故障诊断工具

本节介绍用于配置、监控和排查 Unified Communications Manager 的工具和实用程序，并提供收集信息的一般指导原则，以避免重复测试和重复收集相同的数据。

注释 要访问本文档中列出的部分 URL 站点，您必须是注册用户且必须登录。

Cisco Unified 功能配置故障诊断工具

有关 Cisco Unified 功能配置 提供用于监控和分析各种 Unified Communications Manager 系统的以下不同类型工具的详细信息，请参阅《*Cisco Unified* 功能配置管理指南》。

表 *1:* 功能配置工具

术语	定义
Cisco Unified 实时监控工具 (RTMT)	此工具提供关于 Unified Communications Manager 设备和性能计数器的实时信息，可用于收集跟踪。 性能计数器可以特定于系统，也可以特定于 Unified Communications Manager。对象包含特定设备或功能的类似计数器的逻辑分组，例如 Cisco Unified IP 电话 或 Unified Communications Manager 系统性能。计数器衡量系统性能的各个方面。计数器衡量统计数据，例如已注册电话的数量、尝试的呼叫数以及正在进行的呼叫数。
警报	管理员使用警报来获取 Unified Communications Manager 系统的运行时状态和状况。警报包含关于系统问题的相关信息，例如说明和建议的操作。 管理员可以在警报定义数据库中搜索警报信息。警报定义包含警报和建议操作的说明。
跟踪	管理员和 Cisco 工程师会使用跟踪文件获取有关 Unified Communications Manager 服务问题的特定信息。Cisco Unified 功能配置 会将配置的跟踪信息发送到跟踪日志文件。有两种类型的跟踪日志文件：SDI 和 SDL。 每个服务包含一个默认的跟踪日志文件。系统会跟踪来自服务的系统诊断接口 (SDI) 信息，并将运行时事件和跟踪记录到日志文件。 SDL 跟踪日志文件中包含来自 Cisco CallManager 和 Cisco CTIManager 等服务的呼叫处理信息。系统会跟踪呼叫的信号分布层 (SDL)，并将状态转换记录到日志文件中。 **注释** 大多数情况下，仅当 Cisco 技术支持中心 (TAC) 要求时，才需收集 SDL 跟踪。
质量报告工具	此术语表示 Cisco Unified 功能配置 中的语音质量和一般问题报告实用程序。
可维护性连接器	Cisco Webex Serviceability 服务可加快 Cisco 技术支持人员诊断基础设施问题的速度。它可以自动查找、检索诊断日志和信息并将其存储到 SR 案例中。该服务还会根据诊断签名触发分析，以便 TAC 能够更有效地识别和解决本地设备问题。

命令行界面

使用命令行界面 (CLI) 访问 Unified Communications Manager 系统以进行基本维护和故障恢复。通过硬连线的终端（系统显示器和键盘）或执行 SSH 会话来获取对系统的访问。

安装时会创建帐户名和密码。安装后可以更改密码，但无法更改帐户名。

命令代表使系统执行某些功能的文本指令。命令可以是独立的，也可以有必选或可选的参数或选项。

一个级别包括一组命令；例如，show 指定一个级别，而 show status 指定一个命令。每个级别和命令还包含关联的权限级别。只有当您拥有足够的权限级别时，才能执行命令。

有关 Unified Communications Manager CLI 命令集的完整信息，请参阅《*Cisco Unified* 解决方案的命令行界面参考指南》。

内核转储实用程序

内核转储实用程序允许您在受影响的机器本地收集崩溃转储日志，而无需使用辅助服务器。

在 Unified Communications Manager 群集中，您只需确保在服务器上启用内核转储实用程序，就可以收集崩溃转储信息。

注释 Cisco 建议您在安装 Unified Communications Manager 后验证内核转储实用程序是否已启用，以便更有效地进行故障诊断。如果还没有这样做，请先启用内核转储实用程序，然后再从支持的设备发行版升级 Unified Communications Manager。

重要事项 启用或禁用内核转储实用程序将要求重新启动节点。除非您在可接受重新启动的时间窗内，否则不要执行启用命令。

Cisco Unified Communications 操作系统的命令行界面 (CLI) 可用于启用、禁用或检查内核转储实用程序的状态。

请按以下程序启用内核转储实用程序：

处理通过实用程序收集的文件

要从内核转储实用程序查看崩溃信息，请使用 *Cisco Unified* 实时监控工具或命令行界面 (CLI)。要使用 *Cisco Unified* 实时监控工具收集内核转储日志，请从“跟踪和日志中心”选择“收集文件”选项。从“选择系统服务/应用程序”选项卡，选中“内核转储日志”复选框。有关使用 *Cisco Unified* 实时监控工具收集文件的详细信息，请参阅《*Cisco Unified* 实时监控工具管理指南》。

要使用 CLI 收集内核转储日志，请在崩溃目录中的文件上使用 “file” CLI 命令。这些文件在“activelog” 分区下。日志文件名以内核转储客户端的 IP 地址开头，以文件的创建日期结尾。有关文件命令的详细信息，请参阅《*Cisco Unified* 解决方案的命令行界面参考指南》。

