Meeting Server를 릴리스 4.0으로 업그레이드 - 백서

목차

- 소개
- 배경 정보
- 보안 스토리지 개요
  - 지원되는 플랫폼
  - 구현 참고 사항
- 업그레이드 원칙 및 제약 조건
  - 필수 업그레이드 경로
  - 다운그레이드
  - 4.0 업그레이드를 위한 주요 백업 요구 사항
  - 첫 번째 로그인 및 비밀번호 컨피그레이션
  - 업그레이드 후 네트워크 연결 다시 설정
  - 백업을 만들기 전에 서버 상태 확인
- 업그레이드 전 요구 사항
- 일반적인 백업 및 복원 절차
  - 4.0 업그레이드 후 영향을 받는 데이터
  - 보안 저장소가 비활성화되었거나 사용할 수 없는 경우 백업 수행
  - 보안 스토리지가 활성화된 경우 백업 수행
  - 4.0 업그레이드 후 데이터 복원
  - 복원 후 MeetingApps 비밀 키
- 첫 번째 부팅 및 네트워크 복원
- 업그레이드 시나리오
  - 시나리오 1 - 보안 스토리지가 비활성화되었거나 사용할 수 없는 단일 노드
  - 시나리오 2 - 보안 스토리지가 활성화된 단일 노드
  - 시나리오 3 - 보안 저장소가 비활성화된 데이터베이스 클러스터
    - 클러스터 세부 정보 기록 및 모든 노드 백업
    - 클러스터 분리
    - 노드 업그레이드 및 복원
  - 시나리오 4 - 보안 스토리지가 활성화된 데이터베이스 클러스터
    - 클러스터 세부 정보 기록 및 암호화된 백업 생성
    - 분리, 업그레이드 및 복원
- 업그레이드 후 검증

소개

이 문서에서는 Cisco Meeting Server를 릴리스 4.0으로 업그레이드하는 방법에 대해 설명합니다.

배경 정보

이 문서는 Cisco Meeting Server 릴리스 정보, MMP 명령 참조 설명서 및 Secure Storage Administrator 참조 설명서와 함께 사용하여 요구 사항 및 전제 조건을 이해합니다.

이미지를 적용하면 노드의 공장 재설정이 트리거되므로 Cisco Meeting Server 4.0의 업그레이드 프로세스는 이전 버전과 다릅니다. 서비스 연속성을 보장하려면 업그레이드를 시작하기 전에 외부 위치로 내보낸 백업을 통해 네트워크 설정 및 비밀번호를 포함하는 모든 이전 컨피그레이션을 유지해야 합니다.

또한 Secure Storage는 Cisco Meeting Server 버전 3.11~3.13에서는 선택 사항이었지만 버전 4.0에서는 기본적으로 활성화되어 있습니다. 따라서 Secure Storage를 사용하지 않았거나 3.11x, 3.12x 또는 3.13x에서 이미 활성화한 경우 다른 백업 및 복원 절차를 따라야 합니다.

보안 스토리지는 서버의 개인 키 및 백업 파일을 암호화하며, 외부 스토리지로 전송하기 전에 해당 파일을 암호화해야 합니다.

이 문서에서는 필요한 지침을 단일 참조로 통합하여 동일한 단계를 반복하지 않고도 모든 업그레이드 시나리오에 대한 일반적인 절차를 수행할 수 있습니다.

이 문서에서는 다음 항목에 대해 설명합니다.

- 보안 스토리지가 무엇이며, 어디에 적용되며, 무엇을 하지 않는지 파악합니다.
- 업그레이드 경로. 여기에는 4.0 이전에 3.13.x에 도달해야 한다는 요구 사항과 4.0에서 다운그레이드할 수 없다는 사실이 포함됩니다.
- 보안 스토리지가 활성화된 노드와 사용되지 않거나 사용할 수 없는 노드에 대한 일반적인 백업 및 복원 방법입니다.
- 업그레이드 전에 데이터베이스 클러스터가 해제되는 동안 데이터베이스 클러스터 노드 분리 시퀀싱입니다.
- MeetingApps 비밀 키. Cisco Meeting Server 백업에 저장되지 않으며 복원 후 다시 생성해야 합니다.

참고: 이 문서에서는 4.0 베타 소프트웨어 버전을 포함하여 원래 업그레이드 지침 테스트 중에 캡처된 랩 스크린샷을 사용합니다. 표시된 모든 호스트 이름, IP 주소 및 파일 이름은 엄격하게 예시되며 실제 운영 자격 증명 또는 민감한 암호를 반영하지 않습니다. 클러스터 보기가 필요한 추가 컨텍스트를 제공하지 않는 한 명확성을 유지하고 중복을 방지하기 위해 반복 단계는 일반 절차 섹션에서 한 번만 표시됩니다.

보안 스토리지 개요

Secure Storage는 Meeting Server에 있는 중요한 파일을 암호화하고 이러한 파일이 Call Bridge 서버에서 오프로드되는 방식을 제어하여 데이터 보안을 강화합니다. 이 기능은 Cisco Meeting Server 3.11에서 가상 머신 구축(사양 기반 또는 Meeting Server Small) 및 Meeting Server Medium에서 MMP secure_storage enable 명령을 사용하여 구성 가능한 옵션으로 도입되었습니다.

버전 4.0에서는 보안 스토리지가 기본적으로 활성화되어 있습니다. 이 설정은 이제 영구적이며 되돌릴 수 없으며 secure_storage enable MMP 명령이 제거되었습니다.

Meeting Server는 보안 스토리지를 사용하여 다음 동작을 시행합니다.

- 개인 키는 암호화될 때까지 SFTP를 통해 다운로드할 수 없습니다. pki encrypt MMP 명령 뒤에 최소 14자의 패스프레이즈를 사용하여 개인 키를 암호화합니다. Meeting Server 서비스에서 현재 사용하는 키는 변경되지 않습니다.
- backup encrypt <name> encrypted-name 명령으로 만든 백업 파일은 암호화됩니다. Secure Storage가 활성화된 경우 backup encrypt <name> encrypted-name MMP 명령은 14자 이상의 암호를 입력하라는 메시지를 표시합니다. 백업 복원 시 동일한 암호가 필요합니다.
- 백업 파일을 다운로드하기 전에 암호화된 형식이어야 합니다. 나열된 백업이 아직 익스포트를 위해 암호화되지 않은 경우 backup encrypt <name> encrypted-name을 사용하십시오. 암호화되지 않은 백업의 다운로드는 거부됩니다.
- 버전 3.12에서는 FIPS가 활성화된 경우 보안 스토리지가 작동할 수 있습니다. 3.11에서 생성된 개인 키 파일은 14자 이상의 암호를 사용하여 다시 생성해야 합니다.

팁: 보안 저장소는 Meeting Server에서 암호화되지 않은 개인 키 및 암호화되지 않은 백업 파일의 전송을 제한합니다. 인증서 파일의 전송을 제한하지 않습니다. 인증서는 SFTP로 복사할 수 있습니다. 연결된 암호화되지 않은 개인 키만 pki 암호화로 암호화될 때까지 차단됩니다.

주의: MMP 명령을 사용하면 보안 스토리지를 비활성화할 수 없습니다. 작업을 취소할 수 없습니다. factory_reset full만 Secure Storage를 false로 재설정합니다. 백업 스냅샷으로 컨피그레이션 백업을 수행하고 별도의 디바이스에 저장한 다음 보안 스토리지를 활성화합니다. secure_storage가 완료되면 즉시 재부팅이 가능합니다. 재부팅을 건너뛰면 보안 스토리지가 완전히 초기화되지 않은 채 활성화됨으로 표시될 수 있으며, factory_reset full과 같은 명령이 실패할 수 있습니다. 이 상태의 복구 경로는 이전에 저장된 스냅샷으로 되돌아가는 것입니다(3.13.x에만 유효함). Meeting Server 4.0에서는 secure_storage가 기본적으로 활성화되어 있습니다.

지원되는 플랫폼

- 가상 머신(사양 기반): 지원
- Meeting Server Small/1K: 지원
- 회의 서버 미디어: 지원
- 회의 서버 2000: 지원되지 않음. 보안 스토리지 기능을 사용할 수 없습니다. 이 플랫폼에서는 Secure Storage 명령을 사용하지 마십시오.

Cisco Meeting Server 4.0은 모든 호환 플랫폼에서 기본적으로 보안 스토리지를 활성화합니다. 업그레이드 후에는 보안 스토리지가 비활성화된 상태에서 3.13.x 백업을 수행한 경우에도 데이터가 보안 스토리지에 의해 자동으로 보호됩니다.

구현 참고 사항

- 업그레이드 이미지의 이름을 변경해도 보안 저장소 설정은 변경되지 않습니다.
- 백업을 수행하기 전에 secure_storage 명령을 사용하여 모든 노드에서 보안 스토리지 상태를 확인합니다.
- 이 명령은 보안 스토리지가 활성화되었는지(True) 또는 활성화되지 않았는지(False) 여부를 보고합니다. Meeting Server 2000에서는 명령을 적용할 수 없습니다. cisco Meeting Server 2000을 업그레이드하는 동안 Secure Storage가 비활성화되거나 사용할 수 없는 업그레이드 조건에 설명된 단계를 수행합니다.



보안 저장소가 활성화되지 않은 경우 MMP 출력(활성화됨: False).



그림 2: 보안 저장소가 활성화된 경우 MMP 출력(활성화됨: Cisco Meeting Server 3.13의 경우 true).

자세한 명령 구문 경고 및 사용 예는 현재 사용 중인 Cisco Meeting Server Administrator Quick Reference Guide for Secure Storage 및 MMP Command Reference에서 확인할 수 있습니다.

업그레이드 원칙 및 제약 조건

필수 업그레이드 경로

Cisco Meeting Server 업그레이드는 주요 릴리스를 건너뛰지 않고 순차적 경로를 따라야 합니다. 예를 들어 3.11.x의 노드는 4.0에 도달하기 전에 3.12.x 및 3.13.x를 통해 진행해야 합니다. 3.9.x에서 3.13.x 또는 3.11.x에서 4.0으로 직접 업그레이드하는 것은 지원되지 않으며 일반적으로 복구할 수 없는 구성 오류가 발생합니다. 버전 3.11.5 또는 3.13의 Meeting Server Medium의 경우 업그레이드 경로는 3.11.5 → 3.13 → 4.0입니다.



팁: 4.0 업그레이드를 시작하기 전에 모든 노드에서 Cisco Meeting Server 3.13.x를 실행해야 하며, 3.13.x 시스템에서 내보낸 확인된 컨피그레이션 백업이 포함되어 있습니다. 이 백서의 모든 시나리오 절차에서는 3.13.x로의 업그레이드가 이미 완료된 것으로 가정합니다.

다운그레이드



팁: 4.0.x에서 3.13.x로의 다운그레이드는 지원되지 않습니다. 업그레이드가 실패하거나 시스템이 예상대로 작동하지 않으면 새 3.13.x OVA를 배포하고(또는 어플라이언스를 이미지로 다시 설치) 3.13.x 백업을 복원합니다. 업그레이드 기간 동안 추가 복구 옵션으로 3.13.x 가상 머신의 하이퍼바이저 스냅샷을 보관합니다. VM 스냅샷은 내보낸 컨피그레이션 백업을 대체하지 않습니다.

4.0 업그레이드를 위한 주요 백업 요구 사항

4.0 업그레이드가 확인되면 노드가 첫 번째 부팅 상태로 재부팅됩니다. 업그레이드 실패로 인해 SFTP 액세스가 손실되고 파일에 액세스할 수 없게 될 수 있으므로 업그레이드 프로세스 중에 생성된 자동 백업에 의존하지 마십시오. backup snapshot 명령으로 생성하여 외부 스토리지에 복사한 백업만 복구에 안정적으로 사용할 수 있습니다.

첫 번째 로그인 및 비밀번호 컨피그레이션

버전 4.0의 첫 번째 부팅 시 기존 MMP 비밀번호가 데이터베이스에서 제거됩니다. 사용자 이름 admin을 빈 비밀번호(비밀번호 없음)로 로그인합니다. 시스템에서 새 MMP 비밀번호를 설정해야 합니다. 확인 및 확인을 위해 비밀번호를 두 번 입력하라는 메시지가 표시됩니다. Meeting Server에는 암호 복구 기능이 없으므로 새 암호를 기록하십시오.

참고: 처음 부팅할 때 새 MMP 비밀번호를 설정하면 backup rollback 명령이 3.13.x 백업에 저장된 비밀번호로 대체합니다. 서버에서 백업을 복원한 후에는 백업을 만들 때 활성 상태였던 암호를 사용하여 로그인해야 합니다.

업그레이드 후 네트워크 연결 다시 설정

IPv4 및 IPv6 주소, 마스크 및 게이트웨이는 나머지 컨피그레이션과 함께 손실됩니다. 4.0으로 업그레이드한 후 Meeting Server의 네트워크 연결이 끊어질 수 있습니다. MMP에서 주소 지정을 다시 할당할 수 있도록 하이퍼바이저 콘솔, CIMC 또는 직렬 액세스 권한이 있어야 합니다.



참고: DHCP 예약을 사용하는 구축은 일반적으로 재부팅 후 동일한 IP 주소를 유지합니다. 그러나 콘솔 액세스는 주소가 확인될 때까지 사용 가능해야 합니다. IP 주소가 확인될 때까지 SSH 연결이 복원된다고 가정하지 마십시오.

