Mise à niveau de Meeting Server vers la version 4.0 - Livre blanc

Table des matières

- Introduction
- Informations générales
- Présentation de Secure Storage
  - Plates-formes prises en charge
  - Notes de mise en oeuvre
- Principes et contraintes de mise à niveau
  - Chemin de mise à niveau requis
  - Rétrogradations
  - Exigences de sauvegarde critiques pour les mises à niveau 4.0
  - Première connexion et configuration du mot de passe
  - Rétablir la connectivité réseau après la mise à niveau
  - Valider L'Intégrité Du Serveur Avant De Créer Des Sauvegardes
- Conditions préalables à la mise à niveau
- Procédures courantes de sauvegarde et de restauration
  - Données affectées après la mise à niveau 4.0
  - Effectuer une sauvegarde lorsque le stockage sécurisé est désactivé ou indisponible
  - Effectuer une sauvegarde lorsque le stockage sécurisé est activé
  - Restaurer les données après la mise à niveau 4.0
  - Clé secrète MeetingApps après restauration
- Premier démarrage et restauration du réseau
- Scénarios de mise à niveau
  - Scénario 1 - Noeud unique avec stockage sécurisé désactivé ou indisponible
  - Scénario 2 : noeud unique avec stockage sécurisé activé
  - Scénario 3 - Cluster de base de données avec stockage sécurisé désactivé
    - Enregistrer les détails du cluster et sauvegarder chaque noeud
    - Dissoudre le cluster
    - Mise à niveau et restauration des noeuds
  - Scénario 4 - Cluster de base de données avec stockage sécurisé activé
    - Enregistrer les détails du cluster et créer des sauvegardes chiffrées
    - Dissoudre, mettre à niveau et restaurer
- Validation post-mise à niveau

Introduction

Ce document décrit comment mettre à niveau Cisco Meeting Server vers la version 4.0.

Informations générales

Utilisez ce document avec les notes de version de Cisco Meeting Server, le guide de référence des commandes MMP et le guide de référence de Secure Storage Administrator pour comprendre les exigences et les conditions requises.

Le processus de mise à niveau de Cisco Meeting Server 4.0 diffère des versions précédentes car l'application de l'image déclenche une réinitialisation d'usine du noeud. Pour assurer la continuité du service, toutes les configurations précédentes, y compris les paramètres réseau et les mots de passe, doivent être conservées via une sauvegarde exportée vers un emplacement externe avant de commencer la mise à niveau.

En outre, le stockage sécurisé était facultatif dans les versions 3.11 à 3.13 de Cisco Meeting Server, mais il est activé par défaut dans la version 4.0. Par conséquent, vous devez suivre des procédures de sauvegarde et de restauration différentes si vous n'avez jamais utilisé le stockage sécurisé ou si vous l'avez déjà activé sur 3.11x, 3.12x ou 3.13x.

Le stockage sécurisé chiffre la clé privée et les fichiers de sauvegarde sur le serveur et exige que ces fichiers soient chiffrés avant que vous puissiez les transférer vers un stockage externe.

Ce document regroupe les conseils requis en une seule référence afin que vous puissiez suivre une procédure commune pour tous les scénarios de mise à niveau sans avoir à répéter les mêmes étapes.

Ce document couvre les sujets suivants :

- Qu'est-ce que le stockage sécurisé, où il s'applique et ce qu'il ne fait pas ?
- Le chemin de mise à niveau, qui inclut l'exigence d'atteindre 3.13.x avant 4.0 et le fait qu'une rétrogradation à partir de 4.0 n'est pas prise en charge.
- Méthode de sauvegarde et de restauration courante pour les noeuds où le stockage sécurisé est activé et pour les noeuds où il est désactivé ou indisponible.
- Séquencement de la dissolution des noeuds du cluster de base de données pendant que le cluster de base de données est dissous avant une mise à niveau.
- La clé secrète MeetingApps, qui n'est pas stockée dans une sauvegarde Cisco Meeting Server et doit être régénérée après une restauration.

Remarque : Ce document utilise des captures d'écran de travaux pratiques capturées lors des tests de conseils de mise à niveau d'origine, y compris les versions 4.0 bêta. Tous les noms d'hôte, adresses IP et noms de fichiers affichés sont strictement illustratifs et ne

---

reflètent pas les identifiants de production réels ou les phrases de passe sensibles. Pour plus de clarté et éviter la redondance, les étapes répétées ne sont affichées qu'une seule fois dans la section de procédure commune, à moins que la vue en cluster ne fournisse le contexte nécessaire supplémentaire.

Présentation de Secure Storage

Le stockage sécurisé offre une sécurité des données améliorée en chiffrant les fichiers sensibles qui résident sur le serveur de téléconférence et en contrôlant la façon dont ces fichiers sont déchargés du serveur Call Bridge. Cette fonctionnalité a été introduite dans Cisco Meeting Server 3.11 en tant qu'option configurable à l'aide de la commande MMP secure_storage enable sur les déploiements de machines virtuelles (basés sur les spécifications ou Meeting Server Small) et sur Meeting Server Medium.

Depuis la version 4.0, le stockage sécurisé est activé par défaut. Ce paramètre est désormais permanent et irréversible, et la commande secure_storage enable MMP a été supprimée.

Avec le stockage sécurisé, le serveur de téléconférence applique ce comportement :

- Les clés privées ne peuvent pas être téléchargées via SFTP tant qu'elles ne sont pas chiffrées. Chiffrez une clé privée à l'aide de la commande pki encrypt MMP suivie d'une phrase de passe d'au moins 14 caractères. Cela ne modifie pas les clés actuellement utilisées par les services Meeting Server.
- Les fichiers de sauvegarde créés à l'aide de la commande backup encrypt <name> encryption-name sont chiffrés. Lorsque le stockage sécurisé est activé, la commande backup encrypt <name> encryption-name MMP demande une phrase de passe d'au moins 14 caractères. La même phrase de passe est requise lors de la restauration de sauvegarde.
- Avant de télécharger un fichier de sauvegarde, celui-ci doit être chiffré. Si une sauvegarde répertoriée n'est pas encore chiffrée pour l'exportation, utilisez backup encrypt <name> encryption-name. Les tentatives de téléchargement d'une sauvegarde non chiffrée sont refusées.
- À partir de la version 3.12, Secure Storage peut fonctionner lorsque FIPS est activé. Les fichiers de clés privées créés dans 3.11 avec une phrase de passe plus courte doivent être régénérés à l'aide d'une phrase de passe d'au moins 14 caractères.



Conseil : Le stockage sécurisé limite le transfert de clés privées non chiffrées et de fichiers de sauvegarde non chiffrés à partir du serveur de téléconférence. Il ne limite pas le transfert des fichiers de certificat. Les certificats peuvent toujours être copiés avec SFTP ; seules les clés privées non chiffrées associées sont bloquées jusqu'à ce qu'elles

soient chiffrées avec pki encrypt.

⚠ Mise en garde : Une fois activé, le stockage sécurisé ne peut pas être désactivé avec une commande MMP. L'opération est irréversible. Seul factory_reset full réinitialise le stockage sécurisé sur false. Effectuez une sauvegarde de configuration avec un snapshot de sauvegarde et stockez-le sur un périphérique distinct avant d'activer le stockage sécurisé. Une fois secure_storage activé, redémarrez immédiatement. Si le redémarrage est ignoré, le stockage sécurisé peut être marqué comme activé sans être entièrement initialisé, et des commandes telles que factory_reset full peuvent échouer. Dans cet état, le chemin de récupération doit revenir à un instantané précédemment enregistré (valide uniquement pour 3.13.x). Dans Meeting Server 4.0, secure_storage est activé par défaut.

Plates-formes prises en charge

- Machine virtuelle (basée sur les spécifications) : Pris en charge
- Serveur de réunion petit/1000 : Pris en charge
- Serveur de téléconférence de taille moyenne : Pris en charge
- Meeting Server 2000 : Non pris en charge. La fonction Stockage sécurisé n'est pas disponible. N'utilisez pas les commandes de stockage sécurisé sur cette plate-forme.

Cisco Meeting Server 4.0 active le stockage sécurisé par défaut sur toutes les plates-formes compatibles. Après la mise à niveau, les données sont automatiquement protégées par Secure Storage même si la sauvegarde 3.13.x a été effectuée alors que Secure Storage était désactivé.

Notes de mise en oeuvre

- Le changement de nom de l'image de mise à niveau ne modifie pas les paramètres de stockage sécurisé.
- Confirmez l'état du stockage sécurisé sur chaque noeud à l'aide de la commande secure_storage avant d'effectuer des sauvegardes.
- La commande indique si le stockage sécurisé est activé (True) ou non (False). Sur Meeting Server 2000, la commande n'est pas applicable ; lors de la mise à niveau de Cisco Meeting Server 2000, suivez les étapes mentionnées dans les conditions de mise à niveau lorsque le stockage sécurisé est désactivé ou indisponible.



Sortie MMP lorsque le stockage sécurisé n'est pas activé (Activé : faux).



Figure 2 : Sortie MMP lorsque le stockage sécurisé est activé (Activé : true) sur Cisco Meeting Server 3.13.

Vous trouverez des avertissements détaillés sur la syntaxe des commandes et des exemples d'utilisation dans le Guide de référence rapide de Cisco Meeting Server Administrator pour le stockage sécurisé et dans le Guide de référence des commandes MMP que vous utilisez actuellement.

Principes et contraintes de mise à niveau

Chemin de mise à niveau requis

Les mises à niveau de Cisco Meeting Server doivent suivre un chemin séquentiel sans ignorer les versions majeures. Par exemple, un noeud sur 3.11.x doit passer par 3.12.x et 3.13.x avant d'atteindre la version 4.0. Les mises à niveau directes à partir de versions antérieures telles que 3.9.x vers 3.13.x ou 3.11.x vers 4.0 ne sont pas prises en charge et provoquent généralement des erreurs de configuration irrécupérables. Pour Meeting Server Medium avec les versions 3.11.5 ou 3.13, le chemin de mise à niveau serait 3.11.5 → 3.13 → 4.0.

Conseil : Avant de commencer la mise à niveau vers la version 4.0, chaque noeud doit exécuter Cisco Meeting Server 3.13.x, avec une sauvegarde de configuration vérifiée exportée à partir de ce système 3.13.x. Toutes les procédures de scénario de ce document supposent que la mise à niveau vers la version 3.13.x est déjà terminée.

Rétrogradations



Conseil : Une rétrogradation de 4.0.x à 3.13.x n'est pas prise en charge. Si la mise à niveau échoue ou si le système ne fonctionne pas comme prévu, déployez une nouvelle OVA 3.13.x (ou réinstallez l'appliance) et restaurez la sauvegarde 3.13.x. Conservez les snapshots de l'hyperviseur des machines virtuelles 3.13.x pendant toute la durée de la fenêtre de mise à niveau en tant qu'option de récupération supplémentaire. Les snapshots de VM ne remplacent pas les sauvegardes de configuration exportées.

Exigences de sauvegarde critiques pour les mises à niveau 4.0

Une fois la mise à niveau 4.0 confirmée, le noeud redémarre dans un premier état d'amorçage. Ne dépendez pas de la sauvegarde automatique générée pendant le processus de mise à niveau, car un échec de la mise à niveau peut entraîner une perte d'accès SFTP et rendre le fichier inaccessible. Seules les sauvegardes créées à l'aide de la commande backup snapshot et copiées vers un stockage externe peuvent être utilisées de manière fiable pour la restauration.

Première connexion et configuration du mot de passe

Lors du premier démarrage de la version 4.0, le mot de passe MMP existant est supprimé de la base de données. Connectez-vous avec le nom d'utilisateur admin avec un mot de passe vide (aucun mot de passe). Le système vous demande de configurer un nouveau mot de passe MMP. Le système vous invite à saisir le mot de passe deux fois pour vérification et confirmation. Étant donné qu'il n'existe aucune fonction de récupération de mot de passe pour Meeting Server, veillez à enregistrer votre nouveau mot de passe.

Remarque : Si vous définissez un nouveau mot de passe MMP au premier démarrage, la commande backup rollback le remplace par le mot de passe qui a été stocké dans la sauvegarde 3.13.x. Après avoir restauré la sauvegarde sur le serveur, vous devez vous connecter avec le mot de passe qui était actif au moment de la création de la sauvegarde.

Rétablir la connectivité réseau après la mise à niveau

Les adresses, masques et passerelles IPv4 et IPv6 sont perdus avec le reste de la configuration. La connectivité réseau du serveur de téléconférence peut être perdue après la mise à niveau vers la version 4.0. Vous devez disposer d'un accès console d'hyperviseur, CIMC ou série pour pouvoir attribuer à nouveau l'adressage à partir du MMP.



Remarque : Les déploiements qui utilisent des réservations DHCP conservent

généralement les mêmes adresses IP après le redémarrage. Cependant, l'accès à la console doit rester disponible jusqu'à ce que l'adresse soit vérifiée. Ne supposez pas que la connectivité SSH est restaurée tant que l'adresse IP n'est pas confirmée.

Valider L'Intégrité Du Serveur Avant De Créer Des Sauvegardes

Après chaque étape de mise à niveau vers la version 3.13, assurez-vous que le serveur est en bon état et que tous les services fonctionnent. N'ignorez aucune condition d'erreur sur la page de présentation du serveur. Si vous rencontrez des erreurs, corrigez-les avant la création d'une capture instantanée de sauvegarde sur 3.13. Cela garantit la restauration d'une sauvegarde saine du serveur sur les noeuds 4.0 mis à niveau, ce qui libère les erreurs de déploiement.

Sur Web Admin, ouvrez Status et vérifiez que la section Fault conditions est désactivée. Ignorer les entrées qui apparaissent uniquement sous Erreurs et avertissements récents. Après une mise à niveau, il est courant d'y voir des bases de données transitoires ou des messages Web Bridge ; ce n'est pas une raison pour restaurer ou retarder la sauvegarde.

Si une condition de panne persiste pendant plus d'une dizaine de minutes, résolvez-la avant d'effectuer la sauvegarde. Une restauration d'une sauvegarde 3.13.x contenant déjà des pannes sur 4.0 transfère ces pannes.

