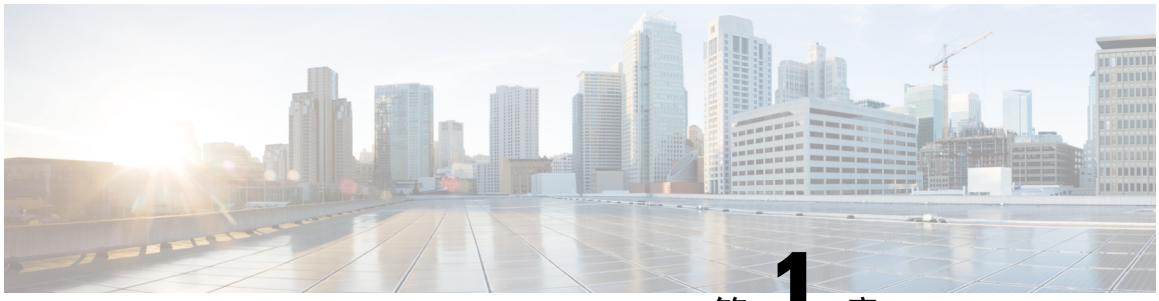
Cisco Unified Communications Manager 管理指南，发行版 15

首次发布日期: 2023 年 12 月 18 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

目录



第 1 章

新增和变更内容

新增和变更内容

下表概述本指南中对此最新版本及之前版本的重大功能更改。 下表未提供对此版本及之前版本的指南或新功能进行的所有更改的详尽列表。

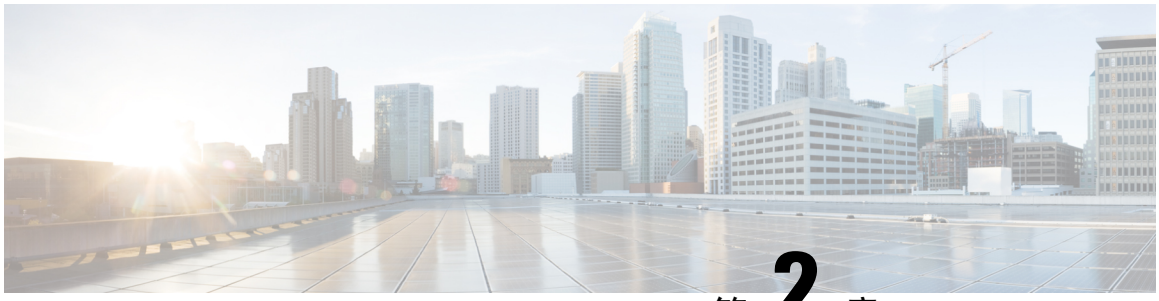
表 *1: Unified Communications Manager* 和 *IM and Presence* 服务中的新增功能和更改的行为

	说明	请参阅
2023 年 12 月 18 日	在“管理 IPsec 策略”部分中新增了 IPsec 策略的注释。	管理 IPsec 策略， 第 345 页
2023 年 12 月 18 日	在“Cisco Unified 功能配置故障排除工具”部分中新增了 .gzo 文件的注释。	Cisco Unified 功能配置故障诊断工具， 第 441 页

新增和变更内容

第 I 部分

管理概述



第 2 章

管理概述

Cisco Unified CM 管理概述

Cisco Unified CM 管理是一个基于 Web 的应用程序，是 Cisco Unified Communications Manager 的主要管理和配置界面。 您可以使用 Cisco Unified CM 管理为您的系统配置广泛的项目，包括一般系统组件、功能、服务器设置，呼叫路由规则、电话、最终用户，以及媒体资源。

配置菜单

Cisco Unified CM 管理的配置窗口组织于以下菜单下：

- 系统—使用此菜单下的配置窗口配置常规系统设置，例如服务器信息、NTP 设置、日期和时间组、区域、DHCP、LDAP 集成，以及企业参数。
- 呼叫路由 — 使用此选项卡下的配置窗口配置有关 Cisco Unified Communications Manager 如何路由呼叫的项目，包括路由模式、路由组、寻线引导、拨号规则、分区、呼叫搜索空间、目录号码，以及转换模式。
- 媒体资源 — 使用此选项卡下的配置窗口配置媒体资源组、会议桥、报警器和代码转换器等项目。
- 高级功能—使用此选项卡下的配置窗口配置诸如语音邮件引导、留言通知以及呼叫控制坐席配置文件等功能。
- 设备—使用此选项卡下的配置窗口设置设备，例如电话、IP 电话服务、干线、网关、软键模板和 SIP 配置文件。

- 应用程序 — 使用此选项卡下的配置窗口下载并安装插件，例如 Cisco Unified JTAPI、Cisco Unified TAPI 和 Cisco Unified 实时监控工具。
- 用户管理—使用“用户管理”选项卡下的配置窗口为您的系统配置最终用户和应用程序用户。
- 批量管理 — 使用批量管理工具一次导入和配置大量最终用户或设备。
- 帮助 — 单击此菜单可访问联机帮助系统。 联机帮助系统包含诸多文档，可帮助您为系统上不同的配置窗口配置设置。

操作系统管理概述

使用“Cisco Unified Communications 操作系统管理”配置和管理您的操作系统并执行以下管理任务：

- 检查软件和硬件状态
- 检查和更新 IP 地址
- Ping 其他网络设备
- 管理 NTP 服务器
- 升级系统软件和选项
- 管理节点安全性，包括 IPsec 和证书
- 管理远程支持帐户
- 重新启动系统

操作系统状态

您可以检查各种操作系统组件的状态，包括以下组件：

- 群集和节点
- 硬件
- 网络
- 系统
- 安装的软件和选项

操作系统设置

您可以查看和更新以下操作系统设置：

- IP — 更新安装应用程序时您输入的 IP 地址和 DHCP 客户端设置。
- NTP 服务器设置 — 配置外部 NTP 服务器的 IP 地址；添加 NTP 服务器。
- SMTP 设置 — 配置操作系统将用来发送电子邮件通知的简单邮件传输协议 (SMTP) 主机。

操作系统安全配置

您可以管理安全证书和 IPsec 设置。从**安全**菜单中，您可以选择以下安全选项：

- 证书管理 — 管理证书和证书签名请求 (CSR)。您可以显示、上传、下载、删除和重新生成证书。通过证书管理，您还可以监控节点上的证书过期时间。

- IPsec 管理 — 显示或更新现有的 IPsec 策略；设置新的 IPsec 策略和关联。

软件升级

您可以升级运行在操作系统上的软件版本，或者安装特定的软件选项，包括 Cisco Unified Communications 操作系统区域设置安装程序、拨号方案，以及 TFTP 服务器文件。

从**安装/升级**菜单选项，您可以从本地磁盘或远程服务器升级系统软件。升级后的软件安装在非活动分区上，然后您可以重新启动系统并切换分区，这样系统就可以在较新的软件版本上运行。有关详细信息，请参阅《*Cisco Unified Communications Manager* 升级指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html。

注释 您必须通过 Cisco Unified Communications 操作系统界面和 CLI 中包含的软件升级功能执行所有的软件安装和升级。系统只能上传和处理 Cisco Systems 认可的软件。您无法安装或使用第三方或基于 Windows 的软件应用程序。

服务

应用程序提供以下操作系统实用程序：

- Ping—检查与其他网络设备的连通性。
- 远程支持—设置一个 Cisco 支持人员可以用来访问系统的帐户。此帐户会在您指定的天数后自动过期。

CLI

您可以从操作系统或通过到服务器的安全外壳连接访问 CLI。有关详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面参考指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

验证的网络时间协议支持

借助 Cisco Unified Communications Manager 发行版 12.0 (1)，支持 Unified Communications Manager 的经验证的网络时间协议 (NTP) 功能。 增加此支持是为了保护 NTP 服务器到 Unified Communications Manager 的连接。 在以前的发行版中，Unified Communications Manager 到 NTP 服务器的连接没有安全保护。

此功能以基于对称密钥的验证为基础，并受 NTPv3 和 NTPv4 服务器支持。 Unified Communications Manager 仅支持基于 SHA1 的加密。 基于 SHA1 的对称密钥支持可从 NTP 版本 4.2.6 或更高版本获得。

- 对称密钥
- 无身份验证

您可以通过 **Cisco Unified 操作系统管理**应用程序的管理 CLI 或 **NTP 服务器列表**页面检查 NTP 服务器的验证状态。

自动密钥验证的网络时间协议支持

Cisco Unified Communications Manager 还支持通过自动秘钥功能验证的网络时间协议 (NTP)（基于公钥基础设施的验证）。 此功能仅在发布方节点上适用。

Redhat 建议通过自动密钥进行对称密钥验证。 有关详细信息，请参阅：https://access.redhat.com/support/cases/#/case/01871532。

添加了此功能，因为基于 PKI 的验证对于通用标准认证是必需的。

仅当您在 Cisco Unified Communication Manager 上启用了通用标准模式时，才可以使用 NTP 服务器上的 IFF 身份方案配置基于 PKI 的验证。

您可以在 Cisco Unified Communications Manager 上启用对称密钥或基于 PKI 的 NTP 验证。

如果您尝试在启用了 PKI 的服务器上启用对称密钥，会显示以下警告消息：

警告 使用自动密钥的 NTP 验证当前已启用，必须将其禁用，才能启用对称密钥。 使用命令 'utils ntp auth auto-key disable' 禁用 NTP 验证，然后重试此命令。

如果您尝试在启用了对称密钥的服务器上启用自动密钥，会显示以下警告消息：

警告 使用对称密钥的 NTP 验证当前已启用，必须将其禁用，才能启用自动密钥。 使用命令 'utils ntp auth symmetric-key disable' 禁用 NTP 验证，然后重试此命令。

注释 NTP 服务器需要 ntp 版本 4 和 rpm 版本 ntp-4.2.6p5-1.el6.x86_64.rpm 及以上版本。

您可以通过“Cisco Unified 操作系统管理”应用程序的管理 CLI 或“NTP 服务器列表”页面检查 NTP 服务器的验证状态。

Cisco Unified 功能配置概述

“Cisco Unified 功能配置”是基于 Web 的故障诊断工具，提供许多服务、警报和协助管理员管理其系统的工具。“Cisco Unified 功能配置”为管理员提供的功能包括：

- 启动和停止服务—管理员可以设置各式各样的服务，以帮助管理员管理其系统。例如，您可以启动 Cisco CallManager 功能配置 RTMT 服务，从而允许管理员使用实时监控工具监控系统的运行状况。

- SNMP — SNMP 便于在网络设备（例如节点、路由器等等）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。
- 警报 — 警报提供有关运行时状态和系统状态的信息，以便您能够对与系统有关的问题进行故障诊断。
- 跟踪 — 跟踪工具可以帮助您排查语音应用程序问题。
- Cisco 功能配置报告程序 — Cisco 功能配置报告程序会在“Cisco Unified 功能配置”中生成每日报告。
- SNMP — SNMP 便于在网络设备（例如节点、路由器等等）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。
- CallHome — 配置 Cisco Unified Communications Manager Call Home 功能，允许 Cisco Unified Communications Manager 与 Smart Call Home 后端服务器通信，并将诊断警告、库存，以及其他消息发送给该服务器

附加管理界面

使用 Cisco Unified 功能配置，您可以启动允许您使用以下附加管理界面的服务：

- 实时监控工具 — “实时监控工具”是一个基于 Web 的界面，可帮助您监控系统的运行状况。使用 RTMT，您可以查看警报、计数器和包含系统运行状况详细信息的报告。
- 被叫号码分析器 —"被叫号码分析器"是一个基于 Web 的界面，可以帮助管理员排查拨号方案问题。
- Cisco Unified CDR 分析和报告 — “CDR 分析和报告”会收集呼叫详细信息记录，显示您系统上发出的呼叫的详细信息。

有关如何使用 Cisco Unified 功能配置的详细信息，请参阅《*Cisco Unified* 功能配置管理指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

Cisco Unified 报告概述

Cisco Unified 报告 Web 应用程序可生成群集数据故障诊断或检查的报告。您可以在 Unified Communications Manager 和 Unified Communications Manager IM and Presence Service 控制台上访问应用程序。

此工具提供了一种简单的方法来大概了解群集数据。该工具可从现有来源收集数据、比较数据，以及报告违规。当您在“Cisco Unified 报告”中生成报告时，报告会将来自一台或多台服务器上的一个或多个来源的数据合并到一个输出视图中。例如，您可以查看以下报告以帮助管理您的系统：

- Unified CM 群集概要 — 查看此报告可大概了解您的群集，包括 Cisco Unified Communications Manager 和 IM and Presence Service 版本、服务器主机名，以及硬件详细信息。

- 电话功能列表 — 如果您要配置功能，可查看此报告。此报告会提供一个哪些电话支持哪些Cisco Unified Communications Manager 功能的列表。
- 没有线路的 Unified CM 电话 — 查看此报告可了解您群集中的哪些电话没有电话线路。

要查看通过“Cisco Unified 报告”提供的报告的完整列表，以及如何使用应用程序的说明，请参阅《*Cisco Unified* 报告管理指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

灾难恢复系统概述

灾难恢复系统 (DRS) 可从 Cisco Unified Communications Manager 管理调用，它提供完整的数据备份和恢复功能。 灾难恢复系统允许您定期执行计划的自动或用户调用的数据备份。

DRS 恢复其自己的设置（备份设备设置和计划设置）作为平台备份/恢复的一部分。 DRS 备份和恢复 `drfDevice.xml` 和 `drfSchedule.xml` 文件。 使用这些文件恢复服务器时，您无需重新配置 DRS 备份设备和计划。

灾难恢复系统包括以下功能：

- 用于执行备份和恢复任务的用户界面。
- 用于执行备份和恢复功能的分布式系统体系结构。
- 计划的备份。
- 将备份存档到物理磁带驱动器或远程 SFTP 服务器。

批量管理工具概述

在 Cisco Unified CM 管理中，使用“批量管理”菜单和子菜单选项通过批量管理工具在 Unified Communications Manager 中配置实体。

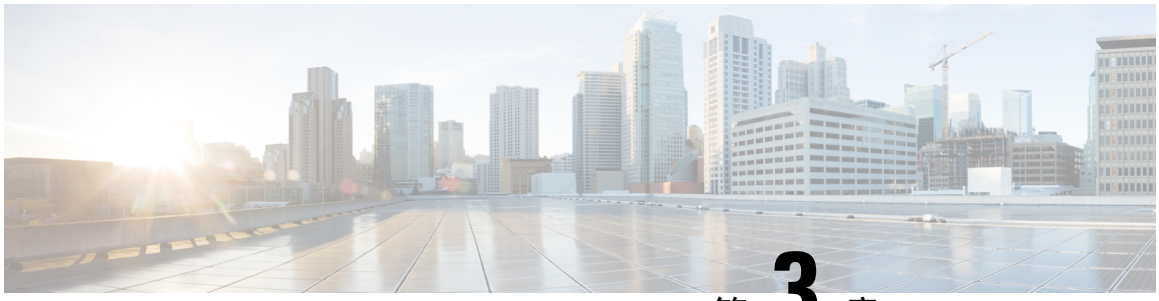
Unified Communications Manager 批量管理工具 (BAT) 是一个基于 Web 的应用程序，让管理员可以批量处理 Unified Communications Manager 数据库中的事务。 BAT 可用于同时添加、更新或删除大量类似的电话、用户或端口。 使用 Cisco Unified CM 管理时，每个数据库事务都需要个别的手动操作，而 BAT 可以自动执行处理，实现更快的添加、更新和删除操作。

您可以对下列类型的设备和记录使用 BAT：

- 添加、更新和删除 Cisco IP 电话、网关、电话、计算机电话接口 (CTI) 端口和 H.323 客户端
- 添加、更新及删除用户、用户设备配置文件、Cisco Unified Communications Manager Assistant 经理和助理
- 添加或删除强制授权码和客户码
- 添加或删除呼叫代答组

- 填充或清空区域矩阵
- 插入、删除或导出访问列表
- 插入、删除或导出远程目标和远程目标配置文件
- 添加基础设施设备

有关如何使用批量管理工具的详细信息，请参阅《*Cisco Unified Communications Manager* 批量管理指南》。



第 3 章

入门

登录到管理界面

使用此程序登录系统中的任何管理界面。

过程

步骤 1 打开 Web 浏览器上的 Unified Communications Manager 界面。

步骤 2 选择**导航**下拉列表中的管理界面。

步骤 3 单击**转至**。

步骤 4 输入您的用户名和密码。

步骤 5 单击**登录**。

重置管理员或安全密码

如果管理员密码丢失，不能访问系统，请按照此程序重置密码。

注释 要在 IM and Presence 节点上更改密码，请在重置管理员密码之前，在所有 IM and Presence 节点中停止 Cisco Presence Engine 服务。重置密码之后，在所有节点中重新启动 Cisco Presence Engine 服务。请确保在维护期间执行此任务，因为当 PE 停止时，您可能会遇到问题。

开始之前

- 您需要对执行此程序的节点拥有物理访问权限。
- 任何时候，当要求插入 CD 或 DVD 介质时，您必须通过 vSphere 客户端为 VMWare 服务器安装 ISO 文件。请参阅“《添加 DVD 或 CD 驱动器至虚拟机》” https://www.vmware.com/support/ws5/doc/ws_disk_add_cd_dvd.html。
- 群集中所有节点的安全密码都必须匹配。修改所有机器的安全密码，否则群集节点不会通信。

过程

步骤 1 使用以下用户名和密码登录发布方节点上的 CLI：

a) 用户名：**pwrecovery**

b) 密码：**pwreset**

步骤 2 按任意键继续。

步骤 3 如果光盘驱动器中有有效 CD/DVD 或您已安装 ISO 文件，将其从 VMWare 客户端删除。

步骤 4 按任意键继续。

步骤 5 将有效 CD 或 DVD 插入驱动器，或安装 ISO 文件。

注释 对于此测试，必须使用仅含有数据的光盘或 ISO 文件。

步骤 6 系统确认上一步后，将提示您输入以下选项之一继续：

- 输入 **a** 重置管理员密码。
- 输入 **s** 重置安全密码。

注释 更改安全密码后，必须重置群集中的各节点。重新启动节点失败将导致系统服务问题以及订阅方节点管理窗口出现问题。

步骤 7 输入新密码，然后再次输入以确认。

管理员凭证必须以字母字符开头，并且长度至少为六个字符，可以包含字母数字字符、连字符和下划线。

步骤 8 系统确认新密码的强度后，密码将被重置，且系统会提示您按任意键退出密码重置实用程序。

如果要设置不同的管理员密码，可使用 CLI 命令 **set password**。有关详细信息，请参阅《*CiscoUnified* 解决方案的命令行界面参考指南》：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

关闭或重新启动系统

如果需要（例如在配置更改后）关闭或重新启动系统，请执行此程序。

开始之前

如果服务器被强制从虚拟机关闭并重新启动，文件系统可能会损坏。 为避免强制关闭，此程序之后或从 CLI 运行 **utils system shutdown** 命令后等待服务器正确关闭。

注释 如果从 VMware 管理工具（vCenter 或嵌入式主机客户端）强制关机或重新启动虚拟机：

- 对于 12.5(1)SU3 或更低版本，这将是不温和关机/重新启动，并且文件系统可能会损坏。 system-history.log 中会显示不温和关机。 相反，建议您通过 utils system shutdown CLI 命令温和关机/重新启动（这将在 system-history.log 中显示为温和关机/重新启动）。

过程

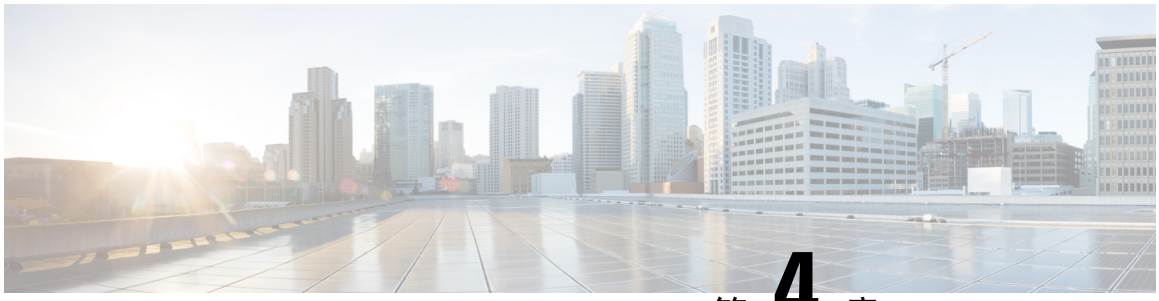
步骤 1 从 Cisco Unified 操作系统管理中，选择**设置** > **版本**。

步骤 2 执行以下操作之一：

- 单击**关闭**停止所有进程并关闭系统。
- 单击**重新启动**停止所有进程并重新启动系统。

第 II 部分

管理用户



第 4 章

管理用户访问

用户访问概述

通过配置以下项目，管理用户对 Cisco Unified Communications Manager 的访问：

- 访问控制组
- 角色
- 用户等级

访问控制组概述

访问控制组是分配给这些用户的用户和角色的列表。 当您将最终用户、应用程序用户或管理员用户分配给访问控制组时，用户将获得与组关联的角色的访问权限。 您可以通过将具有相似访问需求的用户分配给仅具有他们所需角色和权限的访问控制组来管理系统访问。

有两种类型的访问控制组：

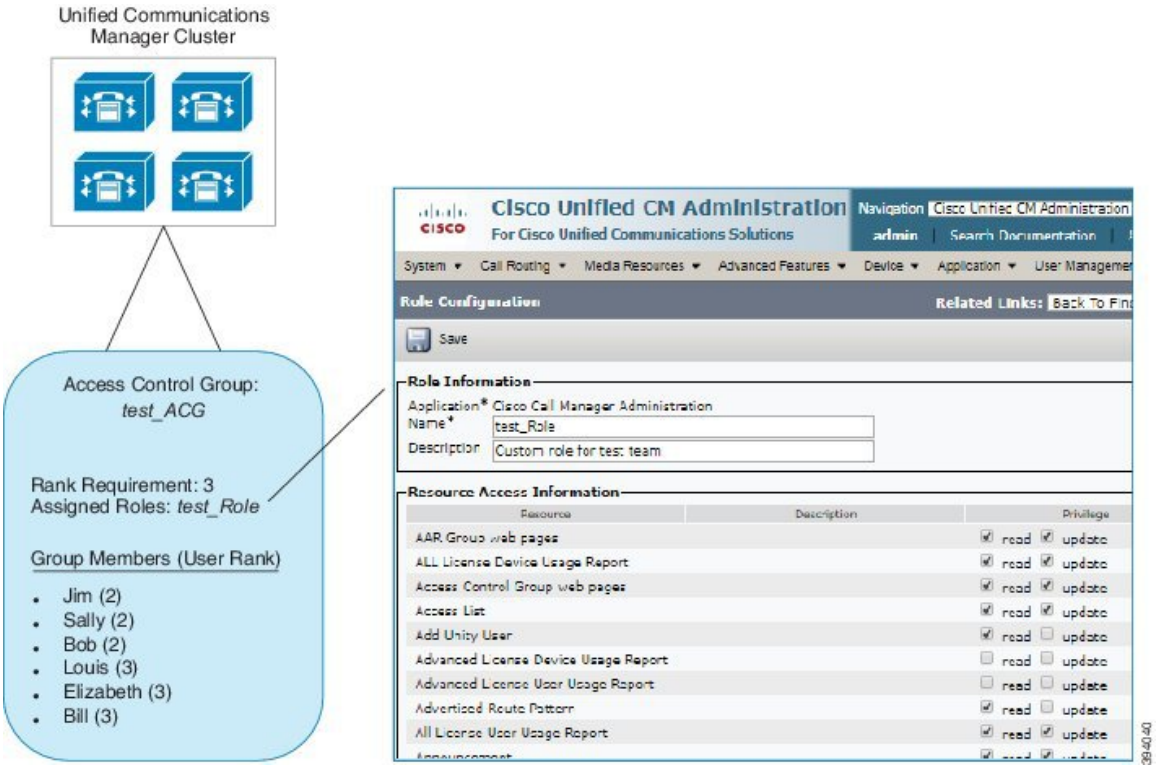
- 标准访问控制组—这些是预定义的默认组，其角色分配能够满足一般的部署需求。 您不能编辑标准组中的角色分配。 不过，除了编辑用户等级要求之外，还可以添加和删除用户。 有关标准访问控制组及其关联角色的列表，请参阅标准角色和访问控制组， 第 32 页。
- 自定义访问控制组—当所有标准组都不包含满足您需求的角色权限时，可以创建自己的访问控制组。

用户等级框架提供一组对可以分配给用户的访问控制组的控制。 要分配给访问控制组，用户必须满足该组的最低等级要求。 例如，用户等级为 4 的最终用户只能被分配给最低等级要求在 4 到 10 之间的访问控制组。不能将它们分配给最低级别为 1 的组。

示例 - 访问控制组的角色权限

以下示例说明了测试团队的成员被分配给访问控制组 **test_ACG** 的群集。 右侧的屏幕截图显示了 test_Role（即与访问控制组关联的角色）的访问设置。 还要注意，访问控制组具有 3 的最小等级要求。所有组成员的级别必须在 1-3 之间才能加入该组。

图 *1:* 访问控制组的角色权限



角色概述

用户通过与用户所属的访问控制组相关联的角色获得系统访问特权。 每个角色包含一组附加到特定资源或应用程序的权限，例如 Cisco Unified CM 管理或 CDR 分析和报告。 对于 Cisco Unified CM 管理之类的应用程序，角色可能包含允许您在应用程序中查看或编辑特定 GUI 页面的权限。 您可以分配给资源或应用程序的权限级别有三个：

- 读取—允许用户查看资源的设置。
- 更新—允许用户编辑资源的设置。
- 无权限—如果用户既没有读取权限，也没有更新权限，则其无权查看或编辑给定资源的设置。

角色类型

在预配置用户时，您必须确定要应用的角色，然后将用户分配到包含该角色的访问控制组。 Cisco Unified Communications Manager 中有以下两种主要类型的角色：

- 标准角色—这些是预先安装的默认角色，旨在满足常见部署的需求。 您无法编辑标准角色的权限。
- 自定义角色—当没有标准角色拥有您所需的权限时，可创建自定义角色。 此外，如果需要更精细级别的访问控制，可以应用高级设置来控制管理员编辑关键用户设置的能力。 请参阅以下部分了解详细信息。

高级角色设置

对于自定义角色，您可以将详细的控制级别添加到**应用程序用户配置**和**最终用户配置**窗口上的所选字段。

在**高级角色配置**窗口中，您可以配置对 Cisco Unified CM 管理的访问权限，同时限制对以下任务的访问：

- 添加用户
- 编辑密码
- 编辑用户等级
- 编辑访问控制组

下表详细说明您可以通过此配置应用的更多控制：

表 *2:* 高级资源访问信息

高级资源	访问控制
权限信息	控制添加或编辑访问控制组的能力： • **查看** - 用户可以查看访问控制组，但不能添加、编辑或删除访问控制组。 • **更新** - 用户可以添加、编辑或删除访问控制组。 **注释** 当两个值都不选时，**权限信息**部分不可用。 **注释** 如果选择**查看**，**用户可以更新自己的权限信息**字段设置为**否**并禁用。 如果希望能够编辑此字段，必须将**权限信息**字段设置为**更新**。

高级资源	访问控制
用户可以更新自己的权限信息	控制用户编辑自己的访问权限的能力： • **是** - 用户可以更新自己的权限信息。 • **否** - 用户无法更新自己的权限信息。 不过，用户可以查看或修改等级相同或较低的用户的权限信息。 **注释** 如果未选中**权限信息更新**复选框，则**用户可以更新自己的权限信息**字段设置为**否**并禁用。
用户等级	控制更改用户等级的能力： • **查看** - 用户可以查看用户等级但不能进行更改。 • **更新** - 用户可以更改用户等级。 **注释** 当两个值都不选时，**用户等级**部分不可用。 **注释** 如果选择**查看** ，**用户可以更新自己的用户等级**字段设置为**否**并禁用。 如果希望能够编辑此字段，必须将**用户等级**字段设置为**更新**。
用户可以更新自己的用户等级	控制用户编辑自己用户等级的能力： • **是** - 用户可以更新自己的用户等级。 • **否** - 用户无法更新自己的用户等级。 不过，用户可以查看或修改等级相同或较低的用户的等级。 **注释** 如果未选中**用户等级更新**复选框，则**用户可以更新自己的用户等级**字段设置为**否**并禁用。
添加新用户	控制添加新用户的能力： • **是** - 用户可以添加新用户。 • **否** - **新增**按键不可用。
密码	控制更改密码的能力： • **是** - 用户可以在**应用程序用户信息**部分更改用户密码。 • **否** - **应用程序用户信息**部分的**密码**和**确认密码**不可用。

用户等级概述

用户等级分层结构提供了一组控制机制，管理员可以通过访问控制组分配给最终用户或应用程序用户。

在预配置最终用户或应用程序用户时，管理员可以为用户分配用户等级。 管理员还可以为每个访问控制组分配用户等级要求。 添加用户以访问控制组时，管理员只能将用户分配给用户的用户等级符合等级要求的组。 例如，管理员可以将用户等级为 3 的用户分配给用户等级要求在 3 到 10 之间的访问控制组。但是，管理员不能将该用户分配给用户等级要求为 1 或 2 的访问控制组。

管理员可以在**用户等级配置**窗口中创建自己的用户等级分层结构，并可在预配置用户和访问控制组时使用该分层结构。 请注意，如果未配置用户等级分层结构，或者您在预配置用户或访问控制组时不指定用户等级设置，则系统会为所有用户和访问控制组分配默认的用户等级 1（可能的最高等级）。

用户访问先决条件

确保查看您的用户需求，了解用户所需的访问级别。 您需要分配具有用户所需访问权限的角色，但这些角色不提供对用户不应访问的系统的访问权限。

在创建新角色和访问控制组之前，查看标准角色和访问控制组的列表，以验证现有访问控制组是否具有所需的角色和访问权限。 有关详细信息，请参阅标准角色和访问控制组，第 32 页。

用户访问配置任务流程

执行以下任务以配置用户访问。

开始之前

如果要使用默认角色和访问控制组，可以跳过创建自定义角色和访问控制组的任务。 您可以将用户分配给现有的默认访问控制组。

过程

	命令或操作	目的
步骤 1	配置用户等级分层结构，第 24 页	设置用户等级分层结构。 请注意，如果跳过此任务，所有用户和访问控制组将分配给默认的用户等级 1（最高等级）。
步骤 2	创建自定义角色，第 24 页	如果默认角色没有您所需的访问权限，请创建自定义角色。
步骤 3	为管理员配置高级角色，第 25 页	可选。 自定义角色中的高级权限可让您控制管理员编辑关键用户设置的能力。
步骤 4	创建访问控制组，第 26 页	如果默认组没有您所需的角色分配，可以创建自定义访问控制组。
步骤 5	向访问控制组分配用户，第 26 页	从标准或自定义访问控制组添加或删除用户

	命令或操作	目的
步骤 6	为访问控制组配置重叠权限策略，第 27 页	可选。 如果用户被分配到权限相互冲突的多个访问控制组，则使用此设置。

配置用户等级分层结构

此程序用于创建自定义用户等级分层结构。

注释 如果未配置用户等级分层结构，则默认情况下系统会为所有用户和访问控制组的用户等级分配 1（可能的最高等级）。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **用户等级**。

步骤 2 单击**新增**。

步骤 3 从**用户等级**下拉菜单中，选择一个介于 1 到 10 之间的等级设置。 最高等级为 1。

步骤 4 输入**等级名称**和**说明**。

步骤 5 单击**保存**。

步骤 6 重复此程序以添加其他用户等级。
您可以将用户等级分配给用户和访问控制组，以控制用户可分配到的组。

创建自定义角色

此程序用于创建具有自定义权限的新角色。 如果没有符合您所需权限的标准角色，则需要执行此操作。 可以通过两种方式来创建角色：

- 使用**新增**按钮从头开始创建和配置新角色。
- 如果现有角色的访问权限与您所需的权限接近，请使用**复制**按键。 可以将现有角色的权限复制到可编辑的新角色。

过程

步骤 1 在 Cisco Unified CM 管理中，单击**用户管理** > **用户设置** > **角色**。

步骤 2 执行以下任一操作：

- 要创建新角色，请单击**新增**。 选择此角色关联的**应用程序**，然后单击**下一步**。

- 要从现有角色复制设置，请单击**查找**并打开现有的角色。 单击**复制**，然后输入新角色的名称。单击**确定**。

步骤 3 输入角色的**名称**和**说明**。

步骤 4 对于每个资源，选中适用的复选框：

- 如果希望用户能够查看资源的设置，选中**读取**复选框。
- 如果希望用户能够编辑资源的自动，选中**更新**复选框。
- 要限制对资源的访问，将两个复选框都保留未选中状态。

步骤 5 单击**授予所有访问权限**或**拒绝所有访问权限**按钮，以授予或删除此角色访问页面上显示的所有资源的权限。

注释 如果资源列表包含多个页面，则此按键仅适用于当前页面上显示的资源。 要更改对其他页面上所列资源的访问权限，必须显示这些页面并在各页面上单击此按钮。

步骤 6 单击**保存**。

为管理员配置高级角色

借助高级角色配置，您可以更细致地编辑自定义角色的权限。 您可以在**最终用户配置**和**应用程序用户配置**窗口中控制管理员编辑以下关键设置的能力：

- 编辑用户等级
- 编辑访问控制组分配
- 添加新用户
- 编辑用户密码

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **角色**。

步骤 2 单击**查找**并选择一个自定义角色。

步骤 3 从**相关链接**中选择**高级角色配置**，然后单击**前往**。

步骤 4 从**资源网页**中，选择**应用程序用户网页**或**用户网页**。

步骤 5 编辑设置。 有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 6 单击**保存**。

创建访问控制组

如果需要创建新的访问控制组，请遵照此程序执行。 如果所有标准组都没有所需的角色和访问权限，您可能需要执行此操作。 有两种方法可以创建自定义的组：

- 使用**新增**按钮从头创建和配置新的访问控制组。
- 如果现有组的角色权限与您的需求接近，请使用**复制**按钮。 您可以将现有组的设置复制到可编辑的新组。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **访问控制组**。

步骤 2 执行以下任一操作：

- 要从头创建新组，请单击**新增**。
- 要从现有组复制设置，请单击**查找**并打开现有的访问控制组。 单击**复制**，然后输入新组的名称。 单击**确定**。

步骤 3 输入访问控制组的**名称**。

步骤 4 从**可用于具有以下用户等级的用户**下拉列表中，选择要分配给该组的用户必须满足的最低用户等级。默认用户等级为 1。

步骤 5 单击**保存**。

步骤 6 向访问控制组分配角色。 您选择的角色将分配给组成员：

a) 从**相关链接**中，选择**分配角色至访问控制组**，并单击**转至**。
b) 单击**查找**以搜索现有的角色。
c) 选中要添加的角色，然后单击**添加选定项**。
d) 单击**保存**。

下一步做什么

向访问控制组分配用户 ， 第 26 页

向访问控制组分配用户

从标准或自定义访问控制组添加或删除用户 .

注释 您只能添加那些用户等级与访问控制组的最低用户等级相同或更高的用户。

注释 如果要从公司 LDAP 目录同步新用户，并且使用适当的权限创建了等级分层结构和访问控制组，则可以将组分配给已同步的用户，作为 LDAP 同步的一部分。 有关如何设置 LDAP 目录同步的详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》。

过程

步骤 1 选择**用户管理** > **用户设置** > **访问控制组**。

此时将出现**查找并列出访问控制组**窗口。

步骤 2 单击**查找**并选择要为其更新用户列表的访问控制组。

步骤 3 从**可用于具有以下用户等级的用户**下拉列表中，选择要分配给该组的用户必须满足的等级要求。

步骤 4 在**用户**部分，单击**查找**以显示用户列表。

步骤 5 如果想要将最终用户或应用程序用户添加到访问控制组，请执行以下操作：

a) 单击**将最终用户添加到访问控制组**或**将应用程序用户添加到访问控制组**。
b) 选择要添加的用户。
c) 单击**添加选定项**。

步骤 6 如果想要从访问控制组删除用户：

a) 选择要删除的用户。
b) 单击**删除选定项**。

步骤 7 单击**保存**。

为访问控制组配置重叠权限策略

配置 Cisco Unified Communications Manager 如何处理可能由访问控制组分配导致的重叠用户权限。这是为了涵盖最终用户被分配到多个访问控制组，而每个访问控制组都有冲突的角色和权限设置的情况。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**系统** > **企业参数**。

步骤 2 在**用户管理参数**下方，如下所示为**重叠用户组和角色的有效访问权限**配置以下值之一：

- **最大值** — 有效权限代表所有重叠访问控制组的最大权限。 这是默认选项。
- **最小值** — 有效权限代表所有重叠访问控制组的最小权限。

步骤 3 单击**保存**。

查看用户权限报告

执行以下程序以查看现有最终用户或现有应用程序用户的用户权限报告。 用户权限报告会显示访问控制组、角色和分配给最终用户或应用程序用户的访问权限。

过程

步骤 1 在 Cisco Unified CM 管理中，执行以下步骤之一：

- 对于最终用户，选择**用户管理** > **最终用户**。
- 对于应用程序用户，选择**用户管理** > **应用程序用户**。

步骤 2 单击**查找**并选择您要为其查看访问权限的用户

步骤 3 从**相关链接**下拉列表中，选择**用户权限报告**，然后单击**转至**。
随即会出现“用户权限”窗口。

创建自定义帮助台角色任务流程

有些公司希望其技术支持人员拥有能够执行某些管理任务的权限。 按照此任务流程中的步骤为技术支持团队成员配置角色和访问控制组，以允许他们执行一些任务，例如添加电话和添加最终用户。

过程

	命令或操作	目的
步骤 1	创建自定义技术支持角色， 第 28 页	为技术支持团队成员创建自定义角色，并为添加新电话和添加新用户等项目分配角色权限。
步骤 2	创建自定义技术支持访问控制组， 第 29 页	为技术支持角色创建新的访问控制组。
步骤 3	将技术支持角色分配到访问控制组， 第 29 页	将技术支持角色分配到技术支持访问控制组。分配到此访问控制组的任何用户都将分配到技术支持角色的权限。
步骤 4	将技术支持成员分配到访问控制组， 第 30 页	为技术支持团队成员分配自定义技术支持角色的权限。

创建自定义技术支持角色

执行此程序以创建自定义技术支持角色，您可以将该角色分配给组织内的技术支持成员。

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择**用户管理** > **用户设置** > **角色**。

步骤 2 单击**新增**。

步骤 3 从“应用程序”下拉列表中，选择要分配给此角色的应用程序。 例如，**Cisco CallManager 管理**。

步骤 4 单击**下一步**。

步骤 5 输入新角色的**名称**。 例如，**Help Desk**。

步骤 6 在**读取和更新权限**下方，选择您要为技术支持用户分配的权限。 例如，如果您希望技术支持成员能够添加用户和电话，请在“用户”网页和“电话”网页上选中**读取**和**更新**复选框。

步骤 7 单击**保存**。

下一步做什么

创建自定义技术支持访问控制组 ， 第 29 页

创建自定义技术支持访问控制组

开始之前

创建自定义技术支持角色 ， 第 28 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **访问控制组**。

步骤 2 单击**新增**。

步骤 3 输入访问控制组的名称。 例如，**Help_Desk**。

步骤 4 单击**保存**。

下一步做什么

将技术支持角色分配到访问控制组 ， 第 29 页

将技术支持角色分配到访问控制组

执行以下步骤为技术支持访问控制组配置来自技术支持角色的权限。

开始之前

创建自定义技术支持访问控制组 ， 第 29 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **访问控制组**。

步骤 2 单击**查找**并选择您为技术支持创建的访问控制组。
此时将显示**访问控制组配置**窗口。

步骤 3 在**相关链接**下拉列表框中，选择**将角色分配到访问控制组**选项，然后单击**转至**。
随即将显示**查找并列出角色**弹出窗口。

步骤 4 单击**将角色分配到组**按钮。

步骤 5 单击**查找**并选择技术支持角色。

步骤 6 单击**添加选定项**。

步骤 7 单击**保存**。

下一步做什么

将技术支持成员分配到访问控制组， 第 30 页

将技术支持成员分配到访问控制组

开始之前

将技术支持角色分配到访问控制组， 第 29 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **访问控制组**。

步骤 2 单击**查找**并选择您创建的自定义技术支持访问控制组。

步骤 3 请执行以下步骤之一：

- 如果您的技术支持团队成员被配置为最终用户，请单击**将最终用户添加到组**。
- 如果您的技术支持团队成员被配置为应用程序用户，请单击**将应用程序用户添加到组**。

步骤 4 单击**查找**并选择您的技术支持用户。

步骤 5 单击**添加选定项**。

步骤 6 单击**保存**。
Cisco Unified Communications Manager 会向您的技术支持团队成员分配您创建的自定义技术支持角色的权限。

删除访问控制组

使用以下程序完全删除访问控制组。

开始之前

删除访问控制组时，Cisco Unified Communications Manager 会从数据库中删除所有访问控制组数据。确保您了解哪些角色正在使用访问控制组。

过程

步骤 1 选择**用户管理** > **用户设置** > **访问控制组**。

此时将显示**查找并列出访问控制组**窗口。

步骤 2 找到您要删除的访问控制组。

步骤 3 单击要删除的访问控制组的名称。

此时将显示所选的访问控制组。 列表按字母顺序显示此访问控制组中的用户。

步骤 4 如果要完全删除访问控制组，请单击**删除**。

此时将显示一个对话框，警告您无法撤消访问控制组的删除。

步骤 5 要删除访问控制组，请单击**确定**；要取消该操作，请单击**取消**。 如果单击**确定**，Cisco Unified Communications Manager 将从数据库中删除访问控制组。

撤销现有的 OAuth 刷新令牌

使用 AXL API 撤销现有的 OAuth 刷新令牌。 例如，如果一名员工离开了您的公司，您可以使用此 API 撤销该员工当前的刷新令牌，以使他们不能获得新的访问令牌，并且将不能再登录到公司帐户。该 API 是一个基于 REST 的 API，受 AXL 凭证保护。 您可以使用任何命令行工具来调用 API。 下面的命令提供了一个可用于撤销刷新令牌的 cURL 命令的示例：

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

其中：

- `admin:password` 是登录 ID 和 Cisco Unified Communications Manager 管理员帐户的密码。
- `UCMaddress` 是 Cisco Unified Communications Manger 发布方节点的 FQDN 或 IP 地址。
- `end_user` 是您要对其撤销刷新令牌的用户的用户 ID。

禁用非活动用户帐户

遵照以下程序使用 Cisco 数据库层监控器服务禁用非活动用户帐户。

如果您在指定的天数内未登录 Cisco Unified Communications Manager，Cisco 数据库层监控器将在预定的维护任务期间将用户帐户状态改为非活动。 在后续的审核日志中，系统会自动审核禁用的用户。

开始之前

在 Cisco 数据库层监控器服务（**系统** > **服务参数**）中输入所选服务器的**维护时间**。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**系统** > **服务参数**。

步骤 2 从**服务器**下拉列表框中选择服务器。

步骤 3 从**服务**下拉列表框中，选择 **Cisco 数据库层监控器**参数。

步骤 4 单击**高级**。

步骤 5 在**禁用未使用用户帐户的天数**字段中，输入天数。 例如，90。系统使用输入的值作为阈值，将帐户状态声明为非活动。 要关闭自动禁用，请输入 0。

注释 这是必填字段。 默认值和最小值为 0，单位为天。

步骤 6 单击**保存**。
如果在配置的天数（例如 90 天）内保持非活动状态，则用户将被禁用。 审核日志中会输入一个条目，其将显示如下消息：“<userID> 用户被标记为非活动”。

设置远程帐户

在 Unified Communications Manager 中配置一个远程帐户，以便 Cisco 支持人员能够暂时访问您的系统进行故障诊断。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**服务** > **远程支持**。

步骤 2 在**帐户名**字段中，输入远程帐户的名称。

步骤 3 在**帐户期限**字段中，输入帐户期限，以天为单位。

步骤 4 单击**保存**。
系统将生成加密的密码短语。

步骤 5 与 Cisco 支持人员联系，向其提供远程支持帐户名和密码短语。

标准角色和访问控制组

下表总结了标准角色和在 Cisco Unified Communications Manager 上预先配置的访问控制组。 标准角色的权限是默认配置的。 此外，与标准角色关联的访问控制组也是默认配置的。

对于标准角色和关联的访问控制组，您都无法编辑任何权限或角色分配。

表 *3:* 标准角色、权限和访问控制组

标准角色	角色的权限/资源	关联的标准访问控制组
标准 AXL API 访问	允许访问 AXL 数据库 API	标准 CCM 超级用户
标准 AXL API 用户	授予登录权限以执行 AXL API。	
标准 AXL 只读 API 访问	默认情况下允许您执行 AXL 只读 API（list API、get API、executeSQLQuery API）。	
标准管理员报告工具管理	允许您查看和配置 Cisco Unified Communications Manager CDR 分析和报告 (CAR)。	标准 CAR 管理员用户、标准 CCM 超级用户
标准审核日志管理	允许您执行审核日志记录功能的以下任务： • 在 Cisco Unified 功能配置的“审核日志配置”窗口中查看和配置审核日志记录 • 在 Cisco Unified 功能配置中查看和配置跟踪并在实时监控工具中收集审核日志功能的跟踪 • 在 Cisco Unified 功能配置中查看和启动/停止 Cisco Audit Event 服务 • 在 RTMT 中查看和更新关联的警告	标准审计用户
标准 CCM 管理员用户	授予 Cisco Unified Communications Manager 管理的登录权限。	标准 CCM 管理员用户、标准 CCM 网关管理、标准 CCM 电话管理、标准 CCM 只读、标准 CCM 服务器监控、标准 CCM 超级用户、标准 CCM 服务器维护、标准信息包探查器用户
标准 CCM 最终用户	授予 Cisco Unified Communications Self Care 门户网站的最终用户登录权限	标准 CCM 最终用户

标准角色	角色的权限/资源	关联的标准访问控制组

标准 CCM 功能管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务：
	• 使用批量管理工具查看、删除和插入以下项目：
	  • 客户码和强制授权码
	  • 呼叫代答组
	• 在 Cisco Unified Communications Manager 管理中查看和配置以下项目：
	  • 客户码和强制授权码
	  • 呼叫暂留
	  • 呼叫代答
	  • Meet-me 号码/模式
	  • 留言通知
	  • Cisco Unified IP 电话服务
	  • 语音信箱引导、语音信箱端口向导、语音信箱端口和语音信箱配置文件
		标准 CCM 服务器维护

标准 CCM 网关管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务： • 在批量管理工具中查看和配置网关模板 • 查看和配置网守、网关和干线	标准 CCM 网关管理

标准角色	角色的权限/资源	关联的标准访问控制组

标准 CCM 电话管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务：
	• 在批量管理工具中查看和导出电话
	• 在批量管理工具中查看和插入用户设备配置文件
	• 在 Cisco Unified Communications Manager 管理中查看和配置以下项目：
	  • BLF 快速拨号
	  • CTI 路由点
	  • 默认设备配置文件或默认配置文件
	  • 目录号码和线路显示
	  • 固件加载信息
	  • 电话按键模板或软键模板
	  • 电话
	  • 特定电话的电话按键重新排序信息（通过单击“电话配置”窗口中的“修改按键项”按钮）
		标准 CCM 电话管理

标准 CCM 路由计划管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务： • 查看和配置应用程序拨号规则 • 查看和配置呼叫搜索空间和分区 • 查看和配置拨号规则，包括拨号规则模式 • 查看和配置寻线列表、寻线引导和线路组 • 查看和配置路由过滤器、路由组、路由寻线列表、路由列表、路由模式和路由计划报告 • 查看和配置时段和时间表 • 查看和配置转换模式	

标准角色	角色的权限/资源	关联的标准访问控制组

标准 CCM 服务管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务：
	• 查看和配置以下项目：
	  • 信号器、会议桥和转码器
	  • 音频来源和 MOH 服务器
	  • 媒体资源组和媒体资源组列表
	  • 媒体终结点
	  • Cisco Unified Communications Manager Assistant 向导
	• 在批量管理工具中查看和配置“删除经理”、“删除经理/助理”和“嵌入经理/助理”窗口
		标准 CCM 服务器维护

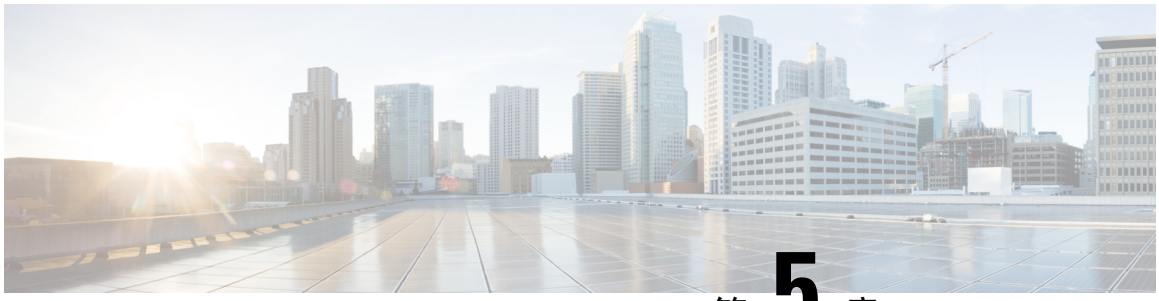
标准角色	角色的权限/资源	关联的标准访问控制组
标准 CCM 系统管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务： • 查看和配置以下项目： • 自动路由迂回 (AAR) 组 • Cisco Unified Communications Manager (Cisco Unified CM) 和 Cisco Unified Communications Manager 组 • 日期和时间组 • 设备默认值 • 设备池 • 企业参数 • 企业电话配置 • 位置 • 网络时间协议 (NTP) 服务器 • 插件 • 用于运行信令呼叫控制协议 (SCCP) 或会话发起协议 (SIP) 的电话的安全性配置文件；用于 SIP 干线的安全性配置文件 • 可存活远程站点电话 (SRST) 引用 • 服务器 • 在批量管理工具中查看和配置“作业计划程序”窗口	标准 CCM 服务器维护
标准 CCM 用户权限管理	允许您在 Cisco Unified Communications Manager 管理中查看和配置应用程序用户。	
标准 CCMADMIN 管理	允许您访问 CCMAdmin 系统的所有方面	
标准 CCMADMIN 管理	允许您在 Cisco Unified Communications Manager 管理和批量管理工具中查看和配置所有项目。	标准 CCM 超级用户
标准 CCMADMIN 管理	允许您在被叫号码分析器中查看和配置信息。	

标准角色	角色的权限/资源	关联的标准访问控制组
标准 CCMADMIN 只读	允许所有 CCMAdmin 资源的读取访问权限	
标准 CCMADMIN 只读	允许您在 Cisco Unified Communications Manager 管理和批量管理工具中查看配置。	标准 CCM 网关管理、标准 CCM 电话管理、标准 CCM 只读、标准 CCM 服务器维护、标准 CCM 服务器监控
标准 CCMADMIN 只读	允许您在被叫号码分析器中分析路由配置。	
标准 CCMUSER 管理	允许访问 Cisco Unified Communications Self Care 门户网站。	标准 CCM 最终用户
标准 CTI 允许呼叫监控	允许 CTI 应用程序/设备监控呼叫	标准 CTI 允许呼叫监控
标准 CTI 允许呼叫暂留监控	允许 CTI 应用程序/设备使用呼叫暂留。 **重要事项** 开放线路和暂留线路的最大数不得超过 65000。 如果总数超过 65,000，请从应用程序用户中删除“标准 CTI 允许呼叫暂留监控”角色或减少配置的暂留线路数。	标准 CTI 允许呼叫暂留监控
标准 CTI 允许呼叫录音	允许 CTI 应用程序/设备录音呼叫	标准 CTI 允许呼叫录音
标准 CTI 允许主叫号码修改	允许 CTI 应用程序在通话期间转换主叫方号码	标准 CTI 允许主叫号码修改
标准 CTI 允许控制所有设备	允许控制所有 CTI 可控制设备	标准 CTI 允许控制所有设备
标准 CTI 允许控制支持已连接转接和会议的电话	允许控制支持已连接转接和会议的所有 CTI 设备	标准 CTI 允许控制支持已连接转接和会议的电话
标准 CTI 允许控制支持跳转模式的电话	允许控制支持跳转模式的所有 CTI 设备	标准 CTI 允许控制支持跳转模式的电话
标准 CTI 允许接收 SRTP 重要材料	允许 CTI 应用程序访问和分发 SRTP 重要材料	标准 CTI 允许接收 SRTP 重要材料
启用标准 CTI	启用 CTI 应用程序控制	启用标准 CTI
标准 CTI 安全连接	启用到 Cisco Unified Communications Manager 的安全 CTI 连接	标准 CTI 安全连接
标准 CU 报告	允许应用程序用户生成各种来源的报告	

标准角色	角色的权限/资源	关联的标准访问控制组
标准 CU 报告	允许您在 Cisco Unified 报告中查看、下载、生成和上传报告	标准 CCM 管理用户、标准 CCM 超级用户
标准 EM 验证代理权限	管理应用程序的 Cisco 分机移动 (EM) 验证权限；与 Cisco 分机移动交互的所有应用程序用户（例如，Cisco Unified Communications Manager Assistant 和 Cisco Web Dialer）必需	标准 CCM 超级用户、标准 EM 验证代理权限
标准信息包探查	允许您访问 Cisco Unified Communications Manager 管理以启用数据包探查（捕获）。	标准信息包探查器用户
标准实时和跟踪收集	允许您访问 Cisco Unified 功能配置和实时监控工具视图并使用以下项目： • 简单对象访问协议 (SOAP) 功能配置 AXL API • SOAP 呼叫记录 API • SOAP Diagnostic Portal (Analysis Manager) 数据库服务 • 配置审核日志追踪功能 • 配置实时监控工具，包括收集跟踪	标准实时和跟踪收集

标准角色	角色的权限/资源	关联的标准访问控制组
标准功能配置	允许您在Cisco Unified 功能配置或实时监控工具中查看和配置以下窗口： • “警报配置”和“警报定义”（Cisco Unified 功能配置） • 审计追踪（标记为只读/仅查看） • SNMP 相关窗口（Cisco Unified 功能配置） • “跟踪配置”和“跟踪配置故障诊断”（Cisco Unified 功能配置）) • 日志分区监控 • 警告配置 (RTMT)、配置文件配置 (RTMT)，以及跟踪收集 (RTMT) 允许您查看和使用 SOAP 功能配置 AXL API、SOAP 呼叫记录 API 和 SOAP Diagnostic Portal (Analysis Manager) 数据库服务。 对于 SOAP 呼叫记录 API，RTMT Analysis Manager呼叫记录权限通过此资源进行控制。 对于 SOAP Diagnostic Portal 数据库服务，RTMT Analysis Manager 托管数据库通过此资源控制访问。	标准 CCM 服务器监控、标准 CCM 超级用户
标准功能配置管理	功能配置管理员可在 Cisco Unified Communications Manager 管理中访问“插件”窗口并从此窗口中下载插件。	
标准功能配置管理	允许您管理被叫号码分析器功能配置的所有方面。	
标准功能配置管理	允许您在Cisco Unified 功能配置和实时监控工具中查看和配置所有窗口。（审计追踪仅支持查看） 允许您查看和使用所有SOAP功能配置AXL API。	
标准功能配置只读	允许您查看被叫号码分析器中组件的所有功能配置相关数据。	标准 CCM 只读

标准角色	角色的权限/资源	关联的标准访问控制组
标准功能配置只读	允许您在Cisco Unified 功能配置和实时监控工具中查看配置。（“审计配置”窗口除外，该窗口由“标准审核日志管理”角色代表） 允许您查看所有 SOAP 功能配置 AXL API、SOAP 呼叫记录 API 和 SOAP Diagnostic Portal (Analysis Manager) 数据库服务。	
标准系统服务管理	允许您在 Cisco Unified 功能配置中查看、激活、启动和停止服务。	
标准 SSO 配置管理员	允许您管理 SAML SSO 配置的所有方面	
标准保密访问级别用户	允许您访问所有保密访问级别页面	标准 Cisco Call Manager 管理
标准 CCMADMIN 管理	允许您管理 CCMAdmin 系统的所有方面	标准 Cisco Unified CM IM and Presence 管理
标准 CCMADMIN 只读	允许所有 CCMAdmin 资源的读取访问权限	标准 Cisco Unified CM IM and Presence 管理
标准 CU 报告	允许应用程序用户生成各种来源的报告	标准 Cisco Unified CM IM and Presence 报告



第 5 章

管理最终用户

最终用户概述

在管理启动并运行的系统时，您可能需要在您的系统中更新所配置的最终用户的列表。 其中包括：

- 设置新用户
- 为新的最终用户设置电话
- 为最终用户更改密码或个人识别码
- 为 IM and Presence Service 启用最终用户

您可以使用 Cisco Unified CM 管理中的**最终用户配置**窗口添加、搜索、显示和维护 Unified CM 最终用户的相关信息。 您还可以使用**快速用户/电话添加**窗口，快速配置新的最终用户并为该最终用户配置新电话。

最终用户管理任务

过程

	命令或操作	目的
步骤 1	配置用户模板， 第 44 页	如果您尚未使用用户配置文件或包含通用线路和设备模板的功能组模板配置您的系统，请执行这些任务以进行设置。 您可以将这些模板应用于任何新的最终用户，以便快速配置新用户和电话。

	命令或操作	目的
步骤 2	使用以下方法之一添加新的最终用户 • 从 LDAP 导入最终用户，第 48 页 • 手动添加最终用户，第 49 页	如果已配置并且系统与公司 LDAP 目录同步，则可以直接从 LDAP 导入新的最终用户。 此外，您可以手动添加和配置最终用户。
步骤 3	通过执行以下任务之一将电话分配给新的或现有的最终用户： • 为最终用户添加新电话，第 50 页 • 将现有电话移至最终用户，第 50 页	您可以使用“添加新电话”程序，使用通用设备模板的设置为最终用户配置新电话。 您还可以使用“移动”程序分配已经配置好的现有电话。
步骤 4	更改最终用户个人识别码，第 51 页	（可选）在 Cisco Unified Communications Manager 管理中为最终用户更改个人识别码。
步骤 5	更改最终用户密码，第 51 页	（可选）在 Cisco Unified Communications Manager 管理中为最终用户更改密码。
步骤 6	创建 Cisco Unity Connection 语音信箱，第 52 页	（可选）在 Cisco Unified Communications Manager 管理中创建单独的 Cisco Unity Connection 语音信箱。

配置用户模板

执行以下任务以设置用户配置文件和功能组模板。 当您添加新的最终用户时，可以使用线路和设备设置快速配置最终用户并为最终用户配置任何电话。

过程

	命令或操作	目的
步骤 1	配置通用线路模板，第 45 页	使用通常应用于目录号码的通用设置配置通用线路模板。
步骤 2	配置通用设备模板，第 45 页	使用通常应用于电话的通用设置配置通用设备模板。
步骤 3	配置用户配置文件，第 46 页	将通用线路和通用设备模板分配给用户配置文件。 如果已经配置了自预配置功能，您可以为使用此配置文件的用户启用自预配置。
步骤 4	配置功能组模板，第 47 页	将用户配置文件分配给功能组模板。 对于 LDAP 同步用户，功能组模板会将用户配置文件设置关联到最终用户。

配置通用线路模板

通过通用线路模板，您可以轻松地将通用设置应用到新分配的目录号码。 配置不同的模板以满足不同用户组的需求。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **通用线路模板**。

步骤 2 单击**新增**。

步骤 3 配置**通用线路模板配置**窗口中的字段。 请参阅联机帮助，了解有关字段及其配置选项的更多信息。

步骤 4 如果要部署具有备用号码的全局拨号方案复制，展开**企业备用号码**和**+E.164 备用号码**部分，然后执行以下操作：

a) 单击**添加企业备用号码**按钮和/或**添加 +E.164 备用号码**按钮。
b) 添加要用于分配到备用号码的**号码掩码**。 例如，一个 4 位分机可能会将 5XXXX 用作企业号码掩码，并将 1972555XXXX 用作 +E.164 备用号码掩码。
c) 分配要为其分配备用号码的分区。
d) 如果想要通过 ILS 通告此号码，请选中**通过 ILS 全局通告**复选框。 请注意，如果您使用通告模式来汇总备用号码的范围，可能不需要通告单独的备用号码。
e) 展开 **PSTN 故障转移**部分，然后选择**企业号码**或 **+E.164 备用号码**作为正常呼叫路由失败时要使用的 PSTN 故障转移。

步骤 5 单击**保存**。

下一步做什么

配置通用设备模板， 第 45 页

配置通用设备模板

通用设备模板可让您轻松地将配置设置应用到新预配置的设备。 预配置的设备使用通用设备模板的设置。 可以配置不同的设备模板来满足不同用户群体的需求。 还可以将已配置的配置文件分配给此模板。

开始之前

配置通用线路模板， 第 45 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **通用设备模板**。

步骤 2 单击**新增**。

步骤 3 输入以下必填字段：

a) 为模板输入**设备说明**。
b) 从下拉列表中选择**设备池**类型。
c) 从下拉列表中选择**设备安全性配置文件**。
d) 从下拉列表中选择 **SIP 配置文件**。
e) 从下拉列表中选择**电话按键模板**。

步骤 4 完成**通用设备模板配置**窗口中其余字段的设置。 要查看字段说明，请参阅联机帮助。

步骤 5 在**电话设置**下，填写以下可选字段：

a) 如果配置了**通用电话配置文件**，分配该配置文件。
b) 如果配置了**通用设备配置**，分配该配置。
c) 如果配置了**功能控制策略**，分配该策略。

步骤 6 单击**保存**。

下一步做什么

配置用户配置文件，第 46 页

配置用户配置文件

通过用户配置文件将通用线路和通用设备模板分配给用户。 为不同的用户组配置多个用户配置文件。 您还可以为使用此服务配置文件的用户启用自预配置。

开始之前

配置通用设备模板，第 45 页

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **用户配置文件**。

步骤 2 单击**新增**。

步骤 3 输入用户配置文件的**名称**和**描述**。

步骤 4 分配**通用设备模板**以应用到用户的**桌面电话**、**移动和桌面设备**，以及**远程目标/设备配置文件**。

步骤 5 分配**通用线路模板**以应用到此用户配置文件中的用户的电话线路。

步骤 6 如果您希望此用户配置文件中的用户能够使用自预配置功能部署他们自己的电话，请执行以下操作：

a) 选中**允许最终用户部署自己的电话**复选框。
b) 在**一旦最终用户拥有这么多电话即限制部署**字段中，输入允许用户部署的最大电话数量。 最大值为 20。
c) 选中**允许预配置已分配给其他最终用户的电话**复选框以确定与此配置文件关联的用户是否有迁移或重新分配已归其他用户所有的设备的权限。 默认情况下，此复选框未选中。

步骤 7 如果您希望与此用户配置文件关联的 Cisco Jabber 用户能够使用 Mobile and Remote Access 功能，请选中**启用 Mobile and Remote Access** 复选框。

注释
- 默认情况下，此复选框为选中状态。 当取消选中此复选框时，**客户端策略**部分会被禁用，并且默认情况下会选中“无服务”客户端策略选项。
- 此设置仅对使用 OAuth 刷新登录名的 Cisco Jabber 用户是必需的。 非 Jabber 用户无需此设置即可使用 Mobile and Remote Access。 Mobile and Remote Access 功能仅适用于 Jabber Mobile and Remote Access 用户，不适用于任何其他终端或客户端。

步骤 8 为此用户配置文件分配 Jabber 策略。 从**桌面客户端策略**以及**移动客户端策略**下拉列表中，选择以下选项之一：

- 无服务 — 此策略禁止访问所有 Cisco Jabber 服务。
- 仅 IM & Presence—此策略仅启用即时消息和在线状态功能。
- IM & Presence、语音和视频呼叫—此策略为所有拥有音频和视频设备的用户启用即时消息、在线状态、语音邮件和会议功能。 这是默认选项。

注释 Jabber 桌面客户包括 Cisco Jabber Windows 版本用户和 Cisco Jabber Mac 版本用户。 Jabber 移动客户包括 Cisco Jabber iPad 和 iPhone 版本用户以及 Cisco Jabber Android 版本用户。

步骤 9 如果想要此用户配置文件中的用户通过 Cisco Unified Communications Self Care 门户为分机移动或跨群集分机移动设置最长登录时间，选中**允许最终用户设置其分机移动最长登录时间**复选框。

注释 **允许最终用户设置其分机移动最长登录时间**复选框默认未选中。

步骤 10 单击**保存**。

下一步做什么

配置功能组模板，第 47 页

配置功能组模板

功能组模板可帮助您非常快速地为预配置的用户配置电话、线路和功能，从而为您的系统部署提供帮助。 如果要从公司 LDAP 目录同步用户，请使用希望用户从目录同步使用的用户配置文件和服务配置文件配置功能组模板。 您也可以通过此模板为同步的用户启用 IM and Presence Service。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **功能组模板**。

步骤 2 单击**新增**。

步骤 3 输入功能组模板的**名称**和**说明**。

步骤 4 如果您想要使用本地群集作为所有使用此模板的用户的主群集，请选中**主群集**复选框。

步骤 5 选中**为 Unified CM IM and Presence 启用用户**复选框，以允许使用此模板的用户交换即时消息和在线状态信息。

步骤 6 从下拉列表中，选择一个**服务配置文件**和**用户配置文件**。

步骤 7 填写**功能组模板配置**窗口中的其余字段。 请参阅联机帮助中的字段说明。

步骤 8 单击**保存**。

下一步做什么

添加新的最终用户。 如果您的系统与公司 LDAP 目录集成，可以直接从 LDAP 目录导入用户。 否则，请手动创建最终用户。

- 从 LDAP 导入最终用户 ， 第 48 页
- 手动添加最终用户 ， 第 49 页

从 LDAP 导入最终用户

执行以下程序以手动从公司 LDAP 目录导入新的最终用户。 如果您的 LDAP 同步配置包含一个带有用户配置文件（包含通用线路和设备模板）的功能组模板，以及一个 DN 池，那么导入过程会自动配置最终用户和主分机。

注释 在发生初始同步后，您无法将新配置（例如添加功能组模板）添加到 LDAP 目录同步中。 如果要编辑现有的 LDAP 同步，必须使用批量管理或者配置新的 LDAP 同步。

开始之前

在开始执行此程序之前，请确保已将 Cisco Unified Communications Manager 与公司 LDAP 目录同步。 LDAP 同步必须包含一个带有通用线路和设备模板的功能组模板。

过程

步骤 1 在 Cisco Unified CM 管理中，依次选择**系统** > **LDAP** > **LDAP 目录**。

步骤 2 单击**查找**并选择要向其添加用户的 LDAP 目录。

步骤 3 单击**执行完全同步**。
Cisco Unified Communications Manager 会与外部 LDAP 目录同步。 LDAP 目录中任何新的最终用户都会导入到 Cisco Unified Communications Manager 数据库中。

下一步做什么

如果为用户启用了自预配置，则最终用户可以使用自预配置互动语音响应 (IVR) 来部署新电话。 否则，执行以下任务之一将电话分配给最终用户：

- 为最终用户添加新电话 ， 第 50 页
- 将现有电话移至最终用户 ， 第 50 页

手动添加最终用户

执行以下程序添加新的最终用户并为他们配置访问控制组和主线路分机。

注释 请确保已设置具有要为用户分配的角色权限的访问控制组。 有关详细信息，请参阅“管理用户访问权限”一章。

开始之前

确认您配置有包含通用线路模板的用户配置文件。 如果您需要配置新的分机，Cisco Unified Communications Manager 将使用通用线路模板中的设置配置主分机。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **快速用户/电话添加**。

步骤 2 输入**用户 ID** 和**姓氏**。

步骤 3 从**功能组模板**下拉列表中，选择功能组模板。

步骤 4 单击**保存**。

步骤 5 从**用户配置文件**下拉列表中，验证所选的用户配置文件包含通用线路模板。

步骤 6 从**访问控制组成员资格**部分，单击 + 图标。

步骤 7 从**用户属于**下拉列表中，选择一个访问控制组。

步骤 8 在**主分机**下方，单击 + 图标。

步骤 9 从**分机**下拉列表中，选择一个显示为（**可用**）的目录号码。

步骤 10 如果所有线路分机都显示为（**已使用**），请执行以下步骤：

a) 单击**新建...** 按键。
随即将显示**添加新分机**弹出窗口。
b) 在**目录号码**字段中，输入新的线路分机。
c) 从**线路模板**下拉列表中，选择一个通用线路模板。
d) 单击**确定**。
Cisco Unified Communications Manager 会使用通用线路模板的设置配置目录号码。

步骤 11 （可选） 填写**快速用户/电话添加配置**窗口中的任何其他字段。

步骤 12 单击**保存**。

下一步做什么

执行以下程序之一将电话分配给该最终用户：

- 为最终用户添加新电话 ， 第 50 页
- 将现有电话移至最终用户 ， 第 50 页

为最终用户添加新电话

执行以下程序为新的或现有的最终用户添加新电话。 确保最终用户的用户配置文件包含通用设备模板。 Cisco Unified Communications Manager 会使用通用设备模板设置配置电话。

开始之前

请执行以下程序之一以添加最终用户：

- 手动添加最终用户 ， 第 49 页
- 从 LDAP 导入最终用户 ， 第 48 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **快速/用户电话添加**。

步骤 2 单击**查找**并选择您要为其添加新电话的最终用户。

步骤 3 单击**管理设备**。
将出现“管理设备”窗口。

步骤 4 单击**添加新电话**。
此时将显示“添加电话至用户”弹出窗口。

步骤 5 从**产品类型**下拉列表中，选择电话型号。

步骤 6 从**设备协议**下拉列表中，选择 SIP 或 SCCP 作为协议。

步骤 7 在**设备名称**文本框中，输入设备的 MAC 地址。

步骤 8 从**通用设备模板**下拉列表中，选择一个通用设备模板。

步骤 9 如果电话支持扩展模块，输入您要部署的扩展模块数量。

步骤 10 如果您想使用分机移动访问电话，选中**在分机移动中**复选框。

步骤 11 单击**添加电话**。
此时“添加新电话”弹出窗口会关闭。 Cisco Unified Communications Manager 会将电话添加至用户，并使用通用设备模板配置电话。

步骤 12 如果您想对电话配置进行其他编辑，单击对应的铅笔图标以在**电话配置**窗口中打开电话。

将现有电话移至最终用户

执行此程序以将现有电话移至新的或现有的最终用户。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **快速用户/电话添加**。

步骤 2 单击**查找**并选择您要向其移动现有电话的用户。

步骤 3 单击**管理设备**按键。

步骤 4 单击**查找要移至此用户的电话**按键。

步骤 5 选择您想要移至此用户的电话。

步骤 6 单击**移动选定项**。

更改最终用户个人识别码

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择**用户管理** > **最终用户**。
此时将出现**查找并列出用户**窗口。

步骤 2 要选择现有用户，请在**查找用户位置**字段中指定合适的过滤器，并单击**查找**以检索用户列表，然后从列表中选择用户。
随即会显示**最终用户配置**窗口。

步骤 3 在**个人识别码**字段中，双击现有的个人识别码（已加密），然后输入新的个人识别码。 至少必须输入分配的凭证策略中指定的最少字符数（1-127 个字符）。

步骤 4 在**确认个人识别码**字段中，双击已加密的现有个人识别码，然后再次输入新的个人识别码。

步骤 5 单击**保存**。

注释 如果 Cisco Unity Connection 的**应用服务器配置**窗口中的**最终用户 PIN 同步**复选框已启用，您可以使用相同的最终用户个人识别码登录到 Extension Mobility、Conference Now、移动连接，以及 Cisco Unity Connection 语音邮件。 最终用户可以使用相同的个人识别码登录到分机移动和访问其语音邮件。

更改最终用户密码

LDAP 验证启用时，您无法更改最终用户密码。

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择**用户管理** > **最终用户**。
此时将出现**查找并列出用户**窗口。

步骤 2 要选择现有用户，请在**查找用户位置**字段中指定合适的过滤器，并单击**查找**以检索用户列表，然后从列表中选择用户。
随即会显示**最终用户配置**窗口。

步骤 3 在**密码**字段中，双击现有的密码（已加密），然后输入新密码。 至少必须输入分配的凭证策略中指定的最少字符数（1-127 个字符）。

步骤 4 在**确认密码**字段中，双击已加密的现有密码，然后再次输入新密码。

步骤 5 单击**保存**。

创建 Cisco Unity Connection 语音信箱

开始之前

- 您必须配置 Cisco Unified Communications Manager 才能使用语音留言。有关配置 Cisco Unified Communications Manager 以使用 Cisco Unity Connection 的详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》，网址：

  http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

- 您必须将设备和主分机号码与最终用户关联。
- 您可以使用 Cisco Unity Connection 中提供的导入功能，而不是执行本节中所述的程序。有关如何使用导入功能的信息，请参阅《*Cisco Unity Connection* 用户移动、添加和更改指南》。

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择**用户管理** > **最终用户**。
此时将出现**查找并列出用户**窗口。

步骤 2 要选择现有用户，请在**查找用户位置**字段中指定合适的过滤器，并单击**查找**以检索用户列表，然后从列表中选择用户。
随即会显示**最终用户配置**窗口。

步骤 3 验证主分机号码与该用户关联。

注释 您必须定义主分机；否则创建 Cisco Unity 用户链接不会在**相关链接**下拉列表中显示。

步骤 4 从**相关链接**下拉列表中，选择创建 Cisco Unity 用户链接，然后单击**转至**。

此时将显示“添加 Cisco Unity 用户”对话框。

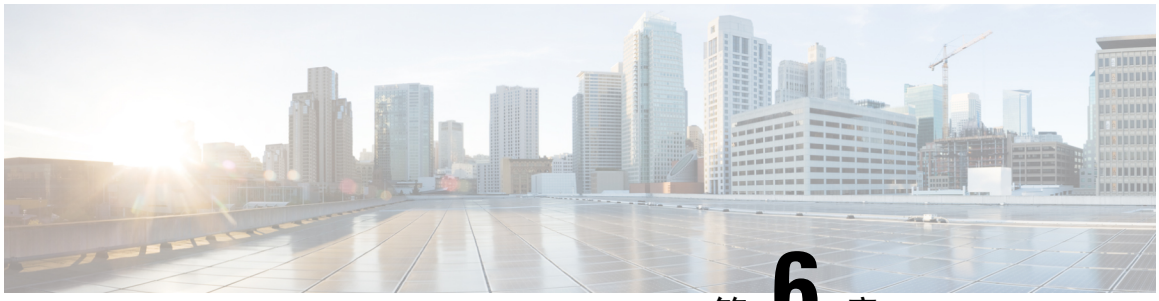
步骤 5 从**应用服务器**下拉列表中，选择您要在其上创建 Cisco Unity Connection 用户的 Cisco Unity Connection 服务器，然后单击**下一步**。

步骤 6 从**订户模板**下拉列表中，选择您要使用的订户模板。

步骤 7 单击**保存**。

此时将创建信箱。**相关链接**下拉列表中的链接会更改为**最终用户配置**窗口中的编辑 Cisco Unity 用户。现在，您可以在 Cisco Unity Connection 管理中查看所创建的用户。

注释 将 Cisco Unity Connection 用户与 Cisco Unified Communications Manager 最终用户集成后，您无法编辑 Cisco Unity Connection 管理中的字段，例如“别名”（Cisco Unified CM 管理中的“用户 ID”）、“名字”、“姓氏”，以及“分机”（Cisco Unified CM 管理中的“主分机”）。您只能在 Cisco Unified CM 管理中更新这些字段。



第 6 章

管理应用程序用户

应用程序用户概述

管理员可以使用 Cisco Unified CM 管理中的**应用程序用户配置**窗口添加、搜索、显示和维护 Cisco Unified Communications Manager 应用程序用户的相关信息。

默认情况下，Cisco Unified CM 管理包括以下应用程序用户：

- CCMAdministrator
- CCMSysUser
- CCMQRTSecureSysUser
- CCMQRTSysUser
- IPMASecureSysUser
- IPMASysUser
- WDSecureSysUser
- WDSysUser
- TabSyncSysUser
- CUCService

注释 “标准 CCM 超级用户”组中的管理员用户可以访问 Cisco Unified Communications Manager 管理、Cisco Unified 功能配置，以及 Cisco Unified 报告（单点登录到应用程序之一）。

应用程序用户任务流程

过程

	命令或操作	目的
步骤 1	添加新的应用程序用户， 第 56 页	添加新的应用程序用户。
步骤 2	将设备与应用程序用户关联， 第 56 页	分配设备以与应用程序用户关联。
步骤 3	添加管理员用户到 Cisco Unity 或 Cisco Unity Connection， 第 57 页	将用户作为管理员用户添加到 Cisco Unity 或 Cisco Unity Connection。 您可在 Cisco Unified CM 管理中配置应用程序用户；然后，配置任何其他设置用于 Cisco Unity 或 Cisco Unity Connection 管理中的用户。
步骤 4	更改应用程序用户密码， 第 58 页	更改应用程序用户密码。
步骤 5	管理应用程序用户密码凭证信息， 第 58 页	更改或查看凭证信息，例如关联的验证规则、关联的凭证策略或应用程序用户上次更改密码的时间。

添加新的应用程序用户

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **应用程序用户**。

步骤 2 单击**新增**。

步骤 3 配置**应用程序用户配置**窗口中的字段。 请参阅联机帮助，了解有关字段及其配置选项的信息。

步骤 4 单击**保存**。

下一步做什么

将设备与应用程序用户关联， 第 56 页

将设备与应用程序用户关联

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **应用程序用户**。

此时将出现**查找并列出用户**窗口。

步骤 2 要选择现有用户，请在**查找用户位置**字段中指定合适的过滤器，并选择**查找**以检索用户列表，然后从列表中选择用户。

步骤 3 在**可用设备**列表中，选择要与应用程序用户关联的设备，然后单击列表下方的**向下箭头**。 所选的设备会移至**受控设备**列表。

注释 要限制可用设备的列表，请单击**查找更多电话**或**查找更多路由点**按钮。

步骤 4 如果单击**查找更多电话**按钮，将显示**查找并列出电话**窗口。 执行搜索，以查找要与此应用程序用户关联的电话。

对要分配给应用程序用户的每个设备重复上述操作。

步骤 5 如果单击**查找更多路由点**按钮，将显示**查找并列出 CTI 路由点**窗口。 执行搜索，以查找要与此应用程序用户关联的 CTI 路由点。

对要分配给应用程序用户的每个设备重复上述操作。

步骤 6 单击**保存**。

添加管理员用户到 Cisco Unity 或 Cisco Unity Connection

如果您将 Cisco Unified Communications Manager 与 Cisco Unity Connection 7.x 或更新版本集成，您可以使用 Cisco Unity Connection 7.x 或更新版本中可用的导入功能，而不是执行本节中所述的程序。有关如何使用导入功能的信息，请参阅 Cisco Unity Connection 7.x 或更新版本的《用户移动、添加和更改指南》，位于：

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html。

当 Cisco Unity 或 Cisco Unity Connection 用户与 Cisco Unified CM 应用程序用户集成时，您无法编辑字段。您只能在 Cisco Unified Communications Manager 管理中更新这些字段。

Cisco Unity 和 Cisco Unity Connection 监控从 Cisco Unified Communications Manager 进行的数据同步。您可以在工具菜单上的 Cisco Unity 管理或 Cisco Unity Connection 管理中配置同步时间。

开始之前

确保您已为打算推送到 Cisco Unity 或 Cisco Unity Connection 的用户定义相应的模板

仅当您安装并配置了相应的 Cisco Unity 或 Cisco Unity Connection 软件后，**创建 Cisco Unity 用户**链接才会显示。请参阅适用的用于 Cisco Unity 的《*Cisco Unified Communications Manager* 集成指南》或适用的用于 Cisco Unity Connection 的《*Cisco Unified Communications Manager SCCP* 集成指南》，位于：

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **应用程序用户**。

步骤 2 要选择现有用户，请在**查找用户位置**字段中指定合适的过滤器，并选择**查找**以检索用户列表，然后从列表中选择用户。

步骤 3 从**相关链接**下拉列表中，选择**创建 Cisco Unity 应用程序用户**链接并单击**转至**。
此时将显示**添加 Cisco Unity 用户**对话框。

步骤 4 从**应用服务器**下拉列表中，选择您要在其上创建 Cisco Unity 或 Cisco Unity Connection 用户的 Cisco Unity 或 Cisco Unity Connection 服务器，然后单击**下一步**。

步骤 5 从**应用程序用户模板**下拉列表中，选择您要使用的模板。

步骤 6 单击**保存**。
此时将在 Cisco Unity 或 Cisco Unity Connection 中创建管理员帐户。“相关链接”中的链接更改为**应用程序用户配置**窗口中的**编辑 Cisco Unity 用户**。现在，您可以查看您在 Cisco Unity 管理或 Cisco Unity Connection 管理中创建的用户。

更改应用程序用户密码

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **应用程序用户**。
此时将出现**查找并列出用户**窗口。

步骤 2 要选择现有用户，请在**查找用户位置**字段中指定合适的过滤器，并选择**查找**以检索用户列表，然后从列表中选择用户。
应用程序用户配置窗口将显示关于所选应用程序用户的信息。

步骤 3 在**密码**字段中，双击已加密的现有密码，然后输入新密码。

步骤 4 在**确认密码**字段中，双击已加密的现有密码，然后再次输入新密码。

步骤 5 单击**保存**。

管理应用程序用户密码凭证信息

执行以下程序管理应用程序用户密码的凭证信息。 这可让您执行管理任务，例如锁定密码、将凭证策略应用到密码，或查看信息，例如上次失败的登录尝试的时间。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **应用程序用户**。
此时将出现**查找并列出用户**窗口。

步骤 2 要选择现有用户，请在**查找用户位置**字段中指定合适的过滤器，并选择**查找**以检索用户列表，然后从列表中选择用户。
应用程序用户配置窗口将显示关于所选应用程序用户的信息。

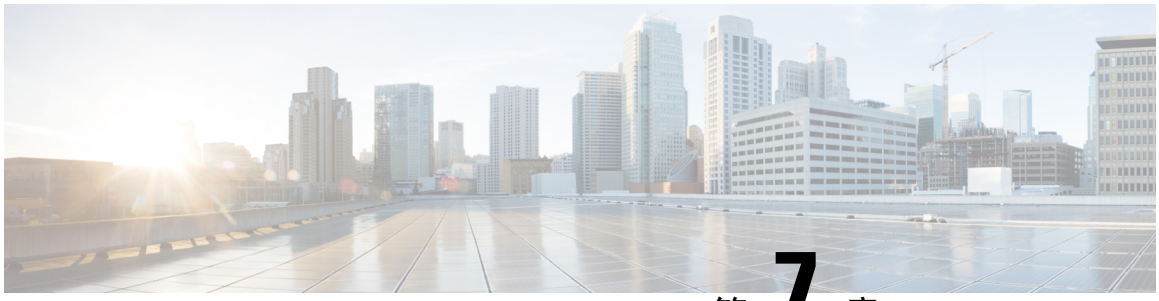
步骤 3 要更改或查看密码信息，请单击**密码**字段旁边的**编辑凭证**按钮。
随即会显示用户**凭证配置**。

步骤 4 配置**凭证配置**窗口中的字段。 请参阅联机帮助，了解有关字段及其配置选项的更多信息。

步骤 5 如果更改了任何设置，请单击**保存**。

第 III 部分

管理设备



第 7 章

管理电话

电话管理概述

本章介绍如何管理您网络中的电话。 各个主题介绍添加新电话、将现有电话移至另一个用户、锁定电话和重置电话等任务。

您的电话型号的《Cisco IP 电话管理指南》中包含特定于电话型号的配置信息。

电话按键模板

电话按键模板是基于电话型号创建的。 有些电话型号不使用任何特定的电话按键模板，但有些电话型号需要特定的模板，即单独的模板或设备默认模板。

企业参数配置页面上的**非尺寸安全电话的电话模板选择**和**自动注册传统模式**企业参数指定使用的电话按钮模板的类型。 请参阅联机帮助，获取有关字段的详细信息。

表 *4:* 不同场景下的电话按键模板

非尺寸安全电话的电话模板选择	自动注册传统模式	Phone
创建单个模板	假	通过通用设备模板添加电话时，系统会创建单个电话按键模板。
使用设备默认设置中的模板	假	不创建单个电话按键模板，它采用设备默认设置中的电话按键模板。
使用设备默认设置中的模板	真	设备池、电话模板、呼叫搜索空间、电话按键模板的值取自设备默认设置。

非尺寸安全电话的电话模板选择	自动注册传统模式	Phone
创建单个模板	真	设备池、电话模板、呼叫搜索空间、电话按键模板的值取自设备默认设置。 不创建单个模板。 自动注册传统模式具有优先权。

电话管理任务

过程

	命令或操作	目的
步骤 1	从有或没有最终用户的模板中新增电话，第 65 页	从有或没有最终用户的通用设备模板新增电话。
步骤 2	手动添加电话，第 64 页	为没有设备模板的最终用户新增电话。
步骤 3	从有最终用户的模板中新增电话，第 66 页	为最终用户添加新电话并分配通用设备模板。
步骤 4	移动现有电话，第 72 页	将已配置的电话移至不同的最终用户。
步骤 5	查找主动登录设备 ，第 72 页	搜索特定的设备，或列出用户主动登录的所有设备。
步骤 6	查找远程登录设备 ，第 73 页	搜索特定的设备，或列出用户远程登录的所有设备。
步骤 7	远程锁定电话，第 74 页	某些电话可以远程锁定。 当远程锁定电话时，电话将无法使用，直到您解锁。
步骤 8	将电话重置为出厂默认设置 ，第 74 页	将电话重置为出厂设置。
步骤 9	电话锁定/擦除报告 ，第 75 页	搜索已被远程锁定和/或远程重置为出厂默认设置的设备。
步骤 10	查看 LSC 状态并为电话生成 CAPF 报告，第 76 页	在电话上搜索 LSC 过期状态，同时生成 CAPF 报告。

手动添加电话

可以遵照以下程序为用户手动新增电话。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**设备** > **电话** > **查找并列出电话**。

步骤 2 在**查找并列出电话**页面，单击**新增**手动添加电话。

新增电话页面即会显示。

在**新增电话**页面，如果单击“单击此处以使用通用设备模板新增电话”超链接，页面将重定向到**新增电话**页面，从模板添加电话，添加或不添加用户均可。 有关详细信息，请参阅从有或没有最终用户的模板中新增电话，第 65 页。

步骤 3 从**电话类型**下拉列表中，选择电话型号。

步骤 4 单击**下一步**。
电话配置页面即会显示。

步骤 5 在**电话配置**页面的必填字段中输入值。 有关字段的详细信息，请参阅联机帮助。

有关“产品特定配置”区域中的字段的其他信息，请参阅您的电话型号对应的《*Cisco IP* 电话管理指南》。

步骤 6 单击**保存**以保存电话配置。

下一步做什么

将现有电话移至最终用户，第 50 页

从有或没有最终用户的模板中新增电话

执行以下程序从有或没有添加用户的模板中添加新电话。 Cisco Unified Communications Manager 会使用通用设备模板设置配置电话。

开始之前

确保已在 Cisco Unified Communications Manager 中配置通用设备模板。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**设备** > **电话** > **查找并列出电话**。

步骤 2 从**查找并列出电话**页面中，单击**从模板新增**以通过设备模板添加电话（添加或不添加最终用户）。

新增电话页面即会显示。

在**新增电话**页面上，如果单击“单击此处手动输入所有电话设置”超链接，页面会重定向到现有的**新增电话**页面以手动添加电话。 有关详细信息，请参阅手动添加电话，第 64 页。

步骤 3 从**电话类型**（**和协议**）下拉列表中，选择电话型号。

仅当电话支持多个协议时，才会显示协议下拉列表。

步骤 4 在**名称或 MAC 地址** 文本框中，输入名称或 MAC 地址。

步骤 5 从**设备模板**下拉列表中，选择一个通用设备模板。

步骤 6 从**目录号码**（**线路 1**）下拉列表中，选择一个目录号码。

如果下拉列表中的目录数目超出下拉列表最大限制，**查找**选项卡将显示。 单击**查找**，随即将打开一个弹出对话框，其中有“查找目录号码”条件。

步骤 7 （可选）如果想要创建新的目录号码并将其分配给设备，单击**新建**，输入目录号码，并选择一个通用线路模板。

或者，您可以使用关联了用户的目录号码创建电话，转到**用户管理**>**用户/电话添加**>**快速用户/电话添加**。

步骤 8 （可选）从**用户**下拉列表中，选择您要为其添加新电话的最终用户。

注释 必须为 Cisco 双模（移动）设备选择用户。

如果下拉列表中的最终用户数目超过下拉列表最大限制，会显示**查找**选项卡。 单击**查找**，随即将打开一个弹出对话框，其中有“查找最终用户”条件。

步骤 9 单击**添加**。

注释 对于非尺寸安全电话，系统会根据**企业参数配置**页面上的**非尺寸安全电话的电话模板选择**和**自动注册传统模式**参数选项，创建电话模板。

随即会显示添加成功的消息。 Cisco Unified Communications Manager 会添加电话，**电话配置**页面将显示。 有关**电话配置**页面上的字段的详细信息，请参阅联机帮助。

下一步做什么

将现有电话移至最终用户，第 50 页

从有最终用户的模板中新增电话

执行以下程序为最终用户添加新电话。

开始之前

要为其添加电话的最终用户拥有包含通用设备模板的用户配置文件设置。 Cisco Unified Communications Manager 会使用通用设备模板的设置配置电话。

- 最终用户管理任务，第 43 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **快速/用户电话添加**。

