户体验度量标准收集。

可以在您的环境中选择性地更改更多 TIM 设置，这些设置在客户体验度量标准的 TIM 设置中定义。如果这些 TIM 设置未在“TIM 设置”页面上显示，则说明它们设置为默认值。

#### 修改 TIM 上的客户体验度量标准处理：

1. 在“Wily 系统设置”页面中，选择“TIM” > “配置 TIM 设置”。  
此时将显示“TIM 设置”页面。
2. 如果 TIM 设置已存在：
  - a. 单击名称。
  - b. 键入新值。
  - c. 单击“变更”。
3. 如果 TIM 设置不存在：
  - a. 单击“定义”以定义新值。
  - b. 键入新名称。

- c. 键入新值。
- d. 单击“添加”。

## 客户体验度量标准的 TIM 设置

这些 TIM 设置有助于对客户体验度量标准进行故障排除。

本部分包括以下主题：

[BtStats/ForceDisabled](#) (p. 341)

[BtStats/Enabled](#) (p. 341)

[BtStats/IntervallInSeconds](#) (p. 342)

[BtStats/LogLevel](#) (p. 342)

[BtStats/WriteEmptyFiles](#) (p. 343)

[BtStats/MaxFileAgeInSeconds](#) (p. 343)

### BtStats/ForceDisabled

通过此设置，可以控制 TIM 本身上的客户体验度量标准功能。还可以覆盖 CA CEM 控制。

设置

数值：

- 0（允许 CA CEM 在此 TIM 上控制该功能）
- 1（在此 TIM 上强制关闭该功能）

默认

0

示例

```
BtStats/ForceDisabled = 0
```

注释

- 可以在 TIM 上禁用客户体验度量标准功能。
- 1 = 忽略 *BtStats/Enabled* TIM 设置（下一个设置）。
- 0 = 客户体验度量标准功能由 CA CEM 控制，并使用 *BtStats/Enabled* TIM 设置（下一个设置）。

### BtStats/Enabled

通过此设置，可以控制 TIM 本身上的客户体验度量标准功能。

设置

数值：

- 0（禁用，默认设置）
- 1（启用）

默认

0

示例

```
BtStats/Enabled = 0
```

注释

- 启动企业管理器时，CA CEM 在 TIM 上控制此设置。但是，*BtStats/ForceDisabled* TIM 设置（上一个设置）可以覆盖此设置。
- 您也可以 [在 TIM 上修改此设置](#)，以临时在 TIM 上禁用客户体验度量标准收集。但是，下次企业管理器重新启动时，将更改该设置。
- 请参阅 [在 TIM 上对客户体验度量标准进行故障排除](#) (p. 339)。

### BtStats/IntervalInSeconds

通过此设置，可以控制 TIM 写入实时事务统计文件的频率。

设置

数值；必须为正整数。

默认

7

示例

```
BtStats/IntervalInSeconds = 7
```

注释

实时事务统计文件存储在 TIM 上的  
*/etc/wily/cem/tim/data/out/btstats* 目录中。

### BtStats/LogLevel

通过此设置，可以控制客户体验度量标准的 TIM 日志文件条目。

设置

数值：

- 0
- 1
- 2

默认

0

示例

```
BtStats/LogLevel = 0
```

注释

- 0 = 无消息（默认值）
- 1 = 在写入 BtStats 文件时，将消息写入 TIM 日志
- 2 = 与消息相同，详细模式

### BtStats/WriteEmptyFiles

通过此设置，可以控制 TIM 是否写入空的实时事务统计文件。

设置

数值：

- 0
- 1

默认

0

示例

```
BtStats/WriteEmptyFiles = 0
```

注释

- 0 = 不写入空文件（默认值）
- 1 = 写入空文件（包含空 BTlist）
- 此设置可用于故障排除。例如，如果在某个 TIM 时间间隔期间未检测到任何事务，仍将写入包含空 BTlist（即未检测到任何事务）的空文件。这可用于测试 TIM 创建 BtStats 文件时企业管理器是正在运行还是未运行。
- 实时事务统计文件存储在 TIM 上的 `/etc/wily/cem/tim/data/out/btstats` 目录中。

### BtStats/MaxFileAgeInSeconds

通过此设置，可以定义实时事务统计文件的保留时间（如果这些文件未被 CA CEM 选取）。TIM 将删除保留时间超过该值的文件。

设置

数值：必须为正整数。

默认

3600

示例

```
BtStats/MaxFileAgeInSeconds = 3600
```

注释

- 3600 = 1 小时（默认值）
- 定义 BtStats 文件的保留时间。TIM 将删除保留时间超过该值的文件。
- 将此值设置得过高可能会导致 TIM 耗尽磁盘空间。
- 将此值设置得过低可能会导致在 CA CEM 检索文件之前，这些文件已被删除。
- 实时事务统计文件存储在 TIM 上的 `/etc/wily/cem/tim/data/out/btstats` 目录中。

## 验证 CA CEM 配置

如果您尚未为 CA APM 配置 CA Introscope，请转到[配置 CA Introscope 的清单](#) (p. 344)。

有关配置验证和故障排除的信息，请参阅 [CA Introscope 与 CA CEM 集成故障排除](#) (p. 352)。

## 配置 Introscope 的清单

该列表显示了您需要执行哪些操作来配置 CA Introscope 以与 CA CEM 集成。

**将 CA Introscope 与 CA CEM 集成：**

1. 决定要使用哪些集成功能。请参阅[决定需要哪些集成功能](#) (p. 345)。
2. 配置企业管理器以启用问题解决方案分类功能。请参阅[配置企业管理器](#) (p. 345)。
3. 集成每个 Java 代理以启用问题解决方案分类功能。请参阅[与 Java 代理集成](#) (p. 347)。
4. 集成每个 .NET 代理以进行问题解决分类。请参阅[与 .NET 代理集成](#) (p. 349)。
5. 验证集成功能是否正常工作。请参阅“[验证 CA Introscope 配置](#) (p. 351)”。



## 决定需要哪些集成功能

有两种类型的 CA APM 集成：

- 问题解决方案分类—允许您使用相关的事务信息来分析问题的根本原因。
- 客户体验度量标准—为业务事务提供量、错误和平均响应时间方面的常规更新。

如果您要启用问题解决方案分类功能，需要配置企业管理器和所有受影响的代理，才可查看有关慢速突发事件的问题解决方案分类信息。

**注意：**仅已使用 AutoProbe 检测过的 Java 和 .NET 代理应用程序支持 CA CEM 问题解决分类集成。

如果需要客户体验度量标准，则需要配置企业管理器显示板以查看已收集的度量标准；请参阅创建自己的 CA CEM 客户体验显示板。

您可以选择同时使用这两种集成功能或者仅使用其中一种，具体取决于您在业务环境中的需求。

**注意：**如果要使用 CA Introscope 代理记录功能，请参阅《CA APM 事务定义指南》。

**详细信息：**

[配置 Introscope 设置](#) (p. 335)

[配置客户体验度量标准集成](#) (p. 338)

[验证 CA CEM 配置](#) (p. 344)

## 配置企业管理器

必须配置企业管理器才能启用 CA CEM 与 CA Introscope 的集成。

**适用于 9.0 以前的代理：**还必须重新部署 4.5 企业管理器扩展：

- 下载企业管理器扩展，并将其安装到 MOM 和每个企业管理器收集器。
- 重新启动每个企业管理器 (JVM) 以重新加载企业管理器扩展。

## 将 CA CEM 建立为虚拟代理

您需要将 CA CEM 配置为企业管理器的虚拟代理。通过以下过程，可以聚合各个代理中的度量标准。它还使“转到 Introscope Workstation Web Start”链接直接链接到调查器树，而不是仅仅链接到 CA Introscope 控制台。

### 将 CA CEM 配置为虚拟代理：

1. 找到 `<EM_Home>\config\agentclusters.xml` 文件。

**重要信息！** 可以将 CA CEM 配置为连接到单个企业管理器或 MOM 企业管理器。如果您的 CA Introscope 环境中存在多个企业管理器，必须只修改 MOM 的 `agentclusters.xml` 文件。

2. 取消注释 `agentclusters.xml` 文件中的相关代理行：

```
<agent-cluster name="CEM Agent" domain="SuperDomain">
  <agent-specifier>.*\.*\.*</agent-specifier>
  <metric-specifier>Customer Experience\.*</metric-specifier>
  <metric-specifier>Business Segment\.*</metric-specifier>
</agent-cluster>
```

**重要信息！** 请勿更改名称或域属性，否则集成将无法正确运行。

3. 保存对 `agentclusters.xml` 文件所做的更改。  
做出此更改之后无需重新启动企业管理器。

## 为 9.0 之前的代理部署企业管理器扩展

**适用于 9.0 以前的代理：** 只有具备与企业管理器连接的 5.0 以前的代理时，才需要部署此 CA CEM 4.5 扩展。

连接到 9.0 之前的代理的每个企业管理器均需安装 CA CEM 4.5 CEMDefinitionHandler 企业管理器扩展，才可使 CA CEM 与 CA Introscope 集成。

### 请执行以下步骤：

1. 联系 CA Support 以获取所需的文件。
2. 使用 CA CEM 软件链接获取 CA CEM 4.5 CEMIntroscopeIntegrationKit。
3. 将 `CEMDefinitionHandler.jar` 下载到企业管理器上的 `<EM_Home>\ext` 目录。
4. 继续执行 [重新加载企业管理器](#) (p. 347)。

## 重新加载企业管理器

必须重新启动企业管理器，才可完成企业管理器集成以启用问题解决方案分类功能。

重新启动 JVM 会启用企业管理器扩展。

### 重新加载企业管理器：

1. 重新启动企业管理器以重新加载企业管理器扩展。
2. 返回到[为 9.0 之前的代理部署企业管理器扩展 \(p. 346\)](#)，并针对连接到 9.0 之前的代理的每个企业管理器重复执行这些步骤。

## 与 Java 代理集成

您需要针对 CA CEM 与 Introscope 集成中包含的每个 Java 代理执行这些过程：

1. 配置对 Introscope 的 AutoProbe 跟踪—启用 CA CEM 事务中涉及到的应用程序。
2. 验证 AutoProbe 和 ServletHeaderDecorator 的代理属性。
3. 重新启动代理 (JVM) 以重新加载代理配置属性。

如果需要与 .NET 代理集成，请参阅[与 .NET 代理集成 \(p. 349\)](#)。

## 在 Java 环境中配置 AutoProbe 跟踪

Introscope 调查器树中的详细信息基于在代理文件夹的 PBL 文件中激活的 BizTrxHttpTracer 和 ServletHeaderDecorator。启用这些 PBD 之后，CA Introscope 可以显示每个业务事务的度量标准。

一旦完成集成，这些业务事务便会显示在树中，并使用在 CA CEM 中显示的相同事务名称。

有关 AutoProbe 的详细信息，请参阅《*CA APM Java 代理实施指南*》。

### 在 Java 代理上配置 AutoProbe 跟踪：

1. 打开 <Agent\_Home>\wily\core\config 目录中的 *IntroscopeAgent.profile* 文件。
2. 找到 *introscope.autoprobe.directivesFile* 属性，例如：

```
introscope.autoprobe.directivesFile=  
default-typical.pbl
```

3. 找到在属性中指定的 PBL 文件。  
在上述示例中，该文件为 *default-typical.pbl*。
4. 使用文本编辑器中打开指定的 PBL 文件。
5. 在 PBL 文件中，取消注释 ServletHeaderDecorator.pbd 行：

```
#####  
# Servlet Header Decorator  
#  
# Enable this PBD for CEM integration. It appends additional  
# information to the HTTP response that is then captured by CEM.  
# =====  
ServletHeaderDecorator.pbd
```

6. 保存对 PBL.profile 文件所做的更改。
7. 继续执行[在 Java 环境中验证默认代理属性](#) (p. 348)。

适用于 CA Introscope 9.0: 默认情况下启用 *biz-trx-http.pbd*。

适用于 9.0 以前的代理: 必须同时取消注释 *CEMTracer.pbd*。

## 在 Java 环境中验证默认代理属性

通过代理配置文件属性文件，可以修改 AutoProbe 和 ServletHeaderDecorator 的默认代理属性。

为实现 CA CEM 到 CA Introscope 的集成，预配置了所有与 CA CEM 相关的属性。您需要验证这些默认值是否适用于您的安装。

**重要信息！** 您应当至少检查与安全有关的属性。例如，*introscope.agent.decorator.security* 属性默认设置为 *clear*。这适于初始测试，但是可能会泄露不希望被防火墙之外的用户知道的事务头中的信息。您可以将该属性设置为 *encrypted*，以实现更安全的生产环境。

有关与 CA CEM 相关的代理属性的详细信息，请参阅 CA Introscope 代理配置文件属性。

有关详细信息，请参阅《CA APM Java 代理实施指南》。

### 验证代理配置文件属性：

1. 打开 <Agent\_Home>\wily\core\config 目录中的 *IntroscopeAgent.profile* 文件。

2. 将在代理配置文件中找到的属性与 CA Introscope 代理配置文件属性中的属性说明进行比较。例如，您可能要从默认设置更改这些属性：
  - `introscope.agent.decorator.enabled`—将默认 Java 代理设置从 `false` 更改为 `true`；这将启用问题解决方案分类功能。
  - `introscope.agent.decorator.security`—将默认设置从 `clear` 更改为 `encrypted`；这可以确保事务头中机密信息的安全。
3. 如果需要修改默认值，可能需要将属性添加到 `IntroscopeAgent.profile` 文件，然后对其进行配置。
4. 保存对 `IntroscopeAgent.profile` 文件所做的更改。
5. 继续执行[在 Java 环境中重新加载代理属性](#) (p. 349)。

**提示：**如果未列出属性，可能会导致混淆，因此，一种好方法是显式包含该属性，即使默认值是所需的值。

## 在 Java 环境中重新加载代理属性

必须重新启动代理才可使受控应用程序完成集成。

重新启动 JVM 将重新加载代理属性，并启用 `AutoProbe` 和 `ServletHeaderDecorator`。

### 在 Java 代理上重新加载代理配置文件属性：

1. 重新启动代理以重新加载代理属性。
2. 返回至[与 Java 代理集成](#) (p. 347)，然后针对每个代理重复这些过程。

## 与 .NET 代理集成

针对 CA CEM 与 CA Introscope 集成中包含的每个 .NET 代理执行以下过程：

1. 配置对 CA Introscope 的 `AutoProbe` 跟踪—启用 CA CEM 事务中涉及到的应用程序。
2. 验证 `AutoProbe` 和 `HTTPHeaderDecorator` 的代理属性。
3. 重新启动代理 (CLR) 以重新加载代理配置属性。

如果与 Java 代理集成，请参阅“[与 Java 代理集成](#) (p. 347)”。

## 在 .NET 环境中配置 AutoProbe 跟踪

Introscope 调查器树中的详细信息基于在代理文件夹的 PBL 文件中激活的 BizTrxHttpTracer 和 HTTPHeaderDecorator。启用 BizTrxHttpTracer 之后，CA Introscope 可以显示每个业务事务的度量标准。

一旦完成集成，这些业务事务便会显示在树中，并使用在 CA CEM 中显示的相同事务名称。

有关 AutoProbe 的详细信息，请参阅《CA APM .NET 代理实施指南》。

### 在 .NET 代理上配置 AutoProbe 跟踪：

1. 打开 <代理主目录> 目录中的 *IntroscopeAgent.profile* 文件。

2. 找到 *introscope.autoprobe.directivesFile* 属性，例如：

```
introscope.autoprobe.directivesFile=  
default-typical.pbl
```

3. 找到在属性中指定的 PBL 文件。

在上述示例中，该文件为 *default-typical.pbl*。

4. 使用文本编辑器中打开指定的 PBL 文件。

5. 在 PBL 文件中，取消注释 *httpheaderdecorator.pbd* 行：

```
#####  
# HTTP Header Decorator  
#  
# Enable this PBD for CEM integration.  
# It appends additional information to the  
# HTTP response that is then captured by CEM.  
# =====  
httpheaderdecorator.pbd
```

6. 保存对 PBL.profile 文件所做的更改。

7. 继续执行在 [.NET 环境中验证默认代理属性](#) (p. 350)。

**适用于 CA Introscope 9.0：** 默认情况下启用 *biz-trx-http.pbd*。

**适用于 9.0 以前的代理：** 必须同时取消注释 *CEMTracer.pbd*。

## 在 .NET 环境中验证默认代理属性

通过代理配置文件属性文件，可以修改 AutoProbe 和 HTTPHeaderDecorator 的默认代理属性。

为实现 CA CEM 到 CA Introscope 的集成，预配置了所有与 CA CEM 相关的属性。您需要验证这些默认值是否适用于您的安装。

**重要信息！** 您应当至少检查与安全有关的属性。例如，`introscope.agent.decorator.security` 属性默认设置为 `clear`。这适于初始测试，但是可能会泄露不希望被防火墙之外的用户知道的事务头中的信息。您可以将该属性设置为 `encrypted`，以实现更安全的生产环境。

有关与 CA CEM 相关的代理属性的详细信息，请参阅《*CA APM .NET 代理实施指南*》。

#### 验证代理配置文件属性：

1. 打开 <代理主目录> 目录中的 `IntroscopeAgent.profile` 文件。
2. 将在代理配置文件中找到的属性与 CA Introscope 代理配置文件属性中的属性说明进行比较。例如，您可能要从默认设置更改这些属性：
  - `introscope.agent.decorator.enabled`— .NET 代理的默认设置为 `true`，这会启用问题解决方案分类功能。
  - `introscope.agent.decorator.security`— 将默认设置从 `clear` 更改为 `encrypted`；这可以确保事务头中机密信息的安全。
3. 如果需要修改默认值，可能需要将属性添加到 `IntroscopeAgent.profile` 文件，然后对其进行配置。
4. 保存对 `IntroscopeAgent.profile` 文件所做的更改。
5. 继续执行在 [.NET 环境中重新加载代理属性](#) (p. 351)。

**提示：** 如果未列出属性，可能会导致混淆，因此，一种好方法是显式包含该属性，即使默认值是所需的值。

### 在 .NET 环境中重新加载代理属性

必须重新启动代理才可使受控应用程序完成集成。

重新启动 CLR 将重新加载代理属性，并启用 `AutoProbe` 和 `HTTPHeaderDecorator`。

#### 在 .NET 代理上重新加载代理配置文件属性：

1. 重新启动代理以重新加载代理属性。
2. 返回至 [与 .NET 代理集成](#) (p. 349)，然后针对每个代理重复这些过程。

### 验证 Introscope 配置

如果您尚未为 CA APM 配置 CA CEM，请转到 [配置 CA CEM 的清单](#) (p. 334)。

有关配置验证和故障排除的信息，请参阅“[Introscope 与 CA CEM 集成故障排除](#) (p. 352)”。

## CA Introscope 与 CA CEM 集成故障排除

可能需要对 CA CEM 与 CA Introscope 的集成进行故障排除。本节介绍了高级别验证步骤并包含故障排除部分。

本部分包括以下主题：

[验证 CA CEM 上的 CA Introscope 集成](#) (p. 352)

[症状和解决方案](#) (p. 353)

### 验证 CA CEM 上的 CA Introscope 集成

可以通过几种方式验证 CA CEM 上的集成。

#### 验证 CA CEM 上的 CA Introscope 功能：

1. 验证企业管理器配置是否正确。  
请参阅[配置 CA Introscope 设置](#) (p. 335)。
2. 验证与企业管理器之间的通信。
  - a. 选择“系统” > “事件”。
  - b. 确保在企业管理器与代理之间没有未解决的通信错误。
  - c. 确保在企业管理器与 TIM 之间没有未解决的通信错误。
  - d. 请参阅[查看 CA CEM 事件](#) (p. 294)。
3. 同步所有监视器，以向代理发送最新的域配置信息，其中包括事务定义、缺陷规范和事务跟踪参数。(也发送给所有已启用的 TIM 监视器。)
  - a. 选择“设置” > “监视器”。
  - b. 单击“同步所有监视器”。
  - c. 确认企业管理器与代理的通信处于活动状态。请查看代理日志文件。
4. 查看企业管理器日志，了解任何相关错误消息。搜索与 CA CEM 相关的消息。例如，在日志的消息中搜索“tess”或“Biz”。
5. 确认事务跟踪会话正在按预期运行。请参阅[查看事务跟踪会话信息](#)。
6. 确认实时事务度量标准功能已通过 TIM 收集服务启用。请参阅[为客户体验度量标准选择 TIM](#) (p. 248)。
7. 验证每个 TIM 上是否均已启用实时事务度量标准功能。  
请参阅[在 TIM 上对客户体验度量标准进行故障排除](#) (p. 339)。



## 症状和解决方案

下列主题提供了一些提示，可帮助您对 CA Introscope 与 CA CEM 的集成进行故障排除。

### 类别

[.NET](#) (p. 353)

[事件和日志](#) (p. 354)

## .NET

### 症状

将 .NET 事务定义为基于 IP 地址的主机名匹配时，无法识别这些事务。（在同样条件下，通过 Java 代理监控的事务可以识别，并通常显示在“调查器”树中。）

### 可能的解决方案

将主机名更改为基于大写主机名匹配，而非基于 IP 地址匹配。（“业务服务” > “业务事务” > “事务” > “组件” > “标识”）。

### 症状

如果 .NET wily.Agent 程序集版本与 CA CEM 的 .NET 代理扩展的版本号不匹配，则 .NET 代理不重新启动。

### 可能的解决方案

按照配置代理 .NET 版本中定义的说明进行操作。

**注意：**必须完全按照步骤执行操作。如果未正确更新 machine.config 文件，.NET 代理将无法启动。

*CA Introscope 上更严重的问题是：*

有时，如果扩展的版本号不同于 .NET 代理的版本号，独立代理安装程序将无法正确安装扩展（如 DLL）。

这种情况的变通方法有以下两种：

- 逐个配置应用程序以接受不同的版本号。

或者

- 全局配置所有应用程序以接受不同的版本号。

**注意：**仅选择使用一个解决方法；不要同时执行这两个解决方法。

有关详细信息，请参阅《CA APM .NET 代理实施指南》。

## 事件和日志

### 症状

当同步监视器时，显示企业管理器日志文件消息：

无法将域配置 xml 文件发送到收集器企业管理器。企业管理器未定义必要服务。

**注意：**当您有 CA CEM 4.x 的代理时，可能会出现这种情况。

### 可能的解决方案

确认 CEMDefinitionHandler 企业管理器扩展已经先安装在 MOM 上，然后再安装在每个收集器上，安装顺序不能更改。

还必须重新启动每个企业管理器的 JVM，才能完成集成。

有关详细信息，请参阅[配置企业管理器](#) (p. 345)。

## 升级注意事项

既然 TESS 是企业管理器的一部分：

- 先前随 CEMTracer 一起提供的功能现在由 BizTrxHttpTracer 提供，这是默认启用的。（BizTrxHttpTracer 也支持代理记录功能。）
- 单击“同步所有监视器”时，CA CEM 会通知企业管理器，且域配置信息文件 (*domainconfig.xml*) 会存储在共享的 APM 数据库中。
- 不再生成 TESS 日志文件。之前写入 TESS 日志文件的消息现在写入位于 *<EM\_Home>/logs* 的企业管理器日志文件中。

在升级 CA CEM 或 CA Introscope 以进行 CA APM 集成之前，应复查《CA APM 安装和升级指南》中的特定产品升级要求。

对于 CA CEM 与 CA Introscope 的集成，强烈建议在实际开始单个过程之前计划您的升级。通过考虑自己的独特环境和特殊要求，可以避免在执行操作过程中出现不必要的问题。

## 设置业务应用程序

当您按照《CA APM 事务定义指南》中介绍的操作设置业务应用程序时，请确保使用 CA SiteMinder 设置。

### 确认业务应用程序的正确设置：

1. 确保“身份验证类型”为 CA SiteMinder。
2. 确保“用户标识”参数类型为 CA SiteMinder，参数名称为 Username 或 DistinguishedName。

对于某些类型的 CA SiteMinder 身份验证（匿名身份验证和基于证书的身份验证），SM\_AGENTAPI\_ATTR\_USERNAME 为空白。在这种情况下，必须使用 SM\_AGENTAPI\_ATTR\_USERDN（可分辨名称）的值来标识用户。

3. 确保“会话标识”参数类型为 CA SiteMinder，参数名称为 SessionId。



## 第 25 章：将 CA SiteMinder 与 CA CEM 集成

---

CA CEM 与 CA SiteMinder 安全软件配合使用。CA SiteMinder 提供安全功能，如单点登录和集中控制对 Web 应用程序的用户访问。

对于简单身份验证，也许可以使用 cookie 标识用户和会话，而无需使用 CA SiteMinder 插件（无需遵循本章中介绍的过程）。

如果始终在头中观测到用户名和会话 ID，并且会话 ID 未更改或过期，请考虑使用 cookie 参数标识用户和会话，例如，SMUSER 和 SMSESSION 或者 HTTP\_SM\_USER 和 HTTP\_SM\_SESSION。

如果使用单点登录 (SSO) 或到期的 cookie，则肯定需要使用本章所述的 CA SiteMinder 插件。在这些情况下，较简单的 cookie 方法将不起作用，因为请求头并非一致性地包含用户名和静态 cookie。然后，TIM 需要与 CA SiteMinder 服务器进行通信，以确定用户和会话。

此部分包含以下主题：

[CA SiteMinder 的清单](#) (p. 357)

[在 CA CEM 上配置 CA SiteMinder](#) (p. 358)

[创建自定义 CA SiteMinder 代理](#) (p. 359)

[定义 CA CEM 上的策略服务器](#) (p. 360)

[定义 CA CEM 上的代理](#) (p. 360)

[查看 TIM SiteMinder 主机配置](#) (p. 361)

[启用 CA SiteMinder](#) (p. 361)

[CA SiteMinder 与 CA CEM 集成故障排除](#) (p. 362)

### CA SiteMinder 的清单

以下列表显示了您需要了解的关于 CA CEM 与 CA SiteMinder 集成的内容。

**与 CA SiteMinder 集成：**

1. 在 CA SiteMinder 中，为 CA CEM 创建自定义代理类型。请参阅“[在 CA SiteMinder 上为 CA CEM 创建自定义代理类型](#) (p. 359)”。
2. 在 CA SiteMinder 中，为每个 TIM 创建自定义代理。请参阅“在 CA SiteMinder 上为每个 TIM 创建自定义代理”。
3. 定义共享密钥。请参阅“[在 CA CEM 上配置 CA SiteMinder](#) (p. 358)”。
4. 定义策略服务器。请参阅“[在 CA CEM 上定义策略服务器](#) (p. 360)”。

5. 定义代理名称。请参阅“[在 CA CEM 上定义代理](#) (p. 360)”。
6. 启用 CA SiteMinder。请参阅“[启用 CA SiteMinder](#) (p. 361)”。
7. 设置业务应用程序，以指定 CA SiteMinder 身份验证。请参阅“[设置业务应用程序](#) (p. 354)”。
8. 确认 CA CEM 与 CA SiteMinder 配合使用。请参阅“[CA SiteMinder 与 CA CEM 集成故障排除](#) (p. 362)”。

