Atualização do Meeting Server para a versão 4.0 - White Paper

Contents

- Introdução
- Informações de Apoio
- Visão geral do armazenamento seguro
  - Plataformas suportadas
  - Notas de implementação
- Princípios e Restrições de Atualização
  - Caminho de Atualização Necessário
  - Downgrades
  - Requisitos críticos de backup para upgrades da versão 4.0
  - Primeira Configuração de Login e Senha
  - Restabeleça a conectividade de rede após a atualização
  - Validar Integridade do Servidor Antes de Criar Backups
- Requisitos de pré-upgrade
- Procedimentos comuns de backup e restauração
  - Dados Afetados Após Atualização 4.0
  - Fazer um Backup Quando o Armazenamento Seguro Estiver Desabilitado ou Indisponível
  - Fazer um backup quando o armazenamento seguro estiver habilitado
  - Restaurar dados após atualização do 4.0
  - Chave Secreta de MeetingApps Após Restauração
- Primeira inicialização e restauração da rede
- Cenários de atualização
  - Cenário 1 - Nó único com armazenamento seguro desativado ou indisponível
  - Cenário 2 - Nó único com armazenamento seguro ativado
  - Cenário 3 - Cluster do Banco de Dados com Armazenamento Seguro Desabilitado
    - Registrar detalhes do cluster e fazer backup de cada nó
    - Dispensar o Cluster
    - Atualizar e restaurar os nós
  - Cenário 4 - Cluster de banco de dados com armazenamento seguro habilitado
    - Registrar detalhes do cluster e criar backups criptografados
    - Disband, Upgrade e Restore
- Validação pós-atualização

Introdução

Este documento descreve como atualizar o Cisco Meeting Server para a versão 4.0.

Informações de Apoio

Use este documento junto com as notas de versão do Cisco Meeting Server, o Guia de Referência de Comandos do MMP e o Guia de Referência do Administrador do Secure Storage para entender os requisitos e pré-requisitos.

O processo de atualização do Cisco Meeting Server 4.0 difere das versões anteriores porque a aplicação da imagem aciona uma redefinição de fábrica do nó. Para garantir a continuidade do serviço, todas as configurações anteriores, que incluem configurações e senhas de rede, devem ser preservadas por meio de um backup exportado para um local externo antes de você iniciar a atualização.

Além disso, o Armazenamento Seguro era opcional nas versões 3.11 a 3.13 do Cisco Meeting Server, mas é habilitado por padrão na versão 4.0. Como resultado, você deve seguir procedimentos diferentes de backup e restauração se nunca tiver usado o Armazenamento Seguro ou se já o tiver habilitado na versão 3.11x, 3.12x ou 3.13x.

O Armazenamento Seguro criptografa a chave privada e os arquivos de backup no servidor e exige que esses arquivos sejam criptografados antes que você possa transferi-los para o armazenamento externo.

Este documento consolida as orientações necessárias em uma única referência para que você possa seguir um procedimento comum para todos os cenários de atualização sem a necessidade de repetir as mesmas etapas.

Este documento aborda estes tópicos:

- O que é Armazenamento Seguro, onde se aplica e o que não faz.
- O caminho de upgrade, que inclui o requisito de acessar o 3.13.x antes do 4.0 e o fato de que um downgrade do 4.0 não é suportado.
- Um método comum de backup e restauração para nós em que o Armazenamento Seguro está habilitado e para nós em que ele está desabilitado ou indisponível.
- O nó de cluster do banco de dados desfaz o sequenciamento enquanto o cluster do banco de dados é desfeito antes de uma atualização.
- A chave secreta do MeetingApps, que não está armazenada em um backup do Cisco Meeting Server e deve ser gerada novamente após uma restauração.



Note: Este documento usa capturas de tela de laboratório capturadas durante o teste de orientação de atualização original, incluindo as versões 4.0 do software beta. Todos os

---

nomes de host, endereços IP e nomes de arquivo exibidos são estritamente ilustrativos e não refletem credenciais de produção reais ou senhas confidenciais. Para manter a clareza e evitar redundância, as etapas repetidas são mostradas apenas uma vez na seção de procedimento comum, a menos que a exibição de cluster forneça contexto necessário adicional.

Visão geral do armazenamento seguro

O Armazenamento Seguro fornece segurança de dados aprimorada criptografando arquivos confidenciais que residem no Servidor de Reunião e controlando como esses arquivos são descarregados do servidor Call Bridge. O recurso foi introduzido no Cisco Meeting Server 3.11 como uma opção configurável com o uso do comando MMP secure_storage enable em implantações de máquina virtual (com base em especificação ou Meeting Server Small) e no Meeting Server Medium.

A partir da versão 4.0, o Armazenamento seguro é ativado por padrão. Essa configuração agora é permanente e irreversível, e o comando secure_storage enable MMP foi removido.

Com o Armazenamento Seguro, o Servidor de Reunião impõe este comportamento:

- As chaves privadas não podem ser baixadas através do SFTP até que sejam criptografadas. Criptografe uma chave privada com o comando pki encrypt MMP seguido por uma senha de pelo menos 14 caracteres. Isso não altera as chaves usadas no momento pelos serviços do Servidor de Reunião.
- Os arquivos de backup criados com o comando backup encrypt **<name>** encrypted-name são criptografados. Quando o armazenamento seguro está ativado, o comando backup encrypt **<name>** encrypted-name MMP solicita uma senha com pelo menos 14 caracteres. A mesma senha é necessária durante a restauração do backup.
- Antes de baixar um arquivo de backup, ele deve estar criptografado. Se um backup listado ainda não estiver criptografado para exportação, use backup encrypt **<name>** encrypted-name. As tentativas de baixar um backup não criptografado são negadas.
- A partir da versão 3.12, o Armazenamento Seguro pode operar quando o FIPS está habilitado. Os arquivos de chave privada que foram criados no 3.11 com uma senha mais curta devem ser regenerados com o uso de uma senha de pelo menos 14 caracteres.



Tip: O Armazenamento Seguro restringe a transferência de chaves privadas não criptografadas e arquivos de backup não criptografados do Servidor de Reunião. Ele não restringe a transferência de arquivos de certificado. Os certificados ainda podem ser copiados com o SFTP; somente as chaves privadas não criptografadas associadas são

bloqueadas até que sejam criptografadas com a criptografia pki.

⚠ Caution: Uma vez habilitado, o Armazenamento seguro não pode ser desabilitado com nenhum comando MMP. Operação irreversível. Somente fatory_reset full redefine o Armazenamento Seguro como falso. Faça um backup de configuração com um instantâneo de backup e armazene-o em um dispositivo separado antes de habilitar o Armazenamento Seguro. Após o secure_storage, habilite a reinicialização imediatamente. Se a reinicialização for ignorada, o Armazenamento Seguro poderá ser marcado como habilitado sem ser totalmente inicializado, e os comandos como fatory_reset full poderão falhar. O caminho de recuperação nesse estado é reverter para um instantâneo salvo anteriormente (isso só é válido para o 3.13.x). No Servidor de Reunião 4.0, o secure_storage é habilitado por padrão.

Plataformas suportadas

- Máquina virtual (baseada em especificação): Supported
- Servidor de Reunião Pequeno/1K: Supported
- Servidor de Reunião Médio: Supported
- Meeting Server 2000: Não suportado. O recurso Armazenamento Seguro não está disponível. Não use comandos do Armazenamento seguro nesta plataforma.

O Cisco Meeting Server 4.0 ativa o Armazenamento Seguro por padrão em todas as plataformas compatíveis. Após o upgrade, os dados são automaticamente protegidos pelo Secure Storage, mesmo que o backup do 3.13.x tenha sido feito com o Secure Storage desabilitado.

Notas de implementação

- Renomear a imagem de atualização não altera as configurações do Armazenamento Seguro.
- Confirme o status do Armazenamento seguro em cada nó com o uso do comando secure_storage antes de fazer backups.
- O comando informa se o Armazenamento Seguro está habilitado (True) ou não (False). No Meeting Server 2000, o comando não é aplicável; ao atualizar o Cisco Meeting Server 2000, siga as etapas mencionadas nas condições de atualização em que o Armazenamento Seguro está desabilitado ou indisponível.



Saída de MMP quando o Armazenamento seguro não está habilitado (Habilitado: falso).



Figura 2: Saída de MMP quando o Armazenamento seguro está habilitado (Habilitado: verdadeiro) no Cisco Meeting Server 3.13.

Avisos detalhados da sintaxe de comandos e exemplos de uso podem ser encontrados no Guia de Referência Rápida do Administrador do Cisco Meeting Server para Armazenamento Seguro e na Referência de Comandos do MMP que você está usando no momento.

Princípios e Restrições de Atualização

Caminho de Atualização Necessário

As atualizações do Cisco Meeting Server devem seguir um caminho sequencial sem ignorar as principais versões. Por exemplo, um nó no 3.11.x deve avançar pelo 3.12.x e 3.13.x antes de alcançar a versão 4.0. Atualizações diretas de versões anteriores, como 3.9.x para 3.13.x ou 3.11.x para 4.0, não são suportadas e geralmente causam erros de configuração irrecuperáveis. Para Meeting Server Medium com versões 3.11.5 ou 3.13, o caminho de atualização seria 3.11.5 → 3.13 → 4.0.

Tip: Antes de iniciar a atualização do 4.0, cada nó deve executar o Cisco Meeting Server 3.13.x, com um backup de configuração verificado exportado do sistema 3.13.x. Todos os procedimentos do cenário neste documento supõem que a atualização para a versão 3.13.x já esteja concluída.

Downgrades

Tip: Não há suporte para downgrade de 4.0.x para 3.13.x. Se a atualização falhar ou o sistema não funcionar como esperado, implante um novo OVA 3.13.x (ou recrie o dispositivo) e restaure o backup do 3.13.x. Mantenha instantâneos de hipervisor das máquinas virtuais 3.13.x durante a janela de atualização como uma opção de recuperação adicional. Os Instantâneos de VM não substituem os backups de configuração exportados.

Requisitos críticos de backup para upgrades da versão 4.0

Depois que a atualização 4.0 é confirmada, o nó é reinicializado em um primeiro estado de inicialização. Não dependa do backup automático gerado durante o processo de atualização, pois uma falha de atualização pode resultar na perda do acesso ao SFTP e tornar o arquivo inacessível. Somente os backups criados com o comando backup snapshot e copiados para o armazenamento externo podem ser usados de forma confiável para recuperação.

Primeira Configuração de Login e Senha

Após a primeira inicialização da versão 4.0, a senha MMP existente é removida do banco de dados. Faça login com o nome de usuário admin com uma senha em branco (sem senha). O sistema exige que você configure uma nova senha de MMP. O sistema solicita que você insira a senha duas vezes para verificação e confirmação. Como não há nenhum recurso de recuperação de senha para o Servidor de Reunião, certifique-se de gravar sua nova senha.

Note: Se você definir uma nova senha MMP na primeira inicialização, o comando backup rollback a substituirá pela senha que foi armazenada no backup do 3.13.x. Depois de restaurar o backup no servidor, você deve efetuar login com a senha que estava ativa no momento em que o backup foi criado.

Restabeleça a conectividade de rede após a atualização

Os endereços, máscaras e gateways IPv4 e IPv6 são perdidos junto com o restante da configuração. A conectividade de rede do Servidor de Reunião pode ser perdida após a atualização para 4.0. Você deve ter acesso serial, ao console do hipervisor ou ao CIMC para que possa atribuir o endereçamento novamente a partir do MMP.



Note: As implantações que usam reservas de DHCP normalmente retêm os mesmos endereços IP após a reinicialização. No entanto, o acesso do console deve permanecer disponível até que o endereço seja verificado. Não suponha que a conectividade SSH

seja restaurada até que o endereço IP seja confirmado.

Validar Integridade do Servidor Antes de Criar Backups

Após cada atualização para a versão 3.13, verifique se o servidor está em boas condições e se todos os serviços estão funcionando. Não ignore nenhuma condição de falha na página de visão geral do servidor. Se você encontrar erros/falhas, corrija-os antes de criar um instantâneo de backup no 3.13. Isso garante que um backup íntegro do servidor seja restaurado nos nós 4.0 atualizados, o que mantém seus erros de implantação livres.

Em Web Admin, abra Status e confirme se a seção Condições de falha está desmarcada. Ignore as entradas que aparecem somente em Erros recentes e avisos. Após uma atualização, é comum ver bancos de dados transitórios ou mensagens de Web Bridge lá; esses não são um motivo para restaurar ou atrasar o backup.

Se uma condição de falha permanecer por mais de dez minutos, resolva-a antes de fazer o backup. Uma restauração de um backup do 3.13.x que já contém falhas no 4.0 as transporta adiante.

Para sistemas em cluster, confirme se todos os tipos de chamada em uso estão funcionando (pontos de extremidade SIP e clientes do Web App) e se nenhuma condição de falha está listada em nenhum nó.

