Guía de planificación y requisitos del sistema de Cisco WebEx Meetings Server, versión 2.6

Primera publicación: 28 de mayo de 2014

Última modificación: 27 de octubre de 2015

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)

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENIDO

Requisitos del sistema WebEx 1

- Requisitos generales del sistema 1
- Herramientas de productividad de WebEx 7
- Usuarios 7
- Tamaños de implementación para el sistema 7
- Requisitos para la corresidencia de vCenter 8
- Máquinas virtuales en el sistema 8
- Requisitos mínimos de hardware 9
  - Recursos consumidos por Cisco WebEx Meetings Server y el host ESXi 11
  - Sistema de 50 usuarios 12
  - Sistema de 250 usuarios 15
  - Sistema de 800 usuarios 18
  - Sistema de 2000 usuarios 21
- Matriz de capacidad del sistema 27
- Actualización de la versión 2.6 y matriz de actualización 31

Introducción y topología del centro de datos para su sistema 33

- Introducción al servidor de Cisco WebEx Meetings 33
- Información para los clientes de Cisco Unified MeetingPlace 35
- Conceptos generales sobre el despliegue del sistema 35
- Despliegue de un solo centro de datos 38
- Unión de centros de datos individuales para crear un sistema con varios centros datos (MDC) 38
- Utilización de VMware vSphere con su sistema 39
  - Ventajas de desplegar su sistema en VMware vSphere 39
- IOPS y rendimiento del sistema de almacenamiento 41
- Instalación de VMware vSphere ESXi y configuración de almacenamiento 43
- Entrada en reuniones 44

Topología de redes para el sistema 47

- Diseño de las máquinas virtuales en su red 48
- Diferentes tipos de topología de red del sistema 48

Topología de red interna de proxy inverso de Internet (IRP) 49
Topología de red de horizonte no dividido 50
Topología de red totalmente interna 51
Topología de red de horizonte dividido 52
Redundancia en despliegues de HA o MDC 54
Consideraciones de red para el proxy inverso de Internet 55
Requisitos de ancho de banda de red 57
Requisitos de la red para varios centros de datos 61
Equipos de NIC para agregación de ancho de banda 62
Equilibrio de la carga 63
Cambios de las comunicaciones de red necesarios para el despliegue 65
Lista de comprobación de comunicaciones de red para el sistema 66
Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático y acceso público 67
Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue manual, acceso público y todas las máquinas virtuales internas 69
Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático, acceso público y un DNS de horizonte no dividido 73
Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue manual, acceso público y un DNS de horizonte no dividido 75
Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático, acceso público y un DNS de horizonte dividido 78
Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue manual, acceso público y un DNS de horizonte dividido 81
Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático y sin acceso público 84
Lista de comprobación de comunicaciones de red para una instalación o expansión con despliegue manual y sin acceso público 86
URL del sitio de WebEx y URL de administración de WebEx 89
Acceso de puerto cuando las máquinas virtuales están en la red interna 90
Acceso de puerto con un proxy inverso de Internet en la red DMZ 91
Puertos de VMware vCenter 97
Puertos de Cisco WebEx Meeting Center 98
Uso de NAT con el sistema 99
Proxies de envío 101

Métodos recomendados 103

Métodos recomendados para Cisco WebEx Meetings Server 103

Configuración de Cisco Unified Communications Manager (CUCM) 105

Configuración de Cisco Unified Communications Manager (CUCM) 105

Lista de comprobación de configuración de CUCM para sistemas con varios centros de datos 107

Lista de comprobación de configuración de CUCM con o sin alta disponibilidad 108

Configuración de CUCM en un sistema con varios centros de datos de CWMS 108

Configuración de CUCM en un sistema de 250 u 800 usuarios con varios centros de datos 109

Configuración de CUCM en un sistema de 2000 usuarios con varios centros de datos 110

Configurar CUCM para sistemas de alta disponibilidad y sistemas que no lo sean 111

Configuración de CUCM en sistemas de 50, 250 y 800 usuarios sin alta disponibilidad 112

Configuración de CUCM en sistemas de 50, 250 u 800 usuarios con alta disponibilidad 113

Configuración de CUCM en sistemas de 2000 usuarios sin alta disponibilidad 114

Configuración de CUCM en sistemas de 2000 usuarios con alta disponibilidad 115

Configurar un perfil de seguridad de troncal SIP 117

Configurar un perfil de seguridad de troncal SIP para un punto de equilibrio de carga 117

Configurar un perfil de seguridad de troncal SIP para un punto de aplicación 118

Configurar un perfil de SIP 118

Configurar un perfil de SIP estándar 118

Configurar un perfil de SIP TLS 119

Configurar un perfil de SIP IPv6 119

Administración de certificados CUCM utilizando TLS 119

Cargar certificados de Cisco WebEx Meetings Server 120

Instalación de un certificado CUCM de terceros 121

Descargar certificados CUCM 122

Configurar un troncal SIP 123

Configurar un troncal SIP en un punto de equilibrio de carga 123

Configurar un troncal SIP para un punto de aplicación 124

Configuración de un grupo de rutas 125

Configuración de una lista de rutas 126

Configuración de un patrón de ruta 127

Configuración de un patrón de ruta SIP 127

Soporte y compatibilidad de la función CUCM 128

Compatibilidad del punto final de audio 132

Aplicaciones de despliegue masivo y descarga 135

Acerca de la descarga de aplicaciones 135
Descarga de aplicaciones desde el sitio de administración 136
Contenido de los archivos ZIP de la aplicación 137
Implementación masiva de las herramientas de productividad de Cisco WebEx 139
Instalación silenciosa de las herramientas de productividad utilizando la línea de comandos 140
Eliminación silenciosa de las herramientas de productividad a través de la interfaz de la línea de comandos 140
Instalación silenciosa con SMS 141
Publicidad de las herramientas de productividad de WebEx mediante el programa SMS por sistema desatendido 141
Eliminación de componentes de herramientas de productividad mediante el programa de SMS por sistema desatendido 143
Añadir componentes de las herramientas de productividad mediante el programa SMS por sistema desatendido 144
Desinstalación de las herramientas de productividad mediante el programa SMS por desinstalación de sistema 145
Publicidad del programa para actualizar la nueva versión de las herramientas de productividad de WebEx 146
Creación de un paquete a partir de la definición 147
Despliegue masivo de la aplicación de reuniones 148
Instalar Cisco WebEx Meetings 148
Desinstalación de Cisco WebEx Meetings localmente 149
Instalación silenciosa de la aplicación de reuniones utilizando la línea de comandos 150
Eliminación silenciosa de la aplicación de reuniones a través de la interfaz de la línea de comandos 150
Instalación silenciosa con SMS 150
Publicidad de la aplicación Cisco WebEx Meetings mediante el programa SMS por sistema desatendido 151
Desinstalación de la aplicación Cisco WebEx Meetings mediante el programa de desinstalación SMS por sistema 152
Despliegue masivo del reproductor de grabación en la red 153
Instalación del reproductor de grabación en la red 153
Instalación silenciosa del Reproductor de grabación utilizando la línea de comandos 154

Desinstalación silenciosa del reproductor de grabación a través de la interfaz de la línea de comandos 154
Instalación silenciosa mediante el programa SMS 155
Publicidad del reproductor de grabación en la red de Cisco WebEx mediante el programa SMS por sistema desatendido 155
Desinstalación del reproductor de grabación en la red de Cisco WebEx mediante el programa de desinstalación SMS por sistema 156
Reconfiguración de los ajustes tras realizar una actualización 157
Configuración del SSO de SAML 159
Descripción general del inicio de sesión único 159
Ventajas de inicio de sesión único 160
Información general de la configuración del inicio de sesión único de SAML 2.0 161
SAML SSO para inicio de sesión en el sitio del usuario final y en el de administración 162
Diferencias de inicio de sesión único SAML 2.0 entre los servicios de reunión de WebEx basados en la nube y el servidor de WebEx Meetings 162
Atributos de aserciones SAML 170
Grabaciones de reuniones 189
Acerca de las grabaciones de reuniones 189
Almacenamiento recomendado para los archivos de copia de seguridad 190
MIB y controles SNMP compatibles 193
MIB SNMP compatibles 193
Controles SNMP compatibles 199
Requisitos del sistema de usuarios 205
Requisitos comunes del sistema de PC 205
Requisitos del sistema operativo Windows 206
Requisitos del sistema operativo Mac 208
Requisitos de los sistemas operativos de dispositivos móviles 209
Matriz de compatibilidad de la aplicación Cisco WebEx Meetings y las herramientas de productividad 210
Integración de Cisco WebEx Meetings Server con CUCM y compatibilidad del extremo de audio 213
Integración de Cisco Unified Communications Manager (CUCM) 213
Integración de Session Manager Edition (SME) 213
Compatibilidad del punto final de audio 214

CAPÍTULO 1

Requisitos del sistema WebEx

Esta sección proporciona una visión general del hardware, la CPU y la memoria, la red y los requisitos de almacenamiento para Cisco WebEx Meetings Server.

- Requisitos generales del sistema, página 1
- Herramientas de productividad de WebEx, página 7
- Usuarios, página 7
- Tamaños de implementación para el sistema, página 7
- Requisitos para la corresidencia de vCenter, página 8
- Máquinas virtuales en el sistema, página 8
- Requisitos mínimos de hardware, página 9
- Matriz de capacidad del sistema, página 27
- Actualización de la versión 2.6 y matriz de actualización, página 31

Requisitos generales del sistema

Cisco WebEx Meetings Server (CWMS) es compatible con los servidores UCS de Cisco que cumplen o superan las especificaciones presentadas en esta sección.

Nota En la tabla se sugiere que despliegue el almacenamiento interno en una configuración RAID. Para obtener información, consulte Instalación de VMware vSphere ESXi y configuración de almacenamiento, en la página 43 en la *Guía de planificación de Cisco WebEx Meetings Server*.

Importante Cuando realiza una *actualización completa* a una versión posterior de Cisco WebEx Meeting Server, como a la versión 2.0 o la 2.5 desde la versión 1.x, los hosts ESXi (servidor Cisco UCS) donde está ubicada la máquina virtual de administración necesitan 1,5 TB de espacio libre de disco como mínimo. Consulte la sección en este documento donde se describen los sistemas de usuarios de distintos tamaños, empezando por Sistema de 50 usuarios, en la página 12. Durante una actualización, hay dos conjuntos de máquinas virtuales en su red al mismo tiempo: las máquinas virtuales *originales* que ejecutan la versión 1.x y las máquinas virtuales *actualizadas* para admitir la versión más reciente. Para obtener más información, consulte "Actualización completa del sistema" en la Guía de administración de CWMS, en http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Módulo	Notas de requisitos
Servidor host y procesadores	• Servidor para montar en bastidor de la *serie C* de Cisco UCS o servidor en formato blade de la *serie B* equivalente. • Compatibilidad con el conjunto de instrucciones de AES-NI. • Velocidad del reloj del procesador de 2,4 GHz o superior.
Interfaces de red Las tarjetas de interfaz de red (NIC) entre los hosts ESXi (para las máquinas virtuales de Cisco WebEx Meetings Server) y el conmutador Ethernet (no a la interfaz de red externa).	• Mínimo 1 NIC física para una configuración no redundante. Consulte la sección Sistema de 50 usuarios, en la página 12 para los requisitos especiales, donde el IRP y la máquina virtual de administración comparten un host. • Las configuraciones redundantes deben tener todas las interfaces NIC duplicadas (*agrupadas* o *unidas*) y conectadas a un tejido de conmutación independiente. • Una NIC adicional para la red de gestión de VMware (opcional).

Módulo	Notas de requisitos
Almacenamiento interno (DAS) para los hosts ESXi donde se han desplegado máquinas virtuales internas.	• Un mínimo de 4 unidades en una configuración de RAID-10 o RAID-5. • Espacio útil mínimo de 1,5 TB para nuevos despliegues o actualizaciones del sistema. • Cuando se actualiza de Cisco WebEx Meetings Server versión 1.x a 2.0 o 2.5, sus hosts ESXi necesitarán entre 172 GB y 1118 GB de espacio libre en disco, dependiendo del tamaño de su sistema y de las máquinas virtuales. Consulte la sección en este documento donde se describen los sistemas de usuarios de distintos tamaños, empezando por Sistema de 50 usuarios, en la página 12. • Segunda matriz opcional para ESXi **Nota** Las máquinas virtuales deben utilizar el aprovisionamiento grueso para el almacenamiento. (Los clientes ligeros de Citrix no son compatibles).
Almacenamiento interno (DAS) para los hosts ESXi donde se han desplegado máquinas virtuales de IRP.	• Un mínimo de 2 unidades en una configuración de 1 RAID • Almacenamiento utilizable mínimo de 300 GB • Puede utilizar las mismas configuraciones que para las máquinas virtuales internas **Nota** Las máquinas virtuales deben utilizar el aprovisionamiento grueso para el almacenamiento. (Los clientes ligeros de Citrix no son compatibles).

Módulo	Notas de requisitos
Almacenamiento SAN	• Se puede utilizar como sustituto de DAS (se recomienda asignar la misma cantidad de espacio de almacenamiento). • Los servidores blade de la serie B solo tienen dos unidades de disco duro. Si utiliza servidores blade de la serie B de Cisco UCS y piensa realizar una actualización a Cisco WebEx Meetings Server versión 2.0 o versión 2.5, deberá utilizar el almacenamiento SAN para cumplir el requisito de 4 unidades de disco duro en configuración RAID 5 o RAID 10. • Solo se recomienda para despliegues donde el personal de soporte tiene experiencia en supervisión y ajuste del rendimiento SAN. **Nota** Usted es responsable de añadir almacenamiento necesario para nuevos requisitos de VMware y para el crecimiento futuro del sistema. • Canal de fibra (FC) o canal de fibra solo en Ethernet 10 GB (FCoE). • Los requisitos de rendimiento son los mismos que para DAS. • La latencia total permisible máxima medida por vSphere es de 20 ms. Para obtener más información, consulte la sección *Almacenamiento* en http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware#Storage. • Espacio total necesario para máquinas virtuales: La suma de los recursos de almacenamiento reservados para cada máquina virtual del sistema CWMS. **Nota** Las máquinas virtuales deben utilizar el aprovisionamiento grueso para el almacenamiento. (Los clientes ligeros de Citrix no son compatibles).

Módulo	Notas de requisitos
Almacenamiento NAS	• Se puede utilizar como sustituto de DAS o SAN (se recomienda asignar la misma cantidad de espacio de almacenamiento). • Recomendamos utilizar servidores de almacenamiento NAS con servidores para montar en bastidor de la serie C de Cisco UCS. • Solo se recomienda para despliegues donde el personal de soporte tiene experiencia en supervisión y ajuste del rendimiento de NAS. Usted es responsable de añadir almacenamiento adicional necesario para nuevos requisitos de VMware y para el crecimiento futuro del sistema. • Canal de fibra (FC), Sistema de archivos de red (NFS) o solo SCSI. Para obtener información adicional, consulte http://docwiki.cisco.com/wiki/UC_Virtualization_Storage_System_Design_Requirements#General_Guidelines_for_SAN.2FNAS. • Los requisitos de rendimiento son los mismos que para DAS. • La latencia total permisible máxima medida por vSphere es de 20 ms. Para obtener más información, consulte http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware#Storage. • Espacio total necesario para máquinas virtuales: La suma de los recursos de almacenamiento reservados para cada máquina virtual del sistema CWMS. • El servidor de archivos debe admitir las API vStorage para Array Integration (VAAI) y debe utilizar el aprovisionamiento grueso. **Nota** Aunque el esquema de aprovisionamiento predeterminado para el almacenamiento NAS es el aprovisionamiento delgado, las máquinas virtuales deben utilizar el aprovisionamiento grueso para el almacenamiento. (Los clientes ligeros de Citrix no son compatibles). Para activar el aprovisionamiento grueso para el despliegue con almacenamiento NAS, se debe instalar el complemento facilitado del proveedor de almacenamiento para VAAI en todos los servidores UCS usados en el despliegue de Cisco WebEx Meetings Server.

Módulo	Notas de requisitos
Hipervisor	Las versiones de ESXi y las licencias de vSphere se describen en la sección Requisitos mínimos de hardware, en la página 9. • Una licencia VMware por ranura de procesador. • Servidor de vCenter 5.0, 5.0 actualización 1, 5.0 actualización 2, 5.1, 5.1 actualización 1, 5.5 **Nota** Por motivos de seguridad, 5.1 debe ser la versión 1900470 o posterior. • vCenter puede corresidir con Cisco WebEx Meetings Server, siempre que los requisitos de memoria y procesador se agreguen a los requisitos del sistema. Las configuraciones corresidentes de vCenter son compatibles solo con sistemas de 50 y 250 usuarios. • La corresidencia con productos Cisco Unified Communications en el mismo host ESXi físico no es compatible. • La corresidencia con máquinas virtuales no pertenecientes a Cisco WebEx Meetings Server en el mismo host ESXi físico no es compatible.
Servidor de correo electrónico	• Nombre de dominio cualificado completo (FQDN) del servidor de correo que el sistema utiliza para enviar correos electrónicos. • Número de puerto: el valor predeterminado del número de puerto SMTP es 25 o 465 (número de puerto SMTP seguro). • Para utilizar un servidor de correo electrónico compatible con TLS con certificados de terceros, debe importar los certificados en su sistema. Si desea más información, consulte "Administración de certificados" en la Guía de administración en http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.
Licencias	Licencias MDC: se requiere una licencia MDC para cada centro de datos de un sistema con varios centros de datos. No se requiere una licencia MDC para un sistema con un solo centro de datos. Para obtener más información sobre las licencias MDC, consulte Acerca de las licencias de MDC. Licencia de organizador: cada usuario que vaya a organizar una reunión debe disponer de una licencia de organizador para iniciar una reunión web de WebEx, audio de WebEx, una conferencia personal o una reunión de llamada general. Para obtener más información sobre las licencias de organizador, consulte Acerca de las licencias de organizador.

Herramientas de productividad de WebEx

Las herramientas de productividad de WebEx permiten a los usuarios iniciar, planificar o unirse a sesiones de reuniones de WebEx desde aplicaciones como Microsoft® Outlook®. Los usuarios encontrarán más información sobre las herramientas de productividad de Cisco WebEx en http://www.webex.com/support/productivity-tools.html.

Cisco WebEx Meetings Server es compatible con la última versión de las aplicaciones WebEx, disponible en **Configuración** > **Descargas**. Si los usuarios ejecutan una versión anterior de las herramientas de productividad de WebEx después de que se haya realizado una actualización del sistema, pueden organizar, iniciar y unirse a reuniones, pero las funciones más recientes no están disponibles. Recomendamos que envíe de forma silenciosa el último archivo .msi de las herramientas de productividad de WebEx para ofrecer una experiencia óptima. (Consulte Matriz de compatibilidad de la aplicación Cisco WebEx Meetings y las herramientas de productividad, en la página 210).

Usuarios

El sistema admite un ciclo de vida máximo de 400.000 cuentas de usuario. Este número representa el total de cuentas de usuario activas e inactivas. Este número máximo de ciclo de vida es lo suficientemente grande para alojar el crecimiento previsto en la base de datos de usuario.

Los administradores no pueden eliminar a usuarios del sistema. En su lugar, los usuarios se desactivan. Este diseño permite a los administradores reactivar cuentas de usuario desactivadas previamente, incluso después de largos períodos de inactividad del usuario. Las reuniones del usuario y otros contenidos (incluidas las grabaciones) se restauran.

Tamaños de implementación para el sistema

Determinar el tamaño del sistema

Al determinar el tamaño del sistema, tenga en cuenta el número de usuarios posibles que van a utilizar el sistema a la vez. Por ejemplo, en un sistema de 50 usuarios el número máximo de usuarios que simultáneamente asisten a reuniones es 50. Si más de 50 usuarios intentan unirse a una reunión, aparece un mensaje de error para todos los usuarios que intentan unirse a una reunión después de que se haya excedido el número máximo de usuarios y el sistema impide a estos usuarios unirse a la reunión. A continuación se indican algunas cuestiones que se deben tener en cuenta al determinar el tamaño del sistema:

- Determine el número de usuarios más grande que prevé que van a unirse a una reunión en cualquier momento, incluso en ocasiones extrañas o inusuales.
- Siempre puede ampliar el tamaño del sistema. No obstante, el hardware debe cumplir o superar los requisitos mínimos para el tamaño de sistema más grande o deberá adquirir hardware adicional.
- Si piensa añadir alta disponibilidad (HA) o varios centros de datos (MDC) a su sistema, asegúrese de incluir máquinas virtuales adicionales para admitir el sistema HA o MDC cuando compre el hardware.
- ◦ Sistema de 50 usuarios, en la página 12

◦ Sistema de 250 usuarios, en la página 15
◦ Sistema de 800 usuarios, en la página 18
◦ Sistema de 2000 usuarios, en la página 21

Requisitos para la corresidencia de vCenter

La coubicación de VMware vCenter (corresidencia) sólo es compatible con las configuraciones de sistema de 50 y 250 usuarios simultáneos.

Nota Si tiene pensado colocar VMware vCenter en el mismo host que un sistema de 50 o 250 usuarios simultáneos, debe solicitar memoria RAM adicional con el servidor UCS. Para la cantidad exacta de RAM requerida, consulte los requisitos para el tamaño del sistema en el capítulo *Requisitos del sistema WebEx*.

Máquinas virtuales en el sistema

Estas son las máquinas virtuales creadas para su sistema. Algunas funciones se combinan en una máquina virtual para los sistemas de tamaños más pequeños.

- Admin: el "nodo corazón" del sistema. Incluye la base de datos del sistema y proporciona funciones administrativas.
- Multimedia: ofrece servicios de multimedia (función audio-vídeo, servicios de telefonía y de reuniones).

  Se incluye en la máquina virtual Admin en un sistema de 50 usuarios simultáneos.
- Web: proporciona servicios Web (lista de reuniones y grabaciones). Permite al usuario planificar reuniones futuras.

  Se incluye en la máquina virtual Admin en un sistema de 50, 250 u 800 usuarios simultáneos.

  Los usuarios finales inician sesión en el sitio Web de WebEx. Los administradores inician sesión en el sitio web de administración.
- Proxy inverso de Internet (IRP): ofrece acceso público, que permite a los usuarios organizar reuniones o asistir a ellas desde Internet y dispositivos móviles. El proxy inverso de Internet es necesario para que sus trabajadores con dispositivos móviles asistan a reuniones.

Nota En este sistema, sólo se puede utilizar el proxy inverso de Internet proporcionado con este producto. Los proxies inversos de Internet o los equilibradores de carga Web proporcionados por otros proveedores no son compatibles. El proxy inverso de Internet proporcionado con este producto se ha optimizado para manejar el tráfico que comparte datos, audio y Web en tiempo real de usuarios externos que se unen a reuniones desde Internet.

Nota Para sistemas de 800 y 2000 usuarios, no recomendamos desplegar máquinas virtuales adicionales en un host DMZ. Esto puede provocar pérdida de paquetes y latencia destacada en conexiones multimedia.

Nota En esta documentación, utilizamos el término "máquinas virtuales internas" para referirnos a la máquina de administración y, si procede, a la máquina multimedia y la máquina virtual Web.

El proxy inverso de Internet se sitúa en la red DMZ (redes de horizonte dividido y no dividido) o a la red interna (todos los tipos de redes internas).

- Topología de red de horizonte no dividido, en la página 50
- Topología de red de horizonte dividido, en la página 52
- Topología de red interna de proxy inverso de Internet (IRP), en la página 49

Requisitos mínimos de hardware

En esta sección se ofrece una lista de algunos de los servidores Cisco UCS que puede utilizar para cada tamaño de sistema. Para conocer los requisitos específicos de cada sistema, consulte:

- Sistema de 50 usuarios
- Sistema de 250 usuarios
- Sistema de 800 usuarios
- Sistema de 2000 usuarios

Consulte también "Cisco WebEx Meetings Server Ordering Guide" (Guía para pedidos de Cisco WebEx Meetings Server) en http://www.cisco.com/c/en/us/products/conferencing/webex-meetings-server/sales-resources-listing.html.

Tabla 1: Versiones y tipos de Licencia de ESXi

Tamaño del sistema	Versión de ESXi	Tipo de licencia de vSphere
50 o 250	5.0, 5.0 actualización 1, 5.1 o 5.5	Standard Edition, Enterprise Edition, Enterprise Plus Edition
800 o 2000	5.0 o 5.0 actualización 1	Solo Enterprise Plus Edition
	5.1 o posterior[1]	Enterprise Edition, Enterprise Plus Edition
	5.5 o posterior[1]	Standard Edition, Enterprise Edition, Enterprise Plus Edition

[1] "o posterior" hace referencia a las actualizaciones, no a las versiones completas. Por ejemplo, 5.5 actualización 1, 5.1 actualización 2.

Tabla 2: Modelos de host

Tamaño del despliegue	Ejemplo de modelo UCS
50 usuarios	• UCS C220 M3 • UCS B200 M3
250 usuarios	• UCS C220 M3 • UCS B200 M3
800 usuarios	• UCS C460 M2 • UCS B440 M2 • UCS B420 M3
2000 usuarios	• UCS C460 M2 • UCS B440 M2 • UCS B420 M3

La corresidencia con vCenter solo es compatible con los despliegues de sistemas de 50 y 250 usuarios. La corresidencia con productos Cisco Unified Communications en el mismo host físico no es compatible.

Puede utilizar los modelos antiguos del hardware UCS con su sistema, pero para una mejor experiencia del usuario le recomendamos que use el hardware especificado en la tabla. Por ejemplo, puede utilizar el UCS C220 M3 para un sistema de 250 usuarios si ya tiene ese hardware disponible.

Al actualizar a Cisco WebEx Meetings Server versión 2.0, es posible utilizar servidores blade Cisco UCS B200 M3 con el doble de discos duros locales mientras el sistema actualizado utilice almacenamiento SAN para sus máquinas virtuales. El uso de almacenamiento SAN con servidores blade de la serie B permite que su sistema cumpla el requisito de 4 unidades de disco duro en una configuración RAID 5 o RAID 10 para Cisco WebEx Meetings Server versión 2.0.

Nota Para sistemas de 800 y 2000 usuarios, no recomendamos desplegar máquinas virtuales adicionales en un host DMZ. Esto puede provocar pérdida de paquetes y latencia destacada en conexiones multimedia.

Recursos consumidos por Cisco WebEx Meetings Server y el host ESXi

Cisco WebEx Meetings Server se despliega en una o más máquinas virtuales en los hosts ESXi. Cisco WebEx Meetings Server y ESXi (el componente de VMware que permite la virtualización en el servidor UCS físico de Cisco) consumen recursos de CPU y de memoria, y espacio de almacenamiento. Dependiendo del tamaño de su sistema, se pueden ejecutar vCenter y varias máquinas virtuales en el mismo servidor UCS de Cisco.

Cisco WebEx Meetings Server utiliza la *reserva de recursos* para sus máquinas virtuales a fin de garantizar la escalabilidad del sistema. Otras cargas de trabajo de VMware no les quitan CPU ni otros recursos a las máquinas virtuales. Los requisitos mínimos para cada tamaño de sistema incluyen recursos suficientes para admitir:

- Calidad continua del servicio de Cisco WebEx Meetings Server en usos punta del sistema (capacidad máxima).
- VMware ESXi.
- VMware vCenter (cuando es corresidente).

  Para conocer los requisitos del servidor vCenter Server, consulte la Base del conocimiento y busque "Prácticas recomendadas para la instalación de vCenter Server 5.0", "Prácticas recomendadas para la instalación de vCenter Server 5.1" o "Prácticas recomendadas para la instalación de vCenter Server 5.5", respectivamente.
- Instantáneas VMware de la máquina virtual (elimínelas lo antes posible; de lo contrario, puede provocar una grave degradación del rendimiento).

  Se requiere espacio extra en disco para las instantáneas, ya que algunas pueden ser tan grandes como la máquina virtual original. En algunos casos, vSphere puede eliminar instantáneas para crear espacio de almacenamiento, poniendo en peligro la posibilidad de recuperar instantáneas anteriores.
- Uso del servidor UCS de Cisco sobrepasando el ciclo de vida típico del servidor.

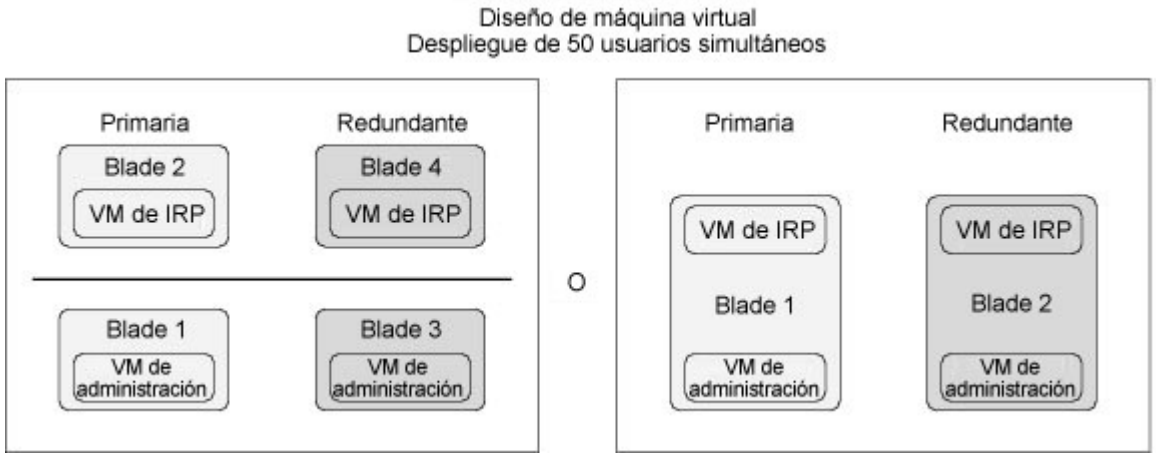
Los requisitos de hardware especificados en el archivo OVA son los requisitos mínimos necesarios para desplegar Cisco WebEx Meetings Server. Estos requisitos *no incluyen* ningún requisito de CPU, memoria o almacenamiento para VMware vCenter o ESXi.

Importante Entre los requisitos para los servidores UCS de Cisco figuran requisitos para Cisco WebEx Meetings Server 2.x, VMware ESXi 5.5, 5.1 y 5.0, y vCenter 5.5, 5.1 y 5.0 (en configuraciones de corresidencia compatibles).

Precaución La corresidencia, a diferencia de las configuraciones mencionadas en las tablas de este documento, no es compatible. Si pasa por alto nuestros requisitos del sistema, es posible que sus máquinas virtuales no puedan arrancar. El despliegue de las máquinas virtuales puede detenerse desde dentro de las pantallas del producto más recientes durante el despliegue de OVA de vCenter.

Sistema de 50 usuarios

Un sistema de 50 usuarios también se describe como un sistema *micro*. (El entorno con varios centros de datos (MDC) no está disponible para los sistemas micro). El diagrama ilustra dos versiones de un despliegue de 50 usuarios. (Las máquinas virtuales "redundantes" demuestran el soporte para la alta disponibilidad (HA).)



En la tabla se muestran los requisitos mínimos de hardware para los hosts ESXi (servidores UCS de Cisco) de su sistema. Las dos últimas columnas muestran la cantidad de espacio de disco necesaria para nuevas instalaciones de Cisco WebEx Meetings Server y el espacio de disco necesario cuando se utiliza la actualización automática para Cisco WebEx Meetings Server de la versión 1.5MR3 a la 2.5 con los servidores Cisco UCS existentes. Para obtener más información, consulte Requisitos generales del sistema.

Para obtener información acerca de los requisitos de ancho de banda, consulte Requisitos de ancho de banda de red, en la página 57.

Nota Para obtener información sobre IOPS, consulte Ventajas de desplegar su sistema en VMware vSphere, en la página 39.

La corresidencia con vCenter es compatible con el despliegue de un sistema de 50 usuarios configurado tal como se indica en la siguiente tabla.

Máquinas virtuales en el host ESXi (servidor UCS de Cisco)	Núcleos de CPU	Memoria (GB)	Puertos Ethernet	Requisitos de almacenamiento en disco duro para nuevas instalaciones	Almacenamiento de disco duro libre necesario para actualizar automáticamente a 2.5 desde 1.5MR3[2]
Admin	4 (ESXi 5.0) 6 (ESXi 5.1 y posterior)	24	2 para la máquina virtual de administración, incluido 1 si se utilizan equipos de NIC para redundancia Se recomienda uno para la red de gestión ESXi	1,5 TB; mínimo de 7200 RPM	1118 GB para una instalación automática.
Admin y vCenter (corresidentes)	6 (ESXi 5.0) 8 (ESXi 5.1 y posterior)	36	2 para la máquina virtual de administración, incluido 1 si se utilizan equipos de NIC para redundancia Uno para vCenter Se recomienda uno para la red de gestión ESXi	1,5 TB; mínimo de 7200 RPM	1.078 GB Esta cifra se basa en la presunción de que ha configurado vCenter con 40 GB.
Proxy inverso de Internet (IRP)	4 (ESXi 5.0) 6 (ESXi 5.1 y posterior)	12	2 para la máquina virtual de IRP, incluido 1 si se utilizan equipos de NIC para redundancia Se recomienda uno para la red de gestión ESXi	300 GB; mínimo de 7200 RPM	172 GB

Máquinas virtuales en el host ESXi (servidor UCS de Cisco)	Núcleos de CPU	Memoria (GB)	Puertos Ethernet	Requisitos de almacenamiento en disco duro para nuevas instalaciones	Almacenamiento de disco duro libre necesario para actualizar automáticamente a 2.5 desde 1.5MR3[2]
Admin e IRP (coresidentes)	8	36	2 para la máquina virtual de administración, incluido 1 si se utilizan equipos de NIC para redundancia 2 para la máquina virtual de IRP, incluido 1 si se utilizan equipos de NIC para redundancia Se recomienda uno para la red de gestión ESXi	1,5 TB; mínimo de 7200 RPM	990 GB
Admin e IRP y vCenter (todos coresidentes)	12	40	2 para la máquina virtual de administración, incluido 1 si se utilizan equipos de NIC para redundancia 2 para la máquina virtual de IRP, incluido 1 si se utilizan equipos de NIC para redundancia Uno para vCenter Se recomienda uno para la red de gestión ESXi	1,5 TB; mínimo de 7200 RPM	950 GB Esta cifra se basa en la presunción de que ha configurado vCenter con 40 GB.

2 Si opta por la actualización completa manual en la que despliega manualmente todas las máquinas virtuales y utiliza el mismo hardware, es necesario que disponga del doble de espacio del necesario para la actualización completa automática.

Nota Si piensa utilizar un sistema de alta disponibilidad (HA), doble los requisitos de hardware y las cantidades del sistema principal para admitir los dos sistemas.

Recursos reservados por las máquinas virtuales en un sistema de 50 usuarios

Esta sección describe cuántos soportes utilizan las máquinas virtuales y está destinada a expertos en VMware. Los recursos de CPU se especifican como vCPUs (núcleos) y Mhz (ciclos de CPU). El VMware VMkernel utiliza ciclos de Mhz para controlar la planificación de la CPU.

Los recursos de memoria se especifican por la memoria máxima y la memoria reservada. La memoria reservada no se comparte con otras máquinas virtuales en el mismo servidor físico UCS de Cisco.

Los recursos de disco (almacenamiento) se controlan en dos zonas separadas. Durante la compilación de OVA, los tamaños de la partición del sistema de archivos de CentOS determinan el tamaño mínimo de disco. En segundo lugar, vCenter controla el espacio máximo disponible de disco.

Si intenta desplegar una máquina virtual sin el número mínimo de vCPU, entonces el despliegue de OVA de la máquina virtual fallará. Si intenta desplegar una máquina virtual sin la velocidad de procesador en MHz mínima total, entonces la máquina virtual no se encenderá.

Importante Los números de esta tabla no incluyen recursos para VMware ESXi o vCenter. Consulte Recursos consumidos por Cisco WebEx Meetings Server y el host ESXi, en la página 11:

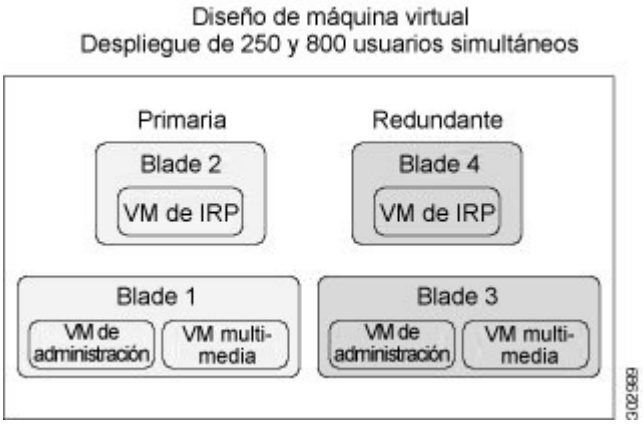
Tipo de máquina virtual	CPU virtual (vCPU)	CPU[3](MHz)	Memoria Reservada/Memoria Total[4](GB)	Discos (GB)
Admin	4	8000	12/14	418
Proxy inverso de Internet	4	8000	4/4	128

3 Número obtenido multiplicando el número de CPU físicas por la velocidad del chip de la CPU (Mhz). Hyperthreading no está incluido en este cálculo. (La CPU física debe tener una velocidad de reloj de 2,4 GHz o superior).

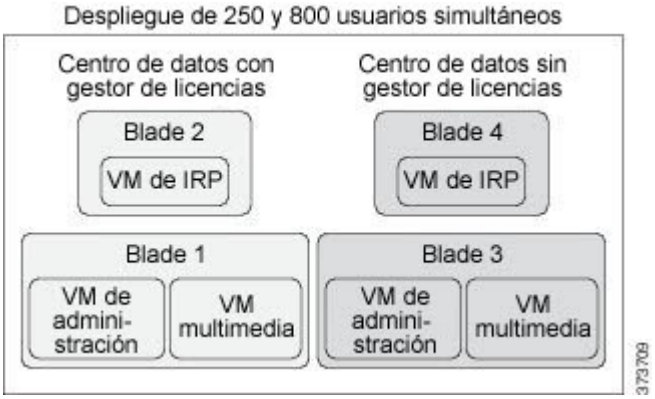
4 Las máquinas virtuales con funcionalidad multimedia tienen memoria adicional no reservada; memoria = reservada/total

Sistema de 250 usuarios

Un sistema de 250 usuarios también se describe como un sistema *pequeño*. Este diagrama esquemático ilustra dos versiones de un despliegue de 250 usuarios. Las máquinas virtuales "redundantes" demuestran el soporte para la alta disponibilidad (HA). Si su sistema no ofrece compatibilidad con HA, entonces despliegue únicamente el sistema **principal**.



Este diagrama muestra la disposición de un sistema de 250 usuarios con dos centros de datos que forman un sistema con varios centros de datos (MDC) con compatibilidad con proxy inverso de Internet (IRP). El Gestor de licencias solo se ejecuta en un centro de datos.



En la tabla se muestran los requisitos mínimos de hardware para los hosts ESXi (servidores UCS de Cisco) de su sistema. Las dos últimas columnas muestran la cantidad de espacio de disco necesaria para nuevas instalaciones de Cisco WebEx Meetings Server y el espacio de disco necesario cuando se utiliza la actualización automática para Cisco WebEx Meetings Server de la versión 1.5MR3 a la 2.5 con los servidores Cisco UCS existentes. Para obtener más información, consulte Requisitos generales del sistema.

Para obtener información acerca de los requisitos de ancho de banda, consulte Requisitos de ancho de banda de red, en la página 57.

Para obtener información sobre IOPS, consulte Ventajas de desplegar su sistema en VMware vSphere, en la página 39.

La corresidencia con vCenter es compatible con el despliegue de un sistema de 250 usuarios configurado tal como se indica en la siguiente tabla.

Máquinas virtuales en el host ESXi (servidor UCS de Cisco)	Núcleos de CPU	Memoria (GB)	Puertos Ethernet	Requisitos de almacenamiento en disco duro para nuevas instalaciones	Almacenamiento de disco duro libre necesario para actualizar automáticamente a 2.5 desde 1.5MR3[5]
Administración y multimedia	12	52	• 2 para multimedia y administración, incluido 1 si se utilizan equipos de NIC para redundancia • Se recomienda uno para la red de gestión ESXi	1,5 TB; mínimo de 7200 RPM	990 GB
(Admin y multimedia) y vCenter (coresidentes)	16	56	• 2 para multimedia y administración, incluido 1 si se utilizan equipos de NIC para redundancia • Se recomienda uno para la red de gestión ESXi • Uno para vCenter	1,5 TB; mínimo de 7200 RPM	950 GB **Nota** Esta cifra se basa en la presunción de que ha configurado vCenter con 40 GB.
Proxy inverso de Internet (IRP)	12	36	• 2 para IRP, incluido 1 si se utilizan equipos de NIC para redundancia • Se recomienda uno para la red de gestión ESXi	300 GB; mínimo de 7200 RPM	172 GB

5 Si opta por la actualización completa manual en la que despliega manualmente todas las máquinas virtuales y utiliza el mismo hardware, es necesario que disponga del doble de espacio del necesario para la actualización completa automática.

Nota Si piensa utilizar un sistema HA, compre el mismo hardware y las mismas cantidades para el sistema HA que para el sistema principal.

Recursos reservados por las máquinas virtuales en un sistema de 250 usuarios

Esta sección describe cuántos soportes utilizan las máquinas virtuales y está destinada a expertos en VMware. Los recursos de CPU se especifican como vCPUs (núcleos) y Mhz (ciclos de CPU). El VMware VMkernel utiliza ciclos de Mhz para controlar la planificación de la CPU.

Los recursos de memoria se especifican por la memoria máxima y la memoria reservada. La memoria reservada no se comparte con otras máquinas virtuales en el mismo servidor físico UCS de Cisco.

Los recursos de disco (almacenamiento) se controlan en dos zonas separadas. Durante la compilación de OVA, los tamaños de la partición del sistema de archivos de CentOS determinan el tamaño mínimo de disco. En segundo lugar, vCenter controla el espacio máximo disponible de disco.

Si intenta desplegar una máquina virtual sin el número mínimo de vCPU, entonces el despliegue de OVA de la máquina virtual fallará. Si intenta desplegar una máquina virtual sin la velocidad de procesador en MHz mínima total, entonces la máquina virtual no se encenderá.

Importante Los números de esta tabla no incluyen recursos para VMware ESXi o vCenter. Consulte Recursos consumidos por Cisco WebEx Meetings Server y el host ESXi.

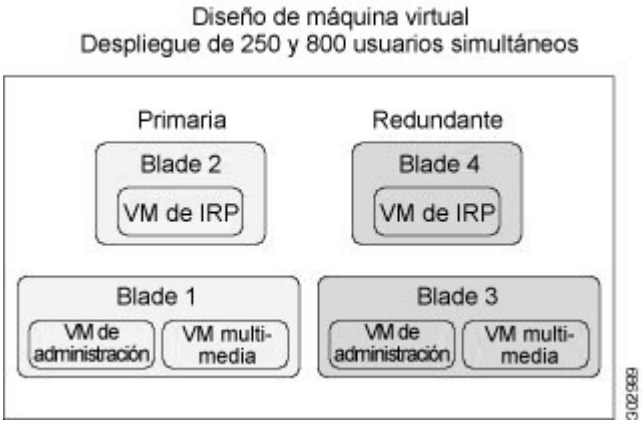
Tipo de máquina virtual	CPU virtual (vCPU)	CPU[6](MHz)	Memoria Reservada/Memoria Total[7](GB)	Discos (GB)
Admin	4	8000	16/16	418
Multimedia	8	16.480	13/23	128
Proxy inverso de Internet	8	16.480	6/6	128

6 Número obtenido multiplicando el número de CPU físicas por la velocidad del chip de la CPU (Mhz). Hyperthreading no está incluido en este cálculo. (La CPU física debe tener una velocidad de reloj de 2,4 GHz o superior).

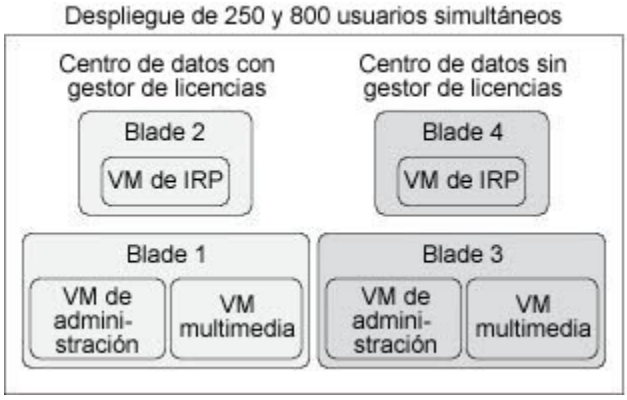
7 Las máquinas virtuales con funcionalidad multimedia tienen memoria adicional no reservada; memoria = reservada/total

Sistema de 800 usuarios

Un sistema de 800 usuarios también se describe como un sistema *medio*. Este diagrama ilustra dos versiones de un despliegue de 800 usuarios. Las máquinas virtuales "redundantes" demuestran el soporte para la alta disponibilidad (HA).



Este diagrama muestra la disposición de un sistema de 800 usuarios con dos centros de datos que forman un sistema con varios centros de datos (MDC) con compatibilidad con proxy inverso de Internet (IRP). El Gestor de licencias solo se ejecuta en un centro de datos.



En la tabla se muestran los requisitos mínimos de hardware para los hosts ESXi (servidores UCS de Cisco) de su sistema. Las dos últimas columnas muestran la cantidad de espacio de disco necesaria para nuevas instalaciones de Cisco WebEx Meetings Server y el espacio de disco necesario cuando se utiliza la actualización automática para Cisco WebEx Meetings Server de la versión 1.5MR3 a la 2.5 con los servidores Cisco UCS existentes. Para obtener más información, consulte Requisitos generales del sistema.

