Meeting Serverのリリース4.0へのアップグレード – ホワイトペーパー

内容

概要

背景説明

セキュアストレージの概要

- 対応プラットフォーム
- 実装の注意事項

アップグレードの原則と制約

- 必要なアップグレードパス
- ダウングレード
- 4.0アップグレードのための重要なバックアップ要件
- 最初のログインとパスワードの設定
- アップグレード後のネットワーク接続の再確立
- バックアップを作成する前にサーバーの状態を検証する

アップグレード前の要件

一般的なバックアップおよび復元手順

- 4.0アップグレード後の影響を受けるデータ
- セキュリティで保護された記憶域が無効または使用できない場合にバックアップを作成する
- セキュアストレージが有効な場合にバックアップを作成する
- 4.0アップグレード後のデータの復元
- 復元後のMeetingApps秘密キー

初回ブートとネットワークの復元

アップグレードシナリオ

- シナリオ1：セキュアストレージが無効または使用できないシングルノード
- シナリオ2：セキュアストレージが有効になっているシングルノード
- シナリオ3:Secure Storageが無効な状態のデータベースクラスタ
  - クラスタの詳細を記録し、すべてのノードをバックアップする
  - クラスタの解体
  - ノードのアップグレードと復元
- シナリオ4：セキュアなストレージが有効になっているデータベースクラスタ
  - クラスタの詳細の記録と暗号化バックアップの作成
  - 解体、アップグレード、復元

アップグレード後の検証

概要

このドキュメントでは、Cisco Meeting Server(CMS)をリリース4.0にアップグレードする方法に

ついて説明します。

背景説明

このドキュメントは、Cisco Meeting Serverリリースノート、MMPコマンドリファレンスガイド、およびSecure Storage Administratorリファレンスガイドと一緒に使用して、要件および前提条件を理解します。

Cisco Meeting Server 4.0のアップグレードプロセスは以前のバージョンとは異なります。これは、イメージを適用すると、ノードが工場出荷時の状態にリセットされるためです。サービスの継続性を確保するには、アップグレードを開始する前に、ネットワーク設定やパスワードを含む以前のすべての設定を、外部の場所にエクスポートしたバックアップを使用して保存しておく必要があります。

また、Cisco Meeting Server(CMS)バージョン3.11 ~ 3.13ではSecure Storageはオプションでしたが、バージョン4.0ではデフォルトで有効になっています。そのため、Secure Storageを使用したことがない場合、または3.11x、3.12x、または3.13xですでに有効にしている場合は、別のバックアップおよび復元手順に従う必要があります。

Secure Storageは、サーバー上の秘密キーとバックアップファイルを暗号化します。これらのファイルは、外部ストレージに転送する前に暗号化する必要があります。

このドキュメントでは、必要なガイダンスを1つのリファレンスにまとめています。そのため、同じ手順を繰り返さなくても、すべてのアップグレードシナリオで共通の手順に従うことができます。

このドキュメントでは、次のトピックを扱っています。

- 「Secure Storageとは何か」、「適用する場所」、「適用しない内容」。
- アップグレードパス。これには、4.0より前の3.13.xに到達する要件と、4.0からのダウングレードがサポートされていないという事実が含まれます。
- Secure Storageが有効になっているノードと、無効または使用できないノードに共通のバックアップおよびリストア方法。
- アップグレードの前にデータベースクラスタを解体する間の、データベースクラスタノードの解体順序。
- MeetingAppsの秘密鍵。Cisco Meeting Serverのバックアップには保存されず、復元後に再生成する必要があります。

注：このドキュメントでは、4.0ベータソフトウェアバージョンを含む最初のアップグレ

ードガイダンステストでキャプチャされたラボのスクリーンショットを使用しています。表示されるすべてのホスト名、IPアドレス、およびファイル名は厳密に例示されており、実際の実稼働環境のクレデンシャルや機密性の高いパスフレーズは反映されていません。明確さを維持し、冗長性を防ぐために、クラスタビューに必要な追加のコンテキストが表示されない限り、手順を繰り返しても共通手順セクションには1回しか表示されません。

セキュアストレージの概要

Secure Storageは、Meeting Serverに存在する機密ファイルを暗号化し、それらのファイルをCall Bridgeサーバからオフロードする方法を制御することで、強化されたデータセキュリティを提供します。この機能は、Cisco Meeting Server 3.11で、仮想マシン（Specificationベースまたは Meeting Server Small）およびMeeting Server Mediumに対してMMPコマンドsecure_storage enableを使用することで設定可能なオプションとして導入されました。

バージョン4.0以降では、セキュアストレージはデフォルトで有効になっています。この設定は永続的で元に戻すことができず、secure_storage enable MMPコマンドは削除されています。

Secure Storageを使用すると、会議サーバは次の動作を実行します。

- 秘密鍵は、暗号化されるまでSFTP経由でダウンロードできません。秘密キーを暗号化するには、pki encrypt MMPコマンドの後に最低14文字のパスフレーズを入力します。これにより、Meeting Serverサービスで現在使用されているキーは変更されません。
- backup encrypt <name> encrypted-nameコマンドで作成されたバックアップファイルは暗号化されます。セキュアな保存が有効な場合、backup encrypt <name> encrypted-name MMPコマンドにより、少なくとも14文字のパスフレーズの入力が求められます。バックアップの復元中も、同じパスフレーズが必要です。
- バックアップファイルは、ダウンロードする前に暗号化形式にする必要があります。リストされたバックアップがまだエクスポート用に暗号化されていない場合は、backup encrypt <name> encrypted-nameを使用します。 暗号化されていないバックアップのダウンロードは拒否されます。
- バージョン3.12から、セキュアストレージはFIPSが有効な場合でも動作できます。3.11で作成された、より短いパスフレーズを使用した秘密キーファイルは、14文字以上のパスフレーズを使用して再生成する必要があります。



ヒント:Secure Storageでは、Meeting Serverからの暗号化されていない秘密キーと暗号化されていないバックアップファイルの転送が制限されます。証明書ファイルの転送は制限されません。証明書はSFTPを使用してコピーできます。pkiで暗号化されるまで、関連付けられた暗号化されていない秘密鍵のみがブロックされます。

⚠ 注意：有効にした後は、どのMMPコマンドでもセキュアストレージを無効にすることはできません。この操作は元に戻せません。factory_reset full のみが、セキュアストレージをfalseにリセットします。セキュアストレージを有効にする前に、バックアップスナップショットを使用して設定のバックアップを作成し、別のデバイスに保存します。secure_storageの後に、ただちに再起動を有効にします。リブートがスキップされると、セキュアストレージが完全に初期化されずに有効とマークされ、factory_reset full などのコマンドが失敗する場合があります。この状態のリカバリパスは、以前に保存したスナップショットに戻すことです（これは3.13.xでのみ有効です）。 Meeting Server 4.0では、secure_storageはデフォルトで有効になっています。

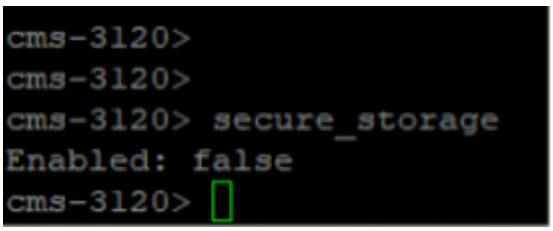
対応プラットフォーム

- 仮想マシン（仕様ベース）：サポート
- Meeting Server Small/1K：サポート
- Meeting Serverメディア：サポート
- Meeting Server 2000：サポートされていません。セキュリティで保護された記憶域の機能は使用できません。このプラットフォームではSecure Storageコマンドを使用しないでください。

Cisco Meeting Server 4.0は、互換性のあるすべてのプラットフォームでデフォルトでSecure Storageを有効にします。アップグレード後は、Secure Storageが無効になっている間に3.13.xバックアップが取られた場合でも、データはSecure Storageによって自動的に保護されます。

実装の注意事項

- アップグレードイメージの名前を変更しても、セキュリティで保護された記憶域の設定は変更されません。
- バックアップを作成する前に、コマンドsecure_storageを使用して、各ノードのセキュアストレージのステータスを確認します。
- このコマンドは、Secure Storageが有効(True)か無効(False)かを示します。 Meeting Server 2000では、このコマンドは適用できません。Cisco Meeting Server 2000をアップグレードする際は、「セキュアストレージが無効または使用できないアップグレード状況」で説明する手順に従ってください。



Secure Storageが有効になっていない場合のMMP出力(Enabled: false)。



図2: Cisco Meeting Server 3.13でSecure Storageが有効(Enabled: true)な場合のMMP出力

コマンド構文の詳細な警告と使用例については、『Cisco Meeting Server Administrator Quick Reference Guide for Secure Storage』および現在使用している『MMP Command Reference』を参照してください。

アップグレードの原則と制約

必要なアップグレードパス

Cisco Meeting Serverのアップグレードは、メジャーリリースをスキップすることなく、順次パスに従う必要があります。たとえば、3.11.x上のノードは、4.0に到達する前に3.12.xと3.13.xを通過する必要があります。3.9.xから3.13.xまたは3.11.xから4.0への初期バージョンからの直接アップグレードはサポートされておらず、通常は回復不能な設定エラーが発生します。バージョン3.11.5または3.13のMeeting Server Mediumの場合、アップグレードパスは3.11.5 → 3.13 → 4.0になります。

ヒント:4.0アップグレードを開始する前に、すべてのノードでCisco Meeting Server(CMS)3.13.xを実行し、その3.13.xシステムからエクスポートされた確認済みの設定バックアップを使用している必要があります。このドキュメントのすべてのシナリオ手順は、3.13.xへのアップグレードがすでに完了していることを前提としています。

ダウングレード

ヒント:4.0.xから3.13.xへのダウングレードはサポートされていません。アップグレードが失敗するか、システムが期待どおりに動作しない場合は、新しい3.13.x OVAを導入し（またはアプライアンスを再イメージングし）、3.13.xバックアップを復元します。追加のリカバリオプションとして、アップグレード期間中は3.13.x仮想マシンのハイパーバイザスナップショットを保持します。VMスナップショットは、エクスポートされた構成バックアップを置き換えません。

4.0アップグレードのための重要なバックアップ要件

4.0のアップグレードを確認した後、ノードは最初のブート状態でリブートします。アップグレードプロセス中に生成される自動バックアップには依存しないでください。アップグレードに失敗すると、SFTPアクセスが失われ、ファイルにアクセスできなくなる可能性があります。backup snapshotコマンドで作成され、外部ストレージにコピーされたバックアップだけを、確実にリカバリに使用できます。

最初のログインとパスワードの設定

バージョン4.0の最初のブート時に、既存のMMPパスワードがデータベースから削除されます。ユーザ名adminを使用し、パスワードを空白（パスワードなし）にしてログインします。 新しいMMPパスワードを設定する必要があります。確認と確認のためにパスワードを2回入力するように求められます。Meeting Serverにはパスワード回復機能がないため、新しいパスワードを記録してください。

注：最初のブート時に新しいMMPパスワードを設定すると、backup rollbackコマンドにより、そのパスワードが3.13.xバックアップに保存されていたパスワードに置き換えられます。サーバでバックアップを復元した後、バックアップの作成時にアクティブだったパスワードでログインする必要があります。

アップグレード後のネットワーク接続の再確立

IPv4およびIPv6アドレス、マスク、ゲートウェイは、残りの設定とともに失われます。Meeting Serverのネットワーク接続は、4.0へのアップグレード後に失われる可能性があります。MMPからアドレスを再度割り当てられるように、ハイパーバイザコンソール、CIMC、またはシリアルアクセスが必要です。

注:DHCP予約を使用する導入では、通常、リブート後も同じIPアドレスが維持されます。ただし、アドレスが確認されるまで、コンソールアクセスを使用できる状態にしておく必要があります。IPアドレスが確認されるまで、SSH接続は復元されません。

バックアップを作成する前にサーバーの状態を検証する

3.13にアップグレードするたびに、サーバが正常な状態であり、すべてのサービスが動作していることを確認します。サーバの概要ページの障害状態を無視しないでください。エラーまたは障害が発生した場合は、3.13でバックアップスナップショットを作成する前にこれらのエラーを修正します。これにより、アップグレードされた4.0ノードで正常なサーババックアップが復元され

、導入エラーが発生しなくなります。

Web AdminでStatusを開き、Fault conditionsセクションがクリアであることを確認します。[最近のエラーと警告]にのみ表示されるエントリを無視します。アップグレード後は、通常、データベースやWeb Bridge(WGB)の一時的なメッセージが表示されますが、これは復元の理由やバックアップの遅延にはなりません。

障害状態が約10分以上続く場合は、バックアップを実行する前に解決します。すでに障害が発生している3.13.xバックアップを4.0にリストアすると、障害が転送されます。

クラスタ化されたシステムでは、使用中のすべてのコールタイプ（SIPエンドポイントおよびWeb Appクライアント）が動作していること、および障害状態がノードにリストされていないことを確認します。

