IM and Presence Service 15 版的配置和管理

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 1

新增和变更内容 1

第 I 部分： 规划系统 3

第 2 章 规划系统 5

IM and Presence Service 概述 5

IM and Presence Service 组件 6

规划概述 8

规划部署 8

IM and Presence Service 部署规模估算 9

功能部署选项 10

标准部署与集中式群集 12

多节点可扩展性功能 12

多节点可扩展性要求 12

OVA 要求 12

部署的可扩展性选项 13

WAN 部署 14

WAN 群集内部署 15

WAN 部署的多节点配置 15

WAN 群集间部署 15

SAML 单点登录部署 16

第三方集成 16

第三方客户端集成 17

第 II 部分： 配置系统 19

第 3 章 配置域 21

配置域概述 21

域配置示例 21

配置域前提条件 24

配置域任务流程 24

禁用高可用性 25

禁用 IM and Presence Service 25

配置 IM and Presence Service 上的默认域 26

添加或更新 IM 地址域 27

删除 IM 地址域 28

重新生成 XMPP 客户端和 TLS 证书 29

启动 IM and Presence 服务 29

启用 Presence 冗余组的高可用性 30

第 4 章 配置 IPv6 33

配置 IPv6 概述 33

配置 IPv6 任务流程 34

在 IM and Presence Service 的 Eth0 上启用 IPv6 34

启用 IPv6 企业参数 35

重新启动服务 35

将 IPv6 地址分配到 IM and Presence 节点 36

在 IM and Presence Service 的 Eth0 上禁用 IPv6 36

第 5 章 配置 IM 寻址方案 39

IM 寻址方案概述 39

使用 User@Default_Domain 的 IM 地址 39

使用目录 URI 的 IM 地址 40

多个 IM 域 40

IM 寻址方案前提条件 40
配置 IM 寻址方案任务流程 41
验证用户设置 41
禁用高可用性 42
停止服务 42
分配 IM 寻址方案 43
IM 地址示例 44
重新启动服务 45
启用高可用性 45
为目录 URI 分配 LDAP 源 46
手动分配目录 URI 47

第 6 章 配置冗余和高可用性 49
Presence 冗余组概述 49
高可用性 50
Presence 冗余组前提条件 50
Presence 冗余组任务流程 50
验证数据库复制 51
验证服务 51
配置 Presence 冗余组 52
配置故障转移的心跳间隔 53
启用高可用性 54
配置用户分配模式 55
启动手动故障转移、回退或恢复 55
节点状态定义 56
节点状态、原因和建议的操作 57
IM and Presence 故障转移增强，停机时间几乎为零 61
冗余相互作用和限制 63

第 7 章 配置用户设置 65
最终用户设置概述 65

服务配置文件 65
功能组模板概述 66
用户设置前提条件 66
配置用户设置任务流程 66
配置用户分配模式 67
添加 IM and Presence UC 服务 67
配置服务配置文件 68
配置功能组模板 69

第 8 章
配置 LDAP 目录 71
LDAP 同步概述 71
最终用户的 LDAP 验证 72
目录服务器用户搜索思科移动和远程访问客户端及终端 72
LDAP 同步前提条件 72
LDAP 同步配置任务流程 73
激活 Cisco DirSync 服务 74
启用 LDAP 目录同步 74
创建 LDAP 过滤器 74
配置 LDAP 目录同步 75
配置企业目录用户搜索 77
目录服务器 UDS 搜索的 LDAP 属性 78
配置 LDAP 验证 79
自定义 LDAP 协议服务参数 79
LDAP 目录服务参数 80
将 LDAP 同步的用户转换为本地用户 81
将 LDAP 同步用户分配给访问控制组 81
集成 LDAP 目录以在 XMPP 客户端上搜索联系人 82
LDAP 帐户锁定问题 82
为 XMPP 客户端配置 LDAP 服务器名称和地址 83
为 XMPP 客户端配置 LDAP 搜索设置 84
打开 Cisco XCP 目录服务 86

第 9 章 为 IM and Presence Service 配置 Cisco Unified Communications Manager 87
集成概述 87
Cisco Unified Communications Manager 集成前提条件 87
Cisco Unified Communications Manager 上的 SIP 干线配置 88
配置 SIP 干线安全性配置文件 89
为 IM and Presence Service 配置 SIP 干线 90
配置 SRV 群集名称 91
配置 SIP PUBLISH 干线 92
配置 Presence 网关 92
验证 Cisco Unified Communications Manager 上的服务 93
配置群集外 Cisco Unified Communications Manager 的电话在线状态 93
将 Cisco Unified Communications Manager 添加为 TLS 对等节点 94
为 Unified Communications Manager 配置 TLS 环境 94

第 10 章 配置集中式部署 97
集中式部署概述 97
集中式群集部署架构 99
集中式群集使用案例 100
集中式部署前提条件 101
集中式部署配置任务流程 102
通过功能组模板启用 IM and Presence 104
在 IM and Presence 中央群集上完成 LDAP 同步 105
通过批量管理为 IM and Presence 启用用户 105
添加远程电话群集 106
配置 IM and Presence UC 服务 107
为 IM and Presence 创建服务配置文件 108
在电话群集中禁用 Presence 用户 108
配置 OAuth 刷新登录 109
配置 ILS 网络 110
为 ILS 配置群集 ID 111

启用电话群集上的 ILS 111
验证 ILS 网络正在运行 112
移动和远程访问配置 112
通过 IM and Presence 集中式部署进行升级需要重新同步 114
IM and Presence 集中式群集设置以及为子域启用了 SSO 的远程电话群集 114
将电话在线状态集成到集中式部署中 115
集中式部署相互作用和限制 116

第 11 章 配置高级路由 117
高级路由概述 117
高级路由前提条件 118
高级路由配置任务流程 118
配置路由通信方法 119
重新启动 Cisco XCP 路由器 120
配置安全的路由器到路由器通信 120
配置群集 ID 121
配置在线状态更新的限流速率 121
配置静态路由 122
配置 SIP 代理服务器设置 122
在 IM and Presence Service 上配置路由嵌入模板 123
在 IM and Presence Service 上配置静态路由 124

第 12 章 配置证书 127
证书概述 127
证书前提条件 129
与 Cisco Unified Communications Manager 交换证书 129
将 Cisco Unified Communications Manager 证书导入到 IM and Presence Service 130
从 IM and Presence Service 下载证书 131
将 IM and Presence 证书导入 Cisco Unified Communications Manager 131
在 IM and Presence Service 上安装证书颁发机构 (CA) 根证书链 132
上传 CA 根证书链 132

重新启动思科群集间同步代理服务 133
验证 CA 证书已同步到其他群集 133
将证书上传到 IM and Presence Service 134
上传证书 135
重新启动 Cisco Tomcat 服务 136
验证群集间同步 136
在所有节点上重新启动 Cisco XCP 路由器服务 137
重新启动 Cisco XCP XMPP 联合连接管理器服务 137
在 XMPP 联合安全证书中启用通配符 137
生成 CSR 138
证书签名请求密钥使用情况扩展 139
生成自签名证书 140
从 IM and Presence Service 删除自签名信任证书 140
从 Cisco Unified Communications Manager 删除自签 Tomcat 信任证书 141
证书监控任务流程 142
配置证书监控通知 142
配置通过 OCSP 吊销证书 143

第 13 章 配置安全设置 145
安全概述 145
安全性设置配置任务流程 145
创建登录提示 146
配置安全 XMPP 连接 146
IM and Presence Service 上的 SIP 安全性设置配置 147
配置 TLS 对等主题 147
配置 TLS 上下文 148
FIPS 模式 148

第 14 章 配置群集间对等 151
群集间对等概述 151
群集间对等前提条件 151

群集间对等配置任务流程 152
检查用户设置 152
启用 Cisco AXL Web 服务 153
启用同步代理 153
配置群集间对等 154
重新启动 XCP 路由器服务 155
验证群集间同步代理是否已打开 156
验证群集间对等状态 156
更新群集间同步代理 Tomcat 信任证书 157
为群集间对等周期性同步失败启用自动恢复 158
配置群集间对等同步时间间隔 158
对群集间对等定期同步禁用证书同步 159
删除群集间对等连接 159
群集间对等相互作用和限制 160

第 15 章 配置推送通知 161
推送通知概述 161
推送通知配置 165

第 III 部分： 配置功能 167

第 16 章 配置可用性和即时消息 169
可用性和即时消息概述 169
可用性和即时消息前提条件 170
可用性和即时消息任务流程 170
配置 Presence 共享 171
配置临时 Presence 订阅 172
启用即时消息 172
可用性和即时消息相互作用及限制 173

第 17 章 配置临时和永久聊天 175

小组聊天室概述 175
群聊前提条件 176
群聊和永久聊天任务流程 176
配置群聊系统管理员 177
配置聊天室设置 178
重新启动 Cisco XCP 文字会议管理器 179
为永久聊天设置外部数据库 179
添加外部数据库连接 180
用于永久聊天的 MSSQL 数据库的 Windows 验证 180
群聊和永久聊天相互作用和限制 181
永久聊天示例（无高可用性） 183
IM and Presence 中的永久聊天边界 184

第 18 章 配置永久聊天的高可用性 189
永久聊天的高可用性概述 189
永久聊天的高可用性 - 群集间示例 189
永久聊天（无高可用性）与永久聊天高可用性要求对比 190
永久聊天的高可用性前提条件 191
永久聊天的高可用性任务流程 192
设置外部数据库 192
添加外部数据库连接 192
验证永久聊天高可用性设置 193
启动 Cisco XCP 文字会议管理器服务 194
合并外部数据库 194
永久聊天的高可用性使用案例 196
永久聊天高可用性故障转移使用案例 197
高可用性永久聊天回退使用案例 198

第 19 章 配置托管文件传输 199
托管文件传输概述 199
托管文件传输呼叫流程 200

托管文件传输前提条件 200
外部数据库前提条件 201
外部文件服务器要求 201
外部文件服务器要求 203
外部文件服务器的分区建议 205
外部文件服务器用户验证 205
外部文件服务器目录结构 206
托管文件传输任务流程 206
添加外部数据库连接 207
设置外部文件服务器 208
为外部文件服务器创建用户 209
设置外部文件服务器目录 210
获取外部文件服务器公钥 211
在 IM and Presence Service 上设置外部文件服务器 212
外部文件服务器字段 213
验证 Cisco XCP 文件传输管理器激活 214
启用托管文件传输 215
文件传输选项 216
验证外部服务器状态 216
排查外部文件服务器公钥和私钥 217
管理托管文件传输 218

第 20 章 配置多设备消息传送 219
多设备消息传送概述 219
多设备消息传送前提条件 219
配置多设备消息传送 220
多设备消息传送流程使用案例 220
多设备消息传送静默模式使用案例 221
多设备消息传送相互作用和限制 222
多设备消息传送计数器 222
设备容量监控 223

用于设备容量监控的用户会话报告 224

第 21 章 配置企业组 227

企业组概览 227

企业组前提条件 228

企业组配置任务流程 229

从 LDAP 目录验证组同步 229

启用企业组 230

更新 OpenLDAP 配置文件 230

启用安全组 230

创建安全组过滤器 231

从 LDAP 目录同步安全组 231

为安全组配置 Cisco Jabber 232

查看用户组 233

企业组部署模型 (Active Directory) 233

企业组限制 236

第 22 章 品牌定制 239

品牌概述 239

品牌前提条件 239

启用品牌 239

禁用品牌 240

品牌文件要求 241

第 23 章 配置高级功能 245

流管理 245

配置流管理 245

与 Microsoft Outlook 集成日历 246

联合 247

消息存档程序 247

第 IV 部分： 管理系统 249

第 24 章 管理聊天 251

管理聊天概述 251

聊天节点别名概述 251

管理聊天前提条件 252

管理聊天任务流程 252

允许聊天室所有者编辑聊天室设置 253

允许客户端记录即时消息历史记录 254

将永久聊天室创建限制在主群集 254

查看外部数据库文字会议报告 255

转移永久聊天室的所有权 256

永久聊天别名报告 257

配置聊天室设置 257

设置聊天室数量 257

配置聊天室成员设置 257

配置可用性设置 259

配置占用设置 260

配置聊天消息设置 260

配置被主持的房间设置 261

配置历史记录设置 261

将聊天室重置为系统默认值 262

聊天节点别名管理 262

管理聊天节点别名 262

分配模式以管理聊天别名 263

手动添加聊天节点别名 263

为永久聊天清理外部数据库 265

管理聊天相互作用 265

第 25 章 托管文件传输管理 267

托管文件传输管理概述 267
托管文件传输管理前提条件 268
托管文件传输管理任务流程 268
AFT_LOG 表示例查询和输出 268
外部数据库磁盘使用情况 269
设置服务参数阈值 270
配置 XCP 文件传输警报 271
托管文件传输警报和计数器 271
为托管文件传输清理外部数据库 273

第 26 章 管理最终用户 275
管理最终用户概述 275
在线状态授权概述 275
验证用户 ID 和目录 URI 276
管理最终用户任务流程 277
分配在线状态授权策略 277
针对用户数据配置数据监控器检查 278
设置用户 ID 和目录 URI 验证检查计划 278
针对电子邮件警报设置电子邮件服务器 279
启用电子邮件警告 279
通过系统故障诊断程序验证用户数据 280
通过 CLI 验证用户 ID 和目录 URI 281
用户 ID 和目录 URI CLI 验证示例 281
用户 ID 和目录 URI 错误 282
查看用户的在线状态设置 284
在线状态授权相互作用和限制 286

第 27 章 将用户迁移到集中式部署 287
集中式部署用户迁移概述 287
中央群集迁移的前提条件任务 287
迁移到中央群集任务流程 288

从迁移群集导出联系人列表 290
在迁移群集中禁用高可用性 291
为 IM and Presence 配置 UC 服务 292
为 IM and Presence 创建服务配置文件 292
在电话群集中禁用 Presence 用户 293
为中央群集启用 OAuth 验证 294
在集中式群集中禁用高可用性 294
删除中央和迁移群集的对等关系 295
阻止思科群集间同步代理 295
通过功能组模板启用 IM and Presence 296
在集中式群集上完成 LDAP 同步 296
通过批量管理为 IM and Presence 启用用户 297
将联系人列表导入集中式群集 298
启动思科群集间同步代理 299
在中央群集中启用高可用性 299
删除迁移群集的剩余对等 300

第 28 章 迁移用户 301
迁移用户概述 301
迁移用户前提条件 301
迁移用户任务流程 301
删除过期的条目 302
为迁移配置标准 Presence 303
群集间同步错误检查 304
为迁移启动基本服务 304
导出用户联系人列表 305
通过 LDAP 迁移用户 305
更新外部 LDAP 目录 306
在新群集中配置 LDAP 307
手动将用户移到新群集 307
手动为用户禁用 IM and Presence 308

手动导入用户 308
在新群集上为 IM and Presence Service 启用用户 309
通过批量管理迁移用户 309
将用户导出到 CSV 文件 310
下载 CSV 导出文件 311
将 CSV 导出文件上传到新群集 311
配置用户模板 311
将用户导入新群集 312
通过批量管理验证迁移用户 312
在主群集上导入联系人列表 313
在旧群集中更新用户 314

第 29 章 管理区域设置 315
管理区域设置概述 315
用户区域设置 315
网络区域设置 316
管理区域设置前提条件 316
在 IM and Presence Service 上安装区域设置安装程序 316
错误消息区域设置参考 317
本地化应用程序 320

第 30 章 管理服务器 321
管理服务器概述 321
更改服务器地址 321
从群集中删除 IM and Presence 节点 322
将已删除的服务器重新添加到群集 322
安装前将节点添加到群集 323
查看 Presence 服务器状态 324
通过高可用性重新启动服务 324
主机名配置 325

第 31 章 备份系统 327
备份概述 327
备份前提条件 329
备份任务流程 330
配置备份设备 330
估算备份文件的大小 331
配置计划的备份 332
开始手动备份 333
查看当前备份状态 334
查看备份历史记录 334
备份相互作用和限制 335
备份限制 335
用于远程备份的 SFTP 服务器 335

第 32 章 恢复系统 339
恢复概述 339
Master Agent 339
Local Agent 339
恢复前提条件 340
恢复任务流程 341
仅恢复第一个节点 341
恢复后续群集节点 343
发布方重建后在一个步骤中恢复群集 344
恢复整个群集 345
将节点或群集恢复到上次已知的良好配置 347
重新启动节点 347
检查恢复作业状态 348
查看恢复历史记录 349
数据验证 349
跟踪文件 349

命令行界面 349
警报和消息 351
警报和消息 351
恢复相互作用和限制 353
恢复限制 353
故障诊断 354
DRS 恢复到较小的虚拟机失败 354

第 33 章 联系人列表的批量管理 355
批量管理概述 355
批量管理前提条件 355
批量管理任务流程 356
批量重命名用户联系人 ID 356
批量重命名用户联系人 ID 文件详细信息 357
批量导出用户联系人列表和非 Presence 联系人列表 358
批量导出用户位置详细信息 358
导出联系人列表文件详细信息 359
导出非 Presence 联系人列表文件详细信息 360
导出用户位置详细信息的文件详细信息 360
批量导入用户联系人列表 361
验证最大联系人列表大小 361
上传输入文件 362
新建批量管理作业 366
检查批量管理作业的结果 367

第 34 章 排查系统 369
故障诊断概述 369
运行系统故障诊断程序 369
运行诊断 370
诊断工具概述 371
使用跟踪日志进行故障诊断 371

通过跟踪发现的常见 IM and Presence 问题 372
通过 CLI 的常见跟踪 374
通过 CLI 运行跟踪 378
通过 RTMT 的常见跟踪 378
用户 ID 和目录 URI 错误故障诊断 379
收到重复的用户 ID 错误 379
收到重复或无效目录 URI 错误 380

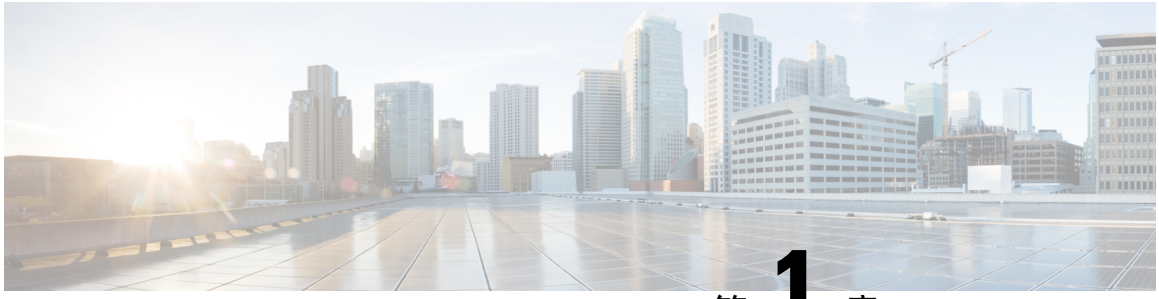
第 V 部分： 参考信息 383

第 35 章 **Cisco Unified Communications Manager TCP 和 UDP 端口使用情况** 385
Cisco Unified Communications Manager TCP 和 UDP 端口使用情况概述 385
端口说明 387
Cisco Unified Communications Manager 服务器之间的群集内端口 387
公共服务端口 390
Cisco Unified Communications Manager 与 LDAP 目录之间的端口 393
从 CCMAdmin 或 CCMUser 到 Cisco Unified Communications Manager 的 Web 请求 393
从 Cisco Unified Communications Manager 到电话的 Web 请求 394
电话和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信 394
网关和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信 396
应用程序和 Cisco Unified Communications Manager 之间的通信 398
CTL 客户端和防火墙之间的通信 399
思科智能许可服务和思科智能软件管理器之间的通信 400
HP 服务器上的特殊端口 400
端口参考 400
防火墙应用程序检测指南 400
IETF TCP/UDP 端口分配列表 401
IP 电话配置和端口利用指南 401
VMware 端口分配列表 401

第 36 章 **IM and Presence Service 的端口使用信息** 403

IM and Presence Service 端口使用概述 403
表中列出的信息 403
IM and Presence Service 端口列表 404

第 37 章 其它要求 419
高可用性登录配置文件 419
有关高可用性登录配置文件的重要说明 419
使用高可用性登录配置文件表 420
高可用性登录配置示例 420
单群集配置 421
500 位用户的完全 UC (1vCPU 700MHz 2GB) 主用/主用配置文件 421
500 位用户的完全 UC (1vCPU 700MHz 2GB) 主用/备用配置文件 421
1000 位用户的完全 UC (1vCPU 1500MHz 2GB) 主用/主用配置文件 422
1000 位用户的完全 UC (1vCPU 1500MHz 2GB) 主用/备用配置文件 422
2000 位用户的完全 UC (1vCPU 1500Mhz 4GB) 主用/主用配置文件 422
2000 位用户的完全 UC (1vCPU 1500Mhz 4GB) 主用/备用配置文件 423
5000 位用户的完全 UC (4 GB 2vCPU) 主用/主用配置文件 423
5000 位用户的完全 UC (4 GB 2vCPU) 主用/备用配置文件 424
15000 位用户的完全 UC (4 vCPU 8GB) 主用/主用配置文件 424
15000 位用户的完全 UC (4 vCPU 8GB) 主用/备用配置文件 425
25000 位用户的完全 UC (6 vCPU 16GB) 主用/主用配置文件 426
25000 位用户的完全 UC (6 vCPU 16GB) 主用/备用配置文件 427
XMPP 标准合规性 428
配置更改和服务重新启动通知 429



第 1 章

新增和变更内容

- 新增和变更内容， 第 1 页

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: IM and Presence Service* 中的新增功能和更改的行为

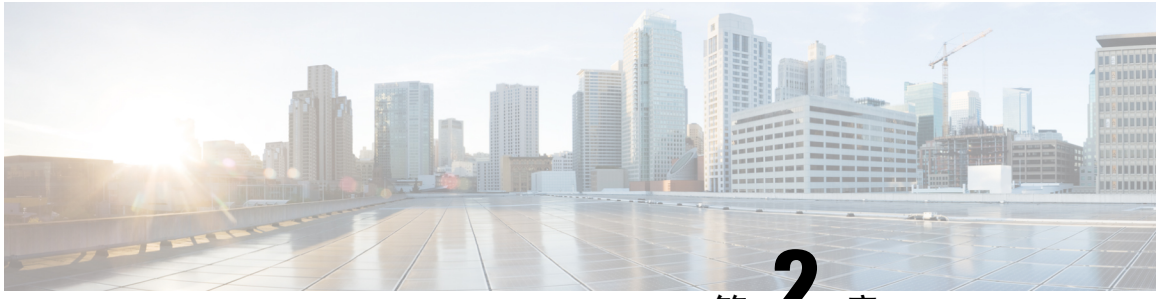
日期	说明	请参阅
2022 年 12 月 18 日	删除 Microsoft 远程呼叫控制功能。	-

新增和变更内容

第 I 部分

规划系统

• 规划系统， 第 5 页



第 2 章

规划系统

- IM and Presence Service 概述， 第 5 页
- 规划概述， 第 8 页
- 规划部署， 第 8 页
- 功能部署选项， 第 10 页
- 标准部署与集中式群集， 第 12 页
- 多节点可扩展性功能， 第 12 页
- WAN 部署， 第 14 页
- SAML 单点登录部署， 第 16 页
- 第三方集成， 第 16 页
- 第三方客户端集成， 第 17 页

IM and Presence Service 概述

IM and Presence Service 管理是一个基于 web 的应用程序，通过它，您可以对 IM and Presence Service 节点进行单独的手动配置更改。本指南中的程序描述了如何使用此应用程序配置功能。

IM and Presence Service 允许在功能丰富的 Cisco Jabber Unified Communications 客户端或任何第三方可兼容 XMPP 的 IM and Presence 客户端之间进行选择。IM and Presence Service 还具备即时消息和文件传输功能，并且能够托管和配置永久群聊聊天室。

在采用了 IM and Presence Service 与 Cisco Unified Communications Manager 的内部部署中，以下服务可用：

- 在线状态
- 即时消息
- 文件传输
- 音频呼叫
- 视频
- 语音邮件

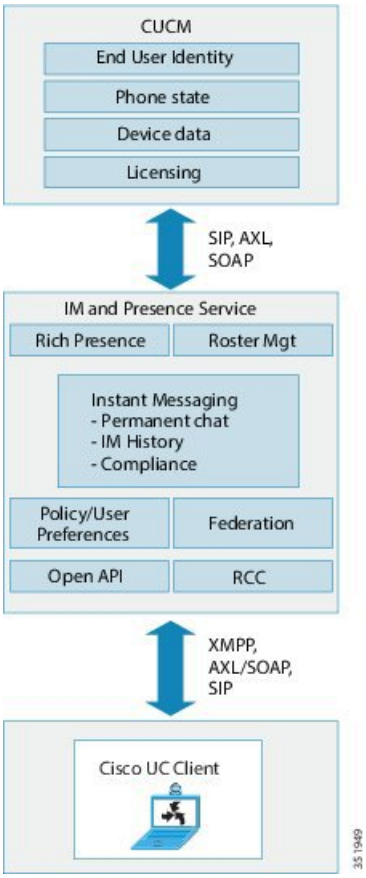
- 会议

有关详细信息，请参阅 Cisco Unified Communications Manager 文档。

IM and Presence Service 组件

下图概述了 IM and Presence Service 部署，包括 Cisco Unified Communications Manager 与 IM and Presence Service 之间的主要组件和接口。

图 *1: IM and Presence Service* 基本部署



SIP 接口

您必须配置以下项来启用 SIP 接口：

- 在 Cisco Unified Communications Manager 中，必须配置指向 IM and Presence Service 的 SIP 干线以进行在线状态信息交换。
- 在 IM and Presence Service 上，将 Cisco Unified Communications Manager 配置为 Presence 网关，以便 IM and Presence Service 可以通过 SIP 干线将 SIP 订阅消息发送至 Cisco Unified Communications Manager。

AXL/SOAP 接口

AXL/SOAP 接口处理来自 Cisco Unified Communications Manager 的数据库同步并填充 IM and Presence Service 数据库。 要激活数据库同步，必须运行思科同步代理网络服务。

默认情况下，同步代理会平衡 IM and Presence Service 群集中所有节点的负载，平均分配所有用户。但是，您也可以选择手动分配用户到群集中的特定节点。

有关执行 Cisco Unified Communications Manager 数据库同步（单节点和双节点 IM and Presence Service）时建议的同步间隔的指导，请参阅 IM and Presence Service SRND 文档。

注释 AXL 接口不支持应用程序开发者交互。

LDAP 接口

Cisco Unified Communications Manager 通过手动配置或直接在 LDAP 上同步来获取所有用户信息。然后，IM and Presence Service 从 Cisco Unified Communications Manager 同步所有此用户信息（使用 AXL/SOAP 接口）。

IM and Presence Service 为 Cisco Jabber 客户端的用户和 IM and Presence Service 用户接口提供 LDAP 身份验证。 如果 Cisco Jabber 用户登录到 IM and Presence Service，并且在 Cisco Unified Communications Manager 上启用了 LDAP 身份验证，IM and Presence Service 将直接访问 LDAP 目录以验证用户。 在验证用户后，IM and Presence Service 会将此信息转发到 Cisco Jabber 以继续用户登录。

XMPP 接口

XMPP 连接可为基于 XMPP 的客户端处理在线状态信息交换和即时消息操作。 IM and Presence Service 针对基于 XMPP 的客户端支持临时会议和永久聊天室。 IM 网关支持 IM and Presence Service 部署中基于 SIP 的客户端与基于 XMPP 的客户端之间的 IM 互操作性。

CTI 接口

CTI（计算机电话集成）接口处理 IM and Presence 节点上用户的所有 CTI 通信，以控制 Cisco Unified Communications Manager 上的电话。 CTI 功能允许 Cisco Jabber 客户端的用户在桌面电话控制模式下运行应用程序。

要为 Cisco Unified Communications Manager 上的 IM and Presence Service 用户配置 CTI 功能，用户必须关联到启用 CTI 的组，并且必须为 CTI 启用分配到该用户的主分机。

要配置 Cisco Jabber 桌面电话控制，必须配置 CTI 服务器和配置文件，并且将任何想在桌面电话模式下使用应用程序的用户分配到该配置文件。 但请注意，所有 CTI 通信都在 Cisco Unified Communications Manager 与 Cisco Jabber 之间直接进行，而不通过 IM and Presence Service 节点。

Cisco IM and Presence 数据监控器服务

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 依赖于 Cisco IM and Presence 数据监控器，因此它们可以延迟启动，直至 IDS 复制处于稳定状态。

Cisco IM and Presence 数据监控器还会从 Cisco Unified Communications Manager 检查思科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 Cisco 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 IM and Presence 数据监控器在 IM and Presence 数据库发布方节点上的行为不同。 它只会将功能服务的启动延迟到超时到期为止。 当超时到期后，即使 IDS 复制未成功建立，它也允许所有功能服务在发布方节点上启动。

当节点上的功能服务延迟启动时，Cisco IM and Presence 数据监控器会生成警报。 在该节点上成功建立 IDS 复制后，它又会生成通知。

Cisco IM and Presence 数据监控器会影响全新多节点安装，也可影响软件升级程序。 仅当发布方节点和订阅方节点运行相同的 IM and Presence 版本并且 IDS 复制已在订阅方节点上成功建立时，这两种程序才会完成。

要检查节点上的 IDS 复制状态，请采用以下方式之一：

- 使用此 CLI 命令：`utils dbreplication runtimestate`
- 使用 Cisco Unified IM and Presence 报告工具。 “IM and Presence 数据库状态”报告显示群集的详细状态。

要检查思科同步代理的状态，请导航到 Cisco Unified CM IM and Presence 管理界面并选择“诊断”>“系统控制板”。 您会找到 Cisco Unified Communications Manager 发布方节点 IP 地址以及同步状态。

规划概述

配置系统之前，请确保规划好系统的部署方式。IM and Presence Service 提供多种部署选项，旨在满足不同公司的需求。

有关如何设计包含满足您需求的 IM and Presence Service 部署的思科协作系统的详细信息，请参阅《思科协作系统解决方案参考网络设计》，网址：http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html。

规划部署

配置系统之前，请确保规划好您的群集拓扑以及系统的部署方式。

过程

	命令或操作	目的
步骤 1	估算协作部署的规模	有关信息，请参阅《思科协作系统解决方案参考网络设计》的“协作解决方案规模估算指南”一章，网址：http://%20www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html。
步骤 2	确定要部署的功能。	有关详细信息，请参阅功能部署选项，第 10 页。
步骤 3	确定要安装标准部署还是 IM and Presence 中央群集部署	确定要在与电话相同的群集上部署 IM and Presence Service，还是要为 IM and Presence 部署集中式群集。 有关详细信息，请参阅标准部署与集中式群集。
步骤 4	规划好想要部署多少群集节点。	通过 IM and Presence 多节点可扩展性功能，您可以根据需求估算部署规模。 有关详细信息，请参阅多节点可扩展性要求，第 12 页。
步骤 5	规划好您将如何添加冗余。	部署的可扩展性选项，第 13 页
步骤 6	规划好您的地理位置	您可以安装在一个站点，以便从一个位置维护硬件。 不过，您还可以通过 WAN 部署群集，以通过部署多个站点来添加地区冗余。 有关详细信息，请参阅： • WAN 群集内部署，第 15 页 • WAN 群集间部署，第 15 页
步骤 7	确定是否要配置 SAML 单点登录。	有关详细信息，请参阅SAML 单点登录部署，第 16 页。
步骤 8	确定是否要与第三方应用程序集成。	这包括 Microsoft Outlook 日历集成以及与第三方系统结合。 有关详细信息，请参阅第三方集成，第 16 页。

IM and Presence Service 部署规模估算

有关如何估算协作部署规模的信息，请参阅《思科协作系统解决方案参考网络设计》的“协作解决方案规模估算指南”一章，网址：http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html。

功能部署选项

基本 IM、可用性和临时群聊是安装 IM and Presence Service 并在基本模式中配置用户后可以使用的核心功能。

您可以添加可选功能来增强基本部署。 下图显示了 IM and Presence Service 的功能部署选项。

下表列出了 IM and Presence Service 的功能部署选项。

表 *2: IM and Presence Service* 功能部署选项

核心 **IM** 和可用性功能	高级 **IM** 功能（可选）	丰富的 **Unified Communications** 可用性功能（可选）	远程桌面电话控制（可选）
查看用户可用性 安全地发送和接收富文本 IM 文件传输 临时群聊 管理联系人 用户历史记录 Cisco Jabber 支持 多客户端设备支持：Microsoft Windows、MAC、移动电话、平板设备、IOS、Android、BB Microsoft Office 集成 LDAP 目录集成 个人目录和好友列表 开放 API 系统故障诊断	永久聊天 托管文件传输 消息存档程序 第三方 XMPP 客户端支持日程安排 高可用性 可扩展性：多节点支持和 WAN 群集 群集间对等 企业联合： • IM and Presence Service 集成 • Cisco Webex Messenger 集成 • Microsoft Lync/Skype for Business/Office365 服务器集成 • IBM SameTime 集成 • Cisco Jabber XCP 公共联合： • Google Talk、AOL 集成 • XMMP 服务或 BOT • 第三方 Exchange 服务集成 即时消息合规性 SAML 单点登录 自定义登录提示	思科电话可用性 Microsoft Outlook 日历集成（内部 Exchange 或托管式 Office 365 部署）	远程 Cisco IP Phone 控制 远程软件电话控制

标准部署与集中式群集

在安装系统之前，您必须决定是要部署标准的 IM and Presence Service，还是想要 IM and Presence Service 中央群集，因为这会影响您的拓扑和安装：

- IM and Presence Service 上的 Cisco Unified Communications Manager（标准部署）—在标准部署中，IM and Presence Service 群集安装在与 Cisco Unified Communications Manager 电话节点相同的服务器上。 IM and Presence 群集与电话群集共享一个平台和许多相同服务。 此选项需要将电话群集 1x1 映射到 IM and Presence 群集。
- 集中式 IM and Presence 群集—在此部署中，IM and Presence Service 群集与电话群集分开安装。 根据您对拓扑的规划方式，IM and Presence 中央群集可能位于与电话群集完全不同的硬件服务器上。 此部署选项删除了电话群集与 IM and Presence 群集的 1x1 映射要求，因此您可以根据自己的需要更好地扩展每种部署类型。

注释 IM and Presence 中央群集仍有 Cisco Unified Communications Manager 实例。 但是，该实例用于用户设置和数据库，并且不处理电话。 对于电话集成，IM and Presence 中央群集必须连接到单独的 Cisco Unified Communictions Manager 电话群集。

本文档中的程序对于标准部署和中央群集部署均适用。 不过，对于中央群集部署，您还必须完成配置集中式部署，第 97 页章节中的任务，以正确调整您的电话群集和 IM and Presence 群集，使之保持一致。

多节点可扩展性功能

多节点可扩展性要求

IM and Presence Service 支持多节点可扩展性：

- 每群集六个节点
- 每群集 75,000 位用户，完整 Unified Communication (UC) 模式部署中每节点最多 25,000 位用户
- Presence 冗余组中 25,000 位用户，高可用性部署中每群集 75,000 位用户。
- 关于每用户最大联系人数（默认为无限）的可管理用户定义限制
- IM and Presence Service 继续通过多节点功能支持群集间部署。

OVA 要求

以下 OVA 要求适用：

- 对于群集间部署，必须部署至少包含 15000 位用户的 OVA。只要所有群集运行的用户 OVA 至少为 15000 位用户，就可以让不同的群集运行不同大小的 OVA。
- 对于永久聊天部署，我们建议您部署至少包含 15000 位用户的 OVA。
- 对于集中式部署，我们建议使用最少 15000 位用户的 OVA 的 25000 位用户 IM and Presence OVA。15000 位用户的 OVA 可以增长到 25000 位用户。借助 25K OVA 模板和启用高可用性的六节点群集，IM and Presence Service 中央部署最多可支持 75,000 个客户端。要通过 25K OVA 支持 75K 位用户，需要将 XCP 路由器的默认跟踪级别从**信息**改为**错误**。对于中央群集中的 Unified Communications Manager 发布方节点，以下要求适用：
  - 25,000 IM and Presence OVA（最多 75000 位用户）可以使用安装在中央群集的 Unified Communications Manager 发布方节点上的 10000 用户 OVA 进行部署
  - 15,000 IM and Presence OVA（最多 45000 位用户）可以使用安装在中央群集的 Unified Communications Manager 发布方节点上的 7500 用户 OVA 进行部署

注释 如果计划启用多设备消息传送，请根据客户端数量而不是用户数量来衡量部署，因为每个用户可能有多个 Jabber 客户端。例如，如果您有 25000 位用户，每位用户有两个 Jabber 客户端，则您的部署需要 50000 位用户的容量。

可扩展性取决于部署中的群集数。有关详细的 VM 配置要求和 OVA 模板，请参阅以下 URL 的 *Unified CM IM and Presence* 的虚拟化：https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html。

部署的可扩展性选项

IM and Presence Service 群集支持最多六个节点。 如果原来安装的节点不到六个，则可以随时安装额外节点。 如要扩展 IM and Presence Service 部署来支持更多用户，必须考虑已配置的多节点部署模型。 下表介绍每种多节点部署模型的可扩展性选项。

表 3:

部署模式	可扩展性选项	
	向现有 **Presence** 冗余组添加新节点	向新 **Presence** 冗余组添加新节点
平衡非冗余高可用性部署	如果向现有 Presence 冗余组添加新节点，则新节点可以支持与现有节点相同的用户数；Presence 冗余组现在可支持双倍的用户数。 它还会为该 Presence 冗余组中现有节点和新节点上的用户提供平衡的高可用性。	如果向新 Presence 冗余组添加新节点，则可以在部署中支持更多用户。 这不会为 Presence 冗余组中的用户提供平衡的高可用性。 要提供平衡的高可用性，必须向 Presence 冗余组添加第二个节点。
平衡冗余高可用性部署	如果向现有 Presence 冗余组添加新节点，则新节点可以支持与现有节点相同的用户数。 例如，如果现有节点支持 5000 位用户，则新节点支持相同的 5000 位用户。 它还会为该 Presence 冗余组中现有节点和新节点上的用户提供平衡的冗余高可用性。 **注释** 可能必须在 Presence 冗余组中重新分配用户，具体取决于现有节点上有多少用户。	如果向新 Presence 冗余组添加新节点，则可以在部署中支持更多用户。 这不会为 Presence 冗余组中的用户提供平衡的高可用性。 要提供平衡的高可用性，必须向 Presence 冗余组添加第二个节点。
主用/备用冗余高可用性部署	如果向现有 Presence 冗余组添加新节点，则会为该 Presence 冗余组现有节点中的用户提供高可用性。 这只会提供高可用性增强，而不会增加部署中可支持的用户数。	如果在新 Presence 冗余组中添加新节点，则可以在部署中支持更多用户。 这不会为 Presence 冗余组中的用户提供高可用性。 要提供高可用性，必须向 Presence 冗余组添加第二个节点。

WAN 部署

IM and Presence Service 支持用于群集内和群集间部署的 WAN 群集。 利用此选项，您可以向部署中添加地区冗余。

WAN 群集内部署

使用本模块中提供的带宽建议，IM and Presence Service 可支持 WAN 群集内部署。 IM and Presence Service 通过 WAN 支持地理上分散的单一 Presence 冗余组，其中 Presence 冗余组中的一个节点位于一个地理位置，另一个节点位于另一个地理位置。

此模型可以提供地区冗余和远程故障转移，例如故障转移到远程站点上的备份 IM and Presence Service 节点。 在此模型中，IM and Presence Service 节点无需与 Cisco Unified Communications Manager 数据库发布方节点位于同一位置中。 Cisco Jabber 客户端对 IM and Presence Service 节点可以是本地或远程。

此模型还支持客户端的高可用性，当主 IM and Presence Service 节点上的服务中断或硬件出现故障时，客户端将故障转移到远程对等 IM and Presence Service 节点。 当断开连接的节点重新上线后，客户端将自动重新连接到主 IM and Presence Service 节点。

在部署通过 WAN 进行远程故障转移的 IM and Presence Service 时，请注意以下限制：

- 此模型仅在系统级别支持高可用性。 特定 IM and Presence Service 组件可能仍然具有单一故障点。 这些组件包括思科同步代理、思科群集间同步代理和 Cisco Unified CM IM and Presence 管理接口等。

IM and Presence Service 还支持 WAN 群集部署中的多个 Presence 冗余组。 有关 WAN 群集部署扩展的信息，请参阅 IM and Presence Service SRND。

有关其他信息，请参阅《*IM and Presence Service* 解决方案参考网络设计》(SRND)。

WAN 部署的多节点配置

为 WAN 群集间部署配置 IM and Presence Service 多节点功能时，请按照多节点部分中的介绍配置 IM and Presence Service Presence 冗余组、节点和用户分配，但是要注意以下建议：

- 为获得最佳性能，思科建议您将大部分用户分配到主 IM and Presence Service 节点。 此部署模型可以降低发送到 WAN 上的远程 IM and Presence Service 节点的消息量，但是故障转移到辅助节点的时间取决于故障转移的用户数量。
- 如果您要配置 WAN 上的高可用性部署模型，可以配置 Presence 冗余组范围的 DNS SRV 地址。 在这种情况下，IM and Presence Service 将初始 PUBLISH 请求消息发送到 DNS SRV 指定的节点，响应消息会指示用户的主机节点。 然后，IM and Presence Service 将该用户的所有后续 PUBLISH 消息发送到主机节点。 在配置此高可用性部署模型前，您必须考虑是否有足够的带宽用于可能在 WAN 上发送的潜在消息量。

WAN 群集间部署

使用本模块中提供的带宽建议，IM and Presence Service 可支持 WAN 群集间部署。 在部署群集间部署时，这些注意事项适用：

- 群集间对等 — 您可以配置互连独立 IM and Presence Service 群集的对等关系，称为群集间对等。 此群集间对等功能允许一个 IM and Presence Service 群集中的用户与同一域中远程 IM and Presence

Service 群集的用户进行通信和订阅该用户的可用性信息。 有关如何设置群集间对等的详细信息，请参阅配置群集间对等，第 154 页。

- 节点名称—为任何 IM and Presence Service 节点定义的节点名称必须可被每个群集上的所有其他 IM and Presence Service 节点解析。 因此，每个 IM and Presence Service 节点名称必须是节点的 FQDN。 如果您的网络中未部署 DNS，则每个节点名称都必须是 IP 地址。
- IM 地址方案—对于群集间部署，每个群集中的所有节点都必须使用相同的 IM 地址方案。 如果群集中有任何节点运行 10 版之前的 IM and Presence Service，则所有节点都必须设置为使用 UserID@Default_Domain IM 地址方案以实现向后兼容。
- 路由器到路由器通信—默认情况下，IM and Presence Service 将群集中的所有节点分配为群集间的路由器-路由器连接器。 当 IM and Presence Service 通过 AXL 接口在群集之间建立群集间对等连接时，它会同步主群集和远程群集中所有群集间路由器-路由器连接器节点的信息。

  您还可以配置安全的路由器到路由器通信，这些通信使用 TLS 来保护本地群集中每个路由器到路由器连接器节点与远程群集中每个路由器连接器节点之间的连接。

SAML 单点登录部署

通过安全断言标记语言 (SAML) 单点登录功能，管理用户可以在仅登录一个应用程序后，访问包括 IM and Presence Service 在内的多个思科协作应用程序。此功能通过以下方式简化了管理员的工作：

- 单点登录后，只需一次登录即可访问多个思科协作应用程序。
- 只需一个密码 – 不再需要为每个应用程序记住不同的密码。
- 管理员可以通过单个身份提供程序 (IdP) 管理所有密码和验证。

有关如何设置和配置 SAML 单点登录的详细信息，请参阅《*Cisco Unified Communications* 解决方案的 *SAML SSO* 部署指南》，网址：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

第三方集成

IM and Presence Service 可与多种第三方系统集成。下表概述了集成并提供了介绍如何进行配置的文档链接。

指南标题	本指南包含 ...
为 IM and Presence Service 集成 Microsoft Outlook 日历	将 IM and Presence Service 配置为与内部部署的 Microsoft Exchange 服务器或托管的 Office 365 服务器连接，以便在 IM and Presence 用户的状态中使用 Microsoft Outlook 中的日历信息。

指南标题	本指南包含 ...
IM and Presence Service 域间联合	配置 IM and Presence Service 以完成与以下系统的域间联合。这可让 IM and Presence 用户与其他系统上的用户交换 IM and Presence。 • Microsoft Lync • Microsoft Skype for Business • Microsoft Office 365 • GoogleTalk • AOL • IBM SameTime • Cisco Webex Messenger • 其他 IM and Presence Service 企业
IM and Presence Service 分区式域内联合	配置 IM and Presence Service 以进行与 Microsoft Lync 或 Skype for Business 的分区式域内联合。在将用户迁移到 IM and Presence Service 的过程中，您可以利用此集成来维护网络中的通信。
使用 Microsoft Lync Server 进行 IM and Presence Service 的远程呼叫控制	配置 Cisco Unified Communications Manager 和 IM and Presence Service 与 Microsoft Lync 集成以实现 Microsoft 远程呼叫控制 (RCC)。这种集成使得企业用户可以通过第三方桌面即时消息 (IM) 应用程序 Microsoft Lync 控制其 Cisco Unified IP Phone 或 Cisco IP Communicator 电话。

第三方客户端集成

本部分概述了对第三方客户端集成的一些要求。

支持的第三方 XMPP 客户端

IM and Presence Service 支持基于标准的 XMPP，以便第三方 XMPP 客户端应用程序能够与 IM and Presence Service 集成提供可用性和即时消息 (IM) 服务。第三方 XMPP 客户端必须符合思科软件开发套件 (SDK) 所述的 XMPP 标准。

本模块介绍将 XMPP 客户端与 IM and Presence Service 集成的配置要求。如果将基于 XMPP 的 API (Web) 客户端应用程序与 IM and Presence Service 集成，另请参阅思科开发者门户网站上适用于 IM and Presence Service API 的开发者文档：

http://developer.cisco.com/

许可要求

您必须为 XMPP 客户端应用程序的每位用户分配 IM and Presence Service 功能。User Connect Licensing (UCL) 和 Cisco Unified Workspace Licensing (CUWL) 中均包含 IM and Presence 功能。

有关许可的更多信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》中的“智能软件许可”一章，网址：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。

Cisco Unified Communications Manager 上的 XMPP 客户端集成

集成 XMPP 客户端前，请在 Cisco Unified Communications Manager 上执行以下任务：

- 配置许可要求。
- 配置用户和设备。将设备与每位用户关联，然后将每位用户与线路显示关联。

集成 LDAP 目录以搜索 XMPP 联系人

为了让 XMPP 客户端应用程序的用户从 LDAP 目录搜索和添加联系人，在 IM and Presence Service 上配置 XMPP 客户端的第三方 LDAP 设置。

XMPP 客户端的 DNS 配置

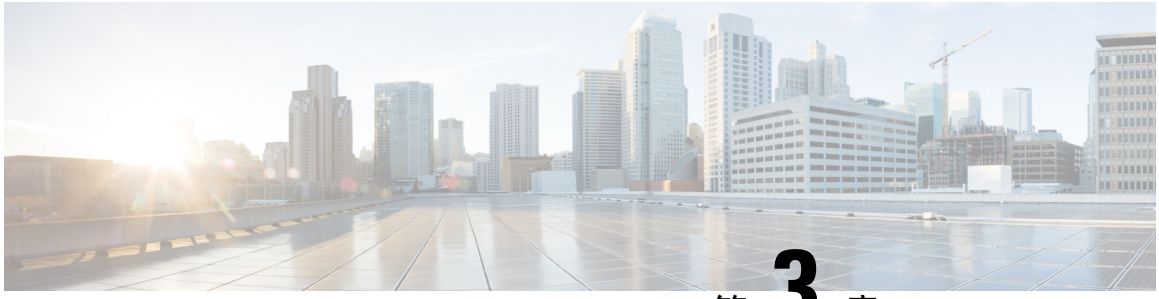
将 XMPP 客户端与 IM and Presence Service 集成时，必须在部署中启用 DNS SRV。XMPP 客户端执行 DNS SRV 查询，查找要与之通信的 XMPP 节点 (IM and Presence Service)，然后执行 XMPP 节点的记录查找以获取 IP 地址。

注释 如果 IM and Presence Service 部署中配置了多个 IM 域，则每个域都需要 DNS SRV 记录。所有 SRV 记录都可解析到同一结果集。

第 II 部分

配置系统

- 配置域， 第 21 页
- 配置 IPv6， 第 33 页
- 配置 IM 寻址方案， 第 39 页
- 配置冗余和高可用性， 第 49 页
- 配置用户设置， 第 65 页
- 配置 LDAP 目录， 第 71 页
- 为 IM and Presence Service 配置 Cisco Unified Communications Manager， 第 87 页
- 配置集中式部署， 第 97 页
- 配置高级路由， 第 117 页
- 配置证书， 第 127 页
- 配置安全设置， 第 145 页
- 配置群集间对等， 第 151 页
- 配置推送通知， 第 161 页



第 3 章

配置域

- 配置域概述， 第 21 页
- 配置域前提条件， 第 24 页
- 配置域任务流程， 第 24 页

配置域概述

IM and Presence 域窗口将显示以下类型的域：

- 管理员管理的 IM 地址域。 这些是您手动添加但尚未分配到任何用户的内部域，或者它们是由同步代理自动添加的，但用户的域已经更改，因此不再使用。
- 系统管理的 IM 地址域。 这些是正被部署中的用户使用的内部域，可以手动或自动添加。

如果域出现在 **IM and Presence 域**窗口中，即表示该域已启用。 您无需启用域。 您可以手动添加、更新和删除本地 IM 地址域。

可以在两个群集中配置一个域，但只能在对等群集中使用。 这在本地群集中显示为系统管理的域，但识别为仅用于对等群集。

思科同步代理服务执行每夜审计，并且检查本地群集和对等群集（如果配置了群集间）上每个用户的目录 URI，同时自动构建唯一域的列表。 当群集中的用户分配到该域时，域将从管理员管理更改为系统管理。 当群集中没有用户使用该域时，域将变回管理员管理。

域配置示例

Cisco Unified Communications Manager IM and Presence Service 支持跨任何数量 DNS 域的灵活节点部署。 要支持此灵活性，部署内的所有 IM and Presence Service 节点必须将节点名称设置为节点的完全限定域名 (FQDN)。 下文描述了 IM and Presence Service 的以下示例节点部署选项。

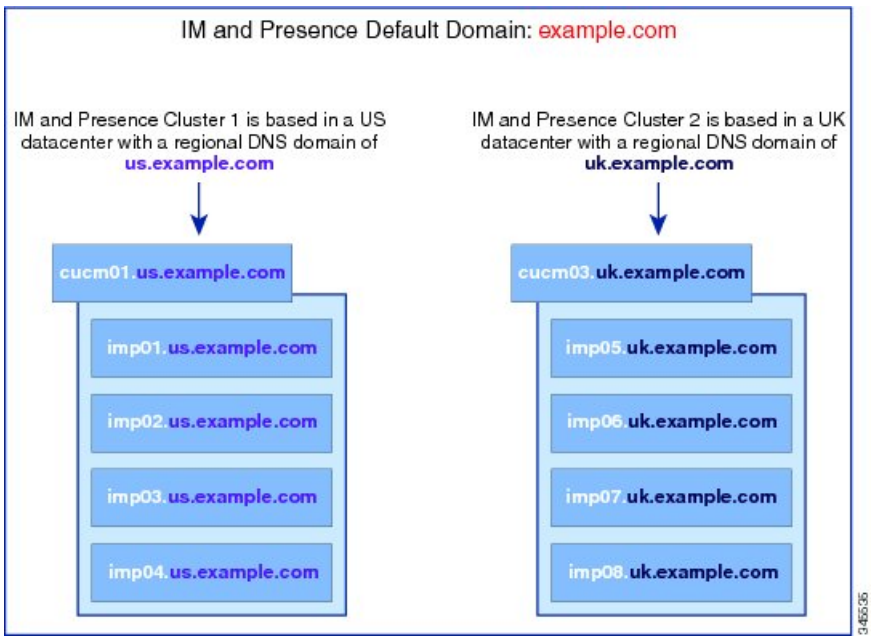
- 多个具有不同 DNS 域和子域的群集
- 单个具有不同 DNS 域或子域的群集
- 单个 DNS 域不同于 Unified Communications Manager 域的群集

注释 如果任何 IM and Presence Service 节点名称仅基于主机名，则所有 IM and Presence Service 节点必须共享同一 DNS 域。

系统不要求 IM and Presence Service 默认域或系统托管的任何其他 IM 域与 DNS 域一致。 IM and Presence Service 部署可以在拥有通用 presence 域的同时，跨多个 DNS 域部署节点

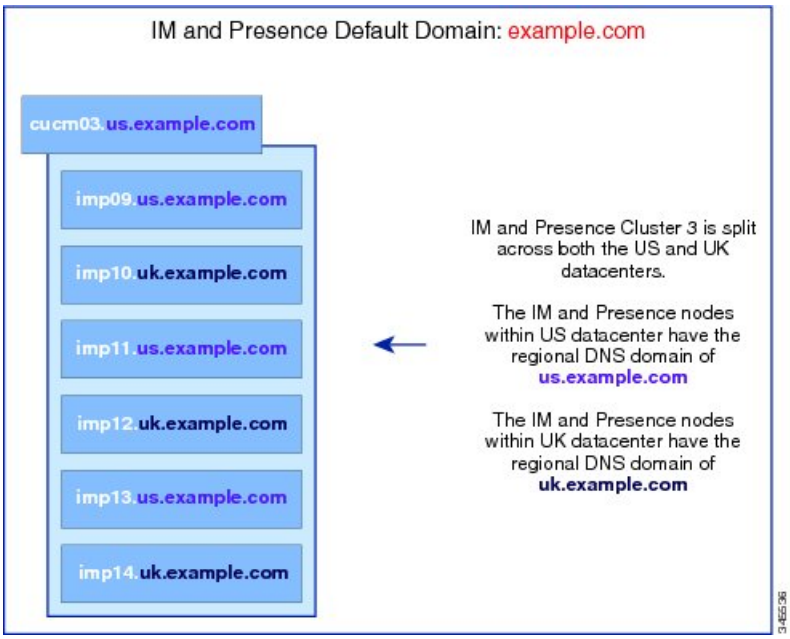
多个具有不同 DNS 域和子域的群集

IM and Presence Service 支持与一个 IM and Presence Service 群集关联的节点，部署在与构成对等 IM and Presence Service 群集之节点不同的 DNS 域或子域中。 下图突出显示了支持的示例部署情景。



单个具有不同 DNS 域或子域的群集

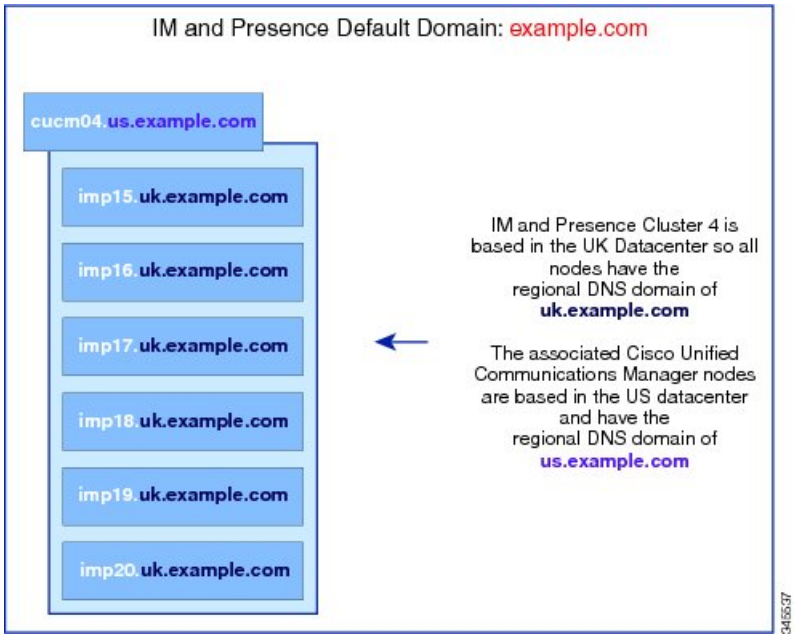
IM and Presence Service 支持在任何 IM and Presence Service 群集内跨多个 DNS 域或子域部署节点。 下图突出显示了支持的示例部署情景。



注释 如果 Presence 冗余组中的两个节点位于不同的 DNS 域或子域中，这种方案也完全支持高可用性。

单个 DNS 域不同于 Unified Communications Manager 域的群集

IM and Presence Service 支持将 IM and Presence Service 节点部署在与其关联 Cisco Unified Communications Manager 群集不同的 DNS 域内。 下图突出显示了支持的示例部署情景。



注释 为支持与 Cisco Unified Communications Manager 的可用性集成，**CUCM Domain** SIP 代理服务参数必须与 Cisco Unified Communications Manager 群集的 DNS 域匹配。

默认情况下，此服务参数设置为 IM and Presence 数据库发布方节点的 DNS 域。 如果 IM and Presence 数据库发布方节点的 DNS 域不同于 Cisco Unified Communications Manager 群集的 DNS 域，您必须使用 Cisco Unified Communications Manager 群集的域来编辑此服务参数。

配置域前提条件

- 所有 IM and Presence Service 以及 Cisco Unified Communications Manager 节点和群集必须支持多个域使用此功能。请确保 IM and Presence Service 群集中的所有节点使用 10.0 或更高版本操作。
- 请确保已配置目录 URI 进行寻址。有关详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》中的“配置 URI 拨号”，网址：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

配置域任务流程

完成以下任务以配置 IM and Presence Service 的域。

过程

	命令或操作	目的
步骤 1	禁用高可用性， 第 25 页	如果已启用高可用性，必须暂时将其禁用。若要更改默认域，必须暂时停止服务；如果在启用高可用性的情况下停止服务，会发生系统故障转移。
步骤 2	禁用 IM and Presence Service， 第 25 页	请先停止关键服务，然后再更改域。
步骤 3	配置 IM and Presence Service 上的默认域 ， 第 26 页	配置 IM and Presence Service 群集的默认域值。 此程序对 DNS 和非 DNS 部署均适用。
步骤 4	请执行以下任意任务： • 添加或更新 IM 地址域， 第 27 页 • 删除 IM 地址域 ， 第 28 页	可选。 仅当您想要在本地群集上添加、编辑或删除管理员管理的域时，完成这些任务。
步骤 5	重新生成 XMPP 客户端和 TLS 证书， 第 29 页	如果您使用的是 TLS XMPP 联合，请继续生成新的 XMPP 客户端和 TLS 证书。

	命令或操作	目的
步骤 6	启动 IM and Presence 服务，第 29 页	完成域配置后，重新启动服务。
步骤 7	启用 Presence 冗余组的高可用性，第 30 页	如已配置高可用性，请再次启用它。 注释　请确保启用高可用性之前，启动的服务在所有群集节点上运行。

禁用高可用性

如已配置高可用性，必须在配置默认域之前在每个 Presence 冗余组中将其禁用。 如果在为默认域更改而停止服务时启用了高可用性，则会发生故障转移。

注释　**Presence 冗余组详细信息**页面将显示所有活动的 JSM 会话，即使群集中禁用了高可用性也不例外。

开始之前

记录每个 Presence 冗余组中每个群集节点的活动用户数。 您可以在 Cisco Unified CM IM and Presence 管理（**系统** > **Presence 拓扑**）窗口中找到此信息。 当您稍后重新启用高可用性时，需要这些数字。

过程

步骤 1 从 Cisco Unified CM 管理用户界面中，选择**系统** > **Presence 冗余组**。

步骤 2 单击**查找**并选择组。

步骤 3 在 Presence 冗余组配置窗口中，取消选中**启用高可用性**复选框。

步骤 4 单击**保存**。

步骤 5 为每个 Presence 冗余组重复执行此步骤。

步骤 6 完成后等待至少两分钟，以便先在群集中同步新的高可用性设置，再做其他进一步更改。

下一步做什么

禁用 IM and Presence Service，第 25 页

禁用 IM and Presence Service

此程序用于在更改默认域之前停止 IM and Presence Service。 在群集中的所有节点上执行此程序。

开始之前

请确保已启用高可用性。 有关详细信息，请参阅禁用高可用性，第 25 页。

过程

步骤 1 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 网络服务**。

步骤 2 从**服务器**列表选择要禁用服务的节点并单击**前往**。

步骤 3 在 **IM and Presence Service** 区域取消选择以下服务：

- **Cisco 客户端配置文件代理**
- **思科同步代理**
- **Cisco XCP 路由器**

步骤 4 单击**停止**。

步骤 5 从**相关链接**下拉列表选择**服务激活**，然后单击**前往**。

步骤 6 在 **IM and Presence Service** 区域取消选择以下服务：

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

步骤 7 单击**保存**。

步骤 8 列出已禁用这些服务的所有节点。 完成对默认域的更改后，您需要重新启动服务。

下一步做什么

为 IM and Presence Service 配置默认域：

- 配置 IM and Presence Service 上的默认域 ，第 26 页

如果已配置默认域，完成以下任务之一来添加、编辑或删除域。

- 添加或更新 IM 地址域，第 27 页
- 删除 IM 地址域 ，第 28 页

配置 IM and Presence Service 上的默认域

此程序用于为 IM and Presence Service 群集配置默认域值。如果您配置了 DNS 或非 DNS 部署，则此过程适用。

此过程仅更改 IM and Presence Service 群集的默认域。它不更改与群集内任何 IM and Presence Service 节点关联的 DNS 域。有关如何更改 IM and Presence Service 节点的 DNS 域的说明，请参阅《更改 *Cisco Unified Communications Manager* 和 *IM and Presence Service* 的 *IP* 地址和主机名》，网址：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

注释 默认域在您向 Cisco Unified Communications Manager 添加 IM and Presence Service 发布方节点时配置。如果系统在节点安装期间无法从 Cisco Unified Communications Manager 检索默认域值，默认域值将重置为 DOMAIN.NOT.SET。此程序用于将 IM and Presence Service 默认域值更改为有效的域值。

开始之前

确保禁用高可用性，并停止基本的 IM and Presence Service。有关详细信息，请参阅：禁用 IM and Presence Service，第 25 页。

过程

步骤 1 登录到 IM and Presence Service 数据库发布方节点。

步骤 2 从 **Cisco Unified CM IM and Presence 管理**选择 **Presence** > **设置** > **高级配置**。

步骤 3 选择**默认域**。

步骤 4 在**域名**字段中，输入新 Presence 域并单击**保存**。

系统更新最多只需 1 小时即可完成。如果更新失败，将显示**重试**按键。单击**重试**以重新应用更改或单击**取消**。

下一步做什么

如果您使用的是 TLS XMPP 联合，请继续重新生成 XMPP 客户端和 TLS 证书，第 29 页。

添加或更新 IM 地址域

您可以在本地群集上添加或编辑管理员管理的域。 不能编辑与其他群集关联的系统管理的域或管理员管理的域。

无法编辑系统管理的域，因为它们正在使用中。 如果系统中再无使用该 IM 地址域的用户（如用户已被删除），则系统管理的域会自动变成管理员管理的域。 您可以编辑或删除管理员管理的域。

开始之前

确保禁用高可用性，并停止基本的 IM and Presence Service。 有关详细信息， 禁用 IM and Presence Service，第 25 页

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中选择 **Presence** > > **域**。

此时**查找并列出域**窗口会显示，其中显示所有管理员管理和系统管理的 IM 地址域。

步骤 2 执行以下操作之一：

- 单击**新增**以添加新域。 此时将显示**域**窗口。
- 从域列表中选择要编辑的域。 此时将显示**域**窗口。

步骤 3 在**域名**字段中输入最多包含 255 个字符的唯一域名，然后单击**保存**。

每个域名在整个群集中必须唯一。 域名可以使用任何大写或小写字母 (a-zA-Z)、任何数字 (0-9)、连字符 (-) 或点号 (.)。 点号作为域标签分隔符。 域标签不得以连字符开头。 最后一个标签（如 .com）不得以数字开头。 Abc.1om 是无效域的示例。

下一步做什么

如果您使用的是 TLS XMPP 联合，请继续重新生成 XMPP 客户端和 TLS 证书，第 29 页。

删除 IM 地址域

您可以使用 Cisco Unified CM IM and Presence 管理 GUI 删除本地群集中管理员管理的 IM 地址域。

不能删除系统管理的域，因为它们正在使用中。 如果系统中再无使用该 IM 地址域的用户（如用户已被删除），则系统管理的域会自动变成管理员管理的域。 您可以编辑或删除管理员管理的域。

注释 如果您删除在本地和对等群集中均已配置的管理员管理的域，该域将保留在管理员管理的域列表中；但是，该域将仅标记为已在对等群集中配置。 要完全删除该条目，必须在配置了该域的所有群集中删除该域。

开始之前

确保禁用高可用性，并停止基本的 IM and Presence Service。 有关详细信息，请参阅：禁用 IM and Presence Service，第 25 页。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中选择 **Presence** > **域**。

此时**查找并列出域**窗口会显示，其中显示所有管理员管理和系统管理的 IM 地址域。

步骤 2 使用以下方法之一选择要删除的管理员管理的域，然后单击**删除选定项**。

- 选中要删除的域旁边的复选框。
- 单击**全部选择**选择管理员管理的域列表中的所有域。

提示 单击**全部清除**以清除所有选定项。

步骤 3 单击**确定**确认删除或单击**取消**。

下一步做什么

如果您使用的是 TLS XMPP 联合，请继续重新生成 XMPP 客户端和 TLS 证书，第 29 页。

重新生成 XMPP 客户端和 TLS 证书

更改 IM 域后，您必须重新生成 XMPP 客户端或 TLS 证书。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 操作系统管理**中选择**安全性** > **证书管理**。
步骤 2 单击**查找**以生成证书列表。
步骤 3 单击 **cup-xmpp-s2s** 证书。
步骤 4 在**证书详细信息**窗口中单击**重新生成**。

启动 IM and Presence 服务

更改默认域后，执行此程序来重新启动所有群集节点上的 IM and Presence Service。

开始之前

重新生成 XMPP 客户端和 TLS 证书，第 29 页

过程

步骤 1 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 网络服务**。
步骤 2 从**服务器**列表选择要重新激活服务的节点并单击**前往**。
步骤 3 在 **IM and Presence Service** 区域选择以下服务：

- **Cisco 客户端配置文件代理**
- **思科同步代理**
- **Cisco XCP 路由器**

步骤 4 单击**重新启动**。
步骤 5 从**相关链接**下拉列表选择**服务激活**，然后单击**前往**。
步骤 6 在 **IM and Presence Service** 区域选择以下服务：

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

步骤 7 单击**保存**。

下一步做什么

启用 Presence 冗余组的高可用性，第 30 页

启用 Presence 冗余组的高可用性

更改默认域并重新启动 IM and Presence Service 后，可以为 Presence 冗余组启用高可用性。

开始之前

启用高可用性之前，所有服务必须在 IM and Presence 数据库发布方节点和订阅方节点上运行。 如果服务重新启动后不到 30 分钟，请确认在启用高可用性之前已重新创建 Cisco Jabber 会话。 否则，Presence 将不适用于未创建会话的 Jabber 客户端。

要获取 Cisco Jabber 的会话数，请在所有群集节点上运行 `show perf query counter "Cisco Presence Engine" Active JsmSessions` 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。

在以下阶段，您应使用 Cisco 实时监控工具 (RTMT) 来监控发布方和订阅方上的性能计数器`"Cisco Presence Engine" ActiveJsmSessions`:

- 发布方或订阅方重新启动后
- Cisco XCP 路由器重新启动后
- Cisco Presence Engine 重新启动后

确保在启用高可用性之前，`"Cisco Presence Engine" ActiveJsmSessions` 的数量必须与分配到该节点的用户数相同。

注释 只有在用户 `ActiveJsmSessions` 创建进度完成后，才能启用高可用性。

过程

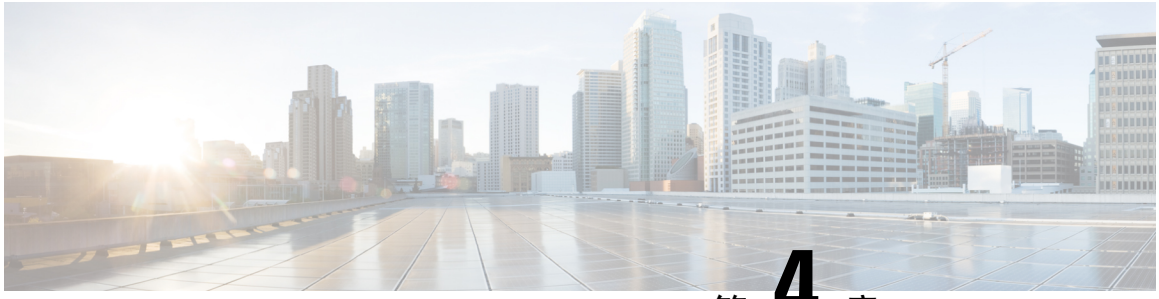
步骤 1 从 Cisco Unified CM 管理用户界面中，选择**系统** > **Presence 冗余组**。

步骤 2 单击**查找**并选择组。
此时将显示 **Presence 冗余组配置**窗口。

步骤 3 选中**启用高可用性**复选框。

步骤 4 单击**保存**。

步骤 5 为每个 Presence 冗余组重复执行此步骤。



第 4 章

配置 IPv6

- 配置 IPv6 概述， 第 33 页
- 配置 IPv6 任务流程， 第 34 页

配置 IPv6 概述

即使 IM and Presence Service 与 Cisco Unified Communications Manager 之间的连接使用 IPv4，也可以对 IM and Presence Service 上的外部接口使用 IPv6。

如果为 IM and Presence Service 节点中的任何以下项目配置了 IPv6，该节点不会接受传入的 IPv4 信息包，也不会自动恢复使用 IPv4：

- 连接到外部数据库
- 连接到 LDAP 服务器
- 连接到 Exchange 服务器
- 进行联合部署

对于联合，如果需要支持联合链接到启用 IPv6 的外部企业，您必须为 IPv6 启用 IM and Presence Service。即使 IM and Presence Service 节点与联合的企业之间安装了 ASA，也是这种情况。ASA 对 IM and Presence Service 节点是透明的。

有关使用命令行界面配置 IPv6 参数的详细信息，请参阅《*Cisco Unified Communications Manager* 管理指南》和《*Cisco Unified Communications* 解决方案的命令行界面指南》，网址：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

配置 IPv6 任务流程

过程

	命令或操作	目的
步骤 1	在 IM and Presence Service 的 Eth0 上启用 IPv6，第 34 页	在群集中的每个 IM and Presence Service 节点的 Eth0 端口上启用 IPv6。 您必须重新启动每个节点以应用更改。
步骤 2	启用 IPv6 企业参数，第 35 页	在 Eth0 端口上启用 IPv6 后，必须为 IM and Presence Service 群集启用 IPv6 企业参数。
步骤 3	重新启动服务 ，第 35 页	您必须重新启动 IM and Presence Service 以应用更改。
步骤 4	将 IPv6 地址分配到 IM and Presence 节点，第 36 页	向您的 IM and Presence Service 节点分配 IPv6 地址。

在 IM and Presence Service 的 Eth0 上启用 IPv6

使用 Cisco Unified IM and Presence 操作系统管理 GUI，在群集的每个 IM and Presence Service 节点的 Eth0 端口上启用 IPv6。

过程

步骤 1 在 **Cisco Unified IM and Presence 操作系统管理**中选择**设置** > **IP** > **以太网 IPv6**。

步骤 2 在“以太网 IPv6 配置”窗口中选中**启用 IPv6** 复选框。

步骤 3 选择**地址源**：

- 路由器通告
- DHCP
- 手动输入

如果已选择“手动输入”，则输入 **IPv6 地址**、**子网掩码**和**默认网关**值。

步骤 4 选中**通过重新启动更新**复选框。

提示　如果要稍后手动重新启动节点（例如在安排的维护时段），则不要选中**通过重新启动更新**复选框；但是，您所做的更改在重新启动节点后才会生效。

步骤 5 单击**保存**。

如果选中**通过重新启动更新**复选框，节点将重新启动，并将应用更改。

下一步做什么

启用 IPv6 企业参数 ，第 35 页

启用 IPv6 企业参数

使用 Cisco Unified CM IM and Presence 管理为 IM and Presence Service 群集启用 IPv6 企业参数。

开始之前

在 IM and Presence Service 的 Eth0 上启用 IPv6 ，第 34 页

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中选择**系统** > **企业参数**。

步骤 2 在**企业参数配置**窗口的 IPv6 面板中选择**真**。

步骤 3 单击**保存**。

下一步做什么

重新启动服务 ，第 35 页 应用更改。

重新启动服务

此程序用于在启用群集的 IPv6 企业参数后，重新启动 IM and Presence Service。

提示 要使用 Cisco Unified CM IM and Presence 管理监控系统重新启动通知，请选择**系统** > **通知**。

开始之前

启用 IPv6 企业参数 ，第 35 页

过程

步骤 1 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 网络服务**。

步骤 2 从**服务器**列表选择要重新激活服务的节点并单击**前往**。

步骤 3 在 **IM and Presence Service** 区域选择 **Cisco XCP 路由器**。

步骤 4 单击**重新启动**。

步骤 5 从**相关链接**下拉列表选择**服务激活**，然后单击**前往**。

步骤 6 在 **IM and Presence Service** 区域选择以下服务：

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

步骤 7 单击**保存**。

将 IPv6 地址分配到 IM and Presence 节点

在 Cisco Unified Communications Manager 按照此程序为您的 IM and Presence 节点分配 IPv6 地址。

开始之前

您还必须在 Cisco Unified 操作系统管理中启用 IPv6 Eth0 端口，并启用 IPv6 企业参数。

过程

步骤 1 登录到 Cisco Unified Communications Manager 发布方节点

步骤 2 从 Cisco Unified CM 管理中，选择**系统** > **服务器**。

步骤 3 完成以下任务之一：

- 要添加新服务器，单击**新增**。
- 要更新现有服务器，单击要编辑的服务器。

步骤 4 如果是添加新服务器，从**服务器类型**下拉菜单选择 **CUCM IM and Presence** 并单击**下一步**。

步骤 5 输入服务器的 **IPv6 地址**。

步骤 6 单击**保存**。

步骤 7 对每个 IM and Presence Service 群集节点重复此操作。

在 IM and Presence Service 的 Eth0 上禁用 IPv6

如要禁用 IPv6，使用 **Cisco Unified IM and Presence 操作系统管理** GUI 在不希望使用 IPv6 的群集中的所有 IM and Presence Service 节点的 Eth0 端口上禁用 IPv6。 您必须重新启动节点以应用更改。

注释 如果您不希望群集中的任何节点使用 IPv6，则确保对群集禁用 IPv6 企业参数。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 操作系统管理**中选择**设置** > **IP** > **以太网 IPv6**。

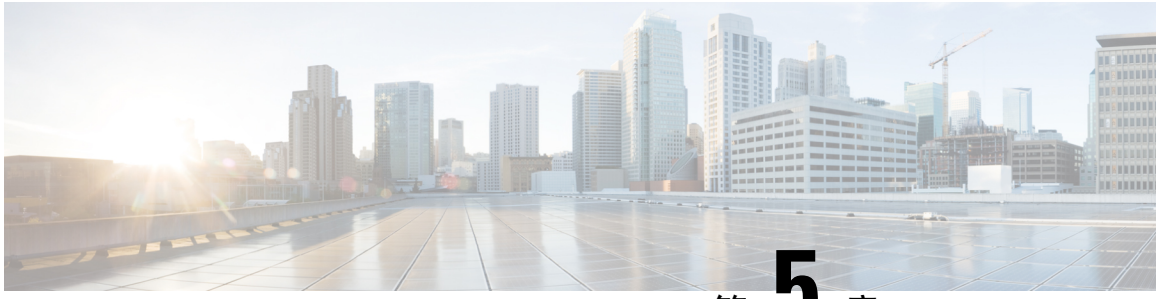
步骤 2 在“以太网 IPv6 配置”窗口中取消选中**启用 IPv6** 复选框。

步骤 3 选中**通过重新启动更新**复选框。

提示 如果要稍后手动重新启动节点（例如在安排的维护时段），则不要选中**通过重新启动更新**复选框；但是，您所做的更改在重新启动节点后才会生效。

步骤 4 单击**保存**。

如果选中**通过重新启动更新**复选框，节点将重新启动，并将应用更改。



第 5 章

配置 IM 寻址方案

- IM 寻址方案概述， 第 39 页
- IM 寻址方案前提条件， 第 40 页
- 配置 IM 寻址方案任务流程， 第 41 页

IM 寻址方案概述

IM and Presence Service 支持两种 IM 寻址方案：

- *UserID@Default_Domain* 是您安装 IM and Presence Service 时的默认 IM 地址方案。
- 目录 URI IM 地址方案支持多个域，与用户的电子邮件地址一致，并且与 Microsoft SIP URI 一致。

您必须在所有 IM and Presence Service 群集中使用相同的 IM 地址方案。

使用 User@Default_Domain 的 IM 地址

IM and Presence Service 的默认寻址方案是 *UserID@Default_Domain*。

当您使用 *UserID@Default_Domain* IM 地址方案时，所有 IM 地址都是一个默认 IM 域的一部分。 默认域值必须在所有群集上保持一致。 因为所有 IM 地址是 IM and Presence 默认域的一部分，所以不支持多个域。

UserID 可以是自由格式的，也可以从 LDAP 同步。 以下字段受支持：

- sAMAccountName
- 用户主体名称 (UPN)
- 电子邮件地址
- 员工编号
- 电话号码

如果 UserID 在 Cisco Unified Communications Manager 上映射到 LDAP 字段，则该 LDAP 映射必须在所有群集上保持一致。

虽然您可以将 UserID 映射到电子邮件地址，但这并不意味着 IM URI 等同于电子邮件地址， 而是变成 *<email-address>@Default_Domain*。 例如，`amckenzie@example.com@sales-example.com`。 您选择的 Active Directory (AD) 映射设置可以应用于该 IM and Presence Service 群集中的所有用户。 无法为各个用户设置不同的映射。

使用目录 URI 的 IM 地址

目录 URI 地址方案让用户的 IM 地址与其 Cisco Unified Communications Manager 目录 URI 保持一致。

目录 URI IM 地址方案提供以下 IM 寻址功能：

- 多域支持。 IM 地址无需使用单个 IM and Presence Service 域。
- 与用户的邮箱地址一致。 您可以将 Cisco Unified Communications Manager 目录 URI 配置为与用户的电子邮件地址保持一致，以便为邮箱、IM、语音和视频通信提供一致的标识。
- 与 Microsoft SIP URI 一致。 Cisco Unified Communications Manager 目录 URI 可配置为与 Microsoft SIP URI 保持一致，以确保在从 Microsoft OCS/Lync 迁移到 IM and Presence Service 时可以保持用户身份。

如果将节点配置为使用目录 URI 作为 IM 地址方案，我们建议您仅部署支持目录 URI 的客户端。 如果启用目录 URI IM 地址方案，则任何不支持目录 URI 的客户端均不起作用。 如果您部署了不支持目录 URI 的客户端，思科建议您使用 *UserID@Default_Domain* IM 地址方案，而不使用目录 URI IM 地址方案。

目录 URI IM 地址设置是全局性设置，应用到群集中的所有用户。 您无法为群集中的个别用户设置不同的目录 URI IM 地址。

有关从外部 LDAP 目录设置目录 URI 的详细信息，请参阅配置 LDAP 目录 ，第 71 页。

多个 IM 域

IM and Presence Service 支持在多个 IM 地址域中进行 IM 寻址，并会自动列出系统中的所有域。您可以添加、编辑或删除域。有关 IM 域的配置信息，请参阅配置域概述 ，第 21 页。

如果您在使用 Cisco Expressway，请参阅《*Cisco Expressway* 管理员指南》，网址：http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html。

IM 寻址方案前提条件

您使用的 IM and Presence Service 默认域和 IM 地址方案必须跨所有 IM and Presence Service 群集一致。 开始之前，配置 IM and Presence Service 上的默认域 ，第 26 页。

您设置的 IM 地址方案将影响所有用户 JID，因此无法以分阶段方式执行而不中断可能有不同设置的群集之间的通信。

如果任何部署的客户端不支持目录 URI 作为 IM 地址，管理员应禁用目录 URI IM 地址方案。

配置 IM 寻址方案任务流程

按以下顺序完成这些任务以配置 IM 寻址方案。

过程

	命令或操作	目的
步骤 1	验证用户设置，第 41 页	验证并确保已正确设置最终用户，并且没有重复或无效的用户。
步骤 2	禁用高可用性，第 42 页	您必须暂时为 Presence 冗余组禁用高可用性。若要配置 IM 寻址方案，必须暂时停止服务；如果在启用高可用性的情况下停止服务，会发生系统故障转移。
步骤 3	停止服务，第 42 页	在更新 IM 寻址方案配置之前，停止基本 IM and Presence Service。 确保按照规定的顺序停止服务。
步骤 4	分配 IM 寻址方案，第 43 页	此程序用于配置新域和 IM 地址方案，或更新现有的域和地址方案。
步骤 5	重新启动服务，第 45 页	配置好 IM 寻址方案之后，重新启动服务。您必须在更新用户地址信息或设置新用户之前执行此操作。 重新启动服务时，请确保遵循规定的顺序。
步骤 6	启用高可用性，第 45 页	配置 IM 寻址方案并重新启动 IM and Presence Service 后，可以为 Presence 冗余组启用高可用性。 启用高可用性之前，所有服务必须在 IM and Presence 数据库发布方节点和订阅方节点上运行。
步骤 7	如果您选择**目录 URI** 作为 IM 寻址方案： • 为目录 URI 分配 LDAP 源，第 46 页 • 手动分配目录 URI，第 47 页	可选。 如果要从外部 LDAP 目录同步用户，请为目录 URI 值设置 LDAP 源字段。 对于非 LDAP 用户，您必须手动设置目录 URI。 您可以逐个用户地执行此操作，也可以通过批量管理工具完成。

验证用户设置

此程序用于在配置寻址方案之前验证是否正确设置了最终用户。

过程

步骤 1 在 Cisco Unified CM IM and Presence 管理中选择**诊断** > **系统故障诊断程序**。
系统故障诊断程序将运行。

步骤 2 在**用户故障诊断程序**部分，验证并确保已正确设置最终用户，并且没有重复或无效的用户。

下一步做什么

禁用高可用性，第 42 页

禁用高可用性

在群集的每个 Presence 冗余组中禁用高可用性。 若要编辑寻址方案，必须先暂停服务。 如果在启用高可用性的情况下停止服务，将会发生系统故障转移。

注释 **Presence 冗余组详细信息**页面将显示所有活动的 JSM 会话，即使群集中禁用了高可用性也不例外。

开始之前

记录每个 Presence 冗余组中每个群集节点的活动用户数。 您可以在 Cisco Unified CM IM and Presence 管理（**系统** > **Presence 拓扑**）窗口中找到此信息。 当您稍后重新启用高可用性时，需要这些数字。