백업을 만들기 전에 서버 상태 확인

3.13으로 업그레이드할 때마다 서버가 정상 상태이고 모든 서비스가 작동 중인지 확인하십시오. Server Overview(서버 개요) 페이지에서 어떤 결함 조건도 무시하지 마십시오. 오류/오류가 발생하면 3.13에 백업 스냅샷이 생성되기 전에 해당 오류를 수정합니다. 이렇게 하면 업그레이드된 4.0 노드에서 서버 백업이 복원되어 배포 오류가 발생하지 않습니다.

Web Admin(웹 관리)에서 Status(상태)를 열고 Fault conditions(결함 조건) 섹션이 비어 있는지 확인합니다. 최근 오류 및 경고 아래에만 나타나는 항목은 무시합니다. 업그레이드 후에는 임시 데이터베이스 또는 Web Bridge 메시지가 표시되는 것이 일반적입니다. 이는 복원 또는 백업을 지연할 이유가 아닙니다.

결함 상태가 10분 이상 남아 있는 경우 백업을 수행하기 전에 해결합니다. 이미 결함이 포함된 3.13.x 백업을 4.0으로 복원하면 해당 결함이 전달됩니다.

클러스터링된 시스템의 경우 사용 중인 모든 통화 유형(SIP 엔드포인트 및 Web App 클라이언트)이 작동 중인지, 어떤 노드에도 결함 조건이 나열되지 않는지 확인합니다.

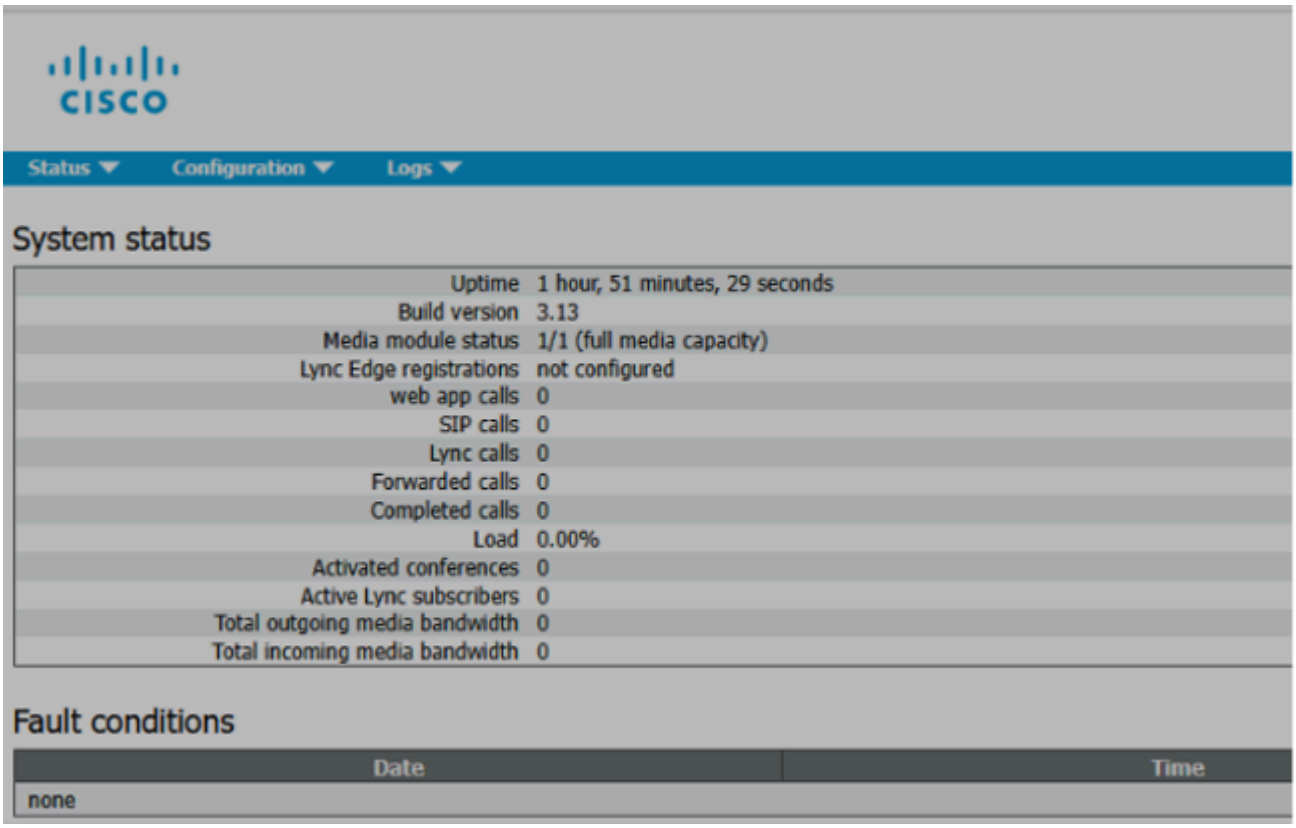


그림 3: Web Admin Status(웹 관리 상태) 페이지(3.13.x)의 Fault(결함) 조건이 비어 있습니다. 4.0에 복원된 백업을 수행하기 전에 이 보기를 사용하십시오.

업그레이드 전 요구 사항

버전 4.0으로의 업그레이드를 시작하기 전에 다음 작업을 완료하십시오. 이러한 요구 사항은 이 문서의 뒷부분에서 다룬 네 가지 시나리오 모두에 적용됩니다.

- 3.13.x로 업그레이드한 다음 컨피그레이션 백업을 내보냅니다. 노드에서 Cisco Meeting Server 3.13.x를 실행 중인지 확인합니다. 백업을 생성하고 로고, 브랜딩 파일, 오디오 프롬프트, SSO 파일 및 기타 사용자 지정 데이터와 같은 모든 사용자 지정 SFTP 데이터와 함께 외부 스토리지로 전송합니다. 일반 백업 및 복원 절차 섹션의 절차를 사용합니다. 클러스터링된 환경에서는 모든 노드, 즉 연결된 주 복제본뿐만 아니라 연결된 복제본에서 백업을 가져옵니다.
- 네트워크 설정을 기록합니다. ipv4 a를 실행하고 출력을 저장합니다. DHCP 예약이 IP 주소를 자동으로 복원하지 않는 한 4.0 재부팅 후 콘솔에서 이 정보를 다시 입력해야 합니다.
- 콘솔 액세스를 확인합니다. 시작하기 전에 하이퍼바이저 콘솔, CIMC 또는 직렬 액세스를 사용할 수 있어야 합니다. 노드가 4.0으로 재부팅되면 SSH가 중단됩니다.
- 보관을 위해 현재 로그 번들을 다운로드합니다. 각 노드에서 logbundle.tar.gz를 저장합니다. 번들은 백업 스냅샷을 대체하지 않습니다.
- upgrade 명령이 실행된 후 표시되는 4.0 업그레이드 경고 배너를 읽습니다.
- 필수 조건이 불완전한 경우 n을 눌러 중단합니다. 진행할 준비가 된 경우에만 Y를 누릅니다.

일반적인 백업 및 복원 절차

이 문서의 뒷부분에서 설명하는 4가지 업그레이드 시나리오에서는 동일한 백업, 내보내기, 처음 부팅 및 복원 패턴을 사용합니다. 이 섹션을 이러한 단계의 단일 소스로 사용한 다음 시나리오별 시퀀싱(단일 노드 대 클러스터 및 보안 스토리지가 이미 활성화되었는지 여부)만 수행합니다.

4.0 업그레이드 후 영향을 받는 데이터

이 데이터는 4.0 업그레이드 후 백업을 복원할 때까지 손실됩니다.

- 스페이스, 사용자 및 통화 프로필을 포함하는 데이터베이스 콘텐츠입니다.
- 인증서 및 개인 키
- 로컬 사용자 지정, SSO 파일 및 오디오 프롬프트 파일
- DHCP 예약에서 주소를 복원하는 경우를 제외한 네트워크 컨피그레이션(IP 주소, 마스크 및 게이트웨이).
- 백업 롤백이 백업에서 비밀번호를 다시 적용할 때까지 이전 MMP 비밀번호입니다.
- 통화 브리지, 웹 관리자, 웹 브리지 및 기타 응용 프로그램 서비스는 복원 후에만 반환됩니다.



팁: Cisco Meeting Server 백업에는 MeetingApps 비밀 키가 포함되어 있지 않습니다. 복원 후에는 해당 키를 다시 생성하여 모든 Web Bridge 노드에 적용해야 합니다. 복원 후 MeetingApps 비밀 키 섹션을 참조하십시오.

보안 저장소가 비활성화되었거나 사용할 수 없는 경우 백업 수행

Secure_storage 보고서가 활성화된 가상 머신, Meeting Server Small 및 Meeting Server Medium에서 다음 절차를 수행합니다. False이고 보안 저장소를 사용할 수 없는 Meeting Server 2000입니다.

1. 각 노드에서 backup snapshot 명령을 사용하여 파일을 생성합니다. 이전 파일 이름을 다시 사용하지 마십시오.

2. SFTP를 사용하여 백업 파일을 즉시 외부 저장소에 복사합니다. Meeting Server에 유일한 복사본을 유지하지 마십시오.

3. 노드가 다시 작성될 경우 여전히 연결 가능한 위치에 파일을 저장합니다.

예:

backup snapshot cms313SecurestorageFalse backup list

4. 파일이 backup list 명령에 나타나는지 확인한 다음 SFTP 클라이언트를 사용하여 외부 디스크로 전송합니다.

5. 클러스터의 모든 노드에서 이 프로세스를 반복합니다. 백업 이름에는 문자, 숫자, 밑줄 및 하이픈만 사용할 수 있습니다. 백업 파일을 만들 때 .bak 파일 확장명을 포함하지 마십시오. 예를 들어, 3.13SecurestorageFalse와 같은 파일 이름은 마침표 때문에 거부됩니다.

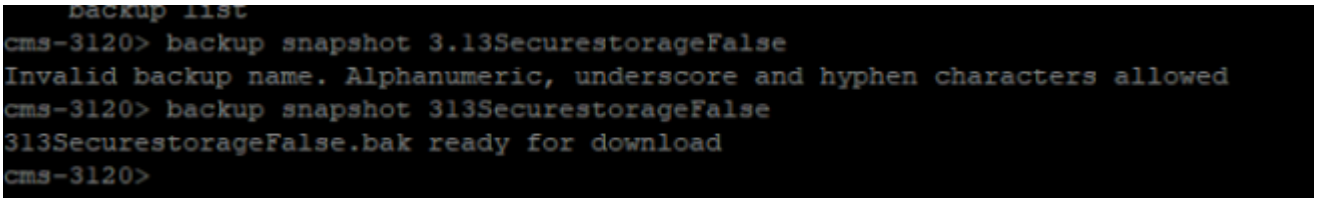


그림 4: 백업 스냅샷은 기간이 포함된 이름을 거부한 다음 영숫자 이름으로 성공합니다. 그러면 .bak 파일을 다운로드할 수 있습니다.



그림 5: Meeting Server SFTP 루트의 .bak 파일을 외부 저장소로 복사합니다. 서버에 복사본만 남겨두지 마십시오.

보안 스토리지가 활성화된 경우 백업 수행

secure_storage 보고서가 활성화된 경우 다음 절차를 수행합니다. 맞아. 암호화되지 않은 백업 파일은 다운로드할 수 없습니다.

1. 각 노드에 백업 스냅샷을 만듭니다. Secure Storage(보안 스토리지)가 활성화된 경우 서버는 14자 이상의 암호를 입력하라는 메시지를 표시합니다. 패스프레이즈는 문자, 숫자, 특수 문자, 기호 또는 공백을 포함할 수 있습니다.

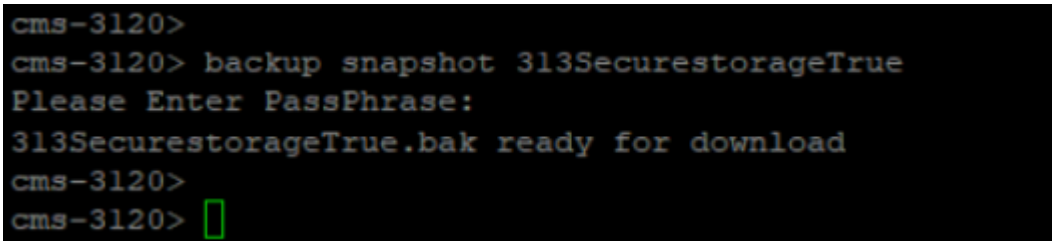


그림 6: Secure Storage가 활성화된 백업 스냅샷은 14자 이상의 암호를 묻는 프롬프트를 한 번 표시합니다. MMP는 확인을 요청하지 않습니다.

2. MMP는 확인을 위해 암호를 다시 입력하도록 요청하지 않습니다. 파일을 복원하기 위해 동일한 패스프레이즈가 필요하므로 패스프레이즈를 보호합니다. 간단한 패스프레이즈나 예제 패스프레이즈는 선택하지 마십시오.

3. backup list 명령에 내보내기 위해 암호화되지 않은 스냅샷이 표시되면 다운로드하기 전에 암호화합니다.

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

그림 7: 암호화 전 백업 목록 Encrypted(암호화됨) 열이 아니오이므로 파일을 다운로드할 수 없습니다.

4. 암호화되지 않은 백업을 다운로드하려고 하면 SFTP는 권한 거부 오류를 반환하고 backup encrypt 명령을 먼저 실행하도록 지시합니다.

