ترقية خادم الاجتماعات إلى الإصدار 4.0 - تقرير

المحتويات

المقدمة

معلومات أساسية

متطلبات التحقق من الصحة قبل الترقية

متطلبات النسخ الاحتياطي والاستعادة الشائعة

إجراءات النسخ الاحتياطي

إجراءات النسخ الاحتياطي عند تكوين التخزين الآمن

إجراءات النسخ الاحتياطي عند تكوين التخزين الآمن

ترقية الإصدار 4.0 باستخدام MeetingApps عبر سطر الأوامر

استعادة الشبكة والتهيئة الأولية

ترقية السيناريوهات

السيناريو 1 - ترقية عقدة واحدة بدون تكوين التخزين الآمن

السيناريو 2 - ترقية عقدة واحدة مع تكوين التخزين الآمن

السيناريو 3 - ترقية عقدة بتكوين التخزين الآمن

ترقية عقدة في مجموعة

ترقية العقدة الأولى في المجموعة

السيناريو 4 - ترقية عقدة في مجموعة مع تكوين التخزين الآمن

ترقية عقدة في مجموعة مع تكوين التخزين الآمن

استكشاف الأخطاء وإصلاحها

التحقق من صحة الترقية

المقدمة

يوضح هذه المستند كيفية ترقية خادم الاجتماعات من Cisco إلى الإصدار 4.0.

معلومات أساسية

يستخدم هذا المستند مع إصدار خادم الاجتماعات من Cisco والدليل المرجعي لمسؤول التخزين الآمن لفهم المتطلبات والمتطلبات MMP والدليل المرجعي للأوامر الأساسية.

قبل ترقية عملية نشر Cisco Meeting Server 4.0 عن الإصدارات السابقة، يجب الاحتفاظ بنسخة من جميع التكوينات السابقة، التي تتضمن إعدادات الشبكة وكلمات المرور، وإجراء نسخ احتياطي للبيانات المخزنة على موقع خارجي قبل بدء الترقية.

بالإضافة إلى ذلك، كانت ميزة التخزين الآمن إختيارية في إصدارات Cisco Meeting Server من 3.11 إلى 3.13، ولكنها ممكنة بشكل افتراضي في الإصدار 4.0. ونتيجة لذلك، يجب عليك اتباع إجراءات مختلفة للنسخ الاحتياطي والاستعادة إذا لم تكن قد أستخدمت وحدة التخزين الآمنة مطلقا أو إذا كنت قد قمت بتمكينها بالفعل على 3.11x أو 3.12x أو 3.13x.

تقوم ميزة Secure Storage بتشفير المفاتيح الخاصة وملفات النسخ الاحتياطي على الخادم وتتطلب تشفير هذه الملفات قبل التمكن من نقلها إلى وحدة التخزين الخارجية.

يقوم هذا المستند بدمج الإرشادات المطلوبة في مرجع واحد حتى يمكنك اتباع إجراء مشترك لجميع سيناريوهات الترقية دون الحاجة إلى تكرار الخطوات نفسها.

يغطي هذا المستند الموضوعات التالية:

- ما هي وحدات التخزين الآمنة وأين يتم تطبيقها وما ال تقوم به.
- مسار الترقية، الذي يتضمن متطلبات الوصول إلى 3.13.x قبل 4.0 وحقيقة عدم دعم 4.0.
- أسلوب شائع للنسخ الاحتياطي والاستعادة للعقد التي يتم فيها تمكين التخزين الآمن وللعقد التي يكون فيها معطل أو غير متوفر.
- تقوم عقدة نظام مجموعة قواعد البيانات بفصل التسلسل أثناء حل نظام مجموعة قواعد البيانات قبل الترقية.
- المفتاح السري MeetingApps، الذي ال يتم تخزينه في نسخة إحتياطية من Cisco Meeting Server ويجب إعادة إنشاؤه بعد الاستعادة.

ملاحظة: يستخدم هذا المستند لقطات شاشة معملية تم التقاطها أثناء إختبار إصدارات برنامج 4.0 بيتا. جميع أسماء المضيف وعناوين IP أو أسماء الملفات المعروضة توضيحية بشكل صارم ولا تعكس بيانات اعتماد الإنتاج الفعلية أو عبارات المرور الحساسة. للحفاظ على الوضوح ومنع التكرار، يتم عرض الخطوات المتكررة مرة واحدة فقط في قسم الإجراءات

.المشتركة ام لم يوفر عرض المجموعة السياق الضروري الإضافي

نظرة عامة على التخزين الآمن

يوفر "التخزين الآمن" أمان بيانات محسنا من خلال تشفير الملفات الحساسة الموجودة على خادم الاجتماعات" والتحكم في كيفية إلغاء تجميل هذه الملفات من خادم Call Bridge. تم إدخال هذه الإمكانية في Cisco Meeting Server 3.11 كخيار قابل للتكوين باستخدام الأمر MMP secure_storage enable (القائمة على الافتراضية) على عمليات نشر الأجهزة الوسيط" (على Meeting Server Small وأ الموصفات).

من الإصدار 4.0، يتم تمكين التخزين الآمن بشكل افتراضي. أصبح هذا الإعداد الآن دائما و secure_storage enable mmp. الأمر تمت إزالة وقد ،فيه رجعة

:باستخدام التخزين الآمن، يقوم خادم الاجتماعات بتنفيذ هذا السلوك

- لا يمكن تنزيل المفاتيح الخاصة عبر SFTP حتى يتم تشفيرها. قم بتشفير مفاتيح خاص باستخدام الأمر pki encrypt MMP متبوعا بعبارة مرور تتألف من 14 حرفا على الأقل. لا يؤدي هذا إلى تغيير المفاتيح المستخدمة حاليا من قبل خدمات Meeting Server.
- يتم تشفير ملفات النسخ الاحتياطي التي تم إنشاؤها باستخدام الأمر <name> backup encrypt <name> encrypted-name MMP، يطلب الأمر، الآمن التخزين ميزة تمكين عند .الخاص بالنسخ الاحتياطي للتشفير encrypted-name عبارة مرور تتكون من 14 حرفا على الأقل. عبارة المرور نفسها مطلوبة أثناء إستعادة النسخ الاحتياطي.
- إذا لم يتم تشفير، يجب أن يكون في نموذج مشفر. قبل تنزيل ملف نسخ إحتياطي، أستخدم تشفير النسخة الاحتياطية المدرجة للتصدير بعد، النسخة الاحتياطية غير مشفرة. يتم رفض محاولات تنزيل نسخة إحتياطية باسم مشفر <name>.
- عند تمكين FIPS. يجب إعادة إنشاء التخزين الآمن، يمكن تشغيل 3.12، من الإصدار أقصر مرور عبارة باستخدام 3.11 في تم إنشاؤها التي الخاصة المفاتيح ملفات .الأقل على حرفا 14 من مكونة مرور عبارة باستخدام

تلميح: تعمل ميزة "التخزين الآمن" على تقييد نقل المفاتيح الخاصة غير المشفرة وملفات النسخ الاحتياطي غير المشفرة من خادم الاجتماعات. لا يقيد نقل ملفات الشهادات. لا يزال يمكن نسخ الشهادات باستخدام SFTP؛ يتم حظر المفاتيح الخاصة غير المشفرة المقترنة فقط حتى يتم تشفيرها باستخدام تشفير PKI.

تحذير: بمجرد تمكينها، لا يمكن تعطيل التخزين الآمن باستخدام أي أمر MMP. ولا

يمكن التراجع عن هذه العملية. يؤدي FACTORY_RESET FULL إلى إعادة ضبط
"التخزين الآمن" إلى خطأ. تمتع بإجراء نسخ إحتياطي للتكوين باستخدام لقطة
للنسخ الاحتياطي وتخزينها على جهاز منفصل قبل تمكين ميزة التخزين الآمن.
بعد تمكين secure_storage لإعادة التمهيد على الفور. في حالة تخطي عملية إعادة
التشغيل، يمكن وضع علامة على وحدة التخزين الآمنة دون التهيئة الكاملة، ويمكن
أن تفشل هذه الأوامر factory_reset full . مسار الاسترداد في تلك الحالة هو الرجوع إلى
لقطة تم حفظها مسبقا (هذا صالح فقط ل 3.13.x). في Meeting Server 4.0، يتم
تمكين secure_storage بشكل افتراضي.

الأنظمة الأساسية المدعومة

- مدعوم: الجهاز الظاهري (المستند إلى المواصفات)
- مدعوم: خادم الاجتماعات صغير/1K
- مدعوم: وسط خادم الاجتماعات
- غير مدعوم: Meeting Server 2000. ميزة التخزين الآمن غير متوفرة. لا تستخدم أوامر التخزين الآمن على هذا النظام الأساسي.

يعمل Cisco Meeting Server 4.0 على تمكين التخزين الآمن بشكل افتراضي على جميع الأنظمة الأساسية المتوافقة. بعد الترقية، تتم حماية البيانات تلقائيا بواسطة "التخزين الآمن" حتى في حالة إجراء النسخ الاحتياطي ل 3.13.x أثناء تعطيل "التخزين الآمن".

ملاحظات التنفيذ

- لا تؤدي إعادة تسمية صورة الترقية إلى تغيير إعدادات التخزين الآمن.
- قم بتأكيد حالة التخزين الآمن على كل عقدة باستخدام الأمر secure_storage قبل إجراء عمليات النسخ الاحتياطي.
- يقوم الأمر بالإبلاغ عما إذا كان يتم تمكين التخزين الآمن (True) أم لا (False). في Meeting Server 2000، اتبع الخطوات المذكورة في شروط الترقية حيث تكون التخزين الآمن معطلا أو غير متوفر؛ أثناء ترقية Cisco Meeting Server 2000 إلى ينطبق الأمر.

```
cms-3120>
cms-3120>
cms-3120> secure_storage
Enabled: false
cms-3120>
```

إخراج MMP عند عدم تمكين التخزين الآمن (تمكين: خطأ).



شكل 2: إخراج MMP عند تمكين التخزين الآمن (تمكين: true) على Cisco Meeting Server 3.13.

يمكن العثور على تخذيرات صياغة أوامر مفصلة ومثال للاستخدام في الدليل المرجعي وأوامر MMP الذي تستخدمه السريع لمسؤول خادم الاجتماعات من Cisco للتخزين الآمن ومرجع حالي.

ترقية المباد ئ والقيود

مسار الترقية المطلوب

يجب أن تتبع ترقيات Cisco Meeting Server مسارا تسلسليا دون تخطي الإصدارات الرئيسية. على سبيل المثال، يجب أن تتقدم عقدة على 3.11.x عبر 3.12.x و 3.13.x قبل أن تصل إلى 4.0. الترقيات المباشرة من الإصدارات السابقة مثل 3.9.x إلى 3.13.x وأ 3.11.x إلى 4.0. بالنسبة لوسيط غير مدعوم وعادة ما تتسبب في أخطاء تكوين لا يمكن إستردادها. 4.0 → 3.13 → 3.11.5 وهو مسار الترقية، سيكون 3.13، وأ 3.11.5 مع الإصدارات Meeting Server.

تلميح: قبل بدء ترقية Cisco Meeting Server 4.0، يجب أن تقوم بتشغيل عقدة كل على حدة. هذا 3.13.x، مع نسخ إحتياطي للتكوين تم التحقق منه وتم تصديره من نظام 3.13.x، تفترض جميع إجراءات السيناريو الواردة في هذه الورقة أن الترقية التدريجية إلى 3.13.x قد اكتملت بالفعل.

خفض الدرجات

تلميح: الخفض من 4.0.x إلى 3.13.x غير مدعوم. في حالة فشل الترقية أو عدم عمل (أو قم بإعادة تكوين الجهاز) النظام كما هو متوقع، فقم بنشر وحدة 3.13.x OVA جديدة، واستعادة النسخة الاحتياطية 3.13.x. احتفظ بلقطات برنامج Hypervisor للأجهزة الافتراضية التي تعمل بمعيار 3.13.x طوال فترة سريان إطار الترقية كخيار إضافي للاسترداد. لا تحل لقطات الأجهزة الافتراضية محل النسخ الاحتياطية للتكوين المصدر.

متطلبات النسخ الاحتياطي الحيوية لعمليات الترقية 4.0

بعد تأكيد ترقية 4.0، تتم إعادة تمهيد العقدة في حالة التمهيد الأولى. لا تعتمد على النسخ الاحتياطي التلقائي الذي تم إنشاؤه أثناء عملية الترقية، نظرًا لأن فشل الترقية يمكن أن يؤدي إلى فقدان وصول SFTP ويجعل الملف غير قابل للوصول. يمكن استخدام عمليات النسخ الاحتياطي التي تم إنشاؤها باستخدام أمر النسخ الاحتياطي فقط للاسترداد الموثوق به على التخزين الخارجي بشكل منتظم ونسخها إلى نقطة.

تسجيل دخول وتكوين كلمة المرور الأول

عند التمهيد الأول من الإصدار 4.0، تتم إزالة كلمة مرور MMP الموجودة من قاعدة البيانات. قم بتسجيل الدخول باستخدام اسم المستخدم باستخدام كلمة مرور فارغة (بدون كلمة مرور). يتطلب النظام منك إدخال كلمة المرور الجديدة. يتطلب النظام منك إعداد كلمة مرور MMP جديدة. ظهرت ميزة استرداد كلمة المرور الخاصة بالاجتماعات، تأكد من التحقق والتأكيد. انظر لعدم وجود ميزة استرداد كلمة المرور الجديدة من تسجيل كلمة المرور.

ملاحظة: إذا قمت بضبط كلمة مرور MMP جديدة في التمهيد الأول، يقوم الأمر الاحتياطي الصادر على النسخ الاحتياطي التي تم تخزينها في النسخ الاحتياطي المستردة باستبدالها بكلمة المرور التي كانت نشطة عند إنشاء النسخة الاحتياطية. بعد استعادة النسخة الاحتياطية على الخادم، يجب تسجيل الدخول باستخدام كلمة المرور 3.13.x.

