Upgrade Meeting Server naar Release 4.0 - Witboek

Inhoud

- Inleiding
- Achtergrondinformatie
- Overzicht van veilige opslag
  - Ondersteunde platforms
  - Implementatienotities
- Principes en beperkingen upgraden
  - Vereist upgradepad
  - downgrades
  - Kritieke back-upvereisten voor 4.0-upgrades
  - Eerste login- en wachtwoordconfiguratie
  - Netwerkverbinding herstellen na upgrade
  - Serverstatus valideren voordat back-ups worden gemaakt
- Voorafgaande upgradevereisten
- Gemeenschappelijke back-up- en terugzetprocedures
  - Gegevens beïnvloed na 4.0-upgrade
  - Maak een back-up wanneer Secure Storage is uitgeschakeld of niet beschikbaar is
  - Maak een back-up wanneer Secure Storage is ingeschakeld
  - Gegevens herstellen na 4.0-upgrade
  - MeetingApps geheime sleutel na herstel
- Eerste opstart en netwerkherstel
- Upgradescenario's
  - Scenario 1 - Single Node met beveiligde opslag uitgeschakeld of niet beschikbaar
  - Scenario 2 - Single Node met veilige opslag ingeschakeld
  - Scenario 3 - Databasecluster met beveiligde opslag uitgeschakeld
    - Clusterdetails opnemen en back-ups maken van elk knooppunt
    - De cluster ontbinden
    - Upgrade en herstel de nodes
  - Scenario 4 - Databasecluster met beveiligde opslag ingeschakeld
    - Clustergegevens opnemen en gecodeerde back-ups maken
    - Ontbinding, upgrade en herstel
- Validatie na upgrade

Inleiding

In dit document wordt beschreven hoe u Cisco Meeting Server kunt upgraden naar versie 4.0.

Achtergrondinformatie

Gebruik dit document samen met de Cisco Meeting Server-releasenota's, de MMP Command Reference Guide en de Secure Storage Administrator Reference Guide om de vereisten en vereisten te begrijpen.

Het upgradeproces voor Cisco Meeting Server 4.0 verschilt van eerdere versies omdat het toepassen van het image een fabrieksreset van het knooppunt activeert. Om de continuïteit van de service te garanderen, moeten alle eerdere configuraties, inclusief netwerkinstellingen en wachtwoorden, worden bewaard via een back-up die naar een externe locatie wordt geëxporteerd voordat u de upgrade start.

Daarnaast was Secure Storage optioneel in Cisco Meeting Server versies 3.11 tot en met 3.13, maar het is standaard ingeschakeld in versie 4.0. Als gevolg hiervan moet u verschillende back-up- en terugzetprocedures volgen als u nog nooit Secure Storage hebt gebruikt of als u het al hebt ingeschakeld op 3.11x, 3.12x of 3.13x.

Secure Storage versleutelt privésleutel- en back-upbestanden op de server en vereist dat deze bestanden worden gecodeerd voordat u ze naar externe opslag kunt overbrengen.

In dit document worden de vereiste richtlijnen samengevoegd tot één verwijzing, zodat u een gemeenschappelijke procedure kunt volgen voor alle upgradescenario's zonder dat u dezelfde stappen hoeft te herhalen.

Dit document behandelt deze onderwerpen:

- Wat is Secure Storage, waar is het van toepassing en wat doet het niet.
- Het upgradepad, dat de vereiste bevat om 3.13.x te bereiken vóór 4.0 en het feit dat een downgrade van 4.0 niet wordt ondersteund.
- Een veelgebruikte back-up- en herstelmethode voor nodes waar Secure Storage is ingeschakeld en voor nodes waar deze is uitgeschakeld of niet beschikbaar is.
- Databasecluster node disband sequencing terwijl het databasecluster wordt ontbonden voorafgaand aan een upgrade.
- De geheime sleutel van MeetingApps, die niet is opgeslagen in een back-up van Cisco Meeting Server en die na een terugzetprocedure opnieuw moet worden gegenereerd.

Opmerking: in dit document worden screenshots van laboratoriumtests gebruikt die zijn gemaakt tijdens het testen van de oorspronkelijke upgraderichtlijnen, waaronder versies van 4.0 bètasoftware. Alle weergegeven hostnamen, IP-adressen en bestandsnamen zijn

---

strikt illustratief en geven geen werkelijke productiereferenties of gevoelige wachtwoordzinnen weer. Om de duidelijkheid te behouden en redundantie te voorkomen, worden herhaalde stappen slechts eenmaal weergegeven in de sectie Gemeenschappelijke procedure, tenzij de clusterweergave aanvullende noodzakelijke context biedt.

Overzicht van veilige opslag

Secure Storage biedt verbeterde gegevensbeveiliging door gevoelige bestanden te coderen die zich op de vergaderserver bevinden en door te bepalen hoe deze bestanden worden gedownload van de Call Bridge-server. De mogelijkheid werd geïntroduceerd in Cisco Meeting Server 3.11 als een configureerbare optie met het gebruik van de MMP-opdracht secure_storage enable op implementaties van virtuele machines (op specificaties gebaseerd of Small Meeting Server) en op Meeting Server Medium.

Vanaf versie 4.0 is Secure Storage standaard ingeschakeld. Deze instelling is nu permanent en onomkeerbaar en de opdracht secure_storage enable MMP is verwijderd.

Met Secure Storage handhaaft de Meeting Server dit gedrag:

- Privésleutels kunnen niet via SFTP worden gedownload totdat ze zijn gecodeerd. Een privésleutel versleutelen met de opdracht pki encrypt MMP gevolgd door een wachtwoordzin van ten minste 14 tekens. Dit verandert niets aan de sleutels die momenteel worden gebruikt door Meeting Server-services.
- Back-upbestanden die zijn gemaakt met de opdracht <naam> voor codering van de back-up zijn gecodeerd. Wanneer Secure Storage is ingeschakeld, vraagt de opdracht <naam> encrypted-name MMP om een wachtwoordzin van ten minste 14 tekens. Dezelfde wachtwoordzin is vereist tijdens het terugzetten van de back-up.
- Voordat een back-upbestand wordt gedownload, moet het in gecodeerde vorm zijn. Als een vermelde back-up nog niet is gecodeerd voor export, gebruikt u back-upcodering <naam> gecodeerde naam. Pogingen om een niet-versleutelde back-up te downloaden worden geweigerd.
- Vanaf versie 3.12 kan Secure Storage werken wanneer FIPS is ingeschakeld. Privésleutelbestanden die in 3.11 zijn gemaakt met een kortere wachtwoordzin, moeten opnieuw worden gegenereerd met een wachtwoordzin van ten minste 14 tekens.



Tip: Secure Storage beperkt de overdracht van niet-versleutelde privésleutels en niet-versleutelde back-upbestanden van de vergaderserver. Het beperkt de overdracht van certificaatbestanden niet. Certificaten kunnen nog steeds worden gekopieerd met SFTP;

alleen de bijbehorende niet-gecodeerde privésleutels worden geblokkeerd totdat ze zijn gecodeerd met pki-encryptie.

⚠ Waarschuwing: als Secure Storage eenmaal is ingeschakeld, kan deze niet worden uitgeschakeld met een MMP-opdracht. De operatie is onomkeerbaar. Alleen factory_reset zet Secure Storage volledig terug op false. Maak een back-upconfiguratie met een back-upmomentopname en sla deze op een apart apparaat op voordat u Secure Storage inschakelt. Na secure_storage onmiddellijk opnieuw opstarten inschakelen. Als de reboot wordt overgeslagen, kan Secure Storage worden gemarkeerd als ingeschakeld zonder volledig te zijn geïnitialiseerd, en opdrachten zoals een factory_reset full kunnen mislukken. Het herstelpad in die staat is om terug te keren naar een eerder opgeslagen momentopname (deze is alleen geldig voor 3.13.x). In Meeting Server 4.0 is secure_storage standaard ingeschakeld.

Ondersteunde platforms

- Virtuele machine (op basis van specificaties): ondersteund
- Vergaderserver klein/1K: ondersteund
- Vergaderservermedium: ondersteund
- Meeting Server 2000: niet ondersteund. De functie voor beveiligde opslag is niet beschikbaar. Gebruik geen opdrachten voor beveiligde opslag op dit platform.

Cisco Meeting Server 4.0 maakt standaard Secure Storage op alle compatibele platforms mogelijk. Na de upgrade worden de gegevens automatisch beveiligd door Secure Storage, zelfs als de 3.13.x-back-up is gemaakt terwijl Secure Storage is uitgeschakeld.

Implementatienotities

- De naam van het upgrade-image wijzigen verandert niets aan de instellingen voor veilige opslag.
- Bevestig de status van de beveiligde opslag op elk knooppunt met behulp van de opdracht secure_storage voordat u back-ups maakt.
- De opdracht meldt of Secure Storage is ingeschakeld (True) of niet (False). Op Meeting Server 2000 is de opdracht niet van toepassing. Terwijl u een upgrade uitvoert naar Cisco Meeting Server 2000, volgt u de stappen die worden vermeld onder upgradevoorwaarden waarbij Secure Storage is uitgeschakeld of niet beschikbaar is.



MMP-uitvoer wanneer Secure Storage niet is ingeschakeld (ingeschakeld: false).



Afbeelding 2: MMP-uitvoer wanneer Secure Storage is ingeschakeld (ingeschakeld: true) op Cisco Meeting Server 3.13.

Gedetailleerde syntaxiswaarschuwingen voor opdrachten en voorbeeldgebruik zijn te vinden in de Cisco Meeting Server Administrator Quick Reference Guide for Secure Storage en de MMP Command Reference die u momenteel gebruikt.

Principes en beperkingen upgraden

Vereist upgradepad

Cisco Meeting Server-upgrades moeten een sequentieel pad volgen zonder belangrijke releases over te slaan. Een node op 3.11.x moet bijvoorbeeld door 3.12.x en 3.13.x gaan voordat het 4.0 bereikt. Directe upgrades van eerdere versies zoals 3.9.x naar 3.13.x of 3.11.x naar 4.0 worden niet ondersteund en veroorzaken doorgaans niet-herstelbare configuratiefouten. Voor Meeting Server Medium met versies 3.11.5 of 3.13 is het upgradepad 3.11.5 → 3.13 → 4.0.

Tip: Voordat u de 4.0-upgrade start, moet elke node Cisco Meeting Server 3.13.x uitvoeren, waarbij een geverifieerde configuratieback-up wordt geëxporteerd van dat 3.13.x-systeem. Alle scenarioprocedures in dit artikel gaan ervan uit dat de stap-upgrade naar 3.13.x al voltooid is.

---

downgrades

Tip: Een downgrade van 4.0.x naar 3.13.x wordt niet ondersteund. Als de upgrade mislukt

---

of het systeem niet werkt zoals verwacht, implementeert u een nieuwe 3.13.x OVA (of maakt u een nieuwe image van het toestel) en zet u de 3.13.x back-up terug. Houd hypervisormomentopnamen van de 3.13.x virtuele machines voor de duur van het upgradevenster als extra hersteloptie. VM-momentopnamen vervangen geëxporteerde configuratieback-ups niet.

Kritieke back-upvereisten voor 4.0-upgrades

Nadat de 4.0-upgrade is bevestigd, start de node opnieuw op in een eerste opstartstatus. Wees niet afhankelijk van de automatische back-up die tijdens het upgradeproces wordt gegenereerd, omdat een upgrade-fout kan leiden tot verlies van SFTP-toegang en het bestand ontoegankelijk kan maken. Alleen back-ups die zijn gemaakt met de opdracht Back-upmomentopname en die zijn gekopieerd naar externe opslag, kunnen op betrouwbare wijze worden gebruikt voor herstel.

Eerste login- en wachtwoordconfiguratie

Bij het eerste opstarten van versie 4.0 wordt het bestaande MMP-wachtwoord uit de database verwijderd. Log in met de gebruikersnaam admin met een leeg wachtwoord (geen wachtwoord). Het systeem vereist dat u een nieuw MMP-wachtwoord instelt. Het systeem vraagt u om het wachtwoord twee keer in te voeren voor verificatie en bevestiging. Aangezien er geen wachtwoordherstelfunctie is voor Meeting Server, moet u uw nieuwe wachtwoord opnemen.

Opmerking: Als u bij het eerste opstarten een nieuw MMP-wachtwoord instelt, vervangt de opdracht Back-up terugdraaien deze door het wachtwoord dat is opgeslagen in de 3.13.x-back-up. Nadat u de back-up op de server hebt teruggezet, moet u zich aanmelden met het wachtwoord dat actief was op het moment dat de back-up werd gemaakt.

Netwerkverbinding herstellen na upgrade

IPv4- en IPv6-adressen, maskers en gateways gaan samen met de rest van de configuratie verloren. De netwerkconnectiviteit van de Meeting Server kan verloren gaan na de upgrade naar 4.0. U moet hypervisorconsole-, CIMC- of seriële toegang hebben, zodat u opnieuw adressen kunt toewijzen vanuit de MMP.



Opmerking: implementaties die DHCP-reserveringen gebruiken, behouden meestal dezelfde IP-adressen na het opnieuw opstarten. De toegang tot de console moet echter beschikbaar blijven totdat het adres is geverifieerd. Ga er niet vanuit dat de SSH-connectiviteit is hersteld totdat het IP-adres is bevestigd.