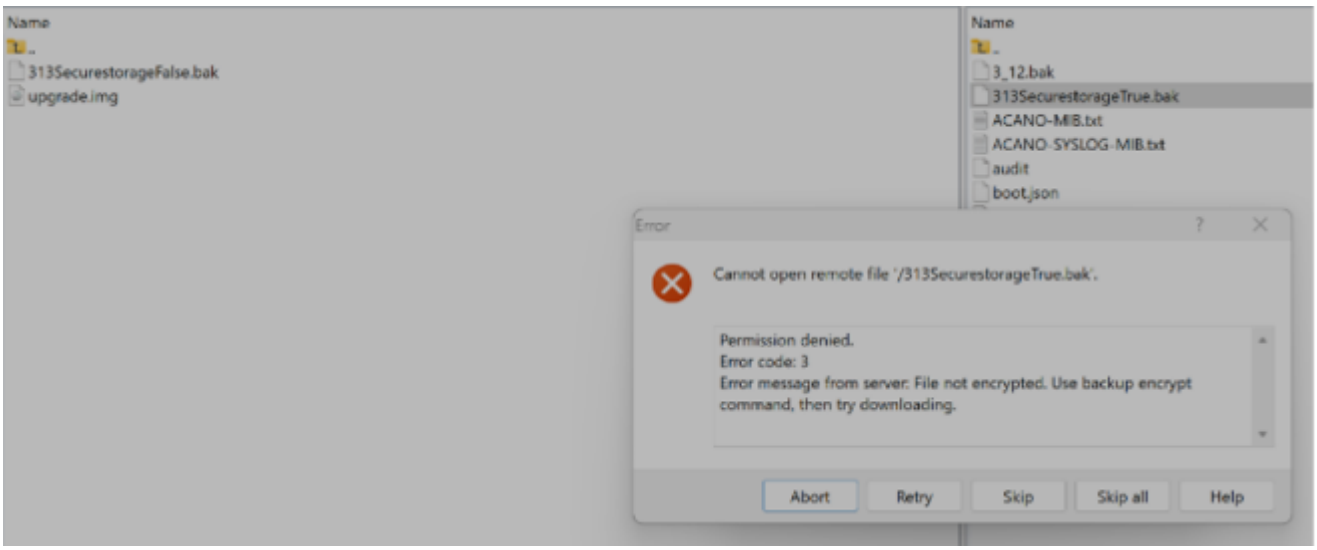


그림 8: SFTP는 보안 저장소가 활성화된 경우 암호화되지 않은 백업의 다운로드를 거부합니다. 서버 메시지는 백업 암호화를 실행하도록 지시합니다.

5. 백업 파일을 암호화하려면 backup encrypt 명령을 실행합니다.

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

그림 9: 스냅샷이 암호화된 후 백업 목록 Encrypted(암호화됨)는 yes이며 SFTP로 파일을 전송할 수 있습니다.

백업 목록에는 암호화 상태 및 원본 파일 이름이 표시됩니다. 클러스터의 각 노드에서 암호화된 파일만 전송합니다. 각 노드, 해당 파일 이름 및 관련 패스프레이즈의 구성된 레코드를 유지 관리합니다.

개인 키도 내보내야 하는 경우 먼저 각 키를 암호화합니다. 인증서 파일은 보안 저장소에 의해 차단되지 않으며 이 추가 단계 없이 복사할 수 있습니다.

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

서비스에서 현재 사용 중인 키를 덮어쓰는 대신 고유한 파일 이름을 사용합니다. 최소 14자 패스프레이즈 요구 사항은 여기에도 적용됩니다.

4.0 업그레이드 후 데이터 복원

1. 첫 번째 부팅 및 네트워크 복원 섹션에서 첫 번째 부팅 로그인 및 네트워크 복구 후, 해당 3.13.x 백업을 SFTP가 있는 노드에 복사하고 복원합니다.

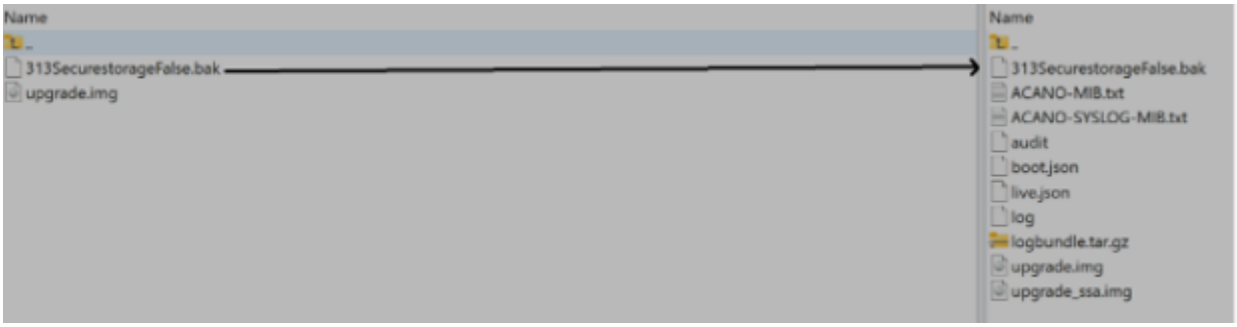


그림 10: 첫 번째 부팅 네트워크 복구 후 3.13.x .bak 파일을 SFTP를 사용하여 4.0 노드에 다시 복사합니다.

2. 파일이 있는지 확인합니다.

백업 목록

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

cms-3120>
```

그림 11: 롤백 전에 업로드된 스냅샷이 있는지 확인하는 4.0의 백업 목록

3. 스냅샷을 복원합니다. 클러스터 구축에서는 먼저 이전 데이터베이스 주 데이터베이스를 복원한 다음 복제본을 복원한 다음 연결된 노드를 복원합니다.

backup rollback name-of-the-backup-file



그림 12: 암호화되지 않은 스냅샷의 백업 롤백 Y에게 확인합니다. 노드가 백업을 추출하고 재부팅합니다.

4. 계속하려면 Y를 누릅니다. 백업을 추출하는 동안 노드가 재부팅됩니다. Secure Storage(보안 스토리지)가 활성화된 상태에서 백업을 수행한 경우 MMP에서 암호를 묻는 프롬프트가 표시됩니다. 올바른 암호가 수락된 후에만 재부팅이 진행됩니다.

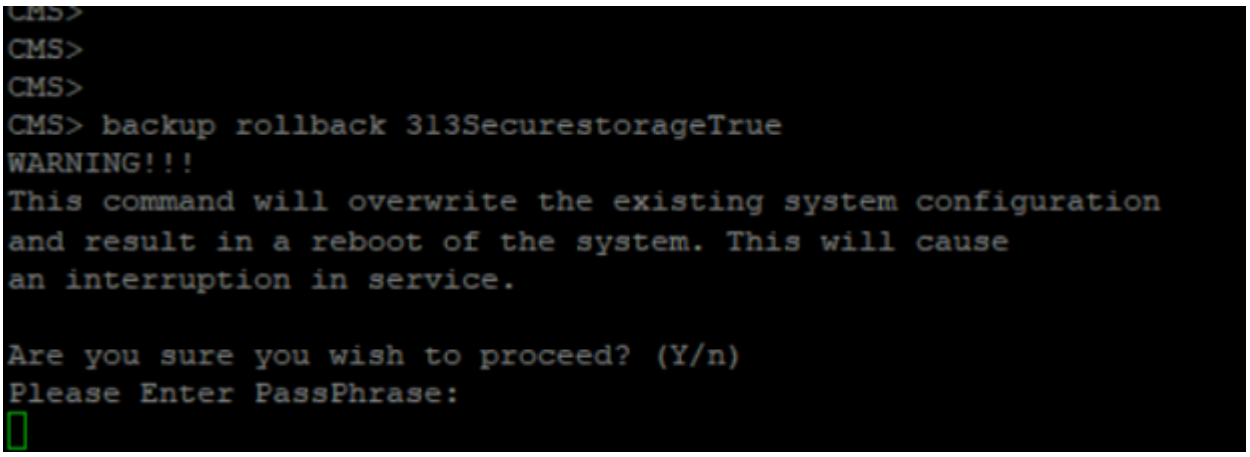


그림 13: 암호화된 스냅샷의 백업 롤백 Y가 끝나면 MMP는 백업이 생성될 때 사용된 패스프레이즈를 묻습니다.

⚠ 주의: 는 **backup rollback** 현재 컨피그레이션, 인증서, 개인 키 및 라이센스 파일을 덮어쓴 다음 서버를 재부팅합니다. 이 업그레이드를 위해 내보낸 3.13.x 백업과 함께만 사용하십시오.

---

5. 노드가 다시 온라인 상태가 되면 백업에서 MMP 자격 증명으로 로그인하고 각 필수 서비스 보고서가 활성화되어 실행 중인지 확인합니다(MMP에서 이를 활성으로 표시함). True)입니다.

일반 검사:

callbridge webbridge3 webadmin scheduler recorder streamer uploader meetingapps

6. 이 노드가 호스팅할 서비스에 대한 명령만 실행합니다.

복원 후 MeetingApps 비밀 키

Cisco Meeting Server 백업은 MeetingApps 비밀 키를 저장하지 않습니다. 백업 롤백이 완료되면 암호를 다시 생성하여 모든 웹 브리지 노드에 적용합니다. 이 단계를 건너뛰면 다른 서비스가 정상인 경우에도 파일 공유를 사용할 수 없습니다.

1. MeetingApps 노드에서 meetingapps gensecret 명령을 실행합니다.

2. 생성된 비밀을 비밀 저장소에 복사합니다. meetingapps gensecret을 실행할 때마다 이전 키가 무효화되므로 키를 한 번 생성하고 모든 웹 브리지에서 동일한 값을 다시 사용합니다.

3. 모든 웹 브리지 노드에서 다음 명령을 실행합니다.

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

마지막 명령은 웹 브리지 서비스가 실행 중이고 MeetingApps가 올바르게 구성되었음을 확인합니다. MeetingApps는 Meeting Server 2000에서 지원되지 않으며 Meeting Server 2000이 포함된 클러스터에서는 파일 공유를 사용할 수 없습니다. 이러한 구축에서는 이 단계를 적용할 수 없습니다.

첫 번째 부팅 및 네트워크 복원

4.0 upgrade 명령은 진행되기 전에 경고 배너를 표시합니다. 메시지를 주의 깊게 검토하고 전제 조건이 불완전한 경우 n으로 중단합니다. Y를 계속하면 노드가 재부팅되고 SSH 세션이 연결 해제되며 나머지 단계는 콘솔에서 완료해야 합니다.

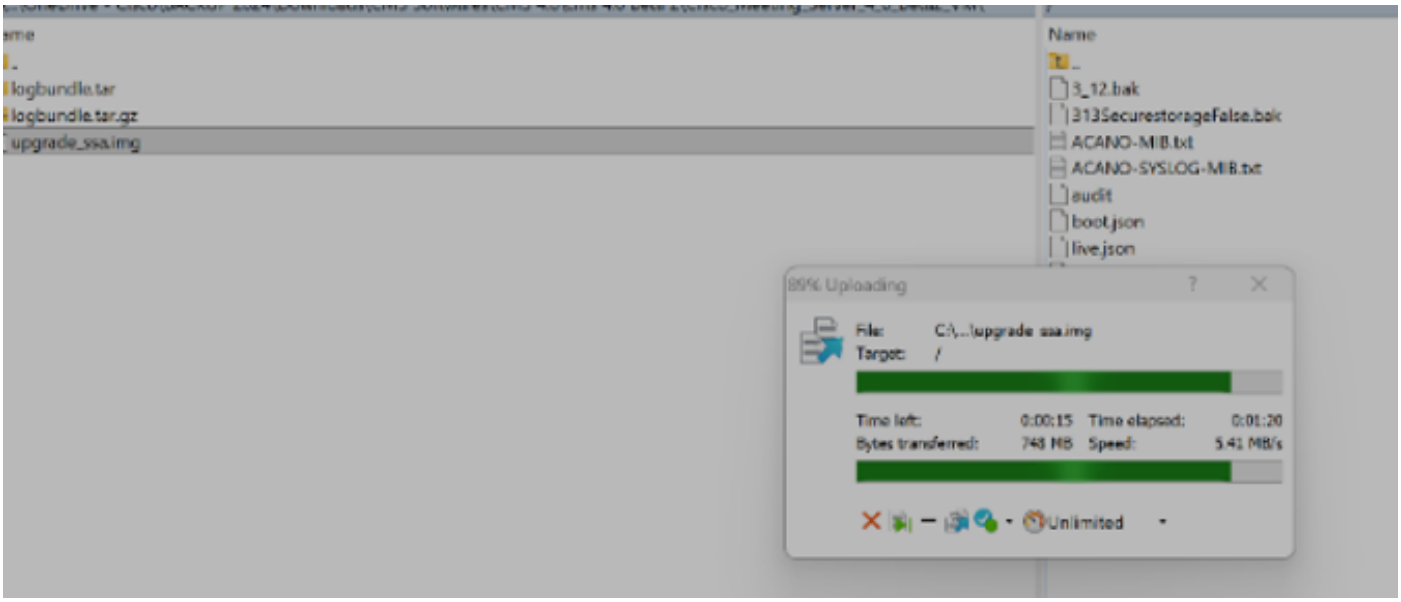


그림 14: 4.0 업그레이드 이미지를 Meeting Server SFTP 루트 디렉터리에 업로드합니다. 업그레이드 이미지 파일 이름은 cisco.com에서 다운로드한 패키지에 따라 달라질 수 있습니다.