步骤 2 单击**查找**并选择您要为其添加新电话的最终用户。

步骤 3 单击**管理设备**。
将出现“管理设备”窗口。

步骤 4 单击**添加新电话**。
此时将显示“添加电话至用户”弹出窗口。

步骤 5 从**产品类型**下拉列表中，选择电话型号。

步骤 6 从**设备协议**下拉列表中，选择 SIP 或 SCCP 作为协议。

步骤 7 在**设备名称**文本框中，输入设备的 MAC 地址。

步骤 8 从**通用设备模板**下拉列表中，选择一个通用设备模板。

步骤 9 如果电话支持扩展模块，输入您要部署的扩展模块数量。

步骤 10 如果您想使用分机移动访问电话，选中**在分机移动中**复选框。

步骤 11 单击**添加电话**。
此时“添加新电话”弹出窗口会关闭。 Cisco Unified Communications Manager 会将电话添加至用户，并使用通用设备模板配置电话。

步骤 12 如果您想对电话配置进行其他编辑，单击对应的铅笔图标以在**电话配置**窗口中打开电话。

协作移动融合虚拟设备概述

CMC 设备是代表与其关联的远程目标的虚拟设备。 当企业电话呼叫 CMC 设备时，呼叫将被重定向到远程目标。此功能旨在创建一种与 Spark 远程设备完全相同的设备类型——**协作移动融合**，几乎不需要自定义，并具有以下优点。

- 支持 Cisco Unified Communications Manager 上的本机移动设备，其功能类似于 Spark 远程设备。
- 充分利用作为 Spark-RD 的优势，具备包括未来开发功能奇偶校验的功能。
- 允许针对特定于移动设备的用例进行自定义，例如将呼叫从移动设备转移到桌面电话、从桌面电话转移到移动设备。（在“标识”页面添加桌面接听计时器并通过产品支持功能设置启用）。
- 可将 CMC 设备加入寻线组。
- 能够使用 Spark 远程设备共享线路。
- 许可证 - 从许可证使用角度来看，算作一个单独的设备。 任何多设备许可证捆绑包都应支持 CMC-RD。

CMC RD 设备的许可调整

新 CMC 设备添加后，它将根据与用户关联的设备的数量/类型使用许可证。 CMC 设备使用的许可证类型取决于与其关联的最终用户的设备数量。

- 如果只部署 CMC 设备，请使用增强版许可证
- 如果部署 CMC 设备和 Spark RD，请使用增强版许可证

- 如果部署 CMC 和物理设备：超级增强版许可证
- 如果部署 CMC、Spark RD 和物理设备：超级增强版许可证

添加协作移动融合虚拟设备

以下程序可用于为最终用户添加 Cisco 协作移动融合 (CMC) 远程设备。

开始之前

您要为其添加电话的最终用户必须拥有包含通用设备模板的用户配置文件设置。 Cisco Unified Communications Manager 会使用通用设备模板的设置配置电话。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**设备** > **电话**。

步骤 2 单击**新增**按钮。

步骤 3 单击**单击此处手动输入所有电话设置**链接。
此时将出现**添加新电话**窗口。

步骤 4 从**电话类型**下拉列表中，选择 Cisco 协作移动融合，然后单击**下一步**。
此时将显示**电话配置**窗口。

步骤 5 从**所有者用户 ID** 下拉列表中，选择将拥有设备的最终用户。

步骤 6 从**设备池**下拉列表中选择设备池。

步骤 7 单击**保存**。
一则警告消息将弹出，单击**应用配置**按键以使更改生效。 单击**确定**。 设备即会成功添加。

步骤 8 要配置**目录号码**，请单击添加的 CMC 设备，输入**目录号码**，然后单击**保存**。

步骤 9 要为添加的 CMC 设备新增**远程目标**，请单击“标识”框中的链接。

步骤 10 在“远程目标配置”窗口中，输入**名称**和**目标号码**，然后单击**保存**。

注释 对于添加的一个 CMC 设备，只能添加一个远程目标。

步骤 11 要更新现有远程目标，请输入**新名称**，然后单击**保存**。

步骤 12 要删除现有远程目标，请单击菜单中的“删除”按钮。
此时将显示一条来自网页的消息，确认永久删除。 单击**确定**。

步骤 13 要从设备页面删除 CMC 设备，请选中**设备**复选框，然后从菜单中单击**删除选定项**。

CMC RD 功能交互

表 *5: CMC RD* 功能交互

功能	互动
共享线路处理	• 如果您采用的是具有关联的 CMC RD 和 Spark RD 的共享桌面电话，当用户从企业电话呼叫 CMC 设备 DN 时，这三者——CMC RD、Spark RD 和共享桌面电话——都会响铃。 • 从任何远程目标应答时，会在共享桌面电话上显示“远程使用中”的消息。 • 从任何共享桌面电话应答都将断开远程目标电话（CMC RD 和 Spark RD 电话）。
CMC 设备可在呼叫管理器组 (CMG) 设置中使用	• CMC 设备与呼叫管理器组关联时，它始终在主服务器上运行，并且仅当主服务器关闭时，在呼叫管理器组的下一个活动辅助服务器上运行。 • 如果主服务器在呼叫过程中中断，则正在进行的呼叫仍会保留，并且在呼叫结束后，CMC 设备会注册到辅助服务器。 注释 当呼叫处于保留模式时，电话之间的媒体仍保持活动状态，但除断开呼叫之外，无法执行其他操作。 • 如果主服务器最初关闭并且呼叫在CMC设备注册至辅助服务器时启动，然后主服务器在呼叫进行过程中出现，则呼叫将进入保留模式，并且呼叫结束后，CMC 设备会注册到主服务器。
呼叫固定	所有从CMC设备和号码到远程目标呼叫的基本来电都将固定在企业网络中。 在配置CMC远程设备后，用户可以从其移动设备发出和接收呼叫，并将所有呼叫固定到企业： • 用户可以从企业号码直接拨号到CMC远程目标。呼叫将锁定在企业网络中。 在这种情况下，桌面电话（CMC 设备的共享线路）不会振铃，而是继续保持**远程使用中**状态。 • 用户可以从CMC远程目标拨号到任何企业号码。呼叫将锁定。在这种情况下，桌面电话（CMC设备的共享线路）会继续保持**远程使用中**状态。

功能	互动
单一号码连系	• 在“远程目标配置”页面中，如果不选中**启用一号通**复选框，呼叫不会扩展到 CMC RD，且呼叫会被拒。 • 无论是否勾选**启用一号通复选框**，从远程目标传入的来电和出站的**远程目标号码**呼叫都不受影响。 • 如果有与CMC设备共享的桌面电话，并且不选中**启用一号通**复选框，则呼叫将扩展至共享桌面电话，而不是转到 CMC RD。 **注释** 如果**一号通语音邮件策略**设置为**用户控制**，在**盲转接**到主分机的情况下，系统**不会**触发移动目标号码。 系统只会触发主分机。 **用户控制**设置支持咨询转接。 **计时器控制**语音邮件回避策略支持咨询和盲转接。
基于每天定时 (ToD) 的呼叫路由	• 您可以使用远程目标的每日定时配置来设置振铃计划（举例来说，您可以配置特定的时间，如周一至周五上午 9 点到下午 5 点）。 呼叫只会在这些时间重定向到您的远程目标。 从企业电话到CMC号码的呼叫将根据“远程目标配置”页面中固定的振铃计划路由。 可按如下方式指定振铃计划： • **所有时间** — 所有时间都会路由呼叫。 没有任何限制。 • **每周的一天** – 仅在所选的特定日期路由呼叫。 • **特定时间** – 仅在所选的办公时间内路由呼叫。 请确保选择时区。 • 在振铃计划期间收到呼叫时，从企业电话到CMC号码的呼叫将根据“远程目标配置”页面的允许访问列表或阻止访问列表中添加的呼叫号码或模式进行路由。 • **允许访问列表** - 仅当允许访问列表中包含主叫方号码或模式时，目标才会振铃。 • **阻止访问列表** - 如果阻止访问列表中包含主叫方号码或模式，目标不振铃。 **注释** 在任何时间点，只能使用允许访问列表或阻止访问列表。

功能	互动
用户区域设置	CMC 虚拟设备使用在“电话配置”窗口中配置的区域设置来确定电话显示和电话通知的区域设置。 此策略适用于常规呼叫以及 Conference Now 号码呼叫。 对于通知部分，在“用户区域设置”设置中选择相同语言的主叫（任何企业电话）和被叫（CMC 设备）电话时，主叫和远程目标上的通知基于在“电话配置”页面中选择的用户区域设置。 注释 例如，从与 CMC 设备关联的**远程目标**呼叫 **Conference Now 号码**时，通知基于在 CMC 设备的“电话配置”页面选择的用户区域设置。
HLogin 和 HLogout 的新访问代码	此功能可帮助管理员使用添加的服务参数为 CMC 设备设置寻线组登录和注销号码： • 用于登录寻线组的企业功能访问号码。 • 用于注销寻线组的企业功能访问号码。 如果用户从与 CMC 设备关联的 RD 输入 Hlogin 号码，只有在拨打与 CMC 设备关联的寻线引导号码时，呼叫才会被重定向到 RD。 如果用户从与 CMC 设备关联的 RD 输入 Hlogout 号码，在拨打与 CMC 设备关联的寻线引导号码时，呼叫不会被重定向到 RD。 默认情况下，CMC 设备为 Hloggedin。 两种情况下，对 CMC 设备的直接呼叫都不受影响。
基于数据库中配置的**振铃计时器之前的延迟**的 CMC 远程目标呼叫分机	**如果数据库中振铃计时器之前的延迟配置为 5000** • 从企业电话呼叫 CMC 号码时，共享线路会振铃，并且呼叫在五秒后到达远程目标。 • 从企业电话呼叫 CMC 号码时，如果共享线路在五秒钟前应答呼叫，呼叫不会扩展到远程目标。 • 从企业电话呼叫 CMC 号码时，共享线路会振铃，如果主叫方在五秒钟之前断开呼叫，呼叫不会扩展到远程目标。 **如果数据库中振铃计时器之前的延迟配置为 0** 从企业电话呼叫 CMC 号码时会同时警告远程目标和共享线路。
批量管理工具 (BAT) 支持	为 CMC 设备提供 BAT 支持

CMC RD 功能限制

表 *6: CMC RD* 功能限制

功能	限制
CMC 远程目标关联	以下限制适用： • 您只能将一台 CMC 设备关联到一个远程目标。 . • 如果删除最终用户，其关联的 CMC 设备和 RD（远程目标）也会删除。 注释 即使选中或取消选中**启用移动性**复选框，CMC 和 RD 也不会受到影响。 CMC 设备不会删除。 注释 Cisco Unified Communications Manager 不支持 CMC 设备的呼叫处理保留。

移动现有电话

执行以下程序将已配置的电话移至最终用户。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **快速用户/电话添加**。
步骤 2 单击**查找**并选择您要向其移动现有电话的用户。
步骤 3 单击**管理设备**按键。
步骤 4 单击**查找要移至此用户的电话**按键。
步骤 5 选择您想要移至此用户的电话。
步骤 6 单击**移动选定项**。

查找主动登录设备

Cisco 分机移动和 Cisco 跨群集分机移动功能记录用户主动登录的设备。对于 Cisco 分机移动功能，主动登录的设备报告跟踪本地用户主动登录的本地电话；对于 Cisco 跨群集分机移动功能，主动登录设备报告跟踪远程用户主动登录的本地电话。

Unified Communications Manager 提供特定的搜索窗口用于搜索用户登录的设备。按照这些步骤搜索特定的设备，或列出用户主动登录的所有设备。

过程

步骤 1 选择**设备** > **电话**。

步骤 2 从右上角的**相关链接**下拉列表中选择**主动登录设备报告**，并单击**转至**。

步骤 3 要查找数据库中所有主动登录设备记录，请确保对话框为空，并转至步骤 4。

要过滤或搜索记录：

a) 从第一个下拉列表中选择搜索参数。
b) 从第二个下拉列表中选择搜索模式。
c) 如果适用，指定适当的搜索文本。

注释 要添加其他搜索条件，请单击 + 按键。 添加条件时，系统将搜索与您指定的所有条件匹配的记录。 要删除条件，请单击 - 按键删除最后添加的条件，或单击**清除过滤器**按键删除所有已添加的搜索条件。

步骤 4 单击**查找**。

此时将显示所有相匹配的记录。 在“每页行数”下拉列表中选择不同的值，可以更改每个页面中显示的项目数量。

步骤 5 从显示的记录列表中，单击要查看的记录的链接。

注释 要反转排序顺序，请单击列表标题中的向上或向下箭头（如果可用）。

窗口中将显示您选择的项目。

查找远程登录设备

Cisco 跨群集分机移动功能记录用户远程登录的设备。 远程登录设备报告跟踪其他群集所拥有但通过使用 EMCC 功能的本地用户主动登录的电话。

Unified Communications Manager 提供特定的搜索窗口，用于搜索用户远程登录的设备。 按照以下步骤搜索特定设备，或列出用户远程登录的所有设备。

过程

步骤 1 选择**设备** > **电话**。

步骤 2 从右上角的**相关链接**下拉列表中选择**远程登录设备**，并单击**转至**。

步骤 3 要查找数据库中所有远程登录设备记录，请确保对话框为空，并转至步骤 4。

要过滤或搜索记录：

a) 从第一个下拉列表中选择搜索参数。
b) 从第二个下拉列表中选择搜索模式。
c) 如果适用，指定适当的搜索文本。

注释　要添加其他搜索条件，请单击 + 按键。 添加条件时，系统将搜索与您指定的所有条件匹配的记录。 要删除条件，请单击 **(** - **)** 按键删除最后添加的条件，或单击“清除过滤器”按键删除所有已添加的搜索条件。

步骤 4 单击**查找**。

此时将显示所有相匹配的记录。 在“每页行数”下拉列表中选择不同的值，可以更改每个页面中显示的项目数量。

步骤 5 从显示的记录列表中，单击要查看的记录的链接。

注释　要反转排序顺序，请单击列表标题中的向上或向下箭头（如果可用）。

窗口中将显示您选择的项目。

远程锁定电话

某些电话可以远程锁定。 当远程锁定电话时，电话将无法使用，直到您解锁。

如果电话支持远程锁定功能，右上角会显示**锁定**按钮。

过程

步骤 1 选择**设备** > **电话**。

步骤 2 从**查找并列出电话**窗口中，输入搜索条件并单击**查找**以查找特定电话。

此时将显示与搜索条件匹配的电话列表。

步骤 3 选择您要远程锁定的电话。

步骤 4 在**电话配置**窗口中，单击**锁定**。

如果电话未注册，将会显示一个弹出窗口，通知您下次注册电话之后将会锁定该电话。 单击**锁定**。

此时将显示**设备锁定/擦除状态**部分，其中包含有关最新请求、它是否挂起以及最新确认的信息。

将电话重置为出厂默认设置

有些电话支持远程擦除功能。 当您远程擦除电话时，该操作会将电话重置为出厂设置。 电话上以前存储的所有内容均被擦除。

如果电话支持远程擦除功能，右上角会显示**擦除**按钮。

⚠

注意 此操作无法撤消。 只有当您确定要将电话重置为出厂设置时，才应执行此操作。

过程

步骤 1 选择**设备** > **电话**。

步骤 2 在**查找并列出电话**窗口中，输入搜索条件并单击**查找**以查找特定电话。

此时将显示与搜索条件匹配的电话列表。

步骤 3 选择您要远程擦除的电话。

步骤 4 在**电话配置**窗口中，单击**擦除**。

如果电话未注册，将会显示一个弹出窗口，通知您下次注册电话之后将会擦除该电话。 单击**擦除**。

此时将显示**设备锁定/擦除状态**部分，其中包含有关最新请求、它是否挂起以及最新确认的信息。

电话锁定/擦除报告

Unified Communications Manager 提供一个特定搜索窗口，用于搜索已被远程锁定和/或远程擦除的设备。 按照以下步骤搜索某个特定设备或列出已被远程锁定和/或远程擦除的所有设备。

过程

步骤 1 选择**设备** > **电话**。

此时将显示“查找并列出电话”窗口。 窗口中可能还会显示当前（之前）查询的记录。

步骤 2 从窗口右上角的**相关链接**下拉列表中选择**电话锁定/擦除报告**，然后单击**转至**。

步骤 3 要在数据库中查找所有远程锁定或远程擦除的设备记录，请确保该文本框为空；转至步骤 4。

要过滤或搜索特定设备的记录：

a) 从第一个下拉列表中选择要搜索的操作类型。
b) 从第二个下拉列表中选择搜索参数。
c) 从第三个下拉列表中选择搜索模式。
d) 如果适用，指定适当的搜索文本。

注释 要添加其他搜索条件，请单击 + 按键。 添加条件时，系统将搜索与您指定的所有条件匹配的记录。 要删除条件，请单击 - 按键删除最后添加的条件，或单击“清除过滤器”按键删除所有已添加的搜索条件。

步骤 4 单击**查找**。

此时将显示所有相匹配的记录。 在“每页行数”下拉列表中选择不同的值，可以更改每个页面中显示的项目数量。

步骤 5 从显示的记录列表中，单击要查看的记录的链接。

注释 要反转排序顺序，请单击列表标题中的向上或向下箭头（如果可用）。

窗口中将显示您选择的项目。

查看 LSC 状态并为电话生成 CAPF 报告

使用此程序以从 Cisco Unified Communications Manager 界面监控当地有效证书 (LSC) 到期信息。 以下搜索过滤器显示 LSC 信息：

- LSC 过期 — 在电话上显示 LSC 到期日期。
- LSC 颁发者 — 显示颁发机构的名称，可以是 CAPF 或第三方。
- LSC 颁发机构过期日期 — 显示颁发机构的到期日期。

注释 当新设备上没有颁发的LSC时，**LSC 过期**和**LSC 颁发机构过期日期**字段的状态设置为“不可用”。

当 LSC 在升级到 Cisco Unified Communications Manager 11.5(1) 之前颁发给设备时，**LSC 过期**和 **LSC 颁发机构过期日期**字段的状态设置为“未知”。

过程

步骤 1 选择**设备** > **电话**。

步骤 2 从第一个**查找电话条件**下拉列表中，选择以下条件之一：

- LSC 过期
- LSC 颁发者
- LSC 颁发机构过期日期

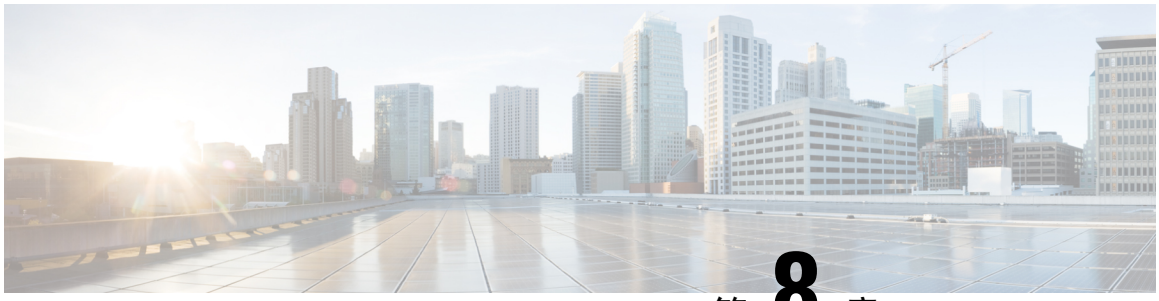
从第二个**查找电话条件**下拉列表中，选择以下条件之一：

- 之前
- 精确等于
- 之后
- 开头为
- 包含

- 结尾为
- 精确等于
- 空白
- 非空白

步骤 3 单击**查找**。
此时将显示发现的电话列表。

步骤 4 在**相关链接**下拉列表中，选择**文件中的 CAPF 报告**，然后单击**转至**。
随即会下载报告。



第 8 章

管理设备固件

设备固件更新概述

设备加载是设备的软件和固件，例如 IP 电话、telepresence 系统，以及其他由 Cisco Unified Communications Manager 部署并注册到 Cisco Unified Communications Manager 的设备。 安装或升级期间，Cisco Unified Communications Manager 包括基于 Cisco Unified Communications Manager 版本的发布时间可用的最新加载。 Cisco 会定期发布更新的固件，以引入新功能和软件修补程序。您可能希望将电话更新到较新的加载，而无需等待包含该加载的 Cisco Unified Communications Manager 升级。

新加载所需的文件必须位于终端可以访问的位置以供下载，终端才可以升级到新版本的软件。 最常用的位置是已激活 Cisco TFTP 服务的 Cisco UCM 节点，称为 “TFTP 服务器”。 某些电话也支持使用备用下载位置，称为“负载服务器”。

如果您想在任何服务器上获得列表、查看或下载已经在 tftp 目录中的文件，可以使用 CLI 命令 file list tftp 查看 TFTP 目录中的文件，使用 file view tftp 查看文件，以及使用 file get tftp 获取 TFTP 目录中文件的副本。 有关详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面参考指南》。 您也可以使用 Web 浏览器，转到 URL “http://<tftp_server>:6970/<filename>” 下载任何 TFTP 文件。

提示 您可以在将新的加载配置为系统范围默认设置之前，将其应用到一台设备。 此方法对于测试用途十分有用。 但是，请记住，该类型的所有其他设备使用旧加载，直至您使用新加载更新系统范围默认设置。

安装设备包或单个固件

安装设备包以引入新的电话类型，并为多个电话型号升级固件。

- 可以使用以下选项安装或升级现有设备的单个固件：Cisco Options Package (COP) 文件 — COP 文件包含固件文件和数据库更新，因此当安装在发布方上时，除了安装固件文件以外，还会更新默认固件。
- 仅固件文件 — 它在一个 zip 文件中提供，包含应手动提取并上传到 TFTP 服务器上相应目录的单独的设备固件文件。

注释 有关特定于 COP 或固件文件包的安装说明，请参阅自述文件。

过程

步骤 1 从 Cisco Unified 操作系统管理，选择**软件升级** > **安装/升级**。

步骤 2 在“软件位置”部分中填写适当的值，然后单击**下一步**。

步骤 3 在**可用软件**下拉列表中，选择设备包文件，然后单击**下一步**。

步骤 4 验证 MD5 值正确，然后单击**下一步**。

步骤 5 在警告框中，验证您已选择正确的固件，然后单击**安装**。

步骤 6 检查您是否收到一条成功消息。

注释 如果要重新启动群集，则跳过步骤 8。

步骤 7 在服务运行的所有节点上重新启动 **Cisco TFTP** 服务。

步骤 8 重置受影响的设备以将设备升级到新加载。

步骤 9 从 Cisco Unified CM 管理中，选择**设备** > **设备设置** > **设备默认值**，然后将加载文件（或特定设备）的名称手动更改为新加载。

步骤 10 单击**保存**，然后重置设备。

步骤 11 在所有群集节点上重新启动 **Cisco Tomcat** 服务。

步骤 12 执行下列操作之一：

- 如果您运行的是 11.5(1)SU4 或更低版本、12.0(1) 或者 12.0(1)SU1，请重新启动群集。
- 如果您在 11.5(1)SU5 或更高版本上运行 11.5(x) 发行版，或者在 12.0(1)SU2 或更高发行版上运行更高版本，请在发布方节点上重新启动 **Cisco CallManager** 服务。 但是，如果您仅在订阅方节点上运行 **Cisco CallManager** 服务，可以跳过此任务。

潜在的固件安装问题

以下是您在安装设备包后可能会遇到的一些潜在问题：

问题	原因/解决办法
新设备无法注册	出现这种情况的原因可能是设备类型不匹配。 这可能是由以下原因引起的： • 在“电话配置”窗口中添加设备时使用的设备类型错误。 例如，选择 Cisco DX80 作为电话类型，而不是 Cisco TelePresence DX80。 使用正确的设备类型重新配置设备。 • **Cisco CallManager** 服务不知道新的设备类型。 这种情况下，请在发布方节点上重新启动 **Cisco CallManager** 服务。
终端不升级到新固件	可能的原因： • TFTP 服务器上未安装设备包。 结果，固件无法通过电话下载。 • **Cisco TFTP** 服务在安装后未重新启动，因此服务不知道新文件。 请确保在 TFTP 服务器上安装设备包。
Cisco Unified CM 管理中的“电话配置”窗口显示断开的链接，其中图标图像应用于新的设备类型	通过 CLI 在所有节点上重新启动 **Cisco Tomcat** 服务。
终端固件下载中途失败，整个下载重新启动或下载看起来很慢。 **重要事项** 适用于 14SU1 及更高版本。	可能的原因： 这可能是由于网络问题或拥塞造成的，并且可能在批量升级情况下更为普遍。 如果您运行的是 14SU1，可能会受益于 TFTP 和代理 TFTP 上的 HTTP 范围请求 (RFC7233) 支持（如果下载文件至少为 100MB）。 支持 HTTP 范围请求的终端可以受益于更高的可靠性和更快的下载速度，尤其是在批量进行电话升级或者网络状况不佳的情况下。 HTTP 范围请求应允许下载暂停和恢复；也就是说，中断的下载可以从最后一个已知的成功字节范围继续，而无需再次重新启动整个下载。 Cisco Webex 840 和 860 无线电话支持 RFC7233。 不支持 RFC7233 的设备不受此功能影响。

从系统中删除未使用的固件

设备加载管理窗口允许您从系统中删除未使用的固件（设备加载）和关联的文件以增加磁盘空间。例如，您可以在升级之前删除未使用的加载，以防升级因磁盘空间不足而失败。 某些固件文件可能有**设备加载管理**窗口中未列出的从属文件。当您删除一个固件时，从属文件也会被删除。但是，如果从属文件与其他固件相关联，则不会被删除。

注释 您必须为群集中的每台服务器分别删除未使用的固件。

开始之前

注意 删除未使用的固件之前，确保您正在删除正确的加载。 如果不执行整个群集的DRS恢复，则无法恢复已删除的加载。 我们建议您在删除固件之前进行备份。

确保不要删除使用多个文件负载的设备的文件。 例如，某些CE终端使用多个负载。 但是，在**设备负载管理**窗口中只会将一个负载称为**使用中**。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**软件升级** > **设备加载管理**。

步骤 2 指定搜索条件，然后单击**查找**。

步骤 3 选择要删除的设备加载。 如果需要，您可以选择多个加载。

步骤 4 单击**删除选定加载**。

步骤 5 单击**确定**。

为电话型号设置默认固件

使用此程序为特定电话型号设置默认固件加载。 当一部新电话注册时，Cisco Unified Communications Manager会尝试将默认固件发送到电话，除非电话配置具有在**电话配置**窗口中指定的覆盖固件加载。

注释 对于单独的电话，**电话配置**窗口中**电话负载名称**字段的设置会覆盖该特定电话的默认固件加载。

开始之前

确保固件加载到了 TFTP 服务器上。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**设备** > **设备设置** > **设备默认值**。
随即会出现**设备默认值配置**窗口，其中显示 Cisco Unified Communications Manager 支持的各种电话型号的默认固件加载。 固件显示在**加载信息**列。

步骤 2 在**设备类型**下方，找到您要为其分配默认固件的电话型号。

步骤 3 在随同的**加载信息**字段中，输入固件负载。

步骤 4 （可选）输入该电话型号的默认**设备池**和默认**电话模板**。

步骤 5 单击**保存**。

为电话设置固件加载

使用此程序为特定电话分配固件加载。 如果您想使用与**设备默认值配置**窗口中指定的默认设置不同的固件加载，不妨执行此操作。

注释 如果想要为许多电话分配一个版本，可以利用批量管理工具，使用CSV文件或查询配置**电话负载名称**字段。 有关详细信息，请参阅《*Cisco Unified Communications Manager* 批量管理指南》。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**设备** > **电话**。

步骤 2 单击**查找**并选择单部电话。

步骤 3 在**电话负载名称**字段中，输入固件组的名称。 对于此电话，在这里指定的固件加载会覆盖在**设备默认值配置**窗口中指定的默认固件加载。

步骤 4 在**电话配置**窗口填写其余的任何字段。 有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 5 单击**保存**。

步骤 6 单击**应用配置**以将更改后的字段推送到电话。

使用负载服务器

如果您希望电话从非TFTP服务器的一台服务器下载固件更新，可以在电话的**电话配置**页面配置“负载服务器”。 负载服务器可能是另一台 Cisco Unified Communications Manager 或第三方服务器。 第三方服务器必须能够通过 TCP 端口 6970（推荐）上的 HTTP 或基于 UDP 的 TFTP 协议提供电话请求的任何文件。 某些电话型号，例如 DX 系列 Cisco TelePresence 设备，仅支持使用 HTTP 进行固件更新。

注释 如果想要为许多电话分配负载服务器，可以利用批量管理工具，使用CSV文件或查询配置**负载服务器**字段。 有关详细信息，请参阅《*Cisco Unified Communications Manager* 批量管理指南》。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**设备** > **电话**。

步骤 2 单击**查找**并选择单部电话。

步骤 3 在**负载服务器**字段中，输入备用服务器的 IP 地址或主机名。

步骤 4 在**电话配置**窗口填写其余的任何字段。 有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 5 单击**保存**。

步骤 6 单击**应用配置**以将更改后的字段推送到电话。

查找具有非默认固件加载设置的设备

通过 Unified Communications Manager 中的“固件加载信息”窗口，您可以快速找到没有使用其设备类型默认固件加载设置的设备。

注释 每个设备均可用单独分配的固件加载设置覆盖默认值。

使用以下程序以查找没有使用默认固件加载设置的设备。

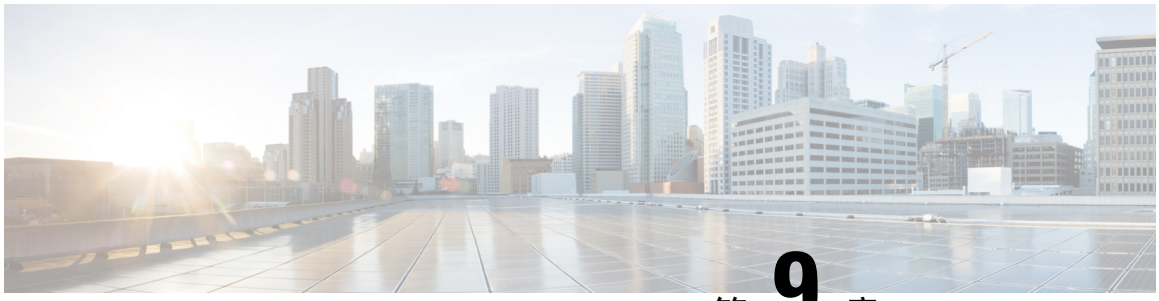
过程

步骤 1 选择**设备** > **设备设置** > **固件加载信息**。

页面将更新以显示需要固件加载设置的设备类型列表。 对于每种设备类型，“未使用默认加载设置的设备”列链接至使用非默认加载设置的任何设备的配置设置。

步骤 2 要查看使用非默认设备加载设置的特定设备类型的设备列表，请单击“未使用默认加载设置的设备”列中该设备类型的条目。

打开的窗口将列出未运行默认设备加载设置的特定设备类型的设备。



第 9 章

管理基础设施设备

管理基础设施概述

本章提供任务以管理网络基础设施设备，例如作为位置感知功能一部分的交换机和无线访问点。 当启用位置感知时，Cisco Unified Communications Manager 数据库会保存您网络中交换机和访问点的状态信息，包括目前关联到每个交换机或访问点的终端的列表。

终端到基础设施设备的映射可帮助 Cisco Unified Communications Manager 和 Cisco Emergency Responder 确定主叫方的物理位置。 例如，如果一个移动客户端在漫游情况下发出紧急呼叫，Cisco Emergency Responder 会使用映射来确定要将紧急服务发送到何处。

存储在数据库中的基础设施信息也有助于您监控基础设施使用情况。 从 Unified Communications Manager 界面，您可以查看网络基础设施设备，例如交换机和无线访问点。 您还可以查看当前关联至特定访问点或交换机的终端的列表。 如果基础设施设备未在使用，您可以停用对基础设施设备的跟踪。

管理基础设施先决条件

您必须先配置“位置感知”功能，才能在 Cisco Unified Communications Manager 界面内管理无线基础设施。 对于您的有线基础设施，该功能默认启用。

有关配置详细信息，请参阅 Cisco Unified Communications Manager 功能配置指南中的“配置位置感知”一章。

您还必须安装您的网络基础设施。 有关详细信息，请参阅您的基础设施设备（例如无线局域网控制器、访问点和交换机）随附的硬件文档。

管理基础设施任务流程

完成以下任务以监控和管理您的网络基础设施设备。

过程

	命令或操作	目的
步骤 1	查看基础设施设备的状态， 第 86 页	获取无线访问点或以太网交换机的当前状态，包括关联终端的列表。
步骤 2	禁用对基础设施设备的跟踪， 第 86 页	如果您有未使用的交换机或访问点，将设备标记为非活动。 系统将停止更新基础设施设备的状态或关联终端的列表。
步骤 3	激活对已禁用基础设施设备的跟踪， 第 87 页	启动对非活动基础设施设备的跟踪。 Cisco Unified Communications Manager 会开始使用基础设施设备的状态和关联终端的列表更新数据库。

查看基础设施设备的状态

使用此程序获取基础设施设备（例如无线访问点或以太网交换机）的当前状态。 在 Cisco Unified Communications Manager 界面中，您可以查看访问点或交换机的状态，并可看到关联终端的当前列表。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**高级功能** > **设备位置跟踪服务** > **交换机和访问点**。

步骤 2 单击**查找**。

步骤 3 单击您要查看状态的交换机或访问点。
交换机和访问点配置窗口会显示当前状态，包括当前关联到该访问点或交换机的终端的列表。

禁用对基础设施设备的跟踪

使用此程序删除对特定基础设施设备（例如交换机或访问点）的跟踪。 您可能希望对未使用的交换机或访问点执行此操作。

注释 如果删除对基础设施设备的跟踪，设备将保留在数据库中，但会变为非活动状态。 Cisco Unified Communications Manager 将不会再更新设备的状态，包括关联到基础设施设备的终端的列表。 您可以从**交换机和访问点**窗口的**相关链接**下拉列表中查看非活动的交换机和访问点。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**高级功能** > **设备位置跟踪服务** > **交换机和访问点**。

步骤 2 单击**查找**并选择您想要停止跟踪的交换机或访问点。

步骤 3 单击**禁用选定项**。

激活对已禁用基础设施设备的跟踪

使用此程序启动对已被禁用的非活动基础设施设备的跟踪。 一旦交换机或访问点变为活动状态，Cisco Unified Communications Manager 将开始动态跟踪状态，包括关联至交换机或访问点的终端列表。

开始之前

必须配置位置感知。 有关详细信息，请参阅 *Cisco Unified Communications Manager* 系统配置指南的“位置感知”一章。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**高级功能** > **设备位置跟踪服务** > **交换机和访问点**。

步骤 2 从**相关链接**中，选择**非活动交换机和访问点**，然后单击**转至**。
查找并列出非活动交换机和访问点窗口中将显示未被跟踪的基础设施设备。

步骤 3 选择您要为其启动跟踪的交换机或访问点。

步骤 4 单击**重新激活选定项**。

第 IV 部分

管理系统

第 10 章

监控系统状态

查看群集节点状态

使用此程序显示群集中节点的信息。

过程

步骤 1 从“Cisco Unified 操作系统管理”中，选择**显示** > **群集**。

步骤 2 查看**群集**窗口中的字段。 请参阅联机帮助，获取有关字段的详细信息。

查看硬件状态

使用此程序可显示硬件状态和有关您系统中的硬件资源的信息。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**显示** > **硬件**。

步骤 2 查看**硬件状态**窗口中的字段。 请参阅联机帮助，获取有关字段的详细信息。

查看网络状态

使用此程序显示您系统的网络状态，例如以太网和 DNS 信息。

显示的网络状态信息取决于是否已启用“网络容错”：

- 如果启用了“网络容错”，则当以太网端口 0 失败时，以太网端口 1 将自动管理网络通信。
- 如果启用了“网络容错”，将会显示网络端口以太网 0、以太网 1 和绑定 0 的网络状态信息。
- 如果未启用“网络容错”，仅会显示以太网 0 的状态信息。

过程

步骤 1 从“Cisco Unified 操作系统管理”中，选择**显示** > **网络**。

步骤 2 查看**网络配置**窗口中的字段。 请参阅联机帮助，获取有关字段的详细信息。

查看已安装的软件

使用此程序显示有关软件版本和已安装软件包的信息。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**显示** > **软件**。

步骤 2 查看**软件包**窗口中的字段。 请参阅联机帮助，获取有关字段的详细信息。

查看系统状态

使用此程序显示整体系统状态，例如区域设置、运行时间、CPU 使用率和内存使用量的相关信息。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**显示** > **系统**。

步骤 2 查看**系统状态**窗口中的字段。 请参阅联机帮助，获取有关字段的详细信息。

查看 IP 首选项

使用此程序显示系统可用的注册端口列表。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**显示** > **IP 首选项**。

步骤 2 （可选） 要过滤或搜索记录，请执行以下任务之一：

- 从第一个列表中，选择搜索参数。
- 从第二个列表中，选择搜索模式。
- 如果适用，指定适当的搜索文本。

步骤 3 单击**查找**。

步骤 4 查看显示在**系统状态**窗口中的字段。 请参阅联机帮助，获取有关字段的详细信息。

查看最后一次登录的详细信息

当最终用户（利用本地或 LDAP 凭证）和管理员登录到 Cisco Unified Communications Manager 或 IM and Presence Service 的 Web 应用程序时，主应用程序窗口会显示最后一次成功和失败登录的详细信息。

使用 SAML SSO 功能登录的用户只能查看最后一次成功的系统登录信息。 用户可以参考身份提供程序 (IdP) 应用程序以跟踪不成功的 SAML SSO 登录信息。

以下 Web 应用程序会显示登录尝试信息：

- Cisco Unified Communications Manager：
  - Cisco Unified CM 管理
  - Cisco Unified 报告
  - Cisco Unified 功能配置
- IM and Presence Service

- Cisco Unified CM IM and Presence 管理
- Cisco Unified IM and Presence 报告
- Cisco Unified IM and Presence 功能配置

只有管理员可以在 Cisco Unified Communications Manager 中登录并查看以下 Web 应用程序的最后一次登录详细信息：

- 灾难恢复系统
- Cisco Unified OS 管理

Ping 节点

使用 Ping 实用程序来 ping 网络中的另一个节点。 这些结果可帮助您检验或排查设备连接性故障。

过程

步骤 1 从“Cisco Unified 操作系统管理”中，选择**服务** > **Ping**。

步骤 2 配置 **Ping 配置**窗口中的字段。 请参阅联机帮助，了解有关字段及其配置选项的更多信息。

步骤 3 选择 **Ping**。

屏幕上会显示 ping 结果。

显示服务参数

您可能需要比较属于群集中所有服务器上某一特定服务的所有服务参数。 您可能还需要仅显示不同步参数（也就是说，一个服务器与另一个服务器值不同的服务参数）或从建议的值进行修改的参数。

使用以下程序以显示群集中所有服务器上特定服务的服务参数。

过程

步骤 1 选择**系统** > **服务参数**。

步骤 2 从“服务器”下拉列表框中选择服务器。

步骤 3 从“服务”下拉列表框中，选择您要在群集中所有服务器上显示服务参数的服务。

注释 “服务参数配置”窗口显示所有服务（活动或不活动）。

步骤 4 在显示的“服务参数配置”窗口中，在“相关链接”下拉列表框中选择“所有服务器的参数”；然后单击“转至”。

此时将显示“所有服务器的参数”窗口。对于当前服务，该列表按字母顺序显示所有参数。对于每个参数，建议值显示在参数名称旁边。在每个参数名称下，都会显示包含此参数的服务器列表。 在每个服务器名称旁边，显示此参数在此服务器上的当前值。

对于指定的参数，单击服务器名称或当前参数值，链接至相应的服务参数窗口更改该值。 单击“上一个”和“下一个”在“所有服务器的参数”窗口之间导航。

步骤 5 如果您需要显示不同步的服务参数，在“相关链接”下拉列表框中选择“所有服务器的不同步参数”，然后单击“转至”。

此时将显示“所有服务器的不同步参数”窗口。 对于当前服务，在不同服务器上有不同值的服务参数将按字母顺序显示。 对于每个参数，建议值显示在参数名称旁边。在每个参数名称下，都会显示包含此参数的服务器列表。 在每个服务器名称旁边，显示此参数在此服务器上的当前值。

对于指定的参数，单击服务器名称或当前参数值，链接至相应的服务参数窗口更改该值。 单击“上一个”和“下一个”在“所有服务器的不同步参数”窗口之间导航。

步骤 6 如果您需要显示从建议值进行修改的服务参数，在“相关链接”下拉列表框中选择“所有服务器的已修改参数”；然后单击“转至”。

此时将显示“所有服务器的已修改参数”窗口。 对于当前服务，与建议值有不同值的服务参数将按字母顺序显示。 对于每个参数，建议值显示在参数名称旁边。在每个参数名称下，都会显示一个服务器列表，这些服务器的值与建议的值不同。 在每个服务器名称旁边，显示此参数在此服务器上的当前值。

对于指定的参数，单击服务器名称或当前参数值，链接至相应的服务参数窗口更改该值。 单击“上一个”和“下一个”在“所有服务器的已修改参数”窗口之间导航。

配置网络 DNS

此程序用于设置网络 DNS

注释 您也可以在 Cisco Unified CM 管理中通过“DHCP 配置”窗口分配 DNS 主服务器和辅助服务器。

过程

步骤 1 登录到命令行界面。

步骤 2 如果要分配 DNS 服务器，请在发布方节点上运行以下命令之一：

- 分配首选 DNS 服务器：**run set network dns primary <ip_address>**

- 分配辅助 DNS 服务器：**run the set network dns secondary <ip_address>**

步骤 3 分配额外的 DNS 选项：**run the set network dns options [timeout| seconds] [attempts| number] [rotate].**

- Timeout 设置 DNS 超时
- Seconds 是超时的秒数
- Attempts 设置尝试 DNS 请求的次数
- Number 指定尝试次数
- Rotate 使系统在配置的 DNS 服务器之间循环并分配负载

例如，set network dns options timeout 60 attempts 4 rotate

运行此命令后，服务器将重新启动。

第 11 章

警报

概述

Cisco Unified 功能配置和 Cisco Unified IM and Presence 功能配置警报提供有关运行时状态和系统状态的信息，以便您能够对与系统有关的问题进行故障诊断；例如，确定灾难恢复系统。 警报信息包含说明和建议的操作，还包含应用程序名称、计算机名称等等，可帮助您执行故障诊断并且也适用于群集。

您可将警报接口配置为将警报信息发送到多个位置，并且每个位置可具有其自己的警报事件级别（从调试到危急）。 您可以将警报指向系统日志查看器（本地系统日志）、系统日志文件（远程系统日志）、SDL 跟踪日志文件（仅限 Cisco CallManager 和 CTIManager 服务）或所有目标。

服务发出警报时，警报接口会将警报信息发送到您所配置并在警报定义的路由列表中指定的位置（例如，SDI 跟踪）。 系统可以转发警报信息（如 SNMP 陷阱的情况），也可以将警报信息写入到其最终目标（例如日志文件）。

您可以在特定节点上配置服务警报（例如 Cisco 数据库层监控器），或者为群集中所有节点上的特定服务配置警报。

注释 Cisco Unity Connection SNMP 不支持陷阱。

提示 对于远程系统日志服务器，请勿指定 Unified Communications Manager 服务器，该服务器无法接受来自其他服务器的系统日志消息。

您可使用 Cisco Unified 实时监控工具 (Unifed RTMT) 中的“跟踪和日志中心”选项来收集发送到 SDL 跟踪日志文件的警报（仅限 Cisco CallManager 和 CTIManager 服务）。 您可使用 Unifed RTMT 中的系统日志查看器来查看发送到本地系统日志的警报信息。

警报配置

您可以在 Cisco Unified 功能配置中配置服务警报，例如数据库层监控器。 然后，您可以配置想要系统在其中发送警报信息的一个位置或多个位置，例如系统日志查看器（本地系统日志）。 使用此选项，您可以执行以下操作：

- 为特定服务器或所有服务器上的服务配置警报（仅限 Unified Communications Manager 群集）
- 为已配置的服务或服务器配置其他远程系统日志服务器
- 为不同的目标配置不同的警报事件级别设置

Cisco Unified Communications Manager 管理中的 Cisco 系统日志代理企业参数可让您将符合或超过所配置阈值的所有警报前转到带有以下两个设置的远程系统日志服务器：远程系统日志服务器名称和系统日志严重性。 要访问这些 Cisco 系统日志代理参数，请转至适用的配置窗口：

Unified Communications Manager	在 Cisco Unified Communications Manager 管理中，选择**系统** > **企业参数**。
Cisco Unity Connection	在 Cisco Unity Connection 管理中，选择**系统设置** > **企业参数**。
Cisco IM and Presence	在 Cisco Unified Communications Manager IM and Presence 管理中，选择**系统** > **企业参数**。

警报包括系统（OS/硬件平台）、应用程序（服务）和安全警告。

注释 如果在 Cisco Unified 功能配置中配置了 Cisco 系统日志代理警报企业参数和应用程序（服务）警报，系统可将相同的警报发送到远程系统日志两次。

如果为应用程序警报启用本地系统日志，则系统仅在警报高于本地系统日志阈值和企业阈值时，才会将警报发送到企业远程系统日志服务器。

如果在 Cisco Unified 功能配置中也启用了远程系统日志，系统会使用 Cisco Unified 功能配置中配置的应用程序阈值将警报前转到远程系统日志服务器，这可能导致警报被发送到远程系统日志服务器两次。

事件级别/严重性设置为系统收集的警报和消息提供过滤机制。此设置有助于防止系统日志和跟踪文件变得过载。 系统只前转超过所配置阈值的警报和消息。

有关附加到警报和事件的严重性级别的详细信息，请参阅警报定义，第 99 页。

警报定义

用于参考，警报定义说明警报消息：其含义以及如何从中恢复。 您可以在“警报定义”窗口中搜索警报信息。 单击任何服务特定的警报定义时，屏幕上会显示警报信息的说明（包括您添加的任何用户定义文本）以及建议的操作。

您可以搜索功能配置GUI中显示的所有警报的警报定义。 为了帮助您诊断问题，相应目录中的定义包括警报名称、描述、说明、建议的操作、严重性、参数和监视器。

当系统生成警报时，它会在警报信息中使用警报定义名称，以便您可以识别警报。 在警报定义中，您可以查看指定系统可以将警报信息发送到的位置的路由列表。 路由列表可能包含以下位置（这些位置与您可以在“警报配置”窗口中配置的位置关联）：

- 仅 Unified Communications Manager：SDL - 如果您启用此选项的警报并在“警报配置”窗口中指定事件级别，系统会将警报信息发送到 SDL 跟踪。
- SDI - 如果您启用此选项的警报并在“警报配置”窗口中指定事件级别，系统会将警报信息发送到 SDI 跟踪。
- 系统日志 - 如果您启用此选项的警报、在“警报配置”窗口中指定事件级别，并输入远程系统日志服务器的服务器名称或 IP 地址，系统会将警报信息发送到远程系统日志服务器。
- 事件日志 - 如果您启用此选项的警报并在“警报配置”窗口中指定事件级别，系统会将警报信息发送到本地系统日志，您可以在 Cisco Unified 实时监控工具 (Unified RTMT) 的系统日志查看器中查看。
- 数据收集器 - 系统将警报信息发送到实时信息系统（RIS 数据收集器）（仅适用于警告）。 您无法在“警报配置”窗口中配置此选项。
- SNMP 陷阱 - 系统生成 SNMP 陷阱。 您无法在“警报配置”窗口中配置此选项。

提示 如果 SNMP 陷阱位置显示在路由列表中，系统会将警报信息转发到 CCM MIB SNMP 代理，该代理将根据 CISCO-CCM-MIB 中的定义生成陷阱。

如果“警报配置”窗口中特定位置的已配置警报事件级别等于或低于警报定义中列出的严重性，系统会发送警报。 例如，如果警报定义中的严重性等于 WARNING_ALARM，在“警报配置”窗口中，您可以将特定目标的警报事件级别配置为“预警”、“通知”、“信息”或“调试”，这是较低的事件级别，系统会将警报发送到相应的目标。 如果您将警报事件级别配置为“危急”、“警告”、“严重”或“错误”，则系统不会将警报发送到相应的位置。

对于每个警报定义，可以添加其他说明或建议。所有管理员都可以访问添加的信息。您可以直接在“警报详细信息”窗口的“用户定义的文本”窗格中输入信息。 标准水平和垂直滚动条支持滚动。Cisco Unified 功能配置会将信息添加到数据库中。

警报信息

您可以查看警报信息以确定问题是否存在。 用于查看警报信息的方法取决于您在配置警报时选择的目标。 可以使用 Unified RTMT 中的“跟踪和日志中心”选项或使用文本编辑器查看发送到 SDL 跟踪日志文件 (Unified Communications Manager) 的警报信息。 可以使用 Unifed RTMT 中的系统日志查看器来查看发送到本地系统日志的警报信息。

设置警报

按以下步骤配置警报。

过程

步骤 1 在 Cisco Unified Communications Manager 管理、Cisco Unity Connection 管理或 Cisco Unified IM and Presence 管理中，将 Cisco 系统日志代理企业参数配置为将系统、应用程序（服务）和安全警报/消息发送到指定的远程系统日志服务器。 跳过此步骤以在 Cisco Unified 功能配置中配置应用程序（服务）警报/消息。

步骤 2 在 Cisco Unified 功能配置中，配置您要收集的应用程序（服务）警报信息的服务器、服务、目标和事件级别。

步骤 3 （可选）向警报添加定义。

- 所有服务均可转至 SDI 日志（但必须在跟踪中配置）。
- 所有服务均可转至系统日志查看器。
- 仅 Unified Communications Manager：只有 Cisco CallManager 和 Cisco CTIManager 服务使用 SDL 日志。
- 要将系统日志消息发送到远程系统日志服务器，请选中远程系统日志目标并指定主机名。如果没有配置远程服务器名称，Cisco Unified 功能配置不会将系统日志消息发送到远程系统日志服务器。

提示 不要将 Unified Communications Manager 服务器配置为远程系统日志服务器。

步骤 4 如果选择 SDL 跟踪文件作为警报目标，则收集跟踪数据并通过 Unified RTMT 中的“跟踪和日志中心”选项查看该信息。

步骤 5 如果选择本地系统日志作为警报目标，则在 Unified RTMT 的系统日志查看器中查看警报信息。

步骤 6 请参阅相应的警报定义以了解说明和建议的操作。

警报服务设置

系统日志代理企业参数

您可以配置 Cisco 系统日志代理企业参数，以将超过所配置阈值的系统、应用程序和安全警报/消息发送到指定的远程系统日志服务器。 要访问 Cisco 系统日志代理参数，请转至适用的配置窗口：

Unified Communications Manager	在 Cisco Unified Communications Manager 管理中，选择**系统** > **企业参数**。
Cisco Unity Connection	在 Cisco Unity Connection 管理中，选择**系统设置** > **企业参数**。
Cisco IM and Presence	在 Cisco Unified Communications Manager IM and Presence 管理中，选择**系统** > **企业参数**。

接下来，配置远程系统日志服务器名称（远程系统日志服务器名称1、远程系统日志服务器名称2、远程系统日志服务器名称3、远程系统日志服务器名称4和远程系统日志服务器名称5）以及系统日志严重性。 在配置服务器名称时，确保指定有效的 IP 地址。 系统日志严重性适用于您配置的所有远程系统日志服务器。 然后单击**保存**。 要输入有效值，请单击 **?** 按钮。 如果未指定服务器名称，Cisco Unified 功能配置不会发送系统日志消息。

注意 在 Unified Communications Manager 中配置远程系统日志服务器时，不要为远程系统日志服务器名称添加重复的条目。 如果添加重复的条目，Cisco 系统日志代理将在发送消息到远程系统日志服务器时忽略重复的条目。

注释 不要将 Unified Communications Manager 配置为远程系统日志服务器。 Unified Communications Manager 节点不接受来自另一台服务器的系统日志消息。

设置警报服务

本节介绍如何为通过 Cisco Unified 功能配置管理的功能或网络服务添加或更新警报。

注释 Cisco 建议您不要更改 SNMP 陷阱和目录配置。

Cisco Unity Connection 还使用警报，这些警报在 Cisco Unity Connection 功能配置中可用。 您无法在 Cisco Unity Connection 功能配置中配置警报。 有关详细信息，请参阅《*Cisco Unity Connection* 功能配置管理指南》。

有关如何使用标准注册表编辑器的详细信息，请参阅您的在线操作系统文档。

过程

步骤 1 选择**警报** > **配置**。

随即显示“警报配置”窗口。

步骤 2 从“服务器”下拉列表中，选择要为其配置警报的服务器；然后单击**前往**。

步骤 3 从“服务组”下拉列表中，选择要为其配置警报的服务类别，例如数据库和管理服务；然后单击**前往**。

提示 有关与服务组对应的服务列表，请参阅服务组。

步骤 4 从“服务”下拉列表中，选择要为其配置警报的服务；然后单击**前往**。

仅支持服务组以及您配置的服务会显示。

提示 下拉列表将显示活动和非活动的服务。

在“警报配置”窗口中，将显示所选服务的警报监控器列表以及事件级别。 此外，“应用至所有节点”复选框将显示。

步骤 5 仅 Unified Communications Manager：如果要执行此操作，只要您的配置支持群集，就可以选中**应用至所有节点**复选框，将服务的警报配置应用到群集中的所有节点。

步骤 6 如“警报配置”设置中所述配置设置，其中包含对监控器和事件级别的说明。

步骤 7 要保存配置，请单击**保存**按钮。

注释 要设置默认值，请单击**设置默认值**按钮，然后单击**保存**。

下一步做什么

提示 如果“警报配置”窗口中特定目标的已配置警报事件级别等于或低于警报定义中列出的严重性，系统会发送警报。 例如，如果警报定义中的严重性等于 WARNING_ALARM，在“警报配置”窗口中，您可以将特定目标的警报事件级别配置为“预警”、“通知”、“信息”或“调试”，这是较低的事件级别，系统会将警报发送到相应的目标。 如果您将警报事件级别配置为“危急”、“警告”、“严重”或“错误”（严重性级别较高），则系统不会将警报发送到相应的位置。

要访问 Cisco Extension Mobility 应用程序服务、Cisco Unified Communications Manager Assistant 服务、Cisco Extension Mobility 服务和 Cisco Web Dialer 服务的警报定义，请如警报定义中所述在“警报消息定义”窗口中选择 **JavaApplications** 目录。

设置使用 Cisco Tomcat 的警报服务

以下服务使用 Cisco Tomcat 生成警报：

- Cisco Extension Mobility 应用程序
- Cisco IP Manager Assistant
- Cisco Extension Mobility
- Cisco Web Dialer

系统登录警报 AuthenticationFailed 也使用 Cisco Tomcat。 要为这些服务生成警报，请执行以下程序。

过程

步骤 1 在 Cisco Unified 功能配置中，选择**警报** > **配置**。

步骤 2 从“服务器”下拉列表中，选择要为其配置警报的服务器；然后单击**前往**。

步骤 3 从“服务组”下拉列表中，选择**平台服务**，然后单击**前往**。

步骤 4 从“服务”下拉列表中，选择**Cisco Tomcat**，然后单击**前往**。

步骤 5 仅 Unified Communications Manager：如果要执行此操作，只要您的配置支持群集，就可以选中**应用至所有节点**复选框，将服务的警报配置应用到群集中的所有节点。

步骤 6 如“警报配置”设置中所述配置设置，其中包含对监控器和事件级别的说明。

步骤 7 要保存配置，请单击**保存**按钮。

服务组

下表列出了与“警报配置”窗口“服务组”下拉列表中的选项对应的服务。

注释 并非列出的所有服务组和服务都适用于所有系统配置。

表 7: 警报配置中的服务组

服务组	服务
CM 服务	Cisco CTIManager、Cisco CallManager、Cisco DHCP 监控器服务、Cisco 被叫号码分析器、Cisco 被叫号码分析器服务器、Cisco 扩展功能、Cisco IP 语音媒体流应用程序、Cisco 消息传送接口、Cisco 头戴式耳机服务和 Cisco TFTP
CTI 服务	Cisco IP Manager Assistant 和 Cisco WebDialer Web 服务
CDR 服务	Cisco CAR 计划程序、Cisco CDR 代理和 Cisco CDR 存储库管理器
数据库和管理服务	Cisco 批量预配置服务和 Cisco 数据库层监控器

服务组	服务
性能和监控服务	Cisco AMC 服务和 Cisco RIS 数据收集器
安全服务	Cisco 证书权限代理功能和 Cisco 证书到期监控
目录服务	Cisco DirSync
备份和恢复服务	Cisco DRF Local 和 Cisco DRF Master
系统服务	Cisco 跟踪收集服务
平台服务	Cisco Tomcat 和 Cisco 智能许可证管理器
基于位置的跟踪服务	Cisco 无线控制器同步服务

警报配置设置

下表介绍了所有警报配置设置，即使服务可能不支持这些设置。

表 *8:* 警报配置设置

名称	说明
服务器	从下拉列表中，选择要为其配置警报的服务器；然后单击**前往**。
服务组	Cisco Unity Connection仅支持以下服务组：数据库和管理员服务、性能和监控服务、备份和恢复服务、系统服务以及平台服务。 从下拉列表中，选择要为其配置警报的服务类别，例如数据库和管理服务；然后单击**前往**。
服务	从“服务”下拉列表中，选择要为其配置警报的服务；然后单击**前往**。 仅支持服务组以及您配置的服务会显示。 **提示** 下拉列表将显示活动和非活动的服务。
仅限 Unified Communications Manager 和 Cisco Unified Communications Manager IM and Presence Service： 应用到所有节点	要将服务的警报设置应用到群集中的所有节点，请选中该复选框。

名称	说明
为本地系统日志启用警报	系统日志查看器用作警报目标。 程序在系统日志查看器内的应用程序日志中记录错误，并提供警报说明和建议操作。 您可以从 Cisco Unified 实时监控工具访问系统日志查看器。 有关使用系统日志查看器查看日志的详细信息，请参阅《*Cisco Unified* 实时监控工具管理指南》。
为远程系统日志启用警报	系统日志文件用作警报目标。 选中此复选框可让系统日志消息存储在系统日志服务器上，并指定系统日志服务器名称。如果未启用此目标并且未指定服务器名称，Cisco Unified 功能配置不会发送系统日志消息。 配置的AMC主收集器和故障转移收集器使用远程系统日志设置。收集器使用的远程系统日志设置在各个单独节点上配置。 如果仅在AMC主收集器上配置远程系统日志，而不在AMC故障转移收集器上配置远程系统日志，并且 AMC 主收集器中发生故障转移，则不会生成远程系统日志。 您必须在所有节点上配置完全相同的设置，以将远程系统日志警报发送到相同的远程系统日志服务器。 当AMC控制器中发生故障转移或收集器配置更改为另一节点时，将会使用备份或新配置节点上的远程系统日志设置。 为防止过多警报向系统洪泛，您可以选中**排除终端警报**复选框。这可确保与终端电话相关的事件记录到单独的文件中。 **排除终端警报**复选框仅对 CallManager 服务显示，默认情况下未选中。当您选中此复选框时，您还需要选中**应用到所有节点**。终端警报的配置选项列在“警报”配置设置中。 **提示** 请勿指定 Unified Communications Manager 或 Cisco Unified Communications Manager IM and Presence Service 节点作为目标，因为该节点不接受来自另一个节点的系统日志消息。
远程系统日志服务器	在每个“服务器名称1”、“服务器名称2”、“服务器名称3”、“服务器名称4”和“服务器名称5”字段中，输入要用于接受系统日志消息的远程系统日志服务器的名称或IP地址。例如，如果要将警报发送到 Cisco Unified Operations Manager，请将 Cisco Unified Operations Manager 指定为服务器名称。 **提示** 请勿指定 Unified Communications Manager 或 Cisco Unified Communications Manager IM and Presence Service 节点作为目标，因为该节点不接受来自另一个节点的系统日志消息。

名称	说明
为 SDI 跟踪启用警报	SDI 跟踪库用作警报目标。 要记录警报，请选中此复选框，然后在“跟踪配置”窗口中选中所选服务的“打开跟踪”复选框。 有关在 Cisco Unified 功能配置中“跟踪配置”窗口内的配置设置的信息，请参阅“设置跟踪参数”。
仅限 Unified Communications Manager 和 Unified Communications Manager BE： 为 SDL 跟踪启用警报	SDL 跟踪库用作警报目标。 此目标仅适用于 Cisco CallManager 服务和 CTIManager 服务。 使用跟踪 SDL 配置来配置此警报目标。要在将警报记录到 SDL 跟踪日志记录中，请选中此复选框，然后在“跟踪配置”窗口中选中所选服务的“打开跟踪”复选框。 有关在 Cisco Unified 功能配置中“跟踪配置”窗口内的配置设置的信息，请参阅“设置跟踪参数”。
警报事件级别	从下拉列表中选择以下选项之一： **危急** 此级别指定系统为不可用。 **警告** 此级别表示需要立即采取措施。 **严重** 系统检测到严重情况。 **错误** 此级别表示存在错误情况。 **预警** 此级别表示检测到预警情况。 **通知** 此级别指定正常但重要的情况。 **信息** 此级别指定仅是信息性消息。 **调试** 此级别指定 Cisco 技术支持中心工程师用于调试的详细事件信息。

下表介绍了默认警报配置设置。

	本地系统日志	远程系统日志	SDI 跟踪	SDL 跟踪
启用警报	选中	未选中	选中	选中

警报事件级别	错误	已禁用	错误	错误

排除终端警报	本地系统日志	替代系统日志	远程系统日志	系统日志严重程度和限制警告	系统日志陷阱
选中	否	是	否	否	否
未选中	否	是	是	是	是

警报定义和用户定义的新增说明

本节提供程序性信息，适用于搜索、查看和创建在功能配置界面中显示的警报定义的用户信息。

查看警报定义并添加用户定义的说明

本节介绍如何搜索和查看警报定义。

提示 仅 Unified Communications Manager 和 Cisco Unity Connection：您可以在 Cisco Unity Connection 功能配置中查看 Cisco Unity Connection 警告定义。 您不能在 Cisco Unity Connection 功能配置中向警报定义添加用户定义的说明。

Cisco Unity Connection 还使用 Cisco Unified 功能配置中的某些警报定义，必须在 Cisco Unified 功能配置中查看这些定义。 请注意，可以查看与系统目录中的目录关联的警报。

开始之前

查看警报定义目录的说明。

过程

步骤 1 选择**警报** > **定义**。

步骤 2 执行以下操作之一：

- 如下所示选择警报：
  - 从**查找警报位置**下拉列表中选择警报目录，例如，系统警报目录或 IM and Presence 警报目录。
  - 从**等于**下拉列表中选择特定的目录名称。
- 在**输入警报名称**字段中输入警报名称。

步骤 3 选择**查找**。

步骤 4 如果存在多个警报定义页面，请执行以下操作之一：

- 要选择其他页面，在**警报消息定义**窗口底部选择相应的导航按钮。
- 要更改窗口中显示的警报数，请从**每页行数**下拉列表中选择一个不同的值。

步骤 5 选择要提供其警报详细信息的警报定义。

步骤 6 如果要向警报添加信息，请在**用户定义的文本**字段中输入文本，然后选择**保存**。

提示 如果在**用户定义的文本**字段中添加文本，则可以随时选择**清除所有**以删除您输入的信息。

步骤 7 选择**保存**。

步骤 8 如果要返回**警告消息定义**窗口，请从“相关链接”下拉列表中选择**返回查找/列出警告**。

步骤 9 选择**前往**。

系统警报目录说明

下表包含系统警报目录警报说明。 系统警报目录支持 Unified Communications Manager 和 Cisco Unity Connection。

表 *9:* 系统目录

名称	说明
ClusterManagerAlarmCatalog	与群集中服务器之间安全关联的建立有关的所有群集管理器警报定义。
DBAlarmCatalog	所有 Cisco 数据库警报定义
DRFAlarmCatalog	所有灾难恢复系统警报定义
GenericAlarmCatalog	所有应用程序共享的所有通用警报定义
JavaApplications	所有 Java 应用程序警报定义。 **提示** 您无法使用警报配置 GUI 配置 JavaApplications 警报。 对于 Communications Manager 和 Cisco Unity Connection，您通常 警报配置为转到事件日志；对于 Unified Communications M 您可以配置这些警报以生成 SNMP 陷阱，从而与 CiscoWo 管理解决方案集成。使用操作系统附带的注册表编辑器可 改警报定义和参数。
EMAlarmCatalog	Extension Mobility 警报
LoginAlarmCatalog	所有与登录相关的警报定义
LpmTctCatalog	所有日志分区监控和跟踪收集警报定义
RTMTAlarmCatalog	所有 Cisco Unified 实时监控工具警报定义

名称	说明
SystemAccessCatalog	用于跟踪 SystemAccess 是否提供所有线程统计计数器以及所有进程的所有警报定义。
ServiceManagerAlarmCatalogs	与激活、停用、启动、重新启动和停止服务相关的所有服务管理器
TFTPAlarmCatalog	所有 Cisco TFTP 警报定义
TVSAlarmCatalog	信任验证服务警报
TestAlarmCatalog	用于通过 SNMP 陷阱从命令行界面 (CLI) 发送测试警报的所有警报 CLI 的信息，请参阅《*Cisco Unified* 解决方案的命令行界面参考指 **提示** Cisco Unity Connection SNMP 在 Unified Communications Cisco Unity Connection 系统中都不支持陷阱。
CertMonitorAlarmCatalog	所有证书过期定义。
CTLproviderAlarmCatalog	证书信任列表 (CTL) 提供程序服务警报
CDPAlarmCatalog	Cisco Discovery Protocol (CDP) 服务警报
IMSAlarmCatalog	所有用户验证和凭证定义。
SLMAlarmCatalog	Cisco 智能许可警报

CallManager 警报目录说明

本节介绍的内容不适用于 Cisco Unity Connection。

下表包含 CallManager 警报目录说明。

表 *10: CallManager* 警报目录

名称	说明
CallManager	所有 Cisco CallManager 服务警报定义
CDRRepAlarmCatalog	所有 CDRRep 警报定义
CARAlarmCatalog	所有 CDR 分析和报告警报定义
CEFAlarmCatalog	所有 Cisco 扩展功能警报定义
CMIAlarmCatalog	所有 Cisco 消息传送接口警报定义
CtiManagerAlarmCatalog	所有 Cisco 计算机电话集成 (CTI) 管理器警报定义
IpVmsAlarmCatalog	所有 IP 语音媒体流应用程序警报定义

名称	说明
TCDSRVAlarmCatalog	所有 Cisco 电话呼叫调度程序服务警报定义
Phone	与下载等电话相关任务的警报
CAPFAlarmCatalog	证书颁发机构代理功能 (CAPF) 服务警报
SAMLSSOAlarmCatalog	SAML 单点登录功能警报。

IM and Presence 警报目录说明

下表包含 IM and Presence Service 警报目录说明。

表 *11: IM and Presence Service* 警报目录

名称	说明
CiscoUPSConfigAgent	所有配置代理警报，用于通知 IM and Presence Service SIP 代理 IM and Presence Service IDS 数据库中的配置更改。
CiscoUPInterclusterSyncAgent	所有群集间同步代理警报，用于在 IM and Presence Service 群集之间同步最终用户信息以实现群集间路由。
CiscoUPSPresenceEngine	所有 Presence Engine 警报，收集有关用户可用性状态和通信功能的信息。
CiscoUPSSIPProxy	与路由、请求者标识和传输互连相关的所有 SIP 代理警报。
CiscoUPSSOAP	所有简单对象访问协议 (SOAP) 警报，提供用于与使用 HTTPS 的外部客户端交互的安全 SOAP 接口。
CiscoUPSSyncAgent	保持 IM and Presence Service 数据与 Unified Communications Manager 数据同步的所有同步代理警报。
CiscoUPXCP	所有 XCP 警报，收集有关 IM and Presence Service 上 XCP 组件和服务状态的信息。
CiscoUPServerRecoveryManager	与 Presence 冗余组中的节点之间的故障转移和回退过程相关的所有服务器恢复管理器警报。
CiscoUPReplWatcher	监控 IDS 复制状态的所有 ReplWatcher 警报。
CiscoUPXCPConfigManager	与 XCP 组件相关的所有 Cisco XCP 配置管理器警报定义。

警报信息包含说明和建议的操作，还包含应用程序名称、服务器名称及其他信息，可帮助您执行故障诊断，甚至解决本地 IM and Presence Service 节点上没有的问题。

有关特定于 IM and Presence Service 的警报的详细信息，请参阅 *Cisco Unified Communications Manager* 上的 *IM and Presence* 系统错误消息。

CiscoSyslog 文件中的默认警报

下表包含在 CiscoSyslog 文件中触发但不含任何警报配置的默认警报的说明：

表 *12: CiscoSyslog* 文件中的默认警报

名称	说明
CLM_IPSecCertUpdated	来自群集中对等节点的 IPSec 自签名证书已因为更改而被导入。
CLM_IPAddressChange	群集中对等节点的 IP 地址已更改。
CLM_PeerState	群集中另一节点的 ClusterMgr 会话状态已更改为当前状态。
CLM_MsgIntChkError	ClusterMgr 收到消息完整性检查失败的消息。 这可能表示群集中的另一节点配置了错误的安全密码。
CLM_UnrecognizedHost	ClusterMgr 接收到来自未配置为此群集中节点的 IP 地址的消息。
CLM_ConnectivityTest	群集管理器检测到网络错误。
ServiceActivated	此服务现已激活。
ServiceDeactivated	此服务现已禁用。
ServiceActivationFailed	无法激活此服务。
ServiceDeactivationFailed	无法禁用此服务。
ServiceFailed	服务突然终止。 服务管理器将尝试重新启动。
ServiceStartFailed	无法启动此服务。 服务管理器将尝试再次启动该服务。
ServiceStopFailed	多次重试后无法停止指定的服务。 该服务将被标记为已停止。
ServiceRestartFailed	无法重新启动指定的服务。

名称	说明
ServiceExceededMaxRestarts	服务无法启动，甚至在达到最大尝试次数后也未能启动。
FailedToReadConfig	无法读取配置文件。 配置文件可能已损坏。
MemAllocFailed	无法分配内存。
SystemResourceError	系统呼叫失败。
ServiceManagerUnexpectedShutdown	服务管理器在意外终止后成功重新启动。
OutOfMemory	该进程已向操作系统请求内存，但没有足够的内存可用。
CREATE-DST-RULE-FILE-CLI	新的 DST 规则文件通过 cli 生成。 电话需要重新启动。否则会导致错误的 DST 开始/停止日期。
CREATE-DST-RULE-FILE-BOOTUP	启动期间会生成新的 DST 规则文件。 电话需要重新启动。否则会导致错误的 DST 开始/停止日期。
CREATE-DST-RULE-FILE-CRON	新的 DST 规则文件会从 cron 生成。 电话需要重新启动。否则会导致错误的DST开始/停止日期。
PermissionDenied	操作无法完成，因为进程没有执行该操作的权限。
ServiceNotInstalled	一个可执行程序正在尝试启动，但未能启动，因为未在服务控制管理器中配置为服务。 服务名称为 %s。
ServiceStopped	服务已停止。
ServiceStarted	服务已启动。
ServiceStartupFailed	服务已启动。
FileWriteError	无法写入到主文件路径。

第 12 章

审核日志

审核日志

使用审核日志，对系统所做的配置更改会记录到单独的日志文件中进行审核。

审核日志（标准）

启用审核日志时不选择详细审核日志选项，即会将系统配置为标准审核日志。

使用标准审核日志，对系统所做的配置更改会记录到单独的日志文件中进行审核。 显示在功能配置 GUI 中的“控制中心 - 网络服务”下的思科审核事件服务，会监控用户对系统所做的任何配置更改，或用户操作导致的任何配置更改。

您可以访问功能配置 GUI 中的**审核日志配置**窗口以配置审核日志的设置。

标准审核日志包含以下部分：

- 审核日志记录框架 - 框架包含使用警报库将审核事件写入审核日志的 API。 定义为 GenericAlarmCatalog.xml 的警报目录适用于这些警报。 不同的系统组件提供自己的日志记录。

  以下示例显示 Unified Communications Manager 组件可用于发送警报的 API：

```
User ID: CCMAdministratorClient IP Address: 172.19.240.207 Severity: 3
EventType: ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:
Successful Description: CallManager Service status is stopped
```

