將會議伺服器升級到4.0版 — 白皮書

目錄

簡介

背景資訊

安全儲存概述

- 支援的平台
- 實施說明

升級原則和限制

- 所需的升級路徑
- 降級
- 4.0升級的關鍵備份要求
- 首次登入和密碼配置
- 升級後重新建立網路連線
- 在建立備份之前驗證伺服器運行狀況

升級前要求

通用備份和還原過程

- 4.0升級後受影響的資料
- 在安全儲存被禁用或不可用時進行備份
- 啟用安全儲存時進行備份
- 在4.0升級後恢複資料
- 還原後的MeetingApps金鑰

首次啟動和網路恢復

升級方案

- 方案1 — 禁用了安全儲存或無法使用安全儲存的單節點
- 案例2 — 啟用了安全儲存的單節點
- 方案3 — 禁用了安全儲存的資料庫群集
  - 記錄群集詳細資訊並備份每個節點
  - 解散集群
  - 升級和還原節點
- 場景4 — 已啟用安全儲存的資料庫群集
  - 記錄群集詳細資訊並建立加密備份
  - 解除、升級和恢復

升級後驗證

簡介

本檔案介紹如何將思科會議伺服器升級至4.0版。

背景資訊

請將此文檔與Cisco Meeting Server發行說明、 MMP命令參考指南以及Secure Storage Administrator Reference Guide結合使用，以瞭解要求和先決條件。

思科會議伺服器4.0的升級程式與之前的版本不同，因為套用映像會觸發節點的出廠重設。為了確保服務連續性，在開始升級之前，必須通過匯出到外部位置的備份來保留所有以前的配置（包括網路設定和密碼）。

此外，Secure Storage在Cisco Meeting Server 3.11到3.13版本中是可選的，但在版本4.0中預設處於啟用狀態。因此，如果您從未使用過Secure Storage，或者您已經在3.11x、3.12x或3.13x上啟用了Secure Storage，則必須執行不同的備份和恢復過程。

安全儲存會加密伺服器上的私鑰和備份檔案，並要求在將這些檔案傳輸到外部儲存之前對其進行加密。

本文檔將所需的指南整合到單個參考中，以便您可以遵循所有升級方案的通用過程，而無需重複相同的步驟。

本檔案介紹以下主題：

- 什麼是安全儲存，它適用於什麼地方，它不做什麼。
- 升級路徑，包括要求在4.0之前到達3.13.x，以及不支援從4.0降級的事實。
- 針對啟用了安全儲存的節點以及禁用或不可用的節點的通用備份和還原方法。
- 資料庫群集節點在升級前解散資料庫群集時，將解散排序。
- MeetingApps金鑰不儲存在思科會議伺服器備份中，必須在還原後重新生成。

附註：本文檔使用原始升級指南測試過程中捕獲的實驗室螢幕截圖，包括4.0測試版軟體版本。所有顯示的主機名、IP地址和檔名都是嚴格說明性的，並不反映實際的生產憑證或敏感密碼。為保持清晰度和防止冗餘，除非群集檢視提供其他必要的上下文，否則在通用過程部分中只顯示一次重複的步驟。

安全儲存概述

Secure Storage通過加密駐留在會議伺服器上的敏感檔案以及控制這些檔案從Call Bridge伺服器解除安裝的方式來提供增強的資料安全性。此功能在Cisco Meeting Server 3.11中作為可配置選項引入，在虛擬機器部署（基於規範或Meeting Server Small）和Meeting Server Medium上使用MMP命令secure_storage enable。

從4.0版開始，預設情況下啟用安全儲存。此設定現在是永久的，不可逆，並且secure_storage enable MMP命令已刪除。

使用安全儲存，會議伺服器會實施以下行為：

- 在對私鑰進行加密之前，無法通過SFTP下載它們。使用pki encrypt MMP命令以及至少14個字元的密碼短語對私鑰進行加密。這不會更改Meeting Server服務當前使用的金鑰。
- 使用backup encrypt <name> encrypted-name命令建立的備份檔案已加密。啟用安全儲存後，backup encrypt <name> encrypted-name MMP命令會提示輸入至少14個字元的密碼。備份還原期間需要相同的密碼短語。
- 下載備份檔案之前，必須採用加密形式。如果列出的備份尚未加密以進行匯出，請使用backup encrypt <name> encrypted-name。將拒絕嘗試下載未加密的備份。
- 從3.12版本起，安全儲存可以在啟用FIPS時運行。在3.11中建立的具有更短密碼短語的私鑰檔案必須使用至少14個字元的密碼重新生成。

提示：安全儲存限制從會議伺服器傳輸未加密的私鑰和未加密的備份檔案。它不會限制證書檔案的傳輸。憑證仍然可以使用SFTP複製；只有關聯的未加密私鑰才會被阻止，直到它們使用pki加密進行加密。

注意：啟用後，無法使用任何MMP命令禁用安全儲存。操作是不可逆的。僅factory_reset full 將Secure Storage重置為false。使用備份快照進行配置備份，並將其儲存在單獨的裝置上，然後啟用「安全儲存」。secure_storage啟用後，立即重新啟動。如果跳過重新啟動，則可以在未完全初始化的情況下將安全儲存標籤為啟用，並且factory_reset full 等命令可能會失敗。處於該狀態的恢復路徑將恢復到以前儲存的快照（這隻對3.13.x有效）。 在Meeting Server 4.0中，預設情況下啟用secure_storage。

支援的平台

- 虛擬機器（基於規範）：支援
- Meeting Server Small/1K:支援
- 會議伺服器媒體：支援
- 會議伺服器2000:不支援.安全儲存功能不可用。請勿在此平台上使用Secure Storage命令。

預設情況下，思科會議伺服器4.0在所有相容平台上啟用安全儲存。升級後，即使3.13.x備份是在禁用安全儲存時執行的，資料也會自動受到安全儲存的保護。

實施說明

- 重新命名升級映像不會更改Secure Storage設定。
- 進行備份之前，請使用命令secure_storage確認每個節點上的安全儲存狀態。
- 該命令報告安全儲存是否已啟用（真）或未啟用（假）。 在Meeting Server 2000上，該命令不適用；在升級Cisco Meeting Server 2000時，請按照升級條件中提到的步驟操作，其中Secure Storage被禁用或不可用。



未啟用Secure Storage時的MMP輸出(啟用：false)。



圖 2:啟用Secure Storage時的MMP輸出(啟用：true)。

詳細的命令語法警告和示例用法可在您當前使用的《Cisco Meeting Server管理員安全儲存快速參考指南》和《MMP命令參考》中找到。

升級原則和限制

所需的升級路徑

思科會議伺服器升級必須依照循序漸進的路徑進行，不能跳過主要版本。例如，3.11.x上的節點必須前進到3.12.x和3.13.x才能到達4.0。不支援從早期版本（如3.9.x到3.13.x或3.11.x到4.0）直接升級，這通常會導致無法恢復的配置錯誤。對於版本為3.11.5或3.13的Meeting Server Medium，升級路徑為3.11.5 → 3.13 → 4.0。

提示：啟動4.0升級之前，每個節點都必須運行思科會議伺服器3.13.x，並且從該3.13.x系統匯出經驗證的配置備份。本文中所有場景過程均假設已完成了到3.13.x的逐步升級。

降級



提示：不支援從4.0.x降級到3.13.x。如果升級失敗或系統無法按預期工作，請部署新的3.13.x OVA（或重新映像裝置）並恢復3.13.x備份。在升級視窗的持續時間內保留3.13.x虛擬機器的虛擬機器管理程式快照作為額外的恢複選項。VM快照不會替換匯出的配置備份。

4.0升級的關鍵備份要求

在確認4.0升級後，節點將重新引導到第一個引導狀態。不要依賴於升級過程中生成的自動備份，因為升級失敗可能會導致SFTP訪問丟失，並使檔案無法訪問。只有使用backup snapshot 命令建立並複製到外部儲存的備份才能可靠地用於恢復。

首次登入和密碼配置

第一次啟動4.0版時，將從資料庫中刪除現有的MMP密碼。使用使用者名稱admin和空白密碼（無密碼）登入。 系統要求您設定新的MMP密碼。系統會提示您輸入兩次密碼以進行驗證和確認。由於Meeting Server沒有密碼恢復功能，請確保錄製新密碼。

附註：如果您在首次啟動時設定新的MMP密碼，backup rollback命令會將其替換為3.13.x備份中儲存的密碼。在伺服器上恢復備份後，必須使用建立備份時處於活動狀態的密碼登入。

升級後重新建立網路連線

IPv4和IPv6地址、掩碼和網關會隨配置的其餘部分一起丟失。升級到4.0後，會丟失會議伺服器的網路連線。您必須擁有虛擬機器監控程式控制檯、CIMC或串列訪問，以便可以再次從MMP分配定址。



附註：使用DHCP保留的部署通常會在重新啟動後保留相同的IP地址。但是，在驗證地址之前，控制檯訪問必須保持可用。在確認IP地址之前，不要假設SSH連線已恢復。

在建立備份之前驗證伺服器運行狀況

每次逐步升級到3.13後，請確保伺服器處於正常狀態，並且所有服務都在工作。不要忽略伺服器概述頁面上的任何故障情況。如果您遇到任何錯誤/故障，請在3.13上建立備份快照之前修復這些錯誤。這可確保在升級的4.0節點上還原正常的伺服器備份，從而避免部署錯誤。

在Web Admin上，開啟狀態並確認「Fault conditions（故障條件）」部分已清除。忽略僅顯示在「最近發生的錯誤和警告」下的條目。升級後，通常會在那裡看到臨時資料庫或Web Bridge消息；這