Para obtener información acerca de los requisitos de ancho de banda, consulte Requisitos de ancho de banda de red, en la página 57.

Nota La corresidencia con vCenter no es compatible con el despliegue de un sistema de 800 usuarios.

Para obtener información sobre IOPS, consulte Ventajas de desplegar su sistema en VMware vSphere, en la página 39.

Máquinas virtuales en el host ESXi (servidor UCS de Cisco)	Núcleos de CPU	Memoria (GB)	Puertos Ethernet	Requisitos de almacenamiento en disco duro para nuevas instalaciones	Almacenamiento de disco duro libre necesario para actualizar automáticamente a 2.5 desde 1.5MR3[8]
Administración y multimedia (combinado)	40	80	• 2 para multimedia y administración, incluido 1 si se utilizan equipos de NIC para redundancia • Se recomienda uno para la red de gestión ESXi	1,5 TB; mínimo de 10.000 RPM	990 GB
Proxy inverso de Internet (IRP)	40	36	• 2 para IRP, incluido 1 si se utilizan equipos de NIC para redundancia • Se recomienda uno para la red de gestión ESXi	300 GB; mínimo de 10.000 RPM	172 GB

8 Si opta por la actualización completa manual en la que despliega manualmente todas las máquinas virtuales y utiliza el mismo hardware, es necesario que disponga del doble de espacio del necesario para la actualización completa automática.

Nota Si tiene previsto utilizar un sistema de HA, adquiera los mismos requisitos de hardware y las mismas cantidades que para el sistema primario.

Nota Para sistemas de 800 usuarios, no recomendamos desplegar máquinas virtuales adicionales en un host DMZ. Esto puede provocar pérdida de paquetes y latencia destacada en conexiones multimedia.

Recursos reservados por las máquinas virtuales en un sistema de 800 usuarios

Esta sección muestra cuántos soportes utilizan las máquinas virtuales y está destinada a expertos en VMware. Los recursos de CPU se especifican como vCPUs (núcleos) y Mhz (ciclos de CPU). El VMware VMkernel utiliza ciclos de Mhz para controlar la planificación de la CPU.

Los recursos de memoria se especifican por la memoria máxima y la memoria reservada. La memoria reservada no se comparte con otras máquinas virtuales en el mismo servidor físico UCS de Cisco.

Los recursos de disco (almacenamiento) se controlan en dos zonas separadas. Durante la compilación de OVA, los tamaños de la partición del sistema de archivos de CentOS determinan el tamaño mínimo de disco. En segundo lugar, vCenter controla el espacio máximo disponible de disco.

Si intenta desplegar una máquina virtual sin el número mínimo de vCPU, entonces el despliegue de OVA de la máquina virtual fallará. Si intenta desplegar una máquina virtual sin la velocidad de procesador en MHz mínima total, entonces la máquina virtual no se encenderá.

Importante Los números de esta tabla no incluyen recursos para VMware ESXi. Consulte Recursos consumidos por Cisco WebEx Meetings Server y el host ESXi, en la página 11:

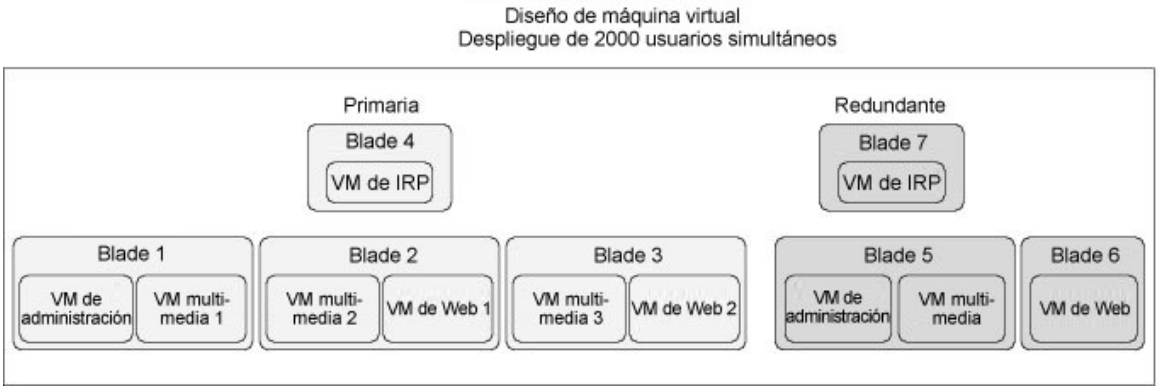
Tipo de máquina virtual	CPU virtual (vCPU)	CPU[9](MHz)	Memoria Reservada/Memoria Total[10](GB)	Discos (GB)
Admin	10	20.600	16/16	418
Multimedia	30	60.800	14/44	128
Proxy inverso de Internet	20	41.200	10/10	128

9 Número obtenido multiplicando el número de CPU físicas por la velocidad del chip de la CPU (Mhz). Hyperthreading no está incluido en este cálculo. (La CPU física debe tener una velocidad de reloj de 2,4 GHz o superior).

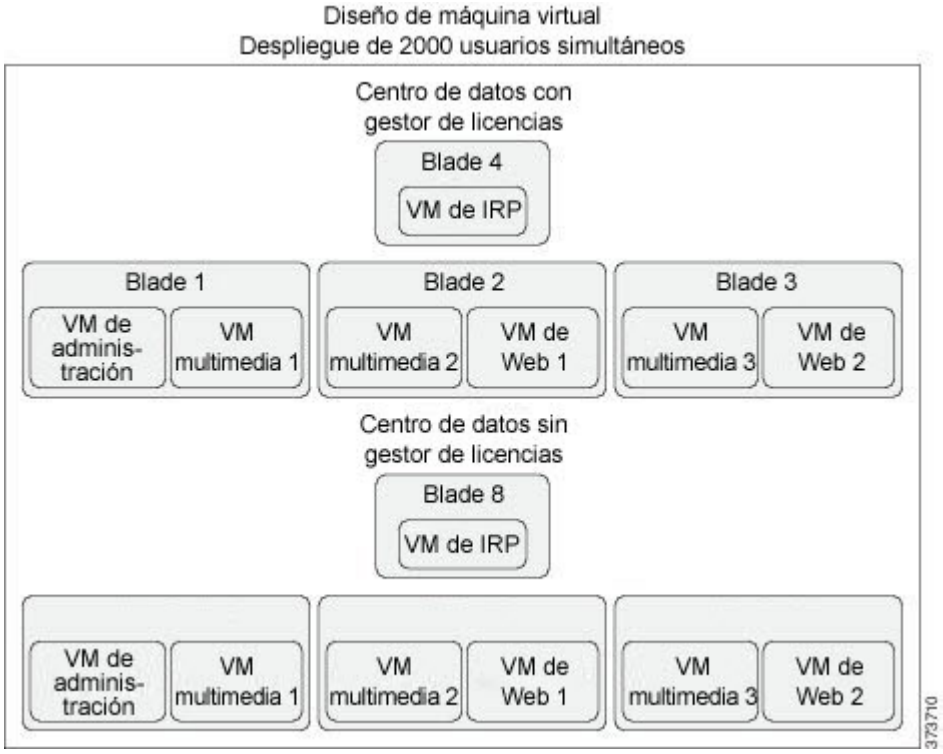
10 Las máquinas virtuales con funcionalidad multimedia tienen memoria adicional no reservada; memoria = reservada/total

Sistema de 2000 usuarios

Un sistema de 2000 usuarios también se describe como un sistema *grande*. Este diagrama muestra un sistema de 2000 usuarios compatible con alta disponibilidad (HA) y proxy inverso de Internet (IRP). Las máquinas virtuales HA se muestran como las máquinas virtuales **redundantes**. Si su sistema no ofrece compatibilidad con HA, entonces despliegue únicamente el sistema **principal**.



Este diagrama muestra el despliegue de un sistema de 2000 usuarios con dos centros de datos que forman un sistema con varios centros de datos (MDC) con compatibilidad con proxy inverso de Internet (IRP). El Gestor de licencias solo se ejecuta en un centro de datos.



Importante Recomendamos que despliegue todas las máquinas virtuales mostradas en el diagrama. Desplegando distintos tipos de máquinas virtuales en un servidor físico, puede evitar una desconexión del sistema en caso de un fallo de hardware. Por ejemplo, colocar máquinas virtuales Web y multimedia en un único servidor físico es más flexible que colocar ambas máquinas virtuales Web en el mismo servidor físico.

En un sistema grande, existe una excepción del reparto equitativo de carga (consulte Equilibrio de la carga, en la página 63 para obtener más información), en la que hay equilibradores de carga del troncal SIP en Media 1 y Media 2, y donde Media 3 y, si quiere, Media HA carecen de equilibrio de carga. Si se produce un error en el sistema principal de Media 1 y de Media 2, se perderán todos los servicios de telefonía de CWMS. Si el sistema es un despliegue de HA, la redundancia atenúa el error de una sola máquina virtual.

En la tabla se muestran los requisitos mínimos de hardware para los hosts ESXi (servidores UCS de Cisco) de su sistema. Las dos últimas columnas muestran la cantidad de espacio de disco necesaria para nuevas instalaciones de Cisco WebEx Meetings Server y el espacio de disco necesario cuando se utiliza la actualización automática para Cisco WebEx Meetings Server de la versión 1.5MR3 a la 2.5 con los servidores Cisco UCS existentes. Para obtener más información, consulte Requisitos generales del sistema.

Para obtener información acerca de los requisitos de ancho de banda, consulte Requisitos de ancho de banda de red, en la página 57.

Si tiene previsto agregar un sistema HA, esas máquinas virtuales se muestran como las máquinas virtuales "redundantes". Si no desea HA, despliegue solo el sistema primario.

Nota La corresidencia con vCenter no es compatible con el despliegue de un sistema de 2000 usuarios.

Nota Para obtener información sobre IOPS, consulte Ventajas de desplegar su sistema en VMware vSphere, en la página 39.

Máquinas virtuales en el host ESXi (servidor UCS de Cisco)	Núcleos de CPU	Memoria (GB)	Puertos Ethernet	Requisitos de almacenamiento en disco duro para nuevas instalaciones	Almacenamiento de disco duro libre necesario para actualizar automáticamente a 2.5 desde 1.5MR3[11]
Multimedia1 y administración (combinado)	40	80	• 2 para multimedia1 y administración, incluido 1 si se utilizan equipos de NIC para redundancia • Se recomienda uno para la red de gestión ESXi	1,5 TB; mínimo de 10.000 RPM	990 GB

Máquinas virtuales en el host ESXi (servidor UCS de Cisco)	Núcleos de CPU	Memoria (GB)	Puertos Ethernet	Requisitos de almacenamiento en disco duro para nuevas instalaciones	Almacenamiento de disco duro libre necesario para actualizar automáticamente a 2.5 desde 1.5MR3[11]
Multimedia2 y Web1 (combinado)	40	80	• 2 para multimedia2 y Web1, incluido 1 si se utilizan equipos de NIC para redundancia • Se recomienda uno para la red de gestión ESXi	1 TB; mínimo de 10.000 RPM	768 GB
Multimedia3 y Web2 (combinado)	40	80	• 2 para multimedia3 y Web2, incluido 1 si se utilizan equipos de NIC para redundancia • Se recomienda uno para la red de gestión ESXi	1 TB; mínimo de 10.000 RPM	768 GB

Máquinas virtuales en el host ESXi (servidor UCS de Cisco)	Núcleos de CPU	Memoria (GB)	Puertos Ethernet	Requisitos de almacenamiento en disco duro para nuevas instalaciones	Almacenamiento de disco duro libre necesario para actualizar automáticamente a 2.5 desde 1.5MR3[11]
Proxy inverso de Internet (IRP)	40	36	• 2 para IRP, incluido 1 si se utilizan equipos de NIC para redundancia • Se recomienda uno para la red de gestión ESXi	300 GB; mínimo de 10.000 RPM	172 GB
Multimedia y administración (combinado) para HA	40	80	• 2 para multimedia y administración, incluido 1 si se utilizan equipos de NIC para redundancia • Se recomienda uno para la red de gestión ESXi	1,5 TB; mínimo de 10.000 RPM	990 GB
Web para HA	40	80	• 2 para Web, incluido 1 si se utilizan equipos de NIC para redundancia • Se recomienda uno para la red de gestión ESXi	1 TB; mínimo de 10.000 RPM	896 GB

Máquinas virtuales en el host ESXi (servidor UCS de Cisco)	Núcleos de CPU	Memoria (GB)	Puertos Ethernet	Requisitos de almacenamiento en disco duro para nuevas instalaciones	Almacenamiento de disco duro libre necesario para actualizar automáticamente a 2.5 desde 1.5MR3[11]
IRP para HA	40	36	• 2 para IRP, incluido 1 si se utilizan equipos de NIC para redundancia • Se recomienda uno para la red de gestión ESXi	300 GB; mínimo de 10.000 RPM	172 GB

11 Si opta por la actualización completa manual en la que despliega manualmente todas las máquinas virtuales y utiliza el mismo hardware, es necesario que disponga del doble de espacio del necesario para la actualización completa automática.

Nota Para sistemas de 2000 usuarios, no recomendamos desplegar máquinas virtuales adicionales en un host DMZ. Esto puede provocar pérdida de paquetes y latencia destacada en conexiones multimedia.

Recursos reservados por las máquinas virtuales en un sistema de 2000 usuarios

Esta sección muestra cuántos soportes utilizan las máquinas virtuales y está destinada a expertos en VMware. Los recursos de CPU se especifican como vCPUs (núcleos) y Mhz (ciclos de CPU). El VMware VMkernel utiliza ciclos de Mhz para controlar la planificación de la CPU.

Los recursos de memoria se especifican por la memoria máxima y la memoria reservada. La memoria reservada no se comparte con otras máquinas virtuales en el mismo servidor físico UCS de Cisco.

Los recursos de disco (almacenamiento) se controlan en dos zonas separadas. Durante la compilación de OVA, los tamaños de la partición del sistema de archivos de CentOS determinan el tamaño mínimo de disco. En segundo lugar, vCenter controla el espacio máximo disponible de disco.

Si intenta desplegar una máquina virtual sin el número mínimo de vCPU, entonces el despliegue de OVA de la máquina virtual fallará. Si intenta desplegar una máquina virtual sin la velocidad de procesador en MHz mínima total, entonces la máquina virtual no se encenderá.

Importante Los números de esta tabla no incluyen recursos para VMware ESXi. Consulte Recursos consumidos por Cisco WebEx Meetings Server y el host ESXi.

Tipo de máquina virtual	CPU virtual (vCPU)	CPU[12](MHz)	Memoria Reservada/Memoria Total[13](GB)	Discos (GB)
Admin	10	20.600	16/16	418 Para la versión 2.6 o las posteriores, los nuevos sistemas desplegados con un archivo OVA tienen que ser 513.
Multimedia	30	60.800	14/44	128
Web	10	20.600	16/16	128
Proxy inverso de Internet	20	41.200	10/10	128

12 Número obtenido multiplicando el número de CPU físicas por la velocidad del chip de la CPU (Mhz). Hyperthreading no está incluido en este cálculo. (La CPU física debe tener una velocidad de reloj de 2,4 GHz o superior).

13 Las máquinas virtuales con funcionalidad multimedia tienen memoria adicional no reservada; memoria = reservada/total

Matriz de capacidad del sistema

Puntos clave:

- Uno de los supuestos básicos para la información presentada en la tabla siguiente es que hay como mínimo dos personas participando en una reunión.
- Las conexiones de reuniones simultáneas se definen como el número de personas que participan en una reunión en un momento específico. Por ejemplo, en un sistema de 50 usuarios, las conexiones de reuniones simultáneas máximas pueden constar de cinco reuniones simultáneas donde cada una tiene un total de 10 personas en la reunión (por ejemplo, un organizador y nueve participantes).
- Después de alcanzar el número máximo de participantes de la reunión en un momento específico, el sistema no permite que otros usuarios empiecen o se unan a reuniones. De ese número máximo de participantes de la reunión (2000, 800, 250 o 50 personas), solo la mitad de los participantes pueden utilizar vídeo. El vídeo se define como el envío o la recepción, por lo que los usuarios pueden utilizar los archivos de su cámara web de WebEx o la opción de compartir archivo de vídeo que permite que los usuarios compartan vídeo.
- El uso compartido del escritorio no se considera vídeo. Esto significa que en un sistema de 250 usuarios, 250 personas pueden compartir sus escritorios durante las reuniones en cualquier momento.
- La adición de alta disponibilidad o un entorno con varios centros de datos no aumenta la capacidad del sistema para realizar reuniones; un sistema de 800 usuarios sigue siendo un sistema de 800 usuarios.

Los números de la tabla siguiente representan la capacidad nominal para el sistema Cisco WebEx Meetings Server. El funcionamiento del sistema a capacidades superiores a las especificadas generará una experiencia degradada del usuario y puede provocar inestabilidad en el sistema. Cisco se reserva el derecho de aplicar límites de capacidad en estos niveles.

Nota Los valores de la tabla siguiente siguen siendo iguales independientemente de si el sistema consta de un solo centro de datos o si es un sistema con varios centros datos.

Tabla 3: Matriz de capacidad del sistema para la versión 2.5 y posteriores

Capacidad del sistema	Sistema de 2000 usuarios	Sistema de 800 usuarios	Sistema de 250 usuarios	Sistema de 50 usuarios	Notas
Conexiones de reuniones simultáneas máximas (usuarios de audio, vídeo y web)	2000	800	250	50	El número de personas que participan en reuniones simultáneas en un momento específico.
Máximo de conexiones de audio simultáneas (llamadas de teléfono de teleconferencia y conexión de voz utilizando el ordenador de los clientes de la reunión)	2000	800	250	50	La capacidad del sistema permanece igual tal y como se indica a la izquierda, independientemente de la combinación de las siguientes funciones que se utilice: • Códecs de audio G.711, G.722, G.729 • Audioconferencia IPv4 o Ipv6 • Cifrado de audio TLS/SRTP
Nº máximo de usuarios simultáneos con vídeo y uso compartido de archivos de vídeo	1000[14]	400	125	25	Estas cifras indican el número máximo de conexiones de reuniones simultáneas (o participantes) que pueden utilizar vídeo compartido al mismo tiempo. Cuando el número de usuarios que comparten vídeo en reuniones simultáneas alcance este límite, los usuarios restantes invitados a las reuniones simultáneas pueden unirse a la reunión, pero sus ventanas de vídeo aparecerán sombreadas. **Nota** Si un participante de una reunión utiliza vídeo, entonces todos los demás usuarios de la misma reunión se cuentan como usuarios de vídeo, aunque no utilicen vídeo. **Nota** El uso compartido del escritorio no se considera vídeo.

Capacidad del sistema	Sistema de 2000 usuarios	Sistema de 800 usuarios	Sistema de 250 usuarios	Sistema de 50 usuarios	Notas
Nº máximo de participantes en una reunión	500	500	250	50	Estas cifras indican el número máximo de participantes que pueden asistir a una reunión.
Reuniones máximas que se pueden grabar simultáneamente	100	40	13	3	Es el número total de reuniones que pueden utilizar la función de Grabación a la vez.
Nº máximo de sesiones de reproducción de grabaciones simultáneas	500	200	63	12	Es el número total de sesiones de reproducción de grabaciones que pueden producirse al mismo tiempo. Hace referencia a las grabaciones que se guardan en su sistema de almacenamiento y no incluye las grabaciones que se han descargado en los escritorios de los usuarios. **Nota** Estas sesiones de reproducción no están incluidas en las conexiones de reuniones simultáneas en el sistema.
Número máximo de perfiles de usuario	400.000	400.000	400.000	400.000	Esta cantidad incluye usuarios activos e inactivos.
Reuniones simultáneas máximas	1000	400	125	25	El número de reuniones individuales que pueden estar activas al mismo tiempo.
Índice máximo de llamadas (llamadas/por segundo)	20	8	3	1	Es el promedio de usuarios que pueden marcar en una reunión durante un periodo de tiempo de un segundo. Cuando el sistema alcanza este número, los siguientes usuarios en marcar en la reunión pueden sufrir una espera de unos pocos segundos adicionales antes de conectarse a la reunión.
Nº máximo de inicios de sesión simultáneos	20 personas por segundo	8 personas por segundo	3 personas por segundo	1 persona por segundo	Es el promedio de usuarios que pueden iniciar sesión simultáneamente en su sitio de WebEx durante un periodo de tiempo de un segundo. Cuando el sistema alcanza este número, los siguientes usuarios en iniciar sesión en el sitio de WebEx pueden sufrir una espera de unos pocos segundos adicionales antes de poder unirse a una reunión.

Capacidad del sistema	Sistema de 2000 usuarios	Sistema de 800 usuarios	Sistema de 250 usuarios	Sistema de 50 usuarios	Notas
Uso máximo de ancho de banda agregado	5 Gbps	2 Gbps	625 Mbps	125 Mbps	Utilizar nuestro sistema de prueba a su ancho de banda máximo, es el ancho de banda máximo que el sistema de pruebas puede gestionar. Para obtener más información sobre la utilización del ancho de banda, consulte la sección de Requisitos de ancho de banda de red en el capítulo *Topología de red para su sistema* en la Guía de planificación. También puede consultar el Documento técnico de ancho de banda de la red WebEx.

14 800 en entornos de Norma federal de procesamiento de la información (FIPS, por sus siglas en inglés)

Nota Para las nuevas instalaciones de Cisco WebEx Meetings Server versión 2.0 y posteriores, los requisitos de almacenamiento son:

- El espacio en disco puede ser local (DAS) o externo (SAN/NAS).
- Los hosts ESXi (servidor Cisco UCS) con la máquina virtual de administración necesitan 1,5 TB de espacio en disco.
- Los hosts ESXi (servidor Cisco UCS) sin una máquina virtual de administración necesitan 1 TB de espacio en disco.
- Al actualizar Cisco WebEx Meetings Server utilizando servidores UCS de Cisco existentes, los hosts ESXi necesitarán 1118 GB de espacio en disco si el servidor UCS solo tiene la máquina virtual de administración (sistema de alta disponibilidad o principal) o 990 GB de espacio en disco si el servidor UCS tiene una máquina virtual multimedia y una de administración (sistema de alta disponibilidad o principal).

Para más información, consulte la sección **Recursos consumidos por Cisco WebEx Meetings Server y el host ESXi** en http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html.

Consejo La duración máxima de una reunión es de 24 horas para los despliegues de sistemas de usuario de todos los tamaños.

Nota Al considerar una actualización, planifique el aumento de tamaño para los almacenes de datos, ya que el sistema original y el sistema actualizado comparten los almacenes de datos hasta que se completan las pruebas del sistema actualizado y se suprime el sistema original.

Para obtener información acerca de los requisitos de ancho de banda de la red para los distintos tamaños de sistemas de usuario, consulte el apartado "Requisitos de ancho de banda de red" del capítulo de Topología de redes para el sistema de este manual.

Actualización de la versión 2.6 y matriz de actualización

Utilice la siguiente tabla para saber cómo iniciar la actualización completa o parcial a la versión 2.6 de Cisco WebEx Meetings Server.

Versión instalada	Versión 2.6	Ruta
De 1.0 a 1.1	2.6	**1** Actualización parcial a 1.5 **2** Actualización parcial a 1.5MR5 **3** Actualización completa a 2.6
De 1.5 a 1.5MR4	2.6	**1** Actualización parcial a 1.5MR5 **2** Actualización completa a 2.6
1.5 MR5 y superior	2.6	Actualización completa a 2.6
De 2.0 a 2.0MR8	2.6	**1** Actualización parcial a 2.0MR9 **2** Actualización parcial a 2.6
2.0MR9 o superior	2.6	Actualización parcial a 2.6
2.5 o cualquier versión 2.5MR Un solo centro de datos (SDC)	2.6	Actualización parcial a 2.6
2.5 o cualquier versión 2.5MR Varios centros de datos (MDC)	2.6[15]	Actualización parcial a 2.6
2.6 o cualquier versión 2.6MR Un solo centro de datos (SDC)	Cualquier versión 2.6MR	Actualización parcial a 2.6MR

Versión instalada	Versión 2.6	Ruta
2.6 o cualquier versión 2.6MR Varios centros de datos (MDC)	Cualquier versión 2.6MR	Actualización parcial a 2.6MR

15 **Importante:** las actualizaciones parciales necesitan que se produzca un tiempo de inactividad, ya que es necesario actualizar los dos centros de datos de forma simultánea. No haga clic en **Reiniciar** para volver a iniciar un centro de datos hasta que termine de actualizarse el otro y ambos muestren el botón **Reiniciar**.

Al actualizar de la versión 2.5 a la 2.6, si se reinicia un centro de datos antes de que finalice la actualización del otro, se rompe la replicación.

CAPÍTULO 2

Introducción y topología del centro de datos para su sistema

En este capítulo se proporciona una introducción, una visión general de un centro de datos y los requisitos de VMware vCenter para su sistema.

- Introducción al servidor de Cisco WebEx Meetings, página 33
- Información para los clientes de Cisco Unified MeetingPlace, página 35
- Conceptos generales sobre el despliegue del sistema, página 35
- Despliegue de un solo centro de datos, página 38
- Unión de centros de datos individuales para crear un sistema con varios centros datos (MDC), página 38
- Utilización de VMware vSphere con su sistema, página 39
- IOPS y rendimiento del sistema de almacenamiento, página 41
- Instalación de VMware vSphere ESXi y configuración de almacenamiento, página 43
- Entrada en reuniones, página 44

Introducción al servidor de Cisco WebEx Meetings

Cisco WebEx Meetings Server es una solución de conferencias segura, completamente virtualizada y de nube privada (local) que combina audio, vídeo y Web para reducir los costes de las conferencias y ampliar sus inversiones en Cisco Unified Communications.

Cisco WebEx Meetings Server satisface las necesidades de las empresas actuales presentando una solución de conferencias completa con todas las herramientas necesarias para una colaboración efectiva y comprometida. Ofrece una experiencia productiva e interactiva a los usuarios.

Puede desplegar y gestionar esta solución de conferencias en su nube privada, detrás del cortafuegos en su centro de datos. Está diseñada para servidores UCS de Cisco y VMware vSphere (Para obtener información sobre requisitos específicos, consulte Requisitos mínimos de hardware, en la página 9). Cuenta con un despliegue virtual rápido y herramientas potentes para que los administradores configuren y gestionen el sistema, además de ver las principales métricas del sistema.

Al igual que otros productos de Cisco WebEx, ofrece herramientas de colaboración en tiempo real, como uso compartido de escritorio, documentos y aplicaciones, herramientas de anotación, control completo del organizador para una gestión efectiva de la reunión, y una lista integrada de participantes con orador activo y cambio de vídeo, grabación y reproducción. Este producto utiliza vídeo de alta calidad para que la experiencia de uso compartido de vídeo sea clara y nítida.

Además, los usuarios con dispositivos móviles pueden asistir y participar en reuniones. Para conocer los dispositivos compatibles, consulte Requisitos de los sistemas operativos de dispositivos móviles, en la página 209.

Consideraciones importantes para su sistema

Tenga en cuenta lo siguiente:

- Proxies de envío: no se recomiendan, pero puede usarlos con restricciones.

  Para obtener información detallada, consulte la *Guía de solución de problemas de Cisco WebEx Meetings Server*.

- Proxies inversos: sólo es compatible el proxy inverso de Internet incluido con este producto.

- NAT: es compatible si cumple los requisitos de este sistema.

  Para obtener detalles completos, consulte Uso de NAT con el sistema.

- Centros de datos únicos: los despliegues con un solo centro de datos se admiten para todas versiones de Cisco WebEx Meetings Server.

  Para ver detalles completos, consulte Despliegue de un solo centro de datos.

- Varios centros de datos: los centros de datos que ejecutan Cisco WebEx Meetings Server versión 2.5 se pueden unir para crear un sistema que conste de varios centros de datos.

  Para obtener información detallada, consulte la sección *Acerca de los centros de datos múltiples* en la Guía de administración de Cisco WebEx Meetings Server.

- Servidor de almacenamiento: cada centro de datos de un sistema con varios centros de datos debe tener un servidor de almacenamiento distinto. El mismo servidor de almacenamiento no puede admitir más de un centro de datos.

- Sistema de alta disponibilidad: un sistema con máquinas virtuales redundantes que ejecutan la misma versión de Cisco WebEx Meetings Server. Si el sistema principal (de un sistema con un solo centro de datos) falla, el sistema de alta disponibilidad sigue prestando el servicio. Las máquinas virtuales de alta disponibilidad redundantes se deben localizar de forma conjunta en el mismo centro de datos con las máquinas virtuales principales. Las máquinas virtuales de los sistemas principal y de alta disponibilidad también deben estar en la misma VLAN o subred.

  No se pueden unir sistemas de alta disponibilidad para crear un entorno con varios centros de datos.

- Servidor de proxy inverso de Internet (IRP): una máquina virtual colocada como un proxy entre la red Internet externa y la red interna de una empresa para proporcionar acceso público a Cisco WebEx Meetings Server. Hará falta un servidor de proxy inverso de Internet si desea permitir a los usuarios planificar y asistir a reuniones desde dispositivos móviles interna y externamente, o si desea proporcionar acceso seguro a su sitio de WebEx desde Internet. El servidor de proxy inverso de Internet no es necesario si va a permitir el acceso a Cisco WebEx Meetings Server solo desde su red interna. Despliegue una máquina virtual de IRP utilizando el mismo archivo OVA que ha usado para desplegar su máquina virtual de administración. La máquina virtual de IRP debe encontrarse en la misma subred que la dirección IP virtual pública.

- Dirección IP virtual (VIP): dirección IP utilizada para comunicarse con las máquinas virtuales de administración, multimedia y web dentro de un centro de datos.
- Dirección IP virtual (VIP) privada: una dirección IP adicional configurada en la máquina virtual de administración y asociada con el URL del sitio de administración. La dirección IP virtual privada también puede estar asociada con el URL del sitio de WebEx si la dirección está configurada en el servidor DNS interno en un despliegue o en despliegues de DNS de horizonte dividido sin un servidor de proxy inverso de Internet.
- Dirección IP virtual (VIP) pública: una dirección IP adicional configurada en la máquina virtual de proxy inverso de Internet y asociada solo con el URL del sitio de WebEx. El URL del sitio de WebEx en los servidores DNS externos se debe poder resolver a la dirección IP virtual pública para proporcionar a los usuarios acceso al sitio de WebEx desde Internet. Una dirección IP virtual pública no está configurada en el sistema si no hay ningún servidor de proxy inverso de Internet.

Precaución Si ignora nuestras recomendaciones y requisitos al desplegar un sistema, no recibirá soporte de Cisco. Cisco no se hace responsable de los problemas que pueda tener por no seguir nuestras instrucciones.

Características nuevas y cambiadas de Cisco WebEx Meetings Server

Para obtener una lista de las características nuevas y modificadas, consulte la sección "Características nuevas y modificadas de Cisco WebEx Meetings Server" en las *Notas de la versión de Cisco WebEx Meetings Server* en Notas de la versión.

Información para los clientes de Cisco Unified MeetingPlace

Importante Debido a diferencias arquitectónicas, no hay ninguna ruta de migración (para cuentas de usuario, personalizaciones y reuniones existentes) de Cisco Unified MeetingPlace a Cisco WebEx Meetings Server. Éstos son dos productos distintos.

Puede facilitar la transición a sus usuarios si sigue dando soporte a ambos, Cisco Unified MeetingPlace y Cisco WebEx Meetings Server, durante un período de tiempo, mientras que anima a sus usuarios a cambiar al nuevo sistema. Para ayudar con la formación de usuario durante esta transición, Cisco proporciona vídeos de formación a los que se puede acceder desde la página Ayuda del usuario final.

Conceptos generales sobre el despliegue del sistema

Tamaños del sistema

Los sistemas se identifican por el número de usuarios simultáneos admitidos:

- 50 usuarios simultáneos (también se conoce como un sistema *micro*).
  - Normalmente es compatible con una empresa que tenga entre 500 y 1000 empleados.

- Un sistema principal [(sin alta disponibilidad (HA)] consta de una máquina virtual de administración y una máquina de proxy inverso de Internet (IRP) opcional.

- 250 usuarios simultáneos (también se conoce como un sistema *pequeño*).
  - Normalmente es compatible con una empresa que tenga entre 2500 y 5000 empleados.
  - Un sistema primario (sin HA) está formado por una máquina virtual de administración, una máquina virtual multimedia y una máquina de proxy inverso de Internet (IRP) opcional.

- 800 usuarios simultáneos (también se conoce como un sistema *medio*).
  - Normalmente es compatible con una empresa que tenga entre 8000 y 16 000 empleados.
  - Un sistema primario (sin HA) está formado por una máquina virtual de administración, una máquina virtual multimedia y una máquina de proxy inverso de Internet (IRP) opcional.

- 2000 usuarios simultáneos (también se conoce como un sistema *grande*).
  - Normalmente es compatible con una empresa que tenga entre 20 000 y 40 000 empleados.
  - El sistema principal (sin HA) está formado por una máquina virtual de administración, tres máquinas virtuales multimedia, dos máquinas web y una máquina de proxy inverso de Internet (IRP) opcional.

Términos utilizados durante el despliegue

URL del sitio de WebEx: dirección URL segura de protocolo HTTP usada para que los usuarios organicen y asistan a reuniones en un entorno de un solo centro de datos.

URL de administración de WebEx: dirección URL segura de protocolo HTTP usada para que los administradores configuren, supervisen y gestionen el sistema en un entorno de un solo centro de datos.

VIP pública: dirección IP virtual de la URL del sitio de WebEx.

VIP privada: dirección IP virtual para la URL del sitio de administración o la dirección IP virtual para la URL del sitio de WebEx (solo para usuarios internos, si tiene un DNS de horizonte dividido).

URL de WebEx común: el DNS la utiliza para redirigir al usuario al centro de datos donde el usuario realiza tareas relacionadas con la reunión, como la planificación u organización de reuniones. El centro de datos que elige el DNS es una cuestión transparente para el usuario. La URL de WebEx común es sencillamente una ubicación conveniente para que un usuario entre en el sistema. Si un centro de datos queda fuera de servicio, nada cambia para el usuario, incluida la URL utilizada para acceder a reuniones, porque el DNS redirigirá al usuario al centro de datos activo alternativo.

URL de administración común: se conoce a menudo como simplemente la *URL de administración*. El DNS la utiliza para redirigir a un administrador al centro de datos de gestión en el que el administrador inicia sesión en el sistema. El centro de datos que elige el DNS es una cuestión transparente para el administrador (no obstante, la serie de la barra de la URL cambia según el centro de datos que el administrador usa para acceder al sistema). La URL de administración común es sencillamente un destino conveniente que un administrador utiliza para entrar en el sistema.

URL de administración locales: son específicas para cada centro de datos en un sistema con varios centros de datos (MDC). Al iniciar sesión por medio de la URL de administración común, el DNS redirige al administrador a la URL de administración local para el centro de datos de gestión. Cualquier modificación del sistema, como la asignación de una licencia a un usuario, se realiza en el centro de datos de gestión y se replica a todos los centros de datos del sistema MDC.

Un administrador puede elegir un centro de datos específico para modificarlo desde dentro de la aplicación CWMS, pero si se selecciona otro centro de datos para modificar, no se cambia la URL de administración local, porque el acceso del administrador al sistema permanece en el centro de datos elegido por el DNS cuando el administrador inició sesión en el sistema. Las modificaciones del administrador a otro centro de datos del sistema MDC pasan a través del centro de datos de gestión elegido por el DNS al centro de datos de destino.

Un sistema MDC tendrá un mínimo de dos URL de administración locales, una para cada centro de datos del sistema.

URL locales que son específicas de cada centro de datos.

Información del perfil del sistema

Complete este gráfico de su sistema.

URL del sitio común		
URL de administración común		
Direcciones IP virtuales DC1 y DC2		
	Centro de datos 1	**Centro de datos 2**
URL de sitio local		
URL de administración local		
Direcciones IP virtuales públicas		
Direcciones IP virtuales privadas		
Servidor DNS		
Dirección IP de la máquina de administración virtual		
Dirección IP 1 de la máquina virtual multimedia		
Dirección IP 2 de la máquina virtual multimedia		
Dirección IP 3 de la máquina virtual multimedia		
Dirección IP 1 de la máquina virtual web		
Dirección IP 2 de la máquina virtual web		

Dirección IP de la máquina virtual DMZ (opcional)		
Direcciones de correo electrónico del administrador de CWMS		
Contraseña del administrador		
Remote Access[16]		
Contraseña de Remote Access		
Dirección IP de Call Manager		
ID de administrador de Cisco Call Manager		
Contraseña de Cisco Call Manager		
Números de teléfono de CWMS		
Números de teléfono		

16 Remote Access no estará disponible, a no ser que se active la cuenta.

Despliegue de un solo centro de datos

Cisco WebEx Meeting Server (CWMS) se puede desplegar como un sistema con un solo centro de datos (SDC) y opcionalmente como un sistema de alta disponibilidad (HA) o un sistema con varios centros de datos (MDC) (consulte Redundancia en despliegues de HA o MDC, en la página 54). Un sistema SDC (incluido un sistema con soporte de HA) solo requiere licencias de organizador después de un período de prueba. Un sistema MDC requiere un mínimo de dos licencias de función MDC, licencias de organizador, y no hay ningún período de prueba de MDC.

Unión de centros de datos individuales para crear un sistema con varios centros datos (MDC)

Puede unir centros de datos individuales que ejecuten Cisco WebEx Meeting Server versión 2.5 para formar un sistema con varios centros de datos (MDC). (Para la versión 2.5, se pueden unir un máximo de dos centros de datos). Los centros de datos pueden encontrarse en ubicaciones geográficas diferentes y funcionar como pares, a diferencia de un sistema que funcione como una copia de seguridad de un sistema CWMS principal. Un sistema de alta disponibilidad que debe estar localizado de forma conjunta en el mismo centro de datos es un ejemplo de una configuración de sistema de copia de seguridad. Consulte Redundancia en despliegues de HA o MDC, en la página 54: Para obtener información detallada sobre cómo preparar los centros de datos que se deben unir y cómo transferir datos de un centro de datos a otro cuando el proceso de unión ha finalizado, consulte el capítulo "Unión de centros de datos para crear un sistema con varios centros datos (MDC)" de la *Guía de administración de Cisco WebEx versión 2.5*.

Utilización de VMware vSphere con su sistema

VMware vSphere

Importante Este producto sólo se instala en una plataforma de virtualización de VMware de vSphere. Recuerde que las herramientas de VMWare para CWMS se instalan automáticamente durante el despliegue del sistema y que no se deben actualizar de forma manual. Consulte docwiki.cisco.com/wiki/VMware_Tools para obtener más información sobre las herramientas de VMWare.

- Cisco WebEx Meetings Server está diseñado para funcionar en cualquier servidor UCS de Cisco equivalente que cumpla o supere las especificaciones del sistema. Sin embargo, para no malgastar su tiempo, le recomendamos que use los servidores UCS de Cisco corrientes. Para obtener detalles completos sobre los requisitos de hardware y de VMware, consulte Requisitos mínimos de hardware, en la página 9.
- Debe comprar VMware vSphere 5.0, 5.0 Actualización 1, 5.0 Actualización 2, 5.1, 5.1 Actualización 1 o 5.5 para utilizarlo como plataforma de hipervisor para Cisco WebEx Meetings Server.

  Nota Por motivos de seguridad, 5.1 debe ser la versión 1900470 o posterior.

  Realice una de estas acciones:

  - Adquiera vSphere directamente de Cisco en la GPL (Lista global de precios). Cisco es un socio y distribuidor autorizado de Vahare.
  - Adquiera vSphere directamente de VMware, a través de los acuerdos empresariales que tenga con VMware.

Ventajas de desplegar su sistema en VMware vSphere

En este apartado se explica por qué VMware vSphere y vCenter son fundamentales para utilizar este producto de Cisco WebEx, y se proporcionan algunas consideraciones.

Despliegue del sistema

- Este producto se empaqueta como un dispositivo virtual OVA compatible con VMware vSphere y no como una colección de paquetes de software en un DVD. Debe tener un vCenter para desplegar el OVA o el producto no se instalará.
- Empaquetándolo como un dispositivo virtual, se permite un despliegue rápido; en algunos casos, en menos de una hora.
- Para facilitar instalaciones rápidas con el dispositivo virtual OVA, puede seleccionar el despliegue automático del sistema para la mayoría de tamaños de sistema. Simplemente proporcione credenciales de vCenter y desplegaremos todas las máquinas virtuales para el sistema sin intervención manual. Esta innovación minimizará sus costes de mano de obra y tiempo.

Nota La plantilla OVA crea dos NIC virtuales para cada máquina virtual. Sin embargo, solo las máquinas virtuales de administración usan ambas NIC virtuales. Para el resto de máquinas virtuales de Cisco WebEx Meetings Server (CWMS), solo se utiliza una NIC virtual y se desconecta la otra.

- CWMS requiere la ejecución de VMware ESXi o la imagen ISO de Cisco instalable de VMware ESXi correspondiente. Estas dos ediciones contienen los controladores necesarios para admitir los servidores UCS de Cisco que CWMS requiere. Para obtener más información, consulte http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/OL_26617.pdf.

Fácil recuperación de errores de sistema

Si el cambio no satisface sus expectativas, utilizando VMware Data Recovery puede invertir cambios que afectan al sistema rápidamente y sin necesidad de volver a desplegar el sistema.

Consideraciones de vSphere

Tenga en cuenta las siguientes consideraciones:

- Puede mover la máquina virtual a otro host ESXi. No obstante, debe conservar el diseño de las máquinas virtuales en el nuevo host ESXi. En otras palabras, si desea mover una máquina virtual multimedia que corresida con una máquina virtual Web, deberá moverla a otro host ESXi (donde sea la única máquina virtual) o moverla a una que ya posea un host ESXi que ya tenga una máquina virtual Web.

Nota Su host ESXi de destino debe cumplir los mismos requisitos del sistema que el host ESXi de origen.

Las siguientes funciones de VMware no son compatibles con CWMS:

- VMotion y Storage VMotion (aunque puede mover sus máquinas virtuales, es posible que no pueda hacerlo utilizando estas herramientas).
- VMware Distributed Resource Schedule (DRS)
- Alta disponibilidad (HA) de vSphere
- Agrupación en clústeres y uso compartido de recursos de vSphere
- Clonación de una máquina virtual

Métodos recomendados de vSphere

- Recomendamos que no utilice instantáneas de máquinas virtuales. Si decide utilizar instantáneas, después de confirmar los cambios en el sistema, asigne las instantáneas o elimínelas lo antes posible. Si conserva una instantánea durante un período de tiempo, el rendimiento se reducirá de forma importante.
- Para entornos SAN, despliegue las imágenes de disco a un SAN con números IOP altos.

  Para un sistema de 800 usuarios, la IOPS media en un despliegue de OVA es de 506 (la IOPS máxima es de 855) para la máquina virtual de administración y de 475 (la IOPS máxima es de 652) para una

máquina virtual multimedia. Una vez que estas máquinas virtuales se hayan creado y encendido, podrá escribir el URL (que distingue entre mayúsculas y minúsculas) y continuar el despliegue del sistema en un explorador web. La IOPS media de un sistema principal es de 108 (la IOPS máxima es de 1558) y la de un sistema secundario es de 163 (la IOPS máxima es de 1736).

- Compruebe que existe espacio libre suficiente en su SAN. Las instantáneas se almacenan en el mismo SAN.
- Despliegue una red de 10 GB para el despliegue más rápido y ancho de banda para el crecimiento futuro.
- Recomendamos que gestione todas las máquinas virtuales utilizando el mismo vCenter. Esto facilita la recuperación en caso de necesidad de recuperar el sistema.

Para obtener más información sobre el ancho de banda de red, consulte Requisitos de ancho de banda de red, en la página 57.

Requisitos del servidor vCenter

Además de vSphere, también se necesita vCenter Server.

- Para desplegar este dispositivo virtual, también debe desplegar vCenter para desplegar y gestionar las máquinas virtuales en el sistema. Este producto no funcionará sin vCenter Server.
- Cisco recomienda realizar copias de seguridad e instantáneas del sistema antes de realizar operaciones que produzcan un impacto en el sistema. Crear copias de seguridad le permite deshacer los cambios en caso de que la actualización no cumpla sus expectativas. Puede automatizar las copias de seguridad y las instantáneas utilizando vCenter
- CWMS es compatible con vSphere Standard Edition.

vSphere Edition para sistemas de 800 y 2000 usuarios

- Los sistemas de 800 y 2000 usuarios constan de máquinas virtuales que requieren entre 30 y 40 vCPU. Estas máquinas virtuales utilizan estas vCPU para realizar tareas muy intensas, como calcular codificación o decodificación SSL, mezclar flujos de audio, etc.

  Para obtener información completa acerca de los requisitos de vCPU, consulte Recursos consumidos por Cisco WebEx Meetings Server y el host ESXi, en la página 11.
- Como mínimo, debe adquirir la edición vSphere 5.0 Enterprise Plus o la edición vSphere 5.1 Enterprise, ya que las ediciones inferiores no son compatibles con el número de vCPU necesarias.

IOPS y rendimiento del sistema de almacenamiento

Máximo previsto de IOPS y rendimiento

En la tabla siguiente se muestran los valores máximos previstos de IOPS y de rendimiento para la carga máxima en el sistema para una sola máquina virtual.