إعادة إنشاء اتصال الشبكة بعد الترقية

يتم فقد عناوين IPv4 و IPv6 والقنعة والعبارات مع باقي التكوين. يمكن فقد اتصال الشبكة الخاص بخادم الاجتماعات بعد الترقية إلى 4.0. يجب أن يكون لديك وحدة تحكم متاحة حتى يمكنك تعيين العنونة مرة أخرى من برنامج hypervisor أو CIMC أو الوصول التسلسلي حتى يمكنك تعيين MMP.

ملاحظة: عادة ما تحتفظ عمليات النشر التي تستخدم حجوزات DHCP بنفس عناوين IP بعد إعادة التشغيل. ومع ذلك، يجب أن يظل الوصول إلى وحدة التحكم متاحًا حتى يتم تأكيد عنوان IP. لا تفترض إستعادة اتصال SSH حتى يتم التحقق من العنوان IP.

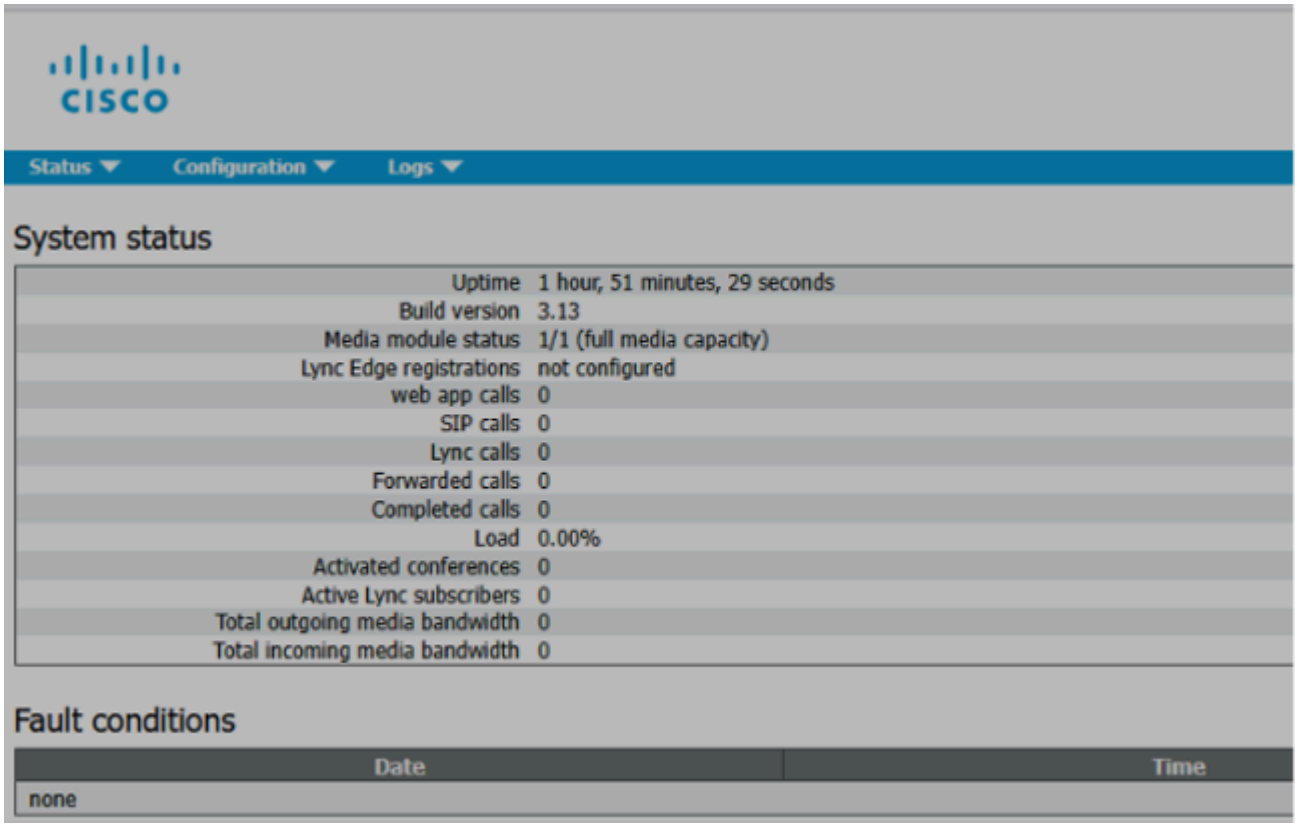
التحقق من صحة الخادم قبل إنشاء النسخ الاحتياطية

قبل الترقية إلى 3.13، تأكد من أن الخادم في حالة صحية وأن جميع الخدمات تعمل. بعد كل خطوة، قم بتسجيل الدخول إلى صفحة مسؤول الخادم. إذا واجهت أية أخطاء/أخطاء، فقم بتسجيل أي حالات خطأ أو تحذير على الخادم. يتضمن إستعادة النسخ الاحتياطي على 3.13. هذه الأخطاء قبل إنشاء نقطة للنسخ الاحتياطي على الخادم، مما يحافظ على سلامة النسخ الاحتياطية التي تمت ترقيتها، ولكن ليس عملية النشر.

على مسؤول الويب، افتح الحالة وأكد أن قسم شروط الخطأ واضح. تجاهل المدخلات التي تظهر فقط تحت الأخطاء والتحذيرات الأخيرة. بعد الترقية، من الشائع رؤية قواعد بيانات عابرة أو رسائل Web Bridge هناك؛ هذه ليست سببا لاستعادة النسخة الاحتياطية أو لتأخيرها.

إذا إستمرت حالة خطأ لأكثر من عشر دقائق تقريبا، فعليك حلها قبل أن تقوم بإجراء النسخ الاحتياطي. تعمل إستعادة النسخة الاحتياطية 3.13.x التي تحتوي بالفعل على أخطاء على الإصدار 4.0 على نقل هذه الأخطاء إلى الأمام.

بالنسبة للأنظمة المجمعة، تأكد من أن جميع أنواع الاستدعاءات المستخدمة تعمل (نقاط نهاية SIP وعملاء Web App) ومن عدم وجود شروط خطأ في أي عقدة.



شكل 3: صفحة حالة مسؤول الويب على 3.13.x مع حالات الخطأ فارغة. أستخدم طريقة العرض هذه قبل إجراء النسخ الاحتياطي الذي تمت استعادته على الإصدار 4.0.

متطلبات ما قبل الترقية

قبل بدء الترقية إلى الإصدار 4.0، أكمل هذه الإجراءات. تنطبق هذه المتطلبات على جميع السيناريوهات الأربعة التي يغطيها هذا المستند لاحقا.

- قم بالترقية إلى 3.13.x، ثم قم بتصدير نسخة إحتياطية من التكوين. تأكد من أن العقدة تقوم بتشغيل Cisco Meeting Server 3.13.x. قم بإنشاء نسخة إحتياطية منها ونقلها، بالإضافة إلى جميع بيانات SFTP المخصصة مثل الشعارات وملفات العلامات التجارية والمطالبات الصوتية وملفات SSO وأي بيانات مخصصة أخرى، إلى التخزين

الخارجي. أستخدم الإجراءات الموجودة في قسم إجراءات النسخ الاحتياطي والاستعادة
طقس ليس ،ةدقع لك نم يطايتحإ خسن ةيلمع عارجإب مق ،ةعومجم ةئيب يف .ةكرتشملا
.ةلصتملا ةمثاتملا ةخسنلا نم نكلو ةلصتملا ةيساسألا
- لإدخال إعادة تشغيل لإعدادات الشبكة. قم بتشغيل IPv4 a وتخزين المخرجات. يجب عليك
DHCP زجح مق مل 4.0 رادصلإا ليغشتل ةدحو مكحتلا دعب ةداعإ نم تامولعملا هذه
.IP نوانع ةداعتسا ىلع رداق
- وأ CIMC وأ Hypervisor جمانرب مكحت ةدحو رفوت .مكحتلا ةدحول لوصولا نم دكأت
ةعقدلا ميدهت ةداعإ دنع SSH لصتي نأ عقوتملا نم .ةدبلا لبق يلسلستلا لوصولا
.4.0 ىلإ
- ةلاحلا لجسلا تازجم نزختل .ةدقع لك نم logbundle.tar.gz ظفحا .ةفشرألل
.يطايتحإلا خسنلا تاطقل نع يدلا تسيل
- .upgrade رمألا ذيفنت دعب هضرع دنع 4.0 ةيقرتلا رخيذت عارش أقرا
- ةلاحإلا ىلإ n طغضا ،كلذ ىلع رداق تنأ تنك اذإ .يرسأ ريغ بلطتم يأ كانه سيل
.ةعباتملل ةدعتسم

ةعئاشلا ةداعتسالا و يطايتحالا خسنلا ءاجرإ

تستخدم سيناريوهات الترقية الأربعة التي تمت مناقشتها في هذا المستند نفس
نمط النسخ الاحتياطي والتصدير والتمهيد الأول والاستعادة. أستخدم هذه القسم كمصدر
واحد لهذه الخطوات، ثم اتبع التسلسل المحدد للسيناريو فقط (عقدة واحدة مقابل مجموعة،
وما إذا كان يتم تمكين التخزين الآمن بالفعل).

4.0 ةيقرتلا دعب رثأتملا تانايبلا

:ةيطايتحإ ةخسن ءاجرإ ةداعتسا ىتح 4.0 ةيقرت دعب تانايبلا هذه دقف متي

- ،تانايبلا ةدعاق ىوتحم ،نيمدختسملا ،تاسفاملا ىلع يوتحي يذلا ،تانايبلا ةدعاق
.تاملكملا
- .حيتافملاو تاداهشلا
- .ةصاخلا حيتافملا و SSO تافلمو ،يلحملا صيخصتلا
- ةيتوصلا ةبلاطملا تافلمو ،(ةباوبلاو ،عانقلاو ،IP نوانعو) ةكبشلا نيوكت
.نوانعلا DHCP زجح
- ةيطايتحإلا ةخسنلا ىلإ ةعوجرلا ىلع رداق ،ةيطايتحإ ةخسن ىلإ ةداعإ طبيق
.ةيطايتحإلا ةخسنلا نم رورملا ةملك
- ةعجارم متي .طقف ةداعتسالا دعب Call Bridge و Web Admin و Web Bridge تاقيبطتلا
.ةداعتسالا

ةظحالم: ال يتضمن النسخ الاحتياطي لـ Cisco Meeting Server المفاتيح السرية
المستخدمة بواسطة MeetingApps. بعد الاستعادة، يجب إعادة إنشاء هذه المفاتيح وتطبيقها على كل عقدة
Web Bridge. راجع المفاتيح السرية MeetingApps بعد قسم الاستعادة.

إجراء عملية نسخ إحتياطي عندما تكون وحدة التخزين الآمنة معطلة أو غير متوفرة

اتبع هذا الإجراء على الأجهزة الافتراضية وخادم الاجتماعات صغير الحجم وخادم الاجتماعات في Meeting Server 2000 حيث، وعلى secure_storage: خطأ تقارير تمكين فيها تم التي الوسائط ال توفر التخزين الآمن.

1. في كل عقدة، قم بإنشاء ملف باستخدام أمر لقطة النسخ الاحتياطي. ال تقم بإعادة إستخدام اسم الملف السابق.

2. انسخ ملف النسخ الاحتياطي إلى التخزين الخارجي باستخدام SFTP على الفور. ال تحتفظ بالنسخة الوحيدة على خادم الاجتماعات.

3. قم بتخزين الملف في موقع ال يزال يمكن الوصول إليه إذا تم إعادة بناء العقدة.

مثال:

backup snapshot cms313SecurestorageFalse backup list

4. تأكد من ظهور الملف في أمر قائمة النسخ الاحتياطي، ثم قم بنقله إلى قرص خارجي باستخدام عميل SFTP.

5. كرر هذه العملية على كل عقدة في نظام المجموعة. يمكن أن تحتوي أسماء النسخ الاحتياطي على أحرف وأرقام وعلامات سفلية وواصلة فقط. ال تقم بتضمين امتداد ملف مثل bak. عند إنشاء ملف نسخ إحتياطي. على سبيل المثال، يتم رفض اسم ملف 3.13SecureStorageFalse بسبب الفترة.

```
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>
```

الشكل 4: ترفض اللقطة الاحتياطية الاسم الذي يحتوي على نقطة، ثم تنجح مع اسم أبجدي رقمي. ويصبح ملف .bak جاهزا للتنزيل.

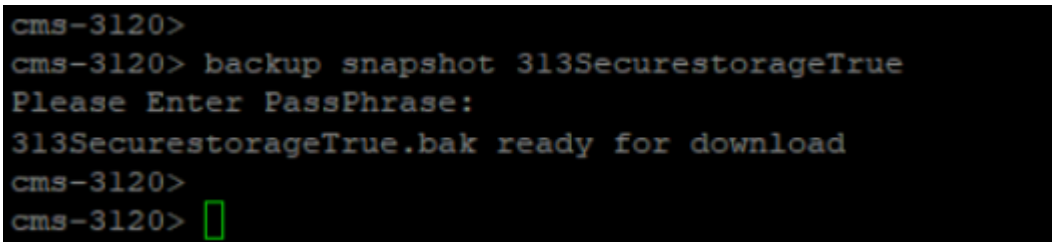


الشكل 5: انسخ ملف .bak من جذر SFTP لخادم الاجتماعات إلى التخزين الخارجي. لا تترك النسخة الوحيدة على الخادم.

إجراء عملية نسخ إحتياطي عند تمكين التخزين الآمن

أستخدم هذه الإجراء عند تمكين تقارير secure_storage: صحيح. يتعذر تنزيل ملفات النسخ الاحتياطي غير المشفرة.

1. إنشاء لقطة إحتياطية على كل عقدة. عند تمكين ميزة التخزين الآمن، يطلب الخادم عبارة مرور تتكون من 14 حرفا على الأقل. يمكن أن تحتوي عبارة المرور على أحرف وأرقام وأحرف خاصة ورموز ومسافات.