```
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...
```

그림 15: upgrade 명령은 이미지 서명을 확인하고 프로세스를 시작합니다. 이 시점에서 생성되는 자동 백업에 의존하지 마십시오.

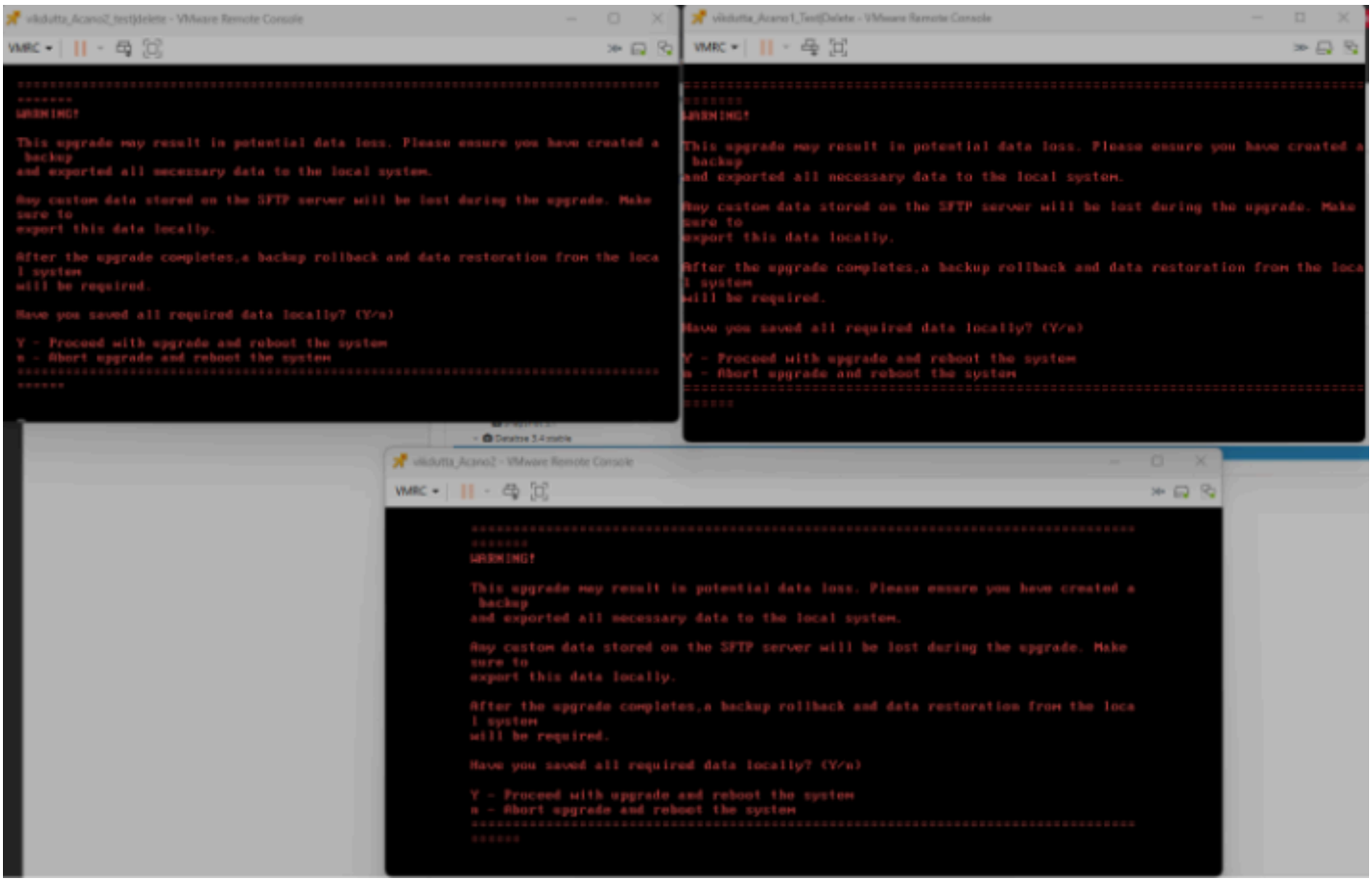


그림 16: 3노드 클러스터의 빨간색 MMP 경고입니다. 동일한 배너가 단일 노드에 나타납니다. 백업 및 사용자 지정 데이터가 서버에 없는 경우 n을 눌러 중단합니다. 계속 진행하여 재부팅하려면 Y만 누릅니다.

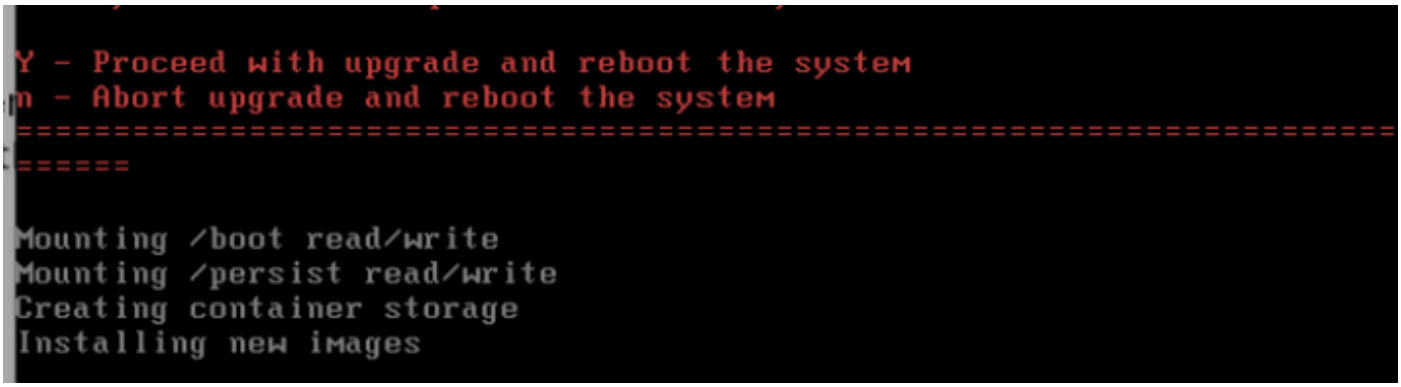


그림 17: Y를 입력하면 노드가 스토리지를 마운트하고 4.0 이미지를 설치합니다. SSH 세션 시간이 초과됩니다. 하이퍼바이저 콘솔에서 계속합니다.

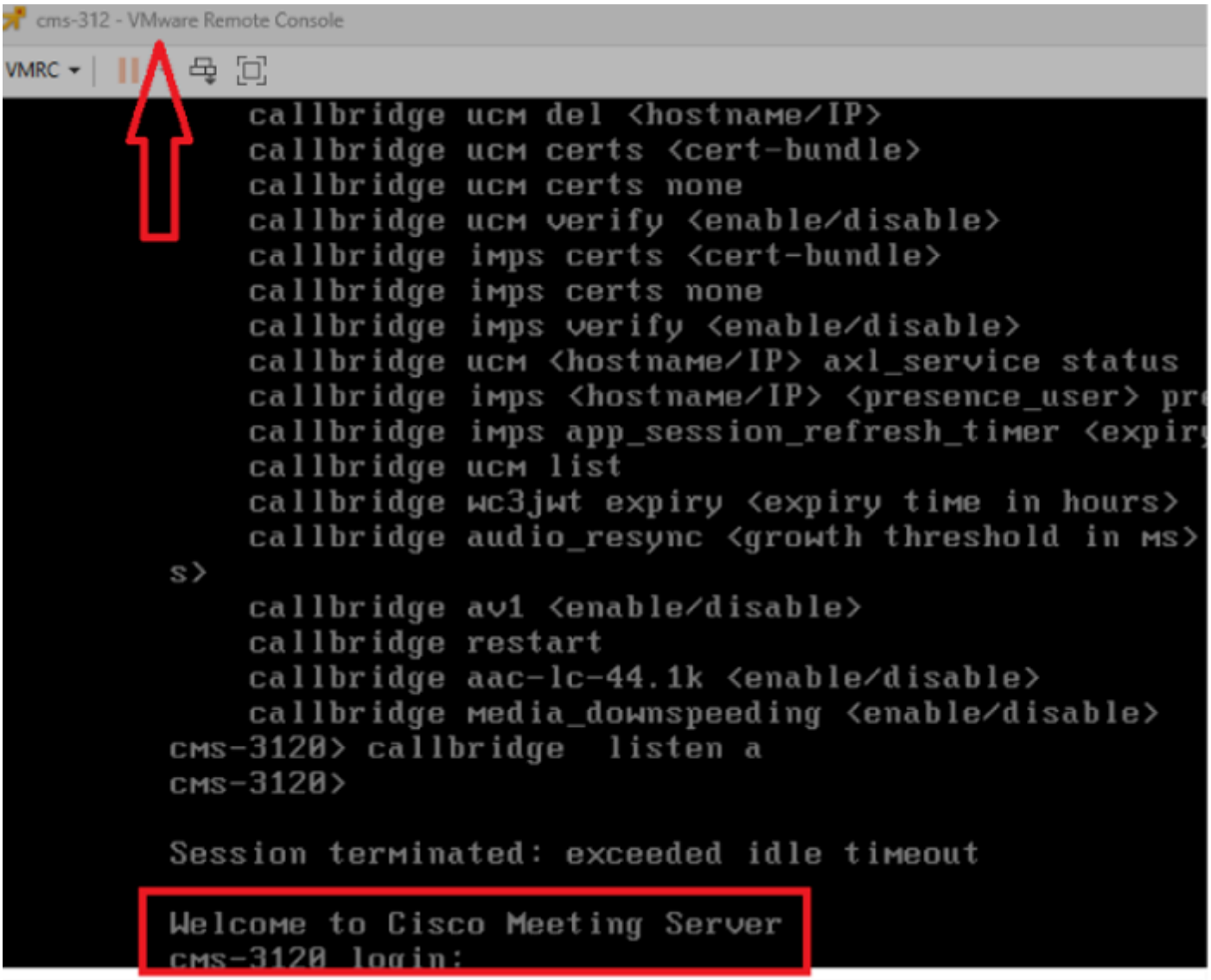


그림 18: SSH 삭제 후 VM 또는 CIMC 콘솔을 사용합니다. 4.0 이미지가 준비되면 첫 번째 부팅 로그인 프롬프트가 나타납니다.

1. 첫 번째 부팅 MMP 계정(사용자 이름 admin 및 비밀번호 없음)으로 로그인한 다음 프롬프트가 표시되면 새 MMP 비밀번호를 설정합니다. 백업 롤백은 이 비밀번호를 백업에 저장된 비밀번호로 대체합니다.

2. 업그레이드 전 요구 사항 섹션에 설명된 메모에서 네트워크 구성을 다시 적용합니다.

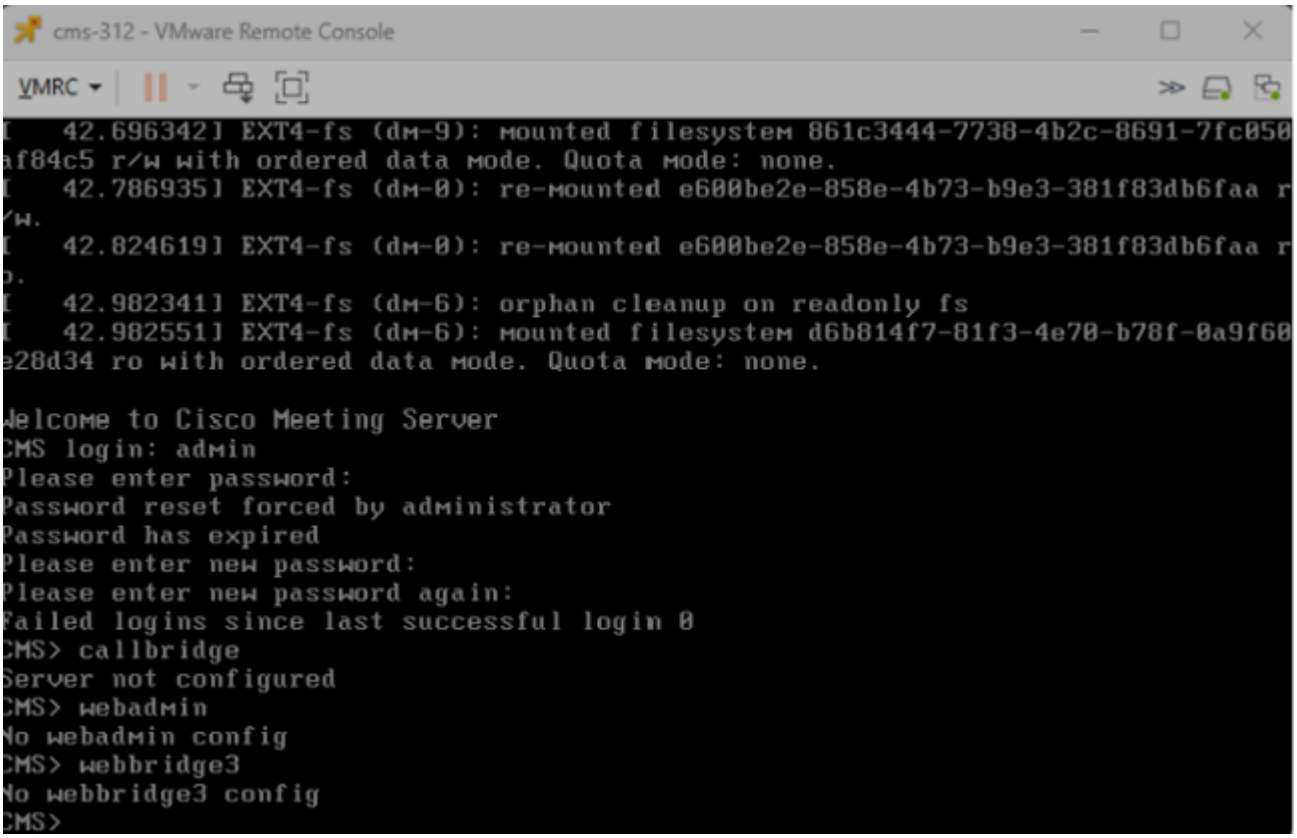


그림 19: 첫 번째 부팅 MMP 로그인

이전 암호가 더 이상 유효하지 않습니다. 새 비밀번호를 설정하면 webadmin 및 webbridge3과 같은 서비스는 백업이 복원될 때까지 구성되지 않은 것으로 나타납니다.

3. 다음 명령을 실행합니다.

ipv4 interface add address/prefix-length gateway

예를 들면 다음과 같습니다.

ipv4 a add 192.0.2.10/24 192.0.2.1

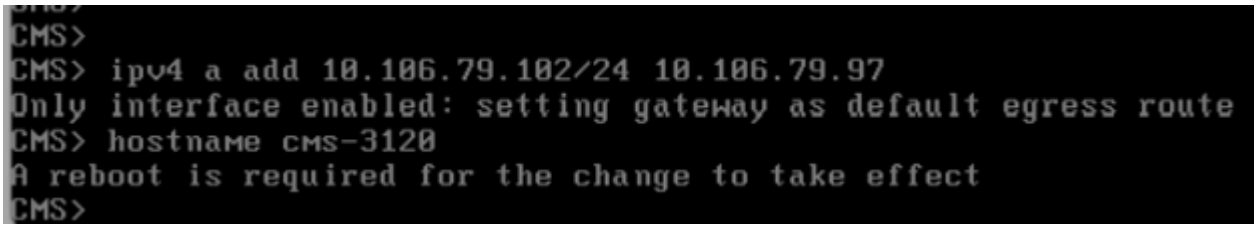


그림 20: 콘솔에서 IPv4 다시 적용

주소를 할당한 후에는 재부팅해야 합니다. 스크린샷에 표시된 주소는 예시용으로만 사용됩니다.

4. 주소가 할당된 후 재부팅합니다. 시스템이 다시 온라인 상태가 되면 백업 SFTP 업로드를 계속하고 4.0 업그레이드 후 데이터 복원 섹션에 설명된 복원 단계를 진행합니다.

참고: DHCP 예약이 구성된 경우 재부팅 후 원래 주소를 이미 할당할 수 있습니다. 관리 워크스테이션에서 SFTP 세션을 시작하기 전에 와(과) 주소를 **ipv4 a** 확인하십시오.

Cisco Meeting Server 4.0에서는 보안 스토리지를 지원하는 플랫폼에서 보안 스토리지가 기본적으로 활성화됩니다. MMP는 업그레이드 후에 더 이상 secure_storage를 토글로서 노출할 수 없습니다 .