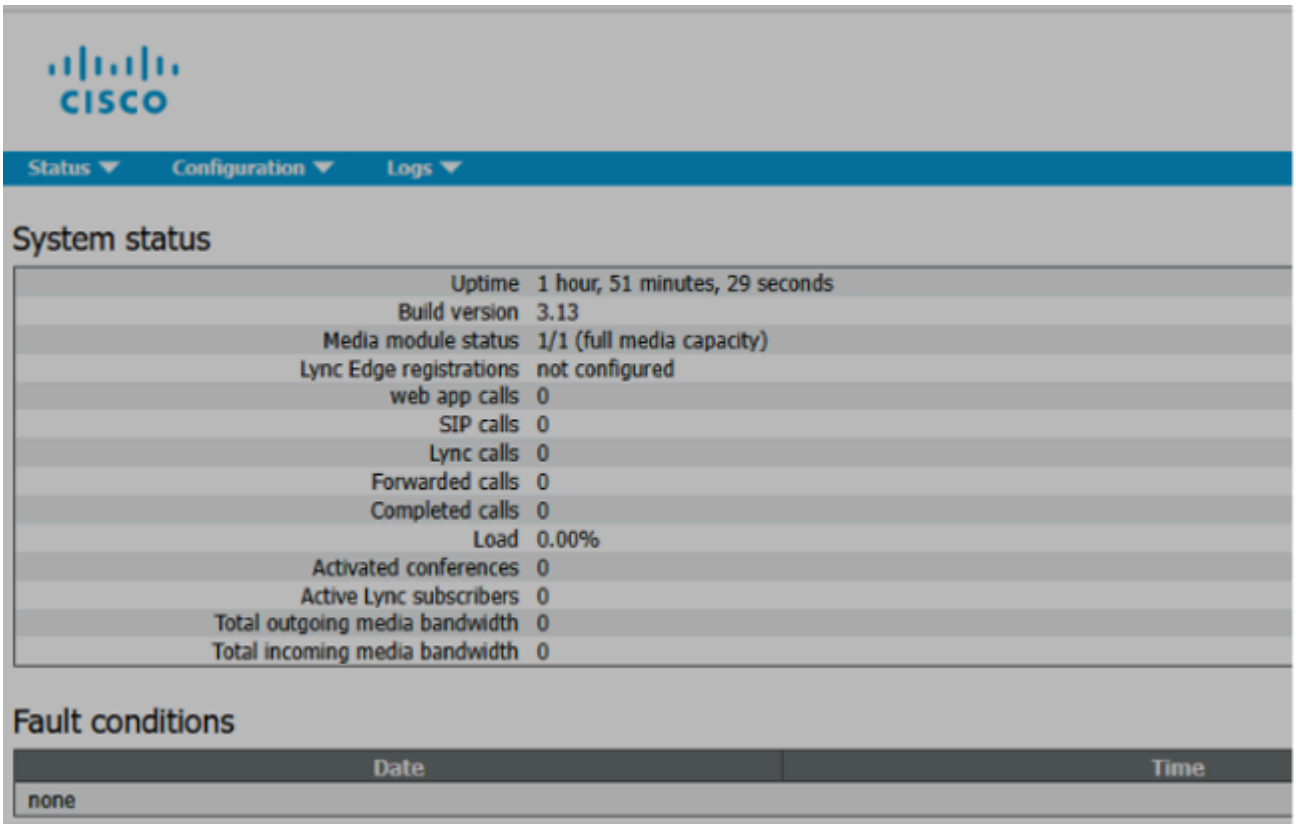


Figura 3: Página de status do administrador da Web no 3.13.x com condições de falha vazias. Use essa exibição antes de fazer o backup que é restaurado no 4.0.

Requisitos de pré-upgrade

Antes de iniciar a atualização para a versão 4.0, conclua estas ações. Esses requisitos se aplicam aos quatro cenários abordados mais adiante neste documento.

- Atualize para a versão 3.13.x e exporte um backup de configuração. Verifique se o nó está executando o Cisco Meeting Server 3.13.x. Crie um backup e transfira-o, juntamente com todos os dados SFTP personalizados, como logotipos, arquivos de marca, prompts de áudio, arquivos SSO e quaisquer outros dados personalizados, para o armazenamento externo. Use os procedimentos da seção Procedimentos Comuns de Backup e Restauração. Em um ambiente clusterizado, faça um backup de cada nó, não apenas do Primário Conectado, mas da Réplica Conectada.
- Registre as configurações de rede. Execute ipv4 a e armazene a saída. Você deve digitar novamente essas informações no console após a reinicialização da versão 4.0, a menos que uma reserva de DHCP restaure o endereço IP automaticamente.
- Confirme o acesso ao console. O console do hipervisor, o CIMC ou o acesso serial devem estar disponíveis antes de você iniciar. Espera-se que o SSH caia quando o nó reinicializar para 4.0.
- Faça download do pacote de log atual para arquivamento. Salve logbundle.tar.gz de cada nó. O pacote não substitui os snapshots de backup.
- Leia o banner de aviso de atualização 4.0 quando exibido após a execução do comando

upgrade.
- Pressione n para abortar se algum pré-requisito estiver incompleto. Pressione Y apenas quando estiver pronto para continuar.

Procedimentos comuns de backup e restauração

Os quatro cenários de atualização discutidos mais adiante neste documento usam o mesmo padrão de backup, exportação, primeira inicialização e restauração. Use esta seção como a única origem dessas etapas e, em seguida, siga apenas a sequência específica do cenário (nó único versus cluster e se o Armazenamento Seguro já está habilitado).

Dados Afetados Após Atualização 4.0

Estes dados são perdidos após a atualização 4.0 até que você restaure um backup:

- Conteúdo de banco de dados, que inclui espaços, usuários e perfis de chamada.
- Certificados e chaves privadas.
- Personalização local, arquivos SSO e arquivos de prompt de áudio.
- Configuração de rede (endereço IP, máscara e gateway), exceto onde uma reserva de DHCP restaura o endereço.
- A senha MMP anterior, até que a reversão do backup reaplique a senha do backup.
- O Call Bridge, o Web Admin, o Web Bridge e outros serviços de aplicativos retornam somente após a restauração.



Tip: O backup do Cisco Meeting Server não inclui a chave secreta do MeetingApps. Após uma restauração, você deve gerar novamente essa chave e aplicá-la a cada nó de Web Bridge. Consulte a seção Chave Secreta do MeetingApps Após a Restauração.

Fazer um Backup Quando o Armazenamento Seguro Estiver Desabilitado ou Indisponível

Siga este procedimento em máquinas virtuais, Meeting Server Small e Meeting Server Medium, onde secure_storage reports Habilitado: False e no Meeting Server 2000, onde o Armazenamento Seguro não está disponível.

1. Em cada nó, crie um arquivo com o comando backup snapshot. Não reutilize o nome de arquivo anterior.

2. Copie o arquivo de backup para o armazenamento externo com o SFTP imediatamente. Não mantenha a única cópia no Servidor de Reunião.

3. Armazene o arquivo em um local que ainda esteja acessível se o nó for reconstruído.

Exemplo:

backup snapshot cms313SecurestorageFalse backup list

4. Confirme se o arquivo aparece no comando backup list e transfira-o para um disco externo com um cliente SFTP.

5. Repita esse processo em todos os nós do cluster. Os nomes de backup podem conter apenas letras, números, sublinhado e hífen. Não inclua a extensão de arquivo .bak ao criar um arquivo de backup. Por exemplo, um nome de arquivo como 3.13SecurestorageFalse é rejeitado devido ao ponto.

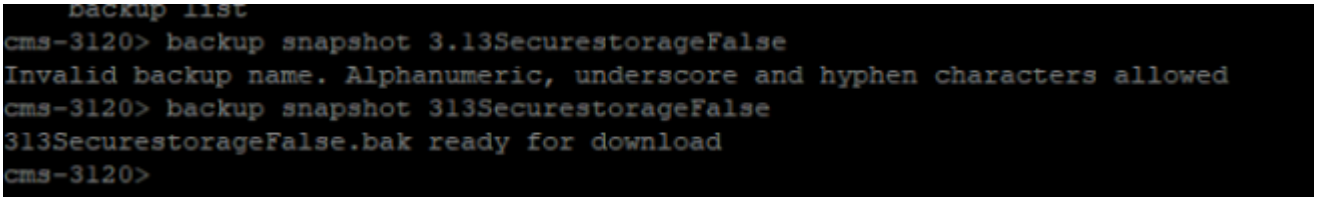


Figura 4: O instantâneo de backup rejeita um nome que contém um ponto e depois é confirmado com um nome alfanumérico. O arquivo .bak está pronto para ser baixado.



Figura 5: Copie o arquivo .bak da raiz SFTP do Servidor de Reunião para o armazenamento externo. Não deixe a única cópia no servidor.

Fazer um backup quando o armazenamento seguro estiver habilitado

Use este procedimento quando os relatórios secure_storage estiverem Habilitados: Verdadeiro. Arquivos de backup não criptografados não podem ser baixados.

1. Crie um instantâneo de backup em cada nó. Quando o Armazenamento Seguro está habilitado, o servidor solicita uma senha com pelo menos 14 caracteres. A senha pode incluir letras, números, caracteres especiais, símbolos ou espaços.

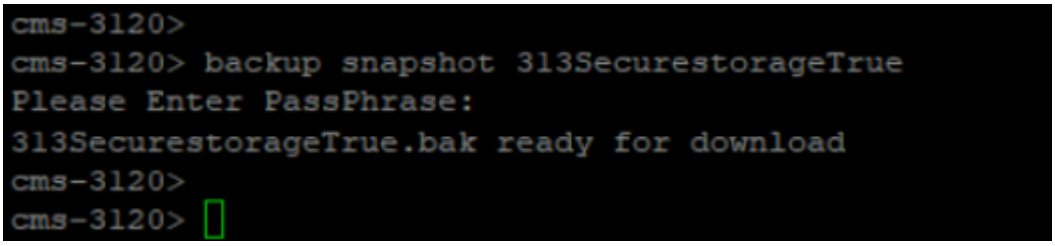


Figura 6: Instantâneo de backup com Armazenamento Seguro habilitado solicita uma vez uma senha com pelo menos 14 caracteres. O MMP não solicita que você confirme.

2. O MMP não solicita que você insira novamente a senha para confirmação. Proteja sua senha, pois você precisa da mesma senha para restaurar o arquivo. Não escolha uma senha trivial ou de exemplo.

3. Se o comando backup list mostrar um snapshot que não foi criptografado para exportação, criptografe-o antes de fazer o download:



Figura 7: Fazer backup da lista antes da criptografia. A coluna Criptografada é não, portanto, o arquivo não pode ser baixado.

4. Se você tentar baixar um backup não criptografado, o SFTP retornará um erro de permissão negada e o instruirá a executar o comando backup encrypt primeiro.

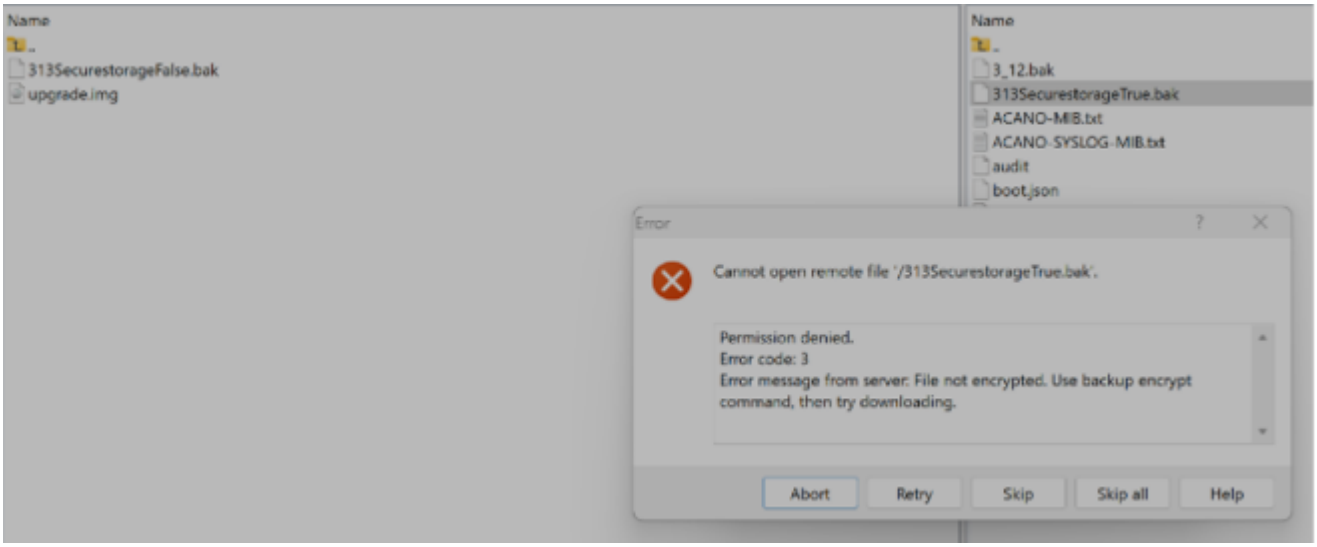


Figura 8: O SFTP nega o download de um backup não criptografado quando o Armazenamento Seguro está habilitado. A mensagem do servidor instrui você a executar a criptografia de backup.

5. Execute o comando backup encrypt para criptografar o arquivo de backup.

```
cms-3120> backup list
Timestamp    Filename                                          Encrypted  Encrypted-from
Sep 01 11:12 3_12                                              no
Sep 01 12:16 313SecurestorageTrue                              yes
cms-3120>
```

Figura 9: Lista de backup após o snapshot ser criptografado. Criptografado é sim e o arquivo pode ser transferido com SFTP.

