Cisco WebEx Meetings Server 发行版 2.8 规划指南和系统要求

首次发布日期: 2016 年 11 月 01 日

上次修改日期: 2017 年 04 月 14 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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 录

常规系统要求 1

Cisco WebEx Meetings Server 最佳实践 6

WebEx 快捷会议工具 7

用户 7

系统的部署规模 8

vCenter 并存的要求 8

系统中的虚拟机 8

最低硬件要求 9

CWMS 和 ESXi 主机耗用的资源 11

50 个用户的系统 12

250 个用户的系统 15

800 个用户的系统 17

2000 个用户的系统 20

系统容量矩阵 25

支持的升级路径 27

支持的升级路径 29

Cisco WebEx Meetings Server 简介 33

Cisco Unified MeetingPlace 客户须知 34

部署单数据中心 35

加入单数据中心以创建多数据中心 (MDC) 系统 35

将 VMware vSphere 与系统配合使用 35

在 VMware vSphere 上部署系统的优点 36

IOPS 和存储系统性能 38

安装 VMware vSphere ESXi 和配置存储空间 39

加入会议 40

网络中的虚拟机布局 43

不同类型的系统网络拓扑结构 44

内部互联网反向代理 (IRP) 网络拓扑 44
非水平分割网络拓扑 45
全内部网络拓扑 46
水平分割网络拓扑 47
HA 或 MDC 部署中的冗余 49
互联网反向代理的网络注意事项 50
网络带宽要求 52
多数据中心的网络要求 56
用于带宽聚合的 NIC Teaming 56
负载平衡 58
系统的网络核对表 59
采用自动部署并包含公开访问的安装或扩展的网络核对表 60
采用手动部署并包含公开访问和所有内部虚拟机的安装或扩展的网络核对表 62
采用自动部署并包含公开访问和非水平分割 DNS 的安装或扩展的网络核对表 65
采用手动部署并包含公开访问和非水平分割 DNS 的安装或扩展的网络核对表 68
采用自动部署并包含公开访问和水平分割 DNS 的安装或扩展的网络核对表 71
采用手动部署并包含公开访问和水平分割 DNS 的安装或扩展的网络核对表 73
采用自动部署且无公开访问的安装或扩展的网络核对表 76
采用手动部署且公开访问的安装或扩展的网络核对表 78
WebEx 站点和 WebEx 管理 URL 80
当所有虚拟机都位于内部网络中时的端口访问 82
DMZ 网络中的互联网反向代理的端口访问 82
外部防火墙中的端口访问 82
内部防火墙中的端口访问 83
VMware vCenter 端口 86
Cisco WebEx Meeting Center 端口 88
对系统采用 NAT 88
正向代理 91
配置 Cisco Unified Communications Manager (CUCM) 93
MDC 环境中的 CUCM 94
准备工作 94
MDC 环境中的 CUCM 安全电话会议 95

多数据中心的 CUCM 配置核对表 95
具有或不具有高可用性的 CUCM 配置核对表 95
在 CWMS 多数据中心系统中配置 CUCM 96
在 250 个或 800 个用户的多数据中心系统中配置 CUCM 97
在 2000 个用户的多数据中心系统中配置 CUCM 98
为高可用性和非高可用性系统配置 CUCM 99
在不具有高可用性系统的 50 个、250 个和 800 个用户的系统上配置 CUCM 99
在具有高可用性系统的 50 个、250 个或 800 个用户的系统上配置 CUCM 100
在不具有高可用性系统的 2000 个用户的系统上配置 CUCM 101
在具有高可用性系统的 2000 个用户的系统上配置 CUCM 102
配置 SIP 中继安全配置文件 103
为负载平衡服务器配置 SIP 中继安全配置文件 103
为应用程序服务器配置 SIP 中继安全配置文件 104
配置 SIP 配置文件 104
配置标准 SIP 配置文件 104
配置 TLS SIP 配置文件 105
配置 IPv6 SIP 配置文件 105
使用 TLS 进行 CUCM 证书管理 106
上传 Cisco WebEx Meetings Server 证书 106
安装第三方 CUCM 证书 107
下载 CUCM 证书 108
生成证书签名请求 (CSR) 2.6 版和更高版本 109
生成证书签名请求 (CSR) 2.5 版和更低版本 110
配置 SIP 中继 112
在负载平衡服务器上配置 SIP 中继 113
为应用程序服务器配置 SIP 中继 114
配置路由组 115
配置路由列表 116
配置路由模式 117
配置 SIP 路由模式 117
CUCM 功能兼容性和支持 118
音频端点兼容性 120

关于应用程序下载 123
从管理站点下载应用程序 124
应用程序 ZIP 文件的内容 125
应用程序语言代码 125
快捷会议工具 ZIP 文件内容 125
WebEx Meetings 客户端 ZIP 文件内容 126
网络录制文件播放器 ZIP 文件内容 127
Cisco WebEx 快捷会议工具的大规模部署 127
使用命令行对快捷会议工具执行无提示安装 128
使用命令行界面对快捷会议工具执行无提示删除 129
使用 SMS 进行 CWMS 应用程序的无提示安装时的限制 129
使用 SMS 每系统无人参与程序播发 WebEx 快捷会议工具 129
使用 SMS 每系统无人参与程序删除快捷会议工具组件 131
使用 SMS 每系统无人参与程序添加快捷会议工具 132
使用 SMS 每系统卸载程序卸载快捷会议工具 133
播发程序以更新新版本的 WebEx 快捷会议工具 133
从定义创建程序包 134
Meetings 应用程序的大规模部署 134
安装 Cisco WebEx Meetings 134
在本地卸载 Cisco WebEx Meetings 135
使用命令行对会议应用程序执行无提示安装 136
使用命令行界面对 WebEx Meetings 应用程序执行无提示删除 136
使用 SMS 进行 CWMS 应用程序的无提示安装时的限制 136
使用 SMS 每系统无人参与程序播发 CWMS 137
使用 SMS 每系统卸载程序卸载 Cisco WebEx Meetings 应用程序 138
网络录制文件播放器的大规模部署 138
安装网络录制文件播放器 138
使用命令行对录制文件播放器执行无提示安装 139
使用命令行界面对录制文件播放器执行无提示卸载 139
使用 Microsoft Systems Management Server 2003 (SMS) 安装 CWMS 应用程序 140
使用 SMS 进行 CWMS 应用程序的无提示安装时的限制 140
使用 SMS 每系统无人参与程序播发 Cisco WebEx 网络录制文件播放器 140

使用 SMS 每系统卸载程序卸载 Cisco WebEx 网络录制文件播放器 141
执行更新之后重新配置设置 142
单点登录概述 143
单点登录的好处 144
设置 SAML 2.0 单点登录概述 145
用于最终用户和管理登录的 SAML SSO 146
云模式 WebEx 会议服务和 WebEx Meetings Server 在 SAML 2.0 单点登录方面的不同 146
SAML 声明属性 149
支持的 SAML 声明属性 150
可选参数 153
时区值 153
国家/地区代码值 157
地区值 166
语言值 168
语言代码 168
会议录制文件的存储要求 171
系统备份文件的存储要求 172
支持的 SNMP MIB 173
CWMS 系统信息 MIBS 173
与 CPU 相关的 MIB 174
CWMS 内存信息 176
磁盘使用情况 177
支持的 SNMP 陷阱 177
通知事件 178
陷阱数据 179
常见 PC 系统要求 181
对于 Windows 的操作系统要求 182
对于 MAC 的操作系统要求 185
移动设备的操作系统要求 186
Citrix XenDesktop 和 XenApp 支持 186
Cisco WebEx Meetings 应用程序和快捷会议工具兼容性矩阵 187
关于主持人许可证 189

Cisco Unified Communications Manager (CUCM) 集成 **191**

Session Manager Edition (SME) 集成 **191**

音频端点兼容性 **192**

第 1 章

常规系统要求

Cisco WebEx Meetings Server (CWMS) 兼容满足或超出本节中所述的规格的 Cisco UCS 服务器。

重要事项

从 CWMS 发行版 1.x 升级到发行版 2.0 或发行版 2.5 等主发行版时，管理虚拟机所在的 ESXi 主机（Cisco UCS 服务器）需要最低 1.5 TB 的可用磁盘空间。 请参阅本文档中描述不同大小用户系统的部分，从 50 个用户的系统，第 12 页 开始。 在升级过程中，您的网络上将同时存在两组虚拟机；运行发行版 1.x 的原始虚拟机和支持新版本的升级虚拟机。 有关更多详细信息，请参阅《CWMS 管理指南》中的“升级系统”一节：http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html。

模块	要求说明
主机服务器和处理器	• Cisco UCS *C* 系列机架服务器或等效的 *B* 系列刀片服务器。 • 支持 AES NI 指令集。 • 2.4 GHz 或更快的处理器时钟速度。 **注释** 不支持第三方硬件。
网络接口 ESXi 主机（适用于 Cisco WebEx Meetings Server 虚拟机）和以太网交换机之间的 NIC（不适用于外部网络接口）。	• 非冗余配置最少有 1 个物理 NIC。 请参阅50 个用户的系统，第 12 页部分，以了解互联网反向代理 (IRP) 和管理虚拟机共享一个主机的特殊要求。 • 冗余配置必须复制（联合或接合）所有 NIC 接口，并将它们连接到独立的交换网。 • 对于 VMware 管理网络，增加一个 NIC（可选）。

模块	要求说明
[1]用于部署内部虚拟机的 ESXi 主机的内部 (DAS) 存储空间	• 至少有 4 个驱动器为 RAID-10 或 RAID-5 配置 • 至少 1.5 TB 可用存储空间用于新系统部署或升级。 • 如果将 CWMS 从发行版 1.X 升级到发行版 2.X，ESXi 主机需要 172 至 1118 GB 可用磁盘空间，具体取决于系统的大小和虚拟机。请参阅本文档中描述不同大小用户系统的部分，从50 个用户的系统，第 12 页开始。 • 第二个用于 ESXi 的磁盘阵列（可选） 注释 虚拟机必须使用密集配置来存储。
用于部署 IRP 虚拟机的 ESXi 主机的内部 (DAS) 存储空间	• 至少有 2 个驱动器为 RAID-1 配置 • 最少 300 GB 可用存储空间 • 可使用与内部虚拟机相同的配置。 注释 虚拟机必须使用密集配置来存储。

模块	要求说明
SAN 存储	• 可用作 DAS 的替代。（我们建议分配相同数目的存储空间。） • B 系列刀片服务器仅有两个硬盘驱动器。 如果是在使用 Cisco UCS B 系列刀片服务器且计划升级到 CWMS 发行版 2.X，您必须使用 SAN 存储来满足 RAID 5 或 RAID 10 配置所要求的 4 个硬盘驱动器的条件。 • 建议仅在配备了有监控和调整 SAN 性能经验的支持人员的部署中使用。 注释 您负责根据新的 VMware 要求和系统的未来扩展添加存储器。 • 仅用于光纤通道 (FC) 或 10 GB 以太网光纤通道 (FCoE)。 • 性能要求与 DAS 相同。 • 如 vSphere 所测量的，最大允许总体延迟为 20 毫秒。有关更多信息，请参阅存储空间部分 (http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware#Storage)。 • 虚拟机所需的空间总量： 为 CWMS 系统中每台虚拟机预留的存储资源总量。 注释 虚拟机必须使用密集配置来存储。

模块	要求说明
[2]NAS 存储	• 可用作 DAS 或 SAN 的替代。（我们建议分配相同数目的存储空间。） • 建议将 NAS 存储服务器与 Cisco UCS C 系列机架服务器一起使用。 • 建议仅在配备了有监控和调整 NAS 性能经验的支持人员的部署中使用。 您应负责针对新的 VMware 要求和系统的未来扩展添加更多存储器。 • 仅光纤通道 (FC)、网络文件系统 (NFS) 或 SCSI。 有关更多信息，请参阅 http://docwiki.cisco.com/wiki/UC_Virtualization_Storage_System_Design_Requirements#General_Guidelines_for_SAN.2FNAS。 • 性能要求与 DAS 相同。 • 如 vSphere 所测量的，最大允许总体延迟为 20 毫秒。有关更多信息，请参阅http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware#Storage。 • 虚拟机所需的空间总量： 为 CWMS 系统中每台虚拟机预留的存储资源总量。 • 文件服务器必须支持用于阵列集成的 vStorage API (VAAI) 并使用密集配置。 **注释** 虽然 NAS 存储的缺省配置方案是精简配置，虚拟机也必须使用密集配置来存储。 （不支持精简配置。）为启用密集配置来部署 NAS 存储，必须在 Cisco WebEx Meetings Server 部署中使用的所有 UCS 服务器上安装存储供应商为 VAAI 提供的插件。

模块	要求说明
虚拟机监控程序	有关 ESXi 版本和 vSphere 许可证，请参阅最低硬件要求，第 9 页一节。 需要使用 VMware Vsphere，它也是唯一受支持的产品；不支持其他虚拟机监控程序产品。 vCenter Server 5.0、5.0 Update 1、5.0 Update 2、5.1、5.1 Update 1、5.5 和 6.0（CWMS 2.6MR1 和更高版本） 最低硬件要求部分中描述了 vSphere 许可证。 每个处理器插座一个 VMware 许可证。 共驻内存： • 如果系统要求中包含了处理器和内存要求，则vCenter 可与 CWMS 共驻内存。 • 仅对 50 和 250 个用户的系统支持 vCenter 共驻内存配置。 • 不支持在同一物理 ESXi 主机上与 Cisco Unified Communications 产品共驻内存。 • 不支持在同一物理 ESXi 主机上与非 CWMS 虚拟机共驻内存。 不支持分布式资源调度程序 (DRS)、克隆、容错 (FT) 和系统启动时的 vMotion 或 Storage vMotion 等高级 VMware vSphere 功能。
电子邮件服务器	• 系统用于发送电子邮件的邮件服务器的标准域名 (FQDN)。 • 端口号 - SMTP 端口号缺省值为 25 或 465（安全 SMTP 端口号）。 • 要将启用 TLS 的电子邮件服务器与第三方证书一起使用，必须将证书导入系统。有关更多信息，请参阅管理指南中的“管理证书”：http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html。
许可证	MDC 许可证 - 多数据中心系统中的每个数据中心都需要 MDC 许可证。 单数据中心系统无需 MDC 许可证。 主持人许可证 - 要开始 WebEx 网络会议、WebEx 音频会议、群拨会议或个人会议，每个要主持会议的用户都必须拥有主持人许可证。有关主持人许可证的更多信息，请参阅关于主持人许可证，第 189 页。

1 如果贵公司有管理存储区域网络 (SAN) 方面的专长，我们建议使用 SAN，而不是使用直连存储 (DAS)。 SAN 可以比本地磁盘阵列更可靠。
2 确保网络文件系统 (NFS) 有足够的存储容量存储数据库和会议录制文件的定期自动备份。 （CWMS 支持 NFS 版本 2、3 和 4。）

- Cisco WebEx Meetings Server 最佳实践， 第 6 页
- WebEx 快捷会议工具， 第 7 页
- 用户， 第 7 页
- 系统的部署规模， 第 8 页
- vCenter 并存的要求， 第 8 页
- 系统中的虚拟机， 第 8 页
- 最低硬件要求， 第 9 页
- 系统容量矩阵， 第 25 页
- 支持的升级路径， 第 27 页
- 支持的升级路径， 第 29 页

Cisco WebEx Meetings Server 最佳实践

以下列出配置和维护 Cisco WebEx Meetings Server 系统时应参考的最佳实践：

- 使用不间断电源 (UPS) 为虚拟机主机供电，以大大减少电源中断状况。 重复启动失败可能损坏主机系统和虚拟机。
- 关闭客户机操作系统之前务必将系统切换到维护模式。
- 对于计划事件和其他要求系统关机的状况，请通过关闭客户机操作系统正常关闭虚拟机。
- 系统设计为必要时自行修复并且重新启动可以中断此过程。 我们不建议您重新启动系统来对其进行修复。 如果系统处于不正常状况，请联系 Cisco TAC。 仅在要求时或在数据中心维护等计划事件中才关闭系统。
- 配置网络冗余以减少网络故障。 请参阅《*Cisco WebEx Meetings Server* 管理指南》中的“添加高可用性系统”以获取更多信息。
- 在虚拟机中使用快照可能会影响系统性能，甚至在系统负载较轻时也影响用户体验。
- 如果系统存在问题，务必检查 VMware VCenter 环境，以确定是否因 VCenter 或网络中的状况导致问题。
- 配置高可用性以提高系统在发生故障后仍能继续运行的可能性。
- 如果您有高可用性系统并且备用系统发生故障，则可以通过删除现有的备用系统（请参阅《*Cisco WebEx Meetings Server* 管理指南)》中的“删除高可用性系统”）并添加新的备用系统（请参阅《*Cisco WebEx Meetings Server* 管理指南》中的“添加高可用性系统”）对其进行修复。 如果高可用性系统上的主系统发生故障，则无法使用此过程对其进行修复。我们建议您使用灾难恢

复过程恢复主系统，然后添加新的备用系统。 在您添加新的备用系统之前，部署会在无完整冗余的状况下运行。 如果任意备用虚拟机发生故障，此过程有助于防止非计划中断。 请参阅《*Cisco WebEx Meetings Server* 管理指南》中的“使用灾难恢复功能”获取更多信息。

- 由于系统仅在NFS上保留最新的系统备份并且每天删除之前的实例，我们建议您在其他介质上保留若干最近的备份。

限制 请勿在 Cisco WebEx Meetings Server 使用的 NFS 共享中手动创建文件或目录，因为它会在 NFS 文件和目录上运行各种脚本。 NFS 存储服务器必须为 Cisco WebEx Meetings Server 专用。

- 用控制板监控 NFS、CPU 和存储器的健康状况。 我们建议启用存储器和 CPU 的控制板警报。
- 如果计划使用目录集成，请参阅《*Cisco WebEx Meetings Server* 管理指南》中“管理用户”一章的“配置目录集成”一节获取更多信息。
- 使用 Cisco WebEx Meetings Server 时，对于 CallManager 服务界面中 CUCN 上相关的 SIP 中继，应该取消勾选**需要媒体终止点**复选框（在**中继配置**页面上）。 有关更多详细信息，请参阅在负载平衡服务器上配置 SIP 中继，第 113 页和为应用程序服务器配置 SIP 中继，第 114 页。
- 如果想运行 Cisco WebEx Meetings Server 发行版 2.0 或更高版本并使用 B 系列刀片服务器，您需要使用 SAN 存储器以满足硬盘要求。 有关 SAN 要求的更多信息，请参阅常规系统要求，第 1 页。

WebEx 快捷会议工具

WebEx 快捷会议工具允许用户从应用程序（如 Microsoft® Outlook®）启动、安排或加入 WebEx Meetings 会话. 有关 Cisco WebEx 快捷会议工具的更多信息，请访问 http://www.webex.com/support/productivity-tools.html。

Cisco WebEx Meetings Server 支持最新版本的 WebEx 应用程序，它可在**设置** > **下载**页面获得。 如果在您执行系统升级后用户仍运行旧版本的 WebEx 快捷会议工具，他们可以安排、开始和加入会议，但无法使用最新的功能。 为获得最佳体验，建议您以无提示方式推送最新的 WebEx 快捷会议工具 .msi。 （请参阅Cisco WebEx Meetings 应用程序和快捷会议工具兼容性矩阵，第 187 页。）

用户

系统在使用期内支持最多 400000 个用户帐户。 此数字代表活动和停用的用户帐户总数。 这个使用期最大值足以容纳用户数据库的预期增长。

管理员无法从系统中删除用户。相反，用户被停用。此设计使管理员能够重新激活之前停用的用户帐户（即使在用户长期不活动之后）。 这将还原用户的会议和其他内容（包括录制文件）。

系统的部署规模

在确定系统的容量时，请考虑在特定时间预计使用系统的用户数。 例如，在 50 个用户的系统中，能同时出席会议的最大用户数为 50。 如果有 50 多个用户试图加入会议，则在超出最大用户数后将为所有试图加入会议的用户显示错误消息，并禁止这些用户加入会议。

- 50 个用户的系统， 第 12 页
- 250 个用户的系统， 第 15 页
- 800 个用户的系统， 第 17 页
- 2000 个用户的系统， 第 20 页

以下是在确定系统规模时需要考虑的一些因素：

- 确定在任何给定时间预期加入会议的最大用户数，包括极少或异常的情况下。
- 只要您的硬件满足或超过扩展后的系统的最低要求，便可以随时扩展系统；否则，您必须购买额外的硬件。
- 如果您计划为系统添加高可用性 (HA) 或多数据中心 (MDC)，请在购买硬件时把需要用来支持 HA 或 MDC 系统的额外的虚拟机考虑在内。
-

vCenter 并存的要求

在某些情况下，VMware vCenter Server 或 vCenter Server Appliance 可以与其他虚拟机或与 Cisco WebEx Meetings Server (CWMS) 虚拟机一起驻留。

在 50 或 250 个用户的系统上，VMware vCenter 可以与 CWMS 驻留在相同的主机上。 但是必须为 Cisco UCS 服务器订购或安装更多内存。 有关所需的确切内存容量，请参阅最低硬件要求中对于该系统大小的要求。

系统中的虚拟机

这些是为系统创建的虚拟机。 为了尽量减小系统容量，一些功能合并在一个虚拟机中。

- 管理 — 系统的心脏节点。 包括系统数据库并提供管理功能。
- 媒体 — 提供媒体服务（音频-视频功能、电话服务和会议服务）。

  包含在 50 个并发用户系统的管理虚拟机中。
- Web — 提供 Web 服务（会议列表和录制文件）。 使用户能够安排将来的会议。

  包含在 50、250 或 800 个并发用户系统的管理虚拟机中。

最终用户登录 WebEx 网站。 管理员登录管理网站。

- 互联网反向代理 (IRP) — 提供公开访问，让用户能够通过互联网和移动设备主持或参加会议。互联网反向代理是移动办公人员参加会议所必需的。

注释 此系统中只能使用随本产品一起提供的 IRP。 不支持其他供应商提供的互联网反向代理或 Web 负载平衡器。 随本产品一起提供的 IRP 已经过优化，可用于处理从互联网加入会议的外部用户产生的实时 Web、音频和数据共享流量。

注释 在本文档中，我们使用术语内部虚拟机指代管理虚拟机及适用的媒体和 Web 虚拟机。

IRP 位于 DMZ 网络（非水平分割和水平分割网络拓扑）或内部网络（全内部网络拓扑）中。

- 非水平分割网络拓扑， 第 45 页
- 水平分割网络拓扑， 第 47 页
- 内部互联网反向代理 (IRP) 网络拓扑， 第 44 页

最低硬件要求

本节列出了一些可供不同规模的系统使用的 Cisco UCS 服务器。 有关每个系统的具体要求，请参阅：

- 50 个用户的系统
- 250 个用户的系统
- 800 个用户的系统
- 2000 个用户的系统

另请参见《Cisco WebEx Meetings Server 订购指南》 (http://www.cisco.com/c/en/us/products/conferencing/webex-meetings-server/sales-resources-listing.html)。

表 *1*：*ESXi* 版本和许可证类型

系统容量	**ESXi** 版本	**vSphere** 许可证类型
50 或 250	5.0、5.0 Update 1、5.1、5.5 或 6.0	Standard Edition、Enterprise Edition、Enterprise Plus Edition

系统容量	**ESXi** 版本	**vSphere** 许可证类型
800 或 2000	5.0 或 5.0 Update 1	仅限 Enterprise Plus Edition
	5.1 至 5.5[3]	Enterprise Edition、Enterprise Plus Edition
	5.5 或更高版本[1]	Standard Edition、Enterprise Edition、Enterprise Plus Edition
	6.0	Standard Edition、Enterprise Edition、Enterprise Plus Edition

[3] “或更高版本”表示更新，而不是完整的版本。 例如，5.5 Update 1 或 5.1 Update 2。

表 *2*：主机模式

部署规模	**UCS** 型号的示例
50 个用户	• UCS C220 M3 • UCS B200 M3 • UCS C220 M4S • C240 M4S2
250 个用户	• UCS C220 M3 • UCS B200 M3 • UCS C220 M4S • C240 M4S2
800 个用户	• UCS C460 M2 • UCS B440 M2 • UCS B420 M3（2.0 和更高版本）
2000 个用户	• UCS C460 M2 • UCS B440 M2 • UCS B420 M3（2.0 和更高版本）

仅支持在 50 个和 250 个用户的系统部署中与 vCenter 共驻内存。 不支持在同一物理主机上与 Cisco Unified Communications 产品共驻内存。

您可以在系统中使用 UCS 硬件的旧模式，但为得到更好的用户体验，请使用表中列出的硬件。 例如，您可对 250 个用户的系统使用 UCS C220 M3，前提是已有该硬件。

升级到 Cisco WebEx Meetings Server 发行版 2.0 或更高版本时，可以使用 Cisco UCS B200 M3 刀片服务器和两个本地硬盘驱动器，前提是升级后的系统的虚拟机使用 SAN 存储。 使用 SAN 存储和 B 系列刀片服务器时，系统可以满足 Cisco WebEx Meetings Server 的 RAID 5 或 RAID 10 配置要求中所需的 4 个硬盘驱动器。

注释 对于运行 2.0 和更高版本的 800 个和 2000 个用户的系统，我们建议不要在 DMZ 主机上部署其他虚拟机。 这可能导致丢包率增加而且媒体连接上出现明显的延迟。

CWMS 和 ESXi 主机耗用的资源

Cisco WebEx Meetings Server 部署在 ESXi 主机上的一个或多个虚拟机上。 Cisco WebEx Meetings Server (CWMS) 和 ESXi（在物理 Cisco UCS 服务器上启用虚拟化的 VMware 组件）会消耗 CPU 和内存资源以及存储空间。 根据系统容量，同一台 Cisco UCS 服务器上可能运行 vCenter 和多个虚拟机。

CWMS 对其虚拟机使用资源保留以保证系统可扩展性。 其他 VMware 工作负载不会占用虚拟机的 CPU 和其他资源。 每种系统大小的最低要求包含了足以支持下列目标的资源：

- CWMS 在系统使用率达到峰值（最大容量）时保持服务质量。
- VMware ESXi。
- VMware vCenter（共驻内存时）。

  有关 vCenter Server 的要求，请参阅知识库并分别搜索“安装 vCenter Server 5.0 最佳实践”、“安装 vCenter Server 5.1 最佳实践”或“安装 vCenter Server 5.5 最佳实践”。
- 虚拟机的 VMware 快照（请尽快删除这些快照，否则性能可能严重下降）。

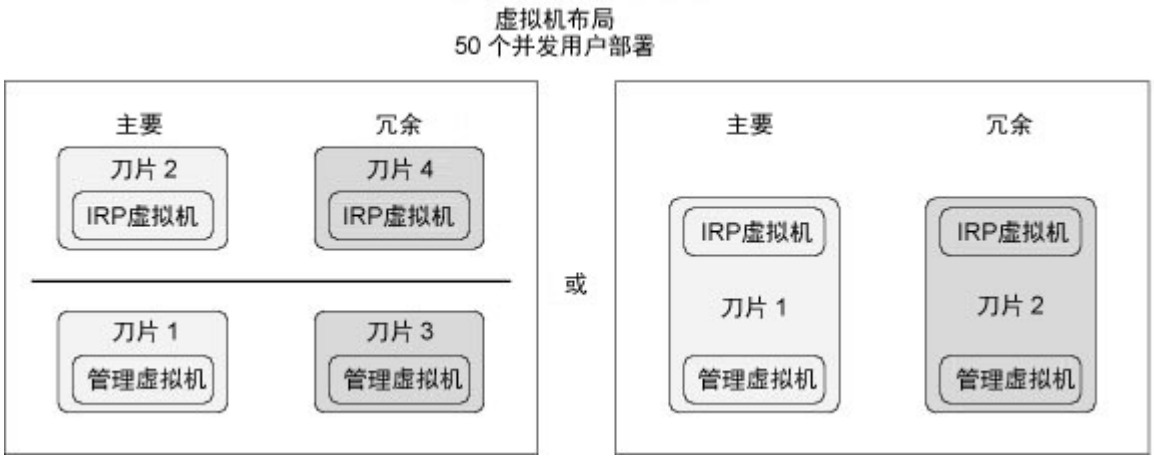
  快照需要额外的磁盘空间，因为有些快照可能和原始虚拟机一样大。 在某些情况下，vSphere 可能会删除快照以释放存储空间，但这会影响回滚到先前快照的能力。
- Cisco UCS 服务器在服务器典型生命周期中的使用。

OVA 文件中指定的硬件要求是部署 Cisco WebEx Meetings Server 所需的最低要求。 这些要求不包括 VMware vCenter 或 ESXi 的任何 CPU、内存或存储要求。

注意 除了本文档的表格中列出的配置外，不支持共驻内存。 如果您无视我们的系统要求，您的虚拟机可能无法启动。 在 vCenter OVA 部署期间，虚拟机部署可能在最初的几个产品屏幕显示时就停滞。

50 个用户的系统

50 个用户的系统也称为微型系统。（微型系统不能使用多数据中心 (MDC)。）下图展示了 50 个用户部署的两个版本。（“冗余”虚拟机支持高可用性 (HA)。）



下表列出了系统中 ESXi 主机（Cisco UCS 服务器）的最低硬件要求。 最后两列显示新安装 Cisco WebEx Meetings Server 需要的磁盘空间量，以及使用现有 Cisco UCS 服务器并利用自动升级功能将 Cisco WebEx Meetings Server 发行版 1.5MR3 升级到发行版 2.X 时需要的可用磁盘空间。 有关更多信息，请参阅常规系统要求。

有关带宽要求的信息，请参阅网络带宽要求，第 52 页。

注释 有关 IOPS 的信息，请参阅在 VMware vSphere 上部署系统的优点，第 36 页。

仅支持按下表配置的 50 个用户的系统部署与 vCenter 共驻内存。

ESXi 主机（Cisco UCS 服务器）上的虚拟机	CPU 核心数	内存 (GB)	以太网端口	新安装的硬盘存储要求	从 1.5MR3 自动升级到 2.X 所需的可用硬盘存储空间[4]
管理虚拟机	4 (ESXi 5.0) 6（ESXi 5.1 及更高版本）	24	对于管理虚拟机，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） 对于 ESXi 管理网络，建议使用 1 个端口	1.5 TB；至少 7,200 RPM	1118 GB（自动安装）。

ESXi 主机（Cisco UCS 服务器）上的虚拟机	CPU 核心数	内存 (GB)	以太网端口	新安装的硬盘存储要求	从 1.5MR3 自动升级到 2.X 所需的可用硬盘存储空间[4]
管理虚拟机和 vCenter（共驻内存）	6 (ESXi 5.0) 8（ESXi 5.1 及更高版本）	36	对于管理虚拟机，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） 对于 vCenter，建议使用 1 个端口 对于 ESXi 管理网络，建议使用 1 个端口	1.5 TB；至少 7,200 RPM	1,078 GB 此数字基于您已用 40 GB 安装 vCenter 的假设。
互联网反向代理 (IRP)	4 (ESXi 5.0) 6（ESXi 5.1 及更高版本）	12	对于 IRP 虚拟机，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） 对于 ESXi 管理网络，建议使用 1 个端口	300 GB；至少 7,200 RPM	172 GB
管理虚拟机和 IRP（共驻内存）	8	36	对于管理虚拟机，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） 对于 IRP 虚拟机，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） 对于 ESXi 管理网络，建议使用 1 个端口	1.5 TB；至少 7,200 RPM	990 GB

ESXi 主机（Cisco UCS 服务器）上的虚拟机	CPU 核心数	内存 (GB)	以太网端口	新安装的硬盘存储要求	从 1.5MR3 自动升级到 2.X 所需的可用硬盘存储空间[4]
虚拟机、IRP 和 vCenter（全部共驻内存）	12	40	对于管理虚拟机，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） 对于 IRP 虚拟机，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） 对于 vCenter，建议使用 1 个端口 对于 ESXi 管理网络，建议使用 1 个端口	1.5 TB；至少 7,200 RPM	950 GB 此数字基于您已用 40 GB 安装 vCenter 的假设。

4 如果选择“手动升级”（即手动部署所有虚拟机）且使用相同的硬件，则所需的可用空间将是自动升级时的两倍。

注释 如果计划使用高可用性 (HA) 系统，则对应主系统的硬件要求及其数量应翻倍，以支撑这两个系统。

在 50 个用户的系统中由虚拟机保留的资源

本节说明虚拟机使用多少介质并且适用于掌握 VMware 专业知识的人员。 CPU 资源是以 vCPU 数（核心数）和 MHz（CPU 周期）的形式指定的。 VMware VMkernel 使用 MHz 周期控制 CPU 调度。

内存资源是按最大内存和保留内存指定的。 保留内存不与同一物理 Cisco UCS 服务器上的其他虚拟机共享。

对磁盘资源（存储）的控制分为两个方面。 在 OVA 构建期间，CentOS 文件系统分区大小决定最小磁盘大小。 其次，vCenter 控制可用的最大磁盘空间。

如果您尝试部署未达到最低 vCPU 数量的虚拟机，那么虚拟机的 OVA 部署将失败。 如果您尝试部署处理器速度未达到最低总 MHz 要求的虚拟机，那么虚拟机将不会启动。

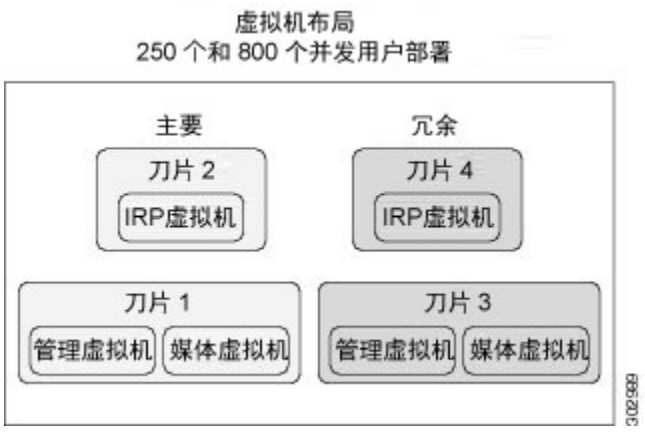
重要事项 本表中的数字不包括 VMware ESXi 或 vCenter 的资源。 请参阅CWMS 和 ESXi 主机耗用的资源，第 11 页。

虚拟机类型	虚拟 CPU (vCPU)	CPU[5](MHz)	保留内存/总内存[6](GB)	磁盘 (GB)
管理虚拟机	4	8000	12/14	418
互联网反向代理	4	8000	4/4	128

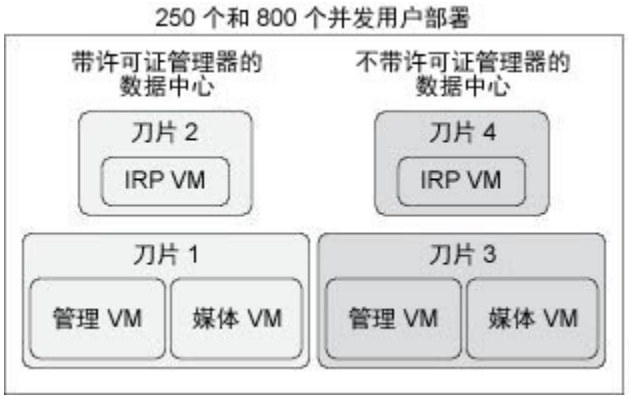
5 将物理 CPU 数乘以 CPU 芯片的速度 (MHz) 得到的数字。 此计算中不考虑超线程。 （物理 CPU 的时钟速度必须为 2.4 GHz 或更快。）
6 有媒体功能的虚拟机可以有附加的非保留内存；内存 = 保留/总计

250 个用户的系统

250 个用户的系统也称为小型系统。 下图展示了 250 个用户的系统部署的两个版本。 “冗余”虚拟机支持高可用性 (HA)。 如果您的系统不支持 HA，则只部署主系统。



本图显示 250 用户系统的布局，它的两个数据中心构成了一个多数据中心 (MDC) 系统，且支持互联网反向代理 (IRP)。 许可证管理器仅在一个数据中心上运行。



下表列出了系统中 ESXi 主机（Cisco UCS 服务器）的最低硬件要求。 最后两列显示新安装 Cisco WebEx Meetings Server 需要的磁盘空间量，以及使用现有 Cisco UCS 服务器并利用自动升级功能将 Cisco WebEx Meetings Server 发行版 1.5MR3 升级到发行版 2.X 时需要的可用磁盘空间。 有关更多信息，请参阅常规系统要求。

有关带宽要求的信息，请参阅网络带宽要求，第 52 页。

有关 IOPS 的信息，请参阅在 VMware vSphere 上部署系统的优点，第 36 页。

仅支持按下表配置的 250 个用户的系统部署与 vCenter 共驻内存。

ESXi 主机（**Cisco UCS** 服务器）上的虚拟机	**CPU** 核心数	内存 **(GB)**	以太网端口	新安装的硬盘存储要求	从 **1.5MR3** 自动升级到 **2.X** 所需的可用硬盘存储空间[7]
管理和媒体虚拟机	12	52	• 对于管理和媒体虚拟机，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） • 对于 ESXi 管理网络，建议使用 1 个端口	1.5 TB；至少 7200 RPM	990 GB
（管理和媒体虚拟机）以及 vCenter（共驻内存）	16	56	• 对于管理和媒体虚拟机，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） • 对于 ESXi 管理网络，建议使用 1 个端口 • 对于 vCenter，建议使用 1 个端口	1.5 TB；至少 7200 RPM	950 GB （此数字基于您已用 40 GB 安装 vCenter 的假设。）
互联网反向代理 (IRP)	12	36	• 对于 IRP，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） • 对于 ESXi 管理网络，建议使用 1 个端口	300 GB；至少 7200 RPM	172 GB

7 如果选择“手动升级”（即手动部署所有虚拟机）且使用相同的硬件，则所需的可用空间将是自动升级时的两倍。

注释 如果计划使用 HA 系统，请为 HA 系统购买与主系统相同的硬件，数量也相同。

在 250 个用户的系统中由虚拟机保留的资源

本节说明虚拟机使用多少介质并且适用于掌握 VMware 专业知识的人员。 CPU 资源是以 vCPU 数（核心数）和 MHz（CPU 周期）的形式指定的。 VMware VMkernel 使用 MHz 周期控制 CPU 调度。

内存资源是按最大内存和保留内存指定的。 保留内存不与同一物理 Cisco UCS 服务器上的其他虚拟机共享。

对磁盘资源（存储）的控制分为两个方面。 在 OVA 构建期间，CentOS 文件系统分区大小决定最小磁盘大小。 其次，vCenter 控制可用的最大磁盘空间。

如果您尝试部署未达到最低 vCPU 数量的虚拟机，那么虚拟机的 OVA 部署将失败。 如果您尝试部署处理器速度未达到最低总 MHz 要求的虚拟机，那么虚拟机将不会启动。

