将会议服务器升级到版本4.0 — 白皮书

目录

简介

背景信息

安全存储概述

- 支持的平台
- 实施说明

升级原则和限制

- 所需的升级路径
- 降级
- 4.0升级的关键备份要求
- 首次登录和密码配置
- 升级后重新建立网络连接
- 在创建备份之前验证服务器运行状况

升级前要求

通用备份和恢复过程

- 在4.0升级后受影响的数据
- 在安全存储被禁用或不可用时进行备份
- 启用安全存储时进行备份
- 在4.0升级后恢复数据
- 恢复后的MeetingApps密钥

首次启动和网络恢复

升级方案

- 方案1 — 禁用或无法使用安全存储的单个节点
- 方案2 — 启用了安全存储的单个节点
- 场景3 — 禁用了安全存储的数据库群集
  - 记录集群详细信息并备份每个节点
  - 解散集群
  - 升级和恢复节点
- 场景4 — 启用了安全存储的数据库群集
  - 记录集群详细信息并创建加密备份
  - 解除、升级和恢复

升级后验证

简介

本文档介绍如何将Cisco Meeting Server升级到版本4.0。

背景信息

请将此文档与Cisco Meeting Server发行说明、 MMP命令参考指南和Secure Storage Administrator参考指南结合使用，了解要求和必备条件。

Cisco Meeting Server 4.0的升级过程与以前的版本不同，因为应用映像会触发节点的出厂重置。为确保服务连续性，在开始升级之前，必须通过导出到外部位置的备份来保留所有以前的配置（包括网络设置和密码）。

此外，Secure Storage在Cisco Meeting Server 3.11到3.13版本中是可选的，但在版本4.0中默认处于启用状态。因此，如果您从未使用过Secure Storage，或者您已经在3.11x、3.12x或3.13x上启用了Secure Storage，则必须执行不同的备份和恢复过程。

Secure Storage对服务器上的私钥和备份文件进行加密，并要求先加密这些文件，然后才能将其传输到外部存储。

本文档将所需的指南整合到单个参考中，以便您可以遵循所有升级方案的通用过程，而无需重复相同的步骤。

本文档涉及以下主题：

- 安全存储是什么？它在什么地方适用？在什么地方不适用？
- 升级路径，包括要求在4.0之前到达3.13.x，并且不支持从4.0降级。
- 一种通用的备份和恢复方法，适用于启用了安全存储的节点以及禁用或无法使用安全存储的节点。
- 数据库群集节点在升级前解散数据库群集时，将解散序列化。
- MeetingApps密钥，不存储在Cisco Meeting Server备份中，必须在恢复后重新生成。



注意：本文档使用在原始升级指南测试（包括4.0测试版软件）中捕获的实验室截图。所有显示的主机名、IP地址和文件名都是严格说明性的，并不反映实际生产凭证或敏感密码。为保持清晰度和防止冗余，除非群集视图提供其他必要的上下文，否则在“通用过程”(common procedure)部分中只会显示一次重复的步骤。

安全存储概述

安全存储通过加密驻留在会议服务器上的敏感文件以及控制这些文件从呼叫网桥服务器卸载的方式提供增强的数据安全性。此功能在Cisco Meeting Server 3.11中作为可配置选项引入，在虚拟机部署（基于规范或Meeting Server Small）和Meeting Server Medium上使用MMP命令secure_storage

enable。

从4.0版本开始，默认情况下启用安全存储。此设置现在为永久性，不可逆，并且secure_storage enable MMP命令已被删除。

使用安全存储，会议服务器将强制执行以下行为：

- 私有密钥加密后才能通过SFTP下载。使用pki encrypt MMP命令后接至少14个字符的口令对私钥进行加密。这不会更改Meeting Server服务当前使用的密钥。
- 使用backup encrypt <name> encrypted-name命令创建的备份文件已加密。当启用安全存储时，backup encrypt <name> encrypted-name MMP命令会提示输入至少14个字符的口令。备份还原期间需要相同的密码。
- 在下载备份文件之前，必须采用加密形式。如果列出的备份尚未加密以供导出，请使用backup encrypt <name> encrypted-name。会拒绝尝试下载未加密的备份。
- 从版本3.12开始，安全存储可以在启用FIPS时运行。在3.11中创建的具有更短密码短语的私钥文件必须使用至少14个字符的密码短语重新生成。



提示：安全存储会限制从会议服务器传输未加密的私钥和未加密的备份文件。它不会限制证书文件的传输。证书仍然可以使用SFTP进行复制；只有关联的未加密私钥才会被阻止，直到它们使用pki加密进行加密。



警告：启用后，无法使用任何MMP命令禁用安全存储。操作是不可逆的。仅factory_reset full将安全存储重置为false。在启用“安全存储”之前,使用备份快照进行配置备份，并将其存储在单独的设备上。在secure_storage启用后，立即重新启动。如果跳过重新启动，可以在未完全初始化的情况下将安全存储标记为启用，并且factory_reset full等命令可能会失败。该状态下的恢复路径将恢复到以前保存的快照（仅对3.13.x有效）。 在Meeting Server 4.0中，默认情况下启用secure_storage。

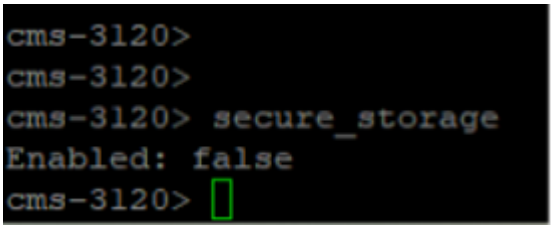
支持的平台

- 虚拟机（基于规范）：受支持
- 小型会议服务器/1000:受支持
- 会议服务器媒体：受支持
- 会议服务器2000:不支持。安全存储功能不可用。请勿在此平台上使用Secure Storage命令。

默认情况下，Cisco Meeting Server 4.0在所有兼容平台上启用安全存储。升级后，即使是在禁用安全存储时进行了3.13.x备份，数据仍自动受到安全存储的保护。

实施说明

- 重命名升级映像不会更改Secure Storage设置。
- 在执行备份之前，使用命令secure_storage确认每个节点上的安全存储状态。
- 该命令报告安全存储是否已启用(True)或未启用(False)。 在Meeting Server 2000上，该命令不适用；在升级Cisco Meeting Server 2000时，请按照在禁用安全存储或无法使用安全存储的升级条件下提到的步骤进行操作。



未启用Secure Storage时的MMP输出(启用：false)。



图 2：启用安全存储时的MMP输出(启用：true)。

有关命令语法警告和示例用法的详细信息，请参阅《Cisco Meeting Server管理员安全存储快速参考指南》和您当前使用的MMP命令参考。

升级原则和限制

所需的升级路径

Cisco Meeting Server升级必须遵循连续路径，不能跳过主要版本。例如，3.11.x上的节点必须前进到3.12.x和3.13.x，才能到达4.0。不支持从早期版本（如3.9.x到3.13.x或3.11.x到4.0）直接升级，通常会导致无法恢复的配置错误。对于版本为3.11.5或3.13的Meeting Server Medium，升级路径为3.11.5 → 3.13 → 4.0。

提示：在开始4.0升级之前，每个节点必须运行Cisco Meeting Server 3.13.x，并从该3.13.x系统导出经验证的配置备份。本文中的所有场景过程都假设已完成了到3.13.x的逐步升级。

降级



提示：不支持从4.0.x降级到3.13.x。如果升级失败或系统无法按预期工作，请部署新的3.13.x OVA（或重新映像设备）并恢复3.13.x备份。在升级窗口期间保留3.13.x虚拟机的虚拟机监控程序快照作为额外的恢复选项。VM快照不会替换导出的配置备份。

4.0升级的关键备份要求

在确认4.0升级后，节点重新引导到第一个引导状态。不要依赖于在升级过程中生成的自动备份，因为升级失败可能会导致SFTP访问丢失，并使文件无法访问。只有使用backup snapshot命令创建并复制到外部存储的备份才能可靠地用于恢复。

首次登录和密码配置

首次启动4.0版时，将从数据库中删除现有的MMP密码。使用用户名admin和空白密码（无密码）登录。 系统要求您设置新的MMP密码。系统会提示您输入两次密码以进行验证和确认。由于会议服务器没有密码恢复功能，请确保录制新密码。

注意：如果在首次启动时设置新的MMP密码，backup rollback命令会将其替换为3.13.x备份中存储的密码。在服务器上恢复备份后，必须使用创建备份时处于活动状态的密码登录。

升级后重新建立网络连接

IPv4和IPv6地址、掩码和网关与配置的其余部分一起丢失。升级到4.0后，会丢失会议服务器的网络连接。您必须具有虚拟机监控程序控制台、CIMC或串行访问，以便可以再次从MMP分配寻址。



注意：使用DHCP保留的部署通常会在重新启动后保留相同的IP地址。但是，在地址验证之前，控制台访问必须保持可用。在确认IP地址之前，不要假设SSH连接已恢复。

在创建备份之前验证服务器运行状况

每次逐步升级到3.13后，请确保服务器处于正常状态，并且所有服务都在工作。请勿忽略服务器概述页面上的任何故障情况。如果您遇到任何错误/故障，请先修复这些错误，然后再在3.13上创建备份快照。这可以确保在升级的4.0节点上还原正常的服务器备份，从而避免部署错误。

在Web Admin上，打开Status（状态），确认Fault conditions（故障条件）部分是明确的。忽略仅在“最近的错误和警告”下显示的条目。在升级后，经常可以看到临时数据库或Web Bridge消息；这些不是恢复或延迟备份的理由。

