Aggiornamento di Meeting Server alla release 4.0 - White paper

Sommario

- Introduzione
- Premesse
- Panoramica sullo storage sicuro
  - Piattaforme supportate
  - Note sull'implementazione
- Principi e vincoli di aggiornamento
  - Percorso di aggiornamento richiesto
  - Declassa
  - Requisiti di backup critici per gli aggiornamenti alla versione 4.0
  - Configurazione primo login e password
  - Ristabilisci connettività di rete dopo l'aggiornamento
  - Convalida integrità server prima della creazione di backup
- Requisiti pre-aggiornamento
- Procedure comuni di backup e ripristino
  - Dati interessati dopo l'aggiornamento alla versione 4.0
  - Esegui backup quando l'archiviazione sicura è disabilitata o non disponibile
  - Esegui backup quando è abilitata l'archiviazione sicura
  - Ripristino dei dati dopo l'aggiornamento alla versione 4.0
  - Chiave segreta MeetingApps dopo il ripristino
- Primo avvio e ripristino della rete
- Scenari di aggiornamento
  - Scenario 1 - Nodo singolo con archiviazione sicura disabilitata o non disponibile
  - Scenario 2 - Nodo singolo con archiviazione sicura abilitata
  - Scenario 3 - Cluster di database con archiviazione sicura disabilitato
    - Registrazione dei dettagli del cluster ed esecuzione del backup di ogni nodo
    - Disconnetti il cluster
    - Aggiornamento e ripristino dei nodi
  - Scenario 4 - Cluster di database con archiviazione sicura abilitata
    - Registrazione dei dettagli del cluster e creazione di backup crittografati
    - Disconnetti, aggiorna e ripristina
- Convalida post-aggiornamento

Introduzione

In questo documento viene descritto come aggiornare Cisco Meeting Server alla versione 4.0.

Premesse

Per informazioni sui requisiti e i prerequisiti, consultare questo documento insieme alle note di rilascio di Cisco Meeting Server, alla guida di riferimento dei comandi MMP e alla guida di riferimento per l'amministratore di Secure Storage.

Il processo di aggiornamento per Cisco Meeting Server 4.0 è diverso dalle versioni precedenti perché l'applicazione dell'immagine attiva un reset di fabbrica del nodo. Per garantire la continuità del servizio, tutte le configurazioni precedenti, incluse le impostazioni di rete e le password, devono essere conservate tramite un backup esportato in una posizione esterna prima di avviare l'aggiornamento.

Inoltre, Secure Storage era opzionale nelle versioni 3.11-3.13 di Cisco Meeting Server, ma è abilitato per impostazione predefinita nella versione 4.0. Di conseguenza, è necessario seguire diverse procedure di backup e ripristino se non si è mai utilizzato Secure Storage o se lo si è già abilitato nella versione 3.11x, 3.12x o 3.13x.

Archiviazione sicura esegue la crittografia della chiave privata e dei file di backup nel server e richiede la crittografia di tali file prima del trasferimento alla memoria esterna.

In questo documento le linee guida necessarie vengono consolidate in un unico riferimento, in modo che sia possibile seguire una procedura comune per tutti gli scenari di aggiornamento senza dover ripetere gli stessi passaggi.

Questo documento tratta i seguenti argomenti:

- Definizione di storage sicuro, applicazione e funzionalità non supportate.
- Il percorso di aggiornamento, che include il requisito di raggiungere 3.13.x prima della 4.0 e il fatto che non è supportato il downgrade da 4.0.
- Metodo di backup e ripristino comune per i nodi in cui è abilitata l'archiviazione sicura e per i nodi in cui è disabilitata o non disponibile.
- Il nodo del cluster di database interrompe la sequenza mentre il cluster di database viene interrotto prima di un aggiornamento.
- La chiave privata MeetingApps, che non è archiviata in un backup di Cisco Meeting Server e deve essere rigenerata dopo un ripristino.



Nota: Questo documento utilizza schermate di laboratorio acquisite durante i test originali della guida all'aggiornamento, incluse le versioni del software 4.0 beta. Tutti i nomi host, gli indirizzi IP e i nomi di file visualizzati sono strettamente illustrativi e non riflettono le

---

credenziali di produzione effettive o le passphrase riservate. Per mantenere la chiarezza ed evitare la ridondanza, i passi ripetuti vengono visualizzati una sola volta nella sezione procedura comune, a meno che la vista cluster non fornisca un contesto aggiuntivo necessario.

Panoramica sullo storage sicuro

L'archiviazione sicura offre una protezione avanzata dei dati tramite la crittografia dei file sensibili che risiedono nel server di riunione e il controllo della modalità di scaricamento di tali file dal server di bridge di chiamate. Questa funzionalità è stata introdotta in Cisco Meeting Server 3.11 come opzione configurabile con l'utilizzo del comando MMP secure_storage enable nelle distribuzioni di macchine virtuali (basate su specifiche o Meeting Server Small) e in Meeting Server Medium.

Dalla versione 4.0, Secure Storage è abilitato per impostazione predefinita. Questa impostazione è ora permanente ed è irreversibile ed il comando secure_storage enable MMP è stato rimosso.

Con l'archiviazione sicura, il server riunioni applica questo comportamento:

- Le chiavi private non possono essere scaricate tramite SFTP finché non vengono crittografate. Crittografare una chiave privata con il comando pki encrypt MMP seguito da una passphrase di almeno 14 caratteri. Le chiavi attualmente utilizzate dai servizi di Meeting Server rimangono invariate.
- I file di backup creati con il comando backup encrypt <name>encrypted-name vengono crittografati. Quando Secure Storage è abilitato, il comando backup encrypt <name> encrypted-name MMP richiede una passphrase di almeno 14 caratteri. La stessa passphrase è richiesta durante il ripristino del backup.
- Prima di poter scaricare un file di backup, è necessario che il file sia crittografato. Se un backup elencato non è ancora crittografato per l'esportazione, utilizzare backup encrypt <nome> nome-crittografato. I tentativi di download di un backup non crittografato vengono negati.
- Dalla versione 3.12, Secure Storage può funzionare quando FIPS è abilitato. I file delle chiavi private creati nella versione 3.11 con una passphrase più breve devono essere rigenerati con una passphrase di almeno 14 caratteri.



Suggerimento: L'archiviazione sicura limita il trasferimento di chiavi private non crittografate e file di backup non crittografati dal server riunioni. Non limita il trasferimento dei file di certificato. I certificati possono ancora essere copiati con SFTP; solo le chiavi private non crittografate associate vengono bloccate finché non vengono crittografate con

pki encrypt.

⚠ Attenzione: Una volta abilitato, Secure Storage non può essere disabilitato con alcun comando MMP. L'operazione è irreversibile. Solo factory_reset full reimposta Secure Storage su false. Eseguire un backup della configurazione con snapshot di backup e archiviarlo in un dispositivo separato prima di abilitare Archiviazione sicura. Dopo aver abilitato secure_storage, riavviare immediatamente. Se il riavvio viene ignorato, è possibile contrassegnare Archiviazione sicura come abilitata senza che sia stata eseguita la completa inizializzazione e i comandi come factory_reset full possono avere esito negativo. Il percorso di ripristino in questo stato deve essere ripristinato a uno snapshot salvato in precedenza (valido solo per la versione 3.13.x). In Meeting Server 4.0, secure_storage è abilitato per impostazione predefinita.

Piattaforme supportate

- Macchina virtuale (basata su specifiche): Supportato
- Meeting Server Small/1K: Supportato
- Mezzo Meeting Server: Supportato
- Meeting Server 2000: Non supportata. La funzionalità Archiviazione sicura non è disponibile. Non utilizzare i comandi di archiviazione sicura su questa piattaforma.

Cisco Meeting Server 4.0 consente l'archiviazione sicura per impostazione predefinita su tutte le piattaforme compatibili. Dopo l'aggiornamento, i dati vengono automaticamente protetti da Secure Storage anche se il backup della versione 3.13.x è stato eseguito mentre Secure Storage è stato disabilitato.

Note sull'implementazione

- La ridenominazione dell'immagine di aggiornamento non modifica le impostazioni di Archiviazione sicura.
- Confermare lo stato di archiviazione sicura su ogni nodo utilizzando il comando secure_storage prima di eseguire i backup.
- Il comando segnala se l'archiviazione sicura è abilitata (True) o meno (False). Il comando non è applicabile a Meeting Server 2000; durante l'aggiornamento di Cisco Meeting Server 2000, eseguire la procedura descritta in condizioni di aggiornamento in cui l'archiviazione sicura è disabilitata o non disponibile.



Output MMP quando l'archiviazione sicura non è abilitata (abilitato: falso).



Figura 2: Output MMP quando l'archiviazione sicura è abilitata (abilitato: true) in Cisco Meeting Server 3.13.

Per informazioni dettagliate sulla sintassi dei comandi e sull'utilizzo dei comandi, vedere la Guida di riferimento rapido per l'amministratore di Cisco Meeting Server per l'archiviazione sicura e la Guida di riferimento ai comandi MMP attualmente in uso.

Principi e vincoli di aggiornamento

Percorso di aggiornamento richiesto

Gli aggiornamenti di Cisco Meeting Server devono seguire un percorso sequenziale senza ignorare le versioni principali. Ad esempio, un nodo della versione 3.11.x deve passare alla versione 3.12.x e alla 3.13.x prima di raggiungere la versione 4.0. Gli aggiornamenti diretti dalle versioni precedenti, ad esempio dalla 3.9.x alla 3.13.x o dalla 3.11.x alla 4.0, non sono supportati e in genere causano errori di configurazione irreversibili. Per Meeting Server Medium con versioni 3.11.5 o 3.13, il percorso di aggiornamento sarebbe 3.11.5 → 3.13 → 4.0.

Suggerimento: Prima di avviare l'aggiornamento alla versione 4.0, su ogni nodo deve essere in esecuzione Cisco Meeting Server 3.13.x, con un backup della configurazione verificato esportato dal sistema 3.13.x. Tutte le procedure relative agli scenari descritte in questo documento presuppongono il completamento dell'aggiornamento alla versione 3.13.x.

Declassa



Suggerimento: Il downgrade da 4.0.x a 3.13.x non è supportato. Se l'aggiornamento non riesce o il sistema non funziona come previsto, installare un nuovo OAV 3.13.x (o ricreare l'immagine dell'accessorio) e ripristinare il backup 3.13.x. Conservare le istantanee dell'hypervisor delle macchine virtuali 3.13.x per la durata della finestra di aggiornamento come opzione di ripristino aggiuntiva. Le istantanee delle VM non sostituiscono i backup di configurazione esportati.

Requisiti di backup critici per gli aggiornamenti alla versione 4.0

Dopo la conferma dell'aggiornamento alla versione 4.0, il nodo viene riavviato in uno stato di primo avvio. Non dipendere dal backup automatico generato durante il processo di aggiornamento, in quanto un errore di aggiornamento può causare la perdita dell'accesso SFTP e rendere il file inaccessibile. Solo i backup creati con il comando backup snapshot e copiati sullo storage esterno possono essere utilizzati in modo affidabile per il ripristino.

Configurazione primo login e password

Al primo avvio della versione 4.0, la password MMP esistente viene rimossa dal database. Accedere con il nome utente admin senza specificare la password. Il sistema richiede di impostare una nuova password MMP. Il sistema richiede di immettere la password due volte per la verifica e la conferma. Poiché non è disponibile una funzionalità di recupero della password per Meeting Server, assicurarsi di registrare la nuova password.

Nota: Se si imposta una nuova password MMP al primo avvio, il comando backup rollback la sostituisce con la password memorizzata nel backup 3.13.x. Dopo aver ripristinato il backup sul server, è necessario accedere con la password attiva al momento della creazione del backup.

Ristabilisci connettività di rete dopo l'aggiornamento

Gli indirizzi IPv4 e IPv6, le maschere e i gateway vengono persi insieme al resto della configurazione. Dopo l'aggiornamento alla versione 4.0, la connettività di rete di Meeting Server può essere interrotta. È necessario disporre dell'accesso alla console dell'hypervisor, a CIMC o seriale in modo da poter assegnare di nuovo gli indirizzi dal pannello di gestione.



Nota: Le distribuzioni che utilizzano le prenotazioni DHCP in genere mantengono gli stessi indirizzi IP dopo il riavvio. Tuttavia, l'accesso alla console deve rimanere disponibile fino alla verifica dell'indirizzo. Non presupporre che la connettività SSH sia ripristinata finché

l'indirizzo IP non viene confermato.

Convalida integrità server prima della creazione di backup

Dopo ogni aggiornamento alla versione 3.13, verificare che il server sia in buone condizioni e che tutti i servizi funzionino. Non ignorare le condizioni di errore nella pagina di panoramica del server. In caso di errori, risolverli prima di creare uno snapshot di backup nella versione 3.13. In questo modo viene ripristinato un backup del server integro nei nodi 4.0 aggiornati, evitando eventuali errori di distribuzione.

In Amministrazione Web aprire Stato e verificare che la sezione Condizioni di errore sia deselezionata. Ignora le voci visualizzate solo in Errori e avvisi recenti. Dopo un aggiornamento, in genere vengono visualizzati database temporanei o messaggi di Web Bridge. questi non sono un motivo per ripristinare o ritardare il backup.

Se una condizione di errore rimane per più di dieci minuti, risolverla prima di eseguire il backup. Il ripristino su 4.0 di un backup 3.13.x che contiene già errori porta avanti tali errori.

Per i sistemi cluster, verificare che tutti i tipi di chiamata in uso siano funzionanti (endpoint SIP e client Web App) e che non siano elencate condizioni di errore in alcun nodo.