Pour les systèmes en cluster, vérifiez que tous les types d'appels utilisés fonctionnent (terminaux SIP et clients Web App) et qu'aucune condition d'erreur n'est répertoriée sur un noeud.

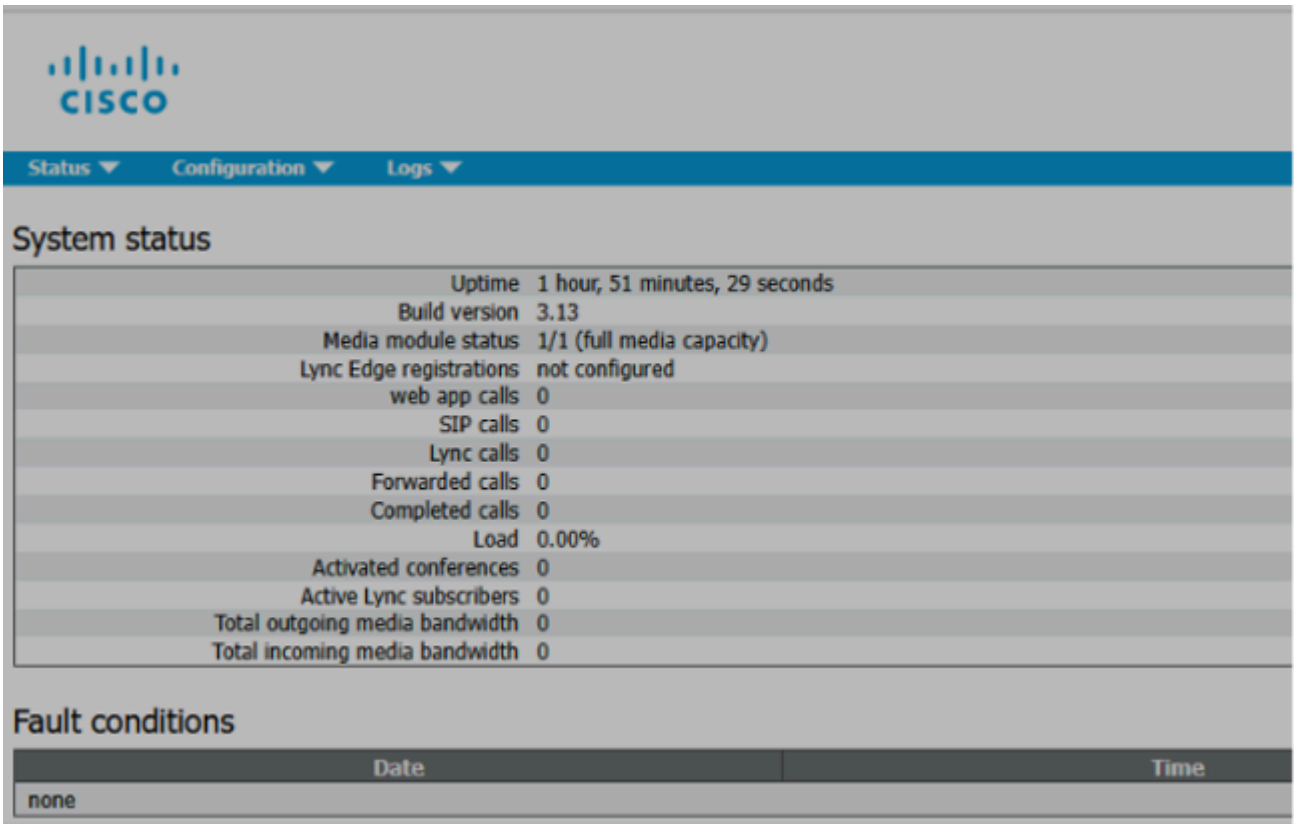


Figure 3 : Page Web Admin Status sur 3.13.x avec les conditions Fault vides. Utilisez cet affichage avant de prendre la sauvegarde qui est restaurée sur 4.0.

Conditions préalables à la mise à niveau

Avant de commencer la mise à niveau vers la version 4.0, effectuez ces actions. Ces exigences s'appliquent aux quatre scénarios abordés plus loin dans ce document.

- Effectuez une mise à niveau vers 3.13.x, puis exportez une sauvegarde de configuration. Assurez-vous que le noeud exécute Cisco Meeting Server 3.13.x. Créez une sauvegarde et transférez-la, ainsi que toutes les données SFTP personnalisées telles que les logos, les fichiers de personnalisation, les invites audio, les fichiers SSO et toutes les autres données personnalisées, vers un stockage externe. Utilisez les procédures de la section Procédures communes de sauvegarde et de restauration. Dans un environnement en cluster, effectuez une sauvegarde à partir de chaque noeud, non seulement du noeud principal connecté, mais aussi du réplica connecté.
- Enregistrez les paramètres réseau. Exécutez ipv4 a et stockez le résultat. Vous devez saisir à nouveau ces informations à partir de la console après le redémarrage de la version 4.0, à moins qu'une réservation DHCP ne restaure automatiquement l'adresse IP.
- Confirmez l'accès console. L'accès à la console de l'hyperviseur, à CIMC ou série doit être disponible avant de démarrer. SSH est censé disparaître lorsque le noeud redémarre à 4.0.
- Téléchargez le bundle de journaux actuel pour l'archivage. Enregistrez logbundle.tar.gz à partir de chaque noeud. L'offre groupée ne remplace pas les snapshots de sauvegarde.
- Lisez la bannière d'avertissement de mise à niveau 4.0 lorsqu'elle est affichée après

l'exécution de la commande upgrade.
- Appuyez sur n pour abandonner si une condition préalable est incomplète. Appuyez sur Y uniquement lorsque vous êtes prêt à continuer.

Procédures courantes de sauvegarde et de restauration

Les quatre scénarios de mise à niveau décrits plus loin dans ce document utilisent le même modèle de sauvegarde, d'exportation, de premier démarrage et de restauration. Utilisez cette section comme source unique de ces étapes, puis suivez uniquement le séquencement spécifique au scénario (noeud unique ou cluster, et si le stockage sécurisé est déjà activé).

Données affectées après la mise à niveau 4.0

Ces données sont perdues après la mise à niveau 4.0 jusqu'à ce que vous restauriez une sauvegarde :

- Contenu de la base de données, qui inclut des espaces, des utilisateurs et des profils d'appel.
- Certificats et clés privées.
- Personnalisation locale, fichiers SSO et fichiers d'invite audio.
- Configuration du réseau (adresse IP, masque et passerelle), sauf lorsqu'une réservation DHCP restaure l'adresse.
- Le mot de passe MMP précédent, jusqu'à ce que la restauration de sauvegarde réapplique le mot de passe de la sauvegarde.
- Call Bridge, Web Admin, Web Bridge et d'autres services d'application ne reviennent qu'après la restauration.



Conseil : La sauvegarde de Cisco Meeting Server n'inclut pas la clé secrète MeetingApps. Après une restauration, vous devez régénérer cette clé et l'appliquer à chaque noeud Web Bridge. Consultez la section Clé secrète MeetingApps après restauration.

Effectuer une sauvegarde lorsque le stockage sécurisé est désactivé ou indisponible

Suivez cette procédure sur les machines virtuelles, Meeting Server Small et Meeting Server Medium où secure_storage rapporte Enabled : False, et sur Meeting Server 2000 où le stockage sécurisé n'est pas disponible.

1. Sur chaque noeud, créez un fichier à l'aide de la commande backup snapshot. Ne réutilisez pas le nom de fichier précédent.

2. Copiez immédiatement le fichier de sauvegarde sur un stockage externe avec SFTP. Ne conservez pas la seule copie sur le serveur de téléconférence.

3. Stockez le fichier dans un emplacement toujours accessible si le noeud est reconstruit.

Exemple :

backup snapshot cms313SecurestorageFalse backup list

4. Vérifiez que le fichier apparaît dans la commande backup list, puis transférez-le sur un disque externe avec un client SFTP.

5. Répétez ce processus sur chaque noeud du cluster. Les noms de sauvegarde ne peuvent contenir que des lettres, des chiffres, des traits de soulignement et des tirets. N'incluez pas l'extension de fichier .bak lorsque vous créez un fichier de sauvegarde. Par exemple, un nom de fichier tel que 3.13SecurestorageFalse est rejeté en raison du point.

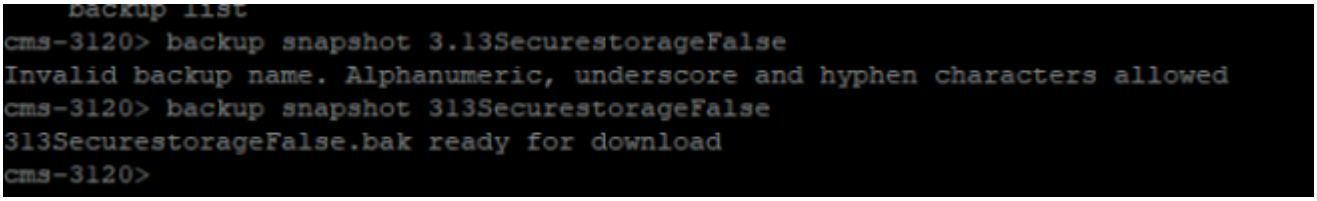


Figure 4 : L'instantané de sauvegarde rejette un nom qui contient un point, puis réussit avec un nom alphanumérique. Le fichier .bak est alors prêt à être téléchargé.



Figure 5 : Copiez le fichier .bak de la racine SFTP de Meeting Server vers un stockage externe. Ne laissez pas la seule copie sur le serveur.

Effectuer une sauvegarde lorsque le stockage sécurisé est activé

Utilisez cette procédure lorsque secure_storage signale Enabled : Vrai. Impossible de télécharger les fichiers de sauvegarde non chiffrés.

1. Créez un snapshot de sauvegarde sur chaque noeud. Lorsque le stockage sécurisé est activé, le serveur demande une phrase de passe d'au moins 14 caractères. La phrase de passe peut inclure des lettres, des chiffres, des caractères spéciaux, des symboles ou des espaces.

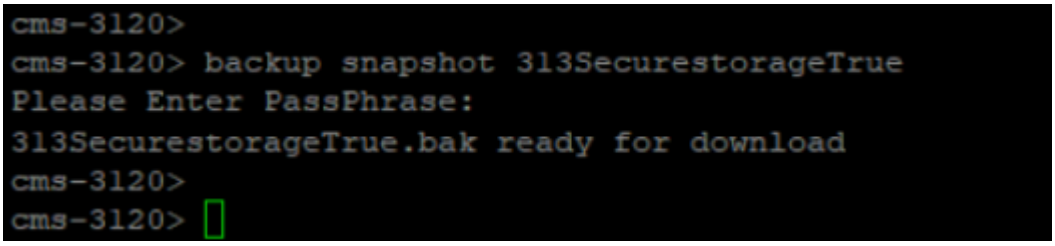


Figure 6 : L'option Sauvegarder un snapshot avec le stockage sécurisé activée vous invite une fois à saisir une phrase de passe d'au moins 14 caractères. Le MMP ne vous demande pas de le confirmer.

2. Le MMP ne vous demande pas de saisir à nouveau la phrase de passe pour confirmation. Sécurisez votre phrase de passe car vous avez besoin de la même phrase de passe afin de restaurer le fichier. Ne choisissez pas une phrase secrète ou un exemple de phrase secrète.

3. Si la commande backup list affiche un snapshot qui n'a pas été chiffré pour l'exportation, chiffrez-le avant de le télécharger :



Figure 7 : Sauvegarder la liste avant le chiffrement. La colonne Chiffré est non, le fichier ne peut donc pas être téléchargé.

4. Si vous tentez de télécharger une sauvegarde non chiffrée, le protocole SFTP renvoie une erreur « autorisation refusée » et vous demande d’exécuter d’abord la commande backup encrypt.

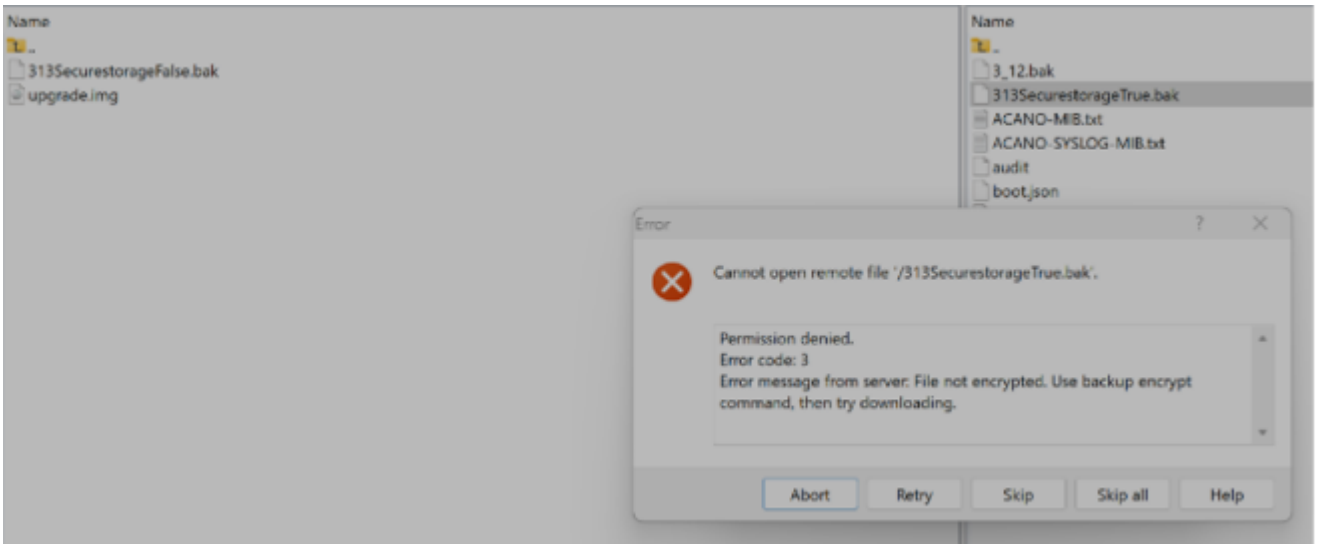


Figure 8 : SFTP refuse le téléchargement d'une sauvegarde non chiffrée lorsque le stockage sécurisé est activé. Le message du serveur vous demande d'exécuter le chiffrement de sauvegarde.

