



## 备份系统

---

- [备份概述，第 1 页](#)
- [备份前提条件，第 1 页](#)
- [备份任务流程，第 2 页](#)
- [备份相互作用和限制，第 7 页](#)

### 备份概述

Cisco 建议定期执行备份。您可以使用灾难恢复系统 (DRS) 为群集中的所有服务器执行完整数据备份。您可以设置自动备份或随时调用备份。

灾难恢复系统执行群集层级备份，这意味着它会将一个 Cisco Unified Communications Manager 群集中所有服务器的备份收集到中心位置，并将备份数据存档到物理存储设备。备份文件已加密，并且只能由系统软件打开。

DRS 恢复其自己的设置（备份设备设置和计划设置）作为平台备份/恢复的一部分。DRS 备份和恢复 drfDevice.xml 和 drfSchedule.xml 文件。使用这些文件恢复服务器时，您无需重新配置 DRS 备份设备和计划。

当您执行系统数据恢复时，可以选择要恢复群集中的哪些节点。

灾难恢复系统包括以下功能：

- 用于执行备份和恢复任务的用户界面。
- 用于执行备份功能的分布式系统架构。
- 计划的备份或手动（用户调用）备份。
- 它会将备份存档到远程 sftp 服务器。

### 备份前提条件

- 确保您符合版本要求：

- 所有 Cisco Unified Communications Manager 群集节点都必须运行相同版本的 Cisco Unified Communications Manager 应用程序。
- 所有 IM and Presence Service 群集节点都必须运行相同版本的 IM and Presence Service 应用程序。
- 备份文件中保存的软件版本必须与群集节点上运行的版本匹配。

整个版本字符串必须匹配。例如，如果 IM and Presence 数据库发布方节点上的版本为 11.5.1.10000-1，则所有 IM and Presence 订阅方节点都必须是 11.5.1.10000-1，并且备份文件也必须是 11.5.1.10000-1。如果您尝试从与当前版本不匹配的备份文件恢复系统，恢复将失败。无论何时升级软件版本，都请确保备份系统，以使备份文件中保存的版本与群集节点上运行的版本匹配。

- 请注意，DRS 加密取决于群集安全密码。运行备份时，DRS 会生成一个随机密码用于加密，然后使用群集安全密码对随机密码进行加密。如果在备份与此次恢复之间，群集安全密码发生了更改，那么您需要知道备份时的密码是什么，才能使用该备份文件恢复系统，或者，在安全密码更改/重置后立即进行备份。
- 如果想要备份到远程设备，请确保您拥有 SFTP 服务器设置。有关可用 SFTP 服务器的详细信息，请参阅 [用于远程备份的 SFTP 服务器](#)，第 8 页

## 备份任务流程

完成这些任务以配置和运行备份。备份正在运行时，不要执行任何操作系统管理任务。这是因为灾难恢复系统会通过锁定平台 API 来阻止所有操作系统管理请求。但是，灾难恢复系统不会阻止大多数 CLI 命令，因为只有基于 CLI 的升级命令使用平台 API 锁定软件包。

### 过程

	命令或操作	目的
步骤 1	<a href="#">配置备份设备</a> ，第 3 页	指定要在其上备份数据的设备。
步骤 2	<a href="#">估算备份文件的大小</a> ，第 4 页	估计在 SFTP 设备上创建的备份文件的大小。
步骤 3	选择下列选项之一： <ul style="list-style-type: none"> <li>• <a href="#">配置计划的备份</a>，第 4 页</li> <li>• <a href="#">开始手动备份</a>，第 6 页</li> </ul>	创建一个备份计划以按计划备份数据。 或者，也可以运行手动备份。
步骤 4	<a href="#">查看当前备份状态</a> ，第 6 页	可选。检查备份的状态。备份运行时，您可以检查当前备份作业的状态。
步骤 5	<a href="#">查看备份历史记录</a> ，第 7 页	可选。查看备份历史记录

## 配置备份设备

最多可以配置 10 个备份设备。执行以下步骤以配置要存储备份文件的位置。

### 开始之前

- 确保您对 SFTP 服务器中的目录路径拥有写入访问权限，以存储备份文件。
- 确保用户名、密码、服务器名称和目录路径有效，因为 DRS Master Agent 会验证备份设备的配置。



**注释** 计划在预期网络通信量较少的时段期间进行备份。

### 过程

**步骤 1** 从灾难恢复系统中，选择**备份 > 备份设备**。

**步骤 2** 在**备份设备列表**窗口中，执行以下任一操作：

- 要配置新设备，请单击**新增**。
- 要编辑现有的备份设备，请输入搜索条件，单击“**查找**”，然后单击**选定编辑**。
- 要删除备份设备，请在**备份设备**列表中将其选中，然后单击**删除选定项**。