过程

步骤 1 从 Cisco Unified CM 管理用户界面中，选择**系统** > **Presence 冗余组**。

步骤 2 单击**查找**并选择组。

步骤 3 在 Presence 冗余组配置窗口中，取消选中**启用高可用性**复选框。

步骤 4 单击**保存**。

步骤 5 为每个 Presence 冗余组重复执行此步骤。

步骤 6 完成后等待至少两分钟，以便先在群集中同步新的高可用性设置，再做其他进一步更改。

下一步做什么

停止服务，第 42 页

停止服务

在更新 IM 寻址方案配置之前，停止基本 IM and Presence Service。 确保按照规定的顺序停止服务。

开始之前

禁用高可用性，第 42 页

过程

步骤 1 在 **Cisco Unified IM and Presence** 功能配置中选择工具 > 控制中心 – 网络服务。

步骤 2 选择服务并单击停止按键，按此顺序停止以下 IM and Presence Service：

a) 思科同步代理

b) **Cisco** 客户端配置文件代理

步骤 3 两种服务停止后，选择工具 > 控制中心 – 功能服务，按此顺序停止以下服务：

a) **Cisco Presence Engine**

b) **Cisco SIP Proxy**

步骤 4 两种服务停止后，选择工具 > 控制中心 – 功能服务，停止以下服务：

- **Cisco XCP** 路由器

注释 停止 XCP 路由器服务后，所有相关 XCP 功能服务都会自动停止。

下一步做什么

分配 IM 寻址方案，第 43 页

分配 IM 寻址方案

此程序用于配置新域和 IM 地址方案，或更新现有的域和地址方案。

注释 确保您配置的 IM 寻址方案在所有群集中保持一致。

开始之前

停止服务，第 42 页

过程

步骤 1 在 **Cisco Unified CM IM and Presence** 管理中选择 **Presence** > 设置 > 高级配置。

步骤 2 要分配一个新的默认域，选中默认域复选框，然后在文本框中输入新域。

步骤 3 要更改地址方案，选中 **IM** 地址方案复选框，然后从下拉列表框选择以下选项之一：

- **UserID@[Default_Domain]** — 每个 IM 用户地址都派生自用户 ID 和默认域。 这是默认设置。

- **目录 URI** — 每个 IM 用户地址匹配在 Cisco Unified Communications Manager 中为该用户配置的目录 URI。

  注释　如果选择此选项，所有部署的客户端必须支持目录 URI 作为 IM 地址，并使用基于 EDI 或 UDS 的目录集成。 对于同 Jabber 基于 UDS 的集成，您必须运行 Jabber 10.6 或更高版本。

步骤 4 单击**保存**。

您可以在状态区域监控更新进度。

如果选择目录 URI 作为 IM 地址方案，系统可能会提醒您确保已部署的客户端支持多个域。 单击**确定**以继续或单击**取消**。

如果任何用户的目录 URI 设置无效，则会显示一个对话框。 单击**确定**继续或单击**取消**，然后在重新配置 IM 地址方案前修改用户设置。

系统更新最多只需 1 小时即可完成。 单击**重试**以重新应用更改或单击**取消**。

下一步做什么

如果将 user@default_domain 配置为寻址方案，并且未使用目录 URI，则继续重新启动服务，第 45 页。

如果将目录 URI 配置为寻址方案，选择下列选项之一：

- 为目录 URI 分配 LDAP 源，第 46 页
- 手动分配目录 URI，第 47 页

IM 地址示例

适用于 IM and Presence Service 的 IM 地址选项示例。

IM and Presence Service 默认域：cisco.com

用户：John Smith

用户 ID：js12345

邮箱 ID：jsmith@cisco-sales.com

SIPURI：john.smith@webex.com

IM 地址格式	目录 URI 映射	IM 地址
<userid>@<domain>	不适用	js12345@cisco.com
目录 URI	mailid	jsmith@cisco-sales.com
目录 URI	msRTCSIP-PrimaryUserAddress	john.smith@webex.com

重新启动服务

配置好 IM 寻址方案之后，重新启动服务。 您必须在更新用户地址信息或设置新用户之前执行此操作。 重新启动服务时，请确保遵循规定的顺序。

开始之前

- 分配 IM 寻址方案，第 43 页
- 如果将目录 URI 配置为寻址方案，请先完成以下选项之一，再重新启动服务：
  - 为目录 URI 分配 LDAP 源，第 46 页
  - 手动分配目录 URI，第 47 页

过程

步骤 1 在 **Cisco Unified IM and Presence 功能配置**中选择**工具** > **控制中心 – 网络服务**。

步骤 2 选择并单击**开始**按键，以启动以下服务：

- **Cisco XCP 路由器**

步骤 3 服务启动后，选择**工具** > **控制中心 – 功能服务**，按此顺序启动以下服务：

a) **Cisco SIP Proxy**
b) **Cisco Presence Engine**

步骤 4 确认 Cisco Presence Engine 服务正在所有节点上运行，再继续执行下一步。

步骤 5 选择**工具** > **控制中心 – 网络服务**，按此顺序启动以下服务：

a) **Cisco 客户端配置文件代理**
b) **思科同步代理**

下一步做什么

启用高可用性，第 45 页

启用高可用性

在配置您的 IM 寻址方案并重新启动服务之后，执行此程序来重新启用群集中每个 presence 冗余组的高可用性

开始之前

启用高可用性之前，所有服务必须在 IM and Presence 数据库发布方节点和订阅方节点上运行。 如果服务重新启动后不到 30 分钟，请确认在启用高可用性之前已重新创建 Cisco Jabber 会话。 否则，Presence 将不适用于未创建会话的 Jabber 客户端。

要获取 Cisco Jabber 的会话数，请在所有群集节点上运行 `show perf query counter Cisco Presence Engine Active JsmSessions` 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。

过程

步骤 1 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 网络服务**。

步骤 2 从**服务器**列表选择要重新激活服务的节点并单击**前往**。

步骤 3 在 **IM and Presence Service** 区域选择以下服务：

- **Cisco 客户端配置文件代理**
- **思科同步代理**
- **Cisco XCP 路由器**

步骤 4 单击**重新启动**。

步骤 5 从**相关链接**下拉列表选择**服务激活**，然后单击**前往**。

步骤 6 在 **IM and Presence Service** 区域选择以下服务：

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

步骤 7 单击**保存**。

为目录 URI 分配 LDAP 源

如果要从外部 LDAP 目录同步用户，可以执行此程序来分配用于分配目录 URI 的外部 LDAP 目录源字段。 发生 LDAP 目录同步时，系统将根据您配置的字段的值分配目录 URI。

注释 如果已经发生初始同步，则无法对 Cisco Unified Communications Manager 中的现有 LDAP 配置应用编辑。 您可以同步添加到外部 LDAP 目录的新项目，但无法在 Cisco Unified Communications Manager 中编辑 LDAP 配置。 如果您已同步 LDAP 目录：

- 使用批量管理工具将目录 URI 分配给用户。 有关详细信息，请参阅《*Cisco Unified Communications Manager* 批量管理指南》。
- 手动将目录 URI 分配给用户

开始之前

分配 IM 寻址方案，第 43 页

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统** > **LDAP** > **LDAP 目录**。

步骤 2 从**目录 URI** 下拉列表中选择以下选项之一：

- **mail**：将目录 URI 映射到用户的电子邮件地址，以便为电子邮件、IM、语音和视频通信提供一致的标识。
- **msRTCSIP-PrimaryUserAddress**：将目录 URI 映射到 Microsoft OCS/Lync SIP URI。

注释 在 LDAP 同步发生之前，不会设置目录 URI。 关于配置 LDAP 目录同步的详细信息，请参阅配置 LDAP 目录，第 71 页。

下一步做什么

重新启动服务，第 45 页

手动分配目录 URI

如果您未使用 LDAP，可以执行此程序来逐个用户手动输入目录 URI。

注释 您还可以使用批量管理工具通过 csv 文件为大量最终用户设置目录 URI。有关批量管理的详细信息，请参阅《*Cisco Unified Communications Manager* 批量管理指南》，网址：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

如果尚未同步 LDAP 目录，可以通过 LDAP 目录同步为用户设置目录 URI。

开始之前

分配 IM 寻址方案，第 43 页

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 输入适当的搜索条件，然后单击**查找**。

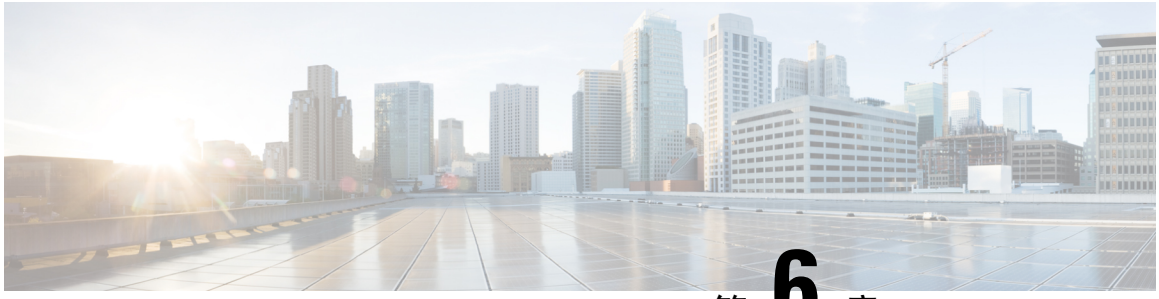
步骤 3 选择您要配置的最终用户。

步骤 4 在**用户信息**区域的**目录 URI** 字段中输入目录 URI。

步骤 5 单击**保存**。

下一步做什么

重新启动服务，第 45 页



第 6 章

配置冗余和高可用性

- Presence 冗余组概述，第 49 页
- Presence 冗余组前提条件，第 50 页
- Presence 冗余组任务流程，第 50 页
- 启动手动故障转移、回退或恢复，第 55 页
- IM and Presence 故障转移增强，停机时间几乎为零，第 61 页
- 冗余相互作用和限制，第 63 页

Presence 冗余组概述

Presence 冗余组由两个来自同一群集的 IM and Presence Service 节点构成。 Presence 冗余组中的每个节点都监控对等节点的状态或心跳。 您可以配置 Presence 冗余组，以便为 IM and Presence Service 客户端和应用程序提供冗余和恢复。

- 故障转移 — 当组中 IM and Presence Service 节点上的一个或多个关键服务失败或组中的节点断开连接时，Presence 冗余组中将发生故障转移。 客户端自动连接到该组中的另一个 IM and Presence Service 节点。
- 回退 — 在发生以下情况期间，从 CLI 或 Cisco Unified Communications Manager 发出回退命令时，即发生回退：
  - 断开连接的 IM and Presence Service 节点恢复服务，且所有关键服务均在运行中。 在节点恢复连接后，该组中故障转移的客户端重新连接到恢复的节点。
  - 备份的已激活 IM and Presence Service 节点由于关键服务失败而断开连接，对等节点处于“故障转移”状态且支持自动恢复回退。

例如，如果您在使用 Presence 冗余组时，本地 IM and Presence Service 节点上的服务失败或硬件出现故障，Cisco Jabber 客户端将故障转移到备份的 IM and Presence Service 节点。 如果您配置了自动回退，当断开连接的节点重新上线后，客户端将自动重新连接到本地 IM and Presence Service 节点。 如果未配置自动回退，当断开连接的节点上线后，您可以手动启动回退。

除冗余和恢复之外，您还可以通过 Presence 冗余组为群集配置高可用性。

高可用性

IM and Presence Service 支持多节点高可用性部署。

配置 Presence 冗余组后，您可以为组启用高可用性。 高可用性需要一对节点。 每个节点都有一个独立的数据库和使用能够支持普通用户的共享可用性数据库操作的一组用户。

所有 IM and Presence Service 节点均须属于某个 Presence 冗余组，该组可以包含一个 IM and Presence Service 节点或一对 IM and Presence Service 节点。

您可以使用两种不同模式配置高可用性：

- 平衡模式：当一个节点因组件故障或电源断开而出现问题时，为冗余高可用性提供自动用户负载均衡和用户故障转移。
- 主用/备用模式：备用节点会在活动节点失败时自动接管活动节点。 它不提供自动负载均衡。

我们建议您将 IM and Presence Service 部署配置为高可用性部署。 虽然您可以在一个部署中同时配置高可用性和非高可用性 Presence 冗余组，但是不建议您使用此配置。

Presence 冗余组前提条件

对于 WAN 上的部署，每个 IM and Presence Service 群集需要至少每秒 10 兆比特的专用带宽，以及不超过 80 毫秒的往返滞后时间。 小于此建议的任何带宽均可对性能造成不良影响。

Presence 冗余组任务流程

IM and Presence Service 节点只能分配给一个 Presence 冗余组。 要获得高可用性，您必须将同一群集中的两个节点分配到 Presence 冗余组，并为该组启用高可用性。

过程

	命令或操作	目的
步骤 1	验证数据库复制， 第 51 页	确保在 IM and Presence Service 群集中设置了数据库复制。
步骤 2	验证服务， 第 51 页	确保关键服务正在您计划添加到 Presence 冗余组的节点上运行。
步骤 3	配置 Presence 冗余组， 第 52 页	为 IM and Presence Service 客户端和应用程序提供冗余和恢复。
步骤 4	配置故障转移的心跳间隔， 第 53 页	可选。 Presence 冗余组中的每个节点都监控其对等节点的状态或心跳。 您可以配置每个节点监控其对等节点的时间间隔。

	命令或操作	目的
步骤 5	启用高可用性，第 54 页	可选。 如果在配置 Presence 冗余组时未启用高可用性，请按此程序操作。
步骤 6	配置用户分配模式，第 55 页	配置您希望同步代理如何在 IM and Presence Service 群集的各个节点上分配用户。 此设置会影响系统处理故障转移和负载均衡的方式。

验证数据库复制

为 Presence 冗余组启用高可用性之前，需确保在 IM and Presence Service 群集中设置了数据库复制。

过程

步骤 1 使用以下方法之一启动一个 CLI 会话：

- 从远程系统，使用 SSH 安全连接到 Cisco Unified 操作系统。 在 SSH 客户端，输入您的 **ssh *adminname@hostname***，然后输入密码。
- 从到串行端口的直接连接，看到自动显示的系统提示时，输入您的凭证。

步骤 2 执行 **utils dbreplication status** 命令以检查数据库表中是否存在错误或不匹配问题。

步骤 3 执行 **utils dbreplication runtimestate** 命令以检查数据库复制在节点上是否处于活动状态。

输出会列出所有节点；如果数据库复制已设置且处于良好状态，每个节点的**复制设置**值为 **2**。

如果返回的值不是 2，则必须先消除错误，然后再继续。

下一步做什么

验证服务，第 51 页

验证服务

确保关键服务正在您计划添加到 Presence 冗余组的节点上运行。 启用高可用性之前，关键服务必须运行。 如果两个节点上都没有运行关键服务，当您启用高可用性时，Presence 冗余组将进入故障状态。 如果关键服务未在一个节点上停止运行，当您启用高可用性时，该节点将会故障转移到另一个节点。

开始之前

验证数据库复制，第 51 页

过程

步骤 1 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 网络服务**。

步骤 2 从**服务器**列表选择合适的节点，然后单击**执行**。

步骤 3 在 **IM and Presence Service** 区域中，确保以下服务已启动：

- **Cisco 客户端配置文件代理**
- **思科同步代理**
- **Cisco XCP 路由器**

步骤 4 从**相关链接**下拉列表选择**控制中心 - 网络服务**，然后单击**前往**。

步骤 5 在 **IM and Presence Service** 区域中，确保以下服务已启动：

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

下一步做什么

配置 Presence 冗余组，第 52 页

配置 Presence 冗余组

使用 Cisco Unified Communications Manager 为 IM and Presence Service 节点配置冗余。

每个 Presence 冗余组可以包含两个 IM and Presence Service 节点。 一个节点只能分配给一个 Presence 冗余组。 Presence 冗余组中的两个节点都必须位于同一群集并且有相同的 IM and Presence Service 数据库发布方节点。

开始之前

- 验证服务，第 51 页
- 确保您添加到 Presence 冗余组的 IM and Presence Service 节点在运行相同的软件版本。

过程

步骤 1 从 **Cisco Unified CM 管理**中，选择**系统** > **Presence 冗余组**。

步骤 2 单击**新增**。

步骤 3 为 Presence 冗余组输入一个唯一的名称。

您最多可以输入 128 个字母数字字符，包括下划线 (_) 和连字符 (-)。

步骤 4 输入组说明。

您最多可以输入128个字母数字字符，可包含符号，但不能包含双引号 (")、百分号 (%)、和号 (&)、反斜线 (\) 或尖括号 (<>)。

步骤 5 在 **Presence 服务器**字段中选择两个不同的 IM and Presence Service 节点，以便将它们分配给该组。

步骤 6 （可选） 选中**启用高可用性**复选框，为 Presence 冗余组启用高可用性。

步骤 7 单击**保存**。

下一步做什么

配置故障转移的心跳间隔 ，第 53 页

配置故障转移的心跳间隔

配置确定保持连接设置的可选服务参数，通过该设置，Presence 冗余组中的每个节点会监控其对等节点的心跳（即状态），以确认该对等节点是否处于活动状态。 如果在配置的计时器到期后对等节点没有响应，可启动故障转移。

注释 思科建议您使用这些服务参数的默认值。 不过，您也可以根据自身需求重新配置值。

过程

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

步骤 2 从**服务器**下拉列表中选择 IM and Presence 节点

步骤 3 从**服务**下拉列表中选择 **Cisco Server Recovery Manager**（**活动**）。

步骤 4 在**常规 Server Recovery Manager 参数**（**群集范围**）下，配置 Presence 冗余组中的每个节点用于监控其对等节点心跳的群集范围内的保持连接设置。 如果对等节点没有响应，可启动故障转移。

- **服务端口** — 此参数指定 Cisco Server Recovery Manager 用于与其对等节点通信的端口。 默认值为 22001。
- **管理 RPC 端口** — 此参数指定 Cisco Server Recovery Manager 用于提供管理 RPC 请求的端口。 默认值为 20075。
- **关键服务延迟** — 此参数指定在启动故障转移之前关键服务可以关闭的时长（以秒为单位）。 默认值为 90。
- **启用自动回退** — 此参数指定是否执行自动回退。 如果发生故障转移，在主节点恢复为健康状态三十分钟后，IM and Presence Service 会自动将用户从备份节点移到主节点。 默认值为 False。
- **初始化保持连接（心跳）超时** — 此参数指定在启动故障转移之前的初始化期间，对等节点可失去心跳的时长（以秒为单位）。 默认值为 120。
- **保持连接（心跳）超时** — 此参数指定在启动故障转移之前，对等节点可失去心跳的时长（以秒为单位），默认值为 60。

- **保持连接（心跳）间隔**—此参数指定两次向对等节点发送保持连接（心跳）消息之间的间隔。默认值为 15。
- **启用 XCP 身份验证服务监控** — 此参数用于配置系统以监控 Cisco XCP 身份验证服务，并在服务在节点上出现故障时启动自动故障转移到对等节点。 在**启用 XCP 身份验证服务监控**字段中，将服务参数的值设置为 **TRUE**。

步骤 5 配置以下附加参数，这些参数指定CUPC 8.5及更高版本的客户端在尝试重新登录之前需要等待多长时间。 与上述参数不同，必须为每个群集节点单独配置这些参数。

- **客户端重新登录下限** — 此参数指定 CUPC 8.5（及更高版本）在尝试重新登录此服务器之前应等待的最小秒数。 默认值为 120。
- **客户端重新登录上限** — 此参数指定 CUPC 8.5（及更高版本）在尝试重新登录此服务器之前应等待的最大秒数。 默认值为 537。

步骤 6 单击**保存**。

下一步做什么

如果在配置 Presence 冗余组时未启用高可用性，请立即启用高可用性，第 54 页。

启用高可用性

⚠

注意 若无法在 IM and Presence Service 集中设置复制并确保所有关键服务运行，则会导致启用在线状态冗余组的高可用性后立即发生故障转移。

开始之前

- 配置 Presence 冗余组，第 52 页
- 确保在 IM and Presence Service 集中设置了复制。
- 确保所有关键服务都在运行。

过程

步骤 1 从 **Cisco Unified CM 管理**中，选择**系统** > **Presence 冗余组**。

步骤 2 指定搜索条件，然后单击**查找**。

步骤 3 选择您配置的 Presence 冗余组。

步骤 4 要启用高可用性，请选中**启用高可用性**复选框。

步骤 5 单击**保存**。

配置用户分配模式

此程序用于配置同步代理将用户分配至群集中节点的方式。 此设置可帮助管理故障转移和负载均衡。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 在**用户管理参数**区域，为 **Presence 服务器的用户分配模式**参数选择以下选项之一：

- **平衡**—此模式会将用户平均分配到每个子群集中的各个节点，并尝试让各个节点上的用户总数达到均衡。 这是默认选项。
- **主用-备用** — 此模式会将所有用户分配至子群集的第一个节点，并让第二个服务器作为备份。
- **无**— 如果选择此模式，同步代理不会将任何用户分配到群集中的节点。

步骤 3 单击**保存**。

启动手动故障转移、回退或恢复

此程序用于启动 Presence 冗余组中 IM and Presence Service 节点的手动故障转移、回退或恢复。

- 手动故障转移 — 当您启动手动故障转移时，**Cisco Server Recovery Manager** 将在故障节点上停止关键服务。 故障节点上的所有用户都将断开连接，必须重新登录到备用节点。 除非我们调用手动回退，否则关键服务不会重新启动。
- 手动回退 — 当您启动手动回退时，**Cisco Server Recovery Manager** 将重新启动主节点上的关键服务，并断开已经故障转移的所有用户。 然后，这些用户必须重新登录到其被分配到的节点。
- 手动恢复 — 当 Presence 冗余组中的两个节点都处于故障状态时，需要进行手动恢复。 此时，IM and Presence Service 会重新启动 Presence 冗余组中两个节点上的 **Cisco Server Recovery Manager** 服务。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统** > **Presence 冗余组**。

步骤 2 单击**查找**并选择具有适用节点的 Presence 冗余组。

步骤 3 执行下列操作之一： 请注意，可用的按键取决于节点当前的状态：

- 单击**故障转移**可启用活动节点的故障转移。
- 单击**回退**可启动故障转移节点的回退。

- 如果两个节点都已进行故障转移并且您想要恢复它们，则单击**恢复**。

注释 还可以从 Cisco Unified Communications Manager 或使用 CLI 从 IM and Presence Service 中启动这些操作。 有关详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面指南》。

注释 如果其中一个节点处于故障转移状态，您就不能将最终用户添加到 IM and Presence Service 群集。

节点状态定义

表 ***4: Presence*** 冗余组节点状态定义

状态	说明
正在初始化	这是 Cisco 服务器恢复管理器服务启动时的初始（过渡）状态；是一个临时状态。
空闲	进行故障转移并且停止服务时，IM and Presence Service 于空闲状态。 在空闲状态下，IM and Presence Service 点不会提供任何可用性或即时消息服务。 在空闲状态下，可以使用 **Cisco Unified CM 管理**用户界面手动启动对此节点的回退。
正常	这是一个稳定的状态。 IM and Presence Service 节点正常运行。 在此状态下，可以使用 **Cisco Unified CM 管理**用户界面手动启动对此节点的故障转移。
正在备份模式下运行	这是一个稳定的状态。 IM and Presence Service 节点充当其对等节点的备份。 用户已移至此（备份）节点。
正在接管	这是一个过渡状态。 IM and Presence Service 节点接管其对等节点。
正在进行故障转移	这是一个过渡状态。 IM and Presence Service 节点由其对等节点接管。
已执行故障转移	这是一个稳定的状态。 IM and Presence Service 节点已故障转移，但关键服务没有关闭。 在此状态下，可以使用 **Cisco Unified CM 管理**用户界面手动启动对此节点的回退。
已执行故障转移，且关键服务没有运行	这是一个稳定的状态。 IM and Presence Service 节点上的一些关键服务已停止或发生故障。
正在回退	这是一个过渡状态。 系统从在备份模式下运行的节点回退到此 IM and Presence Service 节点。

状态	说明
正在收回	这是一个过渡状态。 从其对等节点接管发生故障的 IM and Presence Service 节点。
正在故障模式下运行	过渡状态或“在备份模式下运行”状态期间发生错误。
未知	节点状态未知。 可能的原因是 IM and Presence Service 节点上没有正确启用高可用性。 重新启动 Presence 冗余组中两个节点上的服务器恢复管理器服务。

节点状态、原因和建议的操作

使用 **Cisco Unified CM 管理**用户界面选择一个 Presence 冗余组后，您可以在 **Presence 冗余组配置**窗口中查看该组中节点的状态。

表 ***5: Presence*** 冗余组节点高可用性状态、原因和建议的操作

节点 1		节点 2		
状态	原因	状态	原因	原因/建议的操作
正常	正常	正常	正常	正常
正在进行故障转移	应管理员的请求	正在接管	应管理员的请求	管理员启动从节点 1 到节点 2 的手动故障转移。手动故障转移正在进行中。
空闲	应管理员的请求	正在备份模式下运行	应管理员的请求	管理员启动的、从节点 1 到节点 2 的手动故障转移已完成。
正在收回	应管理员的请求	正在回退	应管理员的请求	管理员启动从节点 2 到节点 1 的手动回退。手动回退正在进行中。
空闲	初始化	正在备份模式下运行	应管理员的请求	管理员当节点 1 处于“空闲”状态时重新启动节点 1 上的 SRM 服务。
空闲	初始化	正在备份模式下运行	初始化	当 Presence 冗余组处于手动故障转移模式时，管理员重新启动 Presence 冗余组中的两个节点，或重新启动两个节点上的 SRM 服务。
空闲	应管理员的请求	正在备份模式下运行	初始化	当节点 2 在备份模式下运行，但节点 1 上的心跳超时之前，管理员重新启动节点 2 上的 SRM 服务。
正在进行故障转移	应管理员的请求	正在接管	初始化	当节点 2 接管，但节点 1 上的心跳超时之前，管理员重新启动节点 2 上的 SRM 服务。

节点 1		节点 2		
状态	原因	状态	原因	原因/建议的操作
正在收回	初始化	正在回退	应管理员的请求	当取回但节点 2 上的心跳超时之前，管理员重新启动节点 1 上的 SRM 服务。 取回过程完成后，两个节点都处于“普通”状态。
正在收回	自动回退	正在回退	自动回退	从节点 2 到节点 1 的自动回退已启动并且当前正在进行。
已执行故障转移	初始化或关键服务关闭	正在备份模式下运行	关键服务关闭	节点 1 在出现以下任一情况时转换为“已故障转移”状态： • 关键服务由于节点 1 重新启动恢复运行。 • 当节点 1 处于“关键服务未运行时故障转移”状态时，管理员启动节点 1 上的关键服务。 节点 1 转换为“已故障转移”状态后，该节点已准备就绪，管理员可执行手动回退，以将 Presence 冗余组中的节点恢复为“普通”状态。
已执行故障转移，且关键服务没有运行	关键服务关闭	正在备份模式下运行	关键服务关闭	节点 1 上的关键服务已关闭。IM and Presence Service 会执行到节点 2 的自动故障转移。 **建议的操作：** **1.** 检查节点 1 有无任何关键服务关闭，并尝试手动启动这些服务。 **2.** 如果节点 1 上的关键服务没有启动，则重新启动节点 1。 **3.** 当所有关键服务均已启动并在重新启动后运行时，执行手动回退以将 Presence 冗余组中的节点恢复为“普通”状态。
已执行故障转移，且关键服务没有运行	数据库失败	正在备份模式下运行	数据库失败	节点 1 上的数据库服务已关闭。IM and Presence Service 会执行到节点 2 的自动故障转移。 **建议的操作：** **1.** 重新启动节点 1。 **2.** 当所有关键服务均已启动并在重新启动后运行时，执行手动回退以将 Presence 冗余组中的节点恢复为“普通”状态。

节点 1		节点 2		
状态	原因	状态	原因	原因/建议的操作
正在故障模式下运行	启动关键服务失败	正在故障模式下运行	启动关键服务失败	Presence 冗余组中的节点从其他节点收回时关键服务无法启动。 **建议的操作**。在收回的节点上，执行以下操作： **1.** 检查该节点有无关键服务关闭。 要手动启动这些服务，单击 **Presence 冗余组配置**窗口中的**恢复**。 **2.** 如果关键服务没有启动，重新启动该节点。 **3.** 当所有关键服务均已启动并在重新启动后运行时，执行手动回退以将 Presence 冗余组中的节点恢复为“普通”状态。
正在故障模式下运行	关键服务关闭	正在故障模式下运行	关键服务关闭	关键服务在备份节点上关闭。 两个节点都进入故障状态。 **建议的操作**： **1.** 检查备份节点有无关键服务关闭。 要手动启动这些服务，单击 **Presence 冗余组配置**窗口中的**恢复**。 **2.** 如果关键服务没有启动，重新启动该节点。
节点 1 由于失去网络连接而关闭，或SRM服务没有运行。		正在备份模式下运行	对等节点关闭	节点 2 失去来自节点 1 的心跳。IM and Presence Service 会执行到节点 2 的自动故障转移。 **建议的操作**。 如果节点 1 已启动，则执行以下操作： **1.** 检查并修复 Presence 冗余组中节点之间的网络连接性。 当您重新建立节点之间的网络连接后，节点可能会进入故障状态。 单击 **Presence 冗余组**配置窗口中的**恢复**以将节点恢复为“普通”状态。 **2.** 启动 SRM 服务并执行手动回退以将 Presence 冗余组中的节点恢复为“普通”状态。 **3.** （如果节点关闭）修复节点 1 并通电。 **4.** 当节点已启动并且所有关键服务均已运行时，执行手动回退以将 Presence 冗余组中的节点恢复为“普通”状态。

节点 1		节点 2		
状态	原因	状态	原因	原因/建议的操作
节点 1 已关闭（由于可能的电源中断、硬件故障、关闭、重新启动）		正在备份模式下运行	对等节点重新启动	由于节点 1 上出现以下可能的情况，IM and Presence Service 执行到节点 2 的自动故障转移： • 硬件故障 • 电源中断 • 重新启动 • shutdown **建议的操作：** **1.** 修复节点 1 并通电。 **2.** 当节点已启动并且所有关键服务均已运行时，执行手动回退以将 Presence 冗余组中的节点恢复为“普通”状态。
“关键服务未运行时故障转移”或“已故障转移”	初始化	备份模式	初始化期间对等节点关闭	节点 2 在启动期间不会看到节点 1。 **建议的操作：** 当节点 1 已启动并且所有关键服务均已运行时，执行手动回退以将 Presence 冗余组中的节点恢复为“普通”状态。
正在故障模式下运行	Cisco 服务器恢复管理器接管用户失败	正在故障模式下运行	Cisco 服务器恢复管理器接管用户失败	用户在接管过程中失败。 **建议的操作：** 可能的数据库错误。 单击 **Presence 冗余组配置**窗口中的**恢复**。 如果问题仍然存在，则重新启动节点。
正在故障模式下运行	Cisco 服务器恢复管理器取回用户失败	正在故障模式下运行	Cisco 服务器恢复管理器取回用户失败	用户在回退过程中失败。 **建议的操作：** 可能的数据库错误。 单击 **Presence 冗余组配置**窗口中的**恢复**。 如果问题仍然存在，则重新启动节点。
正在故障模式下运行	未知	正在故障模式下运行	未知	当其他节点上的 SRM 处于故障状态，或发生内部系统错误时，节点上的 SRM 会重新启动。 **建议的操作：** 单击 **Presence 冗余组配置**窗口中的**恢复**。 如果问题仍然存在，则重新启动节点。

节点 1		节点 2		
状态	原因	状态	原因	原因/建议的操作
备份已激活	自动恢复数据库失败	故障转移受影响的服务	自动恢复数据库失败。	数据库在备份节点上关闭。 对等节点处于故障转移模式并且能够接管 Presence 冗余组中的所有用户。 自动进行自动恢复操作并且所有用户均移至主节点。
备份已激活	自动恢复数据库失败	故障转移受影响的服务	自动恢复关键服务关闭	关键服务在备份节点上关闭。 对等节点处于故障转移模式并且能够接管 Presence 冗余组中的所有用户。 自动进行自动恢复操作并且所有用户均移至对等节点。
未知		未知		节点状态未知。 可能的原因是 IM and Presence Service 节点上没有正确启用高可用性。 **建议的操作：** 重新启动 Presence 冗余组中两个节点上的服务器恢复管理器服务。

IM and Presence 故障转移增强，停机时间几乎为零

IM and Presence Service 得到增强，可减少节点和群集升级及故障转移过程中的影响，从而最大限度地缩短 Jabber 服务中断的时间。

在版本 14 中，IM and Presence Service 服务支持与 Jabber 客户端的双连接。在客户端启用后，此类连接在高可用性故障转移事件期间可确保缩短服务停机时间（至接近零）。

它有助于：

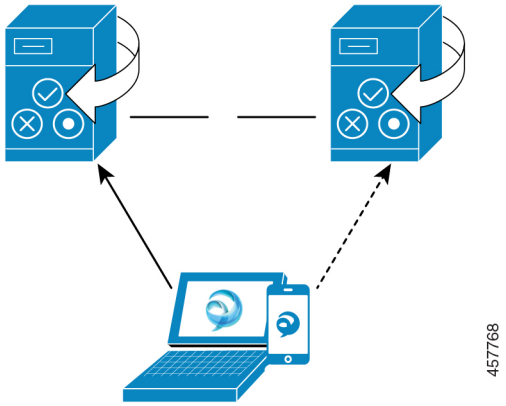
- 在 IM and Presence Service 直接标准升级期间，最大程度减少 Jabber 客户端的服务中断
- 在主节点和辅助节点之间无缝切换用户会话

您可以在 Jabber 客户端中通过一些其他配置来启用此功能。有关如何在 Jabber 中启用双重连接的详细信息，请参阅《Cisco Jabber 14 参数参考指南》中的 *EnableDualConnections* 和 *Inactive_Connection_Activation_Timer* 参数。

要尽可能缩短停机时间，请确保满足以下前提条件以启用此功能增强：

- 在升级过程中保持启用高可用性 (HA)。
- 版本兼容性：Cisco Unified CM 和 IM and Presence 版本 14、Jabber 版本 14 和 Expressway 14（如果是移动和远程访问用户）。

图 *2: IM Presence* 故障转移增强



如果发生故障转移，此增强有助于尽量缩短停机时间至将近零。这是通过启用 Cisco Jabber 客户端以维护与 IM and Presence 节点的双连接来实现的。与在客户端登录过程中创建的主节点保持活动连接。在客户端重新登录下限和客户端重新登录上限值之间的随机秒数后，与备份节点之间的非活动连接将建立。这些限制配置为 Cisco Server Recovery Manager 服务的服务参数。

发生故障转移时，Jabber 客户端将激活“非活动”连接以与服务器通信。由于已在备份节点上创建非活动连接，因此 Jabber 停机时间可缩至最短。

注释 由于 Cisco Jabber 客户端的限制，这种（适用于 Jabber 的）故障转移增强功能不能与 IM and Presence Service 无限制 (XU) 版配合使用。这是因为在无限制版中禁用了 XMPP 客户端（例如 Jabber）与 IM and Presence 服务之间的安全 TLS 连接。

在受限版本中，**启用 XMPP 客户端 IM/P 服务安全模式**选项在**安全设置**页（**系统** > **安全** > **设置**）中默认启用，从而令故障转移增强功能可以与 Jabber 配合使用。如果您要使用故障转移增强功能，我们建议不要禁用此模式。有关此限制的详细信息，请参阅 CSCvx94284。

如何检查是否已建立双重注册

为确保建立双重注册，请考虑在主节点上分配 X 个用户，在辅助节点上分配 Y 个用户的方案。当您检查主节点上的 *JsmSessionsClient* 和 *JsmSessionsClientInactive* 计数器时，可以看到连接至 *JsmSessionsClient* 和 *JsmSessionsClientInactive* 的用户总数分别是 X 和 Y。与此同时，在辅助接点上，连接至 *JsmSessionsClient* 和 *JsmSessionsClientInactive* 的用户总数分别是 Y 和 X。

如何禁用双重注册

您可以禁用双重注册，方法是在客户端禁用 HA，无需在服务器中禁用 HA。此外，如果禁用 HA，则不会从服务器向客户端提供双重注册，并且客户端无法尝试建立非活动连接。有关如何在 Jabber 中启用双重连接的详细信息，请参阅《Cisco Jabber 14 参数参考指南》中的 *EnableDualConnections* 和 *Inactive_Connection_Activation_Timer* 参数。

在升级期间用于监控零停机时间的计数器

要跟踪升级过程以确保零停机时间，您可以通过实时监控工具监控以下计数器：

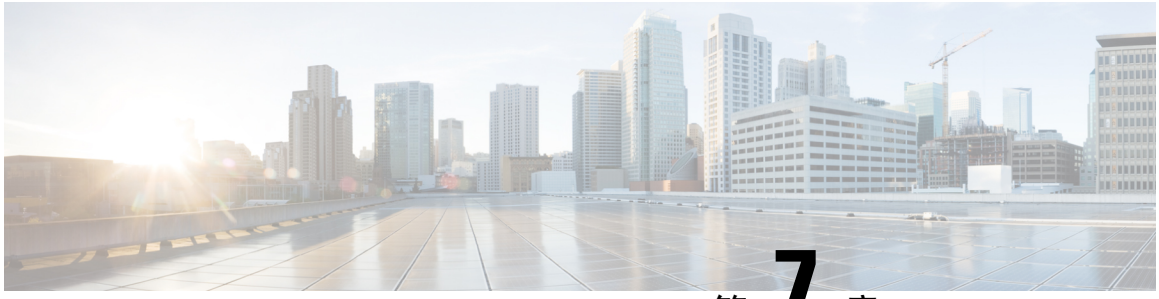
表 *6:* 在升级期间用于监控零停机时间的计数器

计数器	说明
ActiveJsmSessions	此计数器提供分配给发布方节点的活动用户数。在故障转移过程中，它会显示主（升级）节点为零，并将活动用户从主节点添加到备份节点。
InactiveJsmSessions	此计数器提供分配给订阅方节点的活动用户数。
JsmSessionsComposed	此计数器表示JSM处于活动状态的组合会话数。
JsmSessionsClientInactive	此计数器表示JSM处于非活动状态的客户端会话数。
JsmSessionsClient	此计数器表示 JSM 处于活动状态的客户端会话数。
JsmSessionsClientInactive	此计数器表示JSM处于非活动状态的客户端会话数。

冗余相互作用和限制

功能	互动
添加用户	如果其中一个群集节点处于故障转移状态，您就不能将新用户添加到 IM and Presence Service 群集。
多设备消息传送	如果发生故障转移，多设备消息传送功能会导致 IM and Presence Service 上的服务器恢复延迟。 如果配置了多设备消息传送的系统上发生服务器故障转移，则故障转移时间通常是使用 **Cisco Server Recovery** Manager 服务参数指定的时间的两倍。

功能	互动
推送通知高可用性	从 11.5(1)SU3 开始，推送通知部署支持高可用性。 如果启用了推送通知，并且节点进行了故障转移，则 iPhone 和 iPad 客户端上的 Cisco Jabber 会出现以下问题： • 对于处于前台模式的 Cisco Jabber 客户端，Jabber 客户端会自动登录到备份节点，该节点将在主节点恢复之前接管。 无论是备份节点接管还是主节点恢复时，服务都不会中断。 • 对于处于后台模式的 Cisco Jabber 客户端，备份节点将接管，但在发送推送通知之前会有一段延迟。 由于 Jabber 客户端处于后台模式，没有活动的网络连接，因此不会自动登录到备份节点。 在发送任何推送通知之前，备份节点必须为处于后台模式的所有故障转移的用户重新创建 JSM 会话。 延迟的时长取决于系统负载。 测试表明，对于含 15,000 个用户的 OVA（用户均匀分布在 HA 对中），故障转移后发送推送通知需要 10-20 分钟。 当备份节点接管时以及主节点恢复后，会再次出现此延迟。 **注释** 如果节点发生故障或 Cisco XCP 路由器意外崩溃，无需用户执行任何操作，系统即会维护用户的 IM 会话（包括 IM 历史记录）。 但是，如果 iPhone 或 iPad 客户端上的 Cisco Jabber 处于挂起模式，则无法检索服务器崩溃时在其上排队的未读消息。
用户的临时在线状态	在故障转移、回退和用户移动后，用户的临时在线状态会显示过期的在线状态。 这是因为对临时在线状态的订阅将会删除，用户必须重新订阅临时在线状态，才能看到用户的有效临时在线状态。 例如，如果用户 A 订阅用户 B 的临时在线状态，并且用户 B 被分配到的 IM and Presence 节点上发生故障转移，则即使用户 B 重新登录到备份节点后，用户 B 仍会对用户 A 显示离线。 这是因为对用户 B 临时在线状态的订阅删除，而用户 A 对此不知情。 用户 A 必须重新订阅用户 B 的临时在线状态。 当用户 A 从 Jabber 客户端删除用户 B 的搜索时，用户 A 至少需要等待 30 秒，然后才会尝试搜索用户 B 的临时在线状态。如果不是，用户 A 会看到用户 B 过期的在先状态。对于同一用户，Jabber 客户端必须在两次搜索之间至少等待 30 秒，才能获得有效的临时在线状态。
IM and Presence 状态	当用户从一个 Presence 冗余组移动到另一个 Presence 冗余组时，用户必须从 Jabber 会话注销，以便 IM and Presence 状态在用户已移入的当前 Presence 冗余组中可见。



第 7 章

配置用户设置

- 最终用户设置概述， 第 65 页
- 用户设置前提条件， 第 66 页
- 配置用户设置任务流程， 第 66 页

最终用户设置概述

您可以使用服务配置文件和功能组模板等用户设置，通过 LDAP 目录同步将常用设置应用于最终用户。 进行 LDAP 目录同步时，配置的设置将应用于所有同步用户。

注释 本章详细介绍了适用于 IM and Presence Service 的用户设置。 关于常规 UC 用户配置，包括语音邮件和会议等 UC 服务，请参阅《*Cisco Unified Communications Manager* 系统配置指南》的“配置最终用户”部分。 您可以将这些配置作为 LDAP 同步的一部分应用。

服务配置文件

服务配置文件中包含通用 Unified Communications (UC) 服务设置。您可以为不同的用户组配置不同的服务配置文件，以便每组用户都有针对其工作配置的相应服务。为了让最终用户可以访问 IM and Presence Service，请配置服务配置文件，使其包含 IM and Presence Service。

您可以使用以下方法将服务配置文件应用到最终用户：

- 对于 LDAP 同步用户 — 如果已从 LDAP 目录导入最终用户，可以将服务配置文件分配给功能组模板，然后将该功能组模板应用到最终用户。模板中的设置会应用到所有同步用户。
- 对于活动本地用户（即非 LDAP 用户）— 要将设置一次性应用于大量用户，使用批量管理工具通过 csv 文件或电子表格应用服务配置文件设置。有关如何使用批量管理工具的详细信息，请访问 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

  或者，您也可以逐个用户地手动配置用户设置。

功能组模板概述

功能组模板可帮助您通过 LDAP 目录同步，快速将常用设置应用于最终用户组。 例如，您可以使用功能组模板为最终用户启用 IM and Presence Service。 这可以通过将支持 IM and Presence 的服务配置文件应用到模板来实现。 如果要将功能组模板应用到 LDAP 目录同步，当同步发生时，模板中的设置（包括配置的服务配置文件和用户配置文件设置）将应用到所有同步的用户。

功能组模板配置包括可以分配给功能组模板的以下配置文件：

- 用户配置文件 — 包含一组通用的电话和电话线路设置。 您必须使用通用线路模板（分配通用电话线路设置）和通用设备模板（分配通用电话设置）配置用户配置文件。 这些模板可帮助设为自我设置的用户配置自己的电话。
- 服务配置文件 — 包含一组通用的 UC 服务，如 IM and Presence Service、目录或语音邮件。

用户设置前提条件

如果您想要在 IM and Presence Service 群集之间移动用户，必须在配置最终用户之前这样做。 关于如何使用 Cisco Unified CM IM and Presence 管理迁移用户以及导入或导出联系人列表的信息，请参阅。

注释 不应将群集之间的用户迁移同用于分区域内联合的用户迁移工具混淆。

注释 如果您已通过 VPN 连接 Cisco Jabber，则在 IM and Presence Service 与 Cisco Jabber 客户端之间进行 TLS 握手期间，IM and Presence 服务器将对客户端的 IP 子网执行反向查找。 如果反向查找失败，TLS 握手会在客户端计算机上超时。

配置用户设置任务流程

完成这些任务可配置含通用服务和功能设置的用户模板，例如为 IM and Presence Service 启用最终用户。 当您完成 LDAP 同步时，您的模板设置会应用到最终用户。

注释 本章的任务流程特别介绍了适用于 IM and Presence Service 的用户设置。 关于常规 UC 用户配置，包括语音邮件和会议等 UC 服务，请参阅《*Cisco Unified Communications Manager* 系统配置指南》的“配置最终用户”部分。 您可以将这些配置作为 LDAP 同步的一部分应用。

过程

	命令或操作	目的
步骤 1	配置用户分配模式， 第 67 页	将用户分配模式设置为平衡、活动-备用或无。
步骤 2	添加 IM and Presence UC 服务， 第 67 页	在 Cisco Unified Communications Manager 上设置 IM and Presence UC 服务。
步骤 3	配置服务配置文件， 第 68 页	配置包含您添加的 IM and Presence UC 服务的服务配置文件。
步骤 4	配置功能组模板， 第 69 页	配置包含您设置的服务配置文件以及其他通用功能设置的功能组模板。

下一步做什么

完成 LDAP 同步以将设置应用于 LDAP 同步用户。

配置用户分配模式

此程序用于配置同步代理将用户分配至群集中节点的方式。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 在**用户管理参数**区域，为 **Presence 服务器的用户分配模式**参数选择以下选项之一：

- **平衡**—此模式会将用户平均分配到每个子群集中的各个节点，并尝试让各个节点上的用户总数达到均衡。 这是默认选项。
- **主用-备用** — 此模式会将所有用户分配至子群集的第一个节点，并让第二个服务器作为备份。
- **无**— 如果选择此模式，同步代理不会将任何用户分配到群集中的节点。

步骤 3 单击**保存**。

下一步做什么

添加 IM and Presence UC 服务， 第 67 页

添加 IM and Presence UC 服务

在 Cisco Unified Communications Manager 中遵照此程序为 IM and Presence Service 添加 UC 服务。

过程

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

步骤 2 单击**新增**。

步骤 3 从 **UC 服务类型**下拉列表框中选择 **IM and Presence**。

步骤 4 从**产品类型**下拉列表框中选择 **Unified CM (IM and Presence)**。

步骤 5 输入 IM and Presence Service 的**名称**和**说明**。

步骤 6 在**主机名/IP 地址**字段中，输入托管 IM and Presence Service 的服务器的主机名、IP 地址或 DNS SRV。

步骤 7 单击**保存**。

下一步做什么

要为 IM and Presence Service 启用用户，先将 UC 服务分配给服务配置文件，然后将该配置文件分配给您的用户。

配置服务配置文件，第 68 页.

配置服务配置文件

此程序用于配置包含 IM and Presence Service 的服务配置文件。

开始之前

添加 IM and Presence UC 服务，第 67 页

过程

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

步骤 2 执行以下任一操作

- 单击**查找**并选择现有配置文件
- 单击**新增**以创建新的配置文件

步骤 3 在 **IM and Presence 配置文件**部分选择**主** IM and Presence 服务器。

步骤 4 完成**服务配置文件配置**窗口中其余字段的设置。 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**。

下一步做什么

配置功能组模板，第 69 页

配置功能组模板

配置包含通用功能设置以及您设置的 IM and Presence Service 配置文件的功能组模板。

开始之前

配置服务配置文件，第 68 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** > **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。

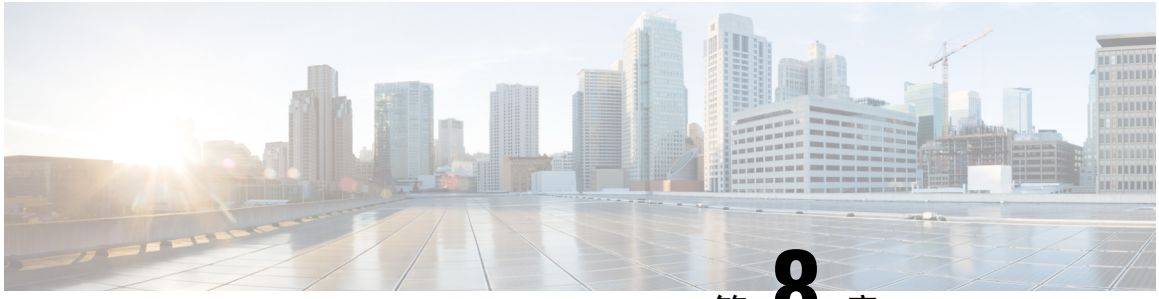
步骤 6 从下拉列表中，选择一个**服务配置文件**和**用户配置文件**。

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

配置包含此功能组模板的 LDAP 目录同步。 当您完成 LDAP 同步时，模板中的 IM and Presence 设置会应用到同步的用户。 请参阅：LDAP 同步配置任务流程，第 73 页。



第 8 章

配置 LDAP 目录

- LDAP 同步概述，第 71 页
- LDAP 同步前提条件，第 72 页
- LDAP 同步配置任务流程，第 73 页

LDAP 同步概述

轻型目录访问协议 (LDAP) 同步可帮助为您的系统设置和配置最终用户。 LDAP 同步期间，系统会将用户和关联的用户数据列表从外部 LDAP 目录导入 Unified Communications Manager 数据库。 您还可以在导入时配置您的最终用户。

注释 Unified Communications Manager 支持 LDAPS（通过 SSL 的 LDAP），但不支持通过 StartTLS 的 LDAP。 确保您将 LDAP 服务器证书作为 Tomcat-Trust 上传到 Unified Communications Manager。

有关受支持的 LDAP 目录的信息，请参阅《*Cisco Unified Communications Manager* 和 *IM and Presence Service* 的兼容性值表》。

LDAP 同步会通告以下功能：

- **导入最终用户**—您可以在初始系统设置期间使用 LDAP 同步将用户列表从公司 LDAP 目录导入 Unified Communications Manager 数据库。 如果您已预先配置了功能组模板、用户配置文件、服务配置文件、通用设备和线路模板等项目，可以将配置应用到您的用户，并在同步过程中分配配置的目录号码和目录 URI。 LDAP 同步过程将导入用户和用户特定数据列表，并应用您设置的配置模板。

  注释 一旦发生初始同步，您将无法编辑 LDAP 同步。

- **计划的更新**—您可以将 Unified Communications Manager 配置为按计划的时间间隔与多个 LDAP 目录同步，以确保定期更新数据库且用户数据为最新。

- **验证最终用户**—您可以将系统配置为针对 LDAP 目录而不是 Cisco Unified Communications Manager 数据库验证最终用户密码。 LDAP 验证使得公司能够为最终用户分配一个适用于所有公司应用程序的密码。 此功能不适用于 PIN 或应用程序用户密码。
- **针对思科移动和远程访问客户端及终端的目录服务器用户搜索**—即使在企业防火墙外部运行，您也可以搜索公司目录服务器。 启用此功能后，用户数据服务 (UDS) 将充当代理，并将用户搜索请求发送到公司目录，而不是发送到 Unified Communications Manager 数据库。

最终用户的 LDAP 验证

通过 LDAP 同步，您可以将系统配置为针对 LDAP 目录而不是 Cisco Unified Communications Manager 数据库验证最终用户密码。 LDAP 验证使得公司能够为最终用户分配一个适用于所有公司应用程序的密码。 此功能不适用于 PIN 或应用程序用户密码。

目录服务器用户搜索思科移动和远程访问客户端及终端

在以前的版本中，当具有思科移动和远程访问客户端（如 Cisco Jabber）或终端（如 Cisco DX 80 电话）的用户在企业防火墙外部执行用户搜索时，结果基于存储在 Cisco Unified Communications Manager 数据库中的用户帐户。 数据库包含本地配置或从公司目录同步的用户帐户。

在此版本中，即使在企业防火墙外部运行，思科移动和远程访问客户端及终端现在也可以搜索公司目录服务器。 启用此功能后，用户数据服务 (UDS) 将充当代理，并将用户搜索请求发送到公司目录，而不是发送到 Cisco Unified Communications Manager 数据库。

可通过此功能实现以下结果：

- 无论地理位置如何，都提供相同的用户搜索结果—移动和远程访问客户端及终端可以使用公司目录执行用户搜索；即使它们在企业防火墙之外连接也不例外。
- 减少 Cisco Unified Communications Manager 数据库中配置的用户帐户数量 — 移动客户端现在可以搜索公司目录中的用户。 在以前的版本中，用户搜索结果基于数据库中配置的用户。 现在，管理员不再需要仅为用户搜索而将用户帐户配置或同步到数据库。 管理员只需配置由群集提供服务的用户帐户。 减少数据库中的用户帐户总数可缩短软件升级所需的时长，同时提高数据库的整体性能。

要配置此功能，您必须启用 **LDAP 搜索配置**窗口的**启用用户搜索企业目录服务器**，并配置 LDAP 目录服务器的详细信息。 有关详细信息，请参阅配置企业目录用户搜索，第 77 页程序。

LDAP 同步前提条件

先决任务

从 LDAP 目录导入最终用户之前，请完成以下任务：

- 配置用户访问权限

- 配置凭证策略
- 配置功能组模板

对于您希望将其数据同步到您的系统的用户，请确保他们在 Active Directory 服务器上的电子邮件 ID 字段是唯一的条目或留空。

LDAP 同步配置任务流程

执行以下任务以从外部 LDAP 目录提取用户列表并将其导入 Cisco Unified Communications Manager 数据库。

注释 如果您已同步 LDAP 目录一次，仍可以从外部 LDAP 目录同步新项目，但无法在 Cisco Unified Communications Manager 中将新配置添加到 LDAP 目录同步。 在这种情况下，您可以使用批量管理工具和菜单，例如“更新用户”或“插入用户”。 请参阅《*Cisco Unified Communications Manager* 批量管理指南》。

过程

	命令或操作	目的
步骤 1	激活 Cisco DirSync 服务， 第 74 页	登录到 Cisco Unified 功能配置并激活 Cisco DirSync 服务。
步骤 2	启用 LDAP 目录同步， 第 74 页	在 Unified Communications Manager 中启用 LDAP 目录同步。
步骤 3	创建 LDAP 过滤器， 第 74 页	**可选**。 如果希望 Unified Communications Manager 只同步公司 LDAP 目录中的一部分用户，请创建 LDAP 过滤器。
步骤 4	配置 LDAP 目录同步， 第 75 页	配置 LDAP 目录同步的设置，例如字段设置、LDAP 服务器位置、同步计划以及访问控制组、功能组模板和主分机的分配。
步骤 5	配置企业目录用户搜索， 第 77 页	**可选**。 配置系统以用于企业目录服务器用户搜索。 请遵照此程序配置系统中的电话和客户端，以对企业目录服务器而不是数据库执行用户搜索。
步骤 6	配置 LDAP 验证， 第 79 页	**可选**。 如果要使用 LDAP 目录进行最终用户密码验证，请配置 LDAP 验证设置。
步骤 7	自定义 LDAP 协议服务参数， 第 79 页	**可选**。 配置可选的 LDAP 同步服务参数。 对于大多数部署而言，默认值已足够。

激活 Cisco DirSync 服务

执行以下程序可在 Cisco Unified 功能配置中激活 Cisco DirSync 服务。 如果要同步公司 LDAP 目录中的最终用户设置，必须激活此服务。

过程

步骤 1 从 Cisco Unified 功能配置中，选择**工具** > **服务激活**。

步骤 2 从**服务器**下拉列表中，选择发布方节点。

步骤 3 在**目录服务**下，单击 **Cisco DirSync** 单选按键。

步骤 4 单击**保存**。

启用 LDAP 目录同步

如果要将 Unified Communications Manager 配置为从公司 LDAP 目录同步最终用户设置，请执行此程序。

注释 如果您已同步 LDAP 目录一次，仍可以从外部 LDAP 目录同步新用户，但无法在 Unified Communications Manager 中将新配置添加到 LDAP 目录同步。 您还不能向基础配置项目（如功能组模板或用户配置文件）添加编辑。 如果已经完成一个 LDAP 同步，并且想要添加具有不同设置的用户，则可以使用批量管理菜单，例如“更新用户”或“插入用户”。

过程

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

步骤 2 如果您希望 Unified Communications Manager 从 LDAP 目录导入用户，选中**从 LDAP 服务器启用同步**复选框。

步骤 3 从 **LDAP 服务器类型**下拉列表中，选择您公司使用的 LDAP 目录服务器类型。

步骤 4 在**用户 ID 的 LDAP 属性**下拉列表中，选择您希望 Unified Communications Manager 为**最终用户配置**窗口中的**用户 ID** 字段同步的公司 LDAP 目录属性。

步骤 5 单击**保存**。

创建 LDAP 过滤器

您可以创建 LDAP 过滤器以将 LDAP 同步范围限制为 LDAP 目录中的部分用户。 将 LDAP 过滤器应用于 LDAP 目录时，Unified Communications Manager 只会导入 LDAP 目录中与过滤器匹配的用户。

注释 您配置的 LDAP 过滤器必须符合 RFC4515 中规定的 LDAP 搜索过滤器标准。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**系统** > **LDAP** > **LDAP 过滤器**。

步骤 2 单击**新增**以创建新的 LDAP 过滤器。

步骤 3 在**过滤器名称**文本框中，输入您的 LDAP 过滤器的名称。

步骤 4 在**过滤器**文本框中，输入过滤器。 过滤器最多可包含 1024 个 UTF-8 字符，且必须括在括号中 ()。

步骤 5 单击**保存**。

配置 LDAP 目录同步

此程序用于将 Unified Communications Manager 配置为与 LDAP 目录同步。 通过 LDAP 目录同步，您可以将最终用户数据从外部 LDAP 目录导入 Unified Communications Manager 数据库，以便其显示在“最终用户配置”窗口中。 如果您具有带通用线路和设备模板的设置功能组模板，可以将设置自动分配给新预配置的用户及其分机。

提示 如果要分配访问控制组或功能组模板，则可以使用 LDAP 过滤器将导入限制为具有相同配置要求的用户组。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统** > **LDAP** > **LDAP 目录**。

步骤 2 请执行以下步骤之一：

- 单击**查找**并选择现有的 LDAP 目录。
- 单击**新增**以创建新的 LDAP 目录。

步骤 3 在 **LDAP 目录配置**窗口中，输入以下内容：

a) 在 **LDAP 配置名称**字段中，为 LDAP 目录分配唯一的名称。

b) 在 **LDAP 管理员判别名**字段中，输入具有 LDAP 目录服务器访问权限的用户 ID。

c) 输入并确认密码详细信息。

d) 在 **LDAP 用户搜索空间**字段中，输入搜索空间详细信息。

e) 在**用户同步的 LDAP 自定义过滤器**字段中，选择**仅限用户**或者**用户和组**。

f) （可选）。 如果要将导入限制为满足特定配置文件的部分用户，请从**适用于组的 LDAP 自定义过滤器**下拉列表中选择 LDAP 过滤器。

步骤 4 在 **LDAP 目录同步计划**字段中，创建 Unified Communications Manager 用于同外部 LDAP 目录同步数据的计划。

步骤 5 填写**要同步的标准用户字段**部分。 对于每个最终用户字段，选择 LDAP 属性。 同步过程会将 LDAP 属性的值分配给 Unified Communications Manager 中的最终用户字段。

步骤 6 如果您正在部署 URI 拨号，请确保分配用于用户主目录 URI 地址的 LDAP 属性。

步骤 7 在**要同步的自定义用户字段**部分，输入具有所需 LDAP 属性的自定义用户字段名称。

步骤 8 要将导入的最终用户分配给所有导入的最终用户通用的访问控制组，请执行以下操作：

a) 单击**添加到访问控制组**。

b) 在弹出窗口中，单击要分配给所导入最终用户的每个访问控制组对应的复选框。

c) 单击**添加选定项**。

步骤 9 如果要分配功能组模板，从**功能组模板**下拉列表中选择模板。

注释 只有在最终用户第一次未显示时，才会将用户与所分配的**功能组模板**同步。 如果现有**功能组模板**被修改且为关联的 LDAP 执行了完全同步，则修改内容不会更新。

步骤 10 如果要对导入的电话号码应用掩码以分配主分机，请执行以下操作：

a) 选中**应用掩码到同步的电话号码以为插入的用户创建新线路**复选框。

b) 输入**掩码**。 例如，如果导入的电话号码是 8889945，则掩码 11XX 会创建一个主分机 1145。

步骤 11 如果要从目录号池分配主分机，请执行以下操作：

a) 选中**如果未根据同步的 LDAP 电话号码创建新线路，请从池列表分配一条新线路**复选框。

b) 在 **DN 池开始**和 **DN 池结束**文本框中，输入要从中选择主分机的目录号码范围。

步骤 12 （可选）如果要创建 Jabber 设备，请在“Jabber 终端预配置”部分中，从下列下拉列表中选择一个所需的 Jabber 设备进行自动预配置：

- 适用于 Android 的 Cisco 双模 (BOT)
- Cisco Dual Mode for iPhone (TCT)
- Cisco Jabber 平板电脑版 (TAB)
- Cisco Unified Client Services Framework (CSF)

注释 **写回到 LDAP** 选项可让您将选中的主目录号码从 Unified CM 写回到 LDAP 服务器。 可用于写回的 LDAP 属性包括：**telephoneNumber**、**ipPhone** 和 **mobile**。

步骤 13 在 **LDAP 服务器信息**部分，输入 LDAP 服务器的主机名或 IP 地址。

步骤 14 如果想使用 TLS 创建到 LDAP 服务器的安全连接，则选中**使用 TLS** 复选框。

注释 有时，当我们在重启 tomcat 后尝试通过安全端口同步用户时，用户无法同步。 您必须重新启动 Cisco DirSync 服务才能成功同步用户。

步骤 15 单击**保存**。

步骤 16 要完成 LDAP 同步，请单击**立即执行完全同步**。 否则，您可以等待预定的同步。

注释 在 LDAP 中删除用户时，他们会在 24 小时后自动从 Unified Communications Manager 中删除。 此外，如果为以下任何设备将已删除用户配置为移动用户，则这些非活动的设备也将自动删除：

- 远程目标配置文件
- 远程目标配置文件模板
- 移动智能客户端
- CTI 远程设备
- Spark 远程设备
- Nokia S60
- Cisco Dual Mode for iPhone
- IMS 集成移动 (基本)
- 运营商集成的移动
- 适用于 Android 的 Cisco 双模

配置企业目录用户搜索

此程序用于配置系统中的电话和客户端，以对企业目录服务器而不是数据库执行用户搜索。

开始之前

- 确保您选择用于 LDAP 用户搜索的主、辅和第三服务器均可通过网络连接到 Unified Communications Manager 订阅方节点。
- 依次选择**系统** > **LDAP** > **LDAP 系统**，从 **LDAP 系统配置**窗口的**LDAP 服务器类型**下拉列表配置 LDAP 服务器的类型。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**系统** > **LDAP** > **LDAP 搜索**。

步骤 2 要使用企业 LDAP 目录服务器执行用户搜索，选中**启用企业目录服务器用户搜索**复选框。

步骤 3 配置 **LDAP 搜索配置**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**。

注释 要在 OpenLDAP 服务器中搜索表示为会议室对象的会议室，请将自定义过滤器配置为 (|(objectClass=intOrgPerson)(objectClass=rooms))。 这将允许 Cisco Jabber 客户端按名称搜索会议室并拨打与聊天室关联的号码。

如果 OpenLDAP 服务器中针对会议室对象配置了 **givenName**、**sn**、**mail**、**displayName** 或 **telephonenumber** 属性，会议室将可搜索。

目录服务器 UDS 搜索的 LDAP 属性

下表列出了**启用企业目录服务器用户搜索**选项启用时，UDS 用户搜索请求使用的 LDAP 属性。 对于这些类型的目录请求，UDS 充当代理并将搜索请求中继到公司目录服务器。

注释 UDS 用户响应标记可以映射到其中一个 LDAP 属性。 属性映射取决于您从 **LDAP 服务器类型**下拉列表中选择的选项。 从**系统** > **LDAP** > **LDAP 系统配置**窗口访问此下拉列表。

UDS 用户响应标记	LDAP 属性
userName	• samAccountName • uid
firstName	givenName
lastName	sn
middleName	• initials • middleName
nickName	nickName
displayName	displayName
phoneNumber	• telephonenumber • ipPhone
homeNumber	homephone
mobileNumber	mobile
email	mail
directoryUri	• msRTCSIP-primaryuseraddress • mail

UDS 用户响应标记	LDAP 属性
department	• department • departmentNumber
manager	manager
title	title
pager	pager

配置 LDAP 验证

如果要启用 LDAP 验证，请执行此程序，以便根据公司 LDAP 目录中分配的密码对最终用户密码进行验证。 此配置仅适用于最终用户密码，不适用于最终用户 PIN 或应用程序用户密码。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**系统** > **LDAP** > **LDAP 验证**。

步骤 2 选中**对最终用户使用 LDAP 验证**复选框以使用 LDAP 目录进行用户验证。

步骤 3 在 **LDAP 管理员判别名**字段中，输入具有 LDAP 目录访问权限的 LDAP 管理员的用户 ID。

步骤 4 在**确认密码**字段中，输入 LDAP 管理器的密码。

步骤 5 在 **LDAP 用户搜索库**字段中，输入搜索条件。

步骤 6 在 **LDAP 服务器信息**部分，输入 LDAP 服务器的主机名或 IP 地址。

步骤 7 如果想使用 TLS 创建到 LDAP 服务器的安全连接，则选中**使用 TLS** 复选框。

步骤 8 单击**保存**。

下一步做什么

自定义 LDAP 协议服务参数，第 79 页

自定义 LDAP 协议服务参数

执行此程序可配置自定义 LDAP 协议的系统级设置的可选服务参数。 如果不配置这些服务参数，Unified Communications Manager 将应用 LDAP 目录集成的默认设置。 对于参数说明，在用户界面中单击参数名称。

您可以使用服务参数自定义以下设置：

- **协议的最大数**—默认值为 20。
- **主机的最大数**—默认值为 3。

- **主机出现故障时的重试延迟（秒）**—主机故障的默认值为 5。
- **HotList 出现故障时的重试延迟（分钟）**—hostlist 故障的默认值为 10。
- **LDAP 连接超时（秒）**—默认值为 5。
- **延迟同步开始时间（分钟）**—默认值为 5。
- **用户客户映射审核时间**

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，选择发布方节点。
步骤 3 从**服务**下拉列表框选择 **Cisco DirSync**。
步骤 4 配置 Cisco DirSync 服务参数的值。
步骤 5 单击**保存**。

LDAP 目录服务参数

服务参数	说明
协议的最大数	您可以配置的 LDAP 目录最大数。 默认设置为 20。
主机的最大数	您可以出于故障转移目的配置的 LDAP 主机名最大数。 默认值为 3。
主机出现故障时的重试延迟（秒）	主机出现故障后，Cisco Unified Communications Manager 在重试与第一个LDAP服务器（主机名）的连接之前延迟的秒数。 默认值为 5。
主机列表出现故障时的重试延迟（分钟）	主机列表出现故障后，Cisco Unified Communications Manager 在重试每一个配置的LDAP服务器（主机名）之前延迟的分钟数。 默认值为 10。
LDAP 连接超时（秒）	Cisco Unified Communications Manager 允许建立 LDAP 连接的秒数。 如果无法在指定的时间内建立连接，LDAP 服务提供程序将中止连接尝试。 默认值为 5。
延迟同步开始时间（分钟）	Cisco DirSync 服务启动后，Cisco Unified Communications Manager 延迟启动目录同步过程的分钟数。 默认值为 5。

将 LDAP 同步的用户转换为本地用户

将 LDAP 目录与 Cisco Unified Communications Manager 同步时，对于 LDAP 同步的最终用户，除非将 LDAP 同步用户转换为本地用户，否则无法编辑**最终用户配置**窗口中的任何字段。

要在**最终用户配置**窗口中编辑 LDAP 同步字段，请将用户转换为本地用户。 不过，如果执行此转换，当 Cisco Unified Communications Manager 与 LDAP 目录同步时，最终用户不会更新。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**最终用户** > **最终用户管理**。

步骤 2 单击**查找**并选择最终用户。

步骤 3 单击**转换为本地用户**按键。

步骤 4 在**最终用户配置**窗口中进行更新。

步骤 5 单击**保存**。

将 LDAP 同步用户分配给访问控制组

执行此程序将 LDAP 同步用户分配给访问控制组。

开始之前

必须配置 Cisco Unified Communications Manager，将最终用户与外部 LDAP 目录同步。

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**并选择配置的 LDAP 目录。

步骤 3 单击**添加到访问控制组**按键。

步骤 4 选择您要应用到此 LDAP 目录中的最终用户的访问控制组。

步骤 5 单击**添加选定项**。

步骤 6 单击**保存**。

步骤 7 单击**执行完全同步**。

Cisco Unified Communications Manager 会与外部 LDAP 目录同步，并且同步的用户会插入到正确的访问控制组中。

注释 仅当您第一次添加访问控制组时，同步的用户才会插入到所选的访问组中。 执行完全同步后，您添加到 LDAP 的任何后续组将不会应用到同步的用户。

集成 LDAP 目录以在 XMPP 客户端上搜索联系人

这些主题介绍如何在 IM and Presence Service 上配置 LDAP 设置，以允许第三方 XMPP 客户端的用户从 LDAP 目录搜索和添加联系人。

IM and Presence Service 上的 JDS 组件负责处理第三方 XMPP 客户端与 LDAP 目录的通信。 第三方 XMPP 客户端发送查询到 IM and Presence Service 上的 JDS 组件。 JDS 组件向已配置的 LDAP 服务器发送 LDAP 查询，然后将结果发送回 XMPP 客户端。

您在执行此处介绍的配置之前，请先执行将 XMPP 客户端与 Cisco Unified Communications Manager 和 IM and Presence Service 集成的配置。 请参阅与第三方 XMPP 客户端应用程序集成相关的主题。

图 *3:* 集成 *LDAP* 目录以在 *XMPP* 客户端上搜索联系人的工作流程

下面的工作流程图显示了集成 LDAP 目录以在 XMPP 客户端上搜索联系人的简要步骤。

下表列出了集成 LDAP 目录以在 XMPP 客户端上搜索联系人所需执行的任务。 有关详细的说明，请参阅相关任务。

表 *7:* 集成 *LDAP* 目录以在 *XMPP* 客户端上搜索联系人的任务列表

任务	说明
配置 XMPP 客户端的 LDAP 服务器名称和地址	如果在 LDAP 服务器与 IM and Presence Service 之间启用了 SSL 并且配置了安全连接，请将根 CA 证书作为 xmpp-trust-certificate 上传到 IM and Presence Service。 **提示** 证书中的主题 CN 必须与 LDAP 服务器的 FQDN 匹配。
配置 XMPP 客户端 LDAP 搜索设置	必须指定可让 IM and Presence Service 对第三方 XMPP 客户端成功执行联系人搜索的 LDAP 搜索设置。 您可以指定一个主要 LDAP 服务器以及最多两个备用 LDAP 服务器。 **提示** 也可以打开从 LDAP 服务器检索 vCards 的功能，或者允许 vCards 存储在 IM and Presence Service 的本地数据库中。
打开 Cisco XCP 目录服务	必须打开 XCP 目录服务，以允许第三方 XMPP 客户端的用户从 LDAP 目录搜索和添加联系人。 **提示** 在为第三方 XMPP 客户端配置 LDAP 服务器和 LDAP 搜索设置之前，不要打开 Cisco XCP 目录服务；否则服务将停止运行。

LDAP 帐户锁定问题

如果针对您为第三方 XMPP 客户端配置的 LDAP 服务器输入错误的密码，并在 IM and Presence Service 上重新启动 XCP 服务，JDS 组件将会多次使用该错误密码尝试登录 LDAP 服务器。 如果将 LDAP

服务器配置为在几次尝试失败后锁定帐户，则 LDAP 服务器将在某个时候锁定 JDS 组件。 如果 JDS 组件与其他连接到 LDAP 的应用程序（这些应用程序不一定在 IM and Presence Service 上）使用相同的凭证，这些应用程序也将被 LDAP 锁定。

要解决此问题，请配置一个单独的用户，使其具有与现有 LDAP 用户相同的角色和权限，并仅允许 JDS 以此辅助用户的身份登录。 如果您针对 LDAP 服务器输入错误的密码，LDAP 服务器将只锁定 JDS 组件。

为 XMPP 客户端配置 LDAP 服务器名称和地址

如果选择启用安全套接字层 (SSL)，请在 LDAP 服务器与 IM and Presence Service 之间配置安全连接，并且将根证书机构 (CA) 证书作为 cup-xmpp-trust 证书上传到 IM and Presence Service。 证书中的主题通用名称 (CN) 必须与 LDAP 服务器的完全限定域名 (FQDN) 匹配。

如果您导入证书链（从根节点到信任节点的多个证书），则会导入链中的所有证书，叶节点除外。 例如，如果 CA 对 LDAP 服务器的证书进行签名，则只需导入 CA 证书，无需导入 LDAP 服务器的证书。

即使 IM and Presence Service 与 Cisco Unified Communications Manager 之间的连接是 IPv4，您也可以使用 IPv6 连接到 LDAP 服务器。 当 IPv6 对 IM and Presence Service 节点上的企业参数或 ETH0 禁用时，如果为第三方 XMPP 客户端配置的外部 LDAP 服务器的主机名是可解析的 IPv6 地址，该节点仍可执行内部 DNS 查询并连接到外部 LDAP 服务器。

提示 您可以在 **LDAP 服务器 - 第三方 XMPP 客户端**窗口中为第三方 XMPP 客户端配置外部 LDAP 服务器的主机名。

开始之前

获取 LDAP 目录的主机名或 IP 地址。

如果使用 IPv6 连接到 LDAP 服务器，请先在企业参数及 Eth0 上为每个 IM and Presence Service 节点启用 IPv6，然后再配置 LDAP 服务器。

过程

步骤 1 选择 **Cisco Unified CM IM and Presence 管理** > **应用程序** > **第三方客户端** > **第三方 LDAP 服务器**。

步骤 2 单击**新增**。

步骤 3 输入 LDAP 服务器的 ID。

步骤 4 输入 LDAP 服务器的主机名。

对于 IPv6 连接，可以输入 LDAP 服务器的 IPv6 地址。

步骤 5 在监听 TCP 或 SSL 连接的 LDAP 服务器上指定端口号。

默认端口为 389。如果启用 SSL，请指定端口 636。

步骤 6 指定 LDAP 服务器的用户名和密码。 这些值必须与您在 LDAP 服务器上配置的凭证匹配。

有关此信息，请参阅 LDAP 目录文档或 LDAP 目录配置。

步骤 7 如果要使用 SSL 与 LDAP 服务器通信，请选中**启用 SSL**。

注释 如果启用了 SSL，则输入的**主机名**值可以是 LDAP 服务器的主机名或 FQDN。 使用的值必须与安全证书 **CN** 或 **SAN** 字段中的值相匹配。

如果必须使用 IP 地址，则此值还必须在证书上用于 **CN** 或 **SAN** 字段。

步骤 8 单击**保存**。

步骤 9 在群集中的所有节点上启动 Cisco XCP 路由器服务（如果此服务未运行）。

提示

- 如果启用 SSL，XMPP 搜索联系人的速度可能较慢，因为 IM and Presence Service 建立 SSL 连接后，设置 SSL 连接设置时要进行协商、数据加密和解密。 这样，如果用户在您的部署中广泛执行 XMPP 联系人搜索，将会影响总体系统性能。
- 在上传 LDAP 服务器的证书后，可以使用证书导入工具检查与 LDAP 服务器主机名及端口值的通信。 选择 **Cisco Unified CM IM and Presence 管理** > **系统** > **安全** > **证书导入工具**。
- 如果为第三方 XMPP 客户端更新 LDAP 服务器配置，请重新启动 Cisco XCP 目录服务。 选择 **Cisco Unified IM and Presence 功能配置** > **工具** > **控制中心 - 功能服务**以重新启动此服务。

下一步做什么

继续为 XMPP 客户端配置 LDAP 搜索设置。

为 XMPP 客户端配置 LDAP 搜索设置

必须指定可让 IM and Presence Service 对第三方 XMPP 客户端成功执行联系人搜索的 LDAP 搜索设置。

第三方 XMPP 客户端在每次搜索时连接到 LDAP 服务器。 如果无法连接到主服务器，XMPP 客户端会尝试第一个备份 LDAP 服务器，如果该服务器不可用，它将尝试第二个备份服务器，以此类推。 如果当系统故障转移时正在进行 LDAP 查询，下一个可用的服务器将完成此 LDAP 查询。

（可选）您可以打开从 LDAP 服务器检索 vCard 的功能。 如果您打开 vCard 检索：

- 公司 LDAP 目录会存储 vCard。
- 当 XMPP 客户端搜索自己的 vCard 或某个联系人的 vCard 时，将通过 JDS 服务从 LDAP 检索 vCard。
- 客户端无法设置或修改自己的 vCard，因为它们未获得编辑 LDAP 目录的授权。

如果打开从 LDAP 服务器检索 vCard 的功能：

- IM and Presence Service 将 vCard 存储在本地数据库中。
- 当 XMPP 客户端搜索自己的 vCard 或某个联系人的 vCard 时，将从本地 IM and Presence Service 数据库检索 vCard。

- 客户端可以设置或修改自己的 vCard。

下表列出了 XMPP 客户端的 LDAP 搜索设置。

表 *8: XMPP* 客户端的 *LDAP* 搜索设置

字段	设置
LDAP 服务器类型	从该列表中选择 LDAP 服务器类型： • Microsoft Active Directory • 通用目录服务器 - 如果要使用任何其他支持的 LDAP 服务器类型（iPlanet、Sun ONE 或 OpenLDAP），请选择此菜单项。
用户对象类	输入与您的 LDAP 服务器类型对应的“用户对象类”值。 此值必须与在您 LDAP 服务器上配置的“用户对象类”值匹配。 如果您使用 Microsoft Active Directory，则默认值为 user。
基本上下文	输入与您的 LDAP 服务器对应的“基本上下文”。 此值必须与以前配置的域和/或 LDAP 服务器上的组织结构相匹配。
用户属性	输入与您的 LDAP 服务器类型对应的“用户属性”值。 此值必须与在您 LDAP 服务器上配置的“用户属性”值匹配。 如果您使用 Microsoft Active Directory，则默认值为 sAMAccountName。 如果使用 Directory URI IM 地址方案，且 Directory URI 映射到 mail 或 msRTCSIPPrimaryUserAddress，则必须在用户属性中指定 mail 或 msRTCSIPPrimaryUserAddress。
LDAP 服务器 1	选择主 LDAP 服务器。
LDAP 服务器 2	（可选）选择备份 LDAP 服务器。
LDAP 服务器 3	（可选）选择备份 LDAP 服务器。

开始之前

为 XMPP 客户端指定 LDAP 服务器名称和地址。

过程

步骤 1 选择 **Cisco Unified CM IM and Presence 管理** > **应用程序** > **第三方客户端** > **第三方 LDAP 设置**。

步骤 2 在字段中输入信息。

步骤 3 如果要使用户能够请求其联系人的 vCard 和从 LDAP 服务器检索 vCard 信息，请选中**从 LDAP 建立 vCard**。 如果希望客户端能够在用户加入联系人列表时自动为用户请求 vCard，则将此复选框保持不选中状态。 在这种情况下，客户端从本地 IM and Presence Service 数据库检索 vCard 信息。

步骤 4 输入构造 vCard FN 字段所需的 LDAP 字段。 在用户请求联系人的 vCard 时，客户端使用 vCard FN 字段中的值显示联系人在联系人列表中的姓名。

步骤 5 在“可搜索 LDAP 属性”表中，将客户端用户字段映射到相应的 LDAP 用户字段。

如果使用 Microsoft Active Directory，IM and Presence Service 会填充表中的默认属性值。

步骤 6 单击**保存**。

步骤 7 启动 Cisco XCP 路由器服务（如果此服务未运行）

提示 如果更新第三方 XMPP 客户端的 LDAP 搜索配置，请重新启动 Cisco XCP 目录服务。 选择 **Cisco Unified IM and Presence 功能配置** > **工具** > **控制中心 - 功能服务**以重新启动此服务。

下一步做什么

继续打开 Cisco XCP 目录服务。

打开 Cisco XCP 目录服务

必须打开 Cisco XCP 目录服务，允许第三方 XMPP 客户端的用户从 LDAP 目录搜索和添加联系人。 在群集中的所有节点上打开 Cisco XCP 目录服务。

注释 不要打开 Cisco XCP 目录服务，直到您为第三方 XMPP 客户端配置 LDAP 服务器和 LDAP 搜索设置。 如果打开了 Cisco XCP 目录服务，但没有为第三方 XMPP 客户端配置 LDAP 服务器和 LDAP 搜索设置，该服务将启动，然后再次停止。

开始之前

为第三方 XMPP 客户端配置 LDAP 服务器和 LDAP 搜索设置。

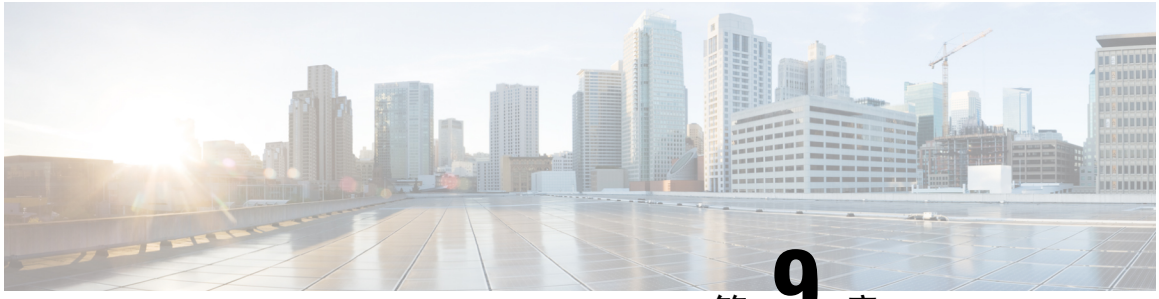
过程

步骤 1 选择 **Cisco Unified IM and Presence 功能配置** > **工具** > **服务启动**。

步骤 2 从“服务器”菜单中选择 IM and Presence Service 节点。

步骤 3 选择 **Cisco XCP 目录服务**。

步骤 4 单击**保存**。



第 9 章

为 IM and Presence Service 配置 Cisco Unified Communications Manager

- 集成概述，第 87 页
- Cisco Unified Communications Manager 集成前提条件，第 87 页
- Cisco Unified Communications Manager 上的 SIP 干线配置，第 88 页