그림 21: 이 4.0 이미지에서는 Secure Storage가 기본적으로 활성화되어 있으므로 secure_storage가 인식되는 명령이 아닙니다.

version 명령을 사용하여 릴리스를 확인합니다.

업그레이드 시나리오

이 장에서는 다양한 업그레이드 시나리오를 다룹니다. 3.13.x로 단계 업그레이드를 완료합니다. 구축 유형을 식별하고 그에 따라 시나리오를 선택합니다. 사용자 환경과 일치하는 절차만 따르며 클러스터 및 단일 노드 구축의 단계를 결합하지 않습니다.

먼저 3.13.x로 지원되는 단계 업그레이드를 완료합니다. 그런 다음 아래에서 정확히 하나의 시나리오를 선택합니다. 단일 노드 및 데이터베이스 클러스터 절차는 결합하지 마십시오.

- 시나리오 1: 단일 노드, 비활성화됨 또는 사용 불가능, VM, Small, Medium 및 Meeting Server 2000
- 시나리오 2: 단일 노드, Enabled(활성화됨), VM, Small(소규모) 및 Medium(중간)만 해당
- 시나리오 3: 데이터베이스 클러스터, 사용 안 함 또는 사용 불가능, VM, Small, Medium 및 Meeting Server 2000
- 시나리오 4: 데이터베이스 클러스터, 활성화됨, VM, 소형 및 중형 전용

Meeting Server 2000에서는 보안 저장소 사용 시나리오를 지원하지 않습니다. 해당 플랫폼의 경우 시나리오 1 또는 3을 적절히 사용합니다.

시나리오 1 - 보안 스토리지가 비활성화되었거나 사용할 수 없는 단일 노드

보안 스토리지가 비활성화된 독립형 서버 또는 보안 스토리지를 사용할 수 없는 Meeting Server 2000에 대해 이 절차를 사용합니다. 소스 릴리스는 3.11.x 이상이 될 수 있지만 4.0으로 업그레이드하기 전에 노드가 3.13.x에 있어야 합니다.

1. 3.13.x로 1단계 업그레이드 지원되는 경로를 따릅니다(예: 3.11.x → 3.12.x → 3.13.x). 각 홉 후 Validate Server Health Before Creating Backups(백업 생성 전 서버 상태 검증) 섹션에 설명된 대로 웹 관리에서 버전을 확인하고 결함 조건이 명확한지 확인합니다.

2. 보안 저장소 상태를 확인합니다. secure_storage 명령을 실행하고 보안 스토리지가 활성화되지 않았는지 확인합니다. Meeting Server 2000에서 명령을 건너뜁니다.

3. 보안 저장소가 비활성화되거나 사용할 수 없을 때 백업 수행 섹션에서 설명한 대로 3.13.x 백업 파일을 만들고 내보냅니다. 또한 업그레이드 전 요구 사항 섹션에 설명된 대로 맞춤형 SFTP 콘텐츠 및 로그 번들을 내보냅니다.

4. Cisco.com에서 4.0 소프트웨어 이미지를 다운로드하고 압축을 푼 다음 upgrade.img를 SFTP를 통해 노드에 복사합니다.

5. 다음 명령을 사용하여 업그레이드를 시작합니다.