Tamaño del sistema	Máquina virtual	Máximo de operaciones de entrada/salida (IOPS)	Máximo de megabytes leídos por segundo	Máximo de megabytes escritos por segundo
Sistema de 50 usuarios	Admin	450	1	15
	DMZ	70	0,3	0,3
Sistema de 250 usuarios	Admin	1400	1	25
	Multimedia	150	1	10
	DMZ	110	0,4	0,6
Sistema de 800 usuarios	Admin	1400	3	50
	Multimedia	300	1	30
	DMZ	150	1	1,5
Sistema de 2000 usuarios	Admin	1600	2,5	60
	Multimedia	300	1	25
	Web	200	3	1,5
	DMZ	200	1,5	3

IOPS para rearranque del sistema para un sistema de 2000 usuarios

La tabla siguiente muestra información de IOPS para un sistema de 2000 usuarios para el proceso de arranque (rearranque).

Máquinas virtuales en un sistema de 2000 usuarios	IOPS para arranque del sistema (rearranque)	IOPS para actualización menor
Admin	2300	3000
Multimedia	2000	2000
Web	1500	2000
Web	1000	2000

IOPS para copia de seguridad para un sistema de 2000 usuarios

En la tabla siguiente se muestra información de IOPS para un sistema de 2000 usuarios para una copia de seguridad realizada fuera del horario de oficina.

Máquina virtual de administración para un sistema de 2000 usuarios	IOPS para copia de seguridad	Máximo de megabytes leídos por segundo	Máximo de megabytes escritos por segundo
Copia de seguridad de 1 GB	2000	220	300
Copia de seguridad de 12 GB	5000	320	600

Instalación de VMware vSphere ESXi y configuración de almacenamiento

Cisco WebEx Meetings Server es una solución basada en software. No es un paquete combinado de software y hardware. Usted elige qué plataformas de hardware desea adquirir y habilitar, siempre que el hardware iguale o supere los requisitos de CPU, memoria y almacenamiento.

Puede desplegar Cisco WebEx Meetings Server en los servidores UCS de Cisco que cumplen nuestras especificaciones mínimas. O puede optar por desplegar este producto en otros servidores UCS más modernos y de mayor calidad que superen nuestras especificaciones mínimas.

Tiene a su disposición varios controladores RAID y diversas opciones de red. Puede optar por usar almacenamiento SAN en lugar de RAID local. No proporcionamos información detallada acerca de cada tipo de configuración de almacenamiento que elija.

Sin embargo, dado que Cisco WebEx Meetings Server se despliega en los servidores UCS de Cisco, consulte la *Guía RAID de servidores UCS de Cisco* en http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/raid/configuration/guide/RAID_GUIDE.html.

- Para instalar VMware vSphere ESXi en un servidor UCS back de la serie B, consulte http://www.cisco.com/en/US/docs/unified_computing/ucs/os-install-guides/vmware/b_B-Series_VMware_Install.html.
- Para instalar VMware vSphere ESXi en un servidor UCS para montar en bastidor de la serie C, consulte http://www.cisco.com/en/US/docs/unified_computing/ucs/os-install-guides/vmware/b_C-Series_VMware_Install.html.

Consulte también docwiki.cisco.com/wiki/VMware_Tools para obtener más información.

Definición de la caché de escritura en un controlador RAID

Para obtener un rendimiento del sistema óptimo, deberá seleccionar la opción Escritura predeterminada en el controlador RAID. Puede establecer Escritura predeterminada en tres valores: *Write-Back con BBU*, *Write-Through* o *Siempre Write-Back*. Algunas directrices para seleccionar el valor apropiado para Escritura predeterminada en los servidores Cisco UCS Server son:

- **Write-Back con BBU**: utilice este valor si ha instalado una unidad de reserva de batería en el controlador RAID. En el supuesto de una pérdida de alimentación del sistema, la unidad de reserva de batería preserva el contenido de la memoria caché del controlador.

En el supuesto de que falle la unidad de reserva de batería o que pase a estar sin conexión en un ciclo de formación, el valor Write-Back con BBU adopta automáticamente el valor de caché **Write-Through**. Sin una unidad de reserva de batería en funcionamiento, el valor Write-Through es más seguro, aunque es posible que advierta alguna degradación en el rendimiento del subsistema de E/S de la máquina host.

- **Write-through**: utilice este valor y active la caché explícitamente (mediante la opción Caché de disco) si necesita extraer la unidad de reserva de batería para reparaciones. Este valor le proporcionará un mejor rendimiento, pero no un rendimiento óptimo. Después de sustituir la batería anómala, podrá devolver sin problemas el valor de Escritura predeterminada al modo Write-back con BBU.
- **Siempre Write-back**: utilice este valor si el organizador que alberga el controlador RAID está conectado a una unidad de sistema de alimentación ininterrumpida.

Entrada en reuniones

La experiencia de usuario final con Cisco WebEx Meetings Server es la de un sitio web, donde los usuarios acceden para planificar y unirse a reuniones. Este sitio web incluye elementos de conferencia en tiempo real que facilitan las reuniones en línea. Los usuarios pueden unirse a las reuniones a través de un explorador o a través de un cliente en sus escritorios.

Para obtener información completa sobre la experiencia del usuario final, inicie sesión en el sitio de WebEx y seleccione **Ayuda**.

Usuarios de Windows

En el siguiente supuesto se propone que un usuario tiene privilegios de administrador de Windows en su PC suficientes para permitirles unirse a reuniones de WebEx. Si no es el caso, los administradores del sistema pueden integrar el cliente de la aplicación WebEx Meetings en los escritorios de los usuarios utilizando un software de gestión de escritorio estándar como IBM Tivoli. Consulte Aplicaciones de despliegue masivo y descarga

- Para Microsoft Internet Explorer, los usuarios pueden instalar un control ActiveX o un complemento de Java, descargar el instalador de la aplicación WebEx Meetings, o ejecutar la aplicación en una carpeta de sistema temporal (como TFS). La primera vez que el usuario se une a una reunión, el software de cliente se descarga e instala automáticamente.
- Para Google Crome y Mozilla Firefox, los usuarios pueden instalar un complemento de Java, descargar la aplicación WebEx Meetings o ejecutar la aplicación en una carpeta de sistema temporal. El software del cliente se descarga y se instala automáticamente la primera vez que el usuario se une a una reunión.

No es necesario cambiar el instalador de ActiveX, el complemento de Java, el instalador de aplicación de WebEx Meetings ni los ajustes de TFS.

Usuarios de Mac

- Si Java está activado (Java está desactivado de forma predeterminada en Mac OS X Lion (versión 10.7) y OS X Mountain Lion (versión 10.8), el software del cliente se descarga y se instala automáticamente la primera vez que un usuario se une a una reunión.
- Si el Java está deshabilitado, el usuario puede descargar e instalar la aplicación WebEx Meetings.

Usuarios de sistemas con varios centros de datos

Si su sitio de WebEx utiliza certificados autofirmados en lugar de certificados de una entidad emisora de certificados conocida, después de que su centro de datos se una a otro centro de datos, los usuarios tienen que instalar un certificado para cada centro de datos en el almacén de Entidades de certificación raíz de confianza antes de iniciar una reunión o unirse a ella.

Uso de los navegadores Chrome y FireFox

Si utiliza Chrome 32 y posterior o Firefox 27[17]y posterior, es posible vea un indicador para instalar un complemento de Cisco WebEx. Seleccione **Descargar** y siga las instrucciones para instalar el complemento necesario.

Nota Después de instalar el complemento, es posible que tenga que activarlo.

- Si está utilizando Chrome, seleccione el icono del complemento que aparece en la parte superior derecha de la página, marque la opción **Permitir siempre complementos...** y seleccione **Aceptar**.
- Si está utilizando Firefox, seleccione el icono de complemento que aparece al principio de su URL (antes de https:) Seleccione **Permitir y recordar**.

Si la reunión no se inicia automáticamente, actualice la página.

Si utiliza el navegador Chrome 38 y posteriores para iniciar una reunión de WebEx o reproducir una grabación de WebEx, es posible que la primera vez se le pida realizar una instalación, para agregar la extensión de Cisco WebEx al navegador Chrome:

1. Seleccione **Agregar WebEx a Chrome**.
2. Seleccione **Gratuito** en el diálogo de extensión de Cisco WebEx.
3. Seleccione **Agregar** para agregar la extensión de Cisco WebEx al navegador Chrome.
4. Abra el archivo Cisco_WebEx_Add-on.exe y seleccione **Ejecutar**.
5. Cuando la instalación termina, la página se renueva. Si la reunión no se inicia automáticamente, actualice la página.

17 Las versiones exactas de Chrome y Firefox que están afectadas por esta política no se han finalizado en el momento de la publicación de este documento.

CAPÍTULO 3

Topología de redes para el sistema

En este capítulo se describen las distintas topologías de red compatibles para este producto, incluidas las ventajas y desventajas de cada una. Seleccione la que mejor se ajuste a sus necesidades y al despliegue de red.

Importante Si desea que los usuarios móviles asistan a reuniones, seleccione una topología de red que incluya la máquina virtual de proxy inverso de Internet. Debe desplegar el proxy inverso de Internet independientemente de cómo asista a las reuniones el usuario móvil.

Al utilizar una red de datos móvil, los usuarios con dispositivos móviles entran en la reunión a través de Internet al proxy inverso de Internet. Al utilizar una conexión Wi-Fi local, los usuarios con dispositivos móviles entran en la reunión a través del proxy inverso de Internet (topología de red de horizonte no dividido) o directamente a las máquinas virtuales internas (topología de red de horizonte dividido).

- Diseño de las máquinas virtuales en su red, página 48
- Diferentes tipos de topología de red del sistema, página 48
- Topología de red interna de proxy inverso de Internet (IRP), página 49
- Topología de red de horizonte no dividido, página 50
- Topología de red totalmente interna, página 51
- Topología de red de horizonte dividido, página 52
- Redundancia en despliegues de HA o MDC, página 54
- Consideraciones de red para el proxy inverso de Internet, página 55
- Requisitos de ancho de banda de red, página 57
- Equipos de NIC para agregación de ancho de banda, página 62
- Equilibrio de la carga, página 63

Diseño de las máquinas virtuales en su red

Cisco WebEx Meetings Server (CWMS) incluye dos grupos de máquinas virtuales: las máquinas virtuales internas y las máquinas virtuales de proxy inverso de Internet (IRP) opcionales. IRP se requiere para los sistemas donde se permite a usuarios externos organizar o asistir a reuniones por Internet sin utilizar VPN o utilizando dispositivos móviles CDMA. Sin IRP, solo los usuarios internos y de VPN pueden organizar o unirse a reuniones. Para obtener más información sobre IRP, consulte Consideraciones de red para el proxy inverso de Internet, en la página 55.

Máquinas virtuales internas

Las máquinas virtuales internas hacen referencia a la máquina virtual Admin y, si procede, a las máquinas virtuales multimedia y Web.

- Las máquinas virtuales internas *deben* estar en una única subred o VLAN común. Durante el despliegue del sistema, verá mensajes de error si sus asignaciones de dirección IP infringen esta regla. El diseño del sistema presupone que todas las máquinas virtuales internas, incluidas las máquinas virtuales de alta disponibilidad (HA), se conecten por medio de una LAN que ofrece un ancho de banda elevado, una pérdida de paquetes insignificante y una latencia inferior a 4 milisegundos

  La voz, los datos, el vídeo y SAN dependen del ancho de banda de red. Es fundamental desplegar una red que pueda gestionar la carga necesaria.

- Cisco recomienda colocar todas las máquinas virtuales en el mismo conmutador Ethernet. No obstante, al aprovisionar un sistema HA, recomendamos que despliegue dos conmutadores Ethernet para garantizar la redundancia de red.

- Si, por el contrario, decide colocar las máquinas virtuales en diferentes conmutadores Ethernet dentro del mismo centro de datos, entonces su red *debe cumplir* los requisitos específicos de ancho de banda y de latencia de red que se describen en Requisitos de ancho de banda de red, en la página 57. En esta situación, el troncal de conmutador-con-conmutador debe cumplir las características de red que la latencia L3 y el mismo rendimiento para un solo conmutador físico.

Si desea información adicional sobre los sistemas HA, consulte Redundancia en despliegues de HA o MDC, en la página 54.

Diferentes tipos de topología de red del sistema

Este producto admite las siguientes topologías de red:

- Topología de red interna de proxy inverso de Internet (IRP), en la página 49
- Topología de red de horizonte no dividido, en la página 50
- Topología de red totalmente interna, en la página 51
- Topología de red de horizonte dividido, en la página 52

Nota Si la topología de su red incluye proxies, debe cumplir requisitos específicos para que el proxy inverso de Internet funcione correctamente. Consulte la *Guía de solución de problemas de Cisco WebEx Meetings Server* para obtener información detallada.

Topología de red interna de proxy inverso de Internet (IRP)

En este apartado se describe la topología de red cuando todas las máquinas virtuales del sistema, incluida la máquina virtual de proxy inverso de Internet (IRP), están en la misma red interna.

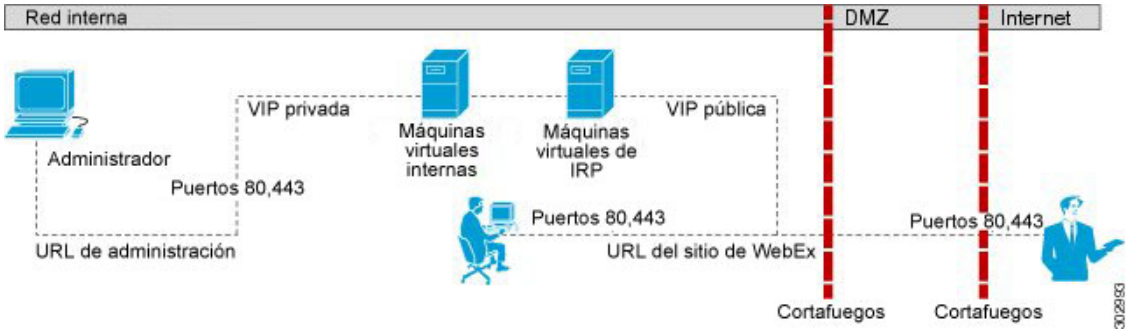
Esta configuración permite a los usuarios iniciar sesión y entrar en reuniones de forma segura desde Internet sin necesidad de una conexión VPN.

Si está utilizando el despliegue automático, los hosts ESXi de todas las máquinas virtuales (incluido el IRP) se deben gestionar desde el mismo VMware vCenter. Esta información de vCenter es necesaria durante un despliegue automático del sistema.

Nota Esta configuración admite acceso móvil.

Definirá la URL de administración, la URL del sitio de WebEx, la dirección VIP privada y la dirección VIP pública durante el despliegue de su sistema. Para obtener más información sobre estos conceptos y sobre cuándo tendrá que proporcionarlos, consulte la sección Instalación y de la *Guía de administración de Cisco WebEx Meetings Server*.

Este es un diagrama de una topología de red IRP totalmente interna.



Para ver una lista completa del acceso de puerto necesario para este despliegue, consulte Acceso de puerto cuando las máquinas virtuales están en la red interna, en la página 90.

Ventajas de una topología de red IRP totalmente interna

En comparación con la topología de red de horizonte no dividido, no hay máquinas virtuales en la DMZ y el tráfico de red para los usuarios internos no está conectado a través de la DMZ para organizar o asistir a reuniones.

Desventajas de una topología de red IRP totalmente interna

El acceso público (permite a los usuarios externos acceder al sistema) requiere abrir puertos de entrada (80 y 443) directamente desde Internet a la red interna.

Para obtener más información sobre IRP, consulte Consideraciones de red para el proxy inverso de Internet, en la página 55 y Agregación de acceso público a su sistema utilizando IRP.

Topología de red de horizonte no dividido

En este apartado se describe la topología de red cuando se tiene un DNS de horizonte no dividido. Las máquinas virtuales de Internet (administración y, si procede, multimedia y web) se encuentran en la misma red interna, y el proxy inverso de Internet está en la red DMZ.

Nota Esta configuración permite a los usuarios iniciar sesión y entrar en reuniones de forma segura desde Internet sin necesidad de una conexión VPN.

Nota Esta configuración admite acceso móvil.

Para este producto, la principal diferencia entre una topología de red de horizonte dividido y no dividido es que, para un sistema de horizonte dividido los usuarios internos acceden a la URL del sitio de WebEx utilizando la dirección VIP privada. Los usuarios externos (fuera del cortafuegos) acceden a la URL del sitio de WebEx utilizando la dirección VIP pública. Para una red de horizonte no dividido, todos los usuarios (internos y externos) acceden a la URL del sitio de WebEx utilizando la dirección VIP pública.

Definirá la URL de administración, la URL del sitio de WebEx, la dirección VIP privada y la dirección VIP pública durante el despliegue de su sistema. Para obtener más información sobre estos conceptos y sobre cuándo tendrá que proporcionarlos, consulte la sección Instalación y de la *Guía de administración de Cisco WebEx Meetings Server*.

Este es un diagrama esquemático de una topología de red de horizonte no dividido.

Nota Para ver una lista completa del acceso de puerto necesario para este despliegue, consulte Acceso de puerto con un proxy inverso de Internet en la red DMZ, en la página 91.

Ventajas de una topología de red de horizonte no dividido

- Control estricto del tráfico que entra y sale de una red.
- Soluciona los requisitos de red DNS sencillos y más comunes.

Desventajas de una topología de red de horizonte no dividido

- Configuración compleja, pero no tanto como la topología de horizonte dividido.
- El tráfico interno se direcciona a la red DMZ. Todo el tráfico de red de Internet, así como el interior (red privada) irá al proxy inverso de Internet en la red DMZ y, a continuación, volverá a las máquinas virtuales internas.
- Necesita abrir más puertos en el cortafuegos entre la red interna y la DMZ, en comparación con la topología de red completamente interna.
- El despliegue automático del sistema (solo para sistemas de 50, 250 y 800 usuarios) requiere una configuración más detallada en vCenter.
- De las tres topologías de red, esta configuración afecta más al rendimiento de la red, puesto que todas las reuniones se cargan a través del proxy inverso de Internet. Puesto que hay varias saltos, también se afecta a la latencia de red.

Nota Consulte Requisitos de ancho de banda de red, en la página 57 para obtener información detallada acerca de los requisitos de velocidad de las NIC para despliegues de DNS de horizonte no dividido.

Topología de red totalmente interna

En este apartado se describe la topología de red cuando todas las máquinas virtuales del sistema están en la misma red interna. No hay ningún acceso público; sólo los usuarios internos y de VPN pueden organizar o unirse a reuniones.

Nota Si está utilizando el despliegue automático, los hosts ESXi de todas las máquinas virtuales deben estar gestionados desde el mismo VMware vCenter. Esta información de vCenter es necesaria durante un despliegue automático del sistema.

Nota Esta configuración no admite acceso móvil.

Definirá la URL de administración, la URL del sitio de WebEx, la dirección VIP privada y la dirección VIP pública durante el despliegue de su sistema. Para obtener más información sobre estos conceptos y sobre cuándo tendrá que proporcionarlos, consulte la sección Instalación de la *Guía de administración de Cisco WebEx Meetings Server*.

Este es un diagrama esquemático de una topología de red totalmente interna.

Ventajas de una topología de red totalmente interna

- Proporciona una latencia inferior, ya que hay menos saltos de red entre las máquinas virtuales.

Desventajas de una topología de red totalmente interna

- No hay ningún acceso público (permite a los usuarios externos acceder al sistema) y ningún acceso para usuarios con dispositivos móviles.

Topología de red de horizonte dividido

En este apartado se describe la topología de red cuando se tiene un DNS de horizonte dividido. Las máquinas virtuales de Internet (administración y, si procede, multimedia y web) se encuentran en la misma red interna, y el proxy inverso de Internet está en la red DMZ.

Nota Esta configuración permite a los usuarios iniciar sesión y entrar en reuniones de forma segura desde Internet sin necesidad de una conexión VPN.

Nota Esta configuración solo admite acceso móvil desde una red de IP pública (Internet). El acceso móvil no está permitido en una red interna (Intranet).

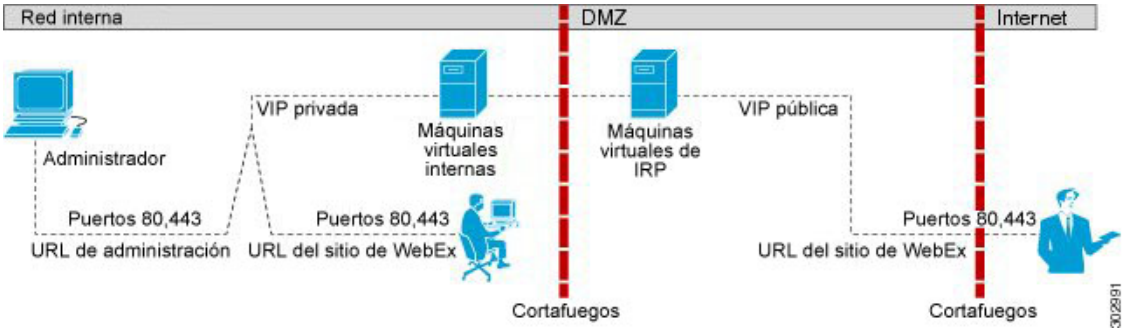
En un despliegue de horizonte dividido, el tráfico procedente de Internet (incluidos los usuarios con dispositivos móviles que utilizan una red de datos móvil) va al proxy inverso de Internet. El tráfico de origen interno (incluidos los usuarios con dispositivos móviles que utilizan una Wi-Fi local) va directamente a las máquinas virtuales internas.

Para este producto, la principal diferencia entre una topología de red de horizonte dividido y no dividido es que, para un sistema de horizonte dividido los usuarios internos acceden a la URL del sitio de WebEx utilizando la dirección VIP privada. Los usuarios externos (fuera del cortafuegos) acceden a la URL del sitio de WebEx utilizando la dirección VIP pública. Para una red de horizonte no dividido, todos los usuarios (internos y externos) acceden a la URL del sitio de WebEx utilizando la dirección VIP pública.

Definirá la URL de administración, la URL del sitio de WebEx, la dirección VIP privada y la dirección VIP pública durante el despliegue de su sistema. Para obtener más información sobre estos conceptos y sobre

cuándo tendrá que proporcionarlos, consulte la sección Instalación y de la *Guía de administración de Cisco WebEx Meetings Server*.

Este es un diagrama esquemático de una topología de red de horizonte dividido.



Nota Para ver una lista completa del acceso de puerto necesario para este despliegue, consulte Acceso de puerto con un proxy inverso de Internet en la red DMZ, en la página 91.

Ventajas de una topología de red de horizonte dividido

- Control estricto del tráfico que entra y sale de una red.
- Hay una separación del tráfico de red que atraviesa el sistema, lo que permite una propagación de la carga más distribuida.

  El tráfico que procede de Internet irá al proxy inverso de Internet. El tráfico procedente del interior (red privada) irá directamente a las máquinas virtuales internas (Admin y, si procede, multimedia y web).
- La latencia de red y el rendimiento son mejores que un DNS de horizonte no dividido, pero peor que una topología de red interna.

Desventajas de una topología de red de horizonte dividido

- De las tres distintas topologías de red que existen, esta es la configuración más compleja.
- Requiere una correlación sofisticada de DNS.
- Necesita abrir más puertos en el cortafuegos entre la red interna y la DMZ, en comparación con la topología de red completamente interna.
- El despliegue automático del sistema (solo para sistemas de 50, 250 y 800 usuarios) requiere una configuración más detallada en vCenter.
- Debido a la redirección de web, para los usuarios internos, la URL del sitio de WebEx se sustituye con la URL que muestra el nombre de host de la máquina virtual que contiene los servicios web, así como las máquinas virtuales multimedia.

Consulte Requisitos de ancho de banda de red, en la página 57 para obtener información detallada acerca de los requisitos de velocidad de las NIC para despliegues de DNS de horizonte dividido.

Redundancia en despliegues de HA o MDC

La alta disponibilidad (HA) proporciona redundancias por medio de la conmutación por error de un sistema Cisco WebEx Meetings Server (CWMS) a un sistema HA CWMS de reserva en la misma ubicación física.

El entorno con varios centros de datos (MDC) de CWMS despliega varios centros de datos y luego los une en un solo sistema CWMS. La conmutación por error es similar a un sistema HA, a excepción de que los centros de datos del sistema MDC son centros iguales que prestan servicio a los usuarios por igual y no están limitados geográficamente. De hecho, el despliegue de varios centros de datos geográficamente cercanos a los usuarios mejora el rendimiento de la red. Un sistema CWMS no puede admitir tanto HA como MDC.

Las condiciones para la redundancia son:

- Las máquinas virtuales HA se deben localizar de forma conjunta en el mismo centro de datos que las máquinas virtuales principales. Todas estas máquinas virtuales deben estar en la misma VLAN o subred. Los requisitos de velocidad y latencia para la conectividad entre los componentes primarios y HA son los mismos que los que se han definido previamente para las máquinas virtuales primarias. La división de componentes principales y HA del sistema entre centros de datos no se admite.

  No es necesario que las máquinas virtuales MDC estén localizadas de forma conjunta en el mismo centro de datos.

- La conectividad entre todas las máquinas virtuales internas debe ser completamente redundante, de forma que el error de un conmutador o de un enlace de red no corte la conectividad entre los componentes principales y HA o MDC. Para conseguir esta redundancia, cada servidor host debe tener conexiones redundantes con varios conmutadores Ethernet.

- Las máquinas virtuales de proxy inverso de Internet (IRP) principales y de HA deben estar en una VLAN o subred común (normalmente, no la misma subred que las máquinas virtuales internas). La conectividad entre las máquinas virtuales de proxy inverso de Internet también debe ser completamente redundante, del mismo modo que las máquinas virtuales internas.

  Después de unir centros de datos en un sistema MDC, se puede configurar IRP en uno o varios centros de datos. Durante una unión, la configuración de IRP en el sistema CWMS y el centro de datos que se une al sistema CWMS debe coincidir. Durante una unión, todos los centros de datos ejecutan IRP o bien ninguno de los centros de datos ejecuta IRP.

La adición de un sistema HA o MDC no aumenta la capacidad total del sistema. Independientemente de que despliegue un sistema de 800 usuarios con HA o sin ella, la capacidad total del sistema sigue siendo la misma; el número máximo de conexiones de audio simultáneas es de 800.

El sistema HA o MDC engloba máquinas virtuales redundantes para cada tipo de máquina virtual de su implementación. (Para obtener una descripción de cada tipo de máquina virtual, consulte Máquinas virtuales en el sistema, en la página 8). Por ejemplo:

- Un sistema de 50 usuarios consta de una máquina virtual de administración y, opcionalmente, una máquina virtual de proxy inverso de Internet (IRP) para el acceso público. Si añade un sistema HA (MDC no está disponible) , el sistema de 50 usuarios combinado consta de dos máquinas virtuales de administración y dos máquinas virtuales IRP.

- Un sistema principal de 250 u 800 usuarios consta de una máquina virtual de administración, una máquina virtual multimedia y, opcionalmente, una máquina virtual IRP. Si añade un sistema HA o MDC, el sistema de 250 u 800 usuarios combinado consta de dos máquinas virtuales de administración, dos máquinas virtuales multimedia y dos máquinas virtuales IRP.

- Un sistema principal de 2000 usuarios consta de una máquina virtual de administración, tres máquinas virtuales multimedia, dos máquinas virtuales Web y, opcionalmente, una máquina virtual IRP. Si añade un sistema HA o MDC, el sistema de 2000 usuarios combinado consta de dos máquinas virtuales de administración, cuatro (tres más una redundante) máquinas virtuales multimedia, tres (dos más una redundante) máquinas virtuales web y dos máquinas virtuales IRP.

En un sistema HA o MDC, se comparte la dirección VIP pública y la privada con el sistema principal. (la dirección VIP pública y la privada son diferentes y no se comparten). Cuando una máquina virtual no funciona, la otra máquina virtual utiliza la misma dirección VIP. Debido a este comportamiento, el error de una máquina virtual es casi completamente transparente para los usuarios finales (ya que las reuniones continuarán), sin realizar solicitudes inusuales en la infraestructura DNS. No obstante, una dirección VIP compartida solo se puede implementar en un segmento de red individual o VLAN; la división de una VLAN entre dos centros de datos crea diversos problemas.

Necesitamos que la conectividad entre las máquinas virtuales internas primaria y HA esté dentro del mismo centro de datos, reduciendo enormemente el problema de distinguir entre un fallo de una máquina virtual y un fallo de la red. Permitir una red dividida podría provocar la división de conexiones de reuniones y conflictos en las actualizaciones de bases de datos. Resulta más práctico construir un verdadero segmento de red HA dentro de un único centro de datos, en lugar de entre varios centros de datos.

En un sistema MDC, los datos se replican entre centros de datos (a excepción del Gestor de licencias). Por lo tanto si un centro de datos queda fuera de servicio o se pierde la conectividad de red, el centro de datos subsistente sigue prestando servicio a los usuarios independientemente de la ubicación geográfica.

La mejor forma de crear un sistema tolerante a errores es que la mayoría de los componentes del sistema funcionen como “todos activos”. Sin embargo, determinados componentes clave, especialmente el servicio de base de datos, están “activos/en espera”. (Los servidores Web y los componentes multimedia del sistema HA dependen de los componentes del sistema principal). Cualquier latencia o interrupción de las conexiones genera retardos para los usuarios finales, especialmente al unirse a reuniones. La latencia entre componentes de servicio multimedia aumenta la latencia de audio y vídeo para algunos usuarios durante las reuniones. (Para Cisco WebEx Meetings Server, es aceptable 1 ms de latencia de red entre las máquinas virtuales internas. Para obtener información detallada, consulte Diseño de las máquinas virtuales en su red, en la página 48).

Consideraciones de red para el proxy inverso de Internet

Las máquinas virtuales de proxy inverso de Internet comparten los mismos requisitos de red generales que las máquinas virtuales internas. Para la configuración de DNS de horizonte dividido y de horizonte no dividido, las máquinas virtuales de proxy inverso de Internet se despliegan en la red DMZ y no en la red interna.

Restricción Incluso si los servidores UCS de Cisco están configurados con dos NIC, Cisco WebEx Meetings Server no admite que una tarjeta apunte a Internet, y la otra, a la intranet. Esta restricción se aplica independientemente de las asignaciones entre las NIC físicas y las virtuales que utilice vSphere (y el proxy inverso de Internet).

La máquina virtual de proxy inverso de Internet siempre se conecta a una sola VLAN externa, independientemente del número de NIC que utilice. Si utiliza varias NIC físicas, y están conectadas a conmutadores o enrutadores diferentes, sigue siendo necesario que las tarjetas estén conectadas a la misma VLAN.

Por tanto, no puede usar el proxy inverso de Internet para unir el tráfico entre dos segmentos de red distintos (uno que apunte a Internet, y el otro, a la intranet). La sección siguiente describe cómo puede lograr este objetivo.

Latencia entre máquinas virtuales internas y el proxy inverso de Internet

La latencia de ida y vuelta máxima aceptable en la ruta entre la NIC del proxy inverso de Internet y la NIC de cualquiera de las máquinas virtuales internas debe establecerse en menos de 4 ms. Un exceso de latencia en esta ruta limitará el ancho de banda utilizable por los usuarios finales para audio, vídeo y uso compartido de escritorio. Si la latencia se incrementa de 4 a 8 ms, por ejemplo, el ancho de banda utilizable se reducirá a la mitad, y el rendimiento se degradará progresivamente a medida que se incremente la latencia.

Nota El límite de latencia de 4 ms no se aplica a la ruta entre cualquiera de los componentes de Cisco WebEx Meetings Server y los terminales de los usuarios finales.

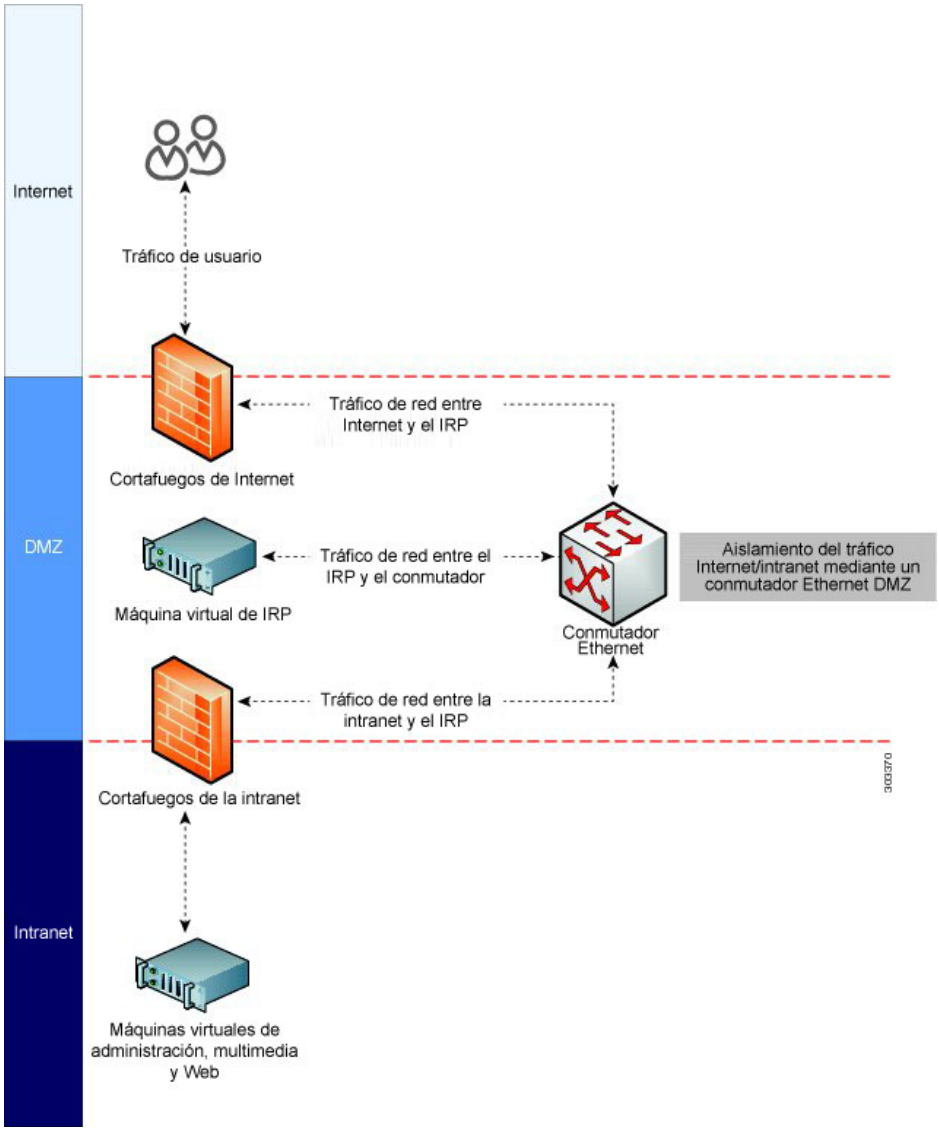
Nota Pueden experimentarse demoras potencialmente graves en las conexiones de usuario final que pasen a través del proxy inverso de Internet (IRP) de Cisco WebEx Meetings Server cuando la latencia supera los 4 ms entre el IRP y las máquinas virtuales internas.

Aislamiento del tráfico de red

Puede configurar el aislamiento del tráfico de red entre Internet y su red interna mediante un conmutador Ethernet DMZ. El siguiente procedimiento y diagrama ilustran un ejemplo:

1. Conecte el proxy inverso de Internet a un conmutador o enrutador de cabecera y utilice ese conmutador o enrutador para separar el tráfico de Internet del de la intranet.
2. Una vez que el conmutador o enrutador divida el tráfico, a continuación, puede llevar esos dos patrones de tráfico a dos puertos físicos separados en el conmutador o enrutador. Un puerto apuntará a Internet, y el otro, a la intranet.

Este es un diagrama de una topología de red de muestra:



Para obtener información acerca de los requisitos de ancho de banda de red, consulte Requisitos de ancho de banda de red, en la página 57.

Requisitos de ancho de banda de red

Esta sección describe los requisitos de ancho de banda para los sistemas de 50, 250, 800 y 2000 usuarios. Cumplir los requisitos de ancho de banda descritos en la sección proporcionará una experiencia de usuario final de calidad a los usuarios que organicen y asistan a reuniones de WebEx, y les ayudará a garantizar que la red pueda soportar las demandas de tráfico derivadas del uso compartido de la Web, el audio y el vídeo.

Estimación del ancho de banda para sesiones de usuario final

Es importante estimar el ancho de banda de red que soportará las demandas de tráfico de vídeo, audio, y uso compartido de la Web según el tamaño de su sistema. Los requisitos de ancho de banda para este producto

son básicamente los mismos que para los servicios de nube de Cisco WebEx. Si desea optimizar el aprovisionamiento de su red, puede obtener información sobre el uso de ancho de banda de los servicios de nube de Cisco WebEx en el Documento técnico sobre ancho de banda de red de WebEx.

La información de la tabla siguiente muestra el ancho de banda esperado para el uso compartido de la Web, el audio y el vídeo.

Componente de la reunión de WebEx	Ancho de banda agregado de la sesión del usuario final
Vídeo (360p + 6 miniaturas)	1,5 MB/s
Audio	0,1 MB/s
Uso compartido de la Web (Este valor asume que usted pasa una diapositiva cada 30 segundos).	0,6 MB/s
Ancho de banda máximo total	2,2 MB/s

Aunque 2,2 MB/s es el máximo ancho de banda estimado para la conexión de un solo usuario, Cisco recomienda utilizar el máximo ancho de banda estimado de 1,5 MB/s a la hora de calcular los requisitos de ancho de banda. Dado que sólo la mitad del número máximo de usuarios pueden emplear vídeo, audio y uso compartido de la Web mientras los usuarios restantes utilizan sólo audio y uso compartido de la Web, esto produce un ancho de banda promedio de aproximadamente 1,5 MB/s por conexión de usuario.

Si consulta el *Documento técnico sobre ancho de banda de red de WebEx*, notará que los valores del ancho de banda de la tabla anterior se basan en las condiciones de tráfico más desfavorables. La utilización media del ancho de banda es *mucho* menor, pero Cisco recomienda utilizar las cifras correspondientes a las peores condiciones por las siguientes razones:

- Usar las cifras correspondientes a las peores condiciones para su cálculo debería ayudarle a proporcionar el ancho de banda necesario para evitar que disminuya la calidad de la experiencia de usuario como resultado de un uso intensivo.
- Cisco WebEx Meetings Server envía los mismos datos de forma simultánea a todos los participantes de una reunión. Cuando un organizador de WebEx pasa una página de una presentación, una imagen de esa página (posiblemente compuesta de varios megabytes) se envía por separado a cada terminal, al mismo tiempo y lo más rápidamente posible.

Ancho de banda en rutas de red

Utilice el siguiente procedimiento para determinar el ancho de banda necesario en varias rutas de red.

1. Determine el ancho de banda medio de la sesión de un usuario utilizando la tabla proporcionada en la sección anterior.
2. Determine el número máximo de usuarios que espera que se conecten simultáneamente a través de dicho enlace.
3. Multiplique el ancho de banda total por el número máximo de usuarios.

Ejemplos de escenarios:

- Si espera que se conecten un máximo de 100 usuarios de forma simultánea desde Internet, probablemente necesitará 1,5 MB/s x 100 = 150 MB/s de ancho de banda disponible en su conexión del ISP y a través de su cortafuegos externo al proxy inverso de Internet. Para obtener detalles acerca del proxy inverso de Internet, consulte Consideraciones de red para el proxy inverso de Internet, en la página 55
- Imagine que tiene un sistema de 2000 usuarios donde todas las conexiones se realizan a través del proxy inverso de Internet. En este escenario, necesita presuponer que el tráfico para la totalidad de los 2000 usuarios se conectará al proxy inverso de Internet y, a continuación, desde el proxy inverso de Internet hasta las máquinas virtuales internas. El ancho de banda agregado que entra en el proxy inverso de Internet de otras partes de la red será aproximadamente de 2000 x 1,5 Mb/s = 3 Gb/s. Para obtener detalles acerca del horizonte no dividido, consulte Topología de red de horizonte no dividido, en la página 50.

Nota Esos mismos 3 GB/s de tráfico entran y salen a través del proxy inverso de Internet, obligando a la NIC del proxy inverso de Internet a gestionar 6 GB/s de tráfico de usuarios. Consulte la sección siguiente para obtener más información acerca de los requisitos de ancho de banda para la NIC en el proxy inverso de Internet.

- Imagine que tiene un sistema de 2000 usuarios en un despliegue de DNS de horizonte dividido. En este escenario, sus usuarios de Internet se conectarán al proxy inverso de Internet mientras que los usuarios de la intranet se conectarán directamente a las máquinas virtuales internas. Supongamos que el 10% de sus usuarios se conectan a sus reuniones mediante Internet frente a un 90% de usuarios que se conectan a sus reuniones a través de la intranet. El resultado es que el ancho de banda agregado que entra en el proxy inverso de Internet ahora será aproximadamente de 300 MB/s (el 10% de 2000 usuarios por 1,5 MB/s es igual a 300 MB/S). Si esos mismos 300 MB/s de tráfico pasan desde el proxy inverso de Internet, puede que se exija a la NIC del proxy inverso de Internet que gestione 600 MB/s de tráfico de usuarios. Este es un requisito de ancho de banda drásticamente inferior al que habría con un despliegue de DNS de horizonte no dividido, descrito en el escenario anterior. Esta reducción en el tráfico de red afecta directamente a las recomendaciones sobre velocidad de la interfaz del conmutador o de la NIC (consulte la sección siguiente), lo que puede permitirle desplegar NICs de 1 GB más económicas en el servidor UCS de Cisco para el proxy inverso de Internet o la infraestructura de conmutador Ethernet de 1 Gigabit en la red DMZ. Para obtener información detallada acerca del horizonte dividido, consulte Topología de red de horizonte dividido, en la página 52.

Nota Puede ser necesario desplegar NICs Ethernet de 1 Gigabit para equipos de NIC si el uso del proxy inverso de Internet es ligeramente cercano al umbral de los 1000 MB/s.

Consulte Equipos de NIC para agregación de ancho de banda, en la página 62, para obtener más detalles.

Ancho de banda en las interfaces de red de Cisco WebEx Meetings Server

Para interfaces directas entre su arquitectura de conmutación y su sistema, le recomendamos que las NIC de su interfaz tengan las velocidades máximas que se muestran en la siguiente tabla. Estas velocidades se aplican a la conectividad entre los servidores UCS de Cisco y los puertos de los conmutadores de cabecera tan solo en su infraestructura de conmutación local. Estas son las velocidades recomendadas necesarias para soportar los requisitos de tráfico en el peor de los casos.

Capacidad del sistema	Velocidad de la interfaz del conmutador o de la NIC
Sistema de 50 usuarios	1 GB/s
Sistema de 250 usuarios	1 GB/s
Sistema de 800 usuarios	10 GB/s[18][19]
Sistema de 2000 usuarios	10 GB/s[20]

18 Opcionalmente, puede optar por reducir los costes de la infraestructura de red desplegando equipos de NIC que utilicen tarjetas Ethernet de dos o más Gigabits en el servidor UCS y equipos de NIC en el conmutador de cabecera.

19 Para sistemas de 800 usuarios, si su despliegue está utilizando almacenamiento DAS interno, puede optar por reducir los costes de infraestructura de red desplegando NIC Teaming mediante dos o más NIC Gigabit Ethernet en el servidor UCS y NIC Teaming en el conmutador de cabecera. Sin embargo, si su despliegue está utilizando el almacenamiento SAN o NAS, necesitará un enlace 10 Gigabit Ethernet.

20 Si tiene un despliegue de DNS de horizonte no dividido, el requisito de 10 GB/s pertenece al proxy inverso de Internet (IRP) y a las máquinas virtuales internas. Si tiene un despliegue de DNS de horizonte dividido, podrá reducir las exigencias de la infraestructura de red en su IRP (y en la red DMZ), lo que puede permitirle desplegar NICs de 1 GB/s más económicas en el servidor UCS de Cisco para el proxy inverso de Internet, o una infraestructura de conmutador Ethernet de 1 Gigabit en la red DMZ, tal como se describe en la sección "Ancho de banda en rutas de red". Sin embargo, el requisito de velocidad de 10 GB/s se mantiene para las máquinas virtuales internas (y la red interna).

Consulte la siguiente sección titulada "Consideraciones sobre el ancho de banda para despliegues de DNS de horizonte dividido" para obtener más información acerca del uso de NIC de 1 GB/s y conmutadores Ethernet para un despliegue de DNS de horizonte dividido.

Supuestos para los cálculos de velocidad de las NIC:

- Para calcular las velocidades de las NIC que se muestran en la tabla anterior, se ha utilizado el ancho de banda agregado de la sesión de usuario final (1,5 MB/s).
- El control de tráfico entre máquinas virtuales debe estar libre de congestión. Eso se aplica especialmente a los sistemas de 2000 usuarios y a cualquier sistema con alta disponibilidad. Una congestión grave en los enlaces de una máquina virtual puede causar inestabilidad en el sistema y la consiguiente interrupción del servicio.
- Las conexiones al almacenamiento NAS, utilizadas para la grabación y la copia de seguridad de bases de datos, no deben estar congestionadas.
- El gasto de los protocolos y las ineficiencias de despliegue darán lugar a un ancho de banda de enlace utilizable que será bastante inferior a las etiquetas de velocidad de 1 GB/s o 10 GB/s.
- Si un gran porcentaje de su tráfico atraviesa el proxy inverso de Internet cuando los usuarios inician sesión en las reuniones, es necesario recordar que la conexión de cada usuario pasa dos veces por la NIC del proxy inverso de Internet (al entrar y al salir). Tomando como ejemplo el sistema de 2000 usuarios, esto significa que puede que se obligue a la NIC del proxy inverso de Internet a gestionar 6 GB/s de tráfico de usuarios (2000 usuarios por 1,5 MB/s es igual a 3 GB/s, multiplicado por dos, por el tráfico entrante y saliente, es igual a 6 GB/s).

