Actualización de Meeting Server a la versión 4.0 - Informe técnico

Contenido

- Introducción
- Antecedentes
- Descripción general de almacenamiento seguro
  - Plataformas Soportadas
  - Notas de implementación
- Principios y restricciones de actualización
  - Ruta de actualización necesaria
  - Reducciones
  - Requisitos críticos de copia de seguridad para las actualizaciones 4.0
  - Configuración del primer inicio de sesión y contraseña
  - Restablecer la conectividad de red después de la actualización
  - Validar el estado del servidor antes de crear copias de seguridad
- Requisitos previos a la actualización
- Procedimientos comunes de backup y restauración
  - Datos afectados tras la actualización a 4.0
  - Realizar una copia de seguridad cuando el almacenamiento seguro esté deshabilitado o no disponible
  - Realizar una copia de seguridad cuando el almacenamiento seguro esté habilitado
  - Restaurar datos después de la actualización 4.0
  - Clave secreta de MeetingApps después de la restauración
- Restauración de la red y primer arranque
- Escenarios de actualización
  - Situación 1: nodo único con almacenamiento seguro deshabilitado o no disponible
  - Situación 2: nodo único con almacenamiento seguro habilitado
  - Situación 3: clúster de base de datos con almacenamiento seguro deshabilitado
    - Registrar detalles de clúster y realizar copias de seguridad de todos los nodos
    - Disolver el clúster
    - Actualizar y restaurar los nodos
  - Situación 4: clúster de base de datos con almacenamiento seguro habilitado
    - Registrar detalles de clúster y crear copias de seguridad cifradas
    - Disolver, actualizar y restaurar
- Validación posterior a la actualización

Introducción

Este documento describe cómo actualizar Cisco Meeting Server a la versión 4.0.

Antecedentes

Utilice este documento junto con las notas de la versión de Cisco Meeting Server, la Guía de referencia de comandos de MMP y la Guía de referencia de Secure Storage Administrator para comprender los requisitos y los requisitos previos.

El proceso de actualización de Cisco Meeting Server 4.0 difiere de las versiones anteriores porque la aplicación de la imagen provoca un restablecimiento de fábrica del nodo. Para garantizar la continuidad del servicio, todas las configuraciones anteriores, que incluyen la configuración de red y las contraseñas, deben conservarse mediante una copia de seguridad exportada a una ubicación externa antes de iniciar la actualización.

Además, el almacenamiento seguro era opcional en Cisco Meeting Server versiones 3.11 a 3.13, pero está habilitado de forma predeterminada en la versión 4.0. Como resultado, debe seguir diferentes procedimientos de copia de seguridad y restauración si nunca ha utilizado el almacenamiento seguro o si ya lo ha habilitado en 3.11x, 3.12x o 3.13x.

Secure Storage cifra los archivos de copia de seguridad y de clave privada en el servidor y requiere que dichos archivos se cifren antes de poder transferirlos al almacenamiento externo.

Este documento consolida la guía requerida en una sola referencia para que pueda seguir un procedimiento común para todos los escenarios de actualización sin la necesidad de repetir los mismos pasos.

En este documento se tratan los siguientes temas:

- Qué es el almacenamiento seguro, dónde se aplica y qué no se hace.
- La ruta de actualización, que incluye el requisito de alcanzar 3.13.x antes de 4.0 y el hecho de que no se admite una degradación de 4.0.
- Un método común de copia de seguridad y restauración para los nodos en los que está habilitado el almacenamiento seguro y para los nodos en los que está deshabilitado o no está disponible.
- Secuencia de disolución de nodo de cluster de base de datos mientras el cluster de base de datos se disuelve antes de una actualización.
- La clave secreta de MeetingApps, que no se almacena en una copia de seguridad de Cisco Meeting Server y se debe volver a generar después de una restauración.



Nota: Este documento utiliza capturas de pantalla de laboratorio capturadas durante las pruebas de guía de actualización originales, incluidas las versiones de software beta 4.0.

Todos los nombres de host, direcciones IP y nombres de archivo mostrados son estrictamente ilustrativos y no reflejan las credenciales de producción reales ni frases de contraseña confidenciales. Para mantener la claridad y evitar la redundancia, los pasos repetidos se muestran sólo una vez en la sección de procedimiento común, a menos que la vista de clúster proporcione el contexto adicional necesario.

Descripción general de almacenamiento seguro

Almacenamiento seguro proporciona una seguridad de datos mejorada mediante el cifrado de los archivos confidenciales que residen en el servidor de la reunión y el control de cómo se descargan esos archivos del servidor de Call Bridge. La función se introdujo en Cisco Meeting Server 3.11 como una opción configurable con el uso del comando MMP secure_storage enable en implementaciones de máquinas virtuales (basadas en especificaciones o Meeting Server Small) y en Meeting Server Medium.

A partir de la versión 4.0, Almacenamiento seguro está activado de forma predeterminada. Esta configuración ahora es permanente y es irreversible y se ha eliminado el comando secure_storage enable MMP.

Con el almacenamiento seguro, Meeting Server aplica este comportamiento:

- Las claves privadas no se pueden descargar a través de SFTP hasta que estén cifradas. Cifre una clave privada con el comando pki encrypt MMP seguido de una frase de contraseña de al menos 14 caracteres. Esto no cambia las claves que utilizan actualmente los servicios de Meeting Server.
- Los archivos de copia de seguridad creados con el comando backup encrypt <nombre> encrypt-name se cifran. Cuando Almacenamiento seguro está habilitado, el comando backup encrypt <name> encrypt-name MMP solicita una frase de contraseña de al menos 14 caracteres. Se requiere la misma frase de contraseña durante la restauración de la copia de seguridad.
- Antes de descargar un archivo de copia de seguridad, debe estar cifrado. Si una copia de seguridad de la lista aún no está cifrada para la exportación, utilice backup encrypt <name> encryption-name. Se rechazarán los intentos de descargar una copia de seguridad sin cifrar.
- A partir de la versión 3.12, el almacenamiento seguro puede funcionar cuando se habilita FIPS. Los archivos de clave privada creados en 3.11 con una frase de contraseña más corta deben regenerarse con una frase de contraseña de al menos 14 caracteres.



Consejo: Almacenamiento seguro restringe la transferencia de claves privadas no cifradas y archivos de copia de seguridad no cifrados desde el servidor de reuniones. No

restringe la transferencia de archivos de certificados. Los certificados se pueden seguir copiando con SFTP; sólo se bloquean las claves privadas no cifradas asociadas hasta que se cifren con pki encrypt.

⚠ Precaución: Una vez habilitada, el almacenamiento seguro no se puede deshabilitar con ningún comando MMP. La operación es irreversible. Sólo factory_reset full restablece Secure Storage en false. Tome una copia de seguridad de la configuración con instantánea de copia de seguridad y guárdela en un dispositivo independiente antes de activar el almacenamiento seguro. Después de secure_storage, habilite el reinicio inmediatamente. Si se omite el reinicio, el almacenamiento seguro se puede marcar como habilitado sin haberse inicializado por completo, y los comandos como factory_reset full pueden fallar. La ruta de recuperación en ese estado es volver a una instantánea guardada anteriormente (esto es válido sólo para 3.13.x). En Meeting Server 4.0, secure_storage está habilitado de forma predeterminada.

Plataformas Soportadas

- Máquina virtual (basada en especificaciones): Supported
- Meeting Server Small/1K: Supported
- Servidor de reuniones medio: Supported
- Meeting Server 2000: No soportados La función de almacenamiento seguro no está disponible. No utilice comandos de almacenamiento seguro en esta plataforma.

Cisco Meeting Server 4.0 habilita el almacenamiento seguro de forma predeterminada en todas las plataformas compatibles. Después de la actualización, los datos se protegen automáticamente mediante Secure Storage, incluso si se ha realizado la copia de seguridad de la versión 3.13.x mientras se desactivaba Secure Storage.

Notas de implementación

- El cambio de nombre de la imagen de actualización no cambia la configuración de Almacenamiento seguro.
- Confirme el estado de Almacenamiento seguro en cada nodo con el comando secure_storage antes de realizar copias de seguridad.
- El comando indica si Almacenamiento seguro está habilitado (True) o no (False). En Meeting Server 2000, el comando no es aplicable; mientras actualiza Cisco Meeting Server 2000, siga los pasos mencionados en las condiciones de actualización en las que Almacenamiento seguro está deshabilitado o no está disponible.



Salida de MMP cuando Almacenamiento seguro no está habilitado (Habilitado: falso).



Figura 2: Salida de MMP cuando el almacenamiento seguro está activado (Activado: true) en Cisco Meeting Server 3.13.

En la Guía de referencia rápida de Cisco Meeting Server Administrator para almacenamiento seguro y en la Referencia de comandos de MMP que está utilizando actualmente encontrará advertencias detalladas sobre la sintaxis de los comandos y ejemplos de uso.

Principios y restricciones de actualización

Ruta de actualización necesaria

Las actualizaciones de Cisco Meeting Server deben seguir una ruta secuencial sin omitir las versiones principales. Por ejemplo, un nodo de 3.11.x debe avanzar hasta 3.12.x y 3.13.x antes de llegar a 4.0. No se admiten las actualizaciones directas de versiones anteriores, como 3.9.x a 3.13.x o 3.11.x a 4.0, y normalmente provocan errores de configuración irrecuperables. Para Meeting Server Medium con las versiones 3.11.5 o 3.13, la ruta de actualización sería 3.11.5 → 3.13 → 4.0.

Consejo: Antes de iniciar la actualización 4.0, cada nodo debe ejecutar Cisco Meeting Server 3.13.x, con una copia de seguridad de la configuración verificada exportada desde ese sistema 3.13.x. Todos los procedimientos de escenario en este documento asumen que el paso de actualización a 3.13.x ya está completo.

Reducciones

Consejo: No se admite una degradación de 4.0.x a 3.13.x. Si la actualización falla o el sistema no funciona como se esperaba, implemente un nuevo OVA 3.13.x (o vuelva a crear una imagen del dispositivo) y restaure la copia de seguridad 3.13.x. Mantenga instantáneas de hipervisor de las máquinas virtuales 3.13.x mientras dure la ventana de actualización como opción de recuperación adicional. Las instantáneas de VM no reemplazan las copias de seguridad de configuración exportadas.

Requisitos críticos de copia de seguridad para las actualizaciones 4.0

Una vez confirmada la actualización 4.0, el nodo se reinicia en un primer estado de arranque. No dependa de la copia de seguridad automática generada durante el proceso de actualización, ya que un fallo de actualización puede provocar la pérdida del acceso a SFTP y hacer que el archivo sea inaccesible. Sólo las copias de seguridad creadas con el comando backup snapshot y copiadas en el almacenamiento externo se pueden utilizar de forma fiable para la recuperación.

Configuración del primer inicio de sesión y contraseña

Al arrancar por primera vez la versión 4.0, la contraseña de MMP existente se elimina de la base de datos. Inicie sesión con el nombre de usuario admin con una contraseña en blanco (sin contraseña). El sistema requiere que configure una nueva contraseña de MMP. El sistema le solicita que introduzca la contraseña dos veces para verificarla y confirmarla. Como no hay ninguna función de recuperación de contraseña para Meeting Server, asegúrese de registrar la nueva contraseña.

Nota: Si configura una nueva contraseña de MMP en el primer arranque, el comando backup rollback la reemplaza por la contraseña almacenada en la copia de seguridad 3.13.x. Después de restaurar la copia de seguridad en el servidor, debe iniciar sesión con la contraseña que estaba activa en el momento en que se creó la copia de seguridad.

Restablecer la conectividad de red después de la actualización

Las direcciones, máscaras y gateways IPv4 e IPv6 se pierden junto con el resto de la configuración. La conectividad de red del servidor de reuniones puede perderse después de la actualización a la versión 4.0. Debe tener acceso a la consola del hipervisor, CIMC o serial para poder asignar direcciones de nuevo desde el MMP.



Nota: Las implementaciones que utilizan reservas DHCP suelen conservar las mismas direcciones IP después del reinicio. Sin embargo, el acceso a la consola debe

permanecer disponible hasta que se verifique la dirección. No asuma que se restaura la conectividad SSH hasta que se confirme la dirección IP.

Validar el estado del servidor antes de crear copias de seguridad

Después de cada paso de actualización a la versión 3.13, asegúrese de que el servidor esté en buen estado y de que todos los servicios funcionen. No ignore ninguna condición de fallo en la página de descripción general del servidor. Si detecta errores o fallos, corríjalos antes de crear una instantánea de copia de seguridad en 3.13. Esto garantiza que se restaure una copia de seguridad del servidor en buen estado en los nodos actualizados de 4.0, lo que evita que se produzcan errores en la implementación.

En Web Admin, abra Status (Estado) y confirme que la sección Fault conditions (Condiciones de fallo) está desactivada. Omitir las entradas que solo aparecen en Errores y advertencias recientes. Después de una actualización, es común ver bases de datos transitorias o mensajes de puente Web allí; no son una razón para restaurar o retrasar la copia de seguridad.

Si una condición de falla permanece por más de diez minutos aproximadamente, resuelva la falla antes de realizar la copia de seguridad. Una restauración de una copia de seguridad de 3.13.x que ya contiene fallas en 4.0 lleva esas fallas hacia adelante.

En el caso de los sistemas agrupados, confirme que todos los tipos de llamadas en uso funcionan (terminales SIP y clientes de Web App) y que no se muestra ninguna condición de error en ningún nodo.

