Aktualisieren von Meeting Server auf Version 4.0 - Whitepaper

Inhalt

- Einleitung
- Hintergrundinformationen
- Überblick über Secure Storage
  - Unterstützte Plattformen
  - Implementierungshinweise
- Upgrade-Prinzipien und -Einschränkungen
  - Erforderlicher Upgrade-Pfad
  - Herabstufungen
  - Wichtige Backup-Anforderungen für 4.0-Upgrades
  - Konfiguration der ersten Anmeldung und des ersten Kennworts
  - Netzwerkverbindung nach dem Upgrade wiederherstellen
  - Serverzustand vor dem Erstellen von Sicherungen überprüfen
- Anforderungen vor dem Upgrade
- Allgemeine Sicherungs- und Wiederherstellungsverfahren
  - Betroffene Daten nach 4.0-Upgrade
  - Sicherung durchführen, wenn der sichere Speicher deaktiviert oder nicht verfügbar ist
  - Sicherung durchführen, wenn sicherer Speicher aktiviert ist
  - Daten nach 4.0-Upgrade wiederherstellen
  - Geheimschlüssel für MeetingApps nach der Wiederherstellung
- First-Boot und Netzwerkwiederherstellung
- Upgrade-Szenarien
  - Szenario 1 - Einzelner Knoten mit deaktiviertem oder nicht verfügbarem sicheren Speicher
  - Szenario 2 - Einzelner Knoten mit aktivierter sicherer Speicherung
  - Szenario 3 - Datenbank-Cluster mit deaktiviertem sicheren Speicher
    - Clusterdetails aufzeichnen und jeden Knoten sichern
    - Cluster auflösen
    - Knoten aktualisieren und wiederherstellen
  - Szenario 4 - Datenbank-Cluster mit aktivierter sicherer Speicherung
    - Clusterdetails erfassen und verschlüsselte Sicherungen erstellen
    - Auflösung, Upgrade und Wiederherstellung
- Validierung nach dem Upgrade

Einleitung

In diesem Dokument wird das Upgrade von Cisco Meeting Server auf Version 4.0 beschrieben.

Hintergrundinformationen

Verwenden Sie dieses Dokument zusammen mit den Versionshinweisen für Cisco Meeting Server, dem MMP-Befehlsreferenz- und dem Secure Storage Administrator-Referenzhandbuch, um die Anforderungen und Voraussetzungen zu verstehen.

Der Upgrade-Prozess für Cisco Meeting Server 4.0 unterscheidet sich von früheren Versionen, da das Anwenden des Images ein Zurücksetzen des Knotens auf die Werkseinstellungen auslöst. Um die Kontinuität der Services sicherzustellen, müssen alle vorherigen Konfigurationen, einschließlich der Netzwerkeinstellungen und Kennwörter, über ein Backup beibehalten werden, das an einen externen Standort exportiert wird, bevor Sie mit dem Upgrade beginnen.

Darüber hinaus war Secure Storage in den Versionen 3.11 bis 3.13 von Cisco Meeting Server optional, ist jedoch in Version 4.0 standardmäßig aktiviert. Daher müssen Sie andere Sicherungs- und Wiederherstellungsverfahren befolgen, wenn Sie Secure Storage noch nie verwendet haben oder wenn Sie Secure Storage bereits für 3.11x, 3.12x oder 3.13x aktiviert haben.

Secure Storage verschlüsselt private Schlüssel und Backup-Dateien auf dem Server und erfordert, dass diese Dateien verschlüsselt werden, bevor Sie sie auf externen Speicher übertragen können.

In diesem Dokument werden die erforderlichen Anleitungen in einer einzigen Referenz zusammengefasst, sodass Sie für alle Upgrade-Szenarien eine einheitliche Vorgehensweise anwenden können, ohne dieselben Schritte wiederholen zu müssen.

In diesem Dokument werden folgende Themen behandelt:

- Was ist Secure Storage, wo wird sie angewendet, und was bewirkt sie nicht?
- Der Upgrade-Pfad, der die Anforderung enthält, 3.13.x vor 4.0 zu erreichen, und die Tatsache, dass ein Downgrade von 4.0 nicht unterstützt wird.
- Eine gängige Sicherungs- und Wiederherstellungsmethode für Knoten, auf denen Secure Storage aktiviert ist, und für Knoten, auf denen Secure Storage deaktiviert oder nicht verfügbar ist.
- Die Sequenzierung des Datenbankclusterknotens wird aufgelöst, während der Datenbankcluster vor einem Upgrade aufgelöst wird.
- Der geheime Schlüssel für MeetingApps, der nicht in einem Cisco Meeting Server-Backup gespeichert wird und nach einer Wiederherstellung neu generiert werden muss.

Anmerkung: Dieses Dokument verwendet Screenshots aus der Testphase des ursprünglichen Upgrades, einschließlich der Beta-Version 4.0. Alle angezeigten

---

Hostnamen, IP-Adressen und Dateinamen dienen lediglich der Veranschaulichung und spiegeln nicht die tatsächlichen Anmeldeinformationen der Produktionsumgebung oder sensible Passphrasen wider. Um Klarheit zu erhalten und Redundanz zu vermeiden, werden wiederholte Schritte nur einmal im Abschnitt für das allgemeine Verfahren angezeigt, es sei denn, die Clusteransicht bietet zusätzlichen erforderlichen Kontext.

Überblick über Secure Storage

Secure Storage bietet eine verbesserte Datensicherheit, indem vertrauliche Dateien auf dem Meeting Server verschlüsselt werden und kontrolliert wird, wie diese Dateien vom Call Bridge-Server ausgelagert werden. Die Funktion wurde in Cisco Meeting Server 3.11 als konfigurierbare Option mit dem MMP-Befehl secure_storage enable bei Bereitstellungen virtueller Systeme (spezifikationsbasiert oder Meeting Server Small) und auf Meeting Server Medium eingeführt.

Ab Version 4.0 ist Secure Storage standardmäßig aktiviert. Diese Einstellung ist jetzt permanent und irreversibel. Der Befehl secure_storage enable MMP wurde entfernt.

Bei Secure Storage erzwingt der Meeting-Server dieses Verhalten:

- Private Schlüssel können erst über SFTP heruntergeladen werden, wenn sie verschlüsselt sind. Verschlüsseln Sie einen privaten Schlüssel mit dem Befehl pki encrypt MMP, gefolgt von einer Passphrase mit mindestens 14 Zeichen. Dies ändert nicht die Schlüssel, die derzeit von Meeting Server-Diensten verwendet werden.
- Mit dem Befehl backup encrypt <Name> encrypted-name erstellte Sicherungsdateien werden verschlüsselt. Wenn die Option "Sicherer Speicher" aktiviert ist, fordert der MMP-Befehl backup encrypt <Name> encrypted-name eine Passphrase mit mindestens 14 Zeichen auf. Die gleiche Passphrase ist bei der Wiederherstellung des Backups erforderlich.
- Bevor eine Sicherungsdatei heruntergeladen wird, muss sie verschlüsselt sein. Wenn eine aufgelistete Sicherung noch nicht für den Export verschlüsselt ist, verwenden Sie backup encrypt <name> encrypted-name. Es wird abgelehnt, eine unverschlüsselte Sicherung herunterzuladen.
- Ab Version 3.12 kann Secure Storage betrieben werden, wenn FIPS aktiviert ist. Private Schlüsseldateien, die in 3.11 mit einer kürzeren Passphrase erstellt wurden, müssen unter Verwendung einer Passphrase mit mindestens 14 Zeichen neu generiert werden.



Tipp: Secure Storage schränkt die Übertragung unverschlüsselter privater Schlüssel und unverschlüsselter Sicherungsdateien vom Meeting Server ein. Die Übertragung von Zertifikatsdateien wird dadurch nicht eingeschränkt. Zertifikate können weiterhin mit SFTP kopiert werden. werden nur die zugehörigen unverschlüsselten privaten Schlüssel

blockiert, bis sie mit pki encrypt verschlüsselt werden.

⚠ Vorsicht: Nach der Aktivierung kann Secure Storage nicht mit einem MMP-Befehl deaktiviert werden. Der Vorgang ist unumkehrbar. Nur factory_reset full setzt Secure Storage auf false zurück. Erstellen Sie ein Konfigurations-Backup mit einem Backup-Snapshot, und speichern Sie es auf einem separaten Gerät, bevor Sie Secure Storage aktivieren. Nach secure_storage aktivieren Sie sofort den Neustart. Wenn der Neustart übersprungen wird, kann Secure Storage als aktiviert markiert werden, ohne vollständig initialisiert zu sein, und Befehle wie factory_reset full können fehlschlagen. Der Wiederherstellungspfad in diesem Zustand muss auf einen zuvor gespeicherten Snapshot zurückgesetzt werden (dies gilt nur für 3.13.x). In Meeting Server 4.0 ist secure_storage standardmäßig aktiviert.

Unterstützte Plattformen

- Virtuelles System (spezifikationsbasiert): Unterstützt
- Meeting Server Small/1K: Unterstützt
- Meeting-Server - Mittel: Unterstützt
- Meeting Server 2000: Nicht unterstützt. Die Secure Storage-Funktion ist nicht verfügbar. Verwenden Sie auf dieser Plattform keine Secure Storage-Befehle.

Cisco Meeting Server 4.0 aktiviert standardmäßig Secure Storage auf allen kompatiblen Plattformen. Nach dem Upgrade werden die Daten automatisch durch Secure Storage geschützt, selbst wenn die 3.13.x-Sicherung durchgeführt wurde, während Secure Storage deaktiviert wurde.

Implementierungshinweise

- Durch Umbenennen des Upgrade-Images werden die Einstellungen für den sicheren Speicher nicht geändert.
- Bestätigen Sie den Status des sicheren Speichers auf jedem Knoten mit dem Befehl secure_storage, bevor Sie Backups erstellen.
- Der Befehl gibt an, ob Secure Storage aktiviert ist (True) oder nicht aktiviert ist (False). Auf Meeting Server 2000 ist der Befehl nicht anwendbar. Führen Sie während des Upgrades von Cisco Meeting Server 2000 die Schritte aus, die unter den Upgrade-Bedingungen erwähnt wurden, bei denen Secure Storage deaktiviert ist oder nicht verfügbar ist.



MMP-Ausgabe, wenn Secure Storage nicht aktiviert ist (Aktiviert: false).



Abbildung 2: MMP-Ausgabe, wenn Secure Storage aktiviert ist (Aktiviert: true) auf Cisco Meeting Server 3.13.

Detaillierte Warnungen zur Befehlssyntax und Beispiele zur Verwendung finden Sie in der Cisco Meeting Server-Administratorkurzreferenz für Secure Storage und in der MMP-Befehlsreferenz, die Sie derzeit verwenden.

Upgrade-Prinzipien und -Einschränkungen

Erforderlicher Upgrade-Pfad

Cisco Meeting Server-Upgrades müssen einem sequenziellen Pfad folgen, ohne wichtige Versionen zu überspringen. Ein Knoten auf 3.11.x muss beispielsweise 3.12.x und 3.13.x durchlaufen, bevor er 4.0 erreicht. Direkte Upgrades von früheren Versionen wie 3.9.x auf 3.13.x oder 3.11.x auf 4.0 werden nicht unterstützt und führen in der Regel zu nicht behebbaren Konfigurationsfehlern. Für Meeting Server Medium mit Version 3.11.5 oder 3.13 lautet der Upgrade-Pfad 3.11.5 → 3.13 → 4.0.

Tipp: Vor dem Start des 4.0-Upgrades muss auf jedem Knoten Cisco Meeting Server 3.13.x ausgeführt werden. Dabei muss ein Backup der verifizierten Konfiguration aus diesem 3.13.x-System exportiert werden. Bei allen Szenarioprozeduren in diesem Dokument wird davon ausgegangen, dass das schrittweise Upgrade auf 3.13.x bereits abgeschlossen ist.

Herabstufungen

Tipp: Ein Downgrade von 4.0.x auf 3.13.x wird nicht unterstützt. Wenn das Upgrade fehlschlägt oder das System nicht wie erwartet funktioniert, stellen Sie eine neue 3.13.x OVA bereit (oder erstellen Sie ein neues Image der Appliance), und stellen Sie die 3.13.x-Sicherung wieder her. Behalten Sie für die Dauer des Upgrade-Fensters Hypervisor-Snapshots der virtuellen Systeme 3.13.x als zusätzliche Wiederherstellungsoption bei. VM-Snapshots ersetzen keine exportierten Konfigurationssicherungen.

Wichtige Backup-Anforderungen für 4.0-Upgrades

Nach der Bestätigung des 4.0-Upgrades wird der Knoten neu gestartet und erhält den ersten Boot-Status. Verlassen Sie sich nicht auf die automatische Sicherung, die während des Upgrade-Vorgangs generiert wird, da ein Upgrade-Fehler zu einem Verlust des SFTP-Zugriffs führen und den Zugriff auf die Datei unmöglich machen kann. Nur Backups, die mit dem Befehl backup snapshot erstellt und in externen Speicher kopiert werden, können zuverlässig für die Wiederherstellung verwendet werden.

Konfiguration der ersten Anmeldung und des ersten Kennworts

Beim ersten Start von Version 4.0 wird das vorhandene MMP-Kennwort aus der Datenbank entfernt. Melden Sie sich mit dem Benutzernamen admin mit einem leeren Kennwort (ohne Kennwort) an. Sie müssen ein neues MMP-Kennwort einrichten. Das System fordert Sie auf, das Kennwort zweimal einzugeben, um es zu überprüfen und zu bestätigen. Da es keine Funktion zur Kennwortwiederherstellung für Meeting Server gibt, vergewissern Sie sich, dass Sie Ihr neues Kennwort speichern.

Anmerkung: Wenn Sie beim ersten Start ein neues MMP-Kennwort festlegen, ersetzt der Befehl backup rollback dieses durch das Kennwort, das in der 3.13.x-Sicherung gespeichert wurde. Nachdem Sie die Sicherung auf dem Server wiederhergestellt haben, müssen Sie sich mit dem Kennwort anmelden, das zum Zeitpunkt der Erstellung der Sicherung aktiv war.

Netzwerkverbindung nach dem Upgrade wiederherstellen

IPv4- und IPv6-Adressen, Masken und Gateways gehen zusammen mit dem Rest der Konfiguration verloren. Nach dem Upgrade auf Version 4.0 kann die Netzwerkverbindung des Meeting Servers unterbrochen werden. Sie benötigen eine Hypervisor-Konsole, einen CIMC oder seriellen Zugriff, damit Sie die Adressierung erneut über die MMP zuweisen können.