- 审核事件日志 - 审核事件代表需要进行记录的任何事件。 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
```

提示 请注意审核事件日志默认为集中式并启用。称为“系统日志审核”的警报监控将写入日志。默认情况下，将日志配置为轮换。 如果 AuditLogAlarmMonitor 无法写入审核事件，AuditLogAlarmMonitor 会将此失败记录为系统日志文件中的严重错误。 警告管理器会将此错误作为 SeverityMatchFound 警告的一部分报告。 即使事件记录失败，实际操作也会继续。 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。

Cisco Unified 功能配置标准事件日志记录

Cisco Unified 功能配置记录以下事件：

- 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。 （仅限 Cisco Unified Communications Manager）
- 查看功能配置报告存档中的任何报告。 此日志在报告器节点上查看。 （仅限 Unified Communications Manager）

Cisco Unified 实时监控工具标准事件登录

Cisco Unified 实时监控工具使用审核事件警报记录以下事件：

- 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

Unified Communications Manager 标准事件日志记录

Cisco CDR 分析和报告 (CAR) 为这些事件创建审核日志：

- 加载程序计划

- 每日、每周和每月报告计划
- 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

Cisco Unified CM 管理标准事件日志记录

以下事件是为 Cisco Unified Communications Manager 管理的各个组件而记录：

- 用户日志记录（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）

Cisco Unified Communications 自助门户标准事件日志记录

将为 Cisco Unified Communications 自助门户记录用户日志记录（用户登录和用户注销）事件。

命令行界面标准事件日志记录

将记录通过命令行界面发出的所有命令（Unified Communications Manager 和 Cisco Unity Connection 都适用）。

Cisco Unity Connection 管理标准事件日志记录

Cisco Unity Connection 管理会记录以下事件：

- 用户日志记录（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）

Cisco Personal Communications Assistant (Cisco PCA) 标准事件日志记录

Cisco Personal Communications Assistant 客户端记录以下事件：

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

Cisco Unity Connection 功能配置标准事件日志记录

Cisco Unity Connection 功能配置记录以下事件：

- 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。

使用具象状态传输 (REST) API 的 Cisco Unity Connection 客户端事件日志记录

使用具象状态传输 (REST) API 的 Cisco Unity Connection 客户端记录以下事件：

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

Cisco Unified IM and Presence 功能配置标准事件日志记录

Cisco Unified IM and Presence 功能配置记录以下事件：

- 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
- 查看功能配置报告存档中的任何报告（可在报告器节点上查看此日志）

Cisco Unified IM and Presence 实时监控工具标准事件日志

Cisco Unified IM and Presence 实时监控工具使用审核事件警报记录以下事件：

- 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

Cisco IM and Presence 管理标准事件日志记录

以下事件是为 Cisco Unified Communications Manager IM and Presence 管理的各个组件而记录：

- 管理员日志记录（登录和注销管理、操作系统管理、灾难恢复系统和报告等 IM and Presence 接口）
- 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 IM and Presence 服务器添加或删除）

IM and Presence 应用程序标准事件日志记录

以下事件是为 IM and Presence 应用程序的各个组件而记录：

- IM 客户端上的最终用户日志记录（用户登录、用户注销和登录尝试失败）
- 用户进入和退出 IM 聊天室
- IM 聊天室的创建和销毁

命令行界面标准事件日志记录

所有通过命令行界面发出的命令都将被记录。

审核日志（详细）

详细审核日志是一项可选功能，用于记录未存储在标准（默认）审核日志中的附加配置修改。 除了在标准审核日志中存储的所有信息外，详细的审核日志还包括添加、更新和删除的配置项目（含修改的值）。 默认情况下禁用详细的审核日志，但您可以在**审核日志配置**窗口中启用它。

Audit Log Types

系统审核日志

系统审核日志跟踪活动（例如创建、修改或删除Linux OS用户，篡改日志，更改文件或目录权限）。由于收集的数据量较大，因此默认情况下禁用此类型的审核日志。 要启用此功能，必须使用CLI手动启用 utils auditd。 在启用系统审核日志功能后，您可以从实时监控工具的跟踪和日志中心收集、查看、下载或删除所选的日志。 系统审核日志采用 `vos-audit.log` 的格式。

有关如何启用此功能的详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面参考指南》。 有关如何从实时监控工具访问收集的目录的信息，请参阅《*Cisco Unified* 实时监控工具管理指南》。

应用程序审核日志

应用程序审核日志监控和记录用户所做的或用户操作导致的任何系统配置更改。

注释 应用程序审核日志 (Linux auditd) 只能通过CLI启用或禁用。 除了通过实时监控工具收集 vos-audit.log 之外，您无法更改此类审核日志的任何设置。

数据库审核日志

数据库审核日志跟踪与访问 Informix 数据库（例如登录）相关的所有活动。

审核日志配置任务流程

完成以下任务以配置审核日志记录。

过程

	命令或操作	目的
步骤1	设置审核日志记录，第 119 页	在“审核日志配置”窗口中设置您的审核日志配置。 您可以配置是否要使用远程审核日志记录以及是否需要详细的审核日志记录选项。
步骤2	配置远程审核日志传输协议，第 119 页	可选。 如果配置了远程审核日志记录，请配置传输协议。 在正常操作模式下，系统默认值为 UDP，但您也可以配置 TCP 或 TLS
步骤3	针对警告通知配置电子邮件服务器，第 120 页	可选。 在 RTMT 中，针对电子邮件警告设置电子邮件服务器。
步骤4	启用电子邮件警告，第 120 页	可选。 设置以下电子邮件警告之一：

	命令或操作	目的
		• 如果使用 TCP 配置远程审核日志记录，请设置 **TCPRemoteSyslogDeliveryFailed** 警告的电子邮件通知。 • 如果使用 TLS 配置远程审核日志记录，请设置 **TLSRemoteSyslogDeliveryFailed** 警告的电子邮件通知。
步骤 5	为平台日志配置远程审核日志记录，第 121 页	为平台审核日志和远程服务器日志设置远程审核日志记录。 对于这些类型的审核日志，必须配置 FileBeat 客户端和外部 logstash 服务器。

设置审核日志记录

开始之前

对于远程审核日志记录，您必须已设置远程系统日志服务器并在每个群集节点和远程系统日志服务器之间配置 IPSec，包括到两者之间任何网关的连接。 有关 IPSec 配置，请参阅《*Cisco IOS* 安全配置指南》。

过程

步骤 1 在 Cisco Unified 功能配置中，选择**工具** > **审核日志配置**。

步骤 2 从**服务器**下拉菜单中选择群集中的任何服务器，然后单击**前往**。

步骤 3 要记录所有群集节点，选中**应用到所有节点**复选框。

步骤 4 在**服务器名称**字段中，输入远程系统日志服务器的 IP 地址或完全限定域名。

步骤 5 可选。 要记录配置更新（包括修改的项目和修改的值），选中**详细审核日志记录**复选框。

步骤 6 在**审核日志配置**窗口完成其余字段的设置。 有关这些字段及其说明的帮助，请参阅联机帮助。

步骤 7 单击**保存**。

下一步做什么

配置远程审核日志传输协议，第 119 页

配置远程审核日志传输协议

此程序可用于更改远程审核日志的传输协议。 系统默认值为 UDP，但您可以重新配置为 TCP 或 TLS。

过程

步骤 1 登录到命令行界面。

步骤 2 运行 **utils remotesyslog show protocol** 命令以确认配置了哪个协议。

步骤 3 如果您需要更改此节点上的协议，请执行以下操作：

- 要配置 TCP，运行 **utils remotesyslog set protocol tcp** 命令。
- 要配置 UDP，运行 **utils remotesyslog set protocol udp** 命令。
- 要配置 TLS，运行 **utils remotesyslog set protocol tls** 命令。

要设置 TLS 连接，必须将安全证书从系统日志服务器上传到 Unified Communications Manager 和 IM and Presence Service 上的 tomcat 信任存储区。

注释 在 Common Criteria 模式下，将实施严格的主机名验证。 因此，需要使用与证书匹配的完全限定域名 (FQDN) 配置服务器。

步骤 4 如果更改了协议，请重新启动节点。

步骤 5 对每个 Unified Communications Manager 和 IM and Presence Service 群集节点重复此程序。

下一步做什么

针对警告通知配置电子邮件服务器， 第 120 页

针对警告通知配置电子邮件服务器

此程序用于针对警告通知设置您的电子邮件服务器。

过程

步骤 1 在实时监控工具的系统窗口中，单击**警告中心**。

步骤 2 选择**系统** > **工具** > **警告** > **配置电子邮件服务器**。

步骤 3 在**邮件服务器配置**弹出窗口中，输入邮件服务器的详细信息。

步骤 4 单击**确定**。

下一步做什么

启用电子邮件警告， 第 120 页

启用电子邮件警告

如果您配置了采用 TCP 或 TLS 进行远程审核日志记录，此程序可用于设置电子邮件警告，让系统在出现传输失败时通知您。

过程

步骤 1 在实时监控工具**系统**区域中，单击**警告中心**。

步骤 2 在**警告中心**窗口中，

- 如果您配置的是采用 TCP 进行远程审核日志记录，选择 **TCPRemoteSyslogDeliveryFailed**
- 如果您配置的是采用 TLS 进行远程审核日志记录，选择 **TLSRemoteSyslogDeliveryFailed**

步骤 3 选择**系统** > **工具** > **警告** > **配置警告操作**。

步骤 4 在**警告操作**弹出窗口中，选择**默认**并单击**编辑**。

步骤 5 在**警告操作**弹出窗口中，**添加**收件人。

步骤 6 在弹出窗口中，输入您要向其发送电子邮件警告的地址，然后单击**确定**。

步骤 7 在**警告操作**弹出窗口中，确保地址显示在**收件人**之下并且已选中**启用**复选框。

步骤 8 单击**确定**。

为平台日志配置远程审核日志记录

完成这些任务，为平台审核日志、远程支持日志和批量管理 csv 文件添加远程审核日志支持。 对于这些类型的日志，将使用 FileBeat 客户端和 logstash 服务器。

开始之前

确保您已设置外部 logstash 服务器。

过程

	命令或操作	目的
步骤 1	配置 Logstash 服务器信息，第 121 页	使用外部 logstash 服务器详细信息（例如 IP 地址、端口和文件类型）配置 FileBeat 客户端。
步骤 2	配置 FileBeat 客户端，第 122 页	为远程审核日志记录启用 FileBeat 客户端。

配置 Logstash 服务器信息

此程序可用于使用外部 logstash 服务器信息（例如 IP 地址、端口号和可下载文件类型）配置 FileBeat 客户端。

开始之前

确保您已设置外部 logstash 服务器。

过程

步骤 1 登录到命令行界面。

步骤 2 运行 **utils FileBeat configure** 命令。

步骤 3 按照提示配置 logstash 服务器详细信息。

配置 FileBeat 客户端

此程序可用于启用或禁用FileBeat客户端以上传平台审核日志、远程支持日志和批量管理csv文件。

过程

步骤 1 登录到命令行界面。

步骤 2 运行 **utils FileBeat status** 命令以确认 FileBeat 客户端是否已启用。

步骤 3 运行以下命令之一：

- 要启用客户端，运行 **utils FileBeat enable** 命令。
- 要禁用客户端，运行 **utils FileBeat disable** 命令。

注释 TCP 是默认的传输协议。

步骤 4 可选。 如果要将 TLS 用作传输协议，请执行以下操作：

- 要启用 TLS 作为传输协议，运行 **utils FileBeat tls enable** 命令。
- 要禁用 TLS 作为传输协议，运行 **utils FileBeat tls disable** 命令。

注释 要使用 TLS，必须将安全证书从 logstash 服务器上传到 Unified Communications Manager 和 IM and Presence Service 上的 tomcat 信任存储区。

步骤 5 对于每个节点重复上述过程。

不要在所有节点上同时运行任何这些命令。

审核日志配置设置

开始之前

请注意，只有拥有审核角色的用户才可更改审核日志设置。 默认情况下，对于Unified Communications Manager，在全新安装和升级后，CCMAdministrator拥有审核角色。 CCMAdministrator可以在Cisco Unified Communications Manager管理的“用户组配置”窗口中将具有审核权限的任何用户分配给“标准审核用户”组分配。 如果想要这样做，您可以从“标准审核用户”组中删除CCMAdministrator。

对于 IM and Presence Service，在全新安装和升级后，管理员拥有审核角色，并且可以将拥有审核权限的任何用户分配给“标准审核用户”组。

对于 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。 您也可以从此帐户删除审核管理员角色。

标准审核日志配置角色能够删除审核日志以及读取/更新 Cisco Unified 实时监控工具、IM and Presence 实时监控工具、跟踪收集工具、实时监控工具 (RTMT) 警告配置、功能配置用户界面中的“控制中心 - 网络服务”、RTMT 配置文件保存、功能配置用户界面中的审核配置以及称为审核跟踪的资源。

标准审核日志配置角色能够删除审核日志以及读取/更新 Cisco Unified RTMT、跟踪收集工具、RTMT 警告配置、Cisco Unified 功能配置中的“控制中心 - 网络服务”、RTMT 配置文件保存、Cisco Unified 功能配置中的审核配置以及称为审核跟踪的资源。

Cisco Unity Connection 中的审核管理员角色能够查看、下载和删除 Cisco Unified RTMT 中的审核日志。

有关 Unified Communications Manager 中角色、用户和用户组的信息，请参阅《*Cisco Unified Communications Manager* 管理指南》。

有关 Cisco Unity Connection 中角色和用户的信息，请参阅《*Cisco Unity Connection* 的用户移动、添加和更改指南》。

有关 IM and Presence 中角色、用户和用户组的信息，请参阅《*Unified Communications Manager* 上 *IM and Presence Service* 的配置和管理》。

下表介绍了您可以在 Cisco Unified 功能配置的“审核日志配置”窗口中配置的设置。

表 *13:* 审核日志配置设置

字段	说明
选择服务器	
服务器	选择要在其中配置审核日志的服务器（节点），然后单击**前往**。
应用到所有节点	如果要将此审核日志应用到群集中的所有节点，请选中**应用到所有节点**复选框。
应用程序审核日志设置	

字段	说明
启用审核日志	选中此复选框时，即会为应用程序审核日志创建审核日志。 对于 Unified Communications Manager，应用程序审核日志支持对 Unified Communications Manager 用户界面的配置更新，例如 Cisco Unified Communications Manager 管理、Cisco Unified RTMT、Cisco Unified Communications Manager CDR 分析和报告以及 Cisco Unified 功能配置。 对于 IM and Presence Service，应用程序审核日志支持对 IM and Presence 用户界面的配置更新，例如 Cisco Unified Communications Manager IM and Presence 管理、Cisco Unified IM and Presence 实时监控工具和 Cisco Unified IM and Presence 功能配置。 对于 Cisco Unity Connection，应用程序审核日志支持对 Cisco Unity Connection 用户界面的配置更新，包括 Cisco Unity Connection 管理、Cisco Unity Connection 功能配置、Cisco Personal Communications Assistant 以及使用 Connection REST API 的客户端。 此设置默认显示为启用。 **注释** 网络服务审核事件服务必须正在运行。
启用清除	日志分区监控(LPM)查看“启用清除”选项以确定其是否需要清除审核日志。选中此复选框时，LPM将在公共分区磁盘使用超出上限时清除RTMT中的所有审核日志文件；不过，您可以通过取消选中该复选框禁用清除。 如果清除已禁用，则审核日志数量继续增加，直到磁盘已满。此操作可导致系统中断。当取消选中“启用清除”复选框时，会显示一条消息说明禁用清除的风险。 请注意，此选项适用于活动分区中的审核日志。 如果审核日志位于非活动分区，则审核日志在磁盘使用超出上限时将被清除。 您可以通过选择RTMT中的**跟踪和日志中心**>**审核日志**来访问审核日志。 **注释** 网络服务 Cisco 日志分区监控工具必须正在运行。
启用日志轮换	系统会读取此选项以确定其需要轮换审核日志文件还是需要继续创建新文件。 最大文件数不得超过 5000。选中“启用轮换”复选框时，系统在达到最大文件数量后将开始覆盖最旧的审核日志文件。 **提示** 日志轮换被禁用时（未选中），审核日志将忽略“最大文件数”设置。
详细审核日志	选中此复选框后，系统将启用详细审核日志。详细审核日志提供的项目与常规审核日志相同，但也包括配置更改。例如，审核日志包含已添加、更新和删除的项目，包括已修改值。

字段	说明
服务器名称	输入您要用于接受系统日志消息的远程系统日志服务器的名称或IP地址。如果未指定服务器名称，Cisco Unified IM and Presence 功能配置不会发送系统日志消息。 请勿指定 Unified Communications Manager 节点作为目标，因为 Unified Communications Manager 节点不接受来自另一个节点的系统日志消息。 这仅适用于 IM and Presence Service。
远程系统日志审核事件级别	选择远程系统日志服务器所需的系统日志消息严重性。具有所选或更高严重性级别的所有系统日志消息都将被发送到远程系统日志。 这仅适用于 IM and Presence Service。
文件最大数	输入想要在日志中包括的最大文件数。 默认设置指定为 250。最大数量指定 5000。
文件最大大小	输入审核日志的文件最大大小。 文件大小值必须介于 1MB 到 10MB 之间。 您必须指定一个介于 1 到 10 之间的数字。
接近日志轮换覆盖的预警阈值 (%)	当审核日志接近被覆盖的程度时，系统会警告您。 使用此字段设置当您处于该值时系统将向您发送警告的阈值。 例如，如果您使用 250 个 2 MB 文件、预警阈值为 80% 的默认设置，则系统会在累积的审核日志到 200 个文件 (80%) 时给您发送警报。 如果想要保留审核历史记录，您可以在系统覆盖日志之前使用 RTMT 检索它们。 在您收集文件后，RTMT 会提供一个选项以将其删除。 输入介于 1 到 99% 之间的值。 默认值为 80%。 在设置此字段时，您还必须选中**启用日志轮换**选项。 **注释** 分配给审核日志的总磁盘空间为最大文件数乘以文件最大大小。 如果磁盘上的审核日志大小超过分配的总磁盘空间百分比，系统会在警告中心发出警报。
数据库审核日志过滤器设置	
启用审核日志	选中此复选框时，将为 Unified Communications Manager 和 Cisco Unity Connection 数据库创建审核日志。 将此设置结合“调试审核级别”设置使用，可让您为数据库的某些方面创建日志。

字段	说明
调试审核级别	此设置可让您选择要在日志中审核的数据库方面。从下拉列表框中选择以下选项之一。 请注意每个审核日志过滤器级别都是累积的。 • **方案** - 跟踪对审核日志数据库设置的更改（例如，数据库表中的列和行）。 • **管理任务** - 跟踪对 Unified Communications Manager 系统的所有管理更改（例如，为了维护系统而作的任何更改）以及所有**方案**更改。 **提示** 大多数管理员会将“管理任务”设置保留为禁用。 对于要审核的用户，请使用数据库更新级别。 • **数据库更新** - 跟踪对数据库的所有更改以及所有**方案**更改和所有**管理任务**更改。 • **数据库读取** - 跟踪对系统的每次读取，以及所有方案更改、管理任务更改和数据库更新更改。 **提示** 仅在您想要快速查看 Unified Communications Manager、IM and Presence Service 或 Cisco Unity Connection 系统时，选择数据库读取级别。 此级别使用大量的系统资源，只能短时使用。
启用审核日志轮换	系统会读取此选项以确定其需要轮换数据库审核日志文件还是需要继续创建新文件。选中“审核启用轮换”复选框时，系统在达到最大文件数量后将开始覆盖最旧的审核日志文件。 此设置复选框未选中时，审核日志将忽略最大文件数设置。
文件最大数	输入想要在日志中包括的最大文件数。确保为“最大文件数”设置输入的值大于为“日志轮换时删除的文件数”设置输入的值。 您可以输入介于 4（最小）到 40（最大）之间的数字。
日志轮换时删除的文件数	输入当发生数据库审核日志轮换时，系统可以删除的最大文件数。 您可以在此字段中输入的最小值为 1。最大值比您为“最大文件数”输入的值小 2。例如，如果您在“最大文件数”字段输入 40，则可以在“日志轮换时删除的文件数”字段中输入的最大数字为 38。
设置为默认值	**设为默认值**按钮指定默认值。建议将审核日志设置为默认模式，除非需要将其设置为不同的级别以进行详细故障诊断。 **设为默认值**选项将最大限度地减少日志文件使用的磁盘空间。

注意 启用后，数据库日志记录可能会在短时间内生成大量数据，特别是调试审核级别设置为**数据库更新**或**数据库读取**时。这可能会对繁忙使用期间的性能造成显著影响。一般情况下，我们建议您保持禁止数据库日志记录。如果您需要启用日志记录以跟踪数据库中的更改，我们建议您使用**数据库更新**级别仅在短时间内使用。同样，管理日志记录对Web用户界面的整体性能也有影响，特别是在轮询数据库条目时（例如，从数据库中轮询 250 台设备）。

第 13 章

Call Home

Call Home

本章概述了 Unified Communications Manager Call Home 服务，并说明了如何配置 Unified Communications Manager Call Home 功能。 Call Home 功能允许通信并将诊断警告、清单和其他消息发送到 Smart Call Home 后端服务器。

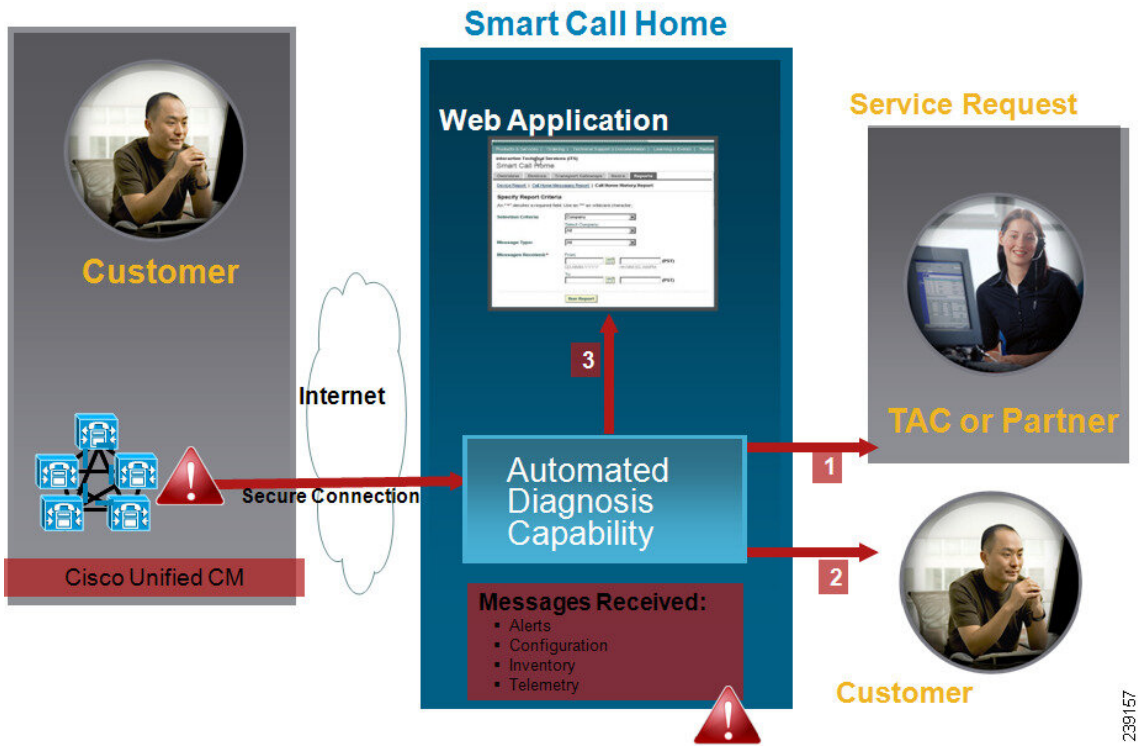
Smart Call Home

Smart Call Home 在一系列 Cisco 设备上提供主动诊断、实时警告和补救，以提高网络可用性和运营效率。 为此，它从启用了 Smart Call Home 的 Unified Communications Manager 接收和分析诊断警告、清单及其他消息。 Unified Communications Manager 的这一特定功能称为 Unified Communications Manager Call Home。

Smart Call Home：

- 通过以下方式主动、快速地解决问题，从而提高网络可用性：
  - 通过持续进行监控、发出实时的主动警告以及进行详细诊断，迅速确定问题。
  - 通过提供仅针对网络中的设备类型的警告，使您意识到潜在的问题。 自动直接联系 Cisco 技术支持中心 (TAC)，更迅速地解决紧急问题。
- 通过为客户提供以下功能提高运营效率：
  - 缩短故障诊断时间，从而更高效地利用员工资源。
- 提供对所需信息基于 Web 的快速访问，使客户能够：
  - 在一个位置查看所有 Call Home 消息、诊断信息和建议。
  - 快速检查服务请求状态。
  - 查看所有支持 Call Home 的设备的最新资产和配置信息。

图 *2: Cisco Smart Call Home* 概述



Smart Call Home 包含执行以下任务的模块：

- 通知客户 Call Home 消息。
- 提供影响分析和补救步骤。

有关 Smart Call Home 的详细信息，请参阅以下位置的 Smart Call Home 页面：

http://www.cisco.com/en/US/products/ps7334/serv_home.html

有关 Smart Call Home 证书续订的信息

从 Cisco Release 10.5(2) 开始，管理员必须为任何续订请求手动上传新证书，以继续支持 Smart Call Home 功能。 您可以通过 Cisco Unified 操作系统管理 web GUI 上传证书。 转至**安全 > 证书管理 > 上传证书/证书链**。 选择 **tomcat-trust** 作为证书用途，然后从保存的目标上传证书。

以下带扩展名 .PEM 的证书应上传至 tomcat-trust。

注释 确保管理员复制整个字符串并包含 -----BEGIN CERTIFICATE----- 和 -----END CERTIFICATE-----，将其粘贴到文本文件中，然后使用扩展名 .PEM 保存。

-----BEGIN CERTIFICATE-----

MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x

GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9
WYWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KFk2f
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2Bl
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl0Ha
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+Oza
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----

Anonymous Call Home

Anonymous Call Home 是 Smart Call Home 功能的子功能，可让 Cisco 匿名接收清单和遥测消息。 启用此功能可让您的身份保持匿名。

以下是 Anonymous Call Home 的特征：

- Unified Communications Manager 仅发送清单和遥测消息，而不会向 Smart Call Home 后端发送诊断和配置信息。
- 它不会发送任何用户相关信息（例如，注册的设备和升级历史记录）。
- Anonymous Call Home 选项不需要向 Cisco 获得 Smart Call Home 注册或授权。
- 清单和遥测消息会定期（每月的第一天）发送至 Call Home 后端。
- 如果 Cisco Unified Communications Manager 配置为使用 Anonymous Call Home，则会禁用**包括跟踪日志和诊断信息**选项。

清单消息包含有关群集、节点和许可证的信息。

下表列出了用于 Smart Call Home 和 Anonymous Call Home 的清单消息。

表 *14: Smart Call Home* 和 *Anonymous Call Home*的清单消息

清单消息	Smart Call Home	Anonymous Call Home
联系电子邮件	适用	不适用
联系人电话号码	适用	不适用
街道地址	适用	不适用
服务器名称	适用	不适用
服务器 IP 地址	适用	不适用
许可证服务器	适用	不适用
OS 版本	适用	适用
模型	适用	适用
序列号	适用	适用
CPU 速度	适用	适用
RAM	适用	适用
存储分区	适用	适用
固件版本	适用	适用

清单消息	Smart Call Home	Anonymous Call Home
BIOS 版本	适用	适用
BIOS 信息	适用	适用
Raid 配置	适用	适用
活动服务	适用	适用
发布方名称	适用	不适用
发布方 IP	适用	不适用
产品 ID	适用	适用
活动版本	适用	适用
非活动版本	适用	适用
产品短名称	适用	适用

遥测消息包含有关在 Unified Communications Manager 上可用的每种设备类型的设备数量（IP 电话、网关、会议网桥等）的信息。 遥测数据包含整个群集的设备计数。

下表列出了用于 Smart Call Home 和 Anonymous Call Home 的遥测消息。

表 *15: Smart Call Home* 和 *Anonymous Call Home* 的遥测消息

遥测消息	Smart Call Home	Anonymous Call Home
联系电子邮件	适用	不适用
联系人电话号码	适用	不适用
街道地址	适用	不适用
服务器名称	适用	不适用
CM 用户计数	适用	不适用
序列号	适用	适用
发布方名称	适用	不适用
设备计数和型号	适用	适用
电话用户计数	适用	适用
CM 呼叫活动	适用	适用
注册的设备计数	适用	不适用

遥测消息	Smart Call Home	Anonymous Call Home
升级历史记录	适用	不适用
系统状态	适用于主机名、日期、区域设置、产品版本、操作系统版本、许可 MAC、运行时间、MP 统计信息、已使用内存、磁盘使用量、活动和非活动分区以及 DNS	适用于日期、区域设置、产品版本、操作系统版本、许可 MAC、运行时间、已使用内存、磁盘使用量、已使用的活动和非活动分区

配置消息包含有关与配置相关的每个数据库表的行计数信息。 配置数据由整个群集中每个表的表名称和行计数组成。

Smart Call Home 交互

如果您直接与 Cisco Systems 签订了服务合同，则可以为 Cisco Smart Call Home 服务注册 Unified Communications Manager。 Smart Call Home 通过分析发自 Unified Communications Manager 的 Call Home 消息并提供背景信息和建议，可帮助快速解决系统问题。

Unified Communications Manager Call Home 功能将以下消息传递到 Smart Call Home 后端服务器：

- 警告 - 包含有关环境、硬件故障和系统性能的各种情况的警告信息。 这些警告可从 Unified Communications Manager 群集内的任何节点生成。 警告详细信息包含节点和进行故障诊断所需的其他信息，具体取决于警告类型。 有关发送到 Smart Call Home 后端服务器的警告，请参阅与 Smart Call Home 交互相关的主题。

以下是 Smart Call Home 的警告。

默认情况下，Smart Call Home 每 24 小时处理一次警告。 混合群集（Unified Communications Manager 和 Cisco Unified Presence）中 24 小时内可能重复出现同一警告，Smart Call Home 不会对其进行处理。

重要事项 48 年后，收集的信息将从主 AMC 服务器中删除。 默认情况下，Unified Communications Manager 发布方是主 AMC 服务器。

- **性能警告**
  - CallProcessingNodeCPUPegging
  - CodeYellow
  - CPUPegging
  - LowActivePartitionAvailableDiskSpace
  - LowAvailableVirtualMemory
  - LowSwapPartitionAvailableDiskSpace

- 与数据库相关的警告
  - DBReplicationFailure
- 呼叫失败警告
  - MediaListExhausted
  - RouteListExhausted
- 与崩溃相关的警告
  - Coredumpfilefound
  - CriticalServiceDown

配置、清单和遥测消息会定期（每月的第一天）发送至 Call Home 后端。 借助这些消息中的信息，TAC 能够及时主动提供服务，以帮助客户管理和维护其网络。

Call Home 的先决条件

要支持 Unified Communications Manager Call Home 服务，您需要以下各项：

- 与相应的 Unified Communications Manager 服务合同关联的 Cisco.com 用户 ID。
- 强烈建议为 Unified Communications Manager Call Home 功能设置域名系统 (DNS) 和简单邮件传输协议 (SMTP) 服务器。
  - 要使用安全 Web (HTTPS) 发送 Call Home 消息，必须进行 DNS 设置。
  - 要将 Call Home 消息发送给 Cisco TAC 或通过电子邮件将消息副本发送给列表上的多个收件人，必须进行 SMTP 设置。

访问 Call Home

要访问 Unified Communications Manager Call Home，请转至 Cisco Unified 功能配置管理，然后选择 **CallHome**（**Cisco Unified 功能配置** > **CallHome** > **Call Home 配置**）。

Call Home 设置

下表列出了默认 Unified Communications Manager Call Home 设置。

表 *16:* 默认 *Call Home* 设置

参数	默认值
Call Home	已启用

参数	默认值
使用以下项将数据发送到 Cisco 技术支持中心 (TAC)	安全 Web (HTTPS)

如果在安装过程中更改了默认的 Smart Call Home 配置，则相同的设置反映在 Smart Call Home 用户界面中。

注释 如果您选择电子**电子邮件**作为传输方法并且对于**安全 Web (HTTPS)**选项不是必需 SMTP 设置，则必须具有 SMTP 设置。

Call Home 配置

Cisco Unified 功能配置中，选择 **Call Home** > **Call Home 配置**。

“Call Home 配置”窗口即会出现。

注释 您也可以在安装 Unified Communications Manager 时配置 Cisco Smart Call Home。

如果您在安装期间配置了 Smart Call Home 选项，则启用 Smart Call Home 功能。 如果您选择**无**，当您登录到 Cisco Unified Communications Manager 管理时，到即会显示提醒消息。 本文提供了使用 Cisco Unified 功能配置配置 Smart Call Home 或禁用提醒的说明。

下表介绍了配置 Unified Communications Manager Call Home 的设置。

表 *17: Unified Communications Manager Call Home* 配置设置

字段名称	说明
Call Home 消息计划	显示已发送的上一条 Call Home 消息以及计划发送的下一条消息的日期和时间。

字段名称	说明
Call Home*	从下拉列表中选择以下选项之一： • **无**： 如果要启用或禁用 Call Home，请选择此选项。 提醒消息 `Smart Call Home 未配置。 要配置 Smart Call Home 或禁用该提醒，请转至 Cisco Unified 功能配置 > Call Home 或单击此处即会出现在管理员页面上。` • **禁用**：如果要禁用 Call Home，请选择此选项。 • **启用 (Smart Call Home)**：如果您在安装期间选择了 Smart Call Home，此选项为启用。 选择了此选项时，会启用**客户联系人详细信息**下的所有字段。 使用相同的配置时，还会启用**发送数据**中的选项。 • **已启用 (Anonymous Call Home)**：如果想要以匿名模式使用 Call Home，请选择此选项。 选择了此选项时，会禁用**客户联系人详细信息**下的所有字段。 使用相同的配置时，会启用**发送数据**中的“将副本发送到以下电子邮件地址（使用逗号分隔多个地址）”字段，会禁用 Call Home 页面上的“包括跟踪日志和诊断信息”。 **注释** 如果启用 Anonymous Call Home，服务器会将使用情况统计信息发送到服务器上的 Cisco 系统。 此信息可帮助 Cisco 了解产品的用户体验，并驱动产品方向。
客户联系人详情	
邮箱地址*	输入客户的联系人电子邮件地址。 这是必填字段。
公司	（可选）输入公司的名称。 最多可以输入 255 个字符。
联系人姓名	（可选）输入客户的联系人姓名。 最多可以输入 128 个字符。 联系人姓名可以包含字母数字字符和一些特殊字符，例如点号（.）、下划线（_）和连字符（-）。
地址	（可选）输入客户的地址。 最多可以输入 1024 个字符。
Phone	（可选）输入客户的电话号码。
发送数据	

字段名称	说明
使用以下项将数据发送到Cisco技术支持中心 (TAC)	这是必填字段。 从下拉列表中选择以下选项之一来发送 Call Home 消息到 Cisco TAC： • **安全 Web (HTTPS)**：如果要使用安全 Web 将数据发送到 Cisco TAC，请选择此选项。 • **电子邮件**：如果想要使用电子邮件将数据发送到 Cisco TAC，请选择此选项。 对于电子邮件，必须配置 SMTP 服务器。 您可以看到配置的 SMTP 服务器的主机名或 IP 地址。 **注释** 如果您没有配置 SMTP 服务器，将会显示一则预警消息。 • **通过代理安全 Web (HTTPS)**：如果想要通过代理将数据发送到 Cisco TAC，请选择此选项。 目前，我们不支持代理级别的验证。 配置此选项时会出现以下字段： • **HTTPS 代理 IP/主机名***：输入代理 IP/主机名。 • **HTTPS 代理端口***：输入要通信的代理端口号。
将副本发送到以下电子邮件地址（用逗号分隔多个地址）	选中此复选框以将 Call Home 消息的副本发送到指定的电子邮件地址。 最多可以输入 1024 个字符。
包括跟踪日志和诊断信息	选中此复选框以激活 Unified Communications Manager 来收集日志和诊断信息。 **注释** 此选项仅在启用了 Smart Call Home 启用时才有效。 该消息包含触发警告时收集的诊断信息以及跟踪消息。 如果跟踪小于 3 MB，则跟踪将被编码并作为警告消息的一部分发送，如果跟踪大于 3 MB，则跟踪位置的路径会显示在警告消息中。
保存	保存您的 Call Home 配置。 **注释** 保存 Call Home 配置后，将显示最终用户许可协议 (EULA) 消息。 如果您是第一次配置，则必须接受许可协议。 **提示** 要禁用您激活的 Call Home 服务，请从下拉列表中选择**禁用**选项，然后单击**保存**。
重置	重置为上次保存的配置。
立即保存并 Call Home	保存并发送 Call Home 消息。 **注释** 如果消息发送成功，将显示 **Call Home 配置已保存并且所有 Call Home 消息已成功发送**消息。

限制

如果 Unified Communications Manager 或 Cisco Unified Presence 服务器关闭或无法接通，以下限制适用：

- 服务器无法接通时，Smart Call Home 无法捕获上次发送的 Call Home 消息和计划的下一条消息的日期和时间。
- 服务器无法接通时，Smart Call Home 不会发送 Call Home 消息。
- 当发布方关闭时，Smart Call Home 将无法捕获库存邮件中的许可信息。

以下限制是因警告管理器和收集器 (AMC) 而起：

- 如果节点 A 上出现警告、主 AMC 服务器（默认情况下为发布方）重新启动，并且 24 小时内同一节点上出现相同的警告，则 Smart Call Home 将从节点 A 重新发送警告数据。由于主 AMC 重新启动，Smart Call Home 无法识别已经发生的警告。
- 如果节点 A 上出现警告、您将主 AMC 服务器改为另一个节点，并且 24 小时内同一节点上出现相同的警告，则 Smart Call Home 会将其识别为节点 A 上的新警告并发送警告数据。
- 少数情况下，在主 AMC 服务器上收集的跟踪可能在主 AMC 服务器上驻留最多 60 小时。

以下是混合群集（Unified Communications Manager 和 IM and Presence）情境下的限制：

- **CallProcessingNodeCpuPegging**、**Media List Exhausted**、**Route List Exhausted** 等警告不适用于 IM and Presence。
- 如果用户将主 AMC 服务器改为 IM and Presence，Smart Call Home 无法生成 **Media List Exhausted** 和 **Route List Exhausted** 的群集概述报告。
- 如果用户将主 AMC 服务器改为 IM and Presence，则 Smart Call Home 无法生成**数据库复制**警告的概述报告。

Call Home 参考

有关 Smart Call Home 的详细信息，请参阅以下 URL：

- Smart Call Home 服务简介

  http://www.cisco.com/en/US/products/ps7334/serv_home.html

第 14 章

可维护性连接器

功能配置连接器概述

您可以使用 Webex 功能配置服务轻松收集日志。 该服务会自动执行查找、检索和存储诊断日志及信息的任务。

此功能会使用部署在本地的功能配置连接器。 功能配置连接器在网络中的专用主机（“连接器主机”）上运行。 您可以将连接器安装到以下任一组件：

- 企业计算平台 (ECP)—推荐

  ECP 使用 Docker 容器隔离、保护和管理其服务。 主机和 Serviceability Connector 应用程序从云端安装。 无需手动升级即可确保其为最新且安全。

重要事项 我们建议使用 ECP。 我们未来的发展将集中在这个平台上。 如果您在 Expressway 上安装了功能配置连接器，则部分些新功能将不可用。

- Cisco Expressway

您可以使用功能配置连接器达成以下目的：

- 服务请求的自动日志和系统信息检索
- Cloud-Connected UC 部署中 Unified CM 群集的日志收集

您可以对两种使用案例使用相同的功能配置连接器。

使用功能配置服务的好处

该服务可带来以下好处：

- 加速日志收集。 TAC 工程师在诊断问题时可以检索相关日志。 他们可以避免请求额外日志以及等待手动收集和交付的延迟。 这种自动化可能会将您解决问题所需的时间缩短数天。
- 与 TAC 的协作解决方案分析器及其诊断签名数据库一起使用。 系统会自动分析日志，发现已知问题，并建议已知的修补程序或解决办法。

与其他混合服务的差异

您可以通过 Control Hub 像其他基于 Expressway 的混合服务（例如混合日历服务和混合呼叫服务）一样部署和管理功能配置连接器。 但有一些非常重要的区别。

此服务没有面向用户的功能。 TAC 是此服务的主要用户。 虽然它可以让使用其他混合服务的组织受益，但不使用其他混合服务的组织才是其一般用户。

如果您已在 Control Hub 中配置组织，可以通过现有的组织管理员帐户启用服务。

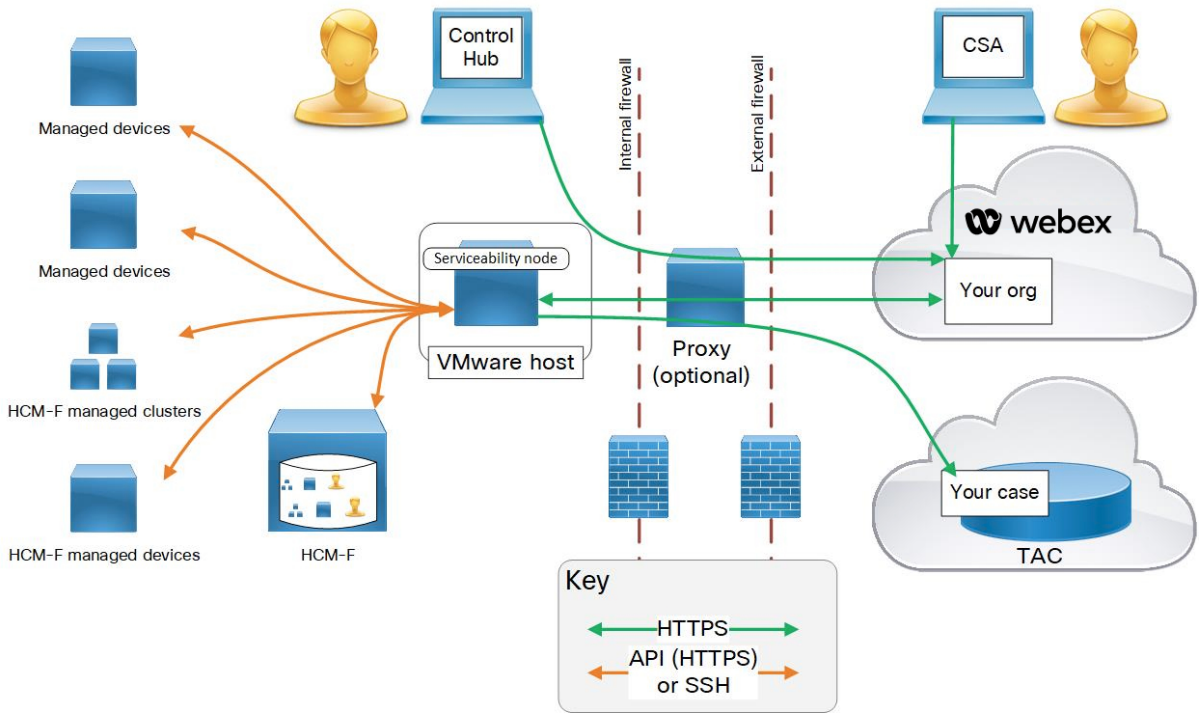
功能配置连接器与直接向用户提供功能的连接器具有不同的负载配置文件。 连接器始终可用，因此 TAC 可以在必要时收集数据。 不过，它在一段时间内没有稳定的负载。 TAC 代表会手动发起数据收集。 他们会协商适当的收集时间，以最大限度减轻对同一基础设施提供的其他服务的影响。

关于工作原理的简短描述

1. 管理员将与 Cisco TAC 一起部署功能配置服务。 请参阅：TAC 案例部署架构 ，第 143 页。
2. TAC 得知您的一台 Cisco 设备出现问题（当您创建案例）。
3. TAC 代表使用协作解决方案分析器 (CSA) Web 界面来请求功能配置连接器，以从相关设备收集数据。
4. 您的功能配置连接器会将请求转换为 API 命令，以从托管的设备收集所请求的数据。
5. 您的功能配置连接器会收集、加密该数据并将其上传到客户体验驱动器(CXD)，然后将数据与服务请求关联起来。
6. 系统将根据超过 1000 个诊断签名的 TAC 数据库对数据进行分析。
7. TAC 代表会查看结果，必要时还会检查原始日志。

TAC 案例部署架构

图 *3:* 在 ***Expressway*** 上使用服务连接器进行部署



元素	说明
受管设备	包括您要向功能配置服务提供日志的任何设备。使用一个功能配置连接器最多可以添加 150 个本地托管的设备。可以从 HCM-F（托管协作中介实现）中导入有关HCS客户的托管设备和群集的信息（如果设备数量较大，请参阅 https://help.webex.com/en-us/142g9e/Limits-and-Bounds-of-Serviceability-Service）。 服务当前可与以下设备配合使用： • Hosted Collaboration Mediation Fulfillment (HCM-F) • Cisco Unified Communications Manager • Cisco Unified CM IM and Presence Service • Cisco Expressway 系列 • Cisco TelePresence Video Communication Server (VCS) • Cisco Unified Contact Center Express (UCCX) • Cisco Unified 边界组件 (CUBE) • Cisco BroadWorks 应用服务器 (AS) • Cisco BroadWorks 配置文件服务器 (PS) • Cisco BroadWorks 消息传送服务器 (UMS) • Cisco BroadWorks 执行服务器 (XS) • Cisco Broadworks Xtended 服务平台 (XSP)
您的管理员	使用 Control Hub 注册连接器主机并启用功能配置服务。URL 是 https://admin.webex.com 并且您需要“组织管理员”凭证。
连接器主机	托管管理连接器和功能配置连接器的企业计算平台 (ECP) 或 Expressway。 • **管理连接器**（在 ECP 或 Expressway 上）以及相应的管理服务（在 Webex 中）管理您的注册。它们会保持连接、在需要时更新连接器，并报告状态和警报。 • **功能配置连接器**—在您为组织启用功能配置服务后，连接器主机（ECP 或 Expressway）从 Webex 下载的小型应用程序。
代理	（可选）如果在启动功能配置连接器后更改代理配置，也需重新启动功能配置连接器。
Webex Cloud	托管 Webex、Webex 呼叫、Webex 会议和 Webex 混合服务。

元素	说明
技术支持中心	包含： • 使用 CSA 通过 Webex Cloud 与您的功能配置连接器通信的 TAC 代表。 • TAC 支持案例管理系统，其中包含您的支持案例以及功能配置连接器收集并上传到 Customer eXperience Drive 的相关日志。

TAC 对于功能配置连接器的支持

有关功能配置连接器的更多详细信息，请参阅 https://www.cisco.com/go/serviceability 或联系您的 TAC 代表。

第 15 章

简单网络管理协议

简单网络管理协议支持

SNMP 是一种应用层协议，能够简化网络设备（如节点和路由器）之间的管理信息交换。 作为 TCP/IP 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。

您可以使用功能配置 GUI 配置与 SNMP 相关的设置，例如 V1、V2c 和 V3 的社区字符串、用户和通知目标。 您配置的 SNMP 设置应用于本地节点；但是，如果您的系统配置支持群集，则可以使用 SNMP 配置窗口中的“应用到所有节点”选项，将设置应用到群集中的所有服务器。

提示 仅 Unified Communications Manager：您在 Cisco Unified CallManager 或 Unified Communications Manager 4.X 中指定的 SNMP 配置参数不会在 Unified Communications Manager 6.0 和更高版本升级期间迁移。必须在 Cisco Unified 功能配置中再次执行 SNMP 配置程序。

SNMP 支持 IPv4 和 IPv6，CISCO-CCM-MIB 包括 IPv4 与 IPv6 地址以及首选项等的列和存储区。

SNMP 基础知识

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 - 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。

  仅 Unified Communications Manager 和 IM and Presence Service：在支持群集的配置中，群集中的第一个节点充当受管设备。

- 代理 - 驻留在受管设备上的网络管理软件模块。 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。

  Master Agent 和子代理组件用于支持 SNMP。 Master Agent 充当代理协议引擎，执行与 SNMP 请求相关的验证、授权、访问控制和隐私功能。 同样，Master Agent 包含与 MIB-II 相关的一些管理信息库 (MIB) 变量。 在子代理完成必要任务后，Master Agent 还会连接和断开子代理。 SNMP Master Agent 侦听端口 161，并转发 SNMP 数据包以获取供应商 MIB。

  Unified Communications Manager 子代理仅与本地 Unified Communications Manager 交互。 Unified Communications Manager 子代理将陷阱和信息消息发送到 SNMP Master Agent，SNMP Master Agent 与 SNMP 陷阱接收器（通知目标）通信。

  IM and Presence Service 子代理仅与本地 IM and Presence Service 交互。 IM and Presence Service 子代理将陷阱和信息消息发送到 SNMP Master Agent，SNMP Master Agent 则与 SNMP 陷阱接收器（通知目标）通信。

- 网络管理系统 (NMS) - SNMP 管理应用程序（与运行它的 PC 一起），提供网络管理所需的大量处理和内存资源。 NMS 执行监控和控制受管设备的应用程序。 以下项支持 NMS：
  - CiscoWorks LAN Management Solution
  - HP OpenView
  - 支持 SNMP 和 Unified Communications Manager SNMP 接口的第三方应用程序

SNMP 管理信息库

SNMP 允许访问管理信息库 (MIB)，即分级组织的信息集合。 MIB 包含由对象标识符来标识的托管对象。 MIB 对象（包含托管设备的特定特征）包括一个或多个对象实例（变量）。

SNMP 界面提供以下 Cisco 标准 MIB：

- CISCO-CDP-MIB
- CISCO-CCM-MIB
- CISCO-SYSLOG-MIB
- CISCO-UNITY-MIB

遵守以下限制：

- Unified Communications Manager 不支持 CISCO-UNITY-MIB。
- Cisco Unity Connection 不支持 CISCO-CCM-MIB。
- IM and Presence Service 不支持 CISCO-CCM-MIB 和 CISCO-UNITY-MIB。

SNMP 扩展代理位于服务器中并显示 CISCO-CCM-MIB，从而提供关于服务器已知设备的详细信息。如果是群集配置，则 SNMP 扩展代理位于群集的每台服务器中。 CISCO-CCM-MIB 提供设备信息，例如设备注册状态、IP 地址、说明和服务器型号类型（并非群集，位于支持群集的配置中）。

SNMP 界面还提供以下行业标准 MIB：

- SYSAPPL-MIB
- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB

CISCO-CDP-MIB

使用 CDP 子代理来读取 Cisco Discovery Protocol MIB (CISCO-CDP-MIB)。 此 MIB 使得 SNMP 受管设备能够将自己通告给网络上的其他 Cisco 设备。

CDP 子代理实现 CDP-MIB。 CDP-MIB 包含以下对象：

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

注释 CISCO-CDP-MIB 取决于是否存在以下 MIB：CISCO-SMI、CISCO-TC、CISCO-VTP-MIB。

SYSAPPL-MIB

使用系统应用程序代理以从 SYSAPPL-MIB 获取信息，例如已安装应用程序、应用程序组件以及系统上运行的进程。

系统应用程序代理支持 SYSAPPL-MIB 的以下对象组：

- sysApplInstallPkg
- sysApplRun
- sysApplMap
- sysApplInstallElmt

- sysApplElmtRun

表 *18: SYSAPPL-MIB* 命令

命令	说明
与设备相关的查询	
sysApplInstallPkgVersion	提供软件制造商分配给应用程序包的版本号。
sysApplElmPastRunUser	提供进程所有者的登录名（例如root）。
与内存、存储和 CPU 相关的查询	
sysApplElmPastRunMemory	提供在终止之前分配给此进程的真实系统内存已知最新总量（以kb为单位）。
sysApplElmtPastRunCPU	提供此进程消耗的总系统CPU资源的已知最新厘秒数。 **注释** 在多处理器系统上，此值可能会在 1 厘秒的实际（挂钟）时间内增加 1 厘秒以上。
sysApplInstallElmtCurSizeLow	提供以2^32字节为模的当前文件大小。例如，对于总计大小为 4,294,967,296 字节的文件，此变量的值为0；对于总计大小为 4,294,967,295 字节的文件，此变量将 4,294,967,295。
sysApplInstallElmtSizeLow	提供以 2^32 字节为模的已安装文件大小。这是安装后磁盘上文件的大小。例如，对于总计大小为 4,294,967,296 字节的文件，此变量的值为0；对于总计大小为 4,294,967,295 字节的文件，此变量将 4,294,967,295。
sysApplElmRunMemory	提供当前分配给此进程的实际系统内存总量（以 kb 为单位）。
sysApplElmRunCPU	提供此进程消耗的总系统CPU资源厘秒数。 **注释** 在多处理器系统上，此值可能在 1 厘秒的实际（挂钟）时间内增加 1 厘秒以上。
与进程相关的查询	

sysApplElmtRunState	提供正在运行的进程的当前状态。 可能的值包括正在运行 (1)、可运行 (2) 但正在等待 CPU 等资源、正在等待 (3) 事件发生、正在退出 (4) 或其他 (5)。
sysApplElmtRunNumFiles	提供进程当前打开的常规文件数量。 传输连接（套接字）不应包括在此值的计算中，也不应包括操作系统特定的特殊文件类型。
sysApplElmtRunTimeStarted	提供启动进程的时间。
sysApplElmtRunMemory	提供当前分配给此进程的实际系统内存总量（以 kb 为单位）。
sysApplElmtPastRunInstallID	提供已安装元素表的索引。 这个对象的值与应用程序元素的 sysApplInstallElmtIndex（表示以前执行过的进程）的值相同。
sysApplElmtPastRunUser	提供进程所有者的登录名（例如root）。
sysApplElmtPastRunTimeEnded	提供进程结束的时间。
sysApplElmtRunUser	提供进程所有者的登录名（例如root）。
sysApplRunStarted	提供应用程序启动的日期和时间。
sysApplElmtRunCPU	提供此进程消耗的总系统 CPU 资源厘秒数。 **注释** 在多处理器系统上，此值可能在 1 厘秒的实际（挂钟）时间内增加 1 厘秒以上。
与软件组件相关的查询	
sysApplInstallPkgProductName	提供制造商分配给软件应用程序包的名称。
sysApplElmtRunParameters	提供进程的开始参数。
sysApplElmtRunName	提供进程的完整路径和文件名。 例如，对于执行路径为 "opt/MYYpkg/bin/myyproc" 的进程 "myyproc"，系统会返回 "/opt/MYYpkg/bin/myyproc"。
sysApplInstallElmtName	提供此元素的名称，该名称包含在应用程序中。
sysApplElmtRunUser	提供进程所有者的登录名（例如root）。

sysApplInstallElmtPath	提供安装此元素的目录的完整路径。 例如，安装于目录 "/opt/EMPuma/bin" 中的元素的值为 "/opt/EMPuma/bin"。 大多数应用程序包都包含程序包中所含元素的相关信息。 此外，元素通常安装在程序包安装目录之下的子目录中。 如果程序包信息本身不包含元素路径名，则路径通常可以通过简单的子目录搜索来确定。 如果该元素未安装在该位置，且没有其他信息可用于代理实施，则该路径未知并且会返回空值。
sysApplMapInstallPkgIndex	提供此对象的值，并标识此进程所属之应用程序的已安装软件包。 如果可以确定进程的父应用程序，此对象的值与 sysApplInstallPkgTable 中对应于此进程所属之已安装应用程序的条目的 sysApplInstallPkgIndex 值相同。 但是，如果无法确定父应用程序（例如，该进程不是特定已安装应用程序的一部分），则此对象的值为 "0"，表明此进程无法与应用程序以及已安装的软件包相关联。
sysApplElmtRunInstallID	提供 sysApplInstallElmtTable 的索引。 这个对象的值与应用程序元素的 sysApplInstallElmtIndex（表示正在运行的实例）的值相同。 如果此进程无法与已安装的可执行文件关联，则此值应为 "0"。
sysApplRunCurrentState	提供正在运行的应用程序实例的当前状态。 可能的值包括正在运行 (1)、可运行 (2) 但正在等待 CPU 等资源、正在等待 (3) 事件发生、正在退出 (4) 或其他 (5)。 此值基于对此应用程序实例的运行元素（请参见 sysApplElmRunState）及其由 sysApplInstallElmtRole 定义的角色的评估。 如果一个应用程序实例的一个或多个 REQUIRED 元素不再运行，则代理实施可能会检测到该应用程序实例正在退出。 大多数代理实施将等到第二次内部轮询完成后，才给系统时间来启动 REQUIRED 元素，然后再将应用程序实例标记为退出。
sysApplInstallPkgDate	提供此软件应用程序在主机上的安装日期和时间。

sysApplInstallPkgVersion	提供软件制造商分配给应用程序包的版本号。
sysApplInstallElmtType	提供属于已安装应用程序的元素的类型。
与日期/时间相关的查询	
sysApplElmtRunCPU	此进程消耗的总系统 CPU 资源厘秒数 **注释** 在多处理器系统上，此值可能在 1 厘秒的实际（挂钟）时间内增加 1 厘秒以上。
sysApplInstallPkgDate	提供此软件应用程序在主机上的安装日期和时间。
sysApplElmtPastRunTimeEnded	提供进程结束的时间。
sysApplRunStarted	提供应用程序启动的日期和时间。

MIB-II

使用 MIB2 代理以从 MIB-II 获取信息。 MIB2 代理提供 RFC 1213 中定义的变量（例如接口、IP 等等）的访问权限，并支持以下对象组：

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

表 *19: MIB-II* 命令

命令	说明
与设备相关的查询	
sysName	为此受管节点提供管理上分配的名称。 按照惯例，此名称是节点的完全限定域名。 如果名称未知，则值为零长度字符串。
sysDescr	提供实体的文字说明。 此值应包括系统硬件类型、软件操作系统和网络软件的全称和版本标识。

SNMP 诊断查询	
sysName	为此受管节点提供管理上分配的名称。 按照惯例，此名称是节点的完全限定域名。如果名称未知，则值为零长度字符串。
sysUpTime	提供自上次重新初始化系统的网络管理部分以来的时间（以百分之一秒为单位）。
snmpInTotalReqVars	提供由于收到有效的 SNMP Get-Request 和 Get-Next PDU 而被 SNMP 协议实体成功检索的 MIB 对象的总数。
snmpOutPkts	提供从 SNMP 实体传递到传输服务的 SNMP 消息总数。
sysServices	提供指示此实体可能提供的服务集的值。此为求和后的值。该总和最初取值为零，然后，对于该节点执行事务的 1 到 7 范围内的每一层 L，升至 (L - 1) 的 2 将加到总和中。 例如，作为提供应用程序服务的主机，节点的值将为 4 (2^(3-1))。 相比之下，作为提供应用程序服务的主机，节点的值将为 72 (2^(4-1) + 2^(7-1))。 **注释** 在 Internet 协议套件环境下，计算：第 1 层物理（例如中继器）、第 2 层数据链/子网（例如桥）、第 3 层 Internet（支持 IP）、第 4 层端到端（支持 TCP）、第 7 层应用程序（支持 SMTP）。 对于包括 OSI 协议的系统，您还可以计算第 5 层和第 6 层。
snmpEnableAuthenTraps	指示是否允许 SNMP 实体生成 authenticationFailure 陷阱。 此对象的值将覆盖任何配置信息，从而提供了一种禁用所有 authenticationFailure 陷阱的方法。 **注释** Cisco 强烈建议将此对象存储在非易失性存储器中，使其在网络管理系统的重新初始化过程中保持不变。
与系统日志相关的查询	

snmpEnabledAuthenTraps	指示是否允许 SNMP 实体生成 authenticationFailure 陷阱。 此对象的值将覆盖任何配置信息，从而提供了一种禁用所有 authenticationFailure 陷阱的方法。 **注释** Cisco 强烈建议将此对象存储在非易失性存储器中，使其在网络管理系统的重新初始化过程中保持不变。
与日期/时间相关的查询	
sysUpTime	提供自上次重新初始化系统的网络管理部分以来的时间（以百分之一秒为单位）。

HOST-RESOURCES MIB

使用主机资源代理以从HOST-RESOURCES-MIB获取值。 主机资源代理提供主机信息（例如存储资源、进程表、设备信息和已安装软件库）的 SNMP 访问权限。 主机资源代理支持以下对象组：

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

表 *20: HOST-RESOURCES MIB* 命令

命令	说明
与设备相关的查询	
hrFSMountPoint	提供此文件系统根目录的路径名。
hrDeviceDescr	提供此设备的文字说明，包括设备制造商和修订版以及序列号（可选）。
hrStorageDescr	提供存储类型和实例的说明。
与内存、存储区和 CPU 相关的查询	
hrMemorySize	提供主机包含的物理读写主内存（通常为 RAM）的容量。

hrStorageSize	提供存储区的大小（以 hrStorageAllocationUnits 为单位）。可写入此对象，以允许在这样的操作有意义并且在基础系统上可行的情况下，远程配置存储区域的大小。 例如，您可以修改分配给缓冲池的主内存量或分配给虚拟内存的磁盘空间量。
与进程相关的查询	
hrSWRunName	提供这个正在运行的软件的文字说明，包括制造商、修订版本以及众所周知的名称。 如果此软件安装在本地，则必须与相应 hrSWInstalledName 中所用的字符串相同。
hrSystemProcesses	提供此系统上当前已加载或正在运行的进程上下文的数量。
hrSWRunIndex	为主机上运行的每个软件提供唯一的值。 尽可能使用系统的本地唯一标识号。
与软件组件相关的查询	
hrSWInstalledName	提供这个已安装软件的文字说明，包括制造商、修订版本、众所周知的名称以及序列号（可选）。
hrSWRunPath	提供从中加载此软件的长期存储区（例如磁盘驱动器）位置的说明。
与日期/时间相关的查询	
hrSystemDate	提供主机的本地日期和时间。
hrFSLastPartialBackupDate	提供将此文件系统的一部分复制到另一个存储设备以进行备份的最后日期。 此信息有助于确保定期执行备份。 如果此信息未知，则此变量的值将对应于 0000 年 1 月 1 日 00:00:00.0，其编码为（十六进制）"00 00 01 01 00 00 00 00"。

CISCO-SYSLOG-MIB

系统日志跟踪并记录从信息到严重的所有系统消息。 使用此 MIB，网络管理应用程序可以将系统日志消息作为 SNMP 陷阱接收：

Cisco Syslog 代理支持以下 MIB 对象的陷阱功能：

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

注释 CISCO-SYSLOG-MIB 取决于是否存在 CISCO-SMI MIB。

表 *21: CISCO-SYSLOG-MIB* 命令

命令	说明
与系统日志相关的查询	
clogNotificationEnabled	指示在设备生成系统日志消息时是否发送 clogMessageGenerated 通知。 禁用通知不会阻止将系统日志消息添加到 clogHistoryTable。
clogMaxSeverity	指示将处理哪些系统日志严重性级别。代理将忽略严重性值大于此值的任何系统日志消息。 注释 严重性数值越高，严重性越低。 例如，错误 (4) 比调试 (8) 更严重。

CISCO-CCM-MIB/CISCO-CCM-CAPABILITY MIB

CISCO-CCM-MIB 包含关于 Unified Communications Manager 及其关联设备（例如电话、网关等）的动态（实时）和已配置（静态）信息，这些信息在此 Unified Communications Manager 节点上可见。简单网络管理协议 (SNMP) 表包含 IP 地址、注册状态和型号类型等信息。

SNMP 支持 IPv4 和 IPv6，CISCO-CCM-MIB 包括 IPv4 与 IPv6 地址以及首选项等的列和存储区。

注释 Unified Communications Manager 在 Unified Communications Manager 系统中支持此 MIB。 IM and Presence Service 和 Cisco Unity Connection 不支持此 MIB。

要查看 CISCO-CCM-MIB 和 MIB 定义的支持列表，请转至以下链接：

ftp://ftp.cisco.com/pub/mibs/supportlists/callmanager/callmanager-supportlist.html

要查看所有 Unified Communications Manager 版本中的 MIB 依赖关系和 MIB 内容（包括过时的对象），请转至以下链接： http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-CCM-CAPABILITY

只有当 Cisco CallManager 服务（如果是 Unified Communications Manager 群集配置，则是本地 Cisco CallManager 服务）启动并正在运行时，才会填充动态表格；静态表格会在 Cisco CallManager SNMP 服务运行时填充。

表 *22: Cisco-CCM-MIB* 动态表格

表格	内容
ccmTable	此表存储本地 Unified Communications Manager 的版本和安装 ID。 表格中还会存储群集中所有 Unified Communications Manager 的相关信息，本地 Unified Communications Manager 知道这些信息，但对版本详情显示“未知”。 如果本地 Unified Communications Manager 关闭，则除版本和安装 ID 值之外，表格仍然为空。
ccmPhoneFailed、ccmPhoneStatusUpdate、ccmPhoneExtn、ccmPhone、ccmPhoneExtension	对于 Cisco Unified IP 电话，ccmPhoneTable 中注册的电话数应与 Unified Communications Manager/RegisteredHardware 电话性能监视计数器匹配。 ccmPhoneTable 中每部已注册、未注册或被拒 Cisco Unified IP 电话有一个条目。 ccmPhoneExtnTable 使用组合索引 ccmPhoneIndex 和 ccmPhoneExtnIndex 来关联 ccmPhoneTable 和 ccmPhoneExtnTable 中的条目。
ccmCTIDevice、ccmCTIDeviceDirNum	ccmCTIDeviceTable 将每个 CTI 设备存储为一个设备。 根据 CTI 路由点或 CTI 端口的注册状态，Unified Communications Manager MIB 中的 ccmRegisteredCTIDevices、ccmUnregisteredCTIDevices 和 ccmRejectedCTIDevices 计数器会更新。
ccmSIPDevice	CCMSIPDeviceTable 将每个 SIP 干线存储为一个设备。
ccmH323Device	ccmH323DeviceTable 包括 Unified Communications Manager（在群集配置的情况下为本地 Unified Communications Manager）包含其信息的 H.323 设备的列表。 对于 H.323 电话或 H.323 网关，ccmH.323DeviceTable 中每个 H.323 设备有一个条目。 （H.323 电话和网关未向 Unified Communications Manager 注册。） 准备好处理指示的 H.323 电话和网关的呼叫时，Unified Communications Manager 会生成 H.323Started 警报。） 系统将网守信息作为 H.323 中继信息的一部分提供。
ccmVoiceMailDevice、ccmVoiceMailDirNum	对于 Cisco uOne、ActiveVoice，ccmVoiceMailDeviceTable 中每个语音留言传送设备有一个条目。 根据注册状态，Cisc MIB 中的 ccmRegisteredVoiceMailDevices、ccmUnregisteredVoiceMailDevices 和 ccmRejectedVoiceMailDevices 计数器会更新。

表格	内容
ccmGateway	ccmRegisteredGateways、ccmUnregisteredGateways 和 ccmRejectedGateways 分别跟踪已注册网关设备或端口的数量、未注册网关设备或端口的数量以及被拒网关设备或端口的数量。 Unified Communications Manager 会在设备或端口级别生成警报。 基于 CallManager 警报的 ccmGatewayTable 中包含设备或端口级别的信息。 ccmGatewayTable 中每个已注册、未注册或被拒的设备或端口都有一个条目。 具有两个 FXS 端口和一个 T1 端口的 VG200 在 ccmGatewayTable 中有三个条目。 ccmActiveGateway 和 ccmInActiveGateway 计数器跟踪活动（已注册）和失去联系（未注册或被拒）之网关设备或端口的数量。 根据注册状态，ccmRegisteredGateways、ccmUnregisteredGateways 和 ccmRejectedGateways 计数器会更新。
ccmMediaDeviceInfo	表格中包含至少尝试过一次向本地 Unified Communications Manager 注册的所有媒体设备列表。
ccmGroup	此表包含 Unified Communications Manager 群集中的 Unified Communications Manager 组。
ccmGroupMapping	此表会将群集中的所有 Unified Communications Manager 映射到一个 Unified Communications Manager 组。 本地 Unified Communications Manager 节点关闭时，此表仍然为空。

表 *23: CISCO-CCM-MIB* 静态表格

表格	内容
ccmProductType	此表包含 Unified Communications Manager（如果是 Unified Communications Manager 群集配置，则为群集）支持的产品类型的列表，包括电话类型、网关类型、媒体设备类型、H.323 设备类型、CTI 设备类型、语音留言传送设备类型和 SIP 设备类型。
ccmRegion、ccmRegionPair	ccmRegionTable 中包含 Cisco Communication Network (CCN) 系统中所有按地理位置分隔的区域的列表。 ccmRegionPairTable 包含 Unified Communications Manager 群集的地理区域对列表。 地理区域对由源区域和目标区域定义。
ccmTimeZone	此表包含 Unified Communications Manager 群集中所有时区组的列表。

表格	内容
ccmDevicePool	此表包含 Unified Communications Manager 群集中所有设备池的列表。 设备池由区域、日期/时间组和 Unified Communications Manager 组定义。

注释 CISCO-CCM-MIB 中的 “ccmAlarmConfigInfo” 和 “ccmQualityReportAlarmConfigInfo” 组定义与所描述的通知有关的配置参数。

CISCO-UNITY-MIB

CISCO-UNITY-MIB 通过连接 SNMP 代理来获取有关 Cisco Unity Connection 的信息。

要查看 CISCO-UNITY-MIB 定义，请转至以下链接并单击 **SNMP V2 MIB**：

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

注释 Cisco Unity Connection 支持此 MIB。 Unified Communications Manager 和 IM and Presence Service 不支持此 MIB。

连接 SNMP 代理支持以下对象。

表 *24: CISCO-UNITY-MIB* 对象

对象	说明
ciscoUnityTable	此表包含 Cisco Unity Connection 服务器的一般信息，例如主机名和版本号。
ciscoUnityPortTable	此表包含 Cisco Unity Connection 语音留言端口的一般信息。
通用 Unity 使用信息对象	此组包含 Cisco Unity Connection 语音留言端口容量和利用率的信息。

SNMP 配置要求

系统不提供默认的 SNMP 配置。 您必须在安装后配置 SNMP 设置以访问 MIB 信息。 Cisco 支持 SNMP V1、V2c 和 V3 版本。

SNMP 代理通过社区名称和身份验证陷阱提供安全性。 您必须配置社区名称以访问 MIB 信息。 下表提供所需的 SNMP 配置设置。

表 *25: SNMP* 配置要求

配置	**Cisco Unified** 功能配置页面
V1/V2c 社区字符串	**SNMP** > **V1/V2c** > 社区字符串

配置	Cisco Unified 功能配置页面
V3 社区字符串	**SNMP** > **V3** > 用户
MIB2 的系统联系人和位置	**SNMP** > 系统组 > **MIB2** 系统组
陷阱目标 (V1/V2c)	**SNMP** > **V1/V2c** > 通知目标
陷阱目标 (V3)	**SNMP** > **V3** > 通知目标

SNMP 版本 1 支持

SNMP 版本 1 (SNMPv1) 是 SNMP 的初始实施版本，它在管理信息结构 (SMI) 规范内运行，并通过用户数据报协议 (UDP)、Internet 协议 (IP) 等协议进行操作。

SNMPv1 SMI 定义高度结构化的表 (MIB)，用于对表格对象（即包含多个变量的对象）的实例进行分组。 表中包含零个或多个被编入索引的行，因此 SNMP 可以使用支持的命令检索或修改整行。

使用 SNMPv1 时，NMS 将发出请求，托管设备则返回响应。 代理使用陷阱操作将重要事件异步通知 NMS。

在功能配置 GUI 中，您可以在 **V1/V2c 配置**窗口中配置 SNMPv1 支持。

SNMP 版本 2c 支持

与 SNMPv1 一样，SNMPv2c 在管理信息结构 (SMI) 规范内工作。 MIB 模块包含相互关联的管理对象的定义。 SNMPv1 中使用的操作与 SNMPv2 中使用的操作类似。 例如，SNMPv2 陷阱操作的功能与 SNMPv1 中使用的功能相同，但它使用不同的消息格式并替换了 SNMPv1 陷阱。

SNMPv2c 中的“通知”操作允许一个 NMS 将陷阱信息发送到另一个 NMS，然后从 NMS 接收响应。

在功能配置 GUI 中，您可以在 **V1/V2c 配置**窗口中配置 SNMPv2c 支持。

SNMP 版本 3 支持

SNMP 版本 3 提供验证（验证请求来自真实来源）、隐私（加密数据）、授权（验证用户允许请求的操作）和访问控制（验证用户拥有所请求对象的访问权限）等安全功能。 要阻止 SNMP 数据包在网络上泄露，您可以配置使用 SNMPv3 加密。

注释 从 12.5(1)SU1 版开始，Unified Communications Manager 中不支持 MD5 或 DES 加密方法。 在添加 SNMPv3 用户时，您可以选择 SHA 或 AES 作为验证协议。

SNMPv3 不使用 SNMPv1 和 v2 之类的团体字符串，而是使用 SNMP 用户。

在功能配置 GUI 中，您可以在 **V3 配置**窗口中配置 SNMPv3 支持。

SNMP 服务

下表中的服务支持 SNMP 操作。

注释 SNMP Master Agent 用作 MIB 接口的主服务。 您必须手动激活 Cisco CallManager SNMP 服务；安装后，所有其他 SNMP 服务都应运行。

表 *26: SNMP* 服务

MIB	服务	窗口
CISCO-CCM-MIB	Cisco CallManager SNMP 服务	**Cisco Unified 功能配置** > **工具** > **控制中心 - 功能服务**。 选择服务器；然后选择“性能和监控”类别。
SNMP 代理	SNMP Master Agent	**Cisco Unified 功能配置** > **工具** > **控制中心 - 网络服务**。 选择服务器；然后选择“平台服务”类别。 **CiscoUnifiedIM and Presence 功能配置** > **工具** > **控制中心 - 网络服务**。 选择服务器；然后选择“平台服务”类别。
CISCO-CDP-MIB	CiscoCDP Agent	
SYSAPPL-MIB	系统应用程序代理	
MIB-II	MIB2 代理	
HOST-RESOURCES-MIB	主机资源代理	
CISCO-SYSLOG-MIB	Cisco Syslog 代理	
硬件 MIB	本机代理适配器	
CISCO-UNITY-MIB	连接 SNMP 代理	**Cisco Unity Connection 功能配置** > **工具** > **服务管理**。选择服务器；然后选择“基础服务”类别。

⚠

注意 停止 SNMP 服务可能会导致数据丢失，因为网络管理系统不再监控 Unified Communications Manager 或 Cisco Unity Connection 网络。 不要停止服务，除非您的技术支持团队告诉您这样做。

SNMP 社区字符串和用户

尽管 SNMP 社区字符串不提供安全性，但它们会验证对 MIB 对象的访问并充当嵌入式密码。 只能为 SNMPv1 和 v2c 配置 SNMP 社区字符串。

SNMPv3 不使用社区字符串。 但版本 3 使用 SNMP 用户。 这些用户的作用与社区字符串相同，但用户可以提供安全性，因为您可以为其配置加密或验证。

在功能配置 GUI 中，不存在默认的社区字符串或用户。

SNMP 陷阱和通知

SNMP 代理会以陷阱或通知的形式将通知发送到 NMS 以标识重要系统事件。 陷阱不会从目标接收确认，而通知会接收确认。 您可以使用功能配置 GUI 中的“SNMP 通知目标配置”窗口配置通知目标。

注释 Unified Communications Manager 在 Unified Communications Manager 和 IM and Presence Service 系统中支持 SNMP 陷阱。

对于 SNMP 通知，如果启用了相应的陷阱标记，则系统会立即发送陷阱。 对于系统日志代理，警报和系统级日志消息将发送到系统日志后台守护程序以进行日志记录。 此外，某些标准的第三方应用程序会将日志消息发送到系统日志后台守护程序以进行日志记录。 这些日志消息将在本地记录在系统日志文件中，并且还将转换为 SNMP 陷阱/通知。

以下列表包含发送到所配置陷阱目标的 Unified Communications Manager SNMP 陷阱/通知消息：

- Unified Communications Manager 发生故障
- 电话发生故障
- 电话状态更新
- 网关发生故障
- 媒体资源列表已耗尽
- 路由列表已耗尽
- 网关第 2 层更改
- 质量报告
- 恶意电话
- 系统日志消息已生成

提示 在配置通知目标之前，请确认所需的 SNMP 服务已激活并正在运行。 此外，请确保已正确为社区字符串/用户配置权限。

您可以在功能配置 GUI 中选择 **SNMP** > **V1/V2** > **通知目标**或 **SNMP** > **V3** > **通知目标**。

下表提供了您在网络管理系统 (NMS) 上配置的陷阱/通知参数的相关信息。 如支持 NMS 的 SNMP 产品文档中所述，您可以通过在 NMS 上发出适当的命令来配置表中的值。

注释 除最后两个参数外，表中所列的所有参数都是 CISCO-CCM-MIB 的一部分。 最后两个参数 clogNotificationsEnabled 和 clogMaxSeverity 包含 CISCO-SYSLOG-MIB 的一部分。

对于 IM and Presence Service，您只能在 NMS 上配置 clogNotificationsEnabled 和 clogMaxSeverity 陷井/通知参数。

表 *27: Cisco Unified Communications Manager* 陷阱/通知配置参数

参数名称	默认值	生成的陷阱	配置建议
ccmCallManagerAlarmEnable	真	ccmCallManagerFailed ccmMediaResourceListExhausted ccmRouteListExhausted ccmTLSConnectionFailure	保留默认规范。
ccmGatewayAlarmEnable	真	ccmGatewayFailed ccmGatewayLayer2Change 尽管您可以在 Cisco Unified Communications Manager 管理中将 CiscoATA 186 设备配置为电话，但当 Unified Communications Manager 为 CiscoATA 设备发送 SNMP 陷阱时，它会发送网关类型的陷阱；例如 ccmGatewayFailed。	无。 此陷阱默认指定为“启用”。
ccmPhoneStatusUpdateStorePeriod ccmPhoneStatusUpdateAlarmInterval	1800 0	ccmPhoneStatusUpdate	将 ccmPhoneStatusUpdateAlarmInterval 设置为介于 30 到 3600 之间的值。
ccmPhoneFailedStorePeriod ccmPhoneFailedAlarmInterval	1800 0	ccmPhoneFailed	将 ccmPhoneFailedAlarmInterval 设置为介于 30 到 3600 之间的值。
ccmMaliciousCallAlarmEnable	真	ccmMaliciousCall	无。 此陷阱默认指定为“启用”。
ccmQualityReportAlarmEnable	真	仅当 CiscoExtended Functions 服务在服务器上（如果是群集配置 [仅 Unified Communications Manager]，则是在本地 Unified Communications Manager 服务器上）激活并运行时，才会生成此陷阱。 ccmQualityReport	无。 此陷阱默认指定为“启用”。
clogNotificationsEnabled	假	clogMessageGenerated	要启用陷阱生成，将 clogNotificationsEnable 设置为 True。
clogMaxSeverity	预警	clogMessageGenerated	当您将 clogMaxSeverity 设置为预警时，如果应用程序生成至少具有预警严重性级别的系统日志消息，将生成 SNMP 陷阱。

SFTP 服务器支持

对于内部测试，我们使用 Cisco Prime Collaboration Deployment (PCD) 上的 SFTP 服务器（由 Cisco 打造，Cisco TAC 提供支持）。 参阅下表可大致了解 SFTP 服务器的选项：

表 *28: SFTP* 服务器支持

SFTP 服务器	支持说明
Cisco Prime Collaboration 部署上的 SFTP 服务器	此服务器是 Cisco 提供和测试的唯一 SFTP 服务器，并且完全受 Cisco TAC 支持。 版本兼容性取决于您的 Emergency Responder 版本和 Cisco Prime Collaboration 部署。 在升级其版本 (SFTP) 或 Emergency Responder 之前，请参阅《Cisco Prime Collaboration 部署管理指南》，以确保版本兼容。
来自技术合作伙伴的 SFTP 服务器	这些服务器由第三方提供，第三方测试。 版本兼容性取决于第三方测试。 如果升级其 SFTP 产品和/或升级版本兼容的 Unified Communications Manager，请参阅“技术合作伙伴”页面： https://marketplace.cisco.com
来自其他第三方的 SFTP 服务器	这些服务器由第三方提供，不受 Cisco TAC 官方支持。 版本兼容性乃尽力提供，以建立兼容的 SFTP 版本和 Emergency Responder 版本。 **注释** 这些产品未经 Cisco 测试，我们无法保证其功能。 Cisco TAC 不支持这些产品。 要获取经过全面测试且受支持的 SFTP 解决方案，请使用 Cisco Prime Collaboration 部署或技术合作伙伴。

SNMP 配置任务流程

完成这些任务以配置简单的网络管理协议。 确保您知道要配置的 SNMP 版本，因为任务可能会有所不同。 您可以从 SNMP V1、V2c 或 V3 中进行选择。

开始之前

安装和配置 SNMP 网络管理系统。

过程

	命令或操作	目的
步骤 1	激活 SNMP 服务，第 166 页	确认基本的 SNMP 服务正在运行。

	命令或操作	目的
步骤 2	根据您的 SNMP 版本完成以下任务之一： • 配置 SNMP 社区字符串，第 167 页 • 配置 SNMP 用户，第 169 页	对于 SNMP V1 或 V2，配置社区字符串。 对于 SNMP V3，配置 SNMP 用户。
步骤 3	获取远程 SNMP 引擎 ID，第 172 页	对于 SNMP V3，获取“通知目标”配置中必需的远程 SNMP 引擎的地址。 注释 对于 SNMP V3，此程序是必需的；但对于 SNMP V1 或 V2c，可选择性执行。
步骤 4	配置 SNMP 通知目标，第 173 页	对于所有 SNMP 版本，配置 SNMP 陷阱和通知的通知目标。
步骤 5	配置 MIB2 系统组，第 177 页	配置 MIB-II 系统组的系统联系人和系统位置。
步骤 6	CISCO-SYSLOG-MIB 陷阱参数，第 178 页	配置 CISCO-SYSLOG-MIB 的陷阱设置。
步骤 7	CISCO-CCM-MIB 陷阱参数，第 179 页	仅 Unified Communications Manager：配置 CISCO-CCM-MIB 的陷阱设置。
步骤 8	重新启动 SNMP Master Agent，第 179 页	完成 SNMP 配置后，重新启动 SNMP Master Agent。
步骤 9	在 SNMP 网络管理系统中，配置 Unified Communications Manager 陷阱参数。	

激活 SNMP 服务

此程序可用于确保 SNMP 服务已启动并正在运行。

过程

步骤 1 登录到 Cisco Unified 功能配置。

步骤 2 确认 **Cisco SNMP Master Agent** 网络服务正在运行。 此服务默认启用。

a) 选择**工具** > **控制中心 - 网络服务**。
b) 选择发布方节点，然后单击**前往**。
c) 验证 **Cisco SNMP Master Agent** 服务是否正在运行。

步骤 3 启动 **Cisco Call Manager SNMP 服务**。

a) 选择**控制中心** > **服务激活**。
b) 从**服务器**下拉列表中，选择发布方节点并单击**前往**。

c) 确认 **Cisco Call Manager SNMP 服务**正在运行。 如果未运行，请选中相应的复选框，然后单击**保存**。

下一步做什么

如果要配置 SNMP V1 或 V2c，配置 SNMP 社区字符串，第 167 页。

如果要配置 SNMP V3，配置 SNMP 用户，第 169 页。

配置 SNMP 社区字符串

如果您部署的是 SNMP V1 或 V2c，此程序可用于设置 SNMP 社区字符串。

注释 必须为 SNMP V1 或 V2c 执行此程序。 对于 SNMP V3，配置 SNMP 用户而不是社区字符串。

过程

步骤 1 从 Cisco Unified 功能配置中，选择 **Snmp** > **V1/V2c** > **社区字符串**。

步骤 2 选择**服务器**，然后单击**查找**以搜索现有的社区字符串。 您也可以输入搜索参数来查找特定的社区字符串。

步骤 3 执行以下任一操作：

- 要编辑现有的 SNMP 社区字符串，请选择该字符串。
- 要添加新的社区字符串，请单击**新增**。

注释 要删除现有的社区字符串，请选择该字符串，然后单击**删除选定项**。 删除用户后，重新启动 Cisco SNMP Master Agent。

步骤 4 输入**社区字符串名称**。

步骤 5 填写**SNMP 社区字符串配置**窗口中的字段。 有关字段及其设置的帮助信息，请参阅：社区字符串配置设置，第 168 页。

步骤 6 从**访问权限**下拉框中，配置此社区字符串的权限。

步骤 7 如果要将这些设置应用到所有群集节点，请选中**应用到所有节点**复选框。

步骤 8 单击**保存**。

步骤 9 单击**确定**重新启动 SNMP Master Agent 服务并使更改生效。

下一步做什么

配置 SNMP 通知目标，第 173 页

社区字符串配置设置

下表介绍了社区字符串配置设置。

表 *29*: 社区字符串配置设置

字段	说明
服务器	“社区字符串配置”窗口中的此设置显示为只读，因为您在查找社区字符串的过程中执行此程序时指定了该服务器选项。 要更改社区字符串的服务器，请执行查找社区字符串程序。
社区字符串	输入社区字符串的名称。 名称最多可以包含 32 个字符，可以包含字母数字字符、连字符 (-) 和下划线字符 (_) 的任意组合。 **提示** 选择社区字符串名称对于局外人来说很难判断。 编辑社区字符串时，您无法更改社区字符串的名称。
接受来自任何主机的 SNMP 数据包	要接受来自任何主机的 SNMP 数据包，请单击此按钮。
仅接受来自这些主机的 SNMP 数据包	要接受来自特定主机的 SNMP 数据包，请单击此单选按钮。 在“主机名/IPv4/IPv6 地址”字段中，输入要接受其 SNMP 数据包的 IPv4 或 IPv6 地址，然后单击**插入**。 以点分十进制格式输入 IPv4 地址。 例如 10.66.34.23。 IPv6 地址以冒号分隔的十六进制格式表示。 例如 2001:0db8:85a3:0000:0000:8a2e:0370:7334 或 2001:0db8:85a3::8a2e:0370:7334。 对要接受其 SNMP 数据包的每个地址重复此过程。 要删除地址，从“主机 IPv4/IPv6 地址”列表框中选择该地址，然后单击**删除**。

字段	说明
访问权限	从下拉列表框的以下列表中选择适当的访问级别： **ReadOnly** 社区字符串只能读取 MIB 对象的值。 **ReadWrite** 社区字符串可以读取和写入 MIB 对象的值。 **ReadWriteNotify** 社区字符串可以读取和写入 MIB 对象的值以及发送 MIB 对象值用于陷阱和通知消息。 **NotifyOnly** 社区字符串只能发送 MIB 对象值用于陷阱和通知消息。 **ReadNotifyOnly** 社区字符串可以读取MIB对象的值，也可以发送该值用于陷阱和通知消息。 无 社区字符串无法读取、写入或发送陷阱信息。 提示 要更改陷阱配置参数，为社区字符串配置 NotifyOnly、ReadNotifyOnly 或 ReadWriteNotify 权限。 IM and Presence Service 不支持 ReadNoticyOnly。
应用到所有节点	要将社区字符串应用到群集中的所有节点，请选中此复选框。 此字段仅适用于 Unified Communications Manager 和 IM and Presence Service 群集。

配置 SNMP 用户

如果您部署的是 SNMP V3，此程序可用于设置 SNMP 用户。

注释 此程序仅适用于 SNMP V3。 对于 SNMP V1 或 V2c，请改为配置社区字符串。

过程

步骤 1 从 Cisco Unified 功能配置中，选择 **Snmp** > **V3** > **用户**。

步骤 2 选择**服务器**，然后单击**查找**以搜索现有的 SNMP 用户。 您也可以输入搜索参数来查找特定的用户。

步骤 3 执行以下任一操作：

- 要编辑现有 SNMP 用户，选择用户。
- 要添加新的 SNMP 用户，单击**新增**。

注释 要删除现有用户，选择用户并单击**删除选定项**。 删除用户后，重新启动 Cisco SNMP Master Agent。

步骤 4 输入 **SNMP 用户名**。

步骤 5 输入 SNMP 用户配置设置。 有关字段及其设置的帮助信息，请参阅：SNMP V3 用户配置设置，第 170 页。

提示 在保存配置之前，您可以随时单击**全部清除**按钮删除您在窗口中为所有设置输入的所有信息。

步骤 6 从**访问权限**下拉框中，配置要分配给此用户的访问权限。

步骤 7 如果要将此配置应用到所有群集节点，请选中**应用到所有节点**复选框。

步骤 8 单击**保存**。

步骤 9 单击**确定**重新启动 SNMP Master Agent。

注释 要使用您配置的用户访问服务器，请确保使用适当的验证和隐私设置在NMS上配置此用户。

下一步做什么

获取远程 SNMP 引擎 ID，第 172 页

SNMP V3 用户配置设置

下表介绍了 SNMP V3 用户配置设置。

表 *30: SNMP V3* 用户配置设置

字段	说明
服务器	此设置显示为只读，因为您在执行查找通知目标程序时指定了服务器。 要更改想为其提供访问权限的服务器，请执行以下程序以查找 SNMP 用户。

字段	说明
用户名	在字段中，输入您要为其提供访问权限的用户的名称。 名称最多可以包含 32 个字符，可以包含字母数字字符、连字符 (-) 和下划线字符 (_) 的任意组合。 **提示** 输入您已为网络管理系统 (NMS) 配置的用户。 对于现有的 SNMP 用户，此设置显示为只读。
需要验证	若要要求验证，请选中该复选框，在“密码”和“重新输入密码”字段中输入密码，然后选择适当的协议。 密码必须至少包含 8 个字符。 **注释** 如果启用了 FIPS 模式或增强的安全模式，请选择 **SHA** 作为协议。
需要隐私	如果选中了“需要验证”复选框，您可以指定隐私信息。 若要要求隐私，请选中该复选框，在“密码”和“重新输入密码”字段中输入密码，然后选中协议复选框。 密码必须至少包含 8 个字符。 **注释** 如果启用了 FIPS 模式或增强的安全模式，请选择 **AES128** 作为协议。
接受来自任何主机的 SNMP 数据包	要接受来自任何主机的 SNMP 数据包，请单击此单选按钮。
仅接受来自这些主机的 SNMP 数据包	要接受来自特定主机的 SNMP 数据包，请单击此单选按钮。 在“主机名/IPv4/IPv6 地址”字段中，输入要接受其 SNMP 数据包的 IPv4 或 IPv6 地址，然后单击**插入**。 以点分十进制格式输入 IPv4 地址。 例如 10.66.34.23。 IPv6 地址以冒号分隔的十六进制格式表示。 例如 2001:0db8:85a3:0000:0000:8a2e:0370:7334 或 2001:0db8:85a3::8a2e:0370:7334。 对要接受其 SNMP 数据包的每个地址重复此过程。 要删除地址，从“主机 IPv4/IPv6 地址”列表框中选择该地址，然后单击**删除**。

字段	说明
访问权限	从下拉列表框中，选择以下选项之一作为访问级别： **ReadOnly** 您只能读取 MIB 对象的值。 **ReadWrite** 您能读取和写入 MIB 对象的值。 **ReadWriteNotify** 您可以读取和写入 MIB 对象的值以及发送 MIB 对象值用于陷阱和通知消息。 **NotifyOnly** 您只能发送 MIB 对象值用于陷阱和通知消息。 **ReadNotifyOnly** 您可以读取 MIB 对象的值，也可以发送该值用于陷阱和通知消息。 无 您无法读取、写入或发送陷阱信息。 **提示** 要更改陷阱配置参数，为用户配置 NotifyOnly、ReadNotifyOnly 或 ReadWriteNotify 权限。
应用到所有节点	要将用户配置应用到群集中的所有节点，请选中此复选框。 这仅适用于 Unified Communications Manager 和 IM and Presence Service 群集。

获取远程 SNMP 引擎 ID

如果要部署 SNMP V3，此程序可用于获取通知目标配置所需的远程 SNMP 引擎 ID。

注释 对于 SNMP V3，此程序是必需的；但对于 SNMP V1 或 2C，可选择性执行。

过程

步骤 1 登录到命令行界面。

步骤 2 运行 `utils snmp walk 1` CLI 命令。

步骤 3 输入配置的团体字符串（对于 SNMP V1/V2）或配置的用户（对于 SNMP V3）。

步骤 4 输入服务器的 IP 地址。 例如，为本地主机输入 `127.0.0.1`。

步骤 5 输入 `1.3.6.1.6.3.10.2.1.1.0` 作为对象 ID (OID)。

步骤 6 对于文件，输入 `file`。

步骤 7 输入 `y`。
系统输出代表远程 SNMP 引擎 ID 的十六进制字符串。

步骤 8 对运行 SNMP 的每个节点重复上述过程。

下一步做什么

配置 SNMP 通知目标，第 173 页

配置 SNMP 通知目标

此程序可用于配置 SNMP 陷阱和通知的通知目标。 您可以对 SNMP V1、V2c 或 V3 执行此程序。

开始之前

如果尚未设置 SNMP 社区字符串或 SNMP 用户，请完成以下任务之一：

- 对于 SNMP V1/V2，请参阅：配置 SNMP 社区字符串，第 167 页
- 对于 SNMP V3，请参阅配置 SNMP 用户，第 169 页

过程

步骤 1 从 Cisco Unified 功能配置中，选择以下各项之一：

- 对于 SNMP V1/V2，选择 **Snmp** > **V1/V2** > **通知目标**
- 对于 SNMP V3，选择 **Snmp** > **V3** > **通知目标**

步骤 2 选择一个**服务器**，然后单击**查找**以搜索现有的 SNMP 通知目标。 您也可以输入搜索参数来查找特定的目标。

步骤 3 执行以下任一操作：

- 要编辑现有的 SNMP 通知目标，选择通知目标。
- 要添加新的 SNMP 通知目标，单击**新增**。

注释 要删除现有的 SNMP 通知目标，选择目标并单击**删除选定项**。 删除用户后，重新启动 **Cisco SNMP Master Agent**。

步骤 4 从**主机 IP 地址**下拉框中，选择现有地址或单击**新增**，然后输入新的主机 IP 地址。

步骤 5 仅 SNMP V1/V2。 在 **SNMP 版本**字段中，选中 V1 或 V2C 单选按钮，具体取决于您配置的是 SNMP V1 还是 V2c。

步骤 6 对于 SNMP V1/V2，请完成以下步骤：

a) 仅 SNMP V2。 从**通知类型**下拉框中，选择**通知**或**陷阱**。
b) 选择您配置的**社区字符串**。

步骤 7 对于 SNMP V3，请完成以下步骤：

a) 从**通知类型**下拉框中，选择**通知**或**陷阱**。
b) 从**远程 SNMP 引擎 ID** 下拉框中，选择现有引擎 ID 或选择**新增**，然后输入新的 ID。
c) 从**安全级别**下拉框中，分配适当的安全级别。

步骤 8 如果要将此配置应用到所有群集节点，请选中**应用到所有节点**复选框。

步骤 9 单击**插入**。

步骤 10 单击**确定**重新启动 SNMP Master Agent。

示例

注释 有关“通知目标配置”窗口中的字段说明帮助，请参阅以下主题之一：

- SNMP V1 和 V2c 的通知目标设置，第 174 页
- SNMP V3 的通知目标设置，第 175 页

下一步做什么

配置 MIB2 系统组，第 177 页

SNMP V1 和 V2c 的通知目标设置

下表介绍了 SNMP V1/V2c 的通知目标配置设置。

表 *31: SNMP V1/V2c* 的通知目标配置设置

字段	说明
服务器	此设置显示为“只读”，因为您在执行查找通知目标程序时指定了服务器。 要更改通知目标的服务器，请执行查找社区字符串程序。
主机 IPv4/IPv6 地址	从下拉列表框中，选择陷阱目标的主机 IPv4/IPv6 地址，或者单击**新增**。如果单击**新增**，请在“主机 IPv4/IPv6 地址”字段中输入陷阱目标的 IPv4/IPv6 地址。 对于现有的通知目标，您无法修改主机 IP 地址配置。

字段	说明
主机 IPv4/IPv6 地址	在该字段中，输入要从中接受 SNMP 数据包的 IPv4 或 IPv6 地址。 以点分十进制格式输入 IPv4 地址。 例如 10.66.34.23。 IPv6 地址以冒号分隔的十六进制格式表示。 例如 2001:0db8:85a3:0000:0000:8a2e:0370:7334 或 2001:0db8:85a3::8a2e:0370:7334。
端口号	在该字段中，输入接收SNMP数据包的目标服务器上的通知接收端口号。
V1 或 V2c	在“SNMP 版本信息”窗格中，单击适当的 SNMP 版本单选按钮，即 V1 或 V2c，具体取决于您使用的 SNMP 版本。 • 如果选择 V1，请配置社区字符串设置。 • 如果选择 V2c，请配置通知类型设置，然后配置社区字符串。
社区字符串	从下拉列表框中，选择要在此主机生成的通知消息中使用的社区字符串名称。 只显示具有最小通知权限（ReadWriteNotify 或仅通知）的社区字符串。 如果您尚未配置具有这些权限的社区字符串，下拉列表框中将不会显示任何选项。 如有必要，单击**创建新社区字符串** 以创建社区字符串。 仅限 IM and Presence：仅显示具有最小通知权限（ReadWriteNotify、ReadNotifyOnly 或仅通知）的社区字符串。 如果您尚未配置具有这些权限的社区字符串，下拉列表框中将不会显示任何选项。 如有必要，单击**创建新社区字符串**以创建社区字符串。
通知类型	从下拉列表框中选择适当的通知类型。
应用到所有节点	要将通知目标配置应用到群集中的所有节点，请选中此复选框。 这仅适用于 Cisco Unified Communications Manager 和 IM and Presence Service 群集。

SNMP V3 的通知目标设置

下表介绍了 SNMP V3 的通知目标配置设置。

表 *32: SNMP V3* 的通知目标配置设置

字段	说明
服务器	此设置显示为“只读”，因为您在执行查找 SNMP V3 通知目标程序时指定了服务器。 要更改通知目标的服务器，请执行查找 SNMP V3 通知目标程序并选择其他服务器。

字段	说明
主机 IPv4/IPv6 地址	从下拉列表框中，选择陷阱目标的主机 IPv4/IPv6 地址，或者单击**新增**。如果单击**新增**，请在“主机 IPv4/IPv6 地址”字段中输入陷阱目标的 IPv4/IPv6 地址。 对于现有的通知目标，您无法修改主机 IP 地址配置。
主机 IPv4/IPv6 地址	在该字段中，输入要从中接受 SNMP 数据包的 IPv4 或 IPv6 地址。 以点分十进制格式输入 IPv4 地址。 例如 10.66.34.23。 IPv6 地址以冒号分隔的十六进制格式表示。 例如 2001:0db8:85a3:0000:0000:8a2e:0370:7334 或 2001:0db8:85a3::8a2e:0370:7334。
端口号	在该字段中，输入目标服务器上的通知接收端口号。
通知类型	从下拉列表框中，选择**通知**或**陷阱**。 **提示** Cisco 建议您选择“通知”选项。“通知”功能会重新传输消息，直到被确认，因此比陷阱更可靠。
远程 SNMP 引擎 ID	如果您从“通知类型”下拉列表框中选择“通知”，则会显示此设置。 从下拉列表框中，选择引擎 ID 或选择**新增**。 如果您选择了“新增”，请在“远程 SNMP 引擎 ID”字段中输入 ID，要求为十六进制值。
安全级别	从下拉列表框中为用户选择适当的安全级别。 **noAuthNoPriv** 未配置身份验证或隐私。 **authNoPriv** 身份验证已配置，但未配置隐私。 **authPriv** 未配置身份验证和隐私。
用户信息窗格	从该窗格中，执行以下任务之一，以将通知目标与用户关联或取消关联。 1. 要创建新用户，请单击**创建新用户**。 2. 要修改现有用户，请单击该用户的单选按钮，然后单击**更新所选用户**。 3. 要删除用户，请单击该用户的单选按钮，然后单击**删除所选用户**。 显示的用户根据您为通知目标配置的安全级别而有所不同。
应用到所有节点	要将通知目标配置应用到群集中的所有节点，请选中此复选框。 这仅适用于 Cisco Unified Communications Manager 和 IM and Presence Service 群集。

配置 MIB2 系统组

此程序可用于配置MIB-II系统组的系统联系人和系统位置。 例如，可为系统联系人输入Administrator, 555-121-6633，为系统位置输入 SanJose, Bldg 23, 2nd floor。 您可以对 SNMP V1、V2 和 V3 执行此程序。

过程

步骤 1 从 Cisco Unified 功能配置中，选择 **Snmp** > **系统组** > **MIB2 系统组**。

步骤 2 从**服务器**下拉列表中选择一个节点，然后单击**前往**。

步骤 3 填写**系统联系人**和**系统位置**字段。

步骤 4 如果要将这些设置应用到所有群集节点，请选中**应用到所有节点**复选框。

步骤 5 单击**保存**。

步骤 6 单击**确定**重新启动 SNMP Master Agent 服务

示例

注释 有关字段说明帮助，请参阅 MIB2 系统组设置 ，第 177 页

注释 您可以单击**全部清除**以清除这些字段。 如果单击**全部清除**，然后单击**保存**，该记录将删除。

MIB2 系统组设置

下表介绍了 MIB2 系统组配置设置。

表 *33: MIB2* 系统组配置设置

字段	说明
服务器	从下拉列表框中，选择要为其配置联系人的服务器，然后单击 **前往**。
系统联系人	输入出现问题时要通知的人员。
系统位置	输入标识为系统联系人的人员位置。
应用到所有节点	选中以将系统配置应用到群集中的所有节点。 这仅适用于 Unified Communications Manager 和 IM and Presence Service 群集。

CISCO-SYSLOG-MIB 陷阱参数

使用以下原则配置您系统中的 CISCO-SYSLOG-MIB 陷阱设置：

- 使用 SNMP 设置操作将 clogsNotificationEnabled (1.3.6.1.4.1.9.9.41.1.1.2) 设置为 True；例如，从 linux 命令行使用以下命令，利用 net-snmp set 实用程序将此 OID 设置为 True：

```
snmpset -c <community string>-v2c <transmitter ipaddress>
1.3.6.1.4.1.9.9.41.1.1.2.0 i 1
```

  您也可以使用任何其他 SNMP 管理应用程序进行 SNMP 设置操作。

- 通过使用 SNMP 设置操作设置 clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) 值；例如，从 linux 命令行使用以下命令，利用 net-snmp set 实用程序设置此 OID 值：

```
snmpset-c public-v2c <transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.3.0 i
<value>
```

  输入 <value> 设置的严重性数值。 严重性值越高，严重性越低。 值为 1（危急）表示严重性最高，而值为 8（调试）表示严重性最低。 系统日志代理将忽略大于您指定的值的任何消息；例如，要捕获所有系统日志消息，使用的值为 8。

  严重性值如下：

  - 1：危急
  - 2：警告
  - 3：严重
  - 4：错误
  - 5：预警
  - 6：通知
  - 7：信息
  - 8：调试

  您也可以使用任何其他 SNMP 管理应用程序进行 SNMP 设置操作。

注释 在日志记录之前，系统日志会截断大于指定系统日志缓冲区大小的任何陷阱消息数据。 系统日志陷阱消息长度的限制为 255 字节。

CISCO-CCM-MIB 陷阱参数

- 使用 SNMP 设置操作将 ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) 设置为一个介于 30-3600 之间的值；例如，从 linux 命令行使用以下命令，利用 net-snmp set 实用程序设置此 OID 值：

```
snmpset -c <community string> -v2c <transmitter ipaddress>
1.3.6.1.4.1.9.9.156.1.9.2 .0 i <value>
```

  您也可以使用任何其他 SNMP 管理应用程序进行 SNMP 设置操作。

- 使用 SNMP 设置操作将 ccmPhoneStatusUpdateAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.4) 设置为一个介于 30-3600 之间的值；例如，从 linux 命令行使用以下命令，利用 net-snmp set 实用程序设置此 OID 值：