شكل 6: لقطة للنسخ الاحتياطي مع مطالبات تمكين التخزين الآمن مرة واحدة لعبارة مرور تتكون من 14 حرفا على الأقل. MMP تأكيدها.

2. الطلب من MMP إعادة إدخال عبارة المرور للتأكيد. قم بتأمين عبارة المرور الخاصة بك وأعد نظرا لأنك تحتاج إلى عبارة المرور نفسها لاستعادة الملف. لا تختار عبارة مرور تافهة مثال.

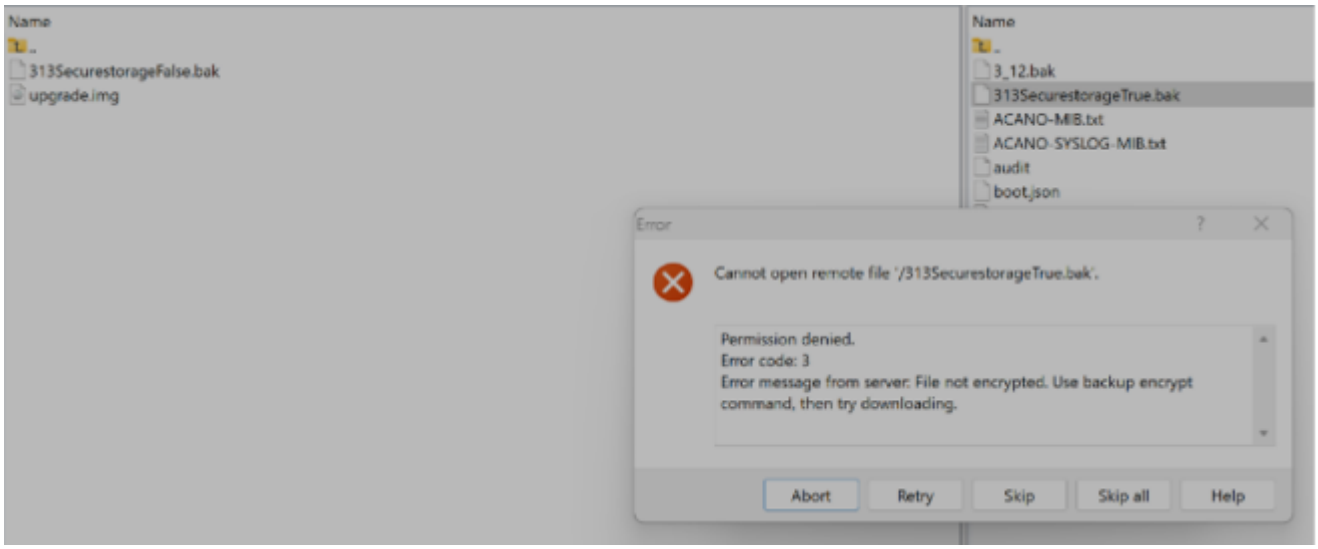
3. إذا كان الأمر backup list يظهر لقطة لم يتم تشفيرها للتصدير، فقم بتشفيرها قبل تنزيلها:



شكل 7: قائمة النسخ الاحتياطي قبل التشفير. لا يعد العمود المشفر، لذلك لا يمكن تنزيل الملف.

4. إذا حاولت تنزيل نسخة إحتياطية غير مشفرة، فإن SFTP يرجع خطأ رفض الإذن ويرشدك

بتشغيل الأمر backup encrypt أولا.



شكل 8: يرفض SFTP تنزيل نسخة إحتياطية غير مشفرة عند تمكين التخزين الآمن. ترشدك رسالة الخادم لتشغيل تشفير النسخ الاحتياطي.

5. قم بتشغيل الأمر backup encrypt لتشفير ملف النسخ الاحتياطي.



شكل 9: قائمة النسخ الاحتياطي بعد تشفير اللقطة. المشفر هو نعم ويمكن نقل الملف باستخدام SFTP.

تعرض قائمة النسخ الاحتياطي حالة التشفير واسم الملف الأصلي. تأكد من نقل الملف المشفر فقط من كل عقدة في نظام المجموعة. الاحتفاظ بسجل منظم لكل عقدة واسم الملف المطابق لها وعبارة المرور المقترنة.

إذا كنت بحاجة أيضا إلى تصدير مفاتيح خاصة، قم بتشفير كل مفتاح أولا. لا يتم حظر ملفات الشهادات بواسطة التخزين الآمن ويمكن نسخها دون هذه الخطوة الإضافية:

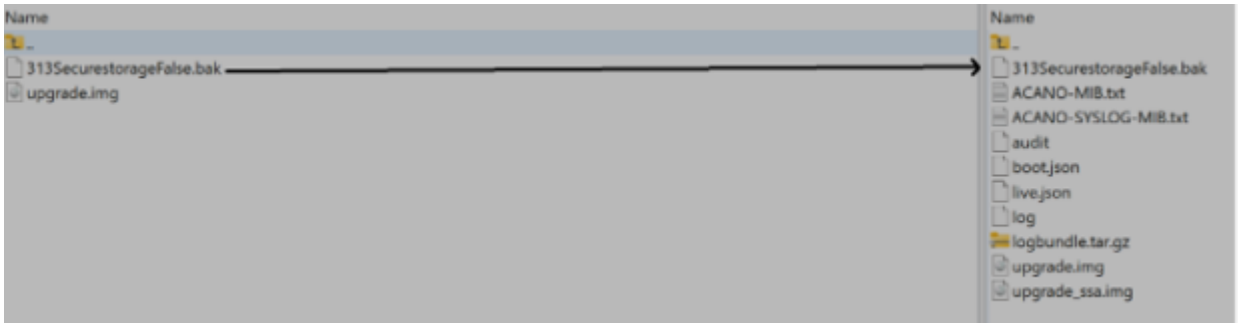
```
pki encrypt private.key encrypted_private.key
```

أستخدم اسم ملف فريد بدلا من إستبدال المفتاح المستخدم حاليا بواسطة الخدمات. الحد الأدنى لمتطلبات عبارة المرور ذات 14 حرفا ينطبق هنا أيضا.

إستعادة البيانات بعد ترقية 4.0

1. بعد تسجيل الدخول من التمهيد الأول واستعادة الشبكة في قسم التمهيد الأول

واستعادة الشبكة ، انسخ النسخ الاحتياطي 3.13.x المتوافق على العقدة باستخدام SFTP واستعادته.



شكل 10: بعد إستردار شبكة التمهيد الأول، انسخ ملف 3.13.x .bak مرة أخرى إلى العقدة 4.0 باستخدام SFTP.

2. تأكد من وجود الملف:

قائمة النسخ الاحتياطي

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

cms-3120>
```

شكل 11: قائمة النسخ الاحتياطي على 4.0 لتأكيد اللقطة التي تم تحميلها موجودة قبل التراجع.

3. قم باستعادة اللقطة. في نشر نظام المجموعة، قم باستعادة قاعدة البيانات الأساسية السابقة أولا، وتليها النسخ المتماثلة ثم العقد المتصلة.

backup rollback name-of-the-backup-file

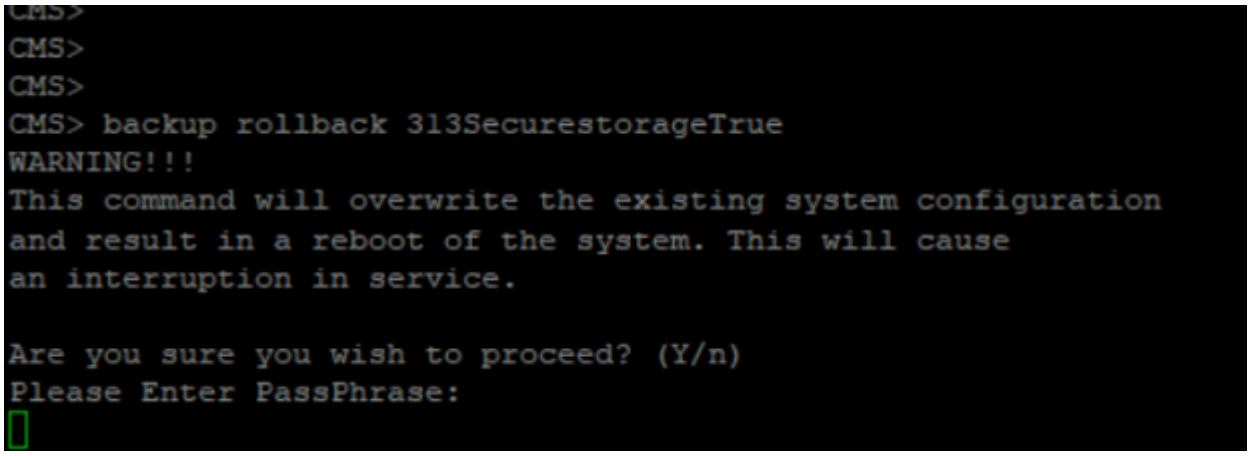
```
cms-3120> backup rollback 313SecurestorageFalse
WARNING!!!
This command will overwrite the existing system configuration
and result in a reboot of the system. This will cause
an interruption in service.

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

شكل 12: النسخ الاحتياطي للقطة غير المشفرة. تأكيد مع Y؛ تستخرج العقدة النسخة الاحتياطية وتعيد التمهيد.

4. اضغط على Y للمتابعة. تتم إعادة تمهيد العقدة أثناء إستخراج النسخة الاحتياطية. إذا تم إجراء النسخ الاحتياطي مع تمكين "التخزين الآمن"، تطالبك MMP بعبارة المرور. يتم

تنفيذ إعادة التشغيل فقط بعد قبول عبارة المرور الصحيحة.



شكل 13: النسخ الاحتياطي للقطة المشفرة. بعد Y، يطلب MMP عبارة المرور المستخدمة عند إنشاء النسخ الاحتياطي.

⚠ تحذير: يؤدي **backup rollback** هذا الخيار إلى إستبدال التكوين الحالي والشهادات والمفاتيح الخاصة وملف الترخيص ثم إعادة تمهيد الخادم. استخدمه فقط مع النسخة الاحتياطية 3.13.x التي قمت بتصديرها لهذه الترقية.

---

5. عندما تكون العقدة متصلة مرة أخرى، قم بتسجيل الدخول باستخدام بيانات اعتماد MMP (يظهر مشغلة ومكنة) وتأكد من أن كل تقارير الخدمة المطلوبة من النسخة الاحتياطية صحيح: هذا MMP).

التحققات النموذجية:

callbridge webbridge3 webadmin scheduler recorder streamer uploader meetingapps

6. قم بتشغيل الأوامر فقط للخدمات التي يفترض أن تستضيفها هذه العقدة.

المفتاح السري لـ MeetingApps بعد الاستعادة

يقوم النسخ الاحتياطي لـ Cisco Meeting Server بتخزين المفتاح السري لـ MeetingApps. بعد اكتمال عملية النسخ الاحتياطي الاحتياطية، قم بإعادة إنشاء المفتاح السري وتطبيقه على كل عقدة في Web Bridge. يؤدي تخطي هذه الخطوة إلى عدم توفر مشاركة الملفات حتى على الرغم من أن الخدمات الأخرى تبدو سليمة.

1. في عقدة MeetingApps، قم بتنفيذ الأمر meetingApps genSecret.

2. انسخ السر الذي تم إنشاؤه إلى المخزن السري. يؤدي كل تنفيذ لـ MeetingApps

GenSecret إلى إبطال المفاتيح السابق، ذا قم بإنشاء المفاتيح مرة واحدة وإعادة إستخدام القيمة نفسها عبر جميع جسور الويب.

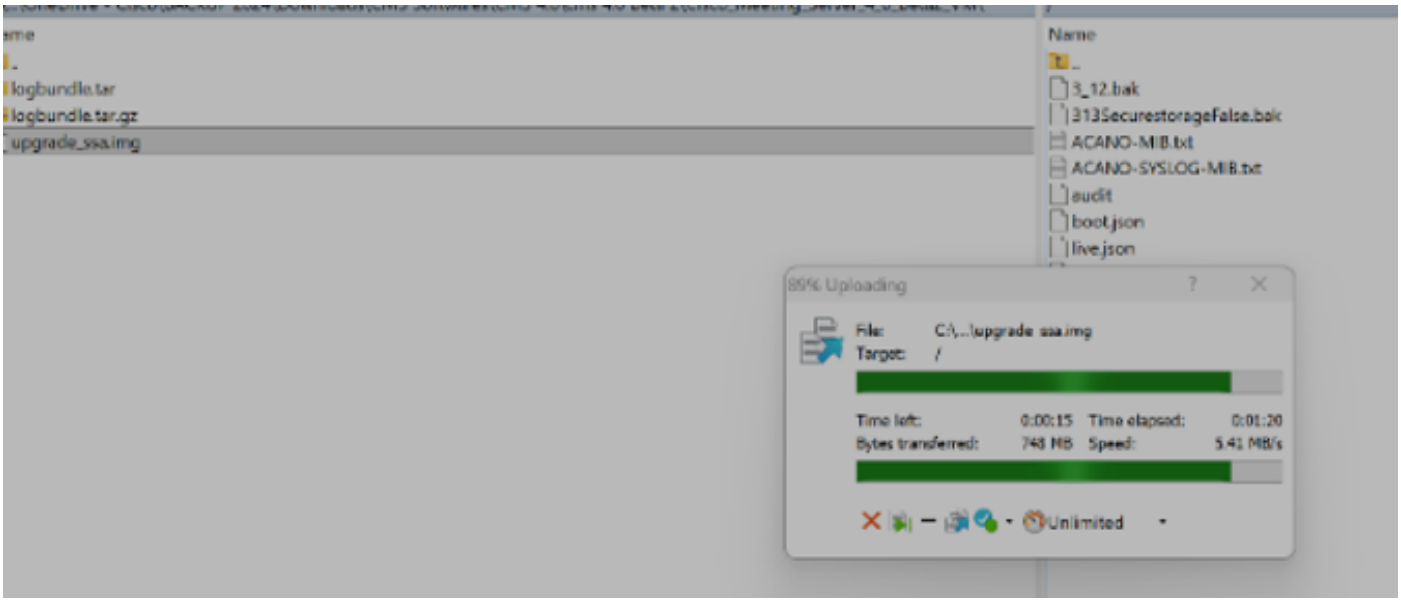
3. قم بتنفيذ هذه الأوامر على كل عقدة في Web Bridge:

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

يؤكد الأمر الأخير أن خدمة Web Bridge قيد التشغيل وأن MeetingApps تم تكوينها بشكل صحيح. MeetingApps غير معتمدة على Meeting Server 2000، ومشاركة الملفات غير متوفرة في مجموعات تتضمن Meeting Server 2000. في عمليات النشر هذه، ال تنطبق هذه الخطوة.