Anmerkung: Bereitstellungen, die DHCP-Reservierungen verwenden, behalten nach dem Neustart in der Regel die gleichen IP-Adressen bei. Der Konsolenzugriff muss jedoch verfügbar bleiben, bis die Adresse verifiziert ist. Gehen Sie erst dann davon aus, dass die SSH-Verbindung wiederhergestellt ist, wenn die IP-Adresse bestätigt wurde.

Serverzustand vor dem Erstellen von Sicherungen überprüfen

Stellen Sie nach jedem Schritt-Upgrade auf Version 3.13 sicher, dass sich der Server in einwandfreiem Zustand befindet und alle Dienste funktionieren. Ignorieren Sie keine Fehlerzustände auf der Server-Übersichtsseite. Wenn Sie Fehler/Fehler feststellen, beheben Sie diese, bevor ein Backup-Snapshot auf 3.13 erstellt wird. Dadurch wird sichergestellt, dass ein fehlerfreies Server-Backup auf aktualisierten 4.0-Knoten wiederhergestellt wird, sodass Ihr Bereitstellungsfehler nicht verloren geht.

Öffnen Sie unter Web-Administrator Status, und stellen Sie sicher, dass der Abschnitt Fehlerbedingungen leer ist. Einträge ignorieren, die nur unter Zuletzt aufgetretene Fehler und Warnungen angezeigt werden. Nach einem Upgrade werden dort in der Regel Übergangsdatenbanken oder Web Bridge-Meldungen angezeigt. Diese stellen keinen Grund für die Wiederherstellung oder die Verzögerung der Sicherung dar.

Wenn eine Fehlerbedingung länger als etwa zehn Minuten besteht, beheben Sie sie, bevor Sie die Sicherung durchführen. Eine Wiederherstellung einer 3.13.x-Sicherung, die bereits Fehler in 4.0 enthält, leitet diese Fehler weiter.

Überprüfen Sie für geclusterte Systeme, ob alle verwendeten Anruftypen (SIP-Endpunkte und Web-App-Clients) funktionieren und keine Fehlerzustände auf den Knoten aufgeführt sind.

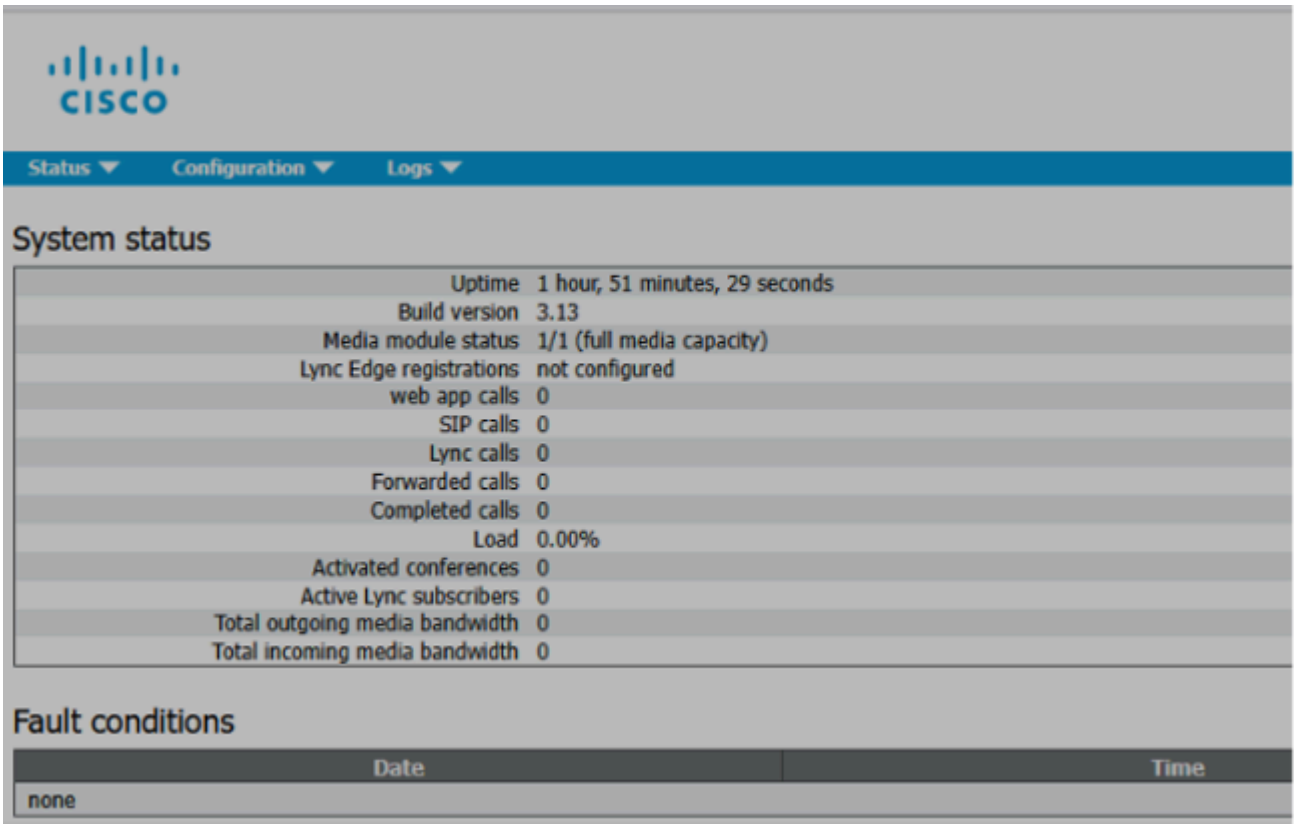


Abbildung 3: Web-Administrator-Statusseite auf 3.13.x mit leeren Fehlerbedingungen. Verwenden Sie diese Ansicht, bevor Sie die Sicherung durchführen, die auf 4.0 wiederhergestellt wurde.

Anforderungen vor dem Upgrade

Führen Sie diese Aktionen aus, bevor Sie mit dem Upgrade auf Version 4.0 beginnen. Diese Anforderungen gelten für alle vier Szenarien, die weiter unten in diesem Dokument behandelt werden.

- Führen Sie ein Upgrade auf 3.13.x durch, und exportieren Sie dann ein Konfigurations-Backup. Stellen Sie sicher, dass auf dem Knoten Cisco Meeting Server 3.13.x ausgeführt wird. Erstellen Sie ein Backup, und übertragen Sie es zusammen mit allen benutzerdefinierten SFTP-Daten wie Logos, Branding-Dateien, Audio-Aufforderungen, SSO-Dateien und anderen benutzerdefinierten Daten an einen externen Speicher. Verwenden Sie die Verfahren im Abschnitt Allgemeine Sicherungs- und Wiederherstellungsverfahren. Sichern Sie in einer Cluster-Umgebung nicht nur den verbundenen primären Knoten, sondern auch das verbundene Replikat von jedem Knoten.
- Netzwerkeinstellungen aufzeichnen. Führen Sie ipv4 a aus, und speichern Sie die Ausgabe. Sie müssen diese Informationen nach dem Neustart von 4.0 über die Konsole erneut eingeben, es sei denn, eine DHCP-Reservierung stellt die IP-Adresse automatisch wieder her.
- Konsolenzugriff bestätigen. Der Zugriff auf die Hypervisor-Konsole, den CIMC oder den seriellen Zugriff muss vor dem Start verfügbar sein. Es wird erwartet, dass SSH beendet wird, wenn der Knoten neu gestartet wird und 4.0 verwendet.

- Aktuelles Protokollpaket für Archivierung herunterladen. Speichern Sie logbundle.tar.gz von jedem Knoten. Das Paket ist kein Ersatz für Backup-Snapshots.
- Lesen Sie das Warnbanner zur Aktualisierung von 4.0, wenn es nach der Ausführung des Befehls upgrade angezeigt wird.
- Drücken Sie n, um den Vorgang abzubrechen, wenn eine erforderliche Komponente unvollständig ist. Drücken Sie nur Y, wenn Sie fortfahren möchten.

Allgemeine Sicherungs- und Wiederherstellungsverfahren

Die vier Upgrade-Szenarien, die weiter unten in diesem Dokument besprochen werden, verwenden dasselbe Sicherungs-, Export-, Erststart- und Wiederherstellungsmuster. Verwenden Sie diesen Abschnitt als einzige Quelle für diese Schritte. Befolgen Sie dann nur die szenarios-spezifische Reihenfolge (einzelner Knoten im Vergleich zu Cluster, und ob Secure Storage bereits aktiviert ist).

Betroffene Daten nach 4.0-Upgrade

Diese Daten gehen nach dem 4.0-Upgrade verloren, bis Sie eine Sicherung wiederherstellen:

- Datenbankinhalt, der Leerzeichen, Benutzer und Anrufprofile enthält.
- Zertifikate und private Schlüssel.
- Lokale Anpassung, SSO-Dateien und Audio-Aufforderungsdateien.
- Netzwerkkonfiguration (IP-Adresse, Maske und Gateway), außer wenn eine DHCP-Reservierung die Adresse wiederherstellt.
- Das vorherige MMP-Kennwort, bis beim Backup-Rollback das Kennwort aus der Sicherung erneut angewendet wird.
- Die Aufrufbrücke, der Webadministrator, die Webbrücke und andere Anwendungsdienste werden erst nach der Wiederherstellung angezeigt.

Tipp: Der geheime Schlüssel für MeetingApps ist in der Cisco Meeting Server-Sicherung nicht enthalten. Nach einer Wiederherstellung müssen Sie diesen Schlüssel neu generieren und auf jeden Web Bridge-Knoten anwenden. Siehe den Abschnitt Geheimer Schlüssel von MeetingApps nach der Wiederherstellung.

Sicherung durchführen, wenn der sichere Speicher deaktiviert oder nicht verfügbar ist

Befolgen Sie diese Vorgehensweise auf virtuellen Systemen, Meeting Server Small und Meeting Server Medium, bei denen secure_storage-Berichte aktiviert sind: False und auf Meeting Server

2000, auf dem Secure Storage nicht verfügbar ist.

1. Erstellen Sie auf jedem Knoten eine Datei mit dem Befehl backup snapshot. Verwenden Sie den vorherigen Dateinamen nicht erneut.

2. Kopieren Sie die Sicherungsdatei mit SFTP sofort in einen externen Speicher. Behalten Sie nicht die einzige Kopie auf dem Meeting-Server bei.

3. Speichern Sie die Datei an einem Speicherort, der nach der Wiederherstellung des Knotens noch erreichbar ist.

Beispiel:

backup snapshot cms313SecurestorageFalse backup list

4. Vergewissern Sie sich, dass die Datei im Befehl der Sicherungsliste angezeigt wird, und übertragen Sie sie dann mit einem SFTP-Client auf eine externe Festplatte.

5. Wiederholen Sie diesen Vorgang für jeden Knoten im Cluster. Sicherungsnamen dürfen nur Buchstaben, Ziffern, Unterstriche und Bindestriche enthalten. Schließen Sie die Dateierweiterung .bak nicht ein, wenn Sie eine Sicherungsdatei erstellen. Beispielsweise wird ein Dateiname wie 3.13SecureStorageFalse aufgrund des Zeitraums abgelehnt.

```
    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>
```

Abbildung 4: Der Backup-Snapshot weist einen Namen zurück, der einen Punkt enthält, und erhält anschließend einen alphanumerischen Namen. Die .bak-Datei kann dann heruntergeladen werden.



Abbildung 5: Kopieren Sie die .bak-Datei vom SFTP-Stamm des Meeting Server in einen externen Speicher. Lassen Sie nicht die einzige Kopie auf dem Server.

Sicherung durchführen, wenn sicherer Speicher aktiviert ist

Gehen Sie folgendermaßen vor, wenn secure_storage-Berichte aktiviert sind: Richtig. Nicht verschlüsselte Sicherungsdateien können nicht heruntergeladen werden.

1. Erstellen Sie einen Backup-Snapshot auf jedem Knoten. Wenn die sichere Speicherung aktiviert ist, fordert der Server eine Passphrase mit mindestens 14 Zeichen an. Die Passphrase kann Buchstaben, Zahlen, Sonderzeichen, Symbole oder Leerzeichen enthalten.

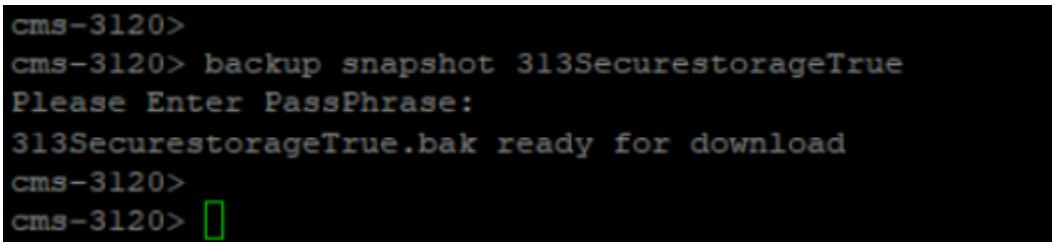


Abbildung 6: Der Backup-Snapshot mit aktiviertem sicherem Speicher fordert eine einmalige Eingabe einer Passphrase von mindestens 14 Zeichen. Der MMP bittet Sie nicht, dies zu bestätigen.

2. Der MMP fordert Sie nicht auf, die Passphrase erneut zur Bestätigung einzugeben. Sichern Sie Ihre Passphrase, da Sie dieselbe Passphrase benötigen, um die Datei wiederherzustellen. Wählen Sie keine triviale oder beispielhafte Passphrase aus.

3. Wenn der Befehl backup list einen Snapshot anzeigt, der nicht für den Export verschlüsselt wurde, verschlüsseln Sie ihn, bevor Sie ihn herunterladen:



Abbildung 7: Sicherungsliste vor der Verschlüsselung. Die verschlüsselte Spalte ist nicht vorhanden, daher kann die Datei nicht heruntergeladen werden.

4. Wenn Sie versuchen, eine unverschlüsselte Sicherung herunterzuladen, gibt SFTP einen Fehler mit verweigerter Berechtigung zurück und fordert Sie auf, den Befehl backup encrypt zuerst auszuführen.