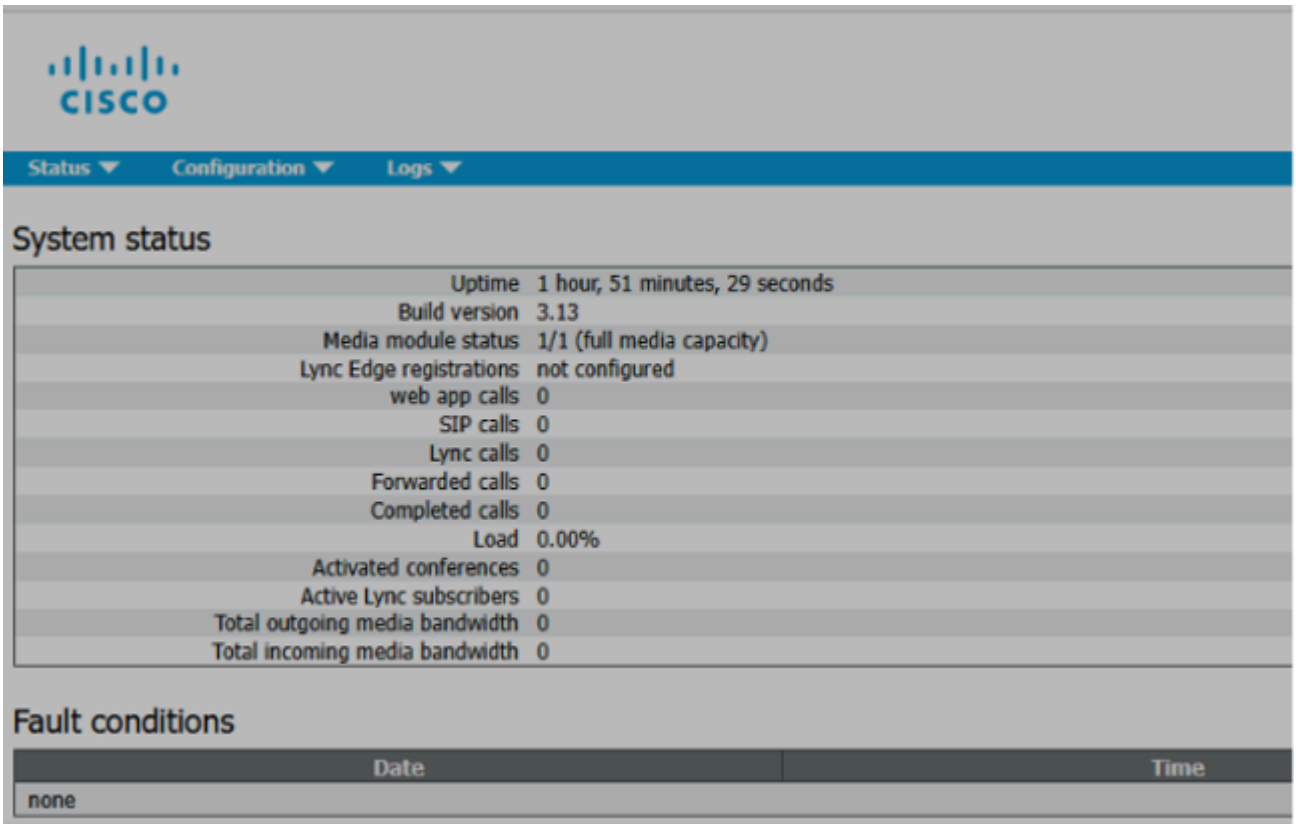


Figura 3: Página de estado de administración web en 3.13.x con condiciones de fallo vacías. Utilice esta vista antes de realizar la copia de seguridad restaurada en 4.0.

Requisitos previos a la actualización

Antes de iniciar la actualización a la versión 4.0, complete estas acciones. Estos requisitos se aplican a los cuatro escenarios que se tratan más adelante en este documento.

- Actualice a 3.13.x y, a continuación, exporte una copia de seguridad de la configuración. Asegúrese de que el nodo esté ejecutando Cisco Meeting Server 3.13.x. Cree una copia de seguridad y transfiérala, junto con todos los datos SFTP personalizados, como logotipos, archivos de marca, avisos de audio, archivos SSO y cualquier otro dato personalizado, al almacenamiento externo. Utilice los procedimientos de la sección Procedimientos Comunes de Copia de Seguridad y Restauración. En un entorno agrupado, realice una copia de seguridad de todos los nodos, no sólo del Connected Primary sino también de Connected Replica.
- Grabe la configuración de red. Ejecute ipv4 a y guarde el resultado. Debe volver a introducir esta información desde la consola después del reinicio 4.0 a menos que una reserva DHCP restaure la dirección IP automáticamente.
- Confirme el acceso a la consola. El acceso a la consola del hipervisor, CIMC o serie debe estar disponible antes de comenzar. Se espera que SSH se descarte cuando el nodo se reinicie a 4.0.
- Descargue el paquete de registro actual para archivarlo. Guarde logbundle.tar.gz desde cada nodo. El paquete no sustituye a las instantáneas de copia de seguridad.

- Lea el banner de advertencia de actualización 4.0 cuando se muestre después de ejecutar el comando upgrade.
- Pulse n para anular si algún requisito previo está incompleto. Presione Y sólo cuando esté listo para continuar.

Procedimientos comunes de backup y restauración

Los cuatro escenarios de actualización que se describen más adelante en este documento utilizan el mismo patrón de copia de seguridad, exportación, primer arranque y restauración. Utilice esta sección como origen único de estos pasos y, a continuación, siga únicamente la secuencia específica del escenario (nodo único frente a clúster y si Almacenamiento seguro ya está habilitado).

Datos afectados tras la actualización a 4.0

Estos datos se pierden después de la actualización 4.0 hasta que se restaura una copia de seguridad:

- Contenido de la base de datos, que incluye espacios, usuarios y perfiles de llamadas.
- Certificados y claves privadas.
- Personalización local, archivos SSO y archivos de avisos de audio.
- Configuración de red (dirección IP, máscara y puerta de enlace), excepto en los casos en los que una reserva DHCP restaura la dirección.
- La contraseña de MMP anterior, hasta que la restauración de la copia de seguridad vuelva a aplicar la contraseña de la copia de seguridad.
- Call Bridge, Web Admin, Web Bridge y otros servicios de aplicaciones solo se devuelven después de la restauración.



Consejo: La copia de seguridad de Cisco Meeting Server no incluye la clave secreta de MeetingApps. Después de una restauración, debe volver a generar esa clave y aplicarla a todos los nodos del puente web. Vea la sección Clave secreta de MeetingApps después de la restauración.

Realizar una copia de seguridad cuando el almacenamiento seguro esté deshabilitado o no disponible

Siga este procedimiento en máquinas virtuales, Meeting Server Small y Meeting Server Medium, donde secure_storage informa Enabled: False y en Meeting Server 2000 donde Almacenamiento seguro no está disponible.

1. En cada nodo, cree un archivo con el comando backup snapshot. No reutilice el nombre de archivo anterior.

2. Copie el archivo de copia de seguridad al almacenamiento externo con SFTP inmediatamente. No guarde la única copia en el servidor de reuniones.

3. Almacene el archivo en una ubicación a la que aún se pueda acceder si se vuelve a generar el nodo.

Ejemplo:

backup snapshot cms313SecurestorageFalse backup list

4. Confirme que el archivo aparece en el comando backup list y, a continuación, transfiéralo al disco externo con un cliente SFTP.

5. Repita este proceso en todos los nodos del cluster. Los nombres de copia de seguridad sólo pueden contener letras, números, guiones bajos y guiones. No incluya la extensión de archivo .bak cuando cree un archivo de copia de seguridad. Por ejemplo, un nombre de archivo como 3.13SecurestorageFalse se rechaza debido al punto.

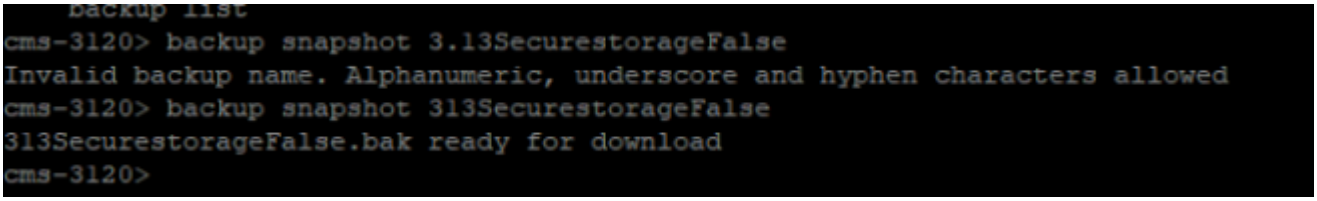


Figura 4: La instantánea de copia de seguridad rechaza un nombre que contiene un punto y, a continuación, se realiza correctamente con un nombre alfanumérico. El archivo .bak está listo para descargarse.



Figura 5: Copie el archivo .bak desde la raíz SFTP del servidor de reuniones al almacenamiento externo. No deje la única copia en el servidor.

Realizar una copia de seguridad cuando el almacenamiento seguro esté habilitado

Utilice este procedimiento cuando secure_storage informe Habilitado: Verdadero. Los archivos de copia de seguridad no cifrados no se pueden descargar.

1. Cree una instantánea de copia de seguridad en cada nodo. Cuando Almacenamiento seguro está habilitado, el servidor solicita una frase de contraseña de al menos 14 caracteres. La frase de paso puede incluir letras, números, caracteres especiales, símbolos o espacios.

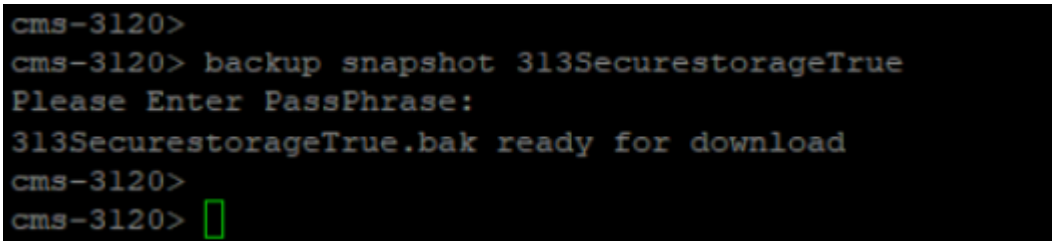


Figura 6: Realice una copia de seguridad de la instantánea con el almacenamiento seguro activado y solicite una frase de contraseña de al menos 14 caracteres. El MMP no le pide que lo confirme.

2. El MMP no le solicita que vuelva a introducir la frase de contraseña para confirmarla. Proteja la frase de contraseña, ya que necesita la misma frase de contraseña para restaurar el archivo. No elija una frase de contraseña trivial o de ejemplo.

3. Si el comando backup list muestra una instantánea que no se ha cifrado para la exportación, cifre la instantánea antes de descargarla:



Figura 7: Copia de seguridad de la lista antes del cifrado. La columna Cifrado es no, por lo que no se puede descargar el archivo.

4. Si intenta descargar una copia de seguridad sin cifrar, SFTP devuelve un error de permiso denegado y le indica que ejecute el comando backup encrypt en primer lugar.

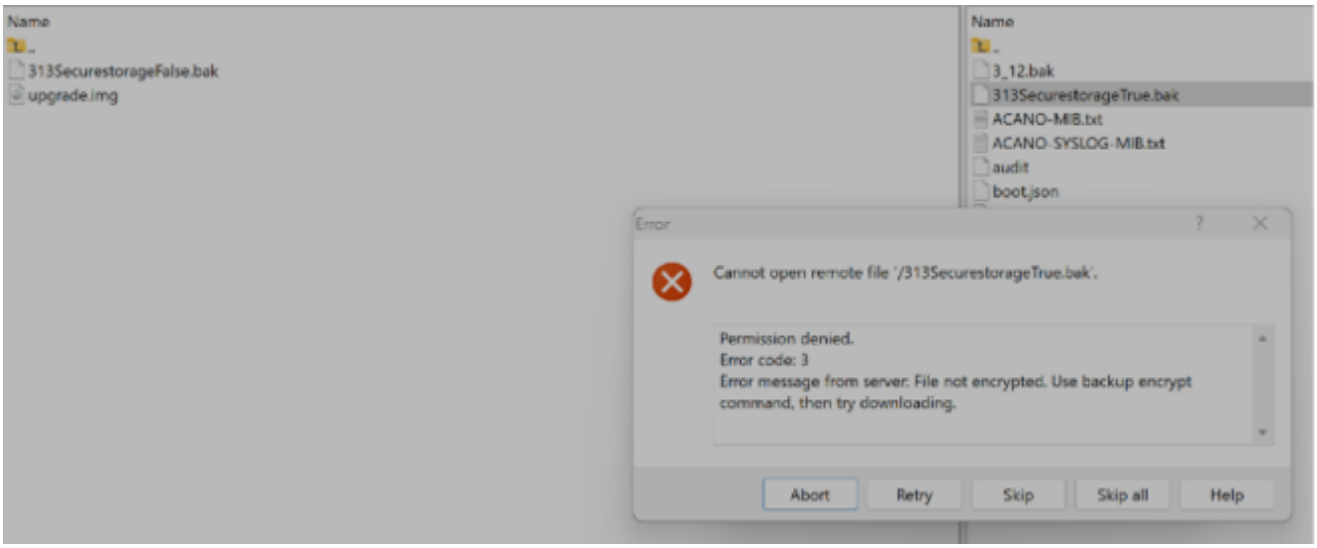


Figura 8: SFTP deniega la descarga de una copia de seguridad sin cifrar cuando Almacenamiento seguro está activado. El mensaje del servidor le indica que ejecute el cifrado de copia de seguridad.

5. Ejecute el comando backup encrypt para cifrar el archivo de copia de seguridad.



Figura 9: Copia de seguridad de la lista después de cifrar la instantánea. Cifrado es sí y el archivo se puede transferir con SFTP.