A lista de backup exibe o status da criptografia e o nome do arquivo original. Assegure-se de transferir somente o arquivo criptografado de cada nó no cluster. Mantenha um registro organizado de cada nó, seu nome de arquivo correspondente e a senha associada.

Se você também precisar exportar chaves privadas, criptografe cada chave primeiro. Os arquivos de certificado não são bloqueados pelo Armazenamento Seguro e podem ser copiados sem esta etapa extra:

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

Use um nome de arquivo exclusivo em vez de substituir a chave atualmente em uso pelos serviços. O requisito mínimo de senha de 14 caracteres também se aplica aqui.

Restaurar dados após atualização do 4.0

1. Após o login na primeira inicialização e a recuperação de rede na seção Primeira inicialização e restauração de rede, copie o backup 3.13.x correspondente no nó com SFTP e restaure-o.

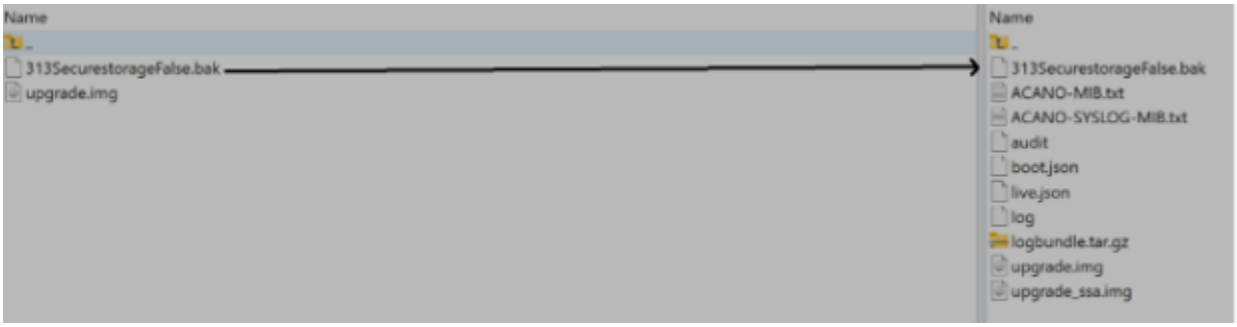


Figura 10: Após a recuperação da primeira inicialização da rede, copie o arquivo 3.13.x .bak de volta para o nó 4.0 com SFTP.

2. Confirme se o arquivo está presente:

lista de backup

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

cms-3120>
```

Figura 11: Uma lista de backup no 4.0 confirmando que o instantâneo carregado está presente antes da reversão.

3. Restaure o instantâneo. Em uma implantação de cluster, restaure primeiro o banco de dados primário anterior, seguido pelas réplicas e, em seguida, os nós 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: Reversão de backup de um instantâneo não criptografado. Confirmar com Y; o nó extrai o backup e reinicializa.

4. Pressione Y para continuar. O nó é reinicializado enquanto extrai o backup. Se o backup tiver sido feito com o Armazenamento seguro ativado, o MMP solicitará a senha. A reinicialização prossegue somente depois que a senha correta é aceita.

```
CMS>
CMS>
CMS>
CMS> backup rollback 313SecurestorageTrue
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)
Please Enter PassPhrase:
```

Figura 13: Reversão de backup de um instantâneo criptografado. Depois de Y, o MMP solicita a senha usada quando o backup foi criado.

⚠ Caution: O **backup rollback** substitui a configuração atual, os certificados, as chaves privadas

---

e o arquivo de licença e, em seguida, reinicializa o servidor. Use-o somente com o backup do 3.13.x que você exportou para este upgrade.

5. Quando o nó estiver novamente on-line, entre com as credenciais MMP do backup e confirme se cada serviço necessário relata como ativado e em execução (o MMP mostra isso como ativo: True).

Verificações típicas:

```
callbridge webbridge3 webadmin scheduler recorder streamer uploader meetingapps
```

6. Execute somente os comandos para serviços que este nó deve hospedar.

Chave Secreta de MeetingApps Após Restauração

O backup do Cisco Meeting Server não armazena a chave secreta do MeetingApps. Após a reversão de backup ser concluída, gere novamente o segredo e aplique-o a cada nó de Web Bridge. Ignorar esta etapa deixa o compartilhamento de arquivos indisponível, mesmo que os outros serviços pareçam íntegros.

1. No nó MeetingApps, execute o comando meetingapps gensecret.

2. Copie o segredo gerado para o armazenamento secreto. Cada execução de meetingapps gensecret invalida a chave anterior, portanto, gere a chave uma vez e reutilize o mesmo valor em todas as Web Bridges.

3. Execute estes comandos em cada nó de Web Bridge:

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

O último comando confirma que o serviço Web Bridge está em execução e que o MeetingApps está configurado corretamente. O MeetingApps não tem suporte no Meeting Server 2000 e o compartilhamento de arquivos não está disponível em clusters que incluam um Meeting Server 2000. Nessas implantações, essa etapa não é aplicável.

Primeira inicialização e restauração da rede

O comando 4.0 upgrade exibe um banner de aviso antes de continuar. Revise a mensagem cuidadosamente e aborte com n se algum pré-requisito estiver incompleto. Se você continuar com Y, o nó será reinicializado, a sessão SSH será desconectada e as etapas restantes deverão ser concluídas no console.

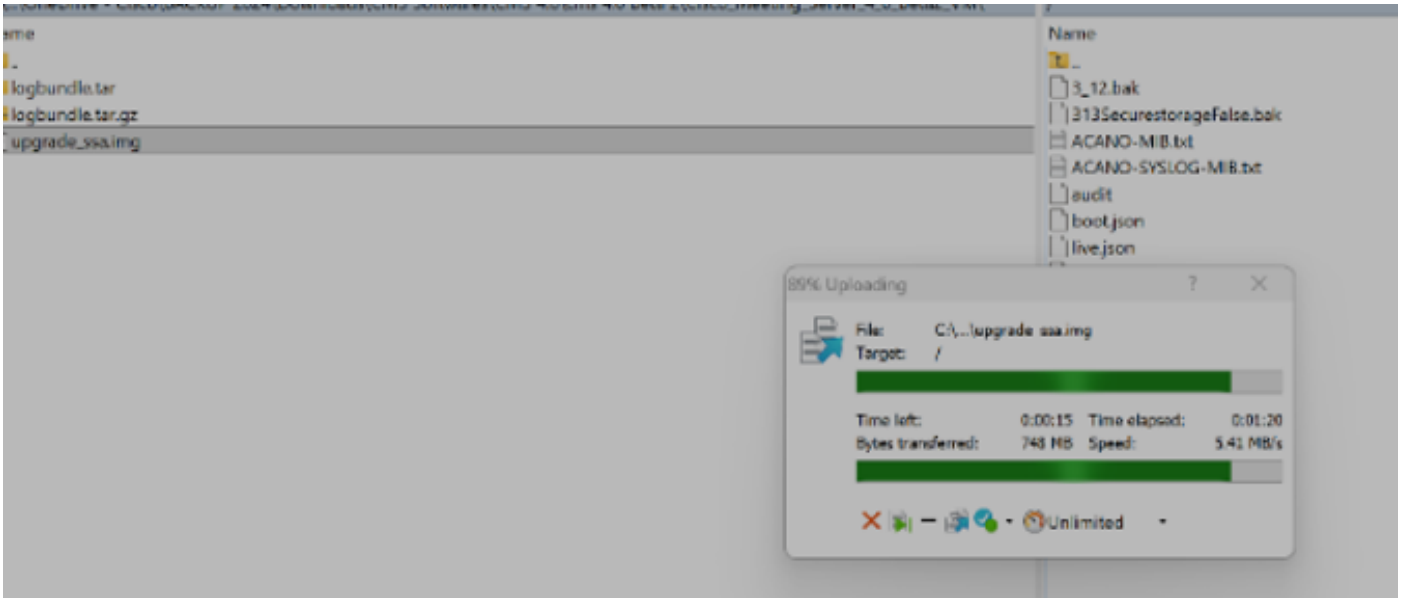


Figura 14: Carregue a imagem de atualização do 4.0 no diretório raiz do SFTP do Servidor de Reunião. O nome do arquivo da imagem de upgrade pode variar dependendo do pacote baixado de cisco.com.



Figura 15: O comando upgrade verifica a assinatura da imagem e inicia o processo. Não confie no backup automático criado neste ponto.

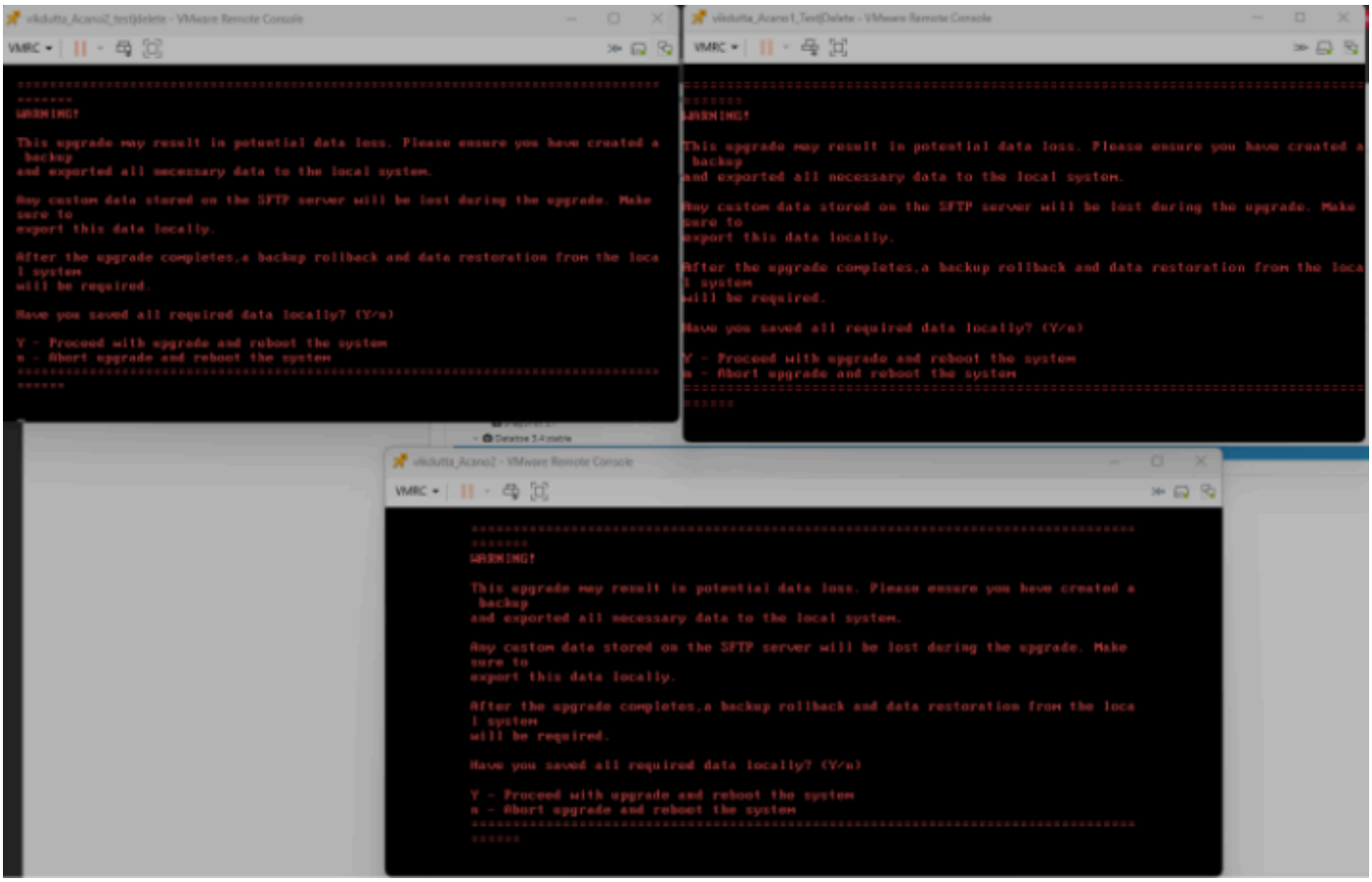


Figura 16: O aviso de MMP vermelho em um cluster de três nós. O mesmo banner aparece em um único nó. Pressione n para abortar se os backups e os dados personalizados não estiverem fora do servidor. Pressione S apenas para continuar e reinicializar.

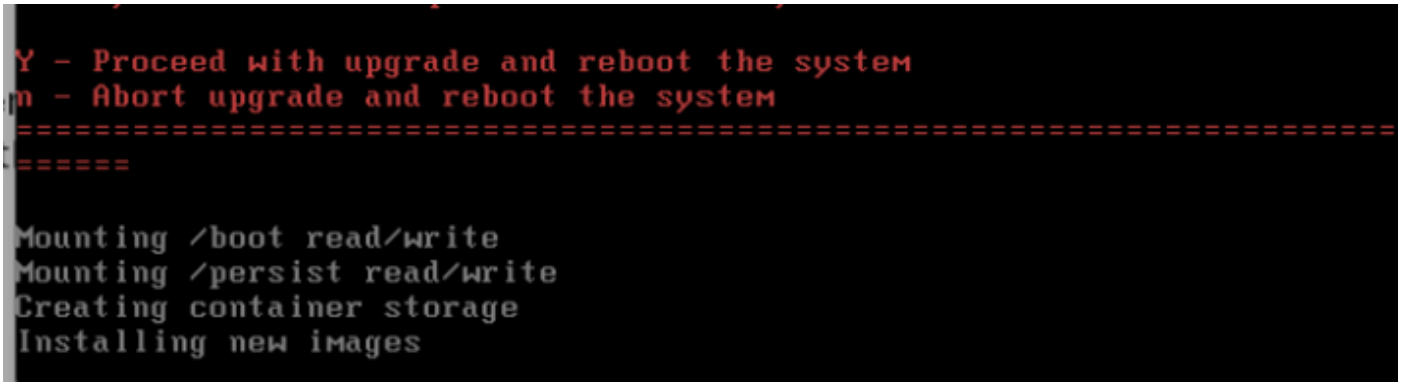


Figura 17: Após Y, o nó monta o armazenamento e instala a imagem 4.0. A sessão SSH expira; continue no console do hipervisor.

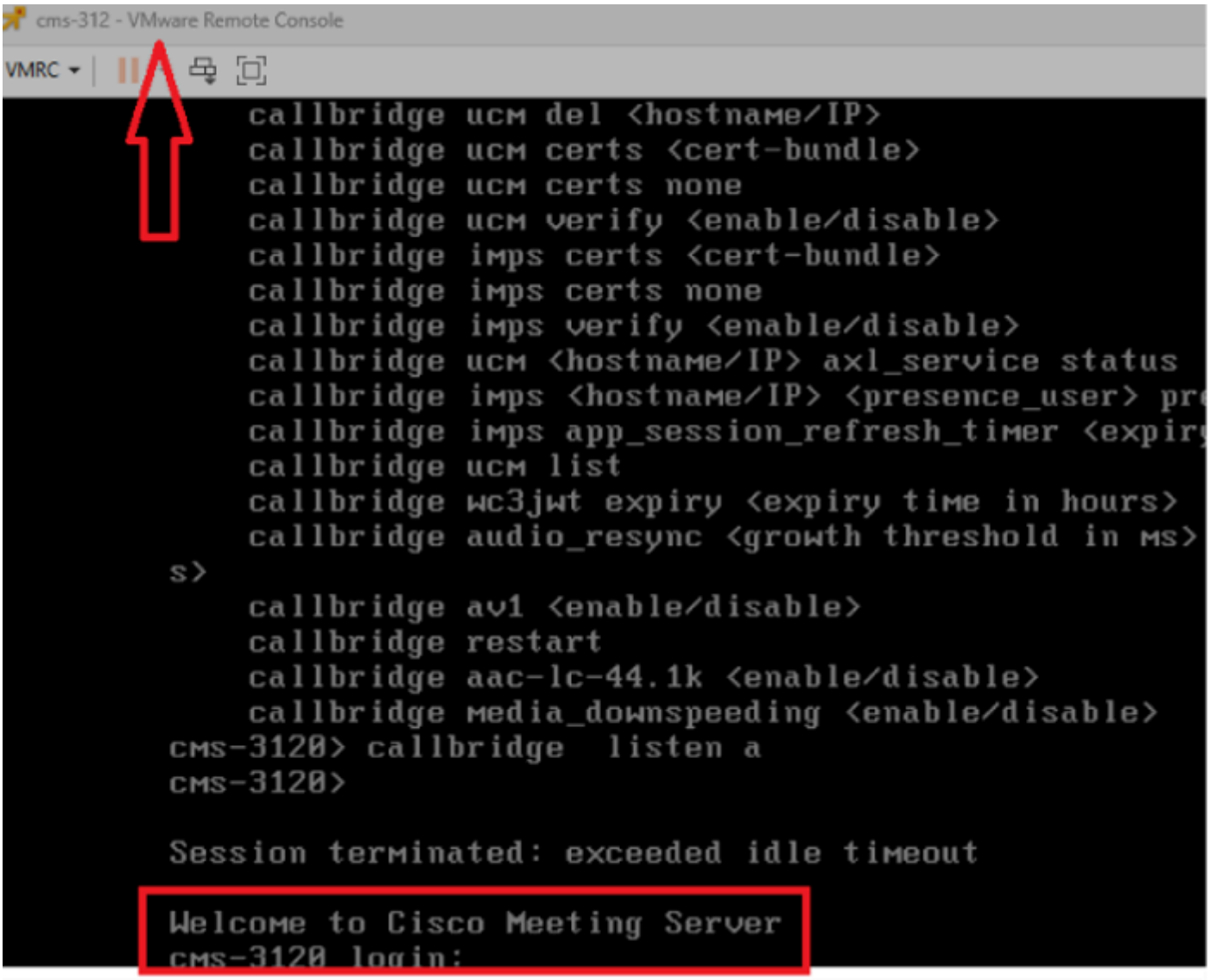


Figura 18: Use a VM ou o console do CIMC depois que o SSH cair. O prompt de login da primeira inicialização aparece quando a imagem 4.0 está pronta.

1. Faça login com a conta MMP de primeira inicialização (nome de usuário admin e sem senha) e defina uma nova senha MMP quando solicitado. Observe que a reversão de backup substitui essa senha pela senha armazenada no backup.

2. Reaplique a configuração de rede a partir das notas capturadas na seção Requisitos de Pré-upgrade:

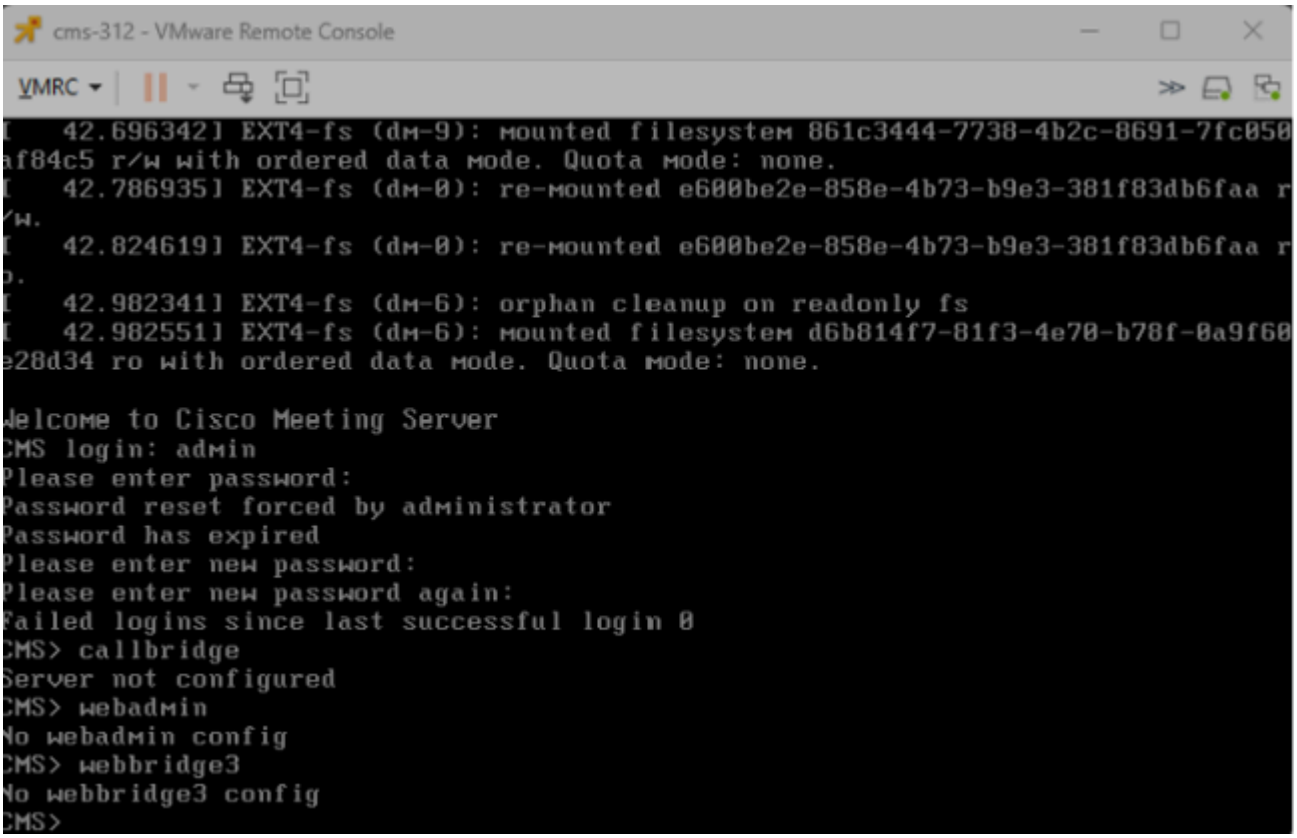


Figura 19: Primeiro login de MMP de inicialização.

A senha anterior não é mais válida. Depois que você definir uma nova senha, serviços como webadmin e webbridge3 serão exibidos como não configurados até que o backup seja restaurado.

3. Execute o comando:

ipv4 interface add address/prefix-length gateway

Por exemplo:

ipv4 a add 192.0.2.10/24 192.0.2.1



Figura 20: Reaplicando IPv4 do console.

Uma reinicialização é necessária depois que você atribui o endereço. Os endereços mostrados na

captura de tela são apenas para fins de exemplo.

4. Reinicialize depois que o endereço for atribuído. Quando o sistema estiver novamente on-line, continue com o carregamento SFTP do backup e com as etapas de restauração mencionadas na seção Restaurar dados após atualização do 4.0.

Note: Se uma reserva de DHCP estiver configurada, o endereço original já poderá ser atribuído após a reinicialização. Verifique o endereço com o **ipv4 a** antes de iniciar uma sessão SFTP a partir da estação de trabalho de gerenciamento.