重要事项 本表中的数字不包括 VMware ESXi 或 vCenter 的资源。 请参阅 CWMS 和 ESXi 主机耗用的资源。

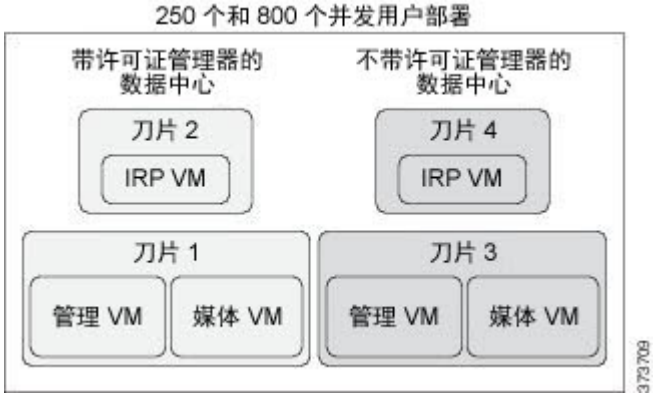
虚拟机类型	虚拟 CPU (vCPU)	CPU[8](MHz)	保留内存/总内存[9](GB)	磁盘 (GB)
管理虚拟机	4	8000	16/16	418
媒体	8	16,480	13/23	128
互联网反向代理	8	16,480	6/6	128

8 将物理 CPU 数乘以 CPU 芯片的速度 (MHz) 得到的数字。 此计算中不考虑超线程。 （物理 CPU 的时钟速度必须为 2.4 GHz 或更快。）
9 有媒体功能的虚拟机可以有附加的非保留内存；内存 = 保留/总计

800 个用户的系统

800 个用户的系统也称为中型系统。 下图展示了 800 个用户部署的两个版本。 “冗余”虚拟机支持高可用性 (HA)。

本图显示 800 用户系统的布局，它的两个数据中心构成了一个多数据中心 (MDC) 系统，且支持互联网反向代理 (IRP)。 许可证管理器仅在一个数据中心上运行。



下表列出了系统中 ESXi 主机（Cisco UCS 服务器）的最低硬件要求。 最后两列显示新安装 Cisco WebEx Meetings Server 需要的磁盘空间量，以及使用现有 Cisco UCS 服务器并利用自动升级功能将 Cisco WebEx Meetings Server 发行版 1.5MR3 升级到发行版 2.X 时需要的可用磁盘空间。 有关更多信息，请参阅常规系统要求。

有关带宽要求的信息，请参阅网络带宽要求，第 52 页。

注释 不支持 800 个用户的系统部署与 vCenter 并存。

有关 IOPS 的信息，请参阅在 VMware vSphere 上部署系统的优点，第 36 页。

ESXi 主机（Cisco UCS 服务器）上的虚拟机	CPU 核心数	内存 (GB)	以太网端口	新安装的硬盘存储要求	从 1.5MR3 自动升级到 2.X 所需的可用硬盘存储空间[10]
管理和媒体虚拟机（组合）	40	80	• 对于管理和媒体虚拟机，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） • 对于 ESXi 管理网络，建议使用 1 个端口	1.5 TB；至少 10,000 RPM	990 GB
互联网反向代理 (IRP)	40	36	• 对于 IRP，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） • 对于 ESXi 管理网络，建议使用 1 个端口	300 GB；至少 10,000 RPM	172 GB

10 如果选择“手动升级”（即手动部署所有虚拟机）且使用相同的硬件，则所需的可用空间将是自动升级时的两倍。

注释 如果计划使用高可用性系统，请购买与主系统相同的硬件和数量。

对于 800 个用户的系统，我们建议不要在 DMZ 主机上配置其他虚拟机。 这可能导致丢包率增加而且媒体连接上出现明显的延迟。

在 800 个用户的系统中由虚拟机保留的资源

本部分说明虚拟机使用多少介质并且适用于掌握 VMware 专业知识的人员。 CPU 资源是以 vCPU 数（核心数）和 MHz（CPU 周期）的形式指定的。 VMware VMkernel 使用 MHz 周期控制 CPU 调度。

内存资源是按最大内存和保留内存指定的。 保留内存不与同一物理 Cisco UCS 服务器上的其他虚拟机共享。

对磁盘资源（存储）的控制分为两个方面。 在 OVA 构建期间，CentOS 文件系统分区大小决定最小磁盘大小。 其次，vCenter 控制可用的最大磁盘空间。

如果您尝试部署未达到最低 vCPU 数量的虚拟机，那么虚拟机的 OVA 部署将失败。 如果您尝试部署处理器速度未达到最低总 MHz 要求的虚拟机，那么虚拟机将不会启动。

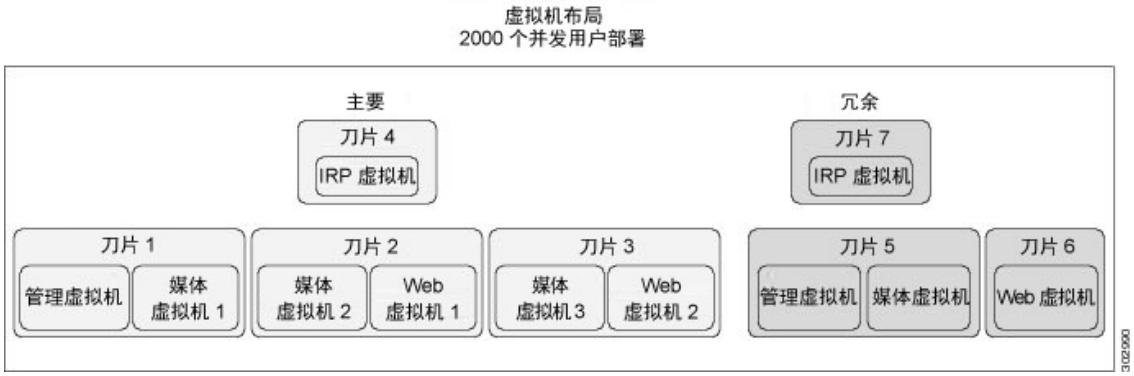
重要事项 本表中的数字不包括 VMware ESXi 的资源。 请参阅CWMS 和 ESXi 主机耗用的资源，第 11 页。

虚拟机类型	虚拟 CPU (vCPU)	CPU[11](MHz)	保留内存/总内存[12](GB)	磁盘 (GB)
管理虚拟机	10	20,600	16/16	418
媒体	30	60,800	14/44	128
互联网反向代理	20	41,200	10/10	128

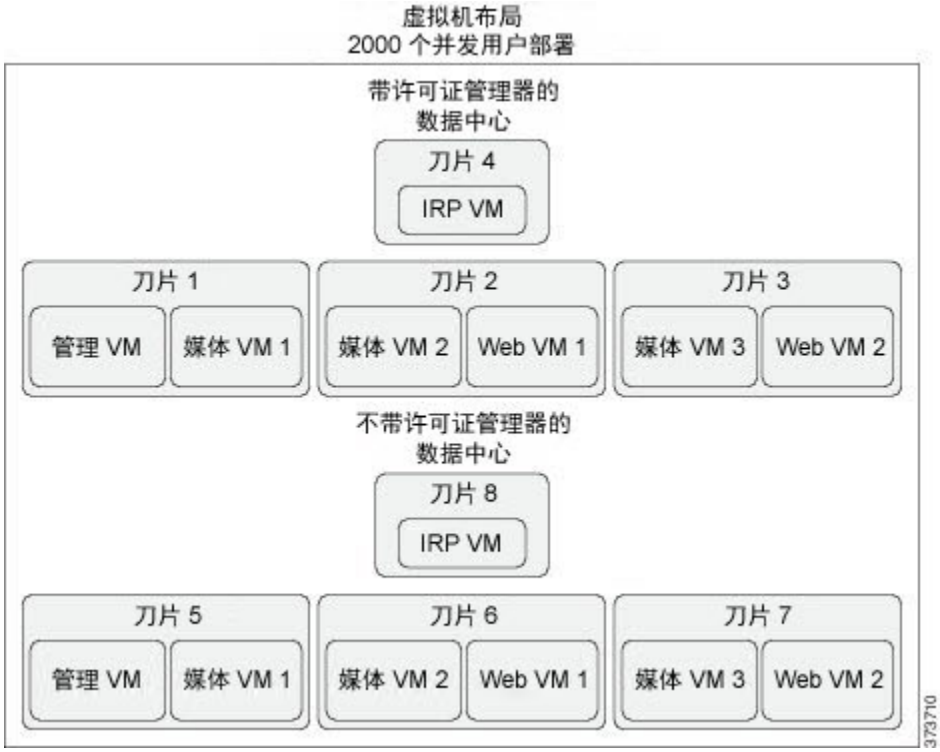
11 将物理 CPU 数乘以 CPU 芯片的速度 (MHz) 得到的数字。 此计算中不考虑超线程。 （物理 CPU 的时钟速度必须为 2.4 GHz 或更快。）
12 有媒体功能的虚拟机可以有附加的非保留内存；内存 = 保留/总计

2000 个用户的系统

2000 个用户的系统也称为大型系统。 本图展示了支持高可用性 (HA) 和互联网反向代理 (IRP) 的 2000 用户系统。 HA 虚拟机显示为**冗余**虚拟机。 如果您的系统不支持 HA，则只部署**主**系统。



本图显示 2000 用户系统的部署，它的两个数据中心构成了一个多数据中心 (MDC) 系统，且支持互联网反向代理 (IRP)。 许可证管理器仅在一个数据中心上运行。



重要事项 我们建议您部署图中所示的所有虚拟机。 通过在物理服务器上部署不同类型的虚拟机，可以更好地避免系统在硬件发生故障时关闭。 例如，在单个物理服务器上放置媒体和 Web 虚拟机比放置两个 Web 虚拟机更具弹性。

在大型系统上存在均等负载平衡规则的例外情况（有关更多信息，请参阅负载平衡，第 58 页），在这种情况下媒体 1 和媒体 2 上存在 SIP 中继负载平衡器，而媒体 3 和可选的媒体 HA 上则没有负载平衡。 如果主系统上的媒体 1 和 2 都存在故障，则 CWMS 上的所有电话服务都将丢失。 如果系统为 HA 部署，则冗余功能可消除单一虚拟机的故障。

下表列出了系统中 ESXi 主机（Cisco UCS 服务器）的最低硬件要求。 最后两列显示新安装 Cisco WebEx Meetings Server 需要的磁盘空间量，以及使用现有 Cisco UCS 服务器并利用自动升级功能将 Cisco WebEx Meetings Server 发行版 1.5MR3 升级到发行版 2.X 时需要的可用磁盘空间。 有关更多信息，请参阅常规系统要求。

有关带宽要求的更多信息，请参阅网络带宽要求，第 52 页。

如果计划添加高可用性系统，则这些虚拟机将显示为“冗余”虚拟机。 如果不想配置高可用性系统，则仅部署主系统。

注释 不支持 2000 个用户的系统部署与 vCenter 并存。

注释 有关 IOPS 的信息，请参阅在 VMware vSphere 上部署系统的优点，第 36 页。

ESXi 主机（Cisco UCS 服务器）上的虚拟机	CPU 核心数	内存 (GB)	以太网端口	新安装的硬盘存储要求	从 1.5MR3 自动升级到 2.X 所需的可用硬盘存储空间[13]
媒体 1 和管理虚拟机（组合）	40	80	• 对于媒体 1 和管理虚拟机，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） • 对于 ESXi 管理网络，建议使用 1 个端口	1.5 TB；至少 10,000 RPM	990 GB
媒体 2 和 Web 1 虚拟机（组合）	40	80	• 对于媒体 2 和 Web 1 虚拟机，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） • 对于 ESXi 管理网络，建议使用 1 个端口	1 TB；至少 10,000 RPM	768 GB
媒体 3 和 Web 2 虚拟机（组合）	40	80	• 对于媒体 3 和 Web 2 虚拟机，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） • 对于 ESXi 管理网络，建议使用 1 个端口	1 TB；至少 10,000 RPM	768 GB

ESXi 主机（Cisco UCS 服务器）上的虚拟机	CPU 核心数	内存 (GB)	以太网端口	新安装的硬盘存储要求	从 1.5MR3 自动升级到 2.X 所需的可用硬盘存储空间[13]
互联网反向代理 (IRP)	40	36	• 对于 IRP，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） • 对于 ESXi 管理网络，建议使用 1 个端口	300 GB；至少 10,000 RPM	172 GB
高可用性系统的媒体和管理虚拟机（组合）	40	80	• 对于媒体和管理虚拟机，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） • 对于 ESXi 管理网络，建议使用 1 个端口	1.5 TB；至少 10,000 RPM	990 GB
高可用性系统的 Web 虚拟机	40	80	• 对于 Web 虚拟机，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） • 对于 ESXi 管理网络，建议使用 1 个端口	1 TB；至少 10,000 RPM	896 GB
高可用性系统	40	36	• 对于 IRP，建议使用 2 个（其中 1 个用于 NIC teaming 冗余） • 对于 ESXi 管理网络，建议使用 1 个端口	300 GB；至少 10,000 RPM	172 GB

13 如果选择“手动升级”（即手动部署所有虚拟机）且使用相同的硬件，则所需的可用空间将是自动升级时的两倍。

注释 对于 2000 个用户的系统，我们建议不要在 DMZ 主机上配置其他虚拟机。 这可能导致丢包率增加而且媒体连接上出现明显的延迟。

在 2000 个用户的系统中由虚拟机保留的资源

本部分说明虚拟机使用多少介质并且适用于掌握 VMware 专业知识的人员。 CPU 资源是以 vCPU 数（核心数）和 MHz（CPU 周期）的形式指定的。 VMware VMkernel 使用 MHz 周期控制 CPU 调度。

内存资源是按最大内存和保留内存指定的。 保留内存不与同一物理 Cisco UCS 服务器上的其他虚拟机共享。

对磁盘资源（存储）的控制分为两个方面。 在 OVA 构建期间，CentOS 文件系统分区大小决定最小磁盘大小。 其次，vCenter 控制可用的最大磁盘空间。

如果您尝试部署未达到最低 vCPU 数量的虚拟机，那么虚拟机的 OVA 部署将失败。 如果您尝试部署处理器速度未达到最低总 MHz 要求的虚拟机，那么虚拟机将不会启动。

重要事项 本表中的数字不包括 VMware ESXi 的资源。 请参阅 CWMS 和 ESXi 主机耗用的资源。

虚拟机类型	虚拟 CPU (vCPU)	CPU[14](MHz)	保留内存/总内存[15](GB)	磁盘 (GB)
管理虚拟机	10	20,600	16/16	418 对于版本 2.6 及更高版本，使用 OVA 文件部署的新系统必须为 513。
媒体	30	60,800	14/44	128
Web	10	20,600	16/16	128
互联网反向代理	20	41,200	10/10	128

14 将物理 CPU 数乘以 CPU 芯片的速度 (MHz) 得到的数字。 此计算中不考虑超线程。 （物理 CPU 的时钟速度必须为 2.4 GHz 或更快。）
15 有媒体功能的虚拟机可以有附加的非保留内存；内存 = 保留/总计

系统容量矩阵

关键点：

- 本节中的信息的一个基本假设是至少有两人参加会议。
- 并发会议连接数被定义为在任意给定时间参加会议的人数。 例如，对于 50 个用户的系统，最大并发会议连接可包括五个并发会议，每个会议都有 10 人参加（例如，1 名主持人和 9 名参加者）。
- 在任何时间点，只要达到会议参加者的最大数量，系统就不再允许其他用户启动或加入会议。在这些最大数量的会议参加者中（2000、800、250 或 50 人），只有半数参加者可以使用视频。视频被定义为发送或接收，这意味着用户可能正在使用他们的 WebEx 网络摄像头视频或正在使用可共享视频的视频文件共享选项。
- 桌面共享并非视频。 这意味着如果使用 250 个用户系统，那么 250 人可以在会议期间的任意给定时间共享他们的桌面。
- 增加高可用性或多数据中心不会增加举行会议的系统容量；800 个用户的系统仍然是 800 个用户的系统。

下表中的数字表示 Cisco WebEx Meetings Server 系统的设计容量。 在超出以下规格的情况下运行系统会导致用户体验下降，并且可能导致系统不稳定。 Cisco 保留在以下级别上执行执行容量限制的权利。

注释 不管您的系统是单数据中心还是多数据中心系统，下表中的这些值都将保持不变。

表 *3*：版本 *2.5* 及更高版本的系统容量矩阵

系统容量	**2000** 个用户的系统	**800** 个用户的系统	**250** 个用户的系统	**50** 个用户的系统	说明
最大并发会议连接数（音频、视频和网络用户）	2000	800	250	50	在任意给定时间参加并发会议的人数。
最大并发音频连接数（电话会议中的电话呼叫以及从会议客户端使用计算机连接语音）	2000	800	250	50	无论使用以下哪些功能组合，系统容量始终为左侧显示的容量。 • G.711、G.722、G.729 音频编解码器 • IPv4 或 IPv6 电话会议 • TLS/SRTP 音频加密

系统容量	2000 个用户的系统	800 个用户的系统	250 个用户的系统	50 个用户的系统	说明
最大并发视频和视频文件共享用户数	1000[16]	400	125	25	这些数字显示允许同时使用视频共享的并发会议连接数（或参加者）的最大数量。 当并发会议中共享视频的用户数量达到此限制时，被邀请到并发会议的其余用户可以加入会议，但其视频窗口将显示为灰色。 **注释** 如果会议中的一个参加者使用了视频，则同一会议上的其他所有用户都将被视为视频用户，即使他们本身并不使用视频。 **注释** 桌面共享并非视频。
一个会议中的最大参加者人数	500	500	250	50	这些数字显示可出席会议的参加者的最大数量。
可同时录制的最大会议数	100	40	13	3	这是可同时使用录制文件功能的会议的总数。
最大并发录制文件播放会话数	500	200	63	12	这是可同时发生的录制文件播放会话总数。 这是指保存在您存储系统上的录制文件，不包括下载到用户桌面上的录制文件。 **注释** 这些播放会话数不包含在系统的并发会议连接数中。
用户配置文件的最大数量	400,000	400,000	400,000	400,000	此数字包括活动和停用的用户数。
最大并发会议数	1000	400	125	25	可以同时活动的单独会议的数量。
最大呼叫率（每秒呼叫数）	20	8	3	1	在一秒钟内可拨入会议的平均用户数。 系统达到此数量后，接下来的几个用户要拨入会议可能会等待几秒钟才可连接到会议。
最大并发登录数	每秒 20 人	每秒 8 人	每秒 3 人	每秒 1 人	在一秒钟内可同时登录 WebEx 站点的平均用户数。 系统达到了该数目之后，接下来登录 WebEx 站点的几名用户可能要等待几秒才能加入会议。

系统容量	2000 个用户的系统	800 个用户的系统	250 个用户的系统	50 个用户的系统	说明
最大聚合带宽利用率	5 Gbps	2 Gbps	625 Mbps	125 Mbps	测试系统以最大带宽运行时，可以处理的最大带宽。 有关带宽利用率的详细信息，请参阅《规划指南》中“系统的网络拓扑”章节的“网络带宽要求”一节。还可参阅《WebEx 网络带宽白皮书》。

16 联邦信息处理标准（FIPS 环境）为 800

注释 对于 Cisco WebEx Meetings Server 发行版 2.0 及更高版本的新安装，存储空间要求为：

- 磁盘空间可以是本地的 (DAS)，也可以是外部的 (SAN/NAS)。
- 带管理虚拟机的 ESXi 主机（Cisco UCS 服务器）需要 1.5 TB 磁盘空间。
- 不带管理虚拟机的 ESXi 主机（Cisco UCS 服务器）需要 1 TB 磁盘空间。
- 使用现有 Cisco UCS 服务器来升级 Cisco WebEx Meetings Server 时，如果 UCS 服务器只有管理虚拟机（主系统或 HA 系统），则 ESXi 主机需要 1118 GB 可用磁盘空间；如果 UCS 服务器有一个管理虚拟机和一个媒体虚拟机（主系统或 HA 系统），则 ESXi 主机需要 990 GB 可用磁盘空间。

有关完整的详细信息，请参阅 **Cisco WebEx Meetings Server 和 ESXi 主机消耗的资源**一节 (http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html)。

提示 所有大小用户系统部署的最大会议长度为 24 个小时。

注释 考虑升级时，请为数据存储提升作规划，因为原始系统和升级系统将共享数据存储空间，直到升级系统的测试完成并删除原始系统为止。

有关不同容量的用户系统的网络带宽要求的信息，请参阅本书“不同类型的系统网络拓扑结构”一章中的“网络带宽要求”一节。

支持的升级路径

本 Cisco WebEx Meetings Server 发行版支持从发行版 1.x 升级到 2.8。 要注意以下几点：

- 升级的定义是更换系统以部署我们对系统所作的重大修改。
- 更新定义为对系统进行递增式修改。 更新将部署修订和次要改进。
- 更新会保留原始系统的所有数据。 升级会保留除日志以外的所有原始系统数据。
- 进行升级时，无法跳过软件的主要版本而直接升级到随附的维护版本 (MR)。

  例如，要从 1.5MR5 升级到 2.8MR，请从 1.5MR5 升级到 2.8，然后更新到 2.8MR。

注释 所有的更新都要求停机。 对于多数据中心，您可以同时更新两个数据中心。

注意 在一个数据中心完成的情况下不要单击**重新启动**，直至另一个数据中心的更新完成并且两个都显示**重新启动**按钮。 从发行版 2.5MR6 或更高版本更新至发行版 2.8 时，在另一个数据中心的更新完成之前重启数据中心会中断复制过程。

使用下表确定如何更新或升级至 Cisco WebEx Meetings Server 发行版 2.8。

已安装的发行版	目标发行版	路径
1.0 至 1.1	2.8	**1** 更新至 1.5。 **2** 更新至 1.5MR5 Patch 2 或更高版本。 **3** 升级至 2.8。
1.5 至 1.5MR4	2.8	**1** 更新至 1.5MR5 Patch 2 或更高版本。 **2** 升级至 2.8。
1.5 MR5	2.8	**1** 更新至 1.5MR5 Patch 2 或更高版本。 **2** 升级至 2.8。
1.5 MR5 Patch 2 或更高版本	2.8	升级至 2.8。
2.0 至 2.0MR8	2.8	**1** 更新至 2.0MR9。 **2** 更新至 2.8。
2.0MR9 或更高版本	2.8	更新至 2.8。

已安装的发行版	目标发行版	路径
2.5 至 2.5MR5	2.8	1 更新至 2.5MR6。 2 更新至 2.8。
2.5MR6	2.8	更新至 2.8。
2.6 至 2.6MR2	2.8	1 更新至 2.6MR3 2 更新至 2.8
2.6MR3 或更高版本	2.8	更新至 2.8。
2.7 或任意 2.7MR	2.8	更新至 2.8。
2.8 或任意 2.8MR	任意 2.8MR	更新至 2.8MR。

重要事项 在升级或更新期间无法更改系统的音频加密类型 (Audio Encrypted -AE/Audio Unencrypted -AU)。完成部署后，将系统从一个类型的音频加密更改为其他类型的唯一方法就是部署一个新系统。

有关更多信息，请参阅以下文档：

- *Cisco WebEx Meetings Server* 管理指南发行版 *2.8*： http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html
- *Cisco WebEx Meetings Server* 规划指南和系统要求发行版 *2.8*： http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html

支持的升级路径

本 Cisco WebEx Meetings Server 发行版支持从发行版 1.x 升级到 3.0。 要注意以下几点：

- 升级的定义是更换系统以部署我们对系统所作的重大修改。
- 更新定义为对系统进行递增式修改。 更新将部署修订和次要改进。
- 更新会保留原始系统的所有数据。 升级会保留除日志以外的所有原始系统数据。
- 进行升级时，无法跳过软件的主要版本而直接升级到随附的维护版本 (MR)。

  例如，要从 1.5MR5 升级到 3.0MR，请从 1.5MR5 升级到 3.0，然后更新到 3.0MR。

注释 所有的更新都要求停机。 对于多数据中心，您可以同时更新两个数据中心。

注意 在一个数据中心完成的情况下不要单击**重新启动**，直至另一个数据中心的更新完成并且两个都显示**重新启动**按钮。 从发行版 2.5MR6 或更高版本更新到发行版 3.0 时，在另一个数据中心的更新完成之前重启数据中心会中断复制过程。

使用下表确定如何更新或升级至 Cisco WebEx Meetings Server 发行版 3.0。

已安装的发行版	目标发行版	路径
1.0 至 1.1	2.8	**1** 更新至 1.5。 **2** 更新至 1.5MR5 Patch 2 或更高版本。 **3** 升级至 2.8。
1.5 至 1.5MR4	2.8	**1** 更新至 1.5MR5 Patch 2 或更高版本。 **2** 升级至 2.8。
1.5 MR5	2.8	**1** 更新至 1.5MR5 Patch 2 或更高版本。 **2** 升级至 2.8。
1.5 MR5 Patch 2 或更高版本	2.8	升级至 2.8。
2.0 至 2.0MR8	3.0	**1** 更新至 2.0MR9。 **2** 更新至 3.0。
2.0MR9 或更高版本	3.0	更新至 3.0。
2.5 至 2.5MR5	3.0	**1** 更新至 2.5MR6。 **2** 更新至 3.0。
2.5MR6	3.0	更新至 3.0。
2.6 或任意 2.6MR	3.0	更新至 3.0。
2.7 或任意 2.7MR	任意 3.0MR	更新至 3.0MR。

重要事项 在升级或更新期间无法更改系统的音频加密类型 (Audio Encrypted -AE/Audio Unencrypted -AU)。完成部署后，将系统从一个类型的音频加密更改为其他类型的唯一方法就是部署一个新系统。

有关更多信息，请参阅以下文档：

- *Cisco WebEx Meetings Server* 管理指南发行版 *3.0*： http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html
- *Cisco WebEx Meetings Server* 规划指南和系统要求发行版 *3.0*： http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html

第 2 章

Cisco WebEx Meetings Server 简介

Cisco Webex Meetings Server (CWMS) 是安全的完全虚拟化私有云（内部部署）会议解决方案，该解决方案通过结合音频、视频和互联网来降低会议成本并扩大 Cisco Unified Communications 的投资利用率。

与其他 Cisco WebEx 产品一样，本产品也提供了实时协作工具，包括文档、应用程序和桌面共享、注释工具、实现高效会议管理的主持人完整控制功能、包含当前发言人的集成参加者列表以及视频切换、录制和播放。 本产品使用高质量视频，为用户提供清晰的视频共享体验。

您可以在数据中心防火墙后的私有云中部署和管理此会议解决方案。 它专用于 Cisco UCS 服务器和 VMware vSphere。 （有关具体要求，请参阅最低硬件要求，第 9 页。）它可快速地进行虚拟部署并具备功能强大的工具，使管理员能够配置和管理系统并查看关键系统度量指标。

此外，移动用户也可以参加会议。 有关支持的设备，请参阅移动设备的操作系统要求，第 186 页。

系统的重要注意事项

请注意下列事项：

- 正向代理 — 不推荐使用，但是您可以限制性地使用正向代理。 有关完整的详细信息，请参阅《*Cisco WebEx Meetings Server* 疑难解答指南》。
- 反向代理 — 仅支持本产品中包含的互联网反向代理服务器。
- NAT — 当满足本系统的要求时受支持。 有关完整的详细信息，请参阅对系统采用 NAT。
- 单数据中心 - 所有发行版 Cisco WebEx Meetings Server 均支持在单个数据中心内部署。 有关完整的详细信息，请参阅部署单数据中心。
- 多数据中心 - 可以让运行 Cisco WebEx Meetings Server 发行版 2.5 或更高版本的数据中心加入，以创建由多个数据中心组成的系统。 关于完整的详细信息，请参阅关于多数据中心部分（《Cisco WebEx Meetings Server 管理员指南》）。
- 存储服务器 - 多数据中心系统中的每个数据中心都必须有一个独立的存储服务器。 同一存储服务器无法支持多个数据中心。
- 高可用性系统 - 定义为具有冗余虚拟机且运行相同 Cisco WebEx Meetings Server 版本的系统。如果主系统（在单数据中心系统中）失败，高可用性系统将继续服务。 冗余高可用性虚拟机

必须与主虚拟机位于同一数据中心中。 主系统和高可用性系统虚拟机必须位于同一 VLAN 或子网上。

您无法加入高可用性系统以创建多数据中心环境。

- 互联网反向代理服务器 (IRP) 服务器 - 定义为充当外部互联网与公司内部网络之间的代理的虚拟机，用于提供到CWMS的公开访问。 如果想允许用户利用移动设备安排和参加会议，或想提供从互联网对 WebEx 站点的安全访问，需要使用互联网反向代理服务器。 如果打算限制为仅从内部网络访问 Cisco WebEx Meetings Server，则无需互联网反向代理服务器。 （通过使用与部署管理虚拟机时相同的 OVA 文件来部署 IRP 虚拟机。 IRP 虚拟机必须和公共虚拟 IP 地址位于同一子网上。）
- 虚拟 IP (VIP) 地址 - 用于与数据中心中的管理、媒体和 Web 虚拟机通信。
- 专用虚拟 IP (VIP) 地址 - 在管理虚拟机上配置并与管理站点 URL 关联。 如果是在水平分割 DNS 部署或在没有互联网反向代理服务器的部署的内部 DNS 服务器中配置此地址，则专用 VIP 也可与 WebEx 站点 URL 关联。
- 公共虚拟 IP (VIP) 地址 - 在互联网反向代理虚拟机上配置且仅与 WebEx 站点 URL 关联。 外部 DNS 服务器上的 WebEx 站点 URL 必须能解析为公共虚拟 IP 地址，以便用户通过互联网访问 WebEx 站点。 如果没有互联网反向代理服务器，系统上将不会配置公共虚拟 IP 地址。

注意 如果您在部署系统时无视我们的建议和要求，那么您将得不到 Cisco 的支持服务。 Cisco 对于您因不遵守我们的指导而可能遇到的任何问题概不负责。

Cisco WebEx Meetings Server 的新增和更改的功能

有关新增和更改的功能列表，请参阅《*Cisco WebEx Meetings Server* 发行说明》（发行说明）中的“Cisco WebEx Meetings Server 的新增和更改的功能”部分。

- Cisco Unified MeetingPlace 客户须知，第 34 页
- 部署单数据中心，第 35 页
- 加入单数据中心以创建多数据中心 (MDC) 系统，第 35 页
- 将 VMware vSphere 与系统配合使用，第 35 页
- IOPS 和存储系统性能，第 38 页
- 安装 VMware vSphere ESXi 和配置存储空间，第 39 页
- 加入会议，第 40 页

Cisco Unified MeetingPlace 客户须知

由于体系结构的差异，尚没有从 Cisco Unified MeetingPlace 迁移到 Cisco WebEx Meetings Server 的途径（对于现有用户帐户、定制内容和会议）。 这是两种不同的产品。

您可以继续支持 Cisco Unified MeetingPlace 和 Cisco WebEx Meetings Server，同时鼓励用户切换到新系统，从而帮助用户更轻松地实现转换。

部署单数据中心

Cisco WebEx Meeting Server (CWMS) 可部署为单数据中心 (SDC) 系统，也可部署为高可用性 (HA) 系统或多数据中心 (MDC) 系统（请参阅HA 或 MDC 部署中的冗余，第 49 页）。 过了试用期后，SDC 系统（包括支持 HA 的系统）仅需要主持人许可证。 MDC 系统则需要至少两个 MDC 功能许可证、相应的主持人许可证，且 MDC 没有试用期。

加入单数据中心以创建多数据中心 (MDC) 系统

您可以连接运行 Cisco WebEx Meeting Server 发行版 2.5 或更高版本的两个数据中心，从而建立一个多数据中心 (MDC) 系统。 最多可连接两个数据中心。 多数据中心系统和高可用性系统之间的区别在于，高可用性系统必须处于同一位置并担当备份系统。 在 MDC 系统中，数据中心可以位于不同的地理位置，而且两个数据中心都可参与系统处理。 请参阅HA 或 MDC 部署中的冗余，第 49 页。 在 MDC 系统中，每个 CWMS 数据中心必须购买一个许可证。 尝试部署 MDC 系统之前，应购买 MDC 许可证。 （具有单数据中心的系统不需要功能许可证。） 有关如何准备要加入的数据中心、加入过程以及如何在加入过程完成后将数据从一个数据中心转移到另一个数据中心的详细信息，请参阅《*Cisco WebEx* 管理指南》 (http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html) 中的“加入数据中心以创建多数据中心 (MDC) 系统”一章。

将 VMware vSphere 与系统配合使用

重要事项 本产品只在 VMWare vSphere 虚拟化平台上安装。 用于 CWMS 的 VMWare Tools 在系统部署期间会自动安装，并且不应进行手动升级。 关于 VMWare Tools 的详细信息，请参阅 docwiki.cisco.com/wiki/VMWare_Tools。

- Cisco WebEx Meetings Server 被设计为可在满足或超出系统要求的任何同等 Cisco UCS 服务器上工作。 但是，为节省您的时间，我们建议使用标准 Cisco UCS 服务器。 有关硬件和 VMware 要求的详细信息，请参阅 最低硬件要求，第 9 页。
- 必须购买 VMWare vSphere 5.0、5.0 Update 1、5.0 Update 2、5.1、5.1 Update 1、5.5 或 6.0，以用作 Cisco WebEx Meetings Server 的虚拟机监控程序平台。

注释 出于安全考虑，5.1 必须是版本 1900470 或更高版本。

完成以下任一操作：

直接从 Cisco 的 GPL（全球价格表，Global Price List）上购买 vSphere。 Cisco 是获得批准的 VMWare 合作伙伴和经销方。

请通过与 VMWare 签订的企业协议从 VMWare 处直接购买 vSphere。

在 VMware vSphere 上部署系统的优点

本节说明了 VMware vSphere 和 vCenter 对使用本 Cisco WebEx 产品必不可少的原因并列出了一些注意事项。

系统的部署

- 本产品是作为与 VMware vSphere 兼容的 OVA 虚拟设备包装的，不是作为 DVD 上的软件包集合而包装的。 您必须具有 vCenter 才能部署 OVA，否则将不能安装产品。
- 通过将其打包为虚拟设备，我们可以进行快速部署；在某些情况下耗时不到 1 小时。
- 要使用 OVA 虚拟设备来实现快速安装，您可以为大部分系统容量选择自动系统部署。 只需提供 vCenter 凭证，我们就会为您的系统部署所有虚拟机，无需手动干预。 这项创新将最大限度地减少劳动力成本和时间。

注释 OVA 模板为每个虚拟机创建两个虚拟 NIC。 但是，只有管理虚拟机会同时使用这两个虚拟 NIC。 对于所有其他 Cisco WebEx Meetings Server (CWMS) 虚拟机，只使用一个虚拟 NIC，而另一个会断开连接。

- CWMS 要求您运行 VMware ESXi 或相应 VMware ESXi 的可安装 Cisco ISO 映像。 这些版本都包含支持 CWMS 要求的 Cisco UCS 服务器所需的驱动程序。 有关更多信息，请参阅http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/OL_26617.pdf。

从系统错误中轻松恢复

如果某项影响系统的更改未能达到您的预期，您可通过使用VMware数据恢复功能快速还原该更改，而无需重新部署系统。

vSphere 注意事项

请注意下列事项：

- 您可以将虚拟机移动到另一个 ESXi 主机上。 但是，您必须在新的 ESXi 主机上保留虚拟机的布局。 也就是说，如果您打算移动与 Web 虚拟机共存的媒体虚拟机，必须将其移动到独立的 ESXi 主机（主机上只有该虚拟机）或移动到已有 Web 虚拟机的 ESXi 主机。

注释 目标 ESXi 主机必须符合与源 ESXi 主机相同的系统要求。

CWMS 不支持以下 VMware 功能：

- VMotion 和 Storage VMotion（虽然可以移动虚拟机，但不能使用这些工具来移动。）
- VMware 分布式资源调度程序 (DRS)
- vSphere 高可用性 (HA)
- vSphere 群集和资源共享
- 克隆虚拟机。

vSphere 最佳实践

- 建议您不要使用虚拟机快照。 如果决定使用快照，请在确认系统更改后提交快照或尽快删除这些快照。 快照无论保留多长时间都会导致性能严重下降。
- 对于 SAN 环境，将磁盘镜像部署到 IOPS 数值较高的 SAN 上。

  对于 800 用户的系统，管理虚拟机的 OVA 部署的平均 IOPS 为 506（最大 IOPS 为 855），而媒体虚拟机的 OVA 部署的平均 IOPS 为 475（最大 IOPS 为 652）。 创建并启动这些虚拟机后，您就可在 Web 浏览器中输入区分大小写的 URL 并继续系统部署。 主系统的平均 IOPS 为 108（最大 IOPS 为 1558），辅助系统的平均 IOPS 为 163（最大 IOPS 为 1736）。
- 验证 SAN 上有足够的可用空间。 快照存储在同一 SAN 上。
- 部署 10 GB 网络，以实现最快速的部署和带宽，满足未来增长的需求。
- 建议您使用同一个 vCenter 来管理所有虚拟机。 这样在需要时可更轻松地恢复系统。

请参阅网络带宽要求，第 52 页以获取关于网络带宽的更多信息。

vCenter Server 要求

除了 vSphere 之外，还需要 vCenter Server。

- 要部署此虚拟设备，还必须使用 vCenter 来部署和管理系统中的虚拟机。 没有 vCenter Server，此产品将无法工作。
- Cisco 建议在执行对系统产生影响的重要操作之前对系统进行备份并截取快照。 通过创建备份，您可在更新不符合期望时回滚各项更改。 可使用 vCenter 自动执行备份和快照。
- CWMS 支持 vSphere Standard Edition。

用于 800 和 2000 个用户的系统的 vSphere 版本

- 800 个和 2000 个用户的系统由要求 30 至 40 个 vCPU 的虚拟机组成。 这些虚拟机使用 vCPU 执行计算密集型任务，如 SSL 编码或解码、混合音频流等等。

  有关 vCPU 要求的完整信息，请参阅CWMS 和 ESXi 主机耗用的资源，第 11 页。
- 您必须至少购买 vSphere 5.0 Enterprise Plus Edition 或 vSphere 5.1 Enterprise Edition，因为低端 vSphere 版本不支持所需的 vCPU 数。

IOPS 和存储系统性能

预期的最大 IOPS 和流量

下表显示在系统最大负载下，单个虚拟机的预期最大 IOPS 和流量值。

系统容量	虚拟机	每秒的输入/输出操作次数 (IOPS) 最大值	每秒读取的最大兆字节数	每秒写入的最大兆字节数
50 个用户的系统	管理虚拟机	450	1	15
	DMZ	70	0.3	0.3
250 个用户的系统	管理虚拟机	1400	1	25
	媒体	150	1	10
	DMZ	110	0.4	0.6
800 个用户的系统	管理虚拟机	1400	3	50
	媒体	300	1	30
	DMZ	150	1	1.5
2000 个用户的系统	管理虚拟机	1600	2.5	60
	媒体	300	1	25
	Web	200	3	1.5
	DMZ	200	1.5	3

2000 个用户的系统重新启动时的 IOPS

下表显示 2000 个用户的系统在启动（重新启动）过程中的 IOPS 信息。

2000 个用户的系统中的虚拟机	系统启动（重新启动）的 IOPS	次要更新的 IOPS
管理虚拟机	2300	3000
媒体	2000	2000
Web	1500	2000

2000 个用户的系统中的虚拟机	系统启动（重新启动）的 IOPS	次要更新的 IOPS
Web	1000	2000

2000 个用户的系统备份时的 IOPS

下表显示 2000 个用户的系统在非工作时间进行备份时的 IOPS 信息。

2000 个用户的系统的管理虚拟机	备份的 IOPS	每秒读取的最大兆字节数	每秒写入的最大兆字节数
1 GB 备份	2000	220	300
12 GB 备份	5000	320	600