La lista de copia de seguridad muestra el estado de cifrado y el nombre del archivo original. Asegúrese de transferir sólo el archivo cifrado de cada nodo del clúster. Mantenga un registro organizado de cada nodo, su nombre de archivo correspondiente y la frase de contraseña asociada.

Si también necesita exportar claves privadas, cifre primero cada clave. Almacenamiento seguro no bloquea los archivos de certificado y se pueden copiar sin este paso adicional:

```
pki encrypt private.key encrypted_private.key
```

Utilice un nombre de archivo único en lugar de sobrescribir la clave que utilizan actualmente los servicios. El requisito mínimo de la frase de contraseña de 14 caracteres también se aplica aquí.

Restaurar datos después de la actualización 4.0

1. Después del inicio de sesión y la recuperación de la red en la sección First-boot and Network Restoration, copie la copia de seguridad 3.13.x correspondiente en el nodo con SFTP y restáurela.

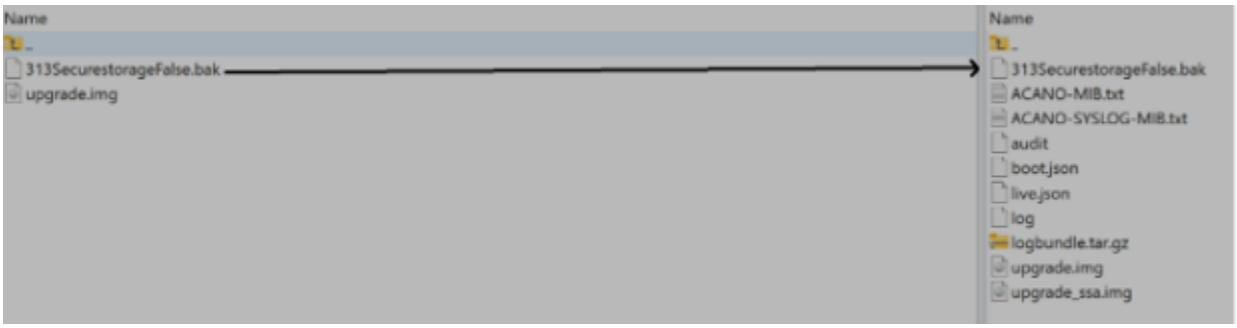


Figura 10: Después de la recuperación de la red durante el primer arranque, copie el archivo .bak 3.13.x nuevamente en el nodo 4.0 con SFTP.

2. Confirme si el archivo está presente:

lista de backup

```
cms-3120> backup list
Timestamp    Filename                                                    Encrypted
 Encrypted-from
Sep 01 11:53 313SecurestorageFalse                                       no

cms-3120>
```

Figura 11: La lista de respaldo en 4.0 confirma que la instantánea cargada está presente antes de la reversión.

3. Restaure la instantánea. En una implementación de clúster, restaure primero la base de datos principal anterior, seguida de las réplicas y, a continuación, de los nodos conectados.

backup rollback name-of-the-backup-file

```
cms-3120> backup rollback 313SecurestorageFalse
WARNING!!!
This command will overwrite the existing system configuration
and result in a reboot of the system. This will cause
an interruption in service.

Are you sure you wish to proceed? (Y/n)
Successful backup extraction
Stopping Application monitor: app_monitor.
Rebooting system...
```

Figura 12: Reversión de copia de seguridad de una instantánea no cifrada. Confirmar con Y; el nodo extrae la copia de seguridad y se reinicia.

4. Pulse Y para continuar. El nodo se reinicia mientras extrae la copia de seguridad. Si la copia de seguridad se realizó con Almacenamiento seguro habilitado, el MMP solicita la frase de contraseña. El reinicio continúa sólo después de que se acepte la frase de contraseña correcta.

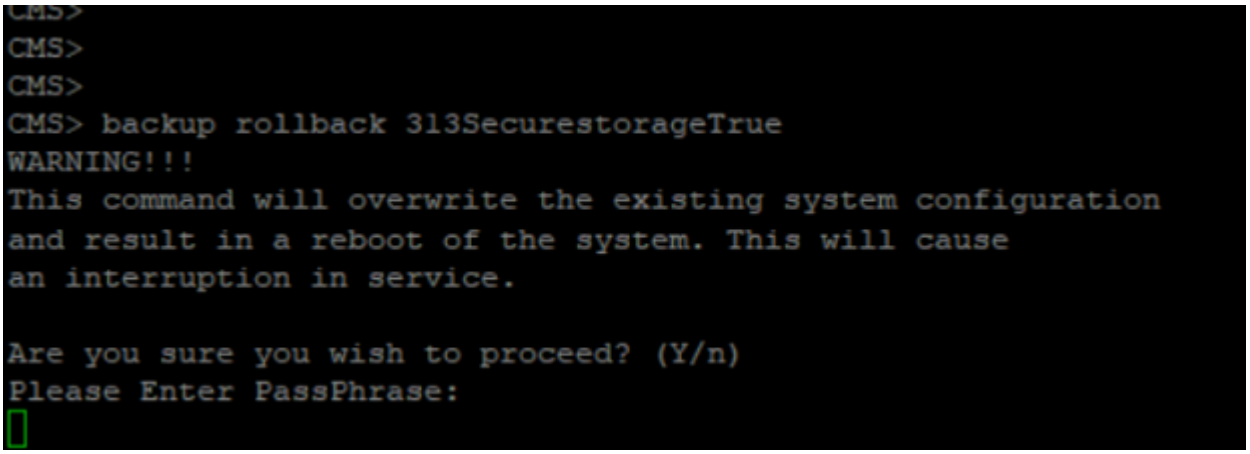


Figura 13: Reversión de copia de seguridad de una instantánea cifrada. Después de Y, el MMP solicita la frase de contraseña utilizada cuando se creó la copia de seguridad.

⚠ Precaución: El **backup rollback** sobrescribe la configuración actual, los certificados, las claves privadas y el archivo de licencia y, a continuación, reinicia el servidor. Utilícelo sólo con la copia de seguridad 3.13.x exportada para esta actualización.

---

5. Cuando el nodo vuelva a estar en línea, inicie sesión con las credenciales de MMP de la copia de seguridad y confirme que cada servicio requerido está activado y en ejecución (el MMP muestra esto como activo: True).

Comprobaciones típicas:

callbridge webbridge3 webadmin scheduler recorder streamer uploader meetingapps

6. Ejecute sólo los comandos para los servicios que este nodo debe alojar.

Clave secreta de MeetingApps después de la restauración

La copia de seguridad de Cisco Meeting Server no almacena la clave secreta de MeetingApps. Una vez completada la restauración de la copia de seguridad, regenere el secreto y aplíquelo a cada nodo del puente web. Al omitir este paso, el uso compartido de archivos deja de estar disponible aunque los demás servicios parezcan adecuados.

1. En el nodo MeetingApps, ejecute el comando meetingapps gensecret.

2. Copie el secreto generado en su almacén secreto. Cada ejecución de meetingapps gensecret invalida la clave anterior, por lo que debe generar la clave una vez y reutilizar el mismo valor en todos los puentes web.

3. Ejecute estos comandos en cada nodo del puente Web:

webbridge3 disable webbridge3 meetingapps add MeetingApps-URL secret webbridge3 enable webbridge3

El último comando confirma que el servicio de puente web se está ejecutando y que MeetingApps está configurado correctamente. MeetingApps no es compatible con Meeting Server 2000 y el uso compartido de archivos no está disponible en clústeres que incluyen Meeting Server 2000. En este tipo de implementaciones, este paso no es aplicable.

Restauración de la red y primer arranque

El comando upgrade 4.0 muestra un banner de advertencia antes de continuar. Revise el mensaje cuidadosamente y aborte con n si alguno de los requisitos previos está incompleto. Si continúa con Y, el nodo se reinicia, la sesión SSH se desconecta y los pasos restantes deben completarse desde la consola.

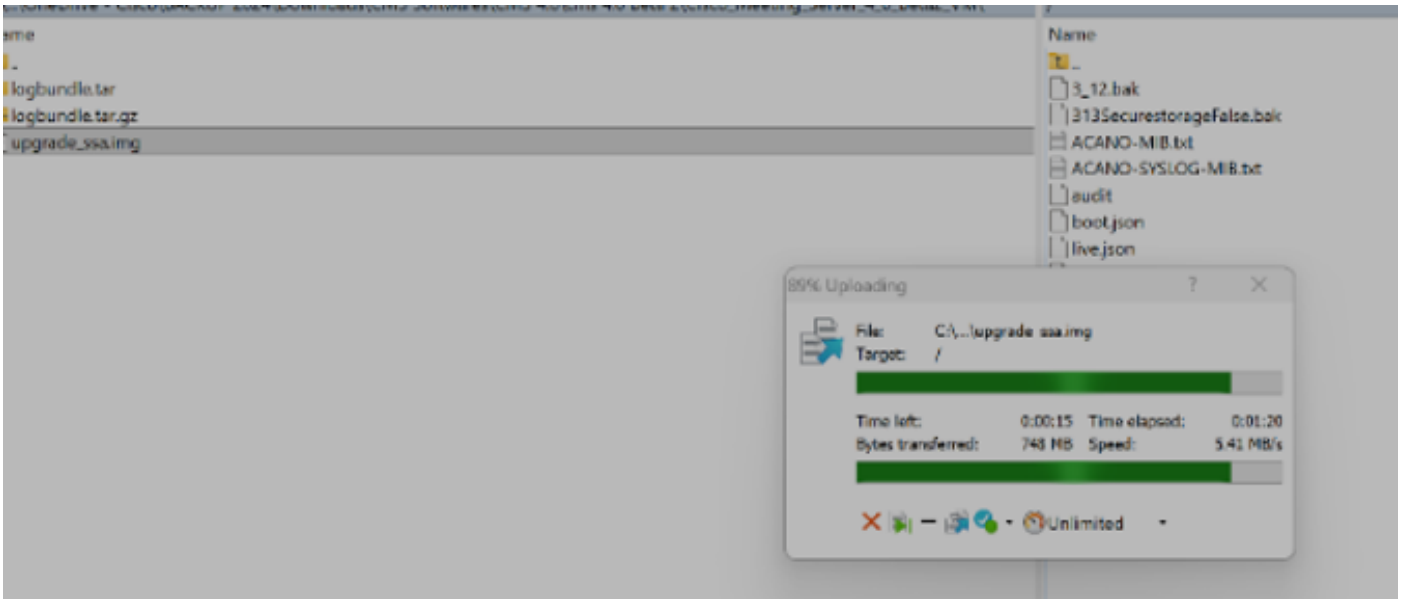


Figura 14: Cargue la imagen de actualización 4.0 en el directorio raíz SFTP de Meeting Server. El nombre de archivo de la imagen de actualización puede variar según el paquete descargado de cisco.com.

```
cms-3120>
cms-3120>
cms-3120>
cms-3120> upgrade upgrade_ssa.img
Verifying upgrade image signature...
Image has been signed with key CMS_EFT_key_a type SPECIAL
CMS_EFT_key_a_SPECIAL.pem external key signature has been verified wi
ey
Image signature has been verified with imported public key CMS_EFT_ke
ECIAL
Image integrity has been verified
Upgrade image 4.0(beta2) is valid
Initiating a backup, please wait...
```

Figura 15: El comando upgrade verifica la firma de la imagen e inicia el proceso. No confíe en la copia de seguridad automática que se crea en este momento.

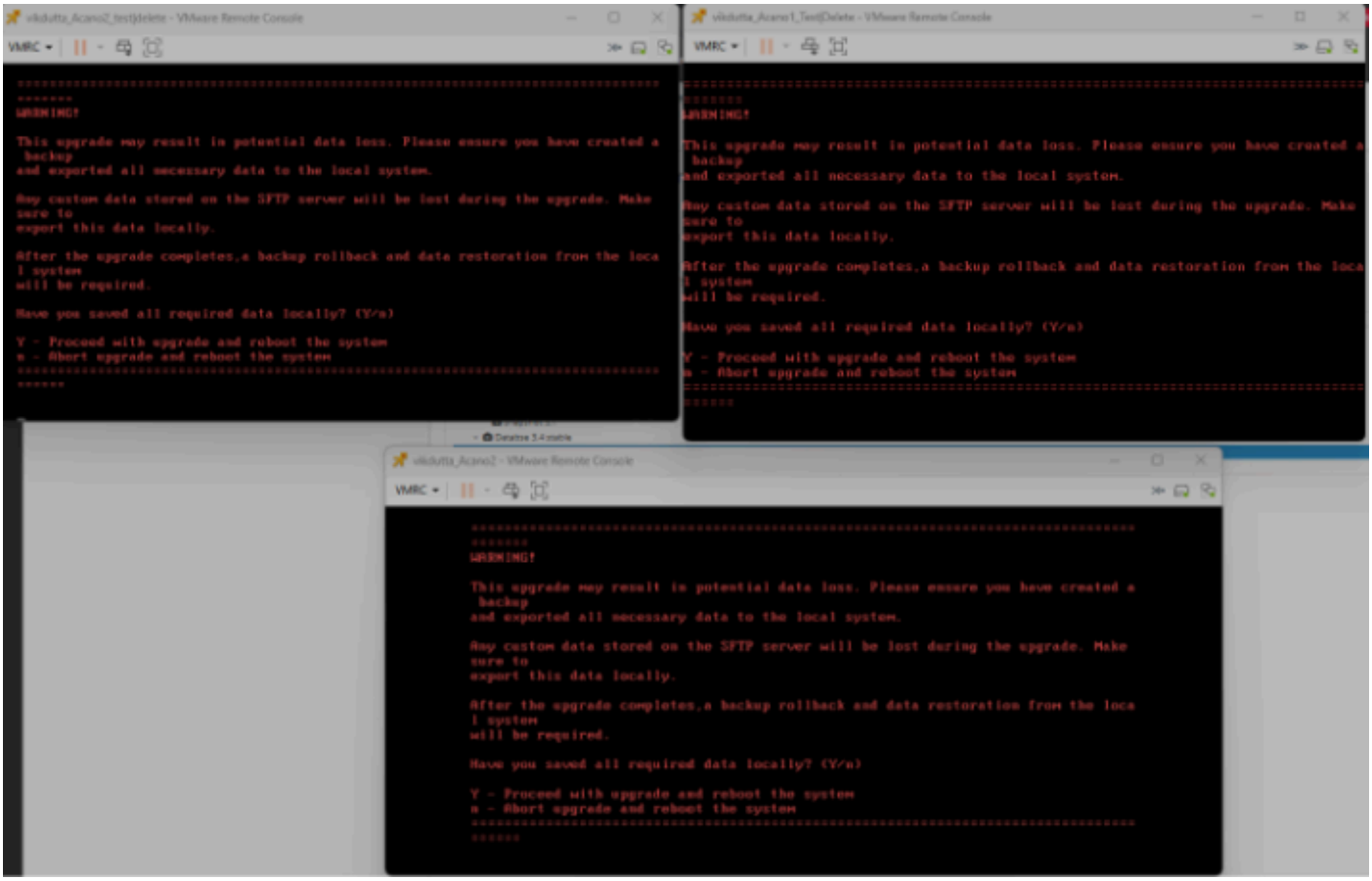


Figura 16: Advertencia MMP roja en un clúster de tres nodos. El mismo banner aparece en un único nodo. Pulse n para cancelar si las copias de seguridad y los datos personalizados no están fuera del servidor. Pulse Sólo Y para continuar y reiniciar.