些不是還原或延遲備份的理由。

如果故障狀態保持時間超過大約10分鐘，請在進行備份之前解決此問題。將已經包含故障的3.13.x備份恢復到4.0後，這些故障就會繼續發生。

對於群集系統，請確認所有正在使用的呼叫型別（SIP終端和Web應用客戶端）都工作正常，並且任何節點上都沒有列出任何故障條件。

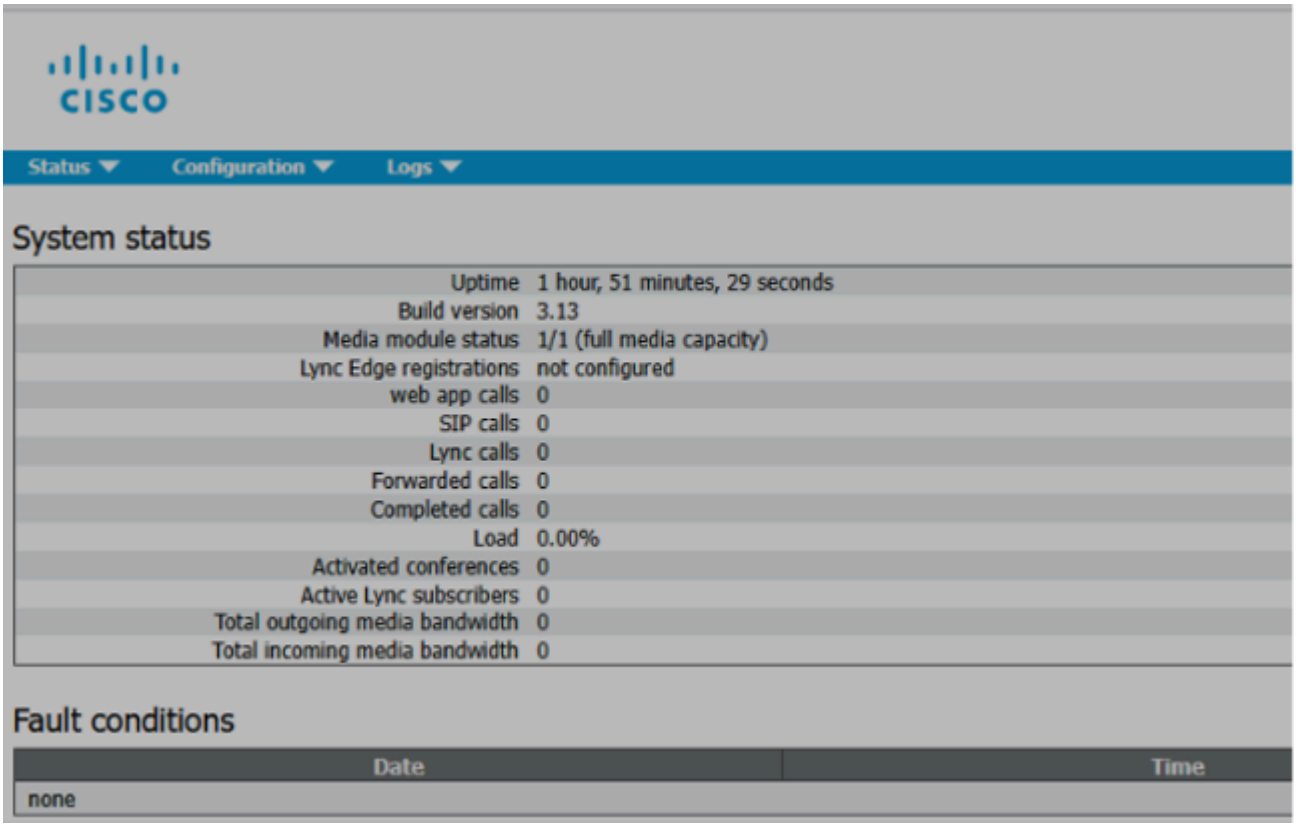


圖 3:3.13.x上的「Web管理狀態」頁，故障條件為空。在獲取已還原到4.0的備份之前，請使用此檢視。

升級前要求

開始升級到版本4.0之前，請完成以下操作。這些要求適用於本文檔後面介紹的所有四種方案。

- 升級到3.13.x，然後匯出配置備份。確保節點正在運行Cisco Meeting Server 3.13.x。建立備份並將其與所有自定義SFTP資料（如徽標、品牌檔案、音訊提示、SSO檔案以及任何其他自定義資料）一起傳輸到外部儲存。使用通用備份和還原過程一節中的過程。在群集環境中，從每個節點（不僅是已連線的主節點，還包括已連線副本）獲取備份。
- 記錄網路設定。執行ipv4 a 並儲存輸出。在4.0重新啟動後，您必須從控制檯重新輸入此資訊，除非DHCP保留自動恢復IP地址。
- 確認控制檯訪問。啟動之前，虛擬機器監控程式控制檯、CIMC或串列訪問必須可用。當節點重新引導至4.0時，SSH應會斷開。

- 下載當前用於存檔的日誌捆綁包。從每個節點儲存logbundle.tar.gz。該捆綁包不能替代備份快照。
- 執行upgrade命令後顯示時，請閱讀4.0升級警告標語。
- 如果任何先決條件不完整，請按n中止。只有在準備繼續時，才按Y。

通用備份和還原過程

本文稍後討論的四個升級方案使用相同的備份、匯出、首次啟動和還原模式。使用此部分作為這些步驟的單一來源，然後僅按照場景特定的順序執行（單節點與群集以及是否已啟用安全儲存）。

4.0升級後受影響的資料

4.0升級後此資料將丟失，直到您還原備份：

- 資料庫內容，包括空間、使用者和呼叫配置檔案。
- 證書和私鑰。
- 本地自定義、SSO檔案和音訊提示檔案。
- 網路配置（IP地址、掩碼和網關），但DHCP保留恢復地址時除外。
- 以前的MMP密碼，直到備份回滾從備份重新應用該密碼。
- Call Bridge、Web Admin、Web Bridge和其他應用程式服務僅在恢復後返回。



提示：思科會議伺服器備份不包括MeetingApps金鑰。恢復後，必須重新生成該金鑰並將其應用到每個Web橋節點。請參見MeetingApps Secret Key After Restore部分。

在安全儲存被禁用或不可用時進行備份

在虛擬機器、Meeting Server Small和Meeting Server Medium(其中secure_storage報告已啟用)上，請執行以下步驟：False，在Meeting Server 2000上安全儲存不可用。

1.在每個節點上，使用backup snapshot命令建立檔案。不要重複使用以前的檔名。

2.立即使用SFTP將備份檔案複製到外部儲存器。請勿在會議伺服器上保留唯一的副本。

3.將檔案儲存在重建節點後仍可訪問的位置。

範例：

backup snapshot cms313SecurestorageFalse backup list

4.確認檔案顯示在backup list命令中，然後使用SFTP客戶端將其傳輸到外部磁碟。

5.在群集中的每個節點上重複此過程。備份名稱只能包含字母、數字、下劃線和連字元。建立備份檔案時不要包含.bak副檔名。例如，由於句點，諸如3.13SecurestorageFalse的檔名被拒絕。

```
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>
```

圖 4:備份快照將拒絕包含句點的名稱，然後使用字母數字名稱后繼該名稱。然後.bak檔案即可下載。



圖 5:將.bak檔案從會議伺服器SFTP根目錄複製到外部儲存。請勿將唯一的副本留在伺服器上。

啟用安全儲存時進行備份

當secure_storage報告Enabled時，請使用此過程：True.無法下載未加密的備份檔案。

1.在每個節點上創建備份快照。啟用「安全儲存」後，伺服器會提示輸入至少14個字元的密碼。密碼可以包含字母、數字、特殊字元、符號或空格。

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

圖 6:啟用安全儲存的備份快照會提示一次至少包含14個字元的密碼。MMP不要求您確認。

2. MMP不會要求您重新輸入密碼進行確認。請根據還原檔案所需的相同密碼保護您的密碼短語。請勿選擇簡單密碼或示例密碼短語。

3.如果backup list命令顯示尚未加密以進行匯出的快照，請在下載快照之前對其進行加密：

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

圖 7:加密前的備份清單。Encrypted（已加密）列為no（否），因此無法下載檔案。

4.如果您嘗試下載未加密的備份，SFTP將返回許可權拒絕錯誤，並指示您先運行backup encrypt命令。

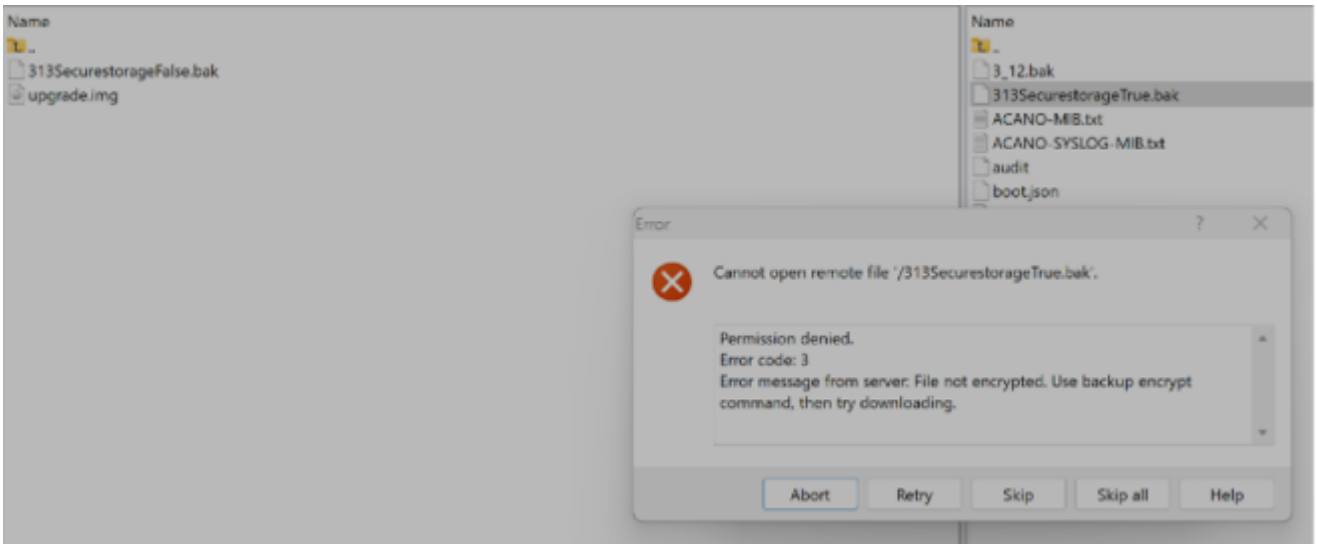


圖 8:啟用安全儲存時，SFTP拒絕下載未加密的備份。伺服器消息指示您運行backup encrypt。

5.執行backup encrypt命令以加密備份檔案。

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

圖 9:加密快照之後的備份清單。Encrypted為yes，並可以使用SFTP傳輸檔案。

備份清單顯示加密狀態和原始檔名。請確保僅從群集中的每個節點傳輸加密檔案。維護每個節點的有組織記錄、其對應檔名和相關聯的密碼。

如果您還需要匯出私鑰，請先加密每個金鑰。安全儲存不會阻止證書檔案，並且可以在不執行此額外步驟的情況下複製這些檔案：

pki encrypt private.key encrypted_private.key

使用唯一的檔名，而不是覆蓋服務當前使用的金鑰。此處也適用最低14個字元的密碼要求。

在4.0升級後恢複資料

1.首次啟動登入和網路恢復後，在首次啟動和網路恢復部分中，將相應的3.13.x備份複製到使用SFTP的節點上，然後進行恢復。

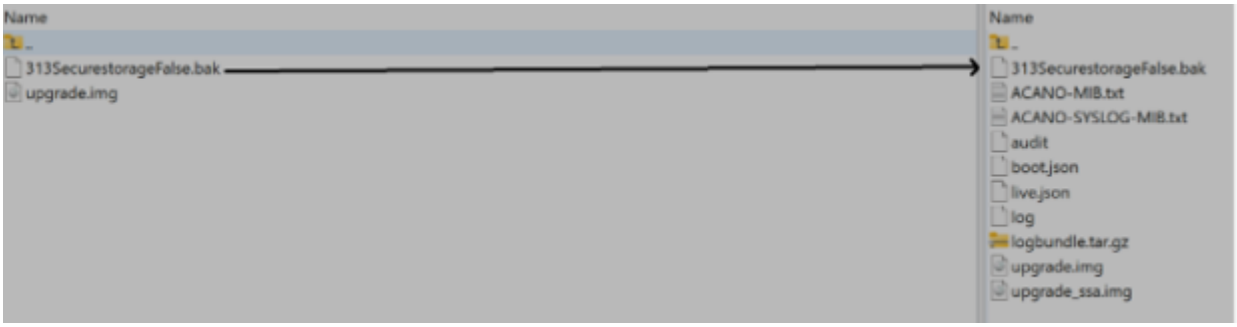


圖 10:首次啟動網路恢復後，使用SFTP將3.13.x .bak檔案複製回4.0節點。

2.確認檔案是否存在：

備份清單

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

cms-3120>
```

圖 11:4.0上的備份清單，確認在回滾之前已上載快照。

3.恢復快照。在群集部署中，首先恢復以前的資料庫主節點，然後恢復複製副本，最後恢復連線的節點。

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...
```