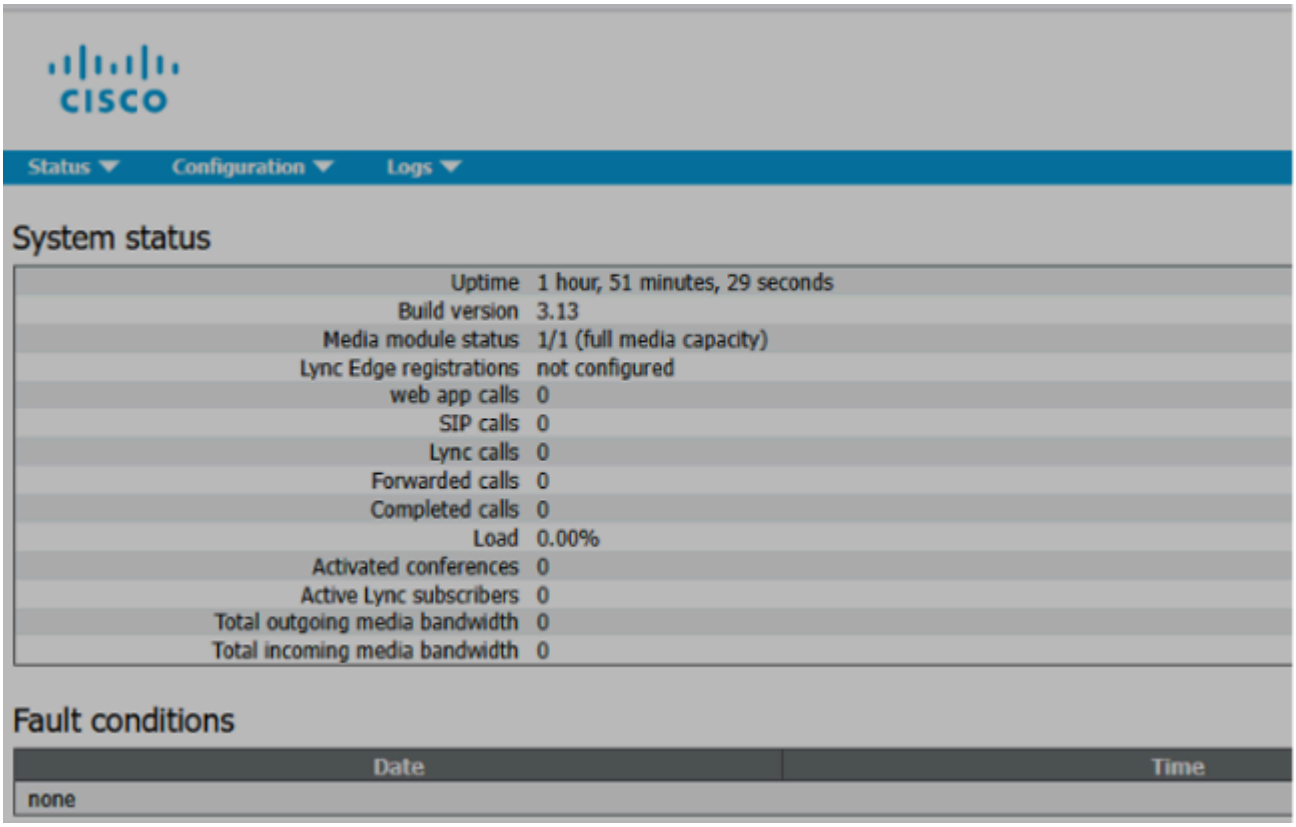


図3：障害状態が空白の3.13.xのWeb Admin Statusページ4.0に復元されたバックアップを作成する前に、このビューを使用します。

アップグレード前の要件

バージョン4.0へのアップグレードを開始する前に、次の操作を実行します。これらの要件は、このドキュメントで後述する4つのシナリオすべてに適用されます。

- 3.13.xにアップグレードしてから、設定バックアップをエクスポートします。ノードでCisco Meeting Server 3.13.xが実行されていることを確認します。バックアップを作成し、ロゴ、ブランディングファイル、音声プロンプト、SSOファイル、その他のカスタムデータなど、すべてのカスタムSFTPデータと一緒に外部ストレージに転送します。「一般的なバックアップと復元の手順」セクションに記載されている手順を使用します。クラスタ環境では、接続されたプライマリだけでなく、接続されたレプリカからもすべてのノードのバックアップを取ります。
- ネットワーク設定を記録します。ipv4 aを実行し、出力を保存します。DHCP予約によってIPアドレスが自動的に復元されない限り、4.0のリブート後にコンソールからこの情報を再入力する必要があります。
- コンソールアクセスを確認します。開始する前に、ハイパーバイザコンソール、CIMC、またはシリアルアクセスを使用できる必要があります。SSHは、ノードが4.0にリブートするとドロップすると想定されます。
- 現在のログバンドルをアーカイブ用にダウンロードします。各ノードからlogbundle.tar.gzを保存します。このバンドルは、バックアップスナップショットの代わりにはなりません。
- upgrade コマンドの実行後に4.0アップグレード警告バナーが表示されることを確認します。
- 前提条件が不完全な場合は、nを押して中止します。続行する準備ができたら、Yを押してください。

一般的なバックアップおよび復元手順

このドキュメントの後半で説明する4つのアップグレードシナリオでは、同じバックアップ、エクスポート、初回ブート、および復元パターンを使用します。このセクションを手順の唯一のソースとして使用し、シナリオ固有の順序（単一ノードとクラスタ、およびSecure Storageがすでに有効になっているかどうか）にのみ従います。

4.0アップグレード後の影響を受けるデータ

このデータは、4.0アップグレード後にバックアップを復元するまで失われます。

- スペース、ユーザ、およびコールプロファイルを含むデータベースの内容。
- 証明書と秘密鍵。
- ローカルカスタマイズ、SSOファイル、および音声プロンプトファイル
- ネットワーク設定（IPアドレス、マスク、およびゲートウェイ）。ただし、DHCP予約によってアドレスが復元される場合を除く。
- バックアップのロールバックによってバックアップからパスワードが再適用されるまで、以前のMMPパスワード。
- Call Bridge、Web Admin、Web Bridge、およびその他のアプリケーションサービスは、復元後にのみ復帰します。

ヒント:Cisco Meeting ServerのバックアップにはMeetingApps秘密キーが含まれていません。復元後、そのキーを再生成し、すべてのWeb Bridgeノードに適用する必要があります。「復元後のMeetingApps秘密鍵」セクションを参照してください。

セキュリティで保護された記憶域が無効または使用できない場合にバックアップを作成する

仮想マシン、Meeting Server Small、およびMeeting Server Medium（secure_storageがEnabled: Falseと報告された場合）、およびMeeting Server 2000（Secure Storageが使用できない場合）で、次の手順を実行します。

1. 各ノードで、backup snapshotコマンドを使用してファイルを作成します。以前のファイル名は再利用しないでください。

2. バックアップファイルをSFTPで外部ストレージに直ちにコピーします。Meeting Serverにコピーのみを保持しないでください。

3. ノードが再構築された場合でも到達可能な場所にファイルを保存します。

例：

バックアップスナップショットcms313SecurestorageFalseバックアップリスト

4. ファイルがbackup listコマンドに表示されることを確認してから、SFTPクライアントを使用して外部ディスクに転送します。

5. クラスタ内のすべてのノードでこのプロセスを繰り返します。バックアップ名に使用できるのは、アルファベット、数字、アンダースコア、ハイフンのみです。バックアップファイルを作成する場合は、.bakファイル拡張子を含めないでください。たとえば、3.13SecurestorageFalseなどのファイル名は、ピリオドが理由で拒否されます。

```
    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>
```

図4：バックアップスナップショットは、ピリオドを含む名前を拒否し、英数字の名前を付けて成功します。これで.bakファイルをダウンロードする準備が整いました。



図5: Meeting ServerのSFTPルートから外部ストレージに.bakファイルをコピーします。サーバにコピーのみを残さないでください。

セキュアストレージが有効な場合にバックアップを作成する

secure_storageがEnabled: Trueをレポートする場合は、次の手順を使用します。暗号化されていないバックアップファイルはダウンロードできません。

1. 各ノードでバックアップスナップショットを作成します。Secure Storageを有効にすると、サーバは少なくとも14文字のパスフレーズの入力を求めます。パスフレーズには、文字、数字、特殊文字、記号、またはスペースを使用できます。

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

図6：バックアップスナップショットとセキュアストレージを有効にすると、パスフレーズの入力が14文字以上で一度求められます。MMPでは、確認は求められません。

2. MMPでは、確認のためにパスフレーズを再入力するように求められることはありません。ファイルを復元するには同じパスフレーズが必要なので、パスフレーズを保護してください。簡単なパスフレーズや例のパスフレーズは選択しないでください。

3. backup listコマンドで、エクスポート用に暗号化されていないスナップショットが表示される場合は、ダウンロードする前に暗号化してください。

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

図7：暗号化前のバックアップリスト[暗号化]列は[いいえ]なので、ファイルをダウンロードできません。

4. 暗号化されていないバックアップをダウンロードしようとすると、SFTPによってアクセス拒否エラーが返され、backup encryptコマンドを最初に実行するように指示されます。

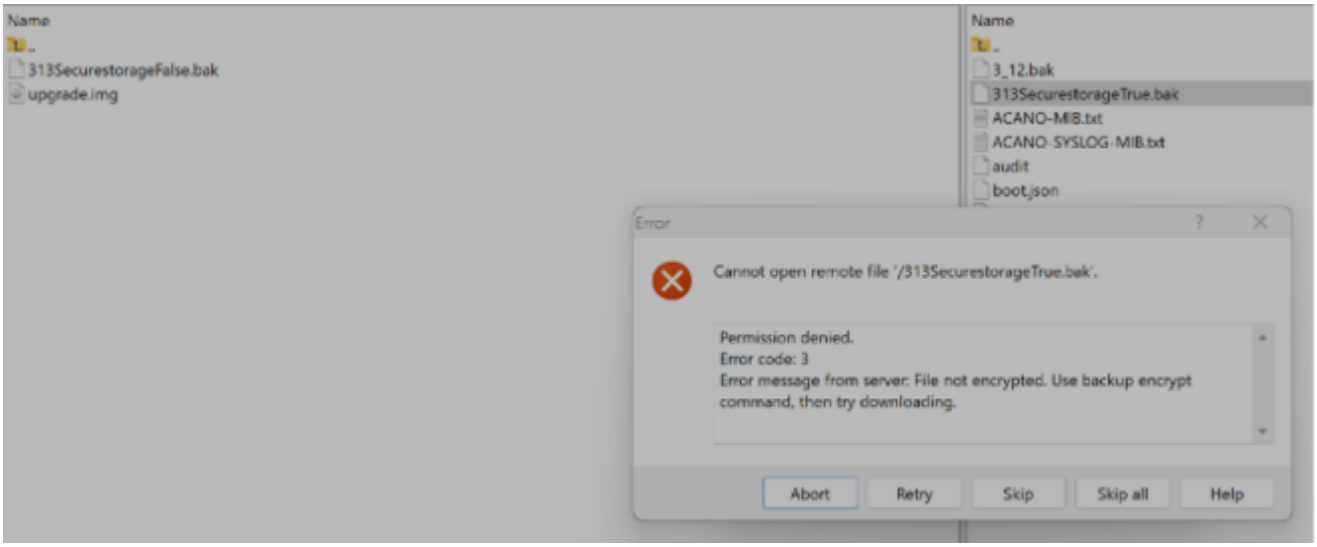


図8：セキュアストレージが有効な場合、SFTPは暗号化されていないバックアップのダウンロードを拒否します。サーバのメッセージは、バックアップの暗号化を実行するように指示しています。

5. バックアップファイルを暗号化するために、backup encryptコマンドを実行します。

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

図9：スナップショットが暗号化された後のバックアップリスト暗号化は可能で、ファイルはSFTPで転送できます。

バックアップ・リストには、暗号化ステータスと元のファイル名が表示されます。クラスタ内の各ノードから暗号化されたファイルだけを転送するようにしてください。各ノード、対応するファイル名、および関連するパスフレーズの記録を整理して保持します。

秘密キーもエクスポートする必要がある場合は、最初に各キーを暗号化します。証明書ファイルはSecure Storageによってブロックされないため、この追加の手順を行わずにコピーできます。

pki暗号化private.key encrypted_private.key

サービスで現在使用されているキーを上書きするのではなく、一意のファイル名を使用します。14文字のパスフレーズの最小要件も同様に適用されます。

4.0アップグレード後のデータの復元

1.「初回ブートとネットワークの復元」セクションで初回ブート時のログインとネットワークの回復後に、対応する3.13.xのバックアップをSFTPを使用してノードにコピーし、復元します。

