Guía de planificación y requisitos del sistema de Cisco WebEx Meetings Server, versión 2.5

Primera publicación: 28 de mayo de 2014

Última modificación: 22 de octubre de 2014

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)

© 2014 Cisco Systems, Inc. All rights reserved.

CONTENIDO

Requisitos del sistema de WebEx 1

- Requisitos generales del sistema 1
- Herramientas de productividad de WebEx 7
- Usuarios 7
- Tamaños de implementación del sistema 7
- Requisitos para la residencia en conjunto en vCenter 8
- Máquinas virtuales en su sistema 8
- Requisitos mínimos de hardware 9
  - Recursos que consumen 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 la capacidad del sistema 26
- Matriz de mejora o actualización de la versión 30

Introducción y topología del centro de datos para su sistema 33

- Introducción a Cisco WebEx Meetings Server 33
- Información para los clientes de Cisco Unified MeetingPlace 35
- Conceptos generales para la implementación del sistema 35
- Implementación de un centro de datos único 38
- Unión de centros de datos únicos para crear un sistema de centro de datos múltiple (MDC) 38
- Uso de vSphere de VMware con su sistema 39
  - Ventajas de la implementación de un sistema en vSphere de VMware 39
- IOPS y rendimiento del sistema de almacenamiento 42
- Instalación de vSphere ESXi de VMware y configuración del almacenamiento 43
- Entrada en reuniones 44

Topología de red para su sistema 47

- Diseño de las máquinas virtuales en su red 47
- Diferentes tipos de topologías de red para su sistema 48

Topología de red del proxy inverso de Internet interno (IRP) 49
Topología de red de horizonte no dividido 50
Topología de red completamente interna 51
Topología de red de horizonte dividido 52
Redundancia en implementaciones de alta disponibilidad o MDC 54
Consideraciones de red para el proxy inverso de Internet 55
Requisitos del ancho de banda de la red 57
Formación de equipos NIC para agregación de ancho de banda 61
Cambios de red necesarios para su implementación 63
Lista de control de red para su sistema 64
Lista de control de la red para una instalación o expansión con una implementación automática y acceso público 65
Lista de control de red para una instalación o expansión con implementación manual, acceso público y todas las máquinas virtuales internas 67
Lista de control de red para una instalación o expansión con implementación automática, acceso público y un DNS de horizonte no dividido 71
Lista de control de red para una instalación o expansión con implementación manual, acceso público y un DNS de horizonte no dividido 73
Lista de control de red para una instalación o expansión con implementación automática, acceso público y un DNS de horizonte dividido 76
Lista de control de red para una instalación o expansión con implementación manual, acceso público y un DNS de horizonte dividido 79
Lista de control de red para una instalación o expansión con implementación automática y sin acceso público 82
Lista de control de red para una instalación o expansión con implementación manual y sin acceso público 84
URL del sitio de WebEx y de la administración de WebEx 87
Acceso al puerto cuando todas las máquinas virtuales están en la red interna 89
Acceso al puerto con un proxy inverso de Internet en la red DMZ 89
Puertos de vCenter de VMware 95
Puertos de Cisco WebEx Meeting Center 96
Uso de NAT con su sistema 97
Proxies de reenvío 100
Mejores prácticas 101
Mejores prácticas para Cisco WebEx Meetings Server 101

Configuración de Cisco Unified Communications Manager (CUCM) 103
Configuración de Cisco Unified Communications Manager (CUCM) 103
Lista de control de configuración de CUCM para un centro de datos múltiple 105
Lista de control de la configuración de CUCM con o sin alta disponibilidad 106
Configuración de CUCM en un sistema de centro de datos múltiple de CWMS 107
Configuración de CUCM en un sistema de centro de datos múltiple de 250 u 800 usuarios 107
Configuración de CUCM en un sistema de centro de datos múltiple de 2000 usuarios 108
Configuración de CUCM para sistemas de alta disponibilidad y sin alta disponibilidad 109
Configuración de CUCM en sistemas de 50, 250 y 800 usuarios sin alta disponibilidad 110
Configuración de CUCM en sistemas de 50, 250 u 800 usuarios con alta disponibilidad 111
Configuración de CUCM en un sistema de 2000 usuarios sin alta disponibilidad 112
Configuración de CUCM en un sistema de 2000 usuarios con alta disponibilidad 113
Configuración de un perfil de seguridad del enlace troncal de SIP 114
Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de nivelador de carga 114
Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de aplicación 115
Configuración de un perfil de SIP 116
Configuración de un perfil de SIP estándar 116
Configuración de un perfil de SIP TLS 117
Configuración de un perfil de SIP IPv6 117
Administración de certificados de CUCM mediante TLS 117
Carga de certificados de Cisco WebEx Meetings Server 118
Instalación de un certificado de CUCM de terceros 119
Descarga de certificados de CUCM 120
Configuración de un enlace troncal de SIP 121
Configuración de un enlace troncal de SIP en un punto de nivelador de carga 121
Configuración de un enlace troncal de SIP para un punto de aplicación 122
Configuración de un grupo de rutas 123
Configuración de una lista de rutas 124
Configuración de un patrón de ruta 125
Configuración de un patrón de ruta SIP 125
Compatibilidad y soporte de las características de CUCM 126
Compatibilidad del extremo de audio 129
Descarga e implementación masiva de aplicaciones 131

Acerca de las descargas de aplicaciones 131
Descarga de aplicaciones desde el sitio de administración 133
Contenido de los archivos ZIP de las aplicaciones 134
Implementación masiva de las herramientas de productividad de Cisco WebEx 136
Instalación silenciosa de las herramientas de productividad a través de la línea de comandos 137
Desinstalación silenciosa de las herramientas de productividad a través de la línea de comandos 138
Instalación silenciosa utilizando SMS 138
Anuncio de las herramientas de productividad de Cisco WebEx mediante el programa sin supervisión por sistema SMS 138
Eliminación de los componentes de las herramientas de productividad utilizando el programa sin supervisión por sistema 140
Adición de los componentes de las herramientas de productividad utilizando el programa sin supervisión por sistema 141
Desinstalación de las herramientas de productividad utilizando el programa de desinstalación por sistema SMS 143
Anuncio del programa para actualizar la nueva versión de las herramientas de productividad de WebEx 143
Creación de un paquete a partir de una definición 144
Implementación masiva de la aplicación de reuniones 145
Instalación de Cisco WebEx Meetings 145
Desinstalación de Cisco WebEx Meetings de forma local 146
Instalación silenciosa de la aplicación Meetings a través de la línea de comandos 147
Desinstalación silenciosa de la aplicación Meetings a través de la línea de comandos 147
Instalación silenciosa utilizando SMS 147
Anuncio de la aplicación de Cisco WebEx Meetings mediante el programa sin supervisión por sistema SMS 148
Desinstalación de la aplicación de Cisco WebEx Meetings mediante el programa de desinstalación por sistema SMS 149
Implementación masiva del reproductor de grabaciones basadas en red 150
Instalación del reproductor de grabaciones basadas en red 150
Instalación silenciosa del reproductor de grabaciones a través de la línea de comandos 151
Desinstalación silenciosa del reproductor de grabaciones a través de la línea de comandos 151

Instalación silenciosa utilizando SMS 152
Anuncio del reproductor de grabaciones basadas en red de Cisco WebEx mediante el programa sin supervisión por sistema SMS 152
Desinstalación del reproductor de grabaciones basadas en red de Cisco WebEx mediante el programa de desinstalación por sistema SMS 153
Reconfiguración de los parámetros después de realizar una actualización 154
Configuración de SSO con SAML 157
Descripción general del inicio de sesión único 157
Beneficios del inicio de sesión único 158
Descripción general de la configuración del inicio de sesión único con SAML 2.0 159
SSO con SAML para el inicio de sesión del usuario final y de administración 160
Diferencias en el inicio de sesión único con SAML 2.0 entre el servicio de reuniones basado en la nube y WebEx Meetings Server 160
Atributos de la aserción SAML 168
Grabaciones de reuniones 185
Acerca de las grabaciones de reuniones 185
Almacenamiento recomendado para los archivos de copia de seguridad 186
Compatibilidad con MIB y alarmas de SNMP 189
MIB de SNMP admitidas 189
Alarmas de SNMP admitidas 195
Requisitos del sistema del usuario 201
Requisitos del sistema de PC comunes 201
Requisitos del sistema operativo Windows 202
Requisitos para el sistema operativo Mac 205
Requisitos de los sistemas operativos de los dispositivos móviles 205
Matriz de compatibilidad de las herramientas de productividad y la aplicación Cisco WebEx Meetings 206

CAPÍTULO 1

Requisitos del sistema de WebEx

En esta sección se proporciona una descripción general de los requisitos de hardware, CPU y memoria, red y 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 del sistema, página 7
- Requisitos para la residencia en conjunto en vCenter, página 8
- Máquinas virtuales en su sistema, página 8
- Requisitos mínimos de hardware, página 9
- Matriz de la capacidad del sistema, página 26
- Matriz de mejora o actualización de la versión, página 30

Requisitos generales del sistema

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

Nota La tabla sugiere que implemente su almacenamiento interno en una configuración RAID. Para obtener más información, consulte Instalación de vSphere ESXi de VMware y configuración del almacenamiento, en la página 43 en la *Guía de planificación de Cisco WebEx Meetings Server*.

Importante Cuando realiza una *mejora* de la versión 1.x de Cisco WebEx Meeting Server a la versión 2.0 o versión 2.5, los hosts ESXi (servidor Cisco UCS) donde está situada la máquina virtual de administración requieren 1.5 TB de espacio en disco. Consulte la sección en este documento que describe los diferentes tamaños de los sistemas de usuario, que comienza con Sistema de 50 usuarios, en la página 12. Durante la mejora, tendrá dos conjuntos de máquinas virtuales presentes al mismo tiempo en su red; las máquinas virtuales *originales* que ejecutan la versión 1.x y las máquinas virtuales de la *mejora* para la versión más reciente. Para obtener más detalles, consulte la sección "Mejora 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 sobre los requisitos
Servidor del host y procesadores	• Servidor en rack Cisco UCS *C-series* o blade *B-series*. • Compatibilidad con el conjunto de instrucciones AES-NI. • Velocidad del reloj de procesador de 2,4 GHz o superior.
Interfaces de red	Estos requisitos se aplican al NIC entre los hosts ESXi (para las máquinas virtuales de Cisco WebEx Meetings Server) y el interruptor de Ethernet (no a la interfaz de red externa). • Un NIC físico como mínimo para una configuración no redundante. Consulte la sección Sistema de 50 usuarios, en la página 12 para conocer los requisitos especiales cuando el proxy inverso de Internet (IRP) y la máquina virtual de administración están compartiendo un host. • Las configuraciones redundantes deben tener todas las interfaces NIC duplicadas (*en equipos* o *vinculadas*) y conectadas a una estructura de conmutación independiente. • Se recomienda un NIC adicional para la red de administración de VMware (opcional).

Módulo	Notas sobre los requisitos
Almacenamiento interno (DAS) para hosts ESXi donde se implementan las máquinas virtuales internas	• Mínimo de 4 unidades en una configuración RAID-10 o RAID-5. • Mínimo de 1,5 TB de almacenamiento utilizable para implementaciones de sistemas nuevos o para mejoras. • Cuando realice una mejora de la versión 1.x de Cisco WebEx Meetings Server a la versión 2.0 o 2.5, cada uno de los hosts ESXi requerirá de 172 GB a 1118 GB de espacio libre en disco, según el tamaño del sistema y de las máquinas virtuales. Consulte la sección en este documento que describe los diferentes tamaños de los sistemas de usuario, que comienza con Sistema de 50 usuarios, en la página 12. • Segundo arreglo opcional para ESXi. **Nota** Las máquinas virtuales deben usar el aprovisionamiento fuerte para el almacenamiento.
Almacenamiento interno (DAS) para hosts ESXi donde se implementan las máquinas virtuales de IRP	• Mínimo de 2 unidades en una configuración RAID-1. • Mínimo de 300 GB de almacenamiento utilizable. • Puede utilizar las mismas configuraciones que se usan para las máquinas virtuales internas. **Nota** Las máquinas virtuales deben usar el aprovisionamiento fuerte para el almacenamiento.

Módulo	Notas sobre los requisitos
Almacenamiento SAN	• Puede utilizarse como sustituto de DAS. Cisco recomienda la asignación de la misma cantidad de espacio de almacenamiento. • Los servidores blade B-series solo tienen dos unidades de disco duro. Si está usando servidores blade Cisco UCS B-series y planea realizar una mejora a Cisco WebEx Meetings Server versión 2.0 o 2.5, debe usar almacenamiento SAN para cumplir con el requisito de 4 unidades de disco duro en una configuración RAID 5 o RAID 10. • Solo se recomienda para implementaciones donde el personal de soporte tenga experiencia en monitoreo y ajuste de rendimiento de SAN. **Nota** Usted asume la responsabilidad de añadir almacenamiento para los nuevos requisitos de VMware y las expansiones futuras del sistema. • Solo canal de fibra (CF) o canal de fibra sobre Ethernet (FCoE) de 10 Gb. • Los requisitos de rendimiento son los mismos que para DAS. • La latencia total máxima autorizada, según vSphere, es 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 las máquinas virtuales: la suma de los recursos de almacenamiento reservados para cada máquina virtual del sistema CWMS. **Nota** Las máquinas virtuales deben usar el aprovisionamiento fuerte para el almacenamiento.

Módulo	Notas sobre los requisitos
Almacenamiento NAS	• Puede utilizarse como sustituto de DAS o SAN. Cisco recomienda la asignación de la misma cantidad de espacio de almacenamiento. • Le recomendamos que use servidores de almacenamiento NAS con los servidores de rack Cisco UCS C-series. • Solo se recomienda para implementaciones donde el personal de soporte tenga experiencia en el control y el ajuste del rendimiento de NAS. **Nota** Usted asume la responsabilidad de añadir almacenamiento adicional para nuevos requisitos de VMware y expansiones futuras del sistema. • Canal de fibra (FC), sistema de archivos de red (NFS) o solo SCSI. Para obtener más información, 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 máxima autorizada, según vSphere, es 20 ms. Para obtener más información, consulte http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware#Storage. • Espacio total necesario para las máquinas virtuales: la suma de los recursos de almacenamiento reservados para cada máquina virtual del sistema CWMS. • El servidor de archivos debe ser compatible con API de vStorage para la integración de arreglos (VAAI) y utilizar el aprovisionamiento fuerte. **Nota** Si bien el esquema de aprovisionamiento predeterminado para el almacenamiento NAS es el aprovisionamiento ligero, las máquinas virtuales deben usar el aprovisionamiento fuerte para el almacenamiento. A fin de habilitar el aprovisionamiento fuerte para la implementación con el proveedor de almacenamiento NAS, el complemento que proporciona el proveedor de almacenamiento para VAAI se debe instalar en todos los servidores UCS que se utilizan en la implementación de Cisco WebEx Meetings Server.

Módulo	Notas sobre los 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 de VMware por socket de procesador. • vCenter Server 5.0, 5.0 actualización 1, 5.0 actualización 2, 5.1, 5.1 actualización 1, 5.5 **Nota** Por razones de seguridad, 5.1 debe ser versión 1900470 o una versión posterior. • vCenter puede residir en conjunto con Cisco WebEx Meetings Server si se agregan los requisitos del procesador y de la memoria a los requisitos del sistema. Las configuraciones de residencia en conjunto de vCenter se admiten para sistemas de 50 y 250 usuarios solamente. • La residencia en conjunto con productos de Cisco Unified Communications en el mismo host ESXi físico no es compatible. • La residencia en conjunto con máquinas virtuales que no son de Cisco WebEx Meetings Server en el mismo host ESXi físico no es compatible.
Servidor de correo electrónico	• Nombre de dominio totalmente calificado (FQDN) de un servidor de correo que el sistema utilizará 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 usar un servidor de correo electrónico compatible con TLS con certificados de terceros, debe importar los certificados a su sistema. Para obtener más información, consulte "Administrar certificados" en la Guía de administración que está 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 en un sistema de centro de datos múltiple. No se requiere una licencia MDC para un sistema con un centro de datos único. Para obtener más información sobre las licencias MDC, consulte Acerca de las licencias MDC. Licencia de organizador: cada usuario que organizará una reunión debe tener una licencia de organizador para iniciar una reunión web de WebEx, una reunión de audio de WebEx, una reunión de conferencia personal o una reunión de Marcado grupal. 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 les permiten a los usuarios iniciar, planificar o entrar a sesiones de WebEx Meetings desde dentro de las aplicaciones, por ejemplo, Microsoft® Outlook®. Los usuarios pueden encontrar más información en las herramientas de productividad de Cisco WebEx en http://www.webex.com/support/productivity-tools.html.

Cisco WebEx Meetings Server admite las versiones más recientes de las aplicaciones de WebEx, disponibles en la página **Configuración** > **Descargas**. Si los usuarios ejecutan una versión más antigua de las herramientas de productividad de WebEx después de que usted ejecuta una mejora del sistema, podrán planificar, iniciar y entrar a reuniones, pero las últimas características no estarán disponibles. Le recomendamos que arrastre el último .msi de las herramientas de productividad de WebEx en forma silenciosas para proporcionar una experiencia óptima. (Consulte Matriz de compatibilidad de las herramientas de productividad y la aplicación Cisco WebEx Meetings, en la página 206).

Usuarios

El sistema admite un máximo de por vida de 400 000 cuentas de usuarios. Este número representa el total de las cuentas de usuarios activas y desactivadas. Este número máximo de por vida es lo suficientemente grande como para acomodar el crecimiento esperado en la base de datos de los usuarios.

Los administradores no pueden eliminar usuarios del sistema. En cambio, los usuarios son desactivados. Este diseño permite a los administradores reactivar cuentas de usuarios desactivadas previamente, incluso después de largos períodos de inactividad del usuario. Se restauran las reuniones del usuario y otro contenido (incluyendo grabaciones).

Tamaños de implementación del sistema

Determinación del tamaño del sistema

A la hora de determinar el tamaño de su sistema, tenga en cuenta cuántos usuarios espera usted que utilicen el sistema en cualquier momento dado. Por ejemplo, en un sistema de 50 usuarios, el número máximo de usuarios que asisten a las reuniones en forma simultánea es 50. Si más de 50 usuarios intentan entrar a una reunión, aparecerá un mensaje de error para todos los usuarios que intenten entrar a una reunión después de que se supere la cantidad máxima de usuarios; el sistema impedirá que dichos usuarios entren a la reunión. A continuación, se detallan algunas cosas que debe considerar al determinar el tamaño de su sistema:

- Determine el número más grande de usuarios que anticipa entrarán a una reunión en un momento dado, incluidas las ocasiones raras o inusuales.
- Siempre puede expandir el tamaño del sistema a un tamaño más grande. No obstante, el hardware debe cumplir o superar los requisitos mínimos para el sistema de tamaño más grande o deberá comprar hardware adicional.
- Si planea agregar alta disponibilidad o la característica de centro de datos múltiple (MDC) a su sistema, asegúrese de incluir máquinas virtuales adicionales para admitir el sistema de alta disponibilidad 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 residencia en conjunto en vCenter

La ubicación en conjunto de vCenter de VMware (residencia en conjunto) solo se admite con las configuraciones de sistema de 50 y 250 usuarios concurrentes.

Nota Si planea colocar vCenter de VMware en el mismo host que el sistema de 50 o 250 usuarios concurrentes, debe pedir RAM adicional con su servidor de UCS. Para la cantidad exacta de RAM necesaria, consulte los requisitos para ese tamaño del sistema en el capítulo *Requisitos del sistema de WebEx*.

Máquinas virtuales en su sistema

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

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

  Incluida en la máquina virtual de administración en un sistema de 50 usuarios concurrentes.
- Web: proporciona servicios web (lista de reuniones y grabaciones). Permite que el usuario planifique reuniones futuras.

  Incluida en la máquina virtual de administración en un sistema de 50, 250 u 800 usuarios concurrentes.

  Los usuarios finales inician sesión en el sitio web de WebEx. Los administradores inician sesión en el sitio de administración.
- Proxy inverso de Internet (IRP): proporciona acceso público, permitiendo a los usuarios organizar o asistir a las reuniones desde Internet y dispositivos móviles. Se requiere el proxy inverso de Internet para que la fuerza de trabajo móvil asista a reuniones.

  Nota Solo el proxy inverso de Internet que se ofrece con este producto puede utilizarse en este sistema. Los proxies inversos de Internet o niveladores de carga web de otros fabricantes no son compatibles. El proxy inverso de Internet suministrado con este producto está optimizado para administrar tráfico web, audio y datos compartidos en tiempo real de usuarios externos que entran en reuniones desde Internet.

Nota Para los sistemas de 800 y de 2000 usuarios, no recomendamos implementar máquinas virtuales adicionales en un host DMZ. Esto puede provocar una pérdida incrementada del paquete y latencia considerable en las conexiones de los medios.

Nota En esta documentación, utilizamos el término "máquinas virtuales internas" para referirnos a la administración, y si corresponde, a las máquinas virtuales web y multimedia.

El proxy inverso de Internet está localizado en la red DMZ (topologías de red de horizonte no dividido y de horizonte dividido) o en la red interna (todas las topologías de red 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 del proxy inverso de Internet interno (IRP), en la página 49

Requisitos mínimos de hardware

En esta sección se detallan algunos de los servidores Cisco UCS que puede usar para cada tamaño de sistema. Para conocer los requisitos específicos para cada sistema, consulte lo siguiente:

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

Consulte también la "Guía de solicitud de Cisco WebEx Meetings Server" en http://www.cisco.com/c/en/us/products/conferencing/webex-meetings-server/sales-resources-listing.html.

Tabla 1: Tipos de licencia y versiones de ESXi

Tamaño del sistema	Versión de ESXi	Tipo de licencia de vSphere
50 o 250	5.0, 5.1, 5.5	Standard Edition, Enterprise Edition, Enterprise Plus Edition
800 o 2000	5.0, 5.1	Enterprise Plus Edition solamente
	5.5	Standard Edition, Enterprise Edition, Enterprise Plus Edition

Tabla 2: Modelos de host

Tamaño de la implementación	Ejemplo de modelo de 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 residencia en conjunto con vCenter es compatible con implementaciones de sistemas de 50 y 250 usuarios solamente. La residencia en conjunto con productos de Cisco Unified Communications en el mismo host físico no es compatible.

Puede utilizar modelos anteriores del hardware de UCS con su sistema, pero para una mejor experiencia del usuario, utilice el hardware que se menciona en la tabla. Por ejemplo, puede utilizar el UCS C220 M3 para un sistema de 250 usuarios si ya tiene disponible ese hardware.

Al realizar una mejora a Cisco WebEx Meetings Server versión 2.0, se pueden usar servidores blade Cisco UCS B200 M3 con 2 unidades de disco duro siempre que el sistema mejorado use almacenamiento SAN para sus máquinas virtuales. Usar almacenamiento SAN con los servidores blade B-series permite que su sistema cumpla con el requisito de 4 unidades de disco duro en una configuración RAID 5 o RAID 10 para la versión 2.0 de Cisco WebEx Meetings Server.

Nota Para los sistemas de 800 y de 2000 usuarios, no recomendamos implementar máquinas virtuales adicionales en un host DMZ. Esto puede provocar una pérdida incrementada del paquete y latencia considerable en las conexiones de los medios.

Nota El servidor UCS C460 M2 no tiene una unidad de batería de respaldo (BBU). Configure las políticas de caché de escritura en escritura simultánea. Consulte la sección "Configuración de la memoria caché de escritura en una controladora RAID" en Instalación de vSphere ESXi de VMware y configuración del almacenamiento, en la página 43 para obtener más información.

Recursos que consumen Cisco WebEx Meetings Server y el host ESXi

Cisco WebEx Meetings Server está implementado en una o más máquinas virtuales en hosts ESXi. Cisco WebEx Meetings Server y ESXi (componente de VMware que permite la virtualización en el servidor físico de Cisco UCS) consumen recursos de CPU y de memoria, y espacio de almacenamiento. Según el tamaño de su sistema, es posible que vCenter y varias máquinas virtuales se ejecuten en el mismo servidor Cisco UCS.

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

- La calidad de servicio continua para Cisco WebEx Meeting Server en un uso pico del sistema (capacidad máxima)
- ESXi de VMware
- vCenter de VMware (cuando residen en conjunto)

  Para conocer los requisitos para el servidor de vCenter, consulte la Base de conocimientos y busque "Mejores prácticas para la instalación de vCenter Server 5.0", "Mejores prácticas para la instalación de vCenter Server 5.1" o "Mejores prácticas para la instalación de vCenter Server 5.5", respectivamente.
- Instantáneas de VMware de la máquina virtual (elimínelas lo antes posible; de lo contrario, puede experimentar degradación importante en el rendimiento).

  Se requiere espacio adicional en el disco para las instantáneas, ya que algunas instantáneas pueden ser tan grandes como la máquina virtual original. En algunos casos, vSphere puede eliminar instantáneas para crear espacio de almacenamiento, y por tanto, imposibilitar la posibilidad de volver a instantáneas anteriores.
- Uso del servidor de Cisco UCS durante el ciclo de vida típico del servidor.

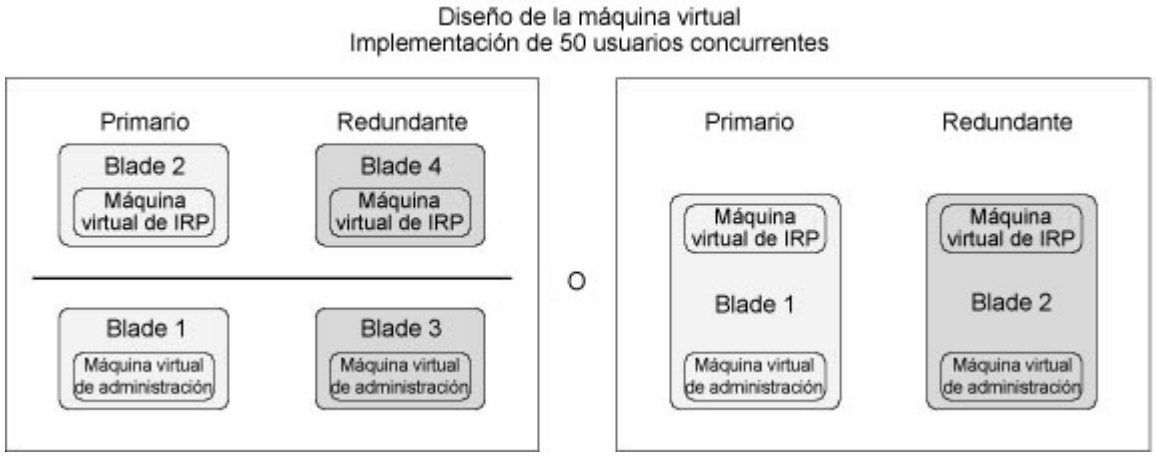
Los requisitos de hardware especificados en los archivos OVA son los requisitos mínimos necesarios para implementar Cisco WebEx Meetings Server. Estos requisitos *no incluyen* ningún requisito de CPU, de memoria o de almacenamiento para ESXi o vCenter de VMware.

Importante Los requisitos para los servidores de Cisco UCS incluyen los 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 residencia en conjunto compatibles).

Precaución La residencia en conjunto de configuraciones distintas a aquellas que figuran en las tablas de este documento no es compatible. Si es indiferente a nuestros requisitos del sistema, es posible que sus máquinas virtuales no se puedan iniciar. La implementación de las máquinas virtuales puede detenerse en las primeras pantallas del producto durante la implementación de OVA de vCenter.

Sistema de 50 usuarios

Un sistema de 50 usuarios también se describe como un *microsistema*. (Los centros de datos múltiples (MDC) no están disponibles para los microsistemas). El diagrama muestra dos versiones de una implementación de 50 usuarios. (Las máquinas virtuales "redundantes" demuestran ser compatibles con la alta disponibilidad).



La tabla enumera los requisitos mínimos de hardware para los hosts ESXi (servidores de Cisco UCS) en su sistema. Las últimas dos columnas muestran la cantidad de espacio en disco requerido para las nuevas instalaciones de Cisco WebEx Meetings Server y el espacio libre en disco requerido cuando usa la mejora automática para realizar una mejora a Cisco WebEx Meetings Server versión 2.x de la versión 1.x utilizando sus servidores Cisco UCS existentes. Para obtener más información, consulte los Requisitos generales del sistema.

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

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

Se admite la residencia en conjunto con vCenter con una implementación de un sistema de 50 usuarios configurado como se detalla en la siguiente tabla.

Máquinas virtuales en host ESXi (servidor Cisco UCS)	Núcleos de la CPU	Memoria (GB)	Puertos Ethernet	Requisitos de almacenamiento del disco duro para nuevas instalaciones	Almacenamiento libre en disco duro requerido para la mejora automática de 1.X a 2.X[1]
Administración	• 4 • 6	24	• 2 para la máquina virtual de administración, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 recomendado para la red de administración de ESXi	1,5 TB; mínimo de 7200 RPM	1118 GB para una instalación automática.
Administración y vCenter (residen en conjunto)	• 8 • 6	36	• 2 para la máquina virtual de administración, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 para vCenter • 1 recomendado para la red de administración de ESXi	1,5 TB; mínimo de 7200 RPM	1078 GB **Nota** Esta cifra se basa en la suposición de que ha configurado vCenter con 40 GB.
Proxy inverso de Internet (IRP)	• 4 • 6	12	• 2 para la máquina virtual de IRP, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 recomendado para la red de administración de ESXi	300 GB; mínimo de 7200 RPM	172 GB

Máquinas virtuales en host ESXi (servidor Cisco UCS)	Núcleos de la CPU	Memoria (GB)	Puertos Ethernet	Requisitos de almacenamiento del disco duro para nuevas instalaciones	Almacenamiento libre en disco duro requerido para la mejora automática de 1.X a 2.X[1]
Administración e IRP (residen en conjunto)	8	36	• 2 para la máquina virtual de administración, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 2 para la máquina virtual de IRP, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 recomendado para la red de administración de ESXi	1,5 TB; mínimo de 7200 RPM	990 GB
Administración e IRP y vCenter (todas residen en conjunto)	12	40	• 2 para la máquina virtual de administración, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 2 para la máquina virtual de IRP, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 para vCenter • 1 recomendado para la red de administración de ESXi	1,5 TB; mínimo de 7200 RPM	950 GB **Nota** Esta cifra se basa en la suposición de que ha configurado vCenter con 40 GB.

1 Si elige la mejora manual donde manualmente usted implementa todas las máquinas virtuales y usa el mismo hardware, debe contar con el doble de espacio libre, como se requiere para la mejora automática.

Nota Si planifica usar un sistema de alta disponibilidad, duplique las cantidades y los requisitos de hardware del sistema primario para admitir ambos sistemas.

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

En esta sección se describe la cantidad de medios que utilizan las máquinas virtuales y la sección está destinada a aquellos con conocimiento experto de VMware. Los recursos de la CPU se especifican como vCPU (núcleos) y MHz (ciclos de la CPU). VMkernel de VMware utiliza ciclos de MHz para controlar la planificación de la CPU.

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

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

Si intenta implementar una máquina virtual sin la cantidad mínima de vCPU, fallará la implementación OVA de la máquina virtual. Si intenta implementar una máquina virtual sin la cantidad mínima total de velocidad de procesador en MHz, la máquina virtual no encenderá.

Importante Las cantidades en esta tabla no incluyen los recursos para ESXi o vCenter de VMware. Consulte Recursos que consumen Cisco WebEx Meetings Server y el host ESXi, en la página 11.

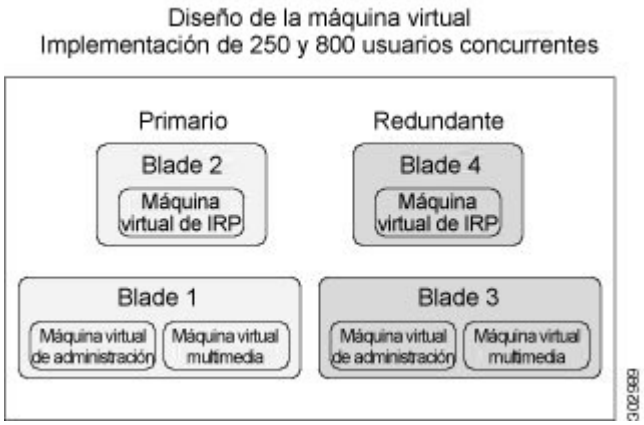
Tipo de máquina virtual	CPU virtual (vCPU)	CPU[2](MHz)	Memoria reservada/memoria total[3](GB)	Discos (GB)
Administración	4	8000	12/14	418
Proxy inverso de Internet	4	8000	4/4	128

2 La cantidad se obtiene multiplicando la cantidad de CPU físicas por la velocidad del chip de la CPU (MHz). No se incluye hyperthreading en este cálculo. (La CPU física debe tener una velocidad del reloj de 2,4 GHz o más rápida).

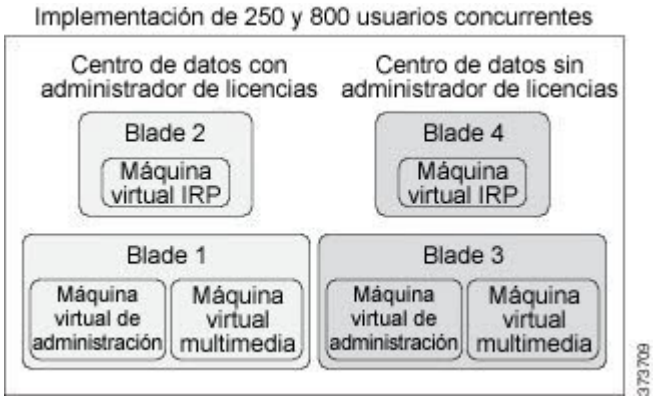
3 Las máquinas virtuales con funcionalidad multimedia tienen memoria no reservada adicional; memoria = memoria reservada/total

Sistema de 250 usuarios

Un sistema de 250 usuarios también se describe como un sistema *pequeño*. Este es un diagrama esquemático que muestra dos versiones de una implementación de 250 usuarios. Las máquinas virtuales "redundantes" demuestran ser compatibles con la alta disponibilidad. Si su sistema no incluye compatibilidad con la alta disponibilidad, solo implemente el sistema **primario**.



Este diagrama muestra el diseño de un sistema de 250 usuarios con dos centros de datos que forman un sistema de centro de datos múltiple (MDC) compatible con el proxy inverso de Internet (IRP). El administrador de licencias se ejecuta en un solo centro de datos.



La tabla enumera los requisitos mínimos de hardware para los hosts ESXi (servidores de Cisco UCS) en su sistema. Las últimas dos columnas muestran la cantidad de espacio en disco requerido para las nuevas instalaciones de Cisco WebEx Meetings Server y el espacio libre en disco requerido cuando usa la mejora automática para realizar una mejora a Cisco WebEx Meetings Server versión 2.x de la versión 1.x utilizando sus servidores Cisco UCS existentes. Para obtener más información, consulte los Requisitos generales del sistema.

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

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

Se admite la residencia en conjunto con vCenter con una implementación de un sistema de 250 usuarios configurado como se detalla en la siguiente tabla.

Máquinas virtuales en host ESXi (servidor Cisco UCS)	Núcleos de la CPU	Memoria (GB)	Puertos Ethernet	Requisitos de almacenamiento del disco duro para nuevas instalaciones	Almacenamiento libre en disco duro requerido para la mejora automática de 1.X a 2.X[4]
Administración y multimedia	12	52	• 2 para administración y multimedia, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 recomendado para la red de administración de ESXi	1,5 TB; mínimo de 7200 RPM	990 GB
(Administración y multimedia) y vCenter (residen en conjunto)	16	56	• 2 para administración y multimedia, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 recomendado para la red de administración de ESXi • 1 para vCenter	1,5 TB; mínimo de 7200 RPM	950 GB **Nota** Esta cifra se basa en la suposición de que ha configurado vCenter con 40 GB.
Proxy inverso de Internet (IRP)	12	36	• 2 para el IRP, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 recomendado para la red de administración de ESXi	300 GB; mínimo de 7200 RPM	172 GB

4 Si elige la mejora manual donde manualmente usted implementa todas las máquinas virtuales y usa el mismo hardware, debe contar con el doble de espacio libre, como se requiere para la mejora automática.

Nota Si planea usar un sistema de alta disponibilidad, compre el mismo hardware y las mismas cantidades que compró para el sistema primario.

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

En esta sección se describe la cantidad de medios que utilizan las máquinas virtuales y la sección está destinada a aquellos con conocimiento experto de VMware. Los recursos de la CPU se especifican como vCPU (núcleos) y MHz (ciclos de la CPU). VMkernel de VMware utiliza ciclos de MHz para controlar la planificación de la CPU.

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

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

Si intenta implementar una máquina virtual sin la cantidad mínima de vCPU, fallará la implementación OVA de la máquina virtual. Si intenta implementar una máquina virtual sin la cantidad mínima total de velocidad de procesador en MHz, la máquina virtual no encenderá.

Importante Las cantidades en esta tabla no incluyen los recursos para ESXi o vCenter de VMware. Consulte Recursos que consumen Cisco WebEx Meetings Server y el host ESXi.

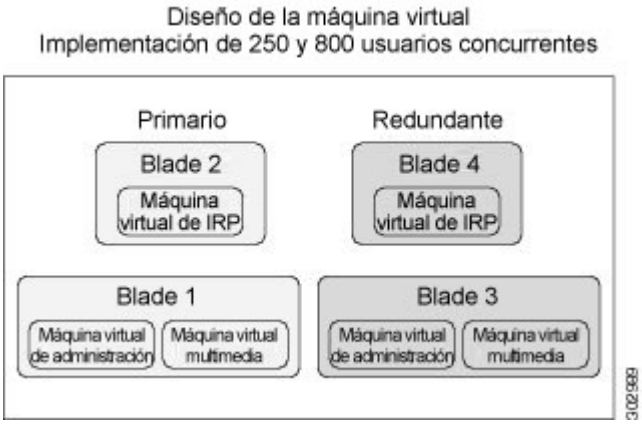
Tipo de máquina virtual	CPU virtual (vCPU)	CPU[5](MHz)	Memoria reservada/memoria total[6](GB)	Discos (GB)
Administración	4	8000	16/16	418
Multimedia	8	16 480	13/23	128
Proxy inverso de Internet	8	16 480	6/6	128

5 La cantidad se obtiene multiplicando la cantidad de CPU físicas por la velocidad del chip de la CPU (MHz). No se incluye hyperthreading en este cálculo. (La CPU física debe tener una velocidad del reloj de 2,4 GHz o más rápida).