5. Exécutez la commande backup encrypt afin de chiffrer le fichier de sauvegarde.

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

Figure 9 : Liste de sauvegarde après le chiffrement du snapshot. Encrypted est yes et le fichier peut être transféré via SFTP.

La liste de sauvegarde affiche l'état de cryptage et le nom du fichier d'origine. Assurez-vous de ne transférer que le fichier chiffré de chaque noeud du cluster. Conservez un enregistrement organisé de chaque noeud, de son nom de fichier correspondant et de la phrase de passe associée.

Si vous devez également exporter des clés privées, chiffrez d'abord chaque clé. Les fichiers de certificat ne sont pas bloqués par le stockage sécurisé et peuvent être copiés sans cette étape supplémentaire :

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

Utilisez un nom de fichier unique au lieu d'écraser la clé actuellement utilisée par les services. La phrase de passe minimale de 14 caractères s'applique également ici.

Restaurer les données après la mise à niveau 4.0

1. Après la connexion au premier démarrage et la restauration du réseau dans la section First-boot and Network Restore, copiez la sauvegarde 3.13.x correspondante sur le noeud avec SFTP

et restaurez-la.

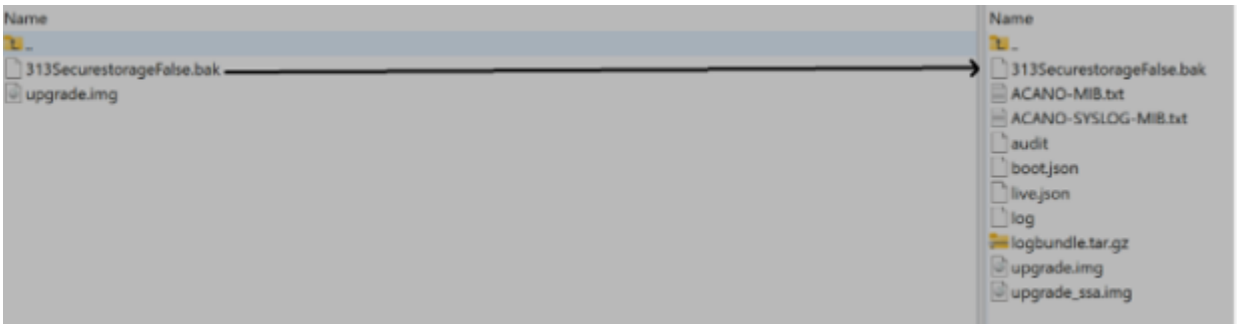


Figure 10 : Après la restauration du réseau au premier démarrage, copiez le fichier .bak 3.13.x sur le noeud 4.0 avec SFTP.

2. Vérifiez si le fichier est présent :

liste de sauvegarde

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

cms-3120>
```

Figure 11 : Liste de sauvegarde sur 4.0 confirmant que le snapshot téléchargé est présent avant la restauration.

3. Restaurez l'instantané. Dans un déploiement en cluster, restaurez d'abord l'ancienne base de données principale, puis les réplicas, puis les noeuds connectés.

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...
```

Figure 12 : Sauvegarde et restauration d'un snapshot non chiffré. Confirmer avec Y ; le noeud extrait la sauvegarde et redémarre.

4. Appuyez sur Y pour continuer. Le noeud redémarre pendant qu'il extrait la sauvegarde. Si la sauvegarde a été effectuée avec le stockage sécurisé activé, le MMP vous invite à saisir la phrase de passe. Le redémarrage se poursuit uniquement après l'acceptation de la phrase de passe

correcte.

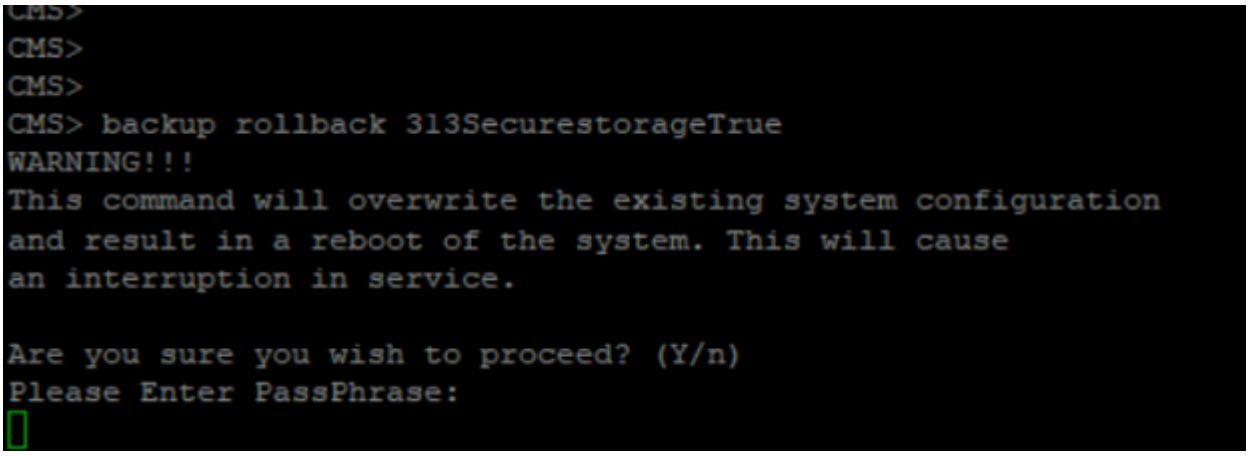


Figure 13 : Sauvegarde et restauration d'un snapshot chiffré. Après Y, le MMP demande la phrase de passe utilisée lors de la création de la sauvegarde.

⚠ Mise en garde : Le **backup rollback** remplace la configuration, les certificats, les clés privées et le fichier de licence actuels, puis redémarre le serveur. Utilisez-la uniquement avec la sauvegarde 3.13.x que vous avez exportée pour cette mise à niveau.

---

5. Lorsque le noeud est de nouveau en ligne, connectez-vous avec les informations d'identification MMP de la sauvegarde et vérifiez que chaque service requis indique qu'il est activé et en cours d'exécution (le MMP affiche ceci comme actif : Vrai).

Contrôles types :

callbridge webbridge3 webadmin scheduler recorder streamer uploader meetingapps

6. Exécutez uniquement les commandes pour les services que ce noeud est censé héberger.

Clé secrète MeetingApps après restauration

La sauvegarde de Cisco Meeting Server ne stocke pas la clé secrète MeetingApps. Une fois la restauration de sauvegarde terminée, régénérez le secret et appliquez-le à chaque noeud Web Bridge. Si vous ignorez cette étape, le partage de fichiers reste indisponible, même si les autres services semblent en bonne santé.

1. Sur le noeud MeetingApps, exécutez la commande meetingapps gensecret.

2. Copiez le secret généré dans votre banque de secrets. Chaque exécution de meetingapps gensecret invalide la clé précédente, donc générez la clé une fois et réutilisez la même valeur sur tous les ponts Web.

3. Exécutez ces commandes sur chaque noeud Web Bridge :

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

La dernière commande confirme que le service Web Bridge est en cours d'exécution et que MeetingApps est correctement configuré. MeetingApps n'est pas pris en charge sur Meeting Server 2000 et le partage de fichiers n'est pas disponible dans les clusters qui incluent Meeting Server 2000. Dans de tels déploiements, cette étape n'est pas applicable.

Premier démarrage et restauration du réseau

La commande upgrade 4.0 affiche une bannière d'avertissement avant de continuer. Examinez attentivement le message et abandonnez avec n si les conditions requises sont incomplètes. Si vous continuez avec Y, le noeud redémarre, la session SSH se déconnecte et les étapes restantes doivent être effectuées à partir de la console.

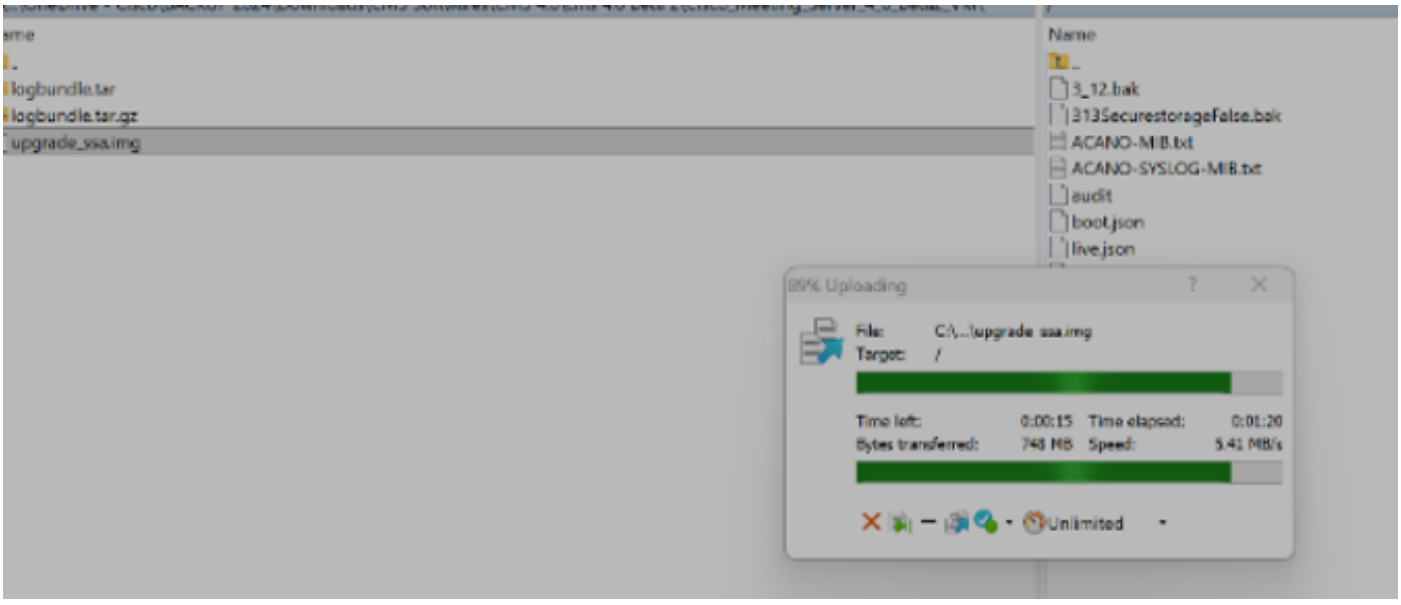


Figure 14 : Téléchargez l'image de mise à niveau 4.0 vers le répertoire racine SFTP de Meeting Server. Le nom de fichier de l'image de mise à niveau peut varier en fonction du package téléchargé à partir de cisco.com.

```
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...
```

Figure 15 : La commande upgrade vérifie la signature de l'image et lance le processus. Ne vous fiez pas à la sauvegarde automatique créée à ce stade.

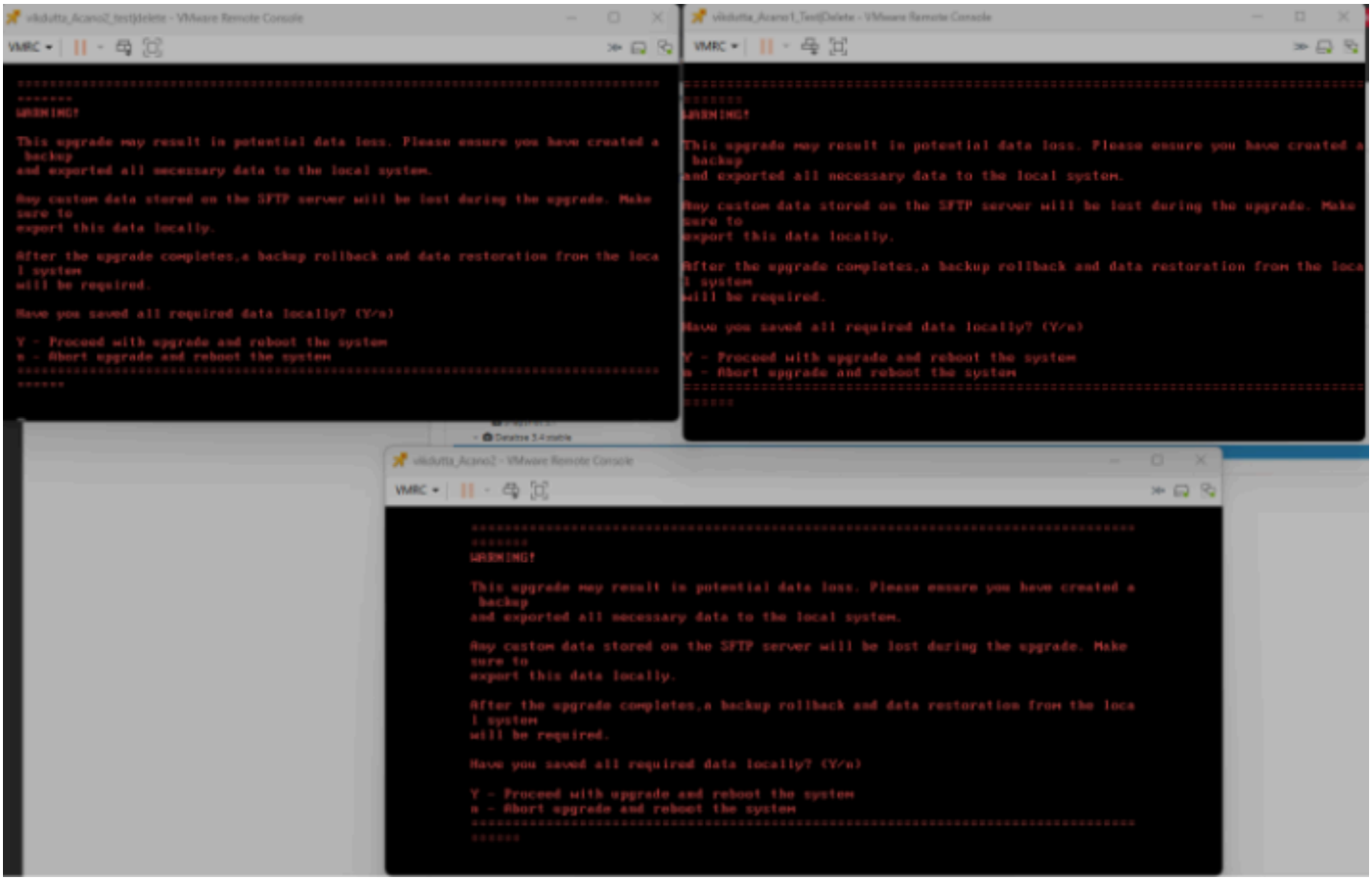


Figure 16 : Avertissement MMP rouge sur un cluster à trois noeuds. La même bannière apparaît sur un seul noeud. Appuyez sur n pour abandonner si les sauvegardes et les données personnalisées ne se trouvent pas hors du serveur. Appuyez sur Y uniquement pour continuer et redémarrer.