启用内核转储实用程序

此程序用于启用内核转储实用程序。在发生内核崩溃时，该实用程序提供崩溃收集和转储机制。您可以将该实用程序配置为将日志转储到本地服务器或外部服务器。

过程

步骤 1 登录到命令行界面。

步骤 2 完成以下任一操作：

- 要转储本地服务器上的内核崩溃，请运行 `utils os kernelcrash enable` CLI 命令。
- 要将内核崩溃转储到外部服务器，请使用外部服务器的 IP 地址运行 `utils os kerneldump ssh enable <ip_address>` CLI 命令。

步骤 3 重新启动服务器。

示例

注释 如果需要禁用内核转储实用程序，可以运行 `utils os kernelcrash disable` CLI 命令禁用内核转储的本地服务器，运行 `utils os kerneldump ssh disable <ip_address>` CLI 命令禁用外部服务器上的实用程序。

下一步做什么

在实时监控工具中配置电子邮件警告，以通知内核转储信息。有关详细信息，请参阅为核心转储启用电子邮件警报

有关内核转储实用程序和故障诊断的详细信息，请参阅《*Cisco Unified Communications Manager* 故障诊断指南》。

为核心转储启用电子邮件警报

此程序用于配置实时监视工具，以在发生核心转储时向管理员发送电子邮件。

过程

步骤 1 选择**系统** > **工具** > **警告** > **警告中心**。

步骤 2 右键单击 **CoreDumpFileFound** 警告，然后选择**设置警告属性**。

步骤 3 按照向导提示设置您的首选条件：

a) 在**警告属性：电子邮件通知**弹出窗口中，确保选中**启用电子邮件**，然后单击**配置**以设置默认警告操作，这将是发送给管理员的电子邮件。

b) 按照提示进行操作，**添加**收件人电子邮件地址。触发此警告时，默认操作是向此邮箱发送电子邮件。

c) 单击**保存**。

步骤 4 设置默认的电子邮件服务器。

a) 选择**系统** > **工具** > **警告** > **配置电子邮件服务器**。
b) 输入电子邮件服务器设置。
c) 单击**确定**。

网络管理

使用网络管理工具来实现 Unified Communications Manager 的远程功能维护。

- 系统日志管理
- Cisco Discovery Protocol 支持
- 简单网络管理协议支持

有关详细信息，请参阅这些网络管理工具的对应章节提供的 URL 上的文档。

系统日志管理

尽管适用于其他网络管理系统，但与资源管理器基础版 (RME) 打包在一起的 Cisco 系统日志分析提供了管理来自 Cisco 设备的系统日志消息的最佳方法。

Cisco 系统日志分析器是 Cisco 系统日志分析组件，为多个应用程序提供通用的系统日志存储和分析。另一个主要组件系统日志分析器收集器会从 Unified Communications Manager 服务器收集日志消息。

这两个 Cisco 应用程序协同工作，以提供集中的 Cisco Unified Communications 解决方案系统日志记录服务。

请访问以下 URL 参阅 RME 文档：
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml

Cisco Discovery Protocol 支持

Cisco Discovery Protocol 支持可用于寻找 Unified Communications Manager 服务器并管理这些服务器。

请访问以下 URL 参阅 RME 文档：
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml

简单网络管理协议支持

网络管理系统 (NMS) 使用行业标准接口 SNMP 在网络设备之间交换管理信息。作为 TCP/IP 协议组的一部分，SNMP 可让管理员远程管理网络性能、查找并解决网络问题，以及计划网络增长。

SNMP 管理的网络包含三个关键组件：受管设备、代理和网络管理系统。

- 受管设备会指定包含 SNMP 代理并驻留在受管网络上的网络节点。受管设备使用 SNMP 来收集和存储管理信息并使其可用。
- 代理（作为网络管理软件）驻留在受管设备上。代理包含有关管理信息的本地知识，并将其转换为与 SNMP 兼容的形式。
- 网络管理系统包含一个SNMP管理应用程序以及运行它的计算机。NMS执行监控和控制受管设备的应用程序。NMS 提供管理网络所需的大量处理和内存资源。以下 NMS 与 Unified Communications Manager 共享兼容性：
  - CiscoWorks 通用服务软件
  - HP OpenView
  - 支持 SNMP 和 Unified Communications Manager SNMP 接口的第三方应用程序

嗅探器跟踪

通常，您可以通过在配置为跨越包含故障信息的 VLAN 或端口（CatOS、Cat6K-IOS、XL-IOS）的 Catalyst 端口上连接便携式计算机或其他装有嗅探器的设备，以收集嗅探器跟踪。如果没有可用端口，请在交换机和设备之间插入的集线器上连接装有嗅探器的设备。

提示 为了便于 TAC 工程师读取和解读跟踪，Cisco 建议使用嗅探 Sniffer Pro 软件，因为它在 TAC 内广泛使用。

提供涉及到的所有设备（如 IP 电话、网关、Unified Communications Manager 等）的 IP/MAC 地址。

调试

debug 权限 EXEC 命令的输出提供与协议状态和网络活动相关的各种互联网络事件的相关诊断信息。

设置您的终端仿真器软件（如HyperTerminal），以使其能够将调试输出捕获到文件。在HyperTerminal中，单击**转接**； 然后单击**捕获文本**并选择适当的选项。

在运行任何 IOS 语音网关调试之前，请确保在网关上全局配置**服务时间戳调试日期时间毫秒**。

注释 避免工作时间内在现场环境中收集调试信息。

最好在非工作时间收集。如果必须在现场环境中收集调试，请配置**无日志记录控制台**和**缓冲日志记录**。要收集调试，请使用**显示日志**。

由于有些调试可能很长，请直接在控制台端口（默认的**日志记录控制台**）或缓冲区（**记录缓冲区** ）中收集。通过 Telnet 会话收集调试可能会影响设备性能，并且收集的调试可能不完整，导致您必须重新收集。