安装 VMware vSphere ESXi 和配置存储空间

Cisco WebEx Meetings Server 是基于软件的解决方案。 它不是硬件/软件组合包。 您可以自行选择如何购买和提供硬件平台，只要硬件达到或超过 CPU、内存和存储容量要求即可。

您可以在符合我们最低规范的 Cisco UCS 服务器上部署 Cisco WebEx Meetings Server。 也可以选择将本产品部署在超过最低规范的更新、更高端的 UCS 服务器上。

有多种 RAID 控制器和网络选项可用。 您可以选择使用 SAN 存储器取代本地 RAID。 我们不提供关于您可以选择的每种存储配置的详细信息。

但是，既然 Cisco WebEx Meetings Server 部署在 Cisco UCS 服务器上，那么请参阅《*Cisco UCS* 服务器 *RAID* 指南》（位于 http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/raid/configuration/guide/RAID_GUIDE.html ）。

- 要在 UCS B 系列后端服务器上安装 VMware vSphere ESXi，请参阅http://www.cisco.com/en/US/docs/unified_computing/ucs/os-install-guides/vmware/b_B-Series_VMware_Install.html。
- 要在 UCS C 系列机架服务器上安装 VMware vSphere ESXi，请参阅http://www.cisco.com/en/US/docs/unified_computing/ucs/os-install-guides/vmware/b_C-Series_VMware_Install.html。

有关更多信息，另请参阅docwiki.cisco.com/wiki/VMware_Tools。

在 RAID 控制器上设置写入缓存

为实现最佳系统性能，应该检查RAID控制器上的缺省写入设置。 可以设置以下三种缺省写入设置：配备 *BBU* 回写、透写或总是回写。 以下是一些关于在Cisco UCS 服务器上选择相应的缺省写入设置的指南：

- **配备 BBU 回写** - 如果 RAID 控制器上安装了电池备份单元，则使用该设置。 在发生系统功率损耗时，电池备份单元保存控制器高速缓存存储器的内容。

在电池备份单元发生故障或脱机进入再学习周期时，配备 BBU 回写设置将自动返回给**透写**缓存。 虽然主机的 I/O 子系统性能会下降，但是在电池备份单元无法正常工作时，透写设置更安全。

- **透写** - 如果需要删除电池备份单元用于修复，则使用该设置并启用显式缓存（使用磁盘缓存选项）。 此设置应该给予更佳的性能，但不是最佳性能。 在替换了损坏的电池之后，可以将缺省写入设置恢复到配备 BBU 回写模式。
- **总是回写** - 如果托管 RAID 控制器的主机已连接到不间断电源单元，则使用该设置。

加入会议

Cisco WebEx Meetings Server 的最终用户体验类似网站体验，用户可访问该网站以安排和加入会议。该网站包含使在线会议变得简单易用的实时会议元素。 用户可以通过浏览器或桌面上的客户端加入会议。

有关最终用户体验的完整详细信息，请登录 WebEx 站点并选择**帮助**。

Windows 用户

以下内容假定用户对 PC 拥有允许他们加入 WebEx 会议的 Windows 管理员权限。 如果情况并非如此，则系统管理员可以使用 IBM Tivoli 等标准桌面管理软件，向用户推送 WebEx Meetings 应用程序客户端。 请参阅从管理站点下载应用程序，第 124 页。

- Microsoft Internet Explorer 用户可以安装 ActiveX 控件或 Java 插件，下载 WebEx Meetings 应用程序安装程序或在临时系统文件夹（例如 TFS）中运行应用程序。 客户端软件将在用户首次加入会议时下载并自动安装。
- Google Chrome 和 Mozilla Firefox 用户可以安装 Java 插件，下载 WebEx Meetings 应用程序或在临时系统文件夹中运行应用程序。 客户端软件将在用户首次加入会议时下载并自动安装。

无需对 ActiveX、Java 插件、WebEx Meetings 应用程序安装程序或 TFS 设置进行任何更改。

Mac 用户

- 如果启用了 Java，客户端软件将在用户首次加入会议时下载并自动安装。 （Mac OS X Lion V10.7 和 OS X Mountain Lion V10.8 缺省情况下关闭 Java。）
- 如果停用了 Java，用户可以下载并安装 WebEx Meetings 应用程序。

多数据中心系统用户

如果您的 WebEx 站点使用自签名证书，而不是由知名的证书机构颁发的证书，则在您的数据中心加入另一个数据中心后，用户在开始或加入会议之前，必须为受信任的根证书颁发机构库中的每个数据中心安装证书。

使用 Chrome 和 FireFox 浏览器

如果使用 Chrome 32 及更高版本或 Firefox 27[17]及更高版本，可能会看到安装 Cisco WebEx 插件的提示。 选择**下载**并按照说明安装所需的插件。

注释 安装插件后，可能需要对其进行启用。

- 如果使用 Chrome，请选择页面右上方的插件图标，选中**始终允许插件...**选项并选择**完成**。
- 如果使用 Firefox，请选择 URL 开头（https: 之前）显示的插件图标 并选择**长期允许**。

如果会议没有自动启动，请刷新页面。

如果使用 Chrome 38 浏览器或更高版本开始 WebEx 会议或播放 WebEx 录制文件，您可能需要完成以下一次性安装任务，从而将 Cisco WebEx 扩展添加到 Chrome 浏览器中：

1. 选择**将 WebEx 添加到 Chrome**。
2. 在“Cisco WebEx 扩展”对话框上选择**免费**。
3. 选择**添加**，将 Cisco WebEx 扩展添加到您的 Chrome 浏览器中。
4. 打开 Cisco_WebEx_Add-on.exe 文件，然后选择**运行**。
5. 完成安装后，系统将刷新页面。 如果会议没有自动启动，请刷新页面。

17 在本文档发布时，尚未最终决定受本策略影响的 Chrome 和 Firefox 的确切版本。

第 3 章

网络中的虚拟机布局

Cisco WebEx Meetings Server (CWMS) 拥有两组虚拟机： 内部虚拟机和可选的互联网反向代理 (IRP) 虚拟机。 对于允许外部用户通过互联网（而不使用 VPN）或使用 CDMA 移动设备来主持或参加会议的系统来说，需要提供 IRP。 若没有 IRP，只有内部和 VPN 用户可以主持或加入会议。 有关 IRP 的更多信息，请参阅互联网反向代理的网络注意事项， 第 50 页。

内部虚拟机

内部虚拟机是指管理虚拟机以及媒体虚拟机和 Web 虚拟机（如适用）。

- 内部虚拟机必须位于单个公共 VLAN 或子网上。 在系统部署期间，如果 IP 地址分配违反此规则，您将会看到错误消息。 系统设计假定所有内部虚拟机（包括任何高可用性 (HA) 虚拟机）都通过 LAN 互相连接，LAN 在这些虚拟机之间提供高带宽、极少的数据包丢失以及 4 毫秒以下的延迟。

  语音、数据、视频和 SAN 都依赖于网络带宽。 部署一个能够处理所需负载的网络非常重要。

- Cisco 建议将所有内部虚拟机放置在同一个以太网交换机上。 但是，在配置 HA 系统时，我们建议您部署两个以太网交换机，以确保网络冗余。

- 如果您决定将虚拟机置于同一数据中心的不同以太网交换机上，那么您的网络必须满足在网络带宽要求， 第 52 页中描述的具体带宽和网络延迟要求。 在这种情况下，交换机到交换机的中继线必须与单个物理交换机的 L3 延迟时间和吞吐量具备相同的联网特征。

有关具有高可用性设备的系统的其他信息，请参阅HA 或 MDC 部署中的冗余， 第 49 页。

- 不同类型的系统网络拓扑结构， 第 44 页
- 内部互联网反向代理 (IRP) 网络拓扑， 第 44 页
- 非水平分割网络拓扑， 第 45 页
- 全内部网络拓扑， 第 46 页
- 水平分割网络拓扑， 第 47 页
- HA 或 MDC 部署中的冗余， 第 49 页
- 互联网反向代理的网络注意事项， 第 50 页

- 网络带宽要求， 第 52 页
- 用于带宽聚合的 NIC Teaming， 第 56 页
- 负载平衡， 第 58 页

不同类型的系统网络拓扑结构

本产品支持下列网络拓扑结构：

- 内部互联网反向代理 (IRP) 网络拓扑， 第 44 页
- 非水平分割网络拓扑， 第 45 页
- 全内部网络拓扑， 第 46 页
- 水平分割网络拓扑， 第 47 页

注释 如果网络拓扑结构包含正向代理，那么这些代理必须满足互联网反向代理的特定要求才能正常工作。 请参阅《*Cisco WebEx Meetings Server* 疑难解答指南》获取完整的详细信息。

内部互联网反向代理 (IRP) 网络拓扑

本节描述当系统中包括互联网反向代理 (IRP) 虚拟机在内的所有虚拟机位于同一内部网络时的网络拓扑结构。

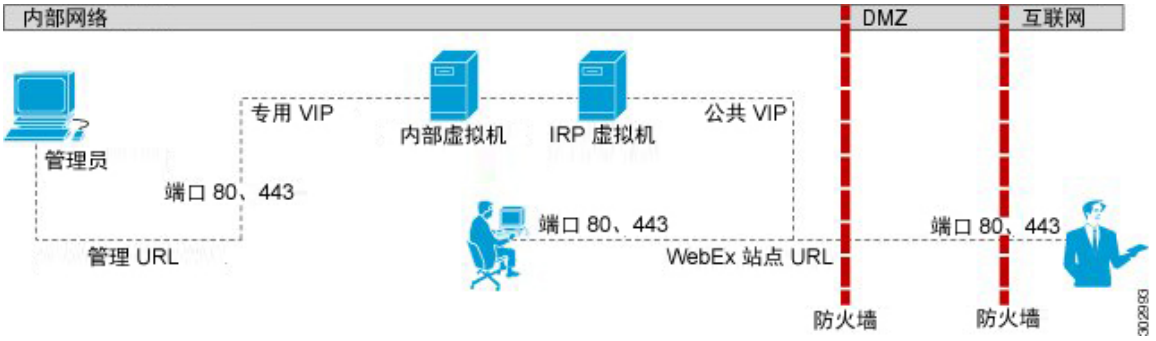
此配置允许用户从互联网安全地登录和加入会议，而无需 VPN 连接。

如果使用自动部署，则所有虚拟机（包括 IRP）的 ESXi 主机都必须从同一 VMware vCenter 进行管理。 自动系统部署过程中需要此 vCenter 信息。

注释 此配置支持移动设备访问。

您将在部署系统期间定义管理 URL、WebEx 站点 URL、专用 VIP 地址和公共 VIP 地址。 有关这些术语以及何时提供这些信息的更多信息，请参阅《*Cisco WebEx Meetings Server* 管理指南》中的“安装”一节。

以下是全内部 IRP 网络拓扑的示意图。



有关此部署所需的端口访问的完整列表，请参阅当所有虚拟机都位于内部网络中时的端口访问，第 82 页。

全内部 IRP 网络拓扑的优点

与非水平分割网络拓扑相比，DMZ 中不存在虚拟机，并且内部用户的网络流量不会通过 DMZ 进行连接以主持或出席会议。

全内部 IRP 网络拓扑的缺点

公开访问（允许外部用户访问系统）需要打开直接从互联网到内部网络的入站端口（80 和 443）。

有关 IRP 的更多信息，请参阅互联网反向代理的网络注意事项，第 50 页和通过使用 IRP 向系统中添加公开访问。

非水平分割网络拓扑

本节描述具备非水平分割DNS时的网络拓扑。内部虚拟机（管理虚拟机以及媒体和Web虚拟机（如适用））位于内部网络中，而互联网反向代理位于 DMZ 网络中。

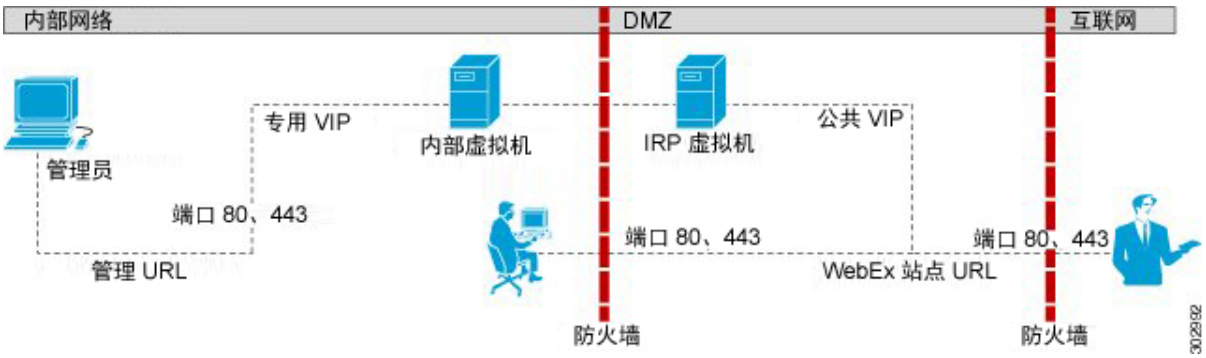
注释 此配置允许用户从互联网安全地登录和加入会议，而无需 VPN 连接。

注释 此配置支持移动设备访问。

对于此产品，水平分割和非水平分割网络拓扑之间的主要区别在于：对于水平分割系统，内部用户通过专用 VIP 地址访问 WebEx 站点 URL。 外部用户（防火墙之外）通过公共 VIP 地址访问 WebEx 站点 URL。 对于非水平分割网络，所有用户（内部和外部）都通过公共 VIP 地址访问 WebEx 站点 URL。

您将在部署系统期间定义管理 URL、WebEx 站点 URL、专用 VIP 地址和公共 VIP 地址。 有关这些术语以及何时提供这些信息的更多信息，请参阅《*Cisco WebEx Meetings Server* 管理指南》中的“安装”一节。

以下是非水平分割网络拓扑的示意图。



注释 有关此部署所需的端口访问的完整列表，请参阅DMZ 网络中的互联网反向代理的端口访问，第 82 页。

非水平分割网络拓扑的优点

- 能够严格控制进出网络的流量。
- 地址更通用，DNS 网络要求简单。

非水平分割拓扑的缺点

- 设置复杂，但是不如水平分割网络拓扑复杂。
- 内部流量导向 DMZ 网络。 所有来自互联网和内部（专用网络）的网络流量都将转至 DMZ 网络中的互联网反向代理，然后返回到内部虚拟机。
- 与各种内部网络拓扑相比，需要在 DMZ 和内部网络之间的防火墙中打开更多的端口。
- 自动系统部署（仅限 50 个、250 个或 800 个并发用户的系统）需要在 vCenter 中进行更详细的设置。
- 由于所有会议的加载都是通过互联网反向代理来进行的，因此在三种网络拓扑中，此配置对网络性能的影响最大。 因为存在多个中继段，所以还会影响网络延迟时间。

注释 请参阅网络带宽要求，第 52 页，了解关于非水平分割 DNS 部署的 NIC 速度要求的详细信息。

全内部网络拓扑

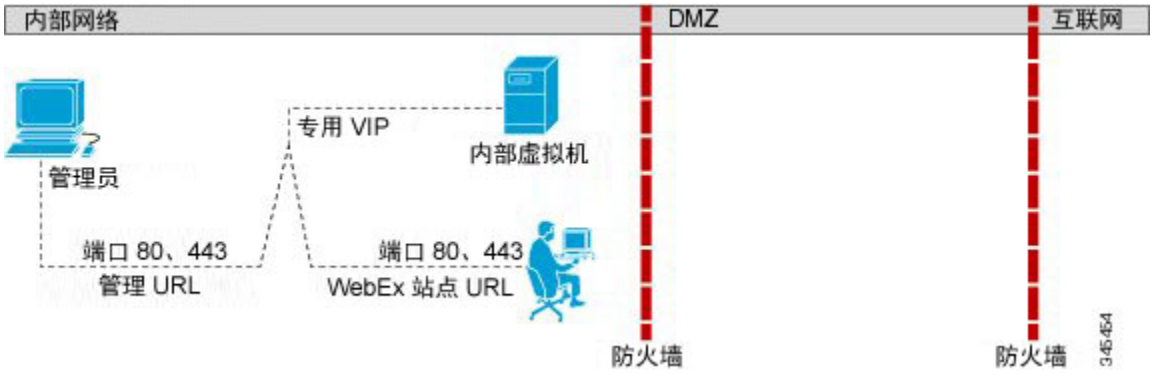
本节描述当系统中的所有虚拟机位于同一内部网络时的网络拓扑。没有公开访问；只有内部和VPN用户可以主持或加入会议。

注释 如果使用自动部署，则所有虚拟机的 ESXi 主机都必须从同一 VMware vCenter 进行管理。 自动系统部署过程中需要此 vCenter 信息。

注释 此配置不支持移动设备访问。

您将在部署系统期间定义管理 URL、WebEx 站点 URL 和专用 VIP 地址。 有关这些术语以及何时提供这些信息的更多信息，请参阅《*Cisco WebEx Meetings Server* 管理指南》中的“安装”一节。

以下是全内部网络拓扑结构的示意图。



全内部网络拓扑的优点

- 提供更低的延迟，因为虚拟机之间的网络跳转更少。

全内部网络拓扑的缺点

- 没有公开访问（允许外部用户访问系统），移动用户也不能访问。

水平分割网络拓扑

本节描述具备水平分割 DNS 时的网络拓扑。 内部虚拟机（管理虚拟机以及媒体和 Web 虚拟机（如适用））位于内部网络中，而互联网反向代理位于 DMZ 网络中。

注释 此配置允许用户从互联网安全地登录和加入会议，而无需 VPN 连接。

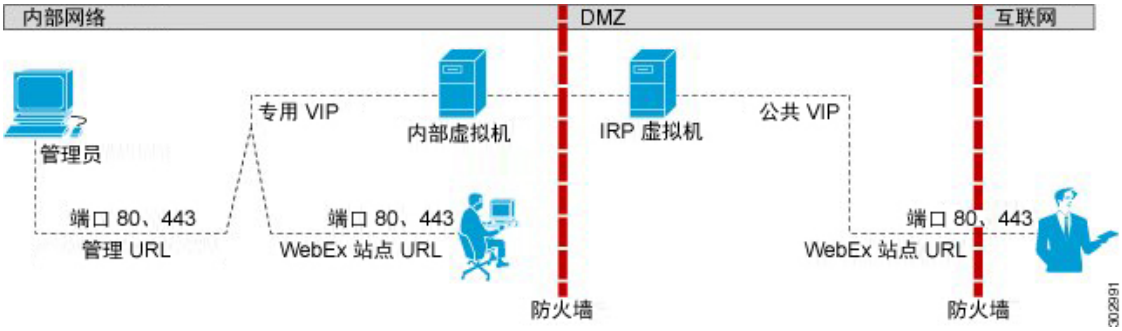
注释 此配置仅支持通过公共 IP（互联网）网络进行移动设备访问。 内部网络（内联网）不支持移动设备访问。

在水平分割部署中，源自互联网的流量（包括使用蜂窝数据网络的移动用户）会转到互联网反向代理。 源自内部的流量（包括使用本地 Wi-Fi 的移动用户）直接转到内部虚拟机。

对于此产品，水平分割和非水平分割网络拓扑之间的主要区别在于：对于水平分割系统，内部用户通过专用 VIP 地址访问 WebEx 站点 URL。 外部用户（防火墙之外）通过公共 VIP 地址访问 WebEx 站点 URL。 对于非水平分割网络，所有用户（内部和外部）都通过公共 VIP 地址访问 WebEx 站点 URL。

您将在部署系统期间定义管理 URL、WebEx 站点 URL、专用 VIP 地址和公共 VIP 地址。 有关这些术语以及何时提供这些信息的更多信息，请参阅《*Cisco WebEx Meetings Server* 管理指南》中的“安装”一节。

以下是水平分割网络拓扑的示意图。



注释 有关此部署所需的端口访问的完整列表，请参阅DMZ 网络中的互联网反向代理的端口访问，第 82 页。

水平分割网络拓扑的优点

- 能够严格控制进出网络的流量。
- 这样做可以将对系统造成冲击的网络流量分开，从而进一步分散负载。

  来自互联网的流量将转至互联网反向代理。 来自内部（专用网络）的流量将直接转至内部虚拟机（管理虚拟机，以及（若适用）媒体和 Web 虚拟机）。
- 性能和网络延迟时间优于非水平分割 DNS，但是比所有的内部网络拓扑差。

水平分割拓扑的缺点

- 在三种不同的网络拓扑中，这种网络拓扑的设置最为复杂。
- 需要复杂的 DNS 映射。
- 与各种内部网络拓扑相比，需要在 DMZ 和内部网络之间的防火墙中打开更多的端口。
- 自动系统部署（仅限 50 个、250 个或 800 个并发用户的系统）需要在 vCenter 中进行更详细的设置。

- 对于内部用户，由于网络重定向，WebEx 站点 URL 将被替换为显示包含 Web 服务的虚拟机以及媒体虚拟机主机名的 URL。

请参阅网络带宽要求，第 52 页，了解关于水平分割 DNS 部署的 NIC 速度要求的详细信息。

HA 或 MDC 部署中的冗余

通过从出现故障的主 Cisco WebEx Meetings Server (CWMS) 系统到同一物理位置中的备用 CWMS HA 系统的故障转移，高可用性 (HA) 为系统提供冗余。

CWMS 多数据中心 (MDC) 部署了多个数据中心，然后将它们加入单个 CWMS 系统。 故障转移与 HA 系统类似，不同之处在于它的MDC 系统数据中心同时服务于用户，且不受地域有限。 事实上，在靠近用户的地方部署多数据中心有助于提高网络性能。 CWMS 系统无法同时支持 HA 和 MDC。

提供冗余的条件为：

- HA 虚拟机必须与主虚拟机位于同一数据中心中。 所有这些虚拟机必须位于同一 VLAN 或子网中。 主组件和高可用性组件之间的连接的速度和延迟要求与之前为主虚拟机所定义的相同。 我们不支持在数据中心之间分割系统的主组件和 HA 组件。

  MDC 虚拟机无需位于同一个数据中心内。

- 所有内部虚拟机之间的连接必须完全冗余，这样如果交换机或网络链路故障，不会切断主组件与 HA 或 MDC 组件之间的连接。 要实现此冗余，每台主机服务器都应具有到多个以太网交换机的冗余连接。

- 主互联网反向代理虚拟机和 HA 互联网反向代理虚拟机必须位于公共 VLAN 或子网（通常是与内部虚拟机不同的子网）中。 与内部虚拟机一样，互联网反向代理虚拟机之间的连接也应该冗余。

  在 MDC 系统中加入数据中心后，可在数据中心上启用或禁用 IRP。 在 CWMS MDC 系统中，所有数据中心的 IRP 配置必须匹配；不允许出现不匹配的情况。

添加 HA 或 MDC 系统不会增加总系统容量。 无论部署的 800 个用户的系统是否具有高可用性，总系统容量仍然相同；最大并发音频连接数均为 800。

HA 或 MDC 系统由部署中的各类虚拟机的冗余虚拟机所组成。 （有关每种虚拟机类型的描述，请参阅系统中的虚拟机，第 8 页。）例如：

- 50 个用户的系统拥有一个管理虚拟机，有时拥有一个互联网反向代理 (IRP) 虚拟机（用于公开访问）。 如果添加 HA（MDC 不可用）系统，则合并后的 50 个用户的系统拥有两个管理虚拟机和两个 IRP 虚拟机。

- 250 个或 800 个用户的主系统由管理虚拟机、媒体虚拟机和 IRP 虚拟机（可选）组成。 如果添加 HA 或 MDC 系统，则合并后的 250 个用户或 800 个用户的系统拥有两个管理虚拟机、两个媒体虚拟机和两个 IRP 虚拟机。

- 2000 个用户的主系统拥有一个管理虚拟机、三个媒体虚拟机、两个 Web 虚拟机和一个 IRP 虚拟机（可选）。 如果添加 HA 或 MDC 系统，则合并后的 2000 个用户的系统拥有两个管理虚拟

机、四个媒体虚拟机（其中一个为冗余）、三个 Web 虚拟机（其中一个为冗余）和两个 IRP 虚拟机。

在 HA 或 MDC 系统中，公共 VIP 地址和专用 VIP 地址是与主系统共享的。（公共 VIP 地址和专用 VIP 地址不同且不共享。）当一个虚拟机停机时，另一个虚拟机将使用相同的 VIP 地址。正因如此，虚拟机故障对用户而言透明，同时会议继续进行，对 DNS 基础结构也没有特殊的需求。但是，只能在单个网段或 VLAN 上实施 VIP 地址共享；跨越两个数据中心分割 VLAN 会造成很多问题。

我们要求主虚拟机和 HA 内部虚拟机之间的连接位于相同的数据中心中，这将显著减少区分虚拟机故障和网络故障所带来的问题。允许网络分割可导致会议连接被分割和数据库更新冲突。更加实用的方法是在单数据中心而不是多数据中心内构建真正的 HA 网段。

在 MDC 系统中，会跨数据中心复制数据（许可证管理器除外）。因此，如果某个数据中心停运或网络连接丢失，续存数据中心将继续为用户提供服务，这与地理位置无关。

在大多数系统组件运行状态为“全部活动”时建立容错系统是最好的方法。然而，某些关键组件（特别是数据库服务）的状态为“活动/待机”。（HA 系统中的 Web 服务器和媒体组件依赖于主系统的组件。）连接中的任何延迟或中断都会对用户造成延迟，尤其是在加入会议时。媒体服务组件之间的延迟将增加会议期间某些用户的音频和视频延迟。（对于 Cisco WebEx Meetings Server，在内部虚拟机之间 4 ms 的网络延迟是可以接受的。有关更多详细信息，请参阅网络中的虚拟机布局，第 43 页。）

互联网反向代理的网络注意事项

互联网反向代理虚拟机的常规联网要求与内部虚拟机相同。对于非水平分割和水平分割 DNS 配置，需要在 DMZ 网络（而非内部网络）中部署互联网反向代理虚拟机。

限制 即使为 Cisco UCS 服务器配置了两个 NIC，Cisco WebEx Meetings Server 也不支持将一个 NIC 指向互联网而另一个 NIC 指向内部网。无论 vSphere（和互联网反向代理）使用的物理 NIC 和虚拟 NIC 之间如何映射，此限制都有效。

无论您使用多少 NIC，互联网反向代理虚拟机总是只连接一个外部 VLAN。如果使用多个物理 NIC，并且它们连接到不同的交换机或路由器，那么这些 NIC 也必须连接到同一个 VLAN。

因此，不能使用互联网反向代理在两个不同的网段（一个指向互联网，另一个指向内部网）之间桥接通信。下一节描述如何能够实现此目的。

内部虚拟机和互联网反向代理之间的延迟

互联网反向代理上的 NIC 和任意内部虚拟机上的 NIC 之间路径上的最大可接受往返延迟应该设置为低于 4 毫秒。此路径上延迟过大将限制最终用户可用于音频、视频和桌面共享的带宽。例如，如果延迟由 4 毫秒增加至 8 毫秒，则可使用带宽将减半，用户体验由于延迟增加将逐渐降级。

注释 4 ms 延迟限制不适用于任意 Cisco WebEx Meetings Server 组件与最终用户端点之间的路径。

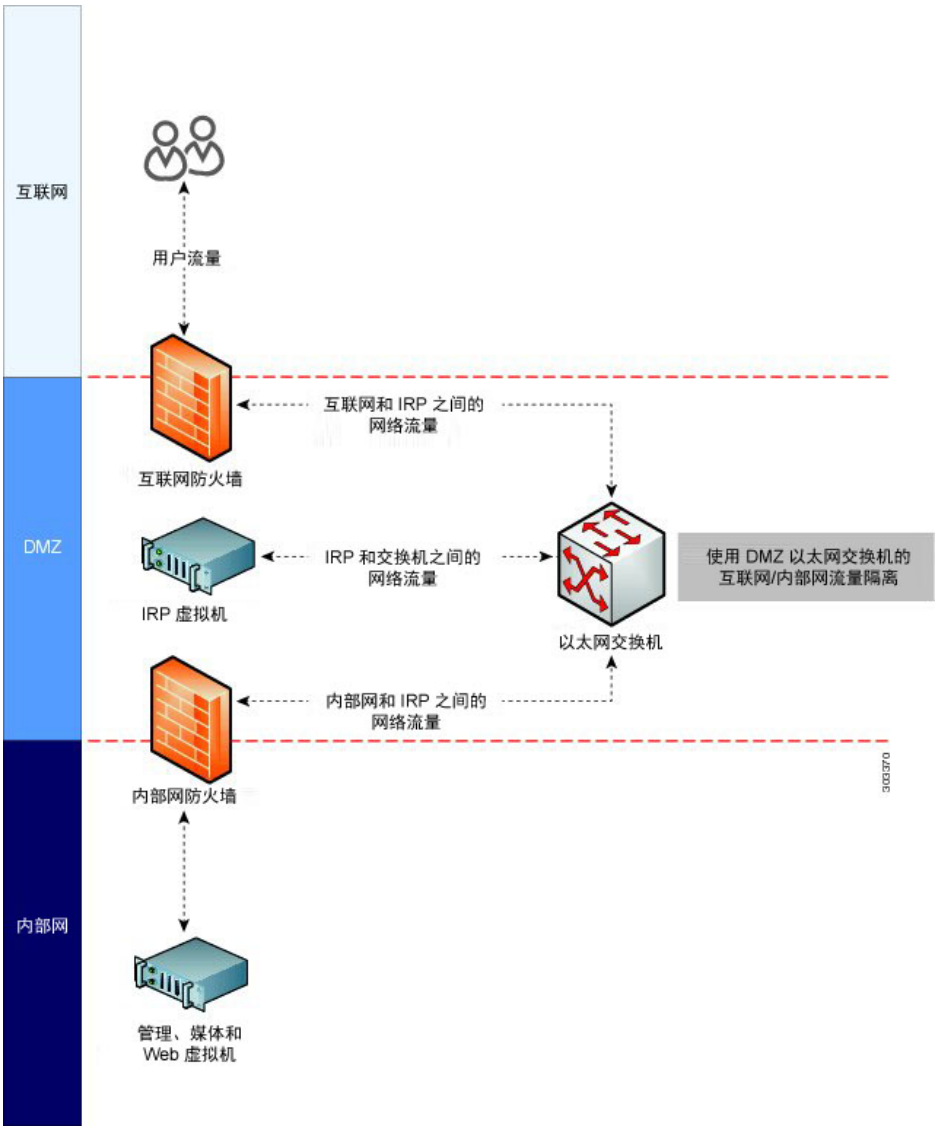
注释 当 IRP 和内部虚拟机之间的延迟超过 4 毫秒时，通过 Cisco WebEx Meetings Server 互联网反向代理的最终用户连接可能导致潜在的严重延迟。

网络流量隔离

可以在互联网和您的内部网络之间使用 DMZ 以太网交换机设置网络流量隔离。 以下过程和示意图描述了一个示例：

1. 将互联网反向代理连接到前端交换机或路由器，并使用该交换机或路由器分割互联网和内部网流量。
2. 交换机或路由器分割流量后，您就可以将这两种流量模式引导到交换机或路由器上两个不同的物理端口。 一个端口指向互联网，另一个端口指向内部网。

此处是示例网络拓扑的示意图：



有关网络带宽要求的信息，请参见网络带宽要求，第 52 页。

网络带宽要求

本节描述 50、250、800 和 2000 个用户的系统的带宽要求。 满足本节中所述的带宽要求可以为主持和参加 WebEx 会议的用户提供优质的最终用户体验，并有助于确保网络支持 Web 共享、音频和视频提出的流量要求。

估计最终用户会话的带宽

必须按照用户系统的大小估计支持视频、音频和 Web 共享的流量要求所需的网络带宽。 此产品的带宽要求基本与 Cisco WebEx 云服务的带宽要求相同。 如果您希望优化网络设置，WebEx 网络带宽白皮书中介绍了 Cisco WebEx 云服务带宽使用情况。

下表中的信息显示了视频、音频和 Web 共享的预期带宽。

WebEx Meeting 组件	最终用户会话聚合带宽
视频（360p + 6 幅缩略图）	1.5 Mb/s
音频	0.1 Mb/s
Web 共享 （此值假定您每 30 秒翻一张幻灯片。）	0.6 Mb/s
最大总带宽	2.2 Mb/s

虽然一个用户连接的预期最大带宽是 2.2 Mb/s，但 Cisco 建议在计算带宽要求时使用 1.5 Mb/s 的预期最大带宽。因为在同一时刻只有占最大数量一半的用户可以使用视频、音频和 Web 共享，而其他用户应该只使用音频和 Web 共享，所以平均带宽大约是每个用户连接 1.5 Mb/s。

如果查阅《*WebEx* 网络带宽白皮书》，您将注意到上表中的带宽值是依据最坏情况下的流量状况计算的。 平均带宽利用率将小得多，但 Cisco 由于以下原因建议使用最坏情况的数字：

- 使用最坏情况的数字进行计算有助于您提供必要带宽，防止用户体验由于用量过大而变差。
- Cisco WebEx Meetings Server 会同时向会议的所有参加者发送相同数据。 当 WebEx 主持人翻动演示文稿的页面时，系统会尽快将该页面的图像（可能有好几兆字节）同时分发到每个端点。

网络路径上的带宽

使用下列过程确定各种网络路径上的必要带宽。

1. 使用前一节提供的表格确定用户会话的平均带宽。
2. 确定您预计通过该链路同时连接的最大用户数。
3. 用总带宽乘以最大用户数。

方案示例：

- 如果您预计最多有 100 个用户从互联网并发连接，那么您可能在 ISP 连接上需要 1.5 Mb/s x 100 = 150 Mb/s 的可用带宽经外部防火墙连接到互联网反向代理。 有关互联网反向代理的详细信息，请参阅 互联网反向代理的网络注意事项 ， 第 50 页
- 假定您有一个 2000 用户的系统，其所有连接都经过互联网反向代理。 在此方案中，您需要假定全部 2000 个用户的流量都将连接到互联网反向代理，然后从互联网反向代理连接到内部虚拟机。 从网络其他部分接入互联网反向代理的聚合出入带宽将为 2000 x 1.5 Mb/s = 3 Gb/s。 有关非水平分割的详细信息，请参阅非水平分割网络拓扑 ， 第 45 页。

注释 通过互联网反向代理入站和出站的流量都是3 Gb/s，这就要求互联网反向代理上的NIC处理6 Gb/s的用户流量。 请参阅下一节，了解互联网反向代理上NIC的带宽要求的更多相关信息。

- 假定您在水平分割的DNS部署中有2000个用户的系统。 在此方案中，您的互联网用户将连接到互联网反向代理，而内部网用户直接连接到内部虚拟机。 假定10%的用户使用互联网连接到会议，而90%的用户通过内部网连接会议。 结果是进入互联网反向代理的聚合带宽约为300 Mb/s（2000个用户的10%乘以1.5 Mb/s等于300 Mb/s）。 如果从互联网反向代理出站的流量也是300 Mb/s，那么互联网反向代理上的NIC需要处理600 Mb/s的用户流量。 这样的带宽要求比前一个方案中描述的非水平分割DNS部署低得多。 网络流量的减少对关于NIC或交换机接口速度的建议（见下一节）有直接影响，可能使您得以在互联网反向代理的Cisco UCS服务器上部署较便宜的1 Gb/s NIC，或在DMZ网络中使用较便宜的千兆位以太网交换机基础结构。 有关水平分割的更多详细信息，请参阅水平分割网络拓扑，第47页。

注释 如果互联网反向代理用量非常接近1000 Mb/s阈值，您可能需要部署配置为使用NIC Teaming的千兆位以太NIC。

请参阅用于带宽聚合的NIC Teaming，第56页以获取更多详细信息。

Cisco WebEx Meetings Server网络接口上的带宽

对于交换架构和系统之间的直接接口，我们建议提供的接口NIC要达到下表中显示的最大速度。 这些速度仅适用于本地交换基础结构中Cisco UCS服务器和前端交换器上端口之间的连接。 这些速度是支持最坏情况流量要求所需的建议速度。

系统容量	NIC或交换机接口速度
50个用户的系统	1 Gb/s
250个用户的系统	1 Gb/s
800个用户的系统	10 Gb/s[18][19]
2000个用户的系统	10 Gb/s[20]

18 您可以选择在UCS服务器上使用两个或更多千兆位以太网NIC部署NIC Teaming，或在前端交换机上部署NIC Teaming，以降低网络基础结构成本。

19 对于800个用户的系统，如果使用内部DAS存储进行部署，您可以选择在UCS服务器上使用两个或两个以上千兆位以太网NIC部署NIC Teaming，或在前端交换机上部署NIC Teaming，以降低网络基础结构成本。 但是，如果使用SAN或NAS存储进行部署，您将需要万兆位以太网链接。

20 如果您有非水平分割DNS部署，那么对于IRP和内部虚拟机有10 Gb/s的要求。 如果使用水平分割DNS部署，您可以降低IRP（和DMZ网络）上的网络基础结构要求，从而能按“网络路径上的带宽”一节所述，在互联网反向代理的Cisco UCS服务器上部署较便宜的1 Gb/s NIC，或在DMZ网络中部署较便宜的千兆位以太网交换机基础结构。 但是对于内部虚拟机（和内部网络）仍有10 Gb/s的速度要求。

请参阅下文的“水平分割 DNS 部署的带宽注意事项”一节，了解关于对水平分割 DNS 部署使用 1 Gb/s NIC 和以太网交换机的更多信息。

NIC 速度计算的假设前提：

- 最终用户会话聚合带宽 (1.5 Mb/s) 用于计算上表中显示的 NIC 速度。
- 虚拟机之间的控制通信必须无拥塞。 这一点对于 2000 个用户的系统和任何为实现高可用性提供的系统特别重要。 虚拟机链路上的严重拥塞可能导致系统不稳定，进而引起服务中断。
- 与 NAS 存储（用于录制文件和数据库备份）的连接不能出现拥塞。
- 协议开销和实施效率低下导致可用的链路带宽明显少于 1 Gb/s 或 10 Gb/s 的标示速度。
- 如果在用户登录到会议时流量有很大一部分命中互联网反向代理，那么您需要记住，每个用户连接都要两次经过互联网反向代理上的 NIC（入站和出站）。 以 2000 个用户的系统为例，这意味着互联网反向代理上的 NIC 可能需要处理 6 Gb/s 的用户流量（2000 个用户乘以 1.5 Mb/s 等于 3 Gb/s，考虑到出站和入站流量还要乘以 2，等于 6 Gb/s）。

我们的保守要求是本地连接最多60%用于最终用户媒体流量，允许剩下的40%用于其他流量、非常流量爆发和网络开销。以800个用户的系统为例，我们估计管理和媒体虚拟机的最终用户流量为1.2 Gb/s，互联网反向代理虚拟机的最终用户流量为 2.4 Gb/s。 按照 60% 规则，我们要求管理虚拟机和媒体虚拟机的 NIC 可以处理 2 Gb/s（管理和媒体虚拟机的评估用户流量 1.2 Gb/s 除于 60% 等于评估标称带宽消耗 2.0 Gb/s），互联网反向代理虚拟机的 NIC 可以处理 4 Gb/s。