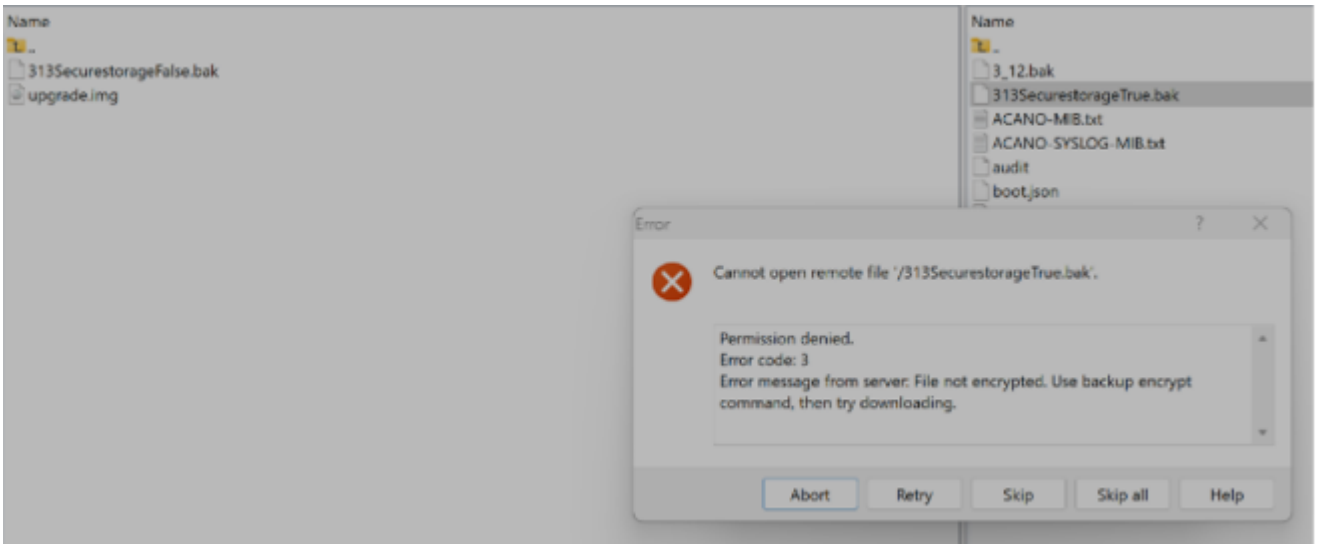


Abbildung 8: SFTP verweigert das Herunterladen einer unverschlüsselten Sicherung, wenn Secure Storage aktiviert ist. Die Servermeldung weist Sie an, die Backup-Verschlüsselung auszuführen.

5. Führen Sie den Befehl backup encrypt aus, um die Sicherungsdatei zu verschlüsseln.

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

Abbildung 9: Backup-Liste, nachdem der Snapshot verschlüsselt wurde. Verschlüsselt ist ja und die Datei kann mit SFTP übertragen werden.

In der Sicherungsliste werden der Verschlüsselungsstatus und der ursprüngliche Dateiname angezeigt. Stellen Sie sicher, dass Sie nur die verschlüsselte Datei von jedem Knoten im Cluster übertragen. Verwalten Sie einen organisierten Datensatz für jeden Knoten, den zugehörigen Dateinamen und die zugehörige Passphrase.

Wenn Sie auch private Schlüssel exportieren müssen, verschlüsseln Sie zuerst jeden Schlüssel. Zertifikatsdateien werden von Secure Storage nicht blockiert und können ohne diesen zusätzlichen Schritt kopiert werden:

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

Verwenden Sie einen eindeutigen Dateinamen, anstatt den derzeit von den Diensten verwendeten Schlüssel zu überschreiben. Auch hier gilt die mindestens 14 Zeichen umfassende Passphrase.

Daten nach 4.0-Upgrade wiederherstellen

1. Kopieren Sie nach der Anmeldung beim ersten Start und der Netzwerkwiederherstellung im

Abschnitt First-boot und Network Restoration das entsprechende 3.13.x-Backup auf den Knoten mit SFTP, und stellen Sie es wieder her.

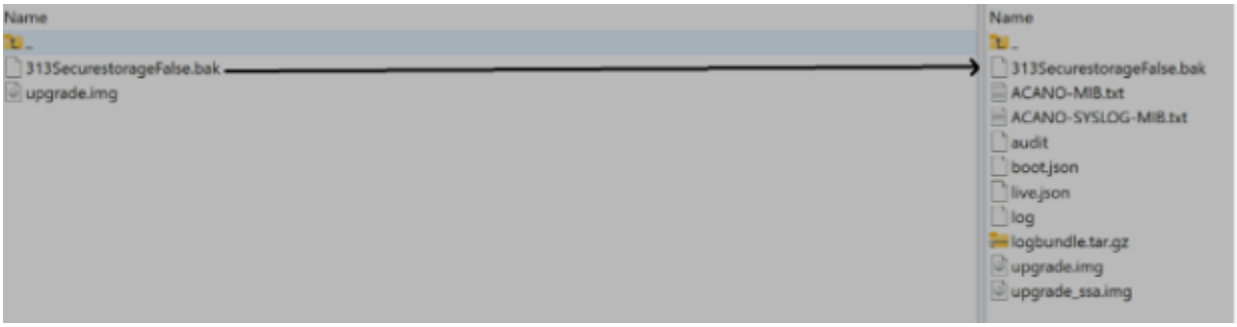


Abbildung 10: Kopieren Sie die .bak-Datei (3.13.x) nach der Wiederherstellung des Erststarts über SFTP wieder auf den 4.0-Knoten.

2. Bestätigen Sie, ob die Datei vorhanden ist:

Sicherungsliste

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

cms-3120>
```

Abbildung 11: Backup-Liste auf 4.0, die bestätigt, dass der hochgeladene Snapshot vor dem Rollback vorhanden ist.

3. Stellen Sie den Snapshot wieder her. In einer Clusterbereitstellung stellen Sie zuerst die ursprüngliche primäre Datenbank, dann die Replikate und dann die verbundenen Knoten wieder her.

backup rollback name-of-the-backup-file

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

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

Abbildung 12: Backup-Rollback eines unverschlüsselten Snapshots. Mit Y bestätigen; Der Knoten extrahiert die Sicherung und startet neu.

4. Drücken Sie Y, um fortzufahren. Der Knoten wird neu gestartet, während die Sicherung extrahiert wird. Wenn die Sicherung mit aktiviertem sicherem Speicher durchgeführt wurde, fordert die MMP die Eingabe der Passphrase an. Der Neustart wird nur fortgesetzt, nachdem die richtige Passphrase akzeptiert wurde.

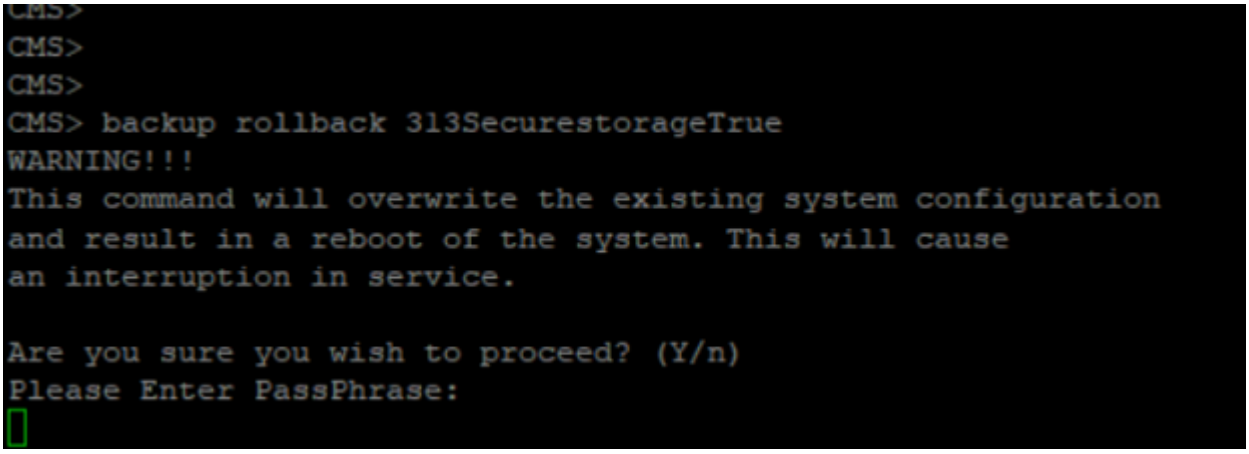


Abbildung 13: Backup-Rollback eines verschlüsselten Snapshots. Nach "Y" gibt die MMP die Passphrase ein, die bei der Erstellung der Sicherung verwendet wurde.

⚠ Vorsicht: Der **backup rollback** überschreibt die aktuelle Konfiguration, die Zertifikate, die privaten Schlüssel und die Lizenzdatei und startet den Server neu. Verwenden Sie es nur mit der 3.13.x-Sicherung, die Sie für dieses Upgrade exportiert haben.

---

5. Wenn der Knoten wieder online ist, melden Sie sich mit den MMP-Anmeldeinformationen aus der Sicherung an, und bestätigen Sie, dass jeder erforderliche Dienst als aktiviert und aktiv gemeldet wird (der MMP zeigt dies als aktiv an: True).

Typische Prüfungen:

callbridge webbridge3 webadmin scheduler recorder streamer uploader meetingapps

6. Führen Sie nur die Befehle für Dienste aus, die dieser Knoten hosten soll.

Geheimschlüssel für MeetingApps nach der Wiederherstellung

In der Cisco Meeting Server-Sicherung wird der geheime Schlüssel für MeetingApps nicht gespeichert. Nach Abschluss des Backup-Rollbacks generieren Sie den Schlüssel neu und wenden ihn auf alle Web Bridge-Knoten an. Wenn Sie diesen Schritt überspringen, ist die Dateifreigabe nicht verfügbar, obwohl die anderen Dienste einwandfrei aussehen.

1. Führen Sie auf dem MeetingApps-Knoten den Befehl meetingapps gensecret aus.

2. Kopieren Sie den generierten geheimen Schlüssel in Ihren geheimen Speicher. Bei jeder Ausführung von Meetingapps wird der vorherige Schlüssel ungültig. Generieren Sie den Schlüssel daher einmal, und verwenden Sie denselben Wert für alle Web Bridges erneut.

3. Führen Sie diese Befehle auf jedem Web Bridge-Knoten aus:

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

Der letzte Befehl bestätigt, dass der Web Bridge-Dienst ausgeführt wird und dass MeetingApps ordnungsgemäß konfiguriert ist. MeetingApps wird auf Meeting Server 2000 nicht unterstützt, und die Dateifreigabe ist in Clustern mit Meeting Server 2000 nicht verfügbar. In solchen Bereitstellungen ist dieser Schritt nicht anwendbar.

First-Boot und Netzwerkwiederherstellung

Der Befehl 4.0 upgrade (4.0-Aktualisierung) zeigt ein Warnbanner an, bevor der Vorgang fortgesetzt wird. Überprüfen Sie die Nachricht sorgfältig, und brechen Sie sie mit n ab, wenn die Voraussetzungen nicht erfüllt sind. Wenn Sie mit Y fortfahren, wird der Knoten neu gestartet, die SSH-Sitzung wird getrennt, und die übrigen Schritte müssen von der Konsole aus ausgeführt werden.

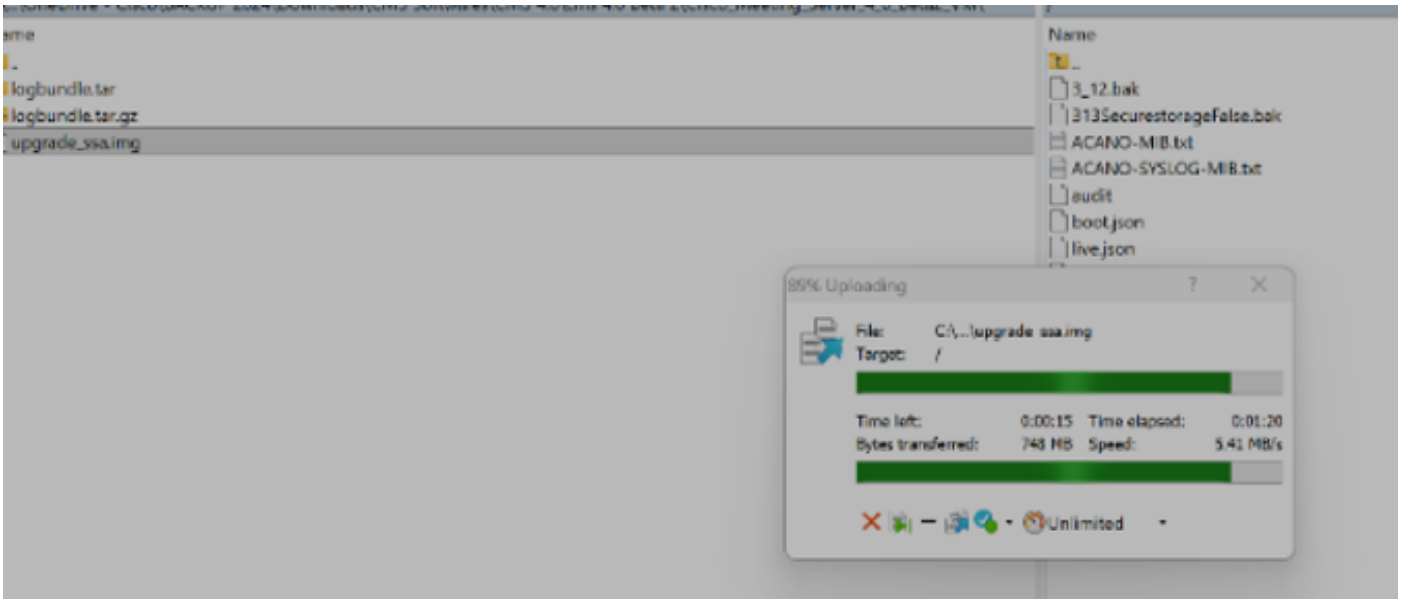


Abbildung 14: Laden Sie das Upgrade-Image für 4.0 in das SFTP-Stammverzeichnis von Meeting Server hoch. Der Dateiname des Upgrade-Images kann je nach dem von cisco.com heruntergeladenen Paket variieren.