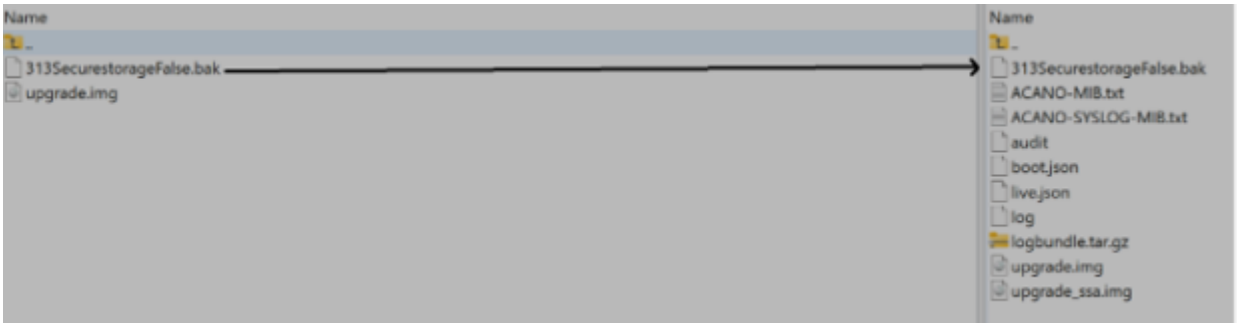


図10：最初のブートネットワークの回復後、SFTPを使用して3.13.x .bakファイルを4.0ノードにコピーし直します。

2. ファイルが存在するかどうかを確認します。

バックアップリスト

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

cms-3120>
```

図11：ロールバックの前に、アップロードされたスナップショットが存在することを確認する4.0のバックアップリスト。

3. スナップショットをリストアします。クラスタ環境では、最初に元のデータベースのプライマリをリストアし、次にレプリカ、続いて接続されたノードをリストアします。

backup rollbackバックアップファイルの名前

```
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...
```

図12：暗号化されていないスナップショットのバックアップロールバックYで確認します。ノードはバックアップを抽出し、リブートします。

4. Yを押して続行します。ノードがバックアップを抽出する間、リブートします。バックアップがSecure Storageを有効にした状態で作成された場合、MMPはパスフレーズの入力を求めます。

正しいパスフレーズが受け入れられるまで、再起動は実行されません。

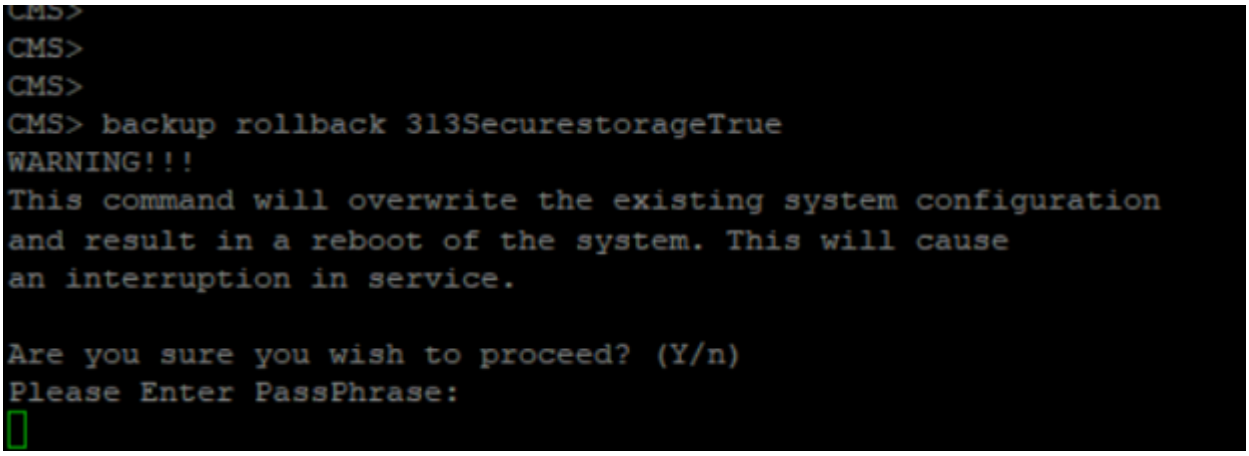


図13：暗号化されたスナップショットのバックアップロールバックYの後、MMPはバックアップが作成されたときに使用されたパスフレーズの入力を求めます。

⚠ 注意:**backup rollback**コマンドを実行すると、現在の設定、証明書、秘密鍵、およびライセンスファイルが上書きされ、サーバがリブートされます。このアップグレード用にエクスポートした3.13.xバックアップでのみ使用してください。

---

5. ノードがオンラインに戻ったら、バックアップからMMPクレデンシャルを使用してサインインし、各必要なサービスが有効で実行中であると報告されることを確認します（MMPはこれをアクティブとして示します： True）。

一般的なチェック：

callbridge webbridge3 webadmin scheduler recorder streamer uploader meetingapps

6. このノードがホストすることになっているサービスのコマンドのみを実行します。

復元後のMeetingApps秘密キー

Cisco Meeting ServerのバックアップにMeetingApps秘密鍵が保存されません。バックアップロールバックが完了したら、シークレットを再生成して、すべてのWeb Bridgeノードに適用します。この手順をスキップすると、他のサービスが正常に動作しているように見えても、ファイル共有は使用できなくなります。

1. MeetingAppsノードで、meetingapps gensecretコマンドを実行します。

2. 生成されたシークレットをシークレットストアにコピーします。meetingapps gensecretを実行するたびに以前のキーが無効になります。そのため、キーを1回生成すると、すべてのWebブリッジで同じ値が再利用されます。

3. すべてのWeb Bridgeノードで次のコマンドを実行します。

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

最後のコマンドは、Web Bridgeサービスが実行されていること、およびMeetingAppsが正しく設定されていることを確認します。MeetingAppsはMeeting Server 2000ではサポートされていません。また、Meeting Server 2000を含むクラスタではファイル共有を使用できません。このような導入では、この手順は適用されません。

初回ブートとネットワークの復元

4.0 upgradeコマンドでは、処理が進む前に警告バナーが表示されます。メッセージを注意深く確認し、前提条件が不完全な場合はnを指定して中断します。Yを押し続けると、ノードがリブートし、SSHセッションが切断されます。残りの手順はコンソールから実行する必要があります。

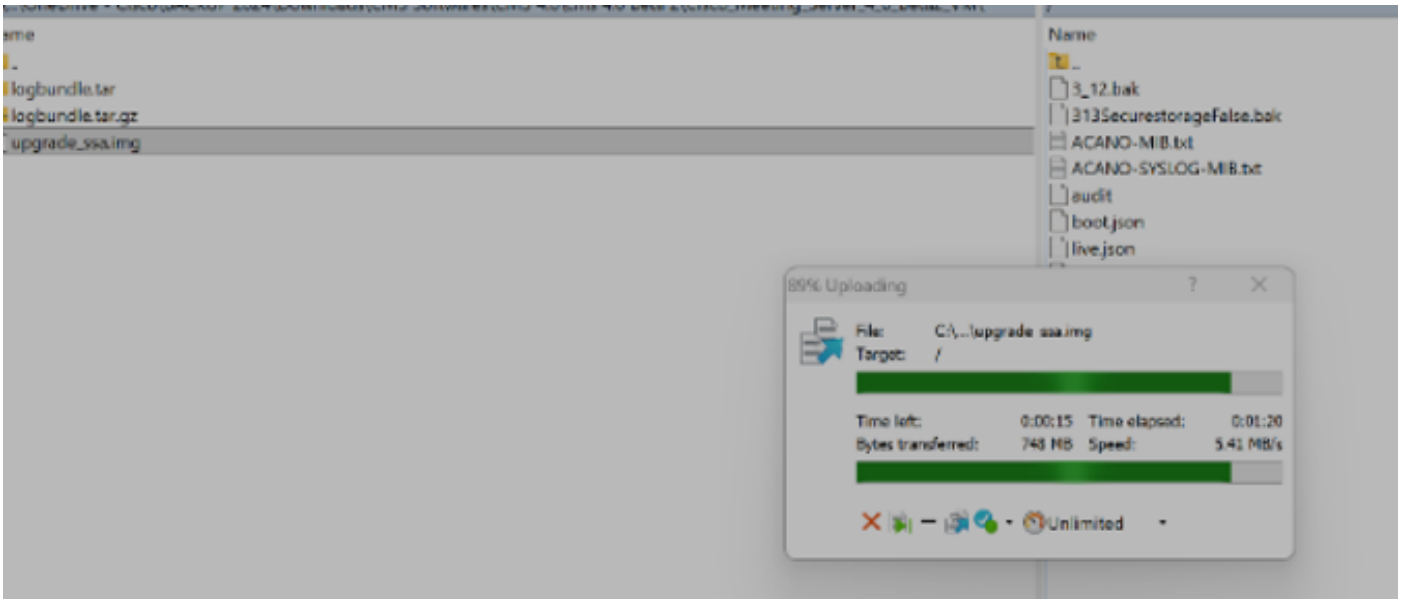


図14:Meeting Server SFTPルートディレクトリへの4.0アップグレードイメージのアップロードアップグレードイメージのファイル名は、cisco.comからダウンロードしたパッケージによって異なる場合があります。