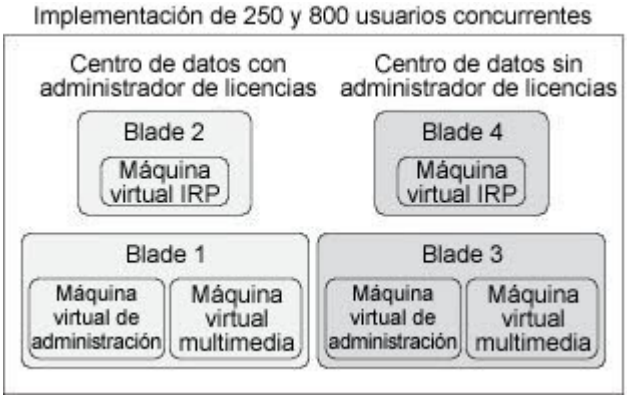
6 Las máquinas virtuales con funcionalidad multimedia tienen memoria no reservada adicional; memoria = memoria reservada/total

Sistema de 800 usuarios

Un sistema de 800 usuarios también se describe como un sistema *mediano*. Este diagrama muestra dos versiones de una implementación de 800 usuarios. Las máquinas virtuales "redundantes" demuestran ser compatibles con la alta disponibilidad.



Este diagrama muestra el diseño de un sistema de 800 usuarios con dos centros de datos que forman un sistema de centro de datos múltiple (MDC) compatible con el proxy inverso de Internet (IRP). El administrador de licencias se ejecuta en un solo centro de datos.



La tabla enumera los requisitos mínimos de hardware para los hosts ESXi (servidores de Cisco UCS) en su sistema. Las últimas dos columnas muestran la cantidad de espacio en disco requerido para las nuevas instalaciones de Cisco WebEx Meetings Server y el espacio libre en disco requerido cuando usa la mejora automática para realizar una mejora a Cisco WebEx Meetings Server versión 2.x de la versión 1.x utilizando sus servidores Cisco UCS existentes. Para obtener más información, consulte los Requisitos generales del sistema.

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

Nota La residencia en conjunto con vCenter no es compatible con una implementación de un sistema de 800 usuarios.

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

Máquinas virtuales en host ESXi (servidor Cisco UCS)	Núcleos de la CPU	Memoria (GB)	Puertos Ethernet	Requisitos de almacenamiento del disco duro para nuevas instalaciones	Almacenamiento libre en disco duro requerido para la mejora automática de 1.X a 2.X[7]
Administración y multimedia (combinadas)	40	80	• 2 para administración y multimedia, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 recomendado para la red de administración de ESXi	1,5 TB; mínimo de 10 000 RPM	990 GB
Proxy inverso de Internet (IRP)	40	36	• 2 para el IRP, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 recomendado para la red de administración de ESXi	300 GB; mínimo de 10 000 RPM	172 GB

7 Si elige la mejora manual donde manualmente usted implementa todas las máquinas virtuales y usa el mismo hardware, debe contar con el doble de espacio libre, como se requiere para la mejora automática.

Nota Si planifica utilizar un sistema de alta disponibilidad, adquiera los mismos requisitos y cantidades de hardware que el sistema primario.

Nota Para los sistemas de 800 usuarios, no recomendamos implementar máquinas virtuales adicionales en un host DMZ. Esto puede provocar una pérdida incrementada del paquete y latencia considerable en las conexiones de los medios.

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

Esta sección muestra qué cantidad de medios utilizan las máquinas virtuales y está destinada a aquellos con conocimiento experto de VMware. Los recursos de la CPU se especifican como vCPU (núcleos) y MHz (ciclos de la CPU). VMkernel de VMware utiliza ciclos de MHz para controlar la planificación de la CPU.

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

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

Si intenta implementar una máquina virtual sin la cantidad mínima de vCPU, fallará la implementación OVA de la máquina virtual. Si intenta implementar una máquina virtual sin la cantidad mínima total de velocidad de procesador en MHz, la máquina virtual no encenderá.

Importante Las cantidades en esta tabla no incluyen los recursos para ESXi de VMware. Consulte Recursos que consumen Cisco WebEx Meetings Server y el host ESXi, en la página 11.

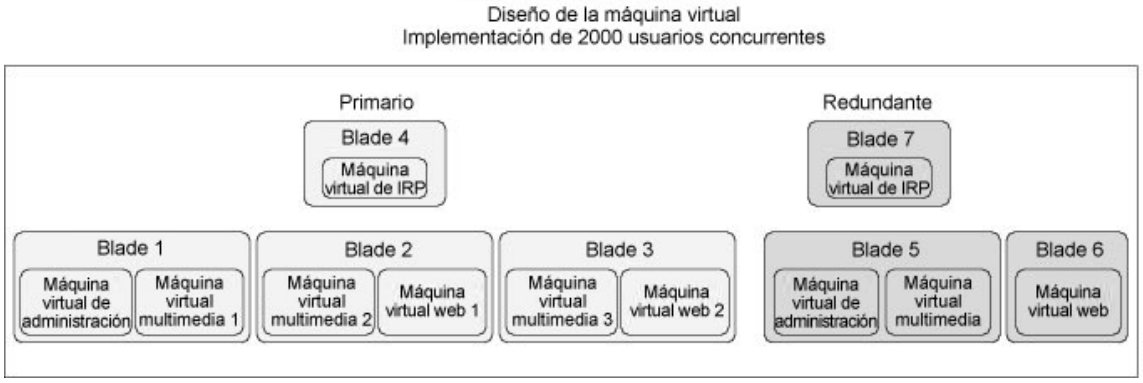
Tipo de máquina virtual	CPU virtual (vCPU)	CPU[8] (MHz)	Memoria reservada/memoria total[9] (GB)	Discos (GB)
Administración	10	20 600	16/16	418
Multimedia	30	60 800	14/44	128
Proxy inverso de Internet	20	41 200	10/10	128

8 La cantidad se obtiene multiplicando la cantidad de CPU físicas por la velocidad del chip de la CPU (MHz). No se incluye hyperthreading en este cálculo. (La CPU física debe tener una velocidad del reloj de 2,4 GHz o más rápida).

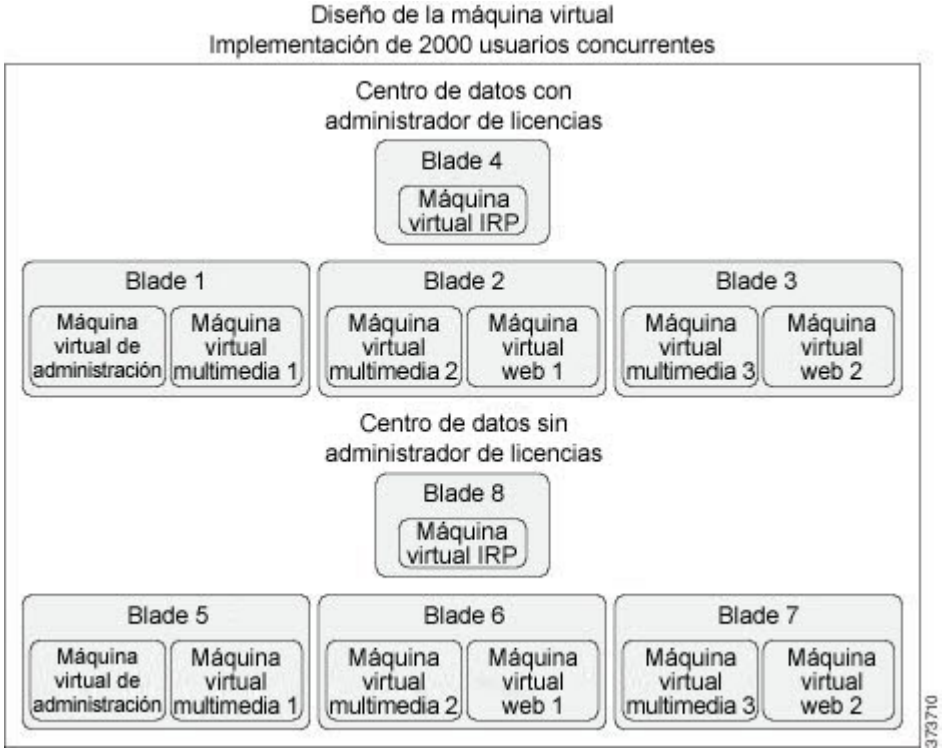
9 Las máquinas virtuales con funcionalidad multimedia tienen memoria no reservada adicional; memoria = memoria reservada/total

Sistema de 2000 usuarios

Un sistema de 2000 usuarios también se describe como un sistema *grande*. Este diagrama muestra un sistema de 2000 usuarios con alta disponibilidad y compatibilidad con un proxy inverso de Internet (IRP). Las máquinas virtuales de alta disponibilidad se muestran como las máquinas virtuales **redundantes**. Si su sistema no incluye compatibilidad con la alta disponibilidad, solo implemente el sistema **primario**.



Este diagrama muestra la implementación de un sistema de 2000 usuarios con dos centros de datos que forman un sistema de centro de datos múltiple (MDC) compatible con el proxy inverso de Internet (IRP). El administrador de licencias se ejecuta en un solo centro de datos.



Importante Le recomendamos que implemente todas las máquinas virtuales que se muestran en el diagrama. Si implementa diferentes tipos de máquinas virtuales en un servidor físico, puede evitar que el sistema se apague en caso de una falla en el hardware. Por ejemplo, la colocación de una máquina virtual multimedia y de una máquina virtual web en un único servidor físico es más resistente que la colocación de ambas máquinas virtuales web en el mismo servidor físico.

La tabla enumera los requisitos mínimos de hardware para los hosts ESXi (servidores de Cisco UCS) en su sistema. Las últimas dos columnas muestran la cantidad de espacio en disco requerido para las nuevas instalaciones de Cisco WebEx Meetings Server y el espacio libre en disco requerido cuando usa la mejora automática para realizar una mejora a Cisco WebEx Meetings Server versión 2.x de la versión 1.x utilizando

sus servidores Cisco UCS existentes. Para obtener más información, consulte los Requisitos generales del sistema.

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

Si desea agregar un sistema de alta disponibilidad, estas máquinas virtuales se muestran como máquinas virtuales "redundantes". Si no desea alta disponibilidad, implemente solamente el sistema primario.

Nota La residencia en conjunto con vCenter no es compatible con una implementación de un sistema de 2000 usuarios.

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

Máquinas virtuales en host ESXi (servidor Cisco UCS)	Núcleos de la CPU	Memoria (GB)	Puertos Ethernet	Requisitos de almacenamiento del disco duro para nuevas instalaciones	Almacenamiento libre en disco duro requerido para la mejora automática de 1.X a 2.X[10]
Multimedia 1 y administración (combinadas)	40	80	• 2 para multimedia 1 y administración, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 recomendado para la red de administración de ESXi	1,5 TB; mínimo de 10 000 RPM	990 GB
Multimedia 2 y web 1 (combinadas)	40	80	• 2 para multimedia 2 y web 1, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 recomendado para la red de administración de ESXi	1 TB; mínimo de 10 000 RPM	768 GB

Máquinas virtuales en host ESXi (servidor Cisco UCS)	Núcleos de la CPU	Memoria (GB)	Puertos Ethernet	Requisitos de almacenamiento del disco duro para nuevas instalaciones	Almacenamiento libre en disco duro requerido para la mejora automática de 1.X a 2.X[10]
Multimedia 3 y web 2 (combinadas)	40	80	• 2 para multimedia 3 y web 2, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 recomendado para la red de administración de ESXi	1 TB; mínimo de 10 000 RPM	768 GB
Proxy inverso de Internet (IRP)	40	36	• 2 para el IRP, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 recomendado para la red de administración de ESXi	300 GB; mínimo de 10 000 RPM	172 GB
Multimedia y administración (combinadas) para alta disponibilidad	40	80	• 2 para multimedia y administración, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 recomendado para la red de administración de ESXi	1,5 TB; mínimo de 10 000 RPM	990 GB

Máquinas virtuales en host ESXi (servidor Cisco UCS)	Núcleos de la CPU	Memoria (GB)	Puertos Ethernet	Requisitos de almacenamiento del disco duro para nuevas instalaciones	Almacenamiento libre en disco duro requerido para la mejora automática de 1.X a 2.X[10]
Web para alta disponibilidad	40	80	• 2 para web, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 recomendado para la red de administración de ESXi	1 TB; mínimo de 10 000 RPM	896 GB
IRP para alta disponibilidad	40	36	• 2 para el IRP, incluyendo 1 si se utiliza la formación de equipos NIC para la redundancia • 1 recomendado para la red de administración de ESXi	300 GB; mínimo de 10 000 RPM	172 GB

10 Si elige la mejora manual donde manualmente usted implementa todas las máquinas virtuales y usa el mismo hardware, debe contar con el doble de espacio libre, como se requiere para la mejora automática.

Nota Para los sistemas de 2000 usuarios, no recomendamos implementar máquinas virtuales adicionales en un host DMZ. Esto puede provocar una pérdida incrementada del paquete y latencia considerable en las conexiones de los medios.

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

Esta sección muestra qué cantidad de medios utilizan las máquinas virtuales y está destinada a aquellos con conocimiento experto de VMware. Los recursos de la CPU se especifican como vCPU (núcleos) y MHz (ciclos de la CPU). VMkernel de VMware utiliza ciclos de MHz para controlar la planificación de la CPU.

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

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

Si intenta implementar una máquina virtual sin la cantidad mínima de vCPU, fallará la implementación OVA de la máquina virtual. Si intenta implementar una máquina virtual sin la cantidad mínima total de velocidad de procesador en MHz, la máquina virtual no encenderá.

Importante Las cantidades en esta tabla no incluyen los recursos para ESXi de VMware. Consulte Recursos que consumen Cisco WebEx Meetings Server y el host ESXi.

Tipo de máquina virtual	CPU virtual (vCPU)	CPU[11] (MHz)	Memoria reservada/memoria total[12] (GB)	Discos (GB)
Administración	10	20 600	16/16	418
Multimedia	30	60 800	14/44	128
Web	10	20 600	16/16	128
Proxy inverso de Internet	20	41 200	10/10	128

11 La cantidad se obtiene multiplicando la cantidad de CPU físicas por la velocidad del chip de la CPU (MHz). No se incluye hyperthreading en este cálculo. (La CPU física debe tener una velocidad del reloj de 2,4 GHz o más rápida).

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

Matriz de la capacidad del sistema

Puntos clave:

- Una de las suposiciones básicas para la información que se presenta en esta sección es que hay al menos dos personas que participan en una reunión.
- Las conexiones de reuniones concurrentes se definen como la cantidad de personas que participan de una reunión en un momento determinado. Por ejemplo, en un sistema de 50 usuarios, la cantidad máxima de conexiones de reuniones concurrentes puede ser cinco reuniones concurrentes, en las que cada una tiene un total de 10 personas (por ejemplo, un organizador y nueve participantes).
- Una vez que en determinado momento se alcanza la cantidad máxima de participantes de la reunión, el sistema no permite que otros usuarios inicien o entren a reuniones. Solo la mitad de los usuarios de esa cantidad máxima de participantes de la reunión (2000, 800, 250 o 50 personas) puede utilizar vídeos. El vídeo se define como el envío o la recepción, lo que significa que los usuarios podrían usar el vídeo de su cámara web de WebEx o la opción de compartición de archivos de vídeo, que permite a los usuarios compartir un vídeo.
- La compartición de escritorio no se considera vídeo. Esto significa que con un sistema de 250 usuarios, 250 personas pueden compartir su escritorio durante las reuniones en un momento determinado.

- La incorporación de alta disponibilidad o de la característica de centro de datos múltiple no aumenta la capacidad del sistema para organizar reuniones; un sistema de 800 usuarios sigue siendo un sistema de 800 usuarios.

Los números de la siguiente tabla representan la capacidad de diseño para el sistema de Cisco WebEx Meetings Server. Si utiliza el sistema con una capacidad más alta que la que se menciona en estas especificaciones, probablemente obtenga una experiencia degradada del usuario e inestabilidad del sistema. Cisco se reserva el derecho de hacer cumplir los límites de capacidad en estos niveles.

Nota Los valores en la siguiente tabla permanecen iguales independientemente de si su sistema consta de un centro de datos único o si es un sistema de centro de datos múltiple.

Tabla 3: Matriz de la capacidad del sistema

Capacidad del sistema	Sistema de 2000 usuarios	Sistema de 800 usuarios	Sistema de 250 usuarios	Sistema de 50 usuarios	Notas
Cantidad máxima de conexiones de reuniones concurrentes (usuarios de audio, vídeo y web)	2000	800	250	50	La cantidad de personas que participan en reuniones concurrentes en un momento determinado.
Máximas conexiones de audio simultáneas (llamadas de teléfonos de teleconferencia y conexión de voz utilizando las computadoras de los clientes de la reunión)	2000	800	250	50	La capacidad del sistema sigue siendo la misma que se muestra a la izquierda, independientemente de qué combinación de las siguientes características se utilicen: • Códecs de audio G.711, G.722, G.729 • Teleconferencia IPv4 o IPv6 • Cifrado de audio TLS/SRTP

Capacidad del sistema	Sistema de 2000 usuarios	Sistema de 800 usuarios	Sistema de 250 usuarios	Sistema de 50 usuarios	Notas
Cantidad máxima de usuarios de vídeo y de compartición de archivos de vídeo concurrentes	1000[13]	400	125	25	Esta cantidad indica la cantidad máxima de conexiones de reuniones concurrentes (o participantes) permitida para compartir vídeos al mismo tiempo. Cuando la cantidad de usuarios que comparten vídeos en las reuniones concurrentes alcanza este límite, el resto de los usuarios invitados a las reuniones concurrentes puede entrar a las reuniones, pero las ventanas de sus vídeos se mostrarán de color gris. **Nota** Si un participante en una reunión usa un vídeo, todos los otros usuarios en la misma reunión se cuentan como usuarios de vídeo, incluso si ellos no están usando vídeo. **Nota** La compartición de escritorio no se considera vídeo.
Cantidad máxima de participantes por reunión	500	500	250	50	Esta cantidad indica la cantidad máxima de participantes que pueden asistir a una reunión.
Cantidad máxima de reuniones que pueden grabarse simultáneamente	100	40	13	3	Esta es la cantidad total de reuniones en las que se puede utilizar la característica Grabación a la vez.
Cantidad máxima de sesiones de reproducción de grabaciones concurrentes	500	200	63	12	Esta es la cantidad total de sesiones de reproducción de grabaciones que se puede llevar a cabo simultáneamente. Esto se refiere a las grabaciones que se guardan en su sistema de almacenamiento y no incluye las grabaciones que se descargan en los escritorios de los usuarios. **Nota** Estas sesiones de reproducción no se incluyen en las conexiones de reuniones concurrentes en el sistema.
Cantidad máxima de perfiles de usuario	400 000	400 000	400 000	400 000	Este número incluye usuarios activos y desactivados.
Cantidad máxima de reuniones concurrentes	1000	400	125	25	La cantidad de reuniones individuales que pueden estar activas de manera concurrente.

Capacidad del sistema	Sistema de 2000 usuarios	Sistema de 800 usuarios	Sistema de 250 usuarios	Sistema de 50 usuarios	Notas
Tasa de llamadas máxima (llamadas/por segundo)	20	8	3	1	Esta es la cantidad promedio de usuarios que pueden marcar en una reunión durante un período de tiempo de un segundo. Una vez que el sistema haya alcanzado esta cantidad, los próximos usuarios que marquen en la reunión podrían experimentar una espera de algunos segundos adicionales antes de conectarse a la reunión.
Cantidad máxima de inicios de sesión concurrentes	20 personas por segundo	8 personas por segundo	3 personas por segundo	1 persona por segundo	Esta es la cantidad promedio de usuarios que pueden iniciar sesión simultáneamente en su sitio de WebEx durante un período de tiempo de un segundo. Una vez que el sistema haya alcanzado esta cantidad, los próximos usuarios que inicien sesión en el sitio de WebEx podrían experimentar una espera de algunos segundos adicionales antes de que puedan entrar a una reunión.
Máxima utilización de ancho de banda promedio	5 Gbps	2 Gbps	625 Mbps	125 Mbps	Si se utiliza nuestro sistema de prueba a su ancho de banda máximo, este es el ancho de banda máximo que el sistema de prueba podría manejar. Para obtener más información acerca de la utilización del ancho de banda, consulte la sección Requisitos de ancho de banda de la red en el capítulo *Topología de red para su sistema* de la Guía de planificación. También puede consultar el informe Ancho de banda de red de WebEx.

[13] 800 en estándares de procesamiento de información federal (entornos FIPS)

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

- El espacio en disco puede ser local (DAS) o externo (SAN o NAS).
- Los hosts ESXi (servidor Cisco UCS) sin la máquina virtual de administración requieren 1,5 TB de espacio en disco.
- Los hosts ESXi (servidor Cisco UCS) sin una máquina virtual de administración requieren 1 TB de espacio en disco.
- Cuando se realiza una mejora de Cisco WebEx Meetings Server mediante los servidores Cisco UCS existentes, los hosts ESXi requieren 1118 GB de espacio libre en disco si el servidor UCS tiene únicamente la máquina virtual de administración (sistema primario o sistema de alta disponibilidad) o 990 GB de espacio libre en disco si el servidor UCS tiene una máquina virtual de administración y una máquina virtual multimedia (sistema primario o sistema de alta disponibilidad).

Para obtener más detalles, consulte la sección **Recursos que consumen 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 longitud máxima de una reunión es de 24 horas para todos los tamaños de las implementaciones de los sistemas de usuarios.

Nota Al considerar una mejora, planifique el aumento del tamaño de los almacenes de datos, ya que el sistema original y el sistema mejorado comparten los almacenes de datos hasta que hayan finalizado las pruebas del sistema mejorado y se haya eliminado el sistema original.

Para obtener información sobre los requisitos de ancho de banda de la red para los diversos tamaños de sistemas de usuarios, consulte la sección "Requisitos de ancho de banda de la red" en el capítulo "Topología de red para su sistema" de este libro.

Matriz de mejora o actualización de la versión

Use la siguiente tabla para determinar si debería llevar a cabo una mejora o una actualización del sistema en un centro de datos para ejecutar una versión específica de Cisco WebEx Meetings Server.

Versión instalada	A la versión…	Actualizar	Actualizar
1.5MR3 o una versión superior	2.0 o 2.5[14]	X	
1.0MR, 1.1MR o 1.5MR	2.5	X	
2.0MR3 o una versión superior	2.5		X

Versión instalada	A la versión…	Actualizar	Actualizar
Centro de datos único (SDC) 2.5	Cualquier 2.5MR		X
Centro de datos múltiple (MDC) 2.5	Cualquier 2.5MR		X

14 Le recomendamos que cualquier versión de 1.0, 1.1 o 1.5 se actualice a la versión 1.5MR3 de los archivos OVA e ISO antes de realizar una mejora a la versión 2.5.

Consulte la guía de administración de Cisco WebEx Meeting Server en http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html para conocer las instrucciones de actualización y mejora.

CAPÍTULO 2

Introducción y topología del centro de datos para su sistema

Este capítulo proporciona una introducción, información general del centro de datos y los requisitos de vCenter de VMware para su sistema.

- Introducción a Cisco WebEx Meetings Server, página 33
- Información para los clientes de Cisco Unified MeetingPlace, página 35
- Conceptos generales para la implementación del sistema, página 35
- Implementación de un centro de datos único, página 38
- Unión de centros de datos únicos para crear un sistema de centro de datos múltiple (MDC), página 38
- Uso de vSphere de VMware con su sistema, página 39
- IOPS y rendimiento del sistema de almacenamiento, página 42
- Instalación de vSphere ESXi de VMware y configuración del almacenamiento, página 43
- Entrada en reuniones, página 44

Introducción a Cisco WebEx Meetings Server

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

Cisco WebEx Meetings Server aborda la necesidad de las empresas actuales al presentar una solución de conferencias integral con todas las herramientas necesarias para una colaboración eficaz y atractiva. Ofrece una experiencia interactiva y productiva para los usuarios.

Puede implementar y administrar esta solución de conferencias en su nube privada, protegida por el firewall de su centro de datos. Está diseñada para los servidores de Cisco UCS y vSphere de VMware. (Para conocer los requisitos específicos, consulte Requisitos mínimos de hardware, en la página 9). Presenta una implementación virtual rápida y herramientas potentes para que los administradores configuren y administren el sistema y vean las medidas clave del sistema.

Al igual que otros productos de Cisco WebEx, ofrece herramientas de colaboración en tiempo real, incluida la compartición de documentos, aplicaciones y escritorio, las herramientas de anotación, el control completo del organizador para una administración eficaz de las reuniones, una lista de participantes integrada con el orador activo, y el cambio, la grabación y la reproducción de vídeo. Este producto utiliza vídeo de alta calidad para que la experiencia de compartición de vídeo sea nítida y clara.

Además, los usuarios móviles pueden asistir a reuniones y participar en ellas. Para conocer los dispositivos compatibles, consulte Requisitos de los sistemas operativos de los dispositivos móviles, en la página 205.

Consideraciones importantes para su sistema

Tenga en cuenta lo siguiente:

- Proxies de reenvío: no se recomiendan, aunque puede usarlos con restricciones.

  Para ver los detalles completos, consulte la *Guía de solución de problemas de Cisco WebEx Meetings Server*.

- Proxies inversos: solo el proxy inverso de Internet incluido con este producto es compatible.
- NAT: compatible cuando cumple con los requisitos para este sistema.

  Para conocer todos los detalles, consulte Uso de NAT con su sistema.

- Centros de datos únicos: las implementaciones dentro de un solo centro de datos son compatibles con todas las versiones de Cisco WebEx Meetings Server.

  Para conocer todos los detalles, consulte Implementación de un centro de datos único.

- Centros de datos múltiples: los centros de datos que ejecutan Cisco WebEx Meetings Server 2.5 pueden unirse para crear un sistema compuesto por varios centros de datos.

  Para obtener información detallada, consulte Acerca de los centros de datos múltiples.

- Servidor de almacenamiento: cada centro de datos en un sistema de centro de datos múltiple debe tener un servidor de almacenamiento independiente. 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 primario (en un sistema de centro de datos único) falla, el sistema de alta disponibilidad continúa prestando servicio. Las máquinas virtuales de alta disponibilidad redundantes se deben colocar en el mismo centro de datos con las máquinas virtuales primarias. Las máquinas virtuales del sistema primario y del sistema de alta disponibilidad también deben estar en la misma VLAN o subred.

  No puede unir sistemas de alta disponibilidad para crear un entorno de centro de datos múltiple.

- Servidor proxy inverso de Internet (IRP): una máquina virtual colocada como un proxy entre la Internet externa y la red interna de una empresa para proporcionar acceso público a Cisco WebEx Meetings Server. Se requiere un servidor proxy inverso de Internet si desea permitir a los usuarios planificar y asistir a reuniones desde dispositivos móviles en forma interna y externa, o si desea proporcionar un acceso seguro a su sitio de WebEx desde Internet. No se requiere un servidor proxy inverso de Internet si permitirá el acceso a Cisco WebEx Meetings Server solo desde su red interna. Implemente una máquina virtual IRP usando el mismo archivo OVA que utilizó para implementar su máquina virtual de administración. Su máquina virtual IRP debe estar en la misma subred que la dirección IP virtual pública.
- Dirección IP virtual (VIP): dirección IP que se usa para la comunicación con las máquinas virtuales de administración, multimedia y web dentro de un centro de datos.

- Dirección IP virtual privada (VIP): una dirección IP adicional que se configura en la máquina virtual de administración y que se asocia con la URL del sitio de administración. La dirección IP virtual privada también se puede asociar con la URL del sitio de WebEx si la dirección se configura en el servidor DNS interno en una implementación o en implementaciones de DNS de horizonte dividido sin un servidor proxy inverso de Internet.
- Dirección IP virtual pública (VIP): una dirección IP adicional que se configura en la máquina virtual de proxy inverso de Internet y que se asocia solamente con la URL del sitio de WebEx. La URL del sitio de WebEx en los servidores DNS externos debe poder resolverse en la dirección IP virtual pública para proporcionar a los usuarios acceso al sitio de WebEx desde Internet. En el sistema no se configura una dirección IP virtual pública si no hay un servidor proxy inverso de Internet.

Precaución Si es indiferente a nuestras recomendaciones y requisitos al implementar su sistema, no recibirá soporte de Cisco. Cisco no se responsabiliza de ningún problema que pueda tener como resultado de no seguir nuestros consejos.

Características nuevas y modificadas para Cisco WebEx Meetings Server

Para obtener una lista de las características nuevas y modificadas, consulte la sección titulada "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 en la arquitectura, no hay una ruta de migración (para las cuentas de usuario existentes, las personalizaciones y las reuniones) de Cisco Unified MeetingPlace a Cisco WebEx Meetings Server. Son dos productos distintos.

Usted puede facilitar la transición para sus usuarios al continuar admitiendo tanto Cisco Unified MeetingPlace como Cisco WebEx Meetings Server por un período de tiempo mientras alienta a sus usuarios a que cambien al nuevo sistema. Para contribuir con la formación del usuario durante esta transición, Cisco proporciona vídeos de formación a los que puede acceder desde la página Ayuda.

Conceptos generales para la implementación del sistema

Tamaños del sistema

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

- 50 usuarios concurrentes (también conocido como un *microsistema*)
  - Generalmente, sirve para una empresa de entre 500 y 1000 empleados
  - El sistema primario (sin alta disponibilidad) se compone de una máquina virtual de administración y un proxy inverso de Internet opcional (para acceso público)

- 250 usuarios concurrentes (también conocido como un sistema *pequeño*)
  - Generalmente, sirve para una empresa de entre 2500 y 5000 empleados
  - El sistema primario (sin alta disponibilidad) se compone de una máquina virtual de administración, una máquina virtual multimedia y un proxy inverso de Internet opcional (para acceso público)
- 800 usuarios concurrentes (también conocido como un sistema *mediano*)
  - Generalmente, sirve para una empresa de entre 8000 y 16 000 empleados
  - El sistema primario (sin alta disponibilidad) se compone de una máquina virtual de administración, una máquina virtual multimedia y un proxy inverso de Internet opcional (para acceso público)
- 2000 usuarios concurrentes (también conocido como un *sistema grande*)
  - Generalmente, sirve para una empresa de entre 20 000 y 40 000 empleados
  - El sistema primario (sin alta disponibilidad) se compone de una máquina virtual de administración, 3 máquinas virtuales multimedia, 2 máquinas web y un proxy inverso de Internet opcional (para acceso público)

Términos utilizados durante la implementación

URL del sitio de WebEx: una URL de http para los usuarios que organizan y asisten a reuniones en un entorno de un centro de datos único.

URL de administración de WebEx: una URL de http segura para que los administradores configuren, supervisen y administren el sistema en un entorno de un centro de datos único.

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

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

URL común de WebEx: el DNS la utiliza para redirigir al usuario al centro de datos donde el usuario realiza tareas relacionadas con las reuniones, por ejemplo, planificar u organizar reuniones. El centro de datos que el DNS elija es transparente para el usuario. La URL común de WebEx es simplemente una ubicación práctica para que un usuario se introduzca en el sistema. Si un centro de datos queda fuera de servicio, no cambia nada para el usuario, incluida la URL que se usa para obtener acceso a las reuniones, porque el DNS redirigirá al usuario al centro de datos sobreviviente.

URL común de administración: con frecuencia, se conoce simplemente como la *URL de administración*. El DNS la utiliza para redirigir a un administrador al centro de datos de administración donde el administrador inicia sesión en el sistema. El centro de datos que el DNS elija es transparente para el administrador (sin embargo, la cadena en la barra de URL cambia según el centro de datos que el administrador usa para obtener acceso al sistema). La URL común de administración es simplemente un destino práctico que un administrador utiliza para introducirse en el sistema.

URL locales de administración: son específicas de cada centro de datos en un sistema de centro de datos múltiple (MDC). Cuando se inicia sesión a través de la URL común de administración, el DNS redirige al administrador a la URL local de administración para el centro de datos de administración. Las modificaciones del sistema, por ejemplo, asignar una licencia a un usuario, se realizan en el centro de datos de administración y se replican en todos los centros de datos en el sistema MDC.

Un administrador puede elegir un centro de datos específico para realizar modificaciones desde dentro de la aplicación CWMS, pero seleccionar otro centro de datos para las modificaciones no cambia la URL local de

administración, 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 en otro centro de datos en el sistema MDC atraviesan el centro de datos de administración elegido por el DNS hasta el centro de datos de destino.

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

Las URL locales son específicas de cada centro de datos.

Información del perfil del sistema

Complete este cuadro 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 los sitios locales		
URL de administración locales		
Direcciones IP virtuales públicas		
Direcciones IP virtuales privadas		
Servidor DNS		
Dirección IP de la máquina virtual de administración		
Dirección IP de la máquina virtual multimedia 1		
Dirección IP de la máquina virtual multimedia 2		
Dirección IP de la máquina virtual multimedia 3		
Dirección IP de la máquina virtual web 1		
Dirección IP de la máquina virtual web 2		

Dirección IP de la máquina virtual DMZ (opcional)		
Direcciones de correo electrónico del administrador de CWMS		
Contraseña		
Remote Access[15]		
Contraseña		
Dirección IP del administrador de llamadas		
ID del administrador de llamadas de Cisco		
Contraseña del administrador de llamadas de Cisco		
Números de llamada entrante de CWMS		
Números telefónicos		

15 Las cuentas de acceso remoto no se habilitarán hasta que la cuenta se active.

Implementación de un centro de datos único

Cisco WebEx Meeting Server (CWMS) puede implementarse como un sistema de centro de datos único (SDC) y, opcionalmente, como un sistema de alta disponibilidad o un sistema de centro de datos múltiple (MDC) (consulte Redundancia en implementaciones de alta disponibilidad o MDC, en la página 54). Un sistema SDC (incluido un sistema compatible con alta disponibilidad) solo requiere licencias de organizador después de un período de prueba. Un sistema MDC requiere un mínimo de dos licencias de la característica MDC, licencias de organizador y no hay un período de prueba de MDC.

Unión de centros de datos únicos para crear un sistema de centro de datos múltiple (MDC)

Puede unir centros de datos únicos que ejecutan Cisco WebEx Meeting Server 2.5 para formar un sistema de centro de datos múltiple (MDC). (Para la versión 2.5, se pueden unir dos centros de datos, como máximo). Los centros de datos pueden ubicarse en distintas ubicaciones geográficas y funcionar como pares, en contraposición a un solo sistema que funciona como copia de seguridad para un sistema CWMS primario. Un sistema de alta disponibilidad que debe ser coubicado en el mismo centro de datos es un ejemplo de la configuración de un sistema de copia de seguridad. Consulte Redundancia en implementaciones de alta disponibilidad o MDC, en la página 54. Para conocer los detalles sobre cómo preparar sus centros de datos para unirlos, el proceso de unión y cómo transferir los datos de un centro de datos al otro cuando finaliza el

proceso de unión, consulte el capítulo "Unión de centros de datos para crear un sistema de centro de datos múltiple (MDC)" en la *Guía de administración de Cisco WebEx, versión 2.5*.

Uso de vSphere de VMware con su sistema

vSphere de VMware

Importante Este producto solo se instala en una plataforma de virtualización vSphere de VMware.

- Para ahorrar tiempo, Cisco recomienda los servidores estándar de Cisco UCS con configuraciones específicas de hardware y productos de VMware.
- Sin embargo, Cisco WebEx Meetings Server está diseñado para funcionar en cualquier servidor de Cisco UCS equivalente que cumpla o supere estas especificaciones.

  Para obtener todos los detalles sobre los requisitos de hardware y 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 usar como la plataforma de hipervisor de Cisco WebEx Meetings Server.

  Nota Por razones de seguridad, 5.1 debe ser versión 1900470 o una versión posterior.

  Complete una de las acciones siguientes:

  - Adquiera vSphere directamente en Cisco a través de la GPL (Lista de precios globales). Cisco es un socio y distribuidor aprobado de VMware.

    Esta es una alternativa conveniente para aquellos que "desean adquirir todo en un único proveedor".
  - O bien, adquiera vSphere directamente de VMware, a través de acuerdos empresariales que tenga directamente con VMware.

Ventajas de la implementación de un sistema en vSphere de VMware

Esta sección explica por qué vSphere y vCenter de VMware son integrales para usar este producto de Cisco WebEx y ofrece algunas consideraciones.

Implementación del sistema

- Este producto está empaquetado como un dispositivo virtual de OVA compatible con vSphere de VMware y no como una colección de paquetes de software en un DVD. Debe tener vCenter para implementar el OVA o el producto no se instalará.
- Al empaquetarlo como un dispositivo virtual, permitimos una implementación rápida; en algunos casos, en menos de una hora.

- Para facilitar instalaciones rápidas con el dispositivo virtual de OVA, puede seleccionar la implementación automática del sistema para la mayoría de los tamaños del sistema. Solo proporcione las credenciales de vCenter e implementaremos todas las máquinas virtuales para su sistema sin intervención manual. Esta innovación minimiza los costos 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 ambos NIC virtuales. Para todas las demás máquinas virtuales de Cisco WebEx Meetings Server (CWMS), solo se utiliza un NIC virtual y el otro se desconecta.

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

Recuperación sencilla de errores del sistema

Si el cambio no satisface sus expectativas, con VMware Data Recovery, puede revertir los cambios que afectan el sistema rápidamente y sin una reimplementación del sistema.

Consideraciones de vSphere

Tenga en cuenta las siguientes consideraciones:

- Puede mover su máquina virtual a otro host ESXi. Sin embargo, debe mantener el diseño de las máquinas virtuales en el nuevo host ESXi. En otras palabras, si planifica mover una máquina virtual multimedia que resida en conjunto con una máquina virtual web, debe moverla a otro host ESXi (en donde es la única máquina virtual) o moverla a un host ESXi que ya tenga una máquina virtual web.

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

Las siguientes características de VMware no son compatibles con CWMS:

- VMotion y Storage VMotion (si bien usted puede mover sus máquinas virtuales, probablemente no pueda hacerlo con estas herramientas)
- Distributed Resource Schedule (DRS) de VMware
- Alta disponibilidad de vSphere
- Agrupamiento y la compartición de recursos de vSphere

Mejores prácticas de vSphere

- Le recomendamos que no use instantáneas de las máquinas virtuales. Si decide utilizar imágenes instantáneas, luego de confirmar los cambios de su sistema, asigne las imágenes instantáneas o elimínelas lo más pronto posible. Mantener una imagen instantánea por cualquier período de tiempo resultará en una degradación del rendimiento grave.

- Para los entornos SAN, implemente las imágenes de disco para un SAN con números IOP altos.