إستعادة الشبكة والتمهيد الأول

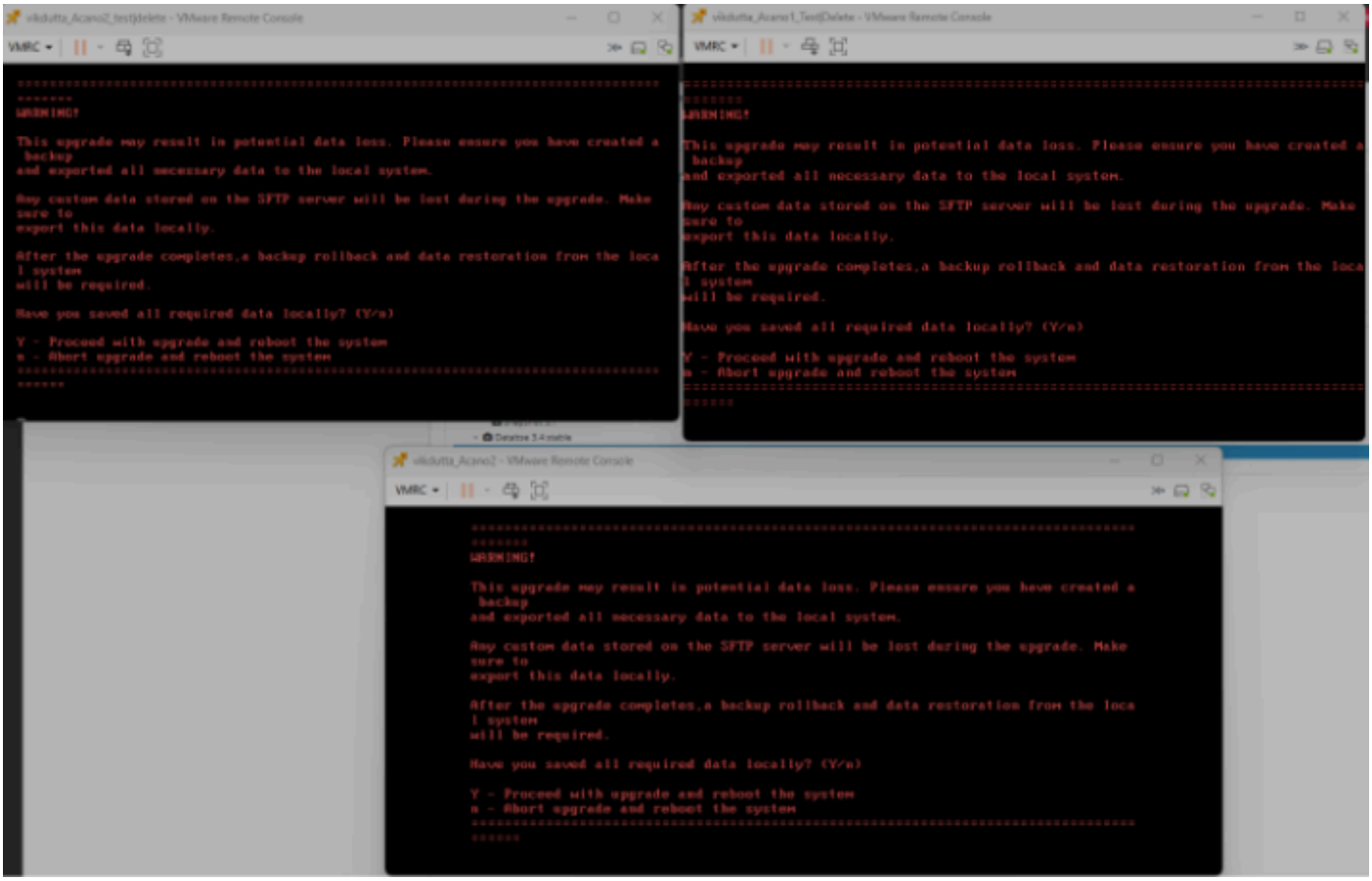
يعرض الأمر 4.0 upgrade شعار تحذير قبل المتابعة. راجع الرسالة بعناية وأجهض باستخدام n إذا لم تكن أي متطلبات أساسية كاملة. إذا قمت بالمتابعة مع Y، تتم إعادة تمهيد العقدة، وينقطع جلسة SSH، ويجب إكمال الخطوات المتبقية من وحدة التحكم.



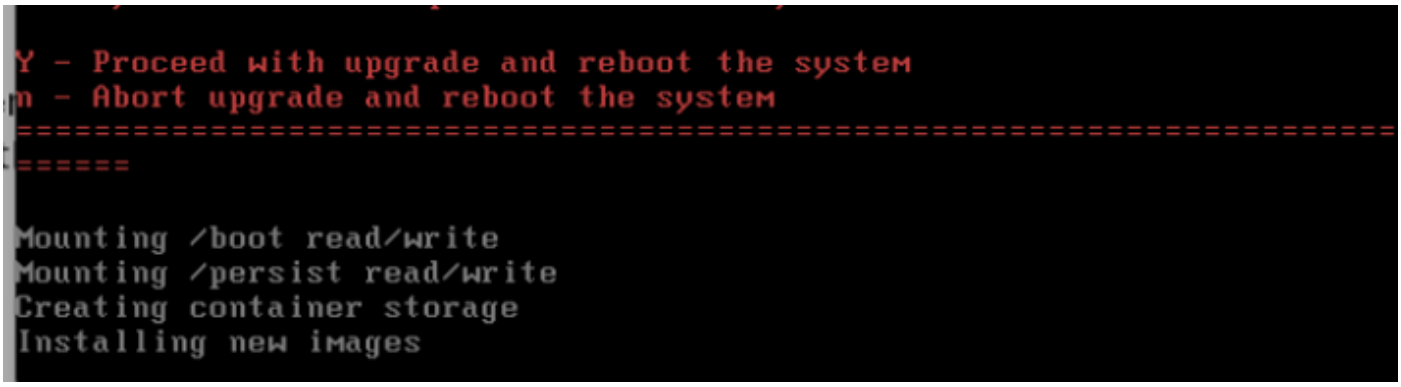
شكل 14: قم بتحميل صورة الترقية 4.0 إلى الدليل الجذر لـ SFTP الخاص بخادم الاجتماعات. يمكن أن يختلف اسم ملف صورة الترقية بناء على الحزمة التي تم تنزيلها من cisco.com.

```
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...
```

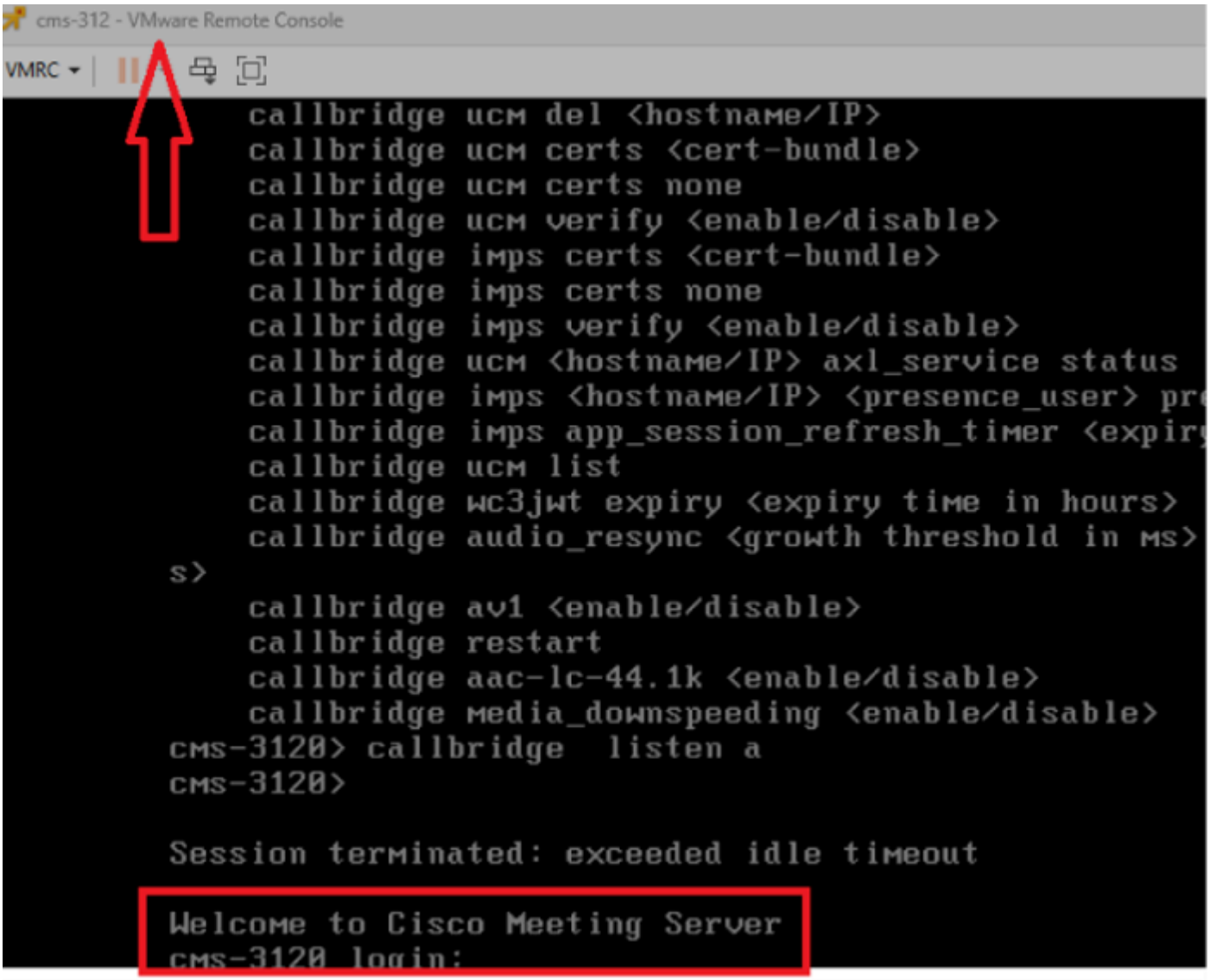
شكل 15: يتحقق أمر الترقية من توقيع الصورة وتبدأ العملية. لا تعتمد على النسخ الاحتياطي التلقائي الذي تم إنشاؤه في هذه المرحلة.



شكل 16: تجذير MMP الأحمر على نظام مجموعة مكون من ثلاث قواطع. يظهر نفس الشعار على عقدة واحدة. اضغط على N للإجهاض إذا لم تكن عمليات النسخ الاحتياطي والبيانات المخصصة خارج الخادم. اضغط على Y فقط للمتابعة وإعادة التشغيل.



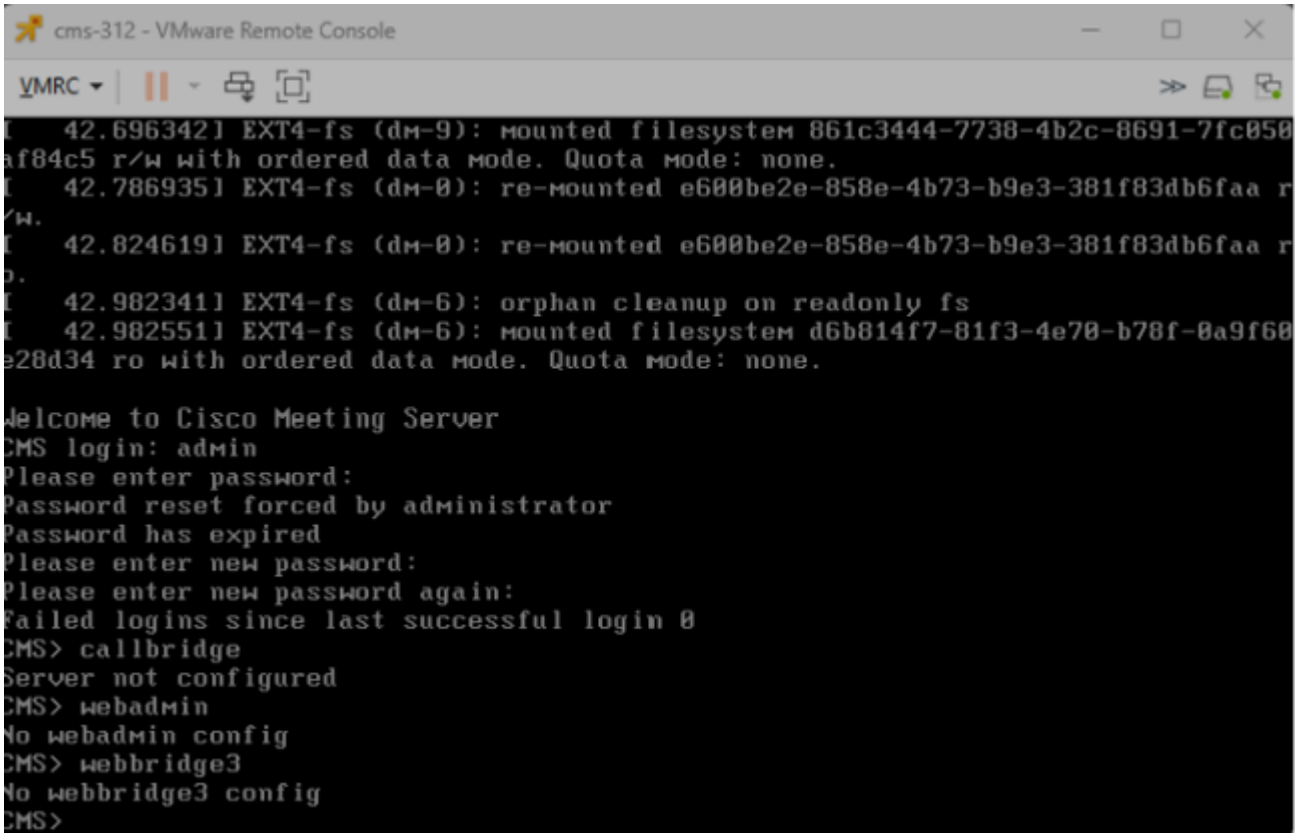
شكل 17: بعد Y، تقوم العقدة بتركيب وحدة التخزين وتثبيت صورة 4.0. انتهت مهلة جلسة SSH؛ المتابعة من وحدة تحكم برنامج مراقبة الأجهزة الافتراضية.