```
upgrade upgrade.img
```

6. 경고 배너를 읽습니다. 모든 필수 구성 요소가 완료된 후에만 Y를 누릅니다. 6. 업그레이드 후 첫 번째 부팅 및 네트워크 복원 섹션에 설명된 대로 노드를 구성한 다음 4.0 업그레이드 후 데이터 복원 섹션을 사용하여 백업을 복원합니다.

시나리오 2 - 보안 스토리지가 활성화된 단일 노드

독립형 VM, Meeting Server Small 또는 보안 스토리지가 활성화된 Meeting Server Medium에 이 절차를 사용합니다. Meeting Server 2000에는 적용되지 않습니다.

서버에서 파일을 전송하기 전에 암호화되지 않은 개인 키와 암호화되지 않은 백업 파일은 전송할 수 없습니다. 인증서 파일은 차단되지 않습니다.

1. 릴리스를 건너뛰지 않고 지원되는 경로를 통해 3.13.x로 업그레이드합니다. 각 홉이 끝나면 Validate Server Health Before Creating Backups(백업 생성 전 서버 상태 검증) 섹션에서 버전 및

Fault(오류) 조건이 지워지는지 확인합니다.

2. secure_storage를 실행하고 출력에 Enabled가 표시되는지 확인합니다. 맞아.

3. [보안 저장소가 활성화된 경우 백업 수행] 섹션을 사용하여 암호화된 3.13.x 백업을 만들고 내보냅니다. 암호를 비밀 저장소에 저장하십시오. 또한 맞춤형 SFTP 콘텐츠 및 로그 번들(업그레이드 전 요구 사항 섹션)도 내보냅니다.

4. upgrade.img를 노드에 복사하고 업그레이드를 실행합니다.

```
upgrade upgrade.img
```

5. 경고 배너를 읽고 Y를 눌러 필수 구성 요소가 완료된 경우에만 계속합니다.

6. 콘솔에서 네트워크를 복구합니다(첫 번째 부팅 및 네트워크 복원 섹션). 그런 다음 암호화된 백업을 암호로 복원합니다(4.0 업그레이드 후 데이터 복원 섹션). 6. MeetingApps를 사용 중인 경우 새 MeetingApps 암호(복원 후 MeetingApps 암호 섹션)를 적용합니다.

보안 저장소는 Meeting Server 4.0에서 기본적으로 사용됩니다. 복원 후 개인 키와 백업 파일을 암호화된 데이터로 계속 처리합니다.

시나리오 3 - 보안 저장소가 비활성화된 데이터베이스 클러스터

Meeting Server 2000을 포함하는 클러스터를 포함하는 보안 저장소가 비활성화된 데이터베이스 클러스터에 대해 이 절차를 사용합니다. 버전 3.5부터 소프트웨어를 업그레이드하기 전에 데이터베이스 클러스터를 해제해야 합니다. 먼저, 모든 노드를 3.13.x로 단계별로 업그레이드합니다.

클러스터 세부 정보 기록 및 모든 노드 백업

1. 모든 노드에서 secure_storage를 실행합니다. Meeting Server 2000 노드에서 명령을 사용할 수 없는 것으로 처리합니다.

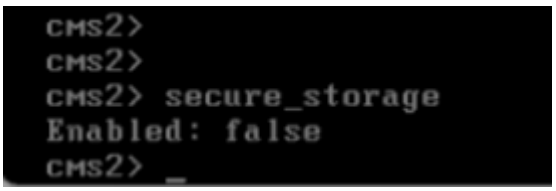


그림 22: 암호화되지 않은 백업을 사용하기 전에 모든 클러스터 노드에서 보안 저장소가 비활성화되어 있는지 확인합니다. Meeting

Server 2000 노드를 사용할 수 없는 경우 해당 명령을 건너뜁니다.

2. 4.0으로 업그레이드한 후 먼저 복원해야 하는 현재 데이터베이스 주 노드를 기록합니다. 복제본이 동기화 중이고 클러스터 상태가 정상인지 확인합니다.

```
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)
```

그림 23: 현재 기본 복제본을 기록하고 복제본이 동기화 중인지 확인합니다.

3. 사용 중인 모든 통화 유형이 작동 중이고 모든 노드에서 장애 상태가 명확한지 확인합니다(백업을 생성하기 전 서버 상태 검증 섹션).

4. [보안 저장소가 비활성화되거나 사용할 수 없을 때 백업 수행] 섹션을 사용하여 모든 노드의 백업을 생성합니다. 클러스터를 분리하기 전에 각 파일의 이름을 해당 노드에 명확하게 매핑하고 모든 백업을 외부 스토리지로 전송합니다.

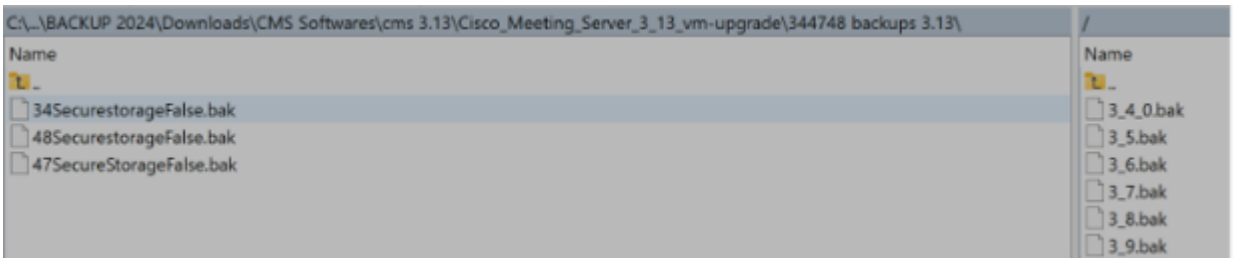


그림 24: 세 가지 예제 노드 백업은 모두 각 파일이 해당 노드에 매핑되도록 이름이 지정된 외부 스토리지를 저장합니다.

클러스터 분리

이 순서로 노드를 제거합니다. 1차 이미지를 마지막까지 유지:

- 연결된(비코어) Meeting Server 노드

- 복제본 데이터베이스 노드
- 기본 데이터베이스 노드

각 노드에서 제거 명령을 실행하고 Y를 누릅니다. 모든 노드가 클러스터를 떠났다고 보고할 때까지 4.0 업그레이드를 계속하지 마십시오. 클러스터 멤버십을 제거하면 해당 노드의 로컬 데이터베이스가 그대로 유지됩니다.

database cluster remove

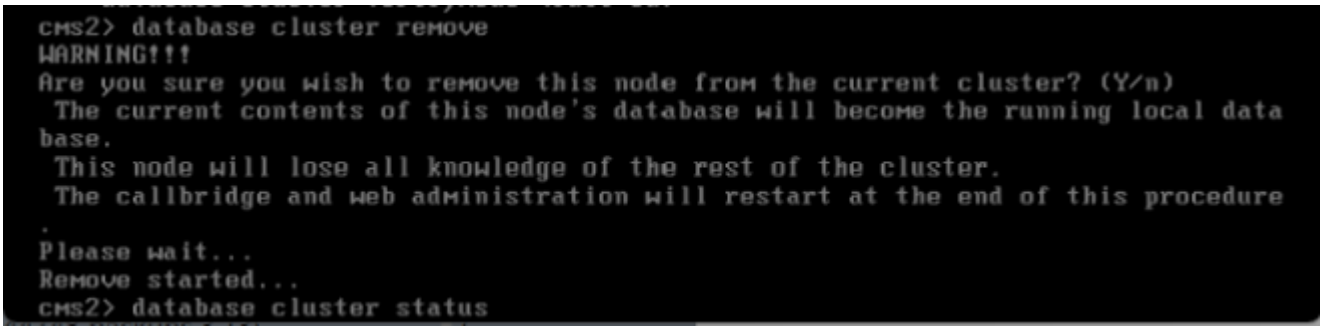


그림 25: 복제본에서 Y를 확인하여 클러스터 멤버십을 제거합니다. 노드의 로컬 데이터베이스는 그대로 유지됩니다.

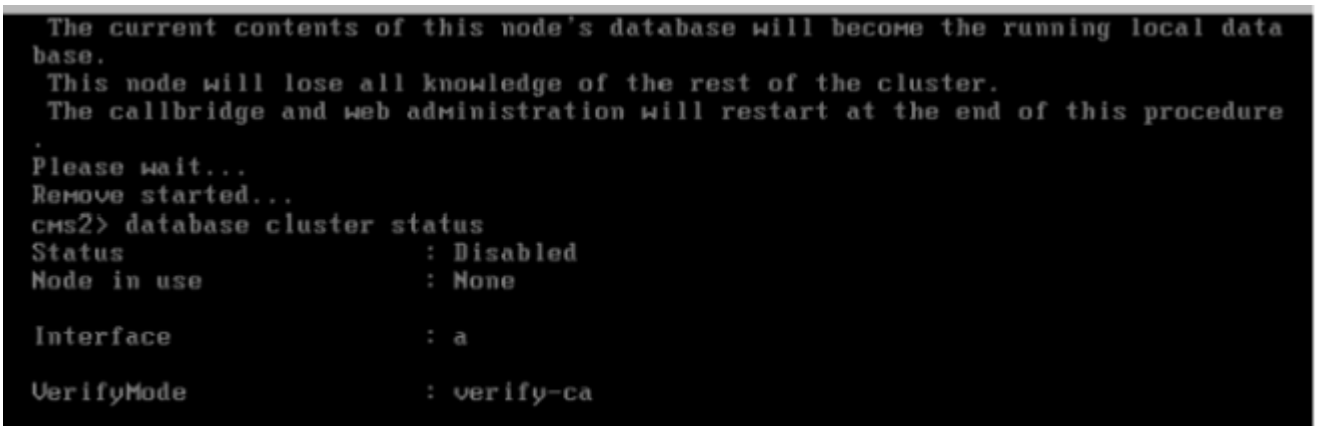


그림 26: 제거한 후 해당 노드에서 클러스터 상태가 Disabled(비활성화됨)이고 사용 중인 노드가 None(없음)인지 확인합니다.