  Para un sistema de 800 usuarios, la IOPS promedio para una implementación OVA es 506 (la IOPS máxima es 855) para la máquina virtual de administración y 475 (la IOPS máxima es 652) para una máquina virtual multimedia. Una vez que estas máquinas virtuales se crean y se encienden, puede introducir la URL que distinga entre mayúsculas y minúsculas y continuar con la implementación del sistema en un explorador web. La IOPS promedio para un sistema primario es 108 (la IOPS máxima es 1558) y 163 (la IOPS máxima es 1736) para un sistema secundario.

- Compruebe que haya suficiente espacio libre para su SAN. Las imágenes instantáneas son almacenadas en el mismo SAN.
- Implemente una red de 10 GB para obtener el ancho de banda y la implementación más rápidos para el crecimiento futuro.
- Le recomendamos que administre todas las máquinas virtuales con el mismo vCenter. Esto permite una recuperación más fácil en caso de que necesite recuperar su sistema.

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

Requisitos del servidor de vCenter

Además de vSphere, también es necesario el servidor de vCenter.

- Para implementar este dispositivo virtual, también debe utilizar vCenter para implementar y administrar las máquinas virtuales en su sistema. Este producto no funcionará sin el servidor de vCenter.
- Cisco recomienda la realización de copias de seguridad e instantáneas del sistema antes de realizar operaciones que puedan afectar el sistema. Crear copias de seguridad le permite revertir los cambios en caso de que la actualización no cumpla con sus expectativas. Puede automatizar las copias de seguridad y las instantáneas mediante vCenter.
- Aunque se requiere vSphere Standard Edition para un sistema de 50 o 250 usuarios, puede considerar la alternativa de adquirir el kit vSphere Essentials Plus. Sin embargo, el kit vSphere Essentials Plus es útil, principalmente, para los clientes que deben ajustarse a un presupuesto y que implementen el sistema de 50 usuarios. No proporciona varias capacidades avanzadas que los clientes empresariales, generalmente, requieren. Consulte con su representante de VMware acerca de la manera más rentable de cumplir con los requisitos del sistema.
- CWMS es compatible con vSphere Standard Edition. CWMS no es compatible con el kit Essentials Plus.

vSphere Edition para sistemas de 800 y 2000 usuarios

- Los sistemas de 800 y 2000 usuarios se componen de máquinas virtuales que requieren entre 30 y 40 vCPU. Estas máquinas virtuales utilizan estas vCPU para la realización de tareas de cómputo muy exigentes, como la codificación o decodificación de SSL, la mezcla de flujos de audio, etc.

  Para obtener toda la información sobre los requisitos de vCPU, consulte Recursos que consumen Cisco WebEx Meetings Server y el host ESXi, en la página 11.

- Como mínimo, debe adquirir la edición vSphere 5.0 Enterprise Plus o vSphere 5.1 Enterprise Edition, ya que las ediciones anteriores de vSphere no admiten la cantidad de vCPU requerida.

IOPS y rendimiento del sistema de almacenamiento

IOPS y rendimiento máximos esperados

La siguiente tabla muestra los valores de IOPS y rendimiento máximos esperados para la carga máxima en el sistema para una sola máquina virtual.

Tamaño del sistema	Máquina virtual	Cantidad máxima de operaciones de entrada/salida (IOPS)	Cantidad máxima de Megabytes de lectura por segundo	Cantidad máxima de Megabytes de escritura por segundo
Sistema de 50 usuarios	Administración	450	1	15
	DMZ	70	0.3	0.3
Sistema de 250 usuarios	Administración	1400	1	25
	Multimedia	150	1	10
	DMZ	110	0.4	0.6
Sistema de 800 usuarios	Administración	1400	3	50
	Multimedia	300	1	30
	DMZ	150	1	1.5
Sistema de 2000 usuarios	Administración	1600	2.5	60
	Multimedia	300	1	25
	Web	200	3	1.5
	DMZ	200	1.5	3

IOPS para el rearranque de un sistema de 2000 usuarios

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

Máquinas virtuales en un sistema de 2000 usuarios	IOPS para volver a arrancar el sistema (rearranque)	IOPS para realizar una actualización menor
Administración	2300	3000
Multimedia	2000	2000
Web	1500	2000

Máquinas virtuales en un sistema de 2000 usuarios	IOPS para volver a arrancar el sistema (rearranque)	IOPS para realizar una actualización menor
Web	1000	2000

IOPS para la copia de seguridad de un sistema de 2000 usuarios

La siguiente tabla muestra la información de IOPS para realizar una copia de seguridad durante un período de inactividad en el caso de un sistema de 2000 usuarios.

Máquina virtual de administración para un sistema de 2000 usuarios	IOPS para realizar una copia de seguridad	Cantidad máxima de Megabytes de lectura por segundo	Cantidad máxima de Megabytes de escritura por segundo
Copia de seguridad de 1 GB	2000	220	300
Copia de seguridad de 12 GB	5000	320	600

Instalación de vSphere ESXi de VMware y configuración del almacenamiento

Cisco WebEx Meetings Server es una solución basada en software. No es un paquete de combinación de hardware/software. Puede elegir cómo adquirir y aprovisionar sus plataformas de hardware siempre y cuando el hardware cumpla o exceda los requisitos de CPU, memoria y almacenamiento.

Puede implementar Cisco WebEx Meetings Server en servidores Cisco UCS que cumplan nuestras especificaciones mínimas. O podrá implementar este producto en servidores UCS nuevos y de gama más alta que excedan nuestras especificaciones mínimas.

Están disponibles varias opciones de red y controladoras RAID. Podrá elegir utilizar almacenamiento SAN en vez de RAID local. No proporcionamos detalles acerca de cada tipo de configuración de almacenamiento que puede elegir.

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

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

Configuración de la memoria caché de escritura en una controladora RAID

Para un rendimiento óptimo del sistema, debe verificar la configuración de escritura predeterminada en su controladora RAID. Puede configurar la escritura predeterminada en tres ajustes: *Escritura no simultánea con unidad de batería de respaldo (Battery Backup Unit, BBU)*, *Escritura simultánea* o *Siempre escritura no simultánea*. Algunas pautas para la selección de la configuración adecuada de la escritura predeterminada en sus servidores UCS de Cisco son:

- **Escritura no simultánea con BBU:** use esta configuración si tiene instalada una batería de respaldo en su controladora RAID. En caso de una pérdida de energía del sistema, la unidad de batería de respaldo conserva el contenido de la memoria caché de la controladora.

  En caso de que se produzca un error en la unidad de batería de respaldo o que se desconecte para un ciclo de reaprendizaje, la configuración de escritura no simultánea con BBU cambia automáticamente a caché de **escritura simultánea**. Sin una unidad de batería de respaldo que funcione, la configuración de escritura simultánea es más segura, aunque puede advertir una degradación del rendimiento en el subsistema de E/S de la máquina host.

- **Escritura simultánea:** use esta configuración y active la memoria caché explícitamente (con la opción Caché de disco) si tiene que retirar la unidad de batería de respaldo para repararla. Esta configuración debería brindarle un mejor rendimiento, aunque no óptimo. Después de reemplazar la batería defectuosa, puede cambiar de manera segura la configuración de escritura predeterminada a escritura no simultánea con el modo de BBU.

- **Siempre escritura no simultánea:** use esta configuración si el organiza que aloja su controladora RAID está conectado a una unidad de suministro de energía ininterrumpida.

Entrada en reuniones

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

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

Usuarios de Windows

Lo siguiente supone que los usuarios tienen privilegios de administrador de Windows en sus PC suficientes para permitirles entrar a reuniones de WebEx. Si esto no es verdadero, los administradores del sistema pueden arrastrar el cliente de la aplicación WebEx Meetings a un usuario mediante un software de administración de escritorio como IBM Tivoli. Consulte Descarga e implementación masiva de aplicaciones.

- Los usuarios de Microsoft Internet Explorer pueden instalar un control ActiveX o un complemento de Java, descargar el programa de instalación de la aplicación WebEx Meetings o ejecutar la aplicación en una carpeta temporal del sistema (como TFS). La primera vez que el usuario entra a una reunión, el software de cliente se descarga y se instala automáticamente.

- Los usuarios de Google Chrome y Mozilla Firefox pueden instalar un complemento de Java, descargar la aplicación WebEx Meetings o ejecutar la aplicación en una carpeta temporal del sistema. El software de cliente se descarga y se instala automáticamente la primera vez que el usuario entra en una reunión.

No es necesario cambiar ninguno de los ajustes de ActiveX, del complemento de Java, del programa de instalación de la aplicación WebEx Meetings o de TFS.

Usuarios de Mac

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

Usuarios de un sistema de centro de datos múltiple

Si su sitio de WebEx usa certificados de firma automática en lugar de certificados de una autoridad de certificación conocida, después de que su centro de datos se une a otro centro de datos, los usuarios deben instalar un certificado para cada centro de datos en la tienda Autoridades de certificación raíz de confianza antes de iniciar o entrar a una reunión.

Uso de los exploradores Chrome y FireFox

Si usa Chrome 32 y las versiones posteriores o Firefox 27[16]y las versiones posteriores, es posible que se le indique que instale un complemento de Cisco WebEx. Seleccione **Descargar** y siga las instrucciones para instalar el complemento requerido.

Nota Después de haber instalado el complemento, es posible que deba activarse.

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

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

Si está usando el explorador Chrome 38 y las versiones posteriores para iniciar una reunión de WebEx o para reproducir una grabación de WebEx, es posible que se le solicite que lleve a cabo la siguiente instalación por única vez para agregar la extensión Cisco WebEx a su explorador Chrome:

1. Seleccione **Agregar WebEx a Chrome**.
2. Seleccione **Gratuito** en el cuadro de diálogo Extensión de Cisco WebEx.
3. Seleccione **Agregar** para agregar la extensión de Cisco WebEx a su explorador Chrome.
4. Abra el archivo Cisco_WebEx_Add-on.exe y seleccione **Ejecutar**.
5. La página se actualizará cuando la instalación finalice. Si la reunión no se inicia automáticamente, actualice la página.

16 Las versiones exactas de Chrome y Firefox a las cuales afecta esta política no se han finalizado al momento de la publicación de este documento.

CAPÍTULO 3

Topología de red para su sistema

Este capítulo describe las diferentes topologías de red compatibles con este producto, incluidas las ventajas y desventajas de cada una. Seleccione la que mejor se ajuste a sus necesidades y a la implementación de su 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 implementar el proxy inverso de Internet independientemente de cómo el usuario móvil asiste a una reunión.

Al utilizar una red de datos de telefonía móvil, los usuarios móviles entran en la reunión a través de Internet al proxy inverso de Internet. Cuando se utiliza una conexión Wi-Fi local, los usuarios 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 47
- Diferentes tipos de topologías de red para su sistema, página 48
- Topología de red del proxy inverso de Internet interno (IRP), página 49
- Topología de red de horizonte no dividido, página 50
- Topología de red completamente interna, página 51
- Topología de red de horizonte dividido, página 52
- Redundancia en implementaciones de alta disponibilidad o MDC, página 54
- Consideraciones de red para el proxy inverso de Internet, página 55
- Requisitos del ancho de banda de la red, página 57
- Formación de equipos NIC para agregación de ancho de banda, página 61

Diseño de las máquinas virtuales en su red

Cisco WebEx Meetings Server (CWMS) se compone de 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 los usuarios externos pueden organizar o asistir a reuniones a través de Internet sin usar

VPN o usando dispositivos móviles CDMA. Sin IRP, solo los usuarios internos y de VPN pueden organizar o entrar 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 de administración, y si corresponde, a las máquinas virtuales multimedia y web.

- Las máquinas virtuales internas *deben* estar en una sola subred o VLAN común. Durante la implementación del sistema verá mensajes de error si las asignaciones de su dirección IP violan esta regla. El diseño del sistema supone que todas las máquinas virtuales internas, incluidas las máquinas virtuales de alta disponibilidad, están conectadas a través de una LAN que ofrece un alto nivel de ancho de banda, una pérdida insignificante del paquete y una latencia por debajo de 4 ms.

  Tanto la voz, los datos, el vídeo y SAN se basan en el ancho de banda de la red. Es importante implementar una red que sea capaz de manejar la carga requerida.

- Cisco recomienda colocar todas las máquinas virtuales internas en el mismo interruptor de Ethernet. Sin embargo, al aprovisionar un sistema de alta disponibilidad, le recomendamos que implemente dos interruptores de Ethernet para garantizar la redundancia de red.

- Si, de lo contrario, decide colocar las máquinas virtuales en distintos interruptores de Ethernet en el mismo centro de datos, su red *debe cumplir* con los requisitos específicos de ancho de banda y de latencia de red como se describen en Requisitos del ancho de banda de la red, en la página 57. En esta situación, el enlace troncal entre interruptores debe cumplir con las mismas características de red que la latencia y rendimiento de L3 para un único interruptor físico.

Para obtener información adicional sobre los sistemas con alta disponibilidad, consulte Redundancia en implementaciones de alta disponibilidad o MDC, en la página 54.

Diferentes tipos de topologías de red para su sistema

Este producto admite las siguientes topologías de red:

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

Nota Si su topología de red incluye proxies de reenvío, estos deben 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 más detalles.

Topología de red del proxy inverso de Internet interno (IRP)

Esta sección 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.

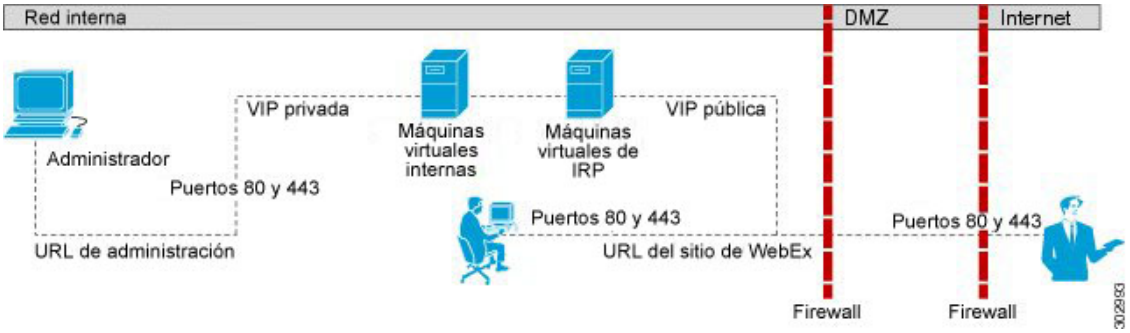
Esta configuración permite a los usuarios iniciar sesión y entrar en reuniones desde Internet de forma segura sin una conexión VPN.

Si utiliza una implementación automática, los hosts ESXi para todas las máquinas virtuales (incluido el IRP) deben estar administrados desde el mismo vCenter de VMware. Se requiere esta información de vCenter durante una implementación automática del sistema.

Nota Esta configuración es compatible con el acceso móvil.

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

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



Para obtener una lista completa del acceso al puerto requerido para esta implementación, consulte Acceso al puerto cuando todas las máquinas virtuales están en la red interna, en la página 89.

Ventajas de una topología de red IRP completamente interna

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

Desventajas de una topología de red IRP completamente interna

El acceso público (que permite que los usuarios externos accedan al sistema) requiere la apertura de puertos de entrada (80 y 443) directamente desde Internet hacia la red interna.

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

Topología de red de horizonte no dividido

Esta sección describe la topología de red cuando tiene un DNS de horizonte no dividido. Las máquinas virtuales internas (de administración, y si corresponde, multimedia y web) están en la red interna y el proxy inverso de Internet está en la red DMZ.

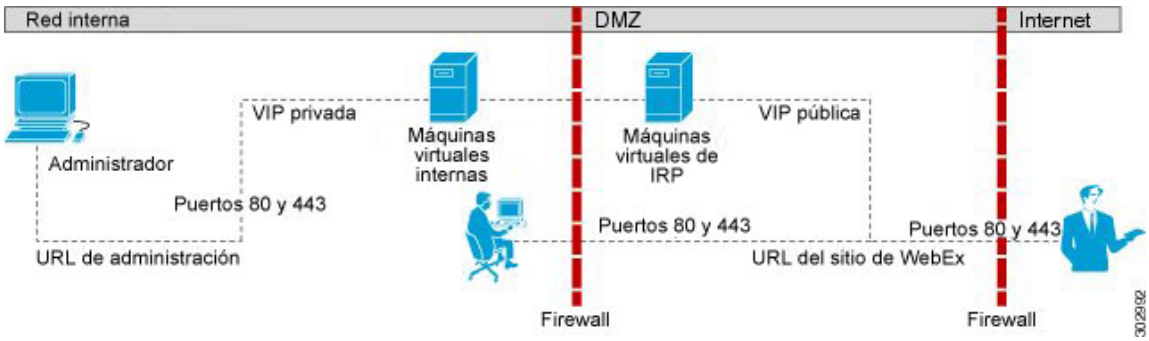
Nota Esta configuración permite a los usuarios iniciar sesión y entrar en reuniones desde Internet de forma segura sin una conexión VPN.

Nota Esta configuración es compatible con el 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 firewall) 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 la implementación de su sistema. Para obtener más información sobre estos términos y cuándo 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 de horizonte no dividido.



Nota Para obtener una lista completa del acceso al puerto requerido para esta implementación, consulte Acceso al puerto con un proxy inverso de Internet en la red DMZ, en la página 89.

Ventajas de una topología de red de horizonte no dividido

- Un estricto control sobre el tráfico que entra y sale de una red.
- Las direcciones son más comunes, simples requisitos de red DNS.

Desventajas de una topología de horizonte no dividido

- Configuración compleja, pero no tan compleja como la topología de red de horizonte dividido.
- El tráfico interno está dirigido a la red DMZ. Todo el tráfico de red desde Internet, así como desde la red privada (interna) va al proxy inverso de Internet en la red DMZ, y luego vuelve a las máquinas virtuales internas.
- Requiere que se abran más puertos en el firewall entre la red DMZ y la red interna que en la topología de red completamente interna.
- La implementación automática del sistema (para sistemas de 50, 250 u 800 usuarios concurrentes únicamente) requiere una configuración más detallada en vCenter.
- De las tres topologías de red, esta configuración afecta en mayor medida al rendimiento de la red, dado que todas las cargas de las reuniones se hacen a través del proxy inverso de Internet. Debido a que existen varios saltos, la latencia de red también se ve afectada.

Nota Consulte Requisitos del ancho de banda de la red, en la página 57 para obtener más detalles acerca de los requisitos de velocidad de NIC para implementaciones de DNS de horizonte no dividido.

Topología de red completamente interna

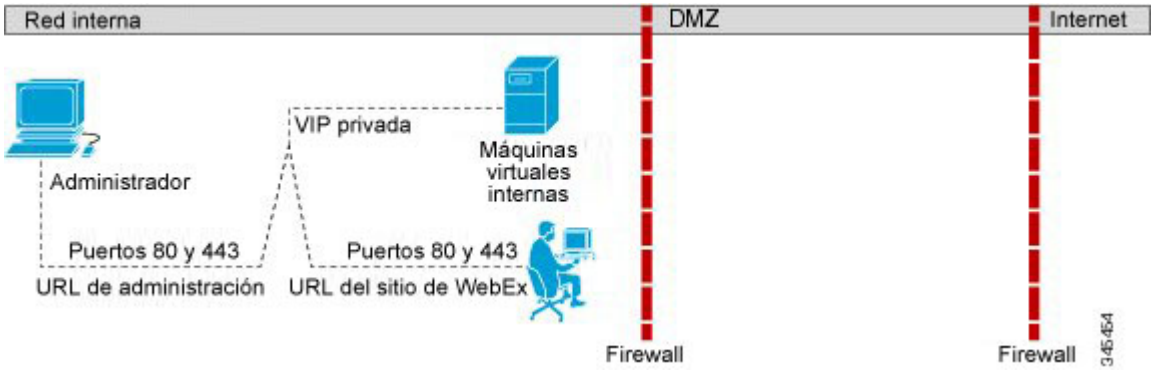
Esta sección describe la topología de red cuando todas las máquinas virtuales en su sistema están en la misma red interna. No hay acceso público; solo los usuarios internos y de VPN pueden organizar o entrar a reuniones.

Nota Si utiliza implementación automática, los hosts ESXi para todas las máquinas virtuales deben estar administrados desde el mismo vCenter de VMware. Se requiere esta información de vCenter durante una implementación automática del sistema.

Nota Esta configuración no es compatible con el acceso móvil.

Definirá la URL de administración, la URL del sitio de WebEx y la dirección VIP privada durante la implementación de su sistema. Para obtener más información sobre estos términos y cuándo 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 completamente interna.



Ventajas de una topología de red completamente interna

- Ofrece una latencia menor ya que hay menos saltos de red entre las máquinas virtuales.

Desventajas de una topología de red completamente interna

- No hay acceso público (que permite que los usuarios externos accedan al sistema) y no hay acceso para usuarios móviles.

Topología de red de horizonte dividido

Esta sección describe la topología de red cuando tiene un DNS de horizonte dividido. Las máquinas virtuales internas (de administración, y si corresponde, multimedia y web) están en la 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 desde Internet de forma segura sin una conexión VPN.

Nota Esta configuración solo puede admitir el acceso móvil desde una red IP pública (Internet). El acceso móvil no es compatible en una red interna (intranet).

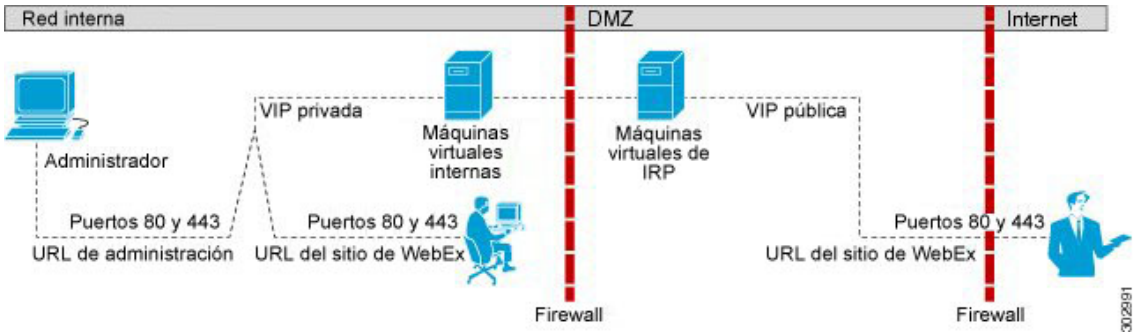
En una implementación de horizonte dividido, el tráfico que se origina desde Internet (incluidos los usuarios móviles que utilizan una red de datos de telefonía móvil) se dirige al proxy inverso de Internet. El tráfico que se origina internamente (incluidos los usuarios móviles que utilizan una conexión Wi-Fi local) se dirige 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 firewall) 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 la implementación de su sistema. Para obtener más información sobre estos términos y cuándo

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 de horizonte dividido.



Nota Para obtener una lista completa del acceso al puerto requerido para esta implementación, consulte Acceso al puerto con un proxy inverso de Internet en la red DMZ, en la página 89.

Ventajas de una topología de red de horizonte dividido

- Un estricto control sobre el tráfico que entra y sale de una red.
- Hay una separación de tráfico de red que atraviesa el sistema, que permite una propagación de la carga más distribuida.

  El tráfico procedente de Internet se dirige al proxy inverso de Internet. El tráfico procedente de la red interna (privada) irá directamente a las máquinas virtuales internas (de administración, y si corresponde, multimedia y web).
- El rendimiento y la latencia de la red son mejores que en un DNS de horizonte no dividido, pero peor que en una topología de red completamente interna.

Desventajas de una topología de red de horizonte dividido

- De las tres topologías de red distintas, esta es la configuración más compleja.
- Requiere asignación de DNS sofisticada.
- Requiere que se abran más puertos en el firewall entre la red DMZ y la red interna que en la topología de red completamente interna.
- La implementación automática del sistema (para sistemas de 50, 250 u 800 usuarios concurrentes únicamente) requiere una configuración más detallada en vCenter.
- Debido a la redirección web, para los usuarios internos, la URL del sitio de WebEx se reemplaza por la URL que muestra el nombre de host de la máquina virtual que contiene los servicios web y las máquinas virtuales multimedia.

Consulte Requisitos del ancho de banda de la red, en la página 57 para obtener más detalles acerca de los requisitos de velocidad de NIC para implementaciones de DNS de horizonte dividido.

Redundancia en implementaciones de alta disponibilidad o MDC

La alta disponibilidad (HA) proporciona redundancia a través de la recuperación de fallas de un sistema Cisco WebEx Meetings Server (CWMS) primario con errores en un sistema de alta disponibilidad CWMS de copia de seguridad en la misma ubicación física.

La característica de centro de datos múltiple (MDC) de CWMS implementa varios centros de datos y luego los une en un solo sistema CWMS. La recuperación de fallas es similar a un sistema de alta disponibilidad, excepto que los centros de datos del sistema MDC son pares en la prestación de servicio a los usuarios y no están limitados geográficamente. De hecho, la implementación de centros de datos múltiples en ubicaciones geográficas cercanas a los usuarios mejora el rendimiento de la red. Un sistema CWMS no puede admitir alta disponibilidad y MDC.

Las condiciones para la redundancia son las siguientes:

- Las máquinas virtuales de alta disponibilidad se deben colocar en el mismo centro de datos que las máquinas virtuales primarias. 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 de alta disponibilidad son los mismos que se definieron anteriormente para las máquinas virtuales primarias. No se admite la división de los componentes primarios y de alta disponibilidad del sistema entre los centros de datos.

  No se requiere que las máquinas virtuales MDC se ubiquen en forma conjunta en el mismo centro de datos.

- La conectividad entre todas las máquinas virtuales internas debe ser completamente redundante, para que la falla de un interruptor o de un enlace de red no interrumpa la conectividad entre los componentes primarios y de alta disponibilidad o MDC. Para lograr esta redundancia, cada servidor de host debe tener conexiones redundantes a diversos interruptores de Ethernet.

- Las máquinas virtuales de proxy inverso de Internet primarias y de alta disponibilidad deben estar en una VLAN o subred común (generalmente, no la misma subred que las máquinas virtuales internas). La conectividad entre las máquinas virtuales de proxy inverso de Internet también debe ser redundante, de la misma manera que las máquinas virtuales internas.

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

Agregar un sistema de alta disponibilidad o MDC no aumenta la capacidad total del sistema. Ya sea que implemente un sistema de 800 usuarios con o sin alta disponibilidad, la capacidad total del sistema sigue siendo la misma, y la cantidad máxima de conexiones de audio simultáneas es 800.

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

- Un sistema de 50 usuarios se compone de una máquina virtual de administración y, de manera opcional, una máquina virtual de proxy inverso de Internet IRP para acceso público. Si agrega un sistema de alta disponibilidad o MDC , el sistema de 50 usuarios combinado consta de dos máquinas virtuales de administración y dos máquinas virtuales IRP.

- Un sistema primario de 250 o 800 usuarios consta de una máquina virtual de administración, una máquina virtual multimedia y, opcionalmente, una máquina virtual IRP. Si agrega un sistema de alta disponibilidad o MDC , el sistema combinado de 250 u 800 usuarios se compone de dos máquinas virtuales de administración, dos máquinas virtuales multimedia y dos máquinas virtuales IRP.
- Un sistema primario de 2000 usuarios se compone de una máquina virtual de administración, tres máquinas virtuales multimedia, dos máquinas virtuales web y, de manera opcional, una máquina virtual IRP. Si agrega un sistema de alta disponibilidad o MDC , el sistema combinado de 2000 usuarios se compone 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 de alta disponibilidad o MDC , la dirección VIP pública y la dirección VIP privada se comparten con el sistema primario. (La dirección VIP pública y la dirección VIP privada son diferentes y no se comparten). Cuando una máquina virtual está fuera de servicio, la otra máquina virtual usa la misma dirección VIP. A causa de este comportamiento, la falla de una máquina virtual es casi totalmente imperceptible para los usuarios finales (ya que las reuniones continuarán), sin imponer exigencias inusuales en la infraestructura DNS. Sin embargo, una dirección VIP compartida solo se puede implementar en un segmento de red único o en una VLAN; la división de una VLAN en dos centros de datos crea diversos problemas.

Requerimos que la conectividad entre las máquinas virtuales internas primarias y de alta disponibilidad esté dentro del mismo centro de datos, lo que reduce en gran medida el problema de distinguir entre una falla de máquina virtual y una falla de red. Permitir una red dividida puede ocasionar conexiones de reuniones divididas y actualizaciones de la base de datos conflictivas. Es más práctico construir un segmento de red de alta disponibilidad dentro de un centro de datos único que entre centros de datos múltiples.

En un sistema MDC, los datos se replican en todos los centros de datos (con excepción del administrador de licencias). Por lo tanto, si un centro de datos se cae o se pierde la conectividad de red, el centro de datos sobreviviente continúa prestando servicio a los usuarios independientemente de la ubicación geográfica.

La mejor manera de crear un sistema que tolere las fallas es cuando la mayoría de los componentes del sistema funcionan en "todos activos". No obstante, ciertos componentes fundamentales, en especial el servicio de la base de datos, están en modo "activo/pasivo". (Los servidores web y los componentes multimedia en el sistema de alta disponibilidad dependen de los componentes en el sistema primario). Toda latencia o interrupción de esas conexiones da lugar a demoras para los usuarios finales, especialmente cuando entran a reuniones. La latencia entre los componentes del servicio multimedia aumenta la latencia del audio y vídeo para algunos usuarios durante las reuniones. (Para Cisco WebEx Meetings Server, es aceptable 4 ms de latencia de red entre las máquinas virtuales internas. Para obtener más detalles, consulte Diseño de las máquinas virtuales en su red, en la página 47).

Consideraciones de red para el proxy inverso de Internet

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

Restricción Incluso si los servidores Cisco UCS están configuradas con dos NIC, Cisco WebEx Meetings Server no admite apuntar un NIC a Internet y el otro a la intranet. Esta restricción se aplica independientemente de las asignaciones entre los NIC físicos y los NIC virtuales utilizadas por vSphere (y el proxy inverso de Internet).

La máquina virtual de proxy inverso de Internet siempre se conecta a una VLAN individual externa independientemente de la cantidad de NIC que utiliza. Si utiliza varios NIC físicos y están conectados a diferentes interruptores o enrutadores, los NIC deben estar conectados a la misma VLAN.

Por lo tanto, no puede utilizar el proxy inverso de Internet como puente para el tráfico entre dos segmentos de red independientes (con uno apuntando a Internet y el otro apuntando a la intranet). La siguiente sección describe cómo puede lograr esta meta.

Latencia entre las máquinas virtuales internas y el proxy inverso de Internet

La latencia máxima aceptable del tráfico de ida y vuelta en la ruta entre el NIC en el proxy inverso de Internet y el NIC en cualquiera de las máquinas virtuales internas debe establecerse en menos de 4 ms. La latencia de exceso en esta ruta limitará el ancho de banda que pueden utilizar los usuarios finales para la compartición de escritorios, audio y vídeo. Si la latencia aumenta de 4 ms a 8 ms, por ejemplo, el ancho de banda que se puede utilizar se reducirá a la mitad, lo que degradará progresivamente la experiencia a medida que aumenta la latencia.

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

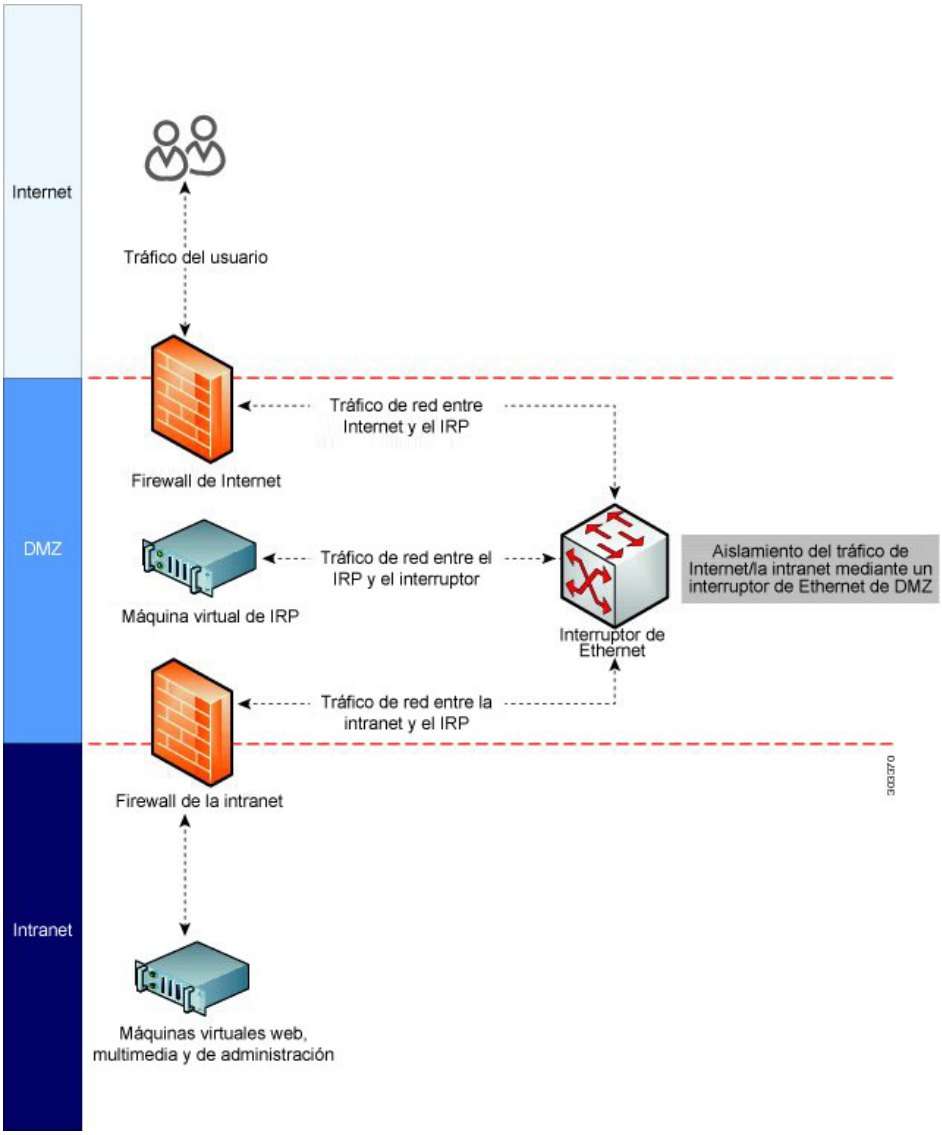
Nota Cuando la latencia excede los 4 ms entre el IRP y las máquinas virtuales internas, es posible que ocurran graves demoras en las conexiones de los usuarios finales que pasan por el proxy inverso de Internet de Cisco WebEx Meetings Server.

Aislamiento del tráfico de red

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

1. Conecte el proxy inverso de Internet al interruptor o enrutador de cabecera y utilice ese interruptor o enrutador para dividir el tráfico de Internet y de la intranet.
2. Una vez que el interruptor o el enrutador divide el tráfico, puede canalizar esos dos patrones de tráfico a dos puertos físicos independientes en el interruptor o en el enrutador. Un puerto apunta a Internet y el otro puerto apunta a la intranet.

El siguiente diagrama muestra una topología de red de ejemplo:



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

Requisitos del ancho de banda de la red

Esta sección describe los requisitos del ancho de banda para sistemas de 50, 250, 800 y 2000 usuarios. Cumplir con los requisitos del ancho de banda indicados en esta sección proporcionará una experiencia de usuario final de calidad para sus usuarios que organizan y asisten a reuniones de WebEx, y ayuda a asegurar que su red pueda soportar las demandas de tráfico de la compartición web, de audio y de vídeo.

Cálculo del ancho de banda para las sesiones del usuario final

Es importante calcular el ancho de banda de la red para soportar las demandas de tráfico de la compartición web, de audio y de vídeo para el tamaño del sistema del usuario. Los requisitos de ancho de banda de este

producto son básicamente los mismos que para los servicios de nube de Cisco WebEx. Si desea optimizar el aprovisionamiento de su red, puede consultar el uso de ancho de banda en servicios de nube de Cisco WebEx en el Informe de ancho de banda de red de WebEx.

La información de la tabla siguiente muestra el ancho de banda esperado para compartir vídeo, audio y web.

Componente de la reunión de WebEx	Ancho de banda agregado para la sesión del usuario final
Vídeo (360 p + 6 miniaturas)	1,5 Mb/s
Audio	0,1 Mb/s
Compartición web (Este valor supone que pasa una diapositiva cada 30 segundos)	0,6 Mb/s
Total del ancho de banda máximo	2,2 Mb/s

A pesar de que 2,2 Mb/s es el ancho de banda máximo esperado para una conexión de un solo usuario, Cisco recomienda utilizar el ancho de banda máximo esperado de 1,5 Mb/s al calcular los requisitos de ancho de banda. Ya que solo la mitad de la cantidad máxima de usuarios puede emplear la compartición web, de audio y de vídeo mientras que los usuarios restantes deben utilizar solo la compartición web y de audio, esto conlleva a que el ancho de banda promedio por conexión de usuario sea aproximadamente de 1,5 Mb/s.

Si consulta el *informe Ancho de banda de red de WebEx*, notará que los valores del ancho de banda en la tabla anterior se basan en las condiciones de tráfico más desfavorables. La utilización del ancho de banda promedio es *mucho* menor, pero Cisco recomienda usar las cantidades más desfavorables por las siguientes razones:

- Usar las cantidades más desfavorables para su cálculo debe ayudarlo a proporcionar el ancho de banda necesario a fin de evitar una experiencia degradada del usuario por un uso intenso.
- Cisco WebEx Meetings Server envía simultáneamente los mismos datos a todos los participantes en una reunión. Cuando un organizador de WebEx pasa una página de una presentación, una imagen de esa página (posiblemente de varios megabytes) se envía por separado a cada extremo, de forma simultánea y lo más rápido posible.

Ancho de banda en las rutas de red

Use el siguiente proceso para determinar el ancho de banda necesario en varias rutas de red.

1. Determine el ancho de banda promedio para una sesión de usuario usando la tabla en la sección anterior.
2. Determine la cantidad máxima de usuarios que espera que se conecten simultáneamente a través de ese enlace.
3. Multiplique el ancho de banda total por la cantidad máxima de usuarios.

Ejemplos de situaciones:

- Si espera que se conecten un máximo de 100 usuarios concurrentes desde Internet, probablemente necesite 1,5 Mb/s x 100 = 150 Mb/s de ancho de banda disponible en su conexión ISP, y de su firewall externo al proxy inverso de Internet. Para obtener más detalles acerca del proxy inverso de Internet, consulte . Consideraciones de red para el proxy inverso de Internet, en la página 55

- Suponga que tiene un sistema de 2000 usuarios con todas las conexiones mediante el proxy inverso de Internet. En esta situación, debe considerar el tráfico para que todos los 2000 usuarios se conecten al proxy inverso de Internet, y luego desde el proxy inverso de Internet a las máquinas virtuales internas. El ancho de banda agregado que ingresa al proxy inverso de Internet desde otras partes de la red será de 2000 x 1,5 Mb/s = 3 Gb/s. Para obtener más detalles sobre el horizonte no dividido, consulte Topología de red de horizonte no dividido, en la página 50.