```
snmpset -c <community string> -v2c <transmitter ipaddress>
1.3.6.1.4.1.9.9.156.1.9.4.0 i <value>
```

  您也可以使用任何其他 SNMP 管理应用程序进行 SNMP 设置操作。

CISCO-UNITY-MIB 陷阱参数

仅 Cisco Unity Connection：Cisco Unity Connection SNMP 代理不会启用陷阱通知，不过可以通过 Cisco Unity Connection 警报触发陷阱。 您可以在 Cisco Unity Connection 功能配置的**警告** > **定义**屏幕上查看 Cisco Unity Connection。

您可以使用 CISCO-SYSLOG-MIB 配置陷阱参数。

相关主题

CISCO-SYSLOG-MIB 陷阱参数 ，第 178 页

重新启动 SNMP Master Agent

完成所有 SNMP 配置后，重新启动 SNMP Master Agent 服务。

过程

步骤 1 在 Cisco Unified 功能配置中，选择**工具** > **控制中心 - 网络服务**。

步骤 2 选择**服务器**并单击**前往**。

步骤 3 选择 **SNMP Master Agent**。

步骤 4 单击**重新启动**。

SNMP 陷阱设置

CLI 命令可用于设置可配置的 SNMP 陷阱设置。 SNMP 陷阱配置参数和建议的配置提示适用于 CISCO-SYSLOG-MIB、CISCO-CCM-MIB 和 CISCO-UNITY-MIB。

配置 SNMP 陷阱

此程序可用于配置 SNMP 陷阱。

开始之前

为 SNMP 配置您的系统。 有关详细信息，请参阅SNMP 配置任务流程，第 165 页。

确保 SNMP 社区字符串（对于 SNMP V1/V2）或 SNMP 用户（对于 SNMP V3）的**访问权限**设置为以下设置之一：**ReadWriteNotify**、**ReadNotify**、**NotifyOnly**。

过程

步骤 1 登录到 CLI 并运行 `utils snmp test` CLI 命令以验证 SNMP 是否正在运行。

步骤 2 按照生成 SNMP 陷阱，第 180 页生成特定的 SNMP 陷阱（例如，ccmPhoneFailed 或 MediaResourceListExhausted 陷阱）。

步骤 3 如果陷阱未生成，请执行以下步骤：

- 在 Cisco Unified 功能配置中，选择**警报** > **配置**，然后选择 **CM 服务**和 **Cisco CallManager**。
- 选中**应用到所有节点**复选框。
- 在“本地系统日志”中，从“警报事件等级”下拉列表选择**信息**。

步骤 4 复制陷阱并检查 CiscoSyslog 文件中是否已记录相应的警报。

生成 SNMP 陷阱

本部分介绍特定类型的 SNMP 陷阱的生成过程。 必须在服务器上设置并运行 SNMP，才能生成单个陷阱。 有关如何设置系统以生成 SNMP 陷阱的说明，请参阅配置 SNMP 陷阱，第 180 页。

注释 各个 SNMP 陷阱的处理时间因您尝试生成的陷阱而异。 有些 SNMP 陷阱可能需要几分钟才能生成。

表 *34:* 生成 *SNMP* 陷阱

SNMP 陷阱	进程
ccmPhoneStatusUpdate	要触发 ccmPhoneStatusUpdate 陷阱： 1. 在 ccmAlarmConfig Info mib 表中，设置 ccmPhoneStatusUpdateAlarmInterv (1.3.6.1.4.1.9.9.156.1.9.4) = 30 或更大值。 2. 登录 Cisco Unified Communications Manager 管理。 3. 重置正在使用并且已注册到 Unified Communications Manager 的电话。 电话将先取消注册，然后重新注册，生成 ccmPhoneStatusUpdate 陷阱。
ccmPhoneFailed	要触发 ccmPhoneFailed 陷阱： 1. 在 ccmAlarmConfigInfo mib 表中，设置 ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) =30 或更大值。 2. 在 Cisco Unified Communications Manager 管理中，将电话的 MAC 地址更改为无效值。 3. 在 Cisco Unified Communications Manager 管理中，重新注册电话。 4. 将电话设置为指向 TFTP 服务器 A，然后将电话插入另一台服务器。
ccmGatewayFailed	要触发 ccmGatewayFailed SNMP 陷阱： 1. 确认 ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6) 设置为 true。 2. 在 Cisco Unified Communications Manager 管理中，将网关的 MAC 地址更改为无效值。 3. 重新启动网关。
ccmGatewayLayer2Change	要在第 2 层受到监控（例如 MGCP 回传负载）的工作网关上触发 ccmGatewayLayer2Change 陷阱： 1. 在 ccmAlarmConfig Info mib 表中，设置 ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6.0) = true。 2. 在 Cisco Unified Communications Manager 管理中，将网关的 MAC 地址更改为无效值。 3. 重置网关。

SNMP 陷阱	进程
MediaResourceListExhausted	要触发 MediaResourceListExhausted 陷阱： 1. 在 Cisco Unified Communications Manager 管理中，创建包含标准会议桥资源 (CFB-2) 之一的媒体资源组。 2. 创建包含您创建的媒体资源组的媒体资源组列表。 3. 在“电话配置”窗口中，将“媒体资源组列表”字段设置为您创建的媒体资源组列表。 4. 停止 IP 语音媒体流服务。 此操作会导致会议桥资源 (CFB-2) 停止工作。 5. 通过使用媒体资源组列表的电话发起会议呼叫。 电话屏幕上将显示消息：“没有可用的会议桥”。
RouteListExhausted	要触发 RouteListExhausted 陷阱： 1. 创建包含一个网关的路由组。 2. 创建包含您刚刚创建的路由组的路由组列表。 3. 创建一个通过路由组列表路由呼叫的唯一路由模式。 4. 取消注册网关。 5. 从其中一部电话拨打与路由模式匹配的号码。
MaliciousCallFailed	要触发 MaliciousCallFailed 陷阱： 1. 创建包含所有可用 "MaliciousCall" 软键的软键模板。 2. 将新的软键模板分配给网络中的电话，然后重置电话。 3. 在电话之间发起呼叫。 4. 在呼叫过程中，选择 "MaliciousCall" 软键。

SNMP 陷阱	进程
ccmCallManagerFailed	1. 运行 `show process list` CLI 命令以获取 CallManager application ccm 的进程标识符。 此命令将返回多个进程及其 PID。 您必须获取 ccm 的PID，因为必须停止该 PID 才能生成警报。 2. 运行 `delete process <pid>` crash CLI 命令 3. 运行 CLI 命令。 生成内部错误时，将生成 CallManager 失败警报。 这些内部错误可能包括由于缺少 CPU 而导致内部线程退出、CallManager 服务器暂停超过 16 秒以及计时器问题。 您无法手动生成此警报。 **注释** 生成 ccmCallManagerFailed 警报或陷阱时，系统将关闭 CallManager 服务并生成核心文件。 为避免混淆，Cisco 建议您立即删除核心文件。
作为陷阱的系统日志消息	要接收特定严重性以上的系统日志消息作为陷阱，请在 clogBasic 表中设置以下两个 mib 对象： 1. 将 clogNotificationsEnabled (1.3.6.1.4.1.9.9.41.1.1.2) 设置为 true(1)。 默认值为 false(2)。 例如，snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1 2. 将 clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) 的级别设置为大于您希望陷阱生成时的级别。 默认值为预警 (5)。 警报严重性小于或等于所配置的严重性级别的所有系统日志消息都作为陷阱发送。 例如，snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>

SNMP 跟踪配置

对于 Unified Communications Manager，您可以在 Cisco Unified 功能配置的“跟踪配置”窗口中为 Cisco CallManager SNMP 代理配置跟踪，方法是在“性能和监控服务”服务组中选择 Cisco CallManager SNMP 服务。 所有代理都有默认设置。 对于 Cisco CDP 代理和 Cisco 系统日志代理，您可以使用 CLI 更改跟踪设置，如《*Cisco Unified* 解决方案的命令行界面参考指南》中所述。

对于 Cisco Unity Connection，您可以在 Cisco Unity Connection 功能配置的“跟踪配置”窗口中为 Cisco Unity Connection SNMP 代理配置跟踪，方法是选择“连接 SNMP 代理”组件。

SNMP 故障诊断

请查看此部分以获取故障诊断提示。 确保所有功能和网络服务都在正常运行。

问题

您无法从系统轮询任何 MIB。

这种情况表明没有在系统上配置社区字符串或 snmp 用户，或者配置的社区字符串或 snmp 用户与系统上配置的不匹配。 默认情况下，系统上未配置任何社区字符串或用户。

解决方案

使用 SNMP 配置窗口检查系统上配置的社区字符串或 snmp 用户是否正确。

问题

您无法从系统收到任何通知。

这种情况表明系统上未正确配置通知目标。

解决方案

确认您已在通知目标（V1/V2c 或 V3）配置窗口中正确配置通知目标。

第 16 章

服务

功能服务

使用功能配置 GUI 激活、启动和停止 Cisco Unified Communications Manager 和 IM and Presence Service。 激活将打开并启动服务。 您必须为想要使用的所有功能手动激活该功能服务。 有关服务激活建议，请参阅与服务激活相关的主题。

注释 如果您尝试从 IM and Presence 节点访问 Unified Communications Manager 服务器（反之亦然），可能会遇到以下错误：“无法建立与服务器的连接（无法访问远程节点）”。 如果出现此错误消息，请参阅《*Cisco Unified Communications Manager* 管理指南》。

注释 使用 IM and Presence 的设备配置为使用 Postgres 外部数据库以支持永久聊天、合规性和文件传输。 不过，IM and Presence 服务器与 Postgres 之间的连接不安全，并且数据传递未经任何检查。 对于不支持 TLS 的服务或设备，可以通过配置 IP Sec 以另一种方式提供安全通信，这是通过身份验证和加密通信会话的每个 IP 数据包进行的标准安全通信协议。

在**服务激活**窗口中激活服务后，无需在**控制中心 - 功能服务**窗口中启动它。 如果服务因任何原因不启动，则必须在**控制中心-功能服务**窗口中启动。

系统安装好后，它不会自动激活功能服务，您需要激活功能服务以使用您的配置功能，例如功能配置报告存档功能。

仅限 Unified Communications Manager 和 Cisco Unified IM and Presence Service：如果升级 Unified Communications Manager，则升级之前在系统激活的那些服务将在升级后自动升级。

激活功能服务后，您可以使用产品的管理 GUI 修改服务参数设置：

- Cisco Unified Communications Manager 管理
- Cisco Unity Connection 管理

功能服务类别

在 Cisco Unified 功能配置中，**服务激活**窗口和**控制中心 - 功能服务**窗口将功能服务归类到以下组中：

- 数据库和管理服务
- 性能和监控服务
- CM 服务
- CTI 服务
- CDR 服务
- 安全服务
- 目录服务
- 语音质量报告程序服务

在 Cisco Unified IM and Presence 功能配置中，**服务激活**窗口和**控制中心 - 功能服务**窗口将功能服务归类到以下组中：

- 数据库和管理服务
- 性能和监控服务
- IM and Presence Service 服务

数据库和管理服务

位置带宽管理器

IM and Presence Service 不支持此服务。

位置带宽管理器服务从一个或多个群集的配置位置和链路数据中组装网络模型，确定位置对之间的有效路径，确定是否基于每种呼叫的带宽可用性承认位置对之间的呼叫，以及在被承认的每个呼叫的持续时间内扣除（保留）带宽。

Cisco AXL Web 服务

Cisco AXL Web 服务允许您从使用 AXL 的基于客户端的应用程序修改数据库条目和执行已存储程序。

在 IM and Presence Service 系统中，此服务支持 Unified Communications Manager 和 Cisco Unity Connection。

Cisco UXL Web 服务

IM and Presence Service 不支持此服务。

Cisco IP 电话通讯簿同步程序中的 TabSync 客户端使用 Cisco UXL Web 服务查询 Unified Communications Manager 数据库，从而确保 Cisco IP 电话通讯簿同步程序用户只能访问与其相关的最终用户数据。Cisco UXL Web 服务执行以下功能：

- 当最终用户登录到 Cisco IP 电话通讯簿同步程序时，通过验证最终用户用户名和密码进行身份验证检查。
- 通过仅允许当前登录到 Cisco IP 电话通讯簿同步程序的用户执行用户授权检查，以执行列示、检索、更新、删除和添加联系人等功能。

Cisco 批量预配置服务

此服务不支持 Cisco Unity Connection。

如果您的配置支持群集（仅限 Unified Communications Manager），则只能在第一台服务器上激活 Cisco 批量预配置服务。 如果使用 Unified Communications Manager 批量管理工具管理电话和用户，则必须激活此服务。

Cisco TAPS 服务

此服务不支持 Cisco Unity Connection 或 IM and Presence Service。

Cisco 自动注册电话支持工具 (TAPS) 服务支持 Cisco Unified Communications Manager 自动注册电话工具，可让用户在响应交互式语音应答 (IVR) 提示后上传自动注册电话上的自定义配置。

如果您的配置支持群集（仅限 Unified Communications Manager），请在第一台服务器上激活此服务。当您要为工具创建虚拟 MAC 地址时，请确保在同一台服务器上激活 Cisco 批量预配置服务。

提示 Cisco Unified Communications Manager 自动注册电话工具依赖 Cisco 客户响应解决方案 (CRS)。 在该工具可按设计工作之前，请确认 CRS 服务器已按 CRS 文档所述进行了配置并正在运行。

平台管理 Web 服务

平台管理 Web 服务是简单对象访问协议 (SOAP) API，可以在 Unified Communications Manager、IM and Presence Service 和 Cisco Unity Connection 系统上激活以允许 PAWS-M 服务器升级系统。

重要事项 不要在 PAWS-M 服务器上激活平台管理 Web 服务。

Performance and monitoring services

Cisco 功能配置报告程序

Cisco 功能配置报告程序服务会生成每日报告。 有关详细信息，请参阅与功能配置报告存档相关的主题。

如果您的配置支持群集（仅限 Unified Communications Manager），则此服务安装在群集中的所有 Unified Communications Manager 服务器上。 报告程序基于记录的信息每天生成一次报告。 您可以从“工具”菜单访问报告程序在 Cisco Unified 功能配置中生成的报告。 每份摘要报告均包含显示该特定报告统计信息的各种图表。 当您激活该服务后，报告生成可能需要长达 24 小时时间。

相关主题

功能配置报告存档，第 269 页

Cisco CallManager SNMP 服务

此服务不支持 IM and Presence Service 和 Cisco Unity Connection。

此服务实施了 CISCO-CCM-MIB，提供适用于 Unified Communications Manager 的预配置和统计信息的 SNMP 访问。

如果您的配置支持群集（仅限 Unified Communications Manager），请在群集中的所有服务器上激活此服务。

CM 服务

本节介绍 CM 服务，不适用于 IM and Presence Service 和 Cisco Unity Connection。

Cisco CallManager

Cisco CallManager 服务提供纯软件呼叫处理以及 Unified Communications Manager 的信令和呼叫控制功能。

提示 仅限 Unified Communications Manager 群集：激活此服务之前，验证 Unified Communications Manager 服务器显示在 Cisco Unified Communications Manager 管理的“查找并列出 Cisco Unified Communications Manager”窗口中。 如果该服务器没有显示，则在激活此服务之前添加 Unified Communications Manager 服务器。 有关如何查找和添加服务器的信息，请参阅《*Cisco Unified Communications Manager* 管理指南》。

仅限 Unified Communications Manager 群集：如果您在服务激活期间停用 Cisco CallManager 或 CTIManager 服务，则您停用该服务的 Unified Communications Manager 服务器将不再存在于数据库中，这意味着您无法在 Cisco Unified Communications Manager 管理中为配置操作选择 Unified Communications Manager 服务器，因为它不会显示在图形用户界面 (GUI) 中。 如果您后来在同一 Unified Communications Manager 服务器上重新激活这些服务，数据库将重新为 Unified Communications Manager 创建一个条目，并添加 “CM_” 前缀到服务器名称或 IP 地址；例如，如果您在 IP 地址为 172.19.140.180 的服务器上重新激活 Cisco CallManager 或 CTIManager 服务，则 CM_ 172.19.140.180 会显示在 Cisco Unified Communications Manager 管理中。 您现在即可在 Cisco Unified Communications Manager 管理中选择服务器，带有新的 “CM_” 前缀。

以下服务依赖于 Cisco CallManager 服务激活：

- CM 服务
- CDR 服务

Cisco TFTP

Cisco 简单文件传输协议 (TFTP) 构建和提供与简单文件传输协议（简化版 FTP）一致的文件。 Cisco TFTP 提供嵌入式组件可执行文件、振铃器文件和设备配置文件。

仅限 Unified Communications Manager：配置文件包含设备（电话和网关）要与之建立连接的 Unified Communications Manager 列表。 设备启动时，组件查询动态主机配置协议 (DHCP) 服务器以获取其网络配置信息。 DHCP 服务器以设备的 IP 地址、子网掩码、默认网关、域名系统 (DNS) 服务器地址以及 TFTP 服务器名称或地址响应。 设备从 TFTP 服务器请求配置文件。 配置文件包含一个列表，列出 Unified Communications Manager 以及设备连接到那些 Unified Communications Manager 要经过的 TCP 端口。 配置文件包含一个列表，列出 Unified Communications Manager 以及设备连接到那些 Unified Communications Manager 要经过的 TCP 端口。

Cisco Unified 移动语音访问服务

Cisco Unified 语音访问服务在 Cisco Unified Mobility 内启动移动语音访问功能；移动语音访问是一个集成语音响应 (IVR) 系统，可让 Cisco Unified Mobility 用户执行以下任务：

- 像从桌面电话发起呼叫一样从蜂窝电话进行呼叫。
- 打开 Cisco Unified Mobility。
- 关闭 Cisco Unified Mobility。

Cisco IP 语音媒体流应用程序

Cisco IP 语音媒体流应用程序服务为 Unified Communications Manager 提供语音媒体流功能，以便与媒体终止点 (MTP)、会议、音乐保持 (MOH) 和报警器一起使用。 Cisco IP 语音媒体流应用程序将消息从 Unified Communications Manager 中继到 IP 语音媒体流驱动程序，后者处理实时协议 (RTP) 流。

Cisco IP 语音媒体流应用程序服务不会为涉及任何 IP 语音媒体流应用程序组件（如会议、MOH、报警器或 MTP）的呼叫分支生成呼叫管理记录 (CMR) 文件。

Cisco CTIManager

Cisco CTI Manager 包含与应用程序交互的 CTI 组件。 此服务允许应用程序监控或控制电话和虚拟设备以执行呼叫控制功能。

仅限 Unified Communications Manager 群集：通过 CTI Manager，应用程序可以访问群集中所有 Unified Communications Manager 的资源和功能，并改进了故障转移功能。 虽然群集中可以有一个或多个 CTI Manager 处于活动状态，但单个服务器上只能存在一个 CTI Manager。 应用程序 (JTAPI/TAPI) 可以同时连接到多个 CTI Manager；但应用程序一次只能让一个连接打开媒体终结设备。

Cisco Extension Mobility

此服务支持 Cisco Extension Mobility 功能，并为其执行登录和自动注销功能。

Cisco 被叫号码分析器

Cisco 被叫号码分析器服务支持 Unified Communications Manager 被叫号码分析器。 激活后，此应用程序会消耗大量资源，因此仅在非高峰时段激活此服务，以尽可能减少呼叫处理中断。

仅限 Unified Communications Manager 群集：Cisco 建议您不要在群集中的所有服务器上激活该服务。Cisco 建议您仅在群集呼叫处理活动最少的一台服务器上激活此服务。

Cisco 被叫号码分析器服务器

Cisco 被叫号码分析器服务器服务以及 Cisco 被叫号码分析器服务支持 Cisco Unified Communications Manager 被叫号码分析器。 此服务只需在专用于 Cisco 被叫号码分析器服务的节点上激活。

仅限 Unified Communications Manager 群集：Cisco 建议您不要在群集中的所有服务器上激活该服务。Cisco 建议您仅在群集呼叫处理活动最少的一台服务器上激活此服务。

Cisco DHCP 监控器服务

Cisco DHCP Monitor 监控服务监控数据库表中 IP 电话的 IP 地址更改。 检测到更改后，它将修改 /etc./dhcpd.conf 文件并重新启动 DHCPD 后台守护程序。

Cisco 群集间查询服务

群集间查询服务 (ILS) 在群集范围内运行。 ILS 可让您创建远程 Unified Communications Manager 群集网络。 ILS 群集发现功能允许 Unified Communications Manager 连接到远程群集，而无需管理员手动配置每个群集之间的连接。 ILS 全局拨号方案复制功能使 ILS 网络中的群集能够与 ILS 网络中的其他群集交换全局拨号方案数据。

可以在 Cisco Unified Communications Manager 管理中选择**高级功能** > **ILS 配置**，从“ILS 配置”窗口激活 ILS。

Cisco UserSync 服务

Cisco UserSync 服务将 Unified Communications Manager 最终用户表中的数据同步到 LDAP 数据库。

Cisco UserLookup Web 服务

Cisco UserLookup Web 服务将商业呼叫（通过外部网关的呼叫）路由到被叫方的备用内线号码，以避免呼叫外线号码的商业成本。

如果 Unified Communications Manager 网络内的主叫方发出外线号码的呼叫，则 Unified Communications Manager 会检查 LDAP 数据库中是否存在被叫方的内线号码。 如果存在内线号码，呼叫将被路由到该内线号码。 如果在 LDAP 数据库中找不到内线号码，则呼叫将路由到原始（外线）号码。

Cisco 头戴式耳机服务

如果您使用兼容的 Cisco IP 电话、Cisco Jabber 或其他 Cisco 设备，Cisco 头戴式耳机服务允许您管理 Cisco 头戴式耳机清单、配置更新和诊断数据。

注释 应在所有已经在运行 Cisco CallManager 服务的 Unified Communications Manager 节点上激活 Cisco 头戴式耳机服务。 确保在您要使用 Cisco Unified CM 管理界面管理头戴式耳机的 Unified Communications Manager 节点上激活 Cisco 头戴式耳机服务。 当您启用 Cisco 头戴式耳机服务时，Cisco CallManager 服务将自动激活。 如果不需要，请取消激活 Cisco CallManager 服务。

IM and Presence Service

IM and Presence 仅适用于 IM and Presence Service。

Cisco SIP Proxy

Cisco SIP Proxy 服务负责提供 SIP 注册器和代理功能。 这包括请求路由、请求者识别和传输互连。

Cisco Presence Engine

Cisco Presence Engine 使用基于这些标准的 SIP 和 SIMPLE 接口收集、汇总并分发用户功能和属性。它会收集有关用户空闲状态和通信功能的信息。

Cisco XCP 文字会议管理器

Cisco XCP 文字会议管理器支持聊天功能。 聊天功能可让用户通过在线聊天室互相沟通。 它通过临时（暂时）和永久聊天室支持聊天功能，这些聊天将保留在 Cisco 支持的外部数据库中，直至其被删除。

Cisco XCP Web 连接管理器

Cisco XCP Web 连接管理器服务可让基于浏览器的客户端连接 IM and Presence Service。

Cisco XCP 连接管理器

Cisco Unified Presence XCP 连接管理器可让 XMPP 客户端连接到 Cisco Unified Presence 服务器。

Cisco XCP SIP 联合连接管理器

Cisco XCP SIP 联合连接管理器支持通过 SIP 协议与 Microsoft OCS 进行域间联合。 当您的部署包含 IM and Presence Service 版本 9.0 群集和 Cisco Unified Presence 版本 8.6 群集之间的群集间连接时，也必须打开此服务。

Cisco XCP XMPP 联合连接管理器

Cisco XCP XMPP 联合连接管理器支持通过 XMPP 协议与 IBM Lotus Sametime、Cisco Webex Meeting Center 和 GoogleTalk 等第三方企业进行域间联合，以及通过 XMPP 协议与其他 IM and Presence Service 企业进行域间联合。

Cisco XCP 消息存档程序

Cisco XCP 消息存档程序服务支持 IM 合规性功能。 IM 合规功能会记录往来于 IM and Presence Service 服务器的所有消息，包括点对点消息以及聊天功能的临时（暂时）和永久聊天室消息。 消息将被记录到 Cisco 支持的外部数据库中。

Cisco XCP 目录服务

Cisco XCP 目录服务支持 XMPP 客户端与 LDAP 目录集成，以允许用户从 LDAP 目录搜索和添加联系人。

Cisco XCP 验证服务

Cisco XCP 验证服务处理连接到 IM and Presence Service 的 XMPP 客户端发起的所有验证请求。

CTI 服务

本节介绍 CTI 服务，不适用于 Cisco Unity Connection 或 IM and Presence Service。

Cisco IP Manager Assistant

此服务支持 Cisco Unified Communications Manager Assistant。 服务激活之后，Cisco Unified Communications Manager Assistant 可让经理及其助理可以更高效地共同工作。 Cisco Unified Communications Manager Assistant 支持两种操作模式：代理线路支持和共享线路支持。

该功能包含呼叫路由服务、经理电话功能增强以及主要供助理使用的桌面界面。

该服务拦截对经理进行的呼叫，然后基于预先配置的呼叫过滤器将这些呼叫路由到选定的助理、经理或其他目标。 经理可以动态更改呼叫路由；例如，通过按电话上的软键，经理可以指示该服务将呼叫路由到助理，并可接收这些呼叫的状态。

Unified Communications Manager用户包括经理和助理。 路由服务拦截经理呼叫并将其相应路由。 助理用户可代表经理处理这些呼叫。

Cisco WebDialer Web 服务

适用于 Cisco Unified Communications Manager 系统的 Cisco WebDialer Web 服务

Cisco Web Dialer 提供单击拨号功能。 它允许 Unified Communications Manager 群集内的用户使用网页或桌面应用程序向群集内部或外部的其他用户发起呼叫。 Cisco Web Dialer提供网页让用户能够在群集内互相呼叫。 Cisco Web Dialer 包含两个组件：WebDialer 小型应用程序和重定向器小型应用程序。

重定向器小型应用程序使第三方应用程序能够使用Cisco Web Dialer。 重定向器小型应用程序为 Cisco Web Dialer 用户找到适当的 Unified Communications Manager 群集，然后将请求重定向到该群集中的 Cisco Web Dialer。 重定向器功能仅适用于基于 HTTP/HTML 的 WebDialer 客户端应用程序，因为它不适用于基于简单对象访问协议 (SOAP) 的 WebDialer 应用程序。

自预配置 IVR

随着自预配置 IVR 服务的引入，可以更便捷地将 Unified Communications Manager 上自动注册的 IP 电话快速分配给用户。 当您从使用 IVR 服务的用户的分机拨打自预配置页面上配置的 CTI RP DN 时，电话连接到“自预配置 IVR”应用程序，并提示您提供自预配置凭证。 根据您提供的自预配置凭证的验证情况，IVR 服务为用户分配自动注册的 IP 电话。

即使该服务被停用，您也可以配置自预配置，但管理员不能使用 IVR 服务为用户分配 IP 电话。 默认情况下，该服务被停用。

要启用自预配置 IVR 服务，必须同时启用 Cisco CTI Manager 服务。

有关如何配置自预配置的详细信息，请参阅《*Cisco Unified Communications Manager* 管理指南》。

CDR 服务

本节介绍 CDR 服务，不适用于 IM and Presence Service 和 Cisco Unity Connection。

CAR Web 服务

Cisco CAR Web 服务加载基于 CAR 用户界面，这是一个使用 CDR 数据生成 CSV 或 PDF 报告的基于 Web 的报告应用程序。

Cisco SOAP - CDRonDemand 服务

Cisco SOAP - CDRonDemand 服务，一项基于 SOAP/HTTPS 的服务，在 CDR 存储库节点上运行。 它根据用户指定的时间间隔（最长 1 小时）接收 CDR 文件名列表的 SOAP 请求，并且返回符合请求

中指定时长的文件名列表。此服务还会通过请求中指定的文件名和传输方法（SFTP/FTP、服务器名称、登录信息和目录）来接收特定 CDR/CMR 文件的传输请求。

如果使用通过 HTTPS/SOAP 接口访问 CDR 数据的第三方计费应用程序，请激活此服务。

对于 Unified Communications Manager 版本 12.x 和更高版本，默认情况下不会启用 CDR onDemand 服务。 如果要启用 CDR onDemand 服务，应手动激活该服务。 在根层级执行以下命令以激活 CDR onDemand 服
务：`/usr/local/cm/bin/soapservicecontrol2.shCDRonDemandServiceCDRonDemanddeploy8443`。

安全服务

本节介绍安全服务，不适用于 IM and Presence Service 和 Cisco Unity Connection。

Cisco CTL 提供程序

仅限 Unified Communications Manager：以本地系统帐户权限运行的Cisco 证书信任列表 (CTL) 提供程序服务配合客户端插件 Cisco CTL 提供程序实用程序使用，可将群集的安全模式从非安全更改为混合模式。 安装插件时，Cisco CTL 提供程序服务会为 CTL 文件检索群集中所有 Unified Communications Manager 和 Cisco TFTP 服务器的列表，其中包含群集中的安全令牌和服务器列表。

您可以安装和配置 Cisco CTL 客户端或 CLI 命令集 **utils ctl**，然后激活此服务，以将群集范围安全模式从非安全更改为安全。

激活服务后，Cisco CTL 提供程序服务将恢复为默认 CTL 端口，即 2444。 如果您想要更改端口，请参阅《*Cisco Unified Communications Manager* 安全指南》了解详细信息。

Cisco 证书颁发机构代理功能 (CAPF)

CAPF 服务与 Cisco 证书颁发机构代理功能 (CAPF) 应用程序配合使用，可执行以下任务，具体取决于您的配置：

- 颁发本地有效证书给受支持的 Cisco Unified IP 电话型号。
- 升级电话上的现有证书。
- 检索电话证书进行故障诊断。
- 删除电话中的本地有效证书。

注释 仅限 Unified Communications Manager：当您在实时监控工具 (RTMT) 中查看实时信息时，CAPF 服务仅为第一台服务器显示。

目录服务

本节介绍目录服务，不适用于 IM and Presence Service 和 Cisco Unity Connection。

Cisco DirSync

Unified Communications Manager：Cisco DirSync 服务确保 Unified Communications Manager 数据库存储所有用户信息。 如果使用集成的公司目录（例如，使用 Unified Communications Manager 的 Microsoft Active Directory 或 Netscape/iPlanet 目录），Cisco DirSync 服务会将用户数据迁移到 Unified Communications Manager 数据库。 Cisco DirSync 服务不会同步公司目录中的密码。

注释 具有重复电子邮件 ID 的用户不会被同步，并且管理员不会收到有关未同步用户列表的通知。 这些 ID 显示在来自 Unified RTMT 的 DirSync 错误日志中。

Cisco Unity Connection：当 Cisco Unity Connection 与 LDAP 目录集成时，Cisco DirSync 服务会将 Cisco Unity Connection 服务器上 Unified Communications Manager 数据库中的一小部分用户数据（名字、姓氏、别名、电话号码等）与 LDAP 目录中的相应数据进行同步。 另一个服务 (CuCmDbEventListener) 会将 Cisco Unity Connection 用户数据库中的数据与 Unified Communications Manager 数据库中的数据进行同步。 配置 Cisco Unity Connection 群集时，Cisco DirSync 服务仅在发布方服务器上运行。

基于位置的跟踪服务

本节介绍基于位置的跟踪服务。

Cisco 无线控制器同步服务

此服务支持位置感知功能，该功能提供网络无线接入点和关联移动设备的状态。

此服务必须运行才能将 Unified Communications Manager 与 Cisco 无线接入点控制器同步。 当服务正在运行并且同步已配置时，Unified Communications Manager 会将其数据库与 Cisco 无线接入点控制器同步，并保存控制器管理的无线接入点的状态信息。 您可以安排同步按定期间隔进行，以便信息保持最新。

注释 在添加新的 Cisco 无线接入点控制器时，请确保此服务正在运行。

语音质量报告程序服务

本节介绍语音质量报告程序服务，不适用于 IM and Presence Service 和 Cisco Unity Connection。

Cisco 扩展功能

Cisco 扩展功能服务支持 Unified Communications Manager 语音质量功能，包括质量报告工具 (QRT)。 有关各个功能的详细信息，请参阅适用于 Cisco Unified Communications Manager 的《*Cisco Unified Communications Manager* 系统配置指南》和《*Cisco Unified IP* 电话管理指南》。

网络服务

自动安装的网络服务包括系统正常工作所需的服务，例如，数据库和平台服务。 由于这些服务是使用基本功能所必需的，因此您无法在“服务激活”窗口中将其激活。 如有必要（例如，出于故障诊断目的），您可能需要在“控制中心 - 网络服务”窗口停止然后启动（或重新启动）网络服务。

安装应用程序后，网络服务会自动启动，如 "控制中心 - 网络服务" 窗口中所述。 功能配置 GUI 将服务归类为逻辑组。

性能和监控服务

Cisco CallManager 功能配置 RTMT

Cisco CallManager 功能配置 RTMT servlet 支持 IM and Presence 实时监控工具 (RTMT)，该功能允许您收集和查看跟踪数据、查看性能监控对象、使用警告以及监控系统性能和性能计数器等等。

Cisco RTMT 报告程序小型应用程序

Cisco RTMT 报告程序小型应用程序可让您发布有关 RTMT 的报告。

Cisco 日志分区监控工具

Cisco 日志分区监控工具服务支持日志分区监控功能，该功能通过使用配置的阈值和轮询间隔监控节点上日志分区的磁盘使用情况。

Cisco Tomcat 统计小型应用程序

Cisco Tomcat 统计小型应用程序可让您使用 RTMT 或 CLI 监控 Tomcat 性能监控计数器。 除非您怀疑此服务使用了过多的资源（例如 CPU 时间），否则不要停止它。

Cisco RIS 数据收集器

实时信息服务器 (RIS) 维护实时信息，例如设备注册状态、性能计数器统计信息、生成的危急警报等等。 Cisco RIS 数据收集器服务为应用程序提供接口（例如 IM and Presence 实时监控工具 (RTMT)、SOAP 应用程序等）以检索存储在群集中所有 RIS 节点中的信息。

Cisco AMC 服务

用于实时监控工具 (RTMT)，此服务、警告管理器和收集器服务允许 RTMT 检索该服务器（或群集中所有服务器）上存在的实时信息。

Cisco Audit Event 服务

Cisco 审核事件服务监控和记录用户或用户操作导致的对 Unified Communications Manager 或 IM and Presence 系统进行的任何管理配置更改。 Cisco 审核服务还会监控和记录最终用户事件，例如登录、注销和 IM 聊天室进入和退出。

备份和恢复服务

Cisco DRF Master

此操作不适用于 IM and Presence Service。

CiscoDRF Master Agent 服务支持 DRF Master Agent，后者与灾难恢复系统 GUI 或 CLI 配合使用以计划备份、执行恢复、查看依赖关系、检查作业状态和取消作业（如有必要）。 Cisco DRF Master Agent 还提供用于备份和恢复过程的存储介质。

Cisco DRF Local

Cisco DRF Local 服务支持 Cisco DRF Local Agent，后者可充当 DRF Master Agent 的主力。 组件可注册 Cisco DRF Local Agent 以使用灾难恢复框架。 Cisco DRF Local Agent 执行从 Cisco DRF Master Agent 接收的命令。 Cisco DRF Local Agent 将状态、日志和命令结果发送到 Cisco DRF Master Agent。

系统服务

Cisco CallManager 功能配置

Cisco CallManager 功能配置服务支持 Cisco Unified 功能配置和 IM and Presence Service 功能配置 GUI，它们是用于故障诊断问题和管理服务的 Web 应用程序/界面。 此服务会自动安装，可让您访问功能配置 GUI。 如果您在服务器上停止此服务，当您浏览到该服务器时，您将无法访问功能配置 GUI。

Cisco CDP

Cisco Discovery Protocol (CDP) 将向其他网络管理应用程序通告语音应用程序，以便网络管理应用程序（例如，SNMP 或 Cisco Unified Operations Manager）能够执行语音应用程序的网络管理任务。

Cisco 跟踪收集 Servlet

Cisco 跟踪收集 Servlet 与 Cisco 跟踪收集服务一起支持跟踪收集，并通过使用 RTMT 允许用户查看跟踪数据。 如果您在服务器上停止此服务，则无法收集或查看该服务器上的跟踪数据。

要使系统日志查看器以及跟踪和日志中心在 RTMT 中正常工作，则 Cisco 跟踪收集 Servlet 和 Cisco 跟踪收集服务必须在该服务器上运行。

Cisco 跟踪收集服务

Cisco 跟踪收集服务与 Cisco 跟踪收集 Servlet 一起支持跟踪收集，并通过使用 RTMT 客户端允许用户查看跟踪数据。 如果您在服务器上停止此服务，则无法收集或查看该服务器上的跟踪数据。

要使系统日志查看器以及跟踪和日志中心在 RTMT 中正常工作，则 Cisco 跟踪收集 Servlet 和 Cisco 跟踪收集服务必须在该服务器上运行。

提示 如有必要，Cisco 建议缩短初始化时间，您可以先重新启动 Cisco 跟踪收集服务，然后再重新启动 Cisco 跟踪收集小型应用程序。

平台服务

Cisco DB

Cisco DB 服务支持 Unified Communications Manager 上的 Progres 数据库引擎。 在 IM and Presence Service 上，Cisco DB 服务支持 IDS 数据库引擎。

Cisco DB 复制器

仅限 Unified Communications Manager 和 IM and Presence：Cisco DB 复制器服务可确保群集中第一个服务器和后续服务器之间的数据库配置和数据同步。

Cisco Tomcat

Cisco Tomcat 服务支持 Web 服务器。

SNMP Master Agent

此服务充当代理协议引擎，提供与 SNMP 请求相关的验证、授权、访问控制和隐私功能。

提示 在功能配置 GUI 中完成 SNMP 配置后，必须在**控制中心—网络功能**窗口中重新启动 SNMP Master Agent 服务。

MIB2 代理

此服务为 RFC 1213 中定义的变量提供读取和写入变量的 SNMP 访问权限；例如，系统、接口和 IP。

主机资源代理

此服务提供主机信息（例如存储资源、进程表、设备信息和已安装软件库）的 SNMP 访问权限。 此服务实现 HOST-RESOURCES-MIB。

本机代理适配器

此服务支持供应商管理信息库 (MIB)，可用于将 SNMP 请求转发到系统上运行的其他 SNMP 代理。

对于 IM and Presence Service 和 Unified Communications Manager，此服务如果安装在虚拟机上，将不会提供。

系统应用程序代理

此服务提供系统上安装和执行的应用程序的 SNMP 访问权限。 此服务实现 SYSAPPL-MIB。

Cisco CDP Agent

此服务使用 Cisco Discovery Protocol 来提供节点上网络连接信息的 SNMP 访问权限。 此服务实现 CISCO-CDP-MIB。

Cisco Syslog 代理

此服务支持收集各种 Unified Communications Manager 组件生成的系统日志消息。 此服务实现 CISCO-SYSLOG-MIB。

注意 停止 SNMP 服务可能会导致数据丢失，因为网络管理系统不再监控网络。 不要停止服务，除非您的技术支持团队告诉您这样做。

Cisco 证书更改通知

此服务可保证 Tomcat、CallManager 和 XMPP 等组件的证书在群集中的所有节点之间自动同步。 此服务停止后，当您重新生成证书时，必须手动将其上传到其他节点上的证书信任。

平台管理 Web 服务

平台管理 Web 服务是简单对象访问协议 (SOAP) API，可以在 Unified Communications Manager、IM and Presence Service 和 Cisco Unity Connection 系统上激活以允许 PAWS-M 服务器升级系统。

重要事项 不要在 PAWS-M 服务器上激活平台管理 Web 服务。

平台通信 Web 服务

平台通信 Web 服务是表现层状态转换协议 (REST) API，可以在 Unified Communications Manager、IM and Presence Service 和 Cisco Unity Connection 系统上运行。

注释 您不能手动启动或停止**平台通信 Web 服务**。

Cisco UDS Tomcat

此服务可避免 UDS 上的资源使用率过高，进而导致其他 Web 应用程序的速度变慢或者 GUI 变慢或无法访问的问题。

Cisco AXL Tomcat

此服务可避免 AXL 上的资源使用率过高，进而导致其他 Web 应用程序的速度变慢或者 GUI 变慢或无法访问的问题。

Cisco SSOSP Tomcat

此服务可避免 SSOSP 上的资源使用率过高，进而导致其他 Web 应用程序的速度变慢或者 GUI 变慢或无法访问的问题。

Cisco 证书到期监控

此服务定期检查系统生成的证书的过期状态，并在证书接近到期日期时发送通知。 对于 Unified Communications Manager，您可以在 Cisco Unified 操作系统管理中管理使用此服务的证书。 对于 IM and Presence Service，您可以在 Cisco Unified IM and Presence 操作系统管理中管理使用此服务的证书。

Cisco 智能许可证管理器

Cisco 智能许可证管理器是仅在发布方上运行的一项网络服务。 它管理 Unified Communications Manager 发布方上的所有 Cisco 智能许可操作。 Cisco 智能许可证管理器服务向 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 报告产品的许可证或权利使用情况，并从 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 获取授权状态。

安全服务

Cisco 认证登记服务

此服务会在在线第三方 CA 和证书颁发机构代理功能之间创建在线连接。 此服务必须激活才能使用具有证书颁发机构代理功能的在线 CA 签署 LSC 证书。

Cisco 信任验证服务

IM and Presence Service 不支持此服务。

Cisco 信任验证服务是在 CallManager 服务器或专用服务器上运行的一项服务，代表电话和其他终端验证证书。 它会将证书所有者的角色列表关联起来。 证书或所有者可以与一个或多个角色关联。

电话与信任验证服务之间的协议允许电话请求验证。 信任验证服务验证证书并返回与之关联的角色列表。 该协议允许信任验证服务验证请求（反之亦然），即电话验证来自信任验证服务的响应。 协议可保护请求和响应的完整性。 请求和响应的机密性不做要求。

Cisco 信任验证服务的多个实例在群集中的不同服务器上运行以提供可扩展性。 这些服务器可以与托管 Cisco Unified CallManager 的服务器相同，也可以不同。 电话将在网络中获取信任验证服务列表，并使用选择算法连接到其中一个服务（例如：轮询）。 如果所联系的信任验证服务没有响应，则电话将切换到列表中的下一个信任验证服务。

数据库服务

Cisco 数据库层监控器

Cisco 数据库层监控器服务监控数据库层的各个方面。 此服务处理更改通知和监控。

注释 Unified Communications Manager 使用自动更新统计信息（即监控数据库表中所做更改的智能统计更新功能），并仅更新需要统计信息更新的表。 此功能节省相当多的带宽，特别是在 Unified Communications Manager 的VMware 部署上。 自动更新统计是默认的索引方法。

SOAP 服务

Cisco SOAP 实时服务 API

仅限 IM and Presence Service：对于在网状态数据，Cisco SOAP 实时服务 API 支持客户端登录和第三方 API。

仅限 Unified Communications Manager 和 Cisco Unity Connection：Cisco SOAP 实时服务 API 可让您收集设备和 CTI 应用程序的实时信息。 此服务还提供用于激活、启动和停止服务的 API。

Cisco SOAP 性能监控 API

Cisco SOAP 性能监控 API 服务可让您通过 SOAP API 对各种应用程序使用性能监控计数器；例如，您可以监控每个服务的内存信息、CPU 使用情况和性能监控计数器。

Cisco SOAP 日志收集 API

Cisco SOAP 日志收集 API 服务可让您收集日志文件，并计划远程 SFTP 服务器上的日志文件收集。例如，您可以收集系统日志、核心转储文件和 Cisco 应用程序跟踪文件等日志文件。

SOAP-Diagnostic Portal 数据库服务

Cisco Unified 实时监控工具 (RTMT) 使用 SOAP-Diagnostic Portal 数据库服务访问 RTMT Analysis Manager 托管数据库。 RTMT 根据操作员定义的过滤器选择来收集呼叫记录。 如果此服务停止，RTMT 将无法从数据库收集呼叫记录。

CM 服务

本节介绍 Unified Communications Manager CM 服务，但不适用于 IM and Presence Service 和 Cisco Unity Connection。

Cisco Extension Mobility 应用程序

Cisco Extension Mobility 应用程序服务允许您定义登录设置，例如针对 Cisco Extension Mobility 功能的电话配置的持续时间限制。

仅限 Unified Communications Manager：Cisco Extension Mobility 功能允许 Unified Communications Manager 群集中的用户通过登录到其他电话临时将群集中的另一部电话配置为自己的电话。 用户登录后，电话将采用个人电话号码、快速拨号、服务链路和其他用户特定属性。 注销后，电话将采用原始用户配置文件。

Cisco 用户数据服务

Cisco 用户数据服务为 Cisco Unified IP 电话提供从 Cisco Unified Communications Manager 数据库访问用户数据的能力。 Cisco 用户数据服务提供对 Cisco 个人目录的支持。

Cisco 推送通知服务

Cisco 推送通知服务提供从 Cisco Unified Communications Manager 发送来电推送通知到的 Apple iOS 设备的功能。 此服务将推送通知消息从 Cisco CallManager 服务中继到 Cisco Collaboration Cloud。 此服务还管理用于发送推送通知的访问令牌。

Cisco 头戴式耳机服务

如果您使用兼容的 Cisco IP 电话、Cisco Jabber 或其他 Cisco 设备，Cisco 头戴式耳机服务允许您管理 Cisco 头戴式耳机清单、配置更新和诊断数据。

注释 应在所有已经在运行 Cisco CallManager 服务的 Unified Communications Manager 节点上激活 Cisco 头戴式耳机服务。 确保在您要使用 Cisco Unified CM 管理界面管理头戴式耳机的 Unified Communications Manager 节点上激活 Cisco 头戴式耳机服务。 当您启用 Cisco 头戴式耳机服务时，Cisco CallManager 服务将自动激活。 如果不需要，请取消激活 Cisco CallManager 服务。

IM and Presence Service 服务

IM and Presence Service 服务仅适用于 IM and Presence Service。

Cisco 登录数据存储器

Cisco 登录数据存储库是将客户端会话存储到 Cisco 客户端配置文件代理的实时数据库。

Cisco 路由数据存储器

Cisco 路由数据存储库是一个实时数据库，用于存储 Cisco SIP Proxy 和Cisco 客户端配置文件代理的路由信息和已分配用户的缓存。

Cisco 配置代理

Cisco 配置代理是一项变更通知服务，用于将 IM and Presence Service IDS 数据库中的配置变更通知 Cisco SIP Proxy。

Cisco 同步代理

Cisco 同步代理会确保 IM and Presence 数据与 Unified Communications Manager 数据同步。 它将 SOAP 请求发送到 Unified Communications Manager，以获取 IM and Presence 感兴趣的数据，订用来自 Unified Communications Manager 的变更通知以及更新 IM and Presence IDS 数据库。

Cisco OAM 代理

Cisco OAM&P 代理服务可监控 IM and Presence Service IDS 数据库中 Presence Engine 感兴趣的配置参数。 在数据库中进行更改后，OAM&P 代理会写入一个配置文件，并将 RPC 通知发送到 Presence Engine。

Cisco 客户端配置文件代理

Cisco 客户端配置文件代理服务使用 HTTPS 提供与外部客户端之间的安全 SOAP 接口。

Cisco 群集间同步代理

Cisco 群集间同步代理服务提供以下功能：DND 传播到 Unified Communications Manager，并在 IM and Presence Service 群集之间同步最终用户信息以进行群集间 SIP 路由。

Cisco XCP 路由器

XCP 路由器是 IM and Presence Service 服务器上的核心通信功能。 它在 IM and Presence Service 上提供基于 XMPP 的路由功能；它将 XMPP 数据路由到 IM and Presence Service 上的其他活动 XCP 服务，并访问 SDNS 以允许系统将 XMPP 数据路由到 IM and Presence Service 用户。 XCP 路由器为用户管理 XMPP 会话，并在这些会话之间路由 XMPP 消息。

IM and Presence Service 安装后，系统会默认打开 Cisco XCP 路由器。

注释 如果重新启动 Cisco XCP 路由器，IM and Presence Service 会自动重新启动所有活动的 XCP 服务。请注意，必须选择“重新启动”选项重新启动 Cisco XCP 路由器；这不同于关闭然后打开 Cisco XCP 路由器。 如果关闭 Cisco XCP 路由器，而不是重新启动此服务，IM and Presence Service 会停止所有其他 XCP 服务。 随后打开 XCP 路由器时，IM and Presence Service 不会自动打开其他 XCP 服务；您需要手动打开其他 XCP 服务。

Cisco XCP 配置管理器

Cisco XCP 配置管理器服务会监控通过管理 GUI 进行的影响其他 XCP 组件（例如路由器和消息存档程序）的配置和系统拓扑更改（以及从对等成员同步的拓扑更改），并根据需要更新这些组件。 Cisco XCP 配置管理器服务为管理员创建通知，指示 XCP 组件何时（因这些更改）需要重新启动，并在重新启动完成后自动清除通知。

Cisco 服务器恢复管理器

Cisco Server Recovery Manager (SRM) 服务管理 Presence 冗余组中节点之间的故障转移。 SRM 管理节点中的所有状态更改；状态更改是自动的或由管理员（手动）启动。 在 Presence 冗余组中启用高可用性后，各节点上的 SRM 会建立与对等节点的信号连接，并开始监控重要流程。

Cisco IM and Presence 数据监控器

Cisco IM and Presence 数据监控器监控 IM and Presence Service 上的 IDS 复制状态。 其他 IM and Presence Service 与 Cisco IM and Presence 数据监控器相关。 这些相关服务使用 Cisco 服务将启动延迟到 IDS 复制处于稳定状态为止。

Cisco IM and Presence 数据监控器还会从 Unified Communications Manager 检查 Cisco 同步代理同步的状态。 仅当 IDS 复制已设置并且 IM and Presence 数据库发布方节点上的同步代理已从 Unified Communications Manager 完成同步后，相关服务才可启动。 达到超时后，即使 IDS 复制和同步代理尚未完成，发布方节点上的 Cisco IM and Presence 数据监控器也允许相关服务启动。

在订阅方节点上，Cisco IM and Presence 数据监控器会将功能服务的启动延迟到 IDS 复制成功建立为止。 Cisco IM and Presence 数据监控器只会延迟群集中问题订阅方节点上功能服务的启动，而不会因一个问题节点而延迟所有订阅方节点上功能服务的启动。 例如，如果 IDS 复制已在节点 1 和节点 2 上成功建立，但未在节点 3 上成功建立，则 Cisco IM and Presence 数据监控器允许功能服务在节点 1 和节点 2 上启动，但会延迟节点 3 上的功能服务启动。

Cisco Presence 数据存储器

Cisco Presence 数据存储库是用于存储瞬时在网状态数据和订用的实时数据库。

Cisco SIP 注册数据存储器

Cisco Presence SIP 注册数据存储库是用于存储 SIP 注册数据的实时数据库。

CDR 服务

本节介绍 CDR 服务，不适用于 IM and Presence Service 和 Cisco Unity Connection。

Cisco CDR 存放库管理器

此服务维护并移动从 Cisco CDR 代理服务获取的已生成呼叫详细信息记录 (CDR)。 在支持群集的系统中（仅限 Unified Communications Manager），该服务位于第一台服务器上。

Cisco CDR 代理

注释 Unified Communications Manager 支持 Cisco Unified Communications Manager 系统中的 Cisco CDR 代理。

此服务不支持 IM and Presence Service 和 Cisco Unity Connection。

Cisco CDR 代理服务将 Unified Communications Manager 从本地主机生成的 CDR 和 CMR 文件转移到通过 SFTP 连接运行 CDR 存储库服务的 CDR 存储库服务器上。

此服务将从本地主机生成的 CDR 和 CMR 文件转移到群集中的 CDR 存储库服务器。 CDR 存储库节点独立服务器中的 CDR 代理将独立服务器生成的文件转移到通过 SFTP 连接的 Cisco CDR 存储库管理器。 CDR 代理维护并移动这些文件。

要使此服务工作，请激活服务器上的 Cisco CallManager 服务并确保其正在运行。 如果您的配置支持群集（仅限 Unified Communications Manager），请在第一台服务器上激活 Cisco CallManager 服务。

Cisco CAR 调度程序

此 Cisco CDR 分析和报告 (CAR) 计划程序服务不支持 IM and Presence Service 和 Cisco Unity Connection。

Cisco CAR 计划程序服务允许您安排 CAR 相关的任务；例如，您可以安排报告生成或 CDR 文件加载到 CAR 数据库中。

Cisco SOAP-CallRecord 服务

默认情况下，Cisco SOAP-CallRecord 服务作为 SOAP 服务器在发布方上运行，以便客户端可以通过 SOAP API 连接到 CAR 数据库。 此连接通过使用 CAR 连接器（使用单独的 CAR ID 实例）进行。

Cisco CAR 数据库

Cisco CAR 数据库管理 CAR 数据库的 Informix 实例，以便服务管理器能够启动或停止此服务，以及分别打开或关闭 CAR ID 实例。 这与用于维护 CCM ID 实例的 Unified Communications Manager 数据库类似。

默认情况下，Cisco CAR 数据库服务在发布方上激活。 CAR 数据库实例在发布方上安装并主动运行，以维护 CAR 数据库。 此网络服务仅在发布方上使用，而不适用于订阅方。

管理服务

本节介绍管理服务，不适用于 Cisco Unity Connection。

Cisco CallManager 管理

IM and Presence Service 和 Cisco Unity Connection 不支持 Cisco CallManager 管理服务。

Cisco CallManager 管理服务支持 Cisco Unified Communications Manager 管理，即用于配置 Unified Communications Manager 设置的 Web 应用程序/界面。 在 Unified Communications Manager 安装之后，此服务就会自动启动，并允许您访问图形用户界面 (GUI)。 如果停止此服务，当您浏览到该服务器时，将无法访问 Cisco Unified Communications Manager 管理图形用户界面。

Cisco IM and Presence 管理员

Unified Communications Manager 和 Cisco Unity Connection 不支持 Cisco IM and Presence 管理服务。

Cisco IM and Presence 管理服务支持 Cisco Unified Communications Manager IM and Presence 管理，即您用于配置 IM and Presence Service 设置的 Web 应用程序/界面。 在安装 IM and Presence Service 之后，此服务会自动启动并让您访问 GUI。 如果您停止此服务，当您浏览到该服务器时，将无法访问 Cisco Unified Communications Manager IM and Presence 管理 GUI。

Services setup

控制中心

从功能配置 GUI 的“控制中心”，您可以同时查看状态和启停一项服务。 要启动、停止和重新启动网络服务，请访问“控制中心”—“网络服务”窗口。 要启动、停止和重新启动功能服务，请访问“控制中心”—“功能服务”窗口。

提示 使用“相关链接”下拉列表框和“前往”按钮导航到“控制中心”和“服务激活”窗口。

仅 Unified Communications Manager 和 IM and Presence：在群集配置中，您可以同时查看群集中一台服务器的状态以及启动和停止服务。

仅 Unified Communications Manager：启动和停止功能服务会导致当前注册到该服务的所有 Cisco Unified IP 电话和网关故障转移到其辅助服务。 设备和电话只有在无法向其辅助服务注册时才需要重新启动。 启动和停止服务可能会导致托管到该 Unified Communications Manager 的其他已安装应用程序（例如会议桥或 Cisco Messaging Interface）也会启动和停止。

注意 仅 Unified Communications Manager：停止服务还将停止该服务控制的所有设备的呼叫处理。 服务停止后，从一部 IP 电话到另一部 IP 电话的呼叫保持连接；从一部 IP 电话到媒体网关控制协议 (MGCP) 网关的进行中呼叫也将保持连接，但其他类型的呼叫将被丢弃。

设置服务

使用服务时，您可以执行以下任务：

过程

步骤 1 激活要运行的功能服务。

步骤 2 配置适当的服务参数。

步骤 3 如有必要，使用功能配置 GUI 跟踪工具诊断问题。

服务激活

注释 您可以激活或停用多项功能服务，或者从功能配置 GUI 中的“服务激活”窗口选择要激活的默认服务。 您可以从 IM and Presence 节点查看、启动和停止 Unified Communications Manager 服务，反之亦然。 您可能会遇到以下错误：“无法建立到服务器的连接（无法访问远程节点）”。 如果出现此错误消息，请参阅《*Cisco Unified Communications Manager* 管理指南》。

注释 从 Unified Communications Manager 版本 6.1.1 开始，最终用户无法再访问 Cisco Unified 功能配置以启动和停止服务。

功能服务在自动模式下激活，功能配置 GUI 基于单节点配置检查服务依赖关系。 当您选择激活功能服务时，系统会提示您选择所有其他依赖该服务运行的服务（如果有）。 单击**设置默认值**时，功能配置 GUI 将选择在服务器上运行所需的服务。

仅 Unified Communications Manager 和 IM and Presence Service：即使在支持群集的配置中，此过程也基于单服务器配置。

激活服务会自动启动该服务。 您可以从控制中心启动和停止服务。

Cisco Unified Communications Manager 的群集服务激活建议

在激活群集中的服务之前，请查看下表，其中提供了对多服务器 Unified Communications Manager 配置的服务建议。

表 *35: Cisco Unified Communications Manager* 服务激活建议

服务/小型应用程序	激活建议
CM 服务	
Cisco CallManager	此服务支持 Unified Communications Manager。 在控制中心 - 网络服务中，确保 Cisco RIS 数据收集器服务和数据库层监控器服务上运行。 **提示** 激活此服务之前，验证 Unified Communications Manager 服务器显示在 Unified Communications Manager 管理的 Unified Communications Mana 找/列出窗口中。 如果该服务器没有显示，则在激活此服务之前添加 U Communications Manager 服务器。 有关如何添加服务器的信息，请参阅《*Cisco Unified Communications M* 系统配置指南》。
Cisco Messaging 接口	仅在使用 SMDI 集成到采用服务器连接的 USB 到串行适配器的第三方语音邮件系活。
Cisco Unified 移动语音访问服务	要使移动语音访问正常工作，您必须在将 H.323 网关配置为指向第一个 VXML 页群集中的第一个节点上激活此服务。 此外，请确保 Cisco CallManager 和 Cisco TI务在群集中的一台服务器上运行，但不一定是运行 Cisco Unified 移动语音访问服台服务器。
Cisco IP 语音媒体流应用程序	如果群集中有多个节点，则每个群集激活一台或两台服务器。 您可以在专用于音的节点上激活。 此服务要求您在群集中的一个节点上激活 Cisco TFTP。 请勿在第点或运行 Cisco CallManager 服务的任何节点上激活此服务。
Cisco CTIManager	在 JTAPI/TAPI 应用程序将要连接的每个节点上激活。 CTIManager 激活要求在节时激活 Cisco CallManager 服务。 有关 CTIManager 和 Cisco CallManager 服务交互信息，请参阅与 CM 服务相关的主题。
Cisco Extension Mobility	在群集中的所有节点上激活。
Cisco 扩展功能	在运行 Cisco RIS 数据收集器的一个或多个服务器上激活这项支持 Quality Report (QRT) 的服务。 确保在群集中的节点上激活 Cisco CTIManager 服务。

服务/小型应用程序	激活建议
Cisco DHCP 监控器服务	当 DHCP 监控器服务启用后，它将检测数据库中影响 IP 电话的 IP 地址的更改，修改/etc/dhcpd.conf 文件，然后使用更新的配置文件停止并重新启动 DHCPD 后台守护程序在启用了 DHCP 的节点上激活此服务。
Cisco 位置带宽管理器	如果您计划使用 Cisco 位置通话准入控制功能来管理音频和视频呼叫的带宽分配，则须激活此服务。 此服务与 Cisco CallManager 服务配合使用。 建议在运行 Cisco CallMan服务的同一台服务器上运行Cisco 位置带宽管理器。 如果位置带宽管理器运行所在的务器不同于 CallManager 服务所在的服务器，请确保正确配置位置带宽管理器组。
Cisco 群集间查询服务	如果计划在多个 Unified Communications Manager 群集之间传播 URI 和数字路由信息，必须在参与此交换的群集发布方上激活此服务。
Cisco 被叫号码分析器服务器	如果群集中有多个节点，请在专用于 Cisco 被叫号码分析器服务的一个节点上激活此务。
Cisco 被叫号码分析器	如果您计划使用 Unified Communications Manager 被叫号码分析器，请激活此服务。服务可能会消耗大量资源，因此仅在呼叫处理活动最少的节点上或在非高峰时段激活服务。
Cisco TFTP	如果群集中有多个节点，请在专用于 Cisco TFTP 服务的一个节点上激活此服务。 如果群集中的多个节点上激活此服务，则配置选项 150。
Cisco 头戴式耳机服务	如果计划从 Unified Communications Manager 管理您的 Cisco 头戴式耳机，请激活此服务。 **注释** 应在所有已经在运行 Cisco CallManager 服务的 Unified Communications Mana节点上激活 Cisco 头戴式耳机服务。 确保在您要使用 Cisco Unified CM 管界面管理头戴式耳机的 Unified Communications Manager 节点上激活 Cisco戴式耳机服务。 当您启用 Cisco 头戴式耳机服务时，Cisco CallManager 服将自动激活。 如果不需要，请取消激活 Cisco CallManager 服务。
CTI 服务	
Cisco IP Manager Assistant	如果您计划使用 Cisco Unified Communications Manager Assistant，请在群集中的任意两服务器（主服务器和备份服务器）上激活此服务。 确保在群集中激活 Cisco CTI Man服务。 有关 Cisco IP Manager Assistant 的详细信息，请参阅《*Cisco Unified Communications Manager* 功能配置指南》。
Cisco WebDialer Web 服务	激活每个群集上的一个节点。
自预配置 IVR	要启用自预配置 IVR 服务，必须同时启用 Cisco CTI Manager 服务。 即使该服务被停用，您也可以配置自预配置，但管理员不能使用 IVR 服务为用户分配电话。 默认情况下，该服务被停用。
CDR 服务	

服务/小型应用程序	激活建议
Cisco SOAP-CDROnDemand 服务	您仅可在第一台服务器上激活 Cisco SOAP-CDROnDemand 服务，并且要求 Cisco 储库管理器和 Cisco CDR 代理服务在同一台服务器上运行。 对于 Unified Communications Manager 版本 12.x 和更高版本，默认情况下不会启用 onDemand 服务。 如果要启用 CDR onDemand 服务，应手动激活该服务。 在根层 以下命令以激活 CDR onDemand 服务：/usr/local/cm/bin/soapservicecontrol2.shCDRonDemandServiceCDRonDemanddeplo
Cisco CAR Web 服务	您只能在第一台服务器上激活 Cisco CAR Web 服务，它要求在 CDR 存储库管理器 运行所在的同一台服务器上激活 Cisco CAR 计划程序并运行。
数据库和管理服务	
Cisco AXL Web 服务	安装之后，Cisco AXL Web 服务默认为在所有群集节点上启用。 Cisco 建议您始终 布方节点上保持激活该服务。 这可确保您能够配置依赖于 AXL 的产品，例如 Un Provisioning Manager。 根据您的需要，您可以在“功能服务”的 Cisco Unified 功能配置下激活或禁用特 方节点上的服务。
Cisco 批量预配置服务	您仅可在第一个节点上激活 Cisco 批量预配置服务。 如果使用批量管理工具 (BA 电话和用户，您必须激活此服务。
Cisco UXL Web 服务	此服务执行身份验证和用户授权检查。 Cisco IP 电话通讯簿同步程序中的 TabSyn 端使用 Cisco UXL Web 服务查询 Cisco Unified Communications Manager 数据库。 如果您计划使用 Cisco IP 电话通讯簿同步程序，则必须在一个节点上激活此服务 是发布方节点。 如果您没有使用 Cisco IP 电话通讯簿同步程序，Cisco 建议您禁用 务。 默认情况下，该服务被停用。
Cisco 平台管理 Web 服务	如果您计划使用 Cisco Prime Collaboration 部署 (PCD) 服务器管理升级、交换机版 新启动或重新寻址操作，则必须激活此服务。 平台管理 Web 服务 (PAWS) 允许 C Manager 与 Prime Collaboration 部署 (PCD) 之间的 SOAP 通信。 如果群集中有多个 则必须在群集中的每台服务器上激活此服务。
Cisco TAPS 服务	在您可以使用 Cisco Unified Communications Manager 自动注册电话工具之前，您 第一个节点上激活此服务。 当您为 Cisco Unified Communications Manager 自动注 工具创建虚拟 MAC 地址时，请确保在同一节点上激活 Cisco 批量预配置服务。
性能和监控服务	
Cisco 功能配置报告程序	仅在第一个节点上激活。 **注释** 即使您在其他节点上激活该服务，它也仅在第一个节点上生成报告。
Cisco CallManager SNMP 服务	如果您使用 SNMP，请在群集中的所有服务器上激活此服务。

服务/小型应用程序	激活建议
安全服务	
Cisco CTL 提供程序	在群集中的所有服务器上激活。
Cisco 证书颁发机构代理功能 (CAPF)	仅在第一个节点上激活。
目录服务	
Cisco DirSync	仅在第一个节点上激活。

IM and Presence Service 的群集服务激活建议

注意 在为某个功能开启任何服务之前，必须在 IM and Presence 上完成该功能的所有必要配置。 请参阅每个 IM and Presence 功能的相关文档。

在群集中打开服务之前，请查看下表，其中提供了多节点 IM and Presence 配置的服务建议。

表 *36: IM and Presence Service* 激活建议

服务/小型应用程序	建议
数据库和管理服务	
Cisco AXL Web 服务	安装之后，Cisco AXL Web 服务默认为在所有群集节点上启用。 Cisco 建议您始终在 IM and Presence Service 数据库发布方节点上激活此服务。 这可确保您能够配置依赖于 AXL 的产品。 如果配置了群集间通信，则必须在子群集的两个节点上启用此服务，以便将远程对等成员配置为从该子群集同步。 如果两个节点上均未启用此服务，则在故障转移方案中，Presence 和 IM 功能都将丢失。 根据您的需要，您可以在“功能服务”的 Cisco Unified 功能配置下激活或禁用特定 IM and Presence 订阅方节点上的服务。
Cisco 批量预配置服务	• 您仅可在第一个节点上打开 Cisco 批量预配置服务。 • 如果使用批量管理工具 (BAT) 管理用户，则必须打开此服务。
性能和监控服务	

服务/小型应用程序	建议
Cisco 功能配置报告程序	只在发布方节点上打开此服务。 **注释** 即使您在其他节点上打开此服务，它也只会在发布方节点上生成报告。
IM and Presence Service	
Cisco SIP Proxy	在群集中的所有节点上打开此服务。
Cisco Presence Engine	在群集中的所有节点上打开此服务。
Cisco 同步代理	在群集中的所有节点上打开此服务。
Cisco XCP 文字会议管理器	• 如果您在 IM and Presence 中部署聊天功能，请打开此服务。 • 在运行聊天功能的每个节点上打开此服务。 **注释** 永久聊天功能需要外部数据库。 如果启用了永久聊天功能，还必须在启动文字会议管理器服务之前配置外部数据库。 如果启用了永久聊天功能但未配置外部数据库，则文字会议管理器服务不会启动。 请参阅 *Unified Communications Manager* 上 IM and Presence 的数据库设置指南。
Cisco XCP Web 连接管理器	• 如果您将 Web 客户端与 IM and Presence 集成，请打开此服务。 • 在群集中的所有节点上打开此服务。
Cisco XCP 连接管理器	• 如果您将 XMPP 客户端与 IM and Presence 集成，请打开此服务。 • 在群集中的所有节点上打开此服务。
Cisco XCP SIP 联合连接管理器	如果您部署以下任何配置，请打开此服务： • 在 IM and Presence 上通过 SIP 协议进行域间联合。 在运行 SIP 联合的每个节点上打开此服务。 • IM and Presence 9.x 版群集与 Cisco Unified Presence 8.6(x) 版群集之间的群集间部署。 在 9.x 版群集中的所有节点上打开此服务。

服务/小型应用程序	建议
Cisco XCP XMPP 联合连接管理器	• 仅当您在 IM and Presence 上通过 XMPP 协议部署域间联合时，才打开此服务。 • 在运行 XMPP 联合的每个节点上打开此服务。 **注释** 在节点上打开 XMPP 联合连接管理器服务之前，必须在该节点上的 Cisco Unified Communications Manager IM and Presence 管理中打开 XMPP 联合。 请参阅 *Unified Communications Manager* 上 IM and Presence 的域间联合。
Cisco XCP 消息存档程序	• 如果您在 IM and Presence 中部署合规性功能，请打开此服务。 • 在运行 IM 合规性功能的所有节点上打开此服务。 **注释** 如果在配置外部数据库之前打开消息存档程序，服务将不会启动。此外，如果无法访问外部数据库，服务也不会启动。 请参阅 *Unified Communications Manager* 上 IM and Presence 的数据库设置指南。
Cisco XCP 目录服务	• 如果将 IM and Presence 上的 XMPP 客户端与 LDAP 目录集成，请打开此服务。 • 在群集中的所有节点上打开此服务。 **注释** 如果在配置第三方 XMPP 客户端的 LDAP 联系人搜索设置之前打开目录服务，服务将启动，然后再次停止。请参阅《*Unified Communications Manager* 上 *IM and Presence Service* 的配置和管理》。
Cisco XCP 验证服务	• 如果您将 XMPP 客户端与 IM and Presence 集成，请打开此服务。 • 在群集中的所有节点上打开此服务。

激活功能服务

您可以在功能配置GUI的**服务激活**窗口中激活和取消激活功能服务。 在您激活之前，**服务激活**窗口中的服务不会启动。

您只能激活和禁用功能服务（无法激活和禁用网络服务）。 您可以同时激活或停用所需数量的服务。 某些功能服务依赖于其他服务，并且相关服务会在功能服务激活之前激活。

提示 仅 Unified Communications Manager 和 IM and Presence Service：在“服务激活”窗口中激活服务之前，请查看与群集服务激活建议相关的主题。

过程

步骤 1 选择**工具** > **服务启动**。

此时将显示**服务启动**窗口。

步骤 2 从**服务器**下拉列表中，选择服务器（节点）并单击**前往**。

您可以从 IM and Presence Service 节点访问 Unified Communications Manager 服务，反之亦然。 尝试访问远程节点时，您可能会遇到以下错误：“无法建立到服务器的连接（无法连接到远程节点）”。 如果出现此错误消息，请参阅《*Cisco Unified Communications Manager* 管理指南》。

步骤 3 要打开或关闭服务，请执行以下操作之一：

a) 要打开在单个服务器上运行所需的默认服务，选择**设置为默认值**。

注释 此选项会根据单个服务器的配置选择默认服务，并检查服务依赖关系。

b) 要打开所有服务，勾选**选中所有服务**。

c) 要打开特定的服务，选中要打开服务旁边的复选框。

d) 要关闭服务，取消选中要关闭服务的复选框。

步骤 4 仅 Unified Communications Manager 和 IM and Presence Service：对于群集配置，请查看群集服务的激活建议，然后选中要激活的服务旁边的复选框。

步骤 5 选中要激活的服务的复选框后，单击**保存**。

提示 要禁用已激活的服务，取消选中要禁用服务旁边的复选框。然后单击**保存**。

提示 要获取服务的最新状态，单击**刷新**按钮。

相关主题

Cisco Unified Communications Manager 的群集服务激活建议，第 207 页
IM and Presence Service 的群集服务激活建议，第 210 页

启动、停止和重新启动控制中心或 CLI 中的服务

为执行这些任务，功能配置GUI提供两个控制中心窗口。 要启动、停止和重新启动网络服务，请访问**控制中心—网络服务**窗口。 要启动、停止和重新启动功能服务，请访问**控制中心—功能服务**窗口。

提示 使用**相关链接**列表框和**转至**按钮导航到控制中心和服务激活窗口。

启动、停止和重新启动控制中心内的服务

控制中心内的功能配置 GUI 可让您：

- 查看状态
- 刷新状态
- 启动、停止和重新启动特定服务器上或用于群集配置中群集服务器的网络服务

当服务正在停止时，您无法启动该服务，直到该服务已停止。

注意 仅 Unified Communications Manager：停止服务还将停止该服务控制的所有设备的呼叫处理。 服务停止后，从一部IP电话到另一部IP电话的呼叫保持连接；从一部IP电话到媒体网关控制协议 (MGCP) 网关的进行中呼叫也将保持连接，但其他类型的呼叫将被丢弃。

过程

步骤 1 根据您要启动/停止/重新启动/刷新的服务类型，执行以下任务之一：

- 选择**工具** > **控制中心 - 功能服务**。

  提示 在启动、停止或重新启动功能服务之前，必须能够激活该服务。

- 选择**工具** > **控制中心 - 网络服务**。

步骤 2 从“服务器”下拉列表中选择服务器，然后单击**执行**。

窗口将显示以下项目：

- 您所选服务器的服务名称。
- 服务组。
- 服务状态，例如“已启动”、“正在运行”、“未运行”等 （“状态”列）。
- 该服务开始运行的确切时间 （“开始时间”列）。
- 服务已运行的时间量 （“运行时间”列）。

步骤 3 请执行以下任务之一：

- 单击要启动的服务旁边的单选按钮，然后单击**启动**。“状态”将更改以体现更新的状态。
- 单击要停止的服务旁边的单选按钮，然后单击**停止**。“状态”将更改以体现更新的状态。
- 单击要重新启动的服务旁边的单选按钮，然后单击**重新启动**。将显示一条消息，表明重新启动可能需要一些时间。单击**确定**。
- 单击**刷新**获取服务的最新状态。
- 要转至**服务激活**窗口或其他控制中心窗口，请从“相关链接”下拉列表中选择一个选项，然后单击**转至**。

使用命令行界面启动、停止和重新启动服务

您可以通过 CLI 启动和停止某些服务。有关您可以通过 CLI 启动和停止的服务的列表以及如何执行这些任务的信息，请参阅《*Cisco Unified Solutions* 命令行界面参考指南》。

提示 您必须从功能配置 GUI 的控制中心启动和停止大多数服务。

第 17 章

跟踪

跟踪

Cisco Unified 功能配置提供跟踪工具，可帮助您诊断语音应用程序的问题。 Cisco Unified 功能配置支持 SDI（系统诊断接口）跟踪、SDL（信令分布层）跟踪（针对 Cisco CallManager 和 Cisco CTIManager 服务，仅适用于 Unified Communications Manager）和 Log4J 跟踪（针对 Java 应用程序）。

您可使用“跟踪配置”窗口指定要跟踪的信息级别以及要包含在每个跟踪文件中的信息类型。

仅 Unified Communications Manager：如果服务是呼叫处理应用程序（例如 Cisco CallManager 或 Cisco CTIManager），则可以在电话和网关等设备上配置跟踪。

仅 Unified Communications Manager：在“警报配置”窗口中，您可以将警报定向到不同的位置，包括 SDL 跟踪日志文件。 如果要执行此操作，可以在 Cisco Unified 实时监控工具 (Unified RTMT) 中配置警告跟踪。

配置要包含在各项服务的跟踪文件中的信息后，可以使用实时监控工具中的“跟踪和日志中心”选项收集及查看跟踪文件。

Cisco Unified IM and Presence 功能配置提供跟踪工具，可帮助您排查即时消息和在网状态应用程序的问题。 Cisco Unified IM and Presence 功能配置支持：

- SDI 跟踪
- Log4J 跟踪（针对 Java 应用程序）

您可以配置要跟踪的信息级别（调试级别）、要跟踪哪些信息（跟踪字段）以及关于跟踪文件的信息（例如每项服务的文件数、文件大小和数据在跟踪文件中存储的时间）。 您可以为单一服务配置跟踪，或者将该服务的跟踪设置应用到群集中的所有服务。

在**警报配置**窗口中，您可以将警报定向到各个位置。 如果要执行此操作，可以在 IM and Presence Unified RTMT 中配置警告跟踪。

配置要包含在各项服务的跟踪文件中的信息后，可以使用Unified RTMT中的“跟踪和日志中心”选项收集及查看跟踪文件。 您可以为群集中任何 IM and Presence 节点上的任何可用功能或网络服务配置跟踪参数。 使用“跟踪配置”窗口指定要跟踪的参数，以便对问题进行故障诊断。 如果想要使用预先确定的故障诊断跟踪设置而不是选择自己的跟踪字段，可以使用**故障诊断跟踪设置**窗口。

注释 启用跟踪会降低系统性能；因此，仅出于故障诊断目的启用跟踪。 有关使用跟踪的帮助，请联系 Cisco 技术支持中心 (TAC)。

跟踪配置

您可以为功能配置界面中的任何功能或网络服务配置跟踪参数。 如有群集，可以为群集中任意服务器上的任何可用功能或网络服务配置跟踪参数。 使用“跟踪配置”窗口指定要跟踪的参数，以便对问题进行故障诊断。

您可以配置要跟踪的信息级别（调试级别）、要跟踪哪些信息（跟踪字段）以及关于跟踪文件的信息（例如每项服务的文件数、文件大小和数据在跟踪文件中存储的时间）。 如有群集，可以为单一服务配置跟踪，或者将该服务的跟踪设置应用到群集中的所有服务。

如果想要使用预先确定的故障诊断跟踪设置而不是选择自己的跟踪字段，可以使用“故障诊断跟踪”窗口。 有关对跟踪进行故障诊断的详细信息，请参阅跟踪设置。

配置要包含在各项服务的跟踪文件中的信息后，可以使用Unified RTMT中的“跟踪和日志中心”选项收集跟踪文件。 有关跟踪收集的详细信息，请参阅跟踪收集。

跟踪设置

“故障诊断跟踪设置”窗口可用于选择要为其设置预定故障诊断跟踪设置的服务。 在此窗口中，您可以选择一项或多项服务，然后将这些服务的跟踪设置更改为预先确定的跟踪设置。 如果有群集，可以在群集中的不同服务器上选择服务，以便所选服务的跟踪设置更改为预定的跟踪设置。 您可以选择单个服务器的特定已激活服务、服务器的所有已激活服务、群集中所有服务器的特定已激活服务或群集中所有服务器的所有已激活服务。 在窗口中，非活动服务旁会显示“不适用”。

注释 功能或网络服务的预定故障诊断跟踪设置包括 SDL、SDI 和 Log4j 跟踪设置。 在应用故障诊断跟踪设置之前，系统会备份原始的跟踪设置。 重置故障诊断跟踪设置后，原始跟踪设置将恢复。

在将故障诊断跟踪设置应用到服务后打开“故障诊断跟踪设置”窗口时，您为故障诊断设置的服务会显示为选中状态。 在“故障诊断跟踪设置”窗口中，可以将跟踪设置重置为原始设置。

将故障诊断跟踪设置应用到服务后，“跟踪配置”窗口中将显示一条消息，表明为该服务设置了故障诊断跟踪。 在“相关链接”下拉列表框中，如果要重置服务的设置，可以选择“故障诊断跟踪设置”选项。 对于给定的服务，“跟踪配置”窗口会将所有设置显示为只读，但某些跟踪输出设置参数除外，例如“文件最大数”。 即使应用故障诊断跟踪设置后，也可以修改这些参数。

跟踪收集

Cisco Unified 实时监控工具中的跟踪和日志中心选项可用于收集、查看和压缩各种服务跟踪数据或其他日志文件。借助跟踪和日志中心选项，您可以收集SDL/SDI跟踪数据、应用程序日志、系统日志（例如事件查看应用程序、安全和系统日志）和故障转储文件。

提示 不要使用 Windows 记事本查看收集的跟踪文件，因为 Windows 记事本不能正确显示换行符。

注释 仅 Unified Communications Manager：对于支持加密的设备，安全实时传输协议 (SRTP) 密钥材料不会在跟踪文件中显示。

有关跟踪收集的详细信息，请参阅《*Cisco Unified* 实时监控工具管理指南》。

被叫方跟踪

被叫方跟踪可让您配置要跟踪的目录号码或目录号码列表。您可以要求按需使用会话跟踪协议跟踪呼叫。

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

设置跟踪配置

以下程序概述了在功能配置界面中为功能和网络服务配置及收集跟踪数据的步骤。

过程

步骤 1 通过执行以下步骤之一，配置“TLC 限制 CPU 目标”和“TLC 限制 IOWait 目标”服务参数（Cisco RIS 数据收集器服务）的值：

- Cisco Unified Communications Manager 管理和 Cisco Unified IM and Presence：选择**系统** > **服务参数**，配置“TLC 限制 CPU 目标”和“TLC 限制 IOWait 目标”服务参数（Cisco RIS 数据收集器服务）的值。
- 仅 Cisco Unity Connection：选择Cisco Unity Connection 管理中的**系统设置** > **服务参数**，配置“TLC 限制 CPU 目标”和“TLC 限制 IOWait 目标”服务参数（Cisco RIS 数据收集器服务）的值。

步骤 2 为您要为其收集跟踪数据的服务配置跟踪设置。如果您有群集，可以为群集中的一台服务器或所有服务器上的服务配置跟踪。

要配置跟踪设置，请选择调试级别和跟踪字段，以选择要在跟踪日志中包含哪些信息。

如果要对服务运行预定义的跟踪，请为这些服务设置故障诊断跟踪。

步骤 3 在本地 PC 上安装 Cisco Unified 实时监控工具。

步骤 4 如果要在监控的跟踪文件中存在指定的搜索字符串时生成警报，请在 Unified RTMT 中启用 LogFileSearchStringFound 警告。

您可以在 LpmTctCatalog 中找到 LogFileSearchStringFound 警报。（选择**警报** > **定义**。 在“查找警报条件”下拉列表框中，选择**系统警报类别**；在“等于”下拉列表框中，选择 **LpmTctCatalog**）。

步骤 5 如果要自动捕获 CriticalServiceDownand CodeYellow 等警告的跟踪数据，请在“设置警告/属性”对话框为 Unified RTMT 中的特定警告选中**启用跟踪下载**复选框；配置您想要的下载频率。

步骤 6 收集跟踪数据。

步骤 7 在适当的查看器中查看日志文件。

步骤 8 如果启用了故障诊断跟踪，请重置跟踪设置服务，以便恢复原来的设置。

注释 长时间启用故障诊断跟踪会增加跟踪文件的大小，并且可能会影响服务的性能。

配置跟踪

本节提供有关配置跟踪设置的信息。

注释 启用跟踪会降低系统性能；因此，仅出于故障诊断目的启用跟踪。 如需有关使用跟踪的帮助，请联系您的技术支持团队。

设置跟踪参数

本节介绍如何配置通过功能配置 GUI 管理的功能和网络服务的跟踪参数。

提示 对于 Cisco Unity Connection，您可能需要在 Cisco Unified 功能配置和 Cisco Unity Connection 功能配置中运行跟踪，以诊断 Cisco Unity Connection 问题。 有关如何在 Cisco Unity Connection 功能配置中运行跟踪的信息，请参阅《*Cisco Unity Connection* 功能配置管理指南》。

过程

步骤 1 选择**跟踪** > **配置**。

此时将显示跟踪配置窗口。

步骤 2 从“服务器”下拉列表框中，选择正在运行要为其配置跟踪的服务的服务器；然后单击**前往**。

步骤 3 从“服务组”下拉列表框中，选择要为其配置跟踪的服务的服务组；然后单击**前往**。

提示 “跟踪配置”表中的服务组会列出与“服务组”下拉列表框中的选项对应的服务和跟踪库。

步骤 4 从“服务”下拉列表框中，选择要为其配置跟踪的服务；然后单击**前往**。

下拉列表框显示活动和非活动服务。

提示 仅 Cisco Unity Connection：对于 Cisco CallManager 和 CTIManager 服务，您可以配置 SDL 跟踪参数。 要执行此操作，请打开其中一项服务的“跟踪配置”窗口，然后单击“相关链接”下拉列表框旁边的**前往**按钮。

如果为服务配置了故障诊断跟踪，窗口顶部会显示一条消息，表明已设置“故障诊断跟踪”功能，这意味着系统会在“跟踪配置”窗口中禁用所有字段，跟踪输出设置除外。 要配置跟踪输出设置，转至步骤 11。要重置故障诊断跟踪，请参阅设置故障诊断跟踪设置。

针对您所选服务的跟踪参数将显示。 此外，“应用至所有节点”复选框将显示（仅 Unified Communications Manager）。

步骤 5 仅 Unified Communications Manager 和 IM and Presence：如果要执行此操作，只要您的配置支持群集，就可以选中**应用至所有节点**复选框，将服务或跟踪库的跟踪设置应用到群集中的所有服务器。

步骤 6 选中**打开跟踪**复选项。

步骤 7 仅 Cisco Unity Connection：如果要配置 SDL 跟踪参数，请转至步骤 10。

步骤 8 如调试跟踪级别设置中所述，从**调试跟踪级别**列表框中选择要跟踪的信息级别。

步骤 9 选中您选择的服务对应的**跟踪字段**（例如，Cisco 日志分区监控工具跟踪字段）复选框。

步骤 10 如果服务没有多个跟踪设置，您可以在其中指定要激活的跟踪，请选中**启用所有跟踪**复选框。 如果您选择的服务有多个跟踪设置，请如跟踪字段说明中所述，选中要启用的跟踪复选框旁边的复选框。

步骤 11 要限制跟踪文件的数量和大小，请指定跟踪输出设置。 有关说明，请参阅跟踪输出设置。

步骤 12 要保存跟踪参数配置，请单击**保存**按钮。

对于所有服务，对跟踪配置的更改会立即生效，Cisco 消息传递接口除外（仅 Unified Communications Manager）。 Cisco 消息传送接口的跟踪配置更改将在 3 到 5 分钟后生效。

注释 要设置默认值，请单击**设置默认值**按钮。

跟踪配置中的服务组

下表列出了与“跟踪配置”窗口“服务组”下拉列表框中的选项对应的服务和跟踪库。

表 *37:* 跟踪配置中的服务组

服务组	服务和跟踪库	备注
Unified Communications Manager CM 服务	• Cisco CTIManager • Cisco CallManager • Cisco CallManager Cisco IP 电话服务 • Cisco DHCP 监控器服务 • Cisco 被叫号码分析器 • Cisco 被叫号码分析器服务器 • Cisco 扩展功能，Cisco Extension Mobility • Cisco Extension Mobility 应用程序 • Cisco IP 语音媒体流应用程序 • Cisco Messaging 接口 • Cisco TFTP • Cisco Unified 移动语音访问服务	对于“CM 服务”组中的大多数服务，您对特定组件运行跟踪，而不是为该服务启用所有跟踪。“跟踪”字段说明列出您可以对特定组件运行跟踪的服务。
Unified Communications Manager CTI 服务	• Cisco IP Manager Assistant • Cisco Web Dialer Web 服务	对于这些服务，您可以对特定的组件运行跟踪，而不是为该服务启用所有跟踪；请参阅“跟踪”字段说明。

服务组	服务和跟踪库	备注
Unified Communications Manager CDR 服务	• Cisco Unified Communications Manager CDR 分析和报告计划程序 • Cisco Unified Communications Manager CDR 分析和报告 Web 服务 • Cisco CDR 代理 • Cisco CDR 存放库管理器	您需要为每项服务启用所有跟踪，而不是为特定组件运行跟踪。 在 Cisco Unified Communications Manager CDR 分析和报告中，当报告运行呼叫已存储程序时，Cisco Unified Communications Manager CDR 分析和报告检查在已存储程序日志记录开始之前在“跟踪配置”窗口中为 Cisco Unified Communications Manager CDR 分析和报告计划程序以及 Cisco Unified Communications Manager CDR 分析和报告 Web 服务配置的调试跟踪级别。对于预生成的报告，Cisco Unified Communications Manager CDR 分析和报告检查 Cisco Unified Communications Manager CDR 分析和报告计划程序服务的级别；对于按需报告，Cisco Unified Communications Manager CDR 分析和报告检查 Cisco Unified Communications Manager CDR 分析和报告 Web 服务的级别。如果从“调试跟踪级别”下拉列表框中选择“调试”，则会启用已存储程序日志记录，并且会持续到您从下拉列表框中选择另一个选项。 以下 Cisco Unified Communications Manager CDR 分析和报告报告使用已存储程序日志记录：网关使用情况报告、路由和线路组使用情况报告、路由/寻线列表使用情况报告、路由模式/寻线引导使用情况报告、会议呼叫详细信息报告、会议呼叫摘要报告、会议网桥使用情况报告、语音留言使用情况报告以及 CDR 搜索报告。

服务组	服务和跟踪库	备注
IM and Presence Service	• Cisco 客户端配置文件代理 • Cisco 配置代理 • Cisco 群集间同步代理 • Cisco 登录数据存储器 • Cisco OAM 代理 • Cisco Presence 数据存储器 • Cisco Presence Engine • Cisco IM and Presence 数据监控器 • Cisco 路由数据存储器 • Cisco SIP Proxy • Cisco SIP 注册数据存储器 • Cisco 服务器恢复管理器 • Cisco 同步代理 • Cisco XCP 验证服务 • Cisco XCP 配置管理器 • Cisco XCP 连接管理器 • Cisco XCP 目录服务 • Cisco XCP 消息存档程序 • Cisco XCP 路由器 • Cisco XCP SIP 联合连接管理器 • Cisco XCP 文字会议管理器 • Cisco XCP Web 连接管理器 • Cisco XCP XMPP 联合连接管理器	有关这些服务的说明，请参阅与 Cisco Unified IM and Presence 功能配置中的功能和网络服务相关的主题。 • 对于这些服务，应该为服务启用所有跟踪，而不是为特定组件运行跟踪。

服务组	服务和跟踪库	备注
数据库和管理服务	Unified Communications Manager 和 Cisco Unity Connection： • Cisco AXL Web 服务 • Cisco CCM DBL Web 库 • Cisco CCMAdmin Web 服务 • Cisco CCMUser Web 服务 • Cisco 数据库层监控器 • Cisco UXL Web 服务 Unified Communications Manager • Cisco 批量预配置服务 • Cisco GRT 通信 Web 服务 • Cisco 基于角色安全性 • Cisco TAPS 服务 • Cisco Unified 报告 Web 服务 IM and Presence Services： • Cisco AXL Web 服务 • Cisco 批量预配置服务 • Cisco CCMUser Web 服务 • Cisco 数据库层监控器 • Cisco GRT 通信 Web 服务 • Cisco IM and Presence 管理员 • Cisco Unified 报告 Web 服务 • 平台管理 Web 服务	选择“Cisco CCM DBL Web 库”选项会激活对 Java 应用程序数据库访问的跟踪。 对于 C++ 应用程序的数据库访问，按照 Cisco 扩展功能跟踪字段中的说明激活对 Cisco 数据库层监控器的跟踪。 选择 Cisco 基于角色的安全选项，它支持 Unified Communications Manager，激活对用户角色授权的跟踪。 对于“数据库和管理服务”组中的大多数服务，您需要启用服务/库的所有跟踪，而不是启用特定组件的跟踪。 对于 Cisco 数据库层监控，您可以对特定的组件运行跟踪。 **注释** 您可以在 Cisco Unified IM and Presence 功能配置 UI 中控制服务的日志记录。 要更改日志级别，请选择“系统服务”组和 Cisco CCMService Web 服务。

服务组	服务和跟踪库	备注
性能和监控服务	Unified Communications Manager 和 Cisco Unity Connection： • Cisco AMC 服务 • Cisco CCM NCS Web 库 • CCM PD Web 服务 • Cisco CallManager SNMP 服务 • Cisco 日志分区监控工具 • Cisco RIS 数据收集器 • Cisco RTMT Web 服务 • Cisco Audit Event 服务 • Cisco RisBean 库 Unified Communications Manager： • Cisco CCM PD Web 服务 IM and Presence Services： • Cisco AMC 服务 • Cisco Audit Event 服务 • Cisco 日志分区监控工具 • Cisco RIS 数据收集器 • Cisco RTMT Web 服务 • Cisco RisBean 库	选择 Cisco CCM NCS Web 库选项会激活对 Java 客户端数据库更改通知的跟踪。 选择 Cisco Unity RTMT Web 服务选项会激活对 Unity RTMT 小型应用程序的跟踪；运行此跟踪将为 Unity RTMT 客户端查询创建服务器端日志。
Unified Communications Manager 安全服务	• Cisco CTL 提供程序 • Cisco 证书权限代理功能 • Cisco 信任验证服务	您需要为每项服务启用所有跟踪，而不是为特定组件运行跟踪。
Unified Communications Manager 目录服务	Cisco DirSync	您需要为此服务启用所有跟踪，而不是为特定组件运行跟踪。
备份和恢复服务	• Cisco DRF Local • 仅限 Unified Communications Manager 和 Cisco Unity Connection：Cisco DRF Master	您需要为每项服务启用所有跟踪，而不是为特定组件运行跟踪。

服务组	服务和跟踪库	备注
系统服务	Unified Communications Manager： • Cisco CCMRealm Web 服务 • Cisco CCMService Web 服务 • Cisco 通用用户界面 • Cisco 跟踪收集服务 IM and Presence Services： • Cisco CCMService Web 服务 • Cisco 跟踪收集服务	选择 Cisco CCMRealm Web 服务选项会激活对登录身份验证的跟踪。 选择“Cisco 通用用户界面”选项会激活对多个应用程序使用的通用代码的跟踪。例如，Cisco Unified 操作系统管理和 Cisco Unified 功能配置。 选择 Cisco CCMService Web 服务选项将激活对 Cisco Unified 功能配置 Web 应用程序 (GUI) 的跟踪。 您需要为每个选项/服务启用所有跟踪，而不是为特定组件运行跟踪。
SOAP 服务	• CiscoSOAP Web 服务 • CiscoSOAPMessage 服务	选择“Cisco SOAP Web 服务”选项将激活对 AXL 功能配置 API 的跟踪。 您需要为此服务启用所有跟踪，而不是为特定组件运行跟踪。
平台服务	Cisco Unified 操作系统管理 Web 服务	Cisco Unified OS 管理 Web 服务支持 Cisco Unified 操作系统管理，它是提供证书管理、版本设置和安装与升级等平台相关功能管理的 Web 应用程序。 您需要为此服务启用所有跟踪，而不是为特定组件运行跟踪。

调试跟踪级别设置

下表介绍了服务的调试跟踪级别设置。

表 *38:* 服务的调试跟踪级别

级别	说明
错误	跟踪警报条件和事件。 用于异常路径中生成的所有跟踪。使用最少的 CPU 周期数。
特殊	跟踪所有错误情况以及过程和设备初始化消息。
状态转换	跟踪正常操作期间发生的所有特殊情况以及子系统状态转换。 跟踪呼叫处理事件。
重要	跟踪所有状态转换条件以及正常操作期间发生的媒体层事件。

级别	说明
入口/出口	**注释** 并非所有服务都使用此跟踪级别。 跟踪所有重要情况以及例程的入口和出口点。
任意	跟踪所有进入/退出条件和低层调试信息。
详细	跟踪所有任意情况以及详细的调试信息。

下表介绍了小型应用程序的调试跟踪级别设置。

表 *39*: 小型应用程序的调试跟踪级别

级别	说明
严重	跟踪可能导致应用程序中止的非常严重的错误事件。
错误	跟踪警报条件和事件。 用于异常路径中生成的所有跟踪。
警告	跟踪可能有害的情况。
信息	跟踪大部分 Servlet 问题，对系统性能的影响最小。
调试	跟踪所有状态转换条件以及正常操作期间发生的媒体层事件。 打开所有日志记录的跟踪级别。

跟踪字段说明

对于某些服务，您可以为特定的组件激活跟踪，而不是为服务启用所有跟踪。 以下列表包括您可以为其特定组件激活跟踪的服务。 单击其中一个交叉引用会转到相应的部分，那里会显示服务的每个跟踪字段的描述。 如果以下列表中没有服务，“跟踪配置”窗口中会显示该服务的“启用所有跟踪”复选框。

以下服务适用于 Unified Communications Manager 和 Cisco Unity Connection：

- 数据库层监控器跟踪字段
- Cisco RIS 数据收集器跟踪字段

以下服务适用于 Unified Communications Manager：

- Cisco CallManager SDI 跟踪字段
- Cisco CallManager SDL 跟踪字段
- Cisco CTIManager SDL 跟踪字段
- Cisco 扩展功能跟踪字段

- Cisco Extension Mobility 跟踪字段
- Cisco IP Manager Assistant 跟踪字段
- Cisco IP 语音媒体流应用程序跟踪字段
- Cisco TFTP 跟踪字段
- Cisco Web Dialer Web 服务跟踪字段

数据库层监控器跟踪字段

下表介绍了 Cisco 数据库层监控器跟踪字段。 Cisco 数据库层监控器服务支持 Unified Communications Manager 和Cisco Unity Connection。

表 *40: Cisco* 数据库层监控器跟踪字段

字段名称	说明
启用数据库库跟踪	激活对 C++ 应用程序的数据库库跟踪。
启用服务跟踪	激活服务跟踪。
启用数据库更改通知跟踪	激活对 C++ 应用程序的数据库更改通知跟踪。
启用单元测试跟踪	请勿选中此复选框。 Cisco 工程人员将其用于调试目的。

Cisco RIS 数据收集器跟踪字段

下表介绍了 Cisco RIS 数据收集器跟踪字段。 Cisco RIS 数据收集器服务支持 Unified Communications Manager 和 Cisco Unity Connection。

表 *41: Cisco RIS* 数据收集器跟踪字段

字段名称	说明
启用 RISDC 跟踪	激活对 RIS 数据收集器服务 (RIS) 的 RISDC 线程的跟踪。
启用系统访问跟踪	激活对 RIS 数据收集器中的系统访问库的跟踪。
启用链路服务跟踪	激活对 RIS 数据收集器中的链路服务库的跟踪。
启用 RISDC 访问跟踪	激活对 RIS 数据收集器中的 RISDC 访问库的跟踪。
启用 RISDB 跟踪	激活对 RIS 数据收集器中的 RISDB 库的跟踪。
启用 PI 跟踪	激活对 RIS 数据收集器中的 PI 库的跟踪。

字段名称	说明
启用 XML 跟踪	激活对 RIS 数据收集器服务的输入/输出 XML 消息的跟踪。
启用性能监控记录器跟踪	激活对 RIS 数据收集器中的故障诊断性能监控数据日志记录的跟踪。 用于跟踪日志文件的名称、所记录的计数器总数、应用程序以及系统计数器和实例的名称、计算的进程和线程CPU百分比以及日志文件的滚动和删除。

Cisco CallManager SDI 跟踪字段

下表介绍了 Cisco CallManager SDI 跟踪字段。 Cisco CallManager 服务支持 Unified Communications Manager。

表 *42: Cisco CallManager SDI* 跟踪字段

字段名称	说明
启用 H245 消息跟踪	激活 H245 消息的跟踪。
启用 DT-24+/DE-30+ 跟踪	激活 DT-24+/DE-30+ 设备跟踪的 ISDN 类型的日志记录。
启用 PRI 跟踪	激活主速率接口 (PRI) 设备的跟踪。
启用 ISDN 转换跟踪	激活 ISDN 消息跟踪。 用于正常调试。
启用 H225 & 网守跟踪	激活 H.225 设备的跟踪。 用于正常调试。
启用其他跟踪	激活其他设备的跟踪。 **注释** 不要在正常的系统操作期间选中此复选框。
启用会议网桥跟踪	激活会议网桥的跟踪。 用于正常调试。
启用音乐保持跟踪	激活音乐保持 (MOH) 设备的跟踪。 用于跟踪 MOH 设备状态，例如已注册到 Unified Communications Manager、未注册 Unified Communications Manager 以及资源分配处理成功或失败。
启用 Unified CM 实时信息服务器跟踪	激活实时信息服务器使用的 Unified Communications Manager 实时信息跟踪。
启用 SIP 堆栈跟踪	激活 SIP 堆栈跟踪。 默认为启用。

字段名称	说明
启用报警器跟踪	激活对报警器的跟踪，报警器是使用 Cisco IP 语音媒体流应用程序服务以向 Cisco Unified IP 电话、网关和其他可配置设备播放预录音通知（.wav 文件）和铃声的 SCCP 设备。
启用 CDR 跟踪	激活对 CDR 的跟踪。
启用模拟干线跟踪	激活所有模拟干线 (AT) 网关的跟踪。
启用所有电话设备跟踪	激活电话设备的跟踪。 跟踪信息包括软件电话设备。 用于正常调试。
启用 MTP 跟踪	激活媒体终止点 (MTP) 设备的跟踪。 用于正常调试。
启用所有网关跟踪	激活所有模拟和数字网关的跟踪。
启用前转和其他跟踪	激活对呼叫前转和未被另一复选框覆盖的所有子系统激活跟踪。 用于正常调试。
启用 MGCP 跟踪	激活对媒体网关控制协议 (MGCP) 设备的跟踪。 用于正常调试。
启用媒体资源管理器跟踪	激活对媒体资源管理器 (MRM) 活动的跟踪。
启用 SIP 呼叫处理跟踪	激活对 SIP 呼叫处理的跟踪。
启用 SCCP 保持连接跟踪	激活对 Cisco CallManager 跟踪中 SCCP 保持连接跟踪信息的跟踪。 因为每个 SCCP 设备每 30 秒报告保持连接消息，并且每个保持连接消息都会创建 3 行跟踪数据，所以系统会在此复选框被选中时会生成大量的跟踪数据。
启用 SIP 保持连接（注册刷新）跟踪	激活对 Cisco CallManager 跟踪中 SIP 保持连接（注册刷新）跟踪信息的跟踪。 因为每个 SIP 设备每 2 分钟报告保持连接消息，并且每条保持连接消息可以创建多行跟踪数据，所以系统会在此复选框被选中时生成大量的跟踪数据。

Cisco CallManager SDL 跟踪字段

下表介绍了 Cisco CallManager SDL 跟踪过滤器字段。 Cisco CallManager 服务支持 Unified Communications Manager。

注释 Cisco 建议使用默认值，除非 Cisco 工程师指示您执行其他操作。

表 *43: Cisco CallManager SDL* 配置跟踪过滤器设置

设置名称	说明
启用所有第 1 层跟踪。	激活对第 1 层的跟踪。
启用详细的第 1 层跟踪。	激活详细的第 1 层跟踪。
启用所有第 2 层跟踪。	激活对第 2 层的跟踪。
启用第 2 层接口跟踪。	激活对第 2 层接口的跟踪。
启用第 2 层 TCP 跟踪。	激活第 2 层传输控制程序 (TCP) 跟踪。
启用详细转储第 2 层跟踪。	激活对第 2 层转储的详细跟踪。
启用所有第 3 层跟踪。	激活对第 3 层的跟踪。
启用所有呼叫控制跟踪。	激活对呼叫控制的跟踪。
启用其他轮询跟踪。	激活对其他轮询的跟踪。
启用其他跟踪（数据库信号）。	激活数据库信号等其他跟踪。
启用消息转换信号跟踪。	激活对消息转换信号的跟踪。
启用 UUIE 输出跟踪。	激活对用户到用户信息元素 (UUIE) 输出的跟踪。
启用网关信号跟踪。	激活对网关信号的跟踪。
启用 CTI 跟踪。	激活 CTI 跟踪。
启用网络服务数据跟踪	激活网络服务数据跟踪。
启用网络服务事件跟踪	激活网络服务事件跟踪。
启用 ICCP 管理跟踪	激活 ICCP 管理跟踪。
启用默认跟踪	激活默认跟踪。

下表介绍了 Cisco CallManager SDL 配置特征。

表 *44: Cisco CallManager SDL* 配置跟踪特征

特征	说明
启用 SDL 链接状态跟踪。	激活对群集内通信协议 (ICCP) 链接状态的跟踪。
启用低级别 SDL 跟踪。	激活对低级别 SDL 的跟踪。
启用 SDL 链接轮询跟踪。	激活对 ICCP 链接轮询的跟踪。
启用 SDL 链接消息跟踪。	激活对 ICCP 原始消息的跟踪。

特征	说明
启用信号数据转储跟踪。	激活对信号数据转储的跟踪。
启用相关标签映射跟踪。	激活对相关标签映射的跟踪。
启用 SDL 进程状态跟踪。	激活对 SDL 进程状态的跟踪。
禁用 SDL 美观打印跟踪。	禁用对 SDL 美观印刷的跟踪。 美观打印会在跟踪文件中添加选项卡和空间而不执行后处理。
启用 SDL TCP 事件跟踪。	激活 SDL TCP 事件跟踪。

Cisco CTIManager SDL 跟踪字段

下表介绍了 Cisco CTIManager SDL 配置跟踪过滤器设置。 Cisco CTIManager 服务支持 Unified Communications Manager。

提示 Cisco 建议使用默认值，除非 Cisco 工程师指示您执行其他操作。

提示 从“服务组”下拉列表框中选择 CTIManager 服务时，将为此服务的 SDI 跟踪显示“跟踪配置”窗口。 要为 Cisco CTI Manager 服务激活 SDI 跟踪，请在 Cisco CTIManager 服务的“跟踪配置”窗口中选中**启用所有跟踪**复选框。要访问 SDL 配置窗口，请从“相关链接”下拉列表框选择**SDL 配置**；“Cisco CTIManager SDL 配置跟踪过滤器设置”表和“Cisco CTIManager SDL 配置跟踪特征”表中介绍的设置将会显示。

表 *45: Cisco CTIManager SDL* 配置跟踪过滤器设置

设置名称	说明
启用其他轮询跟踪。	激活对其他轮询的跟踪。
启用其他跟踪（数据库信号）。	激活数据库信号等其他跟踪。
启用 CTI 跟踪。	激活 CTI 跟踪。
启用网络服务数据跟踪	激活网络服务数据跟踪。
启用网络服务事件跟踪	激活网络服务事件跟踪。
启用 ICCP 管理跟踪	激活 ICCP 管理跟踪。
启用默认跟踪	激活默认跟踪。

下表介绍了 Cisco CTIManager SDL 配置跟踪特征。

表 *46: Cisco CTIManager SDL* 配置跟踪特征

特征	说明
启用 SDL 链接状态跟踪。	激活对 ICCP 链接状态的跟踪。
启用低级别 SDL 跟踪。	激活对低级别 SDL 的跟踪。
启用 SDL 链接轮询跟踪。	激活对 ICCP 链接轮询的跟踪。
启用 SDL 链接消息跟踪。	激活对 ICCP 原始消息的跟踪。
启用信号数据转储跟踪。	激活对信号数据转储的跟踪。
启用相关标签映射跟踪。	激活对相关标签映射的跟踪。
启用 SDL 进程状态跟踪。	激活对 SDL 进程状态的跟踪。
禁用 SDL 美观打印跟踪。	禁用对 SDL 美观印刷的跟踪。 美观打印会在跟踪文件中添加选项卡和空间而不执行后处理。
启用 SDL TCP 事件跟踪	激活 SDL TCP 事件跟踪。

Cisco 扩展功能跟踪字段

下表介绍了 Cisco 扩展功能跟踪字段。 Cisco 扩展功能服务支持 Unified Communications Manager。

表 *47: Cisco* 扩展功能跟踪字段

字段名称	说明
启用 QBE 帮助程序 TSP 跟踪	激活电话服务提供商跟踪。
启用 QBE 帮主程序 TSPI 跟踪	激活 QBE 帮助程序 TSP 接口跟踪。
启用 QRT 字典跟踪	激活质量报告工具服务字典跟踪。
启用 DOM 帮助程序跟踪	激活 DOM 帮助程序跟踪。
启用冗余和更改通知跟踪	激活数据库更改通知跟踪。
启用 QRT 报告处理程序跟踪	激活质量报告工具报告处理程序跟踪。
启用 QBE 帮主程序 CTI 跟踪	激活 QBE 帮主程序 CTI 跟踪。
启用 QRT 服务跟踪	激活质量报告工具服务相关跟踪。
启用 QRT DB 跟踪	激活 QRT DB 访问跟踪。
启用模板映射跟踪	激活标准模板映射和多映射跟踪。
启用 QRT 事件处理程序跟踪	激活质量报告工具事件处理程序跟踪。

字段名称	说明
启用 QRT 实时信息服务器跟踪	激活质量报告工具实时信息服务器跟踪。

Cisco Extension Mobility 跟踪字段

下表介绍了 Cisco Extension Mobility 跟踪字段。 Cisco Extension Mobility 服务支持 Unified Communications Manager。

表 *48: Cisco Extension Mobility* 跟踪字段

字段名称	说明
启用 EM 服务跟踪	激活对分级移动服务的跟踪。

提示 当您激活对 Cisco Extension Mobility 应用程序服务的跟踪时，可在“跟踪配置”窗口中为 Cisco Extension Mobility 应用程序服务选中“启用所有跟踪”复选框。

Cisco IP Manager Assistant 跟踪字段

下表介绍了 Cisco IP Manager Assistant 跟踪字段。 Cisco IP Manager Assistant 服务支持 Cisco Unified Communications Manager Assistant。

表 *49: Cisco IP Manager Assistant* 跟踪字段

字段名称	说明
启用 IPMA 服务跟踪	激活对 Cisco IP Manager Assistant 服务的跟踪。
启用 IPMA Manager 配置更改日志	激活您对经理和助理配置所做更改的跟踪。
启用 IPMA CTI 跟踪	激活对 CTI Manager 连接的跟踪。
启用 IPMA CTI 安全跟踪	激活对通往 CTIManager 的安全连接的跟踪。

Cisco IP 语音媒体流应用程序跟踪字段

本节介绍的内容不适用于 Cisco Unity Connection。

下表介绍了 Cisco IP 语音媒体流应用程序跟踪字段。 Cisco IP 语音媒体流应用程序服务支持 Unified Communications Manager。

表 *50: Cisco IP* 语音媒体流应用程序跟踪字段

字段名称	说明
启用服务初始化跟踪	激活对初始化信息的跟踪。

字段名称	说明
启用 MTP 设备跟踪	激活跟踪以监控已处理的媒体终止点 (MTP) 的消息。
启用设备恢复跟踪	激活对 MTP、会议网桥和 MOH 的设备恢复相关信息的跟踪。
启用瘦站消息跟踪	激活对瘦站协议的跟踪。
启用 WinSock 第 2 级跟踪	激活对高级、详细及 WinSock 相关信息的跟踪。
启用音乐保持管理器跟踪	激活跟踪以监控 MOH 音频来源管理器。
启用报警器跟踪	激活跟踪以监控报警器。
启用数据库设置管理器跟踪	激活跟踪以监控 MTP、会议网桥和 MOH 的数据库设置和更改。
启用会议网桥设备跟踪	激活跟踪以监控会议网桥的已处理消息。
启用设备驱动程序跟踪	激活设备驱动程序跟踪。
启用 WinSock 第 1 级跟踪	激活对低级别、常规及 WinSock 相关信息的跟踪。
启用音乐保持设备跟踪	激活跟踪以监控已处理 MOH 消息。
启用 TFTP 下载跟踪	激活跟踪以监控 MOH 音频来源文件的下载。

Cisco TFTP 跟踪字段

下表介绍了 Cisco TFTP 跟踪字段。 Cisco TFTP 服务支持 Unified Communications Manager。

表 *51: Cisco TFTP* 跟踪字段

字段名称	说明
启用服务系统跟踪	激活对服务系统的跟踪。
启用构建文件跟踪	激活对构建文件的跟踪。
启用服务文件跟踪	激活对服务文件的跟踪。

Cisco Web Dialer Web 服务跟踪字段

下表介绍了 Cisco Web Dialer Web 服务跟踪字段。 Cisco Web Dialer Web 服务支持 Unified Communications Manager。

表 *52: Cisco Web Dialer Web* 服务跟踪字段

字段名称	说明
启用 Web Dialer 小型应用程序跟踪	激活对 Cisco Web Dialer 小型应用程序的跟踪。
启用重定向器小型应用程序跟踪	激活对重定向器小型应用程序的跟踪。

IM and Presence SIP 代理服务跟踪过滤器设置

下表介绍了 IM and Presence SIP 代理的服务跟踪过滤器设置。

表 *53: IM and Presence SIP* 代理服务跟踪过滤器设置

参数	说明
启用访问日志跟踪	此参数启用代理访问日志跟踪；记录代理收到的每条 SIP 消息的第一行。
启用验证跟踪	此参数启用对验证模块的跟踪。
启用日历跟踪	此参数启用对日历模块的跟踪。
启用 CTI 网关跟踪	此参数启用对 CTI 网关的跟踪。
启用枚举跟踪	此参数启用对枚举模块的跟踪。
启用方法/事件路由跟踪	此参数启用对方法/事件路由模块的跟踪。
启用号码扩展跟踪	此参数启用对号码扩展模块的跟踪。
启用解析器跟踪	此参数启用对与每个 sipd 子 SIP 解析器操作相关的解析器信息的跟踪。
启用隐私跟踪	此参数启用对与隐私请求相关的 PAI、RPID 和转移标头的处理信息的跟踪。
启用注册表跟踪	此参数启用对注册表模块的跟踪。
启用路由跟踪	此参数启用对路由模块的跟踪。
启用 SIPUA 跟踪	此参数启用对 SIP UA 应用程序模块的跟踪。
启用服务器跟踪	此参数启用对服务器的跟踪。
启用 SIP 消息和状态机跟踪	此参数启用对与每个 sipd SIP 状态机操作相关的信息的跟踪。
启用 SIP TCP 跟踪	此参数启用对与 TCP 服务 SIP 消息之 TCP 传输有关的信息的跟踪。
启用 SIP TLS 跟踪	此参数启用对与 TCP 服务 SIP 消息之 TLS 传输有关的信息的跟踪。

参数	说明
启用 SIP XMPP IM 网关跟踪	此参数启用对 SIP XMPP IM 网关的跟踪。
启用 Presence Web 服务跟踪	此参数启用对 Presence Web 服务的跟踪。

IM and Presence 跟踪字段说明

下表提供支持特定组件跟踪激活的服务的字段说明。 对于某些服务，您可以为特定的组件激活跟踪，而不是为服务启用所有跟踪。 如果有服务未包含在本章中，跟踪配置窗口中会显示该服务的启用所有跟踪。

Cisco 访问日志跟踪字段

下表介绍了 Cisco 访问日志跟踪字段。

表 *54:* 访问日志跟踪字段

字段名称	说明
启用访问日志跟踪	打开访问日志跟踪。

Cisco 验证跟踪字段

下表介绍了 Cisco 验证跟踪字段。

表 *55:* 验证跟踪字段

字段名称	说明
启用验证跟踪	打开验证跟踪。

Cisco 日历跟踪字段

下表介绍了 Cisco 日历跟踪字段。

表 *56:* 日历跟踪字段

字段名称	说明
启用日历跟踪	打开日历跟踪。

Cisco CTI 网关跟踪字段

下表介绍了 Cisco CTI 网关跟踪字段。

表 *57: CTI* 网关跟踪字段

字段名称	说明
启用 CTI 网关跟踪	开启 CTI 网关跟踪。

Cisco 数据库层监控器跟踪字段

下表介绍了 Cisco 数据库层监控器跟踪字段。

表 *58: Cisco* 数据库层监控器跟踪字段

字段名称	说明
启用数据库库跟踪	打开 C++ 应用程序的数据库库跟踪。
启用服务跟踪	打开服务跟踪。
启用数据库更改通知跟踪	激活对 C++ 应用程序的数据库更改通知跟踪。
启用单元测试跟踪	不检查。 Cisco 工程人员将其用于调试目的。

Cisco 枚举跟踪字段

下表介绍了 Cisco 枚举跟踪字段。

表 *59:* 枚举跟踪字段

字段名称	说明
启用枚举跟踪	打开枚举跟踪。

Cisco 方法/事件跟踪字段

下表介绍了 Cisco 方法/事件跟踪字段。

表 *60:* 方法/事件跟踪字段

字段名称	说明
启用方法/事件跟踪	打开方法/事件跟踪。

Cisco 号码扩展跟踪字段

下表介绍了 Cisco 号码扩展跟踪字段。

表 *61:* 号码扩展跟踪字段

字段名称	说明
启用号码扩展跟踪	激活号码扩展跟踪。

Cisco 解析器跟踪字段

下表介绍了 Cisco 解析器跟踪字段。

表 *62:* 解析器跟踪字段

字段名称	说明
启用解析器跟踪	激活解析器跟踪。

Cisco 隐私跟踪字段

下表介绍了 Cisco 隐私跟踪字段。

表 *63:* 隐私跟踪字段

字段名称	说明
启用隐私跟踪	激活隐私跟踪。

Cisco 代理跟踪字段

下表介绍了 Cisco 代理跟踪字段。

表 *64:* 代理跟踪字段

字段名称	说明
添加代理	打开代理跟踪。

Cisco RIS 数据收集器跟踪字段

下表介绍了 Cisco RIS 数据收集器跟踪字段。

表 *65: Cisco RIS* 数据收集器跟踪字段

字段名称	说明
启用 RISDC 跟踪	激活对 RIS 数据收集器服务 (RIS) 的 RISDC 线程的跟踪。
启用系统访问跟踪	激活对 RIS 数据收集器中的系统访问库的跟踪。

字段名称	说明
启用链路服务跟踪	激活对 RIS 数据收集器中的链路服务库的跟踪。
启用 RISDC 访问跟踪	激活对 RIS 数据收集器中的 RISDC 访问库的跟踪。
启用 RISDB 跟踪	激活对 RIS 数据收集器中的 RISDB 库的跟踪。
启用 PI 跟踪	激活对 RIS 数据收集器中的 PI 库的跟踪。
启用 XML 跟踪	激活对 RIS 数据收集器服务的输入/输出 XML 消息的跟踪。
启用性能监控记录器跟踪	激活对 RIS 数据收集器中的故障诊断性能监控数据日志记录的跟踪。 用于跟踪日志文件的名称、所记录的计数器总数、应用程序以及系统计数器和实例的名称、计算的进程和线程CPU 百分比以及日志文件的滚动和删除。

Cisco 注册表跟踪字段

下表介绍了 Cisco 注册表跟踪字段。

表 *66:* 注册表跟踪字段

字段名称	说明
启用注册表跟踪	激活注册表跟踪。

Cisco 路由跟踪字段

下表介绍了 Cisco 路由跟踪字段。

表 *67:* 路由跟踪字段

字段名称	说明
启用路由跟踪	激活路由跟踪。

Cisco 服务器跟踪字段

下表介绍了 Cisco 服务器跟踪字段。

表 *68:* 服务器跟踪字段

字段名称	说明
启用服务器跟踪	激活服务器跟踪。

Cisco SIP 消息和状态机跟踪字段

下表介绍了 Cisco SIP 消息和状态机跟踪字段。

表 *69: SIP* 消息和状态机跟踪字段

字段名称	说明
启用 SIP 消息和状态机跟踪	激活 SIP 消息和状态机跟踪。

Cisco SIP TCP 跟踪字段

下表介绍了 Cisco SIP TCP 跟踪字段。

表 *70: SIP TCP* 跟踪字段

字段名称	说明
启用 SIP TCP 跟踪	激活 SIP TCP 跟踪。

Cisco SIP TLS 跟踪字段

下表介绍了 Cisco SIP TLS 跟踪字段。

表 *71: SIP TLS* 跟踪字段

字段名称	说明
启用 SIP TLS 跟踪	激活 SIP TLS 跟踪。

Cisco Web 服务跟踪字段

下表介绍了 Cisco Web 服务跟踪字段。

表 *72: Web* 服务跟踪字段

字段名称	说明
启用 Presence Web 服务跟踪	激活 Presence Web 服务跟踪。

跟踪输出设置

下表包含跟踪日志文件说明。

注意 当您在“跟踪配置”窗口中更改“文件最大数”或“文件最大大小”设置时，系统将删除除当前文件（即服务正在运行的文件）以外的所有服务日志文件；如果尚未激活该服务，系统会在您激活该服务后立即删除文件。 在更改“文件最大数”或“文件最大大小”设置之前，如果要保留日志文件的记录，请下载服务日志文件并将其保存到另一台服务器；要执行此任务，请使用 Unity RTMT 中的跟踪和日志中心。

表 *73:* 跟踪输出设置

字段	说明
文件最大数	此字段指定给定服务的跟踪文件总数。 Cisco Unified 功能配置会自动在文件名后附加序列号以指示它是哪个文件，例如 cus299.txt。 当序列中的最后一个文件已满时，跟踪数据开始覆盖第一个文件。 默认值因服务而异。
文件最大大小 (MB)	此字段指定跟踪文件的最大大小，以 MB 为单位。 默认值因服务而异。

跟踪设置故障诊断

故障诊断跟踪设置窗口

在功能配置 GUI 中，**故障诊断跟踪设置**窗口可用于选择要为其设置预定故障诊断跟踪设置的服务。 在此窗口中，您可以选择群集中不同节点上的服务。 这会为您选择的所有服务填充跟踪设置更改。 您可以选择单个节点的特定活动服务、节点的所有活动服务、群集中所有节点的特定活动服务或群集中所有节点的所有活动服务。 在窗口中，非活动服务旁会显示“不适用”。

注释 对于 IM and Presence，IM and Presence 功能或网络服务的预定故障诊断跟踪设置包括 SDI 和 Log4j 跟踪设置。 在应用故障诊断跟踪设置之前，系统会备份原始的跟踪设置。 重置故障诊断跟踪设置后，原始跟踪设置将恢复。

在将故障诊断跟踪设置应用到服务后打开**故障诊断跟踪设置**窗口时，您为故障诊断设置的服务会显示为选中状态。 在**故障诊断跟踪设置**窗口中，可以将跟踪设置重置为原始设置。

将故障诊断跟踪设置应用到服务后，**跟踪配置**窗口中将显示一条消息，表明为该服务设置了故障诊断跟踪。在**相关链接**列表框中，如果要重置服务的设置，可以选择“故障诊断跟踪设置”选项。对于给定的服务，**跟踪配置**窗口会将所有设置显示为只读，但某些跟踪输出设置参数除外，例如“文件最大数”。

故障诊断跟踪设置

开始之前

查看任务设置跟踪配置并设置跟踪参数。

过程

步骤 1 选择**跟踪** > **故障诊断跟踪设置**。

步骤 2 从**服务器**列表框中选择您要对跟踪设置进行故障诊断的服务器。

步骤 3 选择**前往**。

此时服务列表将显示。 处于非活动状态的服务将显示为不适用。

步骤 4 执行以下操作之一：

a) 要监控您在**服务器**列表框中选择的节点上的特定服务，请在**服务**窗格中选中服务。

例如，“数据库和管理服务”窗格、“性能和监控服务”窗格或者“备份和恢复服务”窗格等等。

此任务仅影响您在**服务器**列表框中选择的节点。

b) 要监控您在**服务器**列表框中选择的节点上的所有服务，请选中**检查所有服务**。

c) 仅 Cisco Unified Communications Manager 和 IM and Presence 群集：要监控群集中所有节点上的特定服务，请选中**检查所有节点上的选定服务**。

此设置适用于服务处于活动状态的群集中的所有节点。

d) 仅 Unified Communications Manager 和 IM and Presence群集：要监控群集中所有节点上的所有服务，请选中**检查所有节点上的所有服务**。

步骤 5 选择**保存**。

步骤 6 选择以下按钮之一恢复原来的跟踪设置：

a) **重置故障诊断跟踪**—恢复在“服务器”列表框中选择的节点上服务的原始跟踪设置；同时显示为您可以选择的图标。

b) 仅 Unified Communications Manager 和 IM and Presence 群集：**重置所有节点上的故障诊断跟踪**—恢复群集中所有节点上的服务的原始跟踪设置。

只有为一个或多个服务设置故障诊断跟踪后，“重置故障诊断跟踪”按钮才会显示。

注释 长时间启用故障诊断跟踪会增加跟踪文件的大小，并且可能会影响服务的性能。

选择**重置**按钮后，窗口将会刷新，服务复选框将显示为未选中状态。

第 18 章

查看使用记录

使用记录概述

Cisco Unified Communications Manager 提供各种记录，您可以查看配置的项目如何在您的系统中使用。 配置的项目包括设备，以及系统级设置，例如设备池、日期和时间组，以及路由计划。

从属关系记录

使用从属关系记录用于以下用途：

- 查找关于系统级设置的信息，例如服务器、设备池以及日期和时间组。
- 确定数据库中使用其他记录的记录。 例如，您可以确定哪些设备（例如 CTI 路由点或电话）使用特定的呼叫搜索空间。
- 在删除任何记录之前显示记录之间的从属关系。 例如，删除分区之前，使用从属关系记录可查看哪些呼叫搜索空间 (CSS) 和设备与之关联。 然后，您可以重新配置设置以删除从属关系。

路由计划报告

使用路由计划报告，您可以查看在系统中配置的号码、路由以及模式的部分或完整列表。 当生成报告时，您可以通过单击报告中“模式/目录号码”、“分区”或“路由详细信息”列中的条目，访问每个项目的配置窗口。

此外，路由计划报告还可让您将报告数据保存到可以导入其他应用程序的 .CSV 文件中。 .CSV 文件包含的信息比网页更详细，其中包括电话的目录号码、路由模式、模式的使用、设备名称以及设备说明。

Cisco Unified Communications Manager 使用路由计划来路由内部呼叫和外部公共交换电话网 (PSTN) 呼叫。 由于在您的网络中可能有多个记录，借助 Cisco Unified Communications Manager 管理，您可以根据特定的条件查找特定的路由计划记录。

使用报告任务

过程

	命令或操作	目的
步骤 1	要查看路由计划记录并使用它们管理未分配的目录号码，请参阅以下程序： • 查看路由计划记录， 第 246 页 • 保存路由计划报告， 第 247 页 • 删除未分配的目录号码， 第 247 页 • 更新未分配的目录号码， 第 248 页	使用这些程序查找特定的路由计划记录，将记录保存在 .CSV 文件中，并管理未分配的目录号码。
步骤 2	要使用从属关系记录，请参阅以下程序： • 查看从属关系记录， 第 249 页	使用这些程序查找关于系统级设置的信息并显示数据库中记录之间的从属关系。

路由计划报告任务流程

过程

	命令或操作	目的
步骤 1	查看路由计划记录， 第 246 页.	查看路由计划记录并生成自定义的路由计划报告。
步骤 2	保存路由计划报告， 第 247 页.	查看 .csv 文件格式的路由计划报告。
步骤 3	删除未分配的目录号码， 第 247 页.	从路由计划报告中删除未分配的目录号码。
步骤 4	更新未分配的目录号码， 第 248 页.	从路由计划报告中更新未分配的目录号码的设置。

查看路由计划记录

本节介绍如何查看路由计划记录。 由于在您的网络中可能有多个记录，借助 Cisco Unified Communications Manager 管理，您可以根据特定的条件查找特定的路由计划记录。 按照以下程序生成自定义的路由计划报告。

过程

步骤 1 选择**呼叫路由** > **路由计划报告**。

步骤 2 要查找数据库中的所有记录，请确保对话框为空，并转至第 3 步。

要过滤或搜索记录

a) 从第一个下拉列表框中选择搜索参数。
b) 从第二个下拉列表框中选择搜索模式。
c) 如果适用，指定适当的搜索文本。

步骤 3 单击**查找**。

此时将显示所有相匹配的记录。 在“每页行数”下拉列表框中选择不同的值，可以更改每个页面中显示的项目数量。

步骤 4 从显示的记录列表中，单击要查看的记录的链接。

窗口中将显示您选择的项目。

保存路由计划报告

本节包含有关如何以 .csv 文件查看路由计划报告的信息。

过程

步骤 1 选择**呼叫路由** > **路由计划报告**。

步骤 2 从**路由计划报告**窗口的**相关链接**下拉列表中选择**以文件查看**，然后单击**转至**。

在出现的对话框中，可以保存文件或将其导入到另一个应用程序。

步骤 3 单击**保存**。

另一个窗口将会显示，可让您将此文件保存到选择的位置。

注释 您也可以将文件保存为另一个名称，但文件名必须包含 .CSV 扩展名。

步骤 4 选择文件保存位置，然后单击**保存**。 此操作应会将该文件保存到您指定的位置。

步骤 5 找到您刚才保存的 .CSV 文件，双击其图标即可查看。

删除未分配的目录号码

本节介绍如何从路由计划报告删除未分配的目录号码。 目录号码在 Cisco Unified Communications Manager 管理的“目录号码配置”窗口中配置和删除。 从删除的设备或电话中删除目录号码时，该目录号码在 Cisco Unified Communications Manager 数据库中仍然存在。 要从数据库中删除目录号码，请使用“路由计划报告”窗口。

过程

步骤 1 选择呼叫**呼叫路由** > **路由计划报告**。

步骤 2 在“路由计划报告”窗口中，使用三个下拉列表指定列出所有未分配目录号码的路由计划报告。

步骤 3 存在三种方式可删除目录号码：

a) 单击您要删除的目录号码。 显示“目录号码配置”窗口时，单击“删除”。

b) 选中您要删除的目录号码旁边的复选框。 单击“删除选定项”。

c) 要删除所有找到的未分配的目录号码，请单击“删除所有已找到的项”。

此时将显示警告消息，确认您要删除目录号码。

步骤 4 要删除目录号码，请单击“确定”。 要取消删除请求，请单击“取消”。

更新未分配的目录号码

本节介绍如何从路由计划报告更新未分配的目录号码的设置。 目录号码在Cisco Unified Communications Manager 管理的“目录号码配置”窗口中配置和删除。 目录号码从设备删除后，在 Cisco Unified Communications Manager 数据库中仍然存在。 要更新该目录号码的设置，请使用“路由计划报告”窗口。

过程

步骤 1 选择**呼叫路由** > **路由计划报告**。

步骤 2 在**路由计划报告**窗口中，使用三个下拉列表指定列出所有未分配目录号码的路由计划报告。

步骤 3 单击您要更新的目录号码。

注释 除了目录号码和分区之外，目录号码的所有其他设置都可以更新。

步骤 4 进行所需的更新，例如呼叫搜索空间或前转选项。

步骤 5 单击**保存**。

“目录号码配置”窗口将会重新显示，并且目录号码字段为空。

从属关系记录任务流程

过程

	命令或操作	目的
步骤 1	配置从属关系记录， 第 249 页.	使用此程序启用或禁用从属关系记录。 此程序以低于正常的优先级运行，并且由于拨号方案的大小和复杂程度、CPU 速度以及其他应用程序的 CPU 要求可能需要一段时间来完成。

	命令或操作	目的
步骤 2	查看从属关系记录，第 249 页.	启用从属关系记录后，您可以从界面上的配置窗口访问它们。

配置从属关系记录

使用从属关系记录查看 Cisco Unified Communications Manager 数据库中记录之间的关系。 例如，删除分区之前，使用从属关系记录可查看哪些呼叫搜索空间 (CSS) 和设备与之关联。

注意 从属关系记录会导致高CPU使用率。此程序以低于正常的优先级运行，并且由于拨号方案的大小和复杂程度、CPU 速度以及其他应用程序的 CPU 要求可能需要一段时间来完成。

如果您启用了从属关系记录并且您的系统遇到 CPU 使用率问题，您可以禁用从属关系记录。

过程

步骤 1 在Cisco Unified CM 管理中，选择**系统** > **企业参数**。

步骤 2 滚动至 **CCMAdmin 参数**部分，并从**启用从属关系记录**下拉列表中，选择以下选项之一：

- **真** — 启用从属关系记录。
- **假** — 禁用从属关系记录。

根据您选择的选项，将显示一个对话框及关于启用或禁用从属关系记录后果的消息。 请阅读该消息，然后再单击此对话框中的**确定**。

步骤 3 单击**确定**。

步骤 4 单击**保存**。

随即会出现更新成功消息，确认所作更改。

查看从属关系记录

启用从属关系记录后，您可以从界面上的配置窗口访问它们。

开始之前

配置从属关系记录，第 249 页

过程

步骤 1 从 Cisco Unified CM 管理中，导航到您要查看的记录的配置窗口。

示例：

要查看一个设备池的从属关系记录，请选择**系统** > **设备池**。

注释　无法从**设备默认值**和**企业参数配置**窗口中查看从属关系记录。

步骤 2 单击**查找**。

步骤 3 单击记录之一。
随即会出现配置窗口。

步骤 4 从**相关链接**列表框中，选择**从属关系记录**框，然后单击**转至**。

注释　如果您尚未启用从属关系记录，**从属关系记录摘要**窗口将显示一条消息，而不是关于记录的信息。

从属关系记录摘要窗口将出现，显示被数据库中其他记录使用的记录。

步骤 5 在此窗口中选择以下从属关系记录按钮之一：

- **刷新** — 以当前信息更新窗口。
- **关闭** — 关闭窗口而不返回您在其中单击“从属关系记录”链接的配置窗口。
- **关闭并返回** — 关闭窗口并返回您在其中单击“从属关系记录”链接的配置窗口。

第 19 章

管理企业参数

企业参数概述

企业参数提供适用于跨整个群集中所有设备和服务的默认设置。 例如，您的系统使用企业参数来设置其设备默认值的初始值。

您无法添加或删除企业参数，但可以更新现有的企业参数。 配置窗口会将企业参数列于类别下；例如，CCMAdmin 参数、CCMUser 参数和 CDR 参数。

您可以在**企业参数配置**窗口中查看企业参数的详细的说明。

注意 许多企业参数并不需要更改。但是，除非您完全了解要更改的功能，或者 Cisco 技术支持中心 (TAC) 建议您更改，否则请勿更改企业参数。

查看企业参数信息

通过**企业参数配置**窗口中的嵌入内容，访问有关企业参数的信息。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 请执行以下任务之一：

- 要查看特定企业参数的说明，请单击该参数的名称。
- 要查看所有企业参数的说明，请单击 **?**。

更新企业参数

使用此程序打开**企业参数配置**窗口并配置系统级设置。

注意 许多企业参数并不需要更改。但是，除非您完全了解要更改的功能，或者Cisco技术支持中心(TAC)建议您更改，否则请勿更改企业参数。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 为您想要更改的企业参数选择所需的值。

步骤 3 单击**保存**。

下一步做什么

将配置应用到设备，第 252 页

将配置应用到设备

使用此程序以利用您配置的设置更新群集中所有受影响的设备。

开始之前

更新企业参数，第 252 页

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 检验您的更改，然后单击**保存**。

步骤 3 选择下列选项之一：

- 如果您希望系统确定要重新启动哪些设备，请单击**应用配置**。 在某些情况下，设备可能无需重新启动。 正在进行的呼叫可能会掉线，但已接通的呼叫将被保留，除非设备池包含 SIP 干线。
- 如果想要重新启动群集中的所有设备，请单击**重置**。 我们建议您在非高峰时段执行此步骤。

步骤 4 阅读确认对话框后，单击**确定**。

恢复默认企业参数

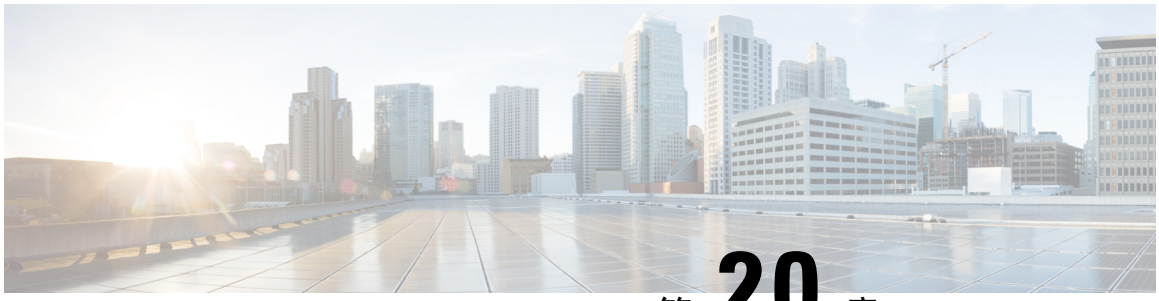
如果您要将企业参数重置为默认设置，请使用此程序。 某些企业参数包含建议的值，如配置窗口的列中所示；此程序使用这些值作为默认设置。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 单击**设置为默认值**。

步骤 3 阅读确认提示后，单击**确定**。



第 20 章

管理服务器

管理服务器概述

本章介绍如何管理 Cisco Unified Communications Manager 节点的属性、查看 Presence 服务器状态，以及为 Unified Communications Manager 服务器配置主机名。

删除服务器

本节介绍如何从 Cisco Unified Communications Manager 数据库删除服务器，以及如何将删除的服务器添加回 Cisco Unified Communications Manager 群集。

在 Cisco Unified Communications Manager 管理中，无法删除群集的第一个节点，但可以删除后续节点。 在“查找并列出服务器”窗口中删除后续节点之前，Cisco UnifiedCM 管理将显示以下消息：“您将要永久删除一台或多台服务器。 此操作无法撤消。 是否继续?”。 如果单击“确定”，该服务器将从 Cisco UnifiedCM 数据库删除，并且不可使用。

提示 尝试从“服务器配置”窗口中删除服务器时，将会出现类似于上一段所示的消息。 如果单击“确定”，该服务器将从 Cisco UnifiedCM 数据库删除，并且不可使用。

在删除服务器之前，请考虑以下信息：

- Cisco Unified Communications Manager 管理不允许删除群集的第一个节点，但可以删除任何后续节点。

- Cisco 建议不要删除其中正在运行 Cisco Unified Communications Manager 的节点，特别是该节点中注册了电话等设备时。
- 虽然后续节点存在从属关系记录，但这些记录不会阻止您删除节点。
- 如果为要删除的节点上的 Cisco Unified Communications Manager 配置了任何呼叫暂留号码，删除将会失败。 您必须在 Cisco Unified Communications Manager 管理中删除呼叫暂留号码，然后才能删除该节点。
- 如果 Cisco Unified Communications Manager 管理中的配置字段包含要删除的服务器的 IP 地址或主机名，请在删除该服务器之前更新配置。 如果不执行此任务，采用该配置的功能在您删除服务器后可能无法运作；例如，如果为服务参数、企业参数、服务URL、目录URL、IP电话服务等输入 IP 地址或主机名，则在删除服务器之前需更新此配置。
- 如果应用程序 GUI（例如 Cisco Unity、Cisco Unity Connection 等）包含要删除的服务器的 IP 地址或主机名，请在删除服务器之前更新相应GUI中的配置。 如果不执行此任务，采用该配置的功能在您删除服务器后可能无法运作。
- 当您删除服务器时，系统可能会自动删除某些设备，例如 MOH 服务器。
- 在删除节点之前，Cisco 建议停止后续节点上活动的服务。 执行此任务可确保服务在删除节点后能继续运作。
- 对服务器配置的更改在重新启动 Cisco Unified Communications Manager 后才会生效。 有关重新启动 Cisco CallManager 服务的信息，请参阅《*Cisco Unified* 功能配置管理指南》。
- 为确保数据库文件正确更新，在删除服务器、Presence 或应用程序服务器之后必须重新启动群集。
- 删除节点后，访问 Cisco Unified 报告以验证 Cisco Unified Communications Manager 是否已从群集中删除该节点。 此外，访问 Cisco Unified 报告、RTMT 或 CLI 以验证现有节点之前正在进行数据库复制；如有必要，使用 CLI 修复节点之间的数据库复制。

注释 从群集中删除订阅方节点后，其证书仍在发布方和其他节点中。管理员必须手动删除：

- 从各个群集成员的信任存储区中删除的订阅方节点的证书。
- 已删除订阅方节点的信任存储区中的各个其他群集成员的证书。

从群集删除 Unified Communications Manager 节点

此程序用于从群集删除 Cisco Unified Communications Manager 节点。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统** > **服务器**。

步骤 2 单击**查找**并选择要删除的节点。

步骤 3 单击**删除**。

步骤 4 当出现警告对话框，表明无法撤消此操作时，单击**确定**。

步骤 5 为您已取消分配的节点关闭主机 VM。

从群集中删除 IM and Presence 节点

如果您需要安全地将 IM and Presence Service 节点从其在线状态冗余组和群集中删除，请按照以下程序执行操作。

注意 删除节点会对 Presence 冗余组中其余节点上的用户造成服务中断。 只有在维护期间才能执行此过程。

过程

步骤 1 在 **Cisco Unified CM 管理** > **系统** > **Presence 冗余组**页面上，禁用高可用性（如果已启用）。

步骤 2 在 **Cisco Unified CM 管理** > **用户管理** > **分配 Presence 用户**页面上，取消分配所有用户，或者将所有用户移离您要删除的节点。

步骤 3 要将节点从其在线状态冗余组中删除，请从该在线状态冗余组的**在线状态冗余组配置**页面上的“在线状态服务器”下拉列表中选择**未选定**。 当出现警告对话框，表明由于取消分配该节点而将要重新启动 Presence 冗余组时，选择**确定**。

注释 您不能直接从在线状态冗余组删除发布方节点。 要删除发布方节点，首先从发布方节点取消分配用户，然后彻底删除在线状态冗余组。

不过，您可以将已删除的 IM and Presence 节点添加回群集中。 有关如何添加已删除节点的详细信息，请参阅将已删除的服务器重新添加到群集，第 258 页。 这种情况下，当在 Cisco Unified CM 管理控制台的**系统** > **服务器**屏幕将删除的发布方节点添加回服务器时，系统会自动创建 **DefaultCUPSubcluster**。

步骤 4 在 Cisco Unified CM 管理中，从**系统** > **服务器**删除已取消分配的节点。 当出现警告对话框，表明无法撤消此操作时，单击**确定**。

步骤 5 为您已取消分配的节点关闭主机 VM 或服务器。

步骤 6 在所有节点上重新启动 **Cisco XCP 路由器**。

将已删除的服务器重新添加到群集

如果从 Cisco Unified Communications Manager 管理中删除了某个后续节点（订阅方），又想将其重新添加到群集中，请执行以下程序。

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择**系统** > **服务器**来添加服务器。

步骤 2 将后续节点添加到 Cisco Unified Communications Manager 管理后，使用 Cisco 在适用于您版本的软件包中提供的磁盘在服务器上执行安装。

提示 确保您安装的版本与发布方节点上运行的版本相匹配。 如果发布方上运行的版本与安装文件不匹配，请在安装过程中选择“安装期间升级”选项。有关详细信息，请参阅《*Cisco Unified Communications Manager* 和 *IM and Presence Service* 安装指南》。

步骤 3 安装 Cisco Unified CM 后，按照支持您的 Cisco Unified CM 版本的安装文档配置后续节点。

步骤 4 访问 Cisco Unified Reporting、RTMT 或 CLI，以确认现有节点之间发生了数据库复制；如有必要，可以修复节点之间的数据库复制。

安装前将节点添加到群集

在安装节点之前，使用 Cisco Unified Communications Manager 管理将新节点添加到群集。添加节点时您选择的服务器类型必须匹配您安装的服务器类型。

安装新节点之前，您必须使用 Cisco Unified Communications Manager 管理在第一个节点中配置新节点。要在群集上安装节点，请参阅《*Cisco Unified Communications Manager* 安装指南》。

对于 Cisco Unified Communications Manager 视频/语音服务器，您在 Cisco Unified Communications Manager 软件初始安装期间添加的第一台服务器指定为发布方节点。所有后续服务器安装或添加都指定为订阅方节点。您添加到群集的第一个 Cisco Unified Communications Manager IM and Presence 节点指定为 IM and Presence Service 据库发布方节点。

注释 您无法使用 Cisco Unified Communications Manager 管理在服务器添加后更改服务器类型。您必须删除现有的服务器实例，然后再次添加新服务器并选择正确的服务器类型设置。

过程

步骤 1 选择**系统** > **服务器**。

此时将显示**查找并列出服务器**窗口。

步骤 2 单击**新增**。

此时将显示**服务器配置 - 添加服务器**窗口。

步骤 3 从**服务器类型**下拉列表框中，选择您要添加的服务器类型，然后单击**下一步**。

- CUCM 视频/语音
- CUCM IM and Presence

步骤 4 在**服务器配置**窗口中，输入相应的服务器设置。

有关服务器配置字段说明，请参阅服务器设置。

步骤 5 单击**保存**。

查看 Presence 服务器状态

使用 Cisco Unified Communications Manager 管理查看 IM and Presence Service 节点的关键服务的状态以及自我诊断测试结果。

过程

步骤 1 选择**系统** > **服务器**。

此时将显示**查找并列出服务器**窗口。

步骤 2 选择服务器搜索参数，然后单击**查找**。

屏幕上将显示相匹配的记录。

步骤 3 选择**查找并列出服务器**窗口中列出的 IM and Presence 服务器。

此时将显示**服务器配置**窗口。

步骤 4 单击**服务器配置**窗口的“IM and Presence 服务器信息”部分中的“Presence 服务器状态”链接。

此时将显示服务器的**节点详细信息**窗口。

配置端口

请遵照此程序来更改用于连接（例如 SCCP 设备注册、SIP 设备注册和 MGCP 网关连接）的端口设置。

注释 正常情况下，您无需更改默认端口设置。 仅当您确实想更改默认值时才执行此程序。

过程

步骤 1 从 Cisco Unified Communications Manager 管理中，选择**系统** > **Cisco Unified CM**。
此时将显示**查找并列出 Cisco Unified CM** 窗口。

步骤 2 输入适当的搜索条件，然后单击**查找**。
此时将显示所有匹配的 Cisco Unified Communications Manager。

步骤 3 选择要查看的 **Cisco Unified CM**。
此时将显示 **Cisco Unified CM 配置**窗口。

步骤 4 导航到**此服务器的 Cisco Unified Communications Manager TCP 端口设置**部分。

步骤 5 配置 Cisco Unified Communications Manager 的端口设置。

请参阅端口设置，第 260 页，了解有关字段及其配置选项的信息。

步骤 6 单击**保存**。

步骤 7 单击**应用配置**。

步骤 8 单击**确定**。

端口设置

字段	说明
以太网电话端口	系统使用此 TCP 端口与网络上的 Cisco Unified IP 电话（仅 SCCP）通信。 • 除非默认端口已在系统中使用，否则请接受默认端口值 2000。 选择 2000 会将此端口标识为非安全。 • 确保所有端口条目唯一。 • 有效的端口号范围从 1024 到 49151。
MGCP 侦听端口	系统使用此 TCP 端口检测来自其关联 MGCP 网关的消息。 • 除非默认端口已在系统中使用，否则请接受默认端口 2427。 • 确保所有端口条目唯一。 • 有效的端口号范围从 1024 到 49151。

字段	说明
MGCP Keep-alive 端口	系统使用此 TCP 端口与其关联的 MGCP 网关交换保持传输消息。 • 除非默认端口已在系统中使用，否则请接受默认端口 2428。 • 确保所有端口条目唯一。 • 有效的端口号范围从 1024 到 49151。
SIP 电话端口	此字段指定 Unified Communications Manager 用来通过 TCP 和 UDP 侦听 SIP 线路注册的端口号。
SIP 电话安全端口	此字段指定系统用来通过 TLS 侦听 SIP 线路注册的端口号。
SIP 电话 OAuth 端口	此字段指定 Cisco Unified Communications Manager 用于通过 TLS（传输层安全）从 Jabber 内部部署设备侦听 SIP 线路注册的端口号。 默认值为 5090。范围为 1024 至 49151。
SIP 移动和远程访问 OAuth 端口	此字段指定 Cisco Unified Communications Manager 用于通过 MTLS（双向传输层安全性）从利用 Expressway 连接的 Jabber 侦听 SIP 线路注册的端口号。 默认值为 5091。范围为 1024 至 49151。

主机名配置

下表列出您可以为 Unified Communications Manager 服务器配置主机名的地方，允许主机名使用的字符数量以及建议主机名使用的第一个和最后一个字符。请注意，如果您没有正确配置主机名，Unified Communications Manager 中的部分组件，例如操作系统、数据库、安装等组件可能无法按预期工作。

表 *74: Cisco Unified Communications Manager* 中的主机名配置

主机名位置	允许的配置	允许的字符数	建议主机名使用的第一个字符	建议主机名使用的最后一个字符
主机名/IP 地址字段 **Cisco Unified Communications Manager 管理中的系统 > 服务器**	您可以添加或更改群集中服务器的主机名。	2-63	字母	字母数字
主机名字段 Cisco Unified Communications Manager 安装向导	您可以添加群集中服务器的主机名。	1-63	字母	字母数字
主机名字段 **Cisco Unified Communications 操作系统中的设置 > IP > 以太网**	您可以更改，但不能添加群集中服务器的主机名。	1-63	字母	字母数字

主机名位置	允许的配置	允许的字符数	建议主机名使用的第一个字符	建议主机名使用的最后一个字符
设置网络主机名 主机名 命令行界面	您可以更改，但不能添加群集中服务器的主机名。	1-63	字母	字母数字

提示 主机名必须遵循 ARPANET 主机名的规则。 在主机名的第一个和最后一个字符之间，您可以输入字母数字字符和连字符。

在任何位置配置主机名之前，请回顾以下信息：

- “服务器配置”窗口中的“主机名/IP 字段”支持设备到服务器、应用程序到服务器和服务器到服务器通信，允许您输入点分十进制格式的 IPv4 地址或主机名。

  您在安装 Unified Communications Manager 发布方节点后，发布方的主机名将自动显示在此字段中。 您在安装 Unified Communications Manager 订户节点之前，在 Unified Communications Manager 发布方节点上的此字段中输入订户节点的 IP 地址或主机名。

  在此字段中，只有 Unified Communications Manager 可以访问 DNS 服务器以将主机名解析为 IP 地址时，才可配置主机名，确保您在 DNS 服务器上配置 Cisco Unified Communications Manager 名称和地址信息。

提示 除了在 DNS 服务器上配置 Unified Communications Manager 信息外，您可以在 Cisco Unified Communications Manager 安装期间输入 DNS 信息。

- 在安装 Unified Communications Manager 发布方节点期间，您输入发布方节点的主机名（必填）和 IP 地址，以配置网络信息，假如您想使用静态网络。

  安装 Unified Communications Manager 订户节点期间，您输入 Unified Communications Manager 发布方节点的主机名和 IP 地址，以便 Unified Communications Manager 可以验证网络连通性和发布方-订户验证。 此外，您必须输入订户节点的主机名和 IP 地址。 当 Unified Communications Manager 安装提示您输入订户服务器的主机名时，输入显示在 Cisco Unified Communications Manager 管理中的“服务器配置”窗口中的值，假如您在“主机名/IP 地址”字段配置订户服务器的主机名。

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，第 264 页

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。 触发此警报时，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和端口信息以发送电子邮件警报。

c) （可选）选中**启用 TLS 模式**复选框，以便启用到 SMTP 服务器的加密通信通道。

d) （可选）选中**启用身份验证模式**复选框以要求对收件人的电子邮件地址进行身份验证。

注释 只有选中了**启用身份验证模式**复选框才能访问**用户名**和**密码**字段。

e) 在**用户名**字段中输入用户名。

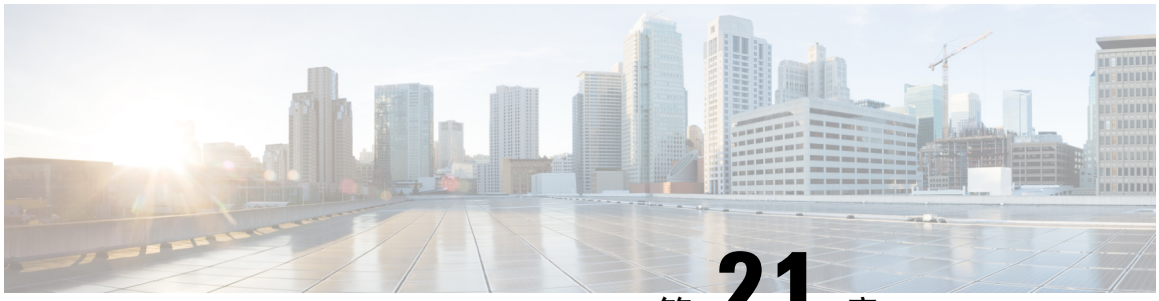
f) 在**密码**字段中输入密码。

g) 输入**发送用户 Id**。

h) 单击**确定**。

第 V 部分

管理报告



第 21 章

Cisco 功能配置报告程序

功能配置报告存档

Cisco 功能配置报告程序服务会生成每日报告，其中包含显示该特定报告统计信息摘要的图表。 报告程序基于记录的信息每天一次生成报告。

使用功能配置 GUI，通过**工具** > **功能配置报告存档**查看报告。 必须先激活 Cisco 功能配置报告程序服务，然后才能查看报告。 当您激活该服务后，报告生成可能需要长达 24 小时时间。

报告中包含前一天 24 小时的数据。 添加到报告名称的后缀将显示报告程序生成报告的日期；例如 AlertRep_mm_dd_yyyy.pdf。 “功能配置报告存档”窗口使用此日期仅显示相关日期的报告。 报告从日志文件中的数据生成，并带有前一天的时间戳。 系统会考虑当前日期和前两天的日志文件来收集数据。

报告中所示的时间反映服务器“系统时间”。

您可以在生成报告时从服务器检索日志文件。

注释 Cisco Unified 报告 Web 应用程序将数据的快照视图提供到一个输出中，然后运行数据检查。 您还可以通过应用程序将生成的报告存档。 有关详细信息，请参阅《*Cisco Unified* 报告管理指南》。

群集配置的功能配置报告存档注意事项

本节仅适用于 Unified Communications Manager 和 IM and Presence Service。

- 因为 Cisco 功能配置报告程序只在第一台服务器上活动，所以在任何时候，报告程序只会在第一台服务器上生成报告，而不会在其他服务器上生成报告。
- 报告中所示的时间反映第一台服务器的“系统时间”。 如果第一台服务器和后续服务器位于不同的时区，报告中将显示第一台服务器的“系统时间”。

- 为报告收集数据时，会考虑群集中服务器位置之间的时区差异。
- 生成报告时，您可以从单台服务器或群集中的所有服务器选择日志文件。
- Cisco Unified 报告 Web 应用程序输出和数据检查涵盖来自所有可访问服务器的群集数据。

Cisco 功能配置报告程序配置任务流程

完成这些任务以通过 Cisco 功能配置报告程序设置每日系统报告。

过程

	命令或操作	目的
步骤 1	激活 Cisco 功能配置报告程序，第 270 页	要生成每日报告，**Cisco 功能配置报告程序**服务必须运行。
步骤 2	配置 Cisco 功能配置报告程序设置，第 270 页	配置 Cisco 功能配置报告程序的安排设置。
步骤 3	查看每日报告存档，第 271 页	在系统生成每日报告后，请执行此任务以查看 PDF 格式的每日报告。

激活 Cisco 功能配置报告程序

执行此程序可使用 **Cisco 功能配置报告程序**打开每日系统报告。 要生成报告，必须**激活**该服务。

过程

步骤 1 从 Cisco Unified 功能配置中，选择**工具** > **服务激活**。
步骤 2 选择**服务器**并单击**前往**。
步骤 3 在**性能和监控服务**下，检查 **Cisco 功能配置报告程序**服务的状态。
步骤 4 如果服务已禁用，选中相邻的单选按钮，然后单击**保存**。

注释 每天生成报告。 最多可能需要 24 小时来生成第一份报告。

配置 Cisco 功能配置报告程序设置

配置 Cisco 功能配置报告程序生成的每日报告的安排设置。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统** > **服务参数**。

步骤 2 选择在其上运行 Cisco 功能配置报告程序的**服务器**。

步骤 3 从**服务**下拉列表中选择 Cisco 功能配置报告程序。

步骤 4 配置以下服务参数的设置：

- **RTMT 报告程序指定节点**—指定运行 RTMT 报告程序的指定节点。 Cisco 建议您分配非呼叫处理节点。
- **报告生成时间**—午夜之后生成报告的分钟数。 范围为 0 到 1439，默认设置为 30 分钟。
- **报告删除时间**—报告保存在磁盘上的天数。 范围为 0-30，默认设置为 7 天。

步骤 5 单击**保存**。

查看每日报告存档

Cisco Serviceability Reporter 生成每日报告后，可遵照此程序查看 PDF 格式的报告。

过程

步骤 1 选择**工具** > **功能配置报告存档**。

步骤 2 选择报告涵盖的月份和年份。
此时将显示对应该月份的日期列表。

步骤 3 单击所生成的报告涵盖的日期。

步骤 4 单击要查看的报告。

注释 要查看 PDF 报告，必须在您的机器上安装 Acrobat Reader。 您可以单击**功能配置报告存档**窗口底部的链接下载 Acrobat Reader。

每日报告概要

Cisco 功能配置报告程序每天会生成以下系统报告：

- 设备统计信息报告
- 服务器统计信息报告
- 服务统计信息报告
- 呼叫活动报告

- 警告摘要报告
- 性能保护报告

设备统计信息报告

设备统计信息报告不适用于 IM and Presence Service 和 Cisco Unity Connection。

设备统计信息报告提供以下折线图：

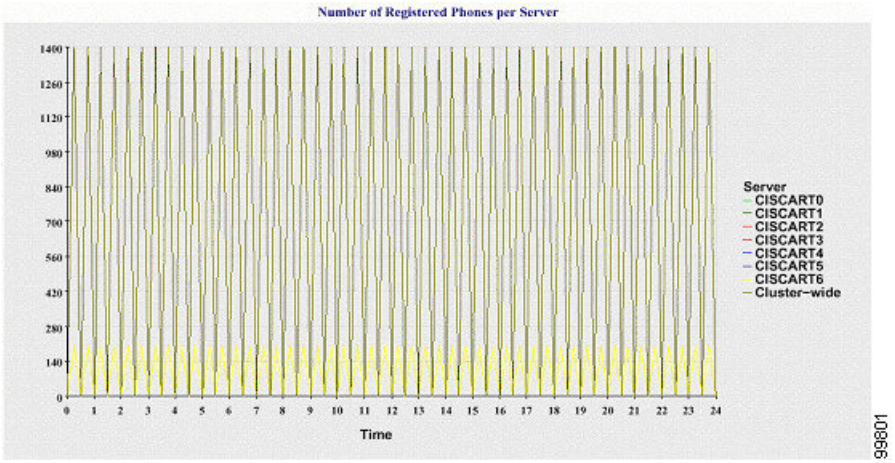
- 每台服务器的注册电话数
- 群集中的 H.323 网关数
- 群集中的干线数

每台服务器的注册电话数

折线图显示每台 Unified Communications Manager 服务器（和 Unified Communications Manager 群集配置中的群集）的注册电话数。 图表中的每条折线代表数据可用的服务器的数据，还有一条额外的折线显示群集范围的数据（仅 Unified Communications Manager 群集）。 图表中的每个数据值表示在 15 分钟持续时间内注册的平均电话数。 如果服务器不显示任何数据，报告程序不会生成代表该服务器的折线。 如果没有服务器（或 Unified Communications Manager 群集配置中的所有服务器）数据，则对于注册的电话，报告程序不会生成图表。 此时屏幕上会显示一条消息：“没有可用于设备统计信息报告的数据”。

图 *4:* 描绘每台服务器的注册电话数的折线图

下图所示为一个折线图示例，表示 Unified Communications Manager 群集配置中每台 Unified Communications Manager 服务器的注册电话数。



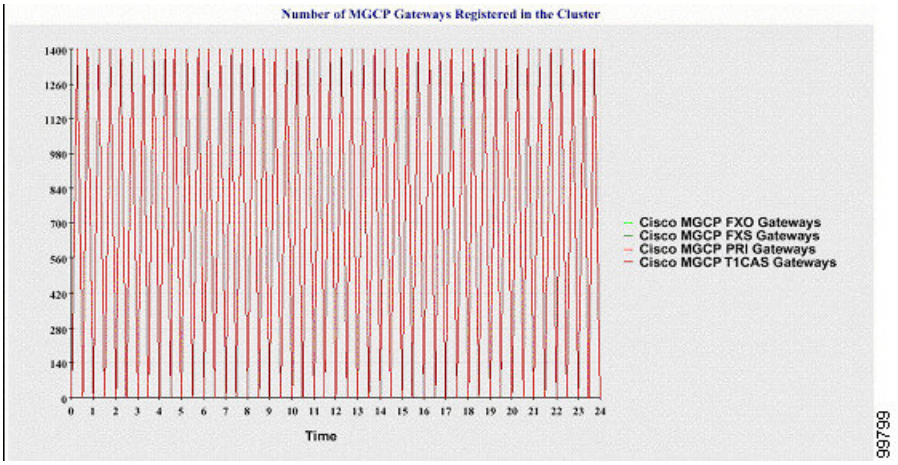
群集中注册的 MGCP 网关数

会有一幅折线图显示注册的 MGCP FXO、FXS、PRI 和 T1CAS 网关数。 每条折线只代表 Unified Communications Manager 服务器（或 Unified Communications Manager 群集配置中的群集）的数据；

因此，四条折线显示了每个网关类型的服务器（或群集范围）详细信息。 图表中的每个数据值表示在 15 分钟持续时间内注册的平均 MGCP 网关数。 如果不存在服务器（或群集中的所有服务器）的网关数据，报告程序不会生成代表该特定网关数据的折线。 如果不存在服务器（或群集中的所有服务器）的所有网关的数据，则报告程序不会生成图表。

图 *5:* 描绘每个群集的注册网关数的折线图

下图所示为一个折线图，表示 Unified Communications Manager 群集配置中每个群集的注册网关数。

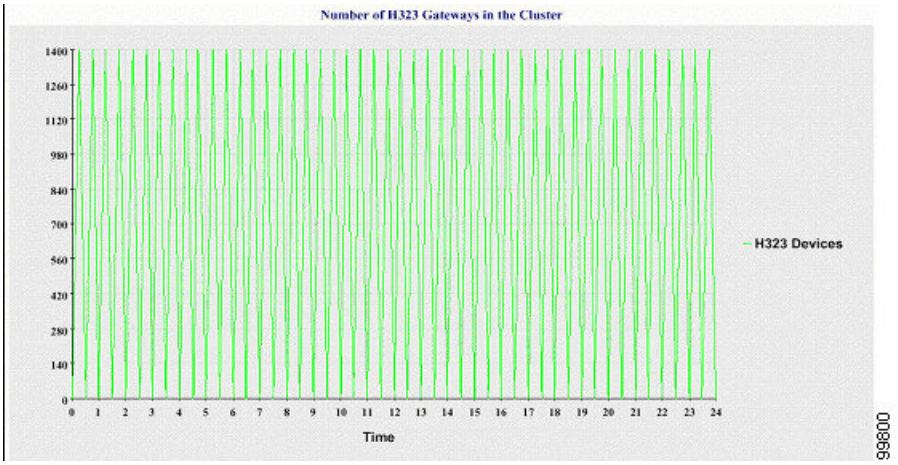


群集中的 H.323 网关数

会有一幅折线图显示 H.323 网关的数量。 一条折线代表 H.323 网关的详细信息（或 Unified Communications Manager 群集配置中的群集范围详细信息）。 图表中的每个数据值表示 15 分钟持续时间内注册的平均 H.323 网关数。 如果不存在服务器（或群集中的所有服务器）的 H.323 网关数据，报告程序不会生成图表。

图 *6:* 描绘每个群集的注册 *H.323* 网关数的折线图

下图所示为一个折线图示例，表示 Unified Communications Manager 群集配置中每个群集的 H.323 网关数。

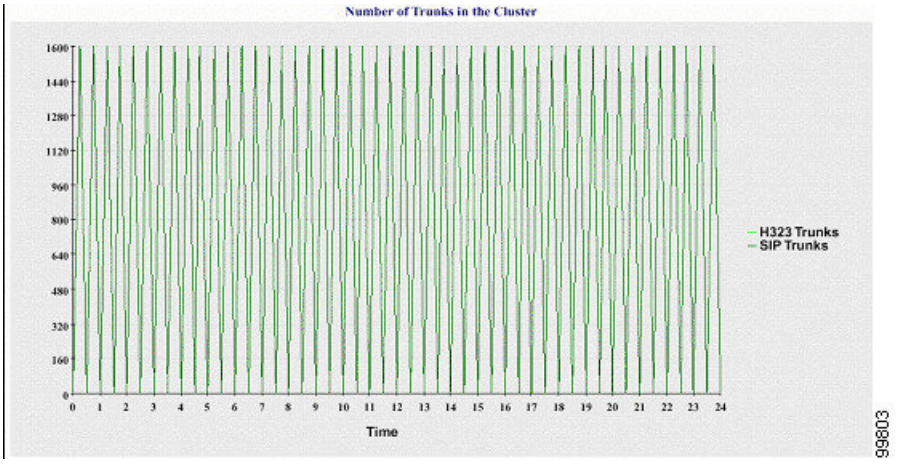


群集中的干线数

会有一幅折线图显示 H.323 和 SIP 干线的数量。 两条折线代表 H.323 干线和 SIP 干线（或 Unified Communications Manager 群集配置中的群集范围详细信息）的详细信息。 图表中的每个数据值表示 15 分钟持续时间内的平均 H.323 和 SIP 干线数。 如果不存在服务器（或群集中的所有服务器）的 H.323 干线数据，报告程序不会生成代表 H.323 干线数据的折线。 如果不存在服务器（或群集中的所有服务器）的 SIP 干线数据，报告程序不会生成代表 SIP 干线数据的折线。 如果没有干线数据，则报告程序不会生成图表。

图 *7:* 描绘每个群集的干线数的折线图

下图所示为一个折线图示例，表示 Unified Communications Manager 群集配置中每个群集的干线数。



服务器（或群集中的每台服务器）包含文件名采用以下命名模式的日志文件：DeviceLog_mm_dd_yyyy_hh_mm.csv。 日志文件中包含以下信息：

- 服务器（或 Unified Communications Manager 群集的每台服务器）上的注册电话数
- 服务器（或 Unified Communications Manager 群集的每台服务器）上的注册 MGCP FXO、FXS、PRI 和 T1CAS 网关数
- 服务器（或 Unified Communications Manager 群集的每台服务器）上的注册 H.323 网关数
- SIP 干线和 H.323 干线的数量

服务器统计信息报告

服务器统计信息报告提供以下折线图：

- 每台服务器的 CPU 百分比
- 每台服务器的内存使用量百分比
- 每台服务器最大分区的硬盘使用量百分比

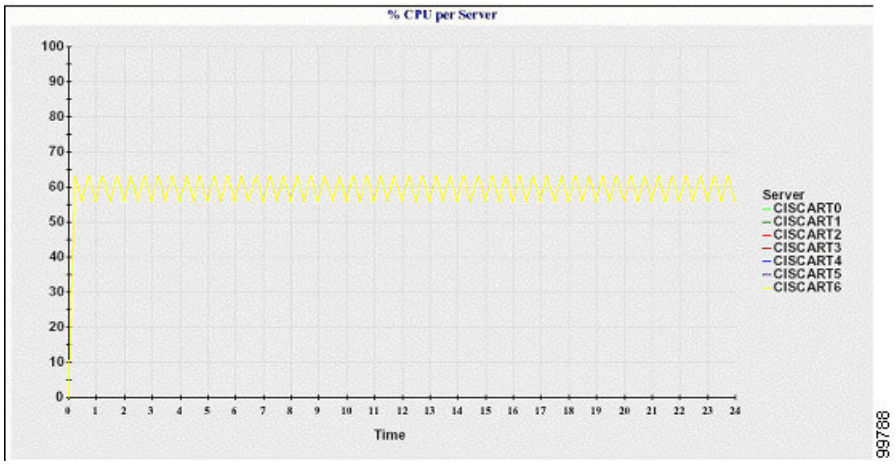
仅 Unified Communications Manager 和 IM and Presence Service 支持群集特定的统计信息。

每台服务器的 CPU 百分比

会有一幅折线图显示服务器（或群集中的每台服务器）的CPU使用量百分比。图表中的折线表示数据可用的服务器（或群集中每台服务器的一条线路）的数据。 图表中的每个数据值表示 15 分钟持续时间内的CPU平均使用量。如果不存在服务器（或群集中的任何一台服务器）的数据，则报告程序不会生成代表该服务器的折线。如果没有要生成的折线，报告程序将不会创建图表。此时屏幕上会显示一条消息：“没有可用于服务器统计信息报告的数据”。

图 *8*: 描绘每台服务器的 *CPU* 百分比的折线图

下图所示为一个折线图示例，表示 Unified Communications Manager 群集配置中每台服务器的 CPU 使用量百分比。

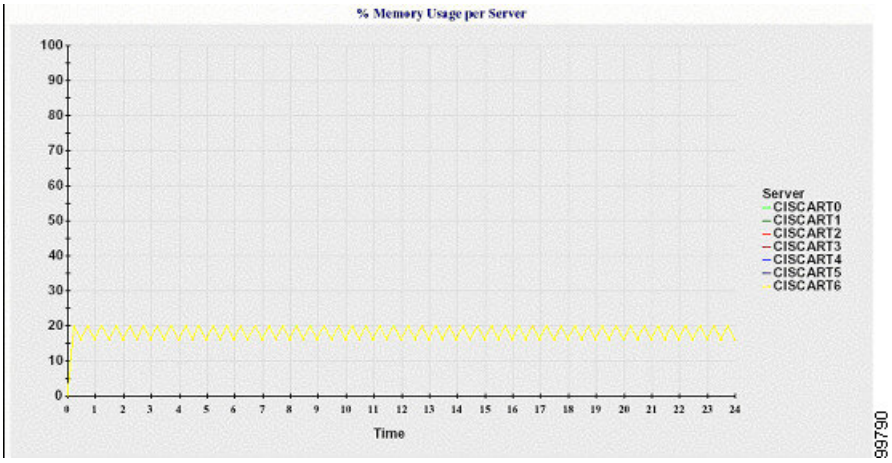


每台服务器的内存使用量百分比

会有一幅折线图显示 Unified Communications Manager 服务器的内存使用量百分比 (%MemoryInUse)。在 Unified Communications Manager 群集配置中，群集中数据可用的每台服务器都有一条对应的折线。 图表中的每个数据值表示 15 分钟持续时间内的内存平均使用量。 如果没有数据，则报告程序不会生成图表。 如果没有群集配置中的任何服务器的数据，则报告程序不会生成代表该服务器的折线。

图 *9*: 描绘每台服务器内存使用量百分比的折线图

下图所示为一个折线图示例，表示群集配置中每台 Unified Communications Manager 服务器的内存使用量百分比。

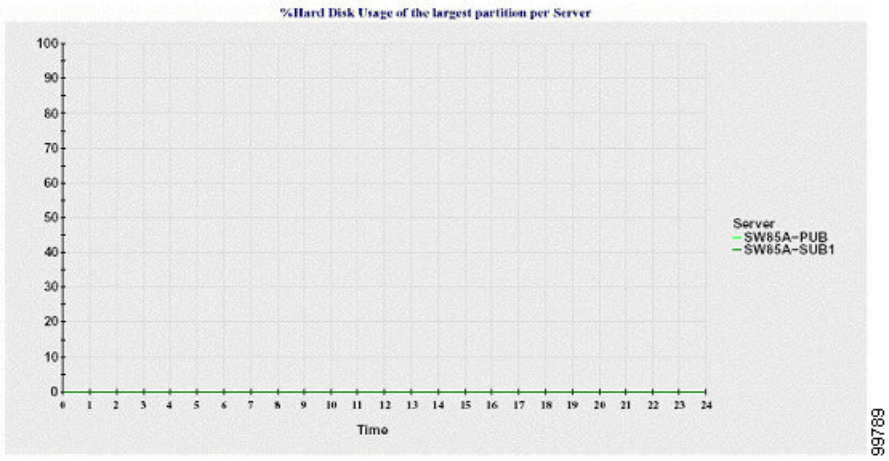


每台服务器最大分区的硬盘使用量百分比

会有一幅折线图显示服务器（或群集配置中每台服务器）上最大分区的磁盘空间使用量百分比 (%DiskSpaceInUse)。 图表中的每个数据值表示 15 分钟持续时间内的磁盘平均使用量。 如果没有数据，则报告程序不会生成图表。 如果没有群集配置中的任何服务器的数据，则报告程序不会生成代表该服务器的折线。

图 *10*: 绘制每台服务器最大分区的硬盘使用量百分比的折线图

下图所示为一个折线图示例，表示 Unified Communications Manager 群集配置中每台服务器最大分区的硬盘使用量百分比。



服务器（或群集配置中的每台服务器）包含文件名采用以下命名模式的日志文件：ServerLog_mm_dd_yyyy_hh_mm.csv。 日志文件中包含以下信息：

- 服务器（或群集中的每台服务器）上的 CPU 使用量百分比
- 服务器（或群集中的每台服务器）上的内存使用量百分比 (%MemoryInUse)
- 服务器（或群集中的每台服务器）上的最大分区硬盘使用量百分比 (%DiskSpaceInUse)

服务统计信息报告

服务统计信息报告不支持 IM and Presence Service 和 Cisco Unity Connection。

服务统计信息报告提供以下折线图：

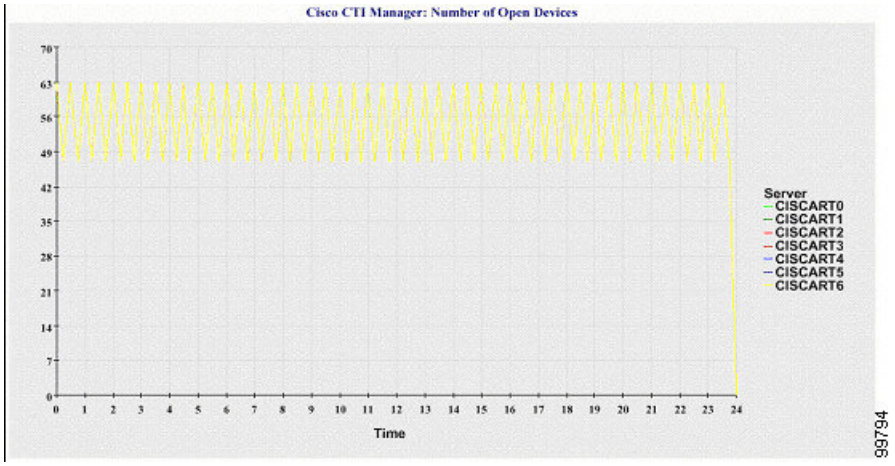
- Cisco CTI Manager：打开的设备数
- Cisco CTI Manager：打开的线路数
- Cisco TFTP：请求数
- Cisco TFTP：放弃的请求数

Cisco CTI Manager：打开的设备数

会有一幅折线图显示 CTI Manager（或 Unified Communications Manager 群集配置中的每个 CTI Manager）的 CTI 打开设备数。 每幅折线图对应激活服务的服务器（或 Unified Communications Manager 群集中的每台服务器）上的数据。 图表中的每个数据值表示 15 分钟持续时间内的 CTI 打开设备平均数。 如果没有数据，则报告程序不会生成图表。 如果没有 Unified Communications Manager 群集配置中的任何服务器的数据，则报告程序不会生成代表该服务器的折线。 此时屏幕上会显示一条消息：“没有可用于服务统计信息报告的数据”。

图 *11:* 描绘 *Cisco CTI Manager* 的折线图：打开的设备数

下图所示为一个折线图示例，表示 Unified Communications Manager 群集配置中每个 Cisco CTI Manager 的打开设备数。

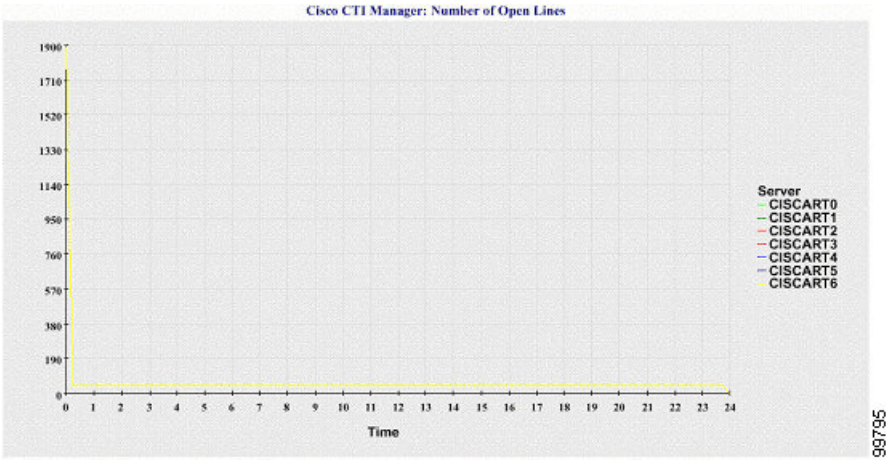


Cisco CTI Manager：打开的线路数

会有一幅折线图显示 CTI Manager（或 Unified Communications Manager 群集配置中的每个 CTI Manager）的 CTI 打开线路数。 图表中的折线对应激活 Cisco CTI Manager 服务的服务器（或 Unified Communications Manager 群集配置中每台服务器的一条线路）的数据。 图表中的每个数据值表示 15 分钟持续时间内的 CTI 打开线路平均数。 如果没有数据，则报告程序不会生成图表。 如果没有 Unified Communications Manager 群集配置中的任何服务器的数据，则报告程序不会生成代表该服务器的折线。

图 *12:* 描绘 ***Cisco CTI Manager*** 的折线图：打开的线路数

下图所示为一个折线图示例，表示 Unified Communications Manager 群集配置中每个 Cisco CTI Manager 的打开线路数。

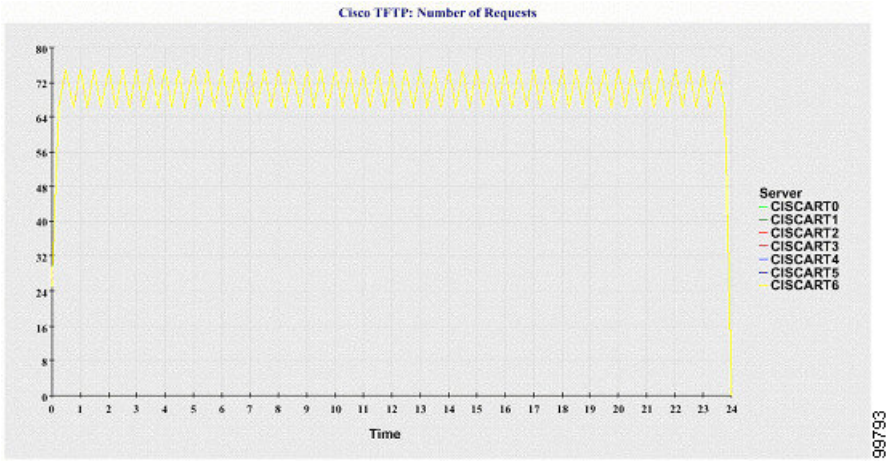


Cisco TFTP：请求数

会有一幅折线图显示 TFTP 服务器（或 Unified Communications Manager 群集配置中的每台 TFTP 服务器）的 Cisco TFTP 请求数。 图表中的折线对应激活 Cisco TFTP 服务的服务器（或 Unified Communications Manager 群集中每台服务器的一条线路）的数据。 图表中的每个数据值表示 15 分钟持续时间内的 TFTP 请求平均数。 如果没有数据，则报告程序不会生成图表。 如果没有 Unified Communications Manager 群集配置中的任何服务器的数据，则报告程序不会生成代表该服务器的折线。

图 *13:* 描绘 ***Cisco TFTP*** 的折线图：请求数

下图所示为一个折线图示例，表示每台 TFTP 服务器的 Cisco TFTP 请求数。



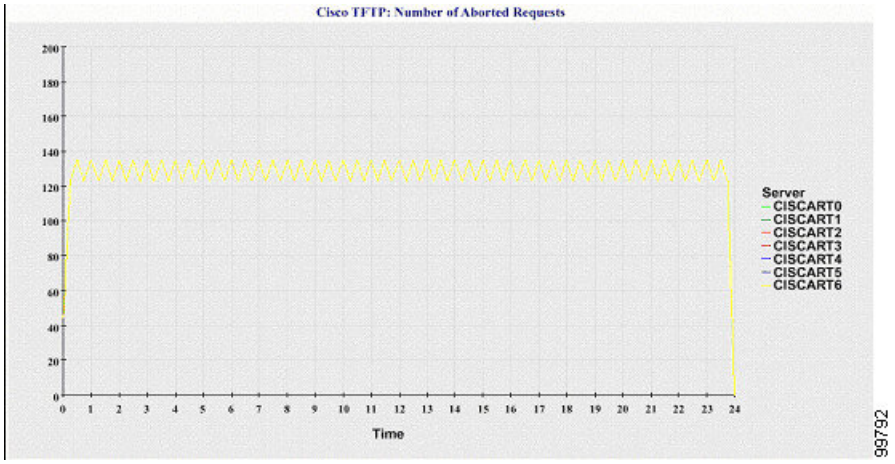
Cisco TFTP：放弃的请求数

会有一幅折线图显示 TFTP 服务器（或 Unified Communications Manager 群集配置中的每台 TFTP 服务器）放弃的 Cisco TFTP 请求数。 图表中的折线对应激活 Cisco TFTP 服务的服务器（或 Unified

Communications Manager 群集中每台服务器的一条线路）的数据。 图表中的每个数据值表示 15 分钟持续时间内放弃的 TFTP 请求平均数。 如果没有数据，则报告程序不会生成图表。 如果没有 Unified Communications Manager 群集配置中的任何服务器的数据，则报告程序不会生成代表该服务器的折线。

图 *14:* 描绘 *Cisco TFTP* 的折线图：放弃的请求数

下图所示为一个折线图示例，表示每台 TFTP 服务器放弃的 Cisco TFTP 请求数。



服务器（或 Unified Communications Manager 群集配置中的每台服务器）包含文件名采用以下命名模式的日志文件：ServiceLog_mm_dd_yyyy_hh_mm.csv。 日志文件中包含以下信息：

- 对于每个 CTI Manager - 打开的设备数
- 对于每个 CTI Manager - 打开的线路数
- 对于每台 Cisco TFTP 服务器 - Tftp 请求总数
- 对于每台 Cisco TFTP 服务器 - 放弃的 Tftp 请求总数

呼叫活动报告

呼叫活动报告不支持 IM and Presence Service 和 Cisco Unity Connection。

呼叫活动报告提供以下折线图：

- 群集的 Unified Communications Manager 呼叫活动
- 群集的 H.323 网关呼叫活动
- 群集的 MGCP 网关呼叫活动
- MGCP 网关
- 群集的干线呼叫活动

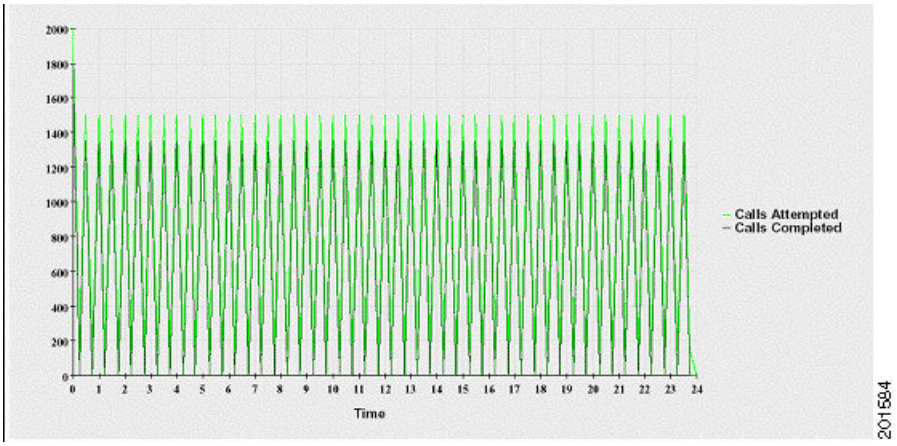
群集的 Cisco Unified Communications Manager 呼叫活动

会有一幅折线图显示尝试和完成的 Unified Communications Manager 呼叫数。 在 Unified Communications Manager 群集配置中，折线图显示整个群集中尝试和完成的呼叫数。 图表中包含两条折线，一条对应尝试的呼叫数，另一条对应完成的呼叫数。 对于 Unified Communications Manager 群集配置，每条折线代表群集值，即群集中所有服务器（数据可用）的值之和。 图表中的每个数据值表示已尝试的呼叫总数或 15 分钟持续时间内完成的呼叫数。

如果没有已完成 Unified Communications Manager 呼叫的数据，则报告程序不会生成代表已完成呼叫的数据的折线。 如果没有已尝试 Unified Communications Manager 呼叫的数据，则报告程序不会生成代表已尝试呼叫的数据的折线。 在 Unified Communications Manager 群集配置中，如果不存在群集中服务器的数据，报告程序不会生成代表该服务器上尝试或完成的呼叫的折线。 如果不存在任何 Unified Communications Manager 呼叫活动数据，则报告程序不会生成图表。 此时屏幕上会显示一条消息：“没有可用于呼叫活动报告的数据”。

图 *15:* 描绘群集 *Cisco Unified Communications Manager* 呼叫活动的折线图

以下折线图所示为 Unified Communications Manager 群集尝试和完成的呼叫数。

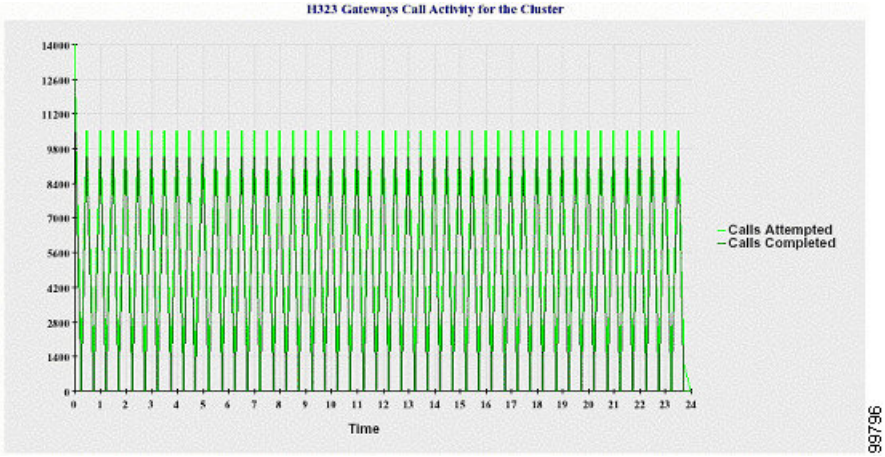


群集的 H.323 网关呼叫活动

会有一幅折线图显示 H.323 网关尝试和完成的呼叫数。 在 Unified Communications Manager 群集配置中，折线图显示整个群集中尝试和完成的呼叫数。 图表中包含两条折线，一条对应尝试的呼叫数，另一条对应完成的呼叫数。 对于 Unified Communications Manager 群集配置，每条折线代表群集值，等于群集中所有服务器（数据可用）的值之和。 图表中的每个数据值表示已尝试的呼叫总数或 15 分钟持续时间内完成的呼叫数。 如果没有已完成 H.323 网关呼叫的数据，则报告程序不会生成代表已完成呼叫的数据的折线。 如果没有已尝试 H.323 网关呼叫的数据，则报告程序不会生成代表已尝试呼叫的数据的折线。 在 Unified Communications Manager 群集配置中，如果不存在群集中服务器的数据，报告程序不会生成代表该服务器上尝试或完成的呼叫的折线。 如果不存在任何 H.323 网关呼叫活动数据，则报告程序不会生成图表。

图 *16:* 描绘群集的 *H.323* 网关呼叫活动的折线图

以下折线图所示为 Unified Communications Manager 群集的 H.323 网关呼叫活动。

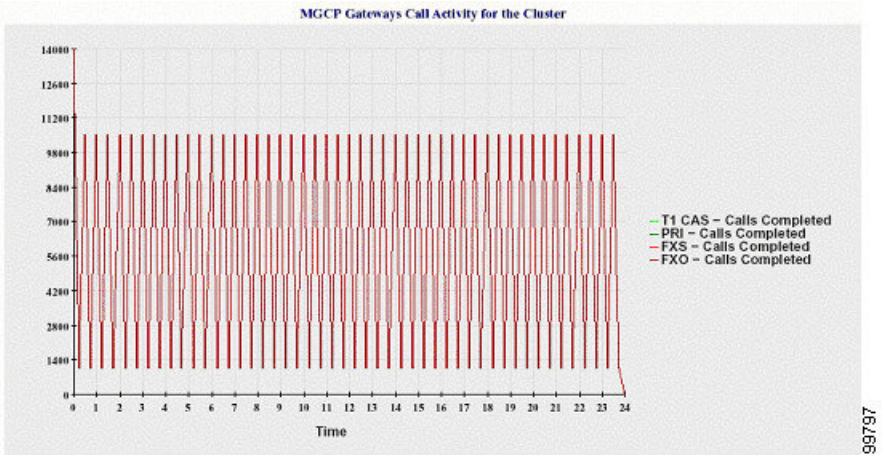


群集的 MGCP 网关呼叫活动

会有一幅折线图显示 MGCP FXO、FXS、PRI 和 T1CAS 网关在一小时内完成的呼叫数。 在 Unified Communications Manager 群集配置中，图表显示整个 Unified Communications Manager 群集中完成的呼叫数。图表中最多包含四条折线，一条对应每个网关类型（数据可用）完成的呼叫数。图表中的每个数据值表示在 15 分钟持续时间内完成的呼叫总数。 如果没有网关数据，则报告程序不会生成代表特定网关完成的呼叫数据的折线。 如果所有网关都无数据，则报告程序不会生成图表。

图 *17:* 描绘群集的 *MGCP* 网关呼叫活动的折线图

以下折线图所示为 Unified Communications Manager 群集的 MGCP 网关呼叫活动。



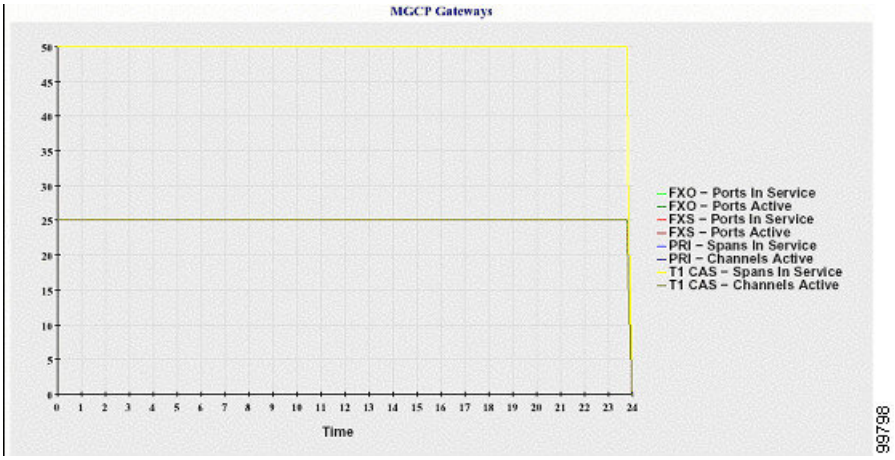
MGCP 网关

会有一幅折线图显示 MGCP FXO、FXS 网关的服务中端口和活动端口数，以及 PRI、T1CAS 网关的服务范围或活动通道数。 对于 Unified Communications Manager 群集配置，图表显示整个 Unified Communications Manager 群集的数据。 图表中包含八条折线，两条分别对应于 MGCP FXO 和 FXS 的服务中端口数，两条分别对应于 MGCP FXO 和 FXS 的活动端口数。 另有四条分别对应于 PRI 和 T1CAS 网关的服务范围和活动通道数。 对于 Unified Communications Manager 群集配置，每条折线代表群集值，即群集中所有服务器（数据可用）的值之和。 图表中的每个数据值代表 15 分钟内服

务中的端口总数、活动端口数、服务范围数或活动通道数。 如果不存在所有服务器的网关（MGCP PRI、T1CAS）服务范围或活动通道数据，则报告程序不会生成代表该特定网关的数据的折线。

图 *18*: 描绘 *MGCP* 网关的折线图

下图所示为代表 MGCP 网关的折线图。

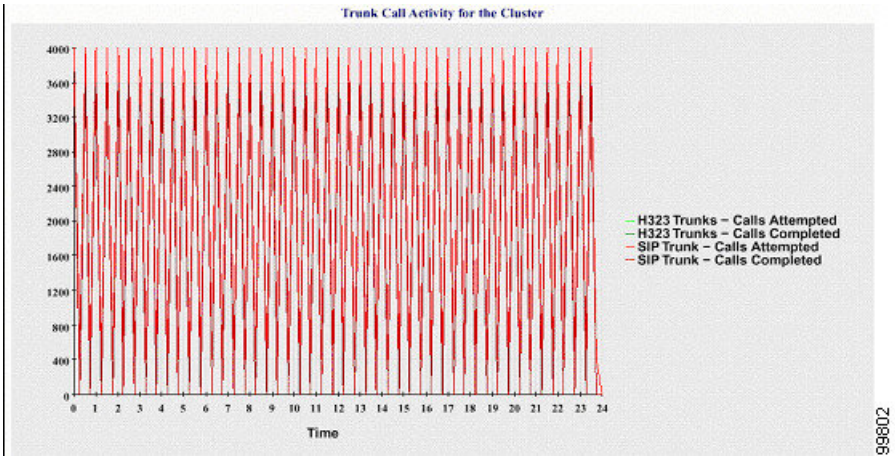


群集的干线呼叫活动

会有一幅折线图显示一小时内 SIP 干线和 H.323 干线已完成的呼叫数和尝试的呼叫数。 对于 Unified Communications Manager 群集配置，图表会显示整个 Unified Communications Manager 群集完成的呼叫数和尝试的呼叫数。 图表中包含四条折线，两条分别对应于 SIP 和 H.323 干线完成的呼叫数（数据可用），两条对应于尝试的呼叫数。 对于 Unified Communications Manager 群集配置，每条折线代表群集值，即群集中所有节点（数据可用）的值之和。 图表中的每个数据值表示在 15 分钟持续时间内完成的呼叫总数和尝试的呼叫数。 如果没有干线数据，则报告程序不会生成代表特定干线完成的呼叫数据或尝试的呼叫数据的折线。 如果两种干线类型均没有数据，则报告程序不会生成图表。

图 *19*: 描绘群集的干线呼叫活动的折线图

以下折线图所示为 Unified Communications Manager 群集的干线呼叫活动。



服务器（或 Unified Communications Manager 群集配置中的每台服务器）包含文件名采用以下命名模式的日志文件：CallLog_mm_dd_yyyy_hh_mm.csv。 日志文件中包含以下信息：

- Unified Communications Manager（或 Unified Communications Manager 群集中的每台服务器）尝试的呼叫数和完成的呼叫数
- H.323（或 Unified Communications Manager 群集中每台服务器的网关）尝试的呼叫数和完成的呼叫数
- MGCP FXO、FXS、PRI 和 T1CAS 网关（或 Unified Communications Manager 群集中每台服务器的网关）完成的呼叫数
- MGCP FXO 和 FXS 网关的服务中端口、活动端口，以及 PRI 和 T1CAS 网关的服务范围、活动通道（Unified Communications Manager 群集中的每台服务器）
- H.323 干线和 SIP 干线完成的呼叫以及尝试的呼叫

警告摘要报告

警告摘要报告提供当天生成的警告的详细信息。

仅 Unified Communications Manager 和 IM and Presence Service 支持群集特定的统计信息。

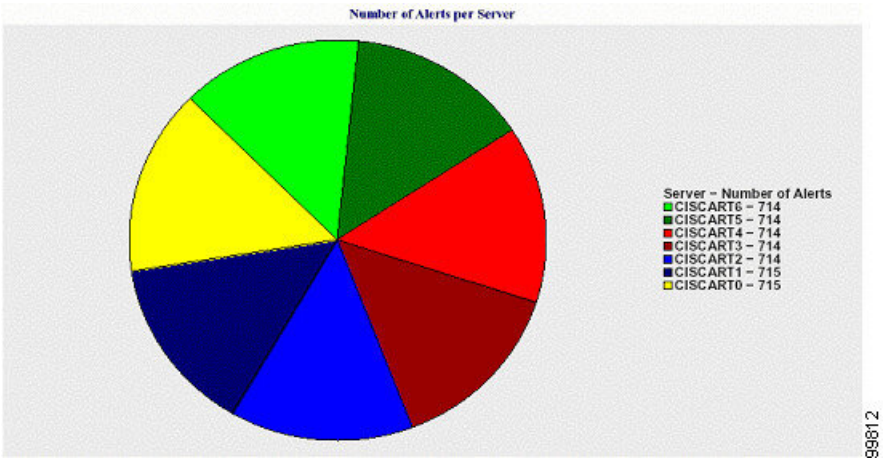
每台服务器的警告数

有一个饼图提供群集中每个节点的警告数。 该图表会显示所生成警告的服务器范围内的详细信息。饼图的每个扇区代表为群集中特定服务器生成的警告数。 图表中的扇区数量与群集中的服务器（报告程序在一天中为其生成警告）数量相同。 如果服务器无数据，图表中不会有任何扇区代表该服务器。 如果所有服务器都无数据，则报告程序不会生成图表。此时会显示消息：“当天未生成任何警告”。

仅 Cisco Unity Connection：将有一个饼图提供服务器的警告数。 该图表会显示所生成警告的服务器范围内的详细信息。 如果服务器无数据，则报告程序不会生成图表。此时会显示消息“当天未生成任何警告”。

下图所示为一个饼图示例，描绘了 Unified Communications Manager 群集中每个服务器的警告数。

图 *20:* 描绘每台服务器的警告数的饼图

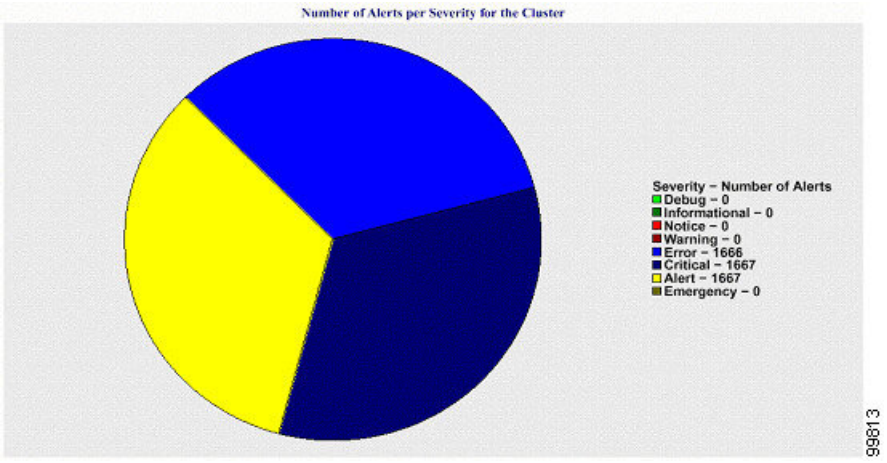


群集中每种严重性的警告数

饼图显示了每种警告严重性的警告数。图表显示所生成的警告的严重性详细信息。饼图的每个扇区代表特定严重性类型的警告生成数量。图表中的扇区数量与严重性（报告程序在一天中为其生成警告）数量相同。如果无严重性数据，图表中不会有任何扇区代表该严重性。如果没有数据，则报告程序不会生成图表。

下图所示为一个饼图示例，描绘了 Unified Communications Manager 群集中每种严重性的警告数。

图 *21:* 描绘群集中每种严重性的警告数的饼图

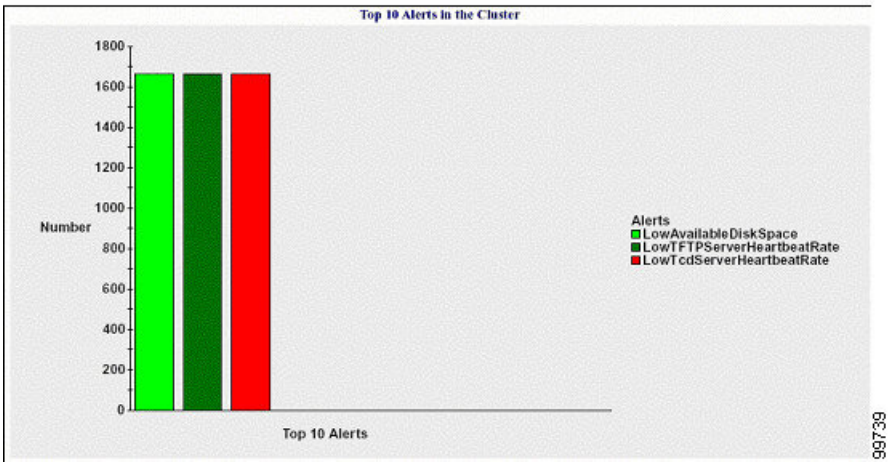


群集中的前十个警告

条形图显示特定警告类型的警告数。图表根据警告类型显示生成的警告的详细信息。每根柱代表一种警告类型的警告数。图表仅基于最高警告数按降序显示前十个警告的详细信息。如果没有特定警告类型的任何数据，则不会有代表该警告的柱。 如果没有任何警告类型的数据，RTMT 不会生成图表。

下图所示为一个条形图示例，描绘了 Unified Communications Manager 群集中的前十个警告。

图 *22:* 描绘群集中的前 *10* 个警告的条形图



服务器（或群集中的每台服务器）包含文件名采用以下命名模式的日志文件：AlertLog_mm_dd_yyyy_hh_mm.csv。 日志文件中包含以下信息：

- 时间 - 出现警告的时间
- 警告名称 - 描述性名称
- 节点名称 - 出现警告的服务器
- 监控对象 - 被监控的对象
- 严重性 - 此警告的严重性

性能保护报告

性能保护报告不支持 IM and Presence Service 和 Cisco Unity Connection。

性能保护报告提供包含显示该特定报告统计信息的各种图表的摘要。 报告程序基于记录的信息每天一次生成报告。

性能保护报告提供最近七个默认监控对象的趋势分析信息，以便您能够跟踪关于 Cisco Intercompany Media Engine 的信息。 报告包括 Cisco IME 客户端呼叫活动图表，其中显示 Cisco IME 客户端的呼叫总数和回退呼叫率。

性能保护报告包含以下图表：

- Cisco Unified Communications Manager 呼叫活动
- 注册电话数和 MGCP 网关数
- 系统资源利用率 (System Resource Utilization)
- 设备和拨号方案数量

Cisco Unified Communications Manager 呼叫活动

会有一幅折线图显示尝试呼叫数以及作为活动呼叫完成的呼叫数每小时的增减率。 对于 Unified Communications Manager 群集配置，将为群集中的每台服务器绘制数据图表。 图表中包含三条折线，一条对应尝试的呼叫数，一个对应完成的呼叫数，一个对应活动的呼叫数。 如果不存在呼叫活动数据，报告程序不会生成图表。

注册电话数和 MGCP 网关数

会有一幅折线图显示注册的电话数和 MGCP 网关数。 对于 Unified Communications Manager 群集配置，图表将显示群集中每台服务器的数据。图表中包含两条折线，一条对应注册的电话数，另一条对应 MGCP 网关数。 如果不存在电话或 MGCP 网关数据，报告程序不会生成图表。

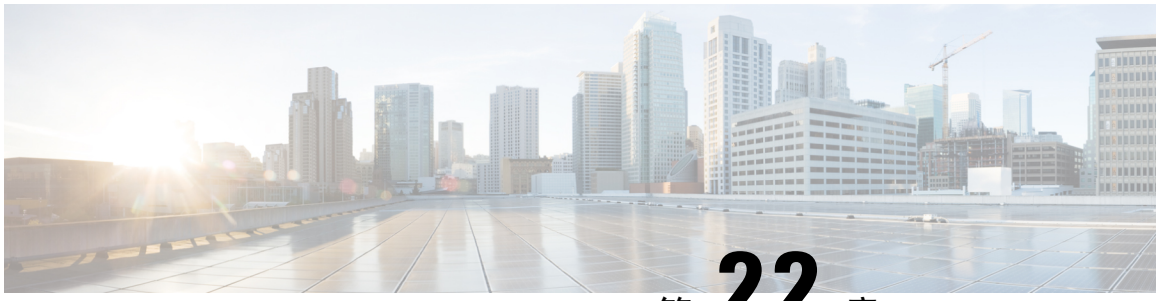
系统资源利用率 (System Resource Utilization)

会有一幅折线图显示服务器（或 Unified Communications Manager 群集配置中的整个群集）使用的 CPU 负载百分比和内存百分比（以字节为单位）。 图表中包含两条折线，一条对应 CPU 负载，一

个对应内存使用量。 在Unified Communications Manager群集配置中，每条折线代表群集值，即群集中所有服务器（数据可用）的值之平均值。 如果不存在电话或MGCP网关数据，报告程序不会生成图表。

设备和拨号方案数量

两个表显示Unified Communications Manager数据库中有关设备数量和拨号方案组件数量的信息。 设备表显示IP电话、Cisco Unity Connection端口、H.323客户端、H.323网关、MGCP网关、MOH资源和MTP资源数量。 拨号方案表显示目录号码和线路、路由模式和转换模式的数量。



第 22 章

Cisco Unified 报告

整合数据报告

Cisco Unified 报告 Web 应用程序在 Cisco Unified Communications Manager 和 Cisco Unified Communications Manager IM and Presence Service 控制台访问，会为故障诊断或检查群集数据生成汇总的报告。

注释 除非另行说明，否则本指南中的信息、注释和程序适用于 Unified Communications Manager 和 IM and Presence Service。

此工具提供了一种简单的方法来大概了解群集数据。 该工具可从现有来源收集数据、比较数据，以及报告违规。 当您在 Cisco Unified 报告中生成报告时，报告会将来自一台或多台服务器上的一个或多个来源的数据合并到一个输出视图中。 例如，您可以查看显示群集中所有服务器主机文件的报告。

Cisco Unified 报告 Web 应用程序在安装时部署到群集中的所有节点。 报告从数据库记录生成。

用于生成报告的数据源

应用程序捕获来自发布方节点和每个订阅方节点上以下任何来源的信息。

- RTMT 计数器
- CDR_CAR（仅限 Unified Communications Manager）
- Unified Communications Manager DB（仅限 Unified Communications Manager）
- IM and Presence DB（仅限 IM and Presence Service）

- 磁盘文件
- OS API 呼叫
- 网络 API 呼叫
- 首选
- CLI
- RIS

报告包含您生成报告时可访问的所有活动群集的数据。 如果发布方节点上的数据库关闭，您可以为活动节点生成报告。 “系统报告”列表中的“报告说明”报告提供报告的信息源。

支持的输出格式

此版本支持 HTML/CSV 格式输出的报告。 您可以通过报告名称和日期时间戳识别 Cisco Unified 报告中的报告。 应用程序会将最新报告的副本存储在本地供您查看。 您可以如“下载新报告”中所述，将最新报告的本地副本或新报告下载到硬盘。 下载报告后，您可以重命名下载的文件或将其存储在不同的文件夹中，以供识别。

系统要求

Cisco Tomcat 服务

Cisco Unified 报告在安装 Unified Communications Manager 和 IM and Presence Service 时激活的 Cisco Tomcat 服务上作为应用程序运行。 确保这些产品正在群集中的所有节点上运行。

HTTPS

报告子系统通过 HTTPS 使用 RPC 机制从其他节点收集信息。 确保 HTTPS 端口已打开，且 Cisco Tomcat 服务正在节点上运行，以成功生成报告。

要启用HTTPS，必须下载用于在连接过程中标识节点的证书。 您只能接受节点证书进行当前会话，也可以将证书下载到信任文件夹（文件）中，以保护当前或将来通过该节点进行的会话。 信任文件夹存储所有受信任站点的证书。 有关 HTTPS 的详细信息，请参阅《*Cisco Unified Communications Manager* 管理指南》的“简介”一章。

要访问应用程序，您可以在浏览器窗口中访问管理界面。 Cisco Unified 报告使用 HTTPS 建立与浏览器的安全连接。

所需访问权限

在允许用户访问 Web 应用程序之前，Cisco Unified Reporting 会使用 Cisco Tomcat 服务对用户进行身份验证。 只有经过授权的用户才能访问 Cisco Unified 报告应用程序。 对于 Unified Communications

Manager，默认情况下只有标准 CCM 超级用户组中的管理员用户才能访问 Cisco Unified 报告以查看和创建报告。

对于 Cisco Unified Communications Manager 和 IM and Presence Service，标准 CUReporting 验证角色中的用户可以访问 Cisco Unified 报告。

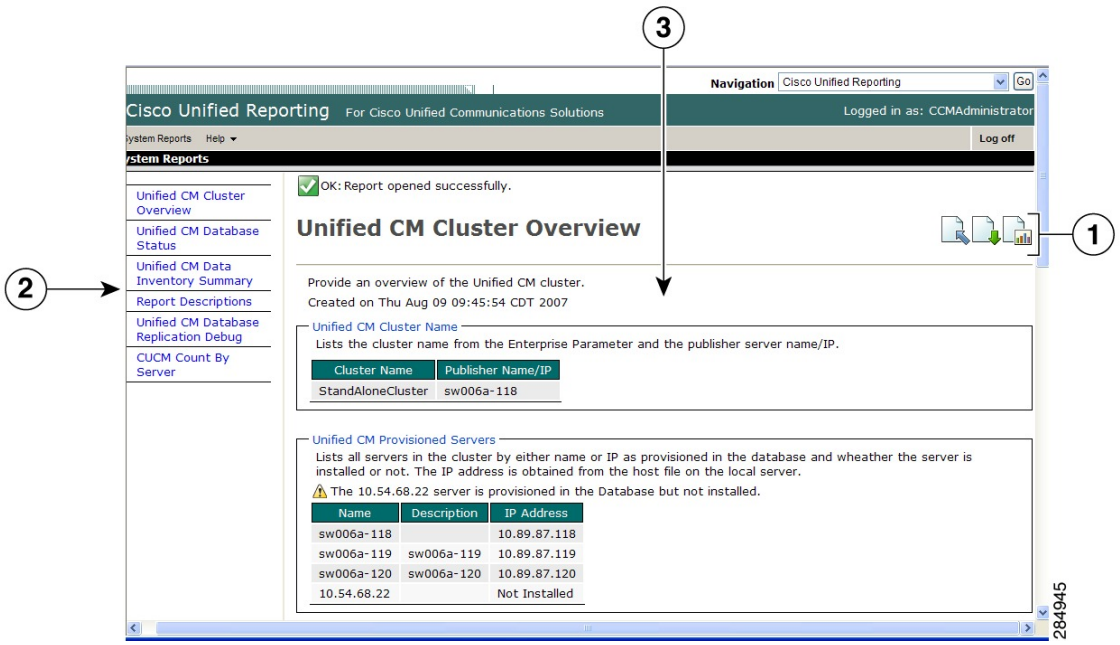
作为授权用户，您可以使用 Cisco Unified 报告用户界面查看报告、生成新报告或下载报告。

注释 对于 Unified Communications Manager，标准 CCM 超级用户组中的管理员用户可以访问 Unified Communications Manager 管理导航菜单（包括 Cisco Unified 报告）中的管理应用程序并单点登录到其中一个应用程序。

UI 组件

下图所示为 Cisco Unified 报告的 UI 组件。

图 *23: UI* 组件



1. 上传、下载、生成图标
2. 报告列表
3. 报告详细信息

注释 报告类别、可用报告和报告数据因版本而异。

从管理界面登录

执行以下任一步骤以从管理界面登录 Cisco Unified 报告。

- 对于 Unified Communications Manager，在 Cisco Unified CM 管理界面的导航菜单中选择 **Cisco Unified 报告**。
- 对于 IM and Presence Service，在 Cisco Unified CM IM and Presence 管理界面的导航菜单中选择 **Cisco Unified IM and Presence 报告**。

开始之前

确保您有权访问 Cisco Unified 报告应用程序。

当您登录 Cisco Unified 报告时，每个用户最后一次成功的系统登录尝试和最后一次不成功的系统登录尝试以及用户 ID、日期、时间和 IP 地址将显示在主 Cisco Unified 报告窗口中。

支持的报告

本节详细介绍 Cisco Unified Communications Manager 和 Cisco Unified Communications Manager IM and Presence Service 支持的报告。 您可以通过报告名称和日期时间戳识别 Cisco Unified 报告中的报告。Cisco Unified 报告会存储最新报告的本地副本供您查看。

Unified Communications Manager 报告

下表介绍了安装 Unified Communications Manager 后，Cisco Unified 报告中出现的系统报告类型。

表 *75: Unified Communications Manager Cisco Unified* 报告中显示的报告

报告	说明
采用过期凭证算法的 UCM 用户	提供使用 SHA1 存储和哈希密码或 PIN 的最终用户的列表。
报告说明	提供有关所显示报告的故障诊断及详细信息。
安全诊断工具	提供关于安全组件的信息摘要视图。

报告	说明
Unified CM 群集概述	提供 Unified Communications Manager 群集的概述。 此报告包括以下详细信息： • 群集中安装的 Unified Communications Manager 或 IM and Presence Service 的版本 • 群集中所有节点的主机名或 IP 地址 • 硬件详细信息摘要
Unified CM 数据摘要	根据 Unified Communications Manager 管理中菜单的结构，提供 Unified Communications Manager 数据库中的数据摘要。 例如，如果配置三个凭据策略、五个会议桥和十个共享线路外观，则可以在此报告中看到该类型的信息。
Unified CM 数据库复制调试	提供数据库复制的调试信息。 **提示** 生成此报告可能会导致 CPU 使用激增，并且群集中每个节点可能需要长达 10 秒的时间。
Unified CM 数据库状态	提供 Unified Communications Manager 数据库运行状况快照。 升级前生成此报告，以确保数据库状态良好。
Unified CM 设备计数摘要	按 Unified Communications Manager 数据库中的型号和协议提供设备数量。
Unified CM 设备分发摘要	提供在整个群集内如何分发设备的摘要。例如，此报告显示了与主节点、第二节点和第三节点关联的设备。
Unified CM 目录 URI 和 GDPR 重复	提供系统上重复的用户目录URI、学习的目录URI、学习的编号以及学习的模式的详细列表。
Unified CM Extension Mobility	提供 Cisco Extension Mobility 使用情况的摘要；例如，有 Cisco Extension Mobility 用户登录的电话数量、与 Cisco Extension Mobility 关联的用户等等。
Unified CM 地理位置策略	提供地理位置逻辑分区策略矩阵中的记录列表。
采用过滤器的 Unified CM 地理位置策略	提供地理位置逻辑分区策略矩阵中所选地理位置策略的记录列表。
无电话的 Unified CM 线路	提供未与电话关联的线路列表。
Unified CM 多线路设备	提供具有多线路显示的电话列表。
Unified CM 电话类别	提供给定类别中用于通用设备模板的电话型号列表。 为用户启用自预配置时，您可以为每个类别提供模板，以选择允许任何或所有这些类别的电话。

报告	说明
Unified CM 电话功能列表	提供 Unified Communications Manager 管理中每种设备类型支持的功能列表。
Unified CM 电话区域设置安装程序	提供安装的电话区域设置软件包支持的 Cisco Unified IP 电话固件版本列表。
含不匹配负载的 Unified CM 电话	提供含不匹配固件负载的所有电话的列表。
无线路的 Unified CM 电话	提供 Unified Communications Manager 数据库中没有关联线路的所有电话的列表。
Unified CM 共享线路	提供 Unified Communications Manager 数据库中至少有一个共享线路显示的所有电话的列表。
Unified CM 表格计数摘要	提供以数据库为中心的数据视图。 此报告对了解数据库架构的管理员或 AXL API 开发人员非常有用。
Unified CM 用户设备计数	提供有关关联设备的信息；例如，此报告会列出没有用户的电话数量、有一部电话的用户数量以及有多部电话的用户数量。
共享主分机的 Unified CM 用户	提供在系统上共享主分机的用户列表。
Unified CM VG2XX 网关	提供网关终端安全配置文件的摘要。
Unified CM 语音邮件	提供 Unified Communications Manager 管理中语音留言相关配置的摘要；例如，此报告会列出已配置的语音邮件端口数量、留言通知指示灯数量、已配置的语音留言配置文件数量、与语音留言配置文件关联的目录号码数量等等。
Unified 保密访问级别矩阵	提供有关保密访问级别矩阵的所有信息。

IM and Presence Service 报告

下表介绍了在 Unified Communications Manager 上安装 IM and Presence Service 后，Cisco Unified 报告中显示的系统报告类型。

注释 从版本 10.0(1) 开始，IM and Presence 群集信息可从 Cisco Unified Communications Manager 节点获得。 从 Cisco Unified Communications Manager 中，选择 **Cisco Unified 报告** > **系统报告** > **Unified CM 群集概述**。

您可以查看和生成下表中的任何报告类型。

表 *76: Cisco Unified Reporting* 中显示的 *IM and Presence Service* 报告

报告	说明
IM and Presence 数据库复制调试	提供数据库复制的调试信息。 **提示** 生成此报告可能会导致 CPU 使用激增，并且群集中每个节点可能需要长达 10 秒的时间。
IM and Presence 数据库状态	提供 IM and Presence Service 数据库运行状况快照。 升级前生成此报告，以确保数据库状态良好。
IM and Presence 表计数摘要	提供以数据库为中心的数据视图。此报告证明对了解数据库方案的管理员或 AXL API 开发人员非常有用。
IM and Presence 用户会话报告	提供与一台或多台设备进行登录会话的所有活动用户列表。
Presence 状态配置报告	提供有关 IM and Presence Service 用户的配置信息。 • 从 Cisco Unified Communications Manager 同步的用户 • 为 IM and Presence Service 启用的用户 • 为 Microsoft 远程呼叫控制启用的用户 • 为 IM and Presence Service 中的日程安排信息启用的用户 单击**查看详细信息**可按可排序列查看用户列表。
IM and Presence 群集概述	提供 IM and Presence Service 群集的概述。 例如，此报告提供群集中安装的 IM and Presence Service 的版本、群集中所有节点的主机名或 IP 地址、硬件详细信息摘要等等。
Presence 限制预警报告	提供有关已达到或超过联系人或观察者最大数量配置限制的用户信息。 单击**查看详细信息**可按可排序列查看用户列表。
Presence 使用情况报告	提供已登录 XMPP 客户端和第三方 API 的使用情况信息。 单击**查看详细信息**可按可排序列查看 XMPP 客户端和第三方 API 列表。
报告说明	提供有关所显示报告的故障诊断及详细信息。 此报告提供有关报告、每个信息组和每个数据项的说明，以及数据源、相关问题的症状以及补救措施。

查看报告说明

Cisco Unified 报告提供报告帮助。“报告说明”链接提供报告、每个信息组和每个数据项的说明，以及数据源、相关问题的症状以及补救措施。

注释 您可能还需要与 TAC 联系以获取有关报告问题的其他帮助。

过程

步骤 1 选择**系统报告**。

步骤 2 在报告列表中选择**报告说明**链接。

注释 如果选择 IM and Presence Service 报告，当系统提示重新登录时，请重新输入您的 Cisco Unified Communications Manager 管理登录凭证。

步骤 3 选择**生成报告**图标。

该报告会生成并显示。

生成新报告

您可以生成和查看新报告。

开始之前

确保 Cisco Tomcat 服务至少在一个节点上运行，并且您正在使用受支持的 Web 浏览器查看报告。

应用程序会通知您报告是否将花费过多时间来生成或是否会消耗过多CPU时间。 在报告生成时，会显示一个进度条。 此时新报告将显示，并且日期和时间会更新。

过程

步骤 1 从菜单栏中选择**系统报告**。

步骤 2 选择报告。

注释 如果选择 IM and Presence Service 报告，当系统提示重新登录时，请重新输入您的 Cisco Unified Communications Manager 管理登录凭证。

步骤 3 在**报告**窗口中选择**生成报告**（条形图）图标。

步骤 4 选择**查看详细信息**链接以显示不会自动显示的部分的详细信息。

下一步做什么

如果报告显示项目的数据检查不成功，请选择**报告说明**报告并查看故障诊断信息以及可能的补救措施。 由于报告说明报告是从数据库动态生成的，因此您还可以生成新的报告说明报告。

查看保存的报告

您可以查看现有报告的副本。

注释 在全新安装或升级期间，Cisco Unified 报告应用程序不会保存最新报告的本地副本。

开始之前

确保 Cisco Tomcat 服务至少在一个节点上运行，并且您正在使用受支持的 Web 浏览器查看报告。

过程

步骤 1 从菜单栏中选择**系统报告**。

步骤 2 从报告列表中选择要查看的报告。

步骤 3 选择报告名称的链接（日期和时间戳）。

步骤 4 选择**查看详细信息**链接以显示不会自动显示的部分的详细信息。

下一步做什么

下载新的或保存的报告。

如果报告显示针对某个项目的数据检查不成功，请选择**报告说明**报告并查看有关可能的补救方法的故障诊断信息。

下载新报告

要下载新报告，请将其存储在本地的硬盘驱动器上。 下载报告时，原始 XML 数据文件也会下载到您的硬盘驱动器上。

过程

步骤 1 生成新报告。

步骤 2 新报告显示后，在**报告**窗口中选择**下载报告**（绿色箭头）图标。

注释 您无需在下载文档之前单击**查看详细信息**链接获取报告的详细信息。 数据捕获在下载的文件中。

步骤 3 选择**保存**以将文件保存到指定的磁盘位置。

要更改文件名或文件在硬盘上的存储位置，请输入新位置或重命名文件（可选）。 进度条会显示下载进度。

文件会下载到您的硬盘上。

步骤 4 下载完成后，选择**打开**以打开 XML 报告。

注释 不要更改 XML 文件中的内容，否则您的报告可能无法在屏幕上正确显示。

下一步做什么

要在浏览器中查看下载的报告文件，请将文件上传到您的节点。

注释 要寻求技术支持，可以将下载的文件附加到电子邮件中，或者将文件上传到另一个节点。

下载保存的报告

要下载保存的报告，可以下载报告并将其存储在本地的硬盘驱动器上。 下载报告时，原始 XML 数据文件也会下载到您的硬盘上。

过程

步骤 1 打开并查看现有报告的详细信息。

步骤 2 在**报告**窗口中选择**下载报告**（绿色箭头）图标。

步骤 3 选择**保存**以将文件保存到指定的磁盘位置。

要更改文件名或文件在硬盘上的存储位置，请输入新位置或重命名文件（可选）。 进度条会显示下载进度。

文件会下载到您的硬盘上。

步骤 4 下载完成后，选择**打开**以打开 XML 报告。

注释 不要更改 XML 文件中的内容，否则您的报告可能无法正确显示。

下一步做什么

要在浏览器中查看下载的报告文件，请将文件上传到您的节点。

注释 要寻求技术支持，可以将下载的文件附加到电子邮件中，或者将文件上传到另一个节点。

上传报告

要在浏览器窗口中查看下载的报告，必须将报告上传到 nodetand。

开始之前

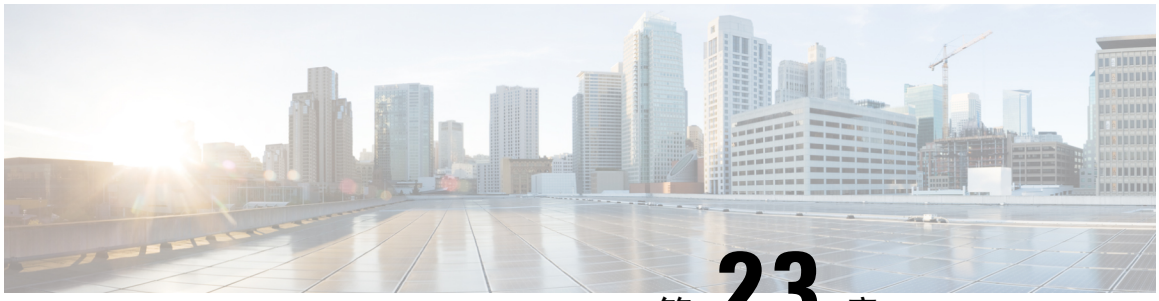
将报告下载到硬盘驱动器。

过程

步骤 1 从菜单栏中选择**系统报告**。
步骤 2 访问任何报告以在**报告**窗口中显示**上传报告**（蓝色箭头）图标。
步骤 3 选择**上传报告**图标。
步骤 4 要定位 .xml 文件，选择**浏览**导航到其在硬盘驱动器上的位置。
步骤 5 选择**上传**。
步骤 6 选择**继续**以在浏览器窗口中显示上传的文件。

下一步做什么

您可以在升级期间并排比较上传的报告和新生成的报告。



第 23 章

为 Cisco IP 电话配置呼叫诊断和质量报告

诊断和报告概述

Cisco Unified Communications Manager 提供两个选项来确保 Cisco IP 电话上的呼叫质量：

- 呼叫诊断—呼叫诊断包括生成呼叫管理记录 (CMR) 和语音质量指标。
- 质量报告工具 QRT)—QRT 是适用于 Cisco IP 电话的语音质量和一般问题报告工具。 此工具可让用户轻松准确地报告其 IP 电话的音频和其他一般问题。

呼叫诊断概述

您可以配置运行 SCCP 和 SIP 的 Cisco IP 电话以收集呼叫诊断。 呼叫诊断包含呼叫管理记录（CMR，也称为诊断记录）和语音质量指标。

语音质量指标默认启用，并且在大多数 Cisco IP 电话上均受支持。 Cisco IP 电话根据 MOS（平均意见平方）值计算语音质量指标。 语音质量指标不考虑噪音和失真，仅考虑丢帧。

CMR 记录存储有关呼叫的流式音频质量的信息。 您可以配置 Unified Communications Manager 以生成 CMR。 此信息对处理后的活动（如生成计费记录和网络分析）非常有用。

质量报告工具概述

质量报告工具 (QRT) 是适用于 Cisco IP 电话的语音质量和一般问题报告工具。 此工具可让用户轻松准确地报告其 IP 电话的音频和其他一般问题。

系统管理员可通过配置和分配软键模板在用户 IP 电话上显示 QRT 软键，进而启用 QRT 功能。 可以从两种不同的用户模式中进行选择，具体取决于您希望与 QRT 进行用户交互的程度。 然后，通过配置系统参数和设置 Cisco Unified 功能配置工具，可定义该功能在系统中如何工作。 您可以使用 QRT 查看器应用程序创建、自定义和查看电话问题报告。

用户的 IP 电话遇到问题时，在呼叫状态为“挂机”或“已连接”期间，通过按 Cisco IP 电话上的 QRT 软键，可以报告问题类型和其他相关统计信息。然后，用户可以选择最贴切地说明所报告的 IP 电话问题的原因代码。 自定义电话问题报告将为您提供特定的信息。

在用户按 QRT 软键选择问题类型后，QRT 将尝试收集流统计信息。呼叫应处于活动状态至少 5 秒，以便 QRT 收集流统计数据。

详细的呼叫报告和计费

Cisco CDR 分析和报告 (CAR) 工具会生成详细的服务质量、流量、用户呼叫量、计费和网关报告。CAR 使用来自呼叫详细信息记录 (CDR)、呼叫管理记录 (CMR) 和 Unified Communications Manager 数据库的数据，以便生成报告。 可以通过 Cisco Unified 功能配置的**工具**菜单访问 CAR 界面。

CAR 的目的不是取代第三方公司提供的呼叫记账和计费解决方案。 您可以通过搜索 Cisco 开发者社区的主页找到提供这些解决方案以及加入 Cisco 技术开发者计划的公司。

有关如何使用 CAR 配置报告的详细信息，请参阅《*Cisco Unified Communications Manager* 呼叫报告和计费管理指南》。

Prerequisites

呼叫诊断先决条件

检查您的 Cisco Unified IP 电话是否支持呼叫诊断。

使用此表可确定您的电话是否支持呼叫诊断。 呼叫诊断支持图例如下：

- X—运行 SCCP 和 SIP 的电话支持
- S—仅 SCCP 功能

表 *77:* 设备对于呼叫诊断的支持

设备	对于呼叫诊断的支持
Cisco 7906 Unified IP 电话	X
Cisco 7911 Unified IP 电话	X
Cisco 7931 Unified IP 电话	X
Cisco 7940 Unified IP 电话	S
Cisco 7941 Unified IP 电话	X
Cisco 7942-G Unified IP 电话	X
Cisco 7942-G/GE Unified IP 电话	X

设备	对于呼叫诊断的支持
Cisco 7945 Unified IP 电话	X
Cisco 7960 Unified IP 电话	S
Cisco 7961 Unified IP 电话	X
Cisco 7962-G Unified IP 电话	X
Cisco 7962-G/GE Unified IP 电话	X
Cisco 7965 Unified IP 电话	X
Cisco 7972-G/GE Unified IP 电话	X
Cisco 7975 Unified IP 电话	X

质量报告工具先决条件

包含以下功能的 Cisco IP 电话：

- 支持软键模板
- 支持 IP 电话服务
- 通过 CTI 可控制
- 包含内部 HTTP 服务器

有关详细信息，请参阅相关电话型号的指南。

诊断和报告配置任务流程

过程

	命令或操作	目的
步骤 1	配置呼叫诊断， 第 302 页	执行此任务可将 Cisco Unified Communications Manager 配置为生成 CMR。 CMR 记录存储有关呼叫的流式音频质量的信息。 有关访问 CMR 的详细信息，请参阅《*Cisco Unified Communications Manager* 呼叫详细信息记录管理指南》。 Cisco IP 电话上会自动启用语音质量指标。有关访问语音质量指标的详细信息，请参阅

	命令或操作	目的
		您的电话型号对应的《Cisco Unified IP 电话管理指南》。
步骤 2	要配置质量报告工具， 第 302 页，请执行以下子任务： • 使用 QRT 软键配置软键模板， 第 303 页 • 将 QRT 软键模板与通用设备配置关联，第 304 页 • 向电话添加 QRT 软键模板， 第 306 页 • 在 Cisco Unified 功能配置中配置 QRT，第 306 页 • 配置质量报告工具的服务参数， 第 309 页	配置质量报告工具 (QRT)，以便遇到 IP 电话相关问题的用户可以通过按下 QRT 软键来报告问题类型和其他相关统计信息。

配置呼叫诊断

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统** > **服务参数**。

步骤 2 从**服务器**下拉列表框中选择运行 Cisco CallManager 服务的服务器。

步骤 3 从**服务**下拉列表中，选择 **Cisco CallManager**。
此时将显示**服务参数配置**窗口。

步骤 4 在**群集范围参数**（**设备-常规**）区域中，配置**启用呼叫诊断**服务参数。 提供以下选项：

- **禁用**—不生成 CMR。
- **仅在 CDR 启用标志为 True 时启用**—仅当“呼叫详细记录 (CDR) 启用标志”服务参数设置为 True 时，才会生成 CMR。
- **不论 CDR 启用标志为何都启用**—无论“CDR 启用标志”服务参数的值为何，都生成 CMR。

注释 生成 CMR 而不启用“CDR 启用标志”服务参数可能会导致磁盘空间消耗失控。 Cisco 建议您在启用 CMR 时启用 CDR。

步骤 5 单击**保存**。

配置质量报告工具

配置质量报告工具 (QRT)，以便遇到 IP 电话相关问题的用户可以通过按下 QRT 软键来报告问题类型和其他相关统计信息。

过程

	命令或操作	目的
步骤 1	使用 QRT 软键配置软键模板， 第 303 页	必须为 QRT 软键配置“挂机”和“已连接”呼叫状态。 以下呼叫状态也可用： • 已连接会议 • 已连接转接
步骤 2	（可选）要将 QRT 软键模板与通用设备配置关联， 第 304 页，请执行以下子任务： • 将 QRT 软键模板添加到通用设备配置， 第 305 页 • 将通用设备配置与电话关联， 第 305 页	要使软键模板对电话可用，必须完成此步骤或以下步骤。 如果您的系统使用**通用设备配置**将配置选项应用到电话，请按照此步骤操作。 这是使软键模板可用于电话的最常用方法。
步骤 3	（可选） 向电话添加 QRT 软键模板， 第 306 页	可以使用此程序作为将软键模板与通用设备配置相关联，或者与通用设备配置结合使用的备用方法。 当您需要分配软键模板覆盖通用设备配置中的分配或任何其他默认软键分配时，请将此程序与通用设备配置结合使用。
步骤 4	要在 Cisco Unified 功能配置中配置 QRT， 第 306 页，请执行以下子任务： • 激活 Cisco 扩展功能服务， 第 307 页 • 配置警报， 第 307 页 • 配置跟踪， 第 308 页	
步骤 5	（可选） 配置质量报告工具的服务参数， 第 309 页	

使用 QRT 软键配置软键模板

必须为 QRT 软键配置“挂机”和“已连接”呼叫状态。 以下呼叫状态也可用：

- 已连接会议
- 已连接转接

过程

步骤 1 从 Cisco Unified CM 管理中，选择**设备** > **设备设置** > **软键模板**。

步骤 2 执行以下步骤以创建新的软键模板；否则，继续下一步。

a) 单击**新增**。

b) 选择默认模板，然后单击**复制**。

c) 在**软键模板名称**字段中输入模板的新名称。
d) 单击**保存**。

步骤 3 执行以下步骤以将软键添加到现有模板。

a) 单击**查找**并输入搜索条件。
b) 选择所需的现有模板。

步骤 4 选中**默认软键模板**复选框以将此软键模板指定为默认软键模板。

注释 如果将软键模板指定为默认软键模板，则除非先删除默认指定，否则无法删除该模板。

步骤 5 从右上角的**相关链接**下拉列表中选择**配置软键布局**，然后单击**转至**。

步骤 6 从**选择要配置的呼叫状态**下拉列表中，选择想要软键显示的呼叫状态。

步骤 7 从**未选择的软键**列表中，选择要添加的软键，然后单击向右箭头将该软键移至**所选软键**列表。 使用向上和向下箭头更改新软键的位置。

步骤 8 要在其他呼叫状态中显示软键，请重复上一步。

步骤 9 单击**保存**。

步骤 10 请执行以下任务之一：

- 如果您修改了已与设备关联的模板，请单击**应用配置**以重新启动设备。
- 如果您创建了新的软键模板，请将模板与设备关联，然后重新启动设备。 有关详细信息，请参阅将软键模板添加到通用设备配置和将软键模板与电话关联部分。

下一步做什么

请执行以下步骤之一：

- 将 QRT 软键模板添加到通用设备配置， 第 305 页
- 向电话添加 QRT 软键模板， 第 306 页

将 QRT 软键模板与通用设备配置关联

可选。 有两种方式可将软键模板与电话关联：

- 将软键模板添加到电话配置。
- 将软键模板添加到通用设备配置。

本节中的程序介绍如何将软键模板与通用设备配置关联。 如果您的系统使用通用设备配置将配置选项应用到电话，请按照以下程序操作。 这是使软键模板可用于电话的最常用方法。

要使用备用方法，请参阅向电话添加 QRT 软键模板， 第 306 页。

过程

	命令或操作	目的
步骤 1	将 QRT 软键模板添加到通用设备配置， 第 305 页	
步骤 2	将通用设备配置与电话关联， 第 305 页	

将 QRT 软键模板添加到通用设备配置

开始之前

使用 QRT 软键配置软键模板， 第 303 页

过程

步骤 1 从 Cisco Unified CM 管理中，选择**设备** > **设备设置** > **通用设备配置**。

步骤 2 执行以下步骤可创建新的通用设备配置，并将软键模板与之关联；否则，继续下一步。

a) 单击**新增**。
b) 在**名称**字段中输入通用设备配置的名称。
c) 单击**保存**。

步骤 3 执行以下步骤，将软键模板添加到现有的通用设备配置。

a) 单击**查找**并输入搜索条件。
b) 单击现有的通用设备配置。

步骤 4 在**软键模板**下拉列表中，选择包含您想要使其可用的软键的软键模板。

步骤 5 单击**保存**。

步骤 6 请执行以下任务之一：

- 如果您修改了已与设备关联的通用设备配置，请单击**应用配置**以重新启动设备。
- 如果您创建了新的通用设备配置，请将配置与设备关联，然后重新启动设备。

下一步做什么

将通用设备配置与电话关联， 第 305 页

将通用设备配置与电话关联

开始之前

将 QRT 软键模板添加到通用设备配置， 第 305 页

过程

步骤 1 从 Cisco Unified CM 管理中，选择**设备** > **电话**。
步骤 2 单击**查找**并选择电话设备以添加软键模板。
步骤 3 从**通用设备配置**下拉列表中，选择包含新软键模板的通用设备配置。
步骤 4 单击**保存**。
步骤 5 单击**重置**以更新电话设置。

向电话添加 QRT 软键模板

开始之前

使用 QRT 软键配置软键模板， 第 303 页

过程

步骤 1 从 Cisco Unified CM 管理中，选择**设备** > **电话**。
步骤 2 单击**查找**以显示配置的电话列表。
步骤 3 选择要向其添加电话按键模板的电话。
步骤 4 在**电话按键模板**下拉列表中，选择包含新功能按键的电话按键模板。
步骤 5 单击**保存**。
将会显示一个对话框，其中的消息指示您按下**重置**来更新电话设置。

在 Cisco Unified 功能配置中配置 QRT

过程

	命令或操作	目的
步骤 1	激活 Cisco 扩展功能服务， 第 307 页	激活Cisco扩展功能服务以支持语音质量功能（例如质量报告工具）。
步骤 2	配置警报， 第 307 页	配置 QRT 警告以在系统日志查看器内的应用程序日志中记录错误。 此功能会记录警报，提供警报的说明和建议的操作。 您可以从 Cisco Unified 实时监控工具访问系统日志查看器。
步骤 3	配置跟踪， 第 308 页	配置 QRT 跟踪以记录语音应用程序的跟踪信息。 配置要包含在 QRT 跟踪文件中的信息

	命令或操作	目的
		后，可以使用 Cisco Unified 实时监控工具中的“跟踪和日志中心”选项收集及查看跟踪文件。

激活 Cisco 扩展功能服务

激活 Cisco 扩展功能服务以支持语音质量功能（例如质量报告工具）。

过程

步骤 1 从 Cisco Unified 功能配置中，选择**工具** > **服务激活**。

步骤 2 从**服务器**下拉列表中，选择要在其中激活 Cisco 扩展功能服务的节点。

步骤 3 选中 **Cisco 扩展功能**复选框。

步骤 4 单击**保存**。

下一步做什么

配置警报，第 307 页

配置警报

配置 QRT 警告以在系统日志查看器内的应用程序日志中记录错误。 此功能会记录警报，提供警报的说明和建议的操作。 您可以从 Cisco Unified 实时监控工具访问系统日志查看器。

开始之前

激活 Cisco 扩展功能服务，第 307 页

过程

步骤 1 从 Cisco Unified 功能配置中，选择**警报** > **配置**。

步骤 2 从**服务器**下拉列表中，选择要为其配置警报的节点。

步骤 3 从**服务组**下拉列表中，选择 **CM 服务**。

步骤 4 从**服务**下拉列表中，选择 **Cisco 扩展功能**。

步骤 5 为“本地系统日志”和“SDI 跟踪”选中**启用警报**复选框。

步骤 6 从下拉列表中选择以下选项之一，为“本地系统日志”和“SDI 跟踪”配置“警报事件级别”：

- **紧急**—将系统指定为不可用。
- **警告**—表示需要立即采取措施。
- **严重**—系统检测到严重情况。
- **错误**—表示检测到错误情况。

- **预警**—表示检测到预警情况。
- **注意**—表示检测到正常但严重的情况。
- **信息性**—表示只是信息性消息。
- **调试**—表示 Cisco 技术支持中心 (TAC) 工程师用于调试的详细事件信息。

默认值为**错误**。

步骤 7 单击**保存**。

下一步做什么

配置跟踪 ， 第 308 页

配置跟踪

配置 QRT 跟踪以记录语音应用程序的跟踪信息。 配置要包含在 QRT 跟踪文件中的信息后，可以使用 Cisco Unified 实时监控工具中的“跟踪和日志中心”选项收集及查看跟踪文件。

开始之前

配置警报 ， 第 307 页

过程

步骤 1 从 Cisco Unified 功能配置中，选择**跟踪** > **配置**。

步骤 2 从**服务器**下拉列表中，选择要为其配置跟踪的节点。

步骤 3 从**服务组**下拉列表中，选择 **CM 服务**。

步骤 4 从**服务**下拉列表中，选择 **Cisco 扩展功能**。

步骤 5 选中**打开跟踪**复选项。

步骤 6 从**调试跟踪级别**下拉列表中选择以下选项之一：

- **错误**—跟踪所有错误情况以及过程和设备初始化消息。
- **特殊**—跟踪正常操作期间发生的所有特殊情况以及子系统状态转换。 跟踪呼叫处理事件。
- **状态转换**—跟踪所有状态转换情况以及正常操作期间发生的媒体层事件。
- **重要**—跟踪所有重要情况以及例程的入口和出口点。 并非所有服务都使用此跟踪级别。
- **进入_退出**—跟踪所有进入和退出的情况以及低层调试信息。
- **任意**—跟踪所有任意情况以及详细的调试信息。
- **详细**— 跟踪警报情况和事件。 用于异常路径中生成的所有跟踪。 使用最少的 CPU 周期数。

默认值为**错误**。

提示 我们建议您选中此部分中的所有复选框，以便进行故障诊断。

步骤 7 单击**保存**。

下一步做什么

（可选） 配置质量报告工具的服务参数，第 309 页

配置质量报告工具的服务参数

注意 我们建议您使用默认的服务参数设置，除非 Cisco 技术支持中心 (TAC) 建议使用其他设置。

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择**系统** > **服务参数**。

步骤 2 选择 QRT 应用程序所在的节点。

步骤 3 选择 **Cisco 扩展功能**服务。

步骤 4 配置服务参数。 请参阅“相关主题”部分，了解有关这些服务参数及其配置选项的更多信息。

步骤 5 单击**保存**。

相关主题

质量报告工具服务参数，第 309 页

质量报告工具服务参数

表 *78:* 质量报告工具服务参数

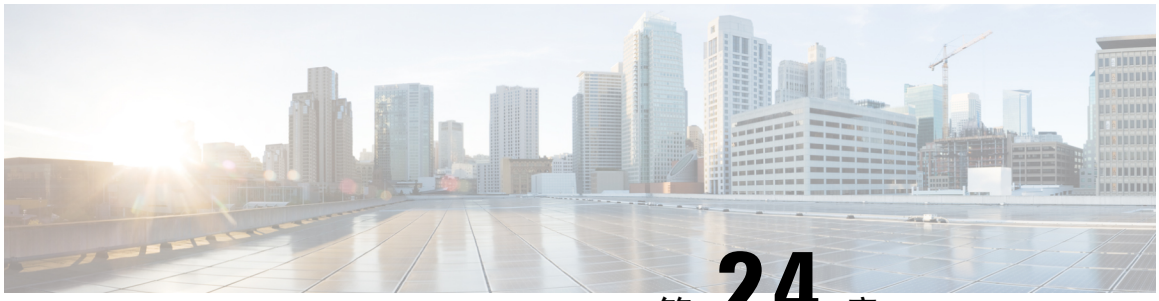
参数	说明
显示扩展的 QRT 菜单选项	确定是否向用户显示扩展的菜单选项。 您可以选择以下配置选项之一： • 将此字段设置为“真”，则显示扩展的菜单选项（交互模式）。 • 将此字段设置为“假”，则不显示扩展的菜单选项（静默模式）。 • 建议的默认值为 false（静默模式）。

参数	说明
流统计轮询持续时间	确定轮询流统计的持续时间。 您可以选择以下配置选项之一： • 将此字段设置为 -1，则一直轮询到呼叫结束。 • 将此字段设置为 0，则完全不轮询。 • 将此字段设置为任何正值，则轮询与此数值相等的秒数。 呼叫结束时，轮询停止。 • 建议的默认值为 -1（一直轮询到呼叫结束）。
流统计轮询频率（秒）	输入两次轮询之间等待的秒数。 该值的范围在 30 到 3600 之间。建议的默认值为 30。
文件最大数	输入重新开始文件计数和覆盖旧文件之前的最大文件数量。 有效值介于 1 到 10000 之间。建议的默认值为 250。
每个文件的最大行数	输入开始下一个文件前每个文件中的最大行数： • 此值的范围为 100 到 2000。 • 建议的默认值为 2000。
至 CTI Manager 安全连接的 CAPF 配置文件实例 ID	输入应用程序用户 CCMQRTSysUser 的应用程序 CAPF 配置文件的实例 ID，Cisco 扩展功能服务将使用此 ID 打开指向 CTI Manager 的安全连接。如果已启用“CTI Manager 连接安全标志”(CTI Manager Connection Security Flag)，则必须配置此参数。 **注释** 通过启用“CTI Manager 连接安全标志”服务参数来开启安全性。 必须重新启动 Cisco 扩展功能服务，更改才能生效。

参数	说明
CTI Manager 连接安全标志	指明启用还是禁用 Cisco 扩展功能服务 CTI Manager 连接的安全性。 如果启用，Cisco 扩展功能将使用为应用程序用户 CCMQRTSysUser 的实例 ID 配置的应用程序 CAPF 配置文件来打开指向 CTI Manager 的安全连接。 此值有“真”和“假”两个选项。如要启用指向 CTI 的安全连接，则必须选择“真”。

第 VI 部分

管理安全性



第 24 章

管理 SAML 单点登录

SAML 单点登录概述

使用 SAML 单点登录 (SSO) 登录到其中一个应用程序后，访问一组定义的 Cisco 应用程序。 SAML 描述了受信任的业务合作伙伴之间安全相关信息的交换。 它是服务提供程序（例如 Cisco Unified Communications Manager）用来验证用户的一种验证协议。 利用 SAML，安全验证信息可在身份提供程序 (IdP) 与服务提供程序之间交换。 该功能提供安全机制来跨各种应用程序使用通用凭证和相关信息。

SAML SSO 在部署过程中通过在 IdP 和服务提供程序之间交换元数据和证书建立信任圈 (CoT)。 服务提供程序信任 IdP 的用户信息，提供对各种服务或应用的访问权限。

客户端根据 IdP 进行验证，IdP 则向客户端授予断言。 客户端将断言提供给服务提供程序。 由于建立了 CoT，服务提供程序信任断言，并授予访问客户端的权限。

Cisco Jabber iOS 版本基于证书的 SSO 验证的选择加入控制

此版本的 Cisco Unified Communications Manager 引入了选择加入配置选项，以使用身份提供程序 (IdP) 控制 Cisco Jabber iOS 版本 SSO 登录行为。使用此选项以允许 Cisco Jabber 在受控的移动设备管理 (MDM) 部署中使用 IdP 执行基于证书的验证。

您可以在 Cisco Unified Communications Manager 中通过 **iOS 的 SSO 登录行为** (SSO Login Behavior for iOS) 企业参数配置选择加入控制。

注释 在更改此参数的默认值之前，请参阅位于 http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html 的 Cisco Jabber 功能支持和文档，以确保 Cisco Jabber iOS 版本支持 SSO 登录行为和基于证书的验证。

要启用此功能，请参阅为 Cisco Jabber iOS 版本配置 SSO 登录行为，第 318 页程序。

SAML 单点登录先决条件

- 为 Cisco Unified Communications Manager 群集配置了 DNS
- 一台身份提供程序 (IdP) 服务器
- 一台受 IdP 服务器信任且受您的系统支持的 LDAP 服务器

以下使用 SAML 2.0 的 Idp 针对 SAML SSO 功能进行了测试：

- OpenAM 10.0.1
- Microsoft® Active Directory® Federation Services 2.0 (AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

这些第三方应用程序必须满足以下配置要求：

- 必须在 IdP 上配置必需属性 “uid”。此属性必须与 Cisco Unified Communications Manager 中用于 LDAP 同步用户 ID 匹配。
- 必须同步所有参与 SAML SSO 的实体的时钟。有关同步时钟的信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》中的 “NTP 设置”，该文档位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。

管理 SAML 单点登录

启用 SAML 单点登录

注释 直到验证同步代理测试成功后，才能启用 SAML SSO。

开始之前

- 确保最终用户数据与 Unified Communications Manager 数据库同步。有关详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。
- 验证 Cisco Unified CM IM and Presence Service Cisco 同步代理服务是否已成功完成数据同步。通过选择 **Cisco Unified CM IM and Presence 管理** > **诊断** > **系统故障诊断程序**，检查此测试的状态。如果数据同步已成功完成，“验证同步代理是否已同步相关数据（例如设备、用户、许可信息）”测试显示“测试通过”结果。
- 确保至少一个 LDAP 同步用户添加到“标准 CCM 超级用户”组以允许访问 Cisco Unified CM 管理。有关详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。
- 要配置 IdP 与服务器之间的信任关系，必须从 IdP 获取信任元数据文件，并将该文件导入到所有服务器中。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**系统** > **SAML 单点登录**。

步骤 2 单击**启用 SAML SSO**。

步骤 3 看到通知您所有服务器连接都将重新启动的警告消息后，单击**继续**。

步骤 4 单击**浏览**查找并上传 IdP 元数据文件。

步骤 5 单击**导入 IdP 元数据**。

步骤 6 单击**下一步**。

步骤 7 单击**下载信任元数据文件集**将服务器元数据下载到系统。

步骤 8 将服务器元数据上传到 IdP 服务器。

步骤 9 单击**下一步**继续操作。

步骤 10 从有效管理员 ID 列表中选择具有管理权限的 LDAP 同步用户。

步骤 11 单击**运行测试**。

步骤 12 输入有效的用户名和密码。

步骤 13 看到成功消息之后，关闭浏览器窗口。

步骤 14 单击**完成**，等待 1 到 2 分钟，让 Web 应用程序重新启动。

为 Cisco Jabber iOS 版本配置 SSO 登录行为

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 要配置选择加入控制，在 SSO 配置部分，为 **iOS 的 SSO 登录行为** (SSO Login Behavior for iOS) 参数选择**使用本机浏览器**选项：

注释 **iOS 的 SSO 登录行为** (SSO Login Behavior for iOS) 参数包括以下选项：

- **使用嵌入式浏览器** — 如果启用此选项，Cisco Jabber 会使用嵌入式浏览器进行 SSO 验证。 使用此选项可允许版本 9 之前的 iOS 设备使用 SSO 而无需交叉启动进入本机 Apple Safari 浏览器。 默认情况下会启用此选项。
- **使用本机浏览器** — 如果启用此选项，Cisco Jabber 会在 iOS 设备上使用 Apple Safari 框架，在 MDM 部署中使用身份提供程序 (IdP) 执行基于证书的验证。

  注释 除了在受控的 MDM 部署中，不建议配置此选项，因为使用本机浏览器不如使用嵌入式浏览器安全。

步骤 3 单击**保存**。

升级后在 WebDialer 上启用 SAML 单点登录

执行这些任务以在升级后在 Cisco WebDialer 上重新激活 SAML 单点登录。 如果在启用 SAML 单点登录之前 Cisco WebDialer 已激活，则默认情况下 SAML 单点登录未在 Cisco WebDialer 上启用。

过程

	命令或操作	目的
步骤 1	禁用 Cisco WebDialer 服务，第 318 页	如果 Cisco WebDialer Web 服务已激活，请将其停用。
步骤 2	禁用 SAML 单点登录，第 319 页	如果 SAML 单点登录已启用，请将其禁用。
步骤 3	激活 Cisco WebDialer 服务，第 319 页	
步骤 4	启用 SAML 单点登录，第 316 页	

禁用 Cisco WebDialer 服务

如果 Cisco WebDialer Web 服务已激活，请将其停用。

过程

步骤 1 从 Cisco Unified 功能配置中，选择**工具** > **服务激活**。

步骤 2 从**服务器**下拉列表中，选择列出的 Cisco Unified Communications Manager 服务器。

步骤 3 从 **CTI 服务**中，取消选中 **Cisco WebDialer Web 服务**复选框。

步骤 4 单击**保存**。

下一步做什么

禁用 SAML 单点登录，第 319 页

禁用 SAML 单点登录

如果 SAML 单点登录已启用，请将其禁用。

开始之前

禁用 Cisco WebDialer 服务，第 318 页

过程

从 CLI，运行命令 **utils sso disable**。

下一步做什么

激活 Cisco WebDialer 服务，第 319 页

激活 Cisco WebDialer 服务

开始之前

禁用 SAML 单点登录，第 319 页

过程

步骤 1 从 Cisco Unified 功能配置中，选择**工具** > **服务激活**。

步骤 2 从**服务器**下拉列表中，选择列出的 Unified Communications Manager 服务器。

步骤 3 从 **CTI 服务**中，选中 **Cisco WebDialer Web 服务**复选框。

步骤 4 单击**保存**。

步骤 5 从 Cisco Unified 功能配置中，选择**工具** > **控制中心 - 功能服务**，以确认 CTI Manager 服务为活动状态且处于启动模式。

要使 WebDialer 正常运行，CTI Manager 服务必须为活动状态且处于启动模式。

下一步做什么

启用 SAML 单点登录，第 316 页

访问恢复 URL

使用恢复 URL 以绕过 SAML 单点登录并登录到“Cisco Unified Communications Manager 管理”和“Cisco Unified CM IM and Presence Service”界面进行故障诊断。 例如，在更改服务器的域或主机名之前启用恢复 URL。 登录恢复 URL 便于更新服务器元数据。

开始之前

- 只有具有管理权限的应用程序用户才能访问恢复 URL。
- 如果启用 SAML SSO，默认情况下启用恢复 URL。 您可以从 CLI 启用或禁用恢复 URL。 有关用于启用和禁用恢复 URL 的 CLI 命令的详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面指南》。

过程

在浏览器中，输入 `https://hostname:8443/ssosp/local/login`。

在域或主机名更改之后更新服务器元数据

域或主机名更改之后，SAML 单点登录将不起作用，直到您执行此程序。

注释 如果即使在执行此程序之后，仍然无法登录 **SAML 单点登录**窗口，请清除浏览器缓存，然后再次尝试登录。

开始之前

如果禁用恢复 URL，则它不会出现以让您绕过单点登录链接。 要启用恢复 URL，请登录 CLI 并执行以下命令：**utils sso recovery-url enable**。

过程

步骤 1 在您的 Web 浏览器的地址栏中，输入以下 URL：

`https://<Unified CM-server-name>`

其中 `<Unified CM-server-name>` 是服务器的主机名或 IP 地址。

步骤 2 单击**恢复 URL 以绕过单点登录 (SSO)**。

步骤 3 输入具有管理员角色的应用程序用户的凭证，然后单击**登录**。

步骤 4 从 Cisco Unified CM 管理中，选择**系统** > **SAML 单点登录**。

步骤 5 单击**导出元数据**，下载服务器元数据。

步骤 6 将服务器元数据文件上传到 IdP。

步骤 7 单击**运行测试**。

步骤 8 输入有效的用户 ID 和密码。

步骤 9 看到此成功消息之后，关闭浏览器窗口。

删除服务器后更新服务器元数据

在群集范围的 SSO 集成中将服务器从群集中删除后，必须重新导入元数据，以避免索引与 IdP 不匹配。

开始之前

注释 如果禁用恢复 URL，则它不会出现以让您绕过单点登录链接。 要启用恢复 URL，请登录 CLI 并执行以下命令：**utils sso recovery-url enable**。

过程

步骤 1 在您的 Web 浏览器的地址栏中，输入以下 URL：

`https://<Unified CM-server-name>`

其中 `<Unified CM-server-name>` 是服务器的主机名或 IP 地址。

步骤 2 单击**恢复 URL 以绕过单点登录 (SSO)**。

步骤 3 输入具有管理员角色的应用程序用户的凭证，然后单击**登录**。

步骤 4 在 Cisco Unified CM 管理中，选择 **系统** > **SAML 单点登录**。

步骤 5 单击**导出元数据**，下载服务器元数据。

步骤 6 将服务器元数据文件上传到 IdP。

步骤 7 单击**运行测试**。

步骤 8 输入有效的用户 ID 和密码。

步骤 9 看到此成功消息之后，关闭浏览器窗口。

手动配置服务器元数据

要在身份提供程序中为多个 UC 应用程序配置一个连接，您必须手动配置服务器元数据，同时配置身份提供程序与服务提供程序之间的信任圈。 有关配置信任圈的详细信息，请参阅 IdP 产品文档。

一般 URL 语法如下：