```
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...
```

Abbildung 15: Der Befehl "upgrade" überprüft die Signatur des Images und startet den Vorgang. Verlassen Sie sich nicht auf die automatische Sicherung, die zu diesem Zeitpunkt erstellt wird.

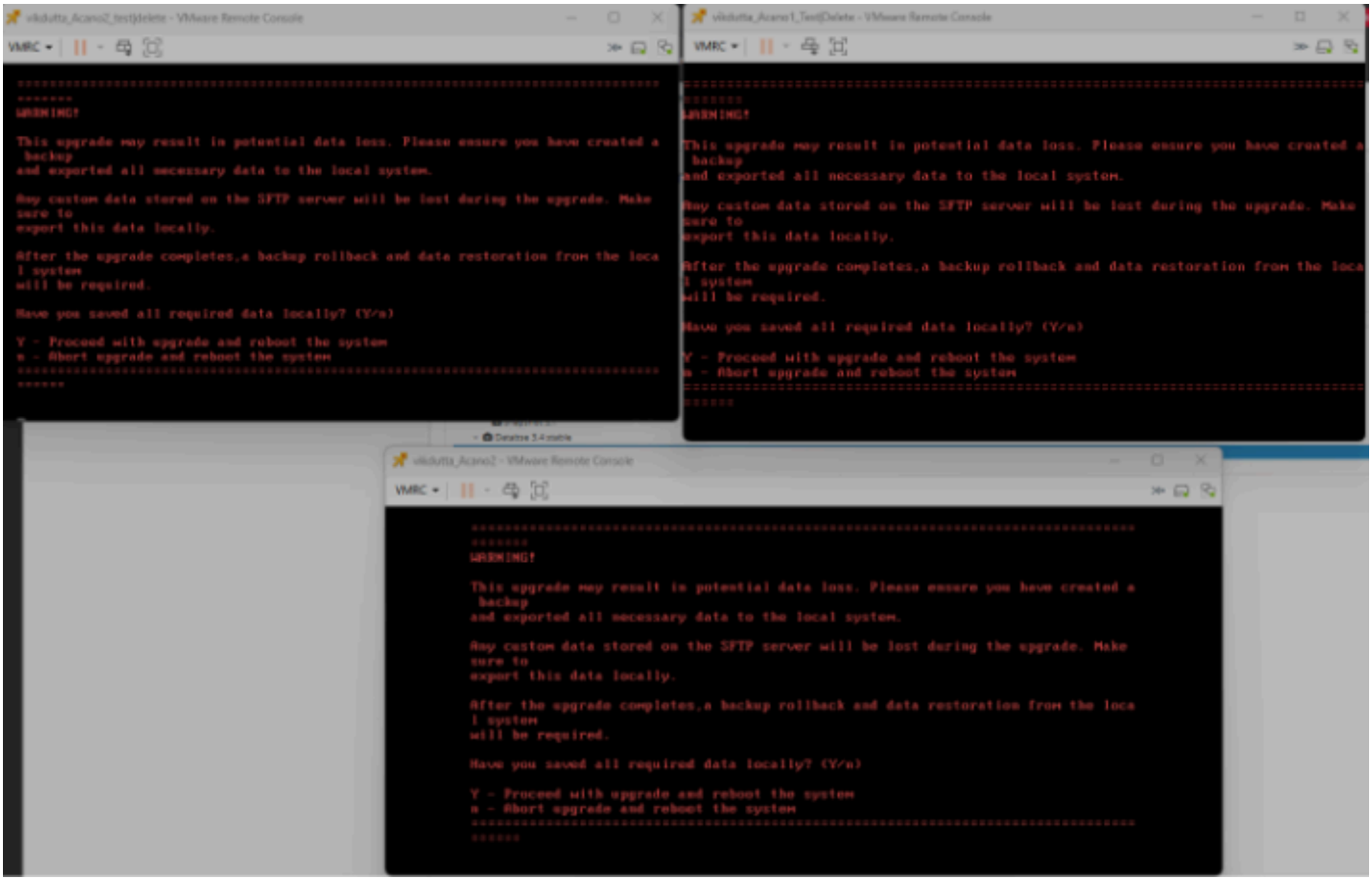


Abbildung 16: Die rote MMP-Warnung in einem Cluster mit drei Knoten. Das gleiche Banner wird auf einem einzelnen Knoten angezeigt. Drücken Sie n, um den Vorgang abzubrechen, wenn Sicherungen und benutzerdefinierte Daten nicht vom Server entfernt werden. Drücken Sie nur Y, um fortzufahren und neu zu starten.

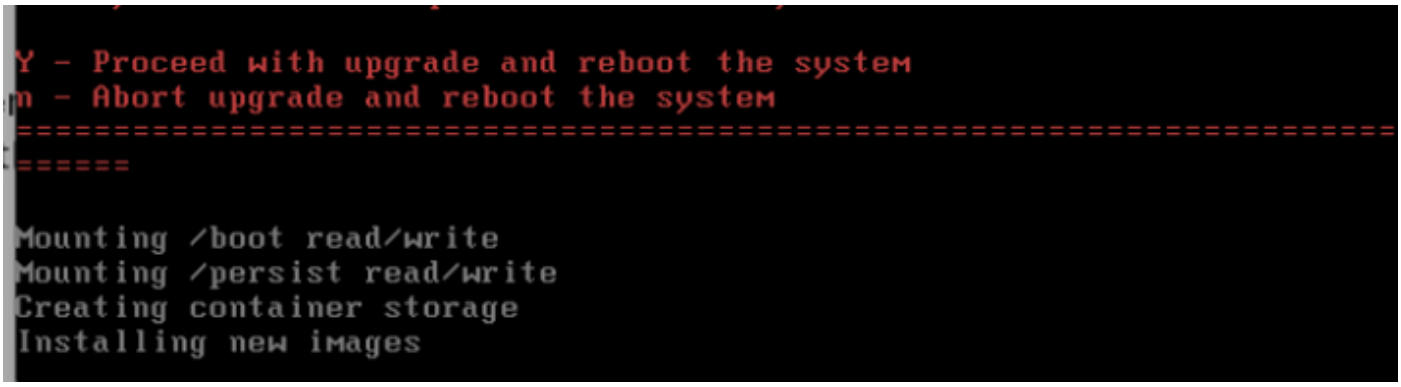


Abbildung 17: Nach Y mountet der Knoten den Speicher und installiert das 4.0-Image. Zeitüberschreitung der SSH-Sitzung; fahren Sie mit der Hypervisor-Konsole fort.

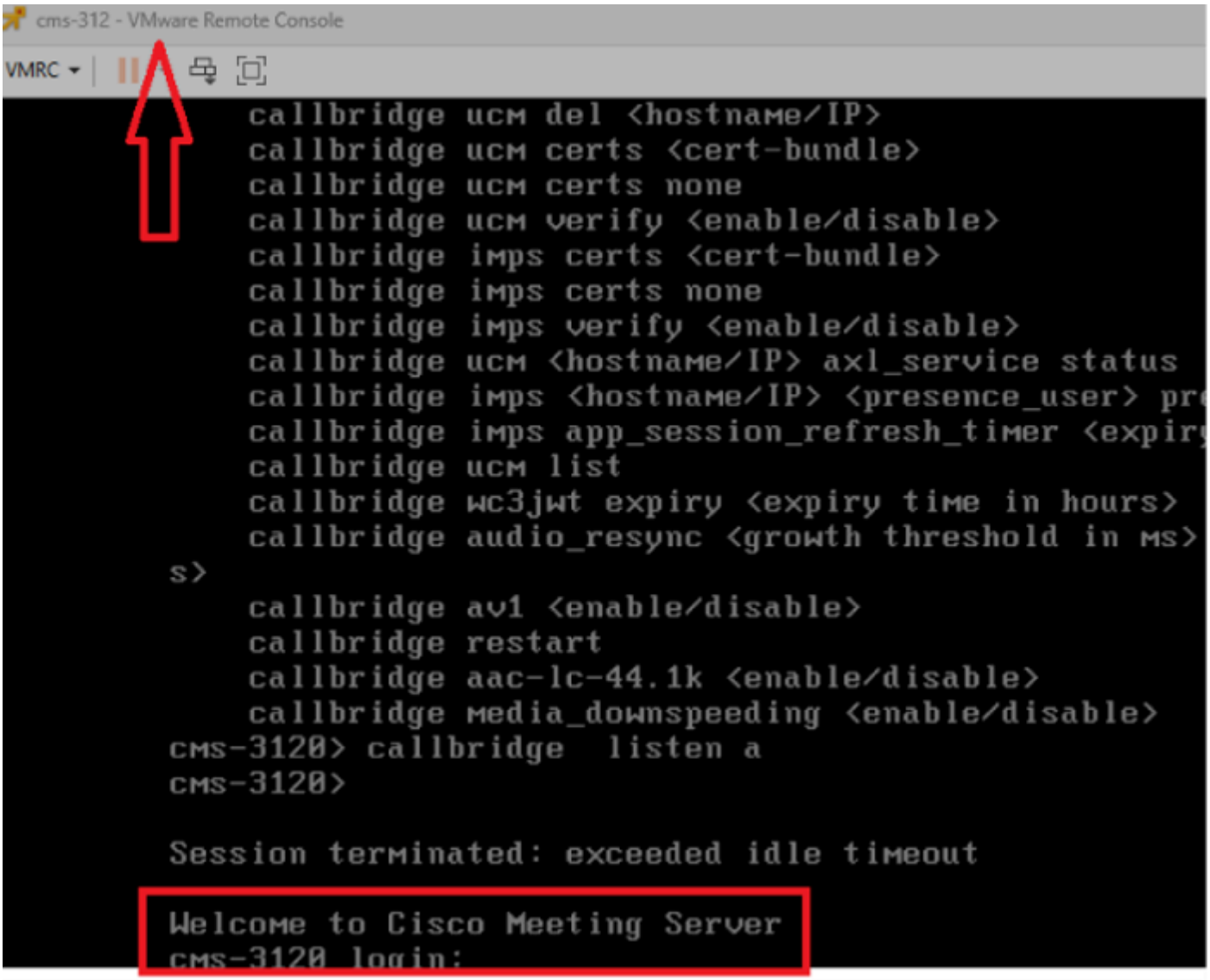


Abbildung 18: Verwenden Sie nach dem Verwerfen von SSH die VM- oder CIMC-Konsole. Die erste Boot-Anmeldeaufforderung wird angezeigt, wenn das 4.0-Image bereit ist.

1. Melden Sie sich mit dem First-Boot-MMP-Konto (Benutzername admin und kein Kennwort) an, und legen Sie bei Aufforderung ein neues MMP-Kennwort fest. Beachten Sie, dass das Backup-Rollback dieses Kennwort durch das in der Sicherung gespeicherte Kennwort ersetzt.

2. Wenden Sie die Netzwerkkonfiguration erneut anhand der Hinweise an, die Sie im Abschnitt Anforderungen vor dem Upgrade erfasst haben:

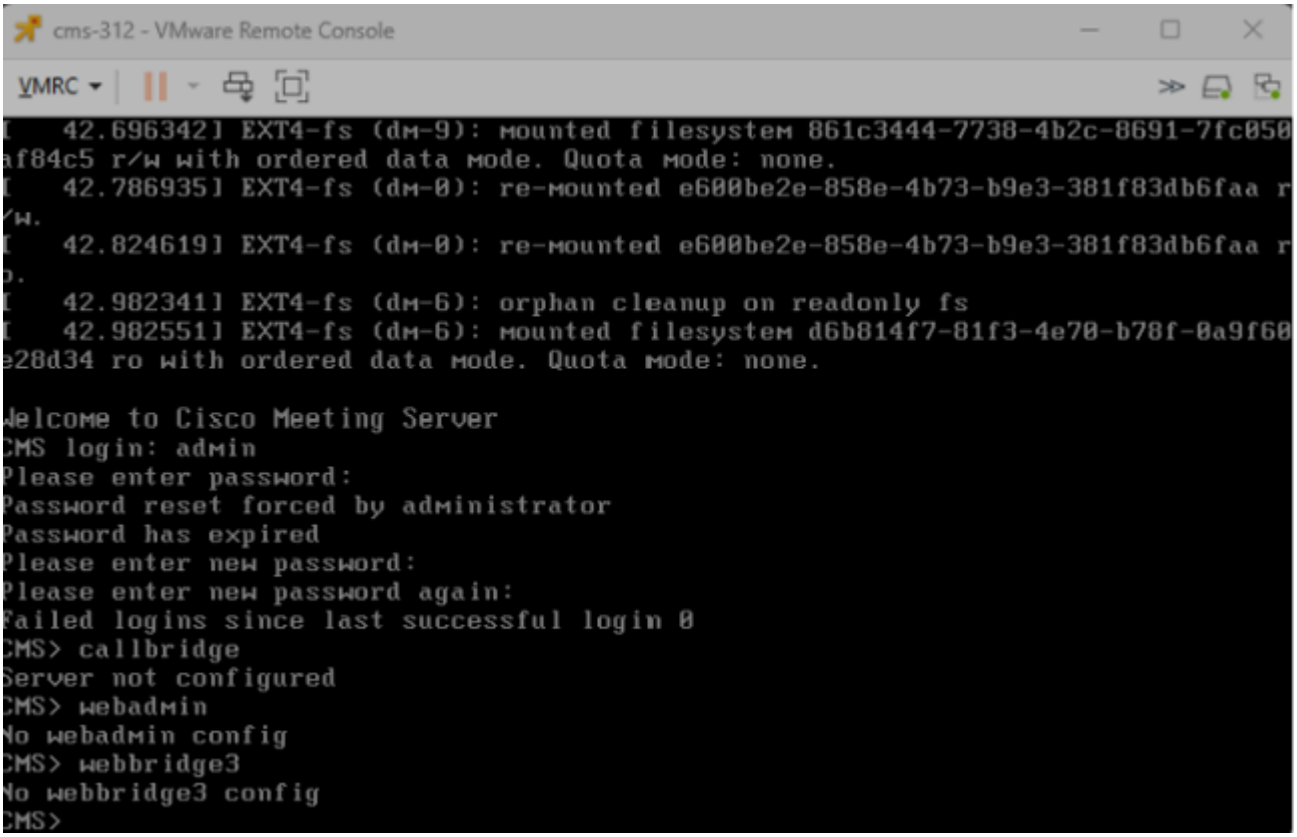


Abbildung 19: MMP-Anmeldung beim ersten Start

Das vorherige Kennwort ist nicht mehr gültig. Nachdem Sie ein neues Kennwort festgelegt haben, werden Dienste wie webadmin und webbridge3 erst nach der Wiederherstellung der Sicherung als konfiguriert angezeigt.

3. Führen Sie den folgenden Befehl aus:

ipv4 interface add address/prefix-length gateway

Beispiele:

ipv4 a add 192.0.2.10/24 192.0.2.1



Abbildung 20: IPv4 wird von der Konsole aus erneut angewendet.

Ein Neustart ist erforderlich, nachdem Sie die Adresse zugewiesen haben. Die im Screenshot gezeigten Adressen dienen lediglich als Beispiel.

4. Starten Sie neu, nachdem die Adresse zugewiesen wurde. Sobald das System wieder online ist, fahren Sie mit dem SFTP-Upload der Sicherung und den Wiederherstellungsschritten fort, die im Abschnitt Daten nach 4.0-Upgrade wiederherstellen erwähnt werden.

Anmerkung: Wenn eine DHCP-Reservierung konfiguriert ist, kann die ursprüngliche Adresse bereits nach dem Neustart zugewiesen werden. Überprüfen Sie die Adresse mit **ipv4 a** , bevor Sie eine SFTP-Sitzung von Ihrer Management-Workstation aus starten.

Auf Cisco Meeting Server 4.0 ist Secure Storage standardmäßig auf den Plattformen aktiviert, die diese Funktion unterstützen. Die MMP kann secure_storage nach dem Upgrade nicht mehr als Umschalter verfügbar machen.



Abbildung 21: Für dieses 4.0-Image ist "secure_storage" kein erkannter Befehl, da "Secure Storage" standardmäßig aktiviert ist.

Bestätigen Sie die Freigabe mit dem Befehl version.

Upgrade-Szenarien

In diesem Kapitel werden verschiedene Upgrade-Szenarien beschrieben. Führen Sie den Upgrade auf Version 3.13.x aus. Identifizieren Sie den Bereitstellungstyp, und wählen Sie das entsprechende Szenario aus. Befolgen Sie nur das Verfahren, das zu Ihrer Umgebung passt, und kombinieren Sie keine Schritte aus Cluster- und Einzelknoten-Bereitstellungen.

Führen Sie zunächst das unterstützte Schritt-Upgrade auf 3.13.x durch. Wählen Sie anschließend genau ein Szenario aus. Kombinieren Sie nicht die Einzelknoten- und Datenbank-Cluster-Prozeduren.

- Szenario 1: Einzelner Knoten, deaktiviert oder nicht verfügbar, virtuelles System, kleine und mittlere Systeme und Meeting Server 2000
- Szenario 2: Nur ein Knoten, aktiviert, VM, kleine und mittlere
- Szenario 3: Datenbank-Cluster, deaktiviert oder nicht verfügbar, virtueller Rechner, kleine und mittlere Rechner und Meeting Server 2000
- Szenario 4: Datenbankcluster, aktiviert, VM, nur kleine und mittlere

Meeting Server 2000 unterstützt die Szenarien mit aktivierter sicherer Speicherung nicht. Verwenden Sie für diese Plattform je nach Fall Szenario 1 oder 3.

Szenario 1 - Einzelner Knoten mit deaktiviertem oder nicht verfügbarem sicheren Speicher

Verwenden Sie dieses Verfahren für einen Standalone-Server mit deaktivierter sicherer Speicherung oder für Meeting Server 2000, auf dem die sichere Speicherung nicht verfügbar ist. Die Quellversion kann 3.11.x oder höher sein, der Knoten muss jedoch auf 3.13.x installiert sein, bevor Sie auf 4.0 aktualisieren.

1. Schritt-Upgrade auf 3.13.x. Folgen Sie dem unterstützten Pfad (beispielsweise 3.11.x → 3.12.x → 3.13.x). Bestätigen Sie nach jedem Hop die Version in Web Admin, und stellen Sie sicher, dass die Fehlerbedingungen klar sind, wie im Abschnitt Serverzustand validieren vor dem Erstellen von Sicherungen beschrieben.

2. Bestätigen Sie den Status des sicheren Speichers. Führen Sie den Befehl secure_storage aus, und stellen Sie sicher, dass Secure Storage nicht aktiviert ist. Überspringen Sie den Befehl auf Meeting Server 2000.

3. Erstellen und exportieren Sie eine 3.13.x-Sicherungsdatei, wie im Abschnitt Sicherung durchführen, wenn der sichere Speicher deaktiviert oder nicht verfügbar ist beschrieben. Exportieren Sie auch benutzerdefinierte SFTP-Inhalte und das Protokollpaket, wie im Abschnitt Voraussetzungen vor dem Upgrade erwähnt.

4. Laden Sie das 4.0-Software-Image von Cisco.com herunter, extrahieren Sie es, und kopieren Sie upgrade.img über SFTP auf den Knoten.

5. Starten Sie das Upgrade mit dem folgenden Befehl:

```
upgrade upgrade.img
```

6. Lesen Sie das Warnbanner. Drücken Sie erst Y, wenn alle Voraussetzungen erfüllt sind. 6. Konfigurieren Sie den Knoten nach dem Upgrade wie im Abschnitt Erststart und Netzwerkwiederherstellung beschrieben, und stellen Sie dann die Sicherung mithilfe des Abschnitts "Daten nach 4.0-Upgrade wiederherstellen" wieder her.

Szenario 2 - Einzelner Knoten mit aktivierter sicherer Speicherung

Verwenden Sie dieses Verfahren für eine eigenständige VM, einen kleinen Meeting-Server oder einen mittleren Meeting-Server, auf dem Secure Storage aktiviert ist. Sie gilt nicht für Meeting Server 2000.

Bevor Sie Dateien vom Server übertragen, beachten Sie, dass unverschlüsselte private Schlüssel und unverschlüsselte Sicherungsdateien nicht übertragen werden können. Zertifikatsdateien werden nicht blockiert.

1. Führen Sie ein Upgrade über den unterstützten Pfad auf 3.13.x durch, ohne die Releases zu überspringen. Überprüfen Sie nach jedem Hop im Abschnitt Serverzustand vor dem Erstellen von Backups validieren, ob die Version und die Fehlerbedingungen eindeutig sind.

2. Führen Sie secure_storage aus, und stellen Sie sicher, dass die Ausgabe Enabled (Aktiviert) anzeigt: Richtig.

3. Erstellen und exportieren Sie eine verschlüsselte 3.13.x-Sicherung mithilfe des Abschnitts Sicherung durchführen, wenn die sichere Speicherung aktiviert ist. Speichern Sie die Passphrase in Ihrem geheimen Speicher. Exportieren Sie auch benutzerdefinierte SFTP-Inhalte und das Protokollpaket (Abschnitt "Voraussetzungen vor dem Upgrade").

4. Kopieren Sie upgrade.img auf den Knoten, und führen Sie das Upgrade aus:

```
upgrade upgrade.img
```

5. Lesen Sie das Warnbanner, und drücken Sie Y, um fortzufahren, wenn die Voraussetzungen erfüllt sind.

6. Stellen Sie das Netzwerk von der Konsole (First-boot und Network Restoration Abschnitt), dann die verschlüsselte Sicherung mit ihrer Passphrase wiederherstellen (Restore Data After 4.0 Upgrade Abschnitt). 6. Wenn MeetingApps verwendet wird, wenden Sie einen neuen geheimen MeetingApps-Schlüssel an (geheimer MeetingApps-Schlüssel nach der Wiederherstellung).

Secure Storage ist auf Meeting Server 4.0 standardmäßig aktiviert. Behandeln Sie private Schlüssel und Sicherungsdateien nach einer Wiederherstellung weiterhin als verschlüsselte Daten.

Szenario 3 - Datenbank-Cluster mit deaktiviertem sicheren Speicher

Verwenden Sie dieses Verfahren für einen Datenbankcluster mit deaktiviertem sicheren Speicher, der einen Cluster mit Meeting Server 2000 enthält. Ab Version 3.5 muss der Datenbank-Cluster vor dem Software-Upgrade aufgelöst werden. Führen Sie zunächst für jeden Knoten ein Upgrade auf 3.13.x durch.

Clusterdetails aufzeichnen und jeden Knoten sichern

1. Führen Sie secure_storage auf jedem Knoten aus. Behandeln Sie den Befehl auf Meeting Server 2000-Knoten als nicht verfügbar.

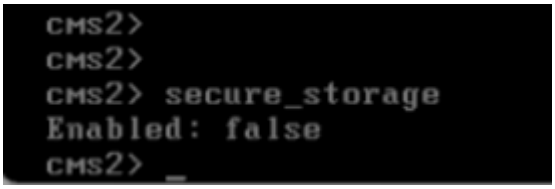


Abbildung 22: Bevor Sie unverschlüsselte Sicherungen verwenden, stellen Sie sicher, dass Secure Storage auf jedem Clusterknoten deaktiviert ist. Überspringen Sie den Befehl für Meeting Server 2000-Knoten, wenn er nicht verfügbar ist.

2. Notieren Sie sich den aktuellen primären Datenbankknoten, da dieser nach dem Upgrade auf 4.0 zuerst wiederhergestellt werden muss. Stellen Sie sicher, dass die Replikate synchronisiert sind und der Clusterstatus "fehlerfrei" ist.

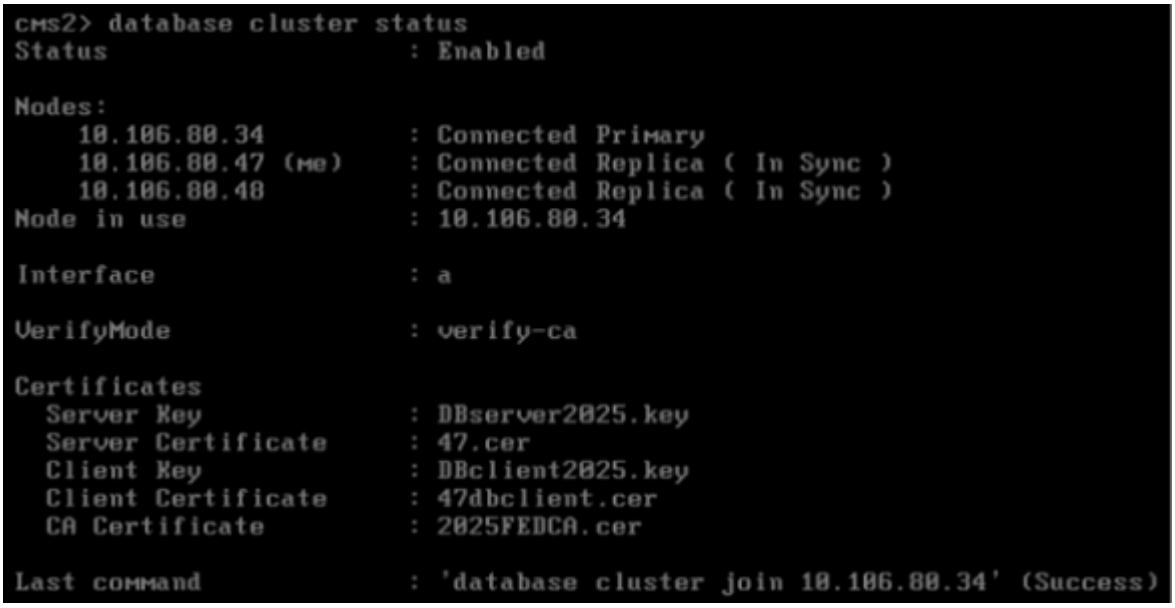


Abbildung 23: Notieren Sie die aktuellen primären und bestätigen Sie, dass die Replikate synchronisiert sind.

3. Bestätigen Sie, dass alle verwendeten Anruftypen funktionieren und die Fehlerbedingungen auf jedem Knoten eindeutig sind (Abschnitt "Serverzustand überprüfen, bevor Backups erstellt werden").

4. Erstellen Sie für jeden Knoten eine Sicherung mithilfe des Abschnitts "Sicherung durchführen, wenn sicherer Speicher deaktiviert oder nicht verfügbar ist". Benennen Sie jede Datei so, dass sie klar ihrem Knoten zugeordnet wird, und übertragen Sie jede Sicherung auf einen externen Speicher, bevor Sie den Cluster auflösen.

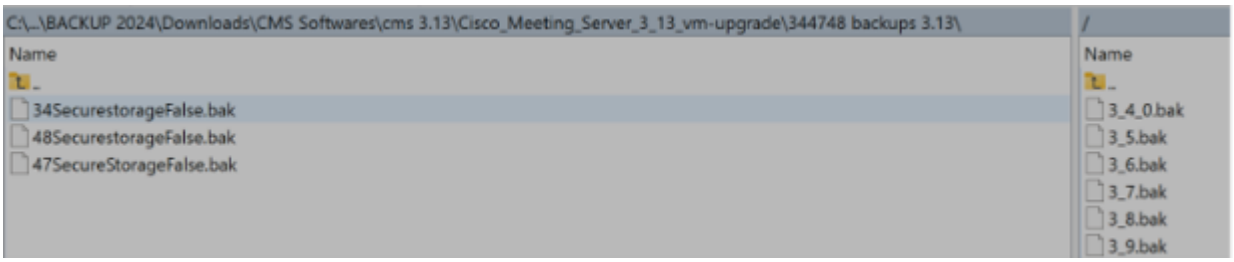


Abbildung 24: Alle drei Beispiel-Knoten-Backups speichern externen Speicher, der so benannt wird, dass jede Datei ihrem Knoten zugeordnet wird.

Cluster auflösen

Entfernen Sie Knoten in dieser Reihenfolge. Primärschlüssel bis zum letzten:

- Verbundene (nicht zum Kern gehörende) Meeting Server-Knoten
- Replikat-Datenbankknoten
- Primärer Datenbankknoten

Führen Sie auf jedem Knoten den Befehl zum Entfernen aus, und drücken Sie Y. Fahren Sie nicht mit dem 4.0-Upgrade fort, bis jeder Knoten meldet, dass er den Cluster verlassen hat. Wenn die Cluster-Zugehörigkeit entfernt wird, bleibt die lokale Datenbank dieses Knotens bestehen.

database cluster remove

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

Abbildung 25: Bestätigen Sie auf einem Replikat Y, um die Clustermitgliedschaft zu entfernen. Die lokale Datenbank des Knotens bleibt in Betrieb.

```
 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
```

Abbildung 26: Überprüfen Sie nach dem Entfernen, ob der Clusterstatus auf Deaktiviert und der verwendete Knoten auf diesem Knoten auf Keine festgelegt ist.