集成概述

本部分详细介绍了为完成 IM and Presence Service 配置，您应该在 Cisco Unified Communications Manager 中完成的任务。

Cisco Unified Communications Manager 集成前提条件

配置 IM and Presence Service 与 Cisco Unified Communications Manager 的集成之前，请确保在 Cisco Unified Communications Manager 上完成以下一般配置任务。有关如何配置 Cisco Unified Communications Manager 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。

下表列出了 IM and Presence Service 集成的基本配置任务。有关字段及其选项的说明，请参阅联机帮助。

表 *9: Cisco Unified Communications Manager* 上的必要配置

任务	说明
修改用户凭证策略	建议您为用户设置凭证策略的过期日期。不需要凭证策略过期日期的唯一类型的用户是应用程序用户。 如果您使用 LDAP 服务器在 Cisco Unified Communications Manager 上验证用户，则 Cisco Unified Communications Manager 不使用凭证策略。 **Cisco Unified CM 管理** > **用户管理** > **用户设置** > **凭证策略默认值**
配置电话设备，并将目录号码 (DN) 与每个设备关联	启用**允许从 CTI 控制设备**以允许电话与客户端互操作。 **Cisco Unified CM 管理** > **设备** > **电话**
配置用户，然后将设备与每位用户关联	确保每个用户的用户 ID 值唯一。 **Cisco Unified CM 管理** > **用户管理** > **最终用户**
将用户与线路显示关联	有关详细信息，请参阅： **Cisco Unified CM 管理** > **设备** > **电话**
将用户添加到启用 CTI 的用户组	要启用桌面电话控制，必须将用户添加到启用 CTI 的用户组。 **Cisco Unified CM 管理** > **用户管理** > **用户组**
证书交换	系统会在安装过程中自动处理 Cisco Unified Communications Manager 与 IM and Presence Service 之间的证书交换。但是，如果出现问题，您需要手动完成证书交换，请参阅与 Cisco Unified Communications Manager 交换证书，第 129 页。

注释 如果在 SAN 字段中，您上传到 IM and Presence Service 的 Cisco Unified Communications Manager Tomcat 证书包含主机名，则所有这些证书都应该可从 IM and Presence Service 解析。IM and Presence Service 必须能够通过 DNS 解析主机名，否则思科同步代理服务将无法启动。无论您是使用 Cisco Unified Communications Manager 服务器的节点名称的主机名、IP 地址还是 FQDN，都是如此。

Cisco Unified Communications Manager 上的 SIP 干线配置

完成这些任务，将 SIP 干线连接配置为 Cisco Unified Communications Manager。

过程

	命令或操作	目的
步骤 1	配置 SIP 干线安全性配置文件， 第 89 页	为 Cisco Unified Communications Manager 与 IM and Presence Service 之间的干线连接配置 SIP 干线安全性配置文件。
步骤 2	为 IM and Presence Service 配置 SIP 干线， 第 90 页	将 SIP 干线安全性配置文件分配到 SIP 干线，并配置 Cisco Unified Communications Manager 与 IM and Presence Service 之间的干线连接。
步骤 3	配置 SRV 群集名称， 第 91 页	可选。 仅当您在 Cisco Unified Communications Manager 与 IM and Presence Service 之间的 SIP 干线上使用 DNS SRV 并且使用 IM and Presence 默认域以外的 SRV 地址时，完成此程序。 在这种情况下，配置 **SRV 群集名称**服务参数。 否则，您可以跳过此任务。
步骤 4	配置 Presence 网关， 第 92 页	在 IM and Presence Service 上，将 Cisco Unified Communications Manager 指定为 Presence 网关，从而允许系统交换 Presence 信息。
步骤 5	配置 SIP PUBLISH 干线， 第 92 页	可选。 执行此程序以便为 IM and Presence 配置 SIP PUBLISH 干线。 打开此设置后，Cisco Unified Communications Manager 会针对与 Cisco Unified Communications Manager 上为 IM and Presence Service 许可的用户关联的所有线路，发布电话在线状态。
步骤 6	验证 Cisco Unified Communications Manager 上的服务， 第 93 页	验证 Cisco Unified Communications Manager 上必要的服务是否在运行。
步骤 7	配置群集外 Cisco Unified Communications Manager 的电话在线状态， 第 93 页	将 Cisco Unified Communications Manager 配置为 IM and Presence Service 的 TLS 对等主题。 如果要允许从 IM and Presence Service 群集外部的 Cisco Unified Communications Manager 显示电话在线状态，则需要 TLS。

配置 SIP 干线安全性配置文件

在 Cisco Unified Communications Manager 上，为与 IM and Presence Service 的干线连接配置 SIP 干线安全性配置文件。

过程

步骤 1 在 **Cisco Unified CM 管理** > **系统** > **安全性** > **SIP Trunk 安全性配置文件**中，单击**查找**。

步骤 2 单击**非安全 SIP 干线配置文件**。

步骤 3 单击**复制**。

步骤 4 输入配置文件的**名称**。 例如 `IMP-SIP-Trunk-Profile`。

步骤 5 完成以下设置：

- **设备安全模式**设置为**非安全**。
- **接入传输类型**设置为 **TCP+UDP**。
- **输出传输类型**设置为 **TCP**。

步骤 6 选中以下复选框：

- **接受 Presence 订阅**
- **接受对话外 REFER**
- **接受主动通知**
- **接受 Replaces 报头**

步骤 7 单击**保存**。

下一步做什么

为 IM and Presence Service 配置 SIP 干线，第 90 页

为 IM and Presence Service 配置 SIP 干线

设置 Cisco Unified Communications Manager 与 IM and Presence Service 群集之间的 SIP 干线连接。

开始之前

配置 SIP 干线安全性配置文件，第 89 页

过程

步骤 1 从 **Cisco Unified CM 管理**中，选择**设备** > **干线**

步骤 2 单击**新增**。

步骤 3 从**干线类型**下拉列表框中，选择 **SIP 干线**。

步骤 4 从**设备协议**下拉列表框中，选择 **SIP**。

步骤 5 从**干线服务类型**下拉列表框中，选择**无**。

步骤 6 单击**下一步**。

步骤 7 在**设备名称**字段中，输入干线的名称。 例如 `IMP-SIP-Trunk`。

步骤 8 从下拉列表框中选择**设备池**。

步骤 9 在 **SIP 信息**部分，输入 IM and Presence 群集的地址信息，以将干线分配给 IM and Presence Service：

- 如果您使用的是 IM and Presence Service 的 DNS SRV 记录，选中**目标地址是 SRV** 复选框并在**目标地址**字段中输入 SRV。
- 否则，在**目标地址**字段中输入 IM and Presence 发布方节点的 IP 地址或 FQDN。 单击 **(+)** 按键可以添加其他节点。 最多可以输入 16 个节点。

a) 在**目标地址**字段中，输入 IM and Presence 节点的 IP 地址、FQDN 或 DNS SRV。

b) 如果要配置多节点部署，请选中**目标地址为 SRV**。

在这种情况下，Cisco Unified Communications Manager 可执行 DNS SRV 记录查询以解析名称，例如 `_sip._tcp.hostname.tld_sip._tcp.hostname.tld`。 如果您配置单节点部署，不要选中此复选框，Cisco Unified Communications Manager 将执行 DNS A 记录查询以解析名称，例如 `hostname.tld`。

思科建议您使用 IM and Presence Service 默认域作为 DNS SRV 记录的目标地址。

注释 您可以指定任何域值作为 DNS SRV 记录的目标地址。 无需向指定的域分配用户。 如果您输入的域值与 IM and Presence Service 默认域不同，则必须确保 IM and Presence Service 上名为“SRV 群集名称”的 SIP 代理服务参数与您在 DNS SRV 记录中指定的域值匹配。 如果您使用默认域，则无需更改“SRV 群集名称”参数。

在这两种情形中，Cisco Unified Communications SIP 干线的“目标地址”必须由 DNS 解析，且要与在 IM and Presence 节点上配置的“SRV 群集名称”匹配。

步骤 10 对于**目标端口**，请输入 `5060`

步骤 11 从 **SIP 干线安全性配置文件**下拉列表框中，选择您在之前任务中创建的 SIP 干线安全性配置文件。

步骤 12 从 **SIP 配置文件**下拉列表框中选择一个配置文件，例如**标准 SIP 配置文件**

步骤 13 单击**保存**。

下一步做什么

当您在 Cisco Unified Communications Manager 与 IM and Presence Service 之间的 SIP 干线上使用 DNS SRV 并且使用 IM and Presence 默认域以外的地址时，配置 SRV 群集名称，第 91 页。

否则，配置 SIP PUBLISH 干线，第 92 页。

配置 SRV 群集名称

仅当您在 Cisco Unified Communications Manager 与 IM and Presence Service 之间的 SIP 干线上使用 DNS SRV 并且使用 IM and Presence 默认域以外的地址时，配置 **SRV 群集名称**服务参数。 否则，您可以跳过此任务。

过程

步骤 1 从 Cisco Unified CM IM and Presence 功能配置中，选择**系统** > **服务参数**。

步骤 2 从**服务器**下拉菜单中选择 IM and Presence 发布方节点，然后单击**前往**。

步骤 3 从**服务**下拉列表中选择 **Cisco SIP Proxy** 服务。

步骤 4 在 **SRV 群集名称**字段中，输入 SRV 地址。

步骤 5 单击**保存**。

配置 SIP PUBLISH 干线

完成此可选程序以便为 IM and Presence 配置 SIP PUBLISH 干线。 打开此设置后，Cisco Unified Communications Manager 会针对与 Cisco Unified Communications Manager 上为 IM and Presence Service 许可的用户关联的所有线路，发布电话在线状态。

过程

步骤 1 从 Cisco Unified CM IM and Presence 管理中，选择 **Presence** > **设置** > **标准配置**。

步骤 2 从 **CUCM IM and Presence Publish 干线**下拉列表中，选择您在 Cisco Unified Communications Manager 上为 IM and Presence Service 配置的 SIP 干线。

步骤 3 单击**保存**。

注释 保存此新设置时，Cisco Unified Communications Manager 中的 **IM and Presence 发布干线**服务参数也会使用此新设置进行更新。

下一步做什么

验证 Cisco Unified Communications Manager 上的服务，第 93 页

配置 Presence 网关

在 IM and Presence Service 上执行此程序可将 Cisco Unified Communications Manager 指定为 Presence 网关。 此配置支持 Cisco Unified Communications Manager 与 IM and Presence Service 之间的 Presence 信息交换。

过程

步骤 1 从 **Cisco Unified CM IM and Presence 管理** > **Presence** > **网关**。

步骤 2 单击**新增**。

步骤 3 从 **Presence 网关**下拉列表框中选择 **CUCM**。

步骤 4 输入 **Description**。

步骤 5 在 **Presence 网关**字段中，输入以下选项之一：

- Cisco Unified Communications Manager 发布方节点的 IP 地址或 FQDN
- 解析到 Cisco Unified Communications Manager 订阅方节点的 DNS SRV

步骤 6 单击**保存**。

下一步做什么

配置 SIP PUBLISH 干线，第 92 页

验证 Cisco Unified Communications Manager 上的服务

此程序用于验证必要的服务是否在 Cisco Unified Communications Manager 节点上运行。

过程

步骤 1 在 Cisco Unified 功能配置中，选择**工具** > **控制中心 - 功能服务**。

步骤 2 从**服务器**菜单中选择 Cisco Unified Communications Manager 群集节点，然后单击**前往**。

步骤 3 确保以下服务正在运行。 如果它们没有运行，请立即启动。

- Cisco CallManager
- Cisco TFTP
- Cisco CTIManager
- Cisco AXL Web 服务（用于 IM and Presence 与 Cisco Unified Communications Manager 之间的数据同步）

步骤 4 如果上面的任何服务没有运行，请选择该服务，然后单击**启动**。

配置群集外 Cisco Unified Communications Manager 的电话在线状态

您可以允许从 IM and Presence Service 群集外部的 Cisco Unified Communications Manager 显示电话在网状态。 但是，为了让 IM and Presence Service 能够从群集外的 Cisco Unified Communications Manager 接受 SIP PUBLISH，Cisco Unified Communications Manager 必须列为 IM and Presence 的 TLS 可信对等节点

过程

	命令或操作	目的
步骤 1	将 Cisco Unified Communications Manager 添加为 TLS 对等节点， 第 94 页	将 Cisco Unified Communications Manager 添加为 IM and Presence Service 的 TLS 对等节点。
步骤 2	为 Unified Communications Manager 配置 TLS 环境， 第 94 页	添加 Cisco Unified Communications Manager TLS 对等节点

将 Cisco Unified Communications Manager 添加为 TLS 对等节点

为了让 IM and Presence Service 能够从群集外的 Cisco Unified Communications Manager 接受 SIP PUBLISH，Cisco Unified Communications Manager 必须列为 IM and Presence Service 的 TLS 可信对等节点。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理** > **系统** > **安全性** > **TLS 对等主题**中，单击**新增**。

步骤 2 在**对等主题名称**字段中输入外部 Cisco Unified Communications Manager 的 IP 地址。

步骤 3 在**说明**字段中输入节点的名称。

步骤 4 单击**保存**。

下一步做什么

配置 TLS 上下文， 第 148 页

为 Unified Communications Manager 配置 TLS 环境

执行以下程序可将您在先前任务中配置的 Cisco Unified Communications Manager TLS 对等节点添加到选定的 TLS 对等节点。

开始之前

将 Cisco Unified Communications Manager 添加为 TLS 对等节点， 第 94 页

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理** > **系统** > **安全性** > **TLS 环境配置**中，单击**查找**。

步骤 2 单击 **Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context**。

步骤 3 从可用 TLS 对等主题列表中，选择您为 Cisco Unified Communications Manager 配置的 TLS 对等主题。

步骤 4 将此 TLS 对等主题移至“选定 TLS 对等主题”。

步骤 5 单击**保存**。

步骤 6 重新启动所有群集节点上的 Cisco OAMAgent：

a) 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 网络服务**。
b) 从**服务器**下拉列表框中，选择 IM and Presence 服务器并单击**前往**
c) 在 **IM and Presence Service** 下，选择 **Cisco OAMAgent** 并单击**重新启动**。
d) 重新启动所有群集节点上的服务。

步骤 7 OAM Agent 重新启动后，重新启动 Cisco Presence Engine。

a) 选择**工具** > **控制中心 - 功能服务**。
b) 从**服务器**下拉列表框中，选择 IM and Presence 节点并单击**前往**。
c) 在 **IM and Presence Service** 下，选择 **Cisco Presence Engine** 并单击**重新启动**。
d) 重新启动所有群集节点上的服务。

下一步做什么

验证 Cisco Unified Communications Manager 上的服务，第 93 页

第 10 章

配置集中式部署

- 集中式部署概述， 第 97 页
- 集中式部署前提条件， 第 101 页
- 集中式部署配置任务流程， 第 102 页
- 通过 IM and Presence 集中式部署进行升级需要重新同步， 第 114 页
- IM and Presence 集中式群集设置以及为子域启用了 SSO 的远程电话群集， 第 114 页
- 将电话在线状态集成到集中式部署中， 第 115 页
- 集中式部署相互作用和限制， 第 116 页

集中式部署概述

通过 IM and Presence 集中式部署，您可以在不同的群集中部署 IM and Presence 和电话。 中央 IM and Presence 群集为企业处理 IM and Presence，而远程 Cisco Unified Communications Manager 电话群集则为企业处理语音和视频呼叫。

与标准部署相比，集中式部署选项可带来以下优点：

- 集中式部署选项不需要 1x1 比例的电话群集与 IM and Presence Service 群集 — 您可以按照需求单独扩展 IM and Presence 部署和电话部署。
- IM and Presence Service 不需要全网状拓扑
- 与电话无关的版本 — 您的 IM and Presence 中央群集可以运行与 Cisco Unified Communications Manager 电话群集不同的版本。
- 可以从中央群集管理 IM and Presence 升级和设置。
- 可降低成本，尤其适用于具有许多 Cisco Unified Communications Manager 群集的大型部署
- 易于与第三方进行 XMPP 联合。
- 支持与 Microsoft Outlook 集成日历。 有关配置详细信息，请参阅为 *IM and Presence Service* 集成 *Microsoft Outlook* 日历。

OVA 要求

对于集中式部署，我们建议使用最少 15000 位用户的 OVA 的 25000 位用户 IM and Presence OVA。15000 位用户的 OVA 可以增长到 25000 位用户。借助 25K OVA 模板和启用高可用性的六节点群集，IM and Presence Service 中央部署最多可支持 75,000 个客户端。要通过 25K OVA 支持 75K 位用户，需要将 XCP 路由器的默认跟踪级别从**信息**改为**错误**。对于中央群集中的 Unified Communications Manager 发布方节点，以下要求适用：

- 25,000 IM and Presence OVA（最多 75000 位用户）可以使用安装在中央群集的 Unified Communications Manager 发布方节点上的 10000 用户 OVA 进行部署
- 15,000 IM and Presence OVA（最多 45000 位用户）可以使用安装在中央群集的 Unified Communications Manager 发布方节点上的 7500 用户 OVA 进行部署

注释 如果计划启用多设备消息传送，请根据客户端数量而不是用户数量来衡量部署，因为每个用户可能有多个 Jabber 客户端。例如，如果您有 25000 位用户，每位用户有两个 Jabber 客户端，则您的部署需要 50000 位用户的容量。

集中式部署的群集间功能

两个集中式群集之间支持群集间功能。 我们使用一个包含 25K（具有 25K OVA）台设备的群集和一个包含 15K（具有 15K OVA）台设备的另一个群集进行了群集间对等测试，未观察到性能问题。

集中式部署设置与标准（分散式）部署

下表讨论了设置 IM and Presence 集中式群集部署与 IM and Presence Service 标准部署之间的一些差异。

设置阶段	与标准部署的差异
安装阶段	IM and Presence 集中式部署的安装程序与标准部署相同。 但是，采用集中式部署时，IM and Presence 中央群集与电话群集分开安装，并且可位于不同的硬件服务器上。 根据您对拓扑的规划方式，IM and Presence 中央群集可能位于与电话群集不同的物理硬件上。 对于 IM and Presence 中央群集，您仍必须安装 Cisco Unified Communications Manager，然后在相同的服务器上安装 IM and Presence Service。 但是，IM and Presence 中央群集的 Cisco Unified Communications Manager 实例主要用于数据库和用户设置，不处理语音或视频呼叫。

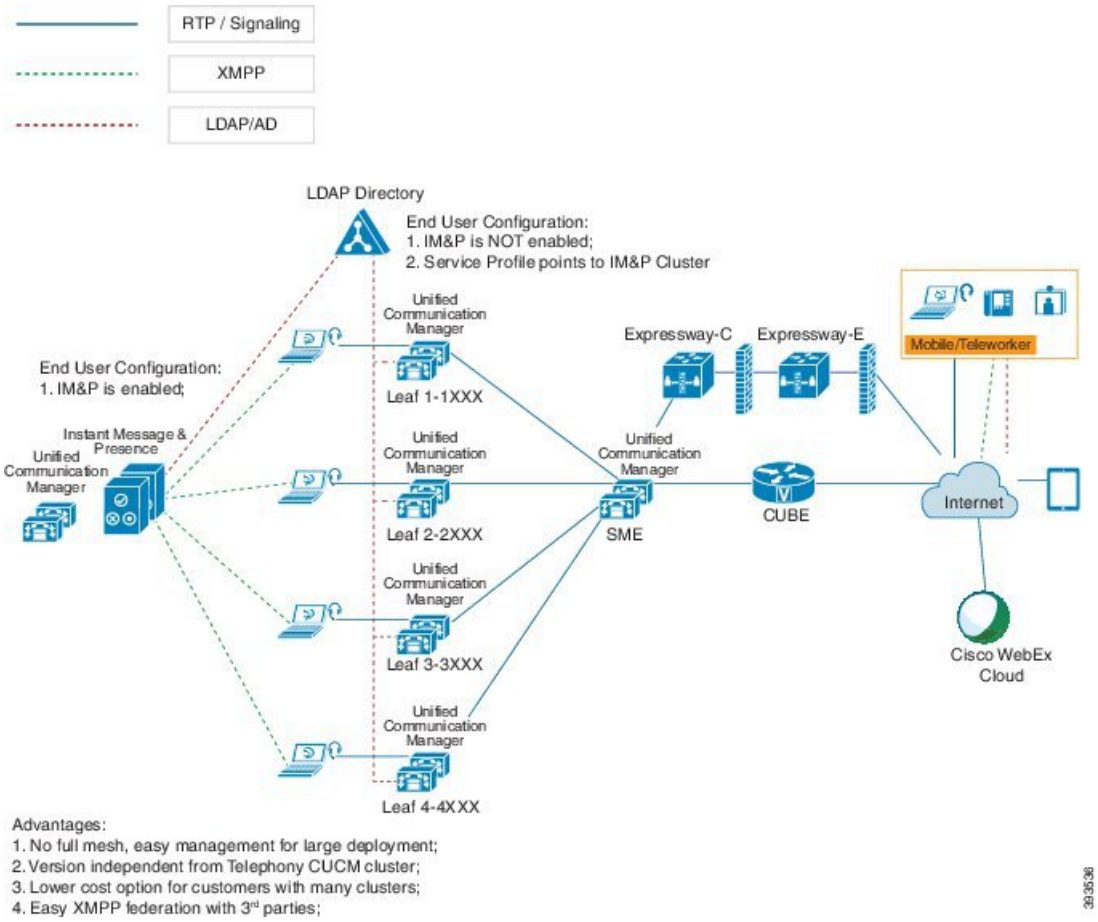
设置阶段	与标准部署的差异
配置阶段	与标准（分散式）部署相比，设置 IM and Presence Service 中央部署需要以下额外配置： • 用户必须同步到电话群集和 IM and Presence Service 中央群集，以便它们同时存在于两个数据库中。 • 在电话群集中，不应为 IM and Presence 启用最终用户。 • 在您的电话群集中，服务配置文件必须包含 IM and Presence Service，并且必须指向 IM and Presence 中央群集。 • 在 IM and Presence 中央群集中，必须为 IM and Presence Service 启用用户。 • 在 IM and Presence 中央群集的数据库发布方节点中，添加远程 Cisco Unified Communications Manager 电话群集对等节点。 以下配置适用于 IM and Presence Service 的标准部署，但中央部署不需要： • 不需要 Presence 网关。 • 不需要 SIP Publish 干线。 • IM and Presence 中央群集不需要服务配置文件 — 服务配置文件在中央群集连接的电话群集上配置。

集中式群集部署架构

下图突出显示了此部署选项的群集架构。 Cisco Jabber 客户端连接到多个 Cisco Unified Communications Manager 群集以进行语音和视频呼叫。 在此示例中，Cisco Unified Communications Manager 电话群集是会话管理版部署中的叶群集。 对于多样的在线状态，Cisco Jabber 客户端连接到 IM and Presence Service 中央群集。 IM and Presence 中央群集管理 Jabber 客户端的即时消息和在线状态。

注释 您的 IM and Presence 群集仍包含 Cisco Unified Communications Manager 实例。 不过，此实例用于处理数据库和用户设置等共享功能，不处理电话。

图 *4: IM and Presence Service* 集中式群集架构

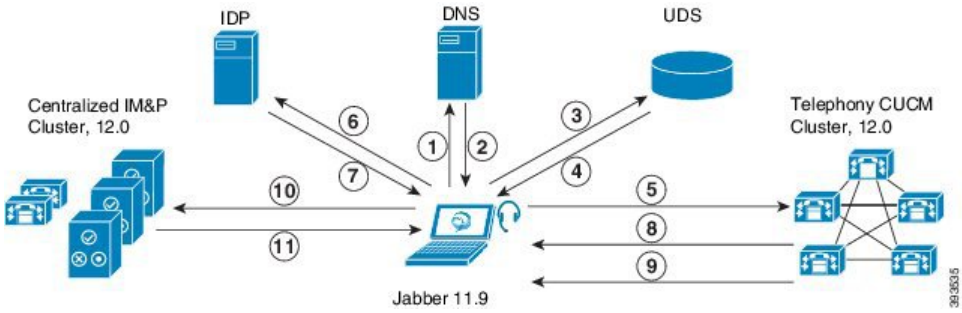


集中式群集使用案例

为连接电话和 IM and Presence 群集，我们引入了一个用于交换访问密钥的新系统。 此图显示了 SSO 登录的流程：

- [1]-[2]：查询 DNS 以获取 SRV 记录。
- [3]-[4]：查询 UDS 以获取主 Cisco Unified Communications Manager 群集。
- [5]-[8]：通过 SAML SSO 从 Cisco Unified Communications Manager 群集获取访问令牌和刷新令牌。
- [9]：读取 UC 服务配置文件。 服务配置文件包含 IM and Presence 配置文件，并指向 IM and Presence 中央群集。
- [10]：客户端通过 SOAP 和 XMPP 接口使用相同的访问令牌注册到 IM and Presence 群集。
- [11]：系统验证令牌并将响应发送回 Jabber 客户端。

图 *5: IM and Presence Service* 集中式群集使用案例



集中式部署前提条件

以下要求适用于 IM and Presence Service 的集中式部署：

- IM and Presence Service 中央群集必须运行版本 11.5(1)SU4 或更高版本。
- 与 IM and Presence 中央群集一起运行的本地 Cisco Unified Communications Manager 实例必须运行与 IM and Presence 中央群集相同的版本。
- 远程 Cisco Unified Communications Manager 电话群集必须运行 10.5 (2) 版或更高版本。
- Cisco Jabber 必须运行 11.9 或更高版本。
- 对于推送通知即时消息支持，IM and Presence Service 必须至少运行 11.5(1)SU4。
- 您需要在集中式 IM and Presence 群集的 CUCM 发布方节点上启用 Cisco Cloud Onboarding，以便 iOS 设备的所有即时消息也可以使用 Apple 推送通知服务 (APNs) 解决方案。

  另外，您还需要在 CUCM 枝叶群集上启用 Cisco Cloud Onboarding 选项，以便当 Jabber iOS 版本设备被 iOS 挂起或终止时，通常注册到这些群集的 TCT 设备可以通过 APN 路由呼叫。

  有关如何在 IM and Presence Service 群集中启用 Cisco Cloud Onboarding 的详细信息，请参阅《推送通知部署指南》中的启用 *Cisco Cloud Onboarding* 一章。
- Cisco Unified Communications Manager 功能基于远程电话群集上运行的 Cisco Unified Communications Manager 版本，而不是基于同 IM and Presence 中央群集一起运行的本地实例。例如：
  - 对于推送通知呼叫支持，远程电话群集必须至少运行 11.5(1)SU4。
  - 对于 OAuth 刷新登录支持，远程 Cisco Unified Communications Manager 电话群集必须至少运行 11.5(1)SU4。
  - 对于 SAML SSO 支持，远程电话群集必须至少运行 11.5(1)SU4。
- **Cisco AXL Web 服务**功能服务必须在所有群集中运行。此服务默认启用，但您可以从 Cisco Unified 功能配置的**服务激活**窗口确认其是否已激活。

- 采用集中式部署时，多样的在线状态由 Cisco Jabber 处理。仅当用户登录到 Cisco Jabber 时，才会显示用户的电话在线状态。

DNS 要求

IM and Presence 中央群集必须具有指向 Cisco Unified Communications Manager 电话群集发布方节点的 DNS SRV 记录。如果您的电话部署包含 ILS 网络，则 DNS SRV 必须指向中枢群集。这个 DNS SRV 记录应该引用 "_cisco-uds"。

SRV 记录是域名系统 (DNS) 资源记录，用于标识托管特定服务的计算机。SRV 资源记录用于查找 Active Directory 的域控制器。要验证域控制器的 SRV 定位器资源记录，请使用以下方法：

Active Directory 在以下文件夹中创建其 SRV 记录，其中域名表示已安装域的名称：

- Forward Lookup Zones/Domain_Name/_msdcs/dc/_sites/Default-First-Site-Name/_tcp
- Forward Lookup Zones/Domain_Name/_msdcs/dc/_tcp

在这些位置，应显示以下服务的 SRV 记录：

- _kerberos
- _ldap
- _cisco_uds：指 SRV 记录

创建 SRV 记录期间必须设置下面提到的参数。

- 服务：_cisco_uds
- 协议：_tcp
- 权重：从 0 开始（0 为最高优先级）
- 端口号：8443
- 主机：服务器的 fqdn 名称

来自运行 Jabber 客户端的计算机的 DNS SRV 记录示例如下：

```
nslookup -type=all _cisco-uds._tcp.dcloud.example.com
Server: ad1.dcloud.example.com
Address: x.x.x.x
_cisco-uds._tcp.dcloud.example.com SRV service location:
priority = 10
weight = 10
port = 8443
svr hostname = cucm2.dcloud.example.com
cucm2.dcloud.example.com internet address = x.x.x.y
```

集中式部署配置任务流程

如果要配置新的 IM and Presence Service 部署以使用集中式部署选项，请完成这些任务。

注释 仅将此任务流程用于新的 IM and Presence Service 部署。

表 *10:* 集中式群集配置任务流程

	IM and Presence 中央群集	远程电话群集	目的
步骤 **1**	通过功能组模板启用 IM and Presence， 第 104 页		在 IM and Presence 中央群集中，配置启用 IM and Presence Service 的模板。
步骤 **2**	在 IM and Presence 中央群集上完成 LDAP 同步， 第 105 页		完成 LDAP 同步，以将设置传播到 IM and Presence 中央群集中的 LDAP 同步用户。
步骤 **3**	通过批量管理为 IM and Presence 启用用户， 第 105 页		可选。 如果您已完成 LDAP 同步，请通过批量管理为用户启用 IM and Presence。
步骤 **4**	添加远程电话群集， 第 106 页		将远程电话群集添加到 IM and Presence 中央群集。
步骤 **5**		配置 IM and Presence UC 服务， 第 107 页	在电话群集中，添加指向 IM and Presence 中央群集的 UC 服务。
步骤 **6**		为 IM and Presence 创建服务配置文件， 第 108 页	将您的 IM and Presence UC 服务添加到服务配置文件。 Cisco Jabber 客户端使用此配置文件来查找 IM and Presence 中央群集。
步骤 **7**		在电话群集中禁用 Presence 用户， 第 108 页	在电话群集中，编辑 Presence 用户设置以指向 IM and Presence 中央群集。
步骤 8		配置 OAuth 刷新登录 ， 第 109 页	在电话群集中配置 OAuth 将启用中央群集的功能。
步骤 **9**		配置 ILS 网络， 第 110 页	如果存在多个电话群集，则必须配置 ILS。
步骤 **10**		移动和远程访问配置	如果是在集中式部署中，配置移动和远程访问。

后续操作

- 如果要将中央群集作为群集间网络的一部分连接到其他 IM and Presence 群集，请配置群集间对等。
- 在 IM and Presence 管理员控制台中向集中式部署新增条目时，必须重新启动 Cisco XCP 身份验证服务。

通过功能组模板启用 IM and Presence

此程序用于为中央群集配置具有 IM and Presence 设置的功能组模板。 您可以将功能组模板添加到 LDAP 目录配置，以便为同步用户配置 IM and Presence。

注释 您只能将功能组模板应用于尚未进行初始同步的 LDAP 目录配置。 从中央群集同步 LDAP 配置后，无法对 Cisco Unified Communications Manager 中的 LDAP 配置应用编辑。 如果您已同步目录，则需要使用批量管理为用户配置 IM and Presence。 有关详细信息，请参阅通过批量管理为 IM and Presence 启用用户，第 105 页。

过程

步骤 1 登录 IM and Presence 集中式群集的 Cisco Unified CM 管理界面。 此服务器应该没有配置电话。

步骤 2 选择**用户管理** > **用户/电话添加** > **功能组模板**。

步骤 3 执行下列操作之一：

- 单击**查找**并选择现有模板
- 单击**新增**以创建新的模板

步骤 4 选中以下两个复选框：

- **主群集**
- **为 Unified CM IM and Presence 启用用户**

步骤 5 填写**功能组模板配置**窗口中的其余字段。 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**。

下一步做什么

要将设置传播给用户，必须将功能组模板添加到尚未进行初始同步的 LDAP 目录配置中，然后完成初始同步。

在 IM and Presence 中央群集上完成 LDAP 同步，第 105 页

在 IM and Presence 中央群集上完成 LDAP 同步

在 IM and Presence Service 中央群集上完成 LDAP 同步，以通过功能组模板为用户配置 IM and Presence Service。

注释 初始同步完成后，您将无法对 LDAP 同步配置应用编辑。 如果初始同步已完成，请使用批量管理工具。 有关如何设置 LDAP 目录同步的更多详情，请参阅《*Cisco Unified Communications Manager* 系统配置指南》的“配置最终用户”部分。

开始之前

通过功能组模板启用 IM and Presence，第 104 页

过程

步骤 1 登录 IM and Presence 集中式群集的 Cisco Unified CM 管理界面。 此服务器应该没有配置电话。

步骤 2 选择**系统** > **LDAP** > **LDAP 目录**。

步骤 3 执行以下任一操作：

a) 单击**查找**并选择现有的 LDAP 目录同步。

b) 单击**新增**以创建新的 LDAP 目录。

步骤 4 从**功能组模板**下拉列表框中，选择您在上一个任务中创建的启用了 IM and Presence 的功能组模板。

步骤 5 填写 **LDAP 目录**窗口中的其余字段。 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**。

步骤 7 单击**执行完全同步**。

Cisco Unified Communications Manager 会与外部 LDAP 目录同步数据库。 最终用户配置了 IM and Presence Service。

下一步做什么

添加远程电话群集，第 106 页

通过批量管理为 IM and Presence 启用用户

如果您已将用户同步到中央群集，并且没有为 IM and Presence Service 启用这些用户，请使用批量管理的更新用户功能为 IM and Presence Service 启用这些用户。

注释 您还可以使用批量管理的导入用户或插入用户功能通过 csv 文件导入新用户。 有关程序，请参阅《*Cisco Unified Communications Manager* 批量管理指南》。 请确保导入的用户选择了以下选项：

- 主群集
- 为 Unified CM IM and Presence 启用用户。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**批量管理** > **用户** > **更新用户** > **查询**。

步骤 2 从**过滤器**中，选择**已启用主群集**并单击**查找**。 该窗口将显示以此为主群集的所有最终用户。

步骤 3 单击**下一步**。
在**更新用户配置**窗口中，最左侧的复选框表示是否要使用此查询编辑此设置。 如果不选中左侧的复选框，查询将不会更新该字段。 右侧的字段表示此字段的新设置。 如果出现两个复选框，必须选中左侧的复选框以更新该字段，并在右侧复选框中输入新设置。

步骤 4 在**服务设置**下，为以下每个字段选中左侧的复选框，表示要更新这些字段，然后编辑相邻字段的设置，如下所示：

- **主群集** — 选中右侧复选框以将此群集启用为主群集。
- **为 Unified CM IM and Presence 启用用户** — 选中右侧复选框。 此设置使中央群集成为这些用户的 IM and Presence Service 提供商。

步骤 5 填写想要更新的所有剩余字段。 有关这些字段及其设置的帮助，请参阅联机帮助：

步骤 6 在**作业信息**下选择**立即运行**。

步骤 7 单击**提交**。

添加远程电话群集

此程序用于将您的远程电话群集添加到集中式 IM and Presence Service 群集。

注释 如果您有多个电话群集，必须部署 ILS。 在这种情况下，IM and Presence 中央群集连接的电话群集必须是中枢群集。

过程

步骤 1 登录到 IM and Presence Service 集中式群集上的数据库发布方节点。

步骤 2 从 Cisco Unified CM IM and Presence 管理中，选择**系统** > **集中式部署**。

步骤 3 单击**查找**查看当前的远程 Cisco Unified Communications Manager 群集列表。 如要编辑群集的详细信息，选择该群集并单击**编辑选定项**。

步骤 4 单击**新增**添加新的远程 Cisco Unified Communications Manager 电话群集。

步骤 5 为要添加的每个电话群集填写以下字段：

- **对等地址** — 远程 Cisco Unified Communications Manager 电话群集发布方节点的 FQDN、主机名、IPv4 地址或 IPv6 地址。
- **AXL 用户名** — 远程群集上的 AXL 帐户的登录用户名。
- **AXL 密码** — 远程群集上的 AXL 帐户的密码。

步骤 6 单击**保存并同步**按键。
IM and Presence Service 与远程群集同步密钥。

下一步做什么

配置 IM and Presence UC 服务， 第 107 页

配置 IM and Presence UC 服务

在远程电话群集中执行此程序可配置指向 IM and Presence Service 中央群集的 UC 服务。 电话群集中的用户将从 IM and Presence 中央群集获取 IM and Presence Service。

过程

步骤 1 登录电话群集的 Cisco Unified CM 管理界面。

步骤 2 选择**用户管理** > **用户设置** > **UC 服务**。

步骤 3 执行以下任一操作：

a) 单击**查找**并选择要编辑的现有服务。
b) 单击**新增**以创建新的 UC 服务。

步骤 4 从 **UC 服务类型**下拉列表框中选择 **IM and Presence** 并单击**下一步**。

步骤 5 从**产品类型**下拉列表框中选择 **IM and Presence Service**。

步骤 6 为群集输入唯一的**名称**。 这不一定是主机名。

步骤 7 从**主机名/IP 地址**，输入 IM and Presence 中央群集数据库发布方节点的主机名、IPv4 地址或 IPv6 地址。

步骤 8 单击**保存**。

步骤 9 建议。 重复此程序以创建第二个 IM and Presence Service，其中**主机名/IP 地址**字段指向中央群集中的订阅方节点。

下一步做什么

为 IM and Presence 创建服务配置文件，第 108 页.

为 IM and Presence 创建服务配置文件

在远程电话群集中执行此程序可创建指向 IM and Presence 中央群集的服务配置文件。 电话群集中的用户将使用此服务配置文件从中央群集获取 IM and Presence Service。

过程

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

步骤 2 执行下列操作之一：

a) 单击**查找**并选择要编辑的现有服务配置文件。

b) 单击**新增**以创建新的服务配置文件。

步骤 3 在 **IM and Presence 配置文件**部分，配置您在上一个任务中配置的 IM and Presence Service：

a) 从**主**下拉列表中，选择数据库发布方节点服务。

b) 从**次要**下拉列表中，选择订阅方节点服务。

步骤 4 单击**保存**。

下一步做什么

在电话群集中禁用 Presence 用户，第 108 页

在电话群集中禁用 Presence 用户

如果您已在电话部署中完成 LDAP 同步，请使用批量管理工具为 IM and Presence 用户编辑电话群集中的用户设置。此配置会将 Presence 用户指向 IM and Presence Service 的中央群集。

注释 此程序假定您已在电话群集中完成 LDAP 同步。但是，如果尚未完成初始 LDAP 同步，可以将 Presence 用户的中央部署设置添加到初始同步中。这种情况下，请在电话群集中执行以下操作：

- 配置包含您刚刚设置的**服务配置文件**的功能组模板。确保选中**主群集**选项，不要选中**为 Unified CM IM and Presence 启用用户**选项。
- 在 **LDAP 目录配置**种，将**功能组模板**添加到您的 LDAP 目录同步。
- 完成初始同步。

有关配置功能组模板和 LDAP 目录的更多详情，请参阅《*Cisco Unified Communications Manager* 系统配置指南》的“配置最终用户”部分。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**查询** > **批量管理** > **用户** > **更新用户** > **查询**。

步骤 2 从过滤器中，选择**已启用主群集**并单击**查找**。该窗口将显示以此为主群集的所有最终用户。

步骤 3 单击**下一步**。
在**更新用户配置**窗口中，最左侧的复选框表示是否要使用此查询编辑此设置。如果不选中左侧的复选框，查询将不会更新该字段。右侧的字段表示此字段的新设置。如果出现两个复选框，必须选中左侧的复选框以更新该字段，并在右侧复选框中输入新设置。

步骤 4 在**服务设置**下，为以下每个字段选中最左侧的复选框，表示要更新这些字段，然后编辑相邻的设置，如下所示：

- **主群集** — 选中右侧复选框以将电话群集启用为主群集。
- **为 Unified CM IM and Presence 启用用户** — 不选中右侧复选框。此设置禁用电话群集作为 IM and Presence 的提供者。
- **UC 服务配置文件** — 从下拉列表中选择您在上一个任务中配置的服务配置文件。此设置将用户指向 IM and Presence 中央群集，该群集将是 IM and Presence Service 的提供者。

注释 有关 Expressway 移动和远程访问配置，请参阅《通过 *Cisco Expressway* 的移动和远程访问部署指南》，网址：https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html。

步骤 5 根据需要填写所有剩余字段。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 6 在**作业信息**下选择**立即运行**。

步骤 7 单击**提交**。

下一步做什么

配置 OAuth 刷新登录 ，第 109 页

配置 OAuth 刷新登录

在电话群集中启用 OAuth 刷新登录。 这还会在中央群集中启用此功能。

过程

步骤 1 登录到电话群集上的 Cisco Unified CM 管理。

步骤 2 选择**系统** > **企业参数**。

步骤 3 在 **SSO 和 OAuth 配置**下，将**具有刷新登录流的 OAuth** 企业参数设置为**启用**。

步骤 4 如果您编辑了参数设置，单击**保存**。

注释　在重新生成 oauth 键时，您必须在所有 IM and Presence 节点上重启 Cisco XCP 验证服务，Jabber OAuth 登录才能正常工作。

配置 ILS 网络

对于存在多个远程电话群集的 IM and Presence 集中式群集，您可以使用群集间查找服务 (ILS) 为 IM and Presence 中央群集设置远程电话群集。ILS 会监控网络并将网络更改（如新的群集或地址更改）传播到整个网络。

注释　此任务流程侧重于有关 IM and Presence 集中式群集部署的 ILS 要求。有关电话的其他 ILS 配置，例如配置全局拨号计划复制或 URI 拨号，请参阅《*Cisco Unified Communications Manager* 系统配置指南》的“配置拨号计划”部分。

开始之前

如果是部署 ILS，请确保您已完成以下操作：

- 规划您的 ILS 网络拓扑。您必须知道哪些电话群集将是中枢群集或星形群集。
- IM and Presence 中央群集连接的电话群集必须是中枢群集。
- 您必须配置指向中央群集的发布方节点的 DNS SRV 记录。

有关设计 ILS 网络的信息，请参阅《思科协作系统解决方案参考网络设计》，网址：http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html。

过程

	命令或操作	目的
步骤 1	为 ILS 配置群集 ID，第 111 页	为每个电话群集设置唯一的群集 ID。群集 ID 设置为 `StandAloneCluster`（默认设置）时，ILS 将不起作用。
步骤 2	启用电话群集上的 ILS，第 111 页	配置并在 ILS 网络中的每个电话群集的发布方节点上激活 ILS。
步骤 3	验证 ILS 网络正在运行，第 112 页	ILS 发挥作用时，您可以在电话群集的 **ILS 配置**窗口中看到您的所有远程群集及其“最新”的同步状态。

为 ILS 配置群集 ID

ILS 网络中的每个群集都必须具有唯一的群集 ID。 此程序用于为电话群集指定唯一的群集 ID。

过程

步骤 1 登录到发布方节点上的 Cisco Unified CM 管理。

步骤 2 选择**系统** > **企业参数**。

步骤 3 从 `StandAloneCluster` 将**群集 ID** 参数的值更改为您设置的唯一值。 群集 ID 为 `StandAloneCluster` 时，ILS 将不起作用。

步骤 4 单击**保存**。

步骤 5 在要加入 ILS 网络的每个电话群集的发布方节点上重复此程序。 每个群集必须具有唯一的 ID。

下一步做什么

启用电话群集上的 ILS，第 111 页

启用电话群集上的 ILS

此程序用于在 Cisco Unified Communications Manager 电话群集上配置和激活 ILS。

注释

- 在配置星形群集之前配置中枢群集。
- 有关这些字段及其设置的帮助，请参阅联机帮助。

开始之前

为 ILS 配置群集 ID，第 111 页

过程

步骤 1 登录到您的电话群集发布方节点上的 Cisco Unified CM 管理。

步骤 2 选择**高级功能** > **ILS 配置**。

步骤 3 从**角色**下拉列表框中，根据您要设置的群集类型，选择**中枢群集**或**星形群集**。

步骤 4 选中**与远程群集交换全局拨号方案复制数据**复选框。

步骤 5 配置 **ILS 验证详细信息**。

a) 如果要在各个群集之间使用 TLS 验证，选中**使用 TLS 证书**复选框。

注释 如果使用 TLS，则必须在群集中的节点之间交换 CA 签名的证书。

b) 如果要使用密码验证（无论是否使用 TLS），请选中**使用密码**复选框并输入密码详细信息。

步骤 6 单击**保存**。

步骤 7 在 **ILS 群集注册**弹出窗口中，配置您的注册详细信息：

- 在**注册服务器**文本框中，输入要将此群集连接到的中枢群集的发布方节点 IP 地址或 FQDN。 如果这是您网络中的第一个中枢群集，可以将此字段留空。
- 确保选中**在此群集中的发布方上激活群集间查询服务**复选框。

步骤 8 单击**确定**。

步骤 9 在要加入到 ILS 网络的每个电话群集的发布方节点上重复此程序。
根据您配置的同步值，群集信息在整个网络中传播时可能会有延迟。

如果您选择在群集之间使用传输层安全 (TLS) 验证，则必须在 ILS 网络中每个群集的发布方节点之间交换 Tomcat 证书。 在 Cisco Unified 操作系统管理中，使用“批量证书管理”功能：

- 将证书从每个群集的发布方节点导出到中心位置
- 在 ILS 网络中合并导出的证书
- 将证书导入网络中每个群集的发布方节点

有关详细信息，请参阅《*Cisco Unified Communications Manager* 管理指南》的“管理证书”一章。

下一步做什么

ILS 启动运行且您交换证书（如果需要）之后， 验证 ILS 网络正在运行 ，第 112 页

验证 ILS 网络正在运行

此程序用于确认您的 ILS 网络是否已启动并运行。

过程

步骤 1 登录到任一电话群集的发布方节点。

步骤 2 从 Cisco Unified CM 管理中，选择**高级功能** > **ILS 配置**。

步骤 3 选中 **ILS 群集和全局拨号方案导入的类目**部分。 此时您的 ILS 网络拓扑会显示。

移动和远程访问配置

Cisco Unified Communications 移动和远程访问是思科协作边缘架构的核心部分。它允许 Cisco Jabber 等终端不在企业网络范围内时，有 Cisco Unified Communications Manager 提供的注册、呼叫控制、设置、消息传送和在线状态服务。Expressway 为 Unified CM 注册提供安全的防火墙穿越和线路端支持。

总体解决方案提供：

1. **场外访问**：为 Jabber 和 EX/MX/SX 系列客户端提供一致的网络外侧体验。
2. **安全**：安全的企业对企业通信。
3. **云服务**：企业级灵活性和可扩展解决方案，提供丰富的 Webex 集成和服务器提供商服务。
4. **网关和互操作性服务**：媒体和信令标准化并支持非标准端点。

配置

要在 Expressway-C 中的所有电话枝叶群集上配置移动和远程访问，选择**配置** → **Unified Communications** → **Unified CM 服务器**。

要在 Expressway-C 中的集中式 IM&P 节点群集上配置移动和远程访问，选择**配置**→ **Unified Communications** → **IM and Presence Service 节点**。

要在 Expressway-C. 中启用“**移动和远程访问**”，选择**配置** → **启用“移动和远程访问”**，然后根据下表选择控制选项。

表 *11: OAuth* 启用配置

验证路径	UCM / LADP 基本验证
通过刷新按 OAuth 令牌授权	开
按 OAuth 令牌授权	开
按用户凭证授权	否
允许 Jabber iOS 客户端使用嵌入式的 Safari 浏览器	否
检查内部验证可用性	是

表 *12: OAuth* 禁用配置

验证路径	UCM / LADP 基本验证
通过刷新按 OAuth 令牌授权	关
按用户凭证授权	开
允许 Jabber iOS 客户端使用嵌入式的 Safari 浏览器	关
检查内部验证可用性	是

注释 **有关基本移动和远程访问配置的信息，请参阅：** https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

通过 IM and Presence 集中式部署进行升级需要重新同步

如果您有 IM and Presence 集中式部署并升级了 IM and Presence 中央群集或任何远程电话对等群集，则必须在升级完成后重新同步群集。 您可以选择群集对等节点并单击**保存并同步**按键，从 Cisco Unified CM IM and Presence 管理的**集中式部署**窗口重新同步群集。

IM and Presence 集中式群集设置以及为子域启用了 SSO 的远程电话群集

在 IM and Presence 集中式部署中，如果您的远程电话群集有多个子域，可以启用 SOAP 登录到启用了 SSO 的远程访问客户端（例如 Jabber）。

本部分介绍在启用 SSO 的远程电话群集中配置子域用户登录到 Jabber 的步骤。 请考虑集中式部署方案，其中包含一个集中式群集和一个与该集中式群集关联的启用 SSO 的远程电话群集。

要为子域设置启用 SSO 的登录，请完成以下步骤：

过程

步骤 1 登录到 Cisco Unified CM 管理并执行以下操作：

a) 将用户从 LDAP 同步到枝叶节点，将**目录 URI** 字段设置为**邮件 ID** 并启用 SSO。 要了解如何同步 LDAP 用户，请参阅 LDAP 同步。

b) 将相同的用户同步到远程电话节点，并将**目录 URI** 字段设置为**邮件 ID**。

c) 在**最终用户配置**页面（**最终用户** > **最终用户管理**），为 IM and Presence 节点选中**服务设置**下的**为 Cisco Unified IM and Presence Service 启用用户**（**在关联的 UC 服务配置文件中配置 IM and Presence**）选项，使用户域集中式群集中的用户相同。

d) 在**最终用户配置**页面（**最终用户** > **最终用户管理**），使用**权限信息**部分将用户添加到 Cisco Call Manager (CCM) 最终用户组。

e) 在远程电话群集上为 IM and Presence 禁用用户。 要执行此操作，请在**服务设置**下取消选中**为 Cisco Unified IM and Presence Service 启用用户**（**在关联的 UC 服务配置文件中配置 IM and Presence**）选项

f) 在中央群集上为远程电话群集创建 UC 服务（**用户管理** > **用户设置** > **UC 服务配置**）。

g) 在中央群集上创建服务配置文件，并将其设置为系统的默认服务配置文件，然后将 IM and Presence 节点添加到 IM and Presence 配置文件（**用户管理** > **用户设置** > **服务配置文件**）。

h) 在中央群集上启用 **OAuth with Refresh Login Flow**。 在**企业参数配置**页面，将 **OAuth with Refresh Login Flow** 参数设置为**启用**。

步骤 2 登录到 Cisco Unified IM and Presence 管理控制台，并将枝叶节点添加到 IM and Presence Service 节点（**系统** > **集中式部署**）。

将电话在线状态集成到集中式部署中

在集中式部署中，您可以通过在集中式 IM and Presence 节点中配置多个 SIP 干线，从远程 Unified CM 群集获取电话在线状态信息。

与标准部署中只能将一个 Unified CM 群集配置为 Presence 网关不同，系统在集中式部署中消除了这一限制。 它允许管理员在 IM and Presence 节点中添加多个 CUCM 群集作为 Presence 网关。 这有助于从远程 Unified CM 群集获取电话在线状态信息。

以下程序提供了在远程 Cisco Unified CM 群集以及相应的 IM and Presence 节点中配置 SIP 干线和其他附加设置的步骤。

过程

步骤 1 从 **Cisco Unified CM 管理**用户界面执行以下操作：

a) 选择**设备** > **干线**。 添加一个新的 SIP 干线，并让其指向 IM and Presence 发布方节点作为枝叶群集。

b) 选择**系统** > **服务参数配置**，选择**呼叫管理器**。 在 **IM and Presence 发布干线**字段中，输入您在上一步中添加的枝叶群集干线的 IP 地址。

c) 为群集中可用的所有用户启用 Presence。 您可以在**最终用户配置**页面为所有用户设置**为 Unified CM IM and Presence 启用用户**（**在关联的 UC 服务配置文件中配置 IM and Presence**）复选框，以尝试在后端使用 BAT 文件。

步骤 2 在 **Cisco Unified CM IM and Presence 管理**中，执行以下操作：

a) 在 **Cisco Unified CM IM and Presence 管理**用户界面，选择**Presence** > **Presence 网关**，然后从下拉列表中选择远程 CUCM 群集的 IP 地址。

注释　确保先从 **Presence 网关配置**窗口删除远程 Unified CM 群集，然后再从**集中式部署页面**将其删除。

要在**集中式部署页面**更新远程 CUCM 群集地址，您需要：

- 从 **Presence 网关配置**窗口中删除远程 Unified CM 群集。
- 在**集中式部署页面**上编辑 CUCM 地址。

.

- 在 **Presence 网关配置**窗口中重新添加 Unified CM 群集。

b) 选择**系统** > **安全性** > **传入 ACL**，并通过添加远程 Cisco Unified CM 的 IP 地址创建新的 ACL。

重要事项　此备注适用于 14SU1 及更高版本。

注释　通过添加 IM and Presence 期望从中发布 SIP 消息的所有远程 Cisco Unified CM 发布方和订阅方节点的 IP 地址来创建新的传入 ACL。

c) 选择**系统** > **安全性** > **TLS 对等主题**，并添加远程 Cisco Unified CM 的 IP 地址。

重要事项 此备注适用于 14SU1 及更高版本。

注释 创建 TLS 对等主题并添加 IM and Presence 期望从中发布 SIP 消息的所有远程 Cisco Unified CM 发布方和订阅方节点的 IP 地址。

d) 选择**系统** > **安全性** > **TLS 环境配置**。 在 **TLS 对等主题映射**部分，从**可用的 TLS 对等主题**框选择在上一步中为远程 Cisco Unified CM 创建的 TLS 对等主题，并将其移至**选定的 TLS 对等主题**框。

步骤 3 重新启动所有群集节点上的 **Cisco OAMAgent**。

步骤 4 重新启动 **Cisco Presence Engine**。

注释 在 IM and Presence Service 集中式部署中，您可以将 Cisco Jabber 状态更改为**免打扰 (DND)**。 受控的 Cisco IP 电话和 Jabber 设备上会反映相同的状态。 但是，如果是共享线路，在集中式部署中使用同一目录号码 (DN) 配置了多台设备，DND 状态更改不会反映。

集中式部署相互作用和限制

功能	互动
ILS 中枢群集	如果 ILS 中枢群集关闭，并且存在多个电话群集，则中央群集功能将不起作用。
ILS 部署	如果您在部署 IM and Presence 中央群集的同时部署 ILS，只能在电话群集中部署 ILS。 您不能在 IM and Presence 中央群集的 Cisco Unified Communications Manager 实例上部署 ILS。 此实例仅用于设置，不处理电话。
多样的在线状态	在集中式部署中，用户多样的在线状态由 Cisco Jabber 计算。 仅当用户登录到 Jabber 时，才会显示用户电话的在线状态。
Unified Communications Manager 群集状态	在集中式部署中，Unified Communications Manager 群集状态将显示为**已针对 OAuth 刷新登录同步**。 此功能从 11.5(1)SU3 开始可用。 将 Unified Communications Manager 群集添加到 11.5(1)SU3 或更早版本时，群集状态在 Cisco Unified CM IM and Presence 管理的**系统** > **集中式部署**下将显示为“未同步”，因为它不支持 OAuth 刷新登录。 而这些群集与使用 SSO 或 LDAP 目录凭证的集中式 IM and Presence Service 部署兼容。 **注释** 对 Cisco Jabber 用户登录没有任何功能影响。

第 11 章

配置高级路由

- 高级路由概述， 第 117 页
- 高级路由前提条件， 第 118 页
- 高级路由配置任务流程， 第 118 页

高级路由概述

配置高级路由可确定系统如何建立以下类型的连接：

- 群集内 IM and Presence Service 节点之间的群集内连接。
- IM and Presence Service 群集间共享相同 Presence 域的群集间连接。
- 用于不同 Presence 域之间的联合连接的 SIP 静态路由。 静态路由是一个固定路径，优先于动态路由。

群集内和群集间连接

有两种模式来建立群集间和群集内连接：

- 多播 DNS (MDNS) — MDNS 路由使用 DNS 记录来设置节点之间的连接。 当群集中的所有节点都在同一多播域中时，您可以使用 MDNS 路由。
- 路由器到路由器（默认选项）—路由器到路由器使用IP地址和用户信息动态配置节点之间的连接。 当群集中的节点不在同一个多播域中时，或者当它们位于不同的子网中时，请使用路由器到路由器连接。

注释 思科建议使用 MDNS 路由，因为它可以无缝支持新的 XCP 路由器加入 XCP 路由交换矩阵。

高级路由前提条件

在配置路由之前，请确保您的系统满足以下要求。 要求取决于您想要使用哪种类型的路由方法：MDNS 路由或者路由器到路由器：

MDNS 路由前提条件

须满足以下前提条件：

- 必须已在 IOS 网络中配置多播 DNS。 当网络中禁用多播 DNS 后，MDNS 数据包无法到达群集中的其他节点。 在一些网络中，多播是默认启用的，或在网络的某个区域中启用。 例如，可在包含形成群集的节点的区域中启用它。 在这些网络中，无需执行任何额外的配置即可使用MDNS路由。 如果网络中已禁用多播 DNS，则必须更改网络设备的配置来使用 MDNS 路由。
- 请确保所有节点都在同一多播域中。

路由器到路由器前提条件

如果网络中有 DNS，可以使用与群集节点名称相同的 IP 地址、主机名或 FQDN。 但是，如果在网络中没有 DNS，则必须为节点名称使用 IP 地址。

如果需要重置您的节点名称以使用 IP 地址，请参阅指南《为 *Cisco Unified Communications Manager* 和 *IM and Presence Service* 更改 *IP* 地址和主机名》的“节点名称更改”主题，网址：http://www.cisco.com/c/en/us/support/%20unified-communications/unified-communications-manager-callmanager/%20products-maintenance-guides-list.html。

高级路由配置任务流程

过程

	命令或操作	目的
步骤 1	配置路由通信方法， 第 119 页	路由通信类型决定 IM and Presence Service 用于在群集节点之间建立路由器连接的路由方法。 对于单节点 IM and Presence Service 部署，建议将路由通信类型保留为默认设置。
步骤 2	重新启动 Cisco XCP 路由器， 第 120 页	如果您编辑了路由通信类型，必须重新启动 Cisco XCP 路由器。
步骤 3	配置安全的路由器到路由器通信， 第 120 页.	可选。 如果已配置路由器到路由器通信，则可以在同一群集或不同群集中的 XMPP 路由器之间配置安全 TLS 连接。

	命令或操作	目的
		注释　仅当 IM and Presence Service 在不安全的网络上运行时，才应启用此选项，因为此选项可能会降低性能
步骤 4	配置群集 ID，第 121 页	如果使用 MDNS 路由，请确认群集中的所有节点都共享群集 ID，且值对于每个群集而言都是唯一。 如果需要，您可以执行此程序以更新群集 ID。
步骤 5	配置在线状态更新的限流速率，第 121 页	可选。 配置发送到 Cisco XCP 路由器的可用性（在线状态）更改速率（每秒消息数）。 当 IM and Presence Service 限制可用性（在线状态）更改速率以满足配置的值时，此设置有助于防止过载。
步骤 6	配置静态路由，第 122 页	如果想要配置静态路由，请完成以下任务。

配置路由通信方法

路由通信类型决定 IM and Presence Service 用于在群集节点之间建立路由器连接的路由方法。 对于单节点 IM and Presence Service 部署，建议将路由通信类型保留为默认设置。

注意　必须先配置路由通信类型，然后再完成群集配置，开始接受进入 IM and Presence Service 部署的用户流量。

开始之前

如果要使用 MDNS 路由，必须在整个 IOS 网络中启用 MDNS。

过程

步骤 1 在 IM and Presence 数据库发布方节点上，登录到 Cisco Unified CM IM and Presence 管理。

步骤 2 选择**系统** > **服务参数**。

步骤 3 从**服务器**下拉列表框中选择 IM and Presence Service 节点。

步骤 4 从**服务**下拉列表框中选择 **Cisco XCP 路由器**

步骤 5 在 **XCP 路由器全局设置**（**群集范围**）下，为**路由通信类型**服务参数选择一个路由类型：

- **多播 DNS (MDNS)** — 如果群集中的节点在同一多播域中，选择此方法。

- **路由器到路由器（自动）**— 如果群集中的节点不在同一多播域中，选择此方法。 这是默认设置。

  注释　当您使用路由器到路由器连接时，在 IM and Presence Service 建立 XCP 路由交换矩阵时，您的部署将产生额外的性能开销。

步骤 6 单击**保存**。

下一步做什么

如果您编辑了此设置，必须 重新启动 Cisco XCP 路由器，第 120 页

重新启动 Cisco XCP 路由器

如果您编辑了路由通信类型，请重新启动 Cisco XCP 路由器服务

开始之前

配置路由通信方法，第 119 页

过程

步骤 1 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 网络服务**。

步骤 2 从**服务器**列表选择要重新激活服务的节点并单击**前往**。

步骤 3 在 **IM and Presence Service** 区域选择 **Cisco XCP 路由器**。

步骤 4 单击**重新启动**。

下一步做什么

如果您配置了路由器到路由器路由，配置安全的路由器到路由器通信，第 120 页。

如果您配置了 MDNS 路由，配置群集 ID，第 121 页。

配置安全的路由器到路由器通信

如果有**路由器到路由器**通信，可以执行此可选程序，以在同一群集或不同群集中的 XMPP 路由器之间配置安全 TLS 连接。 IM and Presence Service 会自动在群集中和跨群集复制 XMPP 证书，并将其作为 XMPP 信任证书。

注释　仅当 IM and Presence Service 在不安全的网络上运行时，才应启用此选项，因为此选项可能会降低性能。

过程

步骤 1 从 Cisco Unified CM IM and Presence 管理中，选择**系统** > **安全性** > **设置**。

步骤 2 选中**启用 XMPP 路由器-路由器安全模式**复选框。

步骤 3 单击**保存**。

下一步做什么

配置在线状态更新的限流速率，第 121 页

配置群集 ID

如果使用 MDNS 路由，请确认群集中的所有节点都共享**群集 ID**，且值对于每个群集而言都是唯一。如果需要，您可以执行此程序以更新**群集 ID**。

注释 安装时，系统会将默认的唯一**群集 ID** 分配到每个 IM and Presence Service 群集。 除非必须更改，否则思科建议您保留默认设置值。

过程

步骤 1 在 IM and Presence Service 数据库发布方节点上，登录到 Cisco Unified CM IM and Presence 管理。

步骤 2 选择 **Presence** > **设置** > **标准配置**。

步骤 3 检查**群集 ID** 字段中的值。 如果需要编辑 ID，输入新值。

IM and Presence Service 不允许在群集 ID 值中使用下划线字符 (_)。 确保群集 ID 值中不包含此字符。

步骤 4 单击**保存**。
如果编辑了**群集 ID**，新设置将复制到群集的所有节点。

下一步做什么

配置在线状态更新的限流速率，第 121 页

配置在线状态更新的限流速率

此可选程序用于配置发送到 Cisco XCP 路由器的可用性（在线状态）更改速率（每秒消息数）。 当 IM and Presence Service 限制可用性（在线状态）更改速率以满足配置的值时，此配置可帮助防止过载。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 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 IM and Presence Service 节点。

步骤 3 从**服务**下拉列表框选择 **Cisco Presence Engine**。

步骤 4 在**群集范围参数（适用于所有服务器的参数）**部分，编辑**在线状态更改限流速率**服务参数。 有效范围为 10-100，默认设置为 50。

步骤 5 单击**保存**。

下一步做什么

如果想要为联合连接配置 SIP 静态路由，配置静态路由 ，第 122 页。

配置静态路由

过程

	命令或操作	目的
步骤 1	配置 SIP 代理服务器设置 ，第 122 页	配置 SIP 代理服务器设置。 对于 WAN 部署，思科建议您在 IM and Presence Service 上启用 TCP 方法事件路由。
步骤 2	在 IM and Presence Service 上配置路由嵌入模板 ，第 123 页	如果您的静态路由包含嵌入的通配符，您必须配置路由嵌入模板。
步骤 3	在 IM and Presence Service 上配置静态路由 ，第 124 页	配置静态路由设置。

配置 SIP 代理服务器设置

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择 **Presence** > **路由** > **设置**。

步骤 2 为“方法/事件路由状态”选择**打开**。 对于 WAN 部署，思科建议您在 IM and Presence Service 上配置 TCP 方法事件路由。

步骤 3 为“首选代理服务器”选择**默认 SIP 代理 TCP 监听程序**。

步骤 4 单击**保存**。

在 IM and Presence Service 上配置路由嵌入模板

如果您的静态路由包含嵌入的通配符，您必须配置路由嵌入模板。

过程

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

步骤 2 从**服务器**下拉列表中选择 IM and Presence Service 节点。

步骤 3 从**服务**下拉列表中选择 **Cisco SIP Proxy**。

步骤 4 在**路由参数**（**群集范围**）下，在**路由嵌入模板**字段中输入您的模板。 您最多可以定义五个模板。 单个路由嵌入模板可以定义的静态路由没有数量限制。

步骤 5 单击**保存**。

下一步做什么

在 IM and Presence Service 上配置静态路由 ，第 124 页

启用路由的模板

必须为包含嵌入式通配符的任何静态路由模式定义路由嵌入模板。 路由嵌入模板包含前导数字、数字长度和嵌入式通配符位置的相关信息。 定义路由嵌入模板前，请考虑我们在下方提供的示例模板。

当定义路由嵌入模板时，“.” 后的字符必须与静态路由中的实际电话数字匹配。 在下面的示例路由嵌入模板中，我们用 “x” 表示这些字符。

示例路由嵌入模板 A

路由嵌入模板：`74..78xxxxx*`

使用此模板，IM and Presence Service 将启用此组使用嵌入式通配符的静态路由：

表 *13:* 包含嵌入通配符的静态路由集 - 模板 *A*

目标模式	下一跃点目标
74..7812345*	1.2.3.4:5060
74..7867890*	5.6.7.8.9:5060
74..7811993*	10.10.11.37:5060

使用此模板，IM and Presence Service 将不会启用这些静态路由条目：

- 73..7812345*（初始字符串不是模板定义的“74”）
- 74..781*（目标模式数字长度与模板不符）
- 74…7812345*（通配符数与模板不符）

示例路由嵌入模板 B

路由嵌入模板：`471…xx*`

使用此模板，IM and Presence Service 将启用此组使用嵌入式通配符的静态路由：

表 *14:* 包含嵌入通配符的静态路由集 - 模板 *B*

目标模式	下一跃点目标
471…34*	20.20.21.22
471…55*	21.21.55.79

使用此模板，IM and Presence Service 将不会启用这些静态路由条目：

- 47…344*（初始字符串不是模板定义的“471”）
- 471…4*（字符串长度与模板不符）
- 471.450*（通配符数与模板不符）

在 IM and Presence Service 上配置静态路由

此程序用于设置您的静态路由。 有关这些字段及其设置的帮助，请参阅联机帮助。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中选择**路由** > **静态路由**。
步骤 2 单击**新增**。
步骤 3 在**目标模式**中输入路由模式。
步骤 4 在**下一跃点**字段中，输入下一跃点服务器的 IP 地址、FQDN 或主机名。
步骤 5 在**下一跃点端口**下，输入下一跃点服务器的目标端口。 默认端口为 5060。
步骤 6 从**路由类型**下拉列表中，选择路由类型：**用户**或**域**。
步骤 7 从**协议类型**下拉列表框中，选择静态路由的协议：**TCP**、**UDP** 或 **TLS**。
步骤 8 在**静态路由配置**窗口完成其余字段的设置。
步骤 9 单击**保存**。

静态路由参数设置

下表列出了可为 IM and Presence Service 配置的静态路由参数设置。

表 *15: IM and Presence Service* 的静态路由参数设置

字段	说明
目标模式	此字段指定来电号码的模式，最多包含 255 个字符。 SIP 代理仅允许 100 个静态路由使用相同的路由模式。 如果超过此限制，IM and Presence Service 会记录错误。 使用通配符 您可以使用 “.” 作为单个字符的通配符，使用 “*” 作为多个字符的通配符。 IM and Presence Service 支持在静态路由中嵌入“.”通配符字符。 但是，您必须为包含嵌入通配符的静态路由定义路由嵌入模板。 任何包含嵌入通配符的静态路由均须至少与一个路由嵌入模板匹配。 有关定义路由嵌入模板的信息，请参阅下文“相关主题”部分列出的路由嵌入模板主题。 对于电话： • 点号可以放在模式末尾，也可以嵌入到模式中。 如果在模式中嵌入点号，您必须创建与模式匹配的路由嵌入模板。 • 星号只能放在模式末尾。 对于 IP 地址和主机名： • 您可以在主机名中使用星号。 • 点号在主机名中作为文字值。 转义星号序列 * 与文字 * 相匹配，可放在任意位置。
说明	指定特定静态路由的说明，最多包含 255 个字符。
下一跃点	指定目标（下一跃点）的域名或 IP 地址，可以是完全限定域名 (FQDN)，也可以是点分 IP 地址。 IM and Presence Service 支持基于 DNS SRV 的呼叫路由。 要将 DNS SRV 指定为静态路由的下一跃点，请将此参数设置为 DNS SRV 名称。
下一跃点端口	指定目标（下一跃点）的端口号。 默认端口为 5060。 IM and Presence Service 支持基于 DNS SRV 的呼叫路由。 要将 DNS SRV 指定为静态路由的下一跃点，请将下一跃点端口参数设置为 0。
路由类型	指定路由类型：“用户”或“域”。 默认值为用户。 例如，在 SIP URI "sip:19194762030@myhost.com" 请求中，用户部分是 "19194762030"，主机部分是 "myhost.com"。 如果您选择“用户”作为路由类型，IM and Presence Service 对路由 SIP 流量使用用户部分值 "19194762030"。 如果选择“域”作为路由类型，IM and Presence Service 将对路由 SIP 流量使用 "myhost.com"。

字段	说明
协议类型	指定此路由的协议类型：TCP、UDP 或 TLS。 默认值为 TCP。
优先	指定路由优先级。 值越低，表示优先级越高。 默认值为 1。 值的范围：1-65535
重量	指定路由权重。 仅当两个或多个路由的优先级相同时，才使用此参数。 值越高，表示路由的优先级越高。 值的范围：1-65535 **示例**：观察下面三个路由及其关联的优先级和权重： • 1, 20 • 1, 10 • 2, 50 在本例中，已按正确的顺序列出静态路由。 优先级路由取决于最低值优先级，即 1。如果两个路由共享同一个优先级，则最大值的权重参数决定优先级路由。 在此示例中，IM and Presence Service 将 SIP 流量定向到使用优先值 1 配置的两个路由，并且根据权重分配流量；权重为 20 的路由将接收两次等于权重为 10 的路由的流量。请注意，在此示例中，如果 IM and Presence Service 尝试了两个优先级为 1 的路由且均失败，它将仅尝试使用优先级为 2 的路由。
允许不太特定的路由	指定路由可以不具体特定。 默认设置为“打开”。
服务中	指定此路由是否已经停用。 指定此路由是否已经停用。
“阻止路由”复选框	选中即可阻止静态路由。 默认设置为“不阻止”。

第 12 章

配置证书

- 证书概述 ， 第 127 页
- 证书前提条件 ， 第 129 页
- 与 Cisco Unified Communications Manager 交换证书 ， 第 129 页
- 在 IM and Presence Service 上安装证书颁发机构 (CA) 根证书链 ， 第 132 页
- 将证书上传到 IM and Presence Service ， 第 134 页
- 生成 CSR ， 第 138 页
- 生成自签名证书 ， 第 140 页
- 证书监控任务流程 ， 第 142 页

证书概述

证书用于保护身份并在 IM and Presence Service 和另一个系统之间建立信任关系。 您可以使用证书将 IM and Presence Service 连接到 Cisco Unified Communications Manager、Cisco Jabber 客户端或任何外部服务器。 没有证书，就无法知道是否使用了流氓 DNS 服务器，或者您是否被路由到了另一台服务器。

IM and Presence Service 可以使用的证书主要有两类：

- 自签名证书 — 自签名证书由颁发证书的同一服务器签名。 在企业内部，您可以使用自签名证书与另一个内部系统连接，不过有一个前提条件：这些连接都不通过不安全的网络传输。 例如，IM and Presence Service 可能会为到 Cisco Unified Communications Manager 的内部连接生成自签名证书。

- CA 签名证书 — 这些是由第三方证书颁发机构 (CA) 签名的证书。 它们可以由控制服务器/服务证书有效性的公共 CA（例如 Verisign、Entrust 或 Digicert）或服务器（例如 Windows 2003、Linux、Unix、IOS）签名。 CA 签名证书比自签名证书更安全，通常用于 WAN 连接。 例如，与另一个企业的联合连接或使用 WAN 连接的群集间对等配置将要求 CA 签名证书与外部系统建立信任关系。

CA 签名证书比自签名证书更安全。 通常，自签名证书被认为适用于内部连接，但对于任何 WAN 连接或通过公共 Internet 的连接，您应使用 CA 签名证书。

多服务器证书

IM and Presence Service 还支持某些系统服务的多服务器 SAN 证书。 为多服务器证书生成证书签名请求 (CSR) 时，一旦将证书上传到任何群集节点，生成的多服务器证书及其关联的签名证书链将自动分发到所有群集节点。

IM and Presence Service 中的证书类型

在 IM and Presence Service 中，不同的系统组件需要不同类型的证书。 下表介绍 IM and Presence Service 上的客户端和服务需要的不同证书。

注释 如果证书名称以 -ECDSA 结尾，证书/密钥类型是椭圆曲线 (EC)。 否则，为 RSA。

表 *16:* 证书类型和服务

证书类型	服务	证书信任存储库	多服务器支持	备注
tomcat、 tomcat-ECDSA	Cisco 客户端配置文件代理、 Cisco AXL Web 服务、 Cisco Tomcat	tomcat- trust	是	在 IM and Presence Service 的客户端验证过程中显示给 Cisco Jabber 客户端。 导航 Cisco Unified CM IM and Presence 管理用户界面时显示给 Web 浏览器。 关联的信任存储在使用配置的 LDAP 服务器验证用户凭证时用于验证 IM and Presence Service 建立的连接。
ipsec		ipsec-trust	否	在 IPSec 策略启用时使用。
cup、 cup-ECDSA	Cisco SIP Proxy、 Cisco Presence Engine	cup-trust	否	向 Expressway-C 颁发证书，以获取 SIP 联合用户的 IM and Presence。 IM and Presence 代理可用作客户端和服务器。 Presence Engine 会将这些证书用于 Exchange/Office 365 通信以获取日历在线状态。 Presence Engine 只能用作客户端。

证书类型	服务	证书信任存储库	多服务器支持	备注
cup-xmpp、 cup-xmpp-ECDSA	Cisco XCP 连接管理器、 Cisco XCP Web 连接管理器、 Cisco XCP 目录服务、 Cisco XCP 路由器服务	cup-xmpp-trust	是	创建 XMPP 会话时显示给 Cisco Jabber 客户端、第三方 XMPP 客户端或基于 CAXL 的应用程序。 关联的信任存储在对第三方 XMPP 客户端执行 LDAP 搜索操作时用于验证 Cisco XCP 目录服务建立的连接。 如果“路由通信类型”设置为“路由器-路由器”，Cisco XCP 路由器服务在 IM and Presence Service 服务器之间建立安全连接时将使用关联的信任存储。
cup-xmpp-s2s、 cup-xmpp-s2s-ECDSA	Cisco XCP XMPP 联合连接管理器	cup-xmpp-trust	是	连接外部联合的 XMPP 系统时显示给 XMPP 域间联合。

证书前提条件

在 Cisco Unified Communications Manager 上配置以下项目：

- 配置 IM and Presence Service 的 SIP 干线安全性配置文件。
- 配置 IM and Presence Service 的 SIP 干线：
  - 将安全性配置文件与 SIP 干线关联。
  - 通过 IM and Presence Service 证书的主题通用名称 (CN) 配置 SIP 干线。

与 Cisco Unified Communications Manager 交换证书

完成这些任务，以与 Cisco Unified Communications Manager 交换证书。

注释 系统会在安装过程中自动处理 Cisco Unified Communications Manager 与 IM and Presence Service 之间的证书交换。 但是，如果您需要手动完成证书交换，请完成以下任务。

过程

	命令或操作	目的
步骤 1	将 Cisco Unified Communications Manager 证书导入到 IM and Presence Service，第 130 页	将证书从 Cisco Unified Communications Manager 导入到 IM and Presence Service。

	命令或操作	目的
步骤 2	从 IM and Presence Service 下载证书，第 131 页	从 IM and Presence Service 下载证书。 证书必须导入到 Cisco Unified Communications Manager。
步骤 3	将 IM and Presence 证书导入 Cisco Unified Communications Manager，第 131 页	要完成证书交换，请将 IM and Presence Service 证书导入到 Cisco Unified Communications Manager 的 CallManager 信任存储区中。

将 Cisco Unified Communications Manager 证书导入到 IM and Presence Service

此程序用于将证书从 Cisco Unified Communications Manager 导入到 IM and Presence Service。

过程

步骤 1 在 **Cisco Unified CM IM and Presence** 管理中，选择系统 > 安全性 > 证书导入工具。

步骤 2 从证书信任存储菜单中选择 **IM and Presence (IM/P)** 服务信任。

步骤 3 输入 Cisco Unified Communications Manager 节点的 IP 地址、主机名或 FQDN。

步骤 4 输入用来与 Cisco Unified Communications Manager 节点通信的端口号。

步骤 5 单击提交。

注释 “证书导入工具”完成导入操作后，它会报告是否已经成功连接到 Cisco Unified Communications Manager，以及是否已成功从 Cisco Unified Communications Manager 下载证书。 如果“证书导入工具”报告失败，请参阅在线帮助获取建议操作。 您也可以通过选择 **Cisco Unified IM and Presence** 操作系统管理 > 安全 > 证书管理来手动导入证书。

注释 根据协商的 TLS 密码，证书导入工具将下载基于 RSA 的证书或基于 ECDSA 的证书。

步骤 6 重新启动 Cisco SIP Proxy 服务：

a) 在 Cisco Unified IM and Presence 功能配置中，选择 IM and Presence 上的工具 > 控制中心 - 功能服务。

b) 从服务器下拉列表框中选择 IM and Presence Service 群集节点，然后单击前往。

c) 选择 **Cisco SIP Proxy** 并单击重新启动。

下一步做什么

从 IM and Presence Service 下载证书，第 131 页

从 IM and Presence Service 下载证书

此程序用于从 IM and Presence Service 下载证书。 证书必须导入到 Cisco Unified Communications Manager。

过程

步骤 1 在 **Cisco Unified IM and Presence 操作系统管理**中，选择 IM and Presence 上的**安全性** > **证书管理**。

步骤 2 单击**查找**。

步骤 3 选择 `cup.pem` 文件。

注释 `cup-ECDSA.pem` 也是一个可用的选项。

步骤 4 单击**下载**并将文件保存到本地计算机。

提示 忽略 IM and Presence Service 所显示的与访问 cup.csr 文件有关的任何错误；CA（证书机构）无需签署您与 Cisco Unified Communications Manager 交换的证书。

下一步做什么

将 IM and Presence 证书导入 Cisco Unified Communications Manager，第 131 页

将 IM and Presence 证书导入 Cisco Unified Communications Manager

要完成证书交换，请将 IM and Presence Service 证书导入到 Cisco Unified Communications Manager 的 CallManager 信任存储区中。

开始之前

从 IM and Presence Service 下载证书，第 131 页

过程

步骤 1 登录到 Cisco Unified 操作系统管理。

步骤 2 选择**安全性** > **证书管理**

步骤 3 单击**上传证书**。

步骤 4 从“证书名称”菜单中选择 **Callmanager-trust**。

步骤 5 **浏览**并选择之前从 IM and Presence Service 下载的证书。

步骤 6 单击**上传文件**。

步骤 7 重新启动 Cisco CallManager 服务：

a) 在 Cisco Unified 功能配置中，选择**工具** > **控制中心 - 功能服务**。

b) 从**服务器**下拉列表框中选择一个 Cisco Unified Communications Manager 群集节点并单击**前往**。
c) 选择 **Cisco CallManager** 服务并单击**重新启动**。

在 IM and Presence Service 上安装证书颁发机构 (CA) 根证书链

要在 IM and Presence Service 中使用由第三方证书颁发机构 (CA) 签名的证书，您必须首先在 IM and Presence Service 上安装该 CA 的根证书信任链。

过程

	命令或操作	目的
步骤 1	上传 CA 根证书链，第 132 页	此程序用于将 CA 根证书链从第三方证书颁发机构上传到 IM and Presence Service。
步骤 2	重新启动思科群集间同步代理服务，第 133 页	上传证书后，重新启动思科群集间同步代理服务。
步骤 3	验证 CA 证书已同步到其他群集，第 133 页	确认您的CA证书链已复制到所有对等群集。

上传 CA 根证书链

此程序用于将证书链从签名的证书颁发机构 (CA) 上传到 IM and Presence 数据库发布方节点。 链可能包含一连串的多个证书，每个证书签署后续证书：

- 根证书 > 中间 1 证书 > 中间 2 证书

过程

步骤 1 在 IM and Presence 数据库发布方节点上，登录到 Cisco Unified IM and Presence 操作系统管理。
步骤 2 选择**安全性** > **证书管理**。
步骤 3 单击**上传证书/证书链**。
步骤 4 从**证书名称**下拉列表中选择以下选项之一：

- 如果要上传 CA 签名的 tomact 证书，选择 **tomcat-trust**
- 如果要上传 CA 签名的 cup-xmpp 证书或 CA 签名的 cup-xmpp-s2s，选择 **cup-xmpp-trust**