如果故障状态保持时间超过10分钟，请在进行备份之前解决此问题。将已经包含故障的3.13.x备份恢复到4.0后，这些故障就会继续发生。

对于集群系统，请确认所有使用的呼叫类型（SIP终端和Web应用客户端）都正常工作，并且任何节点上均未列出任何故障条件。

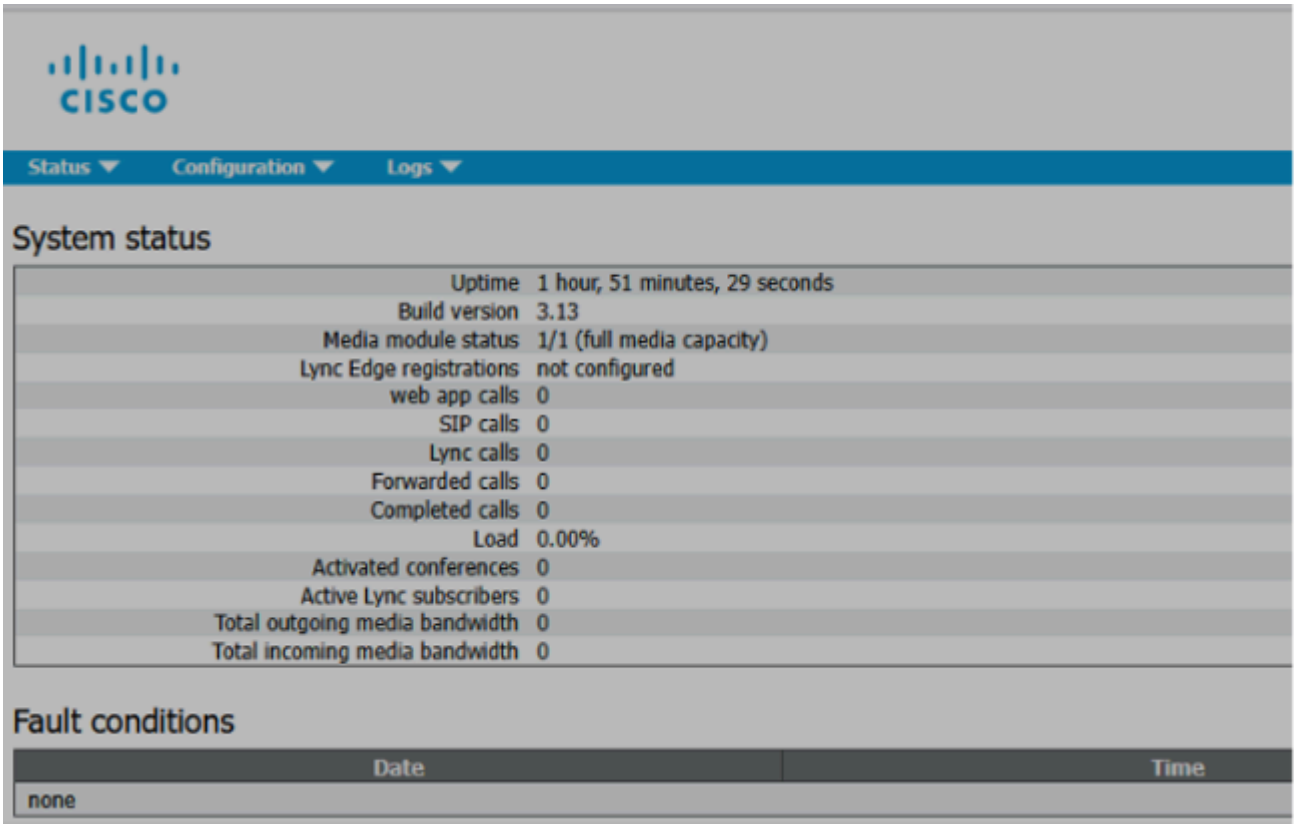


图 3：3.13.x上的Web管理员状态页面，故障条件为空。在您执行恢复到4.0的备份之前，请使用此视图。

升级前要求

开始升级到版本4.0之前，请完成以下操作。这些要求适用于本文档后面介绍的所有四种方案。

- 升级到3.13.x，然后导出配置备份。确保节点正在运行Cisco Meeting Server 3.13.x。创建备份并将其与所有自定义SFTP数据（如徽标、品牌文件、音频提示、SSO文件以及任何其他自定义数据）一起传输到外部存储。使用通用备份和还原过程部分中的过程。在群集环境中，从每个节点进行备份，不仅从连接的主，而且从连接的副本进行备份。
- 记录网络设置。运行ipv4 a并存储输出。在4.0重新启动后，您必须从控制台重新输入此信息，除非DHCP保留自动恢复IP地址。

- 确认控制台访问。启动之前，虚拟机监控程序控制台、CIMC或串行访问必须可用。当节点重启到4.0时，SSH预期会断开。
- 下载用于存档的当前日志捆绑包。从每个节点保存logbundle.tar.gz。该捆绑包不能替代备份快照。
- 执行upgrade命令后显示时，请阅读4.0升级警告标语。
- 如果任何先决条件未完成，请按n中止。只有在准备继续时，才按Y。

通用备份和恢复过程

本文档后面讨论的四个升级方案使用相同的备份、导出、首次启动和恢复模式。使用此部分作为这些步骤的单一来源，然后仅按照场景特定的顺序执行（单节点与群集以及安全存储是否已启用）。

在4.0升级后受影响的数据

此数据在4.0升级后丢失，直到您恢复备份：

- 数据库内容，包括空间、用户和呼叫配置文件。
- 证书和私钥。
- 本地定制、SSO文件和音频提示文件。
- 网络配置（IP地址、掩码和网关），但DHCP保留恢复地址时除外。
- 以前的MMP密码，直到备份回滚从备份重新应用该密码。
- Call Bridge、Web Admin、Web Bridge和其他应用服务仅在恢复后返回。



提示：Cisco MeetingServer备份不包含MeetingApps密钥。恢复后，必须重新生成该密钥，并将其应用于每个Web网桥节点。请参阅恢复后MeetingApps密钥部分。

在安全存储被禁用或不可用时进行备份

在虚拟机、Meeting Server Small和Meeting Server Medium（其中secure_storage报告已启用）上执行以下步骤：False，在Meeting Server 2000上，安全存储不可用。

1.在每个节点上，使用backup snapshot命令创建一个文件。不要重复使用以前的文件名。

2.立即使用SFTP将备份文件复制到外部存储。请勿在会议服务器上保留唯一的副本。

3.将文件存储在重建节点后仍可访问的位置。

示例：

backup snapshot cms313SecurestorageFalse backup list

4.确认该文件显示在backup list命令中，然后使用SFTP客户端将其传输到外部磁盘。

5.对群集中的每个节点重复此过程。备份名称只能包含字母、数字、下划线和连字符。创建备份文件时不要包含.bak文件扩展名。例如，由于句点，诸如3.13SecurestorageFalse的文件名被拒绝。

```
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>
```