```
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)
```

Abbildung 27: Nach dem Entfernen der Replikate ist der erste primäre Knoten der einzige, der im Cluster verbleibt. Entfernen Sie es zuletzt.

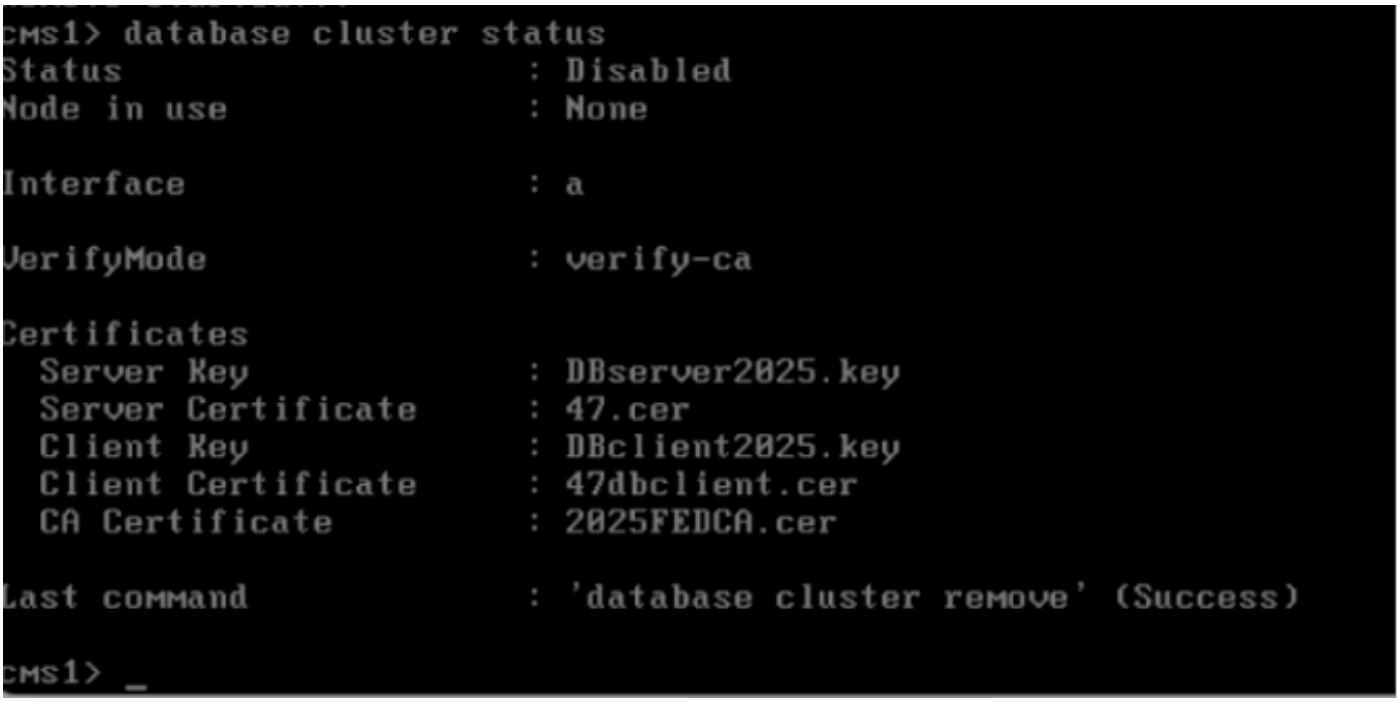


Abbildung 28: Überprüfen Sie nach dem Entfernen des früheren primären Servers, ob der Befehl "Success" und der Clusterstatus "Disabled" (Deaktiviert) meldet.

Knoten aktualisieren und wiederherstellen

1. Nach der Auflösung sind die Knoten eigenständig und können parallel aktualisiert werden. Kopieren Sie auf jedem Knoten upgrade.img über SFTP, und führen Sie den Befehl upgrade aus:

upgrade upgrade.img

2. Stellen Sie die Netzwerkadressen der einzelnen Knoten über die Konsole wieder her (Abschnitt "First-Boot" und "Network Restoration").

3. Kopieren Sie die Sicherungskopien der einzelnen Knoten 3.13.x zurück auf diesen Knoten. Stellen Sie zuerst den ersten primären Knoten, dann die Replikate und dann die verbundenen Knoten wieder her. Verwenden Sie den Abschnitt Daten nach 4.0-Upgrade wiederherstellen. Bei einer Wiederherstellung der Sicherungen wird die Mitgliedschaft im Datenbank-Cluster wiederhergestellt.

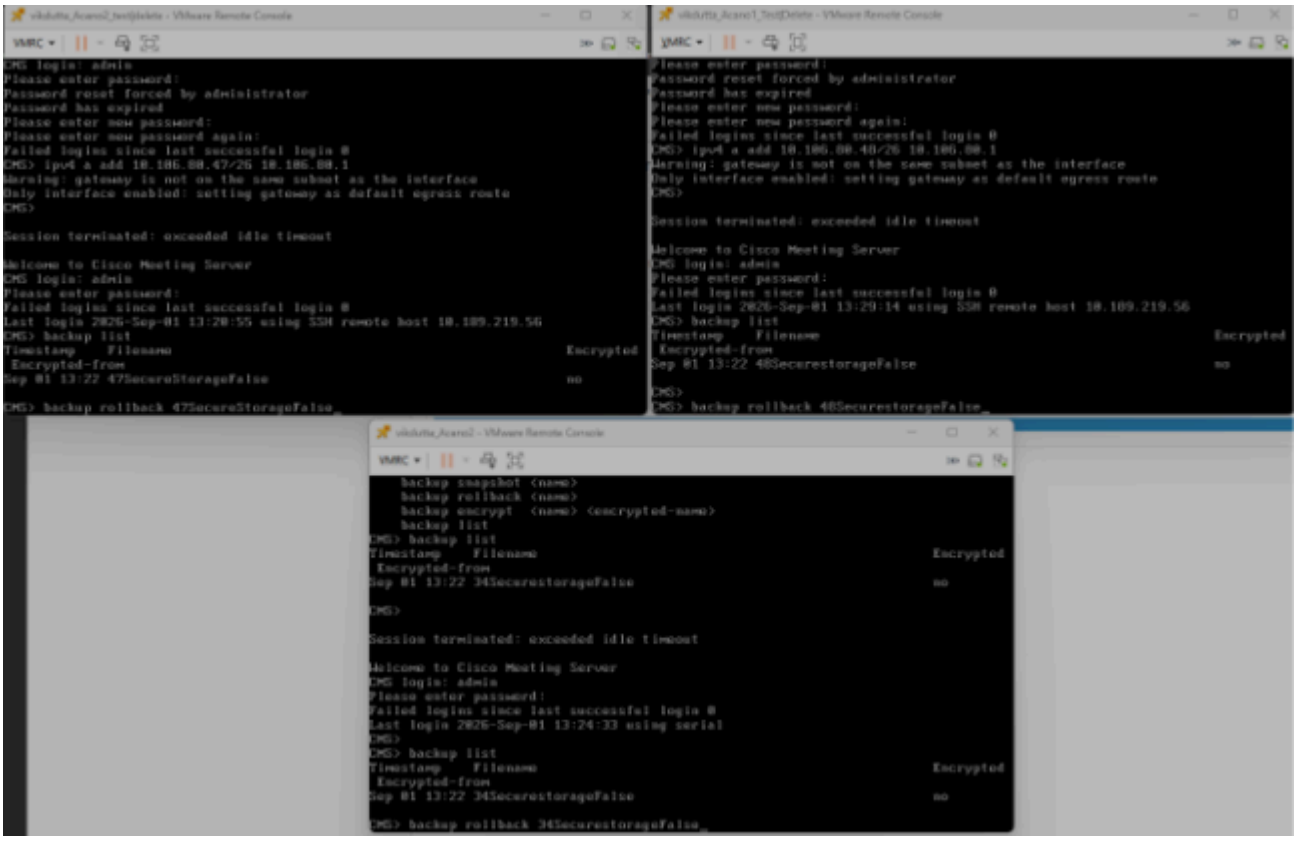


Abbildung 29: Stellen Sie die Snapshots der einzelnen Knoten wieder her. Beginnen Sie mit der ersten primären, dann stellen Sie die Replikate wieder her. Beispieldateinamen identifizieren ihren Knoten.

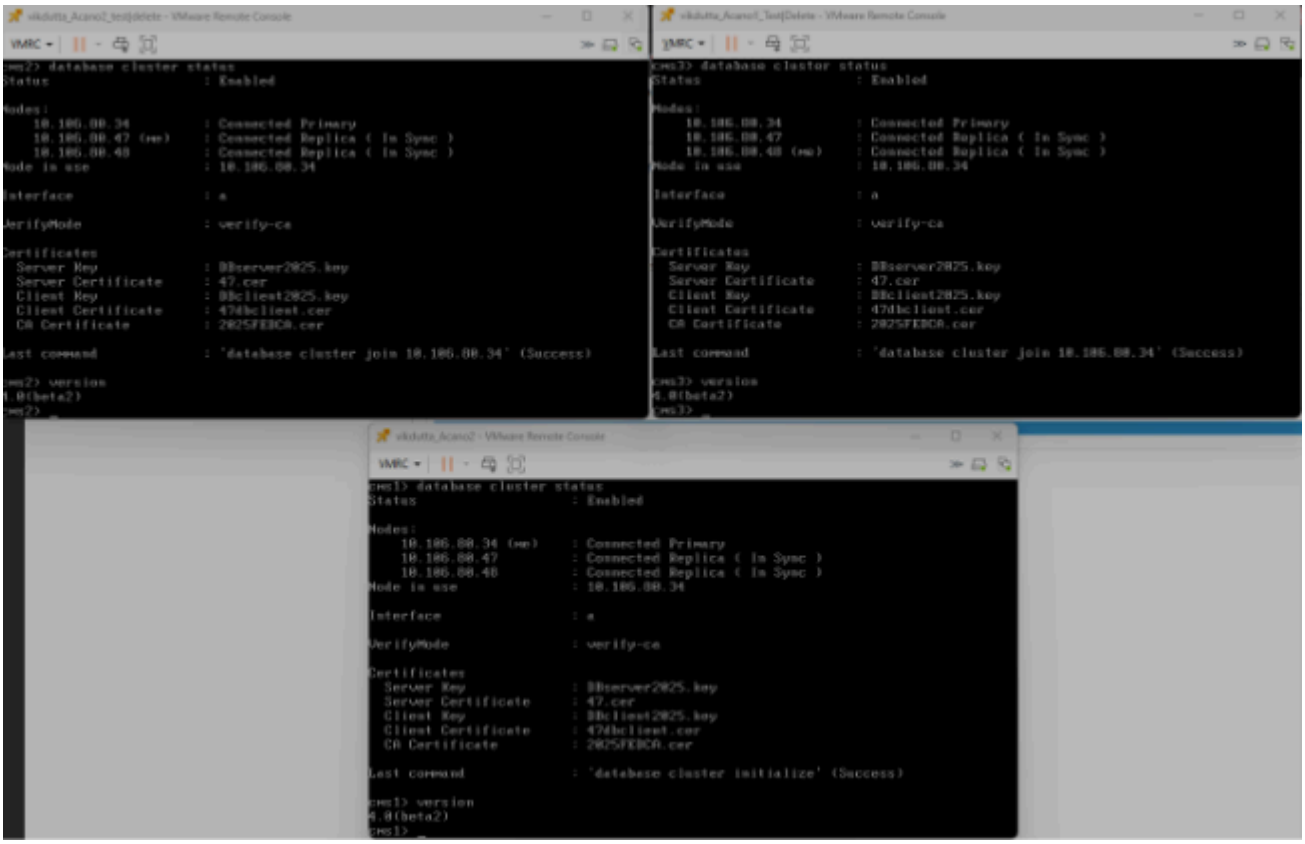


Abbildung 30: Überprüfen Sie nach der Wiederherstellung auf Meeting Server 4.0, ob der Cluster aktiviert ist, ob derselbe primäre Cluster angezeigt wird und ob die Replikate synchronisiert sind.

Anmerkung: Wenn nach dieser Wiederherstellung keine Call Bridge-Clusterverbindungen mehr verfügbar sind, führen Sie das nur auf dem **database cluster upgrade_schema** vorherigen primären System aus, und überprüfen Sie dann erneut den Call Bridge-Status.

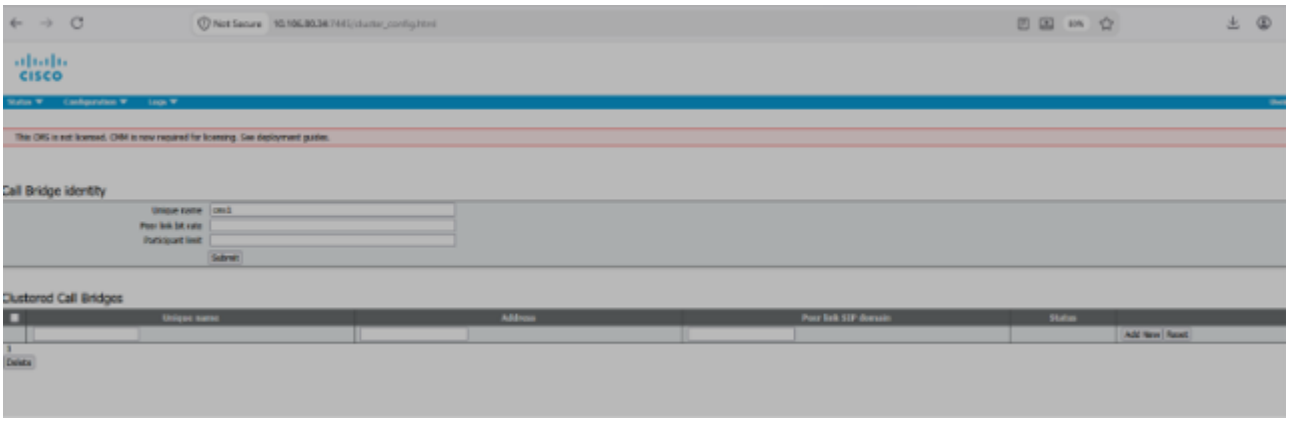


Abbildung 31: Vor der Schemaaktualisierung wird im Beispiel der Datenbankcluster angezeigt, der ausgeführt wird, während die Cluster-Anrufbrücken leer sind.

database cluster upgrade_schema

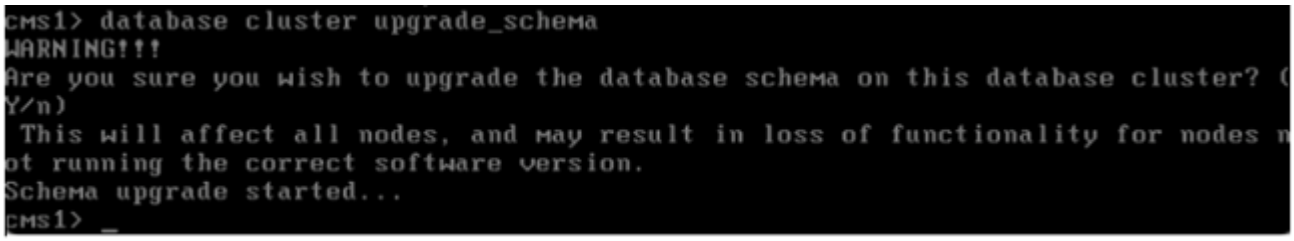


Abbildung 32: Bestätigen Sie auf dem ersten primären Gerät Y nur, wenn die Verbindung des Call Bridge-Clusters nach diesem Upgrade des aufgelösten Clusters fehlschlug.

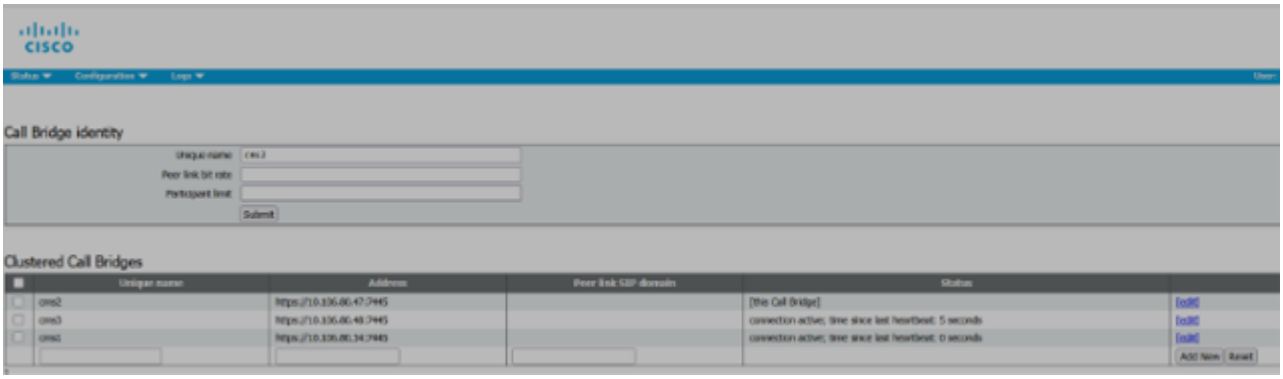


Abbildung 33: Überprüfen Sie nach dem Schema-Upgrade, ob jeder Call Bridge-Peer eine aktive Verbindung anzeigt.

4. Führen Sie das geheime Verfahren für MeetingApps im Abschnitt MeetingApps-Geheimschlüssel nach der Wiederherstellung auf jeder Web Bridge aus, und validieren Sie dann die Bereitstellung mit dem Abschnitt Validierung nach der Aktualisierung.