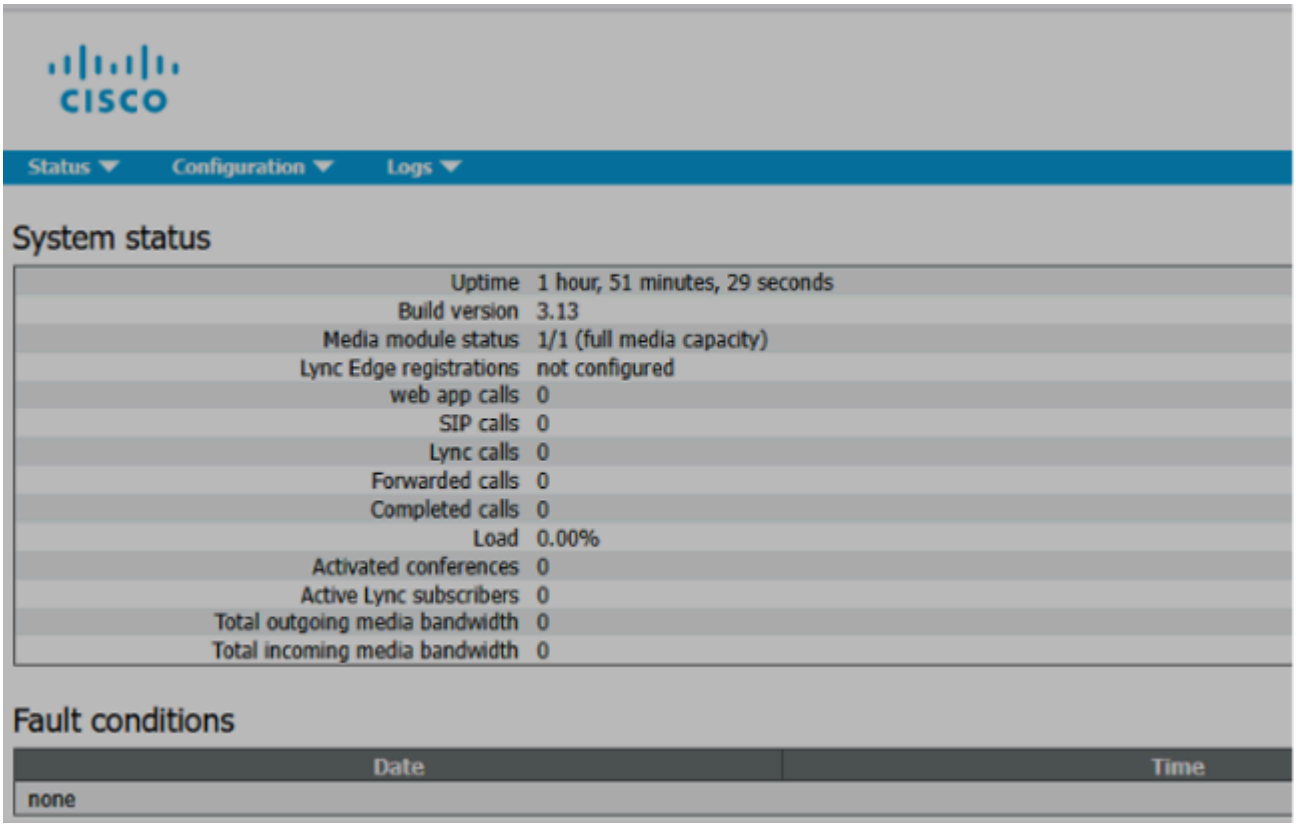
Serverstatus valideren voordat back-ups worden gemaakt

Zorg er na elke stap-upgrade naar 3.13 voor dat de server in goede staat verkeert en dat alle services werken. Negeer geen foutcondities op de overzichtspagina van de server. Als u fouten/fouten tegenkomt, moet u deze oplossen voordat een back-upmomentopname wordt gemaakt op 3.13. Dit zorgt ervoor dat een gezonde serverback-up wordt hersteld op geüpgradede 4.0-knooppunten, waardoor uw implementatiefout vrij blijft.

Open Status in Webbeheer en bevestig dat de sectie Foutvoorwaarden leeg is. Negeer vermeldingen die alleen worden weergegeven onder Recente fouten en waarschuwingen. Na een upgrade is het gebruikelijk om daar tijdelijke databases of Web Bridge-berichten te zien; die zijn geen reden om de back-up te herstellen of uit te stellen.

Als er langer dan tien minuten een foutsituatie blijft bestaan, lost u deze op voordat u de back-up maakt. Een terugzetbewerking van een 3.13.x-back-up die al fouten bevat naar 4.0 voert deze fouten naar voren.

Bevestig voor geclusterde systemen dat alle gebruikte gesprekstypen werken (SIP-eindpunten en Web App-clients) en dat er geen foutvoorwaarden op een knooppunt worden vermeld.



Afbeelding 3: webbeheerderspagina op 3.13.x met foutvoorwaarden leeg. Gebruik deze weergave voordat u de back-up maakt die wordt teruggezet naar 4.0.

Voorafgaande upgradevereisten

Voordat u de upgrade naar versie 4.0 start, voert u deze acties uit. Deze vereisten zijn van toepassing op alle vier scenario's die later in dit document worden behandeld.

- Upgrade naar 3.13.x en exporteer vervolgens een configuratieback-up. Zorg ervoor dat de node Cisco Meeting Server 3.13.x uitvoert. Maak een back-up en breng deze, samen met alle aangepaste SFTP-gegevens zoals logo's, merkbestanden, audioprompts, SSO-bestanden en andere aangepaste gegevens, over naar externe opslag. Gebruik de procedures in het gedeelte Gemeenschappelijke back-up- en terugzetprocedures. In een geclusterde omgeving maakt u een back-up van elk knooppunt, niet alleen van de aangesloten primaire, maar ook van de aangesloten replica.
- Netwerkinstellingen opnemen. Voer ipv4 a uit en sla de uitvoer op. U moet deze informatie opnieuw invoeren vanaf de console na de 4.0-herstart, tenzij een DHCP-reservering het IP-adres automatisch herstelt.
- Consoletoegang bevestigen. Hypervisorconsole, CIMC of seriële toegang moet beschikbaar zijn voordat u begint. SSH zal naar verwachting dalen wanneer de node opnieuw opstart naar 4.0.
- Download de huidige logbundel voor archivering. Sla logbundle.tar.gz op van elk knooppunt. De bundel is geen vervanging voor back-upmomentopnamen.
- Lees de waarschuwingsbanner voor 4.0-upgrades wanneer deze wordt weergegeven nadat de upgrade-opdracht is uitgevoerd.
- Druk op n om af te breken als een vereiste niet volledig is. Druk alleen op Y als u klaar bent om verder te gaan.

Gemeenschappelijke back-up- en terugzetprocedures

De vier upgradescenario's die later in dit document worden besproken, gebruiken hetzelfde back-up-, export-, first-boot- en herstelpatroon. Gebruik deze sectie als de enige bron van die stappen en volg vervolgens alleen de scenariospecifieke sequencing (single node versus cluster, en of Secure Storage al is ingeschakeld).

Gegevens beïnvloed na 4.0-upgrade

Deze gegevens gaan verloren na de 4.0-upgrade totdat u een back-up terugzet:

- Database-inhoud, die spaties, gebruikers en oproepprofielen bevat.
- Certificaten en privésleutels.
- Lokale aanpassing, SSO-bestanden en audiopromptbestanden.
- Netwerkconfiguratie (IP-adres, masker en gateway), behalve wanneer een DHCP-

reservering het adres terugzet.
- Het vorige MMP-wachtwoord, totdat de back-up wordt teruggedraaid, past het wachtwoord van de back-up opnieuw toe.
- Bel Bridge, Web Admin, Web Bridge en andere toepassingsservices komen pas terug na het terugzetten.



Tip: Cisco Meeting Server-back-up bevat niet de geheime sleutel van MeetingApps. Na een terugzetbewerking moet u die sleutel opnieuw genereren en toepassen op elk Web Bridge-knooppunt. Zie de sectie MeetingApps Secret Key After Restore.

Maak een back-up wanneer Secure Storage is uitgeschakeld of niet beschikbaar is

Volg deze procedure op virtuele machines, Meeting Server Small en Meeting Server Medium waar secure_storage rapporten Enabled: False, en op Meeting Server 2000 waar Secure Storage niet beschikbaar is.

1. Maak op elk knooppunt een bestand met de opdracht Snapshot back-up. Gebruik de vorige bestandsnaam niet opnieuw.

2. Kopieer het back-upbestand onmiddellijk naar externe opslag met SFTP. Bewaar niet de enige kopie op de vergaderserver.

3. Sla het bestand op een locatie op die nog steeds bereikbaar is als de node opnieuw is opgebouwd.

Voorbeeld:

```
backup snapshot cms313SecurestorageFalse backup list
```

4. Bevestig dat het bestand wordt weergegeven in de opdracht van de back-uplijst en breng het vervolgens over naar een externe schijf met een SFTP-client.

5. Herhaal dit proces op elk knooppunt in het cluster. Back-upnamen kunnen alleen letters, cijfers, onderstrepingstekens en koppeltekens bevatten. Neem de bestandsextensie .bak niet op wanneer u een back-upbestand maakt. Een bestandsnaam zoals 3.13SecureStorageFalse wordt bijvoorbeeld geweigerd vanwege de periode.

```
    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>
```

Afbeelding 4: Een back-upmomentopname wijst een naam die een punt bevat af en slaagt vervolgens met een alfanumerieke naam. Het .bak bestand is dan klaar om te downloaden.



Afbeelding 5: Kopieer het .bak-bestand van de SFTP-hoofdmap van de Meeting Server naar externe opslag. Laat de enige kopie niet op de server staan.

Maak een back-up wanneer Secure Storage is ingeschakeld

Gebruik deze procedure wanneer secure_storage rapporten Enabled: True rapporteert. Niet-gecodeerde back-upbestanden kunnen niet worden gedownload.

1. Maak een back-upmomentopname op elk knooppunt. Wanneer Secure Storage is ingeschakeld, vraagt de server om een wachtwoordzin van ten minste 14 tekens. De wachtwoordzin kan letters, cijfers, speciale tekens, symbolen of spaties bevatten.

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

Afbeelding 6: Back-upmomentopname met ingeschakelde Secure Storage-prompts voor een wachtwoordzin van ten minste 14 tekens. De MMP vraagt u niet om dit te bevestigen.

2. Het MMP vraagt u niet om de wachtwoordzin opnieuw in te voeren ter bevestiging. Beveilig uw wachtwoordgroep omdat u dezelfde wachtwoordgroep nodig hebt om het bestand te herstellen. Kies geen triviaal voorbeeld of passphrase.

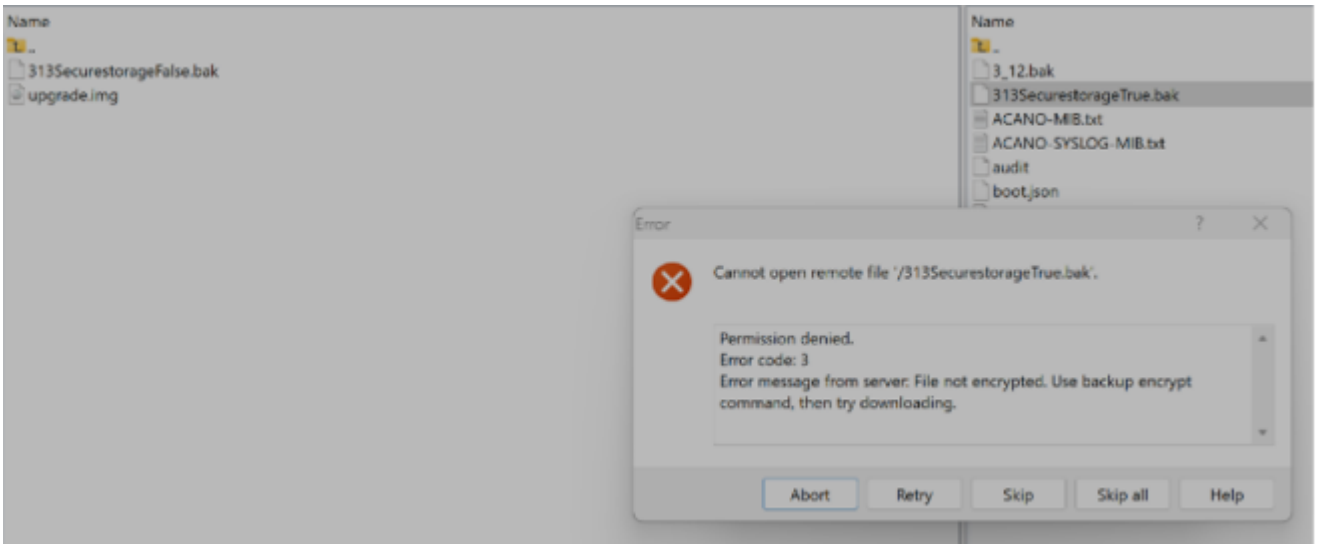
3. Als de opdracht Back-uplijst een momentopname weergeeft die niet is versleuteld voor export,

versleutelt u deze voordat u deze downloadt:

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

Afbeelding 7: Back-uplijst vóór codering. De gecodeerde kolom is niet beschikbaar, dus het bestand kan niet worden gedownload.

4. Als u probeert een niet-gecodeerde back-up te downloaden, geeft SFTP een fout met de toegangsweigering terug en geeft u de opdracht om de opdracht back-upcodering eerst uit te voeren.



Afbeelding 8: SFTP weigert het downloaden van een ongecodeerde back-up wanneer Secure Storage is ingeschakeld. In het serverbericht wordt u geïnstrueerd om back-upcodering uit te voeren.