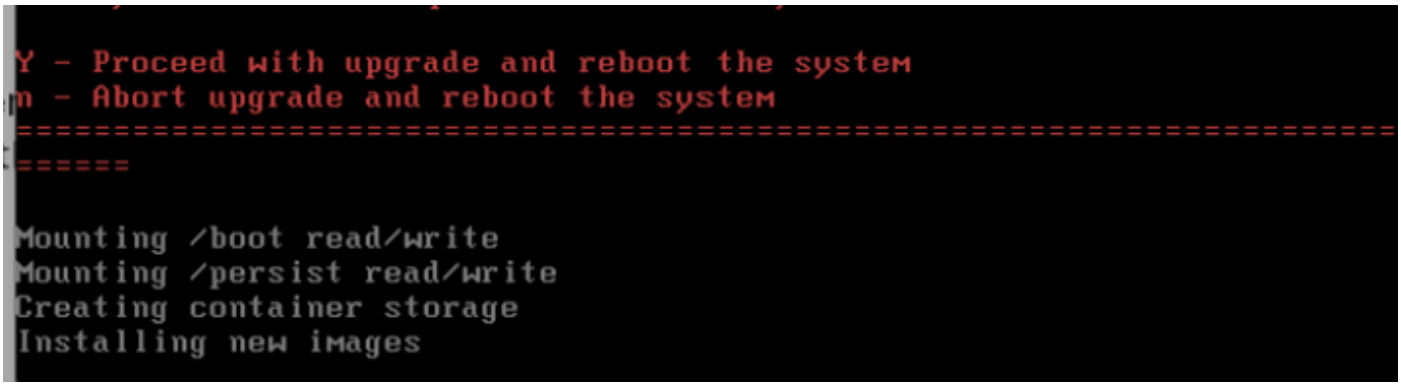


Figure 17 : Après Y, le noeud monte le stockage et installe l'image 4.0. La session SSH expire ; continuez à partir de la console de l'hyperviseur.

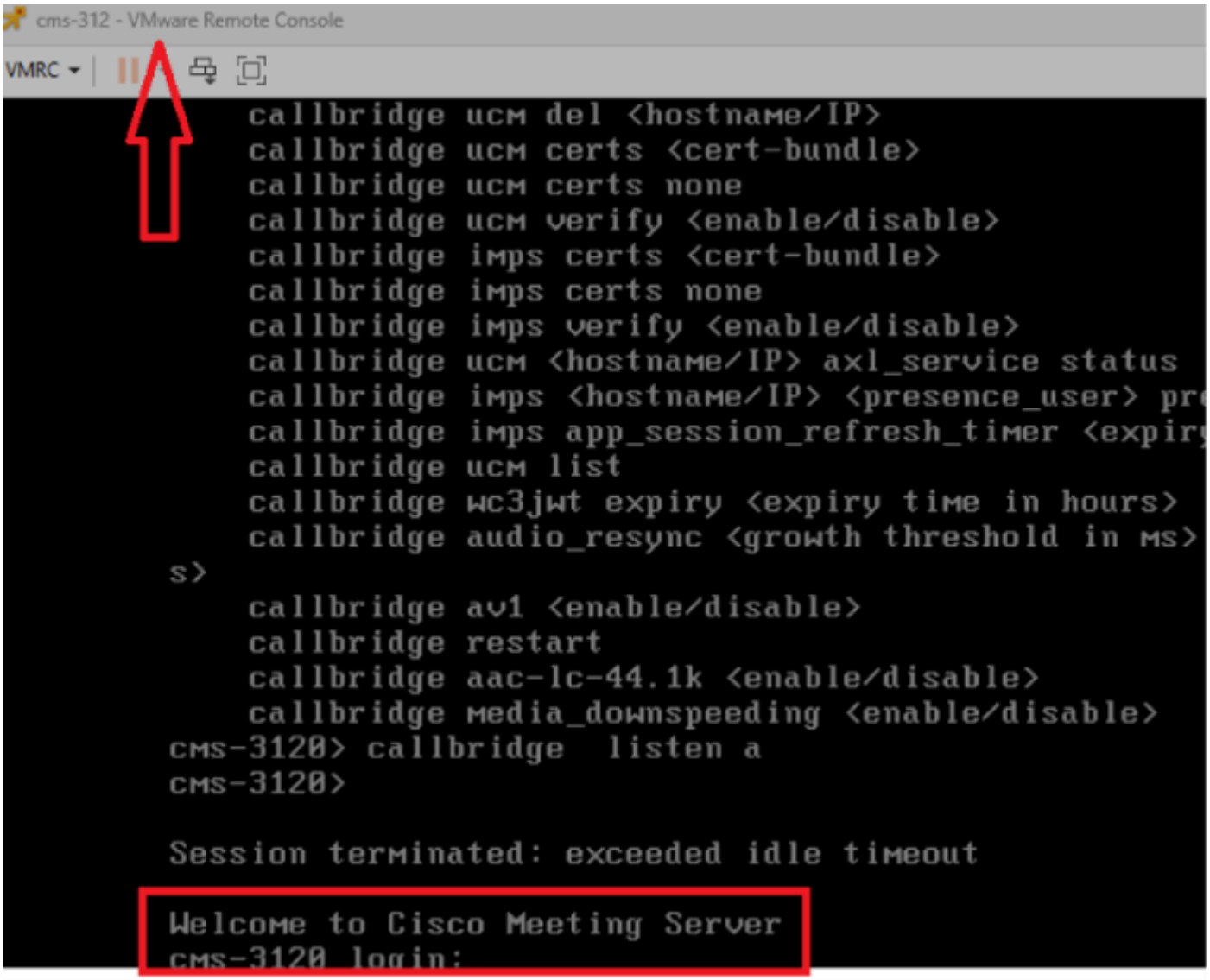


Figure 18 : Utilisez la console VM ou CIMC après l'abandon de SSH. L'invite de connexion au premier démarrage s'affiche lorsque l'image 4.0 est prête.

1. Connectez-vous avec le compte MMP au premier démarrage (nom d'utilisateur admin et aucun mot de passe), puis définissez un nouveau mot de passe MMP lorsque vous y êtes invité. Notez que la restauration de sauvegarde remplace ce mot de passe par le mot de passe stocké dans la

sauvegarde.

2. Réappliquez la configuration réseau à partir des remarques que vous avez saisies dans la section Pre-upgrade Requirements :

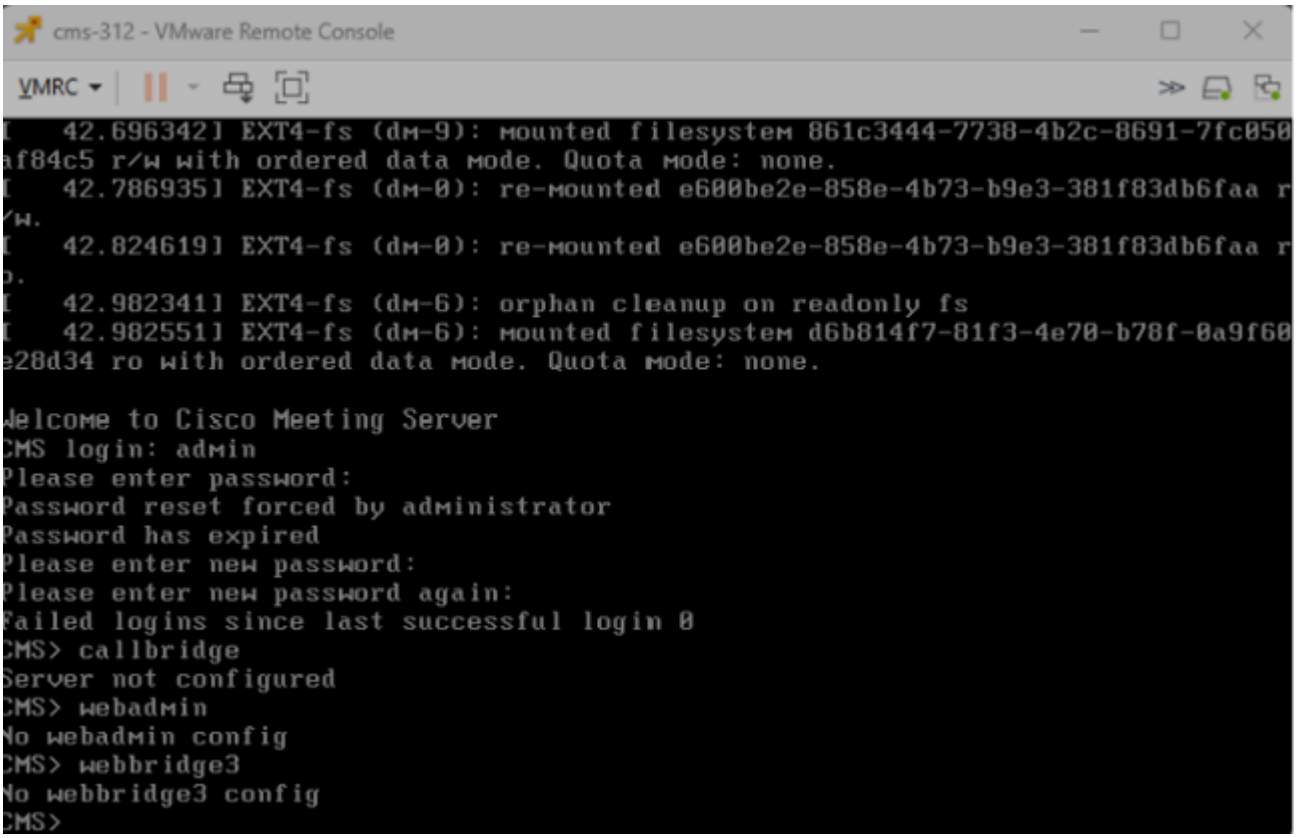


Figure 19 : Première connexion MMP au démarrage.

Le mot de passe précédent n'est plus valide. Une fois que vous avez défini un nouveau mot de passe, des services tels que webadmin et webbridge3 apparaissent comme non configurés jusqu'à ce que la sauvegarde soit restaurée.

3. Exécutez la commande suivante :

```
ipv4 interface add address/prefix-length gateway
```

Exemple :

```
ipv4 a add 192.0.2.10/24 192.0.2.1
```

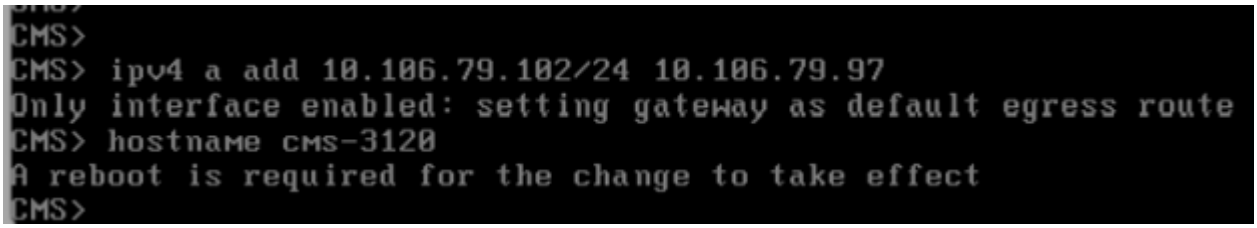


Figure 20 : Réapplication d'IPv4 à partir de la console

Un redémarrage est nécessaire après l'attribution de l'adresse. Les adresses indiquées dans la capture d'écran sont fournies à titre d'exemple uniquement.

4. Redémarrez une fois l'adresse attribuée. Une fois le système de nouveau en ligne, poursuivez le téléchargement SFTP de la sauvegarde et les étapes de restauration mentionnées dans la section Restore Data After 4.0 Upgrade.

Remarque : Si une réservation DHCP est configurée, l'adresse d'origine peut déjà être attribuée après le redémarrage. Vérifiez l'adresse avec **ipv4 a** avant de lancer une session SFTP à partir de votre station de travail de gestion.

Sur Cisco Meeting Server 4.0, le stockage sécurisé est activé par défaut sur les plates-formes qui le prennent en charge. Le MMP ne peut plus exposer secure_storage comme basculement après la mise à niveau.



Figure 21 : Sur cette image 4.0, secure_storage n'est pas une commande reconnue car Secure Storage est activé par défaut.

Confirmez la version avec la commande version.

Scénarios de mise à niveau

Ce chapitre couvre différents scénarios de mise à niveau. Effectuez la mise à niveau vers la version 3.13.x. Identifiez votre type de déploiement et choisissez le scénario en conséquence. Suivez uniquement la procédure qui correspond à votre environnement et ne combinez pas les étapes des déploiements de cluster et de noeud unique.

Commencez par effectuer la mise à niveau vers la version 3.13.x. Sélectionnez ensuite exactement un scénario ci-dessous. N'associez pas les procédures de noeud unique et de cluster de base de données.