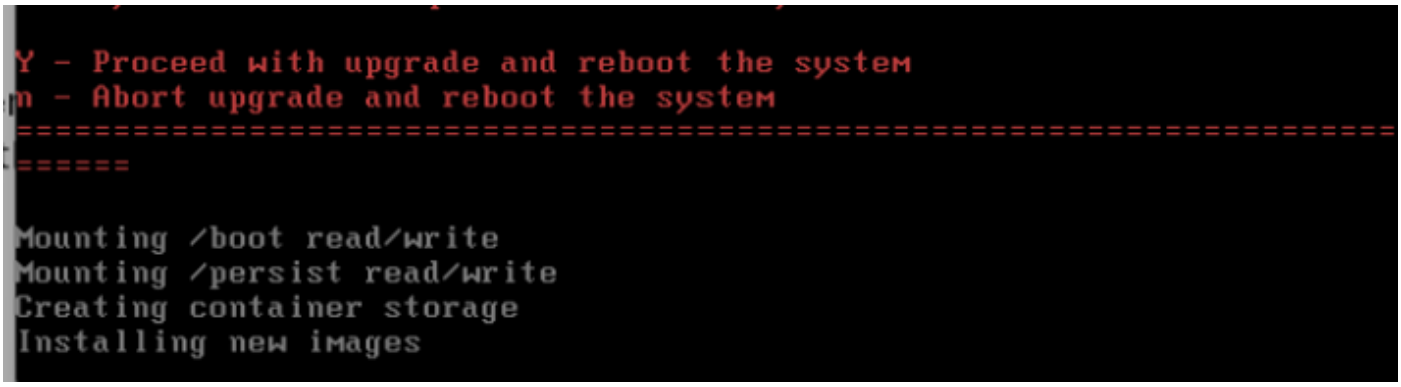


Figura 17: Después de Y, el nodo monta el almacenamiento e instala la imagen 4.0. Se agota el tiempo de espera de la sesión SSH; continúe desde la consola del hipervisor.

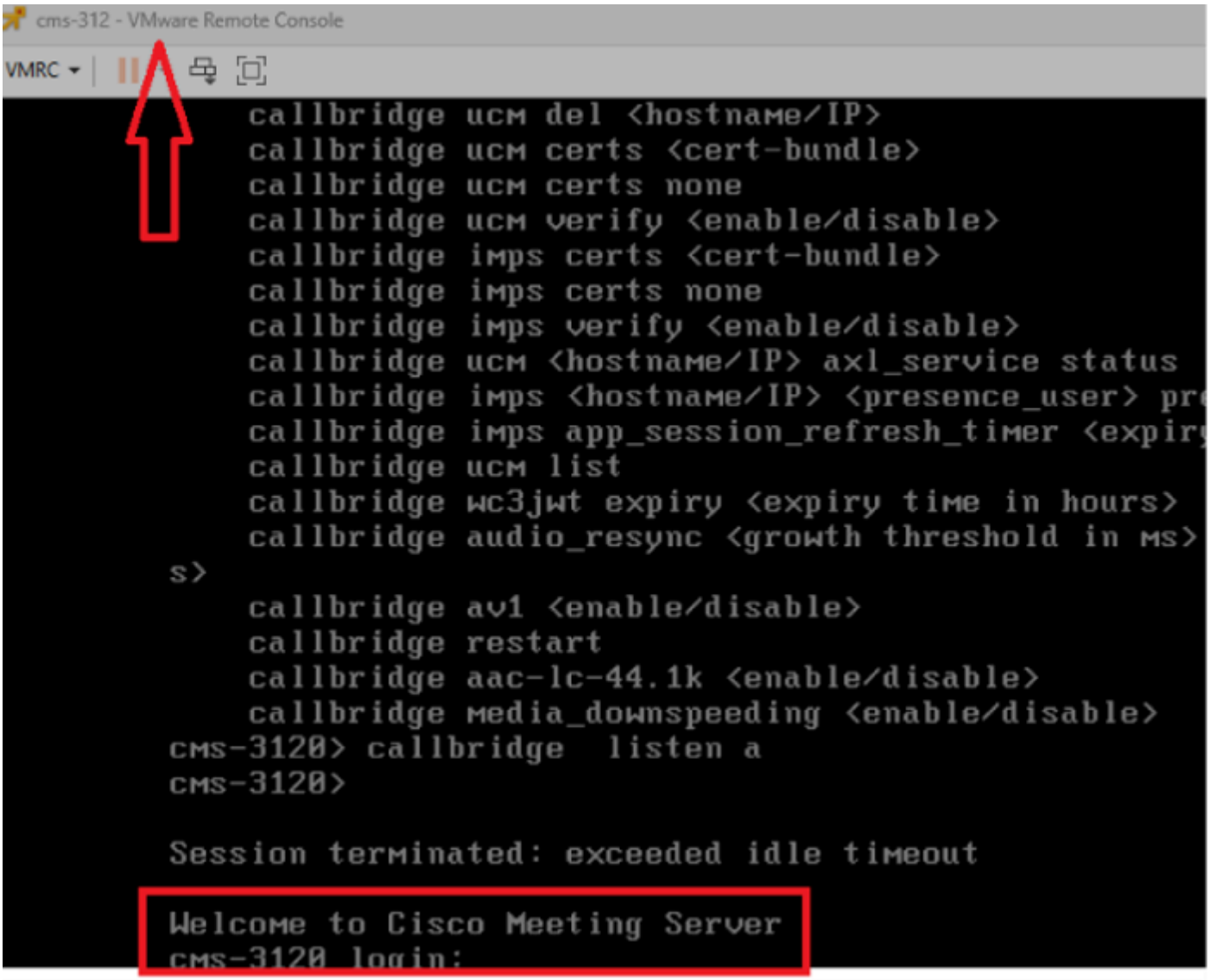


Figura 18: Utilice la consola de VM o CIMC después de que SSH caiga. El mensaje de inicio de sesión de primer arranque aparece cuando la imagen 4.0 está lista.

1. Inicie sesión con la cuenta MMP de primer arranque (nombre de usuario admin y sin contraseña) y luego establezca una nueva contraseña MMP cuando se le solicite. Tenga en cuenta que la restauración de la copia de seguridad sustituye esta contraseña por la contraseña

almacenada en la copia de seguridad.

2. Vuelva a aplicar la configuración de red desde las notas que capturó en la sección Requisitos previos a la actualización:

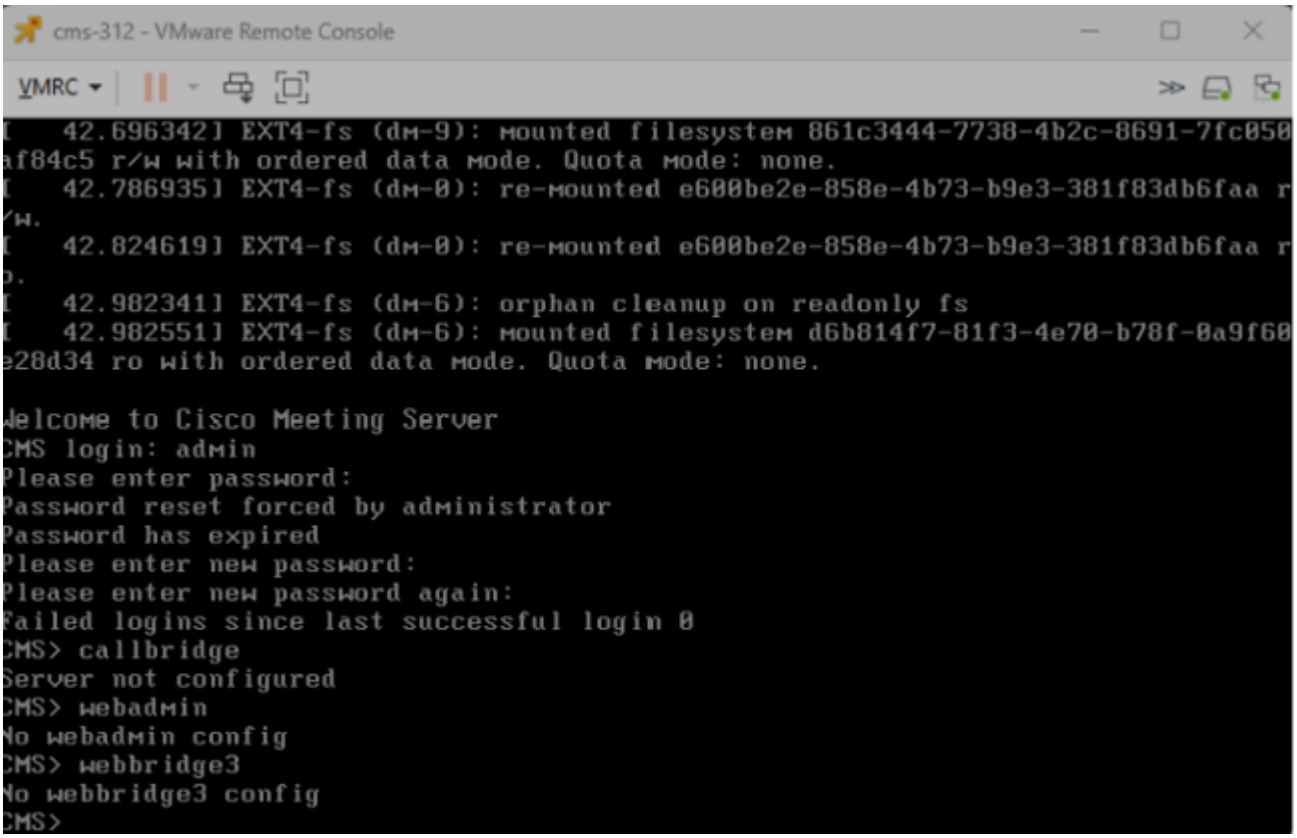


Figura 19: Primer inicio de sesión de MMP.

La contraseña anterior ya no es válida. Después de establecer una nueva contraseña, los servicios como webadmin y webbridge3 aparecen como no configurados hasta que se restaura la copia de seguridad.

3. Ejecute el comando:

```
ipv4 interface add address/prefix-length gateway
```

Por ejemplo:

```
ipv4 a add 192.0.2.10/24 192.0.2.1
```

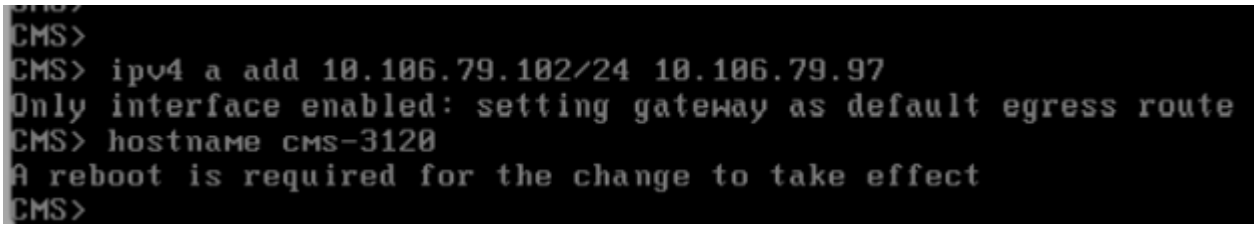


Figura 20: Volver a aplicar IPv4 desde la consola.

Es necesario reiniciar después de asignar la dirección. Las direcciones que se muestran en la captura de pantalla son solo para fines de ejemplo.

4. Reinicie el sistema después de asignar la dirección. Una vez que el sistema vuelva a estar en línea, continúe con la carga en SFTP de la copia de seguridad y los pasos de restauración mencionados en la sección Restaurar datos después de la actualización 4.0.

Nota: Si se configura una reserva DHCP, la dirección original ya se puede asignar después del reinicio. Verifique la dirección con **ipv4 a** antes de iniciar una sesión SFTP desde su estación de trabajo de administración.