图 4：备份快照将拒绝包含句点的名称，然后使用字母数字名称后继。然后.bak文件即可下载。



图 5：将.bak文件从会议服务器SFTP根目录复制到外部存储。请勿将唯一的副本留在服务器上。

启用安全存储时进行备份

当secure_storage报告Enabled:对。无法下载未加密的备份文件。

1.在每个节点上创建备份快照。启用Secure Storage时，服务器会提示输入至少14个字符的口令。密码短语可以包括字母、数字、特殊字符、符号或空格。

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

图 6：启用了Secure Storage的备份快照会提示一次至少包含14个字符的口令。MMP不要求您确认。

2. MMP不会要求您重新输入密码进行确认。保护您的密码，因为恢复文件时需要相同的密码。不要选择简单密码或示例密码。

3.如果backup list命令显示尚未加密以供导出的快照，请在下载之前对其进行加密：

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

图 7：加密前的备份列表。Encrypted列为no，因此无法下载文件。

4.如果您尝试下载未加密的备份，SFTP将返回权限拒绝错误，并指示您首先运行backup encrypt命令。

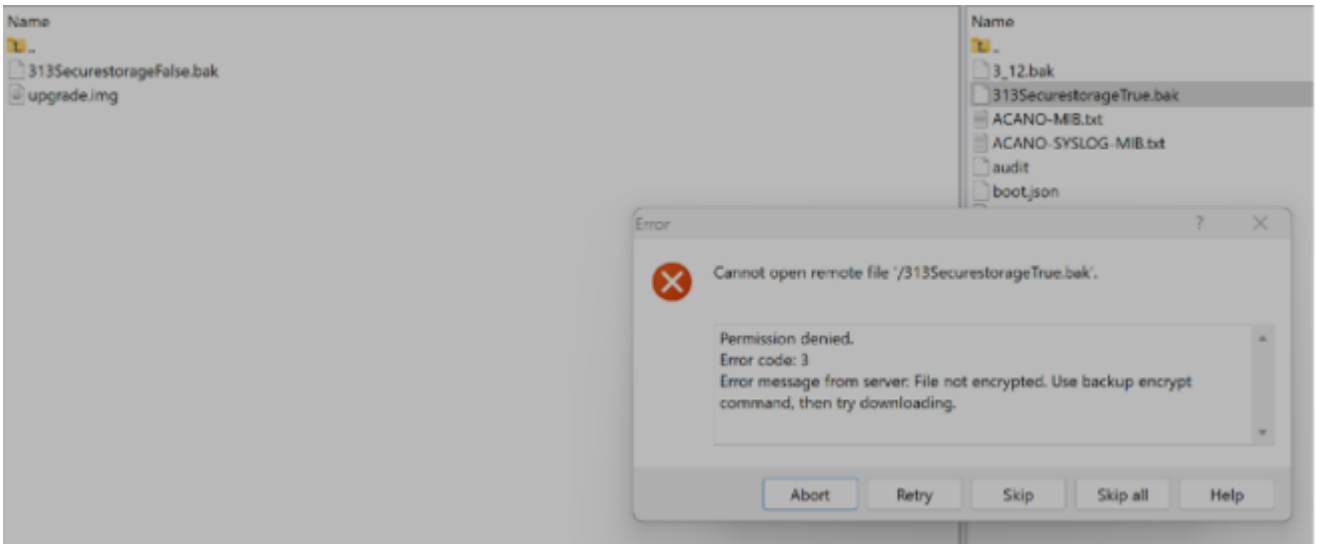


图 8：启用安全存储时，SFTP会拒绝下载未加密的备份。服务器消息指示您运行备份加密。

5.运行backup encrypt命令以加密备份文件。

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

图 9：加密快照之后的备份列表。Encrypted为yes，并且文件可以通过SFTP传输。

备份列表显示加密状态和原始文件名。确保仅传输来自群集中每个节点的加密文件。维护每个节点的有组织记录、其对应文件名和相关密码。

如果您还需要导出私有密钥，请首先加密每个密钥。安全存储不会阻止证书文件，并且可以在不执行此额外步骤的情况下复制这些文件：

pki encrypt private.key encrypted_private.key

使用唯一的文件名，而不是覆盖服务当前使用的密钥。此处也适用至少14个字符的密码短语要求。

在4.0升级后恢复数据

1.首次启动登录和网络恢复后，在首次启动和网络恢复部分中，将相应的3.13.x备份复制到使用SFTP的节点上，然后恢复该备份。

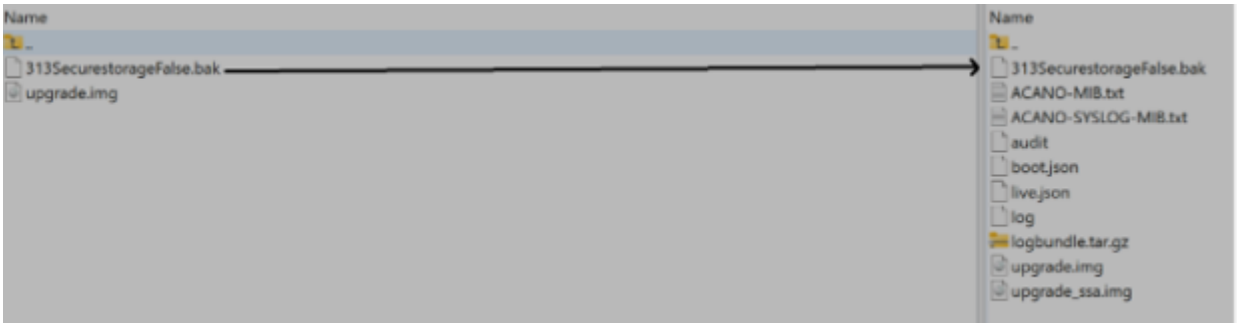


图 10：首次启动网络恢复后，使用SFTP将3.13.x .bak文件复制回4.0节点。

2.确认文件是否存在：

备份列表

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

cms-3120>
```

图 11：4.0上的备份列表，确认在回滚之前已上传快照。

3.恢复快照。在群集部署中，首先恢复以前的数据库主节点，然后恢复副本，最后恢复连接的节点。

backup rollback name-of-the-backup-file



图 12：未加密快照的备份回滚。用Y确认；节点提取备份并重新启动。

4.按Y继续。节点在提取备份时重新启动。如果备份是在启用安全存储的情况下进行的，则MMP会提示输入口令。只有在接受正确的口令后，重新启动才会继续。

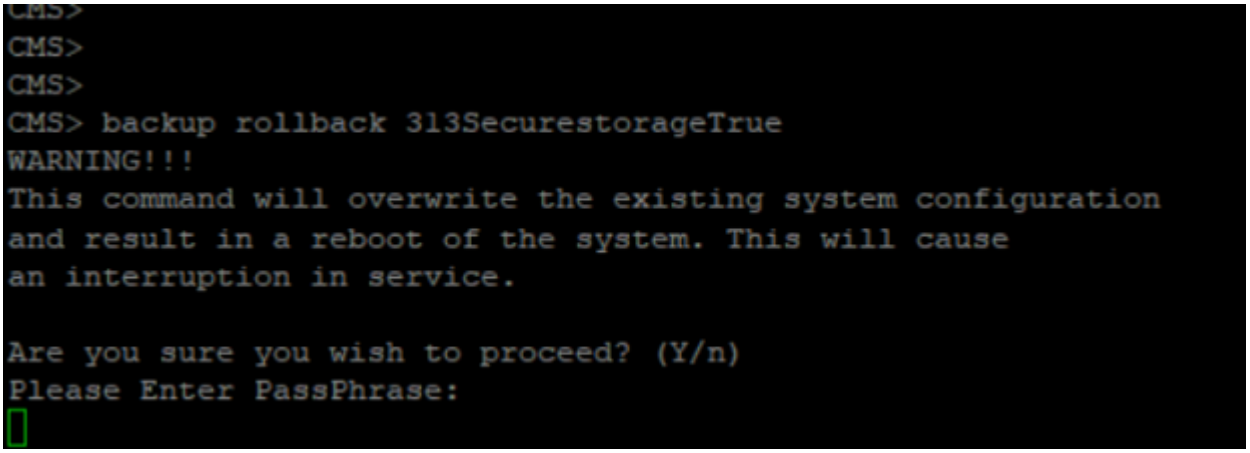


图 13：加密快照的备份回滚。在Y之后，MMP会提示输入创建备份时使用的口令。

⚠ 警告：覆盖**backup rollback**当前配置、证书、私钥和许可证文件，然后重新启动服务器。仅将它用于您为此升级导出的3.13.x备份。

5.当节点重新联机时，使用备份中的MMP凭证登录，并确认每个必需的服务报告为已启用且正在运行(MMP显示以下为活动状态：正确)。

典型检查：

callbridge webbridge3 webadmin scheduler recorder streamer uploader meetingapps

6.只对此节点应承载的服务运行命令。

恢复后的MeetingApps密钥

思科会议服务器备份不存储MeetingApps密钥。备份回滚完成后，重新生成密钥，并将其应用于每个Web网桥节点。跳过此步骤会导致文件共享不可用，即使其他服务看起来正常。

1.在MeetingApps节点上，执行meetingapps gensecret命令。

2.将生成的密钥复制到您的密钥库。每次执行meetingapps gensecret都会使上一个密钥失效，因此只需生成一次密钥并在所有Web网桥之间重复使用相同的值。

3.在每个Web网桥节点上执行以下命令：

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

最后一个命令确认Web Bridge服务正在运行，并且MeetingApps配置正确。Meeting Server 2000不支持MeetingApps，并且在包含Meeting Server 2000的群集中无法共享文件。在此类部署中，此步骤不适用。

首次启动和网络恢复

4.0 upgrade命令在继续之前会显示警告标语。仔细查看该消息，如果任何先决条件未完成，则以n中止。如果继续执行Y，节点将重新启动，SSH会话将断开连接，并且必须从控制台完成其余步骤。

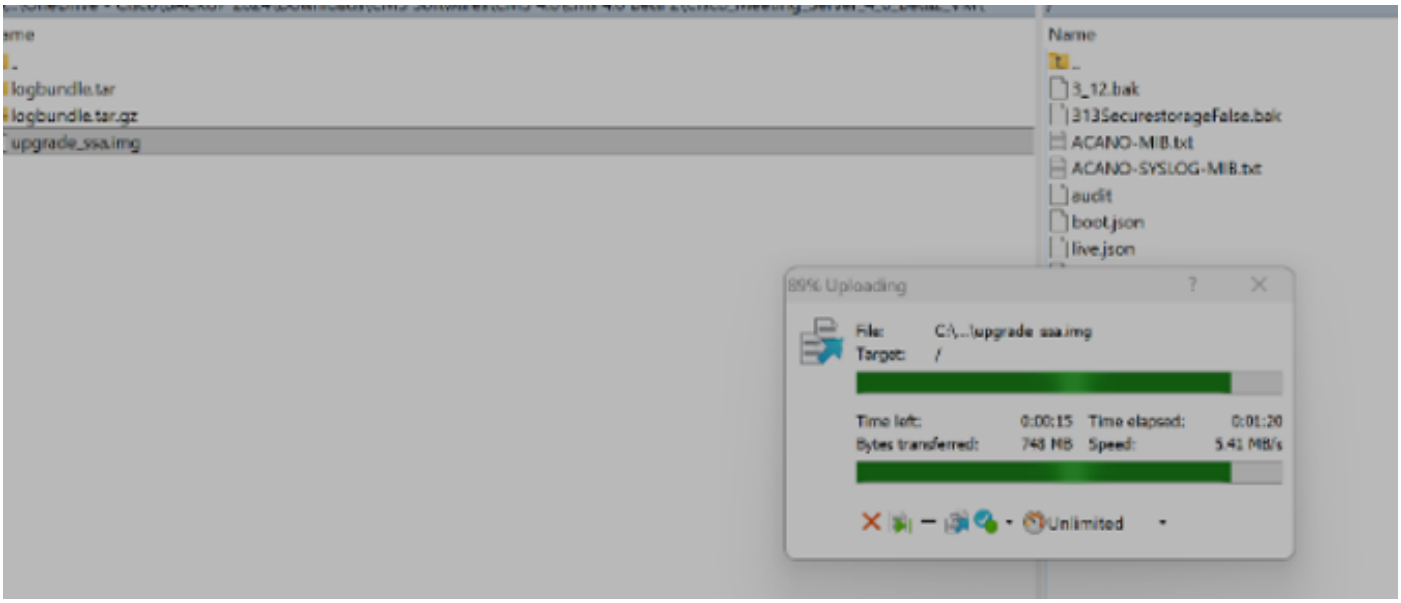


图 14：将4.0升级映像上传到Meeting Server SFTP根目录。升级映像文件名可能因从cisco.com下载的软件包而异。