步骤 5 输入签名证书的**说明**。
步骤 6 单击**浏览**找到根证书的文件。
步骤 7 单击**上传文件**。

步骤 8 使用**上传证书/证书链**窗口以相同方式上传每个中间证书。对于每个中间证书，必须输入链中上一个证书的名称。

下一步做什么

重新启动思科群集间同步代理服务，第 133 页

重新启动思科群集间同步代理服务

将根证书和中间证书上传到 IM and Presence 数据库发布方节点后，必须在该节点上重新启动思科群集间同步代理服务。 此重新启动可确保 CA 证书立即同步到所有其他群集。

过程

步骤 1 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 网络服务**。

步骤 2 从**服务器**下拉列表框中选择要导入证书的 IM and Presence Service 节点，然后单击**前往**。

注释 您可以使用以下命令从命令行界面重新启动思科群集间同步代理服务：`utils service restart Cisco Intercluster Sync Agent`。

步骤 3 选择**思科群集间同步代理**服务并单击**重新启动**。

下一步做什么

验证群集间同步，第 136 页

验证 CA 证书已同步到其他群集

思科群集间同步代理服务重新启动后，必须确保 CA 证书已正确同步到其他群集。 在其他每个 IM and Presence 数据库发布方节点上完成以下步骤。

注释 以下程序中的信息也适用于以 `-ECDSA` 结尾的证书。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**诊断** > **系统故障诊断程序**。

步骤 2 在**群集间故障诊断程序**中，查找测试**验证每个启用 TLS 的群集间对等成员是否已成功交换安全证书**并确认该测试已通过。

步骤 3 如果测试显示错误，记下群集间对等成员的 IP 地址；该地址应引用您上传 CA 证书的群集。 继续以下步骤以解决该问题。

步骤 4 选择 **Presence** > **群集间**，然后单击与**系统故障诊断程序**页面上标识的群集间对等节点关联的链接。

步骤 5 单击**强制手动同步**。

步骤 6 留出 60 秒时间以便“群集间对等成员状态”面板自动刷新。

步骤 7 验证**证书状态**字段显示“连接是安全的”。

步骤 8 如果证书状态字段没有显示“连接是安全的”，在 IM and Presence 数据库发布方节点上重新启动思科群集间同步代理服务，然后重复步骤 5 至 7。

- 从管理 CLI 运行以下命令以重新启动服务：utils service restart Cisco Intercluster Sync Agent
- 或者，可以从 Cisco Unified IM and Presence 功能配置 GUI 重新启动此服务。

步骤 9 验证**证书状态**现在显示为“连接是安全的”。 这意味着群集之间的群集间同步已正确建立，并且您上传的 CA 证书已同步到其他群集。

下一步做什么

将签名证书上传到每个 IM and Presence Service 节点。

将证书上传到 IM and Presence Service

完成这些任务以将证书上传到 IM and Presence Service。 您可以上传 CA 签名证书或自签名证书。

开始之前

要使用第三方证书颁发机构 (CA) 签名的 CA 签名证书，您必须先在 IM and Presence Service 上安装 CA 的根证书链。 有关详细信息，请参阅：在 IM and Presence Service 上安装证书颁发机构 (CA) 根证书链，第 132 页。

过程

	命令或操作	目的
步骤 1	上传证书，第 135 页	将签名的证书上传到 IM and Presence Service。
步骤 2	重新启动 Cisco Tomcat 服务，第 136 页	（仅 Tomcat 证书）。 重新启动 Cisco Tomcat 服务。
步骤 3	验证群集间同步，第 136 页	（仅 Tomcat 证书）。 对群集内所有受影响的节点重新启动 Cisco Tomcat 服务后，必须验证群集间同步是否正确运行。
步骤 4	在所有节点上重新启动 Cisco XCP 路由器服务，第 137 页	将证书上传到 cup-xmpp 存储区后，在所有群集节点上重新启动 Cisco XMP 路由器。

	命令或操作	目的
步骤 5	重新启动 Cisco XCP XMPP 联合连接管理器服务， 第 137 页	（仅 XMPP 联合）。 将证书上传到 XMPP 联合的 cup-xmpp 存储区后，重新启动 Cisco XCPXMPP 联合连接管理器服务。
步骤 6	在 XMPP 联合安全证书中启用通配符， 第 137 页	（仅 XMPP 联合）。 通过 TLS 将证书上传到 XMPP 的 cup-xmpp 存储区后，必须为 XMPP 安全证书启用通配符。 必需为群聊执行此操作。

上传证书

此程序用于将证书上传到每个 IM and Presence Service 节点。

注释 思科建议您为群集签名所有必需的 tomcat 证书，然后同时上传这些证书。 此过程可缩短恢复群集间通信的时间。

注释 以下程序中的信息也适用于以 `-ECDSA` 结尾的证书。

开始之前

如果证书由 CA 签名，您还必须安装该 CA 的根证书链，否则 CA 签名证书将不受信任。 CA 证书正确同步到所有群集后，您可以将适当的签名证书上传到每个 IM and Presence Service 节点。

过程

步骤 1 在 **Cisco Unified IM and Presence 操作系统管理**中选择**安全性** > **证书管理**。

步骤 2 单击**上传证书/证书链**。

步骤 3 选择**证书用途**。 例如，**tomcat**。

步骤 4 输入签名证书的说明。

步骤 5 单击**浏览**找到要上传的文件。

步骤 6 单击**上传文件**。

步骤 7 对每个 IM and Presence Service 节点重复操作。

下一步做什么

重新启动 Cisco Tomcat 服务。

重新启动 Cisco Tomcat 服务

将 tomcat 证书上传到每个 IM and Presence Service 节点后，必须在每个节点上重新启动 Cisco Tomcat 服务。

过程

步骤 1 登录到管理 CLI。

步骤 2 运行以下命令：`utils service restart Cisco Tomcat`。

步骤 3 对每个节点重复操作。

下一步做什么

验证群集间同步正常运行。

验证群集间同步

对群集内所有受影响的节点重新启动 Cisco Tomcat 服务后，必须验证群集间同步是否正确运行。 在其他群集中的每个 IM and Presence 数据库发布方节点上完成以下步骤。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**诊断** > **系统故障诊断程序**。

步骤 2 在**群集间故障诊断程序**中，查找测试**验证每个启用 TLS 的群集间对等成员是否已成功交换安全证书**并确认该测试已通过。

步骤 3 如果测试显示错误，记下群集间对等成员的 IP 地址；该地址应引用您上传 CA 证书的群集。 继续以下步骤以解决该问题。

步骤 4 选择 **Presence** > **群集间**，然后单击与“系统故障诊断程序”页面上标识的群集间对等节点关联的链接。

步骤 5 单击**强制手动同步**。

步骤 6 选中**同时重新同步对等成员的 Tomcat 证书**复选框，然后单击**确定**。

步骤 7 留出 60 秒时间以便“群集间对等成员状态”面板自动刷新。

步骤 8 验证**证书状态**字段显示“连接是安全的”。

步骤 9 如果**证书状态**字段没有显示“连接是安全的”，在 IM and Presence 数据库发布方节点上重新启动思科群集间同步代理服务，然后重复步骤 5 至 8。

- 从管理 CLI 运行以下命令以重新启动服务：utils service restart Cisco Intercluster Sync Agent。
- 或者，可以从 Cisco Unified IM and Presence 功能配置 GUI 重新启动此服务。

步骤 10 验证证书状态现在显示为“连接是安全的”。 这意味着此群集与证书上传的群集之间的群集间同步现已重新建立。

在所有节点上重新启动 Cisco XCP 路由器服务

将 cup-xmpp 和/或 cup-xmpp-ECDSA 证书上传到每个 IM and Presence Service 节点后，必须在每个节点上重新启动 Cisco XCP 路由器服务。

注释 您也可以从 Cisco Unified IM and Presence 功能配置 GUI 重新启动 Cisco XCP 路由器服务。

过程

步骤 1 登录到管理 CLI。

步骤 2 运行以下命令：utils service restart Cisco XCP Router。

步骤 3 对每个节点重复操作。

重新启动 Cisco XCP XMPP 联合连接管理器服务

将 cup-xmpp-s2s 和/或 cup-xmpp-s2s-ECDSA 证书上传到每个 IM and Presence Service 联合节点后，您必须在每个联合节点上重新启动 Cisco XCP XMPP 联合连接管理器服务。

过程

步骤 1 登录到管理 CLI。

步骤 2 运行以下命令：utils service restart Cisco XCP XMPP Federation Connection Manager。

步骤 3 对每个联合节点重复此过程。

在 XMPP 联合安全证书中启用通配符

要支持 XMPP 联合合作伙伴之间在 TLS 上进行群聊，您必须为 XMPP 安全证书启用通配符。

默认情况下，XMPP 联合安全证书 `cup-xmpp-s2s` 和 `cup-xmpp-s2s-ECDSA` 中包含 IM and Presence Service 部署托管的所有域。 这些在证书中作为主题备选名称 (SAN) 条目添加。 您必须为同一证书内所有托管的域提供通配符。 因此，XMPP 安全证书中必须包含 SAN 条目 “*.example.com”，而不是 SAN 条目 “example.com”。 之所以需要通配符，是因为群聊服务器别名是 IM and Presence Service 系统上其中一个托管域的子域。 例如：“conference.example.com”。

注释 要查看任意节点上的 `cup-xmpp-s2s` 或 `cup-xmpp-s2s-ECDSA` 证书，选择 **Cisco Unified IM and Presence 操作系统管理** > **安全性** > **证书管理**，然后单击 **cup-xmpp-s2s** 或 **cup-xmpp-s2s-ECDSA** 链接。

过程

步骤 1 选择**系统** > **安全设置**。

步骤 2 选中**在 XMPP 联合安全证书中启用通配符**。

步骤 3 单击**保存**。

下一步做什么

您必须在正在运行 Cisco XMPP Federation Connection Manager 服务且已启用 XMPP 联合的群集中所有节点上重新生成 XMPP 联合安全证书。 必须在所有 IM and Presence Service 群集上启用此安全设置，以支持基于 TLS 的 XMPP 联合群聊。

生成 CSR

此程序用于生成证书签名请求 (CSR)。 您需要将 CSR 提交到第三方 CA，以便他们可以为您提供 CA 签名的证书。

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 单击**生成 CSR** 按键。 屏幕将弹出**生成证书签署请求**窗口。

步骤 3 从**证书用途**下拉列表中，选择正在生成的证书的类型。

步骤 4 从**分发**下拉列表中，选择 IM and Presence 服务器。 对于多服务器证书，选择**多服务器 (SAN)**。

步骤 5 输入**密钥长度**和**哈希算法**。

步骤 6 填写剩余的字段并单击**生成**。

步骤 7 将 CSR 下载到本地计算机：

a) 单击**下载 CSR**。

b) 从**证书目的**下拉列表中选择证书名称。

c) **下载 CSR**

下一步做什么

将 CSR 提交至第三方证书颁发机构，以便他们可以签发 CA 签名的证书。

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 *17: 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 *18: 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。

生成自签名证书

此程序用于生成证书自签名证书。

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 单击**生成自签名证书**。 屏幕将弹出**生成新的自签名证书**窗口。

步骤 3 从**证书用途**下拉列表中，选择正在生成的证书的类型。

步骤 4 从**分发**下拉列表中，输入服务器的名称。

步骤 5 选择适当的**密钥长度**。

步骤 6 从**哈希算法**中选择加密算法。 例如，SHA256。

步骤 7 单击**生成**。

从 IM and Presence Service 删除自签名信任证书

为支持相同群集中不同节点配置功能交叉导航，IM and Presence Service 与 Cisco Unified Communications Manager 间的 Cisco Tomcat 服务信任存储区将自动同步。

如果您用 CA 签名证书替换了初始自签名信任证书，则初始自签名信任证书将保留在服务信任库中。您可以执行此程序以删除 IM and Presence Service 和 Cisco Unified Communications Manager 节点上的自签名证书。

开始之前

重要事项 如果您添加了 CA 签名的证书，请确保等待 30 分钟让思科群集间同步代理服务在给定 IM and Presence Service 节点上执行其定期清理任务。

过程

步骤 1 在 Cisco Unified IM and Presence 操作系统管理中选择**安全性** > **证书管理**。

步骤 2 单击**查找**。

此时将显示**证书列表**。

注释 证书名称由两部分组成，服务名称和证书类型。 例如，tomcat-trust 中 tomcat 是服务，而 trust 是证书类型。

您可删除的自签信任证书包括：

- Tomcat 和 Tomcat-ECDSA — tomcat-trust
- Cup-xmpp 和 Cup-xmpp-ECDSA — cup-xmpp-trust
- Cup-xmpp-s2s 和 Cup-xmpp-s2s-ECDSA — cup-xmpp-trust
- Cup 和 Cup-ECDSA — cup-trust
- Ipsec — ipsec-trust

步骤 3 单击指向您希望删除的自签信任证书的链接。

重要事项 确保您已为与服务信任存储区相关联的服务配置 CA 签署的证书。

此时将显示一个新窗口，其中将显示证书的详细信息。

步骤 4 单击**删除**。

注释 仅在您有权限删除该证书时，**删除**按键才会显示。

步骤 5 为群集中和任何跨群集对等机上的各个 IM and Presence Service 节点重复上述程序，以确保跨部署完全删除不需要的自签信任证书。

下一步做什么

如果服务是 Tomcat，则您必须在 Cisco Unified Communications Manager 节点上检查 IM and Presence Service 节点的自签 tomcat 信任证书。 请参阅从 Cisco Unified Communications Manager 删除自签 Tomcat 信任证书，第 141 页。

从 Cisco Unified Communications Manager 删除自签 Tomcat 信任证书

Cisco Unified Communications Manager 服务信任存储区中有一个针对群集中各个节点的自签 tomcat 信任证书。 这些是您可从 Cisco Unified Communications Manager 节点中删除的唯一证书。

注释 以下程序中的信息也适用于 `-EC` 证书。

开始之前

确保您已使用 CA 签署证书配置群集的 IM and Presence Service 节点，并等待 30 分钟让证书传播到 Cisco Unified Communications Manager 节点。

过程

步骤 1 在 **Cisco Unified 操作系统管理**中选择**安全性** > **证书管理**。

此时将显示**证书列表**窗口。

步骤 2 要筛选搜索结果，请从下拉列表选择**证书**和**始于**，然后在空字段输入 tomcat 信任。 单击**查找**。

证书列表窗口将展开并列出 tomcat 信任证书。

步骤 3 识别其名称中包含 IM and Presence 服务节点主机名或 FQDN 的链接。这些是与此服务和 IM and Presence 服务节点相关联的自签证书。

步骤 4 单击指向 IM and Presence Service 节点上自签 tomcat 信任证书的链接。

此时将显示一个新窗口，其中将显示 tomcat 信任证书的详细信息。

步骤 5 确保“Issuer Name CN=”与“Subject Name CN=”值相匹配，从而在“证书详细信息”内确认。

步骤 6 如果您确认这是一个自签名证书，并确定 CA 签名证书已经传播到 Cisco Unified Communications Manager 节点，请单击**删除**。

注释 **删除**按键仅针对您拥有删除权限的证书显示。

步骤 7 为群集中 IM and Presence Service 节点重复步骤 4、5 和 6。

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 142 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 143 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 143 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**。

第 13 章

配置安全设置

- 安全概述， 第 145 页
- 安全性设置配置任务流程 ， 第 145 页

安全概述

本章将介绍在 IM and Presence Service 上配置安全设置的程序。 在 IM and Presence Service 上，您可以配置安全 TLS 连接并启用增强的安全设置，例如 FIPS 模式。

IM and Presence Service 与 Cisco Unified Communications Manager 共享一个平台。 有关如何在 Cisco Unified Communications Manager 中配置安全性的信息，请参阅《*Cisco Unified Communications Manager* 安全指南》。

安全性设置配置任务流程

以下可选任务用于通过 IM and Presence Service 设置安全性。

过程

	命令或操作	目的
步骤 1	创建登录提示， 第 146 页	创建用户在登录任何 IM and Presence Service 界面时必须确认的登录提示。
步骤 2	配置安全 XMPP 连接 ， 第 146 页	完成这些任务以配置 XMPP 安全性。
步骤 3	配置 TLS 对等主题， 第 147 页	如果想要设置TLS对等节点，配置这些任务。
步骤 4	配置 TLS 上下文， 第 148 页	为您的 TLS 对等节点配置 TLS 环境和 TLS 密码。
步骤 5	FIPS 模式， 第 148 页	如果您希望部署符合 FIPS 标准，可以启用 FIPS 模式。 为增强安全性，您还可以启用“强化安全性”模式和“通用合规性”模式。

创建登录提示

您可以创建用户在登录任何 IM and Presence Service 界面时确认的提示。 您可以使用任何文本编辑器创建一个 .txt 文件，包括希望用户了解的重要通知，然后将它上传到 Cisco Unified IM and Presence 操作系统管理页面。

此提示随后将于用户登录前在所有 IM and Presence Service 界面上显示，向用户通知重要信息，包括法律警告和义务。 以下界面将在用户登录前后显示此横幅：Cisco Unified CM IM and Presence 管理、Cisco Unified IM and Presence 操作系统管理、Cisco Unified IM and Presence 功能配置、Cisco Unified IM and Presence 报告和 IM and Presence 灾难恢复系统。

过程

步骤 1 创建包含您希望在提示中显示的内容的 .txt 文件。

步骤 2 登录到 Cisco Unified IM and Presence 操作系统管理。

步骤 3 选择**软件升级** > **定制登录消息**。

步骤 4 单击**浏览**并找到 .txt 文件。

步骤 5 单击**上传文件**。

提示将于登录前后在大多数 IM and Presence Service 界面上显示。

注释 .txt 文件必须分别上传到每个 IM and Presence Service 节点。

配置安全 XMPP 连接

此程序用于使用 TLS 启用安全 XMPP 连接。

过程

步骤 1 从 Cisco Unified CM IM and Presence 管理中，选择**系统** > **安全性** > **设置**。

步骤 2 选中相应的复选框以启用以下 XMPP 安全设置：

表 *19: IM and Presence Service* 的 *XMPP* 安全设置

设置	说明
启用 XMPP 客户端 IM/P 服务安全模式	启用后，IM and Presence Service 会与群集中的 XMPP 客户端应用程序建立安全的 TLS 连接。 此设置默认为启用。 建议不要关闭此安全模式，除非 XMPP 客户端应用程序能够在非安全模式下保护客户端登录凭证。 如果确实要关闭安全模式，请确保可以使用其他方法保护 XMPP 客户端-节点通信。

设置	说明
启用 XMPP 路由器-路由器安全模式	如果打开此设置，IM and Presence Service 会在同一群集或不同群集中的 XMPP 路由器之间建立安全 TLS 连接。 IM and Presence Service 会自动在群集中和跨群集复制 XMPP 证书，并将其作为 XMPP 信任证书。 XMPP 路由器将尝试与同一群集或不同群集中的任何其他 XMPP 路由器建立 TLS 连接，且可用于建立 TLS 连接。
启用 Web 客户端 IM/P 服务安全模式	如果打开此设置，IM and Presence Service 会在群集中的 IM and Presence Service 节点和基于 XMPP 的 API 客户端应用程序之间建立安全 TLS 连接。 如果打开此设置，则在 IM and Presence Service 的 cup-xmpp-trust 存放库中上传 Web 客户端的证书或签名证书。

步骤 3 单击**保存**。

下一步做什么

如果您更新了**启用 XMPP 客户端 IM/P 服务安全模式**设置，请重新启动 Cisco XCP 连接管理器。

IM and Presence Service 上的 SIP 安全性设置配置

配置 TLS 对等主题

导入 IM and Presence Service 证书时，IM and Presence Service 会自动尝试将 TLS 对等主题添加到 TLS 对等主题列表和 TLS 上下文列表中。 确认已根据您的要求设置 TLS 对等主题和 TLS 上下文配置。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中选择**系统** > **安全性** > **TLS 对等主题**。

步骤 2 单击**新增**。

步骤 3 对“对等主题名称”执行以下操作之一：

a) 输入节点显示的证书的主题 CN。

b) 打开证书，查找 CN 并将其粘贴在此处。

步骤 4 在“说明”字段中输入节点的名称。

步骤 5 单击**保存**。

下一步做什么

继续配置 TLS 上下文。

配置 TLS 上下文

此程序用于将 TLS 环境和 TLS 对等密码分配给您的 TLS 对等主题。

注释 导入 IM and Presence Service 证书时，IM and Presence Service 会自动尝试将 TLS 对等主题添加到 TLS 对等主题列表和 TLS 环境列表中。

开始之前

配置 TLS 对等主题，第 147 页

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择 **系统** > **安全性** > **TLS 环境配置**。

步骤 2 单击**查找**。

步骤 3 选择 **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**。

步骤 4 从可用 TLS 对等主题列表中选择已配置的 TLS 对等主题。

步骤 5 使用 > 箭头将此 TLS 对等主题移至**选定 TLS 对等主题**。

步骤 6 配置 **TLS 密码映射**选项：

a) 查看**可用的 TLS 密码**和**所选的 TLS 密码**框中可用的 TLS 密码列表。

b) 如果要启用当前未选定的 TLS 密码，使用 > 箭头将该密码移至**所选的 TLS 密码**。

步骤 7 单击**保存**。

步骤 8 重新启动 Cisco SIP Proxy 服务：

a) 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 功能服务**。

b) 从**服务器**下拉列表框中选择 IM and Presence Service 群集节点，然后单击**前往**。

c) 选择 **Cisco SIP Proxy** 服务并单击**重新启动**。

FIPS 模式

IM and Presence Service 包含一组增强的系统安全模式，允许您的系统在一组更严格的安全准则和风险管理控制举措下运行，这些控制举措涉及密码学、数据和信号加密以及审计日志记录等事项。

- FIPS 模式 — IM and Presence Service 可以配置为在 FIPS 模式下运行，这样可确保您的系统符合美国和加拿大加密模块政府标准 — 联邦信息处理标准 (FIPS)。
- 增强的安全模式 — 增强的安全模式在启用 FIPS 的系统上运行，并提供其他风险管理控制举措，如数据加密要求、更严格的凭证策略、联系人搜索用户验证，以及更严格的审计日志记录要求。
- 通用标准模式 — 通用标准模式还在启用 FIPS 的系统上运行，提供额外的控制举措，使得您的系统符合 TLS 等通用标准指南并能够使用 X.509 v3 证书。

注释 如果外部数据库为 MSSQL，要让消息存档程序、文字会议管理器和文件传输管理器等服务在通用条件模式下工作，您必须执行以下操作：

1. 配置托管 MSSQL 数据库的服务器，以支持 TLS 1.1 或更高版本。
2. 将数据库证书重新上传到 IM and Presence Service。
3. 选中**外部数据库配置**页面中的**启用 SSL** 复选框。选择 **Cisco Unified CM IM and Presence 管理** > **消息** > **外部服务器设置** > **外部数据库**以配置外部数据库。

有关如何在 Cisco Unified Communications Manager 和 IM and Presence Service 中启用 FIPS 模式、增强的安全模式和通用标准模式的详细信息，请参阅《*Cisco Unified Communications Manager* 安全指南》的“FIPS 模式设置”一章，网址：https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

Outlook 日历集成的 FIPS

在 IM and Cisco Presence Service 服务器上启用 FIPS 模式时，仅支持使用 NTLMv2 来获取 Exchange Web 服务信息。如果禁用了 FIPS 模式，则根据现有行为支持 NTLMv1 和 NTLMv2。在两种情况下均支持基本验证，无论启用还是禁用 FIPS 模式。

引入了一个新的名为 **FIPS 模式 Exchange 服务器身份验证**服务参数，以验证 Presence Engine 使用的身份验证类型，从而通过 Microsoft Outlook 日历集成功能与 Exchange 服务器建立连接。

您可以将 **FIPS 模式 Exchange 服务器身份验证**服务参数设置为**自动**或**仅基本**。

服务参数设置为**自动**：Presence Engine 先协商 NTLMv2，然后在 NTLMv2 协商失败时回退到仅“基本身份验证”。NTLMv1 在 FIPS 模式下不会协商。

服务参数设置为**仅基本**：即使 Exchange 服务器配置为允许 NTLM 和基本身份验证时，系统会强制 Presence Engine 使用“基本身份验证”。

注释 服务参数设置中的任何更改都要求重新启动 Cisco Presence Engine。

第 14 章

配置群集间对等

- 群集间对等概述， 第 151 页
- 群集间对等前提条件， 第 151 页
- 群集间对等配置任务流程， 第 152 页
- 群集间对等相互作用和限制， 第 160 页

群集间对等概述

群集间对等功能使一个群集中的用户能够通信和订阅相同域中不同群集用户的在线状态。对于大型部署，您可以使用群集间对等连接远程 IM and Presence 群集。

本地和远程群集的数据库发布方节点上都会配置群集间对等。

对于群集间部署规模大小和性能建议，请参阅《思科协作系统解决方案参考网络设计 *(SRND)*》的"协作即时消息和在线状态"一章，网址：http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/UCgoList.html#48016

群集间对等前提条件

在网络中配置 IM and Presence Service 群集间对等成员前，请注意以下内容：

- 根据需要为所有群集配置系统拓扑并分配用户。
- 为使群集间对等连接正常工作，如果两个群集之间存在防火墙，则必须让以下端口保持打开状态：
  - 8443 (AXL)
  - 7400 (XMPP)
  - 使用 SIP 联合时，仅 5060 (SIP)
- 对于群集间部署，必须部署至少包含 15000 位用户的 OVA。只要所有群集运行的用户 OVA 至少为 15000 位用户，就可以让不同的群集运行不同大小的 OVA。

注释 在 Cisco Business Edition 6000 服务器上部署了 IM and Presence Service 时，不支持群集间对等。

群集间对等配置任务流程

过程

	命令或操作	目的
步骤 1	检查用户设置，第 152 页	配置群集间对等之前，验证是否已正确设置最终用户。
步骤 2	启用 Cisco AXL Web 服务，第 153 页	Cisco AXL Web 服务必须在所有本地和远程 IM and Presence 节点上处于活动状态。 此程序用于验证服务是否正在运行。
步骤 3	启用同步代理，第 153 页	在每个群集间对等的数据库发布方节点上启用同步代理。
步骤 4	配置群集间对等，第 154 页	在每个群集中的数据库发布方节点上完成此任务以设置群集间对等。
步骤 5	验证群集间同步代理是否已打开，第 156 页	群集间同步代理必须在 IM and Presence Service 群集中的所有节点上运行。 此程序用于验证群集间同步代理参数是否正在运行。
步骤 6	验证群集间对等状态，第 156 页	验证群集间对等配置是否有效。
步骤 7	更新群集间同步代理 Tomcat 信任证书，第 157 页	如果群集间对等的 tomcat 证书状态为不同步，更新 Tomcat 信任证书。
步骤 8	为群集间对等周期性同步失败启用自动恢复，第 158 页	此程序用于为群集间定期同步失败启用自动恢复。
步骤 9	配置群集间对等同步时间间隔，第 158 页	此程序用于设置群集间对等同步的时间间隔。
步骤 10	对群集间对等定期同步禁用证书同步，第 159 页	此程序用于将群集间定期同步的一部分配置证书同步的禁用/启用。

检查用户设置

此程序用于验证在配置群集间对等之前，是否正确设置了最终用户。

过程

步骤 1 在 Cisco Unified CM IM and Presence 管理中选择**诊断** > **系统故障诊断程序**。
系统故障诊断程序将运行。

步骤 2 在**用户故障诊断程序**部分，验证并确保已正确设置最终用户，并且没有重复或无效的用户。

下一步做什么

启用 Cisco AXL Web 服务，第 153 页

启用 Cisco AXL Web 服务

Cisco AXL Web 服务必须在所有本地和远程 IM and Presence 群集节点上运行。 默认情况下，此服务正在运行。 但是，您可以执行此程序以验证服务是否正在运行。

注释 启用 Cisco AXL Web 服务时，系统会创建具有 AXL 权限的群集间应用程序用户。 在远程 IM and Presence Service 节点上配置群集间对等时，您将需要群集间应用程序用户的用户名和密码。

过程

步骤 1 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 功能服务**。

步骤 2 从**服务器**列表选择要重新激活服务的节点并单击**前往**。

步骤 3 在**数据库和管理服务**区域中，检查 **Cisco AXL Web 服务**的**状态**。

- 如果服务**已启动**，不需要执行任何操作。
- 如果服务**未运行**，选择服务并单击**重新启动**。

步骤 4 在本地和远程群集中的所有群集节点上重复此程序。

下一步做什么

启用同步代理，第 153 页

启用同步代理

思科同步代理必须在本地和远程 IM and Presence 数据库发布方节点上的每个群集间对等的数据库发布方节点上运行。

过程

步骤 1 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 网络服务**。

步骤 2 从**服务器**下拉列表框中，选择 IM and Presence 数据库发布方节点并单击**前往**。

步骤 3 在 **IM and Presence Service** 下，验证**思科同步代理**的状态是否是**正在运行**。

步骤 4 如果服务未运行，选择服务并单击**重新启动**。

步骤 5 在每个群集中重复此程序

下一步做什么

思科同步代理从 Cisco Unified Communications Manager 完成用户同步后，配置群集间对等，第 154 页

配置群集间对等

在数据库发布方节点上对本地和远程群集执行此程序可设置群集间对等关系。

开始之前

- 确认同步代理已从本地和远程群集上的 Cisco Unified Communications Manager 完成用户同步。如果在同步代理完成用户同步之前配置群集间对等连接，群集间对等连接的状态将显示为**失败**。
- 确保在远程 IM and Presence Service 节点上获取群集间应用程序用户的 AXL 用户名和密码。

过程

步骤 1 在 Cisco Unified CM IM and Presence 管理中，选择 **Presence** > **群集间**。

步骤 2 单击**新增**。

步骤 3 在**对等地址**字段中，输入远程群集的数据库发布方节点的节点名称。 此字段可能是IP地址、主机名或 FQDN，但必须匹配定义服务器的实际节点名称。

注释

- 要验证节点名称使用的地址类型，登录到远程群集上的 Cisco Unified CM IM and Presence 管理，然后选择**系统** > **Presence 拓扑**。 此窗口显示每个群集节点的节点名称和服务器详细信息。
- 在隶属多群集环境的群集中可能会发生裂脑情况。 例如，有一个群集 A，其多群集对等成员是群集B、C、D和E。群集A中的节点必须能够在裂脑情况下访问DNS，因为它们必须在裂脑情况下与多群集环境中的其他群集 B、C、D 和 E 通信。

  在裂脑情况下，如果群集 A 中的节点无法访问 DNS，则应将 A、B、C、D 和 E 群集节点的 IP 地址设置为节点名称，而不是主机名和 FQDN。

  如果群集 A、B、C、D 和 E 中的节点是用 FQDN 或主机名定义的，并且在裂脑情况下它们无法访问 DNS，则服务将中断，例如群集 A 与 B、C、D、E 之间丢失 IM Presence 更新以及 IM 历史记录。

步骤 4 输入 AXL 凭证。

步骤 5 输入用于 SIP 通信的首选**协议**。

注释 思科建议您使用 **TCP**（默认设置）作为所有 IM and Presence Service 群集的群集间干线传输协议。 您可以根据您的网络配置和安全需要更改此设置。

步骤 6 单击**保存**。

步骤 7 检查GUI标题右上角的通知。 如果通知提示您重新启动 **Cisco XCP 路由器**，执行以下操作。 否则，您可以跳过此步骤：

a) 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 网络服务**。
b) 从**服务器**下拉列表框中，选择 IM and Presence 节点并单击**前往**。
c) 选择 **Cisco XCP 路由器**并单击**重新启动**。
d) 在所有群集节点上重复这些步骤

步骤 8 在每个远程对等群集的数据库发布方节点上重复此程序。

提示 如果选择 **TLS** 作为群集间传输协议，IM and Presence Service 会尝试自动在群集间对等节点之间交换证书，以建立安全的 TLS 连接。 IM and Presence Service 在群集间对等成员状态部分指示证书交换是否成功。

下一步做什么

验证群集间同步代理是否已打开，第 156 页

重新启动 XCP 路由器服务

在本地群集以及远程群集中的所有节点上重新启动 Cisco XCP 路由器服务。

开始之前

配置群集间对等，第 154 页

过程

步骤 1 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 网络服务**。

步骤 2 从**服务器**列表选择要重新激活服务的节点并单击**前往**。

步骤 3 在 **IM and Presence Service** 区域选择 **Cisco XCP 路由器**。

步骤 4 单击**重新启动**。

下一步做什么

验证群集间同步代理是否已打开，第 156 页

验证群集间同步代理是否已打开

群集间同步代理网络服务会在群集间对等节点之间同步用户信息。 此程序用于确认服务是否正在每个群集间对等节点的所有群集节点上运行。

过程

步骤 1 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 网络服务**。

步骤 2 在**服务器**菜单中，选择 IM and Presence Service 节点并单击**前往**。

步骤 3 确认**思科群集间同步代理**的状态显示为**正在运行**。

步骤 4 如果服务未运行，选择服务并单击**启动**。

步骤 5 为每个群集间对等节点的所有群集节点重复此程序。

下一步做什么

验证群集间对等状态，第 156 页

验证群集间对等状态

此程序用于确认您的群集间对等配置是否在正常工作。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择 **Presence** > **群集间**。

步骤 2 从搜索条件菜单中选择对等成员地址。

步骤 3 单击**查找**。

步骤 4 在“群集间对等成员状态”窗口中：

a) 验证群集间对等成员的每个结果条目旁边都有复选标记。

b) 确保**关联用户数**的值等于远程群集上的用户数。

c) 如果选择 **TLS** 作为群集间传输协议，**证书状态**项目将显示 TLS 连接的状态，并指示 IM and Presence Service 是否已在群集之间成功交换安全证书。 如果证书不同步，则需要手动更新 tomcat 信任证书（如本模块中所述）。 对于任何其他证书交换错误，请查看在线帮助以了解建议的操作。

步骤 5 运行系统故障诊断程序：

a) 在 Cisco Unified CM IM and Presence 管理中选择**诊断** > **系统故障诊断程序**。

b) 在**群集间故障诊断程序**部分，验证每个群集间对等连接条目的状态旁边是否有复选标记。

下一步做什么

更新群集间同步代理 Tomcat 信任证书，第 157 页

更新群集间同步代理 Tomcat 信任证书

如果本地群集上出现连接错误，并且损坏的Tomcat信任证书与远程群集关联，请执行此程序以更新 Tomcat 信任证书。

如果群集间对等的 tomcat 证书状态为不同步，必须更新 Tomcat 信任证书。 如果重新使用现有的群集间对等配置指向新的远程群集，群集间部署中可能会出现此错误。 在更新安装 IM and Presence Service、更改 IM and Presence Service 主机或域名、重新生成 Tomcat 证书时，也可能发生此错误。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择 **Presence** > **群集间**。

步骤 2 单击**强制同步**以将证书与远程群集同步。

步骤 3 在显示的确认窗口中，选择**同时重新同步对等成员的 Tomcat 证书**。

步骤 4 单击**确定**。

注释 如果有任何证书未自动同步，请转到“群集间对等配置”窗口。 标有 X 的所有证书都是您需要手动复制的缺失证书。

为群集间对等周期性同步失败启用自动恢复

如果希望思科群集间同步代理引发“InterClusterSyncAgentPeerPeriodicSyncingFailure”警报并在群集间对等周期性同步卡住超过 2 小时时自动重新启动，请执行此程序以启用此服务参数。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**系统** > **服务参数**。

步骤 2 从服务器列表中，选择想要为其设置“常规群集间同步代理参数”的 IM and Presence 节点。

步骤 3 从**服务**列表中，选择**思科群集间同步代理（活动）**。

步骤 4 将**为群集间对等周期性同步失败启用自动恢复**服务参数设置为**启用**。

步骤 5 单击**保存**。

注释 如果“为群集间对等周期性同步失败启用自动恢复”服务参数设置为启用，且周期性同步卡住超过 2 小时，则：

- 系统将生成 ***InterClusterSyncAgentPeerPeriodicSyncingFailure*** 警报。
- **思科群集间同步代理**服务将自动重新启动。

如果“为群集间对等周期性同步失败启用自动恢复”禁用，则：

- 系统将生成 ***InterClusterSyncAgentPeerPeriodicSyncingFailure*** 警报。
- **思科群集间同步代理**服务将不会自动重新启动。

配置群集间对等同步时间间隔

此程序用于设置群集间对等同步的时间间隔。 服务参数**群集对等端定期同步时间间隔（分钟）**用于配置动态 ICSA 定期同步的时间间隔。 群集间对等同步时间间隔的默认设置为 30 分钟。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**系统** > **服务参数**。

步骤 2 从服务器列表中，选择想要为其设置“常规群集间同步代理参数”的 IM and Presence 节点。

步骤 3 从**服务**列表中，选择**思科群集间同步代理（活动）**。

步骤 4 将**群集对等端定期同步时间间隔（分钟）**服务参数设置为所需的时间间隔。 范围为 30 – 1444 分钟，默认设置为 30 分钟。

步骤 5 单击**保存**。

注释　新设置将在下一次群集间同步后生效。

如果群集间对等同步失败，思科群集间同步代理服务将在完成四个同步周期后重新启动。例如，如果参数设置为 40 分钟，服务将在 160 分钟 (4*40) 后重新启动。

对群集间对等定期同步禁用证书同步

此程序用于在群集间同步过程中禁用证书同步。 服务参数**在群集间定期同步期间同步证书**可让管理员在群集间定期同步过程中禁用或启用证书同步。 此服务参数的默认值为**执行证书同步**。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**系统** > **服务参数**。

步骤 2 从服务器列表中，选择想要为其设置**常规群集间同步代理参数**的 IM and Presence 节点。

步骤 3 从**服务**列表中，选择**思科群集间同步代理（活动）**。

步骤 4 将服务参数**在群集间定期同步期间同步证书**设置为**不执行证书同步**。

步骤 5 单击**保存**。

注释　如果在群集间定期同步期间与证书同步相关的部署中遇到性能下降或CPU峰值过高的问题，您可以遵照此程序来设置服务参数。

删除群集间对等连接

如果您想删除群集间对等关系，请遵照此程序。

过程

步骤 1 登录到 IM and Presence Service 数据库发布方节点。

步骤 2 在 Cisco Unified CM IM and Presence 管理中，选择 **Presence** > **群集间**。

步骤 3 单击**查找**并选择要删除的群集间对等。

步骤 4 单击**删除**。

步骤 5 在对等群集上重复这些步骤。

注释　IM and Presence Service 得到了增强，可以防止群集间对等删除后，在 IM and Presence 群集中的每个节点上重新启动 XCP 路由器。 此增强功能通过在确保 Jabber 服务不中断的同时，显著减少节点按顺序重启带来的开销，可帮助管理员有效管理大型群集。

群集间对等相互作用和限制

功能	交互和限制
Cisco Business Edition 6000	在 Cisco Business Edition 6000 服务器上部署了 IM and Presence Service 时，不支持群集间对等。
群集限制	通过群集间对等，您可以在群集间网格中最多部署 30 个 IM and Presence Service 群集，无论这些群集是集中式还是分散的。
多群集部署中的群集间同步代理资源不足	在具有大量群集的多群集部署中，ICSA 需要更多的资源。 如果因资源短缺而面临任何 ICSA 或 SRM 相关问题。 我们建议您将下方提及的 Cisco SIP Proxy 服务参数从默认值 20 更改为新值 10。 • 进程最大数 • 备用进程最大数 • 进程最大数 重新启动 SIP 代理服务以使更改生效。 重新启动 SRM 和 ICSA 服务。
群集间同步代理和 DNS	群集间同步代理使用 DNS 来解析在对等群集的 tomcat 证书（SAN 条目）中列出的所有 CUCM 和 IM&P 服务器。 如果 DNS 解析失败，集群间同步代理将不会连接到远程对等成员。

第 15 章

配置推送通知

- 推送通知概述， 第 161 页
- 推送通知配置， 第 165 页

推送通知概述

当您的群集启用推送通知时，Unified Communications Manager 和 IM and Presence Service 使用 Google 和 Apple 的基于云的推送通知服务来推送语音和视频呼叫通知、即时消息通知到以挂起模式（也称为后台模式）运行的 Android 和 iOS 客户端上的 Cisco Jabber 或 Cisco Webex。 推送通知可让您的系统与 Cisco Jabber 或 Cisco Webex 保持永久通信。 对于从企业网络内部连接的 Android 和 iOS 客户端上的 Cisco Jabber 和 Cisco Webex，以及通过 Expressway 的移动和远程访问功能注册到内部部署的客户端而言，推送通知都是必需的。

推送通知的工作原理

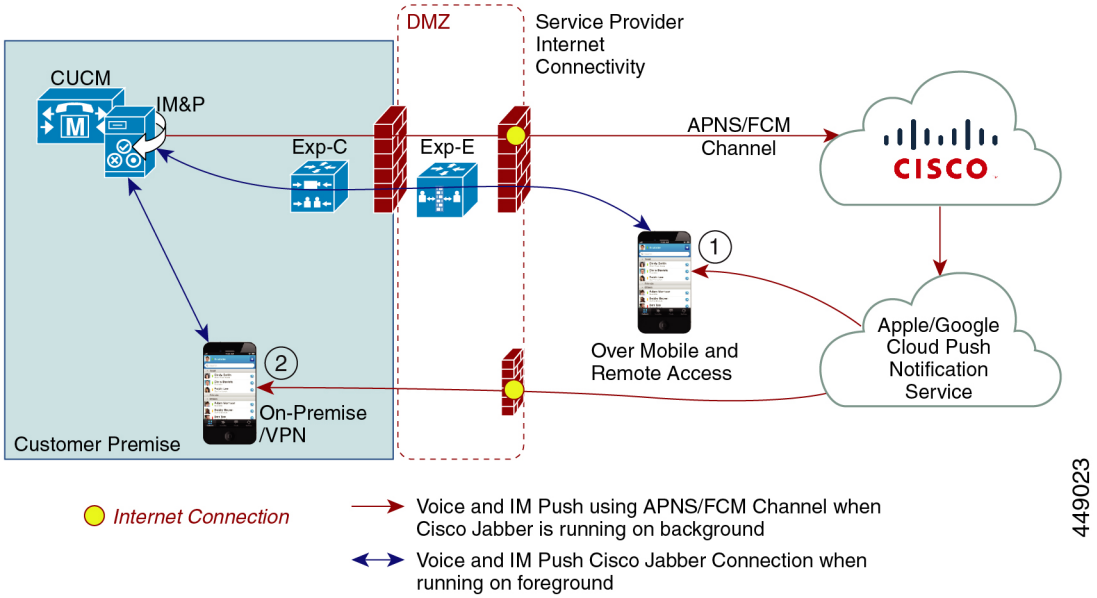
在启动时，安装在 Android 和 iOS 平台设备上的客户端会注册到 Unified Communications Manager、IM and Presence Service 以及 Google 和 Apple 云。 通过移动和远程访问部署，客户端通过 Expressway 注册到内部服务器。 只要 Cisco Jabber 和 Cisco Webex 客户端在前台模式下运行，Unified Communications Manager 和 IM and Presence Service 就可以直接向客户端发送呼叫和即时消息。

但是，一旦 Cisco Jabber 或 Cisco Webex 客户端进入挂起模式（例如为了延长电池使用时间），标准通信通道就不可用，从而导致 Unified Communications Manager 和 IM and Presence Service 无法直接与客户端通信。 推送通知提供了另一个通过合作伙伴云联系客户端的渠道。

注释 如果以下任一情况属实，Cisco Jabber 和 Cisco Webex 将被视为在挂起模式下运行：

- Cisco Jabber 或 Cisco Webex 应用程序离屏运行（例如在后台运行）
- Android 或 iOS 设备已锁定
- Android 或 iOS 设备屏幕关闭

图 6: 推送通知架构



上图显示了当 Cisco Jabber 或 Cisco Webex Android 和 iOS 版本客户端在后台运行或停止运行时会发生什么。 图中展示了：(1) 移动和远程访问部署，其中客户端通过 Expressway 与现场 Cisco Unified Communications Manager 和 IM and Presence Service 部署连接，以及 (2) 直接与企业网络内的现场部署连接的 Cisco Jabber 或 Cisco Webex Android 和 iOS 客户端。

注释 从 iOS13（适用于 Apple 客户端和支持的 Android 客户端）开始，语音呼叫和消息使用单独的推送通知通道（“VoIP”和“消息”）访问在后台模式下运行的客户端。 不过，这两个通道的常规流是相同的。 对于 iOS 12，语音呼叫和消息使用相同的通道发送。

Cisco Jabber 和 Cisco Webex 的推送通知行为

下表介绍了 iOS 12 和 iOS 13 下注册到 Unified Communications Manager 和 IM and Presence Service 的 Cisco Jabber 或 Cisco Webex iOS 客户端的行为。

Cisco Jabber 或 **Cisco Webex** 客户端正在运行...	**Cisco Jabber** 正在 **iOS12** 设备上运行	**Cisco Jabber** 正在 **iOS13** 设备或 **Android** 设备上运行
前台模式	语音和视频呼叫 Unified Communications Manager 使用标准 SIP 通信通道直接向 Cisco Jabber 或 Cisco Webex 客户端发送语音和视频呼叫。 对于呼叫，Unified Communications Manager 还会将推送通知发送到处于前台模式的 Cisco Jabber 或 Cisco Webex 客户端。 不过，标准 SIP 通道（而不是推送通知通道）用于建立呼叫。 留言 IM and Presence Service 服务使用标准 SIP 通信通道直接将消息发送到客户端。 对于消息，推送通知不会发送到处于前台模式的客户端。	行为与 iOS12 相同。

Cisco Jabber 或 Cisco Webex 客户端正在运行...	Cisco Jabber 正在 iOS12 设备上运行	Cisco Jabber 正在 iOS13 设备或 Android 设备上运行
挂起模式（背景模式）	语音或视频呼叫 标准通信通道不可用。 Unified CM 使用推送通知通道。 收到通知后，Cisco Jabber 或 Cisco Webex 客户端将自动重新进入前台模式，客户端会振铃。 消息传送 标准通信通道不可用。 IM and Presence Service 使用通知推送通道发送 IM 通知，如下所示： 1. IM and Presence Service 将 IM 通知发送到思科云中的 Push REST 服务，该服务会将通知转发到 Apple 云。 2. Apple 云将 IM 通知推送到 Cisco Jabber 或 Cisco Webex 客户端，通知显示在 Cisco Jabber 或 Cisco Webex 客户端上。 3. 当用户单击通知时，Cisco Jabber 或 Cisco Webex 客户端将移回前台。Cisco Jabber 或 Cisco Webex 客户端会恢复与 IM and Presence Service 的会话并下载即时消息。 注释 当 Cisco Jabber 或 Cisco Webex 客户端处于挂起模式时，用户的在线状态显示为**离开**。	使用 iOS13 时，呼叫流量和消息流量拆分为单独的推送通知通道：用于呼叫的 "VoIP" 通道，以及用于消息传送的“消息”通道。 语音或视频呼叫 标准通信通道不可用。 Unified CM 使用推送通知 "VoIP" 通道。 在收到 VoIP 通知后，Jabber 将使用主叫号码启动 CallKit。 此行为适用于 Cisco Jabber 或 Cisco Webex iOS 客户端。 消息传送 标准通信通道不可用。 IM and Presence Service 服务使用推送通知“消息”通道。 1. IM and Presence Service 将 IM 通知发送到思科云中的 Push REST 服务，该服务会将通知转发到 Apple 云。 2. Apple 云会将 IM 通知推送到 Cisco Jabber 或 Cisco Webex 客户端。 3. 当用户单击通知时，Cisco Jabber 或 Cisco Webex 客户端将移回前台模式。Cisco Jabber 或 Cisco Webex 客户端会恢复与 IM and Presence Service 的会话并下载消息。 注释 当 Cisco Jabber 或 Cisco Webex 客户端处于挂起模式时，用户的在线状态显示为**离开**。

推送通知支持的客户端

客户端	操作系统	平台云	云服务
Cisco Jabber iPhone 和 iPad 版本	iOS	Apple	Apple 推送通知服务 (APNS)
Cisco Jabber Android 版本	Android	Google	Android PNS 服务
Webex iOS 版本	iOS	Apple	Apple 推送通知服务 (APNS)

客户端	操作系统	平台云	云服务
Webex Android 版本	Android	Google	Android PNS 服务

iOS13 中推送通知的工作原理

与 iOS12 相比，在 iOS13 中，Apple 对 **VoIP** 类型的挂起应用程序的推送通知处理方式有所不同。从 2020 年 7 月开始，所有新应用程序和应用程序更新都使用 iOS 13 SDK 构建。

Cisco Unified Communications Manager 和 IM and Presence Service 使用 VOIP 通知通道来推送语音和 IM 消息。

- 对于所有音频视频呼叫，CUCM 服务器将发送 "**VoIP**" 类型的推送通知
- 对于所有消息，IM&P 服务器将发送“**消息**”类型的推送通知

CUCM 会将 VoIP 推送通知视为高优先级通知，并且没有延迟地传送。

下图显示了 Apple 如何在 **iOS12** 和 **iOS13** 中处理推送通知。

此处为图像

此处为图像

有关每个用例以及各个版本的详细说明，请参见下表：

推送通知配置

有关如何配置和部署推送通知的详细信息，请参阅部署 *iPhone* 和 *iPad* 版 *Cisco Jabber* 的推送通知，网址：https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。

第 III 部分

配置功能

- 配置可用性和即时消息， 第 169 页
- 配置临时和永久聊天， 第 175 页
- 配置永久聊天的高可用性， 第 189 页
- 配置托管文件传输， 第 199 页
- 配置多设备消息传送， 第 219 页
- 配置企业组， 第 227 页
- 品牌定制， 第 239 页
- 配置高级功能， 第 245 页

第 16 章

配置可用性和即时消息

- 可用性和即时消息概述， 第 169 页
- 可用性和即时消息前提条件， 第 170 页
- 可用性和即时消息任务流程， 第 170 页
- 可用性和即时消息相互作用及限制， 第 173 页

可用性和即时消息概述

通过 IM and Presence Service，您的用户可与其联系人共享其可用性状态。

点对点即时消息每次支持两个用户之间实时对话。 IM and Presence Service 直接在用户之间交换消息（从发送者到接收者）。 用户必须在其即时消息客户端中联机才能交换点对点即时消息。

即时消息功能包括：

即时消息分叉

当用户向登录到多个即时消息客户端的联系人发送即时消息时，IM and Presence Service 会将即时消息传送给每个客户端。 IM and Presence Service 继续将即时消息分叉发送到每个客户端，直到联系人回复。 联系人回复后，IM and Presence Service 只将即时消息发送给联系人用于回复的客户端。

离线即时消息

当用户向未登录（离线）的联系人发送即时消息时，IM and Presence Service 会存储即时消息，并在离线联系人重新登录其即时消息客户端后发送。

广播即时消息

使得用户能够同时发送即时消息给多个联系人，例如，当用户想要发送通知到一个大型联系人组时。

请注意，并非所有的即时消息客户端都支持广播。

最大联系人列表大小

配置用户的最大联系人列表大小；这是可以添加到其联系人列表中的联系人数。 此设置应用于 Cisco Jabber 客户端应用程序和第三方客户端应用程序上的联系人列表。

如果用户达到联系人最大数，则无法向其联系人列表中添加新联系人，其他用户也不能将其添加为联系人。 如果用户接近最大联系人列表大小上限，且用户要添加一组导致联系人列表超过最大数上限的联系人，IM and Presence Service 将不添加超过限制的联系人。 例如，如果 IM and Presence Service 上的最大联系人列表大小为 200。一位拥有 195 位联系人的用户试图向列表中添加 6 位新联系人时，IM and Presence Service 将添加 5 位联系人，但不会添加第 6 位联系人。

提示 **Cisco Unified CM IM and Presence 管理**中的系统故障诊断程序指示是否有用户已达到联系人列表上限。

可用性和即时消息前提条件

对于 SIP 到 SIP 即时消息，必须在 IM and Presence Service 上运行以下服务：

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP 路由器

对于 SIP 到 XMPP 即时消息，必须在 IM and Presence Service 上运行以下服务：

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP 路由器
- Cisco XCP 文字会议管理器

可用性和即时消息任务流程

执行以下任务可在 IM and Presence Service 上配置可用性和即时消息。

过程

	命令或操作	目的
步骤 1	配置 Presence 共享， 第 171 页	此程序用于为 Presence 和 IM 可用性共享配置群集范围的设置。 通过 Presence 共享，您的用户可以查看彼此的 IM 可用性状态。
步骤 2	配置临时 Presence 订阅， 第 172 页	配置临时 Presence 订阅。 此设置可让用户临时查看不在其联系人列表中的其他用户的状态。

	命令或操作	目的
步骤 3	启用即时消息，第 172 页	配置系统以允许用户交换即时消息。

配置 Presence 共享

此程序用于为 Presence 和 IM 可用性共享配置群集范围的设置。 通过 Presence 共享，您的用户可以查看彼此的 IM 可用性状态。

注释 当可用性共享关闭时：

- 用户可以在客户端应用程序中查看自己的可用性状态，但其他用户的状态会显示为灰色。
- 当用户进入聊天室时，其可用性状态显示为**未知**。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中选择 **Presence** > **设置** > **标准配置**。

步骤 2 要启用群集范围的 Presence 共享，选中**启用可用性共享**复选框。

注释 通过在 Cisco Jabber 客户端中重新配置策略设置，各个 Cisco Jabber 用户可以为自己的 Jabber 客户端启用或禁用此设置。

步骤 3 如果您希望用户能够在不需要其他用户批准的情况下查看其他用户的状态，选中**允许用户在不提示批准的情况下查看其他用户的可用性**复选框。 否则，所有 Presence 请求必须由其他用户授权。

注释 通过在 Cisco Jabber 客户端中重新配置策略设置，各个最终用户可以改写此设置。

步骤 4 配置**最大联系人列表大小**和**查看器最大数（每用户）**设置的最大值。 如果不想使用最大值，选中每个设置的**无限制**复选框。

步骤 5 可选。 如果您希望 Cisco Jabber 用户能够暂时订阅不在其联系人列表中的其他用户的 Presence 状态，选中**启用临时 presence 订阅**复选框并配置额外的临时 presence 设置。

步骤 6 完成 **Presence 设置**窗口中的所有其他设置。 有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 7 单击**保存**。

步骤 8 重新启动 **Cisco XCP 路由器**和 **Cisco Presence Engine** 服务：

a) 登录到 Cisco Unified IM and Presence 功能配置并选择**工具** > **控制中心 - 功能服务**

b) 选择 **Cisco Presence Engine** 服务并单击**重新启动**。

c) 选择**工具** > **控制中心 - 网络服务**。

d) 选择 **Cisco XCP 路由器**服务并单击**重新启动**。

注释　您可能不需要重新启动服务，具体取决于编辑的字段。 有关您编辑的字段的信息，请参阅联机帮助。

下一步做什么

启用即时消息，第 172 页

配置临时 Presence 订阅

临时 presence 订阅可让用户临时查看不在其联系人列表中的其他用户的状态。

开始之前

配置 Presence 共享，第 171 页

过程

步骤 1　在 **Cisco Unified CM IM and Presence 管理**中选择 **Presence** > **设置** > **标准**。

步骤 2　要为 Cisco Jabber 用户开启临时 presence 订阅，选中**启用临时 Presence 订阅**复选框。

步骤 3　设置 IM and Presence Service 一次允许的最大活动临时订阅数。 如果将值配置为零，IM and Presence Service 将允许无限数量的活动临时订阅。

步骤 4　为临时 Presence 订阅设置保持连接时间值（秒）。

当此保持连接时间值到期后，IM and Presence Service 将丢掉任何临时 Presence 订阅，而不再临时监控该用户的可用性状态。

注释　如果保持连接时间值过期时用户仍在查看来自临时 Presence 订阅的即时消息，显示的可用性状态可能不是最新状态。

步骤 5　单击**保存**。

注释　您无需为此设置在 IM and Presence Service 上重新启动任何服务。 不过，Cisco Jabber 用户必须注销再重新登录，才能检索 IM and Presence Service 上的最新临时 Presence 订阅设置。

下一步做什么

启用即时消息，第 172 页

启用即时消息

配置系统以允许用户交换即时消息。

开始之前

配置 Presence 共享，第 171 页

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**消息** > **设置**。

步骤 2 选中**启用即时消息**复选框。

步骤 3 选中满足您的部署需要的复选框选项。 要查看字段说明，请参阅联机帮助：

- **抑制离线即时消息**
- **允许客户端记录即时消息历史记录（只在支持的客户端上）**
- **允许剪切和粘贴即时消息**

步骤 4 单击**保存**。

可用性和即时消息相互作用及限制

功能	限制
可用性共享	如果关闭此设置，用户只能查看自己的可用性状态。 可用性信息不会与群集中的其他用户共享。 此外，从群集外部接收的可用性信息也不会共享。
即时消息	如果 Cisco XCP Router 突然关闭或用户停止/重启，则在该期间开始或中断期间发送的即时消息可能不会发送到目标用户。 警告消息可能不会被发送到发送消息的用户。 有关详细信息，管理员可以在 Cisco XCP Router 跟踪文件 rtr-jsm-1 上检查是否有包含“Dropping packet after jsm db shutdown“的错误日志行。

第 17 章

配置临时和永久聊天

- 小组聊天室概述， 第 175 页
- 群聊前提条件， 第 176 页
- 群聊和永久聊天任务流程， 第 176 页
- 群聊和永久聊天相互作用和限制， 第 181 页
- 永久聊天示例（无高可用性）， 第 183 页
- IM and Presence 中的永久聊天边界， 第 184 页

小组聊天室概述

群聊是两个以上用户之间的即时消息会话。 IM and Presence Service 支持临时聊天室和永久聊天室中的群聊。 启用即时消息后，默认情况下会启用对临时聊天室的支持，但您必须配置系统以支持永久聊天室。

临时聊天室

临时聊天室是仅当仍有一个人连接到聊天室时才存在的群聊会话。 当最后一个用户离开时，系统会删除临时聊天室。 系统不会永久维护即时消息对话记录。 即时消息启用后，临时聊天室即默认启用。

默认情况下，临时聊天室是公共房间，但可以重新将其配置为私人房间。 但是，用户如何加入公共或私人临时聊天室取决于使用的 XMPP 客户端类型。

- Cisco Jabber 用户必须受邀才能加入任何临时聊天室（公共或私人）
- 第三方 XMPP 客户端上的用户可以受邀加入任何临时聊天室（公共或私人），也可以通过房间发现服务搜索加入仅限公共使用的临时聊天室。

永久聊天室

永久聊天室是即使所有用户离开了聊天室也会存在的群聊会话。 随着时间的推移，用户需要返回同一个聊天室继续讨论。

创建永久聊天室的目的在于，用户可以就特定主题展开协作和分享知识、搜索该主题的相关存档（如果在 IM and Presence Service 上启用了此功能），以及实时参与该主题的讨论。

您必须为永久聊天室配置系统。 此外，永久聊天要求您部署外部数据库

包括 IOS 和 Android 客户端在内的桌面和移动 Jabber 客户端都支持永久聊天室。 对于移动客户端，您运行的 Jabber 版本不能低于 12.1(0)。

群聊前提条件

临时聊天前提条件

如果您部署的是临时聊天室，请确保启用即时消息。有关详细信息，请参阅：启用即时消息，第 172 页。

永久聊天前提条件

如果您部署的是永久聊天室：

- 请确保启用即时消息。有关详细信息，请参阅：启用即时消息，第 172 页。
- 您必须部署外部数据库。有关数据库设置和支持信息，请参阅《*IM and Presence Service* 数据库设置指南》，网址：http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html。
- 确定是否要为永久聊天部署高可用性。此部署类型可为您的永久聊天室添加冗余和故障转移。但是，外部数据库要求与在没有高可用性的情况下部署功能时略有不同。
- 对于永久聊天部署，我们建议您部署至少包含 15000 位用户的 OVA。

群聊和永久聊天任务流程

过程

	命令或操作	目的
步骤 1	配置群聊系统管理员，第 177 页	添加系统管理员以管理永久聊天系统。
步骤 2	配置聊天室设置，第 178 页	配置基础的聊天室设置。 （可选）启用永久聊天。
步骤 3	重新启动 Cisco XCP 文字会议管理器，第 179 页	如果您部署的是永久聊天，请确保 Cisco XCP 文字会议管理器服务正在运行。
步骤 4	为永久聊天设置外部数据库，第 179 页	对于永久聊天，您必须为每个节点配置一个唯一的外部数据库实例。

	命令或操作	目的
		注释 如果您是在为永久聊天部署高可用性，可以跳过本章中的剩余任务，因为部署了 HA 时数据库要求略有不同。
步骤 5	添加外部数据库连接，第 180 页	在 IM and Presence 服务中，设置与外部数据库的连接。
步骤 6	用于永久聊天的 MSSQL 数据库的 Windows 验证，第 180 页	在设置到MSSQL外部数据库的连接时，您可以启用 Windows 验证。
步骤 7	将永久聊天室从一个外部数据库迁移到另一个数据库	在 IM and Presence Service 中，将所有永久聊天室和组从现有的外部数据库迁移到另一个相同数据库类型或不同类型的数据库。 有关如何执行外部数据库迁移的详细信息，请参阅《Cisco IM and Presence 数据库设置指南 12.5(1)SU2 版》的“将永久聊天室从一个外部数据库迁移到另一个数据库”部分。

配置群聊系统管理员

添加系统管理员以管理永久聊天系统。

过程

步骤 1 选择**消息** > **群聊系统管理员**。

步骤 2 选中**启用群聊系统管理员**。

在启用或禁用该设置后，重新启动 Cisco XCP 路由器。 启用“系统管理员”设置后，您可以动态添加系统管理员。

步骤 3 单击**新增**。

步骤 4 输入 IM 地址。

示例

IM 地址的格式必须为 name@domain。

步骤 5 输入**昵称**和**说明**。

步骤 6 单击**保存**。

下一步做什么

配置聊天室设置，第 178 页

配置聊天室设置

配置基础的聊天室设置，例如聊天室成员和占用率设置，以及每个会议室的最大用户数。

（可选）您可以选中**启用永久聊天**复选框以启用永久聊天。

过程

步骤 1 在 Cisco Unified CM IM and Presence 管理中，选择**消息** > **群聊和永久聊天**

步骤 2 选中或取消选中**系统自动管理主群聊服务器别名**复选框，以配置您是否希望系统管理聊天节点别名。

- 选中—系统自动分配聊天节点别名。 这是默认值。
- 不选中—管理员可分配其自己的聊天节点别名。

步骤 3 如果希望所有参与者离开后仍然保持聊天室，选中**启用永久聊天**复选框。

注释 这是群集范围的设置。 如果在群集中的任何节点上启用了永久聊天，则任何群集中的客户端都将能够在该节点以及该节点托管的聊天室中发现文字会议实例。

即使没有为远程群集启用永久聊天，来自远程群集的用户也可以在本地群集中发现文字会议实例和聊天室。

步骤 4 如果您已选择启用永久聊天，请为以下每个字段配置值：

- 允许的最大永久聊天室数量
- 数据库连接数
- 数据库连接心跳间隔（秒）
- 永久聊天室的超时值（分钟）

注释 在与思科支持部门联系前，请勿将**数据库连接心跳间隔**值设置为零。 心跳间隔一般用于让通过防火墙的连接保持有效。

步骤 5 在**聊天室设置**下，分配聊天室最大数。

步骤 6 完成**群聊和永久聊天设置**窗口中的剩余设置。 有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 7 单击**保存**。

下一步做什么

重新启动 Cisco XCP 文字会议管理器，第 179 页

重新启动 Cisco XCP 文字会议管理器

如果您编辑了聊天设置或将一个或多个别名添加到聊天节点，请重新启动 **Cisco XCP 文字会议管理器**服务。

过程

步骤 1 在 **Cisco Unified IM and Presence 功能配置**中，选择**工具** > **控制中心 - 功能服务**。

步骤 2 从**服务器**下拉列表中，选择 IM and Presence 节点并单击**前往**。

步骤 3 在 **IM and Presence Service** 部分，单击 **Cisco XCP 文字会议管理器**单选按键，然后单击**启动**或**重新启动**。

步骤 4 消息表明重新启动可能需要一些时间时，单击**确定**。

步骤 5 （可选）如果要验证服务是否已完全重新启动，请单击**刷新**。

下一步做什么

如果要为永久聊天部署高可用性，请继续永久聊天的高可用性任务流程，第 192 页。

否则，为永久聊天设置外部数据库，第 179 页。

为永久聊天设置外部数据库

注释 本部分讨论未部署高可用性的永久聊天。如果您在为永久聊天部署高可用性，请转到该章节了解外部数据库设置信息。

如果您在配置永久聊天室，必须为托管永久聊天室的每个节点设置单独的外部数据库实例。此外：

- 如果启用了永久聊天，则必须将外部数据库与文字会议管理器服务关联，并且数据库必须活动且可访问，否则文字会议管理器将不会启动。
- 如果将外部数据库用于永久聊天日志记录，请确保数据库容量足够大，能够处理大量信息。存档聊天室中的所有消息是可选的，因为这会增加节点流量和消耗磁盘空间。
- 使用外部数据库清理实用程序设置监控数据库大小并自动删除过期记录的作业。
- 在配置指向外部数据库的连接的数量前，请考虑您要写入的 IM 数量和产生的总流量。您配置的连接数量将允许系统扩展。虽然系统默认适合大多数安装，但您可能想为您的特定部署更改参数。

有关如何设置外部数据库的说明，请参阅《*IM and Presence Service* 外部数据库设置指南》，网址：http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html。

下一步做什么

添加外部数据库连接，第 180 页

添加外部数据库连接

从 IM and Presence Service 配置与永久聊天外部数据库的连接。 整个 IM and Presence Service 群集间至少需要一个唯一的逻辑外部数据库实例（表空间）。

过程

步骤 1 在 Cisco Unified CM IM and Presence 管理中，选择**消息** > **外部服务器设置** > **外部数据库**。

步骤 2 单击**新增**。

步骤 3 在**数据库名称**字段中，输入外部数据库实例的名称。

步骤 4 在**数据库类型**下拉列表中，选择您要部署的外部数据库的类型。

步骤 5 输入数据库的**用户名**和**密码信息**。

步骤 6 在**主机名**字段中，输入数据库的主机名和 IP 地址。

步骤 7 完成**外部数据库设置**窗口的剩余设置。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 8 单击**保存**。

步骤 9 重复此程序以创建到每个外部数据库实例的连接。

用于永久聊天的 MSSQL 数据库的 Windows 验证

为 MSSQL 外部数据库启用 Windows 验证以实现永久聊天。

开始之前

重要事项 从 14SU2 版开始支持。

要配置外部数据库连接，请参阅 添加外部数据库连接，第 180 页。

过程

	命令或操作	目的
步骤 1	从**数据库类型**下拉框中，选择外部数据库的类型作为 **Microsoft SQL 服务器**。	
步骤 2	选中**启用 Windows 验证**复选框。	
步骤 3	在**域**字段中，输入 Windows 域名。	

	命令或操作	目的
步骤 4	输入 Windows 用户的**用户名**和**密码**信息。	**注释** 通过使用 Windows 身份验证，可以在域层级创建 Windows 组，并且可以在 MSSQL 服务器上为整个组创建登录。

群聊和永久聊天相互作用和限制

表 *20:* 群聊和永久聊天相互作用和限制

功能相互作用	限制
存档聊天室加入	存档聊天室加入和离开是可选的，因为这会增加流量和消耗外部数据库服务器空间。
与匿名聊天室聊天	如果您在通过 Cisco Jabber 部署聊天（群聊或永久聊天），请确保在**群聊和永久聊天设置**窗口未选中**默认情况下聊天室是匿名的**和**聊天室所有者可以更改聊天室在默认情况下是否匿名**选项。如果选中其中任何一个复选框，则聊天将失败
数据库连接问题	如果文字会议管理器服务启动后连接外部数据库失败，文字会议管理器服务将保持活动和正常工作，但消息将不再写入数据库，并且无法创建新的永久聊天室，直到连接恢复。
OVA 要求	如果要部署永久聊天或群集间对等，可以为这些功能部署的 OVA 大小下限为 5000 位用户的 OVA。建议您部署至少 15,000 位用户的 OVA。集中式部署可能需要 25,000 位用户的 OVA，具体取决于用户群的规模。有关 OVA 选项和用户容量的其他详细信息，请参阅以下站点： **注释** 强烈建议在所有 IMP 节点上部署至少 15,000 个用户 OVA。 https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html
Microsoft SQL Server 的永久聊天字符限制	系统不会发送消息正文（包括 HTML 标记 + 文本消息）字符数超过 4000 的聊天消息。这些消息会被拒绝，并且不会存档。当 Microsoft SQL Server 用作 11.5(1)SU3 以后版本的外部数据库时，会出现此问题。有关其他详细信息，请参阅 CSCvd89705。

功能相互作用	限制
对等群集正在运行不受支持版本的适用于移动版 Jabber 的永久聊天	适用于移动版 Jabber 的永久聊天被引入 11.5(1)SU5，其在更早版本的 11.5(1)SU 上不受支持。12.0(1) 或 12.0(1)SU1 也不支持此功能。 如果您在此版本中部署了适用于移动版 Jabber 的永久聊天，并且您还使用不支持移动版 Jabber 永久聊天室的对等群集设置了群集间对等，则以下条件适用于 Jabber 移动客户端： 如果永久聊天室被托管在 11.5(1) 等不受支持的版本上： • 驻留在受支持的群集上的 Jabber 移动客户端可以加入托管在不受支持的群集上的永久聊天室，但无法选择将聊天室静音。他们可以看到全局静音选项，但此功能不起作用。 • 驻留在不受支持对等群集的 Jabber 移动客户端将无法加入任何永久聊天室。 如果永久聊天室被托管在 11.5(1)SU5 等受支持的版本上： • 驻留在受支持群集的 Jabber 移动客户端参与者将收到关于移动功能的所有永久聊天。 • 来自不受支持对等群集的 Jabber 移动客户端将无法加入任何永久聊天室。 **注释** 当 Jabber 配置文件 *(jabber-config.xml)* 设置为禁用 IM 历史记录时，永久聊天的搜索功能不起作用。
外部数据库连接和 Cisco XCP 文字会议服务	在裂脑方案中，当订阅方或发布方检测到其对等文字会议服务或任何节点出现故障时，订阅方或发布方将尝试从正常过渡到备份。 在此操作中，如果加载的对等成员的聊天室无法连接到外部数据库，则 Cisco XCP 文字会议服务将关闭。

功能相互作用	限制
如果配置了高可用性，支持永久聊天室数量	IM&P 部署上支持的永久聊天室最大数量为每个子群集 5000。 如果启用了高可用性，建议每个节点最多创建 2500 个聊天室。（尽管系统允许每个节点最多创建 5000 个聊天室）。如果在高可用性部署中为每个节点配置了超过 2500 个聊天室，则在故障转移期间，备份节点上可能会托管超过 5000 个聊天室。这可能会导致意外的性能问题，具体取决于流量负载。 系统上 5000 个聊天室的负载还取决于聊天室中参与者的人数、聊天室中消息交换的速率以及消息的大小。使用思科协作大小估算工具确保您有适当的OVA 设置用于永久聊天部署。有关协作大小估算工具的信息，请参阅： https://cucst.cloudapps.cisco.com/landing 建议在子群集的两个节点之间均衡聊天室负载。如果 IM&P 群集中有多个子群集，建议同时在所有子群集上均衡聊天室的负载。当前 IM&P 没有自动均衡聊天室负载的机制。保持聊天室负载均衡是创建聊天室的用户的责任。在聊天室创建过程中，用户必须确保使用 jabber 功能自动随机选择用于创建聊天室的节点。
将临时聊天室设为私密	临时聊天室默认情况下是公共的，但可以使用以下配置将其配置为仅限成员使用： **1.** 在 Cisco Unified CM IM and Presence 管理中，选择**消息** > **群聊和永久聊天**。 **2.** 选中**聊天室默认仅限成员使用**复选框。 **3.** 取消选中**聊天室所有者可以更改聊天室是否仅限会员使用**复选框。 **4.** 取消选中**只有协调人能够邀请他人进入仅限会员的聊天室**复选框。 **5.** 单击**保存**。 **6.** 重新启动 Cisco XCP 文字会议服务。

永久聊天示例（无高可用性）

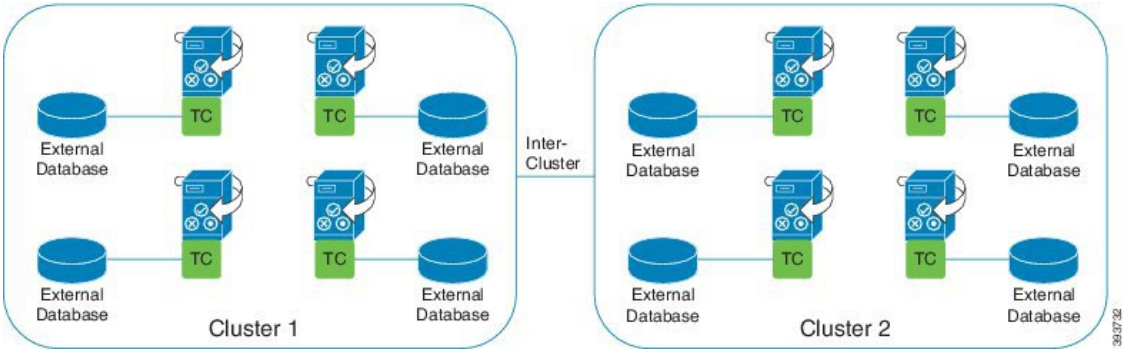
以下两个示例说明了在没有部署永久聊天高可用性情况下的永久聊天功能以及群集间对等。

注释 思科建议，如果您在部署永久聊天，应显示永久聊天的高可用性，以便向永久聊天室添加冗余。

所有群集间节点上启用永久聊天（无高可用性）

群集间网络的所有节点上都启用了永久聊天（无高可用性）。 所有节点都有一个与永久聊天相关联的外部数据库，因而所有节点都可以托管永久聊天室。

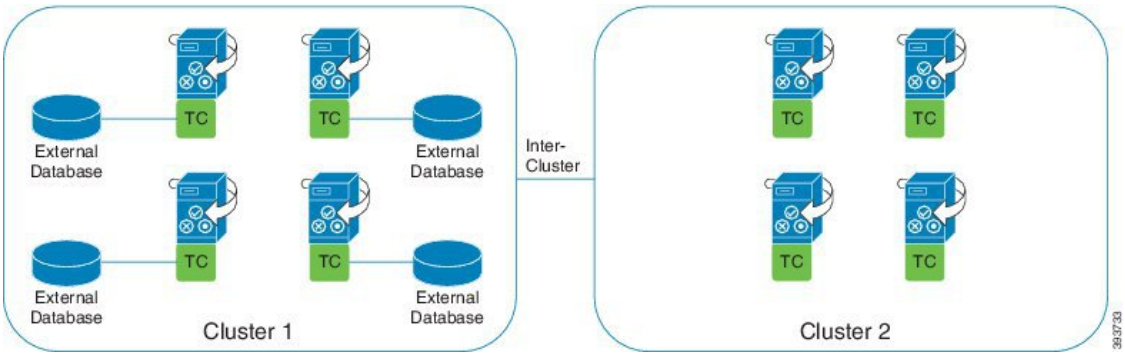
思科文字会议服务在任一群集中的所有节点上运行，使得任一群集中的所有用户都可以加入托管在任一群集任何节点上的永久聊天室。



群集间网络的一个群集中启用永久聊天（无高可用性）

只有群集 1 中的节点配置了永久聊天（无高可用性），且其有外部数据库。 群集 2 中不需要外部数据库，因为节点未配置为托管永久聊天室。

但是，思科文字会议管理器服务在任一群集中的所有节点上运行，使得任一群集中的所有用户都可以加入托管在群集 1 中的永久聊天室。



IM and Presence 中的永久聊天边界

本部分描述了 IM and Presence 中表示永久聊天 (PChat) 边界的矩阵，并举例说明了各种依存关系。

为推导永久聊天边界，我们提出了以下假设：

1. 关于每个别名/服务器/子群集/群集的聊天室数量：
    1. 服务器可能包含多个文字会议别名。
    2. 子群集包含两个服务器（节点）。

   3. 群集最多可能有三个子群集。

2. 如果启用了高可用性 (HA)，则所有支持的聊天室数量将减半。 **允许的永久聊天室最大数**的最大允许值是 2500。
3. 示例：假设每个聊天室平均 100 个用户，IM and Presence Service 可以支持：
   1. 未启用高可用性的每台服务器 3500 个永久聊天室，或
   2. 启用高可用性的每台服务器 1750 个永久聊天室。
   3. 假设每个聊天室每分钟发送一条消息，每台服务器最多可激活 273 个永久聊天室。

以下是一些说明这些依存关系的示例：

可以使用以下公式来增加每个时间段支持的聊天室，以支持的聊天室总数为代价：

新支持的聊天室数量 = 当前支持的聊天室数量 * 每个时间段当前支持的聊天室数量 (%) / 每个时间段新支持的聊天室数量 (%)

表 *21: 25K OVA* 永久聊天容量表（每台服务器）

每个聊天室的平均用户数	支持的永久聊天室数量	每个时间段支持的聊天室 消息频率 = 1/分钟	每个时间段支持的聊天室 消息频率 = 3/分钟
2	5000	100%	100%
5	5000	100%	58%
10	5000	99%	33%
15	5000	69%	23%
20	5000	53%	18%
30	5000	36%	12%
50	5000	22%	7%
100	3497	16%	5%
200	2064	14%	5%
500	926	12%	4%
1,000	482	12%	4%

注释 假设 30% 的用户有两个设备/客户端。

25K OVA 示例：

每个聊天室的平均用户数 = 10

消息频率 = 3/分钟

当前支持的聊天室数量 = 5000

每个时间段当前支持的聊天室 = 33%

每个时间段新支持的聊天室 = 50%

结果：

新支持的聊天室 = 5000 * 33/50 = 3300

表 *22: 15K OVA* 永久聊天容量表（每台服务器）

每个聊天室的平均用户数	支持的永久聊天室数量	每个时间段支持的聊天室 消息频率 **= 1/**分钟	每个时间段支持的聊天室 消息频率 **= 3/**分钟
2	5000	100%	80%
5	5000	100%	41%
10	5000	67%	22%
15	5000	46%	15%
20	5000	35%	12%
30	5000	24%	8%
50	5000	14%	5%
100	3497	10%	3%
200	2064	9%	3%
500	926	8%	3%
1,000	482	7%	2%

注释 假设 30% 的用户有两个设备/客户端。

15K OVA 示例：

每个聊天室的平均用户数 = 5

消息频率 = 3/分钟

当前支持的聊天室数量 = 5000

每个时间段当前支持的聊天室 = 41%

每个时间段新支持的聊天室 = 50%

结果：

新支持的聊天室 = 5000 * 41/50 = 4100

表 *23: 5K OVA* 永久聊天容量表（每台服务器）

每个聊天室的平均用户数	支持的永久聊天室数量	每个时间段支持的聊天室 消息频率 **= 1/**分钟	每个时间段支持的聊天室 消息频率 **= 3/**分钟
2	5000	94%	31%
5	5000	53%	18%
10	4654	33%	11%
15	4261	26%	9%
20	3929	21%	7%
30	3399	17%	6%
50	2677	13%	4%
100	1748	10%	3%
200	1032	9%	3%
500	463	8%	3%
1,000	241	7%	2%

注释 假设 30% 的用户有两个设备/客户端。

5K OVA 示例：

每个聊天室的平均用户数 = 2

消息频率 = 3/分钟

当前支持的聊天室数量 = 5000

每个时间段当前支持的聊天室 = 31%

每个时间段新支持的聊天室 = 50%

结果：

新支持的聊天室 = 5000 * 31/50 = 3100

第 18 章

配置永久聊天的高可用性

- 永久聊天的高可用性概述，第 189 页
- 永久聊天的高可用性前提条件，第 191 页
- 永久聊天的高可用性任务流程，第 192 页
- 永久聊天的高可用性使用案例，第 196 页

永久聊天的高可用性概述

永久聊天的高可用性 (HA) 是一项可选功能，如果您使用的是永久聊天室并且具有使用 Presence 冗余组配置的系统冗余，则可以部署该功能。

永久聊天的高可用性可为您的永久聊天室添加冗余和故障转移功能。 如果 IM and Presence Service 节点或文字会议 (TC) 服务出现故障，由该服务托管的所有永久聊天室将自动由备份节点或 TC 服务托管。 故障转移后，Cisco Jabber 客户端可以无缝继续使用永久聊天室。

外部服务器

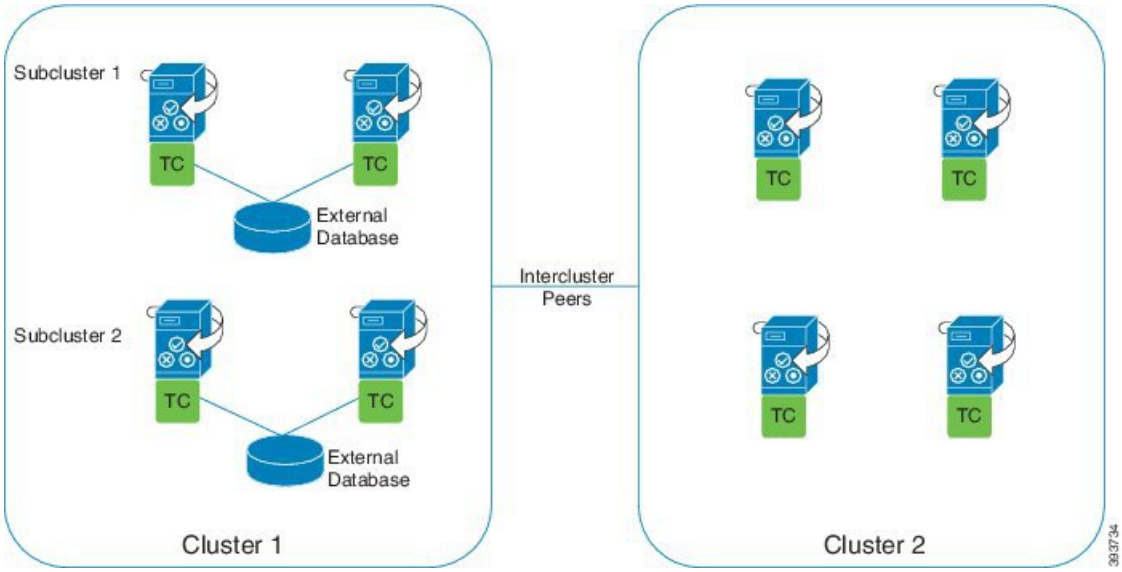
永久聊天（非高可用性）和永久聊天高可用性设置之间的主要区别在于外部数据库要求：

- 如果永久聊天部署为无高可用性，外部数据库只会连接到单个聊天节点。 托管永久聊天室的每个节点都需要一个单独的外部数据库实例。 如果聊天节点发生故障，托管在该节点上的永久聊天室将变为不可用，直到聊天节点重新启动。
- 如果部署了永久聊天的高可用性，则外部数据库实例将连接到子群集（Presence 冗余组）中的两个节点。 如果永久聊天节点出现故障，子群集中的备份节点会接管，因此聊天将继续，不会中断。