En Cisco Meeting Server 4.0, el almacenamiento seguro está habilitado de forma predeterminada en las plataformas que lo admiten. El MMP ya no puede exponer secure_storage como una alternancia después de la actualización.



Figura 21: En esta imagen 4.0, secure_storage no es un comando reconocido porque Secure Storage está habilitado de forma predeterminada.

Confirme la versión con el comando version.

Escenarios de actualización

En este capítulo se tratan diferentes escenarios de actualización. Complete el paso de actualización a 3.13.x. Identifique el tipo de implementación y elija la situación en consecuencia. Siga únicamente el procedimiento que coincida con su entorno y no combine los pasos de las implementaciones de clúster y nodo único.

Primero, complete el paso de actualización compatible a 3.13.x. A continuación, seleccione exactamente un escenario a continuación. No combine los procedimientos de nodo único y de clúster de base de datos.

- Escenario 1: Nodo único, deshabilitado o no disponible, VM, pequeño, mediano y Meeting Server 2000
- Escenario 2: Nodo único, habilitado, VM, pequeño y mediano solamente
- Escenario 3: Clúster de base de datos, Deshabilitado o no disponible, VM, Pequeño, Mediano y Meeting Server 2000
- Escenario 4: Clúster de base de datos, habilitado, VM, pequeño y mediano solamente

Meeting Server 2000 no admite los escenarios habilitados para Almacenamiento seguro. Para esa plataforma, utilice el escenario 1 o 3, según corresponda.

Situación 1: nodo único con almacenamiento seguro deshabilitado o no disponible

Utilice este procedimiento para un servidor independiente con Almacenamiento seguro deshabilitado o Meeting Server 2000 donde Almacenamiento seguro no está disponible. La versión de origen puede ser 3.11.x o posterior, pero el nodo debe estar en 3.13.x antes de actualizar a 4.0.

1. Paso de actualización a 3.13.x. Siga la ruta admitida (por ejemplo, 3.11.x → 3.12.x → 3.13.x). Después de cada salto, confirme la versión en Web Admin y que las condiciones de falla estén claras, como se describe en la sección Validar el estado del servidor antes de crear copias de seguridad.

2. Confirme el estado de Almacenamiento seguro. Ejecute el comando secure_storage y verifique que Secure Storage no esté habilitado. Omita el comando en Meeting Server 2000.

3. Cree y exporte un archivo de copia de seguridad 3.13.x como se menciona en la sección Realizar una copia de seguridad cuando el almacenamiento seguro esté inhabilitado o no disponible. Exporte también contenido SFTP personalizado y el paquete de registro como se menciona en la sección Requisitos previos a la actualización.

4. Descargue la imagen de software 4.0 de Cisco.com, extráigala y copie upgrade.img en el nodo a través de SFTP.

5. Inicie la actualización con este comando:

```
upgrade upgrade.img
```

6. Lea el banner de advertencia. Pulse S sólo después de que se hayan completado todos los requisitos previos. 6. Después de la actualización, configure el nodo como se describe en la sección First-boot and Network Restoration, luego restaure la copia de seguridad con el uso de la sección Restore Data After 4.0 Upgrade.

Situación 2: nodo único con almacenamiento seguro habilitado

Utilice este procedimiento para una máquina virtual independiente, un servidor de reuniones pequeño o un servidor de reuniones medio en el que esté activado el almacenamiento seguro. No se aplica a Meeting Server 2000.

Antes de transferir archivos desde el servidor, tenga en cuenta que las claves privadas no cifradas y los archivos de copia de seguridad no cifrados no se pueden transferir. Los archivos de certificado no están bloqueados.

1. Actualice a través de la ruta admitida a 3.13.x sin omitir las versiones. Después de cada salto, confirme la versión y que las condiciones de falla estén claras en la sección Validar el estado del servidor antes de crear copias de seguridad.

2. Ejecute secure_storage y confirme que la salida muestra Enabled: Verdadero.

3. Cree y exporte una copia de seguridad cifrada de 3.13.x con el uso de la sección Tome una copia de seguridad cuando esté habilitado el almacenamiento seguro. Almacene su frase de contraseña en su almacén secreto. Exporte también contenido SFTP personalizado y el paquete de registro (sección Requisitos previos a la actualización).

4. Copie upgrade.img en el nodo y ejecute la actualización:

```
upgrade upgrade.img
```

5. Lea el banner de advertencia y pulse Y para continuar sólo cuando se hayan completado los requisitos previos.

6. Recupere la red desde la consola (sección First-boot and Network Restoration) y, a continuación, restaure la copia de seguridad cifrada con su frase de paso (sección Restore Data After 4.0 Upgrade). 6. Si MeetingApps está en uso, aplique un nuevo secreto de MeetingApps (sección Clave secreta de MeetingApps después de restaurar).

Almacenamiento seguro está habilitado de forma predeterminada en Meeting Server 4.0.

Después de una restauración, siga administrando claves privadas y archivos de copia de seguridad como datos cifrados.

Situación 3: clúster de base de datos con almacenamiento seguro deshabilitado

Utilice este procedimiento para un clúster de base de datos con Almacenamiento seguro deshabilitado, que incluye un clúster que contiene Meeting Server 2000. A partir de la versión 3.5, el clúster de base de datos se debe disolver antes de la actualización de software. En primer lugar, actualice cada nodo a 3.13.x.

Registrar detalles de clúster y realizar copias de seguridad de todos los nodos

1. Ejecute secure_storage en cada nodo. Trate el comando como no disponible en los nodos de Meeting Server 2000.

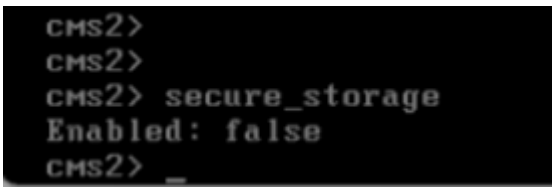


Figura 22: Antes de utilizar copias de seguridad no cifradas, compruebe que Almacenamiento seguro está deshabilitado en todos los nodos del clúster. Omita el comando para los nodos de Meeting Server 2000, donde no está disponible.

2. Registre el nodo principal de la base de datos actual, ya que debe restaurarse primero después de la actualización a 4.0. Confirme que las réplicas están sincronizadas y que el estado del clúster es correcto.

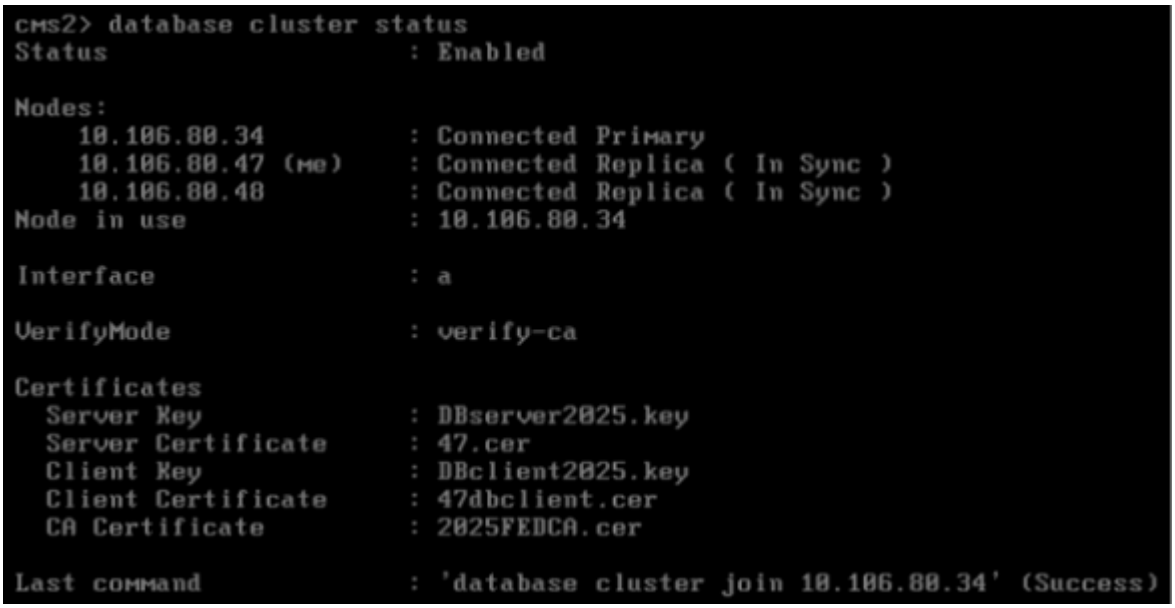


Figura 23: Registre el principal actual y confirme que las réplicas están sincronizadas.

3. Confirme que todos los tipos de llamadas en uso estén funcionando y que las condiciones de error estén despejadas en todos los nodos (sección Validar el estado del servidor antes de crear copias de seguridad).

4. Cree una copia de seguridad de todos los nodos con la sección Realizar Copia de Seguridad cuando Almacenamiento Seguro esté Desactivado o No Disponible. Asigne un nombre a cada archivo para que se asigne claramente a su nodo y transfiera cada copia de seguridad al almacenamiento externo antes de disolver el clúster.

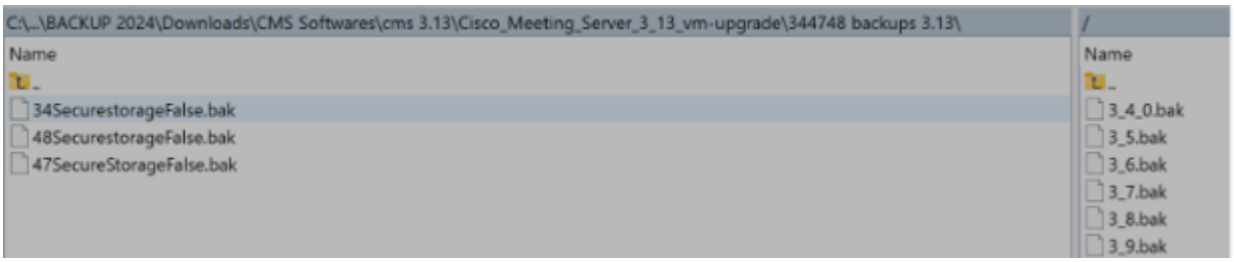


Figura 24: Las tres copias de seguridad de nodo de ejemplo almacenaron almacenamiento externo, denominado de modo que cada archivo se asigna a su nodo.

Disolver el clúster

Elimine los nodos en este orden. Mantener el primario hasta el final:

- Nodos de Meeting Server conectados (no principales)
- nodos de base de datos de réplicas
- Nodo de base de datos principal

En cada nodo, ejecute el comando remove y presione Y. No continúe con la actualización 4.0 hasta que cada nodo informe que ha salido del clúster. Si se elimina la pertenencia al clúster, la base de datos local del nodo permanece activa.

database cluster remove

```
cms2> database cluster remove
WARNING!!!
Are you sure you wish to remove this node from the current cluster? (Y/n)
 The current contents of this node's database will become the running local data
base.
 This node will lose all knowledge of the rest of the cluster.
 The callbridge and web administration will restart at the end of this procedure
.
Please wait...
Remove started...
cms2> database cluster status
```

Figura 25: En una réplica, confirme Y para quitar la pertenencia al clúster. La base de datos local del nodo permanece en su lugar.

```
 The current contents of this node's database will become the running local data
base.
 This node will lose all knowledge of the rest of the cluster.
 The callbridge and web administration will restart at the end of this procedure
.
Please wait...
Remove started...
cms2> database cluster status
Status                  : Disabled
Node in use             : None

Interface               : a

VerifyMode              : verify-ca
```

Figura 26: Después de la eliminación, compruebe que el estado del clúster es Deshabilitado y que Nodo en uso es Ninguno en ese nodo.

```
cms1> database cluster status
Status                  : Enabled

Nodes:
    10.106.80.34 (me)   : Connected Primary
Node in use             : 10.106.80.34

Interface               : a

VerifyMode              : verify-ca

Certificates
  Server Key            : DBserver2025.key
  Server Certificate    : 47.cer
  Client Key            : DBclient2025.key
  Client Certificate    : 47dbclient.cer
  CA Certificate        : 2025FEDCA.cer

Last command            : 'database cluster initialize' (Success)
```

Figura 27: Después de quitar las réplicas, el nodo principal anterior es el único que queda en el clúster. Quítelo el último.