Siendo conservadores, pedimos que las conexiones locales no supongan más del 60% para el tráfico medio de los usuarios finales, dejando el 40% restante disponible para otros tráficos, ráfagas de tráfico inusuales, y gasto de la red. Tomando como ejemplo el sistema de 800 usuarios, calculamos el tráfico de los usuarios finales en 1,2 GB/s para las máquinas virtuales de administración y multimedia, y en 2,4 GB/s para la máquina virtual de proxy inverso de Internet. Aplicando la regla del 60 %, queremos que la NIC sea capaz de gestionar 2 GB/s para las máquinas virtuales de administración y multimedia (el tráfico de usuarios estimado de 1,2

GB/s para las máquinas virtuales de administración y multimedia dividido entre el 60 % del consumo de ancho de banda normal estimado es igual a 2,0 GB/s) y 4 GB/s para la máquina virtual de proxy inverso de Internet.

Nota Las velocidades de NIC que se muestran en la tabla anterior no explican el ancho de banda utilizado para acceder al almacenamiento SAN. Si se utiliza Canal de fibra en Ethernet (FCoE) para una conexión SAN, debería proporcionarse para usar una interfaz de red independiente.

Consideraciones sobre el ancho de banda para despliegues de DNS de horizonte dividido

Con un despliegue de DNS de horizonte dividido, algunos de sus usuarios se conectarán a las reuniones desde Internet y ese tráfico atravesará el proxy inverso de Internet, mientras que la mayoría de los usuarios que estén en la red interna se conectarán a las reuniones sin atravesar el proxy inverso de Internet. Con un despliegue de DNS de horizonte dividido, si acelera su red y segmenta su tráfico de modo que la mayor parte del tráfico permanezca dentro de la red interna (en contraposición al que atraviesa el proxy inverso de Internet), tiene la posibilidad de utilizar equipos de NIC, tener una NIC de bajo coste (de 1 GB/s) en el proxy inverso de Internet, y hacer que la infraestructura de conmutación entre el proxy inverso de Internet e Internet sea de 1 GB/s, o al menos inferior a los 10 GB/s recomendados, para un sistema de 2000 usuarios.

Por ejemplo, si una compañía tiene 100 usuarios que desean acceder a un sistema de 2000 puertos de usuario desde Internet simultáneamente, usted necesitaría un ancho de banda de 150 MB/s (1,5 MB/s de ancho de banda agregado por sesión de usuario * 100 usuarios = 150 MB/s). Esto implica que una infraestructura de red desde la red DMZ hasta el proxy inverso de Internet puede estar compuesta por conmutadores Ethernet de 1 GB/s, y la interfaz de NICs Ethernet en el proxy inverso de Internet puede ser de 1 GB/s, en contraposición al requisito de interfaz de 10 GB/s indicado. Incluso cuando se tiene en cuenta que el proxy inverso de Internet ve el doble de tráfico (lo que significa que su NIC tendría que gestionar 300 Mb/s de tráfico de los usuarios), aplicando la regla del 60 por ciento (lo que se explica en la sección "Ancho de banda en las interfaces de red de Cisco WebEx Meetings Server") se convierte en 500 Mb/s. Un enlace de 1 Gb/s sigue siendo suficiente, pero no sería suficiente si supusiéramos que hay 250 usuarios en lugar 100.

Nota La optimización del ancho de banda solo es aplicable para la NIC del proxy inverso de Internet en despliegues de DNS de horizonte dividido.

Para despliegues de DNS de horizonte no dividido, debe desplegar conmutadores Ethernet de 10 GB /s e interfaces de NICs Ethernet en el proxy inverso de Internet.

Requisitos de la red para varios centros de datos

Requisitos de un enlace de red entre dos centros de datos:

- Se garantiza un ancho de banda de 4,5 Mbps para gestionar las comunicaciones principales entre los centros de datos.
- Latencia inferior a 200 ms (tiempo de retardo de ida y vuelta).

Requisitos de red de los centros de datos para reuniones en cascada entre centros de datos:

- Todas las reuniones en cascada con audio y web requieren 0,16 Mbps.
- Todas las reuniones en cascada con vídeo de baja calidad a 180 p, audio y web requieren 0,66 Mbps.

- Todas las reuniones en cascada con vídeo de alta calidad a 360 p, audio y web requieren 1,20 Mbps.
- Latencia inferior a 200 ms (tiempo de retardo de ida y vuelta).

Por ejemplo, cuando, en el peor de los casos, se trate de un sistema de 2000 usuarios (se permite un máximo de 1000 reuniones para que se organicen en cascada). La mitad de ellas pueden admitir vídeo y la otra mitad, no:

- *Vídeo de alta calidad:* 500 x 1,2 + 500 x 0,16 = 680 Mbps
- *Vídeo de baja calidad:* 500 x 0,66 + 500 x 0,16 = 410 Mbps

Para sistemas de 800 usuarios:

- *Vídeo de alta calidad:* 680 / 2000 x 800 = 272 Mbps
- *Vídeo de baja calidad:* 410 / 2000 x 800 = 164 Mbps

Para sistemas de 250 usuarios:

- *Vídeo de alta calidad:* 680 / 2000 x 250 = 85 Mbps
- *Vídeo de baja calidad:* 410 / 2000 x 250 = 51,25 Mbps

Se podrá encontrar más información en http://www.cisco.com/c/en/us/products/conferencing/webex-meeting-center/white-paper-listing.html.

Equipos de NIC para agregación de ancho de banda

Configurar los equipos de tarjetas de interfaz de red (NIC) en sus servidores UCS que contengan el host ESXi con las máquinas virtuales internas ofrece dos ventajas: la carga de los equipos de NIC equilibra el tráfico de red entre las redes físicas y virtuales, y proporciona conmutación en caso de fallos de hardware o interrupciones de red. Además, para los despliegues en los que no esté disponible una infraestructura de 10 GB/s, es posible formar equipos de múltiples NIC de 1 GB/s para conseguir un resultado equivalente.

Nota Para obtener más información acerca de las velocidades necesarias de las NIC para distintos tamaños de sistema, consulte la sección "Ancho de banda en las interfaces de red de Cisco WebEx Meetings Server" en este capítulo.

Cisco es compatible con equipos de NIC para balanceo de carga de ancho de banda para sistemas de todos los tamaños –de 50, 250, 800 y 2000 usuarios–, pero es a aquellos clientes que estén intentando optimizar los costes de la red en un sistema de 800 usuarios a quienes les resultará más útil. Si su despliegue está utilizando un almacenamiento DAS interno, los requisitos del ancho de banda agregado a y desde los servidores UCS y los conmutadores de cabecera de Cisco para los sistemas de 800 usuarios, serán previsiblemente similares a los necesarios para utilizar NICs Ethernet Dual de 1 Gigabit (o NICs Ethernet Quad de 1 Gigabit en un sistema con HA) para que sean compatibles con los requisitos de tráfico más desfavorables, atenuando así la necesidad de proporcionar a los servidores UCS unas NIC Ethernet de 10 Gigabit (o de adquirir conmutadores de cabecera Ethernet de 10 Gigabit).

Nota Si el despliegue está utilizando almacenamiento SAN o NAS, los requisitos de ancho de banda agregado hasta y desde los servidores Cisco UCS y los conmutadores de cabecera para un sistema de 800 usuarios es Ethernet de 10 Gigabit.

Nota Para obtener información acerca de la habilitación de equipos de NIC en VMware, consulte la documentación de VMware en http://kb.vmware.com y busque "Equipos de NIC en ESXi/ESX".

Asumiendo el uso de conmutadores Ethernet e interfaces de red tradicionales, puede proporcionar redundancia mediante equipos de NIC y conmutadores duplicados, como se indica en el siguiente proceso:

- Configure un conmutador Ethernet que admita el Protocolo de Control de Agregación de Enlaces (LACP) IEEE 802.3ad/IEEE 802.1ax.
- Utilizando vCenter, conecte el grupo de puertos de la máquina virtual asociado a las máquinas virtuales de Cisco WebEx Meetings Server a ambos adaptadores físicos.
- Conecte ambos adaptadores físicos al conmutador.
- Disponga el conmutador para que habilite los dos puertos como un equipo estático.
- Usando VMware vSphere, establezca los equipos de NIC como Activo/Activo para permitir el funcionamiento de las interfaces en ambas NIC.

Por ejemplo, para un despliegue de 800 usuarios, se pueden sustituir dos enlaces de 1 GB/s para cada enlace de 10 GB/s del host ESXi por las máquinas virtuales internas, y cuatro enlaces de 1 GB/s para cada enlace de 10 GB/s del proxy inverso de Internet (para obtener tolerancia a fallos en un sistema con HA, como se describe en la sección "Conexiones de red redundante para despliegues HA", es necesario duplicar el número de enlaces). Con el host ESXi con las máquinas virtuales internas, conecte dos enlaces de 1 GB/s al primer conmutador Ethernet *más* dos enlaces de 1 GB/s al segundo conmutador Ethernet.

Nota El ejemplo de configuraciones del servidor que se muestra en los *Requisitos del sistema de Cisco WebEx Meetings Server* no incluye suficientes interfaces de red para admitir equipos de NIC para este fin.

Equilibrio de la carga

El equilibrio de la carga siempre se realiza en CWMS, independientemente del tipo de tráfico que se está manejando. No es una función que se pueda configurar.

El sistema intenta equilibrar la carga de forma equitativa en todos los nodos web. Cuando el despliegue consiste en un sistema sin alta disponibilidad (HA), se equilibran las conexiones entre todos los nodos web de ese sistema. En un despliegue de HA, el sistema usa los nodos web tanto en el sistema principal como en el sistema de alta disponibilidad para equilibrar la carga. En caso de que se produzca un error en uno de ellos, pero no en los nodos web, el sistema permanece activo, aunque se reduce la capacidad.

El nodo de proxy inverso de Internet (IRP) es un punto de entrada en el que se toman la mayoría de las decisiones sobre el equilibrio de la carga. En un sistema, solo hay un nodo de IRP activo. Un sistema de despliegue sin HA solo tiene un nodo de IRP. Un sistema con despliegue de HA tiene dos nodos de IRP; un

IRP está activo mientras el otro no. Según la configuración del DNS, el IRP ofrece todo el tráfico externo y, en caso de que el DNS no esté divido, todo el tráfico interno.

Si se produce un error que afecta a varios organizadores, la funcionalidad y la capacidad se pueden ver afectadas.

CAPÍTULO 4

Cambios de las comunicaciones de red necesarios para el despliegue

- Lista de comprobación de comunicaciones de red para el sistema, página 66
- Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático y acceso público, página 67
- Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue manual, acceso público y todas las máquinas virtuales internas, página 69
- Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático, acceso público y un DNS de horizonte no dividido, página 73
- Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue manual, acceso público y un DNS de horizonte no dividido, página 75
- Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático, acceso público y un DNS de horizonte dividido, página 78
- Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue manual, acceso público y un DNS de horizonte dividido, página 81
- Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático y sin acceso público, página 84
- Lista de comprobación de comunicaciones de red para una instalación o expansión con despliegue manual y sin acceso público, página 86
- URL del sitio de WebEx y URL de administración de WebEx, página 89
- Acceso de puerto cuando las máquinas virtuales están en la red interna, página 90
- Acceso de puerto con un proxy inverso de Internet en la red DMZ, página 91
- Puertos de VMware vCenter, página 97
- Puertos de Cisco WebEx Meeting Center, página 98
- Uso de NAT con el sistema, página 99
- Proxies de envío, página 101

Lista de comprobación de comunicaciones de red para el sistema

La lista de comprobación de las comunicaciones de red muestra los cambios de red necesarios para el sistema, en función de la configuración de DNS y de si va a activar el acceso público (permitiendo a los usuarios organizar reuniones o asistir a ellas desde Internet o dispositivos móviles).

Elija la lista de comprobación en función de si está utilizando el despliegue de sistema automático (recomendado para los despliegues de 50, 250 u 800 usuarios) o el despliegue del sistema manual (obligatorio para una implementación de 2000 usuarios).

- Todas las máquinas virtuales, incluido el proxy inverso de Internet, están en su red interna (la configuración más sencilla)
  - Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático y acceso público, en la página 67
  - Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue manual, acceso público y todas las máquinas virtuales internas, en la página 69
- DNS de horizonte no dividido (la configuración de DNS más común)
  - Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático, acceso público y un DNS de horizonte no dividido, en la página 73
  - Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue manual, acceso público y un DNS de horizonte no dividido, en la página 75
- DNS de horizonte dividido
  - Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático, acceso público y un DNS de horizonte dividido, en la página 78
  - Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue manual, acceso público y un DNS de horizonte dividido, en la página 81
- Para sistemas sin acceso público
  - Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático y sin acceso público, en la página 84
  - Lista de comprobación de comunicaciones de red para una instalación o expansión con despliegue manual y sin acceso público, en la página 86

Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático y acceso público

Despliegue de máquina virtual

En un despliegue automático, desplegamos todas las máquinas virtuales (excepto la máquina virtual de administración) por usted. Recomendamos que seleccione un despliegue automático si está desplegando un sistema de 50, 250 u 800 usuarios.

- Verifique que la máquina virtual multimedia (si procede) esté en la misma subred que la máquina virtual de administración.
- Verifique que las máquinas virtuales de proxy inverso de Internet estén en su red interna.
- Verifique que los hosts ESXi para todas las máquinas virtuales (incluida la del proxy inverso de Internet) se gestionen desde el mismo VMware vCenter.

Direcciones IP necesarias

Descripción	Ubicación de red	Dirección IP
Dirección IP real de la máquina virtual de administración	Interna	
Dirección IP real de la máquina virtual multimedia (si procede)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real del proxy inverso de Internet	Interna (puede estar en la misma subred que la máquina virtual de administración)	
URL de administración (usada exclusivamente por el sistema, apunta a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
URL del sitio de WebEx (usada exclusivamente por el sistema. apunta a la dirección VIP pública)	Interna (misma subred que el proxy inverso de Internet). Esta dirección IP debe ser de acceso público.	
Dirección IP real de la máquina virtual de administración HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema principal)	

Descripción	Ubicación de red	Dirección IP
Dirección IP real de la máquina virtual multimedia HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema principal)	
Dirección IP real del proxy inverso de Internet HA (si procede)	Interna [misma subred que la del proxy inverso de Internet del sistema principal (pero puede utilizar NAT con una dirección IP privada)]	

CONFIGURACIÓN DE DNS

Actualice al servidor DNS tal como se indica a continuación. Hay algunas limitaciones en cuanto a la parte del nombre de host de la URL del sitio de WebEx y la URL del sitio de administración. Para obtener una lista de las palabras que no se pueden utilizar, consulte URL del sitio de WebEx y URL de administración de WebEx, en la página 89.

Tarea	Ejemplos
Nombres de host y direcciones IP de las máquinas virtuales internas: máquina virtual de administración y, si procede, la máquina virtual multimedia.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Nombre de host y dirección IP de la máquina virtual de proxy inverso de Internet.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
URL del sitio de administración y dirección VIP privada.	• <Administration-site-URL> <Private-VIP-address>
URL del sitio de WebEx y dirección VIP pública.	• <WebEx-site-URL> <Public-VIP-address>

Configuración del cortafuegos

Por motivos de seguridad, recomendamos que coloque el proxy inverso de Internet en una subred que esté separada de las máquinas virtuales internas (administración o multimedia). Consulte Acceso de puerto cuando las máquinas virtuales están en la red interna, en la página 90:

Configuración del enrutamiento de red

Tarea	Ejemplos
Active el enrutamiento de capa 3 entre la red interna y la red DMZ	• Subred interna <internal-subnet>/24 • Subred DMZ <DMZ-subnet>/24
Verifique que la dirección VIP pública y las máquinas virtuales de proxy inverso de Internet se encuentran en la misma subred. [Como está desplegando todas las máquinas virtuales de su sistema internamente (el proxy inverso de Internet no está en el DMZ), esta subred debe estar en la red interna].	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Verifique que la dirección VIP privada y las máquinas virtuales internas se encuentran en la misma subred.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue manual, acceso público y todas las máquinas virtuales internas

Despliegue de máquina virtual

En un despliegue manual, debe crear todas las máquinas virtuales para su sistema utilizando el asistente OVA desde su cliente vSphere. A continuación, deberá instalar su sistema utilizando un despliegue manual.

Debe seleccionar un despliegue manual si está desplegando un sistema de 2000 usuarios.

- Asegúrese de que todas las máquinas virtuales internas adicionales (multimedia y Web, si procede) se encuentran en la misma subred que la máquina virtual del administrador.
- Asegúrese de que las máquinas virtuales de proxy inverso de Internet están en su red interna.

Direcciones IP necesarias

Descripción	Ubicación de red	Dirección IP
Dirección IP real de la máquina virtual de administración	Interna	
Dirección IP real de la máquina virtual multimedia (si procede)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la segunda máquina virtual multimedia (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la tercera máquina virtual multimedia (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la máquina virtual Web (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la segunda máquina virtual Web (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real del proxy inverso de Internet	Interna (puede estar en la misma subred que la máquina virtual de administración)	
URL de administración (usada exclusivamente por el sistema, apunta a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
URL del sitio de WebEx (usada exclusivamente por el sistema. apunta a la dirección VIP pública)	Interna (misma subred que el proxy inverso de Internet) **Nota** Esta dirección IP debe ser de acceso público.	
Dirección IP real de la máquina virtual de administración HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual multimedia HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual Web HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema primario)	

Descripción	Ubicación de red	Dirección IP
Dirección IP real del proxy inverso de Internet HA (si procede)	Interna: misma subred que la del proxy inverso de Internet del sistema primario (pero puede usar NAT con una dirección IP privada)	

CONFIGURACIÓN DE DNS

Haga los cambios siguientes en su configuración de DNS.

Nota Hay algunas limitaciones en cuanto a la parte del nombre de host de la URL del sitio de WebEx y la URL del sitio de administración. Para obtener una lista de las palabras que no se pueden utilizar, consulte URL del sitio de WebEx y URL de administración de WebEx, en la página 89.

Tarea	Ejemplo
Actualizar su servidor DNS con los nombres de host y direcciones IP para las máquinas virtuales internas: administre la máquina virtual y, si procede, las máquinas virtuales Web y multimedia.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Actualizar su servidor DNS con el nombre de host y la dirección IP para la máquina virtual de proxy inverso de Internet.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Actualizar su servidor DNS con la URL del sitio de administración y la información de la dirección VIP privada.	• <Administration-site-URL> <Private-VIP-address>
Actualizar su servidor DNS con la URL del sitio de WebEx y la información de la dirección VIP pública.	• <WebEx-site-URL> <Public-VIP-address>

Configuración del cortafuegos

Por motivos de seguridad, Cisco recomienda que coloque el proxy inverso de Internet en una subred distinta de las máquinas virtuales internas (administración, multimedia y Web, si procede).

Aunque no se recomienda, también se pueden colocar todas las máquinas virtuales (interna y de proxy inverso de Internet) en la misma subred. Consulte Acceso de puerto cuando las máquinas virtuales están en la red interna, en la página 90:

Configuración del enrutamiento de red

Haga los cambios siguientes en su enrutamiento de red.

Tarea	Comparar estas direcciones IP
Active el enrutamiento L3 (capa 3) entre la red interna y la red DMZ para las máquinas virtuales siguientes: máquina virtual de administración y, si procede, la máquina virtual Web y multimedia	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Verifique que la dirección VIP pública y las máquinas virtuales de proxy inverso de Internet se encuentran en la misma subred. **Nota** Como está desplegando todas las máquinas virtuales de su sistema internamente (el proxy inverso de Internet no está en el DMZ), esta subred debe estar en la red interna.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Compruebe que la dirección VIP privada y las máquinas virtuales internas (administración y multimedia, si procede) se encuentran en la misma subred.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático, acceso público y un DNS de horizonte no dividido

Despliegue de máquina virtual

En un despliegue automático, desplegamos todas las máquinas virtuales (excepto la máquina virtual de administración) por usted. Recomendamos que seleccione un despliegue automático si está desplegando un sistema de 50, 250 u 800 usuarios.

- Verifique que la máquina virtual multimedia (si procede) esté en la misma subred que la máquina virtual de administración.
- Verifique que las máquinas virtuales de proxy inverso de Internet estén en su red DMZ.

Direcciones IP necesarias

Descripción	Ubicación de red	Dirección IP
Dirección IP real de la máquina virtual de administración	Interna	
Dirección IP real de la máquina virtual multimedia (si procede)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real del proxy inverso de Internet	DMZ (pero puede utilizar NAT con una dirección IP privada)	
URL de administración (usada exclusivamente por el sistema, apunta a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
URL del sitio de WebEx (usada exclusivamente por el sistema. apunta a la dirección VIP pública)	DMZ (misma subred que el proxy inverso de Internet)	
Dirección IP real de la máquina virtual de administración HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema principal)	
Dirección IP real de la máquina virtual multimedia HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema principal)	

Descripción	Ubicación de red	Dirección IP
Dirección IP real del proxy inverso de Internet HA (si procede)	DMZ [misma subred que la del proxy inverso de Internet del sistema principal (pero puede utilizar NAT con una dirección IP privada)]	

CONFIGURACIÓN DE DNS

Actualice al servidor DNS tal como se indica a continuación. Hay algunas limitaciones en cuanto a la parte del nombre de host de la URL del sitio de WebEx y la URL del sitio de administración. Para obtener una lista de las palabras que no se pueden utilizar, consulte URL del sitio de WebEx y URL de administración de WebEx, en la página 89.

Tarea	Ejemplo
Nombres de host y direcciones IP de las máquinas virtuales internas: máquina virtual de administración y, si procede, la máquina virtual multimedia.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Nombre de host y dirección IP de la máquina virtual de proxy inverso de Internet.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
URL del sitio de administración y dirección VIP privada.	• <Administration-site-URL> <Private-VIP-address>
URL del sitio de WebEx y dirección VIP pública.	• <WebEx-site-URL> <Public-VIP-address>

Configuración del cortafuegos

Por motivos de seguridad, recomendamos que coloque el proxy inverso de Internet en una subred que esté separada de las máquinas virtuales internas (administración o multimedia). Consulte Acceso de puerto cuando las máquinas virtuales están en la red interna, en la página 90:

Configuración del enrutamiento de red

Haga los cambios siguientes en su enrutamiento de red.

Tarea	Comparar estas direcciones IP
Active el enrutamiento de capa 3 entre la red interna y la red DMZ	• Subred interna <internal-subnet>/24 • Subred DMZ <DMZ-subnet>/24
Verifique que la dirección VIP pública y las máquinas virtuales de proxy inverso de Internet se encuentran en la misma subred.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Verifique que la dirección VIP privada y las máquinas virtuales internas se encuentran en la misma subred.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue manual, acceso público y un DNS de horizonte no dividido

Despliegue de máquina virtual

En un despliegue manual, debe crear todas las máquinas virtuales para su sistema utilizando el asistente OVA desde su cliente vSphere. A continuación, deberá instalar su sistema utilizando un despliegue manual.

Debe seleccionar un despliegue manual si está desplegando un sistema de 2000 usuarios.

- Asegúrese de que todas las máquinas virtuales internas adicionales (multimedia y Web, si procede) se encuentran en la misma subred que la máquina virtual del administrador.
- Asegúrese de que las máquinas virtuales de proxy inverso de Internet están en su red DMZ.

Direcciones IP necesarias

Descripción	Ubicación de red	Dirección IP
Dirección IP real de la máquina virtual de administración	Interna	

Descripción	Ubicación de red	Dirección IP
Dirección IP real de la máquina virtual multimedia (si procede)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la segunda máquina virtual multimedia (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la tercera máquina virtual multimedia (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la máquina virtual Web (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la segunda máquina virtual Web (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real del proxy inverso de Internet	DMZ (pero puede usar NAT con una dirección IP privada)	
URL de administración (usada exclusivamente por el sistema, apunta a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
URL del sitio de WebEx (usada exclusivamente por el sistema. apunta a la dirección VIP pública)	DMZ (misma subred que el proxy inverso de Internet)	
Dirección IP real de la máquina virtual de administración HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual multimedia HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual Web HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real del proxy inverso de Internet HA (si procede)	DMZ: misma subred que la del proxy inverso de Internet del sistema primario (pero puede usar NAT con una dirección IP privada)	

CONFIGURACIÓN DE DNS

Haga los cambios siguientes en su configuración de DNS.

Nota Hay algunas limitaciones en cuanto a la parte del nombre de host de la URL del sitio de WebEx y la URL del sitio de administración. Para obtener una lista de las palabras que no se pueden utilizar, consulte URL del sitio de WebEx y URL de administración de WebEx, en la página 89.

Tarea	Ejemplo
Actualice su servidor DNS con los nombres de host y direcciones IP para las máquinas virtuales internas: administre la máquina virtual y, si procede, las máquinas virtuales Web y multimedia.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Actualice su servidor DNS con el nombre de host y la dirección IP para la máquina virtual de proxy inverso de Internet.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Actualice su servidor DNS con la URL del sitio de administración y la información de la dirección VIP privada.	• <Administration-site-URL> <Private-VIP-address>
Actualice su servidor DNS con la URL del sitio de WebEx y la información de la dirección VIP pública.	• <WebEx-site-URL> <Public-VIP-address>

Configuración del cortafuegos

Por motivos de seguridad, Cisco recomienda que coloque el proxy inverso de Internet en una subred distinta de las máquinas virtuales internas (administración, multimedia y Web, si procede). Consulte Acceso de puerto con un proxy inverso de Internet en la red DMZ, en la página 91:

Configuración del enrutamiento de red

Haga los cambios siguientes en su enrutamiento de red.

Tarea	Comparar estas direcciones IP
Active el enrutamiento L3 (capa 3) entre la red interna y la red DMZ para las máquinas virtuales siguientes: máquina virtual de administración y, si procede, la máquina virtual Web y multimedia	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Verifique que la dirección VIP pública y las máquinas virtuales de proxy inverso de Internet se encuentran en la misma subred.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Compruebe que la dirección VIP privada y las máquinas virtuales internas (administración y multimedia, si procede) se encuentran en la misma subred.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático, acceso público y un DNS de horizonte dividido

Despliegue de máquina virtual

En un despliegue automático, desplegamos todas las máquinas virtuales (excepto la máquina virtual de administración) por usted. Recomendamos que seleccione un despliegue automático si está desplegando un sistema de 50, 250 u 800 usuarios.

- Verifique que la máquina virtual multimedia (si procede) esté en la misma subred que la máquina virtual de administración.

- Verifique que las máquinas virtuales de proxy inverso de Internet estén en su red DMZ.

Direcciones IP necesarias

Descripción	Ubicación de red	Dirección IP
Dirección IP real de la máquina virtual de administración	Interna	
Dirección IP real de la máquina virtual multimedia (si procede)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real del proxy inverso de Internet	DMZ (pero puede utilizar NAT con una dirección IP privada)	
URL de administración (usada exclusivamente por el sistema, apunta a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
URL del sitio de WebEx (usada exclusivamente por el sistema. Apunta a dos direcciones VIP): • usuarios internos: dirección VIP privada • usuarios externos: dirección VIP pública	• Usuarios internos: interna (misma subred que la máquina virtual de administración) • Usuarios externos: DMZ (misma subred que el proxy inverso de Internet)	
Dirección IP real de la máquina virtual de administración HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema principal)	
Dirección IP real de la máquina virtual multimedia HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema principal)	
Dirección IP real del proxy inverso de Internet HA (si procede)	DMZ [misma subred que la del proxy inverso de Internet del sistema principal (pero puede utilizar NAT con una dirección IP privada)]	

CONFIGURACIÓN DE DNS

Actualice al servidor DNS tal como se indica a continuación. Hay algunas limitaciones en cuanto a la parte del nombre de host de la URL del sitio de WebEx y la URL del sitio de administración. Para obtener una lista de las palabras que no se pueden utilizar, consulte URL del sitio de WebEx y URL de administración de WebEx, en la página 89.

Tarea	Ejemplo
Nombres de host y direcciones IP de las máquinas virtuales internas: máquina virtual de administración y, si procede, la máquina virtual multimedia.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Nombre de host y dirección IP de la máquina virtual DMZ.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Información del URL del sitio de WebEx, URL del sitio de administración y dirección VIP privada.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>
URL del sitio de WebEx y dirección VIP pública.	• <WebEx-site-URL> <Public-VIP-address>

Configuración del cortafuegos

Por motivos de seguridad, recomendamos que coloque el proxy inverso de Internet en una subred que esté separada de las máquinas virtuales internas (administración o multimedia). Consulte Acceso de puerto cuando las máquinas virtuales están en la red interna, en la página 90:

Configuración del enrutamiento de red

Haga los cambios siguientes en su enrutamiento de red.

Tarea	Comparar estas direcciones IP
Active el enrutamiento de capa 3 entre la red interna y la red DMZ	• Subred interna <internal-subnet>/24 • Subred DMZ <DMZ-subnet>/24
Verifique que la dirección VIP pública y las máquinas virtuales de proxy inverso de Internet se encuentran en la misma subred.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>

Tarea	Comparar estas direcciones IP
Verifique que la dirección VIP privada y las máquinas virtuales internas se encuentran en la misma subred.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue manual, acceso público y un DNS de horizonte dividido

Despliegue de máquina virtual

En un despliegue manual, debe crear todas las máquinas virtuales para su sistema utilizando el asistente OVA desde su cliente vSphere. A continuación, deberá instalar su sistema utilizando un despliegue manual.

Debe seleccionar un despliegue manual si está desplegando un sistema de 2000 usuarios.

- Asegúrese de que todas las máquinas virtuales internas adicionales (multimedia y Web, si procede) se encuentran en la misma subred que la máquina virtual del administrador.
- Asegúrese de que las máquinas virtuales de proxy inverso de Internet están en su red DMZ.

Direcciones IP necesarias

Descripción	Ubicación de red	Dirección IP
Dirección IP real de la máquina virtual de administración	Interna	
Dirección IP real de la máquina virtual multimedia (si procede)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la segunda máquina virtual multimedia (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la tercera máquina virtual multimedia (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	

Descripción	Ubicación de red	Dirección IP
Dirección IP real de la máquina virtual Web (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la segunda máquina virtual Web (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real del proxy inverso de Internet	DMZ (pero puede usar NAT con una dirección IP privada)	
URL de administración (usada exclusivamente por el sistema, apunta a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
URL del sitio de WebEx (usada exclusivamente por el sistema. Apunta a dos direcciones VIP) • usuarios internos: dirección VIP privada • usuarios externos: dirección VIP pública	• Usuarios internos: interna (misma subred que la máquina virtual de administración) • Usuarios externos: DMZ (misma subred que el proxy inverso de Internet)	
Dirección IP real de la máquina virtual de administración HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual multimedia HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual Web HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real del proxy inverso de Internet HA (si procede)	DMZ: misma subred que la del proxy inverso de Internet del sistema primario (pero puede usar NAT con una dirección IP privada)	

CONFIGURACIÓN DE DNS

Haga los cambios siguientes en su configuración de DNS.

Nota Hay algunas limitaciones en cuanto a la parte del nombre de host de la URL del sitio de WebEx y la URL del sitio de administración. Para obtener una lista de las palabras que no se pueden utilizar, consulte URL del sitio de WebEx y URL de administración de WebEx, en la página 89.

Tarea	Ejemplo
Actualice su servidor DNS (que activa la búsqueda interna) con los nombres de host y direcciones IP para las máquinas virtuales internas: administre la máquina virtual y, si procede, las máquinas virtuales Web y multimedia.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Actualice su servidor de DNS (que activa la búsqueda interna) con el nombre de host y la dirección IP para la máquina virtual DMZ.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Actualice su servidor de DNS (que activa la búsqueda interna) con la URL del sitio de WebEx, la URL del sitio de Administración y la información de la dirección VIP privada.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>
Actualice su servidor DNS (que activa la búsqueda externa) con la URL del sitio de WebEx y la información de la dirección VIP pública.	• <WebEx-site-URL> <Public-VIP-address>

Configuración del cortafuegos

Por motivos de seguridad, Cisco recomienda que coloque el proxy inverso de Internet en una subred distinta de las máquinas virtuales internas (administración, multimedia y Web, si procede). Consulte Acceso de puerto con un proxy inverso de Internet en la red DMZ, en la página 91:

Configuración del enrutamiento de red

Haga los cambios siguientes en su enrutamiento de red.

Tarea	Comparar estas direcciones IP
Active el enrutamiento L3 (capa 3) entre la red interna y la red DMZ para las máquinas virtuales siguientes: máquina virtual de administración y, si procede, la máquina virtual Web y multimedia	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Verifique que la dirección VIP pública y las máquinas virtuales de proxy inverso de Internet se encuentran en la misma subred.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Compruebe que la dirección VIP privada y las máquinas virtuales internas (máquina virtual de administración y , si procede, la máquina virtual Web y multimedia) se encuentran en la misma subred.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Lista de comprobación de comunicaciones de red para una instalación o ampliación con despliegue automático y sin acceso público

Despliegue de máquina virtual

En un despliegue automático, desplegamos todas las máquinas virtuales (excepto la máquina virtual de administración) por usted. Recomendamos que seleccione un despliegue automático si está desplegando un sistema de 50, 250 u 800 usuarios.

Verifique que la máquina virtual multimedia (si procede) esté en la misma subred que la máquina virtual de administración.

Direcciones IP necesarias

Descripción	Ubicación de red	Dirección IP
Dirección IP real de la máquina virtual de administración	Interna	
Dirección IP real de la máquina virtual multimedia (si procede)	Interna (misma subred que la máquina virtual de administración)	
URL de administración (usada exclusivamente por el sistema, apunta a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la máquina virtual de administración HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema principal)	
Dirección IP real de la máquina virtual multimedia HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema principal)	
Dirección IP real del proxy inverso de Internet HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema principal)	

CONFIGURACIÓN DE DNS

Actualice al servidor DNS tal como se indica a continuación. Hay algunas limitaciones en cuanto a la parte del nombre de host de la URL del sitio de WebEx y la URL del sitio de administración. Para obtener una lista de las palabras que no se pueden utilizar, consulte URL del sitio de WebEx y URL de administración de WebEx, en la página 89.

Tarea	Ejemplo
Nombres de host y direcciones IP de las máquinas virtuales internas: máquina virtual de administración y, si procede, la máquina virtual multimedia.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Información del URL del sitio de WebEx, URL del sitio de administración y dirección VIP privada.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>

Configuración del cortafuegos

Tarea	Ejemplo
Configure todos los cortafuegos dentro de la red interna para permitir a los exploradores web acceder a la dirección VIP privada.	HTTP <Private-VIP-address>:80 HTTPS <Private-VIP-address>:443

Configuración del enrutamiento de red

Tarea	Comparar estas direcciones IP
Verifique que la dirección VIP privada y las máquinas virtuales internas se encuentran en la misma subred.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Lista de comprobación de comunicaciones de red para una instalación o expansión con despliegue manual y sin acceso público

Despliegue de máquina virtual

En un despliegue manual, debe crear todas las máquinas virtuales para su sistema utilizando el asistente OVA desde su cliente vSphere. A continuación, deberá instalar su sistema utilizando un despliegue manual.

Debe seleccionar un despliegue manual si está desplegando un sistema de 2000 usuarios.

- Asegúrese de que todas las máquinas virtuales internas adicionales (multimedia y Web, si procede) se encuentran en la misma subred que la máquina virtual del administrador.

Direcciones IP necesarias

Descripción	Ubicación de red	Dirección IP
Dirección IP real de la máquina virtual de administración	Interna	

Descripción	Ubicación de red	Dirección IP
Dirección IP real de la máquina virtual multimedia (si procede)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la segunda máquina virtual multimedia (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la tercera máquina virtual multimedia (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la máquina virtual Web (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la segunda máquina virtual Web (solo para sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
URL de administración (usada exclusivamente por el sistema, apunta a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
URL del sitio de WebEx (usada exclusivamente por el sistema. apunta a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la máquina virtual de administración HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual multimedia HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual Web HA (si procede)	Interna (misma subred que la máquina virtual de administración del sistema primario)	

CONFIGURACIÓN DE DNS

Haga los cambios siguientes en su configuración de DNS.

Nota Hay algunas limitaciones en cuanto a la parte del nombre de host de la URL del sitio de WebEx y la URL del sitio de administración. Para obtener una lista de las palabras que no se pueden utilizar, consulte URL del sitio de WebEx y URL de administración de WebEx, en la página 89.

Tarea	Ejemplo
Actualice su servidor DNS (que activa la búsqueda interna) con los nombres de host y direcciones IP para las máquinas virtuales internas: administre la máquina virtual y, si procede, las máquinas virtuales Web y multimedia.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Actualice su servidor de DNS con la URL del sitio de Administración, la URL del sitio de WebEx y la información de dirección VIP privada.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>

Configuración del cortafuegos

Haga los cambios siguientes en sus cortafuegos.

Tarea	Ejemplo
Configure todos los cortafuegos dentro de la red interna para permitir a los exploradores web acceder a la dirección VIP privada.	• HTTP <Private-VIP-address>:80 • HTTPS <Private-VIP-address>:443

Configuración del enrutamiento de red

Haga los cambios siguientes en su enrutamiento de red.

Tarea	Comparar estas direcciones IP
Compruebe que la dirección VIP privada y las máquinas virtuales internas (administración y multimedia, si procede) se encuentran en la misma subred.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

URL del sitio de WebEx y URL de administración de WebEx

URL del sitio de WebEx

Los usuarios acceden a la URL del sitio de WebEx para planificar, organizar o asistir a reuniones. Esta URL se resuelve en la dirección VIP privada o en la dirección VIP pública, dependiendo de si está utilizando un DNS de horizonte dividido.

- Resuelve la dirección VIP pública para todos los usuarios, cuando no se tiene un DNS de horizonte dividido.
- Resuelve la dirección VIP pública para los usuarios externos, cuando tiene un DNS de horizonte dividido.
- Resuelve la dirección VIP privada para los usuarios internos, cuando tiene un DNS de horizonte dividido.

Nota Los puertos 80 y 443 deben estar abiertos para la URL del sitio de WebEx.

URL de administración de WebEx

Los administradores acceden a la URL de administración de WebEx para configurar, gestionar y supervisar el sistema. Esta URL se resuelve en la dirección VIP privada.

Nota Los puertos 80 y 443 deben estar abiertos para la URL de administración de WebEx.

Nombres para las URL del sitio de WebEx y de administración de WebEx

Puede seleccionar casi cualquier nombre para estas URL, utilizando todos los caracteres en minúscula. No obstante, no puede utilizar como nombre de host en las URL:

- el mismo nombre que los nombres de host para cualquier máquina virtual del sistema

- 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

Acceso de puerto cuando las máquinas virtuales están en la red interna

En este apartado se describe el acceso al puerto necesario en los cortafuegos externos, cuando todas las máquinas virtuales del sistema (de administración y, si procede, multimedia, Web y el proxy inverso de Internet) se encuentran en la red interna. Ésta es la topología de red de proxy inverso de Internet interna.

Nota El nodo web y el nodo de administración envían solicitudes SMTP al servidor de correo electrónico configurado. Si hay un cortafuegos entre las máquinas virtuales web y de administración internas y el servidor de correo electrónico, el tráfico SMTP puede bloquearse. Para comprobar que la configuración del servidor del correo electrónico y las notificaciones por correo electrónico funcionan correctamente, asegúrese de que el puerto 25 o 465 (número de puerto SMTP seguro) está abierto entre el servidor de correo electrónico y las máquinas virtuales de administración y web.

Acceso de puertos en el cortafuegos externo

Si ha habilitado el acceso público, entonces los siguientes puertos están abiertos para entrada directa desde Internet a las máquinas virtuales de proxy inverso de Internet en la red interna:

Importante Compruebe que el cortafuegos y cualquier otra solución de equilibrio de carga redirige las solicitudes a los puertos enumerados a continuación para asegurarse de que los usuarios finales pueden organizar y unirse a las reuniones correctamente.

- Puerto TCP 80 a la dirección pública virtual IP (VIP)
- Puerto TCP 443 a la dirección pública virtual IP (VIP)

Acceso de puerto con un proxy inverso de Internet en la red DMZ

En este apartado se describe el puerto de acceso necesario en los cortafuegos internos y externos, cuando posee máquinas virtuales internas (de administración y, si procede, multimedia y web) en la red interna, y el proxy inverso de Internet (IRP) en la red DMZ.

Configurar listas de control de accesos (ACL) en el conmutador que permite el tráfico a los hosts para las máquinas virtuales del sistema.

Acceso de puertos en el cortafuegos externo

Si ha habilitado el acceso público, entonces los siguientes puertos estarán abiertos para la entrada directa desde Internet a las máquinas virtuales de proxy inverso de Internet en la red DMZ:

Importante Compruebe que el cortafuegos y cualquier otra solución de equilibrio de carga redirige las solicitudes a los puertos enumerados a continuación para asegurarse de que los usuarios finales pueden organizar y unirse a las reuniones correctamente.

Nota Cisco recomienda encarecidamente que abra el puerto 80 (http) además del puerto 443 (https) para simplificar la experiencia del usuario final (en un explorador, los usuarios introducen la URL del sitio de WebEx sin tener que recordar si es http o https. Sin embargo, para este producto, el tráfico real de red siempre fluye a través del puerto 443 (https con cifrado de SSL).

Restricción Configure el puerto TCP 64700 en la máquina de proxy inverso de Internet para denegar las solicitudes que lleguen a la dirección VIP pública. En el cortafuegos interno, podrá limitar el acceso a este puerto solamente para las solicitudes de las máquinas virtuales de administración.

Protocolo	Puerto	Source	Destino	¿Por qué es necesario?
TCP	443	Cualquier cliente externo	VIP pública (Eth1) de IRP	Los clientes externos acceden a la URL del sitio de WebEx a través del protocolo HTTPS. Las conexiones TCP se inician desde las máquinas virtuales externas a las máquinas virtuales de IRP.
TCP	80	Cualquier cliente externo	VIP pública (Eth1) de IRP	Los clientes externos acceden a la URL del sitio de WebEx a través del protocolo HTTP. Las conexiones TCP se inician desde las máquinas virtuales externas a las máquinas virtuales de IRP.
TCP	8444 (incorporado en la versión 2.5MR1, 2.6, y 2.0MR6HF).	Cualquier cliente externo	VIP pública (Eth1) de IRP	Los clientes externos acceden a las grabaciones de WebEx a través del protocolo HTTPS. Las conexiones TCP se inician desde las máquinas virtuales externas a las máquinas virtuales de IRP.

Protocolo	Puerto	Source	Destino	¿Por qué es necesario?
UDP	53	VIP pública (Eth0) de IRP	Servidor DNS	Es necesario si tiene un cortafuegos entre las máquinas virtuales y el servidor DNS, para que su sistema se despliegue y funcione correctamente.

Acceso de puerto en el firewall interno

Los siguientes puertos deben estar abiertos cuando el proxy inverso de Internet está en la red DMZ. Si tiene restricciones en las conexiones de la red interna a la red DMZ, se aplica la tabla siguiente. Permita la *salida* de conexiones TCP de la red interna al segmento de red DMZ en los puertos siguientes.

Nota No es necesario permitir ninguna conexión TCP del segmento DMZ en la red interna para que este producto funcione correctamente.

Nota Mediante iptables o listas de control de acceso (ACL), configure el cortafuegos de modo que las conexiones al puerto 64616 sólo procedan de la máquina virtual de administración.

Nota El nodo web y el nodo de administración envían solicitudes SMTP al servidor de correo electrónico configurado. Si hay un cortafuegos entre las máquinas virtuales web y de administración internas y el servidor de correo electrónico, el tráfico SMTP puede bloquearse. Para comprobar que la configuración del servidor del correo electrónico y las notificaciones por correo electrónico funcionan correctamente, asegúrese de que el puerto 25 o 465 (número de puerto SMTP seguro) está abierto entre el servidor de correo electrónico y las máquinas virtuales de administración y web.

Nota Especialmente, cuando el proxy inverso de Internet está en la red DMZ, permita las solicitudes y las respuestas de eco del ICMP (protocolo de mensajes de control de Internet). De lo contrario, la detección del proxy inverso de Internet y la validación del alcance del servidor DNS podrían fallar si no se recibe la respuesta de eco del ICMP.

Protocolo	Puerto	Source	Destino	¿Por qué es necesario?
TCP	64001	Todas las máquinas virtuales internas (IP Eth0)	IP real (Eth0) de las máquina virtuales de IRP	Establece conexiones inversas con el IRP. Las conexiones TCP se establecen desde las máquinas virtuales internas a las máquinas virtuales IRP.
TCP	64002	Máquinas virtuales de administración y web (IP Eth0)	IP real (Eth0) de las máquina virtuales de IRP	Establece conexiones inversas con el IRP. Las conexiones TCP se establecen desde las máquinas virtuales internas a las máquinas virtuales IRP.
TCP	7001	Todas las máquinas virtuales internas (IP Eth0)	IP real (Eth0) de las máquina virtuales de IRP	Establece conexiones inversas con el IRP. Las conexiones TCP se inician desde las máquinas virtuales internas a las máquinas virtuales IRP.

Protocolo	Puerto	Source	Destino	¿Por qué es necesario?
TCP	64616	Máquinas virtuales de administración (IP Eth0)	IP real (Eth0) de las máquina virtuales de IRP	Arranque el IRP. Las conexiones TCP se inician desde las máquinas virtuales de administración a las máquinas virtuales IRP. **Nota** Mediante iptables o listas de control de acceso (ACL), configure el cortafuegos de modo que las conexiones al puerto 64616 sólo procedan de la máquina virtual de administración.
TCP	64700	Máquinas virtuales de administración (IP Eth0)	IP real (Eth0) de las máquina virtuales de IRP	Recopila registros sobre el IRP. Las conexiones TCP se inician desde las máquinas virtuales de administración a las máquinas virtuales IRP. Limita el acceso a este puerto en todas las máquinas virtuales de Cisco WebEx Meetings Server sólo a otras máquinas virtuales de Cisco WebEx Meetings Server con reglas de cortafuegos.