```
https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>
```

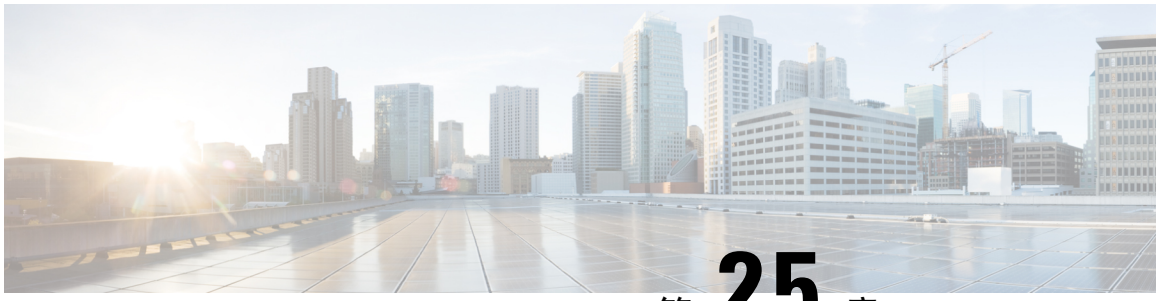
过程

要手动配置服务器元数据，请使用 Assertion Customer Service (ACS) URL。

示例：

示例 ACS URL：