```
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...
```

图 15：upgrade命令验证映像签名并启动进程。此时不依赖于自动备份。

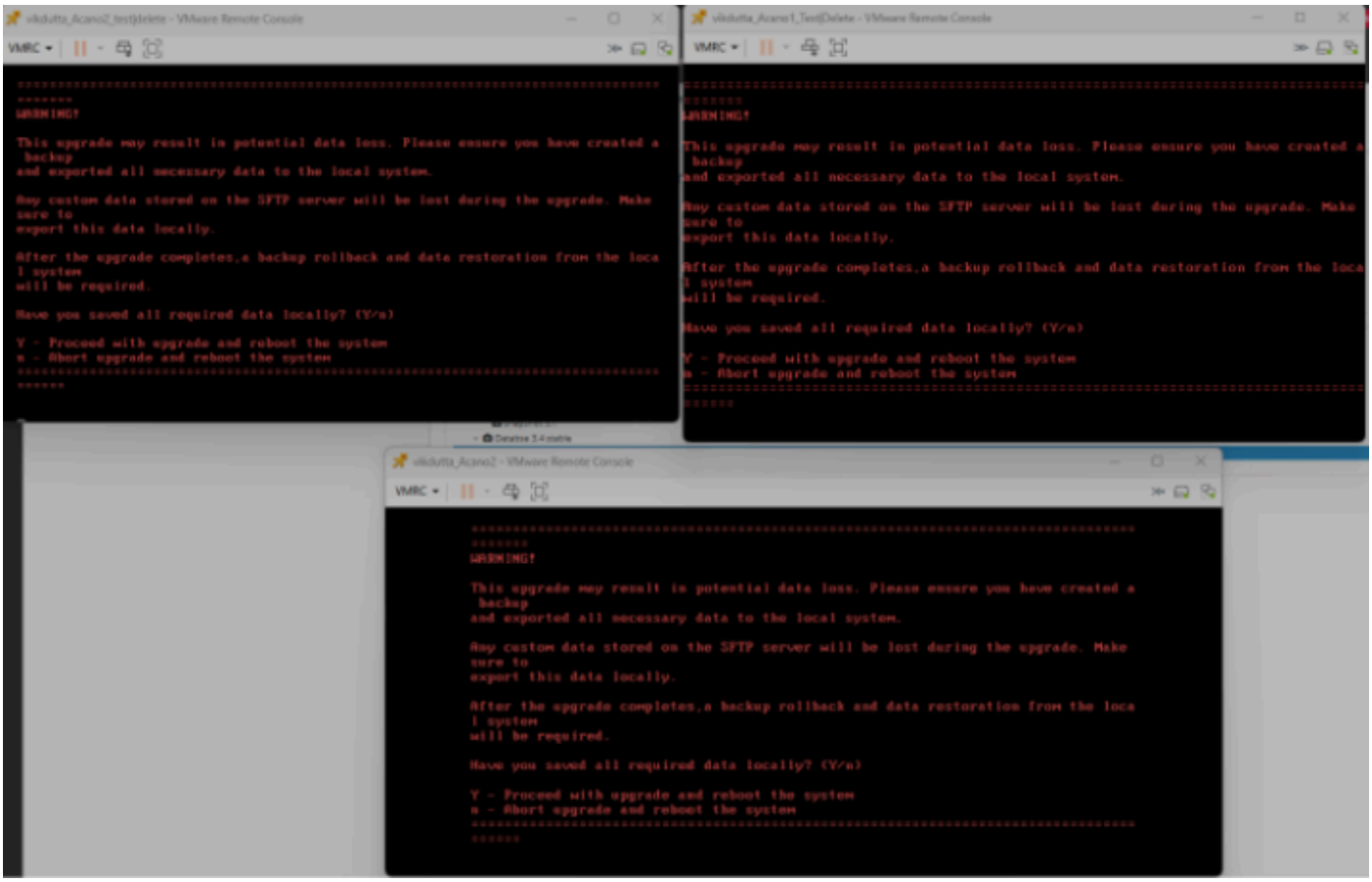


图 16：三节点群集上的红色MMP警告。同一标语显示在单个节点上。如果备份和自定义数据未离开服务器，请按n中止。仅按Y继续并重新启动。

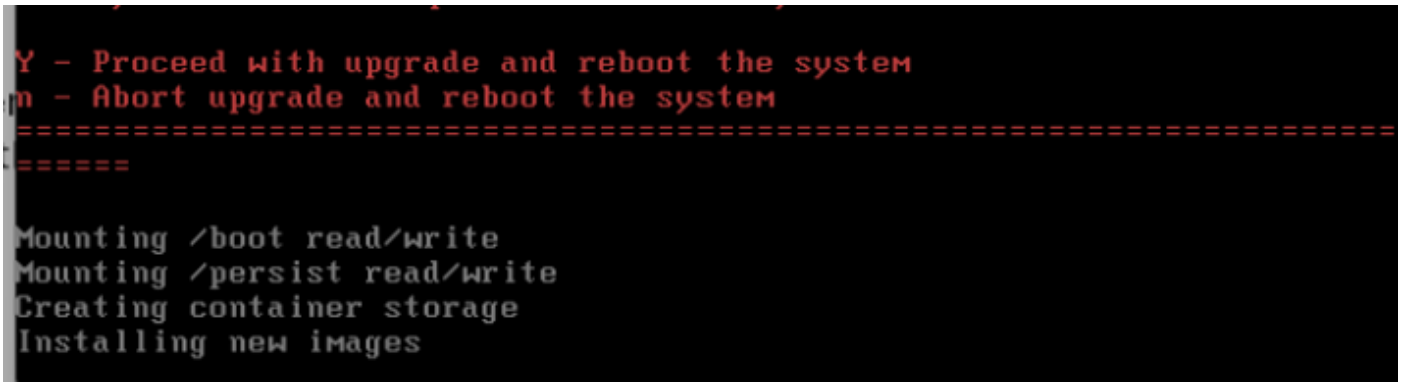


图 17：在Y之后，节点将装载存储并安装4.0映像。SSH会话超时；从虚拟机监控程序控制台继续。

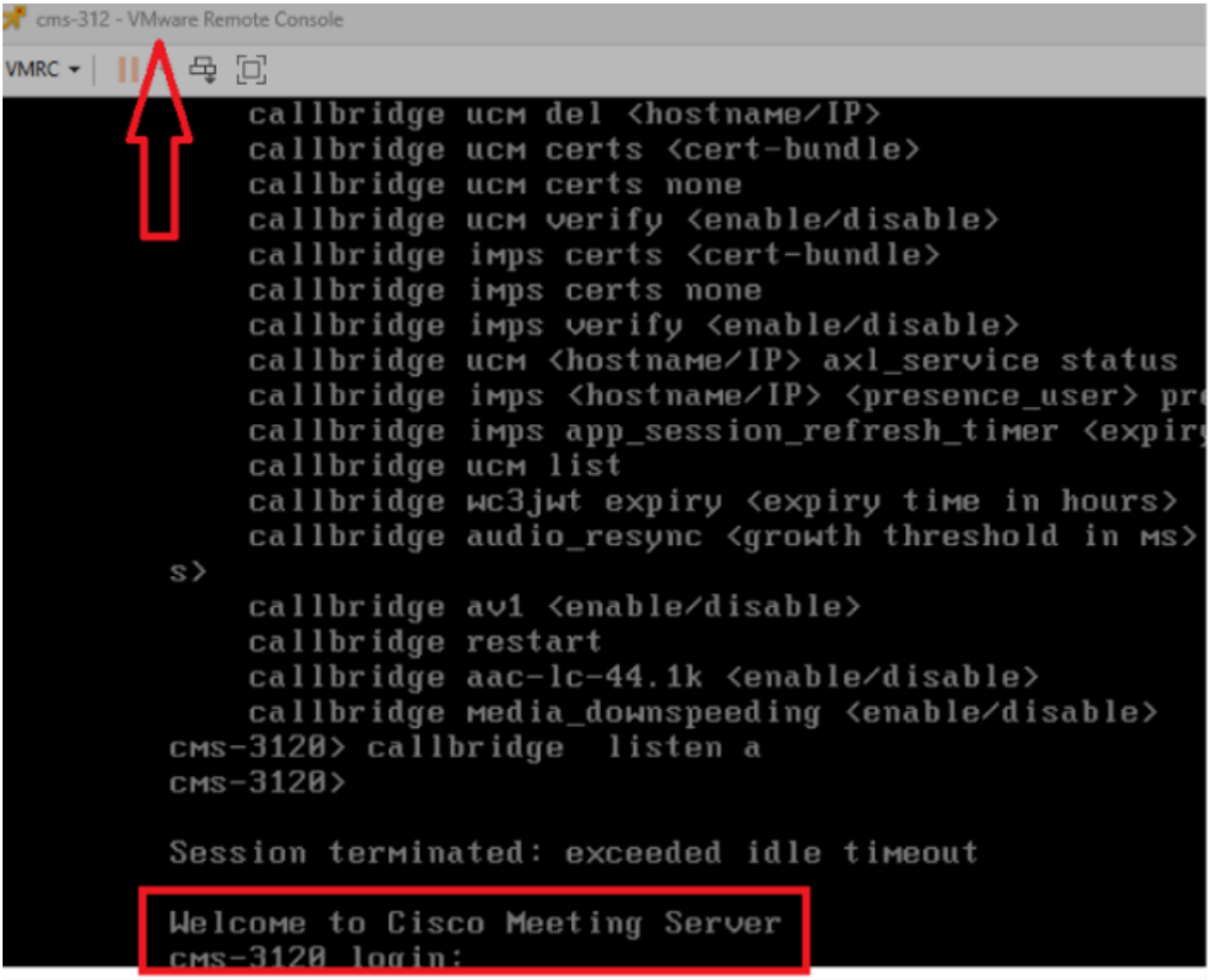


图 18：在SSH丢弃后使用VM或CIMC控制台。当4.0映像准备就绪时，系统将显示首次启动登录提示。

1.使用首次启动MMP帐户（用户名admin且没有密码）登录，然后在系统提示时设置新的MMP密码。请注意，备份回滚会用存储在备份中的密码替换此密码。

2.根据在“升级前要求”部分中捕获的备注重新应用网络配置：

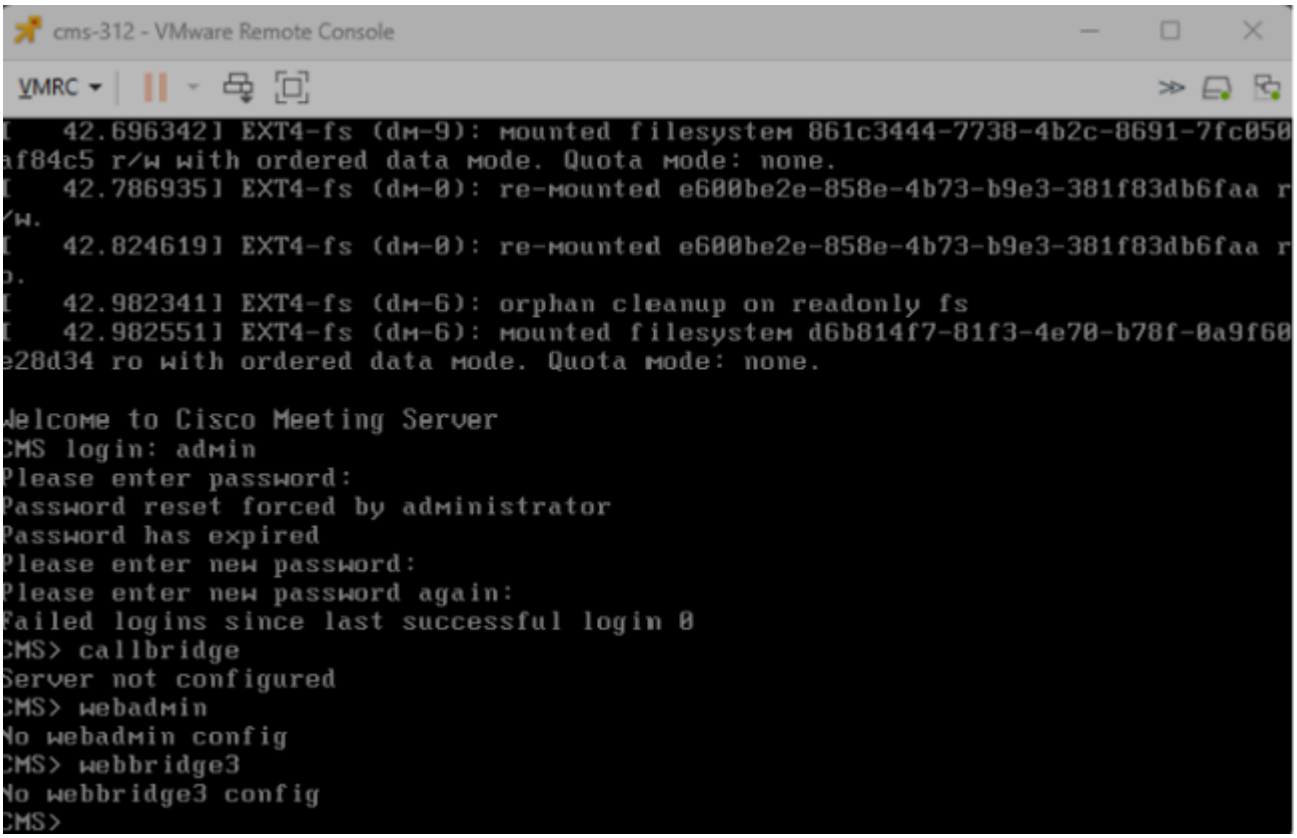


图 19：首次启动MMP登录。

以前的密码不再有效。设置新密码后，webadmin和webbridge3等服务在备份恢复之前显示为未配置。

3.执行命令：

ipv4 interface add address/prefix-length gateway

例如：

ipv4 a add 192.0.2.10/24 192.0.2.1

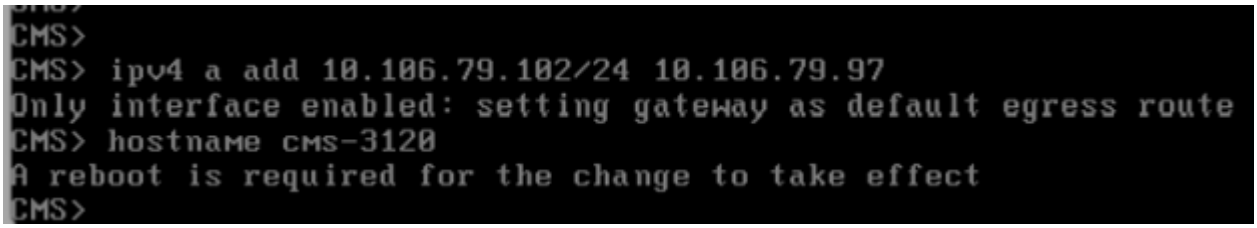


图 20：从控制台重新应用IPv4。

分配地址后需要重新启动。屏幕截图中显示的地址仅供示例使用。

4.分配地址后重新启动。系统重新联机后，继续执行SFTP上传备份和Restore Data After 4.0 Upgrade部分中提到的恢复步骤。

注意：如果配置了DHCP保留，则可以在重新启动后分配原始地址。从管理工作站启ipv4 a动SFTP会话之前，请使用验证该地址。

在Cisco Meeting Server 4.0上，在支持它的平台上默认启用安全存储。升级后，MMP无法再将secure_storage显示为一个切换开关。



图 21：在此4.0映像上，secure_storage不是可识别的命令，因为默认情况下启用安全存储。

使用version命令确认版本。

升级方案

本章介绍不同的升级方案。完成升级到3.13.x的步骤。确定您的部署类型并相应地选择方案。请仅遵循与您的环境相匹配的步骤，不要将集群和单节点部署中的步骤组合在一起。

首先完成支持的逐步升级到3.13.x。然后选择下面的一个场景。不要将单节点和数据库群集过程结合起来。

- 情形 1：单节点、禁用或不可用、VM、小型、中型和会议服务器2000
- 方案 2：单节点、已启用、虚拟机、仅小型和中型
- 情形 3：数据库群集、已禁用或不可用、VM、Small、Medium和Meeting Server 2000
- 场景 4：仅数据库群集、已启用、VM、小型和中型

Meeting Server 2000不支持启用安全存储的场景。对于该平台，请根据需要使用场景1或3。

方案1 — 禁用或无法使用安全存储的单个节点

对于禁用了安全存储的独立服务器或安全存储不可用的会议服务器2000，请使用此过程。源版本可

以是3.11.x或更高版本，但节点必须位于3.13.x上才能升级到4.0。

1.逐步升级到3.13.x。遵循支持的路径（例如3.11.x → 3.12.x → 3.13.x）。 在每一跳之后，在Web Admin中确认版本并且故障条件已清除，如“创建备份前验证服务器运行状况”一节所述。

2.确认“安全存储”状态。运行secure_storage命令并验证是否已启用安全存储。在Meeting Server 2000上跳过该命令。

3.创建并导出3.13.x备份文件，如Take a backup When Secure Storage is Disabled or Unavailable部分所述。另请按照升级前要求部分所述导出自定义SFTP内容和日志捆绑包。

4.从Cisco.com下载4.0软件映像，将其解压缩，然后通过SFTP将upgrade.img复制到节点。

5.使用以下命令开始升级：