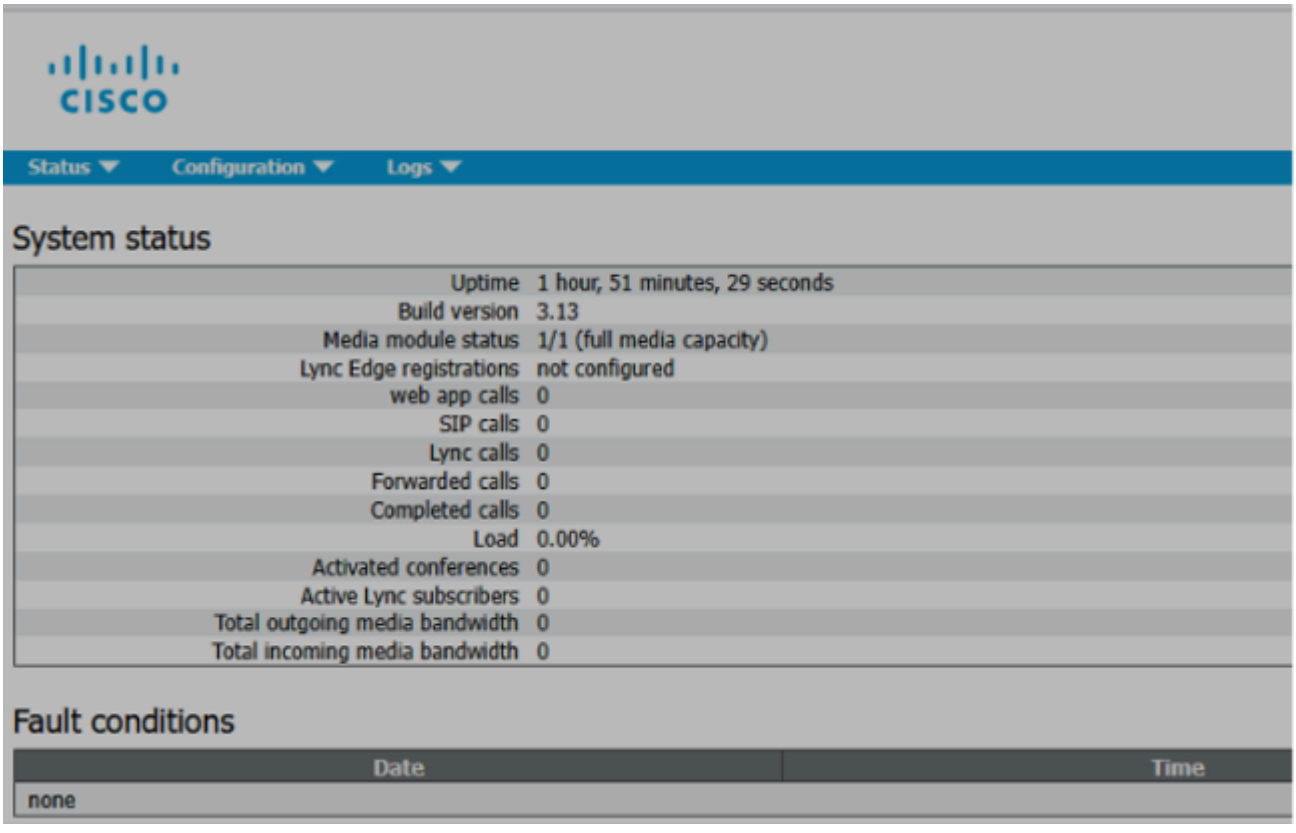


Figura 3: Pagina Web Admin Status sulla versione 3.13.x con le condizioni di errore vuote. Utilizzare questa visualizzazione prima

di eseguire il backup ripristinato nella versione 4.0.

Requisiti pre-aggiornamento

Prima di avviare l'aggiornamento alla versione 4.0, effettuare le seguenti operazioni. Questi requisiti si applicano a tutti e quattro gli scenari illustrati più avanti in questo documento.

- Aggiornare alla versione 3.13.x, quindi esportare un backup della configurazione. Verificare che sul nodo sia in esecuzione Cisco Meeting Server 3.13.x. Create un backup e trasferitelo, insieme a tutti i dati SFTP personalizzati, quali loghi, file di branding, prompt audio, file SSO e altri dati personalizzati, su un supporto di memorizzazione esterno. Utilizzare le procedure descritte nella sezione Procedure comuni di backup e ripristino. In un ambiente cluster, eseguire un backup da ogni nodo, non solo da Connected Primary ma da Connected Replica.
- Registrare le impostazioni di rete. Eseguire il comando ipv4 a e memorizzare l'output. È necessario immettere nuovamente queste informazioni dalla console dopo il riavvio della versione 4.0 a meno che una prenotazione DHCP non ripristini automaticamente l'indirizzo IP.
- Confermare l'accesso alla console L'accesso alla console dell'hypervisor, a CIMC o seriale deve essere disponibile prima di iniziare. Si prevede che SSH venga interrotto quando il nodo viene riavviato alla versione 4.0.
- Scarica il bundle di log corrente per l'archiviazione. Salvare logbundle.tar.gz da ogni nodo. Il bundle non sostituisce le snapshot di backup.
- Leggere il banner di avviso dell'aggiornamento 4.0 quando viene visualizzato dopo l'esecuzione del comando upgrade.
- Premere n per interrompere se uno dei prerequisiti è incompleto. Premere Y solo quando si è pronti per procedere.

Procedure comuni di backup e ripristino

I quattro scenari di aggiornamento descritti più avanti in questo documento utilizzano lo stesso schema di backup, esportazione, primo avvio e ripristino. Utilizzare questa sezione come origine singola di questi passaggi, quindi seguire solo la sequenza specifica dello scenario (nodo singolo rispetto al cluster e se l'archiviazione sicura è già abilitata).

Dati interessati dopo l'aggiornamento alla versione 4.0

Questi dati vengono persi dopo l'aggiornamento alla versione 4.0 finché non si ripristina un backup:

- Contenuto del database, che include spazi, utenti e profili di chiamata.
- Certificati e chiavi private.
- Personalizzazione locale, file SSO e file di prompt audio.
- Configurazione della rete (indirizzo IP, maschera e gateway), a eccezione del caso in cui una prenotazione DHCP ripristini l'indirizzo.
- La password MMP precedente, fino a quando il rollback del backup non riapplica la password del backup.
- Il bridge di chiamate, l'amministratore Web, il bridge Web e altri servizi applicativi vengono restituiti solo dopo il ripristino.



Suggerimento: Il backup di Cisco Meeting Server non include la chiave privata MeetingApps. Dopo un ripristino, è necessario rigenerare tale chiave e applicarla a ogni nodo di Web Bridge. Vedere la sezione Chiave segreta MeetingApps dopo il ripristino.

Esegui backup quando l'archiviazione sicura è disabilitata o non disponibile

Attenersi alla seguente procedura sulle macchine virtuali, su Meeting Server Small e su Meeting Server Medium dove secure_storage segnala Enabled: False e in Meeting Server 2000 in cui l'archiviazione sicura non è disponibile.

1. Su ciascun nodo, creare un file con il comando backup snapshot. Non riutilizzare il nome file precedente.

2. Copiare immediatamente il file di backup sullo storage esterno con SFTP. Non conservare l'unica copia sul Meeting Server.

3. Memorizzare il file in una posizione che sia ancora raggiungibile se il nodo viene ricostruito.

Esempio:

```
backup snapshot cms313SecurestorageFalse backup list
```

4. Confermare che il file venga visualizzato nel comando backup list, quindi trasferirlo su un disco esterno con un client SFTP.

5. Ripetere questo processo su ogni nodo del cluster. I nomi di backup possono contenere solo lettere, numeri, caratteri di sottolineatura e trattini. Quando si crea un file di backup, non includere l'estensione bak. Ad esempio, un nome di file come 3.13SecurestorageFalse viene rifiutato a causa del punto.

```
    backup list
cms-3120> backup snapshot 3.13SecurestorageFalse
Invalid backup name. Alphanumeric, underscore and hyphen characters allowed
cms-3120> backup snapshot 313SecurestorageFalse
313SecurestorageFalse.bak ready for download
cms-3120>
```

Figura 4: Lo snapshot di backup rifiuta un nome che contiene un punto, quindi riesce con un nome alfanumerico. Il file bak è pronto per il download.



Figura 5: Copiare il file bak dalla radice SFTP di Meeting Server nello storage esterno. Non lasciare l'unica copia sul server.

Esegui backup quando è abilitata l'archiviazione sicura

Utilizzare questa procedura quando secure_storage segnala Enabled: Vero. Impossibile scaricare i file di backup non crittografati.

1. Creare uno snapshot di backup in ogni nodo. Quando l'opzione Archiviazione sicura è abilitata, il server richiede una passphrase di almeno 14 caratteri. La passphrase può includere lettere, numeri, caratteri speciali, simboli o spazi.

```
cms-3120>
cms-3120> backup snapshot 313SecurestorageTrue
Please Enter PassPhrase:
313SecurestorageTrue.bak ready for download
cms-3120>
cms-3120>
```

Figura 6: La copia istantanea di backup con archiviazione sicura abilitata richiede una volta una passphrase di almeno 14 caratteri. L'MMP non ti chiede di confermarlo.

2. L'MMP non chiede di inserire nuovamente la passphrase per conferma. Proteggere la passphrase perché è necessaria la stessa passphrase per ripristinare il file. Non scegliere una passphrase semplice o di esempio.

3. Se il comando backup list mostra uno snapshot non crittografato per l'esportazione, crittografarlo prima di scaricarlo:

```
cms-3120> backup list
Timestamp    Filename                                    Encrypted  Encrypted-from
Sep 01 11:12 3_12                                        no
Sep 01 12:06 313SecurestorageTrue                        no
cms-3120>
```

Figura 7: Elenco di backup prima della crittografia. La colonna Encrypted è impostata su no, pertanto non è possibile scaricare il file.

4. Se si tenta di scaricare un backup non crittografato, SFTP restituisce un errore di autorizzazione negata e indica di eseguire prima il comando backup encrypt.

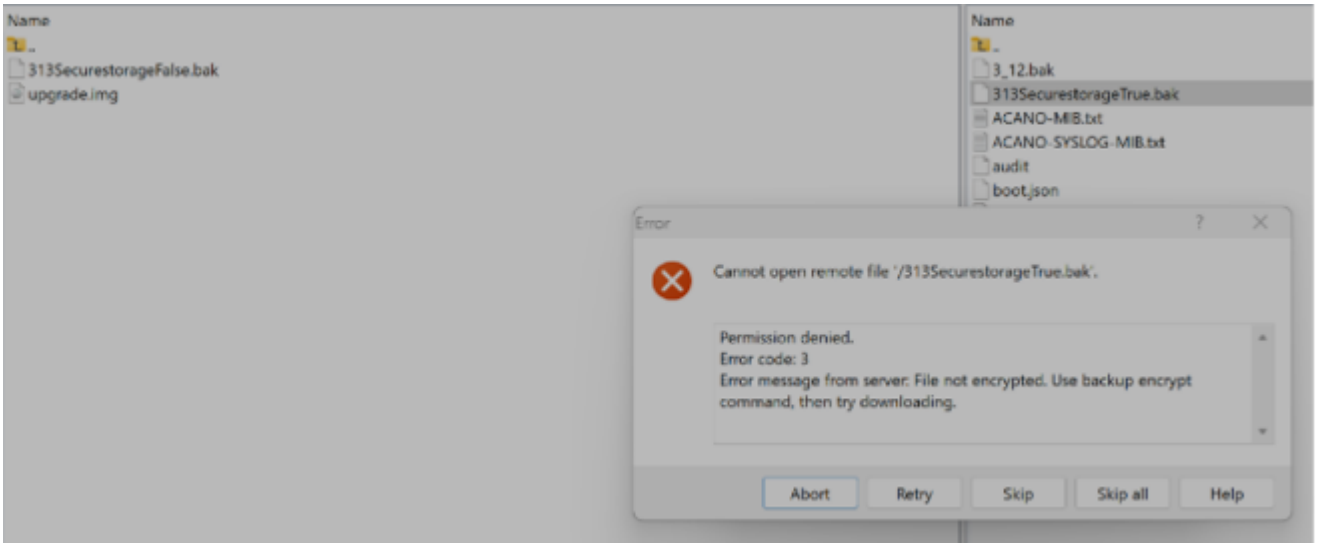


Figura 8: SFTP impedisce il download di un backup non crittografato quando è abilitata l'archiviazione sicura. Il messaggio del server indica di eseguire la crittografia di backup.

5. Eseguire il comando backup encrypt per crittografare il file di 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: Elenco di backup dopo la crittografia della snapshot. Il file crittografato è sì e può essere trasferito con SFTP.

Nell'elenco di backup vengono visualizzati lo stato della crittografia e il nome del file originale. Accertarsi di trasferire solo il file crittografato da ogni nodo del cluster. Gestisce un record organizzato di ogni nodo, il nome file corrispondente e la passphrase associata.

Se è inoltre necessario esportare le chiavi private, crittografare prima ogni chiave. I file dei certificati non vengono bloccati da Archiviazione sicura e possono essere copiati senza questo passaggio aggiuntivo:

pki encrypt private.key encrypted_private.key

Utilizzare un nome di file univoco anziché sovrascrivere la chiave attualmente utilizzata dai servizi. Anche in questo caso si applica il requisito della passphrase di almeno 14 caratteri.

Ripristino dei dati dopo l'aggiornamento alla versione 4.0

1. Dopo il login di primo avvio e il ripristino della rete nella sezione Primo avvio e ripristino della rete, copiare il backup 3.13.x corrispondente nel nodo con SFTP e ripristinarlo.