要停止调试，请使用 **no debug all** 或 **undebug all** 命令。验证是否已使用 **show debug** 命令关闭调试功能。

Cisco Secure Telnet

Cisco Secure Telnet 允许 Cisco 服务工程师 (CSE) 透明防火墙访问站点上的 Unified Communications Manager 节点。使用强加密时，*Cisco Secure Telnet* 使得来自 Cisco Systems 的特殊 Telnet 客户端能够连接到防火墙背后的 Telnet 守护程序。借助此安全连接，您可以远程监控和排查 Unified Communications Manager 节点，而无需修改防火墙。

注释 Cisco 仅在您许可的情况下提供此服务。您必须确保站点上的网络管理员有空，以帮助启动此过程。

信息包捕获

本节包含有关数据包捕获的信息。

相关主题

数据包捕获概述 ， 第 7 页
数据包捕获的配置核对表 ， 第 8 页
将最终用户添加到标准数据包嗅探器访问控制组 ， 第 8 页
配置数据包捕获服务参数 ， 第 9 页
在电话配置窗口中配置数据包捕获 ， 第 10 页
在网关和干线配置窗口中配置数据包捕获 ， 第 10 页
数据包捕获配置设置 ， 第 12 页
分析捕获的数据包 ， 第 13 页

数据包捕获概述

由于启用加密后，监听媒体和 TCP 数据包的第三方故障诊断工具无法正常工作，因此如果发生问题，必须使用 Unified Communications Manager 执行以下任务：

- 分析 Unified Communications Manager 和设备 [Cisco Unified IP 电话（SIP 和 SCCP）、Cisco IOS MGCP 网关、H.323 网关、H.323/H.245/H.225 干线或 SIP 干线] 之间交换的消息的数据包。
- 捕获设备之间的安全实时协议 (SRTP) 数据包。
- 从消息中提取媒体加密密钥材料，然后在设备之间解密媒体。

提示 同时对多个设备执行此任务可能会导致 CPU 使用率过高和呼叫处理中断。Cisco 强烈建议您在可以最大限度减少呼叫处理中断时执行此任务。

有关详细信息，请参阅Cisco Unified Communications Manager 安全指南。

数据包捕获的配置核对表

提取和分析相关数据包括执行以下任务。

程序

1. 将最终用户添加到标准数据包嗅探器用户组。
2. 在 Cisco Unified Communications Manager 管理 的“服务参数配置”窗口中配置数据包捕获服务参数；例如，配置“启用数据包捕获”服务参数。
3. 在电话或网关或“干线配置”窗口中，按设备配置数据包捕获设置。

   注释 Cisco 强烈建议不要同时为多个设备启用数据包捕获，因为此任务可能会导致网络中 CPU 使用率过高。
4. 在受影响的设备之间使用嗅探器跟踪捕获 SRTP 数据包。请参考您的嗅探器跟踪工具的支持文档。
5. 捕获数据包后，将“启用数据包捕获”服务参数设置为 False。
6. 收集分析数据包所需的文件。
7. Cisco 技术支持中心 (TAC) 会分析数据包。请直接联系 TAC 执行此任务。

相关主题

将最终用户添加到标准数据包嗅探器访问控制组 ，第 8 页
分析捕获的数据包，第 13 页
在网关和干线配置窗口中配置数据包捕获，第 10 页
在电话配置窗口中配置数据包捕获，第 10 页
配置数据包捕获服务参数，第 9 页
数据包捕获配置设置，第 12 页

将最终用户添加到标准数据包嗅探器访问控制组

属于标准数据包嗅探器用户组的最终用户可以为支持数据包捕获的设备配置“数据包捕获模式”和“数据包捕获持续时间”设置。如果用户在标准数据包访问控制组中不存在，用户将无法发起数据包捕获。

以下程序介绍了如何将最终用户添加到标准数据包嗅探器访问控制组，其假设您已如 Cisco Unified Communications Manager 管理指南中所述在 Cisco Unified Communications Manager 管理中配置了最终用户。

程序

1. 如Cisco Unified Communications Manager 管理指南中所述查找访问控制组。
2. 在“查找/列出”窗口显示后，单击**标准数据包嗅探器用户**链接。
3. 单击**将用户添加到组**按钮。
4. 如Cisco Unified Communications Manager 管理指南中所述添加最终用户。
5. 添加用户后，单击**保存**。

配置数据包捕获服务参数

要配置用于数据包捕获的参数，请执行以下程序：

程序

1. 在 Unified Communications Manager 中，选择**系统** > **服务参数**。
2. 从“服务器”下拉列表框中，选择您激活 Cisco CallManager 服务的活动服务器。
3. 从“服务”下拉列表框中，选择 **Cisco CallManager**（**活动**）服务。
4. 滚动到“TLS 数据包捕获配置”窗格并配置数据包捕获设置。

提示 有关服务参数的信息，请单击参数名称或窗口中的问号。

注释 要捕获数据包，必须将“启用数据包捕获”服务参数设置为 True。

5. 要让更改生效，请单击**保存**。
6. 您可以继续配置数据包捕获。

相关主题

在网关和干线配置窗口中配置数据包捕获，第 10 页
在电话配置窗口中配置数据包捕获，第 10 页

在电话配置窗口中配置数据包捕获

在“服务参数”窗口中启用数据包捕获后，您可以在 Cisco Unified Communications Manager 管理 的“电话配置”窗口中按设备配置数据包捕获。