Protocolo	Puerto	Source	Destino	¿Por qué es necesario?
TCP	22	Cualquier máquina de cliente interna	IP real (Eth0) de las máquina virtuales de IRP	Solución de problemas de máquinas virtuales IRP utilizando una cuenta de Remote Support.
TCP	443	Cualquier máquina de cliente interna	VIP privada (Eth1) de las máquinas virtuales de administración IP real (Eth0) de las máquinas virtuales multimedia	Usuarios internos que acceden a la URL del sitio de WebEx a través del protocolo https. Las conexiones TCP se establecen desde la máquina de cliente interna a la máquina virtual de administración.
TCP	65002	Cualquier máquina de cliente interna	Cualquier máquina virtual interna	Controla el tráfico de red entre las máquinas virtuales internas
TCP	65102	Cualquier máquina de cliente interna	Cualquier máquina virtual interna	Controla el tráfico de red entre las máquinas virtuales internas
TCP	80	Cualquier máquina de cliente interna	VIP privada (Eth1) de las máquinas virtuales de administración	Usuarios internos que acceden a la URL del sitio de WebEx utilizando http. Las conexiones TCP se establecen desde la máquina de cliente interna a la máquina virtual de administración.
UDP	53	Todas las máquinas virtuales internas (IP Eth0)	Servidor DNS	Si tiene un cortafuegos entre las máquinas virtuales y el servidor DNS, para que su sistema se despliegue y funcione correctamente.

Protocolo	Puerto	Source	Destino	¿Por qué es necesario?
TCP	8443	Nodo web de Cisco WebEx Meetings Server	CUCM	Para que el tráfico AXL en un sistema con varios centros de datos entre Cisco WebEx Meetings Server y CUCM permita la conmutación por error LDAP CUCM.
TCP	8444	El nodo web de Cisco WebEx Meetings Server se utiliza para descargar los archivos de grabación.	VIP privada (Eth1) de las máquinas virtuales de administración IP real (Eth0) de las máquinas virtuales multimedia	Usuarios internos que acceden a la URL del sitio de WebEx a través del protocolo HTTPS. Las conexiones TCP se establecen desde la máquina de cliente interna a la máquina virtual de administración.

Puertos de VMware vCenter

Puertos abiertos para el despliegue

Estos son algunos de los puertos que se utilizan durante el despliegue de un Cisco WebEx Meetings Server (CWMS) con un solo centro de datos (SDC). Una vez que se complete el despliegue, tiene la opción de cerrar los puertos que se abrieron solamente para el despliegue.

Durante un despliegue automático del sistema, el puerto TCP 443 debería estar abierto, en ambas direcciones, entre vCenter y la máquina virtual de administración, para la gestión segura https. La máquina virtual de administración utiliza este puerto para suministrar las credenciales de vCenter a fin de desplegar las máquinas virtuales de manera automática en vCenter.

Los puertos que se enumeran a continuación se utilizan para la comunicación entre el host ESXi y vCenter. Si el host ESXi y vCenter están conectados a una *red de gestión independiente*, es posible que no tenga que abrir estos puertos a través del cortafuegos. Para obtener una lista completa de los puertos que utilizan vCenter y el host ESXi, consulte su documentación de VMware.

- Puertos UDP/TCP 902 en ambas direcciones entre vCenter y los hosts ESXi para la gestión de vCenter
- (Opcional) Puerto TCP 22 del cliente vSphere a los hosts ESXi para la gestión SSH
- Puerto UDP 514 de los hosts ESXi para el sistema al registro del sistema interno
- Puerto TCP 5989 en ambas direcciones entre vCenter y los hosts ESXi para la gestión XML

El puerto UDP predeterminado que se usa para los clientes externos para la transmisión de datos de vídeo y audio es SSL (puerto 443).

Puertos abiertos para admitir varios centros de datos

Puertos que se deben abrir entre las máquinas internas	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
Puertos que se deben abrir entre las máquinas internas y las IP virtuales	tcp 443 tcp 80
Puertos que se deben abrir entre las IP del proxy inverso de Internet y las máquinas internas	tcp 7001 tcp 64001 tcp 64700 tcp 64616
Puertos UDP que se deben abrir entre las máquinas internas	rango udp:10000:19999 rango udp:16000:32000 rango udp:9000:9009 udp 5060 udp 5062

Puertos de Cisco WebEx Meeting Center

Estos puertos se utilizan para la comunicación entre Cisco WebEx Meeting Center y Cisco WebEx Meetings Server.

- Los puertos UDP usados para los clientes internos para la transmisión de datos de vídeo y audio entre UDP y SSL son:
  - Para sistemas de 50 usuarios, utilice el puerto UDP 9000.
  - Para sistemas de 250 usuarios, utilice los puertos UDP 9000, 9001, 9002, 9003.

- Para sistemas de 800 usuarios, utilice los puertos UDP 9000, 9001, 9002, 9003, 9004, 9005, 9006, 9007, 9008, 9009.
- Para sistemas de 2000 usuarios, utilice los puertos UDP 9000, 9001, 9002, 9003, 9004, 9005, 9006, 9007.

- Con la configuración de red adecuada, los servidores multimedia internos permiten conexiones a través de cualquier puerto que utilice Meeting Center.
- El proxy inverso de Internet solo acepta conexiones desde Meeting Center a través de los puertos TCP 80 y 443.
- El tráfico de AXL del nodo web a CUCM pasa a través del puerto 8443. (Consulte también Utilización de CUCM para configurar el servicio web de AXL y la sincronización de directorios).

Uso de NAT con el sistema

Cisco admite el recorrido transversal de traducción de dirección de red (NAT) con este producto para direcciones IP de máquina virtual y para las futuras direcciones IP virtuales (VIP pública y privada) que se están usando en su sistema.

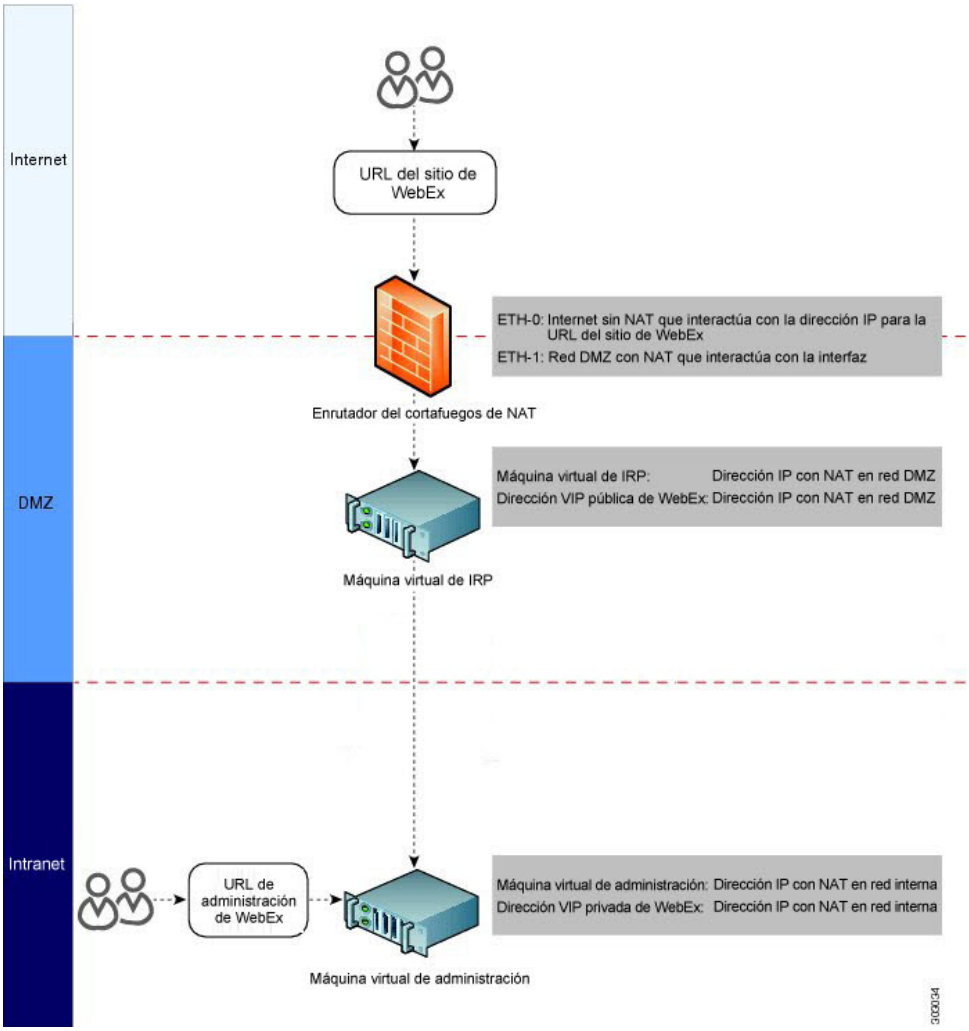
El siguiente diagrama esquemático ilustra un recorrido transversal NAT típico para un sistema de 50 usuarios sin HA. La utilización de NAT ayuda a reducir el número de *direcciones IP públicas* necesarias para el producto a tan solo una dirección IP, en lugar de dos (o tres si despliega HA). También puede implementar despliegues NAT similares siempre y cuando cumplan los requisitos globales del sistema.

Importante La utilización de diversos NAT y cortafuegos tiende a aumentar la latencia, lo que afecta a la calidad del tráfico en tiempo real para los usuarios.

Además, si se utilizan varios dominios NAT, la tarea de enrutar entre estos puede ser problemática. Puede utilizar direcciones IP de NAT siempre que se cumplan los siguientes requisitos:

- Todas las máquinas virtuales del sistema, excepto la máquina virtual del proxy inverso de Internet, pueden utilizar direcciones IP de NAT. No se admite NAT entre la máquina virtual de administración y la máquina virtual del proxy inverso de Internet. La máquina virtual de administración tiene que poder acceder a la dirección IP de la máquina virtual de proxy inverso de Internet (su dirección IP real) a través de la red interna.
- Las direcciones VIP públicas no tienen que ser visibles públicamente, pero deben ser traducibles desde Internet.
- Al desplegar un acceso público, la URL del sitio WebEx debe estar asignada a una dirección IP visible de Internet. Esta dirección IP visible de internet debe ser accesible para los usuarios externos y estar *también* asignada a la dirección VIP pública que configuró durante la implementación del sistema.

  Puede elegir que la dirección VIP pública sea visible desde Internet. Si elige no hacerla visible públicamente debe ser traducible desde Internet.



En el diagrama, un usuario externo accede al sitio de WebEx para organizar o unirse a una reunión. Tras una búsqueda de DNS, la dirección IP del sitio de WebEx es la dirección IP pública de NAT (Eth0). Esta dirección IP pública de NAT es para el router del cortafuegos NAT externo (router 1 de NAT y cortafuegos), entre la red externa y la red DMZ.

El router del cortafuegos recibe esta solicitud del usuario externo y enruta internamente la solicitud a la dirección IP de NAT para el router (Eth1, expuesto a la red DMZ). A continuación, Eth1 envía la solicitud a la dirección VIP pública (también una dirección IP de NAT en el segmento de la red privada para el sitio de WebEx).

Puede utilizar direcciones IP de NAT para las direcciones VIP públicas y las direcciones IP de proxy inverso de Internet. La única dirección IP pública de NAT es la dirección IP Eth0 para el router del cortafuegos NAT.

Nota Para garantizar que este router del cortafuegos NAT (entre Internet y la red DMZ) dirige el paquete de entrada correctamente, establezca la configuración de asignación de puertos en el dispositivo NAT o aplique otros mecanismos similares para garantizar que el paquete se dirige correctamente a la dirección VIP pública y al proxy inverso de Internet.

Normalmente suele existir un segundo router de cortafuegos NAT interno entre la red DMZ y la red interna. De forma similar al router de cortafuegos NAT externo, Eth0 es una dirección IP privada de NAT DMZ y una interfaz para la red DMZ. Eth1 también es una dirección IP privada de NAT que es una interfaz para la red interna.

Puede utilizar direcciones IP de NAT para la dirección VIP privada y para las direcciones IP de la máquina virtual de administración.

Para obtener más información sobre NAT, consulte http://www.cisco.com/c/en/us/tech/ip/ip-addressing-services/tech-tech-notes-list.html.

Proxies de envío

Si la topología de su red incluye proxies, debe cumplir los requisitos específicos para que el proxy inverso de Internet funcione correctamente. Consulte "Uso de proxies de envío en su sistema" en la *Guía de solución de problemas de Cisco WebEx Meetings Server* para ver toda la información en detalle.

CAPÍTULO 5

Métodos recomendados

- Métodos recomendados para Cisco WebEx Meetings Server, página 103

Métodos recomendados para Cisco WebEx Meetings Server

A continuación presentamos una lista de los métodos recomendados que debería consultar para la configuración y el mantenimiento de su sistema Cisco WebEx Meetings Server:

- Suministre alimentación eléctrica a sus hosts de máquina virtual utilizando un sistema de alimentación ininterrumpida (UPS) para minimizar las interrupciones de alimentación. Los fallos de alimentación reiterados pueden dañar los sistemas host y las máquinas virtuales.
- Ponga siempre su sistema en modo de mantenimiento antes de apagar un sistema operativo invitado.
- Para eventos planificados y otras situaciones que precisen el apagado del sistema, apague correctamente sus máquinas virtuales apagando el sistema operativo invitado.
- El sistema está diseñado para repararse a sí mismo cuando sea necesario, y reiniciarlo puede interrumpir este proceso. No le recomendamos reiniciar su sistema para arreglarlo. Si su sistema no funciona bien, póngase en contacto con Cisco TAC. Apague el sistema solo cuando se le indique o durante eventos planificados, como el mantenimiento del centro de datos.
- Configure la redundancia de red para minimizar los fallos de red. Consulte "Agregación de un sistema de alta disponibilidad" en la *Guía de administración de Cisco WebEx Meetings Server* para obtener más información.
- Configure equipos de NIC en su sistema. Los equipos de NIC mejoran el rendimiento y proporcionan redundancia en caso de fallo de NIC.
- Si su organización tiene experiencia en la gestión de redes de área de almacenamiento (SAN), recomendamos SAN en lugar del almacenamiento de conexión directa (DAS). SAN puede ser más fiable que los arrays de discos locales.Consulte Requisitos generales del sistema, en la página 1 para obtener más información sobre los requisitos de almacenamiento de SAN.
- El uso de instantáneas de sus máquinas virtuales puede mermar el rendimiento del sistema de tal modo que afecte a la experiencia del usuario incluso cuando el sistema presente poca carga.
- Si su sistema tiene problemas, asegúrese de comprobar su entorno de VMware VCenter para determinar si son las condiciones VCenter o la red lo que está causando el problema.

- Configure la alta disponibilidad para aumentar las probabilidades de que el sistema continúe funcionando si se produce un fallo.
- Si tiene un sistema de alta disponibilidad y falla su sistema secundario, puede repararlo eliminando el sistema secundario existente (consulte "Eliminación de un sistema de alta disponibilidad" en la *Guía de administración de Cisco WebEx Meetings Server*) y agregando un nuevo sistema secundario (consulte "Agregación de un sistema de alta disponibilidad" en la *Guía de administración de Cisco WebEx Meetings Server*). Si falla el sistema primario del sistema de alta disponibilidad, no puede repararlo mediante este procedimiento. Le recomendamos que restaure su sistema primario mediante el procedimiento de recuperación ante desastres y que, a continuación, agregue un nuevo sistema secundario. Hasta que agregue el nuevo sistema secundario, su despliegue funcionará sin redundancia completa. Este procedimiento ayuda a evitar interrupciones no planeadas en la red si fallara cualquiera de sus máquinas virtuales secundarias. Consulte "Utilizar la función de recuperación ante desastres" en la *Guía de administración de Cisco WebEx Meetings Server* para obtener más información.
- Establezca un sistema de archivos de red (NFS) y asegúrese de que tiene suficiente capacidad de almacenamiento para almacenar copias de seguridad automáticas regulares de su base de datos y de las grabaciones de sus reuniones. (CWMS es compatible con las versiones 2, 3 y 4 de NFS)
- Puesto que su sistema solo guarda la última copia de seguridad del sistema en el NFS y elimina las anteriores todos los días, le recomendamos que conserve varias copias de seguridad recientes en otros soportes.

Restricción No cree manualmente archivos ni directorios en el recurso compartido NFS utilizado por Cisco WebEx Meetings Server, ya que ejecuta varios scripts en archivos y directorios NFS. El servidor de almacenamiento NFS debe ser para uso exclusivo de Cisco WebEx Meetings Server.

- Use su escritorio para supervisar el estado del NFS, la CPU y el almacenamiento. Recomendamos activar las alarmas del escritorio para el almacenamiento y la CPU.
- Si tiene pensado utilizar la integración de directorios, consulte la sección Configuración de la integración de directorios en el capítulo "Administración de usuarios" de la *Guía de configuración de Cisco WebEx Meetings Server* para obtener más información.
- Cuando utilice Cisco WebEx Meetings Server, el troncal SIP relacionado en CUCM en la interfaz de Call Manager debería tener la casilla de verificación **Media Termination Point necesario** desmarcada en la página **Configuración de troncal**. Consulte Configurar un troncal SIP en un punto de equilibrio de carga, en la página 123 y Configurar un troncal SIP para un punto de aplicación, en la página 124 para obtener más detalles.
- Si realiza una actualización a Cisco WebEx Meetings Server versión 2.0 o superior y utiliza servidores blade de la serie B, deberá utilizar almacenamiento SAN para cumplir los requisitos de disco duro. Consulte Requisitos generales del sistema, en la página 1 para obtener más información sobre los requisitos de SAN.

CAPÍTULO 6

Configuración de Cisco Unified Communications Manager (CUCM)

- Configuración de Cisco Unified Communications Manager (CUCM), página 105
- Lista de comprobación de configuración de CUCM para sistemas con varios centros de datos, página 107
- Lista de comprobación de configuración de CUCM con o sin alta disponibilidad, página 108
- Configuración de CUCM en un sistema con varios centros de datos de CWMS, página 108
- Configurar CUCM para sistemas de alta disponibilidad y sistemas que no lo sean, página 111
- Configurar un perfil de seguridad de troncal SIP, página 117
- Configurar un perfil de SIP, página 118
- Administración de certificados CUCM utilizando TLS, página 119
- Configurar un troncal SIP, página 123
- Configuración de un grupo de rutas, página 125
- Configuración de una lista de rutas, página 126
- Configuración de un patrón de ruta, página 127
- Configuración de un patrón de ruta SIP, página 127
- Soporte y compatibilidad de la función CUCM, página 128

Configuración de Cisco Unified Communications Manager (CUCM)

Para permitir la teleconferencia en Cisco WebEx Meetings Server, debe configurar un sistema (o varios) Cisco Unified Communications Manager (CUCM) para gestionar el control de llamadas. Opcionalmente, puede configurar un segundo sistema CUCM para la alta disponibilidad de audio.

CUCM en un entorno MDC

Las configuraciones de CUCM en un entorno con varios centros de datos (MDC) son las mismas que en un entorno con un solo centro de datos (SDC) Los parámetros de configuración modificados en un centro de datos se ajustan de forma coincidente automáticamente en el otro centro de datos.

En CUCM, las configuraciones básicas en un entorno con varios centros de datos (MDC) son las mismas que en un entorno con un solo centro de datos (SDC) No obstante, debe configurar troncales a todos los centros de datos. Cada centro de datos puede tener un patrón de ruta diferente. Si desea utilizar más de un CUCM, cada centro de datos debe tener un troncal SIP al CUCM en los otros centros de datos para las llamadas a transferir.

Instrucciones antes de empezar

Obtenga su información de punto equilibrador de carga y punto de aplicación de la página **Audio** de su Cisco WebEx Meetings Server. Los puntos equilibradores de carga administran el equilibrio de carga de llamadas, mientras que los puntos de aplicación administran las llamadas, el flujo de conferencias y el control de funciones. Según el tamaño de los sistemas, tendrán distinta cantidad de puntos equilibradores de carga y de puntos de aplicación, y esas cantidades no están personalizadas. Inicie sesión en el sitio de administración y seleccione **Configuración** > **Audio** para consultar esta información.

- Tamaño (50/250/800/2000)
- Alta disponibilidad
- Tipo de transporte

En la página **Audio**, existe una "Tabla de configuración de SIP" donde se muestra información sobre el punto equilibrador de carga y el punto de aplicación, como las direcciones IP y los puertos. Esta tabla también se muestra en la página **Configuración de los ajustes de audio por primera vez**, que aparece la primera vez que configura sus ajustes de audio.

Para que CUCM funcione con Cisco WebEx Meetings Server, CUCM necesita la siguiente configuración específica y de base:

- Configuración de base

  Nota Estas configuraciones se pueden compartir entre varios sistemas Cisco WebEx Meetings Server.

  - Perfil de seguridad de troncal SIP
  - Perfil de SIP

- Configuración específica

  Nota Estas configuraciones deben realizarse para sistemas individuales de Cisco WebEx Meetings Server y no se pueden compartir entre varios sistemas.

  - Gestión de certificados
  - Troncal SIP

- Grupo de ruta
- Lista de rutas
- Patrón de ruta
- Patrón de ruta de SIP

Teleconferencia segura CUCM en un entorno MDC

Para proteger las teleconferencias, no se permite importar los certificados de todos los centros de datos de un sistema MDC en un solo CUCM cuando el nombre común de los certificados coincide.

De forma predeterminada, el nombre común para todos los centros de datos es el URL de sitio global del sistema. No obstante, para que el nombre común sea exclusivo, puede generar certificados utilizando Generación de una solicitud de firma de certificado (CSR) o Generación de un certificado autofirmado. Seleccione el URL del sitio local en lugar del URL del sitio global que se debe utilizar en el nombre común.

Los certificados autofirmados generados durante cualquier procedimiento que modifique el sistema (como el cambio del URL del sitio o de administración o el cambio de nombres de host) tienen como resultado un certificado que tiene el URL del sitio global en el nombre común, de modo que debe crear manualmente certificados con el URL del sitio local después de este tipo de operación.

Lista de comprobación de configuración de CUCM para sistemas con varios centros de datos

La lista de comprobación de configuración muestra el número de cada tipo de configuración de Cisco Unified Communication Manager (CUCM) que debe configurar para su sistema con varios centros de datos (MDC).

Tamaño del sistema	Perfiles de seguridad (Configuración base)	Perfiles de SIP (Configuración base)	Troncales SIP (Configuración específica)	Grupos de ruta (Configuración específica)	Listas de rutas (Configuración específica)	Patrones de ruta (Configuración específica)	Patrones de ruta de SIP (Configuración específica)
250 usuarios	2	1	4	1	1	N	2
800 usuarios	2	1	4	1	1	N	2
2000 usuarios con HA	2	1	6	1	1	N	4

Lista de comprobación de configuración de CUCM con o sin alta disponibilidad

La lista de comprobación de configuración muestra el número de cada tipo de configuración de Cisco Unified Communication Manager (CUCM) que debe configurar para su sistema de un solo centro de datos (SDC) con o sin alta disponibilidad (HA).

Tamaño del sistema	Perfiles de seguridad (Configuración base)	Perfiles de SIP (Configuración base)	Troncales SIP (Configuración específica)	Grupos de ruta (Configuración específica)	Listas de rutas (Configuración específica)	Patrones de ruta (Configuración específica)	Patrones de ruta de SIP (Configuración específica)
50 usuarios	2	1	2	1	1	N[21]	1
50 usuarios con HA	2	1	4	1	1	N	2
250 usuarios	2	1	2	1	1	N	1
250 usuarios con HA	2	1	4	1	1	N	2
800 usuarios	2	1	2	1	1	N	1
800 usuarios con HA	2	1	4	1	1	N	2
2000 usuarios	2	1	5	1	1	N	3
2000 usuarios con HA	2	1	6	1	1	N	4

21 N es la cantidad de Números de acceso de llamada directa que configure en Cisco WebEx Meetings Server.

Configuración de CUCM en un sistema con varios centros de datos de CWMS

Normalmente, cada sitio de un entorno con varios centros de datos (MDC) tiene un clúster CUCM dedicado asociado. Los grupos de CUCM se conectan utilizando troncales entre clústeres (ICT). Cada clúster CUCM de tiene troncales de llamada directa/marcación entrante al sitio de CWMS local. Se admite Session Manager Edition (SME). CWMS se puede configurar tras los clústeres CUCM locales. Cada CUCM tiene troncales SIP REFER a todas las máquinas virtuales multimedia del MDC.

Para ofrecer redundancia, cada clúster CUCM puede tener troncales INVITE a todos los centros de datos. El patrón de ruta de llamada directa da prioridad al troncal INVITE asociado con el centro de datos local y utiliza el troncal INVITE al centro de datos remoto solo cuando se produce un fallo.

Tabla 4: Troncales SIP de CUCM configurados en cada grupo de CUCM

Despliegue	Troncales INVITE: equilibrador de carga (MACC)	Troncales REFER: punto de aplicación (TAS)
Pequeña	2	2
Mediana	2	2
Grande	4	6

Configuración de CUCM en un sistema de 250 u 800 usuarios con varios centros de datos

Esta sección describe como configurar Cisco Unified Communication Manager (CUCM) para un sistema de 250 u 800 usuarios con varios centros de datos. Normalmente, cada centro de datos tiene un clúster CUCM local.

Información necesaria

- Una dirección IP de puntos de equilibrio de carga para cada centro de datos
- Una dirección IP de los puntos de aplicación para cada centro de datos
- La cantidad de números de acceso de llamada directa que configurará en su sistema

Procedimiento de configuración

Realice los siguientes pasos:

Tarea	Descripción	Información detallada
1	Revise el perfil de seguridad de troncal SIP existente y determine si cumple los requisitos de configuración de Cisco WebEx Meetings Server. Si no lo hace, configure dos perfiles de seguridad de troncal SIP.	Agregue un perfil de seguridad de troncal SIP para su punto de equilibrio de carga y agregue un perfil de seguridad de troncal SIP para su punto de aplicación. Consulte Configurar un perfil de seguridad de troncal SIP para un punto de equilibrio de carga, en la página 117 y Configurar un perfil de seguridad de troncal SIP para un punto de aplicación, en la página 118.
2	Revise el perfil de SIP existente y determine si cumple su requisito de configuración de Cisco WebEx Meetings Server. Si no lo hace, configure un perfil de SIP.	Configure un perfil de SIP tal como se describe en Configurar un perfil de SIP TLS o Configurar un perfil de SIP IPv6, en la página 119.

Tarea	Descripción	Información detallada
3	Configure dos troncales SIP para sus puntos de equilibrio de carga.	Consulte Configurar un troncal SIP en un punto de equilibrio de carga.
4	Configure dos troncales SIP para sus puntos de aplicación.	Consulte Configurar un troncal SIP para un punto de aplicación.
5	Configure un grupo de ruta utilizando el troncal SIP que ha configurado para su punto de equilibrio de carga en la Tarea 3, descrita anteriormente.	Consulte Configuración de un grupo de rutas.
6	Configure una lista de rutas utilizando el grupo de ruta que ha configurado en la Tarea 5, descrita anteriormente.	Consulte Configuración de una lista de rutas.
7	Configure *N* patrones de ruta utilizando la lista de rutas anterior. *N* es la cantidad de números de acceso de llamada de directa que ha configurado en los ajustes de audio en el sitio de administración.	Consulte Configuración de un patrón de ruta.
8	Configure dos patrones de ruta SIP para sus puntos de aplicación.	Consulte Configuración de un patrón de ruta SIP.

Configuración de CUCM en un sistema de 2000 usuarios con varios centros de datos

Esta sección describe como configurar Cisco Unified Communication Manager (CUCM) para un sistema de 2000 usuarios con varios centros de datos (MDC). Normalmente, cada centro de datos tiene un clúster CUCM local.

Información necesaria

- Dos direcciones IP de puntos de equilibrio de carga para cada centro de datos
- Tres direcciones IP de los puntos de aplicación para cada centro de datos
- La cantidad de números de acceso de llamada directa que piensa configurar en su sistema

Procedimiento de configuración

Realice los siguientes pasos:

Tarea	Descripción	Información detallada
1	Revise el perfil de seguridad de troncal SIP existente y determine si cumple los requisitos de configuración de Cisco WebEx Meetings Server. Si no lo hace, configure dos perfiles de seguridad de troncal SIP.	Agregue un perfil de seguridad de troncal SIP para su punto de equilibrio de carga y agregue un perfil de seguridad de troncal SIP para su punto de aplicación. Consulte Configurar un perfil de seguridad de troncal SIP para un punto de equilibrio de carga, en la página 117 y Configurar un perfil de seguridad de troncal SIP para un punto de aplicación, en la página 118.
2	Revise el perfil de SIP existente y determine si cumple su requisito de configuración de Cisco WebEx Meetings Server. Si no lo hace, configure un perfil de SIP.	Configure un perfil de SIP tal como se describe en Configurar un perfil de SIP TLS o Configurar un perfil de SIP IPv6, en la página 119.
3	Configure dos troncales SIP para sus puntos de equilibrio de carga.	Consulte Configurar un perfil de seguridad de troncal SIP para un punto de equilibrio de carga, en la página 117:
4	Configure cuatro troncales SIP para sus puntos de aplicación.	Consulte Configurar un perfil de seguridad de troncal SIP para un punto de aplicación, en la página 118:
5	Configure un grupo de ruta utilizando el troncal SIP que ha configurado para su punto de equilibrio de carga en la Tarea 3, descrita anteriormente.	Consulte Configuración de un grupo de rutas, en la página 125:
6	Configure una lista de rutas utilizando el grupo de ruta que ha configurado en la Tarea 5, descrita anteriormente.	Consulte Configuración de una lista de rutas, en la página 126:
7	Configure *N* patrones de ruta utilizando la lista de rutas anterior. *N* es la cantidad de números de acceso de llamada de directa que ha configurado en los ajustes de audio en el sitio de administración.	Consulte Configuración de un patrón de ruta, en la página 127:
8	Configure cuatro patrones de ruta SIP para sus puntos de aplicación.	Consulte Configuración de un patrón de ruta SIP, en la página 127:

Configurar CUCM para sistemas de alta disponibilidad y sistemas que no lo sean

Los apartados siguientes proporcionan una descripción de las tareas necesarias para configurar sistemas de alta disponibilidad y que no sean de alta disponibilidad de distintos tamaños.

Configuración de CUCM en sistemas de 50, 250 y 800 usuarios sin alta disponibilidad

En este apartado se describe la información necesaria y las instrucciones detalladas sobre cómo configurar sistemas CUCM para 50, 250 y 800 usuarios sin alta disponibilidad.

Información necesaria

- Una dirección IP de punto de equilibrio de carga
- Una dirección IP de punto de aplicación
- La cantidad de números de acceso de llamada directa que configurará en su sistema

Procedimiento de configuración

Realice los siguientes pasos:

Tarea	Descripción	Información detallada
1	Revise el perfil de seguridad de troncal SIP existente y determine si cumple los requisitos de configuración de Cisco WebEx Meetings Server. Si no lo hace, configure dos perfiles de seguridad de troncal SIP.	Agregue un perfil de seguridad de troncal SIP para su punto de equilibrio de carga y agregue un perfil de seguridad de troncal SIP para su punto de aplicación. Consulte Configurar un perfil de seguridad de troncal SIP para un punto de equilibrio de carga, en la página 117 y Configurar un perfil de seguridad de troncal SIP para un punto de aplicación, en la página 118.
2	Revise el perfil de SIP existente y determine si cumple su requisito de configuración de Cisco WebEx Meetings Server. Si no lo hace, configure un perfil de SIP.	Configure un perfil de SIP tal como se describe en Configurar un perfil de SIP TLS o Configurar un perfil de SIP IPv6, en la página 119.
3	Configure un troncal SIP para su punto de equilibrio de carga.	Consulte Configurar un troncal SIP en un punto de equilibrio de carga.
4	Configure un troncal SIP para su punto de aplicación.	Consulte Configurar un troncal SIP para un punto de aplicación.
5	Configure un grupo de ruta utilizando el troncal SIP que ha configurado para su punto de equilibrio de carga en la Tarea 3, descrita anteriormente.	Consulte Configuración de un grupo de rutas.
6	Configure una lista de rutas utilizando el grupo de ruta que ha configurado en la Tarea 5, descrita anteriormente.	Consulte Configuración de una lista de rutas.

Tarea	Descripción	Información detallada
7	Configure *N* patrones de ruta utilizando la lista de rutas anterior. *N* es la cantidad de números de acceso de llamada de directa que ha configurado en los ajustes de audio en el sitio de administración.	Consulte Configuración de un patrón de ruta.
8	Configure un patrón de ruta SIP para su punto de aplicación.	Consulte Configuración de un patrón de ruta SIP.

Configuración de CUCM en sistemas de 50, 250 u 800 usuarios con alta disponibilidad

En este apartado se describe la información necesaria y las instrucciones detalladas sobre cómo configurar sistemas CUCM para 50, 250 u 800 usuarios con alta disponibilidad.

Información necesaria

- Dos direcciones IP de puntos de equilibrio de carga
- Dos direcciones IP de puntos de aplicación
- La cantidad de números de acceso de llamada directa que configurará en su sistema

Procedimiento de configuración

Realice los siguientes pasos:

Tarea	Descripción	Información detallada
1	Revise el perfil de seguridad de troncal SIP existente y determine si cumple los requisitos de configuración de Cisco WebEx Meetings Server. Si no lo hace, configure dos perfiles de seguridad de troncal SIP.	Agregue un perfil de seguridad de troncal SIP para su punto de equilibrio de carga y agregue un perfil de seguridad de troncal SIP para su punto de aplicación. Consulte Configurar un perfil de seguridad de troncal SIP para un punto de equilibrio de carga, en la página 117 y Configurar un perfil de seguridad de troncal SIP para un punto de aplicación, en la página 118.
2	Revise el perfil de SIP existente y determine si cumple su requisito de configuración de Cisco WebEx Meetings Server. Si no lo hace, configure un perfil de SIP.	Configure un perfil de SIP tal como se describe en Configurar un perfil de SIP TLS o Configurar un perfil de SIP IPv6, en la página 119.
3	Configure dos troncales SIP para sus puntos de equilibrio de carga.	Consulte Configurar un troncal SIP en un punto de equilibrio de carga.
4	Configure dos troncales SIP para sus puntos de aplicación.	Consulte Configurar un troncal SIP para un punto de aplicación.

Tarea	Descripción	Información detallada
5	Configure un grupo de ruta utilizando el troncal SIP que ha configurado para su punto de equilibrio de carga en la Tarea 3, descrita anteriormente.	Consulte Configuración de un grupo de rutas.
6	Configure una lista de rutas utilizando el grupo de ruta que ha configurado en la Tarea 5, descrita anteriormente.	Consulte Configuración de una lista de rutas.
7	Configure *N* patrones de ruta utilizando la lista de rutas anterior. *N* es la cantidad de números de acceso de llamada de directa que ha configurado en los ajustes de audio en el sitio de administración.	Consulte Configuración de un patrón de ruta.
8	Configure dos patrones de ruta SIP para sus puntos de aplicación.	Consulte Configuración de un patrón de ruta SIP.

Configuración de CUCM en sistemas de 2000 usuarios sin alta disponibilidad

Esta sección describe como configurar Cisco Unified Communication Manager (CUCM) para un sistema de 2000 usuarios sin alta disponibilidad.

Información necesaria

- Dos direcciones IP de puntos de equilibrio de carga
- Tres direcciones IP de puntos de aplicación
- La cantidad de números de acceso de llamada directa que configurará en su sistema

Procedimiento de configuración

Realice los siguientes pasos:

Tarea	Descripción	Información detallada
1	Revise el perfil de seguridad de troncal SIP existente y determine si cumple los requisitos de configuración de Cisco WebEx Meetings Server. Si no lo hace, configure dos perfiles de seguridad de troncal SIP.	Agregue un perfil de seguridad de troncal SIP para su punto de equilibrio de carga y agregue un perfil de seguridad de troncal SIP para su punto de aplicación. Consulte Configurar un perfil de seguridad de troncal SIP para un punto de equilibrio de carga, en la página 117 y Configurar un perfil de seguridad de troncal SIP para un punto de aplicación, en la página 118.
2	Revise el perfil de SIP existente y determine si cumple su requisito de configuración de Cisco WebEx Meetings Server. Si no lo hace, configure un perfil de SIP.	Configure un perfil de SIP tal como se describe en Configurar un perfil de SIP TLS o Configurar un perfil de SIP IPv6, en la página 119.

Tarea	Descripción	Información detallada
3	Configure dos troncales SIP para sus puntos de equilibrio de carga.	Consulte Configurar un perfil de seguridad de troncal SIP para un punto de equilibrio de carga, en la página 117:
4	Configure tres troncales SIP para sus puntos de aplicación.	Consulte Configurar un perfil de seguridad de troncal SIP para un punto de aplicación, en la página 118:
5	Configure un grupo de ruta utilizando el troncal SIP que ha configurado para su punto de equilibrio de carga en la Tarea 3, descrita anteriormente.	Consulte Configuración de un grupo de rutas, en la página 125:
6	Configure una lista de rutas utilizando el grupo de ruta que ha configurado en la Tarea 5, descrita anteriormente.	Consulte Configuración de una lista de rutas, en la página 126:
7	Configure *N* patrones de ruta utilizando la lista de rutas anterior. *N* es la cantidad de números de acceso de llamada de directa que ha configurado en los ajustes de audio en el sitio de administración.	Consulte Configuración de un patrón de ruta, en la página 127:
8	Configure tres patrones de ruta SIP para sus puntos de aplicación.	Consulte Configuración de un patrón de ruta SIP, en la página 127:

Configuración de CUCM en sistemas de 2000 usuarios con alta disponibilidad

Esta sección describe como configurar Cisco Unified Communication Manager (CUCM) para un sistema de 2000 usuarios con alta disponibilidad.

Información necesaria

- Dos direcciones IP de puntos de equilibrio de carga
- Cuatro direcciones IP de puntos de aplicación
- La cantidad de números de acceso de llamada directa que configurará en su sistema

Procedimiento de configuración

Realice los siguientes pasos:

Tarea	Descripción	Información detallada
1	Revise el perfil de seguridad de troncal SIP existente y determine si cumple los requisitos de configuración de Cisco WebEx Meetings Server. Si no lo hace, configure dos perfiles de seguridad de troncal SIP.	Agregue un perfil de seguridad de troncal SIP para su punto de equilibrio de carga y agregue un perfil de seguridad de troncal SIP para su punto de aplicación. Consulte Configurar un perfil de seguridad de troncal SIP para un punto de equilibrio de carga, en la página 117 y Configurar un perfil de seguridad de troncal SIP para un punto de aplicación, en la página 118.
2	Revise el perfil de SIP existente y determine si cumple su requisito de configuración de Cisco WebEx Meetings Server. Si no lo hace, configure un perfil de SIP.	Configure un perfil de SIP tal como se describe en Configurar un perfil de SIP TLS o Configurar un perfil de SIP IPv6, en la página 119.
3	Configure dos troncales SIP para sus puntos de equilibrio de carga.	Consulte Configurar un perfil de seguridad de troncal SIP para un punto de equilibrio de carga, en la página 117:
4	Configure cuatro troncales SIP para sus puntos de aplicación.	Consulte Configurar un perfil de seguridad de troncal SIP para un punto de aplicación, en la página 118:
5	Configure un grupo de ruta utilizando el troncal SIP que ha configurado para su punto de equilibrio de carga en la Tarea 3, descrita anteriormente.	Consulte Configuración de un grupo de rutas, en la página 125:
6	Configure una lista de rutas utilizando el grupo de ruta que ha configurado en la Tarea 5, descrita anteriormente.	Consulte Configuración de una lista de rutas, en la página 126:
7	Configure *N* patrones de ruta utilizando la lista de rutas anterior. *N* es la cantidad de números de acceso de llamada de directa que ha configurado en los ajustes de audio en el sitio de administración.	Consulte Configuración de un patrón de ruta, en la página 127:
8	Configure cuatro patrones de ruta SIP para sus puntos de aplicación.	Consulte Configuración de un patrón de ruta SIP, en la página 127:

Configurar un perfil de seguridad de troncal SIP

Configurar un perfil de seguridad de troncal SIP para un punto de equilibrio de carga

Antes de comenzar

Si su sistema Cisco WebEx Meetings Server está configurado para TLS, debe importar un certificado de teleconferencias seguras. Para obtener más información, consulte la sección "Importación de certificados seguros de teleconferencia" de la *Guía de administración de Cisco WebEx Meetings Server* en http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html.

Paso 1 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre completo del dominio o la dirección IP del servidor de Cisco Unified Communications Manager.

Paso 2 Seleccione **Administración de Cisco Unified CM**.

Paso 3 Seleccione **Sistema** > **Seguridad** > **Perfil de seguridad de troncal SIP**.

Paso 4 Seleccione **Agregar nuevo**.

Paso 5 Configure los siguientes campos.

- Nombre: introduzca un nombre para identificar su perfil de seguridad de troncal SIP.
- Modo seguridad dispositivo: seleccione introduzca **No seguro** si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante UDP/TCP. Seleccione **Cifrado** si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante TLS.
- Nombre de asunto X.509: introduzca el nombre de su certificado si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante TLS.

  Nota Si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante TLS, un sistema Cisco WebEx Meetings Server diferente no puede compartir el mismo perfil de seguridad de troncal SIP porque cada sistema debe tener un certificado distinto. Obtenga el nombre de certificado de Cisco WebEx Meetings Server desde el sitio de administración. Si desea más información, consulte "Gestionar certificados" en la *Guía de administración*.
- Puerto de entrada: introduzca 5060 si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante UDP/TCP. Introduzca 5061 si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante TLS.

Nota No configure ningún otro de los campos de la página; deje los valores predeterminados.

Paso 6 Seleccione **Guardar**.

Configurar un perfil de seguridad de troncal SIP para un punto de aplicación

Antes de comenzar

Si su sistema Cisco WebEx Meetings Server está configurado para TLS, debe importar un certificado de teleconferencias seguras. Para obtener más información, consulte la sección "Importación de certificados seguros de teleconferencia" de la *Guía de administración de Cisco WebEx Meetings Server* en http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html.

Paso 1 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre completo del dominio o la dirección IP del servidor de Cisco Unified Communications Manager.

Paso 2 Seleccione **Administración de Cisco Unified CM**.

Paso 3 Seleccione **Sistema** > **Seguridad** > **Perfil de seguridad de troncal SIP**.

Paso 4 Seleccione **Agregar nuevo**.

Paso 5 Configure los siguientes campos:

- Nombre: introduzca un nombre para identificar su perfil de seguridad de troncal SIP.
- Modo seguridad dispositivo: seleccione introduzca **No seguro** si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante UDP/TCP. Seleccione **Cifrado** si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante TLS.
- Nombre de asunto X.509: introduzca el nombre de su certificado si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante TLS.

  Nota Si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante TLS, un sistema Cisco WebEx Meetings Server diferente no puede compartir el mismo perfil de seguridad de troncal SIP porque cada sistema debe tener un certificado distinto. Obtenga el nombre de certificado de Cisco WebEx Meetings Server desde el sitio de administración. Si desea más información, consulte "Gestionar certificados" en la *Guía de administración*.
- Puerto de entrada: introduzca 5062 si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante UDP/TCP. Introduzca 5063 si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante TLS.

Nota No configure ningún otro de los campos de la página; deje los valores predeterminados.

Paso 6 Seleccione **Guardar**.

Configurar un perfil de SIP

Configurar un perfil de SIP estándar

El perfil del protocolo de inicio de sesiones (Session Initiation Protocol, SIP) estándar utiliza la configuración predeterminada y no requiere ningún paso de configuración adicional.

Configurar un perfil de SIP TLS

Paso 1 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre completo del dominio o la dirección IP del servidor de Cisco Unified Communications Manager.

Paso 2 Seleccione **Administración de Cisco Unified CM**.

Paso 3 Seleccione **Dispositivo** > **Configuración de dispositivo** > **Perfil SIP**.

Paso 4 Seleccione **Agregar nuevo**.

Paso 5 Configure los siguientes campos:

- Nombre: introduzca un nombre para su perfil de SIP.
- Redireccionamiento mediante aplicación: seleccione esta casilla.

No configure ningún otro de los campos de la página; deje los valores predeterminados en los campos.

Paso 6 Seleccione **Guardar**.

Configurar un perfil de SIP IPv6

Paso 1 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre completo del dominio o la dirección IP del servidor de Cisco Unified Communications Manager.

Paso 2 Seleccione **Administración de Cisco Unified CM**.

Paso 3 Seleccione **Dispositivo** > **Configuración de dispositivo** > **Perfil SIP**.

Paso 4 Seleccione **Agregar nuevo**.

Paso 5 Configure los siguientes campos:

- Nombre: introduzca un nombre para su perfil de SIP.
- Activar NAT: seleccione la casilla.

No configure ningún otro de los campos de la página; deje los valores predeterminados en los campos.

Paso 6 Seleccione **Guardar**.

Administración de certificados CUCM utilizando TLS

Si desea que Cisco Unified Communications Manager (CUCM) se comunique con Cisco WebEx Meetings Server (CWMS) utilizando TLS, debe realizar las acciones siguientes:

- Obtenga un certificado CWMS del sitio de administración y súbalo a CUCM.

Nota Si CWMS utiliza certificados de terceros, entonces todos los certificados de la cadena de certificados se deben subir a CUCM.

- Descargue su certificado CUCM y luego súbalo al sitio de administración de CWMS.

Nota Si CUCM utiliza certificados de terceros, solo se tiene que subir el último certificado de la cadena de certificados (certificado de la entidad emisora de certificados raíz (CA} a Cisco WebEx Meetings Server.