شكل 18: أستخدم وحدة التحكم في الذاكرة الافتراضية (VM) أو وحدة التحكم في إدارة الهيكل الأساسية (CIMC) بعد عمليات إسقاط SSH. تظهر نافذة مطالبة تسجيل الدخول للتمهيد الأول عندما تكون صورة 4.0 جاهزة.

1. سجل الدخول باستخدام حساب MMP للتمهيد الأول (اسم المستخدم admin وبدون كلمة مرور) ثم قم بتعيين كلمة مرور MMP جديدة عند طلبها. لاحظ أن النسخ الاحتياطي يستبدل كلمة المرور هذه بكلمة المرور المخزنة في النسخة الاحتياطية.

2. إعادة تطبيق تكوين الشبكة من الملاحظات التي قمت بتسجيلها في قسم متطلبات ما قبل الترقية:



شكل 19: تسجيل دخول MMP الأولي.

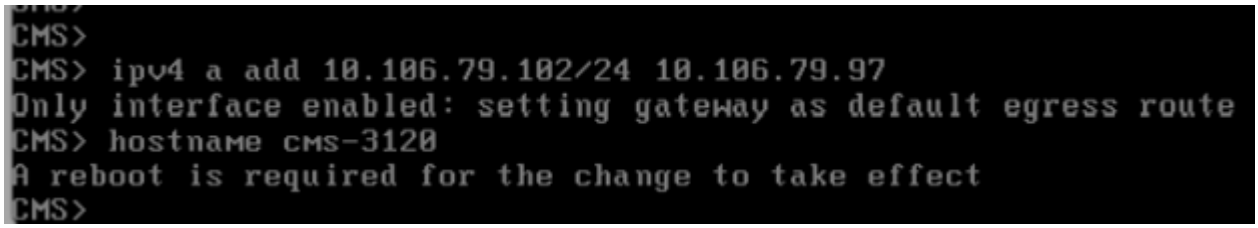
لم تعد كلمة المرور السابقة صالحة. بعد تعيين كلمة مرور جديدة، تظهر الخدمات مثل WebAdmin وWebBridge3 على أنها غير مكونة حتى يتم إستعادة النسخة الاحتياطية.

3. قم بتنفيذ الأمر:

ipv4 interface add address/prefix-length gateway

على سبيل المثال:

ipv4 a add 192.0.2.10/24 192.0.2.1



شكل 20: إعادة تطبيق IPv4 من وحدة التحكم.

يي إعادة التشغيل بعد تعييني العنوان. العناوين الموضحة في لقطة الشاشة هي لألغراض خاصة فقط.

4. قم بإعادة التشغيل بعد تعييني العنوان. بمجرد عودة النظام إلى الاتصال، استمر في استعادة البيانات إسم قسم الذاكرة المستعادة والخطوات الاحتياطي للنسخ SFTP لتحميل بعد ترقية 4.0.

ملاحظة: إذا تم تكوين حجز DHCP، يمكن تعييني العنوان الأصلي بالفعل بعد إعادة التشغيل. تحقق من العنوان باستخدام ipv4 a قبل بدء جلسة SFTP من محطة عمل الإدارة الخاصة بك.

في Cisco Meeting Server 4.0، يتم تمكين التخزين الآمن بشكل افتراضي على الأنظمة الأساسية التي تدعمها. لم يعد بإمكان MMP عرض secure_storage كتبديل بعد الترقية.



شكل 21: في هذه 4.0 قروص، لا يعد secure_storage أمرا معترفا عليه لأن التخزين الآمن بشكل افتراضي يتم تمكينه.

قم بتأكيد الإصدار باستخدام الأمر version.

ترقية السيناريوهات

يغطي هذا الفصل سيناريوهات ترقية مختلفة. أكمل ترقية الخطوة إلى 3.13.x. دون الخوض في نشر الخاص بك واختر السيناريو وفقا لذلك. اتبع الإجراء الذي يطابق بيئتك فقط و تجمع الخطوات من عمليات نشر نظام المجموعة والعقدة المفردة.

قم بالترقية الكامل إلى 3.13.x. ثم قم بدمج سيناريو واحد أو أكثر من الخطوة المجموعة والعقدة المفردة. إجراءات نظام مجموعة البيانات

- السيناريو 1: عقدة واحدة، معطل أو غير متوفر، VM، صغير، متوسط، وخادم الاجتماعات 2000
- السيناريو الثاني: عقدة واحدة، مكثف، VM، صغيرة، ومتوسطة فقط
- السيناريو 3: نظام مجموعة قواعد البيانات، معطل أو غير متوفر، VM و Small و Medium Meeting Server 2000
- السيناريو 4: مجموعة قواعد البيانات، مكثف، VM، صغير، متوسط فقط

.ةنآلما نيزختلا تاوحلد لوطعي ةدحو عم ةدحاو ةعقد - 1 يواريسلا

ثيح Meeting Server 2000 وأ "نمآلا نيزختلا" لوطعي عم لخادملا لإلجاء اذه مدختسأ نأ نكمي .3.11.x ردصملا رادصإ وأ رادصإ ثدحأ، نكلو يجب أن تتوفر ال "نمآلا نيزختلا". 4.0 ىلإ ةيقرتلا لبق 3.13.x ىلع ةدقعلا نوكت.

1. ةيقرتلا ةيجيردتلا ىلإ 3. 13.x. عبتا راسملا ةعومدملا (ىلع ليبس لاثملا 3.11.x → 3.12.x → 3.13.x). دعب لكل ةوطخ، مقا بتأكيدلا يف رادصإلا يلاوتلا وأ طورشلا يف مسؤلا ةحصلا نم ققحتلا لبق ءاشنإ خسنلا يطايتحالا ةيمهألا. وه حضوم يف مسقلا.

2. تأكيد حالة التخزين الآمن. قم بتشغيل الأمر secure_storage وتحقق من عدم تمكين ميزة التخزين الآمن. تخطي الأمر على Meeting Server 2000.

3. قم بإنشاء ملف نسخ إحتياطي 3.13.x وتصديره كما هو مذكور في قسم أخذ نسخة إحتياطية عندما يكون التخزين الآمن معطلا أو غير متوفر. تصدير محتوى SFTP المخصص لإحتياطية وحزمة السجل كما هو مذكور في قسم متطلبات ما قبل الترقية.

4. قم بتنزيل صورة البرنامج upgrade.img واستخراجها ونسخ إلى العقدة من Cisco.com 4.0 عبر SFTP.

5. بدء الترقية باستخدام هذا الأمر:

```
upgrade upgrade.img
```

6. بعد الأساسية. 6. أقر شعار التحذير. اضغط على Y فقط بعد اكتمال جميع المتطلبات، ثم بعد الترقية، قم بتكوين العقدة كما هو موضح في قسم التمهيد الأول واستعادة الشبكة، قم باستعادة النسخة الاحتياطية باستخدام قسم إستعادة البيانات بعد ترقية 4.0.

السيناريو 2 - عقدة واحدة مع تمكين التخزين الآمن

ثيح Meeting Server Medium وأ Meeting Server Small وأ لمستقل VM لجأ من لإلجاء اذه مدختسأ نأ نكمي ال .نمآلا نيزختلا نيكمت متي يتلا Meeting Server 2000 ىلع قبطني.

قبل نقل الملفات من الخادم، لاحظ أنه لا يمكن نقل المفاتيح الخاصة غير المشفرة ومفات النسخ الاحتياطي غير المشفرة. ملفات الشهادات غير محظورة.

1. قم بالترقية من خلال المسار المدعوم إلى 3.13.x دون تخطي الإصدارات. بعد كل خطوة، قم بإنشاء نسخة احتياطية من الخادم قبل التحقق من صحة الخادم وأن شورط الخطأ في قسم التحقق من صحة الخادم وأن الإصدار يتأكد من النسخ الاحتياطية.

2. قم بتشغيل secure_storage وتأكد من أن الإخراج يظهر التمكين: صحيح.

3. إنشاء نسخة إحتياطية مشفرة 3.13.x وتصديرها باستخدام قسم أخذ نسخة إحتياطية من الآمن. قم بتخزين عبارة المرور الخاصة به في متجر السري. أيضا تمكين التخزين عند تصدير محتوى SFTP المخصص وحزمة السجل (قسم متطلبات ما قبل الترقية).

4. انسخ upgrade.img إلى العقدة وتشغيل الترقية:

```
upgrade upgrade.img
```

5. اقرأ شعار التحذير واضغط Y للمتابعة فقط عند اكتمال المتطلبات الأساسية.

6. قم باسترداد الشبكة من وحدة التحكم (قسم التمهيد الأول واستعادة الشبكة)، ثم قم باستعادة النسخ الاحتياطي المشفر باستخدام عبارة المرور الخاصة به (قم باستعادة البيانات بعد قسم الترقية 4.0). 6. إذا كان MeetingApps قيد الاستخدام، فقم بتطبيق مفتاح MeetingApps Secret بعد قسم الاستعادة) مفتاح MeetingApps جديد).

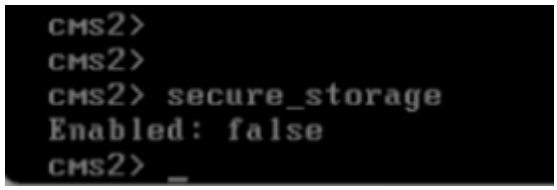
يتم تمكين التخزين الآمن بشكل افتراضي على Meeting Server 4.0. بعد الاستعادة، استمر في معالجة المفاتيح الخاصة وملفات النسخ الاحتياطي كبيانات مشفرة.

السيناريو 3 - تعطيل تخزين آمن لمجموعة قواعد البيانات

أستخدم هذه الإجراء لمجموعة قواعد بيانات مع تعطيل "التخزين الآمن"، الذي يتضمن مجموعة قواعد تحتوي على Meeting Server 2000. من الإصدار 3.5 وما بعده، يجب حل نظام مجموعة قواعد البيانات قبل ترقية البرامج. أولا، ترقية الخطوة لكل عقدة إلى 3.13.x.

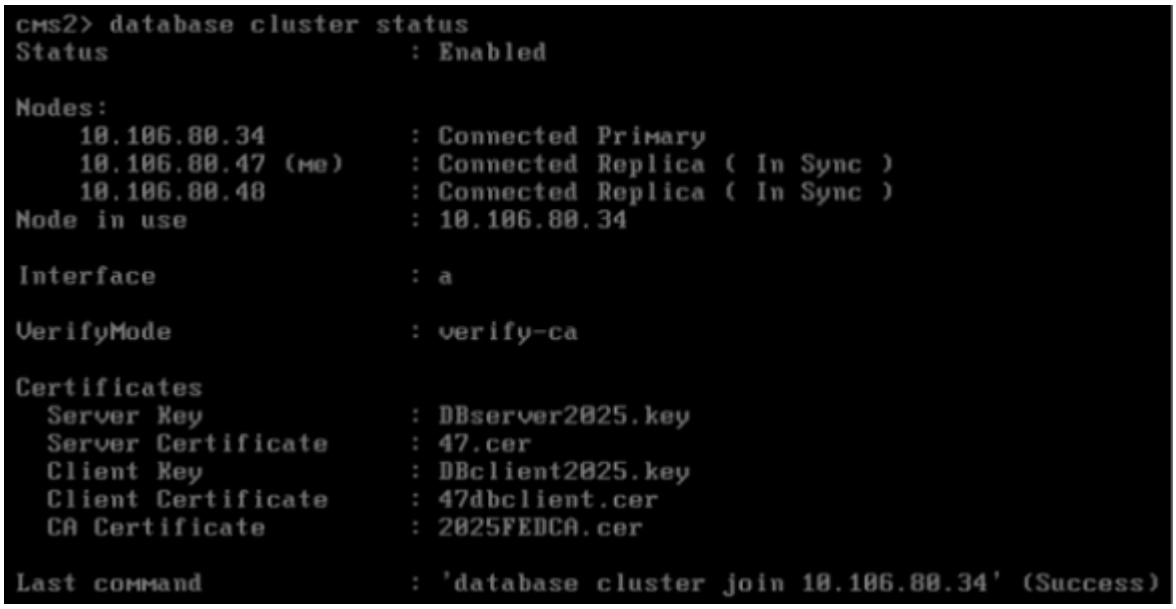
تسجيل تفاصيل نظام المجموعة والنسخ الاحتياطي لكل عقدة

1. قم بتشغيل secure_storage على كل عقدة. تعامل مع الأمر على أنه غير متوفر على عقد Meeting Server 2000.



شكل 22: قبل إستخدام النسخ الاحتياطية غير المشفرة، تحقق من تعطيل "التخزين الآمن" على كل عقدة نظام مجموعة. تخطي الأمر لعقد Meeting Server 2000، حيث ال يتوفر.