您可以按电话启用或禁用数据包捕获。数据包捕获的默认设置为“无”。

注意 Cisco 强烈建议不要同时为多部电话启用数据包捕获，因为此任务可能会导致网络中 CPU 使用率过高。

如果不想捕获数据包，或者如果已经完成任务，请将“启用数据包捕获”服务参数设置为 False。

要配置电话的数据包捕获，请执行以下程序：

程序

1. 在配置数据包捕获设置之前，请参阅与数据包捕获配置相关的主题。
2. 如Cisco Unified Communications Manager 系统配置指南中所述查找 SIP 或 SCCP 电话。
3. 如数据包捕获配置设置中所述，在“电话配置”窗口显示后，配置故障诊断设置。
4. 完成配置后，单击**保存**。
5. 在“重置”对话框中单击**确定**。

提示 尽管 Cisco Unified Communications Manager 管理提示重置设备，您无需重置设备以捕获数据包。

其他步骤

在受影响的设备之间使用嗅探器跟踪捕获 SRTP 数据包。

捕获数据包后，将“启用数据包捕获”服务参数设置为 False。

相关主题

分析捕获的数据包 ，第 13 页
数据包捕获的配置核对表 ，第 8 页

在网关和干线配置窗口中配置数据包捕获

以下网关和干线支持 Unified Communications Manager 中的数据包捕获。

- Cisco IOS MGCP 网关
- H.323 网关

- H.323/H.245/H.225 干线
- SIP 干线

提示 Cisco 强烈建议不要同时为多个设备启用数据包捕获，因为此任务可能会导致网络中 CPU 使用率过高。

如果不想捕获数据包，或者如果已经完成任务，请将“启用数据包捕获”服务参数设置为 False。

要在“网关”或“干线配置”窗口中配置数据包捕获设置，请执行以下程序：

程序

1. 在配置数据包捕获设置之前，请参阅与数据包捕获配置相关的主题。
2. 请执行以下任务之一：
   - 如 Cisco Unified Communications Manager 系统配置指南中所述查找 Cisco IOS MGCP 网关。
   - 如 Cisco Unified Communications Manager 系统配置指南中所述查找 H.323 网关。
   - 如 Cisco Unified Communications Manager 系统配置指南中所述查找 H.323/H.245/H.225 干线。
   - 如 Cisco Unified Communications Manager 系统配置指南中所述查找 SIP 干线。
3. 配置窗口显示后，找到“数据包捕获模式”和“数据包捕获持续时间”设置。

   提示 如果您找到 Cisco IOS MGCP 网关，请确保如 Cisco Unified Communications Manager 管理指南中所述配置了 Cisco IOS MGCP 网关的端口。Cisco IOS MGCP 网关的数据包捕获设置在终端标识符的“网关配置”窗口中显示。要访问此窗口，请单击语音接口卡的终端标识符。
4. 如数据包捕获配置设置中所述配置故障诊断设置。
5. 配置数据包捕获设置后，单击**保存**。
6. 在“重置”对话框中单击**确定**。

   提示 尽管 Cisco Unified Communications Manager 管理提示重置设备，您无需重置设备以捕获数据包。

其他步骤

在受影响的设备之间使用嗅探器跟踪捕获 SRTP 数据包。

捕获数据包后，将“启用数据包捕获”服务参数设置为 False。

相关主题

分析捕获的数据包，第 13 页
数据包捕获的配置核对表，第 8 页

数据包捕获配置设置

下表介绍了配置网关、干线和电话的数据包捕获时“数据包捕获模式”和“数据包捕获持续时间”设置。

设置	说明
数据包捕获模式	此设置仅用于对加密问题进行故障诊断；数据包捕获可能会导致CPU使用率较高或呼叫处理中断现象增多。从下拉列表框中选择以下选项之一： • **无**—此选项是默认设置，表示没有发生数据包捕获。完成数据包捕获后，Unified Communications Manager 会将“数据包捕获模式”设置为“无”。 • **批处理模式**— Unified Communications Manager 将解密或非加密的消息写入文件，系统对每个文件进行加密。系统每天都会使用新的加密密钥创建一个新文件。用于将文件存储七天的 Unified Communications Manager 还会将用于加密文件的密钥存储在安全的位置。Unified Communications Manager 会将文件存储在 PktCap 虚拟目录中。单个文件中包含时间戳、源 IP 地址、源 IP 端口、目标 IP 地址、数据包协议、消息长度和消息。TAC 调试工具使用 HTTPS、管理员用户名和密码以及指定的一天来请求包含所捕获数据包的单个加密文件。同样，该工具还会请求用于对加密文件进行解密的密钥信息。 **提示** 在联系 TAC 之前，必须使用受影响设备之间的探查器跟踪捕获 SRTP 数据包。

设置	说明
数据包捕获持续时间	此设置仅用于对加密问题进行故障诊断；数据包捕获可能会导致CPU 使用率较高或呼叫处理中断现象增多。 此字段指定了为一个数据包捕获会话分配的以分钟为单位的最长时间。默认设置等于 0，可设置范围为 0 到 300 分钟。 要启动数据包捕获，请在此字段中输入非 0 的值。数据包捕获完成后，显示值 0。