圖 12:未加密快照的備份回滾。與Y確認；節點提取備份並重新引導。

4.按Y繼續。節點在提取備份時重新啟動。如果在啟用安全儲存的情況下進行備份，則MMP會提示輸入密碼。只有在接受正確的密碼後，重新啟動才會繼續。

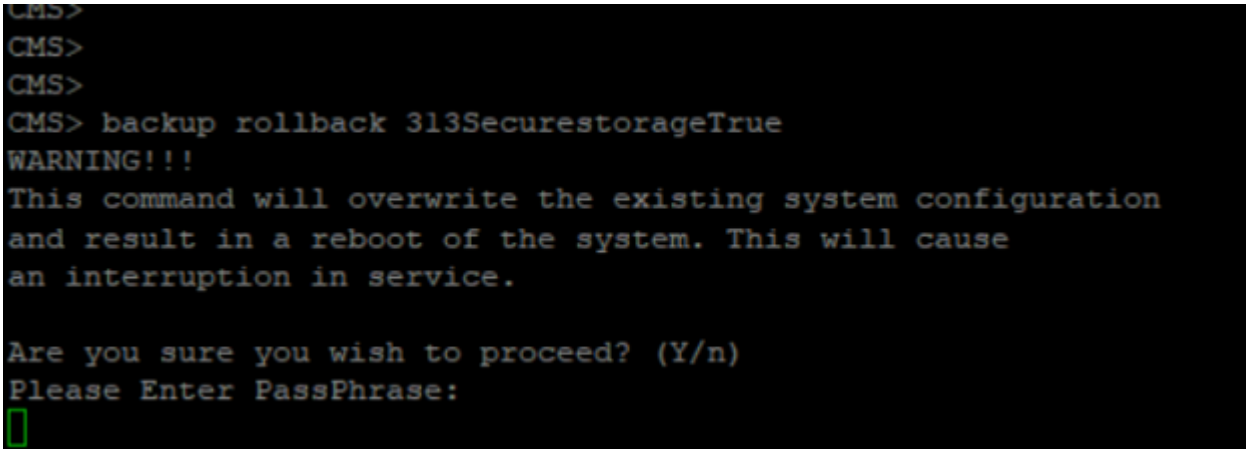


圖 13:加密快照的備份回滾。在Y之後，MMP會提示輸入建立備份時使用的密碼。

⚠ 注意：覆蓋**backup rollback**當前配置、證書、私鑰和許可證檔案，然後重新啟動伺服器。僅將其與為此升級匯出的3.13.x備份結合使用。

5.當節點重新聯機時，使用備份中的MMP憑據登入，並確認每個必需的服務報告均已啟用且正在運行(MMP將以下內容顯示為活動：正確)。

典型檢查：

callbridge webbridge3 webadmin scheduler recorder streamer uploader meetingapps

6.只對此節點應承載的服務運行命令。

還原後的MeetingApps金鑰

思科會議伺服器備份不儲存MeetingApps金鑰。備份回滾完成後，重新生成該金鑰，並將其應用到每個Web Bridge節點。跳過此步驟會導致檔案共用不可用，即使其他服務看起來正常。

1.在MeetingApps節點上，執行meetingapps gensecret命令。

2.將生成的金鑰複製到您的金鑰庫。每次執行meetingapps gensecret都會使先前的金鑰失效，因此

生成金鑰一次並在所有Web網橋中重複使用相同的值。

3.在每個Web Bridge節點上執行以下命令：

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

最後一個命令確認Web Bridge服務正在運行，並且已正確配置MeetingApps。Meeting Server 2000不支援MeetingApps，並且檔案共用在包含Meeting Server 2000的群集中不可用。在此類部署中，此步驟不適用。

首次啟動和網路恢復

4.0 upgrade命令在繼續之前會顯示警告標語。請仔細檢視該訊息，如果有任何先決條件未完成，則以n中止。如果繼續使用Y，節點將重新啟動，SSH會話將斷開，並且必須從控制檯完成其餘步驟。

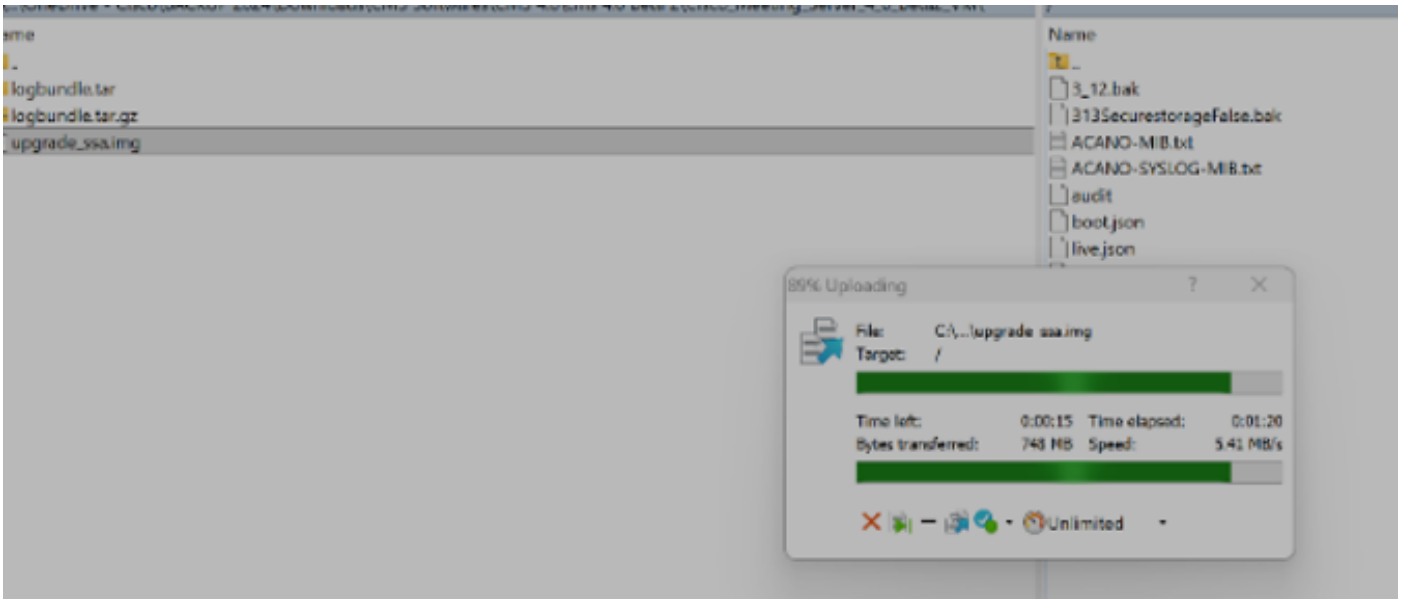


圖 14:將4.0升級映像上傳到會議伺服器SFTP根目錄。升級映像檔名的不同之處取決於從cisco.com下載的軟體包。

```
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...
```