```
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...
```

図15:upgradeコマンドはイメージの署名を確認し、プロセスを開始します。この時点で作成される自動バックアップに依存しないでください。

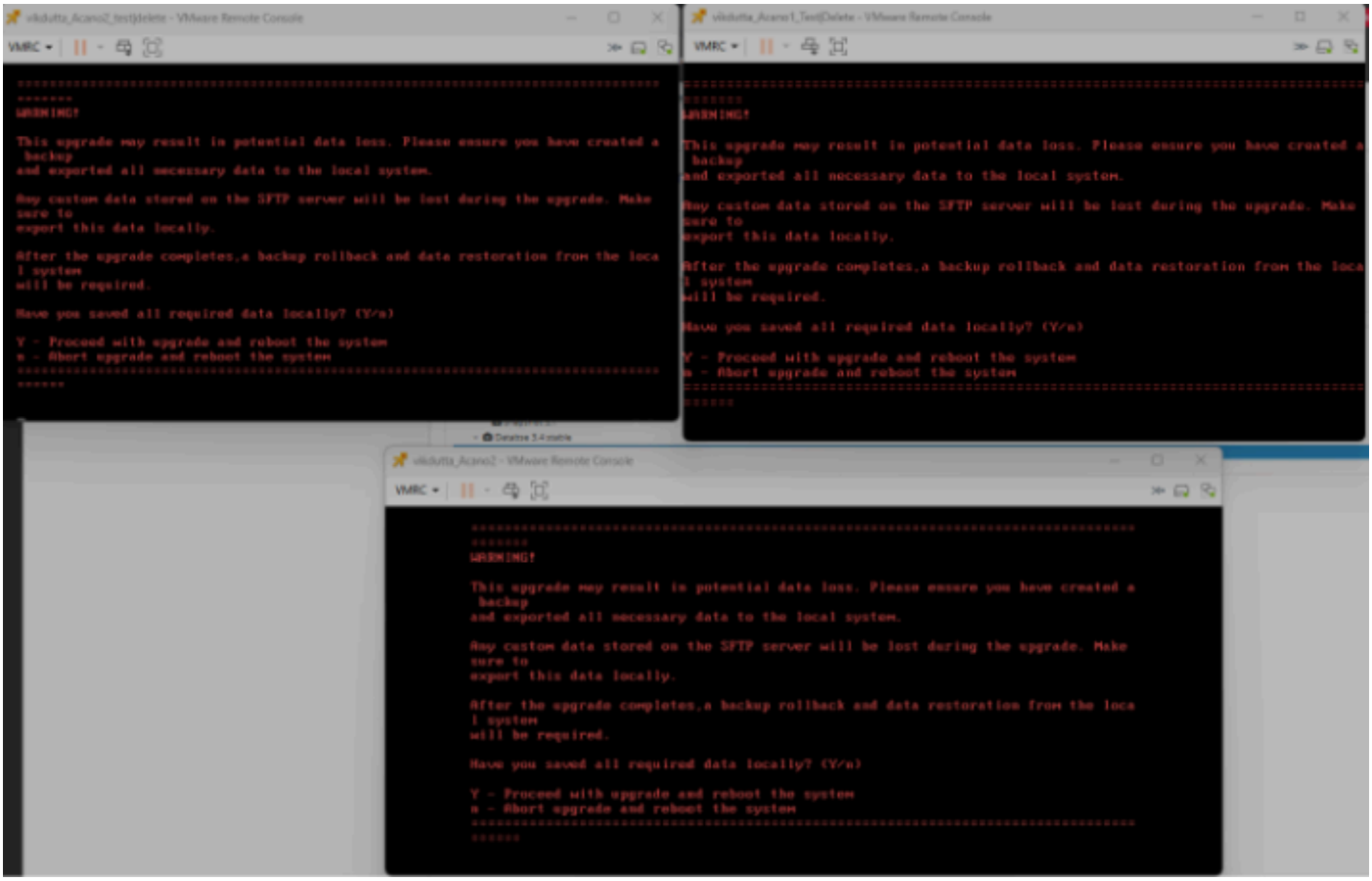


図16:3ノードクラスタでの赤色のMMP警告同じバナーが1つのノードに表示されます。バックアップとカスタムデータがサーバから外れていない場合は、nを押して中止します。続行して再起動する場合のみYを押します。

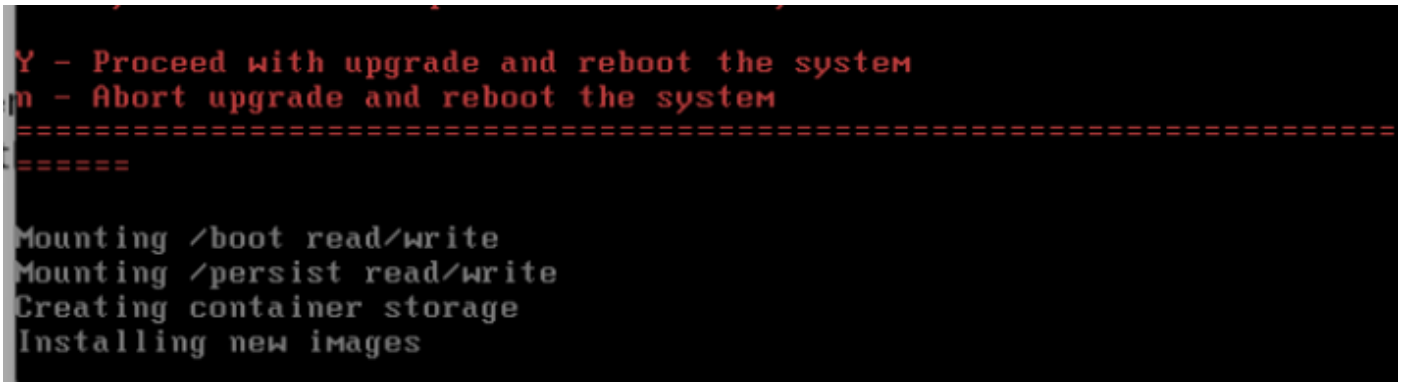


図17: Yの後、ノードはストレージをマウントし、4.0イメージをインストールします。SSHセッションがタイムアウトします。ハイパーバイザコンソールから続行します。

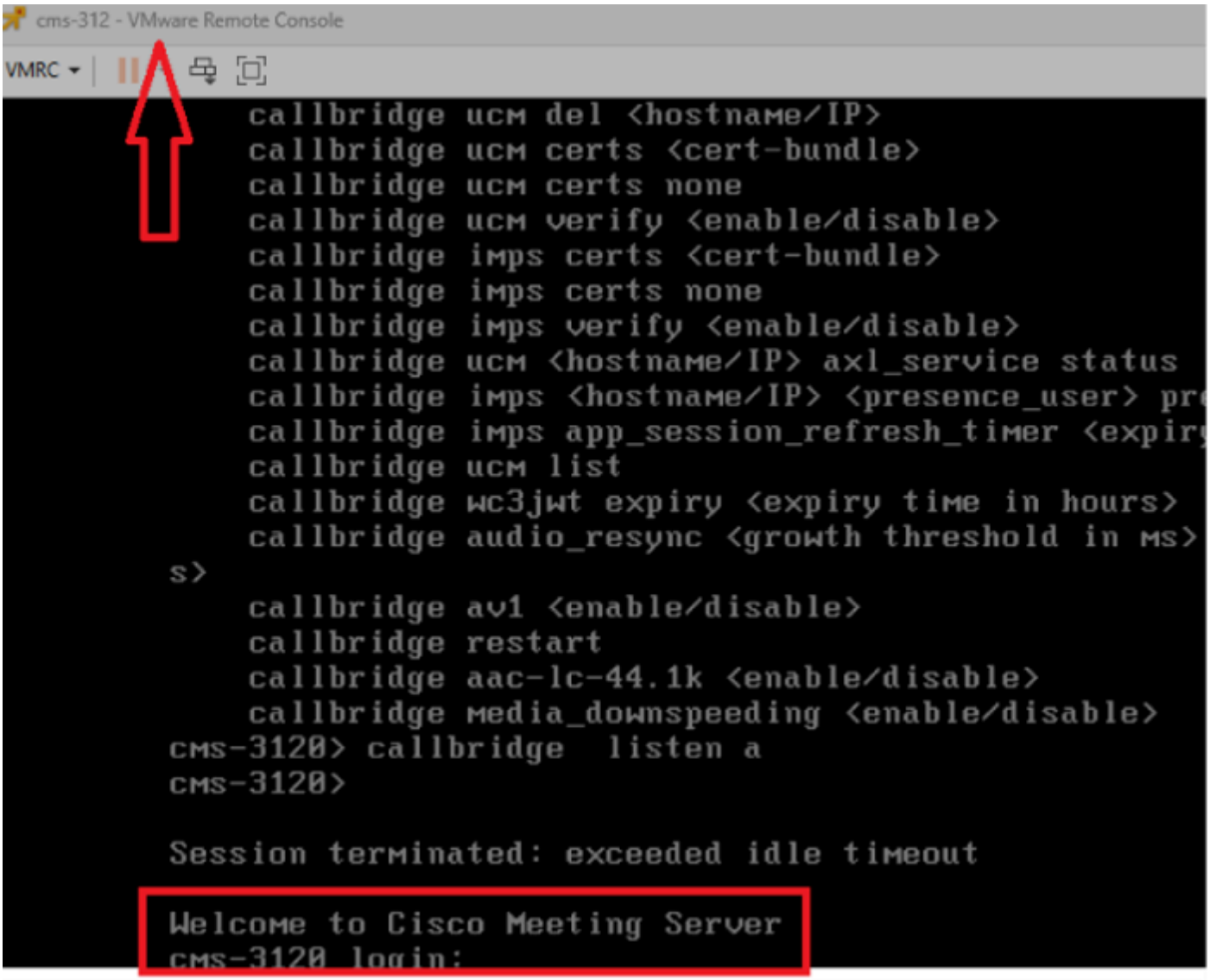


図18:SSHがドロップした後でVMまたはCIMCコンソールを使用する。4.0イメージの準備が整うと、最初のブートログインプロンプトが表示されます。

1. 最初に起動するMMPアカウント（ユーザ名admin、パスワードなし）でログインし、プロンプトが表示されたら新しいMMPパスワードを設定します。backup rollbackは、このパスワードをバックアップに保存されているパスワードに置き換えます。

2. 「アップグレード前の要件」セクションでキャプチャしたメモから、ネットワーク設定を再適用します。

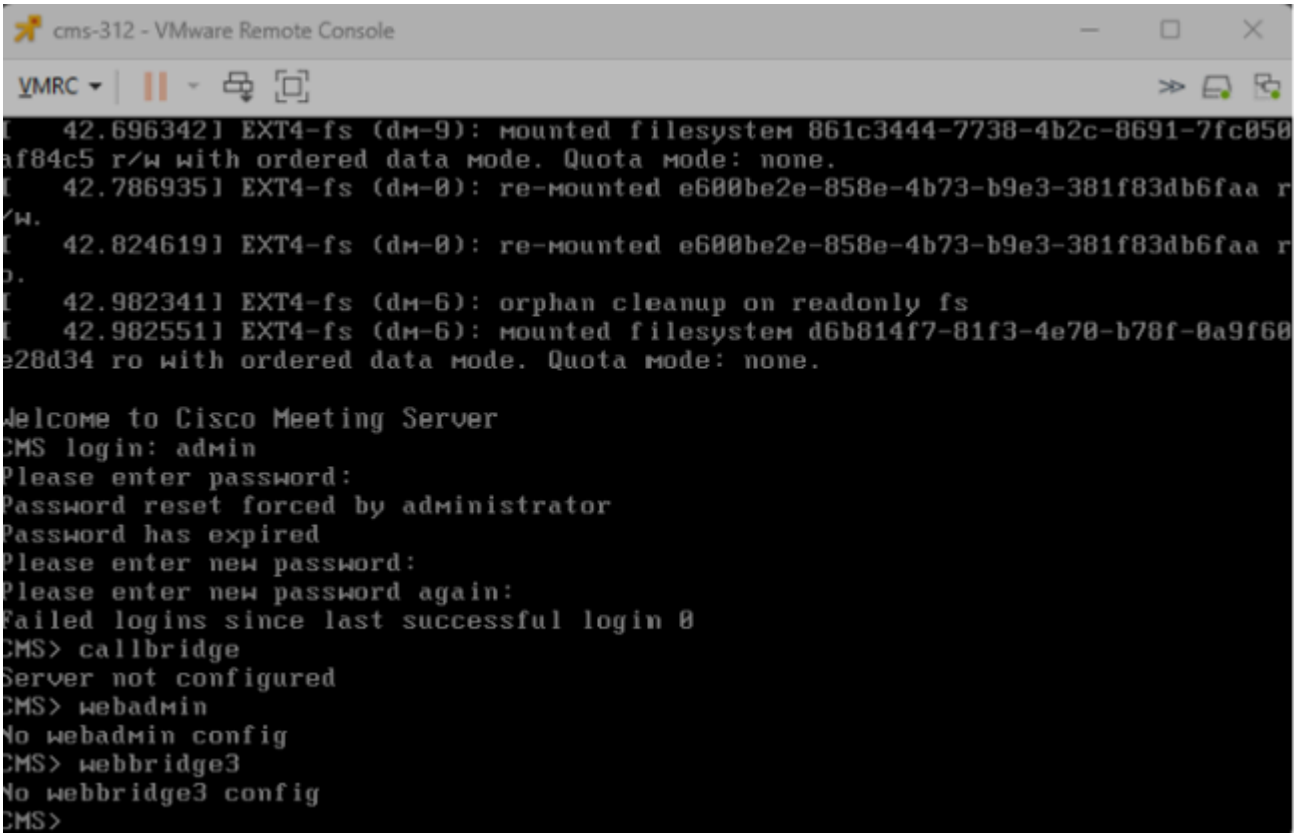


図19：最初のブートMMPログイン

以前のパスワードは無効になりました。新しいパスワードを設定すると、webadminやwebbridge3などのサービスは、バックアップが復元されるまで未設定として表示されます。

3. 次のコマンドを実行します。

ipv4インターフェイスアドレス/プレフィクス長ゲートウェイの追加

以下に、いくつかの例を示します。

ipv4 a add 192.0.2.10/24 192.0.2.1

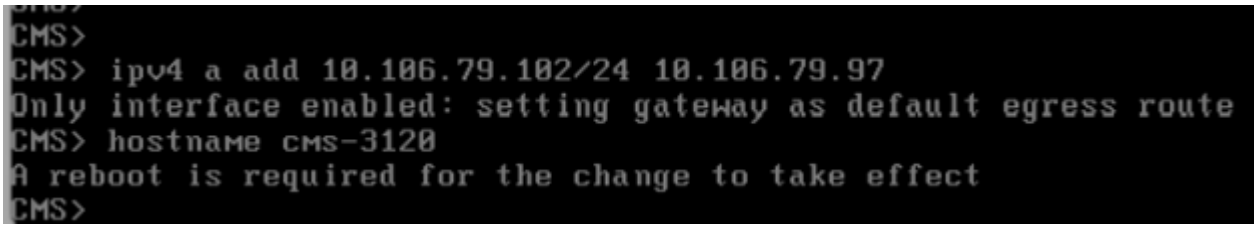


図20：コンソールからのIPv4の再適用

アドレスを割り当てた後、リブートする必要があります。スクリーンショットに示されているアドレスは、単なる例です。

4. アドレスを割り当てた後、再起動します。システムがオンラインに戻ったら、「4.0アップグレード後のデータの復元」セクションで説明されているバックアップと復元のSFTPアップロードを続行します。

注:DHCP予約が設定されている場合は、リブート後に元のアドレスがすでに割り当てられている可能性があります。管理ワークステーションからSFTPセッションを開始する前に、**ipv4 a**を使用してアドレスを確認します。

Cisco Meeting Server 4.0では、Secure Storageをサポートするプラットフォームでは、デフォルトで有効になっています。アップグレード後、MMPではsecure_storageをトグルとして公開できなくなりました。



図21：この4.0イメージでは、secure_storageはデフォルトで有効になっているため、認識されないコマンドです。

versionコマンドを使用して、リリースを確認します。

アップグレードシナリオ

この章では、さまざまなアップグレードシナリオについて説明します。3.13.xへのアップグレード手順を完了します。導入タイプを特定し、それに応じてシナリオを選択します。ご使用の環境に合った手順に従ってください。クラスタ展開とシングルノード展開の手順を組み合わせないでください。

まず、サポートされているステップアップグレードを3.13.xに完了します。次に、次のシナリオを1つだけ選択します。単一ノードとデータベースクラスタの手順を組み合わせないでください。

- シナリオ1：シングルノード、無効または使用不可能、VM、小規模、中規模、および Meeting Server 2000
- シナリオ2：単一ノード、有効、VM、小規模、中規模のみ
- シナリオ3：データベースクラスタ、無効または使用不可能、VM、小規模、中規模、および

Meeting Server 2000
- シナリオ4：データベースクラスタ、有効、VM、小規模、中規模のみ

Meeting Server 2000は、セキュアストレージ対応のシナリオをサポートしていません。そのプラットフォームでは、必要に応じてシナリオ1または3を使用します。

シナリオ1：セキュアストレージが無効または使用できないシングルノード

この手順は、Secure Storageが無効になっているスタンドアロンサーバ、またはSecure Storageが使用できないMeeting Server 2000で使用します。ソースリリースは3.11.x以降でも構いませんが、4.0にアップグレードする前にノードが3.13.x上にある必要があります。

1. 3.13.xにステップアップグレードします。サポートされているパスに従います（3.11.x → 3.12.x → 3.13.xなど）。 各ホップの後、「バックアップを作成する前にサーバの健全性を検証する」セクションで説明されているように、Web Adminでバージョンを確認し、障害状態がクリアであることを確認します。

2. セキュア・ストレージのステータスを確認します。secure_storageコマンドを実行して、Secure Storageが有効になっていないことを確認します。Meeting Server 2000ではコマンドをスキップします。

3.「セキュアなストレージが無効または使用できない場合にバックアップを作成する」セクションで説明されているように、3.13.xバックアップファイルを作成してエクスポートします。また、「アップグレード前要件」セクションの説明に従って、カスタムSFTPコンテンツとログバンドルをエクスポートします。