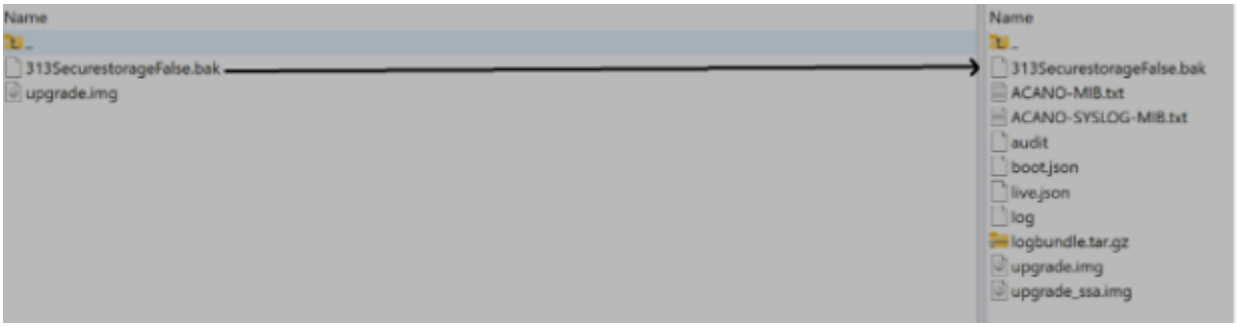


Figura 10: Dopo il primo avvio del ripristino della rete, copiare nuovamente il file .bak 3.13.x sul nodo 4.0 con SFTP.

2. Confermare se il file è presente:

elenco di backup

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

cms-3120>
```

Figura 11: Elenco di backup della versione 4.0 che conferma la presenza dello snapshot caricato prima del rollback.

3. Ripristinare lo snapshot. In una distribuzione cluster, ripristinare prima il database primario precedente, quindi le repliche e quindi i nodi connessi.

backup rollback name-of-the-backup-file



Figura 12: Rollback del backup di uno snapshot non crittografato. Confermare con Y; il nodo estrae il backup e si riavvia.

4. Premere Y per continuare. Il nodo viene riavviato durante l'estrazione del backup. Se il backup è stato eseguito con l'opzione Archiviazione sicura abilitata, il pannello di gestione richiede la passphrase. Il riavvio procede solo dopo l'accettazione della passphrase corretta.

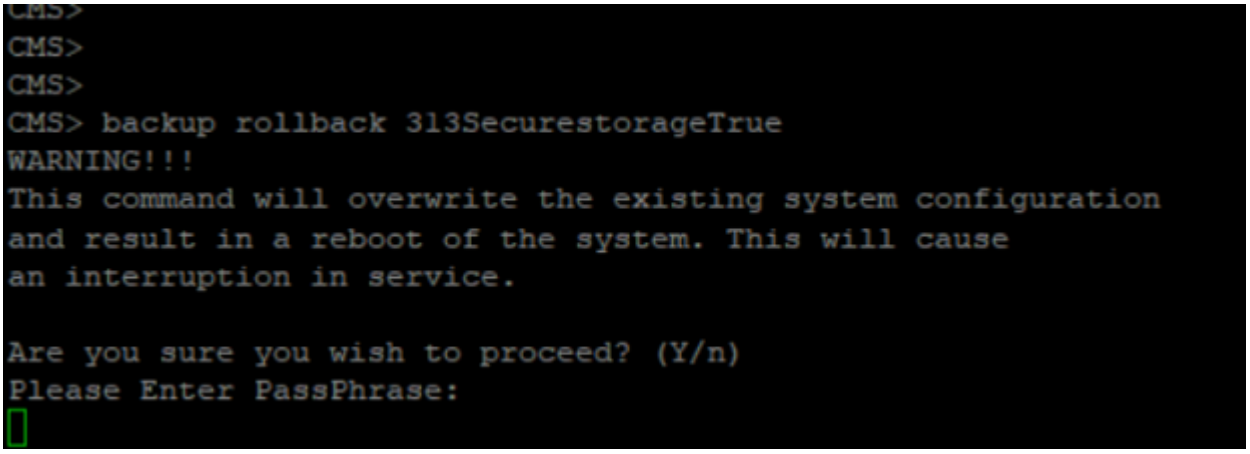


Figura 13: Rollback del backup di uno snapshot crittografato. Dopo Y, il pannello di gestione richiede la passphrase utilizzata al momento della creazione del backup.

⚠ Attenzione: sovrascrive **backup rollback** la configurazione corrente, i certificati, le chiavi private e il file di licenza, quindi riavvia il server. Utilizzarlo solo con il backup 3.13.x esportato per questo aggiornamento.

---

5. Quando il nodo è di nuovo in linea, accedere con le credenziali MMP del backup e confermare che ciascun servizio richiesto sia abilitato e in esecuzione (il piano MMP indica che è attivo: Vero).

Controlli tipici:

callbridge webbridge3 webadmin scheduler recorder streamer uploader meetingapps

6. Eseguire solo i comandi per i servizi che questo nodo deve ospitare.

Chiave segreta MeetingApps dopo il ripristino

Il backup di Cisco Meeting Server non memorizza la chiave segreta di MeetingApps. Al termine del rollback del backup, rigenerare il segreto e applicarlo a ogni nodo di Web Bridge. Se si ignora questo passaggio, la condivisione dei file non sarà disponibile anche se gli altri servizi risultano integri.

1. Sul nodo MeetingApps, eseguire il comando meetingapps gensecret.

2. Copiare il segreto generato nell'archivio segreto. Ogni esecuzione di meetingapps gensecret invalida la chiave precedente, quindi generare la chiave una volta e riutilizzare lo stesso valore in tutti i Web Bridge.

3. Eseguire i seguenti comandi su ogni nodo di Web Bridge:

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

L'ultimo comando conferma che il servizio Web Bridge è in esecuzione e che MeetingApps è configurato correttamente. MeetingApps non è supportato in Meeting Server 2000 e la condivisione di file non è disponibile nei cluster che includono Meeting Server 2000. In tali distribuzioni, questo passaggio non è applicabile.

Primo avvio e ripristino della rete

Il comando upgrade 4.0 visualizza un banner di avviso prima di procedere. Esaminare attentamente il messaggio e interrompere con n se alcuni prerequisiti sono incompleti. Se si continua con Y, il nodo viene riavviato, la sessione SSH viene disconnessa e i passaggi rimanenti devono essere completati dalla console.

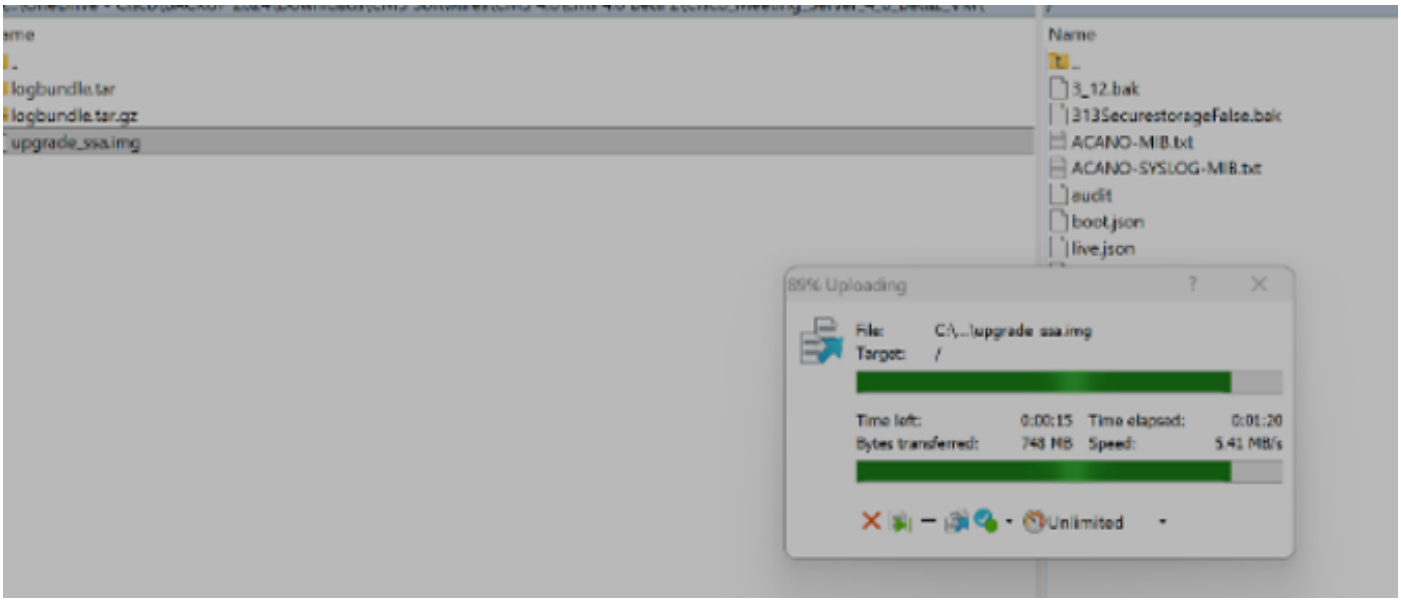


Figura 14: Caricare l'immagine di aggiornamento 4.0 nella directory principale SFTP di Meeting Server. Il nome del file dell'immagine di aggiornamento può variare a seconda del pacchetto scaricato da cisco.com.

```
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: Il comando upgrade verifica la firma dell'immagine e avvia il processo. Non affidarsi al backup automatico creato in questa fase.

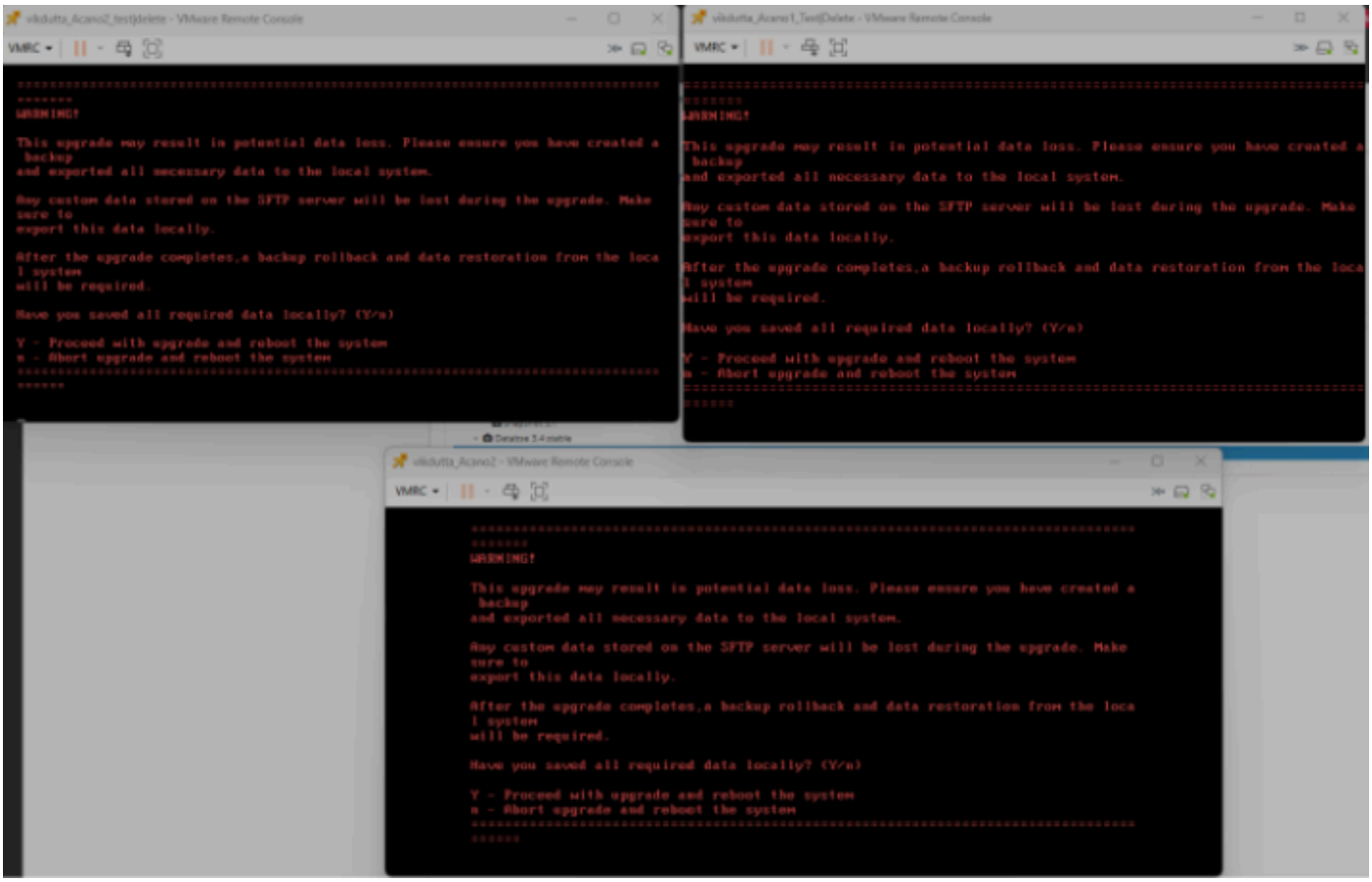


Figura 16: Avviso MMP rosso in un cluster a tre nodi. Lo stesso banner viene visualizzato su un singolo nodo. Premere n per interrompere l'operazione se i backup e i dati personalizzati non sono disattivati dal server. Premere solo Y per continuare e riavviare.