Nota El mismo tráfico de 3 Gb/s pasa de entrada y de salida a través del proxy inverso de Internet, lo que requiere que el NIC en el proxy inverso de Internet soporte 6 Gb/s de tráfico de usuarios. Consulte la siguiente sección para obtener más información acerca de los requisitos de ancho de banda para el NIC en el proxy inverso de Internet.

- Suponga que tiene un sistema de 2000 usuarios en una implementación de DNS de horizonte divido. En esta situación, los 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. Suponga que el diez por ciento de los usuarios se conecta a una reunión utilizando Internet mientras que el 90 por ciento de los usuarios se conecta a las reuniones a través de la intranet. El resultado es que el ancho de banda agregado entrante en proxy inverso de Internet ahora será de aproximadamente 300 Mb/s (el 10 por ciento de 2000 usuarios multiplicado por 1,5 Mb/s es igual a 300 Mb/s). Si ese mismo tráfico de 300 Mb/s pasa desde el proxy inverso de Internet, es posible que el NIC en el proxy inverso de Internet deba soportar 600 Mb/s de tráfico de usuarios. Este es un requisito de ancho de banda considerablemente menor que con una implementación de DNS de horizonte no divido, como se describe en la situación anterior. La reducción en el tráfico de red tiene una influencia directa en las recomendaciones para la velocidad de las interfaces del interruptor o de NIC (ver sección siguiente), por lo que es posible que pueda implementar NIC de 1 Gb/s más baratos en el servidor Cisco UCS para el proxy inverso de Internet o una infraestructura de conmutación de 1 Gigabit Ethernet en una red DMZ. Para obtener más detalles acerca del horizonte dividido, consulte Topología de red de horizonte dividido, en la página 52.

Nota Es posible que deba implementar NIC de 1 Gigabit Ethernet configurados para la formación de equipos NIC si el uso del proxy inverso de Internet está ligeramente cerca del umbral de 1000 Mb/s.

Consulte Formación de equipos NIC para agregación de ancho de banda, en la página 61 para obtener más detalles.

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

Para las interfaces directas entre su arquitectura de conmutación y su sistema, recomendamos aprovisionar sus NIC de interfaz con las velocidades máximas que se muestran en la siguiente tabla. Estas velocidades se aplican a la conectividad entre los servidores de Cisco UCS y los puertos en los interruptores de cabecera en su infraestructura de conmutación local únicamente. Estas son las velocidades recomendadas necesarias para soportar los requisitos de tráfico más desfavorables.

Capacidad del sistema	Velocidad de la interfaz de NIC o del interruptor
Sistema de 50 usuarios	1 Gb/s
Sistema de 250 usuarios	1 Gb/s

Capacidad del sistema	Velocidad de la interfaz de NIC o del interruptor
Sistema de 800 usuarios	10 Gb/s[17][18]
Sistema de 2000 usuarios	10 Gb/s[19]

17 De manera opcional, puede optar por reducir los costos de la infraestructura de red al implementar la formación de equipos NIC mediante dos o más NIC de 1 Gigabit Ethernet en el servidor UCS y la formación de equipos NIC en el interruptor de cabecera.

18 Para sistemas de 800 usuarios, si su implementación utiliza almacenamiento DAS interno, puede seleccionar de manera opcional reducir los costos de infraestructura de red con la implementación de la formación de equipos NIC mediante dos o más NIC de Gigabit Ethernet en el servidor UCS y la formación de equipos NIC en el interruptor de cabecera. Sin embargo, si su implementación utiliza almacenamiento SAN o NAS, necesitará un enlace de Ethernet de 10 Gigabits.

19 Si tiene una implementación de DNS de horizonte no dividido, el requisito de 10 Gb/s corresponde para las máquinas virtuales internas y de proxy inverso de Internet. Si tiene una implementación de DNS de horizonte dividido, es posible que pueda reducir las demandas de la infraestructura de red en el proxy inverso de Internet (y red DMZ), por lo que es posible que pueda implementar NIC de 1 Gb/s más baratos en el servidor Cisco UCS para el proxy inverso de Internet o una infraestructura de conmutación de 1 Gigabit Ethernet en una red DMZ, como se describe en la sección Ancho de banda en las rutas de red. Sin embargo, el requisito de velocidad de 10 Gb/s es válido para las máquinas virtuales internas (y la red interna).

Consulte la siguiente sección "Consideraciones del ancho de banda para implementaciones de DNS de horizonte dividido" para obtener más información acerca del uso de NIC de 1 Gb/s e interruptores de Ethernet para una implementación de DNS de horizonte dividido.

Supuestos para los cálculos de velocidad de NIC:

- Se utilizó el ancho de banda agregado de la sesión del usuario final (1,5 Mb/S) para calcular las velocidades de NIC que se muestran en la tabla anterior.
- El tráfico de control entre las máquinas virtuales debe estar libre de congestión. Esto se aplica especialmente a sistemas de 2000 usuarios y a todo sistema con aprovisionamiento para alta disponibilidad. La congestión grave en enlaces de máquinas virtuales puede provocar la inestabilidad del sistema y, por consiguiente, la interrupción del servicio.
- Las conexiones al almacenamiento NAS, utilizadas para la copia de seguridad de la base de datos y las grabaciones, no deben estar congestionadas.
- La sobrecarga del protocolo y las ineficiencias en la implementación resultarán en un ancho de banda para enlaces utilizable considerablemente menor que las etiquetas de velocidad de 1 Gb/s o 10 Gb/s.
- Si un gran porcentaje de su tráfico se direccionará al proxy inverso de Internet cuando los usuarios se conecten a las reuniones, debe recordar que cada conexión de usuario pasa dos veces por el NIC en el proxy inverso de Internet (de entrada y de salida). Utilizando el sistema de 2000 usuarios como ejemplo, esto significa que, posiblemente, el NIC en el proxy inverso de Internet deba tener que soportar 6 Gb/s de tráfico del usuario (2000 usuarios multiplicado por 1,5 Mb/s es igual a 3 Gb/s, multiplicado por dos para el tráfico de entrada y de salida, es igual a 6 Gb/s).

Por prudencia, pedimos que las conexiones locales no se utilicen más del 60 por ciento para el tráfico multimedia del usuario final, lo que permite que el 40 por ciento restante esté disponible para otro tráfico, ráfagas de tráfico inusual y sobrecargas de la red. Utilizando el sistema de 800 usuarios como ejemplo, calculamos el tráfico del usuario final en 1,2 Gb/s para las máquinas virtuales de administración y multimedia, y 2,4 Gb/s para la máquina virtual de proxy inverso de Internet. Al aplicar la regla del 60 por ciento, deseamos que el NIC sea capaz de soportar 2 Gb/s para las máquinas virtuales de administración y multimedia (un tráfico del usuario estimado en 1,2 Gb/s para las máquinas virtuales de administración y multimedia dividido por el 60 por ciento estimado para el consumo de ancho de banda normal es igual a 2 Gb/s) y 4 Gb/s para la máquina virtual de proxy inverso de Internet.

Nota Las velocidades de los NIC que se muestran en la tabla anterior no consideran el ancho de banda utilizado para acceder al almacenamiento SAN. Si se utiliza el canal de fibra sobre Ethernet (FCoE) para una conexión SAN, se debe aprovisionar para utilizar una interfaz de red independiente.

Consideraciones del ancho de banda para implementaciones de DNS de horizonte dividido

Con una implementación de DNS de horizonte dividido, algunos de sus usuarios se conectarán a las reuniones desde Internet y ese tráfico pasará por el proxy inverso de Internet, mientras que la mayoría de los usuarios que están en la red interna se conectarán a las reuniones sin pasar por el proxy inverso de Internet. Con una implementación de DNS de horizonte dividido, si acelera su red y segmenta su tráfico para que la mayor parte de su tráfico permanezca dentro de la red interna (y que no pase por el proxy inverso de Internet), puede, potencialmente, utilizar la formación de equipos NIC y aprovisionar un NIC de gama más baja (NIC de 1 Gb/s) en el proxy inverso de Internet y aprovisionar la infraestructura de conmutación entre el proxy inverso de Internet e Internet para que sea de 1 Gb/s o, al menos, menor que los 10 Gb/s recomendados para un sistema de 2000 usuarios.

Por ejemplo, si una empresa tiene 100 usuarios que desean acceder a un sistema de 2000 usuarios de puertos al mismo tiempo, necesitaría un ancho de banda de 150 Mb/s (el ancho de banda agregado de 1,5 Mb/s de sesión de usuario x 100 usuarios = 150 Mb/s). Esto implica que una infraestructura de red desde la red DMZ al proxy inverso de Internet puede ser de interruptores de Ethernet de 1 Gb/s, y que la interfaz Ethernet de NIC en el proxy inverso de Internet puede ser de 1 Gb/s, en oposición al requisito de la interfaz de 10 Gb/s mencionado. Incluso cuando calcula que el proxy inverso de Internet ve el tráfico doble (lo que significa que su NIC debería soportar 300 Mb/s de tráfico del usuario), aplicando la regla del 60 por ciento (explicada en la sección "Ancho de banda en las interfaces de red de Cisco WebEx Meetings Server") se traduce a 500 Mb/s. Un enlace de 1 Gb/s es aún suficiente, pero no sería suficiente si suponemos 250 usuarios en lugar de 100 usuarios.

Nota La optimización del ancho de banda solo se aplica al NIC en el proxy inverso de Internet en implementaciones de DNS de horizonte dividido.

Para implementaciones de DNS de horizonte no dividido, debe implementar interruptores de Ethernet de 10 Gb/s e interfaces Ethernet de NIC en el proxy inverso de Internet.

Formación de equipos NIC para agregación de ancho de banda

Configurar la formación de equipos NIC en los servidores UCS que contienen el host ESXi con las máquinas virtuales internas ofrece dos ventajas: La carga de la formación de equipos NIC nivela el tráfico de red entre las redes físicas y virtuales, y proporciona la recuperación de fallas en caso de que se produzca una falla en el hardware o un corte de energía en la red. Además, en las implementaciones en las cuales la infraestructura de 10 Gb/s no está disponible, puede agrupar varios NIC de 1 Gb/s para lograr un resultado equivalente.

Nota Para obtener más información acerca de las velocidades de NIC requeridas para los diferentes tamaños de los sistemas de usuario, consulte la sección "Ancho de banda en las interfaces de red de Cisco WebEx Meetings Server" en este capítulo.

Cisco admite la formación de equipos NIC para el nivelador de carga del ancho de banda para todos los tamaños de sistemas de usuario: sistemas de 50, 250, 800 y 2000 usuarios, pero es más útil para los clientes que están intentando optimizar los costos de red para un sistema de 800 usuarios. Si su implementación utiliza almacenamiento DAS interno, los requisitos del ancho de banda agregado de y hacia los servidores Cisco UCS y los interruptores de cabecera para un sistema de 800 usuarios están previstos para ser similares al uso de NIC duales de 1 Gigabit Ethernet (o NIC cuádruples de 1 Gigabit Ethernet en un sistema con alta disponibilidad) a fin de soportar los requisitos del tráfico más desfavorable, y por lo tanto, reducir la necesidad de aprovisionar los servidores UCS con NIC de 10 Gigabit Ethernet (o de adquirir interruptores de cabecera de 10 Gigabit Ethernet).

Nota Si su implementación utiliza almacenamiento SAN o NAS, el requisito del ancho de banda agregado de y hacia los servidores Cisco UCS y los interruptores de cabecera para un sistema de 800 usuarios es 10 Gigabits Ethernet.

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

Si utiliza interfaces de red tradicionales e interruptores de Ethernet, puede proporcionar redundancia con el uso de la formación de equipos NIC e interruptores duplicados, como se indica en el siguiente proceso:

- Configure un interruptor de Ethernet que admita el Protocolo de control de agregación de enlaces (LACP) IEEE 802.3ad/IEEE 802.1ax.
- Usando vCenter, conecte el grupo de puertos de la máquina virtual asociado con las máquinas virtuales de Cisco WebEx Meetings Server a ambos adaptadores físicos.
- Conecte ambos adaptadores físicos al interruptor.
- Aprovisione el interruptor para aprovisionar de forma estática a los dos puertos como un equipo.
- Con vSphere de VMware, establezca la formación de equipos NIC a activo/activo para permitir el rendimiento en ambas interfaces NIC.

Por ejemplo, para una implementación de 800 usuarios, dos enlaces de 1Gb/s pueden sustituirse por cada enlace de 10 Gb/s en el host ESXi con las máquinas virtuales internas, y cuatro enlaces de 1 Gb/s pueden sustituirse por cada enlace de 10 Gb/s en el proxy inverso de Internet. (Para obtener la tolerancia a fallas en un sistema con alta disponibilidad, como se describe en la sección "Conexiones de red redundantes para implementaciones de alta disponibilidad", es necesario duplicar la cantidad de enlaces). Con el host ESXi con las máquinas virtuales internas, conecte dos enlaces de 1 Gb/s al primer interruptor de Ethernet *y* dos enlaces de 1 Gb/s al segundo interruptor de Ethernet.

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

CAPÍTULO 4

Cambios de red necesarios para su implementación

- Lista de control de red para su sistema, página 64
- Lista de control de la red para una instalación o expansión con una implementación automática y acceso público, página 65
- Lista de control de red para una instalación o expansión con implementación manual, acceso público y todas las máquinas virtuales internas, página 67
- Lista de control de red para una instalación o expansión con implementación automática, acceso público y un DNS de horizonte no dividido, página 71
- Lista de control de red para una instalación o expansión con implementación manual, acceso público y un DNS de horizonte no dividido, página 73
- Lista de control de red para una instalación o expansión con implementación automática, acceso público y un DNS de horizonte dividido, página 76
- Lista de control de red para una instalación o expansión con implementación manual, acceso público y un DNS de horizonte dividido, página 79
- Lista de control de red para una instalación o expansión con implementación automática y sin acceso público, página 82
- Lista de control de red para una instalación o expansión con implementación manual y sin acceso público, página 84
- URL del sitio de WebEx y de la administración de WebEx, página 87
- Acceso al puerto cuando todas las máquinas virtuales están en la red interna, página 89
- Acceso al puerto con un proxy inverso de Internet en la red DMZ, página 89
- Puertos de vCenter de VMware, página 95
- Puertos de Cisco WebEx Meeting Center, página 96
- Uso de NAT con su sistema, página 97
- Proxies de reenvío, página 100

Lista de control de red para su sistema

La lista de control de la red enumera los cambios en la red necesarios para su sistema, según la configuración de DNS y si activa o no el acceso público (lo que les permite a los usuarios organizar o asistir a las reuniones desde Internet o dispositivos móviles).

Seleccione la lista de control adecuada según si está utilizando la implementación automática del sistema (recomendada para implementaciones de 50, 250 u 800 usuarios) o la implementación manual del sistema (necesaria para una implementación de 2000 usuarios).

- Todas las máquinas virtuales, incluido el proxy inverso de Internet, están en su red interna (la configuración)
  - Lista de control de la red para una instalación o expansión con una implementación automática y acceso público, en la página 65
  - Lista de control de red para una instalación o expansión con implementación manual, acceso público y todas las máquinas virtuales internas, en la página 67
- DNS de horizonte no dividido (la configuración más común de DNS)
  - Lista de control de red para una instalación o expansión con implementación automática, acceso público y un DNS de horizonte no dividido, en la página 71
  - Lista de control de red para una instalación o expansión con implementación manual, acceso público y un DNS de horizonte no dividido, en la página 73
- DNS de horizonte dividido
  - Lista de control de red para una instalación o expansión con implementación automática, acceso público y un DNS de horizonte dividido, en la página 76
  - Lista de control de red para una instalación o expansión con implementación manual, acceso público y un DNS de horizonte dividido, en la página 79
- Sistemas sin acceso público
  - Lista de control de red para una instalación o expansión con implementación automática y sin acceso público, en la página 82
  - Lista de control de red para una instalación o expansión con implementación manual y sin acceso público, en la página 84

Lista de control de la red para una instalación o expansión con una implementación automática y acceso público

Implementación de la máquina virtual

En una implementación automática, implementamos todas las máquinas virtuales (excepto la máquina virtual de administración) por usted. Le recomendamos que elija una implementación automática si está implementando un sistema de 50, 250 u 800 usuarios.

- Compruebe que la máquina virtual multimedia (si corresponde) esté en la misma subred que la máquina virtual de administración.
- Compruebe que las máquinas virtuales de proxy inverso de Internet estén en la red interna.
- Compruebe que los hosts ESXi para todas las máquinas virtuales (incluyendo el proxy inverso de Internet) sean administrados desde el mismo vCenter de VMware.

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 corresponde)	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 (utilizada exclusivamente por el sistema. Se asigna a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
URL del sitio de WebEx (utilizada exclusivamente por el sistema. Se asigna 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 de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual multimedia de alta disponibilidad (si corresponde)	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 de alta disponibilidad (si corresponde)	Interna (misma subred que el proxy inverso de Internet del sistema primario [pero puede utilizar NAT con una dirección IP privada])	

Configuración de DNS

Actualice el servidor DNS de la siguiente manera. Existen algunas limitaciones para 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 puede utilizar, consulte URL del sitio de WebEx y de la administración de WebEx, en la página 87.

Tarea	Ejemplos
Nombres de host y direcciones IP de las máquinas virtuales internas: La máquina virtual de administración y, si corresponde, la máquina virtual multimedia.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Nombre de host y dirección IP para 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 firewall

Por motivos de seguridad, le recomendamos colocar el proxy inverso de Internet en otra subred distinta de la de las máquinas virtuales (administración y multimedia) internas. Consulte Acceso al puerto cuando todas las máquinas virtuales están en la red interna, en la página 89.

Configuración del enrutamiento de la red

Tarea	Ejemplos
Active el enrutamiento de Capa 3 entre las redes internas y DMZ.	• Subred interna <internal-subnet>/24 • Subred DMZ <DMZ-subnet>/24
Compruebe que la dirección VIP pública y las máquinas virtuales de proxy inverso de Internet estén en la misma subred. (Como está implementando todas las máquinas virtuales del sistema internamente [el proxy inverso de Internet no está en 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 estén en la misma subred.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Lista de control de red para una instalación o expansión con implementación manual, acceso público y todas las máquinas virtuales internas

Implementación de la máquina virtual

En una implantación manual, se crean todas las máquinas virtuales para su sistema utilizando el asistente de OVA para su cliente vSphere. Luego, se instala el sistema con una implementación manual.

Debe elegir una implementación manual si está implementando un sistema de 2000 usuarios.

- Asegúrese de que toda máquina virtual interna adicional (multimedia y web, si corresponde) esté en la misma subred que la máquina virtual de administración.
- Asegúrese de que las máquinas virtuales de proxy inverso de Internet estén en la 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 corresponde)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la segunda máquina virtual multimedia (solo sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la tercera máquina virtual multimedia (solo sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la máquina virtual web (solo sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la segunda máquina virtual web (solo 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 (utilizada exclusivamente por el sistema. Se asigna a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
URL del sitio de WebEx (utilizada exclusivamente por el sistema. Se asigna 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 de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual multimedia de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual web de alta disponibilidad (si corresponde)	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 de alta disponibilidad (si corresponde)	Interna: misma subred que el proxy inverso de Internet del sistema primario (pero puede utilizar NAT con una dirección IP privada)	

Configuración de DNS

Realice los siguientes cambios en su configuración de DNS.

Nota Existen algunas limitaciones para 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 puede utilizar, consulte URL del sitio de WebEx y de la administración de WebEx, en la página 87.

Tarea	Ejemplo
Actualice su servidor DNS con los nombres de host y las direcciones IP para las máquinas virtuales internas: La máquina virtual de administración y, si corresponde, 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 firewall

Por motivos de seguridad, Cisco recomienda colocar el proxy inverso de Internet en otra subred distinta de la de las máquinas virtuales internas (de administración, multimedia y web, si corresponde).

Aunque no es recomendable, también se admite la colocación de todas sus máquinas virtuales (de proxy inverso de Internet e internas) en la misma subred. Consulte Acceso al puerto cuando todas las máquinas virtuales están en la red interna, en la página 89.

Configuración del enrutamiento de la red

Realice los siguientes cambios en el enrutamiento de su red.

Tarea	Comparar estas direcciones IP
Habilite el enrutamiento L3 (Capa 3) entre las redes internas y DMZ para las siguientes máquinas virtuales: La máquina virtual de administración y, si corresponde, 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>
Asegúrese de que la dirección VIP pública y las máquinas virtuales de proxy inverso de Internet estén en la misma subred. **Nota** Como está implementando todas las máquinas virtuales del sistema internamente (el proxy inverso de Internet no está en DMZ), esta subred debe estar en la red interna.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Asegúrese de que la dirección VIP privada y las máquinas virtuales internas (de administración, multimedia y web, si corresponde) estén 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 control de red para una instalación o expansión con implementación automática, acceso público y un DNS de horizonte no dividido

Implementación de la máquina virtual

En una implementación automática, implementamos todas las máquinas virtuales (excepto la máquina virtual de administración) por usted. Le recomendamos que elija una implementación automática si está implementando un sistema de 50, 250 u 800 usuarios.

- Compruebe que la máquina virtual multimedia (si corresponde) esté en la misma subred que la máquina virtual de administración.
- Compruebe que las máquinas virtuales de proxy inverso de Internet estén en la 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 corresponde)	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 (utilizada exclusivamente por el sistema. Se asigna a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
URL del sitio de WebEx (utilizada exclusivamente por el sistema. Se asigna a la dirección VIP pública)	DMZ (misma subred que el proxy inverso de Internet)	
Dirección IP real de la máquina virtual de administración de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual multimedia de alta disponibilidad (si corresponde)	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 de alta disponibilidad (si corresponde)	DMZ (misma subred que el proxy inverso de Internet del sistema primario [pero puede utilizar NAT con una dirección IP privada])	

Configuración de DNS

Actualice el servidor DNS de la siguiente manera. Existen algunas limitaciones para 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 puede utilizar, consulte URL del sitio de WebEx y de la administración de WebEx, en la página 87.

Tarea	Ejemplo
Nombres de host y direcciones IP de las máquinas virtuales internas: La máquina virtual de administración y, si corresponde, la máquina virtual multimedia.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Nombre de host y dirección IP para 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 firewall

Por motivos de seguridad, le recomendamos colocar el proxy inverso de Internet en otra subred distinta de la de las máquinas virtuales (administración y multimedia) internas. Consulte Acceso al puerto cuando todas las máquinas virtuales están en la red interna, en la página 89.

Configuración del enrutamiento de la red

Realice los siguientes cambios en el enrutamiento de su red.

Tarea	Comparar estas direcciones IP
Active el enrutamiento de Capa 3 entre las redes internas y DMZ.	• Subred interna <internal-subnet>/24 • Subred DMZ <DMZ-subnet>/24
Compruebe que la dirección VIP pública y las máquinas virtuales de proxy inverso de Internet estén 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 estén en la misma subred.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Lista de control de red para una instalación o expansión con implementación manual, acceso público y un DNS de horizonte no dividido

Implementación de la máquina virtual

En una implantación manual, se crean todas las máquinas virtuales para su sistema utilizando el asistente de OVA para su cliente vSphere. Luego, se instala el sistema con una implementación manual.

Debe elegir una implementación manual si está implementando un sistema de 2000 usuarios.

- Asegúrese de que toda máquina virtual interna adicional (multimedia y web, si corresponde) esté en la misma subred que la máquina virtual de administración.
- Asegúrese de que las máquinas virtuales de proxy inverso de Internet estén en la 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 corresponde)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la segunda máquina virtual multimedia (solo sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la tercera máquina virtual multimedia (solo sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la máquina virtual web (solo sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la segunda máquina virtual web (solo sistemas de 2000 usuarios)	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 (utilizada exclusivamente por el sistema. Se asigna a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
URL del sitio de WebEx (utilizada exclusivamente por el sistema. Se asigna a la dirección VIP pública)	DMZ (misma subred que el proxy inverso de Internet)	
Dirección IP real de la máquina virtual de administración de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual multimedia de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual web de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real del proxy inverso de Internet de alta disponibilidad (si corresponde)	DMZ: misma subred que el proxy inverso de Internet del sistema primario (pero puede utilizar NAT con una dirección IP privada)	

Configuración de DNS

Realice los siguientes cambios en su configuración de DNS.

Nota Existen algunas limitaciones para 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 puede utilizar, consulte URL del sitio de WebEx y de la administración de WebEx, en la página 87.

Tarea	Ejemplo
Actualice su servidor DNS con los nombres de host y las direcciones IP para las máquinas virtuales internas: La máquina virtual de administración y, si corresponde, 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 firewall

Por motivos de seguridad, Cisco recomienda colocar el proxy inverso de Internet en otra subred distinta de la de las máquinas virtuales internas (de administración, multimedia y web, si corresponde). Consulte Acceso al puerto con un proxy inverso de Internet en la red DMZ, en la página 89.

Configuración del enrutamiento de la red

Realice los siguientes cambios en el enrutamiento de su red.

Tarea	Comparar estas direcciones IP
Habilite el enrutamiento L3 (Capa 3) entre las redes internas y DMZ para las siguientes máquinas virtuales: La máquina virtual de administración y, si corresponde, 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>
Asegúrese de que la dirección VIP pública y las máquinas virtuales de proxy inverso de Internet estén en la misma subred.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Asegúrese de que la dirección VIP privada y las máquinas virtuales internas (de administración, multimedia y web, si corresponde) estén 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 control de red para una instalación o expansión con implementación automática, acceso público y un DNS de horizonte dividido

Implementación de la máquina virtual

En una implementación automática, implementamos todas las máquinas virtuales (excepto la máquina virtual de administración) por usted. Le recomendamos que elija una implementación automática si está implementando un sistema de 50, 250 u 800 usuarios.

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

- Compruebe que las máquinas virtuales de proxy inverso de Internet estén en la 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 corresponde)	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 (utilizada exclusivamente por el sistema. Se asigna a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
URL del sitio de WebEx (utilizada exclusivamente por el sistema. Se asigna 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 de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual multimedia de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real del proxy inverso de Internet de alta disponibilidad (si corresponde)	DMZ (misma subred que el proxy inverso de Internet del sistema primario [pero puede utilizar NAT con una dirección IP privada])	

Configuración de DNS

Actualice el servidor DNS de la siguiente manera. Existen algunas limitaciones para 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 puede utilizar, consulte URL del sitio de WebEx y de la administración de WebEx, en la página 87.

Tarea	Ejemplo
Nombres de host y direcciones IP de las máquinas virtuales internas: La máquina virtual de administración y, si corresponde, la máquina virtual multimedia.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Nombre de host y dirección IP para la máquina virtual DMZ.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Información de la URL del sitio de WebEx, de la URL del sitio de administración y de la 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 firewall

Por motivos de seguridad, le recomendamos colocar el proxy inverso de Internet en otra subred distinta de la de las máquinas virtuales (administración y multimedia) internas. Consulte Acceso al puerto cuando todas las máquinas virtuales están en la red interna, en la página 89.

Configuración del enrutamiento de la red

Realice los siguientes cambios en el enrutamiento de su red.

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

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

Lista de control de red para una instalación o expansión con implementación manual, acceso público y un DNS de horizonte dividido

Implementación de la máquina virtual

En una implantación manual, se crean todas las máquinas virtuales para su sistema utilizando el asistente de OVA para su cliente vSphere. Luego, se instala el sistema con una implementación manual.

Debe elegir una implementación manual si está implementando un sistema de 2000 usuarios.

- Asegúrese de que toda máquina virtual interna adicional (multimedia y web, si corresponde) esté en la misma subred que la máquina virtual de administración.
- Asegúrese de que las máquinas virtuales de proxy inverso de Internet estén en la 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 corresponde)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la segunda máquina virtual multimedia (solo sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la tercera máquina virtual multimedia (solo 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 sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la segunda máquina virtual web (solo sistemas de 2000 usuarios)	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 (utilizada exclusivamente por el sistema. Se asigna a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
URL del sitio de WebEx (utilizada exclusivamente por el sistema. Se asigna 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 de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual multimedia de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual web de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real del proxy inverso de Internet de alta disponibilidad (si corresponde)	DMZ: misma subred que el proxy inverso de Internet del sistema primario (pero puede utilizar NAT con una dirección IP privada)	

Configuración de DNS

Realice los siguientes cambios en su configuración de DNS.

Nota Existen algunas limitaciones para 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 puede utilizar, consulte URL del sitio de WebEx y de la administración de WebEx, en la página 87.

Tarea	Ejemplo
Actualice su servidor DNS (que permite la búsqueda interna) con los nombres de host y las direcciones IP para las máquinas virtuales internas: La máquina virtual de administración y, si corresponde, 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 (que permite 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 DNS (que permite 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 permite 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 firewall

Por motivos de seguridad, Cisco recomienda colocar el proxy inverso de Internet en otra subred distinta de la de las máquinas virtuales internas (de administración, multimedia y web, si corresponde). Consulte Acceso al puerto con un proxy inverso de Internet en la red DMZ, en la página 89.

Configuración del enrutamiento de la red

Realice los siguientes cambios en el enrutamiento de su red.

Tarea	Comparar estas direcciones IP
Habilite el enrutamiento L3 (Capa 3) entre las redes internas y DMZ para las siguientes máquinas virtuales: La máquina virtual de administración y, si corresponde, 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>
Asegúrese de que la dirección VIP pública y las máquinas virtuales de proxy inverso de Internet estén en la misma subred.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Asegúrese de que la dirección VIP privada y las máquinas virtuales internas (la máquina virtual de administración y, si corresponde, las máquinas virtuales web y multimedia) estén 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 control de red para una instalación o expansión con implementación automática y sin acceso público

Implementación de la máquina virtual

En una implementación automática, implementamos todas las máquinas virtuales (excepto la máquina virtual de administración) por usted. Le recomendamos que elija una implementación automática si está implementando un sistema de 50, 250 u 800 usuarios.

Compruebe que la máquina virtual multimedia (si corresponde) 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 corresponde)	Interna (misma subred que la máquina virtual de administración)	
URL de administración (utilizada exclusivamente por el sistema. Se asigna a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la máquina virtual de administración de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual multimedia de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real del proxy inverso de Internet de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	

Configuración de DNS

Actualice el servidor DNS de la siguiente manera. Existen algunas limitaciones para 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 puede utilizar, consulte URL del sitio de WebEx y de la administración de WebEx, en la página 87.

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

Configuración del firewall

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

Configuración del enrutamiento de la red

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

Lista de control de red para una instalación o expansión con implementación manual y sin acceso público

Implementación de la máquina virtual

En una implantación manual, se crean todas las máquinas virtuales para su sistema utilizando el asistente de OVA para su cliente vSphere. Luego, se instala el sistema con una implementación manual.

Debe elegir una implementación manual si está implementando un sistema de 2000 usuarios.

- Asegúrese de que toda máquina virtual interna adicional (multimedia y web, si corresponde) 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 corresponde)	Interna (misma subred que la máquina virtual de administración)	

Descripción	Ubicación de red	Dirección IP
Dirección IP real de la segunda máquina virtual multimedia (solo sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la tercera máquina virtual multimedia (solo sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la máquina virtual web (solo sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la segunda máquina virtual web (solo sistemas de 2000 usuarios)	Interna (misma subred que la máquina virtual de administración)	
URL de administración (utilizada exclusivamente por el sistema. Se asigna a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
URL del sitio de WebEx (utilizada exclusivamente por el sistema. Se asigna a la dirección VIP privada)	Interna (misma subred que la máquina virtual de administración)	
Dirección IP real de la máquina virtual de administración de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual multimedia de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	
Dirección IP real de la máquina virtual web de alta disponibilidad (si corresponde)	Interna (misma subred que la máquina virtual de administración del sistema primario)	

Configuración de DNS

Realice los siguientes cambios en su configuración de DNS.

Nota Existen algunas limitaciones para 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 puede utilizar, consulte URL del sitio de WebEx y de la administración de WebEx, en la página 87.

Tarea	Ejemplo
Actualice su servidor DNS (que permite la búsqueda interna) con los nombres de host y las direcciones IP para las máquinas virtuales internas: La máquina virtual de administración y, si corresponde, 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 la URL del sitio de administración, la URL del sitio de WebEx y la información de la dirección VIP privada.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>

Configuración del firewall

Realice los siguientes cambios en sus firewalls.

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

Configuración del enrutamiento de la red

Realice los siguientes cambios en el enrutamiento de su red.

Tarea	Comparar estas direcciones IP
Asegúrese de que la dirección VIP privada y las máquinas virtuales internas (de administración, multimedia y web, si corresponde) estén 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 de la administración de WebEx

URL del sitio de WebEx

Los usuarios obtienen acceso 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, según si utiliza un DNS de horizonte dividido o no.

- Se resuelve en la dirección VIP pública para todos los usuarios, cuando no tiene DNS de horizonte dividido.
- Se resuelve en la dirección VIP pública para los usuarios externos cuando tiene DNS de horizonte dividido.
- Se resuelve en la dirección VIP privada para los usuarios internos cuando tiene 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, administrar y controlar 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 la administración de WebEx

Puede elegir casi cualquier nombre para estas URL, y deben componerse de todos caracteres en minúsculas. Sin embargo, en las URL no puede usar lo siguiente como nombre de host:

- el mismo nombre que el nombre de host de cualquiera de las máquinas virtuales del sistema
- autenticación
- cliente
- logotipo de la empresa
- despachador
- documentos
- administrador de elm
- servicios de clientes del elm
- correos electrónicos
- mantenimiento
- administrador
- orion
- datos de orion
- plantilla de orion
- nbr
- npp
- sonda
- recordatorio
- RAÍZ
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- versión
- servicio WBX
- WebEx

Acceso al puerto cuando todas las máquinas virtuales están en la red interna

Esta sección describe el acceso al puerto necesario en el firewall externo cuando todas las máquinas virtuales del sistema (de administración, y si correspondiera, multimedia, web y de proxy inverso de Internet) están en la red interna. Esta es la topología de red del proxy inverso de Internet interno.

Nota El nodo web y el nodo de administración envían solicitudes de SMTP al servidor de correo electrónico configurado. Si hay un firewall entre las máquinas virtuales internas web y de administración, y el servidor de correo electrónico, es posible que el tráfico SMTP se bloquee. Para asegurarse de que la configuración del servidor de correo electrónico y la notificación del correo electrónico funcionan correctamente, el puerto 25 o 465 (número de puerto SMTP seguro) debe estar abierto entre el servidor de correo electrónico y las máquinas virtuales web y de administración.

Acceso al puerto en el firewall externo

Si habilitó el acceso público, los siguientes puertos son entradas abiertas directamente desde Internet a las máquinas virtuales de proxy inverso de Internet en la red interna:

Importante Asegúrese de que el firewall o cualquier solución de nivelador de carga redireccione las solicitudes a los puertos que se enumeran a continuación para garantizar que los usuarios finales puedan organizar reuniones con éxito.

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

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

Esta sección describe el acceso al puerto necesario en los firewalls internos y externos cuando tiene máquinas virtuales internas (de administración, y si corresponde, multimedia y web) en la red interna, y el proxy inverso de Internet en la red DMZ.

Configure listas de control de acceso (ACL) en el interruptor que permite el tráfico a los hosts ESXi para las máquinas virtuales del sistema.

Acceso al puerto en el firewall externo

Si habilitó el acceso público, los siguientes puertos son entradas abiertas de Internet a las máquinas virtuales de proxy inverso de Internet en la red DMZ:

Importante Asegúrese de que el firewall o cualquier solución de nivelador de carga redireccione las solicitudes a los puertos que se enumeran a continuación para garantizar que los usuarios finales puedan organizar reuniones con éxito.

Nota Cisco recomienda enfáticamente 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 de WebEx sin tener que recordar si es http o https). No obstante, para este producto, el tráfico de red real siempre fluye sobre el puerto 443 (https de SSL cifrada).

Restricción Configure el puerto TCP 64700 en el proxy inverso de Internet para denegar todas las solicitudes que lleguen a la dirección VIP pública. En el firewall externo, podrá limitar el acceso a este puerto para las solicitudes solo desde las máquinas virtuales de administración.

Protocolo	Puerto	Origen	Destino	Por qué es necesario
TCP	443	Cualquier cliente externo	VIP pública (Eth1) del proxy inverso de Internet	Los clientes externos acceden a la URL del sitio de WebEx utilizando https. Las conexiones de TCP se inician desde las máquinas del cliente externo a las máquinas virtuales de proxy inverso de Internet.
TCP	80	Cualquier cliente externo	VIP pública (Eth1) del proxy inverso de Internet	Los clientes externos acceden a la URL del sitio de WebEx utilizando http. Las conexiones de TCP se inician desde las máquinas del cliente externo a las máquinas virtuales de proxy inverso de Internet.

Protocolo	Puerto	Origen	Destino	Por qué es necesario
UDP	53	IP real (Eth0) del proxy inverso de Internet	Servidor DNS	Esto es necesario si tiene un firewall entre las máquinas virtuales y el servidor DNS, para que su sistema implemente y opere con éxito.

Acceso al puerto en el firewall interno

Los puertos siguientes se deben abrir cuando el proxy inverso de Internet está en la red DMZ. Si tiene restricciones en las conexiones desde la red interna hacia la red DMZ, se aplica la siguiente tabla. Se permiten las conexiones TCP de *salida* desde la red interna hacia el segmento de la red DMZ en los siguientes puertos.

Nota No es necesario que se permitan las conexiones TCP desde el segmento de DMZ hacia la red interna para que este producto funcione adecuadamente.

Nota Utilizando tablas IP y listas de control de acceso (ACL), configure el firewall para que las conexiones al puerto 64616 solo provengan de la máquina virtual de administración.

Nota El nodo web y el nodo de administración envían solicitudes de SMTP al servidor de correo electrónico configurado. Si hay un firewall entre las máquinas virtuales internas web y de administración, y el servidor de correo electrónico, es posible que el tráfico SMTP se bloquee. Para asegurarse de que la configuración del servidor de correo electrónico y la notificación del correo electrónico funcionan correctamente, el puerto 25 o 465 (número de puerto SMTP seguro) debe estar abierto entre el servidor de correo electrónico y las máquinas virtuales web y de administración.