Si utiliza TLS para conectar todos los centros de datos en un sistema con varios centros de datos (MDC) al mismo CUCM, CWMS no puede utilizar el URL del sitio común para el nombre común del certificado. Debe utilizar el URL del sitio local de cada centro de datos para cada nombre común de certificado, porque CUCM 10.5 y las versiones anteriores tratan varios certificados con un nombre común como el mismo certificado. Si los nombres no son diferentes, el segundo certificado de centro de datos sustituye el primer certificado de centro de datos después de cargar el segundo certificado de centro de datos en CUCM.

Consulte "Administración de certificados" en la *Guía de administración* para obtener más información. Consulte http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html para obtener más detalles.

Cargar certificados de Cisco WebEx Meetings Server

Paso 1 Descargue y exporte su certificado de Cisco WebEx Meetings Server.
a) Inicie sesión en el sitio de administración de Cisco WebEx Meetings Server.
b) Seleccione **Configuración** > **Seguridad** > **Certificados**.
c) Copie el nombre del certificado del apartado Certificado SSL.
d) Seleccione **Más opciones** > **Exportar certificado SSL**.
e) Guarde el certificado en su unidad de disco duro local.

Paso 2 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre completo del dominio o la dirección IP del servidor de Cisco Unified Communications Manager.

Paso 3 Seleccione **Administración de SO Cisco Unified**.

Paso 4 Seleccione **Seguridad** > **Gestión de certificados**.

Paso 5 Seleccione **Cargar certificado/cadena de certificados**.

Paso 6 Seleccione **CallManager-trust** en el menú desplegable Nombre de certificado.

Paso 7 Seleccione el botón **Examinar** y seleccione el certificado que ha guardado en su disco duro local.

Paso 8 Seleccione **Cargar archivo**.

El sistema muestra el mensaje "Correcto: Certificado cargado".

Paso 9 (Opcional) Si Cisco WebEx Meetings Server utiliza certificados autofirmados, repita los pasos del 4 al 8 para cargar el certificado intermedio y el certificado de la entidad emisora de certificados raíz (CA) de la cadena de certificados.

Paso 10 Seleccione **Cerrar**.

Qué hacer a continuación

Para obtener más información sobre los certificados, consulte la sección "Gestión de certificados" en la *Guía de administración* en http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Instalación de un certificado CUCM de terceros

Este procedimiento explica cómo cargar un certificado de tercero a Cisco WebEx Meetings Server.

Antes de comenzar

- Genere una solicitud de firma de certificado (CSR) y envíela a una entidad externa emisora de certificados para solicitar certificados. Consulte Generación de una solicitud de firma de certificado (CSR) para obtener instrucciones.
- La entidad emisora de certificados le enviará una cadena de certificado que puede tener lo siguiente:
  - Certificado 1 (usuario final): emitido por una entidad de certificados intermedia a una entidad de usuario final.
  - Certificado 2 (intermedia): emitido por una entidad emisora de certificados raíz a una autoridad de certificados intermedia.
  - Certificado 3 (entidad emisora de certificados raíz): emitido por la entidad emisora de certificados raíz.
- Cuando recibe múltiples certificados en una cadena de certificados, debe concatenar los tres certificados en un archivo, con el certificado de usuario final primero.

Paso 1 Importe el archivo del certificado de terceros en Cisco WebEx Meetings Server. Consulte Importación de un certificado SSL para obtener instrucciones.

Paso 2 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre completo del dominio o la dirección IP del servidor de Cisco Unified Communications Manager.

Paso 3 Seleccione **Administración de SO Cisco Unified**.

Paso 4 Seleccione **Seguridad** > **Gestión de certificados**.

Paso 5 Seleccione **Cargar certificado/cadena de certificados**.

Paso 6 Seleccione **CallManager-trust** en el menú desplegable Nombre de certificado.

Paso 7 Seleccione el botón **Examinar** y seleccione el certificado de la entidad emisora de certificados raíz (CA) que ha guardado en su disco duro local.

Es el último certificado de autofirma de la cadena de verificación, que se utiliza para comprobar el certificado CallManager.pem.

Nota Puede obtener el certificado de CA raíz de una autoridad emisora de certificados directamente, al mismo tiempo que se crea el certificado CallManager.pem.

Paso 8 Seleccione **Cargar archivo**.
Espere a que su sistema indique "Correcto: Certificado cargado".

Paso 9 Seleccione **Cerrar**.

Qué hacer a continuación

Para obtener más información sobre los certificados, consulte la sección "Gestión de certificados" en la *Guía de administración* en http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Descargar certificados CUCM

Este procedimiento solamente es necesario si CUCM utiliza certificados autofirmados. Si CUCM utiliza certificados de terceros, debe cargar solamente el último certificado (certificado CA raíz) de la cadena de certificados en el Cisco WebEx Meeting Server. Póngase en contacto con su entidad emisora de certificados (CA) para obtener información sobre cómo obtener un certificado CA raíz.

Consulte su documentación CUCM para obtener más información acerca de cómo generar certificados CUCM.

Paso 1 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre completo del dominio o la dirección IP del servidor de Cisco Unified Communications Manager.

Paso 2 Seleccione **Administración de SO Cisco Unified**.

Paso 3 Seleccione **Seguridad** > **Gestión de certificados**.

Paso 4 Busque el certificado en el campo "Nombre de certificado" con el nombre "CallManager". Seleccione el campo "Archivo .PEM".

Paso 5 Seleccione **Descargar** para guardar el certificado CUCM `CallManager.pem` en su disco duro local.

Qué hacer a continuación

Para obtener más información sobre la carga de certificados de CUCM en Cisco WebEx Meetings Server, consulte la "Administración de certificados" en la *Guía de administración*. Consulte http://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.html:

Configurar un troncal SIP

Configurar un troncal SIP en un punto de equilibrio de carga

Paso 1 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre completo del dominio o la dirección IP del servidor de Cisco Unified Communications Manager.

Paso 2 Seleccione **Administración de Cisco Unified CM**.

Paso 3 Seleccione **Dispositivo** > **Troncal**.

Paso 4 Seleccione **Agregar nuevo**.

Paso 5 En el menú desplegable **Tipo de troncal**, seleccione **Troncal SIP**.

Nota No cambie ninguno de los demás campos de la página. Déjelos con sus valores predeterminados.

Nota Deje la casilla de verificación **Media Termination Point necesario** desmarcada en la página **Configuración del troncal** cuando CUCM se esté comunicando con Cisco WebEx Meeting Server. Si no está utilizando Cisco WebEx Meetings Server con audio CUCM SIP, puede seleccionar la casilla de verificación **Media Termination Point necesario** a la hora de suministrar servicios telefónicos usando una infraestructura PBX de terceros.

Paso 6 Seleccione **Siguiente**.

Paso 7 Configure los siguientes campos:

- Nombre de dispositivo: introduzca un nombre para su troncal SIP.
- Grupo de dispositivos: seleccione un grupo de dispositivos adecuado del menú desplegable.

  Para determinar qué grupo de Cisco Unified Communications Manager Group se ha configurado en el grupo de dispositivos, seleccione **Sistema** > **Grupo de dispositivos**. Para comprobar qué Cisco Unified Communications Managers forma parte de este grupo, seleccione **Sistema** > **Cisco Unified CM Group**.

  Nota Registre las direcciones IP del servidor primario y secundario. Tendrá que introducir estas direcciones IP al configurar sus ajustes de audio en Cisco WebEx Meetings Server. Consulte "Configuración de los ajustes de audio por primera vez" en la *Guía de administración* para obtener más información. Consulte las Guías de instalación y actualización de Cisco WebEx Meetings Server.
- Dirección de destino: introduzca la dirección IPv4 de su punto de equilibrio de carga. Consulte la tabla Configuración de SIP en su página Audio del sitio de Administración la dirección IP.
- Dirección IPv6 de destino: introduzca la dirección IPv6 de su punto de equilibrio de carga si desea activar IPv6 entre CUCM y Cisco WebEx Meetings Server.
- Puerto de destino: introduzca 5060 si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante UDP/TCP. Introduzca 5061 si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante TLS.
- Perfil de seguridad de troncal SIP: seleccione el perfil de seguridad del punto de equilibrio de carga en el menú desplegable.
- Perfil de SIP: seleccione **Perfil de SIP estándar** si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante UDP/TCP. Seleccione **Perfil de SIP TLS** si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante TLS. Seleccione **Perfil de SIP IPv6** si desea activar IPv6 entre CUCM y Cisco WebEx Meetings Server.

- Espacio de búsqueda de llamadas: seleccione un espacio de búsqueda de llamadas que pueda llamar a los números de teléfono y patrones de ruta configurados en CUCM a los que desee que Cisco WebEx Meetings Server devuelva la llamada. Seleccione **Enrutamiento de llamadas** > **Clase de control** > **Espacio de búsqueda de llamadas**. Un espacio de búsqueda de llamadas está formado por una lista ordenada de las particiones de ruta que se asignan típicamente a los dispositivos o patrones de ruta. Los espacios de búsqueda de llamadas determinan las particiones que los dispositivos de llamada pueden buscar cuando intentan completar una llamada. Si desea obtener más información, consulte el apartado "Configuración de espacios de búsqueda de llamadas" de la *Guía de administración de Cisco Unified Communications Manager* o la sección "Particiones y espacios de búsqueda de llamadas" de la *Guía del sistema de Cisco Unified Communications Manager*.
- Espacio de búsqueda de llamadas de reenrutamiento: seleccione un espacio de búsqueda de llamadas que contenga la partición de ruta que esté configurada para el patrón de ruta de SIP en la sección "Configuración de un patrón de ruta SIP" que encontrará más adelante. Si se configura como **< None >**, entonces solo podrá dirigir las llamadas a los patrones de ruta que tengan una partición configurada como **< None >**, por lo que el patrón de ruta de SIP necesitará tener la partición de ruta configurada como **< None >**. Esta configuración es necesaria para entrar en reuniones de Cisco WebEx Meetings Server. Si desea obtener más información, consulte el apartado "Configuración de espacios de búsqueda de llamadas" de la *Guía de administración de Cisco Unified Communications Manager* o la sección "Particiones y espacios de búsqueda de llamadas" de la *Guía del sistema de Cisco Unified Communications Manager*.

Nota No cambie ninguno de los demás campos de la página. Déjelos con sus valores predeterminados.

Paso 8 Seleccione **Guardar**.

Paso 9 Seleccione **Restablecer** y, a continuación, seleccione **Restablecer y reiniciar** en la ventana emergente.
Debe restablecer el troncal SIP para completar su configuración.

Configurar un troncal SIP para un punto de aplicación

Paso 1 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre completo del dominio o la dirección IP del servidor de Cisco Unified Communications Manager.

Paso 2 Seleccione **Administración de Cisco Unified CM**.

Paso 3 Seleccione **Dispositivo** > **Troncal**.

Paso 4 Seleccione **Agregar nuevo**.

Paso 5 En el menú desplegable **Tipo de troncal**, seleccione **Troncal SIP**.
Nota No cambie ningún otro campo en esta página; deje los valores predeterminados.

Paso 6 Seleccione **Siguiente**.

Paso 7 Configure los siguientes campos:

- Nombre de dispositivo: introduzca un nombre para su troncal SIP.
- Grupo de dispositivos: seleccione **Predeterminado** en el menú desplegable.
- Dirección de destino: introduzca la dirección IPv4 de su punto de aplicación.

- Dirección IPv6 de destino: introduzca la dirección IPv6 de su punto de aplicación si desea activar IPv6 entre CUCM y Cisco WebEx Meetings Server.
- Puerto de destino: introduzca 5062 si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante UDP/TCP. Introduzca 5063 si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante TLS.
- Perfil de seguridad de troncal SIP: seleccione el perfil de seguridad del punto de aplicación en el menú desplegable.
- Perfil de SIP: seleccione **Perfil de SIP estándar** si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante UDP/TCP. Seleccione **Perfil de SIP TLS** si desea que CUCM se comunique con Cisco WebEx Meetings Server mediante TLS. Seleccione **Perfil de SIP IPv6** si desea activar IPv6 entre CUCM y Cisco WebEx Meetings Server.
- Espacio de búsqueda de llamadas: seleccione un espacio de búsqueda de llamadas que pueda llamar a los números de teléfono y patrones de ruta configurados en CUCM a los que desee que Cisco WebEx Meetings Server pueda llamar. Seleccione **Enrutamiento de llamadas** > **Clase de control** > **Espacio de búsqueda de llamadas**. Un espacio de búsqueda de llamadas está formado por una lista ordenada de las particiones de ruta que se asignan típicamente a los dispositivos o patrones de ruta. Los espacios de búsqueda de llamadas determinan las particiones que los dispositivos de llamada pueden buscar cuando intentan completar una llamada. Si se configura como **< None >**, solo se podrá llamar a dispositivos o patrones de ruta con una partición configurada como **< None >**. Si desea obtener más información, consulte el apartado *Configuración de espacios de búsqueda de llamadas* de la *Guía de administración de Cisco Unified Communications Manager* o la sección *Particiones y espacios de búsqueda de llamadas* de la *Guía del sistema de Cisco Unified Communications Manager*.

Nota No cambie ningún otro campo en esta página; deje los valores predeterminados.

Nota Deje la casilla de verificación **Media Termination Point necesario** desmarcada en la página **Configuración del troncal** cuando CUCM se esté comunicando con Cisco WebEx Meeting Server. Si no está utilizando Cisco WebEx Meetings Server con audio CUCM SIP, puede seleccionar la casilla de verificación **Media Termination Point necesario** a la hora de suministrar servicios telefónicos usando una infraestructura PBX de terceros.

Paso 8 Seleccione **Guardar**.

Paso 9 Seleccione **Restablecer** y, a continuación, seleccione **Restablecer y reiniciar** en la ventana emergente.
Debe restablecer el troncal SIP para completar la configuración.

Configuración de un grupo de rutas

Paso 1 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre completo del dominio o la dirección IP del servidor de Cisco Unified Communications Manager.

Paso 2 Seleccione **Administración de Cisco Unified CM**.

Paso 3 Seleccione **Enrutamiento de llamadas** > **Ruta/Extensión** > **Grupo de rutas**.

Paso 4 Seleccione **Agregar nuevo**.

Paso 5 Configure los siguientes campos

- Nombre de grupo ruta: introduzca un nombre para su grupo de rutas.

- Algoritmo de distribución. Seleccione **Circular** en el menú desplegable.

  Nota Si selecciona **Circular**, permite a CUCM distribuir una llamada a usuarios inactivos o disponibles empezando desde el miembro (N+1) de un grupo de ruta, donde el miembro N es el último miembro al que CUCM ha ampliado una llamada. Si el miembro N es el último miembro de un grupo de ruta, CUCM distribuye una llamada empezando desde el principio del grupo de ruta.

- Encontrar dispositivos para agregar a grupo de ruta: seleccione el **Troncal SIP del punto de equilibrio de carga** en la lista Dispositivos disponibles. A continuación, seleccione **Agregar a grupo de ruta**.

Nota No cambie ninguno de los demás campos de la página. Déjelos con sus valores predeterminados.

Paso 6 Seleccione **Guardar**.

Qué hacer a continuación

Cree una lista de rutas para su grupo de ruta. Vaya a Configuración de una lista de rutas, en la página 126.

Configuración de una lista de rutas

Paso 1 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre completo del dominio o la dirección IP del servidor de Cisco Unified Communications Manager.

Paso 2 Seleccione **Administración de Cisco Unified CM**.

Paso 3 Seleccione **Enrutamiento de llamadas** > **Ruta/Extensión** > **Lista de rutas**.

Paso 4 Seleccione **Agregar nuevo**.

Paso 5 Configure los siguientes campos

- Nombre: introduzca un nombre para su lista de rutas.
- Grupo de Cisco Unified Communications Manager: seleccione **Predeterminado** en el menú desplegable.

Nota No cambie ningún otro campo en esta página; deje los valores predeterminados en los campos.

Paso 6 Seleccione **Guardar**.

Paso 7 Seleccione **Agregar grupo de ruta**.
Aparecerá la página **Configuración de detalles de la lista de rutas**.

Paso 8 Seleccione el grupo de ruta configurado previamente en el menú desplegable **Grupo de ruta** y seleccione **Guardar**.
Aparece la página **Configuración de lista de rutas**.

Paso 9 Seleccione **Guardar**.

Qué hacer a continuación

Configure un patrón de ruta para su lista de rutas. Vaya a Configuración de un patrón de ruta, en la página 127.

Configuración de un patrón de ruta

Paso 1 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre completo del dominio o la dirección IP del servidor de Cisco Unified Communications Manager.

Paso 2 Seleccione **Administración de Cisco Unified CM**.

Paso 3 Seleccione **Enrutamiento de llamadas** > **Ruta/Extensión** > **Patrón de ruta**.

Paso 4 Seleccione **Agregar nuevo**.

Paso 5 Configure los siguientes campos

- **Patrón de ruta**: introduzca un nombre para su patrón de ruta.

  Nota Añada un patrón de ruta para cada grupo de Blast Dial. Registre este nombre porque tendrá que introducirlo en la página de administración en **Configuración** > **Audio** > **Grupo de Blast Dial** cuando cree un grupo de llamada general.

- **Partición de ruta**: seleccione una partición de ruta de acceso para los teléfonos o dispositivos que puedan llamar a Cisco WebEx Meetings Server. Si se configura como **< None >**, cualquier dispositivo configurado en CUCM podría llamar a Cisco WebEx Meetings Server. Si desea obtener más información, consulte el apartado "Configuración de espacios de búsqueda de llamadas" de la *Guía de administración de Cisco Unified Communications Manager* o la sección "Particiones y espacios de búsqueda de llamadas" de la *Guía del sistema de Cisco Unified Communications Manager*.
- **Lista de pasarelas/rutas**: seleccione la lista de rutas configurada previamente en el menú desplegable.

Nota No cambie ningún otro campo en esta página; deje los valores predeterminados en los campos.

Paso 6 Seleccione **Guardar**.

Configuración de un patrón de ruta SIP

Paso 1 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre completo del dominio o la dirección IP del servidor de Cisco Unified Communications Manager.

Paso 2 Seleccione **Administración de Cisco Unified CM**.

Paso 3 Seleccione **Enrutamiento de llamadas** > **Patrón de ruta de SIP**.

Paso 4 Seleccione **Agregar nuevo**.

Paso 5 Configure los siguientes campos

- Partición de ruta: seleccione una partición de ruta que esté incluida en el espacio de búsqueda de llamadas y que esté configurada como espacio de búsqueda de llamadas de reenrutamiento en la sección anterior "Configurar un troncal SIP para un punto de aplicación". Si se configura como **< None >**, entonces el espacio de búsqueda de llamadas de reenrutamiento configurado para el troncal SIP para un punto de aplicación debe estar definido como **< None >**. Si desea obtener más información, consulte el apartado "Configuración de espacios de búsqueda de

llamadas" de la *Guía de administración de Cisco Unified Communications Manager* o la sección "Particiones y espacios de búsqueda de llamadas" de la *Guía del sistema de Cisco Unified Communications Manager*.

- Uso de patrón: seleccione **Direccionamiento de dirección IP**.
- Patrón IPv4: introduzca la dirección IP del punto de aplicación. Consulte la tabla Configuración de SIP en su página Audio del sitio de Administración la dirección IP.
- Troncal SIP: seleccione el troncal SIP configurado previamente para el punto de aplicación en el menú desplegable.

Nota No cambie ningún otro campo en esta página; deje los valores predeterminados en los campos.

Paso 6 Seleccione **Guardar**.

Soporte y compatibilidad de la función CUCM

Compatibilidad de la función CUCM

Cisco WebEx Meetings Server (CWMS) es compatible con Cisco Unified Call Manager (CUCM) 8.6 o 9.0 sin TLS/SRTP, y CUCM 9.1, 10.0 o 10.5.

Importante Las conexiones TLS entre CUCM y CWMS fallan con las versiones antiguas de CUCM que no admiten certificados firmados con un algoritmo de firma SHA256 con cifrado RSA.

Actualice de CUCM a una versión compatible con este algoritmo de firma u obtenga un certificado de terceros firmado con SHA1 con cifrado RSA. Según la última recomendación del Instituto Nacional de Normas y Tecnología (National Institute of Standards and Technology, NIST), SHA1 ya no se debe utilizar para la generación de firmas digitales porque tiene una vulnerabilidad de seguridad.

En la tabla siguiente se especifica la compatibilidad de la función para las versiones admitidas de CUCM. La capacidad del sistema Cisco WebEx Meetings Server no se ve afectada por ninguna de sus opciones de configuración.

Nota CWMS no es compatible con las versiones de CUCM no especificadas, ni con las aplicaciones de gestión de proxy SIP de otros fabricantes.

Característica	CUCM 9.1	CUCM 10.0	CUCM 10.5	CUCM 11.0	Condiciones previas/Notas
Devolución de llamada (IPv6)	Sí	Sí	Sí	Sí	Configure CWMS con direcciones IPv6 durante el proceso de instalación.

Característica	CUCM 9.1	CUCM 10.0	CUCM 10.5	CUCM 11.0	Condiciones previas/Notas
Llamada entrante (IPv6)	Sí	Sí	Sí	Sí	Configure CWMS con direcciones IPv6 durante el proceso de instalación.
TLS/SRTP	Sí	Sí	Sí	Sí	Configure los certificados de seguridad del sistema CWMS.
RFC2833	Sí	Sí	Sí	Sí	Seleccione esta opción durante la configuración del troncal SIP de CUCM.
KPML	Sí	Sí	Sí	Sí	Seleccione esta opción durante la configuración del troncal SIP de CUCM.
Keepalive: envío de CWMS	Sí	Sí	Sí	Sí	Se realiza con el mensaje OPCIONES SIP.
Keepalive: recepción de CWMS	Sí	Sí	Sí	Sí	Se realiza con el mensaje OPCIONES SIP.
Calidad de servicio	Sí	Sí	Sí	Sí	Paquetes de control.
TCP	Sí	Sí	Sí	Sí	Asegúrese de que sus puertos predeterminados sean: 5060 para puntos de equilibrio de carga de conferencias; 5062 para puntos de aplicación de conferencias.

Característica	CUCM 9.1	CUCM 10.0	CUCM 10.5	CUCM 11.0	Condiciones previas/Notas
TLS	Sí	Sí	Sí	Sí	Asegúrese de que sus puertos predeterminados sean: 5061 para puntos de equilibrio de carga de conferencias; 5063 para puntos de aplicación de conferencias.
UDP	Sí	Sí	Sí	Sí	Asegúrese de que sus puertos predeterminados sean: 5060 para puntos de equilibrio de carga de conferencias; 5062 para puntos de aplicación de conferencias.
Certificados autofirmados	Sí	Sí	Sí	Sí	N/D
Certificados de terceros	Sí	Sí	Sí	Sí	N/D

Funciones de llamada telefónica

Nota El software CUCM 9.0, que es parte del producto BE6K (Business Edition 6000) también es compatible con CWMS.

Cisco WebEx Meetings Server admite las siguientes funciones de llamada CUCM:

Característica	CUCM 9.1	CUCM 10.0	CUCM 10.5	CUCM 11.0
Llamada en espera	Sí	Sí	Sí	Sí
Llamada que no está en espera	Sí	Sí	Sí	Sí

Característica	CUCM 9.1	CUCM 10.0	CUCM 10.5	CUCM 11.0
Visualización del identificador de llamada en EP	Sí	Sí	Sí	Sí
Visualización del nombre de la persona que llama en EP	Sí	Sí	Sí	Sí
Transferencia de llamada (IPv4 a IPv4)	Sí	Sí	Sí	Sí
Transferencia de llamada (IPv6 a IPv4)	Sí	Sí	Sí	Sí
Transferencia de llamada (IPv4 a IPv6)	Sí	Sí	Sí	Sí
Transferencia de llamada (IPv6 a IPv6)	Sí	Sí	Sí	Sí

Funciones multimedia telefónicas

CWMS admite participantes con códecs G.711/G.722/G.729 al mismo tiempo. El cambio de la configuración del códec no afecta al rendimiento del sistema. Tamaños de paquete compatibles con CWMS:

- 10 ms, 20 ms y 30 ms para los códecs de audio G.711 y G.729
- 20 ms para el códec de audio G.722

Característica	G.711	G.722	G.729
Compresión de ruido	Sí	Sí	Sí
Ruido cómodo	Sí	No	No
Cancelación de eco	No	No	No
Ocultación de pérdida de paquete	Sí	Sí	No
Obtención automática del control	Sí	Sí	Sí
Calidad de servicio	Sí	Sí	Sí

Nota Todos los mensajes de audio personalizados, incluidos los de llamada general, son de 8 kHz, 16 bits, 64 kB/s, mono, ley u de CCITT (G.711).

Compatibilidad del punto final de audio

Puede utilizar cualquier terminal de audio estándar que se conecte a Cisco Unified Communications Manager para entrar en una reunión de WebEx. Entre los terminales de audio compatibles están los teléfonos IP de Cisco, los terminales de Telepresence y los dispositivos PSTN, como teléfonos móviles y fijos. Muchos terminales de audio admiten conectividad de audio y vídeo. Sin embargo, se admite la conectividad de sólo audio con Cisco WebEx Meetings Server.

Para permitir que usuarios de fuera de la organización se unan a reuniones de WebEx mediante dispositivos PSTN, su empresa debe desplegar puertas de enlace analógico-VoIP, como los enrutadores de servicio integrado (ISR) de Cisco. Se ha probado el funcionamiento de los siguientes teléfonos IP con Cisco WebEx Meetings Server:

- Cisco 7960
- Cisco 7970
- Cisco 7971
- Cisco 7940
- Cisco 9951
- Cisco 9971
- Cisco (Tandberg) 7980
- Cisco 7975
- Cisco E20
- Cisco Telepresence (CTS 1100)
- Cisco IP Communicator
- Teléfono con vídeo Lifesize
- Tandberg 1000
- Tandberg 1700
- Polycom
- Cisco Cius
- C20
- EX 60
- EX 90

Otros extremos compatibles con Cisco UC también deberían funcionar con normalidad. Para obtener una lista de teléfonos IP de Cisco Unified compatibles con Cisco Unified Communications Manager y los paquetes de

dispositivos disponibles para cada modelo, consulte la Matriz de compatibilidad del paquete de dispositivos de la función de teléfono IP de Cisco Unified y Cisco Unified Communications Manager.

CAPÍTULO 7

Aplicaciones de despliegue masivo y descarga

La utilización de este producto requiere aplicaciones adicionales que deben descargarse en los ordenadores de sus usuarios.

- Acerca de la descarga de aplicaciones, página 135
- Descarga de aplicaciones desde el sitio de administración, página 136
- Contenido de los archivos ZIP de la aplicación, página 137
- Implementación masiva de las herramientas de productividad de Cisco WebEx, página 139
- Despliegue masivo de la aplicación de reuniones, página 148
- Despliegue masivo del reproductor de grabación en la red, página 153
- Reconfiguración de los ajustes tras realizar una actualización, página 157

Acerca de la descarga de aplicaciones

Puede desplegar masivamente aplicaciones CWMS utilizando las herramientas disponibles en el sitio de administración. Entre las aplicaciones disponibles para la descarga se encuentran las siguientes:

- Aplicación WebEx Meetings: la aplicación principal para planificar y organizar reuniones y asistir a ellas.

  No es posible ejecutar la aplicación WebEx Meetings en un sistema operativo virtualizado.

  Si un usuario no tiene instalada la aplicación WebEx Meetings, la primera vez que se una a una reunión la aplicación se descargará en su PC. Esto se puede configurar para hacerlo a demanda o de forma silenciosa. El usuario tiene la opción de utilizar la aplicación Cisco WebEx Meetings durante el transcurso de la reunión y eliminarla cuando la reunión haya finalizado o realizar instalación de la aplicación para acelerar el proceso de iniciar futuras reuniones o unirse a ellas. Esto podría fallar si el usuario no tiene privilegios de administrador.

- Herramientas de productividad de WebEx: ofrece una interfaz entre las otras aplicaciones, como Microsoft™ Outlook®, lo que permite que se gestionen las reuniones a través de dichas aplicaciones.

  Después de actualizar parcial o completamente el sistema, se deberá eliminar cualquier versión antigua de las herramientas de productividad de WebEx e instalar la última versión.

- Reproductor de grabación en la red de WebEx: reproduce las grabaciones de las reuniones. Dichas grabaciones pueden incluir cualquier material presentado durante la reunión.

En CWMS el programa de instalación .MSI de las aplicaciones se podrá obtener en la página **Administración** > **Configuración** > **Descargas**. Consulte "Descargar aplicaciones a través del sitio de administración" de la guía de planificación de CWMS para obtener más información.

Recomendamos que transfiera las aplicaciones a los ordenadores de los usuarios fuera de línea, antes de informar a dichos usuarios finales de que se han creado cuentas para ellos. Esto garantiza que los usuarios puedan iniciar y unirse a reuniones y reproducir grabaciones en red la primera vez que inicien sesión.

Si los usuarios poseen privilegios de administrador, podrá permitirles que descarguen las aplicaciones a través de la página de usuario final **Descargas** e instalarlas ellos mismos. No se necesita ninguna acción adicional del administrador.

Al **actualizar** a Cisco WebEx Meetings Server versión 1.5MR3 o superior en un entorno bloqueado en el que los PC de los usuarios no tienen privilegios de administrador, para poder iniciar el procedimiento de actualización, transfiera la nueva versión de la aplicación WebEx Meetings a todos los PC de los usuarios.

Descarga de aplicaciones desde el sitio de administración

Puede configurar su sistema para que los administradores puedan lanzar aplicaciones de escritorio de Cisco WebEx o bien puede habilitar a los usuarios para que realicen sus propias descargas.

Paso 1 Inicie sesión en el sitio de administración.
En un sistema con varios centros de datos, el DNS determina qué escritorio de centro de datos aparece. Podrá gestionar todos los centros de datos a través de dicho escritorio.

Paso 2 Seleccione **Configuración** > **Descargas**.

Paso 3 Seleccione el método de descarga:

- Permitir a los usuarios descargar aplicaciones del escritorio de WebEx.
  Use esta opción para que los usuarios que dispongan de permisos de administrador para sus PC puedan gestionar las aplicaciones de conferencia.
- Arrastre manualmente las aplicaciones del escritorio de WebEx al escritorio del usuario.
  Use esta opción para activar la conferencia para los usuarios que no tiene permisos de administrador en sus PC.

  Si seleccionó esta opción, la ventana se expande para mostrar las reuniones de Cisco WebEx, las herramientas de productividad y las secciones del reproductor de grabaciones en red.

Paso 4 (Opcional) Seleccione **Actualización automática de las herramientas de productividad de WebEx** para configurar las actualizaciones periódicas y automáticas de las herramientas de productividad de WebEx. (**Predet.**: activado).

Paso 5 Seleccione **Lanzar manualmente las aplicaciones del escritorio de WebEx al escritorio del usuario**:

a) En la sección de reuniones de WebEx, seleccione **Descargar** y guarde el archivo ZIP en su sistema.
b) En la sección de herramientas de productividad, seleccione **Descargar** y guarde el archivo ZIP en su sistema.
c) En la sección reproductor de grabaciones en red de WebEx, seleccione **Descargar** y guarde el archivo ZIP en su sistema.

Paso 6 Seleccione **Guardar** para guardar sus ajustes de descarga.
Este paso es de gran importancia si permite a otros usuarios que se descarguen las aplicaciones de escritorio de WebEx.

Paso 7 (Opcional) Seleccione **Lanzar manualmente las aplicaciones del escritorio de WebEx al escritorio del usuario**:

a) Descomprima el archivo descargado.

b) Abra el archivo ZIP.
Cada archivo ZIP contiene el programa de instalación de la aplicación para todos los idiomas compatibles. Consulte Contenido de los archivos ZIP de la aplicación, en la página 137 para obtener información sobre el instalador que se recomienda utilizar.

c) Seleccione el programa de instalación para su plataforma y el idioma, y extraiga la carpeta en un directorio local.
El archivo ZIP contiene instaladores MSI para plataforma Windows en todos los idiomas disponibles.

La versión de la aplicación de las herramientas de productividad correspondiente a cada versión de Cisco WebEx Meeting Server se puede encontrar en Matriz de compatibilidad de la aplicación Cisco WebEx Meetings y las herramientas de productividad, en la página 210.

Qué hacer a continuación

Despliegue los programas de instalación de MSI según se explica en el capítulo.

Contenido de los archivos ZIP de la aplicación

Esta sección describe las aplicaciones del instalador contenidas en cada uno de los archivos ZIP que puede descargar desde el sitio de Administración. Los archivos ZIP contienen una aplicación del instalador por idioma. Esta sección también ofrece una clave para ayudarle a determinar el idioma de cada instalador.

Clave del idioma de la aplicación

El archivo inglés del instalador de la aplicación de cada archivo ZIP no tiene sufijo de idioma. Por ejemplo, el cliente WebEx Meetings se denomina `onpremmc.msi` (Windows). El archivo de instalación de la aplicación para cada uno de los otros idiomas contiene una abreviatura en el título que indica el idioma de la aplicación que contiene. Consulte la siguiente tabla para las abreviaturas utilizadas para cada idioma:

Abreviatura	Idioma
B5	Chino tradicional
de	Alemán
ES	Español de Latinoamérica
fr	Francés
GB	Chino simplificado
it	Italiano
jp	Japonés
KO	Coreano
nl	Neerlandés
PT	Portugués

Abreviatura	Idioma
ru	Ruso
SP	español

Contenido del archivo ZIP de las herramientas de productividad

El archivo ZIP de las herramientas de productividad contiene los siguientes archivos. Utilice la clave de la tabla de claves de idioma de la aplicación para determinar el idioma de cada archivo. Tenga en cuenta que no hay versión de Mac de las herramientas de productividad.

- 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

Contenido del archivo ZIP de WebEx Meetings

El archivo ZIP del cliente de WebEx Meetings contiene los siguientes archivos. Utilice la clave de la tabla de claves de idioma de la aplicación para determinar el idioma de cada archivo.

- onpremmc.msi
- onpremmc_B5.msi
- onpremmc_DE.msi
- onpremmc_ES.msi
- onpremmc_FR.msi
- onpremmc_GB.msi
- onpremmc_IT.msi
- onpremmc_JP.msi
- onpremmc_KO.msi

- onpremmc_NL.msi
- onpremmc_PT.msi
- onpremmc_RU.msi
- onpremmc_SP.msi
- webexmc_onprem.dmg (para Mac)

Contenido del archivo ZIP del reproductor de grabación en red

El reproductor de grabación en red solamente está disponible para descarga y despliegue masivo si ha seleccionado **Permitir a los usuarios descargar aplicaciones de escritorio de WebEx** en la página de Descargas. Consulte el apartado "Configuración de los ajustes de descarga" de la *Guía de administración de Cisco WebEx Meetings Server* si desea más información.

El archivo ZIP del reproductor de grabación en red contiene los siguientes archivos. Utilice la clave de la tabla de claves de idioma de la aplicación para determinar el idioma de cada archivo.

- 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 (para Mac)

Implementación masiva de las herramientas de productividad de Cisco WebEx

Esta sección describe las tareas que hay que realizar a la hora de instalar las herramientas de productividad de Cisco WebEx con el paquete `ptools.ms`. Tanto la instalación en un solo ordenador como una instalación a gran escala se pueden llevar a cabo con Microsoft Systems Management Server 2003 (SMS).

La versión de las herramientas de productividad correspondiente a cada versión de Cisco WebEx Meeting Server se puede encontrar en Matriz de compatibilidad de la aplicación Cisco WebEx Meetings y las herramientas de productividad, en la página 210.

Instalación silenciosa de las herramientas de productividad utilizando la línea de comandos

Los administradores pueden iniciar sesión en el ordenador de un usuario e instalar las herramientas de productividad de WebEx utilizando el modo silencioso.

Antes de comenzar

Antes de instalar una versión de mantenimiento o actualizar su sistema a una versión más reciente, se deben desinstalar las versiones anteriores de las herramientas de productividad de Cisco WebEx.

Paso 1 Inicie sesión en el ordenador del usuario.

Paso 2 Descargue el paquete MSI en el disco duro del ordenador.

Paso 3 Abra la ventana de comandos de Windows.
En Windows 7 y Windows Vista, debe utilizar ejecutar como administrador para abrirla.

Paso 4 Ejecute el comando MSI para instalar las Herramientas de productividad de WebEx de forma silenciosa.

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

Nombre del parámetro	Valor	Descripción
OI	1	Activar la integración de Outlook
	0 (Predeterminado)	Desactivar la integración de Outlook
MSN	1	Activar la integración de mensajería instantánea para Microsoft Office Communicator y Lync

Paso 5 Reinicie el ordenador.

Eliminación silenciosa de las herramientas de productividad a través de la interfaz de la línea de comandos

Los administradores pueden iniciar sesión en el ordenador de un usuario y desinstalar las herramientas de productividad utilizando el modo silencioso.

Paso 1 Inicie sesión en el ordenador del usuario.

Paso 2 Descargue el paquete MSI en el disco duro del ordenador.

Paso 3 Abra la ventana de comandos de Windows.

En Windows 7 y Windows Vista, debe utilizar ejecutar como administrador para abrirla.

Paso 4 Desinstale todos los componentes del paquete ptools.msi MSI introduciendo el comando msiexec.exe /q /x "ptools.msi".

Instalación silenciosa con SMS

Las siguientes limitaciones se aplican cuando se realiza una instalación silenciosa con Microsoft Systems Management Server 2003 (SMS):

- La modalidad por usuario de SMS no es compatible.
- Si el Administrador de SMS desea añadir una función para las herramientas de productividad de WebEx, el administrador debe, en primer lugar, ejecutar el comando **REMOVE** y, a continuación, ejecutar el comando **ADDSOURCE** , aunque la función no se haya instalado antes.
- Si un usuario inicia sesión en un ordenador con el escritorio remoto mientras el administrador anuncia el paquete, debe reiniciar el ordenador para asegurarse de que las herramientas de productividad de WebEx funcionan normalmente.
- El despliegue masivo es posible, pero cada usuario debe introducir información de credenciales.
- Antes de instalar una versión de mantenimiento o actualizar el sistema a una versión más nueva, sus usuarios deben desinstalar las herramientas de productividad de Cisco WebEx que se están ejecutando en sus escritorios. Después de la actualización, puede enviar manualmente las herramientas de productividad a sus usuarios, o los usuarios pueden descargarlas desde la página **Descargas**.
- Si está utilizando la integración Lync, después de una instalación silenciosa sus usuarios deben reiniciar sus ordenadores para que todas las integraciones de mensajería instantánea funcionen correctamente.

Publicidad de las herramientas de productividad de WebEx mediante el programa SMS por sistema desatendido

Después de la actualización, puede utilizar el sitio de administración para enviar manualmente las herramientas de productividad a sus usuarios o permitirles que las descarguen desde la página **Descargas** del usuario final.

Consulte el apartado "Configuración de los ajustes de descarga" de la *Guía de Administración de Cisco WebEx Meetings Server* si desea más información.

Si es el administrador de Microsoft Systems Management Server 2003 (SMS), puede utilizar el programa de SMS por sistema desatendido para anunciar las herramientas de productividad de Cisco WebEx.

Pasos resumidos

1. Cree un paquete a partir de la definición. Consulte Creación de un paquete a partir de la definición, en la página 147 para obtener más información al respecto.
2. Cambie las opciones del programa a **Por sistema desatendido** para lanzar el anuncio:
3. Anuncie el programa.

Pasos detallados

Paso 1 Cree un paquete a partir de la definición. Consulte Creación de un paquete a partir de la definición, en la página 147 para obtener más información al respecto.

Paso 2 Cambie las opciones del programa a **Por sistema desatendido** para lanzar el anuncio:

a) Abra la consola del administrador de SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Herramientas de productividad de Cisco WebEx de Cisco WebEx LLC 2.82** > **Programas**.

b) Haga clic con el botón derecho en Por sistema desatendido y, a continuación, seleccione **Propiedades** para abrir el cuadro de diálogo **Propiedades del programa por sistema desatendido**.

c) Seleccione la pestaña **Entorno**.

- Para la opción **El programa se puede ejecutar**, seleccione **Solo cuando un usuario está registrado**.
- Para la opción **Modo de funcionamiento**, seleccione **Ejecutar con derechos administrativos**. (No activar **Permitir a los usuarios interactuar con este programa**.)

d) Seleccione la pestaña **General**.

e) Añada un parámetro adicional a la opción de línea de comandos para especificar algunas opciones para las herramientas de productividad de Cisco WebEx:

- Añada SITEURL="http://sample.webex.com" para especificar la URL del sitio de WebEx que utiliza su empresa.
- Los códigos de las herramientas de productividad especifican qué componente está activado para las herramientas de productividad de WebEx. Los parámetros deben estar en mayúsculas y el valor predeterminado es 0 (desactivado).

  En el siguiente ejemplo, la línea de comandos inicial es msiexec.exe/q ALLUSERS = 2 /m MSIZWPBY /i "ptools.msi" .
- Añada los códigos de las herramientas de productividad y los parámetros a la línea de comandos: msiexec.exe /q ALLUSERS=2 /m MSIZWPBY /i "ptools.msi" SITEURL="https://sample.webex.com" OI=1MSN=1.

Nota Consulte la tabla de parámetros en Instalación silenciosa de las herramientas de productividad utilizando la línea de comandos, en la página 140 para ver las definiciones de los parámetros.

Paso 3 Anuncie el programa.

a) Abra la consola del administrador de SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Herramientas de productividad de Cisco WebEx de Cisco WebEx LLC 2.82 (inglés)** > **Programas**.

b) Haga clic con el botón derecho del ratón en **Por sistema desatendido**.

c) Seleccione **Todas las tareas** > **Distribuir Software**.

d) Seleccione **Siguiente** en el **Asistente Distribuir programa**.

e) Seleccione el servidor SMS y seleccione **Siguiente**.

f) Seleccione la colección y **Siguiente**.

g) Introduzca el nombre del anuncio en el campo **Nombre** y seleccione **Siguiente**.

h) Especifique si la publicidad debería aplicarse a subcolecciones y seleccione **Siguiente**.

i) Especifique cuándo se anunciará el programa y seleccione **Siguiente**.

j) Especifique si desea asignar el programa o no, y seleccione **Siguiente**.

k) Seleccione **Finalizar** en la página **Completando el asistente Distribuir programa**.

l) Vaya hasta el directorio \Base de datos del sitio\Estado del sistema\Estado del anuncio y compruebe el estado del anuncio.

Si activa la notificación, el usuario verá un mensaje que indica que el programa asignado se va a ejecutar después de que se haya anunciado el programa. El programa asignado se ejecutará de forma silenciosa.

Eliminación de componentes de herramientas de productividad mediante el programa de SMS por sistema desatendido

Lleve a cabo el siguiente procedimiento para eliminar las herramientas de productividad con Microsoft Systems Management Server 2003 (SMS):

Pasos resumidos

1. Cree un programa nuevo, copie todas las opciones del "programa por sistema desatendido" tal como se describe en Publicidad de las herramientas de productividad de WebEx mediante el programa SMS por sistema desatendido, en la página 141 y, a continuación, actualice la línea de comandos:
2. Publique el programa en el conjunto especificado de máquinas de trabajo en el dominio. Consulte Instalación silenciosa con SMS, en la página 141 para obtener más información al respecto.

Pasos detallados

Paso 1 Cree un programa nuevo, copie todas las opciones del "programa por sistema desatendido" tal como se describe en Publicidad de las herramientas de productividad de WebEx mediante el programa SMS por sistema desatendido, en la página 141 y, a continuación, actualice la línea de comandos:

a) Abra la consola de administrador SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Herramientas de productividad de Cisco WebEx 2.82 de Cisco WebEx LLC** > **Programas**.
b) Haga clic con el botón derecho en el área en blanco y seleccione **Nuevo** > **Programa**.
c) Introduzca el nombre del programa y la línea de comando predeterminada.
d) En el cuadro de diálogo **Propiedades** , seleccione la pestaña **Entorno**.

- Para la opción **El programa se puede ejecutar**, seleccione **Solo cuando un usuario está registrado**.
- Para la opción **Modo de funcionamiento**, seleccione **Ejecutar con derechos administrativos**. (No active **Permitir a los usuarios interactuar con este programa**).

e) Actualice la línea de comandos en la pestaña **General**.
f) Agregue REMOVE a la línea de comandos y especifique las características que se deben eliminar.

Ejemplo:
Si desea eliminar OI, introduzca el siguiente comando: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="OI"
El valor PTIM es para la integración de WebEx con la mensajería instantánea. Como utilizar PTIM como se muestra en la siguiente línea de comandos de muestra:
msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="PTIM"

Paso 2 Publique el programa en el conjunto especificado de máquinas de trabajo en el dominio. Consulte Instalación silenciosa con SMS, en la página 141 para obtener más información al respecto.
Las herramientas de productividad de Cisco WebEx se actualizarán en estas máquinas de forma silenciosa.

Añadir componentes de las herramientas de productividad mediante el programa SMS por sistema desatendido

Para que un administrador añada un componente a las herramientas de productividad, debe ejecutar primero REMOVE y, a continuación, ejecutar ADDSOURCE, aunque el componente no se haya instalado antes.

Pasos resumidos

1. Cree un programa nuevo llamado "Add-phase1", copie todas las opciones del "programa por sistema desatendido" y, a continuación, actualice la línea de comandos.
2. Publique el programa en el conjunto especificado de máquinas de trabajo en el dominio. Consulte Instalación silenciosa con SMS, en la página 141 para obtener más información al respecto.
3. Cree un segundo nombre de programa, "Add-phrase2", copie todas las opciones del "programa por sistema desatendido" y, a continuación, actualice la línea de comandos:
4. Publique el programa en el conjunto especificado de máquinas de trabajo en el dominio. Consulte Instalación silenciosa con SMS, en la página 141 para obtener más información al respecto.