圖 15:upgrade命令驗證映像簽名並啟動進程。不要依賴此時建立的自動備份。

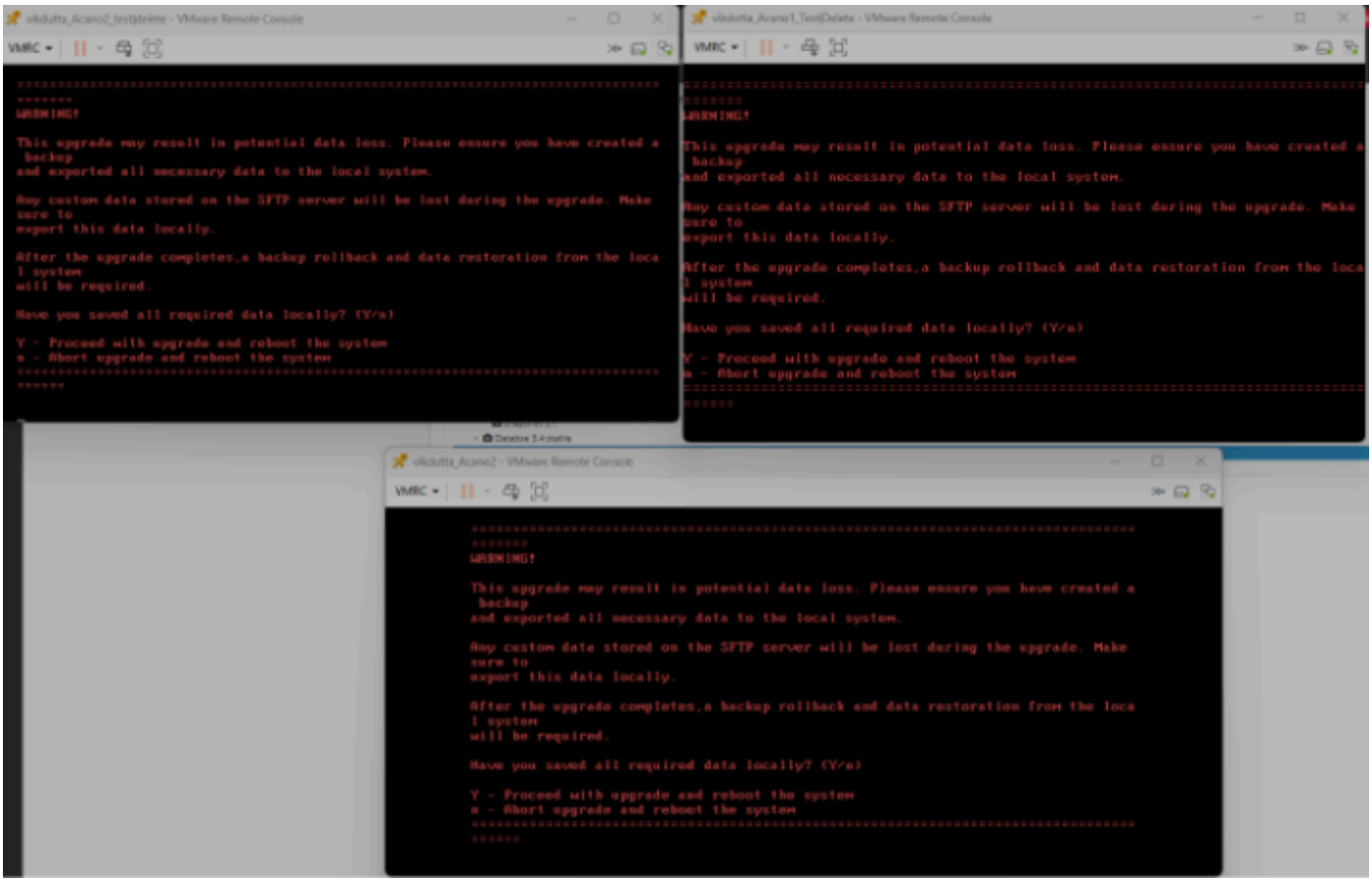


圖 16:三節點群集上的紅色MMP警告。同一個標語出現在單個節點上。如果備份和自定義資料未離開伺服器，請按n中止。僅按Y繼續並重新啟動。

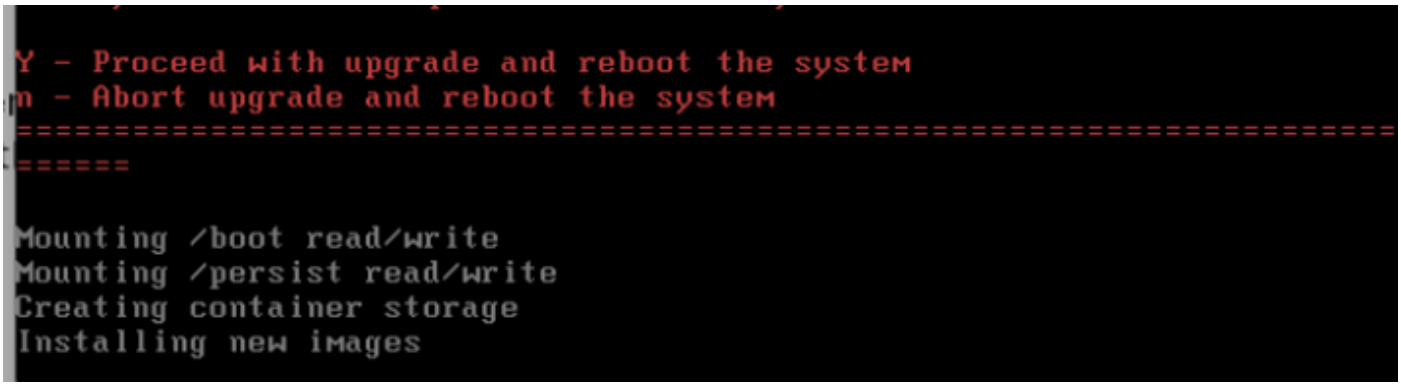


圖 17:在Y之後，節點將裝載儲存並安裝4.0映像。SSH會話超時；從hypervisor控制檯繼續。

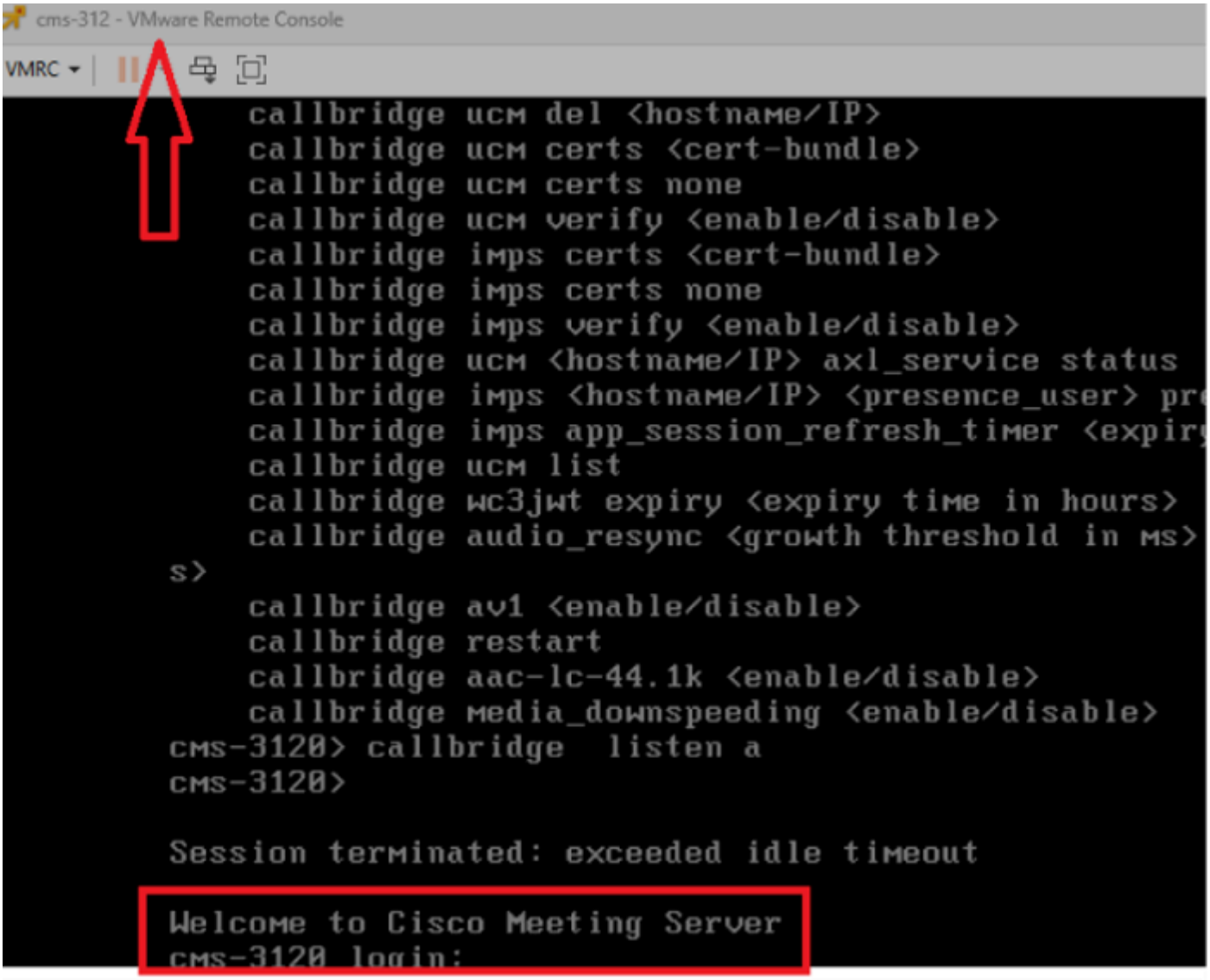


圖 18:SSH丟棄後使用VM或CIMC控制檯。當4.0映像準備就緒時，系統會顯示首次啟動登入提示。

1.使用首次引導MMP帳戶(使用者名稱admin和無密碼)登入，然後在系統提示時設定新的MMP密碼。請注意，備份回滾會用儲存在備份中的密碼替換此密碼。

2.根據在「升級前要求」部分中捕獲的註釋重新應用網路配置：

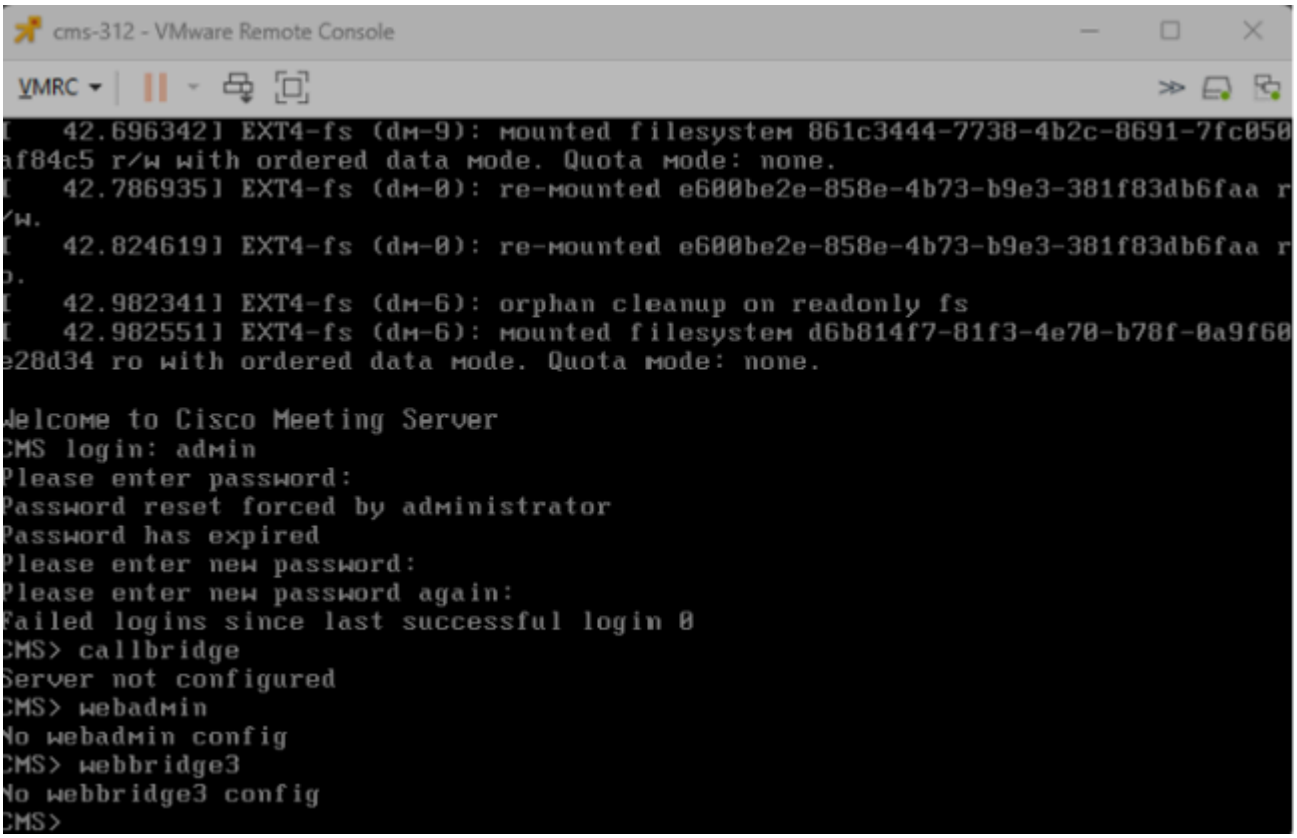


圖 19:首次啟動MMP登入。

以前的密碼不再有效。設定新密碼後，在還原備份之前，webadmin和webbridge3等服務會顯示為未配置。

3.執行命令：

ipv4 interface add address/prefix-length gateway

舉例來說：

ipv4 a add 192.0.2.10/24 192.0.2.1

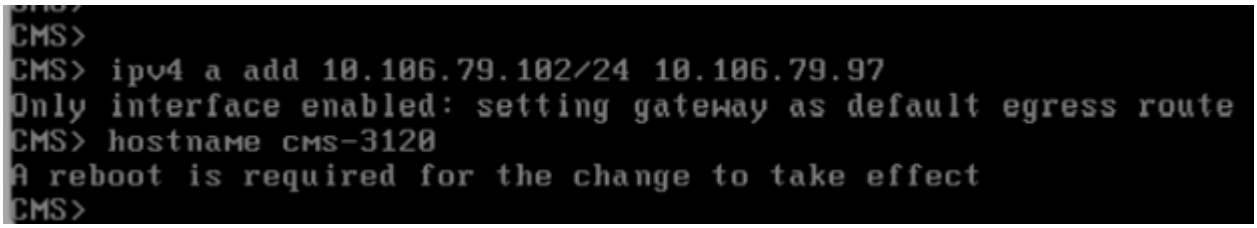


圖 20:從控制檯重新應用IPv4。

分配地址後需要重新啟動。螢幕截圖中顯示的地址僅用於示例目的。

4.分配地址後重新啟動。系統重新聯機後，繼續備份的SFTP上傳和Restore Data After 4.0 Upgrade一節中提到的恢復步驟。

附註：如果配置了DHCP保留，則可以在重新啟動後分配原始地址。從管理工作站啟ipv4 a動SFTP會話之前，請使用驗證該地址。

在Cisco Meeting Server 4.0上，在支援安全儲存的平台上預設啟用安全儲存。升級後，MMP無法再將secure_storage公開為切換開關。



圖 21:在此4.0映像上，secure_storage不是可識別的命令，因為預設情況下啟用了Secure Storage。

使用version指令確認版本。

升級方案

本章介紹不同的升級方案。完成升級到3.13.x的步驟。確定您的部署型別，並相應地選擇方案。僅遵循與您的環境相匹配的過程，不要將集群和單節點部署中的步驟組合在一起。