相关主题

在网关和干线配置窗口中配置数据包捕获，第 10 页
在电话配置窗口中配置数据包捕获，第 10 页

分析捕获的数据包

Cisco 技术支持中心 (TAC) 使用调试工具分析数据包。在联系 TAC 之前，请在受影响的设备之间使用嗅探器跟踪捕获 SRTP 数据包。收集以下信息后直接联系 TAC：

- 数据包捕获文件—**https://<IP address or server name>/pktCap/pktCap.jsp?file=mm-dd-yyyy.pkt**，您可以浏览到服务器并按月、日和年 (mm-dd-yyyy) 查找数据包捕获文件
- 文件的密钥—**https://<IP address or server name>/pktCap/pktCap.jsp?key=mm-dd-yyyy.pkt**，您可以浏览到服务器并按月、日和年 (mm-dd-yyyy) 查找密钥
- 属于标准数据包嗅探器用户组的最终用户的用户名和密码

有关详细信息，请参阅：Cisco Unified Communications Manager 安全指南。

常见故障诊断任务、工具和命令

本节提供命令和实用程序的快速参考，帮助您在 Unified Communications Manager 根访问权限被禁用的情况下对服务器进行故障诊断。下表提供 CLI 命令和 GUI 选项的摘要，您可以使用它们来收集信息以对各种系统问题进行故障诊断。

表 *2: CLI* 命令和 *GUI* 选项摘要

信息	**Linux** 命令	功能配置 **GUI** 工具	**CLI** 命令
CPU 使用率	上	RTMT 转到“查看”选项卡，然后选择**服务器** > **CPU 和内存**	处理器 CPU 使用情况： show perf query class Processor 所有进程的进程 CPU 使用情况： show perf query counter Process “% CPU Time” Individual process counter details (including CPU usage) show perf query instance <Process task_name>
进程状态	ps	RTMT 转到“查看”选项卡，然后选择**服务器** > **进程**	show perf query counter Process “Process Status”
磁盘使用情况	df/du	RTMT 转到“查看”选项卡，然后选择**服务器** > **磁盘使用情况**	show perf query counter Partition “% Used” or show perf query class Partition
内存	可用	RTMT 转到“查看”选项卡，然后选择**服务器** > **CPU 和内存**	show perf query class Memory
网络状态	netstats		show network status
重新启动服务器	reboot	登录到服务器上的“平台”网页 转到**服务器** > **当前版本**	utils system restart
收集跟踪/日志	Sftp、ftp	RTMT 转到“工具”选项卡，然后选择**跟踪** > **跟踪和日志中心**	列示文件：file list 下载文件：file get 查看文件：file view

下表列出了常见的问题以及可用于对这些问题进行故障诊断的工具。

表 *3:* 使用 *CLI* 命令和 *GUI* 选项对常见问题进行故障诊断

任务	GUI 工具	CLI 命令
访问数据库	无	以管理员身份登录，并使用以下任一 **show** 命令： • show tech database • show tech dbinuse • show tech dbschema • show tech devdefaults • show tech gateway • show tech locales • show tech notify • show tech procedures • show tech routepatterns • show tech routeplan • show tech systables • show tech table • show tech triggers • show tech version • show tech params* 要运行 SQL 命令，请使用 **run** 命令： • run sql <sql command>
释放磁盘空间 **注释** 只能从日志分区中删除文件。	使用 RTMT 客户端应用程序，转至**工具**选项卡，然后选择**跟踪和日志中心** > **收集文件** 。 选择条件以选择要收集的文件，然后选中**删除文件**选项。执行此操作会在文件下载到 PC 后删除 Unified Communications Manager 服务器上的文件。	file delete
查看核心文件	您不能查看核心文件；但可以使用 RTMT 应用程序并选择**跟踪和日志中心** > **收集崩溃转储**来下载核心文件。	utils core [options.]

任务	GUI 工具	CLI 命令
重新启动 Unified Communications Manager 服务器	登录到服务器上的平台并转到**重新启动** > **当前版本**。	utils system restart
更改跟踪的调试级别	在 `https://<server_ipaddress>:8443/ccmservice/` 上登录到 *Cisco Unity Connection* 功能配置管理并选择**跟踪** > **配置**。	set trace enable [Detailed, Significant, Error, Arbitrary, Entry_exit, State_Transition, Special] [syslogmib, cdpmib, dbl, dbnotify]
查看 netstat	无	show network status

故障诊断提示

当您对 Unified Communications Manager 进行故障诊断时，以下提示可能会有所帮助。

提示 查看 Unified Communications Manager 的发行说明，了解已知的问题。发行说明提供了有关已知问题的描述和解决方法。

提示 了解您的设备是在哪里注册的。

每个 Unified Communications Manager 日志会在本地跟踪文件。如果电话或网关已注册到特定的 Unified Communications Manager，且呼叫是在那里发起的，则系统会在该 Unified Communications Manager 上完成呼叫处理。您需要捕获该 Unified Communications Manager 上的跟踪信息，以调试问题。

常见的错误涉及在订阅方服务器上注册设备，但在发布方服务器上捕获跟踪信息。这些跟踪文件将接近空白（并且其中一定不包含呼叫）。

另一个常见问题涉及将设备 1 注册到 CM1，将设备 2 注册 CM2。如果设备 1 呼叫设备 2，呼叫跟踪将在 CM1 中进行；如果设备 2 呼叫设备 1，则跟踪会在 CM2 中进行。如果要对双向呼叫问题进行故障诊断，您需要来自两个 Unified Communications Manager 的跟踪数据，以获取故障诊断所需的所有信息。