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

Protocolo	Puerto	Origen	Destino	Por qué es necesario
TCP	64001	Todas las máquinas virtuales internas (Eth0 IP)	IP real (Eth0) de las máquinas virtuales de proxy inverso de Internet	Establece conexiones inversas al proxy inverso de Internet (IRP). Las conexiones de TCP son establecidas desde las máquinas virtuales internas a las máquinas virtuales IRP.
TCP	64002	Máquinas virtuales web y de administración (Eth0 IP)	IP real (Eth0) de las máquinas virtuales de proxy inverso de Internet	Establece conexiones inversas al IRP. Las conexiones de TCP son establecidas desde las máquinas virtuales internas a las máquinas virtuales de proxy inverso de Internet.
TCP	7001	Todas las máquinas virtuales internas (Eth0 IP)	IP real (Eth0) de las máquinas virtuales de proxy inverso de Internet	Establece conexiones inversas al IRP. Las conexiones de TCP son iniciadas desde las máquinas virtuales internas a las máquinas virtuales IRP.

Protocolo	Puerto	Origen	Destino	Por qué es necesario
TCP	64616	Máquinas virtuales de administración (Eth0 IP)	IP real (Eth0) de las máquinas virtuales de proxy inverso de Internet	Inicie el IRP. Las conexiones de TCP son iniciadas desde las máquinas virtuales de administración a las máquinas virtuales IRP. **Nota** Utilizando tablas IP y listas de control de acceso (ACL), configure el firewall para que las conexiones al puerto 64616 solo provengan de la máquina virtual de administración.
TCP	64700	Máquinas virtuales de administración (Eth0 IP)	IP real (Eth0) de las máquinas virtuales de proxy inverso de Internet	Recopila registros sobre el IRP. Las conexiones de TCP son iniciadas desde las máquinas virtuales de administración a las máquinas virtuales IRP. En todas las máquinas virtuales de Cisco WebEx Meetings Server, limite el acceso a este puerto únicamente a otras máquinas virtuales de Cisco WebEx Meetings Server con reglas de firewall.

Protocolo	Puerto	Origen	Destino	Por qué es necesario
TCP	22	Cualquier máquina de cliente interno	IP real (Eth0) de las máquinas virtuales de proxy inverso de Internet	Solución de problemas de las máquinas virtuales IRP mediante la cuenta de soporte remoto.
TCP	443	Cualquier máquina de cliente interno	VIP privada (Eth1) de las máquinas virtuales de administración VIP privada (Eth1) de las máquinas virtuales multimedia	Usuarios internos que obtienen acceso a la URL del sitio de WebEx utilizando https. Las conexiones de TCP son establecidas desde la máquina del cliente interno a la máquina virtual de administración.
TCP	65002	Cualquier máquina de cliente interno	Cualquier máquina de cliente interno	Controla el tráfico de red entre las máquinas virtuales internas
TCP	65102	Cualquier máquina de cliente interno	Cualquier máquina de cliente interno	Controla el tráfico de red entre las máquinas virtuales internas
TCP	80	Cualquier máquina de cliente interno	VIP privada (Eth1) de las máquinas virtuales de administración	Usuarios internos que acceden a la URL del sitio de WebEx utilizando http. Las conexiones de TCP son establecidas desde la máquina del cliente interno a la máquina virtual de administración.

Protocolo	Puerto	Origen	Destino	Por qué es necesario
UDP	53	Todas las máquinas virtuales internas (Eth0 IP)	Servidor DNS	Si tiene un firewall entre las máquinas virtuales y el servidor DNS, para que su sistema se implemente y funcione correctamente.
TCP	8443	Nodo web de Cisco WebEx Meetings Server	CUCM	Para el tráfico AXL en un sistema de centro de datos múltiple entre Cisco WebEx Meetings Server y CUCM para permitir la recuperación de fallas LDAP CUCM.

Puertos de vCenter de VMware

Puertos abiertos para la implementación

Estos son algunos de los puertos que se utilizan durante la implementación de un Cisco WebEx Meetings Server (CWMS) de centro de datos único (SDC). Una vez que finaliza la implementación, puede cerrar todos los puertos que se abrieron exclusivamente para la implementación.

El puerto 443 TCP debe estar abierto, en ambas direcciones, entre vCenter y la máquina virtual de administración para una administración segura de https durante la implementación automática del sistema. La máquina virtual de administración utiliza este puerto para proporcionar las credenciales de vCenter de manera de implementar las máquinas virtuales automáticamente en vCenter.

Los puertos listados a continuación se usan para la comunicación entre el host ESXi y vCenter. Si el host ESXi y vCenter están conectados a una *red de administración aparte*, es posible que no necesite abrir estos puertos por medio del firewall. Para ver una lista completa de los puertos utilizados por vCenter y el host ESXi, consulte la documentación de VMware.

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

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

Puertos abiertos para admitir un centro de datos múltiple

Puertos que deben estar abiertos 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 deben estar abiertos entre las máquinas internas e IP virtuales	tcp 443 tcp 80
Puertos que deben estar abiertos entre las IP de proxy inverso de Internet y las máquinas interna	tcp 7001 tcp 64001 tcp 64700 tcp 64616
Puertos UDP que deben estar abiertos entre las máquinas internas	udp range:10000:19999 udp range:16000:32000 udp range: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 que se utilizan para la transmisión de datos de audio y vídeo entre UDP y SSL para los clientes internos incluyen:
  - 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 de medios internos permiten las conexiones a través de cualquier puerto que Meeting Center utilice.
- El proxy inverso de Internet solo acepta conexiones de Meeting Center a través de los puertos TCP 80 y 443.
- El tráfico AXL del nodo web a CUCM pasa por el puerto 8443. (Consulte también Usar CUCM para configurar el servicio web de AXL y la sincronización de directorios).

Uso de NAT con su sistema

Cisco es compatible con la traducción de la dirección de red (NAT) transversal con este producto para las direcciones IP de la máquina virtual y para las direcciones IP virtuales (VIP pública y privada) que se utilizan en su sistema.

Nota Para obtener más información sobre NAT, consulte http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml.

El siguiente diagrama esquemático muestra una NAT transversal para un sistema de 50 usuarios sin alta disponibilidad. Si utiliza NAT, puede reducir la cantidad de *direcciones IP públicas* requeridas para el producto a solo una dirección IP, en lugar de dos (o tres en caso de implementar alta disponibilidad). También puede realizar implementaciones similares de la NAT siempre que cumplan con los requisitos generales del sistema.

Nota El uso de varias NAT y varios firewalls tiende a aumentar la latencia, lo que afecta la calidad del tráfico en tiempo real para los usuarios.

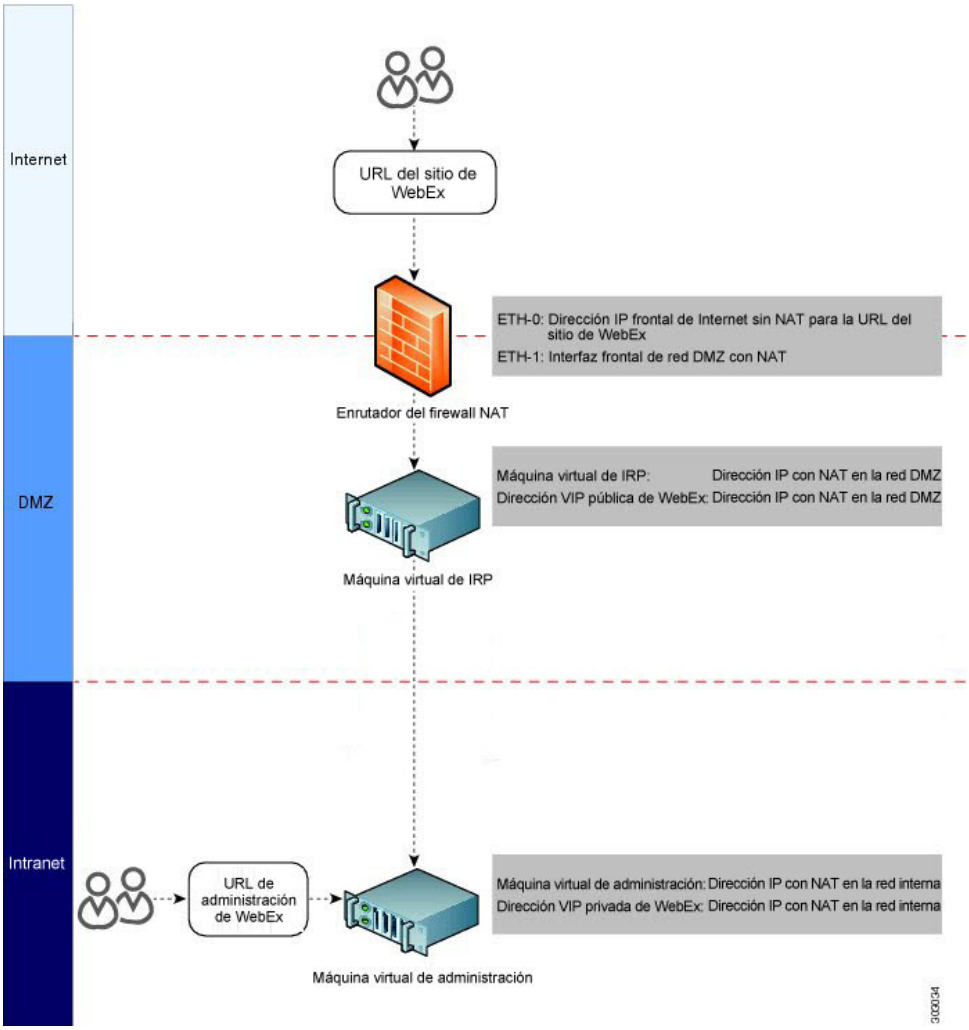
Importante Cuando utilice varios dominios de NAT, el enrutamiento entre estos diferentes dominios de NAT puede ser difícil. Sin embargo, podrá utilizar direcciones IP con NAT siempre que se cumplan los siguientes requisitos:

- Todas las máquinas virtuales en el sistema pueden utilizar direcciones IP con NAT.
- La máquina virtual de administración en la red interna debe poder acceder a la dirección IP de la máquina virtual de proxy inverso de Internet.

  Nota No se admite NAT entre la máquina virtual de administración y la máquina virtual de proxy inverso de Internet. La máquina virtual de administración debe poder tener acceso a la dirección IP de la máquina virtual de proxy inverso de Internet (su verdadera dirección IP) en la red interna.

- La dirección VIP pública no necesita ser públicamente visible, pero se debe poder traducir desde Internet.
- Cuando implemente acceso público, la URL del sitio de WebEx debe ser asignada a una dirección IP de Internet visible. Los usuarios externos deben poder acceder a esta dirección IP de Internet visible, la cual, *también* debe ser asignada a la dirección VIP pública que configure durante la implementación del sistema.

  Puede elegir hacer que la dirección VIP pública sea visible desde Internet. Si elige no hacerla públicamente visible, se debe, por tanto, poder traducir desde Internet.



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

El enrutador del firewall recibe esta solicitud del usuario externo, y enruta internamente la solicitud a la dirección IP privada de NAT para el enrutador (Eth1, expuesta 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 red privado para el sitio de WebEx).

Puede usar direcciones IP de NAT para la dirección VIP pública y para las direcciones IP del proxy inverso de Internet. La única dirección IP pública de NAT es la dirección IP Eth0 para el enrutador del firewall de NAT.

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

Normalmente, hay un segundo enrutador interno del firewall de NAT entre la red DMZ y la red interna. De forma similar al enrutador externo del firewall de NAT, Eth0 es una dirección IP privada de NAT de DMZ y es una interfaz a la red DMZ. Eth1 es también una dirección IP privada de NAT que es una interfaz de la red interna.

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

Proxies de reenvío

Si su topología de red incluye proxies de reenvío, estos *deben cumplir requisitos específicos* para que el proxy inverso de Internet funcione correctamente. Para ver los detalles completos consulte "Uso de proxies de reenvío en el sistema" en la *Guía de solución de problemas de Cisco WebEx Meetings Server*.

CAPÍTULO 5

Mejores prácticas

- Mejores prácticas para Cisco WebEx Meetings Server, página 101

Mejores prácticas para Cisco WebEx Meetings Server

La siguiente es una lista de mejores prácticas que puede consultar cuando configure y mantenga su sistema Cisco WebEx Meetings Server:

- Encienda sus hosts de máquina virtual mediante una unidad de suministro de energía ininterrumpida (UPS) para minimizar las interrupciones de energía. Las fallas de alimentación repetidas pueden dañar los sistemas del host y las máquinas virtuales.
- Siempre coloque el sistema en el modo de mantenimiento antes de apagar el sistema operativo de un invitado.
- Para los eventos planificados y otras situaciones que requieran apagar el sistema, apague sus máquinas virtuales correctamente apagando el sistema operativo del invitado.
- El sistema está diseñado para repararse a sí mismo cuando es necesario y el reinicio puede interrumpir este proceso. No se recomienda reiniciar el sistema para repararlo. Si el sistema se encuentra en estado de mal funcionamiento, comuníquese con el Centro de Asistencia Técnica (TAC) de Cisco. Apague su sistema solo cuando se le solicite hacerlo o durante eventos planificados, como el mantenimiento del centro de datos.
- Configure la redundancia de red para minimizar las fallas de la red. Consulte "Agregar sistema de alta disponibilidad" en la *Guía de administración de Cisco WebEx Meetings Server* para obtener más información.
- Configure la formación de equipos NIC en su sistema. La formación de equipos NIC mejora el rendimiento y ofrece redundancia en el caso de una falla de NIC.
- Si su organización cuenta con experiencia en la administración de una red de área de almacenamiento (SAN), recomendamos utilizar SAN sobre almacenamiento conectado directamente (DAS). SAN puede ser más confiable que los arreglos de discos locales.Consulte Requisitos generales del sistema, en la página 1 para obtener más información sobre los requisitos de almacenamiento SAN.
- El uso de instantáneas en las máquinas virtuales puede afectar el rendimiento del sistema de la misma manera que puede afectar la experiencia del usuario, incluso cuando el sistema está levemente cargado.

- Si el sistema tiene problemas, asegúrese de verificar el entorno de VCenter de VMware para determinar si las condiciones de VCenter o de la red están provocando el problema.
- Configure la alta disponibilidad para aumentar las posibilidades de que su sistema continúe funcionando en el caso de que ocurra una falla.
- Si tiene un sistema de alta disponibilidad y falla el sistema secundario, puede repararlo eliminando el sistema secundario existente (consulte "Eliminar un sistema de alta disponibilidad" en la *Guía de administración de Cisco WebEx Meetings Server*) y agregando un nuevo sistema secundario (consulte "Agregar sistema de alta disponibilidad" en la *Guía de administración de Cisco WebEx Meetings Server*). Si falla el sistema primario en un sistema de alta disponibilidad, no puede repararlo mediante este procedimiento. Le recomendamos que restaure su sistema primario utilizando el procedimiento de recuperación de desastres y, luego, agregue un nuevo sistema secundario. La implementación funcionará sin redundancia completa hasta que agregue un nuevo sistema secundario. Este procedimiento ayuda a evitar las interrupciones no planificadas en caso de que falle alguna de las máquinas virtuales secundarias. Consulte "Uso de la característica de recuperación de desastres" en la *Guía de administración de Cisco WebEx Meetings Server* para obtener más información.
- Proporcione un sistema de archivos en red (NFS) y asegúrese de que posea la capacidad de almacenamiento suficiente para almacenar las copias de seguridad automáticas regulares de la base de datos y de las grabaciones de reuniones.
- Debido a que su sistema solo mantiene la copia de seguridad más reciente del sistema en el NFS y elimina las instancias anteriores todos los días, recomendamos mantener varias copias de seguridad recientes en otro medio.

Restricción No cree manualmente archivos o directorios en el recurso compartido de NFS que utiliza Cisco WebEx Meetings Server, dado que este ejecuta diversas secuencias de comandos en los archivos y directorios de NFS. El servidor de almacenamiento de NFS debe ser para uso exclusivo de Cisco WebEx Meetings Server.

- Utilice la consola para monitorear el estado del NFS, la CPU y el almacenamiento. Le recomendamos que las alarmas de la consola para el almacenamiento y la CPU estén activadas.
- Si planea usar la integración de directorios, consulte la sección Configurar la integración de directorios en el capítulo "Administración de usuarios" de la *Guía de administración de Cisco WebEx Meetings Server* para obtener más información.
- Cuando utiliza Cisco WebEx Meetings Server, el enlace troncal de SIP en CUCM en la interfaz de Call Manager debe tener la casilla de verificación **Punto de terminación de medios requerido** anulada en la página **Configuración de enlace troncal**. Consulte Configuración de un enlace troncal de SIP en un punto de nivelador de carga, en la página 121 y Configuración de un enlace troncal de SIP para un punto de aplicación, en la página 122 para obtener más información.
- Si está realizando una mejora a Cisco WebEx Meetings Server versión 2.0 o superior y está usando servidores blade B-series, debe utilizar almacenamiento SAN para cumplir con 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 103
- Lista de control de configuración de CUCM para un centro de datos múltiple, página 105
- Lista de control de la configuración de CUCM con o sin alta disponibilidad, página 106
- Configuración de CUCM en un sistema de centro de datos múltiple de CWMS, página 107
- Configuración de CUCM para sistemas de alta disponibilidad y sin alta disponibilidad, página 109
- Configuración de un perfil de seguridad del enlace troncal de SIP, página 114
- Configuración de un perfil de SIP, página 116
- Administración de certificados de CUCM mediante TLS, página 117
- Configuración de un enlace troncal de SIP, página 121
- Configuración de un grupo de rutas, página 123
- Configuración de una lista de rutas, página 124
- Configuración de un patrón de ruta, página 125
- Configuración de un patrón de ruta SIP, página 125
- Compatibilidad y soporte de las características de CUCM, página 126

Configuración de Cisco Unified Communications Manager (CUCM)

Para activar las teleconferencias en Cisco WebEx Meetings Server, debe configurar un sistema Cisco Unified Communications Manager (CUCM) o más para administrar 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 de centro de datos múltiple (MDC) son las mismas que en un entorno de centro de datos único (SDC). Los parámetros de configuración modificados en un centro de datos se corresponden automáticamente en el otro centro de datos.

En CUCM, las configuraciones básicas en un entorno de centro de datos múltiple (MDC) son las mismas que en un entorno de centro de datos único (SDC). Sin embargo, debe configurar enlaces troncales a todos los centros de datos. Cada centro de datos puede tener un patrón de ruta diferente. Si desea usar más de un CUCM, cada centro de datos debe tener un enlace troncal SIP al CUCM en los otros centros de datos para transferir las llamadas.

Antes de comenzar

Obtenga la información de su punto de nivelador de carga y de su punto de aplicación en la página **Audio** de Cisco WebEx Meetings Server. Los puntos de nivelador de carga administran el equilibrio de carga de llamadas y los puntos de aplicación administran las llamadas, el flujo de conferencias y el control de las características. Los sistemas de distintos tamaños poseen distintas cantidades de puntos de nivelador de carga y de puntos de aplicación y estas cantidades no son personalizadas. Inicie sesión en el sitio de administración y seleccione **Configuración** > **Audio** para ver esta información.

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

En la página **Audio** existe una Tabla de configuración de SIP que muestra información sobre el punto de nivelador de carga y el punto de aplicación, incluidas las direcciones IP y los puertos. Esta tabla también aparece en la página **Configurar los parámetros de audio por primera vez** que se muestra la primera vez que configura los parámetros de audio.

Para permitir que CUCM funcione con Cisco WebEx Meetings Server, CUCM necesita las siguientes configuraciones base y específica:

- Configuración base

  Nota Estas configuraciones pueden compartirse con varios sistemas de Cisco WebEx Meetings Server.

  - Perfil de seguridad troncal de SIP
  - Perfil de SIP

- Configuración específica

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

  - Administración de certificados
  - Enlace troncal de SIP

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

Teleconferencias seguras de CUCM en un entorno MDC

No es posible importar certificados de todos los centros de datos de un centro de datos múltiple (MDC) a un solo Cisco Unified Call Manager (CUCM) según sea necesario para asegurar las teleconferencias (https://cibu-jira:8443/browse/SECURITY-1432) cuando el nombre común de ambos certificados es el mismo.

En forma predeterminada, el nombre común de todos los centros de datos es la URL del sitio global del sistema. Sin embargo, para hacer que el nombre común sea exclusivo, puede generar certificados usando Generar una Solicitud de firma de certificado (CSR) o Generar un certificado de firma automática. Seleccione la URL del sitio local en lugar de la URL del sitio global para que se use en el nombre común.

Los certificados de firma automática generados durante cualquier procedimiento de modificación del sistema (por ejemplo, cambiar la URL del sitio o de administración, cambiar los nombres de organizador) conllevan un certificado que tiene la URL del sitio global en el nombre común, por lo que, después de este tipo de operación, debe crear los certificados manualmente con la URL del sitio local.

Lista de control de configuración de CUCM para un centro de datos múltiple

La lista de control de configuración muestra el número de cada tipo de configuración de Cisco Unified Communication Manager (CUCM) que debe configurar para su sistema con un centro de datos múltiple (MDC).

Tamaño del sistema	Perfiles de seguridad (configuración base)	Perfiles de SIP (configuración base)	Enlaces troncales de SIP (configuración específica)	Grupos de ruta (configuración específica)	Listas de rutas (configuración específica)	Patrones de ruta (configuración específica)	Patrones de ruta SIP (configuración específica)
250 usuarios	2	1	4	1	1	N	2
800 usuarios	2	1	4	1	1	N	2
2000 usuarios con alta disponibilidad	2	1	6	1	1	N	4

Lista de control de la configuración de CUCM con o sin alta disponibilidad

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

Tamaño del sistema	Perfiles de seguridad (configuración base)	Perfiles de SIP (configuración base)	Enlaces troncales de SIP (configuración específica)	Grupos de ruta (configuración específica)	Listas de rutas (configuración específica)	Patrones de ruta (configuración específica)	Patrones de ruta SIP (configuración específica)
50 usuarios	2	1	2	1	1	N[20]	1
50 usuarios con alta disponibilidad	2	1	4	1	1	N	2
250 usuarios	2	1	2	1	1	N	1
250 usuarios con alta disponibilidad	2	1	4	1	1	N	2
800 usuarios	2	1	2	1	1	N	1
800 usuarios con alta disponibilidad	2	1	4	1	1	N	2
2000 usuarios	2	1	5	1	1	N	3
2000 usuarios con alta disponibilidad	2	1	6	1	1	N	4

20 N es la cantidad de números de acceso de llamadas entrantes que configura en Cisco WebEx Meetings Server.

Configuración de CUCM en un sistema de centro de datos múltiple de CWMS

Generalmente, cada sitio en un entorno de centro de datos múltiple (MDC) tiene un grupo CUCM dedicado asociado con él. Los grupos de CUCM se conectan mediante enlaces troncales intergrupales (ICT). Cada grupo de CUCM tiene enlaces troncales de marcado/llamada entrante al sitio de CWMS local. Session Manager Edition (SME) es compatible. CWMS se puede configurar detrás de los grupos de CUCM locales. Cada CUCM tiene enlaces troncales SIP REFER a todas las máquinas virtuales multimedia en el MDC.

Para redundancia, cada grupo de CUCM puede tener enlaces troncales INVITE a todos los centros de datos. El patrón de ruta de llamadas entrantes prioriza el enlace troncal INVITE asociado con el centro de datos local y usa el enlace troncal INVITE al centro de datos remoto solo en caso de falla.

Tabla 4: Enlaces troncales CUCM SIP configurados en cada grupo de CUCM

Implementación	Enlaces troncales INVITE – Nivelador de carga (MACC)	Enlaces troncales REFER – Punto de aplicación (TAS)
Pequeña	2	2
Media	2	2
Grande	4	6

Configuración de CUCM en un sistema de centro de datos múltiple de 250 u 800 usuarios

En esta sección se describe cómo configurar Cisco Unified Communication Manager (CUCM) para un sistema de centro de datos múltiple de 250 u 800 usuarios. Generalmente, cada centro de datos tiene un grupo de CUCM local.

Información necesaria

- Una dirección IP de punto de nivelador de carga para cada centro de datos
- Una dirección IP de punto de aplicación para cada centro de datos
- La cantidad de números de acceso de llamadas entrantes que configurará en su sistema

Procedimiento de configuración

Realice las siguientes acciones:

Tarea	Descripción	Información detallada
1	Revise el perfil de seguridad del enlace troncal de SIP existente y determine si cumple (o no) con el requisito de configuración de su Cisco WebEx Meetings Server. Si no lo cumple, configure dos perfiles de seguridad del enlace troncal de SIP.	Agregue un perfil de seguridad del enlace troncal de SIP a su punto de nivelador de carga y un perfil de seguridad del enlace troncal de SIP a su punto de aplicación. Consulte Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de nivelador de carga, en la página 114 y Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de aplicación, en la página 115.
2	Revise el perfil de SIP existente y determine si cumple (o no) con el requisito de configuración de su Cisco WebEx Meetings Server. Si no lo cumple, configure un perfil de SIP.	Configure un perfil de SIP como se describe en Configuración de un perfil de SIP TLS o Configuración de un perfil de SIP IPv6, en la página 117.
3	Configure dos enlaces troncales de SIP para sus puntos de nivelador de carga.	Consulte Configuración de un enlace troncal de SIP en un punto de nivelador de carga.
4	Configure dos enlaces troncales de SIP para sus puntos de aplicación.	Consulte Configuración de un enlace troncal de SIP para un punto de aplicación.
5	Configure un grupo de ruta utilizando el enlace troncal de SIP que configuró para su punto de nivelador de carga en la tarea 3 anterior.	Consulte Configuración de un grupo de rutas.
6	Configure una lista de rutas utilizando el grupo de rutas que configuró en la tarea 5 anterior.	Consulte Configuración de una lista de rutas.
7	Configure *N* patrones de ruta con la lista de rutas anterior. *N es la cantidad de números de acceso de llamadas entrantes que configuró en su configuración 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 centro de datos múltiple de 2000 usuarios

En esta sección se describe cómo configurar Cisco Unified Communication Manager (CUCM) para un sistema de centro de datos múltiple de 2000. Generalmente, cada centro de datos tiene un grupo de CUCM local.

Información necesaria

- Dos direcciones IP de punto de nivelador de carga para cada centro de datos
- Tres direcciones IP de punto de aplicación para cada centro de datos
- La cantidad de números de acceso de llamadas entrantes que planea configurar en su sistema

Procedimiento de configuración

Realice las siguientes acciones:

Tarea	Descripción	Información detallada
1	Revise el perfil de seguridad del enlace troncal de SIP existente y determine si cumple (o no) con el requisito de configuración de su Cisco WebEx Meetings Server. Si no lo cumple, configure dos perfiles de seguridad del enlace troncal de SIP.	Agregue un perfil de seguridad del enlace troncal de SIP a su punto de nivelador de carga y un perfil de seguridad del enlace troncal de SIP a su punto de aplicación. Consulte Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de nivelador de carga, en la página 114 y Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de aplicación, en la página 115.
2	Revise el perfil de SIP existente y determine si cumple (o no) con el requisito de configuración de su Cisco WebEx Meetings Server. Si no lo cumple, configure un perfil de SIP.	Configure un perfil de SIP como se describe en Configuración de un perfil de SIP TLS o Configuración de un perfil de SIP IPv6, en la página 117.
3	Configure dos enlaces troncales de SIP para sus puntos de nivelador de carga.	Consulte Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de nivelador de carga, en la página 114.
4	Configure cuatro enlaces troncales de SIP para sus puntos de aplicación.	Consulte Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de aplicación, en la página 115.
5	Configure un grupo de ruta utilizando el enlace troncal de SIP que configuró para su punto de nivelador de carga en la tarea 3 anterior.	Consulte Configuración de un grupo de rutas, en la página 123.
6	Configure una lista de rutas utilizando el grupo de ruta que configuró en la tarea 5 anterior.	Consulte Configuración de una lista de rutas, en la página 124.
7	Configure *N* patrones de ruta con la lista de rutas anterior. *N es la cantidad de números de acceso de llamadas entrantes que configuró en su configuración de audio en el sitio de administración.*	Consulte Configuración de un patrón de ruta, en la página 125.
8	Configure cuatro patrones de ruta SIP para sus puntos de aplicación.	Consulte Configuración de un patrón de ruta SIP, en la página 125.

Configuración de CUCM para sistemas de alta disponibilidad y sin alta disponibilidad

Las siguientes secciones proporcionan información sobre las tareas que se requieren para configurar los sistemas de alta disponibilidad y sin alta disponibilidad de distintos tamaños.

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

Esta sección describe la información necesaria y las instrucciones detalladas sobre cómo configurar CUCM para sistemas de 50, 250 y 800 usuarios sin alta disponibilidad.

Información necesaria

- Una dirección IP del punto de nivelador de carga
- Una dirección IP del punto de aplicación
- La cantidad de números de acceso de llamadas entrantes que configurará en su sistema

Procedimiento de configuración

Realice las siguientes acciones:

Tarea	Descripción	Información detallada
1	Revise el perfil de seguridad del enlace troncal de SIP existente y determine si cumple (o no) con el requisito de configuración de su Cisco WebEx Meetings Server. Si no lo cumple, configure dos perfiles de seguridad del enlace troncal de SIP.	Agregue un perfil de seguridad del enlace troncal de SIP a su punto de nivelador de carga y un perfil de seguridad del enlace troncal de SIP a su punto de aplicación. Consulte Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de nivelador de carga, en la página 114 y Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de aplicación, en la página 115.
2	Revise el perfil de SIP existente y determine si cumple (o no) con el requisito de configuración de su Cisco WebEx Meetings Server. Si no lo cumple, configure un perfil de SIP.	Configure un perfil de SIP como se describe en Configuración de un perfil de SIP TLS o Configuración de un perfil de SIP IPv6, en la página 117.
3	Configure un enlace troncal de SIP para su punto de nivelador de carga.	Consulte Configuración de un enlace troncal de SIP en un punto de nivelador de carga.
4	Configure un enlace troncal de SIP para su punto de aplicación.	Consulte Configuración de un enlace troncal de SIP para un punto de aplicación.
5	Configure un grupo de ruta utilizando el enlace troncal de SIP que configuró para su punto de nivelador de carga en la tarea 3 anterior.	Consulte Configuración de un grupo de rutas.
6	Configure una lista de rutas utilizando el grupo de ruta que configuró en la tarea 5 anterior.	Consulte Configuración de una lista de rutas.
7	Configure *N* patrones de ruta con la lista de rutas anterior. *N es la cantidad de números de acceso de llamadas entrantes que configuró en su configuración de audio en el sitio de administración.*	Consulte Configuración de un patrón de ruta.

Tarea	Descripción	Información detallada
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

Esta sección describe la información necesaria y las instrucciones detalladas sobre cómo configurar CUCM para sistemas de 50, 250 u 800 usuarios con alta disponibilidad.

Información necesaria

- Dos direcciones IP del punto de nivelador de carga
- Dos direcciones IP del punto de aplicación
- La cantidad de números de acceso de llamadas entrantes que configurará en su sistema

Procedimiento de configuración

Realice las siguientes acciones:

Tarea	Descripción	Información detallada
1	Revise el perfil de seguridad del enlace troncal de SIP existente y determine si cumple (o no) con el requisito de configuración de su Cisco WebEx Meetings Server. Si no lo cumple, configure dos perfiles de seguridad del enlace troncal de SIP.	Agregue un perfil de seguridad del enlace troncal de SIP a su punto de nivelador de carga y un perfil de seguridad del enlace troncal de SIP a su punto de aplicación. Consulte Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de nivelador de carga, en la página 114 y Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de aplicación, en la página 115.
2	Revise el perfil de SIP existente y determine si cumple (o no) con el requisito de configuración de su Cisco WebEx Meetings Server. Si no lo cumple, configure un perfil de SIP.	Configure un perfil de SIP como se describe en Configuración de un perfil de SIP TLS o Configuración de un perfil de SIP IPv6, en la página 117.
3	Configure dos enlaces troncales de SIP para sus puntos de nivelador de carga.	Consulte Configuración de un enlace troncal de SIP en un punto de nivelador de carga.
4	Configure dos enlaces troncales de SIP para sus puntos de aplicación.	Consulte Configuración de un enlace troncal de SIP para un punto de aplicación.
5	Configure un grupo de ruta utilizando el enlace troncal de SIP que configuró para su punto de nivelador de carga en la tarea 3 anterior.	Consulte Configuración de un grupo de rutas.
6	Configure una lista de rutas utilizando el grupo de rutas que configuró en la tarea 5 anterior.	Consulte Configuración de una lista de rutas.

Tarea	Descripción	Información detallada
7	Configure *N* patrones de ruta con la lista de rutas anterior. *N es la cantidad de números de acceso de llamadas entrantes que configuró en su configuración 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 sin alta disponibilidad

En esta sección se describe cómo configurar Cisco Unified Communication Manager (CUCM) para un sistema de 2000 usuarios sin alta disponibilidad.

Información necesaria

- Dos direcciones IP del punto de nivelador de carga
- Tres direcciones IP de punto de aplicación
- La cantidad de números de acceso de llamadas entrantes que configurará en su sistema

Procedimiento de configuración

Realice las siguientes acciones:

Tarea	Descripción	Información detallada
1	Revise el perfil de seguridad del enlace troncal de SIP existente y determine si cumple (o no) con el requisito de configuración de su Cisco WebEx Meetings Server. Si no lo cumple, configure dos perfiles de seguridad del enlace troncal de SIP.	Agregue un perfil de seguridad del enlace troncal de SIP a su punto de nivelador de carga y un perfil de seguridad del enlace troncal de SIP a su punto de aplicación. Consulte Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de nivelador de carga, en la página 114 y Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de aplicación, en la página 115.
2	Revise el perfil de SIP existente y determine si cumple (o no) con el requisito de configuración de su Cisco WebEx Meetings Server. Si no lo cumple, configure un perfil de SIP.	Configure un perfil de SIP como se describe en Configuración de un perfil de SIP TLS o Configuración de un perfil de SIP IPv6, en la página 117.
3	Configure dos enlaces troncales de SIP para sus puntos de nivelador de carga.	Consulte Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de nivelador de carga, en la página 114.
4	Configure tres enlaces troncales de SIP para sus puntos de aplicación.	Consulte Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de aplicación, en la página 115.

Tarea	Descripción	Información detallada
5	Configure un grupo de ruta utilizando el enlace troncal de SIP que configuró para su punto de nivelador de carga en la tarea 3 anterior.	Consulte Configuración de un grupo de rutas, en la página 123.
6	Configure una lista de rutas utilizando el grupo de ruta que configuró en la tarea 5 anterior.	Consulte Configuración de una lista de rutas, en la página 124.
7	Configure *N* patrones de ruta con la lista de rutas anterior. *N es la cantidad de números de acceso de llamadas entrantes que configuró en su configuración de audio en el sitio de administración.*	Consulte Configuración de un patrón de ruta, en la página 125.
8	Configure tres patrones de ruta SIP para sus puntos de aplicación.	Consulte Configuración de un patrón de ruta SIP, en la página 125.

Configuración de CUCM en un sistema de 2000 usuarios con alta disponibilidad

En esta sección se describe cómo configurar Cisco Unified Communication Manager (CUCM) para un sistema de 2000 usuarios con alta disponibilidad.

Información necesaria

- Dos direcciones IP del punto de nivelador de carga
- Cuatro direcciones IP de punto de aplicación
- La cantidad de números de acceso de llamadas entrantes que configurará en su sistema

Procedimiento de configuración

Realice las siguientes acciones:

Tarea	Descripción	Información detallada
1	Revise el perfil de seguridad del enlace troncal de SIP existente y determine si cumple (o no) con el requisito de configuración de su Cisco WebEx Meetings Server. Si no lo cumple, configure dos perfiles de seguridad del enlace troncal de SIP.	Agregue un perfil de seguridad del enlace troncal de SIP a su punto de nivelador de carga y un perfil de seguridad del enlace troncal de SIP a su punto de aplicación. Consulte Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de nivelador de carga, en la página 114 y Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de aplicación, en la página 115.
2	Revise el perfil de SIP existente y determine si cumple (o no) con el requisito de configuración de su Cisco WebEx Meetings Server. Si no lo cumple, configure un perfil de SIP.	Configure un perfil de SIP como se describe en Configuración de un perfil de SIP TLS o Configuración de un perfil de SIP IPv6, en la página 117.

Tarea	Descripción	Información detallada
3	Configure dos enlaces troncales de SIP para sus puntos de nivelador de carga.	Consulte Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de nivelador de carga, en la página 114.
4	Configure cuatro enlaces troncales de SIP para sus puntos de aplicación.	Consulte Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de aplicación, en la página 115.
5	Configure un grupo de ruta utilizando el enlace troncal de SIP que configuró para su punto de nivelador de carga en la tarea 3 anterior.	Consulte Configuración de un grupo de rutas, en la página 123.
6	Configure una lista de rutas utilizando el grupo de ruta que configuró en la tarea 5 anterior.	Consulte Configuración de una lista de rutas, en la página 124.
7	Configure *N* patrones de ruta con la lista de rutas anterior. *N es la cantidad de números de acceso de llamadas entrantes que configuró en su configuración de audio en el sitio de administración.*	Consulte Configuración de un patrón de ruta, en la página 125.
8	Configure cuatro patrones de ruta SIP para sus puntos de aplicación.	Consulte Configuración de un patrón de ruta SIP, en la página 125.

Configuración de un perfil de seguridad del enlace troncal de SIP

Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de nivelador de carga

Antes de comenzar

Si su sistema de Cisco WebEx Meetings Server está configurado para TLS, debe importar un certificado de teleconferencia segura. Para obtener más información, consulte la sección "Importación de certificados de

teleconferencia segura" en 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 de dominio totalmente calificado 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 del enlace troncal de SIP**.

Paso 4 Seleccione **Añadir nuevo**.

Paso 5 Configure los siguientes campos.

- Nombre: introduzca un nombre para identificar su perfil de seguridad del enlace troncal de SIP.
- Modo de seguridad del dispositivo: seleccione **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 del sujeto X.509: introduzca su nombre de 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 de Cisco WebEx Meetings Server diferente no puede compartir el mismo perfil de seguridad del enlace troncal de SIP, ya que cada sistema debe tener un certificado diferente. Obtenga el nombre de certificado de Cisco WebEx Meetings Server en el sitio de administración. Para obtener más información, consulte la sección “Administración de certificados” en la *Guía de administración*.
- Puerto entrante: 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 campo en la página; deje los valores predeterminados.

Paso 6 Seleccione **Guardar**.

Configuración de un perfil de seguridad del enlace troncal de SIP para un punto de aplicación

Antes de comenzar

Si su sistema de Cisco WebEx Meetings Server está configurado para TLS, debe importar un certificado de teleconferencia segura. Para obtener más información, consulte la sección "Importación de certificados de

teleconferencia segura" en 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 de dominio totalmente calificado 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 del enlace troncal de SIP**.