Szenario 4 - Datenbank-Cluster mit aktivierter sicherer Speicherung

Verwenden Sie dieses Verfahren für einen Datenbank-Cluster auf VMs, Meeting Server Small oder Meeting Server Medium, bei dem Secure Storage auf den Knoten aktiviert ist. Sie gilt nicht für Meeting Server 2000. Führen Sie zunächst für jeden Knoten ein Upgrade auf 3.13.x durch.

Clusterdetails erfassen und verschlüsselte Sicherungen erstellen

1. Führen Sie secure_storage auf jedem Knoten aus, und bestätigen Sie Enabled: Richtig.

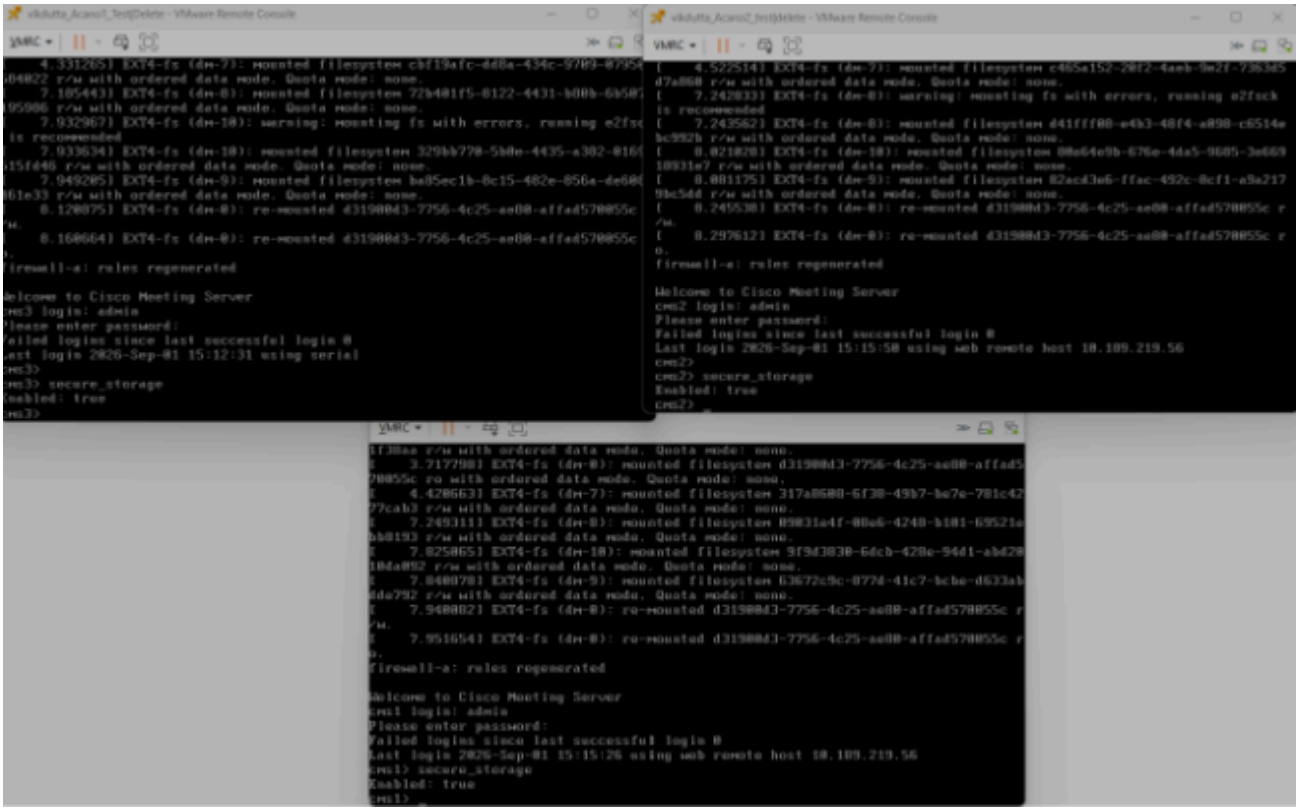


Abbildung 34: Bestätigen Sie für den abgebildeten Cluster mit drei Knoten, dass "Sicherer Speicher" aktiviert anzeigt: True für jeden Knoten vor dem Upgrade.

2. Notieren Sie die aktuelle primäre Datenbank, und stellen Sie sicher, dass die Replikate synchronisiert sind.

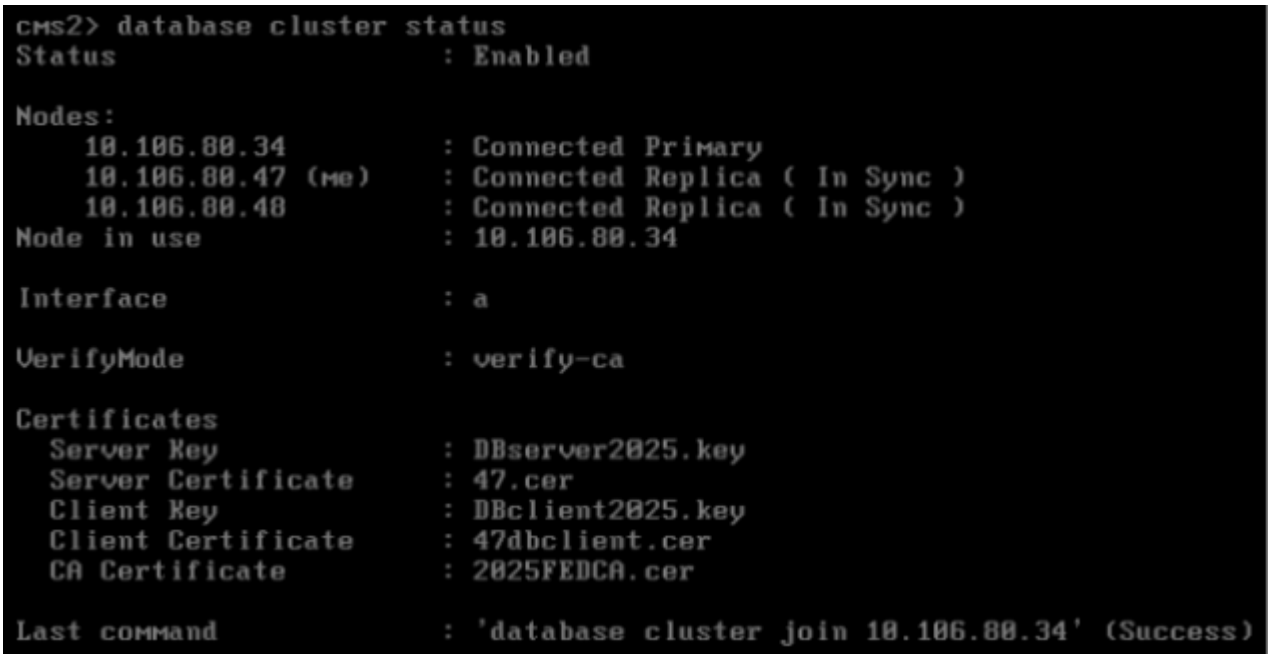


Abbildung 35: Datenbankclusterstatus vor dem Upgrade. Notieren Sie die primären und bestätigen Sie, dass die Replikate synchronisiert sind.

3. Bestätigen Sie, dass alle verwendeten Anruftypen funktionieren und die Fehlerbedingungen auf jedem Knoten klar sind (Abschnitt "Serverzustand vor dem Erstellen von Sicherungen überprüfen").

4. Erstellen Sie für jeden Knoten eine verschlüsselte Sicherung. Verwenden Sie dazu den Abschnitt Sicherung durchführen, wenn die sichere Speicherung aktiviert ist. Weisen Sie jeder Datei eine eindeutige Passphrase zu, und zeichnen Sie sie auf, oder verwenden Sie eine dokumentierte Passphrase-Richtlinie. Übertragen Sie nur verschlüsselte Dateien von den Servern, bevor Sie den Cluster auflösen.

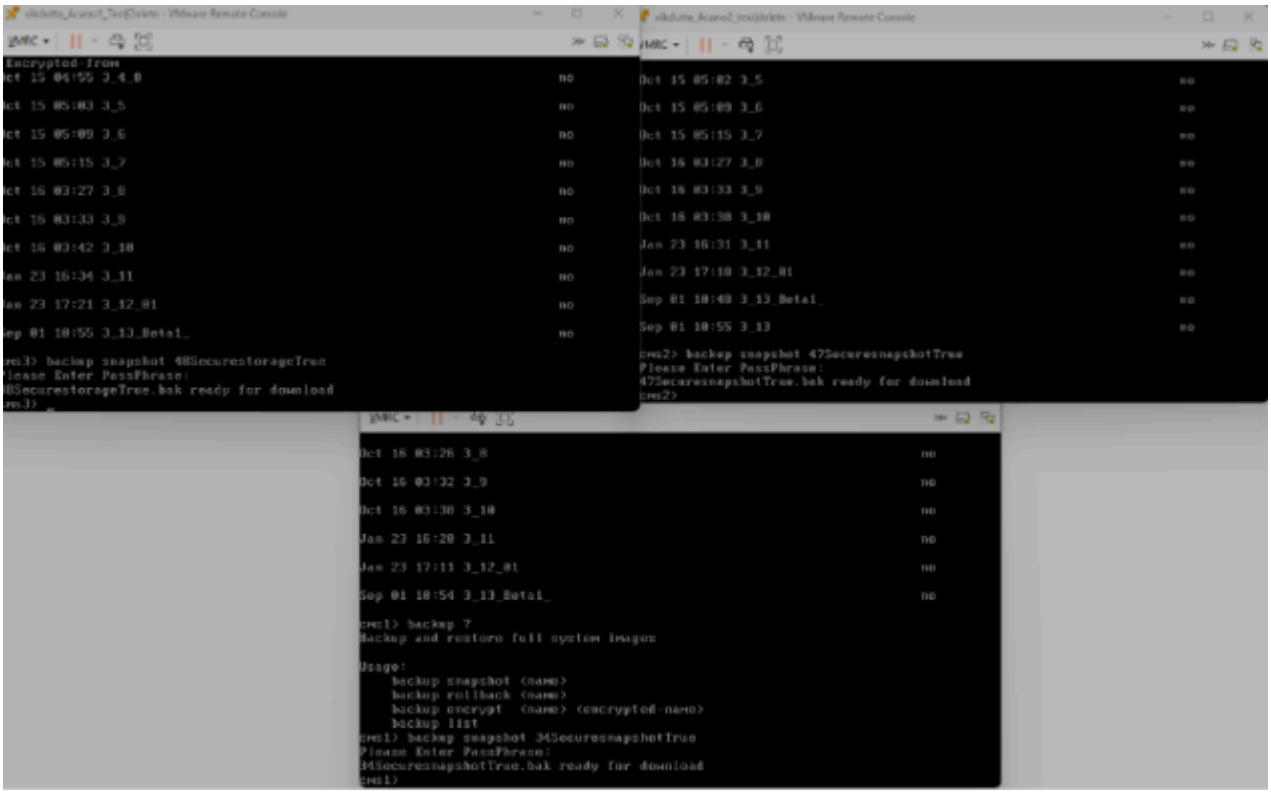


Abbildung 36: Verschlüsselter Backup-Snapshot auf jedem Knoten. Das Beispiel zeigt die Passphrase-Eingabeaufforderung und dann jede .bak-Datei zum Herunterladen bereit.

Auflösung, Upgrade und Wiederherstellung

Trennen Sie den Cluster wie in Szenario 3 beschrieben in der folgenden Reihenfolge: verbundene Knoten, Replikate und die primäre letzte. Verwenden Sie Datenbank-Cluster entfernen und bestätigen Sie, dass jeder Knoten den Cluster verlassen hat.

Parallele Aktualisierung der Standalone-Knoten. Stellen Sie die Netzwerkadressierung über die Konsole wieder her (Abschnitt "First-Boot" und "Network Restoration").

Laden Sie die verschlüsselte Sicherung jedes Knotens hoch. Vergewissern Sie sich vor einem Rollback, dass der hochgeladene Snapshot in der Sicherungsliste als verschlüsselt angezeigt wird: ja. Stellen Sie zuerst die erste primäre, dann die Replikate und die verbundenen Knoten wieder her. Verwenden Sie den Befehl backup rollback unten, bestätigen Sie Y, und geben Sie bei Aufforderung die Passphrase der Sicherung ein. Der Knoten wird neu gestartet, nachdem die Passphrase akzeptiert wurde. Wiederholen Sie den Vorgang für jeden Knoten.