4. Cisco.comから4.0ソフトウェアイメージをダウンロードし、抽出して、SFTP経由でupgrade.imgをノードにコピーします。

5. 次のコマンドを使用して、アップグレードを開始します。

アップグレードアップグレード.img

6. 警告バナーを読みます。すべての前提条件が完了した後にのみ、Yを押します。6.アップグレード後、「初回ブートとネットワークの復元」セクションの説明に従ってノードを設定してから、「4.0アップグレード後にデータを復元」セクションを使用してバックアップを復元します。

シナリオ2：セキュアストレージが有効になっているシングルノード

この手順は、Secure Storageが有効になっているスタンドアロンVM、Meeting Server Small、またはMeeting Server Mediumに対して使用します。これはMeeting Server 2000には適用されません。

サーバからファイルを転送する前に、暗号化されていない秘密鍵と暗号化されていないバックアップファイルは転送できないことに注意してください。証明書ファイルはブロックされません。

1. サポートされているパスを使用して、リリースをスキップせずに3.13.xにアップグレードします。各ホップの後、バージョンを確認し、「バックアップを作成する前にサーバの健全性を検証する」セクションで障害状態がクリアされていることを確認します。

2.secure_storage を実行し、出力にEnabled: Trueと表示されることを確認します。

3. 「セキュアなストレージが有効な場合にバックアップを作成する」セクションを使用して、暗号化された3.13.xバックアップを作成してエクスポートします。パスフレーズをシークレットストアに保存します。また、カスタムSFTPコンテンツとログバンドルもエクスポートします（アップグレード前要件セクション）。

4. upgrade.imgをノードにコピーし、アップグレードを実行します。

アップグレードアップグレード.img

5. 警告バナーを読み、Yを押して、前提条件が完了した場合にのみ続行します。

6.コンソールからネットワークを回復し（「初回ブートとネットワークの復元」のセクション）、パスフレーズを使って暗号化されたバックアップを復元します（「4.0アップグレード後にデータを復元」のセクション）。6.MeetingAppsを使用している場合は、新しいMeetingAppsシークレットを適用します（復元後のMeetingAppsシークレットキー）。

Meeting Server 4.0では、Secure Storageはデフォルトで有効になっています。リストア後も、秘密鍵とバックアップファイルは暗号化されたデータとして処理します。

シナリオ3:Secure Storageが無効な状態のデータベースクラスタ

この手順は、Meeting Server 2000を含むクラスタを含む、Secure Storageが無効になっているデータベースクラスタに対して使用します。バージョン3.5以降では、ソフトウェアをアップグレードする前にデータベースクラスタを解体する必要があります。まず、すべてのノードを3.13.xにステップアップグレードします。

クラスタの詳細を記録し、すべてのノードをバックアップする

1. すべてのノードでsecure_storageを実行します。このコマンドは、Meeting Server 2000ノードでは使用できないものとして扱います。

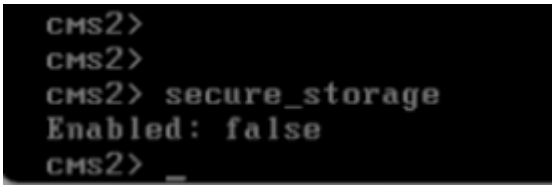


図22：暗号化されていないバックアップを使用する前に、すべてのクラスタノードでセキュアストレージが無効になっていることを確認します。使用できないMeeting Server 2000ノードのコマンドをスキップします。

2. 4.0へのアップグレード後に最初にリストアする必要があるため、現在のデータベースプライマリノードを記録します。レプリカがIn Syncであり、クラスタの状態が正常であることを確認します。

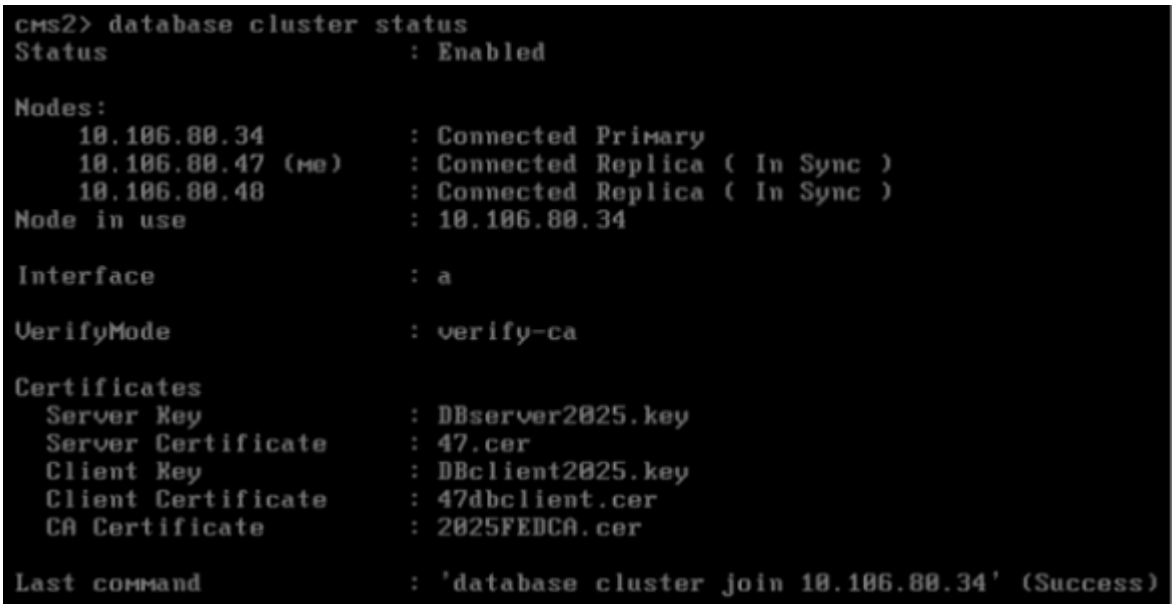


図23：現在のプライマリを記録し、レプリカがIn Syncであることを確認します。

3.すべてのノードで、使用中のすべてのコールタイプが動作していること、および障害状態がクリアであることを確認します（「バックアップを作成する前にサーバの健全性を検証する」セクション）。

4.「セキュアなストレージが無効または使用できない場合にバックアップを作成する」セクションを使用して、すべてのノードのバックアップを作成します。クラスタを解体する前に、各ファイルに名前を付けて、ノードに明確にマッピングし、すべてのバックアップを外部ストレージに転送します。

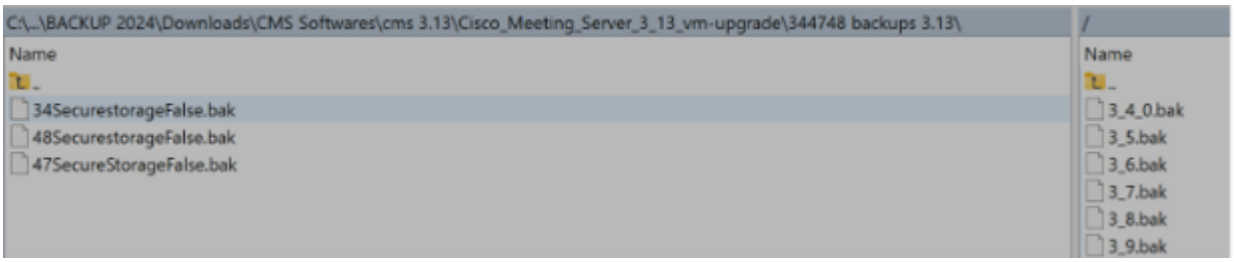


図24:3つのノードバックアップ例はすべて、外部ストレージに保存され、各ファイルがそのノードにマッピングされるように名前が付けられています。

クラスタの解体

この順序でノードを削除します。プライマリを最後まで保持：

- 接続された（コア以外の）Meeting Serverノード
- レプリカ・データベース・ノード
- プライマリデータベースノード

各ノードで、removalコマンドを実行して、Yを押します。すべてのノードがクラスタから離脱したことを報告するまで、4.0へのアップグレードを続行しないでください。クラスタメンバーシップを削除すると、そのノードのローカルデータベースは残ります。

データベースクラスタの削除

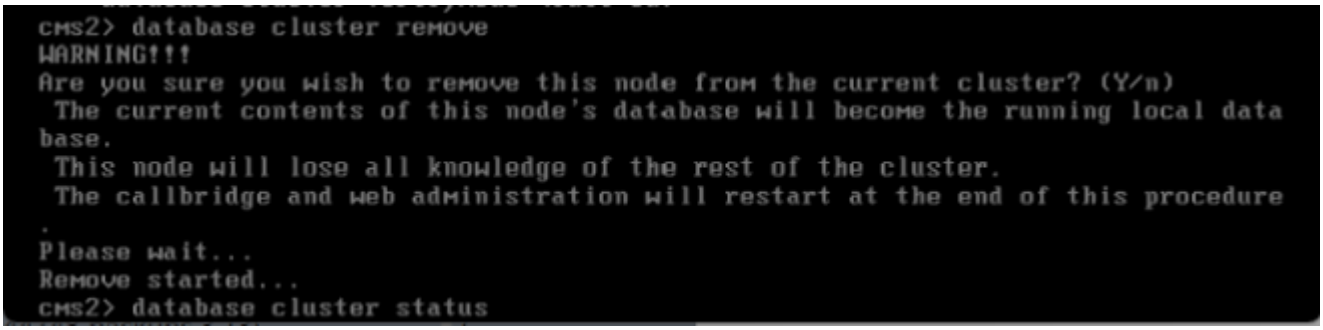


図25：レプリカで、クラスタメンバシップを削除するためにYを確認します。ノードのローカルデータベースは保持されます。