Paso 4 Seleccione **Añadir nuevo**.

Paso 5 Configure los siguientes campos:

- Nombre: introduzca un nombre para identificar su perfil de seguridad del enlace troncal de SIP.
- Modo de seguridad del dispositivo: seleccione **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 del sujeto X.509: introduzca su nombre de 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 de Cisco WebEx Meetings Server diferente no puede compartir el mismo perfil de seguridad del enlace troncal de SIP, ya que cada sistema debe tener un certificado diferente. Obtenga el nombre de certificado de Cisco WebEx Meetings Server en el sitio de administración. Para obtener más información, consulte la sección “Administración de certificados” en la *Guía de administración*.
- Puerto entrante: 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 campo en la página; deje los valores predeterminados.

Paso 6 Seleccione **Guardar**.

Configuración de un perfil de SIP

Configuración de un perfil de SIP estándar

El perfil del Protocolo de iniciación de sesiones (SIP) estándar usa la configuración predeterminada y no requiere pasos de configuración adicionales.

Configuración de un perfil de SIP TLS

Paso 1 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre de dominio totalmente calificado 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 de SIP**.

Paso 4 Seleccione **Añadir nuevo**.

Paso 5 Configure los siguientes campos:

- Nombre: introduzca un nombre para su perfil de SIP.
- Redireccionar por aplicación: seleccione la casilla de verificación.

No configure ningún otro campo en esta página; deje los campos con sus valores predeterminados.

Paso 6 Seleccione **Guardar**.

Configuración de un perfil de SIP IPv6

Paso 1 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre de dominio totalmente calificado 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 de SIP**.

Paso 4 Seleccione **Añadir nuevo**.

Paso 5 Configure los siguientes campos:

- Nombre: introduzca un nombre para su perfil de SIP.
- Habilitar ENAT: seleccione la casilla de verificación.

No configure ningún otro campo en esta página; deje los campos con sus valores predeterminados.

Paso 6 Seleccione **Guardar**.

Administración de certificados de CUCM mediante TLS

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

- Obtenga un certificado CWMS del sitio de administración y cárguelo en el CUCM.

Nota Si CWMS utiliza certificados de terceros, todos los certificados de la cadena de certificados se deben cargar en CUCM.

- Descargue su certificado de CUCM y, luego, cárguelo en el sitio de administración de CWMS.

Nota Si CUCM utiliza certificados de terceros, solo el último certificado de la cadena de certificados (certificado raíz de la autoridad de certificación [CA]) se debe cargar en CWMS.

Si usa TLS para conectar todos los centros de datos en un sistema de centro de datos múltiple (MDC) al mismo CUCM, CWMS no puede usar la URL del sitio común para el nombre común de certificado. Debe usar cada URL del sitio local del centro de datos para cada nombre común de certificado, dado que CUCM 10.5 y las versiones más antiguas tratan los certificados múltiples con un nombre común como el mismo certificado. Si los nombres no son diferentes, el segundo certificado de centro de datos reemplaza al primer certificado de centro de datos tras cargar el segundo certificado de centro de datos en CUCM.

Consulte "Administrar 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.

Carga de 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 de la sección Certificado SSL.
d) Seleccione **Más opciones** > **Exportar el certificado SSL**.
e) Guarde su certificado en su disco duro local.

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

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

Paso 4 Seleccione **Seguridad** > **Administrar certificados**.

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

Paso 6 Seleccione **CallManager-confianza** en el menú desplegable Nombre del certificado.

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

Paso 8 Seleccione **Cargar archivo**.

El sistema muestra el mensaje "Éxito: certificado cargado".

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

Paso 10 Seleccione **Cerrar**.

Qué hacer a continuación

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

Instalación de un certificado de CUCM de terceros

Este procedimiento explica cómo cargar un certificado de terceros en su Cisco WebEx Meetings Server.

Antes de comenzar

- Genere una solicitud de firma de certificado (Certificate Signing Request, CSR) y envíela a una autoridad de certificados de terceros para solicitar certificados. Consulte Generar una Solicitud de firma de certificado (CSR) para obtener instrucciones.
- La autoridad de certificados le enviará una cadena de certificados que puede contener lo siguiente:
  - Certificado 1 (usuario final): lo emite una autoridad de certificados intermedia a una entidad de usuarios finales.
  - Certificado 2 (intermedio): lo emite una autoridad de certificados raíz a una autoridad de certificados intermedia.
  - Certificado 3 (autoridad de certificados raíz): lo emite la autoridad de certificados raíz.
- Cuando recibe diversos certificados en una cadena de certificados, debe concatenar los tres certificados en un archivo; el certificado de usuarios finales primero.

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

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

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

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

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

Paso 6 Seleccione **CallManager-confianza** en el menú desplegable Nombre del certificado.

Paso 7 Seleccione el botón **Examinar** y el certificado de la autoridad de certificados (Certificate Authority, CA) raíz que guardó en su disco duro local.
Este es el último certificado de firma automática de la cadena de verificación, que se utiliza para comprobar el certificado CallManager.pem.

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

Paso 8 Seleccione **Cargar archivo**.
Espere a que el sistema indique "Éxito: certificado cargado".

Paso 9 Seleccione **Cerrar**.

Qué hacer a continuación

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

Descarga de certificados de CUCM

Este procedimiento es necesario solo si CUCM usa certificados de firma automática. Si CUCM usa certificados de terceros, debe cargar solo el último certificado (el certificado de la CA raíz) en la cadena de certificados en su Cisco WebEx Meeting Server. Comuníquese con su autoridad de certificados (CA) para obtener información sobre cómo obtener un certificado raíz de la CA.

Consulte su documentación de CUCM para obtener más información sobre la generación de certificados de CUCM.

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

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

Paso 3 Seleccione **Seguridad** > **Administrar certificados**.

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

Paso 5 Seleccione **Descargar** para guardar el certificado de 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 "Administrar certificados" en la *Guía de administración*. Consulte http://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.html.

Configuración de un enlace troncal de SIP

Configuración de un enlace troncal de SIP en un punto de nivelador de carga

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

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

Paso 3 Seleccione **Dispositivo** > **Enlace troncal**.

Paso 4 Seleccione **Añadir nuevo**.

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

Nota No cambie ninguno de los otros campos en esta página. Conserve las configuraciones predeterminadas.

Nota Deje anulada la casilla **Punto de terminación de medios requerido** en la página **Configuración de enlace troncal** cuando CUCM se esté comunicando con Cisco WebEx Meeting Server. Si no está utilizando Cisco WebEx Meetings Server con el audio de SIP de CUCM, puede seleccionar la casilla de verificación **Punto de terminación de medios requerido** cuando provea servicios de telefonía utilizando una infraestructura PBX de terceros.

Paso 6 Seleccione **Siguiente**.

Paso 7 Configure los siguientes campos:

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

  Para determinar qué grupo de Cisco Unified Communications Manager se ha configurado en ese grupo de dispositivos, seleccione**Sistema** > **menú Grupo de dispositivos**. Para comprobar cuáles de los Cisco Unified Communications Managers son parte de este grupo, seleccione **Sistema** > **Grupo Cisco Unified CM**.

  Nota Registre las direcciones IP del servidor primario y secundario. Introducirá estas direcciones IP al configurar los ajustes de audio en Cisco WebEx Meetings Server. Consulte "Configurar los parámetros de audio por primera vez" en la *Guía de administración* para obtener más detalles. Consulte Guías de instalación y mejora de Cisco WebEx Meetings Server.
- Dirección de destino: introduzca la dirección IPv4 de su punto de nivelador de carga. Consulte la tabla Configuración de SIP en la página Audio del sitio de administración para ver la dirección IP.
- Dirección IPv6 de destino: introduzca la dirección IPv6 de su punto de nivelador 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 del enlace troncal de SIP: seleccione el perfil de seguridad de su punto de nivelador de carga del 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 habilitar 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 telefónicos y dirigir los patrones configurados en CUCM a los que desea que llame Cisco WebEx Meetings Server. Seleccione **Enrutamiento de llamadas** > **Clase de control** > **Espacio de búsqueda de llamadas**. Un espacio de búsqueda de llamadas se compone de una lista ordenada de particiones de ruta que suelen asignarse a dispositivos o patrones de ruta. Los espacios de búsqueda de llamadas determinan las particiones que buscan los dispositivos que llaman cuando intentan completar una llamada. Para obtener más información, consulte "Configuración del espacio de búsqueda de llamadas" en la *Guía de administración de Cisco Unified Communications Manager* o "Particiones y espacios de búsqueda de llamadas" en la *Guía del sistema de Cisco Unified Communications Manager*.
- Espacio de búsqueda de llamadas para volver a enrutar: seleccione el Espacio de búsqueda de llamadas que contenga la partición de ruta configurada para el patrón de ruta SIP de la siguiente sección, "Configuración de un patrón de ruta SIP". Si está establecido en **< None >**, solo podrá enrutar llamadas a patrones de ruta con una partición de ruta establecida en **< None >**, de manera que el patrón de ruta SIP deberá tener la partición de ruta establecida en **< None >**. Esta configuración es necesaria para ingresar a reuniones en Cisco WebEx Meetings Server. Para obtener más información, consulte "Configuración del espacio de búsqueda de llamadas" en la *Guía de administración de Cisco Unified Communications Manager* o "Particiones y espacios de búsqueda de llamadas" en la *Guía del sistema de Cisco Unified Communications Manager* para obtener más detalles.

Nota No cambie ninguno de los otros campos en esta página. Conserve las configuraciones predeterminadas.

Paso 8 Seleccione **Guardar**.

Paso 9 Seleccione **Restablecer** y seleccione **Restablecer y reiniciar** en la ventana emergente.
Debe restablecer el enlace troncal de SIP para finalizar la configuración.

Configuración de un enlace troncal de SIP para un punto de aplicación

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

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

Paso 3 Seleccione **Dispositivo** > **Enlace troncal**.

Paso 4 Seleccione **Añadir nuevo**.

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

Nota No cambie ningún otro campo en esta página; deje los valores en la configuración predeterminada.

Paso 6 Seleccione **Siguiente**.

Paso 7 Configure los siguientes campos:

- Nombre de dispositivo: introduzca un nombre para su enlace troncal de SIP.
- Grupo de dispositivos: seleccione **Predeterminado** del menú desplegable.
- Dirección de destino: introduzca la dirección IPv4 del servidor de aplicaciones.
- Dirección IPv6 de destino: introduzca la dirección IPv6 de su servidor de aplicaciones 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 del enlace troncal de SIP: seleccione el perfil de seguridad de su servidor de aplicaciones del 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 habilitar 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 telefónicos y dirigir los patrones configurados en CUCM a los que desea permitir que Cisco WebEx Meetings Server llame. Seleccione **Enrutamiento de llamadas** > **Clase de control** > **Espacio de búsqueda de llamadas**. Un espacio de búsqueda de llamadas se compone de una lista ordenada de particiones de ruta que suelen asignarse a dispositivos o patrones de ruta. Los espacios de búsqueda de llamadas determinan las particiones que buscan los dispositivos que llaman cuando intentan completar una llamada. Si está establecido en **< None >**, solo podrá llamar a dispositivos o a patrones de ruta con un valor de partición establecido en **< None >**. Para obtener más información, consulte *Configuración del espacio de búsqueda de llamadas* en la *Guía de administración de Cisco Unified Communications Manager* o *Particiones y espacios de búsqueda de llamadas* en la *Guía del sistema de Cisco Unified Communications Manager*.

Nota No cambie ningún otro campo en esta página; deje los valores en la configuración predeterminada.

Nota Deje anulada la casilla **Punto de terminación de medios requerido** en la página **Configuración de enlace troncal** cuando CUCM se esté comunicando con Cisco WebEx Meeting Server. Si no está utilizando Cisco WebEx Meetings Server con el audio de SIP de CUCM, puede seleccionar la casilla de verificación **Punto de terminación de medios requerido** cuando provea servicios de telefonía utilizando una infraestructura PBX de terceros.

Paso 8 Seleccione **Guardar**.

Paso 9 Seleccione **Restablecer** y seleccione **Restablecer y reiniciar** en la ventana emergente.
Debe restablecer el enlace troncal de 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 de dominio totalmente calificado 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 **Añadir nuevo**.

Paso 5 Configure los siguientes campos

- Nombre del grupo de rutas: introduzca un nombre para su grupo de rutas.
- Algoritmo de distribución. Seleccione **Circular** en el menú desplegable.

Nota Seleccione **Circular** para permitir que CUCM distribuya una llamada a usuarios inactivos o disponibles, comenzando desde el miembro número (N+1) de un grupo de rutas, donde el miembro N es el miembro al que CUCM envió recientemente una llamada. Si el miembro N es el último miembro de un grupo de rutas, CUCM distribuye una llamada comenzando desde el principio del grupo de rutas.

- Encontrar dispositivos para agregar al grupo de rutas: seleccione **Enlace troncal de SIP del punto de nivelador de carga** en la lista de dispositivos disponibles. Seleccione **Agregar al grupo de rutas**.

Nota No cambie ninguno de los otros campos en esta página. Conserve las configuraciones predeterminadas.

Paso 6 Seleccione **Guardar**.

Qué hacer a continuación

Cree una lista de rutas para su grupo de rutas. Continúe con Configuración de una lista de rutas, en la página 124.

Configuración de una lista de rutas

Paso 1 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre de dominio totalmente calificado 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 **Añadir 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 campos con la configuración predeterminada.

Paso 6 Seleccione **Guardar**.

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

Paso 8 Seleccione el grupo de rutas configurado anteriormente del menú desplegable **Grupo de rutas** y seleccione **Guardar**.
Aparecerá la página **Configuración de la lista de rutas**.

Paso 9 Seleccione **Guardar**.

Qué hacer a continuación

Configure un patrón de ruta para su lista de rutas. Continúe con Configuración de un patrón de ruta, en la página 125.

Configuración de un patrón de ruta

Paso 1 Inicie sesión en http://ccm-server/, donde *ccm-server* es el nombre de dominio totalmente calificado 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 **Añadir nuevo**.

Paso 5 Configure los siguientes campos

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

  Nota Agregue un patrón de ruta para cada grupo de Marcado grupal. Registre este nombre ya que deberá ingresarlo en la página Administración **Configuración** > **Audio** > **Grupo de marcado grupal** cuando cree un grupo de marcado grupal.

- Partición de ruta: seleccione una partición de ruta que sea accesible para los teléfonos o dispositivos que puedan llamar a Cisco WebEx Meetings Server. Si está establecida en **< None >**, cualquier dispositivo configurado en CUCM podrá llamar a Cisco WebEx Meetings Server. Para obtener más información, consulte "Configuración del espacio de búsqueda de llamadas" en la *Guía de administración de Cisco Unified Communications Manager* o "Particiones y espacios de búsqueda de llamadas" en la *Guía del sistema de Cisco Unified Communications Manager*.
- Puerta de enlace/Lista de rutas: seleccione la lista de rutas configurada anteriormente del menú desplegable.

Nota No cambie ningún otro campo en esta página; deje estos campos con la configuración predeterminada.

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 de dominio totalmente calificado 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 SIP**.

Paso 4 Seleccione **Añadir 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 el Espacio de búsqueda de llamadas para volver a enrutar en la sección "Configuración de un enlace troncal de SIP para un punto de aplicación" más arriba. Si está establecida en **< None >**, el Espacio de búsqueda de llamadas para volver a enrutar para el enlace troncal de SIP para un punto de aplicación debe estar establecido en **< None >**. Para obtener más información, consulte "Configuración del espacio de búsqueda de

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

- Uso de patrón: seleccione **Enrutamiento de dirección IP**.
- Patrón IPv4: introduzca la dirección IP del punto de aplicación. Consulte la tabla Configuración de SIP en la página Audio del sitio de administración para ver la dirección IP.
- Enlace troncal de SIP: seleccione el enlace troncal de SIP configurado anteriormente para el punto de aplicación del menú desplegable.

Nota No cambie ningún otro campo en esta página; deje estos campos con la configuración predeterminada.

Paso 6 Seleccione **Guardar**.

Compatibilidad y soporte de las características de CUCM

Compatibilidad de las características de CUCM

Cisco WebEx Meetings Server (CWMS) es compatible con Cisco Unified Call Manager (CUCM) 9.1, 10.0 y 10.5.

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

Debe mejorar CUCM a una versión posterior que admita este algoritmo de firma o debe obtener un certificado de terceros firmado con SHA1 con cifrado RSA. Sin embargo, según lo que recomienda el Instituto Nacional de Normas y Tecnología (NIST), SHA1 ya no debe usarse para la generación de firmas digitales, dado que esto es una vulnerabilidad para la seguridad.

La siguiente tabla proporciona la compatibilidad de las características para las versiones compatibles de CUCM. La capacidad del sistema de Cisco WebEx Meetings Server no se ve afectada por ninguna de sus opciones de configuración.

Nota CWMS no es compatible con ninguna versión de CUCM no listada ni con otras aplicaciones de administración de proxy SIP de terceros.

Característica	CUCM 9.1	CUCM 10.0	CUCM 10.5	Condiciones previas/Comentarios
Llamada saliente (IPv6)	Sí	Sí	Sí	Configure su sistema CWMS con direcciones IPv6 durante el proceso de instalación.

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

Característica	CUCM 9.1	CUCM 10.0	CUCM 10.5	Condiciones previas/Comentarios
TLS	Sí	Sí	Sí	Asegúrese de que los puertos predeterminados sean los siguientes: 5061 para puntos de nivelador de carga de conferencia; 5063 para puntos de aplicación de conferencia.
UDP	Sí	Sí	Sí	Asegúrese de que los puertos predeterminados sean los siguientes: 5060 para puntos de nivelador de carga de conferencia; 5062 para puntos de aplicación de conferencia.
Certificados de firma automática	Sí	Sí	Sí	No disponible
Certificados de terceros	Sí	Sí	Sí	No disponible

Características de las llamadas telefónicas

Cisco WebEx Meetings Server es compatible con las siguientes características de las llamadas de CUCM.

Nota Cisco WebEx Meetings Server también admite el software de CUCM 9.0 que es parte del producto BE6K (Business Edition 6000).

Característica	CUCM 9.1	CUCM 10.0	CUCM 10.5
Llamada en espera	Sí	Sí	Sí
Llamada no en espera	Sí	Sí	Sí
Visualización del identificador de llamada en EP	Sí	Sí	Sí
Visualización del nombre del autor de la llamada en EP	Sí	Sí	Sí

Característica	CUCM 9.1	CUCM 10.0	CUCM 10.5
Transferencia de llamada (IPv4 a IPv4)	Sí	Sí	Sí
Transferencia de llamada (IPv6 a IPv4)	Sí	Sí	Sí
Transferencia de llamada (IPv4 a IPv6)	Sí	Sí	Sí
Transferencia de llamada (IPv6 a IPv6)	Sí	Sí	Sí

Características telefónicas multimedia

CWMS es compatible con los participantes con códecs G.711/G.722/G.729 al mismo tiempo. El cambio de configuración de su códec no afecta el rendimiento del sistema.

Característica	G.711	G.722	G.729
Compresión de ruido	Sí	Sí	Sí
Ruido reconfortante	Sí	No	No
Cancelación del eco	No	No	No
Encubrimiento de pérdida del paquete	Sí	Sí	No
Control de obtención automática	Sí	Sí	Sí
Calidad de servicio	Sí	Sí	Sí

Compatibilidad del extremo de audio

Puede utilizar cualquier extremo de audio basado en estándares que se conecte a Cisco Unified Communications Manager para entrar a una reunión de WebEx. Los extremos de audio compatibles incluyen los teléfonos IP de Cisco, los extremos de TelePresence y los dispositivos PSTN, como teléfonos móviles y teléfonos fijos. Muchos extremos de audio admiten conectividad de audio y vídeo. Sin embargo, solo se admite la conectividad de audio con Cisco WebEx Meetings Server.

Para permitir a los usuarios fuera de la organización entrar a las reuniones de WebEx a través de dispositivos PSTN, su empresa debe implementar puertas de enlace de análogas a VoIP, como los enrutadores de servicios integrados (ISR) de Cisco.

Para obtener una lista de los teléfonos IP de Cisco Unified compatibles con Cisco Unified Communications Manager y los paquetes de dispositivos disponibles para cada modelo, consulte Matriz de compatibilidad de paquetes de dispositivos de Cisco Unified Communications Manager y la característica de teléfonos IP de Cisco Unified.

CAPÍTULO 7

Descarga e implementación masiva de aplicaciones

El uso de este producto requiere aplicaciones adicionales que se deben descargar de las computadoras de los usuarios.

- Acerca de las descargas de aplicaciones, página 131
- Descarga de aplicaciones desde el sitio de administración, página 133
- Contenido de los archivos ZIP de las aplicaciones, página 134
- Implementación masiva de las herramientas de productividad de Cisco WebEx, página 136
- Implementación masiva de la aplicación de reuniones, página 145
- Implementación masiva del reproductor de grabaciones basadas en red, página 150
- Reconfiguración de los parámetros después de realizar una actualización, página 154

Acerca de las descargas de aplicaciones

Puede implementar de manera masiva las aplicaciones de CWMS mediante las herramientas disponibles en el sitio de administración. Las aplicaciones disponibles para descargar incluyen las siguientes:

- Aplicación WebEx Meetings

  Nota No se admite la ejecución de la aplicación WebEx Meetings en un sistema operativo virtualizado.

- Herramientas de productividad de WebEx

  Después de una actualización o una mejora de un sistema, los usuarios deben desinstalar las versiones anteriores de las herramientas de productividad de WebEx. Después de la actualización o la mejora, puede usar el sitio de administración para arrastrar las herramientas de productividad de WebEx a sus usuarios o puede solicitar a sus usuarios que las descarguen de la página **Descargas** del usuario final.

- Reproductor de grabaciones basadas en red de WebEx

Puede usar el sitio de administración para permitir que los usuarios descarguen las aplicaciones ellos mismos, para arrastrar las aplicaciones a las computadoras de los usuarios, o para descargar los archivos de instalación y solicitar a los usuarios que instalen las aplicaciones manualmente ellos mismos.

Puede adquirir los programas de instalación .MSI para cada uno desde la página **Administración** > **Configuración** > **Descargas**. Consulte Descarga de aplicaciones desde el sitio de administración para obtener más información.

Si los usuarios tienen privilegios de administrador en sus computadoras, puede distribuir las aplicaciones mediante descargas automáticas, mediante la descarga e instalación habilitada por el usuario o arrastrando las aplicaciones a las computadoras de los usuarios. Si su empresa no otorga privilegios de administrador a los usuarios, debe utilizar un enfoque alternativo para instalar las aplicaciones en sus computadoras.

Le recomendamos que arrastre las aplicaciones a las computadoras de los usuarios fuera de línea, antes de informarles a dichos usuarios finales que se han creado cuentas para ellos. Esto garantiza que los usuarios puedan iniciar reuniones y entrar a ellas, y reproducir grabaciones de red la primera vez que inician sesión.

Si un usuario no tiene las aplicaciones instaladas, la primera vez que entre a una reunión, la aplicación WebEx Meetings se descarga en la PC. Esto puede configurarse para que se realice bajo demanda o de modo silencioso. El usuario tiene la opción de usar la aplicación Cisco WebEx Meetings el tiempo que dure la reunión y eliminarla cuando la reunión finalice, o ejecutar una instalación de la aplicación para acelerar el proceso de iniciar o entrar a las reuniones futuras. Esto podría fallar si el usuario no tiene privilegios de administrador.

En las PC donde los usuarios no tienen privilegios de administrador, los usuarios pueden descargar e instalar la aplicación Cisco WebEx Meetings, las herramientas de productividad y el reproductor de grabaciones basadas en red desde las páginas de descarga del usuario final. No es necesaria ninguna acción adicional del administrador.

Al **realizar una mejora** a la versión Cisco WebEx Meetings Server 1.5MR3 o a una versión posterior en un entorno bloqueado donde las PC de los usuarios no tienen privilegios de administrador, antes de iniciar el procedimiento de mejora, arrastre la nueva versión de la aplicación WebEx Meetings a todas las PC de los usuarios. Tener las versiones nuevas y las versiones anteriores de la aplicación Meetings almacenadas en las PC de los usuarios les permite asistir a las reuniones organizadas por los usuarios que ejecutan la última versión o las versiones anteriores de la aplicación Meetings. Los usuarios pueden tener varias versiones de la aplicación WebEx Meetings almacenadas en sus PC siempre que los archivos estén almacenados en las carpetas correctas.

Nota En el caso de los sitios que tienen implementadas la versión Cisco WebEx Meetings Server 1.5 MR3 (compilación 1.5.1.386) o una versión anterior y usan los servicios de reuniones de WebEx basados en la nube, desinstale la aplicación Meetings para WebEx Meetings Server y los servicios de reuniones de WebEx y, luego, vuelva a instalar la aplicación Meetings en las carpetas correctas en las PC de los usuarios. De lo contrario, los usuarios no podrán entrar a las reuniones organizadas por los usuarios de WebEx basados en la nube. Consulte "Los usuarios con PC sin privilegios de administrador no pueden entrar a las reuniones organizadas por los usuarios de WebEx basados en la nube" en la *Guía de solución de problemas de Cisco WebEx Meeting Server* para obtener más detalles.

Descarga de aplicaciones desde el sitio de administración

Puede configurar su sistema para que los administradores puedan descargar manualmente aplicaciones de escritorio de Cisco WebEx a los usuarios o puede permitir a los usuarios realizar sus propias descargas.

Paso 1 inicie sesión en el sitio de administración.

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

Paso 3 Seleccione la casilla de verificación **Actualización automática de las herramientas de productividad de WebEx** para configurar las actualizaciones periódicas automáticas. (**Predeterminado**: Activado).

Paso 4 Seleccione su método de descarga:

- Permitir que los usuarios descarguen aplicaciones de escritorio de WebEx
- Arrastrar manualmente las aplicaciones de escritorio de WebEx al escritorio del usuario

Si selecciona **Permitir que los usuarios descarguen aplicaciones de escritorio de WebEx**, puede seleccionar **Guardar** para finalizar la configuración de descarga. No es necesario tomar acciones adicionales. Si selecciona **Arrastrar manualmente las aplicaciones de escritorio de WebEx al escritorio del usuario**, proceda al siguiente paso.

Utilice la opción **Arrastrar manualmente las aplicaciones de escritorio de WebEx al escritorio del usuario** para habilitar las conferencias para los usuarios que no tienen permisos de administrador.

Si selecciona **Arrastrar manualmente las aplicaciones de escritorio de WebEx al escritorio del usuario**, aparecerán las secciones de Cisco WebEx Meetings, Herramientas de productividad y Reproductor de grabaciones basadas en red en la página.

Paso 5 En la sección WebEx Meetings, seleccione **Descargar** y **Guardar** para guardar el archivo ZIP en su sistema.
Abra el archivo ZIP y seleccione el programa de instalación para su plataforma e idioma, y extráigalo en un directorio. El archivo ZIP contiene los programas de instalación MSI para la plataforma de Windows en todos los idiomas disponibles. Para implementar el programa de instalación, consulte Implementación masiva de la aplicación de reuniones, en la página 145.

Paso 6 En la sección Herramientas de productividad, seleccione **Descargar** y **Guardar** para guardar el archivo ZIP en su sistema.
Abra el archivo ZIP y seleccione el programa de instalación para su plataforma e idioma, y extráigalo en un directorio. El archivo ZIP contiene los programas de instalación MSI para la plataforma de Windows en todos los idiomas disponibles. Para implementar el programa de instalación, consulte Implementación masiva de las herramientas de productividad de Cisco WebEx, en la página 136.

Paso 7 En la sección Reproductor de grabaciones basadas en red de WebEx, seleccione **Descargar** y **Guardar** para guardar el archivo ZIP en su sistema.
Abra el archivo ZIP y seleccione el programa de instalación para su plataforma e idioma, y extráigalo en un directorio. El archivo ZIP contiene los programas de instalación MSI para la plataforma de Windows en todos los idiomas disponibles. Para implementar el programa de instalación, consulte Implementación masiva del reproductor de grabaciones basadas en red, en la página 150.

Paso 8 Seleccione **Guardar** para guardar su configuración de descarga.
Puede descomprimir el archivo descargado e implementar los archivos MSI en los escritorios de los usuarios con el software de implementación masiva que utiliza su empresa. Esto asegura que los clientes estén listos para la operación cuando un usuario desea planificar o entrar a reuniones o ver grabaciones.

Qué hacer a continuación

Cada archivo ZIP contiene el programa de instalación de la aplicación para todos los idiomas admitidos. Consulte Contenido de los archivos ZIP de las aplicaciones, en la página 134 para obtener información sobre el programa de instalación que se recomienda usar.

Nota La versión de las herramientas de productividad y de la aplicación Meetings que se alinea con la versión de Cisco WebEx Meeting Server se puede encontrar en Matriz de compatibilidad de las herramientas de productividad y la aplicación Cisco WebEx Meetings, en la página 206.

Contenido de los archivos ZIP de las aplicaciones

Esta sección describe las aplicaciones del programa de instalación contenidas en cada uno de los archivos ZIP que puede descargar del sitio de administración. Los archivos ZIP contienen una aplicación del programa de instalación por idioma. Esta sección también ofrece una clave que le ayudará a determinar el idioma de cada programa de instalación.

Clave de idioma de las aplicaciones

El archivo del programa de instalación de la aplicación en inglés en cada archivo ZIP no contiene ningún sufijo de idioma. Por ejemplo, el cliente de WebEx Meetings se titula `onpremmc.msi`. (Windows). El archivo del programa de instalación de la aplicación de cada uno de los otros idiomas contiene una abreviatura en su título que indica el idioma de la aplicación que contiene. Consulte la siguiente tabla para conocer la abreviatura utilizada para cada idioma:

Abreviatura	Language
B5	Chino tradicional
DE	Alemán
ES	Español latinoamericano
FR	Francés
GB	Chino simplificado
IT	Italiano
JP	Japonés
KO	Coreano
NL	Holandés
PT	Portugués
RU	Ruso
SP	Español

Contenido de los archivos ZIP de las herramientas de productividad

El archivo ZIP de las herramientas de productividad contiene los siguientes archivos. Utilice la clave de la tabla Clave de idioma de las aplicaciones para determinar el idioma de cada archivo. Tenga en cuenta que no hay una versión para 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 del cliente de reuniones de WebEx

El archivo ZIP del cliente de reuniones de WebEx contiene los siguientes archivos. Utilice la clave de la tabla Clave de idioma de las aplicaciones 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
- webexnbrplayer_onprem.dmg (para Mac)

Contenido del archivo ZIP del reproductor de grabaciones basadas en red

El reproductor de grabaciones basadas en red solo está disponible para descarga e implementación masiva si ha seleccionado **Permitir que los usuarios descarguen aplicaciones de escritorio de WebEx** en la página de descargas. Consulte "Configurar sus parámetros de descarga" en la *Guía de administración de Cisco WebEx Meetings Server* para obtener más información.

El archivo ZIP del reproductor de grabaciones basadas en red contiene los siguientes archivos. Utilice la clave de la tabla Clave de idioma de las aplicaciones 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_onprem.dmg (para Mac)

Implementación masiva de las herramientas de productividad de Cisco WebEx

En esta sección se describen las tareas involucradas en la instalación de las herramientas de productividad de Cisco WebEx. Esta sección es una guía completa que abarca diversos tipos de instalaciones, incluidas una instalación de una única computadora e instalaciones a gran escala con Microsoft Systems Management Server 2003 (SMS). Cisco WebEx Meetings Server admite la Integración con Outlook que está contenida en el paquete ptools.msi.

La versión de las herramientas de productividad que se alinea con la versión Cisco WebEx Meeting Server puede encontrarse en Matriz de compatibilidad de las herramientas de productividad y la aplicación Cisco WebEx Meetings, en la página 206.

Instalación silenciosa de las herramientas de productividad a través de la línea de comandos

Los administradores pueden iniciar sesión en una computadora del usuario e instalar las herramientas de productividad de WebEx utilizando el modo silencioso.

Antes de comenzar

Antes de instalar una versión de mantenimiento o de mejorar su sistema a una versión más nueva, deben desinstalarse las versiones anteriores de las herramientas de productividad de Cisco WebEx.

Paso 1 Inicie sesión en la computadora del usuario.

Paso 2 Descargue el paquete MSI en el disco duro de la computadora.

Paso 3 Abra el símbolo del sistema de Windows.
En Windows 7 o Windows Vista, debe usar Ejecutar como administrador para abrirlo.

Paso 4 Ejecute el comando MSI para instalar las herramientas de productividad de WebEx silenciosamente.

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 con Outlook
	0 (predeterminado)	Desactivar la integración con Outlook
MSN	1	Active la integración de los programas de mensajería instantánea para Microsoft Office Communicator y Lync

Paso 5 Reinicie la computadora.

Desinstalación silenciosa de las herramientas de productividad a través de la línea de comandos

Los administradores pueden iniciar la sesión en una computadora del usuario y desinstalar las herramientas de productividad utilizando el modo silencioso.

Paso 1 Inicie sesión en la computadora del usuario.

Paso 2 Descargue el paquete MSI en el disco duro de la computadora.

Paso 3 Abra el símbolo del sistema de Windows.
En Windows 7 o Windows Vista, debe usar Ejecutar como administrador para abrirlo.

Paso 4 Para desinstalar todos los componentes del paquete ptools.msi MSI , introduzca el comando msiexec.exe /q /x "ptools.msi".

Instalación silenciosa utilizando SMS

Las limitaciones que se detallan a continuación se aplican al realizar una instalación silenciosa utilizando SMS:

- No se admite el modo por usuario de SMS.
- Si el administrador de SMS quiere agregar una característica para las herramientas de productividad de WebEx, el administrador deberá ejecutar el comando **REMOVE** primero y luego ejecutar el comando **ADDSOURCE**, aunque la característica no haya sido instalada antes.
- Si un usuario inicia sesión en un equipo con escritorio remoto, mientras que su administrador anuncia el paquete, debe reiniciar la computadora para asegurarse de que las herramientas de productividad de WebEx funcionen normalmente.
- Es posible la implementación masiva, pero cada usuario debe introducir la información de las credenciales.
- Antes de instalar una versión de mantenimiento o de mejorar su sistema a una versión más nueva, sus usuarios deben desinstalar las Herramientas de productividad de Cisco WebEx que se ejecutan en sus escritorios. Después de la mejora, puede arrastrar manualmente las Herramientas de productividad a sus usuarios o los usuarios pueden descargarlas en la página **Descargas**.
- Si utiliza la integración con Lync, después de una instalación silenciosa, sus usuarios deben reiniciar las computadoras para que todas las integraciones de los programas de mensajería instantánea funcionen correctamente.

Anuncio de las herramientas de productividad de Cisco WebEx mediante el programa sin supervisión por sistema SMS

Si es el administrador de SMS, realice el siguiente procedimiento para anunciar las herramientas de productividad de Cisco WebEx mediante el programa sin supervisión por sistema SMS.

Antes de comenzar

Antes de instalar una versión de mantenimiento o de mejorar su sistema a una versión más nueva, sus usuarios deben desinstalar las Herramientas de productividad de Cisco WebEx que se ejecutan en sus escritorios. Después de la mejora, puede usar el sitio de administración para arrastrar manualmente las Herramientas de productividad a sus usuarios o los usuarios pueden descargarlas en la página **Descargas** del usuario final.

Inicie sesión en el sitio de administración y arrastre manualmente las Herramientas de productividad al escritorio del usuario. Consulte la sección "Configurar sus parámetros de descarga" en la *Guía de administración de Cisco WebEx Meetings Server* para obtener más información.

Pasos resumidos

1. Cree un paquete a partir de la definición. Consulte Creación de un paquete a partir de una definición, en la página 144 para obtener más información.
2. Cambie las opciones del programa a "Sin supervisión 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 una definición, en la página 144 para obtener más información.

Paso 2 Cambie las opciones del programa a "Sin supervisión por sistema" antes del anuncio:

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

b) Haga clic con el botón secundario en la opción **Sin supervisión por sistema** y, a continuación, seleccione **Propiedades** para abrir el cuadro de diálogo **Propiedades del programa sin supervisión por sistema**.

c) Seleccione la ficha **Entorno**.

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

d) Seleccione la ficha **General**.

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

- Anexe SITEURL=″http://sample.webex.com″ para especificar la URL del sitio de WebEx utilizada por la empresa.
- Anexe marcadores de las herramientas de productividad para especificar qué componente está habilitado para las herramientas de productividad de WebEx. Los parámetros deben estar en mayúsculas y el valor predeterminado es 0 (deshabilitado).

  En el ejemplo siguiente, la primera línea del comando es msiexec.exe /q ALLUSERS=2 /m MSIZWPBY /i "ptools.msi".
- Anexe marcadores y parámetros para las herramientas de productividad en 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 a través de la línea de comandos, en la página 137 para ver las definiciones de los parámetros.

Paso 3 Ahora puede anunciar el programa.

a) Abra la consola de administrador de SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Aplicación en inglés Herramientas de productividad 2.82 de Cisco WebEx de Cisco WebEx LLC** > **Programas**.
b) Haga clic con el botón secundario en **Sin supervisión por sistema**.
c) Seleccione **Todas las tareas** > **Distribuir software**.
d) Seleccione **Siguiente** en el **Asistente para distribuir programas**.
e) Seleccione el servidor de SMS y seleccione **Siguiente**.
f) Seleccione la colección y seleccione **Siguiente**.
g) Introduzca el nombre del anuncio en el campo **Nombre** y seleccione **Siguiente**.
h) Especifique si el anuncio debe aplicarse a subcolecciones y seleccione **Siguiente**.
i) Especifique si el programa se anunciará y seleccione **Siguiente**.
j) Especifique si el programa se asignará y seleccione **Siguiente**.
k) Seleccione **Finalizar** en la página **Finalización del Asistente para distribuir programas**.
l) Navegue al directorio \Base de datos del sitio\Estado del sistema\Estado del anuncio y compruebe el estado del anuncio.
Si habilita notificaciones, el usuario verá un mensaje que indica que el programa asignado se va a ejecutar después que se haya anunciado. El programa asignado se ejecutará en silencio.

Eliminación de los componentes de las herramientas de productividad utilizando el programa sin supervisión por sistema

Realice el siguiente procedimiento para eliminar las herramientas de productividad:

Pasos resumidos

1. Cree un nuevo programa y copie todas las opciones del "programa sin supervisión por sistema" como se describe en Anuncio de las herramientas de productividad de Cisco WebEx mediante el programa sin supervisión por sistema SMS, en la página 138, y luego actualice la línea de comandos:
2. Anuncie el programa en la colección especificada de las máquinas de trabajo en el dominio. Consulte Instalación silenciosa utilizando SMS, en la página 138 para obtener más información.