永久聊天的高可用性 - 群集间示例

下图显示的是群集间网络，其中仅在群集 1 中部署了永久聊天高可用性。 配置永久聊天高可用性之后，每个子群集都托管一个外部数据库。 群集 2 没有启用永久聊天高可用性，因此没有外部数据库要求。 但是，由于思科文字会议管理器服务在所有节点上运行，因此群集 2 中的用户可以加入托管在群集 1 中的永久聊天室。

注释 在此示例中，仅群集 1 中的聊天室配置为托管永久聊天室。 您还可以在群集 2 节点上添加永久聊天支持以及外部数据库实例。 在这种情况下，任一群集中的所有用户都可以加入托管在任一群集中的任何节点上的永久聊天室。



永久聊天（无高可用性）与永久聊天高可用性要求对比

如果您在部署永久聊天室，思科建议您部署永久聊天高可用性，这样可为您的永久聊天室添加故障转移功能。 但是，这不是强制性的。

下表介绍了部署以及不部署高可用性的永久聊天之间的差异。

表 *24:* 部署以及不部署高可用性的永久聊天之间的比较

	永久聊天（无高可用性）	永久聊天高可用性
数据库要求	对于托管永久聊天室的每个群集节点，您需要单独的外部数据库实例。 可以在同一外部数据库服务器上创建这些外部数据库实例。 **建议**：为获得最佳性能和可扩展性，请为 IM and Presence 群集的每个节点或冗余组部署唯一的逻辑外部数据库实例。 但是，这不是强制性的。 **最低要求**：您在 IM and Presence 群集间网络中必须至少有一个外部数据库实例用于永久聊天。 但是对于使用率较高的网络来说，这种部署可能不适合。 **受支持的数据库类型** • PostgreSql（版本 9.1 和更高版本） • Oracle • Microsoft SQL Server	对于托管永久聊天室的每个子群集（Presence 冗余组），您需要单独的外部数据库实例。 可以在同一外部数据库服务器上创建这些外部数据库实例。 **建议**：为获得最佳性能和可扩展性，请为 IM and Presence 群集的每个子群集部署单独的外部数据库实例。 但是，这不是强制性的。 **最低要求**：您在 IM and Presence 群集间网络中需要至少有一个外部数据库实例用于永久聊天高可用性。 但是对于使用率较高的网络来说，这种部署可能不适合。 **受支持的数据库类型** • PostgreSql（版本 9.1 和更高版本） • Oracle • Microsoft SQL Server（截至 11.5(1)SU2）
永久聊天节点出现故障时的行为	• 在节点重新启动之前，无法访问托管在故障节点上的永久聊天室。 • 如果配置了群集冗余，则故障节点上的用户将故障转移到子群集中的备份节点。 不过，他们无法从故障节点访问永久聊天室。	• 永久聊天室故障转移到子群集中的备份节点。 用户可以在不中断服务的情况下继续发送消息。 • 驻留在故障节点上的任何用户也会进行故障转移。

永久聊天的高可用性前提条件

在配置永久聊天的高可用性之前，请确保：

- 启用了永久聊天室。 有关详细信息，请参阅配置聊天室设置，第 178 页。
- 在每个 Presence 冗余组中启用了高可用性。 有关详细信息，请参阅Presence 冗余组任务流程，第 50 页。
- 您已配置外部数据库。 有关数据库设置和支持信息，请参阅《*IM and Presence Service* 数据库设置指南》。

永久聊天的高可用性任务流程

过程

	命令或操作	目的
步骤 1	设置外部数据库， 第 192 页	对于托管永久聊天室的每个子群集，您需要单独的外部数据库实例。 这些单独的外部数据库实例可以托管在同一个数据库服务器上
步骤 2	添加外部数据库连接， 第 192 页	从 IM and Presence Service 配置与外部数据库的连接。
步骤 3	验证永久聊天高可用性设置， 第 193 页	确认您的永久聊天高可用性系统设置。
步骤 4	启动 Cisco XCP 文字会议管理器服务， 第 194 页	如果 Cisco XCP 文字会议管理器服务在任何节点上停止，可使用此程序启动它。
步骤 5	合并外部数据库， 第 194 页	可选。 如果要从使用多个外部数据库配置永久聊天的早期版本升级，请执行此程序以将外部数据库合并到单个数据库中。

设置外部数据库

要部署永久聊天的高可用性，您需要为托管永久聊天室的每个子群集提供单独的外部数据库实例。 这些单独的外部数据库实例可以托管在同一个数据库服务器上。

子群集是 IM and Presence 节点的冗余对（Presence 冗余组）。 在包含 6 个节点的 IM and Presence 群集中，最多可以有三个子群集。 如果在 6 个节点的 IM and Presence 群集中启用了永久聊天的高可用性，您将有三个外部数据库实例和三个子群集对。

您可以使用 PostgreSQL、Oracle 或 Microsoft SQL Server 进行外部数据库连接。 有关设置的详细信息，请参阅《*IM and Presence Service* 数据库设置指南》。

下一步做什么

添加外部数据库连接， 第 192 页

添加外部数据库连接

从 IM and Presence Service 配置到永久聊天高可用性外部数据库实例的连接。 确保子群集中的两个节点都分配给同一个唯一的逻辑外部数据库实例。

过程

步骤 1 在 Cisco Unified CM IM and Presence 管理中，选择**消息** > **外部服务器设置** > **外部数据库**。

步骤 2 单击**新增**。

步骤 3 在**数据库名称**字段中，输入外部数据库实例的名称。

步骤 4 在**数据库类型**下拉列表中，选择您要部署的外部数据库的类型。

步骤 5 输入数据库的**用户名**和**密码信息**。

步骤 6 在**主机名**字段中，输入数据库的主机名和 IP 地址。

步骤 7 完成**外部数据库设置**窗口的剩余设置。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 8 单击**保存**。

步骤 9 重复此程序以创建到每个外部数据库实例的连接。

下一步做什么

验证永久聊天高可用性设置，第 193 页

验证永久聊天高可用性设置

此程序用于确认您的系统是否已设置好永久聊天高可用性。

注释 如果您已为 Presence 冗余组（子群集）启用高可用性，并且聊天室配置包括永久聊天，则可以完成永久聊天的高可用性。

过程

步骤 1 确认在每个子群集中启用了高可用性：

a) 从 Cisco Unified CM 管理中，选择**系统** > **Presence 冗余组**。

b) 单击**查找**并选择您想要检查的 Presence 冗余组。

c) 验证是否选中了**启用高可用性**复选框。 如果没有，请选中该复选框。

d) 单击**保存**。

e) 为群集中的每个 presence 冗余组重复上述步骤。

步骤 2 确认是否已启用永久聊天：

a) 在 Cisco Unified CM 管理中，选择**消息** > **群聊和永久聊天**。

b) 确认是否已选中**启用永久聊天**复选框。 如果没有，请选中该复选框。

c) 单击**保存**。

步骤 3 在 Cisco Unified CM 管理中，确认 **Cisco XCP 文字会议管理器服务**是否在所有群集节点上运行。

a) 选择**系统** > **Presence 拓扑**。
b) 对于每个群集节点，单击**视图**查看节点详细信息
c) 在**节点状态**下，验证 **Cisco XCP 文字会议管理器**服务是否**已启动**。
d) 在左侧的导航栏中，单击 **Presence 拓扑**返回至群集拓扑并重复上述步骤，直到您确认所有群集节点的状态。

下一步做什么

如果需要启用 **Cisco XCP 文字会议管理器服务**，启动 Cisco XCP 文字会议管理器服务，第 194 页。

启动 Cisco XCP 文字会议管理器服务

此程序用于启动 Cisco XCP 文字会议管理器服务。 此服务必须在所有群集节点上运行，这些节点上的用户才能够加入永久聊天室。

过程

步骤 1 在 **Cisco Unified IM and Presence 功能配置**中，选择**工具** > **控制中心 - 功能服务**。
步骤 2 从**服务器**下拉列表中，选择 IM and Presence 群集节点并单击**前往**。
步骤 3 在 **IM and Presence Service** 下，选择 **Cisco XCP 文字会议管理器**并单击**启动**。
步骤 4 单击**确定**。
步骤 5 （可选）如果要验证服务是否已完全重新启动，请单击**刷新**。

合并外部数据库

此程序用于合并外部数据库。

注释 Microsoft SQL 数据库不支持合并外部数据库。

可选。 如果您已从 11.5(1) 之前的版本升级，并且使用多个外部数据库来管理冗余，则使用外部数据库合并工具将外部数据库合并到单个数据库中。

示例

如果您已从 11.5(1) 之前的版本升级，并且使用连接到单独外部数据库实例的每个永久聊天节点配置了永久聊天，请执行此程序以将子群集中的两个数据库合并至连接到两个节点的单个数据库中。

开始之前

- 确保为 Presence 冗余组中的每个 IM and Presence Service 节点正确分配了两个源目标数据库。这将验证两个架构是否有效。
- 备份目标数据库的表格空间。
- 确保在目标数据库中为新合并的数据库留有足够的空间。
- 确保为源数据库和目标数据库创建的数据库用户具有运行这些命令的权限：
  - 创建表
  - 创建公共数据库链接
- 如果您的数据库用户没有这些权限，可以使用以下命令授予他们：
  - PostgreSQL：

    `CREATE EXTENTION`—这将创建 dblink，并且需要超级用户或 dbowner 权限。 此后，您可通过运行以下命令来执行 dblink 的权限：

    ```
    GRANT EXECUTE ON FUNCTION DBLINK_CONNECT(text) to <user>
    GRANT EXECUTE ON FUNCTION DBLINK_CONNECT(text,text) to <user>
    ```

  - Oracle：

    ```
    GRANT CREATE TABLE TO <user_name>;
    GRANT CREATE PUBLIC DATABASE LINK TO <user_name>;
    ```

- 如果您使用的是 PostgreSQL 外部数据库，确保在 pg_hba.conf 文件中配置了以下访问权限：
  - IM and Presence 发布方节点必须拥有每个外部数据库的完全访问权限。
  - 外部 PostgreSQL 数据库必须拥有每个数据库实例的完全访问权限。 例如，如果 192.168.10.1 上配置了外部数据库，则必须在 pg_hba.conf 文件中将每个数据库实例必须配置为 `host dbName username 192.168.10.0/24 password`。

过程

步骤 1 登录到 IM and Presence Service 发布方节点上的 **Cisco Unified CM IM and Presence 管理**。

步骤 2 在 Presence 冗余组每个 IM and Presence Service 节点的**系统** > **服务**窗口中停止 Cisco XCP 文字会议服务。

步骤 3 单击**消息** > **外部服务器设置** > **外部数据库作业**。

步骤 4 如果想要查看合并作业列表，单击**查找**。 选择**添加合并作业**以添加新的作业。

步骤 5 在**合并外部数据库**窗口中，输入以下详细信息：

- 从**数据库类型**下拉列表中选择 **Oracle** 或 **Postgres**。
- 选择两个源数据库的 IP 地址和主机名以及将包含合并数据的目标数据库。

如果选择 Oracle 作为**数据库类型**，则输入表格空间名称和数据库名称。如果选择 Postgres 作为**数据库类型**，则提供数据库名称。

步骤 6 在**功能表**窗格中，“文字会议 (TC)”复选框默认选中。 对于当前版本，其他选项不可用。

步骤 7 单击**验证选定表**。

注释 如果 Cisco XCP 文字会议服务未停止，您会收到一条错误消息。 一旦服务停止，验证将完成。

步骤 8 如果**验证详细信息**窗格中没有错误，单击**合并选定表**。

步骤 9 合并成功完成后，系统会加载**查找并列出外部数据库作业**窗口。 单击“查找”刷新窗口并查看新的作业。

单击**查找**刷新窗口并查看新的作业。

如果要查看详细信息，单击作业的 **ID**。

步骤 10 重新启动 Cisco XCP 路由器服务。

步骤 11 在两个 IM and Presence Service 节点上启动 Cisco XCP 文字会议服务。

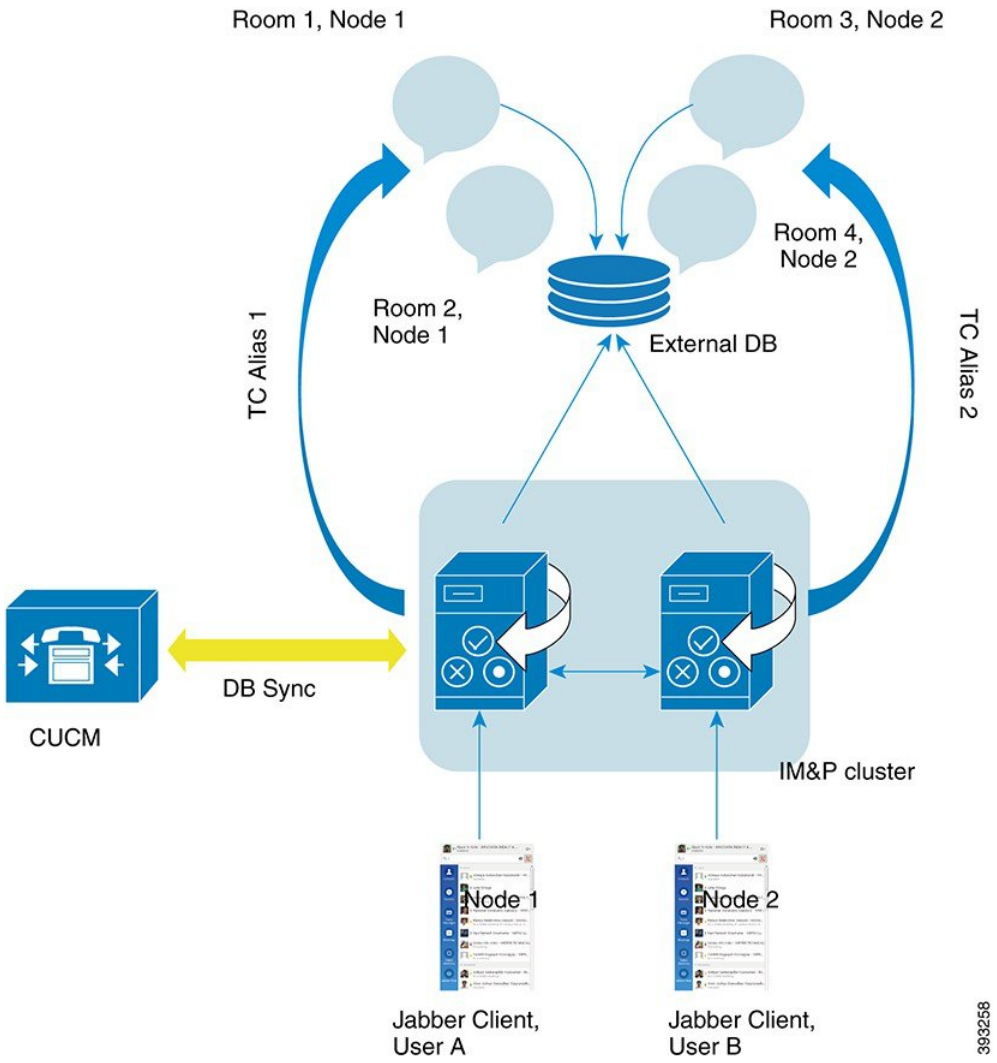
步骤 12 您必须将新合并的外部数据库（目标数据库）重新分配到 Presence 冗余组

永久聊天的高可用性使用案例

以下流展示了故障转移和故障恢复的永久聊天高可用性。 本示例介绍的是具有两个节点的 IM and Presence 群集。 IM and Presence 群集最多可以有 6 个节点，允许三个子群集。 如果永久聊天室托管在所有节点上，则需要三个单独的外部数据库实例。

注释 有了此增强功能，文字会议 (TC) 服务已成为关键服务。 因此，即使故障转移是由节点上的另一个关键服务（例如 Cisco XCP 路由器服务）发生故障引起的，TC 高可用性故障转移流仍保持不变。

图 7: 永久聊天高可用性结构



永久聊天高可用性故障转移使用案例

在本示例中，四个 IM and Presence Service 节点上有四个用户，具有两个高可用性 (HA) 对或子群集。用户分配如下：

子群集 1	子群集 2
• Andy 位于 1A 节点—1A 节点托管聊天室 • Bob 位于 1B 节点	• Catherine 位于 2A 节点 • Deborah 位于 2B 节点

1. 所有四个用户都在托管于 1A 节点上的同一聊天室聊天。
2. 文字会议 (TC) 服务在 1A 节点上无法正常工作。

3. 90 秒后，Server Recovery Manager (SRM) 确定 TC 关键服务出现故障，并启动自动故障转移。
4. 1B 节点会从 1A 节点接管用户并转换到**已执行故障转移，且关键服务没有运行**状态，然后转换到高可用性状态**在备份模式下运行**。
5. 根据高可用性故障转移模型，Andy 将自动从 1A 节点注销并登录到备份的 1B 节点。
6. 其他用户不受影响，可继续在聊天室中发布消息，但聊天室现由 1B 节点托管。
7. Andy 将进入永久聊天室，可继续在聊天室中查看或发布消息。

高可用性永久聊天回退使用案例

在本示例中，四个 IM and Presence Service 节点上有四个用户，具有两个高可用性 (HA) 对或子群集。用户分配如下：

子群集 1	子群集 2
• Andy 位于 1A 节点—1A 节点托管聊天室 • Bob 位于 1B 节点	• Catherine 位于 2A 节点 • Deborah 位于 2B 节点

1. 所有四个用户都在托管于 1A 节点上的同一聊天室聊天。
2. 文字会议 (TC) 服务在 1A 节点上无法正常工作。
3. 1B 节点会从 1A 节点接管用户并转换到**已执行故障转移，且关键服务没有运行**，然后转换到高可用性状态**在备份模式下运行**。
4. 根据高可用性故障转移模型，Andy 将自动注销并登录到备份的 1B 节点。
5. Bob、Catherine 和 Deborah 不受影响，可继续在聊天室中发布消息，但聊天室现由 1B 节点托管。
6. IM and Presence Service 管理员启动手动回退。
7. 1A 节点将转换到**收回**，1B 节点转换到**回退**。
8. Andy 从 1B 节点注销。 Bob、Catherine 和 Deborah 可继续使用永久聊天室，但一旦发生**回退**，聊天室将移回 1A 节点。
9. 1B 节点将从高可用性状态**回退**转换为**正常**，并卸载其对等节点聊天室。
10. 1A 节点将从高可用性状态**收回**转换为**正常**，并重新加载聊天室。
11. Andy 将进入永久聊天室，可继续在聊天室中查看或发布消息。

第 19 章

配置托管文件传输

- 托管文件传输概述， 第 199 页
- 托管文件传输前提条件， 第 200 页
- 托管文件传输任务流程， 第 206 页
- 排查外部文件服务器公钥和私钥， 第 217 页
- 管理托管文件传输， 第 218 页

托管文件传输概述

托管文件传输 (MFT) 可让 IM and Presence Service 客户端（例如 Cisco Jabber）将文件传输到其他用户、临时群聊室和永久聊天室。 文件将存储于外部文件服务器上的库中，事务将记录到外部数据库。

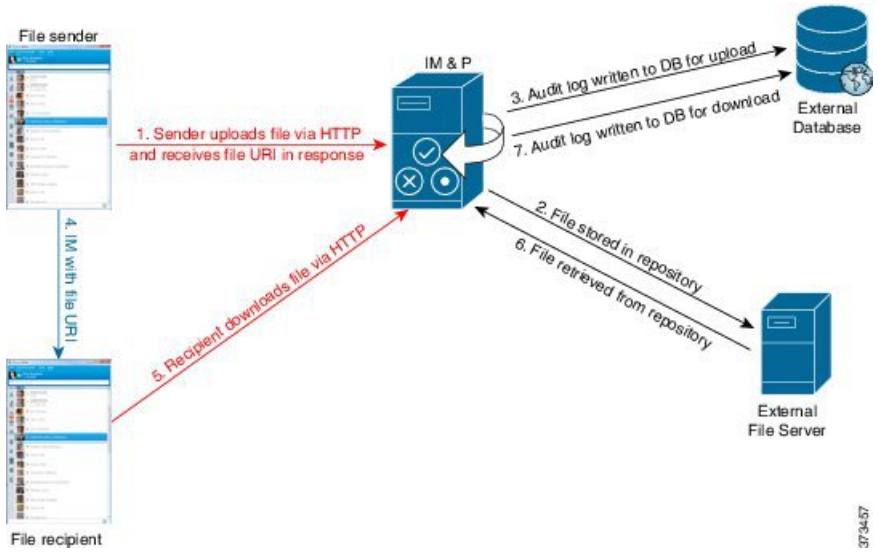
要部署托管文件传输功能，您必须部署以下服务器：

- **外部数据库**—所有文件传输都记录到外部数据库。
- **外部文件服务器**—每个传输文件的副本将保存到外部文件服务器的存储库中。

注释 此配置对于文件传输特定，并对实现法规遵从性的消息存档程序无影响。

有关使用案例，请参阅 托管文件传输呼叫流程， 第 200 页

托管文件传输呼叫流程



1. 发送者通过 HTTP 将文件上传到 IM and Presence 服务器，服务器使用文件的 URI 进行响应。
2. IM and Presence Service 服务器将文件发送到文件服务器存储库以进行存储。
3. IM and Presence Service 会向外部数据库记录表中写入一个条目，以记录此上传。
4. 发件人向接收者发送 IM。 IM 中包含文件的 URI。
5. 接收者将 HTTP 请求发送到 IM and Presence Service 以获取该文件。 IM and Presence Service 会从存储库 (6) 读取文件、将下载记录在日志表中 (7) 并将文件发送给接收者。

将文件传输到群聊或永久聊天室的流程较为相似，除了发送者向聊天室发送 IM，每个聊天室参与者发送单独的请求以下载文件。

注释 发生文件上传时，将从给定域的企业中可用的所有托管文件传输服务中选择托管文件传输服务。 文件上传将记录到外部数据库和与运行此托管文件传输服务的节点相关联的外部文件服务器。 当用户下载此文件时，相同的托管文件传输服务将处理请求，并将其记录到同一外部数据库和同一外部文件服务器，与此第二位用户驻留的位置无关。

托管文件传输前提条件

- 您还必须部署一个外部数据库和外部文件服务器。
- 确保所有服务器能够解析所分配到的 IM and Presence Service 节点上的完整 FQDN。 要让托管文件传输正常工作，必须保证这一点。

外部数据库前提条件

提示 如果您还要部署永久聊天和/或消息归档程序，可以为所有功能分配相同的外部数据库和文件服务器。 确保在确定服务器容量时考虑潜在的 IM 流量、传输的文件数和文件大小。

安装并配置外部数据库。 有关详细信息，包括受支持的数据库，请参阅《*IM and Presence Service* 数据库设置指南》。

此外，请遵循以下原则：

- IM and Presence Service 群集中每个 IM and Presence Service 节点需要一个唯一的逻辑外部数据库实例。
- 虚拟化和非虚拟化平台均支持外部数据库。
- 有关所记录元数据的完整列表，请参阅《*Cisco Unified Communications Manager* 上 *IM and Presence Service* 的数据库设置》“外部数据库工具”一章中的 AFT_LOG 表。
- 如果您是使用 IPv6 连接至外部数据库，则查阅配置 IPv6 任务流程，第 34 页以获取有关设置 IPv6 的详细信息。

外部文件服务器要求

设置外部文件服务器时，请遵循以下原则：

- 根据文件服务器容量的不同，每个 IM and Presence Service 节点都要求有其唯一的 Cisco XCP 文件传输管理器文件服务器目录，但是不同的节点可共享相同的物理文件服务器安装。
- 文件服务器必须支持 ext4 文件系统、SSHv2 和 SSH 工具。
- 文件服务器必须支持 4.9、6.x 和 7.x 的 OpenSSH 版本。

重要事项 此备注适用于 14SU3 及更高版本。

注释 从版本 14SU3 开始支持 OpenSSH 版本 8.x。

- IM and Presence Service 与外部文件服务器之间的网络吞吐量必须大于每秒 60 兆字节。

  启用托管文件传输之后，您可以使用 `show fileserver transferspeed` CLI 命令来确定您的文件服务器传输速度。 请注意，如果在系统繁忙时运行此命令，可能会影响该命令返回的值。 如需有关此命令的更多详细信息，请单击此链接查阅《*Cisco Unified Communications* 解决方案的命令行界面指南》。

外部文件服务器的分区建议

思科建议您创建一个或多个单独的文件传输存储专用的分区，因此服务器上运行的其他应用程序不会对其写入数据。 应在这些分区上创建所有文件存储目录。

请考虑以下方面：

- 在创建分区时，请务必注意 IM and Presence Service 的默认文件大小设置 (0) 允许传输的最大文件容量为 4GB。 此设置可在您设置托管文件传输时降低。
- 考虑每天上传的数量和平均文件大小。
- 确保分区拥有足够的磁盘空间承载预期文件容量。
- 例如，12000 名用户每小时传输 2 个文件，每个文件的平均大小为 100KB，则一天 8 小时的总容量为 19.2GB。

外部文件服务器目录结构

发生首个文件传输时，系统将按照本示例中所描述的自动创建带有时间戳的子目录：

- 我们会在 IM and Presence Service 节点上创建路径 `/opt/mftFileStore/node_1/`。
- 目录 `/files/` 会自动生成。
- 三个 `/chat_type/` 目录（`im`、`persistent`、`groupchat`）会自动生成。
- 日期目录 `/YYYYMMDD/` 会自动生成。
- 小时目录 `/HH/` 会自动生成。 如果一小时内传输超过 1,000 个文件，则将创建一个额外的翻转目录 `/HH.n/`。
- 系统将采用自动生成的编码资源名称保存文件，以下称为 `file_name`。

在此示例中，文件的完整路径为：`/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name`

使用我们的示例路径：

- 2014 年 8 月 11 日 15:00 到 15:59 UTC 间一对一 IM 过程中传输的文件位于以下目录：`/opt/mftFileStore/node_1/files/im/20140811/15/file_name`

  2014 年 8 月 11 日 16:00 到 16:59 UTC 间永久群聊过程中传输的文件位于以下目录：`/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`
- 2014 年 8 月 11 日 16:00 到 16:59 UTC 间临时聊天过程中传输的第 1001 个文件位于以下目录：`/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- 如果一小时内未发生文件传输，则没有为该时间段创建的目录。

注释 M and Presence 服务和文件服务器间的流量已使用 SSHFS 加密，但写入到文件服务器的文件内容采用未加密形式。

外部文件服务器用户验证

IM and Presence Service 使用 SSH 密钥验证自身和文件服务器：

- IM and Presence Service 公钥存储于文件服务器上。
- 连接过程中，SSHFS 将验证 IM and Presence Service 私钥。 这样可确保所有文件的内容均已加密。
- 文件服务器公钥存储于 IM and Presence Service 上。 这可让 IM and Presence Service 确保其连接到配置的文件服务器，并最大程度减少中间人攻击。

注释 节点公钥将在节点分配删除后失效。 如果重新分配节点，系统将自动生成一个新的节点公钥，且必须在外部文件服务器上重新配置密钥。

外部文件服务器要求

设置外部文件服务器时，请遵循以下原则：

- 根据文件服务器容量的不同，每个 IM and Presence Service 节点都要求有其唯一的 Cisco XCP 文件传输管理器文件服务器目录，但是不同的节点可共享相同的物理文件服务器安装。
- 文件服务器必须支持 ext4 文件系统、SSHv2 和 SSH 工具。
- 文件服务器必须支持 4.9、6.x 和 7.x 的 OpenSSH 版本。

重要事项 此备注适用于 14SU3 及更高版本。

注释 从版本 14SU3 开始支持 OpenSSH 版本 8.x。

- IM and Presence Service 与外部文件服务器之间的网络吞吐量必须大于每秒 60 兆字节。

  启用托管文件传输之后，您可以使用 `show fileserver transferspeed` CLI 命令来确定您的文件服务器传输速度。 请注意，如果在系统繁忙时运行此命令，可能会影响该命令返回的值。 如需有关此命令的更多详细信息，请单击此链接查阅《*Cisco Unified Communications* 解决方案的命令行界面指南》。

外部文件服务器的分区建议

思科建议您创建一个或多个单独的文件传输存储专用的分区，因此服务器上运行的其他应用程序不会对其写入数据。 应在这些分区上创建所有文件存储目录。

请考虑以下方面：

- 在创建分区时，请务必注意 IM and Presence Service 的默认文件大小设置 (0) 允许传输的最大文件容量为 4GB。 此设置可在您设置托管文件传输时降低。
- 考虑每天上传的数量和平均文件大小。
- 确保分区拥有足够的磁盘空间承载预期文件容量。
- 例如，12000 名用户每小时传输 2 个文件，每个文件的平均大小为 100KB，则一天 8 小时的总容量为 19.2GB。

外部文件服务器目录结构

发生首个文件传输时，系统将按照本示例中所描述的自动创建带有时间戳的子目录：

- 我们会在 IM and Presence Service 节点上创建路径 `/opt/mftFileStore/node_1/`。
- 目录 `/files/` 会自动生成。
- 三个 `/chat_type/` 目录（`im`、`persistent`、`groupchat`）会自动生成。
- 日期目录 `/YYYYMMDD/` 会自动生成。
- 小时目录 `/HH/` 会自动生成。 如果一小时内传输超过 1,000 个文件，则将创建一个额外的翻转目录 `/HH.n/`。
- 系统将采用自动生成的编码资源名称保存文件，以下称为 `file_name`。

在此示例中，文件的完整路径为：`/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name`

使用我们的示例路径：

- 2014 年 8 月 11 日 15:00 到 15:59 UTC 间一对一 IM 过程中传输的文件位于以下目录：`/opt/mftFileStore/node_1/files/im/20140811/15/file_name`

  2014 年 8 月 11 日 16:00 到 16:59 UTC 间永久群聊过程中传输的文件位于以下目录：`/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`
- 2014 年 8 月 11 日 16:00 到 16:59 UTC 间临时聊天过程中传输的第 1001 个文件位于以下目录：`/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- 如果一小时内未发生文件传输，则没有为该时间段创建的目录。

注释 M and Presence 服务和文件服务器间的流量已使用 SSHFS 加密，但写入到文件服务器的文件内容采用未加密形式。

外部文件服务器用户验证

IM and Presence Service 使用 SSH 密钥验证自身和文件服务器：

- IM and Presence Service 公钥存储于文件服务器上。
- 连接过程中，SSHFS 将验证 IM and Presence Service 私钥。 这样可确保所有文件的内容均已加密。
- 文件服务器公钥存储于 IM and Presence Service 上。 这可让 IM and Presence Service 确保其连接到配置的文件服务器，并最大程度减少中间人攻击。

注释 节点公钥将在节点分配删除后失效。 如果重新分配节点，系统将自动生成一个新的节点公钥，且必须在外部文件服务器上重新配置密钥。

外部文件服务器的分区建议

思科建议您创建一个或多个单独的文件传输存储专用的分区，因此服务器上运行的其他应用程序不会对其写入数据。 应在这些分区上创建所有文件存储目录。

请考虑以下方面：

- 在创建分区时，请务必注意 IM and Presence Service 的默认文件大小设置 (0) 允许传输的最大文件容量为 4GB。 此设置可在您设置托管文件传输时降低。
- 考虑每天上传的数量和平均文件大小。
- 确保分区拥有足够的磁盘空间承载预期文件容量。
- 例如，12000 名用户每小时传输 2 个文件，每个文件的平均大小为 100KB，则一天 8 小时的总容量为 19.2GB。

外部文件服务器用户验证

IM and Presence Service 使用 SSH 密钥验证自身和文件服务器：

- IM and Presence Service 公钥存储于文件服务器上。
- 连接过程中，SSHFS 将验证 IM and Presence Service 私钥。 这样可确保所有文件的内容均已加密。
- 文件服务器公钥存储于 IM and Presence Service 上。 这可让 IM and Presence Service 确保其连接到配置的文件服务器，并最大程度减少中间人攻击。

注释 节点公钥将在节点分配删除后失效。 如果重新分配节点，系统将自动生成一个新的节点公钥，且必须在外部文件服务器上重新配置密钥。

外部文件服务器目录结构

发生首个文件传输时，系统将按照本示例中所描述的自动创建带有时间戳的子目录：

- 我们会在 IM and Presence Service 节点上创建路径 `/opt/mftFileStore/node_1/`。
- 目录 `/files/` 会自动生成。
- 三个 `/chat_type/` 目录（`im`、`persistent`、`groupchat`）会自动生成。
- 日期目录 `/YYYYMMDD/` 会自动生成。
- 小时目录 `/HH/` 会自动生成。 如果一小时内传输超过 1,000 个文件，则将创建一个额外的翻转目录 `/HH.n/`。
- 系统将采用自动生成的编码资源名称保存文件，以下称为 `file_name`。

在此示例中，文件的完整路径为：`/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name`

使用我们的示例路径：

- 2014 年 8 月 11 日 15:00 到 15:59 UTC 间一对一 IM 过程中传输的文件位于以下目录：`/opt/mftFileStore/node_1/files/im/20140811/15/file_name`

  2014 年 8 月 11 日 16:00 到 16:59 UTC 间永久群聊过程中传输的文件位于以下目录：`/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`
- 2014 年 8 月 11 日 16:00 到 16:59 UTC 间临时聊天过程中传输的第 1001 个文件位于以下目录：`/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- 如果一小时内未发生文件传输，则没有为该时间段创建的目录。

注释 M and Presence 服务和文件服务器间的流量已使用 SSHFS 加密，但写入到文件服务器的文件内容采用未加密形式。

托管文件传输任务流程

完成以下任务以在 IM and Presence Service 上设置托管文件传输功能，并设置外部文件服务器。

开始之前

为托管文件传输设置外部数据库和外部文件服务器。有关要求，请参阅

- 外部数据库前提条件，第 201 页
- 外部文件服务器要求，第 201 页

有关如何配置外部数据库的详细信息，请参阅《*IM and Presence Service* 外部数据库设置指南》，网址：https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。

过程

	命令或操作	目的
步骤 1	添加外部数据库连接，第 207 页	从 IM and Presence Service 配置与外部数据库的连接。
步骤 2	设置外部文件服务器，第 208 页	在文件服务器上设置用户、目录、所有权、权限和其他任务前，设置外部文件服务器。
步骤 3	为外部文件服务器创建用户，第 209 页	为外部文件服务器设置用户。
步骤 4	设置外部文件服务器目录，第 210 页	设置外部文件服务器的顶级目录结构。
步骤 5	获取外部文件服务器公钥，第 211 页	获取外部文件服务器的公钥。
步骤 6	在 IM and Presence Service 上设置外部文件服务器，第 212 页	获取外部文件服务器的以下信息：
步骤 7	验证 Cisco XCP 文件传输管理器激活，第 214 页	Cisco XCP 文件传输管理器服务必须在启用了托管文件传输的各个节点上处于活动状态。
步骤 8	启用托管文件传输，第 215 页	在 IM and Presence Service 上启用托管文件传输。
步骤 9	验证外部服务器状态，第 216 页	验证并确保外部数据库设置和外部文件服务器设置不存在任何问题。

添加外部数据库连接

从 IM and Presence Service 配置与外部数据库的连接。使用托管文件传输时，您需要为每个 IM and Presence Service 群集节点提供唯一的逻辑外部数据库实例。

开始之前

设置每个外部数据库。有关详细信息，请参阅《*IM and Presence Service* 外部数据库设置指南》，网址：

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

过程

步骤 1 在 Cisco Unified CM IM and Presence 管理中，选择**消息** > **外部服务器设置** > **外部数据库**。
步骤 2 单击**新增**。
步骤 3 在**数据库名称**字段中，输入外部数据库实例的名称。
步骤 4 在**数据库类型**下拉列表中，选择您要部署的外部数据库的类型。
步骤 5 输入数据库的**用户名**和**密码信息**。
步骤 6 在**主机名**字段中，输入数据库的主机名和 IP 地址。
步骤 7 完成**外部数据库设置**窗口的剩余设置。有关这些字段及其设置的帮助，请参阅联机帮助。
步骤 8 单击**保存**。
步骤 9 重复此程序以创建到每个外部数据库实例的连接。

设置外部文件服务器

在文件服务器上设置用户、目录、所有权、权限和其他任务前，设置外部文件服务器。

开始之前

查看对外部文件服务器的设计建议。 有关详细信息，请参阅外部文件服务器要求，第 201 页。

过程

步骤 1 安装支持的 Linux 版本。
步骤 2 以根用户输入以下命令，验证文件服务器是否支持 SSHv2 和 OpenSSH 4.9 或更高版本：

```
# telnet localhost 22
Trying ::1...
Connected to localhost.
Escape character is '^]'.
SSH-2.0-OpenSSH_5.3
```

或者

```
# ssh -v localhost
OpenSSH_5.3p1, OpenSSL 1.0.0-fips 29 Mar 2010
debug1: Reading configuration data /root/.ssh/config ...
...debug1: Local version string SSH-2.0-OpenSSH_5.3
```

...

步骤 3 为允许私钥/公钥验证，请确保您在 `/etc/ssh/sshd_config` 文件中将以下字段设置为是。

- RSAAuthentication *yes*
- PubkeyAuthentication *yes*

如果文件中已对此加以注释，则可忽略这些设置。

提示 为增强安全性，您也可为文件传输用户禁用密码日志（在我们的示例中为 *mftuser*）。这将仅允许使用 SSH 公钥/私钥身份验证登录。

步骤 4 思科建议您创建一个或多个单独的文件传输存储专用的分区，因此服务器上运行的其他应用程序不会对其写入数据。 应在这些分区上创建所有文件存储目录。

下一步做什么

为外部文件服务器创建用户，第 209 页

为外部文件服务器创建用户

为外部文件服务器设置用户。

开始之前

设置外部文件服务器，第 208 页

过程

步骤 1 在作为根的文件服务器上，为托管文件传输功能创建用户。 此用户拥有文件存储目录结构 (示例使用 *mftuser*）并强制创建主目录 (**-m**)。

```
# useradd -m mftuser
# passwd mftuser
```

步骤 2 切换到托管文件传输用户。

```
# su mftuser
```

步骤 3 在用作密钥库的 *~mftuser* 主目录下创建 `.ssh` 目录。

```
$ mkdir ~mftuser/.ssh/
```

步骤 4 在用于为每个启用托管文件传输的节点保存公钥文本的 `.ssh` 目录下创建 `authorized_keys` 文件。

```
$ touch ~mftuser/.ssh/authorized_keys
```

步骤 5 为无密码 SSH 设置适当的权限，以让其正常运行。

```
$ chmod 700 ~mftuser（目录）
$ chmod 700 ~/.ssh（目录）
$ chmod 700 ~/.ssh/authorized_keys（文件）
```

注释　在一些 Linux 系统上，这些权限可能根据您 SSH 配置的不同而有所差异。

下一步做什么

设置外部文件服务器目录，第 210 页

设置外部文件服务器目录

设置外部文件服务器的顶级目录结构。

您可使用任何目录名称创建您希望创建的任何目录结构。 确保为每个启用了托管文件传输的节点创建一个目录。 稍后，当您在 IM and Presence Service 上启用托管文件传输时，必须为每个节点分配一个目录。

重要事项　您必须为启用了托管文件传输的各个节点创建一个目录。

注释　文件服务器分区/目录安装于用于存储文件的 IM and Presence Service 目录中。

开始之前

为外部文件服务器创建用户，第 209 页

过程

步骤 1 切换回根用户。

```
$ exit
```

步骤 2 创建一个顶级目录结构（示例中使用 `/opt/mftFileStore/`）来为启用了托管文件传输的所有 IM and Presence Service 节点托管目录。

```
# mkdir -p /opt/mftFileStore/
```

步骤 3 授予 *mftuser* 对 `/opt/mftFileStore/` 目录的唯一所有权。

```
# chownmftuser:mftuser /opt/mftFileStore/
```

步骤 4 授予 *mftuser* 对 `mftFileStore` 目录的唯一权限。

```
# chmod 700 /opt/mftFileStore/
```

步骤 5 切换到 *mftuser*。

```
# sumftuser
```

步骤 6 在 /opt/mftFileStore/ 下为每个启用了托管文件传输的节点创建一个子目录。（稍后，当您启用托管文件传输时，您将为节点分配各个目录。）

```
$ mkdir /opt/mftFileStore/{node_1,node_2,node_3}
```

注释

- 当您在 Cisco Unified CM IM and Presence 管理中设置文件服务器时，这些目录和路径将在您配置的**外部文件服务器目录**字段中使用。
- 如果您有多个写入到此文件服务器的 IM and Presence Service 节点，则您必须为各个节点定义目标目录，就像我们在示例中为三个节点 {*node_1*,*node_2*,*node_3*} 所做的一样。
- 在每个节点的目录中，传输类型子目录（im、groupchat 和 persistent) 由 IM and Presence Service 自动创建，所有后续目录也是如此。

下一步做什么

获取外部文件服务器公钥，第 211 页

获取外部文件服务器公钥

获取外部文件服务器的公钥。

开始之前

设置外部文件服务器目录，第 210 页

过程

步骤 1 要检索文件服务器的公钥，请输入：

```
$ ssh-keyscan -t rsa host
```

其中 *host* 是文件服务器的主机名、FQDN 或 IP 地址。

警告

- 为避免中间人攻击（此时文件服务器公钥具有欺骗性），您必须确认通过 **ssh-keyscan -t rsa***host* 命令返回的公钥值是文件服务器的实际公钥。
- 在文件服务器上，转到 ssh_host_rsa_key.pub 文件的位置（在我们的系统中，其位于 /etc/ssh/ 下），并确认公钥文件的内容减去主机（主机不在文件服务器上的 ssh_host_rsa_key.pub 文件中）与命令 **ssh-keyscan -t rsa***host* 返回的公钥值相匹配。

步骤 2 复制 **ssh-keyscan -t rsa***host* 命令的结果，而不是 ssh_host_rsa_key.pub 文件中的值。 确保复制整个密钥值，从服务器主机名、FQDN 或 IP 地址一直到最后。

注释 在大多数情况中，服务器密钥以主机名或 FQDN 开始，但其也有可能以 IP 地址开始。

例如，应复制：

hostname ssh-rsa AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs...

...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/sdug+/+N9MQ==

（使用了省略号）。

步骤 3 将 **ssh-keyscan -t rsa***host* 命令的结果保存到一个文本文件。 您在 *IM and Presence Service* 上部署外部文件服务器时需要用到该文件。

步骤 4 打开您创建的 authorized_keys 文件并将其保持打开状态。 当您稍后在 IM and Presence Service 上设置文件服务器时需要用到它。

注释 如果您不能检索公钥，请参阅排查外部文件服务器公钥和私钥，第 217 页获得进一步的帮助。

下一步做什么

在 IM and Presence Service 上设置外部文件服务器，第 212 页

在 IM and Presence Service 上设置外部文件服务器

您必须为将启用托管文件传输的群集中的每个节点配置一个外部文件服务器实例。

外部文件服务器实例不必是外部文件服务器的物理实例。 但是请注意，对于给定主机名，您必须为各个外部文件服务器实例指定唯一的外部文件服务器目录路径。 您可从一个相同的节点配置所有外部文件服务器实例。

开始之前

获取外部文件服务器公钥，第 211 页

获取外部文件服务器的以下信息：

- 主机名、FQDN 或 IP 地址
- 公钥
- 文件存储目录的路径
- 用户名

过程

步骤 1 在 **Cisco Unified CM IM and Presence** 管理中，选择消息 > 外部服务器设置 > 外部文件服务器。

步骤 2 单击新增。
此时将显示外部文件服务器窗口。

步骤 3 输入服务器详细信息。 有关这些字段及其配置选项的帮助，请参阅外部文件服务器字段，第 213 页。

步骤 4 单击保存。

步骤 5 重复此过程，直到为启用托管文件传输的每个群集节点创建了单独的外部文件服务器实例。

下一步做什么

验证 Cisco XCP 文件传输管理器激活，第 214 页

外部文件服务器字段

字段	说明
名称	输入文件服务器的名称。 理想的情况下，服务器名称应具有足够的描述性，从而能立即识别。 最大字符数：128。允许的值包括字母数字、连字符和下划线。
主机/IP 地址	输入文件服务器的主机名或 IP 地址。 注释 • 为主机/IP 地址字段所输入的值必须与为“外部文件服务器公钥”字段（随后）所输入的密钥开端匹配。 • 如果您更改此设置，则您必须重启 Cisco XCP 路由器服务。

字段	说明
外部文件服务器公钥	将文件服务器公钥（您按桌面保存为文本文件的密钥）粘贴到此字段。 如果您未保存密钥，您可通过在文件服务器上运行以下命令从文件服务器检索该密钥： `$ ssh-keyscan -t rsa`*`host`*（在文件服务器上）。 其中 *`host`* 是文件服务器的 IP 地址、主机名或 FQDN。 您必须复制和粘贴从主机名、FQDN 或 IP 地址开始一直到最后的整个密钥文本。 例如，应复制： extFileServer.cisco.com ssh-rsa AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs... ...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/sdug+/+N9MQ== （使用了省略号）。 **重要事项** 此值必须以您为“主机/IP 地址”字段所输入的主机名、FQDN 或 IP 地址开始。 例如，如果在“主机/IP 地址”字段使用了 extFileServer，则该字段必须以 extFileServer 开始，其后跟整个 rsa 密钥。
外部文件服务器目录	文件服务器目录分层顶部的路径。 例如 `/opt/mftFileStore/node_1/`
用户名	外部文件服务器管理员的用户名。

验证 Cisco XCP 文件传输管理器激活

Cisco XCP 文件传输管理器服务必须在启用了托管文件传输的各个节点上处于活动状态。

该服务仅在分配了外部数据库和外部文件服务器时，以及服务能够连接数据库并安装文件服务器时启动。

开始之前

在 IM and Presence Service 上设置外部文件服务器， 第 212 页

过程

步骤 1 在群集的任何节点上，登录到 **Cisco Unified IM and Presence 功能配置**用户界面。

步骤 2 选择**工具** > **服务启动**。

步骤 3 从**服务器**下拉列表中，选择一个启用了托管文件传输的节点，然后单击**前往**。

步骤 4 确认 **Cisco XCP 文件传输管理器**服务的**激活状态**是否为**已激活**。

步骤 5 如果服务禁用，则选中 **Cisco XCP 文件传输管理器**复选框，然后单击**保存**。

步骤 6 对启用了托管文件传输的所有群集节点重复此程序。

下一步做什么

启用托管文件传输，第 215 页

启用托管文件传输

在 IM and Presence Service 上启用托管文件传输。

过程

步骤 1 登录到 **Cisco Unified CM IM and Presence 管理**，选择**消息** > **文件传输**。 **文件传输**窗口将打开。

步骤 2 在“文件传输配置”区域，根据您的部署，选择**托管文件传输**或**托管和对等文件传输**。 请参阅文件传输选项，第 216 页。

步骤 3 输入最大文件大小。 如果您输入 0，则应用最大大小 (4GB)。

注释 您必须重新启动 Cisco XCP 路由器服务，此更改才能生效。

步骤 4 在“托管文件传输分配”区域，为群集中的各个节点分配外部数据库和外部文件服务器。

a) 外部数据库 - 从下拉列表选择外部数据库的名称。

b) 外部文件服务器 - 从下拉列表选择外部文件服务器的名称。

步骤 5 单击**保存**。

单击**保存**后，将显示各个分配的**节点公钥**链接。

步骤 6 对于启用了托管文件传输的群集中的各个节点，您必须将节点的整个公钥复制到外部文件服务器的 `authorized_keys` 文件。

a) 要显示节点的公钥，向下滚动到“托管文件传输分配”区域，并单击**节点公钥**链接。 复制对话框的整个内容，包括节点的 IP 地址、主机名或 FQDN。

示例：

```
ssh-rsa yc2EAAAABIwAAAQEAp2g+S2XDEzptN11S5h5nwVleKBnfG2pdW6KiLfzu/sFLegioIIqA8jBguNY/...
...5s+tusrtBBuciCkH5gfXwrsFS0O0AlfFvwnfq1xmKmIS9W2rf0Qp+A+G4MVpTxHgaonw== imp@imp_node
```

（使用了省略号）。

警告
- 如果配置了托管文件传输功能，且“文件传输类型”更改为**禁用**或**对等**，则所有托管文件传输设置都将被删除。
- 节点的密钥将在节点从外部数据库和文件服务器取消分配时失效。

b) 在外部文件服务器上，打开您在 *mftuser* 的主目录下创建的 `~mftuser/.ssh/authorized_keys` 文件（如果尚未打开），然后（在新的一行）添加每个节点的公钥。

注释 `authorized_keys` 文件必须包含启用了分配到文件服务器的 IM and Presence Service 节点的各个托管文件传输的公钥。

c) 保存并关闭 `authorized_keys` 文件。

步骤 7 （可选）配置托管文件传输服务参数，以定义为外部文件服务器磁盘空间生成 RTMT 警报的阈值。

步骤 8 在启用了托管文件传输的所有节点上重新启动 Cisco XCP 路由器服务。 请参阅“重新启动 Cisco XCP 路由器服务”。

下一步做什么

验证外部服务器状态，第 216 页

文件传输选项

您可在“文件传输”窗口中配置以下文件传输选项之一：

文件传输选项	说明
禁用	文件传输对群集禁用。
点对点	允许一对一文件传输，但不在服务器上存档或存储文件。 不支持群聊文件传输。
托管文件传输	允许一对一和组文件传输。 文件传输将记录到数据库中，传输的文件将存储于服务器。 客户端还必须支持托管文件传输，否则不允许进行文件传输。
托管和对等文件传输	允许一对一和组文件传输。 仅在客户端支持托管文件传输时，文件传输才将记录到数据库中，且传输的文件将存储于服务器。 如果客户端不支持托管文件传输，此选项等同于“对等”选项。

注释 如果在节点上配置了托管文件传输，且您将“文件传输类型”更改为**禁用**或**对等**，则请注意外部数据库和该节点外部文件服务器的映射设置将删除。 如果您为节点重新启用了托管文件传输，则数据库和文件服务器仍将处于配置状态，但是您必须重新分配它们。

在升级到 IM and Presence Service 10.5(2) 版或更高版本后，根据您预升级设置的不同，系统将选中**禁用**或**对等**选项。

验证外部服务器状态

验证并确保外部数据库设置和外部文件服务器设置不存在任何问题。

开始之前

启用托管文件传输，第 215 页

过程

步骤 1 验证外部数据库的状态：

a) 在 **Cisco Unified CM IM and Presence 管理**中，选择**消息** > **外部服务器设置** > **外部数据库**。

b) 检查“外部数据库状态”区域中提供的信息。

步骤 2 在您需要验证是否已分配外部文件服务器的 IM and Presence Service 节点上：

a) 在 **Cisco Unified CM IM and Presence 管理**中，选择**消息** > **外部服务器设置** > **外部文件服务器**。

b) 检查“外部文件服务器状态”区域中的信息，以验证连接是否无故障。

排查外部文件服务器公钥和私钥

服务器私钥/公钥对生成后，私钥通常将写入到 `/etc/ssh/ssh_host_rsa_key`

公钥将写入到 `/etc/ssh/ssh_host_rsa_key.pub`

如果这些文件不存在，则完成以下程序：

过程

步骤 1 输入以下命令：

```
$ ssh-keygen -t rsa -b 2048
```

步骤 2 复制文件服务器的公钥。

您必须复制整个公钥文本的字符串，包括主机名、FQDN 或 IP 地址（例如 *hostname* ssh-rsa AAAAB3NzaC1yc...）。 在大多数 Linux 部署中，密钥都包含服务器的主机名或 FQDN。

提示 如果 `$ ssh-keygen -t rsa -b 2048` 命令的输出不包含主机名，则使用以下命令的输出：
`$ ssh-keyscan`*`hostname`*

步骤 3 对于每个配置为使用此文件服务器的 IM and Presence Service 节点，请将公钥粘贴到**外部文件服务器配置**窗口中的**外部文件服务器公钥**字段内。

重要事项 必须为托管文件传输功能配置无密码的 SSH。 有关无密码 SSH 的完整配置说明，请参阅 SSHD 主页。

注释 在检查从发布方节点到订阅方节点的状态时，信息消息“可以从此处运行此外部文件服务器的诊断测试”将显示，反之亦然。

在日志中我们会看到"pingable": "-7"，这意味着我们正在查看未配置外部文件服务器的其他节点的状态。

我们在发布方节点上配置外部文件服务器，并在外部文件服务器的“Authorized_key”文件中共享发布方节点公钥。

管理托管文件传输

配置托管文件传输后，您需要持续管理此功能。 例如，您需要建立一个系统来管理文件服务器和数据库增长。 托管文件传输管理概述，第 267 页.

第 20 章

配置多设备消息传送

- 多设备消息传送概述， 第 219 页
- 多设备消息传送前提条件， 第 219 页
- 配置多设备消息传送， 第 220 页
- 多设备消息传送流程使用案例， 第 220 页
- 多设备消息传送静默模式使用案例， 第 221 页
- 多设备消息传送相互作用和限制， 第 222 页
- 多设备消息传送计数器， 第 222 页
- 设备容量监控， 第 223 页
- 用于设备容量监控的用户会话报告， 第 224 页

多设备消息传送概述

通过多设备消息传送 (MDM)，您可以在当前登录的所有设备上跟踪一对一即时消息 (IM) 对话。如果您使用的是启用了 MDM 的桌面客户端和移动设备，消息将发送或复制到这两个设备。 在您参与对话时，读取通知也会在两台设备上同步。

借助 MDM，您可以在任意设备之间切换的同时维护 IM 对话。 例如，如果您在台式机上启动 IM 对话，但必须离开参加一个会议，则可以继续在移动设备上进行 IM 对话。 必须登录客户端才能启用 MDM。 登出客户端将不会显示发送或收到的 IM 或通知。

MDM 支持静默模式，有助于节省移动设备的电池电量。 当不使用移动客户端时，Jabber 客户端会自动打开静默模式。 当客户端再次变为活动状态时，静默模式将关闭。

多设备消息传送前提条件

必须启用即时消息。 有关详细信息，请参阅 群聊和永久聊天任务流程， 第 176 页

注释 如果计划启用多设备消息传送，请根据客户端数量而不是用户数量来衡量部署，因为每个用户可能有多个 Jabber 客户端。例如，如果您有 25000 位用户，每位用户有两个 Jabber 客户端，则您的部署需要 50000 位用户的容量。

配置多设备消息传送

多设备消息传送默认启用。 您可以执行此程序以禁用该功能，或在禁用该功能后将其重新打开。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**系统** > **服务参数**。

步骤 2 从**服务器**下拉列表中，选择 IM and Presence Service 发布方节点。

步骤 3 从**服务**下拉列表中选择 **Cisco XCP 路由器**（**活动**）。

步骤 4 从**启用多设备消息传送**下拉列表中，选择**启用**（默认值）或**禁用**。

步骤 5 单击**保存**。

步骤 6 重新启动 Cisco XCP 路由器服务：

a) 导航到 Cisco Unified IM and Presence 功能配置并选择**工具** > **控制中心 - 网络服务**。

b) 从**服务器**下拉列表框中，选择 IM and Presence 发布方节点。

c) 在 **IM and Presence Service** 下，选择 **Cisco XCP 路由器**并单击**重新启动**。

多设备消息传送流程使用案例

此流程描述了当用户 Alice 在其笔记本电脑和移动设备上启用了 MDM 时系统会如何处理消息和通知。

1. Alice 在她的笔记本电脑上打开了一个 Jabber 客户端，并且还在她的移动设备上使用 Jabber。
2. Alice 从 Bob 处接收即时消息 (IM)。

   她的笔记本电脑上会收到通知并显示新消息指示符。 她的移动设备上会收到一条新消息，但没有通知。

   注释 IM 始终发送给启用 MDM 的所有客户端。 通知仅显示在活动的 Jabber 客户端上，如果没有活动的 Jabber 客户端，系统会向所有 Jabber 客户端发送通知。

3. Alice 与 Bob 聊天 20 分钟。

在聊天过程中，Alice 像往常一样使用笔记本电脑，移动设备上会收到新消息并标记为已读。 系统不会向其移动设备发送任何通知。

4. 当 Alice 收到来自第三个用户 Colin 的三条聊天消息时，Alice 设备的响应与在步骤 2 中一样。
5. Alice 没有回应并合上了笔记本电脑。 在乘坐公共汽车回家的路上，Alice 又收到一条 Bob 发来的消息。

   在这种情况下，她的笔记本电脑和移动设备都会收到新消息和通知。
6. Alice 打开她的移动设备，并看到 Bob 和 Colin 发来的新消息。 这些消息也发送到其笔记本电脑上了。
7. Alice 在她的移动设备上读取消息，当她这样做时，消息在笔记本电脑和移动设备上都会标记为已读。

多设备消息传送静默模式使用案例

此流程描述了多设备消息传送用于在移动设备上启用静默模式的步骤。

1. Alice 正在笔记本电脑和移动设备上使用 Jabber。 她通过笔记本电脑上的 Jabber 读了 Bob 发来的消息并回了信。
2. 然后 Alice 开始使用移动设备上的另一个应用程序。 其移动设备上的 Jabber 在后台继续运行。
3. 因为其移动设备上的 Jabber 现在在后台运行，所以系统会自动启用静默模式。
4. Bob 又给 Alice 发来一条消息。 因为 Alice 移动设备上的 Jabber 处于静默模式，所以消息未送达。 系统对 Bob 回给 Alice 的消息进行了缓冲处理。
5. 消息缓冲将继续，直至发生以下触发事件之一：
   - 收到 `<iq>` 段。
   - 当 Alice 当前没有其他活动客户端在任何其他设备上运行时，收到 `<message>` 段。

     注释 活动客户端是在前五分钟内发送可用在线状态或即时消息的最后一个客户端。
   - 达到此缓冲限制。
6. 当 Alice 在其移动设备上切换回 Jabber 时，它再次变为活动状态。 Bob 经缓冲的消息将送达，Alice 能够看到。

多设备消息传送相互作用和限制

下表总结了多设备消息传送 (MDM) 功能的功能相互作用和限制。

表 *25:* 多设备消息传送相互作用和限制

功能	相互作用或限制
Cisco Jabber 客户端	自 11.7 版起的所有 Jabber 客户端都支持 MDM。
群聊	群聊适用于从任何设备登录的所有 MDM 用户。
消息存档程序	MDM 可与消息存档程序功能兼容。
托管文件传输	文件传输适用于从任何设备登录的所有 MDM 用户。
通过 Expressway 的 Mobile and Remote Access	对于通过 Cisco Expressway 连接到 IM and Presence Service 的 Mobile and Remote Access 客户端，您必须至少运行 Expressway X8.8 才能使用 MDM。
Server Recovery Manager	如果发生故障转移，多设备消息传送功能会导致 IM and Presence Service 上的服务器恢复延迟。 如果配置了多设备消息传送的系统上发生服务器故障转移，则故障转移时间通常是使用 **Cisco Server Recovery Manager** 服务参数指定的时间的两倍。
第三方客户端	MDM 可与不支持此功能的第三方客户端兼容。

多设备消息传送计数器

多设备消息传送 (MDM) 使用 Cisco XCP MDM 计数器组中的以下计数器：

计数器名称	说明
MDMSessions	当前启用了 MDM 的会话数。
MDMSilentModeSessions	当前处于静音模式的会话数。
MDMQuietModeSessions	当前处于静默模式的会话数。
MDMBufferFlushes	MDM 缓存刷新总数。
MDMBufferFlushesLimitReached	由于达到整体缓存大小限制而导致的 MDM 缓存刷新总数。
MDMBufferFlushPacketCount	最后一个时段中刷新的信息包数量。
MDMBufferAvgQueuedTime	MDM缓存刷新之前的平均时间（以秒为单位）。

设备容量监控

当您启用多个设备消息传送 (MDM) 时，从多个设备登录的每个用户都会在 IM and Presence 服务器上添加流量负载。 当活动登录用户的数量达到一定的限制时，这将导致资源短缺（内存消耗、CPU 利用率）以及意外的性能问题和故障。

设备容量监控功能可帮助您解决这些问题，方法是实施额外的计数器来协助监控节点上创建的会话数量。

IM&P 节点上会创建以下 Jabber Session Manager (JSM) 会话：

- 组合 JSM 会话 — 当用户被分配到节点时创建。
- 活动 JSM 会话
  - 内部用户登录。
  - 场外用户登录。
- 幻影 JSM 会话 — 适用于启用了推送的用户，用于处理 HA 故障转移用例。
- Spark 互操作 JSM 会话 — 适用于混合用户。

以下计数器被引入用于监控 JSM 会话：

- **JsmClientSessionsActive**
- **JsmPhantomSessionsActive**
- **JsmHybridSessionsActive**

此外，还引入了一个新的计数器 **JSMSessionsExceedsThreshold** 来监控 JSM 阈值限制，这是基于 JSM 会话计数器和 OVA 大小计算得出的。

如果此计数器的阈值限制超出默认值 80% 的时间达到 10 分钟，系统会在实时监控工具 (RTMT) 中引发 **JSMSessionsExceedsThreshold** 警告。

使用 RTMT 配置警告值

您可以遵照此程序使用 RTMT 配置 **JSMSessionsExceedsThreshold** 警告值。

过程

步骤 1 登录到**实时监控工具 (RTMT)**，选择**系统** > **工具** > **警告中心**。

步骤 2 单击 **IM and Presence**，然后选择 **JSMSessionsExceedsThreshold** 警告名称。

步骤 3 右键单击 **JSMSessionsExceedsThreshold** 并选择**设置警告/属性**。

步骤 4 选中**启用警告**复选框以启用警告。

步骤 5 设置 JSM 会话阈值超出值的数量百分比限制，默认值为 80%。

步骤 6 单击**保存**。

步骤 7 设置警告的频率和安排，默认情况下，警告每 10 分钟触发一次。

步骤 8 单击**下一步**。

步骤 9 单击**保存**。

每个节点支持的 JSM 会话

下表列出了基于测试的每个节点可以支持的 JSM 会话总数：

OVA 大小	**JSM** 会话计数为 **OVA** 容量的 **1.5** 倍
5K OVA	7.5K
15K OVA	22.5K
25K OVA	37.5K

注释 如果启用了高可用性，并且两个节点都处于“主用-主用”配置中，则：

1. 每个节点可以支持的 JSM 会话总数将为上述容量的 50%，因为自定义警报中存在一个限制，即只能按节点配置它。
2. 您必须根据HA 配置修改 **JSMSessionsExceedsThreshold** 计数器值。

建议的措施：

引发自定义警告时，从特定节点的 RTMT 工具检查内存和 CPU 使用率计数器。 如果内存和 CPU 使用率计数器的值超出阈值限制，建议在 IM&P 节点之间均衡用户负载。 当前 IM&P 没有自动在节点之间均衡用户负载的机制。

用于设备容量监控的用户会话报告

此程序用于查看用户会话报告。 您可以通过此报告查看从群集、子群集和节点级别的多个设备登录的活动用户的详细信息。

过程

步骤 1 登录到 **Cisco Unified IM and Presence 报告**。

步骤 2 选择**系统报告** > **IM and Presence 用户会话报告**。

步骤 3 在报告窗口中选择**生成报告**（条形图）图标以生成当前时间的用户会话报告。

步骤 4 单击**确定**。

步骤 5 在**报告名称**列下，单击 **IM and Presence 用户会话报告**。

注释
- 生成此报告可能需要 2 分钟或更长时间。
- 此报告会显示：状态冗余组；节点名称；从一个或多个设备登录的用户数；群集、子群集和节点级别的会话总数；以及生成报告的日期和时间戳。

步骤 6 单击报告窗口右侧的**下载**（绿色箭头）图标，下载CSV格式的群集、子群集和节点级别的用户会话报告。

步骤 7 单击**从一个或多个设备登录的用户数**列中所列的值，为特定节点生成详细的基于用户的报告。

步骤 8 单击报告窗口右侧的**下载**（绿色箭头）图标，以 CSV 格式按节点下载用户级别的详细信息。

注释 当您将鼠标悬停在**会话数**列上时，**设备类型**提示框会显示您登录所使用的设备的类型。

例如，设备类型可以是 Desktop、iPad、iPhone。

第 21 章

配置企业组

- 企业组概览， 第 227 页
- 企业组前提条件， 第 228 页
- 企业组配置任务流程， 第 229 页
- 企业组部署模型 (Active Directory)， 第 233 页
- 企业组限制， 第 236 页

企业组概览

配置企业组时，Cisco Unified Communications Manager 会在将其数据库与外部 LDAP 目录同步时纳入用户组。 在 Cisco Unified CM 管理中，您可以在“用户组”窗口中查看同步的组。

此功能还可以帮助管理员：

- 为具有类似特征的用户设置通用功能集（例如，销售和会计团队）。
- 将消息发送到特定组中的所有用户。
- 为特定组的所有成员配置统一的访问权限

此功能还可以帮助 Cisco Jabber 用户快速构建具有共同特征的用户的联系人列表。 Cisco Jabber 用户可以在外部 LDAP 目录中搜索用户组，然后将其添加到其联系人列表中。 例如，Jabber 用户可以搜索外部LDAP目录并将销售组添加到联系人列表，从而也将所有销售团队成员添加到联系人列表中。 如果组在外部目录中更新，则用户的联系人列表会自动更新。

Windows 上的 Microsoft Active Directory 支持将企业组用作外部 LDAP 目录。

注释 如果禁用“企业组”功能，Cisco Jabber 用户将无法搜索企业组或查看已添加到其联系人列表的组。 如果禁用此功能时用户已经登录，在用户注销前该组将一直可见。 用户再次登录时，该组将不可见

安全组

安全组是企业组的子功能。 Cisco Jabber 用户还可搜索安全组并将其添加至联系人列表。 要设置该功能，管理员必须配置一个自定义LDAP过滤器并将其应用到已配置的LDAP目录同步。 仅Microsoft Active Directory 支持安全组。

可允许的最多条目数

配置企业组时，请确保配置处理组的联系人列表最大值

- 联系人列表中允许的最多条目数是联系人列表条目数与已添加到联系人列表的组中的条目数之和。
- 联系人列表的最多条目数 =（联系人列表条目数）+（组中条目数）
- 启用“企业组”功能时，如果联系人列表的条目数不超过允许的最多条目数，Cisco Jabber用户就可将组添加到联系人列表。 该功能禁用时，如果超过了允许的最多条目数，则在该功能启用前用户不受限制。 如果用户在该功能启用后继续登录，将不会显示错误消息。 用户注销和再次登录时，将显示错误消息，要求用户删除过量条目。

企业组前提条件

此功能假定您已经使用以下条件配置了 LDAP 目录同步计划。 如需有关配置 LDAP 目录同步的详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》的“从 LDAP 目录导入用户”一章。

- 必须激活 Cisco DirSync 服务
- LDAP 目录同步必须包含用户和组
- 必须安排使用 **LDAP 目录同步计划**配置的常规 LDAP 目录同步。

受支持的 LDAP 目录

企业组仅支持 Microsoft Active Directory。

LDAP 目录	企业组支持
Microsoft Active Directory	企业组和安全组均受支持。
OpenLDAP	Windows 上的 OpenLDAP 具有以下支持： • 仅支持 `GroupOfNames` 对象类 • OpenLDAP 不支持安全组。 • 最低版本为 2.4.42。 • 不支持 Linux 上的 OpenLDAP。

LDAP 目录	企业组支持
其他 LDAP 目录	不支持。

企业组配置任务流程

以下任务用于配置企业组功能。

过程

	命令或操作	目的
步骤 1	从 LDAP 目录验证组同步， 第 229 页	确认您的 LDAP 目录同步包括用户和组。
步骤 2	启用企业组， 第 230 页	完成此任务以使 Cisco Jabber 用户能够在 Microsoft Active Directory 中搜索企业组并将其添加到其联系人列表中。
步骤 3	更新 OpenLDAP 配置文件， 第 230 页	（仅 OpenLDAP）编辑 Windows 的 OpenLDAP 目录中的配置文件 `slapd.conf`。
步骤 4	启用安全组， 第 230 页	（可选）如果您希望 Cisco Jabber 用户能够搜索安全组并将安全组添加到其联系人列表，请完成此任务流程。
步骤 5	查看用户组， 第 233 页	（可选）查看与 Cisco Unified Communications Manager 数据库同步的 企业组和安全组。

从 LDAP 目录验证组同步

此程序用于确认您的 LDAP 目录同步是否包含用户和组。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**服务器** > **LDAP** > **LDAP 目录**。

步骤 2 单击**查找**并选择要从中同步企业组的 LDAP 目录。

步骤 3 确认**同步**字段是否选定了**用户和组**。

步骤 4 在“LDAP 目录”配置窗口中完成剩余字段。 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**。

启用企业组

配置系统以在 LDAP 目录同步中包含企业组。

过程

步骤 1 从“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，将 **Cisco IM and Presence 上的目录组操作**参数设置为**启用**。

步骤 3 输入**允许在线状态信息的最大企业组大小**参数的值。 允许的范围是 1 到 200 个用户，默认值为 100 个用户。

步骤 4 从**企业组同步模式**下拉列表中配置您要定期执行的 LDAP 同步：**无**、**差异同步**、**完全同步**。

注释 请参阅企业参数帮助以获取有关配置这些字段的其他帮助。

步骤 5 单击**保存**。

更新 OpenLDAP 配置文件

如果您在 Windows 上通过 OpenLDAP 配置企业组，必须更新 OpenLDAP 目录中的 `slapd.conf` 文件。

过程

步骤 1 在 Windows 的 OpenLDAP 文件目录中，浏览到 `slapd.conf` 文件。

步骤 2 在文本编辑器中打开文件。

步骤 3 在文件中添加以下文本：

```
moduleload memberof.la
overlay memberof
memberof-group-oc groupOfNames
memberof-member-ad member
memberof-memberof-ad memberof
memberof-refint TRUE
cachesize 160000
```

步骤 4 保存文件。

步骤 5 重新启动 OpenLDAP 目录。

启用安全组

如果您要允许 Cisco Jabber 用户能将安全组添加至其联系人列表，请完成这些可选任务以将安全组纳入您的 LDAP 目录同步。

注释 安全组同步仅支持从 Microsoft Active Directory 同步。

注释 如果初始同步已经完成，您将无法在 Cisco Unified Communications Manager 中将新配置添加到现有的 LDAP 目录配置。

过程

	命令或操作	目的
步骤 1	创建安全组过滤器，第 231 页	创建可同时过滤目录组和安全组的 LDAP 过滤器。
步骤 2	从 LDAP 目录同步安全组，第 231 页	添加新的 LDAP 过滤器至 LDAP 目录同步。
步骤 3	为安全组配置 Cisco Jabber，第 232 页	更新现有的服务配置文件以提供相关的 Cisco Jabber 用户可搜索和添加安全组的服务配置文件访问权限。

创建安全组过滤器

创建过滤安全组的 LDAP 过滤器。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统** > **LDAP** > **LDAP 过滤器**。

步骤 2 单击**新增**。

步骤 3 输入一个唯一的 **过滤器名称**。 例如，`syncSecurityGroups`。

步骤 4 输入以下 **过滤器**： `(&(objectClass=group)(CN=*))`。

步骤 5 单击**保存**。

从 LDAP 目录同步安全组

将安全组过滤器添加到 LDAP 目录同步并完成同步。

注释 如果初始 LDAP 同步已经完成，您将无法在 Cisco Unified Communications Manager 中将新配置添加到现有的 LDAP 目录配置。

注释 有关如何设置新 LDAP 目录同步的详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》的“配置最终用户”部分。

开始之前

创建安全组过滤器，第 231 页

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 执行下列操作之一：

- 单击“新增”以创建新的 LDAP 目录。
- 单击**查找**并选择用于同步安全组的 LDAP 目录。

步骤 3 从 **LDAP 自定义组过滤器**下拉列表中，选择您创建的安全组过滤器。

步骤 4 单击**保存**。

步骤 5 在 **LDAP 目录配置**窗口中配置任何剩余字段。 有关字段及其配置选项的更多信息，请参阅联机帮助。

步骤 6 单击**现在执行完整同步**以立即同步。 否则，当下一次预定的 LDAP 同步出现时，安全组才会进行同步。

为安全组配置 Cisco Jabber

更新现有的服务配置文件，以允许与此服务配置文件关联的 Cisco Jabber 用户从 LDAP 目录中将安全组添加至联系人列表。

注释 有关如何设置新的服务配置文件并分配至 Cisco Jabber 用户的详细信息，请参阅 *Cisco Unified Communications Manager* 系统配置指南的“配置服务配置文件”章节。

开始之前

从 LDAP 目录同步安全组，第 231 页

过程

步骤 1 在**服务配置文件配置**窗口完成其余字段的设置。 有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 2 单击**查找**并选择 Jabber 用户使用的服务配置文件。

步骤 3 在**目录配置文件**下，选中**允许 Jabber 搜索和添加安全组**复选框。

步骤 4 单击**保存**。
与此服务配置文件关联的 Cisco Jabber 用户现在可以搜索和添加安全组。

步骤 5 为 Cisco Jabber 用户使用的全部服务配置文件重复此步骤。

查看用户组

您可以使用以下步骤查看与 Cisco Unified Communications Manager 数据库同步的 企业组和安全组。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **用户组**。
此时将出现**查找并列出用户组**窗口。

步骤 2 输入搜索条件，然后单击**查找**。
此时将显示与搜索条件匹配的用户组列表。

步骤 3 要查看属于某个用户组的用户列表，请单击所需用户组。
此时将出现**用户组配置**窗口。

步骤 4 输入搜索条件，然后单击**查找**。
此时将显示与搜索条件匹配的用户列表。

如果单击列表中的用户，将出现**最终用户配置**窗口。

下一步做什么

（可选） 启用安全组 ，第 230 页

企业组部署模型 (Active Directory)

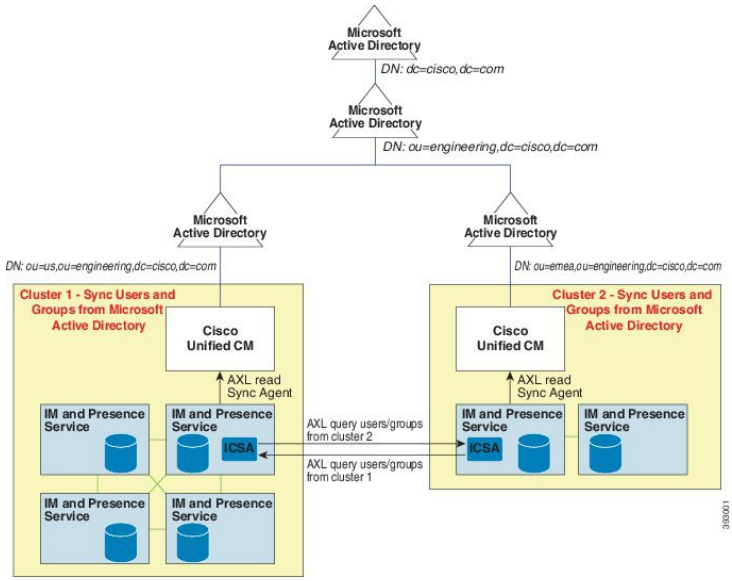
企业组功能为 Active Directory 提供了两个部署选项。

重要事项 在通过思科群集间同步代理服务同步数据之前，确保群集 1 和群集 2 具有一组唯一的 UserGroup、UserGroupMember 和 UserGroupWatcherList 记录。 如果两个群集都有唯一的记录集，则同步后两个群集都将具有所有记录的超级集合。

企业组部署模型 1

在此部署模型中，群集 1 和群集 2 从 Microsoft Active Directory 同步不同的用户和组子集。 思科群集间同步代理服务将数据从群集 2 复制到群集 1 中，以构建用户和组的完整数据库。

图 *8:* 企业组部署模型 *1*



企业组部署模型 2

在此部署模型中，群集 1 从 Microsoft Active Directory 同步所有用户和组。 群集 2 只会从 Microsoft Active Directory 同步用户。 思科群集间同步代理服务将组信息从群集 1 复制到群集 2 中。

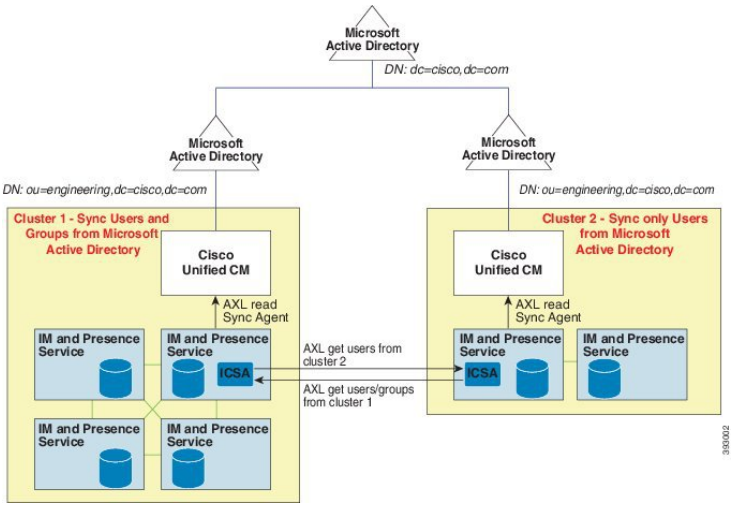
⚠

注意 如果使用此部署模型，请确保仅在一个群集中同步组数据。 如果不这样做，企业组功能将无法按预期工作。

您可以在 **Cisco Unified CM IM and Presence 管理** > **在线状态** > **群集间**窗口中验证您的配置。

检查群集间对等表中的**企业组 LDAP 配置**参数。 **未发现冲突**表示对等节点之间没有错误的配置。 如果发现冲突，单击“企业组冲突”链接，然后单击显示的**详细信息**按键。 这将打开“报告”窗口以显示详细报告。

图 *9:* 企业组部署模型 *2*


Microsoft
Active Directory
DN: dc=cisco,dc=com
Microsoft
Active Directory
Microsoft
Active Directory
DN: ou=engineering,dc=cisco,dc=com
DN: ou=engineering,dc=cisco,dc=com
Cluster 1 - Sync Users and
Groups from Microsoft
Active Directory
Cisco
Unified CM
AXL read
Sync Agent
IM and Presence
Service
IM and Presence
Service
ICSA
IM and Presence
Service
IM and Presence
Service
AXL get users from
cluster 2
AXL get users/groups
from cluster 1
Cluster 2 - Sync only Users
from Microsoft
Active Directory
Cisco
Unified CM
AXL read
Sync Agent
IM and Presence
Service
ICSA
IM and Presence
Service
353002

企业组限制

表 *26:* 企业组限制

限制	说明
阻止所有人	当 Cisco Jabber 用户在其 Cisco Jabber 策略设置中启用“阻止所有人”功能时，会阻止其他 Jabber 用户查看或与阻止的用户交换即时消息和在线状态，除非他们是阻止用户的联系人列表中的联系人。 例如，Cisco Jabber 用户 (Andy) 已在其个人 Jabber 设置中启用阻止所有人。 以下列表分解了 Andy 的阻止设置如何影响其他 Jabber 用户，这些用户可能包括也可能不包含在 Andy 的个人联系人列表中。 除了设置阻止功能之外， Andy 的个人联系人列表中： • 包括 Bob — 由于 Bob 在 Andy 的个人联系人列表中，尽管设置了阻止，但他仍然可以发送即时消息和查看 Andy 的在线状态。 • 忽略 Carol — 由于设置了阻止，Carol 不能查看 Andy 的在线状态或发送即时消息。 • 将 Deborah 作为个人联系人。 然而，Deborah 是 Andy 列为联系人的企业组成员 — Deborah 被禁止查看 Andy 的在线状态或向 Andy 发送 IM。 请注意，尽管 Deborah 在 Andy 的联系人列表中是企业组成员，但他仍然无法查看 Andy 的在线状态，也无法向 Andy 发送即时消息。 有关企业组联系人行为的其他详细信息，请参阅 CSCvg48001。
与 10.x 群集的群集间对等	版本 11.0(1) 及更高版本支持企业组。 如果同步组包含来自 10.x 群集间对等的组成员，则较高群集上的用户无法查看 10.x 群集中的同步成员的在线状态。 这是由于 11.0(1) 为企业组同步引入的数据库更新造成的。 这些更新不是 10.x 版本的一部分。 为了保证驻留在较高群集上的用户可以查看驻留在 10.x 群集上的组成员的在线状态，较高群集上的用户应手动将 10.x 用户添加到其联系人列表中。 手动添加的用户没有在线状态问题。
多级分组	组同步不允许多级分组。
仅组同步	当用户组和用户出现在同一搜索库中时，不允许进行仅组同步。 相反，用户组和用户都是同步的。

限制	说明
最大用户组数量	您可以将 Microsoft Active Directory 服务器中的最多 15000 个用户组同步到 Unified Communications Manager 数据库。 每个用户组可以包含 1 到 200 个用户。您可以在 **Cisco Unified CM IM and Presence 管理** > **系统** > **服务参数**窗口配置具体数量。 数据库中的最大用户帐户数不能超过 160,000。
用户组迁移	如果用户组从一个组织单位移到另一个组织单位，必须先对原始单位执行完全同步，然后对新单位执行完全同步。
本地组	本地组不受支持。 仅支持从 Microsoft Active Directory 同步的组。
未分配给 IM and Presence Service 节点的组成员	未分配给 IM and Presence Service 节点的组成员显示在联系人列表中，并且状态气泡显示为灰色。 但是，在计算联系人列表中允许的最大用户数时会考虑这些成员。
从 Microsoft Office Communication Server 迁移	从 Microsoft Office Communication Server 迁移期间，在用户完全迁移到 IM and Presence Service 节点之前，企业组功能不受支持。
LDAP 同步	如果您在同步过程中更改 **LDAP 目录配置窗口**中的同步选项，现有同步不受影响。 例如，如果您在同步过程中将同步选项从**用户和组**变更为**仅用户**，用户和组同步仍会继续。
通过边缘的组搜索功能	本版本提供通过边缘的组搜索功能，但尚未经过全面测试。 因此，无法保证完全支持通过边缘的组搜索。 预计未来版本中会实现对此功能的全面支持。
思科群集间同步代理服务定期同步	如果在外部 LDAP 目录中更新了组名称或组成员名称，则只有在思科群集间同步代理服务定期同步之后，信息才会在 Cisco Jabber 联系人列表中更新。 通常情况下，思科群集间同步代理服务同步每 30 分钟进行一次。
通过 LDAP 配置中的不同同步协议同步用户和用户组	如果用户和用户组作为同一同步协议的一部分同步到 Cisco Unified Communications Manager 数据库，同步后，Cisco Unified Communications Manager 数据库中的用户和组关联也会按预期更新。 但是，如果用户和用户组作为不同同步协议的一部分同步，则在第一次同步后，用户和组可能无法在数据库中关联。 数据库中的用户和组关联取决于同步协议的处理顺序。 如果用户在组之前同步，则这些组可能在数据库中不可用于关联。 在这种情况下，您必须确保在与用户的同步协议之前安排与组的同步协议。 否则，在组同步到数据库之后，用户将在下一次手动或定期同步后与组关联，并将同步类型设置为“用户和组”。 仅当协议同步类型设置为“用户和组”时，系统才会映射用户和相应组的信息。 .