```
  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
```

図26：削除後、そのノードでクラスタステータスがDisabledで、Node in useがNoneになっていることを確認します。

```
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)
```

図27：レプリカを削除した後、元のプライマリがクラスタに残っている唯一のノードです。最後に削除します。

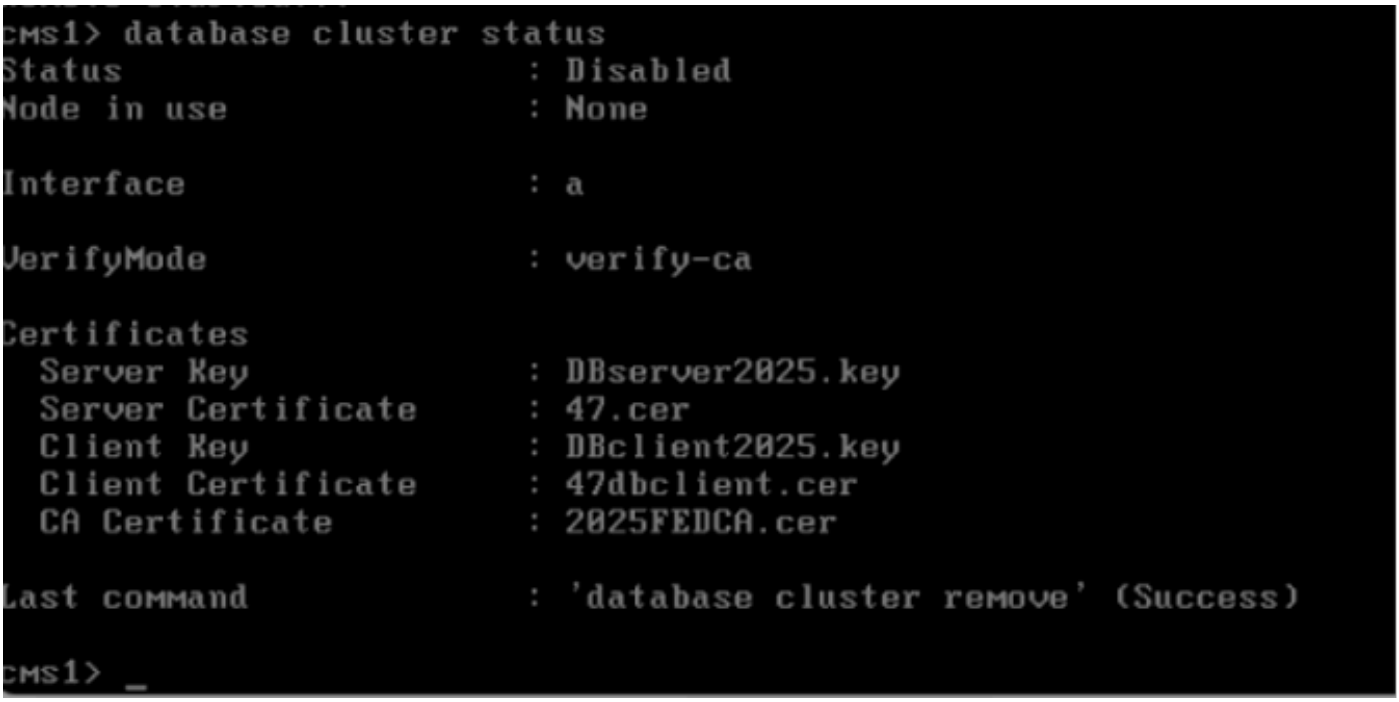


図28：以前のプライマリを削除した後、コマンドが成功を報告し、クラスタステータスが無効になっていることを確認します。

ノードのアップグレードと復元

1. いったん解体されたノードはスタンドアロンであり、並行してアップグレードできます。各ノードで、SFTP経由でupgrade.imgをコピーし、upgrade コマンドを実行します。

アップグレードアップグレード.img

2.コンソールから各ノードのネットワークアドレスを回復する（最初の起動とネットワークの復元セクション）。

3. 各ノード独自の3.13.xバックアップをそのノードにコピーして戻します。最初に元のプライマリをリストアし、次にレプリカ、続いて接続されたノードをリストアします。「4.0アップグレード後のデータの復元」セクションを使用してください。バックアップをリストアすると、データベース・クラスタのメンバーシップが再確立されます。

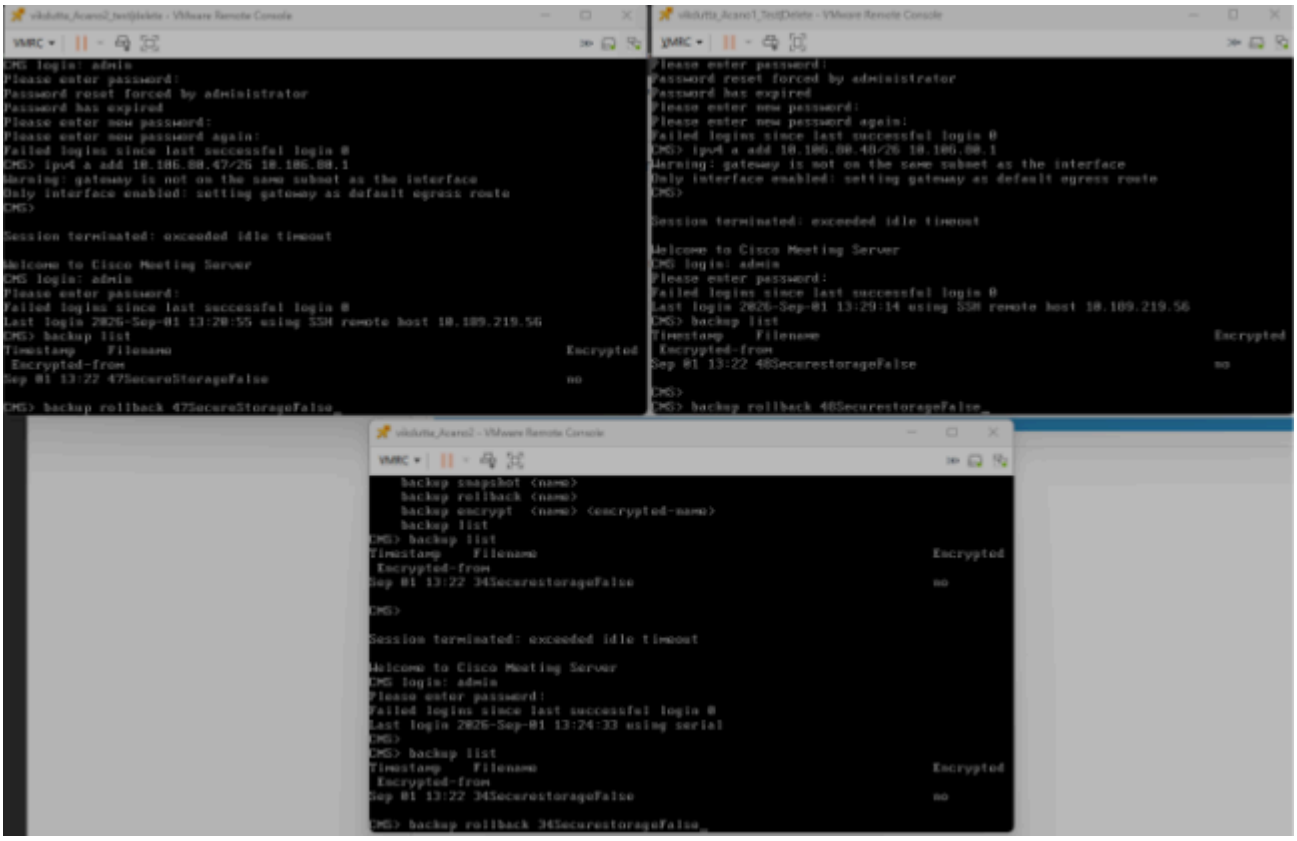


図29：各ノード独自のスナップショットの復元元のプライマリから開始し、レプリカをリストアします。ファイル名の例は、そのノードを示しています。

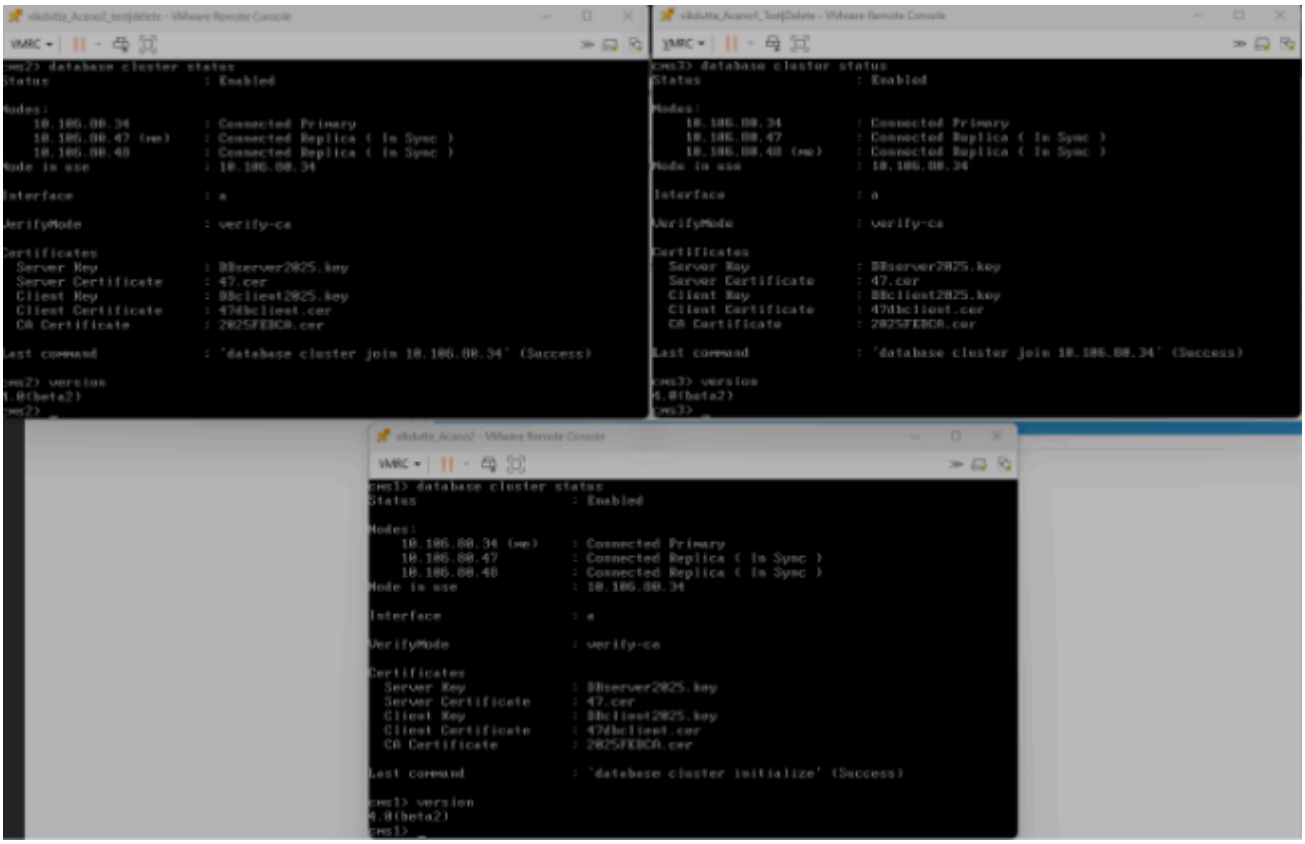


図30:Meeting Server 4.0での復元後、クラスタが有効であり、同じプライマリが表示され、レプリカが同期されていることを確認します。

注：この復元後にCall Bridgeクラスタ接続が確立されない場合は、以前のプライマリでのみ**database cluster upgrade_schema**を実行し、Call Bridgeのステータスを再確認してください。

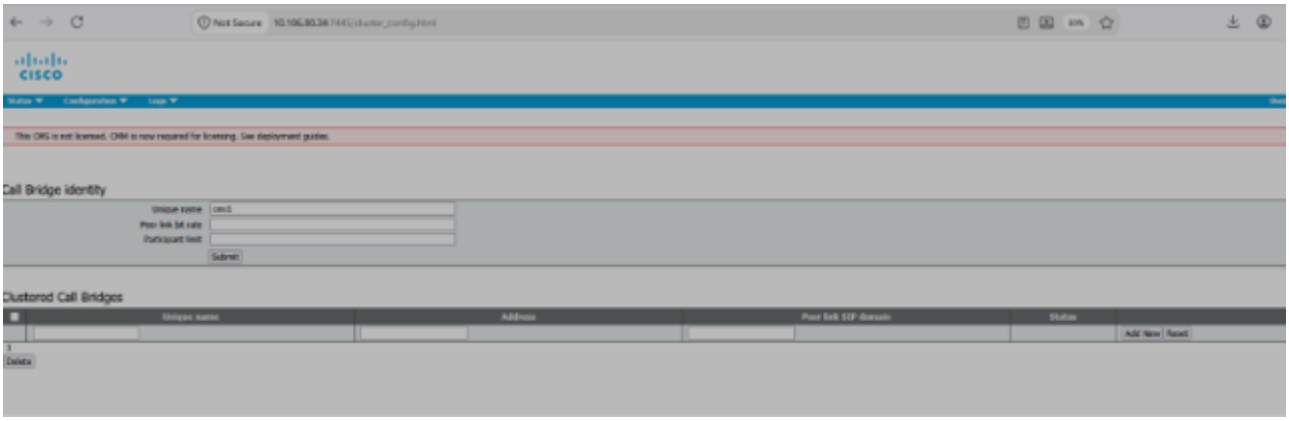


図31：スキーマのアップグレード前の例では、Clustered Call Bridgeが空の状態でデータベースクラスタが実行されています。

database cluster upgrade_schema

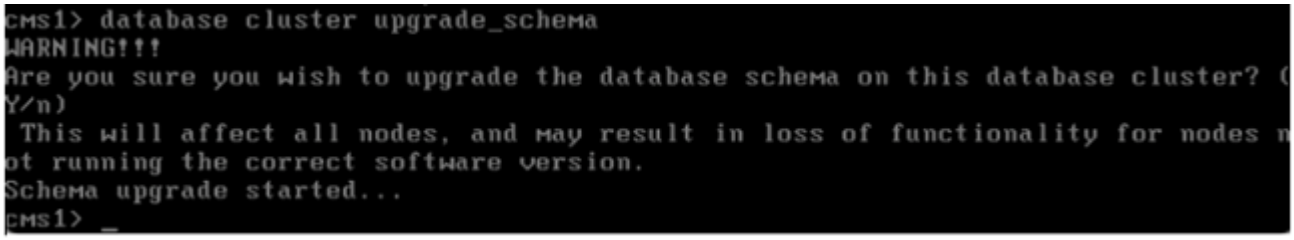


図32：以前のプライマリで、この分散クラスタのアップグレード後にCall Bridgeクラスタ接続が失敗した場合にのみYを確認します。

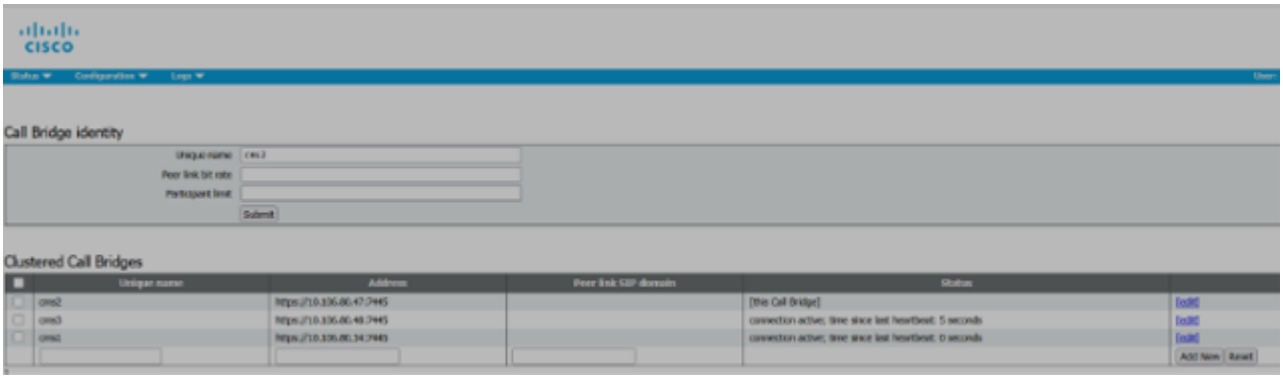


図33：スキーマのアップグレード後、各Call Bridgeピアにアクティブな接続が表示されていることを確認します。