- Scénario 1 : Noeud unique, désactivé ou non disponible, VM, Small, Medium et Meeting Server 2000
- Scénario 2 : Noeud unique, activé, machine virtuelle, petite et moyenne uniquement
- Scénario 3 : Cluster de base de données, désactivé ou non disponible, VM, Small, Medium et Meeting Server 2000
- Scénario 4 : Cluster de base de données, activé, machine virtuelle, petite et moyenne uniquement

Meeting Server 2000 ne prend pas en charge les scénarios activés pour le stockage sécurisé. Pour cette plate-forme, utilisez le scénario 1 ou 3, selon le cas.

Scénario 1 - Noeud unique avec stockage sécurisé désactivé ou indisponible

Suivez cette procédure pour un serveur autonome avec Stockage sécurisé désactivé ou Meeting Server 2000 où Stockage sécurisé n'est pas disponible. La version source peut être 3.11.x ou ultérieure, mais le noeud doit être sur 3.13.x avant la mise à niveau vers 4.0.

1. Effectuez une mise à niveau pas à pas vers 3.13.x. Suivez le chemin pris en charge (par exemple 3.11.x → 3.12.x → 3.13.x). Après chaque saut, confirmez la version dans Web Admin et assurez-vous que les conditions d'erreur sont claires, comme décrit dans la section Valider l'état du serveur avant de créer des sauvegardes.

2. Confirmez l'état du stockage sécurisé. Exécutez la commande secure_storage et vérifiez que le stockage sécurisé n'est pas activé. Ignorez la commande sur Meeting Server 2000.

3. Créez et exportez un fichier de sauvegarde 3.13.x comme indiqué dans la section Effectuer une sauvegarde lorsque le stockage sécurisé est désactivé ou indisponible. Exportez également le contenu SFTP personnalisé et le bundle de journaux, comme indiqué dans la section Conditions requises avant la mise à niveau.

4. Téléchargez l'image logicielle 4.0 à partir de Cisco.com, extrayez-la et copiez upgrade.img sur le noeud via SFTP.

5. Lancez la mise à niveau avec cette commande :

```
upgrade upgrade.img
```

6. Lisez la bannière d'avertissement. Appuyez sur Y uniquement une fois toutes les conditions requises terminées. 6. Après la mise à niveau, configurez le noeud comme décrit dans la section First-boot and Network Restore, puis restaurez la sauvegarde à l'aide de la section Restore Data After 4.0 Upgrade.

Scénario 2 : noeud unique avec stockage sécurisé activé

Suivez cette procédure pour une machine virtuelle autonome, Meeting Server Small ou Meeting Server Medium où le stockage sécurisé est activé. Elle ne s'applique pas à Meeting Server 2000.

Avant de transférer des fichiers à partir du serveur, notez que les clés privées non chiffrées et les fichiers de sauvegarde non chiffrés ne peuvent pas être transférés. Les fichiers de certificats ne sont pas bloqués.

1. Effectuez la mise à niveau via le chemin pris en charge vers 3.13.x sans ignorer les versions. Après chaque saut, confirmez la version et que les conditions d'erreur sont claires dans la section Valider l'état du serveur avant de créer des sauvegardes.

2. Exécutez secure_storage et vérifiez que le résultat indique Enabled : Vrai.

3. Créez et exportez une sauvegarde cryptée 3.13.x à l'aide de la section Effectuer une sauvegarde lorsque le stockage sécurisé est activé. Stockez sa phrase de passe dans votre magasin secret. Exportez également le contenu SFTP personnalisé et l'ensemble de journaux (section Spécifications préalables à la mise à niveau).

4. Copiez upgrade.img sur le noeud et exécutez la mise à niveau :

```
upgrade upgrade.img
```

5. Lisez la bannière d'avertissement et appuyez sur Y pour continuer uniquement lorsque les conditions requises sont remplies.

6. Récupérez le réseau à partir de la console (section First-boot and Network Restore), puis restaurez la sauvegarde chiffrée avec sa phrase de passe (section Restore Data After 4.0 Upgrade). 6. Si MeetingApps est en cours d'utilisation, appliquez un nouveau secret MeetingApps (section Clé secrète MeetingApps après restauration).

Le stockage sécurisé est activé par défaut sur Meeting Server 4.0. Après une restauration, continuez à gérer les clés privées et les fichiers de sauvegarde en tant que données chiffrées.

Scénario 3 - Cluster de base de données avec stockage sécurisé désactivé

Suivez cette procédure pour un cluster de base de données dont l'option Stockage sécurisé est désactivée, qui inclut un cluster contenant Meeting Server 2000. À partir de la version 3.5, le cluster de base de données doit être dissous avant la mise à niveau logicielle. Commencez par mettre à niveau chaque noeud vers la version 3.13.x.

Enregistrer les détails du cluster et sauvegarder chaque noeud

1. Exécutez secure_storage sur chaque noeud. Traitez la commande comme indisponible sur les noeuds Meeting Server 2000.

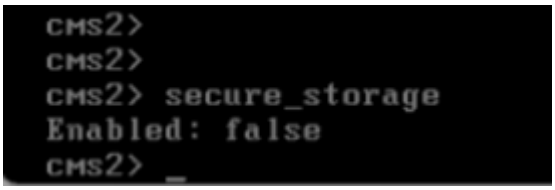


Figure 22 : Avant d'utiliser des sauvegardes non chiffrées, vérifiez que le stockage sécurisé est désactivé sur chaque noeud de cluster. Ignorez la commande pour les noeuds Meeting Server 2000, où elle n'est pas disponible.

2. Enregistrez le noeud principal de la base de données en cours, car il doit être restauré en premier après la mise à niveau vers la version 4.0. Vérifiez que les réplicas sont synchronisés et que l'état du cluster est sain.

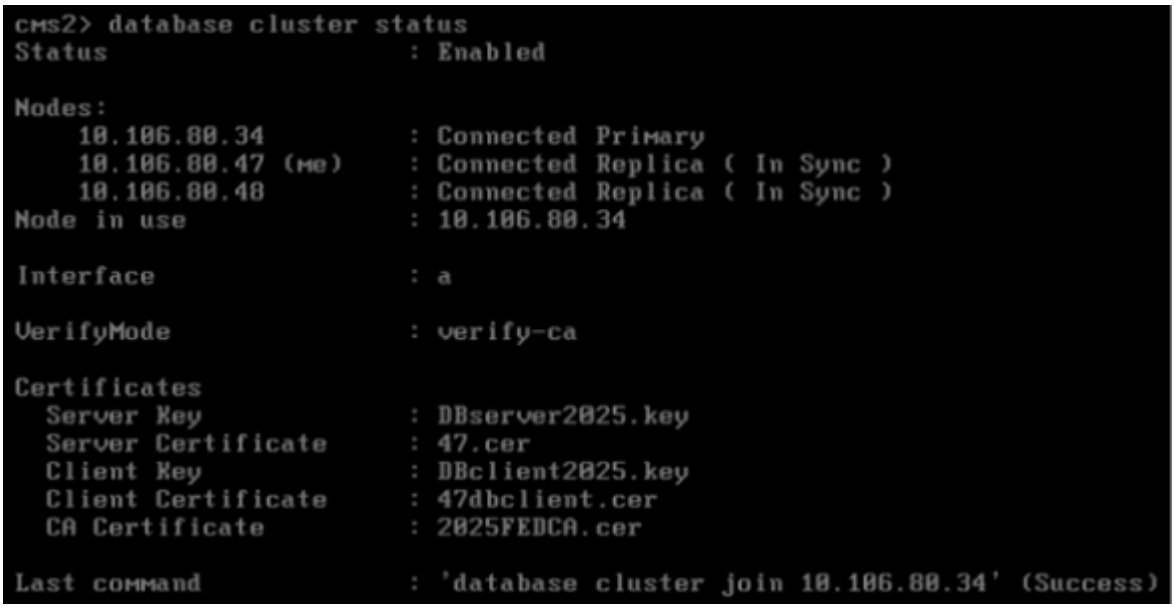


Figure 23 : Enregistrez le principal actuel et confirmez que les réplicas sont synchronisés.

3. Vérifiez que tous les types d'appels utilisés fonctionnent et que les conditions d'erreur sont

claires sur chaque noeud (section Valider l'état du serveur avant de créer des sauvegardes).

4. Créez une sauvegarde de chaque noeud à l'aide de la section Effectuer une sauvegarde lorsque le stockage sécurisé est désactivé ou indisponible. Nommez chaque fichier de sorte qu'il corresponde clairement à son noeud et transférez chaque sauvegarde vers un stockage externe avant de dissoudre le cluster.

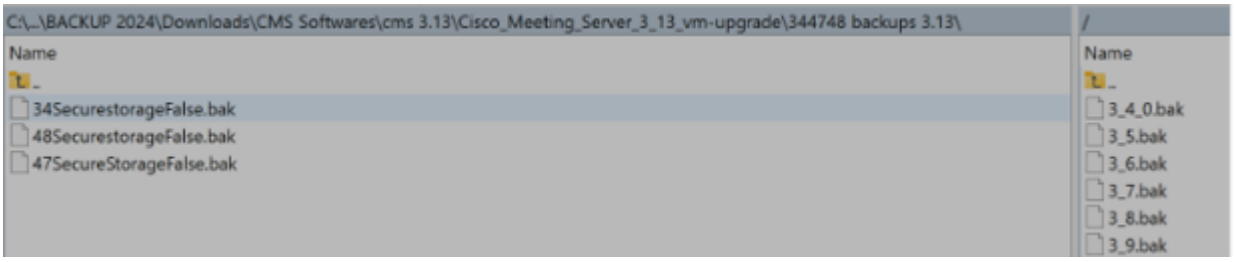


Figure 24 : Les trois exemples de sauvegarde de noeud stockent un stockage externe, nommé de sorte que chaque fichier soit mappé à son noeud.

Dissoudre le cluster

Supprimez les noeuds dans cet ordre. Conserver le principal jusqu'à la dernière :

- Noeuds de serveur de téléconférence connectés (non essentiels)
- Noeuds de base de données réplicas
- Noeud de base de données principal

Sur chaque noeud, exécutez la commande de suppression et appuyez sur Y. Ne passez pas à la mise à niveau 4.0 jusqu'à ce que chaque noeud signale qu'il a quitté le cluster. La suppression de l'appartenance au cluster laisse la base de données locale de ce noeud en place.

database cluster remove

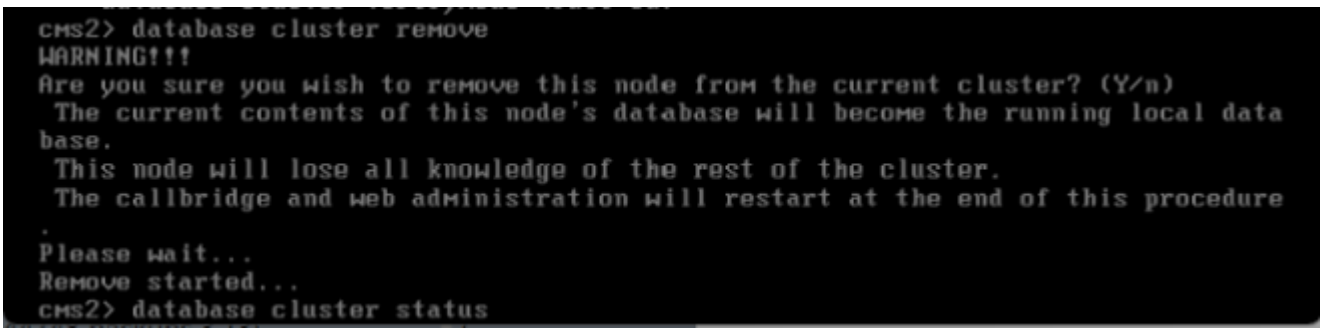


Figure 25 : Sur un réplica, confirmez Y pour supprimer l'appartenance au cluster. La base de données locale du noeud reste en place.

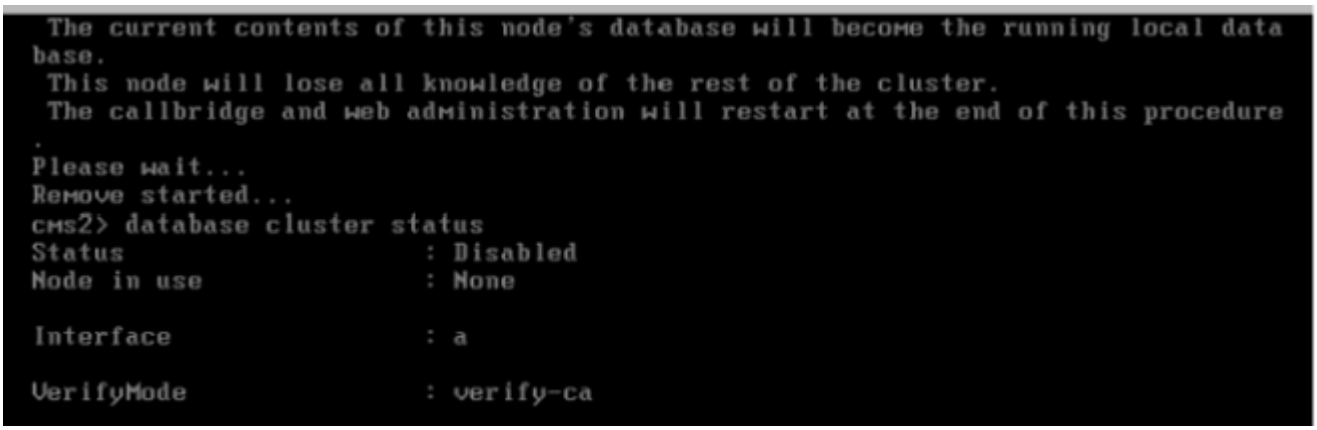


Figure 26 : Après la suppression, vérifiez que l'état du cluster est Désactivé et que le noeud utilisé est Aucun sur ce noeud.