```
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com"
index="0"/>
```



第 25 章

管理证书

证书概述

您的系统使用自签证书和第三方签名证书。 证书在您系统中的设备之间使用，以安全地验证设备、加密数据，并对数据进行散列，以确保其从源到目的地的完整性。 证书允许安全传输带宽、通信以及操作。

证书最重要的部分在于您知道并定义您的数据如何加密，并与诸如预期网站、电话或 FTP 服务器等实体共享。

当您的系统信任一个证书时，意味着您的系统上有一个预安装的证书，该证书声明它完全相信它与正确的目的地共享信息。 否则，它会终止这些点之间的通信。

为了信任证书，必须已经与第三方证书颁发机构 (CA) 建立信任。

您的设备必须知道，它们可以首先信任 CA 和中间证书，然后才能信任由称为安全套接字层 (SSL) 握手的消息交换提供的服务器证书。

注释 支持基于 EC 的 Tomcat 证书。此新证书称为 tomcat-ECDSA。有关详细信息，请参阅在 *Cisco Unified Communications Manager* 上的 *IM and Presence Service* 配置和管理“IM and Presence Service 部分”的增强型 TLS 加密。

默认情况下，Tomcat 接口上的 EC 密码处于禁用状态。您可以使用 Cisco Unified Communications Manager 或 IM and Presence Service 上的 **HTTPS 密码**企业参数启用它们。如果您更改此参数，必须在所有节点上重新启动 Cisco Tomcat 服务。

有关基于 EC 的证书的详细信息，请参阅 Cisco Unified Communications Manager 和 IM and Presence Service 发行说明中的“对认证解决方案通用标准的 ECDSA 支持”。

第三方签名证书或证书链

上传为应用程序证书签名的证书颁发机构的证书颁发机构根证书。如果次级证书颁发机构为应用程序证书签名，您必须上传次级证书颁发机构的证书颁发机构根证书。您还可以上传所有证书颁发机构证书的 PKCS#7 格式的证书链。

您可以使用相同的**上传证书**对话框上传证书颁发机构根证书和应用程序证书。当上传证书颁发机构根证书或仅包含证书颁发机构证书的证书链时，选择格式为“证书类型-信任”的证书名称。当上传应用程序证书或包含应用程序证书和证书颁发机构证书的证书链时，选择仅包含证书类型的证书名称。

例如，当上传 Tomcat 证书颁发机构证书或证书颁发机构证书链时，选择 **tomcat-信任**；当上传 Tomcat 应用程序证书或包含一个应用程序证书和证书颁发机构证书的证书链时，选择 **tomcat** 或 **tomcat-ECDSA**。

当上传 CAPF 证书颁发机构根证书时，该证书会被复制到 CallManager-信任存储库中，因此您无需单独为 CallManager 上传证书颁发机构根证书。

注释 成功上传第三方证书颁发机构签名的证书，会删除最近生成的用于获取签名证书的 CSR，并且会覆盖现有证书，包括第三方签名证书（如果已上传）。

注释 系统会自动将“tomcat-信任”、“CallManager-信任”和“电话-SAST-信任”证书复制到群集中的每个节点。

注释 您可以将目录信任证书上传到 tomcat-信任，这是 DirSync 服务在安全模式下工作所必需的。

第三方证书颁发机构的证书

若要使用第三方证书颁发机构颁发的应用程序证书，您必须向证书颁发机构或 PKCS#7 证书链（可辨别编码规则 [DER]，其中包含应用程序证书和证书颁发机构的证书）获取签署的应用程序证书和证书颁发机构根证书。请检索有关向您的证书颁发机构获取这些证书的信息。证书颁发机构之间的流程各不相同。 签名算法必须使用 RSA 加密。

Cisco Unified Communications 操作系统以隐私增强邮件 (PEM) 编码格式生成 CSR。 系统接受 DER 和 PEM 编码格式的证书和 PEM 格式的 PKCS#7 证书链。 对于除证书权限代理功能 (CAPF) 之外的所有证书类型，您必须获取和上传证书颁发机构根证书和每个节点上的应用程序证书。

对于CAPF，获取并上传证书颁发机构根证书和仅在第一个节点上的应用程序证书。 CAPF 和Unified Communications ManagerCSR 中包含的扩展必须包括在向证书颁发机构申请应用程序证书的请求中。如果您的证书颁发机构不支持扩展请求机制，则您必须启用 X.509 扩展，如下所述：

- CAPF CSR 使用以下扩展：

```
X509v3 Extended Key Usage: TLS Web Server Authentication X509v3 Key Usage:
Digital Signature, Certificate Sign
```

- 适用于 Tomcat 的 CSR 和 Tomcat-ECDSA 使用以下扩展：

注释 Tomcat 或 Tomcat-ECDSA 不要求密钥协议或 IPsec 终端系统密钥用法。

```
X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client
Authentication, IPSec End System X509v3 Key Usage: Digital Signature, Key
Encipherment, Data Encipherment, Key Agreement
```

- 适用于 IPsec 的 CSR 使用以下扩展：

```
 X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client
Authentication, IPSec End System X509v3 Key Usage: Digital Signature, Key
Encipherment, Data Encipherment, Key Agreement
```

- 适用于 Unified Communications Manager 的 CSR 使用以下扩展：

```
X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client
Authentication X509v3 Key Usage: Digital Signature, Key Encipherment, Data
Encipherment, Key Agreement
```

- IM and Presence Service cup 和 cup-xmpp 证书的 CSR 使用以下扩展名：

