Guía de administración de Cisco WebEx Meetings Server, versión 2.0

Primera publicación: 06 de febrero 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

Guía de instalación de Cisco WebEx Meetings Server 1

Utilización de VMware vSphere con su sistema 3

Utilización de VMware vSphere 3

Configurar el host ESXi para usar un servidor NTP 4

Creación de una copia de seguridad por medio de VMware vCenter 4

Tomar una Instantánea utilizando VMware vCenter 5

Adjuntar un archivo VMDK existente a una nueva máquina virtual 6

Lista de comprobación de comunicaciones de red para el sistema 11

Lista de comprobación de comunicaciones de red para un sistema con acceso público y horizonte DNS no dividido 11

Lista de comprobación de comunicaciones de red para un sistema con acceso público y horizonte DNS dividido 12

Lista de comprobación de comunicaciones de red para un sistema sin acceso público 12

Instalación de su sistema usando el despliegue automático 13

Conceptos generales sobre el despliegue de su sistema 14

Lista de comprobación de instalación 15

Información necesaria para un despliegue automático 16

Desplegar el archivo OVA desde un cliente VMware vSphere 18

Comprobación de la configuración de comunicaciones de red después de un despliegue OVA incorrecto 30

Seleccionar su idioma para la configuración 30

Confirmar el despliegue 31

Confirmar el tamaño de su sistema 31

Seleccionar el sistema para instalar 31

Seleccionar el tipo de despliegue de sistema 32

Proporcionar las credenciales de VMware vCenter 32

Seleccionar la configuración de vCenter para su máquina virtual multimedia 33

Introducir la información de comunicaciones de red para la máquina virtual multimedia 33

Agregar acceso público 34

Seleccionar los ajustes de vCenter para su máquina virtual de proxy inverso de Internet 34
Introducir la información de comunicaciones de red para el proxy inverso de Internet 35
Introducir la dirección VIP pública 36
Introducir la dirección VIP privada 36
URL del sitio de WebEx y URL de administración de WebEx 37
Introducción de las URL del sitio de WebEx y de administración de WebEx 38
Confirmación de que la red está configurada correctamente 38
Desplegar sus máquinas virtuales 39
Comprobación de su sistema 39
Instalar su sistema utilizando el despliegue manual 41
Conceptos generales sobre el despliegue de su sistema 41
Lista de comprobación de instalación 42
Información necesaria para un despliegue manual 43
Desplegar el archivo OVA desde un cliente VMware vSphere 45
Comprobación de la configuración de comunicaciones de red después de un despliegue OVA incorrecto 57
Seleccionar su idioma para la configuración 57
Confirmar el despliegue 58
Confirmar el tamaño de su sistema 58
Seleccionar el sistema para instalar 58
Seleccionar el tipo de despliegue de sistema 59
Agregar acceso público 59
Introducir la dirección VIP pública 60
Introducir la dirección VIP privada 61
URL del sitio de WebEx y URL de administración de WebEx 61
Introducción de las URL del sitio de WebEx y de administración de WebEx 62
Confirmación de que la red está configurada correctamente 63
Desplegar sus máquinas virtuales 63
Comprobación de su sistema 64
Configurar el servidor de correo, la zona horaria y la configuración regional 67
Definición del servidor de correo para su sistema 67
Definición de la zona horaria y la configuración regional para el sistema 68
Confirmación de los ajustes de servidor de correo, zona horaria y configuración regional 68
Definición de la primera cuenta de administrador para su sistema 68

Prueba del sistema 69

Modificación del sistema después de la instalación 71

Agregar HA, actualizar o ampliar el sistema 71

Preparación para un procedimiento de modificación del sistema 72

Agregar un sistema de alta disponibilidad 75

Agregar un sistema HA usando el despliegue automático 75

Agregar un sistema HA usando el despliegue manual 77

Comprobar que la versión de su sistema principal y el sistema de alta disponibilidad son la misma 79

Agregar un sistema de alta disponibilidad 81

Prueba del sistema 82

Ampliar su sistema a un tamaño de sistema superior 83

Preparación para la ampliación del sistema 83

Preparación para un procedimiento de modificación del sistema 84

Ampliación del sistema usando el despliegue automático 85

Ampliación del sistema usando el despliegue manual 89

Prueba del sistema 93

Actualización del sistema 95

Actualización del sistema 95

Conexión a una imagen ISO desde la unidad CD/DVD 96

Continuar con el proceso de actualización 97

Completar la actualización 98

Actualización del sistema 101

Preparación de una actualización 101

Actualización automática del sistema 102

Actualización manual del sistema 105

Prueba del sistema 107

Realojamiento y actualización de las licencias 108

Acceder al formulario de solicitud de GLO 108

Realojamiento de licencias después de una actualización de software o la expansión del sistema 108

Guardar una solicitud de licencia 109

Registrar licencias que se realojarán 109

Actualizar las licencias después de una actualización del software 110

Guía de configuración de Cisco WebEx Meetings Server 113

Utilización del escritorio 115

Acerca de su escritorio 115

Ver y editar alarmas 118

Visualización del historial de recursos 120

Uso del gráfico Reuniones en curso para tratar problemas de reuniones 120

Visualización de tendencias de reunión 121

Ver la lista de reuniones 122

Planificación de una ventana de mantenimiento 123

Cambiar una ventana de mantenimiento planificada 124

Acerca del modo de mantenimiento 125

Activar o desactivar el modo de mantenimiento 128

Administrar usuarios 131

Acerca de la administración de usuarios 131

Acerca de los archivos delimitados por comas y tabulaciones 132

Valores de los campos de los archivos CSV 134

agregar usuarios 138

Edición de usuarios 138

Activación de usuarios 139

Desactivación de usuarios 139

Desactivación de usuarios usando la importación 140

Importar usuarios 140

Exportando usuarios 141

Importar usuarios a un nuevo sistema mediante un archivo exportado 141

Configuración de códigos de seguimiento 142

Modificación de los códigos de seguimiento 143

Configuración de la integración de directorios 144

Sincronizar grupos de usuarios 149

Utilización de CUCM para configurar el servicio Web de AXL y la sincronización de directorios 150

Utilización de CUCM para configurar la autenticación y la integración LDAP 150

Enviar correos electrónicos a usuarios 151

Configurar su sitio 153

Configuración de las propiedades del sistema 153

Cambiar la configuración de su máquina virtual 153

Configuración de un sistema de alta disponibilidad 154

Agregar un sistema de alta disponibilidad 154
Eliminar un sistema de alta disponibilidad 156
Comportamiento del sistema después de un fallo de componente 156
Cambiar su dirección IP virtual 158
Configuración del acceso público 158
Agregar el acceso público a su sistema 158
Eliminar el acceso público 160
Expandir el tamaño del sistema 161
Configuración de los ajustes generales 161
Cambiar la configuración de su sitio 162
Cambiar la configuración de administración 162
Configuración de servidores 163
Configurar un servidor de correo 163
Configuración de un servidor SMTP 164
Configuración de un servidor de almacenamiento 164
Utilizar la función de recuperación ante desastres 166
Configuración de los ajustes SNMP 169
Configuración de las cadenas de comunidad 169
Agregar cadenas de comunidad 170
Editar las cadenas de comunidad 171
Configuración de usuarios USM 171
Agregar usuarios USM 172
Edición de usuarios USM 173
Configuración de los destinos de notificación 174
Edición de un destino de notificación 175
Configuración de los destinos de notificación 175
Administración de licencias 176
Acerca de las licencias 176
Tramitación de licencias utilizando el Administrador de licencias 183
Tramitar licencias utilizando eFulfilment 184
Tramitar licencias poniéndose en contacto con TAC 186
Configuración de ajustes 187
Configuración de la información de su empresa 188
Configuración de los ajustes de personalización 189
Eliminar un logotipo de empresa 190

Configuración de sus ajustes de reuniones 190
Acerca de la seguridad de la reunión 191
Acerca de configurar sus ajustes de audio 193
Configuración de los ajustes de audio por primera vez 193
Configuración de los ajustes de audio 195
Configuración de los ajustes de vídeo 197
Configuración de sus ajustes móviles 198
Configuración de la calidad del servicio (QoS) 198
Acerca de la marca de QoS 199
Configuración de contraseñas 200
Configuración de sus ajustes generales de contraseña 200
Configuración de los ajustes de contraseña de usuario 201
Configuración de sus contraseñas de la reunión 202
Configuración de sus ajustes de correo electrónico 204
Acerca de las plantillas de correo electrónico 205
Configuración de los ajustes de descarga 224
Acerca de las descargas 225
Administración de certificados 226
Generar certificados SSL 226
Generar una solicitud de firma de certificado (CSR) 227
Importar un certificado SSL 228
Exportar un certificado SSL 229
Exportar un certificado SSL para dispositivos móviles 230
Descarga de su clave privada y su CSR 231
Generación de un certificado autofirmado 231
Restauración de un certificado SSL 232
Importar certificados de SSO IdP 234
Importación de certificados seguros de teleconferencia 234
Configuración de la seguridad de sesión de usuario 235
Configurar los ajustes de autenticación única (SSO) 236
Desactivar SSO 239
Configuración de las funciones de la nube 240
Configuración de la seguridad de la máquina virtual 240
Actualizar sus claves de cifrado 240
Acerca de FIPS 241

Activación del cifrado compatible con FIPS 242
Desactivación del cifrado compatible con FIPS 242
Gestionar sus informes 243
Descargar informes mensuales 243
Acerca de los informes mensuales 244
Generar informes detallados personalizados 246
Acerca de los informes de detalles personalizados 246
Usar las funciones de soporte 251
Personalizar el registro 251
Definir una cuenta de Remote Support 252
Desactivación de una cuenta de Remote Support 253
Utilización de la prueba de las reuniones 254
Utilización de la prueba de recursos del sistema 254

PARTE I

Guía de instalación de Cisco WebEx Meetings Server

- Utilización de VMware vSphere con su sistema, página 3
- Lista de comprobación de comunicaciones de red para el sistema, página 11
- Instalación de su sistema usando el despliegue automático, página 13
- Instalar su sistema utilizando el despliegue manual, página 41
- Configurar el servidor de correo, la zona horaria y la configuración regional, página 67
- Modificación del sistema después de la instalación, página 71
- Agregar un sistema de alta disponibilidad, página 75
- Ampliar su sistema a un tamaño de sistema superior, página 83
- Actualización del sistema, página 95
- Actualización del sistema, página 101

CAPÍTULO 1

Utilización de VMware vSphere con su sistema

- Utilización de VMware vSphere, página 3
- Configurar el host ESXi para usar un servidor NTP, página 4
- Creación de una copia de seguridad por medio de VMware vCenter, página 4
- Tomar una Instantánea utilizando VMware vCenter, página 5
- Adjuntar un archivo VMDK existente a una nueva máquina virtual, página 6

Utilización de VMware vSphere

Las máquinas virtuales para su sistema se despliegan con VMware vSphere. Cisco WebEx Meetings Server debe estar instalado en las máquinas virtuales VMware, con las siguientes restricciones:

- Use VMware vSphere 5.0, 5.0 actualización 1, o 5.1.

  Las versiones anteriores de vSphere no son compatibles.

- Use VMware ESXi 5.0, 5.0 actualización 1, o 5.1.

  El uso de versiones anteriores de ESXi provoca la aparición de mensajes de error confusos sobre **hardware no compatible** que no describen explícitamente el problema.

- Compruebe que el servidor DNS configurado en el host ESXi puede resolver los nombres de host de las máquinas virtuales que están desplegadas en ese host ESXi.
- Debe utilizar VMware vCenter para administrar los hosts ESXi en los que se despliegue el sistema de Cisco WebEx Meetings Server.
- Cuando apague una máquina virtual, seleccione siempre **Encendido** > **Apagar invitado** en cada máquina virtual. (No utilice la opción **Apagar**.

Nota Para obtener detalles sobre las configuraciones admitidas de VMware, consulte los *Requisitos de sistema de Cisco WebEx Meetings Server*.

Configurar el host ESXi para usar un servidor NTP

El sistema utiliza el host ESXi para definir la hora. Configure el host ESXi para usar el Protocolo de hora de red (NTP) para la sincronización del reloj.

Nota Este es un procedimiento de alto nivel. Para instrucciones detalladas, consulte su documentación de VMware ESXi.

Importante Asegúrese de configurar la configuración NTP del host ESXi.

Procedimiento

Paso 1 Utilizando su cliente vSphere, seleccione el host ESXi en el panel de inventario.

Paso 2 Seleccione la pestaña **Configuration** y seleccione **Time configuration** en la sección Software.

Paso 3 Seleccione **Properties** en la parte superior derecha del panel.

Paso 4 Seleccione **NTP Client Enabled**.

Paso 5 Seleccione **Options** para configurar los ajustes del servidor NTP.
Cisco recomienda que seleccione **Start and stop with host** para reducir la posibilidad de que el tiempo del host ESXi sea incorrecto.

Creación de una copia de seguridad por medio de VMware vCenter

Las copias de seguridad son sistemas de archivos tradicionales que aprovechan la tecnología de VMware y la transferencia de datos basada en SAN. La Recuperación de datos de VMware® Data Recovery crea copias de seguridad de máquinas virtuales sin interrumpir su uso o los datos y servicios que proporcionan. La Recuperación de datos utiliza un dispositivo de máquina virtual y un complemento de cliente para gestionar y restaurar copias de seguridad. El dispositivo de copia de seguridad se proporciona en formato de virtualización abierto (OVF). El complemento de Recuperación de datos requiere el Cliente de VMware vSphere.

La Recuperación de datos gestiona las copias de seguridad existentes, eliminándolas cuando se vuelven obsoletas. También admite la deduplicación para eliminar datos redundantes. Antes de realizar procedimientos que puedan alterar el sistema, le recomendamos que cree una copia de seguridad de cada una de las máquinas virtuales utilizando VMware Data Recovery (disponible en VMware vSphere Versión 5.0) o vSphere Data Protection (disponible en vSphere Versión 5.1). (VMware Data Recovery/vSphere Data Protection se incluye con VMware vSphere, excepto en vSphere Essentials Kit. Consulte http://www.vmware.com/pdf/vdr_11_admin.pdf para obtener más información.)

Las copias de seguridad también se pueden crear mediante un servidor de almacenamiento. Consulte Configuración de un servidor de almacenamiento para obtener más información.

Las *instantáneas* de máquina virtual son *fotografías* de su sistema en un momento específico y no son lo mismo que las copias de seguridad. Por motivos de rendimiento, le recomendamos utilizar copias de seguridad y conservar las copias de seguridad de las máquinas virtuales en una ubicación de almacenamiento que sea

distinta de las unidades físicas que contienen las máquinas virtuales. Para obtener más información sobre las instantánea y los problemas de rendimiento conocidos, consulte Tomar una Instantánea utilizando VMware vCenter.

Procedimiento

Paso 1 Coloque el sistema en modo de mantenimiento. Para información detallada, consulte Acerca del modo de mantenimiento, en la página 125
Compruebe que no existen reuniones activas y que ha seleccionado una hora que afecte mínimamente a sus usuarios.

Paso 2 Siga las instrucciones de la documentación de VMware vSphere y utilice VMware Data Recovery (denominado VMware vSphere Data Protection empezando por vSphere versión 5.1) para crear una copia de seguridad de su sistema y de todas sus máquinas virtuales.
Para obtener información detallada sobre esta copia de seguridad, consulte la *Guía de administración de VMware Data Recovery* o la *Guía de administración de vSphere Data Protection*.

Nota Cisco recomienda eliminar las copias de seguridad después de completar el procedimiento de modificación del sistema, comprobar el funcionamiento del sistema y cuando esté satisfecho con los resultados.

Tomar una Instantánea utilizando VMware vCenter

Las instantáneas de máquina virtual se utilizan para recuperar rápidamente una máquina virtual después de un procedimiento que altere el sistema. Las instantáneas son *fotografías* de su sistema en un momento específico y no son lo mismo que las copias de seguridad (consulte Creación de una copia de seguridad por medio de VMware vCenter). Recomendamos que además de tomar instantáneas, también realice una copia de seguridad del sistema.

Nota Si se pierde el archivo de disco de la máquina virtual original, no puede recuperar la máquina virtual con la instantánea.

Las instantáneas se almacenan en las unidades físicas que contienen sus máquinas virtuales. Si no elimina estas instantáneas de vez en cuando, los usuarios finales podrán experimentar una degradación del audio y del vídeo debido a un problema conocido que afecta al rendimiento de las máquinas virtuales. Así pues, por motivos de rendimiento, le recomendamos que utilice copias de seguridad o que conserve copias de seguridad de las máquinas virtuales en una ubicación de almacenamiento que sea distinta de las unidades físicas que contienen las máquinas virtuales. Además, las instantáneas se pueden utilizar para las actualizaciones, pero para las actualizaciones de sistema recomendamos suprimir todas las instantáneas y realizar una copia de seguridad del sistema original. (Para obtener más información sobre este problema conocido con las instantáneas de VMware, vaya al sitio web de VMware y lea el documento técnico *Buenas prácticas a la hora de ejecutar VMware vSphere en almacenamiento conectado a red*. También puede buscar en VMware KnowledgeBase el **impacto de rendimiento de las instantáneas** para obtener información adicional.)

Antes de realizar la mayoría de procedimientos que alteran el sistema, Cisco recomienda realizar una copia de seguridad del sistema (especialmente cuando se realiza una actualización) o tomar una instantánea (particularmente cuando se realiza una actualización) de cada una de las máquinas virtuales. Puede realizar

la copia de seguridad del sistema por medio de VMware Data Recovery (VMware vSphere Data Protection a partir de vSphere Versión 5.1) o tomar una instantánea de cada máquina virtual. (VMware Data Recovery/vSphere Data Protection está incluido con VMware vSphere, excepto en vSphere Essentials Kit).

Por motivos de rendimiento, no olvide guardar las instantáneas de las máquinas virtuales en una ubicación de almacenamiento que sea distinta de las unidades físicas que contienen las máquinas virtuales.

Asegúrese de leer la sección de preparación del procedimiento específico. Cisco enumera las consideraciones específicas para cada procedimiento.

Recuerde Si su sistema está formado por varias máquinas virtuales, seleccione **Power** > **Shut Down Guest** y realice una instantánea de cada máquina virtual del sistema. Etiquete la instantánea de cada máquina virtual con el mismo prefijo, por ejemplo,20 de agosto, para saber que estas instantáneas se realizaron en el mismo momento.

Nota Cisco le recomienda conservar las instantáneas como máximo durante 24 horas. Si desea conservarlas más tiempo, cree una copia de seguridad en su lugar. Para obtener más información sobre VMware Data Recovery (VMware vSphere Data Protection empezando con vSphere versión 5.1), consulte Creación de una copia de seguridad por medio de VMware vCenter, en la página 4.

Procedimiento

Paso 1 Coloque el sistema en modo de mantenimiento. Para obtener información más detallada, consulte .Acerca del modo de mantenimiento, en la página 125
Compruebe que no existen reuniones activas y que ha seleccionado una hora que afecte mínimamente a sus usuarios.

Paso 2 En VMware vCenter, seleccione **Power** > **Shut Down Guest** para cada una de las máquinas virtuales.

Paso 3 Seleccione **Snapshot** > **Take Snapshot** para cada máquina virtual.

Paso 4 Introduzca un nombre para la instantánea y seleccione **Aceptar**.

Qué hacer a continuación

- Complete el procedimiento y pruebe el sistema para confirmar que es correcto.
- Si necesita revertir una instantánea, asegúrese de que la instantánea se ha tomado al mismo tiempo para cada máquina virtual. Encender un sistema con instantáneas no coincidentes puede resultar en la corrupción de base de datos.

Adjuntar un archivo VMDK existente a una nueva máquina virtual

En esta sección se describe cómo adjuntar archivos VMDK desde una máquina virtual de administración existente a una nueva máquina virtual de administración, utilizando VMware vCenter.

Aunque hay varias razones para desplazar un archivo de disco virtual VMDK, esta sección se centra únicamente en el procedimiento para mover datos desde una máquina virtual de administración a otra máquina virtual de

administración. Utilizará este procedimiento cuando amplíe o actualice su sistema. (Reutilizamos los datos de sistema almacenados en el disco duro 4 de la máquina virtual de administración).

Precaución Haga una copia del archivo de disco duro 4 VMDK y cópielo directamente en la carpeta de la máquina virtual en la máquina virtual de administración en el sistema actualizado o ampliado. Si solamente adjunta el disco duro 4, los datos siguen estando almacenados en la carpeta de la máquina virtual de la máquina virtual de administración antigua. Si elimina accidentalmente la máquina virtual de administración existente en el inventario vCenter, su sistema actual perderá el acceso al disco duro 4.

Nota Si está utilizando almacenamiento con conexión directa (DAS), debe migrar el archivo VMDK de la máquina virtual a un LUN donde pueda acceder la nueva máquina virtual de administración.

Nota Nos referimos a la máquina virtual de administración antes del procedimiento de modificación del sistema como la máquina virtual de administración "existente". La máquina virtual de administración, después de la ampliación o actualización, se denomina "nueva" máquina virtual de administración.

Procedimiento

Paso 1 Navegue por el inventario en VMware vCenter y encuentre la máquina virtual de administración existente para su sistema.

Paso 2 Haga clic con el botón derecho en el nombre de la máquina virtual y seleccione **Edit Settings...**. Aparece la ventana **Virtual Machine Properties**.

Paso 3 Seleccione la pestaña **Hardware**, y después seleccione **Hard disk 4**.

Paso 4 Para referencias futuras, copie y pegue en otro documento la ubicación del archivo de disco (**Disk File**). Este especifica la ubicación de dicho archivo VMDK en VMware vCenter.

La cadena es parecida a `[EMC-LUN10-RAID5] webex-sysA-admin/webex-sysA-admin_3-000001.vmdk`. Si ya ha actualizado su sistema anteriormente, el nombre de archivo no sigue el convenio de denominación de la máquina virtual existente.

Paso 5 Anote e introduzca la ubicación de almacenamiento para el disco duro 4 y el nombre de carpeta de la máquina virtual.

La cadena del nombre de carpeta es parecida a `[EMC-LUN8-RAID5] webex-sysB-admin`.

Paso 6 Cierre la ventana **Edit Settings…** sin hacer ningún cambio.

Paso 7 Cambie la vista de vCenter en la vista del clúster del almacén de datos y el almacén de datos. Seleccione **View** > **Inventory** > **Datastores and Datastore Clusters**.

Paso 8 Seleccione la ubicación de almacenamiento donde se encuentra su máquina virtual de administración (del paso 5) y seleccione **Browse this datastore**.

Paso 9 Seleccione la ubicación de almacenamiento donde se encuentra su nueva máquina virtual de administración desplegada (para el sistema ampliado y actualizado) y seleccione **Browse this datastore**.

Paso 10 Coloque las dos ventanas del explorador del almacén de datos (para la máquina virtual de administración nueva y la existente) una al lado de la otra, para que pueda ver las dos carpetas de ambas máquinas virtuales de administración.

Paso 11 Abra las dos carpetas de las máquinas virtuales y copie el archivo VMDK de la carpeta de la máquina virtual de administración existente a la carpeta de la nueva máquina virtual de administración.

a) En la carpeta de la máquina virtual de administración existente, localice el archivo VMDK que está asociado con el disco duro 4. Consulte la ubicación del archivo que ha escrito en el paso 4 para confirmar su precisión.

b) Haga clic con el botón derecho en el archivo y seleccione **Copiar**.

c) Haga clic con el botón derecho dentro de la carpeta de la máquina virtual de admiración nueva y seleccione **Pegar**.
Cuando haya completado la operación de pegar, cierre las dos ventanas del almacén de datos.

d) Vuelva a vCenter para ver una lista de hosts y grupos seleccionando **View** > **Inventory** > **Hosts and Clusters**.

Paso 12 Navegue por el inventario en VMware vCenter y encuentre la máquina virtual de administración nueva (ampliada o actualizada) para su sistema.

Paso 13 Haga clic con el botón derecho en el nombre de la máquina virtual nueva desplegada y seleccione **Edit Settings...**.
Aparece la ventana **Virtual Machine Properties**.

Paso 14 Seleccione la pestaña **Hardware**, y después seleccione **Hard disk 4**.

Paso 15 Seleccione **Remove**.
Esta acción no elimina el disco virtual inmediatamente. En lugar de ello, el disco virtual existente se programa para su eliminación.

Paso 16 Seleccione **Agregar**.
Aparece el asistente **Add hardware**.

Paso 17 Seleccione **Hard Disk** y a continuación, **Next**.

Paso 18 Seleccione **Use an exisitng virtual disk** y después **Next**.

Paso 19 Seleccione **Browse** y navegue hasta el almacén de datos donde está ubicada la máquina virtual de administración nueva ampliada o actualizada. Navegue hasta la carpeta de la máquina virtual de administración nueva. Haga doble clic en esta carpeta y después seleccione el disco virtual que ha copiado en el paso 11. Seleccione **Aceptar**.

Paso 20 En la lista desplegable **Virtual Device Node**, seleccione **SCSI (0:3)**, y a continuación, **Next**.

Paso 21 Revise sus cambios y si son correctos, seleccione **Finish**. De lo contrario, seleccione **Back** y corrija los errores.

Una vez que el asistente se haya completado, verá un nuevo disco marcado para su incorporación en la pestaña Hardware.

Paso 22 Realice la operaciones de Agregar y eliminar seleccionando **Aceptar**.

Paso 23 Visualice esta tarea de reconfiguración de la máquina virtual en el panel **Recent Tasks** de VMware vCenter para asegurarse de que no existen errores.

CAPÍTULO 2

Lista de comprobación de comunicaciones de red para el sistema

- Lista de comprobación de comunicaciones de red para un sistema con acceso público y horizonte DNS no dividido, página 11
- Lista de comprobación de comunicaciones de red para un sistema con acceso público y horizonte DNS dividido, página 12
- Lista de comprobación de comunicaciones de red para un sistema sin acceso público, página 12

Lista de comprobación de comunicaciones de red para un sistema con acceso público y horizonte DNS no dividido

Durante el despliegue de su sistema, mostramos una página con enlaces a las listas de comprobación de comunicaciones de red. Estas listas de comprobación proporcionan un resumen del servidor DNS, cortafuegos y otros cambios de red que son necesarios para conseguir un despliegue correcto. No olvide hacer estos cambios antes de iniciar el despliegue, ya que realizamos una prueba de conectividad de red casi al final del proceso de despliegue.

Nota El DND de horizonte no dividido es la configuración de DNS más común para las empresas. Para obtener más información sobre el DNS de horizonte no dividido, consulte la *Guía de planificación del Cisco WebEx Meetings Server*.

Nota Si está desplegando un sistema grande, debe seleccionar un despliegue manual.

Seleccione la lista de comprobación correcta en la *Guía de planificación del Cisco WebEx Meetings Server*.

- Despliegue automático: Consulte la "Lista de comprobación de comunicaciones de red para una instalación o expansión con despliegue automático, acceso público y DNS de horizonte no dividido".
- Despliegue manual: Consulte la "Lista de comprobación de comunicaciones de red para una instalación o expansión con despliegue manual, acceso público y DNS de horizonte no dividido".

Lista de comprobación de comunicaciones de red para un sistema con acceso público y horizonte DNS dividido

Durante el despliegue de su sistema, mostramos una página con enlaces a las listas de comprobación de comunicaciones de red. Estas listas de comprobación proporcionan un resumen del servidor DNS, cortafuegos y otros cambios de red que son necesarios para conseguir un despliegue correcto. No olvide hacer estos cambios antes de iniciar el despliegue, ya que realizamos una prueba de conectividad de red casi al final del proceso de despliegue.

Nota Si está desplegando un sistema grande, debe seleccionar un despliegue manual.

Seleccione la lista de comprobación correcta en la *Guía de planificación del Cisco WebEx Meetings Server*.

- Despliegue automático: Consulte la "Lista de comprobación de comunicaciones de red para una instalación o expansión con despliegue automático, acceso público y DNS de horizonte dividido".
- Despliegue manual: Consulte la "Lista de comprobación de comunicaciones de red para una instalación o expansión con despliegue manual, acceso público y DNS de horizonte dividido".

Lista de comprobación de comunicaciones de red para un sistema sin acceso público

Durante el despliegue de su sistema, mostramos una página con enlaces a las listas de comprobación de comunicaciones de red. Estas listas de comprobación proporcionan un resumen del servidor DNS, cortafuegos y otros cambios de red que son necesarios para conseguir un despliegue correcto. No olvide hacer estos cambios antes de iniciar el despliegue, ya que realizamos una prueba de conectividad de red casi al final del proceso de despliegue.

Nota Si está desplegando un sistema grande, debe seleccionar un despliegue manual.

Seleccione la lista de comprobación correcta en la *Guía de planificación del Cisco WebEx Meetings Server*.

- Despliegue automático: Consulte la "Lista de comprobación de comunicaciones de red para una instalación o expansión con despliegue automático y sin acceso público".
- Despliegue manual: Consulte la "Lista de comprobación de comunicaciones de red para una instalación o expansión con despliegue manual y sin acceso público".

CAPÍTULO 3

Instalación de su sistema usando el despliegue automático

- Conceptos generales sobre el despliegue de su sistema, página 14
- Lista de comprobación de instalación, página 15
- Información necesaria para un despliegue automático, página 16
- Desplegar el archivo OVA desde un cliente VMware vSphere, página 18
- Seleccionar su idioma para la configuración, página 30
- Confirmar el despliegue, página 31
- Confirmar el tamaño de su sistema, página 31
- Seleccionar el sistema para instalar, página 31
- Seleccionar el tipo de despliegue de sistema, página 32
- Proporcionar las credenciales de VMware vCenter, página 32
- Seleccionar la configuración de vCenter para su máquina virtual multimedia, página 33
- Introducir la información de comunicaciones de red para la máquina virtual multimedia, página 33
- Agregar acceso público, página 34
- Seleccionar los ajustes de vCenter para su máquina virtual de proxy inverso de Internet, página 34
- Introducir la información de comunicaciones de red para el proxy inverso de Internet, página 35
- Introducir la dirección VIP pública, página 36
- Introducir la dirección VIP privada, página 36
- URL del sitio de WebEx y URL de administración de WebEx, página 37
- Introducción de las URL del sitio de WebEx y de administración de WebEx, página 38
- Confirmación de que la red está configurada correctamente, página 38
- Desplegar sus máquinas virtuales, página 39
- Comprobación de su sistema, página 39

Conceptos generales sobre el despliegue de su sistema

Tamaños del sistema

- Sistema de 50 usuarios simultáneos
  - Normalmente es compatible con una empresa que tenga entre 500 y 1000 empleados
  - El sistema principal (sin HA) está formado por una máquina virtual de administración y un proxy inverso de Internet opcional (para acceso público)
- Sistema de 250 usuarios simultáneos
  - Normalmente es compatible con una empresa que tenga entre 2 500 y 5 000 empleados
  - Un sistema principal (sin HA) está formado por una máquina virtual de administración, una máquina virtual multimedia y un proxy inverso de Internet opcional (para acceso público).
- Sistema de 800 usuarios simultáneos
  - Normalmente es compatible con una empresa que tenga entre 8000 y 16 000 empleados
  - Un sistema principal (sin HA) está formado por una máquina virtual de administración, una máquina virtual multimedia y un proxy inverso de Internet opcional (para acceso público).
- Sistema de 2000 usuarios simultáneos
  - Normalmente es compatible con una empresa que tenga entre 20 000 y 40 000 empleados
  - El sistema principal (sin HA) está formado por una máquina virtual de administración, 3 máquinas virtuales multimedia, 2 máquinas Web y un proxy inverso de Internet opcional (para acceso público).

Términos utilizados durante el despliegue

Nombre del campo	Descripción
URL del sitio de WebEx	URL http segura para que los usuarios organicen y asistan a reuniones.
URL de administración de WebEx	URL http segura para que los administradores configuren, supervisen y administren el sistema.
VIP pública	Dirección IP para la URL del sitio de WebEx
VIP privada	• Dirección IP para la URL del sitio de administración • Dirección IP para la URL del sitio de WebEx (para usuarios internos únicamente, si tiene un DNS de horizonte dividido).

Lista de comprobación de instalación

Restricción Debe utilizar VMware vCenter para administrar los hosts ESXi en los que se despliegue el sistema de Cisco WebEx Meetings Server.

Cambios en las comunicaciones de red

Consulte la lista de comprobación de comunicaciones de red correspondiente a su despliegue. Hay dos consideraciones:

- Acceso público: define si los usuarios externos a su cortafuegos pueden organizar y acceder a reuniones desde Internet o desde dispositivos móviles.

  Cisco recomienda el acceso público, ya que genera una mejor experiencia de usuario para su personal móvil.

- Tipo de configuración DNS de su empresa: DNS de horizonte dividido o DNS de horizonte no dividido (configuración DNS más común).

  Para obtener más información sobre estos tipos de configuración DNS, consulte la *Guía de planificación del Cisco WebEx Meetings Server*.

- Puerto abierto 10200 desde el escritorio del administrador a la máquina virtual de administración.

  El explorador Web utiliza el puerto 10200 durante el despliegue.

Seleccione la lista de comprobación adecuada para su despliegue.

- Lista de comprobación de comunicaciones de red para un sistema con acceso público y horizonte DNS no dividido, en la página 11
- Lista de comprobación de comunicaciones de red para un sistema sin acceso público, en la página 12
- Lista de comprobación de comunicaciones de red para un sistema con acceso público y horizonte DNS dividido, en la página 12

Información necesaria

Nota La información necesaria varía si está realizando el despliegue automático (admitido para 50 usuarios simultáneos, 250 usuarios simultáneos y 800 usuarios simultáneos) de sistemas o un despliegue manual (admitido para todos los tamaños de sistema). Cisco le recomienda que seleccione el despliegue automático a menos que esté desplegando un sistema de 2000 usuarios, que requiere un despliegue manual. Consulte el enlace correspondiente más abajo.

Seleccione una de las siguientes opciones para obtener una lista de comprobación de la información necesaria para su tipo de despliegue:

- Información necesaria para un despliegue automático, en la página 16
- Información necesaria para un despliegue manual, en la página 43

Información necesaria para un despliegue automático

Se trata de la información necesaria para su sistema, en orden.

Nota No olvide agregar los FQDN de la máquina virtual, las direcciones IP, las URL del sitio de administración y del sitio de WebEx y las direcciones VIP a sus servidores DNS antes de iniciar el despliegue del sistema. Utilizaremos esta información para buscar direcciones IP para usted durante el despliegue.

Para evitar cualquier problema de DNS, puede probar estas direcciones URL e IP antes de iniciar el despliegue OVA. De lo contrario, el despliegue del sistema fallará hasta que corrija estos errores.

Nombre del campo	Descripción	Valor para su sistema
URL de vCenter	Dirección http segura del servidor vCenter para las máquinas virtuales en su sistema.	
Nombre de usuario de vCenter	Nombre de usuario para desplegar las máquinas virtuales para su sistema. Este usuario debe tener privilegios de administrador: para desplegar, configurar, encender o apagar y suprimir máquinas virtuales.	
Contraseña de vCenter	Contraseña del usuario de vCenter.	
(Solo para sistemas de 250 y 800 usuarios simultáneos) Host ESXi	Host ESXi para la máquina virtual multimedia. **Nota** Este host ESXi debe estar en el mismo vCenter que la URL vCenter anterior.	
(Solo para sistemas de 250 y 800 usuarios simultáneos) Almacén de datos	Almacén de datos para la máquina virtual multimedia.	
(Solo para sistemas de 250 y 800 usuarios simultáneos) Grupo de puertos de la máquina virtual	Grupo de puertos para la máquina virtual multimedia. **Nota** Cisco recomienda seleccionar el mismo grupo de puertos que ha seleccionado para la máquina virtual de administración.	
(Solo para sistemas de 250 y 800 usuarios simultáneos) FQDN para la máquina virtual multimedia	Nombre de dominio cualificado completo (todo en minúscula) para la máquina virtual multimedia.	

Nombre del campo	Descripción	Valor para su sistema
(Solo para sistemas de 250 y 800 usuarios simultáneos) Dirección IPv4 para la máquina virtual multimedia	Dirección de IPv4 para la máquina virtual multimedia, Buscaremos automáticamente la dirección IPv4 correspondiente para esta máquina virtual multimedia.	
(Solo acceso público) Host ESXi	El host ESXi para la máquina virtual de proxy inverso de Internet. **Nota** Cisco recomienda seleccionar un host ESXi distinto al seleccionado para la máquina virtual de administración y las otras máquinas virtuales internas. Para habilitar el tráfico al proxy inverso de Internet, asegúrese de que el host ESXi está configurado con un grupo de puerto que pueda dirigir la VLAN cuya dirección IP es utilizada por el proxy inverso de Internet.	
(Solo acceso público) Almacén de datos	Almacén de datos para la máquina virtual de proxy inverso de Internet.	
(Solo acceso público) Grupo de puertos de la máquina virtual	Grupo de puertos para la máquina virtual de proxy inverso de Internet. **Nota** Por motivos de seguridad, Cisco recomienda seleccionar un grupo de puertos distinto al seleccionado para la máquina virtual de administración.	
(Solo acceso público) FQDN para el proxy inverso de Internet	Nombre de dominio cualificado completo (todo en minúscula) para la máquina virtual de proxy inverso de Internet.	
(Solo acceso público) Dirección IPv4 de proxy inverso de Internet	Dirección IPv4 para la máquina virtual de proxy inverso de Internet. Buscaremos automáticamente la dirección Ipv4 correspondiente para esta máquina virtual de proxy inverso de Internet.	
(Solo acceso público) Puerta de enlace IPv4	Puerta de enlace de IPv4 para la máquina virtual de proxy inverso de Internet.	
(Solo acceso público) Máscara de subred IPv4	Máscara de subred para la máquina virtual de proxy inverso de Internet.	
(Solo acceso público) Dirección IPv4 del servidor DNS primario	Servidor DNS para la máquina virtual de proxy inverso de Internet.	

Nombre del campo	Descripción	Valor para su sistema
(Solo acceso público) Dirección IPv4 del servidor DNS secundario	(Opcional) Servidor DNS adicional para la máquina virtual de proxy inverso de Internet.	
VIP pública	Dirección IP para la URL del sitio de WebEx (acceso de usuarios del sitio para organizar y asistir a reuniones).	
VIP privada	• Dirección IP para la URL del sitio de administración (para que los administradores puedan configurar, supervisar y administrar el sistema) • Dirección IP para la URL del sitio de WebEx (para usuarios internos únicamente, si tiene un DNS de horizonte dividido).	
URL del sitio de WebEx	URL http segura (todo en minúscula) para que los usuarios puedan organizar y asistir a reuniones.	
URL de administración de WebEx	URL http segura (todo en minúscula) para que los administradores puedan configurar, supervisar y administrar el sistema.	

Qué hacer a continuación

Con esta información, inicie el despliegue del sistema introduciendo la URL de despliegue en una ventana del explorador. (La URL de despliegue se muestra en la ventana de la consola para la máquina virtual de administración).

Nota Si el sistema se reinicia antes de que la configuración se haya completado, se generará una nueva contraseña y deberá utilizar la URL de despliegue con la nueva contraseña.

Desplegar el archivo OVA desde un cliente VMware vSphere

Antes de desplegar sus sistema, debe usar el cliente VMware vSphere para desplegar la máquina virtual de administración para su sistema.

Nota El procedimiento siguiente se proporciona a modo de guía general. Las pantallas exactas que verá durante el despliegue de OVA dependerán de la configuración de vCenter, almacenamiento y red, y pueden ser diferentes a las que se muestran en este procedimiento. Consulte la documentación de VMware vSphere para obtener información completa sobre el asistente OVA.

Antes de comenzar

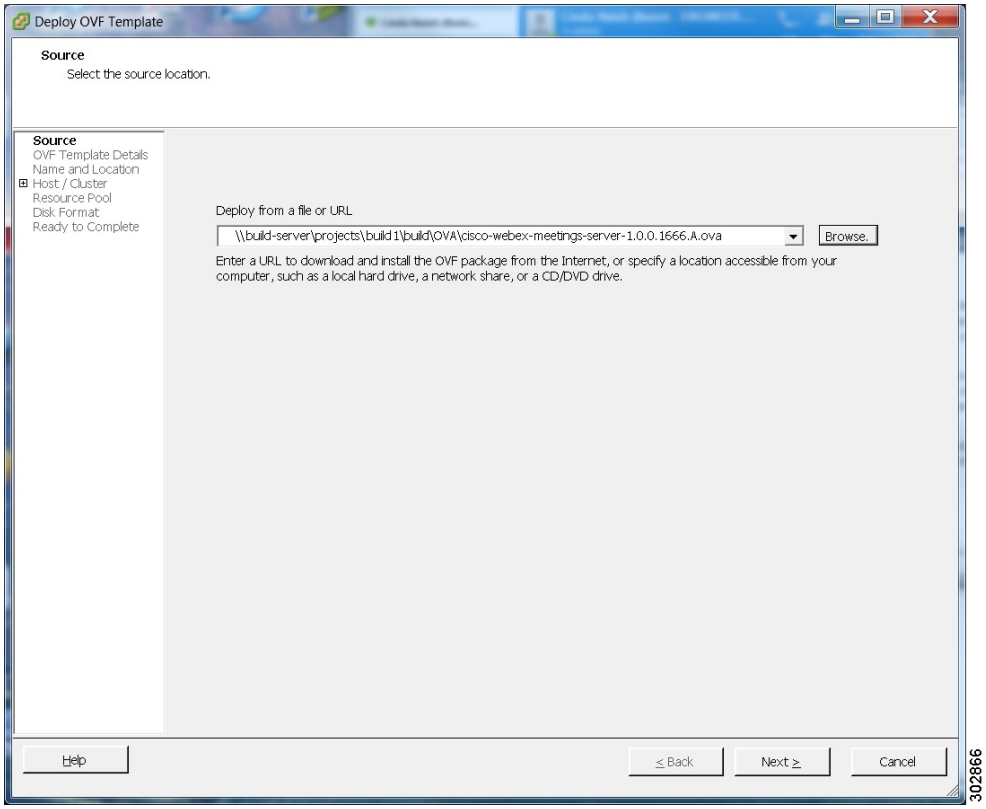
Obtenga el archivo OVA de Cisco WebEx Meetings Server para su sistema y colóquelo en una ubicación que sea accesible desde VMware vSphere.

Debe utilizar VMware vCenter para administrar los hosts ESXi en los que se despliegue el sistema de Cisco WebEx Meetings Server. Mediante el cliente de vSphere, inicie sesión en vCenter y despliegue el archivo OVA para la máquina virtual Administración.

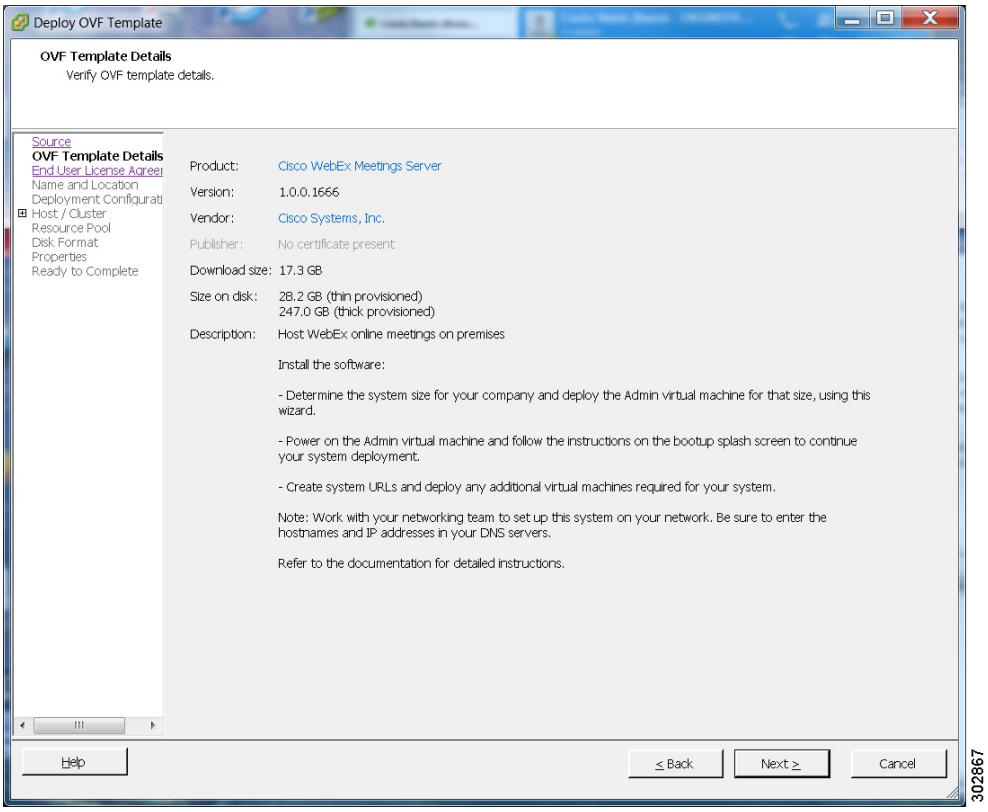
Procedimiento

Paso 1 Inicie sesión en su cliente VMware vSphere.
No olvide iniciar sesión como usuario con privilegios de administrador: para desplegar, configurar, encender o apagar y suprimir máquinas virtuales.

Paso 2 Seleccione **File** > **Deploy OVF Template...**



Paso 3 Seleccione **Explorar** para desplazarse hasta la ubicación del archivo OVA. Seleccione **Siguiente**.
Puede seleccionar el enlace de **Cisco WebEx Meetings Server** para ir a una página Web con información detallada acerca de este sistema.



Paso 4 Lea el Acuerdo de licencia de usuario final y seleccione **Accept** y después **Next**.

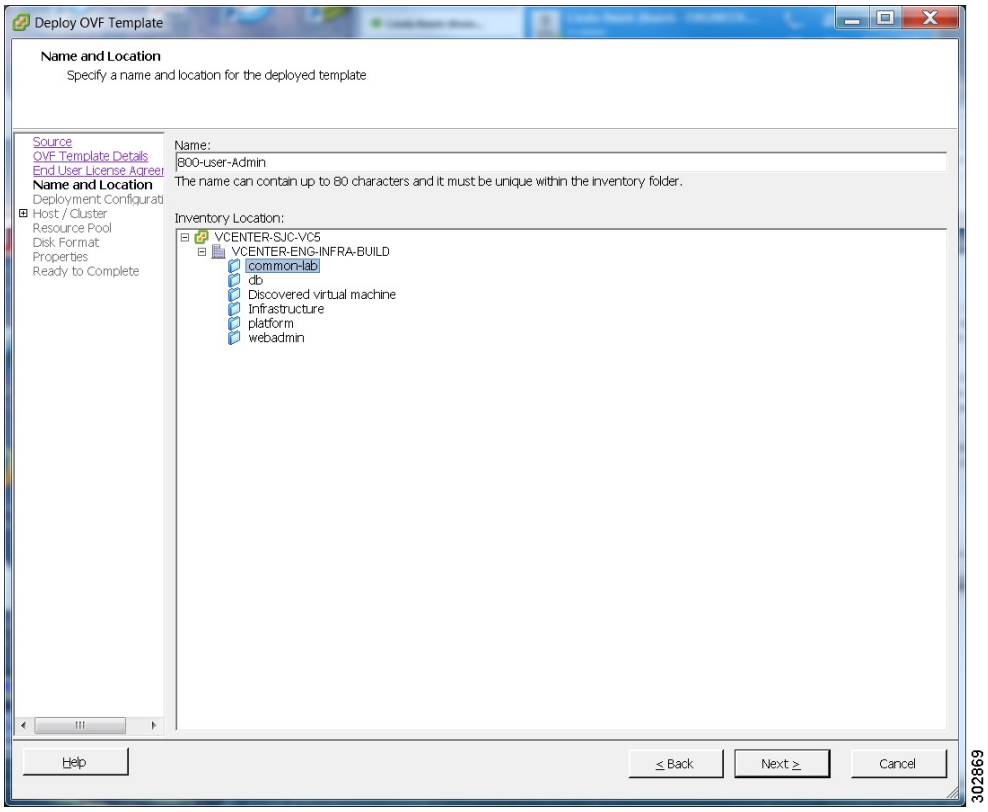
Paso 5 Desplácese hasta la ubicación del inventario vCenter y seleccione el lugar donde desea colocar la máquina virtual de administración.

Paso 6 Introduzca el nombre de la máquina virtual para su sistema y seleccione **Siguiente**. Para obtener más información sobre la selección del tamaño correcto para su empresa, consulte Tamaños del sistema.

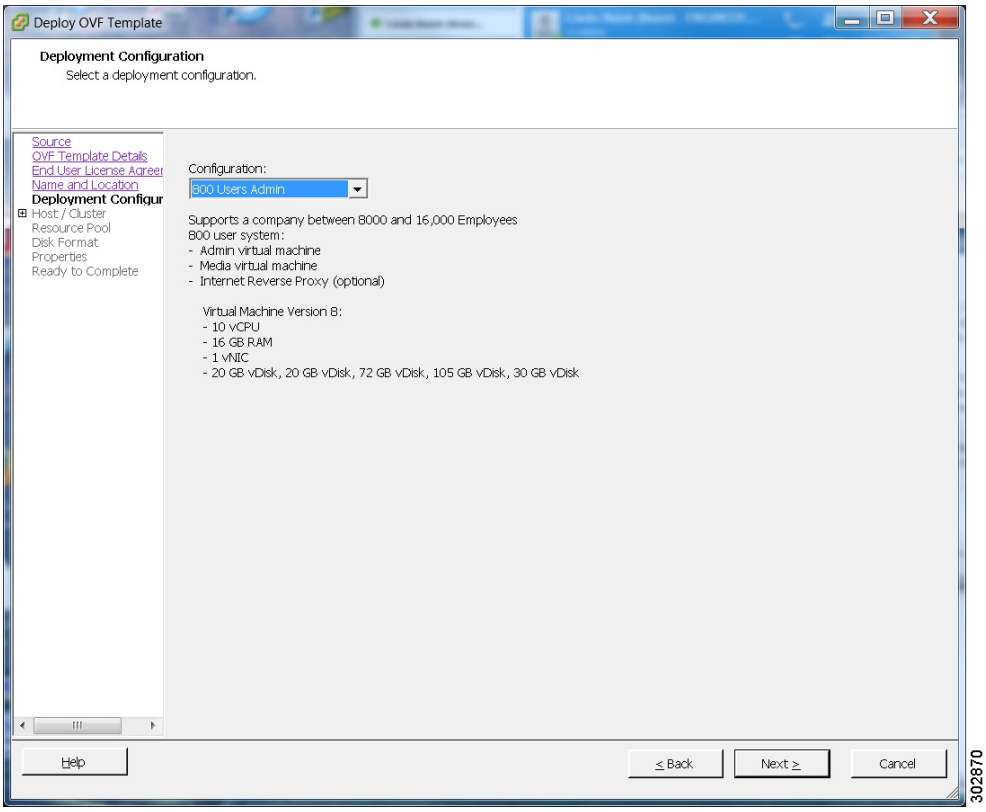
Nota Debe desplegar la máquina virtual de administración antes de desplegar cualquier otra máquina virtual. Si selecciona el despliegue automático (recomendado), las otras máquinas virtuales se despliegan automáticamente. Si selecciona el despliegue manual (necesario en un sistema con 2000 usuarios simultáneos), después de desplegar la máquina virtual de administración, debe desplegar las demás máquinas virtuales utilizando este mismo asistente.

Cisco le recomienda que incluya el tipo en el nombre de la máquina virtual; por ejemplo, incluya "Admin" en el nombre de la máquina virtual de administración para identificarla fácilmente en el inventario de vCenter.

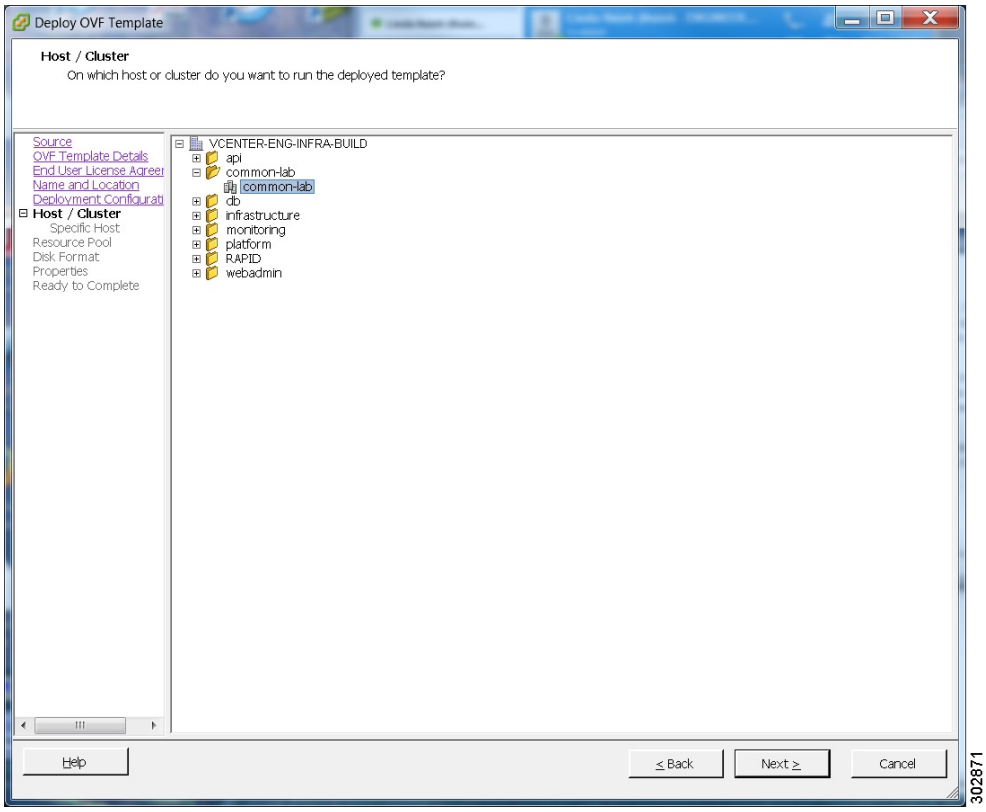
Nota Todas las máquinas virtuales internas para su sistema deben encontrarse en la misma subred que la máquina virtual de administración. (Dependiendo del tamaño de sistema que seleccione, puede que necesite uno o varios soportes y máquinas virtuales internas Web.)



Paso 7 En la lista desplegable, seleccione la máquina virtual para su tamaño de sistema y seleccione **Siguiente**. Asegúrese de desplegar la máquina virtual de administración antes que cualquier otra máquina virtual de su sistema.

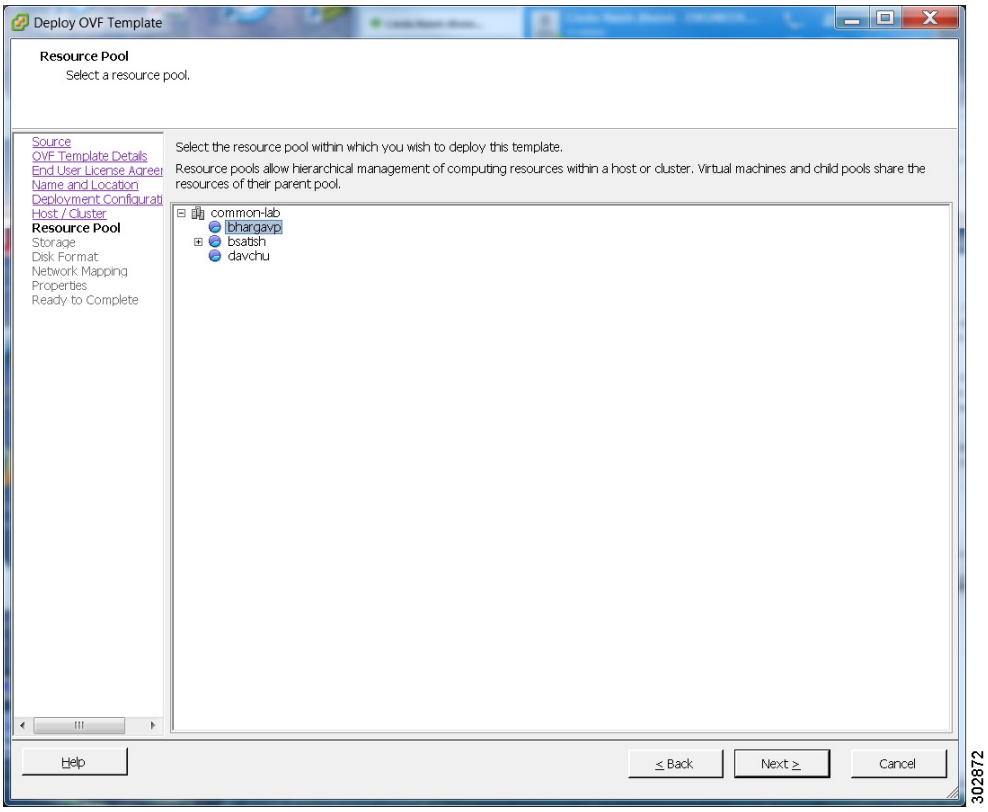


Paso 8 Desplácese por el inventario de vCenter y seleccione el clúster o host ESXi en el que desea desplegar las máquinas virtuales para su sistema. Seleccione **Siguiente**.