Pasos detallados

Paso 1 Cree un programa nuevo llamado "Add-phase1", copie todas las opciones del "programa por sistema desatendido" y, a continuación, actualice la línea de comandos.

a) Abra la consola del administrador de SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Herramientas de productividad de Cisco WebEx de Cisco WebEx LLC 2.82** > **Programas** .
b) Haga clic con el botón derecho en el área en blanco y seleccione **Nuevo** > **Programa**.
c) Introduzca el nombre del programa y la línea de comando predeterminada.
d) En el diálogo Propiedades, seleccione la pestaña **Entorno**.

- Para la opción **El programa se puede ejecutar**, seleccione **Solo cuando un usuario está registrado**.
- Para la opción **Modo de funcionamiento**, seleccione **Ejecutar con derechos administrativos**. (No active **Permitir a los usuarios interactuar con este programa**).

e) Actualice la línea de comandos en la pestaña **General**.
f) Añada REMOVE a la línea de comandos y especifique las características que se deben añadir.

Ejemplo:

Si desea añadir OIy PITM (el valor PITM es para la integración de WebEx con la mensajería instantánea), debe ELIMINARLOS antes, aunque aún no estén instalados: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="OI,PTIM"

Paso 2 Publique el programa en el conjunto especificado de máquinas de trabajo en el dominio. Consulte Instalación silenciosa con SMS, en la página 141 para obtener más información al respecto.

Paso 3 Cree un segundo nombre de programa, "Add-phrase2", copie todas las opciones del "programa por sistema desatendido" y, a continuación, actualice la línea de comandos:

a) Abra la consola del administrador de SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Herramientas de productividad de Cisco WebEx de Cisco WebEx LLC 2.82** > **Programas** .
b) Haga clic con el botón derecho en el área en blanco y seleccione **Nuevo** > **Programa**.
c) Introduzca el nombre del programa y la línea de comando predeterminada.
d) En el cuadro de diálogo Propiedades, seleccione la pestaña **Entorno**.

- Para la opción **El programa se puede ejecutar**, seleccione **Solo cuando un usuario está registrado**.
- Para la opción **Modo de funcionamiento**, seleccione **Ejecutar con derechos administrativos**. (No active **Permitir a los usuarios interactuar con este programa**).

e) En el cuadro de diálogo Propiedades, seleccione la pestaña **Avanzada**.
f) Active **Ejecutar otro programa primero** y seleccione el programa **Add-phase1**.
g) Actualice la línea de comandos en la pestaña **General**.
h) Añada ADDSOURCE a la línea de comandos y especifique las funciones que se deben incluir.

Ejemplo:
Si desea añadir OI, utilice este comando de muestra: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" ADDSOURCE="OI" OI=1

Ejemplo:
Si desea añadir OI y PITM, utilice este comando de muestra: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" ADDSOURCE="OI,PTIM" OI=1 MSN=1

Paso 4 Publique el programa en el conjunto especificado de máquinas de trabajo en el dominio. Consulte Instalación silenciosa con SMS, en la página 141 para obtener más información al respecto.
Las herramientas de productividad de Cisco WebEx se actualizarán en estas máquinas de forma silenciosa.

Desinstalación de las herramientas de productividad mediante el programa SMS por desinstalación de sistema

El administrador SMS puede desinstalar las herramientas de productividad de Cisco WebEx mediante el programa SMS por desinstalación de sistema realizando el siguiente procedimiento.

Pasos resumidos

1. Utilice el paquete de instalación de SMS creado en Creación de un paquete a partir de la definición, en la página 147.
2. Anuncie el programa de desinstalación por sistema para desinstalar las herramientas de productividad de Cisco WebEx.

Pasos detallados

Paso 1	Utilice el paquete de instalación de SMS creado en Creación de un paquete a partir de la definición, en la página 147.
Paso 2	Anuncie el programa de desinstalación por sistema para desinstalar las herramientas de productividad de Cisco WebEx. Las herramientas de productividad de Cisco WebEx se desinstalarán en estas máquinas de forma silenciosa.

Publicidad del programa para actualizar la nueva versión de las herramientas de productividad de WebEx

Realice el siguiente procedimiento para anunciar el programa para actualizar a la nueva versión de las herramientas de productividad de Cisco WebEx.

Antes de comenzar

Antes de instalar una versión de mantenimiento o actualizar el sistema a una versión más nueva, sus usuarios deben desinstalar las herramientas de productividad de Cisco WebEx que se están ejecutando en sus escritorios. Después de la actualización, puede utilizar el portal de Administración para enviar manualmente las herramientas de productividad a sus usuarios, o los usuarios pueden descargarlas desde la página **Descargas** del usuario final.

Inicie sesión en el sitio de Administración, seleccione **Configuración** > **Descargas** y desactive las siguientes configuraciones:

- **Actualización automática de las herramientas de productividad de Cisco WebEx**
- **Permitir a los usuarios descargar aplicaciones del escritorio de WebEx**

Pasos resumidos

1. Cree un nuevo paquete de instalación de SMS utilizando el paquete MSI de las herramientas de productividad de WebEx. Consulte Creación de un paquete a partir de la definición, en la página 147 para obtener más información al respecto.
2. Cambie las opciones del programa para **Por sistema desatendido** antes de anuncio. Consulte Añadir componentes de las herramientas de productividad mediante el programa SMS por sistema desatendido, en la página 144 para obtener más información al respecto.
3. Anuncie el programa. Consulte Añadir componentes de las herramientas de productividad mediante el programa SMS por sistema desatendido, en la página 144 para obtener más información al respecto.

Pasos detallados

Paso 1 Cree un nuevo paquete de instalación de SMS utilizando el paquete MSI de las herramientas de productividad de WebEx. Consulte Creación de un paquete a partir de la definición, en la página 147 para obtener más información al respecto.

Paso 2 Cambie las opciones del programa para **Por sistema desatendido** antes de anuncio. Consulte Añadir componentes de las herramientas de productividad mediante el programa SMS por sistema desatendido, en la página 144 para obtener más información al respecto.

Paso 3 Anuncie el programa. Consulte Añadir componentes de las herramientas de productividad mediante el programa SMS por sistema desatendido, en la página 144 para obtener más información al respecto.
Las antiguas herramientas de productividad de Cisco WebEx se eliminan y se instalan las nuevas de forma silenciosa.

Creación de un paquete a partir de la definición

Realice el siguiente procedimiento para crear un paquete a partir de una definición.

Pasos resumidos

1. Abra la consola de administrador SMS y seleccione **Base de datos del sitio** > **Paquete**.
2. Haga clic con el botón derecho del ratón en **Paquete**.
3. Seleccione **Nuevo** > **Paquete a partir de definición**.
4. En el asistente **Crear paquete a partir de definición**, seleccione **Siguiente**.
5. Seleccione **Examinar** para localizar y seleccionar el paquete MSI de las herramientas de productividad de WebEx y luego seleccione **Siguiente**.
6. Seleccione **Siempre obtener archivos de un directorio fuente** y luego seleccione **Siguiente.**
7. Seleccione Ubicación de directorio de origen. La ruta del directorio es la carpeta donde está el paquete de instalación. A continuación, seleccione **Siguiente**.
8. Seleccione **Finalizar**.
9. Seleccione **Base de datos del sitio** > **Paquetes** > **Herramientas de productividad de Cisco WebEx de Cisco WebEx LLC 2.82 (inglés)** > **Programas**. Hay seis programas predeterminados disponibles.

Pasos detallados

Paso 1 Abra la consola de administrador SMS y seleccione **Base de datos del sitio** > **Paquete**.

Paso 2 Haga clic con el botón derecho del ratón en **Paquete**.

Paso 3 Seleccione **Nuevo** > **Paquete a partir de definición**.

Paso 4 En el asistente **Crear paquete a partir de definición**, seleccione **Siguiente**.

Paso 5 Seleccione **Examinar** para localizar y seleccionar el paquete MSI de las herramientas de productividad de WebEx y luego seleccione **Siguiente**.

Paso 6 Seleccione **Siempre obtener archivos de un directorio fuente** y luego seleccione **Siguiente.**

Paso 7 Seleccione Ubicación de directorio de origen. La ruta del directorio es la carpeta donde está el paquete de instalación. A continuación, seleccione **Siguiente**.

Paso 8 Seleccione **Finalizar**.

Paso 9 Seleccione **Base de datos del sitio** > **Paquetes** > **Herramientas de productividad de Cisco WebEx de Cisco WebEx LLC 2.82 (inglés)** > **Programas**. Hay seis programas predeterminados disponibles.

Despliegue masivo de la aplicación de reuniones

Este apartado se ha diseñado para ayudar a su organización a comprender las tareas que implica la instalación de la aplicación Cisco WebEx Meetings. Esta sección es una guía integral que abarca diversos tipos de instalaciones, incluidas una instalación de un solo ordenador e instalaciones a gran escala Microsoft Systems Management Server 2003 (SMS).

Nota "Instalación silenciosa" significa que la aplicación puede desplegarse silenciosamente, pero es necesario que el usuario final la configure.

Instalar Cisco WebEx Meetings

Antes de comenzar

Los siguientes requisitos previos se aplican al instalador de Cisco WebEx Meetings:

- La instalación del paquete MSI de Cisco WebEx requiere privilegios de administrador. El paquete MSI se instala en la carpeta predeterminada de programas del SO, la cual requiere privilegios de administrador para su acceso.
- El paquete MSI de Cisco WebEx se ha desarrollado para Windows Installer Service 2.0 o superior. Si la máquina local está configurada con una versión anterior, aparecerá un mensaje de error informando al usuario de que para poder instalar este paquete MSI se requiere una versión más reciente de Windows Installer Service. Después de ejecutar el paquete MSI, el usuario verá una interfaz MSI básica.

Pasos resumidos

1. Lance el programa de instalación en el ordenador del usuario.
2. Seleccione **Siguiente** en los cuadros de diálogo sucesivos hasta que llegue al cuadro de diálogo de instalación.
3. Seleccione **Instalar**.
4. Seleccione **Finalizar** cuando se haya completado la instalación.

Pasos detallados

Paso 1 Lance el programa de instalación en el ordenador del usuario.
Aparece el asistente de instalación con un mensaje introductorio.

Paso 2 Seleccione **Siguiente** en los cuadros de diálogo sucesivos hasta que llegue al cuadro de diálogo de instalación.

Paso 3 Seleccione **Instalar**.

Paso 4 Seleccione **Finalizar** cuando se haya completado la instalación.

Desinstalación de Cisco WebEx Meetings localmente

Puede iniciar sesión en el ordenador del usuario y desinstalar la aplicación Cisco WebEx Meetings desde el Panel de control o la carpeta WebEx en el disco duro local.

Antes de comenzar

La aplicación Cisco WebEx Meetings está instalada en el ordenador del usuario.

Paso 1 Inicie sesión en el ordenador del usuario.

Paso 2 Elimine la aplicación Cisco WebEx Meetings usando uno de los métodos siguientes:

- Seleccione **Inicio** > **Panel de control** > **Programas y características**. De la lista de programas, seleccione **Cisco WebEx Meetings** y después **Desinstalar/Cambiar**.
- Seleccione **Inicio** > **Ordenador** > **Sistema (C:)** > **Carpeta ProgramData** > **Carpeta WebEx**. Haga clic con el botón derecho en **atcliun.exe** y seleccione **Eliminar**.

Nota Al desinstalar atcliun.exe desde la carpeta WebEx, se eliminan las versiones en las instalaciones y en la nube de Cisco WebEx Meetings, si ambas versiones de la aplicación se habían guardado en el disco duro local del usuario. Sin embargo, si desinstala la aplicación usando el Panel de control, solo se desinstala la versión en la instalación de la aplicación.

La aplicación Cisco WebEx Meetings se desinstala del ordenador del usuario.

Instalación silenciosa de la aplicación de reuniones utilizando la línea de comandos

Los administradores pueden iniciar sesión en el ordenador de un usuario e instalar la aplicación WebEx Meetings utilizando el modo silencioso.

Paso 1 Inicie sesión en el ordenador del usuario.

Paso 2 Descargue el paquete MSI en el disco duro del ordenador.

Paso 3 Abra la ventana de comandos de Windows.
En Windows 7 y Windows Vista, debe utilizar ejecutar como administrador para abrirla.

Paso 4 Introduzca el comando MSI para instalar las aplicaciones de Cisco WebEx Meetings de forma silenciosa.

Ejemplo:
Introduzca msiexec /i onpremmc.msi /qn.

Paso 5 Reinicie el ordenador.

Eliminación silenciosa de la aplicación de reuniones a través de la interfaz de la línea de comandos

Los administradores pueden iniciar sesión en el ordenador de un usuario y desinstalar la aplicación WebEx Meetings utilizando el modo silencioso.

Paso 1 Inicie sesión en el ordenador del usuario.

Paso 2 Abra la ventana de comandos de Windows.
En Windows 7 y Windows Vista, debe utilizar ejecutar como administrador para abrirla.

Paso 3 Desinstale todos los componentes del paquete onpremmc.msi MSI introduciendo el comando msiexec/x onpremmc.msi/qn.

Instalación silenciosa con SMS

Las siguientes limitaciones se aplican cuando se realiza una instalación silenciosa con Microsoft Systems Management Server 2003 (SMS):

- La modalidad por usuario de SMS no es compatible.
- Si el Administrador de SMS desea añadir una función para las herramientas de productividad de WebEx, el administrador debe, en primer lugar, ejecutar el comando **REMOVE** y, a continuación, ejecutar el comando **ADDSOURCE** , aunque la función no se haya instalado antes.

- Si un usuario inicia sesión en un ordenador con el escritorio remoto mientras el administrador anuncia el paquete, debe reiniciar el ordenador para asegurarse de que las herramientas de productividad de WebEx funcionan normalmente.
- El despliegue masivo es posible, pero cada usuario debe introducir información de credenciales.
- Antes de instalar una versión de mantenimiento o actualizar el sistema a una versión más nueva, sus usuarios deben desinstalar las herramientas de productividad de Cisco WebEx que se están ejecutando en sus escritorios. Después de la actualización, puede enviar manualmente las herramientas de productividad a sus usuarios, o los usuarios pueden descargarlas desde la página **Descargas**.
- Si está utilizando la integración Lync, después de una instalación silenciosa sus usuarios deben reiniciar sus ordenadores para que todas las integraciones de mensajería instantánea funcionen correctamente.

Publicidad de la aplicación Cisco WebEx Meetings mediante el programa SMS por sistema desatendido

Si usted es el administrador SMS, realice el siguiente procedimiento para anunciar la aplicación Cisco WebEx Meetings mediante el programa de SMS por sistema desatendido.

Antes de comenzar

Inicie sesión en el sistema de administración y configure sus ajustes de descarga para arrastrar manualmente las aplicaciones de escritorio de WebEx al escritorio del usuario. Consulte el apartado "Configuración de los ajustes de descarga" de la Guía de Administración de Cisco WebEx Meetings Server si desea más información.

Pasos resumidos

1. Cree un paquete a partir de la definición. Consulte Creación de un paquete a partir de la definición, en la página 147 para obtener más información al respecto.
2. Cambie las opciones del programa a "desatendido por sistema" antes del anuncio:
3. Ahora, puede anunciar el programa.

Pasos detallados

Paso 1 Cree un paquete a partir de la definición. Consulte Creación de un paquete a partir de la definición, en la página 147 para obtener más información al respecto.

Paso 2 Cambie las opciones del programa a "desatendido por sistema" antes del anuncio:

a) Abra la consola de administrador SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Aplicación Cisco WebEx Meetings de Cisco WebEx LLC (inglés)** > **Programas**.

b) Haga clic con el botón derecho del ratón en la opción **Por sistema desatendido** y, a continuación, seleccione **Propiedades** para abrir el cuadro de diálogo **Propiedades del programa por sistema desatendido**.

c) Seleccione la pestaña **Entorno**.

- Para la opción **El programa se puede ejecutar**, seleccione **Solo cuando un usuario está registrado**.
- Para la opción **Modo de funcionamiento**, seleccione **Ejecutar con derechos administrativos**. No seleccione **Permitir a los usuarios interactuar con este programa**.

d) Seleccione la pestaña **General**.
e) Añada un parámetro adicional a la opción de línea de comandos para especificar algunas opciones para la aplicación WebEx Meetings:

Ejemplo:
Por ejemplo, la línea de comando inicial es: msiexec /i "onpremmc.msi" /qn

Paso 3 Ahora, puede anunciar el programa.

a) Abra la consola de administrador SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Aplicación Cisco WebEx Meetings de Cisco WebEx LLC (inglés)** > **Programas**.
b) Haga clic con el botón derecho del ratón en **Por sistema desatendido**.
c) Seleccione **Todas las tareas** > **Distribuir software**.
d) Seleccione **Siguiente** en el **Asistente Distribuir programa**.
e) Seleccione el servidor SMS y seleccione **Siguiente**.
f) Seleccione la colección y **Siguiente**.
g) Introduzca el nombre del anuncio en el campo **Nombre** y seleccione **Siguiente**.
h) Especifique si la publicidad debería aplicarse a subcolecciones y seleccione **Siguiente**.
i) Especifique cuándo se anunciará el programa y seleccione **Siguiente**.
j) Especifique si desea asignar el programa y seleccione **Siguiente**.
k) Seleccione **Finalizar** en la página **Completando el asistente Distribuir programa**.
l) Vaya hasta el directorio \Base de datos del sitio\Estado del sistema\Estado del anuncio y compruebe el estado del anuncio.
Si activa la notificación, el usuario verá un mensaje que indica que el programa asignado se va a ejecutar después de que se haya anunciado el programa. El programa asignado se ejecutará de forma silenciosa.

Desinstalación de la aplicación Cisco WebEx Meetings mediante el programa de desinstalación SMS por sistema

El administrador SMS puede desinstalar la aplicación Cisco WebEx Meetings mediante el programa de desinstalación SMS por sistema realizando el siguiente procedimiento.

Pasos resumidos

1. Utilice el paquete de instalación de SMS creado en Creación de un paquete a partir de la definición, en la página 147.
2. Anuncie el programa de desinstalación por sistema para desinstalar la aplicación Cisco WebEx Meetings.

Pasos detallados

Paso 1 Utilice el paquete de instalación de SMS creado en Creación de un paquete a partir de la definición, en la página 147.
Paso 2 Anuncie el programa de desinstalación por sistema para desinstalar la aplicación Cisco WebEx Meetings.

La aplicación Cisco WebEx Meetings se desinstalará en las máquinas especificadas de forma silenciosa.

Despliegue masivo del reproductor de grabación en la red

Esta sección es una guía integral que abarca diversos tipos de instalaciones, incluidas una instalación de un solo ordenador e instalaciones a gran escala Microsoft Systems Management Server 2003 (SMS).

Nota Los archivos del reproductor de grabación con más de 4 GB solo se pueden reproducir si se accede a ellos desde el explorador web.

Instalación del reproductor de grabación en la red

Antes de comenzar

- Compruebe que dispone de privilegios de administrador porque el paquete de Cisco WebEx MSI se instala de forma predeterminada en la carpeta de programas del SO, para cuyo acceso dichos privilegios son necesarios.
- El paquete MSI de Cisco WebEx se desarrolló para Windows Installer Service 2.0 o superior. Si la máquina local está configurada con una versión anterior, aparecerá un mensaje de error en el que se informa al usuario de que se requiere una versión más reciente de Windows Installer Service para instalar el paquete MSI. Después de ejecutar el paquete MSI, se pregunta al usuario a través de la interfaz de MSI.

Pasos resumidos

1. Lance el programa de instalación en el ordenador del usuario.
2. Seleccione **Siguiente** en cada cuadro de diálogo hasta que aparezca el cuadro de diálogo de la instalación.
3. Seleccione **Instalar**.
4. Seleccione **Finalizar**.

Pasos detallados

Paso 1 Lance el programa de instalación en el ordenador del usuario.
Aparece el asistente de instalación con un mensaje introductorio.

Paso 2 Seleccione **Siguiente** en cada cuadro de diálogo hasta que aparezca el cuadro de diálogo de la instalación.

Paso 3 Seleccione **Instalar**.

Paso 4 Seleccione **Finalizar**.

Instalación silenciosa del Reproductor de grabación utilizando la línea de comandos

Los administradores pueden iniciar sesión en el ordenador de un usuario e instalar el Reproductor de grabación de WebEx utilizando el modo silencioso.

Pasos resumidos

1. Inicie sesión en el ordenador del usuario.
2. Descargue el paquete MSI en el disco duro del ordenador.
3. Abra la ventana de comandos de Windows.
4. Introduzca el comando MSI para instalar el Reproductor de grabación de WebEx de forma silenciosa.
5. Reinicie el ordenador.

Pasos detallados

Paso 1 Inicie sesión en el ordenador del usuario.

Paso 2 Descargue el paquete MSI en el disco duro del ordenador.

Paso 3 Abra la ventana de comandos de Windows.
En Windows 7 y Windows Vista, debe utilizar ejecutar como administrador para abrirla.

Paso 4 Introduzca el comando MSI para instalar el Reproductor de grabación de WebEx de forma silenciosa.

Ejemplo:
Introduzca msiexec/i nbr2player_onprem.msi/qn.

Paso 5 Reinicie el ordenador.

Desinstalación silenciosa del reproductor de grabación a través de la interfaz de la línea de comandos

Los administradores pueden iniciar sesión en el ordenador de un usuario y quitar el reproductor de grabación utilizando el modo silencioso.

Paso 1 Inicie sesión en el ordenador del usuario.

Paso 2 Descargue el paquete MSI en el disco duro del ordenador.

Paso 3 Abra la ventana de comandos de Windows.

En Windows 7 y Windows Vista, debe utilizar ejecutar como administrador para abrirla.

Paso 4 Desinstale todos los componentes del paquete MSI onpremmc.msi introduciendo el comando msiexec/i nbr2player_onprem.msi/qn.

Instalación silenciosa mediante el programa SMS

Antes de comenzar

Las siguientes limitaciones se aplican cuando se realiza una instalación silenciosa con SMS:

- La modalidad por usuario de SMS no es compatible.
- Si un usuario inicia sesión en un ordenador con el escritorio remoto mientras su administrador anuncia el paquete, debe reiniciar el ordenador para asegurarse de que la aplicación WebEx Meetings funciona normalmente.

Publicidad del reproductor de grabación en la red de Cisco WebEx mediante el programa SMS por sistema desatendido

Si usted es el administrador SMS, realice el siguiente procedimiento para anunciar el reproductor de grabación en la red de Cisco WebEx mediante el programa de SMS por sistema desatendido.

Antes de comenzar

Inicie sesión en el sistema de administración y configure sus ajustes de descarga para arrastrar manualmente las aplicaciones de escritorio de WebEx al escritorio del usuario. Consulte el apartado "Configuración de los ajustes de descarga" de la Guía de Administración de Cisco WebEx Meetings Server si desea más información.

Pasos resumidos

1. Cree un paquete a partir de la definición. Consulte Creación de un paquete a partir de la definición, en la página 147 para obtener más información al respecto.
2. Cambie las opciones del programa a "desatendido por sistema" antes del anuncio:
3. Ahora, puede anunciar el programa.

Pasos detallados

Paso 1 Cree un paquete a partir de la definición. Consulte Creación de un paquete a partir de la definición, en la página 147 para obtener más información al respecto.

Paso 2 Cambie las opciones del programa a "desatendido por sistema" antes del anuncio:

a) Abra la consola de administrador SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Reproductor de grabaciones en red de Cisco WebEx de Cisco WebEx LLC (inglés)** > **Programas**.

b) Haga clic con el botón derecho del ratón en la opción **Por sistema desatendido** y, a continuación, seleccione **Propiedades** para abrir el cuadro de diálogo **Propiedades del programa por sistema desatendido**.

c) Seleccione la pestaña **Entorno**.

- Para la opción **El programa se puede ejecutar**, seleccione **Solo cuando un usuario está registrado**.
- Para la opción **Modo de funcionamiento**, seleccione **Ejecutar con derechos administrativos**. No seleccione **Permitir a los usuarios interactuar con este programa**.

d) Seleccione la pestaña **General**.
e) Añada un parámetro adicional a la opción de línea de comandos para especificar algunas opciones para la aplicación WebEx Meetings:

Ejemplo:
Por ejemplo, la línea de comando inicial es: msiexec /i "nbr2player_onprem.msi" /qn

Paso 3 Ahora, puede anunciar el programa.

a) Abra la consola de administrador SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Reproductor de grabaciones en red de Cisco WebEx de Cisco WebEx LLC (inglés)** > **Programas**.
b) Haga clic con el botón derecho del ratón en **Por sistema desatendido**.
c) Seleccione **Todas las tareas** > **Distribuir software**.
d) Seleccione **Siguiente** en el **Asistente Distribuir programa**.
e) Seleccione el servidor SMS y seleccione **Siguiente**.
f) Seleccione la colección y **Siguiente**.
g) Introduzca el nombre del anuncio en el campo **Nombre** y seleccione **Siguiente**.
h) Especifique si la publicidad debería aplicarse a subcolecciones y seleccione **Siguiente**.
i) Especifique cuándo se anunciará el programa y seleccione **Siguiente**.
j) Especifique si desea asignar el programa y seleccione **Siguiente**.
k) Seleccione **Finalizar** en la página **Completando el asistente Distribuir programa**.
l) Vaya hasta el directorio \Base de datos del sitio\Estado del sistema\Estado del anuncio y compruebe el estado del anuncio.
Si activa la notificación, el usuario verá un mensaje que indica que el programa asignado se va a ejecutar después de que se haya anunciado el programa. El programa asignado se ejecutará de forma silenciosa.

Desinstalación del reproductor de grabación en la red de Cisco WebEx mediante el programa de desinstalación SMS por sistema

El administrador SMS puede desinstalar el reproductor de grabación en la red de Cisco WebEx mediante el programa de desinstalación SMS por sistema realizando el siguiente procedimiento.

Pasos resumidos

1. Utilice el paquete de instalación de SMS creado en Creación de un paquete a partir de la definición, en la página 147.
2. Anuncie el programa de desinstalación por sistema para desinstalar el reproductor de grabación en la red de Cisco WebEx.

Pasos detallados

Paso 1 Utilice el paquete de instalación de SMS creado en Creación de un paquete a partir de la definición, en la página 147.

Paso 2 Anuncie el programa de desinstalación por sistema para desinstalar el reproductor de grabación en la red de Cisco WebEx. El reproductor de grabación en la red de Cisco WebEx se desinstalará en las máquinas especificadas de forma silenciosa.

Reconfiguración de los ajustes tras realizar una actualización

Después de realizar una actualización de su software de Cisco WebEx Meetings Server (CWMS), debe actualizar las rutas a sus aplicaciones de despliegue masivo. (Después de una actualización, el reproductor de grabación en la red se actualiza automáticamente la primera vez que se utiliza para reproducir una grabación).

En sistemas Mac, la ruta es `/Usuarios/(Usuario local)/Biblioteca/Soporte de aplicaciones/Carpeta WebEx/`.

En los sistemas Windows, la ruta depende de la versión, el tipo de descarga y el tipo de navegador web:

- Windows 7 y Windows Vista: <SystemDisk>\ProgramData\WebEx
- Desde las Herramientas de productividad o WebEx Connect, utilice la ruta de las Herramientas de productividad o de WebEx Connect.
- Si está utilizando la instalación MSI, utilice siempre una ruta única. El sistema ignora el archivo existente.
- Si está utilizando el tipo de descarga con Windows 7, el sistema utilizará una ruta única. En Windows XP, si el GPC puede encontrar el valor de tabla registrado, el sistema utilizará la carpeta existente. De lo contrario, el sistema utilizará su propia ruta tal como se ha descrito anteriormente.

Las aplicaciones de cliente tanto en sistemas Windows como en sistemas Mac se actualizan automáticamente para mantener la compatibilidad con el sistema actualizado.

En un entorno bloqueado, debe realizar las actualizaciones de forma manual para los sistemas Windows, pero no para los sistemas Mac.

Nota La versión de las herramientas de productividad y la aplicación de reuniones correspondiente a la versión de Cisco WebEx Meeting Server se puede encontrar en Matriz de compatibilidad de la aplicación Cisco WebEx Meetings y las herramientas de productividad, en la página 210.

CAPÍTULO 8

Configuración del SSO de SAML

- Descripción general del inicio de sesión único, página 159
- Ventajas de inicio de sesión único, página 160
- Información general de la configuración del inicio de sesión único de SAML 2.0, página 161
- SAML SSO para inicio de sesión en el sitio del usuario final y en el de administración, página 162
- Diferencias de inicio de sesión único SAML 2.0 entre los servicios de reunión de WebEx basados en la nube y el servidor de WebEx Meetings, página 162
- Atributos de aserciones SAML, página 170

Descripción general del inicio de sesión único

Los estándares del inicio de sesión único (SSO) integrado, como SAML 2.0, proporcionan mecanismos seguros para transferir credenciales e información relacionada entre diferentes sitios web que tienen sus propios sistemas de autorización y autenticación. SAML 2.0 es un estándar abierto desarrollado por OASIS Security Services Technical Committee.

El protocolo SAML 2.0 ha logrado un éxito significativo, ganando impulso en servicios financieros, educación superior, gobiernos y otros segmentos. Todos los grandes proveedores de gestión de acceso Web han implementado el soporte de SAML 2.0. La Administración de servicios general del gobierno de los EE. UU. (GSA) exige a todos los proveedores que participan en el programa E-Authentication Identity Federation compatibilidad con SAML 2.0.

Los sitios Web compatibles con SAML 2.0 intercambian información de credenciales de usuarios a través de aserciones SAML. Una aserción SAML es un documento XML que contiene declaraciones de confianza acerca de un tema que incluya, por ejemplo, un nombre de usuario y privilegios. Las aserciones SAML suelen está firmadas digitalmente con el fin de garantizar su autenticidad.

Muchas grandes empresas han desplegado sistemas de Gestión de acceso e identidad integrada (IAM) y Proveedor de identidad (IdP), como Ping Identity Ping Federate, CA SiteMinder, Open AM y Windows ADFS 2.0, en sus intranets corporativas. Estos sistemas IAM e IdP manejan la autenticación de usuario y los requisitos para empleados y colaboradores. Los sistemas IAM e IdP utilizan los protocolos SAML para interactuar con sitios Web asociados fuera de sus cortafuegos. Los usuarios pueden utilizar sus sistemas IAM e IdP para autenticar automáticamente a sus usuarios en los servicios de reuniones de Cisco WebEx. Esto aumenta la eficiencia, ya que los usuarios no tienen que recordar sus nombres de usuario y contraseñas para iniciar o unirse a reuniones en sus sitios de Cisco WebEx.

Nota El servidor de WebEx Meetings sólo es compatible con el IdP de SAML 2.0. No es compatible con IdP basados en los antiguos estándares SAML 1.1 y WS-Federate. Esta restricción contrasta con los servicios de reuniones de Cisco WebEx basados en la nube, que continúan siendo compatibles con SAML 1.1 y WS-Federate. A continuación, aparece una lista de los IdP de SAML 2.0 que se ha comprobado que funcionan con el servidor de Cisco WebEx Meetings:

- Microsoft ADFS 2.0 (complemento gratuito para Microsoft Windows Server 2008/Windows Server 2008 R2 o la función de servidor ADFS en Windows Server 2012)
- Ping Identity Ping Federate 6.6.0.17
- Forgerock Open AM 10.0.0
- CA SiteMinder 6.0 SP5

Dado que SAML 2.0 es un estándar abierto, puede que otros IdP de SAML 2.0 también funcionen con el servidor de Cisco WebEx Meetings. Sin embargo, otros IdP de SAML 2.0 no han sido probados por Cisco. Por tanto, es responsabilidad del usuario realizar la integración.

Ventajas de inicio de sesión único

El inicio de sesión único (SSO) le puede beneficiar de las siguientes maneras:

- Autenticación de usuario simplificada: De forma predeterminada, el servidor de Cisco WebEx Meetings solicita a los usuarios que inicien sesión utilizando las direcciones de correo electrónico y las contraseñas que han seleccionado específicas del sistema del servidor de reuniones. Los usuarios seleccionan sus contraseñas activando sus cuentas del servidor de reuniones. Este enfoque funciona bien para la mayoría de organizaciones pequeñas y medianas, pero las organizaciones más grandes prefieren utilizar la autenticación de usuario con las credenciales corporativas, es decir, Active Directory, para mayor seguridad. Puede lograr ese objetivo utilizando el SSO de SAML 2.0.

  Nota Una ventaja de seguridad adicional del SSO es que la contraseña corporativa en realidad nunca se envía ni se almacena en el servidor de Cisco WebEx Meetings después de que el usuario se autentica correctamente.

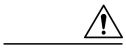
- Gestión de usuarios simplificada: Esto significa que se automatiza lo siguiente:
  - La creación de la cuenta de usuario al entrar en la organización
  - Las actualizaciones de la cuenta de usuario cuando los empleados desarrollan funciones diferentes dentro de la organización
  - La desactivación de la cuenta de usuario al abandonar la organización

  Puede conseguir la automatización para estos eventos configurando **Creación automática de la cuenta** y **Actualización automática de la cuenta** en la sección del servidor de Cisco WebEx Metings Administration Site. Es recomendable activar estas funciones si también las admiten sus IdP de SAML. Las cuentas de usuario se crean y actualizan automáticamente "a petición" cuando los usuarios se autentican correctamente, evitando así la necesidad de crear usuarios manualmente utilizando Cisco

WebEx Admin. Asimismo, los usuarios ya no pueden iniciar sesión en sus cuentas una vez que abandonan la organización, ya que el IdP de SAML 2.0 bloquea el inicio de sesión a esos usuarios tras haber sido eliminados de la base de datos de usuarios del IdP de SAML 2.0, que es por lo general un proxy para el directorio corporativo subyacente.

Información general de la configuración del inicio de sesión único de SAML 2.0

Importante Si usted o el personal de su organización no tiene experiencia con el inicio de sesión única(SSO) de SAML 2.0, le recomendamos que recurra a los servicios de un socio cualificado de AUC de Cisco o Cisco Advanced Services. Le ofrecemos esta recomendación ya que la configuración del SSO de SAML puede ser bastante complicada.



Precaución Si la respuesta SAML tiene un retorno de carro en cualquiera de los campos, entonces la actualización automática, la creación de cuentas y la autenticación fallan. Aunque el proveedor de SAML calcula la firma digital con el retorno de carro, Cisco WebEx Meetings Server elimina el retorno de carro provocando que la firma digital deje de ser válida.

Revise estos pasos generales para el SSO de SAML 2.0:

1. Asegúrese de que la infraestructura del SSO de SAML 2.0 se encuentra ubicada e integrada en el directorio empresarial. Esto implica configurar el software IdP 2.0 de SAML y el sitio web de autenticación del SSO. El sitio web de autenticación es un portal en el que los usuarios introducen sus credenciales corporativas.
2. Asegúrese de que los usuarios pueden acceder al sitio web de autenticación del SSO. Este paso es importante porque, como parte del proceso de inicio de sesión, el servidor de Cisco WebEx Meetings redirecciona a los usuarios al sitio web de autenticación.

Nota Si el sistema del servidor de Cisco WebEx Meetings está habilitado para el acceso público (si permite a los usuarios iniciar sesión y unirse a reuniones desde Internet), es esencial garantizar que la autenticación del sitio web del SSO también sea accesible desde Internet. Normalmente, esto implica implementar IdP de SAML 2.0 en DMZ. Sin este paso extra, los usuarios verán errores de "404 Sitio no encontrado" al iniciar de sesión en el servidor de Cisco WebEx Meetings desde Internet.

3. Conectar el servidor de WebEx Meeting al IdP de SAML 2.0 utilizando estos dos métodos:
   - Seleccione **Configuración** > **Seguridad** > **SSO integrado** en el sitio de administración de Cisco WebEx Meetings Server.
   - Siga las instrucciones en la documentación de IdP de SAML 2.0. Tenga en cuenta que estas instrucciones varían de proveedor a proveedor e incluso podrían cambiar de versión a versión del IdP de SAML 2.0. Éste es otro motivo por el que debe ponerse en contacto con un socio cualificado de AUC de Cisco o con Cisco Advanced Services para que le ayude a implementar la solución.

Nota No utilice las instrucciones que se encuentran en Cisco Developer Network para configurar los IdP de SAML 2.0, ya que están diseñadas para los servicios de reuniones de Cisco WebEx basados en la nube, y por lo tanto, no funcionan de forma óptima con Cisco WebEx Meetings Server.

SAML SSO para inicio de sesión en el sitio del usuario final y en el de administración

SAML SSO se suele configurar sólo para fines de inicio de sesión en el sitio de usuario final y no en el sitio de administración. En los sitios Web de Cisco WebEx Meetings Server con SSO integrado de SAML 2.0, el comportamiento imita el comportamiento de SaaS WebEx en lo referente a la autenticación del usuario. Un administrador de Cisco WebEx Meetings Server (y un administrador de SaaS WebEx) puede iniciar sesión en una cuenta de usuario final mediante SAML SSO, pero debe iniciar sesión en una cuenta de administrador en el mismo sistema utilizando una contraseña distinta. De esta manera, se garantiza que, en caso de errores graves en el IdP de SAML SSO, un administrador seguirá pudiendo acceder al sitio de administración. Sin este sistema a prueba de fallos, puede producirse una situación en la que el sitio de administración quede inaccesible no por un fallo del producto, sino por un problema con el software IdP de SAML SSO. El software IdP de SAML SSO está en un servidor que es externo a Cisco WebEx Meetings Server (o a SaaS WebEx) y, por tanto, fuera de nuestro control.

Diferencias de inicio de sesión único SAML 2.0 entre los servicios de reunión de WebEx basados en la nube y el servidor de WebEx Meetings

Mientras que los servicios de reunión de Cisco WebEx basados en la nube emplean ID de usuarios únicos al crear las cuentas de usuario, el servidor Cisco WebEx Meetings utiliza direcciones de correo electrónico como base para crear cuentas de usuario. Esto tiene las siguientes implicaciones importantes para el inicio de sesión único (SSO) de SAML 2.0:

- Es obligatorio que la aserción SAML lleve la dirección de correo electrónico en el campo NameID. Sin este paso, la autenticación del usuario y la creación de cuenta generan error porque el servidor de Cisco WebEx Meetings no permite la creación de cuentas de usuario sin una dirección de correo electrónico asociada.
- Los servicios de reunión de Cisco WebEx basados en la nube permiten eliminar el dominio del correo electrónico, como "@cisco.com", desde el UPN (nombre principal del usuario) cuando está activada la creación de cuenta automática. Esto causa la creación de una cuenta de usuario que se parece a un ID de usuario. Como WebEx Meetings Server usa una dirección de correo electrónico completa para crear cuentas de usuario, no se puede eliminar el dominio de correo electrónico del UPN.

En la práctica, puede implementar inicialmente el servidor Cisco WebEx Meetings sin SSO SAML 2.0 y activar el SSO más tarde. Hacerlo así conlleva los siguientes efectos importantes en la autenticación de usuario, creación automática de cuenta y las características de actualización automática de cuenta:

Situación	Comportamiento de autenticación de usuario	Creación automática de cuenta (AAC) activada	AAC desactivada	Actualización automática de cuenta (AAU) activada	AAU desactivada
No ha activado SSO. Se han creado cuentas de usuario en el sistema.	Los usuarios inician sesión con sus direcciones de correo electrónico y las contraseñas elegidas por ellos mismos.	No disponible	No disponible	No disponible	No disponible

Situación	Comportamiento de autenticación de usuario	Creación automática de cuenta (AAC) activada	AAC desactivada	Actualización automática de cuenta (AAU) activada	AAU desactivada
A continuación, active el SSO. Los usuarios con cuentas existentes inician sesión en su sitio de WebEx, las herramientas de productividad de WebEx, o la aplicación reuniones Cisco WebEx en sus dispositivos móviles.	Los usuarios son redirigidos al sitio web de autenticación SAML 2.0 IdP y se les solicita que inicien sesión utilizando sus credenciales corporativas, en lugar de direcciones de correo electrónico y contraseñas elegidas por ellos mismos. Los usuarios inician sesión correctamente porque son reconocidos por SAML 2.0 IdP como usuarios válidos. Si no son usuarios válidos, SAML 2.0 IdP les informará de que no pueden utilizar el servidor de WebEx Meetings o de que son usuarios no válidos.	No disponible	No disponible	No disponible	No disponible

Situación	Comportamiento de autenticación de usuario	Creación automática de cuenta (AAC) activada	AAC desactivada	Actualización automática de cuenta (AAU) activada	AAU desactivada
El SSO está activado. Los usuarios no tienen cuentas existentes en el sistema.	Igual que el caso anterior.	Las cuentas de usuario en el servidor de Cisco WebEx Meetings se crean "a demanda" después de que los usuarios inicien sesión. Requisito previo: La aserción SAML contiene una dirección de correo electrónico válida en el campo NameID.	Los usuarios no tienen cuentas existentes en el sistema. Pueden iniciar sesión pero no pueden utilizar el servidor de Cisco WebEx Meetings. La forma más fácil de remediar esta situación es que realice una de las siguientes acciones: • Dejar AAC activado. • Antes de que los usuarios inicien sesión, cree manualmente cuentas de usuario utilizando "Importar archivos CSV" o "Crear usuario" desde el sitio Cisco WebEx Admin.	No disponible	No disponible

Situación	Comportamiento de autenticación de usuario	Creación automática de cuenta (AAC) activada	AAC desactivada	Actualización automática de cuenta (AAU) activada	AAU desactivada
El SSO está activado. Los usuarios iniciaron sesión previamente utilizando el SSO y ahora están intentando iniciar sesión de nuevo.	Igual que el segundo caso.	No disponible	No disponible	Las cuentas de usuario existentes se actualizan automáticamente con cualquier cambio en las credenciales de usuario (normalmente nombre o apellido) mientras que NameID permanezca sin cambios.	No disponible

Situación	Comportamiento de autenticación de usuario	Creación automática de cuenta (AAC) activada	AAC desactivada	Actualización automática de cuenta (AAU) activada	AAU desactivada
Posteriormente desactive el SSO. Este es un caso insólito porque los clientes tienden a dejar activado el SSO después de haberlo activado. Los usuarios iniciaron sesión previamente utilizando el SSO y ahora están intentando iniciar sesión de nuevo.	Si los usuarios introducen sus credenciales corporativas, no pueden iniciar sesión porque el servidor de WebEx Meetings espera que introduzcan sus direcciones de correo electrónico y las contraseñas elegidas por ellos mismos. En esta situación, hay que enseñar a los usuarios a restablecer las contraseñas elegidas por ellos mismos en sus cuentas de WebEx y permitirles tiempo suficiente para actuar antes de desactivar el SSO. Después de restablecer sus contraseñas, los usuarios pueden iniciar sesión con sus direcciones de correo electrónico y las contraseñas elegidas por ellos mismos.	No disponible	No disponible	No disponible	No disponible

Situación	Comportamiento de autenticación de usuario	Creación automática de cuenta (AAC) activada	AAC desactivada	Actualización automática de cuenta (AAU) activada	AAU desactivada
Caso especial: Un usuario es también un administrador del sistema. Caso A: El usuario inicia sesión en el sitio de WebEx. Caso B: El usuario inicia sesión en el sitio de Cisco WebEx Admin.		Caso A: Mismos resultados que el caso anterior. Caso B: No disponible.	Caso A: Mismos resultados que el caso anterior. Caso B: No disponible.	Caso A: Mismos resultados que el caso anterior. Caso B: No disponible.	Caso A: Mismos resultados que el caso anterior. Caso B: No disponible.

Situación	Comportamiento de autenticación de usuario	Creación automática de cuenta (AAC) activada	AAC desactivada	Actualización automática de cuenta (AAU) activada	AAU desactivada
	Caso A: Mismos resultados que el caso anterior Caso B: A diferencia del comportamiento en un sitio de WebEx, cuando el usuario inicia sesión en el sitio Cisco WebEx Admin, siempre se le solicita que introduzca la dirección de correo electrónico y la contraseña que ha elegido por sí mismo. En otras palabras, SSO no tiene efecto cuando inicia sesión en el sitio de Cisco WebEx Admin. Se trata de una medida de seguridad añadida al producto debido a la necesidad de asegurar que los administradores de sistemas siempre pueden iniciar sesión en el sitio Cisco WebEx Admin. Si el sitio Cisco WebEx Admin también admite SSO, el mal funcionamiento de SAML 2.0				

Situación	Comportamiento de autenticación de usuario	Creación automática de cuenta (AAC) activada	AAC desactivada	Actualización automática de cuenta (AAU) activada	AAU desactivada
	IdP o la pérdida de conectividad de red entre el servidor de Cisco WebEx Meetings y SAML 2.0 IdP puede resultar en una situación en la que los administradores de sistemas ya no puedan iniciar sesión y administrar el producto. Esta es la razón por la que SSO no es compatible para el sitio Cisco WebEx Administration.				

Atributos de aserciones SAML

La siguiente tabla enumera los atributos de las aserciones SAML compatibles con Cisco WebEx Meetings Server. Asegúrese de configurar los atributos `lastname`, `firstname`, `email` y `updatetimestamp`. La actualización automática no funciona a menos que esté configurado el atributo `updatetimestamp`.