您无法删除配置为备份计划中备份设备的备份设备。

**步骤 3** 在**备份设备名称**字段中输入备份名称。

备份设备名称只能包含字母数字字符、空格 ()、破折号 (-) 和下划线 (\_)。请勿使用任何其他字符。

**步骤 4** 在**网络目录**下方的**选择目标区域**中，执行以下操作：

- 在**主机名/IP 地址**字段中，输入网络服务器的主机名或 IP 地址。
- 在**路径名**字段中，输入您要存储备份文件的目录路径。
- 在**用户名**字段，输入有效的用户名。
- 在**密码**字段中，输入有效的密码。
- 从**要存储在网络目录上的备份数量**下拉列表中，选择所需的备份数量。

**步骤 5** 单击**保存**。

### 下一步做什么

[估算备份文件的大小，第 4 页](#)

## 估算备份文件的大小

只有当存在一个或多个选定功能的备份历史记录时，Cisco Unified Communications Manager 才会估算备份 tar 的大小。

计算出的大小并非精确值，而是备份 tar 的估计大小。系统会根据上一次成功备份的实际备份大小来计算，如果自上次备份后配置发生了更改，则大小可能会有所变化。

仅当存在先前的备份时，您才能使用此程序。若是第一次备份系统，则不可使用此程序。

按照此程序来估计保存到 SFTP 设备的备份 tar 的大小。

### 过程

---

**步骤 1** 从灾难恢复系统中，选择**备份 > 手动备份**。

**步骤 2** 在**选择功能区域**中，选择要备份的功能。

**步骤 3** 单击**估计大小**以查看所选功能备份的估计大小。

---

### 下一步做什么

执行以下程序之一以备份您的系统：

- [配置计划的备份，第 4 页](#)
- [开始手动备份，第 6 页](#)

## 配置计划的备份

最多可以创建 10 个备份计划。每个备份计划都有自己的一组属性，包括自动备份计划、要备份的功能集和存储位置。

请注意，您的备份 .tar 文件已使用随机生成的密码加密。然后会使用群集安全密码对此密码进行加密，并随备份 .tar 文件一起保存。您必须记住此安全密码，或在安全密码更改或重置后立即进行备份。



---

**注意** 计划在非高峰时段备份以避免呼叫处理中断和影响服务。

---

### 开始之前

[配置备份设备，第 3 页](#)

## 过程

---

**步骤 1** 从灾难恢复系统中，选择**备份计划程序**。

**步骤 2** 在**计划列表**窗口中，执行以下步骤之一以添加新的计划或编辑一个现有的计划。

- 要创建新的计划，单击**新增**。
- 要配置现有的计划，单击“计划列表”列中的名称。

**步骤 3** 在**计划程序**窗口中，在**计划名称**字段中输入计划名称。

**注释** 您无法更改默认计划的名称。

**步骤 4** 在**选择备份设备**区域选择备份设备。

**步骤 5** 在**选择功能**区域选择要备份的功能。必须至少选择一项功能。

**步骤 6** 在**开始备份时间**区域选择您希望开始备份的日期和时间。

**步骤 7** 在**频率**区域选择您希望进行备份的频率。频率可以设置为“每天一次”、“每周”和“每月”。如果选择**每周**，您还可以选择一周内哪几天进行备份。

**提示** 要将备份频率设置为**每周**，从星期二到星期六进行备份，可单击**设置默认值**。

**步骤 8** 要更新这些设置，单击**保存**。

**步骤 9** 选择下列选项之一：

- 要启用所选的计划，单击**启用所选计划**。
- 要禁用所选的计划，单击**禁用所选计划**。
- 要删除所选的计划，单击**删除选定项**。

**步骤 10** 要启用计划，单击**启用计划**。

下次备份将在您设置的时间自动进行。

**注释** 确保群集中的所有服务器都运行相同版本的 Cisco Unified Communications Manager 或 Cisco IM and Presence Service，并可通过网络接通。在计划的备份时间无法接通的服务器将不会备份。

---

## 下一步做什么

执行以下程序：

- [估算备份文件的大小，第 4 页](#)
- (可选) [查看当前备份状态，第 6 页](#)

## 开始手动备份

### 开始之前

- 确保使用网络设备作为备份文件的存储位置。Unified Communications Manager 的虚拟化部署不支持使用磁带驱动器存储备份文件。
- 确保所有群集节点都安装有相同的 Cisco Unified Communications Manager 版本或 IM and Presence Service。
- 备份过程可能会由于远程服务器上没有可用空间或由于网络连接中断而失败。在解决导致备份失败的问题后，您需要开始一个全新备份。
- 确保没有网络中断。
- [配置备份设备，第 3 页](#)
- [估算备份文件的大小，第 4 页](#)
- 确保您有群集安全密码记录。如果在完成此备份之后，群集安全密码发生了更改，您需要知道密码，否则将无法使用备份文件来恢复您的系统。



---

**注释** 备份运行时，您无法在“Cisco Unified 操作系统管理”或“Cisco Unified IM and Presence 操作系统管理”中执行任何任务，因为灾难恢复系统会锁定平台 API 来阻止所有请求。但是，灾难恢复系统不会阻止大多数 CLI 命令，因为只有基于 CLI 的升级命令使用平台 API 锁定软件包。