限制	说明
已测试企业组的 OVA 信息	**测试的场景** 在具有两个群集（群集 A 和群集 B）的群集间部署中： 从 Active Directory 同步的 160K 用户中，群集 A 为 IM and Presence Service 启用了 15K OVA 和 15K 用户。 在 15K OVA 群集上，每个用户经过测试和支持的平均企业组数量为 13 个企业组。 从 Active Directory 同步的 160K 用户中，群集 B 为 IM and Presence Service 启用了 25K OVA 和 25K 用户。 在 25K OVA 上，每个用户经过测试和支持的平均企业组数量为 8 个企业组。 名录中经测试和支持的用户个人联系人与用户名册中来自企业组的联系人的总和小于或等于 200。 **注释** 在具有 2 个以上群集的环境中，这些号码不受支持。
导出联系人列表	在使用**批量管理** > **联系人列表** > **导出联系人列表**来导出用户的联系人列表时，联系人列表 CSV 文件不包含他们在 Jabber 客户端中的企业组的详细信息。

第 22 章

品牌定制

- 品牌概述， 第 239 页
- 品牌前提条件， 第 239 页
- 启用品牌， 第 239 页
- 禁用品牌 ， 第 240 页
- 品牌文件要求， 第 241 页

品牌概述

通过“品牌”功能，您可以为 IM and Presence Service 应用自定义品牌。 品牌自定义显示在 Cisco Unified CM IM and Presence 管理的登录和配置窗口。 您可以添加或修改的项目包括：

- 公司徽标
- 背景颜色
- 边框颜色
- 字体颜色

品牌前提条件

您必须创建具有指定文件夹结构和文件的品牌 zip 文件。 有关详细信息，请参阅品牌文件要求， 第 241 页。

启用品牌

此程序用于为 IM and Presence Service 群集启用品牌自定义。 即使您启用了 SAML SSO，品牌更新也会显示。

注释 要启用品牌，必须使用具有 4 级访问特权的主管理员帐户。 这是安装期间创建的主管理员帐户。

注释 确保仅使用 GUI 和 CLI 中的一项来启用和禁用品牌。 例如，如果您使用 GUI 界面启用品牌，则必须使用 GUI 界面本身来禁用品牌。 否则，它将无法正常工作。

开始之前

通过 IM and Presence 自定义项将 `branding.zip` 文件保存在 IM and Presence Service 可以访问的位置。

过程

步骤 1 登录到 Cisco Unified IM and Presence 操作系统管理。

步骤 2 选择**软件升级** > **品牌**。

步骤 3 **浏览**到您的远程服务器并选择 `branding.zip` 文件。

步骤 4 单击**上传文件**。

步骤 5 单击**启用品牌**。

注释 您还可以运行 **utils branding enable** CLI 命令启用品牌。

步骤 6 刷新浏览器以查看更改。

步骤 7 在所有 IM and Presence Service 群集节点上重复此程序。

禁用品牌

此程序用于在 IM and Presence Service 群集中禁用品牌。

注释 要禁用品牌，您必须使用具有 4 级访问特权的主管理员帐户。 这是安装期间创建的主管理员帐户。

注释 确保仅使用 GUI 和 CLI 中的一项来启用和禁用品牌。 例如，如果您使用 GUI 界面启用品牌，则必须使用 GUI 界面本身来禁用品牌。 否则，它将无法正常工作。

过程

步骤 1 登录到 Cisco Unified IM and Presence 操作系统管理。

步骤 2 选择**软件升级** > **品牌**。

步骤 3 单击**禁用品牌**。

注释 您还可以运行 **utils branding disable** CLI 命令禁用品牌。

步骤 4 刷新浏览器以查看更改。

步骤 5 在所有 IM and Presence Service 群集节点上重复此程序。

品牌文件要求

在将自定义品牌应用于系统之前，请根据规范创建 `branding.zip` 文件。 在远程服务器上，创建 `Branding` 文件夹并使用指定内容填充该文件夹。 添加完所有图像文件和子文件夹后，压缩整个文件夹并将文件保存为 `branding.zip`。

文件夹结构有两个选项，具体取决于您是要将单幅图像用于标题，还是组合使用六幅图像，以便让标题呈现渐变效果。

表 *27:* 文件夹结构选项

品牌选项	文件夹结构

单一标题选项	如果希望将单幅图像用于标题背景（标注项 3），您的品牌文件夹必须包含以下子文件夹和图像文件：
	
	`Branding (folder)`
	`  cup (folder)`
	`  BrandingProperties.properties (properties file)`
	`  brandingHeader.gif (652*1 pixel)`
	`  ciscoLogo12pxMargin.gif (44*44 pixel)`

渐变标题选项	如果想要为标题背景创建渐变图像（标注项 3、4、5），您需要六幅单独的图像文件来创建渐变效果。 品牌文件夹必须包含这些子文件夹和文件
	
	`Branding(folder)`
	`  cup (folder)`
	`  BrandingProperties.properties (file)`
	`  brandingHeaderBegLTR.gif (652*1 pixel image)`
	`  brandingHeaderBegRTR.gif (652*1 pixel image)`
	`  brandingHeaderEndLTR.gif (652*1 pixel image)`
	`  brandingHeaderEndRTR.gif (652*1 pixel image)`
	`  brandingHeaderMidLTR.gif (652*1 pixel image)`
	`  brandingHeaderMidRTR.gif (652*1 pixel image)`
	`  ciscoLogo12pxMargin.gif (44*44 pixel image)`

用户界面品牌选项

以下图像显示 Cisco Unified CM IM and Presence 管理用户界面的品牌选项。

图 *10:* 管理登录屏幕的品牌选项

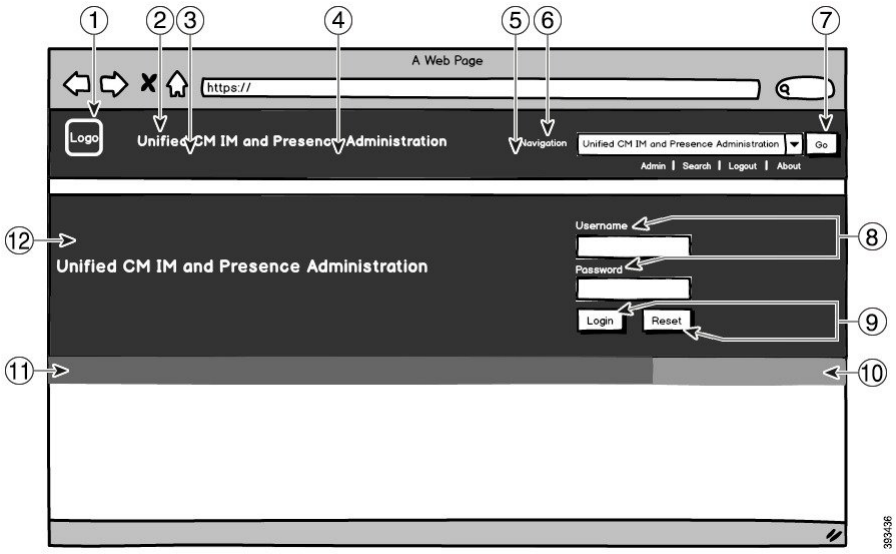
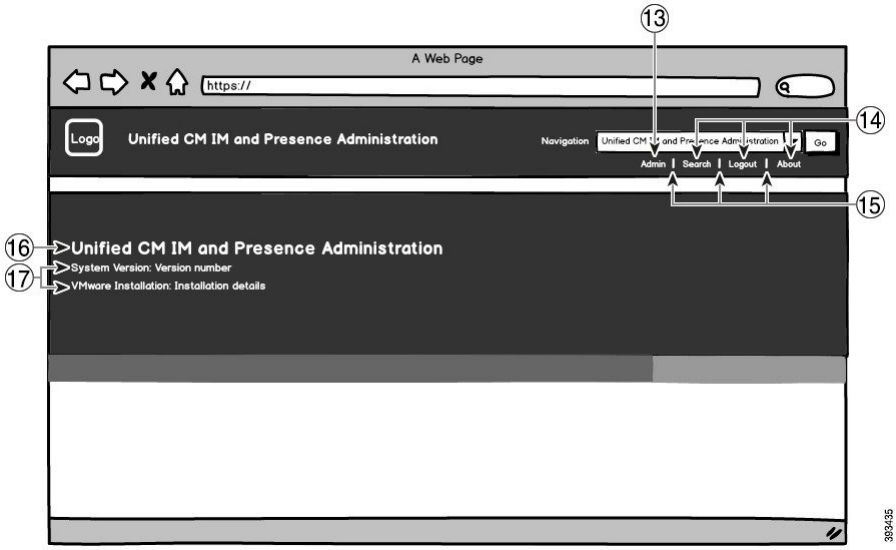


图 *11:* 管理登录屏幕的品牌选项



下表描述了如何自定义上述截屏中的标注项。

表 *28:* 用户界面品牌选项

项目	说明	品牌编辑
登录屏幕图像		

项目	说明	品牌编辑
1	公司徽标	要将徽标添加到 IM and Presence Service 界面，将公司徽标另存为采用以下文件名的 44x44 像素图像： `ciscoLogo12pxMargin.gif`（44*44 像素）
2	标题中的 Unified CM IM and Presence 管理文本	header.heading.color
3	标题背景（渐变选项 - 左侧）	如果您希望标题图像呈现渐变效果，将以下图像用于左侧。 • `brandingHeaderBegLTR.gif`（652 x 1 像素） • `brandingHeaderBegLTR.gif`（652 x 1 像素）
4	页眉背景	如果您想将单幅图像用于标题： • `brandingHeader.gif` （652 x 1 像素） 如果您在创建渐变效果的标题，请使用下列图像： • `brandingHeaderMidLTR.gif`（652 x 1 像素） • `brandingHeaderMidRTR.gif`（652 x 1 像素）
5	标题背景（渐变选项 - 右侧）	如果您想要标题呈现渐变效果，将此图像用于右侧标题： • `brandingHeaderEndLTR`（652 x 1 像素） • `brandingHeaderEndRTR`（652 x 1 像素）
6	导航文本	header.navigation.color
7	“前往”按键	header.go.font.color header.go.background.color
8	用户名和密码文本	splash.loginfield.color

项目	说明	品牌编辑
9	登录和重置按键	splash.button.text.color splash.button.color
10	底部背景颜色 – 右侧	splash.hex.code.3
11	底部背景颜色 – 左侧	splash.hex.code.2
12	横幅	splash.hex.code.1
登录后图像		
13	登录用户文本（例如，'admin' 用户）	header.text.bold.color
14	搜索、关于、注销链接	header.link.color
15	链接分隔符	header.divider.color
16	横幅中的 Unified CM IM and Presence 管理文本（登录后）	splash.login.text.color
17	系统版本以及 VMware 安装文本	splash.version.color

品牌属性编辑示例

可以通过在属性文件 (`BrandingProperties.properties`) 中添加十六进制代码来编辑品牌属性。 属性文件使用基于 HTML 的十六进制代码。 例如，如果要将导航文本项（标注项 #6）的颜色更改为红色，请将以下代码添加到属性文件中：

```
header.navigation.color="#FF0000"
```

在此代码中，`header.navigation.color` 是您要编辑的品牌属性，`"#FF0000"` 是新设置（红色）。

第 23 章

配置高级功能

- 流管理，第 245 页
- 与 Microsoft Outlook 集成日历，第 246 页
- 联合，第 247 页
- 消息存档程序，第 247 页

流管理

IM and Presence Service 支持即时消息的流管理。 流管理是使用 XEP-0198 规范实施的，该规范定义了用于在两个 XMPP 实体之间主动管理 XML 流的可扩展消息传送和在线状态协议 (XMPP) 分机，包括节确认和流恢复功能。 有关 XEP-0198 的详细信息，请参阅以下网址的规范： http://xmpp.org/extensions/xep-0198.html

如果 IM and Presence Service 与 Cisco Jabber 之间的通信暂时丢失，流管理可确保在通信中断期间发送的任何即时消息不会丢失。 可配置的超时时段决定系统对于这类消息的处理方式：

- 如果 Cisco Jabber 在超时期间重建与 IM and Presence Service 的通信，则消息会重发。
- 如果 Cisco Jabber 在超时期间未能重建与 IM and Presence Service 的通信，则消息会返回给发送方。
- 在 Cisco Jabber 恢复与 IM and Presence Service 的通信后，超时期间发送的消息将离线存储并发送。

流管理在群集范围内默认启用。 不过，您可以使用流管理服务参数配置该功能。

配置流管理

此程序用于在 IM and Presence Service 上配置流管理 (XEP-0198)。

过程

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

步骤 2 从**服务器**下拉列表中，选择 IM and Presence 节点。

步骤 3 从**服务**下拉列表中选择 **Cisco XCP 路由器**。

步骤 4 将**启用流管理**服务参数设置为**启用**。

步骤 5 在**流管理参数**（**群集范围**）下，配置任何流管理参数：

表 *29:* 流管理服务参数

服务参数	说明
启用流管理	启用或禁用群集范围的流管理。 默认设置为“启用”。
流管理超时	超时控制会话（连接已被切断）在放弃之前允许恢复的时间（以秒为单位）。如果客户端试图协商较长的超时（或未指定所需的超时），则此最大值将适用。 在此超时结束后和 Cisco Jabber 再次登录之前通过 IM and Presence Service 发送的任何消息都将离线保存，并在重新登录后重新发送。 范围为 30 秒至 90 秒。 默认值为 60 秒。
流管理缓冲区	定义将为启用流管理的会话保留在缓冲区中的数据包最大数（数据包历史记录）。如果客户端所需的历史记录多于缓冲区中可用的内容，则流恢复将失败。 范围为 5-150 个数据包，默认值为 100 个数据包。
确认请求率	定义在要求客户端提供接收到的最后一节的计数之前服务器发送的节数。减小数字可增大网络流量，但有助于服务器修剪节历史记录缓冲区并减少内存使用量。 范围为 1-64 节，默认值为 5。 **注释** 减小确认请求率会导致网络流量增加，但内存使用量减少。

步骤 6 单击**保存**。

与 Microsoft Outlook 集成日历

借助此功能，用户可以将他们的日历和会议状态从 Microsoft Outlook 合并到 IM and Presence Service 服务器上的状态中。如果用户正在开会，该状态将显示为用户 Presence 状态的一部分。可以通过将 IM and Presence Service 连接到内部 Microsoft Exchange 服务器或托管的 Office 365 服务器来配置此功能。

有关如何配置与 Microsoft Outlook 集成日历的详细信息，请参阅文档《为 *IM and Presence Service* 与 *Microsoft Outlook* 集成日历》，网址：http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html。

联合

在 IM and Presence Service 上，您可以从 IM and Presence Service 管理的任何域中创建联合网络。有两种主要类型的联合部署：

- 域间联合 — 此集成使得来自 IM and Presence Service 管理的任何域内的用户能够与外部域中的用户交换可用性信息和即时消息 (IM)。Microsoft、Google、IBM 或 AOL 服务器可管理外部域。IM and Presence Service 可以使用各种协议与外部域中的服务器通信。
- 分区式域内联合 — 通过此集成，IM and Presence Service 和 Microsoft 服务器（例如 Microsoft Lync）托管一个公共域或一组域。该集成允许单个企业内的 IM and Presence Service 客户端用户和 Microsoft Lync 用户交换即时消息和可用性。
- SIP 开放联合—Cisco IM and Presence Service 支持 Cisco Jabber 客户端的 SIP 开放联合。作为管理员，您可以配置 SIP 开放联合，允许 Cisco Jabber 用户与来自所有可用域的用户无缝联合。您可以为包含单个静态路由的所有域配置开放联合。静态路由使得 Cisco Jabber 可与任何外部域联合。更重要的是，它会显著缩短配置和维护各个域的 SIP 联合的时间。

有关配置信息，请参阅《*Cisco Unified Communications Manager* 上的 *IM and Presence Service* 域内联合》或《*Cisco Unified Communications Manager* 上 *IM and Presence Service* 的分区式域内联合》，网址：http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html。

消息存档程序

许多行业要求即时消息遵守与所有其他业务记录相同的法规遵从性准则。为遵守这些法规，您的系统必须记录并归档所有业务记录，并且归档记录必须可供检索。

IM and Presence Service 通过在单个群集、群集间或联合网络配置中收集以下 IM 活动的数据来支持即时消息 (IM) 合规性：

- 端对端消息。
- 群聊 - 这包括临时聊天消息和永久聊天消息。
- IM 合规性组件
- IM 合规性的示例拓扑和消息流

有关配置即时消息合规性的详细信息，请参阅《*Cisco Unified Communications Manager* 上 *IM and Presence Service* 的即时消息合规性》，网址：http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html。

第 IV 部分

管理系统

- 管理聊天， 第 251 页
- 托管文件传输管理， 第 267 页
- 管理最终用户， 第 275 页
- 将用户迁移到集中式部署 ， 第 287 页
- 迁移用户， 第 301 页
- 管理区域设置， 第 315 页
- 管理服务器， 第 321 页
- 备份系统， 第 327 页
- 恢复系统， 第 339 页
- 联系人列表的批量管理， 第 355 页
- 排查系统， 第 369 页

第 24 章

管理聊天

- 管理聊天概述，第 251 页
- 管理聊天前提条件，第 252 页
- 管理聊天任务流程，第 252 页
- 管理聊天相互作用，第 265 页

管理聊天概述

IM and Presence Service 提供可用于管理聊天室以及控制聊天室访问权限的设置。 这包括以下能力：

- 新建聊天室，管理其创建的聊天室的成员和配置。
- 控制对永久聊天室的访问权限，以便只有该会议室的成员才能访问。
- 为聊天室分配管理员。
- 邀请其他用户到聊天室。
- 确定聊天室中显示的成员的在线状态。 聊天室中显示的在线状态用于确认哪些成员在参与聊天，但无法反映他们的整体在线状态。

IM and Presence Service 还可让您管理聊天节点别名。 通过聊天节点别名，您的用户可以搜索特定节点上的特定聊天室，以及加入这些聊天室。

此外，IM and Presence Service 还可存储脚本，并将此聊天室历史记录提供给聊天室成员，包括刚加入聊天室的成员。 您可以配置要向新老成员开放的现有存档的数量。 .

聊天节点别名概述

系统中的每个聊天节点必须有唯一的别名。 聊天节点别名是为每个聊天节点创建的唯一地址，它使得用户（位于任何域中）能够搜索特定节点上的特定聊天室，并加入这些聊天室中的聊天。 聊天节点别名构成在该节点上创建的每个聊天室的唯一 ID 的一部分。 例如，别名 `conference-3-mycup.cisco.com` 用来命名在该节点上创建的聊天室 `roomjid@conference-3-mycup.cisco.com`。

分配聊天节点别名的模式有两种：

- 系统生成 — 系统自动为每个聊天节点分配唯一的别名。 默认情况下，系统使用以下命名约定自动为每个聊天节点生成一个别名：`conference-x-clusterid.domain`，其中：
  - `conference` 是硬编码关键字
  - `x` 是表示节点 ID 的唯一整数值
  - `clusterid` 是配置的企业参数
  - `domain` 是配置的域

  例如，系统可能会分配：`conference-3-mycup.cisco.com`
- 手动 — 您必须禁用系统生成的别名，才能手动分配聊天节点别名。 通过手动分配别名，您可完全灵活地使用适合特定要求的别名来命名聊天节点。 例如，如果 `congerence-x-clusterid.domain` 命名约定不适合您的部署需要，您就可以这样做。

为每个节点分配多个别名

您可以在每个节点的基础上将多个别名与每个聊天节点关联。 每个节点多个别名可让用户使用这些别名创建额外的聊天室。 此功能适用于系统生成的别名和手动创建的别名。

管理聊天前提条件

确保您已启用永久聊天。

管理聊天任务流程

过程

	命令或操作	目的
步骤 1	允许聊天室所有者编辑聊天室设置，第 253 页	配置是否要允许聊天室所有者编辑聊天室设置。 否则，只有管理员能够编辑聊天室设置。
步骤 2	允许客户端记录即时消息历史记录，第 254 页	配置是否允许用户在其计算机本地记录即时消息历史记录。
步骤 3	将永久聊天室创建限制在主群集，第 254 页	遵照此程序可限制 Cisco Jabber 用户主群集内的永久聊天室创建操作。
步骤 4	查看外部数据库文字会议报告，第 255 页	此程序用于查看外部数据库文字会议报告，从而了解有关永久聊天室的详细信息。

	命令或操作	目的
步骤 5	转移永久聊天室的所有权， 第 256 页	遵照此程序可将属于主群集的永久聊天室的所有权转移给该聊天室的任何其他现有成员。
步骤 6	永久聊天别名报告， 第 257 页	遵照此程序可查看外部数据库中存在的自有和对等群集别名的聊天室计数。
步骤 7	编辑聊天室设置。 按任意顺序完成以下任意任务，以更新聊天室设置： • 设置聊天室数量， 第 257 页 • 配置聊天室成员设置， 第 257 页 • 配置可用性设置， 第 259 页 • 配置占用设置， 第 260 页 • 配置聊天消息设置， 第 260 页 • 配置被主持的房间设置， 第 261 页 • 配置历史记录设置， 第 261 页	注释 如果更新任何永久聊天设置，在 Cisco Unified IM and Presence 功能配置上，选择**工具 > 控制中心 - 功能服务**以重新启动 Cisco XCP 文字会议管理器服务。
步骤 8	将聊天室重置为系统默认值， 第 262 页	如果要将聊天配置重置为系统默认值，请完成此可选任务。 请注意，临时聊天默认启用，但永久聊天默认禁用。 完成此任务将禁用永久聊天。
步骤 9	管理聊天节点别名， 第 262 页	别名为每个聊天节点创建唯一的地址，以便用户（位于任何域中）能够搜索特定节点上的特定聊天室，并加入这些聊天室中的聊天。 系统中的每个聊天节点必须有唯一的别名。
步骤 10	为永久聊天清理外部数据库， 第 265 页	可选。 使用外部数据库清理实用程序配置监控外部数据库并删除过期记录的作业。 这将确保始终有足够的磁盘空间用于新记录。

允许聊天室所有者编辑聊天室设置

如果想要让聊天室所有者能够编辑聊天室设置，请按照此程序操作。

注释 是否能从客户端配置这些设置也取决于客户端的实施以及客户端是否提供可以配置这些设置的界面。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**消息** > **群聊和永久聊天**。

步骤 2 配置**聊天室所有者可以更改聊天室是否仅限会员使用**复选框的值。

- 选中 — 聊天室所有者具有编辑聊天室设置的管理能力。
- 取消选中 — 只有管理员可以编辑聊天室设置。

步骤 3 单击**保存**。

步骤 4 在 **Cisco Unified IM and Presence 功能配置**中，选择**工具** > **控制中心 - 功能服务**。

步骤 5 重新启动 Cisco XCP 文字会议管理器服务。

允许客户端记录即时消息历史记录

您可以禁止或允许用户将即时消息历史记录在本地计算机上。 在客户端上，应用程序必须支持此功能；它必须强制禁止记录即时消息

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**消息** > **设置**。

步骤 2 按照以下说明配置日志即时消息历史设置：

- 要允许客户端应用程序的用户记录 IM and Presence Service 上的即时消息历史记录，请选中**允许客户端记录即时消息历史记录（仅支持的客户端）**。
- 要禁止客户端应用程序的用户记录 IM and Presence Service 上的即时消息历史记录，则取消选中**允许客户端记录即时消息历史记录（仅支持的客户端）**。

步骤 3 单击**保存**。

将永久聊天室创建限制在主群集

重要事项 此功能适用于 14 SU1 及更高版本。

遵照此程序可限制 Cisco Jabber 用户主群集内的永久聊天室创建操作。 此功能可减少群集间流量并增加系统带宽。

IM and Presence Service 管理员管理主群集中的用户创建的所有聊天室。 其他群集的维护活动不影响主群集中的用户创建的聊天室。

开始之前

重要事项 从 14SU1 版开始支持。

- 确认是否已启用永久聊天。
- 在启用此功能之前，选中**群聊和永久聊天设置**窗口上的**别名报告**。 有关详细信息，请参阅：永久聊天别名报告，第 257 页。
- 需要 Cisco Jabber 14.1 版或更高版本才能支持此功能。

过程

步骤 1 登录到数据库发布方节点上的 **Cisco Unified CM IM and Presence Service** 管理。

步骤 2 选择**消息** > **群聊和永久聊天**。

步骤 3 在**启用永久聊天**下，选中**将聊天室创建限制在主群集**复选框。

下一步做什么

在主群集中的所有节点上重新启动 **Cisco XCP 文字会议管理器服务**。

查看外部数据库文字会议报告

此程序用于查看外部数据库文字会议报告。 通过此报告，您可以查看部署中永久和临时聊天室的相关详细信息。

过程

步骤 1 登录到 **Cisco Unified CM IM and Presence** 管理。

步骤 2 选择**消息** > **群聊和永久聊天**。

步骤 3 在**永久聊天数据库分配**下，单击**聊天室报告**按键。

步骤 4 如果要将选择限制为符合特定条件的聊天室，请使用过滤工具。

步骤 5 单击**查找**。

步骤 6 选择特定聊天室以查看该聊天室的详细信息。

注释 从数据库中提取的记录数取决于从“提取的记录”下拉列表中选择的值。

转移永久聊天室的所有权

重要事项 此功能适用于 14 SU1 及更高版本。

对有权访问 GUI 的 IM and Presence Service 管理员执行此程序可转移永久聊天室的所有权。

例如，John 创建了一个永久聊天室并添加了一些成员，后来又离开了该组织。

如果 John 是唯一的永久聊天室所有者，并且给定房间仍然需要房间所有者的能力，则 IM and Presence Service 管理员可以选择当前房间的一位或多位成员作为新的房间所有者。

更新**所有者 ID** 时，请考虑以下事项：

- 您可以将聊天室的所有权变更为与以前的所有者属于同一主群集的任何聊天室成员。
- **所有者 ID** 应为**用户 JID**，而不是**用户 ID**。
- 系统会对照 IM and Presence Service 节点数据库对输入的**所有者 ID** 进行验证。
- 管理员无法将聊天室创建者的 ID 设置为聊天室的新所有者 ID。

要更改聊天室的所有权，请执行以下步骤：

开始之前

重要事项 从 14SU1 版开始支持。

在更新**所有者 ID** 之前，停止主群集中所有 IM and Presence Service 节点上的 **Cisco XCP 文字会议管理器服务**。

过程

步骤 1 登录到数据库发布方节点上的 **Cisco Unified Communications Manager IM and Presence Service 管理**。

步骤 2 选择**消息** > **群聊和永久聊天**。

步骤 3 在**永久聊天数据库分配**下，单击**聊天室报告**按键。

步骤 4 如果要将选择限制为符合特定条件的聊天室，请使用过滤工具，然后单击**查找**。

步骤 5 （可选）单击**聊天室 JID** 查看 PChat 聊天室的字段，例如所有者列表、成员列表和最后一条消息的日期。 请参阅联机帮助，获取有关字段的详细信息和说明。

步骤 6 选中**聊天室 JID** 的复选框以编辑**所有者 ID** 字段。

注释 **所有者 ID** 列仅对属于主群集的永久聊天室不可编辑。

步骤 7 以电子邮件格式输入您想将其设为新所有者的聊天室成员的**所有者 ID**。

步骤 8 单击 **更新所有者 ID**。
这将使用相同的**所有者 ID** 更新一个或多个所选永久聊天室的所有者。

下一步做什么

在主群集中的所有节点上启动 **Cisco XCP 文字会议管理器服务**。

永久聊天别名报告

遵照此程序可查看外部数据库永久聊天别名报告，您可以通过该报告了解聊天室计数以及外部数据库中存在的主群集和对等群集别名。

过程

步骤 1 登录到数据库发布方节点上的 **Cisco Unified CM IM and Presence Service 管理**。

步骤 2 选择**消息** > **群聊和永久聊天**。

步骤 3 在**永久聊天数据库分配**下，从下拉列表中选择**外部数据库**。

步骤 4 单击**别名报告**按键。 请参阅联机帮助中的字段说明。

配置聊天室设置

设置聊天室数量

使用聊天室设置限制用户可以创建的聊天室数。 限制聊天室数有助于系统性能并允许其扩展。 还有助于减少可能的服务层级攻击。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**消息** > **群聊和永久聊天**。

步骤 2 要更改允许的最大聊天室数，请在**允许的最大聊天室数**字段中输入一个值。 默认值为 5500。

步骤 3 单击**保存**。

配置聊天室成员设置

成员设置用于管控聊天室中的成员资格。 此类控制可以帮助用户缓解能通过限制成员资格规避的服务级攻击。 可以根据需要配置成员设置。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**消息** > **群聊和永久聊天**。

步骤 2 按“聊天室成员设置”中的说明配置聊天室成员设置。

步骤 3 单击**保存**。

步骤 4 在 **Cisco Unified IM and Presence 功能配置**中，选择**工具** > **控制中心 - 功能服务**。

步骤 5 重新启动 Cisco XCP 文字会议管理器服务。

聊天室成员设置

注释 在您创建聊天室时，永久聊天室会继承其设置。稍后的更改不适用于现有聊天室。这些更改仅适用于更改生效后创建的聊天室。

表 30:

字段	说明
默认情况下聊天室仅限会员使用	如果希望聊天室默认创建为仅成员聊天室，选中此复选框。只有聊天室所有者或管理员配置的允许列表上的用户才能访问仅成员聊天室。 该复选框默认未选中。 注释 允许列表包含聊天室中允许的成员列表，它由仅成员聊天室的所有者或管理员创建。
只有协调人能够邀请他人进入仅限会员的聊天室	如果您想要将聊天室配置为仅允许主持人邀请用户加入聊天室，请选中此复选框。如果未选中此复选框，成员可以邀请其他用户加入聊天室。 该复选框默认选中。
聊天室所有者可以更改聊天室是否仅限会员使用	如果您想要将聊天室配置为允许聊天室所有者更改聊天室是否仅供会员使用，请选中此复选框。 该复选框默认选中。 注释 聊天室所有者是指创建聊天室的用户或被聊天室创建者或所有者指定为具有所有者状态（如果允许）的用户。 除了所有其他管理员功能外，聊天室所有者还可以更改聊天室配置和关闭聊天室。
聊天室所有者可以更改是否只有协调人能够邀请他人进入仅限会员的聊天室	如果您想要将聊天室配置为聊天室所有者可以允许会员邀请其他用户加入聊天室，请选中此复选框。 该复选框默认选中。

字段	说明
用户可以将自身添加为聊天室的会员	如果您想要将聊天室配置为任何用户可以随时请求加入聊天室，请选中此复选框。 如果选中此复选框，聊天室将采用开放式成员制。 该复选框默认未选中。
聊天室所有者能够更改用户是否可以将自身添加为聊天室的会员	如果要配置聊天室，以便聊天室所有者任何时候都能更改步骤 5 中列出的设置，请选中此复选框。 该复选框默认未选中。

配置可用性设置

可用性设置决定用户在聊天室中的可见性。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**消息** > **群聊和永久聊天**。

步骤 2 按“可用性设置”中的说明配置可用性成员设置。

步骤 3 单击**保存**。

步骤 4 在 **Cisco Unified IM and Presence 功能配置**中，选择**工具** > **控制中心 - 功能服务**。

步骤 5 重新启动 Cisco XCP 文字会议管理器服务。

可用性设置

字段	说明
不在聊天室中的会员和管理员仍可在聊天室中看到	如果您想要让用户保持在聊天室名录上（即使他们当前离线），请选中此复选框。 该复选框默认选中。 **注释** 如果管理员离开聊天室，则管理员的用户 ID 仍可在聊天室中看到。 用户需要关闭并重新打开聊天室以刷新用户的列表。
聊天室所有者可以更改不在聊天室中的会员和管理员是否仍可在聊天室中看到	如果您想要允许聊天室所有者能够更改会员或管理员的可见性，请选中此复选框。 该复选框默认选中。
聊天室可以向后兼容旧版客户端	如果您想要服务在旧的群聊 1.0 版客户端上正常运行，请选中此复选框。 该复选框默认未选中。

字段	说明
聊天室所有者能够更改聊天室是否可以向后兼容旧版客户端	如果您想要允许聊天室所有者能够控制聊天室的向后兼容性，请选中此复选框。 该复选框默认未选中。
默认情况下聊天室是匿名的	如果您想要聊天室显示用户昵称，但让 Jabber ID 保密，请选中此复选框。 该复选框默认未选中。
聊天室所有者可以更改聊天室在默认情况下是否匿名	如果您想要允许聊天室所有者控制用户 Jabber ID 的匿名程度，请选中此复选框。 该复选框默认未选中。

配置占用设置

占用设置决定了在给定时间，聊天室中可以有多少用户。

过程

步骤 1 要更改聊天室中允许的系统最大用户数，请在**聊天室内同时可以容纳多少位用户**字段中输入值。 默认值为 1000。

注释 聊天室内的用户总数不应超过设置的值。 聊天室内的用户总数包括普通用户和隐藏用户。

步骤 2 要更改聊天室中允许的隐藏用户数，请在**聊天室内同时可以容纳多少位隐藏用户**字段中输入值。 隐藏用户对于其他用户不可见，无法发送消息到聊天室，也不能发送 Presence 更新。 隐藏用户可以查看聊天室内的所有消息，并接收来自其他用户的 Presence 更新。 默认值为 1000。

步骤 3 要更改默认的聊天室内允许的最大用户数，请在**聊天室的默认最大占用**字段中输入值。 默认值设置为 50，不能大于步骤 1 中设置的值。

步骤 4 如要允许聊天室所有者更改默认的最大聊天室占用，请选中**聊天室所有者可以更改聊天室的默认最大占用**。 该复选框默认选中。

步骤 5 单击**保存**。

配置聊天消息设置

使用聊天消息设置，根据用户角色授予用户权限。 角色主要存在于访客-主持人的层级。 例如，参与者可以执行访客所能执行的全部操作，主持人则可执行参与者所能执行的全部操作。

该复选框默认选中。

过程

步骤 1 从**可在聊天室发送私信的最低用户参与等级**下拉列表中选择一项：

- **访客**，允许访客、参与者和主持人向聊天室内的其他用户发送私信。这是默认设置。
- **参与者**，允许参与者和主持人向聊天室内的其他用户发送私信。
- **主持人**，仅允许主持人向聊天室内的其他用户发送私信。

步骤 2 如果允许聊天室所有者更改发送私信的最低参与等级，请选中**聊天室所有者可以更改可在聊天室内发送私信的最低用户参与等级**。 该复选框默认选中。

步骤 3 在可更改聊天室主题的最低用户参与等级下拉列表中选择一项：

a) **参与者**，允许参与者和主持人更改聊天室主题。 这是默认设置。

b) **主持人**，仅允许主持人更改聊天室主题。

访客则无权更改聊天室主题。

步骤 4 如果您要允许聊天室所有者更改更新聊天室主题的最低参与等级，请选中**聊天室所有者可以更改可更新聊天室主题的最低用户参与等级**。

步骤 5 如果要删除消息中的所有可扩展超文本标记语言 (XHTML)，请选中**删除消息中的所有 XHTML 格式**。 该复选框默认未选中。

步骤 6 如果要允许聊天室所有者更改 XHTML 格式设置，请选中**聊天室所有者可以更改 XHTML 格式设置**。 该复选框默认未选中。

步骤 7 单击**保存**。

配置被主持的房间设置

被主持的房间让主持人能够授予和撤销聊天室内的语音权限（群聊中的语音是指向聊天室发送聊天消息的能力）。 访客不能在被主持的房间中发送即时消息。

过程

步骤 1 如果要在聊天室中使用主持人角色，请选中**默认房间被主持**。 该复选框默认未选中。

步骤 2 如果要允许聊天室所有者更改聊天室是否被主持，请选中**聊天室所有者可以更改房间是否默认被主持**。 该复选框默认选中。

步骤 3 单击**保存**。

配置历史记录设置

使用历史记录设置来设置聊天室中检索和显示的消息数默认值和最大值，以及控制可通过历史记录查询检索的消息数。当用户加入聊天室时，将向该用户发送聊天室的消息历史记录。历史记录设置确定用户可以收到的之前消息数。

过程

步骤 1 要更改用户可从存档中检索的最大消息数，请在**可从存档中检索的最大消息数**对应的字段中输入值。默认值设置为 100。它会用作下一个设置的限制。

步骤 2 要更改当用户加入聊天室时显示的消息数，请在**聊天历史记录中默认显示的消息数**对应的字段中输入值。 默认值设置为 15，不能大于步骤 1 中设置的值。

步骤 3 如果要让聊天室所有者更改用户加入聊天室时显示的之前消息数，请选中**聊天室所有者可更改聊天历史记录中显示的消息数**。 该复选框默认未选中。

步骤 4 单击**保存**。

将聊天室重置为系统默认值

如果要将临时和永久聊天室的群聊设置重置为系统默认值，可按此程序操作。

注释 临时聊天默认启用，但永久聊天默认禁用。 完成此任务将禁用永久聊天

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**消息** > **设置**。

步骤 2 单击**设置为默认值**。

步骤 3 单击**保存**。

聊天节点别名管理

管理聊天节点别名

以下任务用于管理您群集的聊天节点别名。 您可以让系统自动管理别名，也可以自己更新。

过程

	命令或操作	目的
步骤 1	分配模式以管理聊天别名 ，第 263 页	指定是否希望系统管理聊天节点别名，或者是否要手动执行此操作。
步骤 2	手动添加聊天节点别名 ，第 263 页	为您的群集添加、编辑或删除聊天节点别名。

分配模式以管理聊天别名

配置您是否希望系统使用 `conference-x-clusterid.domain` 命名约定自动分配聊天节点别名，或者是否要手动分配它们。

开始之前

有关聊天节点别名的信息，请参阅聊天节点别名概述，第 251 页。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**消息** > **群聊和永久聊天**。

步骤 2 启用或禁用系统生成的别名：

- 如果想要系统自动分配聊天节点别名，选中**系统自动管理主要群聊服务器别名**。

  提示 选择**消息** > **群聊服务器别名映射**，验证系统生成的别名是否在“主要群聊服务器别名”下列出。

- 如果想要手动分配聊天节点别名，取消选中**系统自动管理主要群聊服务器别名**。

下一步做什么

- 即使为聊天节点配置了系统生成的别名，如果需要，仍可将多个别名与该节点关联。
- 如果要与外部域联合，您可能希望将别名已更改且新别名已可用的事项通知联合方。 要外部通告所有别名，请配置 DNS 并将别名作为 DNS 记录发布。
- 如果更新任何系统生成的别名配置，请执行以下操作之一：重新启动 Cisco XCP 文字会议管理器。
- 要添加、编辑或删除聊天节点别名，手动添加聊天节点别名，第 263 页。

手动添加聊天节点别名

此程序用于手动添加、编辑或删除聊天节点别名。 要手动管理聊天节点别名，必须关闭默认设置（默认使用系统生成的别名）。 如果您关闭系统生成的别名，现有别名将 (`conference-x-clusterid.domain`) 恢复为标准的可编辑别名，列在“会议服务器别名”下。 这会保留旧别名及与该别名关联的聊天室地址。

您可以手动为聊天节点分配多个别名。 即使聊天节点已存在系统生成的别名，您也可以手动将其他别名关联到该节点。

对于手动管理的别名，如果更改群集 ID 或域，管理员必须手动更新别名列表。 系统生成的别名将会自动合并更改的值。

注释 我们建议您在向节点分配新聊天节点别名时始终将域包含在内，虽然这并不是必需操作。 请对其他别名使用以下约定：newalias.domain。 选择 **Cisco Unified CM IM and Presence 管理** > **Presence 设置** > **高级设置**以查看域。

开始之前

分配模式以管理聊天别名 ，第 263 页

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**消息** > **群聊服务器别名映射**。

步骤 2 单击**查找**。

“群聊服务器别名”窗口中将显示现有节点别名。

步骤 3 要添加新的别名：

a) 单击**新增**。
b) 在**群聊服务器别名**字段中，输入新的别名。
c) 从**服务器名称**下拉列表框中，选择您要为其分配别名的服务器。
d) 单击**保存**。

步骤 4 要编辑现有别名：

a) 选择别名。
b) 输入您的更新，然后单击**保存**。

步骤 5 要删除别名，请选择别名并单击**删除选定项**。

下一步做什么

- 打开 Cisco XCP 文字会议管理器。

聊天节点别名故障诊断提示

- 每个聊天节点别名都必须是唯一的。 系统将禁止您在群集中创建重复的聊天节点别名。
- 聊天节点别名不能与 IM and Presence 域名匹配。
- 如果不再需要通过旧别名维护聊天室的地址，则删除旧别名。
- 如果要与外部域联合，您可能希望将别名已更改且新别名已可用的事项通知联合方。 要外部通告所有别名，请配置 DNS 并将别名作为 DNS 记录发布。
- 如果更新任何聊天节点别名配置，请重新启动 Cisco XCP Text Conference Manager。

为永久聊天清理外部数据库

配置监控外部数据库并删除过期记录的作业。 这将确保始终有足够的磁盘空间用于新记录。

要清除永久聊天的数据库表，请确保在**功能表**下选择**文字会议 (TC)** 功能。

过程

步骤 1 登录到数据库发布方节点上的 Cisco Unified CM IM and Presence 管理。

步骤 2 选择**消息** > **外部服务器设置** > **外部数据库作业**。

步骤 3 单击**清除外部数据库**。

步骤 4 执行下列操作之一：

- 若要手动清理连接到发布方节点的外部数据库，选择**相同 Cup 节点**。
- 若要手动清理连接到订阅方节点的外部数据库，选择**其他 Cup 节点**，然后选择外部数据库详细信息。
- 如果您将系统配置为自动监控并清除外部数据库，选中**自动清理**单选按键。

注释 我们建议您在设置自动清理之前先运行手动清理。

步骤 5 设置您想要返回以删除文件的**天数**。 例如，如果输入 90，系统将删除早于 90 天的记录。

步骤 6 单击**更新架构**以创建索引和已存储的数据库程序。

注释 您只需在第一次运行作业时更新架构。

步骤 7 设置您想要返回以删除文件的**天数**。 例如，如果输入 **90**，系统将删除早于 90 天的记录。

步骤 8 在**功能表**部分，选择您希望清除其记录的每项功能：

- **文字会议 (TC)**—选择此选项可以清除永久聊天功能的数据库表。
- **消息存档程序 (MA)**—选择此选项可以清除消息存档程序功能的数据库表。
- **托管文件传输 (MFT)**—选择此选项可以清除托管文件传输功能的数据库表

步骤 9 单击**提交清除作业**。

注释 如果您已启用**自动**选项，并且想要禁用它，请单击**禁用自动清除作业**按键。

管理聊天相互作用

更改聊天节点别名会使数据库中的聊天室不可寻址，从而导致您的用户无法查找现有的聊天室。

在更改别名的组成部分或其他节点依赖关系前，请注意下面的结果：

- 群集 ID - 此值是完全限定群集名称 (FQDN) 的一部分。 更改群集 ID（选择系统 > Presence 拓扑：设置）将导致 FQDN 包含新值和系统管理的别名，以自动在整个群集中更改。 对于手动管理的别名，如果更改群集 ID，管理员必须手动更新别名列表。
- 域 - 此值是 FQDN 的一部分。 更改域（选择 Presence > Presence 设置）将导致 FQDN 包含新值和系统管理的别名，以自动在整个群集中更改。 对于手动管理的别名，如果更改域，管理员必须手动更新别名列表。
- 聊天节点与外部数据库之间的连接 - 如果启用永久聊天，且您未能保持与外部数据库的正确连接，聊天节点将不启动。
- 删除聊天节点 - 如果从 Presence 拓扑中删除与现有别名关联的节点，除非采取其他措施，否则使用旧别名创建的聊天室可能不可寻址。

我们建议您，如果更改现有别名没有更深层次的意义，则不要更改，也就是说：

- 确保旧聊天节点的地址位于数据库中，以便用户在需要的时候可以通过旧别名查找到现有聊天室。
- 如果存在与外部域的联合，您可能需要在DNS中发布别名，以通知这些域中的用户：别名已经更改，有新地址可用。 是否执行此操作，取决于您是否想向外部通告所有别名。

第 25 章

托管文件传输管理

- 托管文件传输管理概述，第 267 页
- 托管文件传输管理前提条件，第 268 页
- 托管文件传输管理任务流程，第 268 页

托管文件传输管理概述

作为 IM and Presence Service 管理员，您负责管理用于托管文件传输功能的文件存储区和磁盘的使用情况。 请参照本章内容监控文件存储区和磁盘的使用情况级别，并设置计数器和警报，以便在级别超过定义的阈值时通知您。

管理外部文件服务器和数据库服务器

管理外部数据库大小时，可以将查询与 shell 脚本组合在一起，以便根据您的规范自动从数据库中清除文件。 要创建查询，请使用文件传输元数据。 这包括传输类型、文件类型、时间戳、文件服务器上文件的绝对路径，以及其他信息。

选择 IM 和群聊内的文件传输方式时，请注意一对一 IM 和群聊可能具有临时性，因此传输的文件可能立即删除。 但是请记住：

- 传输到离线用户的 IM 可能触发延迟的文件请求。
- 永久聊天传输可能需要存在更长时间。

注释

- 请勿清除当前 UTC 时间段期间所创建的文件。
- 分配文件服务器后，您可以更改文件服务器配置的名称，但不能更改文件服务器本身的名称。
- 如果配置了托管文件传输并更改了设置，重启 Cisco XCP 路由器服务将重启托管文件传输功能。
- 如果您更改了设置而未在文件服务器上进行更改，文件传输将停止运行，您将收到重启 Cisco XCP 路由器服务的通知。
- 如果数据库或文件服务器发生故障，系统将生成一条指明故障的消息。 但是，错误响应并不能区分数据库、文件服务器或一些其他内部故障。 当数据库或文件服务器发生故障时，实时监控工具也会生成警报。 此警报与文件传输是否正在进行无关。

托管文件传输管理前提条件

配置托管文件传输功能。

托管文件传输管理任务流程

过程

	命令或操作	目的
步骤 1	AFT_LOG 表示例查询和输出 ，第 268 页	以下程序提供了您可以在 AFT_LOG 表上运行的查询示例，以及如何使用输出从文件服务器清除不必要的文件。
步骤 2	设置服务参数阈值 ，第 270 页	配置托管文件传输服务参数，以定义为外部文件服务器磁盘空间生成 RTMT 警报的阈值。
步骤 3	配置 XCP 文件传输警报 ，第 271 页	配置托管文件传输警报，以便在达到定义的阈值时收到通知。
步骤 4	为托管文件传输清理外部数据库 ，第 273 页	可选。 使用外部数据库清理实用程序配置监控外部数据库并删除过期记录的作业。 这将确保始终有足够的磁盘空间用于新记录。

AFT_LOG 表示例查询和输出

以下程序提供了您可以在 AFT_LOG 表上运行的查询示例，以及如何使用输出从文件服务器清除不必要的文件。

此查询会返回指定日期之后每个上传文件的记录。

注释 如需 SQL 命令的示例，请参阅外部数据库磁盘使用情况，第 269 页。

过程

步骤 1 在外部数据库中，输入以下命令：

```
SELECT file_path
FROM aft_log
WHERE method='Post' AND timestampvalue > '2014-12-18 11:58:39';
```

命令会生成以下输出：

```
/opt/mftFileStore/node_1/files/im/20140811/15/file_name1
/opt/mftFileStore/node_1/files/im/20140811/15/file_name2
/opt/mftFileStore/node_1/files/im/20140811/15/file_name3
/opt/mftFileStore/node_1/files/im/20140811/15/file_name4
...
/opt/mftFileStore/node_1/files/im/20140811/15/file_name99
/opt/mftFileStore/node_1/files/im/20140811/15/file_name100
```

步骤 2 使用 `rm` 命令和此输出编写一个脚本，以从外部文件服务器清除上述文件。 如需 SQL 查询的示例，请参阅《*Cisco Unified Communications Manager* 上 *IM and Presence Service* 的数据库设置》。

注释 即使从外部数据库中清除了与这些文件相关的记录，仍然可以访问或下载尚未从外部文件服务器清除的文件。

下一步做什么

设置服务参数阈值，第 270 页

外部数据库磁盘使用情况

您必须确保磁盘或表空间未满，否则托管文件传输功能可能会停止工作。 以下是您可用于从外部数据库中清除记录的 SQL 命令示例。 有关其他查询，请参阅《*Cisco Unified Communications Manager* 上 *IM and Presence Service* 的数据库设置》。

注释 即使从外部数据库中清除了与这些文件相关的记录，仍然可以访问或下载尚未从外部文件服务器清除的文件。

操作	命令示例
删除已上传文件的所有记录。	DELETE FROM *aft_log* WHERE *method* = 'Post';
删除特定用户下载的所有文件的记录。	DELETE FROM *aft_log* WHERE *jid* LIKE '<userid>@<domain>%' AND *method* = 'Get';
删除特定时间后上传的所有文件的记录。	DELETE FROM *aft_log* WHERE *method* = 'Post' AND *timestampvalue* > '2014-12-18 11:58:39';

此外，有计数器和警报帮助您管理数据库磁盘使用情况。 有关详细信息，请参阅托管文件传输警报和计数器，第 271 页。

设置服务参数阈值

配置托管文件传输服务参数，以定义为外部文件服务器磁盘空间生成 RTMT 警报的阈值。

过程

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

步骤 2 为节点选择 **Cisco XCP 文件传输管理器**服务。

步骤 3 输入以下服务参数的值。

- **外部文件服务器可用空间下限阈值**—如果外部文件服务器分区上的可用空间百分比等于或低于此值，系统会生成 XcpMFTExtFsFreeSpaceWarn 警报。 默认值为 10%。
- **外部文件服务器可用空间上限阈值**—如果外部文件服务器分区上的可用空间百分比等于或超过此值，系统会清除 XcpMFTExtFsFreeSpaceWarn 警报。 默认值为 15%。

注释 请确保下限阈值不会大于上限阈值。 否则，重新启动 Cisco XCP 路由器服务后，Cisco XCP 文件传输管理器服务将无法启动。

步骤 4 单击**保存**。

步骤 5 重新启动 Cisco XCP 路由器服务：

a) 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 网络服务**。

b) 从**服务器**下拉列表中选择 IM and Presence 发布方，然后单击**前往**。

c) 在 **IM and Presence Service** 下，选择 **Cisco XCP 路由器**并单击**重新启动**。

下一步做什么

配置 XCP 文件传输警报，第 271 页

配置 XCP 文件传输警报

配置托管文件传输警报，以便在达到定义的阈值时收到通知。

过程

步骤 1 登录到 **Cisco Unified IM and Presence** 功能配置。

步骤 2 选择**警报** > **配置**。

步骤 3 从**服务器**下拉列表中，选择服务器（节点）并单击**前往**。

步骤 4 从**服务组**下拉列表中，选择 **IM and Presence Service** 并单击**前往**。

步骤 5 从**服务**下拉列表中，选择 **Cisco XCP 文件传输管理器（活动）**并单击**前往**。

步骤 6 根据需要配置警报设置。 有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 7 单击**保存**。

下一步做什么

有关可用警报和计数器的详细信息，请参阅 托管文件传输警报和计数器，第 271 页

托管文件传输警报和计数器

通过托管文件传输，传输的文件将仅在成功存档于外部文件服务器和文件元数据记录到外部数据库后提交到用户。 如果 IM and Presence Service 节点失去其与外部服务器或外部数据库的连接，则 IM and Presence Service 将不会向接收者提交文件。

托管文件传输警报

为确保在连接丢失时收到通知，请验证是否在实时监控工具中正确配置了以下警报。

注释 与外部文件服务器连接丢失前上传的任何文件以及正在下载到接收者的文件均无法下载。 然而，外部数据库中有一个失败传输的记录。 为了识别这些文件，外部数据库字段 file_size 和 bytes_transferred 不能匹配。

表 *31:* 托管文件传输警报

警报	问题	解决方案
XcpMFTExtFsMountError	Cisco XCP 文件传输管理器丢失其与外部文件服务器的连接。	单击外部文件服务器故障诊断程序了解详细信息。 检查外部文件服务器是否正常运行。 检查与外部文件服务器的网络连接是否有问题。
XcpMFTExtFsFreeSpaceWarn	Cisco XCP 文件传输管理器检测到外部文件服务器上的可用磁盘空间较少。	通过从用于文件传输的分区删除不需要的文件，释放外部文件服务器空间。
XcpMFTDBConnectError	Cisco XCP 数据访问层无法连接到数据库。	单击系统故障诊断程序了解详细信息。 检查外部数据库是否正常运行，且与外部数据库服务器的网络连接是否有问题。
XcpMFTDBFullError	Cisco XCP 文件传输管理器无法插入或修改外部数据库中的数据，因为磁盘或表空间已满。	检查数据库并评估是否可以释放或恢复任何磁盘空间。 考虑再添加数据库容量。

托管文件传输计数器

为帮助管理托管文件传输，您可以通过实时监控工具监控以下计数器。这些计数器保存在Cisco XCP MFT 计数器文件夹中。

表 *32:* 托管文件传输计数器

计数器	说明
MFTBytesDownloadedLastTimeslice	此计数器代表上一次报告间隔（通常为 60 秒）期间所下载的字节数。
MFTBytesUpoadedLastTimeslice	此计数器代表上一次报告间隔（通常为 60 秒）期间所上传的字节数。
MFTFilesDownloaded	此计数器代表下载的文件总数。
MFTFilesDownloadedLastTimeslice	此计数器代表上一次报告间隔（通常为 60 秒）期间所下载的文件数。
MFTFilesUploaded	此计数器代表上传的文件总数。
MFTFilesUploadedLastTimeslice	此计数器代表上一次报告间隔（通常为 60 秒）期间所上传的文件数。

为托管文件传输清理外部数据库

配置监控外部数据库并删除过期记录的作业。 这将确保始终有足够的磁盘空间用于新记录。

要清除托管文件传输的数据库表，确保选择**功能表**下的**托管文件传输 (MFT)** 功能。

过程

步骤 1 登录到数据库发布方节点上的 Cisco Unified CM IM and Presence 管理。

步骤 2 选择**消息** > **外部服务器设置** > **外部数据库作业**。

步骤 3 单击**清除外部数据库**。

步骤 4 执行下列操作之一：

- 若要手动清理连接到发布方节点的外部数据库，选择**相同 Cup 节点**。
- 若要手动清理连接到订阅方节点的外部数据库，选择**其他 Cup 节点**，然后选择外部数据库详细信息。
- 如果您将系统配置为自动监控并清除外部数据库，选中**自动清理**单选按键。

注释 我们建议您在设置自动清理之前先运行手动清理。

步骤 5 设置您想要返回以删除文件的**天数**。 例如，如果输入 90，系统将删除早于 90 天的记录。

步骤 6 单击**更新架构**以创建索引和已存储的数据库程序。

注释 您只需在第一次运行作业时更新架构。

步骤 7 设置您想要返回以删除文件的**天数**。 例如，如果输入 **90**，系统将删除早于 90 天的记录。

步骤 8 在**功能表**部分，选择您希望清除其记录的每项功能：

- **文字会议 (TC)**—选择此选项可以清除永久聊天功能的数据库表。
- **消息存档程序 (MA)**—选择此选项可以清除消息存档程序功能的数据库表。
- **托管文件传输 (MFT)**—选择此选项可以清除托管文件传输功能的数据库表

步骤 9 单击**提交清除作业**。

注释 如果您已启用**自动**选项，并且想要禁用它，请单击**禁用自动清除作业**按键。

第 26 章

管理最终用户

- 管理最终用户概述，第 275 页
- 管理最终用户任务流程，第 277 页
- 在线状态授权相互作用和限制，第 286 页

管理最终用户概述

有关将用户分配到 IM and Presence Service 节点以及为 IM and Presence Service 设置用户的信息，请参阅以下指南：

作为管理最终用户的管理任务的一部分，您可能必须管理以下任务：

- 配置用于授权在线状态请求的默认策略
- 为重复或无效的用户 ID 和目录 URI 配置计划的系统检查
- 修复出现的用户 ID 和目录 URI 问题

有关如何导入和设置最终用户的详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》的“配置最终用户”部分。

有关完成批量用户联系人列表导入和导出的信息，请参阅联系人列表的批量管理，第 355 页。

在线状态授权概述

您必须为在线状态订阅请求分配系统授权策略。 在线状态授权策略在系统层级确定系统上的最终用户是否可以查看其他最终用户的在线状态，而无需要求该最终用户授权。 此设置通过 **Presence 设置**配置窗口中的**允许用户在不提示其他用户批准的情况下查看其在线状态**复选框配置，可用的设置部分取决于部署的协议：

- 对于基于 SIP 的客户端，您必须配置 IM and Presence Service 以自动授权所有在线状态订阅请求，否则 Presence 将无法正常运行（这是默认设置）。 配置此选项后，IM and Presence Service 会自动授权所有请求，但有一个例外：在线状态被请求的用户在其 Cisco Jabber 客户端中配置了阻止列表，其中包括发出请求的用户。 这种情况下，系统会提示用户批准在线状态请求。

- 对于基于 XMPP 的客户端，您可以配置是否希望 IM and Presence Service 提示用户授权来自其他用户的在线状态请求，或者是否应自动授权这些在线状态请求。

注释 最终用户在其 Cisco Jabber 客户端中配置的用户策略配置可覆盖授权系统设置

Jabber 中的用户策略设置

授权在线状态请求时，IM and Presence Service 还会引用用户在其 Cisco Jabber 客户端中配置的用户策略。 最终用户可以将其他用户添加到阻止列表，这可以防止其他用户在未经授权的情况下查看其在线状态，或者他们可以将这些用户添加到允许列表中，以授权这些用户查看其在线状态。 这些设置会覆盖系统默认设置：

最终用户可以在其 Cisco Jabber 客户端内配置以下项目：

- 阻止列表 — 用户可以将其他用户（本地及外部用户）添加到阻止列表中。 如果任何被阻止的用户查看该用户的在线状态，他们始终会看到用户的可用性状态为不可用，而不管用户的真实状态如何。 用户还可以阻止整个联合域。
- 允许列表 — 用户可以允许其他本地及外部用户始终能够查看其可用性。 用户还可以允许整个外部（联合）域。
- 默认策略 — 用户的默认策略设置。 用户可以将策略设置为阻止或允许所有用户。

验证用户 ID 和目录 URI

对于单群集部署，重复的用户 ID 和目录 URI 不是问题，因为不能在同一群集中分配重复项。 但是，对于群集间部署，您可以偶尔将相同的用户 ID 或目录 URI 值分配给不同群集上的不同用户。

IM and Presence Service 提供以下验证工具来检查重复的用户 ID 和重复的目录 URI：

- Cisco IM and Presence 数据监控器服务 — 您可以使用此服务配置持续的系统检查。 Cisco IM and Presence 数据监控器服务会检查所有 IM and Presence Service 群集间节点的 Active Directory 条目中是否存在重复的用户 ID 以及重复或空的目录 URI。 系统会通过警报或通知通报管理员。 您可以使用 Cisco Unified 实时监控工具监控警报并为 Duplicate UserID 和 DuplicateDirectoryURI 错误设置电子邮件警报。
- 系统故障诊断程序 — 如果要临时检查系统是否存在错误（包括重复的目录 URI 和用户 ID），可使用系统故障诊断程序。 故障诊断程序仅提供最多 10 个用户的详细信息。 可从 Cisco Unified CM IM and Presence 管理界面（**诊断** > **系统故障诊断程序**）访问系统故障诊断程序。
- 命令行界面 — 要获取重复 URI 和用户 ID 的完整详细报告，运行 `utils users validate all` CLI 命令。

管理最终用户任务流程

过程

	命令或操作	目的
步骤 1	分配在线状态授权策略，第 277 页	为在线状态订阅请求分配系统授权策略。
步骤 2	针对用户数据配置数据监控器检查，第 278 页	配置 Cisco IM and Presence 数据监控器服务以对重复的目录 URI 和用户 ID 运行既定检查。发现问题时，系统会发出警报或通知。
步骤 3	通过系统故障诊断程序验证用户数据，第 280 页	如果要运行临时检查，确定是否存在包括重复目录 URI 和用户 ID 的系统问题，可运行系统故障诊断程序。
步骤 4	通过 CLI 验证用户 ID 和目录 URI，第 281 页	运行 CLI 命令以获取重复目录 URI 和用户 ID 的详细报告。
步骤 5	查看用户的在线状态设置，第 284 页	如果要查看启用 IM and Presence 的最终用户的在线状态设置，可以使用在线状态查看器。

分配在线状态授权策略

为在线状态订阅请求分配系统授权策略。

注释 最终用户可以在其 Cisco Jabber 客户端配置是否允许其他用户查看其在线状态。 此用户策略会覆盖系统授权设置。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中选择 **Presence** > **设置**。

步骤 2 选中或取消选中**允许用户查看其他用户的可用性而不收到批准提示**复选框。

- 选中 — IM and Presence 自动授权本地企业内收到的所有在线状态订阅请求。
- 取消选中 — IM and Presence 将所有在线状态订阅请求推介给在线状态被请求的客户。 用户可接受或拒绝请求。

注释 如果要部署基于 SIP 的客户端，必须选中此复选框。如果未选中此复选框，部署仅支持 XMPP 客户端。

步骤 3 单击**保存**。

步骤 4 重新启动 Cisco XCP 路由器服务。

下一步做什么

继续在 IM and Presence Service 上配置 SIP 发布干线。

针对用户数据配置数据监控器检查

完成以下任务可配置 Cisco IM and Presence 数据监控器，以按计划的时间间隔验证目录 URI 和用户 ID。 错误通过 Cisco Unified 实时监控工具的警报或通知传达。

注释 重复的目录 URI 和重复的用户 ID 错误只是群集间部署会遇到的问题。

过程

	命令或操作	目的
步骤 1	设置用户 ID 和目录 URI 验证检查计划， 第 278 页	配置 Cisco IM and Presence 数据监控器检查的计划时间间隔。 此服务会检查活动目录条目是否存在错误，包括重复的目录 URI 和用户 ID。
步骤 2	针对电子邮件警报设置电子邮件服务器， 第 279 页	可选。 如果要在数据监控器服务找到重复的目录 URI 或用户 ID 时接收电子邮件警报，您必须使用实时监控工具设置电子邮件服务器。
步骤 3	启用电子邮件警告， 第 279 页	可选。 完成此程序以启用针对 DuplicateDirectoryURI 和 DuplicateUserid 警报的电子邮件通知。 当 Cisco IM and Presence 数据监控器服务返回其中一个警报时，系统将向管理员发送一封电子邮件。

设置用户 ID 和目录 URI 验证检查计划

设置 Cisco IM and Presence 数据监控器服务的计划时间间隔。 此服务会按计划的时间间隔检查系统是否存在数据错误，包括重复的目录 URI 和用户 ID。 只要发现错误，系统就会发出警报或通知，用户可以通过实时监控工具查看。

开始之前

Cisco IM and Presence 数据监控器网络服务必须运行。 此服务默认在运行。 您可以在 Cisco Unified IM and Presence 功能配置界面的**控制中心 - 网络服务**窗口中确认服务是否正在运行。

过程

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

步骤 2 在**服务**下拉列表中，选择 **Cisco IM and Presence 数据监控器**。

步骤 3 在**用户检查间隔**字段中，以分钟为单位输入时间间隔。 您可以输入从 5 至 1440（分钟）的整数。默认值为 30 分钟。

步骤 4 单击**保存**。

下一步做什么

可选。 如果要设置在出现 DuplicateDirectoryURI 或 DuplicateUserid 警报时收到电子邮件通知， 针对电子邮件警报设置电子邮件服务器，第 279 页

针对电子邮件警报设置电子邮件服务器

只要数据监控器验证检查发现重复的目录 URI 和用户 ID 错误，管理员就可以收到电子邮件警报。如果是，请使用此可选程序为电子邮件警报设置电子邮件服务器。

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 279 页

启用电子邮件警告

此程序用于设置实时监控工具，以便在出现 DuplicateUserID 或 DuplicateDirectoryURI 系统警报时，系统通过电子邮件发送通知给管理员。

开始之前

针对电子邮件警报设置电子邮件服务器，第 279 页

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 单击 **IM and Presence** 选项卡。

步骤 3 单击您要为其添加电子邮件通知的警报。 例如，**DuplicateDirecytoryURI** 或 **DuplicateUserid** 系统警报。

步骤 4 选择**工具** > **警报** > **配置警报操作**。

步骤 5 在**警告操作**弹出窗口中，选择**默认**并单击**编辑**。

步骤 6 在**警告操作**弹出窗口中，**添加**收件人。

步骤 7 在弹出窗口中，输入您要向其发送电子邮件警报的地址，然后单击**确定**。

步骤 8 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 9 单击**确定**。

步骤 10 对要为其启用电子邮件通知的每个系统警报重复此程序。

通过系统故障诊断程序验证用户数据

Cisco Unified CM IM and Presence 管理 GUI 中的系统故障诊断程序可检查您的部署，监控是否存在重复的用户 ID 以及重复或无效的目录 URI。 故障诊断程序会检查部署中的所有节点和群集。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**诊断** > **系统故障诊断程序**。

步骤 2 监控**用户故障诊断程序**区域中用户 ID 和目录 URI 的状态。 如果系统检查检测到任何问题，将填充**问题**列。

- 验证所有用户均已配置唯一的用户 ID。
- 验证所有用户均已配置目录 URI。
- 验证所有用户均已配置唯一的目录 URI。
- 验证所有用户均已配置有效的目录 URI。
- 验证所有用户均已配置唯一的邮件 ID。

注释 重复的邮件 ID 将影响联合和 Exchange 日历集成功能的电子邮件地址。

步骤 3 如果出现问题，单击**解决方案**列中的**修复**链接将您重定向到 Cisco Unified Communications Manager 的**最终用户配置**窗口，您可以在那里重新配置用户设置。

注释 用户配置文件中的用户 ID 和目录 URI 字段可能映射至 LDAP 目录。 这种情况下，请在 LDAP 目录服务器中应用该修复。

下一步做什么

如果出现问题，编辑 Cisco Unified Communications Manager **最终用户配置**窗口中的用户设置。 如果用户从 LDAP 目录同步，您需要在 LDAP 目录中进行编辑。

如果需要更详细的报告，通过 CLI 验证用户 ID 和目录 URI，第 281 页。

通过 CLI 验证用户 ID 和目录 URI

使用命令行界面对部署运行详细的检查，确认是否存在重复的用户 ID 和重复的目录 URI。

过程

步骤 1 登录到命令行界面。

步骤 2 运行以下命令之一：

- `utils users validate all` — 检查系统中是否存在重复的用户 ID 和重复的目录 URI。
- `utils users validate userid` — 检查系统中是否存在重复的用户 ID。
- `utils users validate uri` — 检查系统中是否存在重复的目录 URI。

CLI 返回一份说明重复目录 URI 和/或用户 ID 的报告。 如需报告的示例，请参阅用户 ID 和目录 URI CLI 验证示例，第 281 页

下一步做什么

如果出现问题，编辑 Cisco Unified Communications Manager 最终用户配置窗口中的用户设置。 如果用户从 LDAP 目录同步，您需要在 LDAP 目录中进行编辑。

用户 ID 和目录 URI CLI 验证示例

验证 IM and Presence Service 用户以确定具有重复用户 ID 以及重复或无效目录 URI 的用户的 CLI 命令是 utils 用户验证 { all | userid | uri }。

目录 URI 对每个用户必须都是唯一的。 您不能对多个用户使用相同的目录 URI，无论其是否区分大小写。 例如，您不能有两个不同的目录 URI（例如 `aaa@bbb.ccc` 和 `AAA@BBB.CCC`），尽管它们区分大小写。

有关使用 CLI 和命令说明的详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面指南》。

显示用户 ID 错误的 CLI 示例输出

```
Users with Duplicate User IDs
---------------------------------------------
 User ID: user3
  Node Name
  cucm-imp-1
  cucm-imp-2
```

显示目录 URI 错误的 CLI 示例输出

```
Users with No Directory URI Configured
-----------------------------------------------------
 Node Name: cucm-imp-2
 User ID
 user4

Users with Invalid Directory URI Configured
-----------------------------------------------------
 Node Name: cucm-imp-2
 User ID   Directory URI
 user1     asdf@ASDF@asdf@ADSF@cisco

Users with Duplicate Directory URIs
-----------------------------------------------------
Directory URI: user1@cisco.com
 Node Name   User ID
 cucm-imp-1  user4
 cucm-imp-2  user3
```

用户 ID 和目录 URI 错误

Cisco IM and Presence 数据监控器服务会检查所有 IM and Presence Service 群集间节点的 Active Directory 条目中是否存在重复的用户 ID 以及空或重复的目录 URI。 重复的用户 ID 或目录 URI 不可能在一个群集中出现；但是，有可能无意中将同一用户 ID 或目录 URI 值分配给群集间部署中不同群集上的用户。

以下列表显示可能发现的错误。 您可以在实时监控工具中查看这些错误，这将为每个错误发出警报或通知：

DuplicateDirectoryURI

此警告表示，当配置目录 URI IM 地址方案后，群集间部署中有多位用户分配了相同的目录 URI 值。

DuplicateDirectoryURIWarning

此警告表示，当配置 `userID@Default_Domain` IM 地址方案后，群集间部署中有多位用户分配了相同的目录 URI 值。

DuplicateUserid

此警报表示有重复的用户 ID 分配给群集间部署中不同群集上的一位或多位用户。

InvalidDirectoryURI

此警报表示，当配置目录 URI IM 地址方案后，群集间部署中的一位或多位用户分配了空或无效的目录 URI 值。

InvalidDirectoryURIWarning

此警告表示，当配置 `userID@Default_Domain` IM 地址方案后，群集间部署中的一位或多位用户分配了空的或无效的目录 URI 值。

要收集有关哪些用户存在这些警报情况的具体信息，请使用命令行界面生成完整列表。 系统警报不提供受影响用户的详细信息，系统故障诊断程序只显示最多 10 位用户的详细信息。 使用命令行界面并验证用户以收集有关哪些用户引起了警报的信息。 有关详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面指南》。

注意 采取相应措施来纠正重复的用户 ID 以及重复或无效的目录 URI，避免受影响的用户通信中断。 要修改用户联系人信息，请参阅《*Cisco Unified Communications Manager* 管理指南》。

错误和建议的操作

下表介绍，当在群集间部署中进行针对重复用户 ID 以及重复或无效目录 URI 的系统检查时，可能出现的用户 ID 和目录 URI 错误情况。 发出的警报已列出，以及建议采取以纠正错误的措施。

表 *33*: 用户 *ID* 和目录 *URI* 错误情况以及建议的操作

错误情况	说明	建议的措施
用户 ID 重复	重复的用户 ID 已分配至群集间部署中不同群集上的一位或多位用户。受影响的用户可能驻留在群集间对等成员上。 **相关警报：** `DuplicateUserid`	如果系统发出 `DuplicateUserid` 警报，请立即采取措施并纠正问题。群集间部署中的每位用户必须有唯一的用户 ID。
目录 URI 重复	群集间部署中的多位用户分配到相同的目录 URI 值。 受影响的用户可能驻留在群集间对等成员上。 **相关警报：** • `DuplicateDirectoryURI` • `DuplicateDirectoryURIWarning`	如果系统配置为使用目录 URI IM 地址方案且发出 `DuplicateDirectoryURI` 警报，请立即采取措施并纠正问题。 每位用户必须分配唯一的目录 URI。 如果系统配置为使用 *userID@Default_Domain* IM 地址方案、检测到重复的目录 URI、发出 `DuplicateDirectoryURIWarning` 警报，无需立即采取任何措施，但思科建议您解决该问题。

错误情况	说明	建议的措施
目录 URI 无效	部署内的一位或多位用户分配到无效或空的目录 URI 值。 非 *user@domain* 格式的 URI 不是有效的目录 URI。 受影响的用户可能驻留在群集间对等成员上。 **相关警报：** • `InvalidDirectoryURI` • `InvalidDirectoryURIWarning`	如果系统配置为使用目录 URI IM 地址方案且发出以下警报，请立即采取措施并纠正问题：`InvalidDirectoryURI`。 如果系统配置为使用 *userID@Default_Domain* IM 地址方案、检测到无效的目录 URI、发出 `InvalidDirectoryURIWarning` 警报，无需立即采取任何措施，但思科建议您解决该问题。

查看用户的在线状态设置

使用在线状态查看器可以大致了解启用 IM and Presence 的最终用户的在线状态设置。 在线状态查看器提供在线状态服务器分配、联系人和观察者等信息。

开始之前

Cisco AXL Web 服务、**Cisco SIP Proxy** 服务和 **Cisco Presence Engine** 服务都必须在 Cisco Unified 功能配置中运行。

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 单击**查找**并选择您要查看其在线状态设置的最终用户。

步骤 3 在**服务设置**下，单击**用户的在线状态查看器**打开在线状态查看器。 如果您想要自定义视图，请参阅下表。

表 *34:* 最终用户在线状态查看器字段

在线状态设置	说明
用户状态	标识用户的可用性状态，包括： • 可用 • 离开 • 免打扰 • 无法应答 • 自定义

在线状态设置	说明
用户 ID	标识所选用户 ID。 如果有可用于该用户的用户照片，此时将显示。 您可以单击**提交**选择其他用户 ID。
查看视角	指定用户以从该用户的视角查看可用性状态。 这将允许您确定指定用户的可用性状态对其他用户（称为观察程序）如何显示。 此功能在调试情况下非常有用，例如，用户配置了隐私策略时。 最多允许 128 个字符。
联系人	显示此用户联系人列表中的联系人数量。 单击“联系人和观察者”列表区域中“联系人”标题旁边的箭头，查看特定用户联系人的可用性状态。 单击组名称旁边的箭头，展开该组内联系人的列表。 不属于该组的联系人（无组联系人）在联系人组列表下方显示。 联系人可以属于多个组，但针对该用户的联系人列表大小仅计算一次。 如果超出为最终用户配置的最大联系人数量，则显示警告消息。 有关 IM and Presence Service 配置和最大联系人数设置的详细信息，请参阅 *IM and Presence* 管理在线帮助。
观察者	显示预订查看其联系人列表中此用户可用性状态的用户（称为观察者）的列表。 单击“联系人和观察者”列表区域中“观察者”标题旁边的箭头，查看特定观察者的可用性状态。 单击组名称旁边的箭头，展开该组内观察者的列表。 观察者可以属于多个组，但针对该用户的观察者列表大小仅计算一次。 如果超出为最终用户配置的最大观察者数量，则显示警告消息。 有关 IM and Presence Service 配置和最大观察者数设置的详细信息，请参阅 *IM and Presence* 管理在线帮助。
Presence 服务器分配	识别分配给用户的 IM and Presence Service 服务器。 超链接允许您直接访问服务器配置页面以了解详细信息。
启用可访问的在线状态图标	选中此复选框以启用此最终用户的在线状态可访问性图标。
提交	选择以运行在线状态查看器。 用户必须分配给 IM and Presence 节点才能使有效在线状态信息可用。 AXL、在线状态引擎和代理服务必须都在此 IM and Presence 服务器上运行，才能使此操作正常工作。

在线状态授权相互作用和限制

功能	限制
关闭自动在线状态授权	如果关闭在线状态请求自动授权，IM and Presence Service 仍会自动授权另一位用户的联系人列表中用户的订阅请求。 这适用于同一域中的用户以及不同于域中的用户（联合用户）。 例如： • 用户 A 希望订阅查看用户 B 的可用性状态。IM and Presence Service 上自动授权已关闭，用户 B 不在用户 A 的允许或阻止列表中。 • IM and Presence Service 将在线状态订阅请求发送至用户 B 的客户端应用程序，后者提示用户 B 接受或拒绝该订阅。 • 用户 B 接受在线状态订阅请求，随即用户 B 会添加到用户 A 的联系人列表。 • 然后，用户 A 自动添加到用户 B 的联系人列表，而无需系统提示授权该在线状态订阅。 即使用户 B 的策略阻止外部域，或者用户 B 在用户配置文件中配置了“询问我”，也会发生这种情况。
域间联合 — 从外部域收到在线状态请求	IM and Presence 将仅依赖于请求其在线状态的用户的用户策略设置。 如果用户在其用户策略中选择“询问我”，并且尚未为外部联系人或域添加允许或阻止列表，则 IM and Presence 会将在线状态请求发送给最终用户进行授权。

第 27 章

将用户迁移到集中式部署

- 集中式部署用户迁移概述，第 287 页
- 中央群集迁移的前提条件任务，第 287 页
- 迁移到中央群集任务流程，第 288 页

集中式部署用户迁移概述

本章介绍将现有 IM and Presence Service 用户从标准分散式 IM and Presence 部署（Cisco Unified Communications Manager 上的 IM and Presence Service）迁移到集中式部署的程序。 采用集中式部署时，IM and Presence 部署和电话部署处于单独的群集。

中央群集迁移的前提条件任务

如果要设置新的 IM and Presence 中央群集，以便所有用户都从现有的分散式群集迁移，请完成以下为迁移设置群集的前提条件步骤。

注释 如果添加的是不需要迁移的新用户，可以按照配置集中式部署，第 97 页中的说明使用新用户设置中央群集。 只有在确信配置有效后，才能将现有用户迁移到中央群集。

表 *35:* 迁移前任务

	迁移前任务
步骤 1	将新中央群集连接到迁移的群集。 **1.** 登录到 IM and Presence Service 集中式群集上的数据库发布方节点。 **2.** 从 Cisco Unified CM IM and Presence 管理中，选择**系统** > **集中式部署**。 **3.** 单击**查找**并键入以下任意一项： • 选择现有群集，然后单击**编辑选定项**。 • 单击**新增**以添加迁移的群集。 **4.** 为每个迁移的群集填写以下字段： • **对等地址** — 远程电话发布方节点的 FQDN、主机名、IPv4 地址或 IPv6 地址。 • **AXL 用户名** — 远程电话群集上的 AXL 帐户的登录用户名。 • **AXL 密码** — 远程群集上的 AXL 帐户的密码。 **5.** 单击**保存**。
步骤 2	如果新的中央群集将成为 IM and Presence 群集间网络的一部分，在中央群集与不属于迁移的任何 IM and Presence 对等群集之间配置群集间对等。 以下准则适用： • 您不需要在中央群集和迁移的群集之间配置群集间对等。 但是，如果迁移群集的群集间对等连接在迁移时配置了任意数量的非迁移群集，则必须在迁移之前在中央群集中配置这些群集间对等连接，否则迁移将不起作用。 • 配置群集间对等后，确保验证群集间对等状态，确保配置正常工作 有关详细信息，请参阅配置群集间对等，第 151 页。中的群集间对等配置主题

迁移到中央群集任务流程

完成这些任务以将现有用户从分散式群集（Cisco Unified Communications Manager 上的 IM and Presence Service）迁移到集中式 IM and Presence 群集。 在此任务流程中：

- **IM and Presence 中央群集**指将用户迁移到的群集。 迁移之后，该群集只会处理 IM and Presence。
- **迁移群集**指从中迁移 IM and Presence 用户的群集。 迁移之后，该群集只会处理电话。

开始之前

如果您的 IM and Presence 中央群集是新安装的群集，并且还没有用户，请在迁移用户之前完成中央群集迁移的前提条件任务，第 287 页。

表 *36:* 迁移到中央群集任务流程

	IM and Presence 中央群集	迁移群集	目的
步骤 1		从迁移群集导出联系人列表，第 290 页	将迁移群集中的用户联系人列表导出到 csv 文件。
步骤 2		在迁移群集中禁用高可用性，第 291 页	禁用迁移群集中所有 Presence 冗余组（子群集）的高可用性。
步骤 3		为 IM and Presence 配置 UC 服务，第 292 页	在迁移群集中，配置指向 IM and Presence 中央群集的 IM and Presence UC 服务。
步骤 4		为 IM and Presence 创建服务配置文件，第 292 页	在迁移群集中，创建使用您设置的 IM and Presence UC 服务的服务配置文件。
步骤 5		在电话群集中禁用 Presence 用户，第 293 页	在迁移群集中可使用批量管理为用户禁用 IM and Presence。
步骤 6		为中央群集启用 OAuth 验证，第 294 页	可选。 在迁移群集中，启用 OAuth 刷新登录。 这样将同时为中央群集启用功能。
步骤 7	在集中式群集中禁用高可用性，第 294 页		在 IM and Presence 中央群集的所有 Presence 冗余组（子群集）中禁用高可用性。
步骤 8	删除中央和迁移群集的对等关系，第 295 页		如果中央群集与迁移群集之间存在群集间对等，则在两个群集上删除对等连接。
步骤 9	阻止思科群集间同步代理，第 295 页		在 IM and Presence 中央群集中停止思科群集间同步代理。
步骤 10	通过功能组模板启用 IM and Presence，第 296 页		在中央群集中，配置启用 IM and Presence Service 的功能组模板。

	IM and Presence 中央群集	迁移群集	目的
步骤 11	在集中式群集上完成 LDAP 同步，第 296 页		将功能组模板添加到 LDAP 目录同步。 使用同步从迁移群集添加用户。
步骤 12	将联系人列表导入集中式群集，第 298 页		使用批量管理和先前创建的 csv 导出文件将联系人列表导入中央群集。
步骤 13	启动思科群集间同步代理，第 299 页		在中央群集中启用思科群集间同步代理。
步骤 14	在中央群集中启用高可用性，第 299 页		在中央群集中，启用所有 Presence 冗余组的高可用性。
步骤 15	删除迁移群集的剩余对等，第 300 页		删除迁移群集（现在是电话群集）和其他对等群集之间剩余的群集间对等连接。

从迁移群集导出联系人列表

仅当您从分散式 IM and Presence 部署迁移到集中式部署时，才完成此程序。 在迁移群集中，将用户的联系人列表导出到 csv 文件，以后您可以将其导入中央群集。 您可以导出两种类型的联系人列表：