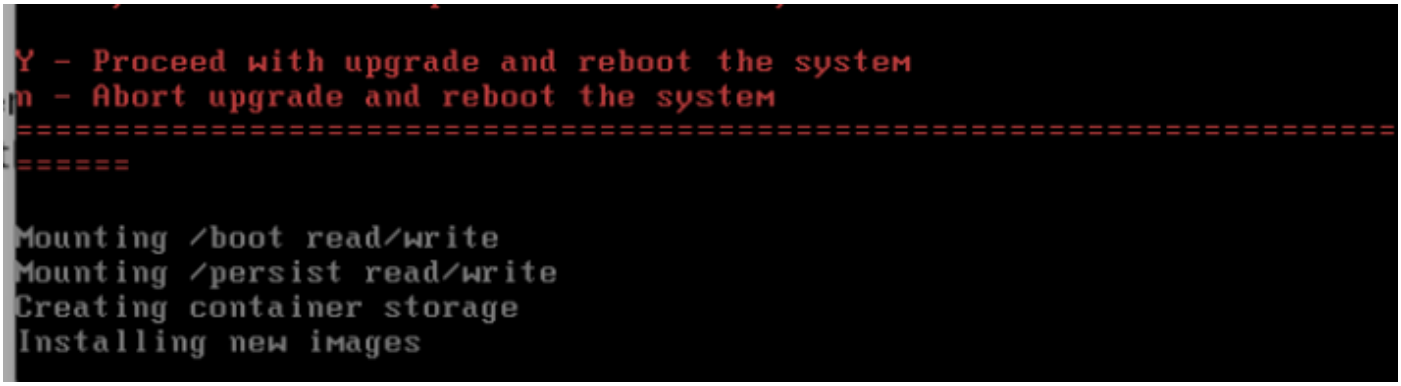


Figura 17: Dopo Y, il nodo monta lo storage e installa l'immagine 4.0. La sessione SSH scade; continuare dalla console hypervisor.

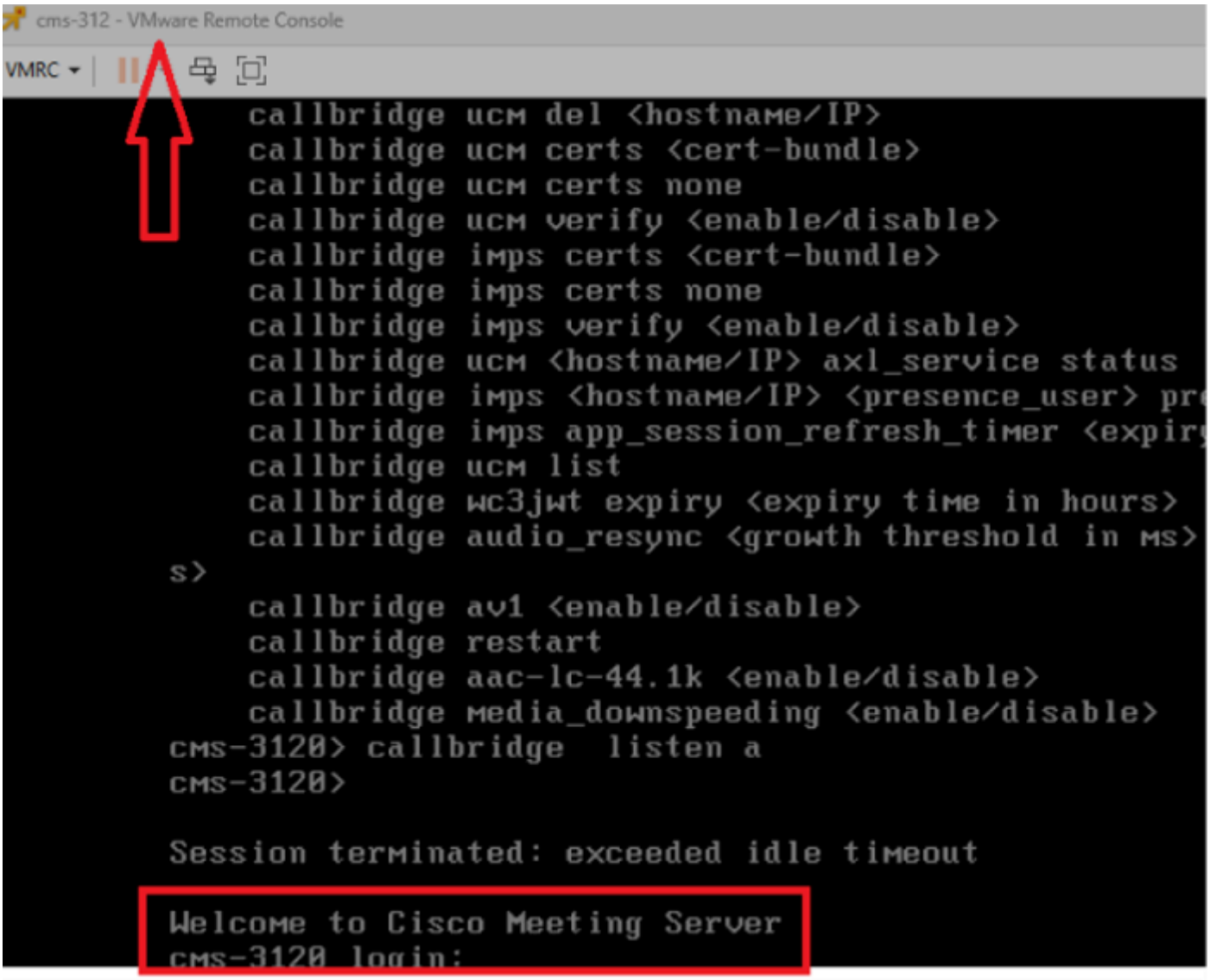


Figura 18: Utilizzare la console VM o CIMC dopo il rilascio di SSH. Quando l'immagine 4.0 è pronta, viene visualizzato il prompt di accesso al primo avvio.

1. Accedere con l'account MMP di primo avvio (nome utente admin e nessuna password), quindi impostare una nuova password MMP quando richiesto. Il rollback del backup sostituisce questa password con la password memorizzata nel backup.

2. Riapplicare la configurazione di rete dalle note acquisite nella sezione Requisiti pre-aggiornamento:

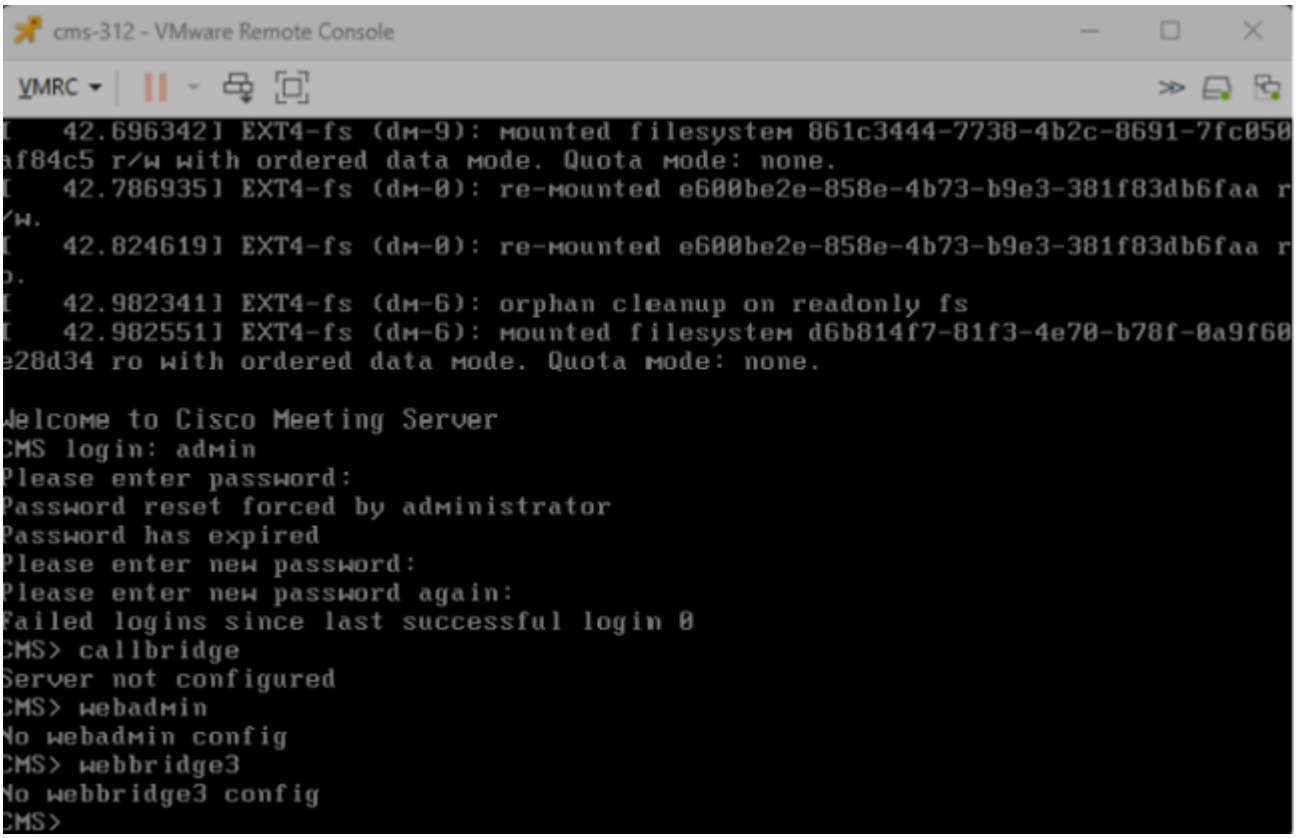


Figura 19: Accesso MMP al primo avvio.

La password precedente non è più valida. Dopo aver impostato una nuova password, i servizi quali webadmin e webbridge3 non vengono configurati fino al ripristino del backup.

3. Eseguire il comando:

ipv4 interface add address/prefix-length gateway

Ad esempio:

ipv4 a add 192.0.2.10/24 192.0.2.1

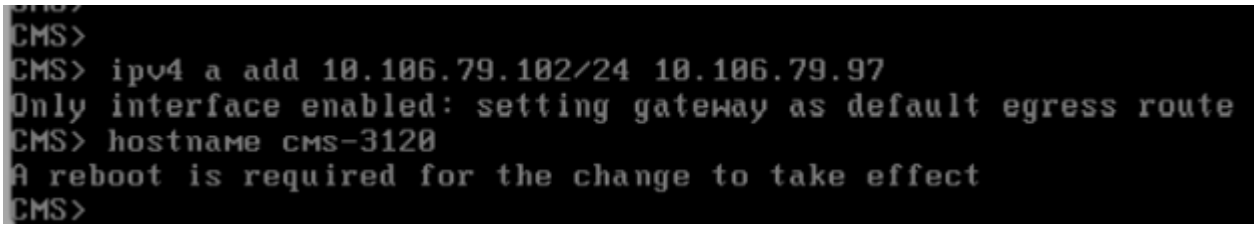


Figura 20: Riapplicare il protocollo IPv4 dalla console.

Dopo aver assegnato l'indirizzo, è necessario riavviare il sistema. Gli indirizzi mostrati nello screenshot sono solo a scopo esemplificativo.

4. Riavviare dopo aver assegnato l'indirizzo. Una volta che il sistema è tornato online, continuare con il caricamento SFTP del backup e le operazioni di ripristino indicate nella sezione Ripristina dati dopo l'aggiornamento alla versione 4.0.

Nota: Se è stata configurata una prenotazione DHCP, l'indirizzo originale può essere già assegnato dopo il riavvio. Verificare l'indirizzo con **ipv4 a** prima di avviare una sessione SFTP dalla workstation di gestione.

Su Cisco Meeting Server 4.0, l'archiviazione sicura è abilitata per impostazione predefinita sulle piattaforme che la supportano. Il pannello di gestione non può più esporre secure_storage come interruttore dopo l'aggiornamento.



Figura 21: In questa immagine 4.0, il comando secure_storage non è riconosciuto perché l'opzione Secure Storage è abilitata per impostazione predefinita.

Confermare il rilascio con il comando version.

Scenari di aggiornamento

In questo capitolo vengono illustrati vari scenari di aggiornamento. Completare l'aggiornamento alla versione 3.13.x. Identificare il tipo di distribuzione e scegliere lo scenario di conseguenza. Seguire solo la procedura corrispondente all'ambiente e non combinare i passaggi delle distribuzioni cluster e a nodo singolo.

Completare innanzitutto l'aggiornamento a 3.13.x. Selezionare quindi uno scenario tra quelli riportati di seguito. Non combinare le procedure a nodo singolo e cluster di database.

- Scenario 1: Nodo singolo, disabilitato o non disponibile, VM, Small, Medium e Meeting Server 2000
- Scenario 2: Nodo singolo, abilitato, solo VM, piccolo e medio
- Scenario 3: Cluster di database, disabilitato o non disponibile, VM, Small, Medium e Meeting Server 2000
- Scenario 4: Cluster di database, abilitato, solo VM, piccolo e medio

Meeting Server 2000 non supporta gli scenari con l'archiviazione sicura abilitata. Per tale piattaforma, utilizzare lo scenario 1 o 3, a seconda dei casi.

Scenario 1 - Nodo singolo con archiviazione sicura disabilitata o non disponibile

Utilizzare questa procedura per un server autonomo con l'opzione Archiviazione sicura disattivata o per Meeting Server 2000 in cui l'opzione Archiviazione sicura non è disponibile. La release di origine può essere 3.11.x o successiva, ma il nodo deve trovarsi sulla versione 3.13.x prima di eseguire l'aggiornamento alla versione 4.0.

1. Aggiornamento graduale alla versione 3.13.x. Seguire il percorso supportato (ad esempio 3.11.x → 3.12.x → 3.13.x). Dopo ogni hop, verificare la versione in Web Admin e che le condizioni di errore siano state cancellate, come descritto nella sezione Convalida dello stato del server prima della creazione dei backup.

2. Confermare lo stato di archiviazione sicura. Eseguire il comando secure_storage e verificare che l'archiviazione sicura non sia abilitata. Ignorare il comando in Meeting Server 2000.

3. Creare ed esportare un file di backup 3.13.x come indicato nella sezione Eseguire un backup quando l'archiviazione sicura è disabilitata o non disponibile. Esportare inoltre il contenuto SFTP personalizzato e il bundle di log come indicato nella sezione Requisiti pre-aggiornamento.