## 在 CA CEM 上配置 CA SiteMinder

为了使 CA CEM 能与 CA SiteMinder 配合使用，必须配置 CA SiteMinder 插件。

### 在 CA CEM 上配置 CA SiteMinder:

1. 选择“设置” > “插件”。  
此时将显示“插件”页面。
2. 选择“CA SiteMinder”。  
此时将显示“CA SiteMinder 插件” > “常规”页面。
3. 在“启用 CA SiteMinder 插件”下选择以下选项之一，以激活 CA CEM 与 CA SiteMinder 的集成：
  - 4.x API
  - 5.x API

**注意：**CA CEM 与 SiteMinder 的集成使用以下两种方法与策略服务器通信：

- 第一种方法称为 4.x API，它使用称为“普通共享密钥”的进程。
- SiteMinder 还支持一种更安全的方法，即使用称为“基于主机的注册”的进程向策略服务器注册代理并使代理与策略服务器通信。这被称为 5.x API。

CA CEM 与 SiteMinder 的集成支持这两种方法。

4. 键入会话 cookie 名称，其将以加密形式存储 CA SiteMinder 用户会话信息。  
**注意：**默认的会话 cookie 名称为 SMSESSION。
5. 键入共享密钥，其将与自定义代理名称一起用于对自定义代理与 CA SiteMinder 策略服务器之间的通信进行加密。

**注意：**仅当您在步骤 3 中选择 4.X API 时才显示“共享密钥”字段。

共享密钥是一个文本值，必须与在 CA SiteMinder 上配置 CA CEM 自定义代理时赋予的值相匹配。

**注意：**配置 CA SiteMinder 时，所有 CA CEM 代理必须使用相同的共享密钥。

6. 单击“强制注册”。

如果要更改主机配置对象名称或在 TIM 中重新生成主机配置文件，您可以使用“强制注册”。

**注意：**仅当您在步骤 3 中选择 5.X API 时才启用“强制注册”字段。

7. 单击“保存”。

## 创建自定义 CA SiteMinder 代理

以下步骤描述了如何将 CA CEM 与 CA SiteMinder 策略服务器集成。您将在 CA SiteMinder 策略服务器上执行这些步骤。

### 在 CA SiteMinder 上为 CA CEM 创建自定义代理类型

仅需要执行以下步骤一次。如果有多个 TIM，无需多个自定义代理类型。

**注意：**以下过程描述了在 CA SiteMinder r6 中执行的步骤。如果您有更高版本，则具体步骤可能会有所不同，但是必须执行相同的功能。

**在 CA SiteMinder 上为 CA CEM 创建自定义代理类型：**

1. 在策略服务器上打开浏览器，然后输入 CA SiteMinder URL。例如：  
`http://<IP_Address>/site minder/smadmin2.html`
2. 单击 **Administer** 策略服务器，并使用 Java 小程序定义新的代理类型。
3. 在“对象”窗格（左）上，单击“系统”选项卡。
4. 从“视图”菜单中，确认已选中“代理类型”。
5. 单击“对象”窗格上的“代理类型”图标。
6. 从“编辑”菜单中，选择“创建代理类型”。
7. 键入自定义代理用于标识自己的名称，例如 *TIMAgent*。
8. 输入自定义代理类型的说明。
9. 在“代理类型定义”选项卡上，将“RADIUS 设备”复选框保留为未选中状态以及将“IETF 供应商 ID”文本框保留为空。
10. 如果未定义任何操作，请定义新的操作并将“类型”设置为“已验证身份”。

## 定义 CA CEM 上的策略服务器

策略服务器是一个 CA SiteMinder 组件,用于为 Web 应用程序提供授权和身份验证。一个 CA SiteMinder 配置可以包括多个策略服务器。

### 定义策略服务器:

1. 选择“设置”>“插件”。此时将显示“插件”页面。
2. 选择“CA SiteMinder Web Access Manager”。
3. 在“CA SiteMinder 插件”页面上,选择“策略服务器”。
4. 单击“新建”。

此时将显示“策略服务器”页面。

**适用于: 5.x API**—如果选择 5.x API 插件,则可以添加包含主机配置对象的单个策略服务器。

可以在主机配置对象中添加多个策略服务器。

有关详细信息,请参阅《CA SiteMinder 策略服务器配置指南》中的主题“受信任主机的主机配置对象”。

5. 输入安装策略服务器的计算机的 IP 地址和身份验证端口。
  6. **适用于: 5.x API**—如果选择了 5.x API 插件,请在以下字段中输入信息:
    - SiteMinder 管理用户名
    - SiteMinder 管理员密码
- 注意:** 要进行注册,您所提供的用户名和密码应具有正确的权限。
7. 单击“保存”。

## 定义 CA CEM 上的代理

CA SiteMinder 代理是一个软件模块,用于授权安全资源请求,并将这些请求转发到 CA SiteMinder 策略服务器。

在“插件代理”页面上,将列出代理和关联的监视器 (TIM)。代理和监视器最初具有相同的名称。更改代理名称,以便与 CA SiteMinder 所使用的代理名称完全匹配。

### 定义代理:

1. 选择“设置”>“插件”。  
此时将显示“插件”页面。



2. 选择“CA SiteMinder”。
3. 在“CA SiteMinder 插件”页面上，选择“代理”。

此时将显示“代理”页面。

**适用于：5.0 API**—如果您已使用 5.0 API 启用 CA SiteMinder，则“SiteMinder 主机配置”字段也会显示在“代理”页面中。

4. 在“代理”页面上，单击代理的“IP 地址”。

此时将显示“监视器”页面。

**适用于：5.0 API**—如果您已使用 5.0 API 启用 CA SiteMinder，则“SiteMinder 代理名称”字段和“SiteMinder 主机配置”字段也会显示在“监视器”页面中。

5. 更新 CA SiteMinder 代理名称，以便与 CA SiteMinder 使用的名称完全匹配。
6. 单击“保存”。

## 查看 TIM SiteMinder 主机配置

请执行以下步骤：

1. 访问 TIM 系统设置页面。
2. 单击“查看 TIM SiteMinder 主机配置”。

将显示主机配置文件。

**注意：**有关如何访问“TIM 系统设置”页面的信息，请参阅“访问 CEM 控制台和设置页面”。

## 启用 CA SiteMinder

为了使 CA CEM 能与 CA SiteMinder 配合使用，必须启用 CA SiteMinder 插件。

**在 CA CEM 上启用 CA SiteMinder：**

1. 选择“设置”>“插件”。
- 此时将显示“插件”页面。
2. 选择“CA SiteMinder”。
  3. 选中“启用 CA SiteMinder 插件”复选框。
  4. 单击“保存”。

## CA SiteMinder 与 CA CEM 集成故障排除

确认 CA CEM 与 CA SiteMinder 配合使用:

1. 确认已启用 CA SiteMinder。  
请参阅[启用 CA SiteMinder](#) (p. 361)。
2. 确认策略服务器使用正确的 IP 地址和端口。  
请参阅[在 CA CEM 上定义策略服务器](#) (p. 360)。
3. 验证 CA CEM 和 CA SiteMinder 是否使用相同的共享密钥。  
请参阅[创建自定义 CA SiteMinder 代理](#)。
4. 验证 CA CEM 和 CA SiteMinder 是否使用相同的代理名称。  
请参阅[在 CA CEM 上定义代理](#) (p. 360)。
5. 确认已正确设置业务应用程序。  
请参阅[设置业务应用程序](#) (p. 354)。
6. 在 CA CEM 中, 选择“设置”>“监视器”>“同步所有监视器”, 以同步监视器。
7. 在 CA CEM 中, 选择“设置”>“监视器”>“IP 地址”, 以在 TIM 日志中查看确认消息或任何 CA SiteMinder 错误消息。
8. 检查 CA SiteMinder 代理日志中是否有错误消息。
9. 在 CA SiteMinder 中, 检查策略服务器日志中是否有错误。

# 第 26 章： 将 CA Service Desk 与 CA CEM 集成

---

可以将 CA CEM 突发事件和缺陷信息发送到 CA Service Desk，以便生成票证并根据需要进行跟踪。

CA Service Desk 通过使服务支持突发事件管理自动执行来利用 IT 基础设施库 (ITIL) 最佳做法流程。

此部分包含以下主题：

[关于 CA Service Desk 与 CA CEM](#) (p. 363)

[CA Service Desk 集成概述](#) (p. 363)

[为 CA CEM 配置 CA Service Desk](#) (p. 364)

[同时使用 CA Service Desk 与 CA CEM](#) (p. 367)

[CA Service Desk 与 CA CEM 集成故障排除](#) (p. 368)

[CA Service Desk 到 CA CEM 的集成术语](#) (p. 370)

## 关于 CA Service Desk 与 CA CEM

CA Service Desk 支持技术支持分析员履行其突发事件管理职责，包括检测和记录、分类和支持以及跟踪并解决突发事件。

您可以配置 CA CEM 和 CA Service Desk，以基于 CA CEM 检测到的突发事件在 CA Service Desk 中创建服务请求（或突发事件）。

## CA Service Desk 集成概述

通过从 CA CEM 突发事件自动生成服务请求，与 CA Service Desk 的集成支持突发事件管理。

要在 CA Service Desk 中创建 CA CEM 突发事件，请配置并启用 CA Service Desk 插件。配置过程中会建立通信，并且定义突发事件在 CA Service Desk 中的显示方式。

如果希望在 CA Service Desk 中分隔开 CA CEM 生成的突发事件，请在 CA Service Desk 中创建请求区域。

有关与集成相关的术语，请参阅 [CA Service Desk 与 CA CEM 集成术语](#) (p. 370)。有关所有 CA APM 术语和定义，请参阅 *CA APM 术语*。

## 为 CA CEM 配置 CA Service Desk

要启用 CA Service Desk，必须首先配置 CA Service Desk 插件。

(可选)可以创建 CA Service Desk 请求区域，以便将 CA CEM 突发事件与 CA Service Desk 中的其他服务请求分开。

### 配置 CA Service Desk 插件

您需要收集用于实施 CA Service Desk 插件的连接和请求信息。

#### 配置 CA CEM 以与 CA Service Desk 通信：

1. 选择“设置” > “插件”。  
此时将显示“插件”页面。
2. 选择“CA Service Desk”。  
此时将显示“CA Service Desk 插件”页面。
3. 选中“启用 CA Service Desk 插件”复选框。  
这将允许 CA CEM 将突发事件信息发送到 CA Service Desk。  
**注意：**您必须启用 CA Service Desk 插件，否则集成将不起作用。
4. 外部可解析主机名—在大多数情况下，该字段已经包含 CA CEM 主机名。如果没有包含，请键入企业管理器的 IP 地址或主机名。  
该信息用于 CA Service Desk 生成的电子邮件中的链接。CA Service Desk 电子邮件包括一个返回到 CA CEM 中突发事件的链接。
5. 端口—在大多数情况下，该字段已经包含 CA CEM 端口。  
**注意：**默认端口为 8081。它在 `IntroscopeEnterpriseManager.properties` 文件中定义为 `introscope.enterprisemanager.webserver.port=8081`，可以进行更改。
6. 输入 CA Service Desk 连接信息：
  - a. 主机名—键入托管 CA CEM 的 CA Service Desk 系统的主机名或 IP 地址。
  - b. 端口—键入 CA CEM 连接到 CA Service Desk 所用的端口。用于 CA Service Desk 的默认端口号为 8080。
  - c. 用户名—键入访问 CA Service Desk 的 CA CEM 用户名。该用户应当具有相应的权限和访问级别，才可在 CA Service Desk 中创建请求。
  - d. 密码—键入与用户名关联的密码。

7. 如果希望在 CA Service Desk 中将 CA CEM 突发事件创建为突发事件（而不是请求），请选中“在 Service Desk 中创建 ITIL 突发事件”复选框。

如果不希望在 CA Service Desk 中创建突发事件，则默认行为是创建请求。

**注意：**只有当已经对 CA Service Desk 配置 ITIL（IT 基础架构库）时，才会创建 CA Service Desk 突发事件。否则，会将 CA CEM 突发事件创建为请求。

8. 键入请求区域一键入在 CA Service Desk 中创建的请求区域，以便将与 CA CEM 相关的问题进行分类。

该请求区域应当与您在 CA Service Desk 中创建的名称相同。

9. 根据需要键入请求筛选。

**提示：**可以使用请求筛选，先测试与单个业务服务和业务事务的集成，而不是允许将所有突发事件立即转发到 CA Service Desk。

语法示例	说明
<i>Request Filter=BusinessServiceName/BusinessTransactionName</i>	只有针对指定的业务服务和业务事务发生突发事件时，才会在 CA Service Desk 中创建请求。
<i>Request Filter=BusinessServiceName/*</i>	在 CA Service Desk 中，为所有突发事件以及针对指定的业务服务触发的任何业务事务创建请求。
<i>Request Filter=BusinessServiceName/Tra*</i>	在 CA Service Desk 中，为所有突发事件以及针对指定的业务服务触发的、并以“Tra”开头的任何业务事务创建请求。
<i>Request Filter=**</i>	在 CA Service Desk 中，为与所有业务服务和所有业务事务关联的突发事件创建请求。

如果业务服务或业务事务名称包含正斜杠（“/”）字符，必须在筛选中将其替换为双斜杠（“//”）。

如果业务服务或业务事务名称包含逗号（“,”）字符，必须在筛选中将其替换为斜杠逗号（“/,”）。

例如，如果

- 业务服务名称 = Trade
- 业务事务名称 = Sell Big/Medium Stocks

筛选应为:

*Request Filter=Trade/Sell Big//Medium Stocks*

例如, 如果

- 业务服务名称 = Trade
- 业务事务名称 = Sell Big, Medium Stocks

筛选应为:

*Request Filter=Trade/Sell Big/, Medium Stocks*

10. 键入请求摘要, 它将显示在 CA Service Desk 摘要。使用以下变量可创建自定义摘要:

- *<defect\_name>*
- *<business\_service>*
- *<business\_transaction>*

您可以重新排列变量来创建自己的请求摘要。当请求摘要在 CA Service Desk 中显示时, 每个变量将替换为实际值。示例:

*<defect\_name> for <business\_service>,<business\_transaction>*

显示为以下类似内容: Slow Time for Support Desk, KB Lookup

*Business Transaction: <business\_transaction> Defect: <defect\_name>*

显示为以下类似内容: Business Transaction: CheckOut Defect: Slow Time

11. 键入请求说明, 它将显示在 CA Service Desk 说明中。使用以下变量可创建自定义说明:

- *<incident\_id>*
- *<defect\_name>*
- *<business\_service>*
- *<business\_transaction>*
- *<user\_count>*
- *<defect\_count>*
- *<incident\_link>*

您可以重新排列变量来创建自己的请求说明。当请求说明在 CA Service Desk 中显示时, 每个变量将替换为实际值。

*<incident\_link>* 变量将在 CA Service Desk 中提供一个链接。您可以使用该链接直接转到突发事件概览信息 ( “CEM” > “突发事件管理” > “突发事件概述” ) 。

12. 创建 Service Desk 请求的条件是，突发事件重要级别为一启用选定的突发事件级别，以在 CA Service Desk 中创建服务请求。选中适当的复选框：

- 低
- 中等
- 严重
- 紧急

13. 单击“保存”。

与您保存的配置相匹配的未来 CA CEM 突发事件将会在 CA Service Desk 中触发服务请求，并且立即生效。

**注意：**如果在 CA CEM 中有任何现有的突发事件处于打开状态，则它们不会触发 CA Service Desk 请求。

## 配置 CA Service Desk 请求区域

如果希望针对 CA CEM 报告的突发事件有一个单独的请求区域，需要在 CA Service Desk 中创建请求区域。

**在 CA Service Desk 中为 CA CEM 配置请求区域：**

1. 创建请求区域，例如 *CEM\_reported*。
2. 将以下三个属性附加到请求区域：
  - 业务服务
  - 业务事务
  - 突发事件

有关创建和配置请求区域的信息，请参阅 CA Service Desk 联机帮助中的“定义请求区域”。

## 同时使用 CA Service Desk 与 CA CEM

在 CA Service Desk 中，会看到 CA CEM 突发事件信息。可以在 CA Service Desk 中单击指向 CA CEM 的链接，以了解有关突发事件的详细信息。

可以在 CA CEM 中浏览，以进行故障排除并发现突发事件的根本原因。

## CA Service Desk 与 CA CEM 集成故障排除

您可能需要对与 CA Service Desk 的集成进行故障排除。本节提供了故障排除表。



## 症状和解决方案

该表提供了一些提示，可帮助您对 CA Service Desk 与 CA CEM 的集成进行故障排除。

### 症状：

CA Service Desk 请求不是针对任何或某些 CA CEM 突发事件创建的。

### 解决方案：

验证是否在 CA CEM 中正确配置了 CA Service Desk 插件：

配置正确的 CA Service Desk 凭据。

针对正确的业务服务和业务事务设置适当筛选。

启用适当的重要级别。

查看日志文件，是否存在连接或其他错误：

`http://<IP_Address>/cgi-bin/wily/packages/cem/service-desk/index`

### 症状：

在没有请求区域的情况下创建了 CA Service Desk 请求。

### 解决方案：

确认 CA Service Desk 管理员创建了请求区域。

确认 CA CEM CA Service Desk 插件配置包括正确的请求区域信息。

### 症状：

从 CA Service Desk 突发事件或请求跳转到 CA CEM 突发事件详细信息的链接不起作用。

### 解决方案：

突发事件可能已从 CA CEM 数据库中删除。

检查“设置”>“突发事件设置”>“突发事件过时规则”。

### 症状：

CA Service Desk 电子邮件中跳转到 CA CEM 突发事件详细信息的链接不起作用。电子邮件中的链接可能如下所示：

`http://localhost.localdomain/wily/cem/tess/...`

### 解决方案：

确认 CA CEM CA Service Desk 插件配置包括 CA CEM 的外部可解析主机名。

突发事件可能已从 CA CEM 数据库中删除。检查“设置”>“突发事件设置”>“突发事件过时规则”。

**症状:**

在 CA CEM 中关闭某突发事件时，该突发事件在 CA Service Desk 中不关闭。

**解决方案:**

必须单独在 CA Service Desk 中关闭突发事件/服务请求。

**症状:**

在 CA Service Desk 中关闭突发事件/服务请求时，该请求在 CA CEM 中不关闭。

**解决方案:**

必须单独在 CA CEM 中关闭突发事件。

## CA Service Desk 到 CA CEM 的集成术语

产品集成的一个重要方面是术语。您需要了解自己不熟悉的产品语言。还需要了解 CA CEM 中的术语和定义如何与 CA Service Desk 中的术语相对应。

### CA Service Desk 术语

这些 CA Service Desk 术语与产品集成有关。

**突发事件**

导致 IT 基础架构的服务质量下降的任何事件。

**请求区域**

CA Service Desk 系统管理员会设置请求区域以按类型分类服务请求。例如，硬件支持或软件安装。

**服务请求**

用户要求提供支持、信息或帮助的请求，这并不代表 IT 基础架构中出现故障。

**票单**

票单是 CA Service Desk 中的常用术语，可以表示请求、突发事件或问题。CA Service Desk 中的 CA CEM 突发事件分类为请求或突发事件。

## CA Service Desk 与 CA CEM 的术语对应关系

产品可能有不同的演变周期和不同的核心用户。这些差异通常意味着产品术语和定义也有所不同。

有时存在一对一的对应关系（例如，一个产品中的突发事件在另一产品中可能称为票单）。并且，有时同一术语在不同的产品中的意思也可能略有不同，这可能会令人困惑。

这些术语对应关系将帮助您完成产品集成。

---

CA CEM 术语	CA Service Desk 术语对应关系
-----------	------------------------

---

突发事件	CA CEM 突发事件将基于 CA Service Desk 配置和 CA CEM 配置（“设置” > “插件”）触发服务请求或突发事件。
------	---

---



# 第 27 章：将 CA APM Cloud Monitor 与 CA APM 相集成

通过 CA APM Cloud Monitor，您可以执行以下任务：

- 了解来自 40 多个国家/地区的 60 多个监控站的完整用户体验。
- 监控实际浏览者以准确衡量用户体验。
- 监控由 SaaS 供应商和 MSP 提供的应用程序使其对 SLA 负责。
- 从防火墙外部测试应用程序响应时间（使用综合事务）来了解全球最终用户体验，并且甚至在没有实际用户流量的时候监控性能。
- 复制实际用户事务以监控整个应用程序基础架构的性能，从而快速地识别、诊断和解决问题。

## 如何将 CA APM Cloud Monitor 与您的 CA APM 部署相集成

作为 APM 管理员，您可以将 CA APM Cloud Monitor 集成到 CA APM 部署中，以便增加额外的监控和分类能力。

以下流程图显示了如何在 CA APM 内部部署中集成 CA APM Cloud Monitor。



1. 下载并安装 CA APM Cloud Monitor 代理。(see page 374)
2. 验证代理连接。(see page 374)

## 下载并安装 CA APM Cloud Monitor 代理

在此任务中，您要下载并安装集成 CA APM Cloud Monitor 和 CA APM 所需的 CA APM Cloud Monitor 代理。

**注意：**您可以在网络中的任何计算机上安装 CA APM Cloud Monitor 代理。其功能是通过 Internet 接收 CA APM Cloud Monitor 数据，并将数据转发给企业管理器，因此它可以是任何计算机（虽然您应选择具有服务器级别 CPU/RAM 的计算机）。

### 下载并安装 CA APM Cloud Monitor 代理：

1. 下载 CA APM Cloud Monitor 代理存档文件。将文件保存到您的计算机。

Windows、Linux 和 Solaris 的安装程序位于 CA APM 软件下载网站上。

2. 安装代理。
  - a. 启动 CA APM Cloud Monitor 安装程序文件。
  - b. 接受许可条款。
  - c. 指定 <代理主目录> 目录。
  - d. 指定代理将连接到的企业管理器主机和端口。
  - e. 在 Cloud Monitor 帐户设置屏幕中，输入您的 CA APM Cloud Monitor 用户 ID 和密码。这与用来登录 CA APM Cloud Monitor 网站的凭据相同。

CA APM Cloud Monitor 代理安装完成。

**注意：**有关启动代理且验证连接方面的说明，请参阅“Validate the CA APM Cloud Monitor Agent Connection (see page 374)”。

## 验证 CA APM Cloud Monitor 代理连接

要验证是否已正确安装 CA APM Cloud Monitor 代理，请启动代理，并使用 CA APM WebView 或 Workstation 检查数据。通过确认来自 CA APM Cloud Monitor 的传入数据是当前的来验证连接。

**注意：**要在 WebView 或 Workstation 中查看 CA APM Cloud Monitor 数据，必须在 CA APM Cloud Monitor 中设置文件夹和监视器。如果尚未执行此步骤，请参阅《CA APM Workstation 用户指南》中与使用 CA APM Cloud Monitor 相关的部分。

**请执行以下步骤：**

1. 导航到安装 CA APM Cloud Monitor 代理的目录，然后运行以下文件之一以启动代理。
  - 在 Windows 中，双击 APMCloudMonitor.bat。
  - 在 Linux 或 Solaris 上，运行 APMCloudMonitor.sh。代理在一个控制台窗口中启动。
2. 启动 CA APM WebView 或 Workstation。
3. 在 CA APM Cloud Monitor 中找到数据。
  - a. 如果未打开“调查器”窗口，请选择“文件” > “新建调查器”。
  - b. 浏览至“度量标准浏览器”选项卡。
  - c. 展开以下节点：

```
SuperDomain | <Host_Name> | APMCloudMonitor |  
APMCloudMonitorAgent | APM Cloud Monitor
```

<Host\_Name> 通常为安装 CA APM Cloud Monitor 代理的计算机，但在“度量标准浏览器”树中会显示 APMCloudMonitor.properties 文件中的属性 apmcm.agent.hostName 的值。
  - d. 展开文件夹以查看各个度量标准，并确认这些度量标准是最新的。

**故障排除**

如果您无法在企业管理器安装过程期间选择“Cloud Monitor”作为监控选项，WebView/Workstation 不会允许全面显示 CA APM Cloud Monitor 数据。

改正此问题：

- 将 <企业管理器主目录>\examples\CAAPMIntegrationForCloudMonitor\ 目录的内容复制到 <企业管理器主目录>/config/modules/ 和 <企业管理器主目录>/ext/xmltv。

这样，系统即可准备好管理模块和其他文件，以便正确地显示 Cloud Monitor 度量标准数据。

## 如何限制数据

为了改善性能，您可以限制 CA APM Cloud Monitor 代理向企业管理器发送的数据量。

### 通过配置 CA APM Cloud Monitor 属性来限制数据

您可以使用文件 `APMCloudMonitor.properties` 中的属性来筛选 CA APM Cloud Monitor 代理向企业管理器发送的数据。

要通过配置 CA APM Cloud Monitor 代理属性来筛选数据，请编辑 `<CloudMonitor 代理主目录>/CloudMon/conf/APMCloudMonitor.properties` 中的度量标准筛选部分。

有关这些设置的信息，请参阅“`APMCloudMonitor.properties` (see page 484)”的属性参考。

### 通过删除检查点来限制数据

CA APM Cloud Monitor 具有对五大洲内超过六十个检查点工作站的访问权限。它从这些工作站中进行随机选择，并检查工作站到您的网站或应用程序的可用性和性能。随着时间的推移，所有启用的工作站都将执行此检查，从而导致记录来自超过六十个站点的数据。

您可以删除一些可用的检查点工作站，以限制 CA APM Cloud Monitor 发送到 CA APM 的数据量。

请执行以下步骤：

1. 登录到 CA APM Cloud Monitor 网站：`cloudmonitor.ca.com`。
2. 选择“订阅” > “首选项”。  
默认情况下，会选择所有工作站。
3. 更改默认选择：
  - 清除各个工作站的复选框，或执行以下操作：
  - 单击“清除”全部清除，然后从列表顶部的组中进行选择。  
例如，要仅选择北美的工作站：
    - a. 单击“清除”。
    - b. 单击“北美”。
4. 在页面的底部，单击“更改”。

### 通过调整排定来限制数据

默认情况下，监视器定期（每天每小时）检查可用性以及性能。随着时间的推移，这可能会导致向 CA APM 返回的数据比您希望的要多。



请执行以下步骤：

1. 登录到 Cloud Monitor 网站：[cloudmonitor.ca.com](https://cloudmonitor.ca.com)。
2. 选择“设置”>“监视器”。
3. 选择单个监视器，然后选择“更多选项”。
4. 重置以下设置：
  - 检查之间的延迟
  - 检查周期
  - 仅在这些日子检查
  - 维护排定