5. Voer de opdracht Back-upcodering uit om het back-upbestand te coderen.

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

Afbeelding 9: Back-uplijst nadat de momentopname is versleuteld. Gecodeerd is ja en het bestand kan worden overgedragen met SFTP.

In de back-uplijst worden de coderingsstatus en de oorspronkelijke bestandsnaam weergegeven. Zorg ervoor dat u alleen het gecodeerde bestand van elk knooppunt in het cluster overdraagt. Houd een georganiseerd record bij van elk knooppunt, de bijbehorende bestandsnaam en de bijbehorende wachtwoordzin.

Als u ook privésleutels moet exporteren, codeert u eerst elke sleutel. Certificaatbestanden worden

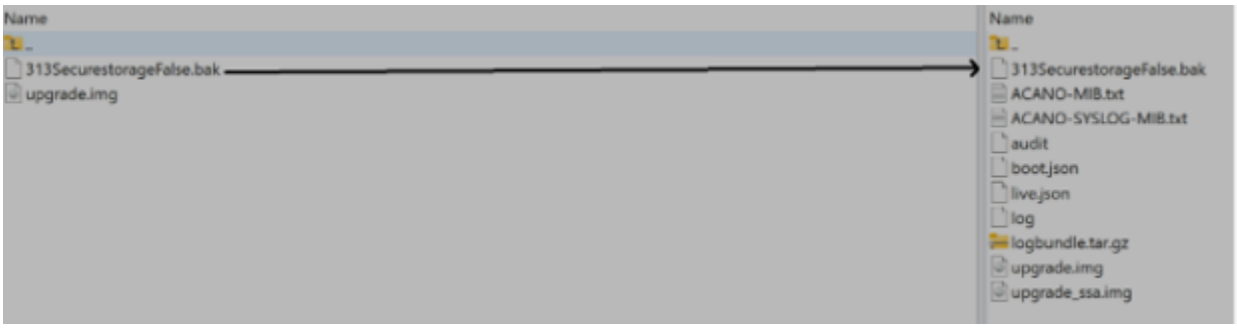
niet geblokkeerd door Secure Storage en kunnen worden gekopieerd zonder deze extra stap:

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

Gebruik een unieke bestandsnaam in plaats van de sleutel te overschrijven die momenteel door services wordt gebruikt. Ook hier geldt het minimum van 14 tekens wachtwoordzin.

Gegevens herstellen na 4.0-upgrade

1. Nadat u zich voor het eerst hebt aangemeld en het netwerk hebt hersteld in de sectie First-boot and Network Restoration, kopieert u de corresponderende 3.13.x-back-up naar de node met SFTP en herstelt u deze.



Afbeelding 10: Kopieer het 3.13.x .bak-bestand na het herstel van het netwerk voor de eerste keer op de 4.0-node met SFTP.

2. Controleer of het bestand aanwezig is:

back-uplijst

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

cms-3120>
```

Afbeelding 11: Back-uplijst op 4.0 die bevestigt dat de geüploade momentopname aanwezig is voordat deze wordt teruggedraaid.

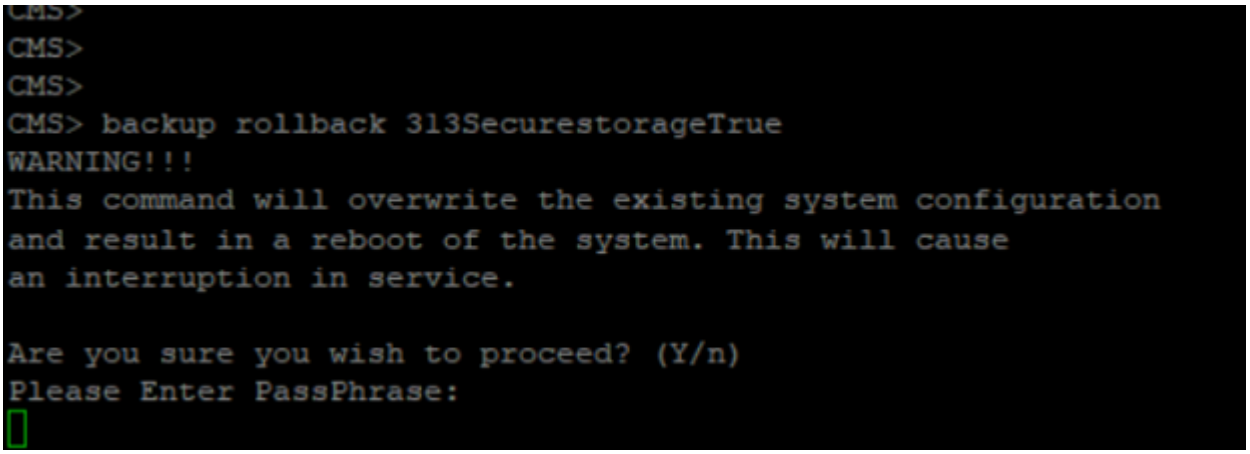
3. Herstel de momentopname. In een clusterimplementatie zet u eerst de voormalige primaire database terug, gevolgd door de replica's en vervolgens de verbonden knooppunten.

```
backup rollback name-of-the-backup-file
```



Afbeelding 12: Back-up terugdraaien van een niet-gecodeerde momentopname. Bevestig met Y; de node haalt de back-up op en start opnieuw op.

4. Druk op Y om door te gaan. Het knooppunt start opnieuw op terwijl het de back-up extraheert. Als de back-up is gemaakt met Secure Storage ingeschakeld, wordt de wachtwoordgroep door de MMP gevraagd. De reboot gaat pas verder nadat de juiste wachtwoordzin is geaccepteerd.



Afbeelding 13: Back-up van een gecodeerde momentopname. Na Y wordt in het MMP gevraagd om de wachtwoordzin die werd gebruikt toen de back-up werd gemaakt.

⚠ Waarschuwing: de **backup rollback** overschrijft de huidige configuratie, certificaten, privésleutels en licentiebestand en start de server opnieuw op. Gebruik het alleen met de 3.13.x-back-up die u voor deze upgrade hebt geëxporteerd.

---

5. Wanneer de node weer online is, meldt u zich aan met de MMP-referenties van de back-up en bevestigt u dat elke vereiste servicerapporten zijn ingeschakeld en actief zijn (de MMP toont dit als actief: true).

Typische controles:

callbridge webbridge3 webadmin scheduler recorder streamer uploader meetingapps

6. Voer alleen de opdrachten uit voor services die deze node moet hosten.

MeetingApps geheime sleutel na herstel

De Cisco Meeting Server-back-up slaat de geheime sleutel van MeetingApps niet op. Nadat de back-up is teruggedraaid, genereert u het geheim en past u het toe op elk Web Bridge-knooppunt. Als u deze stap overslaat, blijft het delen van bestanden onbeschikbaar, hoewel de andere services er gezond uitzien.

1. Voer op het knooppunt MeetingApps de opdracht MeetingApps gensecret uit.

2. Kopieer het gegenereerde geheim naar uw geheime winkel. Elke uitvoering van vergaderapps maakt de vorige sleutel ongeldig, dus genereer de sleutel eenmaal en hergebruik dezelfde waarde voor alle webbruggen.

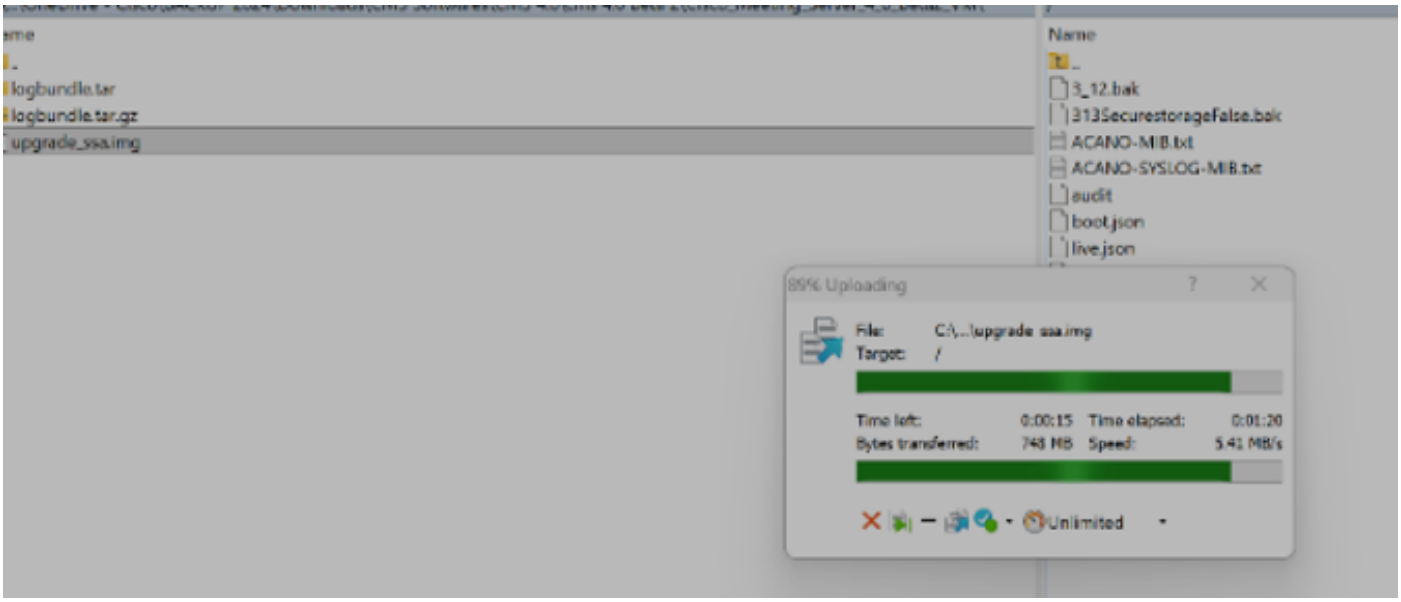
3. Voer deze opdrachten uit op elk Web Bridge-knooppunt:

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

De laatste opdracht bevestigt dat de Web Bridge-service actief is en dat de MeetingApps correct is geconfigureerd. MeetingApps wordt niet ondersteund op Meeting Server 2000 en het delen van bestanden is niet beschikbaar in clusters met een Meeting Server 2000. Bij dergelijke implementaties is deze stap niet van toepassing.

Eerste opstart en netwerkherstel

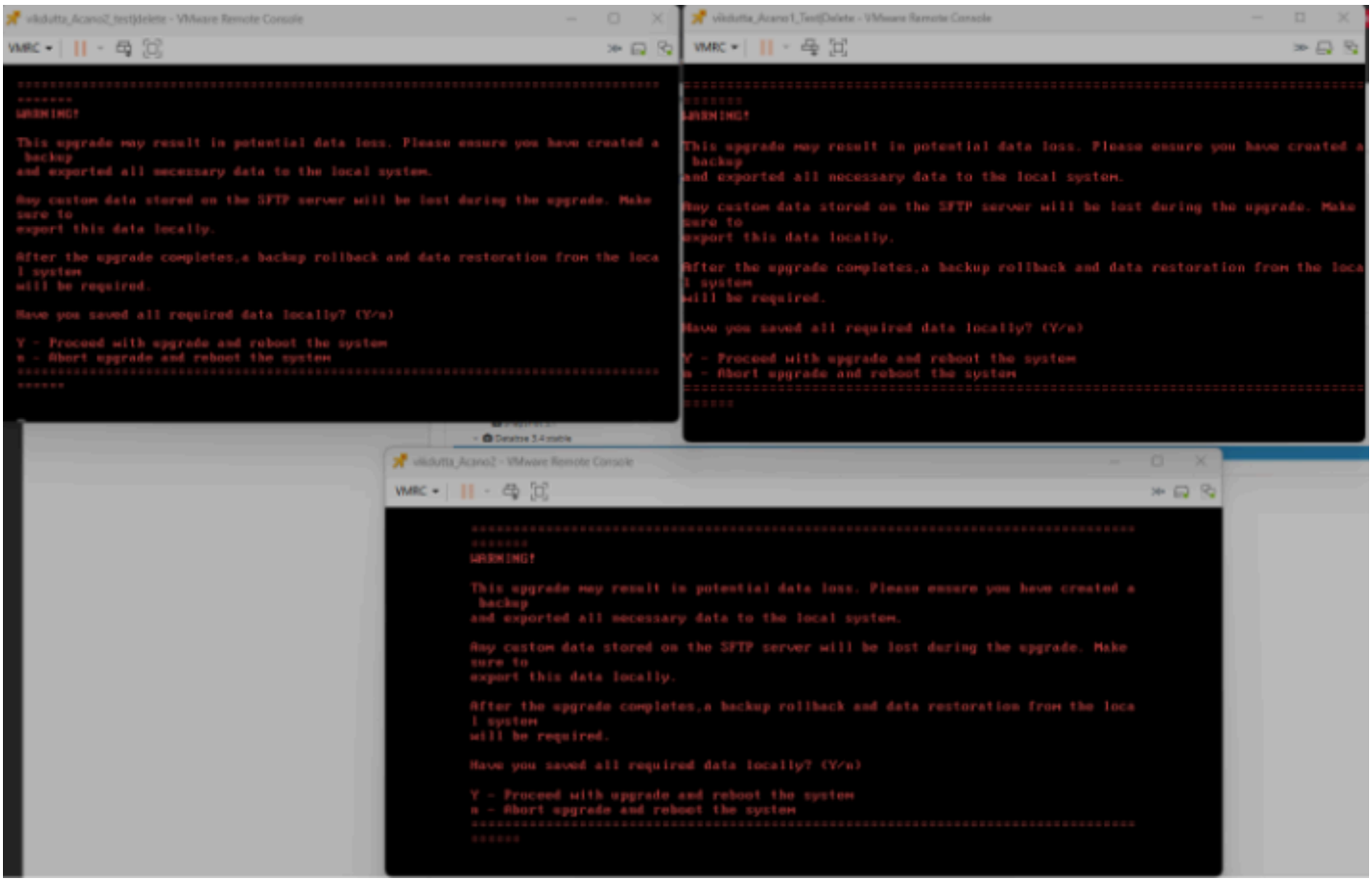
De 4.0-upgrade-opdracht geeft een waarschuwingsbanner weer voordat deze wordt uitgevoerd. Lees het bericht zorgvuldig door en aborteer met n als er geen vereisten zijn. Als u doorgaat met Y, wordt de node opnieuw opgestart, wordt de SSH-sessie verbroken en moeten de resterende stappen vanaf de console worden voltooid.



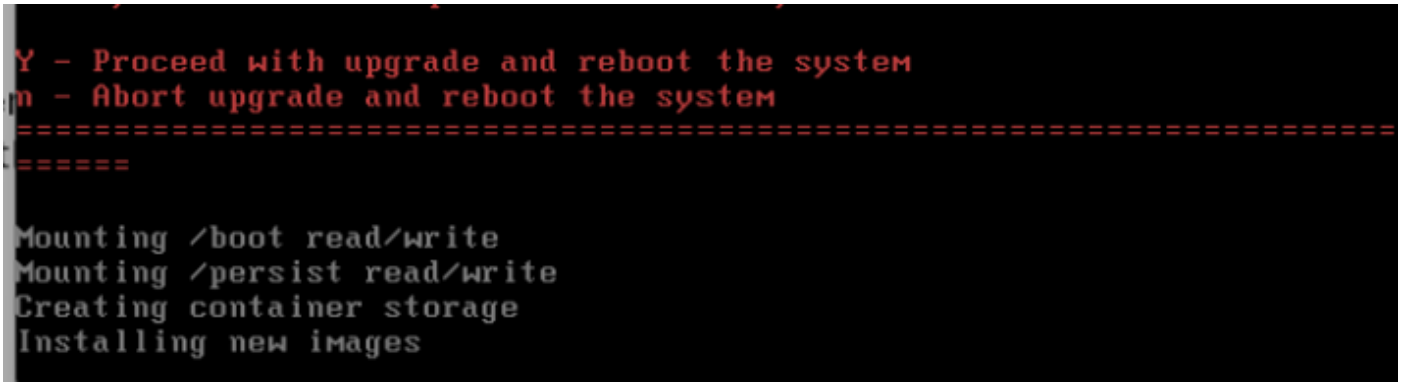
Afbeelding 14: Upload het 4.0-upgradeimage naar de hoofddirectory van Meeting Server SFTP. De bestandsnaam van het upgradeimage kan variëren afhankelijk van het pakket dat is gedownload van cisco.com.