首先完成支援的逐步升級到3.13.x。然後僅選擇下面的一個方案。不要將單節點和資料庫群集過程結合起來。

- 案例 1:單節點、已禁用或不可用、虛擬機器、小型、中型和會議伺服器2000
- 案例 2:單節點、已啟用、虛擬機器、小型和中型
- 案例 3:資料庫群集、已禁用或不可用、虛擬機器、小型、中型和會議伺服器2000
- 案例 4:資料庫群集，僅啟用、VM、小型和中型

Meeting Server 2000不支援啟用安全儲存的方案。對於該平台，請使用場景1或3（如果適用）。

方案1 — 禁用了安全儲存或無法使用安全儲存的單節點

對於已禁用Secure Storage的獨立伺服器或無法使用Secure Storage的Meeting Server 2000，請使

用此過程。源版本可以是3.11.x或更高版本，但節點必須位於3.13.x上才能升級到4.0。

1.逐步升級到3.13.x。遵循支援的路徑(例如3.11.x → 3.12.x → 3.13.x)。 在每一跳之後，在Web Admin中確認該版本，確認故障條件已清除，如Validate Server Health Before Creating Backups一節所述。

2.確認「安全儲存」狀態。運行secure_storage命令並驗證是否已啟用安全儲存。跳過Meeting Server 2000上的命令。

3.建立並匯出3.13.x備份檔案，如Take a backup When Secure Storage is Disabled or Unavailable部分所述。此外，還可匯出在升級前要求一節中提到的自定義SFTP內容和日誌捆綁包。

4.從Cisco.com下載4.0軟體映像，提取該映像，並通過SFTP將upgrade.img複製到節點。

5.使用以下命令開始升級：

```
upgrade upgrade.img
```

6.閱讀警告橫幅。僅在完成所有前提條件後按Y。6.升級後，按照首次啟動和網路恢復一節所述配置節點，然後使用Restore Data After 4.0 Upgrade一節恢復備份。

案例2 — 啟用了安全儲存的單節點

對於啟用了安全儲存的獨立VM、Meeting Server Small或Meeting Server Medium，請使用此過程。它不適用於會議伺服器2000。

從伺服器傳輸檔案之前，請注意，無法傳輸未加密的私鑰和未加密的備份檔案。未阻止證書檔案。

1.在不跳過版本的情況下，通過受支援的路徑升級到3.13.x。在每一跳之後，在建立備份之前驗證伺服器健康狀況部分中確認版本並清除故障條件。

2.運行secure_storage，並確認輸出顯示Enabled:True.

3.使用啟用安全儲存時備份部分，建立和匯出加密的3.13.x備份。將其密碼儲存在您的秘密儲存中。同時匯出自定義SFTP內容和日誌捆綁包(升級前要求部分)。

4.將upgrade.img複製到節點並運行升級：

```
upgrade upgrade.img
```

5.閱讀警告標語，然後按Y以僅在完成先決條件時繼續。

6.從控制檯恢復網路(「首次啟動和網路還原」部分)，然後使用加密的備份的密碼恢復該備份(「在4.0升級後恢複資料」部分)。6.如果正在使用MeetingApps，請應用新的MeetingApps金鑰(還原後的MeetingApps金鑰部分)。

Meeting Server 4.0預設啟用安全儲存。還原後，繼續將私鑰和備份檔案作為加密資料處理。

方案3 — 禁用了安全儲存的資料庫群集

對於禁用「安全儲存」的資料庫群集（包括包含Meeting Server 2000的群集），請使用此過程。從3.5版本開始，必須在軟體升級之前解散資料庫群集。首先，逐步將每個節點升級到3.13.x。

記錄群集詳細資訊並備份每個節點

1.在每個節點上運行secure_storage。將該命令視為在Meeting Server 2000節點上不可用。

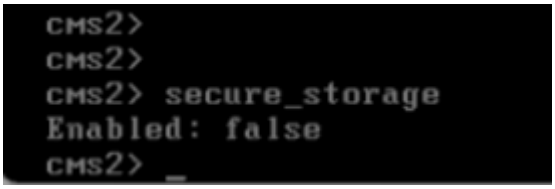


圖 22:在使用未加密的備份之前，請確認每個群集節點上都禁用了安全儲存。跳過不可用的Meeting Server 2000節點的命令。

2.記錄當前資料庫主節點，因為在升級到4.0之後，必須首先還原它。確認副本處於「同步」狀態，並且群集狀態正常。

```
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)
```

圖 23:記錄當前主副本並確認副本處於同步狀態。

3.確認所有正在使用的呼叫型別都工作正常，並且每個節點上的故障條件均已清除(在建立備份之前驗證伺服器運行狀態部分)。

4.使用Take a Backup When Secure Storage is Disabled or Unavailable部分為每個節點建立備份。命名每個檔案，以便它清楚地對映到其節點，並在您解散群集之前將每個備份傳輸到外部儲存。

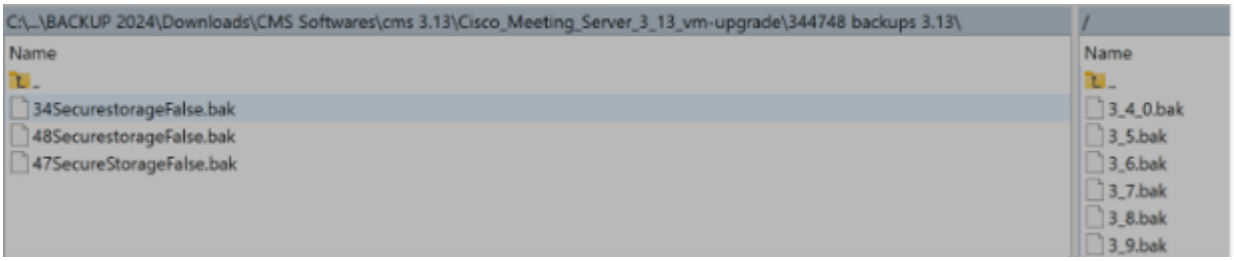


圖 24:所有三個示例節點備份都儲存外部儲存，命名為以便每個檔案對映到其節點。

解散集群

按此順序刪除節點。將主節點保留到最後：

- 已連線（非核心）會議伺服器節點
- 副本資料庫節點
- 主資料庫節點

在每個節點上，運行刪除命令，然後按Y。在每個節點報告其已離開群集之前，不要繼續執行4.0升級。刪除群整合員資格後，該節點的本地資料庫就位。

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
```

圖 25:在複製副本上，確認Y以刪除群整合員身份。節點的本地資料庫保持不變。

```
 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
```

圖 26:刪除後，請確認該節點上的群集狀態為Disabled且Node in use為None。