4. すべてのWebブリッジで「復元後のMeetingApps秘密鍵」セクションのMeetingApps秘密鍵に関する手順を実行してから、「アップグレード後の検証」セクションを使用して導入を検証します。

シナリオ4：セキュアなストレージが有効になっているデータベースクラスタ

この手順は、ノードでセキュアなストレージが有効になっているVM、Meeting Server Small、またはMeeting Server Medium上のデータベースクラスタに使用します。これはMeeting Server 2000には適用されません。まず、すべてのノードを3.13.xにステップアップグレードします。

クラスタの詳細の記録と暗号化バックアップの作成

1. すべてのノードでsecure_storage を実行し、Enabled: Trueであることを確認します。

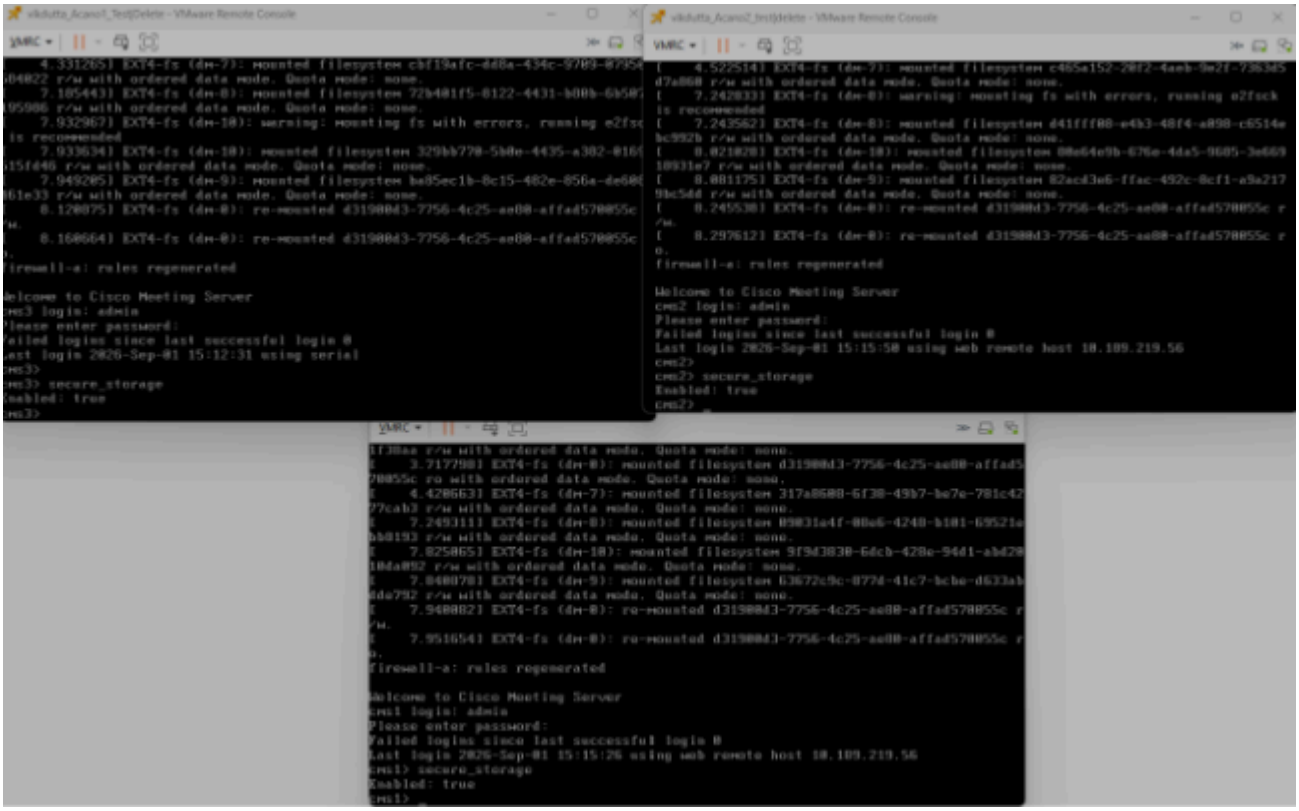


図34：図に示されている3ノードクラスタでは、アップグレードの前に、すべてのノードで「Secure Storage」が「Enabled: True」と表示されていることを確認します。

2. 現在のデータベース・プライマリを記録し、レプリカがIn Syncになっていることを確認します。

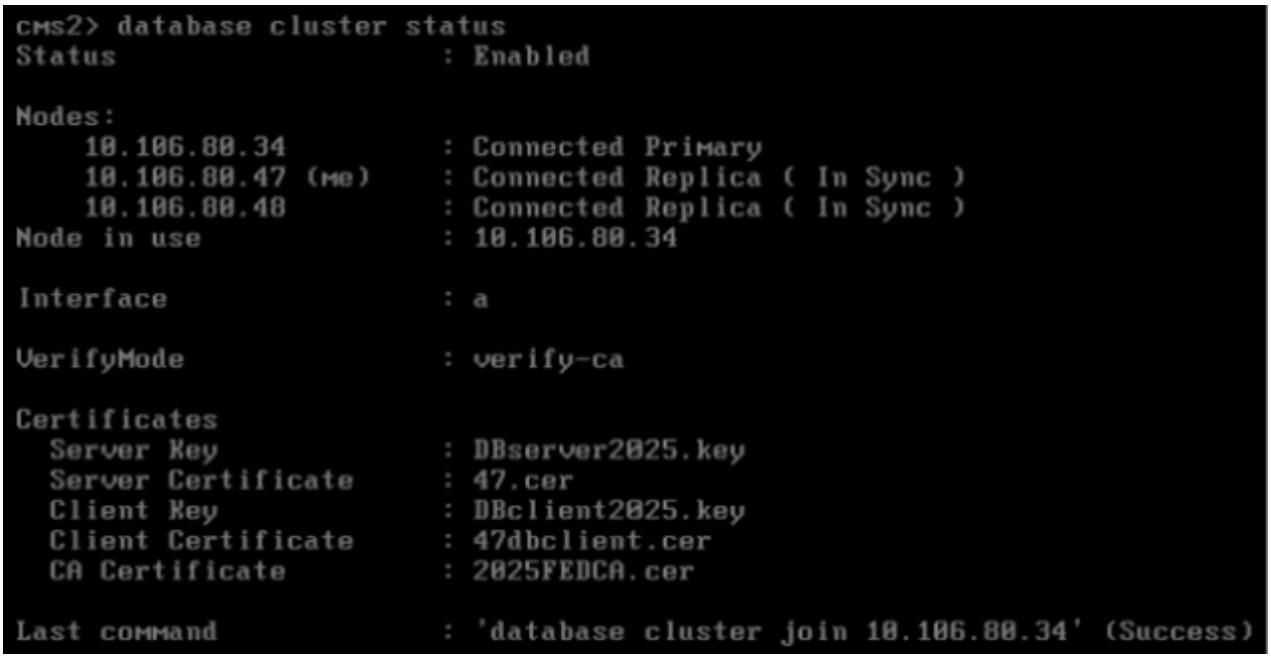


図35：アップグレード前のデータベースクラスタステータスプライマリを記録し、レプリカがIn Syncであることを確認します。

3.すべての使用されているコールタイプが動作していること、および障害状態が各ノードでクリアであることを確認します（「バックアップを作成する前にサーバの健全性を検証する」セクション）。

4.「セキュアなストレージが有効な場合にバックアップを作成する」セクションを使用して、すべてのノードの暗号化されたバックアップを作成します。各ファイルに固有のパスフレーズを割り当てて記録するか、文書化されたパスフレーズポリシーを使用します。クラスタを解体する前に、暗号化されたファイルだけをサーバから転送します。

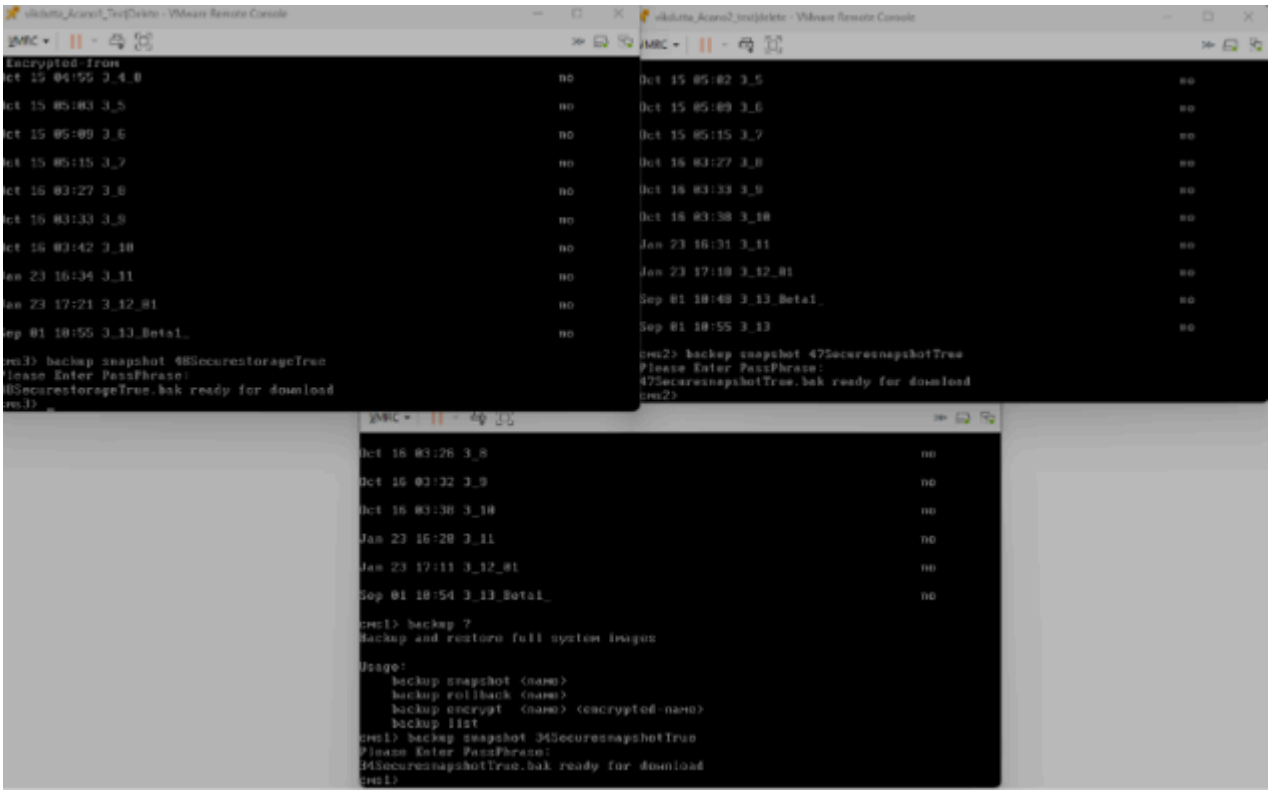


図36：各ノードの暗号化されたバックアップスナップショットこの例では、パスフレーズのプロンプトと、ダウンロード可能な各.bakファイルを示しています。

解体、アップグレード、復元

シナリオ3で説明されているように、接続されたノード、レプリカ、およびプライマリが最後に追加された順序でクラスタを解体します。database cluster remove を使用して、すべてのノードがクラスタから移動したことを確認します。

スタンドアロンノードを並行してアップグレードします。コンソールからネットワークアドレスを回復します（初回ブートおよびネットワーク復元セクション）。

各ノード独自の暗号化バックアップをアップロードします。ロールバックの前に、アップロードされたスナップショットがバックアップリストに「Encrypted: yes」と表示されていることを確認します。最初に元のプライマリをリストアし、次にレプリカと接続されたノードをリストアします。次のbackup rollbackコマンドを使用してYを確認し、プロンプトが表示されたらバックアップのパスフレーズを入力します。パスフレーズが受け入れられると、ノードが再起動します。各ノードに対して繰り返します。