```
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...
```

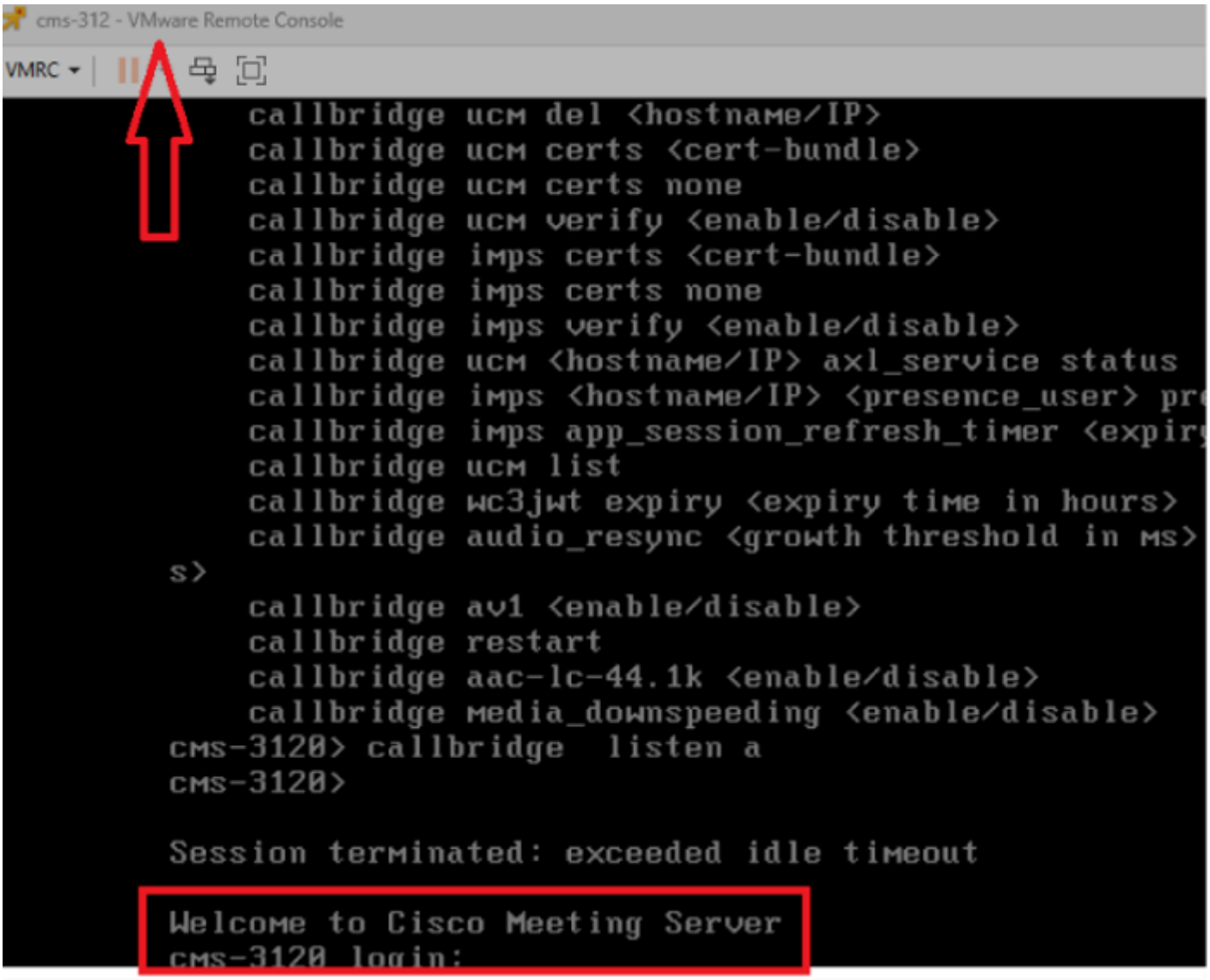
Afbeelding 15: met de opdracht Upgrade wordt de handtekening van het image gecontroleerd en wordt het proces gestart. Vertrouw niet op de automatische back-up die op dit moment wordt gemaakt.



Figuur 16: De rode MMP-waarschuwing op een cluster met drie knooppunten. Dezelfde banner verschijnt op een enkele node. Druk op n om af te breken als back-ups en aangepaste gegevens niet van de server zijn verwijderd. Druk alleen op Y om verder te gaan en opnieuw op te starten.



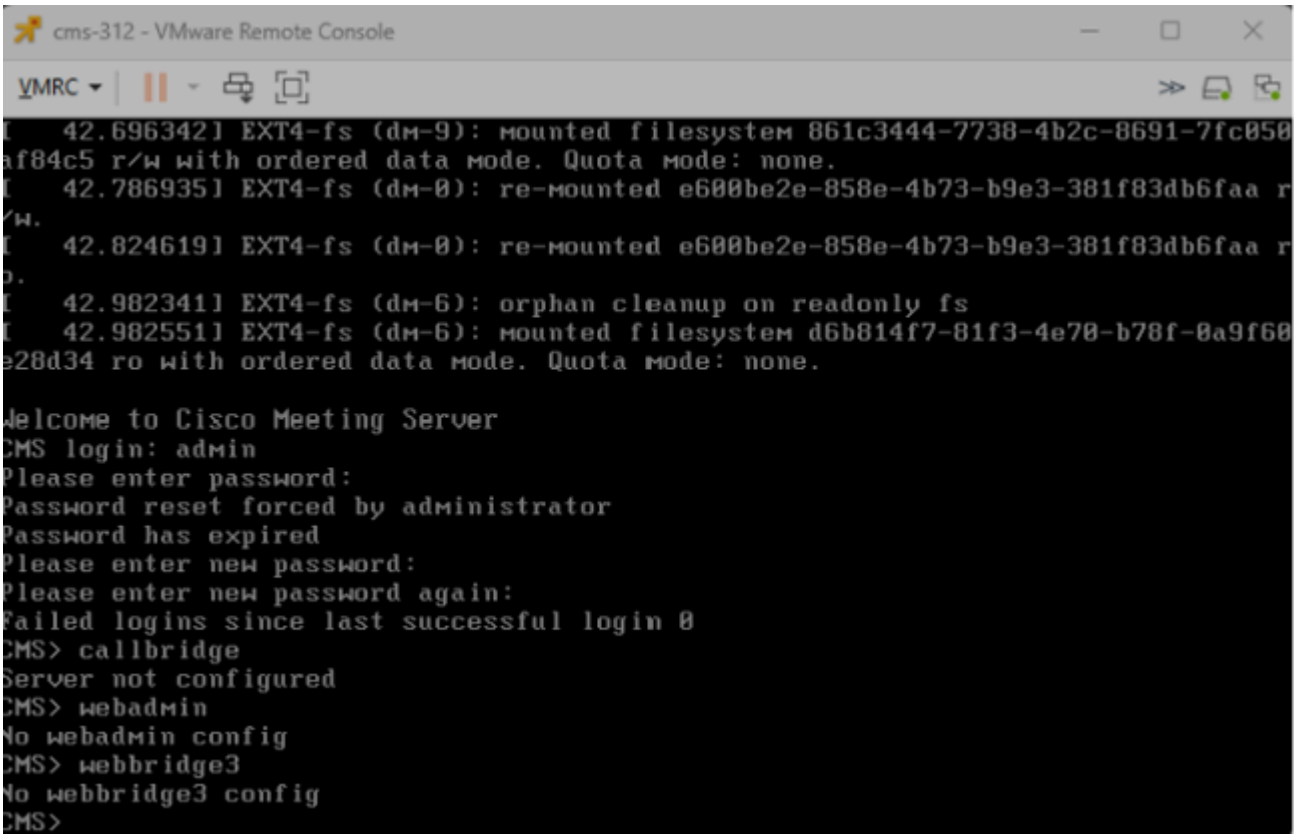
Afbeelding 17: Na Y koppelt het knooppunt de opslag en installeert het 4.0-image. De SSH-sessie wordt onderbroken; ga verder vanaf de hypervisorconsole.



Afbeelding 18: Gebruik de VM- of CIMC-console nadat SSH is gevallen. De eerste aanmeldingsprompt voor het opstarten wordt weergegeven wanneer het 4.0-image gereed is.

1. Log in met de MMP-account voor het eerst opstarten (gebruikersnaam admin en geen wachtwoord) en stel vervolgens een nieuw MMP-wachtwoord in wanneer daarom wordt gevraagd. Merk op dat het terugdraaien van de back-up dit wachtwoord vervangt door het wachtwoord dat in de back-up is opgeslagen.

2. Pas de netwerkconfiguratie opnieuw toe op basis van de opmerkingen die u hebt vastgelegd in de sectie Voorafgaande vereisten voor upgrades:



Afbeelding 19: MMP-aanmelding voor eerste opstart.

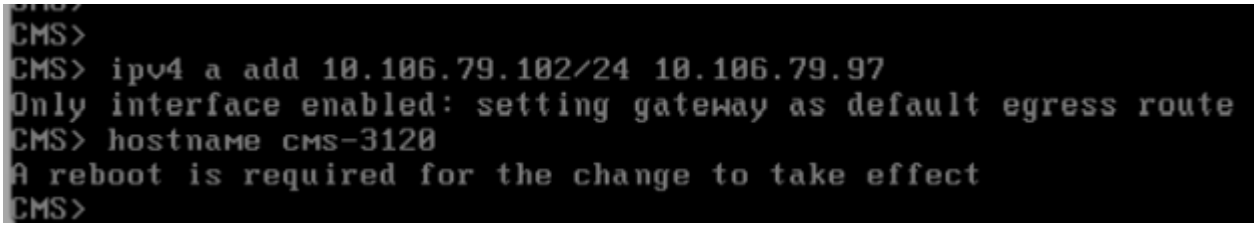
Het vorige wachtwoord is niet meer geldig. Nadat u een nieuw wachtwoord hebt ingesteld, worden services zoals webadmin en webbridge3 niet meer als geconfigureerd weergegeven totdat de back-up is hersteld.

3. Voer het commando uit:

ipv4 interface add address/prefix-length gateway

Voorbeeld:

ipv4 a add 192.0.2.10/24 192.0.2.1



Afbeelding 20: IPv4 opnieuw toepassen vanaf de console.

Een reboot is vereist nadat u het adres hebt toegewezen. De adressen die in de screenshot

worden weergegeven, zijn alleen voor bijvoorbeeld doeleinden.

4. Start opnieuw op nadat het adres is toegewezen. Als het systeem weer online is, gaat u verder met het uploaden van de back-up via SFTP en de stappen voor terugzetten die worden genoemd in het gedeelte Gegevens terugzetten na 4.0-upgrade.

Opmerking: als een DHCP-reservering is geconfigureerd, kan het oorspronkelijke adres al worden toegewezen na het opnieuw opstarten. Controleer het adres met **ipv4 a** voordat u een SFTP-sessie start vanaf uw beheerwerkstation.

Op Cisco Meeting Server 4.0 is Secure Storage standaard ingeschakeld op platforms die het ondersteunen. De MMP kan secure_storage na de upgrade niet langer als een schakelaar blootleggen.



Afbeelding 21: In dit 4.0-image wordt de opdracht secure_storage niet herkend omdat Secure Storage standaard is ingeschakeld.

Bevestig de release met de opdracht versie.

Upgradescenario's

Dit hoofdstuk behandelt verschillende upgradescenario's. Voltooi de stap upgrade naar 3.13.x. Identificeer uw implementatietype en kies het scenario dienovereenkomstig. Volg alleen de procedure die overeenkomt met uw omgeving en combineer geen stappen van cluster- en single node-implementaties.

Voltooi eerst de ondersteunde stap-upgrade naar 3.13.x. Selecteer vervolgens precies één scenario hieronder. Combineer de single-node- en database-clusterprocedures niet.

- Scenario 1: Single node, uitgeschakeld of niet beschikbaar, VM, Small, Medium en Meeting Server 2000
- Scenario 2: Alleen één knooppunt, ingeschakeld, VM, klein en gemiddeld
- Scenario 3: Databasecluster, Uitgeschakeld of niet beschikbaar, VM, Small, Medium en Meeting Server 2000

- Scenario 4: alleen databasecluster, ingeschakeld, VM, klein en gemiddeld

Meeting Server 2000 biedt geen ondersteuning voor scenario's die zijn ingeschakeld voor Secure Storage. Gebruik voor dat platform scenario 1 of 3, indien van toepassing.

Scenario 1 - Single Node met beveiligde opslag uitgeschakeld of niet beschikbaar

Gebruik deze procedure voor een standalone server met Secure Storage uitgeschakeld of Meeting Server 2000 waar Secure Storage niet beschikbaar is. De bronversie kan 3.11.x of hoger zijn, maar de node moet op 3.13.x zijn voordat u naar 4.0 kunt upgraden.

1. Stap-upgrade naar 3.13.x. Volg het ondersteunde pad (bijvoorbeeld 3.11.x → 3.12.x → 3.13.x). Bevestig na elke hop de versie in Webbeheer en controleer of de foutcondities duidelijk zijn, zoals beschreven in het gedeelte Servergezondheid valideren voordat u back-ups maakt.

2. Bevestig de status van de beveiligde opslag. Voer de opdracht secure_storage uit en controleer of Secure Storage niet is ingeschakeld. Sla de opdracht over op Meeting Server 2000.

3. Maak en exporteer een 3.13.x-back-upbestand zoals vermeld in het gedeelte Back-up maken wanneer beveiligde opslag is uitgeschakeld of niet beschikbaar is. Exporteer ook aangepaste SFTP-inhoud en de logbundel zoals vermeld in de sectie Voorafgaande vereisten voor upgrades.

4. Download de 4.0-softwareafbeelding van Cisco.com, haal deze eruit en kopieer upgrade.img naar de node via SFTP.

5. Start de upgrade met deze opdracht:

```
upgrade upgrade.img
```

6. Lees de waarschuwingsbanner. Druk alleen op Y nadat alle voorwaarden zijn vervuld. 6. Configureer na de upgrade het knooppunt zoals beschreven in het gedeelte Eerste opstart en netwerkherstel en herstel de back-up vervolgens met behulp van het gedeelte Gegevens herstellen na upgrade 4.0.

Scenario 2 - Single Node met veilige opslag ingeschakeld

Gebruik deze procedure voor een zelfstandige VM, Small Meeting Server of Meeting Server Medium waarbij Secure Storage is ingeschakeld. Het is niet van toepassing op Meeting Server

2000.

Voordat u bestanden van de server overbrengt, moet u er rekening mee houden dat niet-versleutelde privésleutels en niet-versleutelde back-upbestanden niet kunnen worden overgedragen. Certificaatbestanden worden niet geblokkeerd.

1. Upgrade via het ondersteunde pad naar 3.13.x zonder releases over te slaan. Bevestig na elke hop de versie en controleer of de foutcondities duidelijk zijn in het gedeelte Servergezondheid valideren voordat u back-ups maakt.

2. Voer secure_storage uit en bevestig dat de uitvoer Enabled: True toont.

3. Maak en exporteer een gecodeerde 3.13.x-back-up met behulp van de sectie Een back-up maken wanneer beveiligde opslag is ingeschakeld. Bewaar de wachtwoordzin in uw geheime winkel. Exporteer ook aangepaste SFTP-inhoud en de logbundel (sectie Vereisten voor pre-upgrade).

4. Kopieer upgrade.img naar de node en voer de upgrade uit:

```
upgrade upgrade.img
```

5. Lees de waarschuwingsbanner en druk op Y om alleen door te gaan wanneer de vereisten zijn vervuld.

6. Herstel het netwerk van de console (sectie First-boot en Network Restoration) en herstel vervolgens de gecodeerde back-up met de bijbehorende wachtwoordgroep (sectie Gegevens herstellen na upgrade 4.0). 6. Als MeetingApps in gebruik is, past u een nieuw MeetingApps-geheim toe (sectie MeetingApps Secret Key After Restore).

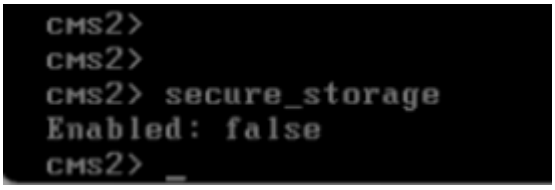
Secure Storage is standaard ingeschakeld op Meeting Server 4.0. Na een terugzetbewerking blijft u privé-sleutels en back-upbestanden als gecodeerde gegevens verwerken.

Scenario 3 - Databasecluster met beveiligde opslag uitgeschakeld

Gebruik deze procedure voor een databasecluster met Secure Storage uitgeschakeld, dat een cluster bevat dat Meeting Server 2000 bevat. Vanaf versie 3.5 moet het databasecluster worden opgeheven voordat de software-upgrade wordt uitgevoerd. Ten eerste, stap-upgrade elke node naar 3.13.x.

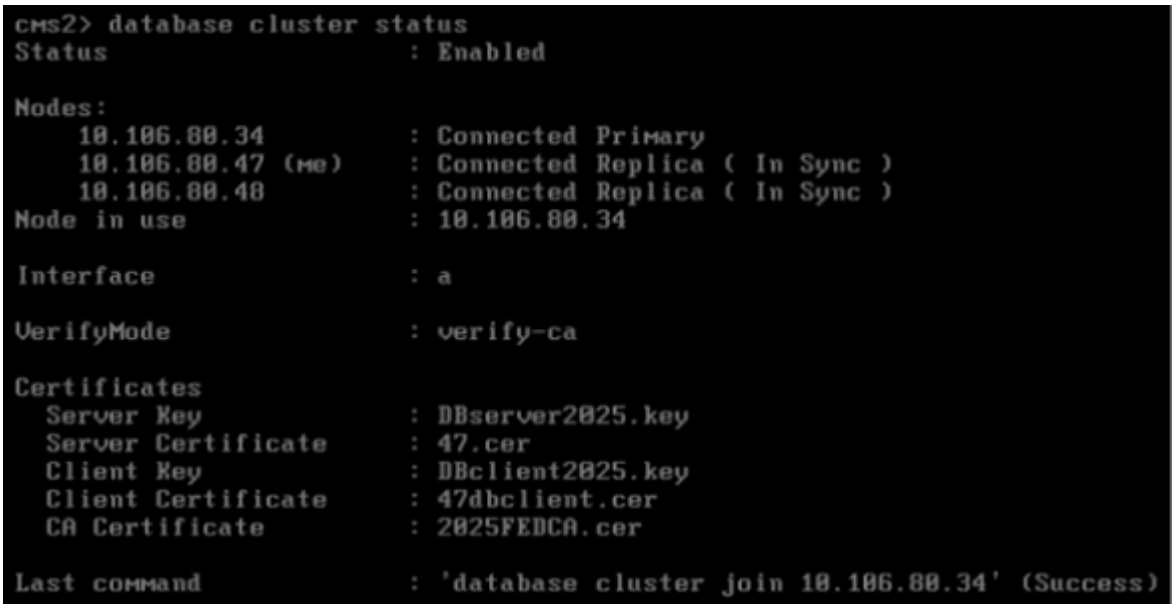
Clusterdetails opnemen en back-ups maken van elk knooppunt

1. Voer secure_storage uit op elk knooppunt. Behandel de opdracht als niet beschikbaar op Meeting Server 2000-knooppunten.



Afbeelding 22: Controleer of Secure Storage is uitgeschakeld op elk clusterknooppunt voordat u niet-versleutelde back-ups gebruikt. Sla de opdracht over voor Meeting Server 2000-knooppunten, waar deze niet beschikbaar is.

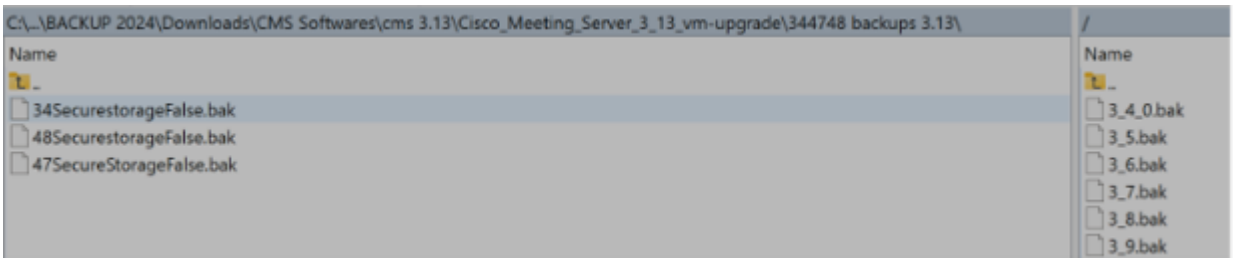
2. Noteer het huidige primaire knooppunt voor de database, aangezien dit eerst na de upgrade naar 4.0 moet worden teruggezet. Bevestig dat replica's in Sync zijn en dat de clusterstatus gezond is.



Figuur 23: Noteer de huidige primaire en bevestig replica's zijn in Sync.

3. Bevestig dat alle gebruikte oproeptypen werken en dat de foutcondities op elk knooppunt duidelijk zijn (sectie Servergezondheid valideren voordat back-ups worden gemaakt).

4. Maak een back-up van elk knooppunt met behulp van de sectie Een back-up maken wanneer beveiligde opslag is uitgeschakeld of niet beschikbaar is. Geef elk bestand een naam zodat het duidelijk wordt toegewezen aan de node en breng elke back-up over naar externe opslag voordat u het cluster ontbindt.



Afbeelding 24: Alle drie de voorbeeldknooppuntback-ups hebben externe opslag opgeslagen, zodat elk bestand wordt toegewezen aan zijn knooppunt.

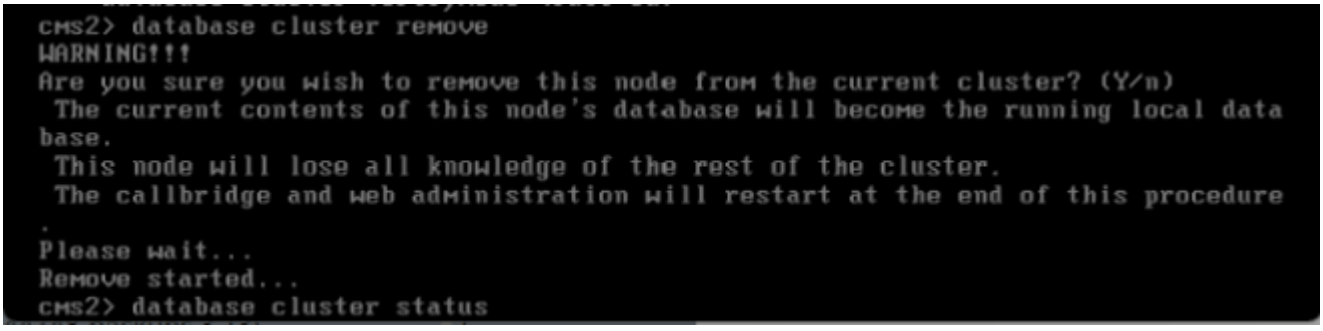
De cluster ontbinden

Verwijder knooppunten in deze volgorde. Houd de primaire tot de laatste:

- Verbonden (niet-core) Meeting Server-nodes
- Replica van databaseknooppunten
- Primaire database node

Voer op elk knooppunt de verwijderingsopdracht uit en druk op Y. Ga niet door met de 4.0-upgrade totdat elk knooppunt meldt dat het het cluster heeft verlaten. Als het clusterlidmaatschap wordt verwijderd, blijft de lokale database van dat knooppunt op zijn plaats.

database cluster remove



Figuur 25: Bevestig Y op een replica om clusterlidmaatschap te verwijderen. De lokale database van het knooppunt blijft op zijn plaats.

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

Interface               : a

VerifyMode              : verify-ca
```