```
upgrade upgrade.img
```

6.阅读警告横幅。仅在完成所有必备条件后按Y。6.升级后，按照首次启动和网络恢复部分所述配置节点，然后使用在4.0升级后恢复数据部分恢复备份。

方案2 — 启用了安全存储的单个节点

将此过程用于启用了安全存储的独立VM、Meeting Server Small或Meeting Server Medium。它不适用于Meeting Server 2000。

在从服务器传输文件之前，请注意无法传输未加密的私钥和未加密的备份文件。证书文件未被阻止。

1.在不跳过版本的情况下，通过受支持的路径升级到3.13.x。在每一跳之后，确认版本并在创建备份之前验证服务器运行状况部分中明确显示故障情况。

2.运行secure_storage，并确认输出显示Enabled:对。

3.使用Take a Backup When Secure Storage is Enabled部分创建和导出加密的3.13.x备份。将其口令存储在您的秘密存储中。同时导出自定义SFTP内容和日志捆绑包（升级前要求部分）。

4.将upgrade.img复制到节点并运行升级：

upgrade upgrade.img

5.阅读警告横幅，并按Y以仅在满足先决条件后继续。

6.从控制台恢复网络（First-boot and Network Restoration部分），然后使用其密码恢复加密的备份（Restore Data After 4.0 Upgrade部分）。6.如果正在使用MeetingApps，请应用新的MeetingApps密钥（恢复后的MeetingApps密钥部分）。

Meeting Server 4.0默认启用安全存储。恢复后，继续将私钥和备份文件作为加密数据处理。

场景3 — 禁用了安全存储的数据库群集

此过程适用于禁用了安全存储的数据库群集，该群集包括包含Meeting Server 2000的群集。从版本3.5开始，必须在软件升级之前解散数据库集群。首先，逐步将每个节点升级到3.13.x。

记录集群详细信息并备份每个节点

1.在每个节点上运行secure_storage。将该命令视为在Meeting Server 2000节点上不可用。

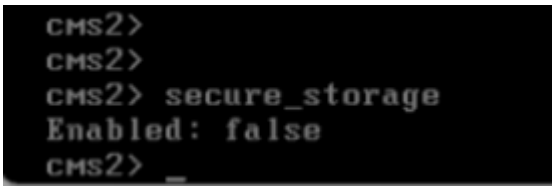


图 22：在使用未加密的备份之前，请验证每个群集节点上是否禁用了安全存储。跳过Meeting Server 2000节点的命令，该节点不可用。

2.记录当前数据库主节点，因为在升级到4.0之后必须首先还原它。确认副本处于“同步”状态且群集状态正常。

```
cms2> database cluster status
Status                    : Enabled

Nodes:
    10.106.80.34          : Connected Primary
    10.106.80.47 (me)     : Connected Replica ( In Sync )
    10.106.80.48          : Connected Replica ( In Sync )
Node in use               : 10.106.80.34

Interface                 : a

VerifyMode                : verify-ca

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

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

图 23：记录当前主副本并确认副本处于同步状态。

3.确认所有正在使用的呼叫类型都工作正常，并且每个节点上的故障条件都已清除（在创建备份之前验证服务器运行状态部分）。

4.使用Take a Backup when Secure Storage is Disabled or Unavailable部分为每个节点创建备份。命名每个文件，使其清楚地映射到其节点，并在解散群集之前将每个备份传输到外部存储。

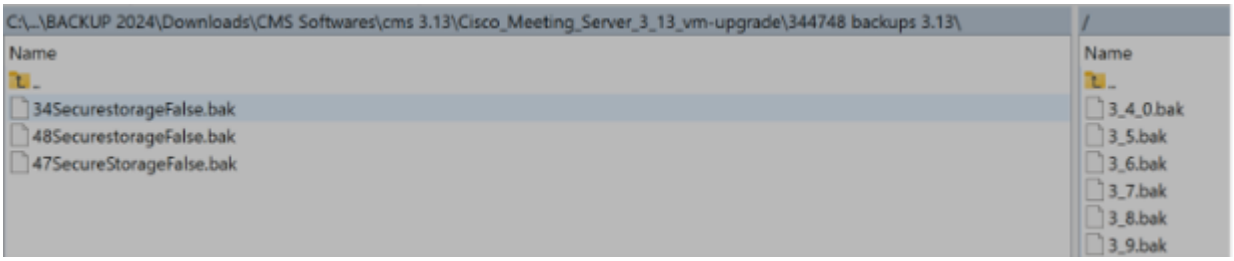


图 24：所有三个示例节点备份都存储外部存储，命名为以便每个文件映射到其节点。

解散集群

按此顺序删除节点。将主路由保留到最后：

- 已连接（非核心）会议服务器节点
- 副本数据库节点
- 主数据库节点

在每个节点上，运行删除命令并按Y。在每个节点报告其已离开集群之前，不要继续执行4.0升级。删除集群成员资格会保留该节点的本地数据库。

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
```

图 25：在复制副本上，确认Y以删除集群成员身份。节点的本地数据库保持不变。

```
 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
```

图 26：删除后，验证该节点上的集群状态为Disabled且正在使用的节点为None。

```
cms1> database cluster status
Status                    : Enabled

Nodes:
    10.106.80.34 (me)     : Connected Primary
Node in use               : 10.106.80.34