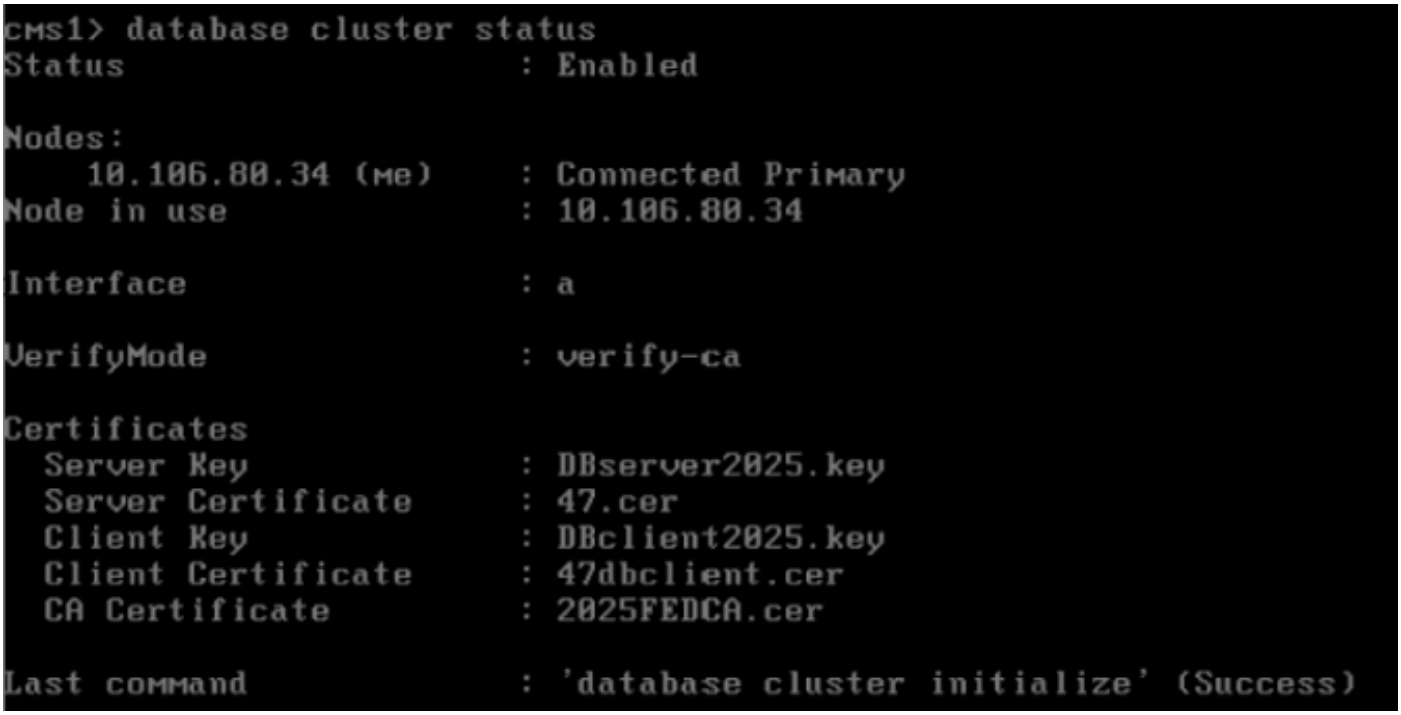


Figure 27 : Après la suppression des réplicas, l'ancien noeud principal est le seul noeud restant dans le cluster. Retirez-le en dernier.

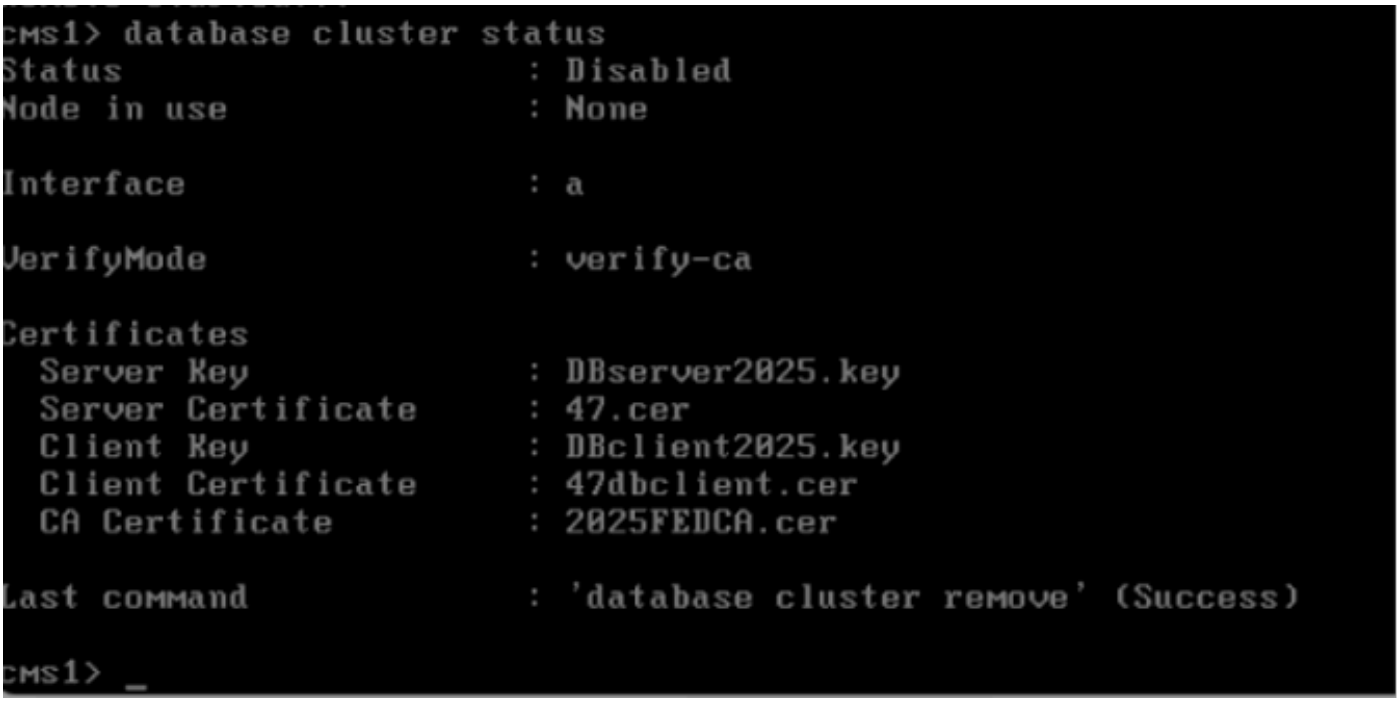


Figure 28 : Après avoir supprimé l'ancien serveur principal, vérifiez que la commande signale Réussite et que l'état du cluster est Désactivé.

Mise à niveau et restauration des noeuds

1. Une fois dissous, les noeuds sont autonomes et peuvent être mis à niveau en parallèle. Sur chaque noeud, copiez upgrade.img sur SFTP et exécutez la commande upgrade :

upgrade upgrade.img

2. Récupérez l’adressage réseau de chaque noeud à partir de la console (section First-boot and Network Restore).

3. Copiez la sauvegarde 3.13.x de chaque noeud sur ce noeud. Restaurez d'abord l'ancien serveur principal, puis les réplicas, puis les noeuds connectés. Utilisez la section Restaurer les données après la mise à niveau de la version 4.0. Une restauration des sauvegardes rétablit l'appartenance au cluster de base de données.

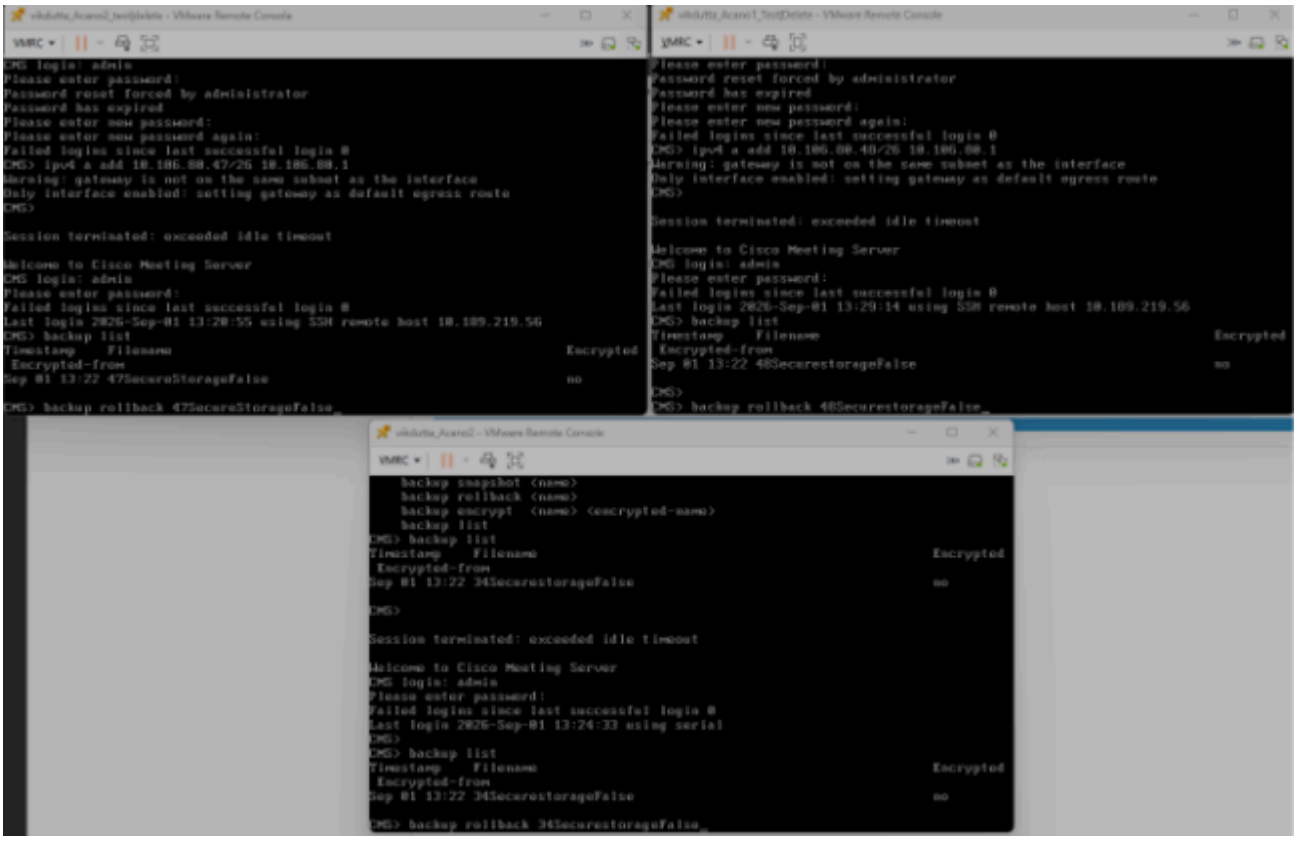


Figure 29 : Restaurer le propre snapshot de chaque noeud. Commencez par l'ancien réplica principal, puis restaurez les réplicas. Les exemples de noms de fichiers identifient leur noeud.

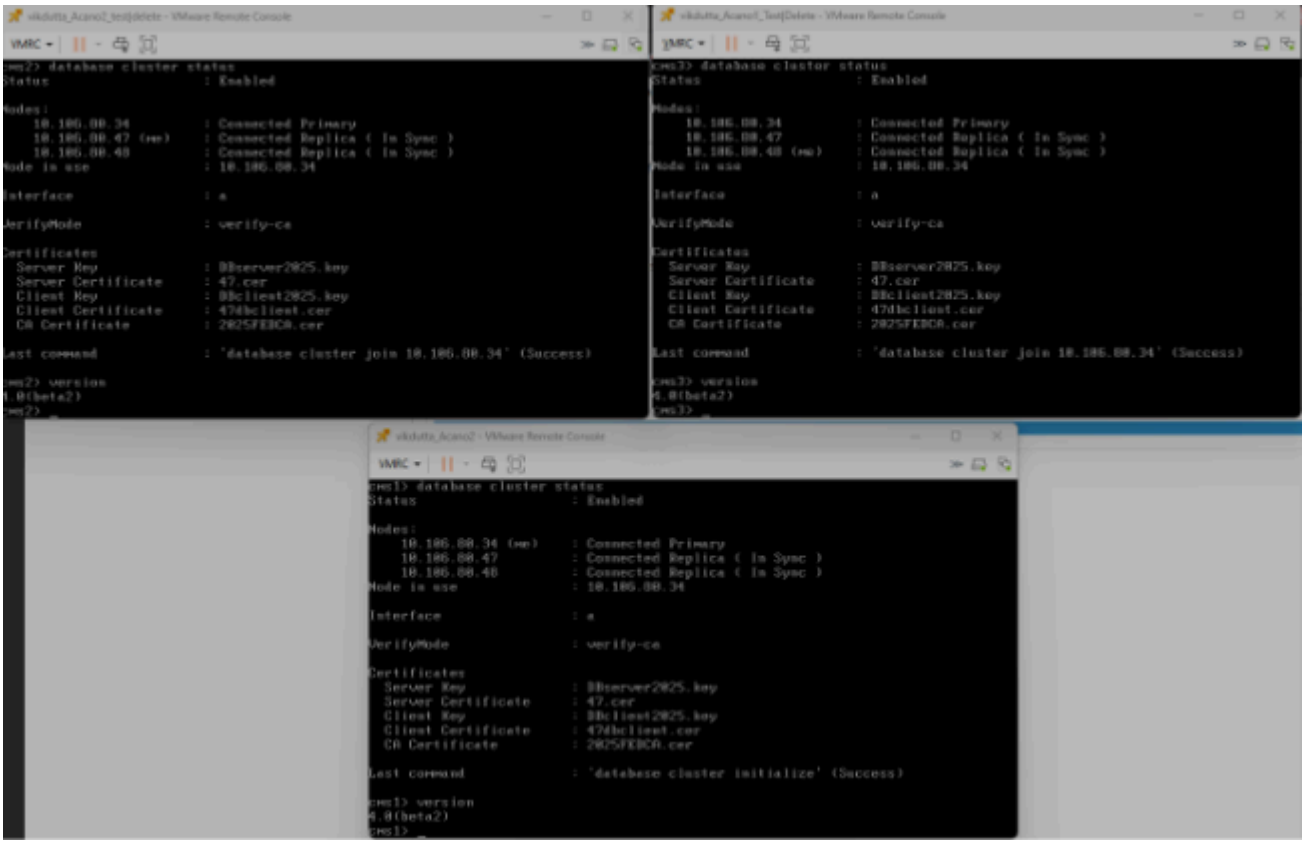


Figure 30 : Une fois la restauration effectuée sur Meeting Server 4.0, vérifiez que le cluster est activé, que le cluster principal est affiché et que les réplicas sont synchronisés.