# 附录 A: 属性文件参考

---

下面是位于这些目录中的、允许您用来控制企业管理器、工作站和 WebView 设置的属性文件。

**重要信息!** 在 Windows 计算机上, 在属性文件中添加路径时, 您必须使用一个反斜线 (\) 对另一个反斜线进行转义 (使用两个反斜线) — 例如: `C:\\Introscope\\lib\\Agent.jar`。

此部分包含以下主题:

[IntroscopeEnterpriseManager.properties](#) (p. 379)

[APMEnterpriseManager.properties](#) (p. 423)

[apm-events-thresholds-config.xml](#) (p. 427)

[ResourceMetricMap.properties](#) (p. 440)

[Catalyst.properties](#) (p. 442)

[EMservice.conf](#) (p. 451)

[Introscope Enterprise Manager.lax](#) (p. 457)

[IntroscopeWorkstation.properties](#) (p. 463)

[Introscope Workstation.lax](#) (p. 467)

[IntroscopeWebView.properties](#) (p. 472)

[Introscope WebView.lax](#) (p. 479)

[APMCloudMonitor.properties](#) (p. 484)

## IntroscopeEnterpriseManager.properties

企业管理器的很多行为是由在三个企业管理器属性文件之一 *IntroscopeEnterpriseManager.properties* 中定义的属性控制的。(另外两个文件是 [APMEnterpriseManager.properties](#) (p. 423) 和 [apm-events-thresholds-config.xml](#) (p. 427)。)

在配置大多数企业管理器属性后, 必须重新启动企业管理器, 您所做的更改才会生效。

不过, 有些企业管理器属性使用 Introscope 热配置服务。更改这些所谓的“热配置”属性之后, 不必重新启动企业管理器。有关更多信息, 请参阅 [热配置服务](#) (p. 387)。

可以在此文件中配置以下属性：

[可用处理器](#) (p. 380)  
[报警行为](#) (p. 381)  
[通讯](#) (p. 381)  
[Workstation 登录参数自动填充部分](#) (p. 386)  
[EM Web 服务器设置](#) (p. 386)  
[热配置服务](#) (p. 387)  
[应用程序启发](#) (p. 388)  
[日志记录](#) (p. 388)  
[永久性集合 - 将数据记录到数据库](#) (p. 389)  
[平面文件属性](#) (p. 391)  
[事务事件数据库](#) (p. 391)  
[事务跟踪采样](#) (p. 392)  
[企业管理器度量标准限制](#) (p. 393)  
[SmartStor](#) (p. 395)  
[基准数据存储](#) (p. 400)  
[SNMP 收集](#) (p. 400)  
[WebView](#) (p. 401)  
[CA APM ChangeDetector](#) (p. 401)  
[管理模块引导](#) (p. 401)  
[管理模块部署](#) (p. 402)  
[群集设置](#) (p. 402)  
[代理交互](#) (p. 406)  
[企业管理器故障切换](#) (p. 410)  
[配置目录](#) (p. 411)  
[应用程序分类地图数据](#) (p. 411)  
[位置视图数据](#) (p. 416)  
[Web Services](#) (p. 416)  
[传出消息队列](#) (p. 416)  
[线程转储](#) (p. 418)  
[用于 Web 服务性能处理的线程属性](#) (p. 420)  
[SNMP 分类视图报警操作](#) (p. 421)  
[应用程序视图对象](#) (p. 423)

## 可用处理器

*IntroscopeEnterpriseManager.properties* 的 Available Processors 节中包含以下属性。

### **introscope.enterprisemanager.availableprocessors**

使用此属性来设置可供此企业管理器使用的处理器数量。如果一台主机上有一个以上的企业管理器，则应使用此属性。

**默认**

<blank>

## **报警行为**

*IntroscopeEnterpriseManager.properties* 的 Alert State Metrics 节中包含以下属性：

### **introscope.enterprisemanager.alertstatemetric.prefix**

在其下显示报警状态度量标准的调查器节点的名称。

**默认**

报警。

## **通讯**

*IntroscopeEnterpriseManager.properties* 的 Port Settings 节中包含以下属性：

### **introscope.enterprisemanager.enabled.channels**

指定企业管理器可以使用的通信通道。要启用某个通信通道，请将该通道类型添加到已启用通道的逗号分隔列表中。要禁用某个通信通道，请将其从列表中删除。

Enabled.channels 属性与

[introscope.enterprisemanager.port.<ChannelName>](#) (p. 382) 属性配合使用。

#### **示例**

如果您具有名为 channel1 和 channel2 的两个通信通道，则您应设置以下属性：

```
introscope.enterprisemanager.enabled.channels=channel1,channel2
introscope.enterprisemanager.port.channel1=5001
introscope.enterprisemanager.port.channel2=5002
```

#### **默认**

channel1

### **introscope.enterprisemanager.port.<ChannelName>**

企业管理器用来与工作站和代理进行加密通信的侦听程序端口。

要创建自定义通信通道，请将下列属性添加到属性文件中：

- introscope.enterprisemanager.port.ChannelName
- introscope.enterprisemanager.serversocketfactory.ChannelName
- *ChannelName* 是新通道的名称。

要启用自定义通道，请将其名称添加到

[introscope.enterprisemanager.enabled.channels](#) (p. 382) 属性中。

#### **默认**

5001

### **introscope.enterprisemanager.serversocketfactory.<ChannelName>**

此属性标识企业管理器用来与工作站和代理进行加密通信的服务器套接字工厂的类名称。

如果您要创建自定义通信通道，请在属性文件中添加一个新属性，例如：

```
introscope.enterprisemanager.serversocketfactory.ChannelName
```

其中，ChannelName 是新通道的名称，将属性值设置为实现了 *com.wily.isengard.postofficehub.link.net.IServerSocketFactory* 接口的自定义服务器套接字工厂的完全限定的类名称。

您还必须指定通道的侦听程序端口，并将其启用，如 [introscope.enterprisemanager.port.<ChannelName>](#) (p. 382) 中所述。

### 示例

如果您具有名为 channel1 和 channel2 的两个通信通道，请进行如下设置：

```
introscope.enterprisemanager.enabled.channels=channel1,channel2
introscope.enterprisemanager.port.channel1=5001
introscope.enterprisemanager.port.channel2=5002
```

您将设置如下所示的 serversocketfactory 属性：

```
introscope.enterprisemanager.serversocketfactory.channel1=<classname>
introscope.enterprisemanager.serversocketfactory.channel2=<classname>
```

### 默认

```
com.wily.isengard.postofficehub.link.net.server.DefaultServerSocketFactory
```

## **introscope.enterprisemanager.serversockets.reuseaddr**

将此属性设置为 true 可允许通信通道服务器套接字重新绑定到处于 *FIN\_WAIT* 或 *TIME\_WAIT* 状态的一个本地端口。在企业管理器重新启动后，应禁用此属性。

默认情况下，不要启用此属性，因为可能有正当的理由表明端口已在使用中。

### 默认

False

### introscope.enterprisemanager.disableInteractiveMode

禁用交互式控制台（决定控制台是否接受输入）。

#### 注释

在许多 UNIX 平台上，如果应用程序试图从标准输入进行读取，则 `nohup` 将不起作用。要以 `nohup` 模式运行，请将此属性设置为 `true`，并在应用程序分类地图数据文件中将 `lax.stdin.redirect` 属性更改为 `<blank>`。如果没有完全按以上所述设置这两个属性，则可能会导致应用程序无法以 `nohup` 模式启动，或导致最大 CPU 使用率。

#### 默认

True

### introscope.enterprisemanager.webserver.port

企业管理器的嵌入式 Web 服务器侦听的端口。

#### 默认

8081

### introscope.enterprisemanager.webserver.portinuse.fail

如果其他应用程序与企业管理器在相同的端口上运行，则阻止企业管理器启动。

如果其他应用程序与企业管理器在相同的端口上运行，则以下属性设置控制是否启动企业管理器：

- 当该属性设置为 `true` 时，将阻止企业管理器启动。
- 当该属性设置为 `false` 时，将显示一条错误消息，指出端口正在使用中。但是，允许启动企业管理器。

#### 默认

true



### introscope.enterprisemanager.ipaddress

将所有企业管理器通信通道（包括嵌入式 Web 服务器）绑定到一个特定的本地 IP 地址。

未配置此属性时，企业管理器接受所有本地地址的连接。

配置此属性时需要考虑的规则：

- 如果此属性配置为 IPv4 地址，则企业管理器将仅接受来自 IPv4 系统上运行的代理或客户端的连接。
- 如果此属性配置为 IPv6 地址，则企业管理器将仅接受来自运行 IPv6 兼容 JVM 的计算机上的代理或客户端的连接。运行 IPv4 JVM 的计算机上的代理或客户端无法使用 IPv6 地址进行连接。
- 如果您没有将在启用了 IPv6 的系统上运行的企业管理器或 WebView 实例绑定到特定的 IP 地址，则该实例将绑定到所有本地地址。它既可以接受来自 IPv4 环境的连接，也可以接受来自 IPv6 环境的连接。
- 工作站、代理、浏览器和其他客户端应当使用 DNS 名称（而不是 IP 地址），来连接到企业管理器或 WebView 实例。
- 代理上的 IPv6 支持依赖于运行该代理的环境（JVM、操作系统、硬件堆栈）中的 IPv6 支持。

默认

<commented out, no value>

### introscope.enterprisemanager.workstation.connection.channel

指定用于连接到 Web Start 工作站的通道。

默认

channel1

### introscope.enterprisemanager.workstation.extendedLiveQuery

这允许 Workstation 用户为实时模式输入自定义时间范围和解析度以代替默认的 8 分钟时间范围和 15 秒的解析度。

**注意：**设置时间范围大于 8 分钟会对企业管理器性能产生负面影响，这是由于 I/O 操作从 smartstor 提取数据)。

默认

TRUE

## Workstation 登录参数自动填充部分

IntroscopeEnterpriseManager.properties 的 Workstation 登录参数部分中包含以下属性：

### **introscope.enterprisemanager.workstation.rememberLogin**

控制 Workstation 是否记住 webstart 的登录参数（企业管理器主机、端口和用户 ID）。如果设为 FALSE，Workstation 不会记住登录参数。

**默认**

TRUE

## EM Web 服务器设置

IntroscopeEnterpriseManager.properties 的“EM Web 服务器设置”部分包含以下属性：

### **introscope.enterprisemanager.webserver.jetty.configurationFile**

Jetty XML 配置文件的路径。要么是绝对路径，要么是 <企业管理器主目录>/config 目录的相对路径。该文件在端口 8444 上创建用于 HTTPS 通信的 SSL 侦听程序。

**注释**

如果您对 introscope.enterprisemanager.webserver.jetty.configurationFile 属性取消注释，则系统不会创建在 IntroscopeEnterpriseManager.properties 文件 introscope.enterprisemanager.webserver.port 属性中指定的不安全的 HTTP 侦听程序。然而，您可以在 Jetty XML 配置文件中配置不安全的 HTTP 侦听程序。

此属性不支持热配置。

**默认**

em-jetty-config.xml

### introscope.enterprisemanager.webserver.max.threads

Web 服务器中的侦听程序线程的最大数量—即企业管理器的嵌入式 Web 服务器能够服务的并发 HTTP 客户端的数量。

#### 注释

仅当超过 80 个 HTTP 隧道代理连接到此企业管理器时才需配置此属性。在这种情况下，CA Technologies 建议您将此属性的值设置为比连接的 HTTP 隧道代理的最大数目大 20。如果您预料并发 HTTP 代理的数目少于 80，则不要修改此属性值。

#### 默认

100

## 热配置服务

企业管理器包括了一个热配置，默认情况下为下列属性启用热配置：

- log4j 日志记录属性—请参阅[日志记录](#) (p. 388)
- 永久性集合—与将数据记录到数据库相关的属性—请参阅[永久性集合—将数据记录到数据库](#) (p. 389)
- 企业管理器度量标准限制属性—请参阅[企业管理器度量标准限制](#) (p. 393)
- 群集属性—请参阅[群集设置](#) (p. 402)

### introscope.enterprisemanager.hotconfig.enable

启用热配置服务。设置为 false 可禁用该服务。

#### 默认

true

### introscope.enterprisemanager.hotconfig.pollingInterval

指定检查文件更改的频率（以秒为单位）。

#### 默认

60 秒

## 应用程序启发

*IntroscopeEnterpriseManager.properties* 的 Application Heuristics 节中包含以下属性：

### **introscope.enterprisemanager.application.overview.baselines**

为改进企业管理器性能，您可以通过将此属性设置为 **false** 来关闭启发。

如果您执行了该操作，则企业管理器会关闭对 JVM、应用程序和后端运行状况的企业管理器评估。它还将关闭基准程序，这意味着工作站中的度量标准将处于非活动状态并且不报告任何值。度量标准将灰显，除非将配置设置回 **true**，设置回 **true** 后它们将重新成为活动的。

#### **默认**

True

## 日志记录

日志记录属性定义企业管理器日志中的详细信息级别和企业管理器日志文件的名称和位置。有关高级 Log4J 函数的信息，请参阅 <http://jakarta.apache.org/log4j/docs/documentation.html> 中的 Log4J 文档。

这些企业管理器属性使用 Introscope 热配置服务。更改这些热配置属性之后，不必重新启动企业管理器。有关更多信息，请参阅[热配置服务](#) (p. 387)。

### **log4j.logger.Manager**

控制日志消息的详细信息级别和目的地。

详细信息级别值可以是：**INFO** 或 **VERBOSE#com.wily.util.feedback.Log4JSeverityLevel**。

目的地值可以是 **console** 或 **logfile**。默认设置将日志信息写入控制台和日志文件。

#### **默认**

INFO、console、logfile

### log4j.appender.logfile.File

企业管理器日志文件的名称和位置，相对于企业管理器主目录。

#### 默认

logs/IntroscopeEnterpriseManager.log

### log4j.appender.logfile.layout.ConversionPattern

允许您自定义日志文件。

此属性可以设置以下值：

```
d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n
```

此模式是在 log4j 库中实施的，格式在以下网页中进行了介绍：

<http://logging.apache.org/log4j/docs/api/org/apache/log4j/PatternLayout.html>

日期/时间格式出现在 `%d{.}` 中并遵循以下网页中描述的模式：

<http://java.sun.com/j2se/1.4.2/docs/api/java/text/SimpleDateFormat.html>

#### 默认

<blank>

## 永久性集合—将数据记录到数据库

您可以配置本节中描述的属性，以将跟踪数据记录到外部的关系型数据库中。有关更多信息，请参阅 *IntroscopeEnterpriseManager.properties* 文件的 **SQL Database Settings** 节。这些设置都是通过热配置部署的，因此它们不要求手工重新启动企业管理器。

Introscope 包括的一个 API 使您能够为历史范围提取度量标准和事件数据，然后使用数据分析工具（如 Excel 或 SAS）来查看 Introscope 数据。CA Technologies 建议您使用此 API 记录数据—请参阅 [JDBC API](#) (p. 489)。您还可以使用命令行 Workstation 命令来提取永久性数据—请参阅“使用命令行 Workstation (see page 129)”。

这些企业管理器属性使用 Introscope 热配置服务。更改这些所谓的“热配置”属性之后，不必重新启动企业管理器。有关更多信息，请参阅 [热配置服务](#) (p. 387)。

### **introscope.enterprisemanager.database.collection.agentExpression**

这是代理正则表达式属性。可将此设置添加到 *IntroscopeEnterpriseManager.properties* 文件中并通过热配置进行部署。

例如：

```
Introscope.enterprisemanager.database.collection.agentExpression=rhart-dt  
1 \\/EPAgentProcess1 \\/EPAgent5
```

**默认**

<blank>

### **introscope.enterprisemanager.database.collection.metricExpression**

此为度量标准正则表达式属性。可将此设置添加到 *IntroscopeEnterpriseManager.properties* 文件中并通过热配置进行部署。

**示例**

```
introscope.enterprisemanager.database.collection.metricExpression=Servlets  
 \\/MyServlet:Average Response Time \\/(ms\\)
```

**默认**

<blank>

### **introscope.enterprisemanager.database.collection.frequencyinseconds**

其中，*agentExpression* 是代理正则表达式，*metricExpression* 是度量标准正则表达式，*frequencyinseconds* 是聚合数据并将其写入数据库的频率（以秒为单位）。可将此设置添加到 *IntroscopeEnterpriseManager.properties* 文件中并通过热配置进行部署。

没有默认设置，因为每个永久性集合可以有不同的值。应当为每个永久性集合设置此属性。

**默认**

无

### introscope.enterprisemanager.database.recordingQueue.upperLimit.value

队列中度量标准数据点的最大数量。度量标准数据点是一个度量标准在一个时间片的数据。此设置是通过热配置部署的。

默认

150k（千）

## 平面文件属性

平面文件是纯文本的逗号分隔值 (.csv) 文件。Introscope 可以向平面文件进行写入，但无法从其中读取。您可以使用数值分析工具来分析平面文件。

平面文件记录在默认情况下启用并且定向到 `<EM_Home>/flatfiles` 目录。您还可以指定将这些文件保存在 Introscope 目录外的某个目录中。请注意，对于 Windows 路径，您必须使用反斜线 (\) 对反斜线进行转义（使用两个反斜线），例如：`C:\\Introscope\\FlatFileDir`。

## 事务事件数据库

企业管理器将所捕获的事务事件在其本地文件系统上存储一段固定的时间，或者一直存储到超出最大的磁盘使用量。您可以通过设置事务事件数据库属性来控制将这些活动存储在何处以及应在何时删除这些事件。

### introscope.enterprisemanager.transactionevents.storage.dir

指定 Introscope 存储事务事件数据的位置，相对于企业管理器主目录。

默认

traces

### introscope.enterprisemanager.transactionevents.storage.max.data.age

指定将事务事件数据存储多长时间（以天为单位）。

默认

14

### **introscope.enterprisemanager.transactionevents.storage.optimize.frequency**

指定清除老化数据以优化跟踪存储的频率（以小时为单位）。

在企业管理器启动时启用事务跟踪数据的老化。

#### **默认**

24 小时

### **introscope.enterprisemanager.transactionevents.storage.optimize.timeoffsethour**

为存储优化指定时间偏移量，这允许您根据时间偏移量将清除排定为在每天的特定时间启动。

例如，如果时间偏移量设为 02 且优化频率（请参阅 [introscope.enterprisemanager.transactionevents.storage.optimize.frequency](#) (p. 392)）设置为 24 小时，则优化过程将从凌晨 02:00 开始每 24 小时运行一次。

为该属性输入一个 00 值后，将显示错误消息，因为该值必须是正整数。

#### **默认**

02 (2AM)

## **事务跟踪采样**

这些事务跟踪采样属性默认情况下位于 *IntroscopeEnterpriseManager.properties* 中。

### **introscope.agent.transactiontracer.sampling.perinterval.count**

默认情况下针对 1 个样本跟踪的情况而配置。此属性与 `introscope.agent.transactiontracer.sampling.interval.seconds` 属性一同使用。

通过在属性文件中修改此属性的值并取消注册此属性，您可以更改每个间隔要跟踪的跟踪数量。

#### **默认**

1



### introscope.agent.transactiontracer.sampling.interval.seconds

默认情况下配置为每 2 分钟跟踪一次。此属性与 introscope.agent.transactiontracer.sampling.perinterval.count 属性结合使用。

通过在属性文件中修改此属性的值并取消注释此属性，您可以更改采样时间间隔。

#### 注释

在覆盖 sampling.perinterval 和 sampling.interval 属性的默认值前，请考虑采用较高的采样率可能会增加企业管理器的负载这一情况。

#### 默认

120 秒

## 企业管理器度量标准限制

这些属性定义您从独立的企业管理器或收集器为度量标准获取的结果数的限制集。它们是可热配置的，这意味着企业管理器在热部署期间检查属性文件时会应用这些值。热部署大约每隔 60 秒发生一次。

#### 禁用限定：

1. 打开 IntroscopeEnterpriseManager.properties 文件进行编辑，并导航到 EM Metric Clamping 节。
2. 要禁用限定，请将限定的值设置为 0。
3. 保存并关闭 IntroscopeEnterpriseManager.properties。

其他企业管理器限定在 <EM\_Home>/config 目录下的 [apm-events-thresholds-config.xml](#) (p. 427) 文件中。

### introscope.enterprisemanager.query.datapointlimit

该属性定义在以下任何单一查询类型的内部处理完成之后，企业管理器发送回发出查询的软件的度量标准数据点的最大数目：

- JDBC
- CLW
- 前 N 个（CLW 和 Workstation）。

发出查询的软件可以是 Workstation、扩展或内部计算器。内部处理可以是前 N 个查询或其他筛选。

该限定的作用是减少群集收集器或独立企业管理器从 SmartStor 检索的度量标准的数目。不过，企业管理器始终会为至少一个度量标准返回完整数据。此限定针对每个 JDBC、CLW 或前 N 个查询，不是针对多个并发的查询。

该属性与 [introscope.enterprisemanager.query.returneddatapointlimit](#) (p. 395) 属性一起使用。

`introscope.enterprisemanager.query.datapointlimit` 属性和 `introscope.enterprisemanager.query.returneddatapointlimit` 属性之间的差异是限定生效的位置。`introscope.enterprisemanager.query.datapointlimit` 属性限定将查询发送回发出查询的软件时的度量标准数据点。`introscope.enterprisemanager.query.datapointlimit` 属性限定 SmartStor 磁盘读取数。

### 示例

#### 示例 1

`introscope.enterprisemanager.query.datapointlimit` 属性设置为 10，`introscope.enterprisemanager.query.returneddatapointlimit` 属性设置为 0（无限制）。

CA APM 用户进行匹配 10,000 个数据点的前 100 查询。企业管理器预期只将前 100 个数据点发送回 Workstation。企业管理器从 SmartStor 读取并处理 10,000 个数据点。但是，由于 `introscope.enterprisemanager.query.datapointlimit` 属性设置为 10，因此企业管理器只将前 10 个数据点发送回 Workstation。

#### 示例 2

`introscope.enterprisemanager.query.datapointlimit` 设置为 0（无限制），`introscope.enterprisemanager.query.returneddatapointlimit` 属性设置为 1000。

CA APM 用户进行匹配 10,000 个数据点的前 100 查询。企业管理器预期只将前 100 个数据点发送回 Workstation。企业管理器从 SmartStor 读取并处理 1,000 个数据点。由于 `introscope.enterprisemanager.query.returneddatapointlimit` 属性设置为 1000，因此企业管理器可自由地将前 100 个数据点发送到 Workstation。

### 注释

您无法设置此属性来限制对 MOM 或 CDV 的查询。

### 默认

0（其中 0 意味着无限制。）

## **introscope.enterprisemanager.query.returneddatapointlimit**

该属性限制 SmartStor 为任何单一 JDBC、CLW 或前 N 个（CLW 和 Workstation）查询返回的数据点的数目。此限制的作用是减少为其将数据返回到群集收集器或独立企业管理器的度量标准数。此限定针对每个 JDBC、CLW 或前 N 个查询，不是针对多个并发的查询。

该属性与 [introscope.enterprisemanager.query.datapointlimit](#) (p. 393) 属性配合使用。

### 示例

**注意：**有关示例，请参阅

[introscope.enterprisemanager.query.datapointlimit](#) (p. 393) 属性。

### 注释

您无法设置此属性来限制对 MOM 或 CDV 的查询。

### 默认

0（其中 0 意味着无限制。）

## **SmartStor**

本节中的属性用于定义 SmartStor 数据的存储目录，并为三层存储配置数据收集和老化行为。如有需要，您还可以禁用 SmartStor。

**注意：**必须定义所有三个层。您不能定义三个以上的层。

### **introscope.enterprisemanager.smartstor.enable**

允许您启用或禁用 SmartStor。虽然禁用 SmartStor 可以节省磁盘空间，但它不会存储统计信息，并且会阻止您监控统计信息。

设置为 False 可禁用 SmartStor。

#### **注释**

如果您在 SmartStor 节中未看到此属性，表明 SmartStor 处于启用状态。要禁用 SmartStor，请将以下行添加到属性文件中：

```
introscope.enterprisemanager.smartstor.enable=false
```

#### **默认**

True

### **introscope.enterprisemanager.smartstor.directory**

指定 SmartStor 将使用的、相对于企业管理器主目录的目录。

#### **默认**

data

### **introscope.enterprisemanager.smartstor.directory.archive**

指定 SmartStor 将用来存储存档数据的目录。

#### **默认**

data/archive。

### **introscope.enterprisemanager.smartstor.dedicatedcontroller**

指定 SmartStor 数据是否写入专用磁盘。

如果将 SmartStor 数据写入专用磁盘中，则设置为 true。

有关使用此属性的详细信息，请参阅《CA APM 规模调整 and 性能指南》。

#### **默认**

false

### **introscope.enterprisemanager.smartstor.tier1.frequency**

指定第一个数据层的数据收集频率（以秒为单位）。频率：

- 必须是 15 秒的倍数。
- 不得大于 1800 秒（30 分钟）。
- 必须是前一层的频率的偶倍数—该倍数可以是一倍；每层可以具有相同的频率。

**默认**

15

### **introscope.enterprisemanager.smartstor.tier1.age**

指定在经过多少天后第一层中的数据从 SmartStor 中老化。该值不能为零。

**默认**

7

### **introscope.enterprisemanager.smartstor.tier2.frequency**

为第二个数据层指定数据集合的频率（以秒为单位）。频率：

- 必须是 15 秒的倍数。
- 不得大于 1800 秒（30 分钟）。
- 必须是前一层的频率的偶倍数—该倍数可以是一倍；每层可以具有相同的频率。

**默认**

60

### **introscope.enterprisemanager.smartstor.tier2.age**

指定相关天数，超过该天数后，第二层中的数据将在 SmartStor 中过期。该值不能为零。

**默认**

23

### introscope.enterprisemanager.smartstor.tier3.frequency

为第三个数据层指定数据集合的频率（以秒为单位）。频率：

- 必须是 15 秒的倍数。
- 不得大于 1800 秒（30 分钟）。
- 必须是前一层的频率的偶倍数—该倍数可以是一倍；每层可以具有相同的频率。

#### 默认

900

### introscope.enterprisemanager.smartstor.tier3.age

指定相关天数，超过该天数后，第三层中的数据将在 SmartStor 中过期。该值不能为零。

#### 默认

335

### introscope.enterprisemanager.memoryCache.elements

此属性控制企业管理器在内部压缩内存缓存中保存的数据点的数量，以提高历史数据查询的速度。

每个数据点各包含 15 秒钟度量标准数据。默认的 32 个数据点包含 8 分钟的历史度量标准数据。

范围是 32（8 分钟）到 11520（48 小时），并且必须可以被 32 除尽。

您可以针对 Workstation 使用率突增的分类情况，将缓存设置为多于 32 个数据点。例如，如果值为 240 个数据点，企业管理器就可以通过内存缓存提供过去一小时中每个历史查询。