No Cisco Meeting Server 4.0, o Armazenamento Seguro é ativado por padrão nas plataformas que o suportam. O MMP não pode mais expor o secure_storage como uma alternância após a atualização.



Figura 21: Nesta imagem 4.0, secure_storage não é um comando reconhecido porque o Armazenamento Seguro está habilitado por padrão.

Confirme a versão com o comando version.

Cenários de atualização

Este capítulo aborda diferentes cenários de atualização. Conclua a etapa de atualização para 3.13.x. Identifique o tipo de implantação e escolha o cenário adequado. Siga apenas o procedimento que corresponde ao seu ambiente e não combine etapas de implantações de cluster e nó único.

Primeiro conclua a atualização de etapa suportada para 3.13.x. Em seguida, selecione exatamente um cenário abaixo. Não combine os procedimentos de nó único e de cluster de banco de dados.

- Cenário 1: Nó único, Desabilitado ou indisponível, VM, Pequeno, Médio e Meeting Server 2000
- Cenário 2: Nó único, Habilitado, VM, Pequeno e Médio apenas

- Cenário 3: Cluster de banco de dados, Desabilitado ou indisponível, VM, Pequeno, Médio e Meeting Server 2000
- Cenário 4 : Cluster de banco de dados, habilitado, VM, pequeno e médio apenas

O Meeting Server 2000 não oferece suporte aos cenários habilitados para Armazenamento Seguro. Para essa plataforma, use o Cenário 1 ou 3, conforme aplicável.

Cenário 1 - Nó único com armazenamento seguro desativado ou indisponível

Use este procedimento para um servidor autônomo com Armazenamento Seguro desabilitado ou para o Meeting Server 2000, onde o Armazenamento Seguro não está disponível. A versão de origem pode ser 3.11.x ou posterior, mas o nó deve estar em 3.13.x antes de atualizar para 4.0.

1. Atualização de etapa para 3.13.x. Siga o caminho suportado (por exemplo, 3.11.x → 3.12.x → 3.13.x). Após cada salto, confirme a versão no Web Admin e se as condições de falha estão limpas, conforme descrito na seção Validar a integridade do servidor antes de criar backups.

2. Confirmar status do Armazenamento Seguro. Execute o comando secure_storage e verifique se o Armazenamento Seguro não está habilitado. Ignore o comando no Meeting Server 2000.

3. Crie e exporte um arquivo de backup do 3.13.x, conforme mencionado na seção Fazer um Backup Quando o Armazenamento Seguro Estiver Desabilitado ou Indisponível. Exporte também o conteúdo SFTP personalizado e o pacote de registro, conforme mencionado na seção Requisitos de pré-atualização.

4. Baixe a imagem do software 4.0 de Cisco.com, extraia-a e copie upgrade.img para o nó sobre SFTP.

5. Inicie a atualização com este comando:

```
upgrade upgrade.img
```

6. Leia o banner de advertência. Pressione S somente depois que todos os pré-requisitos estiverem completos. 6. Após a atualização, configure o nó conforme descrito na seção First-boot and Network Restoration e, em seguida, restaure o backup com o uso da seção Restore Data After 4.0 Upgrade.

Cenário 2 - Nó único com armazenamento seguro ativado

Use este procedimento para uma VM autônoma, um Servidor de Reunião Pequeno ou um Servidor de Reunião Médio onde o Armazenamento Seguro esteja habilitado. Ele não se aplica ao Meeting Server 2000.

Antes de transferir arquivos do servidor, observe que as chaves privadas não criptografadas e os arquivos de backup não criptografados não podem ser transferidos. Os arquivos de certificado não estão bloqueados.

1. Atualize pelo caminho suportado para a versão 3.13.x sem ignorar as versões. Após cada salto, confirme a versão e se as condições de falha estão limpas na seção Validar a integridade do servidor antes de criar backups.

2. Execute secure_storage e confirme se a saída mostra Enabled: Verdadeiro.

3. Crie e exporte um backup 3.13.x criptografado com o uso da seção Fazer um Backup Quando o Armazenamento Seguro Estiver Habilitado. Armazene a senha na sua loja secreta. Exporte também o conteúdo SFTP personalizado e o pacote de log (seção Requisitos de pré-atualização).

4. Copie o arquivo upgrade.img para o nó e execute a atualização:

```
upgrade upgrade.img
```

5. Leia o banner de aviso e pressione Y para continuar somente quando os pré-requisitos estiverem completos.

6. Recupere a rede do console (seção Primeira inicialização e restauração de rede) e restaure o backup criptografado com sua senha (seção Restaurar dados após atualização do 4.0). 6. Se o MeetingApps estiver em uso, aplique um novo segredo do MeetingApps (seção Chave Secreta do MeetingApps Após Restauração).

O Armazenamento Seguro é habilitado por padrão no Meeting Server 4.0. Após uma restauração, continue a tratar chaves privadas e arquivos de backup como dados criptografados.

Cenário 3 - Cluster do Banco de Dados com Armazenamento Seguro Desabilitado

Use este procedimento para um cluster de banco de dados com Armazenamento Seguro desabilitado, que inclui um cluster que contém o Meeting Server 2000. A partir da versão 3.5, o cluster do banco de dados deve ser desfeito antes da atualização do software. Primeiro, atualize cada nó para 3.13.x.

Registrar detalhes do cluster e fazer backup de cada nó

1. Execute secure_storage em cada nó. Trate o comando como indisponível nos nós do Meeting Server 2000.

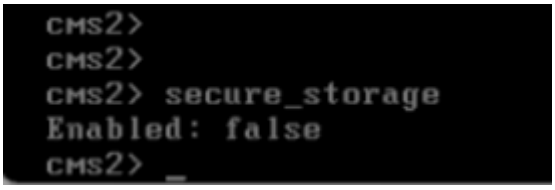


Figura 22: Antes de usar backups não criptografados, verifique se o Armazenamento Seguro está desabilitado em cada nó de cluster. Ignore o comando para nós do Meeting Server 2000, onde ele não estiver disponível.

2. Registre o nó primário do banco de dados atual, pois ele deve ser restaurado primeiro após a atualização para 4.0. Confirme se as réplicas estão Em Sincronia e se o status do cluster está íntegro.

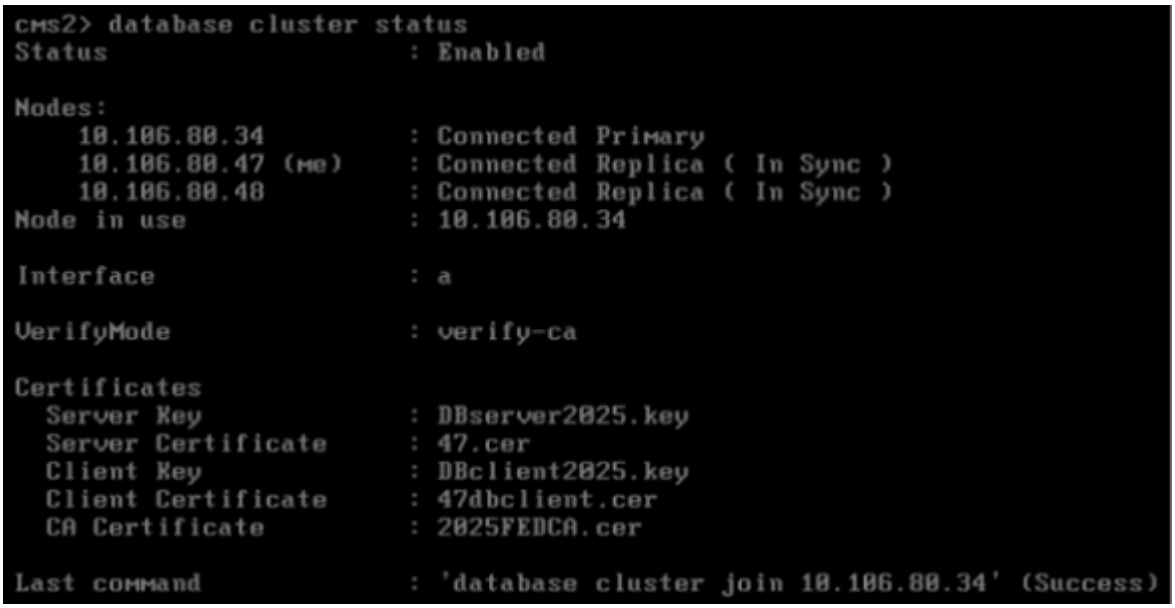


Figura 23: Registre a réplica primária atual e confirme se as réplicas estão em sincronia.

3. Confirme se todos os tipos de chamada em uso estão funcionando e se as condições de falha estão limpas em todos os nós (seção Validar a integridade do servidor antes de criar backups).

4. Crie um backup de cada nó com o uso da seção Fazer um Backup Quando o Armazenamento Seguro Estiver Desabilitado ou Indisponível. Nomeie cada arquivo de forma que ele seja mapeado claramente para o nó e transfira cada backup para o armazenamento externo antes de você dispensar o cluster.

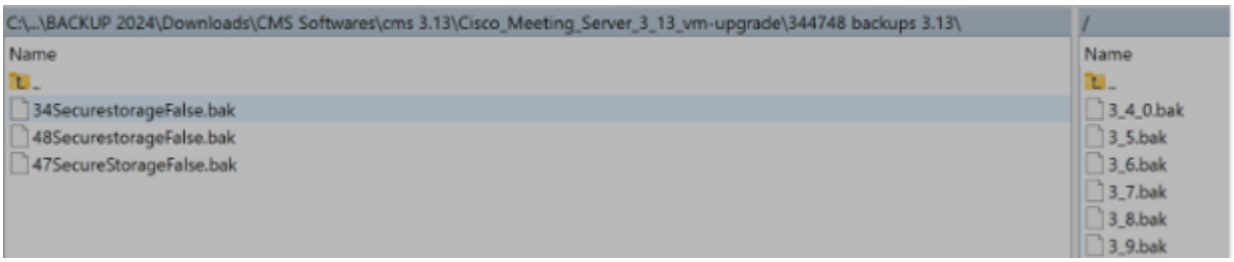


Figura 24: Todos os três exemplos de nó fazem backup de armazenamento externo armazenado, nomeado de modo que cada arquivo seja mapeado para seu nó.

Dispensar o Cluster

Remova os nós nesta ordem. Manter o primário até o fim:

- Nós do Servidor de Reunião conectados (não principais)
- Nós de banco de dados de réplica
- Nó de banco de dados primário

Em cada nó, execute o comando de remoção e pressione Y. Não continue para a atualização 4.0 até que cada nó informe que ele deixou o cluster. Uma remoção da associação do cluster deixa o banco de dados local do nó no lugar.

database cluster remove

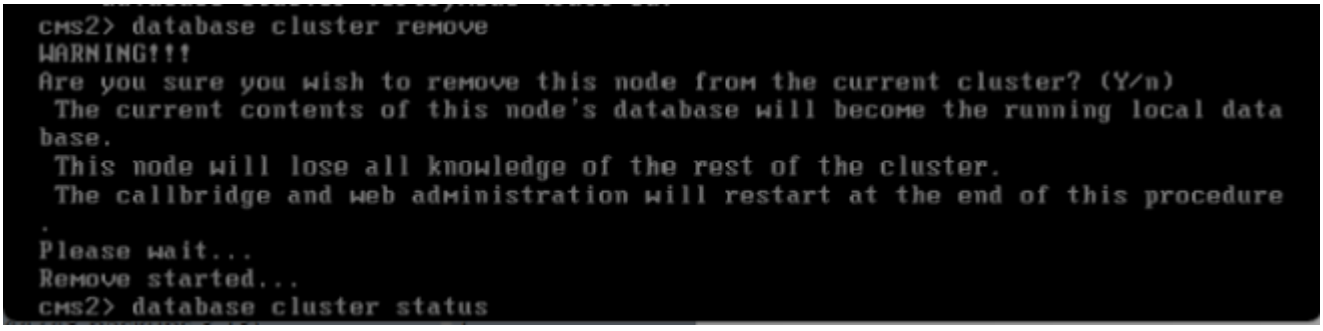


Figura 25: Em uma réplica, confirme Y para remover a associação do cluster. O banco de dados local do nó permanece no lugar.

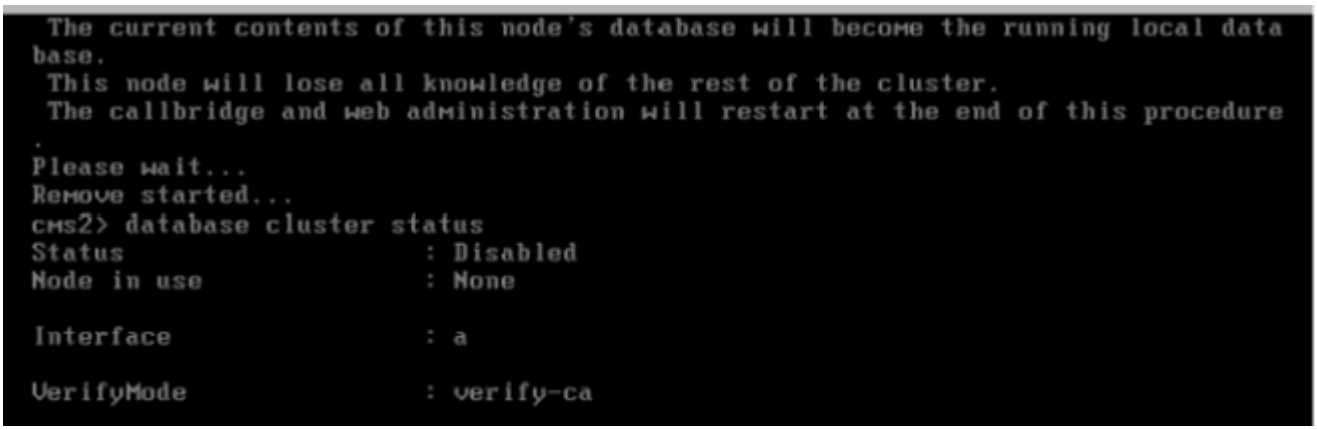