4. Scaricare l'immagine software 4.0 da Cisco.com, estrarla e copiare upgrade.img sul nodo tramite SFTP.

5. Avviare l'aggiornamento con questo comando:

```
upgrade upgrade.img
```

6. Leggere il banner di avvertenza. Premere Y solo dopo il completamento di tutti i prerequisiti. 6. Dopo l'aggiornamento, configurare il nodo come descritto nella sezione Primo avvio e ripristino della rete, quindi ripristinare il backup utilizzando la sezione Ripristina dati dopo l'aggiornamento alla versione 4.0.

Scenario 2 - Nodo singolo con archiviazione sicura abilitata

Utilizzare questa procedura per una macchina virtuale standalone, Meeting Server Small o Meeting Server Medium in cui è attivato lo storage protetto. Non è applicabile a Meeting Server

2000.

Prima di trasferire i file dal server, si noti che non è possibile trasferire chiavi private non crittografate e file di backup non crittografati. I file dei certificati non sono bloccati.

1. Eseguire l'aggiornamento alla versione 3.13.x del percorso supportato senza ignorare le versioni. Dopo ogni hop, verificare la versione e che le condizioni di errore siano chiare nella sezione Convalida integrità server prima della creazione di backup.

2. Eseguire secure_storage e verificare che nell'output sia visualizzato Abilitato: Vero.

3. Creare ed esportare un backup 3.13.x crittografato utilizzando la sezione Esegui backup quando è abilitata l'archiviazione sicura. Memorizza la passphrase nel tuo archivio segreto. Esportare anche il contenuto SFTP personalizzato e il pacchetto di log (sezione Requisiti pre-aggiornamento).

4. Copiare upgrade.img sul nodo ed eseguire l'aggiornamento:

```
upgrade upgrade.img
```

5. Leggere il banner di avvertenza e premere Y per continuare solo quando i prerequisiti sono stati completati.

6. Ripristinare la rete dalla console (sezione Primo avvio e ripristino della rete), quindi ripristinare il backup crittografato con la relativa passphrase (sezione Ripristino dei dati dopo l'aggiornamento alla versione 4.0). 6. Se MeetingApps è in uso, applicare un nuovo segreto MeetingApps (sezione Chiave segreta MeetingApps dopo il ripristino).

L'archiviazione sicura è attivata per impostazione predefinita in Meeting Server 4.0. Dopo un ripristino, continuare a gestire le chiavi private e i file di backup come dati crittografati.

Scenario 3 - Cluster di database con archiviazione sicura disabilitato

Utilizzare questa procedura per un cluster di database con Archiviazione sicura disabilitata, che include un cluster contenente Meeting Server 2000. A partire dalla versione 3.5, il cluster di database deve essere disattivato prima dell'aggiornamento del software. Innanzitutto, aggiornare ogni nodo alla versione 3.13.x.

Registrazione dei dettagli del cluster ed esecuzione del backup di ogni nodo

1. Eseguire secure_storage su ogni nodo. Considerare il comando come non disponibile nei nodi di Meeting Server 2000.

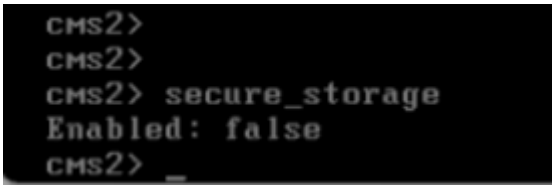


Figura 22: Prima di utilizzare backup non crittografati, verificare che l'archiviazione sicura sia disabilitata in ogni nodo del cluster. Ignorare il comando per i nodi di Meeting Server 2000, dove non è disponibile.

2. Registrare il nodo primario del database corrente in quanto deve essere ripristinato prima dopo l'aggiornamento alla versione 4.0. Confermare che le repliche siano sincronizzate e che lo stato del cluster sia integro.

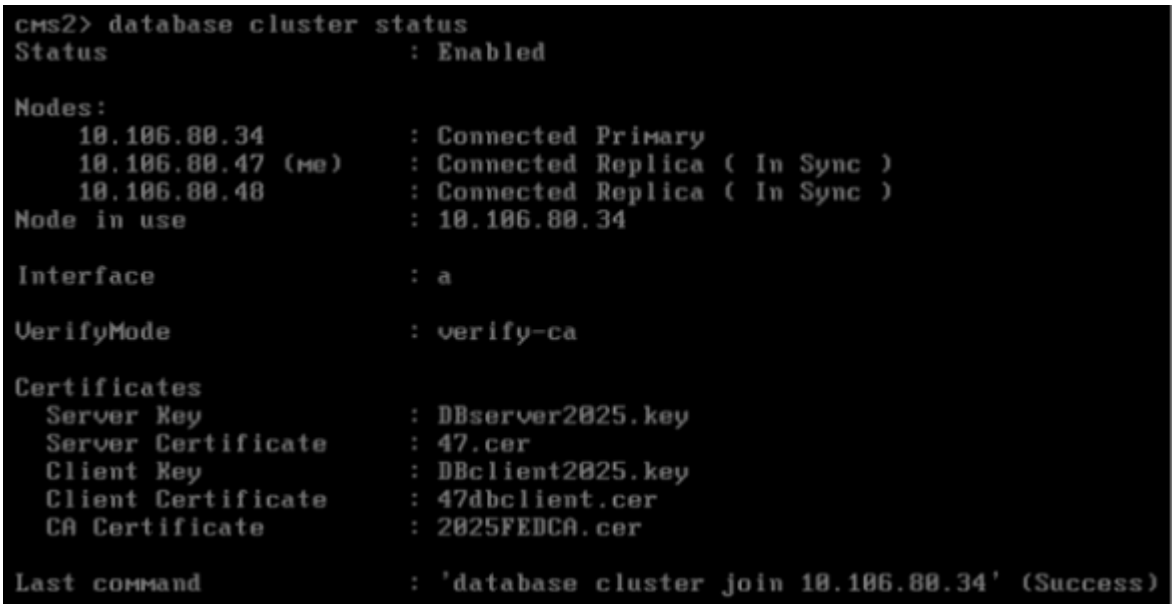


Figura 23: Registrare le repliche primarie correnti e confermare che sono sincronizzate.

3. Verificare che tutti i tipi di chiamata in uso siano funzionanti e che le condizioni di errore siano state eliminate in ogni nodo (sezione Convalida integrità server prima di creare backup).

4. Creare un backup di ogni nodo utilizzando la sezione Esegui backup quando l'archiviazione sicura è disabilitata o non disponibile. Assegnare un nome a ogni file in modo che sia chiaramente mappato al relativo nodo e trasferire ogni backup allo storage esterno prima di scollegare il cluster.

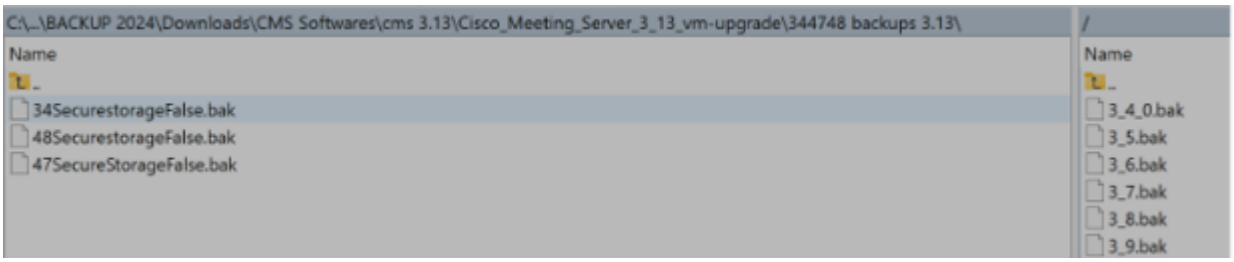


Figura 24: Tutti e tre i backup dei nodi di esempio hanno archiviato lo storage esterno, in modo che ogni file venga mappato al relativo nodo.

Disconnetti il cluster

Rimuovere i nodi nell'ordine indicato. Mantieni il database primario fino all'ultimo:

- Nodi di Meeting Server connessi (non di base)
- Nodi di database di replica
- Nodo di database primario

Su ogni nodo, eseguire il comando di rimozione e premere Y. Non continuare con l'aggiornamento alla versione 4.0 fino a quando tutti i nodi non segnalano che ha lasciato il cluster. La rimozione dell'appartenenza al cluster lascia il database locale di tale nodo sul posto.

database cluster remove

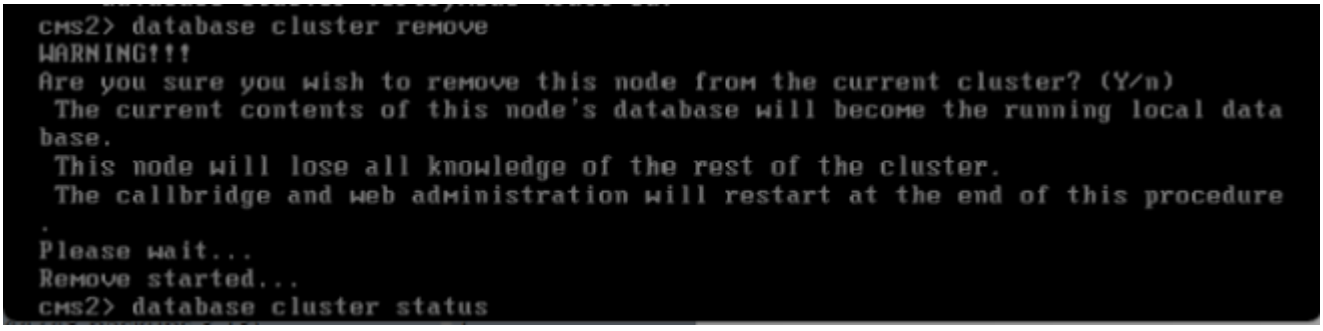


Figura 25: In una replica, confermare Y per rimuovere l'appartenenza al cluster. Il database locale del nodo rimane attivo.

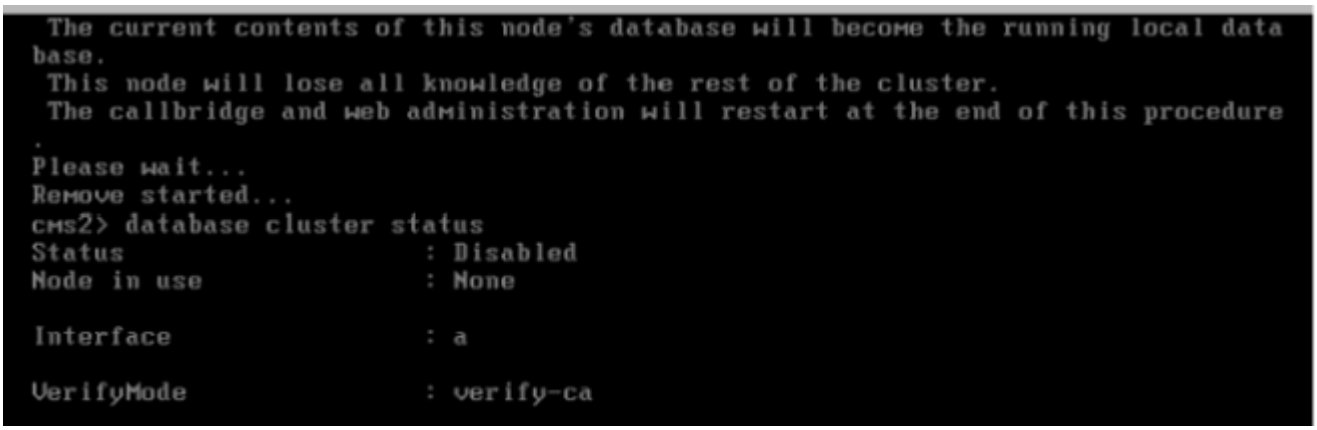


Figura 26: Dopo la rimozione, verificare che lo stato del cluster sia Disabilitato e che il nodo in uso sia Nessuno in tale nodo.

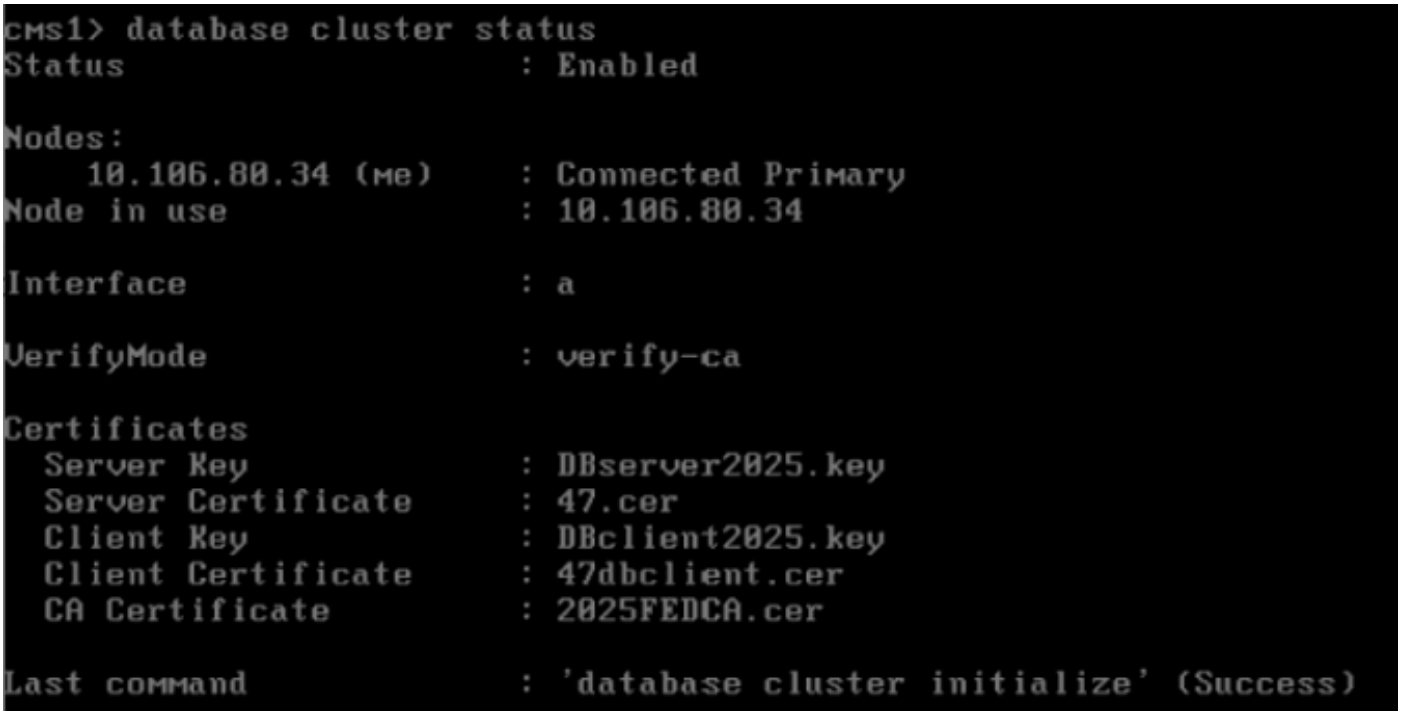


Figura 27: Dopo la rimozione delle repliche, il primo nodo primario è l'unico rimasto nel cluster. Rimuoverlo per ultimo.