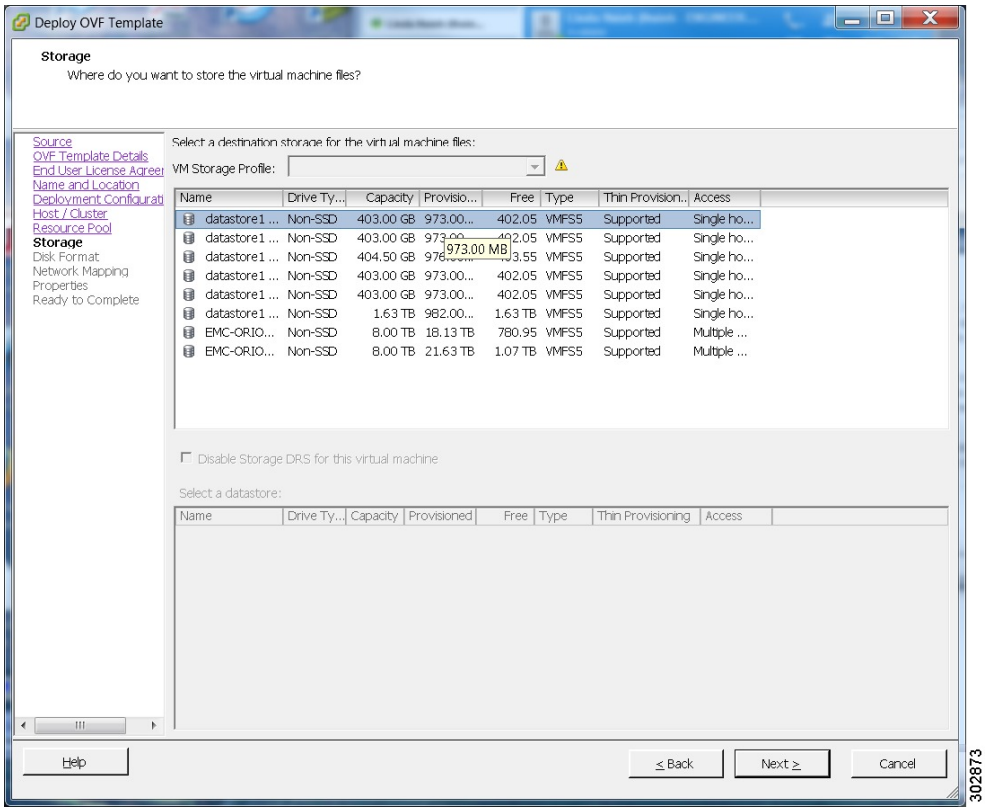


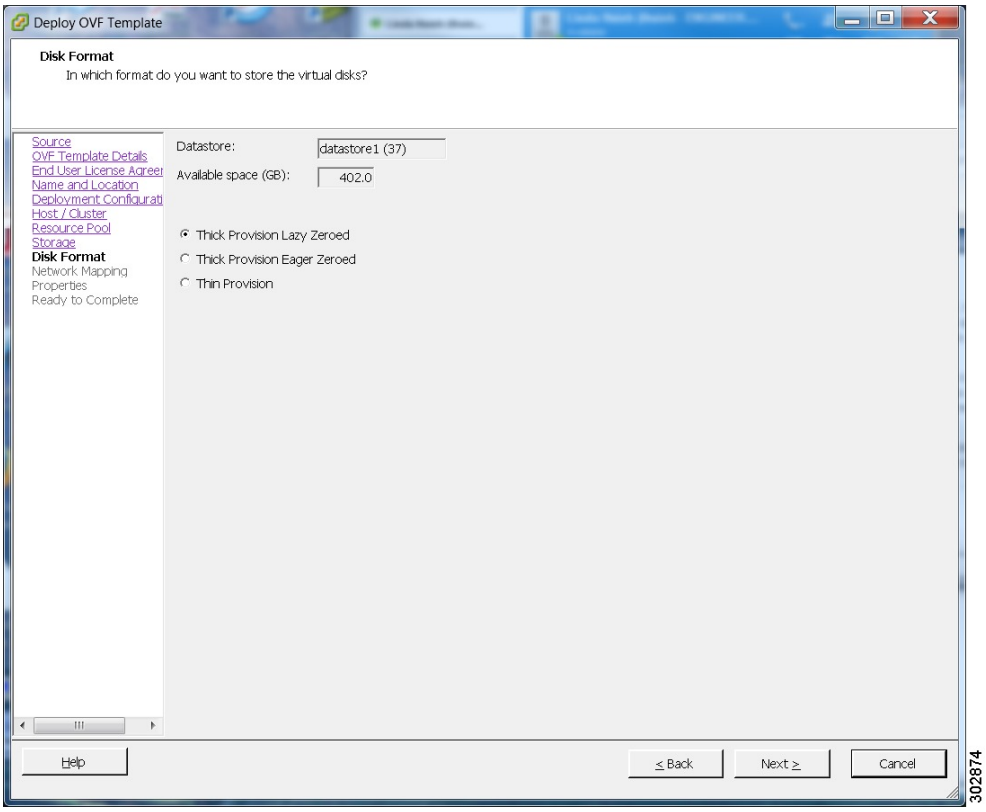
Paso 9 Si el clúster contiene una agrupación de recursos, seleccione la agrupación de recursos en la que desea desplegar la plantilla OVA y seleccione **Siguiente**.

Las agrupaciones de recursos comparten recursos de CPU y memoria o para trabajar con funciones de VMware, tales como DRS o vMotion. Las agrupaciones de recursos deben estar dedicadas para un único host de ESXi. No se recomienda utilizar las agrupaciones de recursos de VMware con Cisco WebEx Meetings Server.



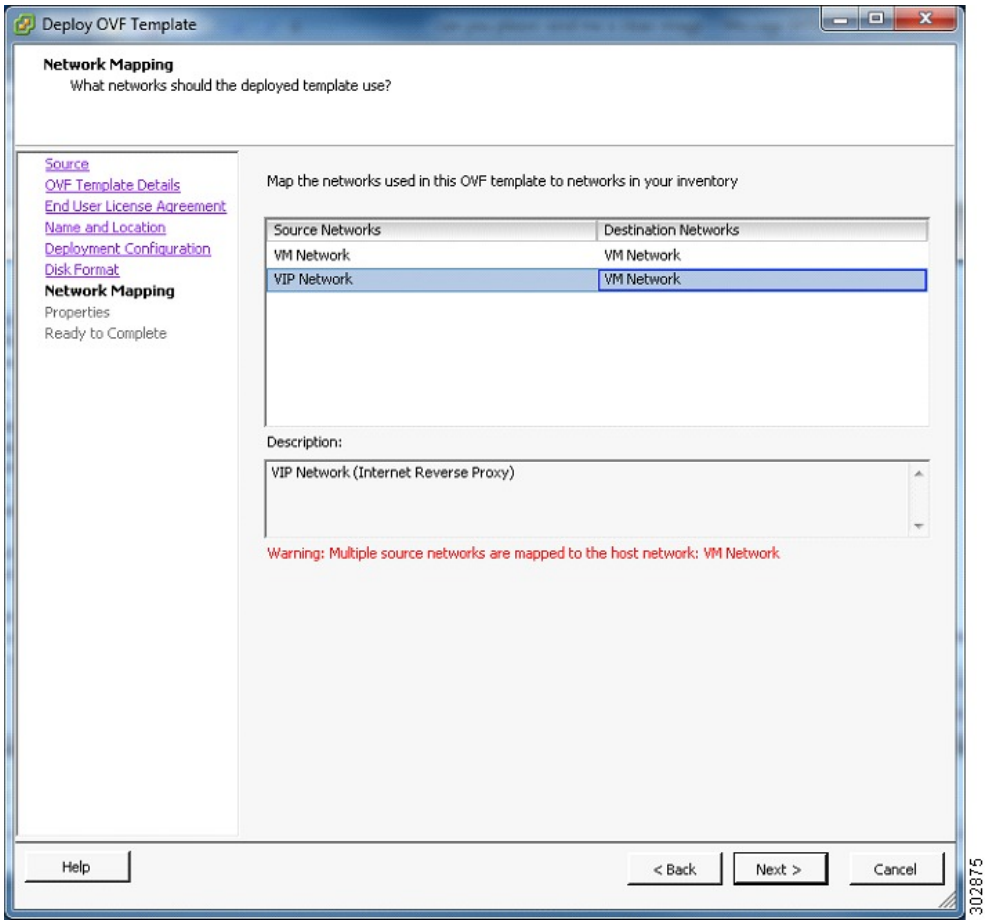
Paso 10 Seleccione el almacén de datos para su máquina virtual y el tipo de suministro para su máquina virtual. Debe seleccionar **Thick Provisioning** y crear el espacio de disco virtual máximo necesario para su sistema. Con Thin Provisioning, VMware asigna el espacio de sistema de archivos *cuando se necesita*, lo que puede causar un bajo rendimiento. Lazy zero es suficiente y eager zero es aceptable, pero eager zero tardará más tiempo en completarse.


Deploy OVF Template
Storage
Where do you want to store the virtual machine files?
Source
OVF Template Details
End User License Agreer
Name and Location
Deployment Configurati
Host / Cluster
Resource Pool
Storage
Disk Format
Network Mapping
Properties
Ready to Complete
Select a destination storage for the virtual machine files:
VM Storage Profile:
Name
Drive Ty...
Capacity
Provisio...
Free
Type
Thin Provision..
Access
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 404.50 GB 973.00... 403.55 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 1.63 TB 982.00... 1.63 TB VMFS5 Supported Single ho...
EMC-ORIO... Non-SSD 8.00 TB 18.13 TB 780.95 VMFS5 Supported Multiple ...
EMC-ORIO... Non-SSD 8.00 TB 21.63 TB 1.07 TB VMFS5 Supported Multiple ...
973.00 MB
Disable Storage DRS for this virtual machine
Select a datastore:
Name
Drive Ty...
Capacity
Provisioned
Free
Type
Thin Provisioning
Access
Help
< Back
Next >
Cancel
302873



Paso 11 Defina una asignación de red. Para cada red de origen, seleccione una red de destino en la lista desplegable en la columna **Destination Networks**. Seleccione **Siguiente**.

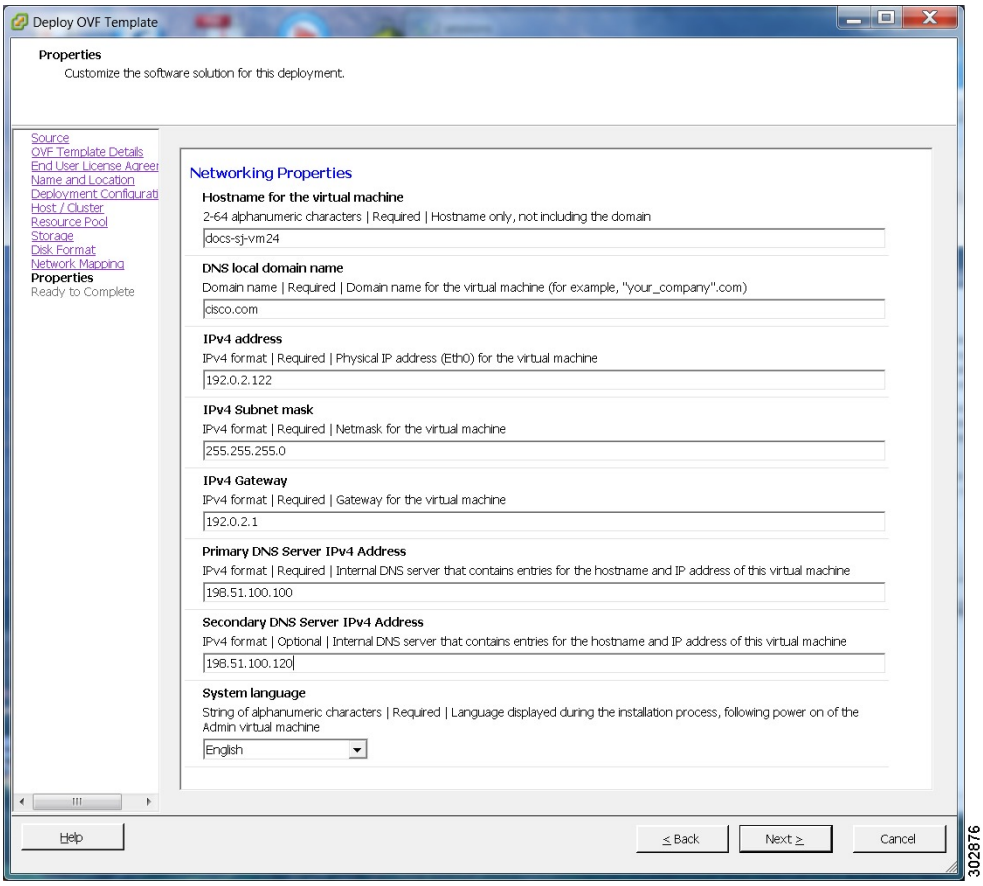
Nota Tanto la red VM como la red VIP deben correlacionarse con el mismo valor en la columna Red de destino. Puede ignorar el mensaje de advertencia acerca de varias redes de origen asignadas a la misma red de host.



Paso 12 Introduzca la siguiente información para la máquina virtual y después seleccione **Siguiente**.

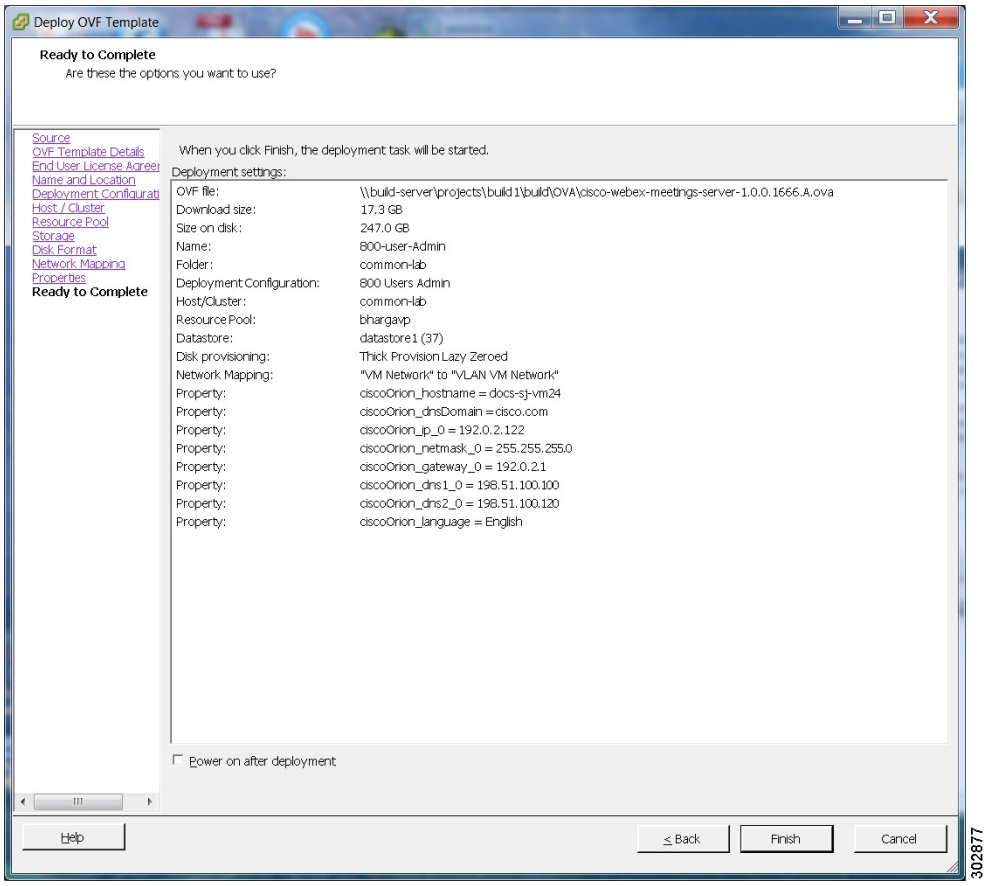
- Nombre de host de la máquina virtual (no incluya aquí el dominio)
- Dominio para la máquina virtual
- Dirección IPv4 (Eth0) para la máquina virtual
- Máscara de subred de la máquina virtual
- Dirección IP de puerta de enlace
- Servidor DNS primario que contiene entradas para el nombre de host y la dirección IP de la máquina virtual.
- Servidor DNS secundario que contiene entradas para el nombre de host y la dirección IP de esta máquina virtual
- El idioma se muestra durante el proceso de instalación, después del encendido de esta máquina virtual.

Nota Para evitar problemas de DNS, puede probar las direcciones URL e IP antes de iniciar el despliegue de OVA. El despliegue fallará si se producen errores.



Paso 13 Confirme la información que ha introducido. Si hay algún error, seleccione **Atrás** y cambie los valores.

Paso 14 Marque **Encender después del despliegue** y, a continuación, seleccione **Finalizar**.



Paso 15 Si está desplegando una máquina virtual de administración, vaya a vCenter y abra la ventana de la consola para la máquina virtual. Después de encenderse, comprobaremos la información de comunicaciones de red que ha introducido durante el despliegue de OVA.

- Si podemos confirmar la conectividad, se muestra una marca de selección de color verde.
- Si hay algún problema, se muestra una X de color rojo. Resuelva el error y vuelva a intentar el despliegue OVA.

Paso 16 Cuando esté confirmada toda la información, anote el URL visualizado que se muestra en la ventana de la consola.
Un administrador de software escribirá esta URL en un explorador Web, y continuará el despliegue del sistema.

Nota Si el sistema se reinicia antes de que la configuración se haya completado, se generará una nueva contraseña y deberá utilizar el URL con la nueva contraseña.

Qué hacer a continuación

Si realiza un despliegue manual, Cisco recomienda desplegar el resto de máquinas virtuales de su sistema en este momento. Esto evita posibles problemas tales como tiempos de espera agotados al encender las máquinas virtuales.

Si el despliegue se realiza correctamente, siga con el despliegue del sistema en una ventana de explorador.

Si el despliegue falla, consulte Comprobación de la configuración de comunicaciones de red después de un despliegue OVA incorrecto.

Comprobación de la configuración de comunicaciones de red después de un despliegue OVA incorrecto

Confirme las entradas de comunicaciones de red para la máquina virtual.

Importante No utilice **Edit Settings...** para ninguna máquina virtual de su sistema, a no ser que sea después de un error de despliegue. Una vez que el sistema está funcionando, deberá utilizar el sitio de administración de WebEx para editar la configuración de la máquina virtual. Si utiliza su cliente vSphere, el sistema no aceptará esos cambios.

Nota Para los pasos detallados, consulte la documentación de VMware vSphere.

Procedimiento

Paso 1 En el cliente Vsphere, seleccione **Power** > **Shut Down Guest** en la máquina virtual.

Paso 2 Encuentre la máquina virtual en el inventario y haga clic con el botón derecho en **Edit Settings...**.

Paso 3 Seleccione la pestaña **Options**.

Paso 4 Seleccione **Properties** y confirme que toda la información de comunicaciones de red se ha introducido correctamente. Si se necesita algún cambio, vuelva a desplegar el OVA con la configuración correcta.
Una posible causa del problema de red es que el enrutamiento VLAN no está configurado correctamente para el host ESXi. Debido a que la máquina virtual está en ese VLAN, la máquina virtual no tendrá conectividad de red. Desde la red en la que se encuentra el host ESXi, usted debería poder hacer una petición a la dirección IP predeterminada de la puerta de enlace de la VLAN que va a utilizar para las máquinas virtuales de su sistema.

Seleccionar su idioma para la configuración

Determine su idioma preferido para configurar el sistema.

Nota No cierre esta ventana del explorador hasta que el despliegue del sistema se haya completado. Si cierra el explorador antes, es posible que tenga que reiniciar el despliegue.

Antes de comenzar

Compruebe que ha desplegado la máquina virtual desde VMware vCenter. ConsulteDesplegar el archivo OVA desde un cliente VMware vSphere, en la página 18

Procedimiento

Paso 1 Seleccione el idioma en el menú desplegable.

Paso 2 Seleccione **Siguiente**.

Confirmar el despliegue

Procedimiento

Paso 1 Confirme si va a desplegar un sistema nuevo o a ampliar un sistema existente.

Paso 2 Seleccione **Siguiente**.

Confirmar el tamaño de su sistema

Usted seleccionó el tamaño de su sistema al desplegar la máquina virtual de administración utilizando el archivo OVA.

- Confirme que el tamaño del sistema que seleccionó durante el despliegue de OVA es correcto.
  - Si el tamaño del sistema seleccionado es correcto, seleccione **Siguiente**.
  - Si el tamaño del sistema seleccionado no es correcto, seleccione **Deseo cambiar el tamaño del sistema**.

a) Utilizando su cliente VMware vSphere, seleccione **Power** > **Shut Down Guest** para la máquina virtual de administración con el tamaño de sistema incorrecto.
b) Haga clic con el botón derecho en la máquina virtual y seleccione **Delete from Disk**.
c) Vuelva a desplegar el archivo OVA y seleccione la máquina virtual de administración del tamaño correcto.

Seleccionar el sistema para instalar

Procedimiento

Paso 1 Determine el tipo de instalación.

- Si está instalando este sistema por primera vez, seleccione **Instalar un sistema principal**.
- Si ha instalado un sistema principal y quiere un sistema redundante de alta disponibilidad, seleccione **Crear un sistema redundante de alta disponibilidad (HA)**.

Nota Usted no debe instalar un sistema HA antes de instalar el sistema principal, como no puede utilizar el sistema HA a menos que el sistema principal se haya instalado.

Paso 2 Seleccione **Siguiente**.

Seleccionar el tipo de despliegue de sistema

Determine cómo quiere desplegar cualquier otra máquina virtual necesaria para su sistema. Si ha seleccionado un sistema de 2000 usuarios, debe seleccionar un despliegue manual.

Procedimiento

Paso 1 Seleccione si desea desplegar las máquinas virtuales usted mismo, o bien si quiere que las despleguemos por usted.

- **Automático:** Es el método de instalación más rápido. Nosotros desplegamos todas las máquinas virtuales necesarias para su sistema.
  Cisco le recomienda que seleccione **Automático** a menos que esté desplegando un sistema de 2000 usuarios, que requiere un despliegue manual.

  Nota Utilizando Administración de Cisco WebEx, puede seguir realizando cambios en el sistema después del despliegue.

- **Manual:** Debe desplegar manualmente cada una de las máquinas virtuales usando VMware vCenter. Después de responder a unas cuantas preguntas sobre su sistema, le proporcionaremos una lista de máquinas virtuales necesarias para su sistema.

Su decisión de despliegue manual o automático depende de lo siguiente:

- Si tiene limitaciones de tiempo, un despliegue automático es más rápido que un despliegue manual.
- Si prefiere una guía paso a paso, seleccione el despliegue automático.
- Si está familiarizado con VMware vCenter y no desea proporcionar sus credenciales vCenter, seleccione el despliegue manual.

Paso 2 Seleccione **Siguiente**.

Proporcionar las credenciales de VMware vCenter

Si selecciona un despliegue automático, Cisco WebEx Meetings Server necesita sus credenciales de vCenter para desplegar automáticamente las máquinas virtuales.

Antes de comenzar

Todos los hosts ESXi de su sistema deben pertenecer al mismo VMware vCenter.

Procedimiento

Paso 1 Especifique el URL de https seguro del vCenter en el que se desplegará el sistema.

Paso 2 Introduzca el nombre de usuario que utilizaremos para desplegar las máquinas virtuales. El usuario de vCenter debe incluir privilegios de administrador que permitan a dicho administrador desplegar, configurar, encender y apagar y suprimir máquinas virtuales.

Paso 3 Especifique la contraseña de este nombre de usuario.

Paso 4 Seleccione **Siguiente**.

Seleccionar la configuración de vCenter para su máquina virtual multimedia

La máquina virtual multimedia es necesaria para despliegues de sistema de 250 usuarios y 800 usuarios.

Procedimiento

Paso 1 En la lista desplegable, seleccione el host de ESXi para la máquina virtual multimedia.

Paso 2 Seleccione el almacén de datos para la máquina virtual multimedia.

Paso 3 Seleccione la máquina virtual para el grupo de puertos de la máquina virtual multimedia.
Cisco recomienda seleccionar el mismo grupo de puertos que ha seleccionado para la máquina virtual de administración.

Paso 4 Seleccione **Siguiente**.

Introducir la información de comunicaciones de red para la máquina virtual multimedia

Al especificar el nombre de dominio cualificado completo de la máquina virtual multimedia, Cisco WebEx Meetings Server intenta llenar la información de red.

Nota La máquina virtual multimedia debe estar en la misma subred que la máquina virtual de administración. No edite el dominio, la pasarela IPv4, la máscara de subred ni los servidores DNS de la máquina virtual multimedia.

Procedimiento

Paso 1 Introduzca el FQDN de la máquina virtual multimedia.
Ya debería haber introducido el nombre de host y la dirección IP de la máquina virtual multimedia en sus servidores DNS. Cisco WebEx Meetings Server busca y completa la **Dirección IPv4**.

Paso 2 Seleccione **Siguiente**.

Agregar acceso público

Si agrega el acceso público, los usuarios pueden organizar y asistir a reuniones desde Internet o dispositivos móviles. Para obtener más información sobre la configuración de este campo para su empresa, consulte la *Guía de planificación del Cisco WebEx Meetings Server*.

Nota Siempre puede cambiar esta opción más tarde a través del sitio de administración de WebEx.

Procedimiento

Paso 1 Seleccione si desea que los usuarios externos puedan organizar o asistir a reuniones.

- Si quiere agregar el acceso público, compruebe que la casilla de verificación **Crear una máquina virtual de proxy inverso de Internet** está marcada.
- Si solo quiere que los usuarios internos (detrás del cortafuegos de su empresa) puedan organizar o asistir a reuniones, elimine la selección de la casilla de verificación **Crear una máquina virtual de proxy inverso de Internet**.

Paso 2 Seleccione **Siguiente**.

Qué hacer a continuación

- Con acceso público: Seleccionar los ajustes de vCenter para su máquina virtual de proxy inverso de Internet, en la página 34
- Sin acceso público: Introducir la dirección VIP privada, en la página 36

Seleccionar los ajustes de vCenter para su máquina virtual de proxy inverso de Internet

El acceso público requiere una máquina virtual de proxy inverso de Internet. Introduzca los valores que anotó en la lista de verificación de la instalación.

Aunque no es obligatorio, por motivos de seguridad, Cisco recomienda que coloque el proxy inverso de Internet en una subred distinta a la de la máquina virtual de administración. De esta forma, se garantiza el aislamiento del nivel de red entre el proxy inverso de Internet y sus máquinas virtuales internas (de administración y multimedia, según proceda).

Nota Compruebe que los puertos del cortafuegos requeridos por VMware vCenter están abiertos para que vCenter pueda desplegar la máquina virtual de proxy inverso de Internet. Para obtener más información sobre los puertos del cortafuegos requeridos, consulte la *Guía de Planificación del Cisco WebEx Meetings Server*.

Procedimiento

Paso 1 En la lista desplegable, seleccione el host ESXi para la máquina virtual de proxy inverso de Internet.

Paso 2 Seleccione el almacén de datos para el proxy inverso de Internet.

Paso 3 Seleccione el grupo de puertos de la máquina virtual para el proxy inverso de Internet.

Paso 4 Seleccione **Siguiente**.

Introducir la información de comunicaciones de red para el proxy inverso de Internet

El proxy inverso de Internet permite a los usuarios organizar reuniones o asistir a ellas desde Internet o desde dispositivos móviles.

Antes de comenzar

- Por motivos de seguridad, Cisco recomienda que el proxy inverso de Internet se coloque en una subred distinta a la de la máquina virtual de administración.
- Introduzca el nombre de host y la dirección IP del proxy inverso de Internet en sus servidores DNS para activar la búsqueda desde una red externa.

Nota Si tiene servidores DNS que habilitan la búsqueda de un proxy inverso de Internet, introduzca el nombre de host y la dirección IP del proxy inverso de Internet en estos servidores DNS del mismo modo. Esto permite establecer una conexión segura entre las máquinas virtuales internas (administración y multimedia, si procede) y el proxy inverso de Internet.

- Introduzca el siguiente proxy inverso de Internet y seleccione **Siguiente**.
  - Nombre de Dominio Cualificado Completo (FQDN)
    Ya debería haber introducido el nombre de host y la dirección IP de la máquina virtual de proxy inverso de Internet en sus servidores DNS. Buscaremos y rellenaremos el campo **Dirección Ipv4** por usted.
  - Puerta de enlace IPv4
  - Máscara de subred IPv4
  - Dirección IPv4 del servidor DNS primario

- (Opcional) Dirección IPv4 del servidor DNS secundario

Introducir la dirección VIP pública

- Esta dirección VIP público debe estar visible tanto desde Internet como desde la red interna (solamente DNS de horizonte dividido).
- La dirección VIP pública debe estar en la misma subred que el proxy inverso de Internet.
- Si no tiene un DNS de horizonte dividido, todos los usuarios utilizan la dirección VIP pública para organizar y asistir a reuniones.
- Si tiene un DNS de horizonte dividido y ha agregado el acceso público, todos los usuarios externos usan la dirección VIP pública para organizar y asistir a reuniones.

Para obtener más información sobre el DNS de horizonte dividido y no dividido, así como del acceso público, consulte la *Guía de planificación del Cisco WebEx Meetings Server*.

Nota Si está creando un sistema de alta disponibilidad (HA), no tiene que volver a introducir esta información, ya que utilizaremos la información introducida en el sistema principal.

- Introduzca la dirección IPv4 VIP pública y seleccione **Siguiente**.

Introducir la dirección VIP privada

Los administradores configuran, supervisan y mantienen el sistema desde la URL del sitio de administración que dirige a la dirección VIP privada.

Nota Si tiene un DNS de horizonte dividido, todos los usuarios internos también usan la dirección VIP privada para organizar y asistir a reuniones.

Nota Si está agregando un sistema de alta disponibilidad (HA), no tiene que volver a introducir esta información, ya que utilizaremos la información introducida en el sistema principal.

Antes de comenzar

La dirección IP virtual privada (VIP) debe encontrarse en la misma subred que sus máquinas virtuales internas (administración y multimedia, si procede).

- Introduzca la dirección VIP privada Ipv4 y seleccione **Siguiente**.

URL del sitio de WebEx y URL de administración de WebEx

URL del sitio de WebEx

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

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

URL de administración de WebEx

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

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

Puede seleccionar casi cualquier nombre para estas URL, utilizando todos los caracteres en minúscula. Sin embargo, no puede usar lo siguiente como nombre de host en las URL del sitio:

- El mismo nombre que los nombres de host para cualquier máquina virtual del sistema
- Autenticación
- Cliente
- Logotipo de la compañía
- Distribuidor
- Docs
- elm-admin
- elm-client-services
- Correos electrónicos
- Mantenimiento
- Manager
- orion
- oriondata
- oriontemp
- nbr
- npp
- Investigación

- Aviso
- Raíz
- Energía solar
- TomcatROOT
- upgradeserver
- url0107ld
- Versión
- WBXService
- Centro de

Introducción de las URL del sitio de WebEx y de administración de WebEx

- No puede reutilizar los nombres de host de las máquinas virtuales en su sistema en la porción de nombre de host de la URL del sitio de WebEx o de administración de WebEx.
- La URL del sitio de WebEx debe ser diferente de la URL de administración de WebEx.

Nota Si está agregando un sistema de alta disponibilidad (HA), no tiene que volver a introducir esta información, ya que utilizaremos la información introducida en el sistema principal.

- Introduzca las URL seguras siguientes y seleccione **Siguiente**.
  - URL del sitio de WebEx para que los usuarios organicen y asistan a reuniones
  - URL de Administración de WebEx para que los administradores del sistema gestionen su sistema

Confirmación de que la red está configurada correctamente

En esta pantalla se proporcionan enlaces a la ayuda en línea para los cambios de comunicaciones de red necesarios para su sistema. La ayuda en línea proporciona información detallada sobre los cambios del servidor DNS, así como los ajustes del cortafuegos.

Nota Debe realizar los cambios necesarios en el cortafuegos y el servidor DNS, ya que probaremos la conectividad de la red en el paso siguiente.

- Si todavía no lo ha hecho, complete la configuración de comunicaciones de red y seleccione **Siguiente**. Después de seleccionar **Siguiente**:
  - Despliegue automático: Empezaremos desplegando las máquinas virtuales necesarias para su sistema.

- Despliegue manual: En la siguiente pantalla, introduzca nombres de host para las máquinas virtuales y despliéguelas, si no lo ha hecho ya. Si ya las ha desplegado, enciéndalas y verifique que todas las máquinas virtuales arrancan correctamente.

Desplegar sus máquinas virtuales

En función de la información introducida anteriormente, desplegaremos las máquinas virtuales necesarias para su sistema.

Nota El despliegue tarda varios minutos en completarse. No salga de esta página hasta que todas las máquinas virtuales se hayan desplegado correctamente o hasta que el despliegue falle muestre mensajes de error indicando el problema.

- Complete una de las siguientes tareas:
  - Si no hay errores, cuando todas las marcas de estado sean de color verde seleccione **Siguiente**.
  - Si ve errores, corríjalos y seleccione **Siguiente**.

Nota Es posible que quiera seleccionar **Descargar archivo de registro** para obtener el archivo de registro para este despliegue. Esto le permite disponer de un registro del despliegue, que puede usarse para solucionar un despliegue con errores.

Nota Antes de la volver a realizar el despliegue, asegúrese de apagar y eliminar cualquier máquina virtual con errores. De lo contrario, puede que vea un mensaje de error sobre la existencia de máquinas virtuales cuando vuelva a intentar el despliegue del sistema.

Comprobación de su sistema

En función de la información introducida anteriormente, comprobaremos la configuración de su sistema. Comprobamos que las máquinas virtuales tienen la configuración mínima y validaremos el sitio WebEx y las URL de Administración de WebEx.

Nota La comprobación del sistema tarda varios minutos en completarse. No salga de esta página hasta que las comprobaciones se hayan completado correctamente o hasta que falle y muestre mensajes de error indicando el problema.

Nota Si vuelve a cargar la página antes de que las comprobaciones se hayan completado, se le devolverá a la primera página de este despliegue de sistema. Sin embargo, si las comprobaciones se han completado, se le llevará a la primera página de configuración básica (donde puede configurar el servidor de correo y un administrador).

Nota La URL del sitio de administración utilizada durante el proceso de despliegue es el nombre de host de la máquina virtual de administración. Sin embargo, durante la configuración básica, el nombre de host se sustituye por la URL del sitio de administración real. Como resultado, la primera vez que Inicie sesión en el sitio de administración, puede que el sistema le solicite que acepte la excepción de certificado.

- Complete una de las siguientes tareas:
  - Si no hay errores, cuando todas las marcas de estado sean de color verde seleccione **Siguiente**. Continúe con Definición del servidor de correo para su sistema, en la página 67.
  - Si existe un problema con la conectividad de red, compruebe que ha introducido correctamente su sitio de WebEx, las URL de administración y las direcciones IP. Verifique que estos sitios están en la subred correcta y que se han introducido en sus servidores DNS correctamente.
  - Si su sistema todavía tiene problemas para cumplir la capacidad mínima del sistema, tiene dos opciones.
    - Recomendamos que apague las máquinas virtuales del VMware vCenter y las elimine manualmente. Después, vuelva a intentar el despliegue del sistema en un sistema con recursos que cumplan o superen los requisitos mínimos.
    - Puede seleccionar proceder con su instalación actual. Si lo hace, deberá confirmar que renuncia a su derecho de solicitar soporte técnico de Cisco. Confirme marcando la casilla de verificación del mensaje de error y después seleccione **Siguiente**.
  - Si existen otros problemas con una o varias de sus máquinas virtuales, desde VMware vCenter, apague estas máquinas virtuales con errores y elimínelas manualmente. Después, vuelva a intentar el despliegue del sistema después de solucionar los problemas.

Nota Antes de la volver a realizar el despliegue, asegúrese de apagar y eliminar cualquier máquina virtual con errores. De lo contrario, puede que vea un mensaje de error sobre la existencia de máquinas virtuales cuando vuelva a intentar el despliegue del sistema.

  - En casos excepcionales, puede que vea **No probado**.
    Esto no significa que hay un problema con sus máquinas virtuales. Simplemente informa de que no hemos completado las comprobaciones del sistema; por ejemplo, debido a una pérdida temporal de la conectividad de red. Una vez finalizado el despliegue, puede iniciar sesión en el sitio de administración y comprobar estos recursos.
- Seleccione **Continuar** para ir a la primera página de la configuración básica (donde configura el servidor de correo y el administrador). Si otro administrador va a realizar la configuración básica, escriba y envíe esta URL al administrador de software.

CAPÍTULO 4

Instalar su sistema utilizando el despliegue manual

- Conceptos generales sobre el despliegue de su sistema, página 41
- Lista de comprobación de instalación, página 42
- Información necesaria para un despliegue manual, página 43
- Desplegar el archivo OVA desde un cliente VMware vSphere, página 45
- Seleccionar su idioma para la configuración, página 57
- Confirmar el despliegue, página 58
- Confirmar el tamaño de su sistema, página 58
- Seleccionar el sistema para instalar, página 58
- Seleccionar el tipo de despliegue de sistema, página 59
- Agregar acceso público, página 59
- Introducir la dirección VIP pública, página 60
- Introducir la dirección VIP privada, página 61
- URL del sitio de WebEx y URL de administración de WebEx, página 61
- Introducción de las URL del sitio de WebEx y de administración de WebEx, página 62
- Confirmación de que la red está configurada correctamente, página 63
- Desplegar sus máquinas virtuales, página 63
- Comprobación de su sistema, página 64

Conceptos generales sobre el despliegue de su sistema

Tamaños del sistema

- Sistema de 50 usuarios simultáneos

  - Normalmente es compatible con una empresa que tenga entre 500 y 1000 empleados
  - El sistema principal (sin HA) está formado por una máquina virtual de administración y un proxy inverso de Internet opcional (para acceso público)

- Sistema de 250 usuarios simultáneos
  - Normalmente es compatible con una empresa que tenga entre 2 500 y 5 000 empleados
  - Un sistema principal (sin HA) está formado por una máquina virtual de administración, una máquina virtual multimedia y un proxy inverso de Internet opcional (para acceso público).

- Sistema de 800 usuarios simultáneos
  - Normalmente es compatible con una empresa que tenga entre 8000 y 16 000 empleados
  - Un sistema principal (sin HA) está formado por una máquina virtual de administración, una máquina virtual multimedia y un proxy inverso de Internet opcional (para acceso público).

- Sistema de 2000 usuarios simultáneos
  - Normalmente es compatible con una empresa que tenga entre 20 000 y 40 000 empleados
  - El sistema principal (sin HA) está formado por una máquina virtual de administración, 3 máquinas virtuales multimedia, 2 máquinas Web y un proxy inverso de Internet opcional (para acceso público).

Términos utilizados durante el despliegue

Nombre del campo	Descripción
URL del sitio de WebEx	URL http segura para que los usuarios organicen y asistan a reuniones.
URL de administración de WebEx	URL http segura para que los administradores configuren, supervisen y administren el sistema.
VIP pública	Dirección IP para la URL del sitio de WebEx
VIP privada	• Dirección IP para la URL del sitio de administración • Dirección IP para la URL del sitio de WebEx (para usuarios internos únicamente, si tiene un DNS de horizonte dividido).

Lista de comprobación de instalación

Restricción Debe utilizar VMware vCenter para administrar los hosts ESXi en los que se despliegue el sistema de Cisco WebEx Meetings Server.

Cambios en las comunicaciones de red

Consulte la lista de comprobación de comunicaciones de red correspondiente a su despliegue. Hay dos consideraciones:

- Acceso público: define si los usuarios externos a su cortafuegos pueden organizar y acceder a reuniones desde Internet o desde dispositivos móviles.

  Cisco recomienda el acceso público, ya que genera una mejor experiencia de usuario para su personal móvil.

- Tipo de configuración DNS de su empresa: DNS de horizonte dividido o DNS de horizonte no dividido (configuración DNS más común).

  Para obtener más información sobre estos tipos de configuración DNS, consulte la *Guía de planificación del Cisco WebEx Meetings Server*.

- Puerto abierto 10200 desde el escritorio del administrador a la máquina virtual de administración.

  El explorador Web utiliza el puerto 10200 durante el despliegue.

Seleccione la lista de comprobación adecuada para su despliegue.

- Lista de comprobación de comunicaciones de red para un sistema con acceso público y horizonte DNS no dividido, en la página 11
- Lista de comprobación de comunicaciones de red para un sistema sin acceso público, en la página 12
- Lista de comprobación de comunicaciones de red para un sistema con acceso público y horizonte DNS dividido, en la página 12

Información necesaria

Nota La información necesaria varía si está realizando el despliegue automático (admitido para 50 usuarios simultáneos, 250 usuarios simultáneos y 800 usuarios simultáneos) de sistemas o un despliegue manual (admitido para todos los tamaños de sistema). Cisco le recomienda que seleccione el despliegue automático a menos que esté desplegando un sistema de 2000 usuarios, que requiere un despliegue manual. Consulte el enlace correspondiente más abajo.

Seleccione una de las siguientes opciones para obtener una lista de comprobación de la información necesaria para su tipo de despliegue:

- Información necesaria para un despliegue automático, en la página 16
- Información necesaria para un despliegue manual, en la página 43

Información necesaria para un despliegue manual

En un despliegue manual, usted crea todas las máquinas virtuales para su sistema utilizando el asistente OVA desde su cliente vSphere. A continuación, instala su sistema utilizando un despliegue manual.

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

Nota No olvide agregar los FQDN de la máquina virtual, las direcciones IP, las URL del sitio de administración y del sitio de WebEx y las direcciones VIP a sus servidores DNS antes de iniciar el despliegue del sistema. Utilizaremos esta información para comprobar la conectividad de la red al final del despliegue.

Para evitar cualquier problema de DNS, puede probar estas direcciones URL e IP antes de iniciar el despliegue OVA. De lo contrario, el despliegue del sistema fallará hasta que corrija estos errores.

Se trata de la información necesaria para su sistema, en orden.

Nombre del campo	Descripción	Valor para su sistema
VIP pública	Dirección IP para la URL del sitio de WebEx (acceso de usuarios del sitio para organizar y asistir a reuniones).	
VIP privada	• Dirección IP para la URL del sitio de administración (para que los administradores puedan configurar, supervisar y administrar el sistema) • Dirección IP para la URL del sitio de WebEx (para usuarios internos únicamente, si tiene un DNS de horizonte dividido).	
URL del sitio de WebEx	URL http segura (todo en minúscula) para que los usuarios puedan organizar y asistir a reuniones.	
URL de administración de WebEx	URL http segura (todo en minúscula) para que los administradores puedan configurar, supervisar y administrar el sistema.	
FQDN para las máquinas virtuales internas	Dependiendo del tamaño de sistema seleccionado, el nombre de dominio cualificado completo (todo en minúscula) de la máquina virtual multimedia y Web.	
(Solo acceso público) FQDN para el proxy inverso de Internet	Si tiene previsto agregar el acceso público, tiene que introducir el nombre de dominio cualificado completo (todo en minúscula) de la máquina virtual de proxy inverso de Internet.	

Qué hacer a continuación

Con esta información, inicie el despliegue del sistema introduciendo la URL de despliegue en una ventana del explorador. (La URL de despliegue se muestra en la ventana de la consola para la máquina virtual de administración).

Nota Si el sistema se reinicia antes de que la configuración se haya completado, se generará una nueva contraseña y deberá utilizar la URL de despliegue con la nueva contraseña.

Desplegar el archivo OVA desde un cliente VMware vSphere

Antes de desplegar sus sistema, debe usar el cliente VMware vSphere para desplegar la máquina virtual de administración para su sistema.

Nota El procedimiento siguiente se proporciona a modo de guía general. Las pantallas exactas que verá durante el despliegue de OVA dependerán de la configuración de vCenter, almacenamiento y red, y pueden ser diferentes a las que se muestran en este procedimiento. Consulte la documentación de VMware vSphere para obtener información completa sobre el asistente OVA.

Antes de comenzar

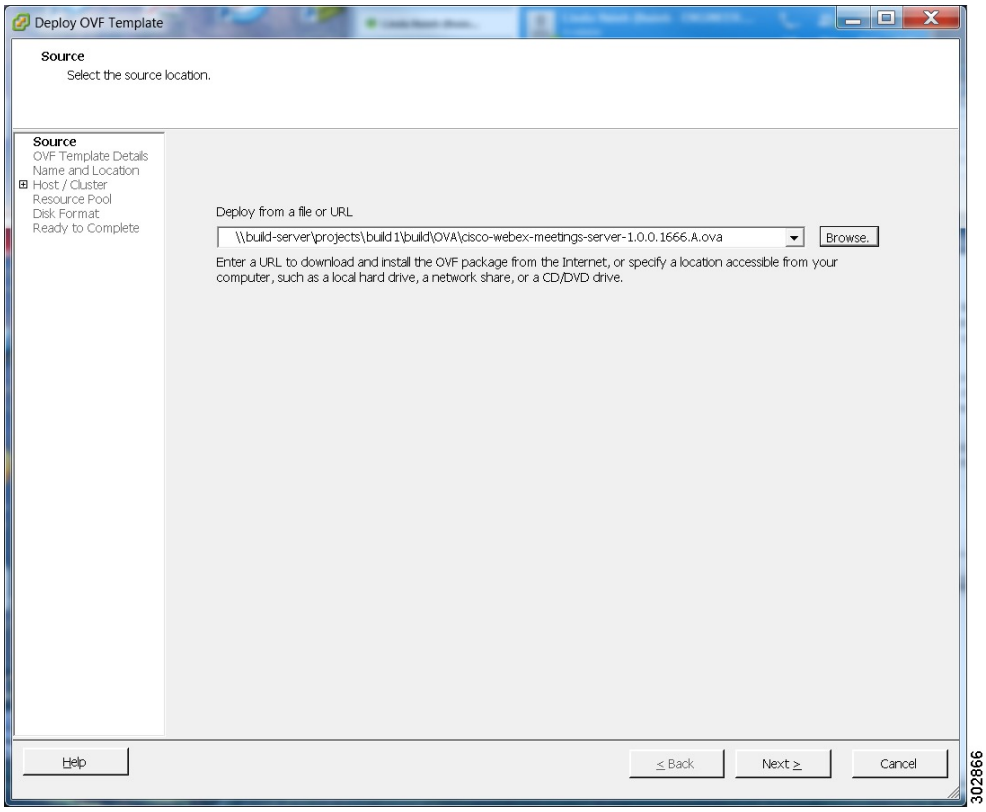
Obtenga el archivo OVA de Cisco WebEx Meetings Server para su sistema y colóquelo en una ubicación que sea accesible desde VMware vSphere.

Debe utilizar VMware vCenter para administrar los hosts ESXi en los que se despliegue el sistema de Cisco WebEx Meetings Server. Mediante el cliente de vSphere, inicie sesión en vCenter y despliegue el archivo OVA para la máquina virtual Administración.

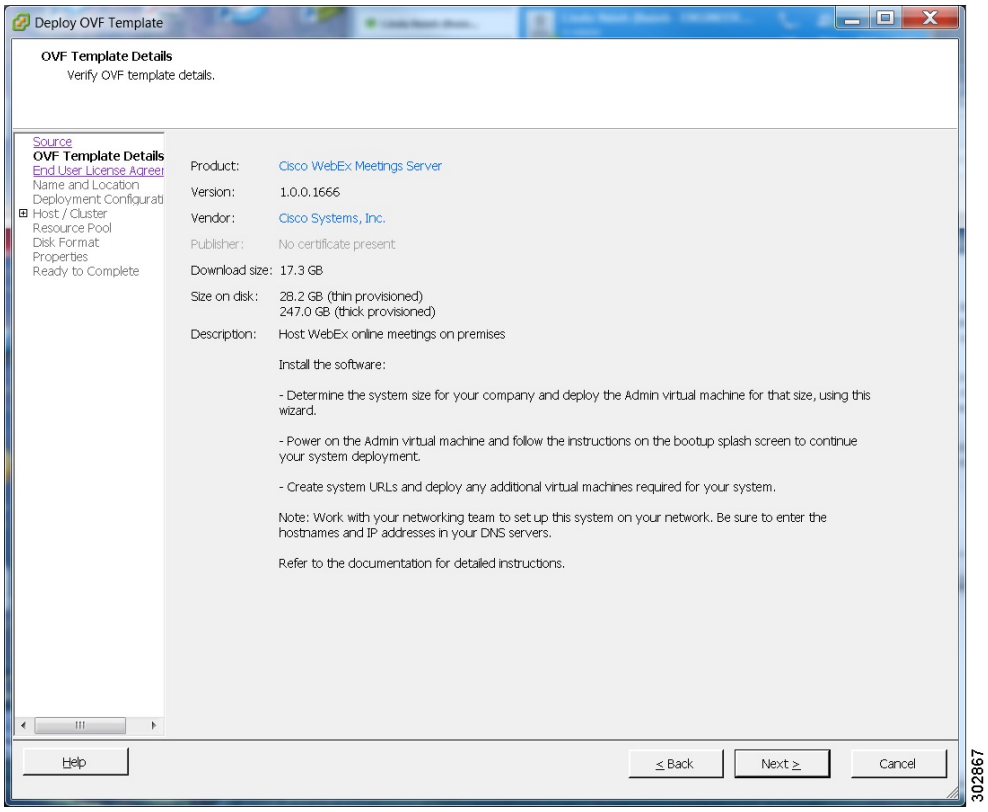
Procedimiento

Paso 1 Inicie sesión en su cliente VMware vSphere.
No olvide iniciar sesión como usuario con privilegios de administrador: para desplegar, configurar, encender o apagar y suprimir máquinas virtuales.

Paso 2 Seleccione **File** > **Deploy OVF Template...**



Paso 3 Seleccione **Explorar** para desplazarse hasta la ubicación del archivo OVA. Seleccione **Siguiente**. Puede seleccionar el enlace de **Cisco WebEx Meetings Server** para ir a una página Web con información detallada acerca de este sistema.



Paso 4 Lea el Acuerdo de licencia de usuario final y seleccione **Accept** y después **Next**.

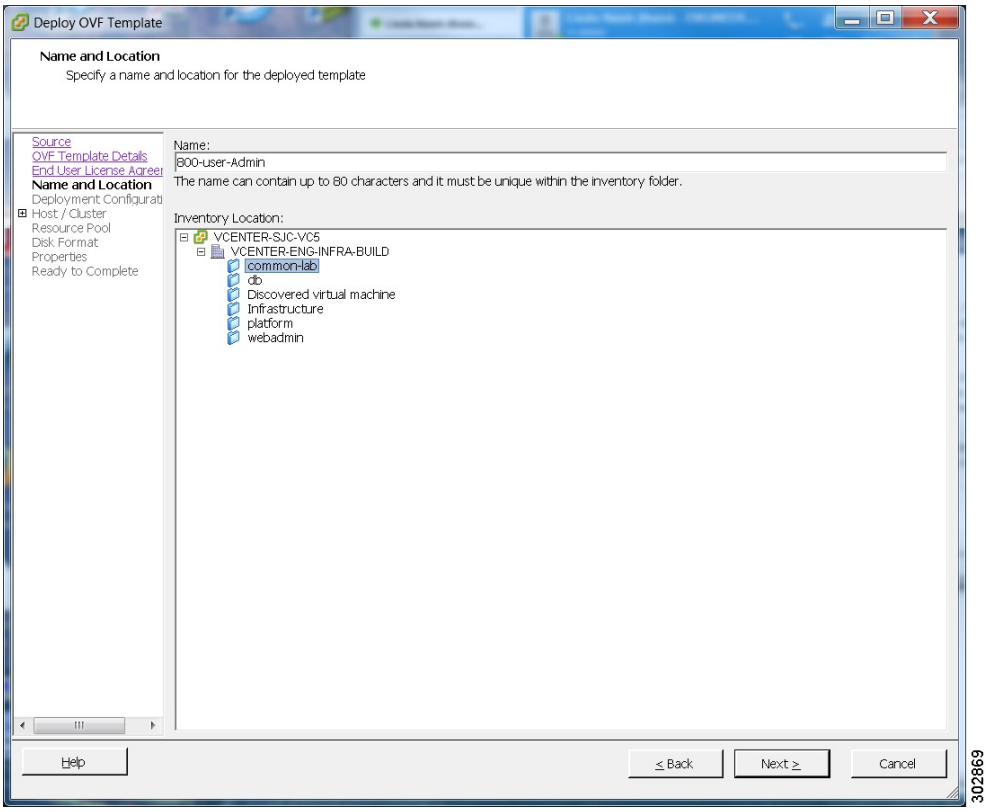
Paso 5 Desplácese hasta la ubicación del inventario vCenter y seleccione el lugar donde desea colocar la máquina virtual de administración.

Paso 6 Introduzca el nombre de la máquina virtual para su sistema y seleccione **Siguiente**. Para obtener más información sobre la selección del tamaño correcto para su empresa, consulte Tamaños del sistema.

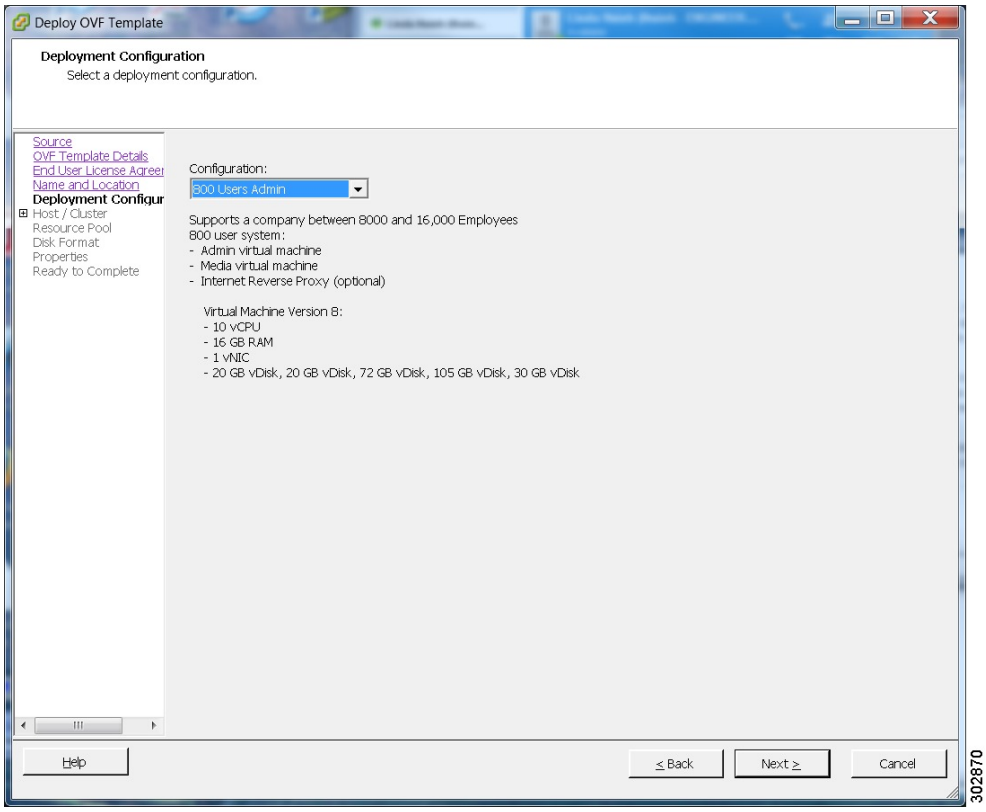
Nota Debe desplegar la máquina virtual de administración antes de desplegar cualquier otra máquina virtual. Si selecciona el despliegue automático (recomendado), las otras máquinas virtuales se despliegan automáticamente. Si selecciona el despliegue manual (necesario en un sistema con 2000 usuarios simultáneos), después de desplegar la máquina virtual de administración, debe desplegar las demás máquinas virtuales utilizando este mismo asistente.

Cisco le recomienda que incluya el tipo en el nombre de la máquina virtual; por ejemplo, incluya "Admin" en el nombre de la máquina virtual de administración para identificarla fácilmente en el inventario de vCenter.

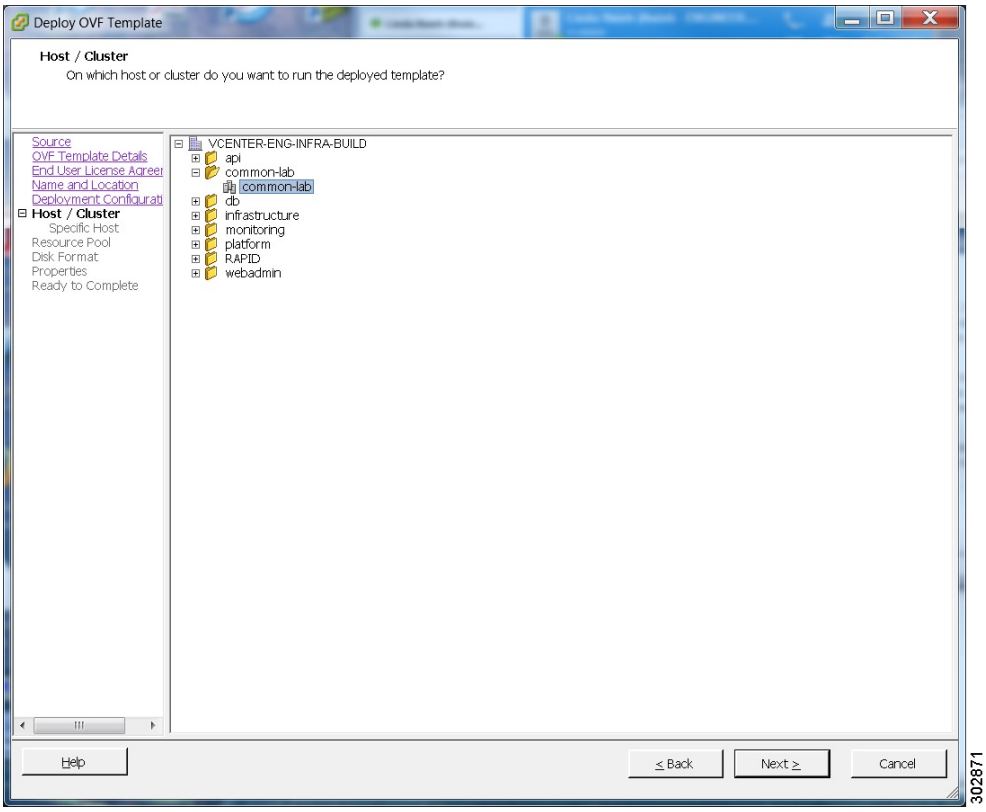
Nota Todas las máquinas virtuales internas para su sistema deben encontrarse en la misma subred que la máquina virtual de administración. (Dependiendo del tamaño de sistema que seleccione, puede que necesite uno o varios soportes y máquinas virtuales internas Web.)



Paso 7 En la lista desplegable, seleccione la máquina virtual para su tamaño de sistema y seleccione **Siguiente**. Asegúrese de desplegar la máquina virtual de administración antes que cualquier otra máquina virtual de su sistema.

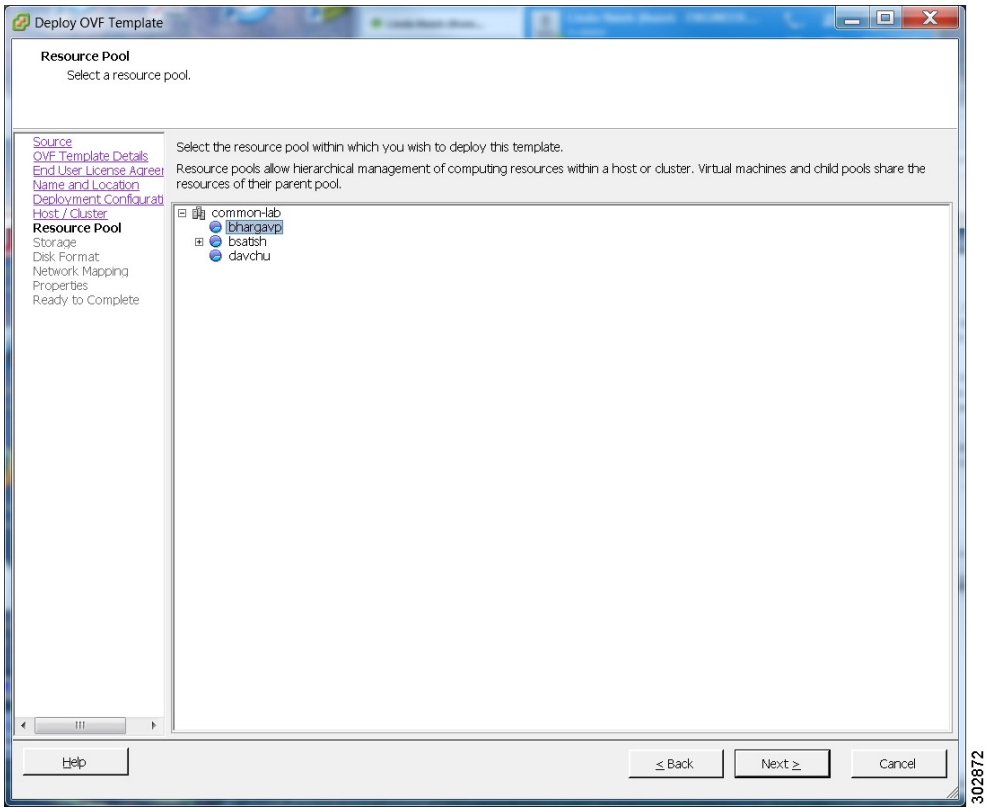


Paso 8 Desplácese por el inventario de vCenter y seleccione el clúster o host ESXi en el que desea desplegar las máquinas virtuales para su sistema. Seleccione **Siguiente**.