Pasos detallados

Paso 1 Cree un nuevo programa y copie todas las opciones del "programa sin supervisión por sistema" como se describe en Anuncio de las herramientas de productividad de Cisco WebEx mediante el programa sin supervisión por sistema SMS, en la página 138, y luego actualice la línea de comandos:

a) Abra la consola de administrador de SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Herramientas de productividad 2.82 de Cisco WebEx de Cisco WebEx LLC** > **Programas**.
b) Haga clic con el botón secundario en el área en blanco y luego seleccione **Nuevo** > **Programa**.
c) Introduzca el nombre del programa y la línea de comandos predeterminada.
d) En el cuadro de diálogo **Propiedades**, seleccione la ficha **Entorno**.

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

e) Actualice la línea de comandos en la ficha **General**.
f) Anexe REMOVE a la línea de comandos y especifique las características que deben eliminarse.

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 los programas de mensajería instantánea. Puede utilizar PTIM como se muestra en la siguiente línea de comandos de ejemplo:
msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="PTIM"

Paso 2 Anuncie el programa en la colección especificada de las máquinas de trabajo en el dominio. Consulte Instalación silenciosa utilizando SMS, en la página 138 para obtener más información.
Las herramientas de productividad de Cisco WebEx se actualizarán en estas máquinas silenciosamente.

Adición de los componentes de las herramientas de productividad utilizando el programa sin supervisión por sistema

Para que un administrador agregue un componente a las herramientas de productividad, debe ejecutar REMOVE primero y luego ejecutar ADDSOURCE, aunque el componente no se haya instalado antes.

Pasos resumidos

1. Cree un nuevo programa llamado "Agregar-fase1" y copie todas las opciones del "programa sin supervisión por sistema" y luego actualice la línea de comandos:
2. Anuncie el programa en la colección especificada de las máquinas de trabajo en el dominio. Consulte Instalación silenciosa utilizando SMS, en la página 138 para obtener más información.
3. Cree un segundo programa llamado "Agregar-fase2" y copie todas las opciones del "programa sin supervisión por sistema" y luego actualice la línea de comandos:
4. Anuncie el programa en la colección especificada de las máquinas de trabajo en el dominio. Consulte Instalación silenciosa utilizando SMS, en la página 138 para obtener más información.

Pasos detallados

Paso 1 Cree un nuevo programa llamado "Agregar-fase1" y copie todas las opciones del "programa sin supervisión por sistema" y luego actualice la línea de comandos:

a) Abra la consola de administrador de SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Herramientas de productividad 2.82 de Cisco WebEx de Cisco WebEx LLC** > **Programas**.
b) Haga clic con el botón secundario en el área en blanco y luego seleccione **Nuevo** > **Programa**.

c) Introduzca el nombre del programa y la línea de comandos predeterminada.
d) En el cuadro de diálogo Propiedades seleccione la ficha **Entorno**.

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

e) Actualice la línea de comandos en la ficha **General**.
f) Anexe REMOVE a la línea de comandos y especifique las características que deben agregarse.

Ejemplo:
Si desea agregar OIy PTIM (el valor PTIM es para la integración de WebEx con los programas de mensajería instantánea), primero debe ELIMINARLOS, incluso si todavía no están instalados: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="OI,PTIM"

Paso 2 Anuncie el programa en la colección especificada de las máquinas de trabajo en el dominio. Consulte Instalación silenciosa utilizando SMS, en la página 138 para obtener más información.

Paso 3 Cree un segundo programa llamado "Agregar-fase2" y copie todas las opciones del "programa sin supervisión por sistema" y luego actualice la línea de comandos:

a) Abra la consola de administrador de SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Herramientas de productividad 2.82 de Cisco WebEx de Cisco WebEx LLC** > **Programas**.
b) Haga clic con el botón secundario en el área en blanco y luego seleccione **Nuevo** > **Programa**.
c) Introduzca el nombre del programa y la línea de comandos predeterminada.
d) En el cuadro de diálogo Propiedades seleccione la ficha **Entorno**.

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

e) En el cuadro de diálogo Propiedades seleccione la ficha **Opciones avanzadas**.
f) Active **Ejecutar otro programa primero** y seleccione el programa **Agregar-fase1**.
g) Actualice la línea de comandos en la ficha **General**.
h) Anexe ADDSOURCE a la línea de comandos y especifique las características que deben agregarse.

Ejemplo:
Si desea agregar OI, utilice este comando de ejemplo: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" ADDSOURCE="OI" OI=1

Ejemplo:
Si desea agregar OI y PTIM, utilice este comando de ejemplo: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" ADDSOURCE="OI,PTIM" OI=1 MSN=1

Paso 4 Anuncie el programa en la colección especificada de las máquinas de trabajo en el dominio. Consulte Instalación silenciosa utilizando SMS, en la página 138 para obtener más información.
Las herramientas de productividad de Cisco WebEx se actualizarán en estas máquinas silenciosamente.

Desinstalación de las herramientas de productividad utilizando el programa de desinstalación por sistema SMS

El administrador de SMS puede desinstalar las herramientas de productividad de Cisco WebEx utilizando el programa de desinstalación por sistema SMS realizando el procedimiento siguiente.

Pasos resumidos

1. Utilice el paquete de instalación de SMS creado en Creación de un paquete a partir de una definición, en la página 144.
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 una definición, en la página 144.

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 silenciosamente.

Anuncio 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 versión nueva de las herramientas de productividad de Cisco WebEx.

Antes de comenzar

Antes de instalar una versión de mantenimiento o de mejorar su sistema a una versión más nueva, sus usuarios deben desinstalar las Herramientas de productividad de Cisco WebEx que se ejecutan en sus escritorios. Después de la mejora, puede usar el sitio de administración para arrastrar manualmente las Herramientas de productividad a sus usuarios o los usuarios pueden descargarlas en la página **Descargas** del usuario final.

Inicie sesión en el sitio de administración, seleccione **Configuración** > **Descargas** y desactive la siguiente configuración:

- **Actualización automática de las herramientas de productividad de Cisco WebEx**
- **Permitir que los usuarios descarguen aplicaciones de escritorio de WebEx**

Pasos resumidos

1. Cree un paquete de instalación de SMS mediante el paquete MSI de las herramientas de productividad de WebEx. Consulte Creación de un paquete a partir de una definición, en la página 144 para obtener más información.
2. Cambie las opciones del programa a **Sin supervisión por sistema** antes del anuncio. Consulte Adición de los componentes de las herramientas de productividad utilizando el programa sin supervisión por sistema, en la página 141 para obtener más información.
3. Anuncie el programa. Consulte Adición de los componentes de las herramientas de productividad utilizando el programa sin supervisión por sistema, en la página 141 para obtener más información.

Pasos detallados

Paso 1 Cree un paquete de instalación de SMS mediante el paquete MSI de las herramientas de productividad de WebEx. Consulte Creación de un paquete a partir de una definición, en la página 144 para obtener más información.

Paso 2 Cambie las opciones del programa a **Sin supervisión por sistema** antes del anuncio. Consulte Adición de los componentes de las herramientas de productividad utilizando el programa sin supervisión por sistema, en la página 141 para obtener más información.

Paso 3 Anuncie el programa. Consulte Adición de los componentes de las herramientas de productividad utilizando el programa sin supervisión por sistema, en la página 141 para obtener más información.
Las herramientas de productividad de Cisco WebEx viejas se eliminan y las nuevas herramientas de productividad de Cisco WebEx se instalan silenciosamente.

Creación de un paquete a partir de una definición

Realice el siguiente procedimiento para crear un paquete a partir de una definición.

Pasos resumidos

1. Abra la consola de administrador de SMS y seleccione **Base de datos del sitio** > **Paquete**.
2. Haga clic con el botón secundario 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 buscar y seleccionar el paquete MSI de las herramientas de productividad de WebEx y luego seleccione **Siguiente**.
6. Seleccione **Obtener siempre archivos de un directorio de origen** y luego seleccione **Siguiente.**
7. Seleccione la ubicación del directorio de origen. La ruta del directorio es la carpeta que contiene el paquete de instalación. Luego seleccione **Siguiente**.
8. Seleccione **Finalizar**.
9. Seleccione **Base de datos del sitio** > **Paquetes** > **Aplicación en inglés Herramienta de productividad 2.82 de Cisco WebEx de Cisco WebEx LLC** > **Programas**. Hay seis programas predeterminados disponibles.

Pasos detallados

Paso 1 Abra la consola de administrador de SMS y seleccione **Base de datos del sitio** > **Paquete**.

Paso 2 Haga clic con el botón secundario 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 buscar y seleccionar el paquete MSI de las herramientas de productividad de WebEx y luego seleccione **Siguiente**.

Paso 6 Seleccione **Obtener siempre archivos de un directorio de origen** y luego seleccione **Siguiente.**

Paso 7 Seleccione la ubicación del directorio de origen. La ruta del directorio es la carpeta que contiene el paquete de instalación. Luego seleccione **Siguiente**.

Paso 8 Seleccione **Finalizar**.

Paso 9 Seleccione **Base de datos del sitio** > **Paquetes** > **Aplicación en inglés Herramienta de productividad 2.82 de Cisco WebEx de Cisco WebEx LLC** > **Programas**. Hay seis programas predeterminados disponibles.

Implementación masiva de la aplicación de reuniones

Esta sección está diseñada para ayudar a su organización a comprender las tareas implicadas en la instalación de la aplicación de Cisco WebEx Meetings. Esta sección es una guía completa que abarca diversos tipos de instalaciones, incluyendo una instalación de una única computadora e instalaciones a gran escala con Microsoft Systems Management Server 2003 (SMS).

Nota Instalación silenciosa significa que la aplicación puede ser implementada de forma silenciosa, pero necesita la configuración del usuario final.

Instalación de Cisco WebEx Meetings

Antes de comenzar

Los siguientes requisitos previos se aplican al programa de instalación de Cisco WebEx Meetings:

- Instalar el paquete MSI de Cisco WebEx requiere privilegios de administrador. El paquete MSI se instala en la carpeta predeterminada de Programas del SO que requiere privilegios de administrador para el acceso.
- El paquete MSI de Cisco WebEx está desarrollado para Windows Installer Service 2.0 o superior. Si la máquina local está configurada con una versión anterior, se mostrará un mensaje de error que le informará al usuario que para instalar el paquete MSI se necesita una versión más actualizada de Windows Installer Service. Cuando ejecuta el paquete MSI, el usuario verá una interfaz básica de MSI.

Pasos resumidos

1. Ejecute el programa de instalación en la computadora del usuario.
2. Seleccione **Siguiente** en los próximos cuadros de diálogo hasta llegar al cuadro de diálogo de la instalación.
3. Seleccione **Instalar**.
4. Seleccione **Finalizar** luego de que la instalación esté completa.

Pasos detallados

Paso 1 Ejecute el programa de instalación en la computadora del usuario.
Aparecerá el asistente de instalación con un mensaje de introducción.

Paso 2 Seleccione **Siguiente** en los próximos cuadros de diálogo hasta llegar al cuadro de diálogo de la instalación.

Paso 3 Seleccione **Instalar**.

Paso 4 Seleccione **Finalizar** luego de que la instalación esté completa.

Desinstalación de Cisco WebEx Meetings de forma local

Puede iniciar sesión en la computadora del usuario y desinstalar la aplicación Cisco WebEx Meetings desde el Panel de control o desde la carpeta WebEx en el disco duro local.

Antes de comenzar

La aplicación Cisco WebEx Meetings se instala en la computadora de un usuario.

Paso 1 Inicie sesión en la computadora del usuario.

Paso 2 Elimine la aplicación Cisco WebEx Meetings utilizando uno de los siguientes métodos:

- Seleccione **Inicio** > **Panel de control** > **Programas y características**. Desde la lista de programas, seleccione **Cisco WebEx Meetings** y, luego, **Desinstalar/Cambiar**.
- Seleccione **Inicio** > **Equipo** > **Sistema (C:)** > **Carpeta ProgramData** > **Carpeta WebEx**. Haga clic con el botón derecho en **atcliun.exe** y seleccione **Eliminar**.

Nota Cuando desinstala atcliun.exe desde la carpeta WebEx, se eliminan tanto la versión física como la versión en la nube de la aplicación Cisco WebEx Meetings, si ambas versiones de la aplicación se guardaron en disco duro local del usuario. Sin embargo, cuando desinstala la aplicación desde el Panel de control, solo se desinstala la versión física de la aplicación.

La aplicación Cisco WebEx Meetings se desinstala de la computadora del usuario.

Instalación silenciosa de la aplicación Meetings a través de la línea de comandos

Los administradores pueden iniciar la sesión en una computadora del usuario e instalar la aplicación WebEx Meetings utilizando el modo silencioso.

Paso 1 Inicie sesión en la computadora del usuario.

Paso 2 Descargue el paquete MSI en el disco duro de la computadora.

Paso 3 Abra el símbolo del sistema de Windows.
En Windows 7 o Windows Vista, debe usar Ejecutar como administrador para abrirlo.

Paso 4 Ingrese el comando MSI para instalar las aplicaciones de Cisco WebEx Meetings silenciosamente.

Ejemplo:
Ingrese msiexec /i onpremmc.msi /qn.

Paso 5 Reinicie la computadora.

Desinstalación silenciosa de la aplicación Meetings a través de la línea de comandos

Los administradores pueden iniciar la sesión en una computadora del usuario y desinstalar la aplicación Meetings utilizando el modo silencioso.

Paso 1 Inicie sesión en la computadora del usuario.

Paso 2 Abra el símbolo del sistema de Windows.
En Windows 7 o Windows Vista, debe usar Ejecutar como administrador para abrirlo.

Paso 3 Para desinstalar todos los componentes del paquete onpremmc.msi MSI , introduzca el comando msiexec/x onpremmc.msi/qn.

Instalación silenciosa utilizando SMS

Antes de comenzar

Las limitaciones que se detallan a continuación se aplican al realizar una instalación silenciosa utilizando SMS:

- No se admite el modo por usuario de SMS.

- Si un usuario inicia sesión en una computadora con escritorio remoto mientras que su administrador anuncia el paquete, debe reiniciar la computadora para asegurarse de que la aplicación WebEx Meetings funcione normalmente.

Anuncio de la aplicación de Cisco WebEx Meetings mediante el programa sin supervisión por sistema SMS

Si es el administrador de SMS, realice el siguiente procedimiento para anunciar la aplicación de Cisco WebEx Meetings mediante el programa sin supervisión por sistema SMS.

Antes de comenzar

Inicie sesión en el sitio de administración y configure los parámetros de descarga para arrastrar manualmente las aplicaciones de escritorio de WebEx al escritorio del usuario. Consulte la sección "Configurar sus parámetros de descarga" en la Guía de administración de Cisco WebEx Meetings Server para obtener más información.

Pasos resumidos

1. Cree un paquete a partir de la definición. Consulte Creación de un paquete a partir de una definición, en la página 144 para obtener más información.
2. Cambie las opciones del programa a "Sin supervisión 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 una definición, en la página 144 para obtener más información.

Paso 2 Cambie las opciones del programa a "Sin supervisión por sistema" antes del anuncio:

a) Abra la consola de administrador de SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Aplicación en inglés Cisco WebEx Meetings de Cisco WebEx LLC** > **Programas**.

b) Haga clic con el botón secundario en la opción **Sin supervisión por sistema** y seleccione **Propiedades** para abrir el cuadro de diálogo **Propiedades del programa sin supervisión por sistema**.

c) Seleccione la ficha **Entorno**.

- Para la opción **El programa se puede ejecutar**, seleccione **Solo cuando el usuario está conectado**.
- Para la opción **Modo de ejecución**, seleccione **Ejecutar con derechos administrativos**. No seleccione **Permitir a los usuarios interactuar con este programa**.

d) Seleccione la ficha **General**.

e) Anexe un parámetro adicional a la opción de la línea de comandos para especificar algunas opciones para la aplicación de Cisco WebEx Meetings:

Ejemplo:
Por ejemplo, la línea de comandos inicial es: msiexec /i "onpremmc.msi" /qn.

Paso 3 Ahora puede anunciar el programa.

a) Abra la consola de administrador de SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Aplicación en inglés Cisco WebEx Meetings de Cisco WebEx LLC** > **Programas**.
b) Haga clic con el botón secundario en **Sin supervisión por sistema**.
c) Seleccione **Todas las tareas** > **Distribuir software**.
d) Seleccione **Siguiente** en el **Asistente para distribuir programas**.
e) Seleccione el servidor de SMS y seleccione **Siguiente**.
f) Seleccione la colección y seleccione **Siguiente**.
g) Introduzca el nombre del anuncio en el campo **Nombre** y seleccione **Siguiente**.
h) Especifique si el anuncio debe aplicarse a subcolecciones y seleccione **Siguiente**.
i) Especifique si el programa se anunciará y seleccione **Siguiente**.
j) Especifique si el programa se asignará y seleccione **Siguiente**.
k) Seleccione **Finalizar** en la página **Finalización del Asistente para distribuir programas**.
l) Navegue al directorio \Base de datos del sitio\Estado del sistema\Estado del anuncio y compruebe el estado del anuncio.
Si habilita notificaciones, el usuario verá un mensaje que indica que el programa asignado se va a ejecutar después que se haya anunciado. El programa asignado se ejecutará en silencio.

Desinstalación de la aplicación de Cisco WebEx Meetings mediante el programa de desinstalación por sistema SMS

El administrador de SMS puede desinstalar la aplicación de Cisco WebEx Meetings utilizando el programa de desinstalación por sistema SMS realizando el procedimiento siguiente.

Pasos resumidos

1. Utilice el paquete de instalación de SMS creado en Creación de un paquete a partir de una definición, en la página 144.
2. Anuncie el programa de desinstalación por sistema para desinstalar la aplicación de Cisco WebEx Meetings.

Pasos detallados

Paso 1 Utilice el paquete de instalación de SMS creado en Creación de un paquete a partir de una definición, en la página 144.

Paso 2 Anuncie el programa de desinstalación por sistema para desinstalar la aplicación de Cisco WebEx Meetings.
La aplicación de Cisco WebEx Meetings se desinstalará en las máquinas especificadas de modo silencioso.

Implementación masiva del reproductor de grabaciones basadas en red

Esta sección está diseñada para ayudar a su organización a comprender las tareas implicadas en la instalación del reproductor de grabaciones basadas en red de Cisco. Esta sección es una guía completa que abarca diversos tipos de instalaciones, incluyendo una instalación de una única computadora e instalaciones a gran escala con Microsoft Systems Management Server 2003 (SMS).

Instalación del reproductor de grabaciones basadas en red

Antes de comenzar

Los siguientes requisitos previos se aplican al programa de instalación del reproductor de grabaciones basadas en red de Cisco WebEx:

- Instalar el paquete MSI de Cisco WebEx requiere privilegios de administrador. El paquete MSI se instala en la carpeta predeterminada de Programas del SO que requiere privilegios de administrador para el acceso.
- El paquete MSI de Cisco WebEx está desarrollado para Windows Installer Service 2.0 o superior. Si la máquina local está configurada con una versión anterior, se mostrará un mensaje de error que le informará al usuario que para instalar el paquete MSI se necesita una versión más actualizada de Windows Installer Service. Cuando ejecuta el paquete MSI, el usuario verá una interfaz básica de MSI.

Pasos resumidos

1. Ejecute el programa de instalación en la computadora del usuario.
2. Seleccione **Siguiente** en los próximos cuadros de diálogo hasta llegar al cuadro de diálogo de la instalación.
3. Seleccione **Instalar**.
4. Seleccione **Finalizar** luego de que la instalación esté completa.

Pasos detallados

Paso 1 Ejecute el programa de instalación en la computadora del usuario.
Aparecerá el asistente de instalación con un mensaje de introducción.

Paso 2 Seleccione **Siguiente** en los próximos cuadros de diálogo hasta llegar al cuadro de diálogo de la instalación.

Paso 3 Seleccione **Instalar**.

Paso 4 Seleccione **Finalizar** luego de que la instalación esté completa.

Instalación silenciosa del reproductor de grabaciones a través de la línea de comandos

Los administradores pueden iniciar la sesión en una computadora del usuario e instalar el reproductor de grabaciones de WebEx utilizando el modo silencioso.

Pasos resumidos

1. Inicie sesión en la computadora del usuario.
2. Descargue el paquete MSI en el disco duro de la computadora.
3. Abra el símbolo del sistema de Windows.
4. Ingrese el comando MSI para instalar el reproductor de grabaciones de WebEx silenciosamente.
5. Reinicie la computadora.

Pasos detallados

Paso 1 Inicie sesión en la computadora del usuario.

Paso 2 Descargue el paquete MSI en el disco duro de la computadora.

Paso 3 Abra el símbolo del sistema de Windows.
En Windows 7 o Windows Vista, debe usar Ejecutar como administrador para abrirlo.

Paso 4 Ingrese el comando MSI para instalar el reproductor de grabaciones de WebEx silenciosamente.

Ejemplo:
Ingrese msiexec/i nbr2player_onprem.msi/qn.

Paso 5 Reinicie la computadora.

Desinstalación silenciosa del reproductor de grabaciones a través de la línea de comandos

Los administradores pueden iniciar la sesión en una computadora del usuario y desinstalar el reproductor de grabaciones utilizando el modo silencioso.

Paso 1 Inicie sesión en la computadora del usuario.

Paso 2 Descargue el paquete MSI en el disco duro de la computadora.

Paso 3 Abra el símbolo del sistema de Windows.
En Windows 7 o Windows Vista, debe usar Ejecutar como administrador para abrirlo.

Paso 4 Desinstale todos los componentes del paquete MSI onpremmc.msi ingresando el comando msiexec/i nbr2player_onprem.msi/qn.

Instalación silenciosa utilizando SMS

Antes de comenzar

Las limitaciones que se detallan a continuación se aplican al realizar una instalación silenciosa utilizando SMS:

- No se admite el modo por usuario de SMS.
- Si un usuario inicia sesión en una computadora con escritorio remoto mientras que su administrador anuncia el paquete, debe reiniciar la computadora para asegurarse de que la aplicación WebEx Meetings funcione normalmente.

Anuncio del reproductor de grabaciones basadas en red de Cisco WebEx mediante el programa sin supervisión por sistema SMS

Si es el administrador de SMS, realice el siguiente procedimiento para anunciar el reproductor de grabaciones basadas en red de Cisco WebEx mediante el programa sin supervisión por sistema SMS.

Antes de comenzar

Inicie sesión en el sitio de administración y configure los parámetros de descarga para arrastrar manualmente las aplicaciones de escritorio de WebEx al escritorio del usuario. Consulte la sección "Configurar sus parámetros de descarga" en la Guía de administración de Cisco WebEx Meetings Server para obtener más información.

Pasos resumidos

1. Cree un paquete a partir de la definición. Consulte Creación de un paquete a partir de una definición, en la página 144 para obtener más información.
2. Cambie las opciones del programa a "Sin supervisión 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 una definición, en la página 144 para obtener más información.

Paso 2 Cambie las opciones del programa a "Sin supervisión por sistema" antes del anuncio:

a) Abra la consola de administrador de SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Aplicación en inglés Reproductor de grabaciones basadas en red de Cisco WebEx de Cisco WebEx LLC** > **Programas**.

b) Haga clic con el botón secundario en la opción **Sin supervisión por sistema** y seleccione **Propiedades** para abrir el cuadro de diálogo **Propiedades del programa sin supervisión por sistema**.

c) Seleccione la ficha **Entorno**.

- Para la opción **El programa se puede ejecutar**, seleccione **Solo cuando el usuario está conectado**.

- Para la opción **Modo de ejecución**, seleccione **Ejecutar con derechos administrativos**. No seleccione **Permitir a los usuarios interactuar con este programa**.

d) Seleccione la ficha **General**.
e) Anexe un parámetro adicional a la opción de la línea de comandos para especificar algunas opciones para la aplicación de Cisco WebEx Meetings:

Ejemplo:
Por ejemplo, la línea de comandos inicial es: msiexec /i "nbr2player_onprem.msi" /qn.

Paso 3 Ahora puede anunciar el programa.

a) Abra la consola de administrador de SMS y seleccione **Base de datos del sitio** > **Paquetes** > **Aplicación en inglés Reproductor de grabaciones basadas en red de Cisco WebEx de Cisco WebEx LLC** > **Programas**.
b) Haga clic con el botón secundario en **Sin supervisión por sistema**.
c) Seleccione **Todas las tareas** > **Distribuir software**.
d) Seleccione **Siguiente** en el **Asistente para distribuir programas**.
e) Seleccione el servidor de SMS y seleccione **Siguiente**.
f) Seleccione la colección y seleccione **Siguiente**.
g) Introduzca el nombre del anuncio en el campo **Nombre** y seleccione **Siguiente**.
h) Especifique si el anuncio debe aplicarse a subcolecciones y seleccione **Siguiente**.
i) Especifique si el programa se anunciará y seleccione **Siguiente**.
j) Especifique si el programa se asignará y seleccione **Siguiente**.
k) Seleccione **Finalizar** en la página **Finalización del Asistente para distribuir programas**.
l) Navegue al directorio \Base de datos del sitio\Estado del sistema\Estado del anuncio y compruebe el estado del anuncio.
Si habilita notificaciones, el usuario verá un mensaje que indica que el programa asignado se va a ejecutar después que se haya anunciado. El programa asignado se ejecutará en silencio.

Desinstalación del reproductor de grabaciones basadas en red de Cisco WebEx mediante el programa de desinstalación por sistema SMS

El administrador de SMS puede desinstalar el reproductor de grabaciones basadas en red de Cisco WebEx utilizando el programa de desinstalación por sistema SMS y realizando el procedimiento siguiente.

Pasos resumidos

1. Utilice el paquete de instalación de SMS creado en Creación de un paquete a partir de una definición, en la página 144.
2. Anuncie el programa de desinstalación por sistema para desinstalar el reproductor de grabaciones basadas en red de Cisco WebEx.

Pasos detallados

Paso 1 Utilice el paquete de instalación de SMS creado en Creación de un paquete a partir de una definición, en la página 144.

Paso 2 Anuncie el programa de desinstalación por sistema para desinstalar el reproductor de grabaciones basadas en red de Cisco WebEx.
El reproductor de grabaciones basadas en red de Cisco WebEx se desinstalará en las máquinas especificadas de modo silencioso.

Reconfiguración de los parámetros después de realizar una actualización

Después de una actualización, la aplicación del reproductor de grabaciones basadas en red se actualiza automáticamente la primera vez que se usa para reproducir una grabación.

Después de realizar una actualización del software de Cisco WebEx Meetings Server (CWMS), debe actualizar las rutas a las aplicaciones implementadas masivamente.

Para los sistemas Mac, la ruta de acceso es /Users/(Usuario local)/Library/Application Support/WebEx Folder/.

Para los sistemas Windows, la ruta depende de la versión, el tipo de descarga y el tipo de explorador web:

- Windows XP, Windows 2000
  - <SystemDisk>\Windows\Downloaded Program Files\WebEx (usuarios administrativos generales)
  - <SystemDisk>\Program Files\WebEx (instalación MSI del cliente de WebEx)
  - <SystemDisk>\Documents and Settings\<UserName>\ WebEx (usuarios generales)
  - <SystemDisk>\Documents and Settings\<UserName>\Application Data\WebEx (para descargas de Java)
  - <SystemDisk>\Documents and Settings\<UserName>\Local Settings\Temporary Internet Files\webexmc (solución .exe)
  - <SystemDisk>\Documents and Settings\<UserName>\Local Settings\Temp\WebEx (escriba <Username\WebEx fail)
  - <Folder name registered by ieatgpc.dll>\WebEx (si ha implementado ieatpgc.dll en su sistema)
  - <FireFoxDir>\plugins\WebEx (para Mozilla Firefox)
- 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. Su sistema omitirá el archivo preexistente.

- 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 una carpeta preexistente. De lo contrario, el sistema utilizará su propia ruta como se describió anteriormente.

Las aplicaciones cliente de los sistemas Windows y Mac se actualizan automáticamente para mantener la compatibilidad con el sistema actualizado.

En un entorno bloqueado, debe llevar a cabo las actualizaciones manualmente para sistemas Windows, pero no para los sistemas Mac.

Nota La versión de las herramientas de productividad y de la aplicación Meetings que se alinea con la versión de Cisco WebEx Meeting Server se puede encontrar en Matriz de compatibilidad de las herramientas de productividad y la aplicación Cisco WebEx Meetings, en la página 206.

CAPÍTULO 8

Configuración de SSO con SAML

- Descripción general del inicio de sesión único, página 157
- Beneficios del inicio de sesión único, página 158
- Descripción general de la configuración del inicio de sesión único con SAML 2.0, página 159
- SSO con SAML para el inicio de sesión del usuario final y de administración, página 160
- Diferencias en el inicio de sesión único con SAML 2.0 entre el servicio de reuniones basado en la nube y WebEx Meetings Server, página 160
- Atributos de la aserción SAML, página 168

Descripción general del inicio de sesión único

Los estándares del inicio de sesión único (SSO) federado como SAML 2.0 proporcionan mecanismos seguros para la transmisión de 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 el comité técnico de servicios de seguridad de OASIS.

El protocolo SAML 2.0 ha tenido un éxito significativo, logrando relevancia en los servicios financieros, la enseñanza superior, el gobierno y otros segmentos de la industria. El soporte SAML 2.0 se ha implementado por todos los principales proveedores de administración de acceso web. La Administración de servicios generales (GSA) del gobierno de los Estados Unidos requiere que todos los proveedores que participan en el programa de federación de identidad de autenticación electrónica de lo Estados Unidos cumplan con SAML 2.0.

Los sitios web compatibles con SAML 2.0 intercambian la información de las credenciales de los usuarios mediante aserciones SAML. Una aserción SAML es un documento XML que contiene declaraciones confiables acerca de un sujeto incluyendo, por ejemplo, un nombre de usuario y sus privilegios. Las aserciones SAML generalmente se firman digitalmente para garantizar la autenticidad.

Muchas grandes empresas han implementado la administración de identidad y acceso (IAM) federada y los sistemas de proveedores de identidad (IdP), como Ping Federate de Ping Identity, CA SiteMinder, Open AM y Windows ADFS 2.0, en sus intranets corporativas. Estos sistemas IAM e IdP manejan la autenticación de usuarios y los requisitos de SSO para empleados y socios. Los sistemas IAM e IdP utilizan los protocolos SAML para interoperar con los sitios web de los socios fuera de sus firewalls. Los usuarios pueden utilizar sus sistemas IAM e IdP para autenticar automáticamente a sus usuarios de los servicios de reuniones de Cisco

WebEx. Esto aumenta la eficiencia, ya que los usuarios no tienen que recordar sus nombres de usuario y sus contraseñas para iniciar o entrar a reuniones en sus sitios de Cisco WebEx.

Nota WebEx Meetings Server admite IdP de SAML 2.0 solamente. No admite IdP basados en los estándares antiguos de SAML 1.1 y WS-Federate. Esta restricción es contraria a los servicios de reuniones basados en la nube de Cisco WebEx que aún admiten SAML 1.1 y WS-Federate. La siguiente es una lista de IdP de SAML 2.0 que han sido validados para trabajar con Cisco WebEx Meetings Server:

- ADFS 2.0 de Microsoft (un complemento gratuito para Microsoft Windows Server 2008/Windows Server 2008 R2 o a la función de servidor de AD FS en Windows Server 2012)
- Ping Federate 6.6.0.17 de Ping Identity
- Forgerock Open AM 10.0.0
- CA SiteMinder 6.0 SP5

Como SAML 2.0 es un estándar abierto, otros IdP de SAML 2.0 pueden también operar con Cisco WebEx Meetings Server. Sin embargo, Cisco no ha probado otros IdP de SAML 2.0. Es, por tanto, responsabilidad del usuario hacer que esta integración sea operativa.

Beneficios del inicio de sesión único

El inicio de sesión único (SSO) puede beneficiarlo de las siguientes maneras:

- Autenticación de usuarios simplificada: de manera predeterminada, Cisco WebEx Meetings Server requiere que los usuarios inicien sesión utilizando las direcciones de correo electrónico y las contraseñas que hayan seleccionado individualmente y que sean específicas para el sistema del servidor de reuniones. Los usuarios seleccionan sus contraseñas al activar sus cuentas del servidor de reuniones. Aunque este enfoque funciona bien en la mayoría de las organizaciones pequeñas y de tamaño medio, las organizaciones más grandes prefieren la autenticación de usuarios mediante credenciales corporativas (es decir, Active Directory) para así mejorar la seguridad. Puede lograr este objetivo al utilizar SSO con SAML 2.0.

  Nota Un beneficio de seguridad agregado del SSO es que la contraseña corporativa nunca se envía o se guarda realmente en Cisco WebEx Meetings Server luego de que el usuario se autentica correctamente.

- Administración de usuarios simplificada: las grandes organizaciones con empleados que cambian debido a la rotación normal del personal prefieren automatizar el proceso de administración de usuarios en la integración con WebEx Meetings Server. Esto significa la automatización de las siguientes acciones:
  - Creación de cuentas de usuario cuando los empleados entran a la organización
  - Actualizaciones de las cuentas de usuario cuando los empleados obtienen diferentes funciones dentro de la organización
  - Desactivación de las cuentas de usuario cuando los empleados dejan la organización

Puede lograr la automatización de estos eventos al configurar la **Creación automática de cuenta** y la **Actualización automática de cuenta** en la sección SSO del sitio de administración de Cisco WebEx Meetings Server. Se recomienda activar estas características si también son compatibles con sus IdP de SAML. Las cuentas de usuario se crean y se actualizan automáticamente "bajo demanda" cuando los usuarios se autentican con éxito, eliminando así la necesidad de crear usuarios manualmente con la administración de Cisco WebEx. Asimismo, los usuarios no pueden continuar iniciando sesión en sus cuentas una vez que dejan la organización, ya que el IdP de SAML 2.0 bloquea el inicio de sesión a aquellos usuarios que son eliminados de la base de datos de usuarios del IdP de SAML 2.0, que generalmente es un proxy para el directorio corporativo subyacente.

Descripción general de la configuración del inicio de sesión único con SAML 2.0

Importante A menos que alguien en su organización tenga experiencia en el inicio de sesión único (SSO) con SAML 2.0, recomendamos que obtenga los servicios de un socio cualificado de Cisco AUC o los servicios avanzados de Cisco. Realizamos esta recomendación ya que la configuración del SSO con SAML puede ser bastante complicada.

Precaución Si la respuesta de SAML tiene un retorno de carro en cualquiera de los campos, la actualización automática, la creación de cuentas y la autenticación fallarán. Si bien el proveedor de SAML calcula la firma digital con el retorno de carro, Cisco WebEx Meetings Server elimina el retorno de carro, lo que torna la firma digital inválida.

Repase estos pasos generales para configurar el SSO con SAML 2.0:

1. Asegúrese de que su infraestructura de SSO con SAML 2.0 esté en su lugar y esté integrada con su directorio corporativo. Esto implica configurar el software de IdP de SAML 2.0 y el sitio web de autenticación de SSO. El sitio web de autenticación es un portal donde los usuarios introducen sus credenciales corporativas.
2. Asegúrese de que los usuarios puedan acceder al sitio web de autenticación de SSO. Este paso es importante porque, como parte del proceso de inicio de sesión, Cisco WebEx Meetings Server redirecciona a los usuarios a este sitio web de autenticación.

Nota Si su sistema de Cisco WebEx Meetings Server está activado para acceso público (es decir, permite a los usuarios iniciar sesión y entrar a reuniones desde Internet) es esencial garantizar que el sitio web de autenticación de SSO también sea accesible desde Internet. Esto generalmente implica implementar el IdP de SAML 2.0 en su DMZ. Sin este paso extra, los usuarios verán los errores "404 sitio no encontrado" cuando inicien sesión en Cisco WebEx Meetings Server desde Internet.

3. Conecte WebEx Meetings Server al IdP de SAML 2.0 mediante estos dos métodos:
   - Seleccione **Configuración** > **Seguridad** > **SSO federado** en su sitio de administración de Cisco WebEx Meetings Server.

- Siga las instrucciones en su documentación de IdP de SAML 2.0. Tenga en cuenta que estas instrucciones varían de proveedor a proveedor y de que incluso pueden cambiar según la versión de IdP de SAML 2.0. Esta es otra razón para que contacte con un socio cualificado de Cisco AUC o con los servicios avanzados de Cisco para que le ayuden a implementar la solución.

Nota No utilice las instrucciones que se encuentran en Red para desarrolladores de Cisco para configurar IdP de SAML 2.0, ya que estas instrucciones están desarrolladas para los servicios de reuniones basados en la nube de Cisco WebEx y, por consiguiente, no funcionan de forma óptima con Cisco WebEx Meetings Server.

SSO con SAML para el inicio de sesión del usuario final y de administración

Generalmente, SSO con SAML se configura solo para el inicio de sesión en el sitio del usuario final y no en el sitio de administración. En los sitios de Cisco WebEx Meetings Server integrados con SSO con SAML 2.0, el comportamiento de la autenticación de usuarios se asemeja al comportamiento SaaS de WebEx. Un administrador de Cisco WebEx Meetings Server (y un administrador de SaaS de WebEx) puede iniciar sesión en una cuenta de usuario final utilizando SSO con SAML, pero debe iniciar sesión en una cuenta de administrador en el mismo sistema usando una contraseña distinta. Esto garantiza que en el caso de errores muy graves en el IdP de SSO con SAML, un administrador podrá aún tener acceso al sitio de administración. Sin esta protección contra fallas, podría encontrarse en una situación en la cual el sitio de administración esté inaccesible, no por una falla del producto sino no por un problema con el software de IdP de SSO con SAML. El software de IdP de SSO con SAML se encuentra en un servidor externo a Cisco WebEx Meetings Server (o Saas de WebEx) y, por tanto, está fuera de nuestro control.

Diferencias en el inicio de sesión único con SAML 2.0 entre el servicio de reuniones basado en la nube y WebEx Meetings Server

Mientras que los servicios de reuniones basados en la nube de Cisco WebEx emplean ID de usuarios únicos al crear cuentas de usuario, Cisco WebEx Meetings Server 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) con SAML 2.0:

- Contener la dirección de correo electrónico en el campo NameID es obligatorio para la aserción SAML. Sin este paso, la autenticación del usuario y la creación de cuenta fallan porque Cisco WebEx Meetings Server no permite la creación de cuentas de usuario sin una dirección de correo electrónico asociada.
- Los servicios de reuniones basados en la nube de Cisco WebEx permiten la eliminación del dominio de correo electrónico, como "@cisco.com", del UPN (nombre principal del usuario) cuando la creación automática de cuenta está activada. Esto conlleva la creación de una cuenta de usuario que se asemeja a ID de usuario. Dado que WebEx Meetings Server usa una dirección de correo electrónico complete para crear cuentas de usuario, no puede eliminar dominio de correo electrónico desde UPN.