Remarque : Si les connexions de cluster Pont d'appel ne s'établissent pas après cette restauration, exécutez l' **database cluster upgrade_schema** sur l'ancien pont principal uniquement, puis vérifiez à nouveau l'état Pont d'appel.

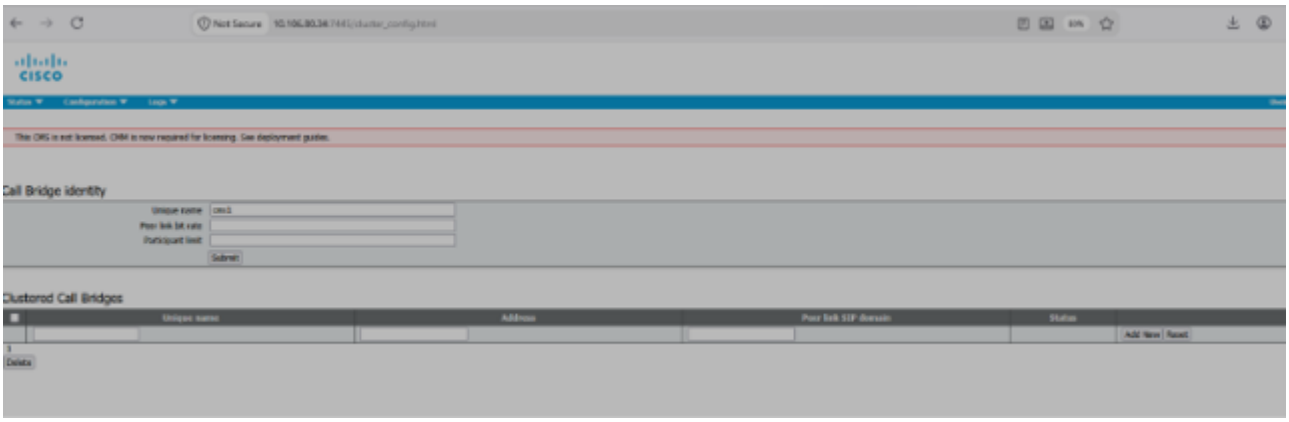


Figure 31 : Avant la mise à niveau du schéma, l'exemple montre le cluster de base de données en cours d'exécution alors que les ponts d'appels en cluster sont vides.

database cluster upgrade_schema

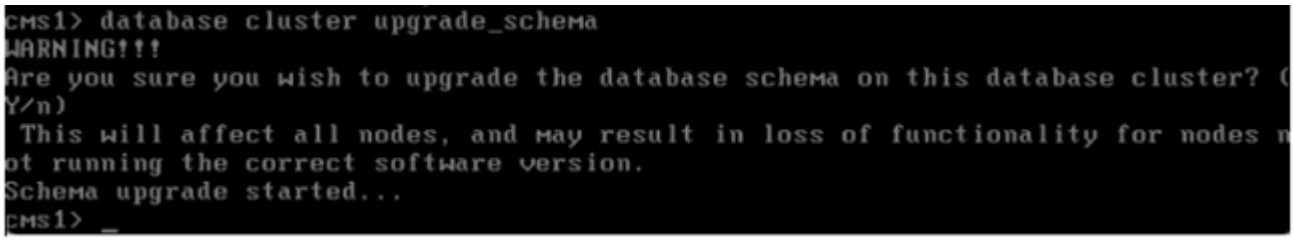


Figure 32 : Sur l'ancien cluster principal, confirmez Y uniquement lorsque les connexions de cluster Pont d'appel ont échoué après cette mise à niveau de cluster dissous.

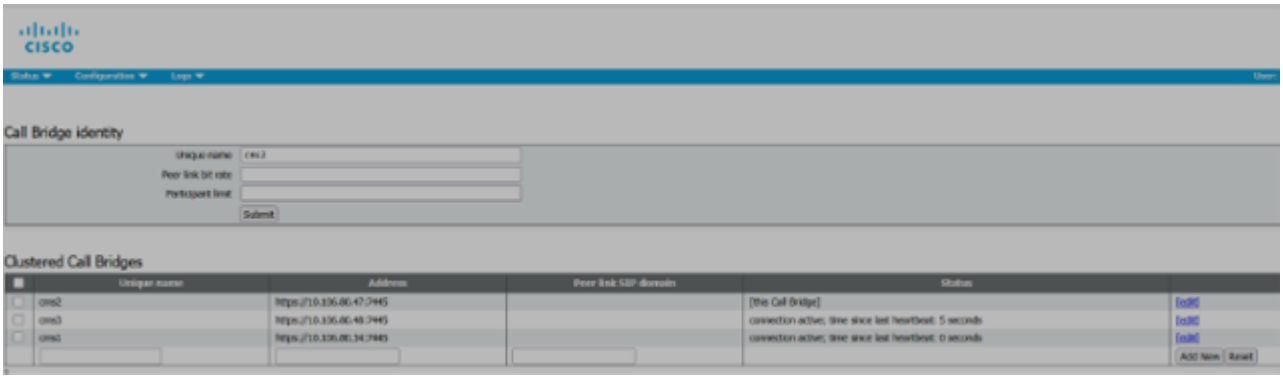


Figure 33 : Après la mise à niveau du schéma, vérifiez que chaque homologue Call Bridge affiche une connexion active.

4. Exécutez la procédure secrète MeetingApps dans la section MeetingApps Secret Key After Restore sur chaque pont Web, puis validez le déploiement à l'aide de la section Validation post-mise à niveau.

Scénario 4 - Cluster de base de données avec stockage sécurisé activé

Suivez cette procédure pour un cluster de base de données sur des machines virtuelles, Meeting Server Small ou Meeting Server Medium où le stockage sécurisé est activé sur les noeuds. Elle ne s'applique pas à Meeting Server 2000. Commencez par mettre à niveau chaque noeud vers la version 3.13.x.

Enregistrer les détails du cluster et créer des sauvegardes chiffrées

1. Exécutez secure_storage sur chaque noeud et confirmez Enabled : Vrai.

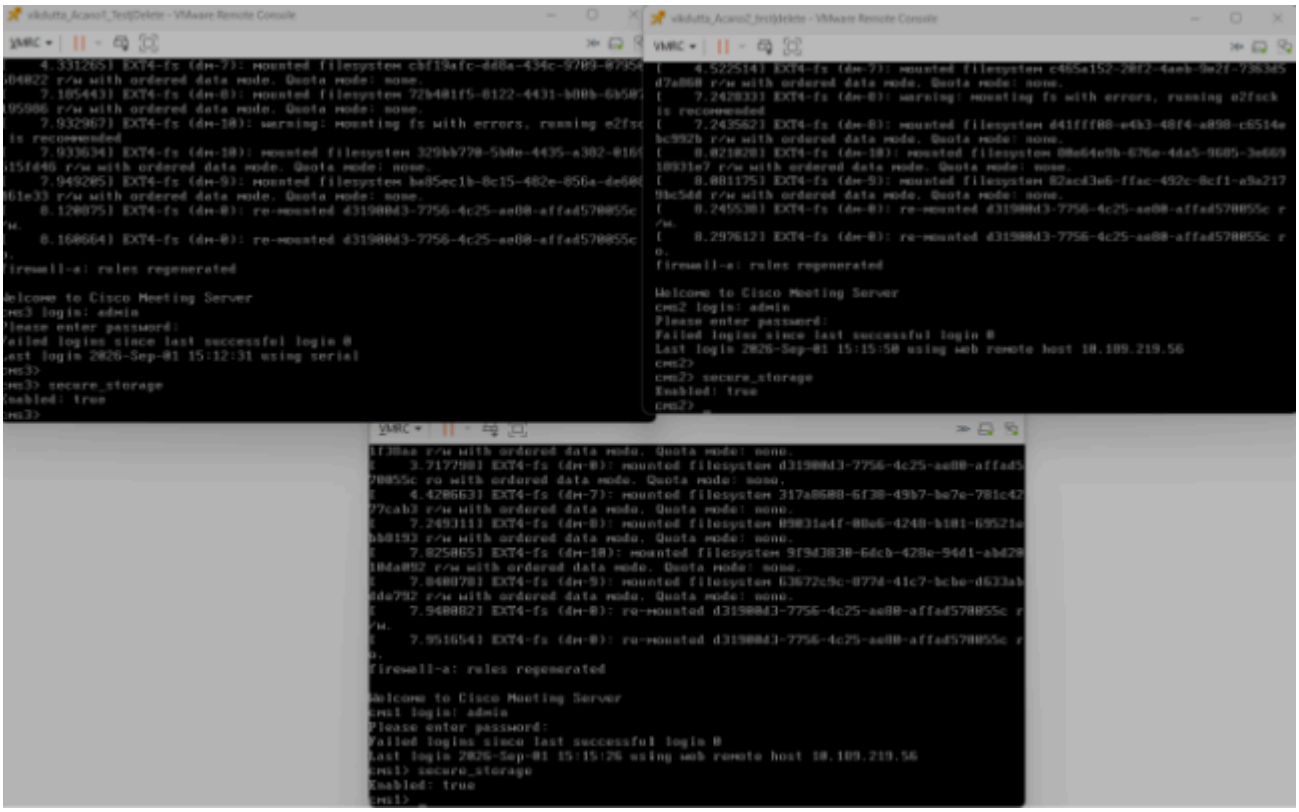


Figure 34 : Pour le cluster à trois noeuds illustré, vérifiez que le stockage sécurisé affiche Activé : True sur chaque noeud avant la mise à niveau.

2. Enregistrez la base de données principale actuelle et vérifiez que les réplicas sont synchronisés.

```
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)
```

Figure 35 : état du cluster de base de données avant la mise à niveau. Enregistrez les réplicas principaux et confirmez qu'ils sont synchronisés.

3. Vérifiez que tous les types d'appels utilisés fonctionnent et que les conditions de panne sont claires sur chaque noeud (section Valider l'état du serveur avant de créer des sauvegardes).

4. Créez une sauvegarde chiffrée de chaque noeud à l'aide de la section Effectuer une sauvegarde lorsque le stockage sécurisé est activé. Attribuez et enregistrez une phrase de passe unique pour chaque fichier ou utilisez une stratégie de phrase de passe documentée. Transférez uniquement les fichiers chiffrés hors des serveurs avant de dissoudre le cluster.

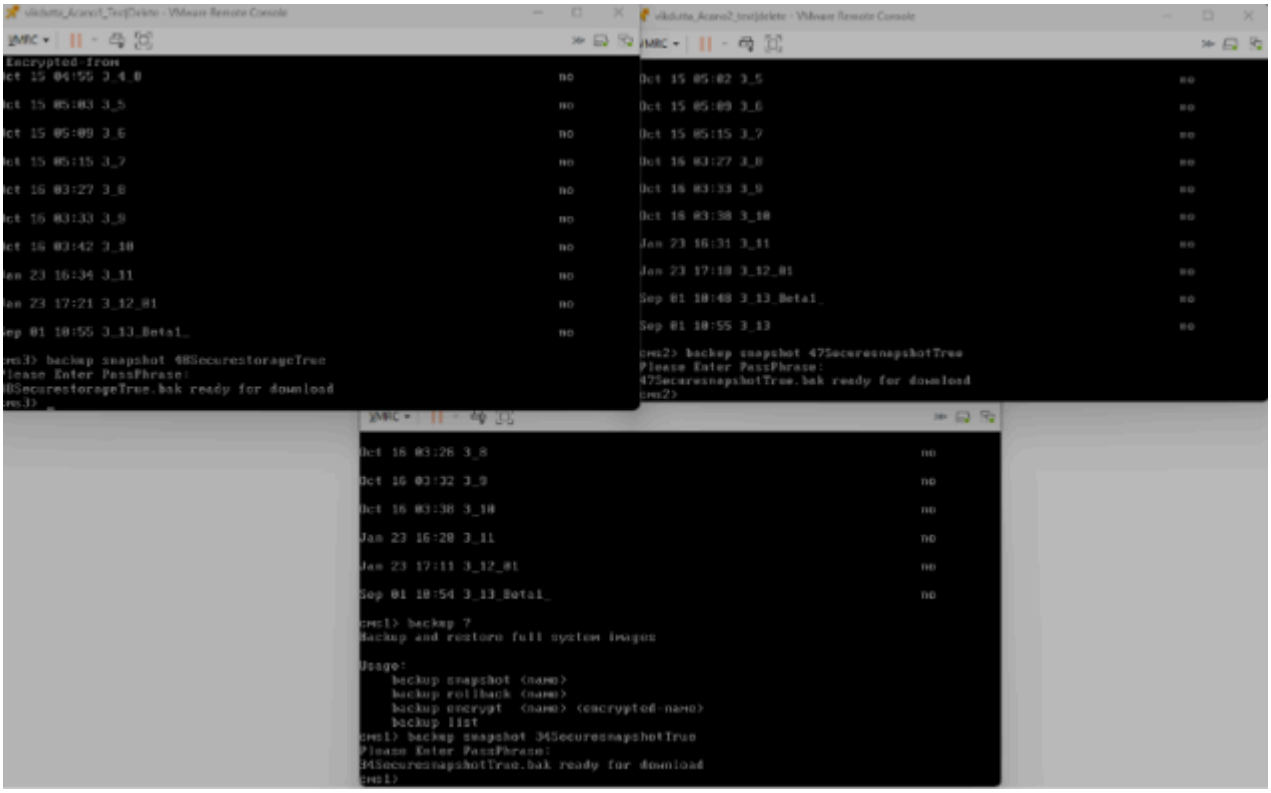


Figure 36 : Instantané de sauvegarde chiffré sur chaque noeud. L'exemple montre l'invite de phrase de passe, puis chaque fichier .bak prêt à être téléchargé.