#### 注释

此属性是不可热配置的。如果更改了该属性，请重新启动企业管理器，以使所做的更改生效。

此值不得少于 32 个数据点。如果您将它设置为少于 32，它将被设置成默认值。

如果值不能被 32 除尽，它会减少为可被 32 除尽的最接近数目。

**重要信息！** 增加缓存中的数据点的数目需要 RAM。不要设置比默认值高的值，除非您使用的是 64 位计算机，它具有数千兆字节额外的堆内存。有关堆调整的详细信息，请参阅《CA APM 规模调整 and 性能指南》。

使用以下计算方法来计算缓存需要的堆内存。假定每个缓存数据点平均为 32 字节。

数据点数 \* 32 字节 \* 度量标准数 = 必要的缓存堆内存

### 示例

您希望增加缓存，以保存大约一小时数据量，将值设置为 256 个数据点。使用下列方程式来计算所需堆内存：

256 个数据点 \* 32 字节 \* 50 万个度量标准 = 4.1 GB 缓存堆内存

检查企业管理器堆大小，根据缓存堆内存要求确认是否需要调整。

### 默认

32 个数据点

## introscope.enterprisemanager.smartstor.reperiodizationOffsetHour

此属性允许您为数据分层配置时间偏移。

### 约束

必须是介于 0 到 23 之间的整数，表示当天的小时数，其中 0 表示午夜，13 表示下午 1:00。

### 默认

0（0 意味着数据分层在午夜开始）。

### 示例

如果您将此属性设置为 2，则数据分层从凌晨 2 点开始。

## introscope.enterprisemanager.smartstor.conversionOffsetMinute

此属性允许您为转换为数据的后台打印配置时间偏移。

### 约束

必须是介于 0 到 59 之间的整数，表示小时数后面的分钟数。

### 默认

0（例如，将值设置为 xx:00 意味着转换在整点开始）。

### 示例

如果您将值设置为 10 (xx:10)，则缓冲池转换在整点后的第 10 分钟开始。

## 基准数据存储

*IntroscopeEnterpriseManager.properties* 的 EM Object Database Settings 节中包含以下属性：

### introscope.enterprisemanager.dbfile

指定 Introscope 将度量标准基准信息存储在其中的数据库的文件名和位置，相对于企业管理器主目录。

### 默认

data/baselines.db

## SNMP 收集

*IntroscopeEnterpriseManager.properties* 的 SNMP Adapter 节中包含以下属性：

### introscope.enterprisemanager.snmp.enable

启用 SNMP 代理（仅适用于安装有 SNMPServices.jar 的情况）

### 默认

false

### introscope.enterprisemanager.snmp.agent.port

与 SNMP 代理进行通信的企业管理器端口

### 默认

161



## WebView

*IntroscopeEnterpriseManager.properties* 的 WebView Configuration 节中包含以下属性:

### **introscope.enterprisemanager.webview.disableLogin**

决定 WebView 是否可以建立与企业管理器的连接。

**默认**

false

### **introscope.enterprisemanager.webview.password**

指定 WebView 用户来连接到企业管理器的密码。

**默认**

WebView

## CA APM ChangeDetector

*IntroscopeEnterpriseManager.properties* 的 CA APM ChangeDetector 部分包含以下属性:

### **introscope.changeDetector.disable**

该属性允许您启用或禁用 CA APM ChangeDetector。

**默认**

true

## 管理模块引导

*IntroscopeEnterpriseManager.properties* 的 Management Module Bootstrapping 节中包含以下属性:

### **introscope.enterprisemanager.managementModules.invalid.references.as.errors**

将无效引用记录为警告。如果设置为 **true**，无效引用将阻止启动企业管理器。

**默认**

false

## **管理模块部署**

*IntroscopeEnterpriseManager.properties* 的 Management Module Deployment 节中包含以下属性：

### **introscope.enterprisemanager.hotdeploy.directory**

定义要从其中检查要部署的已更新应用程序的目录，相对于企业管理器主目录。

**默认**

deploy

### **introscope.enterprisemanager.hotdeploy.checkFrequencyInSeconds**

指定检查要部署的已更新管理模块的频率（以秒为单位）。

**默认**

60

## **群集设置**

其中一些属性需要重新启动企业管理器才能使设置生效。有些属性使用 Introscope [热配置服务](#) (p. 387)。更改这些所谓的“热配置”属性之后，不必重新启动企业管理器。

### **introscope.enterprisemanager.clustering.manager.slowcollectorthreshold**

设置此属性可以为您的环境的 ping 度量标准定义阈值。ping 度量标准只监控从 MOM 到每个收集器的往返行程响应时间下限。

**默认**

10000（以毫秒为单位）

### **introscope.enterprisemanager.clustering.manager.slowcollectordisconnectthresholdseconds**

设置此属性可以定义一个时间阈值，超出该阈值后，MOM 将自动断开与收集器的连接。这将防止整个群集挂起，整个群集挂起是群集中的一个收集器性能极其低下时的副作用。

如果此属性设置为零或负值（建议不要采用该设置），将不会启用此属性。

#### **注释**

MOM 每 7.5 秒检查一次收集器，因此小更改不会影响其行为。

#### **默认**

60（以秒为单位）

### **introscope.enterprisemanager.clustering.mode**

该属性指定 CA APM 环境中的企业管理器角色。

#### **选项**

CDV—企业管理器作为跨群集数据查看器运行

收集器—企业管理器作为收集器运行

MOM—企业管理器作为管理器运行

独立—企业管理器作为独立企业管理器运行

#### **注意**

重新启动企业管理器使该属性设置生效。

如果企业管理器配置成 CDV，之后更改为以上任何角色，则计算机需要 APM 数据库：

- MOM
- 收集器
- 独立企业管理器

#### **默认值**

StandAlone

#### **示例**

```
introscope.enterprisemanager.clustering.mode=StandAlone
```

### **introscope.enterprisemanager.clustering.login.<emName>.host**

收集器企业管理器的主机名或 IP 地址。

**默认**

<blank>

### **introscope.enterprisemanager.clustering.login.<emName>.port**

收集器企业管理器的 [introscope.enterprisemanager.port.<ChannelName>](#) (p. 382) 属性的值。

**默认**

<blank>

### **introscope.enterprisemanager.clustering.login.<emName>.publickey**

指定用来对 MOM 用于连接到收集器企业管理器的密码进行加密的公钥。

**默认**

config/internal/server/EM.public、注释掉

### **introscope.enterprisemanager.clustering.privatekey**

指定收集器企业管理器用于解密 MOM 用来与其建立连接的密码的公钥。

**默认**

config/internal/server/EM.private

### **introscope.enterprisemanager.clustering.collector.identifier**

可选。如果您想为该收集器指定一个描述性的名称，则可以设置此属性。

如果您不指定标识符，则 Introscope 使用默认标识符 `host@port`，其中，`host` 是企业管理器的主机名，`port` 是企业管理器的连接端口。

**默认**

false

### **introscope.enterprisemanager.clustering.manager.staggeredstartdelay**

在 MOM 上设置此可选属性，可以更改 MOM 在尝试连接到群集收集器时各次尝试相隔的时长。如果未设置此属性，则连接尝试之间的默认时间是 0 秒，这意味着一旦收集器可用，MOM 就可识别每个收集器。

设置此属性有助于平抑 MOM 的启动开销。这给了 MOM 一段时间，让其在每个收集器正在联机时处理连接，然后再启动与另一正在等待的收集器的连接过程。

最小值为 0 秒。

#### **默认**

0（秒）。最小值为 0 秒。

### **introscope.enterprisemanager.loadbalancing.threshold**

设置此属性可以定义负载均衡器的不均衡容差。收集器中度量标准的数量与加权调整的群集平均值（即所有收集器的平均值）之间的差额必须至少达到该阈值，负载均衡器才会重新对群集进行平衡。

重新平衡的意思是，在各个收集器间重新分布各个代理来平衡加权调整的度量标准负载。

#### **默认**

20000（度量标准）

### **introscope.enterprisemanager.loadbalancing.interval**

设置此属性可以决定负载均衡器的重新平衡频率（以秒为单位）。最小值为 120 秒。

#### **默认**

600（10 分钟）

### introscope.enterprisemanager.clustering.login.em1.weight

设置此可选属性可以控制收集器的相对负载。

所有其他条件都相同时，收集器的权重除以群集的总权重得到的值就是分配给该收集器的度量标准负载的百分比。例如，如果某个收集器的权重是 50，并且所有收集器的权重总和是 250，则该收集器应得到群集的度量标准负载的 20% 份额。

使用此权重作为该企业管理器收集器的负载平衡权重，对群集的值进行分摊。

## 代理交互

有些代理交互属性要求企业管理器在配置之后重新启动。有些属性使用企业管理器热部署配置服务自动部署，热部署在属性说明中进行了介绍。

有些代理交互属性没有包括在企业管理器属性文件中。要更改其默认值，请将其添加到 *IntroscopeEnterpriseManager.properties* 文件并保存该文件。如果某个属性未进行热部署，请关闭企业管理器并重新启动以启用新值。

### introscope.apm.agentcontrol.agent.allowed

代理与 *loadbalancing.xml* 中的任何正则表达式均不匹配时，此设置可确定是否允许该代理连接到以下任意企业管理器：

- 特定的独立企业管理器。
- 收集器。

#### 默认

true

#### 示例

```
introscope.apm.agentcontrol.agent.allowed=true
```

#### 注释

此设置是使用热配置进行部署的。

如果该属性设置如下：

- 在 *IntroscopeEnterpriseManager.properties* 文件中缺失，则值为 true。
- 在 MOM 上设置为 true，则在群集中允许与 *loadbalancing.xml* 不匹配的所有代理。

- 设置为 false，则与 loadbalancing.xml 不匹配的所有代理都将配置为不允许，结果如下：
  - **适用于：9.1 以前的代理**—9.1 以前的代理未连接到任何企业管理器。
  - **适用于：9.1 代理**—9.1 代理被动地连接到企业管理器，且不发送任何度量标准数据。
  - 代理已添加到 APM 状态控制台“拒绝的代理”列表。

**适用于：9.1 以前的代理**—如果 9.1 以前的代理具备以下条件：

- 已连接到企业管理器。
- 基于此属性设置的更改被禁止。

则企业管理器会断开与代理的连接。企业管理器拒绝所有进一步的代理连接尝试，直到通过更改该属性或配置 loadbalancing.xml 而允许代理。代理基于

[introscope.enterprisemanager.agent.disallowed.connection.limit](#) (p. 409) 属性中配置的时间等待重新连接。

### introscope.apm.agentcontrol.agent.emlistlookup.enable

确定以下对象是否可以向每个代理发送允许该代理连接到的企业管理器列表：

- MOM。
- 收集器。
- 独立企业管理器。

如果在代理连接的情况下以下任何设备关闭，该列表会告诉代理接下来连接到哪个企业管理器：

- MOM。
- 独立企业管理器。
- 代理连接到的初始收集器。

#### 默认

true

#### 示例

introscope.apm.agentcontrol.agent.emlistlookup.enable=true

### 注释

此设置是使用热配置进行部署的。

如果代理重新启动，则会将其代理配置文件 `introscope.agent.enterprisemanager.connectionorder` 属性用于初始收集器连接信息。

### `introscope.apm.agentcontrol.agent.reconnect.wait`

此设置可提供代理尝试重新连接到独立企业管理器或收集器之前等待的基本持续时间（以秒为单位）。

### 默认

45（秒）

### 示例

```
introscope.apm.agentcontrol.agent.reconnect.wait=45
```

### 注释

此设置是使用热配置进行部署的。

最小值为 45。如果该值设置为小于 45，则值默认为 45。

为了避免同时出现许多代理连接，企业管理器将以下值集中的一个随机秒数与该属性值相加：-30、-15、0、15、30。企业管理器随机选择计算的值之一，并将该值提供给代理。代理在尝试重新连接之前等待给定的时间。

例如，如果值设置为 60，企业管理器会将 60 与 -30、-15、0、15 和 30 相加。企业管理器创建以下计算的值集：30、45、60、75 和 90。企业管理器随机选择 75，并将该值提供给代理。代理在尝试重新连接之前等待 75 秒。

### `introscope.enterprisemanager.agentconnection.metrics.enable`

控制企业管理器是否生成代理连接度量标准。您可以将此属性设置为 True 或 False。

此属性未包括在企业管理器属性文件中。要更改值，请将此属性添加到属性文件中，并重新启动企业管理器来启用此属性。

### 默认

True



### **introscope.enterprisemanager.agentconnection.metrics.agentTimeoutInMinutes**

指定在代理断开连接多少分钟后，企业管理器停止生成该代理的连接度量标准。

此属性未包括在企业管理器属性文件中。要更改值，请将此属性添加到属性文件中，并重新启动企业管理器来启用此属性。

#### **默认**

30（分钟）

### **introscope.enterprisemanager.agent.disallowed.connection.limit**

限制配置为禁止连接但可以被动地连接到企业管理器的代理的数目。被动连接的代理不发送任何度量标准数据。

此限定属性适用于 MOM、独立企业管理器和收集器。

达到该限定时，如果某个禁止的代理尝试连接，则企业管理器会拒绝新的连接。此外，企业管理器会记录该活动，并且代理将添加到 APM 状态控制台“拒绝的代理”列表。

#### **默认**

0（无限制）

#### **示例**

```
introscope.enterprisemanager.agent.disallowed.connection.limit=0
```

#### **注释**

此设置是使用热配置进行部署的。

此属性适用于 9.1 和更高版本的代理。

如果在 MOM 上设置该属性，MOM 值不会覆盖收集器值。

### **introscope.enterprisemanager.autoUnmountDelayInMinutes**

在代理断开连接后，为防止是暂时断开连接，企业管理器继续跟踪代理的分钟数。在此时间过后，企业管理器将释放代理跟踪资源。

#### **默认**

60（分钟）

## 企业管理器故障切换

这些属性允许您启用并应用故障切换设置，这些设置可以用于具有相同的安装目录的企业管理器。设置这些属性时，您可能需要考虑企业管理器故障切换规则。

### **introscope.enterprisemanager.failover.enable**

此属性启用故障切换。

**默认**

false

### **introscope.enterprisemanager.failover.primary**

此属性允许您设置主企业管理器的主机名或 IP 地址。要同时将两个企业管理器配置为主企业管理器，请将此属性设置为主企业管理器的主机名或 IP 地址的逗号分隔列表。下面是同时将两个企业管理器配置为主企业管理器的示例：*introscope.enterprisemanager.failover.primary=myhost1, myhost2*。

如果为单个主机而不是共享的文件系统配置企业管理器故障切换，则需要将主企业管理器设置为自身。此外，*introscope.enterprisemanager.failover.secondary* 属性必须为空。

**默认**

<blank>

### **introscope.enterprisemanager.failover.secondary**

此属性允许您通过指定企业管理器主机的主机名或 IP 地址，设置次企业管理器的主机名或 IP 地址。例如，*introscope.enterprisemanager.failover.secondary=myhost2*。

**默认**

<blank>

### introscope.enterprisemanager.failover.interval

此属性允许您设置正在运行的次企业管理器检查主企业管理器是否正在等待启动的频率（以秒为单位）。此设置是通过热配置部署的。

#### 默认

120（2 分钟）

## 配置目录

在 EM Config Directory 节中，此属性允许您指定企业管理器 *config* 目录的位置。

### introscope.enterprisemanager.directory.config

企业管理器用于配置的目录。在 Windows 中，必须对反斜线进行转义（使用两个反斜线）。例如：`C:\\Introscope\\config`

#### 默认

原始 Introscope 安装中的 config 目录。

## 应用程序分类地图数据

这些属性允许您启用并应用应用程序分类地图数据设置。有关配置说明，请参阅“[配置应用程序分类视图 \(p. 215\)](#)”。

与应用程序分类地图相关的其他属性是在 *APMEnterpriseManager.properties* 文件中配置的。请参阅 [APMEnterpriseManager.properties \(p. 423\)](#)。

### introscope.apm.data.agingTime

此属性由代理进行加载，控制代理将应用程序分类视图数据报告给企业管理器的频率。

#### 注释

此属性是不可热配置的。如果您更改了此属性，则需要重新启动代理和企业管理器才能使更改生效。

**警告！** 在更改此属性前，请从 APM 数据库中删除分类视图数据。当更改了此值且旧的分类视图数据与新的分类视图数据一起使用时，历史查询将显示涉及新值的不一致结果。有关从 APM 数据库中删除分类视图数据的信息，请参阅[应用程序分类视图数据清除](#) (p. 220)。

此值不得低于 1 分钟。如果您设置的值小于 1 分钟，则此属性默认为 1 天。

在决定此设置时，请考虑您的组织添加和修改应用程序的频率。如果您设置了较低的值，那么分类视图将实时地显示应用程序依赖关系，但这将使用代理和企业管理器开销。如果您设置了较高的值，则视图会显示较早的应用程序依赖关系，但这样会使用较少的代理，并且会降低企业管理器的开销。

有关代理和企业管理器开销的信息，请参阅《CA APM 规模调整 and 性能指南》。

使用下面的任意时间单位，不区分大小写。如下所述：

- 对于天数，使用：days、D
- 对于分钟数，使用：mins、M
- 对于小时数，使用：hours、H

此 `agingTime` 属性与 `introscope.apm.data.timeWindow` 属性一同使用，这样，`agingTime` 通常是 `timeWindow` 的一个子集。

### 示例

如果 `introscope.apm.data.agingTime` 值为 3 天，`introscope.apm.data.timeWindow` 值为 10 天，则应用程序分类视图会显示在过去的 10 天内代理报告的应用程序依赖关系。如果在那 10 天内没有报告关于依赖关系的数据，则在 `agingTime` 时段（即 3 天）过期后，依赖关系将显示为老化状态，并仍作为已老化元素保留在分类视图上，直到 10 天的 `timeWindow` 结束。

### 默认

1 天

## introscope.apm.data.timeWindow

除 *introscope.apm.data.agingTime* 属性中定义的时段外，此属性也定义一个时段。

### 注释

此属性是不可热配置的。如果您更改了此属性，请重新启动企业管理器，以使所做的更改生效。

此值不得低于 1 分钟。如果您设置的值小于 1 分钟，则此属性默认为 1 天。

使用下面的任意时间单位，不区分大小写。如下所述：

- 对于天数，使用：days、D
- 对于分钟数，使用：mins、M
- 对于小时数，使用：hours、H
- 对于秒数，使用：secs、S
- 对于毫秒数，使用：MS

此属性与 *introscope.apm.data.timeWindow* 属性结合使用，因此，*agingTime* 通常是 *timeWindow* 的子集。

### 示例

如果 *introscope.apm.data.agingTime* 值为 3 天，*introscope.apm.data.timeWindow* 值为 10 天，则应用程序分类视图会显示在过去的 10 天内代理报告的应用程序依赖关系。如果在那 10 天内没有报告关于依赖关系的数据，则在 *agingTime* 时段（即 3 天）过期后，依赖关系将显示为老化状态，并仍作为已老化元素保留在分类视图上，直到 10 天的 *timeWindow* 结束。

在决定此设置时，请考虑您的组织添加和修改应用程序的频率。如果您设置了较低的值，那么分类视图将实时地显示应用程序依赖关系，但这将使用代理和企业管理器开销。如果您设置了较高的值，则视图会显示较早的应用程序依赖关系，但这样会使用较少的代理，并且会降低企业管理器的开销。

有关代理和企业管理器开销的信息，请参阅《CA APM 规模调整 and 性能指南》。

### 默认

3 天

### introscope.apm.pruning.enabled

此属性启用从 APM 数据库中清理应用程序分类视图数据的功能。

#### 注释

- 此属性是不可热配置的。如果您更改了此属性，请重新启动企业管理器，以使所做的更改生效。
- 此属性设置为 `true` 时，会从 APM 数据库中清理应用程序分类视图数据。
- 此属性设置为 `false` 时，不会从 APM 数据库中清理应用程序分类视图数据，并且将无期限地存储该数据。

#### 默认

默认情况下，可以在独立企业管理器和 MOM 的群集环境的 APM 数据库中完成应用程序分类视图数据清除操作。

**重要信息！** 无法为应用程序分类数据清除操作配置收集器。如果将收集器的 `introscope.apm.pruning.enabled` 属性设置为 `true`，则会返回错误。

### introscope.apm.data.preserving.time

此属性控制应用程序分类地图数据在 APM 数据库中的存储时间。比保留时间值久的分类视图数据将被视为已老化，可以进行清理。

#### 注释

此属性是不可热配置的。如果您更改了此属性，请重新启动企业管理器，以使所做的更改生效。

清理过程中，将删除早于 `introscope.apm.data.preserving.time` 值和 `Introscope.apm.data.agingTime` 值之和的应用程序分类地图数据。

例如，如果 `introscope.apm.data.preserving.time` 值为 30 天，`introscope.apm.data.agingTime` 值为 1 天，则会删除  $30 + 1 = 31$  天前的视图数据。

**警告！** 如果所设置的保留时间值太低（数秒或数毫秒），则应用程序分类地图数据可能刚从企业管理器到达后就被从 APM 数据库中删除。

使用下面的任意时间单位，不区分大小写。如下所述：

- 对于天数，使用：days、D
- 对于分钟数，使用：mins、M
- 对于小时数，使用：hours、H
- 对于秒数，使用：secs、S
- 对于毫秒数，使用：MS

### 默认

365 天

## introscope.apm.pruning.cron.trigger.expression

此属性排定从 APM 数据库清理已老化的应用程序分类视图数据的频率。

### 注释

此属性是不可热配置的。如果您更改了此属性，请重新启动企业管理器，以使所做的更改生效。

*introscope.apm.pruning.cron.trigger.expression* 属性的格式为 Open Symphony Quartz CronTrigger 排定程序表达式。有关 Quartz CronTrigger 的信息，请访问 [www.quartz-scheduler.org](http://www.quartz-scheduler.org) ([www.quartz-scheduler.org](http://www.quartz-scheduler.org))。

该表达式是以空格分隔的 6 字段或 7 字段的字符串。字符串中的字段从左到右依次是：

秒、分钟、小时、日、月、星期、年

字段可以包含：

- 任何允许的值
- 该字段允许的特殊字符的各种组合。

有关允许的值、特殊字符以及示例表达式，请参阅 [www.quartz-scheduler.org](http://www.quartz-scheduler.org) ([www.quartz-scheduler.org](http://www.quartz-scheduler.org))。

### 默认

006 \* \* ? — 此默认表达式指定在每天早上 6 点清理分类视图数据。

## 位置视图数据

通过这些属性，您可以配置位置视图上的设置。

### `introscope.workstation.locationmap.clamp`

该属性用于控制位置映射可以包含的最大元素数。限定的作用是控制位置映射的大小。

#### 注释

当返回的元素数超出限定值时，则不会显示某些映射元素。用户将看到一条错误消息，指出一些元素未显示。

#### 默认

500

## Web Services

定期访问 Web 服务 API 的用户可能会注意到，大量调用 Web 服务会导致性能降低。默认情况下，用于 Web 服务的线程数设置为 10。可以通过在 `IntroscopeEnterpriseManager.properties` 文件中添加属性来更改该设置。

### `introscope.apm.model.webservices.threadpool.numberofthreads`

此属性指定线程池中使用的线程数。此属性的使用是可选的。

**警告！** 将此属性设置为较大的数可能会导致性能降低。设置该属性时请谨慎。

#### 约束

必须为整数。

#### 默认值

10

#### 示例

```
introscope.apm.model.webservices.threadpool.numberofthreads=15
```

《CA APM Catalyst 连接器指南》中也对此属性进行了介绍。

## 传出消息队列

通过这些属性，您可以配置传出消息队列设置。



## transport.outgoingMessageQueueSize

此属性指定传出消息队列中的消息数。

注意

增加传出消息队列的长度需要使用更多 RAM。

约束

必须为整数。

默认值

3000

示例

```
transport.outgoingMessageQueueSize=3000
```

《CA APM 规模调整 and 性能指南》中也对此属性进行了介绍。

## transport.override.isengard.high.concurrency.pool.max.size

此属性为同步输出套接字连接指定最大线程数。大量线程不会直接缩短响应时间，但却可以防止隔离的慢速连接大幅度降低企业管理器的速度。

默认情况下，对于大多数独立的企业管理器 and 收集器，5 个线程比较适合。MOM 的每个收集器应具有一个线程，大约每 10 个 Workstation 应具有一个线程。

由于它们的角色是网络通信路由器，因此如果 MOM 具有较多传出线程时，会尤其有利。因为这不仅使 MOM 可以同时为多个 Workstation 提供服务，还可以在单个收集器超载时有助于防止整个群集冻结。

**重要信息!** 请不要超过规定大小，因为线程超载可能会导致 OutOfMemory 异常（尤其是在 32 位 JVM 上）。

约束

必须为整数。

默认值

5

示例

```
transport.override.isengard.high.concurrency.pool.max.size=5
```

《CA APM 规模调整 and 性能指南》中也对此属性进行了介绍。

## 线程转储

通过这些属性，您可以配置线程转储。

有关启用和配置线程转储的信息，请参阅《CA APM Java 代理实施指南》。

可以针对该功能配置这些属性：

[introscope.enterprisemanager.threaddump.enable](#) (p. 418)

[introscope.enterprisemanager.threaddump.storage.dir](#) (p. 419)

[introscope.enterprisemanager.threaddump.storage.clean.disk.freq.days](#) (p. 419)

[introscope.enterprisemanager.threaddump.storage.clean.disk.olderthan.days](#) (p. 419)

[introscope.enterprisemanager.threaddump.storage.max.disk.usage](#) (p. 420)

### **introscope.enterprisemanager.threaddump.enable**

该属性用于为连接到企业管理器的任何代理启用度量标准浏览器树代理节点上的“线程转储”选项卡。

#### 注释

该属性是可热配置的。如果您更改了该属性，无需重新启动企业管理器，更改即可生效。

该属性与 IntroscopeAgentProfile `introscope.agent.threaddump.enable` 属性一起使用。有关详细信息，请参阅《CA APM Java 代理实施指南》。

当该属性设置为 `true` 且 IntroscopeAgentProfile `introscope.agent.threaddump.enable` 属性设置为 `true` 时，用户可以看到“线程转储”选项卡。

当该属性设置为 `false` 时，用户看不到“线程转储”选项卡。

#### 默认

`true`

### **introscope.enterprisemanager.threaddump.storage.dir**

指定存储线程转储的目录（相对于企业管理器主目录）。

#### **注释**

此属性是不可热配置的。如果更改了该属性，请重新启动企业管理器，以使所做的更改生效。

<EM\_Home>/threaddumps 不是用户保存线程转储文本文件的目录。用户可以将线程转储文本文件保存到任意位置。

#### **默认**

threaddumps

### **introscope.enterprisemanager.threaddump.storage.clean.disk.freq.days**

CA Introscope 清除线程转储文件的频率（以天为单位）。

#### **注释**

该属性与 `introscope.enterprisemanager.threaddump.storage.clean.disk.olderthan.days` 属性一起使用。设置这两个属性，以便企业管理器知道存储和清除线程转储文件的时间长度。