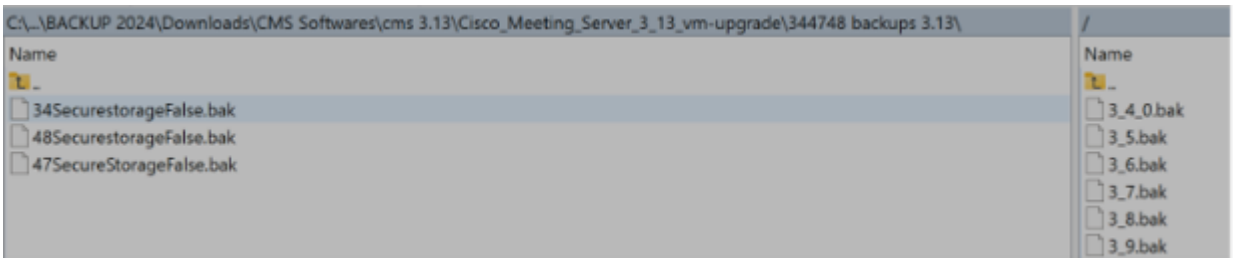
2. قم بتسجيل العقدة الأساسية لقاعدة البيانات الحالية لأنه يجب استعادتها أوال بعد الترقية إلى 4.0. تأكد من أن النسخ المتماثلة في Sync وأن حالة نظام المجموعة سليمة.



شكل 23: قم بتسجيل النسخ المتماثلة الأساسية الحالية وأكدها في المزامنة.

3. تأكد من أن جميع أنواع االستدعاءات قيد االستخدام تعمل وأن حاالت الأعطال واضحة في كل عقدة (التحقق من صحة الخادم قبل إنشاء قسم النسخ االحتياطية).

4. قم بإنشاء نسخة إحتياطية من كل عقدة باستخدام القسم "أخذ نسخة إحتياطية" عند تعطيل التخزين الآمن وأ عدم توفره. قم بتسمية كل ملف بحيث يتم تعيينه بوضوح إلى العقدة الخاصة به ونقل كل عملية نسخ إحتياطي إلى وحدة تخزين خارجية قبل حل نظام المجموعة.



شكل 24: تعمل جميع عقد الأمثلة الثالثة على إجراء عمليات نسخ إحتياطي لوحدات التخزين الخارجية المخزنة، المسماة لذلك يقوم كل ملف بتعيين عقده.

حل المجموعة

إزالة العقد بهذا الترتيب. احتفظ بالأساسي حتى الأخير:

- عقد خادم الاجتماعات المتصلة (غير الأساسية)
- عقد قاعدة بيانات النسخ المتماثل
- عقدة قاعدة البيانات الأساسية

على كل عقدة، قم بتشغيل الأمر الإزالة واضغط Y. لا تستمر في الترقية إلى الإصدار 4.0 حتى تبلغ كل عقدة بأنها قد غادرت المجموعة. تؤدي إزالة عضوية نظام المجموعة إلى ترك قاعدة البيانات المحلية الخاصة بهذه العقدة في مكانها.

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
```

شكل 25: في نسخة متماثلة، قم بتأكيد Y لإزالة عضوية نظام المجموعة. قاعدة البيانات المحلية للعقدة تبقى في مكانها.

```
 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
```

شكل 26: بعد الإزالة، تحقق من أن حالة نظام المجموعة معطلة وأن العقدة قيد الاستخدام هي "لا" على هذه العقدة.

```
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)
```

شكل 27: بعد إزالة النسخ المتماثلة، تعد النقطة الأساسية السابقة هي العقدة الوحيدة المتبقية في نظام المجموعة. قم بإزالته للمرة الأخيرة.

```
cms1> database cluster status
Status                    : Disabled
Node in use               : None

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 remove' (Success)

cms1> _
```

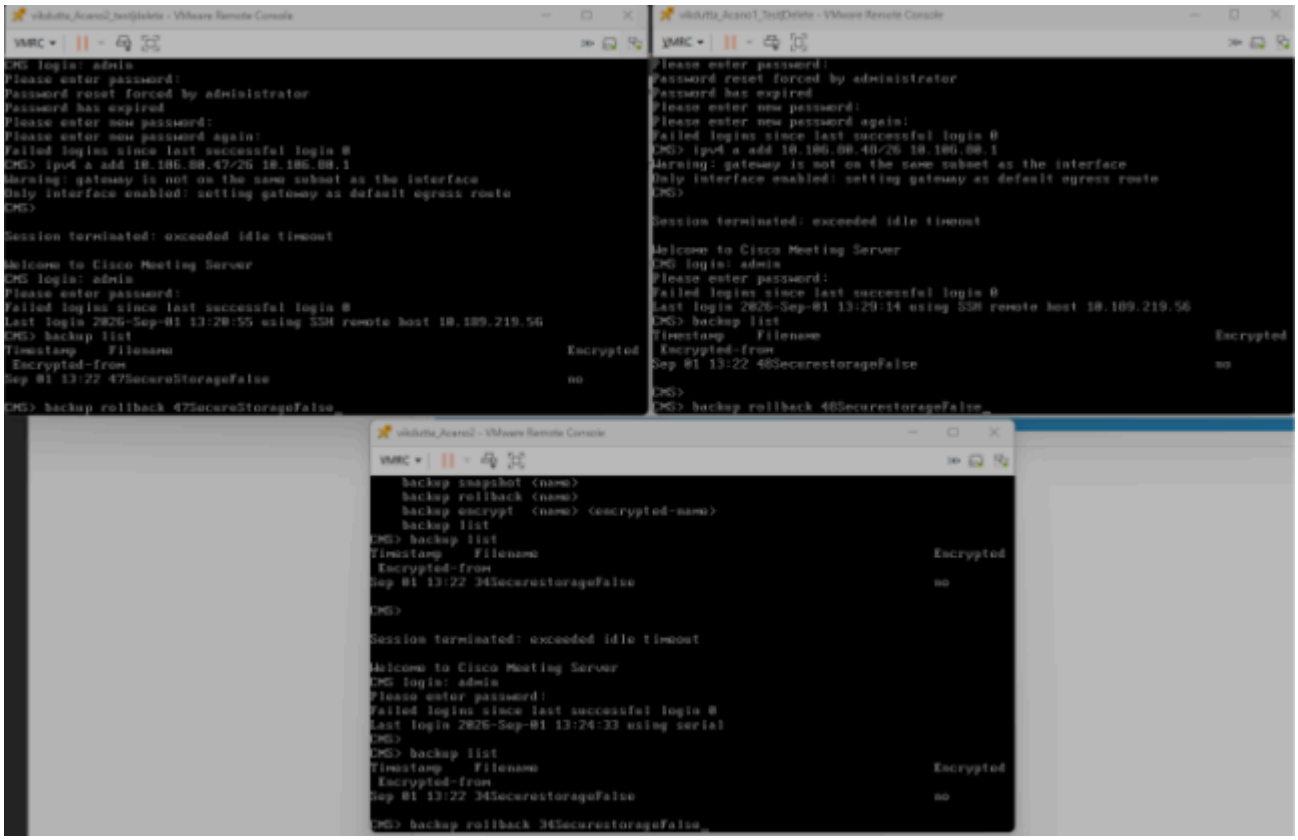
شكل 28: بعد إزالة الأساسي السابق، تحقق من أن الأمر يبلغ عن النجاح وأن حالة نظام المجموعة معطلة.

ترقية العقد واستعادتها

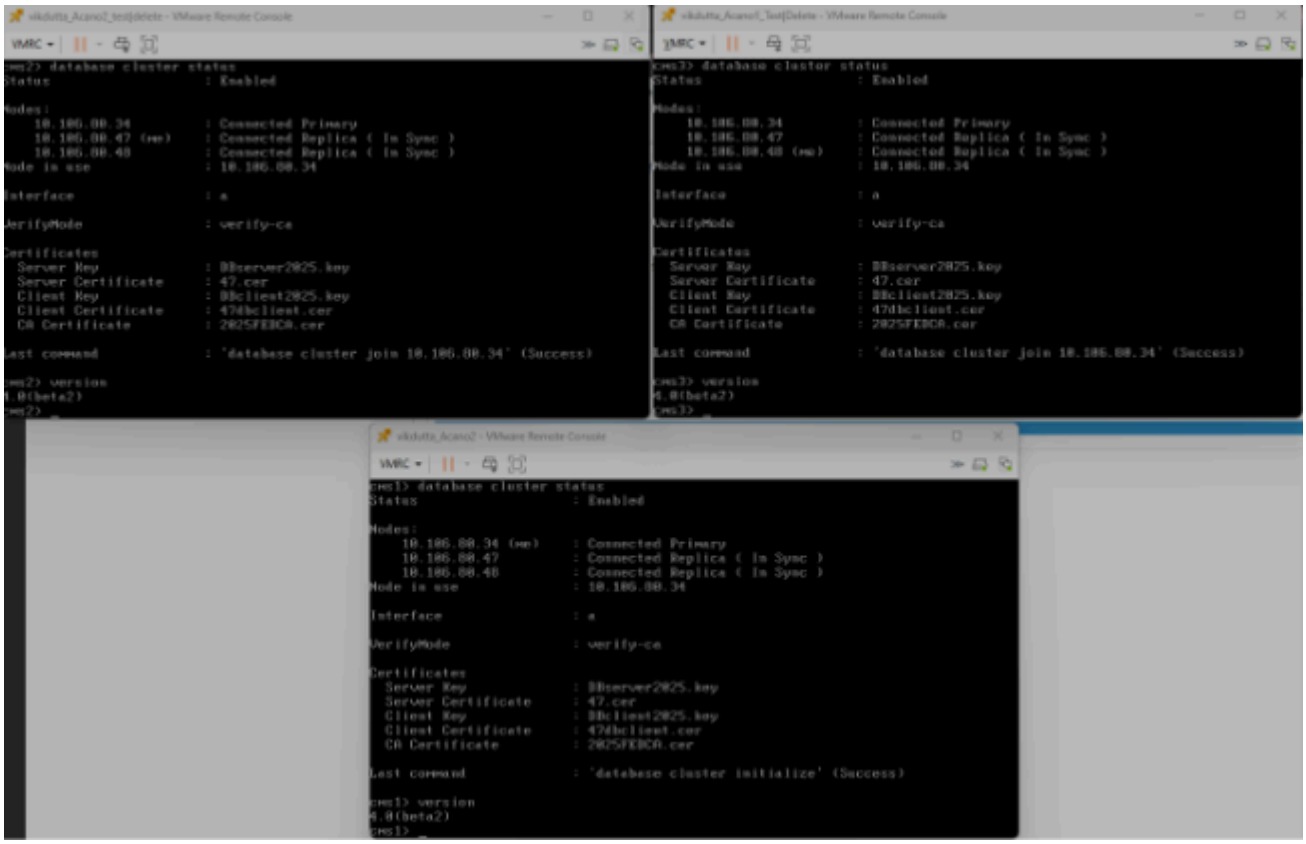
1. بمجرد حلها، تكون العقد مستقلة ويمكن ترقيتها بالتوازي. على كل عقدة، قم بنسخ upgrade.img عبر SFTP وقم بتشغيل الأمر upgrade:

2. قم باستعادة عنونة الشبكة لكل عقدة من وحدة التحكم (قسم التمهيد الأول واستعادة الشبكة).

3. انسخ النسخ الاحتياطي لـ 3.13.x الخاص بكل عقدة إلى تلك العقدة. قم باستعادة القسم الأساسي السابق أولاً، ثم يتبعه النسخ المتماثلة، ثم العقد المتصلة. أستخدم قسم إستعادة البيانات بعد ترقية 4.0. تؤدي عملية إستعادة النسخ الاحتياطية إلى إعادة إنشاء عضوية مجموعة قواعد البيانات.

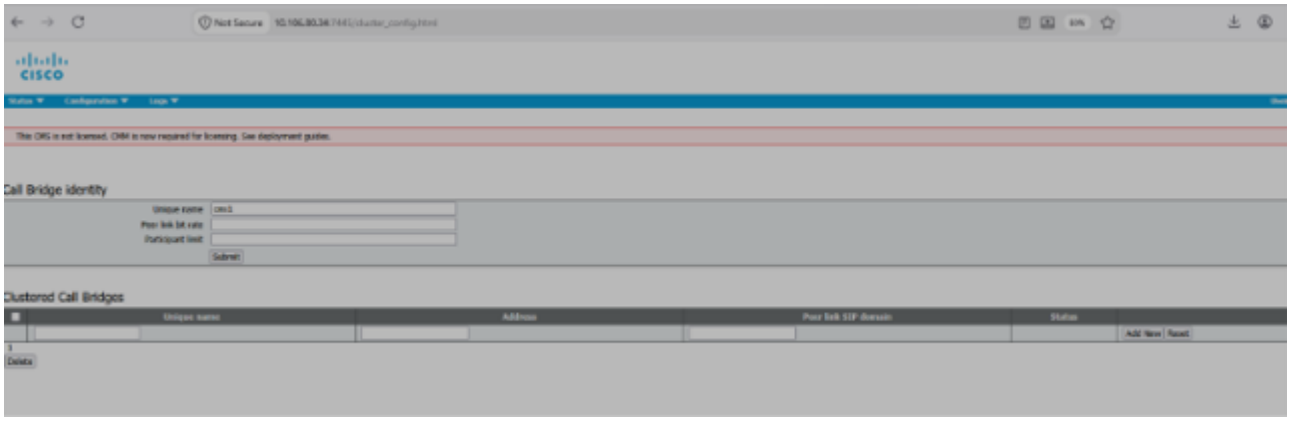


شكل 29: قم باستعادة اللقطة الخاصة بكل عقدة. ابدأ مع الأساسي السابق، ثم قم باستعادة النسخ المتماثلة. مثال أسماء الملفات يحدد عقدتهم.



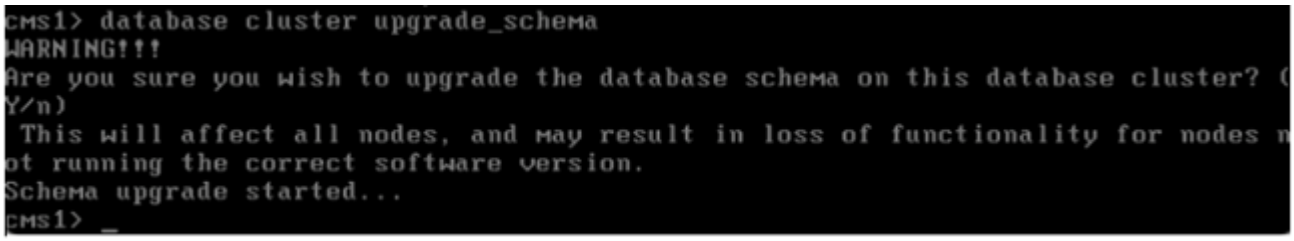
شكل 30: بعد الاستعادة على Meeting Server 4.0، تحقق من تمكين نظام المجموعة ومن عرض نفس الأساسي ومن مزامنة النسخ المتماثلة.

ملاحظة: إذا لم تظهر إتصالات نظام مجموعة Call Bridge بعد هذه الاستعادة، فقم بتشغيل الأمر **database cluster upgrade_schema** على الأساسي السابق فقط، ثم أعد التحقق من حالة "جسر المكالمات".

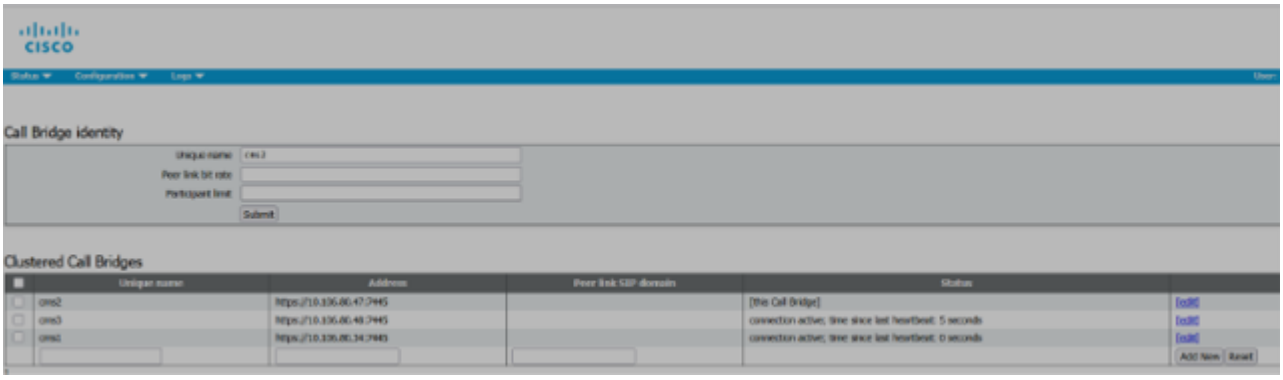


شكل 31: قبل ترقية المخطط، يظهر المثال نظام مجموعة قاعدة البيانات قيد التشغيل بينما "الاتصال المجمع" فارغ.

database cluster upgrade_schema



شكل 32: في الأساسي السابق، تأكد من Y فقط عند فشل إتصالات نظام مجموعة Call Bridge بعد ترقية نظام المجموعة الذي تم حله.



شكل 33: بعد ترقية المخطط، تحقق من أن كل نظير من نظراء "جسر المكالمات" يظهر اتصال نشط.

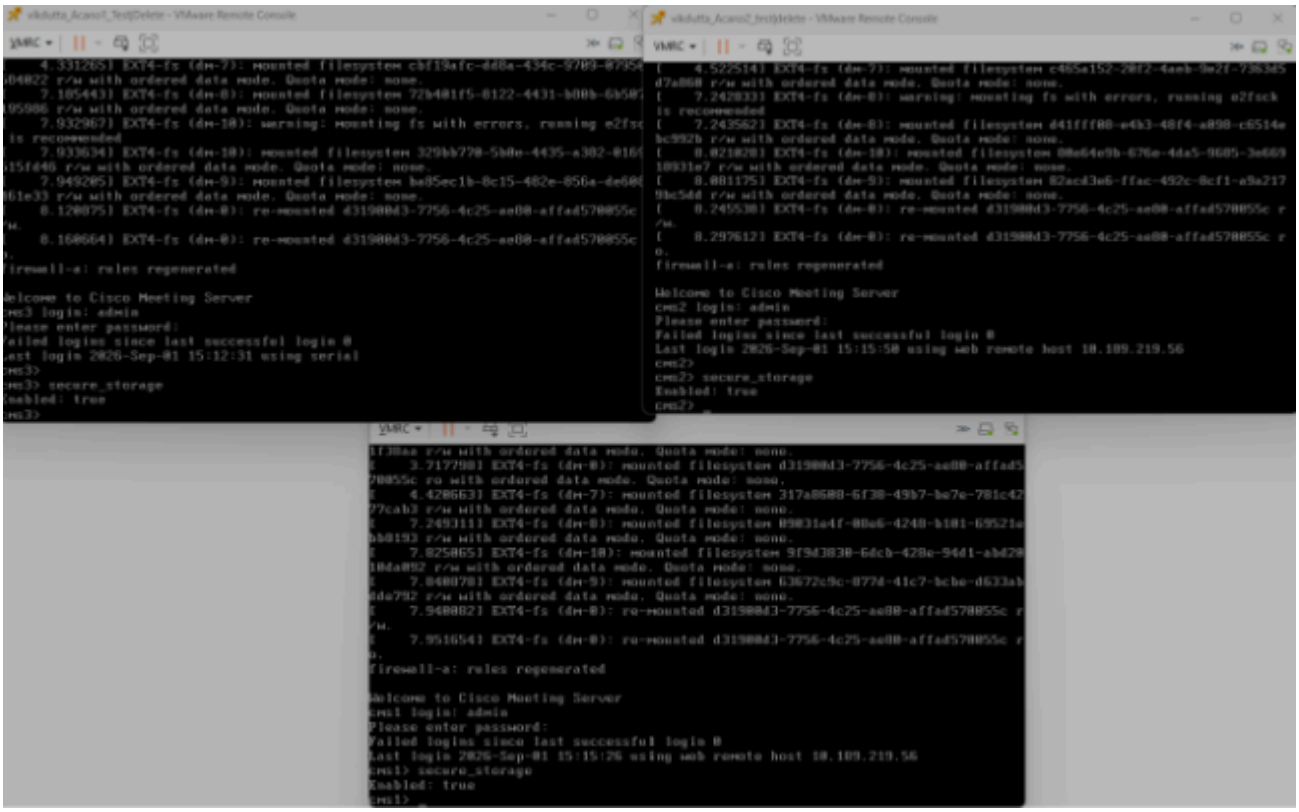
4. قم بإكمال الإجراء MeetingApps Secret في "المفتاح السري ل MeetingApps بعد الاستعادة على كل جسر ويب، ثم قم بالتحقق من النشر باستخدام قسم التحقق من الصحة بعد الترقية.

السيناريو 4 - مجموعة قواعد البيانات مع تمكين التخزين الآمن

أستخدم هذا الإجراء لمجموعة قواعد البيانات على الأجهزة الافتراضية (VM) أو خادم الاجتماعات الصغير أو وسط الاجتماعات حيث يتم تمكين التخزين الآمن على العقد. لا ينطبق على Meeting Server 2000. أولا، ترقية الخطوة لكل عقدة إلى 3.13.x.

تسجيل تفاصيل نظام المجموعة وإنشاء نسخ إحتياطية مشفرة

1. قم بتشغيل secure_storage على كل عقدة وتأكد من تمكينها: صحيح.



شكل 34: بالنسبة للمجموعة التوضيحية المكونة من ثلاث عقد، تأكد من تمكين عرض التخزين الآمن: صواب على كل عقدة قبل الترقية.

2. قم بتسجيل قاعدة البيانات الأساسية الحالية وتأكد من أن النسخ المتماثلة متزامنة.