Afbeelding 26: Controleer na verwijdering of de clusterstatus is uitgeschakeld en de gebruikte node Geen is op die node.

```
cms1> database cluster status
Status                  : Enabled

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

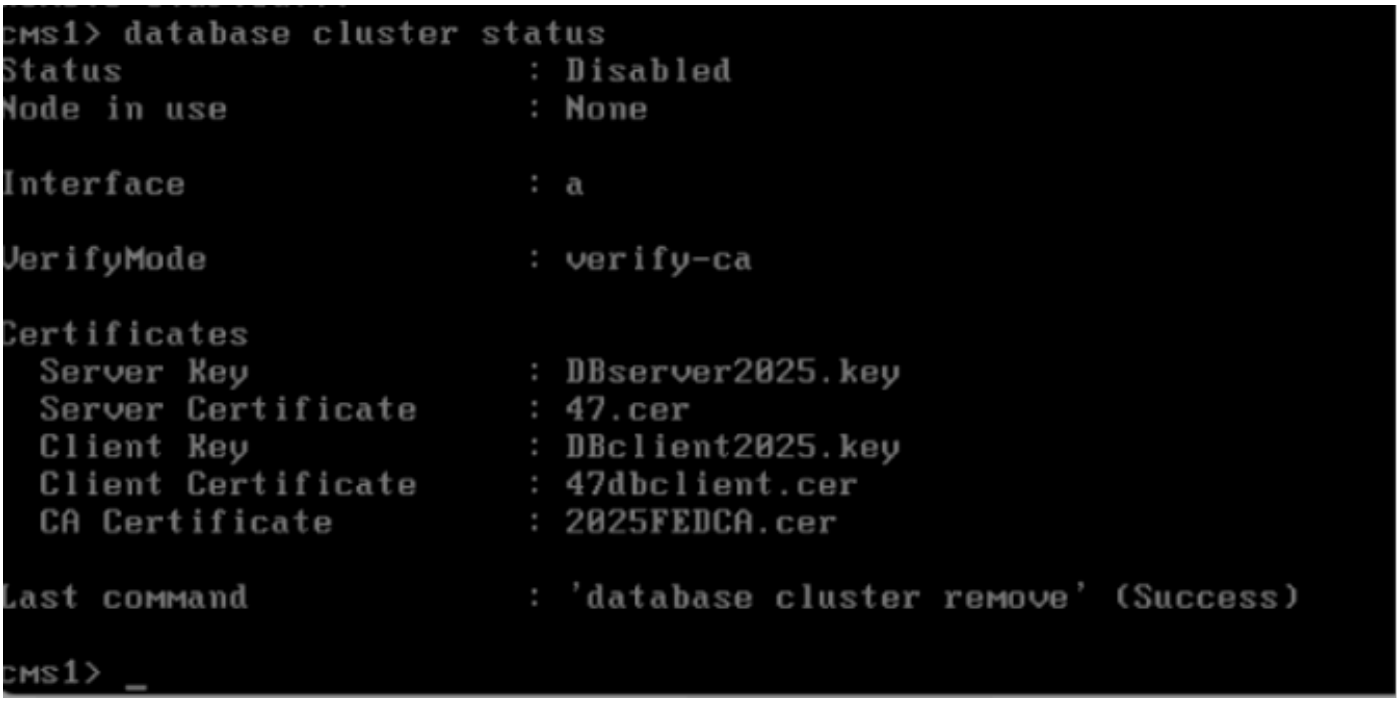
Interface               : a

VerifyMode              : verify-ca

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

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

Afbeelding 27: Nadat de replica's zijn verwijderd, is het voormalige primaire knooppunt het enige knooppunt dat nog in het cluster aanwezig is. Verwijder het als laatste.



Afbeelding 28: Controleer na het verwijderen van de voormalige primaire map of de opdracht meldt dat de clusterstatus is uitgeschakeld.

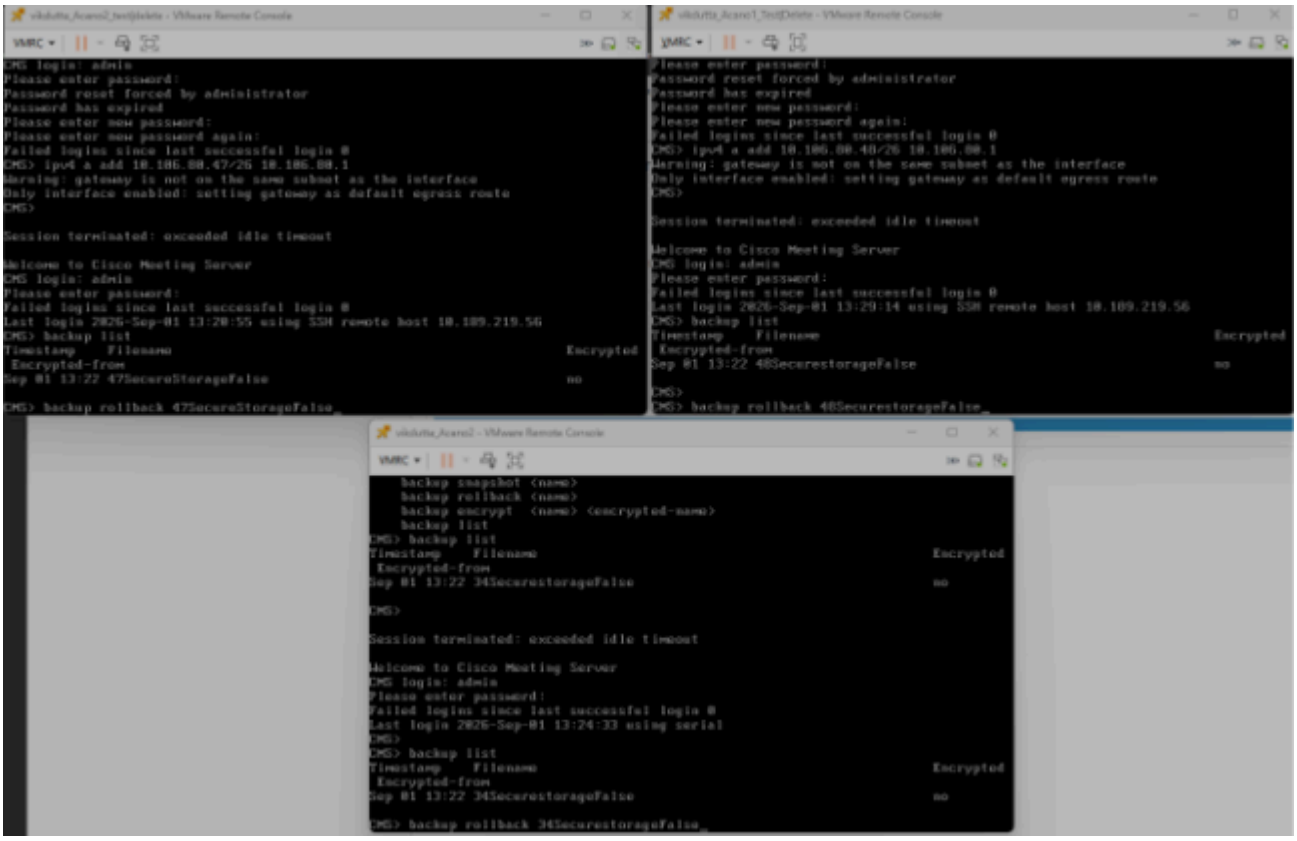
Upgrade en herstel de nodes

1. Eenmaal ontbonden, zijn de knooppunten standalone en kunnen parallel worden opgewaardeerd. Kopieer upgrade.img over SFTP op elk knooppunt en voer de opdracht upgrade uit:

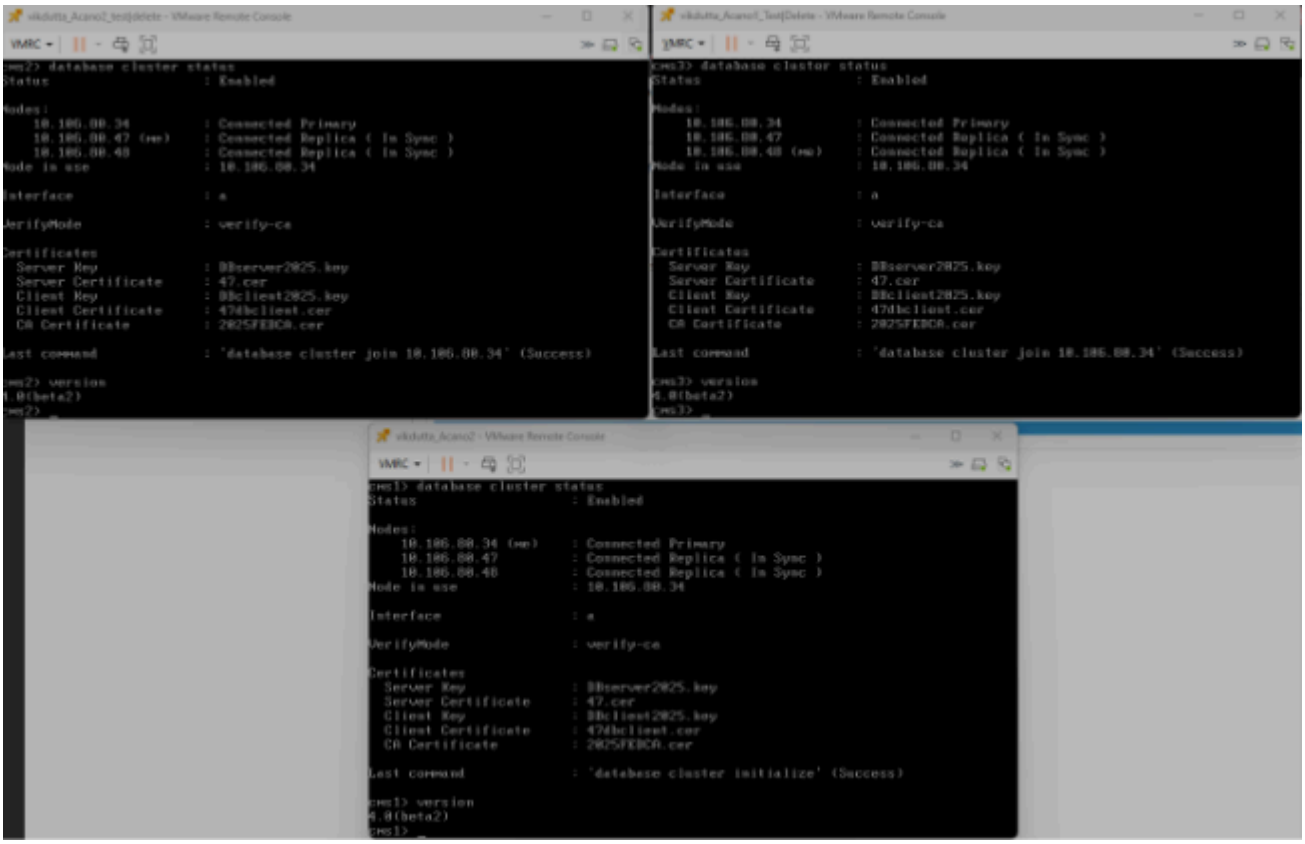
upgrade upgrade.img

2. Herstel het netwerkadres van elke node van de console (sectie Eerste opstart en netwerkherstel).

3. Kopieer de eigen 3.13.x-back-up van elk knooppunt naar dat knooppunt. Herstel eerst de voormalige primaire, gevolgd door de replica's en vervolgens de verbonden knooppunten. Gebruik de sectie Gegevens herstellen na 4.0-upgrade. Bij het terugzetten van de back-ups wordt het database-clusterlidmaatschap opnieuw ingesteld.

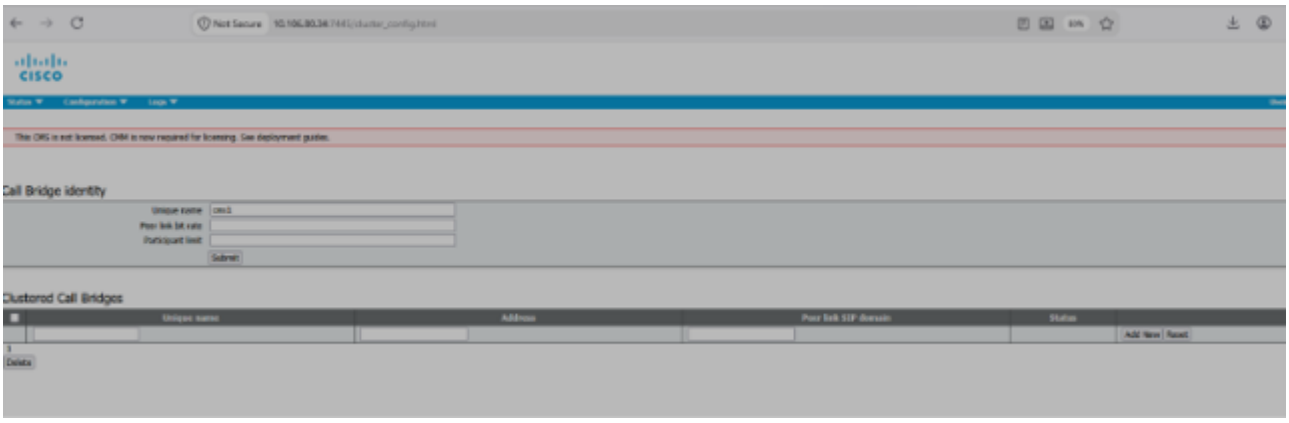


Afbeelding 29: De eigen momentopname van elk knooppunt herstellen. Begin met de voormalige primaire en herstel vervolgens de replica's. Voorbeeldbestandsnamen identificeren hun node.



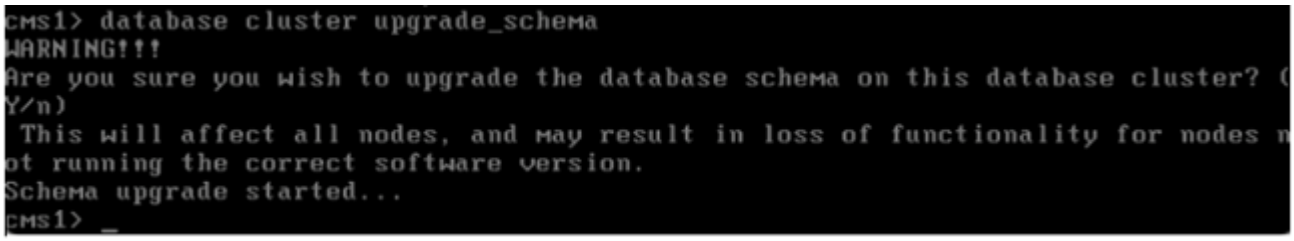
Afbeelding 30: Controleer na terugzetten op Meeting Server 4.0 of het cluster is ingeschakeld, dezelfde primaire server wordt weergegeven en of replica's zijn gesynchroniseerd.

Opmerking: Als er na deze terugzetbewerking geen clusterverbindingen met de oproepbrug worden gemaakt, voert u de **database cluster upgrade_schema** alleen uit op de voormalige primaire en controleert u de status van de oproepbrug opnieuw.

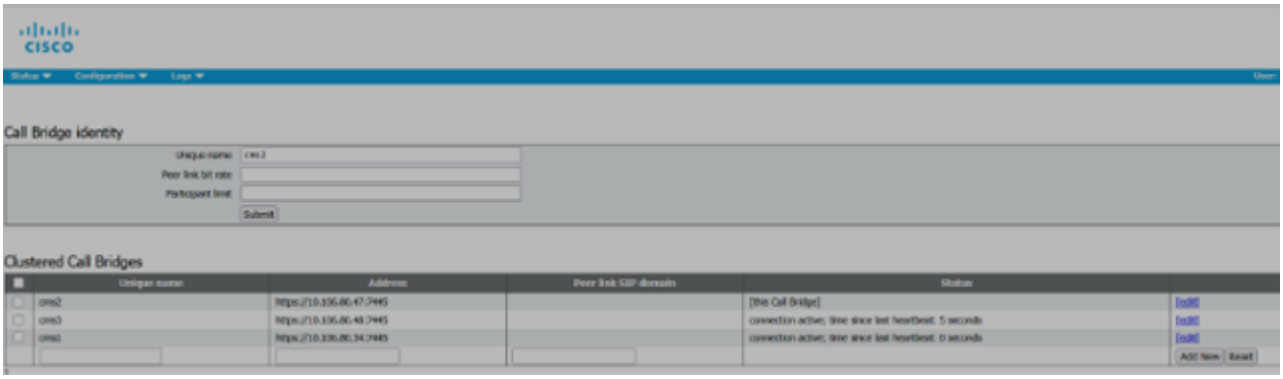


Afbeelding 31: Vóór de upgrade van het schema wordt in het voorbeeld het databasecluster weergegeven dat wordt uitgevoerd terwijl de geclusterde oproepbruggen leeg zijn.

database cluster upgrade_schema



Afbeelding 32: Bevestig Y alleen op de voormalige primaire locatie wanneer de clusterverbindingen van de oproepbrug zijn mislukt na deze upgrade van het cluster met opgeheven capaciteit.



Afbeelding 33: Controleer na de schema-upgrade of elke Call Bridge-peer een actieve verbinding toont.

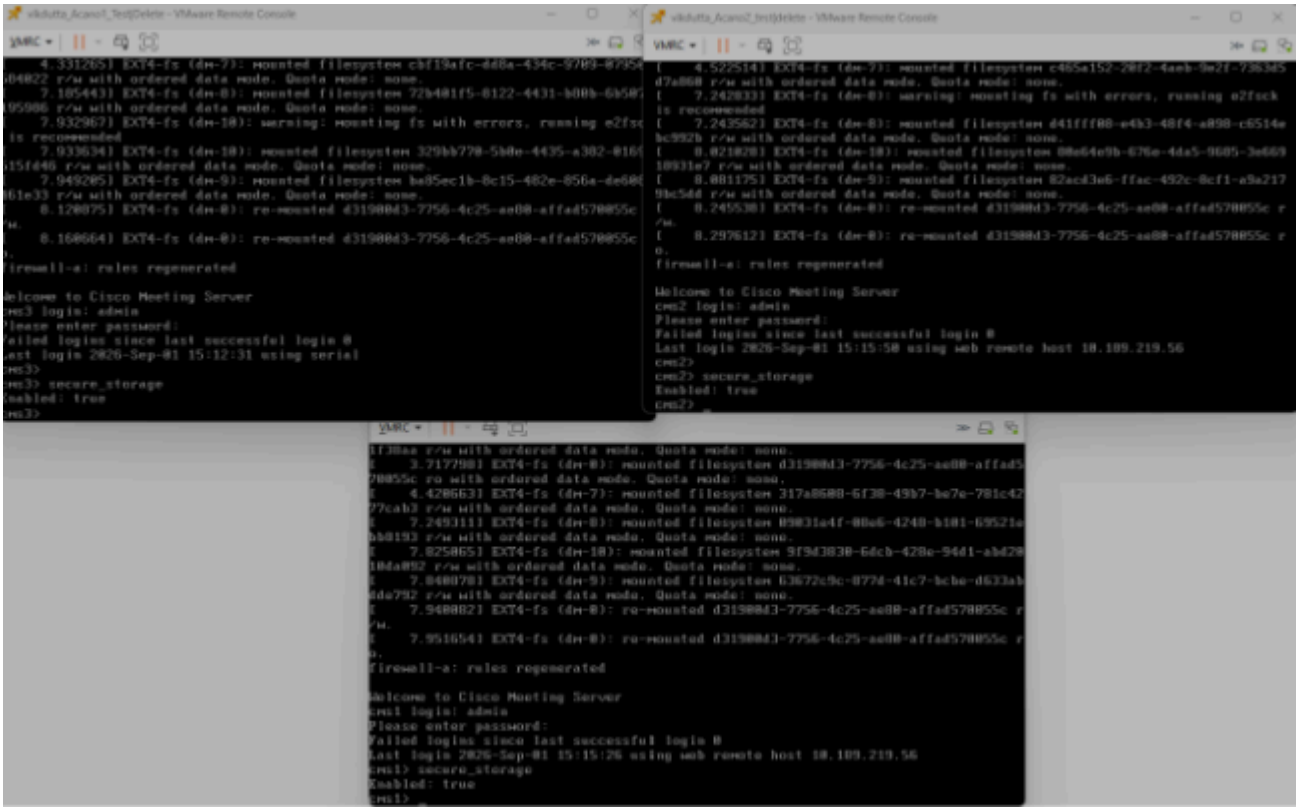
4. Voltooi de geheime procedure van MeetingApps in de sectie MeetingApps Secret Key After Restore op elke webbrug en valideer de implementatie vervolgens met behulp van de sectie Post-upgrade Validation.

Scenario 4 - Databasecluster met beveiligde opslag ingeschakeld

Gebruik deze procedure voor een databasecluster op VM's, Small Meeting Server of Medium Meeting Server waar Secure Storage is ingeschakeld op de knooppunten. Het is niet van toepassing op Meeting Server 2000. Ten eerste, stap-upgrade elke node naar 3.13.x.

Clustergegevens opnemen en gecodeerde back-ups maken

1. Voer secure_storage uit op elk knooppunt en bevestig Enabled: True.



Afbeelding 34: Bevestig voor het geïllustreerde cluster met drie knooppunten dat Secure Storage shows Enabled: True op elk knooppunt wordt weergegeven voordat een upgrade wordt uitgevoerd.

2. Noteer de huidige primaire database en bevestig dat replica's in Sync zijn.