此属性是不可热配置的。如果更改了该属性，请重新启动企业管理器，以使所做的更改生效。

#### **默认**

1（天）

### **introscope.enterprisemanager.threaddump.storage.clean.disk.olderthan.days**

CA Introscope 清除线程转储文件的期限（以天为单位）。

#### **注释**

该属性与 `introscope.enterprisemanager.threaddump.storage.clean.disk.freq.days` 属性一起使用。设置这两个属性，以便企业管理器知道存储和清除线程转储文件的时间长度。

此属性是不可热配置的。如果更改了该属性，请重新启动企业管理器，以使所做的更改生效。

### 默认

30 (天)

## introscope.enterprisemanager.threaddump.storage.max.disk.usage

可以存储在企业管理器中的线程转储数。

### 注释

此属性是不可热配置的。如果更改了该属性，请重新启动企业管理器，以使所做的更改生效。

### 约束

必须是不超过 8000 的整数

### 默认值

5000

## 用于 Web 服务性能处理的线程属性

定期访问 Web 服务 API 的用户可能会注意到，大量调用 Web 服务会导致性能降低。默认情况下，用于 Web 服务的线程数设置为 10。可以通过在 IntroscopeEnterpriseManager.properties 文件中添加属性来更改该设置。

### 属性名称

introscope.apm.model.webservices.threadpool.numberofthreads

### 说明

指定线程池中使用的线程数。此属性的使用是可选的。

### 约束

必须为整数。

### 默认值

10

### 示例

```
introscope.apm.model.webservices.threadpool.numberofthreads=15
```

**使用此属性:**

1. 打开 IntroscopeEnterpriseManager.properties 文件以进行编辑。
2. 添加 introscope.apm.model.webservices.threadpool.numberofthreads 属性并指定值。

**注意:** 将此属性设置为较大的数会导致性能降低。设置该属性时请谨慎。

3. 保存并关闭该属性文件。

**注意:** 编辑 IntroscopeEnterpriseManager.properties 文件后必须重新启动企业管理器，更改才生效。

## SNMP 分类视图报警操作

SNMP 分类视图报警操作插件作为企业管理器安装程序的一部分进行安装。设置这些配置以指定 SNMP 分类视图报警操作的属性。

**注意:** SNMP 分类视图报警操作插件的属性不同于现有 SNMP 报警操作适配器的属性。可以通过前缀 *introscope.apm.catalyst.triagemapalert.snmp* 区分新的 SNMP 分类视图报警。

### **introscope.apm.catalyst.triagemapalert.snmp.destination.host.ip**

使用 APM 连接器的 IP 地址设置该属性。

### **introscope.apm.catalyst.triagemapalert.snmp.destination.trap.port**

使用发送 SNMP 陷阱的 SNMP 端口设置该属性。

#### **默认**

162

#### **示例**

*introscope.apm.catalyst.triagemapalert.snmp.destination.trap.port=162*

### **introscope.apm.catalyst.triagemapalert.snmp.community**

使用 SNMP 团体字符串设置该属性。

**默认**

public

**示例**

*introscope.apm.catalyst.triagemapalert.snmp.community=public*

### **introscope.apm.catalyst.triagemapalert.snmp.trigger**

使用 SNMP 陷阱通知需要的触发器类型设置该属性。

**默认**

3

**选项**

**1**

出现问题的每个时期

**2**

重要级别增加时

**3**

只要重要级别更改

**4**

不管什么重要级别，仅报告最终状态

**示例**

*introscope.apm.catalyst.triagemapalert.snmp.trigger=3*

## 应用程序视图对象

设置该属性，以指定将应用程序视图对象视为过时的限制。

默认

300 天

示例

```
introscope.apm.data.obsolete.time=300
```

## APMEnterpriseManager.properties

在 *APMEnterpriseManager.properties* 文件中定义的属性控制企业管理器的各种行为。*APMEnterpriseManager.properties* 文件主要支持应用程序分类视图。（用于配置企业管理器行为的其他属性文件包括 [IntroscopeEnterpriseManager.properties](#) (p. 379) 和 [apm-events-thresholds-config.xml](#) (p. 427)。）

在配置许多企业管理器属性之后，必须重新启动企业管理器才能使更改生效。不过，有些企业管理器属性使用 Introscope [热配置服务](#) (p. 387)。这些属性称为 *热配置* 属性。配置热配置属性之后，不必重新启动企业管理器。

## c3p0 属性

c3p0 properties 节配置用于 APM 数据库连接池的属性。有关 c3p0 的完整文档，请参阅 <http://www.mchange.com/projects/c3p0/index.html>。

**重要信息！** 在更改 c3p0 属性值之前，强烈建议您查看《*CA APM 规模调整 and 性能指南*》中有关这些属性的说明。

### c3p0.dataSourceName

要连接的数据源的名称。将默认名称替换为您的 APM 数据库的名称。

默认

apmDataSource

### **c3p0.acquireIncrement**

决定当池中的连接已用完时，c3p0 一次尝试获取的连接数。

**默认**

3

### **c3p0.idleConnectionTestPeriod**

连接空闲时，c3p0 将对连接进行测试的时间段（秒数）。在该时间段末，C3p0 将测试池中在该时间间隔内空闲的所有连接。

**默认**

120

### **c3p0.maxIdleTime**

在将空闲从连接池中删除之前，允许其持续存在的时间（秒数）。将此属性设置为 0 意味着池中的连接从不超时。

**默认**

0

### **c3p0.initialPoolSize**

在启动时，池尝试获取的连接数。应当介于 minPoolSize 和 maxPoolSize 之间。

**默认**

2

### **c3p0.minPoolSize**

池在任何时间将要维护的最小连接数。

**默认**

2



### c3p0.maxPoolSize

池在任何时间将要维护的最大连接数。

**默认**

4

## 特定于 Hibernate 的属性

“特定于 Hibernate 的属性”一节用于配置开源 Hibernate API 的各个方面，该 API 启用了透明的永久性，因此简化了 APM 数据库的数据存储。有关 Hibernate 的更多信息，请参阅 <http://www.hibernate.org>。

### hibernate.jdbc.batch\_size

指定 JDBC 批处理大小。

**默认**

10

### hibernate.order\_inserts

启用批量插入。

这对于使 Hibernate 能够为每个实体进行批量插入至关重要。强烈告诫用户不要编辑此属性。

**默认**

true

### hibernate.order\_updates

启用批处理更新。对每个实体而言，启用睡眠模式来执行批处理更新非常重要。强烈告诫用户不要编辑此属性。

**默认**

true

## Hibernate 缓存设置

Hibernate cache settings 节用于配置 APM 数据库中的数据缓存属性。

### **hibernate.cache.provider\_class**

指定要使用的 Hibernate 缓存类型。

不要更改此属性。

**默认**

org.hibernate.cache.EhCacheProvider

### **hibernate.cache.use\_second\_level\_cache**

启用 Hibernate 二级缓存。

**默认**

true

### **hibernate.statement\_cache.size**

指定语句缓存大小。

**默认**

10

## **ApplicationTriageMap 设置**

本节允许您自定义应用程序分类视图的设置。

### **hibernate.cache.provider\_configuration\_file\_resource\_path**

指定 Hibernate ehCache 配置文件。

**默认**

apm-ehcache.xml

### **introscope.apm.query.max.results**

使用此属性作为一个阈值，用以限制代理返回给应用程序分类视图显示的数据量。该值大约等于前端或业务事务的依赖关系数量，乘以其中部署有前端或业务事务并且在所查询的时段内报告了数据的代理的数量。

**默认**

20000

## apm-events-thresholds-config.xml

在三个企业管理器属性文件之一中定义的属性控制大量企业管理器行为。本节介绍 *apm-events-thresholds-config.xml* 中的属性。（其他两个属性文件是 *IntroscopeEnterpriseMangager.properties* (p. 379) 和 *APMEnterpriseManager.properties* (p. 423)。）位于 `<EM_Home>/config` 目录中的 *apm-events-thresholds-config.xml* 文件包含 CA Introscope、CA CEM 限定和 CA APM 重要事件的属性。

- 在这些限定达到或超过配置的阈值时，企业管理器会通知 APM 状态控制台“限定”选项卡。
- 在“重要事件”达到或超过配置的阈值时，企业管理器会通知 APM 状态控制台“重要事件”表视图。

**重要信息！** 请仅配置 *阈值* 字段中的阈值。不要更改其他任何字段，如限定 ID、重要事件 ID 和说明，因为 CA Introscope 使用这些字段进行系统监控。

无需重新启动企业管理器或受监控应用程序，*apm-events-thresholds-config.xml* 配置更改即可生效。这些属性使用 Introscope [热配置](#) (p. 387) 服务。如果属性使用热配置，那么您不需要在做出配置更改之后重新启动企业管理器。

**重要信息！** 请在做出任何配置更改之前备份 *apm-events-thresholds-config.xml* 文件。如果配置导致 *apm-events-thresholds-config.xml* 文件出错，则企业管理器无法读取该文件，并会使默认限定阈值设置生效。例如，如果 *apm-events-thresholds-config.xml* 中缺少右括号，则企业管理器无法读取该文件。如果新配置或更新的文件不能正常起作用，请执行以下操作之一：

- 排除最后更新的文件的故障，最好使用 XML 编辑器。
- 恢复前一个可正常起作用的备份。

### Introscope 限定属性

这些属性为 Introscope 特定的限定属性定义限制集。当达到或超过这些属性阈值时，企业管理器会通知 APM 状态控制台。

这些属性是可热配置的，这意味着企业管理器在热部署期间检查属性文件时会应用这些值。热部署大约每隔 60 秒发生一次。

在 `<EM_Home>/config` 目录下的 [IntroscopeEnterpriseManager.properties](#) (p. 379) 文件中查找其他企业管理器限定。

## introscope.clw.max.users

该属性限制在任何给定时间允许连接到企业管理器的命令行 Workstation (CLW) 的数目。

如果 CLW 连接会导致企业管理器速度降低，请使用该限定。CLW 连接尝试提取过多度量标准时，会导致企业管理器超载。

### 注释

您可以为独立企业管理器、MOM 和 CDV 使用该限定。然而，通常无法与收集器建立 Workstation 连接。

用户运行 CLW 命令时，企业管理器会为每个查询都建立两个连接。一个连接确定企业管理器是否可用，而第二个连接用于查询。这意味着每个 CLW 命令会以 2 而不是 1 为单位增加 introscope.clw.max.users 计数。此外，某些 CLW 会建立两个以上的企业管理器连接。设置 introscope.clw.max.users 属性阈值时，请考虑这些因素。

### 默认

500

## introscope.enterprisemanager.agent.connection.limit

introscope.enterprisemanager.agent.connection.limit 属性限制可以连接到一个企业管理器的代理的数量。

此属性对独立的企业管理器和收集器均适用。

达到限定阈值并且新的代理尝试连接到企业管理器时，会发生以下操作：

- 企业管理器记录该限定激活。
- 企业管理器不接受新的连接。

### 注释

企业管理器在 [em-jetty-config.xml 文件](#) (p. 40) 中使用 maxThreads 属性来限制企业管理器可为其提供服务的 HTTPS 代理连接的数量。如果线程不充足，企业管理器将无法从中识别连接的代理或进程度量标准。

使用 HTTPS 时，企业管理器仅服务于在 maxThreads 属性中配置的数量代理。请确保 maxThreads 值大于或等于 introscope.enterprisemanager.agent.connection.limit 值。当代理配置为通过 HTTPS 进行连接时，如果没有足够的线程，某些 HTTPS 代理可能不会显示在客户端中或报告任何度量标准。

当 `maxThreads` 属性限制企业管理器服务的代理数时，企业管理器和代理日志将不包含有关非服务代理的错误、警告或消息。

默认情况下，内部安装中的代理不使用 HTTPS 进行连接。

#### 默认

400

#### 示例

```
introscope.enterprisemanager.agent.connection.limit=400
```

## introscope.enterprisemanager.agent.error.limit

`introscope.enterprisemanager.agent.error.limit` 属性限制错误快照数。属性定义企业管理器在每个时间间隔内可以为每个代理处理的错误快照数限制。

此属性对独立的企业经理器和收集器均适用。

如果代理报告的错误快照数超出指定的限制，企业管理器会删除其余的所有错误。

#### 默认

10

#### 示例

```
introscope.enterprisemanager.agent.error.limit=10
```

## introscope.enterprisemanager.agent.metrics.limit

使用超过时代理报告受限的值设置此属性。

例如，如果达到度量标准的默认数量 1200.000，则会发生以下情况：

- 代理仅报告 120,000 个度量标准。
- 代理不会将新度量标准发送到企业管理器。

配置不当的代理会连续地快速创建数千个度量标准，使企业管理器超载。

可使用此属性来防止度量标准超载。如果代理生成的度量标准数量多于指定数量，则企业管理器会将其丢弃。如果发生此情况，请修改代理配置以减少所报告的度量标准的数量。

**注意：**有关详细信息，请参阅《CA APM Java 代理实施指南》或《CA APM .NET 代理实施指南》。

### 默认

120000

### 注意

该限定属性与位于 `Introscope.Agent.profile` 文件中的 `introscope.agent.metricClamp` 属性一起使用。

如果 `introscope.enterprisemanager.agent.metrics.limit` 限定值在 `introscope.agent.metricClamp` 值之前触发，企业管理器会读取代理度量标准，但是不会在调查器度量标准浏览器树中报告它们。

如果 `introscope.agent.metricClamp` 限定值在 `introscope.enterprisemanager.agent.metrics.limit` 限定值之前触发，代理会停止将度量标准发送到企业管理器。

## introscope.enterprisemanager.agent.trace.limit

`introscope.enterprisemanager.agent.trace.limit` 属性限定事务跟踪。此属性定义每个时间间隔内企业管理器可以为每个代理处理的事务事件数目的限制。

此属性对独立的企业经理器和收集器均适用。

如果代理报告的事务跟踪的数量超过了指定限制，则企业管理器将删除剩余的所有跟踪。

### 默认

1000

### 示例

```
introscope.enterprisemanager.agent.trace.limit=1000
```

## introscope.cdv.max.users

该属性限制可以连接到单个收集器的跨群集数据查看器 (CDV) 的数目。跨群集数据查看器通常连接到两个或更多群集中的多个收集器。

CDV 连接会因提取度量标准而增加收集器性能负载。使用该限定可限制收集器可以接受的 CDV 连接数。

### 默认

5

## introscope.enterprisemanager.disconnected.historical.agent.limit

该属性限制已断开连接但仍然安装的历史代理的数目。该限定最大程度地减少企业管理器运行时内存的使用。

该限定同时限制以下两种历史代理：

- 企业管理器可以自动卸载。
- CA APM 用户必须手工卸载。

有关安装和卸载代理的信息，请参阅《CA APM Workstation 用户指南》。

在达到限定阈值时，企业管理器会尝试卸载可以自动卸载的最早断开连接的历史代理。如果没有企业管理器可以自动卸载的历史代理，这意味着所有断开连接的历史代理都是 CA APM 用户手工安装的。企业管理器从不尝试卸载 CA APM 用户手工安装的已断开连接的历史代理。

### 示例

`introscope.enterprisemanager.disconnected.historical.agent.limit=400`

限定阈值设置为 400。一个名为 Tomcat 的代理和 399 个名为“Other”的代理连接到企业管理器。400 个代理中，Tomcat 代理是最早一个可以自动卸载的代理。企业管理器断开与全部 400 个代理的连接。当代理重新连接时，企业管理器会评估已断开连接但仍然安装的代理计数是否低于 400 个代理的阈值。名为“Other”的所有 399 个代理重新连接，然后 Tomcat 代理尝试重新连接。企业管理器执行以下操作：

- 在 400 个已断开连接的代理中，确定 Tomcat 代理是最早一个可以自动卸载的代理。
- 卸载 Tomcat 代理。

在卸载 Tomcat 代理之后，已断开连接的代理数为 399，再次低于 400 个代理的限定阈值。

### 注释

在发生以下情况时，企业管理器会通知 APM 状态控制台：

- 由于限定，已断开连接的已安装代理被卸载。
- 手工安装代理失败。

当发生以下情况时，该限定不清理已断开连接的已安装代理：

- 企业管理器内存不足。
- 已断开连接的历史代理超时并且已自动卸载。

当发生以下情况时，已断开连接的历史代理保持已安装：

- 历史代理已断开连接并且可以自动卸载。
- 已断开连接的历史代理计数低于 `introscope.enterprisemanager.disconnected.historical.agent.limit` 值。

当发生以下情况时，企业管理器会安装已断开连接的历史代理：

- CA APM 用户尝试手工安装已断开连接的历史代理。
- 已断开连接的历史代理计数低于 `introscope.enterprisemanager.disconnected.historical.agent.limit` 值。

当发生以下情况时，企业管理器会搜索可以自动卸载的已断开连接的已安装代理：

- 可以自动卸载的历史代理已断开连接。
- CA APM 用户尝试手工安装历史代理。
- 已断开连接的历史代理计数等于 `introscope.enterprisemanager.disconnected.historical.agent.limit` 值。

如果企业管理器找到已断开连接的已安装代理，那么它会卸载最早的已断开连接的历史代理，并且使新断开连接的代理保持安装状态。如果没有企业管理器可以自动卸载的历史代理，那么企业管理器会立即卸载新断开连接的历史代理。如果 CA APM 用户随后尝试手工安装历史代理，那么：

- Workstation 显示错误消息，指示用户卸载部分历史代理以便留出空间安装新历史代理。
- 企业管理器将向 APM 状态控制台发送通知。

## 默认

400



## introscope.enterprisemanager.events.limit

`introscope.enterprisemanager.events.limit` 属性限制事务跟踪。此属性定义每个时间间隔内由企业管理器处理的事务事件的数量限制。

此属性应用于独立的企业管理器、收集器和 MOM。

此限制应用于所有代理生成的所有事务事件的总数。当达到此限制时，对于该时间间隔，代理报告的所有其余事务事件将被丢弃。

### 默认

1250

### 示例

```
introscope.enterprisemanager.events.limit=1250
```

## introscope.enterprisemanager.metrics.historical.limit

此属性限制企业管理器中的历史度量标准的数量。每 15 秒检查一次限制，因此在应用限制前企业管理器可以超过该值。如果企业管理器检测到它已超过此限制，企业管理器将停止所有代理，不再注册新度量标准。旧度量标准将继续报告。

### 默认

1200000

## introscope.enterprisemanager.metrics.live.limit

此属性限制当前从代理报告的实时度量标准。当企业管理器检测到度量标准数已超过限制时，企业管理器将使所有代理停止注册新的度量标准。每 15 秒检查一次限制，因此在应用限制前企业管理器可以超过该值。旧度量标准将继续报告。具有历史数据的度量标准将从不会受限制。

### 示例

如果在应用限制之前，代理已向企业管理器报告了 60k 度量标准，然后我们应用了 50k 的限制，则所有 60k 旧度量标准仍可以向企业管理器进行注册。但是，如果我们尚未为其收集历史数据的新度量标准尝试注册，则不会允许其进行注册。

### 默认

500000

## introscope.enterprisemanager.transactionevents.storage.max.disk.usage

确定事务跟踪存储所需的最大磁盘使用量（以 MB 为单位）。如果超出了该最大使用量，则将从最早的第一个开始删除每日历史跟踪存储，直至总的历史跟踪存储大小低于该属性值。即使超出了该属性值的大小，也可能无法删除所存储的跟踪，因为确定要删除的历史跟踪存储时，不会考虑跟踪索引的大小。

负值或零值指示应当删除所存储的全部历史跟踪值。

如果事务事件数据库大于该值，则会从最早的存储文件开始删除历史存储文件，直到总数据库大小小于该值。

即使历史数据没到达完全老化日期，也可能会删除该数据。不会删除当前的实时存储，即使其大小超出了最大数据库大小也是如此。

如果您判定事务事件数据库太大，可以在关闭企业管理器的情况下手工删除数据库文件。企业管理器重新启动时，事务跟踪存储系统会检测到文件已手工删除并相应地调整跟踪索引。

### 注释

如果您手工删除文件，请仅删除跟踪目录中具有以下格式的文件：*traces\_yyyyMMdd.db*，其中 *yyyyMMdd* 代表该文件中的跟踪的年、月、日。  
不要删除该目录或子目录中的任何其他文件。

### 默认

1024

## introscope.workstation.max.users

该属性限制在任何给定时间允许连接到企业管理器的 Workstation 的数目。

如果 Workstation 连接会导致企业管理器速度降低，请使用该限定。Workstation 连接尝试提取过多度量标准时，会导致企业管理器超载。

### 注意

您可以为独立企业管理器、MOM 和 CDV 使用该限定。然而，通常无法与收集器建立 Workstation 连接。

### 默认

40

## 客户体验限定属性

这些属性为 CA CEM 特定的限定属性定义限制集。当达到或超过这些属性阈值时，企业管理器会通知 APM 状态控制台。

这些属性是可热配置的，这意味着企业管理器在热部署期间检查属性文件时会应用这些值。热部署大约每隔 60 秒发生一次。

### **introscope.enterprisemanager.max.application.user.rows**

检索的最大应用程序用户数。

应用程序用户过多会对性能产生负面影响。

#### 选项

数值

#### 默认

1000

#### 示例

```
introscope.enterprisemanager.max.application.user.rows =1000
```

#### 注释

达到最大值时，CA CEM 控制台会限制在列出应用程序用户的网页上显示的内容。

## 限制自上次同步以来列出的更改的数量

在同步监控之前，您可以复查自上次同步以来所做的配置更改。此内容在[查看自上次同步以来的配置更改](#) (p. 274)中有介绍。

配置更改显示在“监视器”页面的“域配置更改历史”表中。

`introscope.enterprisemanager.max.number.domain.configuration.changes` 属性确定该表中的最大行数。

### **introscope.enterprisemanager.max.number.domain.configuration.changes**

设置在单击“查看自上次同步以来的更改”（在“设置” > “监视器”上）时显示在“域配置更改历史”表中的最大更改数。

如果值为 -1，则显示所有更改。

#### 选项

数值

**默认**

0（无限制）

**示例**

```
introscope.enterprisemanager.max.number.domain.configuration.changes=1000
```

**注释**

请参阅[同步监控器](#) (p. 273)。

**introscope.enterprisemanager.max.transaction.user.groups**

自动创建的用户组的最大数。

该属性与通过请求属性或 IP 子网自动创建的用户组一起使用。

用户组太多，即使组中没有任何用户，都可能对性能产生负面影响。

**选项**

数值

允许的最大值为 10,000。

**默认**

5000

**示例**

```
introscope.enterprisemanager.max.transaction.user.groups=5000
```

**注释**

当达到最大数时：

- 不再自动创建用户组。
- 用户将分配到“新用户”组中，而不是创建新组。
- “系统” > “事件” 列表显示警告消息。

请参阅[在 CA CEM 上管理用户和组](#) (p. 277)。

**introscope.enterprisemanager.transaction.discovery.max.nonidentifying.components**

为当前定义的事务保留的已发现非标识组件的最大数量。（这不包括任何原始非标识组件。）

**选项**

数值（正整数）

### 默认

50

### 示例

```
introscope.enterprisemanager.transaction.discovery.max.nonidentifying  
.component=60
```

### 注释

该限制对非标识组件更改频繁的事务非常重要，例如，如果组件是每日更改的 GIF 文件，便是如此。设置该限制可防止为某个事务保存过多数量的（可能过期的）非标识组件。

在每次新的非标识组件替换旧的非标识组件时，系统都会记录称为“已超过添加新组件的限制”的 CA CEM 事件。

有关自动发现非标识组件的一般信息，请参阅《CA APM 事务定义指南》。

## 设置重要事件阈值

这些属性定义通知 APM 状态控制台有关对于企业管理器运行状况监控非常重要的事件所用的限制。它们是可热配置的，这意味着企业管理器在热部署期间检查属性文件时会应用这些值。热部署大约每隔 60 秒发生一次。

### apm.events.thresholds.config.error

该属性监控 apm-events-thresholds-config.xml 文件的语法错误。企业管理器找到错误时，会采取以下操作：

- 通知 APM 状态控制台“重要事件”表视图。
- 将所有 apm-events-thresholds-config.xml 文件限定和重要事件属性值恢复为默认值。

该属性适用于群集中的所有收集器或独立企业管理器。

### 默认

不适用。该属性仅供参考，无法修改。

### introscope.enterprisemanager.cpu.usage

该属性定义企业管理器 CPU 使用率被认为是重要事件的限制（百分比 (%)）。在达到或超过该阈值时，企业管理器会通知 APM 状态控制台“重要事件”表视图。

该属性基于对“CPU 容量 (%)”度量标准的企业管理器监控。CPU 使用率大于 60% 表示存在企业管理器资源问题。有关 CPU 使用率和企业管理器性能的信息，请参阅《CA APM 规模调整 and 性能指南》。

该属性适用于群集中的所有收集器或独立企业管理器。

#### 默认

60

#### 示例

```
introscope.enterprisemanager.cpu.usage=60
```

### introscope.enterprisemanager.database.connectivity

该属性监控企业管理器与 APM 数据库之间的连接。当连接断开时，企业管理器会通知 APM 状态控制台“重要事件”表视图。

该属性适用于群集中的所有收集器或独立企业管理器。

#### 默认

不适用。该属性仅供参考，无法修改。

### introscope.enterprisemanager.harvest.cycle.diff

该属性定义收集器和 MOM 搜集周期不同步的限制（时间片数）。在达到或超过该阈值时，企业管理器会通知 APM 状态控制台“重要事件”表视图。

该属性基于收集器度量标准搜集周期与 MOM 度量标准搜集周期的比较。在每个 15 秒搜集周期期间，将发生以下操作：

- 收集器收集和聚合代理度量标准数据。

- 收集器将度量标准数据发送到 MOM。
- MOM 聚合来自收集器的数据。
- MOM 将数据报告给 Workstation。

搜集周期完成之前，收集器不会将数据发送到 MOM。如果收集器搜集周期在 MOM 搜集周期内未完成，则收集器和 MOM 上的数据聚合不同步。

如果收集器和 MOM 在比该属性值更长的连续 MOM 搜集周期内不同步，CA APM 将群集视为不正常。

#### 默认

4

#### 示例

```
introscope.enterprisemanager.harvest.cycle.diff=4
```

#### 注释

仅在 MOM 上配置该属性。

### **introscope.enterprisemanager.harvest.duration**

该属性定义企业管理器搜集持续时间被认为是重要事件的限制（毫秒 (ms)）。在达到或超过该阈值时，企业管理器会通知 APM 状态控制台“重要事件”表视图。

该属性基于对“搜集持续时间 (ms)”度量标准的企业管理器监控。搜集持续时间超过 3500 毫秒表示存在企业管理器资源问题。有关搜集持续时间和企业管理器性能的信息，请参阅《CA APM 规模调整 and 性能指南》。