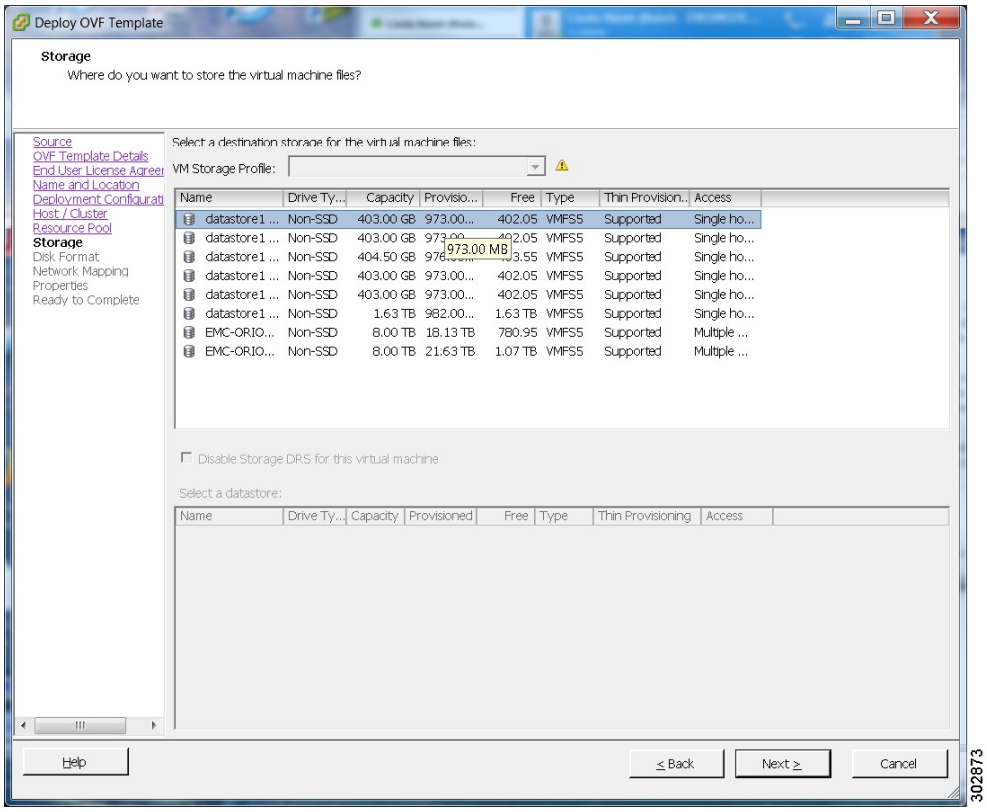


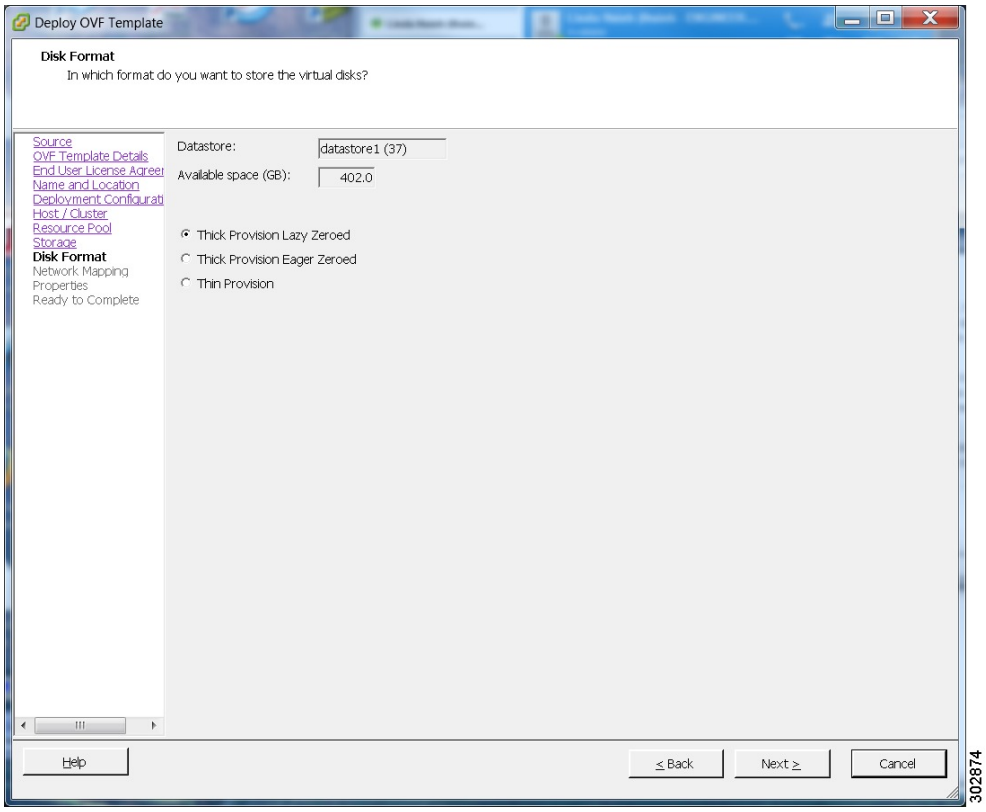
Paso 9 Si el clúster contiene una agrupación de recursos, seleccione la agrupación de recursos en la que desea desplegar la plantilla OVA y seleccione **Siguiente**.

Las agrupaciones de recursos comparten recursos de CPU y memoria o para trabajar con funciones de VMware, tales como DRS o vMotion. Las agrupaciones de recursos deben estar dedicadas para un único host de ESXi. No se recomienda utilizar las agrupaciones de recursos de VMware con Cisco WebEx Meetings Server.



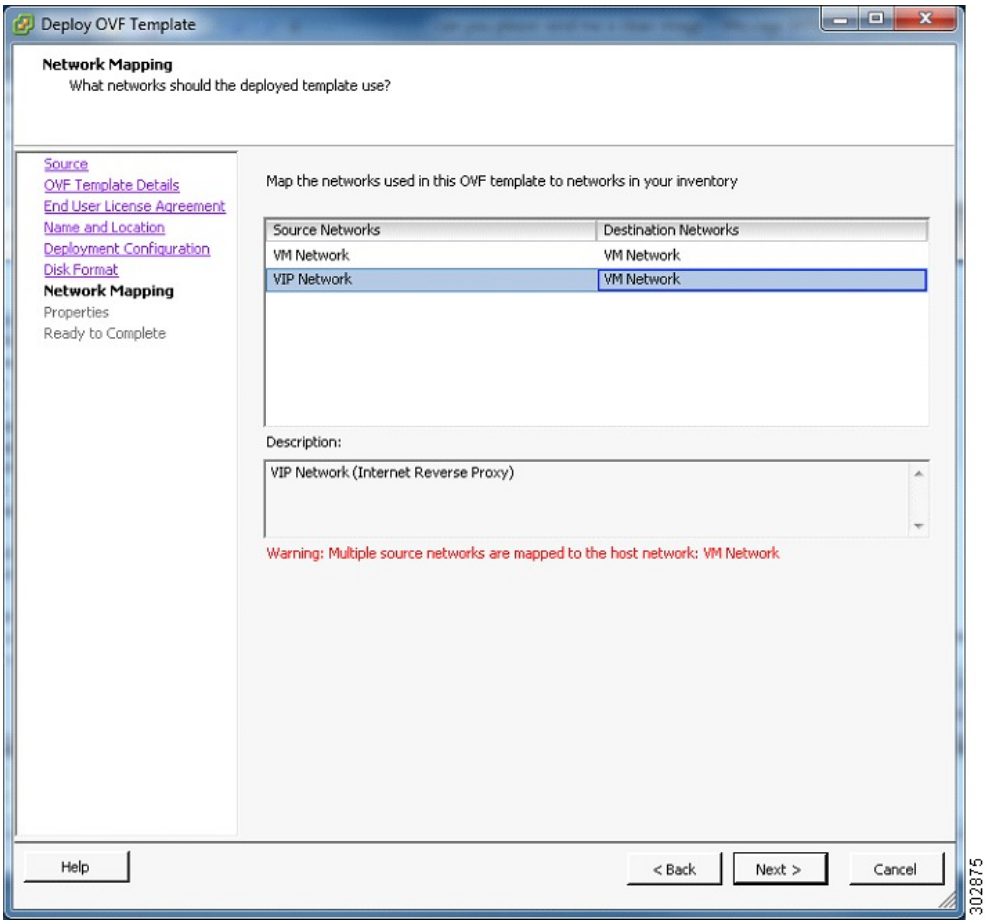
Paso 10 Seleccione el almacén de datos para su máquina virtual y el tipo de suministro para su máquina virtual. Debe seleccionar **Thick Provisioning** y crear el espacio de disco virtual máximo necesario para su sistema. Con Thin Provisioning, VMware asigna el espacio de sistema de archivos *cuando se necesita*, lo que puede causar un bajo rendimiento. Lazy zero es suficiente y eager zero es aceptable, pero eager zero tardará más tiempo en completarse.


Deploy OVF Template
Storage
Where do you want to store the virtual machine files?
Source
OVF Template Details
End User License Agreer
Name and Location
Deployment Configurati
Host / Cluster
Resource Pool
Storage
Disk Format
Network Mapping
Properties
Ready to Complete
Select a destination storage for the virtual machine files:
VM Storage Profile:
Name | Drive Ty... | Capacity | Provisio... | Free | Type | Thin Provision... | Access
datastore1 ... | Non-SSD | 403.00 GB | 973.00... | 402.05 | VMFS5 | Supported | Single ho...
datastore1 ... | Non-SSD | 403.00 GB | 973.00... | 402.05 | VMFS5 | Supported | Single ho...
datastore1 ... | Non-SSD | 404.50 GB | 973.00 MB | 3.55 | VMFS5 | Supported | Single ho...
datastore1 ... | Non-SSD | 403.00 GB | 973.00... | 402.05 | VMFS5 | Supported | Single ho...
datastore1 ... | Non-SSD | 403.00 GB | 973.00... | 402.05 | VMFS5 | Supported | Single ho...
datastore1 ... | Non-SSD | 1.63 TB | 982.00... | 1.63 TB | VMFS5 | Supported | Single ho...
EMC-ORIO... | Non-SSD | 8.00 TB | 18.13 TB | 780.95 | VMFS5 | Supported | Multiple ...
EMC-ORIO... | Non-SSD | 8.00 TB | 21.63 TB | 1.07 TB | VMFS5 | Supported | Multiple ...
Disable Storage DRS for this virtual machine
Select a datastore:
Name | Drive Ty... | Capacity | Provisioned | Free | Type | Thin Provisioning | Access
Help
< Back
Next >
Cancel
302873



Paso 11 Defina una asignación de red. Para cada red de origen, seleccione una red de destino en la lista desplegable en la columna **Destination Networks**. Seleccione **Siguiente**.

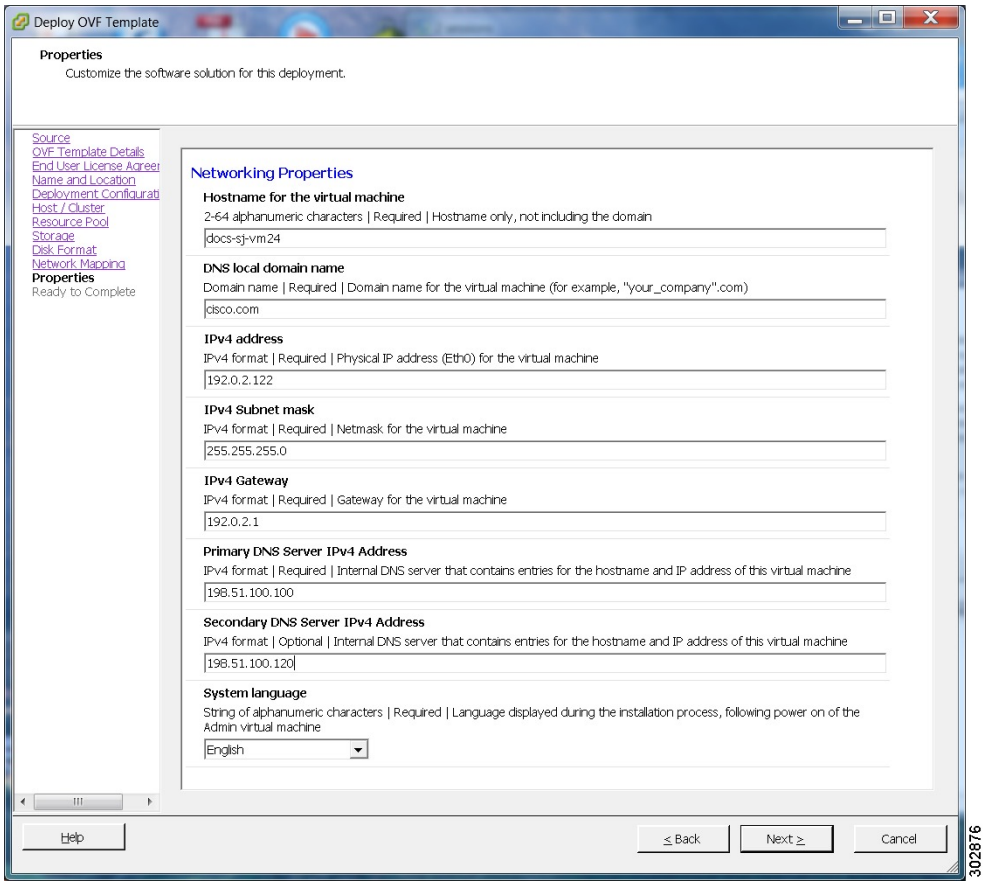
Nota Tanto la red VM como la red VIP deben correlacionarse con el mismo valor en la columna Red de destino. Puede ignorar el mensaje de advertencia acerca de varias redes de origen asignadas a la misma red de host.



Paso 12 Introduzca la siguiente información para la máquina virtual y después seleccione **Siguiente**.

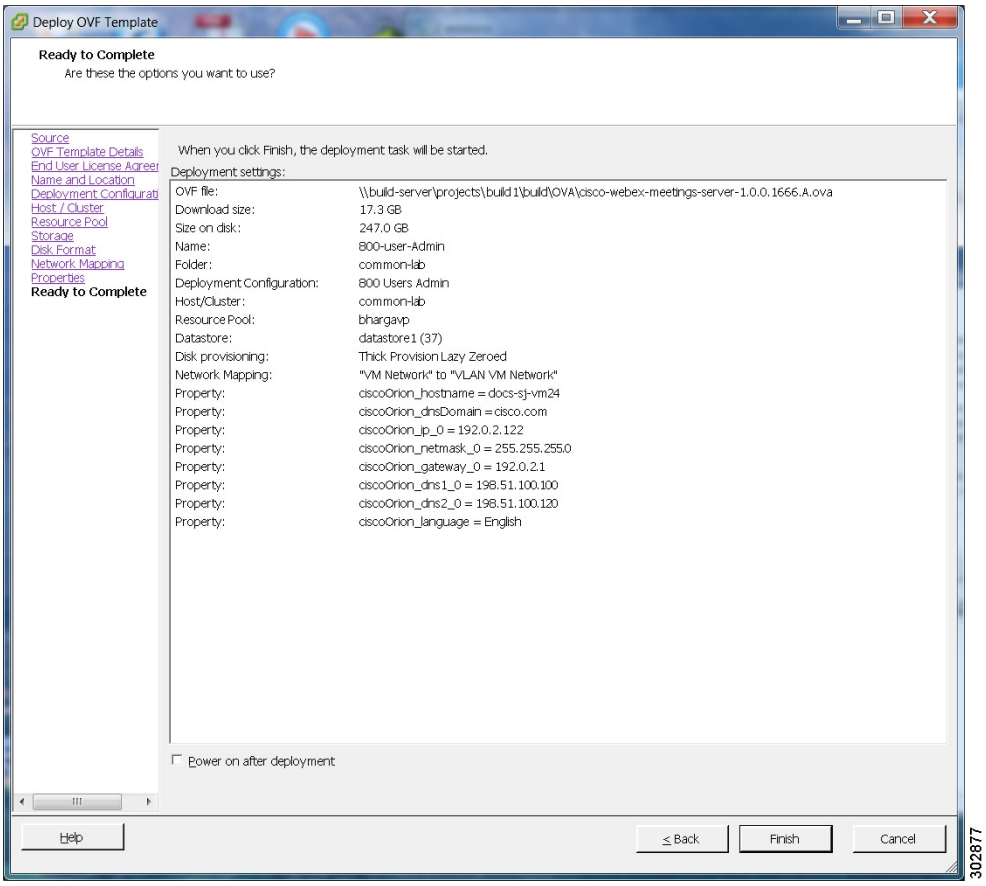
- Nombre de host de la máquina virtual (no incluya aquí el dominio)
- Dominio para la máquina virtual
- Dirección IPv4 (Eth0) para la máquina virtual
- Máscara de subred de la máquina virtual
- Dirección IP de puerta de enlace
- Servidor DNS primario que contiene entradas para el nombre de host y la dirección IP de la máquina virtual.
- Servidor DNS secundario que contiene entradas para el nombre de host y la dirección IP de esta máquina virtual
- El idioma se muestra durante el proceso de instalación, después del encendido de esta máquina virtual.

Nota Para evitar problemas de DNS, puede probar las direcciones URL e IP antes de iniciar el despliegue de OVA. El despliegue fallará si se producen errores.



Paso 13 Confirme la información que ha introducido. Si hay algún error, seleccione **Atrás** y cambie los valores.

Paso 14 Marque **Encender después del despliegue** y, a continuación, seleccione **Finalizar**.



Paso 15 Si está desplegando una máquina virtual de administración, vaya a vCenter y abra la ventana de la consola para la máquina virtual. Después de encenderse, comprobaremos la información de comunicaciones de red que ha introducido durante el despliegue de OVA.

- Si podemos confirmar la conectividad, se muestra una marca de selección de color verde.
- Si hay algún problema, se muestra una X de color rojo. Resuelva el error y vuelva a intentar el despliegue OVA.

Paso 16 Cuando esté confirmada toda la información, anote el URL visualizado que se muestra en la ventana de la consola.
Un administrador de software escribirá esta URL en un explorador Web, y continuará el despliegue del sistema.

Nota Si el sistema se reinicia antes de que la configuración se haya completado, se generará una nueva contraseña y deberá utilizar el URL con la nueva contraseña.

Qué hacer a continuación

Si realiza un despliegue manual, Cisco recomienda desplegar el resto de máquinas virtuales de su sistema en este momento. Esto evita posibles problemas tales como tiempos de espera agotados al encender las máquinas virtuales.

Si el despliegue se realiza correctamente, siga con el despliegue del sistema en una ventana de explorador.

Si el despliegue falla, consulte Comprobación de la configuración de comunicaciones de red después de un despliegue OVA incorrecto.

Comprobación de la configuración de comunicaciones de red después de un despliegue OVA incorrecto

Confirme las entradas de comunicaciones de red para la máquina virtual.

Importante No utilice **Edit Settings...** para ninguna máquina virtual de su sistema, a no ser que sea después de un error de despliegue. Una vez que el sistema está funcionando, deberá utilizar el sitio de administración de WebEx para editar la configuración de la máquina virtual. Si utiliza su cliente vSphere, el sistema no aceptará esos cambios.

Nota Para los pasos detallados, consulte la documentación de VMware vSphere.

Procedimiento

Paso 1 En el cliente Vsphere, seleccione **Power** > **Shut Down Guest** en la máquina virtual.

Paso 2 Encuentre la máquina virtual en el inventario y haga clic con el botón derecho en **Edit Settings...**.

Paso 3 Seleccione la pestaña **Options**.

Paso 4 Seleccione **Properties** y confirme que toda la información de comunicaciones de red se ha introducido correctamente. Si se necesita algún cambio, vuelva a desplegar el OVA con la configuración correcta.
Una posible causa del problema de red es que el enrutamiento VLAN no está configurado correctamente para el host ESXi. Debido a que la máquina virtual está en ese VLAN, la máquina virtual no tendrá conectividad de red. Desde la red en la que se encuentra el host ESXi, usted debería poder hacer una petición a la dirección IP predeterminada de la puerta de enlace de la VLAN que va a utilizar para las máquinas virtuales de su sistema.

Seleccionar su idioma para la configuración

Determine su idioma preferido para configurar el sistema.

Nota No cierre esta ventana del explorador hasta que el despliegue del sistema se haya completado. Si cierra el explorador antes, es posible que tenga que reiniciar el despliegue.

Antes de comenzar

Compruebe que ha desplegado la máquina virtual desde VMware vCenter. ConsulteDesplegar el archivo OVA desde un cliente VMware vSphere, en la página 18

Procedimiento

Paso 1 Seleccione el idioma en el menú desplegable.

Paso 2 Seleccione **Siguiente**.

Confirmar el despliegue

Procedimiento

Paso 1 Confirme si va a desplegar un sistema nuevo o a ampliar un sistema existente.

Paso 2 Seleccione **Siguiente**.

Confirmar el tamaño de su sistema

Usted seleccionó el tamaño de su sistema al desplegar la máquina virtual de administración utilizando el archivo OVA.

- Confirme que el tamaño del sistema que seleccionó durante el despliegue de OVA es correcto.
  - Si el tamaño del sistema seleccionado es correcto, seleccione **Siguiente**.
  - Si el tamaño del sistema seleccionado no es correcto, seleccione **Deseo cambiar el tamaño del sistema**.

a) Utilizando su cliente VMware vSphere, seleccione **Power** > **Shut Down Guest** para la máquina virtual de administración con el tamaño de sistema incorrecto.
b) Haga clic con el botón derecho en la máquina virtual y seleccione **Delete from Disk**.
c) Vuelva a desplegar el archivo OVA y seleccione la máquina virtual de administración del tamaño correcto.

Seleccionar el sistema para instalar

Procedimiento

Paso 1 Determine el tipo de instalación.

- Si está instalando este sistema por primera vez, seleccione **Instalar un sistema principal**.
- Si ha instalado un sistema principal y quiere un sistema redundante de alta disponibilidad, seleccione **Crear un sistema redundante de alta disponibilidad (HA)**.

Nota Usted no debe instalar un sistema HA antes de instalar el sistema principal, como no puede utilizar el sistema HA a menos que el sistema principal se haya instalado.

Paso 2 Seleccione **Siguiente**.

Seleccionar el tipo de despliegue de sistema

Determine cómo quiere desplegar cualquier otra máquina virtual necesaria para su sistema. Si ha seleccionado un sistema de 2000 usuarios, debe seleccionar un despliegue manual.

Procedimiento

Paso 1 Seleccione si desea desplegar las máquinas virtuales usted mismo, o bien si quiere que las despleguemos por usted.

- **Automático:** Es el método de instalación más rápido. Nosotros desplegamos todas las máquinas virtuales necesarias para su sistema.
  Cisco le recomienda que seleccione **Automático** a menos que esté desplegando un sistema de 2000 usuarios, que requiere un despliegue manual.

  Nota Utilizando Administración de Cisco WebEx, puede seguir realizando cambios en el sistema después del despliegue.

- **Manual:** Debe desplegar manualmente cada una de las máquinas virtuales usando VMware vCenter. Después de responder a unas cuantas preguntas sobre su sistema, le proporcionaremos una lista de máquinas virtuales necesarias para su sistema.

Su decisión de despliegue manual o automático depende de lo siguiente:

- Si tiene limitaciones de tiempo, un despliegue automático es más rápido que un despliegue manual.
- Si prefiere una guía paso a paso, seleccione el despliegue automático.
- Si está familiarizado con VMware vCenter y no desea proporcionar sus credenciales vCenter, seleccione el despliegue manual.

Paso 2 Seleccione **Siguiente**.

Agregar acceso público

Si agrega el acceso público, los usuarios pueden organizar y asistir a reuniones desde Internet o dispositivos móviles. Para obtener más información sobre la configuración de este campo para su empresa, consulte la *Guía de planificación del Cisco WebEx Meetings Server*.

Nota Siempre puede cambiar esta opción más tarde a través del sitio de administración de WebEx.

Procedimiento

Paso 1 Seleccione si desea que los usuarios externos puedan organizar o asistir a reuniones.

- Si quiere agregar el acceso público, compruebe que la casilla de verificación **Crear una máquina virtual de proxy inverso de Internet** está marcada.
- Si solo quiere que los usuarios internos (detrás del cortafuegos de su empresa) puedan organizar o asistir a reuniones, elimine la selección de la casilla de verificación **Crear una máquina virtual de proxy inverso de Internet**.

Paso 2 Seleccione **Siguiente**.

Qué hacer a continuación

- Con acceso público: Seleccionar los ajustes de vCenter para su máquina virtual de proxy inverso de Internet, en la página 34
- Sin acceso público: Introducir la dirección VIP privada, en la página 36

Introducir la dirección VIP pública

- Esta dirección VIP público debe estar visible tanto desde Internet como desde la red interna (solamente DNS de horizonte dividido).
- La dirección VIP pública debe estar en la misma subred que el proxy inverso de Internet.
- Si no tiene un DNS de horizonte dividido, todos los usuarios utilizan la dirección VIP pública para organizar y asistir a reuniones.
- Si tiene un DNS de horizonte dividido y ha agregado el acceso público, todos los usuarios externos usan la dirección VIP pública para organizar y asistir a reuniones.

Para obtener más información sobre el DNS de horizonte dividido y no dividido, así como del acceso público, consulte la *Guía de planificación del Cisco WebEx Meetings Server*.

Nota Si está creando un sistema de alta disponibilidad (HA), no tiene que volver a introducir esta información, ya que utilizaremos la información introducida en el sistema principal.

- Introduzca la dirección IPv4 VIP pública y seleccione **Siguiente**.

Introducir la dirección VIP privada

Los administradores configuran, supervisan y mantienen el sistema desde la URL del sitio de administración que dirige a la dirección VIP privada.

Nota Si tiene un DNS de horizonte dividido, todos los usuarios internos también usan la dirección VIP privada para organizar y asistir a reuniones.

Nota Si está agregando un sistema de alta disponibilidad (HA), no tiene que volver a introducir esta información, ya que utilizaremos la información introducida en el sistema principal.

Antes de comenzar

La dirección IP virtual privada (VIP) debe encontrarse en la misma subred que sus máquinas virtuales internas (administración y multimedia, si procede).

- Introduzca la dirección VIP privada Ipv4 y seleccione **Siguiente**.

URL del sitio de WebEx y URL de administración de WebEx

URL del sitio de WebEx

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

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

URL de administración de WebEx

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

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

Puede seleccionar casi cualquier nombre para estas URL, utilizando todos los caracteres en minúscula. Sin embargo, no puede usar lo siguiente como nombre de host en las URL del sitio:

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

- Cliente
- Logotipo de la compañía
- Distribuidor
- Docs
- elm-admin
- elm-client-services
- Correos electrónicos
- Mantenimiento
- Manager
- orion
- oriondata
- oriontemp
- nbr
- npp
- Investigación
- Aviso
- Raíz
- Energía solar
- TomcatROOT
- upgradeserver
- url0107ld
- Versión
- WBXService
- Centro de

Introducción de las URL del sitio de WebEx y de administración de WebEx

- No puede reutilizar los nombres de host de las máquinas virtuales en su sistema en la porción de nombre de host de la URL del sitio de WebEx o de administración de WebEx.
- La URL del sitio de WebEx debe ser diferente de la URL de administración de WebEx.

Nota Si está agregando un sistema de alta disponibilidad (HA), no tiene que volver a introducir esta información, ya que utilizaremos la información introducida en el sistema principal.

- Introduzca las URL seguras siguientes y seleccione **Siguiente**.
  - URL del sitio de WebEx para que los usuarios organicen y asistan a reuniones
  - URL de Administración de WebEx para que los administradores del sistema gestionen su sistema

Confirmación de que la red está configurada correctamente

En esta pantalla se proporcionan enlaces a la ayuda en línea para los cambios de comunicaciones de red necesarios para su sistema. La ayuda en línea proporciona información detallada sobre los cambios del servidor DNS, así como los ajustes del cortafuegos.

Nota Debe realizar los cambios necesarios en el cortafuegos y el servidor DNS, ya que probaremos la conectividad de la red en el paso siguiente.

- Si todavía no lo ha hecho, complete la configuración de comunicaciones de red y seleccione **Siguiente**. Después de seleccionar **Siguiente**:
  - Despliegue automático: Empezaremos desplegando las máquinas virtuales necesarias para su sistema.
  - Despliegue manual: En la siguiente pantalla, introduzca nombres de host para las máquinas virtuales y despliéguelas, si no lo ha hecho ya. Si ya las ha desplegado, enciéndalas y verifique que todas las máquinas virtuales arrancan correctamente.

Desplegar sus máquinas virtuales

Después de proporcionar información sobre las máquinas virtuales en el sistema, intentaremos conectar con cada una de las máquinas virtuales desplegadas para su sistema.

Nota No salga de esta página hasta que el sistema haya conectado con todas las máquinas virtuales, o hasta que la conexión falle muestre mensajes de error que indican el problema.

Procedimiento

Paso 1 Introduzca los nombres de dominio cualificados completos (FQDNs) para cualquier máquina virtual adicional necesaria para su sistema. (Ha introducido anteriormente el FQDN de la máquina virtual de administración al desplegarla desde el archivo OVA).

Paso 2 Si todavía no lo ha hecho, utilizando VMware vCenter, despliegue todas las máquinas virtuales adicionales necesarias para su sistema.

Paso 3 Encienda todas las máquinas virtuales y compruebe que reciben alimentación. A continuación, seleccione **Detectar máquinas virtuales**.

Estamos intentando conectar con estas máquinas virtuales. Esto podría llevar varios minutos.

Paso 4 Espere hasta que el estado **Conectada** se muestre para todas las máquinas virtuales y después complete uno de los pasos siguientes.

- Si no hay errores, el estado muestra marcas de comprobación verdes. Si está satisfecho, seleccione **Siguiente**. De lo contrario, todavía puede cambiar los FQDNs de las máquinas virtuales; a continuación, seleccione de nuevo **Detectar máquinas virtuales**.
- Si ve errores, corríjalos y seleccione **Siguiente**.

  Nota Es posible que quiera seleccionar **Descargar archivo de registro** para obtener el archivo de registro para este despliegue. Esto le permite disponer de un registro del despliegue, que puede usarse para solucionar un despliegue con errores.
- Si existen otros problemas con una o varias de sus máquinas virtuales, desde VMware vCenter, apague estas máquinas virtuales con errores y elimínelas manualmente. Después de solucionar los problemas, vuelva a desplegar las máquinas virtuales desde el archivo OVA y después seleccione **Detectar máquinas virtuales**.

  Nota Antes de la volver a realizar el despliegue, asegúrese de apagar y eliminar cualquier máquina virtual con errores. De lo contrario, es posible que vea mensajes de error sobre máquinas virtuales existentes.

Comprobación de su sistema

En función de la información introducida anteriormente, comprobaremos la configuración de su sistema. Comprobamos que las máquinas virtuales tienen la configuración mínima y validaremos el sitio WebEx y las URL de Administración de WebEx.

Nota La comprobación del sistema tarda varios minutos en completarse. No salga de esta página hasta que las comprobaciones se hayan completado correctamente o hasta que falle y muestre mensajes de error indicando el problema.

Nota Si vuelve a cargar la página antes de que las comprobaciones se hayan completado, se le devolverá a la primera página de este despliegue de sistema. Sin embargo, si las comprobaciones se han completado, se le llevará a la primera página de configuración básica (donde puede configurar el servidor de correo y un administrador).

Nota La URL del sitio de administración utilizada durante el proceso de despliegue es el nombre de host de la máquina virtual de administración. Sin embargo, durante la configuración básica, el nombre de host se sustituye por la URL del sitio de administración real. Como resultado, la primera vez que Inicie sesión en el sitio de administración, puede que el sistema le solicite que acepte la excepción de certificado.

- Complete una de las siguientes tareas:

- Si no hay errores, cuando todas las marcas de estado sean de color verde seleccione **Siguiente**. Continúe con Definición del servidor de correo para su sistema, en la página 67.
- Si existe un problema con la conectividad de red, compruebe que ha introducido correctamente su sitio de WebEx, las URL de administración y las direcciones IP. Verifique que estos sitios están en la subred correcta y que se han introducido en sus servidores DNS correctamente.
- Si su sistema todavía tiene problemas para cumplir la capacidad mínima del sistema, tiene dos opciones.
  - Recomendamos que apague las máquinas virtuales del VMware vCenter y las elimine manualmente. Después, vuelva a intentar el despliegue del sistema en un sistema con recursos que cumplan o superen los requisitos mínimos.
  - Puede seleccionar proceder con su instalación actual. Si lo hace, deberá confirmar que renuncia a su derecho de solicitar soporte técnico de Cisco. Confirme marcando la casilla de verificación del mensaje de error y después seleccione **Siguiente**.
- Si existen otros problemas con una o varias de sus máquinas virtuales, desde VMware vCenter, apague estas máquinas virtuales con errores y elimínelas manualmente. Después, vuelva a intentar el despliegue del sistema después de solucionar los problemas.

Nota Antes de la volver a realizar el despliegue, asegúrese de apagar y eliminar cualquier máquina virtual con errores. De lo contrario, puede que vea un mensaje de error sobre la existencia de máquinas virtuales cuando vuelva a intentar el despliegue del sistema.

- En casos excepcionales, puede que vea **No probado**.
  Esto no significa que hay un problema con sus máquinas virtuales. Simplemente informa de que no hemos completado las comprobaciones del sistema; por ejemplo, debido a una pérdida temporal de la conectividad de red. Una vez finalizado el despliegue, puede iniciar sesión en el sitio de administración y comprobar estos recursos.

- Seleccione **Continuar** para ir a la primera página de la configuración básica (donde configura el servidor de correo y el administrador). Si otro administrador va a realizar la configuración básica, escriba y envíe esta URL al administrador de software.

CAPÍTULO 5

Configurar el servidor de correo, la zona horaria y la configuración regional

- Definición del servidor de correo para su sistema, página 67
- Definición de la zona horaria y la configuración regional para el sistema, página 68
- Confirmación de los ajustes de servidor de correo, zona horaria y configuración regional, página 68
- Definición de la primera cuenta de administrador para su sistema, página 68
- Prueba del sistema, página 69

Definición del servidor de correo para su sistema

Al definir el servidor de correo, el sistema puede usar su servidor de correo corporativo para enviar correos electrónicos a los administradores (alertas, alarmas, informes, etc.) y a los usuarios (invitaciones para reuniones, reinicios de contraseña, etc.)

Antes de comenzar

Debe haber completado correctamente el despliegue de las máquinas virtuales necesarias para su sistema.

Procedimiento

Paso 1 Introduzca el nombre de dominio cualificado completo (FQDN) de un servidor de correo que su sistema utilizará para enviar los correos electrónicos.

Paso 2 Si quiere la opción **TLS activado**, marque esta casilla de verificación.

Paso 3 Puede editar el campo **Puerto** si no quiere usar el valor predeterminado.
De forma predeterminada, el número de puerto SMTP es 25 o 465 (número de puerto SMTP seguro).

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

Paso 4 Si quiere activar la autenticación del servidor de correo, marque la casilla de verificación **Autenticación de servidor activada**.
Si activa la autenticación del servidor, aparecen los campos **Nombre de usuario** y **Contraseña**.

Paso 5 Si aparecen, introduzca las credenciales de **Nombre de usuario** y **Contraseña** del sistema para acceder al servidor de correo corporativo.
Se envían correos electrónicos desde el sistema por admin @<WebEx-site-URL>. Asegúrese de que el servidor de correo puede reconocer este usuario.

Paso 6 Seleccione **Siguiente**.

Definición de la zona horaria y la configuración regional para el sistema

Antes de comenzar

Si está ejecutando Windows 7 y tiene el sitio de Cisco WebEx abierto en un explorador Internet Explorer 10, tal vez desee seleccionar los estándares de Internet Explorer 10 de documentos para asegurarse de que todos los botones de la aplicación funcionen correctamente.

- Seleccione **Herramientas** > **Herramientas de desarrollo**.
- En la parte superior de la ventana Herramientas de desarrollo, seleccione **Modo de documento: Estándares de IE7** > **Estándares de Internet Explorer 10**.

Procedimiento

Paso 1 Seleccione la zona horaria para su sistema de la lista desplegable.

Paso 2 Seleccione la configuración regional para su sistema de la lista desplegable.

Paso 3 Seleccione **Siguiente**.

Confirmación de los ajustes de servidor de correo, zona horaria y configuración regional

Ha introducido estos ajustes en la pantalla anterior.

- Revise la información que ha introducido anteriormente. Si hay algún error, seleccione **Atrás**. De lo contrario, seleccione **Siguiente**.

Definición de la primera cuenta de administrador para su sistema

El sistema crea una única cuenta de administrador como parte del proceso de despliegue.

Precaución Este administrador debe iniciar sesión en el sistema, crear una contraseña y agregar usuarios y administradores adicionales. De lo contrario, ningún otro usuario tendrá acceso al sistema.

Antes de comenzar

Debe definir correctamente un servidor de correo para el sistema para enviar correos electrónicos a los administradores y usuarios.

Procedimiento

Paso 1 Introduzca el nombre y los apellidos del administrador.

Paso 2 Introduzca la dirección de correo electrónico completa del administrador y después confírmela introduciéndola por segunda vez.

Paso 3 Seleccione **Siguiente** para crear su contraseña.

Paso 4 Introduzca su contraseña y después confírmela introduciéndola por segunda vez.

Paso 5 Seleccione **Enviar** para iniciar sesión en el sitio de administración de WebEx.

Paso 6 Debe iniciar sesión en el sistema y agregar usuarios adicionales. Después de la creación de cada nuevo usuario, el sistema envía un correo electrónico a cada usuario, dándole la bienvenida y pidiéndole que inicie sesión y que cree una contraseña.
Después del primer inicio de sesión, cada administrador tendrá la oportunidad de ver un tutorial del sistema. Los administradores pueden ver el tutorial inmediatamente, o bien verlo posteriormente.

Prueba del sistema

Algunas de las pruebas recomendadas para ejecutar en el sistema se muestran en esta sección. Puede realizar estas pruebas y validar su sistema utilizando dos herramientas de diagnóstico descritas en las páginas de soporte para este producto: La prueba de reuniones y la prueba de recursos del sistema.

Cuando se prueba un sistema actualizado, puede conservar el sistema original hasta que haya terminado de probar el sistema actualizado (pero no puede encender los dos sistemas al mismo tiempo). Una vez que esté conforme con los resultados de la pruebas del sistema actualizado, puede eliminar (de forma definitiva) el sistema existente. Asegúrese de que su sistema actualizado está funcionando al suprimir o eliminar el sistema existente. De esta forma, se evita la eliminación accidental del archivo de disco de máquina virtual (VMDK) base, al cual puede acceder el sistema actualizado.

- Agregar, editar, activar y desactivar usuarios.
- Planificar y organizar una reunión.
- Volver a planificar una reunión existente.
- Eliminar una serie de reuniones o una reunión futura.
- Abrir un adjunto de la reunión.
- Reproducir una grabación de la reunión.

CAPÍTULO 6

Modificación del sistema después de la instalación

En este capítulo se explican los distintos procedimientos de modificación del sistema que puede hacer después del despliegue inicial de su sistema.

- Agregar HA, actualizar o ampliar el sistema, página 71
- Preparación para un procedimiento de modificación del sistema, página 72

Agregar HA, actualizar o ampliar el sistema

Se considera que los siguientes procedimientos modifican el sistema y requieren una preparación avanzada por parte del administrador.

- Agregar o eliminar un sistema de alta disponibilidad (HA)
- Actualizar el sistema a una versión más reciente usando un archivo de actualización OVA
- Actualizar el sistema volviendo a desplegarlo desde un archivo OVA para la versión de actualización
- Ampliar el tamaño del sistema del tamaño actual a un tamaño superior

Colocará el sistema en modo de mantenimiento cuando realice estos procedimientos. Por ello, es posible que quiera programar algunos de estos procedimientos juntos, por ejemplo, ampliar el sistema y actualizarlo durante la misma ventana de mantenimiento.

Tenga en cuenta las restricciones siguientes:

- Si ya ha agregado HA a su sistema y quiere ampliar o actualizar el sistema, tendrá que volver a desplegar el sistema HA después de la actualización.

  Las ampliaciones o actualizaciones del sistema requieren el despliegue de un nuevo sistema, con la transferencia de los datos del sistema al sistema ampliado o actualizado. Cuando despliegue un nuevo sistema, tendrá que seleccionar entre desplegar un sistema principal o el sistema HA; no puede desplegar ambos a la vez. Por lo tanto, primero debe desplegar el sistema principal con el archivo OVA y después desplegar el sistema HA otra vez, con el mismo archivo OVA usado para el sistema principal.

- Si está planificando agregar un sistema HA y actualizarlo (con un archivo de actualización ISO), le recomendamos que primero añada el sistema HA y después actualice el sistema combinado (primario y HA).

  El procedimiento de actualización actualiza el sistema completo, con o sin el sistema HA. Si actualiza primero el sistema y después agrega el HA, primero tiene que desplegar el sistema HA y después actualizarlo (para que el sistema principal y el HA tengan la misma versión). Si agrega primero el HA, el procedimiento de actualización actualiza el sistema combinado primario y HA al mismo tiempo.

- El procedimiento de actualización actualiza el sistema completo, con o sin un proxy inverso de Internet.

Preparación para un procedimiento de modificación del sistema

En esta sección se describe cómo prepararse para un procedimiento de modificación del sistema: ampliar su sistema, agregar un sistema de alta disponibilidad, activar el acceso público, actualizar su sistema, etc. creando una copia de seguridad de su sistema.

Aunque puede seleccionar hacerlo, las copias de seguridad no son necesarias para una expansión o actualización de su sistema. Durante una expansión o actualización, usted despliega un nuevo sistema y transfiere los datos de su sistema existente al nuevo sistema. Si hay un problema con la expansión o actualización, puede apagar el nuevo sistema y seguir usando el sistema existente.

Precaución Los usuarios no pueden acceder al sistema para reuniones, ya que este procedimiento requiere un acceso exclusivo al sistema. No olvide programar este procedimiento durante un periodo de tiempo que no interrumpa demasiado las actividades de sus usuarios.

Los otros administradores del sistema no deben acceder al sistema durante este procedimiento. Si lo hacen, sus cambios no se guardarán y el resultado puede ser impredecible. Deberán esperar hasta que este procedimiento se complete y después iniciar sesión en Administración de Cisco WebEx para completar sus tareas.

Nota Asegúrese de ponerse de acuerdo con otros administradores del sistema antes de iniciar un procedimiento de modificación del sistema.

Atención Si no necesita crear una copia de seguridad de los equipos virtuales, entonces no necesita completar este procedimiento. Sin embargo, como una buena práctica, Cisco recomienda crear una copia de seguridad. Las copias de seguridad permiten revertir el sistema, si el procedimiento genera un error.

Procedimiento

Paso 1 Inicie sesión en el sitio de Administración de Cisco WebEx.

Paso 2 Seleccione **Activar el modo de mantenimiento**.

Paso 3 Utilice VMware Data Recovery (denominado VMware vSphere Data Protection empezando por vSphere versión 5.1) para crear una copia de seguridad de cada una de sus máquinas virtuales.

La copia de seguridad le ayudará a revertir su máquina virtual al estado anterior al procedimiento de modificación del sistema. Para obtener información adicional, consulte Creación de una copia de seguridad por medio de VMware vCenter, en la página 4. Para obtener información detallada sobre esta copia de seguridad, consulte la *Guía de administración de VMware Data Recovery* o la *Guía de administración de vSphere Data Protection*.

Nota Si tiene previsto hacer una expansión o actualización, elimine todas las instantáneas VMware en el sistema existente. De esta forma, se evita la eliminación accidental del archivo VMDK de base 4 del disco duro, al cual puede acceder el sistema ampliado o actualizado.

Paso 4 Vuelva a iniciar sesión en el sitio de Administración de Cisco WebEx pero no apague el modo de mantenimiento.

Paso 5 Continúe con el procedimiento de modificación del sistema.

CAPÍTULO 7

Agregar un sistema de alta disponibilidad

- Agregar un sistema HA usando el despliegue automático, página 75
- Agregar un sistema HA usando el despliegue manual, página 77
- Comprobar que la versión de su sistema principal y el sistema de alta disponibilidad son la misma, página 79
- Agregar un sistema de alta disponibilidad, página 81
- Prueba del sistema, página 82

Agregar un sistema HA usando el despliegue automático

Instrucciones antes de empezar

- Debe haber desplegado correctamente un sistema principal.
- El sistema principal está en modo de mantenimiento.
- Cree una copia de seguridad de los sistemas principal y de alta disponibilidad. Consulte .Creación de una copia de seguridad por medio de VMware vCenter, en la página 4

Consideraciones previas a la adición de un sistema de alta disponibilidad

Un sistema de alta disponibilidad es un sistema redundante que se agrega y pasa a formar parte de su sistema. Proporciona alta disponibilidad en caso de producirse un fallo de una máquina virtual.

El sistema de alta disponibilidad (HA) tiene los requisitos siguientes:

- El sistema HA debe tener la misma versión que el sistema principal.

  Si ha actualizado el sistema principal, no olvide hacer lo mismo para el sistema HA.
- Si tiene autorización para ello (con el contrato de servicio pertinente), Cisco le recomienda desplegar el sistema de alta disponibilidad utilizando el archivo OVA que sea de la misma versión (antes de aplicar parches) que el sistema principal.
- El tamaño del sistema HA debe ser el mismo que el tamaño del sistema principal.
- Si ha agregado el acceso público en el sistema principal, tiene que agregarlo también al sistema HA.

- Las máquinas virtuales internas del sistema HA deben encontrarse en la misma subred que las máquinas virtuales internas del sistema principal.
- Si ha agregado el acceso público, la máquina virtual de proxy inverso de Internet del sistema HA debe encontrarse en la misma subred que la máquina virtual de proxy inverso de Internet del sistema principal.
- Dado que este proceso agrega máquinas virtuales a su sistema, su certificado de seguridad actual será invalidado y tendrá que actualizarlo, a no ser que esté utilizando un certificado autofirmado.
- Si tenía anteriormente un sistema de alta disponibilidad, retírelo. Si está desplegando un nuevo sistema de alta disponibilidad, no podrá volver a utilizar las máquinas virtuales en el sistema HA anterior. Debe volver a desplegar un nuevo sistema de alta disponibilidad con nuevas máquinas virtuales.

Resumen de tareas para agregar un sistema de alta disponibilidad utilizando el despliegue automático

Siga estas tareas en orden.

Tarea	Descripción	Para obtener información detallada, consulte
1	Utilizando el cliente VMware vSphere, despliegue la máquina virtual de administración para el sistema HA.	Desplegar el archivo OVA desde un cliente VMware vSphere, en la página 18
2	Encienda la máquina virtual de administración para el sistema HA y escriba la URL de despliegue.	
3	Introduzca la URL en un explorador Web y continúe con el despliegue del sistema HA.	
4	Seleccione su idioma preferido para el despliegue del sistema HA.	Seleccionar su idioma para la configuración, en la página 30
5	Confirme el tamaño del sistema para el sistema HA. (Este tamaño de sistema debe coincidir con el tamaño del sistema principal).	Confirmar el tamaño de su sistema, en la página 31
6	Seleccione **Crear un sistema redundante de alta disponibilidad (HA)**.	Seleccionar el sistema para instalar, en la página 31
7	Seleccione un despliegue automático. (Para simplificar el proceso, Cisco recomienda hacer las mismas selecciones que para su sistema principal).	Seleccionar el tipo de despliegue de sistema, en la página 32
8	Introduzca sus credenciales de vCenter para que podamos desplegar las máquinas virtuales del sistema HA por usted.	Proporcionar las credenciales de VMware vCenter, en la página 32
9	Según proceda, seleccione el host ESXi, el almacén de datos y el grupo de puerto de máquina virtual para su máquina virtual multimedia del sistema HA. **Nota** Seleccione el mismo grupo de puertos de la máquina virtual que para el sistema principal.	Seleccionar la configuración de vCenter para su máquina virtual multimedia, en la página 33

Tarea	Descripción	Para obtener información detallada, consulte
10	Según proceda, introduzca el nombre de dominio cualificado completo de la máquina virtual multimedia del sistema HA. (Si ya ha actualizado el servidor DNS con entradas para el sistema HA, buscaremos la dirección IP por usted).	Introducir la información de comunicaciones de red para la máquina virtual multimedia, en la página 33
11	Si ha agregado el acceso público para su sistema principal, compruebe que ha marcado la casilla de verificación **Crear una máquina virtual de proxy inverso de Internet**. De lo contrario, elimine la selección de esta casilla de verificación. **Nota** Si no ha activado el acceso público, pase a la Tarea 14.	Agregar acceso público, en la página 34
12	Si ha agregado el acceso público, seleccione el host ESXi, el almacén de datos y el grupo de puerto de la máquina virtual para la máquina virtual de proxy inverso de Internet del sistema HA. **Nota** Seleccione el mismo grupo de puertos de la máquina virtual que para el sistema principal.	Seleccionar los ajustes de vCenter para su máquina virtual de proxy inverso de Internet, en la página 34
13	Introduzca la información de comunicaciones de red y el nombre de host para el proxy inverso de Internet.	Introducir la información de comunicaciones de red para el proxy inverso de Internet, en la página 35
14	Compruebe que ha hecho todos los cambios de comunicaciones de red, servidor DNS y configuración de cortafuegos necesarios para su sistema HA.	Confirmación de que la red está configurada correctamente, en la página 38
15	Una vez que las máquinas virtuales del sistema HA se hayan desplegado correctamente, seleccione **Siguiente** para continuar con la comprobación del sistema HA.	Desplegar sus máquinas virtuales, en la página 39
16	Cuando la comprobación del sistema HA se complete correctamente, seleccione **Siguiente**.	Comprobación de su sistema, en la página 39
17	Confirme que el sistema principal y el sistema HA tienen la misma versión. De lo contrario, actualice el sistema HA.	Comprobar que la versión de su sistema principal y el sistema de alta disponibilidad son la misma, en la página 79
18	Agregue este sistema de alta disponibilidad al sistema principal en Administración de Cisco WebEx.	Agregar un sistema de alta disponibilidad, en la página 81

Agregar un sistema HA usando el despliegue manual

Instrucciones antes de empezar

- Debe haber desplegado correctamente un sistema principal.

- El sistema principal está en modo de mantenimiento.
- Cree una copia de seguridad de los sistemas principal y de alta disponibilidad. Consulte .Creación de una copia de seguridad por medio de VMware vCenter, en la página 4

Consideraciones previas a la adición de un sistema de alta disponibilidad

Un sistema de alta disponibilidad es un sistema redundante que se agrega y pasa a formar parte de su sistema. Proporciona alta disponibilidad en caso de producirse un fallo de una máquina virtual.

El sistema de alta disponibilidad (HA) tiene los requisitos siguientes:

- El sistema HA debe tener la misma versión que el sistema principal.

  Si ha actualizado el sistema principal, no olvide hacer lo mismo para el sistema HA.
- Si tiene autorización para ello (con el contrato de servicio pertinente), Cisco le recomienda desplegar el sistema de alta disponibilidad utilizando el archivo OVA que sea de la misma versión (antes de aplicar parches) que el sistema principal.
- El tamaño del sistema HA debe ser el mismo que el tamaño del sistema principal.
- Si ha agregado el acceso público en el sistema principal, tiene que agregarlo también al sistema HA.
- Las máquinas virtuales internas del sistema HA deben encontrarse en la misma subred que las máquinas virtuales internas del sistema principal.
- Si ha agregado el acceso público, la máquina virtual de proxy inverso de Internet del sistema HA debe encontrarse en la misma subred que la máquina virtual de proxy inverso de Internet del sistema principal.
- Dado que este proceso agrega máquinas virtuales a su sistema, su certificado de seguridad actual será invalidado y tendrá que actualizarlo, a no ser que esté utilizando un certificado autofirmado.
- Si tenía anteriormente un sistema de alta disponibilidad, retírelo. Si está desplegando un nuevo sistema de alta disponibilidad, no podrá volver a utilizar las máquinas virtuales en el sistema HA anterior. Debe volver a desplegar un nuevo sistema de alta disponibilidad con nuevas máquinas virtuales.

Resumen de tareas para agregar un sistema de alta disponibilidad usando el despliegue manual

Siga estas tareas en orden.

Tarea	Descripción	Para obtener información detallada, consulte
1	Utilizando el cliente VMware vSphere, despliegue la máquina virtual de administración para el sistema HA.	Desplegar el archivo OVA desde un cliente VMware vSphere, en la página 18
2	Encienda la máquina virtual de administración para el sistema HA y escriba la URL de despliegue.	
3	Introduzca la URL en un explorador Web y continúe con el despliegue del sistema HA.	
4	Seleccione su idioma preferido para el despliegue del sistema HA.	Seleccionar su idioma para la configuración, en la página 30

Tarea	Descripción	Para obtener información detallada, consulte
5	Confirme el tamaño del sistema para el sistema HA. (Este tamaño de sistema debe coincidir con el tamaño del sistema principal).	Confirmar el tamaño de su sistema, en la página 31
6	Seleccione **Crear un sistema redundante de alta disponibilidad (HA)**.	Seleccionar el sistema para instalar, en la página 31
7	Seleccione un despliegue manual. (Para simplificar el proceso, Cisco recomienda hacer las mismas selecciones que para su sistema principal).	Seleccionar el tipo de despliegue de sistema, en la página 32
8	Si ha agregado el acceso público para su sistema principal, compruebe que ha marcado la casilla de verificación **Crear una máquina virtual de proxy inverso de Internet**. De lo contrario, elimine la selección de esta casilla de verificación.	Agregar acceso público, en la página 34
9	Compruebe que ha hecho todos los cambios de comunicaciones de red, servidor DNS y configuración de cortafuegos necesarios para su sistema HA.	Confirmación de que la red está configurada correctamente, en la página 38
10	Una vez que las máquinas virtuales del sistema HA se hayan desplegado correctamente, seleccione **Siguiente** para continuar con la comprobación del sistema HA.	Desplegar sus máquinas virtuales, en la página 63
11	Cuando la comprobación del sistema HA se complete correctamente, seleccione **Siguiente**.	Comprobación de su sistema, en la página 39
12	Confirme que el sistema principal y el sistema HA tienen la misma versión. De lo contrario, actualice el sistema HA.	Comprobar que la versión de su sistema principal y el sistema de alta disponibilidad son la misma, en la página 79
13	Agregue este sistema de alta disponibilidad al sistema principal en Administración de Cisco WebEx.	Agregar un sistema de alta disponibilidad, en la página 81

Comprobar que la versión de su sistema principal y el sistema de alta disponibilidad son la misma

El sistema de alta disponibilidad (HA) debe tener exactamente la misma versión que la del sistema principal. La versión del sistema HA figura en la página del explorador. Para comprobar la versión del sistema principal, realice los siguientes pasos en el sistema principal:

Procedimiento

Paso 1 En una ventana individual del explorador, inicie sesión en el sitio de administración de WebEx en el sistema principal.

Paso 2 En la pestaña del **Escritorio**, marque el número de versión del sistema principal en el panel **Sistema**.

Paso 3 Si el sistema principal tiene una versión posterior a la del sistema HA, debe volver a desplegar el sistema HA utilizando un archivo OVA más reciente (para obtener una versión posterior del software) o actualizar el sistema HA.

Nota Para actualizar el sistema HA, primero debe realizar una copia de seguridad de las máquinas virtuales. Para obtener detalles, consulte Creación de una copia de seguridad por medio de VMware vCenter.

Paso 4 Cuando sea necesario actualizar HA, después de desplegar el sistema HA, seleccione **actualizar** en el explorador conectado al sistema HA.

Paso 5 Descargue el correspondiente archivo de actualización de Cisco:
Descargar software

Coloque el archivo de actualización en un disco local o en un almacén de datos disponible en el sistema de alta disponibilidad.

Paso 6 Seleccione **Continuar** en el explorador conectado al sistema HA.

Paso 7 Conecte la unidad de CD/DVD al archivo de actualización ISO en la máquina virtual de administración del sistema de alta disponibilidad.
Consulte Conexión a una imagen ISO desde la unidad CD/DVD.

Paso 8 Marque **Me he conectado al archivo ISO y estoy preparado para continuar** y seleccione **Continuar**.

Precaución Después de seleccionar **Continuar**, no podrá detener el proceso de actualización. Si se produce algún error durante el procedimiento de actualización y no se completa correctamente, debe usar los archivos de copia de seguridad para restaurar el sistema.

El procedimiento de actualización puede tardar hasta una hora. No cierre la ventana del explorador, ya que no podrá volver a esta página.

Después de completar la actualización, aparece un nuevo diálogo que confirma que la actualización se ha realizado correctamente.

Paso 9 Seleccione **Reiniciar**.
Una vez que el sistema se ha reiniciado, aparece la página de sistema HA creado con un mensaje que indica que la actualización se ha realizado correctamente.

Qué hacer a continuación

Agregue este sistema de alta disponibilidad al sistema principal en Administración de Cisco WebEx en el sistema principal.

Agregar un sistema de alta disponibilidad

Nota La mayoría de las funciones de su sistema de alta disponibilidad están prohibidas. Por ejemplo, no tiene acceso a la actualización, configuración de SNMP, acceso de almacenamiento y servidores de correo electrónico en el sistema de alta disponibilidad. Puede ver las propiedades del sistema, pero está prohibida su modificación.

Nota Complete el siguiente procedimiento en el sistema principal.

Antes de comenzar

- Instale Cisco WebEx en una segunda máquina virtual a partir del archivo OVA para ser usada como su sistema de alta disponibilidad.

  Nota Su sistema de alta disponibilidad debe tener el mismo tamaño que su sistema principal.

- Su sistema de alta disponibilidad debe configurarse con la misma ruta y OVA que su sistema principal. Si las versiones de su sistema principal y del sistema HA no coinciden, se le pedirá que actualice al nivel de versión más alto.
- Copie el nombre de dominio cualificado completo (FQDN) de su máquina virtual de alta disponibilidad. Debe conocer el FQDN para agregar su sistema de alta disponibilidad.
- Compruebe que todas las máquinas virtuales funcionan correctamente. Determine el estado de la máquina virtual visualizando el monitor del sistema como se describe en Acerca de su escritorio, en la página 115.
- Le recomendamos que tome una instantánea de las máquinas virtuales de alta disponibilidad antes de realizar este procedimiento. Repita el procedimiento desde la instantánea en caso de error.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento**.