Dissoudre, mettre à niveau et restaurer

Dissoudre le cluster comme décrit dans le scénario 3 dans cet ordre : les noeuds connectés, les réplicas et le dernier principal. Utilisez la suppression de cluster de base de données et vérifiez que chaque noeud a quitté le cluster.

Mettez à niveau les noeuds autonomes en parallèle. Récupérez l'adressage réseau à partir de la console (section First-boot and Network Restore).

Téléchargez la sauvegarde chiffrée de chaque noeud. Avant une restauration, vérifiez que le snapshot téléchargé apparaît dans la liste de sauvegarde en tant que Chiffré : oui. Restaurez d'abord l'ancien serveur principal, puis les réplicas et les noeuds connectés. Utilisez la commande backup rollback ci-dessous, confirmez Y, et entrez la phrase de passe de la sauvegarde lorsque vous y êtes invité. Le noeud redémarre une fois la phrase de passe acceptée. Répétez l' pour chaque noeud.

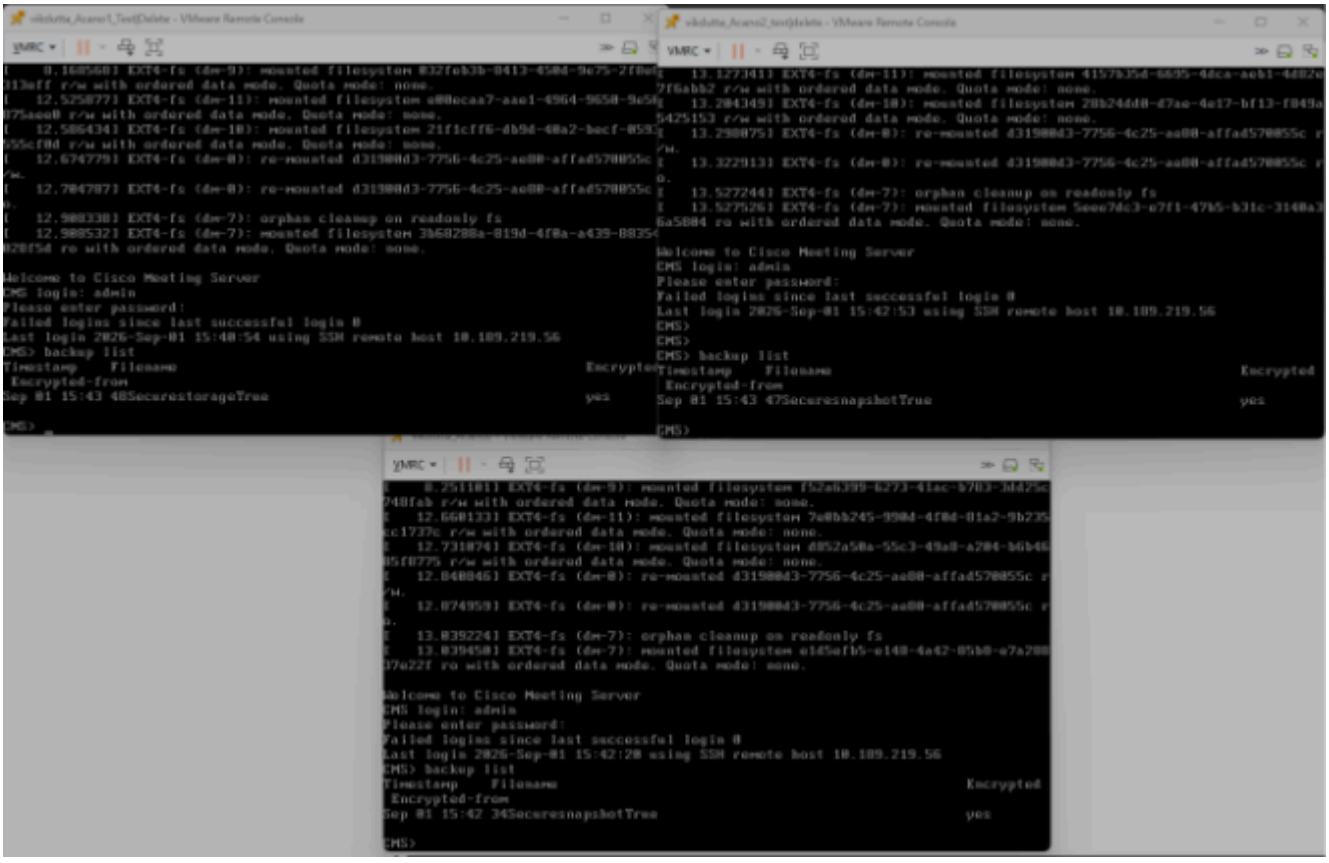


Figure 37 : Après le premier démarrage de la version 4.0, le snapshot chargé doit apparaître dans la liste de sauvegarde en tant que Encrypted : oui et soyez prêt pour la restauration.

backup rollback encrypted-filename

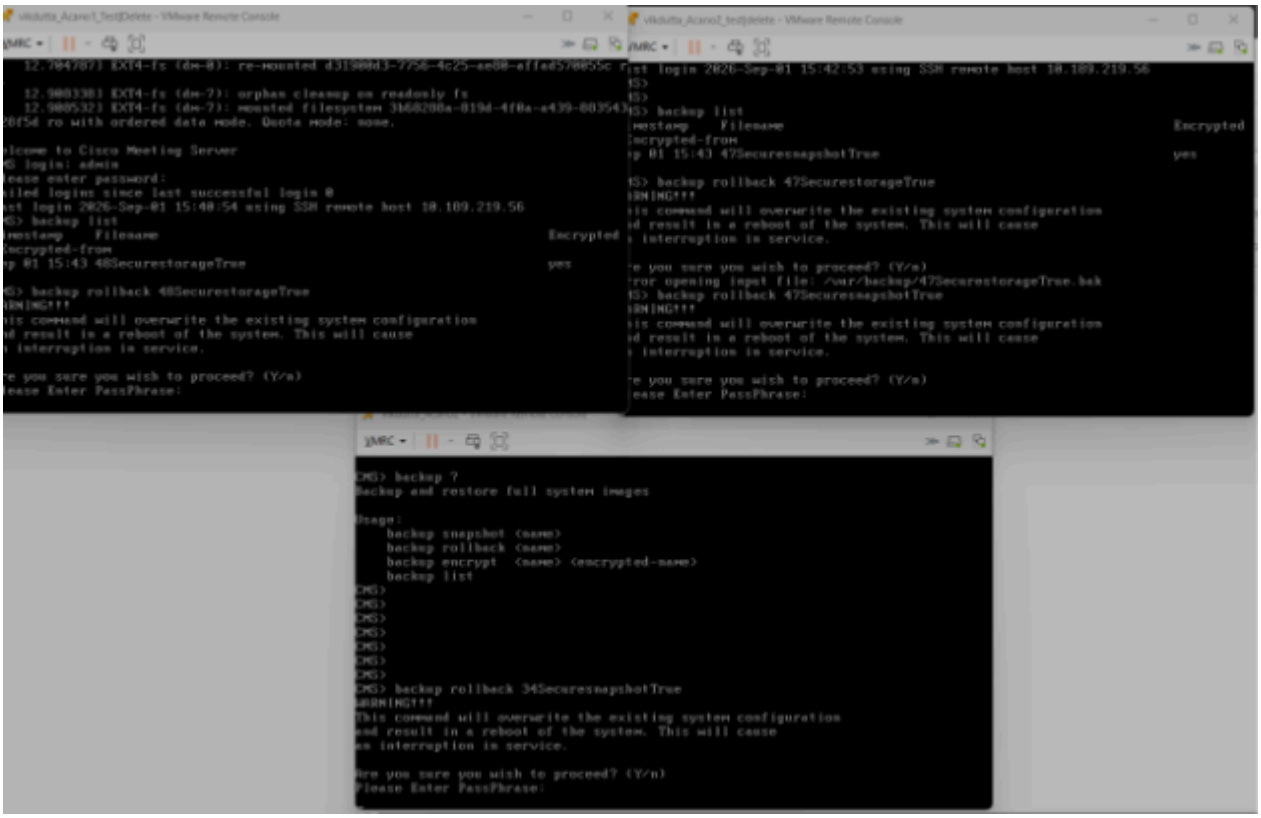


Figure 38 : Confirmez Y, saisissez la phrase de passe et restaurez d'abord l'ancien principal.

Remarque : Si les connexions de cluster Pont d'appel ne s'établissent pas après cette restauration, exécutez l' **database cluster upgrade_schema** sur l'ancien pont principal uniquement, puis vérifiez à nouveau l'état Pont d'appel.

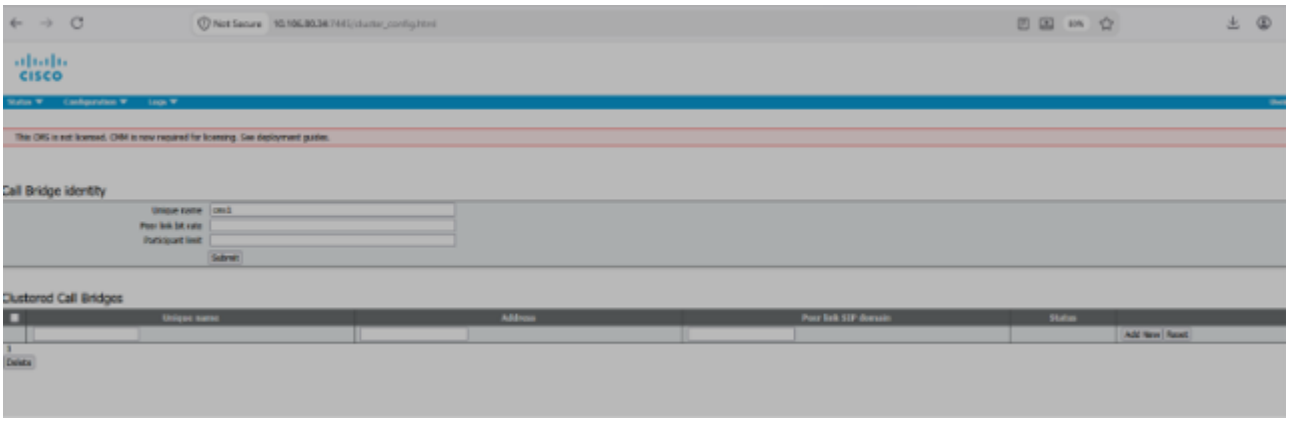


Figure 39 : Avant la mise à niveau du schéma, l'exemple montre le cluster de base de données en cours d'exécution alors que les ponts d'appels en cluster sont vides.

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> _
```

Figure 40 : Sur l'ancien cluster principal, confirmez Y uniquement lorsque les connexions de cluster Pont d'appel ont échoué après cette mise à niveau de cluster dissous.

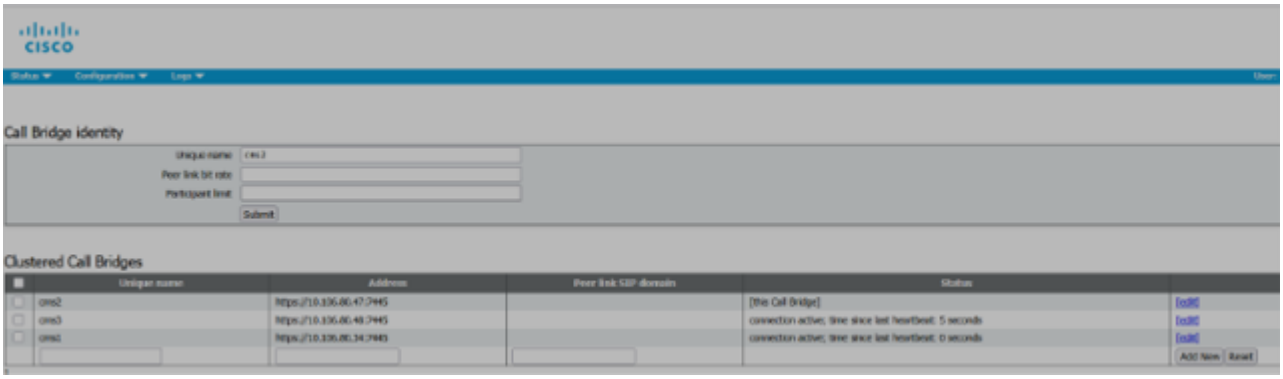


Figure 41 : Après la mise à niveau du schéma, vérifiez que chaque homologue Call Bridge affiche une connexion active.

Exécutez la procédure secrète MeetingApps dans la section MeetingApps Secret Key After Restore sur chaque pont Web, puis validez le déploiement à l'aide de la section Post-upgrade Validation.

Validation post-mise à niveau

Complétez cette liste de contrôle après la restauration et avant de remettre le système en production :

- L'administrateur Web de chaque noeud affiche Cisco Meeting Server 4.0.
- Les services MMP requis sont activés et en cours d'exécution (actif : Vrai).
- Les conditions de défaillance sont claires. Traiter les erreurs et avertissements récents comme des informations, sauf s'il existe une erreur correspondante.
- Le cas échéant, l'état du cluster de base de données indique les réplicas et le principal attendus.
- Les licences Smart et la connectivité Call Bridge sont restaurées.
- Les appels SIP et les appels du client Web App pris en charge par ce déploiement sont terminés avec succès.
- Les marques, les invites audio et les fichiers SSO copiés à partir du serveur dans la section Pre-upgrade Requirements sont restaurés s'ils n'étaient pas déjà inclus dans la sauvegarde.
- Si MeetingApps est déployé, Web Bridge affiche la nouvelle relation MeetingApps et le partage de fichiers fonctionne.
- Ne supprimez les instantanés de courte durée qu'après l'acceptation du déploiement.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.