Interface                 : a

VerifyMode                : verify-ca

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

Last command              : 'database cluster initialize' (Success)
```

图 27：删除复制副本后，前一个主节点是群集中剩下的唯一节点。最后删除它。

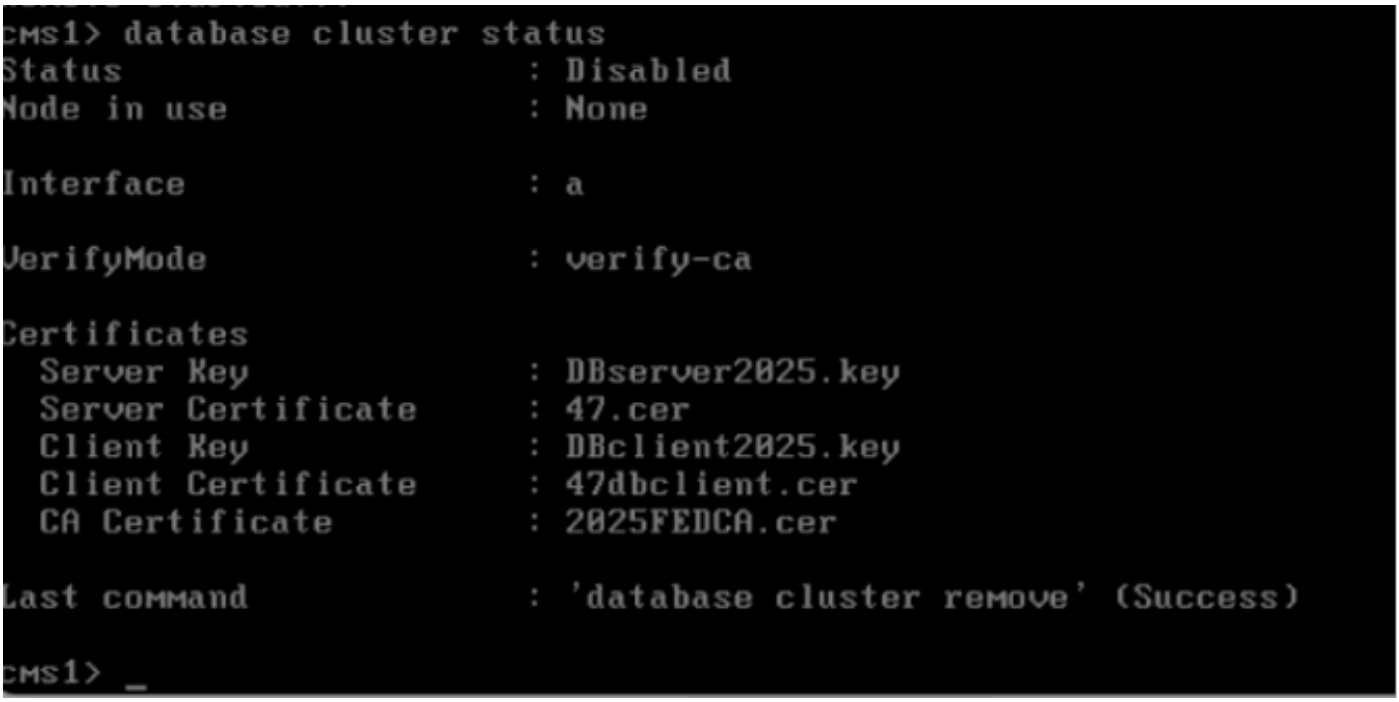


图 28：删除前一个主用后，验证该命令是否报告Success并且集群状态为Disabled。

升级和恢复节点

1.一旦解散，节点将独立且可以并行升级。在每个节点上，通过SFTP复制upgrade.img并运行upgrade命令：

upgrade upgrade.img

2.从控制台恢复每个节点的网络编址（首次引导和网络恢复部分）。

3.将每个节点自己的3.13.x备份复制回该节点。首先恢复前一个主节点，然后恢复复制副本，最后恢复连接的节点。使用Restore Data After 4.0 Upgrade部分。备份的还原将重新建立数据库群集成员身份。

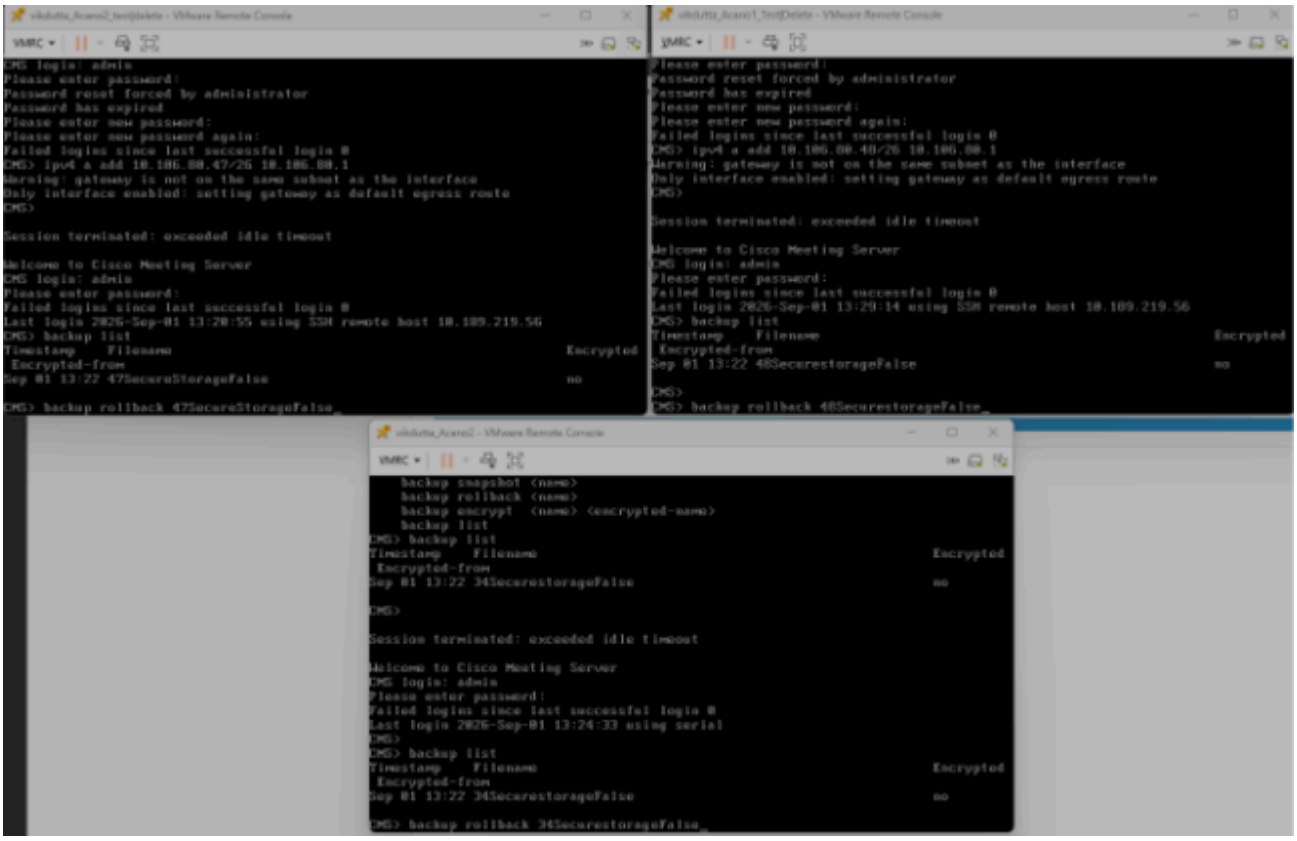


图 29：恢复每个节点自己的快照。从以前的主副本开始，然后恢复副本。示例文件名标识其节点。

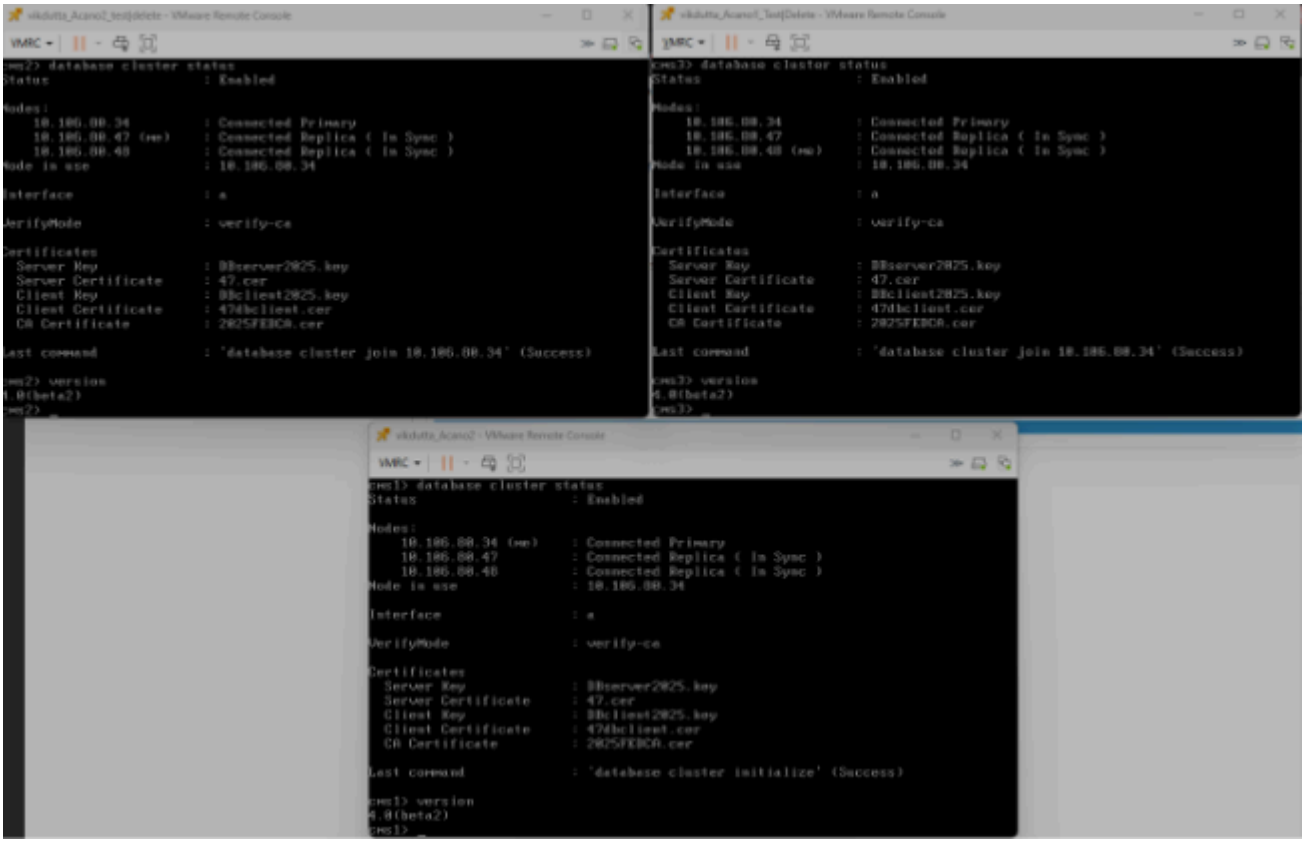


图 30：在Meeting Server 4.0上恢复后，验证群集是否已启用、是否显示相同的主群集以及是否处于同步状态。