该属性适用于群集中的所有收集器或独立企业管理器。

#### 默认

3500

#### 示例

```
introscope.enterprisemanager.harvest.duration=3500
```

### **introscope.enterprisemanager.smartstor.duration**

该属性定义企业管理器 Smartstor 持续时间被认为是重要事件的限制（以毫秒 (ms) 为单位）。在达到或超过该阈值时，企业管理器会通知 APM 状态控制台“重要事件”表视图。

该属性基于对“Smartstor 持续时间 (ms)”度量标准的企业管理器监控。Smartstor 持续时间超过 3500 毫秒表示存在企业管理器资源问题。有关 Smartstor 持续时间和企业管理器性能的信息，请参阅《CA APM 规模调整 and 性能指南》。

该属性适用于群集中的所有收集器或独立企业管理器。

### 默认

3500

### 示例

```
introscope.enterprisemanager.smarstor.duration=3500
```

## ResourceMetricMap.properties

各种代理中的资源度量标准类别在 Workstation 中报告。资源度量标准类别已预定义。无法添加或删除预定义的资源度量标准组时，您可以添加、更改或删除指定为每个资源度量标准组报告的数据的资源度量标准映射（如果您具有管理员权限）。

### 将资源度量标准映射到资源度量标准类别：

1. 确认已在代理上启用 JMX 报告。有关详细信息，请参阅《CA APM Java 代理实施指南》中的 *启用 JMX 报告*。
2. 通过将资源度量标准映射到资源度量标准类别，编辑 MOM 上位于 `<EM_Home>/Config` 目录中的 `ResourceMetricMap.properties` 文件。有关映射资源度量标准的详细信息，请参阅您的应用程序服务器文档。

- a. 使用 `<categoryName>.path<recordID>:<agentMetricPath>` 格式添加度量标准条目。例如：

```
threads.used.path.1=Tomcat|ThreadPool|getCurrentThreadsBusy.path.1=CPU:Processor Count
```

其中，`memory.utilization` 是度量标准的名称，`CPU:Processor Count` 是其默认度量标准路径。

- b. 使用数字添加增量记录 ID 度量标准。例如：

```
cpu.utilization.path.1=Non Existent metric  
cpu.utilization.path.2=CPU|Processor 0:Utilization % (aggregate)
```

可以使用同一个度量标准组中的多个路径配置名称相同但路径不同的度量标准。例如，这允许您从部署了前端的不同应用程序服务器获取相同的度量标准。

3. 重新启动 MOM 和收集器。

新映射的资源度量标准值在 Workstation 中报告。



## 为相同度量标准的多个实例配置的 ResourceMetricMap.properties 文件的示例

以下是 ResourceMetricMap.properties 文件的一部分，其中“Threads in Use”度量标准的多个实例已配置为指向群集中的三个收集器。

```
#CPU utilization

cpu.utilization.path.1=CPU:Utilization % (process)

#Time Spent in GC

memory.utilization.path.1=GC Monitor|Percentage of Time Spent in GC during last
15 minutes

#Threads in Use

threads.used.path.1=WebSpherePMI|threadPoolModule|webContainer:ActiveCount

threads.used.path.2=WebLogic|JMX Aggregate|Thread Pool:Waiting Request Count

threads.used.path.3=Tomcat|ThreadPool|default thread
pool:getCurrentThreadsBusy

#JDBC Connections in Use

connections.used.path.1=WebSpherePMI|connectionPoolModule:waitingThreadCount

connections.used.path.2=WebLogic|JMX Aggregate|JDBC Connection Pool:Waiting
Thread Count
```

您可以将资源度量标准映射到以下资源度量标准类别：

[CPU 使用率](#) (p. 441)

[在 GC 中耗费的时间](#) (p. 442)

[使用中的线程](#) (p. 442)

[使用中的 JDBC 连接](#) (p. 442)

## CPU 使用率

CPU 使用率可测量正使用的 CPU 量。

**映射示例：**

```
cpu.utilization.path.1=CPU:Utilization % (process)
cpu.utilization.path.2=Some other metrics path
```

## 在 GC 中耗费的时间

在 GC 中耗费的时间可测量垃圾回收器中耗费的时间，以帮助您了解工作量对于应用程序性能是否有重大影响。

**映射示例：**

`memory.utilization.path.1=memory utilization path`

## 使用中的线程

使用中的线程可测量使用中的线程数。

**映射示例：**

`threads.used.path.1=threads used path`

## 使用中的 JDBC 连接

使用中的 JDBC 连接可测量处于活动状态的 Java 数据库连接实例数。

**映射示例：**

`connections.used.path.1=connections used path`

## Catalyst.properties

通过 Catalyst 属性，您可以配置 CA APM，以加载 CA Catalyst 数据并筛选从 Catalyst 数据报告的报警。

**详细信息:**

[catalyst.host](#) (p. 443)  
[catalyst.protocol](#) (p. 443)  
[catalyst.port](#) (p. 444)  
[catalyst.login](#) (p. 444)  
[catalyst.password](#) (p. 444)  
[catalyst.rest.entrypoint](#) (p. 444)  
[catalyst.rest.alerts.pollingperiodsec](#) (p. 445)  
[catalyst.rest.virtualhosts.pollingperiodsec](#) (p. 445)  
[catalyst.product.url](#) (p. 445)  
[catalyst.alert.filter.total](#) (p. 446)  
[catalyst.alert.filter.time](#) (p. 446)  
[catalyst.alert.filter.products](#) (p. 446)  
[catalyst.alert.filter.types](#) (p. 447)  
[catalyst.alert.filter.severities](#) (p. 448)  
[catalyst.rest.maxFailures](#) (p. 448)  
[catalyst.rest.maxAlertsPerPage](#) (p. 449)  
[catalyst.rest.alerts.threads](#) (p. 449)  
[catalyst.rest.virtualhosts.threads](#) (p. 449)  
[catalyst.entity.cache.size](#) (p. 450)  
[catalyst.entity.cache.expirationsec](#) (p. 450)  
[catalyst.database.alerts.enabled](#) (p. 450)  
[catalyst.database.map.name](#) (p. 451)  
[配置 APM 以加载 Catalyst 数据](#) (p. 225)  
[配置 CA APM 以加载 CA Catalyst 数据](#) (p. 225)  
[配置 CatalystPolicy.xml 文件](#) (p. 226)

## catalyst.host

使用 CA Catalyst 闲置 API 主机名设置该必需属性。在取消注释此行后，将值添加到 CA Catalyst。

### 默认

默认情况下，禁用该属性。

## catalyst.protocol

使用 CA Catalyst Web 访问的协议设置该必需属性。

### 示例

```
catalyst.protocol = http
```

## **catalyst.port**

使用 CA Catalyst Web 访问的端口号设置该必需属性。

示例

```
catalyst.port = 7070
```

## **catalyst.login**

使用用于登录 CA Catalyst 的用户名设置该必需属性。

示例

```
catalyst.login =<输入 CA Catalyst 用户名>
```

## **catalyst.password**

使用用于登录 CA Catalyst 的密码设置该必需属性。

示例

```
catalyst.password =<输入 CA Catalyst 密码>
```

## **catalyst.rest.entrypoint**

使用 CA Catalyst 闲置 API 入口点的 URL 上下文设置该必需属性。

示例

```
catalyst.rest.entrypoint = /ssaweb/search
```

## catalyst.rest.alerts.pollingperiodsec

设置该可选属性可确定在 CA Catalyst 中检查新报警的频率。

默认

15（秒）

示例

```
catalyst.rest.alerts.pollingperiodsec = 15
```

## catalyst.rest.virtualhosts.pollingperiodsec

设置该可选属性可确定在 CA Catalyst 中检查虚拟主机更新的频率。

默认

60（秒）

示例

```
catalyst.rest.virtualhosts.pollingperiodsec = 60
```

## catalyst.product.url

使用参与产品的基本 URL 地址设置该属性。

示例

```
# Spectrum
# catalyst.product.url = CA:00005->http[s]://<host>[:CA
Portal]/spectrum/oneclick.jsp?explorer={Entity.MdrElementID}
# eHealth
# catalyst.product.url = CA:00002->http[s]://<host>[:CA
Portal]/{Alert.UrlParams}
# Insight
# catalyst.product.url = CA:00048->http[s]://<host>[:CA Portal]
# NetQoS
# catalyst.product.url = CA:00034->http[s]://<host>[:CA
Portal]/npc/Default.aspx?pg={Alert.UrlParams}
```

### **catalyst.alert.filter.total**

设置该可选属性可设置要加载到 Workstation 的最大 CA Catalyst 报警数。

默认

250

示例

*catalyst.alert.filter.total = 250*

### **catalyst.alert.filter.time**

设置该可选属性可设置 CA Catalyst 报警显示在 Workstation 中的时间长度。

默认

72（小时）

示例

*catalyst.alert.filter.time = 72*

### **catalyst.alert.filter.products**

设置该可选属性可排除指定产品的所有报警。

示例

*catalyst.alert.filter.products = CA:00030*

## **catalyst.alert.filter.types**

设置该可选属性可标识不显示在 Workstation 中的 CA Catalyst 报警类型。  
使用逗号分隔报警类型。

### **选项**

- 风险
- Risk-Capacity
- Risk-Change
- Risk-Fault
- Risk-Security
- Risk-Performance
- Risk-Root Cause
- Quality
- Compliance
- 成本

### **示例**

*catalyst.alert.filter.types = Risk-Security,Compliance,Cost*

## **catalyst.alert.filter.severities**

设置该可选属性可确定不应显示在 Workstation 中的 CA Catalyst 报警重要级别。在两个重要级别值之间使用连字符 (-) 来定义范围，使用重要级别值右侧或左侧的连字符或者使用逗号设置多个值来扩大范围。

### **默认**

未知

### **选项**

可以为该属性设置下列选项，并允许您使用扩大范围：

- 正常
- 参考性
- 未知
- 轻微
- 重大
- 紧急
- 致命

### **示例**

*catalyst.alert.filter.severities = -Unknown*

## **catalyst.rest.maxFailures**

设置该可选属性可指定在取消轮询之前允许出现的最大 CA Catalyst 错误数。

### **默认**

10

### **示例**

*catalyst.rest.maxFailures = 10*



## **catalyst.rest.maxAlertsPerPage**

设置该可选属性可指定要在单个 REST 查询中返回的最大 CA Catalyst 报警数。

**默认**

250

**示例**

*catalyst.rest.maxAlertsPerPage = 250*

## **catalyst.rest.alerts.threads**

设置该可选属性可指定要用于报警的最大线程数。

**默认**

2

**示例**

*catalyst.rest.alerts.threads = 2*

## **catalyst.rest.virtualhosts.threads**

设置该可选属性可指定要用于虚拟主机的最大线程数。

**默认**

1

**示例**

*catalyst.rest.virtualhosts.threads = 1*

### **catalyst.entity.cache.size**

设置该可选属性可指定要用于 CA Catalyst 的实体内存缓存的大小。

**默认**

3000（兆字节）

**示例**

*catalyst.entity.cache.size = 3000*

### **catalyst.entity.cache.expirationsec**

设置该可选属性可指定实体缓存的到期时间（秒）。

**默认**

36000（秒）

**示例**

*catalyst.entity.cache.expirationsec = 36000*

### **catalyst.database.alerts.enabled**

设置该属性可向 Workstation 发送 CA Catalyst 数据库报警。默认情况下，向 Workstation 发送 CA Catalyst 数据库报警。将该设置更改为 *false* 可停止发送 CA Catalyst 数据库报警。

**默认**

true

**默认**

*catalyst.database.alerts.enabled=true*

## catalyst.database.map.name

设置该可选属性，以指定将数据库连接字符串映射到 CA Catalyst 数据库参数的文件的位置。仅当开箱即用型映射不能正常工作时，才设置该属性。

### Microsoft SQL 数据库示例：

1. 打开位于 `<Agent_Home>/wily/core/config` 目录中的 `IntroscopeAgent.profile` 文件，并将以下属性设置为 true：  
`catalyst.database.map.name = CatalystDatabaseMap.txt`
2. 打开位于 `<EM_Home>/config` 目录中的 `CatalystDatabaseMap.txt` 文件并定义等式：
  - a. 等式的左边代表 JDBC URL 匹配的完全 Java 正则表达式。
  - b. 以下等式分隔符将等式的左边与右边分开：竖线 (|)、箭头 (=>)、等号 (=) 或双等号 (==)，这些也可用作记录分隔符。
  - c. 等式的右边列出数据库参数：服务器名称、数据库名称和数据库实例名称

例如：

```
^jdbc:sqlserver.+1433.* = deviaat011|apmtest|default
^jdbc:sqlserver.+1533.* = deviaat011|apmtest|testinstance
```

## EMservice.conf

`EMService.conf` 文件（位于 `<EM_Home>\bin` 中）包含企业管理器作为 Windows 服务运行时使用的设置。

**注意：**在配置这些属性前，您必须取消注册企业管理器服务。配置属性后，重新注册企业管理器服务。

## wrapper.java.command

Java 应用程序包装器命令。

默认

```
jre\\bin\\java.exe
```

## wrapper.java.mainclass

Java 主类包装命令。

默认

*org.tanukisoftware.wrapper.WrapperSimpleApp*

## wrapper.java.classpath.x

包含 *wrapper.jar* 的 Java 类路径。类路径元素应当按顺序添加，如下所示：

- *wrapper.java.classpath.1=./lib/ServiceWrapper.jar*
- *wrapper.java.classpath.2=./launcher.jar*
- *wrapper.java.classpath.3=*

## wrapper.java.library.path.1

Java 库路径是 *Wrapper.DLL* 或 *libwrapper.so* 的位置。

默认

*./lib*

## wrapper.java.additional.x=

仅在 64 位 Windows 系统上适用的附加 Java 参数。

第一个附加参数必须为 *-Xrs*。此后，您可以按需要添加参数。例如：

- *wrapper.java.additional.1=-Xrs*
- *wrapper.java.additional.1=-Djava.awt.headless=false*
- *wrapper.java.additional.2=-showversion*
- *wrapper.java.additional.3=-XX:+UseConcMarkSweepGC*
- *wrapper.java.additional.4=-XX:+UseParNewGC*

默认

*-Xrs*

## wrapper.java.initmemory

包装器的初始内存大小 (MB)。

默认

128

## wrapper.java.maxmemory

包装的最大内存大小（以兆字节为单位）。

默认

512

## wrapper.app.parameter.x

应用程序参数。可以根据需要添加参数。例如：

- *wrapper.app.parameter.1=org.eclipse.core.launcher.Main*
- *wrapper.app.parameter.2=-consolelog*
- *wrapper.app.parameter.3=-noExit*
- *wrapper.app.parameter.4=-product*
- *wrapper.app.parameter.5=com.wily.introscope.em.product*
- *wrapper.app.parameter.6=-install*
- *wrapper.app.parameter.7=./product/enterprisemanager*
- *wrapper.app.parameter.8=-configuration*
- *wrapper.app.parameter.9=./product/enterprisemanager/configuration*

## wrapper.startup.timeout

从包装器启动 JVM 进程之时起到包装器的 JVM 端响应指出应用程序已启动止，这两个时间点之间所允许的秒数。输入 0 值意味着系统永远不会超时。

默认

30（秒）

### **wrapper.console.format**

控制台的输出格式。

默认

PM

### **wrapper.console.loglevel**

控制台输出的日志级别。

默认

INFO

### **wrapper.logfile**

用于包装器输出日志记录的日志文件的名称和位置。

默认

*./logs/EMService.log*

### **wrapper.logfile.format**

日志文件输出的格式。

默认

LPTM

### **wrapper.logfile.loglevel**

日志文件输出的日志级别。

默认

INFO

## wrapper.logfile.maxsize

在轮转日志之前，允许日志文件增长到的最大大小。大小是以字节为单位指定的。使用默认值 `0` 将禁用日志轮转。您可以使用缩写的 `k (kb)` 或 `m (mb)` 后缀。例如，`10m = 10 megabytes`。

**默认**

`0`

## wrapper.logfile.maxfiles

删除旧文件前允许的轮转日志文件的最大数量。默认值 `0` 表示无限制。

**默认**

`0`

## wrapper.syslog.loglevel

系统和事件日志输出的日志级别。

**默认**

`NONE`

**注释**

当使用该配置文件的应用程序已安装为服务时，不要修改以下任何 `ntservice` 属性。在修改此节之前，请卸载该服务。在进行修改后，可以重新安装该服务。

## wrapper.ntservice.name

服务的名称。

**默认**

`IScopeEM`

### **wrapper.nts.service.displayname**

显示服务名称。

**默认**

Introscope Enterprise Manager

### **wrapper.nts.service.description**

服务的说明。

**默认**

Introscope Enterprise Manager

### **wrapper.nts.service.dependency.x**

服务依赖关系。从 1 开始按需要添加依赖关系。例如：

- *wrapper.nts.service.dependency.1=*
- *wrapper.nts.service.dependency.2=*
- *wrapper.nts.service.dependency.3=*

### **wrapper.nts.service.starttype**

服务的安装模式。设置包括 *AUTO\_START* 或 *DEMAND\_START*。

**默认**

*AUTO\_START*

### **wrapper.nts.service.interactive**

如果将此值设置为 *true*，则会启动服务以与桌面进行交互。

**默认**

*false*



## Introscope Enterprise Manager.lax

*Introscope Enterprise Manager.lax file* 位于 <EM\_Home> 目录中。企业管理器的运行时行为是由此文件中定义的属性控制的。

### lax.application.name

企业管理器可执行文件的默认名称。

**警告！** 请勿编辑。

默认

Introscope Enterprise Manager.exe

### lax.class.path

运行该应用程序时需要的 Java 类路径。

可以为其附加 JDBC 驱动程序和许可证。

可以通过冒号 (Mac OS/UNIX) 或分号 (Windows) 来分隔。

示例

```
lax.class.path=launcher.jar;lax.jar
```

默认

<blank>

### lax.command.line.args

这将传递到主方法。输入此值时，请确保将带空格的参数用引号引起来。例如：

```
lax.command.line.args=$CMD_LINE_ARGUMENTS$ -consolelog -noExit -product  
com.wily.introscope.em.product -install ".\\product\\enterprisemanager"  
-configuration ".\\product\\enterprisemanager\\configuration"
```

默认

<blank>

## **lax.dir**

包含 LaunchAnywhere 的本地启动程序的目录路径。

**默认**

<blank>

## **lax.main.class**

包含应用程序的主方法的类。

**示例**

*lax.main.class=org.eclipse.core.launcher.Main*

**默认**

main

## **lax.main.method**

LaunchAnywhere 的 Java 启动程序的主方法。不应调整此属性，其默认值为：*lax.nl.java.launcher.main.method=main*

**默认**

main

## **lax.nl.current.vm**

此属性代表在下次启动企业管理器时要使用的虚拟机。可将其设置为使用某个已安装的 JRE。有关 JVM 版本要求的信息，请参阅《*CA APM 安装和升级指南*》。

**示例**

如果您配置此属性以使用所提供的绑定 JVM，则此属性将如下所示：

*lax.nl.current.vm=jre\bin\java.exe*

**默认**

默认值因操作系统而异。

## **lax.nl.java.launcher.main.class**

LaunchAnywhere Java 启动程序的主类。不应调整此属性，其默认值为：  
*lax.nl.java.launcher.main.class=com.zerog.lax.LAX*

默认

*com.zerog.lax.LAX*

## **lax.nl.java.launcher.main.method**

LaunchAnywhere 的 Java 启动程序的主方法。不应调整此属性，其默认值为：  
*lax.nl.java.launcher.main.method=main*

默认

main

## lax.nl.java.option.additional

可选 Java 参数（例如，堆大小）。

### 示例

```
lax.nl.java.option.additional=-Xms512m -Xmx1024m  
-Djava.awt.headless=false -XX:MaxPermSize=256m  
-XX:+UseConcMarkSweepGC -XX:+UseParNewGC  
-XX:CMSInitiatingOccupancyFraction=50 -Dorg.cleanclean=false
```

对于 32 位 Sun JVM，建议使用以下开关：

```
-showversion -XX:+UseConcMarkSweepGC -XX:+UseParNewGC  
-XX:CMSInitiatingOccupancyFraction=50 -XX:MaxPermSize=256m
```

例如：

```
lax.nl.java.option.additional=-Xms512m -Xmx1024m  
-Djava.awt.headless=false -XX:MaxPermSize=256m  
-showversion -XX:+UseConcMarkSweepGC -XX:+UseParNewGC  
-XX:CMSInitiatingOccupancyFraction=50
```

**注意：**以下开关仅适用于 32 位 Sun JVM：-showversion  
-XX:+UseConcMarkSweepGC -XX:+UseParNewGC。

如果您使用的是 64 位平台，请将 -Xss 开关设置为 512k。

例如：

```
lax.nl.java.option.additional=-Xms512m -Xmx1024m  
-Djava.awt.headless=false -XX:MaxPermSize=256m  
-Dmail.mime.charset=UTF-8  
-Dorg.owasp.esapi.resources=./config/esapi -Xss512k
```

### 默认

<blank>

## lax.nl.message.vm.not.loaded

在 *lax.nl.valid.vm.list* 中找不到虚拟机时，显示在用户对话框中的消息。此属性是 InstallAnywhere 启动程序的内部属性。Introscope 具有不同的 Java 要求。有关 JVM 要求的信息，请参阅《CA APM 安装和升级指南》。

lax.nl.message.vm.not.loaded=LaunchAnywhere 找不到 Java VM，或者该系统上的 Java VM 太旧。LaunchAnywhere 需要 Java 2 VM 才能启动 Introscope。

## **lax.nl.valid.vm.list**

字符串值，其中包含以空格或逗号分隔的一个或多个 [ *ALL JDK JRE J1 J2 JRE\_J1 JDK\_J1 JRE\_J2 JDK\_J2 MSJ* ]。如果本地启动程序无法找到当前的虚拟机，则它将在以下列表中搜索值：*lax.nl.valid.vm.list=J2*。

默认

J2

## **lax.nl.win32.microsoftvm.min.version**

可以与此启动程序一起运行的 Microsoft 虚拟机的最小版本。例如：

*lax.nl.win32.microsoftvm.min.version=2750*。

默认

2750

## **lax.root.install.dir**

*installdir* magic 文件夹的路径。例如：

*lax.root.install.dir=*。

默认

<blank>

## **lax.stderr.redirect**

标准错误输出。

设置为：

- 空白，表示无输出。
- *console*，表示发送到控制台窗口。
- 任意文件路径，表示将保存到文件。

默认

console

## lax.stdin.redirect

设置为:

- 空白, 表示无输出。
- *console*, 表示发送到控制台窗口。
- 任意文件路径, 表示将保存到文件。

### 注释

如果您正在针对 UNIX 平台以 `nohup` 模式运行企业管理器, 请不要更改此设置, 否则企业管理器可能无法启动。

如果本地要求指示您将此属性设置为空白, 则您必须将 [introscope.enterprisemanager.disableInteractiveMode](#) (p. 384) 设置为 `true`。

### 默认

`console`

## lax.stdout.redirect

标准输出。

设置为:

- 空白, 表示无输出。
- *console*, 表示发送到控制台窗口。
- 任意文件路径, 表示将保存到文件。

### 默认

`console`

## **lax.user.dir**

如果保留为空白，则此属性会导致本地启动程序不更改用于设置用户目录的平台默认行为。

要覆盖此属性，您可以将此属性设置为相对路径或绝对路径，相对路径相对于启动程序。

### **示例**

`lax.user.dir=.`

### **默认**

<blank>

## **lax.version**

创建属性文件时使用的 LaunchAnywhere 版本。例如，  
`lax.version=<VersionNumber>`

### **默认**

10.0

## **IntroScopeWorkstation.properties**

工作站的很多行为是由该文件中的属性控制的。

## log4j.logger.Workstation

控制日志记录详细信息数量和 workstation 日志的输出位置。

详细信息级别值可以是：

- 致命
- 警告
- INFO
- `VERBOSE#com.wily.util.feedback.Log4JSeverityLevel`  
(该值增大所记录的详细信息的级别。)
- 调试
- TRACE

目标值可以为：

- `console`
- 日志文件

默认

`INFO, console`

## log4j.appender.logfile.File

workstation 日志文件的名称和位置。

默认

`IntroscopeWorkstation.log`

## Introscope.workstation.graph.antialiased

这用于控制图形中的线条和符号的抗锯齿处理。如果将此值设置为 `False`，则禁用抗锯齿处理。

默认

`true`



## transport.http.proxy.host

一个 HTTP 隧道代理服务器属性，指定工作站基于 HTTP 在其上执行隧道操作的主机。如果选择了此方式，则必须通过一个代理服务器（转发代理）连接到企业管理器。如果无法在指定的主机和端口到达代理服务器，则在连接尝试失败前，工作站尝试建立到企业管理器的直接 HTTP 隧道连接。

**默认**

<blank>

## transport.http.proxy.port

“HTTP 隧道代理服务器”属性，指定工作站通过 HTTP 传送的端口。如果选择了此方式，则必须通过一个代理服务器（转发代理）连接到企业管理器。如果无法在指定的主机和端口到达代理服务器，则在连接尝试失败前，工作站尝试建立到企业管理器的直接 HTTP 隧道连接。

**默认**

<blank>

## transport.http.proxy.username

仅当代理服务器要求进行身份验证时才会应用用户名，在此时您需要输入一个值来表示用户名。

**默认**

<blank>

## transport.http.proxy.password

仅当代理服务器需要进行身份验证时才会应用用户名，此时输入一个值来表示用户必须输入的密码。

**默认**

<blank>

## transport.tcp.truststore

如果您配置 SSL，则此可选属性指定包含可信企业管理器证书的 truststore 的位置。此值可以是绝对路径，也可以是相对于工作站工作目录的相对路径。

如果您是在 Windows 上，必须对反斜线进行转义。例如：

```
transport.tcp.truststore=C:\\Introscope\\config\\internal\\server\\keystore
```

如果没有指定 truststore，则工作站信任所有证书。

**默认**

<blank>

## transport.tcp.trustpassword

truststore 的密码。

**默认**

password

## transport.tcp.keystore

包含工作站证书的 keystore 的位置。绝对路径或相对于工作站工作目录的相对路径。如果您是在 Windows 上，必须对反斜线进行转义。

**示例**

```
..\\Introscope\\config\\internal\\server\\keystore
```

## transport.tcp.keystore

keystore 位置的属性。仅当企业管理器要求客户端身份验证时才需要此属性。

**默认**

internal/server/keystore

## transport.tcp.keypassword

keystore 的密码。

默认

password

## transport.tcp.ciphersuites

设置此属性以启用密码套件（使用密码套件的逗号分隔列表）。如果未指定此属性，则将使用默认的已启用密码套件。

默认

<blank>

注释

当该文件包含以下属性时，在正常使用时不应修改这些属性：

- log4j.additivity.Workstation=false
- log4j.appender.console=com.wily.org.apache.log4j.ConsoleAppender
- log4j.appender.console.layout=com.wily.org.apache.log4j.PatternLayout
- log4j.appender.console.layout.ConversionPattern=%d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n
- log4j.appender.logfile=com.wily.org.apache.log4j.RollingFileAppender
- log4j.appender.logfile.layout=com.wily.org.apache.log4j.PatternLayout
- log4j.appender.logfile.layout.ConversionPattern=%d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n
- log4j.appender.logfile.MaxBackupIndex=4
- log4j.appender.logfile.MaxFileSize=200MB