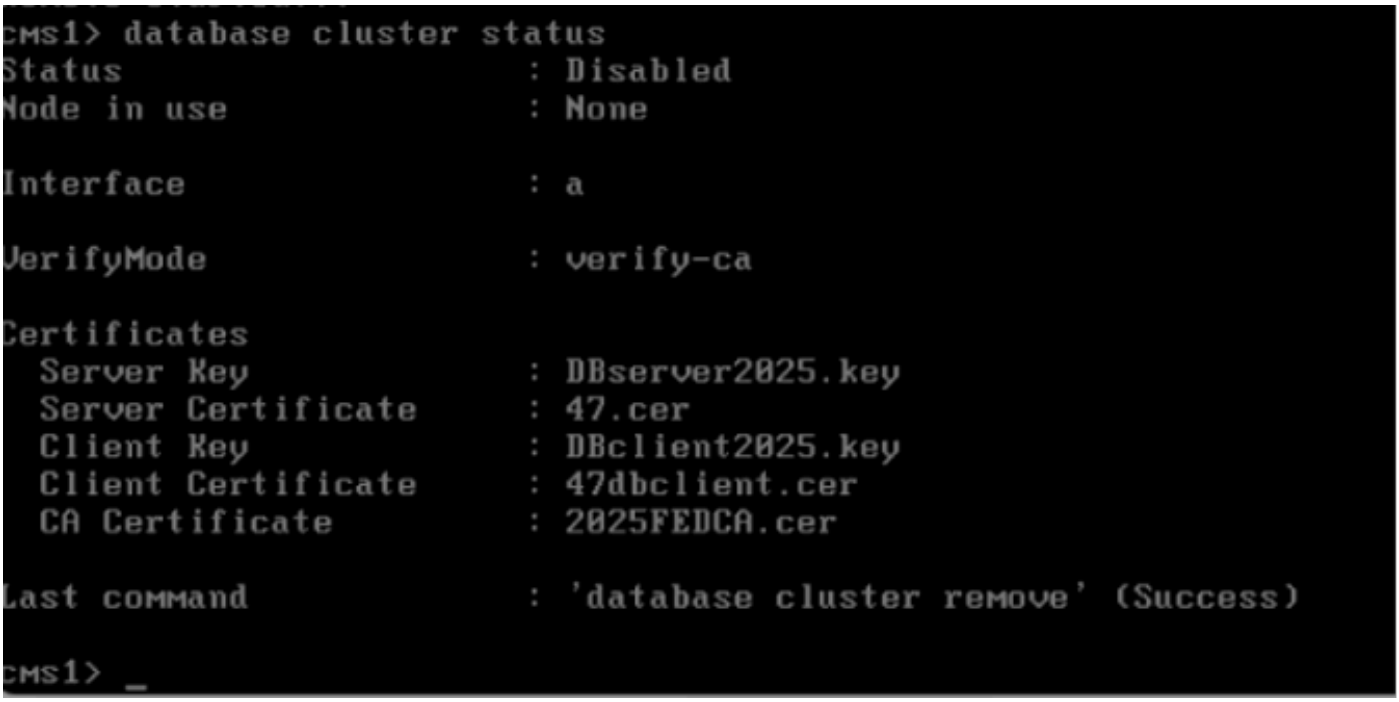


Figura 28: Dopo aver rimosso il server primario precedente, verificare che il comando segnali l'esito positivo e che lo stato del cluster sia Disabilitato.

Aggiornamento e ripristino dei nodi

1. Una volta disattivati, i nodi sono autonomi e possono essere aggiornati in parallelo. Su ciascun nodo, copiare upgrade.img su SFTP ed eseguire il comando upgrade:

upgrade upgrade.img

2. Ripristinare l'indirizzamento di rete di ciascun nodo dalla console (sezione Primo avvio e ripristino della rete).

3. Copiare il backup 3.13.x di ciascun nodo in quel nodo. Ripristinare prima la versione primaria precedente, quindi le repliche e infine i nodi connessi. Utilizzare la sezione Ripristino dei dati dopo l'aggiornamento alla versione 4.0. Il ripristino dei backup ristabilisce l'appartenenza al cluster di database.

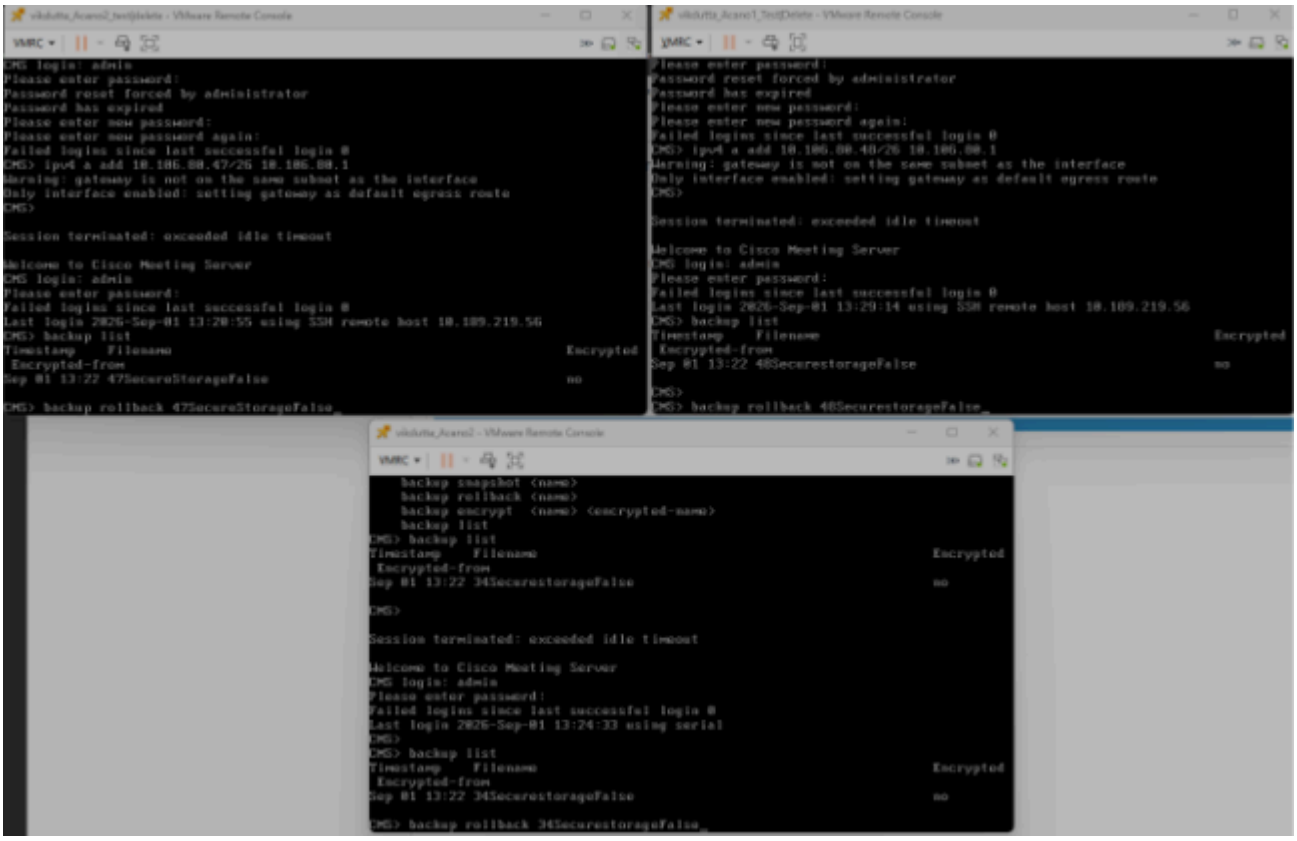


Figura 29: Ripristinare lo snapshot di ogni nodo. Iniziare con la versione primaria precedente, quindi ripristinare le repliche. I nomi file di esempio identificano il nodo corrispondente.

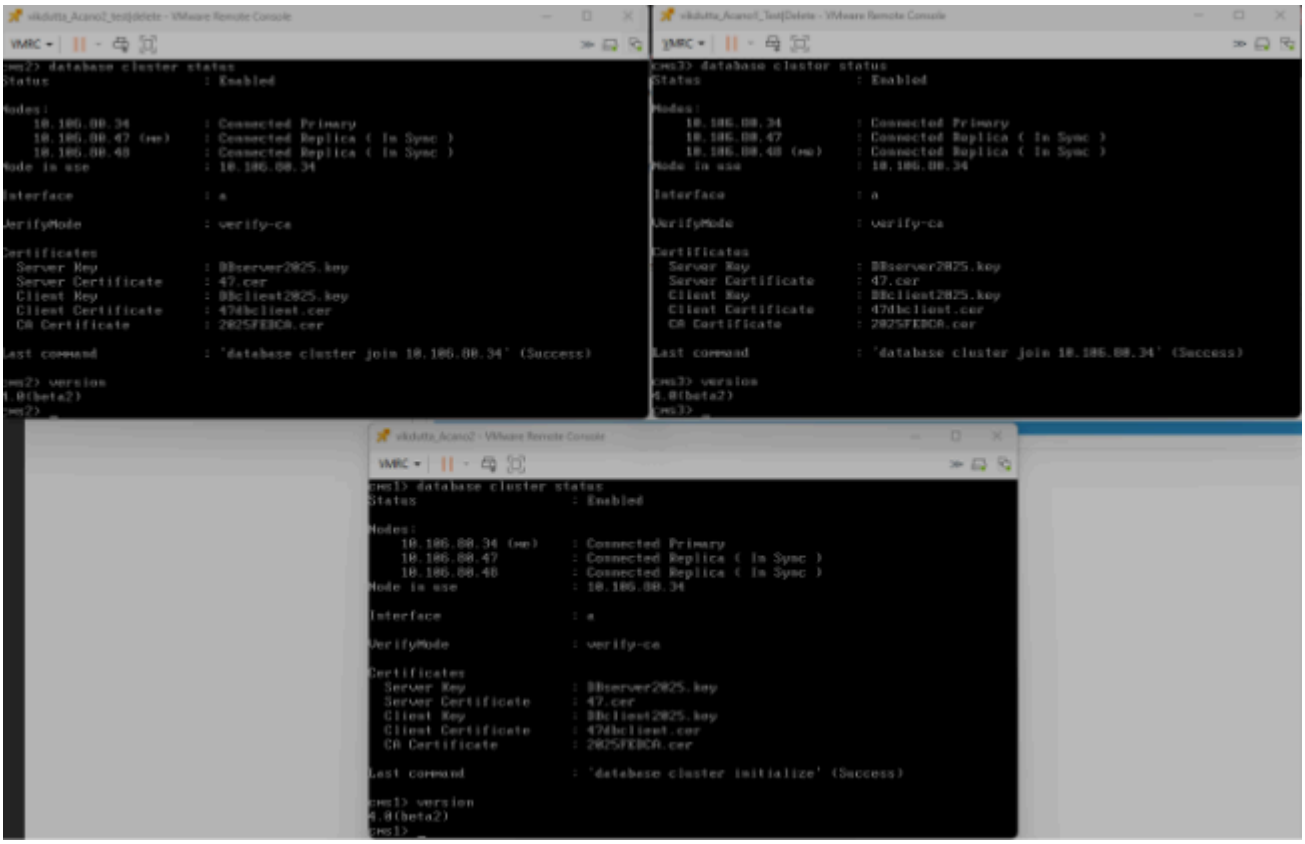


Figura 30: Dopo il ripristino in Meeting Server 4.0, verificare che il cluster sia Abilitato, che venga visualizzato lo stesso database primario e che le repliche siano Sincronizzate.

Nota: Se dopo il ripristino non vengono attivate le connessioni del cluster di tipo Call Bridge, eseguire il comando solo sul **database cluster upgrade_schema** server primario precedente, quindi ricontrollare lo stato del bridge di chiamate.