注释 上表中显示的 NIC 速度未考虑用于访问 SAN 存储器的带宽。 如果对 SAN 连接使用以太网光纤通道 (FCoE)，应该配置其使用一个独立的网络接口。

水平分割 DNS 部署的带宽注意事项

使用水平分割DNS部署时，有些用户将从互联网登录到会议，其流量将命中互联网反向代理，而在内部网上的大多数用户登录到会议时不命中互联网反向代理。 使用水平分割 DNS 部署时，如果您加快网络速度并将通信分段，使大多数流量留在内部网络中（而不命中互联网反向代理），那么可以使用 NIC Teaming 并在互联网反向代理上配置较低端的 NIC (1 Gb/s NIC)，将互联网反向代理和互联网之间的交换基础结构配置为 1 Gb/s，或至少降低 2000 个用户的系统的 10 Gb/s 建议要求。

例如，如果一家公司有 100 个用户要从互联网并发访问 2000 端口用户的系统，您需要 150 Mb/s 的带宽（1.5 Mb/s 用户会话聚合带宽 * 100 个用户 = 150 Mb/s）。 这意味着从 DMZ 网络到互联网反向代理的网络基础结构可以是 1 Gb/s 以太网交换机，而互联网反向代理上的以太网 NIC 接口可以是 1 Gb/s，而非所谓的 10 Gb/s 接口要求。 即使考虑到互联网反向代理上通过的流量会翻倍（也就是说它的 NIC 将必须处理 300 Mb/s 的用户流量），按照 60% 规则（已在“Cisco WebEx Meetings Server 网络接口上的带宽”一节中说明）需要 500 Mb/s， 那么 1 Gb/s 的链路也已足够。但如果我们假设外部用户是 250 人而非 100 人，那就不够了。

注释 带宽优化只能用于水平分割 DNS 部署中互联网反向代理上的 NIC。

对于非水平分割 DNS 部署，您必须部署 10 Gb/s 以太网交换机和互联网反向代理上的 10 Gb/s 以太网 NIC 接口。

多数据中心的网络要求

两个数据中心之间的网络链接要求：

- 保证 4.5 Mbps 的带宽，以实现基本的数据中心间通信。
- 低于 200 ms 延迟（往返时间延迟）。

实现数据中心间级联会议的数据中心网络要求：

- 每个具有音频和 Web 的级联会议要求 0.16 Mbps。
- 每个具有低画质视频（按 180p）、音频和 Web 的级联会议要求 0.66 Mbps。
- 每个具有高清视频（按 360p）、音频和 Web 的级联会议要求 1.20 Mbps。
- 低于 200 ms 延迟（往返时间延迟）。

例如最坏情况下对于 2000 个用户的系统（级联了最大数目 1000 个会议）。 其中一半有视频、一半没有：

- 高清视频： 500 x 1.2 + 500 x 0.16 = 680 Mbps
- 低画质视频： 500 x 0.66 + 500 x 0.16 = 410 Mbps

对于 800 个用户的系统：

- 高清视频： 680 / 2000 x 800 = 272 Mbps
- 低画质视频： 410 / 2000 x 800 = 164 Mbps

对于 250 个用户的系统：

- 高清视频： 680 / 2000 x 250 = 85 Mbps
- 低画质视频： 410 / 2000 x 250 = 51.25 Mbps

要了解更多信息，请访问http://www.cisco.com/c/en/us/products/conferencing/webex-meeting-center/white-paper-listing.html。

用于带宽聚合的 NIC Teaming

在包含带内部虚拟机的 ESXi 主机的 UCS 服务器上配置 NIC Teaming 可带来两个好处： NIC Teaming 可在物理和虚拟网络之间进行网络流量负载平衡，并在硬件故障或网络断电情况下提供故障转移。此外，对于没有 10 Gb/s 基础结构的部署，您还可以聚合多个 1 Gb/s NIC 以获得相当于 10 Gb/s 的效果。

注释 有关不同大小用户系统所需的NIC速度的更多信息，请参阅本章中“Cisco WebEx Meetings Server网络接口上的带宽”一节。

Cisco 支持对各种大小的用户系统（50、250、800 和 2000 个用户的系统）使用 NIC Teaming 进行带宽负载平衡，但该功能最适合客户用于优化 800 个用户的系统的联网成本。 如果使用内部 DAS 存储进行部署，则对于 800 个用户系统的 Cisco UCS 服务器和前端交换机的聚合出入带宽需求，预计使用两块千兆位以太网 NIC（或者在带 HA 的系统上使用四块千兆位以太网 NIC）支持即可基本支持最坏情况下的流量需求，从而免于为 UCS 服务器提供万兆位以太网 NIC（或购买万兆位以太网前端交换机）。

注释 如果使用 SAN 或 NAS 存储进行部署，则对于 800 个用户系统的 Cisco UCS 服务器和前端交换机的聚合出入带宽需求为万兆位以太网。

注释 有关在 VMware 中提供 NIC teaming 的信息，请参阅位于 http://kb.vmware.com 的 VMware 文档，搜索“NIC teaming in ESXi/ESX”。

在使用传统网络接口和以太网交换机的前提下，可以按下列过程所述使用NIC teaming和双工交换机提供冗余：

- 设置支持 IEEE 802.3ad/IEEE 802.1ax 链路聚合控制协议 (LACP) 的以太网交换机。
- 使用 vCenter 将与 Cisco WebEx Meetings Server 虚拟机关联的虚拟机端口组连接到两个物理适配器。
- 将两个物理适配器都连接到交换机。
- 配置交换机，使其将两个端口作为一个组静态地进行供应。
- 使用 VMware vSphere 将 NIC Teaming 设置为“活动/活动”，以允许在两个 NIC 接口上通信。

例如，对于 800 用户部署，可以将有内部虚拟机的 ESXi 主机上的每条 10 Gb/s 链路替换为两条 1 Gb/s 链路，将互联网反向代理上的每条 10 Gb/s 链路替换为四条 1 Gb/s 链路。 （按照“HA 部署的冗余网络连接”所述，要在有 HA 的系统上实现容错，必须将链路数翻倍。） 对于有内部虚拟机的 ESXi 主机，应将两条 1 Gb/s 链路连接到第一个以太网交换机，将另两条 1 Gb/s 链路连接到第二个以太网交换机。

注释 《*Cisco WebEx Meetings Server* 系统要求》中显示的服务器配置示例没有包括足以支持用于此目的的 NIC Teaming 的网络接口。

负载平衡

负载平衡始终在 CWMS 上完成，不管正在处理什么类型的通信，并且它不可配置。

系统设法在所有 Web 节点上均等地平衡负载。 当部署为不具有高可用性 (HA) 的系统时，连接在该系统的所有 Web 节点之间进行平衡。 在具有 HA 功能的部署情况下，系统使用主系统和 HA 系统上的 Web 节点进行负载平衡。 如果其中之一，而不是全部 Web 节点出现故障，那么系统保持活动，但是容量减少。

互联网反向代理 (IRP) 节点是入口点，并且在该处进行大多数负载平衡决定。 系统中仅一个 IRP 节点是活动的。 不具有 HA 部署的系统只有一个 IRP 节点。 具有 HA 部署的系统具有两个 IRP 节点，一个 IRP 活动，另一个停用。 根据 DNS 配置，IRP 处理所有外部通信（并且在非分割 DNS 情况下，还处理所有内部通信）。

如果存在涉及多个主机的故障，那么可能会影响功能和容量。

第 4 章

系统的网络核对表

网络核对表列出系统所需的网络更改，这取决于您的 DNS 配置以及您是否启用了公开访问（允许用户从互联网或移动设备主持或参加会议）。

根据正在使用的是自动系统部署（推荐用于 50、250 或 800 个用户的部署）还是手动系统部署（必须用于 2000 个用户的部署）来选择相应的核对表。

- 所有虚拟机（包括互联网反向代理）位于内部网络中（最简单的配置）

  采用自动部署并包含公开访问的安装或扩展的网络核对表， 第 60 页

  采用手动部署并包含公开访问和所有内部虚拟机的安装或扩展的网络核对表， 第 62 页

- 非水平分割 DNS（最常用的 DNS 配置）

  采用自动部署并包含公开访问和非水平分割 DNS 的安装或扩展的网络核对表， 第 65 页

  采用手动部署并包含公开访问和非水平分割 DNS 的安装或扩展的网络核对表， 第 68 页

- 水平分割 DNS

  采用自动部署并包含公开访问和水平分割 DNS 的安装或扩展的网络核对表， 第 71 页

  采用手动部署并包含公开访问和水平分割 DNS 的安装或扩展的网络核对表， 第 73 页

- 无公开访问的系统

  采用自动部署且无公开访问的安装或扩展的网络核对表， 第 76 页

  采用手动部署且公开访问的安装或扩展的网络核对表， 第 78 页

- 采用自动部署并包含公开访问的安装或扩展的网络核对表， 第 60 页
- 采用手动部署并包含公开访问和所有内部虚拟机的安装或扩展的网络核对表， 第 62 页
- 采用自动部署并包含公开访问和非水平分割 DNS 的安装或扩展的网络核对表， 第 65 页
- 采用手动部署并包含公开访问和非水平分割 DNS 的安装或扩展的网络核对表， 第 68 页

- 采用自动部署并包含公开访问和水平分割 DNS 的安装或扩展的网络核对表， 第 71 页
- 采用手动部署并包含公开访问和水平分割 DNS 的安装或扩展的网络核对表， 第 73 页
- 采用自动部署且无公开访问的安装或扩展的网络核对表， 第 76 页
- 采用手动部署且公开访问的安装或扩展的网络核对表， 第 78 页
- WebEx 站点和 WebEx 管理 URL， 第 80 页
- 当所有虚拟机都位于内部网络中时的端口访问， 第 82 页
- DMZ 网络中的互联网反向代理的端口访问， 第 82 页
- VMware vCenter 端口， 第 86 页
- Cisco WebEx Meeting Center 端口， 第 88 页
- 对系统采用 NAT， 第 88 页
- 正向代理， 第 91 页

采用自动部署并包含公开访问的安装或扩展的网络核对表

虚拟机部署

在自动部署过程中，我们将为您部署除管理虚拟机之外的所有虚拟机。 如果您准备部署 50 个、250 个或 800 个用户的系统，我们建议您选择自动部署。

- 验证媒体虚拟机（如适用）与管理虚拟机位于同一子网中。
- 验证内部网络中存在互联网反向代理虚拟机。
- 验证从同一 VMware vCenter 管理所有虚拟机的 ESXi 主机（包括互联网反向代理）。

所需的 IP 地址

描述	网络位置	IP 地址
管理虚拟机的实际 IP 地址	内部	
媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
互联网反向代理的实际 IP 地址	内部虚拟机（可能和管理虚拟机位于同一子网中）	
管理URL（由系统专用。 映射到专用VIP地址）	内部虚拟机（与管理虚拟机位于同一子网中）	

描述	网络位置	IP 地址
WebEx 站点 URL（由系统专用。 映射到公共 VIP 地址）	内部虚拟机（与互联网反向代理位于同一子网中） 此IP地址必须是可公开路由的。	
高可用性管理虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性互联网反向代理（如适用）的实际 IP 地址	内部虚拟机[与主系统的互联网反向代理位于同一子网中（但可以将 NAT 与专用 IP 地址配合使用）]	

DNS 配置

按如下所示更新 DNS 服务器。 对于 WebEx 站点 URL 和管理站点 URL 的主机名部分，有一些限制。 有关不能使用的单词的列表，请参阅WebEx 站点和 WebEx 管理 URL ， 第 80 页。

任务	示例
内部虚拟机的主机名和 IP 地址： 管理虚拟机及适用的媒体虚拟机。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
互联网反向代理虚拟机的主机名和 IP 地址。	• <IRP-vm-FQDN> <IRP-vm-IP-address>
管理站点 URL 和专用 VIP 地址。	• <Administration-site-URL> <Private-VIP-address>
WebEx 站点 URL 和公共 VIP 地址。	• <WebEx-site-URL> <Public-VIP-address>

防火墙配置

出于安全性考虑，我们建议您将互联网反向代理置于与内部虚拟机（管理虚拟机或媒体虚拟机）不同的子网中。 请参阅当所有虚拟机都位于内部网络中时的端口访问，第 82 页。

网络路由配置

任务	示例
在内部网络和 DMZ 网络之间启用 Layer 3 路由。	• 内部子网<internal-subnet>/24 • DMZ 子网<DMZ-subnet>/24
验证公共 VIP 地址和互联网反向代理虚拟机位于同一子网中。 [如果您准备将所有系统虚拟机部署在内部（互联网反向代理不在 DMZ 内），那么该子网必须位于内部网络中。]	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
验证专用 VIP 地址和内部虚拟机位于同一子网中。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

采用手动部署并包含公开访问和所有内部虚拟机的安装或扩展的网络核对表

虚拟机部署

在手动部署过程中，您可以从 vSphere 客户端使用 OVA 向导来为系统创建所有虚拟机。 然后可以通过手动部署安装系统。

如果您准备部署 2000 个用户的系统，则必须选择手动部署。

- 确保任何其他内部虚拟机（适用的媒体和 Web 虚拟机）与管理虚拟机位于同一子网中。
- 确保内部网络中存在互联网反向代理虚拟机。

所需的 **IP** 地址

描述	网络位置	**IP** 地址
管理虚拟机的实际 IP 地址	内部	
媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
第二台媒体虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
第三台媒体虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
Web 虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
第二台 Web 虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
互联网反向代理的实际 IP 地址	内部虚拟机（可能和管理虚拟机位于同一子网中）	
管理URL（由系统专用。 映射到专用VIP地址）	内部虚拟机（与管理虚拟机位于同一子网中）	
WebEx 站点 URL（由系统专用。 映射到公共 VIP 地址）	内部虚拟机（与互联网反向代理位于同一子网中） **注释** 此 IP 地址必须是可公开路由的。	
高可用性管理虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性 Web 虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性互联网反向代理（如适用）的实际 IP 地址	内部虚拟机—与主系统的互联网反向代理位于同一子网中（但可以将 NAT 与专用 IP 地址配合使用）	

DNS 配置

对 DNS 配置进行以下更改。

注释 对于 WebEx 站点 URL 和管理站点 URL 的主机名部分，有一些限制。 要查看您不能使用的单词的列表，请参见WebEx 站点和 WebEx 管理 URL，第 80 页。

任务	示例
使用以下内部虚拟机的主机名和IP地址更新DNS服务器： 管理虚拟机及适用的媒体和 Web 虚拟机。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
用互联网逆向代理虚拟机的主机名和 IP 地址更新 DNS 服务器。	• <IRP-vm-FQDN> <IRP-vm-IP-address>
用管理站点 URL 和专用 VIP 地址信息更新 DNS 服务器。	• <Administration-site-URL> <Private-VIP-address>
用 WebEx 站点 URL 和公共 VIP 地址信息更新 DNS 服务器。	• <WebEx-site-URL> <Public-VIP-address>

防火墙配置

出于安全考虑，Cisco 建议您将互联网反向代理置于与内部虚拟机（管理虚拟机及适用的媒体和 Web 虚拟机）不同的子网中。

虽然我们也支持将所有虚拟机（互联网反向代理虚拟机和内部虚拟机）置于同一子网中，但是不建议这样做。 请参阅当所有虚拟机都位于内部网络中时的端口访问，第 82 页。

网络路由配置

对网络路由进行以下更改。

任务	比较这些 IP 地址
对于下列虚拟机，在内部网络和 DMZ 网络之间启用 L3 (Layer 3) 路由： 管理虚拟机及适用的媒体和 Web 虚拟机	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
确保公共VIP地址和互联网反向代理虚拟机位于同一子网中。 注释 如果您准备将所有系统虚拟机部署在内部（互联网反向代理不在DMZ内），那么该子网必须位于内部网络中。	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
确保专用VIP地址和内部虚拟机（管理虚拟机及适用的媒体和 Web 虚拟机）位于同一子网中。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

采用自动部署并包含公开访问和非水平分割DNS的安装或扩展的网络核对表

虚拟机部署

在自动部署过程中，我们将为您部署除管理虚拟机之外的所有虚拟机。 如果您准备部署 50 个、250 个或 800 个用户的系统，我们建议您选择自动部署。

- 验证媒体虚拟机（如适用）与管理虚拟机位于同一子网中。
- 验证 DMZ 网络中存在互联网反向代理虚拟机。

所需的 IP 地址

描述	网络位置	IP 地址
管理虚拟机的实际 IP 地址	内部	
媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
互联网反向代理的实际 IP 地址	DMZ（但是可以将 NAT 与专用 IP 地址配合使用）	
管理URL（由系统专用。 映射到专用VIP地址）	内部虚拟机（与管理虚拟机位于同一子网中）	
WebEx 站点 URL（由系统专用。 映射到公共 VIP 地址）	DMZ（与互联网反向代理位于同一子网中）	
高可用性管理虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性互联网反向代理（如适用）的实际 IP 地址	DMZ [与主系统的互联网反向代理位于同一子网中（但可以将 NAT 与专用 IP 地址配合使用）]	

DNS 配置

按如下所示更新 DNS 服务器。 对于 WebEx 站点 URL 和管理站点 URL 的主机名部分，有一些限制。 有关不能使用的单词的列表，请参阅WebEx 站点和 WebEx 管理 URL ， 第 80 页。

任务	示例
内部虚拟机的主机名和 IP 地址： 管理虚拟机及适用的媒体虚拟机。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
互联网反向代理虚拟机的主机名和 IP 地址。	• <IRP-vm-FQDN> <IRP-vm-IP-address>

任务	示例
管理站点 URL 和专用 VIP 地址。	• <Administration-site-URL> <Private-VIP-address>
WebEx 站点 URL 和公共 VIP 地址。	• <WebEx-site-URL> <Public-VIP-address>

防火墙配置

出于安全性考虑，我们建议您将互联网反向代理置于与内部虚拟机（管理虚拟机或媒体虚拟机）不同的子网中。 请参阅当所有虚拟机都位于内部网络中时的端口访问，第 82 页。

网络路由配置

对网络路由进行以下更改。

任务	比较这些 IP 地址
在内部网络和 DMZ 网络之间启用 Layer 3 路由。	• 内部子网<internal-subnet>/24 • DMZ 子网<DMZ-subnet>/24
验证公共 VIP 地址和互联网反向代理虚拟机位于同一子网中。	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
验证专用 VIP 地址和内部虚拟机位于同一子网中。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

采用手动部署并包含公开访问和非水平分割DNS的安装或扩展的网络核对表

虚拟机部署

在手动部署过程中，您可以从 vSphere 客户端使用 OVA 向导来为系统创建所有虚拟机。 然后可以通过手动部署安装系统。

如果您准备部署 2000 个用户的系统，则必须选择手动部署。

- 确保任何其他内部虚拟机（适用的媒体和 Web 虚拟机）与管理虚拟机位于同一子网中。
- 确保互联网反向代理虚拟机位于 DMZ 网络中。

所需的 IP 地址

描述	网络位置	IP 地址
管理虚拟机的实际 IP 地址	内部	
媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
第二台媒体虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
第三台媒体虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
Web 虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
第二台 Web 虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
互联网反向代理的实际 IP 地址	DMZ（但是可以将 NAT 与专用 IP 地址配合使用）	
管理URL（由系统专用。 映射到专用VIP地址）	内部虚拟机（与管理虚拟机位于同一子网中）	
WebEx 站点 URL（由系统专用。 映射到公共 VIP 地址）	DMZ（与互联网反向代理位于同一子网中）	
高可用性管理虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	

描述	网络位置	IP 地址
高可用性 Web 虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性互联网反向代理（如适用）的实际 IP 地址	DMZ—与主系统的互联网反向代理位于同一子网中（但可以将 NAT 与专用 IP 地址配合使用）	

DNS 配置

对 DNS 配置进行以下更改。

注释 对于 WebEx 站点 URL 和管理站点 URL 的主机名部分，有一些限制。 要查看您不能使用的单词的列表，请参见WebEx 站点和 WebEx 管理 URL，第 80 页。

任务	示例
使用以下内部虚拟机的主机名和IP地址更新DNS服务器： 管理虚拟机及适用的媒体和 Web 虚拟机。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
用互联网逆向代理虚拟机的主机名和 IP 地址更新 DNS 服务器。	• <IRP-vm-FQDN> <IRP-vm-IP-address>
用管理站点 URL 和专用 VIP 地址信息更新 DNS 服务器。	• <Administration-site-URL> <Private-VIP-address>
用 WebEx 站点 URL 和公共 VIP 地址信息更新 DNS 服务器。	• <WebEx-site-URL> <Public-VIP-address>

防火墙配置

出于安全考虑，Cisco 建议您将互联网反向代理置于与内部虚拟机（管理虚拟机及适用的媒体和 Web 虚拟机）不同的子网中。 请参阅DMZ 网络中的互联网反向代理的端口访问 ， 第 82 页。

网络路由配置

对网络路由进行以下更改。

任务	比较这些 IP 地址
对于下列虚拟机，在内部网络和 DMZ 网络之间启用 L3 (Layer 3) 路由： 管理虚拟机及适用的媒体和 Web 虚拟机	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
确保公共 VIP 地址和互联网反向代理虚拟机位于同一子网中。	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
确保专用 VIP 地址和内部虚拟机（管理虚拟机及适用的媒体和 Web 虚拟机）位于同一子网中。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

采用自动部署并包含公开访问和水平分割DNS的安装或扩展的网络核对表

虚拟机部署

在自动部署过程中，我们将为您部署除管理虚拟机之外的所有虚拟机。 如果您准备部署 50 个、250 个或 800 个用户的系统，我们建议您选择自动部署。

- 验证媒体虚拟机（如适用）与管理虚拟机位于同一子网中。
- 验证 DMZ 网络中存在互联网反向代理虚拟机。

所需的 IP 地址

描述	网络位置	IP 地址
管理虚拟机的实际 IP 地址	内部	
媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
互联网反向代理的实际 IP 地址	DMZ（但是可以将 NAT 与专用 IP 地址配合使用）	
管理URL（由系统专用。 映射到专用VIP地址）	内部虚拟机（与管理虚拟机位于同一子网中）	
WebEx 站点 URL（由系统专用。 映射到两个 VIP 地址）： • 内部用户 - 专用 VIP 地址 • 外部用户 - 公共 VIP 地址	• 内部用户 — 内部虚拟机（与管理虚拟机位于同一子网） • 外部用户 — DMZ（与互联网反向代理位于同一子网）	
高可用性管理虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	

描述	网络位置	IP 地址
高可用性互联网反向代理（如适用）的实际 IP 地址	DMZ [与主系统的互联网反向代理位于同一子网中（但可以将 NAT 与专用 IP 地址配合使用）]	

DNS 配置

按如下所示更新 DNS 服务器。 对于 WebEx 站点 URL 和管理站点 URL 的主机名部分，有一些限制。 有关不能使用的单词的列表，请参阅WebEx 站点和 WebEx 管理 URL ， 第 80 页。

任务	示例
内部虚拟机的主机名和 IP 地址： 管理虚拟机及适用的媒体虚拟机。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
DMZ 虚拟机的主机名和 IP 地址。	• <IRP-vm-FQDN> <IRP-vm-IP-address>
WebEx 站点 URL、管理网站 URL 和专用 VIP 地址信息。	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>
WebEx 站点 URL 和公共 VIP 地址。	• <WebEx-site-URL> <Public-VIP-address>

防火墙配置

出于安全性考虑，我们建议您将互联网反向代理置于与内部虚拟机（管理虚拟机或媒体虚拟机）不同的子网中。 请参阅当所有虚拟机都位于内部网络中时的端口访问 ， 第 82 页。

网络路由配置

对网络路由进行以下更改。

任务	比较这些 IP 地址
在内部网络和 DMZ 网络之间启用 Layer 3 路由。	• 内部子网<internal-subnet>/24 • DMZ 子网<DMZ-subnet>/24
验证公共 VIP 地址和互联网反向代理虚拟机位于同一子网中。	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
验证专用 VIP 地址和内部虚拟机位于同一子网中。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

采用手动部署并包含公开访问和水平分割DNS的安装或扩展的网络核对表

虚拟机部署

在手动部署过程中，您可以从 vSphere 客户端使用 OVA 向导来为系统创建所有虚拟机。 然后可以通过手动部署安装系统。

如果您准备部署 2000 个用户的系统，则必须选择手动部署。

- 确保任何其他内部虚拟机（适用的媒体和 Web 虚拟机）与管理虚拟机位于同一子网中。
- 确保互联网反向代理虚拟机位于 DMZ 网络中。

所需的 IP 地址

描述	网络位置	IP 地址
管理虚拟机的实际 IP 地址	内部	
媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	

描述	网络位置	IP 地址
第二台媒体虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
第三台媒体虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
Web 虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
第二台 Web 虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
互联网反向代理的实际 IP 地址	DMZ（但是可以将 NAT 与专用 IP 地址配合使用）	
管理URL（由系统专用。 映射到专用VIP地址）	内部虚拟机（与管理虚拟机位于同一子网中）	
WebEx 站点 URL（由系统专用。 映射到两个 VIP 地址） • 内部用户 - 专用 VIP 地址 • 外部用户 - 公共 VIP 地址	• 内部用户 — 内部虚拟机（与管理虚拟机位于同一子网） • 外部用户 — DMZ（与互联网反向代理位于同一子网）	
高可用性管理虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性 Web 虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性互联网反向代理（如适用）的实际 IP 地址	DMZ—与主系统的互联网反向代理位于同一子网中（但可以将 NAT 与专用 IP 地址配合使用）	

DNS 配置

对 DNS 配置进行以下更改。

注释 对于 WebEx 站点 URL 和管理站点 URL 的主机名部分，有一些限制。 要查看您不能使用的单词的列表，请参见WebEx 站点和 WebEx 管理 URL，第 80 页。

任务	示例
使用以下内部虚拟机的主机名和IP地址更新DNS服务器（启用内部查找）： 管理虚拟机及适用的媒体和 Web 虚拟机。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
使用 DMZ 虚拟机的主机名和 IP 地址来更新 DNS 服务器（启用内部查找）：	• <IRP-vm-FQDN> <IRP-vm-IP-address>
使用 WebEx 站点 URL、管理站点 URL 和专用 VIP 地址信息来更新 DNS 服务器（启用内部查找）。	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>
使用 WebEx 站点 URL 和公共 VIP 地址信息来更新 DNS 服务器（启用外部查找）。	• <WebEx-site-URL> <Public-VIP-address>

防火墙配置

出于安全考虑，Cisco 建议您将互联网反向代理置于与内部虚拟机（管理虚拟机及适用的媒体和 Web 虚拟机）不同的子网中。 请参阅DMZ 网络中的互联网反向代理的端口访问，第 82 页。

网络路由配置

对网络路由进行以下更改。

任务	比较这些 IP 地址
对于下列虚拟机，在内部网络和 DMZ 网络之间启用 L3 (Layer 3) 路由： 管理虚拟机及适用的媒体和 Web 虚拟机	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
确保公共 VIP 地址和互联网反向代理虚拟机位于同一子网中。	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
确保专用 VIP 地址和内部虚拟机（管理虚拟机及（如果适用）媒体和 Web 虚拟机）位于同一子网。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

采用自动部署且无公开访问的安装或扩展的网络核对表

虚拟机部署

在自动部署过程中，我们将为您部署除管理虚拟机之外的所有虚拟机。 如果您准备部署 50 个、250 个或 800 个用户的系统，我们建议您选择自动部署。

验证媒体虚拟机（如适用）与管理虚拟机位于同一子网中。

所需的 IP 地址

描述	网络位置	IP 地址
管理虚拟机的实际 IP 地址	内部	

描述	网络位置	IP 地址
媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
管理URL（由系统专用。 映射到专用VIP地址）	内部虚拟机（与管理虚拟机位于同一子网中）	
高可用性管理虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性互联网反向代理（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	

DNS 配置

按如下所示更新 DNS 服务器。 对于 WebEx 站点 URL 和管理站点 URL 的主机名部分，有一些限制。 有关不能使用的单词的列表，请参阅WebEx 站点和 WebEx 管理 URL ， 第 80 页。

任务	示例
内部虚拟机的主机名和 IP 地址： 管理虚拟机及适用的媒体虚拟机。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
WebEx 站点 URL、管理网站 URL 和专用 VIP 地址信息。	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>

防火墙配置

任务	示例
配置内部网络中的所有防火墙，以允许 Web 浏览器访问专用 VIP 地址。	HTTP <Private-VIP-address>:80 HTTPS <Private-VIP-address>:443

网络路由配置

任务	比较这些 IP 地址
验证专用 VIP 地址和内部虚拟机位于同一子网中。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

采用手动部署且公开访问的安装或扩展的网络核对表

虚拟机部署

在手动部署过程中，您可以从 vSphere 客户端使用 OVA 向导来为系统创建所有虚拟机。 然后可以通过手动部署安装系统。

如果您准备部署 2000 个用户的系统，则必须选择手动部署。

- 确保任何其他内部虚拟机（适用的媒体和 Web 虚拟机）与管理虚拟机位于同一子网中。

所需的 IP 地址

描述	网络位置	IP 地址
管理虚拟机的实际 IP 地址	内部	
媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
第二台媒体虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
第三台媒体虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
Web 虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
第二台 Web 虚拟机（仅限 2000 个用户的系统）的实际 IP 地址	内部虚拟机（与管理虚拟机位于同一子网中）	
管理URL（由系统专用。 映射到专用VIP地址）	内部虚拟机（与管理虚拟机位于同一子网中）	

描述	网络位置	IP 地址
WebEx 站点 URL（由系统专用。 映射到专用 VIP 地址）	内部虚拟机（与管理虚拟机位于同一子网中）	
高可用性管理虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性媒体虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	
高可用性 Web 虚拟机（如适用）的实际 IP 地址	内部虚拟机（与主系统的管理虚拟机位于同一子网中）	

DNS 配置

对 DNS 配置进行以下更改。

注释 对于 WebEx 站点 URL 和管理站点 URL 的主机名部分，有一些限制。 要查看您不能使用的单词的列表，请参见WebEx 站点和 WebEx 管理 URL，第 80 页。

任务	示例
使用以下内部虚拟机的主机名和IP地址更新DNS服务器（启用内部查找）： 管理虚拟机及适用的媒体和 Web 虚拟机。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
使用管理站点 URL、WebEx 站点 URL 和专用 VIP 地址信息更新 DNS 服务器。	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>

防火墙配置

对防火墙进行以下更改。

任务	示例
配置内部网络中的所有防火墙，以允许 Web 浏览器访问专用 VIP 地址。	• HTTP <Private-VIP-address>:80 • HTTPS <Private-VIP-address>:443

网络路由配置

对网络路由进行以下更改。

任务	比较这些 IP 地址
确保专用VIP地址和内部虚拟机（管理虚拟机及适用的媒体和 Web 虚拟机）位于同一子网中。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

WebEx 站点和 WebEx 管理 URL

WebEx 站点 URL

用户可访问 WebEx 站点 URL 以安排、主持或出席会议。 根据您是否使用水平分割 DNS，此 URL 将解析为专用 VIP 地址或公用 VIP 地址。

- 如果您没有水平分割 DNS，它会为所有用户解析为公共 VIP 地址。
- 如果您有水平分割 DNS，则对外部用户将解析为公用 VIP 地址。
- 如果您有水平分割 DNS，则对内部用户会解析为专用 VIP 地址。

注释 必须对 WebEx 站点 URL 打开端口 80 和 443。

WebEx 管理 URL

管理员可访问 WebEx 管理 URL 以配置、管理和监控系统。 该 URL 将解析到专用 VIP 地址。

注释 必须对 WebEx 管理 URL 打开端口 80 和 443。

WebEx 站点和 WebEx 管理 URL 的名称

几乎可以为这些 URL 选择任何由全小写字符组成的名称。 但是，不能使用下列名称作为 URL 中的主机名：

- 与系统中任何虚拟机的主机名相同的名称
- authentication
- client
- companylogo
- dispatcher
- docs
- elm-admin
- elm-client-services
- emails
- maintenance
- Manager
- orion
- oriondata
- oriontemp
- NBR
- npp
- probe
- reminder
- ROOT
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- version
- WBXService

- WebEx

当所有虚拟机都位于内部网络中时的端口访问

本节描述当所有的系统虚拟机（管理虚拟机以及适用的媒体、Web 和互联网反向代理虚拟机）都位于内部网络时，外部防火墙中所需要的端口访问。这是内部互联网反向代理网络拓扑。（另请参阅Cisco WebEx Meeting Center 端口，第 88 页。）

确保防火墙或负载均衡解决方案将请求重定向到下方列出的端口，以确保最终用户可以成功主持和加入会议。

- 到公用虚拟 IP (VIP) 地址的 TCP 端口 80
- 到公用虚拟 IP (VIP) 地址的 TCP 端口 443

注释 Web 节点和管理节点会将 SMTP 请求发送到已配置的电子邮件服务器。 如果在内部 Web 及管理虚拟机与电子邮件服务器之间有防火墙，则 SMTP 通信可能被拦截。 要确保电子邮件服务器配置和电子邮件通知正常工作，必须在电子邮件服务器与 Web 及管理虚拟机之间打开端口 25 或 465（安全 SMTP 端口号）。

外部防火墙中的端口访问

如果您已启用公开访问，那么以下端口会在从互联网直接入站到内部网络中的互联网反向代理虚拟机时打开：

DMZ 网络中的互联网反向代理的端口访问

本节描述了当内部网络中具备内部虚拟机（管理虚拟机以及适用的媒体和 Web 虚拟机），并且 DMZ 网络中具备互联网反向代理 (IRP) 时，内部和外部防火墙中所要求的端口访问。（另请参阅Cisco WebEx Meeting Center 端口，第 88 页。）

在允许向系统虚拟机的 ESXi 主机传输信息的交换机上配置访问控制列表 (ACL)。

外部防火墙中的端口访问

请打开端口 80 (HTTP) 以及端口 443 (HTTPS) 来启用公开访问，使用户不需要记住是 HTTP 还是 HTTPS 就可输入 WebEx 站点 URL。 虽然端口 80 是打开的，但所有网络流量都会经过端口 443（SSL 加密的 HTTPS）。

重要事项 确保防火墙或负载均衡解决方案将请求重定向到下方列出的端口，以确保用户可以成功主持和加入会议。

限制 在 IRP 机器上配置 TCP 端口 64700 以拒绝发到公共 VIP 地址的任意请求。 在外部防火墙中，这会将对此端口的访问仅限于来自管理虚拟机的请求。

协议	端口	Target	目标位置	需要的原因
TCP	443	任何外部客户端。	IRP 的公共 VIP (Eth1)。	使用 HTTPS 访问 WebEx 站点 URL 的外部客户端。将发起从外部客户端计算机到 IRP 虚拟机的 TCP 连接。
TCP	80	任何外部客户端。	IRP 的公共 VIP (Eth1)。	使用 HTTP 访问 WebEx 站点 URL 的外部客户端。将发起从外部客户端计算机到 IRP 虚拟机的 TCP 连接。
TCP	8444 （在 2.5MR1、2.6 和 2.0MR6HF 中引入。）	任何外部客户端。	IRP 的公共 VIP (Eth1)。	使用 HTTPS 访问 WebEx 录制文件的外部客户端。将发起从外部客户端计算机到 IRP 虚拟机的 TCP 连接。
UDP	53	IRP 的实际 IP (Eth0)。	DNS 服务器。	如果您在虚拟机和 DNS 服务器之间设有防火墙，则需要此端口才能让系统成功部署并运行。

内部防火墙中的端口访问

如果您从内部网络到 DMZ 网络的连接受到限制，则本部分中的表格将适用。 允许从内部网络到 DMZ 网段的出站 TCP 连接。

注释 要让本产品正常工作，并不需要允许 TCP 连接从 DMZ 网段进入到内部网络。

注释 使用 IP 表或访问控制列表 (ACL) 配置防火墙，使到端口 64616 的连接只来自管理虚拟机。

注释 Web 节点和管理节点会将 SMTP 请求发送到已配置的电子邮件服务器。 如果在内部 Web 及管理虚拟机与电子邮件服务器之间有防火墙，则 SMTP 通信可能被拦截。 要确保电子邮件服务器配置和电子邮件通知正常工作，必须在电子邮件服务器与 Web 及管理虚拟机之间打开端口 25 或 465（安全 SMTP 端口号）。

注释 尤其当 IRP 处于 DMZ 网络中时，允许互联网控制消息协议 (ICMP) 回音请求和答复。 否则，如果 ICMP 回音答复未收到，则 IRP 检测和 DNS 服务器可用性验证可能失败。

协议	端口	Target	目标位置	需要的原因
TCP	64001	所有内部虚拟机 (Eth0 IP)。	IRP 虚拟机的实际 IP (Eth0)。	建立 IRP 的反向连接。将建立从内部虚拟机到 IRP 虚拟机的 TCP 连接。
TCP	64002	管理和 Web 虚拟机 (Eth0 IP)。	IRP 虚拟机的实际 IP (Eth0)。	建立 IRP 的反向连接。将建立从内部虚拟机到 IRP 虚拟机的 TCP 连接。
TCP	7001	所有内部虚拟机 (Eth0 IP)。	IRP 虚拟机的实际 IP (Eth0)。	建立 IRP 的反向连接。将发起从内部虚拟机到 IRP 虚拟机的 TCP 连接。

协议	端口	Target	目标位置	需要的原因
TCP	64616	管理虚拟机 (Eth0 IP)。	IRP 虚拟机的实际 IP (Eth0)。	引导 IRP。将发起从管理虚拟机到 IRP 虚拟机的 TCP 连接。 注释 使用 IP 表或访问控制列表 (ACL) 配置防火墙，使到端口 64616 的连接只来自管理虚拟机。
TCP	64700	管理虚拟机 (Eth0 IP)。	IRP 虚拟机的实际 IP (Eth0)。	收集有关 IRP 的日志。将发起从管理虚拟机到 IRP 虚拟机的 TCP 连接。 使用防火墙规则，使所有 Cisco WebEx Meetings Server 虚拟机上的此端口仅限其他 Cisco WebEx Meetings Server 虚拟机访问。
TCP	22	任何内部客户端计算机。	IRP 虚拟机的实际 IP (Eth0)。	使用 Remote Support 帐户对 IRP 虚拟机进行诊断。
TCP	443	任何内部客户端计算机。	管理虚拟机的专用 VIP (Eth1)。 媒体虚拟机的实际 IP (Eth0)。	使用 HTTPS 访问 WebEx 站点 URL 的内部用户。将建立从内部客户端计算机到管理虚拟机的 TCP 连接。
TCP	443	管理虚拟机的专用 VIP (Eth1) 和媒体虚拟机的实际 IP (Eth0)。	IRP 的公共 VIP (Eth1)。	

协议	端口	Target	目标位置	需要的原因
TCP	65002	任何内部客户端计算机。	任何内部虚拟机。	控制内部虚拟机之间的网络流量。
TCP	65102	任何内部客户端计算机。	任何内部虚拟机。	控制内部虚拟机之间的网络流量。
TCP	80	任何内部客户端计算机。	管理虚拟机的专用 VIP (Eth1)。	使用 HTTP 访问 WebEx 站点 URL 的内部用户。将建立从内部客户端计算机到管理虚拟机的 TCP 连接。
UDP	53	所有内部虚拟机 (Eth0 IP)。	DNS 服务器。	如果虚拟机和DNS服务器之间设有防火墙，则用于让系统成功部署并运行。
TCP	8443	Cisco WebEx Meetings Server Web 节点。	CUCM	用于多数据中心系统中的 Cisco WebEx Meetings Server 和 CUCM 之间的 AXL 流量，以允许 LDAP CUCM 故障转移。
TCP	8444	用于下载录制文件的 Cisco WebEx Meetings Server Web 节点。	管理虚拟机的专用 VIP (Eth1)。 媒体虚拟机的实际 IP (Eth0)。	使用 HTTPS 访问 WebEx 站点 URL 的内部用户。将建立从内部客户端计算机到管理虚拟机的 TCP 连接。