```
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)
```

圖 27:刪除複製副本後，前一個主節點是群集中剩下的唯一節點。最後刪除它。

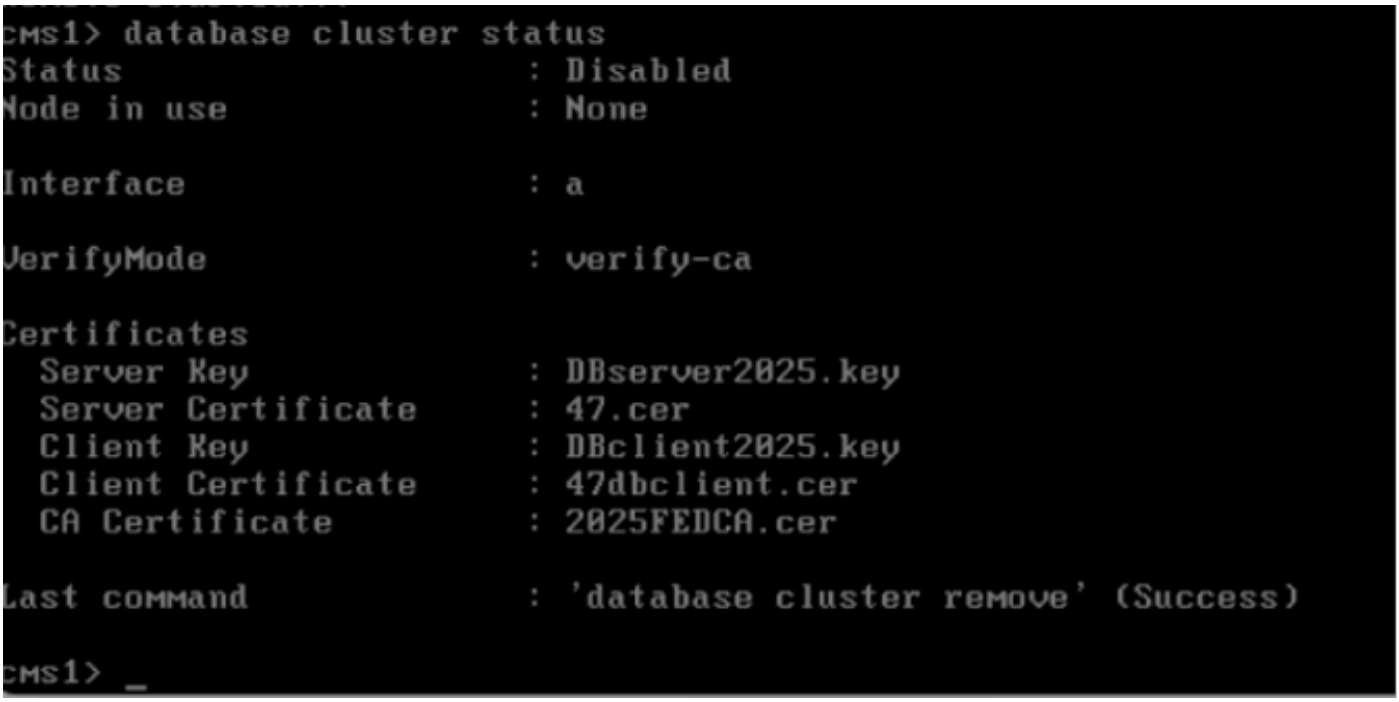


圖 28:刪除前一個主節點後，驗證該命令是否報告Success（成功），並且群集狀態為Disabled（禁用）。

升級和還原節點

1.一旦解散，節點將獨立，並且可以並行升級。在每個節點上，通過SFTP複製upgrade.img並運行upgrade命令：

upgrade upgrade.img

2.從控制檯恢復每個節點的網路編址(首次啟動和網路恢復部分)。

3.將每個節點自己的3.13.x備份複製回該節點。首先恢復前一個主節點，然後恢復複製副本，再恢復連線的節點。使用Restore Data After 4.0 Upgrade部分。備份的還原將重新建立資料庫群整合員身份。

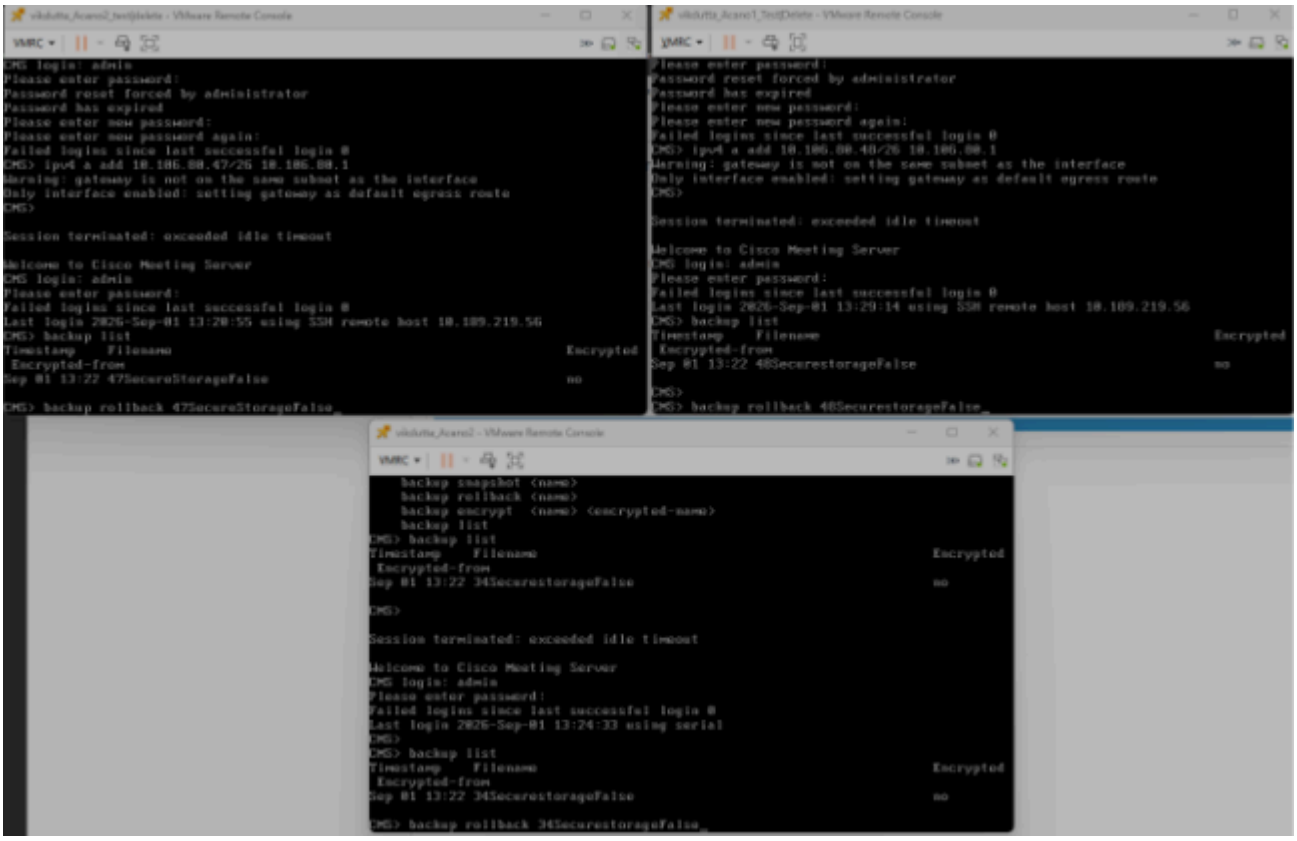


圖 29:恢復每個節點自己的快照。從原來的主副本開始，然後恢復副本。示例檔名標識其節點。

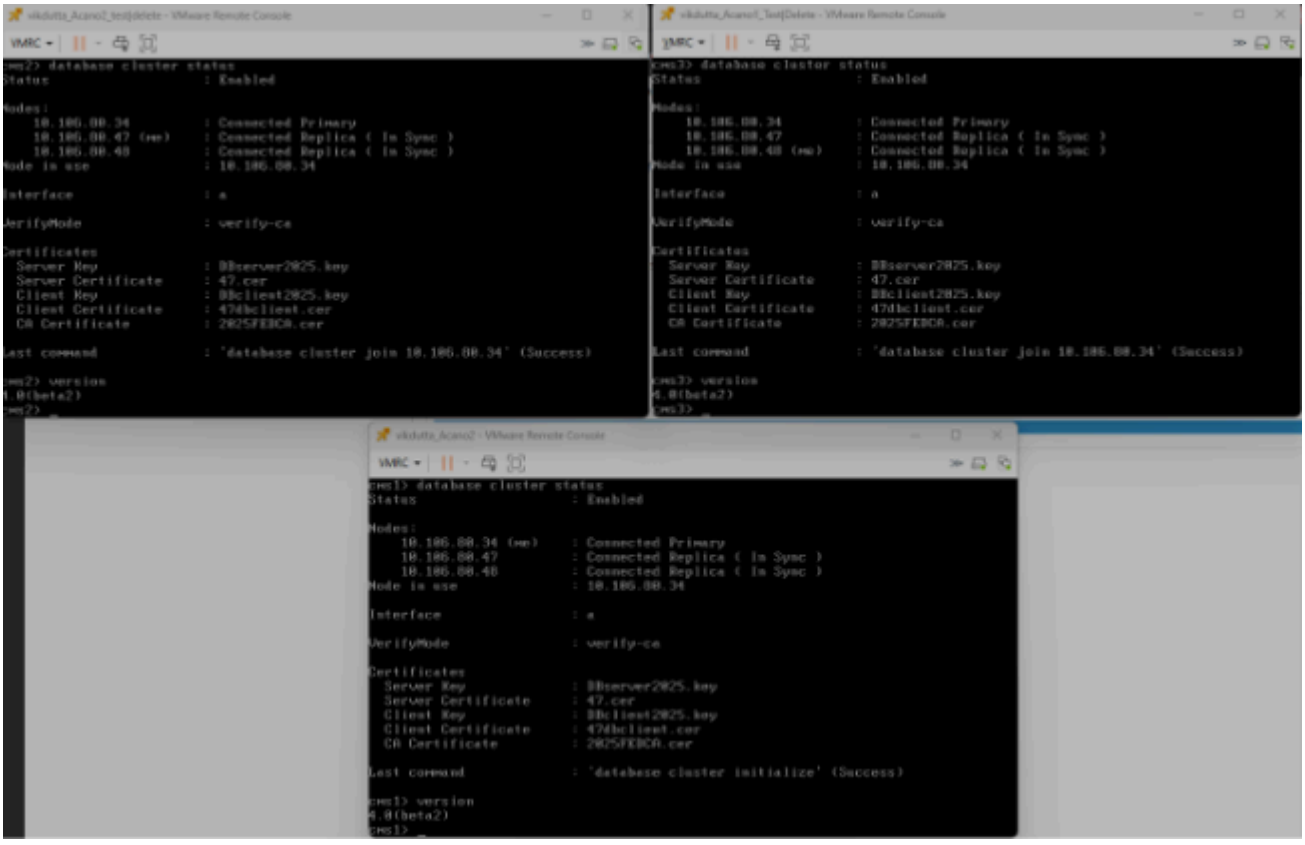


圖 30:在Meeting Server 4.0上恢復後，驗證群集是否已啟用，是否顯示相同的主群集，以及複製副本是否處於同步狀態。

附註：如果在此恢復後呼叫網橋群集連線沒有啟動，請僅對前一個主節點運行**database cluster upgrade_schema**，然後重新檢查呼叫網橋狀態。

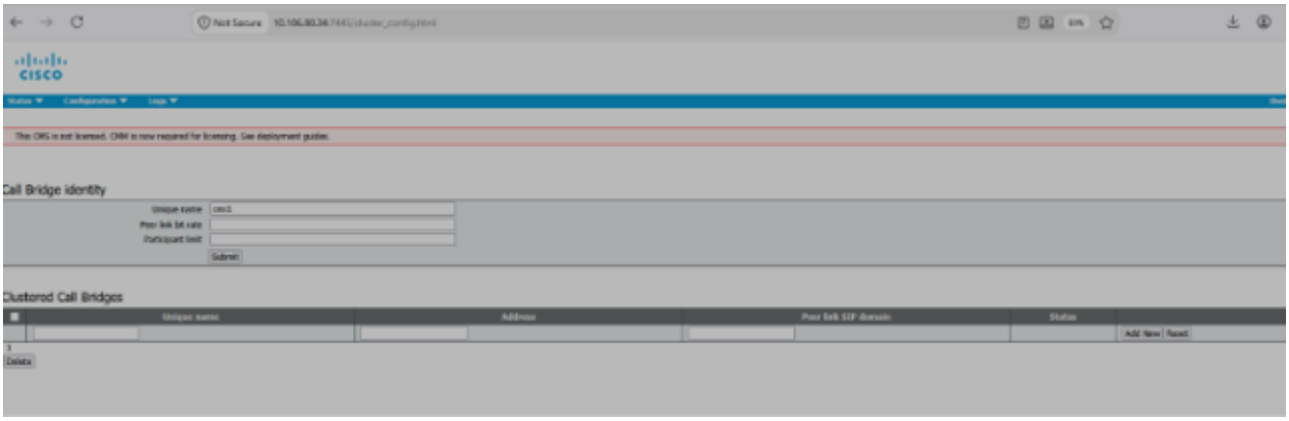


圖 31:在模式升級之前，該示例顯示了當集群呼叫網橋為空時正在運行的資料庫集群。

database cluster upgrade_schema

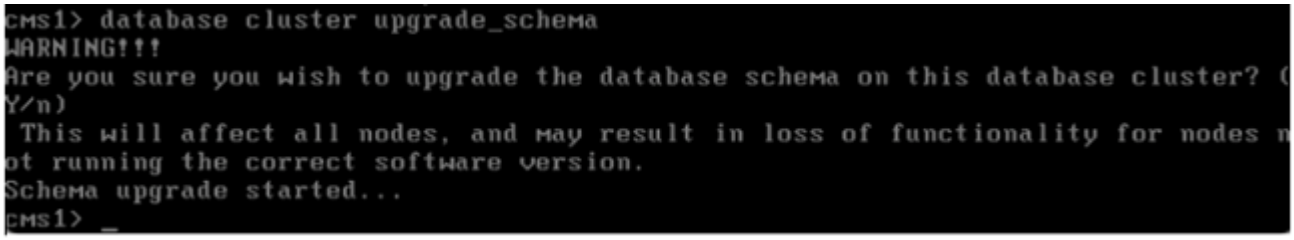


圖 32:在原來的主群集上，僅當在此已解散群集升級後Call Bridge群集連線失敗時確認Y。

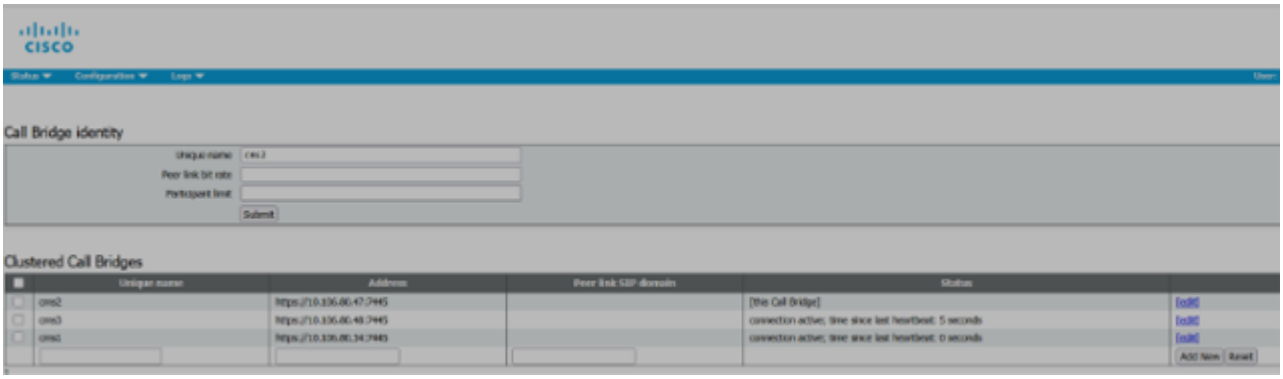


圖 33:架構升級後，驗證每個呼叫網橋對等體是否顯示活動連線。

4.在每個Web Bridge上，完成MeetingApps Secret Key After Restore部分中的MeetingApps加密過程，然後使用Post-upgrade Validation部分驗證部署。

場景4 — 已啟用安全儲存的資料庫群集

對節點上啟用了安全儲存的VM、Meeting Server Small或Meeting Server Medium上的資料庫群集使用此過程。它不適用於會議伺服器2000。首先，逐步將每個節點升級到3.13.x。

記錄群集詳細資訊並建立加密備份

1.在每個節點上運行secure_storage並確認已啟用：True.

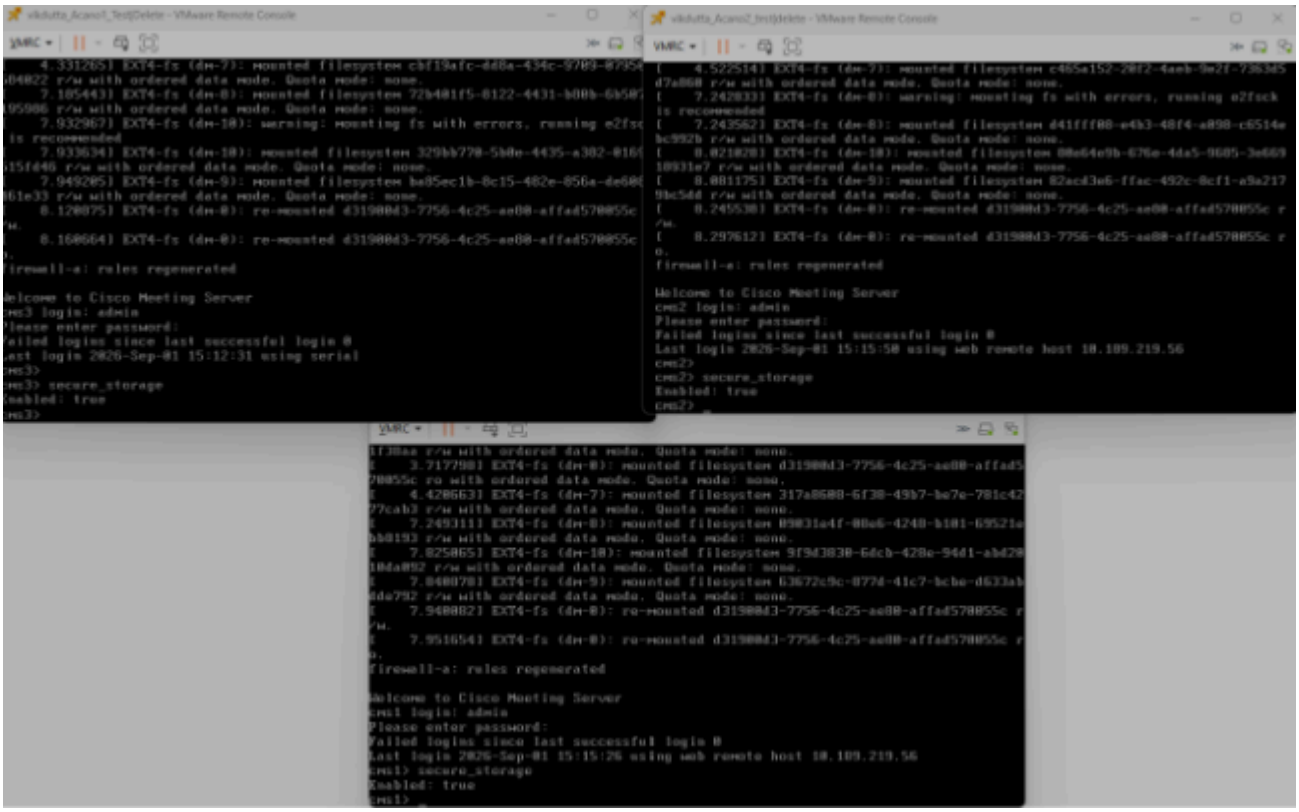


圖 34:對於圖示的三節點群集，確認安全儲存顯示已啟用：在升級之前，每個節點都為True。

2.記錄當前資料庫主副本並確認副本處於同步狀態。