Figura 26: Após a remoção, verifique se o status do cluster está Desabilitado e se o Nó em uso é Nenhum nesse nó.

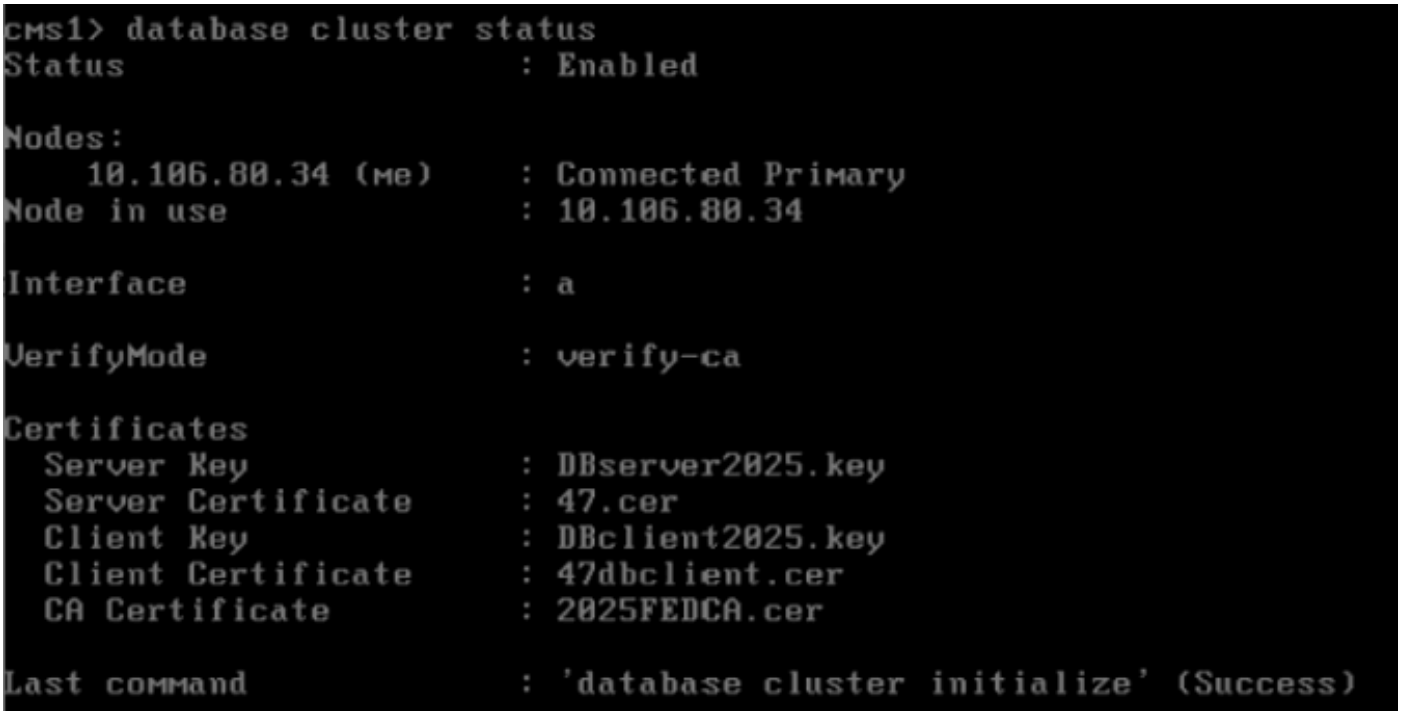


Figura 27: Após a remoção das réplicas, o primeiro principal é o único nó restante no cluster. Remova-o por último.

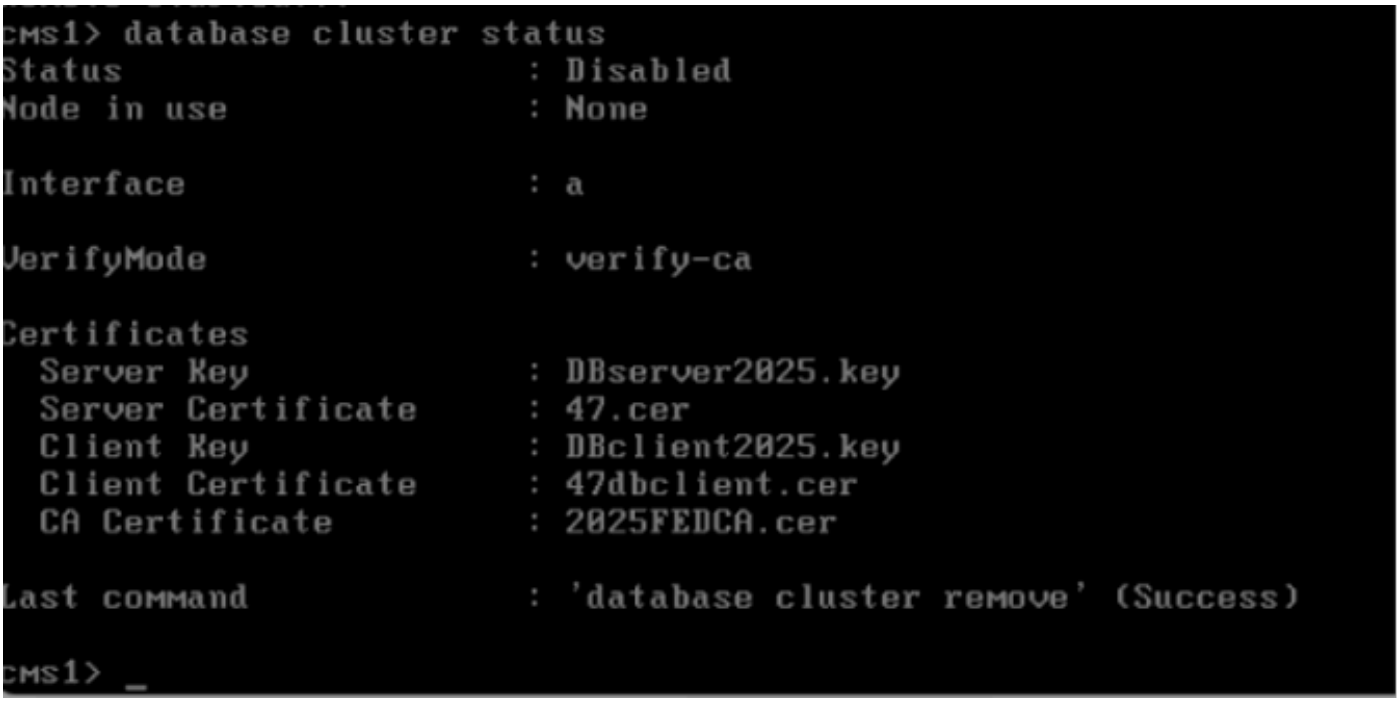


Figura 28: Após remover o primário anterior, verifique se o comando informa Success e o status do cluster está Desabilitado.

Atualizar e restaurar os nós

1. Uma vez dissolvidos, os nós são autônomos e podem ser atualizados em paralelo. Em cada nó, copie upgrade.img sobre SFTP e execute o comando upgrade:

upgrade upgrade.img

2. Recupere o endereçamento de rede de cada nó a partir do console (seção Primeira inicialização e Restauração de rede).

3. Copie o backup do 3.13.x de cada nó de volta para esse nó. Restaure primeiro o primeiro principal anterior, seguido pelas réplicas e, em seguida, os nós conectados. Use a seção Restaurar dados após atualização do 4.0. Uma restauração dos backups restabelece a associação do cluster de banco de dados.

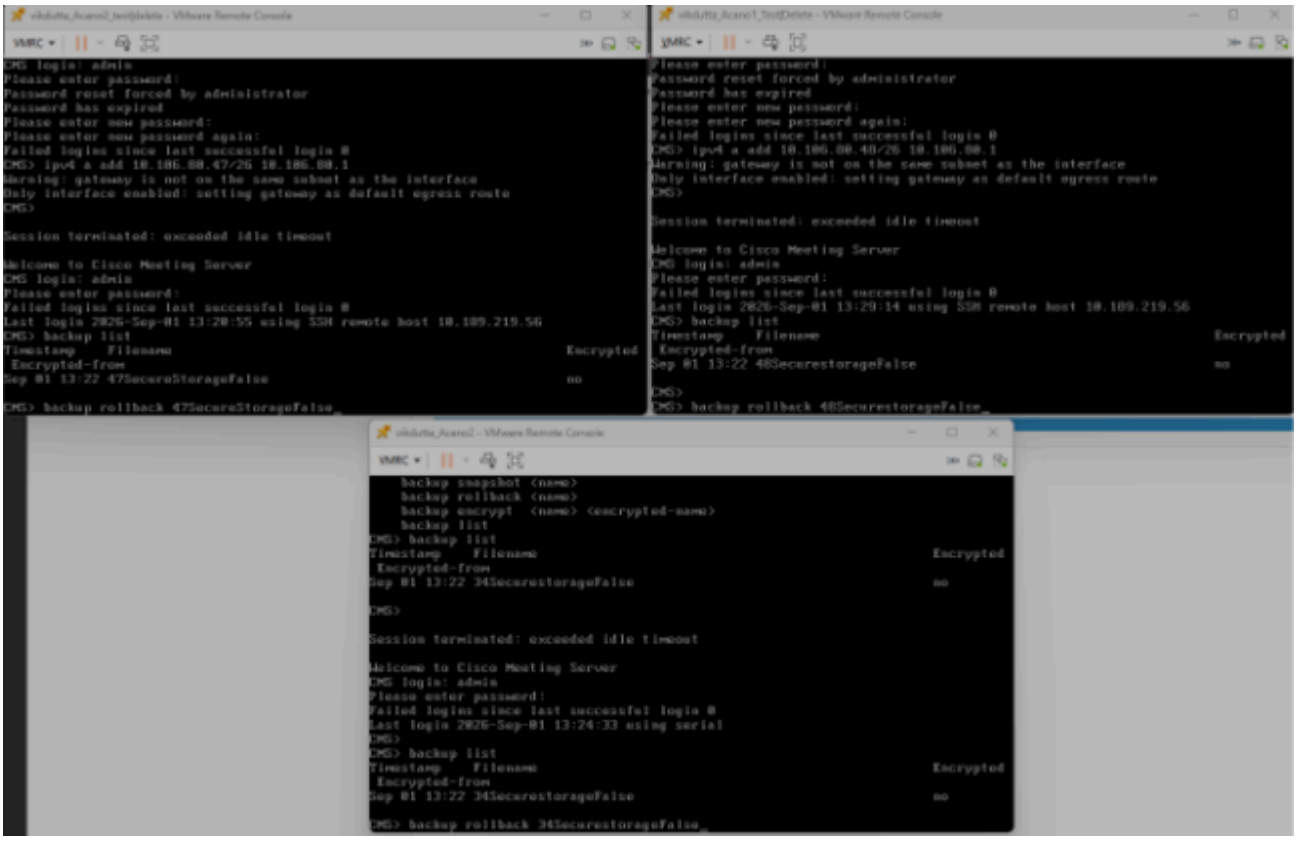


Figura 29: Restaure o instantâneo de cada nó. Comece pelo primário anterior e restaure as réplicas. Os nomes de arquivo de exemplo identificam seu nó.

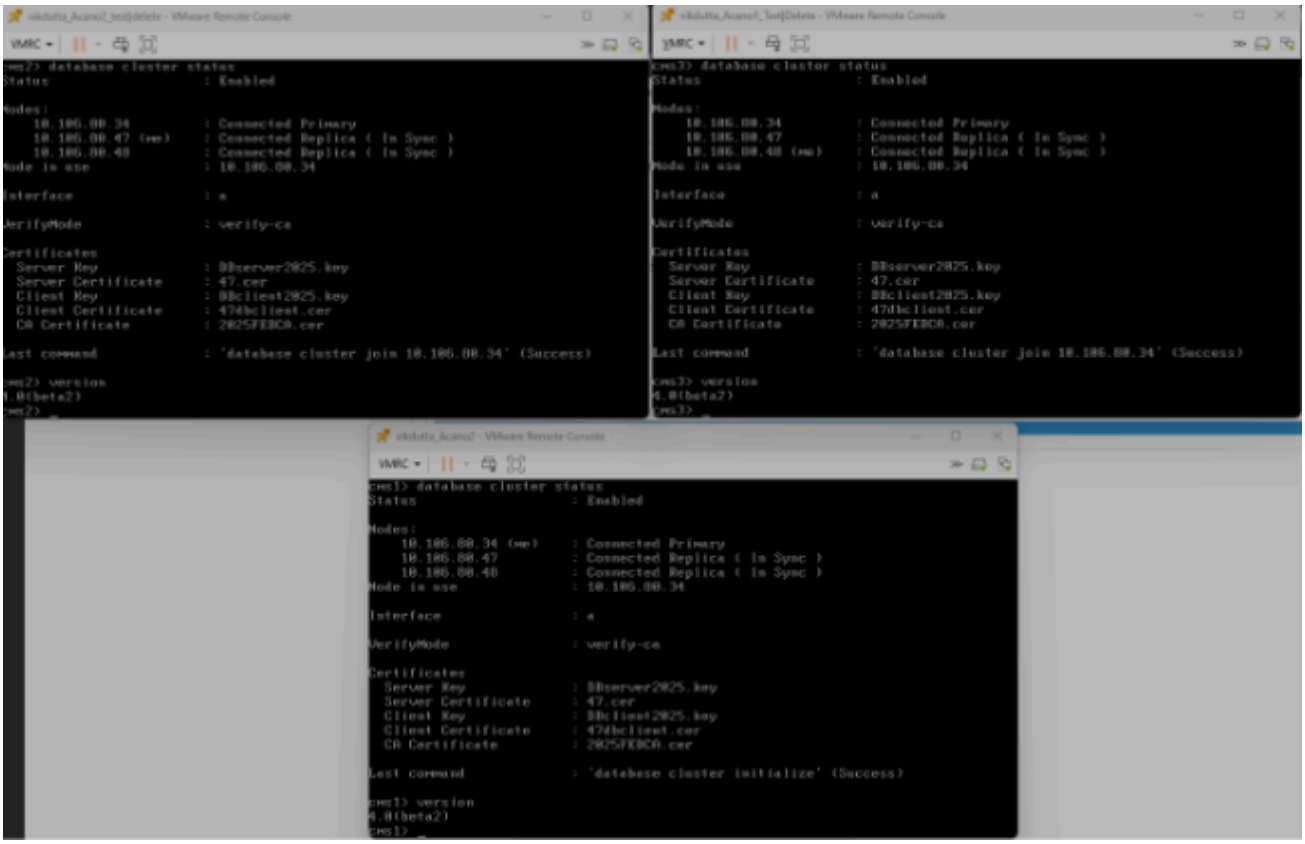


Figura 30: Após a restauração no Servidor de Reunião 4.0, verifique se o cluster está Habilitado, se o mesmo primário é mostrado e se as réplicas estão Em Sincronia.

Note: Se as conexões de cluster de Call Bridge não surgirem após essa restauração, execute o **database cluster upgrade_schema** somente no primário anterior e verifique novamente o status da Call Bridge.

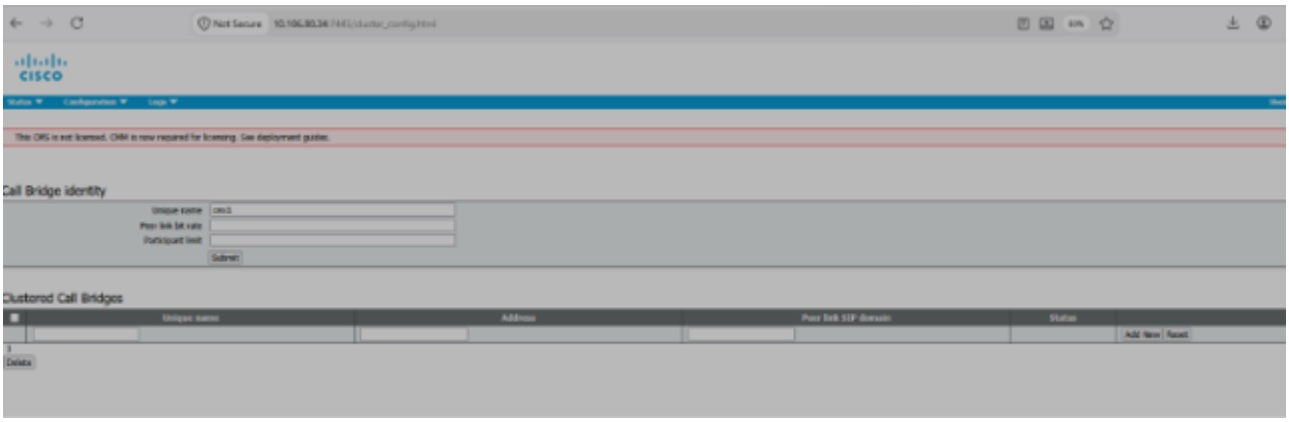


Figura 31: Antes da atualização do esquema, o exemplo mostra o cluster de banco de dados sendo executado enquanto as Call Bridges clusterizadas estão vazias.

database cluster upgrade_schema

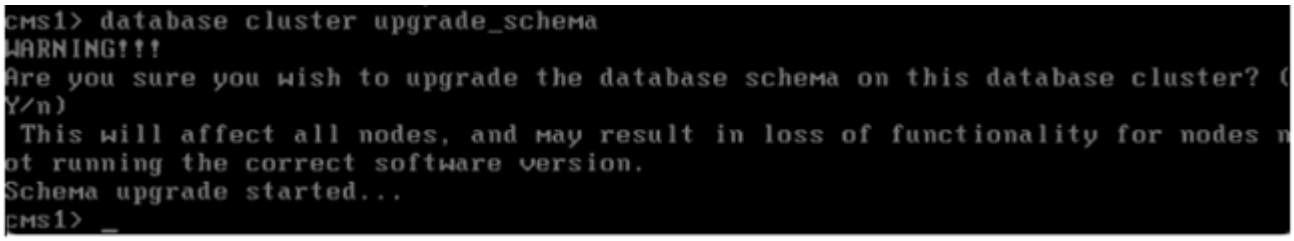


Figura 32: No primário anterior, confirme Y somente quando as conexões de cluster Call Bridge falharem após essa atualização de cluster desfeito.

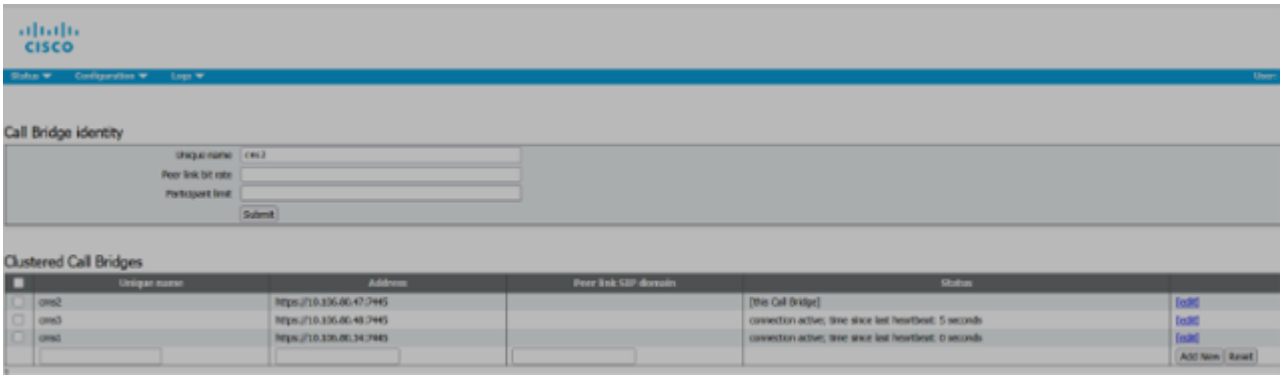


Figura 33: Após a atualização do esquema, verifique se cada peer de Call Bridge mostra uma conexão ativa.

4. Conclua o procedimento secreto do MeetingApps na seção Chave Secreta do MeetingApps Após a Restauração em cada Ponte Web e valide a implantação com o uso da seção Validação Pós-atualização.

Cenário 4 - Cluster de banco de dados com armazenamento seguro habilitado

Use este procedimento para um cluster de banco de dados em VMs, Meeting Server Small ou Meeting Server Medium onde o Armazenamento Seguro está habilitado nos nós. Ele não se aplica ao Meeting Server 2000. Primeiro, atualize cada nó para 3.13.x.

Registrar detalhes do cluster e criar backups criptografados

1. Execute secure_storage em cada nó e confirme Enabled: Verdadeiro.

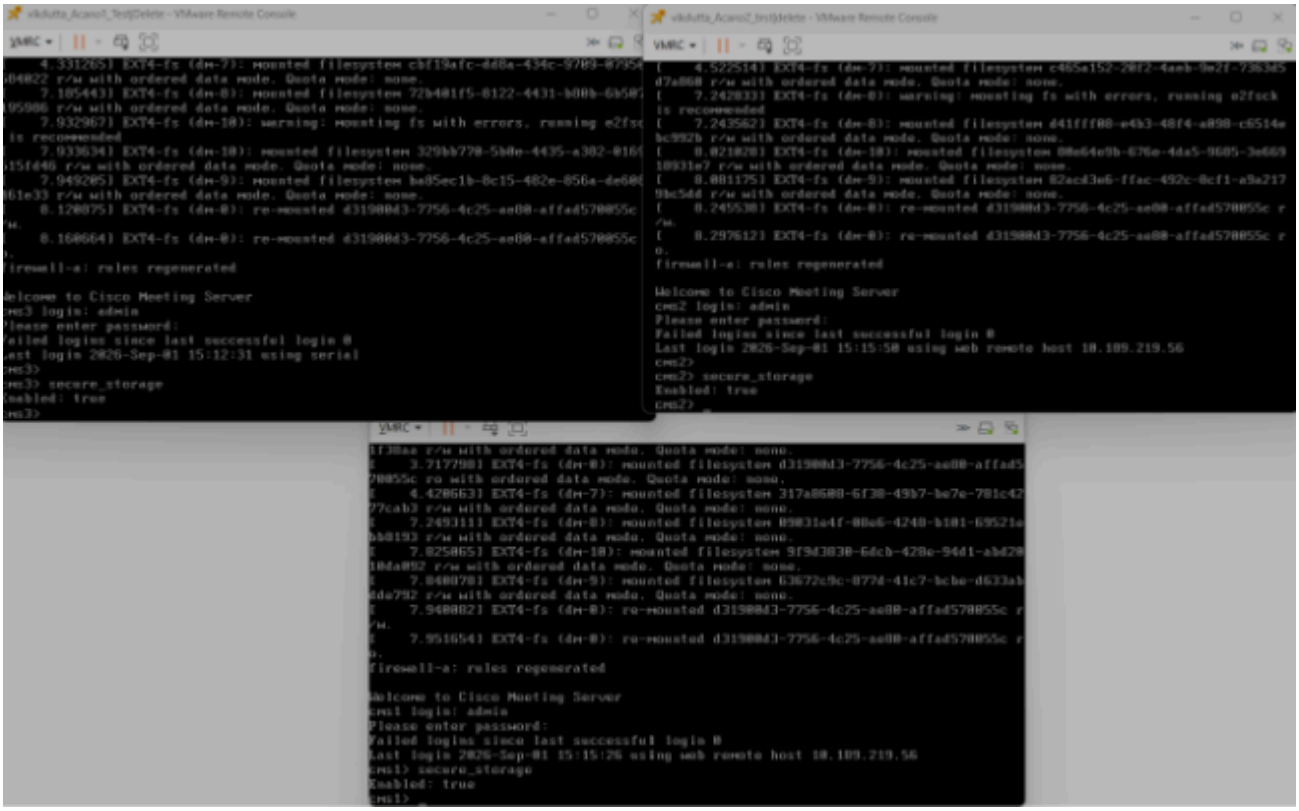


Figura 34: Para o cluster de três nós ilustrado, confirme se o Armazenamento seguro mostra Habilitado: Verdadeiro em todos os nós antes da atualização.

2. Registre o banco de dados principal atual e confirme se as réplicas estão Em Sincronia.