VMware vCenter 端口

为部署打开的端口

这些是在单数据中心 (SDC) Cisco WebEx Meetings Server 的部署期间使用的一些端口。 部署完成后，您可以关闭纯粹为部署而打开的端口。

在自动系统部署期间，用于安全 https 管理的 vCenter 与管理虚拟机之间的双向 TCP 端口 443 应打开。 管理虚拟机使用此端口提供 vCenter 凭证，以在 vCenter 中自动部署虚拟机。

下面列出的端口用于 ESXi 主机和 vCenter 之间的通信。 如果 ESXi 主机和 vCenter 连接到单独的管理网络，您可能不需要通过防火墙打开这些端口。 有关 vCenter 和 ESXi 主机所用端口的完整列表，请参阅 VMware 文档。

- vCenter 和用于 vCenter 管理的 ESXi 主机之间的双向 UDP/TCP 端口 902
- （可选）从 vSphere 客户端到用于 SSH 管理的 ESXi 主机的 TCP 端口 22
- 从系统的 ESXi 主机到内部系统日志的 UDP 端口 514
- vCenter 和用于 XML 管理的 ESXi 主机之间的双向 TCP 端口 5989

用于音频和视频数据传输的外部客户端的缺省 UDP 端口是 SSL（端口 443）。

为支持多数据中心而打开的端口

在内部虚拟机之间打开的端口	tcp 8080 tcp 8081 tcp 8082 tcp 9809 tcp 9810 tcp 9811 tcp 9812 tcp 9813 tcp 9814 tcp 9815 tcp 9816 tcp 9817 tcp 9818 tcp 9819 tcp 9820 tcp 9840 tcp 6502 tcp 12340 tcp 12342 tcp 12442 tcp 7001 tcp 7003 tcp 7004 tcp 7005 tcp:5060 tcp 5061 tcp 5062 tcp 5063 tcp 22
在内部虚拟机和虚拟 IP 之间打开的端口	tcp 443 tcp 80
在互联网反向代理 IP 和内部虚拟机之间打开的端口	tcp 7001 tcp 64001 tcp 64700 tcp 64616
在内部虚拟机之间打开的 UDP 端口	udp 范围：10000:19999 udp 范围：16000:32000 udp 范围：9000:9009 udp 5060 udp 5062

Cisco WebEx Meeting Center 端口

这些端口用于 Cisco WebEx Meeting Center 和 Cisco WebEx Meetings Server 之间的通信。

- 内部客户端用于 UDP 和 SSL 之间的音频和视频数据传输的 UDP 端口包括：
  - 对于 50 个用户的系统，使用 UDP 端口 9000
  - 对于 250 个用户的系统，使用 UDP 端口 9000、9001、9002 和 9003
  - 对于 800 个用户的系统，使用 UDP 端口 9000、9001、9002、9003、9004、9005、9006、9007、9008 和 9009
  - 对于 2000 个用户的系统，使用 UDP 端口 9000、9001、9002、9003、9004、9005、9006 和 9007
- 在合适的网络设置下，内部媒体服务器允许通过由 Meeting Center 使用的任何端口进行连接。
- 互联网反向代理仅接受 Meeting Center 通过 TCP 端口 80 和 443 建立的连接。
- 从 Web 节点到 CUCM 的 AXL 流量将通过端口 8443（另请参见使用 CUCM 配置 AXL Web 服务和目录同步）。

对系统采用 NAT

Cisco 支持在本产品中对虚拟机 IP 地址和系统所用的虚拟 IP 地址（公共和专用 VIP）使用“网络地址转换”（NAT）遍历。

以下示意图演示在不具有高可用性 (HA) 系统的情况下，50 个用户的系统的典型 NAT 遍历。 使用 NAT，您可以将产品所需的公共 *IP* 地址数减少到只有一个 IP 地址，而不是两个或三个（在部署了高可用性系统的情况下）。 只要满足总体系统要求，您也可以进行类似的 NAT 部署。

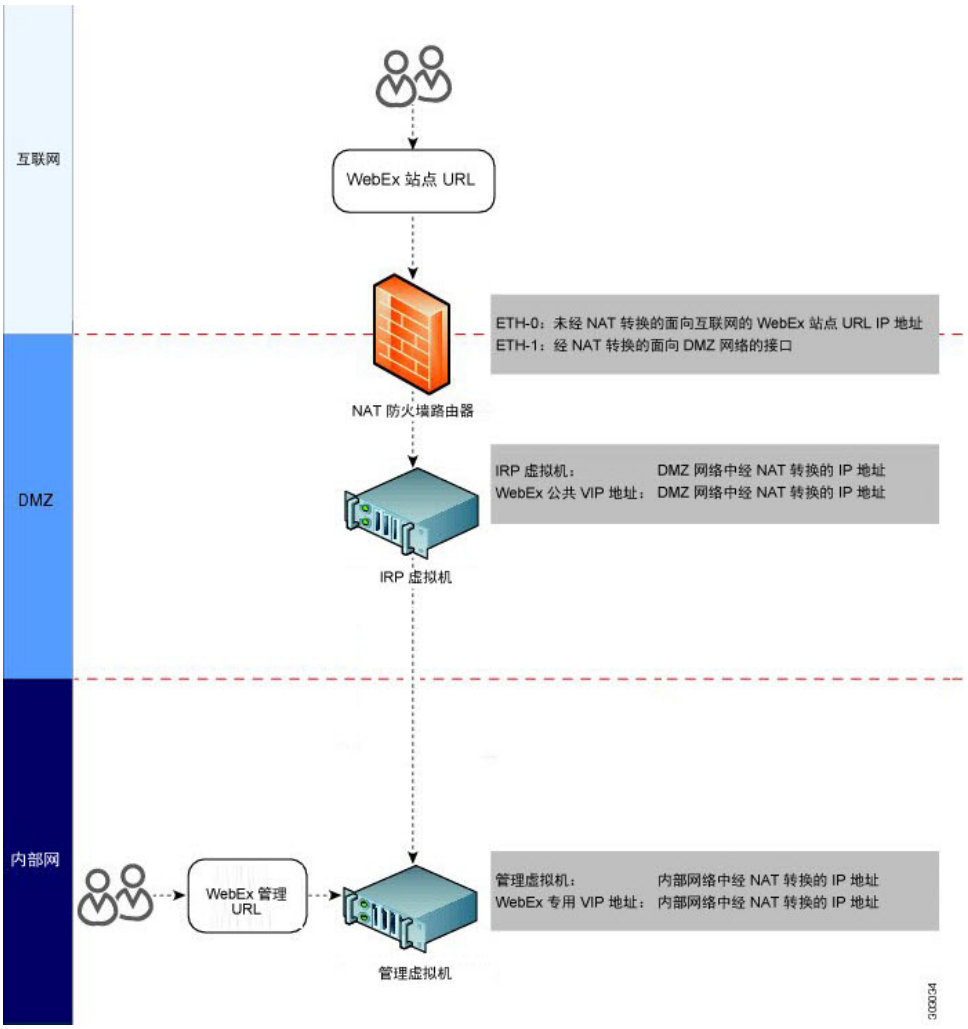
重要事项

使用多个 NAT 和防火墙容易增加延迟时间，从而影响用户的实时流量的质量。

此外，使用多个 NAT 域后，在这些不同的 NAT 域之间进行路由可能会有些困难。 只要满足以下要求，您就可以使用经过 NAT 转换的 IP 地址：

- 除了互联网反向代理虚拟机外，系统中的所有虚拟机可以使用经过 NAT 转换的 IP 地址。 管理虚拟机和互联网反向代理虚拟机之间的 NAT 不受支持。 互联网反向代理虚拟机的 IP 地址（其真实 IP 地址）必须可由管理虚拟机通过内部网络进行访问。
- 公共 VIP 地址本身不需公开可见，但是必须可从互联网进行转换。
- 部署公开访问时，WebEx 站点 URL 必须映射至互联网可见的 IP 地址。 此互联网可见的 IP 地址必须可被外部用户所访问，而且要映射至系统部署过程中配置的公共 VIP 地址。

  您可选择使该公共 VIP 地址在互联网上可见。 如果您选择不使其公开可见，那么它必须可从互联网进行转换。



在上图中，某个外部用户访问 WebEx 站点来加入或主持会议。 在 DNS 查找之后，WebEx 站点的 IP 地址是 NAT 公共 IP 地址（Eth0）。 此 NAT 公共 IP 地址用于外部网络与 DMZ 网络之间的外部 NAT 防火墙路由器（防火墙和 NAT 路由器 1）。

防火墙路由器从外部用户接收此请求，并在内部将此请求路由到路由器的NAT专用IP地址（Eth1，向 DMZ 网络公开）。 Eth1 然后将此请求发送到公共 VIP 地址（也是 WebEx 站点专用网段的 NAT IP 地址）。

您可使用公共 VIP 地址的 NAT IP 地址以及互联网反向代理 IP 地址。 唯一 NAT 公共 IP 地址是 NAT 防火墙路由器的 Eth0 IP 地址。

注释 要确保此 NAT 防火墙路由器（位于互联网和 DMZ 网络之间）对传入数据包进行正确路由，请设置 NAT 设备上的端口映射配置或应用其他相似机制，以确保数据包正确路由至公共 VIP 地址和互联网反向代理。

DMZ 网络与内部网络之间通常还有一个内部 NAT 防火墙路由器。 与外部 NAT 防火墙路由器类似，Eth0 是 DMZ NAT 专用 IP 地址以及到 DMZ 网络的接口。 Eth1 也是 NAT 专用 IP 地址以及到内部网络的接口。

您可使用专用 VIP 地址的 NAT IP 地址以及管理虚拟机 IP 地址。

有关 NAT 的更多信息，请参阅http://www.cisco.com/c/en/us/tech/ip/ip-addressing-services/tech-tech-notes-list.html。

正向代理

如果网络拓扑结构包含正向代理，那么这些代理必须满足互联网反向代理的特定要求才能正常工作。请参阅《*Cisco WebEx Meetings Server* 疑难解答指南》中的“系统中的正向代理的使用”以获取完整的详细信息。

第 5 章

配置 Cisco Unified Communications Manager (CUCM)

要在 Cisco WebEx Meetings Server 上启用电话会议，必须配置一个（或多个）Cisco Unified Communications Manager (CUCM) 系统来管理呼叫控制。 您可以选择为音频高可用性配置另一个 CUCM 系统。

- MDC 环境中的 CUCM， 第 94 页
- 准备工作， 第 94 页
- MDC 环境中的 CUCM 安全电话会议， 第 95 页
- 多数据中心的 CUCM 配置核对表， 第 95 页
- 具有或不具有高可用性的 CUCM 配置核对表， 第 95 页
- 在 CWMS 多数据中心系统中配置 CUCM， 第 96 页
- 为高可用性和非高可用性系统配置 CUCM， 第 99 页
- 配置 SIP 中继安全配置文件， 第 103 页
- 配置 SIP 配置文件， 第 104 页
- 使用 TLS 进行 CUCM 证书管理， 第 106 页
- 配置 SIP 中继， 第 112 页
- 配置路由组， 第 115 页
- 配置路由列表， 第 116 页
- 配置路由模式， 第 117 页
- 配置 SIP 路由模式， 第 117 页
- CUCM 功能兼容性和支持， 第 118 页

MDC 环境中的 CUCM

多数据中心 (MDC) 环境中的 CUCM 配置与单数据中心 (SDC) 环境中相同。 在一个数据中心上修改的配置参数将自动在另一个数据中心上进行匹配。

就 CUCM 而言，多数据中心 (MDC) 环境中的基本配置与单数据中心 (SDC) 环境中相同。 但是，您必须为所有数据中心配置中继。 每个数据中心可以有不同的路由模式。 如果想使用多个CUCM，则每个数据中心必须为另一个数据中心的 CUCM 配置 SIP 中继，用于转移呼叫。

准备工作

从 Cisco WebEx Meetings Server **音频**页面获取负载平衡器服务器和应用程序服务器信息。 负载平衡器服务器管理呼叫负载平衡，应用程序服务器管理呼叫、会议流和功能控制。 不同大小的系统具有不同数目的负载平衡器服务器和应用程序服务器，并且数目不是定制的。 登录管理站点并选择**设置** > **音频**以查看此信息。

- 大小 (50/250/800/2000)
- 高可用性
- 传输类型

在**音频**页面，存在显示负载平衡器服务器和应用程序服务器信息（包括 IP 地址和端口）的 SIP 配置表。 此表还显示在首次配置音频设置时出现的**首次配置音频设置**页面上。

要使 CUCM 与 Cisco WebEx Meetings Server 配合使用，CUCM 需要以下基本和特定配置：

- 基本配置

  注释 这些配置可以与多个 Cisco WebEx Meetings Server 系统共享。

  SIP 中继安全配置文件

  SIP 配置文件

- 特定配置

  注释 必须针对单个 Cisco WebEx Meetings Server 系统进行这些配置，并且无法由多个系统共享。

  证书管理

  SIP 中继

  路由组

路由列表

路由模式

SIP 路由模式

MDC 环境中的 CUCM 安全电话会议

当证书的公用名相同时，为确保电话会议的安全，不能将多数据中心 (MDC) 中所有数据中心的证书导入到单个 Cisco Unified Call Manager (CUCM) 中。

缺省情况下，所有数据中心的公用名均为系统的全球站点 URL。但是，为了使公用名唯一，您可以通过对 2.6 版和更高版本使用 生成证书签名请求 (CSR) 2.6 版和更高版本，第 109 页 或对 2.5 版和更低版本使用 生成证书签名请求 (CSR) 2.5 版和更低版本，第 110 页 来生成证书。 选择在公用名中使用本地站点 URL，而非全球站点 URL。

在任何系统改动过程（例如更改站点或管理 URL、更改主机名）中生成的自签名证书，其公用名将使用全球站点 URL，因此必须在此类操作后手动创建使用本地站点 URL 的证书。

多数据中心的 CUCM 配置核对表

配置核对表显示须为多数据中心 (MDC) 系统配置的各 Cisco Unified Communication Manager (CUCM) 配置类型。

系统容量	安全配置文件（基本配置）	SIP 配置文件（基本配置）	SIP 中继（特定配置）	路由组（特定配置）	路由列表（特定配置）	路由模式（特定配置）	SIP 路由模式（特定配置）
250 个用户	2	1	4	1	1	N	2
800 个用户	2	1	4	1	1	N	2
2000 个用户（带有 HA）	2	1	6	1	1	N	4

具有或不具有高可用性的 CUCM 配置核对表

配置核对表显示须为带有或不带有高可用性的单数据中心 (SDC) 系统配置的各 Cisco Unified Communication Manager (CUCM) 配置类型。

系统容量	安全配置文件（基本配置）	SIP 配置文件（基本配置）	SIP 中继（特定配置）	路由组（特定配置）	路由列表（特定配置）	路由模式（特定配置）	SIP 路由模式（特定配置）
50 个用户	2	1	2	1	1	N[21]	1
50 个用户（带有 HA）	2	1	4	1	1	N	2
250 个用户	2	1	2	1	1	N	1
250 个用户（带有 HA）	2	1	4	1	1	N	2
800 个用户	2	1	2	1	1	N	1
800 个用户（带有 HA）	2	1	4	1	1	N	2
2000 个用户	2	1	5	1	1	N	3
2000 个用户（带有 HA）	2	1	6	1	1	N	4

21 N 是指您在 Cisco WebEx Meetings Server 中配置的呼入接入号码的数量。

在 CWMS 多数据中心系统中配置 CUCM

通常，多数据中心 (MDC) 环境中的每个站点都有与之关联的专用 CUCM 群集。 CUCM 集群之间使用集群间中继 (ICT) 进行连接。 每个 CUCM 集群都有本地 CWMS 站点的呼入/拨号中继。 支持 Session Manager Edition (SME)。 可在本地 CUCM 集群之后配置 CWMS。 每个 CUCM 都有 MDC 中所有媒体虚拟机的 SIP REFER 中继。

为实现冗余，每个 CUCM 群集都可以有所有数据中心的 INVITE 中继。 呼入路由模式为与本地数据中心关联的 INVITE 中继赋予优先权，且仅在失败时才使用远程数据中心的 INVITE 中继。

表 *4*：各个 *CUCM* 群集上配置的 *CUCM SIP* 中继

部署	INVITE 中继 - 负载平衡器 (MACC)	REFER 中继 - 应用程序服务器 (TAS)
小	2	2

部署	INVITE 中继 - 负载平衡器 (MACC)	REFER 中继 - 应用程序服务器 (TAS)
中	2	2
大	4	6

在 250 个或 800 个用户的多数据中心系统中配置 CUCM

为一个 250 个或 800 个用户的多数据中心系统配置 Cisco Unified Communication Manager (CUCM)。通常，每个数据中心都有本地 CUCM 群集。

开始之前

需要的信息：

- 每个数据中心一个负载平衡服务器的 IP 地址
- 每个数据中心一个应用程序服务器的 IP 地址
- 您将在系统上配置的呼入接入号码的数量

步骤 1 复查现有 SIP 中继安全配置文件并确定其是否满足 Cisco WebEx Meetings Server 设置要求。 如果不满足，请配置两个 SIP 中继安全配置文件。
为负载平衡服务器和应用程序服务器各添加 SIP 中继安全配置文件。 请参阅为负载平衡服务器配置 SIP 中继安全配置文件 ， 第 103 页和为应用程序服务器配置 SIP 中继安全配置文件 ， 第 104 页。

步骤 2 复查现有 SIP 配置文件并确定其是否满足 Cisco WebEx Meetings Server 设置要求。 如果不满足，请配置一个 SIP 配置文件。
按照 配置 TLS SIP 配置文件或配置 IPv6 SIP 配置文件 ， 第 105 页中的描述配置 SIP 配置文件。

步骤 3 为负载平衡服务器配置两个 SIP 中继。
请参阅在负载平衡服务器上配置 SIP 中继。

步骤 4 为应用程序服务器配置两个 SIP 中继。
请参阅为应用程序服务器配置 SIP 中继。

步骤 5 通过使用您为负载平衡服务器配置的 SIP 中继来配置一个路由组。
请参阅配置路由组。

步骤 6 通过使用您在上一步配置的路由组来配置一个路由列表。
请参阅配置路由列表。

步骤 7 通过使用上述路由列表来配置 *N* 个路由模式。
N 是指您在管理站点上的音频设置中配置的呼入接入号码的数量。 请参阅配置路由模式。

步骤 8 为应用程序服务器配置两个 SIP 路由模式。
请参阅配置 SIP 路由模式。

在 2000 个用户的多数据中心系统中配置 CUCM

为一个 2000 个用户的多数据中心系统配置 Cisco Unified Communication Manager (CUCM)。 通常，每个数据中心都有本地 CUCM 群集。

开始之前

需要的信息：

- 每个数据中心两个负载平衡服务器的 IP 地址
- 每个数据中心三个应用程序服务器的 IP 地址
- 您将在系统上配置的呼入接入号码的数量

步骤 1 复查现有 SIP 中继安全配置文件并确定其是否满足 Cisco WebEx Meetings Server 设置要求。 如果不满足，请配置两个 SIP 中继安全配置文件。
为负载平衡服务器和应用程序服务器各添加 SIP 中继安全配置文件。 请参阅为负载平衡服务器配置 SIP 中继安全配置文件， 第 103 页和为应用程序服务器配置 SIP 中继安全配置文件， 第 104 页。

步骤 2 复查现有 SIP 配置文件并确定其是否满足 Cisco WebEx Meetings Server 设置要求。 如果不满足，请配置一个 SIP 配置文件。
按照 配置 TLS SIP 配置文件或配置 IPv6 SIP 配置文件， 第 105 页中的描述配置 SIP 配置文件。

步骤 3 为负载平衡服务器配置两个 SIP 中继。
请参阅在负载平衡服务器上配置 SIP 中继。

步骤 4 为应用程序服务器配置四个 SIP 中继。
请参阅为应用程序服务器配置 SIP 中继。

步骤 5 通过使用您为负载平衡服务器配置的 SIP 中继来配置一个路由组。
请参阅配置路由组。

步骤 6 通过使用您在上一步配置的路由组来配置一个路由列表。
请参阅配置路由列表。

步骤 7 通过使用上述路由列表来配置 *N* 个路由模式。
N 是指您在管理站点上的音频设置中配置的呼入接入号码的数量。 请参阅配置路由模式。

步骤 8 为应用程序服务器配置四个 SIP 路由模式。
请参阅配置 SIP 路由模式。

为高可用性和非高可用性系统配置 CUCM

以下各节描述了配置不同大小的高可用性和非高可用性系统所需的任务。

在不具有高可用性系统的 50 个、250 个和 800 个用户的系统上配置 CUCM

为无高可用性系统的 50 个、250 个和 800 个用户的系统配置 CUCM。

开始之前

需要的信息：

- 一个负载平衡服务器的 IP 地址
- 一个应用程序服务器的 IP 地址
- 您将在系统上配置的呼入接入号码的数量

步骤 1 复查现有 SIP 中继安全配置文件并确定其是否满足 Cisco WebEx Meetings Server 设置要求。 如果不满足，请配置两个 SIP 中继安全配置文件。
为负载平衡服务器和应用程序服务器各添加 SIP 中继安全配置文件。 请参阅为负载平衡服务器配置 SIP 中继安全配置文件 ， 第 103 页和为应用程序服务器配置 SIP 中继安全配置文件 ， 第 104 页。

步骤 2 复查现有 SIP 配置文件并确定其是否满足 Cisco WebEx Meetings Server 设置要求。 如果不满足，请配置一个 SIP 配置文件。
按照 配置 TLS SIP 配置文件或配置 IPv6 SIP 配置文件 ， 第 105 页中的描述配置 SIP 配置文件。

步骤 3 为负载平衡服务器配置一个 SIP 中继。
请参阅在负载平衡服务器上配置 SIP 中继。

步骤 4 为应用程序服务器配置一个 SIP 中继。
请参阅为应用程序服务器配置 SIP 中继。

步骤 5 通过使用您为负载平衡服务器配置的 SIP 中继来配置一个路由组。
请参阅配置路由组。

步骤 6 通过使用您在上一步配置的路由组来配置一个路由列表。
请参阅配置路由列表。

步骤 7 通过使用上述路由列表来配置 *N* 个路由模式。
N 是指您在管理站点上的音频设置中配置的呼入接入号码的数量。 请参阅配置路由模式。

步骤 8 为应用程序服务器配置两个 SIP 路由模式。

请参阅配置 SIP 路由模式。

在具有高可用性系统的 50 个、250 个或 800 个用户的系统上配置 CUCM

本节描述为具有高可用性系统的 50 个、250 个或 800 个用户的系统配置 CUCM 所需要的信息以及如何进行配置的详细说明。

需要的信息

- 两个负载平衡服务器的 IP 地址
- 两个应用程序服务器的 IP 地址
- 您将在系统上配置的呼入接入号码的数量

配置过程

执行下列步骤：

任务	描述	详细信息
1	复查现有 SIP 中继安全配置文件并确定其是否满足 Cisco WebEx Meetings Server 设置要求。如果不满足，请配置两个 SIP 中继安全配置文件。	为负载平衡服务器和应用程序服务器各添加 SIP 中继安全配置文件。 请参阅为负载平衡服务器配置 SIP 中继安全配置文件，第 103 页和为应用程序服务器配置 SIP 中继安全配置文件，第 104 页。
2	复查现有 SIP 配置文件并确定其是否满足 Cisco WebEx Meetings Server 设置要求。 如果不满足，请配置一个 SIP 配置文件。	按照 配置 TLS SIP 配置文件或配置 IPv6 SIP 配置文件，第 105 页中的描述配置 SIP 配置文件。
3	为负载平衡服务器配置两个 SIP 中继。	请参阅在负载平衡服务器上配置 SIP 中继。
4	为应用程序服务器配置两个 SIP 中继。	请参阅为应用程序服务器配置 SIP 中继。
5	通过使用您在上述任务 3 中为负载平衡服务器配置的 SIP 中继来配置一个路由组。	请参阅配置路由组。
6	通过使用您在上述任务 5 中配置的路由组来配置一个路由列表。	请参阅配置路由列表。
7	通过使用上述路由列表来配置 *N* 个路由模式。*N* 是指您在管理站点上的音频设置中配置的呼入接入号码的数量。	请参阅配置路由模式。
8	为应用程序服务器配置两个 SIP 路由模式。	请参阅配置 SIP 路由模式。

在不具有高可用性系统的 2000 个用户的系统上配置 CUCM

为一个无高可用性系统的 2000 个用户的系统配置 Cisco Unified Communication Manager (CUCM)。

开始之前

需要的信息：

- 两个负载平衡服务器的 IP 地址
- 三个应用程序服务器的 IP 地址
- 您将在系统上配置的呼入接入号码的数量

步骤 1 复查现有 SIP 中继安全配置文件并确定其是否满足 Cisco WebEx Meetings Server 设置要求。 如果不满足，请配置两个 SIP 中继安全配置文件。
为负载平衡服务器和应用程序服务器各添加 SIP 中继安全配置文件。 请参阅为负载平衡服务器配置 SIP 中继安全配置文件，第 103 页和为应用程序服务器配置 SIP 中继安全配置文件，第 104 页。

步骤 2 复查现有 SIP 配置文件并确定其是否满足 Cisco WebEx Meetings Server 设置要求。 如果不满足，请配置一个 SIP 配置文件。
按照 配置 TLS SIP 配置文件或配置 IPv6 SIP 配置文件，第 105 页中的描述配置 SIP 配置文件。

步骤 3 为负载平衡服务器配置两个 SIP 中继。
请参阅在负载平衡服务器上配置 SIP 中继。

步骤 4 为应用程序服务器配置三个 SIP 中继。
请参阅为应用程序服务器配置 SIP 中继。

步骤 5 通过使用您为负载平衡服务器配置的 SIP 中继来配置一个路由组。
请参阅配置路由组。

步骤 6 通过使用您在上一步配置的路由组来配置一个路由列表。
请参阅配置路由列表。

步骤 7 通过使用上述路由列表来配置 *N* 个路由模式。
N 是指您在管理站点上的音频设置中配置的呼入接入号码的数量。 请参阅配置路由模式。

步骤 8 为应用程序服务器配置两个 SIP 路由模式。
请参阅配置 SIP 路由模式。

接下来的操作

在具有高可用性系统的 2000 个用户的系统上配置 CUCM

为一个具有高可用性系统的 2000 个用户的系统配置 Cisco Unified Communication Manager (CUCM)。

开始之前

需要的信息：

- 两个负载平衡服务器的 IP 地址
- 四个应用程序服务器的 IP 地址
- 您将在系统上配置的呼入接入号码的数量

步骤 1 复查现有 SIP 中继安全配置文件并确定其是否满足 Cisco WebEx Meetings Server 设置要求。 如果不满足，请配置两个 SIP 中继安全配置文件。
为负载平衡服务器和应用程序服务器各添加 SIP 中继安全配置文件。 请参阅为负载平衡服务器配置 SIP 中继安全配置文件，第 103 页和为应用程序服务器配置 SIP 中继安全配置文件，第 104 页。

步骤 2 复查现有 SIP 配置文件并确定其是否满足 Cisco WebEx Meetings Server 设置要求。 如果不满足，请配置一个 SIP 配置文件。
按照配置 TLS SIP 配置文件或配置 IPv6 SIP 配置文件，第 105 页中的描述配置 SIP 配置文件。

步骤 3 为负载平衡服务器配置两个 SIP 中继。
请参阅在负载平衡服务器上配置 SIP 中继。

步骤 4 为应用程序服务器配置四个 SIP 中继。
请参阅为应用程序服务器配置 SIP 中继。

步骤 5 通过使用您为负载平衡服务器配置的 SIP 中继来配置一个路由组。
请参阅配置路由组。

步骤 6 通过使用您在上一步配置的路由组来配置一个路由列表。
请参阅配置路由列表。

步骤 7 通过使用上述路由列表来配置 *N* 个路由模式。
N 是指您在管理站点上的音频设置中配置的呼入接入号码的数量。 请参阅配置路由模式。

步骤 8 为应用程序服务器配置两个 SIP 路由模式。
请参阅配置 SIP 路由模式。

接下来的操作

配置 SIP 中继安全配置文件

为负载平衡服务器配置 SIP 中继安全配置文件

开始之前

如果 Cisco WebEx Meetings Server 系统配置了 TLS，您必须导入安全电话会议证书。 有关更多信息，请参阅《*Cisco WebEx Meetings Server* 管理指南》中的“导入安全电话会议证书”一节 (http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html)。

步骤 1 请登录 http://ccm-server/，其中 *ccm-server* 是 Cisco Unified Communications Manager 服务器的标准域名或 IP 地址。

步骤 2 选择 **Cisco Unified CM 管理**。

步骤 3 选择**系统** > **安全** > **SIP 中继安全配置文件**。

步骤 4 选择**添加新项**。

步骤 5 配置以下字段。

- 名称 — 输入标识 SIP 中继安全配置文件的名称。
- 设备安全性模式 — 如果希望 CUCM 使用 UDP/TCP 与 Cisco WebEx Meetings Server 通信，请选择**非安全**。 如果希望 CUCM 使用 TLS 与 Cisco WebEx Meetings Server 通信，请选择**加密**。
- X.509 使用者名称 — 如果希望 CUCM 使用 TLS 与 Cisco WebEx Meetings Server 通信，请输入证书名称。

  注释 如果希望 CUCM 使用 TLS 与 Cisco WebEx Meetings Server 通信，那么其他 Cisco WebEx Meetings Server 系统不能共享同一 SIP 中继安全配置文件，因为每个系统的证书必须不同。 从管理站点获取 Cisco WebEx Meetings Server 证书名称。 有关更多信息，请参阅管理指南中的“管理证书”。
- 传入端口 — 如果希望 CUCM 使用 UDP/TCP 与 Cisco WebEx Meetings Server 通信，请输入 5060。 如果希望 CUCM 使用 TLS 与 Cisco WebEx Meetings Server 通信，请输入 5061。

注释 切勿配置此页面上的任何其他字段；保留缺省设置。

步骤 6 选择**保存**。

为应用程序服务器配置 SIP 中继安全配置文件

开始之前

如果 Cisco WebEx Meetings Server 系统配置了 TLS，您必须导入安全电话会议证书。 有关更多信息，请参阅《*Cisco WebEx Meetings Server* 管理指南》中的“导入安全电话会议证书”一节 (http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html)。

步骤 1 请登录 http://ccm-server/，其中 *ccm-server* 是 Cisco Unified Communications Manager 服务器的标准域名或 IP 地址。

步骤 2 选择 **Cisco Unified CM 管理**。

步骤 3 选择**系统** > **安全** > **SIP 中继安全配置文件**。

步骤 4 选择**添加新项**。

步骤 5 配置以下字段：

- 名称 — 输入标识 SIP 中继安全配置文件的名称。
- 设备安全性模式 — 如果希望 CUCM 使用 UDP/TCP 与 Cisco WebEx Meetings Server 通信，请选择**非安全**。 如果希望 CUCM 使用 TLS 与 Cisco WebEx Meetings Server 通信，请选择**加密**。
- X.509 使用者名称 — 如果希望 CUCM 使用 TLS 与 Cisco WebEx Meetings Server 通信，请输入证书名称。

  注释 如果希望 CUCM 使用 TLS 与 Cisco WebEx Meetings Server 通信，那么其他 Cisco WebEx Meetings Server 系统不能共享同一 SIP 中继安全配置文件，因为每个系统的证书必须不同。 从管理站点获取 Cisco WebEx Meetings Server 证书名称。 有关更多信息，请参阅管理指南中的“管理证书”。
- 传入端口 — 如果希望 CUCM 使用 UDP/TCP 与 Cisco WebEx Meetings Server 通信，请输入 5062。 如果希望 CUCM 使用 TLS 与 Cisco WebEx Meetings Server 通信，请输入 5063。

注释 切勿配置此页面上的任何其他字段；保留缺省设置。

步骤 6 选择**保存**。

配置 SIP 配置文件

配置标准 SIP 配置文件

标准会话初始化协议 (SIP) 配置文件使用缺省设置，不需要其他配置步骤。

配置 TLS SIP 配置文件

步骤 1 请登录 http://ccm-server/，其中 *ccm-server* 是 Cisco Unified Communications Manager 服务器的标准域名或 IP 地址。

步骤 2 选择 **Cisco Unified CM 管理**。

步骤 3 选择**设备** > **设备设置** > **SIP 配置文件**。

步骤 4 选择**添加新项**。

步骤 5 配置以下字段：

- 名称 — 输入 SIP 配置文件的名称。
- 由应用程序重定向 — 选中此复选框。

切勿配置此页面上的任何其他字段；将字段保留为它们的缺省设置。

步骤 6 选择**保存**。

配置 IPv6 SIP 配置文件

步骤 1 请登录 http://ccm-server/，其中 *ccm-server* 是 Cisco Unified Communications Manager 服务器的标准域名或 IP 地址。

步骤 2 选择 **Cisco Unified CM 管理**。

步骤 3 选择**设备** > **设备设置** > **SIP 配置文件**。

步骤 4 选择**添加新项**。

步骤 5 配置以下字段：

- 名称 — 输入 SIP 配置文件的名称。
- 启用 ENAT — 选中此复选框。

切勿配置此页面上的任何其他字段；将字段保留为它们的缺省设置。

步骤 6 选择**保存**。

使用 TLS 进行 CUCM 证书管理

如果希望 Cisco Unified Communications Manager (CUCM) 使用 TLS 与 Cisco WebEx Meetings Server (CWMS) 通信，必须执行以下操作：

- 从管理站点获取 CWMS 证书并将其上传到 CUCM。

注释 如果 CWMS 使用第三方证书，则必须将证书链中的所有证书上传到 CUCM。

- 下载 CUCM 证书，然后将其上传到 CWMS 管理站点。

注释 如果 CUCM 使用第三方证书，则只需将证书链中最后一个证书（根证书中心 (CA) 证书）上传到 CWMS。

如果使用 TLS 将多数据中心（MDC) 系统中的所有数据中心连接到同一 CUCM，则 CWMS 将不能对证书的公用名使用公共站点 URL。 由于 CUCM 10.5 及较旧的版本将具有相同公用名的多个证书视为同一证书，因此必须为每个证书的公用名使用各数据中心的本地站点URL。如果名称相同，在将第二个数据中心证书上传到 CUCM 后，第二个数据中心证书就会替换第一个数据中心证书。

请参阅《管理指南》中的“管理证书”获取更多信息。 请参阅http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html以获取更多详细信息。

上传 Cisco WebEx Meetings Server 证书

步骤 1 下载并导出 Cisco WebEx Meetings Server 证书。

a) 登录 Cisco WebEx Meetings Server 管理站点。
b) 选择**设置** > **安全** > **证书**。
c) 从SSL 证书部分复制证书名称。
d) 选择**更多选项** > **导出 SSL 证书**。

e) 将证书保存到本地硬盘。

步骤 2 请登录 http://ccm-server/，其中 *ccm-server* 是 Cisco Unified Communications Manager 服务器的标准域名或 IP 地址。

步骤 3 选择 **Cisco Unified OS 管理**。

步骤 4 选择**安全** > **证书管理**。

步骤 5 选择**上传证书/证书链**。

步骤 6 在证书名称下拉菜单中选择 **CallManager-trust**。

步骤 7 选择**浏览**按钮，然后选择已保存到本地硬盘的证书。

步骤 8 选择**上传文件**。
系统将显示“成功： 证书已上传”消息。

步骤 9 （可选）如果 Cisco WebEx Meetings Server 使用自签名证书，请重复第 4 步到第 8 步上传中间证书和证书链的根证书中心 (CA) 证书。

步骤 10 选择**关闭**。

接下来的操作

有关证书的更多信息，请参阅“管理证书”一节（在《管理指南》中，可从 http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html 获取。）

安装第三方 CUCM 证书

本过程说明了如何将第三方证书上传到 Cisco WebEx Meetings Server。

开始之前

- 生成证书签名请求 (CSR)，并将其发送给第三方证书中心以申请证书。 请参见生成证书签名请求 (CSR) 2.6 版和更高版本（用于 2.6 版和更高版本）或生成证书签名请求 (CSR) 2.5 版和更低版本，第 110 页（用于 2.5 版和更低版本）获取说明。
- 证书中心将向您发送证书链，可能包含下列内容：

  证书 1（用户） - 中间证书中心颁发给用户实体。

  证书 2（中间） - 根证书中心颁发给中间证书中心。

  证书 3（根 CA） - 根证书中心颁发。

- 在证书链中收到多个证书时，请将三个证书合并到一个文件中，并将用户证书放在首位。

步骤 1 按《*Cisco WebEx Meetings Server* 管理指南》 (http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html) 中的说明，将第三方证书文件导入 Cisco WebEx Meetings Server 中。

步骤 2 请登录 http://ccm-server/，其中 *ccm-server* 是 Cisco Unified Communications Manager 服务器的标准域名或 IP 地址。

步骤 3 选择 **Cisco Unified OS 管理**。

步骤 4 选择**安全** > **证书管理**。

步骤 5 选择**上传证书/证书链**。

步骤 6 在证书名称下拉菜单中选择 **CallManager-trust**。

步骤 7 选择**浏览**按钮，然后选择已保存到本地硬盘的根证书中心 (CA) 证书。
这是验证链中最后一个自签名证书，用于验证 `CallManager.pem` 证书。

注释 可以直接从证书中心获取根 CA 证书，同时创建 `CallManager.pem` 证书。

步骤 8 选择**上传文件**。
等待系统指示“成功： 证书已上传。”

步骤 9 选择**关闭**。

接下来的操作

有关证书的更多信息，请参阅管理证书一节（在《*Cisco WebEx Meetings Server* 管理指南》 (http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html) 中）。

下载 CUCM 证书

仅在 CUCM 使用自签名证书的情况下才需要使用本步骤。 如果 CUCM 使用第三方证书，只需将证书链中最后一个证书（根 CA 证书）上传到 Cisco WebEx Meeting Server。 有关如何获取根 CA 证书的信息，请联系证书中心 (CA)。

有关生成 CUCM 证书，请参阅CUCM 文档获取更多信息。

步骤 1 请登录 http://ccm-server/，其中 *ccm-server* 是 Cisco Unified Communications Manager 服务器的标准域名或 IP 地址。

步骤 2 选择 **Cisco Unified OS 管理**。

步骤 3 选择**安全** > **证书管理**。

步骤 4 在“证书名称”字段中搜索名称为“CallManager”的证书。 选择“.PEM 文件”字段。

步骤 5 选择**下载**以将 CUCM 证书 `CallManager.pem` 保存到本地硬盘。

接下来的操作

有关将 CUCM 证书上传至 Cisco WebEx Meetings Server 的更多信息，请参阅《管理指南》中的“管理证书”。 请参阅 http://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.html。

生成证书签名请求 (CSR) 2.6 版和更高版本

用于在 CWMS 2.5 及更高版本中为 SSL 证书生成证书签名请求 (CSR) 和密钥的哈希方法使用 SHA2 (SHA256)。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 使用此控制板管理此系统中的所有数据中心。

步骤 2 选择**设置** > **安全** > **证书** > **CWMS 系统上的证书**。
在多数据中心系统上，继续使用 **CWMS 系统上的证书或数据中心上的证书** ***N***