注意：如果在此恢复后呼叫网桥集群连接未启动，请仅在前一个主上运**database cluster upgrade_schema**行，然后重新检查呼叫网桥状态。

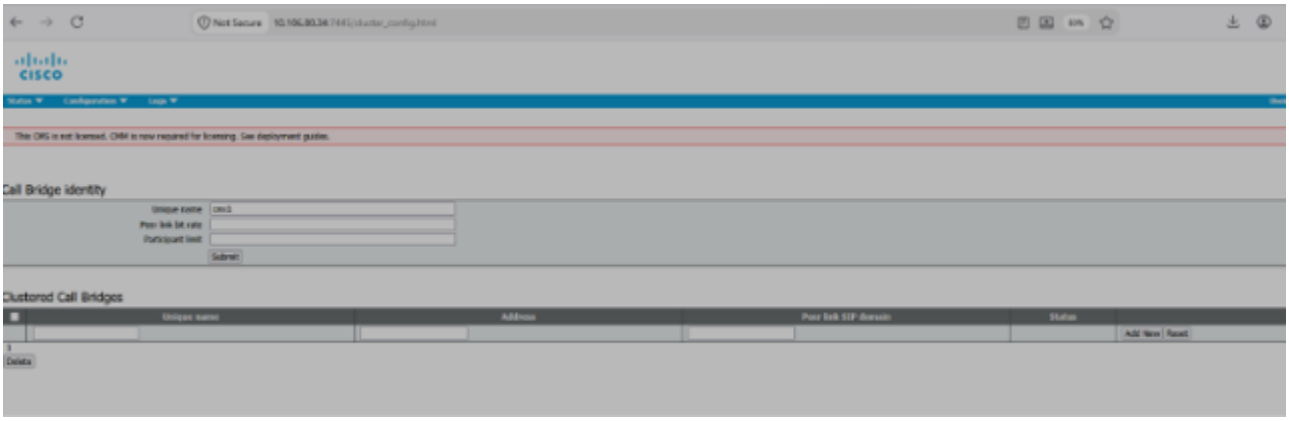


图 31：在模式升级之前，该示例显示当集群呼叫网桥为空时正在运行的数据库集群。

database cluster upgrade_schema

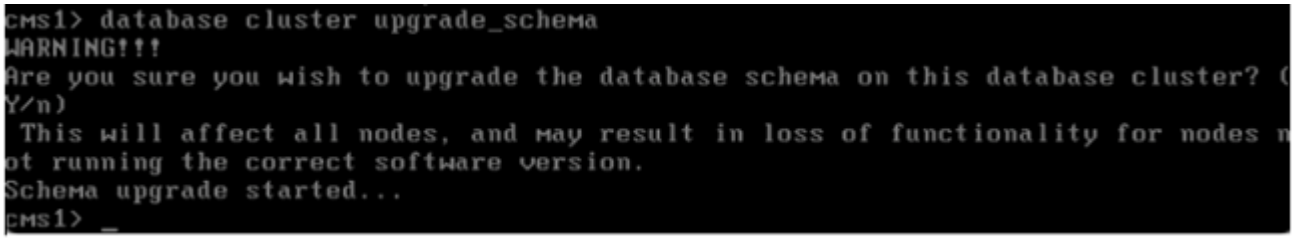


图 32：在前一个主上，只有在此已解散集群升级后Call Bridge集群连接失败时才确认Y。

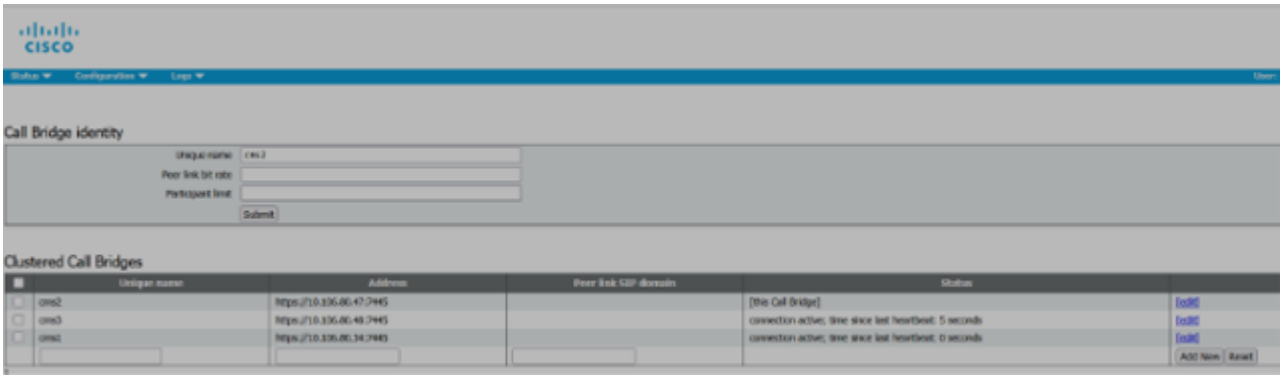


图 33：在模式升级后，验证每个呼叫网桥对等体是否显示活动连接。

4.在每个Web网桥的MeetingApps Secret Key After Restore部分中完成MeetingApps加密过程，然后使用“升级后验证”部分来验证部署情况。

场景4 — 启用了安全存储的数据库群集

对于节点上启用了安全存储的VM、Meeting Server Small或Meeting Server Medium上的数据库集群，请使用此过程。它不适用于Meeting Server 2000。首先，逐步将每个节点升级到3.13.x。

记录集群详细信息并创建加密备份

1.在每个节点上运行secure_storage并确认Enabled:对。

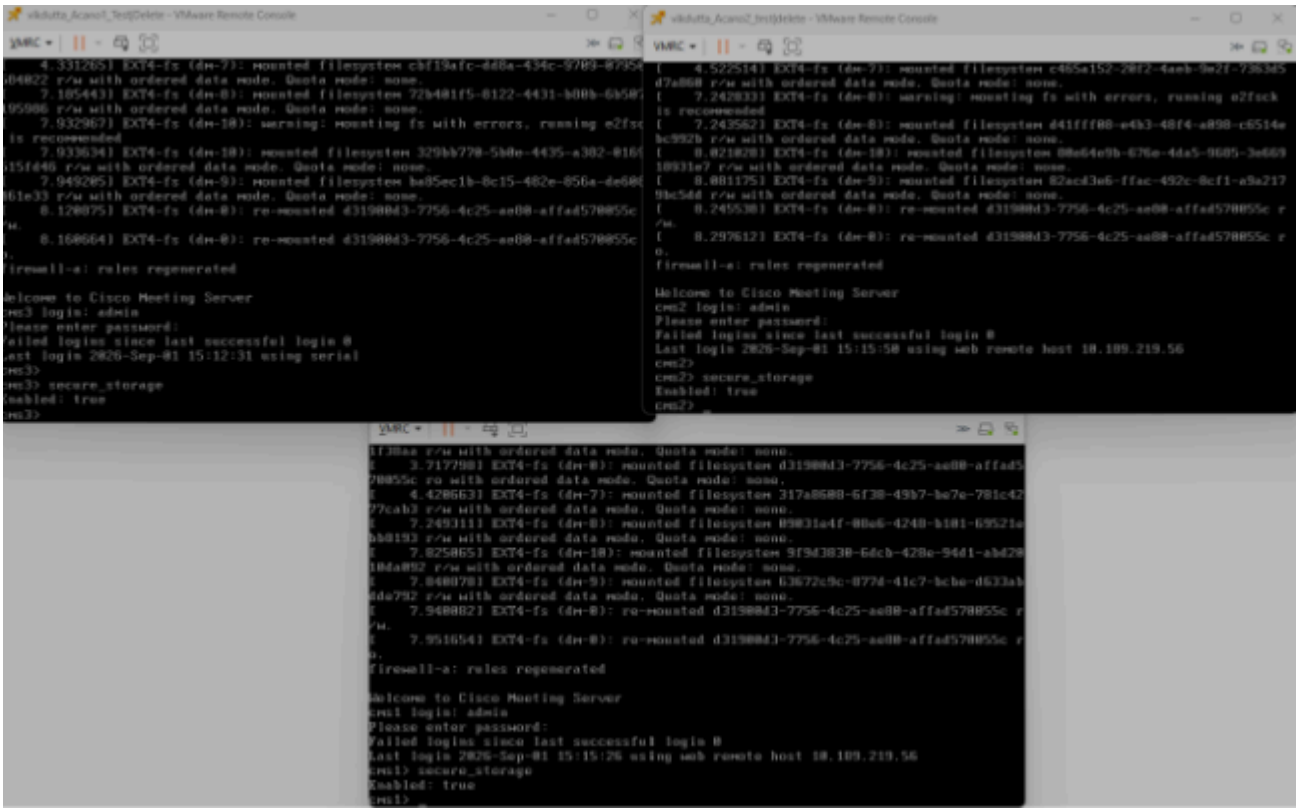


图 34：对于图示的三节点集群，请确认Secure Storage显示已启用：在升级之前每个节点都为true。

2.记录当前数据库主副本并确认副本处于同步状态。