提示 知道问题发生的大致时间。

您可能已处理了多个呼叫，因此知道呼叫的大致时间有助于 TAC 快速找出问题。

您可以在活动呼叫期间按 **i** 或 **?** 按键两次，以获取 Cisco Unified IP 电话 79xx 上的电话统计信息。

当运行测试以重现问题和产生信息时，请了解以下数据，这些数据对理解问题至关重要：

- 主叫号码/被叫号码
- 特定情形中涉及到的任何其他号码
- 呼叫的时间

注释 请记住，所有设备的时间同步对故障诊断非常重要。

如果要重现问题，请在文件中查看修改日期和时间戳，确保选择相应时间段的文件。收集正确跟踪数据的最佳方式是：重现问题，然后快速从 Unified Communications Manager 服务器找到最新的文件并复制它。

提示 保存日志文件以防止它们被改写。

一段时间后文件会被改写。知道正在记录哪个文件的唯一方法是在菜单栏中选择**查看** > **刷新**，然后查看文件上的日期和时间。

系统历史记录日志

此系统历史记录日志提供快速概览初始系统安装、系统升级、Cisco Option 安装、DRS 备份和 DRS 恢复以及切换版本和重新启动历史记录的中心位置。

相关主题

系统历史记录日志概述，第 17 页
系统历史记录日志字段，第 18 页
访问系统历史记录日志，第 19 页

系统历史记录日志概述

系统历史记录日志以简单 ASCII 文件 (**system-history.log**) 的形式存在，数据不会在数据库中进行维护。由于其不会变得过大，因此系统历史记录文件不会进行轮换。

系统历史记录日志提供以下功能：

- 记录服务器上的初始软件安装。
- 记录每次软件升级的成功、失败或取消（Cisco Option 文件和修补程序）。
- 记录执行的每次 DRS 备份和恢复。
- 记录通过 CLI 或 GUI 发出的切换版本的每次调用。
- 记录通过 CLI 或 GUI 发出的重新启动和关闭的每次调用。

- 记录系统的每次启动。如果与重新启动或关闭输入无关，则启动是手动重新启动、电源循环或内核崩溃的结果。
- 维护包含系统历史记录（自初始安装起或自功能可用时起）的单一文件。
- 存在于安装文件夹中。您可以通过使用 **file** 命令从 CLI 或从实时监控工具 (RTMT) 访问日志。

系统历史记录日志字段

日志显示包含产品名称、产品版本和内核映像相关信息的通用标头；例如：

==========

产品名称 - Unified Communications Manager

产品版本 - 7.1.0.39000-9023

内核图像 - 2.6.9-67.EL

==========

每个系统历史记录日志条目都包含以下字段：

时间戳 用户 *ID* 操作 说明 开始/结果

系统历史记录日志字段可能包含以下值：

- 时间戳—显示服务器上的本地时间和日期，格式为 *mm/dd/yyyy hh:mm:ss*。
- 用户 *ID*—显示调用操作的用户的用户名。
- 操作—显示以下操作之一：
  - 安装
  - Windows 升级
  - 安装期间升级
  - 升级
  - Cisco Option 安装
  - 切换版本
  - 系统重新启动
  - 关闭
  - 启动
  - DRS 备份
  - DRS 恢复
- 说明—显示以下消息之一：

- 版本：对基本安装、Windows 升级、安装期间升级和升级操作显示。
- *Cisco Option* 文件名：对 Cisco Option 安装操作显示。
- 时间戳：对 DRS 备份和 DRS 恢复操作显示。
- 活动版本到非活动版本：对切换版本操作显示。
- 活动版本：对系统重新启动、关闭和启动操作显示。

- 结果—显示以下结果：
  - 开始
  - 成功或失败
  - 取消

以下所示为系统历史记录日志的示例。

```
admin:file dump install system-history.log=======================================
 Product Name - Cisco Unified Communications Manager Product Version -
6.1.2.9901-117 Kernel Image - 2.4.21-47.EL.cs.3BOOT
======================================== 07/25/2008 14:20:06 | root: Install
6.1.2.9901-117 Start 07/25/2008 15:05:37 | root: Install 6.1.2.9901-117 Success
07/25/2008 15:05:38 | root: Boot 6.1.2.9901-117 Start 07/30/2008 10:08:56 | root:
 Upgrade 6.1.2.9901-126 Start 07/30/2008 10:46:31 | root: Upgrade 6.1.2.9901-126
 Success 07/30/2008 10:46:43 | root: Switch Version 6.1.2.9901-117 to
6.1.2.9901-126 Start 07/30/2008 10:48:39 | root: Switch Version 6.1.2.9901-117
to 6.1.2.9901-126 Success 07/30/2008 10:48:39 | root: Restart 6.1.2.9901-126 Start
 07/30/2008 10:51:27 | root: Boot 6.1.2.9901-126 Start 08/01/2008 16:29:31 | root:
 Restart 6.1.2.9901-126 Start 08/01/2008 16:32:31 | root: Boot 6.1.2.9901-126
Start
```

访问系统历史记录日志

您可以使用 CLI 或 RTMT 访问系统历史记录日志。

使用 CLI

您可以使用 CLI **file** 命令访问系统历史记录日志；例如：

- **file view install system-history.log**
- **file get install system-history.log**