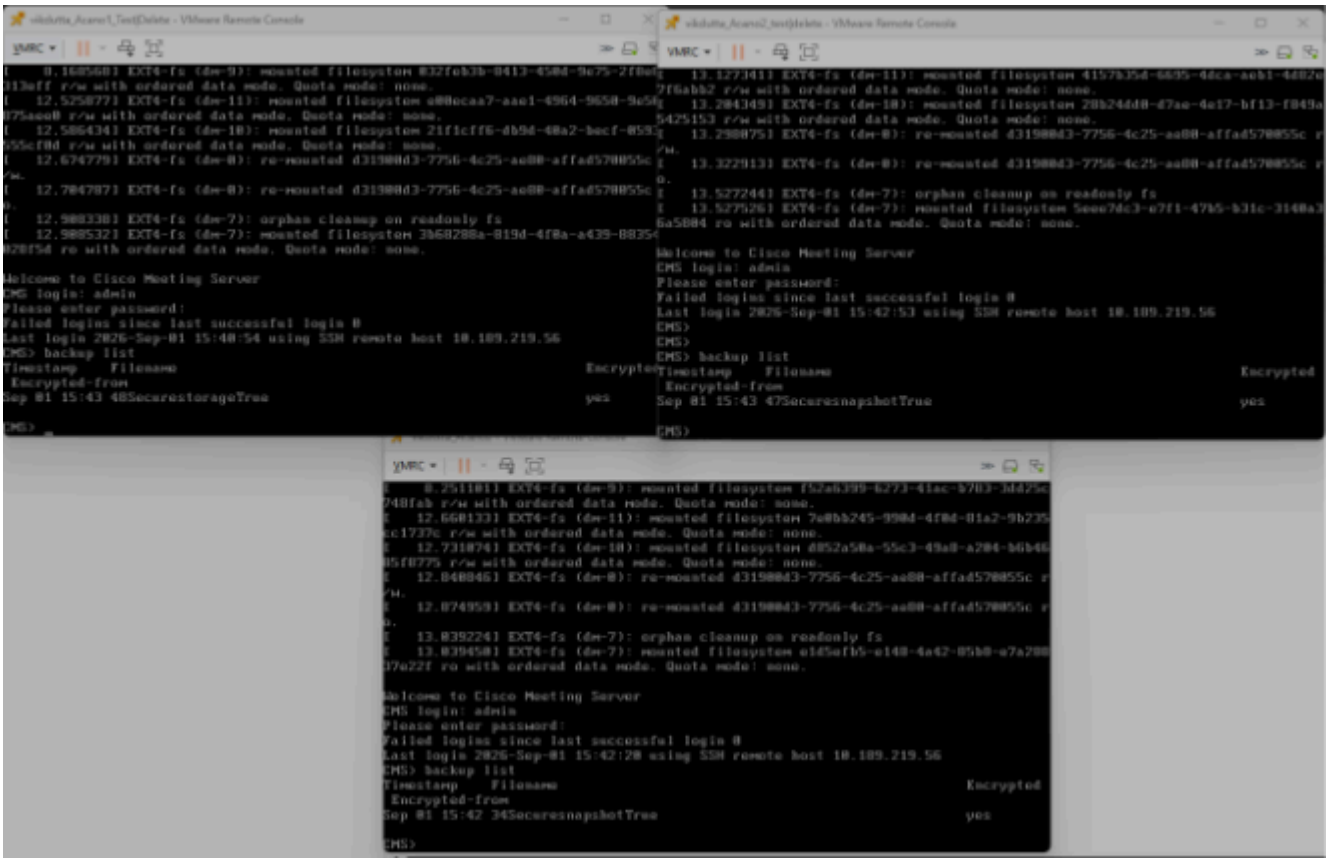


Abbildung 37: Nach dem ersten 4.0-Start muss der hochgeladene Snapshot in der Backup-Liste als verschlüsselt erscheinen: Ja, und seien Sie bereit für das Rollback.

backup rollback encrypted-filename

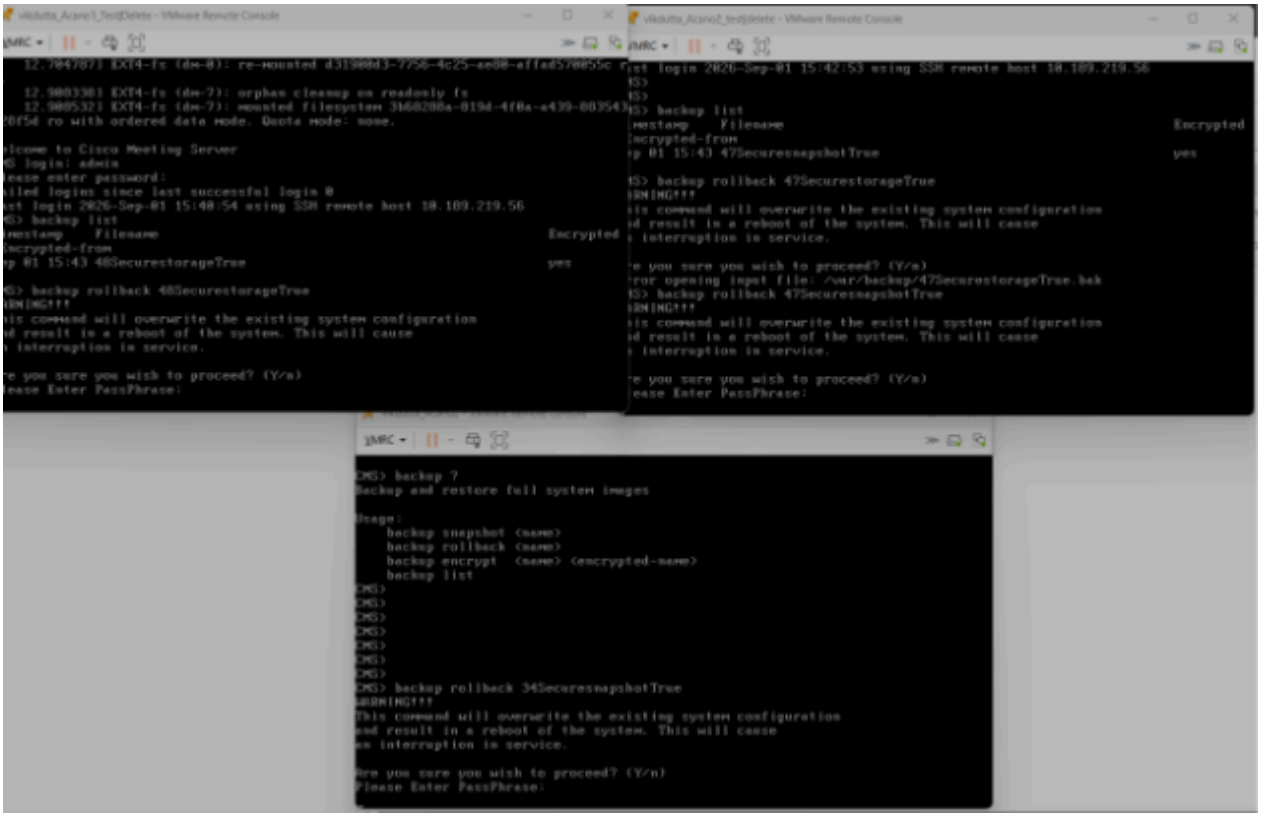


Abbildung 38: Bestätigen Sie Y, geben Sie die Passphrase ein, und stellen Sie zuerst die frühere primäre Passphrase wieder her.

Anmerkung: Wenn nach dieser Wiederherstellung keine Call Bridge-Clusterverbindungen mehr verfügbar sind, führen Sie das nur auf dem **database cluster upgrade_schema** vorherigen primären System aus, und überprüfen Sie dann erneut den Call Bridge-Status.

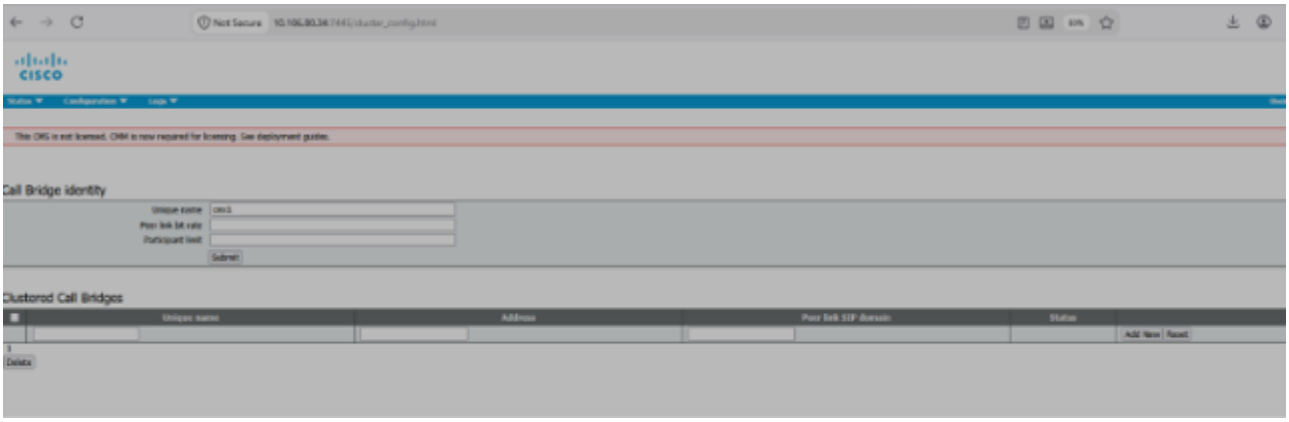


Abbildung 39: Vor der Schemaaktualisierung wird im Beispiel der Datenbankcluster angezeigt, der ausgeführt wird, während die Cluster-Anrufbrücken leer sind.

database cluster upgrade_schema

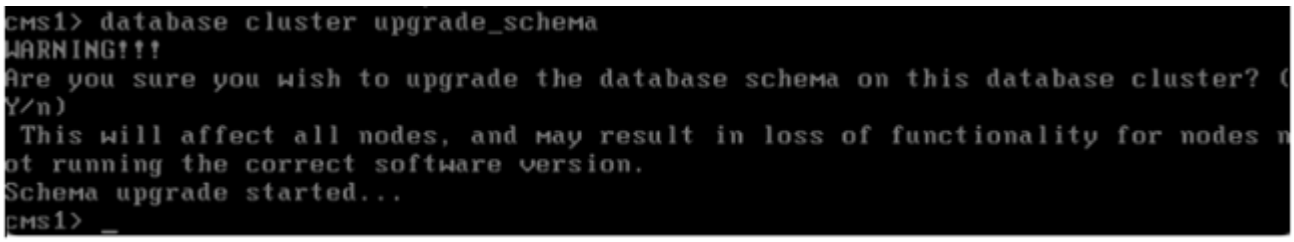


Abbildung 40: Bestätigen Sie auf dem ersten primären Gerät Y nur, wenn die Verbindung des Call Bridge-Clusters nach diesem Upgrade des aufgelösten Clusters fehlschlug.

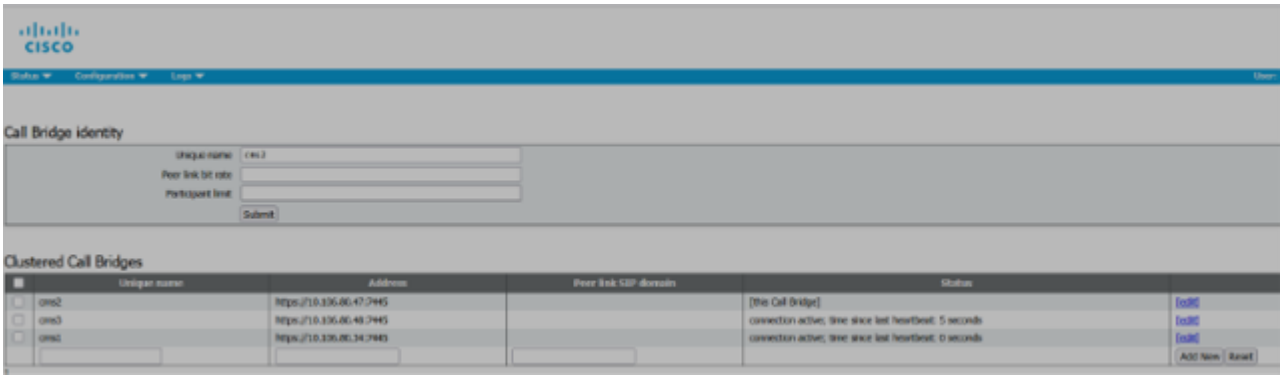


Abbildung 41: Überprüfen Sie nach dem Schema-Upgrade, ob jeder Call Bridge-Peer eine aktive Verbindung anzeigt.

Führen Sie das geheime Verfahren für MeetingApps im Abschnitt "Geheimer Schlüssel für MeetingApps nach der Wiederherstellung" auf jeder Web Bridge aus, und validieren Sie dann die Bereitstellung mithilfe des Abschnitts zur Validierung nach der Aktualisierung.

Validierung nach dem Upgrade

Vervollständigen Sie diese Checkliste nach der Wiederherstellung, bevor Sie das System wieder in Betrieb nehmen:

- "Web Admin" auf jedem Knoten zeigt Cisco Meeting Server 4.0 an.
- Erforderliche MMP-Dienste sind aktiviert und werden ausgeführt (aktiv: True).
- Die Fehlerbedingungen sind eindeutig. Behandeln Sie aktuelle Fehler und Warnungen als informativ, sofern kein entsprechender Fehler vorliegt.
- Falls zutreffend, zeigt der Datenbank-Cluster-Status die erwarteten primären und Replikate an.
- Smart Licensing und Call Bridge-Verbindungen werden wiederhergestellt.
- Die von dieser Bereitstellung unterstützten SIP- und Web App-Clientaufrufe wurden erfolgreich abgeschlossen.
- Branding, Audio-Aufforderungen und SSO-Dateien, die vom Server im Abschnitt Voraussetzungen vor dem Upgrade kopiert werden, werden wiederhergestellt, wenn sie nicht bereits in der Sicherung enthalten waren.
- Wenn MeetingApps bereitgestellt ist, zeigt Web Bridge die neue Beziehung zu MeetingApps und die Dateifreigabe an.
- Entfernen Sie kurzlebige Snapshots erst, nachdem die Bereitstellung akzeptiert wurde.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.