```
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)
```

图 35：升级前的数据库群集状态。记录主副本并确认副本处于同步状态。

3.确认所有正在使用的呼叫类型都工作正常，并且每个节点上的故障条件都已清除（在创建备份之前验证服务器运行状态部分）。

4.使用启用安全存储时备份部分为每个节点创建加密备份。为每个文件分配并记录唯一的密码短语，或使用记录的密码短语策略。在解散集群之前，仅从服务器传输加密文件。

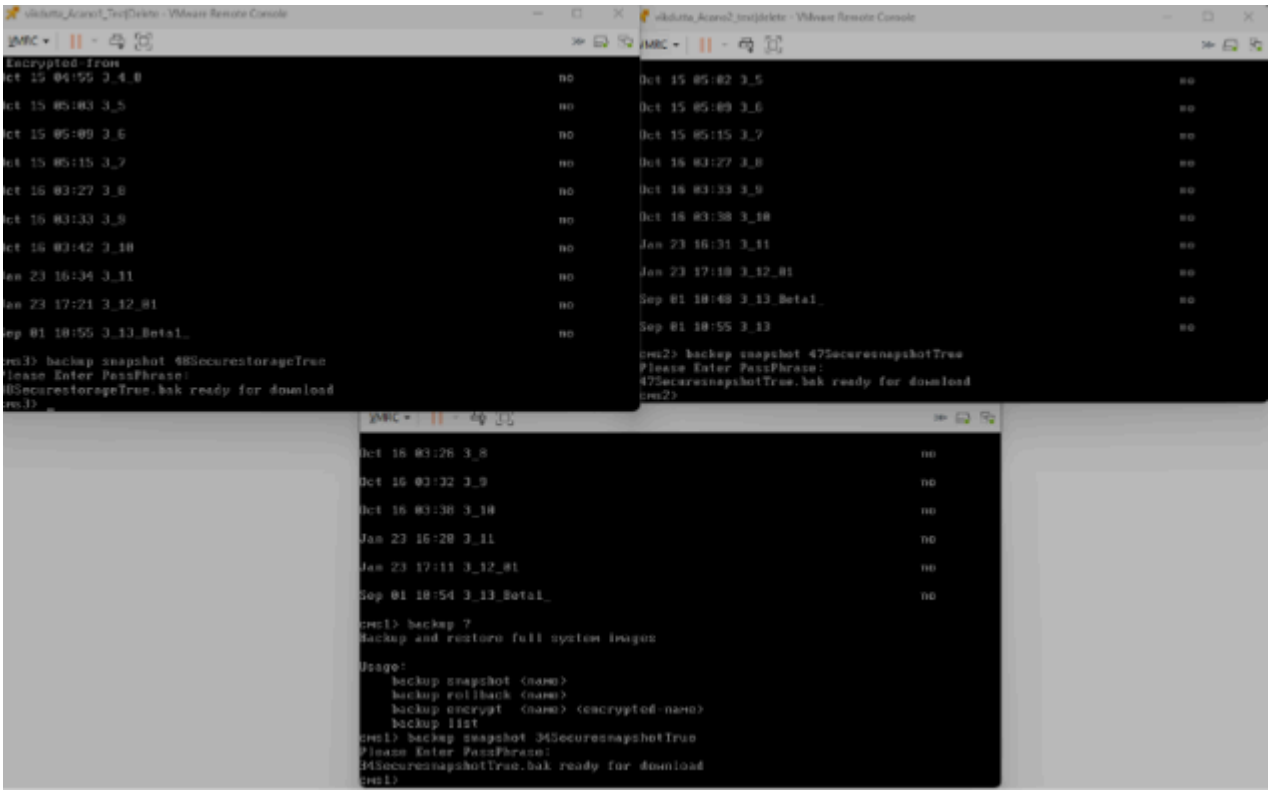


图 36：每个节点上的加密备份快照。该示例显示密码提示符，然后显示每个准备下载的.bak文件。

解除、升级和恢复

按场景3中的说明按以下顺序解散集群：连接的节点、复制副本和主最后一个。使用database cluster remove确认每个节点都已离开集群。

并行升级独立节点。从控制台恢复网络编址（首次引导和网络恢复部分）。

上传每个节点自己的加密备份。在回滚之前，请确认上传的快照在备份列表中显示为已加密：yes.首先恢复前一个主节点，然后恢复副本和连接的节点。使用下面的backup rollback命令，确认Y，并在出现提示时输入备份的口令。接受口令后，节点将重新启动。对每个节点重复上述步骤。

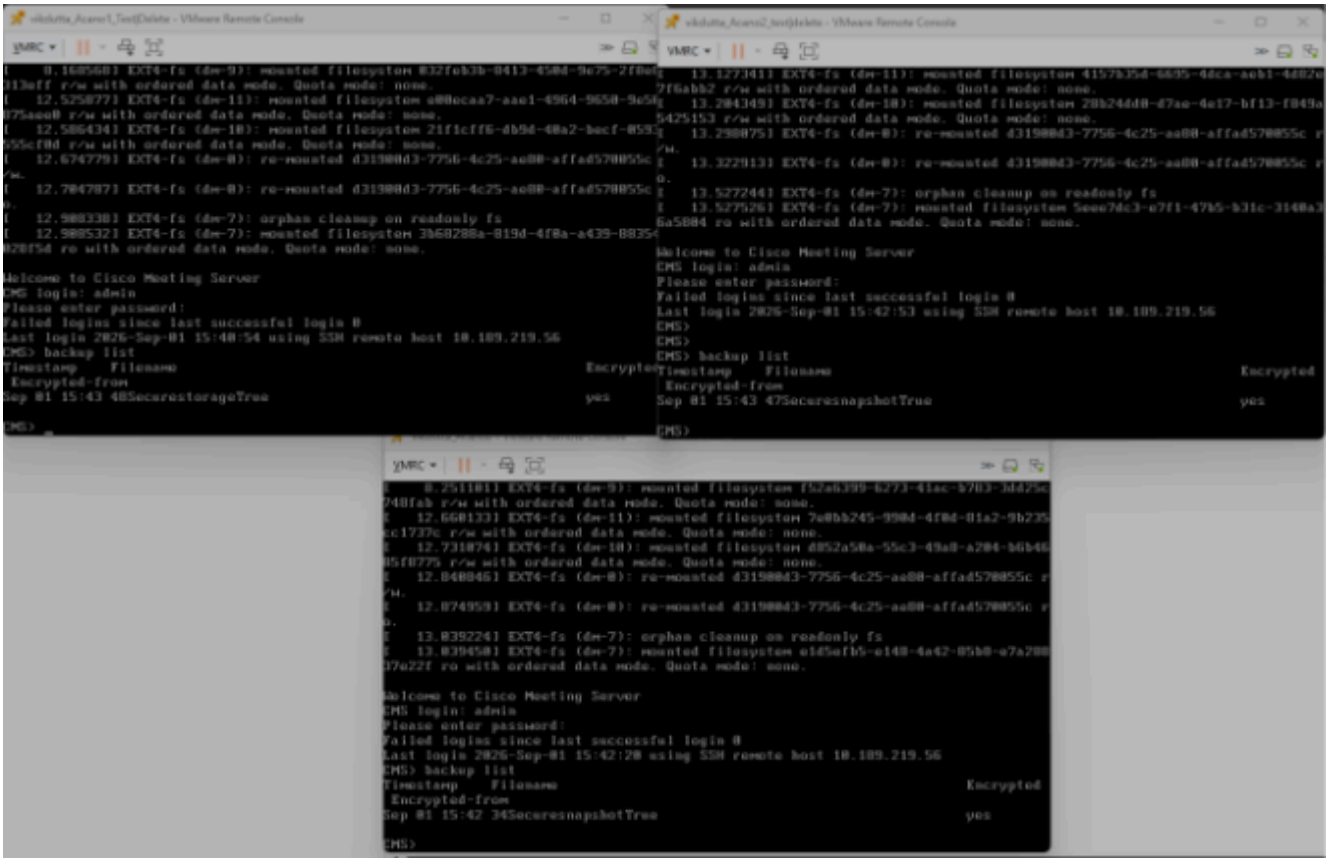


图 37：在第一次4.0启动后，上传的快照必须在备份列表中显示为Encrypted:是，并准备好回滚。

backup rollback encrypted-filename

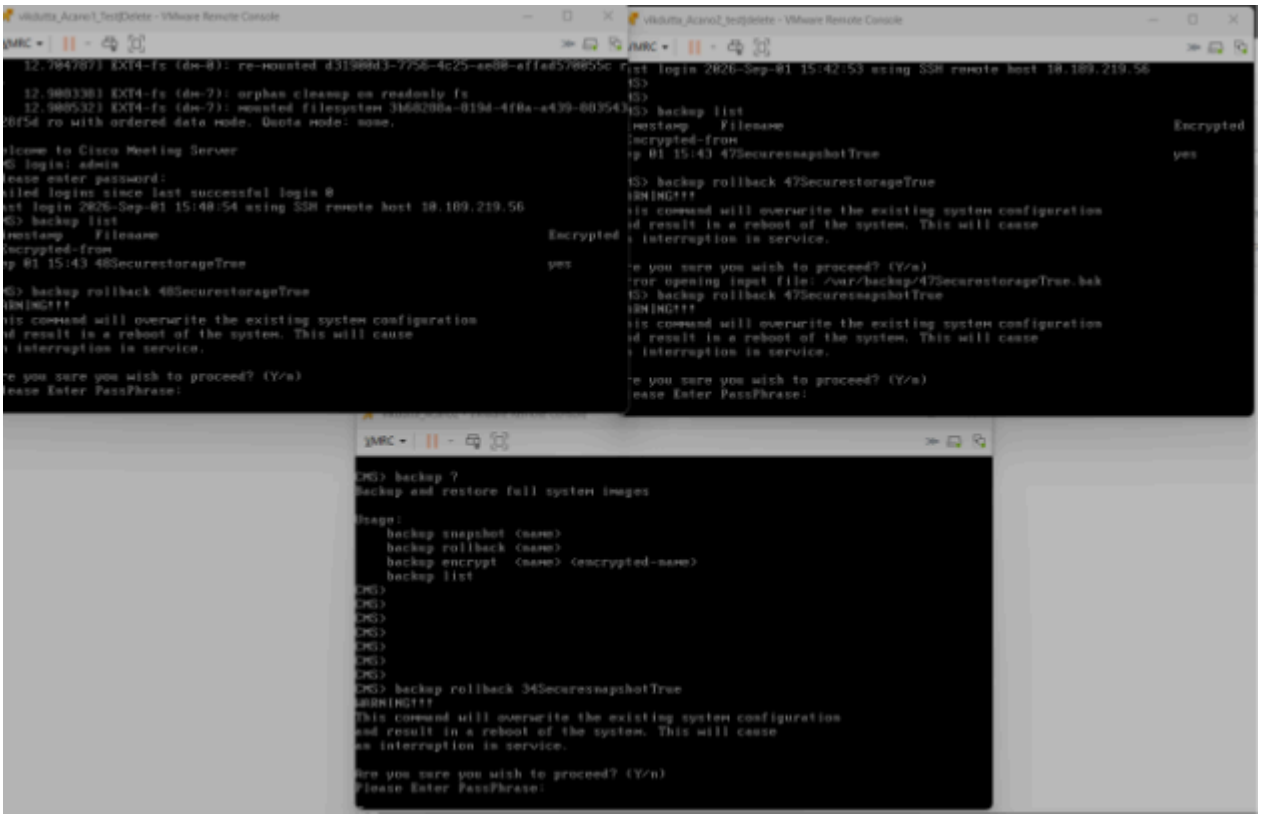


图 38：确认Y，输入密码，然后首先恢复前一个主密码。

注意：如果在此恢复后呼叫网桥集群连接未启动，请仅在前一个主上运**database cluster upgrade_schema**行，然后重新检查呼叫网桥状态。

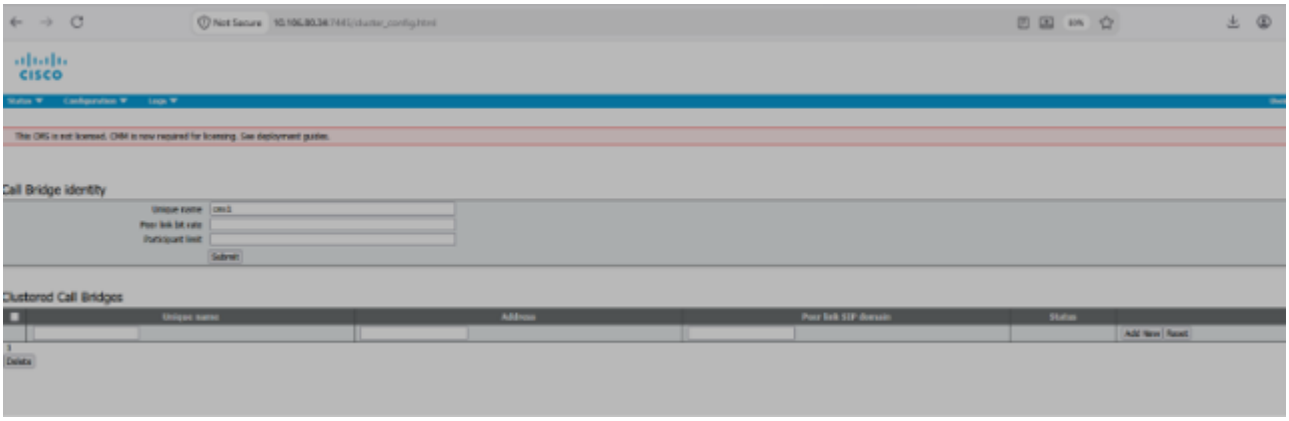


图 39：在模式升级之前，该示例显示当集群呼叫网桥为空时正在运行的数据库集群。

database cluster upgrade_schema

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

图 40：在前一个主上，只有在此已解散集群升级后Call Bridge集群连接失败时才确认Y。

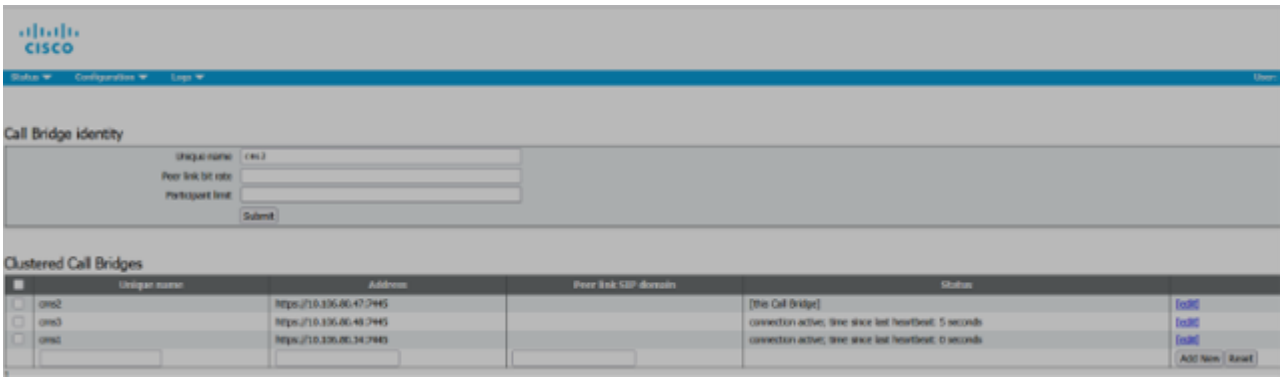


图 41：在模式升级后，验证每个呼叫网桥对等体是否显示活动连接。

在每个Web网桥的MeetingApps Secret Key After Restore部分中完成MeetingApps加密过程，然后使用Post-upgrade Validation部分验证部署。

升级后验证

在恢复后和使系统恢复生产之前，请完成以下核对表：

- 每个节点上的Web Admin显示思科会议服务器4.0。
- 所需的MMP服务已启用并正在运行(活动：正确)。
- 故障情况很明显。将最近的错误和警告视为信息性错误，除非存在相应的故障。
- 如果适用，数据库群集状态将显示预期的主副本和副本。
- 智能许可和呼叫网桥连接已恢复。
- 此部署支持的SIP呼叫和Web应用客户端呼叫已成功完成。
- 如果升级前要求部分中从服务器复制的品牌、音频提示和SSO文件尚未包含在备份中，则这些文件会被还原。
- 如果部署了MeetingApps，Web Bridge将显示新的MeetingApps关系和文件共享工作。
- 仅在接受部署后删除短期快照。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。