```
X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client
Authentication, IPSec End System X509v3 Key Usage: Digital Signature, Key
Encipherment, Data Encipherment, Key Agreement,
```

注释 您可以为您的证书生成CSR并让具有SHA256签名的第三方证书颁发机构对其进行签名。然后，您可以将该签名证书上传回Unified Communications Manager，允许Tomcat和其他证书支持SHA256。

证书签名请求密钥使用情况扩展

下表显示了Unified Communications Manager和IM and Presence Service CA证书的证书签名请求(CSR)的密钥使用扩展。

表 *79: Cisco Unified Communications Manager CSR* 密钥使用扩展

	多服务器	扩展密钥使用			密钥使用				
		服务器身份验证 (1.3.6.1.5.5.7.3.1)	客户端验证 (1.3.6.1.5.5.7.3.2)	IP安全端系统 (1.3.6.1.5.5.7.3.5)	数字签名	密钥加密	数据加密	密钥证书签名	密钥协议
CallManager CallManager-ECDSA	Y	Y	Y		Y	N	Y		
CAPF（仅发布方）	N	Y	N		Y	N		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	N	Y		
TVS	N	Y	Y		Y	Y	Y		

表 *80: IM and Presence Service CSR* 密钥使用扩展

	多服务器	扩展密钥使用			密钥使用				
		服务器身份验证 (1.3.6.1.5.5.7.3.1)	客户端验证 (1.3.6.1.5.5.7.3.2)	IP安全端系统 (1.3.6.1.5.5.7.3.5)	数字签名	密钥加密	数据加密	密钥证书签名	密钥协议
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

注释 确保“数据加密”位未作为 CA 签名证书过程的一部分进行更改或删除。

显示证书

使用“证书列表”页上的过滤器选项，可以根据证书的通用名称、到期日期、密钥类型和使用来排序和查看证书列表。 这样，过滤选项可让您有效地对数据进行排序、查看和管理。

从 Unified Communications Manager 版本 14 中，您可以选择使用选项来排序和查看身份或信任证书列表。

过程

步骤 1 从 Cisco Unified OS 管理中，选择**安全** > **证书管理**。
“证书列表”页将会显示。

步骤 2 从**查找证书列表位置**下拉列表中，选择所需的过滤器选项，在**查找**字段中输入搜索项目，然后单击**查找**按钮。

例如，要仅查看身份证书，请从**查找证书列表位置**下拉列表中选择**使用**，在**查找**字段中输入身份，然后单击**查找**按钮。

证书显示 14SU2 和更高版本已修改 BCFIPS 提供商的数据。

14SU1 之前的标记名称	**从 14SU2 开始的标记名称**
颁发机构名称	IssuerDN
有效期	开始日期
至	最终日期
主题名称	SubjectDN
密钥	公共密钥
键值	模量

注释 X509 分机以 OID 名称显示，而不是显示实际的密钥使用名称。

下载证书

提交 CSR 请求时，使用下载证书任务复制证书或上传证书。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 指定搜索条件，然后单击**查找**。

步骤 3 选择所需的文件名，然后单击**下载**。

安装中间证书

要安装中间证书，您必须首先安装根证书，然后上传签名证书。 仅当证书颁发机构在证书链中提供了签名证书及多个证书时，才需要执行此步骤。

过程

步骤 1 从 Cisco Unified 操作系统管理中，单击**安全** > **证书管理**。

步骤 2 单击**上传证书 / 证书链**。

步骤 3 从**证书目的**下拉列表中选择适当的信任存储库以安装根证书。

步骤 4 输入所选证书用途的说明。

步骤 5 通过执行以下操作之一选择要上传的文件：

- 在**上传文件**文本框中，输入文件的路径。
- 单击**浏览**并导航至文件，然后单击**打开**。

步骤 6 单击**上传**。

步骤 7 安装客户证书后，使用 FQDN 访问 Cisco Unified Intelligence Center URL。 如果使用 IP 地址访问 Cisco Unified Intelligence Center，即使成功安装了自定义证书，您也会看到消息“单击此处以继续”。

注释
- 上传 Tomcat 证书时，应重新启动 TFTP 服务。 否则 TFTP 会继续提供缓存的旧自签 tomcat 证书。

删除信任证书

信任的证书是您可以删除的唯一一种证书类型。 您无法删除由您的系统生成的自签证书。

⚠

注意 删除证书可能会影响您的系统操作。 如果证书是现有证书链的一部分，也可能会破坏证书链。 通过**证书列表**窗口中相关证书的用户名和主题名称来验证此关系。 您无法撤销此操作。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 使用**查找**控件过滤证书列表。

步骤 3 选择证书的文件名。

步骤 4 单击**删除**。

步骤 5 单击**确定**。

注释
- 如果您删除 “CAPF-trust”、“tomcat-trust”、“CallManager-trust” 或 “Phone-SAST-trust” 证书类型，证书将跨群集中的所有服务器删除。
- 如果您将证书导入到 CAPF-trust 中，它将仅在该特定节点上启用，并且不会跨群集复制。

重新生成证书

建议您在证书到期之前重新生成证书。 当证书即将到期时，您将在 RTMT（系统日志查看器）和电子邮件通知中收到警告。

不过，您也可以重新生成过期的证书。 在下班时间执行此任务，因为您必须重新启动电话并重启服务。 您只能重新生成在 Cisco Unified 操作系统管理中被列为“cert”类型的证书。

⚠

注意 重新生成证书可能影响您的系统操作。 重新生成证书会覆盖现有证书，包括第三方签名证书（如果已上传）。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

输入搜索参数以查找证书并查看其配置详细信息。 系统会在**证书列表**窗口中显示与所有条件匹配的记录。

单击证书详细信息页面中的**重新生成**按钮，此时将会重新生成具有相同密钥长度的自签证书。

注释 重新生成证书时，**证书说明**字段将不会更新，直到您关闭**重新生成**窗口并打开新生成的证书。

单击**生成自签证书**以重新生成密钥长度为 3072 或 4096 的自签证书。

步骤 2 配置**生成新的自签名证书**窗口中的字段。 有关这些字段及其配置选项的更多信息，请参阅联机帮助。

步骤 3 单击**生成**。

步骤 4 重新启动受重新生成的证书影响的所有服务。 有关详细信息，请参阅证书名称和说明，第 330 页。

步骤 5 重新生成 CAPF、ITLRecovery 证书或 CallManager 证书之后，更新 CTL 文件（如配置有）。

注释 重新生成证书后，您必须执行系统备份，以使最新备份包含重新生成的证书。 如果您的备份不包含重新生成的证书，而您要执行系统恢复任务，则您必须手动解锁系统中的每部电话，以使电话可以注册。

证书名称和说明

下表说明您可以重新生成的系统安全证书，以及必须重新启动的相关服务。有关重新生成 TFTP 证书的信息，请参阅《*Cisco Unified Communications Manager* 安全指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

表 *81:* 证书名称和说明

名称	说明	相关服务
tomcat tomcat-ECDSA	此证书由 WebServices、Cisco DRF 服务和 Cisco CallManager 服务在 SIP Oauth 模式启用时使用。	Cisco Tomcat 服务、CallManager 服务、H 以及 Cisco 灾难恢复 Local 和 Master 服务
ipsec	此自签根证书是在安装期间为与 Unified Communications Manager、MGCP、H.323 和 IM and Presence Service 的 IPsec 连接生成的。	IPsec 服务
CallManager CallManager-ECDSA	此功能用于 SIP、SIP 干线、SCCP、TFTP 等。	CallManager - HAProc CallManager-ECDSA CallManager 服务
CAPF	由运行在 Unified Communications Manager 发布方上的 CAPF 服务使用。此证书用于颁发 LSC 到终端（在线和离线 CAPF 模式除外）	不适用
TVS	此功能由信任验证服务使用，可用作电话在服务器证书更改时的辅助信任验证机制。	不适用

注释 在“安全参数”部分的“证书更新”下，引入了新的企业参数“电话相互作用”，用于在 TVS、CAPF 或 TFTP 证书中的任意一个更新时手动或自动重置电话。此参数默认设置为自动重置电话。

重新生成 OAuth 刷新登录的密钥

使用此程序以使用命令行界面重新生成加密密钥和签名密钥。 仅当 Cisco Jabber 用来在 Unified Communications Manager 中进行 OAuth 验证的加密密钥或签名密钥已经被入侵时，才完成此任务。 签名密钥是一种不对称密钥，基于 RSA，而加密秘钥是一种对称密钥。

完成此任务后，使用这些秘钥的当前访问和刷新令牌将失效。

我们建议您在非高峰时段完成此任务，以将对最终用户的影响降至最低。

加密密钥仅可通过下面的 CLI 重新生成，但您也可以使用发布方的 Cisco Unified 操作系统管理 GUI 重新生成签名密钥。 选择**安全** > **证书管理**，然后选择 **AUTHZ** 证书，并单击**重新生成**。

过程

步骤 1 从 Unified Communications Manager 发布方节点登录到**命令行**界面。

步骤 2 如果想要重新生成加密密钥：

a) 运行 `set key regen authz encryption` 命令。

b) 输入 `yes`。

步骤 3 如果想要重新生成签名密钥：

a) 运行 `set key regen authz signing` 命令。

b) 输入 `yes`。
Unified Communications Manager 发布方节点会重新生成密钥并将新密钥复制到所有 Unified Communications Manager 群集节点，包括任何本地 IM and Presence Service 节点。

您必须重新生成新密钥并在所有 UC 群集上同步：

- IM and Presence 中心群集 — 如果您有一个 IM and Presence 集中式部署，您的 IM and Presence 节点会运行在与您的电话分离的群集上。 在这种情况下，在 IM and Presence Service 中心群集的 Unified Communications Manager 发布方节点上重复此程序。
- Cisco Expressway 或 Cisco Unity Connection — 同样在那些群集上重新生成秘钥。 有关详细信息，请参阅您的 Cisco Expressway 和 Cisco Unity Connection 文档。

注释 在以下情况下，您必须重新启动 Cisco XCP 验证服务：

- 重新生成 Authz 证书时
- 在 IM and Presence 管理员控制台中向集中式部署新增条目时

上传证书或证书链

上传您希望您的系统信任的任何新证书或证书链。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 单击**上传证书/证书链**。

步骤 3 从**证书目的**下拉列表中选择证书名称。

步骤 4 通过执行以下操作之一选择要上传的文件：

- 在**上传文件**文本框中，输入文件的路径。
- 单击**浏览**，导航至文件，然后单击**打开**。

步骤 5 要将文件上传到服务器，请单击**上传文件**。

注释 上传证书后，重新启动受影响的服务。 当服务器恢复时，您可以访问 CCMAdmin 或 CCMUser GUI，检验是否在使用您新添加的证书。

管理第三方证书颁发机构的证书

此任务流程提供第三方证书流程的概述，以及对序列中每个步骤的参考。 您的系统支持由第三方证书颁发机构使用 PKCS # 10 证书签名请求 (CSR) 签发的证书。

过程

	命令或操作	目的
步骤 1	生成证书签名请求， 第 333 页	生成证书签名请求 (CSR) 是一块加密的文本，其中包含证书应用程序信息、公钥、组织名称、通用名称、所在地，以及国家/地区。证书颁发机构使用此 CSR 为您的系统生成信任证书。
步骤 2	下载证书签名请求， 第 333 页	下载所生成的 CSR 并准备好将其提交给您的证书颁发机构。
步骤 3	请参阅您的证书颁发机构文档。	向您的证书颁发机构获取应用程序证书。
步骤 4	请参阅您的证书颁发机构文档。	向您的证书颁发机构获取根证书。
步骤 5	将证书颁发机构签名的 CAPF 根证书添加到信任存储库 ， 第 334 页	将根证书添加到信任存储库中。当使用证书颁发机构签名的 CAPF 证书时，请执行此步骤。
步骤 6	上传证书或证书链， 第 331 页	将证书颁发机构根证书上传到节点。

	命令或操作	目的
步骤 7	如果您更新了 CAPF 或 Cisco Unified Communications Manager 的证书，请生成新的 CTL 文件。	请参阅《*Cisco Unified Communications Manager* 安全指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。 上传第三方签名的 CAPF 或 CallManager 证书之后，重新运行 CTL 客户端（如配置有）。
步骤 8	重新启动服务，第 334 页	重新启动受新证书影响的服务。对于所有证书类型，重新启动相应的服务（例如，如果您更新了 Tomcat 或 Tomcat-ECDSA 证书，则重新启动 Cisco Tomcat 服务）。

生成证书签名请求

生成证书签名请求 (CSR) 是一块加密的文本，其中包含证书应用程序信息、公钥、组织名称、通用名称、所在地，以及国家/地区。证书颁发机构使用此 CSR 为您的系统生成信任证书。

注释 如果您生成新的 CSR，将覆盖任何现有的 CSR。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 单击**生成 CSR**。

步骤 3 配置**生成证书签名请求**窗口中的字段。 请参阅联机帮助，了解有关字段及其配置选项的更多信息。

步骤 4 单击**生成**。

下载证书签名请求

下载所生成的 CSR 并准备好将其提交给您的证书颁发机构。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 单击**下载 CSR**。

步骤 3 从**证书目的**下拉列表中选择证书名称。

步骤 4 单击**下载 CSR**。

步骤 5 （可选） 如果收到提示，请单击**保存**。

将证书颁发机构签名的 CAPF 根证书添加到信任存储库

当使用证书颁发机构签名的 CAPF 证书时，请将根证书添加到 Unified Communications Manager 信任存储库。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 单击**上传证书/证书链**。

步骤 3 在**上传证书/证书链**弹出窗口中，从**证书用途**下拉列表中选择 **CallManager-trust** 并浏览至证书颁发机构签名的 CAPF 根证书。

步骤 4 证书出现在**上传文件**字段中后，单击**上传**。

重新启动服务

如果您的系统需要您在群集中的特定节点上重新启动任何功能或网络服务，请使用此程序。

过程

步骤 1 根据您要重新启动的服务类型，执行以下任务之一：

- 选择**工具** > **控制中心 - 功能服务**。
- 选择**工具** > **控制中心 - 网络服务**。

步骤 2 从**服务器**下拉列表中选择您的系统节点，然后单击**前往**。

步骤 3 单击要重新启动的服务旁边的单选按钮，然后单击**重新启动**。

步骤 4 看到重新启动需要一些时间的消息之后，单击**确定**。

通过在线证书状态协议吊销证书

Unified Communications Manager 预配置了用于监控证书吊销的 OCSP。 系统将检查证书状态以确认在预定时间间隔的有效性，并且每次都有上传的证书。

在线证书状态协议(OCSP)可帮助管理员管理其系统的证书要求。 OCSP配置后，它将提供简单、安全和自动的方法来检查证书的有效性并实时吊销过期的证书。

对于启用 Common Criteria 模式的 FIPS 部署，OCSP 还可帮助确保您的系统符合 Common Criteria 要求。

验证检查

Unified Communications Manager 会检查证书状态并确认有效性。

证书按以下方式进行验证：

- Unified Communications Manager 使用委托的信任模型 (DTM) 并检查根 CA 或中间 CA 的 OCSP 签名属性。 根 CA 或中间 CA 必须对 OCSP 证书签名，才能检查状态。 如果委托的信任模型失败，Unified Communications Manager 会退回到信任响应者模型 (TRP)，并使用来自 OCSP 服务器的指定 OCSP 响应签名证书来验证证书。

注释 OCSP 响应器必须运行以检查证书的吊销状态。

- 在**证书吊销**窗口中启用 OCSP 选项，以提供最安全的方式实时检查证书吊销。 从选项中选择以使用来自证书或者所配置 OCSP URI 的 OCSP URI。 有关手动 OCSP 配置的详细信息，请参阅配置通过 OCSP 吊销证书。

注释 对于叶证书，TLS 客户端（例如 syslog、FileBeat、SIP、ILS、LBM 等）会将 OCSP 请求发送到 OCSP 响应器，并从 OCSP 响应器实时接收证书吊销响应。

执行验证并且 Common Criteria 模式设为“开”后，系统将为证书返回以下状态之一。

- **良好**--状态为**良好**表示对状态查询的响应积极。 此积极响应至少表示证书未被吊销，但不一定意味着证书曾被颁发，或者响应的生成时间在证书的有效期内。 响应分机可用于传达响应器就证书状态所做的断言的其他信息，例如关于发行、有效期等的肯定声明。
- **已吊销**--状态为**已吊销**表示证书已被吊销（永久或临时（保留））。
- **未知**--状态为**未知**表示 OCSP 响应器不知道所请求的证书。

注释 在 Common Criteria 模式下，如果状态为**已吊销**和**未知**，连接将失败；未启用 Common Criteria 时，如果状态为**未知**，连接将成功。

证书监控任务流程

完成以下任务可将系统配置为自动监控证书状态和到期时间。

- 证书即将到期时通过电子邮件通知您。
- 吊销到期的证书。

过程

	命令或操作	目的
步骤 1	配置证书监控通知，第 336 页	配置自动证书监控。 当证书即将到期时，系统会定期检查证书状态并向您发送电子邮件。
步骤 2	配置通过 OCSP 吊销证书，第 337 页	配置 OCSP，以便系统自动吊销到期的证书。

配置证书监控通知

为 Unified Communications Manager 或 IM and Presence Service 配置自动证书监控。 当证书即将到期时，系统会定期检查证书状态并向您发送电子邮件。

注释 **Cisco 证书到期监控**网络服务必须运行。 此服务默认启用，但您也可以在 Cisco Unified 功能配置中手动确认该服务是否在运行，方法是选择**工具 > 控制中心 - 网络服务**，然后验证 **Cisco 证书到期监控服务**状态是否是**正在运行**。

过程

步骤 1 登录到 Cisco Unified 操作系统管理（适用于 Unified Communications Manager 证书监控）或 Cisco Unified IM and Presence 管理（适用于 IM and Presence Service 证书监控）。

步骤 2 选择**安全性 > 证书监控**。

步骤 3 在**通知开始时间**字段中输入一个数值。 此值表示证书到期前系统开始通知您即将到期的天数。

步骤 4 在**通知频率**字段中，输入通知的频率。

步骤 5 可选。 选中**启用电子邮件通知**复选框以让系统发送证书即将到期的电子邮件通知。

步骤 6 选中**启用 LSC 监控**复选框以在证书状态检查种包含 LSC 证书。

步骤 7 在**电子邮件 ID** 字段中，输入您希望系统将通知发送到的电子邮件地址。 您可以输入多个电子邮件地址，用分号分隔。

步骤 8 单击**保存**。

注释　默认情况下，证书监控服务每 24 小时运行一次。 当重新启动证书监控服务时，它将启动服务，然后计算下一个计划，仅在24个小时后运行。即使证书接近七天的到期日期，间隔也不会改变。 当证书已经过期或将在一天内过期时，服务会每 1 小时运行一次。

下一步做什么

配置在线证书状态协议 (OCSP)，以便系统自动吊销到期的证书。 有关详细信息，请参阅配置通过 OCSP 吊销证书，第 337 页

配置通过 OCSP 吊销证书

启用在线证书状态协议 (OCSP) 定期检查证书状态并自动吊销到期的证书。

开始之前

确保您的系统具有是 OCSP 检查所需的证书。 您可以使用通过 OCSP 响应属性配置的根证书或中间 CA 证书，也可以使用已上传到 tomcat-trust 的指定 OCSP 签名证书。

过程

步骤 1 登录到 Cisco Unified 操作系统管理（适用于 Unified Communications Manager 证书吊销）或 Cisco Unified IM and Presence 管理（适用于 IM and Presence Service 证书吊销）。

步骤 2 选择**安全性** > **证书吊销**。

步骤 3 选中**启用 OCSP** 复选框，然后执行以下任务之一：

- 如果要为 OCSP 检查指定 OCSP 响应器，选择**使用配置的 OCSP URI** 按键并在 **OCSP 配置的 URI** 字段中输入响应器的 URI。
- 如果采用 OCSP 响应器 URI 配置证书，选择**使用来自证书的 OCSP URI** 按键。

步骤 4 选中**启用吊销检查**复选框。

步骤 5 使用吊销检查的间隔时间填写**检查间隔**字段。

步骤 6 单击**保存**。

步骤 7 可选。 如果您有 CTI、IPsec 或 LDAP 链接，除上述步骤之外，还必须完成以下操作，以便为这些长期连接启用 OCSP 吊销支持：

a) 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。
b) 在**证书撤消和过期**下，将**证书有效性检查**参数设置为**真**。
c) 配置**有效性检查频率**参数的值。

注释　**证书吊销**窗口中**启用吊销检查**参数的时间间隔值优先于**有效性检查频率**企业参数的值。

d) 单击**保存**。

对证书错误进行故障诊断

开始之前

如果您在尝试从 IM and Presence Service 节点或来自 Unified Communications Manager 节点的 IM and Presence Service 功能访问 Unified Communications Manager 服务时遇到错误，问题的根源在于 tomcat-trust 证书。错误消息 `Connection to the Server cannot be established (unable to connect to Remote Node)`（无法建立与服务器的连接（无法连接到远程节点））出现在以下功能配置界面窗口中：

- **服务激活**
- **控制中心 - 功能服务**
- **控制中心 - 网络服务**

使用此程序帮助您解决证书错误。从第一个步骤开始，如有必要，继续后面的步骤。有时，您可能只需要完成第一个步骤便可解决错误；有时则必须完成所有步骤。

过程

步骤 1 从 Cisco Unified 操作系统管理中，确认存在必需的 tomcat-信任证书：**安全** > **证书管理**。

如果所需的证书不存在，请等待 30 分钟，然后再次检查。

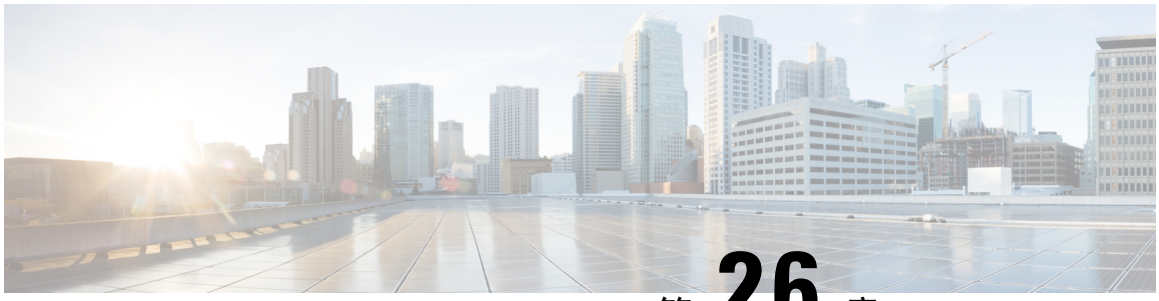
步骤 2 选择要查看其信息的证书。 确认内容与远程节点上的相应证书匹配。

步骤 3 从 CLI 中，重新启动 Cisco 群集间同步代理服务：**utils service restart Cisco Intercluster Sync Agent**。

步骤 4 Cisco 群集间同步代理服务重新启动后，重新启动 Cisco Tomcat 服务：**utils service restart Cisco Tomcat**。

步骤 5 等待 30 分钟。 如果前面的步骤不能解决证书错误，而 tomcat-信任证书存在，请删除该证书。 删除证书后，您必须通过以下方法手动交换证书：下载用于每个节点的 Tomcat 和 Tomcat-ECDSA 证书并将其作为 tomcat 信任证书上传到其对等机。

步骤 6 证书交换完成后，重新启动每台受影响服务器上的 Cisco Tomcat：**utils service restart Cisco Tomcat**。



第 26 章

管理批量证书

管理批量证书

如果您想在群集之间共享一组证书，可以使用批量证书管理。 对于需要在群集之间建立信任的系统功能，例如跨群集分机移动，此步骤是必需的。

过程

	命令或操作	目的
步骤 1	导出证书，第 339 页	此程序为群集中的所有节点创建包含证书的 PKCS12 文件。
步骤 2	导入证书，第 340 页	将证书导回到主群集和远程（访问）群集中。

导出证书

此程序为群集中的所有节点创建包含证书的 PKCS12 文件。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **批量证书管理**。

步骤 2 配置主群集和远程群集都可以到达的 TFTP 服务器的设置。 请参阅联机帮助，了解有关字段及其配置选项的信息。

步骤 3 单击**保存**。

步骤 4 单击**导出**。

步骤 5 在**批量证书导出**窗口中，为**证书类型**字段选择**全部**。

步骤 6 单击**导出**。

步骤 7 单击**关闭**。

注释 执行批量证书导出时，证书随后会如下所示上传到远程群集：

- CAPF 证书作为 CallManager-trust 上传
- Tomcat 证书作为 Tomcat-trust 上传
- CallManager 证书作为 CallManager-trust 上传
- CallManager 证书作为 Phone-SAST-trust 上传
- ITLRecovery 证书作为 PhoneSast-trust 和 CallManager-trust 上传

如果是自签证书，并且在另一个群集中没有公共信任，将执行上述步骤。 如果存在公共信任或相同的签名者，则不需要导出所有证书。

导入证书

将证书导回到主群集和远程（访问）群集中。

注释 使用批量证书管理导入证书会导致电话重置。

开始之前

“导入”按钮出现之前，您必须完成以下活动：

- 将证书从至少两个群集导出到 SFTP 服务器。
- 合并导出的证书。

过程

步骤 1 从从 Cisco Unified 操作系统管理中，选择**安全** > **批量证书管理** > **导入** > **批量证书导入**。

步骤 2 从**证书类型**下拉列表中，选择**全部**。

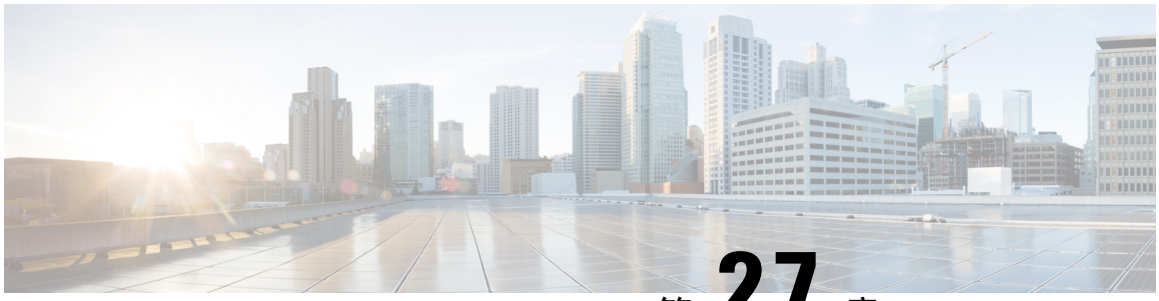
步骤 3 选择**导入**。

注释 执行批量证书导入时，证书随后会如下所示上传到远程群集：

- CAPF 证书作为 CallManager-trust 上传
- Tomcat 证书作为 Tomcat-trust 上传
- CallManager 证书作为 CallManager-trust 上传
- CallManager 证书作为 Phone-SAST-trust 上传
- ITLRecovery 证书作为 PhoneSast-trust 和 CallManager-trust 上传

注释　以下证书类型决定重新启动的电话：

- Callmanager - 所有电话，前提是证书所属的节点上激活 TFTP 服务。
- TVS - 部分电话，基于 Callmanager 组成员身份。
- CAPF - 所有电话，前提是激活了 CAPF。



第 27 章

管理 IPSec 策略

IPsec 策略概述

IPsec 是一个框架，它通过使用加密安全服务确保私人、安全的 IP 网络通信。 IPsec 策略用于配置 IPsec 安全服务。 策略为您网络中的大多数流量类型提供不同级别的保护。 您可以配置 IPsec 策略，以满足计算机、组织单位 (OU)、域、站点或全球企业的安全需求。

配置 IPsec 策略

注释

- 由于在系统升级过程中对IPsec策略所做的任何更改都会丢失，所以在升级期间不要修改或创建IPsec 策略。
- IPsec 需要双向部署，或每个主机（或网关）一个对等机。
- 当您在两个节点上部署 IPsec 策略时，Unified Communications Manager一个 IPsec 策略协议设置为 “ANY”，另一个 IPsec 策略协议设置为 “UDP” 或 “TCP”，如果从使用 “ANY” 协议的节点运行验证，可能会导致漏报。
- IPsec，尤其是使用加密时，会影响系统性能。
- 如果在当前或升级版本上配置了IPsec策略，但没有在基本版本上配置，请确保在尝试将此版本切换到基本版本时删除或禁用IPsec策略。 这是因为IPsec策略将仅在其中一个节点上配置，而在切换回这两个版本之前，其他节点不会配置 IPsec 策略。 否则，这会导致连接问题。
- Unified CM 节点重新启动后，如果 IPsec 连接未启动，请确保使用命令 **utils ipsec restart** 重新启动 IPsec 服务，以成功建立 IPsec 连接。 此解决方法是用来在建立网络连接之前缓解 IPsec 服务重新启动的任何问题。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **IPSec 配置**。

步骤 2 单击**新增**。

步骤 3 配置 **IPSEC 策略配置**窗口中的字段。 请参阅联机帮助，了解有关字段及其配置选项的更多信息。

步骤 4 单击**保存**。

步骤 5 （可选） 要验证 IPsec，选择**服务** > **Ping**，选中**验证 IPsec** 复选框，然后单击 **Ping**。

选中 IPsec 证书

使用此过程选中 IPsec 证书：

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **管理证书**。

步骤 2 指定搜索条件，然后单击**查找**。

步骤 3 搜索 IPsec 证书（分别登录到发布方和订阅方节点）。

注释 通常，无法在发布方节点上查看订阅方节点 IPsec 证书。 但是，可以在 IM-P 节点的订阅方节点上查看发布方节点 IPsec 证书。

若要启用 IPsec 连接，必须使用来自一个节点的 CA 签名的 IPsec 证书作为另一个节点上的 **IPsec-信任**证书。

在将新证书上载到 **IPsec-信任**之前，必须删除 **IPsec-信任**中具有相同公用名称的以前的证书

管理 IPsec 策略

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **IPSEC 配置**。

步骤 2 要显示、启用或禁用策略，请执行这些步骤：

a) 单击策略名称。

b) 要启用或禁用策略，请选中或取消选中**启用策略**复选框。

c) 单击**保存**。

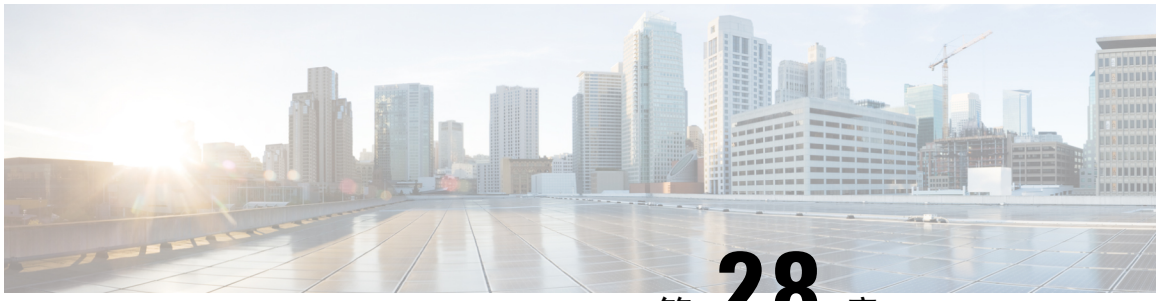
注释 在禁用 IPsec 策略后，请使用 **show network cluster** 命令来检查集群的身份验证状态。如果在其间创建和禁用 IPsec 策略的节点未经过身份验证，请确保使用 **utils ipsec restart** 命令在两个节点上重新启动 IPsec 服务。

步骤 3 要删除一项或多项策略，请执行这些步骤：

a) 选中您要删除的各项策略旁边的复选框。

您可以单击**全部选择**以选择所有策略，或单击**全部清除**以清除所有复选框。

b) 单击**删除选定项**。



第 28 章

管理凭证策略

凭证策略和验证

验证功能会验证用户、更新凭证信息、跟踪和记录用户事件和错误、记录凭证更改历史记录，以及加密或解密数据存储的用户凭证。

系统始终根据 Unified Communications Manager 数据库验证应用程序用户密码和最终用户个人识别码。 系统可以根据公司目录或数据库验证最终用户密码。

如果系统与公司目录同步，Unified Communications Manager或轻量级目录访问协议 (LDAP) 中的验证功能可以验证密码：

- 启用 LDAP 验证时，用户密码和凭证策略不适用。 这些默认值会应用于通过目录同步（DirSync 服务）创建的用户。
- 禁用 LDAP 验证后，系统根据数据库验证用户凭证。 通过此选项，您可以分配凭证策略、管理验证事件和管理密码。 最终用户可以通过电话用户界面更改密码和个人识别码。

凭证策略不适用于操作系统用户或 CLI 用户。 这些管理员使用操作系统支持的标准密码验证程序。

在数据库中配置用户后，系统将在数据库中存储用户凭证的历史记录，以防用户在收到提示其更改其凭证的消息时输入之前用过的信息。

凭证策略的 JTAPI 和 TAPI 支持

由于 Cisco Unified Communications Manager Java 电话应用程序编程接口 (JTAPI) 和电话应用程序编程接口 (TAPI) 支持分配给应用程序用户的凭证策略，所以开发者必须创建应用程序以应对凭证策略执行时的密码过期、个人识别码过期以及锁定返回码。

应用程序使用 API 验证数据库或公司目录，而不管应用程序使用何种验证模型。

有关开发人员 JTAPI 和 TAPI 的详细信息，请参阅开发人员手册，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html。

配置凭证策略

凭证策略适用于应用程序用户和最终用户。 可将密码策略分配给最终用户和应用程序用户，将个人识别码策略分配给最终用户。 “凭证策略默认值配置”列出这些组的策略分配。 向数据库添加新用户时，系统会分配默认策略。 您可以更改分配的策略并管理用户验证事件。

注释 确保 CTI 应用用户的凭证策略设置下的允许非活动天数参数设置为 0（无限制）。 否则，应用程序用户会意外地变为非活动状态，并且 CTI 应用在重新启动后可能无法连接到 Unified CM。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **凭证策略**。

步骤 2 请执行以下步骤之一：

- 单击**查找**并选择一个现有的凭证策略。
- 单击**新增**以创建新的凭证策略。

步骤 3 填写**凭证策略配置**窗口中的字段。 请参阅联机帮助，了解有关字段及其配置设置的更多信息。

步骤 4 单击**保存**。

配置凭证策略默认设置

安装时，Cisco Unified Communications Manager 将静态默认凭证策略分配给用户组。 它不提供默认凭证。 您的系统提供了一些选项来分配新的默认策略，以及为用户配置新的默认凭证和凭证要求。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **凭证策略默认设置**。

步骤 2 从**凭证策略**下拉列表框中，选择此组的凭证策略。

步骤 3 在**更改凭证**和**确认凭证**配置窗口中输入密码。

步骤 4 如果您不希望用户可以更改此凭证，请选中**用户无法更改**复选框。

步骤 5 如果您想将此凭证用作临时凭证，最终用户必须在下次登录时更改，请选中**用户必须在下次登录时更改**复选框。

注释 请注意，如果选中此复选框，您的用户将无法使用个人目录服务更改个人识别码。

步骤 6 如果您不希望凭证过期，请选中**没有过期**复选框。

步骤 7 单击**保存**。

监控验证活动

系统显示最近的验证结果，例如上次黑客尝试时间以及登录尝试失败计数。

系统将为以下凭证策略事件生成日志文件条目：

- 验证成功
- 验证失败（密码错误或未知）
- 由于以下原因验证失败：
  - 管理锁定
  - 黑客行为锁定（登录失败锁定）
  - 过期软锁定（过期的凭证）
  - 非活动锁定（凭证有一段时间未使用）
  - 用户必须更改（凭证设置为“用户必须更改”）
  - LDAP 非活动（切换到 LDAP 验证且 LDAP 非活动）
- 用户凭证更新成功
- 用户凭证更新失败

注释 如果对最终用户密码使用 LDAP 验证，LDAP 仅跟踪验证成功和失败。

所有事件消息都包含字符串 “ims-auth” 和尝试验证的用户 ID。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **最终用户**。

步骤 2 输入搜索条件，单击**查找**，然后从结果列表中选择用户。

步骤 3 单击**编辑凭证**以查看用户的验证活动。

下一步做什么

您可以通过 Cisco Unified 实时监控工具 (Unified RTMT) 查看日志文件。还可以将捕获的事件收集到报告中。有关如何使用 Unified RTMT 的详细步骤，请参阅《*Cisco Unified* 实时监控工具管理指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

配置凭证缓存

启用凭证缓存以提高系统效率。 您的系统不必为每一个单点登录请求执行数据库查找或调用存储的程序。 关联的凭证策略不会执行，直至缓存时间到期。

此设置适用于所有调用用户验证的 Java 应用程序。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 根据需要执行以下任务：

- 将**启用缓存**企业参数设置为**真**。 启用此参数后，Cisco Unified Communications Manager 会使用缓存的凭证最多 2 分钟。
- 将**启用缓存**企业参数设为**假**以禁用缓存，这样系统就不会使用缓存的凭证进行验证。 对于 LDAP 验证，系统会忽略此设置。 凭证缓存要求每位用户具备最小额外内存量。

步骤 3 单击**保存**。

管理会话终止

管理员可以遵照此程序终止特定于每个节点的用户的活动登录会话。

注释

- 权限级别为 4 的管理员才可终止会话。
- 会话管理终止特定节点上的活动登录会话。 如果管理员想要终止跨不同节点的所有用户会话，则管理员必须登录每个节点并终止会话。

这适用于以下接口：

- Cisco Unified CM 管理

- Cisco Unified 功能配置
- Cisco Unified 报告
- Cisco Unified Communications Self Care 门户网站
- Cisco Unified CM IM and Presence 管理
- Cisco Unified IM and Presence 功能配置
- Cisco Unified IM and Presence 报告

过程

步骤 1 从 Cisco Unified 操作系统管理或 Cisco Unified IM and Presence 操作系统管理中，选择**安全** > **会话管理**。
此时“会话管理”窗口将显示。

步骤 2 在**用户 ID** 字段中输入活动登录用户的用户 ID。

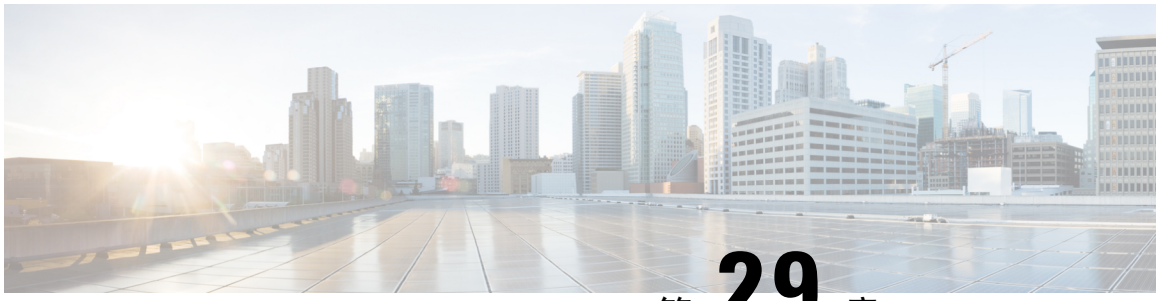
步骤 3 单击**终止会话**。

步骤 4 单击**确定**。

如果终止的用户刷新登录的界面页面，用户将被注销。 审核日志中会输入一个条目，其中显示终止的用户 ID。

第 VII 部分

IP 地址、主机名和域名更改



第 29 章

更改前任务和系统运行状况检查

更改前任务

IP 地址、主机名和其他网络标识符更改

可以出于多种原因更改部署中节点的网络级 IP 地址和主机名名称，包括将节点从一个群集移到另一个群集，或者解决重复的 IP 地址问题。 IP 地址是与节点关联的网络级 Internet 协议 (IP)，主机名是节点的网络级主机名。

注释 所有 Unified Communications 产品（例如 Cisco Unified Communications Manager、Cisco Unity Connections 以及 Cisco IM and Presence 等）都只有一个接口。 因此，您只能为这些产品分配一个 IP 地址。

对于其他网络标识符（例如节点名称和域名）更改，请参阅以下资源：

- 《Cisco Unified Communications Manager 系统配置指南》
- 《*IM and Presence Service* 的配置和管理指南》
- *Cisco Unified Communications Manager* 和 *IM and Presence Service* 安装指南

对于 IM and Presence Service，更改节点名称以及节点的网络级 DNS 默认域名的说明也包含在本文档中。

IM and Presence Service 节点名称和默认域名更改

节点名称使用 Cisco Unified CM 管理 GUI 配置，并且必须能够从所有其他 IM and Presence Service 节点和所有客户端计算机解析。 因此，建议的节点名称值为节点的网络 FQDN。 但是，系统也支持在某些部署中将 IP 地址和主机名用作节点名称的值。 有关节点名称建议和支持的部署类型的详细信息，请参阅主机名配置，第 261 页。

节点的网络级 DNS 默认域名与主机名组合，构成节点的完全限定域名 (FQDN)。 例如，主机名为“imp-server”、域为 “example.com” 的节点的 FQDN 为 “imp-server.example.com”。

请勿将节点的网络级 DNS 默认域与 IM and Presence Service 应用程序的企业范围的域混淆。

- 网络级 DNS 默认域仅用作节点的网络标识符。
- 企业范围的 IM and Presence Service 域是在最终用户的 IM 地址中使用的应用程序级域。

您可以使用 Cisco Unified CM IM and Presence 管理 GUI 或 Cisco Unified Communications Manager 管理配置企业范围的域。 如需有关企业范围的域及受支持的部署类型的详细信息，请参阅《*Cisco Unified Communications Manager* 上 *IM and Presence Service* 的部署指南》。

主机名配置

下表列出您可以为 Unified Communications Manager 服务器配置主机名的地方，允许主机名使用的字符数量以及建议主机名使用的第一个和最后一个字符。请注意，如果您没有正确配置主机名，Unified Communications Manager 中的部分组件，例如操作系统、数据库、安装等组件可能无法按预期工作。

表 *82: Cisco Unified Communications Manager* 中的主机名配置

主机名位置	允许的配置	允许的字符数	建议主机名使用的第一个字符	建议主机名使用的最后一个字符
主机名/IP 地址字段 **Cisco Unified Communications Manager 管理中的系统 > 服务器**	您可以添加或更改群集中服务器的主机名。	2-63	字母	字母数字
主机名字段 Cisco Unified Communications Manager 安装向导	您可以添加群集中服务器的主机名。	1-63	字母	字母数字
主机名字段 **Cisco Unified Communications 操作系统中的设置 > IP > 以太网**	您可以更改，但不能添加群集中服务器的主机名。	1-63	字母	字母数字
设置网络主机名 主机名 命令行界面	您可以更改，但不能添加群集中服务器的主机名。	1-63	字母	字母数字

提示 主机名必须遵循 ARPANET 主机名的规则。 在主机名的第一个和最后一个字符之间，您可以输入字母数字字符和连字符。

在任何位置配置主机名之前，请回顾以下信息：

- “服务器配置”窗口中的“主机名/IP字段”支持设备到服务器、应用程序到服务器和服务器到服务器通信，允许您输入点分十进制格式的 IPv4 地址或主机名。

  您在安装 Unified Communications Manager 发布方节点后，发布方的主机名将自动显示在此字段中。 您在安装 Unified Communications Manager 订户节点之前，在 Unified Communications Manager 发布方节点上的此字段中输入订户节点的 IP 地址或主机名。

  在此字段中，只有 Unified Communications Manager 可以访问 DNS 服务器以将主机名解析为 IP 地址时，才可配置主机名，确保您在 DNS 服务器上配置 Cisco Unified Communications Manager 名称和地址信息。

提示 除了在 DNS 服务器上配置 Unified Communications Manager 信息外，您可以在 Cisco Unified Communications Manager 安装期间输入 DNS 信息。

- 在安装 Unified Communications Manager 发布方节点期间，您输入发布方节点的主机名（必填）和 IP 地址，以配置网络信息，假如您想使用静态网络。

  安装 Unified Communications Manager 订户节点期间，您输入 Unified Communications Manager 发布方节点的主机名和 IP 地址，以便 Unified Communications Manager 可以验证网络连通性和发布方-订户验证。 此外，您必须输入订户节点的主机名和 IP 地址。 当 Unified Communications Manager 安装提示您输入订户服务器的主机名时，输入显示在 Cisco Unified Communications Manager 管理中的“服务器配置”窗口中的值，假如您在“主机名/IP 地址”字段配置订户服务器的主机名。

Procedure workflows

Cisco Unified Communications Manager 工作流程

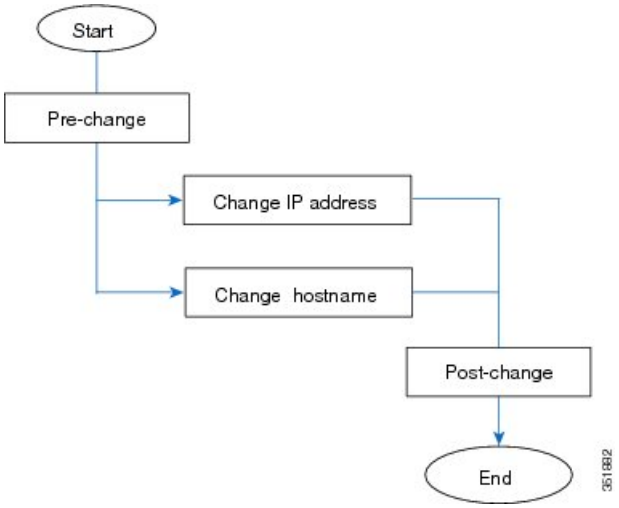
本文档为 Cisco Unified Communications Manager 节点提供以下任务的详细程序：

- 更改节点的 IP 地址
- 更改节点的主机名

每个程序都有任务列表，其中总结了要执行的步骤。

注释 在进行这些更改之前，必须完成所有更改前任务和系统运行状况检查；完成这些更改后，必须完成更改后任务。

图 *24: Cisco Unified Communications Manager* 工作流程



IM and Presence Service 工作流程

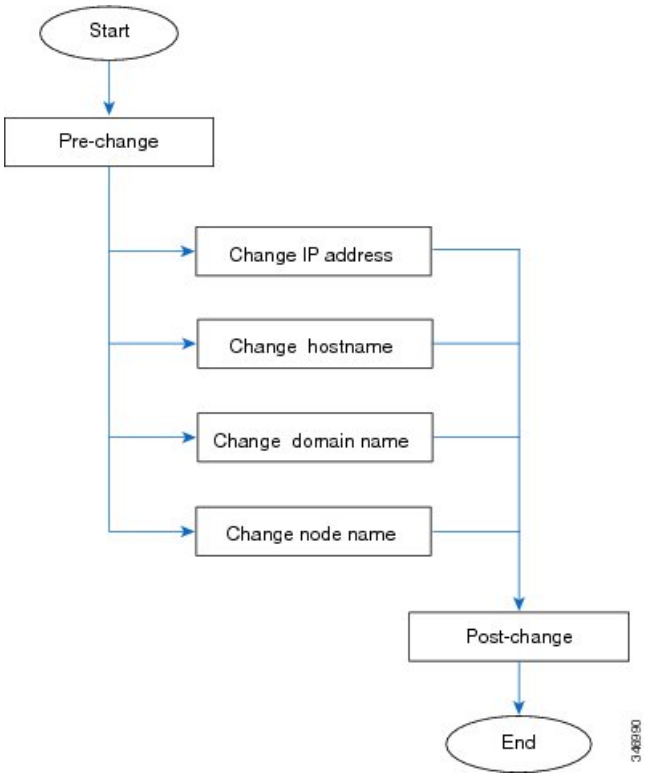
本文档提供为 IM and Presence Service 节点执行以下任务的详细程序：

- 更改节点的 IP 地址
- 更改节点的主机名
- 更改 DNS 默认域名
- 更改节点的节点名称

每个程序都有任务列表，其中总结了要执行的步骤。

注释 在进行这些更改之前，必须完成所有更改前任务和系统运行状况检查；完成这些更改后，必须完成更改后任务。

图 *25: IM and Presence Service* 工作流程



Cisco Unified Communications Manager 节点的更改前任务

以下程序说明了更改 Cisco Unified Communications Manager 节点的 IP 地址和主机名的任务。 必须在预定的维护期执行这些程序。

注意 如果执行这些任务时没有收到预期的结果，请先妥善解决问题，然后再继续。

过程

步骤 1 如果您在 Cisco Unified Communications Manager 服务器上的任何位置配置了 DNS，请确保配置了正向和反向记录（例如，A 记录和 PTR 记录），并且 DNS 可以访问且在正常工作。

步骤 2 检查活动的服务器关机警告，确保群集中的所有服务器都在运行并可用。 使用 Cisco Unified 实时监控工具 (RTMT) 或在第一个节点上使用命令行界面 (CLI) 进行检查。

a) 要使用 Unified RTMT 进行检查，请访问警告中心并检查服务器关机警告。

b) 要在第一个节点上使用 CLI 进行检查，请输入以下 CLI 命令并检查应用程序事件日志：

```
file search activelog syslog/CiscoSyslog ServerDown
```

对于输出示例，请参阅与数据库复制输出示例相关的主题。 有关详细的程序和故障诊断，请参阅与数据库复制验证和数据库复制故障诊断相关的主题。

步骤 3 检查群集中所有 Cisco Unified Communications Manager 节点的数据库复制状态，确保所有服务器均已成功复制数据库更改。 对于 IM and Presence Service，如果您的部署中有多个节点，请使用 CLI 检查数据库发布方节点上的数据库复制状态。 请使用 Unified RTMT 或 CLI。 所有节点的状态应显示为 2。

1. 要使用 RTMT 进行检查，请访问“数据库摘要”并检查复制状态。
2. 要使用 CLI 进行检查，请输入 **utils dbreplication runtimestate**。

步骤 4 如以下示例中所示输入 CLI 命令 utils diagnose，以检查网络连接和 DNS 服务器配置。

示例：

```
admin: utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1.log
Starting diagnostic test(s)
===========================
test - validate_network : Passed
Diagnostics Completed
admin:
```

步骤 5 在 Cisco Unified 报告中，生成 Unified CM 数据库状态报告。 在此报告中查找任何错误或警告。

步骤 6 在 Cisco Unified 报告中，生成 Unified CM 群集概述报告。 在此报告中查找任何错误或警告。

步骤 7 从第一个节点的 Cisco Unified Communications Manager 管理中，选择**系统** > **服务器**，然后单击**查找**。此时将显示群集中所有服务器的列表。保留此服务器列表以供将来参考。确保保存群集中每个节点的主机名和 IP 地址清单。

步骤 8 运行手动灾难恢复系统备份，确保所有节点和活动服务均已成功备份。有关详细信息，请参阅《*Cisco Unified Communications Manager* 管理指南》

步骤 9 如果要更改主机名，请禁用 SAML 单点登录 (SSO)。 有关 SAML SSO 的详细信息，请参阅《*Cisco Unified Communications Manager* 上 *IM and Presence Service* 的部署指南》。

步骤 10 对于启用安全性的群集（群集安全模式 1 - 混合），更新证书信任列表 (CTL) 文件。 有关更新和管理 CTL 文件（包括将新 TFTP 服务器添加到现有 CTL 文件）的详细说明，请参阅《*Cisco Unified Communications Manager* 安全指南》。

注释 为避免不必要的延迟，必须使用 TFTP 服务器的新 IP 地址更新 CTL 文件，然后再更改 TFTP 服务器的 IP 地址。 如果没有执行此步骤，则必须手动更新所有安全 IP 电话。

注释 支持安全性的所有 IP 电话始终下载 CTL 文件，其中包括允许电话与之通信的 TFTP 服务器的 IP 地址。 如果更改一台或多台 TFTP 服务器的 IP 地址，则必须首先将新 IP 地址添加到 CTL 文件，以便电话能够与其 TFTP 服务器通信。

IM and Presence Service 节点的更改前设置任务

执行相应的更改前设置任务，以确保系统做好准备，可成功更改 IP 地址、主机名、域或节点名称。必须在预定的维护期执行这些任务。

注意 如果执行这些任务时没有收到预期的结果，请先妥善解决问题，然后再继续。

注释 除非您正在更改域名或节点名，否则您不需要执行验证 Cisco AXL Web 服务以及 IM 和 Presence Cisco Sync Agent 服务是否已启动的步骤。有关要执行的任务的完整列表，请参阅更改前任务列表。

过程

步骤 1 检查群集中所有节点的数据库复制状态，确保所有服务器均已成功复制数据库更改。

对于 IM and Presence Service，如果您的部署中有多个节点，请使用 CLI 检查数据库发布方节点上的数据库复制状态。

请使用 Unified RTMT 或 CLI。 所有节点的状态应显示为 **2**。

a) 要使用 RTMT 进行检查，请访问“数据库摘要”并检查复制状态。
b) 要使用 CLI 进行检查，请输入 **utils dbreplication runtimestate**。

对于输出示例，请参阅与数据库复制输出示例相关的主题。 有关详细的程序和故障诊断，请参阅与数据库复制验证和数据库复制故障诊断相关的主题。

步骤 2 如以下示例中所示输入 CLI 命令 **utils diagnose**，以检查网络连接和 DNS 服务器配置。

示例：

```
admin: utils diagnose module validate_network Log file:
/var/log/active/platform/log/diag1.log Starting diagnostic test(s)
========================== test - validate_network : Passed Diagnostics Completed
 admin:
```

步骤 3 运行手动灾难恢复系统备份，确保所有节点和活动服务均已成功备份。

有关详细信息，请参阅《*Cisco Unified Communications Manager* 管理指南》。

步骤 4 禁用所有在线状态冗余组的高可用性 (HA)。有关在线状态冗余组配置的信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》中的“配置在线状态冗余组”一章。

注释
- 在禁用 HA 之前，请记下每个节点和子群集中的用户数。您可以在 Cisco Unified CM IM and Presence 管理的**系统** > **Presence 拓扑**窗口中找到此信息。
- 禁用 HA 后，请至少等待 2 分钟，以便先让设置同步到整个群集，然后再完成任何进一步的更改。

步骤 5 如果要更改主机名，请禁用 SAML 单点登录 (SSO)。 有关 SAML SSO 的详细信息，请参阅《*Cisco Unified Communications Manager* 上 *IM and Presence Service* 的部署指南》。

步骤 6 汇总当前激活的所有服务的列表。 保留这些列表以供将来参考。

a) 要使用 Cisco Unified 功能配置查看已激活的网络服务的列表，请选择**工具** > **控制中心 - 网络服务**。

b) 要使用 Cisco Unified 功能配置查看已激活的功能服务的列表，请选择**工具** > **控制中心 - 功能服务**。

步骤 7 要使用 Cisco Unified 功能配置停止所有功能服务，选择**工具** > **控制中心 - 功能服务**。 停止功能服务的顺序并不重要。

提示 如果您要更改IP地址或主机名，或者同时更改二者，则无需完成此步骤。 系统会针对这些名称更改自动停止功能服务。

步骤 8 选择**工具** > **控制中心 - 网络服务**时，使用 Cisco Unified 功能配置停止 IM and Presence Service 服务组下所列的以下网络服务。

您必须按以下顺序停止这些 IM and Presence Service 网络服务：

1. Cisco 配置代理
2. Cisco 群集间同步代理
3. Cisco 客户端配置文件代理
4. Cisco OAM 代理
5. Cisco XCP 配置管理器
6. Cisco XCP 路由器
7. Cisco Presence 数据存储器
8. Cisco SIP 注册数据存储器
9. Cisco 登录数据存储器
10. Cisco 路由数据存储器
11. Cisco 服务器恢复管理器
12. Cisco IM and Presence 数据监控器

步骤 9 验证是否使用 Cisco Unified 功能配置的**工具** > **控制中心 - 功能服务**在 Cisco Unified Communications Manager 发布方节点上启用了 Cisco AXL Web 服务。

注释 仅在更改域名或节点名称时执行此步骤。

步骤 10 验证 IM and Presence Cisco 同步代理服务是否已启动以及同步是否已完成。

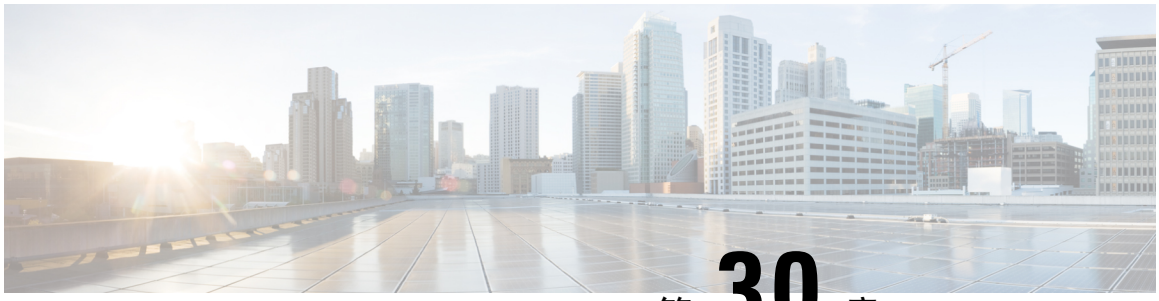
注释 仅在更改域名或节点名称时执行此步骤。

a) 要使用 Cisco Unified 功能配置，请执行以下步骤：

1. 选择**工具** > **控制中心 - 网络服务**。
2. 选择 IM and Presence 数据库发布方节点。
3. 选择 **IM and Presence Service 服务**。

4. 验证 Cisco 同步代理服务是否已启动。
5. 在 Cisco Unified CM IM and Presence 管理 GUI 中，选择**诊断** > **系统控制板** > **同步状态**。
6. 确认同步已完成并且同步状态区域中没有显示任何错误。

b) 要在 IM and Presence 数据库发布方节点上使用 Cisco Unified CM IM and Presence 管理 GUI 进行验证，请选择**诊断** > **系统控制板**。



第 30 章

IP 地址和主机名更改

更改 IP 地址和主机名任务列表

下表列出了在更改 Cisco Unified Communications Manager 和 IM and Presence Service 节点的 IP 地址和主机名时要执行的任务。

表 *83:* 更改 *IP* 地址和主机名任务列表

项目	任务
1	执行更改前任务和系统运行状况检查。
2	您可以使用命令行界面 (CLI) 或 Unified 操作系统 GUI 更改节点的 IP 地址或主机名。 对于 IM and Presence Service 节点，请遵守以下条件： • 在更改任何订阅方节点之前，更改数据库发布方节点的 IP 地址和主机名。 • 您可以同时更改所有订阅方节点的 IP 地址和主机名，也可以一次更改一个。 **注释** 在更改 IM and Presence Service 节点的 IP 地址或主机名后，必须在 Cisco Unified Communications Manager 上更改 SIP 发布干线的目标地址值。 请参阅更改后任务列表。
3	执行更改后任务。

通过操作系统管理 GUI 更改 IP 地址或主机名

您可以使用 Cisco Unified 操作系统管理更改由部署中的主机名定义的发布方和订阅方节点的 IP 地址或主机名。 除非另有说明，否则此程序中的每个步骤都适用于 Unified Communications Manager 和 IM and Presence Service 群集上的发布方和订阅方节点。

通过 **set network hostname** 命令更改主机名会触发自动自签名证书重新生成。 这将导致群集中的所有设备重置，以便能够下载更新的ITL文件。 如果您的群集使用CA签名的证书，您需要重新签名。

使用 **set network hostname** 命令仅更改 IP 地址会导致群集中的所有设备重置，以便它们可以下载更新的 ITL 文件。 证书未更新。

注释 更改主机名不会触发 ITL 恢复证书的重新生成。

注意

- 通过 Cisco Unified 操作系统管理，我们建议您每次只更改这些设置中的一项。 要同时更改 IP 地址和主机名，请使用 CLI 命令 **set network hostname**。
- 如果 Unified Communications Manager 群集安全功能在混合模式下运行，则更改主机名或 IP 地址后，在运行 CTL 客户端并更新 CTL 文件之前（如果您使用的是去令牌 CTL 功能，则是在运行 **utils ctl update CTLFile** 之前），与该节点的安全连接都会失败。

开始之前

对您的部署执行更改前任务和系统运行状况检查。

注释 如果您必须从 vcenter 更改 vNIC，请使用 CLI 命令 **set network hostname**。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**设置** > **IP** > **以太网**

步骤 2 更改主机名、IP 地址以及默认网关（必要时）。

步骤 3 单击**保存**。

节点服务会随着新更改自动重新启动。 重新启动服务可确保按正确的顺序更新和重新启动服务，以使更改生效。

更改主机名会触发自动重新生成自签证书，导致群集中的所有设备重置，以便其能够下载更新的ITL文件。 更改主机名不会触发 ITL 恢复证书的重新生成。

下一步做什么

执行所有适用的更改后任务，确保更改在部署中正确实施。

注释 如果新主机名没有解析为正确的 IP 地址，请勿继续。

如果您的群集使用 CA 签名的证书，您需要重新签名。

如果遵照该过程将群集置于混合模式，请运行 CTL 客户端以更新 CTL 文件。 如果使用的是去令牌 CTL 功能，则运行 CLI 命令 **utils ctl update CTLFile**

通过 Unified CM 管理 GUI 更改 IP 地址或主机名

您可以使用 Cisco Unified CM Administration 更改发布方和订阅方节点的 IP 地址或主机名（在数据库中定义）。 这样做可以确保主机名条目与系统定义的主机名或 IP 值一致。

更改 IP 地址或 主机名会触发自动重新生成自签证书。 这将导致群集中的所有设备重置，以便能够下载更新的 ITL 文件。 如果您的群集使用 CA 签名的证书，则必须重新签名。

注意

- 更改主机名或 IP 地址需要重新启动系统服务。 因此，不要在正常工作时间内进行此更改。
- 通过 Cisco Unified CM 管理，我们建议您每次只更改这些设置中的一项。 要同时更改 IP 地址和主机名，请使用 CLI 命令 **set network hostname**。
- 如果 Unified Communications Manager 群集安全功能在混合模式下运行，则更改主机名或 IP 地址后，在运行 CTL 客户端并更新 CTL 文件之前（如果您使用的是去令牌 CTL 功能，则是在运行 **utils ctl update CTLFile** 之前），与该节点的安全连接都会失败。
- 如果在 Cisco Unified 操作系统管理和 Cisco Unified CM 管理页面上定义的主机名或 IP 地址不匹配，则应用程序无法获取正确的电话状态。 此外，由于证书不匹配，TLS 握手失败。 因此，请确保 Cisco Unified 操作系统管理和 Cisco Unified CM 管理页面中的 IP 地址和主机名条目相同。

开始之前

对您的部署执行更改前任务和系统运行状况检查。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统** > **服务器**。

此时将显示**查找并列出服务器**窗口。

步骤 2 要获取所有服务器的列表，请单击**查找**。

步骤 3 从列表中，单击要修改其主机名的服务器。

步骤 4 在**主机名/IP 地址***字段中，输入新主机名或 IP 地址并单击**保存**。

步骤 5 使用 Admin CLI GUI，使用 **utils system restart** CLI 命令重新启动节点。

通过 CLI 更改 IP 地址或主机名

可以使用 CLI 更改由部署中的主机名定义的发布方和订阅方节点的 IP 地址或主机名。 除非另有说明，否则此程序中的每个步骤都适用于 Cisco Unified Communication Manager 和 IM and Presence Service 群集上的发布方和订阅方节点。

更改主机名会触发自动自签证书自动重新生成。 这将导致群集中的所有设备重置，以便能够下载更新的 ITL 文件。 如果您的群集使用 CA 签名的证书，则必须重新签名。 更改主机名不会触发 ITL 恢复证书的重新生成。

注意 如果 Cisco Unified Communications Manager 群集安全功能在混合模式下运行，则更改主机名或 IP 地址后，在运行 CTL 客户端并更新 CTL 文件之前（如果您使用的是去令牌 CTL 功能，则是在运行 **utils ctl update CTLFile** 之前），与该节点的安全连接都会失败。

注释 必须安装 COP 文件，以避免在更改 Unified Communications Manager 以及 Instant Messaging and Presence 服务器中的 IP/域/主机名的过程中出现故障。

开始之前

对您的部署执行更改前任务和系统运行状况检查。

过程

步骤 1 登录到要更改的节点的 CLI。

步骤 2 输入 **`set network hostname`**。

步骤 3 按照提示更改主机名、IP 地址或默认网关。

a) 输入新的主机名，然后按 **Enter** 键。
b) 如果还想更改 IP 地址，输入 **`yes`**；否则转至步骤 4。
c) 输入新的 IP 地址。
d) 输入子网掩码。
e) 输入网关的地址。

步骤 4 验证您的所有输入均正确无误，然后输入 **`yes`** 开始该过程。

下一步做什么

执行所有适用的更改后任务，确保更改在部署中正确实施。

注释 如果新主机名没有解析为正确的 IP 地址，请勿继续。

如果您的群集使用 CA 签名的证书，则必须重新签名。

如果遵照该过程将群集置于混合模式，请运行 CTL 客户端以更新 CTL 文件。 如果使用的是去令牌 CTL 功能，则运行 CLI 命令 **utils ctl update CTLFile**

设置网络主机名的 CLI 输出示例

注释 如果您需要从 vcenter 更改 vNIC，请在调用 4 个（共 5 个）组件通知脚本：regenerate_all_certs.sh 步骤后更新 vNIC，如以下输出中所示。

```
 admin:set network hostname ctrl-c: To quit the input. *** W A R N I N G *** Do
not close this window without first canceling the command. This command will
automatically restart system services. The command should not be issued during
normal operating hours. ======================================================
Note: Please verify that the new hostname is a unique name across the cluster
and, if DNS services are utilized, any DNS configuration is completed before
proceeding. ====================================================== Security
Warning : This operation will regenerate all CUCM Certificates including any third
 party signed Certificates that have been uploaded. Enter the hostname::
newHostname Would you like to change the network ip address at this time [yes]::
 Warning: Do not close this window until command finishes. ctrl-c: To quit the
input. *** W A R N I N G ***
====================================================== Note: Please verify that
 the new ip address is unique across the cluster.
====================================================== Enter the ip address::
10.10.10.28 Enter the ip subnet mask:: 255.255.255.0 Enter the ip address of the
 gateway:: 10.10.10.1 Hostname: newHostname IP Address: 10.10.10.28 IP Subnet
Mask: 255.255.255.0 Gateway: 10.10.10.1 Do you want to continue [yes/no]? yes
calling 1 of 5 component notification script: ahostname_callback.sh Info(0):
Processnode query returned = name ========== bldr-vcm18 updating server table
from:'oldHostname', to: 'newHostname' Rows: 1 updating database, please wait 90
seconds updating database, please wait 60 seconds updating database, please wait
 30 seconds Going to trigger /usr/local/cm/bin/dbl updatefiles
--remote=newHostname,oldHostname calling 2 of 5 component notification script:
clm_notify_hostname.sh notification Verifying update across cluster nodes...
platformConfig.xml is up-to-date: bldr-vcm21 cluster update successfull calling
3 of 5 component notification script: drf_notify_hostname_change.py calling 4 of
 5 component notification script: regenerate_all_certs.sh calling 5 of 5 component
 notification script: update_idsenv.sh calling 1 of 2 component notification
script: ahostname_callback.sh Info(0): Processnode query returned = name ====
Going to trigger /usr/local/cm/bin/dbl updatefiles
--remote=10.10.10.28,10.67.142.24 calling 2 of 2 component notification script:
clm_notify_hostname.sh Verifying update across cluster nodes... Shutting down
interface eth0:
```

仅更改 IP 地址

您可以使用 CLI 更改节点的 IP 地址。

如果节点由主机名或 FQDN 定义，则更改之前必须仅更新 DNS（如果使用了 DNS）。

注释 对于 IM and Presence Service：

- 先更改并验证 IM and Presence 数据库发布方节点。
- 您可以同时更改 IM and Presence Service 订阅方节点，也可以一次更改一个。

开始之前

对您的部署执行更改前任务和系统运行状况检查。

过程

步骤 1 登录到要更改的节点的 CLI。

步骤 2 输入 **set network ip eth0** *new-ip_address new_netmask new_gateway* 以更改节点的 IP 地址。

注释 仅使用 **set network ip eth0** 命令更改 IP 地址不会触发证书重新生成。

其中 *new_ip_address* 指定新的服务器 IP 地址，*new_netmask* 指定新的服务器网络掩码，*new_gateway* 指定网关地址。

此时会显示如下输出：

```
admin:set network ip eth0 10.53.57.101 255.255.255.224 10.53.56.1 WARNING: Changing
 this setting will invalidate software license on this server. The license will
have to be re-hosted. Continue (y/n)?
```

步骤 3 验证 CLI 命令的输出。 输入 **yes**，然后按 **Enter** 开始该过程。

下一步做什么

执行所有适用的更改后任务，确保更改在部署中正确实施。

设置网络 IP 地址的输出示例

注释 如果您需要从 vcenter 更改 vNIC，请在调用 3 个（共 6 个）组件通知脚本：aetc_hosts_verify.sh 步骤后更新 vNIC，如以下输出中所示。

```
admin:set network ip eth0 10.77.30.34 255.255.255.0 10.77.30.1 *** W A R N I N G
 *** This command will restart system services
========================================================= Note: Please verify that
 the new ip address is unique across the cluster and, if DNS services are utilized,
 any DNS configuration is completed before proceeding.
========================================================= Continue (y/n)?y calling
 1 of 6 component notification script: acluster_healthcheck.sh calling 2 of 6
component notification script: adns_verify.sh No Primary DNS server defined No
Secondary DNS server defined calling 3 of 6 component notification script:
aetc_hosts_verify.sh calling 4 of 6 component notification script: afupdateip.sh
 calling 5 of 6 component notification script: ahostname_callback.sh Info(0):
Processnode query returned using 10.77.30.33: name ==== calling 6 of 6 component
 notification script: clm_notify_hostname.sh
```

使用 CLI 更改 DNS IP 地址

可以使用 CLI 更改部署中的发布方和订阅方节点的 DNS IP 地址。 此程序对 Unified Communications Manager 和 IM and Presence Service 群集上的发布方及订阅方节点均适用。

注释 如果任何 DNS 服务器记录发生任何更改，或者 DNS 服务器本身发生更改，用户应重新启动 nscd 服务。 此重新启动会清除缓存记录并将新记录加载到缓存中。

开始之前

对您的部署执行更改前任务和系统运行状况检查。

过程

步骤 1 登录到要更改的节点的 CLI。

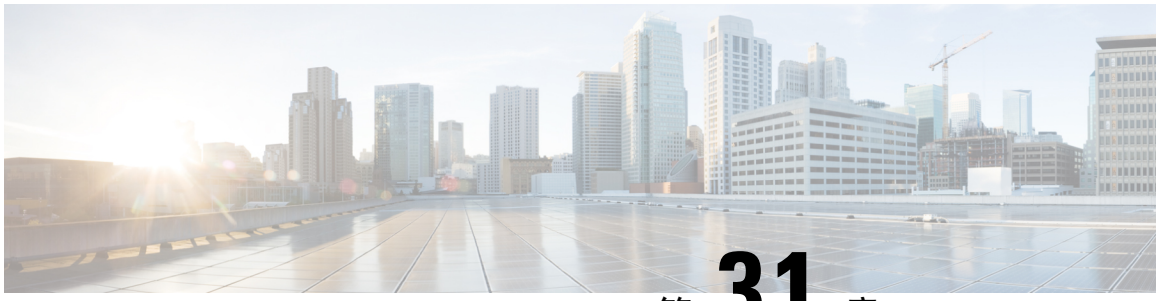
步骤 2 输入 `set network dns primary/secondary <new IP address of the DNS>`

注释 如果更改 DNS 服务器的 IP 地址，则必须通过 **utils system restart** CLI 命令重新启动服务器。

此时会显示如下输出：

```
admin:set network dns primary/secondary <new IP address of DNS> *** W A R N I N
G *** This will cause the system to temporarily lose network connectivity
```

步骤 3 验证 CLI 命令的输出。 输入 **yes**，然后按 **Enter** 开始该过程。



第 31 章

域名和节点名称更改

域名更改

管理员可以修改与 IM and Presence Service 节点或节点组相关联的网络级 DNS 默认域。

企业范围的 IM and Presence Service 域不需要与任何 IM and Presence Service 节点的 DNS 默认域一致。 要为您的部署修改企业范围的域，请参阅《*Cisco Unified Communications Manager* 上 *IM and Presence Service* 的部署指南》《*IM and Presence Service* 配置和管理指南》。

注意 如果在 IM and Presence Service 群集中的任何节点上更改默认域，将导致节点重新启动并中断 Presence 服务和其他系统功能。 由于其对系统的影响，必须在预定的维护期执行此域更改程序。

更改节点的默认域名时，所有第三方签名的安全证书会自动被新的自签证书覆盖。 如果想要第三方证书颁发机构重新签署这些证书，必须手动请求并上传新证书。 可能需要重新启动服务以获取这些新证书。 根据请求新证书所需的时间，可能需要安排单独的维护期让服务重新启动。

注释 不能在更改节点的默认域名之前请求新证书。 只有在节点上更改域并且节点重新启动后，才可生成证书签名请求 (CSR)。

IM and Presence Service 默认域名更改任务

下表包含用于修改与 IM and Presence Service 节点或节点组关联的网络级 DNS 默认域名的分步说明。此程序的详细说明指定了在群集中的多个节点上执行更改的具体步骤顺序。

如果您在多个群集上执行此程序，必须一次在一个群集上按顺序完成更改。

注释 您必须严格按照此工作流程中的顺序完成此程序中的每项任务。

过程

步骤 1 在群集中的所有适用节点上完成更改前任务。 某些更改前任务可能仅适用于 IM and Presence 数据库发布方节点；如果修改的是订阅方节点，可以跳过这些任务。

步骤 2 更新群集中所有适用节点上 IM and Presence Service 节点的 DNS 记录。 还要适当地更新 SRV、正向 (A) 和反向 (PTR) 记录以合并新的节点域。

步骤 3 使用 Cisco Unified Communications Manager 管理在群集中的所有适用节点上更新 IM and Presence Service 节点名称。

注释 此步骤对于 FQDN 节点名称格式是必需的。 如果节点名称是 IP 地址或主机名，则不适用。

- 如果节点名称是 FQDN，则它引用旧的节点域名。因此，必须更新节点名称，以便 FQDN 值反映新域名。
- 如果节点名称是 IP 地址或主机名，则不会引用域，因此无需更改。

步骤 4 使用命令行界面 (CLI) 更新所有适用节点上的 DNS 域。 CLI 命令在节点操作系统上进行必要的域更改，并触发每个节点自动重新启动。

步骤 5 在域名更新后重新启动群集中所有节点的 'A Cisco DB' 服务，以确保所有节点上的操作系统配置文件都获取与所修改节点关联的 DNS 域名更改。

注释 验证系统是否正确工作。 如果您观察到任何复制问题，请确保重新启动群集中的所有节点。

步骤 6 使用 CLI 验证数据库复制。 有关详细信息，请参阅与执行系统运行状况检查和数据库复制故障诊断相关的主题。 在群集内同步所有系统文件后，必须验证数据库复制。

步骤 7 在节点上重新生成安全证书。

- 所有 IM and Presence Service 安全证书上的主题通用名称设置为节点 FQDN。 因此，要合并新节点域，在 DNS 域更改后，系统会自动重新生成所有证书。
- 以前由证书签名的任何证书。

步骤 8 完成群集内所有适用节点的更改后任务，以确保群集完全可操作。

更新 DNS 记录

由于您要更改节点的 DNS 域，因此还必须更新与该节点关联的所有现有 DNS 记录。 这包括以下类型的记录：

- A 记录
- PTR 记录
- SRV 记录

如果要修改群集中的多个节点，必须为每个节点完成以下程序。

如果要修改 IM and Presence 数据库发布方节点，则必须在 IM and Presence 数据库发布方节点上完成此程序，然后在所有适用的 IM and Presence Service 发布方节点上重复。

注释
- 这些 DNS 记录必须在相同的维护时段更新，因为 DNS 域在节点上会自行更改。
- 在计划的维护时段之前更新 DNS 记录可能会对 IM and Presence Service 功能产生负面影响。

开始之前

对您的部署执行所有更改前任务和适用的系统运行状况检查。

过程

步骤 1 从旧域中删除节点的旧 DNS 前转 (A) 记录。

步骤 2 为新域中的节点创建新的 DNS 前转 (A) 记录。

步骤 3 更新节点的 DNS 反向 (PTR) 记录，使其指向节点的更新的完全限定域名 (FQDN)。

步骤 4 更新指向节点的所有 DNS SRV 记录。

步骤 5 更新指向节点的任何其他 DNS 记录。

步骤 6 通过在每个节点上运行以下命令行界面 (CLI) 命令，验证所有上述 DNS 更改是否已传播到群集中的所有其他节点：

a) 要验证新的 A 记录，请输入 **utils network host new-fqdn**，其中 `new-fqdn` 是节点的更新 FQDN。

示例：

```
admin: utils network host server1.new-domain.com Local Resolution:
server1.new-domain.com resolves locally to 10.53.50.219 External Resolution:
server1.new-domain.com has address 10.53.50.219
```

b) 要验证更新的 PTR 记录，请输入 **utils network host ip-addr**，其中 `ip-addr` 是节点的 IP 地址。

```
admin: utils network host 10.53.50.219 Local Resolution: 10.53.50.219 resolves
 locally to server1.new-domain.com External Resolution: server1.new-domain.com
 has address 10.53.50.219 219.50.53.10.in-addr.arpa domain name pointer
server1.new-domain.com.
```

注释 在程序的这一时点，IP 地址的**本地解析**结果将继续指向旧的 FQDN 值，直到该节点上的 DNS 域发生变化。

c) 要验证所有更新的 SRV 记录，请输入 **utils network host srv-name srv**，其中 srv-name 是 SRV 记录。

示例：

_xmpp-server SRV record lookup example.

```
admin: utils network host _xmpp-server._tcp.galway-imp.com srv Local Resolution:
 Nothing found External Resolution: _xmpp-server._tcp.sample.com has SRV record
 0 0 5269 server1.new-domain.com.
```

下一步做什么

更新 IM and Presence Service 节点名称。

在 FQDN 值中更新节点名称

如果 Cisco Unified CM IM and Presence 管理 GUI 的“Presence 拓扑”窗口中为节点定义的节点名称设置为节点的完全限定域名 (FQDN)，其将引用旧的域名。因此，您必须更新节点名称以引用新的域名。

注释 只有当此节点的节点名值设置为 FQDN 时，才需要执行此程序。 如果节点名称与节点的 IP 地址或主机名匹配，则不需要执行此程序。

如果要修改群集中的多个节点，必须按顺序对每个节点执行以下程序。

如果正在修改的是 IM and Presence 数据库发布方节点，则必须先对 IM and Presence Service 订阅方节点执行此程序，然后再在发布方节点上完成。

开始之前

更新节点的 DNS 记录。

过程

步骤 1 修改 IM and Presence Service 节点的节点名称。

a) 登录到 Cisco Unified Communications Manager 管理。
b) 选择**系统** > **服务器**。
c) 搜索并选择节点。
d) 更新**完全限定域名/IP 地址**字段，以便 FQDN 引用新的域值。 例如，将**完全限定域名/IP 地址**的值从 server1.old-domain.com 更新为 server1.new-domain.com。
e) 选择**保存**。

步骤 2 确认此节点的应用程序服务器条目已更新，反映了 Cisco Unified CM IM and Presence 管理 GUI **Presence 拓扑**窗口中的新节点名称。

a) 登录到 Cisco Unified Communications Manager 管理并选择**系统** > **应用程序服务器**。
b) 需要时，单击**查找并列出应用服务器**窗口中的**查找**。
c) 确保应用程序服务器列表中存在与更新的节点名称对应的条目。

注释 如果此节点没有条目，或者条目对应的是节点的旧名称，请勿继续。

下一步做什么

在所有适用的节点上更新 DNS 域。

更新 DNS 域

您可以使用命令行界面 (CLI) 更改 IM and Presence Service 的 DNS 域。

企业范围的 IM and Presence Service 域不需要与任何 IM and Presence Service 节点的网络层级 DNS 默认域一致。 要为您的部署修改企业范围的域，请参阅《*Cisco Unified Communications Manager* 上 *IM and Presence Service* 的部署指南》。

如果要修改群集中的多个节点，则必须依次为每个节点完成以下程序。

如果要修改 IM and Presence 数据库发布方节点，则必须先在数据库发布方节点上完成此程序，然后再修改任何订阅方节点。

开始之前

更新 IM and Presence Service 节点名称。

过程

步骤 1 登录到节点上的 CLI，然后输入 **set network domain new-domain**，其中 `new-domain` 是要设置的新域值。

示例：

```
admin: set network domain new-domain.com *** W A R N I N G *** Adding/deleting
or changing domain name on this server will break database replication. Once you
 have completed domain modification on all systems that you intend to modify,
please reboot all the servers in the cluster. This will ensure that replication
keeps working correctly. After the service is rebooted, please confirm that there
 are no issues reported on the Cisco Unified Reporting report for Database
Replication. The server will now be rebooted. Do you wish to continue. Security
Warning : This operation will regenerate all CUP Certificates including any third
 party signed Certificates that have been uploaded. Continue (y/n)?
```

步骤 2 输入 **y** 并按**返回**确认域更改并重新启动节点，或者输入 **n** 取消。

提示 节点名称更改完成后，将在节点上重新生成所有证书。 如果其中任一证书由第三方证书颁发机构签名，则必须在此程序的稍后阶段重新请求这些签名的证书。

步骤 3 节点重新启动后，输入 `show network eth0` 以确认域名更改生效。

示例：

下例中的新域为 new-domain.com。

```
admin: show network eth0 Ethernet 0 DHCP : disabled Status : up IP Address :
10.53.50.219 IP Mask : 255.255.255.000 Link Detected: yes Mode : Auto disabled,
Full, 1000 Mbits/s Duplicate IP : no DNS Primary : 10.53.51.234 Secondary : Not
Configured Options : timeout:5 attempts:2 Domain : new-domain.com Gateway :
10.53.50.1 on Ethernet 0
```

步骤 4 在群集中的所有适用节点上重复前面的步骤。

下一步做什么

重新启动群集中的所有节点。

群集节点注意事项

可以使用命令行界面 (CLI) 重新启动群集节点中的 "A Cisco DB" 服务。

更改域名且节点重新启动后，您需要重新启动群集中所有节点的 'A Cisco DB' 服务，包括自动重新启动的节点，从 Unified CM 发布方开始，然后在发布的数据库出现时针对所有订阅方。 这样可确保所有节点上的操作系统配置文件与新的域值保持一致。

验证系统是否正确工作。 如果您观察到任何复制问题，请确保重新启动群集中的所有节点。

首先在 IM and Presence 数据库发布方节点上启动重启过程。 当数据库发布方节点重新启动后，继续以任意顺序重启剩余的 IM and Presence Service 订阅方节点。

开始之前

确保节点的 DNS 域名已更改。

过程

步骤 1 使用 CLI 重启 IM and Presence 数据库发布方节点。 输入 **utils system restart**。

示例：

```
admin: utils system restart Do you really want to restart ? Enter (yes/no)?
```

步骤 2 输入 **yes**，然后按**返回**重新启动。

步骤 3 等待直到您看到以下消息，指示 IM and Presence 数据库发布方节点已重新启动。

示例：

```
Broadcast message from root (Wed Oct 24 16:14:55 2012): The system is going down
 for reboot NOW! Waiting . Operation succeeded restart now.
```

步骤 4 在每个 IM and Presence Service 订阅方节点上登录 CLI，然后输入 **utils system restart** 重启每个订阅方节点。

注释　在尝试停止服务几分钟后，CLI 可能会要求您强制重新启动。 这时请输入 **yes**。

下一步做什么

验证数据库复制。 有关详细信息，请参阅与系统运行状况检查相关的主题。

重新生成安全证书

节点的完全限定域名 (FQDN) 在所有 IM and Presence Service 安全证书中用作主题通用名称。 因此，在节点上更新 DNS 域时，会自动重新生成所有安全证书。

如果任何证书由第三方证书颁发机构签名，则必须手动生成新的证书颁发机构签名证书。

如果要修改群集中的多个节点，则必须为每个节点完成以下程序。

注释　不能在更改节点的默认域名之前请求新证书。 只有在节点上更改域并且节点重新启动后，才可生成证书签名请求 (CSR)。

开始之前

验证数据库复制，确保已成功在所有节点上建立数据库复制。

过程

步骤 1 如果证书必须由第三方证书颁发机构签名，请登录到 Cisco Unified 操作系统管理 GUI，并对每个相关的证书执行所需的步骤。

步骤 2 上传签名的证书后，需要在 IM and Presence Service 节点上重新启动服务。

所需的服务重新启动如下：

- Tomcat 证书：通过运行以下命令行界面 (CLI) 命令重新启动 tomcat 服务：

  utils service restart Cisco Tomcat。

- Cup-xmpp 证书：从 Cisco Unified 功能配置 GUI 重新启动 Cisco XCP 路由器服务。
- Cup-xmpp-s2s 证书：从 Cisco Unified 功能配置 GUI 重新启动 Cisco XCP 路由器服务。

注释
- 这些操作会重新启动影响服务。 因此，根据获取签名证书的时间延迟，您可能需要为稍后的维护期安排重新启动。 同时，自签证书将继续在相关界面上显示，直到服务重新启动。
- 如果前面的列表中未指定证书，则不需要重新启动该证书的服务。

下一步做什么

在群集中的所有适用节点上执行更改后任务列表。

节点名称更改

您可以修改与 IM and Presence Service 节点或节点组相关联的节点名称。 更新会显示在 Cisco Unified Communications Manager 管理的**服务器配置**窗口中。

遵照以下程序来执行以下节点名称更改：

- IP 地址到主机名
- IP 地址到完全限定的域名 (FQDN)
- 主机名到 IP 地址
- 主机名到 FQDN
- FQDN 到主机名
- FQDN 到 IP 地址

有关节点名称建议的详细信息，请参阅《*Cisco Unified Communications Manager* 上 *IM and Presence Service* 的部署指南》。

⚠

注意 此程序仅适用于为不需要网络级更改的 IM and Presence Service 节点更改节点名称。 在这种情况下，执行特定于更改网络 IP 地址、主机名或域名的程序。 您必须在预定的维护期执行此节点名称更改程序。 如果在 IM and Presence Service 群集中的任何节点上更改节点名称，将导致节点重新启动并中断 Presence 服务和其他系统功能。

IM and Presence Service 节点名称更改任务列表

下表包含更改与 IM and Presence Service 节点或节点组关联的节点名称的分步说明。 此程序的详细说明指定了执行更改的具体步骤顺序。

如果要在多个群集上执行此程序，请按顺序完成所有步骤以同时更改一个群集上的节点名称。

表 *84:* 更改 *IM and Presence Service* 节点名称任务列表

项目	任务
1	在群集中的所有适用节点上完成更改前任务。 某些更改前任务可能仅适用于 IM and Presence 数据库发布方节点；如果修改的是订阅方节点，可以跳过这些任务。
2	通过 Cisco Unified Communications Manager 管理更改 IM and Presence Service 节点名称。
3	验证节点名称更新并确保节点名称更改与 IM and Presence Service 同步。
4	节点名称更新完成后，使用命令行界面 (CLI) 验证数据库复制。 确保已跨群集复制新节点名称并且数据库复制在所有节点上均可操作。
5	完成更新节点上的更改后任务列表，然后验证节点能否完全正常工作。

更新节点名称

如果要修改群集中的多个节点，则必须依次为每个节点完成以下程序。

如果正在修改的是 IM and Presence 数据库发布方节点，则必须先对 IM and Presence Service 订阅方节点执行此程序，然后再在发布方节点上完成。

注释 对于 IM 和在线状态节点，建议使用完全限定域名。但是，也支持 IP 地址和主机名。

开始之前

对您的部署执行所有更改前任务和适用的系统运行状况检查。

过程

步骤 1 登录到 Cisco Unified CM 管理。

步骤 2 选择**系统** > **服务器**。

步骤 3 选择要修改的节点。

步骤 4 使用新节点名称更新**主机名/IP 地址**字段。

注释 确保将新生成的 SP 元数据上传到 IDP 服务器。

步骤 5 如果要修改群集中的多个节点，请对每个节点重复此程序。

注释 如果您更新 IM and Presence Service 节点名称，并且还配置了第三方合规性，则必须更新合规服务器以使用基于节点名称的新领域。此配置更新是在第三方合规性服务器上进行的。 新的领域将显示在 **Cisco Unified CM IM and Presence 管理** > **消息** > **合规性** > **合规性设置**窗口中。

下一步做什么

验证节点名称更改。

使用 CLI 验证节点名称更改

您可以使用命令行界面 (CLI) 验证新节点名称是否已在整个群集中复制。

过程

步骤 1 输入 **run sql name select from processnode** 验证新节点名称是否已在群集中的每个节点上正确复制。

示例：

```
admin:run sql select name from processnode name ======================
EnterpriseWideData server1.example.com server2.example.com server3.example.com
server4.example.com
```

步骤 2 验证群集中每个节点是否都有一个指定新节点名称的条目。输出中不应出现旧的节点名称。

a) 如果输出符合预期，则验证通过，您无需验证节点的数据库复制。
b) 如果缺少任何新节点名称，或者存在对旧节点名称的引用，继续执行步骤 3。

步骤 3 要解决缺少节点名称或显示旧节点名称的问题，请执行以下操作：

a) 对于 IM and Presence 数据库发布方节点，请使用 Cisco Unified CM IM and Presence 管理 GUI 上的控制板检查同步代理是否运行正常，并验证同步代理状态中是否没有错误。
b) 对于订阅方节点，执行验证数据库复制程序。

使用 Cisco Unified CM IM and Presence 管理验证节点名称更改

仅对于 IM and Presence Service 节点而言，请验证此节点的应用服务器条目是否已更新，以反映 Cisco Unified CM IM and Presence 管理 GUI 上的新节点名称。

开始之前

更新 IM and Presence Service 节点名称。

过程

步骤 1 登录到 Cisco Unified CM IM and Presence 管理 GUI。

步骤 2 选择**系统** > **Presence 拓扑**。

步骤 3 验证新节点名称是否出现在 **Presence 拓扑**窗格中。

下一步做什么

验证数据库复制。

更新 Cisco Unified Communications Manager 的域名

您可以使用命令行界面 (CLI) 更改 Cisco Unified Communications Manager 的域名。 使用 CLI 更新所有适用节点上的DNS域名。 CLI 命令会在节点上更改所需的域名，并触发每个节点自动重新启动。

如果 Unified CM 群集安全模式是不安全的，并且您正在更新或更改域，那么作为域更改的一部分，将重新生成所有证书。 要确保在电话上更新国际交易日志，请在更新域名之前执行以下所需步骤：

1. 确保所有电话都处于在线状态并且已注册，以便它们能够处理更新的ITL。 对于执行此程序时未处于在线状态的电话，必须手动删除 ITL。
2. 将**预备回滚至 8.0 之前的群集企业**参数设置为 **True**。 所有电话会自动重置和下载包含空白信任验证服务 (TVS) 及 TFTP 证书部分的 ITL 文件。
3. 在电话上，选择**设置 > 安全 > 信任列表 > ITL 文件**，以验证 ITL 文件的 TVS 和 TFTP 证书部分是否为空。
4. 更改服务器的域名，并让配置用于回滚的电话注册到群集。
5. 在所有电话成功注册到群集后，将**预备回滚至 8.0 之前的群集**企业参数设置为 **False**。

开始之前

- 在更改域名之前，请确保启用了 DNS。
- 登录 Cisco Unified Communications Manager 管理，然后导航至**系统 >服务器字段**页面。 如果该服务器配置设置页面已有主机名条目，则应首先更改域名的主机名条目。
- 执行所有变更前任务和适用的系统运行状况检查。 有关详细信息，请参阅“相关主题”部分。

过程

步骤 1 登录到命令行界面。

步骤 2 输入 **run set network domain <new_domain_name>**。

命令会提示系统重新启动。

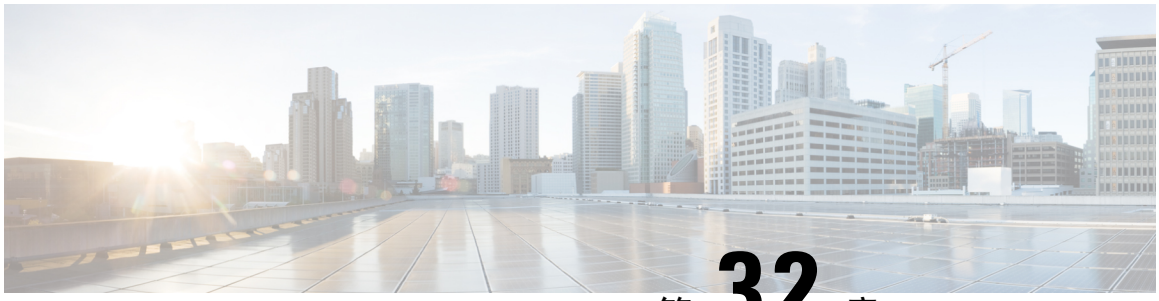
步骤 3 单击**是**重新启动系统。
新域名在系统重新启动后更新。

步骤 4 输入命令 **show network eth0**，以检查新域名在重新启动后是否会更新。

步骤 5 对所有群集节点重复次程序。

下一步做什么

执行所有适用的更改后任务，确保更改在部署中正确实施。



第 32 章

更改后任务和验证

Cisco Unified Communications Manager 节点的更改后任务

执行所有更改后任务，以确保更改在部署中正确实施。

⚠

注意 如果执行这些任务时没有收到预期的结果，请先妥善解决问题，然后再继续。

过程

步骤 1 如果在 Cisco Unified Communications Manager 服务器上的任何位置配置了 DNS，请确保已配置正向和反向查找区域，并且 DNS 可访问且在正常工作。

步骤 2 检查活动的服务器关机警告，确保群集中的所有服务器都在运行并可用。 使用 Cisco Unified 实时监控工具 (RTMT) 或在第一个节点上使用命令行界面 (CLI) 进行检查。

a) 要使用 Unified RTMT 进行检查，请访问警告中心并检查服务器关机警告。

b) 要在第一个节点上使用 CLI 进行检查，请输入以下 CLI 命令并检查应用程序事件日志：

```
file search activelog syslog/CiscoSyslog ServerDown
```

步骤 3 检查群集中所有节点的数据库复制状态，确保所有服务器均已成功复制数据库更改。

对于 IM and Presence Service，如果您的部署中有多个节点，请使用 CLI 检查数据库发布方节点上的数据库复制状态。

请使用 Unified RTMT 或 CLI。 所有节点的状态应显示为 **2**。

a) 要使用 RTMT 进行检查，请访问“数据库摘要”并检查复制状态。

b) 要使用 CLI 进行检查，请输入 **utils dbreplication runtimestate**。

对于输出示例，请参阅与数据库复制输出示例相关的主题。 有关详细的程序和故障诊断，请参阅与数据库复制验证和数据库复制故障诊断相关的主题。

步骤 4 如以下示例中所示输入 CLI 命令 **utils diagnose**，以检查网络连接和 DNS 服务器配置。

示例：

```
admin: utils diagnose module validate_network Log file:
/var/log/active/platform/log/diag1.log Starting diagnostic test(s)
========================== test - validate_network : Passed Diagnostics Completed
 admin:
```

如果执行的是更改前系统运行状况检查，则任务已完成；否则，继续执行更改后验证步骤。

步骤 5 验证新的主机名或 IP 地址是出现在 Cisco Unified Communications Manager 服务器列表中。 在 Cisco Unified Communications Manager 管理中，选择**系统** > **服务器**。

注释 仅作为更改后任务的一部分执行此步骤。

步骤 6 验证是否在网络中完全实施了对 IP 地址、主机名或两者的更改。 在群集中的每个节点上输入 CLI 命令 **show network cluster**。

注释 仅作为更改后任务的一部分执行此步骤。

输出应包含节点的新 IP 地址或主机名。

示例：

```
admin:show network cluster 10.63.70.125 hippo2.burren.pst hippo2 Subscriber cups
 DBPub authenticated 10.63.70.48 aligator.burren.pst aligator Publisher callmanager
 DBPub authenticated using TCP since Wed May 29 17:44:48 2013
```

步骤 7 验证主机名的更改是否已在网络中完全实施。 在群集中的每个节点上输入 CLI 命令 **utils network host**<*new_hostname*>。

注释 仅作为更改后任务的一部分执行此步骤。

输出应确认新的主机名在本地和外部解析为 IP 地址。

示例：