## Introscope Workstation.lax

各种工作站行为由在此文件中定义的属性进行控制。

## **lax.application.name**

**重要信息！** 不要编辑此可执行文件的默认名称，这一点很重要。

**默认**

Introscope Workstation.exe

## **lax.class.path**

运行该应用程序时需要的 Java 类路径。可以用冒号 (Mac OS/UNIX) 或分号 (Windows) 分隔。

**默认**

launcher.jar;lax.jar

## **lax.command.line.args**

将传递给主方法的命令行参数。可以使用此属性向工作站提供登录值，以便在启动工作站时绕过登录屏幕。

**默认**

\$CMD\_LINE\_ARGUMENTS\$

## **lax.dir**

包含 LaunchAnywhere 的本地启动程序的目录路径。

**默认**

<blank>

## **lax.main.class**

包含应用程序的主方法的类。

**默认**

org.eclipse.core.launcher.Main

## **lax.main.method**

要调用的主类中的方法。

**默认**

main

## **lax.nl.current.vm**

在 Workstation 下次启动时要使用的 VM。可以设置为任何已安装的 JRE 版本。有关 JVM 版本要求的信息，请参阅《CA APM 安装和升级指南》。

**默认**

因操作系统而异。

## **lax.nl.java.launcher.main.class**

**注释**

不要修改此属性，因为它是 LaunchAnywhere 的 java 启动程序的主类。

**默认**

com.zerog.lax.LAX

## **lax.nl.java.launcher.main.method**

**注释**

请勿修改此属性，这一点非常重要，因为此属性是 LaunchAnywhere 的 Java 启动程序的主要方法。

**默认**

main

## **lax.nl.java.option.additional**

JVM 的其他选项设置。

初始的最小和最大堆大小。

**默认**

```
-client -Xms64m -Xmx256m -Dsun.java2d.noddraw=true
```

## **lax.nl.message.vm.not.loaded**

在 *lax.nl.valid.vm.list* 中找不到虚拟机时，显示在用户对话框中的消息。

**注释**

此属性是 InstallAnywhere 启动程序的内部属性。Introscope 具有不同的 Java 要求。有关详细信息，请参阅《CA APM 安装和升级指南》中的系统要求。

**默认**

LaunchAnywhere 找不到 Java VM，或者此系统上的 Java VM 太旧。  
LaunchAnywhere 需要 Java 2 VM 才能启动 Introscope。

## **lax.nl.valid.vm.list**

字符串值，其中包含以空格或逗号分隔的一个或多个 [ ALL JDK JRE J1 J2 JRE\_J1 JDK\_J1 JRE\_J2 JDK\_J2 MSJ ]。如果本机启动程序找不到当前的虚拟机，则将搜索在此列表中定义的虚拟机。

**默认**

J2

## **lax.nl.win32.microsoftvm.min.version**

可以与该版本的 Microsoft 虚拟机启动程序一起运行的最低版本。

**默认**

2750

## lax.root.install.dir

*install*dir magic 文件夹的路径。

默认

<blank>

## lax.stderr.redirect

标准错误输出。

可能的值：

- <blank>—无输出
- *console*—将输出发送到控制台窗口
- <path\_to\_a\_file>—将输出保存到指定文件。

默认

<blank>

## lax.stdin.redirect

标准输入。

可能的值：

- <blank>—无输入
- *console*—从控制台窗口读取
- <path\_to\_a\_file>—从指定文件读取输入

默认

<blank>

## lax.stdout.redirect

标准输出。

可能的值：

- `<blank>`—无输出
- `console`—将输出发送到控制台窗口
- `<path_to_a_file>`—将输出保存到指定文件。

**默认**

`<blank>`

## lax.user.dir

此属性将导致本机启动程序无法改变平台的默认行为，因而无法设置用户目录。

要覆盖此属性，您可以将此属性设置为一个相对路径或绝对路径。相对路径是相对于启动程序的。

**默认**

`<blank>`

## lax.version

创建此属性文件的 LaunchAnywhere 版本。

**默认**

9.0

## IntroscopeWebView.properties

各种 WebView 行为由在此文件中定义的属性进行控制。



## introscope.webview.jetty.configurationFile

Jetty XML 配置文件的路径。绝对路径或相对于配置目录的相对路径。该文件在端口 8443 上创建用于 HTTPS 通信的 SSL 侦听程序。

要使用高级 Jetty 配置，请在 Jetty 配置文件中取消注释此属性，然后修改设置。

introscope.webview.tcp.port 属性可指定 HTTP 侦听程序。如果已取消注释，则不会创建 HTTP 侦听程序。

**默认**

*webview-jetty-config.xml*

## introscope.webview.tcp.ipaddress

一个 WebView HTTP 服务器设置属性，用于将 WebView 绑定到指定的本地 IP 地址。如果未配置此属性，WebView 会接受所有本地地址（通配符地址）上的传入连接。

**默认**

（设置为 WebView 计算机上的一个有效 IP 地址）

## introscope.webview.tcp.port

WebView 用来侦听 HTTP 通信的端口。

**默认**

8080

## introscope.webview.context.path

WebView 的应用程序上下文路径。上下文路径将附加到 WebView 服务器的完全限定主机名和端口号之后，以形成 WebView 根—用于访问 WebView 的 URL。利用此功能，用户可以为 WebView 定义应用程序名称。

如果上下文路径是：

*/webview*

那么，用于访问 WebView 的 URL 是：

*http://host:port/webview/*

默认

*/*

**注意：**如果您正在 SAP 环境中使用 WebView，那么默认是 */webview*

## introscope.webview.enterprisemanager.tcp.host

要连接的企业管理器主机名。

默认

localhost

## introscope.enterprisemanager.webview.disableLogin

决定 WebView 是否可以建立与企业管理器的连接。

默认

false

## introscope.webview.enterprisemanager.tcp.port

要连接到的企业管理器端口。

默认

5001

## log4j.logger.WebView

WebView 日志的日志记录详细信息量。

详细信息级别值可以是：

- *INFO*
- *VERBOSE#com.wily.util.feedback.Log4JSeverityLevel*

目标值可以为：

- *console*
- *日志文件*

**默认**

INFO, console

## log4j.logger.WebServer

WebServer 日志的日志记录详细信息量。

详细信息级别值可以是：

- *INFO*
- *VERBOSE com.wily.util.feedback.Log4JSeverityLevel*

目标值可以为：

- *console*
- *日志文件*

**默认**

INFO, console

## log4j.logger

WebView 使用的第三方软件的日志记录属性。

详细信息级别值可以是：

- *INFO*
- *VERBOSE com.wily.util.feedback.Log4JSeverityLevel*

目标值可以为：

- *console*
- *日志文件*

**默认**

INFO, console

## log4j.logger.com.wily

CA APM 日志的日志记录详细信息量。

详细信息级别值可以是：

- *INFO*
- *VERBOSE com.wily.util.feedback.Log4JSeverityLevel*

目标值可以为：

- *console*
- *日志文件*

**默认**

INFO, console

## log4j.logger.org.apache.myfaces

Apache Myfaces 日志的日志记录详细信息量。

如果在上面指定了 *logfile*，则日志文件的位置会配置为以下属性：*log4j.appender.logfile.File*。如果需要，可以使用完整路径。

**默认**

ERROR、console

## log4j.logger.org.apache.jasper

Apache Jasper 日志的日志记录详细信息量。

如果在上面指定了 `logfile`，则日志文件的位置会配置为以下属性：  
`log4j.appender.logfile.File`。如果需要，可以使用完整路径。

**默认**

ERROR、console

## log4j.logger.org.apache.struts

Apache Struts 日志的日志记录详细信息量。

如果在上面指定了 `logfile`，则日志文件的位置会配置为以下属性：  
`log4j.appender.logfile.File`。如果需要，可以使用完整路径。

**默认**

ERROR、console

## log4j.logger.org.mortbay

Mortbay 日志的日志记录详细信息量。

如果在上面指定了 `logfile`，则日志文件的位置会配置为以下属性：  
`log4j.appender.logfile.File`。如果需要，可以使用完整路径。

**默认**

ERROR、console

## 日志记录配置属性

在正常使用时不应修改下列属性:

- log4j.additivity.WebView=false
- log4j.additivity.WebServer=false
- log4j.additivity.com.wily=false
- log4j.appender.console=com.wily.org.apache.log4j.ConsoleAppender
- log4j.appender.console.layout=com.wily.org.apache.log4j.PatternLayout
- log4j.appender.console.layout.ConversionPattern=%d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n
- log4j.appender.logfile=com.wily.org.apache.log4j.RollingFileAppender
- log4j.appender.logfile.layout=com.wily.org.apache.log4j.PatternLayout
- log4j.appender.logfile.layout.ConversionPattern=%d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n
- log4j.appender.logfile.MaxBackupIndex=4
- log4j.appender.logfile.MaxFileSize=200MB

### 注意

如果该值设置为 `true`，则图形将进行抗锯齿处理（外观更好）。例如，`introscope.workstation.graph.antialiased=true`

### 默认

默认值取决于属性。

## log4j.appender.console

可将此属性添加到 `WebView` 属性文件中，以将消息写入控制台。

### 默认

`logs/IntroscopeWebView.log`

## log4j.appender.logfile

可以将此属性添加到 `WebView` 属性文件，以将消息添加到日志文件。

### 默认

`com.wily.org.apache.log4j.RollingFileAppender`

## log4j.appender.logfile.File

WebView 日志文件的名称和位置（相对于企业管理器主目录）。

默认

logs/IntroscopeWebView.log

## Introscope WebView.lax

WebView 的运行时行为是由该文件中定义的属性控制的。

## 可执行文件的名称

LaunchAnywhere 可执行文件属性文件—Macrovision Corp.

默认

<blank>

## lax.class.path

运行该应用程序时需要的 Java 类路径。

默认

*lib/WebServices.jar:lib/IntroscopeClient.jar:lib/Workstation.jar:lib/WebView  
API.jar:lib/WebViewServer.jar:lib/IntroscopeServices.jar*

## lax.command.line.args

要传递到主方法的命令行参数。可以使用此属性为 WebView 提供登录值，从而在启动 WebView 时绕过登录屏幕。

默认

*\$CMD\_LINE\_ARGUMENTS\$*

## **lax.dir**

LaunchAnywhere 本地启动程序所在目录的路径。

**默认**

<blank>

## **lax.main.class**

包含应用程序的主方法的类。

**默认**

*org.eclipse.core.launcher.Main*

## **lax.main.method**

要调用的主类中的方法。

**默认**

main

## **lax.nl.current.vm**

在 Workstation 下次启动时要使用的 VM。可以设置为任何已安装的 JDK 或 JRE 版本。有关 JVM 版本要求的信息，请参阅《CA APM 安装和升级指南》。

**默认**

因操作系统而异



## **lax.nl.java.launcher.main.class**

LaunchAnywhere Java 启动程序的主类。

### **注释**

不得调整此属性。

### **默认**

com.zerog.lax.LAX

## **lax.nl.java.launcher.main.method**

LaunchAnywhere 的 Java 启动程序的主方法。

### **注释**

不得调整此属性。

### **默认**

main

## **lax.nl.java.option.additional**

JVM 的可选设置，如堆大小。

### **默认**

*-Xms128m -Xmx512m -Djava.awt.headless=false  
-Dsun.java2d.noddraw=true*

## **lax.nl.message.vm.not.loaded**

如果从 *lax.nl.valid.vm.list* 中找不到 VM，消息将显示在用户对话框中。

### **注释**

此属性是 InstallAnywhere 启动程序的内部属性。Introscope 具有不同的 Java 要求。有关详细信息，请参阅《CA APM 安装和升级指南》的系统要求一节。

### **默认**

n/a

## **lax.nl.valid.vm.list**

字符串值，其中包含以空格或逗号分隔的一个或多个 [ ALL JDK JRE J1 J2 JRE\_J1 JDK\_J1 JRE\_J2 JDK\_J2 MSJ ]。如果本机启动程序找不到当前的虚拟机，则将搜索在此列表中定义的虚拟机。

### **默认**

J2

## **lax.nl.win32.microsoftvm.min.version**

可以与该应用程序一起运行的 Microsoft VM 的最低版本。

### **默认**

2750

## **lax.root.installation.dir**

installdir magic 文件夹的路径。

### **默认**

<blank>

## **lax.stderr.redirect**

标准输出。

可能的值：

- `<blank>`—无输出
- `console`—将输出发送到控制台窗口
- `<path_to_a_file>`—将输出保存到指定文件。

**默认**

console

## **lax.stdin.redirect**

标准输入。

可能的值：

- `<blank>`—无输入
- `console`—从控制台窗口读取
- `<path_to_a_file>`—从指定文件读取输入

**默认**

console

## **lax.stdout.redirect**

标准输出。

可能的值：

- `<blank>`—无输出
- `console`—将输出发送到控制台窗口
- `<path_to_a_file>`—将输出保存到指定文件。

**默认**

console

## lax.user.dir

此属性保留为空，因为此属性会导致本地启动程序不更改用于设置用户目录的平台默认行为。要覆盖此行为，请将此属性设置为相对路径或绝对路径。相对路径是相对于启动程序的。

### 默认

<blank>

## lax.version

创建此属性文件的 LaunchAnywhere 版本。

### 默认

9.0

## APMCloudMonitor.properties

您可以使用文件 APMCloudMonitor.properties 中的属性来控制 CA APM Cloud Monitor 行为，并筛选 CA APM Cloud Monitor 代理向企业管理器发送的数据。

默认情况下，CA APM Cloud Monitor 代理安装程序在以下位置安装此文件：

```
<CloudMonitor 代理主目录>/CloudMon/conf/APMCloudMonitor.properties
```

## apmcm.folders.include

定义向企业管理器发送数据的 CA APM Cloud Monitor 文件夹。

### 默认

已注释掉

### 可能的值

- 全部
- 一个或多个文件夹的列表（按名称）

### 格式

逗号分隔的列表

### 示例

folder0, folder1, folder two, folder3

## apmcm.monitors.include

定义向企业管理器发送数据的 CA APM Cloud Monitor 监视器。

### 默认

已注释掉

### 可能的值

- 全部
- 逗号分隔的监视器列表

### 示例

monitor0, monitor1, monitor two, monitor3

## apmcm.checkpoints.include

定义发出测试查询的 CA APM Cloud Monitor 检查点或监控站点。

### 默认

已注释掉

### 可能的值

- 全部
- 一个或多个检查点的列表（按名称）

### 格式

逗号分隔的列表

### 示例

gr, uk, f2, mb, it, nl

**注意：**可以通过选择“产品” > “监控工作站”，来查看检查点缩写的完整列表。

## apmcm.include.inactive.monitors

定义非活动的 CA APM Cloud Monitor 监视器是否向企业管理器发送数据。

### 默认

False

### 可能的值

- false
- true

## apmcm.folder.metrics.include

定义代理向企业管理器发送的 CA APM Cloud Monitor 文件夹度量标准。

### 默认

已注释掉

### 可能的值

查看属性文件中的探测列表。

### 格式

逗号分隔的列表

### 示例

```
probes,probe_errors,checks,check_errors,uptime,ttime,ctime,ptime,dtime,dsize
```

## apmcm.monitor.psp.metrics.include

定义返回度量标准的 CA APM Cloud Monitor 公共状态页。

### 默认

```
color,errors,avg_uptime_cur,avg_uptime_day,avg_perf_cur,avg_perf_day
```

### 可能的值

查看属性文件中的页面列表。

### 格式

逗号分隔的列表

### 示例

```
color,errors,avg_uptime_cur
```

## apmcm.monitor.checkpoint.metrics.include

定义 CA APM Cloud Monitor 代理向企业管理器发送的 CA APM Cloud Monitor 检查点度量标准。

### 默认

rtime,ctime,ptime,ttime,dtime,descry

### 可能的值

查看属性文件中的度量标准列表。

### 格式

逗号分隔的列表

### 示例

rtime,ctime,ptime

## apmcm.force.global.update

默认情况下，CA APM Cloud Monitor 代理每隔 3600 秒检查对以下元数据的更改：

- 重新登录
- 监视器列表的更新
- 文件夹列表的更新
- 检查点列表的更新

如果要强制代理检查更改并立即更新这些元数据，请将默认值更改为任何其他整数。

**注意：**此属性的值不表示任何意义。它只是元数据，当它的值更改为当前值以外的任何值时，它将强制检查元数据（如上所述）。

### 默认值

1

### 可能的值

任何整数。

## apmcm.log.adjustment

CA APM Cloud Monitor 代理将从日志中检索的最大记录数。

每当代理查询度量标准的日志时，它都检查最后一项。日志项的示例如下：

```
[CloudMonitorIntegration.CloudMonitorAgent] Log record found with k=4/21
```

... 其中分母（以上示例中为 21）= 代理每分钟可从日志中检索的最大项数，分子（以上示例中为 4）是在最后一分钟内实际检索的记录数。

当  $k > 1$  时，日志中将显示以下消息：

```
Some probe data may be missing. Automatically adjusting monitor log query. Please consider increasing apmcm.log.adjustment property.
```

此消息指示的自动调整意味着，代理采用 `apmcm.log.adjustment` 的值并将其添加到分母。因此，如果您设置 `apmcm.log.adjustment = 1`，则检索的最大项数将更改为 22。下次当  $k > 1$  时，分母将再增加 1，依此类推。

#### 默认

0

#### 可能的值

任何整数。

#### 其它

该属性是可热配置的。如果您更改了该属性，无需重新启动企业管理器，更改即可生效。



## 附录 B: JDBC API

---

Introscope 包括的一个 API 允许您使用数据分析工具（如 Excel 或 SAS）来查看 Introscope 数据。使用 JDBC 接口，您可以为指定的历史范围提取度量标准和事件数据。数据将与包含 XML 字符串（用于描述表的元数据）的单个列一起返回到表中，并包含结果表。

此部分包含以下主题：

[配置 JDBC API](#) (p. 489)

[使用 JDBC API](#) (p. 489)

### 配置 JDBC API

文件 *IntroscopeJDBC.jar* 包含 JDBC 驱动程序类和该驱动程序需要的所有类。它是客户端应用程序的类路径上需要的唯一文件。

驱动程序类为 *com.wily.introscope.jdbc.IntroscopeDriver*。

URL 格式是（请注意，这非常重要）：

```
jdbc:introscope:net://{username}{:password}@{host}:{em port}
```

例如：

```
jdbc:introscope:net//Admin:@localhost:5001
```

### 使用 JDBC API

Introscope JDBC API 的语法支持下列虚拟视图：

- metric\_data
- trace\_headers
- traces

## 度量标准查询

在执行度量标准查询时，请使用 Introscope JDBC 驱动程序支持的下列数据格式之一：

- *mm/dd/yy hh:mm:ss*
- *EEE MMM dd HH:mm:ss zzz yyyy*

例如，一个度量标准查询可能如下所示：

```
select * from metric_data where agent={regex} and metric={regex} and
timestamp between {starttime} and {endtime}
```

或：

```
select * from metric_data where agent='.*Custom Metric Host.*' and
metric='.*' and timestamp between '01/01/01 00:00:00' and '01/01/07 00:00:00'
```

这些限定符在 SQL 语句中必须按以下顺序出现：

```
[sort by value {ascending|descending}] [maxmatches={max metrics}]
[period={period in seconds}] [aggregateall]
```

**注意：**如果您查询使用 JDBC 驱动程序关闭的代理，则返回“0”值。

这些限定符支持企业管理器的度量标准聚合功能：

限定符	执行的操作
<i>sort by value {a /d}</i>	指示企业管理器对 <i>每个时间片</i> 的度量标准值执行升序或降序 <i>N</i> 排序。将此限定符与 <i>maxmatches</i> 标志一起使用可以为 Top N 匹配指定度量标准限制。
<i>maxmatches</i>	指示企业管理器最多仅为该数量的度量标准返回数据。如果 <i>maxmatches=2</i> ，则仅返回两个度量标准的数据。 这不同于 <i>sql limit</i> 关键字，该关键字限制返回的行数。我们的 <i>maxmatches=2</i> 示例可以为 2 个度量标准返回 50 个时间片，总计 100 行数据。
<i>period</i>	指示企业管理器将数据点聚合到给定期间。例如，企业管理器通常报告 15 秒数据值，但如果 <i>period=60</i> ，则可以聚合到 60 秒。
<i>aggregateall</i>	指示企业管理器将所有度量标准数据聚合到一个汇总的时间片中。例如，您可以使用此限定符为度量标准指定一周内的单一平均响应时间。 请尽量不要将 <i>aggregateall</i> 与 <i>period</i> 限定符一起使用，因为它们都处理聚合并且可能会冲突。

## 度量标准查询示例

```
select * from metric_data where agent='.*' and metric='.*Average Response.*' and
timestamp between '01/01/01 00:00:00' and '01/01/07 00:00:00' maxmatches=10
```

```
select * from metric_data where agent='.*' and metric='.*Average Response.*' and
timestamp between '01/01/01 00:00:00' and '01/01/07 00:00:00' maxmatches=1
```

```
select * from metric_data where agent='.*' and metric='.*Average Response.*' and
timestamp between '01/01/01 00:00:00' and '01/01/07 00:00:00' maxmatches=1
period=120
```

```
// match one metric_data and aggregate all values. This returns one row of data
select * from metrics where agent='.*' and metric='.*Average Response.*' and
timestamp between '01/01/01 00:00:00' and '01/01/07 00:00:00' maxmatches=1
aggregateall
```

```
// this is a top 10 query select * from metric_data where agent='.*' and
metric='.*Average Response.*' and timestamp between '01/01/01 00:00:00' and
'01/01/07 00:00:00' sort by value d maxmatches=10
```

## 事务跟踪查询

基本的事务头查询语法是：

```
select * from trace_headers where timestamp between {starttime} and {endtime} and
query={lucene query string} [limit {rows}]
```

其中，*lucene query string* 是有效的 Lucene 查询字符串，如同在 Workstation 的历史查询中一样（有关详细信息，请参阅《CA APM Workstation 用户指南》）。

可选的 *limit* 标志限制查询返回的行数。如果未指定限制，则将使用服务器中定义的默认事务限制。

用于跟踪正文的查询是相同的，但引用一个不同的视图：

```
select * from traces where timestamp between {starttime} and {endtime} and
query={lucene query string} [limit {rows}]
```

### 事务跟踪查询示例:

```
select * from trace_headers where timestamp between '01/01/01 00:00:00' and  
'01/01/07 00:00:00' and query='s*'
```

```
select * from trace_headers where timestamp between '01/01/01 00:00:00' and  
'01/01/07 00:00:00' and query='host:blinkys'
```

```
select * from traces where timestamp between '01/01/01 00:00:00' and '01/01/07  
00:00:00' and query='host:blinkys' limit 100
```

跟踪查询返回的数据行包括代理信息，例如域、主机、进程和代理名称，以及事务跟踪的 XML 表示形式。

## 附录 C: 配置 Introscope 扩展

---

如果安装时启用了 Introscope 扩展，则必须配置这些扩展。有关安装的详细信息，请参阅《CA APM 安装和升级指南》。

此部分包含以下主题：

[配置 SNMP 适配器](#) (p. 493)

[配置 Introscope 报警 Web 服务扩展](#) (p. 502)

### 配置 SNMP 适配器

SNMP(简单网络管理协议)是用于监控和控制网络组件的一个标准协议。SNMP 适配器使得 Introscope 能够将度量标准报告给外部 SNMP 框架。有关 SNMP 适配器的更多一般信息，请参阅《CA APM Workstation 用户指南》。

#### SNMP 适配器限制

在 SNMP 管理器中读取 Introscope 特定度量标准的能力，使得您可以方便地从一个位置监控来自所有网络组件的数据。不过，请注意 Introscope SNMP 功能的下列限制：

- 在 SNMP 管理器中只能查看 Introscope 度量标准。
- 其他 Introscope 功能（例如报警和操作）不会作为 Introscope 特定信息的一部分来发布。
- Introscope 信息是只读的。
- 不支持对其进行设置。

#### SNMP 适配器组件

SNMP 适配器组件有：

##### SNMP 收集

SNMP 收集是一个 Introscope 元素，它定义将发布到 MIB 文件的度量标准。SNMP 收集存储在一个管理模块中。

## MIB 文件（管理信息库）

MIB 是一个文本文件，用于描述 SNMP 代理所报告的信息。可以将 MIB 文件加载到 SNMP 管理器中，以便管理器了解 SNMP 代理可以报告哪些信息。

Introscope 生成的 MIB 文件是当前活动的 SNMP 收集的时间点快照，以 SNMP 兼容格式描述匹配的 Introscope 度量标准。

## SNMP 代理

系统会在企业管理器部署中安装 Introscope SNMP 代理。代理从企业管理器收集 Introscope 特定的度量标准数据，将其转换为 SNMP 特定的格式，并将其发送到 SNMP 管理器。

## 报警通知

如果触发了报警，并触发了某个 SNMP 通知操作，则 SNMP 适配器会将描述报警的 SNMP 通知（陷阱）发送到在企业管理器属性文件中指定的已配置 SNMP 管理器。

## 报警

如果已经为报警配置了 SNMP 通知操作，则在报警触发时，企业管理器会将 SNMP 通知（陷阱）发送到已配置的 SNMP 管理器。包含报警消息的通知具有一个类型为 *octet string* 的值对象。该内容与用于控制台通知操作的内容相同。

这些 SNMP 对象自动发布在 MIB 中。

通知使用固定的 OID（唯一的对象 ID），如下所述，其中 *xxxx* 是随机选取的 *SnmpAdapter* 标识符（例如 5527）：

## 通知（数值格式）

值: 1.3.6.1.4.1.10480.1.1.xxxx.5000

## 通知（名称格式）

Value:  
*iso.org.dod.internet.private.enterprises.wily.products.introscope.snmpAdapterxxxx.wilyAlertNotif*

## 报警（数值格式）

Value: *1.3.6.1.4.1.10480.1.1.xxxx.6000*

## 报警消息（名称格式）

Value:

*iso.org.dod.internet.private.enterprises.wily.products.introscope.snmpAdapt  
erxxxx.wilyAlertNotifMessage*