Paso 3 En el sistema principal, en la sección Sistema, seleccione el enlace **Ver más**.

Paso 4 Seleccione **Agregar sistema de alta disponibilidad**.

Paso 5 Siga las instrucciones en la página **Propiedades del sistema** para agregar este sistema de alta disponibilidad.

Paso 6 Introduzca el FQDN de la máquina virtual del sitio de administración del sistema de alta disponibilidad y seleccione **Continuar**.
Validaremos el estado de preparación del sistema principal y del sistema HA para este procedimiento de añadir HA.

- Si ambos sistemas están listos, entonces verá un botón verde de **Agregar**. No lo seleccione hasta que ponga el sistema en modo de mantenimiento.

- Si alguno de los sistemas no está preparado verá un mensaje de error. Solucione el error e intente de nuevo el procedimiento de adición de alta disponibilidad.

Paso 7 Seleccione **Agregar**.

Nota Si el error "Código de error: Database-64" aparece, repita este procedimiento usando la instantánea de las máquinas virtuales de alta disponibilidad.

Su sistema de alta disponibilidad se añade y se configura automáticamente para servir como sistema de reserva en caso de producirse un fallo en el sistema principal.

Paso 8 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.

El sistema rearranca después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Prueba del sistema

Algunas de las pruebas recomendadas para ejecutar en el sistema se muestran en esta sección. Puede realizar estas pruebas y validar su sistema utilizando dos herramientas de diagnóstico descritas en las páginas de soporte para este producto: La prueba de reuniones y la prueba de recursos del sistema.

Cuando se prueba un sistema actualizado, puede conservar el sistema original hasta que haya terminado de probar el sistema actualizado (pero no puede encender los dos sistemas al mismo tiempo). Una vez que esté conforme con los resultados de la pruebas del sistema actualizado, puede eliminar (de forma definitiva) el sistema existente. Asegúrese de que su sistema actualizado está funcionando al suprimir o eliminar el sistema existente. De esta forma, se evita la eliminación accidental del archivo de disco de máquina virtual (VMDK) base, al cual puede acceder el sistema actualizado.

- Agregar, editar, activar y desactivar usuarios.
- Planificar y organizar una reunión.
- Volver a planificar una reunión existente.
- Eliminar una serie de reuniones o una reunión futura.
- Abrir un adjunto de la reunión.
- Reproducir una grabación de la reunión.

CAPÍTULO 8

Ampliar su sistema a un tamaño de sistema superior

- Preparación para la ampliación del sistema, página 83
- Preparación para un procedimiento de modificación del sistema, página 84
- Ampliación del sistema usando el despliegue automático, página 85
- Ampliación del sistema usando el despliegue manual, página 89
- Prueba del sistema, página 93

Preparación para la ampliación del sistema

Esta sección describe los requisitos previos de una ampliación del sistema.

La ampliación de un sistema requiere el realojamiento de las licencias existentes en el sistema ampliado. (Consulte Realojamiento de licencias después de una actualización de software o la expansión del sistema.)

Determinar el tamaño del nuevo sistema

Tenga en cuenta lo siguiente:

- Un presupuesto para el posible hardware adicional
- El número previsto de reuniones simultáneas y su tamaño medio en los próximos meses

Obtención de la información necesaria para la ampliación de su sistema

- Obtenga el archivo OVA utilizado para instalar la versión del sistema existente.
- Complete la lista de comprobación de la ampliación.

Nombre del campo	Valor actual para su sistema
URL del sitio de WebEx	
URL del sitio de administración	

Nombre del campo	Valor actual para su sistema
Dirección VIP privada	
Dirección VIP pública	

Preparación para un procedimiento de modificación del sistema

En esta sección se describe cómo prepararse para un procedimiento de modificación del sistema: ampliar su sistema, agregar un sistema de alta disponibilidad, activar el acceso público, actualizar su sistema, etc. creando una copia de seguridad de su sistema.

Aunque puede seleccionar hacerlo, las copias de seguridad no son necesarias para una expansión o actualización de su sistema. Durante una expansión o actualización, usted despliega un nuevo sistema y transfiere los datos de su sistema existente al nuevo sistema. Si hay un problema con la expansión o actualización, puede apagar el nuevo sistema y seguir usando el sistema existente.

Precaución Los usuarios no pueden acceder al sistema para reuniones, ya que este procedimiento requiere un acceso exclusivo al sistema. No olvide programar este procedimiento durante un periodo de tiempo que no interrumpa demasiado las actividades de sus usuarios.

Los otros administradores del sistema no deben acceder al sistema durante este procedimiento. Si lo hacen, sus cambios no se guardarán y el resultado puede ser impredecible. Deberán esperar hasta que este procedimiento se complete y después iniciar sesión en Administración de Cisco WebEx para completar sus tareas.

Nota Asegúrese de ponerse de acuerdo con otros administradores del sistema antes de iniciar un procedimiento de modificación del sistema.

Atención Si no necesita crear una copia de seguridad de los equipos virtuales, entonces no necesita completar este procedimiento. Sin embargo, como una buena práctica, Cisco recomienda crear una copia de seguridad. Las copias de seguridad permiten revertir el sistema, si el procedimiento genera un error.

Procedimiento

Paso 1 Inicie sesión en el sitio de Administración de Cisco WebEx.

Paso 2 Seleccione **Activar el modo de mantenimiento**.

Paso 3 Utilice VMware Data Recovery (denominado VMware vSphere Data Protection empezando por vSphere versión 5.1) para crear una copia de seguridad de cada una de sus máquinas virtuales.
La copia de seguridad le ayudará a revertir su máquina virtual al estado anterior al procedimiento de modificación del sistema. Para obtener información adicional, consulte Creación de una copia de seguridad por medio de VMware vCenter, en la página 4. Para obtener información detallada sobre esta copia de seguridad, consulte la *Guía de administración de VMware Data Recovery* o la *Guía de administración de vSphere Data Protection*.

Nota Si tiene previsto hacer una expansión o actualización, elimine todas las instantáneas VMware en el sistema existente. De esta forma, se evita la eliminación accidental del archivo VMDK de base 4 del disco duro, al cual puede acceder el sistema ampliado o actualizado.

Paso 4 Vuelva a iniciar sesión en el sitio de Administración de Cisco WebEx pero no apague el modo de mantenimiento.

Paso 5 Continúe con el procedimiento de modificación del sistema.

Ampliación del sistema usando el despliegue automático

Instrucciones antes de empezar

Nota Al sistema antes de la ampliación se le conoce como sistema *original*. El sistema posterior a la ampliación es el sistema *ampliado*.

Programe una hora que no interrumpa demasiado a sus usuarios para hacer la ampliación del sistema.

Coloque el sistema principal en modo de mantenimiento antes de iniciar la expansión del sistema.

Precaución Los usuarios no pueden acceder al sistema para reuniones, ya que este procedimiento requiere un acceso exclusivo al sistema. No olvide programar este procedimiento durante un periodo de tiempo que no interrumpa demasiado las actividades de sus usuarios.

Póngase de acuerdo con otros administradores del sistema antes de iniciar un procedimiento de modificación del sistema. Los otros administradores del sistema no deben acceder al sistema durante este procedimiento. Si lo hacen, sus cambios no se guardarán y el resultado puede ser impredecible.

Consideraciones previas a la ampliación del sistema

- No olvide eliminar todas las instantáneas de VMware del sistema original antes de iniciar el procedimiento de ampliación.
- Puede volver a usar los mismos nombres de host y direcciones IP de las máquinas virtuales originales en el sistema ampliado. Sin embargo, solamente puede estar encendido el sistema original o el sistema ampliado; los dos sistemas no pueden estar encendidos y ejecutarse al mismo tiempo.
- Si tenía HA en el sistema original, tras el despliegue del sistema ampliado debe agregar HA en el sistema ampliado. No puede reutilizar el sistema HA, ya que no se mantiene tras una ampliación.
- Puede conservar el sistema original hasta que haya finalizado la prueba del sistema ampliado. Una vez haya realizado la prueba y esté satisfecho con el sistema ampliado, puede eliminar el sistema original (anterior a la ampliación).
- Las máquinas virtuales internas del sistema original y del sistema ampliado deben estar en la misma subred.
- Si ha agregado acceso público, las máquinas virtuales de proxy inverso de Internet del sistema original y del sistema ampliado deben estar en la misma subred.

- Al agregar una nueva máquina virtual al sistema, su certificado de seguridad actual y las claves públicas y privadas serán invalidadas y necesitarán una actualización, a no ser que esté utilizando un certificado autofirmado.

  Los certificados incluyen nombres de host y URL. El certificado y las claves serán invalidados porque no incluyen la nueva máquina virtual. Para obtener información detallada sobre los certificados y las claves, consulte Administración de certificados.

- Compruebe que el sistema ampliado puede acceder a los discos de la máquina virtual de administración del sistema original. Copiará el disco duro 4 en el sistema ampliado.
- Compruebe que el sistema ampliado está en funcionamiento cuando elimine o suprima el sistema original. De esta forma, se evita la eliminación accidental del archivo VMDK base del disco duro 4, al cual podría acceder el sistema ampliado.

Ampliación del sistema

Las tareas generales para ampliar el sistema son:

1. Cree una copia de seguridad del sistema original.
2. Utilice el mismo archivo OVA que ha utilizado para desplegar el sistema original y despliegue la máquina virtual de administración para el nuevo tamaño de sistema.
3. Copie los datos del sistema original a la máquina virtual de administración para el sistema ampliado.
4. Despliegue las máquinas virtuales adicionales, si procede, para el nuevo tamaño de sistema.
5. Pruebe el sistema ampliado.
6. Realoje las licencias.

Resumen de tareas para ampliar el sistema utilizando un despliegue automático

Nota Esta tabla incluye enlaces a otras secciones de la *Guía de administración de Cisco WebEx Meetings Server*. Cada una de las secciones proporciona información detallada sobre una tarea específica. Después de completar cada tarea, vuelva a esta tabla y complete la nueva tarea. (Utilice las funciones Vista anterior y Vista siguiente en Adobe Acrobat para moverse fácilmente entre esta tabla y los procedimientos de tarea individuales).

Tarea	Descripción	Para obtener información detallada, consulte
1	Prepare el sistema original para su ampliación.	Ya ha completado esta tarea anteriormente en este capítulo. Se ha incluido en esta tabla para reflejar la totalidad del proceso.
2	Preparación para un procedimiento de alteración del sistema.	Ya ha completado esta tarea anteriormente en este capítulo. Se ha incluido en esta tabla para reflejar la totalidad del proceso.

Tarea	Descripción	Para obtener información detallada, consulte
3	Inicie el procedimiento de ampliación en el sitio de Administración del sistema original.	Expandir el tamaño del sistema
4	Mediante el cliente VMware vSphere, seleccione **Power** > **Shut Down Guest**en las máquinas virtuales del sistema original.	
5	Utilizando el cliente vSphere, despliegue la máquina virtual de administración para el nuevo tamaño de sistema.	Desplegar el archivo OVA desde un cliente VMware vSphere, en la página 18
6	Conecte el **Disco duro 4** de la máquina virtual de administración del sistema original a la máquina virtual de administración del sistema ampliado.	Adjuntar un archivo VMDK existente a una nueva máquina virtual, en la página 6
7	Encienda la máquina virtual de administración para el sistema ampliado y escriba la URL de despliegue.	
9	Introduzca la URL de despliegue en un explorador Web y continúe con el despliegue de su sistema ampliado.	
10	Seleccione su idioma preferido para el despliegue del sistema ampliado.	Seleccionar su idioma para la configuración, en la página 30
11	Confirme el tamaño del sistema. (El tamaño de este sistema debe ser mayor o igual al del sistema original.)	Confirmar el tamaño de su sistema, en la página 31
13	Seleccione **Instalar un sistema principal**.	Seleccionar el sistema para instalar, en la página 31
14	Seleccione un despliegue automático.	Seleccionar el tipo de despliegue de sistema, en la página 32
15	Introduzca sus credenciales de vCenter para que podamos desplegar las máquinas virtuales por usted.	Proporcionar las credenciales de VMware vCenter, en la página 32
16	Seleccione el host ESXi, el almacén de datos y el grupo de puerto de máquina virtual para la máquina virtual multimedia.	Seleccionar la configuración de vCenter para su máquina virtual multimedia, en la página 33
17	Introduzca el nombre de dominio cualificado completo de la máquina virtual multimedia. (Si ya ha actualizado el servidor DNS con entradas para el sistema ampliado, buscaremos la dirección IP por usted).	Introducir la información de comunicaciones de red para la máquina virtual multimedia, en la página 33
18	Si desea un acceso público para su sistema ampliado, compruebe que la casilla de verificación **Crear una máquina virtual de proxy inverso de Internet** está seleccionada. De lo contrario, elimine la selección de esta casilla de verificación. **Nota** Si no ha activado el acceso público, pase a la Tarea 19.	Agregar acceso público, en la página 34

Tarea	Descripción	Para obtener información detallada, consulte
19	Si ha agregado el acceso público, seleccione el host ESXi, el almacén de datos y el grupo de puertos de la máquina virtual para la máquina virtual de proxy inverso de Internet.	Seleccionar los ajustes de vCenter para su máquina virtual de proxy inverso de Internet, en la página 34
20	Introduzca la información de comunicaciones de red y el nombre de host para el proxy inverso de Internet.	Introducir la información de comunicaciones de red para el proxy inverso de Internet, en la página 35
21	Introduzca la dirección VIP pública para la URL del sitio de WebEx. **Nota** Puede especificar la misma dirección VIP pública que utiliza en el sistema original o cambiarla por una nueva dirección IP. Si la cambia, realice las actualizaciones necesarias en el servidor DNS.	Introducir la dirección VIP pública, en la página 36
22	Introduzca la dirección VIP privada para la URL de administración de WebEx. **Nota** Puede especificar la misma dirección VIP privada que utiliza en el sistema original o cambiarla por una nueva dirección IP. Si la cambia, realice las actualizaciones necesarias en el servidor DNS.	Introducir la dirección VIP privada, en la página 36
23	Introduzca la URL del sitio de WebEx. Los participantes acceden a esta URL para organizar y asistir a reuniones. (Esta URL se resuelve en la dirección VIP privada o en la dirección VIP pública, dependiendo de si está utilizando o no un DNS de horizonte dividido). **Nota** Puede especificar el mismo URL de sitio WebEx que utiliza en el sistema original o cambiarla por uno nuevo. Si la cambia, realice las actualizaciones necesarias en el servidor DNS. Asegúrese de conservar la URL del sitio original en el servidor DNS. Redirija su URL del sitio original al URL del sitio nuevo. Si los usuarios intentan utilizar la URL original y no la ha redirigido a la nueva URL, no podrán organizar ni unirse a reuniones.	Introducción de las URL del sitio de WebEx y de administración de WebEx, en la página 38
24	Introduzca la URL de administración de WebEx para que los administradores accedan a Administración de Cisco WebEx y los participantes internos puedan organizar o asistir a reuniones (solo con DNS de horizonte dividido). (Esta URL se resuelve en la dirección VIP privada). **Nota** Puede especificar el mismo URL de administrador WebEx que utiliza en el sistema original o cambiarla por uno nuevo. Si la cambia, realice las actualizaciones necesarias en el servidor DNS.	Introducción de las URL del sitio de WebEx y de administración de WebEx, en la página 38

Tarea	Descripción	Para obtener información detallada, consulte
25	Compruebe que ha hecho todos los cambios de comunicaciones de red, servidor DNS y configuración de cortafuegos necesarios para su sistema.	Confirmación de que la red está configurada correctamente, en la página 38
26	Una vez que sus máquinas virtuales se hayan desplegado correctamente, seleccione **Siguiente** para continuar con la comprobación del sistema.	Desplegar sus máquinas virtuales
27	Junto con la comprobación del sistema, actualizamos el sistema ampliado con las actualizaciones necesarias para coincidir con la versión de software del sistema original, antes de la ampliación. (Estas actualizaciones pueden durar hasta una hora). Cuando se completen, el sistema se reiniciará.	Comprobación de su sistema
28	Inicie sesión en Administración de Cisco WebEx.	
29	Pruebe el sistema ampliado. Si la ampliación no es satisfactoria, apague el sistema ampliado y encienda el sistema original. Póngase en contacto con el TAC de Cisco para obtener asistencia.	Prueba del sistema
30	Realoje las licencias según proceda para el sistema ampliado.	Acerca de las licencias - Realojamiento de licencias después de una actualización de software o la expansión del sistema

Ampliación del sistema usando el despliegue manual

Instrucciones antes de empezar

Nota Al sistema antes de la ampliación se le conoce como sistema *original*. El sistema posterior a la ampliación es el sistema *ampliado*.

Programe una hora que no interrumpa demasiado a sus usuarios para hacer la ampliación del sistema.

Coloque el sistema principal en modo de mantenimiento antes de iniciar la expansión del sistema.

Precaución Los usuarios no pueden acceder al sistema para reuniones, ya que este procedimiento requiere un acceso exclusivo al sistema. No olvide programar este procedimiento durante un periodo de tiempo que no interrumpa demasiado las actividades de sus usuarios.

Póngase de acuerdo con otros administradores del sistema antes de iniciar un procedimiento de modificación del sistema. Los otros administradores del sistema no deben acceder al sistema durante este procedimiento. Si lo hacen, sus cambios no se guardarán y el resultado puede ser impredecible.

Consideraciones previas a la ampliación del sistema

- No olvide eliminar todas las instantáneas de VMware del sistema original antes de iniciar el procedimiento de ampliación.
- Puede volver a usar los mismos nombres de host y direcciones IP de las máquinas virtuales originales en el sistema ampliado. Sin embargo, solamente puede estar encendido el sistema original o el sistema ampliado al mismo tiempo. Ambos sistemas no pueden encenderse y ejecutarse al mismo tiempo.
- Si ya ha agregado un sistema HA a su sistema original, después del despliegue del sistema ampliado debe agregar un nuevo sistema HA. No puede volver a usar el sistema HA original, ya que no se retiene tras una ampliación.
- Puede conservar el sistema original hasta que haya finalizado la prueba del sistema ampliado. Una vez haya realizado la prueba y esté satisfecho con el sistema ampliado, puede eliminar el sistema original (anterior a la ampliación).
- Las máquinas virtuales internas del sistema original y del sistema ampliado deben estar en la misma subred.
- Si ha agregado acceso público, las máquinas virtuales de proxy inverso de Internet del sistema original y del sistema ampliado deben estar en la misma subred.
- Al agregar una nueva máquina virtual al sistema, su certificado de seguridad actual y las claves públicas y privadas serán invalidadas y necesitarán una actualización, a no ser que esté utilizando un certificado autofirmado.

  Los certificados incluyen nombres de host y URL. El certificado y las claves serán invalidados porque no incluyen la nueva máquina virtual. Para obtener información detallada sobre los certificados y las claves, consulte Administración de certificados, en la página 226.
- Compruebe que el sistema ampliado puede acceder a los discos de la máquina virtual de administración del sistema original. Copiará el disco duro 4 al sistema ampliado.
- Compruebe que el sistema ampliado está en funcionamiento cuando elimine o suprima el sistema original. De esta forma, se previene la eliminación accidental del archivo VMDK de la base 4 del disco duro, al cual puede acceder el sistema ampliado.

Ampliación del sistema

Las tareas generales para ampliar el sistema son:

1. Cree una copia de seguridad del sistema original.
2. Utilice el mismo archivo OVA que ha utilizado para desplegar el sistema original y despliegue la máquina virtual de administración para el nuevo tamaño de sistema.
3. Copie los datos del sistema original a la máquina virtual de administración para el sistema ampliado.
4. Utilizando el archivo OVA, despliegue máquinas virtuales adicionales para el nuevo tamaño de sistema.
5. Pruebe el sistema ampliado.
6. Realoje las licencias.

Resumen de tareas para expandir el sistema utilizando un despliegue manual

Nota Esta tabla incluye enlaces a otras secciones de la *Guía de administración de Cisco WebEx Meetings Server*. Cada una de las secciones proporciona información detallada sobre una tarea específica. Después de completar cada tarea, vuelva a esta tabla y complete la nueva tarea. (Utilice las funciones Vista anterior y Vista siguiente en Adobe Acrobat para moverse fácilmente entre esta tabla y los procedimientos de tarea individuales).

Tarea	Descripción	Para obtener información detallada, consulte
1	Prepare el sistema original para su ampliación.	Ya ha completado esta tarea anteriormente en este capítulo. Se ha incluido en esta tabla para reflejar la totalidad del proceso.
2	Preparación para un procedimiento de alteración del sistema.	Ya ha completado esta tarea anteriormente en este capítulo. Se ha incluido en esta tabla para reflejar la totalidad del proceso.
3	Inicie el procedimiento de ampliación en el sitio de Administración del sistema original.	Expandir el tamaño del sistema
4	Mediante el cliente VMware vSphere, seleccione **Power** > **Shut Down Guest**en las máquinas virtuales del sistema original.	
5	Utilizando el cliente vSphere, despliegue la máquina virtual de administración para el nuevo tamaño de sistema. **Nota** En este momento, también puede crear las otras máquinas virtuales para su sistema.	Desplegar el archivo OVA desde un cliente VMware vSphere, en la página 18
6	Conecte el **Disco duro 4** de la máquina virtual de administración del sistema original a la máquina virtual de administración del sistema ampliado.	Adjuntar un archivo VMDK existente a una nueva máquina virtual, en la página 6
7	Encienda la máquina virtual de administración para el sistema ampliado y escriba la URL de despliegue. **Nota** En este momento, también puede activar las máquinas virtuales en su sistema. Asegúrese de que todas las máquinas virtuales se enciendan correctamente.	
9	Introduzca la URL de despliegue en un explorador Web y continúe con el despliegue de su sistema ampliado.	
10	Seleccione su idioma preferido para el despliegue del sistema ampliado.	Seleccionar su idioma para la configuración, en la página 30

Tarea	Descripción	Para obtener información detallada, consulte
11	Confirme el tamaño del sistema. (El tamaño de este sistema debe ser mayor o igual al del sistema original.)	Confirmar el tamaño de su sistema, en la página 31
12	Seleccione **Instalar un sistema principal**.	Seleccionar el sistema para instalar, en la página 31
13	Seleccione un despliegue manual.	Seleccionar el tipo de despliegue de sistema, en la página 32
14	Si desea un acceso público para su sistema ampliado, compruebe que la casilla de verificación **Crear una máquina virtual de proxy inverso de Internet** está seleccionada. De lo contrario, elimine la selección de esta casilla de verificación.	Agregar acceso público, en la página 34
15	Introduzca la dirección VIP pública para la URL del sitio de WebEx. **Nota** Puede especificar la misma dirección VIP pública que utiliza en el sistema original o cambiarla por una nueva dirección IP. Si la cambia, realice las actualizaciones necesarias en el servidor DNS.	Introducir la dirección VIP pública, en la página 36
16	Introduzca la dirección VIP privada para la URL de administración de WebEx. **Nota** Puede especificar la misma dirección VIP privada que utiliza en el sistema original o cambiarla por una nueva dirección IP. Si la cambia, realice las actualizaciones necesarias en el servidor DNS.	Introducir la dirección VIP privada, en la página 36
17	Introduzca la URL del sitio de WebEx. Los participantes acceden a esta URL para organizar y asistir a reuniones. (Esta URL se resuelve en la dirección VIP privada o en la dirección VIP pública, dependiendo de si está utilizando o no un DNS de horizonte dividido). **Nota** Puede especificar el mismo URL de sitio WebEx que utiliza en el sistema original o cambiarla por uno nuevo. Si la cambia, realice las actualizaciones necesarias en el servidor DNS. Asegúrese de conservar la URL del sitio original en el servidor DNS. Redirija su URL del sitio original al URL del sitio nuevo. Si los usuarios intentan utilizar la URL original y no la ha redirigido a la nueva URL, no podrán organizar ni unirse a reuniones.	Introducción de las URL del sitio de WebEx y de administración de WebEx, en la página 38

Tarea	Descripción	Para obtener información detallada, consulte
18	Introduzca la URL de administración de WebEx para que los administradores accedan a Administración de Cisco WebEx y los participantes internos puedan organizar o asistir a reuniones (solo con DNS de horizonte dividido). (Esta URL se resuelve en la dirección VIP privada). **Nota** Puede especificar el mismo URL de administrador WebEx que utiliza en el sistema original o cambiarla por uno nuevo. Si la cambia, realice las actualizaciones necesarias en el servidor DNS.	Introducción de las URL del sitio de WebEx y de administración de WebEx, en la página 38
19	Compruebe que ha hecho todos los cambios de comunicaciones de red, servidor DNS y configuración de cortafuegos necesarios para su sistema.	Confirmación de que la red está configurada correctamente, en la página 38
20	Una vez que sus máquinas virtuales se hayan desplegado correctamente, seleccione **Siguiente** para continuar con la comprobación del sistema.	Desplegar sus máquinas virtuales
21	Junto con la comprobación del sistema, actualizamos el sistema ampliado con las actualizaciones necesarias para coincidir con la versión de software del sistema original, antes de la ampliación. (Estas actualizaciones pueden durar hasta una hora). Cuando se completen, el sistema se reiniciará.	Comprobación de su sistema
22	Inicie sesión en Administración de Cisco WebEx.	
23	Pruebe el sistema ampliado. Si la ampliación no es satisfactoria, apague el sistema ampliado y encienda el sistema original. Póngase en contacto con el TAC de Cisco para obtener asistencia.	Prueba del sistema
24	Realoje las licencias según proceda para el sistema ampliado.	Acerca de las licencias - Realojamiento de licencias después de una actualización de software o la expansión del sistema

Prueba del sistema

Algunas de las pruebas recomendadas para ejecutar en el sistema se muestran en esta sección. Puede realizar estas pruebas y validar su sistema utilizando dos herramientas de diagnóstico descritas en las páginas de soporte para este producto: La prueba de reuniones y la prueba de recursos del sistema.

Cuando se prueba un sistema actualizado, puede conservar el sistema original hasta que haya terminado de probar el sistema actualizado (pero no puede encender los dos sistemas al mismo tiempo). Una vez que esté conforme con los resultados de la pruebas del sistema actualizado, puede eliminar (de forma definitiva) el sistema existente. Asegúrese de que su sistema actualizado está funcionando al suprimir o eliminar el sistema

existente. De esta forma, se evita la eliminación accidental del archivo de disco de máquina virtual (VMDK) base, al cual puede acceder el sistema actualizado.

- Agregar, editar, activar y desactivar usuarios.
- Planificar y organizar una reunión.
- Volver a planificar una reunión existente.
- Eliminar una serie de reuniones o una reunión futura.
- Abrir un adjunto de la reunión.
- Reproducir una grabación de la reunión.

CAPÍTULO 9

Actualización del sistema

- Actualización del sistema, página 95
- Conexión a una imagen ISO desde la unidad CD/DVD, página 96
- Continuar con el proceso de actualización, página 97
- Completar la actualización, página 98

Actualización del sistema

Los usuarios no pueden acceder al sistema para reuniones, ya que el procedimiento de actualización requiere un acceso exclusivo al sistema. Procure programar la actualización en un tiempo que no interrumpa demasiado a sus usuarios.

Los otros administradores del sistema no deben acceder al sistema durante este procedimiento. Si lo hacen, sus cambios no se guardarán y el resultado puede ser imprevisible; deben esperar hasta que este procedimiento se haya completado antes de iniciar sesión en el sitio de administración de Cisco WebEx.

El procedimiento de actualización completo, incluyendo la copia de seguridad de las máquinas virtuales, puede tardar hasta una hora dependiendo del tamaño del sistema y el tamaño de la base de datos.

Antes de comenzar

Obtenga el archivo de actualización más reciente de Cisco:

Cisco Software Download (externo)

El paquete de actualización de su sistema incluye una imagen ISO. No puede *saltarse* algunas versiones del software. Por ejemplo, debe instalar Cisco WebEx Meetings Server versión 1.1 (Build 1.1.1.9.A) o versión 1.5 (Build 1.5.1.6.A) antes de aplicar 1.5 MR2.

Procedimiento

Paso 1 Inicie sesión en el sitio de Administración de Cisco WebEx.

Paso 2 Seleccione **Activar el modo de mantenimiento**.

Paso 3 Seleccione la pestaña **Sistema** y, a continuación, seleccione **Actualizar**.

Paso 4 Seleccione **Actualizar**.

Paso 5 En el cliente VMware vSphere, seleccione **Power** > **Shut Down Guest** en cada una de las máquinas virtuales de su sistema.
Para obtener información detallada sobre la utilización de vSphere, consulte la documentación de VMware ESXi y vCenter Server.

Paso 6 Una vez se enciendan las máquinas virtuales, utilice VMware Data Recovery (o VMware vSphere Data Protection disponible con vSphere Versión 5.1) para crear una copia de seguridad de cada una de las máquinas virtuales.
La copia de seguridad devolverá la máquina virtual a su estado anterior a la actualización si fuera necesario. Para obtener información adicional, consulte Creación de una copia de seguridad por medio de VMware vCenter, en la página 4. Para obtener información detallada sobre esta copia de seguridad, consulte la *Guía de administración de VMware Data Recovery* o la *Guía de administración de vSphere Data Protection*.

Nota También puede tomar una instantánea, pero debe suprimir todas las instantáneas en aproximadamente 24 horas, o de lo contrario podría sufrir problemas de rendimiento de los datos. Para obtener más información, consulte Tomar una Instantánea utilizando VMware vCenter.

Precaución Cree copias de seguridad de todas las máquinas virtuales, porque el procedimiento de actualización efectúa cambios en las máquinas virtuales existentes y, una vez empiece el procedimiento de actualización no podrá deshacerla.

Paso 7 En el cliente VMware vSphere, encienda todas las máquinas virtuales de su sistema.

Paso 8 Inicie sesión en el sitio de administración de Cisco WebEx pero no desactive el modo de mantenimiento.

Paso 9 Seleccione la pestaña **Sistema** y, a continuación, seleccione **Actualizar**.

Paso 10 Seleccione **Actualizar** para volver a la página **Actualizar sistema**.

Qué hacer a continuación

Vaya a Conexión a una imagen ISO desde la unidad CD/DVD.

Conexión a una imagen ISO desde la unidad CD/DVD

Para una actualización más rápida, Cisco recomienda montar la imagen ISO en el almacenamiento de datos vCenter. Sin embargo, si la coloca en un disco local del cliente vSphere, asegúrese de que el cliente vSphere tiene una conexión física con la intranet de la empresa (no a través de VPN).

Para colocar la imagen ISO en el almacén de datos de vCenter y conectarse a la unidad CD/DVD, complete los pasos siguientes:

Antes de comenzar

Obtenga la imagen ISO deseada de Cisco:

Descargar software

Compruebe que tiene los permisos adecuados.

Procedimiento

Paso 1 Seleccione el host de ESXi para la máquina virtual de administración. Seleccione la pestaña **Resumen** y haga doble clic en el nombre del **datastore1** (almacén de datos 1) en **Almacenamiento**.

Paso 2 En la ventana **Datastore and Datastore clusters**, seleccione **Browse this datastore**.

Paso 3 Seleccione el icono de flecha arriba de color verde (cargar archivo) y cargue el archivo ISO de actualización.

Paso 4 Seleccione la máquina virtual de administración en el inventario VMware vCenter.

Paso 5 Seleccione el icono **CD/DVD** de la máquina virtual de administración.

Paso 6 Seleccione la **unidad CD/DVD 1** > **Conectar a la imagen ISO** en un disco local o en un datastore.

Paso 7 Confirme que la unidad de CD/DVD está conectada.

a) Haga clic con el botón derecho en el nombre de la máquina virtual de administración en el inventario vCenter y seleccione **Edit Settings...**.

b) En la pestaña **Hardware** seleccione **CD/DVD drive 1**.

c) Si no está marcada, marque la casilla de verificación **Conectado**.

d) Seleccione **Aceptar**.

Continuar con el proceso de actualización

Antes de comenzar

Ha completado:

- Actualización del sistema, en la página 95
- Conexión a una imagen ISO desde la unidad CD/DVD, en la página 96

Procedimiento

Paso 1 Después de conectar la imagen ISO de actualización, seleccione **Continuar** en la página **Actualizar sistema** en el sitio de administración de Cisco WebEx.

Paso 2 Marque la casilla de verificación **Me he conectado al archivo ISP y estoy preparado para continuar**.

Paso 3 Seleccione **Continuar**.

Precaución Después de seleccionar **Continuar**, no podrá detener el proceso de actualización. Si se produce algún error durante el procedimiento de actualización y no se completa correctamente, debe usar las copias de seguridad para restaurar el sistema.

El procedimiento de actualización puede tardar hasta una hora. No cierre la ventana del explorador, ya que no podrá volver a esta página.

Después de completar la actualización, aparece una nueva página que confirma que la actualización se ha realizado correctamente.

Nota Hay un problema intermitente en el que la actualización se completa correctamente, pero no verá ningún texto que diga **Sistema actualizado** ni un botón **Reiniciar**. Si la actualización no se completa y ha pasado más de una hora, puede intentar desactivar el modo de mantenimiento. Si no puede desactivar el modo de mantenimiento, la actualización aún está en curso. Cuando la actualización finalice, reinicie todas las máquinas virtuales desde vCenter. Espere a que las máquinas virtuales se conecten y compruebe la versión del sistema en el escritorio.

Paso 4 Seleccione **Reiniciar** para reiniciar el sistema.
Esta página tiene un valor de tiempo de espera predeterminado de 90 minutos. No olvide reiniciar el sistema dentro de este periodo de tiempo, o bien cambie el tiempo de espera predeterminado a un periodo de tiempo superior.

Qué hacer a continuación

Continúe con Completar la actualización, en la página 98.

Completar la actualización

Antes de comenzar

Esta es una confirmación desde Continuar con el proceso de actualización, en la página 97.

Procedimiento

Paso 1 Una vez que la actualización se ha completado correctamente, seleccione **Reiniciar**.
Una vez que el sistema se ha reiniciado, aparece la página de inicio de sesión del sitio de administración de Cisco WebEx.

Paso 2 Inicie sesión en Administración de Cisco WebEx. La versión actualizada aparece en el escritorio.

Paso 3 Compruebe las notas de la versión para esta actualización y determine si se requiere alguna tarea posterior a la actualización. Si se requieren tareas adicionales, complételas antes de poner el sistema en modo de mantenimiento.

Paso 4 Después de completar las configuraciones posteriores a la actualización, seleccione **Desactivar el modo de mantenimiento**.

Paso 5 Pruebe y verifique el sistema. Puede realizar estas pruebas y validar su sistema utilizando dos herramientas de diagnóstico descritas en las páginas de soporte para este producto: La prueba de reuniones y la prueba de recursos del sistema.

- Agregar, editar, activar y desactivar usuarios.
- Planificar y organizar una reunión.
- Volver a planificar una reunión existente.
- Eliminar una serie de reuniones o una reunión futura.
- Abrir un adjunto de la reunión.
- Reproducir una grabación de la reunión.

Qué hacer a continuación

- Si experimenta algún problema, utilice VMware Data Recovery (vSphere Data Protection) o las instantáneas de su sistema para volver a la versión anterior. Compruebe la conexión de red ISO y asegúrese de que no hay problemas.
- Si la actualización se ha realizado correctamente, utilice el sistema actualizado durante un rato. Cuando haya terminado, no olvide eliminar las copias de seguridad de la máquina virtual o las instantáneas antes de la actualización.

CAPÍTULO 10

Actualización del sistema

- Preparación de una actualización, página 101
- Actualización automática del sistema, página 102
- Actualización manual del sistema, página 105
- Prueba del sistema, página 107
- Realojamiento y actualización de las licencias, página 108

Preparación de una actualización

El sistema se puede actualizar volviéndolo a desplegar con un archivo OVA (plantilla de servidor virtual, Virtual Server Template por sus siglas en inglés) actualizado. Una *actualización* se define como una sustitución del sistema para desplegar las modificaciones importantes que realicemos en el sistema. Por ejemplo, la sustitución de un sistema en el que se ejecuta la versión 1.0 para ejecutar la versión 2.0, que incluye soporte para un nuevo sistema operativo. Si va a actualizarse a una versión o revisión de mantenimiento (MR), utilice siempre el procedimiento de Actualización del sistema. Consulte las notas de versión para conocer el procedimiento correcto que debe utilizarse. En ambos casos, todos los datos del sistema original se transfieren al sistema actualizado.

El sistema se puede actualizar manual o automáticamente. **Se recomienda actualizar el sistema mediante el proceso automático.**

Cuando realice la actualización:

- Puede *actualizar* a la siguiente versión completa de la aplicación. Por ejemplo, *actualizar* el sistema de la 1.5 a la 2.0. *Actualice* el sistema de la 1.1 a la 1.5; no intente *actualizar* el sistema a una versión incremental.
- Al actualizar Cisco WebEx Meeting Server, las capturas del registro guardadas en el sistema *original* no se transfieren al sistema Cisco WebEx Meeting Server *actualizado*. Por lo tanto, debería capturar y descargar todos los registros y las capturas del registro que necesite del sistema original antes de iniciar la actualización.
- Para nuevas instalaciones de Cisco WebEx Meetings Server versión 2.0, los hosts ESXi (servidor Cisco UCS) con la máquina virtual de administración necesitan 1,5 TB de espacio en disco. Los hosts ESXi (servidor Cisco UCS) sin una máquina virtual de administración necesitan 1 TB de espacio en disco. Al actualizar a Cisco WebEx Meetings Server versión 2.0 desde la versión 1.x usando sus servidores

existentes Cisco UCS, los hosts ESXi necesitarán 1118 GB de espacio en disco si el servidor UCS solo tiene la máquina virtual de administración (sistema de alta disponibilidad o principal) o 990 GB de espacio en disco si el servidor UCS tiene una máquina virtual multimedia y una de administración (sistema de alta disponibilidad o principal). El espacio en disco puede ser local (DAS) o externo (SAN/NAS). Para más información, consulte la sección "Recursos consumidos por Cisco WebEx Meetings Server y el host ESXi" en Requisitos del sistema.

Nota En este capítulo, al sistema disponible antes de iniciar la actualización se le llama sistema *original*. Al sistema disponible después de la actualización se le llama sistema *actualizado*.

Antes de comenzar una actualización automática o manual

Antes de actualizar un sistema automática o manualmente, deben abordarse las siguientes cuestiones:

- Obtenga el archivo OVA necesario para la actualización.
- Cree una copia de seguridad de cada máquina virtual en el sistema original (existente). (Consulte Creación de una copia de seguridad por medio de VMware vCenter).
- Planifique una interrupción para mantenimiento. Durante el proceso de actualización, el sistema original se coloca en modo de mantenimiento y requiere acceso exclusivo al sistema; los usuarios no pueden acceder al sistema para celebrar reuniones durante este tiempo. Planifique esta parte de la actualización para una hora a la que se interrumpa menos el trabajo de los usuarios.
- Planifique el mayor tamaño de los almacenes de datos, ya que el sistema original y el sistema actualizado comparten los almacenes de datos hasta que finalice la prueba del sistema actualizado y se elimine el sistema original.
- Los nombres de host y las direcciones IP del sistema original se reutilizan en el sistema actualizado. Además, las máquinas virtuales para ambos sistemas se encuentran en la misma subred. Si ha agregado acceso público, las máquinas virtuales de proxy inverso de Internet del sistema original y del sistema actualizado deben estar en la misma subred.

Actualización automática del sistema

Antes de comenzar una actualización automática

Antes de actualizar un sistema mediante el proceso de actualización automática, deben abordarse las siguientes cuestiones:

- Notifique a otros administradores del sistema que no deben acceder al sistema original ni hacer cambios en él durante la actualización, ya que los resultados de los cambios serían impredecibles.
- Proporcione y configure una dirección de IP adicional que se utilizará temporalmente para el sistema actualizado.
- No apague ni desconecte manualmente ninguno de los sistemas.
- Asegúrese de que el sistema actualizado puede acceder a los discos de la máquina virtual de administración del sistema original.

Utilización de la actualización automática

En esta tabla se enumeran las tareas de alto nivel necesarias para completar una actualización automática. Incluye enlaces a las secciones de la *Guía de administración de Cisco WebEx Meetings Server*, en la que se proporcionan los pasos detallados necesarios para completar cada tarea. (Para desplazarse fácilmente entre esta tabla y la tarea individual en Adobe Acrobat, seleccione Vista anterior o Vista siguiente).

Tarea	Descripción	Para obtener información detallada, consulte
1	Vaya al administrador de licencias del sistema original y genere una solicitud de licencias seleccionando **Sistema** > **Ver más** > **Administrar licencias**. El administrador de licencias se abre en una nueva pestaña. Seleccione **Generar solicitud de licencia**. Aparece una ventana emergente con el texto de la solicitud de licencia. Copie el texto y guarde la solicitud de licencia en un lugar conveniente, ya que podría ser necesario utilizar el procedimiento de realojamiento manual para reclamar sus licencias. Esta información también puede ayudar a Cisco a encontrar sus licencias.	Tramitación de licencias utilizando el Administrador de licencias
2	Mediante el cliente vSphere, despliegue la máquina virtual de administración para el sistema actualizado seleccionando la configuración con el sufijo **Auto-upgrade**; por ejemplo, **Admin 250 usuarios Auto-upgrade**.	
3	Encienda la máquina virtual de administración correspondiente al sistema actualizado y anote el URL que aparece en la consola de la máquina virtual.	
4	Escriba la URL de despliegue en el campo de URL de un explorador Web.	
5	Introduzca los URL y las credenciales de administración de vCenter, de modo que podamos desplegar las máquinas virtuales para usted.	Proporcionar las credenciales de VMware vCenter

Tarea	Descripción	Para obtener información detallada, consulte
6	Para desplegar máquinas virtuales adicionales, seleccione **Continuar**. (Hasta comenzar la configuración de la actualización del sistema y mientras el sistema original se encuentre en modo de mantenimiento, los usuarios pueden celebrar reuniones, pero los administradores no deben modificar las máquinas virtuales del sistema original).	El progreso de la actualización se muestra en el URL de despliegue del sistema actualizado y en la consola de VMware conectada a la máquina virtual de administración del sistema principal. La consola de VMware proporciona el URL de despliegue que se utilizará en el caso de que la ventana se cierre accidentalmente durante el proceso de actualización.
7	Anote los nombres de las máquinas virtuales creadas automáticamente que figuran en vCenter. El formato de los nombres de las máquinas virtuales es: CWMS_nombrehost_MMDDHHmm donde mm = minuto Cuando la actualización se haya completado, las máquinas virtuales no se mostrarán. Para encontrar las máquinas virtuales que se han creado como parte de la actualización de CWMS, puede realizar búsquedas según este formato.	
8	Para poner el sistema en modo de mantenimiento y comenzar la configuración del sistema actualizado, seleccione **Continuar**. Aparece un mensaje cuando el modo de mantenimiento se activa y puede durar hasta 30 minutos.	
9	Para abrir el sitio de Administración de Cisco WebEx, seleccione **Iniciar sesión en sitio de Administración**.	
10	Desactive el modo de mantenimiento en el sistema actualizado. El sistema se reinicia.	El servicio de reuniones tardará unos minutos en estar disponible. Su sistema está listo para que los usuarios puedan iniciar reuniones cuando todas las máquinas virtuales listadas en la página **Propiedades del sistema** muestran un estado Correcto (verde). Consulte Activar o desactivar el modo de mantenimiento para obtener más información.
11	Pruebe el sistema actualizado. Si la actualización no se realiza correctamente, apague el sistema actualizado, encienda el sistema original y póngase en contacto con el Centro de asistencia técnica de Cisco.	Prueba del sistema

Tarea	Descripción	Para obtener información detallada, consulte
12	Realoje y actualice la versión de la licencia según convenga para el sistema actualizado. El periodo de gracia sin necesidad de licencias caducará antes de 180 días. Si el sistema original tenía licencias válidas, dichas licencias deberán realojarse antes de 180 días. Si el sistema original estaba funcionado en el periodo de gracia sin licencias, el número de días sin licencia restantes se transfiere al sistema actualizado.	Acerca de las licencias - Realojamiento de licencias después de una actualización de software o la expansión del sistema

Actualización manual del sistema

Antes de comenzar una actualización manual

Antes de actualizar un sistema, deben abordarse las siguientes cuestiones:

- Elimine todas las instantáneas VMware del sistema original (existente).
- No encienda ni ejecute los dos sistemas al mismo tiempo, porque los nombres de host y las direcciones IP de las máquinas virtuales originales se usan en el sistema actualizado.
- Asegúrese de que el sistema actualizado puede acceder a los discos de la máquina virtual de administración del sistema original. (El disco duro 4 se copiará del sistema original al sistema actualizado).

Tareas para actualizar el sistema manualmente

Algunas de las tareas de esta tabla incluyen enlaces a otras secciones de la *Guía de administración de Cisco WebEx Meetings Server*. Estas secciones proporcionan información detallada sobre esa tarea. (Para desplazarse fácilmente entre esta tabla y la tarea individual en Adobe Acrobat, seleccione Vista anterior o Vista siguiente).

Tarea	Descripción	Para obtener información detallada, consulte
1	Vaya al administrador de licencias del sistema original y genere una solicitud de licencias seleccionando **Sistema** > **Ver más** > **Administrar licencias**. El administrador de licencias se abre en una nueva pestaña. Seleccione **Generar solicitud de licencia**. Aparece una ventana emergente con el texto de la solicitud de licencia. Copie el texto y guarde la solicitud de licencia en un lugar conveniente, ya que podría ser necesario utilizar el procedimiento de realojamiento manual para reclamar sus licencias. Esta información también puede ayudar a Cisco a encontrar sus licencias.	Acerca de las licencias
2	Inicie la sesión en el sitio de Administración del sistema original.	
3	Vaya a la pestaña Sistema y seleccione **Actualizar**.	

Tarea	Descripción	Para obtener información detallada, consulte
4	Seleccione **Actualización general**.	
5	Seleccione **Continuar** para archivar los datos del sistema original y poner el sistema en modo de mantenimiento.	
6	Mediante el cliente VMware vSphere, seleccione **Power** > **Shut Down Guest**en las máquinas virtuales del sistema original.	
7	Despliegue todas las máquinas virtuales del sistema actualizado, incluidas las máquinas virtuales de alta disponibilidad e IRP.	Desplegar el archivo OVA desde un cliente VMware vSphere
8	Copie los datos del sistema original a la máquina virtual de administración para el sistema actualizado.	Adjuntar un archivo VMDK existente a una nueva máquina virtual
9	Encienda la máquina virtual de administración actualizada y anote la URL de despliegue en la consola de la máquina virtual. Si el sistema incluirá alta disponibilidad (HA), no configure las máquinas virtuales HA en el despliegue de administrador HA; deje que el script de actualización descubra las máquinas virtuales HA. (Consulte Configuración de un sistema de alta disponibilidad.)	
10	Encienda las demás máquinas virtuales actualizadas.	
11	Escriba el URL de despliegue en un explorador web.	
12	Seleccione **Continuar** para iniciar la configuración del sistema.	El progreso de la actualización se muestra en el URL de despliegue del sistema actualizado y en la consola de VMware conectada a la máquina virtual de administración del sistema principal. La consola de VMware proporciona el URL de despliegue que se utilizará en el caso de que la ventana se cierre accidentalmente durante el proceso de actualización.

Tarea	Descripción	Para obtener información detallada, consulte
13	Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.	El servicio de reuniones tardará unos minutos en estar disponible. Su sistema está listo para que los usuarios puedan iniciar reuniones cuando todas las máquinas virtuales listadas en la página **Propiedades del sistema** muestran un estado Correcto (verde). Consulte Activar o desactivar el modo de mantenimiento para obtener más información.
14	Cuando la configuración del sistema haya acabado, **Iniciar sesión en sitio de Administración**.	
15	Pruebe el sistema actualizado. Cuando el sistema actualizado está funcionando correctamente, podrá eliminar su sistema original para liberar recursos del sistema original. Mantenga el sistema actualizado en ejecución al eliminar el sistema original para evitar la supresión accidental del archivo VMDK base del disco duro 4, al que el sistema actualizado podría acceder. Si la actualización no es satisfactoria, póngase en contacto con el TAC de Cisco, apague el sistema actualizado y encienda el sistema original.	Prueba del sistema
16	Realoje y actualice la versión de la licencia según convenga para el sistema actualizado. El periodo de gracia sin necesidad de licencias caducará antes de 180 días. Si el sistema original tenía licencias válidas, dichas licencias deberán realojarse antes de 180 días. Si el sistema original estaba funcionado en el periodo de gracia sin licencias, el número de días sin licencia restantes se transfiere al sistema actualizado.	Acerca de las licencias - Realojamiento de licencias después de una actualización de software o la expansión del sistema

Prueba del sistema

Algunas de las pruebas recomendadas para ejecutar en el sistema se muestran en esta sección. Puede realizar estas pruebas y validar su sistema utilizando dos herramientas de diagnóstico descritas en las páginas de soporte para este producto: La prueba de reuniones y la prueba de recursos del sistema.

Cuando se prueba un sistema actualizado, puede conservar el sistema original hasta que haya terminado de probar el sistema actualizado (pero no puede encender los dos sistemas al mismo tiempo). Una vez que esté conforme con los resultados de la pruebas del sistema actualizado, puede eliminar (de forma definitiva) el sistema existente. Asegúrese de que su sistema actualizado está funcionando al suprimir o eliminar el sistema

existente. De esta forma, se evita la eliminación accidental del archivo de disco de máquina virtual (VMDK) base, al cual puede acceder el sistema actualizado.

- Agregar, editar, activar y desactivar usuarios.
- Planificar y organizar una reunión.
- Volver a planificar una reunión existente.
- Eliminar una serie de reuniones o una reunión futura.
- Abrir un adjunto de la reunión.
- Reproducir una grabación de la reunión.

Realojamiento y actualización de las licencias

El realojamiento permite utilizar licencias de sistema originales en el sistema actualizado durante un tiempo limitado. Si no se realojan las licencias, no se pueden actualizar completamente. El periodo de gracia caducará antes de 180 días. A continuación de una actualización de software:

- Si el sistema original estaba funcionado sin licencias y en el periodo de gracia sin licencias, el número de días sin licencia restantes se transfiere al sistema actualizado.
- Si el sistema original tenía licencias válidas, dichas licencias serán válidas hasta un máximo de 180 días antes de que deban realojarse (consulte Realojamiento de licencias después de una actualización de software o la expansión del sistema) y actualizarse.

Acceder al formulario de solicitud de GLO

Para visualizar el formulario de solicitud de Operaciones globales de licencias (GLO), seleccione **Contacto** en la página de registro de licencia del producto (https://tools.cisco.com/SWIFT/LicensingUI/Quickstart). En la página de información de contacto de soporte de GLO, seleccione **solicitar**.

Antes de comenzar

Prepárese para proporcionar la siguiente información:

- Información de contacto
- Descripción del problema
- Nombre del producto y actividad de licencias (como el reenvío de información de licencia o la actualización de licencias)
- Información de privilegio (como el número de serie del producto)

Realojamiento de licencias después de una actualización de software o la expansión del sistema

Después de actualizar o ampliar el software de CWMS y de completar las pruebas, el siguiente paso consiste en realojar las licencias. Las licencias realojadas se invalidan automáticamente en el sistema original. Antes

de empezar el realojamiento, conserve una petición de licencias del sistema original por si es necesaria para realojar las licencias.

Cuando realoje las licencias, el número de ellas que puede realojar está limitado al número de licencias del sistema original. El método recomendado para realojar licencias es a través del portal de registro de licencias de productos.

Si el sistema original tenía licencias, el sistema actualizado le permite tener un periodo de gracia de 180 días antes de que sean necesarias las licencias, lo que le deja tiempo para probar el sistema actualizado antes de realojar las licencias originales en el sistema actualizado. El realojamiento se puede realizar por medio del portal de registro de licencias de producto en http://cisco.com/go/license (consulte Acceder al formulario de solicitud de GLO. Si el sistema original ya estaba funcionando en un periodo de gracia, el periodo de gracia del sistema actualizado es igual al periodo de gracia del sistema original cuando éste se actualizó. Si el sistema original estaba bloqueado como consecuencia de la falta de licencias, el sistema actualizado también estará bloqueado.

Guardar una solicitud de licencia

Para adquirir una solicitud de licencia para el sistema original:

Procedimiento

Paso 1 En la ventana de administración del sistema original, seleccione la ventana **Sistema**.

Paso 2 Seleccione **(en Licencias) ver más** > **Administrar licencias**.

Paso 3 Seleccione **Generar solicitud de licencia**.

Paso 4 Guarde la solicitud en una carpeta local del PC.

Registrar licencias que se realojarán

Para utilizar el portal de registro de licencias de producto:

Procedimiento

Paso 1 Inicie sesión en el portal de registro de licencias de producto en https://tools.cisco.com/SWIFT/LicensingUI/Quickstart.

Paso 2 Inicie sesión en la cuenta de cisco.com que se utilizó al tramitar las licencias del sistema original.
Si esta cuenta no está disponible o si inicia sesión y no encuentra licencias asociadas a esta cuenta, abra una incidencia en Cisco (consulte Acceder al formulario de solicitud de GLO.

Paso 3 Seleccione **Licencia para transferir: Iniciar** en el menú **transferir**. Aparece la ventana **Especificar origen de licencia**.

Paso 4 Marque la casilla de verificación situada junto al UUID del sistema desde el que desea realojar licencias. Por ejemplo, el UUID del sistema 1.x. Si tiene varios sistemas y no sabe el UUID del sistema desde el que desea realojar, vuelva al sistema original y lance el administrador de licencias. En la ventana **Licencias**, busque en la columna **Nombre de archivo** una cadena de licencia, por ejemplo

c8be79aeecaba5922955b53679527463_201311182150051080. Los caracteres desde el principio de la cadena hasta el delimitador de guión bajo (_) forman el UUID.

Paso 5 Vuelva al portal de registro de licencias de producto.

Paso 6 Seleccione las licencias que desee realojar y seleccione **Siguiente**. Se muestra la ventana **Especificar destino y opciones**.

Paso 7 Pegue la solicitud de licencia en el campo **Solicitud de licencia** del sistema de destino y seleccione **Siguiente**. El sistema de destino es el sistema al que se mueven las licencias. Si se trata de una actualización de software, el destino es el sistema actualizado. Si se trata de una expansión del sistema, el destino es el sistema más grande. Si se trata de una recuperación de desastre, el destino es el sistema posterior a la recuperación. Aparece la ventana **Revisar**.

Paso 8 Seleccione la casilla de verificación **Acepto los términos del acuerdo de licencia** y haga clic en **Enviar**. Recibirá un correo electrónico que contendrá las licencias realojadas. Tenga en cuenta que si está realizando el realojamiento en el contexto de una actualización de software, debe realojar (consulte Realojamiento de licencias después de una actualización de software o la expansión del sistema) y actualizar las licencias 1.0 en el sistema 2.0. Puede mostrarse un mensaje de error, como por ejemplo **Está utilizando un archivo de licencia no válido en su despliegue actual** en el sitio de administración del sistema actualizado. Se trata de una situación prevista. En el mensaje se incluye una fecha de caducidad que indica la fecha en que se deshabilitará su sistema. Actualice las licencias antes de la fecha de caducidad o su sistema se deshabilitará.

Qué hacer a continuación

Las licencias realojadas instaladas en el sistema actualizado tendrán la misma versión que las licencias existentes en el sistema original. Por ejemplo, cuando actualice de 1.X a 2.0, recibirá licencias 1.X que se reconocerán en el sistema 2.0. Cuando se instalan las licencias, se muestra un error: **Está utilizando un archivo de licencia no válido para su despliegue actual. Su sistema se deshabilitará el *dd/mm/yy* si continua esta situación.** Se trata de una situación prevista. (Este mensaje también puede enviarse por correo electrónico al administrador del sistema.)

Tras realojar las licencias, complete la actualización de licencias antes de la fecha mostrada para garantizar el uso ininterrumpido del sistema. (Consulte Tramitación de licencias utilizando el Administrador de licencias.)

Actualizar las licencias después de una actualización del software

Después de una actualización del software, las licencias se realojan del sistema original al sistema actualizado. (Consulte Realojamiento de licencias después de una actualización de software o la expansión del sistema para obtener más información). Después de que las licencias se hayan realojado, se pueden actualizar para su uso en el sistema actualizado.

Para actualizar sus licencias mediante eFulfilment:

1. Obtenga un código de clave de autorización de producto (PAK) de su proveedor.
2. En la ventana **Sistema**, seleccione **(en Licencias) Ver más**>**Administrar licencias**> **Licencias**> **Tramitar licencias desde PAK**. Se muestra la ventana **Tramitar licencias desde PAK**.
3. Introduzca el código PAK y seleccione **Siguiente**.
4. Inicie sesión mediante sus credenciales de cuenta de cisco.com. Se muestra la ventana **Tramitar licencias desde PAK**.
5. Haga clic en la columna de instalación para seleccionar el número de licencias que quiere instalar.
6. Indique el número de licencias que deben instalarse y seleccione **Guardar**. Las licencias se instalan en el sistema formando parte del eFulfillment de PAK.

Nota El número de licencias que puede instalar está limitado al número de licencias disponibles en el PAK de actualización y no puede superar el número de licencias que se realojaron del sistema original.

Para actualizar sus licencia desde un archivo de licencia:

1. Obtenga un archivo de licencia de Cisco mediante **cisco.com/go/license**.
2. En la ventana **Sistema**, seleccione **(en Licencias) Ver más**>**Administrar licencias**> **Licencias**> **Tramitar licencias desde archivo**. Se muestra la ventana **Instalar archivo de licencia**.
3. Busque el archivo de licencia. El archivo se muestra en la ventana **Licencias**.

Las licencias se actualizan automáticamente.

PARTE II

Guía de configuración de Cisco WebEx Meetings Server

- Utilización del escritorio, página 115
- Administrar usuarios, página 131
- Configurar su sitio, página 153
- Configuración de ajustes, página 187
- Gestionar sus informes, página 243
- Usar las funciones de soporte, página 251

CAPÍTULO 11

Utilización del escritorio

En este módulo se describen las funciones del escritorio de Cisco WebEx Server y cómo usarlas.

- Acerca de su escritorio, página 115
- Ver y editar alarmas, página 118
- Visualización del historial de recursos, página 120
- Visualización de tendencias de reunión, página 121
- Ver la lista de reuniones, página 122
- Planificación de una ventana de mantenimiento, página 123
- Cambiar una ventana de mantenimiento planificada, página 124
- Acerca del modo de mantenimiento, página 125
- Activar o desactivar el modo de mantenimiento, página 128

Acerca de su escritorio

En esta sección se describen las funciones del escritorio y cómo usarlas. El escritorio es la página de inicio del sitio de administración y proporciona varios parámetros y gráficos de las principales funciones de supervisión.