```
admin:utils network host hippo2 Local Resolution: hippo2.burren.pst resolves
locally to 10.63.70.125 External Resolution: hippo2.burren.pst has address
10.63.70.125
```

tasks.

步骤 8 对于启用安全性的群集（群集安全模式 1 - 混合），更新 CTL 文件，然后重新启动群集中的所有节点，再执行系统运行状况检查和其他更改后任务。

有关详细信息，请参阅多服务器群集电话的证书和 ITL 重新生成，第 389 页部分。

步骤 9 如果您使用证书信任列表 (CTL) 文件和 USB 电子令牌启用了群集安全性，必须在更改 8.0 或更高版本节点的 IP 地址或主机名后，重新生成初始信任列表 (ITL) 文件和 ITL 中的证书。 如果没有使用证书信任列表 (CTL) 文件和 USB 电子令牌启用群集安全性，则跳过此步骤。

步骤 10 运行手动 DRS 备份并确保成功备份所有节点和活动服务。

有关详细信息，请参阅《*Cisco Unified Communications Manager* 管理指南》。

注释 更改节点的 IP 地址后，必须运行手动 DRS 备份，因为无法使用包含不同 IP 地址或主机名的 DRS 文件恢复节点。 更改后 DRS 文件将包含新的 IP 地址或主机名。

步骤 11 更新所有相关的 IP 电话 URL 参数。

步骤 12 使用 Cisco Unified Communications Manager 管理更新所有相关的 IP 电话服务。 选择**系统** > **企业参数**。

步骤 13 更新 Unified RTMT 自定义警告和保存的配置文件。

- 从性能计数器派生的 Unified RTMT 自定义警告包括硬编码的服务器 IP 地址。 必须删除并重新配置这些自定义警告。
- 具有性能计数器的 Unified RTMT 已保存配置文件中包括硬编码的服务器 IP 地址。 必须删除并重新添加这些计数器，然后保存配置文件以将其更新为新的 IP 地址。

步骤 14 如果使用的是 Cisco Unified Communications Manager 上运行的集成式 DHCP 服务器，请更新该 DHCP 服务器。

步骤 15 检查并对其他关联的 Cisco Unified Communications 组件进行所需的配置更改。

以下是要检查的部分组件的部分列表：

- Cisco Unity
- Cisco Unity Connection
- CiscoUnity Express
- SIP/H.323 干线
- IOS 网守
- Cisco Unified MeetingPlace
- Cisco Unified MeetingPlace Express
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- IP 电话的 DHCP 作用域
- 用于 CDR 导出的 Cisco Unified Communications Manager 跟踪集合或作为 DRS 备份目标的 SFTP 服务器
- 向 Cisco Unified Communications Manager 注册的 IOS 硬件资源（会议桥、媒体终结点、代码转换器、RSVP 座席）
- 注册或与 Cisco Unified Communications Manager 集成的 IPVC 视频 MCU
- Cisco Emergency Responder

- Cisco Unified Application Environment
- Cisco Unified Presence
- Cisco Unified Personal Communicator
- 关联的路由器和网关

注释　　请查阅产品文档以确定如何进行必要的配置更改。

Cisco Unified Communications Manager 节点的启用安全的群集任务

初始信任列表和证书重新生成

如果在 Cisco Unified Communications Manager 发行版 8.0 或更高版本的群集中更改服务器的 IP 地址或主机名，则会重新生成初始信任列表 (ITL) 文件和 ITL 中的证书。 重新生成的文件与电话上存储的文件不匹配。

注释　如果使用证书信任列表 (CTL) 文件和 USB 电子令牌启用群集安全性，则无需执行以下程序中的步骤，因为信任由电子令牌维护，且电子令牌不会更改。

如果群集安全性未启用，请执行单服务器群集或多服务器群集程序中的步骤以重置电话。

重新生成单服务器群集电话的证书和 ITL

如果是在 Cisco Unified Communications Manager 发行版 8.0 或更高版本的单服务器群集中更改服务器的 IP 地址或主机名，并且使用了 ITL 文件，请执行以下步骤重置电话。

在更改服务器的 IP 地址或主机名之前启用回滚。

过程

步骤 1　确保所有电话都处于在线状态并且已注册，以便它们能够处理更新的 ITL。 对于执行此程序时未处于在线状态的电话，必须手动删除 ITL。

步骤 2　将“预备回滚至 8.0 之前的群集”企业参数设置为 True。 所有电话会自动重置和下载包含空白信任验证服务 (TVS) 及 TFTP 证书部分的 ITL 文件。

步骤 3　在电话上，选择**设置** > **安全** > **信任列表** > **ITL 文件**，以验证 ITL 文件的 TVS 和 TFTP 证书部分是否为空。

步骤 4 更改服务器的 IP 地址或主机名，并让配置用于回滚的电话注册到群集。

步骤 5 在所有电话成功注册到群集后，将“预备回滚至 8.0 之前的群集”企业参数设置为 **False**。

下一步做什么

如果使用 CTL 文件或令牌，请在更改服务器的 IP 地址或主机名后，或者更改 DNS 域名后，重新运行 CTL 客户端。

多服务器群集电话的证书和 ITL 重新生成

在多服务器群集中，电话应具有主要和辅助 TVS 服务器，以验证重新生成的 ITL 文件和证书。 如果电话无法联系主要 TVS 服务器（由于最近的配置更改），它将回滚到辅助服务器。 TVS 服务器通过分配给电话的 CM 组标识。

在多服务器群集中，请确保一次仅更改一台服务器上的 IP 地址或主机名。 如果使用 CTL 文件或令牌，请在更改服务器的 IP 地址或主机名后，或者更改 DNS 域名后，重新运行 CTL 客户端或 CLI 命令 set **utils ctl**。

IM and Presence Service 节点的更改后任务

执行所有更改后任务，以确保更改在部署中正确实施。

⚠

注意 如果执行这些任务时没有收到预期的结果，请先妥善解决问题，然后再继续。

过程

步骤 1 验证对主机名或 IP 地址的更改是否已在 Cisco Unified Communications Manager 服务器上更新。

步骤 2 检查节点上的网络连接和 DNS 服务器配置是否已更改。

注释 如果将 IP 地址更改为不同的子网，请确保您的网络适配器现已连接到正确的 VLAN。 此外，如果 IP 地址更改后 IM and Presence Service 节点属于不同的子网，请确保 Cisco XCP 路由器服务参数的“路由通信类型”字段设置为“路由器到路由器”。 否则，“路由通信类型”字段应设置为“组播 DNS”。

步骤 3 验证对 IP 地址、主机名或两者的更改是否已在网络中完全实施。

步骤 4 如果更改了主机名，请验证主机名更改是否已在网络中完全实施。

步骤 5 验证是否已成功建立数据库复制。 所有节点的状态应显示为 2 并已连接。 如果未设置复制，请参阅与数据库复制故障诊断相关的主题。

步骤 6 如果禁用了 SAML 单点登录 (SSO)，现在可以启用它。 有关 SAML SSO 的详细信息，请参阅《*Cisco Unified Communications Manager* 上 *IM and Presence Service* 的部署指南》。

步骤 7 如果更改了主机名，必须确保 cup、cup-xmpp 和 Tomcat 证书中包含新的主机名。

a) 从 Cisco Unified 操作系统管理 GUI 中，选择**安全** > **证书管理**。
b) 验证信任证书的名称中是否包含新的主机名。
c) 如果证书中不含新的主机名，请重新生成证书。

有关详细信息，请参阅《*Cisco Unified Communications Manager* 管理指南》。

步骤 8 如果节点的 IP 地址已更改，则更新 Cisco Unified 实时监控工具 (RTMT) 自定义警告和保存的配置文件：

- 源自性能计数器的 RTMT 自定义警告中包含硬编码的服务器地址。 必须删除并重新配置这些自定义警告。
- 具有性能计数器的 RTMT 已保存配置文件中包括硬编码的服务器地址。 必须删除并重新添加这些计数器，然后保存配置文件以将其更新为新的地址。

步骤 9 检查并对其他关联的 Cisco Unified Communications 组件（例如 Cisco Unified Communications Manager 上的 SIP 干线）进行任何必要的配置更改。

步骤 10 使用 Cisco Unified 功能配置启用 CUP 服务组下所列的所有网络服务，选择**工具** > **控制中心 - 网络服务**。

提示 如果您要更改IP地址或主机名，或者同时更改二者，则无需完成此步骤。 系统会针对这些名称更改自动启动网络服务。 但是，如果某些服务在更改后没有自动启动，请完成此步骤以确保所有网络服务均已启动。

必须按以下顺序启动“CUP 服务”网络服务：

1. Cisco IM and Presence 数据监控器
2. Cisco 服务器恢复管理器
3. Cisco 路由数据存储器
4. Cisco 登录数据存储器
5. Cisco SIP 注册数据存储器
6. Cisco Presence 数据存储器
7. Cisco XCP 配置管理器
8. Cisco XCP 路由器
9. Cisco OAM 代理
10. Cisco 客户端配置文件代理
11. Cisco 群集间同步代理
12. Cisco 配置代理

步骤 11 要使用 Cisco Unified 功能配置启动所有功能服务，选择**工具** > **控制中心 - 功能服务**。 启动功能服务的顺序并不重要。

提示 如果您要更改IP地址或主机名，或者同时更改二者，则无需完成此步骤。 系统会针对这些名称更改自动启动功能服务。 但是，如果某些服务在更改后没有自动启动，请完成此步骤以确保所有功能服务均已启动。

步骤 12 确认在重新启用高可用性之前已重新创建 Cisco Jabber 会话。 否则，已创建会话的 Jabber 客户端将无法连接。

在所有群集节点上运行 `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI 命令。 活动会话数应与您禁用高可用性时记录的用户数一致。 如果会话启动时间超过 30 分钟，您可能会遇到更大的系统问题。

步骤 13 如果在更改前设置期间禁用了高可用性 (HA)，请在所有在线状态冗余组上启用 HA。

步骤 14 验证更改后 IM and Presence Service 是否正常工作。

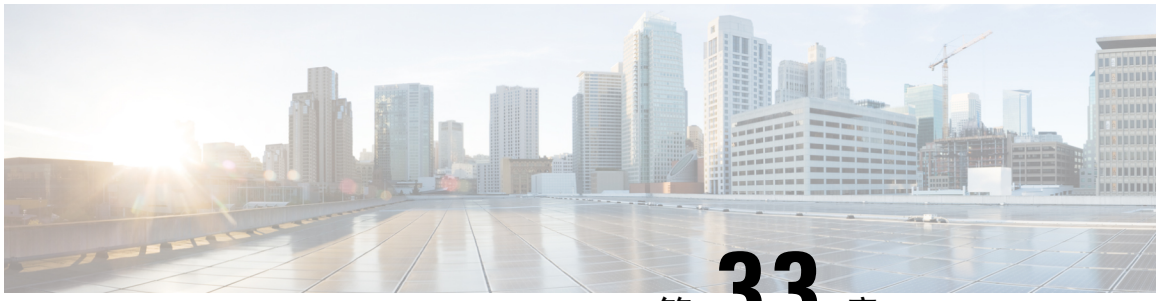
a) 从 Cisco Unified 功能配置 GUI 中，选择**系统** > **Presence 拓扑**。

- 如果 HA 已启用，验证是否所有 HA 节点都处于“正常”状态。
- 验证所有服务是否均已启动。

b) 从 Cisco Unified CM IM and Presence 管理 GUI 运行系统故障诊断程序，并确保没有测试失败。选择**诊断** > **系统故障诊断程序**。

步骤 15 更改节点的 IP 地址或主机名后，必须运行手动灾难恢复系统备份，因为无法使用包含不同 IP 地址或主机名的 DRS 文件恢复节点。 更改后 DRS 文件将包含新的 IP 地址或主机名。

有关详细信息，请参阅《*Cisco Unified Communications Manager* 管理指南》。



第 33 章

地址更改问题故障诊断

群集验证故障诊断

您可以使用命令行界面 (CLI) 对订阅方节点上的群集验证问题进行故障诊断。

过程

步骤 1 输入 **show network eth0 [detail]** 验证网络配置。

步骤 2 输入 **show network cluster** 验证网络群集信息。

- 如果输出显示不正确的发布方信息，请在订阅方节点上输入 **set network cluster publisher [hostname/IP address]** CLI 命令以更正信息。
- 如果您在发布方节点上，并且 `show network cluster` CLI 命令显示不正确的订阅方信息，请登录 Cisco Unified Communications Manager 管理，然后选择**系统** > **服务器**以检查输出。
- 如果您在订阅方节点上，并且 `show network cluster` 输出显示不正确的发布方信息，请使用 `set network cluster publisher [hostname | IP_address]` CLI 命令来更改发布方主机名或 IP 地址。

数据库复制故障诊断

您可以使用命令行界面 (CLI) 对群集节点上的数据库复制进行故障诊断。

- 验证数据库复制在群集中是否处于正确的状态。
- 为节点修复并重新建立数据库复制。

- 重置数据库复制。

有关这些命令或使用 CLI 的详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面指南》。

验证数据库复制

使用命令行界面 (CLI) 检查群集中所有节点的数据库复制状态。 验证复制设置 (RTMT) 和详细信息的值是否显示为 **2**。 如果是除 2 以外的其他值，表示数据库复制存在问题，您需要为该节点重置复制。 有关输出的示例，请参阅与数据库复制示例相关的主题。

过程

步骤 1 在第一个节点上输入 **utils dbreplication runtimestate**，以检查群集中所有节点上的数据库复制。

对于 IM and Presence Service，如果您的部署中有多个节点，则在数据库发布方节点上输入命令。

提示 如果没有为群集中的节点设置复制，您可以使用 CLI 重置节点的数据库复制。 有关详细信息，请参阅与使用 CLI 重置数据库复制相关的主题。

示例：

```
admin: utils dbreplication runtimestate DDB and Replication Services: ALL RUNNING
 DB CLI Status: No other dbreplication CLI is running... Cluster Replication
State: BROADCAST SYNC Completed on 1 servers at: 2013-09-26-15-18 Last Sync Result:
 SYNC COMPLETED 257 tables sync'ed out of 257 Sync Errors: NO ERRORS DB Version:
 ccm9_0_1_10000_9000 Number of replicated tables: 257 Repltimeout set to: 300s
Cluster Detailed View from PUB (2 Servers): PING REPLICATION REPL. DBver& REPL.
REPLICATION SETUP SERVER-NAME IP ADDRESS (msec) RPC? STATUS QUEUE TABLES LOOP?
(RTMT) & details ----------- ------------ ------ ---- ----------- ----- ------
----- ----------------- server1 100.10.10.17 0.052 Yes Connected 0 match Yes (2)
 PUB Setup Completed server2 100.10.10.14 0.166 Yes Connected 0 match Yes (2)
Setup Completed
```

步骤 2 验证输出。

输出应显示每个节点的复制状态为**已连接**，并且复制设置值为 **(2) 设置完成**。 这意味着群集中的复制网络运行正常。 如果输出结果不同，请继续进行故障诊断并修复数据库复制。

数据库复制 CLI 输出示例

以下列表显示了当您在群集的第一个节点上运行 `utils dbreplication runtimestate` 命令行界面 (CLI) 命令时，Replicate_State 的可能值。

对于 IM and Presence Service，如果您的部署中有多个节点，则在数据库发布方节点上输入命令。

- 0 - 复制未启动。 订阅方不存在，或自从订阅方安装后没有运行过数据库层监控服务。
- 1 - 复制已创建，但其计数不正确。

- 2 - 复制正常工作。
- 3 - 群集中的复制有错误。
- 4 - 复制设置失败。

注释 验证复制设置 (RTMT) 和详细信息的值是否显示为 2 非常重要。 如果是除 2 以外的其他值，表示数据库复制存在问题，您需要重置复制。 有关解决数据库复制问题的信息，请参阅与数据库复制故障诊断相关的主题。

Cisco Unified Communications Manager 节点 CLI 输出示例

在本例中，复制设置 (RTMT) 和详细信息的值显示为 2。 复制正常工作。

```
admin: utils dbreplication runtimestate Server Time: Mon Jun 1 12:00:00 EDT 2013
Cluster Replication State: BROADCAST SYNC Completed on 1 servers at:
2013-06-01-12-00 Last Sync Result: SYNC COMPLETED on 672 tables out of 672 Sync
Status: NO ERRORS Use CLI to see detail: 'file view activelog
cm/trace/dbl/2013_06_01_12_00_00_dbl_repl_output_Broadcast.log' DB Version:
ccm10_0_1_10000_1 Repltimeout set to: 300s PROCESS option set to: 1 Cluster
Detailed View from uc10-pub (2 Servers): PING Replication REPLICATION SETUP
SERVER-NAME IP ADDRESS (msec) RPC? Group ID (RTMT) & Details ----------- ----------
 ------ ---- ----------- -------------------- uc10-pub 192.0.2.95 0.040 Yes (g_2)
 (2) Setup Completed uc10-sub1 192.0.2.96 0.282 Yes (g_3) (2) Setup Completed
```

IM and Presence Service 节点 CLI 输出示例

在本例中，复制设置 (RTMT) 和详细信息的值显示为 2。 复制正常工作。

```
admin: utils dbreplication runtimestate Server Time: Mon Jun 1 12:00:00 EDT 2013 DB
and Replication Services: ALL RUNNING Cluster Replication State: Replication
status command started at: 2012-02-26-09-40 Replication status command COMPLETED
 269 tables checked out of 269 No Errors or Mismatches found. Use 'file view
activelog cm/trace/dbl/sdi/ReplicationStatus.2012_02_26_09_40_34.out' to see the
 details DB Version: ccm8_6_3_10000_23 Number of replicated tables: 269 Cluster
Detailed View from PUB (2 Servers): PING REPLICATION REPL. DBver& REPL. REPLICATION
 SETUP SERVER-NAME IP ADDRESS (msec) RPC? STATUS QUEUE TABLES LOOP? (RTMT) &
details ----------- ------------ ------ ---- ----------- ----- ------- -----
----------------- gwydla020218 10.53.46.130 0.038 Yes Connected 0 match Yes (2)
PUB Setup Completed gwydla020220 10.53.46.133 0.248 Yes Connected 128 match Yes
(2) Setup Completed
```

修复数据库复制

使用命令行界面 (CLI) 修复数据库复制。

过程

步骤 1 在第一个节点上输入 **utils dbreplication repair all** 修复所有，以尝试修复数据库复制。

对于 IM and Presence Service，如果您的部署中有多个节点，请从数据库发布方节点修复数据库复制状态。

根据数据库的大小，可能需要几分钟的时间来修复数据库复制。 继续执行下个步骤，以监控数据库复制修复的进度。

示例：

```
admin:utils dbreplication repair all -------------------- utils dbreplication
repair -------------------- Replication Repair is now running in the background.
 Use command 'utils dbreplication runtimestate' to check its progress Output will
 be in file cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out Please use
 "file view activelog cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out
 " command to see the output
```

步骤 2 在第一个节点上输入 **utils dbreplication runtimestate**，以检查复制修复的进度。

对于 IM and Presence Service，如果您的部署中有多个节点，则在数据库发布方节点上输入命令。

复制输出示例中的粗体文本高亮显示复制修复的最终状态。

示例：

```
admin:utils dbreplication runtimestate DB and Replication Services: ALL RUNNING
Cluster Replication State: Replication repair command started at: 2013-05-11-12-33
 Replication repair command COMPLETED 269 tables processed out of 269 No Errors
or Mismatches found. Use 'file view activelog
cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out' to see the details
DB Version: ccm8_6_4_98000_192 Number of replicated tables: 269 Cluster Detailed
 View from PUB (2 Servers): PING REPLICATION REPL. DBver& REPL. REPLICATION SETUP
 SERVER-NAME IP ADDRESS (msec) RPC? STATUS QUEUE TABLES LOOP? (RTMT) & details
----------- ------------ ------ ---- ------------ ----- ------ -----
----------------- server1 100.10.10.17 0.052 Yes Connected 0 match Yes (2) PUB
Setup Completed server2 100.10.10.14 0.166 Yes Connected 0 match Yes (2) Setup
Completed
```

a) 如果复制修复运行完成而没有任何错误或不匹配，请运行该程序以再次验证节点名称是否更改，确认现在是否已正确复制新节点名称。

b) 如果发现错误或不匹配，节点之间可能存在瞬态不匹配。 再次运行该程序以修复数据库复制。

注释 如果在多次尝试修复复制后，系统报告不匹配或错误，请与您的 Cisco 支持代表联系解决此问题。

步骤 3 在第一个节点上输入 **utils dbreplication reset all**，以尝试重新建立复制。

对于 IM and Presence Service，如果您的部署中有多个节点，则在数据库发布方节点中输入命令。

根据数据库的大小，完全重新建立复制可能需要几分钟到一个小时以上的时间。 继续执行下个步骤，以监控数据库复制重新建立的进度。

示例：

```
admin:utils dbreplication reset all This command will try to start Replication
reset and will return in 1-2 minutes. Background repair of replication will
continue after that for 1 hour. Please watch RTMT replication state. 此值应 0 到
2 之间的值。当所有子节点的 RTMT Replicate State 为 2 时，复制就完成了。 If Sub replication
 state becomes 4 or 1, there is an error in replication setup. Monitor the RTMT
counters on all subs to determine when replication is complete. Error details if
 found will be listed below OK [10.53.56.14]
```

步骤 4 在第一个节点上输入 **utils dbreplication runtimestate**，以监控尝试重新建立数据库复制的进度。

对于 IM and Presence Service，如果您的部署中有多个节点，则在数据库发布方节点上输入命令。

当所有节点的复制状态都显示为**已连接**且复制设置值为 **(2) 设置完成**时，系统会视为已重新建立复制。

示例：

```
admin: utils dbreplication runtimestate DDB and Replication Services: ALL RUNNING
 DB CLI Status: No other dbreplication CLI is running... Cluster Replication
State: BROADCAST SYNC Completed on 1 servers at: 2013-09-26-15-18 Last Sync Result:
 SYNC COMPLETED 257 tables sync'ed out of 257 Sync Errors: NO ERRORS DB Version:
 ccm9_0_1_10000_9000 Number of replicated tables: 257 Repltimeout set to: 300s
Cluster Detailed View from newserver100 (2 Servers): PING REPLICATION REPL. DBver&
 REPL. REPLICATION SETUP SERVER-NAME IP ADDRESS (msec) RPC? STATUS QUEUE TABLES
LOOP? (RTMT) & details ----------- -------------- ------ ---- ----------- -----
------ ----- ----------------- server1 100.10.10.201 0.038 Yes Connected 0 match
 Yes (2) PUB Setup Completed server2 100.10.10.202 0.248 Yes Connected 0 match
Yes (2) Setup Completed server3 100.10.10.203 0.248 Yes Connected 0 match Yes (2)
 Setup Completed server4 100.10.10.204 0.248 Yes Connected 0
```

a) 如果复制已重新建立，请运行该程序以再次验证节点名称是否更改，确认现在是否已正确复制新节点名称。

b) 如果复制没有恢复，请与您的 Cisco 支持代表联系以解决此问题。

注意 如果数据库复制中断，请不要继续此操作之后的步骤。

重置数据库复制

如果没有为群集中的节点设置复制，请重置数据库复制。 您可以使用命令行界面 (CLI) 重置数据库复制。

开始之前

检查群集中所有节点的数据库复制状态。 验证复制设置 (RTMT) 和详细信息的值是否显示为 2。 如果是除 2 以外的其他值，表示数据库复制存在问题，您需要为该节点重置复制。

过程

步骤 1 在群集中的节点上重置复制。 执行下列操作之一：

a) 对于 Unified Communications Manager，请输入 **utils db replication reset all**。

在任何 Cisco Unified Communications Manager 节点上运行此 CLI 命令之前，先在重置的所有订阅方节点上运行命令 **utils dbreplication stop**，然后在发布方服务器上运行。有关详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面指南》。

b) 对于 IM and Presence Service，在所有数据库发布方节点上输入 **utils db replication reset all**，以重置群集中的所有 IM and Presence Service 节点。

提示 您可以输入特定的主机名，而不是 **all**，仅重置该节点上的数据库复制。有关详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面指南》。

步骤 2 输入 **utils dbreplication runtimestate** 以检查数据库复制状态。

对于 IM and Presence Service，在 IM and Presence 数据库发布方节点上运行 CLI 命令

网络故障诊断

您可以使用命令行界面 (CLI) 对节点上的网络问题进行故障诊断。

过程

步骤 1 输入 **show network eth0 [detail]** 验证网络配置。

步骤 2 如果任何字段缺失，则重置网络接口。

a) 输入 **set network status eth0 down**。

b) 输入 **set network status eth0 up**。

步骤 3 验证 IP 地址、掩码和网关。

确保这些值在整个网络中是唯一的。

Network Time Protocol troubleshooting

对订阅方节点上的 NTP 进行故障诊断

您可以使用命令行界面 (CLI) 对订阅方节点上的网络时间协议 (NTP) 问题进行故障诊断。

过程

步骤 1 输入 **show network eth0 [detail]** 验证网络配置。

步骤 2 输入 **utils ntp status** 验证 NTP 状态。

步骤 3 输入 **utils ntp restart** 重新启动 NTP。

步骤 4 输入 **show network cluster** 验证网络群集。

如果输出显示不正确的发布方信息，请使用 **set network cluster publisher [hostname/IP_address]** CLI 命令重置发布方。

对发布方节点上的 NTP 进行故障诊断

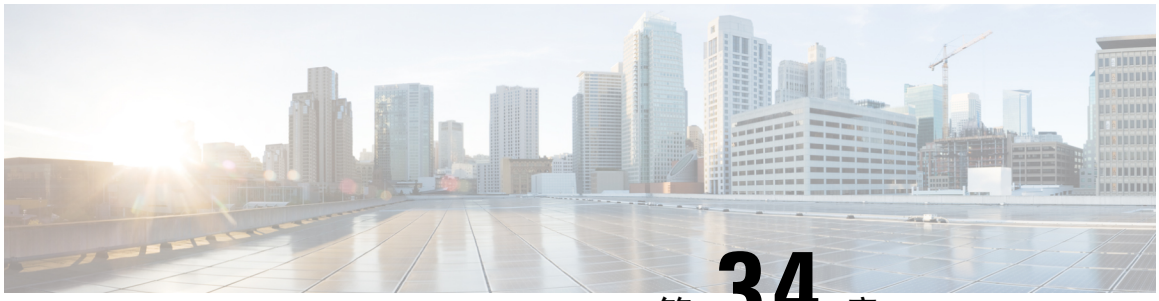
您可以使用命令行界面 (CLI) 对发布方节点上的网络时间协议 (NTP) 问题进行故障诊断。

过程

	命令或操作	目的
步骤 1	输入 **show network eth0 [detail]** 验证网络配置。	
步骤 2	输入 **utils ntp status** 验证 NTP 状态。	
步骤 3	输入 **utils ntp restart** 重新启动 NTP。	
步骤 4	输入 **utils ntp server list** 验证 NTP 服务器。	要添加或删除 NTP 服务器，请使用 **utils ntp server [add/delete]** CLI 命令。

第 VIII 部分

灾难恢复



第 34 章

备份系统

备份概述

Cisco 建议定期执行备份。 您可以使用灾难恢复系统 (DRS) 为群集中的所有服务器执行完整数据备份。 您可以设置自动备份或随时调用备份。

灾难恢复系统执行群集层级备份，这意味着它会将一个 Cisco Unified Communications Manager 群集中所有服务器的备份收集到中心位置，并将备份数据存档到物理存储设备。 备份文件已加密，并且只能由系统软件打开。

DRS 恢复其自己的设置（备份设备设置和计划设置）作为平台备份/恢复的一部分。 DRS 备份和恢复 drfDevice.xml 和 drfSchedule.xml 文件。 使用这些文件恢复服务器时，您无需重新配置 DRS 备份设备和计划。

当您执行系统数据恢复时，可以选择要恢复群集中的哪些节点。

灾难恢复系统包括以下功能：

- 用于执行备份和恢复任务的用户界面。
- 用于执行备份功能的分布式系统架构。
- 计划的备份或手动（用户调用）备份。
- 它会将备份存档到远程 sftp 服务器。

下表显示了灾难恢复系统可以备份和恢复的功能和组件。 对于您选择的每项功能，系统会自动备份所有的组件。

表 *85: Cisco Unified CM* 功能和组件

功能	组件
CCM - Unified Communications Manager	Unified Communications Manager 数据库
	平台
	功能配置
	音乐保持 (MOH)
	Cisco Emergency Responder
	批量工具 (BAT)
	首选项
	电话设备文件(TFTP)
	syslogagt（SNMP syslog 代理）
	cdpagent（SNMP cdp 代理）
	tct（跟踪收集工具）
	呼叫详细信息记录 (CDR)
	CDR 报告和分析 (CAR)

表 *86: IM and Presence* 功能和组件

功能	组件
IM and Presence Service	IM and Presence 数据库
	syslogagt（SNMP syslog 代理）
	cdpagent（SNMP cdp 代理）
	平台
	报告程序（功能配置报告程序）
	CUP SIP 代理
	XCP
	CLM
	批量工具 (BAT)
	首选项
	tct（跟踪收集工具）

备份前提条件

- 确保您符合版本要求：
  - 所有 Cisco Unified Communications Manager 群集节点都必须运行相同版本的 Cisco Unified Communications Manager 应用程序。
  - 所有 IM and Presence Service 群集节点都必须运行相同版本的 IM and Presence Service 应用程序。
  - 备份文件中保存的软件版本必须与群集节点上运行的版本匹配。

  整个版本字符串必须匹配。 例如，如果 IM and Presence 数据库发布方节点上的版本为 11.5.1.10000-1，则所有 IM and Presence 订阅方节点都必须是 11.5.1.10000-1，并且备份文件也必须是 11.5.1.10000-1。 如果您尝试从与当前版本不匹配的备份文件恢复系统，恢复将失败。 无论何时升级软件版本，都请确保备份系统，以使备份文件中保存的版本与群集节点上运行的版本匹配。
- 请注意，DRS 加密取决于群集安全密码。运行备份时，DRS 会生成一个随机密码用于加密，然后使用群集安全密码对随机密码进行加密。 如果在备份与此次恢复之间，群集安全密码发生了更改，那么您需要知道备份时的密码是什么，才能使用该备份文件恢复系统，或者，在安全密码更改/重置后立即进行备份。

- 如果想要备份到远程设备，请确保您拥有 SFTP 服务器设置。 有关可用 SFTP 服务器的详细信息，请参阅用于远程备份的 SFTP 服务器 ， 第 411 页

备份任务流程

完成这些任务以配置和运行备份。 备份正在运行时，不要执行任何操作系统管理任务。 这是因为灾难恢复系统会通过锁定平台 API 来阻止所有操作系统管理请求。 但是，灾难恢复系统不会阻止大多数 CLI 命令，因为只有基于 CLI 的升级命令使用平台 API 锁定软件包。

过程

	命令或操作	目的
步骤 1	配置备份设备 ， 第 406 页	指定要在其上备份数据的设备。
步骤 2	估算备份文件的大小 ， 第 407 页	估计在 SFTP 设备上创建的备份文件的大小。
步骤 3	选择下列选项之一： • 配置计划的备份 ， 第 408 页 • 开始手动备份 ， 第 409 页	创建一个备份计划以按计划备份数据。 或者，也可以运行手动备份。
步骤 4	查看当前备份状态 ， 第 410 页	可选。 检查备份的状态。 备份运行时，您可以检查当前备份作业的状态。
步骤 5	查看备份历史记录 ， 第 410 页	可选。 查看备份历史记录

配置备份设备

最多可以配置 10 个备份设备。 执行以下步骤以配置要存储备份文件的位置。

开始之前

- 确保您对 SFTP 服务器中的目录路径拥有写入访问权限，以存储备份文件。
- 确保用户名、密码、服务器名称和目录路径有效，因为 DRS Master Agent 会验证备份设备的配置。

注释 计划在预期网络通信量较少的时段期间进行备份。

过程

步骤 1 从灾难恢复系统中，选择**备份** > **备份设备**。

步骤 2 在**备份设备列表**窗口中，执行以下任一操作：

- 要配置新设备，请单击**新增**。
- 要编辑现有的备份设备，请输入搜索条件，单击“查找”，然后单击**选定编辑**。
- 要删除备份设备，请在**备份设备**列表中将其选中，然后单击**删除选定项**。

如果您将某备份设备配置为备份计划中的备份设备，则不能将其删除。

步骤 3 在**备份设备名称**字段中输入备份名称。

备份设备名称只能包含字母数字字符、空格 ()、破折号 (-) 和下划线 (_)。 请勿使用任何其他字符。

步骤 4 在**网络目录**下方的**选择目标**区域中，执行以下操作：

- 在**主机名/IP 地址**字段中，输入网络服务器的主机名或 IP 地址。
- 在**路径名**字段中，输入您要存储备份文件的目录路径。
- 在**用户名**字段，输入有效的用户名。
- 在**密码**字段中，输入有效的密码。
- 从**要存储在网络目录上的备份数量**下拉列表中，选择所需的备份数量。

步骤 5 单击**保存**。

下一步做什么

估算备份文件的大小，第 407 页

估算备份文件的大小

只有当存在一个或多个选定功能的备份历史记录时，Cisco Unified Communications Manager 才会估算备份 tar 的大小。

计算出的大小并非精确值，而是备份 tar 的估计大小。 系统会根据上一次成功备份的实际备份大小来计算，如果自上次备份后配置发生了更改，则大小可能会有所变化。

仅当存在先前的备份时，您才能使用此程序。若是第一次备份系统，则不可使用此程序。

按照此程序来估计保存到 SFTP 设备的备份 tar 的大小。

过程

步骤 1 从灾难恢复系统中，选择**备份** > **手动备份**。

步骤 2 在**选择功能**区域中，选择要备份的功能。

步骤 3 单击**估计大小**以查看所选功能备份的估计大小。

下一步做什么

执行以下程序之一以备份您的系统：

- 配置计划的备份，第 408 页
- 开始手动备份，第 409 页

配置计划的备份

最多可以创建 10 个备份计划。 每个备份计划都有自己的一组属性，包括自动备份计划、要备份的功能集和存储位置。

请注意，您的备份 .tar 文件已使用随机生成的密码加密。 然后会使用群集安全密码对此密码进行加密，并随备份 .tar 文件一起保存。 您必须记住此安全密码，或在安全密码更改或重置后立即进行备份。

注意 计划在非高峰时段备份以避免呼叫处理中断和影响服务。

开始之前

配置备份设备，第 406 页

过程

步骤 1 从灾难恢复系统中，选择**备份计划程序**。

步骤 2 在**计划列表**窗口中，执行以下步骤之一以添加新的计划或编辑一个现有的计划。

- 要创建新的计划，单击**新增**。
- 要配置现有的计划，单击“计划列表”列中的名称。

步骤 3 在**计划程序**窗口中，在**计划名称**字段中输入计划名称。

注释 您无法更改默认计划的名称。

步骤 4 在**选择备份设备**区域选择备份设备。

步骤 5 在**选择功能**区域选择要备份的功能。 必须至少选择一项功能。

步骤 6 在**开始备份时间**区域选择您希望开始备份的日期和时间。

步骤 7 在**频率**区域选择您希望进行备份的频率。 频率可以设置为“每天一次”、“每周”和“每月"。 如果选择**每周**，您还可以选择一周内哪几天进行备份。

提示 要将备份频率设置为**每周**，从星期二到星期六进行备份，可单击**设置默认值**。

步骤 8 要更新这些设置，单击**保存**。

步骤 9 选择下列选项之一：

- 要启用所选的计划，单击**启用所选计划**。
- 要禁用所选的计划，单击**禁用所选计划**。
- 要删除所选的计划，单击**删除选定项**。

步骤 10 要启用计划，单击**启用计划**。

下次备份将在您设置的时间自动进行。

注释 确保群集中的所有服务器都运行相同版本的 Cisco Unified Communications Manager 或 Cisco IM and Presence Service，并可通过网络接通。 在计划的备份时间无法接通的服务器将不会备份。

下一步做什么

执行以下程序：

- 估算备份文件的大小， 第 407 页
- （可选） 查看当前备份状态， 第 410 页

开始手动备份

开始之前

- 确保使用网络设备作为备份文件的存储位置。 Unified Communications Manager 的虚拟化部署不支持使用磁带驱动器存储备份文件。
- 确保所有群集节点都安装有相同的 Cisco Unified Communications Manager 版本或 IM and Presence Service。
- 备份过程可能会由于远程服务器上没有可用空间或由于网络连接中断而失败。 在解决导致备份失败的问题后，您需要开始一个全新备份。
- 确保没有网络中断。
- 配置备份设备， 第 406 页
- 估算备份文件的大小， 第 407 页
- 确保您有群集安全密码记录。 如果在完成此备份之后，群集安全密码发生了更改，您需要知道密码，否则将无法使用备份文件来恢复您的系统。

注释 备份运行时，您无法在“Cisco Unified 操作系统管理”或“Cisco Unified IM and Presence 操作系统管理”中执行任何任务，因为灾难恢复系统会锁定平台 API 来阻止所有请求。 但是，灾难恢复系统不会阻止大多数 CLI 命令，因为只有基于 CLI 的升级命令使用平台 API 锁定软件包。

过程

步骤 1 从灾难恢复系统中，选择**备份** > **手动备份**。

步骤 2 在**手动备份**窗口中，从**备份设备名称**区域选择备份设备。

步骤 3 从**选择功能**区域选择一项功能。

步骤 4 单击**开始备份**。

下一步做什么

（可选） 查看当前备份状态，第 410 页

查看当前备份状态

执行以下步骤以检查当前备份作业的状态。

注意 请注意，如果备份到远程服务器没有在 20 小时内完成，备份会话将超时，您必须开始一个全新备份。

过程

步骤 1 从灾难恢复系统中，选择**备份** > **当前状态**。

步骤 2 要查看备份日志文件，请单击日志文件名链接。

步骤 3 要取消当前备份，请单击**取消备份**。

注释 备份将在当前组件完成其备份操作后取消。

下一步做什么

查看备份历史记录，第 410 页

查看备份历史记录

如要查看备份历史记录，请执行以下步骤。

过程

步骤 1 从灾难恢复系统中，选择**备份** > **历史记录**。

步骤 2 从**备份历史记录**窗口中，您可以查看已执行的备份，包括文件名、备份设备、完成日期、结果、版本、已备份的功能，以及失败的功能。

注释 **备份历史记录**窗口只显示最近 20 次备份作业。

备份相互作用和限制

备份限制

以下限制适用于备份：

表 *87:* 备份限制

限制	说明
群集安全密码	我们建议您每当更改群集安全密码时都运行备份。 备份加密使用群集安全密码加密备份文件上的数据。 如果在创建备份文件后编辑群集安全密码，您将无法使用该备份文件恢复数据，除非您记得旧密码。
证书管理	灾难恢复系统 (DRS) 使用 Master Agent 与 Local Agent 之间基于 SSL 的通信，验证和加密 Unified Communications Manager群集节点之间的数据。 DRS 使用 Tomcat 证书进行其公钥/私钥加密。 请注意，如果您从“证书管理”页面删除 Tomcat 信任存储库 (hostname.pem) 文件，DRS 将不会按预期工作。 如果您手动删除 Tomcat-信任文件，必须确保将 Tomcat 证书上传到 Tomcat-信任。 有关更多详细信息，请参阅《Cisco Unified Communications Manager 安全指南》中的“证书管理”部分。

用于远程备份的 SFTP 服务器

要在网络上将数据备份到远程设备，您必须有经过配置的 SFTP 服务器。 对于内部测试，Cisco 使用 Cisco Prime Collaboration Deployment (PCD) 上的 SFTP 服务器（由 Cisco 打造，Cisco TAC 提供支持）。 参阅下表可大致了解 SFTP 服务器的选项：

使用下表中的信息来确定要在您的系统中使用哪种 SFTP 服务器解决方案。

表 *88: SFTP* 服务器信息

SFTP 服务器	信息
Cisco Prime Collaboration 部署上的 SFTP 服务器	此服务器是 Cisco 提供和测试的唯一 SFTP 服务器，并且完全受 Cisco TAC 支持。 版本兼容性取决于您的 Unified Communications Manager 版本和 Cisco Prime Collaboration 部署。 在升级其版本 (SFTP) 或 Unified Communications Manager 之前，请参阅《*Cisco Prime Collaboration* 部署管理指南》，以确保版本兼容。
来自技术合作伙伴的 SFTP 服务器	这些服务器由第三方提供，第三方测试。版本兼容性取决于第三方测试。如果升级其 SFTP 产品和/或升级版本兼容的 Unified Communications Manager，请参阅“技术合作伙伴”页面： https://marketplace.cisco.com
来自其他第三方的SFTP服务器	这些服务器由第三方提供，不受 Cisco TAC 官方支持。 版本兼容性乃尽力提供，以建立兼容的SFTP版本和Unified Communications Manager 版本。 **注释** 这些产品未经 Cisco 测试，我们无法保证其功能。 Cisco TAC 不支持这些产品。 要获取经过全面测试且受支持的 SFTP 解决方案，请使用 Cisco Prime Collaboration 部署或技术合作伙伴。

加密支持

对于 Unified Communications Manager 11.5，Unified Communications Manager 会为 SFTP 连接通告以下 CBC 密码：

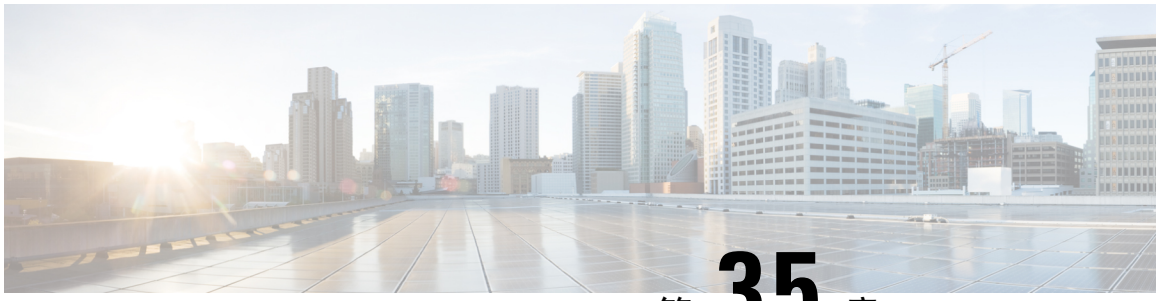
- aes128-cbc
- 3des-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr

注释 确保备份 SFTP 服务器支持其中一个密码以与 Unified Communications Manager 进行通信。

从 Unified Communications Manager 12.0 版起，不支持 CBC 密码。 Unified Communications Manager 仅支持和通告以下 CTR 密码：

- aes256-ctr
- aes128-ctr
- aes192-ctr

注释 确保备份 SFTP 服务器支持其中一个 CTR 密码与 Unified Communications Manager 进行通信。



第 35 章

恢复系统

恢复概述

灾难恢复系统 (DRS) 提供了一个向导，可带您了解恢复系统的过程。

备份文件是加密的，只有 DRS 系统可以打开它们以恢复数据。 灾难恢复系统包括以下功能：

- 用于执行恢复任务的用户界面。
- 用于执行恢复功能的分布式系统架构。

Master Agent

系统会自动在群集中的每个节点上启动 Master Agent 服务，但 Master Agent 仅在发布方节点上工作。订阅方节点上的 Master Agent 不执行任何功能。

Local Agent

服务器利用 Local Agent 执行备份和恢复功能。

Cisco Unified Communications Manager 群集中的每个节点，包括包含 Master Agent 的节点，必须有自己的 Local Agent 来执行备份和恢复功能。

注释 默认情况下，Local Agent 会在群集的每个节点自动启动，包括 IM and Presence 节点。

恢复前提条件

- 确保您符合版本要求：
  - 所有 Cisco Unified Communications Manager 群集节点都必须运行相同版本的 Cisco Unified Communications Manager 应用程序。
  - 所有 IM and Presence Service 群集节点都必须运行相同版本的 IM and Presence Service 应用程序。
  - 备份文件中保存的版本必须与群集节点上运行的版本匹配。

  整个版本字符串必须匹配。 例如，如果 IM and Presence 数据库发布方节点上的版本为 11.5.1.10000-1，则所有 IM and Presence 订阅方节点都必须是 11.5.1.10000-1，并且备份文件也必须是 11.5.1.10000-1。 如果您尝试从与当前版本不匹配的备份文件恢复系统，恢复将失败。
- 确保服务器的 IP 地址、主机名、DNS 配置和部署类型与备份文件上存储的 IP 地址、主机名、DNS 配置和部署类型匹配。
- 如果您自运行备份后更改了群集安全密码，请确保您有旧密码的记录，否则恢复将失败。
- 如果在群集中启用了 IPsec 策略，请确保在启动还原操作之前将其禁用。

恢复后重新启用 SAML SSO

重要事项 此部分仅适用于版本 12.5(1)SU7。

使用 DRS 恢复系统后，可以在群集中的任何节点间歇性禁用 SAML SSO。 要在受影响的节点上重新启用 SAML SSO，您必须执行以下操作：

1. 从 Cisco Unified CM 管理中，选择**系统** > **SAML 单点登录**。
2. 单击**运行 SSO 测试**。
3. 在您看到“**SSO 测试成功！**”消息，请关闭浏览器窗口；单击**完成**。

注释 在 SAML SSO 重新启用过程中，Cisco Tomcat 会重启。 它对已启用 SAML SSO 的节点不会有任何影响。

恢复任务流程

在恢复过程中，不要使用 Cisco Unified Communications Manager 操作系统管理或 Cisco Unified IM and Presence 操作系统管理执行任何任务。

过程

	命令或操作	目的
步骤 1	仅恢复第一个节点，第 417 页	（可选）使用此程序仅恢复群集中的第一个发布方节点。
步骤 2	恢复后续群集节点，第 419 页	（可选）使用此程序恢复群集中的订阅方节点。
步骤 3	发布方重建后在一个步骤中恢复群集，第420页	（可选）如果发布方已重建，按照此程序在一个步骤中恢复整个群集。
步骤 4	恢复整个群集，第 421 页	（可选）使用此程序恢复群集中的所有节点，包括发布方节点。 如果发生重大硬盘驱动器故障或升级，或如果硬盘驱动器迁移，您可能需要重建群集中的所有节点。
步骤 5	将节点或群集恢复到上次已知的良好配置，第 423 页	（可选）仅当将节点恢复到上次已知的良好配置时，才使用此程序。 硬盘驱动器故障或其他硬件故障后不要使用此程序。
步骤 6	重新启动节点，第 423 页	使用此程序重新启动节点。
步骤 7	检查恢复作业状态，第 424 页	（可选）使用此程序检查恢复作业状态。
步骤 8	查看恢复历史记录，第 425 页	（可选）使用此程序查看恢复历史记录。

仅恢复第一个节点

若要在重建后恢复第一个节点，您必须配置备份设备。

此程序适用于 Cisco Unified Communications Manager 第一个节点，也称为发布方节点。 其他 Cisco Unified Communications Manager 节点和所有 IM and Presence Service 节点均被视为辅助节点或订阅方。

开始之前

如果群集中有 IM and Presence Service 节点，确保当您恢复第一个节点时该节点正在运行并且可以访问。 这是必需的，以便在执行程序期间可以找到有效的备份文件。

过程

步骤 1 从灾难恢复系统中，选择**恢复** > **恢复向导**。

步骤 2 在**恢复向导步骤 1** 窗口中，**选择备份设备**区域，选择要恢复的适当的备份设备。

步骤 3 单击**下一步**。

步骤 4 在**恢复向导步骤 2** 窗口中，选择要恢复的备份文件。

注释 备份文件名会指示系统创建备份文件的日期和时间。

步骤 5 单击**下一步**。

步骤 6 在**恢复向导步骤 3** 窗口中，单击**下一步**。

步骤 7 选择要恢复的功能。

注释 随即将显示您为备份选择的功能。

步骤 8 单击**下一步**。 此时将显示“恢复向导步骤 4”窗口。

步骤 9 如果要运行文件完整性检查，请选中“使用 SHA1 消息摘要执行文件完整性检查”复选框。

注释 文件完整性检查是可选操作，仅在 SFTP 备份中需要。

请注意，文件完整性检查过程会消耗大量的 CPU 和网络带宽，从而减慢恢复速度。

我们也可以在 FIPS 模式下使用 SHA-1 进行消息摘要验证。 SHA-1 允许哈希函数应用程序（如 HMAC 和随机位生成）中使用的所有非数字签名，这些应用程序不用于数字签名。 例如，SHA-1 仍可用于计算校验和。 仅用于签名生成和验证，不能使用 SHA-1。

步骤 10 选择要恢复的节点。

步骤 11 单击**恢复**以恢复数据。

步骤 12 单击**下一步**。

步骤 13 当系统提示您选择要恢复的节点时，仅选择第一个节点（发布方）。

注意 在此情况下，不要选择后续（订阅方）节点，因为这将导致恢复尝试失败。

步骤 14 （可选）从**选择服务器名称**下拉列表中，选择要从其中恢复发布方数据库的订阅方节点。 确保您选择的订阅方节点正在运行并连接到群集。
灾难恢复系统会从备份文件恢复所有非数据库信息，并从所选的订阅方节点拉取最新的数据库。

注释 仅当您选择的备份文件包含 CCMDB 数据库组件，此选项才会出现。 最初，仅发布方节点会完全恢复，但当您执行第 14 步并重新启动后续群集节点时，灾难恢复系统将执行数据库复制，并完全同步所有群集节点数据库。 这可确保所有群集节点都使用当前数据。

步骤 15 单击**恢复**。

步骤 16 您的数据会在发布方节点上恢复。 视您的数据库大小和选择要恢复的组件，系统可能需要几个小时才能恢复。

注释 恢复第一个节点，会将整个 Cisco Unified Communications Manager 数据库恢复到群集。这可能需要几个小时，具体取决于节点的数量和正在恢复的数据库的大小。 视您的数据库大小和选择要恢复的组件，系统可能需要几个小时才能恢复。

步骤 17 当**恢复状态**窗口上的**完成百分比**字段显示 100% 时，重启服务器。 如果仅恢复到第一个节点，需要重新启动群集中的所有节点。确保先重启第一个节点，然后再重启后续节点。有关如何重启服务器的信息，请参阅“下一步操作”部分。

注释 如果您要仅恢复 Cisco Unified Communications Manager 节点，必须重新启动 Cisco Unified Communications Manager 和 IM and Presence Service 群集。

如果您要仅恢复 IM and Presence Service 发布方节点，必须重新启动 IM and Presence Service 群集。

下一步做什么

- （可选）要查看恢复状态，请参阅检查恢复作业状态，第 424 页
- 要重新启动节点，请参阅 重新启动节点，第 423 页

恢复后续群集节点

此程序仅适用于 Cisco Unified Communications Manager 订阅方（后续）节点。 安装的第一个 Cisco Unified Communications Manager 节点是发布方节点。 所有其他 Cisco Unified Communications Manager 节点和所有 IM and Presence Service 节点都是订阅方节点。

按照此程序恢复群集中的一个或多个 Cisco Unified Communications Manager 订阅方节点。

开始之前

在执行恢复操作之前，确保恢复的主机名、IP 地址、DNS 配置和部署类型与您要恢复的备份文件的主机名、IP 地址、DNS 配置和部署类型匹配。 灾难恢复系统不会跨不同的主机名、IP 地址、DNS 配置和部署类型恢复。

确保服务器上安装的软件版本与您要恢复的备份文件的版本匹配。 灾难恢复系统只支持匹配的软件版本进行恢复操作。 若要在重建后恢复后续节点，您必须配置备份设备。

过程

步骤 1 从灾难恢复系统中，选择**恢复** > **恢复向导**。

步骤 2 在**恢复向导步骤 1** 窗口中，**选择备份设备**区域，选择要从其中恢复的备份设备。

步骤 3 单击**下一步**。

步骤 4 在**恢复向导步骤 2** 窗口中，选择要恢复的备份文件。

步骤 5 单击**下一步**。

步骤 6 在**恢复向导步骤 3** 窗口中，选择要恢复的功能。

注释 只会显示那些备份到您所选文件的功能。

步骤 7 单击**下一步**。 此时将显示“恢复向导步骤 4”窗口。

步骤 8 在**恢复向导步骤 4** 窗口中，当系统提示您选择要恢复的节点时，请只选择后续节点。

步骤 9 单击**恢复**。

步骤 10 您的数据会在后续节点上恢复。 有关如何查看恢复状态的详细信息，请参阅“下一步操作”部分。

注释 在恢复过程中，不要使用“Cisco Unified Communications Manager 管理”或“用户选项”执行任何任务。

步骤 11 当**恢复状态**窗口上的**完成百分比**字段显示 100% 时，重启刚刚恢复的辅助服务器。 如果仅恢复到第一个节点，需要重新启动群集中的所有节点。确保先重启第一个节点，然后再重启后续节点。有关如何重启服务器的信息，请参阅“下一步操作”部分。

注释 如果恢复了 IM and Presence Service 第一个节点， 确保在重新启动 IM and Presence Service 后续节点之前，重新启动 IM and Presence Service 第一个节点。

下一步做什么

- （可选）要查看恢复状态，请参阅检查恢复作业状态， 第 424 页
- 要重新启动节点，请参阅 重新启动节点， 第 423 页

发布方重建后在一个步骤中恢复群集

视您的数据库大小和选择要恢复的组件，系统可能需要几个小时才能恢复。（可选）如果发布方已重建或新装，按照此程序在一个步骤中恢复整个群集。

过程

步骤 1 从灾难恢复系统中，选择**恢复** > **恢复向导**。

步骤 2 在**恢复向导步骤 1** 窗口中，**选择备份设备**区域，选择要从其中恢复的备份设备。

步骤 3 单击**下一步**。

步骤 4 在**恢复向导步骤 2** 窗口中，选择要恢复的备份文件。

备份文件名会指示系统创建备份文件的日期和时间。

仅选择您要从其中恢复整个群集的那一个群集的备份文件。

步骤 5 单击**下一步**。

步骤 6 在**恢复向导步骤 3** 窗口中，选择要恢复的功能。

屏幕仅会显示那些被保存到备份文件中的功能。

步骤 7 单击**下一步**。

步骤 8 在**恢复向导步骤 4** 窗口中，单击**一步恢复**。

仅当选择进行恢复的备份文件为群集的备份文件，且选择进行恢复的功能包括在发布方和订阅方节点都进行了注册的功能时，此选项才会出现在**恢复向导步骤 4** 窗口中。 有关详细信息，请参阅仅恢复第一个节点，第 417 页和恢复后续群集节点，第 419 页。

注释 如果状态消息指示“发布方未能变成群集感知。 无法开始一步恢复”，则您需要恢复发布方节点，然后再恢复订阅方节点。 有关详细信息，请参阅相关主题。

此选项允许发布方变成群集感知，将需要五分钟来执行此操作。 单击此选项后，即会显示一条状态消息：“请等待 5 分钟，直到发布方变成群集感知，在此期间请不要开始任何备份或恢复活动”。

延迟后，如果发布方变成群集感知，则会一条状态消息：“发布方已变成群集感知。请选择服务器，然后单击“恢复”以开始恢复整个群集”。”

延迟后，如果发布方未变成群集感知，则会一条状态消息：“发布方未能变成群集感知。无法开始一步恢复。 请继续并执行正常的两步恢复。" 要以两步（先发布方，然后订阅方）恢复整个群集，请执行仅恢复第一个节点，第 417 页和恢复后续群集节点，第 419 页中所述的步骤。

步骤 9 当系统提示您选择要恢复的节点时，选择群集中的所有节点。

当恢复第一个节点后，灾难恢复系统会自动在后续节点上恢复 Cisco Unified Communications Manager 数据库 (CCMDB)。 这可能需要几个小时，具体取决于节点的数量和正在恢复的数据库的大小。

步骤 10 单击**恢复**。
您的数据会在群集中的所有节点上恢复。

步骤 11 当**恢复状态窗口**上的**完成百分比**字段显示 100% 时，重启服务器。 如果仅恢复到第一个节点，需要重新启动群集中的所有节点。确保先重启第一个节点，然后再重启后续节点。有关如何重启服务器的信息，请参阅“下一步操作”部分。

下一步做什么

- （可选）要查看恢复状态，请参阅检查恢复作业状态，第 424 页
- 要重新启动节点，请参阅 重新启动节点，第 423 页

恢复整个群集

如果发生重大硬盘驱动器故障或升级，或如果硬盘驱动器迁移，您得重建群集中的所有节点。 执行这些步骤以恢复整个群集。

如果您正在做大多数其他类型的硬件升级，例如更换网卡或添加内存，则您不需要执行此程序。

过程

步骤 1 从灾难恢复系统中，选择**恢复** > **恢复向导**。

步骤 2 在**选择备份设备**区域，选择要恢复的适当的备份设备。

步骤 3 单击**下一步**。

步骤 4 在**恢复向导步骤 2** 窗口中，选择要恢复的备份文件。

注释 备份文件名会指示系统创建备份文件的日期和时间。

步骤 5 单击**下一步**。

步骤 6 在**恢复向导步骤 3** 窗口中，单击**下一步**。

步骤 7 在**恢复向导步骤 4** 窗口中，当提示选择恢复节点时，选择所有节点。

步骤 8 单击**恢复**以恢复数据。

当恢复第一个节点后，灾难恢复系统会自动在后续节点上恢复 Cisco Unified Communications Manager 数据库 (CCMDB)。 这可能需要几个小时，具体取决于节点的数量和数据库的大小。

数据会恢复到所有节点上。

注释 在恢复过程中，不要使用“Cisco Unified Communications Manager 管理”或“用户选项”执行任何任务。

视您的数据库大小和选择要恢复的组件，系统可能需要几个小时才能恢复。

步骤 9 在恢复过程完成后，重新启动服务器。 请参阅“下一步操作”部分，了解有关如何重启服务器的详细信息。

注释 确保先重启第一个节点，然后再重启后续节点。

在第一个节点重新启动并运行恢复的 Cisco Unified Communications Manager 版本后，重新启动后续节点。

步骤 10 群集重启后，将会自动设置复制。 通过使用《*Cisco Unified Communications* 解决方案的命令行界面参考指南》中所述的 “utils dbreplication runtimestate” CLI 命令，检查所有节点上的“复制状态”值。 每个节点上的值应等于 2。

注释 后续节点重新启动后，在后续节点上的数据库复制可能需要足够的时间才能完成，具体视群集的大小而定。

提示 如果复制未正确设置，使用如《*Cisco Unified Communications* 解决方案的命令行界面参考指南》中所述的 "utils dbreplication rebuild" CLI 命令。

下一步做什么

- （可选）要查看恢复状态，请参阅检查恢复作业状态， 第 424 页

- 要重新启动节点，请参阅 重新启动节点 ，第 423 页

将节点或群集恢复到上次已知的良好配置

按照此程序将节点或群集恢复到上次已知的良好配置。

开始之前

- 确保恢复文件包含主机名、IP 地址、DNS 配置，以及在备份文件中配置的部署类型。
- 确保服务器上安装的 Cisco Unified Communications Manager 版本与您要恢复的备份文件的版本匹配。
- 确保仅将此程序用于将节点恢复到上次已知的良好配置。

过程

步骤 1 从灾难恢复系统中，选择**恢复** > **恢复向导**。

步骤 2 在**选择备份设备**区域，选择要恢复的适当的备份设备。

步骤 3 单击**下一步**。

步骤 4 在**恢复向导步骤 2** 窗口中，选择要恢复的备份文件。

注释 备份文件名会指示系统创建备份文件的日期和时间。

步骤 5 单击**下一步**。

步骤 6 在**恢复向导步骤 3** 窗口中，单击**下一步**。

步骤 7 当系统提示选择恢复节点时，选择适当的节点。
数据会恢复到所选的节点上。

步骤 8 重新启动群集中的所有节点。 重新启动第一个 Cisco Unified Communications Manager 节点，然后再重启后续 Cisco Unified Communications Manager 节点。 如果群集还有 Cisco IM and Presence 节点，则重新启动第一个 Cisco IM and Presence 节点，然后再重启后续 IM and Presence 节点。 请参阅“下一步操作”部分，了解详细信息。

重新启动节点

恢复数据之后，您必须重新启动节点。

如果要恢复发布方节点（第一个节点），您必须先重新启动发布方节点。仅在发布方节点已重新启动并成功运行恢复的软件版本后，才重新启动订阅方节点。

注释 如果 CUCM 发布方节点离线，请勿重新启动 IM and Presence 订阅方节点。在这种情况下，节点服务将无法启动，因为订阅方节点无法连接到 CUCM 发布方。

注意 此程序将导致系统重新启动，并且临时停止服务。

在需要重新启动的群集中的每个节点上执行此程序。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**设置** > **版本**。

步骤 2 要重新启动节点，单击**重新启动**。

步骤 3 群集重启后，将会自动设置复制。通过使用 **utils dbreplication runtimestate** CLI 命令，检查所有节点上的“复制状态”值。每个节点上的值应等于2。有关CLI命令的详细信息，请参阅《Cisco Unified Communications (CallManager) 命令参考。

如果复制未正确设置，使用如《*Cisco Unified Communications* 解决方案的命令行界面参考指南》中所述的 **utils dbreplication reset** CLI 命令。

注释 后续节点重新启动后，在后续节点上的数据库复制可能需要几个小时才能完成，具体视群集的大小而定。

下一步做什么

（可选）要查看恢复状态，请参阅检查恢复作业状态 ， 第 424 页。

检查恢复作业状态

按照此程序检查恢复作业状态。

过程

步骤 1 从灾难恢复系统中，选择**恢复** > **当前状态**。

步骤 2 在**恢复状态**窗口中，单击日志文件名链接以查看恢复状态。

查看恢复历史记录

如要查看恢复历史记录，请执行以下步骤。

过程

步骤 1 从灾难恢复系统中，选择**恢复** > **历史记录**。

步骤 2 从**恢复历史记录**窗口中，您可以查看已执行的恢复，包括文件名、备份设备、完成日期、结果、版本、已恢复的功能，以及失败的功能。

恢复历史记录窗口只显示最近 20 次恢复作业。

数据验证

跟踪文件

在故障诊断或收集日志期间使用以下跟踪文件位置。

Master Agent、GUI、每个 Local Agent 和 JSch 库的跟踪文件将写入到以下位置：

- 对于 Master Agent，查找位于 platform/drf/trace/drfMA0* 的跟踪文件
- 对于每个 Local Agent，查找位于 platform/drf/trace/drfLA0* 的跟踪文件
- 对于 GUI，查找位于 platform/drf/trace/drfConfLib0* 的跟踪文件
- 对于 JSch，查找位于 platform/drf/trace/drfJSch* 的跟踪文件

有关详细信息，请参阅位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html 的《*Cisco Unified Communications* 解决方案的命令行界面参考指南》。

命令行界面

灾难恢复系统还提供对备份和恢复功能子集的命令行访问，如下表中所示。有关这些命令和使用命令行界面的详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面参考指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html。

表 *89:* 灾难恢复系统命令行界面

命令	说明
utils disaster_recovery estimate_tar_size	显示来自 SFTP /本地设备的备份 tar 的估计大小，需要一个功能列表的参数
utils disaster_recovery backup	通过使用在灾难恢复系统界面中配置的功能开始手动备份
utils disaster_recovery jschLogs	启用或禁用 JSch 库日志记录
utils disaster_recovery restore	开始恢复，需要备份位置、文件名、功能以及要恢复的节点的参数
utils disaster_recovery status	显示正在进行的备份或恢复作业的状态
utils disaster_recovery show_backupfiles	显示现有备份文件
utils disaster_recovery cancel_backup	取消正在进行的备份作业
utils disaster_recovery show_registration	显示当前配置的注册
utils disaster_recovery device add	添加网络设备
utils disaster_recovery device delete	删除设备
utils disaster_recovery device list	列出所有设备
utils disaster_recovery schedule add	添加计划
utils disaster_recovery schedule delete	删除计划
utils disaster_recovery schedule disable	禁用计划
utils disaster_recovery schedule enable	启用计划
utils disaster_recovery schedule list	列出所有计划
utils disaster_recovery backup	通过使用在灾难恢复系统界面中配置的功能开始手动备份。
utils disaster_recovery restore	开始恢复，需要备份位置、文件名、功能以及要恢复的节点的参数。
utils disaster_recovery status	显示正在进行的备份或恢复作业的状态。

命令	说明
utils disaster_recovery show_backupfiles	显示现有备份文件。
utils disaster_recovery cancel_backup	取消正在进行的备份作业。
utils disaster_recovery show_registration	显示当前配置的注册。

警报和消息

警报和消息

灾难恢复系统会发出备份或恢复程序期间可能发生的各种错误的警报。 下表提供了 Cisco 灾难恢复系统警报的列表。

表 *90:* 灾难恢复系统警报和消息

警报名称	说明	说明
DRFBackupDeviceError	DRF 备份过程在访问设备时出现问题。	DRS 备份过程在访问设备时
DRFBackupFailure	Cisco DRF 备份过程失败。	DRS 备份过程遇到错误。
DRFBackupInProgress	其他备份仍在运行时，新备份无法启动	DRS 在其他备份仍在运行时 备份。
DRFInternalProcessFailure	DRF 内部过程遇到错误。	DRS 内部过程遇到错误。
DRFLA2MAFailure	DRF Local Agent 无法连接到 Master Agent。	DRS Local Agent 无法连接 Agent。
DRFLocalAgentStartFailure	DRF Local Agent 未启动。	DRS Local Agent 可能已关
DRFMA2LAFailure	DRF Master Agent 没有连接到 Local Agent。	DRS Master Agent 无法连接 Agent。
DRFMABackupComponentFailure	DRF 无法备份至少一个组件。	DRS 请求组件备份其数据； 中发生错误，该组件没有
DRFMABackupNodeDisconnect	进行备份的节点在完全备份之前即从 Master Agent 断开连接。	DRS Master Agent 在 Cisco Communications Manager 节 份操作时，节点在备份操作 开连接。

警报名称	说明	说明
DRFMARestoreComponentFailure	DRF 无法恢复至少一个组件。	DRS 请求组件恢复其数据；但中发生错误，该组件没有得到
DRFMARestoreNodeDisconnect	进行恢复的节点在完全恢复之前即从 Master Agent 断开连接。	DRS Master Agent 在 Cisco Un Communications Manager 节点复操作时，节点在恢复操作完开连接。
DRFMasterAgentStartFailure	DRF Master Agent 未启动。	DRS Master Agent 可能出现故
DRFNoRegisteredComponent	没有可用的注册组件，因此备份失败。	由于没有可用的注册组件，因备份失败。
DRFNoRegisteredFeature	没有为备份选择任何功能。	没有为备份选择任何功能。
DRFRestoreDeviceError	DRF 恢复过程在访问设备时出现问题。	DRS 恢复过程无法从设备读取
DRFRestoreFailure	DRF 恢复过程失败。	DRS 恢复过程遇到错误。
DRFSftpFailure	DRF SFTP 操作有错误。	DRS SFTP 操作中存在错误。
DRFSecurityViolation	DRF 系统检测到可导致安全违规的恶意模式。	DRF 网络消息包含可导致安全意模式，如代码注入或目录遍网络消息已被阻止。
DRFTruststoreMissing	节点上缺少 IPsec 信任库。	节点上缺少 IPsec 信任库。 DF Agent 无法连接到 Master Ager
DRFUnknownClient	公共网络上的 DRF Master Agent 收到来自群集外部未知服务器的客户端连接请求。 该请求已被拒绝。	公共网络上的 DRF Master Age 自群集外部未知服务器的客户求。 该请求已被拒绝。
DRFBackupCompleted	DRF 备份成功完成。	DRF 备份成功完成。
DRFRestoreCompleted	DRF 恢复成功完成。	DRF 恢复成功完成。
DRFNoBackupTaken	DRF 找不到当前系统的有效备份。	DRF 在升级/迁移或全新安装后当前系统的有效备份。
DRFComponentRegistered	DRF 成功注册所请求的组件。	DRF 成功注册所请求的组件。
DRFRegistrationFailure	DRF 注册操作失败。	DRF 对组件的注册操作由于某误而失败。
DRFComponentDeRegistered	DRF 成功注销所请求的组件。	DRF 成功注销所请求的组件。
DRFDeRegistrationFailure	DRF 对组件的注销请求失败。	DRF 对组件的注销请求失败。
DRFFailure	DRF 备份或恢复过程失败。	DRF 备份或恢复过程遇到错误

警报名称	说明	说明
DRFRestoreInternalError	DRF 恢复操作遇到错误。 恢复已内部取消。	DRF 恢复操作遇到错误。取消。
DRFLogDirAccessFailure	DRF 无法访问日志目录。	DRF 无法访问日志目录。
DRFDeRegisteredServer	DRF 自动注销服务器的所有组件。	服务器可能已从 Unified Co Manager 群集断开连接。
DRFSchedulerDisabled	DRF 计划程序被禁用，因为没有配置的功能可用于备份。	DRF 计划程序被禁用，因为功能可用于备份
DRFSchedulerUpdated	DRF 计划的备份配置由于功能注销而自动更新。	DRF 计划的备份配置由于功动更新

许可证预留

许可证预留

重要事项 以下许可证功能表在 Unified CM 14SU1 发行版之前一直受支持。

在启用特定许可证保留或永久许可证保留的 Unified Communications Manager 上执行恢复操作后，执行以下步骤。

表 *91:* 用于许可证预留的灾难恢复系统

恢复后的状态	**CSSM** 上的产品	解决方案
未注册	是	联系 Cisco 以从 CSSM 中删除产品，然后从产品注册。
	否	无需任何操作

恢复后的状态	CSSM 上的产品	解决方案
正在保留	是	完成以下任一程序： 程序 1： 1. 从 CSSM 获取产品的授权码。 2. 提供授权码以运行以下 CLI **license smart reservation return-authorization "<authorization-code>"**。 程序 2： 1. 联系 Cisco 以从 CSSM 中删除产品。
	否	从产品执行 CLI **license smart reservation cancel**。
已注册 - 特定许可证预留或已注册 - 通用许可证预留 **注释** 智能代理可能会将状态视为通用许可证预留，但适用于永久许可证预留功能。	是	1. 从产品执行以下 CLI **license smart reservation return**。 保留返回代码将打印在控制台上。 2. 在 CSSM 上输入保留返回代码以删除产品。
	否	从产品执行 CLI **license smart reservation return**。

许可证信息

许可证信息

重要事项 以下许可证功能表从 Unified CM 14SU2 发行版起受支持。

在同意通信管理器上执行恢复操作后，执行以下步骤。

表 *92:* 用于许可的灾难恢复系统

恢复后的状态	备份状态	CSSM或卫星上的产品	解决方案
未注册	在启用特定许可证保留或永久许可证保留的统一通信管理器上执行恢复操作	是	与 Cisco 联系以从 CSSM 中删除该产品，然后从Unified CM执行许可证预留操作。
		否	不需要操作。
	在为CSSM或附属注册的统一通信管理器上恢复操作	是	CSSM 或卫星上无需任何操作。 从产品重新注册。
		否	不需要操作。
	在已注册用于CSSM和授权导出限制许可的统一通信管理器上恢复操作	是	CSSM 或卫星上无需任何操作。 从产品重新注册并请求导出受限制的许可。
		否	不需要操作。
	在为CSSM附属和授权导出限制许可证注册的统一通信管理器上恢复操作	是	联系 Cisco 以从 CSSM 和 Cisco Smart Software Manager satellite 中删除该产品。然后，从产品注册，并要求从产品导出限制的许可。
		否	不需要操作。

恢复相互作用和限制

恢复相互作用和限制

以下限制适用于使用灾难恢复系统恢复 Cisco Unified Communications Manager 或 IM and Presence Service

表 *93:* 恢复限制

限制	说明
出口受限	来自受限版本的 DRS 备份只能恢复到受限版本，而来自不受限版本的备份只能恢复到不受限版本。请注意，如果您升级到美国出口不受限版本的统一通信管理器，日后您将无法升级到该软件的美国出口受限版本，或无法执行受限版本的全新安装
平台迁移	您不能使用灾难恢复系统在平台之间（例如，从 Windows 到 Linux 或从 Linux 到 Windows）迁移数据。 恢复必须运行在与备份相同的产品版本上。 有关从基于 Windows 的平台将数据迁移到基于 Linux 的平台的信息，请参阅数据迁移助手用户手册。
硬件更换和迁移	当您执行 DRS 恢复将数据迁移到新服务器时，必须为新服务器分配与旧服务器所使用的完全相同的 IP 地址和主机名。 此外，如果进行备份时配置了 DNS，则在执行恢复之前，必须进行相同的 DNS 配置。 有关更换服务器的详细信息，请参阅 《为 *Cisco* 统一通信管理器更换单个服务器或群集指南》。 此外，更换硬件后，您必须运行证书信任列表 (CTL) 客户端。 如果不恢复后续节点（订阅方）服务器，您必须运行 CTL 客户端。在其他情况下，DRS 会备份您需要的证书。 有关详细信息，请参阅《*Cisco Unified Communications Manager* 安全指南》中的“安装 CTL 客户端”和“配置 CTL 客户端”程序。
跨群集分机移动	备份时登录到远程群集的跨群集分机移动用户，恢复后应会保持登录。

注释 智能许可证管理器不会作为 DRS 备份/恢复的一部分进行备份或恢复。

在成功恢复统一通信管理器服务器组件后，统一通信管理器将处于未注册状态。 然后，向 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 注册 Cisco 统一通信管理器。

如果执行备份之前产品已注册，那么重新注册产品以更新许可证信息。

如果产品在进行备份之前已获得出口限制的许可，并且 Cisco Smart Software Manager 或 cisco Smart Software Manager 卫星中存在产品实例，请联系 Cisco 以从 CSSM 和 Cisco Smart Software Manager 卫星中删除该产品，然后在使用卫星部署时从产品注册。 对于直接部署，重新注册产品并请求导出受限制的许可。

有关如何使用 Cisco Smart Software Manager 或 Cisco Smart Software Manager 卫星注册产品的详细信息，请参阅您版本的 Cisco Unified Communications Manager 系统配置指南 。

故障诊断

DRS 恢复到较小的虚拟机失败

问题

如果您将 IM and Presence Service 节点恢复到磁盘较小的 VM 上，数据库恢复可能会失败。

原因

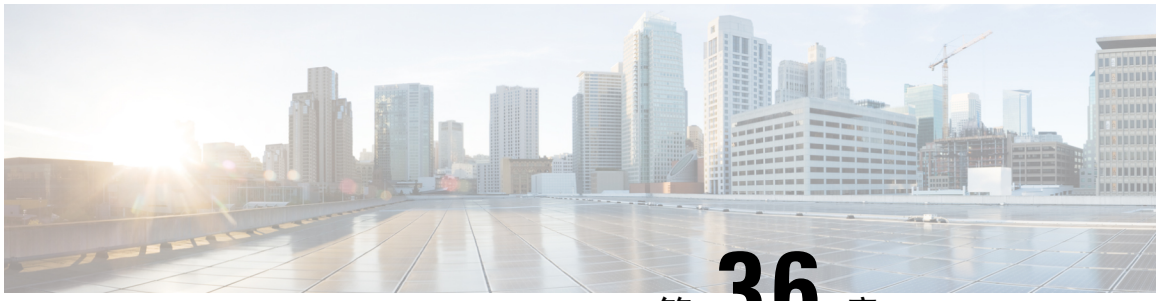
当从较大的磁盘迁移到较小的磁盘时会发生此故障。

解决方案

部署 VM 以从具有 2 个虚拟磁盘的 OVA 模板恢复。

第 IX 部分

故障诊断



第 36 章

故障诊断概述

本节提供对 Unified Communications Manager 进行故障诊断所需的背景信息和可用资源。

Cisco Unified 功能配置

Cisco Unified 功能配置 是基于 Web 的故障诊断工具，适用于 Unified Communications Manager，它提供以下功能，可帮助管理员排查系统问题：

- 保存用于故障诊断的 Unified Communications Manager 服务警报和事件，并提供警报消息定义。
- 将 Unified Communications Manager 服务跟踪信息保存到各种日志文件中，用于排除诊断。 管理员可以配置、收集和查看跟踪信息。
- 通过实时监控工具 (RTMT) 来监控 Unified Communications Manager 群集中各组件的实时操作。
- 通过 Unified Communications Manager CDR 分析和报告 (CAR) 生成服务质量、流量和计费信息的报告。
- 提供功能服务，您可通过“服务启动”窗口来激活、禁用和查看这些服务。
- 提供用于启动和停止功能及网络服务的界面。
- 存档与 Cisco Unified 功能配置 工具关联的报告。
- 允许 Unified Communications Manager 像受管设备一样工作，以便进行 SNMP 远程管理和故障诊断。
- 监控一个服务器（或群集中的所有服务器）上日志分区的磁盘使用量。

从“导航”下拉列表框中选择 Cisco Unified 功能配置，以便从 Cisco Unified Communications Manager 管理 窗口访问 Cisco Unified 功能配置。 安装 Unified Communications Manager 软件时会自动安装 Cisco Unified 功能配置 并使其可用。

有关功能配置工具的详细信息和配置程序，请参阅《*Cisco Unified* 功能配置管理指南》。

Cisco Unified Communications 操作系统管理

借助 *Cisco Unified Communications* 操作系统管理，您可以执行以下任务来配置和管理 *Cisco Unified Communications* 操作系统：

- 检查软件和硬件状态。
- 检查和更新 IP 地址。
- Ping 其他网络设备。
- 管理网络时间协议服务器。
- 升级系统软件和选项。
- 重新启动系统。

有关功能配置工具的详细信息和配置程序，请参阅 Cisco Unified Communications Manager 管理指南。

解决问题的一般模式

排查电话或 IP 网络环境的故障时，请界定具体的故障现象，确定会造成这些现象的所有可能的问题，然后系统地消除每个可能的问题（从最有可能的问题到最不可能的问题），直至现象消失。

以下步骤提供了在解决问题的过程中要使用的指导信息。

程序

1. 分析网络故障并创建清晰的问题说明。 界定故障现象和可能的原因。
2. 收集必要的实际情况来帮助分析出可能的原因。
3. 根据您收集到的实际情况考虑可能的原因。
4. 根据这些原因制定行动计划。 从最有可能的问题开始，并制定一个计划，在该计划中仅处理一个变量。
5. 实施行动计划。在测试期间仔细执行每个步骤，观察故障现象是否消失。
6. 分析结果以确定问题是否已解决。 如果问题已解决，则可以考虑结束故障诊断过程。
7. 如果问题仍未解决，请根据清单上的下一个最可能原因制定行动计划。 返回4，第 438 页并重复故障诊断过程，直至问题得到解决。

请确保撤消实施行动计划时所作的任何更改。 请记住，一次仅可更改一个变量。

注释 如果您用尽了所有常见的原因和措施（无论是本文档中列出的，还是您在环境中确定的其他措施），请联系 Cisco TAC。

网络故障准备

如果事先做好准备，则可以更容易地从网络故障中恢复。 要确定您是否对网络故障做好了准备，请回答以下问题：

- 您是否有您的互联网络的准确物理图和逻辑图（其中描绘了网络中所有设备的物理位置和连接方式）以及网络地址、网络编号和子网的逻辑图？
- 您是否维护了一份清单，其中包含您在网络中为实施的每个协议实施的所有网络协议，并列出了与之关联的网络号、子网络、区域和领域？
- 您是否知道正在使用哪些路由协议，以及每个协议最新的正确配置信息？
- 您是否知道桥接了哪些协议？ 这些桥中是否配置了任何过滤器，是否有这些配置的副本？ 这是否适用于 Unified Communications Manager？
- 您是否知道与外部网络（包括到 Internet 的任何连接）的所有接触点？ 对于每个外部网络连接，您是否知道使用的是哪种路由协议？
- 您的组织是否已记录正常的网络行为和性能，以便将其作为基准与当前的问题进行比较？

如果您对这些问题的回答都为“是”，则可以从网络故障中快速恢复。

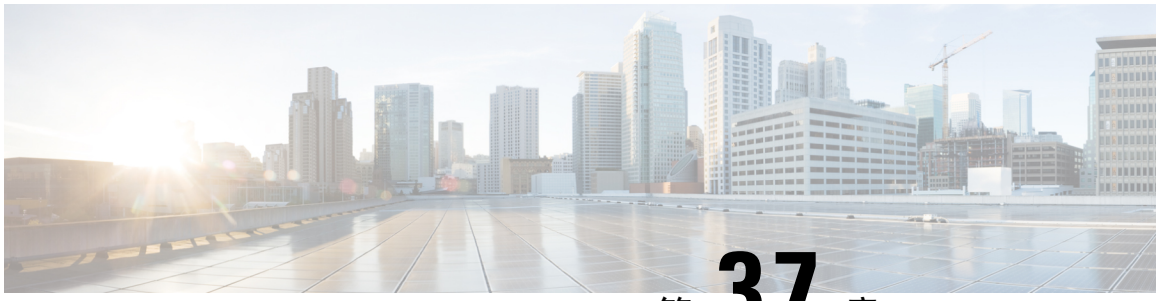
获取详细信息的渠道

有关各种 IP 电话主题的信息，请访问以下链接：

- 有关相关 Cisco IP 电话应用程序和产品的进一步信息，请参阅《*Cisco Unified Communications Manager* 文档指南》。以下 URL 显示了文档指南的路径示例：

  https://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html
- 与 Cisco Unity 相关的文档，请参阅以下 URL：
  https://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html
- 与 Cisco Emergency Responder 相关的文档，请参阅以下 URL：
  https://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html
- 与 Cisco Unified IP 电话 相关的文档，请参阅以下 URL：
  https://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

- 有关设计和排查 IP 电话网络的信息，请参阅《Cisco IP 电话解决方案参考网络设计指南》，网址：*https://www.cisco.com/go/srnd*



第 37 章

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 *94:* 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** .gzo 文件不再是一个压缩文件，而是一个文本文件。 因此，.gzo 文件无需解压缩，应作为纯文本进行读取。 **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，第 264 页

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。 触发此警报时，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和端口信息以发送电子邮件警报。
c) （可选）选中**启用 TLS 模式**复选框，以便启用到 SMTP 服务器的加密通信通道。
d) （可选）选中**启用身份验证模式**复选框以要求对收件人的电子邮件地址进行身份验证。

注释 只有选中了**启用身份验证模式**复选框才能访问**用户名**和**密码**字段。

e) 在**用户名**字段中输入用户名。
f) 在**密码**字段中输入密码。
g) 输入**发送用户 Id**。
h) 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 448 页
数据包捕获的配置核对表， 第 448 页
将最终用户添加到标准数据包嗅探器访问控制组 ， 第 449 页
配置数据包捕获服务参数， 第 449 页
在电话配置窗口中配置数据包捕获， 第 450 页
在网关和干线配置窗口中配置数据包捕获， 第 451 页
数据包捕获配置设置， 第 452 页
分析捕获的数据包， 第 453 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 449 页
分析捕获的数据包，第 453 页

在网关和干线配置窗口中配置数据包捕获，第 451 页
在电话配置窗口中配置数据包捕获，第 450 页
配置数据包捕获服务参数，第 449 页
数据包捕获配置设置，第 452 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 451 页
在电话配置窗口中配置数据包捕获，第 450 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 453 页
数据包捕获的配置核对表，第 448 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 453 页
数据包捕获的配置核对表 ，第 448 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。 系统每天使用新的加密密钥创建一个新文件。 Unified Communications Manager 将文件存储七天，还将加密文件的密钥存储在一个安全的位置。Unified Communications Manager 将该文件存储在 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。
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 451 页
在电话配置窗口中配置数据包捕获，第 450 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 *95: 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

信息	**Linux** 命令	功能配置 **GUI** 工具	**CLI** 命令
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 *96:* 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 457 页
系统历史记录日志字段，第 458 页
访问系统历史记录日志，第 459 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
  - Boot
  - 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。

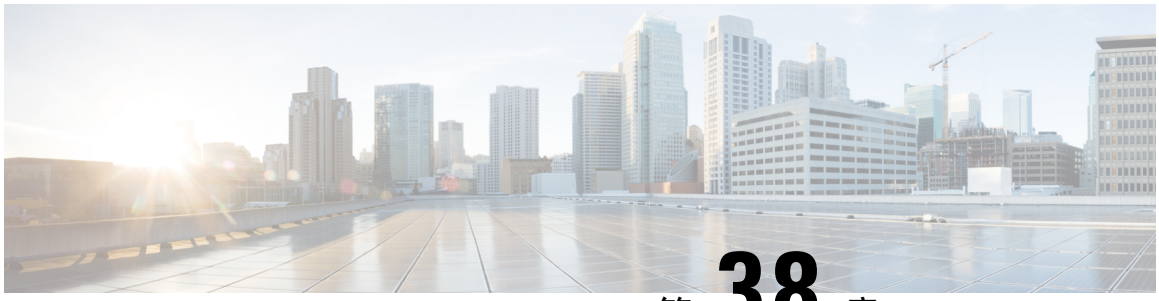
   “激活状态”列在指定的 Cisco CallManager 服务行中显示**已激活**。

   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。



第 38 章

通过 TAC 创建支持案例

本部分包含您与 TAC 联系时需要的信息类型，以及与 TAC 人员分享信息的方式的相关详情。

对于持有有效的 Cisco 服务合同的所有客户、合作伙伴、经销商和分销商，Cisco 技术支持中心将提供每天 24 小时的优质技术支持服务。 Cisco 技术支持网站提供了联机文档和工具，用于排除和解决与 Cisco 产品和技术相关的技术问题。 每年 365 天、每天 24 小时都可以访问以下 URL 的网站：*http://www.cisco.com/techsupport*

使用联机 TAC 服务请求工具是发出 S3 和 S4 服务请求的最为快捷的方法。 （S3 和 S4 服务请求是指网络影响较轻，或为了获取产品信息的情形。） 说明您的情况之后，TAC 服务请求工具会自动提供建议的解决方案。 如果使用推荐的资源后仍未解决问题，您的服务请求将交由 Cisco TAC 工程师处理。 请通过以下 URL 查找 TAC 服务请求工具：*http://www.cisco.com/techsupport/servicerequest*

对于 S1 或 S2 服务请求，或者如果您没不具备 Internet 接入，请通过电话联系 Cisco TAC。 （S1 或 S2 服务请求是指营运网络无法运行或严重受损情形下的请求。） 我们会立即派 Cisco TAC 工程师处理 S1 和 S2 服务请求，以确保您的业务能正常运作。

要通过电话发出服务请求，请使用下面的电话号码：

亚太：+61 2 8446 7411（澳大利亚：1 800 805 227）

欧洲、中东及非洲 (EMEA)：+32 2 704 55 55

美国：1 800 553 2447

要获得 Cisco TAC 联系方式的完整列表，请访问以下 URL：*http://www.cisco.com/techsupport/contacts*

您将需要的信息

当您使用 Cisco TAC 开启案例时，必须提供一些初步信息来更好地确定和限定问题。 根据问题性质的不同，您可能需要提供其他信息。 如果等到开启案例之后应工程师要求才开始收集以下信息，将不可避免地会耽搁解决问题的时间。

相关主题

Cisco Live!，第 471 页
Cisco Secure Telnet，第 472 页
常规信息，第 469 页
网络布局，第 468 页
联机案例，第 470 页
问题说明，第 469 页
Remote Access，第 471 页
必需的初步信息，第 468 页

必需的初步信息

对于所有问题，都必须将以下信息提供给 TAC。 收集并保存这些信息以便在开启 TAC 案例时使用，并定期更新所作的任何更改。

相关主题

常规信息，第 469 页
网络布局，第 468 页
问题说明，第 469 页

网络布局

提供物理和逻辑设置的详细说明，以及语音网络（如果适用）中涉及到的以下网络元素：

- Unified Communications Manager
  - 版本（在 Unified Communications Manager 管理中，选择**详细信息**）
  - Unified Communications Manager 的数目
  - 设置（独立、群集）
    - Unity
  - 版本（在 Unified Communications Manager 管理中）
  - 集成类型
    - 应用程序

- 安装的应用程序列表
- 每个应用程序的版本号
    - IP/语音网关
- 操作系统版本
- 显示技术（IOS 网关）
- Unified Communications Manager 负载（Skinny 网关）
    - 切换
- 操作系统版本
- VLAN 配置
    - 拨号方案—编号方案、呼叫路由

最好能够提交 Visio 或其他详图，例如 JPG。 如果使用白板，您还可以通过 Cisco Live! 会话提供图表。

问题说明

提供出现问题时用户执行的逐步操作详细说明。 确保提供的详细信息包括：

- 预期行为
- 观察到的详细行为

常规信息

确保随时能够获得以下信息：

- 是新安装吗？
- 如果安装的是 Unified Communications Manager 的早期版本，是否从一开始就发生了这个问题？（如果不是，近期对系统做过什么更改？）
- 该问题可重现吗？
    - 如果可重现，是在正常情况还是特殊情况下？
    - 如果不可重现，该问题出现时是否有什么特殊情况？
    - 该问题出现的频率有多高？
- 受影响的设备有哪些？
    - 如果特定设备受到影响（非随机），它们有何共同之处？

- 包含此问题涉及的所有设备的 DN 或 IP 地址（如果为网关）。

- 哪些设备位于 Call-Path 上（如果适用）？

联机案例

通过 Cisco.com 在线创建支持案例是初始方法，优先于所有其他支持案例创建方法。 但高优先级案例（P1 和 P2）例外。

开启案例时，请提供准确的问题说明。 提供问题说明之后，系统会返回可以为您提供即时解决方案的 URL 链接。

如果未找到可解决问题的方案，请继续将您的案例发送给 TAC 工程师。

可维护性连接器

功能配置连接器概述

您可以使用 Webex 功能配置服务轻松收集日志。 该服务会自动执行查找、检索和存储诊断日志及信息的任务。

此功能会使用部署在本地的功能配置连接器。 功能配置连接器在网络中的专用主机（“连接器主机”）上运行。 您可以将连接器安装到以下任一组件：

- 企业计算平台 (ECP)—推荐

  ECP 使用 Docker 容器隔离、保护和管理其服务。 主机和 Serviceability Connector 应用程序从云端安装。 无需手动升级即可确保其为最新且安全。

重要事项 我们建议使用 ECP。 我们未来的发展将集中在这个平台上。 如果您在 Expressway 上安装了功能配置连接器，则部分些新功能将不可用。

- Cisco Expressway

您可以使用功能配置连接器达成以下目的：

- 服务请求的自动日志和系统信息检索
- Cloud-Connected UC 部署中 Unified CM 群集的日志收集

您可以对两种使用案例使用相同的功能配置连接器。

使用功能配置服务的好处

该服务可带来以下好处：

- 加速日志收集。 TAC 工程师在诊断问题时可以检索相关日志。 他们可以避免请求额外日志以及等待手动收集和交付的延迟。 这种自动化可能会将您解决问题所需的时间缩短数天。
- 与 TAC 的协作解决方案分析器及其诊断签名数据库一起使用。 系统会自动分析日志，发现已知问题，并建议已知的修补程序或解决办法。

TAC 对于功能配置连接器的支持

有关功能配置连接器的更多详细信息，请参阅 https://www.cisco.com/go/serviceability 或联系您的 TAC 代表。

Cisco Live!

Cisco Live! 是一种经过加密的安全 Java 小程序，可让您和您的 Cisco TAC 工程师通过使用协作 Web 浏览/ URL 共享、白板、Telnet 和剪贴板工具更有效地协作。

通过以下 URL 访问 Cisco Live!：

`http://c3.cisco.com/`

Remote Access

借助远程访问功能，您可以与所有必要设备建立终端服务（远程端口 3389）、HTTP（远程端口 80）和 Telnet（远程端口 23）会话。

⚠

注意 在设置拨入时，不要使用 **login:cisco** 或 **password:cisco**，因为它们构成了系统的漏洞。

允许 TAC 工程师通过以下方法之一远程访问设备之后，您可以很快解决许多问题：

- 具有公共 IP 地址的设备。
- 拨号访问—按首选项的递减顺序排列：模拟调制解调器、集成服务数字网络 (ISDN) 调制解调器、虚拟专用网 (VPN)。
- 网络地址转换 (NAT)IOS 和专用 Internet 交换 (PIX) 允许访问具有专用 IP 地址的设备。

确保工程师干预期间防火墙不会阻碍 IOS 流量和 PIX 流量，并确保所有必要服务（例如终端服务）在服务器上启动。

注释 TAC 会非常审慎地处理所有访问信息，未经客户同意，不会对系统作任何更改。

Cisco Secure Telnet

Cisco Secure Telnet 为 Cisco 服务工程师 (CSE) 提供对您站点上的 Unified Communications Manager 服务器的透明防火墙访问权限。

Cisco Secure Telnet 可让 Cisco Systems 防火墙内的 Telnet 客户端连接到防火墙后面的 Telnet 守护程序。 此安全连接可让您远程监控和维护 Unified Communications Manager 服务器，无需修改防火墙。

注释 Cisco 只会在您允许的情况下访问您的网络。 您必须提供站点的网络管理员，以帮助启动此过程。

防火墙保护

几乎所有内部网络都使用防火墙应用程序来限制外部对内部主机系统的访问。 这些应用程序通过限制网络与公共 Internet 之间的 IP 连接来保护您的网络。

防火墙会自动阻止从外部发起的 TCP/IP 连接，除非软件重新配置为允许此类访问。

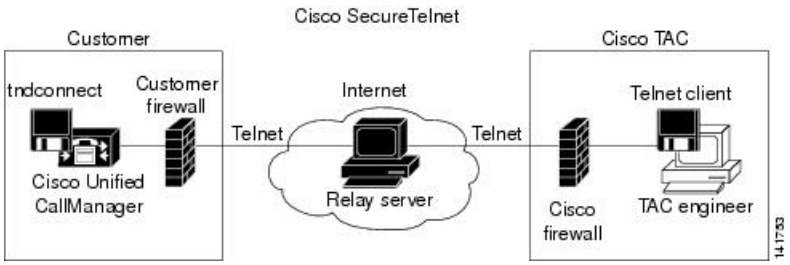
公司网络通常允许与公共 Internet 进行通信，但前提是指向外部主机的连接来自防火墙内部。

Cisco Secure Telnet 设计

Cisco Secure Telnet 利用了一个事实：可以很容易地从防火墙背后启动 Telnet 连接。 使用外部代理计算机时，系统会将 TCP/IP 通信从防火墙背后中继到位于 *Cisco* 技术支持中心 (TAC) 的另一台防火墙背后的主机。

使用此中继服务器可以维护两个防火墙的完整性，同时支持受屏蔽的远程系统之间的安全通信。

图 ***26: Cisco Secure Telnet*** 系统



Cisco Secure Telnet 结构

外部中继服务器通过建立 Telnet 隧道在网络和 Cisco Systems 之间建立连接。 这可让您将 Unified Communications Manager 服务器的 IP 地址和密码标识符传输到 CSE。

注释 密码包含您的管理员和 CSE 共同商定的文本字符串。

您的管理员通过启动 Telnet 隧道启动此过程，该隧道建立从防火墙内部到公共 Internet 上的中继服务器的 TCP 连接。 然后，Telnet 隧道将与本地 Telnet 服务器建立另一个连接，在两个实体之间创建双向链路。

注释 Cisco TAC 的 Telnet 客户端与 Windows NT 和 Windows 2000 上运行的系统或 UNIX 操作系统兼容。

当您站点上的 Cisco Communications Manager 接受密码后，在 Cisco TAC 运行的 Telnet 客户端会连接到在您的防火墙背后运行的 Telnet 后台守护程序。 产生的透明连接允许与本地使用机器相同的访问权限。

Telnet 连接稳定后，CSE 可以实施所有远程功能配置功能，在您的 Unified Communications Manager 服务器上执行维护、排查和故障诊断任务。

您可以查看 CSE 发送的命令和您 Unified Communications Manager 的服务器发布的响应，但命令和响应可能并非始终完全格式化。

设置远程帐户

在 Unified Communications Manager 中配置一个远程帐户，以便 Cisco 支持人员能够暂时访问您的系统进行故障诊断。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**服务** > **远程支持**。

步骤 2 在**帐户名**字段中，输入远程帐户的名称。

步骤 3 在**帐户期限**字段中，输入帐户期限，以天为单位。

步骤 4 单击**保存**。
系统将生成加密的密码短语。

步骤 5 与 Cisco 支持人员联系，向其提供远程支持帐户名和密码短语。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。