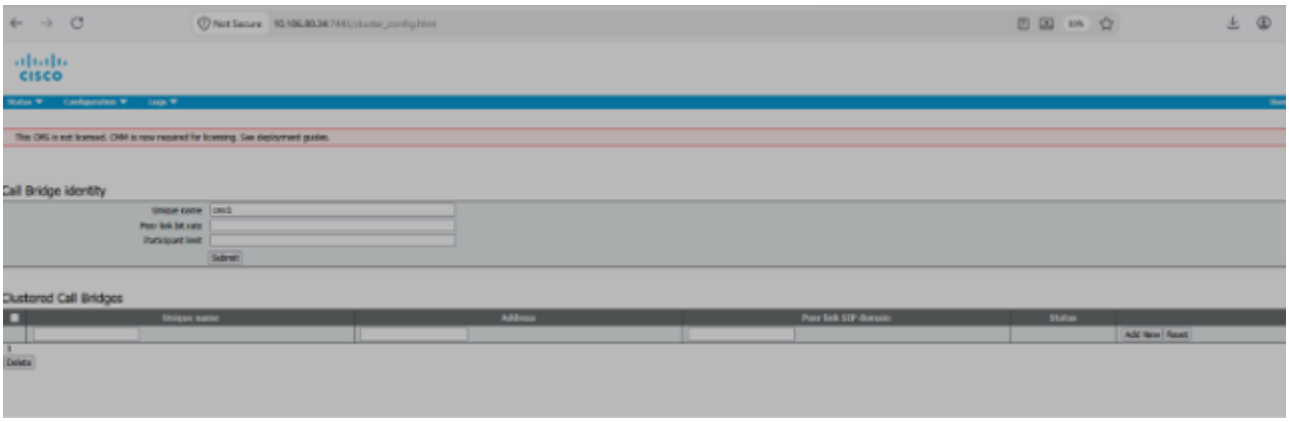


Figura 31: Prima dell'aggiornamento dello schema, nell'esempio viene illustrato il cluster di database in esecuzione mentre Clustered Call Bridges è vuoto.

database cluster upgrade_schema

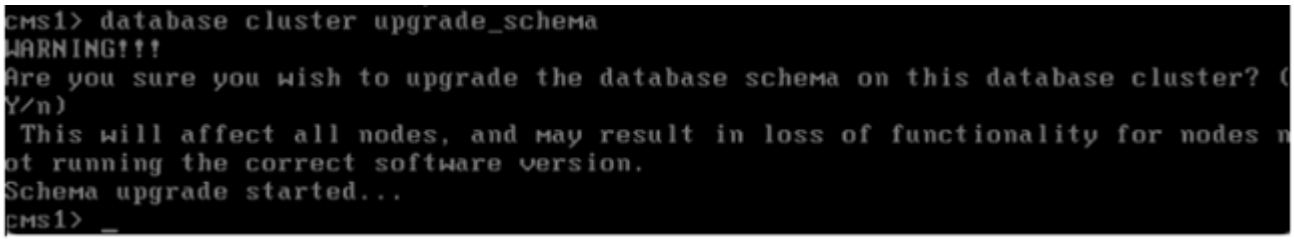


Figura 32: Sul primo server primario, confermare Y solo quando le connessioni del cluster di tipo Call Bridge non sono riuscite dopo l'aggiornamento del cluster disattivato.

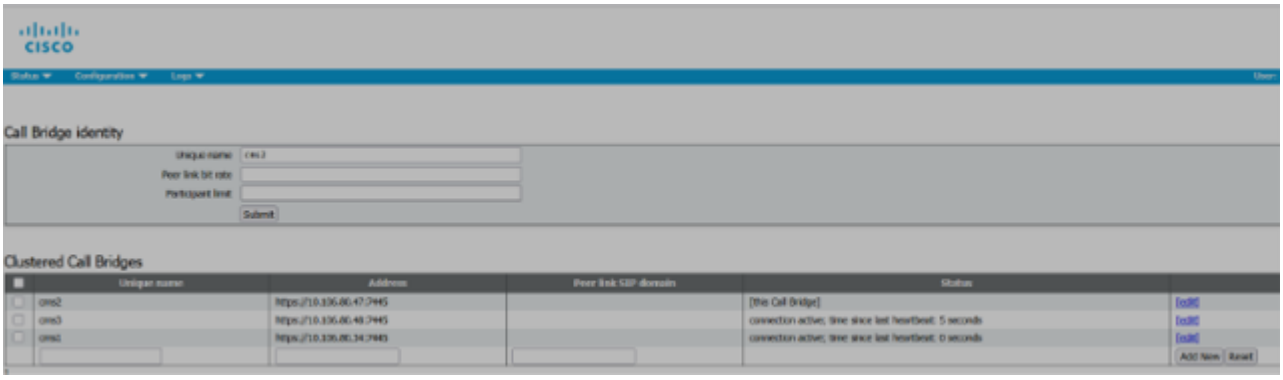


Figura 33: Dopo l'aggiornamento dello schema, verificare che ogni peer del bridge di chiamate mostri una connessione attiva.

4. Completare la procedura segreta MeetingApps nella sezione Chiave segreta MeetingApps dopo il ripristino in ogni Web Bridge, quindi convalidare la distribuzione utilizzando la sezione Convalida post-aggiornamento.

Scenario 4 - Cluster di database con archiviazione sicura abilitata

Utilizzare questa procedura per un cluster di database su macchine virtuali, Meeting Server Small o Meeting Server Medium in cui è abilitata l'archiviazione sicura sui nodi. Non è applicabile a Meeting Server 2000. Innanzitutto, aggiornare ogni nodo alla versione 3.13.x.

Registrazione dei dettagli del cluster e creazione di backup crittografati

1. Eseguire secure_storage su ogni nodo e confermare Abilitato: Vero.

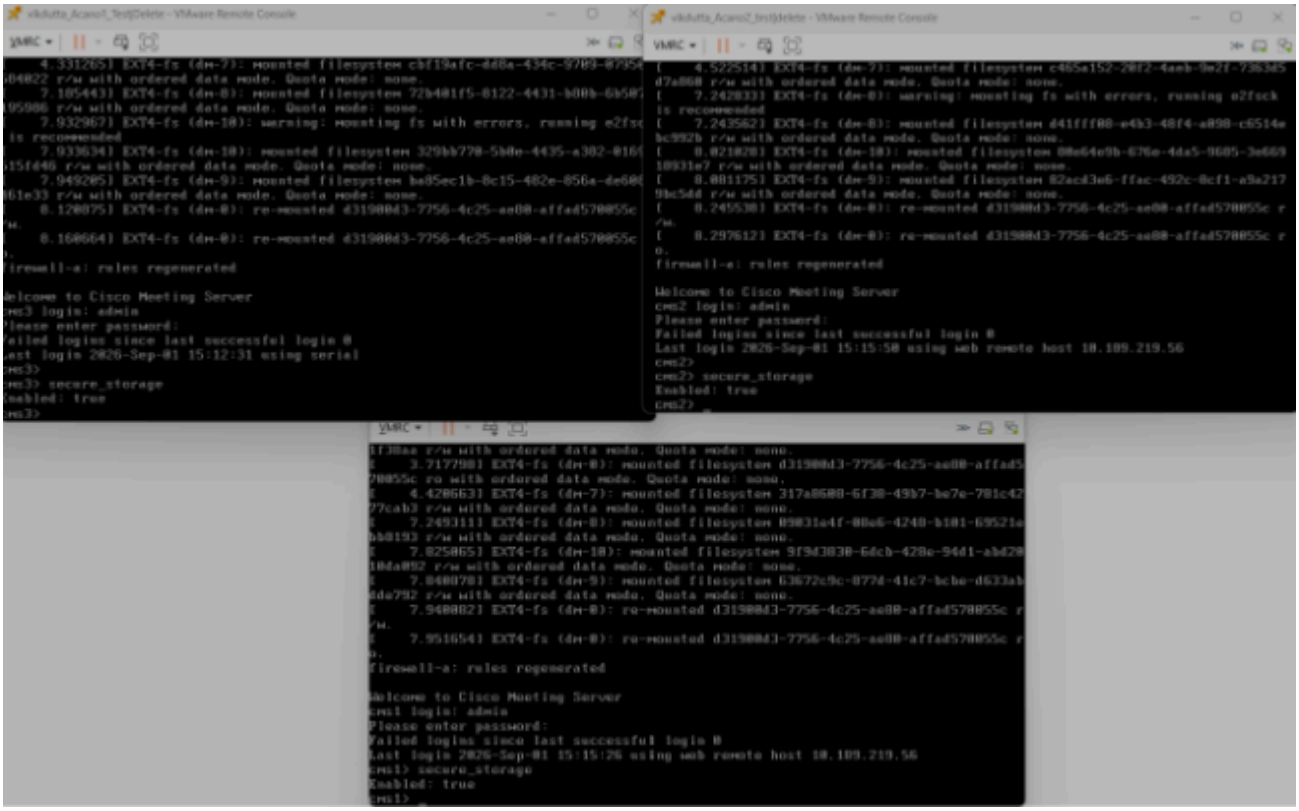


Figura 34: Per il cluster a tre nodi illustrato, confermare che l'opzione Archiviazione sicura visualizzi Attivato: True su ogni nodo prima dell'aggiornamento.