El escritorio contiene las secciones siguientes:

- Monitor del sistema: muestra el estado del sistema y la marca de hora, y además incluye las subsecciones siguientes:
  - Reuniones y usuarios: estado de las reuniones en curso y su uso. Muestra el número de reuniones actualmente en curso y el número de usuarios que participan en las reuniones (uso). El LED de estado indica si las reuniones están en curso y si el uso está por debajo o por encima del umbral de alarma configurado. Un LED de estado de color verde indica que está por debajo del umbral configurado, mientras que si es de color rojo indica que está por encima del umbral configurado. Consulte Ver y editar alarmas, en la página 118 para obtener información sobre la configuración de alarmas.

- Icono de alarma: seleccione el icono de alarma que desea ver y edite los ajustes de umbral de alarma que ha configurado. Los umbrales de alarmas aparecen en la página **Alarmas** en formato numérico. De forma predeterminada, los umbrales de alarmas aparecen como un porcentaje. Consulte Ver y editar alarmas, en la página 118 para obtener información sobre la configuración de alarmas.

  Puede configurar alarmas para lo siguiente:

  - Reuniones en curso: indica cuándo las reuniones en curso experimentan problemas.
  - Uso: número total de usuarios que están usando actualmente el sistema.
  - CPU: uso de CPU de la máquina virtual con el uso de CPU más elevado de todas las máquinas virtuales de este sistema.
  - Memoria: cantidad aproximada de memoria utilizada por la máquina virtual que tiene la mayor carga de memoria.

    Nota Cuando el LED es de color rojo durante breves periodos de tiempo, no es una indicación de que el sistema está en un estado crítico ni de que necesite atención inmediata. Un uso de memoria elevado podría indicar que hay otros problemas de rendimiento del sistema. Si el uso de memoria supera el 90 por ciento durante un largo periodo de tiempo, le recomendamos revisar las estadísticas de uso de memoria y CPU de vCenter. Si las estadísticas resultan estar fuera de rango, considere la posibilidad de modificar el sistema para reducir la carga.

  - Red: ancho de banda total del sistema usado.
  - Almacenamiento: espacio de almacenamiento de copia de seguridad de la base de datos y de grabaciones que se ha usado.

    Nota La alarma de almacenamiento solo aparece si ha configurado un servidor de almacenamiento. Consulte Configuración de un servidor de almacenamiento, en la página 164 para obtener más información.

    Nota Si el uso de almacenamiento se encuentra por encima del umbral, se inhabilita la grabación de reuniones.

- CPU, memoria, red y almacenamiento: muestra el porcentaje y la cantidad real de recursos usados y un LED de estado para cada uno de los recursos. Un LED de estado de color verde indica que está por debajo del umbral configurado, mientras que si es de color rojo indica que está por encima del umbral configurado. Consulte Ver y editar alarmas, en la página 118 para obtener información sobre la configuración de alarmas.

  Seleccione el enlace de CPU, memoria, red o almacenamiento para acceder a la página **Historial de recursos** o **Historial de almacenamiento**.

- Gráfico de tendencias de reuniones y lista de reuniones: gráfico que muestra el número de reuniones celebradas en el sistema durante un período de tiempo especificado. Utilice los campos **Desde** y **Hasta**

para definir el período de tiempo de la información de tendencias de reuniones y de las reuniones mostradas en la lista de reuniones. Puede seleccionar un punto en el gráfico de tendencias de reuniones para mostrar en la lista de reuniones las reuniones que se produjeron durante el intervalo de tiempo especificado en el gráfico. Para ver las reuniones que se han producido durante una hora específica del día, pase el ratón por encima del gráfico y seleccione la hora deseada. La lista de reuniones muestra el número total de reuniones que se produjeron durante el período de tiempo seleccionado, los temas de las reuniones, organizadores, número de participantes y el estado de la reunión. Puede ordenar por cada una de las columnas de información de la lista de reuniones y éstas se muestran en orden por estado: En curso, finalizadas y no iniciadas.

- Mantenimiento: permite planificar una ventana de mantenimiento para configurar el sistema o cambiar los ajustes, así como activar y desactivar el modo de mantenimiento. Consulte Planificación de una ventana de mantenimiento, en la página 123 y Acerca del modo de mantenimiento, en la página 125 para obtener más información.
- Última copia de seguridad: fecha y hora de la última copia de seguridad realizada; nombre de archivo, tamaño y ubicación de la copia de seguridad; y la fecha y hora de la siguiente copia de seguridad. También le notificará si la copia de seguridad ha fallado y la fecha del primer intento de realizar la copia de seguridad si todavía no se ha creado una.

Nota Solo aparece si ha configurado un servidor de almacenamiento.

- Sistema: muestra el número máximo de usuarios que pueden participar al mismo tiempo en reuniones, el número de versión, el URL del producto, si se permite el acceso público, si es un sistema de alta disponibilidad y el número de licencias de usuario. Si utiliza una versión de prueba de Cisco WebEx Server y quedan 30 o menos días del período de evaluación, esta sección también indicará cuántos días le quedan hasta que caduque el período de prueba. Seleccione **Ver más** para ir a Configurar su sitio, en la página 153.
- Usuarios: muestra el número total de usuarios activos, si se ha configurado la integración de directorio, cuándo se producirá la próxima sincronización (si se ha configurado) y el tipo seleccionado de autenticación. Seleccione **Ver más** para ir a Edición de usuarios, en la página 138.
- Ajustes: muestra el número máximo de participantes permitidos en cada reunión, tipo de audio y si se ha activado el vídeo HQ de WebHex. Seleccione **Ver más** para ir a Configuración de ajustes, en la página 187.

Temas relacionados

Visualización del historial de recursos, en la página 120

Uso del gráfico Reuniones en curso para tratar problemas de reuniones, en la página 120

Planificación de una ventana de mantenimiento, en la página 123

Activar o desactivar el modo de mantenimiento, en la página 128

Ver y editar alarmas

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Escritorio** > **Alarmas**.
Aparece la página **Alarmas** mostrando el umbral de la alarma actual.

Paso 3 Seleccione **Editar**.
Aparecerá la página **Editar alarmas**. Seleccione **Porcentaje %** para ver el umbral de la alarma como un porcentaje o **Número #** para ver el umbral de la alarma como un número. La configuración predeterminada es **Porcentaje %**.

Paso 4 Seleccione las casillas de verificación para las alarmas que desee activar y elija el intervalo para cada alarma activada.

Opción	Descripción
Reuniones en curso	Muestra el umbral de las reuniones en curso. • Si selecciona **Porcentaje %**, mueva la barra del selector para definir un porcentaje de 2 a 99. • Si selecciona **Número #**, introduzca un número de 2 a 99 por ciento. **Predet.**: Seleccionado con el intervalo de **una hora**.
Uso	Muestra el umbral del sistema actual. • Si selecciona **Porcentaje %**, mueva la barra del selector para definir un porcentaje de 2 a 99. • Si selecciona **Número #**, introduzca el número de usuarios. **Predet.**: Seleccionado con el intervalo de **12 horas**.
CPU	Muestra el umbral de la CPU actual en MHz. • Si selecciona **Porcentaje %**, mueva la barra del selector para definir un porcentaje de 2 a 99. • Si selecciona **Número #**, introduzca el número de MHz. **Predet.**: No seleccionado. El intervalo es de **una hora**.

Opción	Descripción
Memoria	Muestra el umbral actual de la memoria en GB. • Si selecciona **Porcentaje %**, mueva la barra del selector para definir un porcentaje de 2 a 99. • Si selecciona **Número #**, introduzca el número de GB **Predet.**: No seleccionado. El intervalo es de **una hora**. **Nota** El indicador Memoria muestra una aproximación de la memoria usada por la máquina virtual que tiene la mayor carga de memoria. Cuando el indicador se encuentra en la zona roja durante breves periodos de tiempo, no es una indicación de que el sistema está en un estado crítico ni de que necesite atención inmediata. Un uso de memoria elevado podría ser un indicador de que hay otros problemas de rendimiento del sistema que deben solucionarse. Si el uso de memoria supera el 90 por ciento durante un largo periodo de tiempo, le recomendamos revisar las estadísticas de uso de memoria y CPU de vCenter. Si las estadísticas resultan estar fuera de rango, considere la posibilidad de modificar el sistema para reducir la carga.
Red	Muestra el umbral actual de ancho de banda de la red en Mbps. • Si selecciona **Porcentaje %**, mueva la barra del selector para definir un porcentaje de 2 a 99. • Si selecciona **Número #**, introduzca el número de Mbps. **Predet.**: No seleccionado. El intervalo es de **una hora**.
Almacenamiento	Muestra el umbral actual de almacenamiento en Gb. El umbral de almacenamiento máximo se calcula así: espacio total-tamaño del búfer de grabación), en donde el tamaño del búfer de grabación es de 1 GB para micro, 5 GB para pequeño, 16 GB para mediano, y 40 GB para grande. • Si selecciona **Porcentaje %**, mueva la barra del selector para definir un porcentaje de 2 a 99. • Si selecciona **Número #**, introduzca el número de GB. **Predet.**: No seleccionado. El intervalo es de **una hora**. **Nota** Esta sección solamente aparece si ha configurado un servidor de almacenamiento. Consulte Configuración de un servidor de almacenamiento, en la página 164 para obtener más información.

Cuando una alarma excede un umbral, se envía un mensaje de correo electrónico a los administradores. El intervalo se utiliza para suprimir varias alarmas en el tiempo especificado para evitar enviar demasiados mensajes de correo electrónico acerca del mismo problema. El intervalo para cada alarma puede ser:

- una hora
- seis horas
- 12 horas

- 24 horas

Paso 5 Seleccione **Guardar**.
Sus ajustes de alarma se guardan y la página **Alarmas** se actualiza con sus cambios.

Visualización del historial de recursos

Su historial de recursos contiene gráficos detallados para cada alarma configurada en su sistema. Los valores actuales para estado del sistema reuniones, participantes y almacenamiento se muestran en los paneles de la derecha. Consulte Ver y editar alarmas para obtener más información sobre las alarmas que puede configurar.

Puede ver su historial de recursos seleccionando un enlace de alarma de **CPU**, **Memoria** o **Red** en la ventana **Escritorio**. Por ejemplo, seleccione el gráfico CPU y aparece la ventana **Historial de recursos**.

Si ha configurado un servidor de almacenamiento, puede ver su historial de almacenamiento seleccionando el enlace **Almacenamiento** en la ventana **Escritorio**. La página **Historial de almacenamiento** muestra la cantidad de espacio que se ha usado en su servidor de almacenamiento y un gráfico con el espacio de almacenamiento usado en los últimos seis meses. Mueva el ratón sobre el gráfico de uso de color azul para ver el porcentaje de espacio usado para días y horas específicos durante el periodo de seis meses.

Uso del gráfico Reuniones en curso para tratar problemas de reuniones

Cuando recibe un correo electrónico que indica que hay problemas con las reuniones, siga los siguientes pasos para determinar la causa.

Procedimiento

Paso 1 Seleccione el enlace del correo electrónico del error de la reunión que ha recibido.

Paso 2 Inicie sesión en el sitio de administración.

Paso 3 En el Escritorio, seleccione el enlace **CPU, Memoria** o **Red**.
Aparece el **Historial de recursos**.

Paso 4 En el panel lateral mostrado a la derecha de los gráficos de recursos, seleccione el enlace **Reuniones en curso**.

Paso 5 Opcionalmente, seleccione una opción de **Vista** o el icono de calendario para mostrar las reuniones para un periodo de tiempo específico.

Paso 6 Opcionalmente, seleccione la casilla de verificación **Mostrar reuniones futuras** para incluir las reuniones programas futuras en la lista **Reuniones**.

Paso 7 Haga clic en un punto de datos en el gráfico **Participantes** o **Reuniones** para mostrar la información de la reunión.
Puede utilizar la información detallada presentada en la tabla para ayudar a determinar la causa del problema descrito en el correo electrónico que ha recibido. La lista de reuniones muestra los detalles de las reuniones correspondientes al punto de datos seleccionado. Las reuniones con problemas de funcionamiento se muestran en la columna Estado de color rojo o amarillo.

Introduzca términos de búsqueda en el campo encima de la tabla para filtrar la lista de reuniones. La lista de reuniones puede ordenarse seleccionando la cabecera de la columna.

Paso 8 El estado actual del sistema se muestra en la columna derecha de la página. Seleccione esta línea para volver al escritorio.
El estado del sistema puede ser:

- Bueno: todos los servicios de su sistema están funcionando.
- Bajo: ningún servicio en su sistema se está ejecutando. Póngase en contacto con el Centro de asistencia técnica de Cisco (TAC) para obtener ayuda. Consulte Usar las funciones de soporte para obtener más información.

Paso 9 Seleccione la casilla de estado de la alarma en la columna derecha para ver el Historial de recursos para las alarmas. Consulte Visualización del historial de recursos para obtener más información.

Paso 10 Si ha configurado un servidor de almacenamiento, la cantidad de espacio de almacenamiento aparece en la columna derecha de la página. Consulte Ver y editar alarmas, en la página 118 para obtener más detalles.

Visualización de tendencias de reunión

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Escritorio**.

Paso 3 Encima del gráfico de **Tendencia de reunión** defina un periodo de tendencia seleccionando la fecha y hora **Desde** y **Hasta**.

- Las reuniones programadas para antes de medianoche y que se extienden hasta el día siguiente, se muestran en el gráfico para la fecha de inicio de la reunión.
- Si una reunión se desconecta debido a un problema del sistema y después vuelve a conectarse, se cuenta dos veces en el gráfico Tendencias de reunión.
- Los datos de tendencia de reunión para las vistas de un mes y seis meses se basan en la zona horaria de Greenwich (GMT) y, por lo tanto, no se muestran con precisión durante un periodo de 24 horas. Por ejemplo, si su sistema organiza 200 reuniones durante un día, la base de datos registra la frecuencia de esas reuniones basándose en GMT y no en la hora local. Los datos de tendencia de reunión para las vistas de un mes y seis meses se basan en la zona horaria del usuario.
- Una pista de color verde indica que la reunión está en curso o que ha finalizado. Las reuniones futuras se muestran en amarillo.
- Si el intervalo de tiempo seleccionado es de 24 horas, los puntos de datos de las reuniones pasadas o en curso se muestran en intervalos de cinco minutos y las reuniones futuras en intervalos de una hora.
- Si el intervalo de tiempo seleccionado es mayor que un día pero menor o igual que una semana, los puntos de datos de las reuniones pasadas, en curso o futuras se muestran en intervalos de una hora.
- Si el intervalo de tiempo seleccionado es mayor que una semana, los puntos de datos de las reuniones pasadas, en curso o futuras se muestran en intervalos de un día.

El gráfico de **Tendencia de reunión** muestra el número total de reuniones que se han producido durante el periodo de tiempo seleccionado. La lista de **Reuniones** que se muestra por debajo del gráfico visualiza todas las reuniones que se producen durante el período de tendencia seleccionado.

Nota Puede que algunas entradas de tendencia de reunión parezcan estar duplicadas, porque tienen el mismo nombre. Cada vez que se inicia una reunión se crea una entrada. Por lo tanto, si se inicia, se detiene y se reinicia una reunión, se mostrarán varias entradas con el mismo nombre de reunión.

Paso 4 Para ver una lista de reuniones que se han producido en un momento concreto:

a) Haga clic en una ubicación concreta del gráfico de **Tendencia de reunión** para mostrar una lista de las reuniones que se han producido en menos de 5 minutos de la hora seleccionada en la lista **Reuniones** que se encuentra a continuación del gráfico. Consulte Ver la lista de reuniones, en la página 122 para obtener más información.

b) Seleccione el símbolo de gráfico situado a continuación de los campos **Desde** y **Hasta** para visualizar una lista de fechas y horas en las que se han realizado reuniones en el periodo Desde y Hasta. A continuación, elija una fecha en la lista desplegable.

Nota Los puntos de datos mostrados en el menú desplegable son los mismos que los mostrados en el gráfico. Son accesibles para los usuarios con teclado y un lector de pantalla.

Nota Pase el ratón por encima del gráfico para ver el número total de reuniones que se han realizado en dicho momento.

Ver la lista de reuniones

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Escritorio**.

Paso 3 Encima del gráfico de tendencia de reuniones, defina un período de tendencia seleccionando la fecha y hora **Desde** y **Hasta**. Consulte Visualización de tendencias de reunión, en la página 121 para obtener más información.

Nota
- De forma predeterminada, la lista de reuniones muestra las reuniones correspondientes al período de 24 horas actual.
- Las reuniones planificadas que aún no se han iniciado en la hora planificada no se incluyen en el gráfico de tendencia de reuniones ni en la lista de reuniones.

La lista de reuniones muestra el número total de reuniones y en ella figuran todas las reuniones que están planificadas, en curso o que han finalizado durante el período de tendencia seleccionado. Las reuniones se muestran por orden de estado: En curso, finalizadas y no iniciadas. La información visualizada en la lista de reuniones es la siguiente:

- Intervalo de tiempo seleccionado en el gráfico de tendencia
- Tema de la reunión
- Organizador
- Número de participantes
- Estado de la reunión: En curso, finalizada y no iniciada

Nota Las reuniones que tienen el estado de *En curso* o *Finalizada* muestran un LED de color verde, amarillo o rojo en la primera columna para indicar el estado de la reunión como *buena*, *regular* o *pobre*. Regular (amarillo) indica que el retraso o jitter del audio o vídeo que tiene lugar durante la reunión ha alcanzado un umbral menor y debe supervisarse e investigarse para determinar la causa. Pobre (rojo) indica que el retraso o jitter del audio o vídeo que tiene lugar durante la reunión ha alcanzado un umbral mayor y el administrador debe ponerse en contacto con el grupo de Cisco Technical Assistance (TAC) para obtener ayuda.

Paso 4 Opcionalmente, seleccione una cabecera de columna para ordenar las reuniones.

Paso 5 Utilice la función de paginación para ver la página siguiente o anterior.

Nota
- En cada página se muestra un máximo de 10 reuniones.
- El número total máximo de reuniones a visualizar es de 125 para cualquier periodo de tendencia. Divida el período de tendencia en períodos de tiempo más breves si existen muchas reuniones en un período dado.
- En la lista de reuniones puede que vea entradas de reunión duplicadas. Cada vez que se inicia una reunión se crea una entrada de reunión. Por lo tanto, si se inicia, se detiene y se reinicia una reunión, en la lista se mostrarán varias entradas de reunión con el mismo nombre.

Planificación de una ventana de mantenimiento

Antes de realizar el mantenimiento del sistema, debe planificar una ventana de mantenimiento. La única limitación cuando la ventana de mantenimiento está activa es que los usuarios no pueden programar reuniones que están dentro de una ventana de mantenimiento o que se superponen. Por ejemplo, un administrador desea apagar el sistema durante aproximadamente una hora para mantenimiento, por ejemplo de las 05:00 a las 06:00, una hora en la que no parecen existir reuniones planificadas. Si existen reuniones planificadas, el administrador debe ponerse en contacto con el organizador de cada reunión para comunicarle que se ha planificado una ventana de mantenimiento en la hora de su reunión. Una vez se ha definido la ventana de mantenimiento, los usuarios no pueden planificar reuniones durante dicho periodo. Sin embargo, los usuarios pueden iniciar una reunión instantánea usando la función **Reunirse ahora**.

Después de activar el modo de mantenimiento, todas las reuniones actualmente en curso se finalizan y la función Reunirse ahora deja de estar disponible. Supongamos que cree que necesitaría unas dos horas para hacer los cambios necesarios en el sistema. Una de las tareas que tiene que realizar es cargar un nuevo certificado de una entidad emisora de certificados (CA), lo que puede requerir un reinicio del sistema después de desactivar el modo de mantenimiento. Tiene previsto iniciar el mantenimiento del sistema a las 4:00 horas. Programa una ventana de mantenimiento especificando una hora de inicio de 04/15/2014 3:30 horas y una duración de 3 horas. 30 min. Esto significa que la ventana de mantenimiento estará vigente desde las 03:00 horas (permitiendo finalizar todas las reuniones y no programar más reuniones hasta 30 minutos antes de que el administrador pretenda iniciar el mantenimiento del sistema) hasta las 07:00 horas. Este periodo de tiempo proporciona más tiempo para que el sistema esté operativo después de un reinicio posterior a la activación del modo de mantenimiento, y tiempo para que el administrador inicie una o más reuniones instantáneas para probar los ajustes modificados antes de que los usuarios puedan programar y organizar reuniones.

Mientras que ciertas tareas de mantenimiento del sistema no necesitan la activación del modo de mantenimiento, tenga presente que las tareas que sí requieren que el sistema esté en modo de mantenimiento necesitarán un tiempo adicional para completar un reinicio o un rearranque tras activar el modo de mantenimiento. El *reinicio* del sistema solamente tarda unos minutos (aproximadamente de 3 a 5 minutos) pero el *rearranque* tarda aproximadamente 30 minutos. Recuerde tener en cuenta este periodo de tiempo adicional para que su sistema

esté completamente operativo después de programar una ventana de mantenimiento. Consulte Activar o desactivar el modo de mantenimiento, en la página 128 para obtener más detalles.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Planificar mantenimiento**.
Se muestra **Planificar ventana de mantenimiento**.

Paso 3 Seleccione la fecha y hora inicial de la ventana de mantenimiento por medio de la herramienta de calendario y el menú desplegable de hora.

Paso 4 Especifique la duración de la ventana de mantenimiento especificando el número de horas y minutos.

Paso 5 Seleccione **Planificar**.
La fecha, hora inicial y duración de la ventana de mantenimiento planificada se muestra en el panel de Mantenimiento.

Nota Cuando empieza la ventana de mantenimiento, los usuarios reciben un mensaje de error si intentan planificar una reunión que se solape con la ventana de mantenimiento planificada.

Qué hacer a continuación

- Consulte Activar o desactivar el modo de mantenimiento para obtener información sobre la activación del modo de mantenimiento.
- Consulte Enviar correos electrónicos a usuarios para obtener información detallada sobre la notificación a los usuarios del mantenimiento del sistema.

Cambiar una ventana de mantenimiento planificada

Después de planificar una ventana de mantenimiento, puede volver a planificar la fecha y hora o suprimirla.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Escritorio**.

Paso 3 Seleccione la fecha y hora de mantenimiento del sistema mostrada.

Paso 4 En **Planificar ventana de mantenimiento**, puede:

- Introducir una fecha y hora de inicio diferente.
- Modificar las horas y minutos de duración.
- Seleccione **Suprimir** para eliminar la ventana de mantenimiento.

Nota Si finaliza antes el mantenimiento del sistema, puede reducir el tiempo de duración o seleccionar **Suprimir** en **Planificar ventana de mantenimiento**.

Qué hacer a continuación

Recuerde activar el modo de mantenimiento antes de modificar las propiedades del sistema. Consulte Acerca del modo de mantenimiento, en la página 125 para obtener información sobre las propiedades del sistema que requieren que se active el modo de mantenimiento.

Acerca del modo de mantenimiento

Muchos cambios de configuración requieren que coloque el sistema en modo de mantenimiento. El modo de mantenimiento desconecta la actividad de las conferencias, por lo que tendrá que programar sus ventanas de mantenimiento para interrumpir mínimamente a sus usuarios. Aunque le recomendamos planificar una ventana de mantenimiento antes de activar el modo de mantenimiento, no es necesario hacerlo. Puede activar el modo de mantenimiento en cualquier momento. El botón **Activación del modo de mantenimiento** aparece en la página **Escritorio**.

Después de determinar cuándo quiere realizar el mantenimiento del sistema, utilice la función **Planificar mantenimiento** en la página **Escritorio** para programar una ventana de mantenimiento. Consulte Planificación de una ventana de mantenimiento, en la página 123 para obtener información detallada. A continuación, seleccione la función **Enviar correo electrónico a usuarios** para notificar a sus usuarios con antelación que no podrán unirse ni organizar reuniones durante la ventana de mantenimiento. Consulte Enviar correos electrónicos a usuarios, en la página 151 para obtener más información.

Al activar el modo de mantenimiento, ocurre lo siguiente:

- Las reuniones actualmente en curso finalizarán.
- Los usuarios no pueden programar ni organizar reuniones nuevas.
- Los usuarios no pueden iniciar sesión en el sitio de WebEx desde páginas web, el complemento de Microsoft Outlook o aplicaciones móviles.
- El sistema seguirá enviando correos electrónicos de notificación de forma automática a los usuarios y administradores.

Utilice la tabla siguiente para determinar qué tareas requieren que active el modo de mantenimiento y la acción que realiza su sistema después de desactivar el modo de mantenimiento. El sistema proporciona mensajes de recordatorio si intenta llevar a cabo estas tareas sin activar antes el modo de mantenimiento.

Tarea	Referencia	Modo de mantenimiento necesario	Reinicios o rearranques del sistema después de desactivar el modo de mantenimiento
Agregar y suprimir sistemas de alta disponibilidad	Configuración de un sistema de alta disponibilidad, en la página 154	S	Reiniciar
Agregar y suprimir acceso público desplegando o quitando un proxy inverso de Internet	Agregar el acceso público a su sistema, en la página 158 y Eliminar el acceso público, en la página 160	S	Reiniciar

Tarea	Referencia	Modo de mantenimiento necesario	Reinicios o rearranques del sistema después de desactivar el modo de mantenimiento
Cambiar el idioma predeterminado del sistema	Configuración de la información de su empresa, en la página 188	S	Reiniciar
Cambiar las URL de la cuenta de organizador o administrador	Cambiar la configuración de su sitio, en la página 162	S	Reiniciar
Cambiar su servidor de correo	Configurar un servidor de correo, en la página 163	N	N/D
Cambiar la dirección IP virtual	Cambiar su dirección IP virtual, en la página 158	S	Reiniciar
Configurar y cambiar los ajustes de personalización	Configuración de los ajustes de personalización, en la página 189	N	N/D
Configurar y cambiar muchos de los ajustes de audio	Acerca de configurar sus ajustes de audio, en la página 193	S	Reiniciar
Configurar y cambiar los números de acceso de llamada directa, el nombre de visualización y los ajustes de audio del identificador de llamada.	Configuración de los ajustes de audio, en la página 195	N	N/D
Configurar y cambiar la calidad de los ajustes de servicio	Configuración de la calidad del servicio (QoS), en la página 198	N	N/D
Configurar y cambiar los ajustes SNMP	Configuración de los ajustes SNMP, en la página 169	S	Reiniciar
Configurar certificados	Administración de certificados, en la página 226	S	Reinicio o rearranque (determinado por el sistema)
Configurar los ajustes de recuperación ante desastres	Utilizar la función de recuperación ante desastres, en la página 166	S	Reiniciar
Configurar el cifrado compatible con FIPS	Activación del cifrado compatible con FIPS, en la página 242	S	Reiniciar

Tarea	Referencia	Modo de mantenimiento necesario	Reinicios o rearranques del sistema después de desactivar el modo de mantenimiento
Configurar servidores de almacenamiento	Configuración de un servidor de almacenamiento, en la página 164	S	Reiniciar
Configurar la seguridad de la máquina virtual	Configuración de la seguridad de la máquina virtual, en la página 240	S	Reiniciar
Expandir tamaño del sistema	Expandir el tamaño del sistema, en la página 161	S	Reiniciar
Realizar actualizaciones menores, actualizaciones mayores y ampliar su sistema	Actualización del sistema, en la página 95	S	Reiniciar
Actualizar claves compartidas	Administración de certificados, en la página 226	S	Reiniciar
Utilización de la prueba de recursos del sistema	Utilización de la prueba de recursos del sistema, en la página 254	S	Reiniciar

Cada una de sus máquinas virtuales tiene una ventana de consola que indica cuándo está en modo de mantenimiento. Puede abrir las ventanas de consola en la barra de inventario vCenter (para navegar). Las ventanas de consola proporcionan la URL del sistema, el tipo de sistema (principal, alta disponibilidad o acceso público), el tipo de despliegue (sistema de 50, 250, 800 o 2000 usuarios) y el estado actual del sistema, incluyendo si el modo de mantenimiento está activado o desactivado y la fecha y hora del cambio de estado. La hora que se muestra se configura en los ajustes de Información de la empresa. Consulte Configuración de la información de su empresa, en la página 188 para obtener más información.

Finalización de las tareas de mantenimiento del sistema

Cuando haya acabado de modificar la configuración de su sistema, puede desactivar el modo de mantenimiento. En función de las tareas realizadas, su sistema:

- Puede estar operativo rápidamente si no hizo falta el modo de mantenimiento para las actualizaciones.
- Puede visualizar un mensaje para indicar que los cambios efectuados requieren un*rearranque* del sistema que solamente tarda unos minutos.
- Puede visualizar un mensaje para indicar que los cambios efectuados requieren un *reinicio* del sistema que tarda aproximadamente 30 minutos, en función del tamaño del sistema.

Un rearranque del sistema dura unos pocos minutos pero un reinicio del sistema puede durar hasta 30 minutos. Durante este tiempo, la actividad de las conferencias no está disponible. El sistema determina la acción necesaria y visualiza el correspondiente mensaje al desactivar el modo de mantenimiento.

Cuando el modo de mantenimiento está desactivado, la página **Escritorio** se actualiza. Su sistema está listo para que los usuarios puedan iniciar reuniones cuando todas las máquinas virtuales listadas en la página **Propiedades del sistema** muestran un estado Correcto (verde). Consulte Activar o desactivar el modo de mantenimiento, en la página 128 para obtener más información.

Si desactiva el modo de mantenimiento y la ventana de mantenimiento planificado sigue activa, los usuarios podrán organizar y asistir a reuniones anteriormente planificadas, pero no podrán planificar nuevas reuniones hasta que finalice la ventana de mantenimiento.

Activación y desactivación del modo de mantenimiento para una actualización del sistema

Si actualiza *manualmente* su sistema a Cisco WebEx Meetings Server versión 2.0 desde la versión 1.x, después de desplegar todas las máquinas virtuales para su sistema actualizado, aparece un mensaje cuando es necesario activar el modo de mantenimiento. Debe activar manualmente el modo de mantenimiento.

Si escoge el proceso de actualización *automática*, se activa automáticamente el modo de mantenimiento en el momento oportuno y se visualiza un mensaje para que pueda saber cuándo se produce.

Cuando se completa el proceso de actualización manual o automática, debe desactivar manualmente el modo de mantenimiento en el sistema actualizado de Cisco WebEx Meetings Server versión 2.0. El servicio de reuniones tardará unos minutos en estar disponible.

Temas relacionados

Planificación de una ventana de mantenimiento, en la página 123
Activar o desactivar el modo de mantenimiento, en la página 128

Activar o desactivar el modo de mantenimiento

Antes de modificar la configuración de su sistema, debería programar una ventana de mantenimiento y notificar a los usuarios la hora de mantenimiento programada para el sistema. Consulte Planificación de una ventana de mantenimiento, en la página 123 para obtener información detallada.

Nota Cuando se activa el modo de mantenimiento, los usuarios no pueden planificar, organizar o asistir a reuniones. Las reuniones actualmente en curso finalizarán.

Antes de comenzar

Al activar el modo de mantenimiento, se interrumpe la actividad de las conferencias y se impide que los usuarios inicien sesión en su sitio de WebEx, programando o uniéndose a reuniones y reproduciendo grabaciones de reuniones. Al desactivar el modo de mantenimiento, el sistema determina si se necesita un *rearranque* (tarda unos 3-5 minutos) o un *reinicio* (tarda unos 30 minutos) y muestra el mensaje adecuado. Consulte Acerca del modo de mantenimiento para obtener información sobre las tareas del sistema que requieren que se active el modo de mantenimiento.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento**.

Se muestra el diálogo **Activar modo de mantenimiento**. No olvide leer la condición del sistema mientras esté activado el modo de mantenimiento.

Paso 3 Seleccione **Continuar** cuando esté preparado para iniciar el modo de mantenimiento.
Se muestra un mensaje que indica que el sistema se encuentra en modo de mantenimiento. Se muestra el botón **Desactivar el modo de mantenimiento**.

Paso 4 (Opcional) Realice una copia de seguridad de las máquinas virtuales.

Paso 5 Seleccione **Desactivar modo de mantenimiento** cuando finalice la configuración del sistema.
Dependiendo de las propiedades del sistema que haya modificado, puede tardar unos minutos o aproximadamente 30 minutos para que los usuarios puedan iniciar sesión y reanudar las actividades de conferencias.

Paso 6 (Opcional) Para determinar si el sistema está operativo, seleccione **Escritorio** > **Sistema** > **Ver más** (en la sección Sistema).
La actividad de conferencias puede reanudarse cuando el **Estado** para todas las máquinas virtuales listadas es **Correcto** (verde).

Qué hacer a continuación

Si la ventana de mantenimiento sigue vigente después de desactivar el modo de mantenimiento y su sistema ha terminado el rearranque o el reinicio, los usuarios pueden iniciar reuniones instantáneas seleccionando **Reunirse ahora** en la página **Reuniones**. Consulte "Iniciar una reunión instantánea" en la *Guía del usuario* en http://www.cisco.com/en/US/products/ps12732/tsd_products_support_maintain_and_operate.html.

CAPÍTULO 12

Administrar usuarios

En esta sección se describe cómo administrar usuarios en su sistema.

- Acerca de la administración de usuarios, página 131
- Acerca de los archivos delimitados por comas y tabulaciones, página 132
- agregar usuarios, página 138
- Edición de usuarios, página 138
- Activación de usuarios, página 139
- Desactivación de usuarios, página 139
- Desactivación de usuarios usando la importación, página 140
- Importar usuarios, página 140
- Exportando usuarios, página 141
- Importar usuarios a un nuevo sistema mediante un archivo exportado, página 141
- Configuración de códigos de seguimiento, página 142
- Configuración de la integración de directorios, página 144
- Sincronizar grupos de usuarios, página 149
- Utilización de CUCM para configurar el servicio Web de AXL y la sincronización de directorios, página 150
- Utilización de CUCM para configurar la autenticación y la integración LDAP, página 150
- Enviar correos electrónicos a usuarios, página 151

Acerca de la administración de usuarios

Puede agregar usuarios individualmente o importar listas de usuarios almacenados en un archivo delimitado por comas o tabulaciones.

Puede agregar y desactivar cuentas de usuario, pero no puede eliminarlas. La desactivación le permite desactivar a un usuario, pero proporciona la habilidad de reactivar al usuario más tarde si fuese necesario. Una cuenta

de usuario reactivada vuelve a obtener acceso a las reuniones, grabaciones y a otros datos a los que se tenía acceso antes de la desactivación.

El sistema admite un ciclo de vida máximo de 400 000 cuentas de usuario. Este número representa el total de cuentas de usuario activas e inactivas. Este número máximo de ciclo de vida es lo suficientemente grande para alojar el crecimiento previsto en la base de datos de usuario.

Para impedir el inicio de sesión no autorizado en el sistema, no olvide desactivar cualquier usuario que abandone su organización. Puede desactivar usuarios de las formas siguientes:

- Si su sistema no utiliza el SSO integrado, puede desactivar usuarios individualmente o importando un archivo delimitado por comas o tabulaciones con el campo ACTIVO definido en N para cada usuario que desee desactivar. Consulte Desactivación de usuarios, en la página 139 y Acerca de los archivos delimitados por comas y tabulaciones, en la página 132 para obtener más información.
- Si su sistema utiliza el SSO integrado, puede desactivar a los usuarios eliminándolos del directorio corporativo en su SAML 2.0 iDP. Este procedimiento no lo realiza este producto.
- Utilice la función de configuración de contraseña para desactivar usuarios después de un periodo de tiempo específico. Consulte Configuración de sus ajustes generales de contraseña, en la página 200 para obtener más información.

Acerca de los archivos delimitados por comas y tabulaciones

Para utilizar una aplicación de hoja de cálculo, como Microsoft Excel, para organizar los datos de usuario, guarde o exporte su hoja de cálculo como archivo delimitado por comas o tabulaciones (CSV). Su sistema admite el formato de transformación UCS de 8 bits (UTF-8). Los caracteres que introduce en su archivo se limitan a los especificados en UTF-8. Si su archivo contiene caracteres distintos a ASCII, compruebe que utiliza un delimitador Unicode por comas o tabulaciones.

Para importar correctamente un archivo delimitado por comas o tabulaciones, todos los campos indicados en la tabla son obligatorios. Los valores de los campos pueden estar vacíos. Si falta un campo, aparecerá un mensaje de error. Por ejemplo, "Formato de archivo incorrecto. Custom10 es obligatorio."

Pueden definir hasta diez **Grupos de código de rastreo**. Los nombres del grupo de código de rastreo deben ser únicos y no deben usar nombres de campo predefinidos (USERID, ACTIVE, FIRSTNAME, LASTNAME, EMAIL, LANGUAGE, HOSTPRIVILEGE, TIMEZONE).

Nombre del campo	Descripción	Tamaño y tipo de valor
USERID	ID de usuario **Nota** Este campo está generado automáticamente por el sistema y se debe dejar en blanco al importar un archivo CSV.	Entre 1 y 19 caracteres alfanuméricos
ACTIVE	Si este usuario está activo o no.	Sí o No
FIRSTNAME	Nombre del usuario.	Cadena de entre 1 y 32 caracteres
LASTNAME	Apellidos del usuario.	Cadena de entre 1 y 32 caracteres

Nombre del campo	Descripción	Tamaño y tipo de valor
EMAIL	Dirección de correo electrónico del usuario.	Cadena de entre 1 y 192 caracteres alfanuméricos
LANGUAGE	Idioma del usuario. Consulte Valores de los campos de los archivos CSV para obtener más información.	Cadena de entre 1 y 64 caracteres
HOSTPRIVILEGE	Privilegios de organizador.	ADMN o HOST
TIMEZONE	Zona horaria en la que se encuentra el usuario. Consulte Valores de los campos de los archivos CSV para obtener más información.	Nombre de la zona horaria
DIVISION	División del usuario. Para el grupo de código de seguimiento 1. Este campo puede configurarse en la página Códigos de seguimiento. Consulte Configuración de códigos de seguimiento para obtener más información.	Cadena de entre 1 y 128 caracteres
DEPARTMENT	Departamento del usuario. Para el grupo de código de seguimiento 2. Este campo se puede configurar en la página Códigos de seguimiento. Consulte Configuración de códigos de seguimiento para obtener más información.	Cadena de entre 1 y 128 caracteres
PROJECT	Proyecto del usuario. Para el grupo de código de seguimiento 3. Este campo se puede configurar en la página Códigos de seguimiento. Consulte Configuración de códigos de seguimiento para obtener más información.	Cadena de entre 1 y 128 caracteres
OTHER	Otros datos. Para el grupo de código de seguimiento 4. Este campo se puede configurar en la página Códigos de seguimiento. Consulte Configuración de códigos de seguimiento para obtener más información.	Cadena de entre 1 y 128 caracteres
CUSTOM5	Campo personalizado 5.	Cadena de entre 1 y 128 caracteres
CUSTOM6	Campo personalizado 6.	Cadena de entre 1 y 128 caracteres
CUSTOM7	Campo personalizado 7.	Cadena de entre 1 y 128 caracteres

Nombre del campo	Descripción	Tamaño y tipo de valor
CUSTOM8	Campo personalizado 8.	Cadena de entre 1 y 128 caracteres
CUSTOM9	Campo personalizado 9.	Cadena de entre 1 y 128 caracteres
CUSTOM10	Campo personalizado 10.	Cadena de entre 1 y 128 caracteres

Valores de los campos de los archivos CSV

Valores de campo idioma

A continuación se proporcionan ejemplos de los códigos de país que puede utilizar en un archivo CSV.

Valor de campo	Idioma
es-es	Inglés de EE.UU.
zh-cn	Chino simplificado
zh-tw	Chino tradicional
JP	Japonés
KO	Coreano
Vier	Francés
DE	Alemán
IT	Italiano
es-es	Español de España
ES	Español de Latinoamérica
NL	Holandés
pt-br	Portugués
RU	Ruso

Valores de campo de zona horaria

A continuación se indican los valores de los campos de zona horaria (TIMEZONE) que puede establecer en un archivo CSV.

Valor de campo	GMT
Islas Marshall	-12 h
Samoa	-11 h
Honolulu	-10 h
Anchorage	-9 h
San Francisco	-8 h
Tijuana	-8 h
Arizona	-7 h
Denver	-7 h
Chihuahua	-7 h
Chicago	-6 h
Ciudad de México	-6 h
Saskatchewan	-6 h
Tegucigalpa	-6 h
Bogotá	-5 h
Panamá	-5 h
Nueva York	-5 h
Indiana	-5 h
Caracas	-4,5 h
Santiago	-4 h
Halifax	-4 h
Terranova	-3,5 h
Brasilia	-3 h
Buenos Aires	-3 h
Recife	-3 h

Valor de campo	GMT
Nuuk	-3 h
Atlántico Medio	-2 h
Azores	-1 h
Reikiavik	0 h
Londres	0 h
Casablanca	0 h
África Occidental	1 hora
Amsterdam	1 hora
Berlín	1 hora
Madrid	1 hora
París	1 hora
Roma	1 hora
Estocolmo	1 hora
Atenas	2 h
El Cairo	2 h
Pretoria	2 h
Helsinki	2 h
Tel Aviv	2 h
Amán	2 h
Estambul	2 h
Riyadh	3 h
Nairobi	3 h
Teherán	3,5 h
Moscú	4 h

Valor de campo	GMT
Abu Dhabi	4 h
Baku	4 h
Kabul	4,5 h
Islamabad	5 h
Bombay	5,5 h
Colombo	5,5 h
Ekaterimburgo	6 h
Almaty	6 h
Katmandú	6,75 h
Bangkok	7 h
Pekín	8 h
Perth	8 h
Singapur	8 h
Taipéi	8 h
Kuala Lumpur	8 h
Tokio	9 h
Seúl	9 h
Adelaida	9,5 h
Darwin	9,5 h
Yakutsk	10 h
Brisbane	10 h
Sídney	10 h
Guam	10 h
Hobart	10 h

Valor de campo	GMT
Vladivostok	11 h
Islas Salomón	11 h
Wellington	12 h
Fiji	12 h

agregar usuarios

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Usuarios** > **Añadir usuario**.

Paso 3 Seleccione el tipo de cuenta (**Organizador** o **Administrador**).

Paso 4 Complete los campos con la información del usuario. Los campos marcados con un asterisco son obligatorios.

Paso 5 Seleccione **Guardar**.
Cisco WebEx Meetings Server envía un correo electrónico al usuario con un enlace de **Crear contraseña**. El usuario debe crear una contraseña antes de iniciar sesión en el sitio de WebEx.

Nota El enlace para crear la contraseña caduca en 72 horas.

Edición de usuarios

Puede cambiar la información del usuario y activar o desactivar las cuentas de usuario con la función de editar usuario.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Usuarios**.
Aparece la lista de usuarios. La cantidad predeterminada de los usuarios que se muestran en cada página es 50. Opcionalmente, puede seleccionar el menú desplegable **Usuarios por página** y cambiar la configuración a **50** o **100**.

Paso 3 Seleccione un usuario para editarlo.

Paso 4 Haga los cambios en los campos editables. Los campos marcados con un asterisco son obligatorios.

Paso 5 Opcionalmente, seleccione la casilla de verificación **Obligar a este usuario a modificar la contraseña la próxima vez que inicie la sesión**.

Nota Si SSO está habilitado en su sistema, esta función no se aplica a las cuentas de organizador.

Paso 6 Activar o desactivar una cuenta opcionalmente:

- Seleccione **Activar** para reactivar una cuenta inactiva.
- Seleccione **Desactivar** para desactivar una cuenta.

Nota Activar o desactivar una cuenta no guarda cualquier otro cambio que haya realizado en la cuenta. Debe seleccionar **Guardar** para guardar sus cambios.

Paso 7 Seleccione **Guardar**. Guarda sus cambios sin modificar el estado de la cuenta.

Activación de usuarios

Después de agregar o importar cuentas de host y administrador, éstas se encuentran activas de forma predeterminada. Utilice esta función para volver a activar a usuarios inactivos.

También puede activar una cuenta en la página **Editar usuario**. Consulte Edición de usuarios, en la página 138 para obtener más información.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Usuarios**.

Paso 3 Seleccione las casillas de verificación para los usuarios inactivos que desee activar.

Paso 4 Seleccione **Acciones** > **Activar**.
Las cuentas seleccionadas se activan y el estado para cada cuenta debería ser "Activo".

Desactivación de usuarios

Puede desactivar las cuentas de organizador y administrador. Desactivar una cuenta impide que el propietario de la cuenta haga lo siguiente:

- Iniciar sesión desde páginas Web, el complemento de Outlook y aplicaciones móviles
- Organizar o asistir a reuniones
- Administración del sistema (si el usuario es un administrador)

Alternativamente, puede desactivar una cuenta en la página **Editar usuario**. Consulte Edición de usuarios, en la página 138 para obtener más información.

Nota Los administradores no pueden desactivar sus propias cuentas.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Usuarios**.

Paso 3 Seleccione las casillas de verificación para cualquier usuario activo que quiera desactivar.

Paso 4 Seleccione **Acciones** > **Desactivar** y confirme seleccionando **Aceptar**.
Las cuentas seleccionadas se desactivan y el estado para cada cuenta debería mostrar "Inactivo".

Desactivación de usuarios usando la importación

Puede utilizar la función de importación para desactivar cuentas de usuario.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Usuarios** > **Importar/exportar usuarios**> **Exportar**.
Espere unos momentos hasta que aparezca el enlace **Descargar archivo CSV exportado**.

Paso 3 Seleccione **Descargar archivo CSV exportado** y guarde el archivo CSV en su disco duro.

Paso 4 Abra el archivo CSV. Vaya a la columna ACTIVO y haga los cambios siguientes:

a) Introduzca N para cada usuario que quiera desactivar.

b) Elimine todos los registros para los usuarios que no desea cambiar.

Paso 5 Seleccione **Usuarios** > **Importar/exportar usuarios** > **Importar**.

Paso 6 Seleccione **Examinar**, seleccione su archivo CSV actualizado, seleccione **Comas** y a continuación, seleccione **Importar**.
Los registros de usuario actualizados se sobrescriben y las cuentas de usuario seleccionadas se desactivan.

Importar usuarios

Antes de comenzar

Prepare un archivo de datos delimitados por comas o tabulaciones que contenga la información de sus usuarios. Consulte Acerca de los archivos delimitados por comas y tabulaciones, en la página 132 para obtener más información.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Usuarios** > **Importar/exportar usuarios**.

Aparecerá la página Importar/exportar usuarios.

Paso 3 Seleccione **Importar**.
Aparece la página Importar usuarios.

Paso 4 Seleccione **Examinar** y, a continuación, seleccione el archivo delimitado por comas o tabulaciones que desee importar.

Paso 5 Seleccione el botón de opción **Tabulaciones** o **Comas** para indicar el tipo de archivo que está importando.

Paso 6 Seleccione **Importar**.
Su archivo se ha importado. Después de completarse la importación, el sistema envía un correo electrónico indicando cuántos registros se han importado correctamente y cuántos no.

Qué hacer a continuación

Seleccione **Usuarios** para ver los usuarios en su sistema. Compruebe que los usuarios se han importado correctamente.

Exportando usuarios

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Usuarios** > **Importar/exportar usuarios**.

Paso 3 Seleccione **Exportar**.
Sus datos de usuario se exportan a un archivo CSV. El sistema le envía un correo electrónico al administrador con el enlace para descargar el archivo exportado.

Importar usuarios a un nuevo sistema mediante un archivo exportado

Realice los siguientes pasos para Importar usuarios a un nuevo sistema utilizando un archivo exportado.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración en el sistema cuyos usuarios quiere exportar.

Paso 2 Seleccione **Usuarios** > **Importar/exportar usuarios**.

Paso 3 Seleccione **Exportar**.

Sus datos de usuario se exportan a un archivo de datos delimitados por comas o tabulaciones.

Paso 4 Abra el archivo exportado, elimine todos los ID de usuario (USERID) del archivo y vuelva a guardar el archivo.

Paso 5 Inicie sesión en el sitio de administración en el sistema cuyos usuarios quiere importar.

Paso 6 Seleccione **Usuarios** > **Importar/exportar usuarios**.
Aparecerá la página Importar/exportar usuarios.

Paso 7 Seleccione **Importar**.
Aparece la página Importar usuarios.

Paso 8 Seleccione **Examinar** y después seleccione el archivo que ha exportado anteriormente.

Paso 9 Seleccione el botón de opción **Tabulaciones** o **Comas** para indicar el tipo de archivo que está importando.

Paso 10 Seleccione **Importar**.
Su archivo se ha importado. Después de completarse la importación, el sistema envía un correo electrónico indicando cuántos registros se han importado correctamente y cuántos no.

Qué hacer a continuación

Seleccione **Usuarios** para ver los usuarios en su sistema. Compruebe que los usuarios se han importado correctamente.

Configuración de códigos de seguimiento

Puede configurar códigos de seguimiento para controlar el uso del organizador en grupos especificados. Por ejemplo, puede configurar los códigos de seguimiento para proyectos o departamentos. Los códigos de seguimiento que configura aparecen como opciones cuando agrega o edita usuarios.

Debe configurar lo siguiente para cada código de seguimiento:

- Grupo de código de seguimiento: configure sus grupos de código de seguimiento. Los grupos de código de seguimiento se utilizan cuando agrega y edita usuarios. Los valores predeterminados son División, Departamento, Proyecto, Otro y Personalizado 5 a Personalizado 10.

  Nota Los nombres del grupo de código de rastreo deben ser únicos y no deben usar nombres de campo predefinidos (USERID, ACTIVE, FIRSTNAME, LASTNAME, EMAIL, LANGUAGE, HOSTPRIVILEGE, TIMEZONE).

- Modo de introducción: seleccione **Campo de texto** o **Menú desplegable**.
- Uso: seleccione **No se utiliza**, **Opcional** o **Necesario**.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Usuarios** > **Códigos de seguimiento**.

Paso 3 Opcionalmente, puede introducir el nombre de todos los grupos de seguimiento que desee configurar en la columna **Grupo de código de seguimiento**. No tiene que cambiar ningún campo si quiere usar los valores predeterminados.

Paso 4 Seleccione **Introducción de texto** o **Menú desplegable** en la columna **Modo de introducción** para cada código de seguimiento.
Si selecciona **Introducción de texto** configurará su nombre de código de seguimiento en un campo de texto. Si selecciona **Menú desplegable**, aparecerá un enlace **Editar lista** al lado del campo **Modo de introducción**. Seleccione el enlace **Editar lista** para configurar los valores en el menú desplegable para ese código de seguimiento. Consulte Modificación de los códigos de seguimiento, en la página 143 para obtener más información.

Nota Si selecciona **Menú desplegable** para uno de sus grupos de código de seguimiento, debe seleccionar **Editar lista** e introducir una o más opciones para el menú desplegable asociado.

Paso 5 Seleccione **No se utiliza**, **Opcional** o **Necesario** en la columna **Uso** para cada código de seguimiento.

Nota Solo debería cambiar el uso a **Necesario** u **Opcional** si ha configurado una lista de menú desplegable. Aparece un mensaje de error si intenta configurar un ajuste de uso con otros valores distintos a **No se utiliza**, si no ha configurado antes del Grupo de código de seguimiento y el Modo de introducción.

Paso 6 Seleccione **Guardar**.
Sus ajustes de código de seguimiento se han guardado.

Modificación de los códigos de seguimiento

De forma predeterminada, los códigos de seguimiento se muestran en las casillas de texto. Si quiere mostrar las opciones de código de seguimiento en un menú desplegable, debe configurar una lista de opciones. Después de seleccionar **Menú desplegable** en el menú desplegable **Modo de introducción**, aparece el enlace **Editar lista**.

Antes de comenzar

Para editar sus códigos de seguimiento debe seleccionar **Usuarios** > **Códigos de seguimiento** y seleccionar el **Menú desplegable** para su **Modo de introducción**.

Procedimiento

Paso 1 Seleccione el enlace **Editar lista**.
Aparece el cuadro de diálogo **Editar lista de códigos de seguimiento**.

Paso 2 Configure los campos en el cuadro de diálogo **Editar lista de códigos de seguimiento**.

a) Seleccione **Mostrar sólo códigos activos** para mostrar únicamente los códigos de seguimiento activos al abrir este cuadro de diálogo. Elimine la selección de esta opción para mostrar todos los códigos de seguimiento. Tenga en cuenta que no puede seleccionar esta opción la primera vez que configure los códigos de seguimiento para cada **Modo de introducción**.

b) Seleccione **Ir al primer código de seguimiento vacío** para ir a la primera página con campos de código vacíos.
c) De forma predeterminada, está seleccionado **Activo.** Puede eliminar la selección de **Activo** para desactivar un código de seguimiento. Los códigos de seguimiento inactivos no aparecen en el menú desplegable del grupo de códigos de seguimiento. Marque **Activo** para activar un código de seguimiento inactivo.
d) Introduzca el nombre del elemento de menú en el cuadro de texto **Código**. Límite: 128 caracteres.
e) Seleccione el botón de opción **Predeterminado** para hacer que este elemento de menú sea la selección predeterminada para el menú desplegable.
f) Seleccione **Agregar 20 líneas más** para agregar 20 líneas de código de seguimiento configurables. Si tiene más de 20 líneas para mostrar, se agregan los enlaces de navegación (**Siguiente**, **Anterior** y números de página). Límite: 500 líneas (25 páginas).
g) Seleccione el botón de opción **Ordenar** para definir el método de ordenación **No ordenar**, **Orden ascendente**, **Orden descendente**, para los códigos de seguimiento. Tenga en cuenta que **Ordenar** solo funciona para la página actual.

Paso 3 Haga clic en **Actualizar** para guardar su configuración.
Sus ajustes se guardan y la página **Editar lista de códigos de seguimiento** se cierra.

Configuración de la integración de directorios

La integración de directorios permite que el sistema llene y sincronice su base de datos de Cisco WebEx Meetings Server con la base de datos de usuarios de Cisco Unified Communications Manager (CUCM) que se integra después con un directorio LDAP.

La integración de directorios simplifica la administración de los perfiles de usuario de las siguientes maneras:

- Importa los perfiles de usuario de CUCM a Cisco WebEx Meetings Server.
- Actualiza periódicamente la base de datos de Cisco WebEx Meetings Server con los atributos de usuarios nuevos o modificados de la base de datos de CUCM, que incluyen el nombre, el apellido y la dirección de correo electrónico de cada usuario. Cisco WebEx Meetings Server diferencia a los usuarios por su dirección de correo electrónico; si los usuarios tienen el mismo nombre y apellidos pero diferentes direcciones de correo electrónico, Cisco WebEx Meetings Server los trata como usuarios diferentes.
- Comprueba periódicamente si hay entradas de usuarios inactivos en la base de datos de CUCM y desactiva sus perfiles de usuario en la base de datos de Cisco WebEx Meetings Server.
- Permite al sistema utilizar la autenticación LDAP para autenticar los usuarios de integración de directorios de Cisco WebEx Meetings Server con el directorio externo.
- Es compatible con la integración LDAP totalmente cifrada si SLDAP (LDAP seguro) está habilitado en los servidores CUCM y LDAP.
- Todos los usuarios configurados en CUCM se sincronizan con Cisco WebEx Meetings Server y sus cuentas se activan. Si lo desea, puede desactivar cuentas una vez finalizada la sincronización. Todos los usuarios activos en CUCM se sincronizan con Cisco WebEx Meetings Server. Los usuarios inactivos no se importan a Cisco WebEx Meetings Server.

Antes de comenzar

Asegúrese de que se cumplen los siguientes requisitos previos antes de continuar con la integración de directorios:

- Le recomendamos que planifique la sincronización durante las horas de menor actividad o en fines de semana para minimizar el impacto en los usuarios.
- Asegúrese de que tiene una versión compatible de Cisco Unified Communications Manager (CUCM). Consulte los Requisitos del sistema de Cisco WebEx Meetings Server para obtener más información.
- Obtenga las credenciales de usuario administrativo de CUCM (necesarias para agregar un servidor CUCM para la integración de directorios).
- Debe configurar el servicio de directorio LDAP y AXL en CUCM para poder utilizar la función de integración de directorios. CUCM se necesita para importar usuarios al sistema Cisco WebEx Meetings Server. Utilice CUCM para realizar las siguientes acciones:
  - Habilitar el servicio Web Cisco AXL
  - Habilitar la sincronización de directorios de Cisco
  - Configurar la integración de LDAP
  - Configurar la autenticación LDAP

  Consulte Utilización de CUCM para configurar el servicio Web de AXL y la sincronización de directorios y Utilización de CUCM para configurar la autenticación y la integración LDAP. Consulte la documentación de CUCM para obtener información adicional.
- Asegúrese de que todos los usuarios que requieren privilegios de organizador están disponibles en CUCM. Los usuarios que no figuren en CUCM no podrán iniciar sesión ni organizar reuniones (todos los usuarios pueden entrar como invitado). Si es necesario, cree grupos de CUCM o filtros formados únicamente por los usuarios que desee importar de CUCM.

  Nota Si no utiliza grupos de CUCM, todos los usuarios de CUCM activos se importan a Cisco WebEx Meetings Server durante la primera sincronización de directorios. Los usuarios CUCM inactivos no se importan. Durante las posteriores sincronizaciones solamente se importan los usuarios nuevos y modificados activos. Debe desactivar las cuentas de usuario en Cisco WebEx Meetings Server a las que no desea otorgar acceso de organizador. Tenga en cuenta que una licencia de organizador se agota Cisco WebEx Meetings Server solamente cuando el usuario organiza realmente una reunión. Las cuentas que no organizan reuniones no agotan licencias. Consulte "Administración de licencias" en Configurar su sitio para obtener más información sobre el agotamiento de licencias.
- Los usuarios sin dirección de correo electrónico no se importan.
- Si los usuarios tienen varias cuentas que utilizan el mismo nombre y apellidos pero que tienen asignadas direcciones de correo electrónico diferentes en CUCM, cuando se importen estos usuarios Cisco WebEx Meetings Server dichas direcciones se tratan como usuarios distintos. Los usuarios de CUCM son únicos por nombre de usuario, por lo que un administrador puede crear varias cuentas de usuario con la misma dirección de correo electrónico. Sin embargo, las cuentas en Cisco WebEx Meeting Server son únicas por dirección de correo electrónico. Por lo tanto, si varias cuentas de usuario de CUCM tienen la misma

dirección de correo electrónico, el administrador de CUCM debe editar manualmente dichas cuentas de usuario para que las direcciones de correo electrónico sean únicas antes de importar dichas cuentas en Cisco WebEx Meetings Server.

- Cuando se activa la autenticación LDAP, Cisco WebEx Meetings Server utiliza el puerto 8443 para conectarse a CUCM cuando seleccione **Sincronizar ahora** o marque la opción **Siguiente sincronización** y especifique una fecha y hora.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración de Cisco WebEx Meetings Server.

Paso 2 (Opcional) Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Nota El modo de mantenimiento no es necesario para realizar la integración de directorio, pero una sincronización importante puede afectar al rendimiento del sistema. Puede poner el sistema en modo de mantenimiento para evitar que los usuarios utilicen el sistema durante una sincronización.

Paso 3 Seleccione **Usuarios** > **Integración de directorios**.