- 联系人列表 — 此列表包含 IM and Presence 联系人。 没有 IM 地址的联系人将不会与此列表一起导出（您必须导出非 Presence 联系人列表）。
- 非 Presence 联系人列表 — 此列表包含没有 IM 地址的联系人。

过程

步骤 1 在旧群集（电话群集）中登录 Cisco Unified CM IM and Presence 管理。

步骤 2 根据要导出的联系人列表类型，选择以下选项之一：

- 对于联系人列表导出，选择**批量管理** > **联系人列表** > **导出联系人列表**
- 对于非 Presence 联系人列表导出，选择**批量管理** > **非 presence 联系人列表** > **导出非 Presence 联系人列表**并跳过下一个步骤。

步骤 3 仅联系人列表。 选择要导出其联系人列表的用户：

a) 在**导出联系人列表选项**下，选择要导出其联系人列表的用户的类别。 默认选项为**群集中的所有用户**。

b) 单击**查找**以显示用户列表，然后单击**下一步**。

步骤 4 输入**文件名**。

步骤 5 在**作业信息**下，配置要运行此作业的时间：

- **立即运行** — 如果选中此按键，联系人列表会立即导出。
- **稍后运行** — 如果要安排作业运行的时间，选中此按键。

步骤 6 单击**提交**。

注释 如果选择**立即运行**，导出文件将会立即生成。 如果选择**稍后运行**，必须使用任务调度（**批量管理** > **任务调度**）来安排此作业运行的时间。

步骤 7 导出文件生成后，下载 csv 文件：

a) 选择**批量管理** > **上传/下载文件**。
b) 单击**查找**。
c) 选择要下载的导出文件，然后单击**下载选定项**。
d) 将文件保存到安全的位置。

步骤 8 如果要创建另一个 csv 导出文件，请重复此程序。 例如，如果您为联系人列表创建导出文件，则可能需要为非 Presence 联系人列表创建另一个文件。

下一步做什么

在迁移群集中禁用高可用性，第 291 页

在迁移群集中禁用高可用性

对于到集中式部署的迁移，在迁移电话群集中禁用每个 Presence 冗余组（子群集）中的高可用性。

注释 **Presence 冗余组详细信息**页面将显示所有活动的 JSM 会话，即使群集中禁用了高可用性也不例外。

过程

步骤 1 在旧群集上登录到 Cisco Unified Communications Manager 发布方节点。

步骤 2 从 Cisco Unified CM 管理中，选择**系统** > **Presence 冗余组**。

步骤 3 单击**查找**并选择一个子群集。

步骤 4 取消选中**启用高可用性**复选框。

步骤 5 单击**保存**。

步骤 6 为每个子群集重复此程序。

注释 为所有子群集完成此程序后，请至少等待 2 分钟，然后再在此群集上完成任何其他配置。

下一步做什么

为 IM and Presence 配置 UC 服务，第 292 页

为 IM and Presence 配置 UC 服务

在远程电话群集中执行此程序可配置指向 IM and Presence Service 中央群集的 UC 服务。 电话群集中的用户将从 IM and Presence 中央群集获取 IM and Presence Service。

过程

步骤 1 登录电话群集的 Cisco Unified CM 管理界面。

步骤 2 选择**用户管理** > **用户设置** > **UC 服务**。

步骤 3 执行以下任一操作：

a) 单击**查找**并选择要编辑的现有服务。

b) 单击**新增**以创建新的 UC 服务。

步骤 4 从 **UC 服务类型**下拉列表框中选择 **IM and Presence** 并单击**下一步**。

步骤 5 从**产品类型**下拉列表框中选择 **IM and Presence Service**。

步骤 6 为群集输入唯一的**名称**。 这不一定是主机名。

步骤 7 从**主机名/IP 地址**，输入 IM and Presence 中央群集数据库发布方节点的主机名、IPv4 地址或 IPv6 地址。

步骤 8 单击**保存**。

步骤 9 建议。 重复此程序以创建第二个 IM and Presence Service，其中**主机名/IP 地址**字段指向中央群集中的订阅方节点。

下一步做什么

为 IM and Presence 创建服务配置文件，第 292 页

为 IM and Presence 创建服务配置文件

在远程电话群集中执行此程序可创建指向 IM and Presence 中央群集的服务配置文件。 电话群集中的用户将使用此服务配置文件从中央群集获取 IM and Presence Service。

过程

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

步骤 2 执行下列操作之一：

a) 单击**查找**并选择要编辑的现有服务配置文件。

b) 单击**新增**以创建新的服务配置文件。

步骤 3 在 **IM and Presence 配置文件**部分，配置您在上一个任务中配置的 IM and Presence Service：

a) 从**主**下拉列表中，选择数据库发布方节点服务。

b) 从**次要**下拉列表中，选择订阅方节点服务。

步骤 4 单击**保存**。

下一步做什么

在电话群集中禁用 Presence 用户，第 293 页

在电话群集中禁用 Presence 用户

如果您已在电话部署中完成 LDAP 同步，请使用批量管理工具为 IM and Presence 用户编辑电话群集中的用户设置。此配置会将 Presence 用户指向 IM and Presence Service 的中央群集。

注释 此程序假定您已在电话群集中完成 LDAP 同步。但是，如果尚未完成初始 LDAP 同步，可以将 Presence 用户的中央部署设置添加到初始同步中。这种情况下，请在电话群集中执行以下操作：

- 配置包含您刚刚设置的**服务配置文件**的功能组模板。确保选中**主群集**选项，不要选中**为 Unified CM IM and Presence 启用用户**选项。
- 在 **LDAP 目录配置**种，将**功能组模板**添加到您的 LDAP 目录同步。
- 完成初始同步。

有关配置功能组模板和 LDAP 目录的更多详情，请参阅《*Cisco Unified Communications Manager* 系统配置指南》的“配置最终用户”部分。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**查询** > **批量管理** > **用户** > **更新用户** > **查询**。

步骤 2 从过滤器中，选择**已启用主群集**并单击**查找**。该窗口将显示以此为主群集的所有最终用户。

步骤 3 单击**下一步**。

在**更新用户配置**窗口中，最左侧的复选框表示是否要使用此查询编辑此设置。如果不选中左侧的复选框，查询将不会更新该字段。右侧的字段表示此字段的新设置。如果出现两个复选框，必须选中左侧的复选框以更新该字段，并在右侧复选框中输入新设置。

步骤 4 在**服务设置**下，为以下每个字段选中最左侧的复选框，表示要更新这些字段，然后编辑相邻的设置，如下所示：

- **主群集** — 选中右侧复选框以将电话群集启用为主群集。
- **为 Unified CM IM and Presence 启用用户** — 不选中右侧复选框。此设置禁用电话群集作为 IM and Presence 的提供者。

- **UC 服务配置文件** — 从下拉列表中选择您在上一个任务中配置的服务配置文件。此设置将用户指向 IM and Presence 中央群集，该群集将是 IM and Presence Service 的提供者。

注释 有关 Expressway 移动和远程访问配置，请参阅《通过 *Cisco Expressway* 的移动和远程访问部署指南》，网址：https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html。

步骤 5 根据需要填写所有剩余字段。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 6 在**作业信息**下选择**立即运行**。

步骤 7 单击**提交**。

下一步做什么

为中央群集启用 OAuth 验证，第 294 页

为中央群集启用 OAuth 验证

此程序用于在电话群集中启用 OAuth 验证。 这还可以在 IM and Presence 中央群集中启用 OAuth 验证。

过程

步骤 1 登录到电话群集上的 Cisco Unified CM 管理。

步骤 2 选择**系统** > **企业参数**

步骤 3 在 **SSO 和 OAuth 配置**下，将**具有刷新登录流的 OAuth** 企业参数设置为**启用**。

步骤 4 如果您编辑了参数设置，单击**保存**。

在集中式群集中禁用高可用性

请确保在 IM and Presence 中央群集的每个所有 Presence 冗余组（子群集）中禁用高可用性。 必须在应用配置或迁移用户之前执行此操作。

注释 **Presence 冗余组详细信息**页面将显示所有活动的 JSM 会话，即使群集中禁用了高可用性也不例外。

过程

步骤 1 登录到中央群集的 Cisco Unified CM 管理实例。

步骤 2 选择**系统** > **Presence 冗余组**。

步骤 3 单击**查找**并选择现有子群集。

步骤 4 取消选中**启用高可用性**复选框。

步骤 5 单击**保存**。

步骤 6 为每个子群集重复此步骤。

下一步做什么

阻止思科群集间同步代理，第 295 页

删除中央和迁移群集的对等关系

如果 IM and Presence 中央群集与迁移群集之间存在群集间对等，则删除该对等关系。

过程

步骤 1 登录到 IM and Presence Service 中央群集的数据库发布方节点。

步骤 2 在 Cisco Unified CM IM and Presence 管理中，选择 **Presence** > **群集间**。

步骤 3 单击**查找**并选择迁移群集。

步骤 4 单击**删除**。

步骤 5 重新启动 **Cisco XCP 路由器**：

a) 登录到 Unified IM and Presence 功能配置并选择**工具** > **控制中心 - 网络服务**。

b) 从**服务器**列表中，选择数据库发布方节点并单击**前往**。

c) 在 **IM and Presence Service** 下，选择 **Cisco XCP 路由器**并单击**重新启动**。

步骤 6 在迁移群集上重复这些步骤。

阻止思科群集间同步代理

配置 IM and Presence 中央群集之前，请确保在中央群集上停止**思科群集间同步代理**服务。

过程

步骤 1 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 网络服务**。

步骤 2 从**服务器**下拉列表中选择中央群集数据库发布方节点，然后单击**前往**。

步骤 3 确认**思科群集间同步代理**服务的状态。 如果服务正在运行或已激活，选择相邻的单选按键，然后单击**停止**。

下一步做什么

通过功能组模板启用 IM and Presence，第 296 页

通过功能组模板启用 IM and Presence

此程序用于为中央群集配置具有 IM and Presence 设置的功能组模板。 您可以将功能组模板添加到 LDAP 目录配置，以便为同步用户配置 IM and Presence。

注释 您只能将功能组模板应用于尚未进行初始同步的 LDAP 目录配置。 从中央群集同步 LDAP 配置后，无法对 Cisco Unified Communications Manager 中的 LDAP 配置应用编辑。 如果您已同步目录，则需要使用批量管理为用户配置 IM and Presence。 有关详细信息，请参阅通过批量管理为 IM and Presence 启用用户，第 105 页。

过程

步骤 1 登录 IM and Presence 集中式群集的 Cisco Unified CM 管理界面。 此服务器应该没有配置电话。

步骤 2 选择**用户管理** > **用户/电话添加** > **功能组模板**。

步骤 3 执行下列操作之一：

- 单击**查找**并选择现有模板
- 单击**新增**以创建新的模板

步骤 4 选中以下两个复选框：

- **主群集**
- **为 Unified CM IM and Presence 启用用户**

步骤 5 填写**功能组模板配置**窗口中的其余字段。 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**。

下一步做什么

要将设置传播给用户，必须将功能组模板添加到尚未进行初始同步的 LDAP 目录配置中，然后完成初始同步。

在集中式群集上完成 LDAP 同步，第 296 页

在集中式群集上完成 LDAP 同步

在远程 Cisco Unified Communications Manager 电话群集上执行此程序，可使用 LDAP 同步将集中式 IM and Presence 设置部署到 Cisco Unified Communications Manager 部署。

注释 有关如何设置 LDAP 目录同步的更多详情，请参阅《*Cisco Unified Communications Manager* 系统配置指南》的“配置最终用户”部分。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统** > **LDAP** > **LDAP 目录**。

步骤 2 执行以下任一操作：

- 单击**查找**并选择现有的 LDAP 目录同步。
- 单击**新增**以创建新的 LDAP 目录同步。

步骤 3 从**功能组模板**下拉列表框中，选择您在上一个任务中创建的功能组模板。 必须在此模板上禁用 IM and Presence。

步骤 4 填写 **LDAP 目录**窗口中的其余字段。 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**执行完全同步**。
Cisco Unified Communications Manager 会将其数据库与 LDAP 目录同步，并分配更新的 IM and Presence 设置。

下一步做什么

将联系人列表导入集中式群集，第 298 页

通过批量管理为 IM and Presence 启用用户

如果您已将用户同步到中央群集，并且没有为 IM and Presence Service 启用这些用户，请使用批量管理的更新用户功能为 IM and Presence Service 启用这些用户。

注释 您还可以使用批量管理的导入用户或插入用户功能通过 csv 文件导入新用户。 有关程序，请参阅《*Cisco Unified Communications Manager* 批量管理指南》。 请确保导入的用户选择了以下选项：

- 主群集
- 为 Unified CM IM and Presence 启用用户。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**批量管理** > **用户** > **更新用户** > **查询**。

步骤 2 从**过滤器**中，选择**已启用主群集**并单击**查找**。 该窗口将显示以此为主群集的所有最终用户。

步骤 3 单击**下一步**。

在**更新用户配置**窗口中，最左侧的复选框表示是否要使用此查询编辑此设置。 如果不选中左侧的复选框，查询将不会更新该字段。 右侧的字段表示此字段的新设置。 如果出现两个复选框，必须选中左侧的复选框以更新该字段，并在右侧复选框中输入新设置。

步骤 4 在**服务设置**下，为以下每个字段选中左侧的复选框，表示要更新这些字段，然后编辑相邻字段的设置，如下所示：

- **主群集** — 选中右侧复选框以将此群集启用为主群集。
- **为 Unified CM IM and Presence 启用用户** — 选中右侧复选框。 此设置使中央群集成为这些用户的 IM and Presence Service 提供商。

步骤 5 填写想要更新的所有剩余字段。 有关这些字段及其设置的帮助，请参阅联机帮助：

步骤 6 在**作业信息**下选择**立即运行**。

步骤 7 单击**提交**。

将联系人列表导入集中式群集

如果已将用户迁移到 IM and Presence 中央群集，可以执行此程序以将用户的联系人列表导入 IM and Presence 中央群集。 您可以导入以下任一类型的联系人列表：

- 联系人列表 — 此列表包含 IM and Presence 联系人。
- 非 Presence 联系人列表 — 此列表包含没有 IM 地址的联系人。

开始之前

您需要从旧群集（电话群集）导出的联系人列表 csv 文件。

过程

步骤 1 登录 IM and Presence 中央群集上的 Cisco Unified CM IM and Presence 管理。

步骤 2 上传从电话群集导出的 csv 文件：

a) 选择**批量管理** > **上传/下载文件**。
b) 单击**新增**。
c) 单击**选择文件**并选择您要导入的 csv 文件。
d) 根据要导入的联系人列表类型，从**选择目标**下拉列表中选择以下任一项：**联系人列表**或**非 Presence 联系人列表**。
e) 从**选择事务类型**中选择导入作业。
f) 单击**保存**。

步骤 3 将 csv 信息导入到中央群集：

a) 在 Cisco Unified CM IM and Presence 管理中，执行以下任一操作：

- 对于联系人列表导入，选择**批量管理** > **联系人列表** > **更新联系人列表**。
- 对于非 Presence 联系人列表导入，选择**批量管理** > **非 presence 联系人列表** > **导入非 Presence 联系人列表**。

b) 在**文件名**下拉列表中，选择上传的 csv 文件。
c) 在**作业信息**下，根据要运行的作业选择**立即运行**或**稍后运行**。
d) 单击**提交**。 如果您选择**立即运行**，系统会立即导入联系人列表

注释 . 如果您选择**稍后运行**，必须进入**批量管理** > **任务调度**，然后选择作业并安排此作业运行的时间。

步骤 4 如果您有第二个 csv 文件要导入，重复执行此程序。

下一步做什么

启动思科群集间同步代理，第 299 页

启动思科群集间同步代理

配置或迁移完成后，启动 IM and Presence 中央群集中的**思科群集间同步代理**。 如果使用群集间对等，则需要此服务。

过程

步骤 1 在 Cisco Unified IM and Presence 功能配置中，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 IM and Presence 数据库发布方节点，然后单击**前往**。
步骤 3 在 **IM and Presence Service** 下，选择**思科群集间同步代理**并单击**启动**。

下一步做什么

在中央群集中启用高可用性，第 299 页

在中央群集中启用高可用性

配置或用户迁移完成后，在 IM and Presence 中央群集的 Presence 冗余组（子群集）中启用高可用性。

过程

步骤 1 登录 IM and Presence 中央群集上的 Cisco Unified CM 管理实例。

步骤 2 选择**系统** > **Presence 冗余组**。

步骤 3 单击**查找**并选择现有子群集。

步骤 4 选中**启用高可用性**复选框。

步骤 5 单击**保存**。

步骤 6 为 IM and Presence 中央群集中的每个子群集重复此程序。

删除迁移群集的剩余对等

删除迁移群集（现在是电话群集）与任何剩余的 IM and Presence Service 对等群集之间的群集间对等关系。

注释 删除群集间连接可推迟到更靠后的日期，具体取决于整个网格中的 Cisco XCP 路由器重新启动可用性。 只要电话群集与任意数量的对等群集之间存在现有群集间连接，当前正在运行的 Cisco XCP 路由器服务应在电话群集上保持**运行**状态。

过程

步骤 1 登录到迁移群集的 IM and Presence 数据库发布方节点。

步骤 2 在 Cisco Unified CM IM and Presence 管理中，选择 **Presence** > **群集间**。

步骤 3 单击**查找**并选择对等群集。

步骤 4 单击**删除**。

步骤 5 重新启动 **Cisco XCP 路由器**：

a) 登录到 Unified IM and Presence 功能配置并选择**工具** > **控制中心 - 网络服务**。

b) 从**服务器**列表中，选择数据库发布方节点并单击**前往**。

c) 在 **IM and Presence Service** 下，选择 **Cisco XCP 路由器**并单击**重新启动**。

步骤 6 在 IM and Presence Service 对等群集上重复这些步骤。

注释 如果迁移群集有到多个群集的群集间对等连接，则必须对保留在群集间网络中的每个对等群集重复此程序。 这意味着在迁移群集中，**Cisco XCP 路由器**重新启动的次数将与被中断的对等群集连接数量一样多。

第 28 章

迁移用户

- 迁移用户概述， 第 301 页
- 迁移用户前提条件， 第 301 页
- 迁移用户任务流程， 第 301 页

迁移用户概述

本部分介绍如何在 IM and Presence Service 群集之间迁移用户。

迁移用户前提条件

- 运行当前和目标群集的完整备份。 有关详细信息，请参阅 备份任务流程， 第 330 页。
- 确保要迁移的用户仅在其当前主群集上获得 IM and Presence Service 或 Cisco Jabber 的许可。 如果这些用户在预迁移群集以外的任何群集上获得许可，则在继续执行迁移任务之前，必须完全取消给予他们的许可。

迁移用户任务流程

完成这些任务可将 IM and Presence 用户迁移到新群集。

过程

	命令或操作	目的
步骤 1	删除过期的条目， 第 302 页	在迁移用户之前，删除所有过期的名录、组条目和不存在的联系记录。
步骤 2	为迁移启动基本服务， 第 304 页	在迁移之前，确认以下服务正在运行： • Cisco AXL Web 服务

	命令或操作	目的
		• Cisco 同步代理 • Cisco 群集间同步代理
步骤 3	群集间同步错误检查，第 304 页	运行系统故障诊断程序，并确认未报告任何群集间同步问题。
步骤 4	为迁移配置标准 Presence，第 303 页	在迁移用户之前配置这些标准 Presence 设置。
步骤 5	导出用户联系人列表，第 305 页	完成此程序，以从当前群集导出迁移用户的联系人列表。
步骤 6	完成这些小的任务流程之一，以将用户移到新群集： • 通过 LDAP 迁移用户，第 305 页 • 手动将用户移到新群集，第 307 页 • 通过批量管理迁移用户，第 309 页	将用户移到新群集。 您可以使用 LDAP 在新群集中设置用户、手动移动用户，或使用批量管理将用户迁移到新群集。
步骤 7	在主群集上导入联系人列表，第 313 页	将用户迁移到新群集后，导入联系人列表以恢复迁移用户的联系人数据。
步骤 8	在旧群集中更新用户，第 314 页	在确认新群集中的所有事务一切正常之前，不要从旧群集中删除用户。 此程序用于使用批量管理的更新用户功能从旧群集中删除 IM and Presence 功能。

删除过期的条目

在迁移用户之前，删除过期的名录、组条目和不存在的联系记录。 此操作将在用户禁用在线状态的发布方 IM&P 节点上完成。

注释 如有必要，请在批处理 2000 中重复这些步骤。如果通过 CLI 删除大量过期条目时需要耗费很多时间，请在本部分结尾需要根访问时创建一个 TAC 案例以利用过期的名录脚本。

过程

步骤 1 启动 CLI 会话。 有关如何启动 CLI 会话的详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面参考指南》的“启动 CLI 会话”部分。

步骤 2 检查并删除过期的名录项。 要执行此操作，请运行以下查询：

a) 检查过期的名录项：

```
run sql select count(*) from rosters where user_id in (select xcp_user_id from enduser
where primarynodeid is NULL)
```

b) 删除过期的名录项：

```
run sql delete from rosters where pkid in (select * from (select first 2000 pkid from
rosters where user_id in (select xcp_user_id from enduser where primarynodeid is NULL)))
```

步骤 3 检查并删除过期的组记录。 要执行此操作，请运行以下查询：

a) 检查过期的组记录：

```
run sql select count(*) from groups where user_id in (select xcp_user_id from enduser
where primarynodeid is NULL)
```

b) 删除过期的组记录：

```
run sql delete from groups where pkid in (select * from (select first 2000 pkid from
groups where user_id in (select xcp_user_id from enduser where primarynodeid is NULL)))
```

步骤 4 检查并删除过期的非联系记录（按顺序）。 要执行此操作，请运行以下查询：

a) 检查过期的非联系记录（按顺序）：

```
run sql select count(*) from nonpresencecontacts where fkenduser in (select pkid from
enduser where primarynodeid is null)
```

b) 删除过期的非联系人记录（按顺序）：

```
run sql delete from nonpresencecontacts where pkid in (select * from (select first 2000
 pkid from nonpresencecontacts where fkenduser in (select pkid from enduser where
primarynodeid is null)))
```

c) 如果您有根访问权限，请使用此查询：

```
run sql delete from epascontactaddinfo where pkid in (select * from (select first 2000
pkid from epascontactaddinfo where pkid not in (select fkepascontactaddinfo from
nonpresencecontacts)))
```

为迁移配置标准 Presence

在迁移用户之前配置这些 Presence 设置。

过程

步骤 1 从 Cisco Unified CM IM and Presence 管理中，选择 **Presence** > **设置** > **标准配置**。

步骤 2 选中**允许用户查看其他用户的可用性而不收到批准提示**复选框。

步骤 3 对于**最大联系人列表大小(每用户)**设置，选中**无限制**复选框。

步骤 4 对于**查看器最大数(每用户)**设置，选中**无限制**复选框

步骤 5 单击**保存**。

下一步做什么

群集间同步错误检查，第 304 页

群集间同步错误检查

在迁移之前，确认不存在任何群集间同步错误。

过程

步骤 1 在 Cisco Unified CM IM and Presence 管理中选择**诊断** > **系统故障诊断程序**。

步骤 2 确认不存在任何群集间同步错误。 如果错误，请先更正再继续。

下一步做什么

为迁移启动基本服务，第 304 页

为迁移启动基本服务

在 Cisco Unified IM and Presence 功能配置中，确认以下基本迁移服务正在运行：

- Cisco AXL Web 服务
- Cisco 同步代理
- Cisco 群集间同步代理

过程

步骤 1 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 功能服务**。

步骤 2 从**服务器**下拉列表中选择您的 IM and Presence 节点，然后单击**前往**。

步骤 3 在**数据库和管理服务**下，确认 **Cisco AXL Web 服务**已启动。 如果服务未运行（默认设置是不运行），选择服务并单击**启动**。

步骤 4 选择**工具** > **控制中心 - 网络服务**。

步骤 5 从**服务器**下拉列表中选择您的 IM and Presence 节点，然后单击**前往**。

步骤 6 在 **IM and Presence Service** 下，确保**思科同步代理**和**思科群集间同步代理**服务均在运行。 如果它们没有运行，请立即**启动**。

下一步做什么

导出用户联系人列表，第 305 页

导出用户联系人列表

完成此程序，以从当前群集导出迁移用户的联系人列表。

过程

步骤 1 从当前主群集导出迁移用户的联系人列表。

a) 在 **Cisco Unified CM IM and Presence 管理**中，选择**批量管理** > **联系人列表** > **导出**。
b) 选择**群集中所有未分配的用户**并单击**查找**。
c) 查看结果，并根据需要使用 **AND/OR** 过滤器过滤搜索结果。
d) 完成列表后，单击**下一步**。
e) 为导出的联系人列表数据选择一个文件名。
f) （可选）更新“作业说明”。
g) 单击**立即运行**或计划稍后运行作业。

步骤 2 监控联系人列表导出作业的状态。

a) 在 **Cisco Unified CM IM and Presence 管理**中，选择**批量管理** > **任务调度**。
b) 单击**查找**列出所有 BAT 作业。
c) 查找您的联系人列表导出作业，当报告为已完成后，选择作业。
d) 选择“CSV 文件名”链接查看联系人列表导出文件的内容。 文件名中会附加一个时间戳。
e) 在**作业结果**部分，选择日志文件以查看已上传内容的摘要。 日志文件包括作业的开始和结束时间以及结果摘要。

步骤 3 当用户迁移完成后，下载并存储联系人列表导出文件，以供日后使用。

a) 在 **Cisco Unified CM IM and Presence 管理**中，选择**批量管理** > **上传/下载文件**。
b) 单击**查找**。
c) 选择联系人列表导出文件，并单击**下载选定项**。
d) 将 CSV 文件保存到本地，以供稍后上传使用。

下一步做什么

转到以下任务流程之一以在新群集中分配用户：

- 通过 LDAP 迁移用户 ， 第 305 页
- 手动将用户移到新群集 ， 第 307 页

通过 LDAP 迁移用户

如果您的用户与 LDAP目录同步并且您想要迁移到新群集，请完成以下任务。

注释 您必须将 LDAP 目录配置添加到新群集。 这包括任何服务配置文件、用户配置文件以及功能组模板。 确保您的功能组模板配置选中了**为 Unified CM IM and Presence 启用用户**复选框。

过程

	命令或操作	目的
步骤 1	更新外部 LDAP 目录， 第 306 页	如果您的部署是每个群集使用单独的 LDAP 结构，并且用户仅与其主群集同步，则可能需要更新外部 LDAP 目录。
步骤 2	在新群集中配置 LDAP， 第 307 页	如果 Cisco Unified Communications Manager 上启用了 LDAP，将新群集与更新的 LDAP 目录同步，从而将用户导入新群集。

下一步做什么

在主群集上导入联系人列表， 第 313 页

更新外部 LDAP 目录

如果您的部署是每个群集使用单独的 LDAP 结构，并且用户仅与其主群集同步，则可能需要更新外部 LDAP 目录。

注释 如果部署使用扁平的 LDAP 结构，即所有用户同步到所有 Cisco Unified Communications Manager 和 IM and Presence Service 群集（其中用户只许可到一个群集），则无需移动用户。

注释 根据您在旧群集和新群集中配置的 LDAP 目录同步方式，在外部 LDAP 目录中，移动用户可能会在下次同步时自动将这些用户迁移到新的 IM and Presence Service 群集。

过程

步骤 1 更新外部 LDAP 目录中的用户。

步骤 2 移动用户后，从旧 LDAP 群集中删除 LDAP 条目。

下一步做什么

在新群集中配置 LDAP， 第 307 页

在新群集中配置 LDAP

开始之前

在新群集中设置 LDAP 目录。 如果 LDAP 目录同步包括通用线路和设备模板以及功能组模板，则必须在新群集中配置这些模板。 请确保您的功能组模板选中以下选项：

- 主群集
- 为 Unified CM IM and Presence 启用用户

有关如何配置 LDAP 目录同步的详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》的“配置最终用户”部分。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统** > **LDAP** > **LDAP 目录**。

步骤 2 单击**查找**并选择配置的 LDAP 目录

步骤 3 单击**立即执行完全同步**。

下一步做什么

在主群集上导入联系人列表，第 313 页

手动将用户移到新群集

完成以下任务可手动将用户移到新群集。

注释 如果您有大量用户，可能需要使用 Cisco Unified Communications Manager 中的批量管理工具通过 csv 文件更新大量用户。 有关详细信息，请参阅《*Cisco Unified Communications Manager* 批量管理指南》。

过程

	命令或操作	目的
步骤 1	手动为用户禁用 IM and Presence，第 308 页	在迁移用户当前所在的主群集上对 IM and Presence Service 和 Cisco Jabber 禁用这些用户。
步骤 2	手动导入用户，第 308 页	如果未在新群集中配置 LDAP 同步，手动将用户设置到新的 Cisco Unified Communications Manager 群集。

	命令或操作	目的
步骤 3	在新群集上为 IM and Presence Service 启用用户，第 309 页	在新主群集上同步用户或手动配置用户后，必须为 IM and Presence Service 和 Cisco Jabber 启用用户。

下一步做什么

在主群集上导入联系人列表，第 313 页

手动为用户禁用 IM and Presence

以下步骤说明如何在当前主群集上禁用 IM and Presence Service 和 Cisco Jabber 的用户。

注释 如果同时迁移大量用户，可使用 Cisco Unified Communications Manager 中的批量管理工具。 有关详细信息，请参阅《*Cisco Unified Communications Manager* 批量管理指南》。

开始之前

导出用户联系人列表，第 305 页

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 使用过滤器查找您要为 IM and Presence 禁用的用户。

步骤 3 在**最终用户配置**屏幕中，取消选中**启用 Unified CM IM and Presence 的用户**。

步骤 4 单击**保存**。

下一步做什么

手动导入用户，第 308 页

手动导入用户

如果未在新群集中配置 LDAP 同步，手动将用户导入到新的 Cisco Unified Communications Manager 群集。

有关详细信息，请参阅配置用户设置，第 65 页。

下一步做什么

在新群集上为 IM and Presence Service 启用用户，第 309 页

在新群集上为 IM and Presence Service 启用用户

在新主群集上同步用户或手动配置用户后，必须为 IM and Presence Service 和 Cisco Jabber 启用用户。

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 使用过滤器查找您要为 IM and Presence Service 启用的用户。

步骤 3 在**最终用户配置**屏幕中，选中**为 IM and Presence 启用用户**。

步骤 4 单击**保存**。

步骤 5 在 Cisco Unified Communications Manager 上为电话和 CSF 部署用户。 有关详细信息，请参阅《*Cisco Unified Communications Manager* 管理指南》。

下一步做什么

在主群集上导入联系人列表，第 313 页

通过批量管理迁移用户

通过批量管理工具将用户移到新群集（例如，从群集 1 迁移到群集 2）。

开始之前

Cisco 批量设置服务必须在两个群集中运行。

注释 如果在 IM and Presence 群集中从来源移至目标的用户数量小于 100，请不要启动或停止思科群集间同步代理服务。

如果要从任何源/目标群集中移动 100 到 1,000 个用户，请在源群集和目标群集上都停止群集间同步代理服务，以执行以下步骤。

如果要移动的用户数量超过 1000，例如，如果必须移动 16K 用户，则首先按照以下步骤移动 8K 用户，并停止群集间同步代理服务，同时将用户移入 1K 用户块中。 稍后在 1K 用户块中以均衡和连续的顺序移动下一个 8K。

在要将用户从来源移动到的 IM and Presence 群集上：

步骤 1 在 IM and Presence 发布方 Presence 冗余组 (PRG) 对的关联订阅方节点上，停止群集间同步代理服务。

步骤 2 在 IM and Presence 发布方 Presence 冗余组对的发布方节点上，停止群集间同步代理服务。

在要将用户从目标移动到的 IM and Presence 群集上：

步骤 3 在发布方 Presence 冗余组对的辅助节点上，停止群集间同步代理服务。

步骤 4 在发布方 Presence 冗余组对的发布方节点上，停止群集间同步代理服务。

注释　任何其他群集节点都不需要停止群集间同步代理服务。

步骤 5 通过批量管理执行“迁移用户”中所述的步骤。

步骤 6 在目标群集和源群集上的 IM and Presence 发布方和订阅方节点上启动群集间同步代理服务。

步骤 7 所有其他群集可能需要长达 30 分钟的时间来完成与目标群集的同步。

过程

	命令或操作	目的
步骤 1	将用户导出到 CSV 文件，第 310 页	在初始群集（群集 1）中，将迁移用户导出到 CSV 文件。
步骤 2	下载 CSV 导出文件，第 311 页	下载 CSV 导出文件。
步骤 3	将 CSV 导出文件上传到新群集，第 311 页	将 CSV 文件上传到的目标群集（群集 2）。
步骤 4	配置用户模板，第 311 页	在目标群集中，使用用户设置配置用户模板。
步骤 5	将用户导入新群集，第 312 页	使用批量管理中的“插入用户”菜单从 CSV 文件导入用户。
步骤 6	通过批量管理验证迁移用户，第 312 页	通过批量管理验证用户迁移。

将用户导出到 CSV 文件

在初始群集中，使用批量管理工具将要迁移的用户导出到 CSV 文件。

注意：作业运行后，您可以转到“任务调度”检查作业的状态并确认文件已创建。 如果选择“稍后运行”，则可以使用“任务调度”设置作业的运行时间。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**批量管理** > **用户** > **导出用户**。

步骤 2 使用**过滤器**工具来搜索并选择要迁移的用户，然后单击**查找**。

步骤 3 单击**下一步**。

步骤 4 输入文件的**文件名**。
工具会在您文件的末尾附加 `.txt` 扩展名。 例如，`<csvfilename>.txt`。

步骤 5 从**文件格式**下拉列表中，选择导出文件的格式。

步骤 6 要立即运行作业，选择**立即运行**并单击**提交**。

下一步做什么

作业运行后，您可以转到**任务调度**检查作业的状态并确认文件已创建。 如果选择**稍后运行**，则可以使用“任务调度”设置作业的运行时间。

一旦确认文件已创建，下载 CSV 导出文件，第 311 页。

下载 CSV 导出文件

一旦您确认导出文件已创建，下载该文件。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**批量管理** > **上传/下载文件**。

步骤 2 单击**查找**。

步骤 3 选择已创建的文件，然后单击**下载选定项**。

步骤 4 下载文件。

下一步做什么

将 CSV 导出文件上传到新群集，第 311 页

将 CSV 导出文件上传到新群集

在目标群集（群集 2）中，上传您从群集 1 中导出的 csv 文件。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**批量管理** > **上传/下载文件**。

步骤 2 单击**新增**。

步骤 3 单击**选择文件**。 浏览并选择从其他系统导出的文件。

步骤 4 在**目标**下拉列表中选择您要用于导入文件内容的批量管理菜单。 例如，**用户**或**电话和用户**。

步骤 5 从**事务类型**下拉列表中，选择您要用于导入文件内容的子菜单。 例如，**插入用户**或**插入电话/用户**。

步骤 6 单击**保存**。

下一步做什么

配置用户模板，第 311 页

配置用户模板

在目标群集中，使用要应用于导入用户的设置配置用户模板。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**批量管理** > **用户** > **用户模板**。

步骤 2 执行以下任一操作：

- 单击**查找**并选择现有模板。
- 单击**新增**以创建新的模板。

步骤 3 配置您要应用到导入用户的用户设置。 例如，确保以下字段已选中

- **主群集**
- **为 Unified CM IM and Presence 启用用户**

步骤 4 如果您希望启用用户以便与 Microsoft Outlook 集成日历，选中**在 Presence 中包含会议信息**复选框。

步骤 5 配置任何剩余的字段。

步骤 6 单击**保存**。

下一步做什么

将用户导入新群集，第 312 页

将用户导入新群集

使用批量管理的“插入用户”菜单可将导出的用户导入到新群集。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**批量管理** > **用户** > **插入用户**。

步骤 2 从**文件名**中选择要从其他系统导出的文件。

步骤 3 从**用户模板名**中选择您刚刚创建的用户模板。

步骤 4 选中**使用导出用户创建文件**复选框。

步骤 5 选中**立即运行**，然后单击**提交**。

下一步做什么

在主群集上导入联系人列表，第 313 页

通过批量管理验证迁移用户

在通过批量管理迁移用户并在源和目标群集上启动思科群集间同步代理服务后，有必要验证除源群集和目标群集以外的其他群集是否收到了发生用户移动的通知。

所有其他群集最多需要 30 分钟才能完成与目标群集的同步。 在等待期间，您可以打开与不属于更改（源或目标）的示例 (5) IMP 发布方的终端会话，以监控思科系统日志。

过程

步骤 1 运行以下命令以观察示例 IMP 发布方节点是否在通过批量管理迁移用户，并在源群集和目标群集上启动思科群集间同步代理服务之后完成其同步。 通知此时的时间戳。 在以下示例语法中，目标群集名称为 dst-name。 将其替换为您的目标群集名称。

```
admin:file search activelog syslog/CiscoSyslog ".*InterClusterSyncAgentStatus:.*dst-name.*"
```

步骤 2 如果处于 ICSA 状态的时间戳不早于记录的时间戳，则使用以下命令最多 30 分钟以成功进行同步：

```
admin:file tail activelog syslog/CiscoSyslog regexp
".*InterClusterSyncAgentStatus:.*dst-name.*"
```

如果您在选定的示例群集/节点上看到 ICSA 同步失败的状态警报，请等待 5-10 分钟以获取同步成功的状态警报。 ICSA 将每 5 分钟重试一次。 如果没有同步成功的警报或者持续同步失败，请创建 TAC 案例。

此时，如果当前时间比通过批量管理迁移用户并在源和目标群集上启动思科群集间同步代理服务后记录的时间戳晚 30 分钟，则您已验证了 5 个远程样本群集。 现在，您可以继续执行下一个移动过程；如果没有其他移动，则操作完成。

在主群集上导入联系人列表

将用户迁移到新群集后，导入联系人列表以恢复迁移用户的联系人数据。

过程

步骤 1 上传以前导入的联系人列表 CSV 文件。

a) 在 **Cisco Unified CM IM and Presence 管理**中，选择**批量管理** > **上传/下载文件**。
b) 单击**新增**。
c) 单击**浏览**查找并选择联系人列表 CSV 文件。
d) 选择**联系人列表**作为“目标”。
e) 选择**导入用户的联系人 – 自定义文件**作为“事务类型”。
f) （可选）选中**如果文件已存在，则覆盖该文件**。
g) 单击**保存**上传该文件。
h) 单击**保存**上传该文件。

步骤 2 运行导入联系人列表作业。

a) 在 **Cisco Unified CM IM and Presence 管理**中，选择**批量管理** > **联系人列表** > **更新**。
b) 选择您在步骤 1 上传的 CSV 文件。
c) （可选）更新“作业说明”。

d) 要立即运行作业，请单击**立即运行**。 单击**稍后运行**安排稍后进行更新。
e) 单击**提交**。

步骤 3 监控联系人列表导入状态

a) 在 **Cisco Unified CM IM and Presence 管理**中，选择**批量管理** > **联系人列表** > **任务调度**。
b) 单击**查找**列出所有 BAT 作业。
c) 联系人列表导入作业的状态显示为完成时，选择该作业的作业 ID。
d) 要查看联系人列表文件的内容，请选择 **CSV 文件名**中列出的文件。
e) 单击**记录文件名**链接即可打开日志。

其中列出了作业的开始和结束时间，并会显示结果摘要。

在旧群集中更新用户

在确认新群集中的所有事务一切正常之前，不要从旧群集中删除用户。 此程序用于使用批量管理的更新用户功能从旧群集中删除 IM and Presence 功能。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**批量管理** > **用户** > **更新用户** > **查询**。

步骤 2 使用过滤器工具搜索迁移用户。 例如，您可以搜索满足此条件的所有用户：**已启用 IM and Presence**。

步骤 3 单击**下一步**。

步骤 4 对于以下两个字段中的每个字段，请选中最左侧的框，并取消选中右侧相邻的框。 左侧框表示您要更新字段，右侧框表示新设置：未选中。

- **主群集**
- **为 Unified CM IM and Presence 启用用户**

步骤 5 在**作业信息**下选择**立即运行**。

步骤 6 单击**提交**。

下一步做什么

一旦您确信迁移有效，并且在新群集中正确配置了所有用户，就可以删除旧群集中的迁移用户。

第 29 章

管理区域设置

- 管理区域设置概述， 第 315 页
- 管理区域设置前提条件， 第 316 页
- 在 IM and Presence Service 上安装区域设置安装程序， 第 316 页

管理区域设置概述

您可以配置 Cisco Unified Communications Manager 和 IM and Presence Service 支持多种语言。 可以安装的支持语言数目没有限制。

思科在 www.cisco.com 上提供区域设置特定版本的 Cisco Unified Communications Manager 区域设置安装程序和 IM and Presence Service 区域设置安装程序。 区域设置安装程序由系统管理员安装，当用户使用支持的界面时，它允许用户查看/接收所选的翻译文本或音频（如果适用）。

升级 Cisco Unified Communications Manager 或 IM & Presence 服务后，必须重新安装所有区域设置。安装与 Cisco Unified Communications Manager 节点或 IM and Presence Service 节点的 major.minor 版本号匹配的最新版本的区域设置。

当您在群集中的每个节点上安装 Cisco Unified Communications Manager 并设置数据库后，请安装区域设置。 如果要在 IM and Presence Service 节点上安装特定的区域设置，必须首先在 Cisco Unified Communications Manager 群集上安装相同国家/地区的 Cisco Unified Communications Manager 区域设置文件。

完成软件升级后，使用以下各节中的信息在 Cisco Unified Communications Manager 节点和 IM and Presence Service 节点上安装区域设置。

用户区域设置

用户区域设置文件包含特定语言和国家/地区的语言信息。 它们以用户所选的区域设置为电话显示屏、用户应用程序和用户网页提供翻译的文本和语音提示（如果可用）。 这些文件使用以下命名约定：

- cm-locale-language-country-version.cop (Cisco Unified Communications Manager)
- ps-locale-language_country-version.cop (IM and Presence Service)

如果您的系统仅需要用户区域设置，在安装 CUCM 区域设置后安装它们。

网络区域设置

网络区域设置文件提供适用于各种网络项目（包括电话音频、信号器和网关音频）的国家/地区特定文件。 组合的网络区域设置文件使用以下命名约定：

- cm-locale-combinednetworklocale-version.cop (Cisco Unified Communications Manager)

思科可能会在一个区域设置安装程序中组合多个网络区域设置。

注释 思科认可、客户提供的服务器上的 Cisco Unified Communications Manager 和 IM and Presence Service 可以支持多个区域设置。 安装多个区域设置安装程序可确保用户能够从众多区域设置进行选择。

您可以使用与安装软件升级相同的过程从本地或远程源安装区域设置文件。 您可以在群集中的每个节点上安装多个区域设置文件。 更改不会生效，直到您重新启动群集中的每个节点。 思科强烈建议您不要重新启动节点，直到在群集中的所有节点上安装所有区域设置。 通过在正常上班时间后重新启动节点，将呼叫处理中断减至最少。

管理区域设置前提条件

区域设置安装注意事项

- 在安装区域设置之前，安装所有 Cisco Unified Communications Manager 和 IM and Presence Service 群集节点并设置数据库。
- 如果要在 IM and Presence Service 节点上安装特定的区域设置，必须首先在 Cisco Unified Communications Manager 群集上安装相同国家/地区的 Cisco Unified Communications Manager 区域设置文件。
- 您可以在群集中的每个节点上安装多个区域设置文件。 要激活新的区域设置，您必须在安装后重新启动群集中的每个节点。
- 您可以使用与安装软件升级相同的过程从本地或远程源安装区域设置文件。 有关从本地或远程源升级的详细信息，请参阅《*Cisco Unified Communications Manager* 升级指南》。

在 IM and Presence Service 上安装区域设置安装程序

- 安装 IM and Presence Service 的区域设置之前，先在 Cisco Unified Communications Manager 上安装区域设置安装程序。 如果要使用“英语”以外的区域设置，则必须在 Cisco Unified Communications Manager 及 IM and Presence Service 上安装适当的语言安装程序。

- 如果您的 IM and Presence Service 群集有多个节点，请确保在群集中的每个节点上安装区域设置安装程序（先在 IM and Presence 数据库发布方节点上安装，然后在订户节点上安装）。
- 在两个系统上加载所有适用的区域设置安装程序前，不应配置用户区域设置。 如果用户在区域设置安装程序加载到 Cisco Unified Communications Manager 之后但尚未加载到 IM and Presence Service 时不小心设置了用户区域设置，可能会出现问题。 如果接到问题报告，我们建议您通知每位用户进入 Cisco Unified Communications Self Care 门户网站，将区域设置从当前设置更改为英语，然后再更改回合适的语言。 您也可以使用 BAT 工具将用户区域设置同步到合适的语言。

过程

步骤 1 导航到 `cisco.com` 并为您版本的 IM and Presence Service 选择区域设置安装程序。
http://software.cisco.com/download/navigator.html?mdfid=285971059

步骤 2 单击适合您工作环境的 IM and Presence 区域设置安装程序的版本。

步骤 3 下载文件后，将文件保存至硬盘驱动器，并注意保存文件的位置。

步骤 4 将此文件复制到支持 SFTP 的服务器。

步骤 5 使用管理员帐户和密码登录 Cisco Unified IM and Presence 操作系统管理。

步骤 6 选择**软件升级** > **安装/升级**。

步骤 7 选择“远程文件系统”作为软件位置源。

步骤 8 在“目录”字段中输入文件位置，如 `/tmp`。

步骤 9 在“服务器”字段中输入 IM and Presence Service 的服务器名称。

步骤 10 在“用户名称”和“用户密码”字段中输入您的用户名和密码凭证。

步骤 11 对“传输”协议选择 SFTP。

步骤 12 单击**下一步**。

步骤 13 从搜索结果列表中选择 IM and Presence Service 区域设置安装程序。

步骤 14 单击**下一步**加载安装程序文件并进行验证。

步骤 15 完成区域设置安装后，重新启动群集中的每个服务器。

步骤 16 已安装区域设置的默认设置为“English, United States”。 在 IM and Presence Service 节点重新启动时，更改浏览器的语言（如有必要）以匹配您下载的安装程序的区域设置。

步骤 17 确认您的用户可为受支持的产品选择区域设置。

提示 确保在群集中的每个服务器上安装相同的组件。

错误消息区域设置参考

请参阅下表，以了解区域设置安装程序激活期间可能出现的消息的说明。 如果出现错误，您可以查看安装日志中的消息。

表 *37:* 区域设置安装程序消息和说明

消息	说明
[LOCALE] 找不到文件：<language>_<country>_user_locale.csv，用户区域设置尚未添加到数据库。	当系统无法找到CSV文件（其中包含要添加到数据库的用户区域设置信息）时发生此错误。这表示构建过程出错。
[LOCALE] 找不到文件：<country>_network_locale.csv，网络区域设置尚未添加到数据库。	当系统无法找到CSV文件（其中包含要添加到数据库的网络区域设置信息）时发生此错误。这表示构建过程出错。
[LOCALE] CSV 文件安装程序 installdb 不存在或不可执行。	必须确保应用程序 installdb 存在。 它读取 CSV 文件包含的信息并将其正确应用到目标数据库。如果找不到该应用程序，可能是没有通过 Cisco Unified Communications 应用程序安装（不太可能）、已删除（很有可能）或节点没有 Cisco Unified Communications 应用程序，例如 Cisco Unified Communications Manager 或 IM and Presence Service（最有可能）。 区域设置安装将终止，因为如果数据库中的记录不正确，区域设置将不起作用。
[LOCALE] 无法创建 /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_<ll>_<CC>.properties.Checksum。 [LOCALE] 无法创建 /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum。 [LOCALE] 无法创建 /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum。 [LOCALE] 无法创建 /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt.Checksum。	当系统无法创建校验和文件（原因是Java可执行文件 `/usr/local/thirdparty/java/j2sdk/jre/bin/java` 缺失、Java 存档文件 `/usr/local/cm/jar/cmutil.jar` 缺失或损坏，或者 Java 类 `com.cisco.ccm.util.Zipper` 缺失或损坏），就可能发生这些错误。 即使发生这些错误，区域设置仍将继续正常工作；Cisco Unified Communications Manager Assistant 除外，因为它无法检测本地化 Cisco Unified Communications Manager Assistant 文件中的更改。
[LOCALE] 找不到 /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt 来更新 Unified CM Assistant 区域设置信息。	当系统在正确位置找不到文件（很可能是由于构建过程出错）时，就会发生此错误。
[LOCALE] 添加 <locale-installer-file-name> 到数据库失败！	发生此错误是由于安装区域设置时出现任何故障的共同结果；它表示终止条件。

消息	说明
[LOCALE] 找不到 <locale-installer-file-name>	系统在升级过程中不会迁移此区域设置。 已下载的区域设置安装程序文件不再位于下载位置。 平台可能已将其移动或删除。 这不是严重错误，表示在 Cisco Unified Communications 应用程序升级后，您需要重新应用区域设置安装程序或者下载并应用新的区域设置安装程序。
[LOCALE] 无法将 <locale-installer-file-name> 复制到迁移路径。 此区域设置在升级过程中不会迁移！	您无法将下载的区域设置安装程序文件复制到迁移路径。 这不是严重错误，表示在 Cisco Unified Communications 应用程序升级后，您需要重新应用区域设置安装程序或者下载并应用新的区域设置安装程序。
[LOCALE] DRS 取消注册失败	区域设置安装程序无法从灾难恢复系统取消注册。 备份或恢复记录不会包含区域设置安装程序。 记录安装日志并联系 Cisco TAC。
[LOCALE] 备份失败！	灾难恢复系统无法从下载的区域设置安装程序文件创建 tarball。 在尝试备份之前重新应用区域设置安装程序。 **注释** 在系统恢复后手动重新安装区域设置可达到同样的目标。
[LOCALE] 在恢复的 tarball 中找不到 COP 文件！	备份文件的损坏可能导致无法成功提取区域设置安装程序文件。 **注释** 手动重新应用区域设置安装程序将会完全恢复区域设置。
[LOCALE] 无法成功重新安装 COP 文件！	备份文件的损坏可能导致区域设置安装程序文件损坏。 **注释** 手动重新应用区域设置安装程序将会完全恢复区域设置。
[LOCALE] 无法构建脚本来重新安装 COP 文件！	平台无法动态创建用于重新安装区域设置的脚本。 **注释** 手动重新应用区域设置安装程序将会完全恢复区域设置。 记录安装日志并联系 TAC。

本地化应用程序

IM and Presence Service 应用程序支持多种不同的语言。 请参阅下表，了解已本地化的应用程序和可用语言的列表。

表 *38:* 已本地化的应用程序和支持的语言列表

界面	支持的语言
管理应用	
Cisco Unified CM IM and Presence 管理	中文（中国）、英语、日语（日本）、韩语（韩国）
Cisco Unified IM and Presence 操作系统	中文（中国）、英语、日语（日本）、韩语（韩国）

第 30 章

管理服务器

- 管理服务器概述， 第 321 页
- 更改服务器地址， 第 321 页
- 从群集中删除 IM and Presence 节点 ， 第 322 页
- 将已删除的服务器重新添加到群集， 第 322 页
- 安装前将节点添加到群集， 第 323 页
- 查看 Presence 服务器状态， 第 324 页
- 通过高可用性重新启动服务， 第 324 页
- 主机名配置， 第 325 页

管理服务器概述

本章主要介绍如何为已部署的系统编辑服务器详细信息。 包括将新节点分配给群集、从群集中删除节点、查看在线状态和更改服务器地址详细信息。

更改服务器地址

如果您有一个正在运行的系统，并且需要对服务器寻址进行以下任何更改，请参阅文档《更改 *Cisco Unified Communications Manager* 和 *IM and Presence Service* 的 *IP* 地址和主机名》中的步骤，网址：https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

这适用于以下类型的地址变更：

- 更改服务器 IP 地址
- 更改服务器主机名
- 更改节点名称（例如，如果您使用 IP 地址来定义节点名称，而您希望使用主机名）。
- 为 IM and Presence Service 配置默认域

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 322 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。

通过高可用性重新启动服务

如果进行任何系统配置更改或系统升级时需要禁用高可用性，然后重新启动 Cisco XCP 路由器、Cisco Presence Engine 或服务器本身，必须留出足够的时间在启用高可用性之前重新创建 Cisco Jabber 会话。 否则，Presence 将不适用于未创建会话的 Jabber 客户端。

确保按照以下步骤操作：

过程

步骤 1 进行任何更改之前，检查 Cisco Unified CM IM and Presence 管理窗口（**系统** > **Presence 拓扑**）的 **Presence 拓扑**窗口。 记录每个 Presence 冗余组中每个节点的已分配用户数。

步骤 2 在每个 Presence 冗余组中禁用高可用性，并等待至少两分钟以使新的高可用性设置同步。

步骤 3 为您的更新执行以下任一必要操作：

- 重新启动 Cisco XCP 路由器
- 重新启动 Cisco Presence Engine
- 重新启动服务器

步骤 4 重新启动后，监控所有节点上的活动会话数。

步骤 5 对于每个节点，在每个节点上运行 `how perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI 命令，以确认每个节点上的活动会话数。 活动会话数应与您在步骤 1 中为分配的用户记录的数量相匹配。 所有会话恢复用时应该不会超过 15 分钟。

步骤 6 创建所有会话后，您可以在 Presence 冗余组中启用高可用性。

注释 如果 30 分钟过去且尚未创建活动会话，重新启动 Cisco Presence Engine。 如果这样不起作用，可能存在亟待解决的较大系统问题。

注释 建议不要背靠背重启 Cisco XCP 路由器和/或 Cisco Presence Engine。 但是，如果确实需要重新启动：重新启动第一个服务，等待重新创建所有 JSM 会话。 当所有 JSM 会话创建完成之后，执行第二个重新启动。

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 *39: 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。

第 31 章

备份系统

- 备份概述，第 327 页
- 备份前提条件，第 329 页
- 备份任务流程，第 330 页
- 备份相互作用和限制，第 335 页

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 *40: 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 *41: 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 335 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 330 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 331 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 332 页 • 开始手动备份 ，第 333 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 334 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 334 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 331 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 332 页
- 开始手动备份，第 333 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 330 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 331 页
- （可选） 查看当前备份状态，第 334 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 330 页
- 估算备份文件的大小，第 331 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 334 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 334 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 ，第 335 页

备份限制

以下限制适用于备份：

表 *42:* 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 Cisco Unified Communications Manager群集节点之间的数据。DRS 使用 IPsec 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 IPSEC 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 IPSEC-信任文件，必须确保将 IPSEC 证书上传到 IPSEC-信任。有关详细信息，请参阅《*Cisco Unified Communications Manager* 安全指南》中的“证书管理”部分，该文档位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

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 *43: 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 32 章

恢复系统

- 恢复概述， 第 339 页
- 恢复前提条件， 第 340 页
- 恢复任务流程， 第 341 页
- 数据验证， 第 349 页
- 警报和消息， 第 351 页
- 恢复相互作用和限制， 第 353 页
- 故障诊断， 第 354 页

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**修复所有禁用的服务器**。

   此时将显示 **SAML 单点登录配置**窗口；单击**下一步**。
3. 单击**运行 SSO 测试**。
4. 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 341 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 343 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344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 345 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 347 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 347 页	使用此程序重新启动节点。
步骤 7	检查恢复作业状态，第 348 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 349 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 348 页
- 要重新启动节点，请参阅 重新启动节点，第 347 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 348 页
- 要重新启动节点，请参阅 重新启动节点 ，第 347 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 341 页和恢复后续群集节点，第 343 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 341 页和恢复后续群集节点，第 343 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 348 页
- 要重新启动节点，请参阅 重新启动节点，第 347 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 348 页

- 要重新启动节点，请参阅 重新启动节点，第 347 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 348 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 *44:* 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 *45:* 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，该组件没有得
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。 DR Agent 无法连接到 Master Agen
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

恢复相互作用和限制

恢复限制

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 *46:* 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 Cisco Unified Communications Manager，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。

限制	说明
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 Unified Communications Manager* 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 DRS 备份/还原是一个高度面向 CPU 的过程。 智能许可证管理器是备份和恢复的组件之一。 在此过程中，智能许可证管理器服务会重新启动。 资源利用率预期会很高，因此建议将此过程安排在维护期间完成。

成功恢复 Cisco Unified Communications 服务器组件后，向 Cisco Smart Software Manager 或 Cisco Smart Software Manager 卫星注册 Cisco Unified Communications Manager。 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。

有关如何使用 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 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 33 章

联系人列表的批量管理

- 批量管理概述，第 355 页
- 批量管理前提条件，第 355 页
- 批量管理任务流程，第 356 页

批量管理概述

使用 IM and Presence Service 批量管理工具，您可以对许多 IM and Presence Service 用户执行批量事务，包括：

- 重命名用户联系人 ID 以在 Microsoft 迁移过程中使用。
- 将属于特定节点或 Presence 冗余组的用户的联系人列表、非 Presence 联系人列表和位置详细信息导出到 CSV 数据文件。

注释 非 Presence 联系人都没有 IM 地址，并且只能通过此程序导出。

- 您可以导入已导出到不同群集中的另一个节点或Presence冗余组的用户联系人列表、非Presence联系人列表和用户位置迁移详细信息。 为新用户预填联系人列表或添加到现有联系人列表。
- 这些功能简化了群集之间的用户迁移。

批量管理前提条件

在导入用户联系人列表之前：

1. 在 Cisco Unified Communications Manager 上部署用户。
2. 确保在 Cisco Unified Communications Manager 上为 IM and Presence Service 许可用户。

注释 默认联系人列表导入速度取决于虚拟机部署硬件类型。 可以选择 **Cisco Unified CM IM and Presence 管理** > **系统** > **服务参数** > **Cisco 批量部署服务**来更改联系人列表导入速度。 但是，如果您增大默认导入速度，将会在 IM and Presence Service 上消耗更多的 CPU 和内存。

批量管理任务流程

过程

	命令或操作	目的
步骤 1	批量重命名用户联系人 ID， 第 356 页	上传 CSV 文件并重命名用户列表的联系人 ID。
步骤 2	批量导出用户联系人列表和非 Presence 联系人列表， 第 358 页	此程序用于将用户的联系人列表导出到 CSV 文件。 然后，您可以使用批量管理将用户联系人列表移到另一个节点或群集。
步骤 3	批量导出用户位置详细信息 ， 第 358 页	此程序用于将用户位置详细信息导出到 CSV 文件。 然后，您可以使用批量管理将用户位置详细信息列表移到另一个节点或群集。
步骤 4	完成以下任务以将用户联系人列表导入 IM and Presence Service： • 验证最大联系人列表大小， 第 361 页 • 上传输入文件， 第 362 页 • 新建批量管理作业， 第 366 页 • 检查批量管理作业的结果， 第 367 页	

批量重命名用户联系人 ID

注意 批量重命名联系人 ID 操作在将用户从 Microsoft 服务器（如 Lync）迁移到 IM and Presence Service 的时候使用。 有关如何在用户迁移过程中使用此工具的详细说明，请参阅 Cisco.com 上的《分区式域内联合指南》。 任何其他情形均不支持使用此工具。

上传 CSV 文件并重命名用户列表的联系人 ID。

过程

步骤 1 上传包含了您希望在所有联系人列表中重命名的联系人 ID 列表的 CSV 文件。

a) 转到 IM and Presence Service 数据库发布方节点。
b) 在 **Cisco Unified CM IM and Presence 管理**中，选择**批量管理** > **上传/下载文件**。
c) 单击**新增**。
d) 单击**浏览**找到并选择 CSV 文件。 有关输入文件的更多信息，请参阅批量重命名用户联系人 ID 文件详细信息，第 357 页。
e) 选择**联系人**作为“目标”。
f) 选择**重命名联系人 – 自定义文件**作为“事务类型”。
g) 单击**保存**上传该文件。

步骤 2 在发布方节点的 **Cisco Unified CM IM and Presence 管理**中，选择**批量管理** > **联系人列表** > **重命名联系人**。

步骤 3 在**文件名**字段中，选择您要上传的文件。

步骤 4 选择如下操作之一：

- 单击**立即运行**，以立即执行批量管理作业。
- 单击**稍后运行**，以安排执行批量管理作业的时间。 有关在批量管理工具中安排作业的详细信息，请参阅 Cisco Unified CM IM and Presence 管理中的在线帮助。

步骤 5 单击**提交**。

如果选择立即运行作业，将在您单击“提交”后运行作业。

下一步做什么

批量导出用户联系人列表和非 Presence 联系人列表，第 358 页

批量重命名用户联系人 ID 文件详细信息

您在运行此作业之前上传的文件必须是以下格式的 CSV 文件：

<Contact ID>、<New Contact ID>

其中 <Contact ID> 是现有的联系人 ID，而 <New Contact ID> 是联系人 ID 的新格式。

<Contact ID> 是在 **Presence 拓扑用户分配窗口**上显示的用户 IM 地址。

下面是 CSV 文件示例，有一个条目：

```
Contact ID, New Contact ID
john.smith@example.com, jsmith@example.com
```

批量导出用户联系人列表和非 Presence 联系人列表

此程序用于将用户的联系人列表导出到CSV文件。 然后，您可以使用批量管理将用户联系人列表移到另一个节点或群集。

- 联系人列表 — 此列表包含 IM and Presence 联系人。 没有 IM 地址的联系人将不会导出（您必须导出非 Presence 联系人列表）。
- 非 Presence 联系人列表 — 此列表包含没有 IM 地址的联系人。

过程

步骤 1 在 Cisco Unified CM IM and Presence 管理中，执行以下任一操作：

- 要导出联系人列表，选择**批量管理** > **联系人列表** > **导出联系人列表**
- 要导出非 presence 联系人列表，选择**批量管理** > **非 presence 联系人列表** > **导出非 Presence 联系人列表**并跳过下一个步骤。

步骤 2 仅联系人列表。 选择要导出其联系人列表的用户：

a) 在**导出联系人列表选项**下，选择要导出其联系人列表的用户的类别。 默认是导出所有用户的联系人列表。

b) 单击**查找**以显示用户列表，然后单击**下一步**。

步骤 3 在**文件名**字段中，输入 CSV 文件的名称。

步骤 4 在**作业信息**下，配置要运行此作业的时间：

- **立即运行** — 如果选中此按键，联系人列表会立即导出。
- **稍后运行** — 如果要安排作业的运行时间，选中此按键。 如果选择此选项，您将需要在任务调度页面（**批量管理** > **任务调度**）安排此作业运行的时间。

步骤 5 单击**提交**。

如果您选择**立即运行**，导出作业会立即运行。

步骤 6 在创建导出文件后，下载导出的文件：

a) 在 Cisco Unified CM IM and Presence 管理中，选择**批量管理** > **上传/下载文件**。

b) 单击**查找**并选择导出文件。

c) 单击**下载选定项**并将文件下载到您可以访问的位置。

批量导出用户位置详细信息

此程序用于将用户位置详细信息导出到CSV文件。 然后，您可以使用批量管理将用户位置详细信息移到另一个节点或群集。

过程

步骤 1 在 Cisco Unified CM IM and Presence 管理中，选择**批量管理** > **用户位置迁移** > **导出用户位置详细信息**。

步骤 2 在**用户位置详细信息导出**下的**文件名**字段中，输入 CSV 文件的名称。

步骤 3 在**作业信息**下，配置要运行此作业的时间：

- **立即运行**—选中此按键可立即导出用户位置详细信息。
- **稍后运行** — 如果要安排作业的运行时间，选中此按键。 如果选择此选项，您将需要在**批量管理** > **任务调度**中的**任务调度**页面安排此作业运行的时间。

步骤 4 单击**提交**。
如果选择**立即运行**，会立即执行导出作业。

步骤 5 在创建导出文件后，下载导出的文件：

a) 在 Cisco Unified CM IM and Presence 管理中，选择**批量管理** > **上传/下载文件**。
b) 单击**查找**并选择导出文件。
c) 单击**下载选定项**并将文件下载到您可以访问的位置。

导出联系人列表文件详细信息

以下是 CSV 文件示例条目：

```
userA,example.com,userB,example.com,buddyB,General,0
```

BAT 允许您查找和选择要导出其联系人列表的用户。 用户联系人列表将导出为格式如下的 CSV 文件：

```
<User ID>、<User Domain>、<Contact ID>、<Contact Domain>、<Nickname>、<Group Name>、<State>
```

下表介绍了导出文件中的参数。

参数	说明
用户 ID	IM and Presence Service 用户的用户 ID。 **注释** 此值是用户 IM 地址的用户部分。
用户域名	IM and Presence Service 用户的 Presence 域名。 **注释** 此值是用户 IM 地址的域名部分。 **示例 1**：bjones@example.com—bjones 是用户 ID，example.com 是用户域。 **示例 2**：bjones@usa@example.com—bjones@usa 是用户 ID，example.com 是用户域。
联络人 ID	联系人列表条目的用户 ID。

参数	说明
联系人域名	联系人列表条目的 Presence 域名。
Nickname	联系人列表条目的昵称。 如果用户未为联系人指定昵称，则“昵称”参数将为空。
组名称	要添加联系人列表条目的组的名称。 如果用户的联系人未分类到组中，默认组名将在“组名”字段中指定。
状态	名录的状态，名录数据库以十进制格式存储它。

导出非 Presence 联系人列表文件详细信息

非 Presence 用户联系人列表将导出为格式如下的 CSV 文件：

```
<User JID>、<Contact JID>、<Group Name>、<Content Type>、<Version>、<Info>
```

下表介绍了导出文件中的参数：

参数	说明
用户 JID	用户 JID。 这是用户的 IM 地址。
联系人 JID	联系人列表条目的用户 JID（如果可用），否则为 UUID。
组名称	要添加联系人列表条目的组的名称。
内容类型	信息字段中使用的 textmime 类型和子类型。
版本	信息字段中使用的内容类型。
信息	vCard 格式的联系人列表条目的联系信息。

以下是 CSV 文件示例条目：

```
user2@cisco.com,ce463d44-02c3-4975-a37f-d4553e3f17e1,group01,text/directory,3,BEGIN:VCARD
ADR;TYPE=WORK:ADR\;WORK:\;\;123 Dublin rd\,\;Oranmore\;Galway\;\;Ireland
EMAIL;TYPE=X-CUSTOM1;X LABEL=Custom:testuser01@test.com N:test;user;;; NICKNAME:pizzaguy01
ORG:ABC TEL;TYPE=WORK,VOICE:5323534535 TITLE:QA VERSION:3.0 END:VCARD
```

导出用户位置详细信息的文件详细信息

用户位置详细信息将导出为格式如下的 CSV 文件：

```
<User JID>、<Access Type>、<Create Time>、<Item ID>、<Resource ID>、<Message Text>
```

注意 由于文件本身的大小以及存在损坏用户位置信息的风险，我们建议您不要手动修改导出的 CSV 文件。

下表介绍了导出文件中的参数：

参数	说明
用户 JID	用户 JID。 这是用户的 IM 地址。
访问类型	访问类型定义用户的访问类型。 访问类型的值如下： • W：白名单 • R：名录组 • O：开放 **注释** 对 Jabber 使用 'W'。
创建时间	“创建时间”显示项目创建或更新的日期和时间。
项目 ID	“项 ID”标识用户的特定记录。
资源 ID	“资源 ID”是 Jabber 实例 ID。
消息文本	“消息文本”是用户的位置信息。

以下是 CSV 文件示例条目：

```
userA@example.com,W,2021-01-22
10:11:18.000001,7d0ec34c-458f-4fd2-9d15-58accac4af00,jabber_7151,

<geoloc
xmlns='http://jabber.org/protocol/geoloc'><description>newlocation104</description><street>104</street><mobile>0</mobile><enable>1</enable></geoloc>
```

批量导入用户联系人列表

验证最大联系人列表大小

检查 IM and Presence Service 上的“最大联系人列表大小”和“最大查看器数”设置。 “最大联系人列表大小”的系统默认值为 200，“最大查看器数”的系统默认值为 200。

思科建议导入用户联系人列表时将“最大联系人列表大小”和“最大查看器数”设置设为“无限制”。 即使在使用 BAT 导入联系人列表时超过最大联系人列表大小而未丢失数据，此步骤也可确保完全导入每个迁移用户的联系人列表。 迁移所有用户后，您可以将“最大联系人列表大小”和“最大查看器数”设置重置为首选值。

您只需在群集上检查最大联系人列表大小（这些群集包含希望要对其导入联系人的用户）。 更改 Presence 设置时，更改会应用到群集中的所有节点；因此您只需在群集中的 IM and Presence 数据库发布方节点上更改这些设置。

下一步做什么

上传输入文件，第 362 页

上传输入文件

以下程序介绍如何使用 BAT 上传联系人列表和非 Presence 联系人列表的 CSV 输入文件。

开始之前

验证最大联系人列表大小，第 361 页

过程

步骤 1 在 **Cisco Unified CM IM and Presence** 管理中，选择**批量管理** > **上传/下载文件**。

步骤 2 单击**新增**。

步骤 3 单击**浏览**找到并选择 CSV 文件。

步骤 4 对于目标设置：

- 如果您想要上传联系人列表的输入文件，选择**联系人列表**。 有关用户联系人列表输入文件的详细信息，请参阅导入联系人列表文件详细信息，第 362 页。
- 如果您想要上传非 Presence 联系人列表的输入文件，选择**非 Presence 联系人列表**。 有关非 Presence 用户联系人列表输入文件的详细信息，请参阅导入非 Presence 联系人列表文件详细信息，第 364 页。
- 如果要上传用户位置迁移详细信息的输入文件，请选择**用户位置迁移**。 有关用户位置详细信息输入文件的详细信息，请参阅导入用户位置详细信息的文件详细信息，第 365 页。

步骤 5 对于事务类型：选择作为事务类型。

- 如果您想要上传联系人列表的输入文件，选择**导入用户的联系人 – 自定义文件**。
- 如果您想要上传非 Presence 联系人列表的输入文件，选择**导入用户的非 Presence 联系人**
- 如果要上传用户位置迁移详细信息的输入文件，请选择**导入用户位置详细信息**

步骤 6 单击**保存**上传该文件。

下一步做什么

新建批量管理作业，第 366 页

导入联系人列表文件详细信息

输入文件必须是采用以下格式的 CSV 文件：

<User ID>、<User Domain>、<Contact ID>、<Contact Domain>、<Nickname>、<Group Name>、<State>

以下是 CSV 文件示例条目：

```
userA,example.com,userB,example.com,buddyB,General,0
```

下表说明输入文件中的参数。

参数	说明
用户 ID	这是必要参数。 IM and Presence Service 用户的用户 ID。 最多可包含 132 个字符。 **注释** • 此值是用户 IM 地址的用户部分。 • 对于包含以下字符的用户 ID，将不会创建 JSM 会话： o a 2 ¼ ¾ - 3 µ 1 ½ β ´ ¨ ¸ ¯ Æ

参数	说明
用户域名	这是必要参数。 IM and Presence Service 用户的 Presence 域名。 最多可包含 128 个字符。 **注释** 此值是用户 IM 地址的域名部分。 **示例 1**：bjones@example.com—bjones 是用户 ID，example.com 是用户域。 **示例 2**：bjones@usa@example.com—bjones@usa 是用户 ID，example.com 是用户域。
联络人 ID	这是必要参数。 联系人列表条目的用户 ID。 最多可包含 132 个字符。
联系人域名	这是必要参数。 联系人列表条目的 Presence 域名。 域名格式需遵守以下限制： • 长度不能超过 128 个字符 • 只能包含数字、大小写字母和连字符 (-) • 不能以连字符 (-) 开头或结尾 • 标签长度不能超过 63 个字符 • 顶级域名只能包含字符，并且至少要有两个字符
Nickname	联系人列表条目的昵称。 最多可包含 255 个字符。
组名称	“组名称”是必填参数。 要添加联系人列表条目的组的名称。 最多可包含 255 个字符。
状态	名录的状态，名录数据库以十进制格式存储它。

导入非 Presence 联系人列表文件详细信息

输入文件必须是采用以下格式的 CSV 文件：

```
<User JID>、<Contact JID>、<Group Name>、<Content Type>、<Version>、<Info>
```

以下是 CSV 文件示例条目：

```
user2@cisco.com,ce463d44-02c3-4975-a37f-d4553e3f17e1,group01,text/directory,3,BEGIN:VCARD
ADR;TYPE=WORK:ADR\;WORK:\;\;123 Dublin rd\,\;Oranmore\;Galway\;\;Ireland
EMAIL;TYPE=X-CUSTOM1;X LABEL=Custom:testuser01@test.com N:test;user;;; NICKNAME:pizzaguy01
ORG:ABC TEL;TYPE=WORK,VOICE:5323534535 TITLE:QA VERSION:3.0 END:VCARD
```

注意 由于文件本身的大小以及存在损坏 vCard 信息的风险，我们建议您不要手动修改 CSV 文件。

下表说明非 Presence 联系人输入文件中的参数。

参数	说明
用户 JID	用户 JID。 这是用户的 IM 地址。
联系人 JID	联系人列表条目的用户 JID（如果可用），否则为 UUID。
组名称	要添加联系人列表条目的组的名称。
内容类型	信息字段中使用的 textmime 类型和子类型。
版本	信息字段中使用的内容类型。
信息	vCard 格式的联系人列表条目的联系信息。

导入用户位置详细信息的文件详细信息

输入文件必须是采用以下格式的 CSV 文件：

```
<User JID>、<Access Type>、<Item ID>、<Create Time>、<Resource ID>、<Message Text>
```

以下是 CSV 文件示例条目：

```
userA@example.com,W,7d0ec34c-458f-4fd2-9d15-58accac4af00,2021-01-22
10:11:18.000001,jabber_7151,

<geoloc
xmlns='http://jabber.org/protocol/geoloc'><description>newlocation104</description><street>104</street><mobile>0</mobile><enable>1</enable></geoloc>
```

注意 由于文件本身的大小以及存在损坏用户位置信息的风险，我们建议您不要手动修改 CSV 文件。

下表描述了输入文件中用于用户位置迁移的参数：

参数	说明
用户 JID	这是必要参数。 “用户 JID”是用户的 IM 地址。 最多可包含 255 个字符。

参数	说明
访问类型	这是必选参数。访问类型定义用户的访问类型。最多可包含 128 个字符。 访问类型的值如下： • W：白名单 • R：名录组 • O：开放 **注释** 对 Jabber 使用 'W'。
项目 ID	这是必要参数。 “项 ID”标识用户的特定记录。 “项 ID”的值应为“忽略”或字母数字值。联系人列表条目的用户 ID。 最多可包含 50 个字符。
创建时间	这是必要参数。 “创建时间”显示项目创建或更新的日期和时间。 最多可包含 26 个字符。
资源 ID	这是必要参数。 “资源 ID”是 Jabber 实例 ID。 最多可包含 1023 个字符。
消息文本	这是必要参数。 “消息文本”是用户的位置信息。 最多可包含 30000 个字符。

新建批量管理作业

为联系人列表和非 Presence 联系人列表创建新的批量管理作业。

开始之前

上传输入文件，第 362 页

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中：

- 如果要为联系人列表创建新的批量管理作业，选择**批量管理** > **联系人列表** > **更新**

- 如果您想要创建新的联系人列表的批量管理作业，选择**批量管理** > **联系人非 Presence 列表** > **导入非 Presence 联系人列表**。
- 如果要为用户位置迁移创建新的批量管理作业，请选择**批量管理** > **用户位置迁移** > **导入用户位置详细信息**。

步骤 2 从“文件名”下拉列表中，选择要导入的文件。

步骤 3 在“作业说明”字段中，输入此批量管理作业的说明。

步骤 4 选择下列操作之一：

- 单击**立即运行**，以立即执行批量管理作业。
- 单击**稍后运行**，以安排执行批量管理作业的时间。 有关在 BAT 中安排作业时间的详细信息，请参阅 Cisco Unified CM IM and Presence 管理中的在线帮助。

步骤 5 单击**提交**。 如果选择立即运行作业，将在您单击“提交”后运行作业。

下一步做什么

检查批量管理作业的结果，第 367 页

检查批量管理作业的结果

当批量管理作业完成后，IM and Presence Service BAT 工具会将联系人列表导入作业的结果写入日志文件。 该日志文件包含以下信息：

- 已成功导入的联系人数量。
- 尝试导入联系人时遇到的内部服务器错误的数量。
- 未导入（忽略）的联系人数量。 日志文件会在日志文件末尾针对每个被忽略的联系人列出未导入的原因。 下面是未导入联系人的原因：
  - 格式无效 - 行格式无效，如必需字段缺失或为空
  - 联系人域无效 - 联系人域的格式无效。 有关联系人域的有效格式，请参阅与批量导入用户联系人列表相关的主题。
  - 不能将自己添加为联系人 - 如果联系人为用户本人，则无法导入该联系人。
  - 用户联系人列表大小超过上限 - 用户已达到最大联系人列表大小，无法导入该用户的更多联系人
  - 用户未分配给本地节点 - 用户尚未分配到本地节点
- CSV 文件中由于导致 BAT 作业过早结束的错误而未处理的联系人数量。 此错误极少发生。

完成以下过程即可访问此日志文件。

开始之前

新建批量管理作业，第 366 页

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**批量管理** > **任务调度**。

步骤 2 单击**查找**并选择联系人列表导入作业的作业 ID。

步骤 3 单击**记录文件名**链接即可打开日志。

第 34 章

排查系统

- 故障诊断概述， 第 369 页
- 运行系统故障诊断程序， 第 369 页
- 运行诊断， 第 370 页
- 使用跟踪日志进行故障诊断， 第 371 页
- 用户 ID 和目录 URI 错误故障诊断， 第 379 页

故障诊断概述

本章中的程序用于排查 IM and Presence 部署相关问题。 利用 IM and Presence Service 部署，您可以：

- 使用命令行界面 (CLI) 构建可用于检查以解决问题的跟踪日志。
- 运行诊断以检查您的系统问题。
- 运行系统故障诊断程序，确认您系统的运行状况。
- 排查重复的目录 URI 问题。

运行系统故障诊断程序

运行故障诊断程序可诊断 IM and Presence Service 部署相关问题。 故障诊断程序会自动检查部署中的各种问题，包括：

- 系统问题
- 同步代理问题
- Presence Engine 问题
- SIP 代理问题
- 日历问题
- 群集间问题

- 拓扑问题
- Cisco Jabber 冗余分配
- 外部服务器条目
- 第三方合规服务器
- 第三方 LDAP 连接
- LDAP 连接
- XCP 状态
- 用户配置

过程

步骤 1 在 Cisco Unified CM IM and Presence 管理中选择**诊断** > **系统故障诊断程序**。
故障诊断程序会根据您的系统运行一系列自动检查。 结果显示在**系统配置故障诊断程序**窗口。

步骤 2 解决故障诊断程序突出显示的所有问题。

运行诊断

管理正在运行的系统时，可能会遇到影响系统正常运行的问题。 您可以使用 IM and Presence Service 诊断工具来帮助确定出现这些问题的根本原因。

此程序用于访问 IM and Presence Service 的诊断工具。

可以单击**诊断**并选择以下选项之一，以在 **Cisco Unified CM IM and Presence 管理**中访问这些工具：

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**诊断**。

步骤 2 从下拉列表中单击您想要使用的诊断工具。

有关这些工具用途的详细信息，请参阅“诊断工具概述”。

诊断工具概述

诊断工具	目的
系统控制板	使用系统仪表盘可获取 IM and Presence Service 系统的状态快照，包括以下系统组件的汇总数据视图：设备的数量、用户的数量、每个用户数据（如联系人）以及主分机。
系统配置故障诊断程序	系统配置故障诊断程序可用于在初始配置后或更改配置时诊断 IM and Presence Service 配置问题。故障诊断程序会在 IM and Presence Service 群集和 Cisco Unified Communications Manager 群集上执行一系列测试，以验证 IM and Presence Service 配置。 该故障诊断程序完成测试后，将报告每个测试的三种可能状态之一： • 测试通过 • 测试失败 • 测试预警，指出可能存在的配置问题 对于每个失败的或产生预警的测试，该故障诊断程序会提供有关问题和可能的解决方案的说明。对于任何测试失败或测试警告，单击解决方案列中的修复链接以转至 Cisco Unified Communications Manager IM and Presence 管理窗口，该故障诊断程序在其中找到了问题。请更正找到的任何配置错误并返回该故障诊断程序。

使用跟踪日志进行故障诊断

使用跟踪日志来排除 IM and Presence Service 和功能相关系统问题。 您可以为各种服务、功能和系统组件配置自动系统跟踪。 结果存储在系统日志中，您可以使用 Cisco Unified 实时监控工具浏览和查看。 或者，您可以使用命令行界面提取一部分系统日志文件，并将其上传到您自己的 PC 或笔记本电脑以进行进一步分析。

要使用跟踪功能，必须先配置系统以进行跟踪。 有关如何配置系统跟踪的详细信息，请参阅《*Cisco Unified* 功能配置管理指南》的“跟踪”一章。

配置好跟踪后，您可以使用两种方法之一来查看跟踪文件的内容：

- 实时监控工具—使用实时监控工具，您可以浏览和查看由于系统跟踪而创建的各个日志文件。有关如何使用实时监控工具的详细信息，请参阅《*Cisco Unified* 实时监控工具管理指南》。
- 命令行界面 (CLI) — 如果配置了系统跟踪，使用 CLI 从系统日志构建自定义跟踪。 使用 CLI，您可以指定要包含在自定义跟踪文件中的特定日期。 CLI 会从系统中提取关联的跟踪文件，并将其保存在压缩的 zip 文件中，您可以将其复制到 PC 或笔记本电脑进行进一步分析，从而确保日志不会被系统覆盖。

  本部分的后续表格和任务描述了如何使用 CLI 命令为 IM and Presence Service 构建跟踪日志文件。

通过跟踪发现的常见 IM and Presence 问题

下表列出了 IM and Presence Service 的常见问题，以及可以运行哪些跟踪记录来解决问题。

表 *47:* 常见的 *IM and Presence* 问题排查

问题	查看这些服务的跟踪记录	其他说明
登录和验证跟踪	客户端配置文件代理 Cisco XCP 连接管理器 Cisco XCP 路由器 Cisco XCP 验证服务 Cisco Tomcat 安全日志	请参阅通过 CLI 的常见跟踪，第 374 页了解生成日志和输出位置的 CLI 命令。
可用性状态	Cisco XCP 连接管理器 Cisco XCP 路由器 Cisco Presence Engine	请参阅通过 CLI 的常见跟踪，第 374 页了解生成日志和输出位置的 CLI 命令。
发送和接收即时消息	Cisco XCP 连接管理器 Cisco XCP 路由器	请参阅通过 CLI 的常见跟踪，第 374 页了解生成日志和输出位置的 CLI 命令。
联系人列表	Cisco XCP 连接管理器 Cisco XCP 路由器 Cisco Presence Engine	请参阅通过 CLI 的常见跟踪，第 374 页了解生成日志和输出位置的 CLI 命令。
聊天室	Cisco XCP 连接管理器 Cisco XCP 路由器 Cisco XCP 文字会议管理器	请参阅通过 CLI 的常见跟踪，第 374 页了解生成日志和输出位置的 CLI 命令。