有关 CLI **file** 命令的详细信息，请参阅《*Cisco Unified* 解决方案的命令行界面参考指南》。

使用 RTMT

您也可以使用 RTMT 访问系统历史记录日志。从“跟踪和日志中心”选项卡，单击**收集安装日志**。

有关使用 RTMT 的详细信息，请参阅《*Cisco Unified* 实时监控工具管理指南》。

审核日志记录

集中的审核日志记录可确保对 Unified Communications Manager 系统的配置更改记录在单独的日志文件中进行审计。审计事件表示需要进行记录的任何事件。以下 Unified Communications Manager 系统组件会生成审计事件：

- Cisco Unified Communications Manager 管理
- Cisco Unified 功能配置
- *Unified Communications Manager CDR* 分析和报告
- *Cisco Unified* 实时监控工具
- *Cisco Unified Communications* 操作系统
- 灾难恢复系统
- 数据库
- 命令行界面
- 启用远程支持帐户（由技术支持团队发出 CLI 命令）

在 *Cisco Business Edition 5000* 中，以下 Cisco Unity Connection 组件也会生成审计事件：

- Cisco Unity Connection 管理
- *Cisco Personal Communications Assistant* (Cisco PCA)
- Cisco Unity Connection 功能配置
- Cisco Unity Connection 使用具象状态传输 (REST) API 的客户端