步骤 3 选择所需类型 CSR 的**生成 CSR**。
2015 年 11 月 1 日，证书颁发机构（例如 VeriSign、GoDaddy 等）将停止颁发内部域名（例如 domain.local、domain.internal）的证书。 在 CWMS 版本 2.0MR9 之前，您仅可以通过部署中所有组件的使用者备用名称上传单个 SSL 证书，但这要求您购买用于整个解决方案的昂贵的 SAN SSL 证书。 自 CWMS 版本 2.5MR5 起，您可以通过 WebEx 站点 URL SSL 从证书颁发机构购买证书用于 IRP 服务器，并使用自签名 SSL 证书用于内部网络虚拟机。

步骤 4 在**生成 CSR**（**证书签名请求**）页面中将字段填写完整。

选项	描述
公用名	选择**本地站点 URL** 证书、**全球站点 URL** 证书或**通配符**证书。
使用者备用名称 只有在为公用名类型选择了**使用者备用名称**时才会出现此选项。	管理站点和虚拟机名称。 如果选择了通配符公用名，则不需要使用者备用名称。

选项	描述
组织	输入组织名称。
部门	输入部门名称。
县/市	输入城市。
省/自治区	输入省/市/自治区。
国家/地区	选择国家/地区。
密钥大小	选择密钥大小 2048。
哈希算法	选择哈希算法 SHA256。

步骤 5 选择**生成 CSR**。
系统将弹出**下载 CSR** 对话框。

步骤 6 选择**下载**。
您将收到 ZIP 文件，其中包含 CSR 和关联的私钥。 CSR 文件名为 `csr.pem`，私钥文件名为 `csr_private_key.pem`。

步骤 7 使用 VMware 数据恢复或 VMware vSphere 数据保护来备份系统。 请参阅通过使用 VMware vCenter 创建备份。
备份系统将保留私钥以防需要对其进行恢复。

生成证书签名请求 (CSR) 2.5 版和更低版本

用于在 CWMS 2.0 及更低版本中为 SSL 证书生成证书签名请求 (CSR) 和秘钥的哈希方法使用 SHA1。CWMS 2.5 及更高版本使用 SHA2 (SHA256)。

内部和外部应用程序证书和 CSR 两者均具有以下选项：

- 密钥类型：

  RSA

  EC

- 对于 RSA 密钥类型，密钥长度为 2048。
- RSA 哈希算法：

  SHA1

  SHA224

  SHA256

SHA384

SHA512

- EC 证书的密钥大小和哈希算法：

  密钥大小 256：

  SHA256

  SHA384

  SHA512

  密钥大小 384：

  SHA384

  SHA512

  密钥大小 512：

  SHA512

外部和内部证书必须为相同类型。 外部证书具体取决于内部证书。 例如，如果系统具有 RSA 内部证书，那么**生成外部自签名**页面仅有一个密钥类型选项RSA（与外部证书密钥类型相同）。 您无法生成或上传密钥类型与安装的内部密钥类型不同的外部证书。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 使用此控制板管理此系统中的所有数据中心。

步骤 2 选择**设置** > **安全** > **证书** > **CWMS 系统上的证书**。
在多数据中心系统上，继续使用 **CWMS 系统上的证书或数据中心上的证书** ***N***

步骤 3 选择所需类型 CSR 的**生成 CSR**。
2015 年 11 月 1 日，证书颁发机构（例如 VeriSign、GoDaddy 等）将停止颁发内部域名（例如 domain.local、domain.internal）的证书。 在 CWMS 版本 2.0MR9 之前，您仅可以通过部署中所有组件的使用者备用名称上传单个 SSL 证书，但这要求您购买用于整个解决方案的昂贵的 SAN SSL 证书。 自 CWMS 版本 2.5MR5 起，您可以通过 WebEx 站点 URL SSL 从证书颁发机构购买证书用于 IRP 服务器，并使用自签名 SSL 证书用于内部网络虚拟机。

步骤 4 在**生成 CSR**（**证书签名请求**）页面中将字段填写完整。

选项	描述
公用名	选择**本地站点 URL** 证书、**全球站点 URL** 证书或**通配符**证书。
使用者备用名称 只有在为公用名类型选择了**使用者备用名称**时才会出现此选项。	管理站点和虚拟机名称。 如果选择了通配符公用名，则不需要使用者备用名称。

选项	描述
组织	输入组织名称。
部门	输入部门名称。
县/市	输入城市。
省/自治区	输入省/市/自治区。
国家/地区	选择国家/地区。
密钥大小	选择密钥大小 2048。

步骤 5 选择**生成 CSR**。
系统将弹出**下载 CSR** 对话框。

步骤 6 选择**下载**。
您将收到 ZIP 文件，其中包含 CSR 和关联的私钥。 CSR 文件名为 `csr.pem`，私钥文件名为 `csr_private_key.pem`。

步骤 7 使用 VMware 数据恢复或 VMware vSphere 数据保护来备份系统。 请参阅通过使用 VMware vCenter 创建备份。
备份系统将保留私钥以防需要对其进行恢复。

配置 SIP 中继

注释 如果部署具有高可用性 (HA) 和多个负载平衡服务器及应用程序服务器的 2000 用户系统，则 CWMS 解决方案中的每个负载平衡器服务器和应用程序服务器都应该有一个专用的 SIP 中继；不支持在同一个 SIP 中继中设置多个目标 IP 地址。

在负载平衡服务器上配置 SIP 中继

步骤 1 请登录 http://ccm-server/，其中 *ccm-server* 是 Cisco Unified Communications Manager 服务器的标准域名或 IP 地址。

步骤 2 选择 **Cisco Unified CM 管理**。

步骤 3 选择**设备** > **中继**。

步骤 4 选择**添加新项**。

步骤 5 在**中继类型**下拉菜单中选择 **SIP 中继**。

注释 切勿更改此页面上的任何其他字段，让参数保留它们的缺省设置。

如果 **CUCM 与 Cisco WebEx Meeting Server 通信，则需要取消选中需要媒体终止点**复选框（在**中继配置**页面上）。 如果您不使用带 CUCM SIP 音频的 Cisco WebEx Meetings Server，在使用第三方 PBX 基础结构提供电话服务时可以选择**需要媒体终止点**复选框。

步骤 6 选择**下一步**。

步骤 7 配置以下字段：

- 设备名称 — 输入 SIP 中继的名称。
- 设备池 - 从下拉菜单中选择相应的设备池。

  要确定在该设备池已配置了哪个 Cisco Unified Communications Manager 组，请选择**系统** > **设备池菜单**。要验证该组包含哪些 Cisco Unified Communications Manager，请选择**系统** > **Cisco Unified CM 组**。

  注释 记录主服务器和备用服务器的 IP 地址。 在 Cisco WebEx Meetings Server 中配置音频设置时应输入这些 IP 地址。 请参阅《管理指南》中的“首次配置音频设置”以获取更多详细信息。 请参阅 Cisco WebEx Meetings Server 安装和升级指南。
- 目标地址 — 输入负载平衡服务器的 IPv4 地址。 请参阅管理站点“音频”页面上的“SIP 配置”表获取 IP 地址。
- 目标地址 IPv6 — 如果希望在 CUCM 和 Cisco WebEx Meetings Server 之间启用 IPv6，请输入负载平衡服务器的 IPv6 地址。
- 目标端口 — 如果希望 CUCM 使用 UDP/TCP 与 Cisco WebEx Meetings Server 通信，请输入 5060。 如果希望 CUCM 使用 TLS 与 Cisco WebEx Meetings Server 通信，请输入 5061。
- SIP 中继安全配置文件 — 从下拉菜单中选择负载平衡服务器的安全配置文件。
- SIP 配置文件 — 如果希望 CUCM 使用 UDP/TCP 与 Cisco WebEx Meetings Server 通信，请选择**标准 SIP 配置文件**。 如果希望 CUCM 使用 TLS 与 Cisco WebEx Meetings Server 通信，请选择 **TLS SIP 配置文件**。如果希望在 CUCM 和 Cisco WebEx Meetings Server 之间启用 IPv6，请选择 **IPv6 SIP 配置文件**。
- 呼叫搜索空间 — 选择希望 Cisco WebEx Meetings Server 呼叫的呼叫搜索空间，该空间可以呼叫 CUCM 中所配置的电话号码和路由模式。 选择**呼叫路由** > **控制类** > **呼叫搜索空间**。 呼叫搜索空间包含一个有序的路由分区列表，这些路由分区通常会分配到设备或路由模式。 呼叫搜索空间将决定呼叫设备在尝试完成呼叫时所搜索的分区。 有关更多信息，请参阅《*Cisco Unified Communications Manager* 管理指南》中的

“呼叫搜索空间配置”或《*Cisco Unified Communications Manager* 系统指南》中的“分区和呼叫搜索空间”。

- 重新路由呼叫搜索空间和对话外引用呼叫搜索空间—选择一个包含为 SIP 路由模式所配置的路由分区的呼叫搜索空间和对话外引用呼叫搜索空间。 请参阅配置 SIP 路由模式。 如果将其设置为 **< 无 >**，则系统只会将呼叫路由到路由分区设置为 **< 无 >** 的路由模式，因此 SIP 路由模式需要将路由分区设置为 **< 无 >**。要进入 Cisco WebEx Meetings Server 中的会议，则必须设置此配置。 有关更多信息，请参阅《*Cisco Unified Communications Manager* 管理指南》中的“呼叫搜索空间配置”或《*Cisco Unified Communications Manager* 系统指南》中的“分区和呼叫搜索空间”。

注释 切勿更改此页面上的任何其他字段，让参数保留它们的缺省设置。

步骤 8 选择**保存**。

步骤 9 选择**重设**，然后在弹出窗口中选择**重设并重启**。

为应用程序服务器配置 SIP 中继

步骤 1 请登录 http://ccm-server/，其中 *ccm-server* 是 Cisco Unified Communications Manager 服务器的标准域名或 IP 地址。

步骤 2 选择 **Cisco Unified CM 管理**。

步骤 3 选择**设备** > **中继**。

步骤 4 选择**添加新项**。

步骤 5 在**中继类型**下拉菜单中选择 **SIP 中继**。

注释 切勿更改此页面上的任何其他字段；将值保留为它们的缺省设置。

步骤 6 选择**下一步**。

步骤 7 配置以下字段：

- 设备名称 — 输入 SIP 中继的名称。
- 设备池 — 从下拉菜单中选择**缺省**。
- 目标地址 — 输入应用程序服务器的 IPv4 地址。
- 目标地址 IPv6 — 可以选择输入应用程序服务器的 IPv6 地址，以在 CUCM 和 Cisco WebEx Meetings Server 之间启用 IPv6。
- 目标端口 — 如果希望 CUCM 使用 UDP/TCP 与 Cisco WebEx Meetings Server 通信，请输入 5062。 如果希望 CUCM 使用 TLS 与 Cisco WebEx Meetings Server 通信，请输入 5063。
- SIP 中继安全配置文件 — 从下拉菜单中选择应用程序服务器的安全配置文件。

- SIP 配置文件 — 如果希望 CUCM 使用 UDP/TCP 与 Cisco WebEx Meetings Server 通信，请选择**标准 SIP 配置文件**。 如果希望 CUCM 使用 TLS 与 Cisco WebEx Meetings Server 通信，请选择 **TLS SIP 档案**。 如果希望在 CUCM 和 Cisco WebEx Meetings Server 之间启用 IPv6，请选择 **IPv6 SIP 配置文件**。
- 呼叫搜索空间 — 选择希望 Cisco WebEx Meetings Server 能够呼叫的呼叫搜索空间，该空间可以呼叫 CUCM 中所配置的电话号码或路由模式。 选择**呼叫路由** > **控制类** > **呼叫搜索空间**。 呼叫搜索空间包含一个有序的路由分区列表，这些路由分区通常会分配到设备或路由模式。 呼叫搜索空间将决定呼叫设备在尝试完成呼叫时所搜索的分区。 如果将其设置为 **< 无 >**，那么只能呼叫分区设置为 **< 无 >** 的设备或路由模式。 有关更多信息，请参阅《*Cisco Unified Communications Manager* 管理指南》中的呼叫搜索空间配置或《*Cisco Unified Communications Manager* 系统指南》中的分区和呼叫搜索空间。

注释 切勿更改此页面上的任何其他字段；将值保留为它们的缺省设置。

如果 CUCM 与 Cisco WebEx Meeting Server 通信，则取消选中**中继配置**页面上的**需要媒体终止点**复选框。 如果您不使用带 CUCM SIP 音频的 Cisco WebEx Meetings Server，在使用第三方 PBX 基础结构提供电话服务时可以选择**需要媒体终止点**复选框。

步骤 8 选择**保存**。

步骤 9 选择**重设**，然后在弹出窗口中选择**重设并重启**。
您必须重设 SIP 中继才能完成配置。

配置路由组

步骤 1 请登录 http://ccm-server/，其中 *ccm-server* 是 Cisco Unified Communications Manager 服务器的标准域名或 IP 地址。

步骤 2 选择 **Cisco Unified CM 管理**。

步骤 3 选择**呼叫路由** > **路由/智能寻线** > **路由组**。

步骤 4 选择**添加新项**。

步骤 5 配置以下字段

- 路由组名称 — 输入路由组的名称。
- 分发算法。 在下拉菜单中选择**循环**。

  注释 选择**循环**后，可以使 CUCM 从路由组中的第 (N+1) 个成员开始将呼叫分发给空闲或有空的用户，其中第 N 个成员是 CUCM 最近向其分发呼叫的成员。 如果第 N 个成员是路由组中的最后一名成员，CUCM 将从路由组顶部开始分发呼叫。
- 查找要添加到路由组的设备 — 在“可用设备”列表中选择**负载平衡服务器的 SIP 中继**。 然后选择**添加到路由组**。

注释 请勿更改页面上的任何其他字段。 保留它们的缺省设置。

步骤 6 选择**保存**。

接下来的操作

为路由组创建路由列表。 继续转至配置路由列表，第 116 页。

配置路由列表

步骤 1 请登录 http://ccm-server/，其中 *ccm-server* 是 Cisco Unified Communications Manager 服务器的标准域名或 IP 地址。

步骤 2 选择 **Cisco Unified CM 管理**。

步骤 3 选择**呼叫路由** > **路由/智能寻线** > **路由列表**。

步骤 4 选择**添加新项**。

步骤 5 配置以下字段

- 名称 — 输入路由列表的名称。
- Cisco Unified Communications Manager 组 — 在下拉菜单中选择**缺省**。

注释 切勿更改此页面上的任何其他字段；将字段保留为它们的缺省设置。

步骤 6 选择**保存**。

步骤 7 选择**添加路由组**。
此时将显示**路由列表详细信息配置**页面。

步骤 8 从**路由组**下拉菜单中选择之前配置的路由组，然后选择**保存**。
此时将显示**路由列表配置**页面。

步骤 9 选择**保存**。

接下来的操作

为路由列表配置路由模式。 继续转至配置路由模式，第 117 页。

配置路由模式

步骤 1 请登录 http://ccm-server/，其中 *ccm-server* 是 Cisco Unified Communications Manager 服务器的标准域名或 IP 地址。

步骤 2 选择 **Cisco Unified CM 管理**。

步骤 3 选择**呼叫路由** > **路由/智能寻线** > **路由模式**。

步骤 4 选择**添加新项**。

步骤 5 配置以下字段

- **路由模式** - 输入路由模式的名称。

  注释 为每个群拨组添加路由模式。 请记下此名称，因为创建群拨组时必须在管理**设置** > **音频** > **群拨组**页面上输入此名称。

- **路由分区** - 选择可呼叫 Cisco WebEx Meetings Server 的电话或设备能够访问的路由分区。 如果设置为 **< 无 >**，则 CUCM 中的任何设备都可以呼叫 Cisco WebEx Meetings Server。 有关更多信息，请参阅《*Cisco Unified Communications Manager* 管理指南》中的“呼叫搜索空间配置”或《*Cisco Unified Communications Manager* 系统指南》中的“分区和呼叫搜索空间”。
- **网关/路由列表** - 从下拉菜单中选择之前配置的路由列表。

注释 切勿更改此页面上的任何其他字段；将这些字段保留为它们的缺省设置。

步骤 6 选择**保存**。

配置 SIP 路由模式

步骤 1 请登录 http://ccm-server/，其中 *ccm-server* 是 Cisco Unified Communications Manager 服务器的标准域名或 IP 地址。

步骤 2 选择 **Cisco Unified CM 管理**。

步骤 3 选择**呼叫路由** > **SIP 路由模式**。

步骤 4 选择**添加新项**。

步骤 5 配置以下字段

- 路由分区 — 选择一个包括在呼叫搜索空间（该空间在上面的“为应用程序服务器配置 SIP 中继”部分被配置为重新路由呼叫搜索空间）中的路由分区。 如果设置为 **< 无 >**，则为应用程序服务器的 SIP 中继所配置的重新路由呼叫搜索空间必须设置为 **< 无 >**。 有关更多信息，请参阅《*Cisco Unified Communications*

Manager 管理指南》中的“呼叫搜索空间配置”或《*Cisco Unified Communications Manager* 系统指南》中的“分区和呼叫搜索空间”。

- 模式使用 — 选择 **IP 地址路由**。
- IPv4 模式 — 输入应用程序服务器的 IP 地址。 请参阅管理站点“音频”页面上的 SIP 配置表获取 IP 地址。
- SIP 中继 — 从下拉菜单中选择之前为应用程序服务器配置的 SIP 中继。

注释 切勿更改此页面上的任何其他字段；将这些字段保留为它们的缺省设置。

步骤 6 选择**保存**。

CUCM 功能兼容性和支持

CUCM 功能兼容性

Cisco WebEx Meetings Server (CWMS) 支持 Cisco Unified Call Manager (CUCM) 8.6 或 9.0（不带 TLS/SRTP），以及 CUCM 9.1、10.0、10.5、11.0(1a) 或 11.5(1)SU1。

重要事项 有些发行版的 CUCM 不支持采用 RSA 加密并以签名算法 SHA256 签署的证书，在这种情况下，CUCM 和 CWMS 之间的 TLS 连接会失败。

将 CUCM 升级到支持此签名算法的版本，或获取采用 RSA 加密并以 SHA1 签署的第三方证书。根据美国国家标准和技术研究所 (NIST) 的最新建议，SHA1 不应再用于生成数字签名，因为它具有安全漏洞。

下表提供了受支持的 CUCM 版本的功能兼容性。 Cisco WebEx Meetings Server 系统容量不受任何配置选项的影响。

注释 CWMS 不支持任何非公开 CUCM 版本或其他第三方 SIP 代理管理应用程序。

表 *5*: 受支持的 *CUCM* 版本的功能兼容性

功能	前提/备注
呼出 (IPv6)	在安装过程中使用 IPv6 地址配置 CWMS。
呼入 (IPv6)	在安装过程中使用 IPv6 地址配置 CWMS。
TLS/SRTP	配置 CWMS 系统安全证书。

功能	前提/备注
RFC2833	在 CUCM SIP 中继配置过程中选择此选项。
KPML	在 CUCM SIP 中继配置过程中选择此选项。
保持连接 - CWMS 发送	使用 SIP OPTIONS 消息执行。
保持连接 - CWMS 接收	使用 SIP OPTIONS 消息执行。
服务质量	控制包。
TCP	确保缺省端口为： 5060 用于会议负载平衡服务器；5062 用于会议应用程序服务器。
TLS	确保缺省端口为： 5061 用于会议负载平衡服务器；5063 用于会议应用程序服务器。
UDP	确保缺省端口为： 5060 用于会议负载平衡服务器；5062 用于会议应用程序服务器。
自签名证书	不适用
第三方证书	不适用

受支持的电话呼叫功能

注释 作为 BE6K (Business Edition 6000) 产品的一部分，CUCM 9.0 软件受 CWMS 支持。

- 呼叫保持
- 取消呼叫保持
- EP 上显示呼叫者标识
- EP 上显示呼叫姓名
- 呼叫转移（IPv4 到 IPv4）
- 呼叫转移（IPv6 到 IPv4）
- 呼叫转移（IPv4 到 IPv6）
- 呼叫转移（IPv6 到 IPv6）

电话媒体功能

CWMS 同时支持使用 G.711、G.722 和 G.729 编解码器的参加者。 更改编解码器配置不会影响系统性能。 CWMS 上支持的包大小：

- 对于 G.711 音频编解码器为 10ms、20ms 或 30ms

- 对于 G.722 音频编解码器为 20ms
- 对于 G.729 音频编解码器为 10ms、20ms、30ms、40ms、50ms 或 60ms

功能	G0.711	G0.722	G0.729
噪音抑制	是	是	是
舒适噪音	是	否	否
回音消除	否	否	否
丢包补偿	是	是	否
自动获得控制权	是	是	是
服务质量	是	是	是

注释 所有自定义音频提示，包括群拨提示，是：8KHz、16 位、64kbps、单声道、CCITT u-law (G.711)。

音频端点兼容性

可以使用任何基于标准并连接到 Cisco Unified Communications Manager 的音频端点加入 WebEx 会议。 支持的音频端点包括 Cisco IP Phone、Telepresence 端点和各种 PSTN 设备，例如移动电话与座机。 许多音频端点支持音频和视频连接。 但是，系统只支持与 Cisco WebEx Meetings Server 的音频连接。

要允许组织外的用户使用 PSTN 设备加入 WebEx 会议，公司必须部署模拟转网络语音网关，例如 Cisco Integrated Service Router (ISR)。 下面列出的 IP 电话已通过 Cisco WebEx Meetings Server 的测试：

- Cisco 7960
- Cisco 7970
- Cisco 7971
- Cisco 7940
- Cisco 9951
- Cisco 9971
- Cisco 7980 (Tandberg)
- Cisco 7975
- Cisco E20
- Cisco Telepresence (CTS 1100)
- Cisco IP Communicator

- Lifesize 视频电话
- Tandberg 1000
- Tandberg 1700
- Polycom
- Cisco Cius
- C20
- EX 60
- EX 90

其他与 Cisco UC 兼容的端点也应能够正常运作。 有关 Cisco Unified Communications Manager 支持的 Cisco Unified IP Phone 和每种型号可用的设备包列表，请参阅 Cisco Unified IP Phone 功能和 Cisco Unified Communications Manager 设备包兼容性矩阵。

第 6 章

关于应用程序下载

您可以使用管理站点上提供的工具大规模部署 CWMS 应用程序。 可供下载的应用程序包括：

- WebEx Meetings 应用程序 - 安排、出席或主持会议的核心应用程序。

  不支持在虚拟操作系统上运行 WebEx Meetings 应用程序。

  如果用户没有安装 WebEx Meetings 应用程序，那么用户首次加入会议时，WebEx Meetings 应用程序会下载到 PC 中。 这可以配置为随需或以无提示方式完成。 用户可以在会议期间使用 Cisco WebEx Meetings 应用程序然后在会议结束时删除它，也可以安装应用程序以加快今后开始或加入会议的速度。 该操作可能发生故障，原因是用户没有管理员权限。

- WebEx 快捷会议工具 - 提供连接 Microsoft™ Outlook® 等其他应用程序的接口，允许通过这些应用程序进行会议管理。

  更新或升级至某个系统之后，应删除所有旧版本的 WebEx 快捷会议工具并安装最新版本。

- WebEx 网络录制文件播放器 - 播放会议录制文件。 这可能包括会议期间展示的任意资料。

在 CWMS 中，应用程序的 .MSI 安装程序位于**管理** > **设置** > **下载**页面。 有关更多信息，请参阅《CWMS 规划指南》中的“从管理站点下载应用程序”。

我们建议您先向用户计算机脱机推送应用程序，然后再通知这些最终用户已为其创建帐户。 这将确保用户首次登录时可以开始和加入会议，以及播放网络录制文件。

如果用户具有管理员权限，您可以让用户从最终用户**下载**页面下载应用程序并自行安装该应用程序。 无需其他管理员操作。

在用户对 PC 没有管理员权限的锁定环境中，**升级**至 Cisco WebEx Meetings Server 发行版 1.5MR3 或更高版本时，请先向所有用户 PC 推送新版本的 WebEx Meetings 应用程序，然后再开始升级过程。

- 从管理站点下载应用程序， 第 124 页
- 应用程序 ZIP 文件的内容， 第 125 页
- Cisco WebEx 快捷会议工具的大规模部署， 第 127 页
- Meetings 应用程序的大规模部署， 第 134 页

- 网络录制文件播放器的大规模部署，第 138 页
- 执行更新之后重新配置设置，第 142 页

从管理站点下载应用程序

您可以对系统进行配置以使管理员可以将 Cisco WebEx 桌面应用程序推送给用户，或者您可以让用户自己进行下载。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 使用此控制板管理此系统中的所有数据中心。

步骤 2 选择**设置** > **下载**。

步骤 3 选择下载方法：

- 允许用户下载 WebEx 桌面应用程序。
  使用此选项允许具有 PC 管理员权限的用户管理会议应用程序。
- 手动将 WebEx 桌面应用程序推送到用户的桌面。
  使用此选项为没有 PC 管理员权限的用户启用会议。

  如果您选定此选项，窗口将展开，以显示“Cisco WebEx Meetings”、“快捷会议工具”和“网络录制文件播放器”部分。

步骤 4 （可选） 选择**自动更新 WebEx 快捷会议工具**以配置 WebEx 快捷会议工具定期的自动更新。（**缺省值**： 选中。）

步骤 5 如果您选择**手动将 WebEx 桌面应用程序推送到用户的桌面**：

a) 在“WebEx Meetings”部分，选择**下载**，然后将 ZIP 文件保存到系统中。
b) 在“快捷会议工具”部分，选择**下载**，然后将 ZIP 文件保存到系统中。
c) 在“WebEx 网络录制文件播放器”部分，选择**下载**，然后将 ZIP 文件保存到系统中。

步骤 6 选择**保存**以保存下载设置。
如果您允许用户下载 WebEx 桌面应用程序，这尤其重要。

步骤 7 （可选） 如果您选择**手动将 WebEx 桌面应用程序推送到用户的桌面**：

a) 解压缩下载的文件。
b) 打开 ZIP 文件。
   每个 ZIP 文件包含所有支持语言的应用程序安装程序。 有关建议使用的安装程序的信息，请参阅应用程序 ZIP 文件的内容，第 125 页。
c) 选择适合您的平台和语言的安装程序，然后将其提取到本地目录文件夹中。
   ZIP 文件包含适用于 Windows 平台的所有可用语言的 MSI 安装程序。

与 Cisco WebEx Meeting Server 的各个版本对应的快捷会议工具和 WebEx Meetings 应用程序版本可以在Cisco WebEx Meetings 应用程序和快捷会议工具兼容性矩阵，第 187 页中找到。

接下来的操作

按照本章所述部署 MSI 安装程序。

应用程序 ZIP 文件的内容

ZIP 文件包含各语言的安装程序应用程序。

应用程序语言代码

各个 ZIP 文件中的英语版应用程序的安装程序文件不带语言后缀。 其他语言版本应用程序的安装程序文件的文件名包含表明其所含应用程序的语言的缩写。 下表列出了用于各语言的缩写：

缩写	语言
B5	繁体中文
de	德语
es	西班牙语（拉丁美洲）
FR	法语
GB	简体中文
IT	意大利语
JP	JAPANESE
KO	韩文
NL	荷兰语
PT	葡萄牙语
RU	俄语
SP	西班牙语

快捷会议工具 ZIP 文件内容

快捷会议工具 ZIP 文件包含以下文件。 请使用“应用程序语言代码”表中的代码来确定各文件的语言。 注意没有 Mac 版本的快捷会议工具。

- ptools.msi
- ptools_B5.msi

- ptools_DE.msi
- ptools_ES.msi
- ptools_FR.msi
- ptools_GB.msi
- ptools_IT.msi
- ptools_JP.msi
- ptools_KO.msi
- ptools_NL.msi
- ptools_PT.msi
- ptools_RU.msi
- ptools_SP.msi

WebEx Meetings 客户端 ZIP 文件内容

使用 应用程序语言代码， 第 125 页 中的关键字确定每个 ZIP 文件所含应用程序的语言。

V2.7 及更高版本	V2.6 及更低版本
webexmc.msi.msi	onpremmc.msi
webexmc_allinone.msi	onpremmc_B5.msi
webexmc.msi_B5.msi	onpremmc_DE.msi
webexmc.msi_DE.msi	onpremmc_ES.msi
webexmc.msi_ES.msi	onpremmc_FR.msi
webexmc.msi_FR.msi	onpremmc_GB.msi
webexmc.msi_GB.msi	onpremmc_IT.msi
webexmc.msi_IT.msi	onpremmc_JP.msi
webexmc.msi_JP.msi	onpremmc_KO.msi
webexmc.msi_KO.msi	onpremmc_NL.msi
webexmc.msi_NL.msi	onpremmc_PT.msi
webexmc.msi_PT.msi	onpremmc_RU.msi
webexmc.msi_RU.msi	onpremmc_SP.msi

V2.7 及更高版本	V2.6 及更低版本
webexmc.msi_SP.msi	webexmc_onprem.dmg (Mac)
webexmc_onprem.dmg (Mac)	

网络录制文件播放器 ZIP 文件内容

如果您在“下载”页面上选择了**允许用户下载 WebEx 桌面应用程序**，则网络录制文件播放器只能用于下载和大规模部署。 请参阅配置下载设置（在《*Cisco WebEx Meetings Server* 管理指南》中）以获取更多信息。

网络录制文件播放器 ZIP 文件包含以下文件。 请使用“应用程序语言代码”表中的代码来确定各文件的语言。

- nbr2player_onprem.msi
- nbr2player_onprem_B5.msi
- nbr2player_onprem_DE.msi
- nbr2player_onprem_ES.msi
- nbr2player_onprem_FR.msi
- nbr2player_onprem_GB.msi
- nbr2player_onprem_IT.msi
- nbr2player_onprem_JP.msi
- nbr2player_onprem_KO.msi
- nbr2player_onprem_NL.msi
- nbr2player_onprem_PT.msi
- nbr2player_onprem_RU.msi
- nbr2player_onprem_SP.msi
- webexnbrplayer_intel.dmg (Mac)

Cisco WebEx 快捷会议工具的大规模部署

本节介绍使用 `ptools.ms` 软件包安装“Cisco WebEx 快捷会议工具”所涉及的任务。 单个计算机安装和大规模安装可以利用 Microsoft Systems Management Server 2003 (SMS) 来完成。

与 Cisco WebEx Meeting Server 的各个版本对应的快捷会议工具版本可以在Cisco WebEx Meetings 应用程序和快捷会议工具兼容性矩阵，第 187 页中找到。

使用命令行对快捷会议工具执行无提示安装

管理员可以登录用户的计算机，然后用无提示模式安装 WebEx 快捷会议工具。

开始之前

在安装维护发行版或将系统升级到新版本之前，应卸载以前版本的 Cisco WebEx 快捷会议工具。

步骤 1 登录到用户的计算机。

步骤 2 将 MSI 软件包下载到计算机的硬盘上。

步骤 3 打开 Windows 命令提示符。
在 Windows 7 或 Windows Vista 上，必须使用以管理员身份运行来打开命令提示窗口。

步骤 4 运行 MSI 命令□□静默方式安装WebEx 快捷会议工具。

示例：
msiexec.exe /q /i "ptools.msi" SITEURL="https://sample.webex.com" OI=1 MSN=1

参数名称	值	描述
OI	1	启用 Outlook 集成
	0（缺省）	禁用 Outlook 集成
MSN	1	启用与 Microsoft Office Communicator 和 Lync 的即时消息程序集成
MSN	0（缺省）	禁用与 Microsoft Office Communicator 和 Lync 的即时消息程序集成

步骤 5 重启计算机。

使用命令行界面对快捷会议工具执行无提示删除

管理员可以登录用户的计算机，然后用无提示模式卸载快捷会议工具。

步骤 1 登录到用户的计算机。

步骤 2 将 MSI 软件包下载到计算机的硬盘上。

步骤 3 打开 Windows 命令提示符。
在 Windows 7 或 Windows Vista 上，必须使用以管理员身份运行来打开命令提示窗口。

步骤 4 输入以下命令来卸载 MSI 软件包 ptools.msi 的所有组件： msiexec.exe /q /x "ptools.msi"。

使用 SMS 进行 CWMS 应用程序的无提示安装时的限制

如果使用 Microsoft Systems Management Server 2003 (SMS) 执行无提示安装，则会有下列限制：

- SMS 每用户模式不受支持。
- 如果 SMS 管理员希望为 WebEx 快捷会议工具添加功能，那么管理员必须先运行 **REMOVE** 命令，然后运行 **ADDSOURCE** 命令，即使此功能之前从未安装。
- 如果用户在其管理员播发软件包时使用远程桌面登录计算机，那么他必须重启计算机以确保“WebEx 快捷会议工具”正常运行。
- 可以进行大规模部署，但每个用户都必须输入凭证信息。
- 在更新到维护发行版或升级到更新的发行版之前，用户必须卸载 Cisco WebEx 快捷会议工具。更新或升级后，您可以手动向用户推送快捷会议工具，也可以请用户从**下载**页面下载快捷会议工具。
- 如果您使用的是 Lync 集成，则在无提示安装后，用户必须重新启动计算机，才能使所有即时消息程序集成功能正常工作。

使用 SMS 每系统无人参与程序播发 WebEx 快捷会议工具

更新或升级后，您可以使用管理站点手动向用户推送快捷会议工具，也可以让用户从最终用户**下载**页面下载快捷会议工具。

请参阅《*Cisco WebEx Meetings Server* 管理指南》中的“配置下载设置”一节以获取更多信息。

如果您是 Microsoft Systems Management Server 2003 (SMS) 管理员，您可以使用 SMS 每系统无人参与程序播发 Cisco WebEx 快捷会议工具。

步骤 1 通过定义创建包。 请参阅从定义创建程序包 ， 第 134 页以获取更多信息。

步骤 2 在播发之前先更改**每系统无人参与**的程序选项：

a) 打开 SMS 管理员控制台，并选择**站点数据库** > **包** > **Cisco WebEx LLC Cisco WebEx 快捷会议工具 2.82** > **程序**。

b) 右键单击每系统无人参与，然后选择**属性**以打开**每系统无人参与程序属性**对话框。

c) 选择**环境**标签页。

- 对于**程序可以运行**选项，选择**仅当用户登录时**。
- 对于**运行方式**选项，选择**使用管理权限运行**。 （请不要打开**允许用户与此程序交互**）。

d) 选择**常规**标签页。

e) 向命令行选项附加其他参数以指定“Cisco WebEx 快捷会议工具”的某些选项：

- SITEURL=″ http://sample.webex.com″ 指定公司所使用的 WebEx 站点 URL。
- 快捷会议工具标记可指定启用了 WebEx 快捷会议工具的哪个组件。 参数应该大写，且缺省值为 0（已停用）。

  在以下示例中，初始命令行是 msiexec.exe /q ALLUSERS=2 /m MSIZWPBY /i "ptools.msi"。
- 向指令行附加快捷会议工具标记与参数： msiexec.exe /q ALLUSERS=2 /m MSIZWPBY /i "ptools.msi" SITEURL="https://sample.webex.com" OI=1MSN=1。

  注释 有关参数的定义，请参阅使用命令行对快捷会议工具执行无提示安装 ， 第 128 页中的参数表。

步骤 3 播发该程序。

a) 打开 SMS 管理员控制台，并选择**站点数据库** > **包** > **Cisco WebEx LLC Cisco WebEx 快捷会议工具 2.82 英文版** > **程序**。

b) 右键单击**每系统无人参与**。

c) 选择**所有任务** > **分发软件**。

d) 选择**下一步**（在**分发程序向导**中）。

e) 选择 SMS 服务器，然后选择**下一步**。

f) 选择集合，然后选择**下一步**。

g) 在**名称**字段中输入播发名称，然后选择**下一步**。

h) 指定播发是否应用到子集合，然后选择**下一步**。

i) 指定将要播发程序的时间，然后选择**下一步**。

j) 指定是否分配程序，然后选择**下一步**。

k) 选择**完成**（在**完成分发程序向导**页中）。

l) 浏览至 \Site Database\System Status\Advertisement Status 目录并检查播发状态。

如果启用了通知，那么用户将会看到一条消息，该消息显示在播发程序后，已分配的程序将会运行。指定的程序将以无提示方式运行。

使用 SMS 每系统无人参与程序删除快捷会议工具组件

执行以下过程以通过使用 Microsoft Systems Management Server 2003 (SMS) 删除快捷会议工具：

简要步骤

1. 创建一个新程序，并按照使用 SMS 每系统无人参与程序播发 WebEx 快捷会议工具，第 129 页中所述复制“每系统无人参与程序”中的所有选项，然后更新命令行：
2. 将程序引入到域中的指定任务机器集合。请参阅使用 SMS 进行 CWMS 应用程序的无提示安装时的限制，第 129 页以获取更多信息。

详细步骤

步骤 1 创建一个新程序，并按照使用 SMS 每系统无人参与程序播发 WebEx 快捷会议工具，第 129 页中所述复制“每系统无人参与程序”中的所有选项，然后更新命令行：

a) 打开 SMS 管理员控制台，并选择**站点数据库** > **包** > **Cisco WebEx LLC Cisco WebEx 快捷会议工具 2.82** > **程序**。

b) 右键单击空白区域，然后选择**新建** > **程序**。

c) 输入程序名称和缺省指令行。

d) 在**属性**对话框中选择**环境**标签页。

- 对于**程序可以运行**选项，选择**仅当用户登录时**。
- 对于**运行方式**选项，选择**使用管理权限运行**。（请不要打开**允许用户与此程序交互**）。

e) 在**常规**标签页上更新指令行。

f) 将 REMOVE 附加到命令行，并指定需要删除的功能。

示例：
如果要删除 OI，请输入以下命令： msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="OI"
PTIM 值用于 CWMS 与即时消息传递程序的集成。例如：
msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="PTIM"

步骤 2 将程序引入到域中的指定任务机器集合。请参阅使用 SMS 进行 CWMS 应用程序的无提示安装时的限制，第 129 页以获取更多信息。
将在这些机器上以无提示方式更新 Cisco WebEx 快捷会议工具。

使用 SMS 每系统无人参与程序添加快捷会议工具

要将组件添加到快捷会议工具，即使之前没有安装过该组件，您也必须先运行REMOVE，然后再运行 ADDSOURCE。

步骤 1 创建一个名为 `Add-phase1` 的新程序，并复制“每系统无人参与程序”中的所有选项，然后更新命令行：

a) 打开 SMS 管理员控制台，并选择**站点数据库** > **包** > **Cisco WebEx LLC Cisco WebEx 快捷会议工具 2.82** > **程序**。
b) 右键单击空白区域，然后选择**新建** > **程序**。
c) 输入程序名称和缺省指令行。
d) 在属性对话框中选择**环境**标签页。
   - 对于**程序可以运行**选项，选择**仅当用户登录时**。
   - 对于**运行方式**选项，选择**使用管理权限运行**。（请不要打开**允许用户与此程序交互**）。
e) 在**常规**标签页上更新指令行。
f) 将 REMOVE 附加到指令行并指定必须添加的功能。

   示例：
   如果要添加 OI和 PITM（PITM 值用于 WebEx 与即时消息传递程序相集成），那么必须先执行 REMOVE（即使尚未安装过 OI 和 PITM）： msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="OI,PTIM"