问题	查看这些服务的跟踪记录	其他说明
分区式域内联合	Cisco XCP 路由器 Cisco XCP SIP 联合连接管理器 Cisco SIP Proxy Cisco Presence Engine	请参阅通过 CLI 的常见跟踪，第 374 页了解生成日志和输出位置的 CLI 命令。 **注释** 需要从 Cisco SIP Proxy 调试日志查看 SIP 消息交换
基于 XMPP 的域间联合联系人的可用性和 IM	Cisco XCP 连接管理器 Cisco XCP 路由器 Cisco Presence Engine Cisco XCP XMPP 联合连接管理器	请参阅通过 CLI 的常见跟踪，第 374 页了解生成日志和输出位置的 CLI 命令。 在启用了 XMPP 联合的每个 IM and Presence 节点上执行跟踪
SIP 域间联合联系人的可用性和 IM	Cisco XCP 连接管理器 Cisco XCP 路由器 Cisco Presence Engine Cisco SIP Proxy Cisco XCP SIP 联合连接管理器	请参阅通过 CLI 的常见跟踪，第 374 页了解生成日志和输出位置的 CLI 命令。
日历跟踪	Cisco Presence Engine	请参阅通过 CLI 的常见跟踪，第 374 页了解生成日志和输出位置的 CLI 命令。
群集间同步跟踪和群集间故障诊断程序	Cisco 群集间同步代理 Cisco AXL Web 服务 Cisco Tomcat 安全日志 Cisco Syslog 代理	通过**诊断** > **系统故障诊断程序**运行系统故障诊断程序，以检查群集间错误。
SIP 联合跟踪	Cisco SIP Proxy Cisco XCP 路由器 Cisco XCP SIP 联合连接管理器	请参阅通过 CLI 的常见跟踪，第 374 页了解生成日志和文件输出位置的 CLI 命令。
XMPP 联合跟踪	Cisco XCP 路由器 Cisco XCP XMPP 联合连接管理器	请参阅通过 CLI 的常见跟踪，第 374 页了解生成日志和文件输出位置的 CLI 命令。

问题	查看这些服务的跟踪记录	其他说明
高 CPU 和低 VM 警告故障诊断	Cisco XCP 路由器 Cisco XCP SIP 联合连接管理器 Cisco SIP Proxy Cisco Presence Engine Cisco Tomcat 安全日志 Cisco Syslog 代理	如需其他故障诊断信息，运行以下 CLI 命令： • `show process using-most cpu` • `show process using-most memory` • `utils dbreplication runtimestate` • `utils service list` 运行以下 CLI 以获取 RIS（实时信息服务）数据： • `file get activelog cm/log/ris/csv` 也可以设置 Cisco Unified IM and Presence 功能配置警报向本地系统日志提供有关运行时状态和系统状态的信息。

通过 CLI 的常见跟踪

命令行界面可用于构建跟踪日志文件以对系统进行故障诊断。 使用 CLI，您可以选择要为其运行跟踪的组件，并指定 <duration>，这是从您希望包含在日志文件中的今天往后数的天数。

以下两个表包含可用于构建跟踪日志文件和日志输出位置的 CLI 命令：

- IM and Presence Service
- IM and Presence 功能

注释 CLI 会提取您可以使用 Cisco Unified 实时监控工具 (RTMT) 查看的部分相同单个跟踪文件，但将它们分组并存储在单个压缩 zip 文件中。 有关 RTMT 跟踪的信息，请参阅通过 RTMT 的常见跟踪，第 378 页。

表 *48:* 使用 *CLI* 对 *IM and Presence Service* 进行的常见跟踪

服务	生成日志的 CLI	CLI 输出文件
Cisco 审计日志	file build log cisco_audit_logs <duration>	`/epas/trace/log_cisco_audit_logs_*.tar.gz`

服务	生成日志的 CLI	CLI 输出文件
Cisco 客户端配置文件代理	file build log cisco_client_profile_agent <duration>	/epas/trace/log_cisco_client_profile_agent_*.tar.gz
Cisco 群集管理器	file build log cisco_config_agent <duration>	/epas/trace/log_cisco_cluster_manager_*.tar.gz
Cisco 配置代理	file build log cisco_config_agent <duration>	/epas/trace/log_cisco_config_agent_*.tar.gz
Cisco 数据库层监控器	file build log cisco_database_layer_monitor <duration>	/epas/trace/log_cisco_database_layer_monitor_*.tar.gz
Cisco 群集间同步代理	file build log cisco_inter_cluster_sync_agent <duration>	/epas/trace/log_cisco_inter_cluster_sync_agent_*.tar.gz
Cisco OAM 代理	file build log cisco_oam_agent <duration>	/epas/trace/log_cisco_oam_agent_*.gz
Cisco Presence Engine	file build log cisco_presence_engine <duration>	/epas/trace/log_cisco_presence_engine_*.tar.gz
Cisco RIS（实时信息服务）数据收集器	file build log cisco_ris_data_collector <duration>	/epas/trace/log_cisco_ris_data_collector_*.tar.gz
思科服务管理	file build log cisco_service_management <duration>	/epas/trace/log_cisco_service_management_*.tar.gz
Cisco SIP Proxy	file build log cisco_sip_proxy <duration>	/epas/trace/log_cisco_sip_proxy_*.tar.gz
Cisco 同步代理	file build log cisco_sync_agent <duration>	/epas/trace/log_cisco_sync_agent_*.tar.gz
Cisco XCP 配置管理器	file build log cisco_xcp_config_mgr <duration>	/epas/trace/log_cisco_xcp_config_mgr_*.tar.gz
Cisco XCP 路由器	file build log cisco_xcp_router <duration>	/epas/trace/log_cisco_xcp_router_*.tar.gz

表 *49:* 使用 *CLI* 对 *IM and Presence* 功能进行的常见跟踪

功能名称	生成日志的 CLI	CLI 输出文件
管理 GUI	file build log admin_ui <duration>	/epas/trace/log_admin_ui_*.tar.gz
批量管理	file build log bat <duration>	/epas/trace/log_bat_*.tar.gz
同步 HTTP 上的双向流	file build log bosh <duration>	/epas/trace/log_bosh_*.tar.gz
证书	file build log certificates <duration>	/epas/trace/log_certificates_*.tar.gz
配置代理核心	file build log cfg_agent_core <duration>	/epas/trace/log_cfg_agent_core_*.tar.gz
客户语音门户	file build log cvp <duration>	/epas/trace/log_cvp_*.tar.gz
目录组	file build log directory_groups <duration>	/epas/trace/log_directory_groups_*.tar.gz
灾难恢复	file build log disaster_recovery <duration>	/epas/trace/log_disaster_recovery_*.tar.gz
灵活的 IM 地址	file build log flexable_im_address <duration>	/epas/trace/log_flexible_im_address_*.tar.gz
一般核心	file build log general_core <duration>	/epas/trace/log_general_core_*.tar.gz
高可用性	file build log ha <duration>	/epas/trace/log_ha_*.tar.gz
高 CPU	file build log high_cpu <duration>	/epas/trace/log_high_cpu_*.tar.gz
高内存	file build log high_memory <duration>	/epas/trace/log_high_memory_*.tar.gz
即时消息数据库核心	file build log imdb <duration>	/epas/trace/log_imdb_core_*.tar.gz
群集间对等	file build log inter_cluster <duration>	/epas/trace/log_inter_cluster_*.tar.gz
托管文件传输	file build log managed_file_transfer <duration>	/epas/trace/log_managed_file_transfer_*.tar.gz
Microsoft Exchange	file build log msft_exchange <duration>	/epas/trace/log_msft_exchange_*.tar.gz
消息存档程序	file build log msg_archiver <duration>	/epas/trace/log_msg_archiver_*.tar.gz

功能名称	生成日志的 CLI	CLI 输出文件
Presence Engine 核心	file build log pe_core <duration>	/epas/trace/log_pe_core_*.tar.gz
Presence and IM 消息交换	file build log presence_im_exchange <duration>	/epas/trace/log_presence_im_exchange_*.tar.gz
SIP 登录问题	file build log pws <duration>	/epas/trace/log_pws_*.tar.gz
安全漏洞	file build log sec_vulnerability <duration>	/epas/trace/log_sec_vulnerability_*.tar.gz
功能配置 GUI	file build log serviceability_ui <duration>	/epas/trace/log_serviceability_ui_*.tar.gz
SIP 域间联合	file build log sip_inter_federation <duration>	/epas/trace/log_sip_inter_federation_*.tar.gz
SIP 分区式域内联合	file build log sip_partitioned_federation <duration>	/epas/trace/log_sip_partitioned_federation_*.tar.gz
SIP 代理核心	file build log sipd_core <duration>	/epas/trace/log_sipd_core_*.tar.gz
永久聊天高可用性	file build log tc_ha <duration>	/epas/trace/log_tc_ha_*.tar.gz
永久聊天	file build log text_conference <duration>	/epas/trace/log_text_conference_*.tar.gz
升级问题	file build log upgrade_issues <duration>	/epas/trace/log_upgrade_issues_*.tar.gz
用户连接	file build log user_connectivity <duration>	/epas/trace/log_user_connectivity_*.tar.gz
名录	file build log user_rosters <duration>	/epas/trace/log_user_rosters_*.tar.gz
XCP 路由器核心	file build log xcp_core <duration>	/epas/trace/log_xcp_core_*.tar.gz
XMPP 域间联合	file build log xmpp_inter_federation <duration>	/epas/trace/log_xmpp_inter_federation_*.tar.gz
部署信息	file build log deployment_info <duration>	/epas/trace/log_deployment_info_*.tar.gz

通过 CLI 运行跟踪

此程序用于通过命令行界面 (CLI) 创建自定义跟踪文件。 使用 CLI，您可以通过持续时间参数指定要往后跟踪的天数。 CLI 将提取部分系统日志。

注释 确保只使用 SFTP 服务器传输文件。

开始之前

您必须为您的系统配置跟踪。 有关设置跟踪的详细信息，请参阅《*Cisco Unified* 功能配置管理指南》的“跟踪”一章。

查阅通过 CLI 的常见跟踪，第 374 页了解您可以运行的跟踪列表。

过程

步骤 1 登录到命令行界面。

步骤 2 要生成日志，运行 `file build log <name of service> <duration>` CLI 命令，其中持续时间是跟踪涵盖的天数。

例如，运行 `file build log cisco_cluster_manager 7` 可查看过去一周的 Cisco 群集管理器日志。

步骤 3 要获取日志，请运行 `file get activelog <log filepath>` CLI 命令以获取跟踪文件。

例如，**file get activelog epas/trace/log_cisco_cluster_manager__2016-09-30-09h41m37s.tar.gz**。

步骤 4 要保持系统稳定，可在检索后删除日志。 运行 `file delete activelog <filepath>` 命令可删除日志。

例如，`file delete activelog epas/trace/log_cisco_cluster_manager__2016-09-30-09h41m37s.tar.gz`。

通过 RTMT 的常见跟踪

下表列出了可对 IM and Presence Service 执行的常见跟踪以及生成的日志文件。您可以使用实时监控工具 (RTMT) 查看跟踪日志文件。

注释 CLI 可用于提取您可以使用 RTMT 查看的部分相同单个跟踪文件，但将它们分组并存储在单个压缩 zip 文件中。有关 CLI 跟踪的信息，请参阅通过 CLI 的常见跟踪，第 374 页。

表 *50: IM and Presence* 节点的常见跟踪和日志文件

服务	跟踪日志文件名
Cisco AXL Web 服务	/tomcat/logs/axl/log4j/axl*.log
Cisco 群集间同步代理	/epas/trace/cupicsa/log4j/icSyncAgent*.log
Cisco Presence Engine	/epas/trace/epe/sdi/epe*.txt.gz
Cisco SIP Proxy	/epas/trace/esp/sdi/esp*.txt.gz
Cisco Syslog 代理	/cm/trace/syslogmib/sdi/syslogmib*.txt
Cisco Tomcat 安全日志	/tomcat/logs/security/log4/security*.log
Cisco XCP 验证服务	/epas/trace/xcp/log/auth-svc-1*.log.gz
Cisco XCP 配置管理器	/epas/trace/xcpconfigmgr/log4j/xcpconfigmgr*.log
Cisco XCP 连接管理器	/epas/trace/xcp/log/client-cm-1*.log.gz
Cisco XCP 路由器	/epas/trace/xcp/log/rtr-jsm-1*.log.gz
Cisco XCP SIP 联合连接管理器	/epas/trace/xcp/log/sip-cm-3*.log
Cisco XCP 文字会议管理器	/epas/trace/xcp/log/txt-conf-1*.log.gz
Cisco XCP XMPP 联合连接管理器	/epas/trace/xcp/log/xmpp-cm-4*.log
群集管理器	/platform/log/clustermgr*.log
Cisco 客户端配置文件代理 (CPA)	/tomcat/logs/epassoap/log4j/EPASSoap*.log
dbmon	/cm/trace/dbl/sdi/dbmon*.txt

用户 ID 和目录 URI 错误故障诊断

收到重复的用户 ID 错误

问题 我收到警报，表明存在重复用户 ID，我必须修改这些用户的联系人信息。

解决方法 请执行下列步骤。

1. 使用 **utilsusersvalidate{ all | userid | uri }** CLI 命令生成完整用户列表。 有关使用 CLI 的详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面指南》。

   用户 ID 在结果集中输入，后面是重复用户 ID 所驻留服务器的列表。 以下示例 CLI 输出显示输出过程中的用户 ID 错误：

```
Users with Duplicate User IDs
---------------------------------------------
 User ID: user3
  Node Name
  cucm-imp-1
  cucm-imp-2
```

2. 如果同一用户分配到两个不同群集，则从其中一个群集取消分配该用户。
3. 如果不同群集上的不同用户分配了同一用户 ID，则重命名其中一位用户的用户 ID 值，确保不再有重复情况。
4. 如果用户信息无效或为空，请使用 Cisco Unified Communications Manager 管理 GUI 继续更正该用户的用户 ID 信息。
5. 可以使用**最终用户配置**窗口（**用户管理** > **最终用户**）修改 Cisco Unified Communications Manager 中的用户记录，确保所有用户都有必要的有效用户 ID 或目录 URI 值。 有关详细信息，请参阅《*Cisco Unified Communications Manager* 管理指南》。

注释 用户配置文件中的用户 ID 和目录 URI 字段可能映射至 LDAP 目录。 这种情况下，请在 LDAP 目录服务器中应用该修复。

6. 运行 CLI 命令再次验证用户，确保不再有重复用户 ID 错误。

收到重复或无效目录 URI 错误

问题 我收到警报，表明存在重复或无效用户目录 URI，我必须修改这些用户的联系人信息。

解决方法 请执行下列步骤。

1. 使用 **utilsusersvalidate{ all | userid | uri }** CLI 命令生成完整用户列表。 有关使用 CLI 的详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面指南》。

   目录 URI 值在结果集中输入，后面是重复或无效目录 URI 所驻留服务器的列表。 以下示例 CLI 输出显示验证检查过程中检测到的目录 URI 错误：

```
Users with No Directory URI Configured
-----------------------------------------------------
 Node Name: cucm-imp-2
 User ID
 user4

Users with Invalid Directory URI Configured
-----------------------------------------------------
 Node Name: cucm-imp-2
 User ID   Directory URI
 user1     asdf@ASDF@asdf@ADSF@cisco

Users with Duplicate Directory URIs
-----------------------------------------------------
Directory URI: user1@cisco.com
 Node Name   User ID
```

```
cucm-imp-1  user4
cucm-imp-2  user3
```

2. 如果同一用户分配到两个不同群集，则从其中一个群集取消分配该用户。
3. 如果不同群集上的不同用户分配了同一目录 URI 值，则重命名其中一位用户的目录 URI 值，确保不再有重复情况。
4. 如果用户信息无效或为空，请继续更正该用户的目录 URI 信息。
5. 可以使用**最终用户配置**窗口（**用户管理** > **最终用户**）修改 Cisco Unified Communications Manager 中的用户记录，确保所有用户都有必要的有效用户 ID 或目录 URI 值。 有关详细信息，请参阅《*Cisco Unified Communications Manager* 管理指南》。

注释 用户配置文件中的用户 ID 和目录 URI 字段可能映射至 LDAP 目录。 这种情况下，请在 LDAP 目录服务器中应用该修复。

6. 运行 CLI 命令再次验证用户，确保不再有重复或无效目录 URI 错误。

第 V 部分

参考信息

- Cisco Unified Communications Manager TCP 和 UDP 端口使用情况， 第 385 页
- IM and Presence Service 的端口使用信息， 第 403 页
- 其它要求， 第 419 页

第 35 章

Cisco Unified Communications Manager TCP 和 UDP 端口使用情况

本章介绍了 Cisco Unified Communications Manager 用于群集内连接以及与外部应用程序或设备通信的 TCP 和 UDP 端口列表。 在实施 IP 通信解决方案时，您还可以找到有关网络上防火墙、访问控制列表 (ACL) 和服务质量 (QoS) 配置的重要信息。

- Cisco Unified Communications Manager TCP 和 UDP 端口使用情况概述， 第 385 页
- 端口说明， 第 387 页
- 端口参考， 第 400 页

Cisco Unified Communications Manager TCP 和 UDP 端口使用情况概述

Cisco Unified Communications Manager TCP 和 UDP 端口分为以下几类：

- Cisco Unified Communications Manager 服务器之间的群集内端口
- 公共服务端口
- Cisco Unified Communications Manager 与 LDAP 目录之间的端口
- 从 CCMAdmin 或 CCMUser 到 Cisco Unified Communications Manager 的 Web 请求
- 从 Cisco Unified Communications Manager 到电话的 Web 请求
- 电话和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信
- 网关和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信
- 应用程序和 Cisco Unified Communications Manager 之间的通信
- CTL 客户端和防火墙之间的通信
- HP 服务器上的特殊端口

有关上述每个类别中的端口详细信息，请参阅“端口说明”。

注释 对于这些端口，Cisco 并未验证所有可能的配置情形。如果您在使用此列表时遇到配置问题，请联系 Cisco 技术支持人员寻求帮助。

提及的端口只适用于 Cisco Unified Communications Manager。某些端口因版本而异，而且将来的版本可能会引入新的端口。因此，对于所安装的 Cisco Unified Communications Manager 版本，请确保使用本文档的正确版本。

虽然几乎所有协议都是双向的，但是假定从会话发起者的角度看待方向性。在某些情况下，管理员可以手动更改默认端口号，但思科不建议将此作为最佳做法。请注意，Cisco Unified Communications Manager 会严格打开多个端口以供内部使用。

安装 Cisco Unified Communications Manager 软件会自动安装以下网络服务以实现可维护性并默认激活它们。请参阅“《Cisco Unified Communications Manager 服务器之间的群集内端口》”获取详细信息：

- Cisco 日志分区监控（监控并清理通用分区。此过程不使用自定义通用端口。）
- Cisco 跟踪收集服务（TCTS 端口使用情况）
- Cisco RIS 数据收集器（RIS 服务器端口使用情况）
- Cisco AMC 服务（AMC 端口使用情况）

根据拓扑、电话设备的放置以及与网络安全设备的放置相关的服务以及所用的应用程序和电话扩展，防火墙、ACL 或 QoS 的配置将有所不同。另外，请记住，ACL 的格式因设备和版本不同而异。

注释 您也可以在 Cisco Unified Communications Manager 中配置多播音乐保持 (MOH) 端口。多播 MOH 的端口值未提供，因为管理员指定了实际的端口值。

注释 系统的临时端口范围为 32768 至 61000，端口需要打开以保持电话为注册状态。有关详细信息，请参阅 http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html。

注释 请确保配置防火墙，以便与端口 22 的连接处于打开状态，并且不受限制。在安装 IM and Presence 订阅方节点期间，到 Cisco Unified Communications Manager 发布方节点的多个连接将连续快速打开。限制这些连接可能会导致安装失败。

端口说明

- Cisco Unified Communications Manager 服务器之间的群集内端口， 第 387 页
- 公共服务端口， 第 390 页
- Cisco Unified Communications Manager 与 LDAP 目录之间的端口， 第 393 页
- 从 CCMAdmin 或 CCMUser 到 Cisco Unified Communications Manager 的 Web 请求， 第 393 页
- 从 Cisco Unified Communications Manager 到电话的 Web 请求， 第 394 页
- 电话和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信， 第 394 页
- 网关和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信， 第 396 页
- 应用程序和 Cisco Unified Communications Manager 之间的通信， 第 398 页
- CTL 客户端和防火墙之间的通信， 第 399 页
- 思科智能许可服务和思科智能软件管理器之间的通信， 第 400 页
- HP 服务器上的特殊端口， 第 400 页

Cisco Unified Communications Manager 服务器之间的群集内端口

表 *51: Cisco Unified Communications Manager* 服务器之间的群集内端口

从（发送方）	至（监听方）	目标端口	目的
终端	Unified Communications Manager	514 / UDP	系统日志记录服
终端	Unified Communications Manager	514 / UDP	系统日志记录服
Unified Communications Manager	Unified Communications Manager	443 / TCP	在订阅方节点中 件期间，此端口 发布方之间的通
Unified Communications Manager	RTMT	1090、1099 / TCP	Cisco AMC 服务， 性能监控、数据 录和警报
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1500、1501 / TCP	数据库连接（15 要连接）
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1510 / TCP	CAR IDS DB。 C 侦听并等待来自 请求。

从（发送方）	至（监听方）	目标端口	目的
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1511 / TCP	CAR IDS DB。 用于间调出第二个 CAR 的备用端口。
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1515 / TCP	安装期间节点之间的制
Cisco 扩展功能 (QRT)	Unified Communications Manager (DB)	2552 / TCP	允许订阅方接收 Cisc Communications Man 库更改通知
Unified Communications Manager	Unified Communications Manager	2551 / TCP	Cisco扩展服务之间 备份确定的群集内通
Unified Communications Manager (RIS)	Unified Communications Manager (RIS)	2555 / TCP	实时信息服务器 (RI 服务器
Unified Communications Manager (AMC/RTMT/SOAP)	Unified Communications Manager (RIS)	2556 / TCP	适用于 Cisco RIS 的 服务 (RIS) 数据库客
Unified Communications Manager (DRS)	Unified Communications Manager (DRS)	4040 / TCP	DRS 主要代理
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5001/TCP	SOAP 监控器将此端 时监控服务。
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5002/TCP	SOAP 监控器将此端 能监控服务。
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5003/TCP	SOAP 监控器将此端 制中心服务。
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5004/TCP	SOAP 监控器将此端 志收集服务。
标准 CCM 管理员用户 / 管理员	Unified Communications Manager	5005 / TCP	此端口由 SOAP CDROnDemand2 服
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5007 / TCP	SOAP 监控器
Unified Communications Manager (RTMT)	Unified Communications Manager (TCTS)	临时 / TCP	Cisco 跟踪收集工具 (TCTS) -- 用于 RTM 日志中心 (TLC) 的
Unified Communications Manager (Tomcat)	Unified Communications Manager (TCTS)	7000、7001、7002 / TCP	此端口用于Cisco跟 具服务和Cisco跟踪 务程序之间的通信。

从（发送方）	至（监听方）	目标端口	目的
Unified Communications Manager	证书管理器	7070 / TCP	证书管理器服务
Unified Communications Manager (DB)	Unified Communications Manager (CDLM)	8001 / TCP	客户端数据库更
Unified Communications Manager (SDL)	Unified Communications Manager (SDL)	8002 / TCP	群集内通信服务
Unified Communications Manager (SDL)	Unified Communications Manager (SDL)	8003 / TCP	群集内通信服务
Unified Communications Manager	CMI 管理器	8004 / TCP	Cisco Unified Co Manager 和 CMI 的群集内通信
Unified Communications Manager (Tomcat)	Unified Communications Manager (Tomcat)	8005 / TCP	Tomcat 关闭脚本 侦听端口
Unified Communications Manager (Tomcat)	Unified Communications Manager (Tomcat)	8080 / TCP	用于诊断测试的 通信
网关	Unified Communications Manager	8090	用于 CuCM 和 G 接口）之间通信 口，针对网关录
Unified Communications Manager	网关		
Unified Communications Manager (IPSec)	Unified Communications Manager (IPSec)	8500 / TCP 和 UDP	IPSec 群集管理器 的群集内复制
Unified Communications Manager (RIS)	Unified Communications Manager (RIS)	8888-8889 / TCP	RIS 服务管理器 复
位置带宽管理器 (LBM)	位置带宽管理器 (LBM)	9004 / TCP	LBM 之间的群集
Unified Communications Manager [被叫号码分析器 (DNA) 初始化服务器]	JNIWrapper 服务器	30000 / TCP	被叫号码分析器 处理 DNA 初始化 用的端口。 JNIW 响应 DNA Java 服 求。
Unified Communications Manager 发布方	Unified Communications Manager 订阅方	22 / TCP	Cisco SFTP 服务 阅方时，您必须
Unified Communications Manager	Unified Communications Manager	8443 / TCP	允许访问控制中 的功能和网络服

公共服务端口

表 *52:* 公共服务端口

从（发送方）	至（监听方）	目标端口	目的
终端	Unified Communications Manager	7	互联网控制消息协议 (ICMP) 此协议号携带与回声相关的流量。 它不构成列标题中指示的端口。
Unified Communications Manager	终端		
Unified Communications Manager（DRS、呼叫详细信息记录）	SFTP 服务器	22 / TCP	发送备份数据到 SFTP 服务器。 （DRS 本地代理） 将呼叫详细信息记录数据发送到 SFTP 服务器。
终端	Unified Communications Manager（DNS 服务器）	临时 / UDP	Cisco Unified Communications Manager 充当 DNS 服务器或 DNS 客户端 **注释** 思科建议不要让 Cisco Unified Communications Manager 充当 DNS 服务器，并且所有 IP 电话应用程序和终端都使用静态 IP 地址而不是主机名。
Unified Communications Manager	DNS 服务器		
终端	Unified Communications Manager（DHCP 服务器）	67 / UDP	Cisco Unified Communications Manager 充当 DHCP 服务器 **注释** 思科不建议在 Cisco Unified Communications Manager 上运行 DHCP 服务器。

从（发送方）	至（监听方）	目标端口	目的
Unified Communications Manager	DHCP 服务器	68 / UDP	Cisco Unified Communications Manager 充当 DHCP 客户端 注释 思科不建议在 Cisco Unified Communications Manager 上运行 DHCP 客户端。使用静态 IP 地址配置 Cisco Unified Communications Manager。）
终端设备或网关	Unified Communications Manager	69，6969，然后临时 / UDP	TFTP 服务至电话和网关
终端设备或网关	Unified Communications Manager	6970 / TCP	主服务器与代理服务器之间的 TFTP。 从 TFTP 服务器到电话和网关的 HTTP 服务。
Unified Communications Manager	NTP 服务器	123 / UDP	网络时间协议 (NTP)
SNMP 服务器	Unified Communications Manager	161 / UDP	SNMP 服务响应（来自管理应用程序的请求）
CUCM 服务器 SNMP 主代理应用程序	SNMP 陷阱目标	162 / UDP	SNMP 陷阱
SNMP 服务器	Unified Communications Manager	199 / TCP	用于 SMUX 支持的内置 SNMP 代理侦听端口
Unified Communications Manager	DHCP 服务器	546 / UDP	DHCPv6. IPv6 的 DHCP 端口。
Unified Communications Manager 功能配置	位置带宽管理器 (LBM)	5546 / TCP	增强位置 CAC 功能配置
Unified Communications Manager	位置带宽管理器 (LBM)	5547 / TCP	呼叫准入请求和带宽扣除
Unified Communications Manager	Unified Communications Manager	6161 / UDP	用于主代理与本机代理之间的通信，以处理本机代理 MIB 请求

从（发送方）	至（监听方）	目标端口	目的
Unified Communications Manager	Unified Communications Manager	6162 / UDP	用于主代理与本机代理之间的通信，以前转本机代理生成的通知
Unified Communications Manager	Unified Communications Manager	6666 / UDP	Netdump 服务器
集中 TFTP	备用 TFTP	6970 / TCP	集中式 TFTP 文件定位器服务
Unified Communications Manager	Unified Communications Manager	7161 / TCP	用于 SNMP 主代理和子代理之间的通信
SNMP 服务器	Unified Communications Manager	7999 / TCP	Cisco Discovery Protocol 代理与 CDP 可执行程序之间的通信
终端	Unified Communications Manager	443、 8443 / TCP	使用 Cisco 用户数据服务 (UDS) 请求
Unified Communications Manager	Unified Communications Manager	9050 / TCP	通过 TAPS 驻留在 Cisco Unified Communications Manager 上的服务 CRS 请求
Unified Communications Manager	Unified Communications Manager	61441 / UDP	Cisco Unified Communications Manager 应用程序通过 UDP 向此端口发出警报。 Cisco Unified Communications Manager MIB 代理侦听此端口，并按照 Cisco Unified Communications Manager MIB 定义生成 SNMP 陷阱。
Unified Communications Manager	Unified Communications Manager	5060、5061 / TCP	提供基于干线的 SIP 服务
Unified Communications Manager	Unified Communications Manager	7501	由群集间查询服务 (ILS) 用于基于证书的验证。
Unified Communications Manager	Unified Communications Manager	7502	由 ILS 用于基于密码的验证。
Unified Communications Manager	Unified Communications Manager	9966	启用防火墙时，Cisco 推送通知服务用于在群集中的节点之间通信。
Unified Communications Manager	Unified Communications Manager	9560	由本地推送通知服务 (LPNS) 使用。

从（发送方）	至（监听方）	目标端口	目的
--	--	8000-48200	ASR 和 ISR G3 平台默认端口范围。
		16384-32766	ISR G2 平台默认端口范围。

Cisco Unified Communications Manager 与 LDAP 目录之间的端口

表 *53: Cisco Unified Communications Manager* 与 *LDAP* 目录之间的端口

从（发送方）	至（监听方）	目标端口	目的
Unified Communications Manager	外线目录	389、636、3268、3269 / TCP	轻型目录访问协议 (LDAP) 对外部目录（Active Directory、Netscape Directory）的查询
外线目录	Unified Communications Manager	临时	

从 CCMAdmin 或 CCMUser 到 Cisco Unified Communications Manager 的 Web 请求

表 *54:* 从 *CCMAdmin* 或 *CCMUser* 到 *Cisco Unified Communications Manager* 的 *Web* 请求

从（发送方）	至（监听方）	目标端口	目的
浏览器	Unified Communications Manager	80、8080 / TCP	超文本传输协议
浏览器	Unified Communications Manager	443、8443 / TCP	通过 SSL 的超文 (HTTPS)
浏览器	Unified Communications Manager	9463 / TCP	SSL 上的超文本 (HTTPS) 仅支持
浏览器或 CLI	Unified Communications Manager	2355、2356 / TCP	记录 CLI 和 Web 的审计事件
Unified Communications Manager	Cisco License Manager	5555 / TCP	Cisco License Ma 端口上的许可请

从 Cisco Unified Communications Manager 到电话的 Web 请求

表 *55:* 从 *Cisco Unified Communications Manager* 到电话的 *Web* 请求

从（发送方）	至（监听方）	目标端口	目的
Unified Communications Manager • QRT • RTMT • 查找并列出电话页面 • 电话配置页面	Phone	80 / TCP	超文本传输协议 (HT

电话和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信

表 *56:* 电话和 *Cisco Unified Communications Manager* 之间的信令、媒体和其他通信

从（发送方）	至（监听方）	目标端口	目的
Phone	DNS 服务器	53/ TCP	会话发起协议 (SIP) 电话会使用域名系统 (DNS) 解析完全限定域名 (FQDN) 注释 默认情况下，某些无线接入点会阻止 TCP 53 端口，这会在使用 FQDN 配置 CUCM 时阻止无线 SIP 电话注册。
Phone	Unified Communications Manager (TFTP)	69，然后临时 / UDP	用于下载固件和配置文件的普通文件传输协议 (TFTP)
Phone	Unified Communications Manager	2000 / TCP	信令客户端控制协议 (SCCP)
Phone	Unified Communications Manager	2443 / TCP	安全信令客户端控制协议 (SCCPS)
Phone	Unified Communications Manager	2445 / TCP	为终端提供信任验证服务。

从（发送方）	至（监听方）	目标端口	目的
Phone	Unified Communications Manager (CAPF)	3804 / TCP	证书颁发机构代理职能 (CAPF) 侦听端口以颁发本地有效证书 (LSC) 给 IP 电话
Phone	Unified Communications Manager	5060 / TCP 和 UDP	会话发起协议 (SIP) 电话
Unified Communications Manager	Phone		
Phone	Unified Communications Manager	5061 TCP	安全会话发起协议 (SIPS) 电话
Unified Communications Manager	Phone		
Phone	Unified Communications Manager (TFTP)	6970 TCP	基于HTTP下载固件和配置文件
Phone	Unified Communications Manager (TFTP)	6971、6972 / TCP	TFTP 的 HTTPS 接口。 电话使用此端口将从TFTP下载安全配置文件。
Phone	Unified Communications Manager	8080 / TCP	用于XML应用程序、验证、目录、服务等的电话 URL。您可以基于每个服务配置这些端口。
Phone	Unified Communications Manager	9443 / TCP	电话使用此端口进行经过验证的联系人搜索。
Phone	Unified Communications Manager	9444	电话利用此端口号码使用头戴式耳机管理功能。
iPhone/iPad（Webex 应用）	Unified Communications Manager	9560/安全 Web 套接字	Webex 应用使用此端口号来实现 LPNS 功能。
IP VMS	Phone	16384 - 32767 / UDP	实时协议 (RTP)、安全实时协议 (SRTP) 注释 Cisco Unified Communications Manager 只使用 24576-32767，尽管其他设备使用整个范围。
Phone	IP VMS		

网关和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信

表 *57:* 网关和 *Cisco Unified Communications Manager* 之间的信令、媒体和其他通信

从（发送方）	至（监听方）	目标端口	目的
网关	Unified Communications Manager	47, 50, 51	通用路由封装 (GRE) 全负载 (ESP)、验证 (AH)。 这些协议号 密的 IPSec 流量。 它 成列标题中指示的端
Unified Communications Manager	网关		
网关	Unified Communications Manager	500 / UDP	用于建立 IP 安全协议 的 Internet 密钥交换
Unified Communications Manager	网关		
网关	Unified Communications Manager (TFTP)	69，然后临时 / UDP	普通文件传输协议 (
Unified Communications Manager 与 Cisco Intercompany Media Engine (CIME) 干线	CIME ASA	1024-65535 / TCP	端口映射服务。 仅在 路径外部署模型中使
网守	Unified Communications Manager	1719 / UDP	网守 (H.225) RAS
网关	Unified Communications Manager	1720 / TCP	用于 H.323 网关和群 (ICT) 的 H.225 信令
Unified Communications Manager	网关		
网关	Unified Communications Manager	临时 / TCP	网守控制干线上的 H 服务
Unified Communications Manager	网关		

从（发送方）	至（监听方）	目标端口	目的
网关	Unified Communications Manager	临时 / TCP	建立语音、视频 H.245 信令服务 注释 远程 H.245 于网 对于 H.24 是 11 6553
Unified Communications Manager	网关		
网关	Unified Communications Manager	2000 / TCP	信令客户端控制
网关	Unified Communications Manager	2001 / TCP	使用 Cisco Unifie Communications I 升级 6608 网关的
网关	Unified Communications Manager	2002 / TCP	使用 Cisco Unifie Communications I 升级 6624 网关的
网关	Unified Communications Manager	2427 / UDP	媒体网关控制协 关控制
网关	Unified Communications Manager	2428 / TCP	媒体网关控制协 传
--	--	4000-4005 / TCP	当 Cisco Unified Communications I 用于这些媒体的 端口用作音频、 道的虚拟实时传 和实时传输控制 端口。
网关	Unified Communications Manager	5060 / TCP 和 UDP	会话初始协议 (S 集间干线 (ICT)
Unified Communications Manager	网关		
网关	Unified Communications Manager	5061 / TCP	安全会话发起协 和群集间干线 (I
Unified Communications Manager	网关		

从（发送方）	至（监听方）	目标端口	目的
网关	Unified Communications Manager	16384 - 32767 / UDP	实时协议 (RTP)、安 议 (SRTP) 注释 Cisco Ur Commur Manager 24576-32 管其他设 整个范围
Unified Communications Manager	网关		

应用程序和 Cisco Unified Communications Manager 之间的通信

表 *58:* 应用程序和 *Cisco Unified Communications Manager* 之间的通信

从（发送方）	至（监听方）	目标端口	目的
CTL 客户端	Unified Communications Manager CTL 提供程序	2444 / TCP	Cisco Unified Commu Manager 中的证书信 (CTL) 提供程序侦听
Cisco Unified Communications 应用程序	Unified Communications Manager	2748 / TCP	CTI 应用程序服务器
Cisco Unified Communications 应用程序	Unified Communications Manager	2749 / TCP	CTI 应用程序 (JTAP CTIManager 之间的
Cisco Unified Communications 应用程序	Unified Communications Manager	2789 / TCP	JTAPI 应用程序服务
Unified Communications Manager Assistant Console	Unified Communications Manager	2912 / TCP	Cisco Unified Commu Manager Assistant 服 称 IPMA）
Unified Communications Manager Attendant Console	Unified Communications Manager	1103-1129 / TCP	Cisco Unified Commu Manager Attendant C (AC) JAVA RMI 注册
Unified Communications Manager Attendant Console	Unified Communications Manager	1101 / TCP	RMI 服务器将 RMI 发送到这些端口上的
Unified Communications Manager Attendant Console	Unified Communications Manager	1102 / TCP	Attendant Console (A 服务器绑定端口 -- R 器在这些端口上发送 息。

从（发送方）	至（监听方）	目标端口	目的
Unified Communications Manager Attendant Console	Unified Communications Manager	3223 / UDP	Cisco Unified Co Manager Attenda (AC) 服务器线路 话务台服务器接 册消息，并将线路 话务台服务器。
Unified Communications Manager Attendant Console	Unified Communications Manager	3224 / UDP	Cisco Unified Co Manager Attenda (AC) 客户端向 A 册以获取线路和 息。
Unified Communications Manager Attendant Console	Unified Communications Manager	4321 / UDP	Cisco Unified Co Manager Attenda (AC) 客户端向 A 册以进行呼叫控
Unified Communications Manager 与 SAF/CCD	IOS 路由器运行 SAF 图像	5050 / TCP	多服务 IOS 路由 EIGRP/SAF 协议
Unified Communications Manager	Cisco Intercompany Media Engine (IME) 服务器	5620 / TCP 思科建议此端口的值为 5620，但您可以在 Cisco IME 服务器上执行 add ime vapserver 或 set ime vapserver port CLI 命令以更改值。	用于与 Cisco Inte Media Engine 服 VAP 协议。
Cisco Unified Communications 应用程序	Unified Communications Manager	8443 / TCP	AXL / SOAP AP 程方式读取或写 计费或电话管理 用的 Cisco Unifie Communications 库。

CTL 客户端和防火墙之间的通信

表 *59: CTL* 客户端和防火墙之间的通信

从（发送方）	至（监听方）	目标端口	目的
CTL 客户端	TLS 代理服务器	2444 / TCP	证书信任列表 (C 序在 ASA 防火墙

思科智能许可服务和思科智能软件管理器之间的通信

Unified Communications Manager 中的思科智能许可服务通过 Call Home 与思科智能软件服务器建立直接通信。

表 *60:* 思科智能许可服务和思科智能软件管理器之间的通信

从（发送方）	至（监听方）	目标端口	目的
Unified Communications Manager（思科智能许可服务）	思科智能软件管理器 (CSSM)	443 / HTTPS	智能许可服务会将许可证使用情况发送给 CSSM 以检查 Unified CM 是否为投诉。

HP 服务器上的特殊端口

表 *61: HP* 服务器上的特殊端口

从（发送方）	至（监听方）	目标端口	目的
终端	HP SIM	2301 / TCP	HP 代理的 HTTP 端
终端	HP SIM	2381 / TCP	HP 代理的 HTTPS 端
终端	Compaq 管理代理	25375、25376、25393 / UDP	COMPAQ 管理代理 (cmaX)
终端	HP SIM	50000-50004 / TCP	HP SIM 的 HTTPS 端

端口参考

防火墙应用程序检测指南

ASA 系列参考信息

http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html

PIX 应用程序检测配置指南

http://www.cisco.com/c/en/us/support/security/pix-firewall-software/products-installation-and-configuration-guides-list.html

FWSM 3.1 应用程序检测配置指南

http://www-author.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg/inspct_f.html

IETF TCP/UDP 端口分配列表

互联网地址分配机构 (IANA) IETF 分配的端口列表

http://www.iana.org/assignments/port-numbers

IP 电话配置和端口利用指南

Cisco CRS 4.0（IP IVR 和 IPCC Express）端口利用指南

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Cisco ICM/IPCC 企业和托管版端口利用指南

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

Cisco Unified Communications Manager Express 最佳实践安全指南

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html

Cisco Unity Express 最佳实践安全指南

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e31.html#wp41149

VMware 端口分配列表

vCenter 服务器、ESX 主机和其他网络组件管理访问的 TCP 和 UDP 端口

第 36 章

IM and Presence Service 的端口使用信息

- IM and Presence Service 端口使用概述， 第 403 页
- 表中列出的信息， 第 403 页
- IM and Presence Service 端口列表， 第 404 页

IM and Presence Service 端口使用概述

本章介绍了 IM and Presence Service 用于群集内连接以及与外部应用程序或设备通信的 TCP 和 UDP 端口列表。 其中包含实施 IP 通信解决方案时，用于在网络上配置防火墙、访问控制列表 (ACL) 和服务质量 (QoS) 的重要信息。

注释 对于这些端口，Cisco 并未验证所有可能的配置情形。 如果您在使用此列表时遇到配置问题，请联系 Cisco 技术支持人员寻求帮助。

虽然几乎所有协议都是双向的，但本文档从会话发起者的角度看待方向性。 在某些情况下，管理员可以手动更改默认端口号，但思科不建议将此作为最佳做法。 请注意， IM and Presence Service 会严格打开多个端口以供内部使用。

本文档中的端口只适用于 IM and Presence Service。 某些端口因版本而异，而且将来的版本可能会引入新的端口。 因此，对于所安装的 IM and Presence Service 版本，请确保使用本文档的正确版本。

根据拓扑、设备的放置以及与网络安全设备的放置相关的服务以及所用的应用程序和电话扩展，防火墙、ACL 或 QoS 的配置将有所不同。 另外，请记住，ACL 的格式因设备和版本不同而异。

表中列出的信息

此表定义了本文档中每个表中的信息。

表 *62:* 表信息定义

表标题	说明
从	客户端将请求发送到此端口
至	客户端在此端口上接收请求
角色	客户端或服务器应用程序或过程
协议	用于建立和结束通信的会话层协议，或用于请求和响应事务的应用层协议
传输协议	传输层协议，面向连接 (TCP) 或无连接 (UDP)
目的地 / 侦听程序	用于接收请求的端口
源 / 发送方	用于发送请求的端口

IM and Presence Service 端口列表

下表显示 IM and Presence Service 用于群集内和群集间流量的端口。

表 *63: IM and Presence Service* 端口 *- SIP* 代理请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
SIP 网关 ---------- IM and Presence	IM and Presence ---------- SIP 网关	SIP	TCP/UDP	5060	临时	默认 SIP 代理 UDP 和 TCP 侦听程序
SIP 网关	IM and Presence	SIP	TLS	5061	临时	TLS 服务器验证侦听程序端口
IM and Presence	IM and Presence	SIP	TLS	5062	临时	TLS 相互验证侦听程序端口
IM and Presence	IM and Presence	SIP	UDP / TCP	5049	临时	内部端口。仅限本地主机流量。
IM and Presence	IM and Presence	HTTP	TCP	8081	临时	用于来自配置代理的 HTTP 请求，用以指示配置更改。
第三方客户端	IM and Presence	HTTP	TCP	8082	临时	默认 IM and Presence HTTP 侦听程序。 用于要连接的第三方客户端

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
第三方客户端	IM and Presence	HTTPS	TLS / TCP	8083	临时	默认 IM and Presence HTTPS 侦听程序。 用于要连接的第三方客户端

表 *64: IM and Presence Service* 端口 *- Presence Engine* 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	IM and Presence (Presence Engine)	SIP	UDP / TCP	5080	临时	默认 SIP UDP/TCP 侦听程序端口
IM and Presence (Presence Engine)	IM and Presence (Presence Engine)	Livebus	UDP	50000	临时	内部端口。 仅限本地主机流量。 LiveBus 消息传送端口。 IM and Presence Service 使用此端口进行群集通信。

表 *65: IM and Presence Service* 端口 *- Cisco Tomcat WebRequests*

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
浏览器	IM and Presence	HTTPS	TCP	8080	临时	用于 web 访问
浏览器	IM and Presence	AXL / HTTPS	TLS / TCP	8443	临时	提供通过 SOAP 访问数据库和功能配置的权限
浏览器	IM and Presence	HTTPS	TLS / TCP	8443	临时	提供 Web 管理访问权限
浏览器	IM and Presence	HTTPS	TLS / TCP	8443	临时	提供用户选项页面的访问权限
浏览器	IM and Presence	SOAP	TLS / TCP	8443	临时	可以通过 SOAP 访问 Cisco Unified Personal Communicator、Cisco Unified Mobility Advantage 和第三方 API 客户端的权限

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
浏览器	即时消息和在线状态	HTTPS	TCP	9463	临时	SSL 上的超文本传输协议 (HTTPS) 仅支持 TLS1.3 (v6)。

表 *66: IM and Presence Service* 端口 - 外部公司目录请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence ---------- 外部公司目录	外部公司目录 ---------- IM and Presence	LDAP	TCP	389 / 3268	临时	允许目录协议与外部公司目录集成。 LDAP 端口取决于公司目录（389 为默认值）。 对于 Netscape Directory，客户可以配置不同的端口来接受 LDAP 流量。 允许 LDAP 在 IM&P 和 LDAP 服务器之间通信以进行验证。
IM and Presence	外部公司目录	LDAPS	TCP	636	临时	允许目录协议与外部公司目录集成。 LDAP 端口取决于公司目录（636 为默认值）。

表 *67: IM and Presence Service* 端口 - 配置请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence（配置代理）	IM and Presence（配置代理）	TCP	TCP	8600	临时	配置代理心跳端口

表 *68: IM and Presence*服务端口 - 证书管理器请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	证书管理器	TCP	TCP	7070	临时	内部端口 - 仅限本地主机流量

表 *69: IM and Presence Service* 端口 - *IDS* 数据库请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence（数据库）	IM and Presence（数据库）	TCP	TCP	1500	临时	数据库客户端的内部 IDS 端口。 仅限本地主机流量。
IM and Presence（数据库）	IM and Presence（数据库）	TCP	TCP	1501	临时	内部端口 - 用于在升级期间调出第二个 IDS 实例的备用端口。 仅限本地主机流量。
IM and Presence（数据库）	IM and Presence（数据库）	XML	TCP	1515	临时	内部端口。 仅限本地主机流量。 数据库复制端口

表 *70: IM and Presence Service* 端口 - *IPSec* 管理器请求

从发送方	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence (IPSec)	IM and Presence (IPSec)	受限于专有环境	UDP/TCP	8500	8500	内部端口 - ipsec_mgr 守护程序用于平台数据（主机）证书群集复制的群集管理器端口

表 *71: IM and Presence Service* 端口 - *DRF* 主代理服务器请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence (DRF)	IM and Presence (DRF)	TCP	TCP	4040	临时	DRF 主代理服务端口，从本地代理、GUI 和 CLI 接受连接

表 *72: IM and Presence Service* 端口 - *RISDC* 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence (RIS)	IM and Presence (RIS)	TCP	TCP	2555	临时	实时信息服务器 (RIS) 数据库服务器。 连接到群集中的其他 RISDC 服务，以提供群集范围的实时信息

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence (AMC RTMT / / SOAP)	IM and Presence (RIS)	TCP	TCP	2556	临时	适用于 Cisco RIS 的实时信息服务 (RIS) 数据库客户端。 允许 RIS 客户端连接以检索实时信息
IM and Presence (RIS)	IM and Presence (RIS)	TCP	TCP	8889	8888	内部端口。 仅限本地主机流量。 RISDC (System Access) 用来通过 TCP 链接到 servM，以进行服务状态请求和获取回复

表 *73: IM and Presence Service* 端口 - *SNMP* 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
SNMP 服务器	IM and Presence	SNMP	UDP	161, 8161	临时	为基于 SNMP 的管理应用程序提供服务
IM and Presence	IM and Presence	SNMP	UDP	6162	临时	本地 SNMP 代理侦听 SNMP 主代理转发的请求
IM and Presence	IM and Presence	SNMP	UDP	6161	临时	SNMP 主代理从本地 SNMP 代理侦听陷阱并转发到管理应用程序
SNMP 服务器	IM and Presence	TCP	TCP	7999	临时	用作 cdp 代理与 cdp 二进制通信的套接字
IM and Presence	IM and Presence	TCP	TCP	7161	临时	用于 SNMP 主代理和子代理之间的通信
IM and Presence	SNMP 陷阱监控	SNMP	UDP	162	临时	发送 SNMP 陷阱到管理应用程序
IM and Presence	IM and Presence	SNMP	UDP	最大值	61441	内部 SNMP 陷阱接收者

表 *74: IM and Presence Service* 端口 - *Racoon* 服务器请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
网关 ---------- IM and Presence	IM and Presence ---------- 网关	Ipsec	UDP	500	临时	启用互联网安全关联和密钥管理协议

表 *75: IM and Presence Service* 端口 - 系统服务请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence (RIS)	IM and Presence (RIS)	XML	TCP	8888 和 8889	临时	内部端口。仅限本地主机流量。用于侦听客户端域 RIS 服务管理器 (servM) 的通信。

表 *76: IM and Presence Service* 端口 - *DNS* 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	DNS 服务器	DNS	UDP	53	临时	DNS 服务器侦听 IM and Presence DNS 查询的端口。 到：DNS 服务器 | 从：IM and Presence

表 *77: IM and Presence Service* 端口 - *SSH/SFTP* 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	终端	SSH / SFTP	TCP	22	临时	许多应用程序使用它来获取对服务器的命令行访问权限。也在节点之间用于证书和其他文件交换 (sftp)

表 *78: IM and Presence Service* 端口 - *ICMP* 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence ---------- Cisco Unified Communications Manager	Cisco Unified Communications Manager ---------- IM and Presence	ICMP	IP	不适用	临时	互联网控制信息协议 (ICMP)。 用于同 Cisco Unified Communications Manager 服务器通信

表 *79: IM and Presence Service* 端口 - *NTP* 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	NTP 服务器	NTP	UDP	123	临时	Cisco Unified Communications Manager 充当 NTP 服务器。 订阅方节点使用它来同发布方节点同步时间。

表 *80: IM and Presence Service* 端口 - *Microsoft Exchange* 通知请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
Microsoft Exchange	IM and Presence	HTTP (HTTPu)	) WebDAV - HTTP /UDP/IP 通知 2) EWS - HTTP/TCP /IP SOAP 通知	IM and Presence 服务器端口（默认值为 50020）	临时	Microsoft Exchange 使用此端口来发送通知（使用 NOTIFY 消息），以指明对日历事件特定订阅标识符的更改。 用于与网络配置中的任何 Exchange 服务器集成。 两个端口都会创建。 发送的消息类型取决于配置的日历在线状态后端网关的类型。

表 *81: IM and Presence Service* 端口 *- SOAP* 服务请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence (Tomcat)	IM and Presence (SOAP)	TCP	TCP	5007	临时	SOAP 监控器端口

表 *82: IM and Presence Service* 端口 *- AMC RMI* 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	RTMT	TCP	TCP	1090	临时	AMC RMI 对象端口。Cisco AMC 服务，用于 RTMT 性能监控、数据收集、日志记录和警报。
IM and Presence	RTMT	TCP	TCP	1099	临时	AMC RMI 注册端口。Cisco AMC 服务，用于 RTMT 性能监控、数据收集、日志记录和警报。

表 *83: IM and Presence Service* 端口 *- XCP* 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
XMPP 客户端	IM and Presence	TCP	TCP	5222	临时	客户端访问端口
IM and Presence	IM and Presence	TCP	TCP	5269	临时	服务器到服务器连接 (S2S) 端口
第三方 BOSH 客户端	IM and Presence	TCP	TCP	7335	临时	HTTP 侦听端口由 XCP Web 连接管理器用于 BOSH 第三方 API 连接
IM and Presence（XCP 服务）	IM and Presence（XCP 路由器）	TCP	TCP	7400	临时	XCP 路由器主机接受端口。 从开放端口配置（例如 XCP 验证组件服务）连接到路由器的 XCP 服务通常在此端口上连接。

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence（XCP 路由器）	IM and Presence（XCP 路由器）	UDP	UDP	5353	临时	MDNS 端口。群集中的 XCP 路由器使用此端口来发现彼此。
IM and Presence（XCP 路由器）	IM and Presence（XCP 路由器）	TCP	TCP	7336	HTTPS	MFT 文件传输（仅限内部）。

表 *84: IM and Presence Service* 端口 - 外部数据库请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	PostgreSQL 数据库	TCP	TCP	5432[1]	临时	PostgreSQL 数据库侦听端口
即时消息和在线状态	Oracle 数据库	TCP	TCP	1521	临时	Oracle 数据库侦听端口
IM and Presenc	MSSQL 数据库	TCP	TCP	1433	临时	MSSQL 数据库侦听端口

[1] 这是默认端口，但您可以将 PostgreSQL 数据库配置为侦听任意端口。

表 *85: IM and Presence Service* 端口 - 高可用性请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence (Server Recovery Manager)	IM and Presence (Server Recovery Manager)	TCP	TCP	20075	临时	Cisco Server Recovery Manager 用于提供管理 rpc 请求的端口。
IM and Presence (Server Recovery Manager)	IM and Presence (Server Recovery Manager)	UDP	UDP	21999	临时	Cisco Server Recovery Manager 用于同其对等节点通信的端口。

表 *86: IM and Presence Service* 端口 - 内存中的数据库复制消息

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	IM and Presence	受限于专有环境	TCP	6603*	临时	Cisco Presence 数据存储器
IM and Presence	IM and Presence	受限于专有环境	TCP	6604*	临时	Cisco 登录数据存储器
IM and Presence	IM and Presence	受限于专有环境	TCP	6605*	临时	Cisco SIP 注册数据存储器
IM and Presence	IM and Presence	受限于专有环境	TCP	9003	临时	Cisco 在线状态数据存储器双节点 presence 冗余组复制。
IM and Presence	IM and Presence	受限于专有环境	TCP	9004	临时	Cisco 登录数据存储器双节点 presence 冗余组复制。
IM and Presence	IM and Presence	受限于专有环境	TCP	9005	临时	Cisco SIP 注册数据存储器双节点 presence 冗余组复制。

* 如果使用 `utils imdb_replication status` 命令运行管理 CLI 诊断实用程序，必须在群集中的 IM and Presence Service 节点之间配置的所有防火墙上打开这些端口。 正常操作不需要此设置。

表 *87: IM and Presence Service* 端口 - 内存中的数据库 *SQL* 消息

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	IM and Presence	受限于专有环境	TCP	6603	临时	Cisco 在线状态数据存储器 SQL 查询。
IM and Presence	IM and Presence	受限于专有环境	TCP	6604	临时	Cisco 登录数据存储器 SQL 查询。
IM and Presence	IM and Presence	受限于专有环境	TCP	6605	临时	Cisco SIP 注册数据存储器 SQL 查询。
IM and Presence	IM and Presence	受限于专有环境	TCP	6606	临时	Cisco 路由数据存储器 SQL 查询。

表 *88: IM and Presence Service* 端口 - 内存中的数据库通知消息

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	IM and Presence	受限于专有环境	TCP	6607	临时	Cisco 在线状态数据存储器基于 XML 的更改通知。
IM and Presence	IM and Presence	受限于专有环境	TCP	6608	临时	Cisco 登录数据存储器基于 XML 的更改通知。
IM and Presence	IM and Presence	受限于专有环境	TCP	6609	临时	Cisco SIP 注册数据存储器基于 XML 的更改通知。
IM and Presence	IM and Presence	受限于专有环境	TCP	6610	临时	Cisco 路由数据存储器基于 XML 的更改通知。

表 *89: IM and Presence Service* 端口 - 强制手动同步*/X.509* 证书更新请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence（群集间同步代理）	IM and Presence（群集间同步代理）	TCP	TCP	37239	临时	思科群集间同步代理服务使用此端口建立用于处理命令的套接字连接。

表 *90: IM and Presence Service* 端口 - *ICMP* 请求

从（发送方）	至（监听方）	目标端口	目的
终端/IM and Presence	即时消息和在线状态	7	互联网控制消息协议此协议号携带与回声量。 它不构成列标的端口。
即时消息和在线状态	终端/IM and Presence		

表 *91:* 用于 *IM and Presence* 的端口 - *Cisco Unified CM* 通信以及 *IM and Presence* 发布方 - 订阅方通信

从（发送方）	至（监听方）	传输协议	目的地 / 侦听程序	源 / 发送方	备注
Cisco Unified Communications Manager	IM and Presence 发布方	TCP	1500	双向	数据库客户端的内部 ID 端口。 仅限本地主机流量。

从（发送方）	至（监听方）	传输协议	目的地 / 侦听程序	源 / 发送方	备注
Cisco Unified Communications Manager	IM and Presence 发布方	TCP	8443	双向	提供 Web 管理访问权限。
Cisco Unified Communications Manager	IM and Presence 发布方	TCP	1090	双向	AMC RMI 对象端口。 Cisco AMC 服务，用于 RTMT 性能监控、数据收集、日志记录和警报。
Cisco Unified Communications Manager	IM and Presence 发布方	TCP	2555	双向	双向实时信息服务器 (RIS) 数据库服务器。 连接到群集中的其他 RISDC 服务，以提供群集范围的实时信息。
Cisco Unified Communications Manager	IM and Presence 发布方	TCP	8500	双向	内部端口 - ipsec_mgr 守护程序用于平台数据（主机）证书群集复制的群集管理器端口。
Cisco Unified Communications Manager	IM and Presence 发布方	TCP	8600	双向	配置代理心跳端口
Cisco Unified Communications Manager	IM and Presence 发布方	UDP	123	双向	用于网络时间同步的网络时间协议 (NTP)。
IM and Presence 发布方	IM and Presence 订阅方	UDP	50000	双向	内部端口。 仅限本地主机流量。 LiveBus 消息传送端口。 IM and Presence Service 使用此端口进行群集通信。
IM and Presence 发布方	IM and Presence 订阅方	UDP	21999	双向	Cisco Server Recovery Manager用于同其对等节点通信的端口。
IM and Presence 发布方	Cisco Unified Communications Manager	TCP	4040	双向	从本地代理、GUI 和 CLI 接受连接的 DRF 主代理服务器端口。
IM and Presence 发布方	Cisco Unified Communications Manager	TCP	8001	双向	在配置永久聊天时使用。

从（发送方）	至（监听方）	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence 发布方	Cisco Unified Communications Manager	TCP	6379	双向	在配置托管文件传输 (MFT) 时使用。
IM and Presence 发布方	IM and Presence 订阅方	TCP	7	双向	在配置外部数据库 (MSSQL) 时使用。
IM and Presence 发布方	IM and Presence 订阅方	TCP	20075	双向	Cisco Server Recovery Manager 用于提供管理 RPC 请求的端口。
IM and Presence 发布方	IM and Presence 订阅方	TCP	8600	双向	配置代理心跳端口
IM and Presence 订阅方	IM and Presence 发布方	TCP	9005	双向	Cisco SIP 注册数据存储器双节点 presence 冗余组复制。
IM and Presence 订阅方	IM and Presence 发布方	TCP	9003	双向	Cisco 在线状态数据存储器双节点 presence 冗余组复制。
IM and Presence 订阅方	IM and Presence 发布方	TCP	20075	双向	Cisco Server Recovery Manager 用于提供管理 RPC 请求的端口。
IM and Presence 订阅方	IM and Presence 发布方	TCP	9004	双向	Cisco 登录数据存储器双节点 presence 冗余组复制。
Cisco Unified Communications Manager	IM and Presence 发布方	TCP	5070	双向	在呼叫配置中使用
IM and Presence 发布方	IM and Presence 订阅方	TCP	44000	双向	在呼叫配置中使用

表 *92: On-a-call_Presence*

从（发送方）	至（监听方）	源端口	目标端口	协议	备注
Cisco Unified Communications Manager	IM and Presence 发布方	[37240 – 61000]	5070	TCP	
IM and Presence 发布方	XMPP 客户端 (Jabber)	5222	64846	TCP	客户端访问端口
IM and Presence 发布方	XMPP 客户端 (Jabber)	5222	56361	TCP	客户端访问端口

表 *93: MS-SQL* 数据库配置

从（发送方）	至（监听方）	源端口	目标端口	协议
IM and Presence 发布方	数据库	[37240 – 61000]	7	TCP

表 *94: MS-SQL* 永久聊天配置

从（发送方）	至（监听方）	源端口	目标端口	协议
IM and Presence 发布方	数据库	37240 – 61000	1433	TCP

表 *95:* 托管文件传输 *(MFT)* 配置

从（发送方）	至（监听方）	源端口	目标端口	协议
IM and Presence 发布方	外部文件服务器	37240 – 61000	7	TCP
IM and Presence 发布方	外部文件服务器	37240 – 61000	22	TCP
IM and Presence 发布方	外部文件服务器	37240 – 61000	5432	TCP
IM and Presence 发布方	数据库	54288 - 54292	5432	TCP

有关 SNMP 的信息，请参阅《*Cisco Unified* 功能配置管理指南》。

第 37 章

其它要求

- 高可用性登录配置文件，第 419 页
- 单群集配置，第 421 页
- XMPP 标准合规性，第 428 页
- 配置更改和服务重新启动通知，第 429 页

高可用性登录配置文件

有关高可用性登录配置文件的重要说明

- 您可以使用本部分的高可用性登录配置文件表为您的 Presence 冗余组配置客户端重新登录上限值和下限值。 选择 **Cisco Unified CM IM and Presence 管理** > **系统** > **服务参数**，再从“服务”菜单中选择 **Cisco 服务器恢复管理器**，即可配置客户端重新登录上限值和下限值。
- 高可用性客户端登录配置文件仅适用于单群集部署。 如果存在多个群集，则高可用性客户端登录配置文件无法为冗余组配置上客户端重新登录上限和下限值。 您必须执行更多测试以发现多群集部署中的高可用性客户端登录配置文件。
- 如果为 Cisco XCP 路由器服务启用了调试日志记录，应预计 IM and Presence Service 的 CPU 使用率会增加，并且当前支持的日志记录级别会降低。
- 根据我们此处提供的表配置 Presence 冗余组的客户端重新登录上限和下限，可以避免群集中出现性能问题和较高的 CPU 峰值。
- 我们为每个 IM and Presence Service 节点内存大小和每个高可用性部署类型（主用/主用或主用/备用）提供高可用性登录配置文件。
- 高可用性登录配置文件表根据以下输入计算：
  - 客户端重新登录下限根据服务器恢复管理器服务参数“关键服务关闭延迟”确定，该参数的默认值为 90 秒。 如果“关键服务关闭延迟”发生变更，则下限也必须变更。
  - 主用/备用部署的 Presence 冗余组中的用户总数，或主用/主用部署中的用户数量最大的节点。

- 您必须在Presence冗余组的两个节点上配置客户端重新登录上限值和下限值。 您必须在Presence冗余组的两个节点上手动配置所有这些值。
- Presence 冗余组中每个节点上的客户端重新登录上限值和下限值都必须相同。
- 如果您要**重新平衡**用户，则必须根据高可用性登录配置文件表重新配置客户端重新登录上限值和下限值。

使用高可用性登录配置文件表

使用高可用性登录配置文件表可检索以下值：

- **客户端重新登录下限**服务参数值。
- **客户端重新登录上限**服务参数值。

过程

步骤 1 根据虚拟硬件配置以及高可用性部署类型选择配置文件表。

步骤 2 在配置文件表中，选择部署中的用户数（取整为最接近的值）。 如果有主用/备用部署，请使用具有最高用户数的节点。

步骤 3 根据 presence 冗余组的“用户数量”值，检索配置文件表中对应的重试上限和下限。

步骤 4 在 IM and Presence Service 上配置重试次数下限和上限，方法是选择 **Cisco Unified CM IM and Presence 管理** > **系统** > **服务参数**，然后从“服务”菜单中选择 **Cisco 服务器恢复管理器**。

步骤 5 选择**Cisco Unified CM IM and Presence 管理** > **系统** > **服务参数**，并从**服务**菜单中选择 **Cisco 服务器恢复管理器**，检查“关键服务关闭延迟”值。 默认值为 90 秒。 重试下限应设置为该值。

高可用性登录配置示例

示例 1：15000 用户完全 UC 配置文件 - 主用/主用部署

您的 Presence 冗余组中有 3000 个用户，其中 2000 个用户在节点一上，1000 个用户在节点二上。 对于不平衡的主用/主用部署，思科建议使用用户数量最多的节点，在本例中为拥有 2000 个用户的节点。 使用 15000 位用户的完全 US (4 vCPU 8GB) 主用/主用配置文件，检索以下重试下限和上限值：

预期活动用户数量	重试下限	重试上限
2000	120	253

注释 重试上限是所有客户端在故障转移后登录到其备份节点的大致时间（秒）。

注释 下限 120 假设**关键服务关闭延迟**服务参数设置为 120。

示例 2：5000 用户完全 UC 配置文件 - 主用/主用部署

Presence 冗余组的每个节点有 4700 个用户。 思科建议四舍五入至最接近的值，使用 5000 位用户的完全 US (4 vCPU 8GB) 主用/主用配置文件，根据用户数量值 5000 检索重试下限和上限值：

预期活动用户数量	重试下限	重试上限
5000	120	953

单群集配置

500 位用户的完全 UC (1vCPU 700MHz 2GB) 主用/主用配置文件

表 *96:* 标准部署的用户登录重试限制（*500* 位用户的完全 *UC* 主用/主用）

预期活动用户数量	重试下限	重试上限
完全 **UC**		
100	120	187
250	120	287

500 位用户的完全 UC (1vCPU 700MHz 2GB) 主用/备用配置文件

表 *97:* 标准部署的用户登录重试限制（*500* 位用户的完全 *UC* 主用/备用）

预期活动用户数量	重试下限	重试上限
完全 **UC**		
100	120	187
250	120	287
500	120	453

1000 位用户的完全 UC (1vCPU 1500MHz 2GB) 主用/主用配置文件

表 *98:* 标准部署的用户登录重试限制（*1000* 位用户的完全 *UC* 主用/主用）

预期活动用户数量	重试下限	重试上限
完全 UC		
100	120	153
250	120	203
500	120	287

1000 位用户的完全 UC (1vCPU 1500MHz 2GB) 主用/备用配置文件

表 *99:* 标准部署的用户登录重试限制（*1000* 位用户的完全 *UC* 主用/备用）

预期活动用户数量	重试下限	重试上限
完全 UC		
100	120	153
250	120	203
500	120	287
750	120	370
1000	120	453

2000 位用户的完全 UC (1vCPU 1500Mhz 4GB) 主用/主用配置文件

表 *100:* 标准部署的用户登录重试限制（*2000* 位用户的完全 *UC* 主用/主用）

预期活动用户数量	重试下限	重试上限
完全 UC		
100	120	153
500	120	287
1000	120	453

2000 位用户的完全 UC (1vCPU 1500Mhz 4GB) 主用/备用配置文件

表 *101:* 标准部署的用户登录重试限制（*2000* 位用户的完全 *UC* 主用/备用）

预期活动用户数量	重试下限	重试上限
完全 **UC**		
100	120	153
250	120	203
500	120	287
750	120	370
1000	120	453
1250	120	537
1500	120	620
1750	120	703
2000	120	787

5000 位用户的完全 UC (4 GB 2vCPU) 主用/主用配置文件

表 *102:* 标准部署的用户登录重试限制（*5000* 位用户的完全 *UC* 主用/主用）

预期活动用户数量	重试下限	重试上限
完全 **UC**		
100	120	137
500	120	203
1000	120	287
1500	120	370
2000	120	453
2500	120	537

5000 位用户的完全 UC (4 GB 2vCPU) 主用/备用配置文件

注意 为了在 5000 用户系统上获得最大客户端登录吞吐量，思科建议 CPU 时钟速度最低应达到 2.6GHz。

表 *103:* 标准部署的用户登录重试限制（*5000* 位用户的完全 *UC* 主用/备用）

预期活动用户数量	重试下限	重试上限
完全 UC		
100	120	154
500	120	287
1000	120	453
1500	120	620
2000	120	787
2500	120	953
3000	120	1120
3500	120	1287
4000	120	1453
4500	120	1620
5000	120	1787

15000 位用户的完全 UC (4 vCPU 8GB) 主用/主用配置文件

注意 为了在 15000 用户系统上获得最大客户端登录吞吐量，思科建议 CPU 时钟速度最低应达到 2.5GHz。

表 *104:* 标准部署的用户登录重试限制（*15000* 位用户的完全 *UC* 主用/主用）

预期活动用户数量	重试下限	重试上限
完全 UC		
100	120	127
500	120	153
1000	120	187
1500	120	220

预期活动用户数量	重试下限	重试上限
2000	120	253
2500	120	287
3000	120	320
3500	120	353
4000	120	387
4500	120	420
5000	120	453
6000	120	520
7000	120	587
7500	120	620

15000 位用户的完全 UC (4 vCPU 8GB) 主用/备用配置文件

注意　为了在 15000 用户系统上获得最大客户端登录吞吐量，思科建议 CPU 时钟速度最低应达到 2.6GHz。

表 *105:* 标准部署的用户登录重试限制（*15000* 位用户的完全 *UC* 主用/备用）

预期活动用户数量	重试下限	重试上限
完全 **UC**		
100	120	137
500	120	203
1000	120	287
1500	120	370
2000	120	453
2500	120	537
3000	120	620
3500	120	703
4000	120	787
4500	120	870
5000	120	953

预期活动用户数量	重试下限	重试上限
6000	120	1120
7000	120	1287
8000	120	1453
9000	120	1620
10000	120	1787
11000	120	1953
12000	120	2120
13000	120	2287
14000	120	2453
15000	120	2620

25000 位用户的完全 UC (6 vCPU 16GB) 主用/主用配置文件

注意　为了在25000用户系统上获得最大客户端登录吞吐量，思科建议CPU时钟速度最低应达到2.8GHz。

表 *106:* 主用/主用配置文件的登录速率：*9* 使用 *45% CPU*

预期活动用户数量	重试下限	重试上限
100	120	131
500	120	176
1000	120	231
1500	120	287
2000	120	342
2500	120	398
3000	120	453
3500	120	509
4000	120	564
4500	120	620
5000	120	676

预期活动用户数量	重试下限	重试上限
6000	120	787
7000	120	898
7500	120	953
8000	120	1009
9000	120	1120
10000	120	1231
11000	120	1342
12000	120	1453
12500	120	1509

25000 位用户的完全 UC (6 vCPU 16GB) 主用/备用配置文件

注意 为了在25000用户系统上获得最大客户端登录吞吐量，思科建议CPU时钟速度最低应达到2.6GHz。

表 *107:* 主用/备用配置文件的登录速率：*16* 位用户 *80% CPU*

预期活动用户数量	重试下限	重试上限
100	120	133
500	120	183
1000	120	245
1500	120	308
2000	120	370
2500	120	433
3000	120	495
3500	120	558
4000	120	620
4500	120	683
5000	120	745
6000	120	870

预期活动用户数量	重试下限	重试上限
7000	120	995
8000	120	1058
9000	120	1120
10000	120	1245
11000	120	1370
12000	120	1495
13000	120	1620
14000	120	1870
15000	120	1995
16000	120	2120
17000	120	2245
18000	120	2370
19000	120	2495
20000	120	2620
21000	120	2745
22000	120	2870
23000	120	2995
24000	120	3120
25000	120	3245

XMPP 标准合规性

IM and Presence Service 与以下 XMPP 标准兼容：

- RFC 3920 可扩展消息传送和在线状态协议 (XMPP)：核心 RFC 3921 可扩展消息传送和在线状态协议 (XMPP)：即时消息和在线状态
  - XEP-0004 Data Forms
  - XEP-0012 Last Activity
  - XEP-0013 Flexible Offline Message Retrieval
  - XEP-0016 Privacy Lists

- XEP-0030 Service Discovery
- XEP-0045 Multi-User Chat
- XEP-0054 Vcard-temp
- XEP-0055 Jabber Search
- XEP-0060 Publish-Subscribe
- XEP-0065 SOCKS5 Bystreams
- XEP-0066 Out of Band Data Archive OOB requests
- XEP-0068 Field Standardization for Data Forms
- XEP-0071 XHTML-IM
- XEP-0082 XMPP Date and Time Profiles
- XEP-0092 Software Version
- XEP-0106 JID Escaping
- XEP-0114 Jabber Component Protocol
- XEP-0115 Entity Capabilities
- XEP-0124 Bidirectional Streams over Synchronous HTTP (BOSH)
- XEP-0126 Invisibility
- XEP-0128 Service Discovery Extensions
- XEP-0160 Best Practices for Handling Offline Messages
- XEP-0163 Personal Eventing Via PubSub
- XEP-0170 Recommended Order of Stream Feature Negotiation
- XEP-0178 Best Practices for Use of SASL EXTERNAL
- XEP-0220 Server Dialback
- XEP-0273 SIFT (Stanza Interception and Filtering Technology)

配置更改和服务重新启动通知

无论何时需要重新启动服务，系统都会弹出**活动通知**窗口。 Cisco Unified CM IM and Presence 管理 GUI 页眉的右上角有一个**活动通知摘要**。

此外，您还可以从 Cisco Unified CM IM and Presence 管理界面选择**系统** > **通知**，以访问活动通知列表。

需要重新启动的配置更改

对于许多 IM and Presence 配置更改和更新，您必须重新启动 Cisco XCP 路由器、Cisco SIP Proxy 或 Cisco Presence Engine。

下表显示了需要重新启动任何这些服务的配置更改。 此列表包含配置更改，但不包括平台更改，例如安装或升级。

需要重新启动的配置	重新启动此服务
应用侦听程序配置 （系统 > 应用侦听程序） 编辑应用侦听程序	Cisco SIP Proxy
符合性配置文件配置 （消息 > 合规性 > 合规性设置） （消息 > 合规性 > 合规性配置文件） 如果您要为分配给第三方合规性服务器的事件编辑设置	Cisco XCP 路由器
群聊系统管理员 （消息 > 群聊系统管理员） 如果您启用或禁用此设置	Cisco XCP 路由器
外部文件服务器配置 （消息 > 外部服务器设置 > 外部文件服务器） 如果您编辑**主机 /IP 地址设置** 如果您重新生成**外部文件服务器公钥**	Cisco XCP 路由器
群聊和永久聊天配置 （消息 > 群聊和永久聊天） 如果某个聊天节点在启动时无法接通其外部数据库，那么 Cisco XCP 文字会议管理器服务不会运行	Cisco XCP 路由器
群聊服务器别名映射 （消息 > 群聊服务器别名映射） 添加聊天别名	Cisco XCP 路由器
ACL 配置 （系统 > 安全 > 传入 ACL） （系统 > 安全 > 传出 ACL） 编辑传入或传出 ACL 配置	Cisco SIP Proxy

需要重新启动的配置	重新启动此服务
符合性设置 消息存档程序 - 编辑设置	Cisco XCP 路由器
LDAP 服务器 （应用程序 > 第三方客户端 > 第三方 LDAP 设置) LDAP 搜索 - 编辑 LDAP 搜索 从 LDAP 编辑构建 vCard 编辑用于 vCard FN 的 LDAP 属性	Cisco XCP 路由器
消息设置配置 （消息 > 设置） 编辑启用即时消息 抑制离线即时消息	Cisco XCP 路由器
在网状态网关 （Presence > 网关） 添加、编辑和删除 Presence 网关 上传 MS Exchange 证书后	Cisco Presence Engine
Presence 设置配置 （Presence > 设置 > 标准配置） 编辑启用可用性共享设置 允许用户在不提示其他用户批准的情况下查看其在线状态 最大联系人列表大小(每用户) 查看器最大数	Cisco Presence Engine Cisco XCP 路由器
Presence 设置配置 （Presence > 设置 > 标准配置） 编辑**针对域间联合使用电子邮件地址**字段	Cisco XCP 路由器
分区式域内联合配置 Presence > 设置 > 标准配置（复选框） Presence > 域内联合设置（向导） 通过复选框或向导启用 LCS/OCS/Lync 分区式域内联合 分区式域内路由模式 - 通过标准配置窗口或向导配置	编辑这些设置会导致 Cisco SIP Proxy 自动重新启动 此外，您必须重新启动 XCP 路由器

需要重新启动的配置	重新启动此服务
代理配置 （Presence > 路由 > 设置） 对代理配置的任何编辑	Cisco SIP Proxy
安全设置 （系统 > 安全 > 设置） 编辑任何 SIP 安全设置，例如 SIP 群集内代理到代理传输协议 编辑任何 XMPP 安全设置	Cisco SIP Proxy（适用于 SIP 安全编辑） Cisco XCP 路由器（适用于 XMPP 安全编辑）
SIP 联合域 （Presence > 域间联合 > SIP 联合） 添加、编辑、删除此配置	Cisco XCP 路由器
第三方合规性服务 （应用程序 > 第三方客户端 > 第三方 LDAP 服务器） 编辑主机名 /IP 地址、端口、密码/确认密码字段	Cisco XCP 路由器
TLS 对等机主题配置 （系统 > 安全 > TLS 对等主题） 此页面上的任何编辑	Cisco SIP Proxy
TLS 上下文 （系统 > 安全 > TLS 环境配置） 此页面上的任何编辑	您可能需要重新启动关联的聊天服务器
XMPP 联合 （Presence > 域间联合 > XMPP 联合 > 设置） （Presence > 域间联合 > XMPP 联合 > 策略） 对 XMPP 联合的任何编辑	Cisco XCP 路由器
群集间对等 （Presence 群集间） 编辑群集间对等配置	在某些情况下，您可能需要重新启动 Cisco XCP 路由器（右上角窗口中会显示一则通知）

需要重新启动的配置	重新启动此服务
以太网设置 （在 Cisco Unified IM and Presence 操作系统管理中，设置 > IP > 以太网/以太网 IPv6） 编辑任何以太网设置	导致系统立即重启
IPv6 配置 （系统 > 企业参数） 编辑启用 IPv6 企业参数	Cisco XCP 路由器 Cisco SIP Proxy Cisco Presence Engine
故障诊断 如果订阅方离线时 IM and Presence 发布方更改 编辑设置 > IP > 来自订阅方的发布方设置	重新启动订阅方节点
升级 IM and Presence 并且您需要切换到之前的版本	重新启动系统
重新生成 cup 证书	Cisco SIP Proxy Cisco Presence Engine
重新生成 cup-xmpp	Cisco XCP 路由器
重新生成 cup-xmpp-s2s 证书	Cisco XCP 路由器
上传新证书	重新启动该证书的相关服务。 对于 Cup-trust 证书，重新启动 Cisco SIP Proxy
远程审计日志传输协议 如果您运行任何 utils remotesyslog set protocol * CLI 命令	重新启动节点
如果您收到以下任何警报： • PEIDSQueryError • PEIDStoIMDBDatabaseSyncError • PEIDSSubscribeError • PEWebDAVInitializationFailure	建议重新启动 Cisco Presence Engine

需要重新启动的配置	重新启动此服务
如果您收到以下任何警报： • • XCPConfigMgrJabberRestartRequired • XCPConfigMgrR2RPasswordEncryptionFailed • XCPConfigMgrR2RRequestTimedOut • XCPConfigMgrHostNameResolutionFailed	建议重新启动 Cisco XCP 路由器
PWSSCBInitFailed	建议重新启动 Cisco SIP Proxy
编辑任何 Exchange 服务参数 • Microsoft Exchange 通知端口 • 日历范围 • Exchange 超时（秒） • Exchange 队列 • Exchange 线程 • EWS 状态频率	Cisco Presence Engine
上传 Exchange 证书	Cisco SIP Proxy Cisco Presence Engine
安装区域设置	重新启动 IM and Presence Service
创建新的 MSSQL 外部数据库	Cisco XCP 路由器
编辑外部数据库配置	Cisco XCP 路由器
合并外部数据库	Cisco XCP 路由器
配置 TLS 对等主题	Cisco SIP Proxy
配置对等验证 TLS 环境	Cisco SIP Proxy

需要重新启动的配置	重新启动此服务
编辑以下 Cisco SIP Proxy 服务参数： • CUCM 域 • 服务器名称（补充） • HTTP 端口 • 有状态服务器（事务有状态） • 永久 TCP 连接 • 共享内存大小（字节） • 联合路由 IM/P FQDN • Microsoft 联合用户-代理报头（逗号分隔）	Cisco SIP Proxy
编辑**路由通信类型**服务参数	Cisco XCP 路由器
编辑 IM 地址方案	Cisco XCP 路由器
分配一个默认域	Cisco XCP 路由器
从群集删除或移除节点	Cisco XCP 路由器
如果对影响 Cisco XCP 路由器的参数进行任何编辑，都必须重新启动 Cisco XCP 路由器	Cisco XCP 路由器
路由通信类型服务参数	Cisco XCP 路由器
编辑任一 Cisco XCP 文件传输管理器服务参数： • **外部文件服务器可用空间下限阈值** • **外部文件服务器可用空间上限阈值**	Cisco XCP 路由器
编辑**启用多设备消息传送**服务参数	Cisco XCP 路由器
编辑**每用户最大登录会话数**服务参数	Cisco XCP 路由器
更新外部数据库上的 `install_dir /data/pg_hba.conf` 或 `install_dir /data/postgresql.conf` 配置文件	Cisco XCP 路由器
迁移实用程序： • 编辑“Presence 设置”窗口中的**允许用户查看其他用户的可用性而不收到批准提示**设置。 • 编辑“Presence 设置”配置窗口中的**最大联系人列表大小(每用户)**和**查看器最大数(每用户)**设置。	Cisco XCP 路由器

需要重新启动的配置	重新启动此服务
从群集删除或移除节点	Cisco XCP 路由器

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。