```
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)
```

圖 35:升級前的資料庫群集狀態。記錄主副本並確認副本處於同步狀態。

3.確認所有正在使用的呼叫型別都工作正常，並且每個節點上的故障條件都已清除(在建立備份之前驗證伺服器健康狀態部分)。

4.使用啟用安全儲存時進行備份部分，為每個節點建立加密備份。為每個檔案分配並記錄唯一的密碼短語，或使用已記錄的密碼策略。在解散群集之前，僅從伺服器傳輸加密檔案。

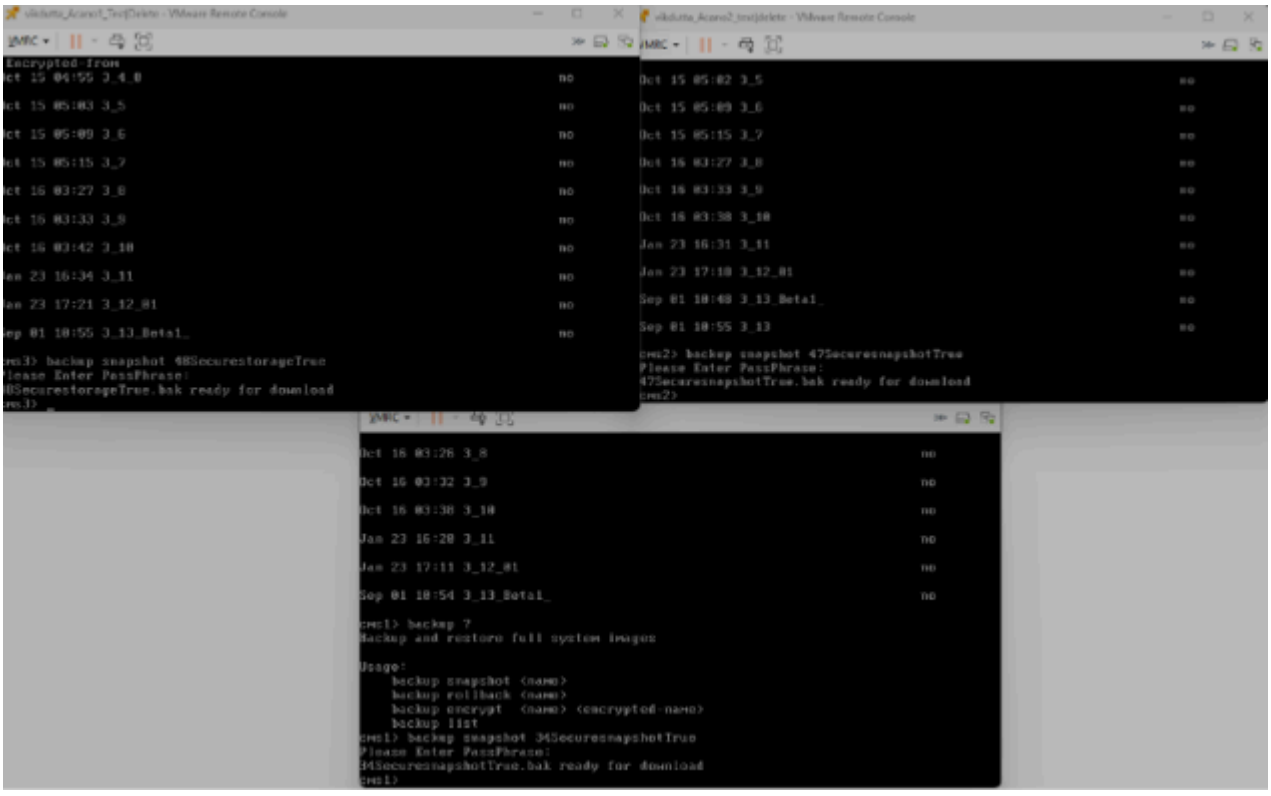


圖 36:每個節點上的加密備份快照。此範例顯示密碼提示符，然後顯示每個準備下載的.bak檔案。

解除、升級和恢復

按照案例3中的說明按以下順序解散集群：連線的節點、複製副本和主最後一個。使用database cluster remove並確認每個節點都已離開群集。

並行升級獨立節點。從控制檯恢復網路定址(首次啟動和網路恢復部分)。

上傳每個節點自己的加密備份。在回滾之前，請確認上載的快照在備份清單中顯示為已加密的:會。首先恢復前一個主節點，然後恢復副本和連線的節點。使用下面的backup rollback 命令，確認 Y，並在系統提示時輸入備份的口令。接受密碼後，節點將重新啟動。對每個節點重複上述步驟。

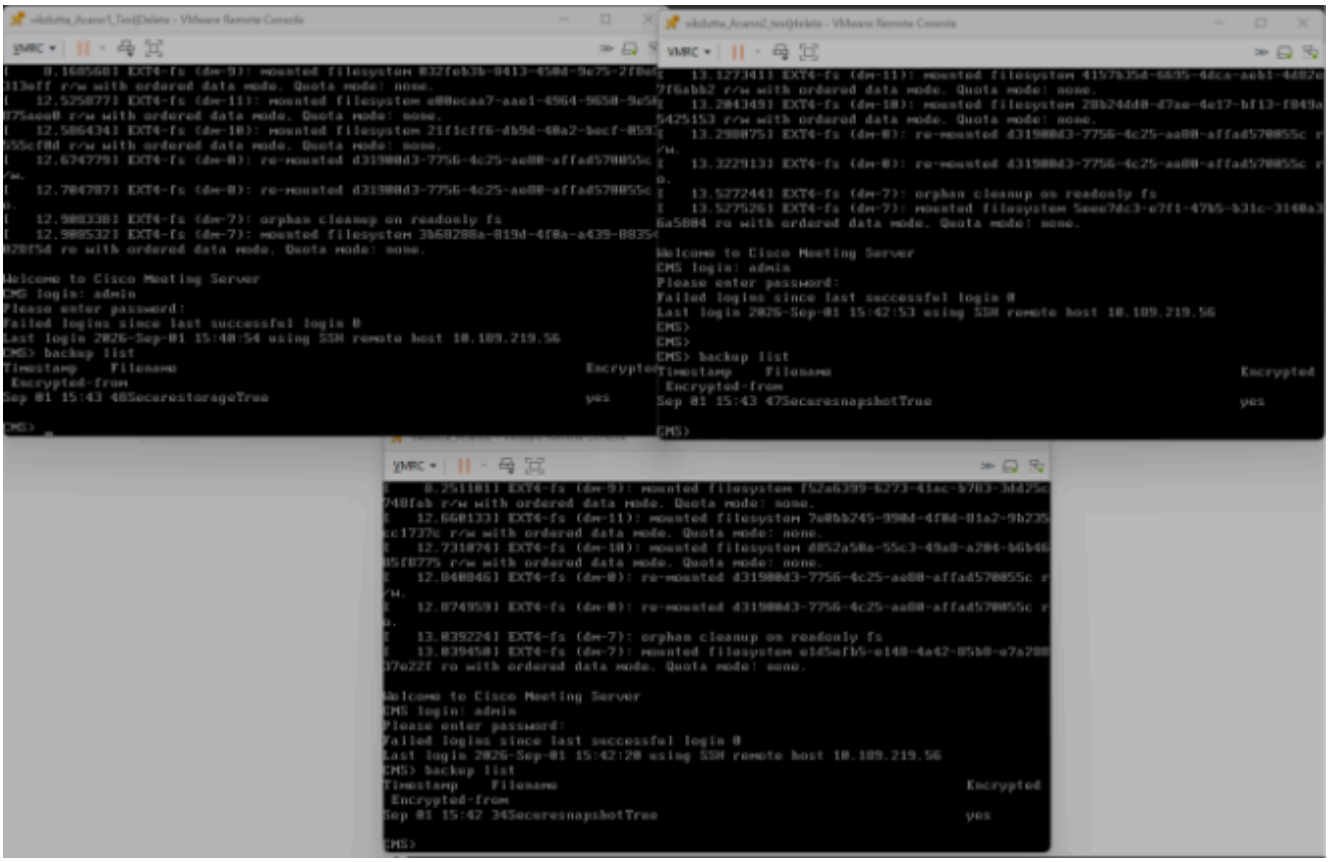


圖 37:在第一次4.0啟動後，上載的快照必須在備份清單中顯示為「已加密」：是，並準備好回滾。

backup rollback encrypted-filename

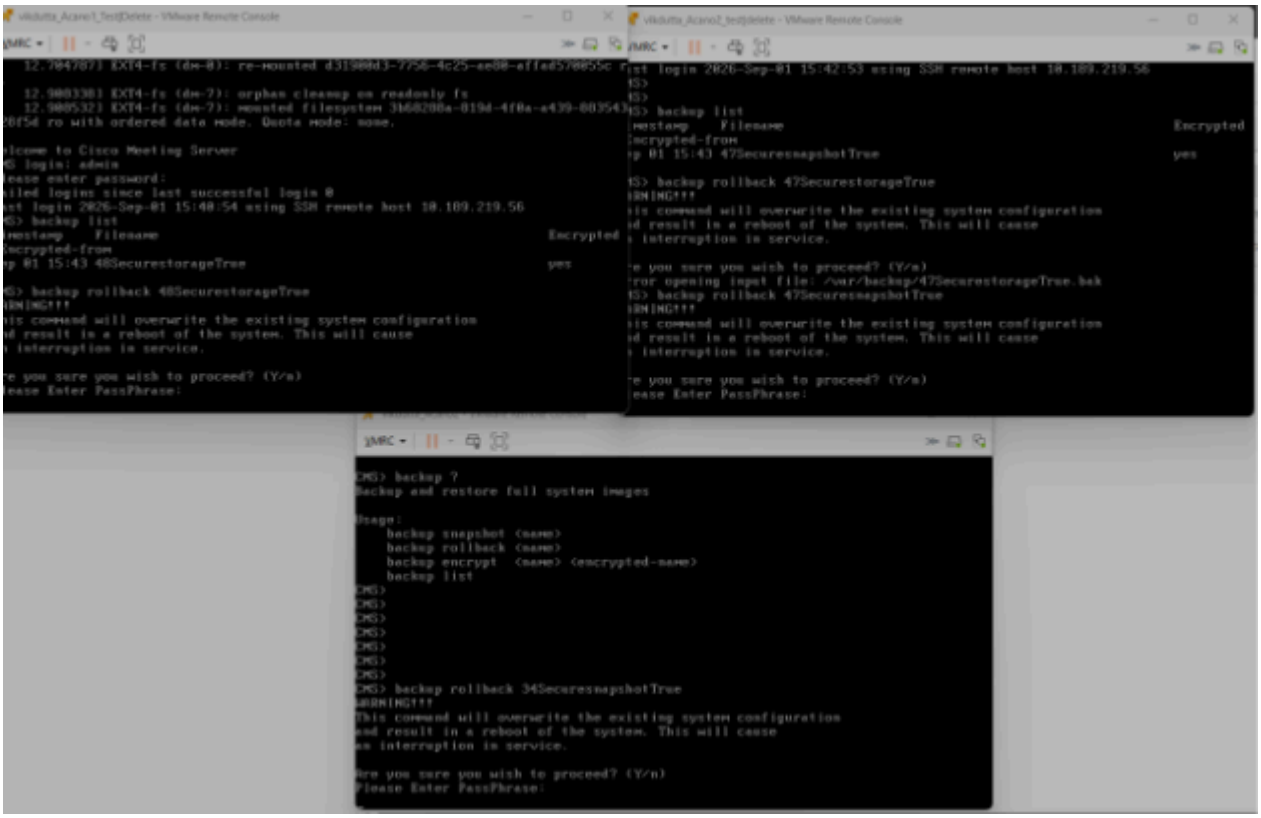


圖 38:確認Y，輸入密碼短語，然後首先恢復前一個主密碼。

附註：如果在此恢復後呼叫網橋群集連線沒有啟動，請僅對前一個主節點運行database cluster upgrade_schema，然後重新檢查呼叫網橋狀態。

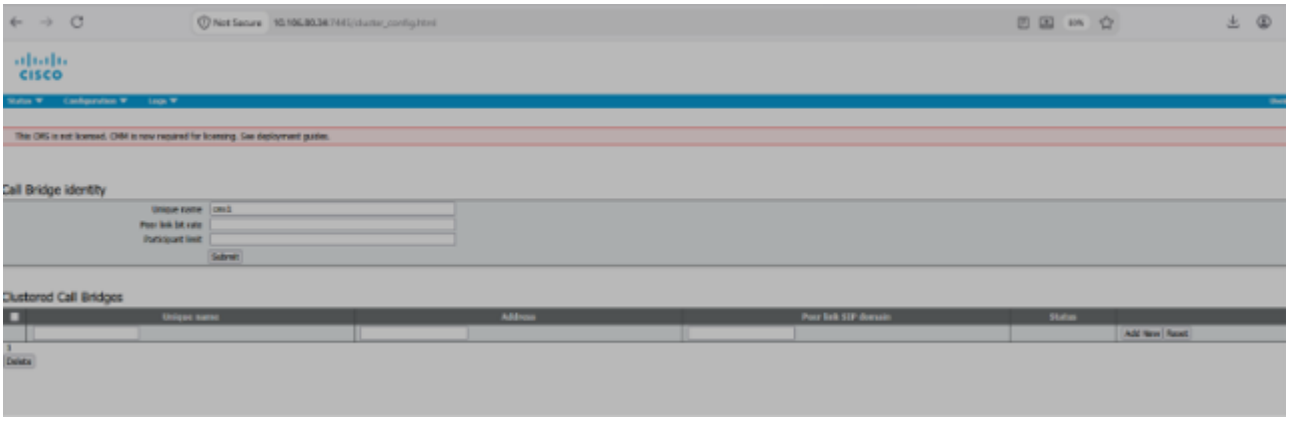


圖 39:在模式升級之前，該示例顯示了當集群呼叫網橋為空時正在運行的資料庫集群。

database cluster upgrade_schema