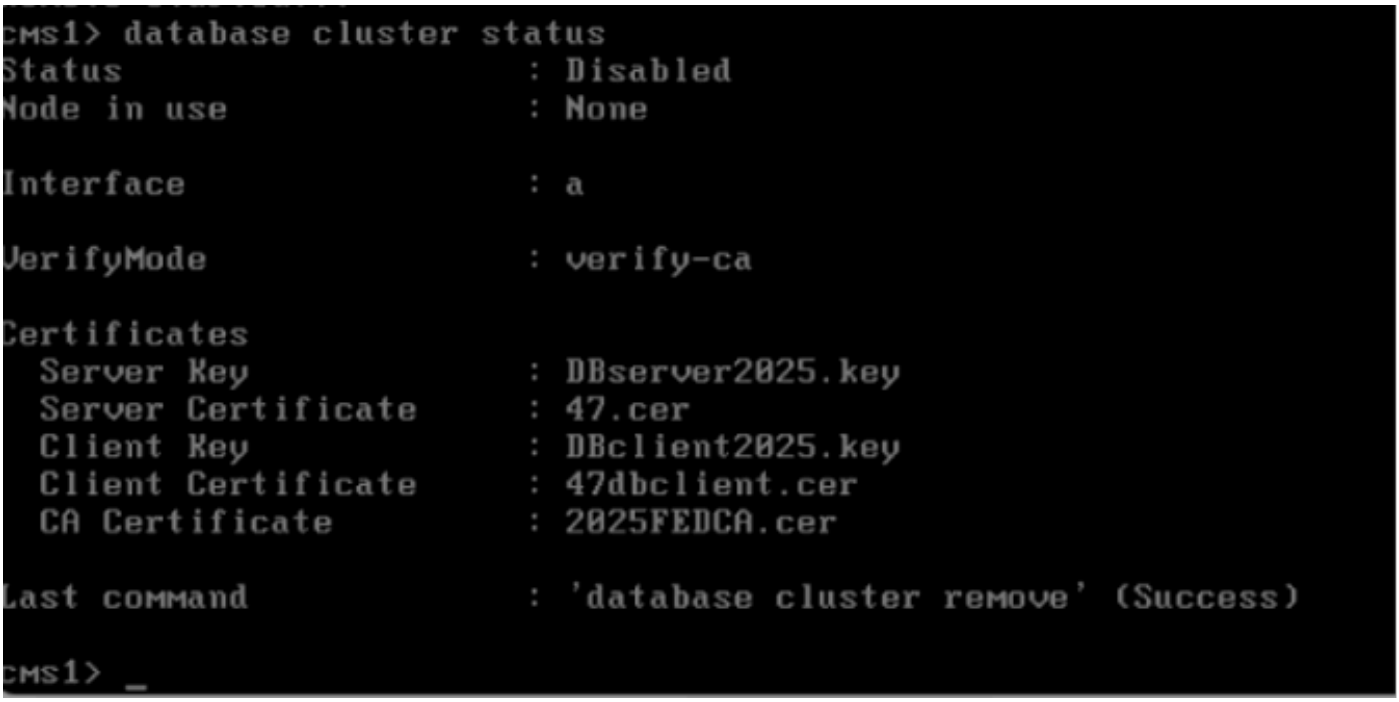


Figura 28: Después de quitar el anterior primario, verifique que el comando notifique Success y que el estado del clúster sea Disabled (Desactivado).

Actualizar y restaurar los nodos

1. Una vez disueltos, los nodos son independientes y se pueden actualizar en paralelo. En cada nodo, copie upgrade.img sobre SFTP y ejecute el comando upgrade:

```
upgrade upgrade.img
```

2. Recupere el direccionamiento de red de cada nodo desde la consola (sección Primer arranque y Restauración de red).

3. Copie la copia de seguridad 3.13.x propia de cada nodo en ese nodo. Restaure primero el primer nodo primario anterior, seguido de las réplicas y, a continuación, los nodos conectados. Utilice la sección Restaurar datos después de la actualización 4.0. Una restauración de las copias de seguridad restablece la pertenencia al clúster de base de datos.

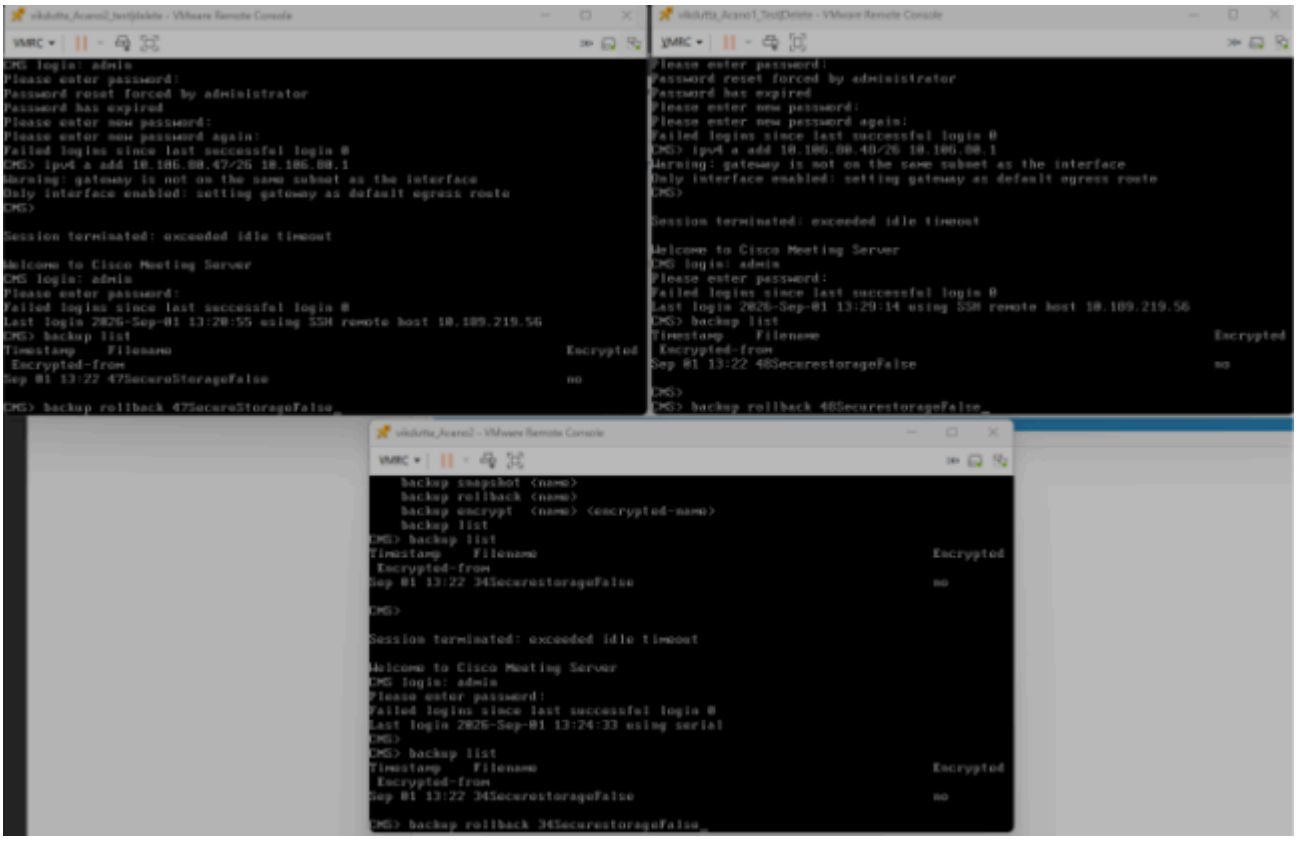


Figura 29: Restaure la propia instantánea de cada nodo. Comience con la anterior clave principal y, a continuación, restaure las réplicas. Los nombres de archivo de ejemplo identifican su nodo.

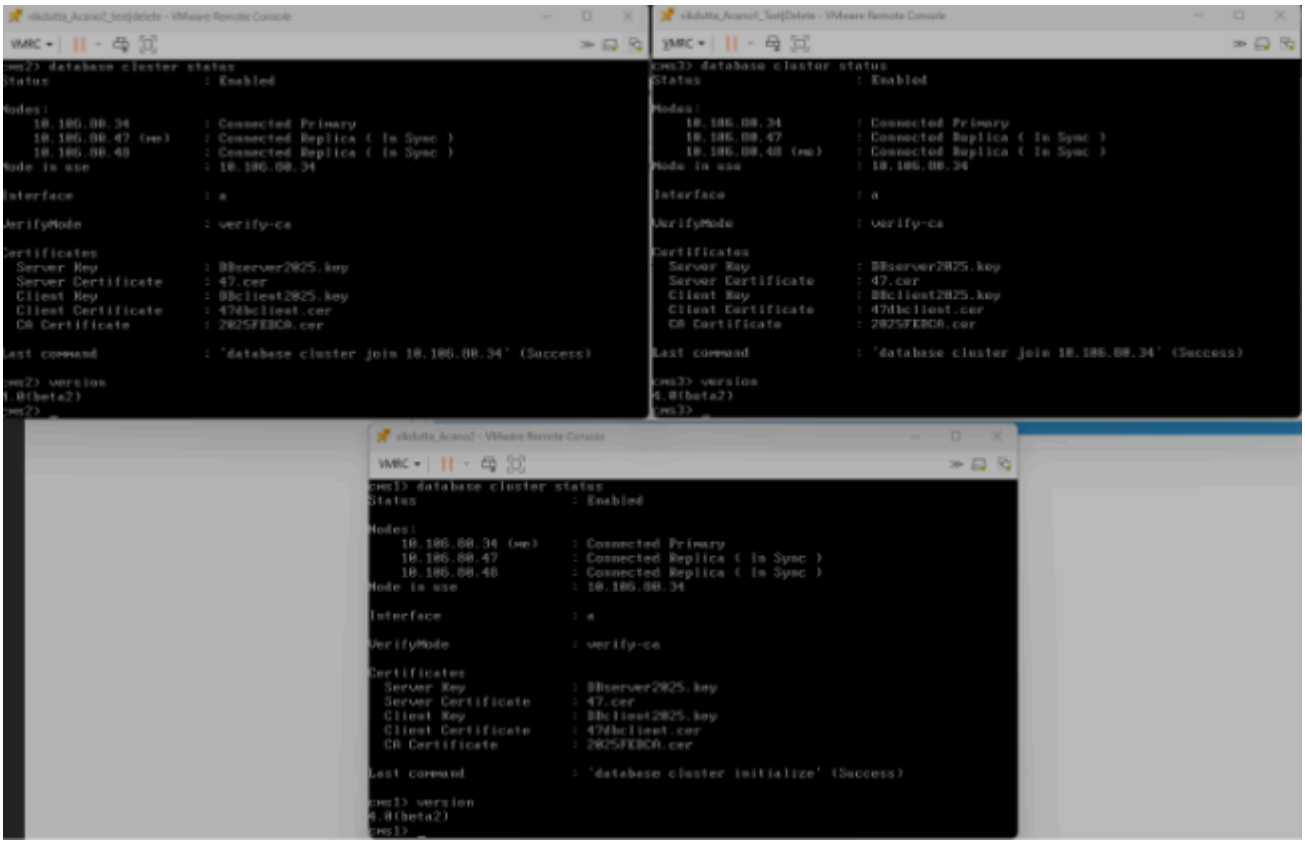


Figura 30: Después de la restauración en Meeting Server 4.0, compruebe que el clúster está habilitado, que se muestra el mismo servidor principal y que las réplicas están sincronizadas.

Nota: Si las conexiones de clúster de Call Bridge no se activan después de esta restauración, ejecute el **database cluster upgrade_schema** en la anterior conexión principal solamente y vuelva a comprobar el estado de Call Bridge.

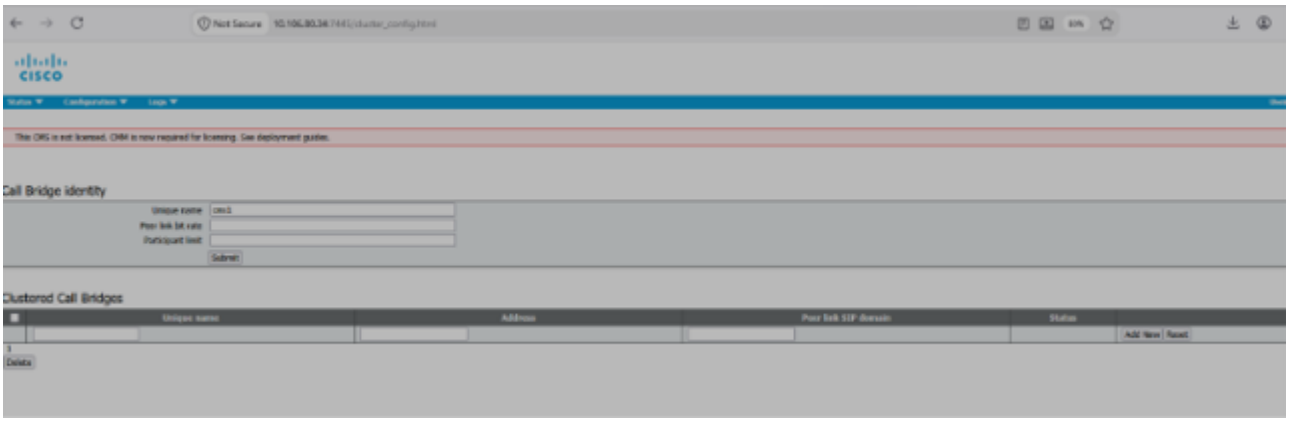


Figura 31: Antes de la actualización del esquema, el ejemplo muestra el clúster de base de datos que se ejecuta mientras Clustered Call Bridges está vacío.

database cluster upgrade_schema

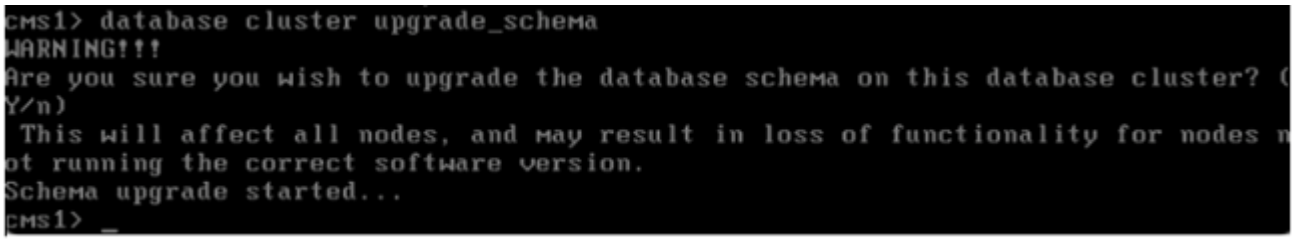


Figura 32: En la primera, confirme Y solo cuando las conexiones del clúster de Call Bridge hayan fallado después de esta actualización de clúster desordenada.