2. Registrare il database primario corrente e confermare che le repliche sono sincronizzate.

```
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: stato del cluster di database prima dell'aggiornamento. Registrare le repliche primarie e confermare che sono sincronizzate.

3. Verificare che tutti i tipi di chiamata in uso funzionino e che le condizioni di errore siano state cancellate in ogni nodo (sezione Convalida integrità server prima di creare backup).

4. Creare un backup crittografato di ogni nodo utilizzando la sezione Esegui backup quando l'archiviazione sicura è abilitata. Assegnare e registrare una passphrase univoca per ogni file o utilizzare una policy di passphrase documentata. Trasferire dai server solo i file crittografati prima di scollegare il cluster.

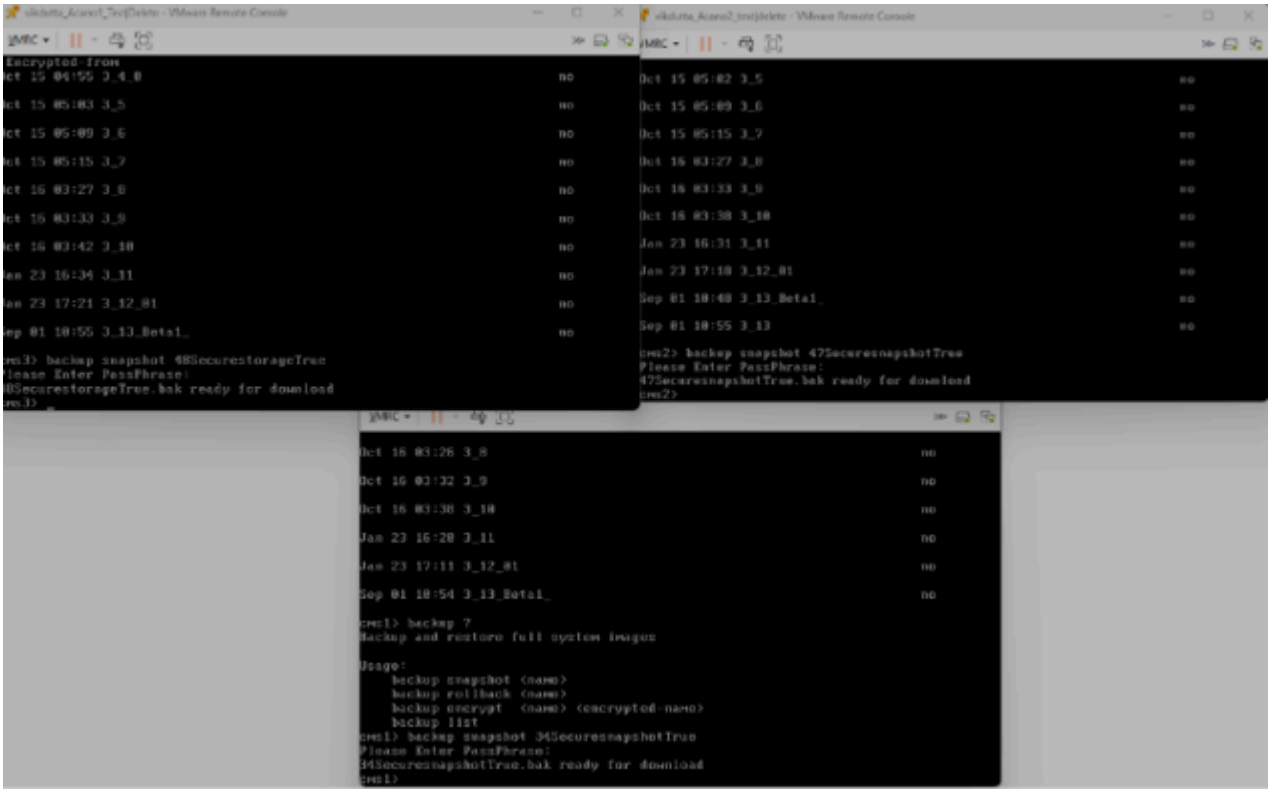


Figura 36: Snapshot di backup crittografato in ogni nodo. Nell'esempio viene visualizzata la richiesta della passphrase e quindi ogni file con estensione bak pronto per il download.

Disconnetti, aggiorna e ripristina

Scollegare il cluster come descritto nello scenario 3 nell'ordine seguente: nodi connessi, repliche e ultimo nodo primario. Utilizzare cluster di database per rimuovere e verificare che ogni nodo abbia lasciato il cluster.

Aggiornare i nodi autonomi in parallelo. Ripristinare gli indirizzi di rete dalla console (sezione Primo avvio e ripristino della rete).

Caricare il backup crittografato di ciascun nodo. Prima di un rollback, verificare che lo snapshot caricato venga visualizzato nell'elenco di backup come Crittografato: sì. Ripristinare prima la versione primaria precedente, quindi le repliche e i nodi connessi. Usare il comando backup rollback riportato di seguito, confermare Y e immettere la passphrase del backup quando richiesto. Il nodo viene riavviato dopo l'accettazione della passphrase. Ripetere l'operazione per ogni nodo.

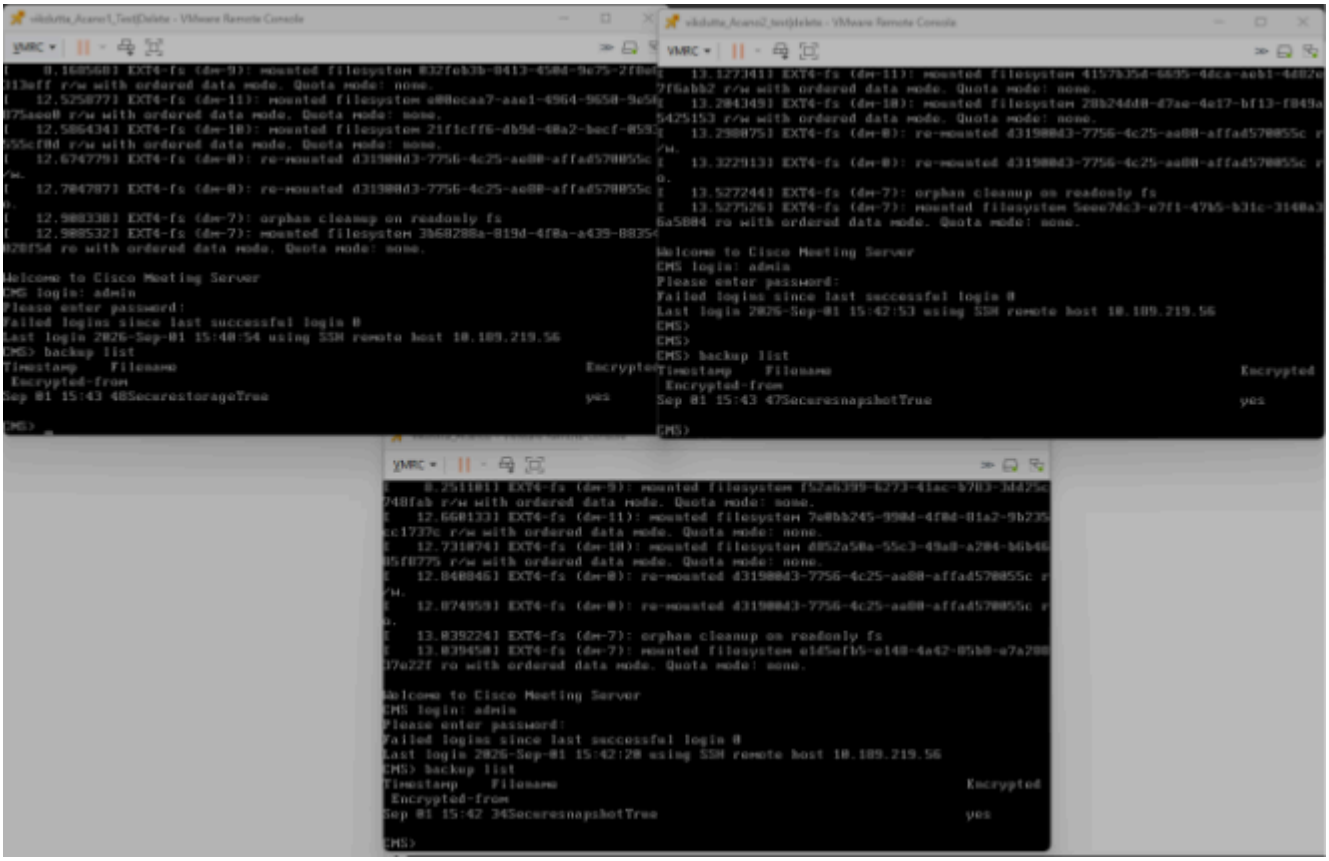


Figura 37: Dopo il primo avvio della versione 4.0, lo snapshot caricato deve essere visualizzato nell'elenco dei backup come Crittografato: sì, ed essere pronti per il rollback.

backup rollback encrypted-filename

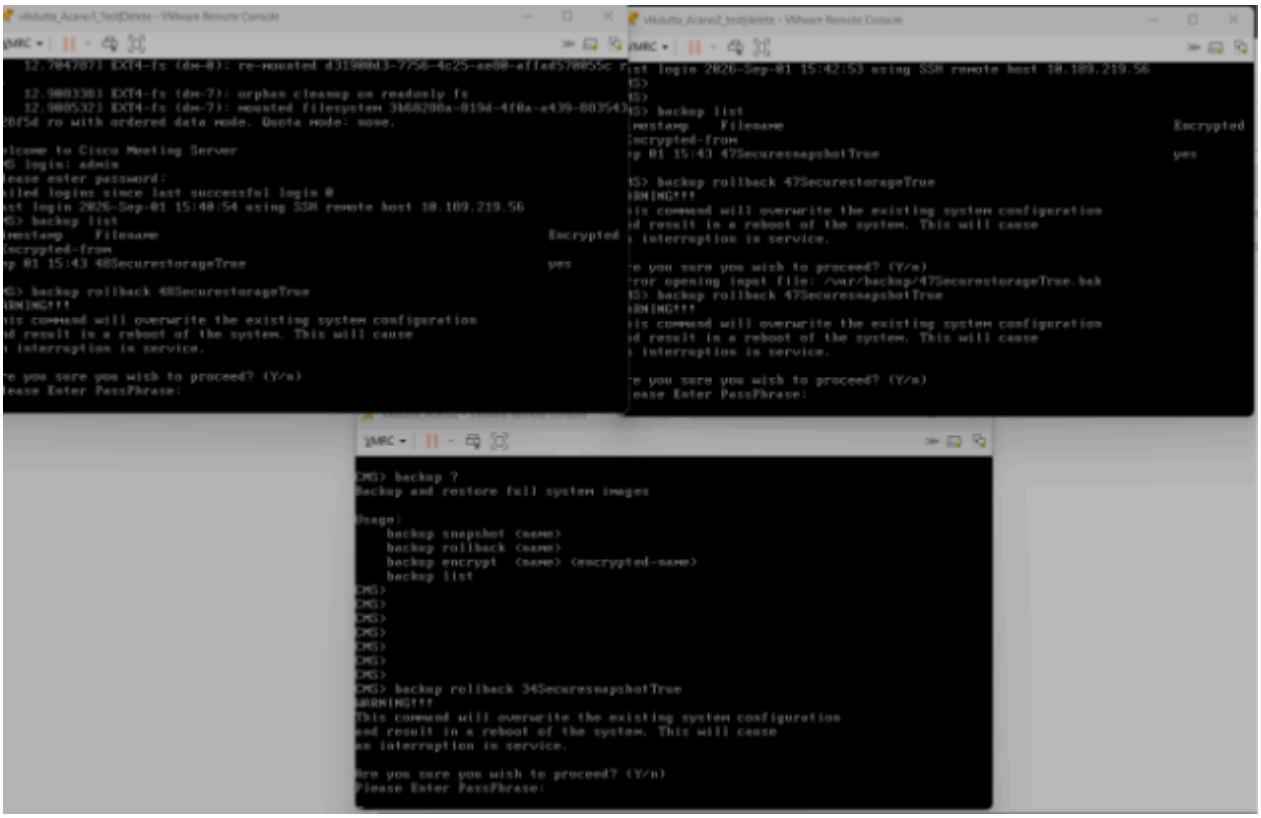


Figura 38: Confermare Y, immettere la passphrase e ripristinare prima la versione primaria precedente.

Nota: Se dopo il ripristino non vengono attivate le connessioni del cluster di tipo Call Bridge, eseguire il comando solo sul **database cluster upgrade_schema** server primario precedente, quindi ricontrollare lo stato del bridge di chiamate.

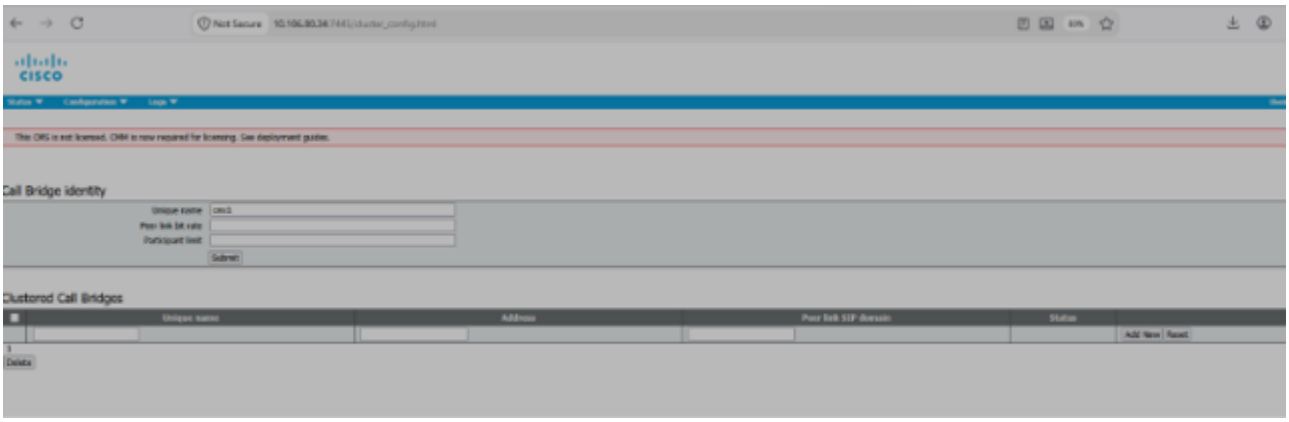


Figura 39: Prima dell'aggiornamento dello schema, nell'esempio viene illustrato il cluster di database in esecuzione mentre Clustered Call Bridges è vuoto.

database cluster upgrade_schema

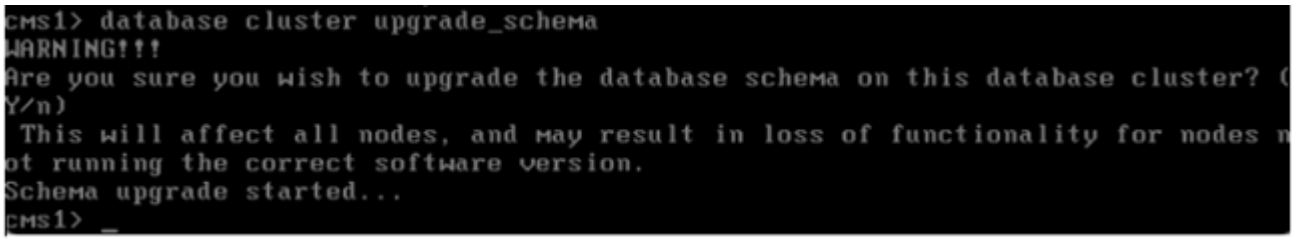


Figura 40: Sul primo server primario, confermare Y solo quando le connessioni del cluster di tipo Call Bridge non sono riuscite dopo l'aggiornamento del cluster disattivato.

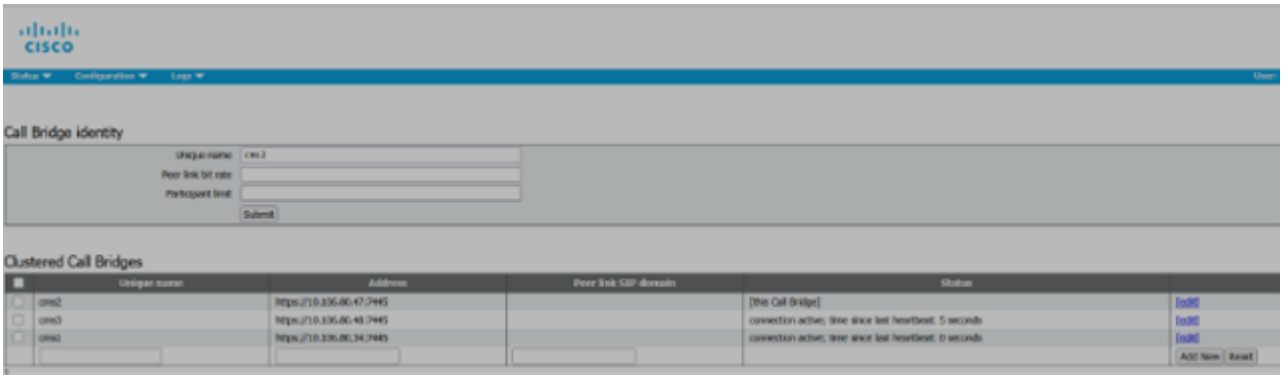


Figura 41: Dopo l'aggiornamento dello schema, verificare che ogni peer del bridge di chiamate mostri una connessione attiva.

Completare la procedura segreta MeetingApps nella sezione Chiave segreta MeetingApps dopo il ripristino in ogni Web Bridge, quindi convalidare la distribuzione utilizzando la sezione Convalida post-aggiornamento.

Convalida post-aggiornamento

Completare questo elenco di controllo dopo il ripristino e prima di riportare il sistema in produzione:

- In Amministrazione Web su ogni nodo è visualizzato Cisco Meeting Server 4.0.
- I servizi MMP richiesti sono abilitati e in esecuzione (attivi: Vero).
- Le condizioni di errore sono chiare. Considera gli errori e gli avvisi recenti come informazioni, a meno che non esista un errore corrispondente.
- Se applicabile, lo stato del cluster di database mostra le repliche e le primarie previste.
- Smart Licensing e la connettività del bridge di chiamate vengono ripristinate.
- Le chiamate SIP e le chiamate client dell'app Web supportate da questa distribuzione sono state completate.
- I messaggi di branding, le richieste audio e i file SSO copiati dal server nella sezione Requisiti pre-aggiornamento vengono ripristinati se non sono già stati inclusi nel backup.
- Se MeetingApps è distribuito, Bridge Web visualizza la nuova relazione MeetingApps e funziona la condivisione di file.
- Rimuovere gli snapshot di breve durata solo dopo l'accettazione della distribuzione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).