步骤 2 将程序引入到域中的指定任务机器集合。 请参阅使用 SMS 进行 CWMS 应用程序的无提示安装时的限制，第 129 页以获取更多信息。

步骤 3 创建名为“Add-phase2”的第二个程序，并复制“每系统无人参与程序”中的所有选项，然后更新命令行：

a) 打开 SMS 管理员控制台，并选择**站点数据库** > **包** > **Cisco WebEx LLC Cisco WebEx 快捷会议工具 2.82** > **程序**。
b) 右键单击空白区域，然后选择**新建** > **程序**。
c) 输入程序名称和缺省指令行。
d) 在属性对话框中选择**环境**标签页。
   - 对于**程序可以运行**选项，选择**仅当用户登录时**。
   - 对于**运行方式**选项，选择**使用管理权限运行**。（请不要打开**允许用户与此程序交互**）。
e) 在属性对话框中选择**高级**标签页。
f) 打开**首先运行其他程序**并选择程序 **Add-phase1**。
g) 在**常规**标签页上更新指令行。
h) 将 ADDSOURCE 附加到命令行，并指定需要添加的功能。

   示例：

如果要添加 OI 和 PITM，请使用该命令示例： msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" ADDSOURCE="OI,PTIM" OI=1 MSN=1

步骤 4 将程序引入到域中的指定任务机器集合。 请参阅使用 SMS 进行 CWMS 应用程序的无提示安装时的限制，第 129 页以获取更多信息。
会在这些机器上以无提示方式更新 Cisco WebEx 快捷会议工具。

使用 SMS 每系统卸载程序卸载快捷会议工具

SMS 管理员可以用 SMS 每系统卸载程序来卸载 Cisco WebEx 快捷会议工具。

步骤 1 使用在从定义创建程序包，第 134 页中创建的 SMS 安装软件包。

步骤 2 播发每系统卸载程序以卸载“Cisco WebEx 快捷会议工具”。
将在这些机器上以无提示方式卸载“Cisco WebEx 快捷会议工具”。

播发程序以更新新版本的 WebEx 快捷会议工具

执行以下步骤来播发该程序，从而更新至Cisco WebEx 快捷会议工具的新版本。

开始之前

在安装维护发行版或系统升级到新版本之前，用户必须卸载在其桌面运行的 Cisco WebEx 快捷会议工具。 升级后，您可以使用管理站点手动向用户推送快捷会议工具，也可以请用户从最终用户**下载**页面下载快捷会议工具。

登录到管理站点，选择**设置** > **下载**，然后禁用以下设置：

- **自动更新“Cisco WebEx 快捷会议工具”**
- **允许用户下载 WebEx 桌面应用程序**

步骤 1 使用 WebEx 快捷会议工具 MSI 包创建新的 SMS 安装包。
请参阅从定义创建程序包，第 134 页以获取更多信息。

步骤 2 在播发之前先更改**每系统无人参与**的程序选项。
请参阅使用 SMS 每系统无人参与程序添加快捷会议工具，第 132 页以获取更多信息。

步骤 3 播发该程序。 请参阅使用 SMS 每系统无人参与程序添加快捷会议工具，第 132 页以获取更多信息。

会删除旧版的 Cisco WebEx 快捷会议工具，然后以无提示方式安装新版的 Cisco WebEx 快捷会议工具。

从定义创建程序包

步骤 1 打开 SMS 管理员控制台，然后选择**站点数据库** > **包**。

步骤 2 右键单击**包**。

步骤 3 选择**新建** > **来自定义的包**。

步骤 4 在**从定义创建包**向导中选择**下一步**。

步骤 5 选择**浏览**以定位，选择 WebEx 快捷会议工具 MSI 软件包，然后选择**下一步**。

步骤 6 选择**始终从源目录获取文件**，然后选择**下一步**。

步骤 7 选择源目录位置，然后选择**下一步**。

步骤 8 选择**完成**。

步骤 9 选择**站点数据库** > **包** > **Cisco WebEx LLC Cisco WebEx 快捷会议工具 2.82 英文版** > **程序**。
共有六个程序可选择。

Meetings 应用程序的大规模部署

本节旨在帮助您的组织了解安装 Cisco WebEx Meetings 应用程序涉及的任务。 本节是涉及各类型的安装的综合指南，包括单台计算机安装和通过 Microsoft Systems Management Server 2003 (SMS) 进行的大规模安装。

注释 “无提示安装”意味着可以在无提示的情况下部署应用程序，但需要最终用户配置。

安装 Cisco WebEx Meetings

开始之前

以下前提条件适用于 Cisco WebEx Meetings 安装程序：

- 安装 Cisco WebEx MSI 软件包需要管理员权限。 MSI 软件包安装到缺省 OS Programs 文件夹下，该文件夹需要管理员权限才能访问。

- Cisco WebEx MSI 软件包是针对 Windows Installer 服务 2.0 或更高版本开发的。 如果本地计算机是用较低版本配置的，将显示错误消息，通知用户需要更高版本的 Windows Installer 服务。执行 MSI 软件包时，系统将向用户提示基本 MSI 界面。

步骤 1 在用户计算机上启动安装程序。
将显示安装向导，其中包含介绍消息。

步骤 2 在接下来的几个对话框上选择**下一步**，直到看到安装对话框。

步骤 3 选择**安装**。

步骤 4 安装完成后选择**完成**。

在本地卸载 Cisco WebEx Meetings

您可以登录用户的计算机，然后从控制面板或本地硬盘上的 WebEx 文件夹卸载 Cisco WebEx Meetings 应用程序。

开始之前

Cisco WebEx Meetings 应用程序安装在用户的计算机上。

步骤 1 登录到用户的计算机。

步骤 2 可使用以下方式之一删除 Cisco WebEx Meetings 应用程序：

- 选择**开始** > **控制面板** > **程序和功能**。 从程序列表选择 **Cisco WebEx Meetings**，然后选择**卸载/更改**。
- 选择**开始** > **计算机** > **系统 (C:)** > **ProgramData 文件夹** > **WebEx 文件夹**。 右键单击 **atcliun.exe**，然后选择**删除**。

注释 如果从 WebEx 文件夹卸载 atcliun.exe，而且 Cisco WebEx Meetings 应用程序的内建版本和云版本都保存在用户的本地硬盘上，则这两个版本都会被删除。但是，当您使用控制面板来卸载该应用程序时，只有该应用程序的内建版本会被卸载。

Cisco WebEx Meetings 应用程序会从用户的计算机中卸载。

使用命令行对会议应用程序执行无提示安装

管理员可以登录用户的计算机，然后用无提示模式安装 WebEx Meetings 应用程序。

步骤 1 登录到用户的计算机。

步骤 2 将 MSI 软件包下载到计算机的硬盘上。

步骤 3 打开 Windows 命令提示符。
在 Windows 7 或 Windows Vista 上，必须使用以管理员身份运行来打开命令提示窗口。

步骤 4 输入 MSI 命令以无提示方式安装 Cisco WebEx Meetings 应用程序。

示例：
输入 msiexec /i onpremmc.msi /qn。

步骤 5 重启计算机。

使用命令行界面对 WebEx Meetings 应用程序执行无提示删除

管理员可以登录用户的计算机，然后用无提示模式卸载 Meetings 应用程序。

步骤 1 登录到用户的计算机。

步骤 2 打开 Windows 命令提示符。
在 Windows 7 或 Windows Vista 上，必须使用以管理员身份运行来打开命令提示窗口。

步骤 3 输入以下命令来卸载 MSI 软件包 onpremmc.msi 的所有组件： msiexec/x onpremmc.msi/qn msiexec/x /qn。

使用 SMS 进行 CWMS 应用程序的无提示安装时的限制

如果使用 Microsoft Systems Management Server 2003 (SMS) 执行无提示安装，则会有下列限制：

- SMS 每用户模式不受支持。
- 如果 SMS 管理员希望为 WebEx 快捷会议工具添加功能，那么管理员必须先运行 **REMOVE** 命令，然后运行 **ADDSOURCE** 命令，即使此功能之前从未安装。
- 如果用户在其管理员播发软件包时使用远程桌面登录计算机，那么他必须重启计算机以确保“WebEx 快捷会议工具”正常运行。
- 可以进行大规模部署，但每个用户都必须输入凭证信息。

- 在更新到维护发行版或升级到更新的发行版之前，用户必须卸载 Cisco WebEx 快捷会议工具。更新或升级后，您可以手动向用户推送快捷会议工具，也可以请用户从**下载**页面下载快捷会议工具。
- 如果您使用的是 Lync 集成，则在无提示安装后，用户必须重新启动计算机，才能使所有即时消息程序集成功能正常工作。

使用 SMS 每系统无人参与程序播发 CWMS

Microsoft Systems Management Server 2003 (SMS) 管理员可以使用每系统无人参与程序播发 Cisco WebEx Meetings 应用程序的可用消息。

开始之前

登录管理站点并将下载设置配置为手动将 WebEx 桌面应用程序推送到用户的计算机。请参阅《Cisco WebEx Meetings Server 管理指南》中的配置下载设置一节以获取更多信息。

步骤 1 通过定义创建包。 请参阅从定义创建程序包，第 134 页以获取更多信息。

步骤 2 在播发之前，请先更改“每系统无人参与”的程序选项：

a) 打开 SMS 管理员控制台，并选择**站点数据库** > **包** > **Cisco WebEx LLC Cisco WebEx Meeting 应用程序英文版** > **程序**。

b) 右键单击**每系统无人参与**选项，然后选择**属性**以打开**每系统无人参与程序属性**对话框。

c) 选择**环境**标签页。

- 对于**程序可以运行**选项，选择**仅当用户登录时**。
- 对于**运行方式**选项，选择**使用管理权限运行**。 请不要选择**允许用户与此程序交互**。

d) 选择**常规**标签页。

e) 向命令行选项附加其他参数以指定 WebEx Meetings 应用程序的某些选项：

示例：
例如，初始命令行为： msiexec /i "onpremmc.msi" /qn

步骤 3 现在您可以播发该程序了。

a) 打开 SMS 管理员控制台，并选择**站点数据库** > **包** > **Cisco WebEx LLC Cisco WebEx Meeting 应用程序英文版** > **程序**。

b) 右键单击**每系统无人参与**。

c) 选择**所有任务** > **分发软件**。

d) 选择**下一步**（在**分发程序向导**中）。

e) 选择 SMS 服务器，然后选择**下一步**。

f) 选择集合，然后选择**下一步**。

g) 在**名称**字段中输入播发名称，然后选择**下一步**。

h) 指定播发是否应用到子集合，然后选择**下一步**。
i) 指定将要播发程序的时间，然后选择**下一步**。
j) 指定是否分配程序，然后选择**下一步**。
k) 选择**完成**（在**完成分发程序向导**页中）。
l) 浏览至 \Site Database\System Status\Advertisement Status 目录并检查播发状态。
如果启用了通知，那么用户将会看到一条消息，该消息显示在播发程序后，已分配的程序将会运行。指定的程序将以无提示方式运行。

使用 SMS 每系统卸载程序卸载 Cisco WebEx Meetings 应用程序

SMS 管理员可以用 SMS 每系统卸载程序来卸载 Cisco WebEx Meetings 应用程序。

步骤 1 使用在从定义创建程序包，第 134 页中创建的 SMS 安装软件包。

步骤 2 播发每系统卸载程序以卸载 Cisco WebEx Meetings 应用程序。
将以无提示方式卸载指定计算机上的 Cisco WebEx Meetings 应用程序。

网络录制文件播放器的大规模部署

本节是涉及各类型的安装的综合指南，包括单台计算机安装和通过 Microsoft Systems Management Server 2003 (SMS) 进行的大规模安装。

注释 大于 4 GB 的网络录制文件播放器文件仅可以从 Web 浏览器中访问时播放。

安装网络录制文件播放器

开始之前

- 验证您在目标设备上具有管理员权限，因为要安装 Cisco WebEx MSI 软件包的缺省操作系统 Programs 文件夹需要该访问权限。

如果启用了通知，那么用户将会看到一条消息，该消息显示在播发程序后，已分配的程序将会运行。指定的程序将以无提示方式运行。

使用 SMS 每系统无人参与程序删除快捷会议工具组件

执行以下过程以通过使用 Microsoft Systems Management Server 2003 (SMS) 删除快捷会议工具：

简要步骤

1. 创建一个新程序，并按照使用 SMS 每系统无人参与程序播发 WebEx 快捷会议工具，第 129 页中所述复制“每系统无人参与程序”中的所有选项，然后更新命令行：
2. 将程序引入到域中的指定任务机器集合。请参阅使用 SMS 进行 CWMS 应用程序的无提示安装时的限制，第 129 页以获取更多信息。

详细步骤

步骤 1 创建一个新程序，并按照使用 SMS 每系统无人参与程序播发 WebEx 快捷会议工具，第 129 页中所述复制“每系统无人参与程序”中的所有选项，然后更新命令行：

a) 打开 SMS 管理员控制台，并选择**站点数据库** > **包** > **Cisco WebEx LLC Cisco WebEx 快捷会议工具 2.82** > **程序**。

b) 右键单击空白区域，然后选择**新建** > **程序**。

c) 输入程序名称和缺省指令行。

d) 在**属性**对话框中选择**环境**标签页。

- 对于**程序可以运行**选项，选择**仅当用户登录时**。
- 对于**运行方式**选项，选择**使用管理权限运行**。（请不要打开**允许用户与此程序交互**）。

e) 在**常规**标签页上更新指令行。

f) 将 REMOVE 附加到命令行，并指定需要删除的功能。

示例：
如果要删除 OI，请输入以下命令： msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="OI"
PTIM 值用于 CWMS 与即时消息传递程序的集成。例如：
msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="PTIM"

步骤 2 将程序引入到域中的指定任务机器集合。请参阅使用 SMS 进行 CWMS 应用程序的无提示安装时的限制，第 129 页以获取更多信息。
将在这些机器上以无提示方式更新 Cisco WebEx 快捷会议工具。

在 Windows 7 或 Windows Vista 上，必须使用以管理员身份运行来打开命令提示窗口。

步骤 4 卸载 MSI 软件包 onpremmc.msi 的所有组件，方法是输入命令 msiexec/i nbr2player_onprem.msi/qn。

使用 Microsoft Systems Management Server 2003 (SMS) 安装 CWMS 应用程序

使用 SMS 进行 CWMS 应用程序的无提示安装时的限制

如果使用 Microsoft Systems Management Server 2003 (SMS) 执行无提示安装，则会有下列限制：

- SMS 每用户模式不受支持。
- 如果 SMS 管理员希望为 WebEx 快捷会议工具添加功能，那么管理员必须先运行 **REMOVE** 命令，然后运行 **ADDSOURCE** 命令，即使此功能之前从未安装。
- 如果用户在其管理员播发软件包时使用远程桌面登录计算机，那么他必须重启计算机以确保“WebEx 快捷会议工具”正常运行。
- 可以进行大规模部署，但每个用户都必须输入凭证信息。
- 在更新到维护发行版或升级到更新的发行版之前，用户必须卸载 Cisco WebEx 快捷会议工具。更新或升级后，您可以手动向用户推送快捷会议工具，也可以请用户从**下载**页面下载快捷会议工具。
- 如果您使用的是 Lync 集成，则在无提示安装后，用户必须重新启动计算机，才能使所有即时消息程序集成功能正常工作。

使用 SMS 每系统无人参与程序播发 Cisco WebEx 网络录制文件播放器

如果您是 SMS 管理员，请遵循以下步骤，使用 SMS 每系统无人参与程序来播发 Cisco WebEx 网络录制文件播放器。

开始之前

登录管理站点并将下载设置配置为手动将 WebEx 桌面应用程序推送到用户的桌面。 请参阅《Cisco WebEx Meetings Server 管理指南》中的“配置下载设置”一节以获取更多信息。

简要步骤

1. 通过定义创建包。 请参阅从定义创建程序包，第 134 页以获取更多信息。
2. 在播发之前，请先更改“每系统无人参与”的程序选项：
3. 现在您可以播发该程序了。

详细步骤

步骤 1 通过定义创建包。 请参阅从定义创建程序包，第 134 页以获取更多信息。

步骤 2 在播发之前，请先更改“每系统无人参与”的程序选项：

a) 打开 SMS 管理员控制台，并选择**站点数据库** > **包** > **Cisco WebEx LLC Cisco WebEx 网络录制文件播放器英文版** > **程序**。

b) 右键单击**每系统无人参与**选项，然后选择**属性**以打开**每系统无人参与程序属性**对话框。

c) 选择**环境**标签页。

- 对于**程序可以运行**选项，选择**仅当用户登录时**。
- 对于**运行方式**选项，选择**使用管理权限运行**。 请不要选择**允许用户与此程序交互**。

d) 选择**常规**标签页。

e) 向命令行选项附加其他参数以指定 WebEx Meetings 应用程序的某些选项：

示例：
例如，初始命令行为： msiexec /i "nbr2player_onprem.msi" /qn

步骤 3 现在您可以播发该程序了。

a) 打开 SMS 管理员控制台，并选择**站点数据库** > **包** > **Cisco WebEx LLC Cisco WebEx 网络录制文件播放器英文版** > **程序**。

b) 右键单击**每系统无人参与**。

c) 选择**所有任务** > **分发软件**。

d) 选择**下一步**（在**分发程序向导**中）。

e) 选择 SMS 服务器，然后选择**下一步**。

f) 选择集合，然后选择**下一步**。

g) 在**名称**字段中输入播发名称，然后选择**下一步**。

h) 指定播发是否应用到子集合，然后选择**下一步**。

i) 指定将要播发程序的时间，然后选择**下一步**。

j) 指定是否分配程序，然后选择**下一步**。

k) 选择**完成**（在**完成分发程序向导**页中）。

l) 浏览至 \Site Database\System Status\Advertisement Status 目录并检查播发状态。
如果启用了通知，那么用户将会看到一条消息，该消息显示在播发程序后，已分配的程序将会运行。 指定的程序将以无提示方式运行。

使用 SMS 每系统卸载程序卸载 Cisco WebEx 网络录制文件播放器

SMS 管理员可以通过执行以下步骤用 SMS 每系统卸载程序来卸载 Cisco WebEx 网络录制文件播放器。

简要步骤

1. 使用在从定义创建程序包， 第 134 页中创建的 SMS 安装软件包。
2. 播发每系统卸载程序以卸载 Cisco WebEx 网络录制文件播放器。

详细步骤

步骤 1 使用在从定义创建程序包， 第 134 页中创建的 SMS 安装软件包。

步骤 2 播发每系统卸载程序以卸载 Cisco WebEx 网络录制文件播放器。
将以无提示方式卸载指定计算机上的 Cisco WebEx 网络录制文件播放器。

执行更新之后重新配置设置

对 Cisco WebEx Meetings Server (CWMS) 软件执行更新之后，您必须更新大规模部署的应用程序的路径。（更新后，网络录制文件播放器将在首次用于播放录制文件时自动更新。）

对于 Mac 系统，该路径为 `/Users/(Local User)/Library/Application Support/WebEx Folder/`。

对于 Windows 系统，路径与版本、下载类型和 Web 浏览器类型有关：

- Windows 7 和 Windows Vista： <SystemDisk>\ProgramData\WebEx
- 从快捷会议工具或 WebEx 连接中，使用快捷会议工具或 WebEx 连接路径。
- 如果您使用的是 MSI 安装，则务必使用唯一的路径。 系统将忽略现有的文件。
- 如果您在 Windows 7 下使用下载类型，则系统将使用唯一的路径。 在 Windows XP 中，如果 GPC 可以找到已注册的表值，则系统将使用现有的文件夹。 否则，系统将如上所述使用其自身的路径。

Windows 和 Mac 系统上的客户端应用程序自动更新以保持与更新系统之间的兼容性。

在已锁定的环境中，必须对 Windows 系统手动执行更新，但是对 MAC 系统则不必这样做。

注释 有关与 Cisco WebEx Meeting Server 版本一致的快捷会议工具和 Meetings 应用程序的版本，请参阅Cisco WebEx Meetings 应用程序和快捷会议工具兼容性矩阵， 第 187 页。

第 7 章

单点登录概述

联合单点登录 (SSO) 标准（例如 SAML 2.0）提供了安全机制，有利于在拥有各自授权的不同网站和验证系统间传递凭证和其他相关信息。 SAML 2.0 是由 OASIS 安全服务技术委员会制定的开放标准。

SAML 2.0 协议已取得了重大成功，在金融服务、高等教育、政府及其他行业部门发展势头良好。所有主要的 Web 访问管理供应商均已实施 SAML 2.0 支持。 美国政府服务管理局 (GSA) 要求所有参与美国电子验证身份联盟计划的供应商都必须符合 SAML 2.0。

符合 SAML 2.0 的网站使用 SAML 断言交换用户凭证信息。 SAML 断言是一个 XML 文档，包含关于某主题（例如用户名和权限）的受信任声明。 SAML 声明通过数字签发来确保其真实性。

许多大型企业均已在其公司内部网上部署了联合身份认证和访问管理 (IAM) 和身份提供程序 (IdP) 系统，如 Ping Identity Ping Federate、CA SiteMinder、Open AM 和 Windows ADFS 2.0。 这些 IAM 和 IdP 系统会为员工和合作伙伴处理用户验证和 SSO 要求。 IAM 和 IdP 系统使用 SAML 协议与防火墙外的合作伙伴网站进行交互操作。 用户可以利用 IAM 和 IdP 系统自动验证使用 Cisco WebEx 会议服务的用户。 这样可提高效率，因为用户不必记住用户名与密码就可以在 Cisco WebEx 站点上开始或加入会议。

注释

WebEx Meetings Server 仅支持 SAML 2.0 IdP。 它不支持基于旧版 SAML 1.1 和 WS-Federate 标准的 IdP。 这一限制与继续支持 SAML 1.1 和 WS-Federate 的云模式 Cisco WebEx Meeting 服务形成了鲜明对比。 以下是经过验证可与 Cisco WebEx Meetings Server 配合使用的 SAML 2.0 IdP 列表：

- Microsoft ADFS 2.0（Microsoft Windows Server 2008/Windows Server 2008 R2 或 Windows Server 2012 中 AD FS 服务器角色的免费加载项）
- Microsoft ADFS 3.0（Windows Server 2012 中的 AD FS 服务器角色）
- Ping Identity Ping Federate 6.6.0.17
- Forgerock Open AM 10.0.0
- CA SiteMinder 6.0 SP5

因为 SAML 2.0 是开放的标准，所以其他 SAML 2.0 IdP 也可与 Cisco WebEx Meetings Server 配合使用。 但是，其他 SAML 2.0 IdP 未经过 Cisco 测试。 因此，管理员要对进行任何此类集成自行负责。

- 单点登录的好处， 第 144 页
- 设置 SAML 2.0 单点登录概述， 第 145 页
- 用于最终用户和管理登录的 SAML SSO， 第 146 页
- 云模式 WebEx 会议服务和 WebEx Meetings Server 在 SAML 2.0 单点登录方面的不同， 第 146 页
- SAML 声明属性， 第 149 页

单点登录的好处

单点登录 (SSO) 可以通过以下方式使您受益：

- 简化用户验证 — 即装即用的 Cisco WebEx Meetings Server 要求用户使用电子邮件地址和特定于 Meetings Server 系统的密码登录。 尽管此方法适用于某些中小型组织，大型组织还是希望使用公司凭证（即 Active Directory）进行用户验证以增强安全性。 您可以使用 SAML 2.0 SSO 达成此目标。

  注释 安全的验证 — 系统始终不会在用户验证之后发送 SSO 密码或将其存储在 Cisco WebEx Meetings Server 中。

- 简化用户管理 — 员工队伍因正常人员缩减而不断变化的大型组织希望在与 WebEx Meetings Server 集成时，能够实现用户管理过程的自动化。 这意味着要使以下操作自动化：
  - 员工加入组织时创建用户帐户

- 员工在组织内的职务发生变化时更新用户帐户
- 员工离开组织时停用用户帐户

可通过在 Cisco WebEx Meetings Server 管理站点的 SSO 章节中配置**自动创建帐户**和**自动更新帐户**实现这些活动的自动化。 如果 SAML IdP 也支持这些功能，我们建议您打开这些功能。 用户帐户会在用户验证后自动创建并“按需”更新，因而无需手动创建用户帐户。 同样，用户在离开组织后将无法再登录帐户，因为 SAML 2.0 IdP 会在将这些用户从数据库（通常是底层企业目录的代理）中删除后阻止他们进行登录。

设置 SAML 2.0 单点登录概述

重要事项 除非您或您所在组织内的人员拥有 SAML 2.0 单点登录 (SSO) 的经验，否则我们建议您向合格的 Cisco AUC 合作伙伴或 Cisco 高级服务求助。 鉴于 SAML SSO 配置可能很复杂，我们才提出此建议。

注意 如果 SAML 响应的某个字段中有回车符，则更新、帐户创建及验证都将失败。 尽管 SAML 提供程序会计算带有回车符的数字签名，但 Cisco WebEx Meetings Server 却要删除回车符，从而导致数字签名无效。

查看以下用于设置 SAML 2.0 SSO 的常规步骤：

1. 确保 SAML 2.0 SSO 基础结构就绪并与企业目录集成。 这包括设置 SAML 2.0 IdP 软件和 SSO 验证网站。 验证网站是一个供用户输入公司凭证的门户。
2. 确保用户可以访问 SSO 验证网站。 此步骤很重要，因为在登录过程中，Cisco WebEx Meetings Server 会将用户重定向到此验证网站。

注释 如果 Cisco WebEx Meetings Server 系统已启用公开访问，允许用户从互联网登录并加入会议，则务必确保 SSO 验证网站也可从互联网进行访问。 这通常意味着要在 DMZ 中部署 SAML 2.0 IdP。 否则，用户将在从互联网登录 Cisco WebEx Meetings Server 时看到“404 找不到站点”错误。

3. 使用以下两种方式将 WebEx Meetings Server 连接至 SAML 2.0 IdP：
   - 选择 Cisco WebEx Meetings Server 管理站点上的**设置** > **安全** > **联合 SSO**，并设置 IdP 参数。（请参见《Cisco WebEx Meetings Server 管理指南》中的配置联合单点登录 *(SSO)* 设置部分。）
   - 按 SAML 2.0 IdP 文档中的说明进行操作。 请注意，对应不同供应商的说明也是不同的。 我们建议您联系合格的 Cisco AUC 合作伙伴或 Cisco 高级服务来帮助您实施解决方案。

注释 不要使用在 Cisco Developer Network 上的说明来设置 SAML 2.0 IdP。 那些说明是用于云模式 Cisco WebEx 会议服务的，因此不适用于 Cisco WebEx Meetings Server。

用于最终用户和管理登录的 SAML SSO

通常配置 SAML SSO 只是用于登录最终用户站点，而非管理站点。 在集成 SAML 2.0 SSO 的 Cisco WebEx Meetings Server 站点上，关于用户验证的行为与 SaaS WebEx 行为相同。 Cisco WebEx Meetings Server 管理员（和 SaaS WebEx 管理员）可以使用 SAML SSO 登录最终用户帐户，但必须使用另外设置的密码登录同一系统上的管理员帐户。 这确保了在 SAML SSO iDP 上发生灾难性故障时，管理员仍能访问管理站点。 如果没有这一故障保护措施，您可能遇到这样的情况：管理站点不是由于产品故障，而是由于 SAML SSO IdP 软件的问题无法访问。 SAML SSO IdP 软件在 Cisco WebEx Meetings Server（或 SaaS WebEx）之外的服务器上，因此我们无法控制。

云模式 WebEx 会议服务和 WebEx Meetings Server 在 SAML 2.0 单点登录方面的不同

云模式 Cisco WebEx 会议服务在创建用户帐户时采用唯一用户标识，而 Cisco WebEx Meetings Server 基于电子邮件地址创建用户帐户。 部署 SAML 2.0 单点登录 (SSO) 时，注意：启用自动帐户创建功能后，云模式 Cisco WebEx 会议服务允许删除用户主要名称 (UPN) 中的电子邮件域（例如“@cisco.com”）。 这将导致创建类似于用户标识的用户帐户。 因为 Cisco WebEx Meetings Server 需要完整电子邮件地址来创建用户帐户，所以您无法删除 UPN 中的电子邮件域。

身份提供程序 (IdP) 服务器可以使用任何唯一的 Active Directory (AD) 字段作为用于 SSO 配置的 NameID。 如果您使用 SSO 并且更改某个活动用户的电子邮件地址，应在 IdP 服务器上更改 NameID 字段的映射。

云模式 Cisco WebEx 会议服务在创建用户帐户时采用唯一用户标识，而 Cisco WebEx Meetings Server 基于电子邮件地址创建用户帐户。 这在部署 SAML 2.0 单点登录 (SSO) 时有以下重要影响：

- SAML 断言的 NameID 字段中必须带有电子邮件地址。 如果没有此参数，用户验证和帐户创建将失败，因为 Cisco WebEx Meetings 不允许创建没有关联电子邮件地址的用户帐户。
- 打开自动创建帐户后，云模式 Cisco WebEx Meeting 服务允许删除用户主要名称 (UPN) 中的电子邮件域（例如“@cisco.com”）。 这将导致创建类似于用户标识的用户帐户。 因为 Cisco WebEx Meetings Server 需要完整电子邮件地址来创建用户帐户，所以您无法删除 UPN 中的电子邮件域。

您可以部署 Cisco WebEx Meetings Server 而不使用 SAML 2.0 SSO，部署后再打开 SSO。 这样做将对用户验证、自动创建帐户和自动更新帐户功能产生以下重要影响：

情景	用户验证行为	自动创建帐户 (AAC) 打开	AAC 关闭	自动更新帐户 (AAU) 打开	AAU 关闭
SSO 未打开。已在 CWMS 系统中创建用户帐户。	用户使用电子邮件地址和唯一密码进行登录。	不适用	不适用	不适用	不适用
打开 SSO。拥有现有帐户的用户在移动设备上登录 WebEx 站点、WebEx 快捷会议工具或 Cisco WebEx Meetings 应用程序。	用户将被重定向至 SAML 2.0 IdP 验证网站并使用其公司凭证而不是唯一密码进行登录。 如果他们不是有效用户，SAML 2.0 IdP 会通知他们无法使用 Cisco WebEx 或他们是无效用户。	不适用	不适用	不适用	不适用
SSO 已打开。 用户在系统中没有现有帐户。	同前一场景。	Cisco WebEx Meetings 的用户帐户在用户登录后“按需”创建。 前提条件：SAML 断言的 NameID 字段中包含有效电子邮件地址。	在系统中没有帐户的用户可以登录，但不能访问 Cisco WebEx。要补救此情况： • 保持 AAC 开启。 • 手动创建用户帐户。	不适用	不适用
SSO 已打开。先前使用 SSO 登录的用户再次登录。	与“打开 SSO”情境相同。	不适用	不适用	只要 NameID 保持不变，现有用户帐户就会根据用户凭证的任何更改自动更新。	不适用

情景	用户验证行为	自动创建帐户 (AAC) 打开	AAC 关闭	自动更新帐户 (AAU) 打开	AAU 关闭
您关闭了 SSO。（这是不常见的情境。） 先前使用 SSO 登录的用户现在再次登录。	如果用户输入公司凭证，他们将无法登录，因为 Cisco WebEx 希望他们输入电子邮件地址和唯一密码。 在这种情况下，应指导用户重设 Cisco WebEx 帐户中的唯一密码并在您关闭 SSO 之前给他们足够的时间进行操作。 重设密码后，用户可以使用电子邮件地址和唯一密码进行登录。	不适用	不适用	不适用	不适用

情景	用户验证行为	自动创建帐户 (AAC) 打开	AAC 关闭	自动更新帐户 (AAU) 打开	AAU 关闭
特殊情况：用户是系统管理员。 场景 A：用户登录至 WebEx 站点。 场景 B：用户登录至 Cisco WebEx 管理站点。	场景 A：结果同前一场景。 场景 B：当用户登录至 Cisco WebEx 管理站点时，系统始终会提示该用户输入电子邮件地址和唯一密码；SSO 在用户登录 Cisco WebEx 管理站点时不起作用。 这是产品内置的安全措施。它确保了系统管理员始终可以登录到 Cisco WebEx 管理站点。 如果 Cisco WebEx 管理站点支持 SSO，那么 SAML 2.0 IdP 中的故障或在 Cisco WebEx Meetings Server 和 SAML 2.0 IdP 之间失去网络连接可能导致系统管理员无法登录和管理该产品。	场景 A：结果同前一场景。 场景 B：不适用。	场景 A：结果同前一场景。 场景 B：不适用。	场景 A：结果同前一场景。 场景 B：不适用。	场景 A：结果同前一场景。 场景 B：不适用。

SAML 声明属性

下列表列出 Cisco WebEx Meetings Server 支持的 SAML 声明属性。 确保配置姓、名、电子邮件和 updatetimestamp 属性。 自动更新不会工作，除非已配置 updatetimestamp 属性。

支持的 SAML 声明属性

属性名称	属性含义	对于自动创建用户是必需的	输入值范围	意见、评论
lastName		是		
firstname		是		
email		是	有效的电子邮件格式	始终为必填项，即使在 SSO 配置中禁用了自动帐户创建和更新也不例外。
updatetimestamp	用户信息更新时间	否	支持格式 **长格式：** 示例：System.currentTimeMillis() **LDIF 格式：** yyyyMMddHHmmss 年 □ 月 □ 日 时：分：秒 示例：20090115213256 **UTC 格式** ("2009-10-09T06:00:32Z")	如果缺少 updateTimeStamp，则无法执行自动更新用户；如果 IdP 链接到 AD，它通常映射到 whenChanged 项。
optionalparams		否		请参阅可选参数，第 153 页。
OPhoneCountry		否		办公电话国家/地区代码
OPhoneArea		否		办公室电话区号
OPhoneLocal		否	仅输入数字字符。例如，5551212。切勿输入非数字字符，例如破折号或括号。	办公室电话本地号

属性名称	属性含义	对于自动创建用户是必需的	输入值范围	意见、评论
OPhoneExt		否		办公室电话分机号
FPhoneCountry		否		备用电话国家/地区代码
FPhoneArea		否		备用电话区号
FPhoneLocal		否		备用电话本地号
FPhoneExt		否		备用电话分机号
PPhoneCountry		否		备用电话 2 国家/地区代码
PPhoneArea		否		备用电话 2 区号
PPhoneLocal		否		备用电话 2 本地号
PPhoneExt		否		备用电话 2 分机号
MPhoneCountry		否		移动电话国家/地区代码
MPhoneArea		否		移动电话区号
MPhoneLocal		否		移动电话本地号
MPhoneExt		否		移动电话分机号
时区		否		请参阅时区值，第 153 页。
地址1		否		地址1
Address2		否		Address2
县/市		否		县/市
状态		否		状态
邮政编码		否		邮政编码
国家/地区		否		请参阅国家/地区代码值，第 157 页。

属性名称	属性含义	对于自动创建用户是必需的	输入值范围	意见、评论
地区		否		请参阅地区值，第 166 页。
语言		否		请参阅语言值，第 168 页。
TC1	字符串	否	由用户在管理站点输入的跟踪代码组 1	索引 1
TC2	字符串	否	由用户在管理站点输入的跟踪代码组 2	索引 2
TC3	字符串	否	由用户在管理站点输入的跟踪代码组 3	索引 3
TC4	字符串	否	由用户在管理站点输入的跟踪代码组 4	索引 4
TC5	字符串	否	由用户在管理站点输入的跟踪代码组 5	索引 5
TC6	字符串	否	由用户在管理站点输入的跟踪代码组 6	索引 6
TC7	字符串	否	由用户在管理站点输入的跟踪代码组 7	索引 7
TC8	字符串	否	由用户在管理站点输入的跟踪代码组 8	索引 8
TC9	字符串	否	由用户在管理站点输入的跟踪代码组 9	索引 9

属性名称	属性含义	对于自动创建用户是必需的	输入值范围	意见、评论
TC10	字符串	否	由用户在管理站点输入的跟踪代码组 10	索引 10

可选参数

可以按以下方式设置可选参数：

- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="optionalparams">
- <saml:AttributeValue xsi:type="xs:string">县□市=多伦多</saml:AttributeValue >
- <saml:AttributeValue xsi:type="xs:string">AA=关</saml:AttributeValue >
- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="City">
- <saml:AttributeValue xsi:type="xs:string">多伦多</saml:AttributeValue>
- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="AA">
- <saml:AttributeValue xsi:type="xs:string">关</saml:AttributeValue>

时区值

时区	值
马绍尔群岛（国际日期变更线时间，GMT-12:00）	0
萨摩亚（萨摩亚时间，GMT-11:00）	1
檀香山（夏威夷时间，GMT-10:00）	2
安克雷奇（阿拉斯加夏令时，GMT-08:00）	3
旧金山（太平洋夏令时，GMT-07:00）	4
亚利桑那（山地时间，GMT-07:00）	5
丹佛（山地夏令时，GMT-06:00）	6
芝加哥（中部夏令时，GMT-05:00）	7
墨西哥市（墨西哥夏令时，GMT-05:00）	8

时区	值
萨斯喀彻温（中部时间，GMT-06:00）	9
波哥大（ 南美太平洋时间，GMT-05:00）	10
纽约（东部夏令时，GMT-04:00）	11
印第安纳州（东部夏令时，GMT-04:00）	12
哈利法克斯（大西洋夏令时，GMT-03:00）	13
拉巴斯（ 南美西部时间，GMT-04:00）	14
纽芬兰（纽芬兰夏令时，GMT-02:30）	15
巴西利亚（ 南美东部标准时间，GMT-03:00）	16
布宜诺斯艾利斯（南美东部时间，GMT-03:00）	17
中部大西洋（中部大西洋时间，GMT-02:00）	18
亚速群岛（亚速群岛夏令时，GMT）	19
雷克雅未克（格林威治时间，GMT）	20
伦敦（GMT 夏令时，GMT+01:00）	21
阿姆斯特丹（欧洲夏令时，GMT+02:00）	22
巴黎（欧洲夏令时，GMT+02:00）	23
柏林（欧洲夏令时，GMT+02:00）	25
雅典（希腊夏令时，GMT+03:00）	26
开罗（埃及时间，GMT+02:00）	28
比勒陀利亚（南非时间，GMT+02:00）	29
赫尔辛基（北欧夏令时，GMT+03:00）	30
特拉维夫（以色列夏令时，GMT+03:00）	31
利雅得（沙特阿拉伯时间，GMT+03:00）	32
莫斯科（俄罗斯时间，GMT+04:00）	33

时区	值
内罗毕（内罗毕时间，GMT+03:00）	34
德黑兰（伊朗时间，GMT+04:30）	35
阿布扎比、马斯喀特（阿拉伯时间，GMT+04:00）	36
巴库（巴库夏令时，GMT+05:00）	37
喀布尔（阿富汗时间，GMT+04:30）	38
叶卡特琳堡（西亚时间，GMT+06:00）	39
伊斯兰堡（西亚时间，GMT+05:00）	40
孟买（印度时间，GMT+05:30）	41
科伦坡（科伦坡时间，GMT+05:30）	42
阿拉木图（中亚时间，GMT+06:00）	43
曼谷（曼谷时间，GMT+07:00）	44
北京（中国时间，GMT+08:00）	45
佩思（澳大利亚西部时间，GMT+08:00）	46
新加坡（新加坡时间，GMT+08:00）	47
台北（台北时间，GMT+08:00）	48
东京（日本时间，GMT+09:00）	49
首尔（韩国时间，GMT+09:00）	50
雅库茨克（雅库茨克时间，GMT+10:00）	51
阿德雷德（澳大利亚中部标准时间，GMT+09:30）	52
达尔文（澳大利亚中部时间，GMT+09:30）	53
布里斯班（澳大利亚东部时间，GMT+10:00）	54
悉尼（澳大利亚东部标准时间，GMT+10:00）	55