```
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

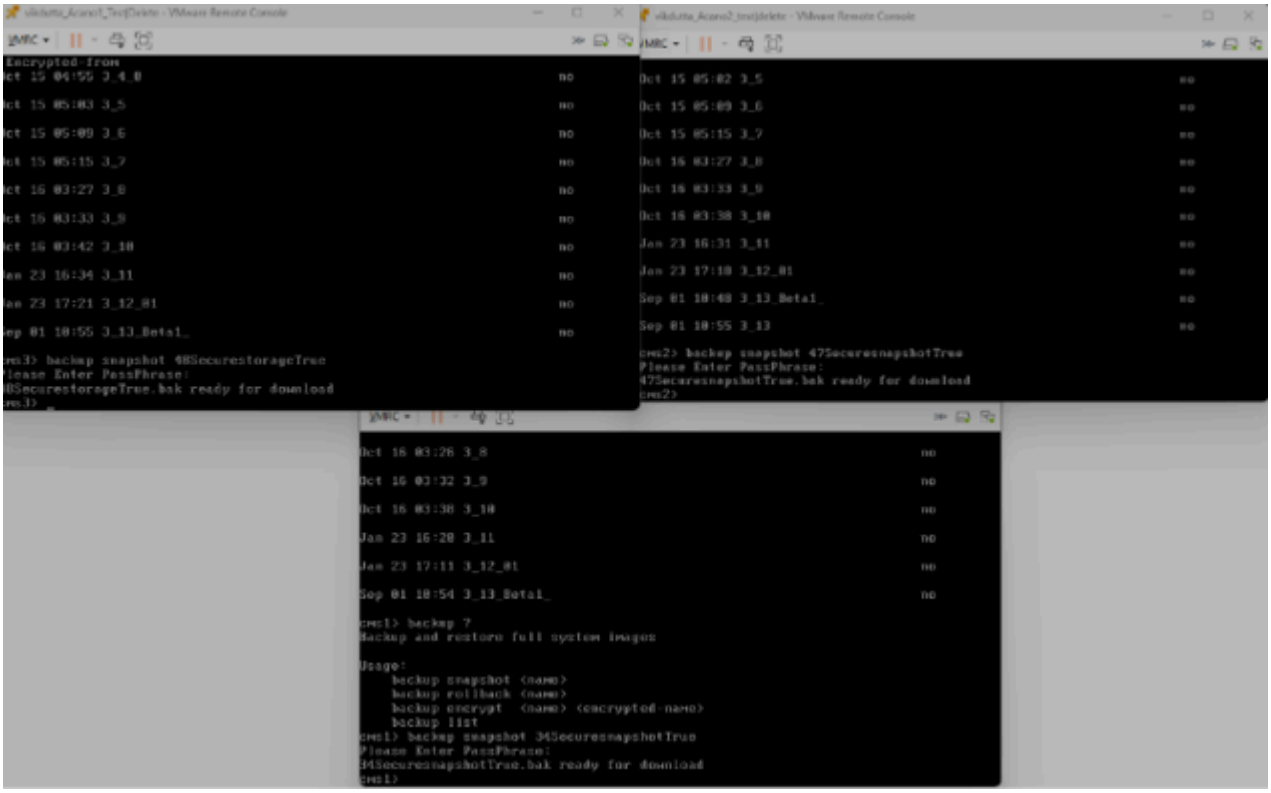
Certificates
  Server Key              : DBserver2025.key
  Server Certificate      : 47.cer
  Client Key              : DBclient2025.key
  Client Certificate      : 47dbclient.cer
  CA Certificate          : 2025FEDCA.cer

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

شكل 35: حالة مجموعة قاعدة البيانات قبل الترقية. قم بتسجيل النسخ المتماثلة الأساسية والتأكيد منها في المزامنة.

3. تأكد من جميع أنواع الاستدعاءات قيد الاستخدام ومن أن حالات الأعطال واضحة في كل عقدة (التحقق من صحة الخادم قبل إنشاء قسم النسخ الاحتياطية).

4. قم بإنشاء نسخة إحتياطية مشفرة من كل عقدة باستخدام قسم أخذ نسخة إحتياطية عند تمكين التخزين الآمن. قم بتعيين عبارة مرور فريدة وتسجيلها لكل ملف أو أستخدم سياسة عبارة مرور موثقة. قم بنقل الملفات المشفرة فقط خارج الخوادم قبل حل نظام المجموعة.