Paso 4 Introduzca la información del servidor CUCM si no lo ha hecho ya:

- Dirección IP o nombre de dominio cualificado completo (FQDN)
- Nombre de usuario
- Contraseña

El nombre de usuario y la contraseña pueden ser los del administrador de CUCM o los de AXL. Después de configurar la información de CUCM, la dirección IP o el FQDN del servidor CUCM aparecerán debajo del icono de CUCM.

Nota Si ya ha configurado los ajustes de CUCM, este paso no es necesario y puede ir al paso siguiente. Una vez que haya configurado la información de CUCM, cambiarla es un procedimiento complejo que puede provocar problemas de sincronización y no se recomienda.

Paso 5 Seleccione **Grupos de usuarios CUCM para el filtrado** para agregar únicamente los usuarios seleccionados en los grupos de usuarios CUCM a Cisco WebEx Meeting Server.

Paso 6 Sincronice el sistema de Cisco WebEx Meetings Server con su servicio de directorio LDAP. Puede realizar la sincronización de las siguientes maneras:

- Seleccione **Sincronizar ahora** para realizar una sincronización inmediatamente.

  Nota No puede cancelar la sincronización una vez comenzada.

- Seleccione la casilla de verificación **Siguiente sincronización**, introduzca una fecha y una hora y repita el mecanismo para planificar futuras sincronizaciones.

Si selecciona **Sincronizar ahora**, el sistema realiza una sincronización inmediatamente. El tiempo que este proceso tarda en efectuarse varía en función del número de usuarios que se estén sincronizando. Recibirá un correo electrónico cuando la sincronización finalice. Los demás administradores del sistema recibirán una notificación después de utilizar **Sincronizar ahora**. Si planifica una sincronización, se lleva a cabo en la fecha y la hora especificadas. Todos los administradores recibirán un correo electrónico una vez que se haya completado una sincronización planificada. Si desea impedir la sincronización futura, puede anular la selección de **Siguiente sincronización**.

Los siguientes atributos se asignan durante el proceso de sincronización:

Atributo de CUCM	Atributo de Cisco WebEx Meetings Server
Nombre	Nombre
Apellidos	Apellidos
ID de correo electrónico	Dirección de correo electrónico

Nota El nombre y los apellidos en Cisco WebEx Meetings Server son componentes del nombre completo que se muestra a los usuarios.

Los atributos asignados en Cisco WebEx Meetings Server no pueden ser actualizados por los usuarios finales.

Si la sincronización falla, aparece un mensaje de error en la página y se envía al administrador un correo electrónico con información detallada sobre el error. Seleccione **Ver registro** para ver una explicación detallada del error. Los registros proporcionados incluyen un informe de usuarios desactivados, un informe de usuarios fallidos y un resumen.

Después de haber realizado al menos una sincronización, aparece un resumen de la última sincronización en el que se indica si se ha completado o no, la hora y la fecha de finalización (utilizando la hora y la fecha configuradas en los ajustes de Información de la empresa), así como una lista de los cambios de usuarios que incluye lo siguiente:

- Añadidos: número de nuevos usuarios añadidos.
- Desactivados: número de usuarios que se han desactivado.

Paso 7 Seleccione **Guardar** si ha configurado o cambiado la planificación de sincronización o los ajustes de notificación a los administradores.

Paso 8 Seleccione la pestaña **Usuarios** y asegúrese de que los usuarios correctos se han sincronizado.

a) Seleccione **Usuarios remotos** en el menú desplegable para filtrar la lista de usuarios. Asegúrese de que los usuarios que quería sincronizar están presentes en la lista. Los usuarios remotos se importan a Cisco WebEx Meetings Server mediante una sincronización de directorios. Si primero se crea un usuario localmente y se sobrescribe con una sincronización de directorios, este usuario se convertirá en un usuario remoto, no en un usuario local.

b) Seleccione **Usuarios locales** para ver los usuarios que no se han incluido en la sincronización. Los usuarios locales los crea localmente un administrador de Cisco WebEx Meetings Server. Los usuarios locales se pueden agregar manualmente o se pueden importar mediante un archivo CSV.

Paso 9 Asegúrese de que las planificaciones de sincronizaciones de CUCM y Cisco WebEx Meetings Server sean secuenciales. Primero debe llevarse a cabo la sincronización de CUCM y la sincronización de Cisco WebEx Meetings Server debe producirse inmediatamente después.

Paso 10 (Opcional) Seleccione o deseleccione **Avisar a los administradores cuando la sincronización finalice** y luego seleccione **Guardar**. Esta opción está seleccionada de manera predeterminada y solamente informa a los administradores después de las sincronizaciones planificadas.

Paso 11 Seleccione **Activar autenticación LDAP**.

Nota Si el sistema está configurado para utilizar SSO, primero debe desactivar SSO. Consulte Desactivar SSO para obtener más información. Si el sistema no está configurado para utilizar SSO, utiliza la autenticación predeterminada hasta que active la autenticación LDAP.

Después de activar LDAP, se recomienda que los administradores utilicen el servidor Active Directory para la gestión de los usuarios, que incluye la adición, la desactivación y la modificación de los usuarios. Después de activar la autenticación LDAP, todos los participantes deben usar sus credenciales LDAP para iniciar sesión en el sitio de WebEx. Los administradores, sin embargo, siguen utilizando sus credenciales de Cisco WebEx Meetings Server para iniciar sesión en el sitio de administración.

Paso 12 Asegúrese de que los usuarios pueden iniciar sesión en el sistema con sus credenciales de dominio de AD.

Paso 13 Si pone el sistema en modo de mantenimiento, seleccione **Desactivar el modo de mantenimiento**.

Paso 14 (Opcional) Si ha realizado una sincronización, puede seleccionar **Avisar ahora** para informar por correo electrónico a los usuarios de que se han creado cuentas para ellos en el sistema Cisco WebEx Meetings Server o de que sus cuentas han cambiado. Opcionalmente puede seleccionar **Enviar notificaciones automáticamente**, que automáticamente envía un correo electrónico a los usuarios recién agregados después de cada sincronización. Después de cualquier cambio en los ajustes de autenticación (por ejemplo, activar LDAP), se envía un correo electrónico con los usuarios y contraseñas que se han cambiado a los usuarios afectados.
Cuando selecciona **Avisar ahora**

- Todos los usuarios reciben una única notificación en su ciclo de vida. Las posteriores sincronizaciones no causarán el envío de mensajes de correo electrónico adicionales.
- "Usuarios que necesitan notificación" indica todos los usuarios que están activos y que aún no han recibido ninguna notificación.
- A los usuarios inactivos y los usuarios locales no se les envía ninguna notificación.
- Al agregar un usuario local en Cisco WebEx Meetings Server se envía a este usuario un correo electrónico. Sin embargo, este usuario debe agregarse al servidor Active Directory CUCM para que pueda iniciar sesión en el sitio de WebEx.
- Solamente puede enviar notificaciones a los usuarios que se agregaron mediante la característica de sincronización.
- El envío de notificaciones por correo electrónico a los usuarios puede tardar unos minutos. Este retraso está provocado por varios factores que son externos a su sistema Cisco WebEx Meetings Server, incluyendo el servidor de correo, problemas de conectividad de red y receptores de correo basura en cuentas de correo electrónico individuales.

El sistema envía los siguientes mensajes de correo electrónico:

- El mensaje de correo electrónico de activación de AD se envía a todos los usuarios la primera vez que se importan en una sincronización. Los usuarios no reciben este correo electrónico en las posteriores sincronizaciones.
- El mensaje de correo electrónico de cambio de usuario o contraseña se envía a los usuarios que se han creado localmente en el sistema.

Consulte Acerca de las plantillas de correo electrónico para obtener información sobre la personalización de estas plantillas de correo electrónico.

Nota Si utiliza la integración de directorio con autenticación LDAP, los usuarios configurados en CUCM se sincronizan en Cisco WebEx Meeting Server como organizadores y utilizan sus credenciales LDAP para iniciar sesión en su sitio de WebEx. Sin embargo, si cambia el tipo de cuenta de un usuario importado de organizador a administrador, el usuario recibe un correo electrónico con un enlace de Crear contraseña. El usuario selecciona este enlace y especifica una nueva contraseña para Cisco WebEx Meetings Server. El usuario utilizará esta contraseña que acaba de crear para iniciar sesión en el sitio de Administración, pero seguirá utilizando las credenciales LDAP para iniciar sesión en su sitio WebEx.

Sincronizar grupos de usuarios

El administrador puede crear grupos de usuarios en CUCM. Por ejemplo, un administrador puede crear un grupo de usuarios formado por usuarios a los que se les permite utilizar Cisco WebEx Meetings Server. Desde CWMS, el administrador puede filtrar e importar determinados usuarios mediante la selección de determinados grupos de usuarios.

Antes de comenzar

Utilice CUCM para crear grupos de usuarios. Consulte la sección referente a la configuración de la administración de usuarios en la *Guía de administración de Cisco Unified Communications Manager*http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html para obtener más información.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración de Cisco WebEx Meetings Server.

Paso 2 Seleccione **Usuarios** > **Integración de directorios**.

Paso 3 Seleccione el enlace de **Grupos CUCM para filtrado**.

Paso 4 Seleccione los grupos de usuarios que se sincronizarán.

Nota Si no hay grupos seleccionados, la integración de directorios sincroniza todos los grupos de usuarios.

Paso 5 Seleccione **Guardar**.

Paso 6 Seleccione Sincronizar ahora para realizar la sincronización. El tiempo que este proceso tarda en efectuarse varía en función del número de usuarios que se estén sincronizando.

Nota El sistema recuerda qué grupos de usuarios se habían sincronizado anteriormente. Si no selecciona un grupo de usuarios que ya se había sincronizado, los usuarios del grupo de usuarios no seleccionado se desactivarán durante el proceso de sincronización.

Cuando finalice la sincronización, el sistema muestra el número de usuarios agregados y desactivados.

Paso 7 Seleccione **Ver registro** para obtener información resumida acerca de los usuarios que se han importado o desactivado durante el proceso de sincronización.

Utilización de CUCM para configurar el servicio Web de AXL y la sincronización de directorios

Utilice CUCM para configurar el servicio Web de AXL y la sincronización de directorios.

Antes de comenzar

Realice este procedimiento antes de utilizar la función de Integración de directorios. Consulte Configuración de la integración de directorios, en la página 144 para obtener más información.

Procedimiento

	Comando o Acción	Propósito
Paso 1	Inicie sesión con su cuenta de CUCM.	
Paso 2	Seleccione **Serviciabilidad de Cisco Unified** en el menú desplegable de la parte superior derecha y, a continuación, seleccione **Ir**.	
Paso 3	Seleccione **Herramientas** > **Activación del servicio**.	
Paso 4	Seleccione **Cisco AXL Web Service** y **Cisco DirSync** y luego seleccione **Guardar**.	

Qué hacer a continuación

Utilice CUCM para configurar la autenticación y la integración LDAP si aún no lo ha hecho. Consulte Utilización de CUCM para configurar la autenticación y la integración LDAP, en la página 150 para obtener más información.

Utilización de CUCM para configurar la autenticación y la integración LDAP

Utilice CUCM para configurar la autenticación y la integración LDAP.

Nota Si se configura CUCM para la integración de directorio, puede elegir entre utilizar SSO, LDAP o autenticación local.

Antes de comenzar

Realice este procedimiento antes de utilizar la función de Integración de directorios. Consulte Configuración de la integración de directorios para obtener más información.

Procedimiento

	Comando o Acción	Propósito
Paso 1	Inicie sesión con su cuenta de CUCM.	

	Comando o Acción	Propósito
Paso 2	Seleccione **Administración de Cisco Unified CM** en el menú desplegable de la parte superior derecha y, a continuación, seleccione **Ir**.	
Paso 3	Seleccione **Archivo** > **LDAP** > **Sistema LDAP**.	
Paso 4	Seleccione **Activar sincronización del servidor LDAP**, seleccione **Microsoft Active Directory** como tipo de servidor LDAP, seleccione **Nombre de cuenta sAM** como Atributo LDAP para el ID de usuario y seleccione **Guardar**.	
Paso 5	Seleccione la casilla de verificación correspondiente a su servidor LDAP y, a continuación, seleccione **Agregar nuevo**..	
Paso 6	Rellene los campos de la página Directorio LDAP y seleccione **Guardar**.	
Paso 7	En la página Autenticación LDAP, seleccione la casilla de verificación **Utilizar autenticación LDAP para usuarios finales**, rellene los campos de la página y, a continuación, seleccione **Guardar**.	

Qué hacer a continuación

Utilice CUCM para configurar el servicio Web de Cisco AXL y la sincronización de directorios de Cisco si aún no lo ha hecho. Consulte Utilización de CUCM para configurar el servicio Web de AXL y la sincronización de directorios para obtener más información.

Enviar correos electrónicos a usuarios

Utilice esta herramienta para enviar correos electrónicos a sus usuarios.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Usuarios** > **Enviar un correo electrónico a los usuarios**.

Paso 3 Especifique una dirección de correo electrónico de usuario de destino o un alias de correo electrónico en el campo **Para**.

Paso 4 Opcionalmente, especifique direcciones de correo electrónico en el campo **Cco**.

Paso 5 Especifique el asunto en el campo **Asunto**.

Paso 6 Especifique el mensaje en el campo **Mensaje**.

Paso 7 Seleccione **Enviar**.
Se envía el correo electrónico.

Nota Los usuarios pueden tardar unos minutos en recibir sus mensajes de correo electrónico. Este retraso puede estar provocado por varios factores que son externos a su sistema Cisco WebEx Meetings Server, incluyendo el servidor de correo, velocidad de la conexión de red y receptores de correo basura en cuentas de correo electrónico concretas.

CAPÍTULO 13

Configurar su sitio

En este módulo se describe cómo usar las páginas de administrador para configurar su sistema.

- Configuración de las propiedades del sistema, página 153
- Configuración de los ajustes generales, página 161
- Configuración de servidores, página 163
- Configuración de los ajustes SNMP, página 169
- Administración de licencias, página 176

Configuración de las propiedades del sistema

Configure las propiedades del sistema seleccionando Sistema y Ver más en la sección Sistema.

Cambiar la configuración de su máquina virtual

Utilice esta función para cambiar la configuración de su máquina virtual.

Nota No utilice VMware vCenter para editar la configuración de su máquina virtual.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Sistema** y seleccione **Ver más** en la sección Sistema.

Paso 3 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 4 Para modificar los ajustes de una máquina virtual, seleccione el enlace con el nombre de la máquina virtual en la sección del sistema principal o del sistema de alta disponibilidad.

Paso 5 Puede modificar los siguientes ajustes de la máquina virtual:

- Nombre de dominio cualificado completo: el FQDN de su sistema.

- Máquina virtual: la dirección IP de su máquina virtual.
- Servidor DNS primario
- Servidor DNS secundario
- Máscara de subred/ Prefijo
- Puerta de enlace

Nota Puede configurar su sistema con los ajustes de la máquina virtual IPv4 o IPv6. Durante el despliegue, solo podrá configurar los ajustes de IPv4, pero podrá actualizar su máquina virtual a IPv6 en esta página.

Paso 6 Seleccione **Guardar**.
Los cambios se guardan y el equipo virtual se reinicia.

Paso 7 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Qué hacer a continuación

Si realiza algún cambio en sus máquinas virtuales, debe obtener nuevos certificados para cada máquina virtual en su sistema, a no ser que esté utilizando certificados comodines para sistemas en el mismo dominio. Para obtener más información, consulte Administración de certificados, en la página 226.

Configuración de un sistema de alta disponibilidad

Un sistema de alta disponibilidad es un sistema redundante que proporciona una copia de seguridad en el caso de una anomalía del sistema principal.

Nota Active el modo de mantenimiento antes de agregar o eliminar un sistema de alta disponibilidad. Cuando planifique una ventana de mantenimiento para realizar esta tarea, tenga en cuenta que el sistema lleva a cabo un rearranque del mismo cuando desactive el modo de mantenimiento. Un rearranque del sistema tarda aproximadamente 30 minutos, en función del tamaño del sistema.

Agregar un sistema de alta disponibilidad

Nota La mayoría de las funciones de su sistema de alta disponibilidad están prohibidas. Por ejemplo, no tiene acceso a la actualización, configuración de SNMP, acceso de almacenamiento y servidores de correo electrónico en el sistema de alta disponibilidad. Puede ver las propiedades del sistema, pero está prohibida su modificación.

Nota Complete el siguiente procedimiento en el sistema principal.

Antes de comenzar

- Instale Cisco WebEx en una segunda máquina virtual a partir del archivo OVA para ser usada como su sistema de alta disponibilidad.

  Nota Su sistema de alta disponibilidad debe tener el mismo tamaño que su sistema principal.

- Su sistema de alta disponibilidad debe configurarse con la misma ruta y OVA que su sistema principal. Si las versiones de su sistema principal y del sistema HA no coinciden, se le pedirá que actualice al nivel de versión más alto.
- Copie el nombre de dominio cualificado completo (FQDN) de su máquina virtual de alta disponibilidad. Debe conocer el FQDN para agregar su sistema de alta disponibilidad.
- Compruebe que todas las máquinas virtuales funcionan correctamente. Determine el estado de la máquina virtual visualizando el monitor del sistema como se describe en Acerca de su escritorio, en la página 115.
- Le recomendamos que tome una instantánea de las máquinas virtuales de alta disponibilidad antes de realizar este procedimiento. Repita el procedimiento desde la instantánea en caso de error.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento**.

Paso 3 En el sistema principal, en la sección Sistema, seleccione el enlace **Ver más**.

Paso 4 Seleccione **Agregar sistema de alta disponibilidad**.

Paso 5 Siga las instrucciones en la página **Propiedades del sistema** para agregar este sistema de alta disponibilidad.

Paso 6 Introduzca el FQDN de la máquina virtual del sitio de administración del sistema de alta disponibilidad y seleccione **Continuar**.
Validaremos el estado de preparación del sistema principal y del sistema HA para este procedimiento de añadir HA.

- Si ambos sistemas están listos, entonces verá un botón verde de **Agregar**. No lo seleccione hasta que ponga el sistema en modo de mantenimiento.
- Si alguno de los sistemas no está preparado verá un mensaje de error. Solucione el error e intente de nuevo el procedimiento de adición de alta disponibilidad.

Paso 7 Seleccione **Agregar**.

Nota Si el error "Código de error: Database-64" aparece, repita este procedimiento usando la instantánea de las máquinas virtuales de alta disponibilidad.

Su sistema de alta disponibilidad se añade y se configura automáticamente para servir como sistema de reserva en caso de producirse un fallo en el sistema principal.

Paso 8 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema rearranca después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Eliminar un sistema de alta disponibilidad

Antes de comenzar

Debe tener un sistema secundario actualmente configurado como su sistema de alta disponibilidad.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento**.

Paso 3 En la sección Sistema, seleccione el enlace **Ver más**.

Paso 4 Seleccione **Eliminar sistema de alta disponibilidad**.
Aparece la página **Eliminar sistema de alta disponibilidad** mostrando el nombre de dominio cualificado completo (FQDN) de su sistema de alta disponibilidad.

Paso 5 Seleccione **Continuar**.

Nota Después de suprimir un sistema de alta disponibilidad, no puede agregar el mismo sistema de alta disponibilidad a su sitio. Para volver a configurar la alta disponibilidad, debe empezar por volver a desplegar un sistema de alta disponibilidad desde el archivo OVA. Consulte Agregar un sistema de alta disponibilidad, en la página 75 para obtener más información.

Se ha eliminado su sistema de alta disponibilidad

Paso 6 Abra VMware vCenter y elimine el sistema de alta disponibilidad utilizando el comando **Delete from Disk**.

Paso 7 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema rearranca después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Comportamiento del sistema después de un fallo de componente

Componentes y plataformas multimedia específico cuando ejecute en una máquina virtual vaya abajo, estos componentes están reinicia de forma automática por el sistema. Las reuniones afectadas pasan a otros recursos disponibles en la misma máquina virtual, u otra distinta, en el sistema (para sistemas que no sean independientes de 50 usuarios).

Sistemas de alta disponibilidad

En sistemas de alta disponibilidad (HA), Cisco WebEx Meetings Server se recuperará para estos componentes cuando exista un fallo de componente único:

- Un único servicio en una máquina virtual.
- Una máquina virtual.
- Un único servidor físico o servidor blade, que aloja hasta dos máquinas virtuales (siempre que el diseño de la máquina virtual diseño cumpla las especificaciones enumeradas en los *Requisitos del sistema de Cisco WebEx Meetings Server* y la *Guía de planificación de Cisco WebEx Meetings Server*).
- Un único enlace de red, suponiendo que la red se proporciona en una forma totalmente redundante.
- Un nodo único de Cisco Unified Communications Manager (CUCM), siempre y cuando CUCM esté suministrado de forma redundante.

Tras el fallo de componente único, el sistema del servidor Cisco WebEx Meetings se comporta como se indica a continuación:

- Durante un período de hasta tres minutos, el uso compartido de aplicaciones, la conexión de voz de audio mediante el ordenador y el vídeo pueden interrumpirse. Cisco WebEx Meetings Server concede tres minutos para detectar el error y para volver a conectar a todos los clientes de las reuniones afectadas automáticamente. Los usuarios no deberían tener que cerrar sus clientes de reuniones y volver a unirse a su reunión.
- Algunos errores pueden provocar que se pierdan las conexiones de audio de las teleconferencias. Si esto ocurre, los usuarios tendrán que volver a conectarse manualmente. La reconexión debería poder realizarse correctamente en un margen de dos minutos.
- No todos los clientes y reuniones pueden verse afectados por algunos errores. Normalmente las conexiones de reunión están redistribuidas en varias máquinas virtuales y hosts.

Información adicional para un sistema de 2000 usuarios

Un sistema de 2000 usuarios proporciona algunas funcionalidades de alta disponibilidad sin la adición de un sistema HA. Para un sistema de 2000 usuarios sin alta disponibilidad:

- Su sistema sigue funcionando después de la pérdida de una máquina virtual multimedia o una máquina Web, pero la capacidad del sistema se verá reducida.
- La pérdida de la máquina virtual de administración hace que no se pueda utilizar el sistema.

Para un sistema de 2000 usuarios con alta disponibilidad:

- La pérdida de una máquina virtual (administración, multimedia o web) no afecta a su sistema. Su sistema seguirá funcionando con plena capacidad incluso con la pérdida de un servidor físico que esté alojando las máquinas virtuales primarias (administración y multimedia, o Web y multimedia) o las máquinas virtuales HA (administración y multimedia o Web).
- Cuando se reinicia la máquina virtual que ha fallado, se vuelve a unir al sistema y el sistema vuelve a su estado de funcionamiento normal.
- Cuando falla una máquina virtual multimedia, las reuniones organizadas en ese servidor se interrumpen brevemente, pero la reunión se recupera mediante la migración a una máquina virtual multimedia alternativa. Los usuarios deben volver a unirse manualmente a las sesiones de vídeo y audio de escritorio.
- Cuando una máquina virtual web falla, también fallan las sesiones web existentes organizadas en dicha máquina virtual. Los usuarios deben iniciar sesión en el sitio de Cisco WebEx y establecer una nueva sesión del explorador que se alojará en una máquina virtual Web alternativa.

- Cuando falla una máquina virtual de administración, también falla cualquier sesión de administrador existente. Los administradores deben iniciar sesión de nuevo en el sitio de administración y establecer una nueva sesión del explorador que se alojará en la máquina virtual de administración alternativa. Es posible que también se interrumpa brevemente cualquier sesión de reunión de usuario final o de administrador.

Cambiar su dirección IP virtual

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Sistema** y seleccione **Ver más** en la sección Sistema.

Paso 4 En la sección Dirección IP virtual, seleccione un enlace en la columna Tipo.

Ejemplo:
Seleccione **Privada** para la dirección IP virtual privada.

Paso 5 Introduzca su nueva dirección IP virtual en el cuadro de diálogo Dirección Ipv4 VIP.

Paso 6 Seleccione **Guardar**.

Paso 7 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema rearranca después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Nota El sistema tarda aproximadamente 30 minutos en realizar el rearranque del sistema. Cuando planifique una ventana de mantenimiento para el mantenimiento del sistema que incluya esta tarea, no olvide tener en cuenta el período de tiempo del rearranque del sistema cuando especifique la duración de la ventana de mantenimiento planificada. Consulte Planificación de una ventana de mantenimiento, en la página 123 para obtener más información.

Configuración del acceso público

El acceso público permite a las personas externas a la red organizar o asistir a reuniones en línea a través de Internet o de dispositivos móviles. La desactivación del acceso público eliminará la configuración de la dirección IP virtual pública de la URL del sitio de WebEx y terminará el acceso externo al sitio.

Agregar el acceso público a su sistema

Antes de comenzar

Para activar el acceso público, primero debe configurar una máquina virtual de proxy inverso de Internet para que sirva como su sistema de acceso público.

Lance VMware vCenter y realice lo siguiente:

- Haga una copia de seguridad de sus máquinas virtuales utilizando VMware Data Recovery (vSphere 5.0) o VMware vSphere Data Protection (vSphere 5.1). Esto le permite revertir los cambios si es necesario.

Consulte Creación de una copia de seguridad por medio de VMware vCenter, en la página 4 para obtener más información.

- Despliegue una máquina virtual de proxy inverso de Internet utilizando el mismo archivo OVA que ha usado para desplegar su máquina virtual de administrador. Su máquina virtual de proxy inverso de Internet debe encontrarse en la misma subred que la dirección IP virtual pública. Consulte Agregar acceso público, en la página 34 para obtener más información.

Nota Si tiene un sistema de alta disponibilidad, deberá desplegar una máquina virtual de proxy inverso de Internet también para su sistema de alta disponibilidad.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Sistema** y después seleccione el enlace **Ver más** en la sección Sistema.

Paso 4 Seleccione **Agregar acceso público**.

Paso 5 Introduzca su máquina virtual de proxy inverso de Internet el campo **FDQN**.

Nota Hay dos campos de nombre de dominio cualificado completo (FQDN) si su sistema está configurado para alta disponibilidad. Introduzca su FDQN de alta disponibilidad en el segundo campo.

Paso 6 Seleccione **Detectar máquinas virtuales**.

- Si su sistema no está configurado para alta disponibilidad, aparecerá una tabla mostrando la máquina virtual de proxy inverso de Internet.
- Si su sistema está configurado para alta disponibilidad, aparecerá una tabla que mostrará el sistema principal de la máquina virtual de proxy inverso de Internet y la máquina virtual de proxy inverso de Internet.

Si su sistema tiene una actualización que es incompatible con la versión OVA que utilizó para crear la máquina virtual de proxy inverso de Internet, recibirá un mensaje de error y no podrá continuar hasta que haya vuelto a desplegar la máquina virtual de proxy inverso de Internet utilizando un archivo OVA compatible con las actualizaciones en su sistema principal.

Paso 7 Seleccione **Continuar**.

Paso 8 Introduzca la dirección IP de la misma subred que utilizó para configurar su máquina virtual de proxy inverso de Internet en el campo **Dirección IPv4 virtual pública (VIP)** y seleccione **Guardar**.
Su sistema se actualiza y el acceso público se configura. No olvide mantener abierta la ventana de su explorador durante todo el proceso.

Si su sistema principal necesita actualizaciones secundarias compatibles con la versión OVA que utilizó para crear la máquina virtual de proxy inverso de Internet, éstas se aplican automáticamente a su máquina virtual de proxy inverso de Internet.

Paso 9 Si su sistema requiere actualizaciones secundarias, se le solicitará que seleccione **Reiniciar** después de que las actualizaciones se completen. Si no se necesita ninguna actualización, continúe al siguiente paso.

Después del reinicio de su sistema, recibirá un mensaje de confirmación indicando que ha agregado el acceso público.

Paso 10 Compruebe su configuración. Si está satisfecho, puede eliminar la copia de seguridad de la máquina virtual que ha configurado antes de realizar este procedimiento.

Paso 11 Seleccione **Hecho**.

Paso 12 Compruebe que su certificado de seguridad sigue siendo válido. Este procedimiento puede afectar a los certificados, ya que cambia sus máquinas virtuales. Si es necesario, su sistema proporciona un certificado autofirmado para mantener su sistema en funcionamiento hasta que pueda configurar sus certificados. Consulte Administración de certificados, en la página 226 para obtener más información.

Paso 13 Realice cualquier cambio necesario en sus servidores DNS.

Paso 14 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Eliminar el acceso público

Antes de comenzar

Haga una copia de seguridad de sus máquinas virtuales utilizando VMware Data Recovery (vSphere 5.0) o VMware vSphere Data Protection (vSphere 5.1). Esto le permite revertir los cambios si es necesario. Consulte Creación de una copia de seguridad por medio de VMware vCenter, en la página 4 para obtener más información. Asegúrese de que enciende su equipos virtuales después de que se haya completado la copia de seguridad.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Sistema** y después seleccione el enlace **Ver más** en la sección Sistema.

Paso 4 Seleccione el sitio deseado, seleccione **Eliminar acceso público** y después **Continuar**.
El acceso público se elimina del sitio.

Nota Después de suprimir el acceso público de su sitio, no puede agregar la misma máquina virtual de proxy inverso de Internet a ese sitio. Para volver a configurar el acceso público, debe empezar por desplegar una máquina virtual de proxy inverso de Internet desde el archivo OVA. Consulte Agregar el acceso público a su sistema, en la página 158 para obtener más información.

Paso 5 Seleccione **Hecho**.

Paso 6 Abra VMware vCenter, apague y elimine la máquina de proxy inverso de Internet (y la máquina de proxy inverso de Internet de alta disponibilidad, si está desplegada) desde su sistema.

Paso 7 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Expandir el tamaño del sistema

Antes de comenzar

Antes de realizar una expansión del sistema, consulte Ampliar su sistema a un tamaño de sistema superior, que describe todos los pasos de requisitos previos que debe dar antes de utilizar esta función y cómo expandir el sistema utilizando el despliegue automático o manual.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Sistema** y haga clic en el enlace **Ver más** en la sección Sistema.

Paso 4 Seleccione **Expandir tamaño del sistema**.

Paso 5 Seleccione **Continuar**.
El sistema comprueba la conectividad con las máquinas virtuales. Si existen problemas de conectividad con una o más máquinas virtuales, deberá corregir los problemas antes de seguir. Si no hay problemas de conectividad, el sistema crea una copia de seguridad automática. Después de que la copia de seguridad se haya completado, se le notificará que puede continuar con la ampliación.

Paso 6 Despliegue el archivo OVA con uno de los siguientes métodos:

- Ampliación del sistema usando el despliegue automático
- Ampliación del sistema usando el despliegue manual

El sistema le notifica una vez que se complete la ampliación.

Paso 7 Seleccione **Reiniciar**.

Paso 8 Inicie sesión en el sitio de administración.

Paso 9 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Configuración de los ajustes generales

Para acceder a sus ajustes generales, seleccione **Sistema** y el enlace **Ver más** en Configuración > Ajustes generales. Los ajustes generales incluyen lo siguiente:

- Ajustes del sitio: utilice esta función para configurar o cambiar su URL del sitio. Esta función también muestra la dirección IP virtual privada del sitio y la dirección IP virtual pública del sitio.
- Ajustes de administración: utilice esta función para configurar o cambiar su URL del sitio de administración. Esta función también muestra la dirección IP virtual privada del sitio de administración.

Cambiar la configuración de su sitio

Utilice esta función para cambiar la URL de su sitio. La configuración de la URL del sitio original se configura durante el despliegue. Para obtener más información sobre la configuración de la URL del sitio y las convenciones sobre nombres, consulte URL del sitio de WebEx y URL de administración de WebEx, en la página 37.

Antes de comenzar

Asegúrese de conservar la URL del sitio original en el servidor DNS. Redirija su URL del sitio original a la URL del sitio actualizado. Si los usuarios intentan compartir la URL original y no la ha redirigido al URL nuevo, no podrán organizar ni unirse a reuniones, ni tampoco iniciar sesión desde páginas Web, herramientas de productividad y aplicaciones móviles.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Sistema** > **Configuración** > **Configuración general** > **Ver más**.

Paso 4 En la sección Configuración, seleccione **Editar**.

Paso 5 Introduzca la nueva URL del sitio en el cuadro de diálogo y seleccione **Guardar**.

Paso 6 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Qué hacer a continuación

Actualice el certificado de su sitio para garantizar un acceso seguro. Consulte Administración de certificados, en la página 226 para obtener más información.

Cambiar la configuración de administración

La URL del sitio de administración original se configura durante el despliegue. Para obtener más información sobre la configuración del sitio de administración y las convenciones sobre nombres, consulte URL del sitio de WebEx y URL de administración de WebEx, en la página 37.

Antes de comenzar

Asegúrese de conservar la URL del sitio de administración original en el servidor DNS. Redirija su URL del sitio de administración original al URL del sitio de administración actualizado. Si los usuarios intentan compartir la URL original y no la ha redirigido al URL nuevo, no podrán organizar ni unirse a reuniones, ni tampoco iniciar sesión desde páginas Web, herramientas de productividad y aplicaciones móviles.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Sistema** > **Configuración** > **Configuración general** > **Ver más**.
Aparece la página **Configuración general**.

Paso 4 En la sección de Configuración de administración, seleccione **Editar**.

Paso 5 Introduzca la URL del nuevo sitio de administración en el cuadro de diálogo y seleccione **Guardar**.

Paso 6 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Qué hacer a continuación

Actualice el certificado de su sitio para garantizar un acceso seguro. Consulte Administración de certificados, en la página 226 para obtener más información.

Configuración de servidores

Utilice esta función para configurar sus servidores:

- Servidor SMTP: el servidor SMTP gestiona el envío de correo electrónico desde el servidor de reuniones de Cisco WebEx hasta su destino.
- Servidor de almacenamiento: el servidor NFS es el servidor de almacenamiento en el que se almacenan todas las grabaciones de reuniones.

Configurar un servidor de correo

Configure un servidor de correo para habilitar su sistema para enviar invitaciones de reuniones y otras comunicaciones a los usuarios.

Nota Es muy importante que su servidor de correo siempre esté operativo. El correo electrónico es el principal método de comunicación con sus usuarios e incluye notificaciones de grabaciones, cambios en la información de la reunión, estado de la cuenta y muchos otros avisos importantes.

Nota Para cambiar estas propiedades no es necesario activar el modo de mantenimiento.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Sistema** y seleccione **Ver más** en la sección Servidores.

Paso 3 Seleccione **Editar** en la sección Servidor de correo.

Paso 4 Introduzca el nombre de host de su servidor de correo y puede seleccionar opcionalmente la casilla de verificación **TLS activado**.

Paso 5 Introduzca el número de puerto del servidor de correo electrónico y opcionalmente seleccione la casilla de verificación **Autenticación de servidor activada**.

Paso 6 Seleccione **Continuar**.

Configuración de un servidor SMTP

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Sistema**.

Paso 3 En Servidores, seleccione el enlace **Ver más**.

Paso 4 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 5 En Servidor SMTP, seleccione el enlace **Editar**.

Paso 6 Rellene los campos del servidor SMTP:

- Nombre de host: el nombre de host de su servidor SMTP.
- Puerto: el número de puerto para su servidor SMTP.
- Nombre de usuario: el nombre de usuario para el cliente de correo electrónico.
- Contraseña: contraseña para el usuario.

Paso 7 Puede seleccionar las casillas de verificación **TLS activado** y **Autenticación de servidor activada**.

Paso 8 Seleccione **Guardar**.

Paso 9 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Configuración de un servidor de almacenamiento

Utilice el servidor de almacenamiento para hacer una copia de seguridad del sistema y almacenar las grabaciones de reunión. Durante una recuperación de desastres (consulte Utilizar la función de recuperación ante desastres), estas copias de seguridad se pueden utilizar para restaurar el sistema. (El método de almacenamiento actualmente

admitido es Network File System (NFS). Asegúrese de que se puede acceder al servidor de almacenamiento desde todas las máquinas virtuales internas. (Existe también la función VMware Data Recovery proporcionada por VMware para realizar la copia de seguridad de las máquinas virtuales. Consulte http://www.vmware.com/pdf/vdr_11_admin.pdf para obtener más información.)

Nota No es necesario que conecte el servidor de almacenamiento a las máquinas virtuales externas como, por ejemplo, servidores de proxy inverso de Internet (IRP).

Su servidor de almacenamiento hace una copia de seguridad de lo siguiente diariamente:

- Determinados ajustes del sistema
- Información de usuario
- Información de la reunión
- Certificados SSL cargados en el sistema
- URL del sitio

Las copias de seguridad se realizan cada día y están establecidas inicialmente para las 04:20 h, hora local. Cisco WebEx Meetings Server se ejecuta durante el proceso de copia de seguridad sin interrumpir las reuniones, grabaciones u otras funciones. El sistema no quita la copia de seguridad anterior hasta que se completa la siguiente copia de seguridad diaria para garantizar que está disponible una copia de seguridad.

El sistema tarda aproximadamente unos cinco minutos en hacer una copia de seguridad de 500 MB. El tiempo que se tarde en hacer una copia de seguridad del sistema depende de la velocidad de almacenamiento, la velocidad de NFS y otros factores. Una base de datos de 70 GB tarda aproximadamente una hora en hacer una copia de seguridad y 10 minutos en transferirse al NFS. El tiempo de transferencia es 12 MB/segundo para poder permitir otras comunicaciones de red y garantizar el funcionamiento continuo del producto.

Antes de comenzar

Asegúrese de configurar sus privilegios de acceso Unix para que su sistema pueda almacenar contenido generado por el usuario y copias de seguridad del sistema.

En los sistemas de almacenamiento basados en Linux, esto depende de la configuración de los permisos de lectura/escritura de los usuarios anónimos sobre un directorio específico que se va a utilizar para NFS (sistema de archivos de red, Network File System por sus siglas en inglés).

En los sistemas de almacenamiento basados en Windows, esto depende del ajuste **Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos**. Además, debe proporcionar al grupo de usuarios Todos permisos de lectura y escritura sobre el NFS.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Sistema**.

Paso 4 En el apartado Servidores, seleccione **Ver más**.

Si hay un servidor de almacenamiento en su sistema, se mostrará en esta página. Si no hay un servidor de almacenamiento en su sistema, se le ofrecerá la opción de configurar uno.

Paso 5 En el apartado Servidor de almacenamiento, seleccione **Agregar ahora un servidor de almacenamiento**.

Paso 6 Introduzca el punto de montaje NFS y seleccione **Guardar**.
El sistema confirma su punto de montaje NFS.

Paso 7 Seleccione **Continuar**.
Recibe un mensaje de confirmación que le indicará que su servidor de almacenamiento se ha agregado.

Paso 8 Seleccione **Hecho**.

Paso 9 Opcionalmente, puede cambiar la hora predeterminada para la copia de seguridad diaria. En la sección de Servidor de almacenamiento, haga clic en Hora programada para copia de seguridad del sistema **y** seleccione otra hora en el menú desplegable. A continuación, seleccione **Guardar**.
La copia de seguridad diaria se realiza en la hora seleccionada, en lugar de la hora configurada inicialmente de las 4:20 a.m. hora local.

Paso 10 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Qué hacer a continuación

Configure su sistema para utilizar el servidor de almacenamiento para lo siguiente:

- Grabaciones de reuniones
- Recuperación ante desastres. Consulte Utilizar la función de recuperación ante desastres, en la página 166 para obtener más información.

Para garantizar el correcto funcionamiento del servidor de almacenamiento, asegúrese de que:

- Se puede acceder al servidor de almacenamiento desde fuera de Cisco WebEx Meetings Server.
- El servidor de almacenamiento está encendido.
- Hay conectividad de red a su servidor de almacenamiento.
- El montaje/acceso es posible desde una máquina que no sea de Cisco WebEx Meetings Server.
- El servidor de almacenamiento no está lleno.

Nota Si un usuario sin darse cuenta elimina una grabación de la página **Grabaciones de reunión de Cisco WebEx** pero la grabación está guardada en el servidor de almacenamiento NFS (el sistema de archivos de red), póngase en contacto con el Centro de asistencia técnica (TAC) de Cisco para obtener ayuda acerca de la recuperación de la grabación.

Utilizar la función de recuperación ante desastres

Utilice las características de recuperación ante desastres para recuperar su despliegue después de un fallo del sistema o de algún otro desastre. Un desastre podría ser un bloqueo de la red, un fallo del servidor, una

desconexión del centro de datos u otros eventos que hagan que su sistema no pueda utilizarse. Hay dos tipos de recuperación ante desastres:

- Recuperación ante desastres de un centro de datos: si tiene un único centro de datos y el sistema no está disponible, puede volver a instalar el sistema en el mismo centro de datos y restaurarlo al mismo estado.
- Recuperación de desastres de dos centros de datos: si tiene dos centros de datos y el sistema no está disponible en el primer centro de datos, puede acceder al sistema del segundo centro de datos y restaurar el primer centro de datos al mismo estado.

Una vez haya configurado un servidor de almacenamiento, se realiza una copia de seguridad del sistema a diario. En el escritorio aparece un aviso de copia de seguridad del sistema que incluye información sobre la copia de seguridad más reciente. Solo se conserva almacenada una copia de seguridad del sistema. Una vez haya realizado una actualización, se mantiene la copia de seguridad de la versión anterior de Cisco WebEx Meetings Server. Le recomendamos que no utilice el mismo directorio de almacenamiento para distintas instalaciones de Cisco WebEx Meetings Server.

Tenga en cuenta que la recuperación ante desastres:

- Dura más de 30 minutos.
- Sobrescribe su configuración con la configuración de la copia de seguridad más reciente.
- Necesita que realice pasos adicionales para restaurar el servicio a sus usuarios (detallados en *Qué hacer a continuación* en este capítulo).

Este procedimiento realiza una copia de seguridad de determinados ajustes del sistema, información de usuario, información de la reunión, certificados SSL cargados en el sistema y la URL del sitio. El proceso de copia de seguridad no almacena las credenciales de VMware ni la información de la dirección IP para cada una de las máquinas virtuales. (Existe también la función VMware Data Recovery proporcionada por VMware para realizar la copia de seguridad de las máquinas virtuales. Consulte http://www.vmware.com/pdf/vdr_11_admin.pdf para obtener más información.) En caso de que realice una recuperación ante desastres, debe volver a aplicar manualmente determinados ajustes, incluidos los siguientes:

- Conexiones a determinados componentes externos, por ejemplo Cisco Unified Communications Manager (CUCM)
- Certificados SSL (en caso de que los nombres de host del sistema de recuperación ante desastres difieran de los que había en el sistema original)
- En los despliegues con un solo centro de datos, opcionalmente puede utilizar la misma dirección IP o el mismo nombre de host. En los despliegues con dos centros de datos, opcionalmente puede utilizar la misma dirección IP o el mismo nombre de host para el sistema principal.

Realice este procedimiento después de que se produzca un desastre y no pueda usar su sistema.

Antes de comenzar

Para realizar los procedimientos de recuperación ante desastres:

- Debe haberse configurado un servidor de almacenamiento. Si no tiene configurado un servidor de almacenamiento, la opción **Recuperación ante desastres** no estará disponible ni se crearán copias de seguridad. Consulte Configuración de un servidor de almacenamiento para obtener más información.
- Debe tener acceso a un sistema desde el que pueda restaurar su despliegue. Consulte la información que aparece a continuación sobre la recuperación ante desastres de un centro de datos y de dos centros de datos.

- Su sistema de recuperación debe tener el mismo tamaño de despliegue y la misma versión de software que el sistema original.

  Para un sistema de alta disponibilidad, primero debe configurar la recuperación de desastres y después configurar la alta disponibilidad en dicho sistema. Si tiene un sistema de alta disponibilidad que requiere la recuperación ante un desastre, primero debe restaurar el sistema y después configurar la alta disponibilidad en el sistema restaurado. Para obtener más información sobre la alta disponibilidad, consulte Agregar un sistema de alta disponibilidad.

Procedimiento

Paso 1 Inicie sesión en el sitio de Administración en un sistema desde donde pueda restaurar su despliegue.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Sistema** > **Servidores** > **Añadir servidor de almacenamiento**.

Paso 4 Introduzca el nombre de su servidor de almacenamiento en el campo **Punto de montaje de NFS** y seleccione **Guardar**.

Ejemplo:
192.168.10.10:/CWMS/backup.

Paso 5 Seleccione **Continuar** para proceder con la recuperación ante desastres.
Si el tamaño de despliegue del sistema de recuperación y la versión de software coinciden con su sistema original, puede proceder con la recuperación ante desastres. Si el sistema tiene un tamaño de despliegue o una versión de software diferentes, no puede continuar hasta que vuelva a desplegar la aplicación en el sistema de recuperación para que el tamaño del despliegue y la versión de software coincidan con los del despliegue original. No es necesario que la dirección IP o el nombre de host coincida con los del despliegue original.

Paso 6 Seleccione una de las siguientes acciones para continuar:

- **Cancelar**: hacer una copia de seguridad de su sistema preexistente antes de añadir un servidor de almacenamiento. Después de hacer una copia de seguridad del sistema regresará a esta página y podrá seleccionar **Continuar** para proseguir.
- **Continuar**: sobrescribir su sistema preexistente y continuar con la recuperación ante desastres.

El proceso de recuperación ante desastres se inicia. Si cierra el explorador, no podrá volver a iniciar sesión en el sistema hasta que el proceso se haya completado.

Paso 7 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Qué hacer a continuación

Debe realizar los siguientes procedimientos para restaurar el servicio para sus usuarios:

- Vuelva a configurar los ajustes de teleconferencia. Consulte "Configuración de CUCM" en la Guía de planificación para obtener más información.
- Vuelva a configurar los ajustes de SSO. Consulte Configurar los ajustes de autenticación única (SSO) para obtener más información.

- Vuelva a configurar los ajustes de SNMP. Consulte Configuración de los ajustes SNMP para obtener más información.
- Vuelva a configurar sus certificados. Puede que tenga que volver a cargar sus certificados SSL si no coinciden con los certificados SSL que están configurados en el sistema de recuperación. Consulte Restauración de un certificado SSL para obtener más información.
- El sistema recuperado está inicialmente configurado para el modo sin licencias que caducará a los 180 días. Realoje las licencias del sistema anterior en el sistema recuperado. Consulte Realojamiento de licencias después de una actualización de software o la expansión del sistema y Acerca de las licencias para obtener más información.
- Configure sus ajustes DNS para que la URL de su sitio dirija a la dirección VIP actual. Su dirección VIP en el sistema restaurado puede ser distinta a la que tenía en su sistema original. Debe completar su configuración DNS para usuarios finales para que puedan usar sus enlaces originales para iniciar sesión o unirse a reuniones en el sistema restaurado. Consulte Cambiar su dirección IP virtual para obtener más información.
- Si tiene configurado su sistema para la integración de directorios y ha activado la autenticación LDAP, verifique que sus credenciales de CUCM funcionan. Después de que el sistema deje de estar en modo de mantenimiento y de que el sistema haya acabado de reiniciarse, inicie sesión en el sitio de administración, seleccione **Usuarios** > **Integración de directorios**, y a continuación seleccione **Guardar**. Si las credenciales de CUCM no son correctas, recibirá el mensaje de error **Credenciales no válidas**. Si recibe este mensaje de error, escriba las credenciales correctas y seleccione **Guardar** de nuevo. Consulte Configuración de la integración de directorios para obtener más información.

Configuración de los ajustes SNMP

Puede configurar los ajustes SNMP siguientes:

- Cadenas de comunidad: las cadenas de comunidad SNMP autentican el acceso a objetos MIB y funcionan como una contraseña incorporada.
- Usuarios USM: configure la seguridad basada en el usuario (USM) para proporcionar un nivel de seguridad de mensajes adicional. Seleccione una configuración USM existente para editarla o agregue configuraciones USM adicionales. Aparte del usuario USM predeterminado, serveradmin, que tiene privilegios de lectura y escritura con la información MIB, todos los nuevos usuarios USM que usted configure sólo tendrán privilegios de sólo lectura con la información MIB.
- Destinos de notificaciones: utilice esta función para configurar el receptor de información/control.

Configuración de las cadenas de comunidad

Puede agregar y editar las cadenas de comunidad y los privilegios de acceso de la cadena de comunidad.

Agregar cadenas de comunidad

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Sistema** y haga clic en el enlace **Ver más** en la sección SNMP.

Paso 4 Seleccione **Agregar** en la sección de Cadenas de comunidad.

Paso 5 Rellene los campos en la página **Agregar cadena de comunidad**.

Opción	Descripción
Nombre de cadena de comunidad	Introduzca el nombre de su cadena de comunidad. Longitud mínima: 256 caracteres.
Privilegios de acceso	Defina los privilegios de acceso para la cadena de comunidad. Las opciones incluyen: • Solo lectura • Lectura y escritura • Lectura, escritura y notificación • Solo notificación • Ninguno **Predet.**: Solo lectura
Información de dirección IP del host	Seleccione el tipo de información de la dirección IP del host. (Predeterminado: **Aceptar paquetes SNMP de cualquier organizador)** Si selecciona **Aceptar paquetes SNMP de estos organizadores**, aparece un cuadro de diálogo debajo de la selección. Introduzca los nombres de host y las direcciones de IP separados por comas.

Seleccione **Agregar**.

La cadena de comunidad se ha agregado a su sistema.

Paso 6 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Editar las cadenas de comunidad

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Sistema** y haga clic en el enlace **Ver más** en la sección SNMP.

Paso 4 Seleccione un enlace de nombre de cadena de comunidad en la sección Cadenas de comunidad.

Paso 5 Cambie los campos deseados en la página **Editar cadena de comunidad**.

Opción	Descripción
Nombre de cadena de comunidad	Cambie el nombre de su cadena de comunidad. Longitud mínima: 256 caracteres.
Privilegios de acceso	Defina los privilegios de acceso para la cadena de comunidad. Las opciones incluyen: • Solo lectura • Lectura y escritura • Lectura, escritura y notificación • Solo notificación • Ninguno **Predet.**: Solo lectura
Información de dirección IP del host	Seleccione el tipo de información de la dirección IP del host. **Predet.**: Aceptar paquetes SNMP de cualquier organizador Si selecciona **Aceptar paquetes SNMP de estos organizadores**, aparece un cuadro de diálogo debajo de la selección. Introduzca los nombres de host y las direcciones de IP separados por comas.

Seleccione **Editar**.

La información de su cadena de comunidad cambia.

Paso 6 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Configuración de usuarios USM

Puede agregar y editar sus usuarios USM.

Agregar usuarios USM

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Sistema** y después seleccione **Ver más** en la sección SNMP.

Paso 3 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 4 Seleccione **Agregar** en la sección Usuarios USM.

Paso 5 Rellene los campos en la página **Agregar usuario USM**.

Opción	Descripción
Nombre de usuario USM	Introduzca el nombre de usuario USM que quiere configurar. Máximo 256 caracteres.
Nivel de seguridad	Seleccione el nivel de seguridad. El nivel de seguridad que seleccione determinará los algoritmos y contraseñas que puede definir para el usuario. Las opciones incluyen: • noAuthNoPriv: ningún algoritmo y contraseña de autenticación, y ningún algoritmo y contraseña de privacidad para el usuario. • authPriv: le permite configurar un algoritmo y una contraseña de autenticación, y un algoritmo y una contraseña de privacidad para el usuario. • authNoPriv: le permite configurar un algoritmo de autenticación y una contraseña de autenticación para el usuario. **Predet.**: noAuthNoPriv
Algoritmo de Autenticación	Seleccione el algoritmo de autenticación para el usuario. **Nota** Esta opción solo aparece si el nivel de seguridad se configure en **authPriv** o **authNoPriv**. **Predet.**: SHA
Contraseña de autenticación	Introduzca la contraseña de autenticación para el usuario. **Nota** Esta opción solo aparece si el nivel de seguridad se configure en **authPriv** o **authNoPriv**.
Algoritmo de Privacidad	Seleccione el algoritmo de privacidad para el usuario. **Nota** Esta opción solo aparece si el nivel de seguridad se configura en **authPriv**. **Predet.**: AES128

Opción	Descripción
Contraseña de privacidad	Introduzca la contraseña de privacidad para el usuario. **Nota** Esta opción solo aparece si el nivel de seguridad se configura en **authPriv**.

Paso 6 Seleccione **Agregar**.
El usuario USM se agrega a su sistema.

Paso 7 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Edición de usuarios USM

Nota El usuario USM predeterminado, serveradmin, se utiliza internamente y el usuario puede cambiar la contraseña pero no el nivel de seguridad, autenticación y algoritmo de privacidad.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Sistema** y después seleccione **Ver más** en la sección SNMP.

Paso 3 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 4 Seleccione un usuario USM en la sección Usuarios USM.

Paso 5 Cambie los campos deseados en la página **Editar usuario USM**.

Opción	Descripción
Nombre de usuario USM	Cambiar nombre de usuario USM. Máximo 256 caracteres.
Nivel de seguridad	Seleccione el nivel de seguridad. El nivel de seguridad que seleccione determinará los algoritmos y contraseñas que puede definir para el usuario. Las opciones incluyen: • noAuthNoPriv: ningún algoritmo y contraseña de autenticación, y ningún algoritmo y contraseña de privacidad para el usuario. • authPriv: le permite configurar un algoritmo y una contraseña de autenticación, y un algoritmo y una contraseña de privacidad para el usuario. • authNoPriv: le permite configurar un algoritmo de autenticación y una contraseña de autenticación para el usuario. **Predet.**: noAuthNoPriv

Opción	Descripción
Algoritmo de Autenticación	Seleccione el algoritmo de autenticación para el usuario. **Nota** Esta opción solo aparece si el nivel de seguridad se configure en **authPriv** o **authNoPriv**. **Predet.**: SHA
Contraseña de autenticación	Cambie la contraseña de autenticación del usuario. **Nota** Esta opción solo aparece si el nivel de seguridad se configure en **authPriv** o **authNoPriv**.
Algoritmo de Privacidad	Seleccione el algoritmo de privacidad para el usuario. **Nota** Esta opción solo aparece si el nivel de seguridad se configura en **authPriv**. **Predet.**: AES128
Contraseña de privacidad	Cambie la contraseña de privacidad para el usuario. **Nota** Esta opción solo aparece si el nivel de seguridad se configura en **authPriv**.

Paso 6 Seleccione **Editar**.
La información del usuario USM cambia.

Paso 7 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Configuración de los destinos de notificación

Puede configurar las máquinas virtuales en su sistema para generar notificaciones o controles SNMP para lo siguiente:

- Arranque de la máquina virtual (control de arranque en frío)
- Todas las condiciones de alarma

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Sistema** y haga clic en el enlace **Ver más** en la sección SNMP.

Paso 3 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 4 Seleccione **Agregar destino de notificación nuevo** en **Destinos de notificación**.

Paso 5 Configure los campos siguientes para sus destinos de notificación:

Opción	Descripción
Nombre de host de destino / Dirección IP	El nombre de host o la dirección IP de la máquina virtual que quiere configurar como destino de notificación.
Número de puerto	El número de puerto para su máquina virtual. **Predet.**: 162
Versión de SNMP	Su versión de SNMP. **Predet.**: v3
Tipo de notificación	Seleccione **Inform** o **Traps**. **Predet.**: Traps
Usuarios USM **Nota** Esta opción aparece solo cuando la versión SNMP es V3.	Seleccione los usuarios USM. Consulte Configuración de usuarios USM, en la página 171 para obtener más información.
cadena de comunidad **Nota** Esta opción aparece solo cuando la versión SNMP no es V3.	Seleccione las cadenas de comunidad. Consulte Configuración de las cadenas de comunidad, en la página 169 para obtener más información.

Paso 6 Seleccione **Agregar**.
Su destino de notificación se ha agregado.Paso

Paso 7 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Edición de un destino de notificación

Configuración de los destinos de notificación

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Sistema** y haga clic en el enlace **Ver más** en la sección SNMP.

Paso 3 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 4 Seleccione un enlace de destino de notificación de la lista **Destinos de notificación**.

Paso 5 Puede editar los campos siguientes para su destino de notificación:

Opción	Descripción
Nombre de host de destino / Dirección IP	El nombre de host o la dirección IP de la máquina virtual que quiere configurar como destino de notificación.
Número de puerto	El número de puerto para su máquina virtual. **Predet.**: 162
Versión de SNMP	Su versión de SNMP. **Predet.**: v3
Tipo de notificación	Seleccione **Inform** o **Traps**. **Predet.**: Inform
Usuarios USM **Nota** Esta opción aparece solo cuando la versión SNMP es V3.	Seleccione los usuarios USM. Consulte Configuración de usuarios USM, en la página171 para obtener más información.
cadena de comunidad **Nota** Esta opción aparece solo cuando la versión SNMP no es V3.	Seleccione las cadenas de comunidad. Consulte Configuración de las cadenas de comunidad, en la página169 para obtener más información.

Paso 6 Seleccione **Guardar**.
Su destino de notificación se ha guardado.

Paso 7 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Administración de licencias

Cuando compra este producto, se le proporciona un periodo de prueba de seis meses. Después de que expire el periodo de prueba, tendrá que comprar licencias para sus usuarios.

Las licencias se pueden obtener por medio del Cisco Enterprise License Manager incorporado (consulte Tramitación de licencias utilizando el Administrador de licencias), eFulfilment (consulte Pedido de licencias utilizando eFulfilment) o poniéndose en contacto con TAC (consulte Tramitar licencias poniéndose en contacto con TAC).

Acerca de las licencias

Acerca de la obtención de licencias basada en el usuario

Este producto tiene licencias basadas en organizador. Debe comprar una licencia para cada usuario que desee que organice reuniones. Es importante comprender los términos siguientes:

- Participante--Persona que asiste a reuniones, pero que no planifica ni organiza reuniones, ni tampoco controla las funciones de la organización, tales como la presentación de contenidos, a menos que el participante sea también el presentador designado por un organizador.
- Organizador de la reunión--Planifica reuniones, asiste a reuniones con capacidad de un organizador y se le permite controlar determinadas funciones, tales como la identificación de un presentador o la capacidad de silenciado.
- Organizador alternativo--Identificado en el momento de planificar la reunión, es alguien que puede asumir la función de organizador en ausencia del organizador de la reunión. Si el organizador de la reunión que ha planificado dicha reunión no asiste a ella, el organizador alternativo controla gran parte de las mismas funciones que el organizador de la reunión. Si tanto la persona identificada como organizador alternativo como el organizador de la reunión asisten a la reunión, el estado del organizador alternativo desde la perspectiva de las licencias es el de *participante*.
- Unirse antes que el organizador (JBH): permite a los participantes unirse a una reunión antes de la llegada del organizador o de un organizador alternativo.
- Solapamiento de reuniones: dos o más reuniones planificadas en la misma hora por el mismo organizador. Cuando el organizador de la reunión o un organizador alternativo inician reuniones solapadas, es posible que se consuman licencias adicionales. Una persona puede planificar reuniones solapadas, pero dicha persona no puede organizar más de una reunión en una misma hora. El solapamiento de reuniones se produce cuando el organizador de una reunión abandona dicha reunión para iniciar otra reunión y la primera reunión continua bajo la dirección de una persona distinta que actúa como organizador.
- Período de gracia--Período de solapamiento de 15 minutos. El periodo de gracia solamente se aplica cuando se permite la función JBH y la reunión la inicia un asistente que no es el organizador.