时区	值
关岛（西太平洋时间，GMT+10:00）	56
霍巴特（塔斯马尼亚岛标准时间，GMT+10:00）	57
符拉迪沃斯托克（符拉迪沃斯托克时间，GMT+11:00）	58
所罗门群岛（中部太平洋时间，GMT+11:00）	59
威灵顿（新西兰标准时间，GMT+12:00）	60
斐济（斐济时间，GMT+12:00）	61
斯德哥尔摩（瑞典夏令时，GMT+02:00）	130
蒂华纳（墨西哥太平洋夏令时，GMT-07:00）	131
奇瓦瓦（墨西哥山地夏令时，GMT-06:00）	132
加拉加斯（ 南美西部时间，GMT-04:30）	133
吉隆坡（马来西亚时间，GMT+08:00）	134
累西腓（ 南美东部时间，GMT-03:00）	135
卡萨布兰卡（摩洛哥夏令时，GMT+01:00）	136
特古西加尔巴城（洪都拉斯时间，GMT-06:00）	137
努克（格陵兰夏令时，GMT-02:00）	138
阿曼（约旦夏令时，GMT+03:00）	139
伊斯坦布尔（东欧夏令时，GMT+03:00）	140
加德满都（尼泊尔时间，GMT+05:45）	141
罗马（欧洲夏令时，GMT+02:00）	142
西非（西非时间，GMT+01:00）	143
马德里（欧洲夏令时，GMT+02:00）	144

国家/地区代码值

国家/地区	代码
阿富汗	93
阿尔巴尼亚	355
阿尔及利亚	213
美属萨摩亚	1684
安道尔共和国	376
安哥拉	244
安圭拉	1264
南极洲	672_1
安提瓜（包括巴布达）	1268
阿根廷	54
亚美尼亚	374
阿鲁巴	297
阿森松岛	247
澳大利亚	61
奥地利	43
阿塞拜疆	994
巴哈马	1242
巴林	973
孟加拉	880
巴巴多斯	1246
白俄罗斯	375

国家/地区	代码
比利时	32
伯利兹	501
贝宁	229
百慕大	1441
不丹	975
玻利维亚	591
波斯尼亚-黑塞哥维那	387
博茨瓦纳	267
巴西	55
大不列颠维琴岛	1284
文莱	673
保加利亚	359
布基纳法索	226
布隆迪	257
柬埔寨	855
喀麦隆	237
加拿大	1_1
佛得角群岛	238
开曼群岛	1_9
中非共和国	236
乍得共和国	235
智利	56
中国	86

国家/地区	代码
哥伦比亚	57
科摩罗	269_1
库克群岛	682
哥斯达黎加	506
克罗地亚	385
古巴	53
塞浦路斯	357
捷克共和国	420
丹麦	45
迪哥加西亚	246
吉布提	253
多米尼加	1767
多米尼加共和国	1809
厄瓜多尔	593
埃及	20
萨尔瓦多	503
赤道几内亚	240
厄立特里亚	291
爱沙尼亚	372
埃塞俄比亚	251
法罗群岛	298
福克兰群岛	500
斐济群岛	679

国家/地区	代码
芬兰	358
法国	33
法属 印度洋诸岛	262
法属圭亚那	594
法属波利尼西亚	689
加蓬共和国	241
冈比亚	220
格鲁吉亚	995
德国	49
加纳	233
直布罗陀	350
希腊	30
格陵兰	299
格林纳达	1473
瓜德罗普	590
关塔那摩（美国海军基地）	53_1
危地马拉	502
几内亚	224
几内亚比绍	245
圭亚那	592
海地	509
洪都拉斯	504
中国香港	852

国家/地区	代码
匈牙利	36
冰岛	354
印度	91
印尼	62
伊朗	98
伊拉克	964
爱尔兰	353
以色列	972
意大利	39_1
象牙海岸	225
牙买加	1876
日本	81
约旦	962
哈萨克斯坦	7_1
肯尼亚	254
基里巴斯	686
朝鲜	850
韩国	82
科威特	965
吉尔吉斯斯坦	996
老挝	856
拉脱维亚	371
黎巴嫩	961

国家/地区	代码
莱索托	266
利比里亚	231
利比亚	218
列支敦士登	423
立陶宛	370
卢森堡	352
中国澳门	853
马其顿	389
马达加斯加	261
马拉维	265
马来西亚	60
马尔代夫	960
马里	223
马耳他	356
马歇尔群岛	692
毛里塔尼亚	222
毛里求斯	230
马约特岛	269
墨西哥	52
密克罗尼西亚	691
摩尔多瓦	373
摩纳哥	377
蒙古	976

国家/地区	代码
蒙特塞拉特	1664
摩洛哥	212
莫桑比克	258
缅甸	95
纳米比亚	264
瑙鲁	674
尼泊尔	977
荷兰	31
荷属安的列斯群岛	599_2
新喀里多尼亚	687
新西兰	64
尼加拉瓜	505
尼日尔	227
纽埃岛	683
诺福克岛	672
北马里亚纳群岛	1670
挪威	47
阿曼	968
巴基斯坦	92
帕劳群岛	680
巴拿马	507
巴布亚新几内亚	675
巴拉圭	595

国家/地区	代码
秘鲁	51
菲律宾	63
波兰	48
葡萄牙	351
波多黎各	1787
卡塔尔	974
罗马尼亚	40
俄罗斯	7
卢旺达	250
圣马利诺	378
圣多美	239
沙特阿拉伯	966
塞内加尔共和国	221
塞尔维亚	381
塞舌尔群岛	248
塞拉利昂	232
新加坡	65
斯洛伐克	421
斯洛文尼亚	386
所罗门群岛	677
索马里	252
南非	27
西班牙	34

国家/地区	代码
斯里兰卡	94
圣赫勒拿	290
圣基茨和尼维斯	1869
圣露西亚	1758
圣皮埃尔和密克隆岛	508
圣文森特	1784
苏丹	249
苏里南	597
斯威士兰	268
瑞典	46
瑞士	41
叙利亚	963
台湾	886
塔吉克斯坦	992
坦桑尼亚	255
泰国	66
多哥	228
汤加群岛	676
特立尼达和多巴哥	1868
突尼斯	216
土耳其	90
土库曼斯坦	993
特克斯和凯科斯	1649

国家/地区	代码
图瓦卢	688
乌干达	256
乌克兰	380
阿拉伯联合酋长国	971
英国	41
美国	1
乌拉圭	598
乌兹别克斯坦	998
瓦努阿图	678
梵蒂冈	39
委内瑞拉	58
越南	84
瓦里司和佛图那群岛	681
西萨摩亚	685
也门	967
赞比亚	260
津巴布韦	263

地区值

地区	值
美国	2
澳大利亚	3
加拿大	4

地区	值
法语区加拿大	5
中国	6
法国	7
德国	8
中国香港	9
意大利	10
日本	11
韩国	12
新西兰	13
西班牙	14
瑞士	15
台湾	16
英国	17
墨西哥	18
阿根廷	19
智利	20
哥伦比亚	21
委内瑞拉	22
巴西	23
葡萄牙	24
比利时	25
荷兰	26
俄罗斯	28

地区	值
印度	29

语言值

语言	值
卡斯特利翁西班牙语	11
荷兰语	14
英语	1
法语	7
德语	9
意大利语	10
JAPANESE	5
韩文	6
西班牙语（拉丁美洲）	12
葡萄牙语	15
俄语	16
简体中文	3
繁体中文	4

语言代码

语言	国家或地区代码
卡斯特利翁西班牙语	34
中文	852, 853, 886

语言	国家或地区代码
荷兰语	31, 32
法语	33, 242, 243
德语	41, 43, 49
意大利语	39
JAPANESE	81
韩文	82
西班牙语（拉丁美洲）	52, 54, 56, 57, 58
国语	86
葡萄牙语	55, 351
俄语	7
美国英语	44, 61, 64, 91
美国英语	1

第 8 章

会议录制文件的存储要求

可配置任意容量的存储服务器。 所保存的 Cisco WebEx 录制文件数取决于配置的存储空间量。

如果用户将录制文件标记为删除，它就立刻不会再显示在用户界面中。 但它会在存储器中保存 3 到 6 个月。 因此，录制文件即使被用户标记为删除，也可以在最多 6 个月时间内复制、备份或使用。（如果用户不小心从 Cisco WebEx Meeting“录制文件”页面删除了录制文件，但该录制文件保存在网络文件系统 (NFS) 存储服务器上，则必须联系 Cisco 技术支持中心 (TAC) 才能恢复录制文件。）

如果系统上的录制文件在 3 个月时间内一直没有占用超过 75% 的已分配空间，则系统会在 6 个月后删除录制文件。 如果录制文件在 3 个月内的任一时刻占用了 75% 以上的已分配空间，则系统会自动删除用户设置为删除的前 10 个文件。

例如，用户在今天将两个文件标记为删除，然后在明天标记了五个文件，后天又标记了九个文件。如果存储空间的使用量超出 75% 的阈值，系统会在三个月后删除前两个文件，过一天再删除接下来的五个文件，再过一天又删除标记为删除的九个文件中的前三个。

如果您的组织要求您将会议录制文件保存六个月以上，请定期将录制文件存档到其他媒体。

下表提供了保存长度为一小时的录制文件大体需要的存储空间量。 使用这些值可以帮您估算出系统保存六个月的会议录制文件所需的存储空间量。

会议内容	保存一小时的会议录制文件大致所需的存储空间
应用程序共享	36 MB
语音	30 MB
180p 视频	104 MB
360p 视频	337 MB

网络摄像头视频将以会议录制时的原始分辨率进行存储。 但是，当播放录制文件时，视频分辨率被限制为 180p 视频。

- 系统备份文件的存储要求，第 172 页

系统备份文件的存储要求

不包括会议录制文件，对系统备份所需的存储空间量的一般建议为至少 900 MB 或能够容纳最多三个系统备份文件的足够空间。 系统会自动删除较旧的备份文件并存储最新的备份。

确定备份所需的存储空间时应考虑的因素：

- 用户数
- 每天举行的平均会议数
- 数据库大小（随时间增加）
- 对于 HA 部署，复制数据期间由于出现网络延迟或高系统负载，事务日志传输可能存在延迟。这可能增加备份文件的大小。

控制板会显示系统备份的大致存储要求。 应使存储服务器上有足够的空间，至少是显示的备份大小的三倍。

第 9 章

支持的 SNMP MIB

Cisco WebEx Meetings Server 支持 SNMP MIB ftp://ftp.cisco.com/pub/mibs/v2/CISCO-WBX-MEETING-MIB.my。 并非所有 MIB 变量都适用于 Cisco WebEx Meetings Server 或适用于所有 Cisco WebEx Meetings Server 部署类型。 比如，与数据中心相关的 MIB 不适用于 Cisco WebEx Meetings Server 系统。

- CWMS 系统信息 MIBS， 第 173 页
- 与 CPU 相关的 MIB， 第 174 页
- CWMS 内存信息， 第 176 页
- 磁盘使用情况， 第 177 页
- 支持的 SNMP 陷阱， 第 177 页

CWMS 系统信息 MIBS

对象[22]	OID	描述
cwCommSystemVersion 类型： 字符串	.1.3.6.1.4.1.9.9.809.1.1.1	Cisco WebEx 系统版本。
cwCommSystemObjectID 类型： 自主	.1.3.6.1.4.1.9.9.809.1.1.2	在 SNMPv2-MIB 中定义的 sysObjectID。

22 此表中所有对象都是只读的 (RO)。

与 CPU 相关的 MIB

对象	读/写权限	OID	描述
cwCommCPUTotalUsage 类型： Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.1	主机组件的CPU使用百分比。 总 CPU 使用率包含CPU用户使用率、CPU 系统使用率和CPU nice 使用率。 CPU 用户时间：用户空间中占用的 CPU 时间。 CPU 系统时间：内核空间中占用的 CPU 时间。 CPU nice 时间： 低优先级进程上占用的CPU时间。
cwCommCPUUsageWindow 类型： Gauge32	RW	.1.3.6.1.4.1.9.9.809.1.2.1.2	发送表明系统超越 CPU 使用率阈值（正常/轻微/严重）并在新阈值水平保持的通知（陷阱）之前的等待持续时间（秒）。
cwCommCPUTotalNumber 类型： Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.3	系统上的 CPU 数。
cwCommCPUUsageTable 类型： 不适用	不可访问	.1.3.6.1.4.1.9.9.809.1.2.1.4	该设备上记录的CPU使用率列表。
cwCommCPUIndex 类型： 无正负号	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.1	唯一的 CPU 标识符。 每个CPU都有自己的使用率值和统计分析值。
cwCommCPUName 类型： 字符串	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.2	CPU 名称。 例如，Intel® Xeon™ CPU 3.00GHz。

对象	读/写权限	OID	描述
cwCommCPUUsage 类型： Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.3	总计使用的CPU资源百分比。 通常使用GHz测量 CPU 功率。 由于 GHz 过大而无法用于测量某些 CPU 使用率类别，因此使用KHz作为测量单位。 系统速度乘以每个CPU部分（例如空闲、NICE、用户）的分数，可得到每个类别的CPU KHz。 此表中使用 KHz 作为所有 CPU 类别的计量单位。
cwCommCPUUsageUser 类型： Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.4	在用户模式下执行的 CPU 功率。
cwCommCPUUsageNice 类型： Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.5	低优先级进程上执行的CPU功率。 Nice是出现在 UNIX 和 Linux 上的程序。 它直接映射到同名的内核调用。 Nice用于调用有特定优先级的实用程序或shell脚本，从而使进程获得多于或少于其他进程的CPU时间。
cwCommCPUUsageSystem 类型： Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.6	在内核模式下执行的 CPU 功率。
cwCommCPUUsageIdle 类型： Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.7	在空闲状态下的CPU功率。
cwCommCPUUsageIOWait 类型： Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.8	在等待磁盘 I/O 完成时使用的 CPU 功率。
cwCommCPUUsageIRQ 类型： Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.9	在处理中断请求时使用的 CPU 功率。
cwCommCPUUsageSoftIRQ 类型： Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.10	在处理软件中断请求时使用的 CPU 功率。

对象	读/写权限	OID	描述
cwCommCPUUsageSteal 类型： Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.11	在虚拟环境中运行时其他任务所使用的CPU功率。
cwCommCPUUsageCapacitySubTotal 类型： Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.12	当前 CPU 总功率。
cwCommCPUMonitoringStatus 类型： 字符串	RO	.1.3.6.1.4.1.9.9.809.1.2.1.5	CPU 资源的监控状态： • 关闭 (0)— 资源不可用。 • 打开 (1)— 资源可用。
cwCommCPUCapacityTotal 类型： Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.6	CPU 总计算能力。

CWMS 内存信息

对象[23]	OID	描述
cwCommMEMUsage 类型： Gauge32	.1.3.6.1.4.1.9.9.809.1.2.2.1	虚拟机的物理内存使用率。
cwCommMEMMonitoringStatus 类型： 字符串	.1.3.6.1.4.1.9.9.809.1.2.2.2	内存资源的监控状态： 关闭 (0)— 资源不可用。 打开 (1)— 资源可用。
cwCommMEMTotal 类型： Gauge32	.1.3.6.1.4.1.9.9.809.1.2.2.3	主机的物理内存总大小 (KB)。
cwCommMEMSwapUsage 类型： Gauge32	.1.3.6.1.4.1.9.9.809.1.2.3.1	主机的物理内存使用率 (%) 和交换内存使用率。

对象[23]	OID	描述
cwCommMEMSwapMonitoringStatus 类型： 字符串	.1.3.6.1.4.1.9.9.809.1.2.3.2	此对象提供内存和交换内存的监控状态。 关闭 (0) — 内存和交换内存状态可用。 打开 (1) — 内存和交换内存状态不可用。

23 此表中所有对象都是只读的 (RO)。

磁盘使用情况

对象[24]	OID	描述
cwCommDiskUsageCount	.1.3.6.1.4.1.9.9.809.1.2.5.1	系统中可用磁盘（例如，本地磁盘、远程磁盘、会议录制磁盘）的数目。
cwCommDiskUsageIndex	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.1	表中条目的索引，其包含通用于磁盘使用率的管理信息。
cwCommDiskPartitionName	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.2	磁盘分区名称。 例如，分区 /opt 或 /dev。
cwCommDiskUsage	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.3	主机上的当前磁盘使用率 (%)。
cwCommDiskTotal	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.4	主机的磁盘空间总大小 (KB)。
cwCommDiskMonitoringStatus	1.3.6.1.4.1.9.9.809.1.2.5.3	磁盘资源的监控状态。 关闭 (0) — 磁盘使用率状态不可用。 打开 (1) — 磁盘使用率状态可用。

24 此表中所有对象都是只读的 (RO)。

支持的 SNMP 陷阱

Cisco WebEx Meetings Server 支持的 SNMP 陷阱。

通知事件

cwCommSystemResourceUsageNormalEvent (.1.3.6.1.4.1.9.9.809.0.1)

系统资源使用率变为非正常状态时的通知。 系统可能在下列情况下发送此通知：

- 一个 CPU 的 `cwCommCPUUsage` 值变为低于预定义的 CPU 轻微阈值。
- `cwCommMEMUsage` 的值变为低于预定义的内存轻微阈值。
- `cwCommMEMSwapUsage` 的值变为低于预定义的交换内存轻微阈值。
- `cwCommFileUsage` 的值变为低于预定义的文件轻微阈值。
- 一个磁盘上的 `cwCommDiskUsage` 的值变为低于预定义的磁盘轻微阈值。

cwCommSystemResourceUsageMinorEvent (.1.3.6.1.4.1.9.9.809.0.2)

系统资源使用率变为非轻微状态时的通知。 轻微通知意味着系统有一些问题并且系统管理员必须解决它们。 系统可能在下列情况下发送此通知：

- 一个 CPU 的 `cwCommCPUUsage` 值变为大于或等于预定义的 CPU 轻微阈值并且低于 cwCommCPUMajorThreshold 的值。
- `cwCommMEMUsage` 值变为大于或等于预定义的内存轻微阈值并且低于预定义的内存严重阈值。
- `cwCommMEMSwapUsage` 值变为大于或等于预定义的交换内存轻微阈值并且低于预定义的交换内存严重阈值。
- `cwCommFileUsage` 值变为大于或等于预定义的文件轻微阈值并且低于预定义的文件严重阈值。
- 一个磁盘的 `cwCommDiskUsage` 值变为大于或等于预定义的磁盘轻微阈值并且低于预定义的磁盘严重阈值。

cwCommSystemResourceUsageMajorEvent (.1.3.6.1.4.1.9.9.809.0.3)

此通知指示某些系统资源使用率变为严重状态。 严重通知意味着系统处于临界状态，要求系统管理员立即采取措施。 系统可能在下列情况下发送此通知：

- 一个 CPU 的 `cwCommCPUUsage` 值变为大于或等于预定义的 CPU 严重阈值。
- `cwCommMEMUsage` 值变为大于或等于预定义的 MEM 严重阈值。
- `cwCommMEMSwapUsage` 值变为大于或等于预定义的 MEM 交换严重阈值。
- `cwCommFileUsage` 值变为大于或等于预定义的文件严重阈值。
- 一个磁盘的 `cwCommDiskUsage` 值变为大于或等于预定义的磁盘严重阈值。

陷阱数据

支持的陷阱数据。 我们建议您将 MIB 过滤器设置为仅接收这些陷阱。

姓名	OID	文本规则	描述
cwCommNotificationHostAddressType	.1.3.6.1.4.1.9.9.809.1.2.4.1	InetAddressType	通过 cwCommNotificationHostAddress 提供的网络地址的类型。
cwCommNotificationHostAddress	.1.3.6.1.4.1.9.9.809.1.2.4.2	InetAddress	随通知一起发送的主机 IP 地址。
cwCommNotificationResName	.1.3.6.1.4.1.9.9.809.1.2.4.3	CiscoWebExCommSysRes	随通知一起发送的系统资源名称。 其指示指定系统资源超过了预定义的警告水平。 0. cwCommTtoalCPUUsage 1. cwCommMemUsage 2. cwCommMemSwapUsage 3. 打开文件描述符（无 MIB 数据） 4. cwCommSocketUsage 5. cwCommDiskTotal 中的一个
cwCommNotificationResValue	.1.3.6.1.4.1.9.9.809.1.2.4.4	Unsigned32	随通知发送的系统资源使用百分比值。
cwCommNotificationSeqNum	.1.3.6.1.4.1.9.9.809.1.2.4.5	Counter32	跟踪通知的顺序的序列号。

第 10 章

常见 PC 系统要求

浏览器和操作系统的 Cisco WebEx Meeting Server (CWMS) 系统常见要求。 管理员 PC 和快捷会议工具用户 PC 的要求相同。

客户端和浏览器要求

- 启用 JavaScript 和 cookie
- 启用 Java 6、Java 7 或 Java 8（适用于支持 Java 的 Web 浏览器）
- 启用 Cisco WebEx 插件（对于 Chrome 32 及更高版本或 Firefox 27 及更高版本）
- 在 Safari 中启用插件
- 对于 Microsoft Internet Explorer 启用 Active X 并且不拦截（推荐）

注释

由于 Google 和 Mozilla 政策的改变，从 Chrome 32 和 Firefox 27 开始，用户在使用这些浏览器时可能需要手动启用 WebEx 插件，[25]才能加入 WebEx 会议或播放 WebEx 录制文件。 有关更多信息和说明，请访问 https://support.webex.com/webex/meetings/en_US/chrome-firefox-join-faq.htm。

如果客户端使用的浏览器并非 Chrome 或 Firefox 的指定版本且启用了 Java，则 Cisco WebEx Meetings 应用程序将在客户端首次开始或加入会议时自动下载到客户端系统上。 我们建议您引导所有客户端安装 Java 版本的最新更新。

TLS 要求

在所有用户计算机上将**互联网设置**配置为使用 TLS 加密。 例如，在运行 Windows 操作系统的 PC 上选择**控制面板** > **Internet 选项** > **高级** > **安全** > **使用 TLS 1.1** 和**使用 TLS 1.2**。 我们建议将这两个选项都选上以获得最大兼容性。 （V2.7 或更高版本不支持**使用 TLS 1.0**。）

如果您的用户要为访客（例如非公司员工）主持会议，必须在这些会议访客加入会议之前通知他们手动更新其操作系统和浏览器以确保与 TLS 设置匹配。 如果会议访客不修改其操作系统，就会遇

[25] 在本文档发布时，尚未最终决定受本策略影响的 Chrome 和 Firefox 的确切版本。

到兼容性问题。 我们建议将这些说明写入会议邀请中。 您可以通过在管理站点上编辑相应的会议邀请来完成此操作，选择**设置** > **电子邮件** > **模板**。

SSL 和 TLS 要求

在所有用户计算机上将**互联网设置**配置为使用 SSL 和 TLS 加密。 例如，在 Windows PC 上：

- 选择**控制面板** > **Internet 选项** > **高级** > **安全** > **使用 SSL 3.0**。 我们建议您选择该选项以获得最大兼容性。
- 选择**控制面板** > **Internet 选项** > **高级** > **安全** > **使用 TLS 1.0** 和**使用 TLS 1.2** 以获得最大兼容性。

如果您的用户要为访客（例如非公司员工）主持会议，必须在这些会议访客加入会议之前通知他们手动更新其操作系统和浏览器以确保与 SSL 或 TLS 设置匹配。 如果不执行这些步骤，就会遇到兼容性问题。 我们建议将这些说明写入会议邀请中。 可以通过在管理站点上编辑相应的会议邀请来完成此操作，选择**设置** > **电子邮件** > **模板**。

- 对于 Windows 的操作系统要求， 第 182 页
- 对于 MAC 的操作系统要求， 第 185 页
- 移动设备的操作系统要求， 第 186 页
- Citrix XenDesktop 和 XenApp 支持， 第 186 页
- Cisco WebEx Meetings 应用程序和快捷会议工具兼容性矩阵， 第 187 页
- 关于主持人许可证， 第 189 页

对于 Windows 的操作系统要求

支持的 Windows 操作系统

- Windows Vista（32 位或 64 位）
- Windows 7（32 位或 64 位）
- Windows 8（32 位或 64 位）
- Windows 8.1（32 位或 64 位）
- Windows 10（32 位或 64 位）（CWMS 2.6MR1 及更高版本）
- Edge（仅限 Windows 10）20.10240.16384.0 - 38.14393.00

注释 在 CWMS V2.7 中增加了对 Microsoft Windows 10 Redstone 1（又称为 Windows 10 Anniversary Update (V1607)）的支持。

Windows 硬件要求

Intel Core2 Duo 或 AMD CPU 2.XX GHz 或更快的处理器。

建议至少使用 2 GB 的 RAM。

支持的 Windows 浏览器

- Internet Explorer： 8 - 11.103.14393.0

  在 Windows 7 SP1 和 Windows 8.1 上测试了 IE 11

- Mozilla Firefox： 10 - 50

  Mozilla Firefox： 在版本 2.5MR4 中测试了 34 - 37

  请通过以下网址了解 FireFox 的发行计划： https://wiki.mozilla.org/RapidRelease/Calendar

- Google Chrome： 23 - 54.0.2840.99

  Google Chrome： 在版本 2.5MR4 中测试了 39 - 42

  请通过以下网址了解 Chrome 的发行计划： http://www.chromium.org/developers/calendar

Microsoft Outlook Integration

- Microsoft Outlook 2007 SP2 和更高版本
- Microsoft Outlook 2010（32 位和 64 位版本；所有 Service Pack）
- Microsoft Outlook 2013
- Microsoft Outlook 2016 (CWMS 2.6MR1)

下表描述了各操作系统对各版本的 Microsoft Outlook 的支持情况。

Microsoft Outlook 版本（客户端/Exchange 服务器）	Vista	Windows 7	Windows 8（仅限桌面模式）	Windows 10
Outlook 2007/ Exchange 2007	Y	Y	N	N
Outlook 2010/ Exchange 2007	Y	Y	Y	Y
Outlook 2010/ Exchange 2010	Y	Y	Y	Y
Outlook 2013/ Exchange 2010	N	Y	Y	Y

Microsoft Outlook 版本（客户端/Exchange 服务器）	Vista	Windows 7	Windows 8（仅限桌面模式）	Windows 10
Outlook 2010/ Exchange 365 Hosted	N	Y	Y	Y
Outlook 2013/ Exchange 2013	N	Y	Y	Y
Outlook 2013/ Exchange 365 Hosted	N	Y	Y	Y
Outlook 2016/ Exchange 365 Hosted	N	Y	Y	Y
Outlook 2010/ Exchange 2016	N	Y	Y	Y - 支持 Windows 7、8、10
Outlook 2013/ Exchange 2016	N	Y	Y	Y - 支持 Windows 7、8、10
Outlook 2016/ Exchange 2016	N	Y	Y	Y - 支持 Windows 7、8、10
Outlook 2016/ Exchange 2010	N	Y	Y	Y - 支持 Windows 7、8、10
Outlook 2016/ Exchange 2013	N	Y	Y	Y - 支持 Windows 7、8、10

受支持的即时消息客户端

即时消息程序版本	Windows XP SP3	Windows 7	Windows 8
Communicator 2007	Y	Y	Y
Communicator 2007 R2	Y	Y	Y
Lync 2010（32 位）	N	Y	Y
Lync 2013（32 位）	N	Y	Y

Windows 版 Cisco Jabber 集成

- Windows 版 Cisco Jabber 9.2.6
- Windows 版 Cisco Jabber 9.6.1
- Windows 版 Cisco Jabber 9.7
- Windows 版 Cisco Jabber 10.5
- Windows 版 Cisco Jabber 11.0
- Windows 版 Cisco Jabber 11.5 (CWMS 2.6MR1)
- Windows 版 Cisco Jabber 11.6
- 支持 Cisco WebEx Meetings Server 与 LDAP/Active Directory 集成。

限制

Windows 版 Jabber 9.2.6 支持与配置了 SAML 2.0 单点登录 (SSO) 的 Cisco WebEx Meetings Server 1.5 及更高版本站点集成。 早期版本的 Windows 版 Jabber 不支持单点登录。

并非所有 Cisco Jabber 版本或平台都支持与 Cisco WebEx Meetings Server 集成。 （例如，云模式 Jabber 和 WebEx Communicator。） 有关与 Cisco WebEx Meetings Server 集成的信息，请参见位于 http://www.cisco.com/en/US/products/ps12511/tsd_products_support_series_home.html 的 Windows 版 Cisco Jabber 文档。

对于 MAC 的操作系统要求

支持的 Mac 操作系统

- Mac OS X 10.7 Lion
- Mac OS X 10.8 Mountain Lion
- Mac OS X 10.9 Mavericks
- OS X 10.11 El Capitan (CWMS 2.6MR1)
- OS X 10.12 Sierra (CWMS 2.7MR2)

Mac 硬件要求

2.0 GHz 或更快的 CPU。

建议至少使用 512 MB 的 RAM。

支持的 Mac 浏览器

- Apple Safari： 6 - 9.1.3
- Google Chrome： 23 - 53.0.2743.116

请通过以下网址了解 Chrome 的发行计划： http://www.chromium.org/developers/calendar

- Mozilla Firefox： 10 - 48.1

Mac 版 Cisco Jabber 集成

配置了 SAML 2.0 单点登录 (SSO) 或 LDAP/Active Directory 的 Cisco WebEx Meetings Server 站点支持以下 Mac 版 Cisco Jabber 集成。

- Cisco Jabber for Mac 11.6 支持与 Cisco WebEx Meetings Server 发行版 2.6 及更高版本集成
- Cisco Jabber for Mac 10.5 支持与 Cisco WebEx Meetings Server 发行版 2.5 及更高版本集成
- Cisco Jabber for Mac 9.6 支持与 Cisco WebEx Meetings Server 发行版 2.0 及更高版本集成

移动设备的操作系统要求

将 Cisco WebEx 应用程序手动下载到 iOS 或 Android 系统且启用 WebEx 移动功能后，用户可使用应用程序来加入或开始会议。 用户也可利用浏览器访问移动设备上的 Cisco WebEx，但可能无法提供最佳用户体验。

Cisco WebEx Meeting Server 2.0 及更高版本支持：

- 使用 iOS 6.0 及更高版本的 Apple iPhone 和 iPad。
- 使用 Android 2.1 及更高版本的 Android 移动设备。
- iPhone 和 Android 版 Jabber 9.6 及更高版本。

注释 不能在移动设备上播放录制文件。 如果是使用 Android 移动设备开始的会议，则可启动和管理会议录制文件。 如果是使用 iOS 移动设备开始的会议，则无法在 iOS 设备上启动或管理会议录制文件。

Citrix XenDesktop 和 XenApp 支持

Cisco Webex Meeting Server 在主机操作系统和虚拟操作系统均为 Windows 7 或 Windows 8 的情况下支持 Citrix XenDesktop 7.6。（主机操作系统是在最终用户的计算机中安装的操作系统。 虚拟操作系统是服务器提供的操作系统。）

已知问题和局限

- 由于虚拟桌面环境的体系结构限制，可能无法流畅地发送视频。 此外，在会议中发送视频时，帧率可能很低，导致用户体验欠佳。
- 一些视频文件无法在虚拟桌面环境中共享。

- 运行 Mac OS 时，系统可能无法识别（外部或集成的）网络摄像头和麦克风并用于会议。
- 不支持 Remote Access 和 Access Anywhere，因为 Remote Access 和 Access Anywhere 代理在操作系统重启后会被底层的 Citrix 平台自动删除。
- 快捷会议工具用户无法从 Outlook 中开始便捷式会议或已安排的会议。

Cisco WebEx Meetings 应用程序和快捷会议工具兼容性矩阵

此表针对 Cisco WebEx Meetings Server 的各个发行版列出了 WebEx Meetings 应用程序和快捷会议工具下载的内部版本号。

Cisco WebEx Meetings Server 发行版	ISO 号码	Cisco WebEx 快捷会议工具	Cisco WebEx Meetings 应用程序
1.5 MR3	1.5.1.323	2.80.501.321	27.32.151.321
1.5 MR4	1.5.1.402/1.5.1.400	2.80.501.401	27.32.151.401
1.5 MR5	1.5.1.503	2.80.501.503	27.32.151.503 (Windows) orion1.5.MR3.FCS.0.0.503 (Mac)
2.0[26]	2.0.1.2	2.82.0.1713	27.32.200.1713
2.0 MR1	2.0.1.107	2.82.0.1713	27.32.200.1713
2.0 MR2	2.0.1.205	2.82.0.1713	27.32.200.1713
2.0 MR3	2.0.1.302	2.82.1.302	27.32.200.302
2.0 MR4	2.0.1.407	2.82.1.407	27.32.200.407 orion2.0.MR4.0.0.407 (MAC OS)
2.0MR5	2.0.1.507	2.82.1.507	27.32.201.507 (Windows) orion2.0.MR5.0.0.507 (Mac)
2.0MR6	2.0.1.611	2.82.1.606	27.32.200.606 (Windows) orion2.0.MR6.0.0.606 (Mac)

Cisco WebEx Meetings Server 发行版	ISO 号码	Cisco WebEx 快捷会议工具	Cisco WebEx Meetings 应用程序
2.0MR7	2.0.1.707	2.82.1.701	27.32.201.701 (Windows) orion2.0.MR7.0.0.701 (Mac)
2.0MR8	2.0.1.809	2.82.1.701	27.32.201.701 (Windows) orion2.0.MR7.0.0.701 (Mac)
2.0MR8 安全补丁 1	2.0.1.839	2.82.1.839	27.32.201.839 (Windows) orion2.0.MR8.0.0.839 (Mac)
2.0MR9	2.0.1.918	2.82.1.910	27.32.201.910 (Windows) orion2.0.MR9.0.0.910 (Mac)
2.5	2.5.1.29	2.82.500.2353	29.9.2.10085（Windows 和 Mac）
2.5MR1	2.5.1.132	2.82.500.3339	29.11.3.4858（Windows 和 Mac）
2.5MR2	2.5.1.227	2.82.501.10002	29.12.0.10076（Windows 和 Mac）
2.5MR3	2.5.1.3009	2.82.501.10008	29.12.0.10076（Windows 和 Mac）
2.5MR4	2.5.1.4378	2.82.502.8	29.13.11.10173（Windows 和 Mac）
2.5MR5	2.5.1.5033	2.82.502.9	29.13.12.10182（Windows 和 Mac）
2.5MR6	2.5.1.6139	2.82.502.11	29.13.41.30001（Windows 和 Mac）
2.6	2.6.1.39	2.82.502.1078	30.1.0.20002（Windows 和 Mac）
2.6MR1	2.6.1.1099	2.82.6501.1082	30.5.2.10002（Windows 和 Mac）

Cisco WebEx Meetings Server 发行版	ISO 号码	Cisco WebEx 快捷会议工具	Cisco WebEx Meetings 应用程序
2.6MR2	2.6.1.2097	2.82.6520.1083	30.6.4.10003（Windows 和 Mac）
2.6MR3	2.6.1.3096	2.82.6520.1090	30.10.1.10008（Windows 和 Mac）
2.7	2.7.1.12	2.82.7000.1150	31.4.0.41（Windows 和 Mac）
2.7MR1	2.7.1.1073	2.82.7000.1159	31.5.20.63（Windows 和 Mac）
2.7MR2	2.7.1.2048 [27]	2.82.7000.1161	31.8.0.167（Windows 和 Mac）
2.8	2.8.1.12（已推迟。 使用版本 2.8.1.17。）	不适用	不适用
2.8	2.8.1.17	2.82.7000.1174	31.11.6.9

[26] 不再可用。

[27] 2.7MR2 软件更新仅适用于当前正在运行 Cisco WebEx Meetings Server 发行版 2.7.1.12 或 2.7.1.1073 或更高版本的系统。

关于主持人许可证

本产品的**许可方式基于主持人**，要求您为每个**主持**会议的用户购买许可证，或者为这些用户手动分配许可证。用户代表他人出席或安排会议时，不会耗用主持人许可证。出于报告目的，每月计算一次许可证使用量，例如，从 1 月 1 日至 31 日计算一次，从 2 月 1 日至 28 日计算一次，以此类推。

注释 从先前版本升级至版本 2.5 或更高版本时，原始系统上的所有许可证会从用户分配中释放出来。用户可以通过主持会议或者手动分配许可证的方式重新获取许可证。 安装多数据中心 (MDC) 系统时，也可以这样做。 加入MDC 系统的数据中心将丢失主持人许可证。 加入之后，可以在MDC 系统上重新托管这些许可证。

可以从**报告**页面请求提供许可证消耗总数的报告。 此外，我们建议您查看显示许可证消耗趋势的 PDF 摘要报告。 通过查看许可证的总体趋势，您可以更有效地计划未来许可证的购买，以适应公司内对此系统日益增加的使用。

第 11 章

Cisco Unified Communications Manager (CUCM) 集成

Cisco WebEx Meetings Server 发行版 2.8 与下列的 Cisco Unified Communications Manager 发行版兼容：

- 11.5(1)SU1
- 11.0(1a)
- 10.5.2
- 10.5
- 10.0
- 9.1
- 9.0

注释 在 CWMS 2.7 及更高版本中删除了对 TLS 1.0 的支持 (CSCuu40706)。 在 CUCM 10.5 及更高版本中引入了对 TLS 1.2 的支持。

- Session Manager Edition (SME) 集成， 第 191 页
- 音频端点兼容性， 第 192 页

Session Manager Edition (SME) 集成

CWMS 支持 Session Manager Edition (SME)。

安排 Unified MP 会议时，Unified MP 用户可以选择 Cisco WebEx 为网络会议提供商。 Cisco WebEx 集成在 Cisco Unified MP 6.0.2 及更高发行版中提供。 语音和视频会议由 Unified MP 提供。 必须向 WebEx 用户提供语音和视频拨入信息以便他们加入会议，他们也可以使用 WebEx 中提供的外拨功能加入会议。

音频端点兼容性

可以使用任何基于标准并连接到 Cisco Unified Communications Manager 的音频端点加入 WebEx 会议。 支持的音频端点包括 Cisco IP Phone、Telepresence 端点和各种 PSTN 设备，例如移动电话与座机。 许多音频端点支持音频和视频连接。 但是，系统只支持与 Cisco WebEx Meetings Server 的音频连接。

要允许组织外的用户使用 PSTN 设备加入 WebEx 会议，公司必须部署模拟转网络语音网关，例如 Cisco Integrated Service Router (ISR)。 下面列出的 IP 电话已通过 Cisco WebEx Meetings Server 的测试：

- Cisco 7960
- Cisco 7970
- Cisco 7971
- Cisco 7940
- Cisco 9951
- Cisco 9971
- Cisco 7980 (Tandberg)
- Cisco 7975
- Cisco E20
- Cisco Telepresence (CTS 1100)
- Cisco IP Communicator
- Lifesize 视频电话
- Tandberg 1000
- Tandberg 1700
- Polycom
- Cisco Cius
- C20
- EX 60
- EX 90

其他与 Cisco UC 兼容的端点也应能够正常运作。 有关 Cisco Unified Communications Manager 支持的 Cisco Unified IP Phone 和每种型号可用的设备包列表，请参阅 Cisco Unified IP Phone 功能和 Cisco Unified Communications Manager 设备包兼容性矩阵。