```
cms1> database cluster upgrade_schema
WARNING!!!
Are you sure you wish to upgrade the database schema on this database cluster? (
Y/n)
 This will affect all nodes, and may result in loss of functionality for nodes n
ot running the correct software version.
Schema upgrade started...
cms1> _
```

圖 40:在原來的主群集上，僅當在此已解散群集升級後Call Bridge群集連線失敗時確認Y。

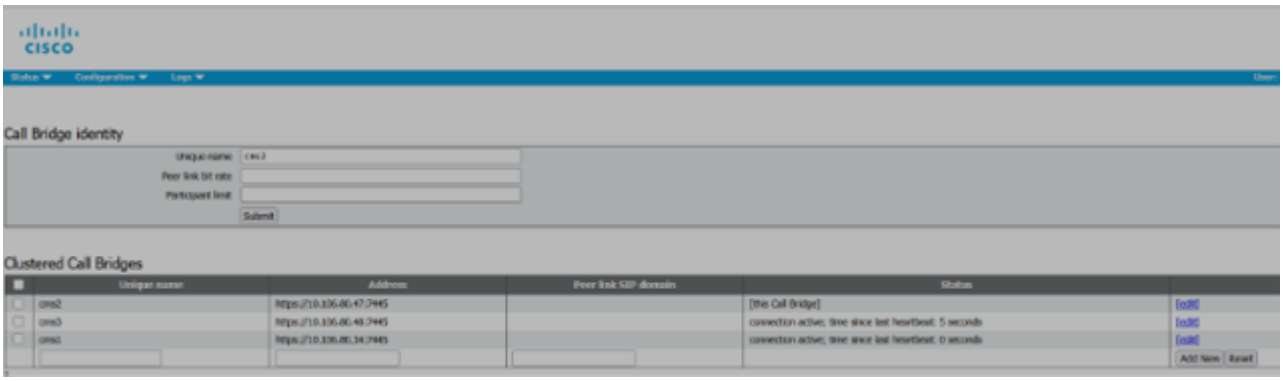


圖 41:架構升級後，驗證每個呼叫網橋對等體是否顯示活動連線。

在每個Web Bridge上MeetingApps Secret Key After Restore部分中完成MeetingApps加密過程，然後使用Post-upgrade Validation部分驗證部署。

升級後驗證

在恢復後和將系統恢復正常運行之前，請完成以下核對表：

- 每個節點上的Web管理顯示思科會議伺服器4.0。
- 所需的MMP服務已啟用且正在運行(活動：正確)。
- 故障情況很明顯。將最近的錯誤和警告視為資訊性錯誤，除非存在相應的故障。
- 如果適用，資料庫群集狀態顯示預期的主副本和副本。
- 智慧許可和呼叫網橋連線已恢復。
- 此部署支援的SIP呼叫和Web應用客戶端呼叫已成功完成。
- 如果在升級前要求部分中從伺服器複製的品牌、音訊提示和SSO檔案尚未包含在備份中，則這些檔案將被還原。
- 如果部署了MeetingApps，Web Bridge將顯示新的MeetingApps關係和檔案共用工作。
- 僅在接受部署後刪除短期快照。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。