El cálculo por el uso de licencias se realiza una vez al mes, por ejemplo, una vez desde el 1 al 31 de enero, una vez desde el 1 al 28 de febrero, etc. Las licencias se contabilizan del modo siguiente:

- No se consumen (utilizan) licencias por *planificar* reuniones. Al planificar una reunión, el organizador de dicha reunión puede identificar organizadores alternativos. La identificación de organizadores alternativos o la planificación de una reunión en nombre de otros no consume licencias. Al asistir a una reunión, la persona que planifica una reunión se identifica como el organizador de dicha reunión por defecto.
- Los participantes nunca consumen licencias. Si una persona ha asistido a reuniones durante el mes como participante y nunca ha actuado como organizador, dicha persona consume cero licencias.
- Se utiliza una licencia y se asocia a una persona la primera vez que inicie una reunión en un mes dado y se identifique como el organizador de dicha reunión. Si una persona inicia más reuniones no solapadas durante el mes, no se agotan licencias adicionales. Si durante el siguiente mes la misma persona no asiste a ninguna reunión como organizador, dicha persona agota cero licencias en dicho mes. Dicha persona puede asistir a reuniones como participante sin consumir licencias.
- Se utiliza una licencia adicional y se asocia a una persona por cada reunión solapada a la que asista dicha persona como organizador de dichas reuniones. El número total de licencias consumidas por una persona viene determinado por el mayor número de reuniones solapadas que dicha persona haya organizado. Una persona que asista a dos reuniones en calidad de organizador en el mismo período de tiempo agota y se le asocian dos licencias en el mes en curso. Si dicha persona inicia tres reuniones que se solapan en el mismo período de tiempo, se agotan tres licencias. Etcétera. Si la misma persona asiste a una reunión como organizador, abandona la primera reunión antes de que ésta finalice y asiste a otra reunión en calidad de organizador, se necesitan dos licencias para dicha persona.

- No se consumen licencias adicionales cuando la persona identificada como organizador alternativo que no ha consumido aún una licencia en dicho mes, inicia una reunión y el organizador de la reunión se une a la reunión.
- Se utiliza una licencia y se asocia a un organizador alternativo cuando un organizador activo que aún no ha consumido una licencia en dicho mes asiste a una reunión en calidad de organizador y el organizador que ha planificado dicha reunión no se une a ella.

Si lleva a cabo un procedimiento de actualización general o recuperación de desastres en el sistema, debe configurar nuevas máquinas virtuales y realojar las licencias. (Consulte Realojamiento de licencias después de una actualización de software o la expansión del sistema.)

El sistema cuenta el uso de licencias por cada usuario y mes, como muestran los ejemplos de situaciones de la tabla. Las situaciones de la tabla asumen que en cada ejemplo es la primera vez que el usuario ha organizado una reunión en dicho mes.

Situación	Fecha de la reunión	Hora de la reunión	Licencias utilizadas
El usuario A planifica una reunión, pero dicha reunión nunca se inicia.	1 de enero	De 9:00 a 10:00	0
El usuario B inicia una reunión.	2 de enero	De 9:00 a 10:00	1
El usuario C organiza dos o más reuniones que no se solapan.	3 de enero 3 de enero 4 de enero	De 9:00 a 10:00 De 2:00 a 2:30 De 10:00 a 11:00	1
El usuario D asiste a dos reuniones que se solapan en la misma fecha y hora.	6 de enero 6 de enero	De 9:00 a 10:00 De 9:30 a 10:00	2
El usuario E inicia dos reuniones que se solapan en la misma fecha y hora. El organizador que ha iniciado las dos reuniones y un organizador alternativo organiza la segunda reunión.	6 de enero 6 de enero	De 9:00 a 10:00 De 9:30 a 10:00	3 El organizador que ha iniciado cada una de las reuniones agota una licencia y el organizador alternativo agota una licencia.
El usuario F inicia dos reuniones en la misma fecha y abandona las dos reuniones. Las reuniones son organizadas por un organizador alternativo.	7 de enero 7 de enero	De 9:00 a 10:00 De 9:00 a 10:00	2 Una por cada organizador original y una por los organizadores alternativos que continuaron una de las reuniones.

Situación	Fecha de la reunión	Hora de la reunión	Licencias utilizadas
El usuario G organiza una reunión y pasa los derechos de organizador a otro participante durante la reunión. El organizador de la primera reunión inicia posteriormente una segunda reunión que se celebra al mismo tiempo que la primera reunión.	8 de enero 8 de enero	De 9:00 a 10:00 De 9:30 a 10:00	2 Una por cada organizador original y una por los organizadores alternativos que continuaron una de las reuniones.
El usuario H inicia una reunión que tiene activada la función **Unirse antes que el organizador**. Un organizador se une a la reunión. Después, el primer usuario planifica una segunda reunión que se celebra al mismo tiempo que la primera reunión, pero todos los participantes de la segunda reunión solamente se unen a la teleconferencia (no la parte Web) con la opción seleccionada.	11 de enero 11 de enero	De 9:00 a 10:00 De 9:00 a 10:00	2
El usuario J planifica una reunión. Se activa la opción **Unirse antes que el organizador**. Los participantes se unen, pero ni el organizador de la reunión ni los organizadores alternativos asisten a la reunión y todos los participantes abandonan dicha reunión.	11 de enero	De 9:00 a 10:00	1
El usuario K inicia una sesión con la opción **Unirse antes que el organizador** activada. El asistente JBH inicia una segunda reunión en nombre del organizador. Antes de que caduque el periodo de gracia, el organizador abandona y finaliza la primera reunión.	12 de enero 12 de enero	De 9:00 a 10:00 De 9:10 a 10:00	1

Situación	Fecha de la reunión	Hora de la reunión	Licencias utilizadas
El usuario L organiza tres conferencias personales (sin la parte web) con las cuentas 1, 2 y 3 en la misma fecha pero a distintas horas.	12 de enero 12 de enero January12	De 9:00 a 10:00 De 10:00 a 11:00 De 11:00 a 12:00	1
El usuario M inicia tres conferencias personales (sin la parte web) con las cuentas 1, 2 y 3 en la misma fecha y a la misma hora.	14 de enero	De 9:00 a 10:00	3
El usuario N inicia una reunión con la opción **Unirse antes que el organizador** activada y una conferencia personal (sin la parte Web) en la misma fecha pero en horas diferentes.	14 de enero 14 de enero	De 9:00 a 10:00 De 11:00 a 12:00	1
El usuario P inicia una reunión con la opción **Unirse antes que el organizador** activada y una conferencia personal (sin la parte Web) en la misma fecha y hora.	15 de enero 15 de enero	De 9:00 a 10:00 De 9:00 a 10:00	2
El usuario Q inicia una conferencia personal (sin la parte Web) y poco después lanza la parte web solapada.	16 de enero 16 de enero	De 9:00 a 10:00 (conferencia personal) De 9:15 a 10:00 (reunión web iniciada conjuntamente con la conferencia personal)	1

Desde la página **Informes**, puede solicitar un informe que especifique el número total de licencias consumidas durante el mes. Además, le recomendamos que vea el informe resumido en PDF que muestra las tendencias de consumo de licencias mes a mes. Mediante la visualización de la tendencia global de licencias, puede planificar las compras de licencias futuras de forma más efectiva, para adaptarse a la creciente adopción de este sistema en su empresa.

Precaución Su sistema permite que el consumo de licencias exceda el número de licencias instaladas. Los administradores reciben mensajes de correo electrónico y avisos en el escritorio de **licencias excedidas** para informarles de que deben reducir el consumo de licencias o comprar más licencias en los próximos seis meses. Durante este periodo de seis meses, el sistema seguirá funcionando normalmente para sus usuarios. Si no ha reducido el consumo de licencias ni ha comprado más licencias en seis meses, el sistema se desconecta para todos los usuarios hasta que un administrador instale más licencias.

Cuando el sistema está desconectado, los usuarios no pueden planificar, organizar ni asistir a reuniones, ni tampoco acceder a grabaciones de reuniones. Los usuarios ven el mensaje **Sitio en mantenimiento** en el sitio de WebEx. El sitio de administración funcionará normalmente: de modo que un administrador puede iniciar sesión y agregar licencias para solucionar el problema de las licencias excedidas. Una vez se han instalado licencias adicionales, los usuarios pueden acceder al sitio de WebEx, organizar reuniones, finalizar reuniones y acceder a grabaciones.

Período de prueba gratuito de seis meses

Después de iniciar sesión en este producto por primera vez y completar el asistente de introducción, se inicia su periodo de prueba gratuito de seis meses. Durante el periodo de prueba, los administradores pueden configurar el sistema y sus usuarios pueden planificar, organizar y asistir a reuniones. Aparece una pancarta en la parte superior del sitio de administración indicando cuántos meses le quedan del periodo de prueba. Un mes antes de que finalice su periodo de prueba, recibirá un correo electrónico informándole de que debe comprar una licencia e instalarla o, de lo contrario, su sistema se deshabilitará.

Al final del periodo de prueba, su sistema se deshabilitará. Puede iniciar sesión en su sistema pero no puede utilizar ninguna otra función hasta que agregue licencias. Consulte la sección Administración de licencias de la *Guía de administración de Cisco WebEx Meetings Server* para obtener más información sobre la administración de sus licencias.

Realojamiento de licencias

Una vez se haya actualizado el software de CWMS o se haya ampliado un sistema existente, el realojamiento de licencias permite utilizar licencias válidas más antiguas en un sistema actualizado o ampliado. Consulte Realojamiento de licencias después de una actualización de software o la expansión del sistema en la *Guía de administración de Cisco WebEx Meetings Server*.

Obtención de licencias

Póngase en contacto con su representante de ventas de Cisco para solicitar licencias para su sistema. Cuando se ponga en contacto con su representante de ventas, tendrá que especificar cuántas licencias quiere. Necesitará una licencia para cada empleado de su organización que quiera organizar reuniones.

Hay varias formas de determinar cuántas licencias necesitará. Puede utilizar su escritorio para ver el uso, el historial de recursos y las tendencias de reuniones con el propósito de determinar cuántos usuarios están organizando y asistiendo a reuniones en su sistema. Después de utilizar el producto durante unos meses, puede usar sus informes resumidos mensuales y los informes detallados personalizados para ayudarle a determinar cuántas licencias necesitará. Sus informes resumidos mensuales muestran estadísticas sobre la adopción de servicios y el uso de la licencia de usuario. Las estadísticas de adopción de servicios le muestran el índice con el cual los nuevos usuarios están adoptando su sistema, mostrando el índice de adopción para los anteriores tres meses y prediciendo el índice de crecimiento para los próximos tres meses. Las estadísticas de licencia de usuario muestran el uso de la licencia en los tres meses anteriores y el crecimiento previsto para los próximos tres meses.

Las licencias se pueden obtener utilizando el Cisco Enterprise License Manager incorporado, eFulfilment o poniéndose en contacto con el TAC. Consulte la sección Administración de licencias de la *Guía de administración de Cisco WebEx Meetings Server* para obtener más información sobre la administración de licencias.

Superar sus licencias

Después de comprar y configurar licencias en su sistema, debe comprobar que tiene licencias suficientes para alojar a todos los organizadores activos en su sistema. Su sistema comprueba cada mes si existen suficientes licencias para cada organizador activo. El número de licencias se restablece cada mes natural. Si el número de organizadores activos en su sistema supera el número de licencias, se envía un correo electrónico al administrador notificándole que ha superado sus licencias. Tiene un periodo de gracia de seis meses para reducir el uso de licencias, o aumentar el número de licencias en su sistema para que iguale o supere el número de organizadores activos. Si no reduce el uso de licencias ni compra suficientes licencias para cubrir el uso antes de que finalice el periodo de seis meses, su sistema se deshabilitará. El mensaje de correo electrónico informa al administrador de la fecha en que ocurrirá.

El sistema compruebe y ajusta los números de licencia mostrados en el sitio de administración. El gestor de auditorías se ejecuta una vez al día (a las 2:00 a.m.) para ajustar el número licencias utilizadas según sea necesario. Al final de cada mes, el sistema comprueba el uso de licencias. Si el número de organizadores ha caído por debajo del número de licencias, la condición de excedente finaliza. Si el número de organizadores sigue superando el número de licencias, se envía un nuevo correo electrónico a su administrador cada mes notificándole que la condición de excedente sigue existiendo y especificando la fecha en que se deshabilitará el sistema.

Si sigue teniendo una condición de excedente después de seis meses, su sistema se deshabilita y el administrador recibe un correo electrónico notificándole lo que ha ocurrido. Una vez se deshabilite su sistema, sus usuarios no podrán programar, organizar ni asistir a reuniones en su sistema, ni tampoco acceder a las grabaciones. El sitio de administración seguirá funcionando normalmente para que el administrador pueda iniciar sesión y agregar licencias. Una vez que el administrador haya agregado licencias al sistema, los usuarios podrán volver a programar, organizar y asistir a reuniones, así como acceder a las grabaciones.

Licencias temporales

Si tiene licencias temporales configuradas en su sistema, su estado de licencia temporal aparece en una pancarta en cada página del sitio de administración. Esta pancarta le informe de cuántas licencias temporales tiene configuradas y de cuándo caducarán esas licencias temporales. Cuando las licencias temporales caducan, su sistema vuelve a su estado de licencia anterior.

Licencias desactualizadas

Si actualiza su sistema, también debe actualizar sus licencias. Una vez que ha actualizado su sistema, se envía un correo electrónico a su administrador notificándole que se le ha concedido un periodo de gracia de seis meses para actualizar las licencias. Si no actualiza sus licencias antes del final del periodo de seis meses, su sistema se deshabilitará. El mensaje de correo electrónico informa al administrador de la fecha en que ocurrirá.

El sistema compruebe y ajusta los números de licencia mostrados en el sitio de administración. El gestor de auditorías se ejecuta una vez al día (a las 2:00 h) para ajustar el número licencias desactualizadas según sea necesario. Al final de cada mes, el sistema comprueba si las licencias se han actualizado desde el periodo anterior. Si las licencias se han actualizado, la condición de licencia desactualizada termina. Si las licencias todavía no se han actualizado, se envía un nuevo correo electrónico a su administrador cada mes notificándole que la condición de licencia desactualizada todavía existe y la fecha en que el sistema se deshabilitará.

Si sigue teniendo una condición de licencia desactualizada después de seis meses, su sistema se deshabilita y el administrador recibe un correo electrónico notificándole lo que ha ocurrido. Una vez se deshabilite su

sistema, sus usuarios no podrán programar, organizar ni asistir a reuniones en su sistema, ni tampoco acceder a las grabaciones. El sitio de administración seguirá funcionando normalmente para que un administrador pueda iniciar sesión y actualizar las licencias. Una vez que el administrador haya actualizado las licencias, los usuarios podrán volver a programar, organizar y asistir a reuniones, así como acceder a las grabaciones.

Conexión perdida de Prime License Manager (PLM)

Cuando adquiera licencias, utilizará una herramienta PLM incorporada para especificar su PAK y registrar sus licencias. PLM lleva a cabo una sincronización cada 12 horas para actualizar el estado de las licencias y la última fecha de cumplimiento de normas. Si pasan dos días sin conexión con PLM, se envía un correo electrónico a su administrador para informarle de que PLM no puede sincronizarse con sus sistema. Tiene un período de gracia de seis meses para volver a conectarse con PLM. Si su sistema no vuelve a conectarse con PLM antes de finalizar el período de seis meses, se deshabilitará su sistema. El mensaje de correo electrónico informa al administrador de la fecha en que ocurrirá.

Se envía un nuevo correo electrónico a su administrador al final de cada mes para notificar que el sistema no puede conectarse con PLM informando al administrador de la fecha en que se deshabilitará el sistema. Si su sistema vuelve a conectarse con PLM antes de finalizar el periodo de gracia de seis meses, esta condición finaliza.

Si su sistema sigue sin poderse conectar con PLM después de seis meses, su sistema se deshabilita y el administrador recibe un correo electrónico notificándole lo que ha ocurrido. Cuando se deshabilita su sistema, los usuarios no pueden planificar, organizar o asistir a reuniones, ni acceder a grabaciones en el sistema. El sitio de administración funciona normalmente, por lo que un administrador puede iniciar una sesión en el sistema, pero el sistema debe volver a conectarse con PLM para finalizar esta condición y restaurar la posibilidad de que los usuarios planifiquen, organicen y asistan a reuniones y accedan a grabaciones.

Acciones que necesitan nuevas licencias

Las siguientes acciones que alteran el sistema requieren que instale nuevas licencias:

- Ampliación: consulte Ampliar su sistema a un tamaño de sistema superior para obtener más información.
- Actualización: consulte Actualización del sistema para obtener más información.
- Recuperación de desastres: consulte Utilizar la función de recuperación ante desastres para obtener más información.

Tramitación de licencias utilizando el Administrador de licencias

Obtenga las licencias utilizando el Cisco Enterprise License Manager incorporado:

Antes de comenzar

Póngase en contacto con su representante de ventas de Cisco para solicitar licencias para su sistema. El representante de ventas le enviará un correo electrónico que contiene la clave de autorización de su producto (PAK) .

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Sistema** y después seleccione el enlace **Ver más** en la sección Licencias.

Paso 3 Seleccione **Administrar licencias**

El explorador abre una nueva pestaña o ventana que contiene Cisco Prime License Manager (PLM).

Nota Esta versión de PLM está incorporada en Cisco WebEx Meetings Server. El PLM no es un sitio web externo.

Paso 4 Seleccione **Gestión de licencias** > **Licencias**.

Paso 5 Seleccione **Generar solicitud de licencia**.
Aparece el cuadro de diálogo **Solicitud de licencia y pasos siguientes**.

Paso 6 Copie el texto seleccionado en el campo y seleccione **Registro de licencia de Cisco**.

Paso 7 Inicie sesión en su cuenta de Cisco.

Paso 8 Introduzca el PAK que ha recibido de su representante de ventas Cisco en el campo **Clave de autorización de producto** y seleccione **Siguiente**.
Aparece la página **Tramitar PAK**.

Paso 9 Pegue el contenido de la Solicitud de licencia que copió anteriormente en el campo, escriba la cantidad de licencias que va a comprar y seleccione **Siguiente**.

Paso 10 Revise la página y seleccione **Estoy de acuerdo con los términos de la licencia**.

Paso 11 Asegúrese de que la dirección de correo electrónico de contacto es correcta. Opcionalmente, puede cambiar la dirección de correo electrónico de contacto en el campo **Enviar a**.

Paso 12 Seleccione **Obtener licencia**
Aparecerá el cuadro de diálogo **Estado de solicitud de licencia**.

Paso 13 Obtenga el archivo de licencia de una de las siguientes maneras:

- Seleccione **Descargar** para descargar su archivo de licencia (.bin).
- Extraiga el archivo de licencia (.bin) desde el archivo ZIP que se le ha enviado por correo electrónico.

Paso 14 Vuelva al sitio de administración y seleccione **Sistema** y, a continuación, seleccione el enlace **Ver más** en la sección Licencias.

Paso 15 Seleccione **Administrar licencias**.
El explorador abre una nueva pestaña o ventana que contiene Cisco Prime License Manager (PLM).

Paso 16 Seleccione **Instalar archivo de licencia**.

Paso 17 Seleccione **Examinar** y seleccione el archivo de licencia (.bin) que ha descargado o extraído del archivo ZIP en su correo electrónico.

Paso 18 Seleccione **Instalar**.
Su archivo de licencia se ha instalado. Compruebe la información de licencia que se muestra para garantizar que sea correcta.

Paso 19 Seleccione **Actual** en la columna de Fecha de tramitación.
Aparece la página **Tramitación de licencia**. Compruebe que la información visualizada en la sección **Licencias tramitadas** es correcta.

Tramitar licencias utilizando eFulfilment

Tramite el pedido de licencias especificando la clave de autorización de producto (PAK) en el administrador de licencias sin utilizar el sitio web.

Antes de comenzar

Póngase en contacto con su representante de ventas de Cisco para solicitar licencias para su sistema. El representante de ventas le enviará un correo electrónico que contiene la clave de autorización de su producto (PAK) .

eFulfillment necesita que sea posible establecer una conexión de red entre el sistema y Cisco Systems, Inc. Compruebe que su sistema no se encuentra detrás de un cortafuegos que impida el acceso. Si no se permite el acceso, utilice la tramitación basada en archivo (consulte Tramitación de licencias utilizando el Administrador de licencias) o póngase en contacto con TAC para abrir una incidencia de pedido de licencias (consulte Tramitar licencias poniéndose en contacto con TAC.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Sistema** y después seleccione el enlace **Ver más** en la sección Licencias.

Paso 3 Seleccione **Administrar licencias**
El explorador abre una nueva pestaña o ventana que contiene Cisco Prime License Manager (PLM) incorporado en Cisco WebEx Meetings Server. (El sitio PLM no es un sitio web externo.)

Paso 4 Seleccione **Tramitar licencias de PAK**.
Aparece el asistente **Tramitar licencias de PAK**.

Paso 5 Introduzca el PAK que ha recibido de su representante de ventas Cisco en el campo **Clave de autorización de producto** y seleccione **Siguiente**.
Aparece la página **Tramitar PAK**.

Paso 6 Seleccione **Agregar licencias de un nuevo PAK**.

Paso 7 Especifique el código PAK en el cuadro *** código PAK** y seleccione **Siguiente**.

Paso 8 Inicie sesión utilizando el ID de usuario y contraseña de cisco.com.
Aparece la ventana **Tramitar licencias** que indica el número de licencias disponibles.

Paso 9 Seleccione **Tramitar** en la columna **Acciones**.

Paso 10 Haga clic en la columna **Instalar** para editar los valores.

Paso 11 Especifique el número de licencias que desea tramitar para este sistema. Si el PAK admite tramitaciones parciales, el intervalo es de 1 al número de licencias restantes en el PAK.

Paso 12 Seleccione **Guardar**.

Paso 13 Seleccione **Aceptar**.
Aparece la ventana **Tramitar licencias**. El valor de la columna **Instalar** muestra el número de licencias que desea tramitar.

Paso 14 Seleccione **Siguiente**.
Aparece la ventana **Revisar contenidos**. La columna **Valores actuales** muestra el número de licencias activas. La columna **Después de la tramitación** muestra el número de licencias que tendrá cuando finalice el eFulfillment.

Paso 15 Seleccione **Siguiente**.

Paso 16 Seleccione **Al marcar esta casilla acepto que he leído, he comprendido y acepto vincularme a los términos y condiciones del Acuerdo de licencia de usuario final.**

Paso 17 Seleccione **Finalizar**.
Se muestra la barra de progreso **Conexión con el servidor de licencias** mientras el administrador de licencias se conecta con Cisco para tramitar las licencias. Cuando finalice eFulfillment, se agrega una nueva línea a la

ventana **Licencias**. La columna **Fecha de tramitación** muestra la fecha actual seguida de **- Actual**. Puede seleccionar este enlace para visualizar los detalles de las licencias, incluido el tipo y número de licencias instaladas en este sistema.

Tramitar licencias poniéndose en contacto con TAC

Antes de comenzar

Obtenga su número de ID de registro. Puede encontrar su número de ID de registro abriendo su herramienta Enterprise License Management y seleccionando **Acerca de**.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Soporte** y llame al CAT al número especificado.

Paso 3 Presente una solicitud, solicitando el número de licencias adicionales que desee.
Cisco procesa su solicitud y activa las licencias adicionales en su sistema.

Paso 4 Seleccione **Sistema**.

Paso 5 Compruebe la sección Licencia para confirmar que las licencias se han agregado.

CAPÍTULO 14

Configuración de ajustes

En este módulo se describe cómo configurar sus ajustes.

- Configuración de la información de su empresa, página 188
- Configuración de los ajustes de personalización, página 189
- Configuración de sus ajustes de reuniones, página 190
- Acerca de configurar sus ajustes de audio, página 193
- Configuración de los ajustes de vídeo, página 197
- Configuración de sus ajustes móviles, página 198
- Configuración de la calidad del servicio (QoS), página 198
- Configuración de contraseñas, página 200
- Configuración de sus ajustes de correo electrónico, página 204
- Configuración de los ajustes de descarga, página 224
- Administración de certificados, página 226
- Generar certificados SSL, página 226
- Importar certificados de SSO IdP, página 234
- Importación de certificados seguros de teleconferencia, página 234
- Configuración de la seguridad de sesión de usuario, página 235
- Configurar los ajustes de autenticación única (SSO), página 236
- Configuración de las funciones de la nube, página 240
- Configuración de la seguridad de la máquina virtual, página 240

Configuración de la información de su empresa

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Si desea cambiar el ajuste Idioma, seleccione **Activación del modo de mantenimiento** y **Continuar** para confirmar.

Nota No tiene que activar el modo de mantenimiento para modificar los otros ajustes en la página **Información de la empresa**.

Paso 3 Seleccionar **Configuración**. Si está viendo una de las páginas de ajustes, también puede seleccionar **Información de la empresa** en la sección Configuración.

Paso 4 Rellene los campos en la página y seleccione **Guardar**.

Opción	Descripción
Nombre de la empresa	Su nombre de empresa u organización.
Dirección 1	Línea dirección 1.
Dirección 2	Línea dirección 2.
Ciudad	Su ciudad.
Estado/Provincia	El nombre de su estado o provincia.
Código postal	Código postal.
País/región	El nombre de su país o región.
Teléfono del trabajo	Menú desplegable con código de país y campo para el número de teléfono de empresa con código de área.
Zona horaria	Su zona horaria.
Idioma	Su idioma. La configuración del idioma afecta a lo siguiente: • La página de inicio de sesión que ven los administradores cuando activan su cuenta de administrador por primera vez. • Las instrucciones de audio predeterminadas que se reproducen para los usuarios de teleconferencia que entran a través de la llamada directa.

Opción	Descripción
Configuración regional	Su configuración regional. La configuración regional afecta a la visualización de horas, fechas, divisas y números.

Paso 5 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Configuración de los ajustes de personalización

Antes de comenzar

Prepare lo siguiente antes de configurar sus ajustes de personalización:

- Una imagen de 120 x 32 en formato PNG, GIF o JPEG que contenga el logotipo de su empresa
- La URL de la declaración de privacidad de su empresa
- La URL de la declaración de condiciones de servicio de su empresa
- La URL de soporte de su empresa

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Personalización**.

Paso 3 Rellene los campos en la página y seleccione **Guardar**.

Opción	Descripción
Logotipo de la empresa	Navegue hasta el archivo del logotipo. El logotipo debe tener el formato PNG, JPEG o GIF. Las dimensiones máximas son 120 x 32 píxeles y el tamaño máximo de archivo es 5 MB.
Declaración de privacidad	Introduzca la URL de la declaración de privacidad de su empresa.
Condiciones del servicio	Introduzca la URL de las condiciones de servicio de su empresa.
Texto de pie de página personalizado	El texto que introduzca estará en el pie de página de todos los correos electrónicos de administrador y usuario final enviados por su sistema.
Color de fondo del encabezado	Seleccione esta opción para eliminar el color de fondo predeterminado. Esto afectará a todas las barras y mensajes de correo electrónico del explorador.

Opción	Descripción
URL de contacto de soporte	Introduzca la URL de la página Web de soporte de su empresa.

Eliminar un logotipo de empresa

Antes de comenzar

Cree un archivo transparente PNG o GIF de 120 x 32.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Personalización**.

Paso 3 Para el campo Logotipo de empresa, seleccione **Examinar** y elija su archivo transparente PNG o GIF de 120 x 32.

Paso 4 Seleccione **Guardar**.
Su logotipo de empresa anterior se sustituye por el archivo PNG o GIF en blanco. Compruebe que el logotipo original se ha suprimido.

Configuración de sus ajustes de reuniones

Configure sus ajustes de reuniones para controlar las funciones que pueden usar los participantes. Configure los ajustes siguientes:

- Configuración de Unirse a reunión
- Máximo de participantes por reunión (tamaño de reunión)

Nota Este ajuste está limitado por el tamaño del sistema que se ha configurado durante el despliegue. Consulte Confirmar el tamaño de su sistema, en la página 31 para obtener más información.

- Privilegios de los participantes

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Reuniones**.

Paso 3 En la sección de ajustes Unirse a la reunión, seleccione sus opciones.
Los ajustes predeterminados son **Permitir a los participantes unirse a reuniones antes que el organizador**, **Permitir a los participantes unirse a teleconferencia antes que el organizador**, y **El primer participante en unirse será el presentador**. Los participantes pueden unirse a reuniones hasta 15 minutos antes de la hora de inicio si se ha seleccionado **Permitir a los participantes unirse a reuniones antes que el organizador** y **Permitir a los participantes unirse a teleconferencia antes que el organizador**. Opcionalmente, seleccione **Cualquiera puede presentar la reunión**.

Nota Si elimina la selección de la opción **Permitir a los participantes unirse a reuniones antes que el organizador**, se eliminará automáticamente la selección de la opción **El primer participante en unirse será el presentador**.

Paso 4 Seleccione el máximo de participantes por reunión arrastrando el control deslizante. El número máximo de participantes para su sistema se configura durante el despliegue. A continuación, mostramos los ajustes de tamaño del sistema y los tamaños máximos de reunión correspondientes.

Tamaño del sistema	Tamaño máximo de la reunión
50	50
250	100
800	100 (sin HA), 250 (con HA)
2,000	100 (sin HA), 250 (con HA)

Paso 5 En la sección de privilegios del participante, seleccione sus opciones. **Chat**, **Sondeo**, **Revisión y presentación de documentos** y **Uso compartido y control remoto** están seleccionados de forma predeterminada. Los privilegios del participante seleccionados aparecen en los controles del usuario.
La grabación está desactivada de forma predeterminada. Seleccione **Registro** para grabar y almacenar las reuniones en su servidor de almacenamiento.

Nota Debe configurar un servidor de almacenamiento para activar la grabación. Consulte Configuración de un servidor de almacenamiento, en la página 164 para obtener más información.

Paso 6 Seleccione **Guardar**.

Acerca de la seguridad de la reunión

Cisco WebEx Meetings Server permite distintas características de seguridad de reunión en función de los siguientes factores:

- Tipo de usuario: organizador, organizador alternativo, usuario (con sesión iniciada) e invitado.
- La reunión tiene o no contraseña.
- La contraseña está oculta o visible en la invitación de la reunión.

- La contraseña está oculta o visible en el correo electrónico de la invitación de la reunión.
- El comportamiento que se muestra en la página de entrada de la reunión (consulte las tablas siguientes).

Tabla 1: La contraseña se excluye al planificar la reunión

Tipo de usuario	La contraseña se muestra en los correos electrónicos de invitación y recordatorio	Página Detalle de la reunión
Organizador	Sí	Sí
Organizador alternativo	Sí	Sí
Asistente invitado	No	No
Asistente enviado	No	No

Tabla 2: La contraseña se incluye al planificar la reunión

Tipo de usuario	La contraseña se muestra en los correos electrónicos de invitación y recordatorio	Página Detalle de la reunión
Organizador	Sí	Sí
Organizador alternativo	Sí	Sí
Asistente invitado	Sí	Sí
Asistente enviado	Sí	Sí

- Unirse antes de que el organizador esté activado/desactivado.
  - Activado: El asistente/invitado/asistente invitado puede unirse a la reunión antes que el organizador, 15 minutos antes de la hora de inicio planificada.
  - Desactivado: El asistente/invitado/asistente invitado no puede unirse a la reunión antes que el organizador. El organizador o el organizador alternativo pueden iniciar la reunión y, después, los asistentes se pueden unir.
- Unirse a la teleconferencia antes de que el organizador esté activado/desactivado.
  - Activado: Si el organizador no inicia la teleconferencia en el cliente de la reunión, los asistentes se pueden unir a la teleconferencia antes que el organizador.
  - Desactivado: Si el organizador no inicia la teleconferencia en el cliente de la reunión, los asistentes no se pueden unir a la teleconferencia antes que el organizador.
- El primer asistente puede presentar está activado/desactivado.
  - Activado: Cuando se ha configurado Unirse antes que el organizador, el primer asistente es el presentador.
  - Desactivado: El organizador siempre tiene el control.

Acerca de configurar sus ajustes de audio

La primera vez que configura sus ajustes de audio, se le guía a través del proceso por medio de un asistente que le ayuda a definir la configuración CUCM SIP y los números de acceso de llamada. Después de completar el asistente y configurar sus ajustes de audio iniciales, puede configurar todos los demás ajustes de audio.

Configuración de los ajustes de audio por primera vez

La primera vez que configure los ajustes de audio, debe especificar las funciones deseadas y debe configurar los ajustes CUCM. Un asistente le guía a través del proceso de instalación la primera vez.

Antes de comenzar

Debe activar la teleconferencia y configurar CUCM antes de proceder con la configuración del audio. Debe configurar CUCM en dos sistemas si quiere proporcionar alta disponibilidad de teleconferencia. Consulte la Guía de planificación para obtener más información. Para proceder, debe obtener la información siguiente:

- Preparar una lista de números de acceso de llamada directa usados por sus participantes para llamar a las reuniones.
- Su dirección IP de CUCM.
- (Opcional) Obtenga un certificado de conferencias seguro y válido si planea utilizar el cifrado de teleconferencia TLS/SRTP. Consulte Importación de certificados seguros de teleconferencia para obtener más información.

Nota Esta función no está disponible en Rusia o Turquía.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Ajustes** > **Audio**.
Aparece la página **Audio** y se muestran las funciones de audio actuales.

Paso 4 Seleccione **Siguiente**.
Aparece la página **Configuración de SIP**. Esta página muestra la información de configuración SIP que necesita para configurar CUCM incluyendo la dirección IP y el número de puerto de cada tipo de servidor.

Paso 5 Seleccione **Siguiente**.
Aparece la página **Activar teleconferencia: Configuración de CUCM**, que muestra sus ajustes actuales.

Paso 6 Seleccione **Editar** para cambiar sus ajustes.
Aparecerá el cuadro de diálogo **CUCM (Cisco Unified Communications Manager)**.

Paso 7 Rellene los campos en el cuadro de diálogo **CUCM (Cisco Unified Communications Manager)** de la siguiente forma:

a) Introduzca una dirección IP para la Dirección IP de CUCM 1 y opcionalmente para la Dirección IP de CUCM2.
Estas direcciones IP deben corresponderse con el nodo CUCM principal y opcionalmente secundario que forman parte del grupo de administradores de comunicaciones unificadas de Cisco tal como se define en la agrupación de dispositivos que se configura en los Troncos SIP de punto de aplicación de CUCM. Consulte "Configuración de un troncal SIP para un punto de la aplicación" en la *Guía de planificación* para obtener más información.

Nota CUCM 2 no es obligatorio, pero se recomienda para alta disponibilidad de teleconferencias.

b) Introduzca el número de puerto para su sistema. El número de puerto debe coincidir con el número de puerto asignado en CUCM. (**Predet.:** 5062)

c) Utilice el menú desplegable **Transporte** para seleccionar el tipo de transporte para su sistema. (**Predet.:** TCP)

Nota Si selecciona TLS como tipo de transporte, debe importar un certificado de conferencia segura válido para cada uno de sus servidores CUCM, exportar el certificado SSL y cargarlo en CUCM, y configurar el nombre de dominio cualificado completo (FQDN) de su sistema como el nombre de dominio SIP en cada servidor CUCM. Consulte Importación de certificados seguros de teleconferencia para obtener más información sobre la importación de certificados y la configuración de CUCM en la Guía de planificación para obtener más información sobre CUCM.

d) Seleccione **Continuar**.

Sus ajustes de CUCM nuevos o actualizados aparecen en la página **Activar teleconferencia: Configuración de CUCM**.

Paso 8 Seleccione **Siguiente**.
Aparece la página **Activar teleconferencia: Configuración de número de acceso**.

Paso 9 Seleccione **Editar**.
Aparecerá el cuadro de diálogo **Números de acceso de llamada directa**.

Paso 10 Seleccione **Agregar** para agregar un número de acceso de llamada directa.
Se agrega una línea en el cuadro de diálogo para el número y la etiqueta de teléfono. Cada vez que seleccione **Agregar**, aparece una línea adicional en el cuadro de diálogo.

Paso 11 Introduzca la **Etiqueta de teléfono** y el **Número telefónico** para cada número de acceso que agregue y seleccione **Continuar** cuando haya acabado de agregar números.

Nota Asegúrese de que solo agrega números que ha configurado en CUCM. Los números que agregue aparecen en las invitaciones de correo electrónico y en su cliente Cisco WebEx Meetings.

Ejemplo:
Introduzca "Sede" para la **Etiqueta de teléfono** y "888-555-1212" para el **Número telefónico**.
Los números de acceso que ha introducido se agregan a su sistema y se le devuelve a la página **Activar teleconferencia: Configuración de número de acceso,** La página ahora indica cuántos números de acceso se han configurado.

Paso 12 Seleccione **Guardar**.
El asistente le informa de que ha configurado correctamente sus funciones de teleconferencia.

Paso 13 (Opcional) Introduzca un nombre de visualización en el cuadro de diálogo **Nombre a mostrar**.

Paso 14 (Opcional) Introduzca un identificador de llamada válido en el cuadro de diálogo **ID de la persona que llama**.

Nota El ID de la persona que llama se limita a los caracteres numéricos y un guión (-), y tiene una longitud máxima de 32 caracteres.

Paso 15 (Opcional) Configure la opción Llamarme de WebEx en **Predeterminado**: Pulse 1 para conectarse a la reunión). También puede seleccionar esta opción para omitir el requisito de pulsar **1** para conectarse a la reunión.

Nota Cisco no recomienda que seleccione esta opción, a no ser que su sistema de teléfono no pueda enviar el dígito **1**.

Paso 16 (Opcional) Seleccione su **Tono telefónico de entrada y salida**.

- Pitido (predeterminado)
- Sin tono
- Anunciar nombre

Paso 17 (Opcional) Si IPv6 está configurado en el sistema, establezca la configuración **Audio conferencia IPv6** en **Activado** o **Desactivado**. (**Predet.**: Desactivado. Un ajuste **Desactivado** indica que IPv4 es el ajuste).

Nota La opción **Audio conferencia IPv6** no está disponible en los sistemas no configurados para IPv6.

Paso 18 Seleccione en **Idioma de audio del sistema** el idioma que los usuarios oirán al marcar el número en la parte de audio de una reunión de Cisco WebEx o cuando utilice el servicio Llamarme.

Paso 19 Seleccione **Guardar**.

Paso 20 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Configuración de los ajustes de audio

Antes de comenzar

Si no ha configurado sus ajustes de audio, consulte la sección Configuración de los ajustes de audio por primera vez, en la página 193.

Nota Para cambiar o configurar los ajustes de audio Número de acceso de llamada entrante, Nombre a mostrar o Id de la persona que llama, no es necesario activar el modo de mantenimiento.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Configuración** > **Audio**.

Paso 4 Configure sus ajustes de **Editar características de audio**.

Opción	Descripción
Audio de WebEx	• Llamada entrante del usuario y servicio Llamarme: permite a los usuarios asistir a teleconferencias llamando a números de teléfono especificados o recibiendo una llamada Llamarme desde el sistema. • Llamada entrante: permite a los usuarios asistir a teleconferencias llamando a números de teléfono especificados. • Desactivado: desactiva todas las funciones de llamada.
Conexión de voz a través del ordenador	• ACTIVADO • DESACTIVADO

Paso 5 En la sección Editar ajustes de teleconferencia, seleccione el enlace **Editar** en CUCM (Cisco Unified Communication Manager) para cambiar sus ajustes.

Opción	Descripción
CUCM 1 dirección IP	Introduzca el nombre de host o una dirección de IP para su sistema CUCM 1.
CUCM 2 direcciones IP	(Opcional) Introduzca el nombre de host o la dirección IP para su sistema CUCM 2 (servicio de equilibrio de carga). **Nota** CUCM 2 no es obligatorio, pero se recomienda para alta disponibilidad de teleconferencias.
Número de puerto	Introduzca un número de puerto válido. Asegúrese de que el número de puerto coincide con la configuración de CUCM. **Predet.:** 5062
Transporte	Seleccione el tipo de transporte. **Nota** Si selecciona TLS como tipo de transporte, debe importar un certificado de conferencia segura válido para cada uno de sus servidores CUCM, exportar el certificado SSL y cargarlo en CUCM, y configurar el nombre de dominio cualificado completo (FQDN) de su sistema como el nombre de dominio SIP en cada servidor CUCM. Consulte Importación de certificados seguros de teleconferencia, en la página 234 para obtener más información sobre la importación de sus certificados y sobre cómo configurar CUCM en la *Guía de planificación de Cisco WebEx Meetings Server* para obtener más información sobre CUCM. **Predet.:** TCP

Aparecerá el cuadro de diálogo **CUCM (Cisco Unified Communications Manager)**. Complete los campos y seleccione **Continuar**.

Paso 6 En la sección Editar ajustes de teleconferencia, seleccione el enlace **Editar** en Llamar a números de acceso para agregar, cambiar o eliminar sus números de acceso.

a) Seleccione **Agregar** e introduzca una etiqueta de teléfono y un número de teléfono para cada nuevo número de acceso que quiera agregar.
b) Para eliminar un número, seleccione el enlace **Eliminar** al final de la línea.
c) Introduzca la información actualizada en los campos de etiqueta del teléfono y el número de teléfono para todos los números de acceso que desee cambiar.
d) Seleccione **Continuar** cuando haya acabado.

Nota Asegúrese de que solo agrega números que ha configurado en CUCM. Los números que agregue aparecen en las invitaciones de correo electrónico y en su cliente Cisco WebEx Meetings.

Paso 7 Introduzca un nombre de visualización en el cuadro de diálogo **Nombre a mostrar**.

Paso 8 Introduzca un identificador de llamada válido en el cuadro de diálogo **ID de la persona que llama**.

Nota El ID de la persona que llama se limita a los caracteres numéricos y un guión (-), y tiene una longitud máxima de 32 caracteres.

Paso 9 Configure la opción Llamarme de WebEx a (**Predeterminado**: Pulse 1 para conectarse a la reunión). También puede seleccionar esta opción para omitir el requisito de pulsar **1** para conectarse a la reunión.

Nota Cisco no recomienda que seleccione esta opción, a no ser que su sistema de teléfono no pueda enviar el dígito **1**.

Paso 10 Seleccione el **Tono telefónico de entrada y salida**.

- Pitido (predeterminado)
- Sin tono
- Anunciar nombre

Paso 11 Si IPv6 está configurado en su sistema, establezca la configuración **Audio conferencia IPv6** en **Activado** o **Desactivado**. (**Predet.**: Desactivado. Un ajuste **Desactivado** indica que IPv4 es el ajuste).

Nota La opción **Audio conferencia IPv6** no está disponible en los sistemas no configurados para IPv6.

Paso 12 Seleccione **Guardar**.

Paso 13 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Configuración de los ajustes de vídeo

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Vídeo**.

Paso 3 Seleccione **Activado** o **Desactivado** y después seleccione **Guardar**. (**Predet.:** activado).

Configuración de sus ajustes móviles

Nota Android es compatible con Cisco WebEx Meetings Server 2.0 y superior. Las aplicaciones WebEx tanto iOS como Android están activadas de forma predeterminada.

Antes de comenzar

Para configurar los ajustes móviles, debe agregar un acceso público a su sistema durante el despliegue. Consulte Agregar el acceso público a su sistema para obtener más información.

Tenga en cuenta que, si su sistema está configurado para permitir más de un número de acceso de llamada entrante, el sistema asume que el primer número es un número de acceso gratuito y la aplicación móvil intenta este número en primer lugar. La aplicación no se conectará si este número no es accesible desde la red móvil. Asegúrese de que este número es accesible desde la red móvil.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Móvil**.

Paso 3 Configure sus ajustes móviles seleccionando qué plataformas móviles de su sistema son compatibles y después seleccione **Guardar**. (**Predet.:** se selecciona la aplicación WebEx iOS y la aplicación WebEx Android)

Nota
- Debe disponer de una red DMZ para poder utilizar dispositivos móviles Android para acceder a una reunión. Si no dispone de una red DMZ, las opciones de aplicación WebEx iOS y Android aparecen de color gris.
- Las aplicaciones WebEx iOS y Android funcionan del mismo modo que las aplicaciones de escritorio WebEx; desde una intranet interna o Internet externa.

Configuración de la calidad del servicio (QoS)

Los ajustes de punto de código (DSCP) de los servicios diferenciados (DiffServ) determinan la QoS para la señalización de soporte de vídeo y audio, como se define en RFC 2475. Cisco recomienda mantener el valor predeterminado. Los otros valores están disponibles para ocasiones anómalas cuando la red requiere un ajuste de DSCP distinto. Para obtener más información, consulte el capítulo "Infraestructura de red" del Diseño de Red de Referencia de la Solución de Comunicaciones Unificadas de Cisco (SRND) que se aplica a su versión de Cisco Unified Communications Manager en http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html.

A continuación, se especifican los valores predeterminados:

- WebEx Audio (multimedia)
  - Marca de QoS de IPv4: **EF DSCP 101110**
  - Marca de QoS de IPv6: **EF DSCP 101110**

- WebEx Audio (señalización)
  - Marca de QoS de IPv4: **CS3 (precedencia 3) DSCP 011000**

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Calidad de servicio**.

Paso 3 Seleccione los ajustes de marcado QoS utilizando los menús desplegables adecuados y después seleccione **Guardar**.

Acerca de la marca de QoS

Consulte las tablas siguientes para información de marca QoS para despliegues que tienen tráfico que pasa por un servidor de proxy inverso de Internet vs. un despliegue donde el tráfico no pasa por un servidor de proxy inverso de Internet.

Marca QoS en sistemas Cisco WebEx Server con tráfico que pasa por un proxy inverso de Internet

Tráfico	Marca de QoS
Audio SIP—multimedia—CWMS al terminal	Sí
Audio SIP—señalización—CWMS al terminal	Sí
Audio PC—multimedia—CWMS al cliente	No
Audio PC—señalización—CWMS al cliente	No
Audio PC—multimedia—cliente a CWMS	No
Audio PC—señalización—cliente a CWMS	No
Vídeo PC—multimedia—CWMS al cliente	No
Vídeo PC—señalización—CWMS al cliente	No
Vídeo PC—multimedia—cliente a CWMS	No
Vídeo PC—señalización—cliente a CWMS	No

Marca QoS en sistemas Cisco WebEx Server con tráfico que no pasa por un proxy inverso de Internet

Tráfico	Marca de QoS
Audio SIP—multimedia—CWMS al terminal	Sí
Audio SIP—señalización—CWMS al terminal	Sí
Audio PC—multimedia—CWMS al cliente	Sí

Tráfico	Marca de QoS
Audio PC—señalización—CWMS al cliente	Sí
Audio PC—multimedia—cliente a CWMS	No
Audio PC—señalización—cliente a CWMS	No
Vídeo PC—multimedia—CWMS al cliente	Sí
Vídeo PC—señalización—CWMS al cliente	Sí
Vídeo PC—multimedia—cliente a CWMS	No
Vídeo PC—señalización—cliente a CWMS	No

Configuración de contraseñas

Puede configurar los ajustes de contraseña para lo siguiente:

- Contraseñas generales: controla los periodos de caducidad de la contraseña y le permite obligar a los usuarios a cambiar sus contraseñas inmediatamente o en un intervalo especificado.
- Contraseñas de usuario: le permite configurar el nivel de seguridad de la contraseña para cuentas de usuario incluyendo combinación de mayúsculas y minúsculas, longitud, tipos de caracteres y uso, controles de texto de página Web dinámica y definición de una lista de contraseñas inaceptables.
- Contraseñas de reunión: le permite hacer obligatorio el uso de contraseñas para las reuniones y configurar el nivel de seguridad de las contraseñas para las reuniones incluyendo combinación de mayúsculas y minúsculas, longitud, tipos de caracteres y uso, controles de texto de página Web dinámica y definición de una lista de contraseñas inaceptables.

Nota Si SSO está activado en su sistema, los ajustes en las páginas **Contraseña general** y **Contraseña de usuario** y los controles de cambio de contraseña en la página **Editar usuario** no son aplicables a las cuentas de organizador.

Configuración de sus ajustes generales de contraseña

Sus ajustes generales de contraseña le permiten configurar límites de edad de contraseñas y desactivaciones de cuentas. Todos los ajustes de contraseña de esta página son opcionales y pueden cambiarse entre activado (marcado) o desactivado (no marcado).

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Administración de contraseñas** > **Contraseña general**.

Paso 3 (Opcional) Seleccione la casilla de verificación **Desactivar la cuenta de organizador después de número día(s) de inactividad** e introduzca el número de días en el campo de texto. (**Predet.**: Marcado y definido durante 90 días)
Si utiliza los ajustes predeterminados, un usuario se desactiva si no ha organizado ni ha planificado una reunión durante 90 días consecutivos.

Nota Esta función solo se aplica a cuentas de organizador. No puede desactivar una cuenta de administrador utilizando esta función. Para desactivar una cuenta de administrador, consulte Desactivación de usuarios, en la página 139.

Paso 4 (Opcional) Seleccione la casilla de verificación **Obligar a todos los usuarios a modificar la contraseña cada número día(s)** e introduzca el número de días en el campo de texto. (**Predet.**: Desactivado

Paso 5 (Opcional) Seleccione **Obligar a todos los usuarios a cambiar la contraseña la próxima vez que se conecten**. (**Predet.**: Desactivado

Paso 6 Seleccione **Guardar**.

Configuración de los ajustes de contraseña de usuario

Configure las limitaciones y los requisitos de su contraseña de usuario.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Administración de contraseñas** > **Contraseña de usuario**.

Paso 3 Cambie los ajustes de la contraseña de usuario configurando los campos en la página.

Opción	Descripción
Requerir contraseñas seguras para cuentas de usuario	Seleccione esta opción par activar las opciones restantes. **Predet.**: Seleccionado
Longitud mínima de caracteres	Requisito de caracteres mínimos. **Predet.**: Seleccionado y **6** caracteres
Número mínimo de caracteres alfabéticos	Mínimo alfabético (caracteres no numéricos, no especiales) **Predet.**: Seleccionado y **1** carácter

Opción	Descripción
número mínimo de caracteres numéricos	Mínimo numérico (caracteres no alfabéticos, no especiales). **Predet.**: Seleccionado y **1** número
Número mínimo de caracteres especiales	Mínimo especial (caracteres no alfabéticos, no numéricos) **Predet.**: No seleccionado y **1** carácter
Debe incluir mayúsculas y minúsculas	La contraseña debe contener caracteres alfabéticos en letras minúsculas y mayúsculas. **Predet.**: Seleccionado
No permita que un carácter se repita más de tres veces.	No puede repetirse ningún carácter (alfabético, numérico o especial) más de tres veces. **Predet.**: Seleccionado
Lista de contraseñas inaceptables	Lista de contraseñas inaceptables especificada por el administrador. **Predet.**: Not Selected
El nombre de la empresa, el nombre del sitio, la dirección de correo electrónico del usuario, y el nombre de host no son siempre aceptables.	No usar estos nombres específicos. **Predet.**: Seleccionado
No deben incluir *n* contraseñas anteriores.	No utilizar contraseñas usadas anteriormente. Seleccione un número de la lista desplegable menú para especificar el número de contraseñas previas que no puede utilizar. **Predet.**: Seleccionado **Número predeterminado**: 5

Paso 4 Seleccione **Guardar**.

Configuración de sus contraseñas de la reunión

Use esta función para configurar los parámetros de la contraseña de la reunión. La tabla siguiente describe qué usuarios deben introducir una contraseña cuando la reunión está configurada con contraseña.

Contraseña configurada	Contraseña excluida de la invitación por correo electrónico	El creador de la reunión ha iniciado sesión	El organizador ha iniciado sesión	El invitado ha iniciado sesión	El invitado ha iniciado sesión	El invitado no ha iniciado sesión
No	N/D	No se requiere contraseña.	No se requiere contraseña.	No se requiere contraseña.	No se requiere contraseña.	No se requiere contraseña.
Sí	Sí	No se requiere contraseña.	No se requiere contraseña.	No se requiere contraseña.	Se requiere contraseña.	Se requiere contraseña.
Sí	No	No se requiere contraseña.	No se requiere contraseña.	No se requiere contraseña.	Se requiere contraseña. La contraseña puede completarse automáticamente.	Se requiere contraseña. La contraseña puede completarse automáticamente.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Administración de contraseñas** > **Contraseña de la reunión**.

Paso 3 Cambie los ajustes de contraseña de la reunión configurando los campos en la página.

Nota No todas las opciones están seleccionada de manera predeterminada.

Opción	Descripción
Todas las reuniones deben tener contraseñas	Requiere que todas las reuniones tengan contraseñas.
Requerir contraseña segura para reuniones	Seleccione esta opción par activar las opciones restantes.
Longitud mínima de caracteres	Requisito de caracteres mínimos. **Predet.**: 6
Número mínimo de caracteres alfabéticos	Mínimo alfabético (caracteres no numéricos, no especiales) **Predet.**: 1
número mínimo de caracteres numéricos	Mínimo numérico (caracteres no alfabéticos, no especiales). **Predet.**: 1

Opción	Descripción
Número mínimo de caracteres especiales	Mínimo especial (caracteres no alfabéticos, no numéricos) **Predet.**: 1
No debe contener estos caracteres especiales (espacio, \, ', ", /, &, <, >, =, [,])	Seleccione esta opción para prohibir el uso de estos caracteres.
Debe incluir mayúsculas y minúsculas	La contraseña debe contener caracteres alfabéticos en letras minúsculas y mayúsculas.
Lista de contraseñas inaceptables	Lista de contraseñas inaceptables especificada por el administrador.
El nombre de la empresa, el nombre del sitio, la dirección de correo electrónico del usuario, el nombre de host, y el tema de la reunión no son siempre aceptables.	Seleccione esta opción para prohibir el uso de estas palabras o cadenas de caracteres.

Paso 4 Seleccione **Guardar**.

Configuración de sus ajustes de correo electrónico

Puede configurar sus plantillas y ajustes de correo electrónico. Sus plantillas de correo electrónico tienen ajustes predeterminados que puede cambiar si lo desea.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Correo electrónico**.
Se abre la página **Variables**.

Paso 3 Introduzca los valores oportunos en **De nombre**, **De correo electrónico**, **Responder a** (su dirección de correo electrónico) y, a continuación, seleccione **Guardar**.

Nota Si especifica el nombre de una persona en el campo De nombre de la página Variables, las invitaciones a reuniones reflejarán la dirección de correo electrónico del organizador.

Paso 4 Seleccione **Plantillas**. Consulte Acerca de las plantillas de correo electrónico, en la página 205 para ver las descripciones de cada tipo de plantilla.

Aparecerá la página **Plantillas**. Seleccione la pestaña **Común** o **Reuniones**. **Común** se selecciona de forma predeterminada.

Paso 5 Para configurar las plantillas de correo electrónico, seleccione el enlace de plantilla deseado en la pestaña **Común** y **Reuniones**.

Paso 6 Realice los cambios oportunos en la plantilla de correo electrónico y seleccione **Guardar**.

Ejemplo:
Seleccione el enlace de plantilla **Cuenta reactivada** en la pestaña **Común**. Haga los cambios en los campos en el cuadro de diálogo **Cuenta reactivada** y seleccione **Guardar**.
Los valores predeterminados de **De nombre** y **De correo electrónico** y **Responder a** se toman de los ajustes que ha configurado en la página **Variables**.

Nota Si especifica el nombre de una persona en **De nombre** en la página **Variables**, el sistema sustituye automáticamente el nombre de la persona por el URL del sitio de WebEx en todas las invitaciones a reuniones.

Acerca de las plantillas de correo electrónico

Utilice las plantillas de correo electrónico para comunicar eventos importantes a los usuarios. Cada plantilla de correo electrónico tiene variables que debe configurar. Consulte la tabla siguiente para ver descripciones de las variables en cada plantilla.

Hay dos tipos de plantillas de correo electrónico:

- Común: incluye contraseñas perdidas, notificaciones de organizador e invitado, disponibilidad de grabación y otros avisos generales.
- Reuniones: incluye invitaciones de reuniones, cancelaciones, actualizaciones, recordatorios y avisos informativos.