```
cms2> database cluster status
Status                    : Enabled

Nodes:
    10.106.80.34          : Connected Primary
    10.106.80.47 (me)     : Connected Replica ( In Sync )
    10.106.80.48          : Connected Replica ( In Sync )
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 join 10.106.80.34' (Success)
```

Figura 35: status do cluster do banco de dados antes da atualização. Registre a réplica primária e confirme se as réplicas estão em sincronia.

3. Confirme se todos os tipos de chamada em uso estão funcionando e se as condições de falha estão limpas em todos os nós (seção Validar a integridade do servidor antes de criar backups).

4. Crie um backup criptografado de cada nó com o uso da seção Fazer um Backup Quando o Armazenamento Seguro Estiver Habilitado. Atribua e registre uma senha exclusiva para cada arquivo ou use uma política de senha documentada. Transfira somente arquivos criptografados dos servidores antes de dissolver o cluster.

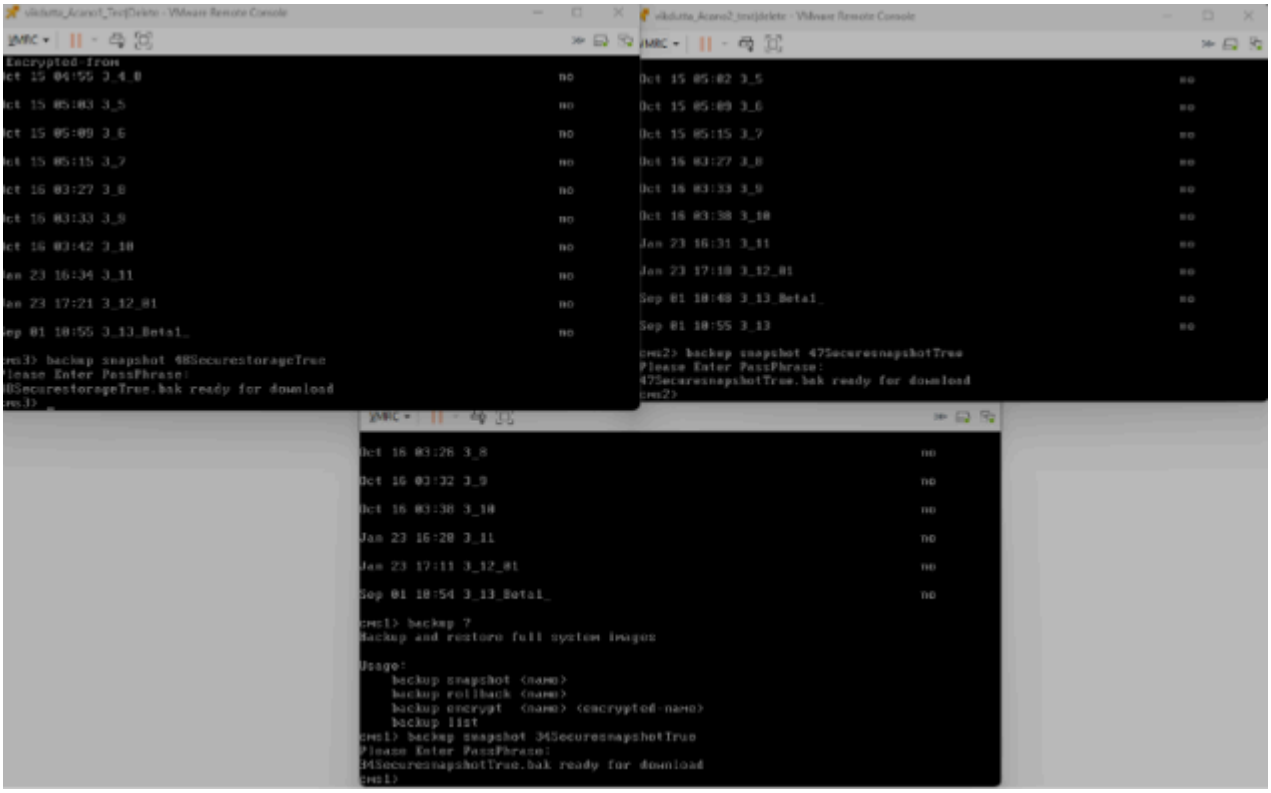


Figura 36: Instantâneo de backup criptografado em cada nó. O exemplo mostra o prompt da senha e, em seguida, cada arquivo .bak pronto para download.

Disband, Upgrade e Restore

Desfaça o cluster conforme descrito no Cenário 3 nesta ordem: nós conectados, réplicas e o principal por último. Use database cluster remove e confirme se cada nó saiu do cluster.

Atualize os nós independentes em paralelo. Recupere o endereçamento de rede do console (seção Primeira inicialização e Restauração de rede).

Carregue o próprio backup criptografado de cada nó. Antes de uma reversão, confirme se o snapshot carregado aparece na lista de backup como Criptografado: yes. Restaure primeiro o primário anterior e depois as réplicas e os nós conectados. Use o comando backup rollback abaixo, confirme Y e insira a senha do backup quando solicitado. O nó é reinicializado depois que a senha é aceita. Repita o procedimento para cada nó.

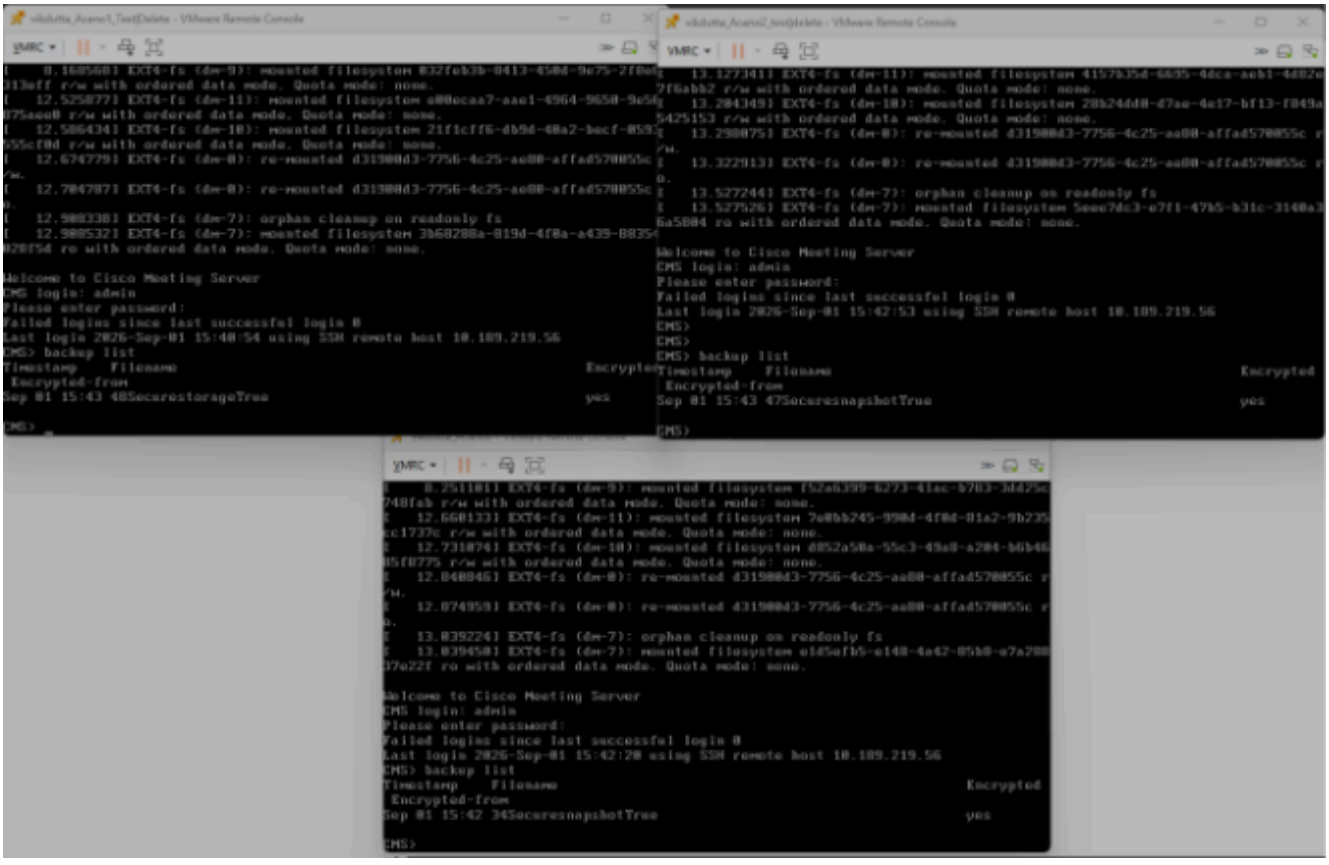


Figura 37: Após a primeira inicialização da versão 4.0, o snapshot carregado deve aparecer na lista de backup como Encrypted: sim e estar pronto para a reversão.

backup rollback encrypted-filename

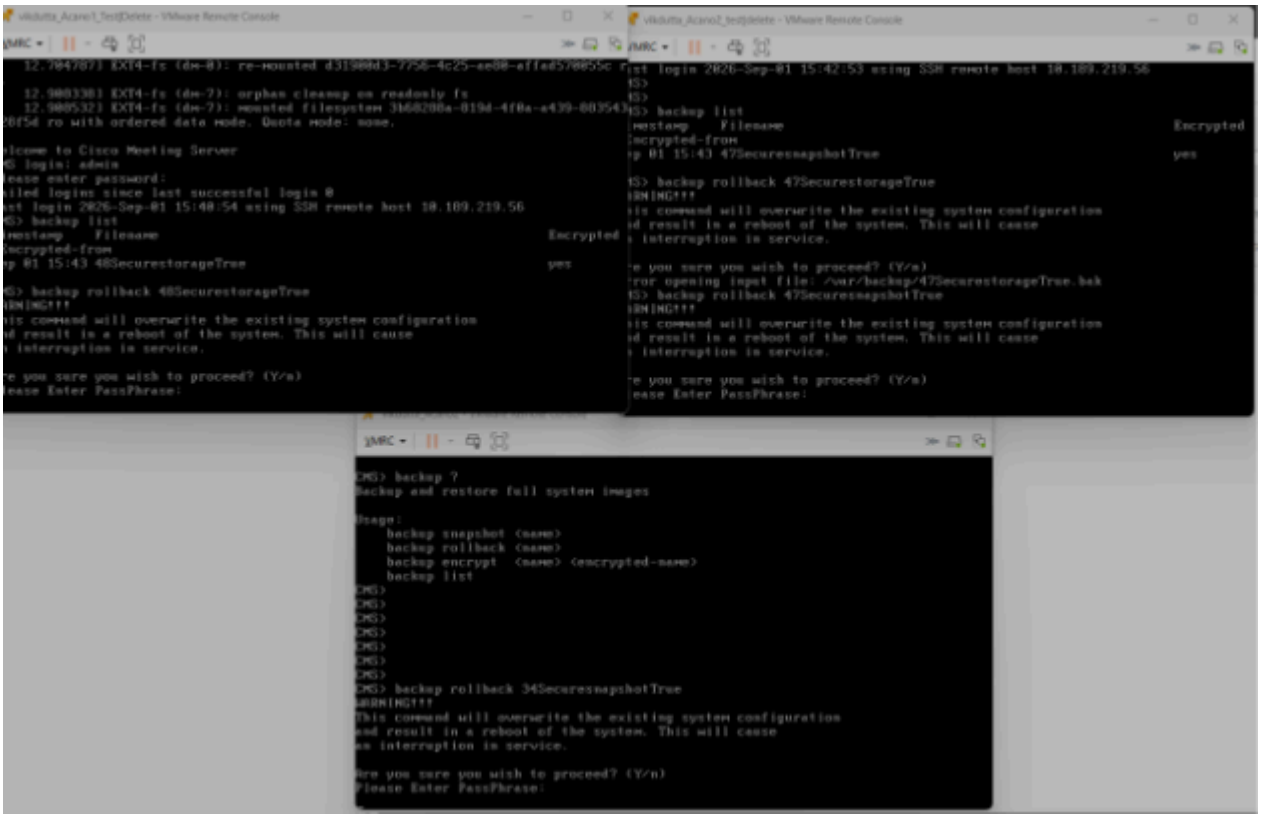


Figura 38: Confirme Y, insira a senha e restaure primeiro o primário anterior.

Note: Se as conexões de cluster de Call Bridge não surgirem após essa restauração, execute o **database cluster upgrade_schema** somente no primário anterior e verifique novamente o status da Call Bridge.

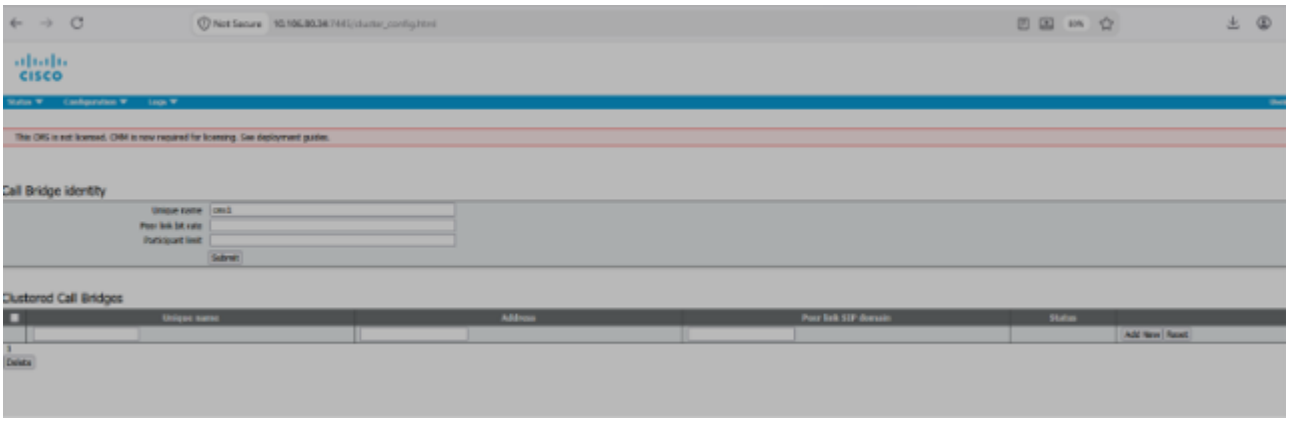


Figura 39: Antes da atualização do esquema, o exemplo mostra o cluster de banco de dados sendo executado enquanto as Call Bridges clusterizadas estão vazias.

database cluster upgrade_schema

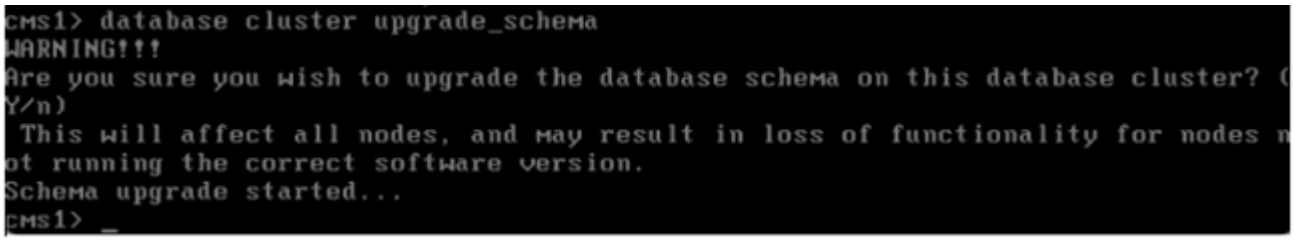


Figura 40: No primário anterior, confirme Y somente quando as conexões de cluster Call Bridge falharem após essa atualização de cluster desfeito.

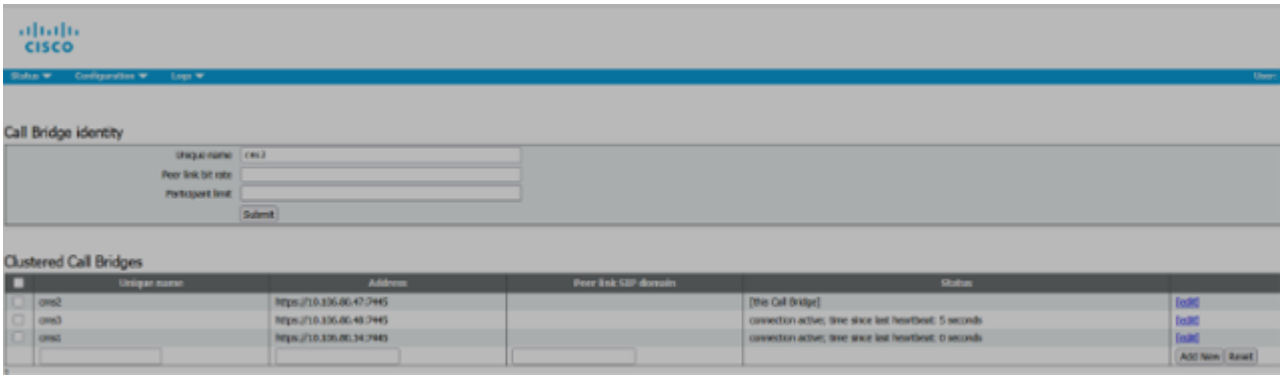


Figura 41: Após a atualização do esquema, verifique se cada peer de Call Bridge mostra uma conexão ativa.

Conclua o procedimento secreto do MeetingApps na seção Chave Secreta do MeetingApps Após a Restauração em cada Web Bridge e, em seguida, valide a implantação com o uso da seção Validação Pós-atualização.

Validação pós-atualização

Conclua esta lista de verificação após a restauração e antes de retornar o sistema à produção:

- O Web Admin em cada nó mostra o Cisco Meeting Server 4.0.
- Os serviços MMP necessários estão ativados e em execução (ativo: True).
- As condições de falha são claras. Trate erros e avisos recentes como informativos, a menos que exista uma falha correspondente.
- Se aplicável, o status do cluster do banco de dados mostrará as réplicas e o principal esperados.
- O Smart Licensing e a conectividade do Call Bridge são restaurados.
- Chamadas SIP e chamadas de cliente de Aplicativo Web com suporte nesta implantação foram concluídas com êxito.
- As marcas, os avisos de áudio e os arquivos SSO que são copiados do servidor na seção Requisitos de pré-upgrade são restaurados se ainda não tiverem sido incluídos no backup.
- Se o MeetingApps for implantado, o Web Bridge mostrará o novo relacionamento do MeetingApps e o compartilhamento de arquivos funcionará.
- Remova instantâneos de vida curta somente depois que a implantação tiver sido aceita.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.