```
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)
```

그림 27: 복제본을 제거한 후 이전의 기본 노드가 클러스터에 남아 있는 유일한 노드입니다. 마지막으로 제거합니다.

```
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> _
```

그림 28: 이전의 기본 를 제거한 후 명령이 Success(성공) 및 cluster status(클러스터 상태)를 Disabled(비활성화됨)로 보고하는지 확인합니다.

노드 업그레이드 및 복원

1. 노드가 해체되면 노드는 독립형이며 동시에 업그레이드할 수 있습니다. 각 노드에서 SFTP를 통해 upgrade.img를 복사하고 upgrade 명령을 실행합니다.

upgrade upgrade.img

2. 콘솔에서 각 노드의 네트워크 주소 지정을 복구합니다(첫 번째 부팅 및 네트워크 복원 섹션).

3. 각 노드의 고유한 3.13.x 백업을 해당 노드로 다시 복사합니다. 먼저 이전의 운영 노드를 복구한 다음 복제본을 복구한 다음 연결된 노드를 복구합니다. 4.0 업그레이드 후 데이터 복원 섹션을 사용합니다. 백업을 복원하면 데이터베이스 클러스터 멤버십이 다시 설정됩니다.

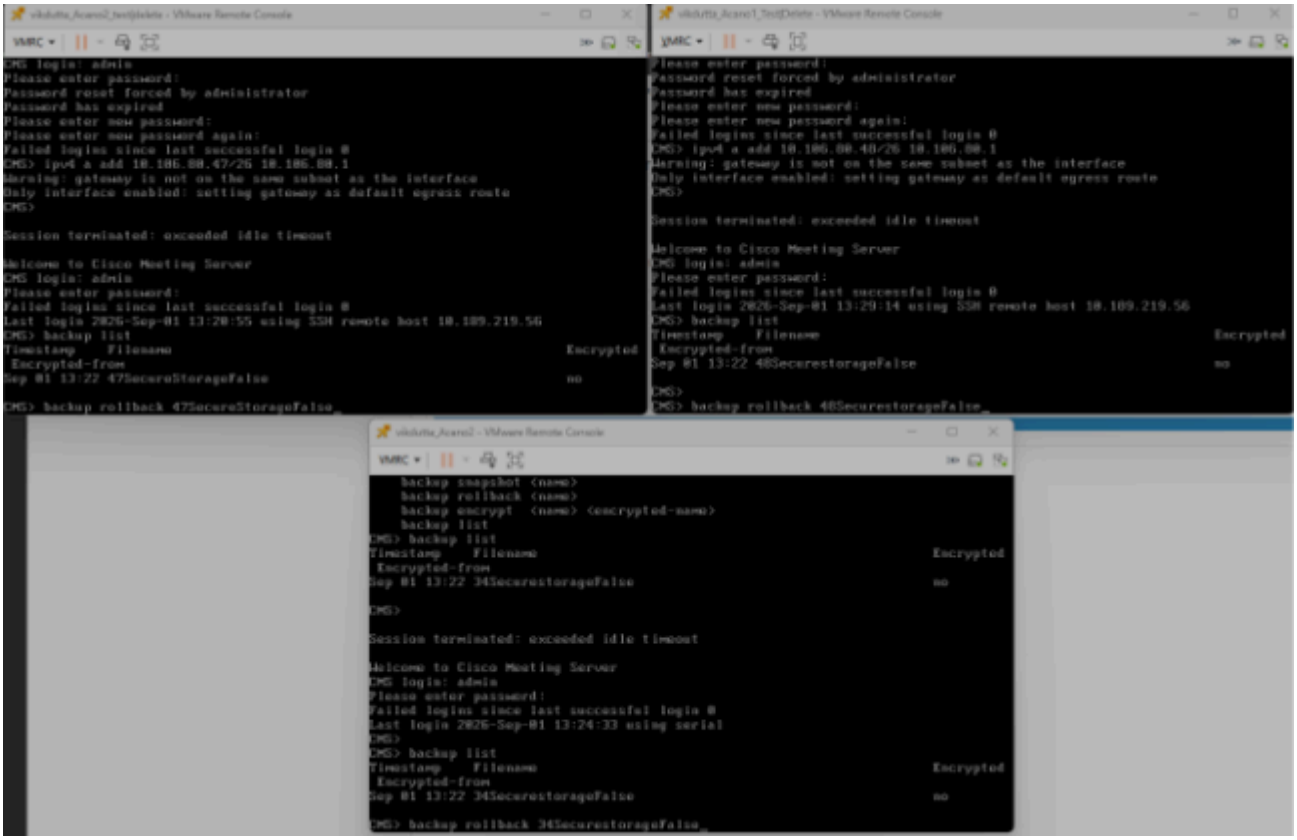


그림 29: 각 노드의 고유한 스냅샷을 복원합니다. 이전의 운영 스토리지로 시작한 다음 복제본을 복구합니다. 파일 이름의 예는 해당 노드를 식별합니다.

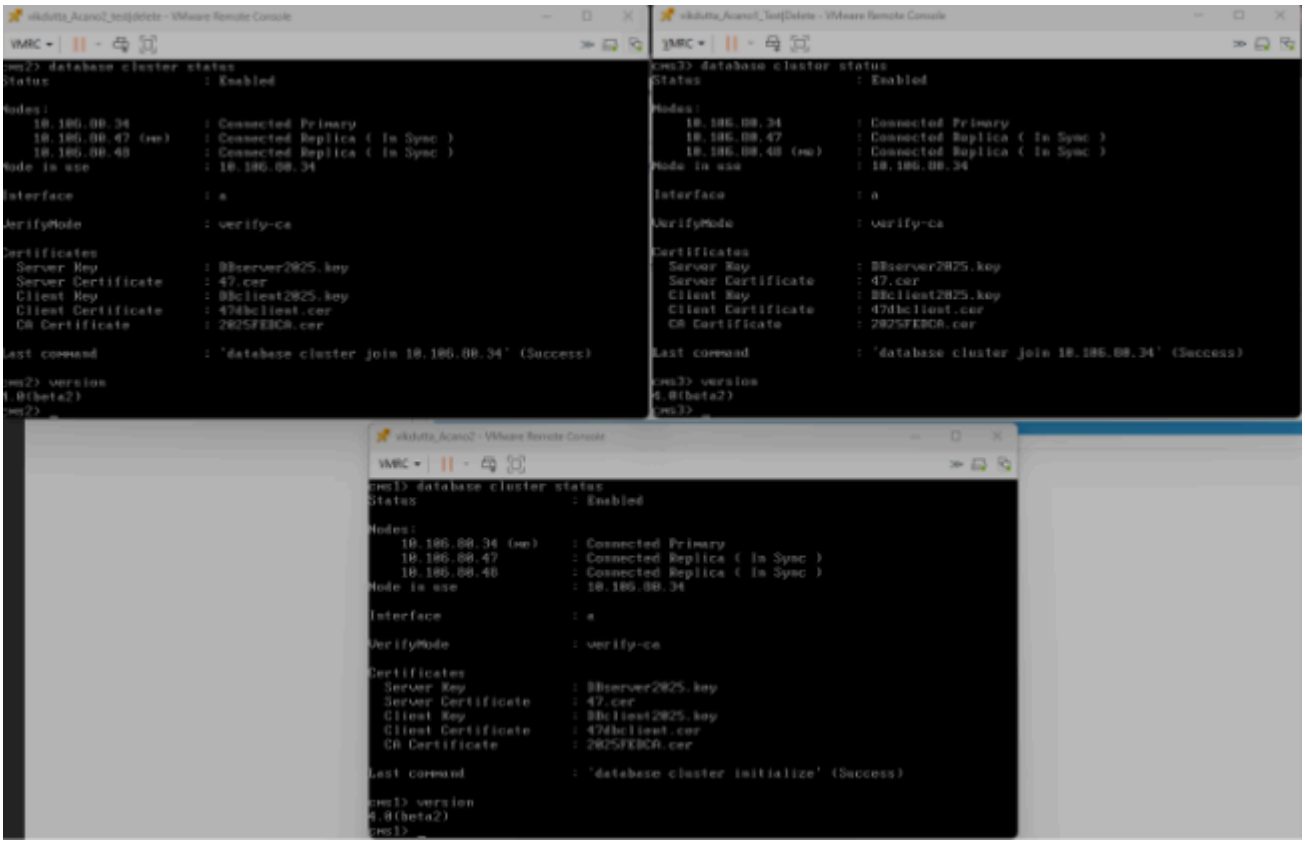


그림 30: Meeting Server 4.0에서 복구한 후 클러스터가 Enabled(활성화됨)이고, 동일한 기본 복제본이 In Sync(동기화 중)인지 확인합니다.

참고: 이 복원 후에 통화 브리지 클러스터 연결이 나타나지 않으면 이전 기본 에서만 를 **database cluster upgrade_schema** 실행한 다음 통화 브리지 상태를 다시 확인하십시오.

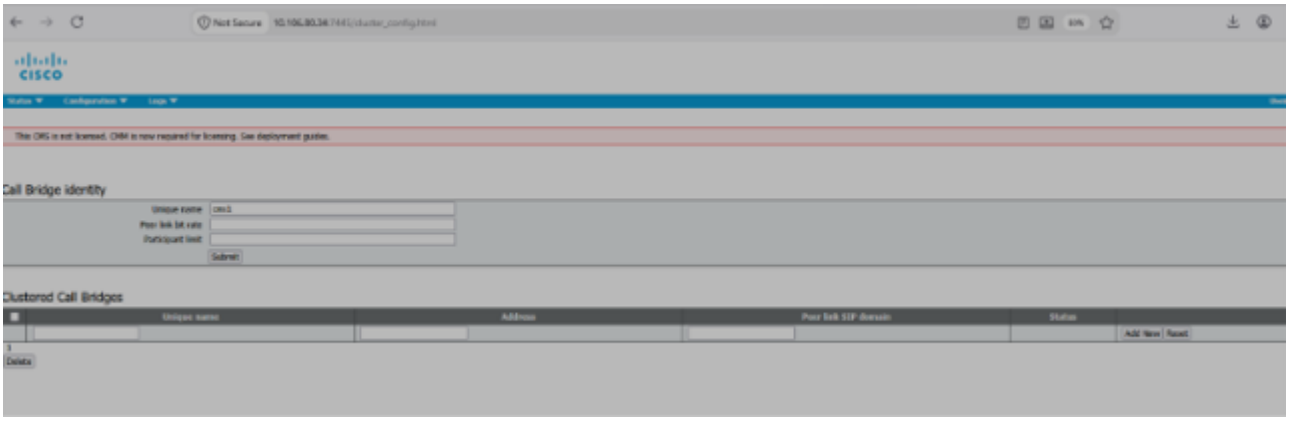


그림 31: 스키마 업그레이드 전에 이 예에서는 클러스터된 통화 브리지가 비어 있는 동안 실행되는 데이터베이스 클러스터를 보여 줍니다.

database cluster upgrade_schema

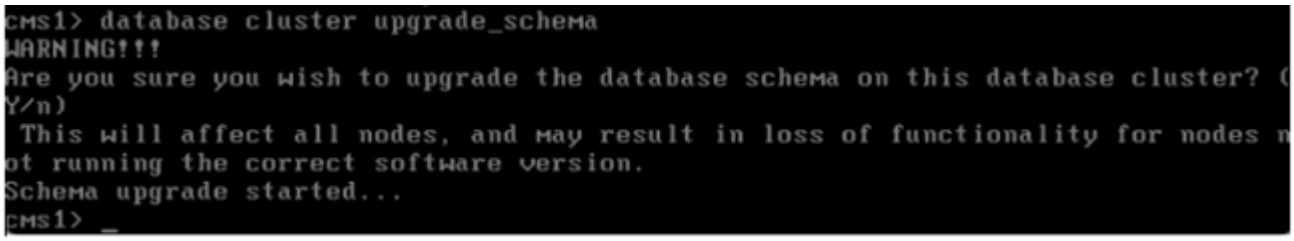


그림 32: 이전 기본 의 경우, 이 분리된 클러스터 업그레이드 후 Call Bridge 클러스터 연결이 실패한 경우에만 Y를 확인합니다.

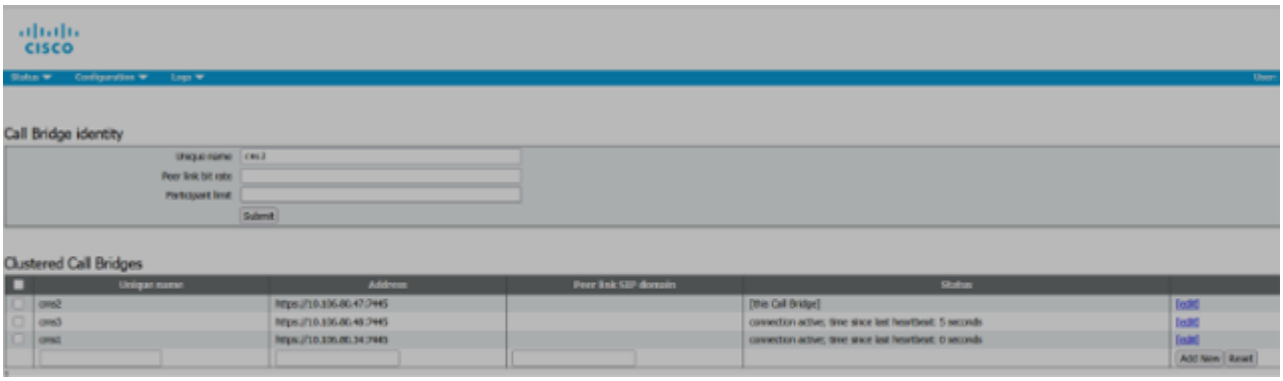


그림 33: 스키마 업그레이드 후 각 통화 브리지 피어에 활성 연결이 표시되는지 확인합니다.

4. 모든 웹 브리지의 MeetingApps Secret Key After Restore(복원 후 MeetingApps 비밀 키) 섹션에서 MeetingApps 비밀 절차를 완료한 다음 업그레이드 후 검증 섹션을 사용하여 배포를 검증합니다.

시나리오 4 - 보안 스토리지가 활성화된 데이터베이스 클러스터

노드에서 보안 스토리지가 활성화된 VM, Meeting Server Small 또는 Meeting Server Medium의 데이터베이스 클러스터에 대해 이 절차를 사용합니다. Meeting Server 2000에는 적용되지 않습니다. 먼저, 모든 노드를 3.13.x로 단계별로 업그레이드합니다.

클러스터 세부 정보 기록 및 암호화된 백업 생성

1. 모든 노드에서 secure_storage를 실행하고 Enabled를 확인합니다. 맞아.

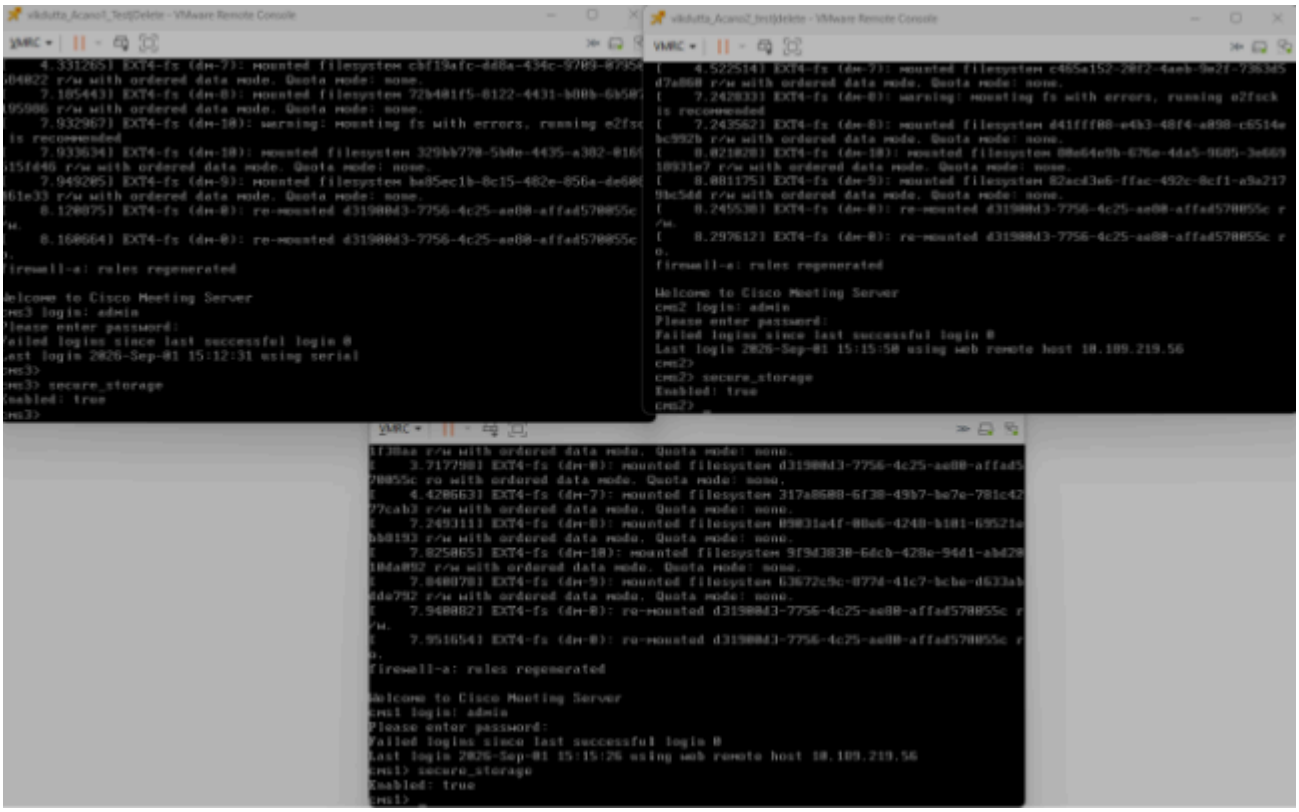


그림 34: 예시된 3노드 클러스터의 경우 Secure Storage(보안 스토리지)에 Enabled(활성화됨)가 표시되는지 확인합니다. 업그레이드 전에 모든 노드에서 True입니다.

2. 현재 데이터베이스를 기본 데이터베이스에 기록하고 복제본이 동기화 중인지 확인합니다.