## 配置通知和报警

配置通知（陷阱）：

- 编辑 *IntroscopeEnterpriseManager.properties* 并设置以下属性。

### **introscope.agent.enterprisemanager.snmp.target.port**

SNMP 管理器的端口

默认

*162*

### **introscope.agent.enterprisemanager.snmp.target.destination**

SNMP 管理器的主机名或 IP 地址

默认

*localhost*

### **introscope.agent.enterprisemanager.snmp.target.community**

SNMP 管理器的 SNMPv2 团体

默认

*public*

### **introscope.enterprisemanager.snmp.notification.enable**

打开 (*true*) 或关闭 (*false*) 通知

**默认**

true

**注释**

热配置支持 *snmp.notification.enable* 属性，因此设置此属性后不需要重新启动企业管理器。对于其他属性，必须重新启动企业管理器，它才能获取这些属性。

您还可以在 Workstation /企业管理器上配置报警和 SNMP 通知操作。有关详细信息，请参阅《CA APM Workstation 用户指南》以及本指南中的各种主题。

## **配置 SNMP 功能**

使 Introscope 特定的度量标准可在 SNMP 框架中查看：

- 在企业管理器属性文件中启用 SNMP—请参阅[通过配置属性设置启用 SNMP](#) (p. 497)
- 创建 SNMP 收集—有关详细信息，请参阅《CA APM Workstation 用户指南》
- 发布 MIB—有关详细信息，请参阅《CA APM Workstation 用户指南》
- 将 MIB 加载到 SNMP 管理器—请参阅[将 MIB 文件加载到 SNMP 框架](#) (p. 498)



## 通过配置属性设置启用 SNMP

要启用 SNMP, 您需要在 *IntroscopeEnterpriseManager.properties* 文件中配置两个设置。

### 配置设置:

1. 关闭企业管理器（如果企业管理器正在运行）。
2. 打开文件  
`<EM_Home>/config/IntroscopeEnterpriseManager.properties`。
3. 在 `introscope.enterprisemanager.snmp.enable` 设置中, 输入 `true` 值。
4. 在 `introscope.enterprisemanager.snmp.agent.port` 设置中, 接受默认值 161。

**注意:** 如果您正在使用 UNIX 平台, 则必须以 `root` 的身份登录, 或者具有 `root` 的权限, 才能使用低于 1000 的任意端口（默认 SNMP 代理端口是 161）。

1. 保存更改。
2. 重新启动企业管理器。

## 关于 MIB 文件

MIB 文件是根据主机命名的, 并保存在以下目录中:

`<EM_Home>/snmp/`

MIB 文件是使用以下语法发布并唯一地命名的:

- HP LoadRunner: `Introscope-<hostname>.lr.mib`
- HP OpenView: `Introscope-<hostname>.mib`
- BMC Patrol
  - `Introscope-<hostname>.bmc.mib`
  - `Introscope-<hostname>.bmc.smi`
- 其他: `Introscope-<hostname>.other.mib`

主机名中的任何非法字符都将被删除; 主机名中的句点将被转换为破折号。

## 将 MIB 文件加载到 SNMP 框架

SNMP 管理器必须具有 MIB 的副本，才能识别可以从 SNMP 代理获取什么度量标准。在发布一个 MIB 后，必须将该 MIB 文件加载到 SNMP 管理器。

在下列情况下，必须将 MIB 文件上传到 SNMP 管理器：

- 发布了新的 MIB 时。
- 企业管理器或托管应用程序迁移到另一台主机上时。

要在您的 SNMP 框架中使用 Introscope 生成的 MIB，请查阅适用于您的特定 SNMP 框架的文档来了解如何准备 MIB。请与 CA Technologies 专业服务联系以获取帮助。

## 上传到 HP LoadRunner

以下信息截至发布时是最新的。联系 HP 获得更新。

### 将 Introscope 生成的 MIB 文件上传到 HP LoadRunner：

1. 安装 SNMP 适配器：
  - a. 将 *SNMPAdapter.jar* 复制到  
`<EM_Home>/product/enterprisemanager/plugins`。
  - b. 编辑 *IntroscopeEnterpriseManager.properties* 文件（位于  
`<EM_Home>/config/` 中）以设置以下属性：  
`introscope.enterprisemanager.snmp.enable=true`
2. 重新启动企业管理器。
3. 创建一个 SNMP 收集。有关详细信息，请参阅《*CA APM Workstation 用户指南*》。
4. 发布 MIB 文件：
  - a. 如果该文件未打开，请通过选择“文件” > “新建管理模块编辑器”，在 Introscope 调查器中启动管理模块编辑器。
  - b. 通过单击“管理器” > “发布 MIB...” 来发布 MIB 文件。
  - c. 选择“LoadRunner”。
  - d. 单击“发布”。
5. 复制 MIB 文件：
  - 从：`<EM_Home>/snmp`
  - 到：`SiteScope: <SiteScope>/templates.mib`
6. 重新启动 SiteScope Windows 服务。

7. 使用 SiteScope SNMP Browser 确认已加载了 MIB 文件：
  - a. 转到“开始”>“程序”>“HP SiteScope”>“打开 HP SiteScope LR”。
  - b. 单击“打开 SiteScope”。
  - c. 打开“监视器”选项卡。
  - d. 选择“SiteScope”>“工具”>“SNMP Browser”。
  - e. 输入企业管理器主机名，版本为 V2。
  - f. 选择 MIB 文件。
  - g. 单击“浏览”。
8. 添加度量：
  - a. 打开 LoadRunner Controller。单击“开始”>“程序”>“HP LoadRunner”>“应用程序”>“Controller”。
  - b. 创建一个手工场景。
  - c. 在“场景”窗口中，单击“运行”选项卡。
  - d. 在“可用图表”>“系统资源图表”列表中双击“SNMP”。
  - e. 选择“SNMP 图表”。
  - f. 选择“监视器”>“添加度量”。
9. 在“SNMP”对话框中：
  - a. 单击“高级”。
  - b. 选择“SiteScope”并单击“确定”。
  - c. 选择“添加”以添加新的受监控服务器计算机。
  - d. 将企业管理器主机设置为受监控的服务器，然后单击“确定”。
  - e. 选择“添加”以添加资源度量。
  - f. 确认服务器已设置为企业管理器计算机名称。
  - g. 将 SNMP 版本更改为 V2。
  - h. 将“每...”更新为较高的值。如果此设置太低，HP LoadRunner 可能会显示错误。
10. 展开树并选择所需的 OID（度量标准）。
11. 在 HP LoadRunner 中验证数据。

## 注意：

如果您使用 HP LoadRunner：

- 要查看已发布的数据，需要使用 HP LoadRunner SNMP 监控器。
- 如果 MIB 没有显示在 SiteScope SNMP Browser 中，请检查错误日志文件。
- 因为 HP LoadRunner 不允许 MIB 中的任何节点具有相同的名称，所以，MIB 中具有相同名称的度量标准在显示时名称中会附加数字。例如：  
fileInputRateBytesPerSecond23
- HP LoadRunner 不会在图表中绘制负数。

## 上传到 HP OpenView

将 Introscope 生成的 MIB 文件上传到 HP OpenView：

1. 安装 SNMP 适配器：
  - a. 将 *SNMPAdapter.jar* 复制到  
<EM\_Home>/product/enterprisemanager/plugins。
  - b. 编辑 *IntroscopeEnterpriseManager.properties* 文件（位于  
<EM\_Home>/config/ 中）以设置以下属性：  
introscope.enterprisemanager.snmp.enable=true
2. 重新启动企业管理器。
3. 创建一个 SNMP 收集。有关详细信息，请参阅《CA APM Workstation 用户指南》。
4. 发布 MIB 文件：
  - a. 如果管理模块编辑器未打开，请通过依次选择“文件”>“新建管理模块编辑器”在 Introscope 调查器中启动该编辑器。
  - b. 通过单击“管理器”>“发布 MIB...”来发布 MIB 文件。
  - c. 选择“HP OpenView”。
  - d. 单击“发布”。
5. 复制 MIB 文件：
  - 从：<EM\_Home>/snmp
  - 到：安装有 HP OpenView 的计算机
6. 在 HP OpenView 计算机上，执行“开始”>“程序”>“HP OpenView”>“Network Node Manager Admin”>“Network Node Manager”

7. 在根控制台中，转到“设置” > “加载”。
8. 在“卸载 .mib”下，选择“SNMP”。
9. 单击“加载”。
10. 选择 Introscope MIB 文件。  
文件名将包括生成 MIB 文件的企业管理器的名称。
11. 在加载完成后，单击“关闭”。
12. 打开 MIB 浏览器。执行“工具” > “SNMP”。
  - a. 在“名称”或“地址”字段中，输入企业管理器主机名。  
这将是 Introscope 中在 MIB 文件名中引用的同一主机名。
  - b. 在“团体名称”字段中，输入 *public*。
  - c. 展开节点：  
iso > org > dod > private > enterprises > wily > products > introscope > snmpAdapter > hostname

#### 在图表中显示度量标准:

1. 选择一个度量标准。
2. 单击“图表”。

#### 在 MIB 中查找度量标准:

1. 从 MIB 中选择任意主机名、代理名称、资源名称。
2. 单击“启动查询”。

## 将 Introscope 度量标准转换为 SNMP 度量标准

Introscope 将 Introscope 度量标准类型和 Introscope 度量标准名称转换为 SNMP 兼容的信息。

### 度量标准类型转换

SNMP 代理将 Introscope 度量标准转换为 SMiv2 度量标准类型，如下所示:

Introscope 度量标准类型	常规 MIB SMiv 2 度量标准类型	HP OpenView 或 LoadRunner MIB SMiv 2 度量标准类型	BMC MIB SMiv 2 度量标准类型
Int	INTEGER32(-2147483648...2147483647	INTEGER32(-2147483648...2147483647	COUNTER32(-2147483648...2147483647

长整型	INTEGER32 (同上)	INTEGER32 (同上)	COUNTER32 (同上)
字符串	OCTETSTRING	OCTETSTRING	OCTETSTRING

SNMP 不支持大于 32 位的整数。Long 类型的数据将使用以下算法转换为 32 位整数：

- 如果 long 类型的数据大于 Integer.MAX\_VALUE，则将其设置为 Integer\_MAX\_VALUE
- 如果 long 类型的数据小于 MIN\_VALUE，则将其设置为 MIN\_VALUE
- 其他情况下，简单地将其转换为一个 Int 数据

## 度量标准名称转换

SNMP 代理使用以下规则将 Introscope 度量标准名称段转换为 MIB 标识符：

1. 段必须仅包含合法字符 (A-Z|a-z|-|0-9)。段中的任何非法字符都将被删除。
2. 每个段必须以小写字母开头。如果段以大写字母开头，则会将其转变为小写。如果段以数字开头，则会在数字前附加字母“a”作为前缀。
3. 段不能以连字符结尾。结尾的连字符将被删除。
4. 段不能包含两个连续的连字符。将删除一个连字符。

段中包含的字符数必须等于或小于 64 个。如果段多于 64 个字符，则会将其截短到 64 个字符。如果截短导致存在相同的段，则会进一步截短段，并添加一条短划线和一个数字，例如 (-2)。

## 配置 Introscope 报警 Web 服务扩展

Introscope 提供了各种 CA APM Web 服务 API，以便您可以使用第三方应用程序将 CA Introscope 用作报警和度量标准的来源。您需要配置 CA Introscope 报警 Web 服务扩展以配置可供您的第三方应用程序使用的 CA Introscope 报警。

下面的属性没有出现在 IntroscopeEnterpriseManager.properties 中。您必须手动在文件中添加它们以进行配置。

有关随企业管理器一起安装的 Web 服务文件的详细信息，请参阅《CA APM 安装和升级指南》。

**配置 Introscope 报警 Web 服务扩展:**

1. 打开 *IntroscopeEnterpriseManager.properties* 文件，它位于 `<EM_Home>/config` 目录中。
2. 添加 *introscope.alerts.extension.managementmodules.enable* 属性，并列出您要为其提供报警的管理模块。如果您将该属性值保留为空或指定了“ALL”，则 CA Introscope 将提供来自所有管理模块的报警。
3. 添加以下属性：  
*introscope.alerts.extension.inventory.updatecheckintervalsecs*。该属性指定报警扩展检查报警的频率（以秒为单位）。如果您未指定值，则默认情况下 Introscope 每 60 秒检查一次。您不能指定低于 15 秒的值；如果指定的值小于 15 秒，则 Introscope 默认为 15 秒。  
如果您在上述时间间隔内添加代理、删除代理或者保存对管理模块的更改，则 CA Introscope 会针对代理和管理模块执行内部清单检查。Introscope 在处理报警状态更改之前会更新清单。
4. 重新启动企业管理器以使属性文件更改生效。





## 附录 D: 默认 `tess-default.properties` 文件

---

`tess-default.properties` 文件包含很少修改的已分类属性，这些属性只应由有经验的 CA CEM 管理员修改，或在 CA Support 的指导下进行修改。

此部分包含以下主题：

[修改 `tess-default.properties` 属性默认文件](#) (p. 505)

[设置用于证据收集的 Perl 或 Python 路径](#) (p. 506)

[设置“其他缺陷信息”链接的目录路径](#) (p. 507)

[改进缺陷处理性能](#) (p. 508)

[更改损坏文件的目录位置](#) (p. 510)

[其他 CA CEM 默认属性](#) (p. 511)

### 修改 `tess-default.properties` 属性默认文件

CA CEM `tess-default.properties` 文件位于 `<EM_Home>/config` 目录中。

**重要信息！** 如果需要编辑任何默认的属性，需要创建该文件的自定义版本；将其命名为：

`tess-customer.properties`

通过创建自己的名为 `tess-customer.properties` 的属性文件，确保您的属性修改在随后 CA CEM 软件升级期间不会丢失。

**警告！** 在群集环境中，创建或编辑 `tess-customer.properties` 文件之后，必须将该文件复制到每个企业管理器。

每个企业管理器都有一个 `tess-default.properties` 文件。企业管理器从其本地文件读取的属性取决于在该企业管理器上运行的服务。例如，与客户体验度量标准相关的属性从运行 TIM 收集服务的企业管理器中读取，而与最大用户组数相关的属性从管理器的管理器中读取。

请执行以下步骤：

1. 找到文件：

`<EM_Home>/config/tess-default.properties`

2. 在同一目录中创建自己的 `tess-default.properties` 文件版本，并将其命名为 `tess-customer.properties`。

3. 修改 `tess-customer.properties` 文件，只添加您需要针对自己的 CA CEM 环境修改的属性。
  - a. 编辑新的属性文件。

例如，使用 vi 编辑器：

```
vi tess-customer.properties
```

**重要信息!** `tess-customer.properties` 文件应只包含值与 CA CEM 系统默认值不同的属性。如果您将所有属性都保留在 `tess-customer.properties` 文件中，则系统升级可能不会充分利用将来系统的性能或者经优化的属性更新。
  - b. 保存 `tess-customer.properties` 文件。
4. 将 `tess-customer.properties` 文件复制到群集中的所有企业管理器。
5. 重新启动群集中的每个企业管理器。

## 设置用于证据收集的 Perl 或 Python 路径

要使用证据收集（[为突发事件设置业务影响并收集证据](#) (p. 264)），您需要在 MOM 或单独的企业管理器上安装 Python 或 Perl。编辑 `python.path` 或 `perl.path` 属性来指定 Python 或 Perl 的位置。

### perl.path

已经安装 Perl 的目录。

#### 选项

Perl 可执行文件的目录路径

#### 默认

`/usr/bin/perl`

#### 示例

`C:\\perl\\bin\\perl.exe`

#### 注释

如果为 Windows 平台使用反斜线，则需要使用双斜线 (\\)，因为单斜线 (\) 将解析为转义字符。

## python.path

已经安装 Python 的目录。

### 选项

Python 可执行文件的目录路径

### 默认

/usr/bin/python

### 示例

C:\\python\\bin\\python.exe

### 注释

如果为 Windows 平台使用反斜线，则需要使用双斜线 (\\)，因为单斜线 (\) 将解析为转义字符。

## 设置“其他缺陷信息”链接的目录路径

为了使“其他缺陷信息”链接显示在缺陷详细信息页面上，必须存在使用缺陷编号命名的 HTML 文件。

缺陷详细信息页面可以链接到可包含其他缺陷信息的自定义网页。当前的缺陷详细信息页面显示有关于缺陷的各种详细信息，如时间、吞吐量和 Web 服务器地址。不过，可能还有一个有关缺陷的其他详细信息（与公司需求联系更为紧密的详细信息），您也可能希望添加到缺陷详细信息页面。

CA Technologies 专业服务可以提供该缺陷信息，并将其保存在 CA CEM 的目录中。这个其他缺陷信息（可从缺陷详细信息页面上的“其他缺陷信息”链接访问），有助于对最终用户问题归类，并显示与各缺陷相关的上下文信息。

要使“其他缺陷信息”链接显示在给定缺陷的缺陷详细信息页面的底部，必须符合以下条件：

- 必须存在使用此约定命名的文件：**defect-`<defectId>`.htm**
- 文件必须放在 `additionalDefectDetailFileLocation` 属性指定的目录中。

例如，如果该文件位于 MOM

`<EM_Home>/cem/tess/additionaldefectdetails/defect-60000000000000026.htm`，则指向此页面的链接显示在缺陷编号为 60000000000000026 的缺陷详细信息页面上。

如果您有该 HTML 文件的读取权限，则当您单击“其他缺陷信息”链接时，会显示该 HTML 页面。

**重要信息！** 确认您已编写用于删除旧的 `defect-<defectId>.htm` 文件的脚本。当缺陷过期时，系统不自动删除这些文件。

## additionalDefectDetailFileLocation

如果名为 `defect-<DefectID>.htm` 的文件位于 MOM 上的该目录中，则指向该文件的链接显示在缺陷的“缺陷详细信息”页面的底部。

在群集环境中：

- 该目录必须位于 MOM 上。
- `additionalDefectDetailFileLocation` 属性从 MOM、`tess-customer.properties` 文件或 `tess-default.properties` 文件读取。

### 选项

目录路径。这可能是绝对路径或相对于 MOM `<EM_Home>` 的相对路径。

### 默认

`cem/tess/additionaldefectdetails`

### 示例

`C:\\test\\evidence_for_defects` (Windows 示例)

`/test/evidence_for_defects` (UNIX 示例)

### 注释

如果为 Windows 平台使用反斜线，则需要使用双斜线 (\\)，因为单斜线 (\) 将解析为转义字符。

## 改进缺陷处理性能

查询数据库以确定受突发事件影响的用户组数可能占用大量 CPU 资源。如果突发事件包含许多缺陷，这种情况尤甚。查询受影响的用户组可能推迟缺陷的处理。减少查询频率可以减少这些延迟。

默认情况下，只要将缺陷添加到突发事件中，系统便执行 `affected-user-group` 查询。不过，您可以选择减少执行该查询的频率（以特定的 `更新时间间隔` 查询），而不是在每次发现缺陷时都查询。

如果按一定的时间间隔执行 `affected-user-group` 查询，则在该时间间隔内会创建一个缓存，用于存放当前 `affected-user-group` 计数。除了设置更新时间间隔之外，还需设置 `过期时间间隔` 属性，以确定从缓存中删除空闲突发事件的频率。

**注意：**降低执行该查询的频率的负面影响是，`affected-user-group` 计数可能会因更新时间间隔长度，或在极少情况下，因过期时间间隔的长度而过期。不过，如果这能提高处理缺陷的性能，稍微延迟的计数对您而言可能是一个很好的折中。

### 减少查询 `affected-user-groups` 的频率：

1. （可选）确认缺陷处理延迟。

例如，选择“CEM” > “突发事件管理” > “缺陷”并显示所有缺陷。缺陷是否如预期那样出现或者是否有延迟？

2. 按照 [修改 `tess-default.properties` 文件](#) (p. 505) 中的过程执行操作。指定这些属性的值：

- `defects.affectedUserGroupUpdateInterval_Secs`（更新时间间隔）
- `defects.affectedUserGroupAgeoutInterval_Mins`（过期时间间隔）

例如：

```
defects.affectedUserGroupUpdateInterval_Secs=180
defects.affectedUserGroupAgeoutInterval_Mins=10
```

CA Technologies 建议更新时间间隔的初始值为 180 秒，过期时间间隔的初始值为 10 分钟。如果 `affected-user-group` 查询导致缺陷处理延迟，则您应看到这些值带来的改进效果。

有关这些属性的详细信息，请参阅

[defects.affectedUserGroupUpdateInterval\\_Secs](#) (p. 509) 和 [defects.affectedUserGroupAgeoutInterval\\_Mins](#) (p. 510)。

## `defects.affectedUserGroupUpdateInterval_Secs`

查询和与突发事件关联的受影响的用户组数之间的时间间隔（以秒为单位）。

### 选项

数值，表示秒数：

- 最小值 0，指定只要将缺陷添加到突发事件中，便会执行 `affected-user-group` 查询。
- 建议的最大值为 3600（1 小时）。

### 默认

0

### 示例

```
defects.affectedUserGroupUpdateInterval_Secs=180
```

### 注释

所报告的 **affected-user-group** 计数可能因时间间隔值太大，或在极少情况下，因过期时间间隔长度而过期。

## defects.affectedUserGroupAgeoutInterval\_Mins

如果某个突发事件的空闲（未更新）时间超过该值，则系统会从 **affected-user-group** 缓存中删除该突发事件（过期）。

### 选项

数值，表示分钟数：

- 最小值，将过期时间间隔设置为更新时间间隔值的两倍多。否则，IntroscopeEnterpriseManager 日志中会显示警告，并将该值重置为更新时间间隔的两倍。
- 建议的最大值为 121 分钟（刚超过 2 小时）。

### 默认

1

### 示例

```
defects.affectedUserGroupAgeoutInterval_Mins=10
```

### 注释

该值应大于更新时间间隔的两倍，并小于更新时间间隔的四倍。例如，如果更新时间间隔为 180 秒，过期时间间隔应介于 7 到 11 分钟。

当将某个突发事件从缓存中删除时，会运行 **affected-user-group** 查询，同时会更新该突发事件的 **affected-user-group** 计数。这将防止计数因超过过期时间间隔而过期。

## 更改损坏文件的目录位置

默认情况下，从 TIM 发送到企业管理器的数据文件存储在以下目录中：

- **cem/tess/badfiles**（因存在问题而无法处理的文件将放入该目录。日志文件会报告将文件移到该目录的时间。该目录中的文件不会自动删除。如果该目录中有许多文件，请将其删除。）

可以通过[修改 tess-default.properties 文件](#) (p. 505)来更改这些目录。

以下是您可能要配置这些目录的原因：

- 磁盘空间问题：将目录移至更大的驱动器。
- 如果您将 TIM 收集服务从一个企业管理器移到另一个企业管理器，而且如果这两个企业管理器上的 `tess-customer.properties` 文件都指向同一台（第三台）计算机上的同一目录，则当您移动 TIM 收集服务时不会丢失数据。

默认情况下，当 TIM 收集服务移至其他企业管理器时，系统不会处理原始企业管理器上余留的任何未处理数据文件（除非该服务又移回到原始企业管理器）。

## collectors.badDataDirectory

如果文件因包含错误而不能进行处理，则将文件移到该目录。

### 选项

目录路径。如果路径是相对路径，则它是相对于 `<EM_Home>` 的路径。如果指定了绝对路径，则按原样使用。

### 默认

`cem/tess/badfiles`

### 示例

`collectors.badDataDirectory=cem/TIMdatafiles/badfiles`

`collectors.badDataDirectory=/tmp/badfiles`

`collectors.badDataDirectory=N:\\cem\\badfilesfromtess`

`collectors.badDataDirectory=\\\\server2\\c$\\cem\\tess\\badfiles`

### 注释

如果为 Windows 平台使用反斜线，则需要使用双斜线 (\\)，因为单斜线 (\) 将解析为转义字符。

如果该目录不存在，系统会创建该目录。

## 其他 CA CEM 默认属性

本主题提供了有关其他一些 <wcem> 默认属性的信息：

[baseline.durationInDays](#) (p. 512)

[BTStatsMetricName.backwardCompatible](#) (p. 513)

[email.defaultFromAddress](#) (p. 513)

[invalid.importexport.filename.chars](#) (p. 514)

[timTessCommunication.useSsl](#) (p. 514)

## baseline.durationInDays

用于基准计算的每小时数据的天数。

默认值为 **28**。这意味着基准计算基于在过去 **28** 天内收集到的每小时数据。

用法示例：您知道 CA CEM 10 天来一直在收集数据，但因为前 3 天在实验和更改事务定义，因此这 3 天的数据无效。因此，您将值设置为 7。随着收集到有效数据的天数越来越多，您后来增加了该值。

### 选项

数值

### 默认

28

### 示例

baseline.durationInDays=7

### 注释

使用的数字为 7 的倍数是因为，在大多数情况下，受监控的事务的常规业务周期是一周。

有关基准的一般信息，请参阅《CA APM 事务定义指南》。



## BTStatsMetricName.backwardCompatible

适用于：CA CEM 5.0 和 4.5 兼容性。

在 CA CEM 5.0 中，术语“业务流程”已更改为“业务服务”。该属性允许您继续将 CA CEM 4.5 显示板度量标准名称用于客户体验度量标准。

### 选项

true 或 false

如果为 true，则使用 CA CEM 4.5 度量标准名称“业务流程”。

如果为 false，则使用名称“业务服务”。

### 默认

false

### 示例

```
BTStatsMetricName.backwardCompatible=false
```

### 注释

如果将该设置更改为 true，则必须使用 CA CEM 4.5 的 Javascript 计算器。

## email.defaultFromAddress

如果 Embedded Entitlements Manager 未用于身份验证，或在 Embedded Entitlements Manager 中没有指定用户的电子邮件地址，则使用该地址测试 SMTP 服务器设置，并可能将其作为电子邮件报告的“发件人”地址。

### 选项

有效的电子邮件地址

### 默认

```
support@catechnologies.com
```

### 示例

```
email.defaultFromAddress=my.email@company.com
```

### 注释

如果使用该属性，则该属性显示在“系统” > “电子邮件设置”页面的“发件人地址”和“收件人”字段中。

## invalid.importexport.filename.chars

指定可在导出的业务服务名称中使用的特殊字符。

### 选项

在 Linux 文件名中不允许使用的特殊字符。

### 默认

```
/\:*?<>&|
```

### 示例

```
invalid.importexport.filename.chars=/\:*?<>&|
```

### 注释

当导出业务服务时，导出文件的名称基于业务服务的名称。如果该名称包含不允许在文件名中使用的字符，则导出失败。

为防止发生该故障，确保使用该属性列表中的字符。在创建导出文件时，这些字符将由下划线取代。例如，当导出名为 my&BP 的业务服务时，导出文件名为 BTEExport\_my\_BP\_<timestamp>.zip。

## timTessCommunication.useSsl

确定企业管理器/TIM 通信是通过 HTTP 还是 HTTPS。

### 选项

0 或 1

如果为 0，则企业管理器和 TIM 通过 HTTP 通信。

如果为 1，则企业管理器和 TIM 通过 HTTPS 通信。

### 默认

0

### 示例

```
timTessCommunication.useSsl=1
```

### 注释

tess-default.properties 文件中不存在该属性。您需要将其添加到 tess-customer.properties 文件。