Tabla 3: Plantillas comunes de correo electrónico

Título	Descripción	variables
Activación de AD	Se ha enviado a un usuario después de que se haya activado una cuenta AD.	• %SiteURL% • %DisplayName% • %SSOSignINLink% • %OrgLogo% • %participants% • %Support% • %CustomFooterText% • %Year%

Título	Descripción	variables
Error de sincronización de AD	Se envía a un administrador tras una sincronización fallida.	• %FullName% • %Failure_Reason% • %DownloadLogURL% • %Sync_Start_Time% • %Sync_Completion_Time% • %Users_Added% • %Users_Deactivated% • %Users_Failed_to_Sync% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Sincronización de AD correcta	Se envía a un administrador tras una sincronización correcta.	• %FullName% • %DownloadLogURL% • %Sync_Start_Time% • %Sync_Completion_Time% • %Users_Added% • %Users_Deactivated% • %Users_Failed_to_Sync% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Cuenta reactivada	Se envía a un usuario después de que el administrador reactive la cuenta de usuario.	• %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Título	Descripción	variables
Contraseña olvidada, contraseña cambiada	Se envía a un usuario después de que haya restablecido su contraseña desde un sitio de usuario final.	• %SiteURL% • %DisplayName% • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Contraseña olvidada, restablecer contraseña	Se envía a un usuario después de que haya restablecido su contraseña desde un sitio de usuario final. Este correo electrónico pide al usuario que cree una nueva contraseña.	• %SiteURL% • %DisplayName% • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Invitación de reunión PCN PT: Invitado	Se envía a los invitados de la reunión después de planificar una reunión usando las Herramientas de productividad desde una cuenta PCN.	• %HostName% • %Topic% • %TeleconferencingInfo% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %Meeting Space% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Título	Descripción	variables
Notificación de reunión PCN PT: Organizador	Se envía a un organizador de reunión después de planificar una reunión usando las Herramientas de productividad desde una cuenta PCN.	• %HostName% • %Topic% • %TeleconferencingInfo% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %Meeting Space% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
PT: Notificación de organizador	Se envía a un organizador de reunión después de planificar una reunión usando las Herramientas de productividad.	• %Topic% • %HostName% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%
PT: notificación de invitado	Se envía a los invitados de la reunión después de planificar una reunión usando las Herramientas de productividad.	• %Topic% • %HostName% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%

Título	Descripción	variables
Grabación disponible para el organizador	Se envía al organizador un enlace con la grabación de la reunión.	• %SiteURL% • %OrgLogo% • %DisplayName% • %Topic Name% • %Duration% • %Recording Time% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Correo electrónico de activación de SSO	Se envía después de activar un inicio de sesión único (SSO).	• %SiteURL% • %DisplayName% • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Enviar correo electrónico a todos los usuarios	Envía un correo electrónico a todos los usuarios en el sistema.	• %SiteURL% • %Subject% • %OrgLogo% • %AttendeeName% • %Body% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Título	Descripción	variables
Configurar Cisco WebEx: Android	Informa a los usuarios sobre la aplicación de Cisco WebEx para Android y proporciona un enlace de descarga para la aplicación.	• %SiteURL% • %Subject% • %OrgLogo% • %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Configurar Cisco WebEx: iPhone/iPad	Informa a los usuarios sobre la aplicación de Cisco WebEx para iPhone/iPad y proporciona un enlace de descarga para la aplicación.	• %SiteURL% • %Subject% • %OrgLogo% • %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Compartir grabación	Envía a los asistentes de la reunión seleccionados un enlace para la grabación de la reunión.	• %HostName% • %HostEmail% • %OrgLogo% • %AttendeeName% • %HostName% • %Topic Name% • %Duration% • %Recording Time% • %Personalized Message% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Título	Descripción	variables
Compartir grabación desde MC	Envía a los asistentes de la reunión seleccionados un enlace para la grabación de la reunión. Los asistentes seleccionados por el organizador en el Meeting Center después de seleccionar **Abandonar la reunión**.	• %HostName% • %HostEmail% • %OrgLogo% • %AttendeeName% • %Topic Name% • %Duration% • %Recording Time% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Usuarios: Contraseña modificada	Envía a los usuarios un correo electrónico cuando se modifican sus contraseñas.	• %SiteURL% • %OrgLogo% • %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Mensaje de correo de bienvenida.	Se envía a un nuevo administrador después de crear su cuenta.	• %SiteURL% • %DisplayName% • %SiteURL% • %Support% • %participants% • %CustomFooterText% • %Year%

Tabla 4: Plantillas de correo electrónico de reuniones

Título	Descripción	variables
Invitación de la reunión en curso para un asistente	Se envía a los usuarios cuando un organizador los invita a la reunión mientras la reunión está en curso.	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Invitación de la reunión inmediata para el organizador	Se envía al organizador y a los asistentes cuando el organizador selecciona **Reunirse ahora**.	• %SiteURL% • %Topic% • %HostName% • %Topic_HTML% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Título	Descripción	variables
Reunión cancelada para asistente	Informa al usuario de que una reunión programada se ha cancelado.	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %Topic_HTML% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL% • %CustomFooterText% • %Year%
Reunión cancelada para organizador	Se envía al organizador de la reunión para confirmar la cancelación de una reunión.	• %SiteURL% • %Topic% • %HostName% • %Topic_HTML% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL% • %CustomFooterText% • %Year%

Título	Descripción	variables
Información de reunión actualizada para organizador alternativo	Proporciona información sobre la reunión al organizador alternativo cuando se cambian los ajustes de la reunión.	• %HostName% • %HostEmail% • %Topic% • %OrgLogo% • %AlternateHostName% • %MeetingTime% • %HostName% • %Duration% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Información de reunión actualizada para asistente	Proporciona información sobre la reunión para el invitado de la reunión cuando se cambian los ajustes de la reunión.	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Título	Descripción	variables
Información de la reunión actualizada	Proporciona información sobre la reunión al organizador cuando se cambian los ajustes de la reunión.	• %SiteURL% • %Topic% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Recordatorio de reunión para organizador alternativo	Envía un recordatorio de la reunión al organizador alternativo de esta.	• %HostName% • %HostEmail% • %Topic% • %OrgLogo% • %AlternateHostName% • %MeetingTime% • %HostName% • %Duration% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Título	Descripción	variables
Recordatorio de reunión para organizador	Envía un recordatorio de la reunión al organizador.	• %SiteURL% • %Topic% • %OrgLogo% • %HostName% • %MeetingTime% • %HostName% • %Duration% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Reunión replanificada para organizador alternativo	Envía información sobre la reunión actualizada al organizador alternativo.	• %HostName% • %HostEmail% • %Topic% • %AlternateHostName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Título	Descripción	variables
Reunión replanificada para asistente	Envía información sobre la reunión actualizada a los asistentes.	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Información de reunión para organizador alternativo	Envía una confirmación de la reunión al organizador alternativo.	• %HostName% • %HostEmail% • %Topic% • %AlternateHostName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Título	Descripción	variables
Información de reunión para asistente	Envía una invitación para la reunión a los asistentes.	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Información de reunión para organizador	Envía una confirmación de la reunión al organizador.	• %SiteURL% • %Topic% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Título	Descripción	variables
Recordatorio automático de reunión PCN: Organizador	Envía un recordatorio automático de la invitación al organizador de la reunión (solamente cuentas PCN).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%
Invitación de reunión PCN: Invitado	Envía una invitación de reunión a los invitados (solamente cuentas PCN).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

Título	Descripción	variables
Recordatorio manual de reunión PCN: Organizador	Envía un recordatorio manual de la reunión al organizador de la reunión (solamente cuentas PCN).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%
Recordatorio manual de reunión PCN: Invitado	Envía un recordatorio manual de la reunión a los invitados (solamente cuentas PCN).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

Título	Descripción	variables
Notificación de reunión PCN: Organizador	Envía una notificación de reunión al organizador (solamente cuentas PCN).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%
Invitación a reunión PCN instantánea: Organizador	Envía una notificación de reunión instantánea al organizador (solamente cuentas PCN).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %SiteURL% • %Support%

Título	Descripción	variables
Invitación a reunión PCN en curso: Invitado	Envía una notificación de reunión instantánea a un invitado (solamente cuentas PCN).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%
Cambio de planificación de reunión PCN: Organizador	Envía una notificación de cambio de planificación de reunión al organizador (solamente cuentas PCN).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%

Título	Descripción	variables
Cambio de planificación de reunión PCN: Invitado	Envía una notificación de cambio de planificación a un invitado (solamente cuentas PCN).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%
Reunión PCN replanificada: Invitado	Envía una notificación de replanificación de reunión a un invitado (solamente cuentas PCN).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

Título	Descripción	variables
Reunión PCN cancelada: Organizador	Envía una notificación de cancelación de reunión a un organizador (solamente cuentas PCN).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL%
Reunión PCN cancelada: Invitado	Envía una notificación de cancelación de reunión a un invitado (solamente cuentas PCN).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL%

Configuración de los ajustes de descarga

Procedimiento

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 automáticas periódicas. (**Predet.**: activado).

Nota Si piensa enviar manualmente las herramientas de productividad de WebEx a sus usuarios, le recomendamos que desmarque esta opción.

Paso 4 Seleccione el método de descarga:

- Permitir a los usuarios descargar aplicaciones del escritorio de WebEx
- Trasladar manualmente las Herramientas de productividad y WebEx Meetings al escritorio del usuario

Si selecciona **Permitir a los usuarios descargar aplicaciones del escritorio de WebEx**, puede seleccionar **Guardar** para finalizar la configuración de las descargas. No tiene que hacer nada más. Si selecciona **Enviar**

manualmente WebEx Meetings y las herramientas de productividad al escritorio del usuario, vaya al paso siguiente.

Si selecciona **Enviar manualmente WebEx Meetings y las herramientas de productividad al escritorio del usuario**, aparecerán en la página las secciones Aplicación de WebEx Meetings, Herramientas de productividad y Reproductor de grabación en la red.

Paso 5 Para cada aplicación que desee descargar e instalar, seleccione **Descargar** y a continuación, **Guardar**, para guardar un archivo ZIP en su sistema que contenga instaladores para la aplicación correspondiente.
Cada archivo ZIP contiene los programas de instalación de la aplicación para todos los idiomas y plataformas compatibles.

Paso 6 Seleccione **Guardar** para guardar sus ajustes de descarga.

Acerca de las descargas

Este producto se puede utilizar en PC con Windows en los que los usuarios tengan privilegios de administrador y en los que no. Esta sección proporciona información básica acerca de las descargas. Para obtener información detallada sobre la configuración de las descargas, consulte la sección "Acerca de las descargas" en la Guía de planificación.

En los PC sin privilegios de administrador:

- Recomendamos que active la aplicación WebEx Meetings y las herramientas de productividad en los escritorios de usuario final desconectados antes de informar a los usuarios finales de que se han creado cuentas de usuario para ellos. De esta manera, se garantiza que los usuarios pueden iniciar y unirse a reuniones desde sus exploradores Web y escritorios Windows la primera vez que inicien sesión.
- Puede adquirir los programas de instalación .MSI para cada uno de ellos desde el sitio de Administración en la página **Configuración** > **Descargas**. Consulte Configuración de los ajustes de descarga, en la página 224 para obtener más información.
- Si decide no activar las aplicaciones para sus usuarios, aún pueden acceder a estas aplicaciones desde las páginas de descarga del usuario final. Sin embargo, si sus PC no permiten la instalación de aplicaciones descargadas, no podrán completar el proceso de instalación.
- Cuando los usuarios se unen a reuniones utilizando el explorador Web (la aplicación WebEx Meetings aún puede descargarse bajo demanda), pueden unirse a las reuniones correctamente. Además, la aplicación WebEx Meetings intenta realizar una instalación para acelerar el proceso de iniciar o unirse a futuras reuniones. Se produce un error porque el ordenador no tiene privilegios de administrador.

En los PC con privilegios de administrador:

- Los usuarios pueden descargar e instalar la aplicación WebEx Meetings y las herramientas de productividad desde páginas de descarga del usuario final. No se necesita ninguna acción adicional del administrador.
- Se aconseja a los usuarios instalar las herramientas de productividad la primera vez que inicien sesión.
- La aplicación WebEx Meetings se descarga bajo demanda la primera vez que un usuario se une a una reunión y se instala silenciosamente en el PC del usuario.

Administración de certificados

Los certificados se utilizan para garantizar una comunicación segura entre los componentes de su sistema. Cuando su sistema se despliega por primera vez, se configura con un certificado autofirmado. Si bien un certificado autofirmado puede durar hasta cinco años, le recomendamos encarecidamente que configure certificados validados por una autoridad certificadora. Una autoridad de certificado garantiza que la comunicación entre sus máquinas virtuales está autenticada. Tenga en cuenta que debe instalar un certificado para cada máquina virtual en su sistema.

Se admiten los siguientes tipos de certificados:

- SSL: necesarios en todos los sistemas.
- SSO IdP: para SSO con certificados de proveedor de identidad (IdP).
- Teleconferencia segura: necesario para teleconferencias TLS. Puede configurar hasta dos certificados de audioconferencia seguros, uno por cada sistema CUCM que elija configurar.

Todos los sistemas deben tener un certificado SSL. Este producto admite los siguientes certificados SSL:

- Autofirmados
- Firmados por una autoridad de certificados
- Firmados por una autoridad de certificados externa

No puede actualizar sus certificados. Si agrega máquinas virtuales a su sistema o cambia cualquier máquina virtual existente, debe generar un nuevo certificado para cada máquina virtual de su sistema.

Los certificados SSL pueden dejar de ser válidos por las siguientes razones:

- El tamaño de su sistema ha aumentado, generando el despliegue de nuevas máquinas virtuales. Los nombres de dominio cualificados completos (FQDN) de estas nuevas máquinas virtuales no están presentes en el original del certificado SSL.
- Se ha añadido un sistema de alta disponibilidad, generando el despliegue de nuevas máquinas virtuales. Los FQDN de estas nuevas máquinas virtuales no existen en su certificado SSL original.
- La dirección URL del sitio Cisco WebEx ha cambiado. Esta URL no existe en su certificado SSL original.
- La URL del sitio de administración ha cambiado. Esta URL no existe en su certificado SSL original.
- El FDQN de la máquina virtual de administración ha cambiado. Este FQDN no existe en su certificado SSL original.
- Su certificado SSL actual ha caducado.

Si su certificado SSL deja de ser válido por cualquier razón, el sistema automáticamente generará certificados autofirmados nuevos y se le informará de este cambio por un mensaje de advertencia global en la parte superior de la página del sitio de administración indicando que el SSL ha dejado de ser válido.

Generar certificados SSL

Su sistema debe tener un certificado SSL configurado. Este producto admite los siguientes tipos de certificados SSL:

- Autofirmados
- Firmados por una autoridad de certificados
- Firmados por una autoridad de certificados externa

Generar una solicitud de firma de certificado (CSR)

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Configuración** > **Seguridad** > **Certificados** > **Generar CSR**.

Paso 4 Complete los campos en la página **Generar CSR (solicitud de firma de certificado)**.

Opción	Descripción
Nombre común	Seleccione el certificado **Nombre de asunto alternativo** o el certificado **Comodín**.
Nombres de asunto alternativos **Nota** Esta opción aparece solamente si selecciona **Nombre de asunto alternativo** como su tipo de nombre común.	El nombre de la máquina virtual y del sitio de administración. No se requieren nombres de asunto alternativos si ha seleccionado el nombre común comodín.
Organización	Introduzca el nombre de su organización.
Departamento	Introduzca el nombre de su departamento.
Ciudad	Introduzca su ciudad.
Estado/Provincia	Introduzca su estado o provincia.
País	Seleccione su país.
Tamaño de clave	Seleccione el tamaño de la clave entre las siguientes opciones: • 2048 **Predet.**: 2048 (recomendado)

Paso 5 Seleccione **Generar CSR**.
Aparecerá el cuadro de diálogo **Descargar CSR**.

Paso 6 Seleccione **Descargar**.

Recibirá un archivo ZIP que contiene el CSR y la clave privada asociada. El archivo CSR se llama csr.pem y el archivo de la clave privada se llama csr_private_key. pem.

Paso 7 Haga una copia de seguridad de su sistema utilizando VMware Data Recovery (vSphere 5.0) o VMware vSphere Data Protection (vSphere 5.1). Consulte Creación de una copia de seguridad por medio de VMware vCenter, en la página 4 para obtener más información.

Nota La copia de seguridad de sus sistema conserva la clave privada en caso de que necesite restablecerla.

Paso 8 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Importar un certificado SSL

Puede importar un certificado SSL mediante esta función. Cisco WebEx Meetings Server es compatible con certificados X.509 de codificación PEM y DER y con archivos PKCS12.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Configuración** > **Seguridad** > **Certificados** > **Más opciones** > **Importar certificado SSL/clave privada**.
Si ya tiene un certificado instalado, el sistema le advierte de que importar un nuevo certificado sobrescribirá el existente.

Paso 4 Seleccione **Continuar**.

Paso 5 Seleccione **Examinar** y elija el archivo de certificado.
Deberá seleccionar un certificado o cadena de certificados compatible con X.509. Los tipos válidos son:

- Certificado codificado en PEM/DER: .CER / .CRT / .PEM / .KEY
- Certificado cifrado PKCS12: .P12 / .PFX

Puede importar una cadena de certificado utilizando un archivo PKCS n.º 12 o un archivo único de bloques PEM. Si utiliza un archivo PEM, deberá tener el siguiente formato:

- (Opcional) Si desea cargar una clave privada, ésta deberá ser el primer bloque en el archivo. Puede cifrarse o descifrarse. Deberá tener el formato PKCS n.º 8, cifrado en PEM. Si está cifrado, debe introducir la contraseña para descifrarlo en el campo de frase de contraseña.
- El siguiente elemento debe ser el certificado de la autoridad de certificados intermedia que emitió su certificado en formato X.509 cifrado en PEM.
- Puede incluir tantos certificados intermedios como utilice en su infraestructura. El certificado de la autoridad de certificados raíz no debe incluirse. Si está utilizando una autoridad de certificados privada, debe asegurarse de que el certificado raíz se distribuye a todos los clientes.

Todos los certificados deben cargarse juntos en un archivo. No puede cargar un certificado y después agregar los certificados intermedios más tarde. Es posible que quiera cargar los certificados intermedios si está utilizando una autoridad de certificados que utiliza certificados intermedios y los certificados intermedios no se distribuyen entre sus clientes. Si los carga, bloqueará las advertencias de certificados.

Los archivos PKCS n.º 12 deben tener la extensión .p12. Solo deben contener los certificados y la clave privada (opcional).

Paso 6 Seleccione **Cargar**.
Después de seleccionar **Cargar**, el sistema determinará si su certificado es válido. Un certificado puede no ser válido por las siguientes razones:

- El archivo de certificado no es un archivo de certificado válido.
- El archivo de certificado que ha seleccionado ha caducado.
- Su clave pública deben tener como mínimo 2 048 bits.
- Los dominios del servidor en el certificado no coinciden con la URL del sitio.
- La clave privada generada automáticamente por el sistema no es compatible con el certificado.

Si el certificado es válido, vaya al paso siguiente. Si el certificado no es válido, no podrá cargarlo. Debe seleccionar un certificado válido antes de poder continuar.

Paso 7 (Opcional) Introduzca una frase de contraseña en el campo **Frase de contraseña**.
Nota Se necesita una frase de contraseña para descifrar archivos PKCS12 o una clave privada cifrada (si los archivos .pem cargados contienen la clave privada).

Paso 8 Seleccione **Continuar**.
Su sistema importa su certificado SSL y lo muestra en un cuadro de diálogo de archivo de certificado desplazable.

Paso 9 Seleccione **Hecho**.

Paso 10 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Exportar un certificado SSL

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Seguridad** > **Certificados** > **Más opciones** > **Exportar certificado SSL**.

Paso 3 Guarde el archivo del certificado.

Qué hacer a continuación

Asegúrese de que tanto los administradores como los usuarios finales son capaces de iniciar sesión en la administración o páginas Web sin ver ninguna advertencia de sitio no confiable en el explorador.

Exportar un certificado SSL para dispositivos móviles

Los iPhones o iPads de Apple que ejecuten Apple iOS 5.0 o posterior deben tener un certificado raíz de confianza incorporado. Si su empresa utiliza un certificado autofirmado o si el certificado raíz instalado en Cisco WebEx Meetings Server no figura en la lista de entidades certificadoras de confianza de Apple, debe exportar un certificado SSL y enviarlo por correo electrónico a los usuarios para que lo instalen en sus dispositivos móviles antes de unirse a una reunión de WebEx.

Nota Solo es necesario exportar un certificado SSL si está utilizando un certificado de autofirma. Si está utilizando un certificado firmado de una entidad emisora de certificados de confianza, no tiene que exportar el certificado SSL.

Antes de comenzar

Compruebe que el certificado raíz de confianza preinstalado en el iPhone o iPad de un usuario figura en la lista de entidades certificadoras de confianza de Apple. Consulte http://support.apple.com/kb/ht5012 para obtener información detallada.

Nota Los usuarios deben tener una conexión Internet de alta velocidad activa en sus dispositivos móviles.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Ajustes** > **Seguridad** > **Certificados**.

Paso 3 Copie el nombre del certificado del apartado Certificado SSL.

Paso 4 Seleccione **Más opciones** > **Exportar certificado SSL**.

Paso 5 Guarde el archivo de certificado en el disco duro local.

Paso 6 Adjunte el archivo de certificado guardado a un correo electrónico y envíelo a la cuenta de correo electrónico iOS de cada usuario.

Paso 7 Los usuarios deben abrir el correo electrónico en sus dispositivos móviles y guardar el archivo.

Paso 8 Los usuarios deben instalar el archivo de certificado en sus dispositivos móviles:

a) Toque **Instalar** en la página **Instalar perfil**.
b) Toque **Instalar ahora** en el cuadro de diálogo Perfil sin firmar.
c) Introduzca su contraseña de iOS.
d) Toque **Siguiente**.
e) Toque **Hecho**.

Descarga de su clave privada y su CSR

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Seguridad** > **Más opciones** > **Descargar CSR**.
Aparecerá un cuadro de diálogo preguntándole si desea guardar el archivo CSR.zip que contiene la clave privada y CSR.

Paso 3 Seleccione una ubicación en su sistema para guardar el archivo y seleccione **Aceptar**.

Paso 4 Haga una copia de seguridad de su archivo de clave privada, csr-private-key.pem, en caso de que la necesite posteriormente.

Generación de un certificado autofirmado

Un certificado autofirmado se genera automáticamente después de desplegar su sistema. Le recomendamos que instale un certificado que esté firmado por una autoridad de certificados. Puede generar un certificado autofirmado nuevo en cualquier momento utilizando esta función.

Nota Los usuarios podrían tener problemas para unirse a reuniones si su sistema utiliza un certificado de autofirma, a menos que el administrador del lado del cliente haya configurado su sistema para que pueda utilizar certificados de autofirma.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Configuración** > **Seguridad** > **Certificados** > **Más opciones** > **Generar el certificado autofirmado**.

Paso 4 Rellene los campos en la página **Certificado general autofirmado**.

Opción	Descripción
Nombre del certificado	Introduzca un nombre para su certificado autofirmado. (Obligatorio)
Nombre de asunto X.509	El nombre de host de su sistema. (No se puede configurar)
Organización	Introduzca el nombre de su organización.
Departamento	Introduzca el nombre de su departamento.
Ciudad	Introduzca el nombre de su ciudad.

Opción	Descripción
Estado/Provincia	Introduzca el nombre de su estado o provincia.
País	Seleccione el nombre de su país.

Paso 5 Seleccione **Generar certificado y clave privada**.

Nota Si tiene que usar el mismo certificado SSL después de una actualización general, deberá cargar la clave privada generada con el CSR utilizado para obtener el certificado. La clave privada debe ser el primer bloque en el archivo del certificado.

Su archivo de certificado se genera y aparece.

Paso 6 Seleccione **Hecho**.

Paso 7 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Restauración de un certificado SSL

Si su certificado no es válido o ha realizado una recuperación ante desastres en su sistema, podrá restaurar un certificado SSL utilizando esta función. Cisco WebEx Meetings Server es compatible con certificados X.509 de codificación PEM y DER y con archivos PKCS12.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Configuración** > **Seguridad** > **Certificados** > **Más opciones** > **Importar certificado SSL**.
Si ya tiene un certificado instalado, el sistema le advierte de que importar un nuevo certificado sobrescribirá el existente.

Paso 4 Seleccione **Continuar**.

Paso 5 Seleccione **Examinar** y elija el archivo de certificado.
Deberá seleccionar un certificado o cadena de certificados compatible con X.509. Los tipos válidos son:

- Certificado codificado en PEM/DER: .CER / .CRT / .PEM / .KEY
- Certificado cifrado PKCS12: .P12 / .PFX

Puede importar una cadena de certificado utilizando un archivo PKCS n.º 12 o un archivo único de bloques PEM. Si utiliza un archivo PEM, deberá tener el siguiente formato:

- (Opcional) Si quiere volver a aplicar un par de claves privadas/públicas anterior para una recuperación ante desastres, combine el archivo de clave pública (csr_private_key.pem) y el certificado recibido de su autoridad de certificados (CA) en un único archivo. La clave privada debe ser el primer bloque en el archivo seguido de la clave pública. Puede cifrarse y descifrarse. Debe tener el formato PKCS n.º 8,

cifrado en PEM. Si está cifrado, debe introducir la contraseña para descifrarlo en el campo de frase de contraseña.

- El siguiente elemento debe ser el certificado de la autoridad de certificados intermedia que emitió su certificado en formato X.509 cifrado en PEM.
- Puede incluir tantos certificados intermedios como utilice en su infraestructura. El certificado de la autoridad de certificados raíz no debe incluirse. Si está utilizando una autoridad de certificados privada, debe asegurarse de que el certificado raíz se distribuye a todos los clientes.

Todos los certificados deben cargarse juntos en un archivo. No puede cargar un certificado y después agregar los certificados intermedios más tarde. Es posible que quiera cargar los certificados intermedios si está utilizando una autoridad de certificados que utiliza certificados intermedios y los certificados intermedios no se distribuyen entre sus clientes. Si los carga, bloqueará las advertencias de certificados.

Los archivos PKCS n.º 12 deben tener la extensión .p12. Solo deben contener los certificados y la clave privada (opcional).

Paso 6 Seleccione **Cargar**.
Después de seleccionar **Cargar**, el sistema determinará si su certificado es válido. Un certificado puede no ser válido por las siguientes razones:

- El archivo de certificado no es un archivo de certificado válido.
- El archivo de certificado que ha seleccionado ha caducado.
- Su clave pública deben tener como mínimo 2 048 bits.
- Los dominios del servidor en el certificado no coinciden con la URL del sitio.
- La clave privada generada automáticamente por el sistema no es compatible con el certificado.

Si el certificado es válido, vaya al paso siguiente. Si el certificado no es válido, no podrá cargarlo. Debe seleccionar un certificado válido antes de poder continuar.

Paso 7 (Opcional) Introduzca una frase de contraseña en el campo **Frase de contraseña**.

Nota Se necesita una frase de contraseña para descifrar archivos PKCS12 o una clave privada cifrada (si los archivos .pem cargados contienen la clave privada).

Paso 8 Seleccione **Continuar**.
Su sistema importa su certificado SSL y lo muestra en un cuadro de diálogo de archivo de certificado desplazable.

Paso 9 Seleccione **Continuar** en la página **Certificado SSL** para completar la importación.

Paso 10 Seleccione **Hecho**.

Paso 11 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Importar certificados de SSO IdP

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Seguridad** > **Certificado de IdP SSO**.

Paso 3 Seleccione **Examinar** y elija su certificado de SSO IdP.

Paso 4 Seleccione **Cargar**.
Aparece su archivo de certificado.

Paso 5 Seleccione **Finalizar** para enviar su certificado.

Importación de certificados seguros de teleconferencia

Los certificados de seguridad de teleconferencia solamente se necesitan si la conferencia TLS está activada. Si la conferencia TLS no está activada, esta opción no está disponible.

Antes de comenzar

Los certificados de seguridad de teleconferencia son necesarios para los servidores CUCM cuando TLS está seleccionado como el tipo de transporte en su configuración de audio. Consulte Acerca de configurar sus ajustes de audio, en la página 193 para obtener más información.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Configuración** > **Seguridad** > **Certificados**.
La sección de certificado de seguridad de teleconferencia muestra uno de los siguientes dos mensajes:

- El sistema no requiere certificados de seguridad de teleconferencia porque la teleconferencia TLS no está activada.
- Se requieren certificados de seguridad CUCM para las teleconferencias TLS, que están activadas en este sistema.

Si los certificados de seguridad de teleconferencia son necesarios, se muestra un botón **Importar certificado** para cada servidor CUCM que se debe configurar.

Paso 4 Seleccione **Importar certificado** para CUCM 1.
Aparece la página **Certificado de audio conferencia seguro**.

Paso 5 Introduzca un nombre de certificado.

Paso 6 Seleccione **Examinar** y elija el archivo de certificado.

Nota Si CUCM utiliza certificados autofirmados, utilice el archivo CallManager.pem. Si CUCM utiliza certificados de terceros, utilice el certificado de la entidad emisora de certificados raíz (CA). Consulte "Descarga de certificados CUCM" en la *Guía de planificación* para obtener más información sobre cómo descargar un certificado CUCM en su disco duro local.

Paso 7 Seleccione **Cargar**.
Después de seleccionar **Cargar**, el sistema determinará si su certificado es válido.

Si el certificado es válido, vaya al paso siguiente. Si el certificado no es válido, no podrá cargarlo. Debe seleccionar un certificado válido antes de poder continuar.

Paso 8 Seleccione **Continuar**.
Su sistema importa su certificado SSL y lo muestra en un cuadro de diálogo de archivo de certificado desplazable. Usted recibe una notificación comunicando que ha importado un certificado SSL.

Paso 9 Seleccione **Hecho**.

Paso 10 Vuelva al paso 4 y repita el proceso para el servidor CUCM 2.

Paso 11 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Configuración de la seguridad de sesión de usuario

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Seguridad** > **Sesiones de usuario**.

Paso 3 Rellene los campos en la página **Sesiones de usuario** para definir el tiempo de caducidad de la página Web.

Opción	Descripción
Caducidad de la página Web	Configure los días, horas y minutos antes de que se cierre automáticamente la sesión de los usuarios. **Predet.**: Una hora y 30 minutos.
Caducidad de las herramientas de productividad o móviles (SSO)	Configure los días, horas y minutos antes de que se cierre automáticamente la sesión de los usuarios. **Predet.**: 14 días **Nota** Este campo solo aparece si se ha configurado SSO.

Paso 4 Seleccione **Guardar**.

Configurar los ajustes de autenticación única (SSO)

Configurar el SSO permite a los usuarios finales que inicien sesión en el sistema utilizando sus credenciales corporativas, dándole así una forma de integrar el producto con su directorio empresarial. También puede configurar SSO para crear o administrar las cuentas de usuario en el momento cuando los usuarios intentan iniciar sesión.

Nota Configurar el SSO puede ser una operación compleja y recomendamos encarecidamente que se ponga en contacto con su socio del canal Cisco o con los servicios avanzados Cisco antes de continuar.

Antes de comenzar

- Antes de activar la función de autenticación única, tendrá que generar un conjunto de claves públicas y privadas y un certificado X.509 que contenga la clave pública. Cuando tenga una clave pública o certificado, deberá cargarla en la sección Administración de certificados, en la página 226.

  Nota Después de activar la SSO, las credenciales de usuario son gestionadas por su sistema de autenticación corporativa. Algunas funciones de gestión de contraseñas no se aplican a sus usuarios. Consulte Configuración de contraseñas, en la página 200 y Edición de usuarios, en la página 138 para obtener más información. Tenga en cuenta que aunque los administradores también son usuarios finales, los administradores no iniciar sesión con SSO. Inician sesión utilizando sus credenciales de administrador para este producto.

- Configure un certificado SSO IdP para usar esta función. Consulte Importar certificados de SSO IdP, en la página 234 para obtener más información.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Seguridad** > **SSO única**.

Paso 3 Después de generar las claves públicas y privadas y un certificado X,509, como se describe en los requisitos previos, seleccione **Continuar**.

Paso 4 Seleccione su método de iniciación:

- Inicio de sesión iniciado por el SP (proveedor de servicios): los usuarios seleccionan un enlace al proveedor de servicios y se redirigen temporalmente a un proveedor de identidad para la autenticación. A continuación, los usuarios vuelven al enlace que han solicitado inicialmente.
- Inicio de sesión iniciado por el proveedor de identidad: los usuarios empiezan en su proveedor de identidad, inician sesión y después son redirigidos a una página de bienvenida del proveedor de servicios.

Paso 5 Rellene los campos y seleccione sus opciones en la página **Configuración SSO**:

Nota Consulte el archivo de configuración de IdP para completar los campos IdP. Seleccione en enlace **Certificado de IdP**.

Campo	Descripción
SP (proveedor de servicios) iniciado	Seleccione esta opción para el inicio de sesión iniciado por el proveedor de servicios.
AuthnRequest firmado	Seleccione esta opción para requerir que el mensaje AuthRequest debe estar firmado por la clave privada del proveedor de servicios. **Nota** Debe selecciona esta opción si quiere que su archivo de metadatos SAML exportado se incluya en el certificado SSL de su sitio.
Destino	La URL de implementación de SAML 2.0 de IdP que recibe solicitudes de autenticación para su procesamiento. **Nota** Este campo aparece únicamente cuando se selecciona **AuthnRequest firmado**.
IdP (proveedor de identidad) iniciado	Seleccione esta opción para el inicio de sesión iniciado por el proveedor de identidad.
Nombre de parámetro de URL de página de destino	Su sistema se redirige a esta URL cuando el SSO es correcto. **Predet.**: Source **Nota** En un sistema iniciado por IdP, la URL debe ser una URL combinada en el formato siguiente: su URL de inicio de sesión de servicio, "?" o "&," el parámetro de URL de la página de destino, "=" (si no está presente), y la URL de destino.
Emisor para SAML (ID de SP)	Introduzca el mismo ID del SP para IdP. Consulte el protocolo SAML2.
Emisor para SAML (ID de IdP)	Introduzca el mismo ID configurado para IdP. Consulte el protocolo SAML2.
URL de inicio de sesión en el servicio SSO de cliente	La URL de consumo de aserción para SAML2 en IdP.

Campo	Descripción
Formato de NameID	Seleccione el mismo formato de NameID que ha definido en IdP. El NameID es el formato en el que envía el ID de usuario en la solicitud de cierre de sesión individual y aserción desde Cisco WebEx. Consulte el protocolo SAML para más información. Le recomendamos que defina la dirección de correo electrónico como su ID de nombre. De esta forma, se facilita el proceso de utilizar SSO para los usuarios finales que ya han definido sus cuentas en función de su dirección de correo electrónico en el sistema. La utilización de otros formatos de ID de nombre es compatible, pero no se recomienda. Si utiliza un formato distinto de una dirección de correo electrónico, los usuarios no podrán iniciar sesión en un sitio de WebEx si el SSO está desactivado. **Predet.**: Sin especificar
AuthnContextClassRef	Introduzca el valor que ha configurado en IdP. AuthnContextClassRef es el valor que aparece en el mensaje AuthnRequest. **Predet.**: urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
URL de la página de destino de WebEx predeterminada	Su sistema se redirige a esta URL cuando el SSO es correcto. La página predeterminada es la página de la reunión de Cisco WebEx que es la misma que con el inicio de sesión normal.
URL de error de SSO del cliente	Su sistema se redirige a esta URL cuando el SSO es incorrecto. De forma predeterminada, la página de error es una página de error común de Cisco WebEx.
Cierre de sesión único	Esta opción habilita el cierre de sesión único que se ha definido por el protocolo SAML2. Si ha seleccionado la opción SSO pero no ha seleccionado la opción de cierre de sesión único, la opción de cerrar sesión no aparecerá en las páginas del usuario final. Elimine la selección de esta opción para ADFS 2.0. **Nota** SLO iniciado por IdP no es compatible con esta versión.
URL de desconexión del servicio SSO de cliente **Nota** Esta opción solamente aparece cuando Cierre de sesión único está seleccionado .	Introduzca la URL de consumo de aserción para SAML2 en IdP.

Campo	Descripción
Creación automática de cuenta	Los usuarios sin una cuenta de Cisco WebEx no pueden iniciar sesión. Si selecciona esta opción, se crea una cuenta automáticamente para nuevos usuarios cuando intentan iniciar sesión.
Actualización automática de cuenta	Si selecciona esta opción, la información del usuario se actualiza cuando exista una "updateTimeStamp" en la aserción SAML2 con información de usuario más reciente que los datos actuales en Cisco WebEx.
Quite el sufijo de dominio de uid para UPN del directorio activo	Seleccione esta opción para autenticar a usuarios sin un sufijo de dominio. La opción **Eliminar el sufijo de dominio de UID para UPN del directorio activo** funciona en los casos siguientes: • El formato NameId es un correo electrónico, y el formato UID es el nombre de sujeto X509 o el nombre principal de usuario (UPN). • El formato NameId es el nombre de sujeto X509 o el UPN.

Paso 6 Seleccione **Activar SSO**.
Aparece la página **Revisar configuración de SSO**. Revise los ajustes y seleccione **Guardar**.

Desactivar SSO

Antes de comenzar

Desactivar SSO desactivará la capacidad del usuario para iniciar sesión con sus credenciales de empresa. No olvide informar a sus usuarios de que está desactivando SSO y que podrán seguir iniciando sesión con sus credenciales de Cisco WebEx.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Seguridad** > **SSO única**.

Paso 3 Buscar la frase "Si desea desactivar SSO haga clic aquí". Seleccione el enlace **haga clic aquí**.

Paso 4 Seleccione **Desactivar SSO** para confirmar.
Aparece la página **SSO federado** con un cartel que le informa de que ha desactivado SSO.

Configuración de las funciones de la nube

Puede configurar su sistema para que los usuarios utilicen una versión única de las herramientas de productividad de Cisco WebEx que pueden usarse con las cuentas de Cisco WebEx Meetings Server y SaaS WebEx, o para ver vídeos formativos alojados en línea por Cisco WebEx.

Nota Su sistema admite Cisco WebEx SaaS, versiones WBS27 y WBS28, y Cisco WebEx Meetings 1.2.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Configuración** > **Seguridad** > **Características de la nube**.

Paso 3 (Opcional) Seleccione la casilla de verificación **Permite a los usuarios iniciar una sesión en las cuentas de SaaS WebEx desde las Herramientas de productividad de WebEx**.

Paso 4 Seleccione **Guardar**.

Configuración de la seguridad de la máquina virtual

Las funciones de seguridad de su máquina virtual incluyen la capacidad de actualizar sus claves de cifrado y activar o desactivar cifrados que cumplan el FIPS.

Actualizar sus claves de cifrado

Cisco WebEx Meetings Server utiliza claves de cifrado generadas internamente para asegurar todas las comunicaciones entre las máquinas virtuales en su sistema. Utilice esta función para actualizar sus claves de cifrado periódicamente.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Configuración** > **Seguridad** > **Máquinas virtuales**.

Paso 4 Seleccione **Actualizar claves de cifrado**.

Paso 5 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Acerca de FIPS

La Norma federal de procesamiento de la información (FIPS, por sus siglas en inglés) 140 es una normativa gubernamental de EE.UU. y Canadá que especifica los requisitos de seguridad para los módulos criptográficos. Un módulo criptográfico es un "conjunto de hardware, software o firmware que implementa las funciones de seguridad aprobadas (incluidos los algoritmos criptográficos y la generación de claves) y que está contenido dentro del límite criptográfico". El módulo criptográfico es lo que se está validando.

Requisitos de FIPS 140

En un nivel muy alto, los requisitos de FIPS 140 se aplican a las siguientes características del módulo:

- Implementación de algoritmos aprobados por FIPS
- Gestión específica del ciclo de vida de las claves
- Generación aprobada de números aleatorios
- Pruebas automáticas de algoritmos criptográficos, integridad de imagen, y generadores de números aleatorios (RNG)

Cisco WebEx Meetings Server utiliza CiscoSSL 2.0 para alcanzar el nivel 2 de cumplimiento de FIPS 140-2.

Con FIPS activado

La activación de FIPS podría dar lugar a una menor compatibilidad con los exploradores web y los sistemas operativos más habituales. Los síntomas podrían ser, entre otros, problemas para iniciar sesión en el sistema, errores 404, así como problemas para iniciar reuniones y entrar en ellas.

Cisco recomienda que realice las siguientes acciones:

- Asegúrese de que sus ordenadores Windows funcionan con Windows XP SP3 o superior.
- Actualice todos los ordenadores Windows a Microsoft Internet Explorer 8 o superior, independientemente de si el explorador Web preferido de sus usuarios es Internet Explorer, Mozilla Firefox o Google Chrome. Sus usuarios deben tener Internet Explorer 8 en todos los ordenadores porque nuestros clientes con FIPS activado (Reuniones de Cisco WebEx, herramientas de productividad y Reproductor de grabación de WebEx) utilizan bibliotecas de sistema con FIPS activado que sólo están disponibles en Internet Explorer 8 y superiores.
- Ajuste la **Configuración de Internet** en los ordenadores de todos los usuarios a cifrado TLS. En el escritorio de su ordenador, seleccione **Panel de control** > **Opciones de Internet** > **Avanzado** > **Seguridad** > **Usar TLS 1.0** y **Usar TLS 1.2**. Recomendamos seleccionar ambas opciones para maximizar la compatibilidad, pero debe seleccionar al menos Utilizar TLS 1.0.
- Si sus usuarios planean organizar reuniones para invitados (por ejemplo, usuarios que no trabajan para su empresa) deberá informar a sus usuarios invitados de que tienen que actualizar manualmente los sistemas operativos y los exploradores antes de unirse a sus reuniones tal y como se describe más arriba . Si no realizan los pasos anteriores, experimentarán problemas de compatibilidad. Le recomendamos que incluya las instrucciones anteriores en sus invitaciones a reuniones. Puede hacerlo editando las invitaciones a reuniones adecuadas disponibles en su sitio Administración del sitio en **Configuración** > **Correo electrónico** > **Plantillas.**

Activación del cifrado compatible con FIPS

Utilice esta función para habilitar la configuración de cifrado compatible con el estándar federal de procesamiento de información (FIPS).

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Configuración** > **Seguridad** > **Máquinas virtuales**.

Paso 4 Seleccione **Activar** para activar el cifrado compatible con FIPS y **Continuar** para confirmar.
El cifrado compatible con FIPS está configurado en su sistema.

Paso 5 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

Desactivación del cifrado compatible con FIPS

Utilice esta función para desactivar el cifrado compatible con el estándar federal de procesamiento de información (FIPS) en su sistema.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Configuración** > **Seguridad** > **Máquinas virtuales**.

Paso 4 Seleccione **Desactivar** para desactivar el cifrado compatible con FIPS y **Continuar** para confirmar.
El cifrado compatible con FIPS está deshabilitada en su sistema.

Paso 5 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.

CAPÍTULO 15

Gestionar sus informes

Puede ver los informes mensuales y personalizarlos para intervalos de fechas específicos. Sus informes utilizan los ajustes de idioma, configuración regional y zona horaria configurados en la página **Información de la empresa**. Consulte Configuración de la información de su empresa, en la página 188 para obtener más información.

Nota Cuando su sistema está recién desplegado o recientemente actualizado, no hay datos disponibles para cualquiera de los informes excepto el informe detalles personalizados hasta el final del primer mes. En ese caso, los enlaces **Descargar** y todos los demás informes descritos en esta sección no estarán disponibles hasta después del final del primer mes.

- Descargar informes mensuales, página 243
- Acerca de los informes mensuales, página 244
- Generar informes detallados personalizados, página 246
- Acerca de los informes de detalles personalizados, página 246

Descargar informes mensuales

Puede ver y descargar los informes resumidos mensuales desde esta página. Los informes se visualizan en formato PDF.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Informes**.

Paso 3 Haga clic en el enlace **Descargar** para el informe mensual que desee ver.

Acerca de los informes mensuales

Su informe resumido mensual contiene las secciones siguientes:

Informe de resumen del sistema

Su informe resumido del sistema incluye los informes siguientes:

- Adopción de servicio: este informe muestra un gráfico que especifica el número de organizadores y asistentes únicos en los últimos tres meses, así como la tasa de crecimiento prevista en los próximos tres meses.
- Licencias de usuario: este informe muestra el porcentaje de licencias compradas que está usando y un gráfico que especifica el número de licencias utilizadas en los últimos tres meses y la tasa de crecimiento prevista para los próximos tres meses. Puede utilizar estos números para predecir el uso futuro de las licencias y ajustar las compras de licencias en función de los resultados. Consulte Tramitación de licencias utilizando el Administrador de licencias, en la página 183 para obtener más información.
- Tamaño del sistema: este informe muestra el máximo de participantes de su reunión y el porcentaje del tamaño del sistema que ha consumido el uso máximo. El gráfico muestra los picos de participantes máximos de la reunión en los tres últimos meses y la tasa de crecimiento prevista para los siguientes tres meses.
- Almacenamiento: este informe muestra el uso de almacenamiento de su archivo de datos y las grabaciones a modo de porcentaje del espacio de almacenamiento total en gigabytes (GB). El gráfico muestra el almacenamiento total en los últimos tres meses y la tasa de crecimiento prevista para los siguientes tres meses. Utilice este informe para supervisar su uso de almacenamiento. Si necesita agregar espacio de almacenamiento adicional, debe copiar manualmente las grabaciones y el archivo de datos de almacenamiento existentes a su nuevo servidor de almacenamiento antes de activarlo.

  Nota Este informe solamente aparece si ha configurado un servidor de almacenamiento. Consulte Configuración de un servidor de almacenamiento, en la página 164 para obtener más información.

- Red: este informe muestra lo siguiente.
  - Su consumo máximo de ancho de banda de red en Mbps.
  - Gráfico que muestra el consumo máximo de ancho de banda de red en Mbps en los últimos tres meses y la tasa de crecimiento prevista para los siguientes tres meses (la barra roja indica el ancho de banda máximo de la red).
  - Gráfico circular que indica el porcentaje de ancho de banda consumido por cada uno de los recursos de su sistema.
- Tiempo de inactividad previsto y desconexiones imprevistas de su sistema: este informe muestra lo siguiente.
  - El tiempo de actividad medio del sistema en los últimos tres meses.
  - El promedio de las desconexiones imprevistas del sistema en los últimos tres meses.
  - El promedio de reuniones interrumpidas debido a desconexiones en los últimos tres meses.

- Gráfico que muestra los tiempos de inactividad planificados y las desconexiones imprevistas en los últimos tres meses y la tasa de crecimiento prevista para los siguientes tres meses.

Nota El aumento de los tiempos de inactividad suele asociarse al aumento del uso. No olvide comprar sus estadísticas de tiempos de inactividad con las estadísticas de uso mostradas en otros informes.

Informe de resumen de reuniones

Su informe resumido de la reunión contiene los informes siguientes:

- Estado de la reunión: este informe muestra un gráfico que ilustra el estado de la reunión en el último mes, el porcentaje de reuniones que han experimentado problemas y el número total de reuniones celebradas durante el mes. Para saber el estado de la reunión en tiempo real, consulte su escritorio. Consulte Acerca de su escritorio, en la página 115 para obtener más información.
- Tamaño de la reunión: este informe muestra un gráfico que muestra los tamaños de las reuniones celebradas en su sistema en el último mes, un desglose de los tamaños de las reuniones e información detallada sobre la reunión más larga celebrada durante el mes.
- Uso de funciones de la reunión: este informe muestra lo siguiente.
  - La función más utilizada en el último mes, incluyendo el número total de minutos durante los cuales se utilizó la función.
  - La función con el crecimiento más rápido en su sistema en el último mes, incluyendo la tasa de crecimiento.
  - Un gráfico que muestra el uso en minutos para cada función de su sistema.
  - Un gráfico que muestra la tasa de crecimiento de la función con el crecimiento más rápido en su sistema.
- Dominios de correo electrónicos de participantes más activos: este informe muestra lo siguiente.
  - Un gráfico que muestra los dominios de correo electrónico de participantes más activos.
  - Un desglose de los dominios de correo electrónico de participantes.
  - Una lista de los tres dominios de correo electrónico más usados por los participantes de la reunión en su sistema.
- Fecha y hora punta: este informe muestra dos gráficos. El primer gráfico muestra el día más ocupado de la semana en el último mes. El segundo gráfico muestra la hora más ocupada del día en su sistema en el último mes.

Generar informes detallados personalizados

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Informes** > **Personalizar el informe**.

Paso 3 Seleccione el intervalo de fechas de los informes que quiere ver y seleccione **Enviar**.
El mes predeterminado es el más reciente. Puede seleccionar un intervalo de fechas que se extienda hasta seis meses atrás.

Aparece la página **Solicitud de informe personalizado enviado** mostrando las fechas de su informe personalizado. Se envía un correo electrónico con un enlace a su informe personalizado en formato CSV.

Paso 4 Seleccione **Hecho**.

Acerca de los informes de detalles personalizados

Cuando genere informes detallados personalizados recibirá un correo electrónico con un archivo que tiene los informes siguientes en el formato CSV:

- Informe de intentos de fraude: en este informe se muestran todos los intentos de acceso por telefonía fallidos en los que la persona que llama introduce códigos de acceso de organizador o participante incorrectos o un PIN de organizador incorrecto tres veces al intentar iniciar o unirse a una reunión de conferencia personal. El informe contiene los campos siguientes:
  - Número de acceso llamado: número de llamada directa de Cisco WebEx para iniciar o unirse a una reunión de conferencia personal.
  - Número de llamada: número de teléfono utilizado para realizar la llamada.
  - Hora de inicio de llamada: fecha y hora de la llamada.
  - Primer código de acceso intentado: primer código de acceso no válido introducido por la persona que llama.
  - Correo electrónico del propietario del primer código de acceso (si está disponible): dirección de correo electrónico del usuario asociado con el primer código de acceso no válido, si el código de acceso está asociado a una cuenta válida de Cisco WebEx Meetings Server.
  - Segundo código de acceso intentado: segundo código de acceso no válido introducido por la persona que llama.
  - Correo electrónico del propietario del segundo código de acceso (si está disponible): dirección de correo electrónico del usuario asociado con el segundo código de acceso no válido, si el código de acceso está asociado a una cuenta válida de Cisco WebEx Meetings Server.
  - Tercer código de acceso intentado: tercer código de acceso no válido introducido por la persona que llama.

  - Correo electrónico del propietario del tercer código de acceso (si está disponible): dirección de correo electrónico del usuario asociado con el tercer código de acceso no válido, si el código de acceso está asociado a una cuenta válida de Cisco WebEx Meetings Server.

- Informe de reunión: este informe contiene información sobre todas las reuniones que se han celebrado durante el periodo de tiempo especificado, e incluye los campos siguientes:
  - ID de reunión: el ID de conferencia único generado por su sistema cuando se programa la reunión.
  - Número de reunión: el número de reunión de Cisco WebEx.
  - Asunto: el nombre de la reunión configurada por el organizador.
  - Nombre de organizador: el organizador de la reunión.
  - Hora de inicio: la hora de inicio y la fecha de inicio de la reunión.
  - Duración: la duración de la reunión en minutos.
  - Número de participantes: número de participantes incluidos los organizadores.
  - Estado
  - Número de minutos de audio de realización de llamada
  - Número de minutos de audio de devolución de llamada
  - Número de minutos de VoIP
  - Número de minutos de vídeo
  - Número de minutos de grabación
  - Intervalo de grabación: especifica la hora de inicio y detención de cada una de las grabaciones creadas durante la reunión.
  - Número de minutos de uso compartido en Web: número total de minutos que todos los participantes pasan en la reunión Web (por ejemplo, si tres participantes asisten a la parte Web de una reunión que dura 10 minutos, el número de minutos de uso compartido en Web es 30).
  - Participantes: una lista de los participantes de la reunión.
  - Plataforma/explorador de host: versión del sistema operativo y explorador que utilizó el organizador cuando éste inició una reunión de Cisco WebEx.
  - Dirección IP del host: dirección IP utilizada por el organizador cuando éste inició una reunión de Cisco WebEx.
  - Códigos de seguimiento: los códigos de seguimiento aplicados por el organizador cuando programa la reunión.

- Informe de uso de ancho de banda de red: este informe contiene una lista del consumo de ancho de banda de red para cada día en el periodo especificado para cada una de las funciones siguientes:
  - Consumo de ancho de banda máximo para audio (Mbps)
  - Consumo de ancho de banda máximo para audio VoIP (Mbps)
  - Consumo de ancho de banda máximo para vídeo (Mbps)
  - Consumo de ancho de banda máximo para uso compartido en Web (Mbps)

Un consumo de 0 (cero) indica que la función no se ha utilizado en esa fecha. Se muestra un consumo de menos de 1 si se ha consumido menos de 1 Mbps en la fecha especificada.

El consumo de ancho de banda de la red para el vídeo incluye vídeo de cámaras y el uso compartido de archivos de vídeo de reuniones Web. Si el vídeo está desactivado para el sitio, no puede activar una cámara para el vídeo, pero puede seguir compartiendo archivos de vídeo. Esto genera algo de consumo en el ancho de banda de la red para el vídeo que se incluye en los informes. Esta es la única situación que genera consumo de ancho de banda de la red para el vídeo cuando el vídeo está desactivado para un sitio.

- Informe de uso de capacidad de almacenamiento: este informe muestra el espacio de disco total utilizado en la fecha especificada y el número de reuniones grabadas para cada fecha.

Nota Este informe solamente aparece si ha configurado un servidor de almacenamiento. Consulte Configuración de un servidor de almacenamiento para obtener más información.

- Informe de participantes: este informe muestra el historial de reuniones, la hora en que se inició cada una de ellas y el código de seguimiento aplicado en cada reunión.
  - ID de reunión: ID de conferencia único generado por su sistema cuando se programa la reunión.
  - Nombre de conferencia: nombre de la reunión que el organizador ha especificado en el campo **Qué** al planificar una reunión.
  - Nombre de usuario: nombre de usuario del organizador.
  - Hora de unión: fecha y hora en la que un usuario se une a una reunión de Cisco WebEx.
  - Hora de salida: fecha y hora en la que un usuario abandona una reunión de Cisco WebEx.
  - Duración: tiempo, en minutos, que un usuario participa en una reunión de Cisco WebEx.
  - Plataforma/explorador: versión del sistema operativo y explorador utilizados por un organizador cuando éste inicia una reunión de Cisco WebEx.
  - Dirección IP del cliente: dirección IP del cliente de WebEx utilizado por un organizador o participante para iniciar o asistir a una reunión de Cisco WebEx.
  - Hora inicial de sesión: hora en la que se inicia la sesión.
  - Hora final de sesión: hora en la que finaliza la sesión.
  - Tipo de sesión: el tipo de sesión puede ser vídeo (uso compartido en Web), VoIP (conexión telefónica), llamada o devolución de llamada.
  - Duración de sesión: tiempo que ha durado la sesión.
  - Número de teléfono: número del teléfono utilizado para realizar la llamada a la reunión de WebEx.
  - Tel. Servidor: servidor de teléfonos.

- Informe de tiempo de inactividad del sistema: este informe contiene la información de inactividad del sistema para el periodo especificado e incluye los campos siguientes:
  - Categoría: fuera de servicio o mantenimiento. Fuera de servicio indica una interrupción en la red. Mantenimiento indica una ventana de mantenimiento planificada.
  - Servicio: enumera las características afectadas.

- Inicio de inactividad: fecha y hora en que empezó la inactividad.
- Fin de inactividad: fecha y hora en que finalizó la inactividad.
- Número de reuniones interrumpidas: especifica el número de reuniones interrumpidas. Este campo está en blanco para los tiempos de inactividad de mantenimiento porque dichos tiempos están planificados. Si no se han programado reuniones durante un tiempo de inactividad fuera de servicio, el número es 0.

- Informe de uso de licencias de usuario: hay dos versiones de este informe. Una versión muestra el uso de licencias para los 30 días anteriores y se titula UserLicenseUtilizationReportForLastMonth.csv, y la otra versión muestra el uso de licencias para el mes actual (el primer día del mes hasta el día actual) y se titula UserLicenseUtilizationForThisMonth.csv. Cada uno de esos informes incluye los campos siguientes:
  - Nombre de usuario: el nombre de usuario del organizador de la reunión.
  - Dirección de correo electrónico: la dirección de correo electrónico del organizador de la reunión.
  - ID de reunión: el ID de conferencia único generado por su sistema cuando se programa la reunión.
  - Número de reunión: el número de reunión de Cisco WebEx.
  - Hora de inicio: la hora de inicio y la fecha de inicio de la reunión.
  - Reunión simultánea: indica el número de reuniones simultáneas programadas por el mismo usuario. Cada reunión simultánea que se registra genera una línea adicional que se agrega a este informe para el usuario que ha programado la reunión simultánea.

CAPÍTULO 16

Usar las funciones de soporte

- Personalizar el registro, página 251
- Definir una cuenta de Remote Support, página 252
- Desactivación de una cuenta de Remote Support, página 253
- Utilización de la prueba de las reuniones, página 254
- Utilización de la prueba de recursos del sistema, página 254

Personalizar el registro

Puede generar archivos de registro que muestren la actividad de todo su sistema o solo para reuniones específicas. Utilice los archivos de registro para solucionar problemas o para enviar una solicitud al Centro de asistencia técnica (TAC) de Cisco cuando necesite ayuda.

Nota Le recomendamos que genere su archivo de registro en horario no laborable. El gran tamaño del archivo de registro puede afectar al rendimiento del sistema.

Nota Los datos de registro se conservan durante 30 días. Sin embargo, si actualiza un despliegue de Cisco WebEx Meetings Server 1.x a la versión 2.0, los datos del registro de la versión 1.x no se transferirán al sistema Cisco WebEx Meetings Server 2.0 y, por lo tanto, no estarán disponibles después de completarse la actualización a la versión 2.0.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Soporte** > **Registros**.

Paso 3 Rellene los campos en la página **Personalizar el registro** y seleccione **Enviar**.

Campo	Descripción
ID de caso (opcional)	Introduzca el ID de caso del TAC de Cisco. Los ID de caso los facilita el TAC cuando le asiste con un caso. La utilización de esta función le permite asociar los registros que ha generado con el ID de caso.
Tipo	Seleccione el tipo de registro. Puede seleccionar **Registro general del sistema** o **Registro de una reunión concreta**. Un Registro de todo el sistema contiene toda la información de registro especificada en el sistema y el Registro de reunión recauda registros y datos de la base de datos para procesamiento de MATS. **Predet.**: Registro general del sistema
Intervalo	Seleccione el intervalo para su registro. Debe especificar la fecha de inicio y fin y la hora de inicio y fin para su registro. El límite es 24 horas. Los datos de registro solamente están disponibles desde los últimos 30 días. **Nota** Para generar registros de más de 24 horas tiene que repetir esta operación, seleccionando rangos de día-hora consecutivamente. Cada operación resulta en la creación de un archivo de registro separado. Por ejemplo: Para generar registros desde el 1 de enero hasta el 3 de enero, seleccione primero un rango de fechas desde el 1 hasta el 2 de enero, seleccione **Enviar** y descargue el archivo del registro creado. Después seleccione un rango de fechas desde el 2 al 3 de enero. Seleccione **Enviar** y descargue el archivo del registro creado.
Incluir	Especifique los datos que desea incluir en su registro. **Predet.**: Todas las Actividades

Se genera el registro y se le envía un correo electrónico que contiene un enlace para descargarlo.

Definir una cuenta de Remote Support

Si tiene problemas técnicos y se ha puesto en contacto con el TAC de Cisco para obtener ayuda, puede configurar una cuenta de Remote Support para conceder a un representante del TAC acceso temporal a su

sistema. Este producto no proporciona acceso CLI a administradores y, por tanto, requiere que un representante del TAC solucione algunos problemas.

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Soporte** > **Cuenta de Remote Support**.

Paso 3 Seleccione **Activar Remote Support**.

Paso 4 Rellene los campos en la página **Cuenta de Remote Support** y seleccione **Crear cuenta**.

Campo	Descripción
Nombre de cuenta de Remote Support	Introduzca un nombre para su cuenta de Remote Support (6-30 caracteres).
Vida de la cuenta	Especifique la cuenta de la cuenta en horas. El máximo es de 720 horas (30 días).
Versión del descodificador	Seleccione **2- Webex Meetings Server**. **Nota** Si tiene una cuenta de Remote Support que estaba activa antes del lanzamiento de Cisco WebEx Meetings Server Versión 1.5, no necesita configurar este ajuste.

Aparece el cuadro de diálogo **Creación de cuenta de Remote Support** en el que se muestra el código de frase de contraseña. Póngase en contacto con Cisco TAC y proporcione el nombre de cuenta de Remote Support y el código de frase de contraseña para que el personal de soporte de Cisco pueda acceder a su sistema.

Desactivación de una cuenta de Remote Support

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Soporte** > **Cuenta de Remote Support**.

Paso 3 Junto al mensaje de estado, "Remote Support activado", seleccione el enlace **Desactivarla**.
Su cuenta de Remote Support está desactivada.

Utilización de la prueba de las reuniones

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Soporte** > **Prueba de reuniones**.

Paso 3 Seleccione **Siguiente**.
Su sistema ejecuta una prueba de reuniones y comprueba su capacidad para programar, iniciar y unirse a reuniones. Los resultados de la prueba aparecerán en unos minutos.

Utilización de la prueba de recursos del sistema

Procedimiento

Paso 1 Inicie sesión en el sitio de administración.

Paso 2 Seleccione **Activar el modo de mantenimiento** y **Continuar** para confirmar.

Paso 3 Seleccione **Soporte** > **Prueba de recursos del sistema**.

Paso 4 Seleccione **Siguiente**.
Los resultados de la prueba se publican para lo siguiente:

- CPU, memoria, red, y almacenamiento para cada host en el sistema
- Comprobaciones de conectividad interna y externa para su sitio y sus URL de Administración

Paso 5 Seleccione **Desactivar el modo de mantenimiento** y seleccione **Continuar** para confirmar.
El sistema se reinicia después de desactivar modo de mantenimiento. Puede iniciar sesión en el sitio de administración una vez que se haya completado el reinicio.