```
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

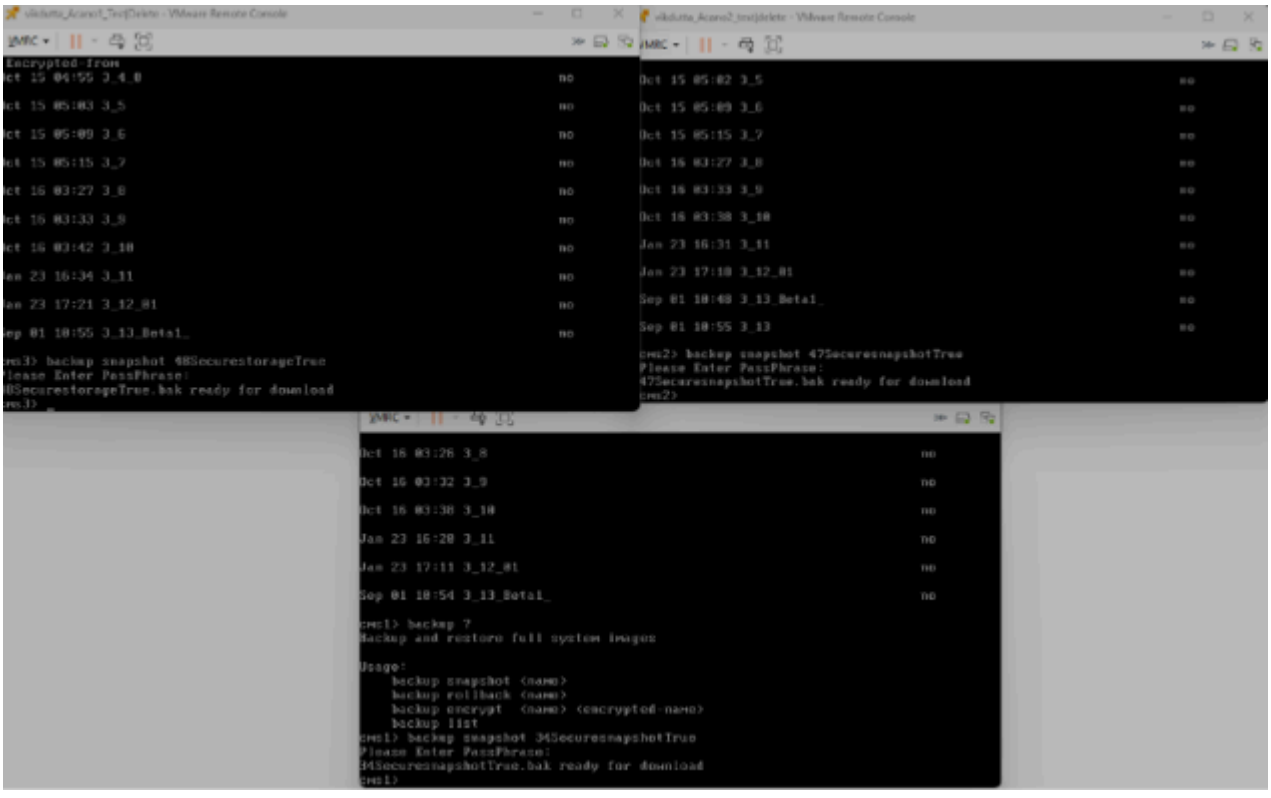
Certificates
  Server Key              : DBserver2025.key
  Server Certificate      : 47.cer
  Client Key              : DBclient2025.key
  Client Certificate      : 47dbclient.cer
  CA Certificate          : 2025FEDCA.cer