En la práctica, al principio puede implementar Cisco WebEx Meetings Server sin SSO con SAML 2.0 y activarlo más tarde. Hacer esto tiene los siguientes efectos importantes en la autenticación del usuario, la creación automática de cuenta y las características de actualización automática de cuenta:

Situación	Comportamiento de la autenticación del usuario	Creación automática de cuenta (ACC) activada	Creación automática de cuenta (ACC) desactivada	Actualización automática de cuenta (AAU) activada	Actualización automática de cuenta (AAU) desactivada
No ha activado el SSO. Las cuentas de usuario se crearon en el sistema.	Los usuarios inician sesión utilizando sus direcciones de correo electrónico y las contraseñas que hayan seleccionado.	No disponible	No disponible	No disponible	No disponible

Situación	Comportamiento de la autenticación del usuario	Creación automática de cuenta (ACC) activada	Creación automática de cuenta (ACC) desactivada	Actualización automática de cuenta (AAU) activada	Actualización automática de cuenta (AAU) desactivada
Luego, activa el SSO. Los usuarios con cuentas existentes inician sesión en sus sitios de WebEx, en las herramientas de productividad de WebEx o en la aplicación de Cisco WebEx Meetings en sus dispositivos móviles.	Los usuarios son redireccionados al sitio web de autenticación de IdP de SAML 2.0 y se les solicita que inicien sesión con sus credenciales corporativas, en lugar de con las direcciones de correo electrónico y las contraseñas que hayan seleccionado. Los usuarios inician sesión con éxito porque el IdP de SAML 2.0 los reconoce como usuarios válidos. Si no son usuarios válidos, el IdP de SAML 2.0 les informará de que no pueden utilizar WebEx Meetings Server o de que son usuarios no válidos.	No disponible	No disponible	No disponible	No disponible

Situación	Comportamiento de la autenticación del usuario	Creación automática de cuenta (ACC) activada	Creación automática de cuenta (ACC) desactivada	Actualización automática de cuenta (AAU) activada	Actualización automática de cuenta (AAU) desactivada
El SSO está activado. Los usuarios no tienen cuentas existentes en el sistema.	Lo mismo que para la situación anterior.	Luego de que los usuarios inician sesión, se crean las cuentas de usuario "bajo demanda" en Cisco WebEx Meetings Server. 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 podrán utilizar Cisco WebEx Meetings Server. El modo más fácil de corregir esta situación es que realice una de las siguientes acciones: • Deje la creación automática de cuenta (ACC) activada. • Antes de que los usuarios inicien sesión, cree cuentas de usuario de forma manual mediante "Importar archivo CSV" o "Crear usuario" desde el sitio de administración de Cisco WebEx.	No disponible	No disponible

Situación	Comportamiento de la autenticación del usuario	Creación automática de cuenta (ACC) activada	Creación automática de cuenta (ACC) desactivada	Actualización automática de cuenta (AAU) activada	Actualización automática de cuenta (AAU) desactivada
El SSO está activado. Los usuarios iniciaban sesión previamente mediante SSO y ahora vuelven a iniciar sesión.	Lo mismo que para la situación anterior.	No disponible	No disponible	Las cuentas de usuarios existentes se actualizan automáticamente con cualquier cambio en las credenciales del usuario (generalmente, nombre o apellido) siempre y cuando el campo NameID permanezca sin cambios.	No disponible

Situación	Comportamiento de la autenticación del usuario	Creación automática de cuenta (ACC) activada	Creación automática de cuenta (ACC) desactivada	Actualización automática de cuenta (AAU) activada	Actualización automática de cuenta (AAU) desactivada
Posteriormente, desactiva el SSO. Esta es una situación poco común porque los clientes tienden a dejar el SSO activado tras su activación inicial. Los usuarios iniciaban sesión previamente mediante SSO y ahora vuelven a iniciar sesión.	Si los usuarios introducen sus credenciales corporativas, no pueden iniciar sesión porque WebEx Meetings Server espera que introduzcan sus direcciones de correo electrónico y las contraseñas que hayan seleccionado. En esta situación, instruya a los usuarios acerca del restablecimiento de las contraseñas que hayan seleccionado en sus cuentas de WebEx y permítales el tiempo suficiente para actuar antes de desactivar el SSO. Después de restablecer sus contraseñas, los usuarios pueden iniciar sesión utilizando sus direcciones de correo electrónico y las contraseñas que hayan seleccionado.	No disponible	No disponible	No disponible	No disponible

Situación	Comportamiento de la autenticación del usuario	Creación automática de cuenta (ACC) activada	Creación automática de cuenta (ACC) desactivada	Actualización automática de cuenta (AAU) activada	Actualización automática de cuenta (AAU) desactivada
Caso especial: Un usuario es también un administrador del sistema. Situación A: el usuario inicia sesión en el sitio de WebEx. Situación B: el usuario inicia sesión en el sitio de administración de Cisco WebEx.		Situación A: los mismos resultados que para la situación anterior. Situación B: no disponible.	Situación A: los mismos resultados que para la situación anterior. Situación B: no disponible.	Situación A: los mismos resultados que para la situación anterior. Situación B: no disponible.	Situación A: los mismos resultados que para la situación anterior. Situación B: no disponible.

Situación	Comportamiento de la autenticación del usuario	Creación automática de cuenta (ACC) activada	Creación automática de cuenta (ACC) desactivada	Actualización automática de cuenta (AAU) activada	Actualización automática de cuenta (AAU) desactivada
	Situación A: los mismos resultados que para la situación anterior. Situación B: en contraste con el comportamiento en el sitio de WebEx, cuando el usuario inicia sesión en el sitio de administración de Cisco WebEx, siempre se le solicita que introduzca la dirección de correo electrónico y la contraseña que haya seleccionado. En otras palabras, el SSO no tiene efecto cuando inicia sesión en el sitio de administración de Cisco WebEx. Se trata de una medida de seguridad incorporada al producto debido a la necesidad de garantizar que los administradores del sistema siempre puedan iniciar sesión en el sitio de administración				

Situación	Comportamiento de la autenticación del usuario	Creación automática de cuenta (ACC) activada	Creación automática de cuenta (ACC) desactivada	Actualización automática de cuenta (AAU) activada	Actualización automática de cuenta (AAU) desactivada
	de Cisco WebEx. Si el sitio de administración de Cisco WebEx también admite SSO, el mal funcionamiento en el IdP de SAML 2.0 o una pérdida en la conectividad de red entre Cisco WebEx Meetings Server y el IdP de SAML 2.0 resultarán en una situación en la cual los administradores de los sistemas ya no podrán iniciar sesión y administrar el producto. Esta es la razón por la cual el sitio de administración de Cisco WebEx no admite SSO.				

Atributos de la aserción SAML

La siguiente tabla enumera los atributos de la aserción SAML admitidos por Cisco WebEx Meetings Server. Asegúrese de configurar los atributos lastname, firstname, email y updatetimestamp. La actualización automática no funciona al menos que esté configurado el atributo updatetimestamp.

Atributos de la aserción SAML compatibles

Nombre del atributo	Significado del atributo	Obligatorio para la creación automática de usuarios	Rango de valor de entrada	Comentarios
lastname		Sí		
firstname		Sí		
email		Sí	Formato de correo electrónico válido	
updatetimestamp	La hora actualizada de la información de usuario	No	Formato admitido **Formato largo:** Ejemplo: System.currentTimeMillis() **Formato LDIF:** yyyyMMddHHmmss yyyy-MM-dd HH:mm:ss Ejemplo: 20090115213256 **Formato UTC** ("2009-10-09T06:00:32Z")	Si falta el atributo updateTimeStamp, no puede realizar la actualización automática del usuario, normalmente asignada al elemento whenChanged si el IdP está vinculado a AD.
optionalparams		No		Los parámetros opcionales pueden establecerse en los formatos descritos en la sección "Parámetros opcionales" a continuación.
OPhoneCountry		No		Código de país del teléfono de la oficina
OPhoneArea		No		Área del teléfono de la oficina
OPhoneLocal		No	Introduzca solo caracteres numéricos. Por ejemplo, 5551212. No introduzca caracteres no numéricos como guiones o paréntesis.	Teléfono de la oficina local
OPhoneExt		No		Extensión del teléfono de la oficina
FPhoneCountry		No		Código de país del teléfono alternativo

Nombre del atributo	Significado del atributo	Obligatorio para la creación automática de usuarios	Rango de valor de entrada	Comentarios
FPhoneArea		No		Área del teléfono alternativo
FPhoneLocal		No		Teléfono alternativo local
FPhoneExt		No		Extensión del teléfono alternativo
PPhoneCountry		No		Código de país del teléfono alternativo 2
PPhoneArea		No		Área del teléfono alternativo 2
PPhoneLocal		No		Teléfono alternativo local 2
PPhoneExt		No		Extensión del teléfono alternativo 2
MPhoneCountry		No		Código de país del teléfono móvil
MPhoneArea		No		Área del teléfono móvil
MPhoneLocal		No		Teléfono móvil local
MPhoneExt		No		Extensión del teléfono móvil
TimeZone		No		Zona horaria (consulte la sección "Zonas horarias" a continuación)
Address1		No		Address1
Address2		No		Address2
City		No		City
State		No		State
ZIP Code		No		ZIP Code
País		No		País (consulte la sección "Valores de países" a continuación)
Región		No		Región (consulte la sección "Valores de regiones" a continuación)

Nombre del atributo	Significado del atributo	Obligatorio para la creación automática de usuarios	Rango de valor de entrada	Comentarios
Language		No		Idioma (consulte la sección "Valores de idiomas" a continuación)
TC1	Cadena	No	Grupo de códigos de seguimiento 1 introducido por el usuario en el sitio de administración	Índice 1
TC2	Cadena	No	Grupo de códigos de seguimiento 2 introducido por el usuario en el sitio de administración	Índice 2
TC3	Cadena	No	Grupo de códigos de seguimiento 3 introducido por el usuario en el sitio de administración	Índice 3
TC4	Cadena	No	Grupo de códigos de seguimiento 4 introducido por el usuario en el sitio de administración	Índice 4
TC5	Cadena	No	Grupo de códigos de seguimiento 5 introducido por el usuario en el sitio de administración	Índice 5
TC6	Cadena	No	Grupo de códigos de seguimiento 6 introducido por el usuario en el sitio de administración	Índice 6
TC7	Cadena	No	Grupo de códigos de seguimiento 7 introducido por el usuario en el sitio de administración	Índice 7
TC8	Cadena	No	Grupo de códigos de seguimiento 8 introducido por el usuario en el sitio de administración	Índice 8
TC9	Cadena	No	Grupo de códigos de seguimiento 9 introducido por el usuario en el sitio de administración	Índice 9

Nombre del atributo	Significado del atributo	Obligatorio para la creación automática de usuarios	Rango de valor de entrada	Comentarios
TC10	Cadena	No	Grupo de códigos de seguimiento 10 introducido por el usuario en el sitio de administración	Índice 10

Parámetros opcionales

Puede establecer el valor 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">City=Toronto</saml:AttributeValue >
- <saml:AttributeValue xsi:type="xs:string">AA=OFF</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 zonas horarias

La siguiente tabla proporciona los valores para el atributo TimeZone.

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 Hawái, 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 montaña, GMT-07:00)	5
Denver (Hora de verano de la montaña, 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

Zona horaria	Valor
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 del Oeste de Sudamérica, 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
Buenos Aires (Hora del Este de Sudamérica, GMT-03:00)	17
Atlántico medio (Hora del Atlántico medio, GMT-02:00)	18
Azores (Hora de verano de Azores, GMT)	19
Reikiavik (Hora de Greenwich, GMT)	20
Londres (Hora de verano de 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
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 Dabi, Mascate (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

Zona horaria	Valor
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
Almaty (Hora de Asia central, GMT+06:00)	43
Bangkok (Hora de Bangkok, GMT+07:00)	44
Pekín (Hora de China, GMT+08:00)	73
Perth (Hora occidental de Australia, GMT+08:00)	46
Singapur (Hora de Singapur, GMT+08:00)	47
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 central de Australia, GMT+09:30)	52
Darwin (Hora central de Australia, GMT+09:30)	53
Brisbane (Hora del Este de Australia, GMT+10:00)	54
Sídney (Hora estándar del Este de Australia, GMT+10:00)	55
Guam (Hora de 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 del Pacífico de México, GMT-07:00)	131
Chihuahua (Hora de verano de la montaña de México, GMT-06:00)	132

Zona horaria	Valor
Caracas (Hora del Oeste de Sudamérica, 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 del Este, GMT+03:00)	140
Katmandú (Hora de Nepal, GMT+05:45)	141
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 países

La siguiente tabla proporciona los valores para el atributo Country.

País	Valor
Estado Islámico de Afganistán	93
Albania	355
Argelia	213
Samoa Americana	1684
Andorra	376
Angola	244
Anguila	1264
Antártida	672_1
Antigua (incluida Barbuda)	1268
Argentina	54
Armenia	374
Aruba	297
Islas de la Ascensión	247

País	Valor
Australia	61
Austria	43
Azerbaiyán	994
Bahamas	1242
Bahréin	973
Bangladés	880
Barbados	1246
Bielorrusia	375
Bélgica	32
Belice	501
Benín	229
Bermudas	1441
Bután	975
Bolivia	591
Bosnia-Herzegovina	387
Botsuana	267
Brasil	55
Islas Vírgenes (R. U.)	1284
Brunéi	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

País	Valor
Colombia	57
Comores	269_1
Islas Cook	682
Costa Rica	506
Croacia	385
Cuba	53
Chipre	357
República Checa	420
Dinamarca	73
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 Feroe	298
Islas Malvinas	500
Islas Fiyi	679
Finlandia	358
Francia	33
Deptos. Franceses (Océano Índico)	262
Guayana Francesa	594
Polinesia Francesa	689
Gabón	241
Gambia	220
Georgia	995

País	Valor
Alemania	49
Ghana	233
Gibraltar	350
Grecia	30
Groenlandia	299
Granada	1473
Guadalupe	590
Guantánamo (Base Naval de los Estados Unidos)	53_1
Guatemala	502
Guinea	224
Guinea-Bissau	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
Kazajistán	7_1
Kenia	254
Kiribati	686

País	Valor
Corea del Norte	850
Corea del Sur	82
Kuwait	965
Kirguistán	996
Laos	856
Letonia	371
Líbano	961
Lesoto	266
Liberia	231
Libia	218
Liechtenstein	423
Lituania	370
Luxemburgo	352
Macao	853
Macedonia	389
Madagascar	261
Malaui	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

País	Valor
Marruecos	212
Mozambique	258
Birmania	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
Pakistán	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

País	Valor
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 Nevis	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
Tayikistán	992
Tanzania	255
Tailandia	66
Togo	228

País	Valor
Islas Tonga	676
Trinidad y Tobago	1868
Túnez	216
Turquía	90
Turkmenistán	993
Turcas 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
Zimbabue	263

Valores de regiones

La siguiente tabla proporciona los valores para el atributo Region.

Región	Valor
EE. UU.	2
Australia	3
Canadá	4
Canadá francófona	5

Región	Valor
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
Países Bajos	27
Rusia	28
India	29

Valores de idiomas

La siguiente tabla proporciona los valores para el atributo Language.

Language	Valor
Castellano	11
Holandés	14
Inglés	1
Francés	7

Language	Valor
Alemán	9
Italiano	10
Japonés	5
Coreano	6
Español latinoamericano	12
Portugués	15
Ruso	16
Chino simplificado	3
Chino tradicional	4

CAPÍTULO 9

Grabaciones de reuniones

Las grabaciones de reuniones ocupan espacio en su servidor de almacenamiento. Esta sección describe los umbrales del servidor de almacenamiento, las alarmas, el consumo de las grabaciones de reuniones del espacio del servidor de almacenamiento y el proceso de depuración de registros antiguos.

- Acerca de las grabaciones de reuniones, página 185
- Almacenamiento recomendado para los archivos de copia de seguridad, página 186

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 espacio de almacenamiento configurado. Debe archivar periódicamente las grabaciones guardadas en otros medios, si su organización requiere que conserve las grabaciones de reuniones durante más de seis meses.

La siguiente tabla proporciona un cálculo general de la cantidad de espacio de almacenamiento necesario para una hora de grabaciones de reuniones. Use estos valores para calcular aproximadamente la cantidad de espacio de almacenamiento necesaria para seis mesas de grabaciones de reuniones.

Contenido de la reunión	Espacio de almacenamiento aproximado necesario para una hora de grabaciones de reuniones
Compartición de aplicaciones	36 MB
Voz	30 MB
Vídeo 180p	104 MB
Vídeo 360p	337 MB

Nota Los vídeos de la cámara web se almacenan en la resolución original para la grabación de la reunión. Sin embargo, al reproducir la grabación, la resolución de vídeo se restringe a vídeo 180p.

Su sistema realiza dos tareas para mantener el espacio de grabación:

- Después de seis meses, elimina las grabaciones configuradas para ser eliminadas por sus usuarios.
- Elimina las grabaciones que fueron configuradas para ser eliminadas antes de los seis meses si sus grabaciones superan un umbral determinado durante un período de tres meses.

Cuando un usuario elimina una grabación, esta ya no está disponible desde la interfaz del usuario, pero se mantiene en el almacenamiento por seis meses. Por lo tanto, aún puede acceder al servidor de almacenamiento para copiar, realizar una copia de seguridad o utilizar los archivos de las grabaciones por seis meses después de que el usuario los haya seleccionado para su eliminación, pero deberá comunicarse con el Centro de ayuda técnica de Cisco (TAC) para recuperar la grabación.

Como punto inicial, asigne 1 TB de espacio de almacenamiento para almacenar seis meses de grabaciones de reuniones. Si las grabaciones de su sistema consumen más de un 75 por ciento del espacio asignado luego de tres meses, el sistema elimina automáticamente los primeros 10 archivos que el usuario configuró para ser eliminados.

Por ejemplo, si un usuario elimina dos archivos hoy, cinco archivos mañana y nueve archivos pasado mañana, y el uso del almacenamiento supera el límite del 75 por ciento después de 3 meses, el sistema elimina los primeros dos archivos de hoy, los siguientes cinco archivos de mañana y, luego, los primeros tres eliminados pasado mañana.

Nota Si un usuario sin quererlo elimina una grabación de la página de grabaciones de reuniones de Cisco WebEx, pero la grabación se guarda en el servidor de almacenamiento del sistema de archivos en red (NFS), comuníquese con el Centro de ayuda técnica de Cisco (TAC) para obtener ayuda para recuperar la grabación.

Almacenamiento recomendado para los archivos de copia de seguridad

Archivos de copia de seguridad de Cisco WebEx Meetings Server

La recomendación general para la cantidad de almacenamiento requerido para las copias de seguridad del sistema, que no incluye las grabaciones de reuniones es, como mínimo, 900 MB o espacio suficiente para acomodar hasta tres archivos de copia de seguridad. El sistema automáticamente purga los archivos de copia de seguridad más antiguos y almacena solo la copia de seguridad más reciente.

Tenga en cuenta las siguientes consideraciones al determinar el espacio de almacenamiento necesario para las copias de seguridad:

- El número de usuarios
- El número promedio de reuniones que se llevan a cabo cada día
- El tamaño de su base de datos, que crecerá con el tiempo
- Con las implementaciones de alta disponibilidad, puede haber retrasos en el transporte diario de transacciones debido a la latencia de red o a una alta carga del sistema durante la replicación de datos. Esto puede aumentar el tamaño de un archivo de copia de seguridad.

Controlar el tamaño de la copia de seguridad en la consola mostrará los requisitos aproximados para el tamaño de almacenamiento. Deje suficiente espacio en el servidor de almacenamiento para cubrir, como mínimo, tres veces el tamaño de la copia de seguridad observado.

CAPÍTULO 10

Compatibilidad con MIB y alarmas de SNMP

Esta sección describe las MIB disponibles en su sistema. Al acceder a sus datos MIB, se expondrán las MIB adicionales no enumeradas en esta sección. Las MIB adicionales que expone en el proceso son, principalmente, utilizadas de forma interna para tareas como la administración entre máquinas virtuales. Cisco no admite la supervisión de SNMP por parte del cliente que utilice estas MIB, ni tampoco hay garantía alguna de que estas MIB se utilizarán en versiones futuras de Cisco WebEx Meetings Server.

- MIB de SNMP admitidas, página 189
- Alarmas de SNMP admitidas, página 195

MIB de SNMP admitidas

Las siguientes secciones describen las MIB de SNMP admitidas por Cisco WebEx Meetings Server.

Información del 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 de host. El uso total de CPU contiene el uso de CPU del usuario, el uso de CPU del sistema y el uso de CPU de nice. El tiempo de CPU del usuario: el tiempo de CPU utilizado en el espacio del usuario. El tiempo de CPU del sistema: el tiempo de CPU utilizado en espacio del kernel. El tiempo de CPU de nice: el tiempo de CPU utilizado en procesos de prioridad baja.
cwCommCPUUsageWindow	Gauge32	RW	.1.3.6.1.4.1.9.9.809.1.2.1.2	Este objeto controla la duración (en segundos) que se debe esperar antes de enviar una notificación (alarma) después de pasar un umbral de uso de CPU. La notificación se envía solamente si el uso de CPU pasa el nivel (normal/menor/mayor) de un umbral y permanece en el nuevo nivel de umbral durante la duración definida en esta ventana.
cwCommCPUTotalNumber	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.3	Este objeto proporciona la cantidad total de CPU en el sistema.
cwCommCPUUsageTable	No disponible	No accesible	.1.3.6.1.4.1.9.9.809.1.2.1.4	Una lista del 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 solo identifica una CPU en la tabla. Cada CPU tiene su propio uso y sus propios valores subdivididos.
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 3.00 GHz.
cwCommCPUUsage	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.3	Este objeto proporciona el porcentaje de los recursos de CPU totales utilizado. Generalmente, se utiliza GHz para medir la energía de la CPU. Ya que GHz es demasiado grande como 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, inactivo, nice, usuario) para obtener los KHz de CPU de cada categoría. KHz se utiliza como la unidad para todas las categorías de CPU a continuación.
cwCommCPUUsageUser	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.4	Este objeto proporciona la energía 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 proporciona la energía de la CPU utilizada en procesos de baja prioridad. Nice es un programa que puede encontrarse en UNIX y Linux. Se asigna directamente a una llamada de kernel del mismo nombre. Nice se utiliza para invocar una utilidad o una secuencia de comandos shell con una prioridad en particular, lo que le asigna 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 proporciona la energía de la CPU utilizada en el modo kernel.
cwCommCPUUsageIdle	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.7	Este objeto proporciona la energía de la CPU en el estado inactivo.
cwCommCPUUsageIOWait	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.8	Este objeto proporciona la energía de la CPU utilizada cuando se espera que se complete una E/S de disco.
cwCommCPUUsageIRQ	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.9	Este objeto proporciona la energía de la CPU utilizada cuando se gestiona una solicitud de interrupción.
cwCommCPUUsageSoftIRQ	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.10	Este objeto proporciona la energía de la CPU utilizada cuando se gestiona una solicitud de interrupción de software.

Objeto	Tipo	Privilegios de lectura/ escritura	OID	Descripción
cwCommCPUUsageSteal	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.11	Este objeto proporciona la energía de la CPU utilizada en otras tareas cuando se ejecuta en un entorno virtualizado.
cwCommCPUUsageCapacitySubTotal	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.12	Este objeto proporciona la energía total actual de la CPU.
cwCommCPUMonitoringStatus	Cadena	RO	.1.3.6.1.4.1.9.9.809.1.2.1.5	Este objeto proporciona el estado de control 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 proporciona la capacidad total de la CPU.

Información acerca de la 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 la memoria física de la máquina virtual.
cwCommMEMMonitoringStatus	Cadena	RO	.1.3.6.1.4.1.9.9.809.1.2.2.2	Este objeto proporciona el estado de control del recurso de la memoria: • Cerrado (0): recurso no disponible. • Abierto (1): recurso disponible.

Objeto	Tipo	Privilegios de lectura/ escritura	OID	Descripción
cwCommMEMTotal	Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.2.3	Este objeto proporciona 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 proporciona el uso de la memoria física del host (en porcentaje) y el uso de la memoria de intercambio.
cwCommMEMSwapMonitoringStatus	Cadena	RO	.1.3.6.1.4.1.9.9.809.1.2.3.2	Este objeto proporciona el estado de control de la memoria y de la memoria de intercambio. • Cerrado (0): el estado de la memoria y de la memoria de intercambio es disponible. • Abierto(1): el estado de la memoria y de la memoria de intercambio es no disponible.

Uso del 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 el recuento de cuántos discos (por ejemplo, disco local, disco remoto, disco de la grabación de reuniones) se encuentran 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 las entradas en la tabla que contiene información de administración genérica para el uso del disco.

Objeto	Tipo	Privilegios de lectura/ escritura	OID	Descripción
cwCommDiskPartitionName	Cadena	RO	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.2	Este objeto proporciona 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 actual del disco (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 proporciona el tamaño total del espacio de disco (en MB) de este host.
cwCommDiskMonitoringStatus	Cadena	RO	1.3.6.1.4.1.9.9.809.1.2.5.3	Este objeto proporciona el estado de control de los recursos del disco. • Cerrado (0): el estado del uso del disco es no disponible. • Abierto (1): el estado del uso del disco es disponible.

Alarmas de SNMP admitidas

Las siguientes secciones describen las alarmas de SNMP admitidas por Cisco WebEx Meetings Server.

Eventos de notificación

A continuación, se presentan los eventos de notificación compatibles.

Nombre	OID	Descripción
cwCommSystemResourceUsageNormalEvent	.1.3.6.1.4.1.9.9.809.0.1	Esta notificación indica que algunos usos de los recursos del sistema cambian al estado normal. El sistema puede enviar esta notificación una vez que ocurra uno de los siguientes casos: **1** El valor de cwCommCPUUsage de una CPU cambia a uno menor que el valor del umbral menor predefinido de CPU. **2** El valor de cwCommMEMUsage cambia a uno menor que el valor del umbral menor predefinido de MEM. **3** El valor de cwCommMEMSwapUsage cambia a uno menor que el valor del umbral menor predefinido de MEM Swap. **4** El valor de cwCommFileUsage cambia a uno menor que el valor del umbral menor predefinido del archivo. **5** El valor de cwCommDiskUsage en un disco cambia a uno menor que el valor del umbral menor predefinido del disco.

Nombre	OID	Descripción
cwCommSystemResourceUsageMinorEvent	.1.3.6.1.4.1.9.9.809.0.2	Esta notificación indica que algunos usos de los recursos del sistema cambian al estado menor. El sistema puede enviar esta notificación una vez que ocurra uno de los siguientes casos: **1** El valor de cwCommCPUUsage de una CPU cambia a uno mayor o igual que el valor del umbral menor predefinido de CPU y es menor que el valor de cwCommCPUMajorThreshold. **2** El valor de cwCommMEMUsage cambia a uno mayor o igual que el valor del umbral menor predefinido de MEM y es menor que el valor del umbral mayor predefinido de MEM. **3** El valor de cwCommMEMSwapUsage cambia a uno mayor o igual que el valor del umbral menor predefinido de MEM Swap y es menor que el valor del umbral mayor predefinido de MEM Swap. **4** El valor de cwCommFileUsage cambia a uno mayor o igual que el valor del umbral menor predefinido del archivo y es menor que el valor del umbral mayor predefinido del archivo. **5** El valor de cwCommDiskUsage de uno de los discos cambia a uno mayor o igual que el valor del umbral menor predefinido del disco y es menor que el valor del umbral mayor predefinido del disco. La notificación menor significa que el sistema tiene algunos problemas y que el administrador del sistema debe resolverlos.

Nombre	OID	Descripción
cwCommSystemResourceUsageMinorEvent	.1.3.6.1.4.1.9.9.809.0.3	Esta notificación indica que algunos usos de los recursos del sistema cambian al estado mayor. El sistema puede enviar esta notificación una vez que ocurra uno de los siguientes casos: **1** El valor de cwCommCPUUsage de una CPU cambia a uno mayor o igual que el valor del umbral mayor predefinido de CPU. **2** El valor de cwCommMEMUsage cambia a uno mayor o igual que el valor del umbral mayor predefinido de MEM. **3** El valor de cwCommMEMSwapUsage cambia a uno mayor o igual que el valor del umbral mayor predefinido de MEM Swap. **4** El valor de cwCommFileUsage cambia a uno mayor o igual que el valor del umbral mayor predefinido del archivo. **5** El valor de cwCommDiskUsage de un disco cambia a uno mayor o igual que el valor del umbral mayor predefinido del disco. La notificación mayor significa que el estado del sistema es crítico y que el administrador del sistema debe tomar medidas inmediatamente.

Datos de las alarmas

A continuación, se presentan los datos las alarmas compatibles. Configure su filtro MIB para únicamente recibir las alarmas que se describen a continuación.

Nombre	OID	Convención textual	Descripción
cwCommNotificationHostAddressType	.1.3.6.1.4.1.9.9.809.1.2.4.1	InetAddressType	Este objeto representa el tipo de 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	Convención 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 dicho recurso del sistema tiene niveles que sobrepasan los niveles de advertencia predefinidos. 0. cwCommTtoalCPUUsage 1. cwCommMemUsage 2. cwCommMemSwapUsage 3. descriptor de archivo abierto (sin datos MIB) 4. uno de cwCommDiskTotal
cwCommNotificationResValue	.1.3.6.1.4.1.9.9.809.1.2.4.4	Unsigned32	Este objeto proporciona el valor del porcentaje de uso de los recursos del sistema con la 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 seguir el orden de las notificaciones.

CAPÍTULO 11

Requisitos del sistema del usuario

Los requisitos del sistema para los usuarios finales para organizar y obtener acceso a reuniones.

- Requisitos del sistema de PC comunes, página 201
- Requisitos del sistema operativo Windows, página 202
- Requisitos para el sistema operativo Mac, página 205
- Requisitos de los sistemas operativos de los dispositivos móviles, página 205
- Matriz de compatibilidad de las herramientas de productividad y la aplicación Cisco WebEx Meetings, página 206

Requisitos del sistema de PC comunes

Requisitos del sistema Cisco WebEx Meeting Server (CWMS) comunes a los exploradores y los sistemas operativos.

Requisitos de clientes y exploradores

- JavaScript y cookies habilitadas
- Java 6 y Java 7 (para los exploradores web que son compatibles con Java) habilitados
- Complementos de Cisco WebEx habilitados para Chrome 32 y las versiones posteriores y Firefox 27 y las versiones posteriores
- Complementos habilitados en Safari
- Active X habilitado y desbloqueado para Microsoft Internet Explorer (recomendado)

Nota Debido a cambios en las políticas de Google y Mozilla, a partir de Chrome 32 y Firefox 27, es posible que los usuarios deban activar manualmente el complemento de WebEx al usar estos exploradores[21] para entrar a una reunión de WebEx o para reproducir una grabación de WebEx. En https://support.webex.com/webex/meetings/en_US/chrome-firefox-join-faq.htm puede encontrar más información e instrucciones.

Si un cliente usa un explorador diferente a las versiones especificadas de Chrome o Firefox y tiene Java habilitado, la aplicación Cisco WebEx Meetings se descargará automáticamente en el sistema del cliente la primera vez que el cliente inicie o entre a una reunión. Le recomendamos que les indique a todos los clientes que instalen la actualización más reciente de la versión de Java.

Requisitos de SSL y TLS

Configure la **Configuración de Internet** en todas las computadoras de sus usuarios con cifrado SSL y TLS. Por ejemplo, en una PC de Windows:

- Seleccione **Panel de control** > **Opciones de Internet** > **Avanzadas** > **Seguridad** > **Usar SSL 3.0**. Recomendamos seleccionar esta opción para obtener máxima compatibilidad.
- Seleccione**Panel de control** > **Opciones de Internet** > **Avanzadas** > **Seguridad** > **Usar TLS 1.0** y **Usar TLS 1.2**. Recomendamos seleccionar ambas opciones para la máxima compatibilidad, pero debe seleccionar **Usar TLS 1.0**.

Si los usuarios organizarán reuniones para invitados (por ejemplo, personas que no trabajan para su empresa), usted debe informar a sus usuarios invitados que deben actualizar manualmente sus sistemas operativos y exploradores para que admitan SSL y TLS antes de entrar a las reuniones. Si no realizan estos pasos, tendrán problemas de compatibilidad. Se recomienda incluir las instrucciones anteriores en las invitaciones a reuniones. Esto se puede hacer editando las invitaciones a reuniones adecuadas disponibles en el sitio de administración en **Configuración** > **Correo electrónico** > **Plantillas.**.

Requisitos del sistema operativo Windows

Sistemas operativos Windows compatibles

- Windows Vista (32 bits/64 bits)
- Windows 7 (32 bits/64 bits)
- Windows 8 (32 bits/64 bits)
- Windows 8.1 (32 bits/64 bits)

Requisitos de hardware de Windows

Procesador Intel Core2 Duo o AMD CPU 2.XX GHz o superior.

Se recomienda un mínimo de 2 GB de RAM.

21 Las versiones exactas de Chrome y Firefox a las cuales afecta esta política no se han finalizado al momento de la publicación de este documento.

Exploradores de Windows comprobados

- Internet Explorer: 8 a 11 (32 bits/64 bits)

Nota IE 11 se probó únicamente en Windows 7 SP1 and Windows 8.1

- Mozilla Firefox: 10 - 32
- Google Chrome: 23 - 37

Integración con Microsoft Outlook

- Microsoft Outlook 2007 SP2 y posterior
- Microsoft Outlook 2010 (ediciones de 32 bits y 64 bits; todos los Service Packs)
- Microsoft Outlook 2013

En la siguiente tabla se describen las versiones de Microsoft Outlook compatibles con cada sistema operativo.

Versión de Microsoft Outlook (Client/Exchange Server)	Windows XP SP3	Vista	Windows 7	Windows 8 (solo modo de 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 hospedado	N	N	S	S
Outlook 2013/Exchange 2013	N	N	S	S

Versión de Microsoft Outlook (Client/Exchange Server)	Windows XP SP3	Vista	Windows 7	Windows 8 (solo modo de escritorio)
Outlook 2013/Exchange 365 hospedado	N	N	S	S

Clientes de programas de mensajería instantánea compatibles

- Lync 2010 (32 bits)
- Lync 2013 (32 bits)
- Microsoft Office Communicator 2007
- Microsoft Office Communicator 2007 R2

En la siguiente tabla se describen las versiones de los clientes de programas de mensajería instantánea compatibles con cada sistema operativo.

Versión del programa de mensajería instantánea	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 de Cisco Jabber para Windows

- Cisco Jabber para Windows 9.2.6
- Cisco Jabber para Windows 9.6.1
- Cisco Jabber for Windows 9.7
- Cisco Jabber for Windows 10.5
- Compatible con Cisco WebEx Meetings Server con integración de LDAP/Active Directory.

Restricción Jabber para Windows 9.2.6 es compatible con la integración con sitios de Cisco WebEx Meetings Server 1.5 y los sitios 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 el inicio de sesión único.

No todas las versiones o plataformas de Cisco Jabber admiten la integración con Cisco WebEx Meetings Server. (Por ejemplo, WebEx Communicator y Jabber basado en la nube). Para obtener más información

sobre 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 para el sistema operativo Mac

Sistemas operativos MAC compatibles

- Mac OS X 10.6 Snow Leopard
- 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.

Exploradores de Mac comprobados

- Mozilla Firefox: 10 - 32
- Apple Safari: 6 y 7
- Google Chrome: 23 - 37

Integración de Cisco Jabber for Mac

Las siguientes integraciones de Cisco Jabber for Mac son compatibles con los sitios de Cisco WebEx Meetings Server configurados para el inicio de sesión único (SSO) SAML 2.0 o LDAP/Active Directory.

- Cisco Jabber for Mac 10.5 admite la integración con la versión 2.5 y posteriores de Cisco WebEx Meetings Server.
- Cisco Jabber for Mac 9.6 admite la integración con la versión 2.0 y posteriores de Cisco WebEx Meetings Server.

Requisitos de los sistemas operativos de los dispositivos móviles

Después de descargar manualmente la aplicación Cisco WebEx en iOS o Android y de activar la característica móvil de WebEx, un usuario puede usar la aplicación para iniciar o asistir a una reunión. Un usuario también puede obtener acceso a Cisco WebEx en un dispositivo móvil usando un explorador, pero es probable que no tenga la misma experiencia de usuario óptima.

Cisco WebEx Meeting Server versión 2.0 y las versiones posteriores admiten lo siguiente:

- iPhone y iPad de Apple con iOS 6.0 y versiones posteriores.

- Dispositivos móviles Android con Android 2.1 y versiones posteriores.
- Jabber for iPhone y Jabber for Android 9.6 y versiones posteriores.

Nota No puede reproducir grabaciones en un dispositivo móvil. Si inició una reunión en un dispositivo móvil de Android, puede iniciar y administrar la grabación de una reunión. Si inició una reunión en un dispositivo móvil de iOS, no puede iniciar y administrar la grabación de una reunión en el dispositivo iOS.

Matriz de compatibilidad de las herramientas de productividad y la aplicación Cisco WebEx Meetings

En la tabla se detallan los números de compilación para las descargas de las herramientas de productividad y la aplicación WebEx Meetings para cada versión de Cisco WebEx Meetings Server.

Nota Cuando mira las páginas **Acerca de** de las herramientas de productividad de WebEx y de la aplicación WebEx Meetings, los últimos tres dígitos de la información de la versión que se muestran en estas páginas deben coincidir con los últimos tres dígitos de los números de la versión incluidos en la siguiente tabla. Por ejemplo, en el caso de la versión de Cisco WebEx Meetings Server 2.0 MR4, debe mirar los dígitos 407.

Versión de Cisco WebEx Meetings Server	Número ISO	Herramientas de productividad de Cisco WebEx[22]	Aplicación Cisco WebEx Meetings
1.5	1.5.1.6	2.80.500.179	27.32.150.179
1.5 HF1	1.5.1.57	2.80.501.52	27.32.151.52
1.5 HF2	1.5.1.65/1.5.1.68	2.80.501.52	27.32.151.52
1.5 HF4	1.5.1.68/1.5.1.69	2.80.501.52	27.32.151.52
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)

Versión de Cisco WebEx Meetings Server	Número ISO	Herramientas de productividad de Cisco WebEx[22]	Aplicación Cisco WebEx Meetings
2.0	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	2.80.1.507	27.32.201.507 (Windows) orion2.0.MR5.0.0.507 (Mac)

22 Los usuarios pueden encontrar más información en las herramientas de productividad de Cisco WebEx en http://www.webex.com/support/productivity-tools.html.