---

### 过程

- 
- 步骤 1** 从灾难恢复系统中，选择**备份 > 手动备份**。
  - 步骤 2** 在**手动备份**窗口中，从**备份设备名称**区域选择备份设备。
  - 步骤 3** 从**选择功能**区域选择一项功能。
  - 步骤 4** 单击**开始备份**。
- 

### 下一步做什么

(可选) [查看当前备份状态，第 6 页](#)

## 查看当前备份状态

执行以下步骤以检查当前备份作业的状态。



**注意** 请注意，如果备份到远程服务器没有在 20 小时内完成，备份会话将超时，您必须开始一个全新备份。

#### 过程

**步骤 1** 从灾难恢复系统中，选择**备份 > 当前状态**。

**步骤 2** 要查看备份日志文件，请单击日志文件名链接。

**步骤 3** 要取消当前备份，请单击**取消备份**。

**注释** 备份将在当前组件完成其备份操作后取消。

#### 下一步做什么

[查看备份历史记录，第 7 页](#)

## 查看备份历史记录

如要查看备份历史记录，请执行以下步骤。

#### 过程

**步骤 1** 从灾难恢复系统中，选择**备份 > 历史记录**。

**步骤 2** 从**备份历史记录**窗口中，您可以查看已执行的备份，包括文件名、备份设备、完成日期、结果、版本、已备份的功能，以及失败的功能。

**注释** 备份历史记录窗口只显示最近 20 次备份作业。

## 备份相互作用和限制

• [备份限制，第 8 页](#)

## 备份限制

以下限制适用于备份:

表 1: 备份限制

限制	说明
群集安全密码	我们建议您每当更改群集安全密码时都运行备份。  备份加密使用群集安全密码加密备份文件上的数据。如果在创建备份文件后编辑群集安全密码，您将无法使用该备份文件恢复数据，除非您记得旧密码。
证书管理	灾难恢复系统 (DRS) 使用 Master Agent 与 Local Agent 之间基于 SSL 的通信，验证和加密 Cisco Unified Communications Manager 群集节点之间的数据。DRS 使用 IPsec 证书进行其公钥/私钥加密。请注意，如果您从“证书管理”页面删除 IPSEC 信任存储库 (hostname.pem) 文件，DRS 将不会按预期工作。如果您手动删除 IPSEC-信任文件，必须确保将 IPSEC 证书上传到 IPSEC-信任。有关详细信息，请参阅《Cisco Unified Communications Manager 安全指南》中的“证书管理”部分，该文档位于 <a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a> 。

## 用于远程备份的 SFTP 服务器

要在网络上将数据备份到远程设备，您必须有经过配置的 SFTP 服务器。对于内部测试，Cisco 使用 Cisco Prime Collaboration Deployment (PCD) 上的 SFTP 服务器（由 Cisco 打造，Cisco TAC 提供支持）。参阅下表可大致了解 SFTP 服务器的选项：

使用下表中的信息来确定要在您的系统中使用哪种 SFTP 服务器解决方案。

表 2: SFTP 服务器信息

SFTP 服务器	信息
Cisco Prime Collaboration 部署上的 SFTP 服务器	此服务器是 Cisco 提供和测试的唯一 SFTP 服务器，并且完全受 Cisco TAC 支持。  版本兼容性取决于您的 Unified Communications Manager 版本和 Cisco Prime Collaboration 部署。在升级其版本 (SFTP) 或 Unified Communications Manager 之前，请参阅《Cisco Prime Collaboration 部署管理指南》，以确保版本兼容。



SFTP 服务器	信息
来自技术合作伙伴的 SFTP 服务器	这些服务器由第三方提供，第三方测试。版本兼容性取决于第三方测试。如果升级其 SFTP 产品和/或升级版本兼容的 Unified Communications Manager，请参阅“技术合作伙伴”页面： <a href="https://marketplace.cisco.com">https://marketplace.cisco.com</a>
来自其他第三方的 SFTP 服务器	这些服务器由第三方提供，不受 Cisco TAC 官方支持。 版本兼容性乃尽力提供，以建立兼容的 SFTP 版本和 Unified Communications Manager 版本。  <b>注释</b> 这些产品未经 Cisco 测试，我们无法保证其功能。Cisco TAC 不支持这些产品。要获取经过全面测试且受支持的 SFTP 解决方案，请使用 Cisco Prime Collaboration 部署或技术合作伙伴。

### 加密支持

对于 Unified Communications Manager 11.5，Unified Communications Manager 会为 SFTP 连接通告以下 CBC 密码：

- aes128-cbc
- 3des-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr



**注释** 确保备份 SFTP 服务器支持其中一个密码以与 Unified Communications Manager 进行通信。

从 Unified Communications Manager 12.0 版起，不支持 CBC 密码。Unified Communications Manager 仅支持和通告以下 CTR 密码：

- aes256-ctr
- aes128-ctr
- aes192-ctr



**注释** 确保备份 SFTP 服务器支持其中一个 CTR 密码与 Unified Communications Manager 进行通信。

