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 *1: 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 *2: 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 3: 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 *4: 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 *5: 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。

表格	内容
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。
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 *6: 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。
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 *7: 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 *8: 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**
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 *9: 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。

MIB	服务	窗口
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 *10: 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。

参数名称	默认值	生成的陷阱	配置建议
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 *11: 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 21 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 22 页 • 配置 SNMP 用户， 第 24 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 27 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 28 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 32 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 33 页	配置 CISCO-SYSLOG-MIB 的陷阱设置。
步骤 7	CISCO-CCM-MIB 陷阱参数， 第 33 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 34 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 22 页。

如果要配置 SNMP V3，配置 SNMP 用户 ， 第 24 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 23 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 28 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 *12:* 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 25 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 27 页

SNMP V3 用户配置设置

下表介绍了 SNMP V3 用户配置设置。

表 *13: 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 28 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 22 页
- 对于 SNMP V3，请参阅配置 SNMP 用户，第 24 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 29 页
- SNMP V3 的通知目标设置，第 30 页

下一步做什么

配置 MIB2 系统组，第 32 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 14: 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 *15: 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 32 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 *16: 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 <社区字符串>-v2c <发射器 ip 地址> 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 <发射器 ip 地址> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <值>
```

  输入 <值> 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 <社区字符串> -v2c <发射器 ip 地址> 1.3.6.1.4.1.9.9.156.1.9.2 .0 i <值
>
```

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 <社区字符串> -v2c <发射器 ip 地址> 1.3.6.1.4.1.9.9.156.1.9.4.0 i <值>
```

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**警报** > **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 33 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 20 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 35 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 35 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 *17:* 生成 *SNMP* 陷阱

SNMP 陷阱	处理
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	处理
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	处理
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 <社区字符串> -v 2c <发射器 ip 地址> 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 <社区字符串> -v 2c <发射器 ip 地址> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <值>

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。