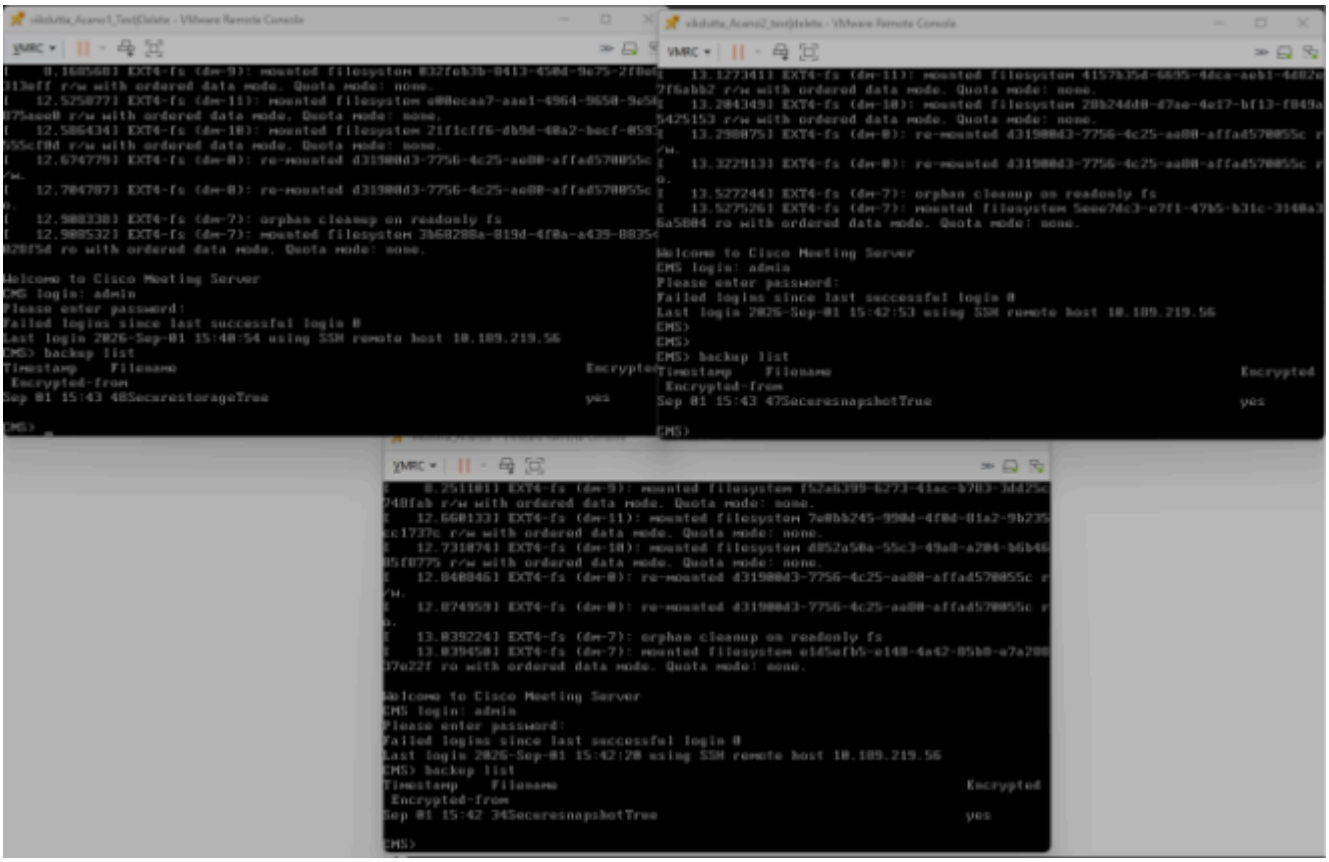
شكل 36: لقطة نسخ إحتياطي مشفرة على كل عقدة. يوضح المثال مطالبة عبارة المرور ثم كل ملف .bak جاهز للتنزيل.

حل النطاق والترقية والاستعادة

حل المجموعة كما هو موضح في السيناريو 3 بهذا الترتيب: العقد المتصلة والنسخ المتماثلة والنسخة الأساسية الأخيرة. أستخدم إزالة نظام مجموعة قواعد البيانات وتأكيد أن كل عقدة قد تركت نظام المجموعة.

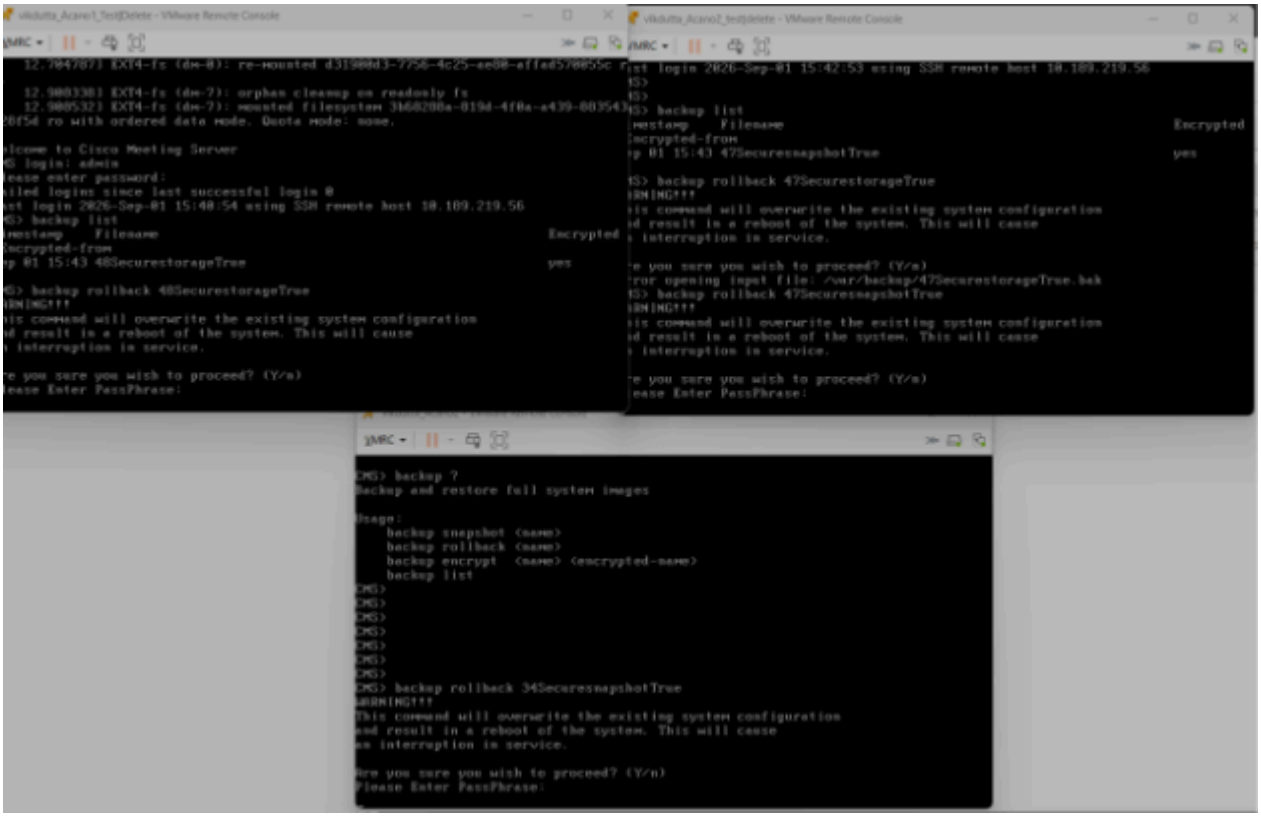
ترقية العقد المستقلة بالتوازي. إسترداد شبكة عنونة من الوحدة طرفية للتحكم (التمهيد الأول واستعادة الشبكة قسم).

قم بتحميل النسخ الاحتياطي المشفر الخاص بكل عقدة. قبل التراجع، تأكد من ظهور اللقطة التي تم تحميلها في قائمة النسخ الاحتياطي على أنها مشفرة: نعم. قم باستعادة الأساسي السابق أولا، ثم النسخ المتماثلة والعقد المتصلة. أستخدم الأمر backup backlback أدناه، وقم بتأكيد Y، وأدخل عبارة مرور النسخ الاحتياطي عند طلبها. تتم إعادة تمهيد العقدة بعد قبول عبارة المرور. تكرار لكل عقدة.



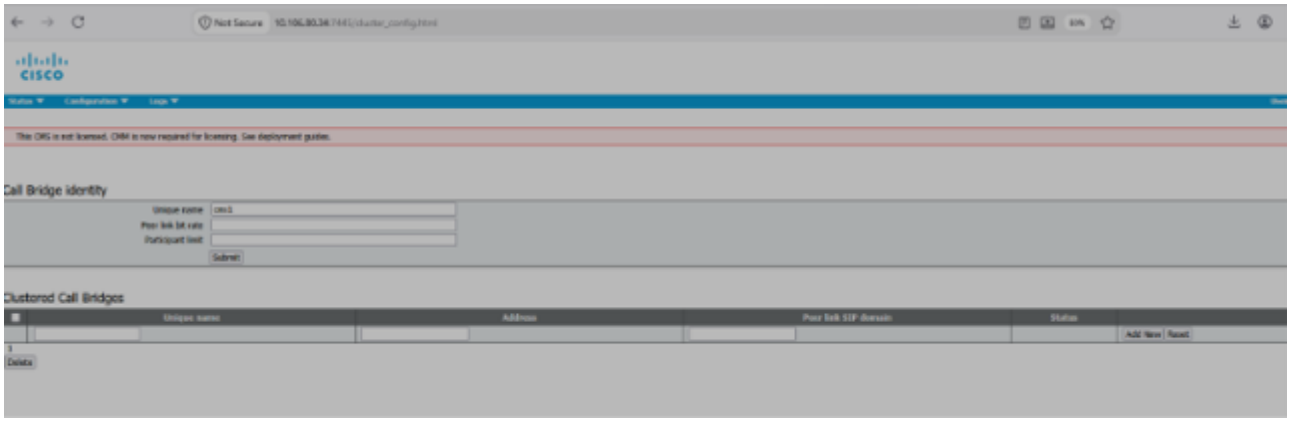
شكل 37: بعد التمهيد الأول وقبل المعيار 4. 0، يجب أن تظهر اللقطة التي تم تحميلها في قائمة النسخ الاحتياطي على أنها مشفرة: أيقونة وتكوين جاهزة للرجوع لورا.

backup rollback encrypted-filename



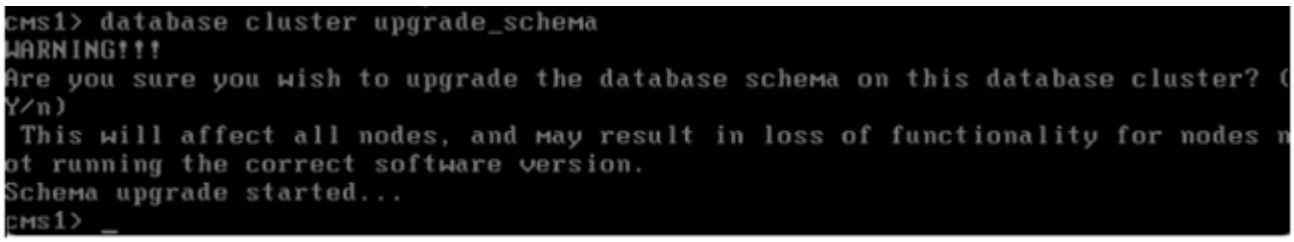
شكل 38: قم بتأكيد Y، وأدخل عبارة المرور، ثم قم باستعادة الأساسي السابق أولا.

ملاحظة: إذا لم تظهر إتصالات نظام مجموعة Call Bridge بعد هذه الاستعادة، فقم بتشغيل الأمر **database cluster upgrade_schema** على الأساسي السابق فقط، ثم أعد التحقق من حالة "جسر المكالمات".

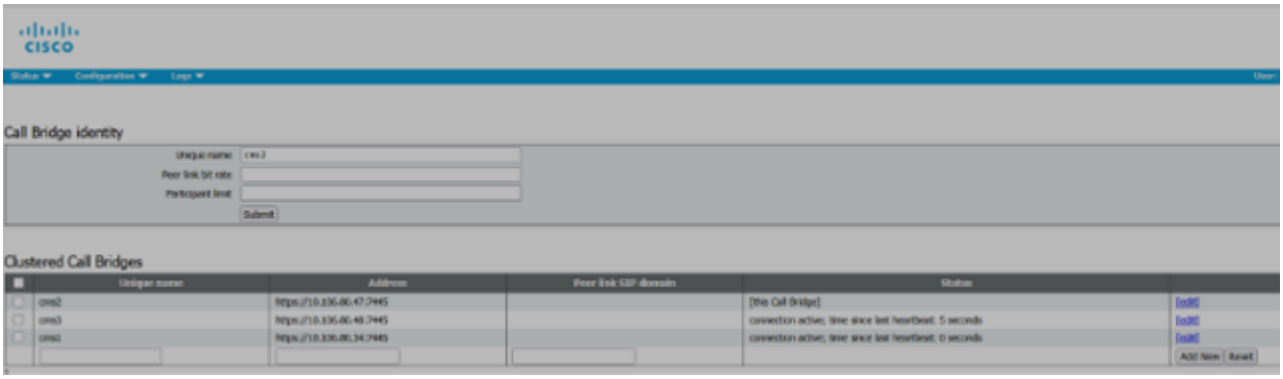


شكل 39: قبل ترقية المخطط، يظهر المثال نظام مجموعة قاعدة البيانات قيد التشغيل بينما "الاتصال المجمع" فارغ.

database cluster upgrade_schema



شكل 40: في الأساسي السابق، تأكد من Y قطع عند فشل إتصالات نظام مجموعة Call Bridge بعد ترقية نظام المجموعة الذي تم حله.



شكل 41: بعد ترقية المخطط، تحقق من أن كل نظير من نظراء "جسر المكالمات" يظهر اتصالا نشطا.

قم بإكمال الإجراء MeetingApps Secret في المفتاح MeetingApps Secret بعد قسم الاستعادة في دليل التثبيت.

التحقق من صحة ما بعد الترقية

أكمل قائمة التحقق هذه بعد الاستعادة وقبل إعادة النظام إلى الإنتاج:

- تظهر مسؤول الويب على كل عقدة Cisco Meeting Server 4.0.
- تم تمكين خدمات MMP المطلوبة وتشغيلها (نشطة: صحيح).
- حالات الأعطال والصحة. تعامل مع الأخطاء والتحذيرات الأخيرة كمعلومات ما لم يوجد خطأ مطابق.
- إن أمكن، تظهر حالة نظام مجموعة قاعدة البيانات الأساسي والنسخ المتماثلة المتوقعة.
- يتم إستعادة الترخيص الذكي واتصال Call Bridge.
- تم إكمال مكالمات SIP و Web App client التي يدعمها هذا النشر بنجاح.
- يتم إستعادة العلامة التجارية ومطالبات الصوت وملفات SSO التي يتم نسخها من النسخة الخادم في قسم متطلبات ما قبل الترقية إذا لم تكن مضمنة بالفعل في النسخة الاحتياطية.
- في حالة نشر MeetingApps، يعرض Web Bridge علامة MeetingApps الجديدة أو العلامة مشاركة الملفات.
- قم بإزالة اللقطات قصيرة العمر فقط بعد قبول النشر.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).