Last command              : 'database cluster join 10.106.80.34' (Success)
```

Afbeelding 35: Databaseclusterstatus vóór de upgrade. Noteer de primaire replica's en bevestig dat deze in Sync zijn.

3. Bevestig dat alle aanroeptypen in gebruik zijn en dat de foutcondities op elk knooppunt duidelijk zijn (sectie Servergezondheid valideren voordat back-ups worden gemaakt).

4. Maak een gecodeerde back-up van elk knooppunt met behulp van de sectie Een back-up maken wanneer beveiligde opslag is ingeschakeld. Wijs een unieke wachtwoordzin toe en neem deze op voor elk bestand of gebruik een gedocumenteerd wachtwoordbeleid. Verplaats alleen gecodeerde bestanden van de servers voordat u het cluster ontbindt.



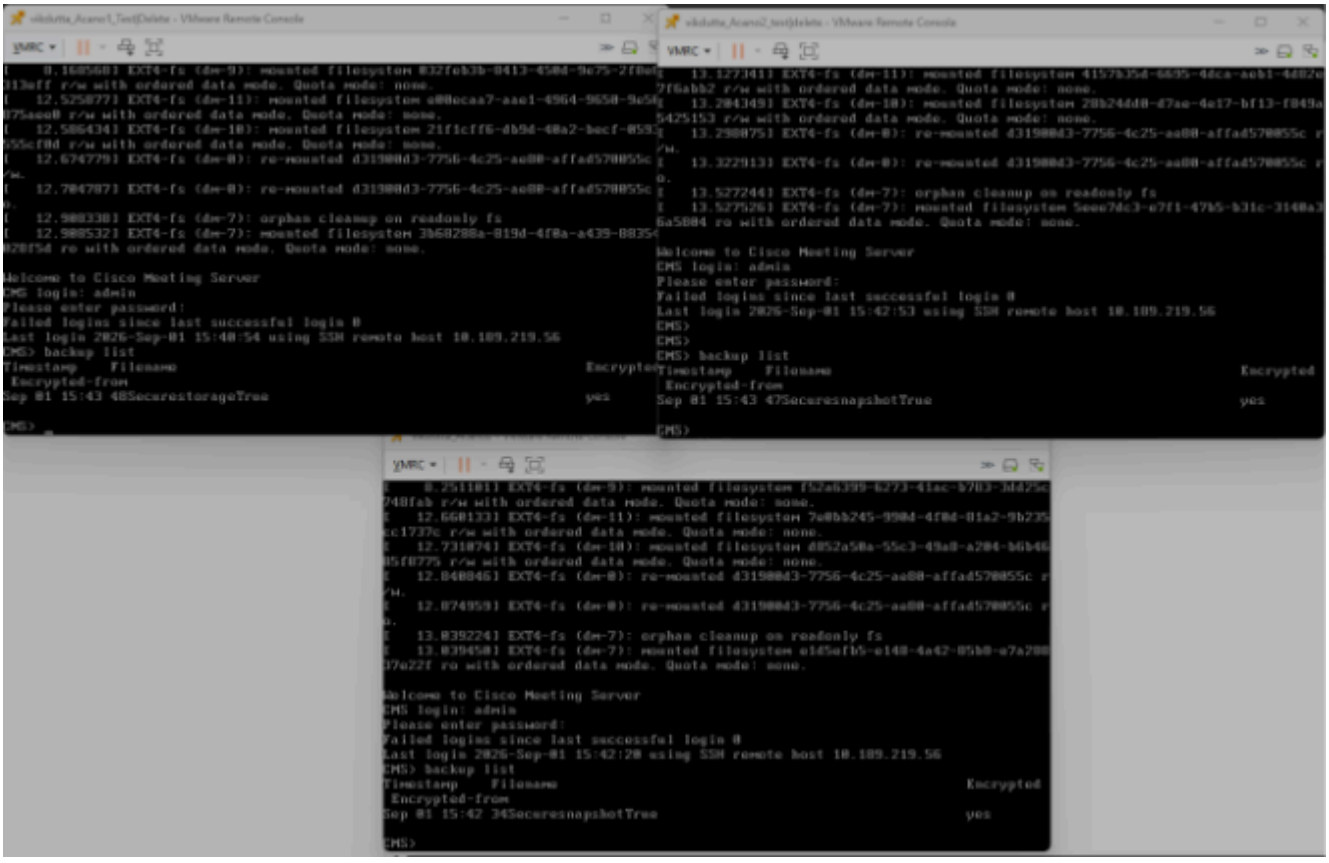
Afbeelding 36: Versleutelde back-upmomentopname op elk knooppunt. Het voorbeeld toont de wachtwoordzin prompt en vervolgens elk .bak bestand klaar om te downloaden.

Ontbinding, upgrade en herstel

Ontbind het cluster zoals beschreven in Scenario 3 in deze volgorde: verbonden knooppunten, replica's en de primaire laatste. Gebruik databasecluster verwijderen en bevestig dat elk knooppunt het cluster heeft verlaten.

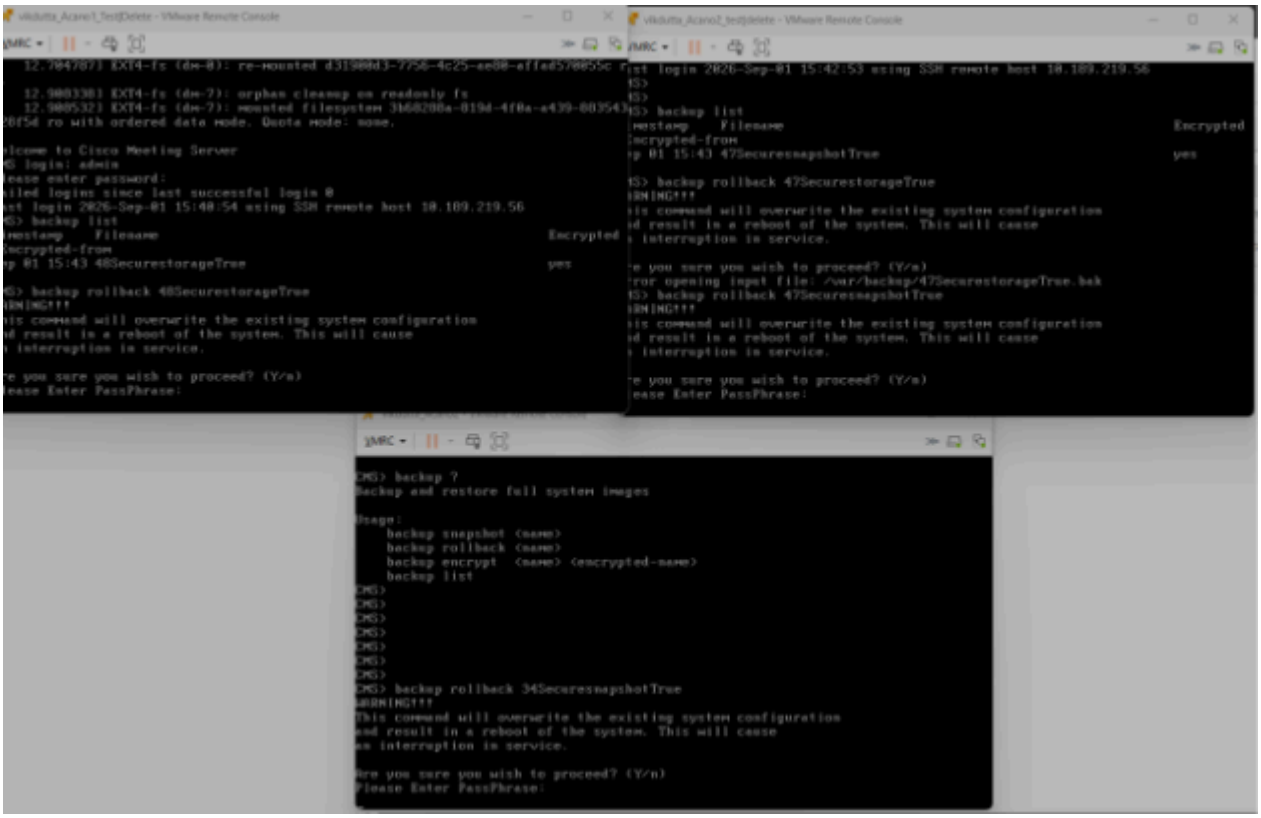
Upgrade de standalone nodes parallel. Netwerkadressen herstellen van de console (sectie Eerste opstart en netwerkherstel).

Upload de eigen gecodeerde back-up van elk knooppunt. Controleer voor een terugdraaiing of de geüploade momentopname in de back-uplijst wordt weergegeven als Gecodeerd: ja. Herstel eerst de voormalige primaire, dan de replica's en verbonden knooppunten. Gebruik de onderstaande back-upopdracht, bevestig Y en voer de wachtwoordzin van de back-up in wanneer daarom wordt gevraagd. De node wordt opnieuw opgestart nadat de wachtwoordzin is geaccepteerd. Herhaal dit voor elk knooppunt.



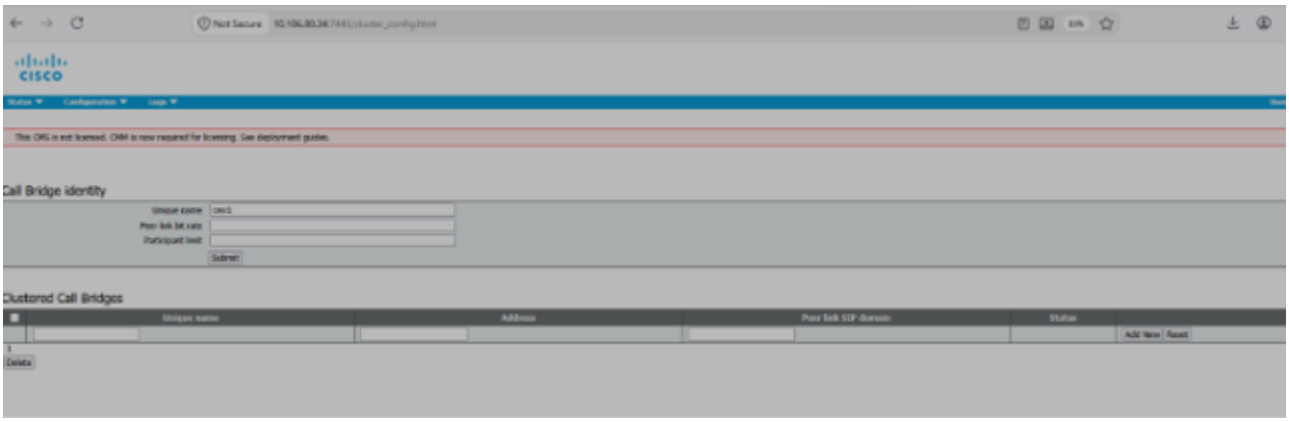
Afbeelding 37: Na de eerste 4.0-opstart moet de geüploade momentopname in de back-uplijst worden weergegeven als Gecodeerd: ja en klaar zijn voor terugdraaiing.

backup rollback encrypted-filename



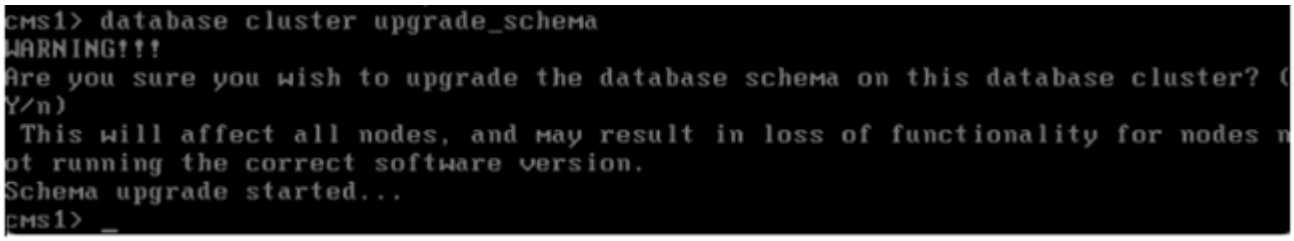
Afbeelding 38: Bevestig Y, voer de wachtwoordzin in en herstel eerst de voormalige primaire.

Opmerking: Als er na deze terugzetbewerking geen clusterverbindingen met de oproepbrug worden gemaakt, voert u de **database cluster upgrade_schema** alleen uit op de voormalige primaire en controleert u de status van de oproepbrug opnieuw.

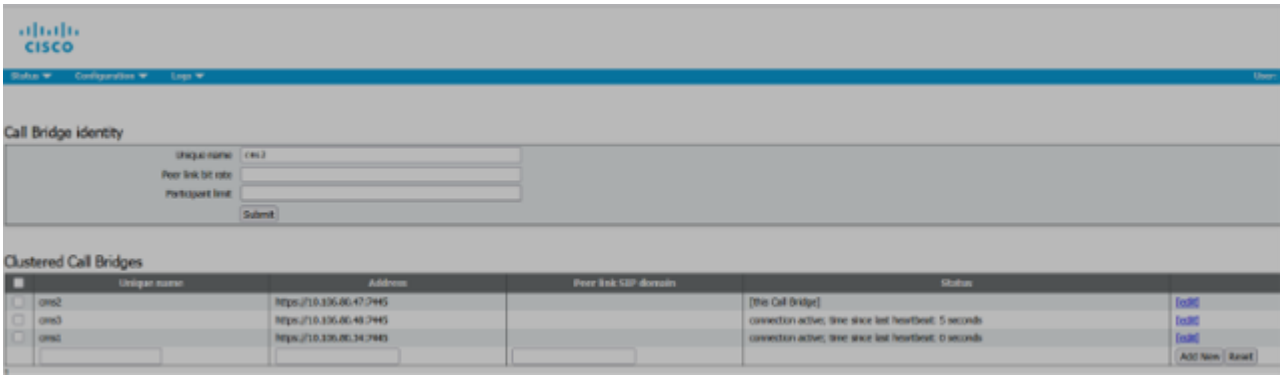


Afbeelding 39: Vóór de upgrade van het schema wordt in het voorbeeld het databasecluster weergegeven dat wordt uitgevoerd terwijl de geclusterde oproepbruggen leeg zijn.

database cluster upgrade_schema



Afbeelding 40: Bevestig Y alleen op de voormalige primaire locatie wanneer de clusterverbindingen van de oproepbrug zijn mislukt na deze upgrade van het cluster met opgeheven capaciteit.



Afbeelding 41: Controleer na de schema-upgrade of elke Call Bridge-peer een actieve verbinding toont.

Voltooi de geheime procedure van MeetingApps in de sectie MeetingApps Secret Key After Restore op elke webbrug en valideer de implementatie vervolgens met behulp van de sectie Post-upgrade Validation.

Validatie na upgrade

Vul deze checklist in na het terugzetten en voordat u het systeem weer in productie neemt:

- Web Admin op elk knooppunt toont Cisco Meeting Server 4.0.
- Vereiste MMP-services zijn ingeschakeld en actief (actief: true).
- De foutcondities zijn duidelijk. Behandel recente fouten en waarschuwingen als informatief, tenzij er een overeenkomstige fout bestaat.
- Indien van toepassing, geeft de databaseclusterstatus de verwachte primaire en replica's weer.
- Smart Licensing en Call Bridge-connectiviteit worden hersteld.
- SIP-oproepen en Web App-clientoproepen die door deze implementatie worden ondersteund, worden met succes voltooid.
- Branding-, audio-prompts- en SSO-bestanden die van de server zijn gekopieerd in de sectie Voorafgaande vereisten worden teruggezet als ze nog niet in de back-up waren opgenomen.
- Als MeetingApps wordt geïmplementeerd, toont Web Bridge de nieuwe MeetingApps-relatie en werkt het delen van bestanden.
- Verwijder kortstondige momentopnamen pas nadat de implementatie is geaccepteerd.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.