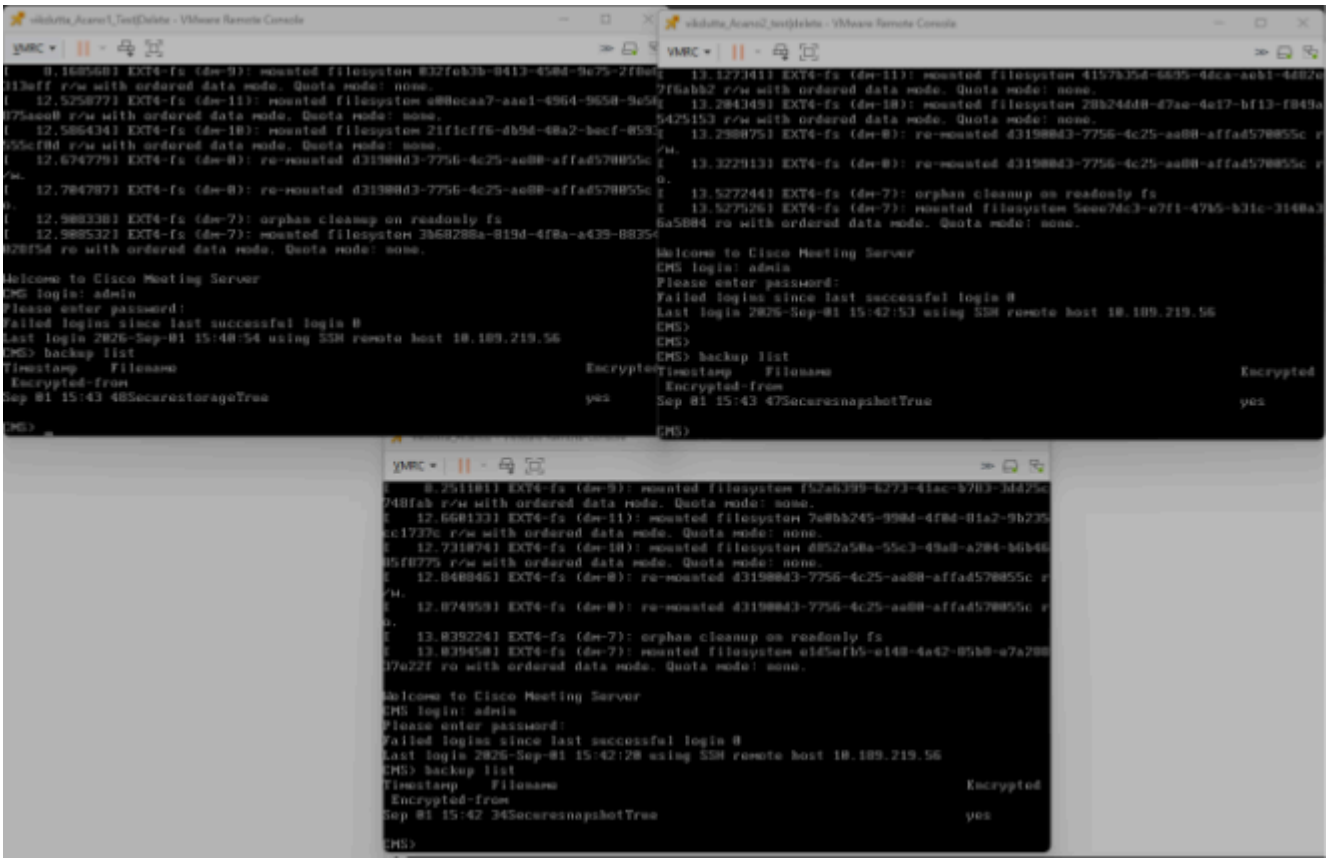


図37：最初の4.0ブート後、アップロードされたスナップショットがバックアップリストに「Encrypted: yes and be ready for rollback」と表示される必要があります。

backup rollback encrypted-filename（バックアップロールバック暗号化ファイル名）

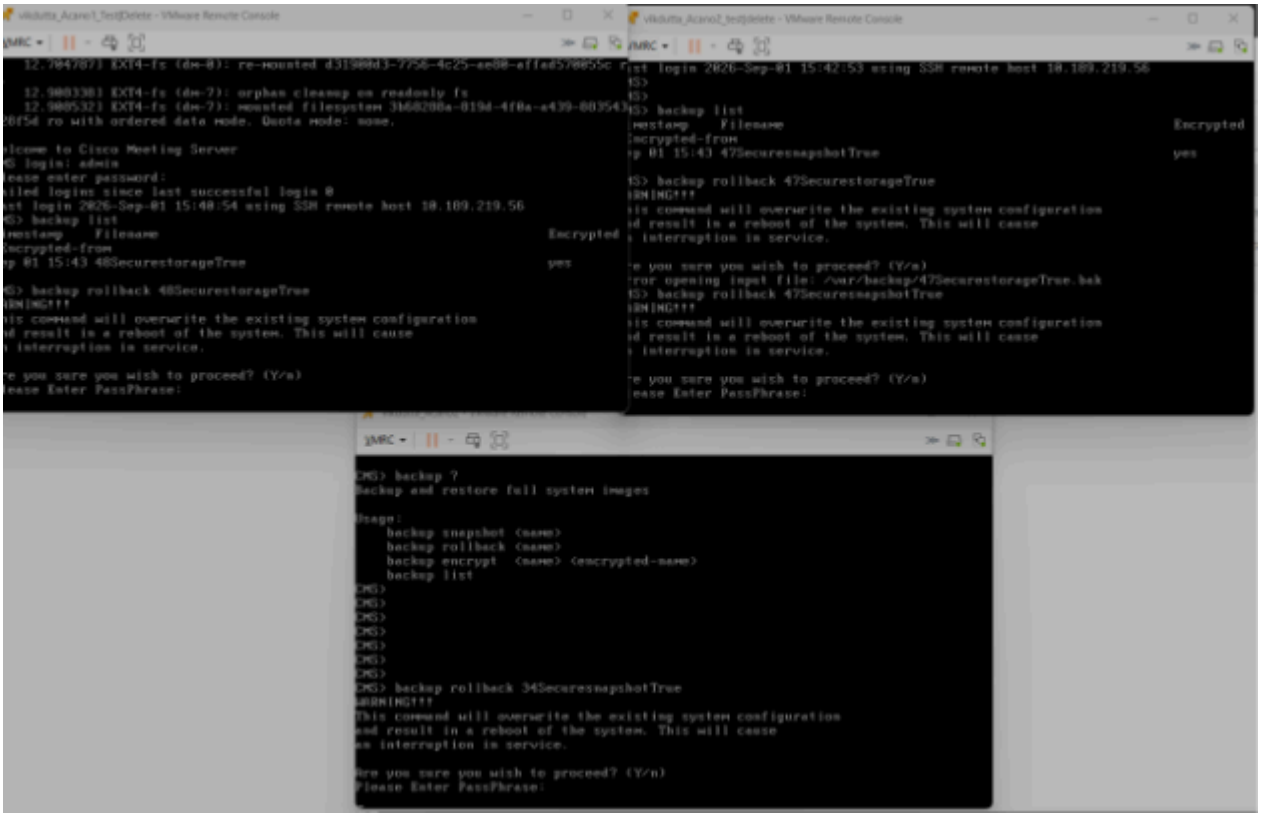


図38:Yを確認し、パスフレーズを入力して、最初に元のプライマリを復元します。

注：この復元後にCall Bridgeクラスタ接続が確立されない場合は、以前のプライマリでのみ**database cluster upgrade_schema**を実行し、Call Bridgeのステータスを再確認してください。

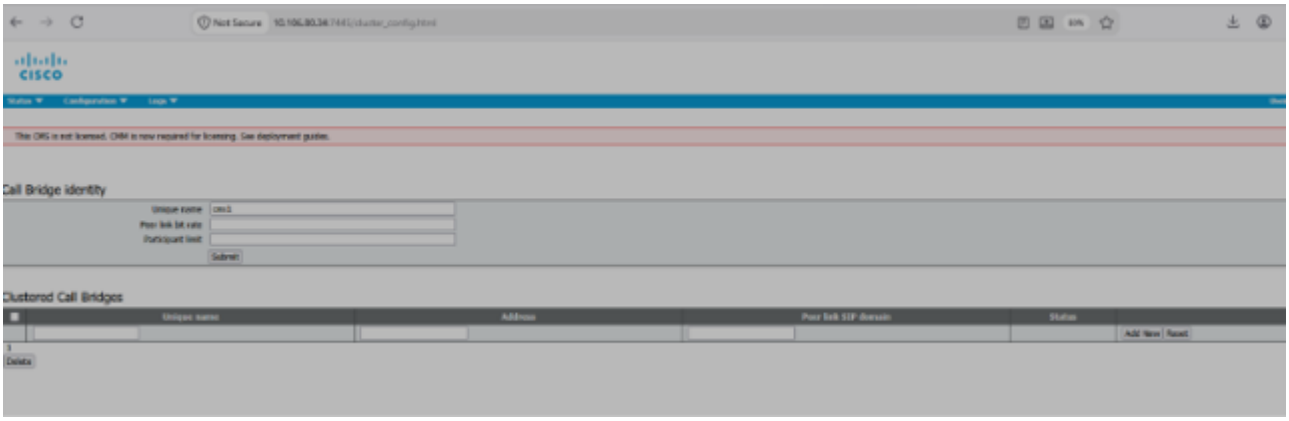


図39：スキーマのアップグレード前の例では、Clustered Call Bridgeが空の状態でデータベースクラスタが実行されています。

database cluster upgrade_schema

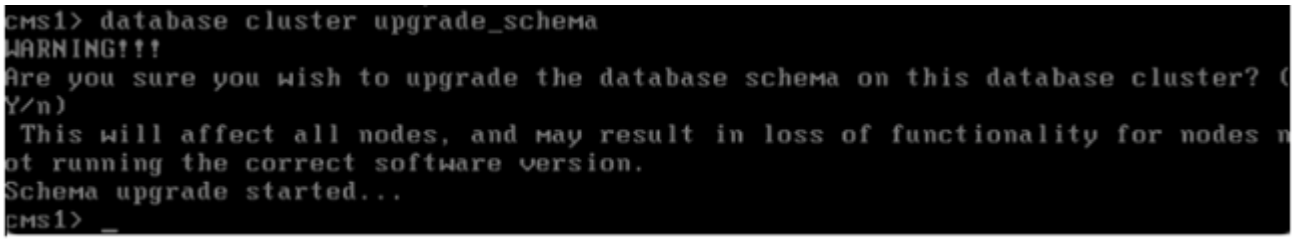


図40：以前のプライマリで、この分散クラスタのアップグレード後にCall Bridgeクラスタ接続が失敗した場合にのみYを確認します。

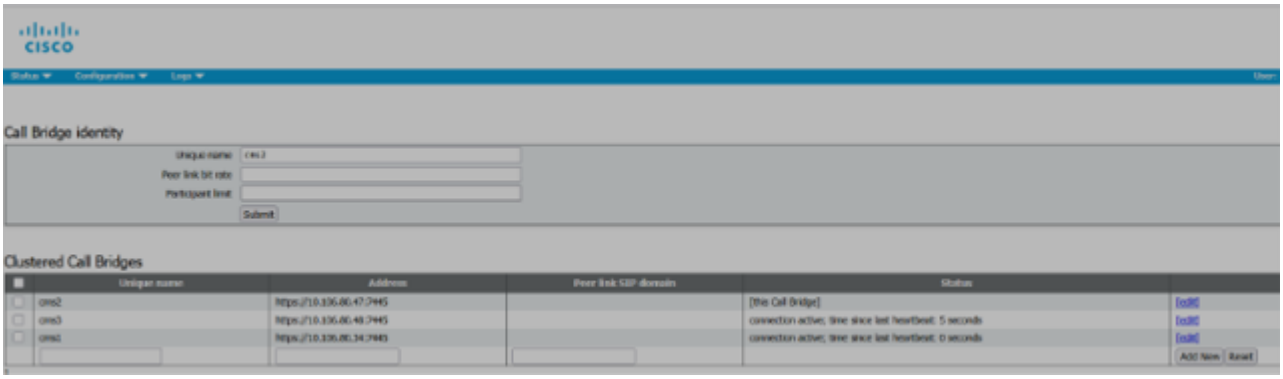


図41：スキーマのアップグレード後、各Call Bridgeピアにアクティブな接続が表示されていることを確認します。

すべてのWebブリッジで「復元後のMeetingApps秘密鍵」セクションのMeetingAppsシークレッ

ト手順を実行してから、「アップグレード後の検証」セクションを使用して導入を検証します。

アップグレード後の検証

復元後、システムを実稼働に戻す前に、次のチェックリストを完了してください。

- 各ノードのWeb AdminにCisco Meeting Server 4.0と表示されます。
- 必要なMMPサービスが有効で実行中です（アクティブ： True）。
- 障害状態はクリアです。対応する障害がない限り、最近のエラーと警告を情報として扱います。
- 該当する場合、データベースクラスタのステータスには、予想されるプライマリとレプリカが表示されます。
- Smart LicensingとCall Bridgeの接続が復元されます。
- この展開でサポートされるSIP呼び出しとWeb Appクライアント呼び出しは正常に完了します。
- 「アップグレード前要件」セクションのサーバからコピーされたブランディング、音声プロンプト、およびSSOファイルは、まだバックアップに含まれていなかった場合には復元されます。
- MeetingAppsが展開されている場合、Web Bridgeは新しいMeetingAppsの関係を表示し、ファイル共有が機能します。
- 展開が受け入れられた後にのみ、一時的なスナップショットを削除します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。