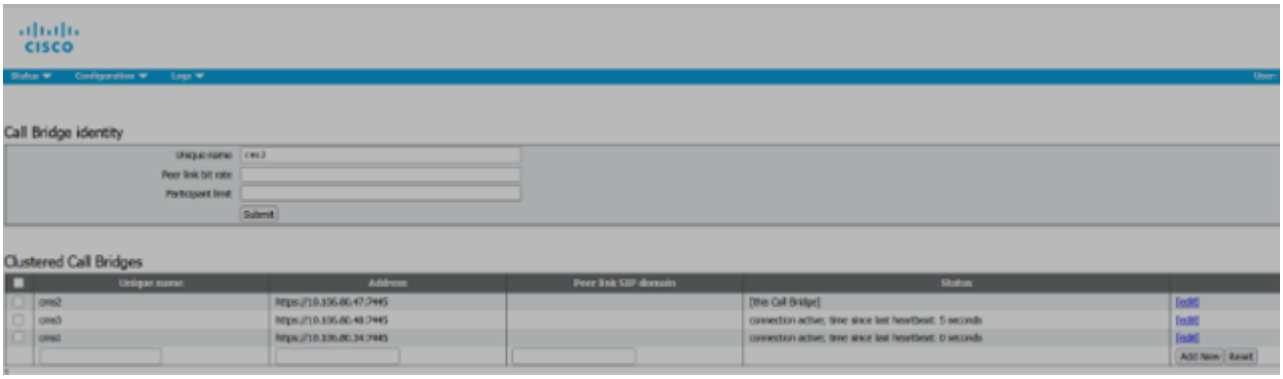


Figura 33: Después de la actualización del esquema, verifique que cada par de Call Bridge muestre una conexión activa.

4. Complete el procedimiento secreto de MeetingApps en la sección Clave secreta de MeetingApps después de la restauración en cada puente web, luego valide la implementación con el uso de la sección Validación posterior a la actualización.

Situación 4: clúster de base de datos con almacenamiento seguro habilitado

Utilice este procedimiento para un clúster de base de datos en VM, Meeting Server Small o Meeting Server Medium, donde Almacenamiento seguro está habilitado en los nodos. No se aplica a Meeting Server 2000. En primer lugar, actualice cada nodo a 3.13.x.

Registrar detalles de clúster y crear copias de seguridad cifradas

1. Ejecute secure_storage en cada nodo y confirme Enabled: Verdadero.

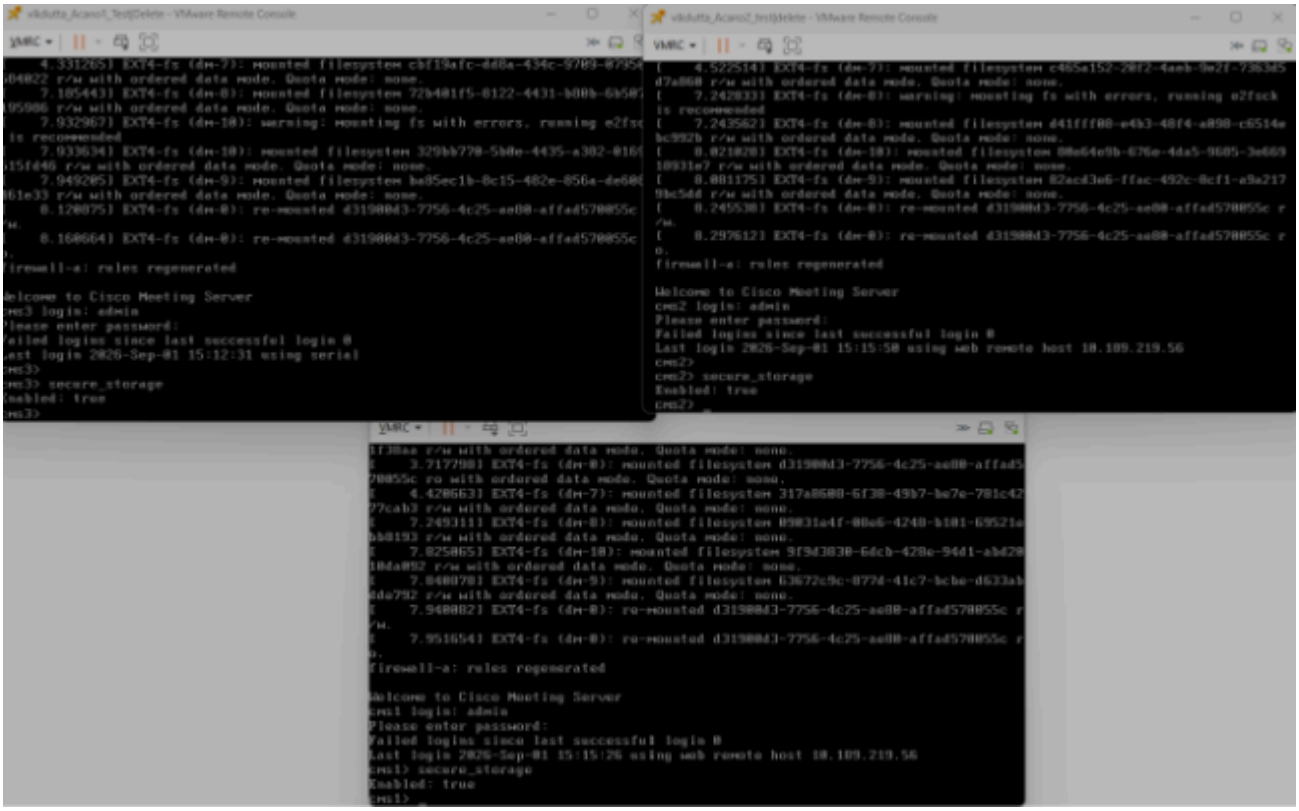


Figura 34: Para el clúster de tres nodos ilustrado, confirme que Almacenamiento seguro muestra Habilitado: True en todos los nodos antes de actualizar.

2. Registre la base de datos principal actual y confirme que las réplicas están en sincronización.

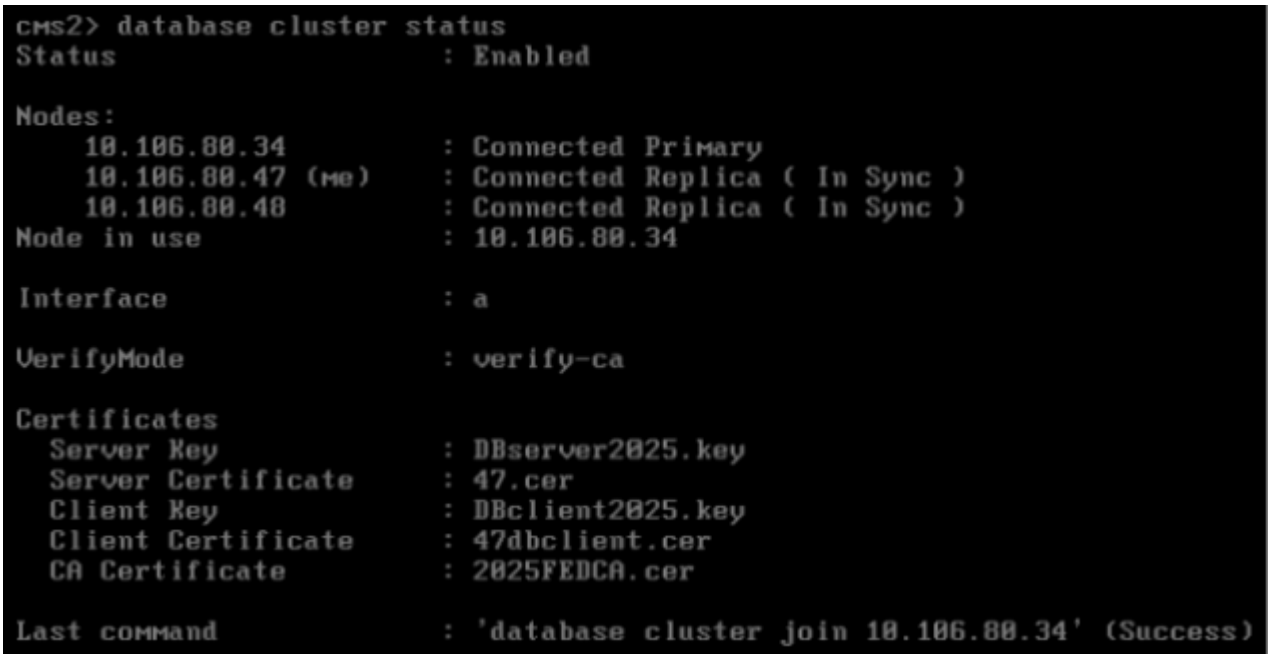


Figura 35: estado del clúster de base de datos antes de la actualización. Registre las réplicas principales y confirme que están sincronizadas.

3. Confirme que todos los tipos de llamadas en uso funcionan y que las condiciones de error están desactivadas en todos los nodos (sección Validar el estado del servidor antes de crear copias de seguridad).

4. Cree una copia de seguridad cifrada de todos los nodos con la sección Realizar una Copia de Seguridad cuando esté Activado el Almacenamiento Seguro. Asigne y registre una frase de contraseña única para cada archivo o utilice una política de frases de contraseña documentada. Transfiera sólo los archivos cifrados de los servidores antes de disolver el clúster.

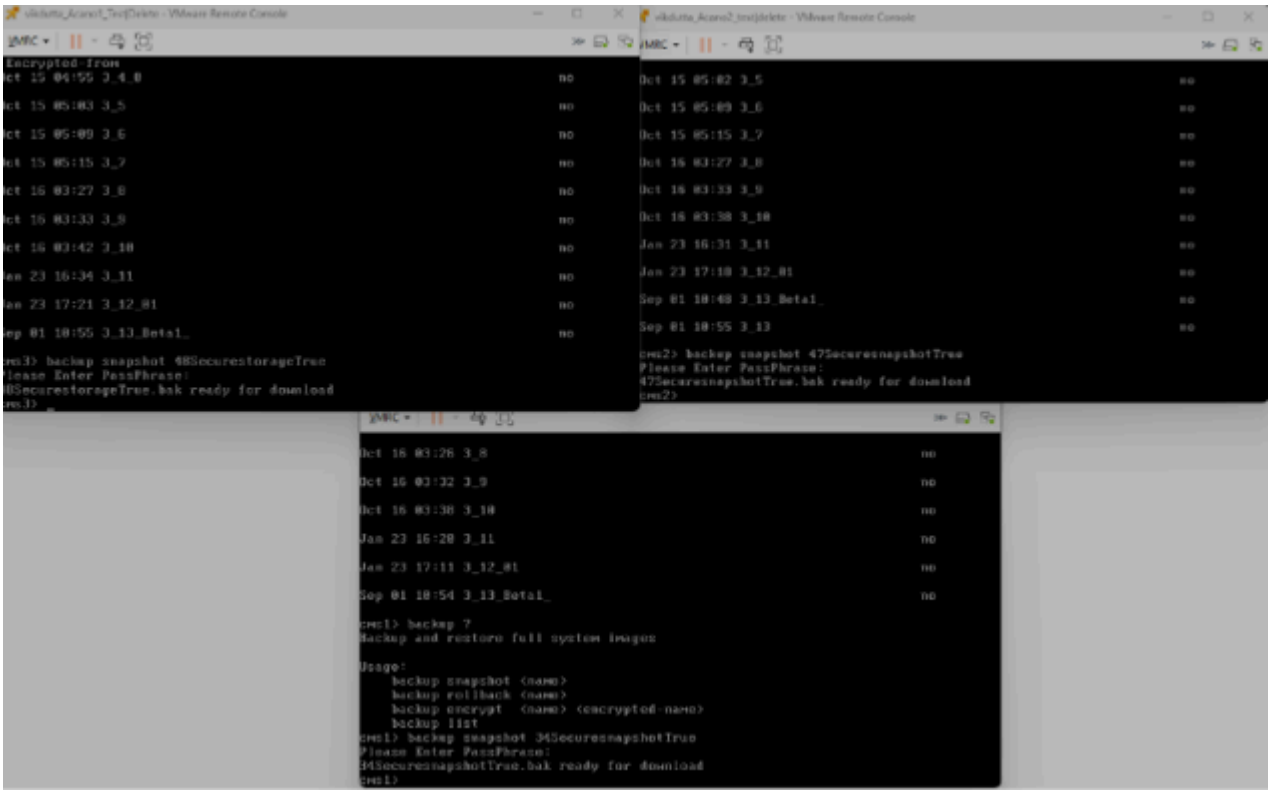


Figura 36: Instantánea de seguridad cifrada en cada nodo. El ejemplo muestra el mensaje de la frase de contraseña y, a continuación, cada archivo .bak listo para descargar.

Disolver, actualizar y restaurar

Desasocie el clúster como se describe en el Escenario 3 en este orden: nodos conectados, réplicas y el último nodo principal. Utilice database cluster remove y confirme que todos los nodos han salido del clúster.

Actualice los nodos independientes en paralelo. Recupere el direccionamiento de red desde la consola (sección Primer arranque y Restauración de red).

Cargue la copia de seguridad cifrada de cada nodo. Antes de realizar una reversión, confirme que la instantánea cargada aparece en la lista de copia de seguridad como cifrada: yes. Restaure primero el primario anterior y, a continuación, las réplicas y los nodos conectados. Utilice el comando backup rollback que aparece a continuación, confirme Y e introduzca la frase de contraseña de la copia de seguridad cuando se le solicite. El nodo se reinicia después de que se acepte la frase de contraseña. Repita este procedimiento para cada nodo.