以下示例显示示例审核事件：

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:Successful
 Description: Call Manager Service status is stopped App ID:Cisco Tomcat Cluster
 ID:StandAloneCluster Node ID:sa-cm1-3
```

审核日志，其中包含关于审计事件的信息，将在公共分区中写入。日志分区监控 (LPM) 管理根据需要清除这些审核日志，与跟踪文件类似。默认情况下，LPM 会清除审核日志，但审计用户可以在 Cisco Unified 功能配置 的“审计用户配置”窗口更改此设置。LPM 在公共分区磁盘使用率超出阈值时发送一条警告；但由于审核日志或跟踪文件，该警告没有关于磁盘是否已满的信息。

提示 Cisco Audit Event 服务是一项支持审核日志记录的网络服务，在 Cisco Unified 功能配置 的“控制中心”-“网络服务”中显示。如果审核日志未写入，则在 Cisco Unified 功能配置 中选择**工具** > **控制中心—网络服务**以停止并启动此服务。

系统将从 *Cisco Unified* 实时监控工具中的“跟踪和日志中心”收集、查看和删除所有审核日志。访问 RTMT 的“跟踪和日志中心”内的审核日志。转至**系统** > **实时跟踪** > **审核日志** > **节点**。选择节点后，另一个窗口将显示**系统** > **Cisco 审核日志**。

RTMT 中显示以下类型的审核日志：

- 应用程序日志
- 数据库日志
- 操作系统日志
- 远程 SupportAccEnabled 日志

应用程序日志

显示在 RTMT 的 AuditApp 文件夹中的应用程序审核日志提供 Cisco Unified Communications Manager 管理、Cisco Unified 功能配置、*CLI*、*Cisco Unified* 实时监控工具 (RTMT)、灾难恢复系统以及 Cisco Unified CDR 分析和报告 (CAR) 的配置更改。对于 *Cisco Business Edition 5000*，应用程序审核日志还会记录 Cisco Unity Connection 管理、*Cisco Personal Communications Assistant* (Cisco PCA)、Cisco Unity Connection 功能配置以及使用具象状态传输 (REST) API 的客户端的更改。

虽然应用程序日志默认保持启用状态，您可以选择**工具** > **审核日志配置**以在 Cisco Unified 功能配置中对其进行配置。有关可以为审核日志配置的设置的说明，请参阅《*Cisco Unified* 功能配置管理指南》。

如果审核日志在 Cisco Unified 功能配置 中被禁用，则不会生成新的审核日志文件。

提示 只有拥有审核角色的用户才有权限更改审核日志设置。默认情况下，在全新安装和升级后，CCMAdministrator 拥有审核角色。CCMAdministrator 可以将“标准审核用户”组分配给 CCMAdministrator 专门为审核目的而创建的新用户。然后，可以将 CCMAdministrator 从审核用户组中删除。“标准审核日志配置”角色能够删除审核日志以及读取/更新对于 *Cisco Unified* 实时监控工具、跟踪收集工具、RTMT 警告配置、“控制中心 - 网络服务”窗口、RTMT 配置文件保存、“审核配置”窗口以及称为审核跟踪的新资源的访问。对于 *Cisco Business Edition 5000* 中的 Cisco Unity Connection，在安装过程中创建的应用程序管理帐户具有审核管理员角色，并可以分配其他管理用户到该角色。

Unified Communications Manager 创建一个应用程序审核日志文件，直到其达到配置的最大文件大小；然后，它将关闭并创建新的应用程序审核日志文件。如果系统指定轮换日志文件，Unified Communications Manager 将保存配置数量的文件。一些日志记录事件可使用 RTMT SyslogViewer 进行查看。

系统会记录 Cisco Unified Communications Manager 管理 的以下事件：

- 用户登录（用户登录和用户注销）。
- 用户角色成员资格更新（添加用户、删除用户、更新用户角色）。
- 角色更新（添加、删除或更新新角色）。

- 设备更新（电话和网关）。
- 服务器配置更新（更改警报或跟踪配置、服务参数、企业参数、IP 地址、主机名、以太网设置和 Unified Communications Manager 服务器添加或删除）。

系统会记录 Cisco Unified 功能配置 的以下事件：

- 从任何“功能配置”窗口激活、停用、启动或停止服务。
- 跟踪配置和警报配置更改。
- SNMP 配置更改。
- CDR 管理中的更改。
- 查看功能配置报告存档中的任何报告。在报告器节点上查看此日志。

RTMT 记录以下事件及审计事件警报：

- 警告配置。
- 警告暂停。
- 电子邮件配置。
- 设置节点警告状态。
- 警告添加。
- 添加警告操作。
- 清除警告。
- 启用警告。
- 删除警告操作。
- 删除警告。

系统会记录 *Unified Communications Manager CDR* 分析和报告的以下事件：

- 安排 CDR 加载程序。
- 安排每日、每周和每月用户报告、系统报告和设备报告。
- 邮件参数配置。
- 拨号方案配置。
- 网关配置。
- 系统首选项配置。
- 自动清除配置。
- 持续时间、一天中的时间和语音质量的评级引擎配置。

- QoS 配置。
- 预生成报告配置的自动生成/警告。
- 通知限制配置。

系统会记录灾难恢复系统的以下事件：

- 启动成功/失败的备份
- 启动成功/失败的恢复
- 取消成功的备份
- 成功/未成功完成的备份
- 成功/未成功完成的恢复
- 保存/更新/删除/启用/禁用备份计划
- 保存/更新/删除目标设备以进行备份

对于 *Cisco Business Edition 5000*，Cisco Unity Connection 管理会记录以下事件：

- 用户登录（用户登录和用户注销）。
- 所有配置更改，包括但不限于用户、联系人、呼叫管理对象、网络、系统设置和电话。
- 任务管理（启用或禁用任务）。
- 批量管理工具（批量创建、批量删除）。
- 自定义键盘映射（映射更新）

对于 *Cisco Business Edition 5000*，Cisco PCA 会记录以下事件：

- 用户登录（用户登录和用户注销）。
- 通过 Messaging Assistant 进行的所有配置更改。

对于 *Cisco Business Edition 5000*，Cisco Unity Connection 功能配置会记录以下事件：

- 用户登录（用户登录和用户注销）。
- 所有配置更改。
- 激活、停用、启动或停止服务。

对于 *Cisco Business Edition 5000*，使用 REST API 记录以下事件的客户端：

- 用户日志记录（用户 API 身份验证）。
- 使用 Cisco Unity Connection 预配置接口 (CUPI) 的 API 呼叫。

数据库日志

RTMT 的 informix 文件夹中的数据库审核日志会报告数据库更改。此日志默认不启用，可以选择**工具** > **审核日志配置**在 Cisco Unified 功能配置 中配置。有关可以为审核日志配置的设置的说明，请参阅Cisco Unified 功能配置。

此审核不同于应用程序审核，因为其记录数据库更改，应用程序审核日志则记录应用程序配置更改。除非在 Cisco Unified 功能配置 中启用数据库审核，否则 informix 文件夹不会在 RTMT 中显示。

操作系统日志

操作系统审核日志在 RTMT 的 vos 文件夹中显示，报告操作系统所触发的事件。该功能在默认情况下未启用。**utils auditd** CLI 命令将启用、禁用或指定事件的相关状态。

除非在 CLI 中启用审计，否则 vos 文件夹不会在 RTMT 中显示。

有关 CLI 的信息，请参阅《*Cisco Unified* 解决方案的命令行界面参考指南》。

远程支持帐户启用的日志

远程支持帐户启用的审核日志在 RTMT 的 vos 文件夹中显示，报告由技术支持团队发出的 CLI 命令。您无法对其进行配置，并且仅当技术支持团队启用远程支持帐户时创建日志。

验证 Cisco Unified Communications Manager 服务正在运行

遵照以下程序验证哪些 Cisco CallManager 服务在服务器上处于活动状态。

程序

1. 从 Cisco Unified Communications Manager 管理 中，选择**导航** > **Cisco Unified 功能配置**。
2. 选择**工具** > **服务启动**。
3. 从“服务器”列中，选择所需的服务器。

   您选择的服务器将会显示在当前服务器标题旁边，并且会显示一系列带已配置服务的框。

   “激活状态”列的 Cisco CallManager 行中会显示“已激活”或“已禁用”。

   如果显示的状态为**已激活**，指定的 Cisco CallManager 服务在所选服务器上将保持活动状态。

   如果显示的状态为**已禁用**，请继续执行以下步骤。
4. 选中所需 Cisco CallManager 服务的复选框。
5. 单击**更新**按钮。

   “激活状态”列在指定的 Cisco CallManager 服务行中显示**已激活**。

   指定的服务现在会显示所选服务器为活动状态。

如果 Cisco CallManager 服务已激活并且您想要验证服务当前是否正在运行，请执行以下程序。

程序

1. 从 Cisco Unified Communications Manager 管理 中，选择**导航** > **Cisco Unified 功能配置**。
   此时将显示 Cisco Unified 功能配置窗口。
2. 选择**工具** > **控制中心 - 功能服务**。
3. 从“服务器”列中选择服务器。
   您选择的服务器将会显示在当前服务器标题旁边，并且会显示一个带已配置服务的框。
   “状态”列将显示所选服务器正在运行的服务。