Atributos de aserciones SAML compatibles

Nombre del atributo	Significado del atributo	Obligatorio para crear usuario automáticamente	Intervalo de valor de entrada	Comentarios
lastname		Sí		
firstname		Sí		
correo electrónico		Sí	Formato de correo electrónico válido	

Nombre del atributo	Significado del atributo	Obligatorio para crear usuario automáticamente	Intervalo de valor de entrada	Comentarios
updateTimeStamp	La hora de actualización de la información del usuario	No	Formato de soporte **formato largo:** muestra: System.currentTimeMillis() **formato LDIF:** AAAAMMDDHHMMSS. AAAA-MM-DD HH:MM:SS muestra: 20090115213256 **formato UTC** ("2009-10-09T06:00:32Z")	Si falta el updateTimeStamp, no puede realizar la actualización automática del usuario, normalmente asignada al elemento whenChanged si el IdP está vinculado a AD.
optionalparams		No		Esos parámetros opcionales pueden configurarse en los formatos que se describen en la sección "Parámetros opcionales" que encontrará más adelante.
OphoneCountry		No		Código de país del teléfono de la oficina
OphoneArea		No		Código de área del teléfono de la oficina
OphoneLocal		No	Introduzca solamente caracteres numéricos. Por ejemplo, 5551212. No introduzca caracteres que no sean numéricos, como guiones o paréntesis.	Prefijo local del teléfono de la oficina
OphoneExt		No		Extensión del teléfono de la oficina
FphoneCountry		No		Código de país del teléfono alternativo
FphoneArea		No		Área del teléfono alternativo
FphoneLocal		No		Teléfono alternativo local
FphoneExt		No		Extensión del teléfono alternativo

Nombre del atributo	Significado del atributo	Obligatorio para crear usuario automáticamente	Intervalo de valor de entrada	Comentarios
PPhoneCountry		No		Código de país del teléfono alternativo 2
PPhoneArea		No		Código de área del teléfono alternativo 2
PPhoneLocal		No		Prefijo local del teléfono alternativo 2
PPhoneExt		No		Extensión del teléfono alternativo 2
MPhoneCountry		No		Código de país del teléfono móvil
MPhoneArea		No		Código de área del teléfono móvil
MPhoneLocal		No		Prefijo local del teléfono móvil
MPhoneExt		No		Extensión del teléfono móvil
Zona horaria		No		Zona horaria (consulte la sección "Zonas horarias" que encontrará más adelante)
Dirección1		No		Dirección1
Dirección2		No		Dirección2
Ciudad		No		Ciudad
State		No		State
ZIP Code		No		ZIP Code
País		No		País (consulte la sección "Valores de país" que encontrará más adelante)
Región		No		Región (consulte la sección "Valores de región" que encontrará más adelante)
Idioma		No		Idioma (consulte la sección "Valores de idioma" que encontrará más adelante)

Nombre del atributo	Significado del atributo	Obligatorio para crear usuario automáticamente	Intervalo de valor de entrada	Comentarios
TC1	cadena	No	Grupo de códigos de seguimiento 1 introducido por un usuario en el sitio de administración	Índice 1
TC2	cadena	No	Grupo de códigos de seguimiento 2 introducido por un usuario en el sitio de administración	Índice 2
TC3	cadena	No	Grupo de códigos de seguimiento 3 introducido por un usuario en el sitio de administración	Índice 3
TC4	cadena	No	Grupo de códigos de seguimiento 4 introducido por un usuario en el sitio de administración	Índice 4
TC5	cadena	No	Grupo de códigos de seguimiento 5 introducido por un usuario en el sitio de administración	Índice 5
TC6	cadena	No	Grupo de códigos de seguimiento 6 introducido por un usuario en el sitio de administración	Índice 6
TC7	cadena	No	Grupo de códigos de seguimiento 7 introducido por un usuario en el sitio de administración	Índice 7
TC8	cadena	No	Grupo de códigos de seguimiento 8 introducido por un usuario en el sitio de administración	Índice 8
TC9	cadena	No	Grupo de códigos de seguimiento 9 introducido por un usuario en el sitio de administración	Índice 9
TC10	cadena	No	Grupo de códigos de seguimiento 10 introducido por un usuario en el sitio de administración	Índice 10

Parámetros opcionales

Puede configurar los ajustes de optionalparams de la siguiente manera:

- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="optionalparams">
- <saml:AttributeValue xsi:type="xs:string">Ciudad=Toronto</saml:AttributeValue >
- <saml:AttributeValue xsi:type="xs:string">AA=DESACTIVADO</saml:AttributeValue >
- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="City">
- <saml:AttributeValue xsi:type="xs:string">Toronto</saml:AttributeValue>
- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="AA">
- <saml:AttributeValue xsi:type="xs:string">DESACTIVADO</saml:AttributeValue>

Valores de zona horaria

Zona horaria	Valor
Islas Marshall (hora de línea de fecha, GMT-12:00)	0
Samoa (hora de Samoa, GMT-11:00)	1
Honolulu (hora de Hawai, GMT-10:00)	2
Anchorage (hora de verano de Alaska, GMT-08:00)	3
San Francisco (hora de verano del Pacífico, GMT-07:00)	4
Arizona (hora de la región montañosa, GMT-07:00)	5
Denver (hora de verano de la región montañosa, GMT-06:00)	6
Chicago (hora de verano central, GMT-05:00)	7
Ciudad de México (hora de verano de México, GMT-05:00)	8
Saskatchewan (hora central, GMT-06:00)	9
Bogotá (hora del Pacífico de Sudamérica, GMT-05:00)	10
Nueva York (hora de verano del Este, GMT-04:00)	11
Indiana (hora de verano del Este, GMT-04:00)	12
Halifax (hora de verano del Atlántico, GMT-03:00)	13
La Paz (hora de Sudamérica Occidental, GMT-04:00)	14
Terranova (hora de verano de Terranova, GMT-02:30)	15
Brasilia (hora estándar del Este de Sudamérica, GMT-03:00)	16

Zona horaria	Valor
Buenos Aires (hora del Este de Sudamérica, GMT-03:00)	17
Atlántico central (hora del Atlántico central, GMT-02:00)	18
Azores (hora de verano de Azores, GMT)	19
Reikiavik (hora de Greenwich, GMT)	20
Londres (hora de verano GMT, GMT+01:00)	21
Ámsterdam (hora de verano de Europa, GMT+02:00)	22
París (hora de verano de Europa, GMT+02:00)	23
Berlín (hora de verano de Europa, GMT+02:00)	25
Atenas (hora de verano de Grecia, GMT+03:00)	26
El Cairo (hora de Egipto, GMT+02:00)	28
Pretoria (hora de Sudáfrica, GMT+02:00)	29
Helsinki (hora de verano de Europa del norte, GMT+03:00)	30
Tel Aviv (hora de verano de Israel, GMT+03:00)	31
Riad (hora de Arabia Saudita, GMT+03:00)	32
Moscú (hora de Rusia, GMT+04:00)	33
Nairobi (hora de Nairobi, GMT+03:00)	34
Teherán (hora de verano de Irán, GMT+04:30)	35
Abu Dhabi, Muscat (hora de Arabia, GMT+04:00)	36
Bakú (hora de verano de Bakú, GMT+05:00)	37
Kabul (hora de Afganistán, GMT+04:30)	38
Ekaterimburgo (hora de Asia occidental, GMT+06:00)	39
Islamabad (hora de Asia occidental, GMT+05:00)	40
Bombay (hora de India, GMT+05:30)	41
Colombo (hora de Colombo, GMT+05:30)	42
Almatý (hora de Asia central, GMT+06:00)	43
Bangkok (hora de Bangkok, GMT+07:00)	44
Pekín (hora de China, GMT+08:00)	45
Perth (hora de Australia occidental, GMT+08:00)	46
Singapur (hora de Singapur, GMT+08:00)	47

Zona horaria	Valor
Taipéi (hora de Taipéi, GMT+08:00)	48
Tokio (hora de Japón, GMT+09:00)	49
Seúl (hora de Corea, GMT+09:00)	50
Yakutsk (hora de Yakutsk, GMT+10:00)	51
Adelaida (hora estándar de Australia central, GMT+09:30)	52
Darwin (hora de Australia central, GMT+09:30)	53
Brisbane (hora de Australia oriental, GMT+10:00)	54
Sídney (hora estándar de Australia oriental, GMT+10:00)	55
Guam (hora del Pacífico occidental, GMT+10:00)	56
Hobart (hora estándar de Tasmania, GMT+10:00)	57
Vladivostok (hora de Vladivostok, GMT+11:00)	58
Islas Salomón (hora del Pacífico central, GMT+11:00)	59
Wellington (hora estándar de Nueva Zelanda, GMT+12:00)	60
Fiyi (hora de Fiyi, GMT+12:00)	61
Estocolmo (hora de verano de Suecia, GMT+02:00)	130
Tijuana (hora de verano de México Pacífico, GMT-07:00)	131
Chihuahua (hora de verano de México, región montañosa, GMT-06:00)	132
Caracas (hora de Sudamérica Occidental, GMT-04:30)	133
Kuala Lumpur (hora de Malasia, GMT+08:00)	134
Recife (hora del Este de Sudamérica, GMT-03:00)	135
Casablanca (hora de verano de Marruecos, GMT+01:00)	136
Tegucigalpa (hora de Honduras, GMT-06:00)	137
Nuuk (hora de verano de Groenlandia, GMT-02:00)	138
Amán (hora de verano de Jordania, GMT+03:00)	139
Estambul (hora de verano de Europa oriental, GMT+03:00)	140
Katmandú (hora de Nepal, GMT+05:45)	141

Zona horaria	Valor
Roma (hora de verano de Europa, GMT+02:00)	142
África occidental (hora de África occidental, GMT+01:00)	143
Madrid (hora de verano de Europa, GMT+02:00)	144

Valores de los códigos de los países o regiones

Estado Islámico de Afganistán	93
Albania	355
Argelia	213
Samoa Americana	1684
Andorra	376
Angola	244
Anguilla	1264
Antártida	672_1
Antigüa (incluida Barbuda)	1268
Argentina	54
Armenia	374
Aruba	297
Islas de la Ascensión	247
Australia	61
Austria	43
Azerbaiyán	994
Bahamas	1242
Bahrein	973
Bangladesh	880

Barbados	1246
Bielorrusia	375
Bélgica	32
Belice	501
Benín	229
Bermudas	1441
Bután	975
Bolivia	591
Bosnia_Herzegovina	387
Botswana	267
Brasil	55
Islas Vírgenes (R.U.)	1284
Brunei	673
Bulgaria	359
Burkina Faso	226
Burundi	257
Camboya	855
Camerún	237
Canadá	1_1
Isla de Cabo Verde	238
Islas Caimán	1_9
República Centroafricana	236
República del Chad	235
Chile	56
China	86

Colombia	57
Comores	269_1
Islas Cook	682
Costa Rica	506
Croacia	385
Cuba	53
Chipre	357
República Checa	420
Dinamarca	45
Isla de Diego García	246
Yibuti	253
Dominica	1767
República Dominicana	1809
Ecuador	593
Egipto (El Cairo no incluido)	20
El Salvador	503
Guinea Ecuatorial	240
Eritrea	291
Estonia	372
Etiopía	251
Islas Faroe	298
Islas Malvinas	500
Islas Fiji	679
Finlandia	358
Francia	33

Departamentos Franceses (Océano Índico)	262
Guayana Francesa	594
Polinesia Francesa	689
Gabón	241
Gambia	220
Georgia	995
Alemania	49
Ghana	233
Gibraltar	350
Grecia	30
Groenlandia	299
Granada	1473
Guadalupe	590
Guantánamo (Base militar de los EE. UU.)	53_1
Guatemala	502
Guinea	224
Guinea-Bisáu	245
Guyana	592
Haití	509
Honduras	504
Hong Kong	852
Hungría	36
Islandia	354
India	91
Indonesia	62

Irán	98
Irak	964
Irlanda	353
Israel	972
Italia	39_1
Costa de Marfil	225
Jamaica	1876
Japón	81
Jordania	962
Kazajstán	7_1
Kenia	254
Kiribati	686
Corea del Norte	850
Corea del Sur	82
Kuwait	965
Kirguizistán	996
Laos	856
Letonia	371
Líbano	961
Lesotho	266
Liberia	231
Libia	218
Liechtenstein	423
Lituania	370
Luxemburgo	352

Macao	853
Macedonia	389
Madagascar	261
Malawi	265
Malasia	60
Maldivas	960
Mali	223
Malta	356
Islas Marshall	692
Mauritania	222
Mauricio	230
Isla Mayotte	269
México	52
Micronesia	691
Moldavia	373
Mónaco	377
Mongolia	976
Montserrat	1664
Marruecos	212
Mozambique	258
Myanmar	95
Namibia	264
Nauru	674
Nepal	977
Países Bajos	31

Antillas Holandesas	599_2
Nueva Caledonia	687
Nueva Zelanda	64
Nicaragua	505
Níger	227
Niue	683
Islas Norfolk	672
Islas Marianas del Norte, Commonwealth de las	1670
Noruega	47
Omán	968
Paquistán	92
Palau	680
Panamá	507
Papúa Nueva Guinea	675
Paraguay	595
Perú	51
Filipinas	63
Polonia	48
Portugal	351
Puerto Rico	1787
Qatar	974
Rumanía	40
Rusia	7
Ruanda	250
San Marino	378

Santo Tomé	239
Arabia Saudí	966
República de Senegal	221
Serbia	381
Islas Seychelles	248
Sierra Leona	232
Singapur	65
Eslovaquia	421
Eslovenia	386
Islas Salomón	677
Somalia	252
Sudáfrica	27
España	34
Sri Lanka	94
Santa Elena	290
San Cristóbal y Nieves	1869
Santa Lucía	1758
San Pedro y Miquelón	508
San Vicente	1784
Sudán	249
Surinam	597
Suazilandia	268
Suecia	46
Suiza	41
Siria	963

Taiwán	886
Tajikistán	992
Tanzania	255
Tailandia	66
Togo	228
Islas Tonga	676
Trinidad y Tobago	1868
Túnez	216
Turquía	90
Turkmenistán	993
Turks y Caicos	1649
Tuvalu	688
Uganda	256
Ucrania	380
Emiratos Árabes Unidos	971
Reino Unido	41
Estados Unidos de América	1
Uruguay	598
Uzbekistán	998
Vanuatu	678
Ciudad del Vaticano	39
Venezuela	58
Vietnam	84
Islas Wallis y Futuna	681
Samoa Occidental	685

Yemen	967
Zambia	260
Zimbabwe	263

Valores de región

Región	Valor
EE. UU.:	2
Australia	3
Canadá	4
Canadá francófona	5
China	6
Francia	7
Alemania	8
Hong Kong	9
Italia	10
Japón	11
Corea	12
Nueva Zelanda	13
España	14
Suiza	16
Taiwán	17
R.U.	18
México	19
Argentina	20
Chile	21
Colombia	22
Venezuela	23
Brasil	24
Portugal	25
Bélgica	26

Región	Valor
Países Bajos	27
Rusia	28
India	29

Valores de idioma

Idioma	Valor
Español castellano	11
Neerlandés	14
Inglés de Reino Unido	1
Francés	7
Alemán	9
Italiano	10
Japonés	5
Coreano	6
Español de Latinoamérica	12
Portugués	15
Ruso	16
Chino simplificado	3
Chino tradicional	4

Códigos de idioma

Idioma	País/Región
Español castellano	34
Chino	852, 853, 886
Neerlandés	31, 32
Francés	33, 242, 243
Alemán	41, 43, 49
Italiano	39
Japonés	81
Coreano	82

Idioma	País/Región
Español de Latinoamérica	52, 54, 56, 57, 58,
Mandarín	86
Portugués	55, 351
Ruso	7
Inglés de Reino Unido	44, 61, 64, 91
EE. UU.: Español	1

CAPÍTULO 9

Grabaciones de reuniones

Las grabaciones de reuniones consumen espacio en su servidor de almacenamiento. En esta sección se describen los umbrales del servidor de almacenamiento, las alarmas, el consumo de grabación de reuniones del espacio del servidor de almacenamiento y el proceso de purgado de grabaciones antiguas.

- Acerca de las grabaciones de reuniones, página 189
- Almacenamiento recomendado para los archivos de copia de seguridad, página 190

Acerca de las grabaciones de reuniones

Puede configurar un servidor de almacenamiento de cualquier capacidad. El número de grabaciones de reuniones de WebEx guardadas depende de la cantidad de almacenamiento que se haya configurado. Periódicamente, debería archivar las grabaciones guardadas en otros soportes si su empresa requiere que almacene más de seis meses de grabaciones de reuniones.

La tabla siguiente proporciona una estimación general de la cantidad de almacenamiento que se necesita para una hora de grabaciones de reuniones. Utilice estos valores para que le ayuden a calcular la cantidad de almacenamiento que se necesita para seis meses de grabaciones de reuniones.

Contenido de la reunión	Espacio de almacenamiento aproximado necesario para una hora de grabaciones de reuniones
Uso compartido de aplicaciones	36 MB
Voz	30 MB
Vídeo de 180p	104 MB
Vídeo de 360p	337 MB

Nota Los vídeos de webcams se almacenan en la resolución original para la grabación de la reunión. No obstante, al reproducir la grabación, la resolución del vídeo se limita a vídeo de 180p.

Su sistema lleva a cabo dos tareas para mantener el espacio de grabación:

- Después de seis meses, elimina las grabaciones definidas para eliminación por parte de sus usuarios.
- Si sus grabaciones superan un umbral específico durante un periodo de tres meses, elimina las grabaciones definidas para eliminación antes de seis meses.

Cuando un usuario elimina una grabación, deja de estar disponible en la interfaz de usuario pero se conserva en el almacenamiento durante seis meses. Por lo tanto, podrá tener acceso al servidor de almacenamiento para copiar, hacer copias de seguridad o utilizar los archivos de grabación durante seis meses después de que el usuario los haya marcado para su supresión, pero necesitará ponerse en contacto con el Centro de asistencia técnica (TAC) de Cisco para recuperar la grabación.

Como punto de partida, asigne 1 TB de almacenamiento para almacenar seis meses de grabaciones de reuniones. Si las grabaciones de su sistema consumen más del 75 por ciento del espacio asignado después de tres meses, el sistema elimina automáticamente los 10 primeros archivos que el usuario haya establecido para la eliminación.

Por ejemplo, si un usuario elimina dos archivos hoy, y después cinco archivos mañana, y después nueve archivos pasado mañana, y después el uso del almacenamiento supera el límite del 75% después de 3 meses, el sistema elimina los primeros dos archivos hoy, los siguientes cinco archivos mañana y después los primeros tres archivos eliminados pasado mañana.

Nota Si un usuario sin darse cuenta elimina una grabación de la página Grabaciones de reunión de Cisco WebEx pero la grabación está guardada en el servidor de almacenamiento NFS (el sistema de archivos de red), póngase en contacto con el Centro de asistencia técnica (TAC) de Cisco para obtener ayuda acerca de la recuperación de la grabación.

Almacenamiento recomendado para los archivos de copia de seguridad

Archivos de copia de seguridad de Cisco WebEx Meetings

La recomendación general para la cantidad de almacenamiento necesario para las copias de seguridad del sistema, que no incluye las grabaciones de reuniones, es de como mínimo 900 MB o espacio suficiente para dar cabida a hasta tres archivos de copia de seguridad. El sistema purga automáticamente los archivos de copia de seguridad más antiguos y almacena únicamente la copia de seguridad más reciente.

Tenga presentes las cuestiones siguientes al determinar el espacio de almacenamiento necesario para las copias de seguridad:

- El número de usuarios
- El número medio de reuniones que se llevan a cabo cada día
- El tamaño de la base de datos, que aumentará con el tiempo
- Con los despliegues de HA, puede haber retrasos en el transporte de diarios de transacciones debido a la latencia de la red o a una elevada carga del sistema durante la réplica de datos. Esto puede aumentar el tamaño de un archivo de copia de seguridad.

La supervisión del tamaño de la copia de seguridad en el escritorio mostrará las necesidades aproximadas de espacio de almacenamiento. Deje suficiente espacio en el servidor de almacenamiento para al menos el triple del tamaño de copia de seguridad observado.

CAPÍTULO 10

MIB y controles SNMP compatibles

En este apartado se describen las MIB disponibles en su sistema. Al acceder a los datos de su MIB, expondrá MIB adicionales no mencionadas en esta sección. Las MIB adicionales que exponga en el proceso se utilizarán principalmente de forma interna para cuestiones como administración entre máquinas virtuales. Cisco no admite la supervisión SNMP del cliente a través de estas MIB, ni existe ninguna garantía de que estas MIB vayan a utilizarse en futuras versiones de Cisco WebEx Meetings Server.

- MIB SNMP compatibles, página 193
- Controles SNMP compatibles, página 199

MIB SNMP compatibles

Las siguientes secciones describen las MIB SNMP compatibles con Cisco WebEx Meetings Server.

Información sobre el sistema de Cisco WebEx Meetings Server

Objeto	Tipo	Privilegios de lectura/ escritura	OID	Descripción
cwCommSystemVersion	cadena	RO	.1.3.6.1.4.1.9.9.809.1.1.1	Este objeto proporciona la versión del sistema de WebEx.
cwCommSystemObjectID	AutonomousType	RO	.1.3.6.1.4.1.9.9.809.1.1.2	Este objeto proporciona el sysObjectID definido en SNMPv2-MIB.

MIB relacionadas con la CPU

Objeto	Tipo	Privilegios de lectura/ escritura	OID	Descripción
cwCommCPUTotalUsage	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.1	Este objeto proporciona el porcentaje total de uso de CPU de un componente del host. El uso total de CPU incluye el uso de CPU del usuario, el uso de CPU del sistema y el uso de CPU de Nice. Tiempo de usuario de CPU: Tiempo de CPU transcurrido en el espacio de usuario. Tiempo de CPU del sistema: Tiempo de CPU transcurrido en el espacio de kernel. Tiempo de CPU de Nice: Tiempo de CPU dedicado a los procesos de prioridad baja.
cwCommCPUUsageWindow	Gauge32	RW	.1.3.6.1.4.1.9.9.809.1.2.1.2	Este objeto controla el tiempo (en segundos) que se debe esperar antes de enviar un error de tipo trap tras traspasar un umbral de uso de CPU. La notificación se envía solamente si el uso de la CPU traspasa un nivel de umbral (normal/importante/menor) y permanece en el nuevo nivel de umbral más tiempo del definido en esta ventana.
cwCommCPUTotalNumber	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.3	Este objeto indica el número total de las CPU del sistema.
cwCommCPUUsageTable	N/D	No accesible	.1.3.6.1.4.1.9.9.809.1.2.1.4	Lista de uso de CPU que se registra en el dispositivo.

Objeto	Tipo	Privilegios de lectura/ escritura	OID	Descripción
cwCommCPUIndex	Unsigned32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.1	Este objeto identifica de forma exclusiva a una CPU en la tabla. Cada CPU tiene sus propios valores de uso y desglose.
cwCommCPUName	cadena	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.2	Este objeto proporciona el nombre de la CPU. Por ejemplo, Intel® Xeon™ CPU 3.00GHz.
cwCommCPUUsage	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.3	Este objeto indica qué porcentaje de los recursos totales de la CPU se han utilizado. Normalmente se utiliza Ghz para medir la capacidad de la CPU. Puesto que Ghz es demasiado grande para medir algunas categorías de uso de CPU, se utiliza KHz como unidad de medida. La velocidad del sistema (en KHz) se multiplica por la fracción de cada sección de CPU (por ejemplo, Nice, usuario) para obtener el valor de KHz de CPU de cada categoría. Se utiliza KHz como unidad para todas las categorías de CPU indicadas a continuación.
cwCommCPUUsageUser	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.4	Este objeto indica la capacidad de la CPU utilizada en el modo de usuario.

Objeto	Tipo	Privilegios de lectura/ escritura	OID	Descripción
cwCommCPUUsageNice	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.5	Este objeto indica la capacidad de la CPU utilizada en procesos de baja prioridad. Nice es un programa que se encuentra en UNIX y Linux. Se correlaciona directamente con una llamada de kernel del mismo nombre. Nice se utiliza para invocar una utilidad o secuencia de comandos de consola (shell) con una determinada prioridad, para otorgar al proceso más o menos tiempo de CPU que a otros procesos.
cwCommCPUUsageSystem	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.6	Este objeto indica la capacidad de la CPU utilizada en el modo de kernel.
cwCommCPUUsageIdle	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.7	Este objeto indica la capacidad de la CPU utilizada en estado de inactividad.
cwCommCPUUsageIOWait	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.8	Este objeto indica la capacidad de la CPU utilizada cuando se espera a que se complete el proceso de entrada/salida del disco.
cwCommCPUUsageIRQ	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.9	Este objeto indica la capacidad de la CPU utilizada cuando se gestiona una solicitud de interrupción.

Objeto	Tipo	Privilegios de lectura/ escritura	OID	Descripción
cwCommCPUUsageSoftIRQ	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.10	Este objeto indica la capacidad de la CPU utilizada cuando se gestiona una solicitud de interrupción de software.
cwCommCPUUsageSteal	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.11	Este objeto indica la capacidad de la CPU utilizada en otras tareas en ejecución en un entorno virtualizado.
cwCommCPUUsageCapacitySubTotal	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.12	Este objeto indica la capacidad total actual de la CPU.
cwCommCPUMonitoringStatus	cadena	RO	.1.3.6.1.4.1.9.9.809.1.2.1.5	Este objeto indica el estado de supervisión de los recursos de la CPU: • cerrado (0): recurso no disponible. • abierto (1): recurso disponible.
cwCommCPUCapacityTotal	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.6	Este objeto indica la capacidad general de la CPU.

Información de memoria de Cisco WebEx Meetings Server

Objeto	Tipo	Privilegios de lectura/ escritura	OID	Descripción
cwCommMEMUsage	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.2.1	Este objeto indica el uso de memoria física de la máquina virtual.

Objeto	Tipo	Privilegios de lectura/ escritura	OID	Descripción
cwCommMEMMonitoringStatus	cadena	RO	.1.3.6.1.4.1.9.9.809.1.2.2.2	Este objeto indica el estado de supervisión de los recursos de la memoria: • cerrado (0): recurso no disponible. • abierto (1): recurso disponible.
cwCommMEMTotal	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.2.3	Este objeto indica el tamaño total de la memoria física (en KB) del host.
cwCommMEMSwapUsage	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.3.1	Este objeto indica el uso de la memoria física (en porcentaje) y de la memoria de intercambio del host.
cwCommMEMSwapMonitoringStatus	cadena	RO	.1.3.6.1.4.1.9.9.809.1.2.3.2	Este objeto indica el estado de supervisión de la memoria y de la memoria de intercambio. • cerrado (0): está disponible el estado de la memoria y la memoria de intercambio. • abierto (1): no está disponible el estado de la memoria y la memoria de intercambio.

Uso de disco

Objeto	Tipo	Privilegios de lectura/ escritura	OID	Descripción
cwCommDiskUsageCount	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.5.1	Este objeto proporciona un recuento de cuántos discos (por ejemplo, disco local, disco remoto, disco de grabaciones de reuniones) están disponibles en el sistema.
cwCommDiskUsageIndex	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.1	Este objeto es un índice de entradas en la tabla que contiene la información de gestión genérica relativa al uso de disco.
cwCommDiskPartitionName	cadena	RO	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.2	Este objeto indica el nombre de la partición de disco. Por ejemplo, la partición /opt o /dev.
cwCommDiskUsage	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.3	Este objeto proporciona el uso de disco actual (en porcentaje) en el host.
cwCommDiskTotal	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.4	Este objeto indica el tamaño de espacio de disco total (en MB) de este host.
cwCommDiskMonitoringStatus	cadena	RO	1.3.6.1.4.1.9.9.809.1.2.5.3	Este objeto indica el estado de supervisión de los recursos de disco. • cerrado (0): no está disponible el estado de uso de disco. • abierto (1): está disponible el estado de uso de disco.

Controles SNMP compatibles

Las siguientes secciones describen los controles SNMP compatibles con Cisco WebEx Meetings Server.

Eventos de notificación

Los siguientes eventos son eventos de notificación compatibles.

Nombre	OID	Descripción
cwCommSystemResourceUsageNormalEvent	.1.3.6.1.4.1.9.9.809.0.1	Esta notificación indica que el uso de algunos recursos del sistema pasa a tener el estado normal. El sistema podría enviar esta notificación cuando se da alguno de los siguientes casos: **1** El valor cwCommCPUUsage de una CPU pasa a ser menor que el valor del umbral menor de CPU predefinido. **2** El valor de cwCommMEMUsage pasa a ser menor que el valor del umbral menor de memoria predefinido. **3** El valor de cwCommMEMSwapUsage pasa a ser menor que el valor del umbral menor de memoria de intercambio predefinido. **4** El valor de cwCommFileUsage pasa a ser menor que el valor del umbral menor de archivo predefinido. **5** El valor de cwCommDiskUsage en un disco pasa a ser menor que el valor del umbral menor de disco predefinido.

Nombre	OID	Descripción
cwCommSystemResourceUsageMinorEvent	.1.3.6.1.4.1.9.9.809.0.2	Esta notificación indica que el uso de algunos recursos del sistema pasa a tener el estado menor. El sistema podría enviar esta notificación cuando se da alguno de los siguientes casos: **1** El valor de cwCommCPUUsage de una CPU pasa a ser mayor que o igual al valor del umbral menor de CPU predefinido y menor que el valor de cwCommCPUMajorThreshold. **2** El valor de cwCommMEMUsage pasa a ser mayor que o igual al valor del umbral menor de memoria predefinido y menor que el valor del umbral importante de memoria predefinido. **3** El valor de cwCommMEMSwapUsage pasa a ser mayor que o igual al valor del umbral menor de memoria de intercambio predefinido y menor que el valor del umbral importante de memoria de intercambio predefinido. **4** El valor de cwCommFileUsage pasa a ser mayor que o igual al valor del umbral menor de archivo predefinido y menor que el valor del umbral importante de archivo predefinido. **5** El valor de cwCommDiskUsage de un disco pasa a ser mayor que o igual al valor del umbral menor de disco predefinido y menor que el valor del umbral importante de disco predefinido. La notificación menor significa que el sistema tiene algunos problemas y que el administrador del sistema debe resolverlos.

Nombre	OID	Descripción
cwCommSystemResourceUsageMajorEvent	.1.3.6.1.4.1.9.9.809.0.3	Esta notificación indica que el uso de algunos recursos del sistema pasa a tener el estado importante. El sistema podría enviar esta notificación cuando se da alguno de los siguientes casos: **1** El valor cwCommCPUUsage de una CPU pasa a ser mayor que o igual al valor del umbral importante de CPU predefinido. **2** El valor cwCommMEMUsage pasa a ser mayor que o igual al valor del umbral importante de memoria predefinido. **3** El valor cwCommMEMSwapUsage pasa a ser mayor que o igual al valor del umbral importante de memoria de intercambio predefinido. **4** El valor cwCommFileUsage pasa a ser mayor que o igual al valor del umbral importante de archivo predefinido. **5** El valor cwCommDiskUsage de un disco pasa a ser mayor que o igual al valor del umbral importante de disco predefinido. La notificación importante significa que el sistema está en estado crítico y necesita que el administrador del sistema emprenda acciones inmediatamente.

Datos de controles

Los siguientes datos son datos de error de tipo trap compatibles. Configure el filtro de MIB para recibir solamente los errores de tipo trap descritos a continuación.

Nombre	OID	Convenio textual	Descripción
cwCommNotificationHostAddressType	.1.3.6.1.4.1.9.9.809.1.2.4.1	InetAddressType	Este objeto representa el tipo de la dirección de red disponible mediante cwCommNotificationHostAddress.
cwCommNotificationHostAddress	.1.3.6.1.4.1.9.9.809.1.2.4.2	InetAddress	Este objeto proporciona la dirección IP del host enviada con la notificación.

Nombre	OID	Convenio textual	Descripción
cwCommNotificationResName	.1.3.6.1.4.1.9.9.809.1.2.4.3	CiscoWebExCommSysRes	Este objeto proporciona el nombre del recurso del sistema que se envía con la notificación. Indica que el recurso del sistema mencionado tiene niveles de advertencia predefinidos sobrepasados. 0. cwCommTtoalCPUUsage 1. cwCommMemUsage 2. cwCommMemSwapUsage 3. descriptor de archivo abierto (sin datos MIB) 4. uno de los cwCommDiskTotal
cwCommNotificationResValue	.1.3.6.1.4.1.9.9.809.1.2.4.4	Unsigned32	Este objeto proporciona el valor de porcentaje de uso de recursos del sistema con notificación.
cwCommNotificationSeqNum	.1.3.6.1.4.1.9.9.809.1.2.4.5	Counter32	Este objeto proporciona el número de secuencia. Se utiliza para el seguimiento del orden de las notificaciones.

CAPÍTULO 11

Requisitos del sistema de usuarios

Los requisitos del sistema para que los usuarios finales organicen y accedan a reuniones.

- Requisitos comunes del sistema de PC, página 205
- Requisitos del sistema operativo Windows, página 206
- Requisitos del sistema operativo Mac, página 208
- Requisitos de los sistemas operativos de dispositivos móviles, página 209
- Matriz de compatibilidad de la aplicación Cisco WebEx Meetings y las herramientas de productividad, página 210

Requisitos comunes del sistema de PC

Requisitos del sistema Cisco WebEx Meeting Server (CWMS) comunes a navegadores y sistemas operativos. Los requisitos para el PC del administrador y para el PC del usuario que utiliza las herramientas de productividad son los mismos.

Requisitos del cliente y el navegador

- JavaScript y cookies activadas
- Java 6, Java 7 o Java 8 activado (para navegadores web compatibles con Java)
- Complementos de Cisco WebEx activados para Chrome 32 y posterior o Firefox 27 y posterior
- Complementos habilitados en Safari
- Active X activo y desbloqueado para Microsoft Internet Explorer (recomendado)

Nota Debido a los cambios de políticas de Google y Mozilla, a partir de Chrome 32 y Firefox 27, es posible que los usuarios tengan que activar manualmente el complemento de WebEx al utilizar estos navegadores[22] para unirse a una reunión de WebEx o reproducir una grabación de WebEx. Encontrará más información e instrucciones en https://support.webex.com/webex/meetings/en_US/chrome-firefox-join-faq.htm.

Si un cliente utiliza un navegador distinto de las versiones especificadas de Chrome o Firefox y tiene activado Java, la aplicación Cisco WebEx Meetings se descargará automáticamente en el sistema del cliente la primera vez que el cliente inicie o se incorpore a una reunión. Le recomendamos que indique a todos los clientes que instalen la última actualización para la versión de Java.

Requisitos de SSL y TLS

Ajuste la **Configuración de Internet** en los ordenadores de todos los usuarios para utilizar el cifrado SSL y TLS. Por ejemplo, en un PC Windows:

- Seleccione **Panel de control** > **Opciones de Internet** > **Avanzadas** > **Seguridad** > **Utilizar SSL 3.0**. Recomendamos seleccionar esta opción para mayor compatibilidad.
- Seleccione**Panel de control** > **Opciones de Internet** > **Avanzadas** > **Seguridad** > **Utilizar TLS 1.0** y **Utilizar TLS 1.2**. Recomendamos seleccionar ambas opciones para mayor compatibilidad, pero debe seleccionar **Utilizar TLS 1.0**.

Si sus usuarios van a organizar reuniones para invitados (por ejemplo, usuarios que no trabajan para su empresa), deberá solicitar a sus usuarios invitados que actualicen manualmente los sistemas operativos y los exploradores para admitir SSL y TLS antes de unirse a sus reuniones. Si no realizan estos pasos, experimentarán problemas de compatibilidad. Le recomendamos que incluya las instrucciones anteriores en sus invitaciones a reuniones. Para ello, edite las invitaciones a reuniones correspondientes que encontrará en su sitio de administración en **Configuración** > **Correo electrónico** > **Plantillas.**.

Requisitos del sistema operativo Windows

Sistemas operativos Windows admitidos

- Windows Vista (32/64 bits)
- Windows 7 (32/64 bits)
- Windows 8 (32/64 bits)
- Windows 8,1 (32/64 bits)

Requisitos de hardware para Windows

CPU Intel Core2 Duo o AMD de 2,XX GHz o procesador superior.

Se recomienda un mínimo de 2 GB de RAM.

22 Las versiones exactas de Chrome y Firefox que están afectadas por esta política no se han finalizado en el momento de la publicación de este documento.

Navegadores Windows probados

- Internet Explorer: 8 - 11
- Mozilla Firefox: 10 - 41
- Google Chrome: 23 - 45

Integración con Microsoft Outlook

- Microsoft Outlook 2007 SP2 y superior
- Microsoft Outlook 2010 (ediciones de 32 y 64 bits; todos los Service Packs)
- Microsoft Outlook 2013

La tabla siguiente describe las versiones de Microsoft Outlook que son compatibles en los diversos sistemas operativos.

Versión de Microsoft Outlook (Versión de Cliente/Exchange)	Windows XP SP3	Vista	Windows 7	Windows 8 (solo en modo escritorio)
Outlook 2007/ Exchange 2007	S	S	S	N
Outlook 2010 (32 bits)/ Exchange 2007	S	S	S	S
Outlook 2010 (32 bits)/ Exchange 2010	S	S	S	S
Outlook 2010 (64 bits)/ Exchange 2007	S	S	S	S
Outlook 2010 (64 bits)/ Exchange 2010	S	S	S	S
Outlook 2013/ Exchange 2010	N	N	S	S
Outlook 2010/ Exchange 365 alojado	N	N	S	S
Outlook 2013/ Exchange 2013	N	N	S	S
Outlook 2013/ Exchange 365 alojado	N	N	S	S

Clientes de mensajería instantánea compatibles

- Lync 2010 (32 bits)
- Lync 2013 (32 bits)
- Microsoft Office Communicator 2007
- Microsoft Office Communicator 2007 R2

La tabla siguiente describe las versiones de clientes de mensajería instantánea que son compatibles en los diversos sistemas operativos.

Versión de Instant Messenger	Windows XP SP3	Windows 7	Windows 8
Communicator 2007	S	S	S
Communicator 2007 R2	S	S	S
Lync 2010 (32 bits)	N	S	S
Lync 2013 (32 bits)	N	S	S

Integración con Cisco Jabber para Windows

- Cisco Jabber para Windows 9.2.6
- Cisco Jabber para Windows 9.6.1
- Cisco Jabber para Windows 9.7
- Cisco Jabber para Windows 10.5
- Cisco Jabber para Windows 11.0
- Admite Cisco WebEx Meetings Server con integración de directorio activo/LDAP.

Restricción Jabber for Windows 9.2.6 admite las integraciones con sitios Cisco WebEx Meetings Server versión 1.5 y versiones posteriores que estén configurados para el inicio de sesión único (SSO) de SAML 2.0. Las versiones anteriores de Jabber para Windows no son compatibles con inicio de sesión único.

No todas las versiones o plataformas de Cisco Jabber admiten la integración con Cisco WebEx Meetings Server. (Por ejemplo, Jabber basado en la nube y WebEx Communicator). Para obtener información acerca de la integración con Cisco WebEx Meetings Server, consulte la documentación de Cisco Jabber para Windows en http://www.cisco.com/en/US/products/ps12511/tsd_products_support_series_home.html.

Requisitos del sistema operativo Mac

Sistemas operativos Mac admitidos

- Mac OS X 10.7 Lion

- Mac OS X 10.8 Mountain Lion
- Mac OS X 10.9 Mavericks

Requisitos de hardware de Mac

CPU de 2,0 GHz o más.

Se recomienda un mínimo de 512 MB de RAM.

Navegadores Mac probados

- Mozilla Firefox: 10 - 41
- Apple Safari: 6 - 8
- Google Chrome: 23 - 45

  Consulte la planificación de versiones de Chrome en http://www.chromium.org/developers/calendar

Integración con Cisco Jabber para Mac

Las siguientes integraciones de Cisco Jabber para Mac se admiten para los sitios de Cisco WebEx Meetings Server configurados para el inicio de sesión único (SSO) SAML 2.0 o LDAP/Active Directory.

- Cisco Jabber para Mac 10.5 admite la integración con Cisco WebEx Meetings Server versión 2.5 y posteriores
- Cisco Jabber para Mac 9.6 admite la integración con Cisco WebEx Meetings Server versión 2.0 y posteriores

Requisitos de los sistemas operativos de dispositivos móviles

Después de descargar manualmente la aplicación Cisco WebEx en iOS o Android y de activar la función móvil de WebEx, un usuario puede utilizar la aplicación para iniciar o asistir a una reunión. Un usuario también puede acceder a Cisco WebEx en un dispositivo móvil usando un navegador, pero es posible que no le proporcione la misma experiencia de usuario óptima.

Cisco WebEx Meeting Server versión 2.0 y superiores es compatible con:

- iPhone e iPad de Apple con iOS 6.0 y versiones posteriores.
- Dispositivos móviles Android con Android 2.1 y versiones posteriores.
- Jabber para iPhone y para Android 9.6 y versiones posteriores.

Nota No se pueden reproducir grabaciones en dispositivos móviles. Si ha iniciado una reunión utilizando un dispositivo móvil Android, puede iniciar y gestionar la grabación de una reunión. Si ha iniciado una reunión utilizando un dispositivo móvil iOS, no puede iniciar ni gestionar la grabación de una reunión en el dispositivo iOS.

Matriz de compatibilidad de la aplicación Cisco WebEx Meetings y las herramientas de productividad

La tabla lista los números de compilación de las descargas de la aplicación WebEx Meetings y las herramientas de productividad correspondientes a cada versión de Cisco WebEx Meetings Server.

Versión de Cisco WebEx Meetings Server	Número ISO	Herramientas de productividad de Cisco WebEx[23]	Aplicación Cisco WebEx Meetings
1,5	1.5.1.6	2.80.500.179	27.32.150.179
1.5 MR1	1.5.1.131	2.80.501.130	27.32.151.130
1.5 MR2	1.5.1.223	2.80.501.223	27.32.151.223
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[24]	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)
2.0MR7	2.0.1.707	2.82.1.701	27.32.201.701 (Windows) orion2.0.MR7.0.0.701 (Mac)

Versión de Cisco WebEx Meetings Server	Número ISO	Herramientas de productividad de Cisco WebEx[23]	Aplicación Cisco WebEx Meetings
2.0MR8	2.0.1.809	2.82.1.701	27.32.201.701 (Windows) orion2.0.MR7.0.0.701 (Mac)
2.0MR8 parche de seguridad 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 y Mac)
2.5MR1	2.5.1.132	2.82.500.3339	29.11.3.4858 (Windows y Mac)
2.5MR2	2.5.1.227	2.82.501.10002	29.12.0.10076 (Windows y Mac)
2.5MR3	2.5.1.3009	2.82.501.10008	29.12.0.10076 (Windows y Mac)
2.5MR4	2.5.1.4378	2.82.502.8	29.13.11.10173 (Windows y Mac)
2.5MR5	2.5.1.5033	2.82.502.9	29.13.12.10182 (Windows y Mac)
2.5MR6	2.5.1.6139	2.82.502.11	29.13.41.30001 (Windows y Mac)

23 Los usuarios encontrarán más información sobre las herramientas de productividad de Cisco WebEx en http://www.webex.com/support/productivity-tools.html.

24 Ya no está disponible.

CAPÍTULO 12

Integración de Cisco WebEx Meetings Server con CUCM y compatibilidad del extremo de audio

En este apartado, se proporciona información sobre la integración de Cisco WebEx Meetings Server (CWMS) con Cisco Unified Communications Manager (CUCM), la Session Manager Edition (SME) y la compatibilidad del extremo de audio.

- Integración de Cisco Unified Communications Manager (CUCM), página 213
- Integración de Session Manager Edition (SME), página 213
- Compatibilidad del punto final de audio, página 214

Integración de Cisco Unified Communications Manager (CUCM)

Compatibilidad con Cisco Unified Communications Manager

Cisco WebEx Meetings Server es compatible con las versiones siguientes de Cisco Unified Communications Manager:

- 10.5 (compatible con la versión 2.0MR3 y posteriores).
- 10,0
- 9,1
- 9,0
- 8,6

Integración de Session Manager Edition (SME)

CWMS admite Session Manager Edition (SME).

Los usuarios de Unified MP pueden elegir Cisco WebEx como proveedor de conferencia web al planificar una reunión de Unified MP. La integración de Cisco WebEx está disponible en todas las versiones de Cisco Unified MP a partir de la 6.0.2. Unified MP proporciona conferencias de voz y de vídeo. Los usuarios de

WebEx deben proporcionar la información de la llamada de entrada de voz y vídeo para unirse a la reunión. También pueden usar la función de llamada que está disponible en WebEx para unirse a la reunión.

Compatibilidad del punto final de audio

Puede utilizar cualquier terminal de audio estándar que se conecte a Cisco Unified Communications Manager para entrar en una reunión de WebEx. Entre los terminales de audio compatibles están los teléfonos IP de Cisco, los terminales de Telepresence y los dispositivos PSTN, como teléfonos móviles y fijos. Muchos terminales de audio admiten conectividad de audio y vídeo. Sin embargo, se admite la conectividad de sólo audio con Cisco WebEx Meetings Server.

Para permitir que usuarios de fuera de la organización se unan a reuniones de WebEx mediante dispositivos PSTN, su empresa debe desplegar puertas de enlace analógico-VoIP, como los enrutadores de servicio integrado (ISR) de Cisco. Se ha probado el funcionamiento de los siguientes teléfonos IP con Cisco WebEx Meetings Server:

- Cisco 7960
- Cisco 7970
- Cisco 7971
- Cisco 7940
- Cisco 9951
- Cisco 9971
- Cisco (Tandberg) 7980
- Cisco 7975
- Cisco E20
- Cisco Telepresence (CTS 1100)
- Cisco IP Communicator
- Teléfono con vídeo Lifesize
- Tandberg 1000
- Tandberg 1700
- Polycom
- Cisco Cius
- C20
- EX 60
- EX 90

Otros extremos compatibles con Cisco UC también deberían funcionar con normalidad. Para obtener una lista de teléfonos IP de Cisco Unified compatibles con Cisco Unified Communications Manager y los paquetes de dispositivos disponibles para cada modelo, consulte la Matriz de compatibilidad del paquete de dispositivos de la función de teléfono IP de Cisco Unified y Cisco Unified Communications Manager.