```
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)
```

그림 35: 업그레이드 전의 데이터베이스 클러스터 상태입니다. 기본 복제본을 기록하고 복제본이 동기화 중인지 확인합니다.

3. 모든 노드에서 사용 중인 모든 통화 유형 및 오류 조건이 명확한지 확인합니다(백업을 생성하기 전에 서버 상태 검증 섹션).

4. 보안 저장소가 활성화된 경우 백업 수행 섹션을 사용하여 모든 노드의 암호화된 백업을 생성합니다. 각 파일에 대해 고유한 패스프레이즈를 할당 및 기록하거나 문서화된 패스프레이즈 정책을 사용합니다. 클러스터를 분리하기 전에 서버에서 암호화된 파일만 전송합니다.

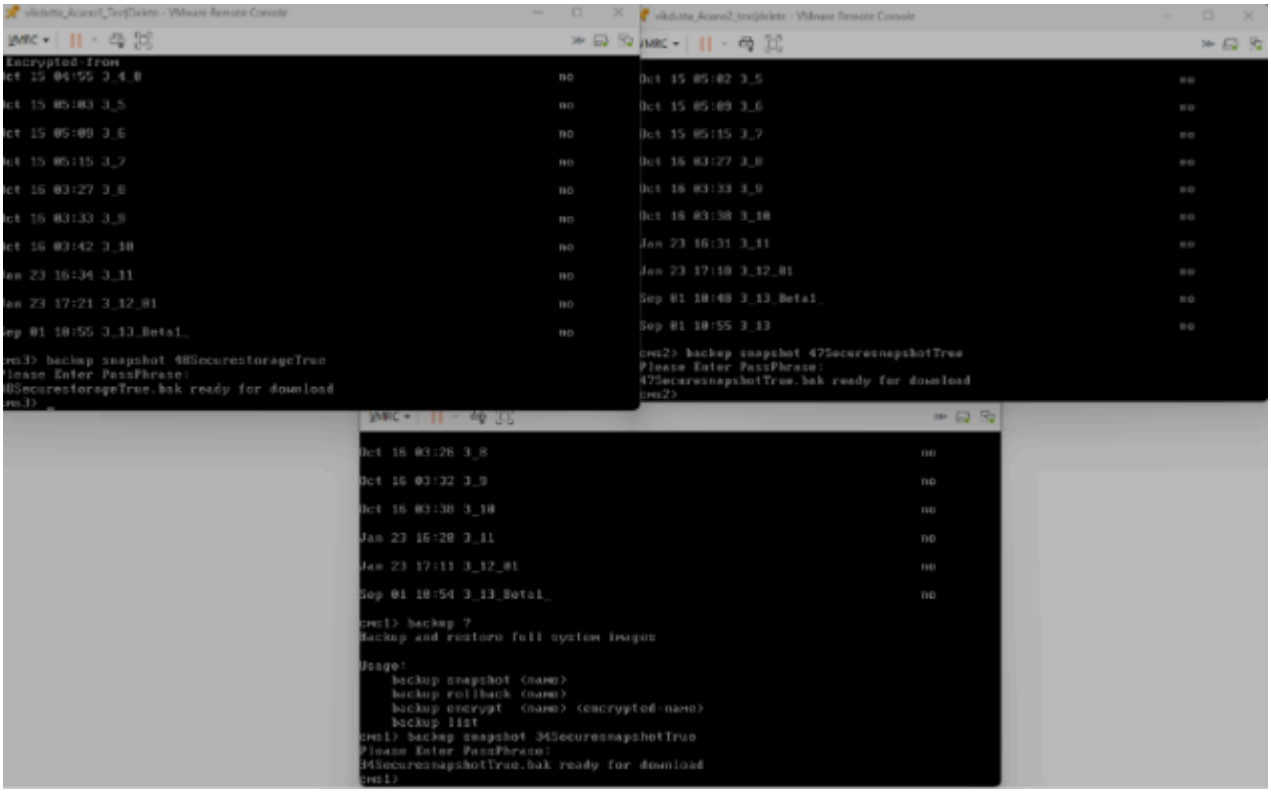


그림 36: 각 노드의 암호화된 백업 스냅샷. 이 예에서는 암호 프롬프트를 표시한 다음 각 .bak 파일을 다운로드할 준비가 된 것을 보여줍니다.

분리, 업그레이드 및 복원

시나리오 3에 설명된 대로 클러스터를 다음 순서로 분리합니다. 연결된 노드, 복제본 및 기본 마지막 데이터베이스 클러스터를 사용하여 모든 노드가 클러스터를 떠났는지 확인합니다.

독립형 노드를 병렬로 업그레이드합니다. 콘솔에서 네트워크 주소 지정을 복구합니다(첫 번째 부팅 및 네트워크 복원 섹션).

각 노드의 고유한 암호화 백업을 업로드합니다. 롤백 전에 업로드된 스냅샷이 백업 목록에 Encrypted(암호화됨)로 표시되는지 확인합니다. 예. 이전의 운영 노드를 먼저 복구한 다음 복제본 및 연결된 노드를 복구합니다. 아래의 backup rollback 명령을 사용하고 Y를 확인한 다음 메시지가 표시되면 백업 암호를 입력합니다. 패스프레이즈가 승인되면 노드가 재부팅됩니다. 각 노드에 대해 반복합니다.

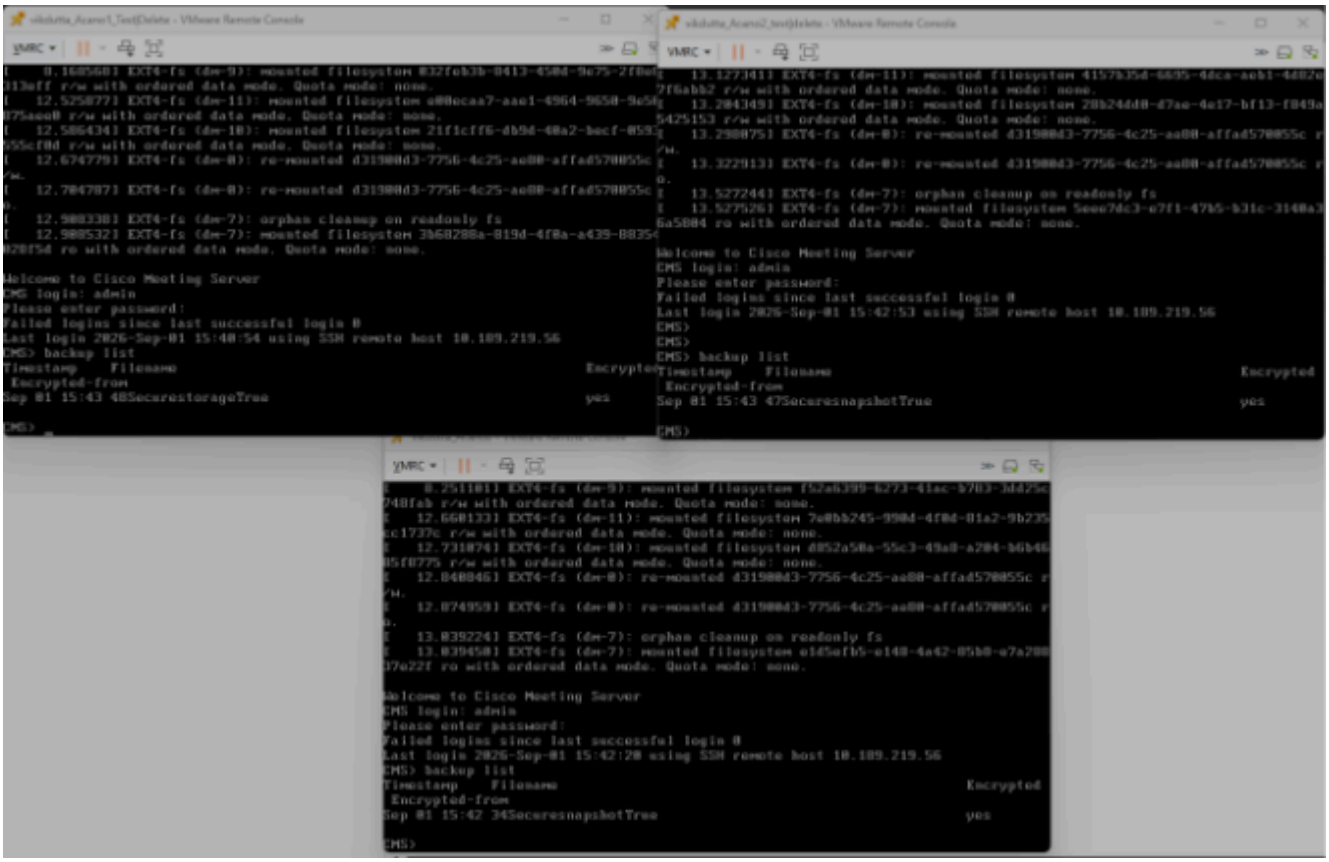


그림 37: 첫 4.0 부팅 후 업로드된 스냅샷은 백업 목록에 Encrypted(암호화됨)로 표시되어야 합니다. 예. 롤백할 준비가 되어 있습니다.

backup rollback encrypted-filename

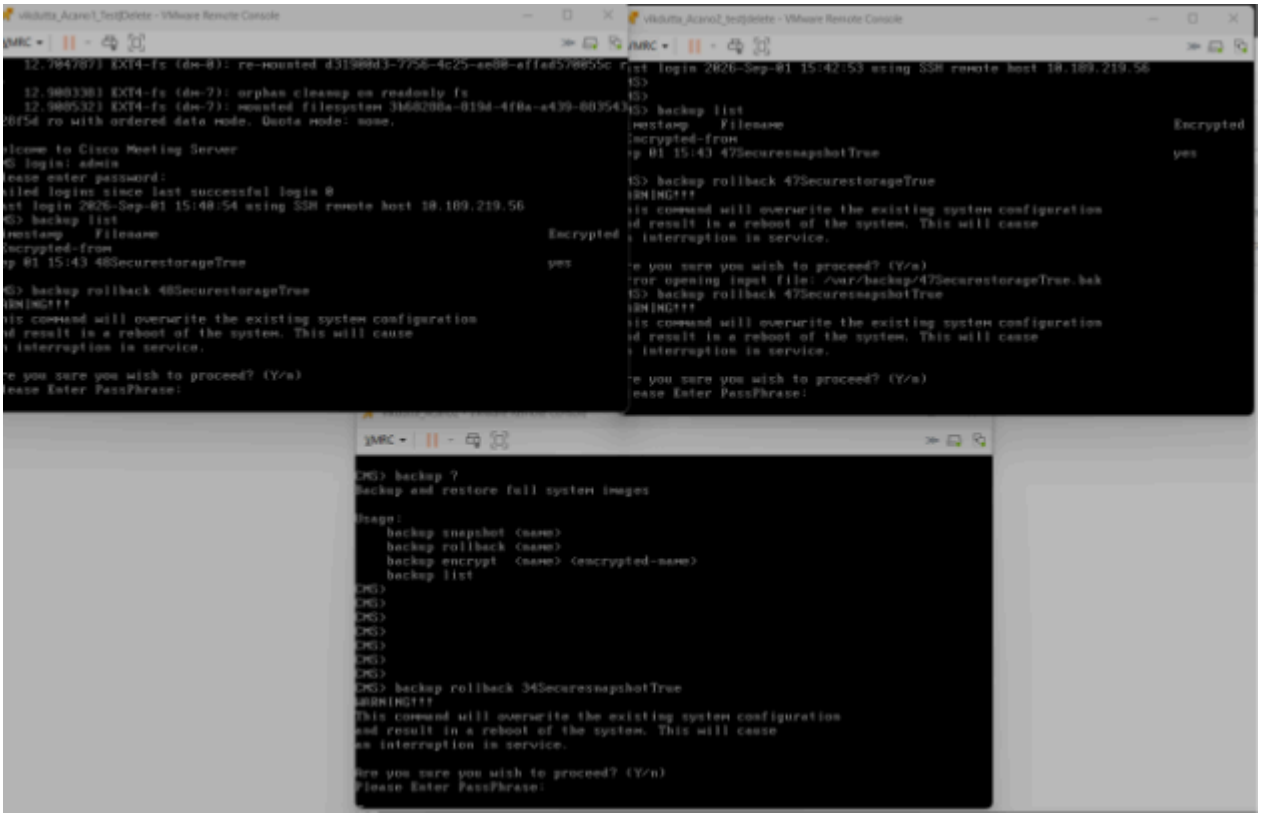


그림 38: Y를 확인하고 암호를 입력한 다음 이전 주 서버를 먼저 복원합니다.

참고: 이 복원 후에 통화 브리지 클러스터 연결이 나타나지 않으면 이전 기본 에서만 를 **database cluster upgrade_schema** 실행한 다음 통화 브리지 상태를 다시 확인하십시오.

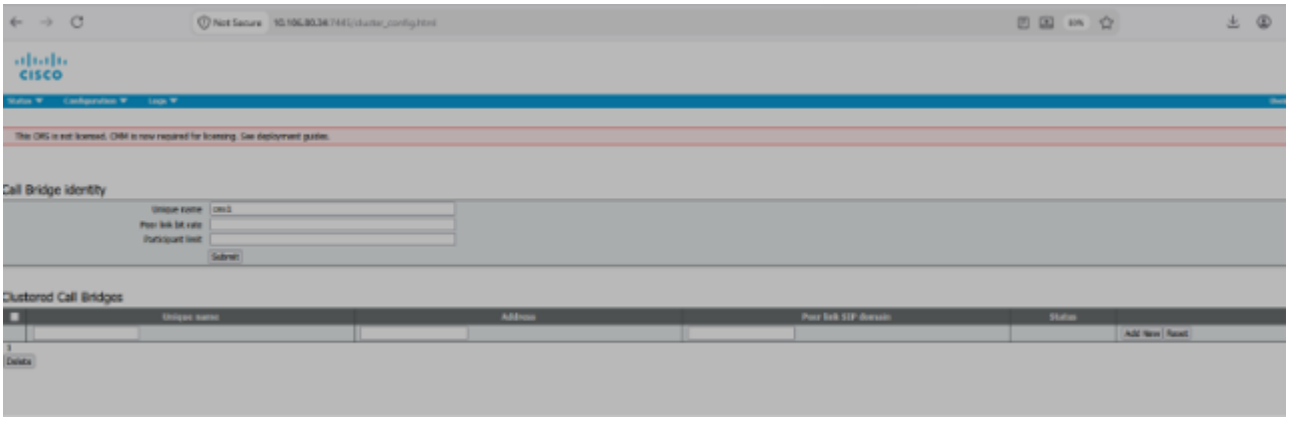


그림 39: 스키마 업그레이드 전에 이 예에서는 클러스터된 통화 브리지가 비어 있는 동안 실행되는 데이터베이스 클러스터를 보여 줍니다.

database cluster upgrade_schema

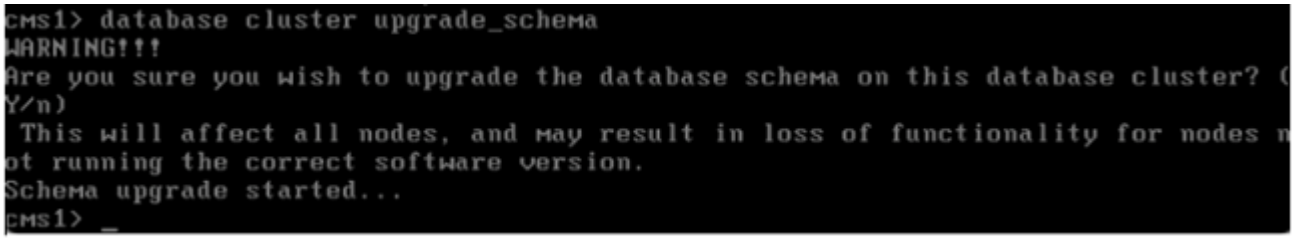


그림 40: 이전 기본 의 경우, 이 분리된 클러스터 업그레이드 후 Call Bridge 클러스터 연결이 실패한 경우에만 Y를 확인합니다.

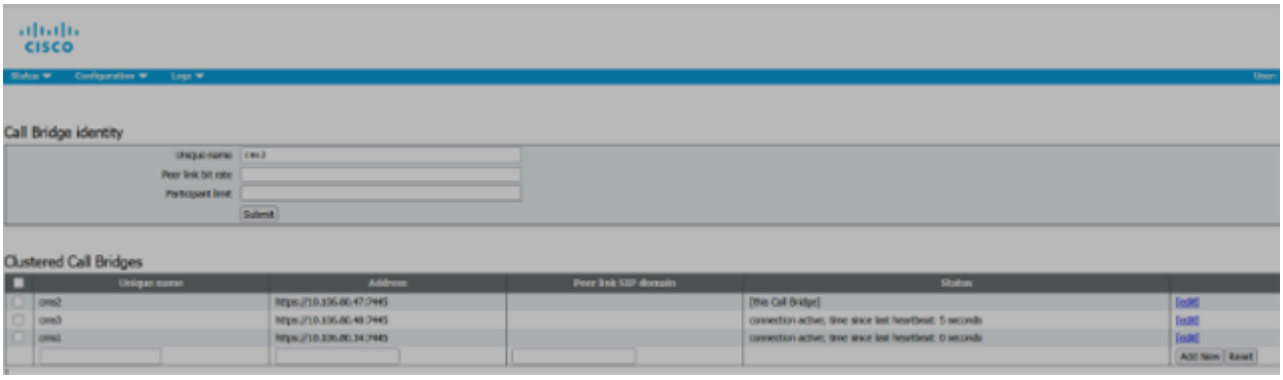


그림 41: 스키마 업그레이드 후 각 통화 브리지 피어에 활성 연결이 표시되는지 확인합니다.

모든 웹 브리지의 MeetingApps Secret Key After Restore(복원 후의 MeetingApps 비밀 키) 섹션에

서 MeetingApps 비밀 절차를 완료한 다음 업그레이드 후 검증 섹션을 사용하여 배포를 검증합니다.

업그레이드 후 검증

복원 후 시스템을 운영 시스템으로 되돌리기 전에 이 체크리스트를 작성합니다.

- 모든 노드의 웹 관리자는 Cisco Meeting Server 4.0을 표시합니다.
- 필수 MMP 서비스가 활성화되어 실행 중입니다(활성: True)입니다.
- 결함 상태는 명확합니다. 해당 결함이 없는 경우 최근 오류 및 경고를 정보 제공으로 처리합니다.
- 필요한 경우 데이터베이스 클러스터 상태에 예상 기본 및 복제본이 표시됩니다.
- Smart Licensing 및 Call Bridge 연결이 복원됩니다.
- 이 배포에서 지원되는 SIP 통화 및 Web App 클라이언트 통화가 성공적으로 완료되었습니다.
- 브랜딩, 오디오 프롬프트 및 업그레이드 전 요구 사항 섹션에 있는 서버에서 복사한 SSO 파일이 백업에 아직 포함되지 않은 경우 복원됩니다.
- MeetingApps가 배포된 경우 웹 브리지에 새 MeetingApps 관계 및 파일 공유 작업이 표시됩니다.
- 배포가 수락된 후에만 짧은 스냅숏을 제거합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.