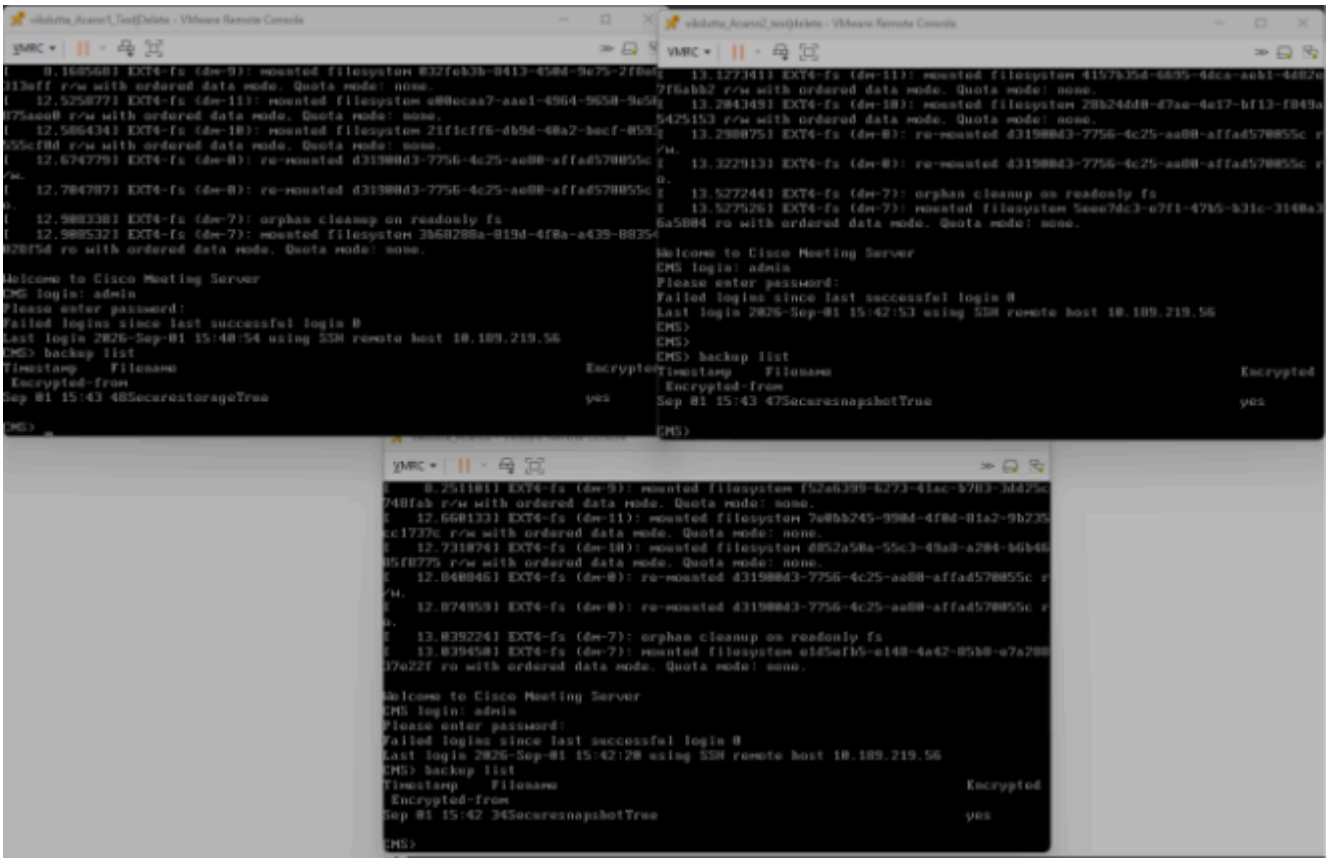


Figura 37: Después del primer inicio 4.0, la instantánea cargada debe aparecer en la lista de copia de seguridad como cifrada: sí y esté preparado para la reversión.

backup rollback encrypted-filename

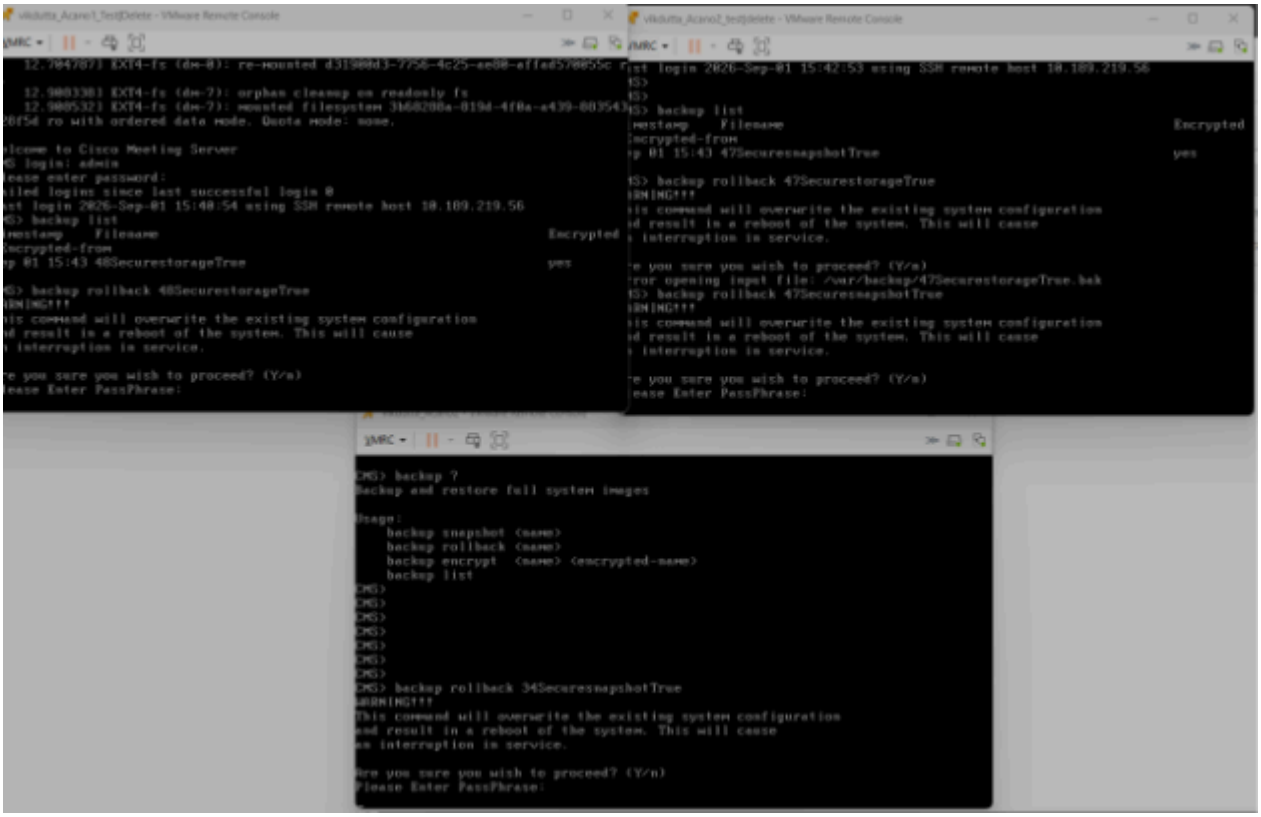


Figura 38: Confirme Y, introduzca la frase de paso y restaure en primer lugar la primera frase de contraseña principal.

Nota: Si las conexiones de clúster de Call Bridge no se activan después de esta restauración, ejecute el **database cluster upgrade_schema** en la anterior conexión principal solamente y vuelva a comprobar el estado de Call Bridge.

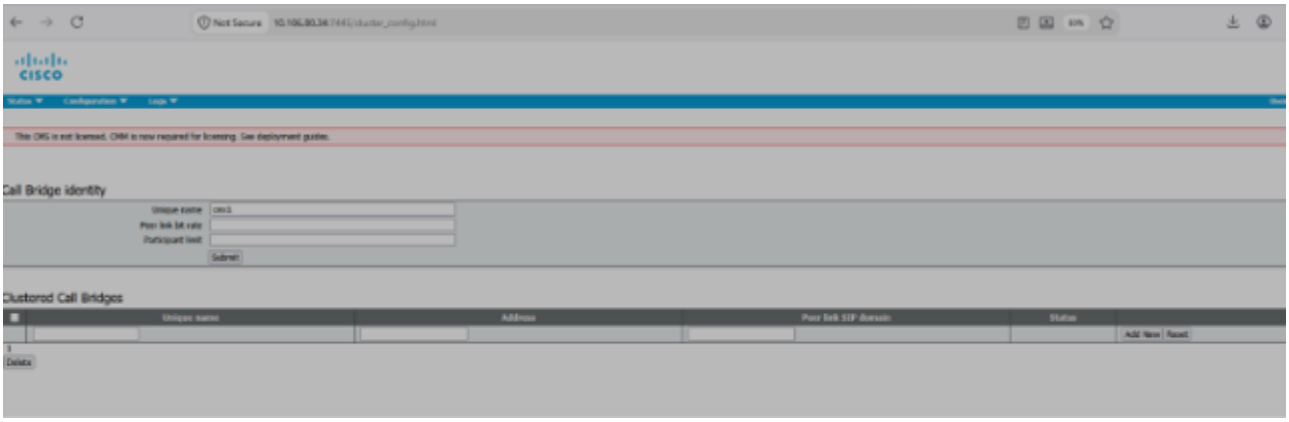


Figura 39: Antes de la actualización del esquema, el ejemplo muestra el clúster de base de datos que se ejecuta mientras Clustered Call Bridges está vacío.

database cluster upgrade_schema

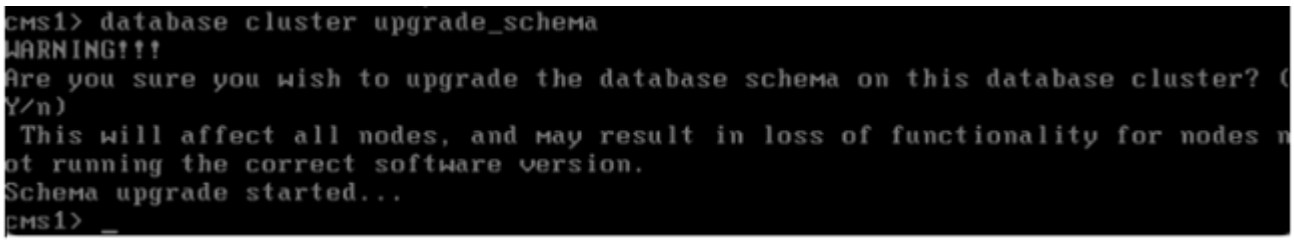


Figura 40: En la primera, confirme Y solo cuando las conexiones del clúster de Call Bridge hayan fallado después de esta actualización de clúster desordenada.

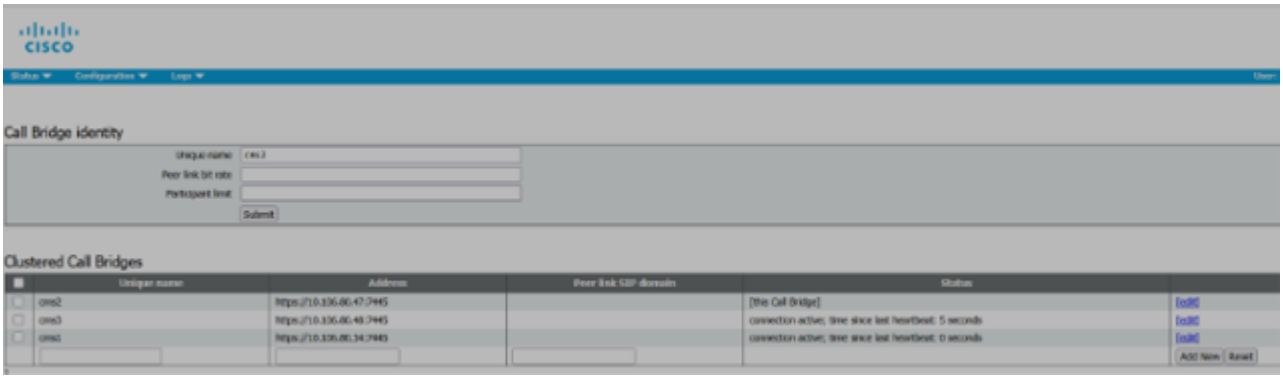


Figura 41: Después de la actualización del esquema, verifique que cada par de Call Bridge muestre una conexión activa.

Complete el procedimiento secreto de MeetingApps en la sección Clave secreta de MeetingApps después de la restauración en cada puente web, luego valide la implementación con el uso de la sección Validación posterior a la actualización.

Validación posterior a la actualización

Complete esta lista de comprobación después de la restauración y antes de devolver el sistema a producción:

- Administración web en cada nodo muestra Cisco Meeting Server 4.0.
- Los servicios MMP necesarios están habilitados y en ejecución (activo: True).
- Las condiciones de falla son claras. Tratar los errores y advertencias recientes como informativos a menos que exista un error correspondiente.
- Si procede, el estado del clúster de la base de datos muestra las réplicas y principales esperadas.
- Se restauran las licencias inteligentes y la conectividad de Call Bridge.
- Las llamadas SIP y las llamadas de cliente de Web App admitidas por esta implementación se han completado correctamente.
- La personalización de marca, las indicaciones de audio y los archivos SSO que se copian del servidor en la sección Requisitos previos a la actualización se restauran si no se han incluido ya en la copia de seguridad.
- Si se implementa MeetingApps, el puente web muestra la nueva relación entre MeetingApps y funciona el uso compartido de archivos.
- Elimine las instantáneas de corta duración solo después de que se haya aceptado la implementación.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).