配置托管文件传输

托管文件传输概述

托管文件传输 (MFT) 可让 IM and Presence Service 客户端（例如 Cisco Jabber）将文件传输到其他用户、临时群聊室和永久聊天室。 文件将存储于外部文件服务器上的库中，事务将记录到外部数据库。

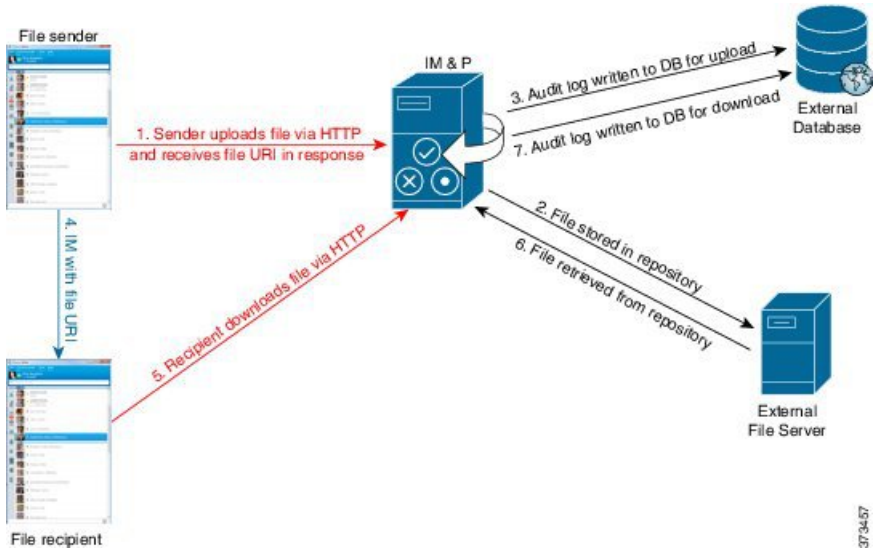
要部署托管文件传输功能，您必须部署以下服务器：

- **外部数据库**—所有文件传输都记录到外部数据库。
- **外部文件服务器**—每个传输文件的副本将保存到外部文件服务器的存储库中。

注释 此配置对于文件传输特定，并对实现法规遵从性的消息存档程序无影响。

有关使用案例，请参阅 托管文件传输呼叫流程， 第 2 页

托管文件传输呼叫流程



1. 发送者通过 HTTP 将文件上传到 IM and Presence 服务器，服务器使用文件的 URI 进行响应。
2. IM and Presence Service 服务器将文件发送到文件服务器存储库以进行存储。
3. IM and Presence Service 会向外部数据库记录表中写入一个条目，以记录此上传。
4. 发件人向接收者发送 IM。 IM 中包含文件的 URI。
5. 接收者将 HTTP 请求发送到 IM and Presence Service 以获取该文件。 IM and Presence Service 会从存储库 (6) 读取文件、将下载记录在日志表中 (7) 并将文件发送给接收者。

将文件传输到群聊或永久聊天室的流程较为相似，除了发送者向聊天室发送 IM，每个聊天室参与者发送单独的请求以下载文件。

注释 发生文件上传时，将从给定域的企业中可用的所有托管文件传输服务中选择托管文件传输服务。 文件上传将记录到外部数据库和与运行此托管文件传输服务的节点相关联的外部文件服务器。 当用户下载此文件时，相同的托管文件传输服务将处理请求，并将其记录到同一外部数据库和同一外部文件服务器，与此第二位用户驻留的位置无关。

托管文件传输前提条件

- 您还必须部署一个外部数据库和外部文件服务器。
- 确保所有服务器能够解析所分配到的 IM and Presence Service 节点上的完整 FQDN。 要让托管文件传输正常工作，必须保证这一点。

外部数据库前提条件

提示 如果您还要部署永久聊天和/或消息归档程序，可以为所有功能分配相同的外部数据库和文件服务器。 确保在确定服务器容量时考虑潜在的 IM 流量、传输的文件数和文件大小。

安装并配置外部数据库。 有关详细信息，包括受支持的数据库，请参阅《*IM and Presence Service* 数据库设置指南》。

此外，请遵循以下原则：

- IM and Presence Service 群集中每个 IM and Presence Service 节点需要一个唯一的逻辑外部数据库实例。
- 虚拟化和非虚拟化平台均支持外部数据库。
- 有关所记录元数据的完整列表，请参阅《*Cisco Unified Communications Manager* 上 *IM and Presence Service* 的数据库设置》“外部数据库工具”一章中的 AFT_LOG 表。
- 如果您是使用 IPv6 连接至外部数据库，则查阅配置 IPv6 任务流程以获取有关设置 IPv6 的详细信息。

外部文件服务器要求

设置外部文件服务器时，请遵循以下原则：

- 根据文件服务器容量的不同，每个 IM and Presence Service 节点都要求有其唯一的 Cisco XCP 文件传输管理器文件服务器目录，但是不同的节点可共享相同的物理文件服务器安装。
- 文件服务器必须支持 ext4 文件系统、SSHv2 和 SSH 工具。
- 文件服务器必须支持 4.9、6.x 和 7.x 的 OpenSSH 版本。

重要事项 此备注适用于 14SU3 及更高版本。

注释 从版本 14SU3 开始支持 OpenSSH 版本 8.x。

- IM and Presence Service 与外部文件服务器之间的网络吞吐量必须大于每秒 60 兆字节。

  启用托管文件传输之后，您可以使用 `show fileserver transferspeed` CLI 命令来确定您的文件服务器传输速度。 请注意，如果在系统繁忙时运行此命令，可能会影响该命令返回的值。 如需有关此命令的更多详细信息，请单击此链接查阅《*Cisco Unified Communications* 解决方案的命令行界面指南》。

外部文件服务器的分区建议

思科建议您创建一个或多个单独的文件传输存储专用的分区，因此服务器上运行的其他应用程序不会对其写入数据。 应在这些分区上创建所有文件存储目录。

请考虑以下方面：

- 在创建分区时，请务必注意 IM and Presence Service 的默认文件大小设置 (0) 允许传输的最大文件容量为 4GB。 此设置可在您设置托管文件传输时降低。
- 考虑每天上传的数量和平均文件大小。
- 确保分区拥有足够的磁盘空间承载预期文件容量。
- 例如，12000 名用户每小时传输 2 个文件，每个文件的平均大小为 100KB，则一天 8 小时的总容量为 19.2GB。

外部文件服务器目录结构

发生首个文件传输时，系统将按照本示例中所描述的自动创建带有时间戳的子目录：

- 我们会在 IM and Presence Service 节点上创建路径 `/opt/mftFileStore/node_1/`。
- 目录 `/files/` 会自动生成。
- 三个 `/chat_type/` 目录（`im`、`persistent`、`groupchat`）会自动生成。
- 日期目录 `/YYYYMMDD/` 会自动生成。
- 小时目录 `/HH/` 会自动生成。 如果一小时内传输超过 1,000 个文件，则将创建一个额外的翻转目录 `/HH.n/`。
- 系统将采用自动生成的编码资源名称保存文件，以下称为 `file_name`。

在此示例中，文件的完整路径为：`/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name`

使用我们的示例路径：

- 2014 年 8 月 11 日 15:00 到 15:59 UTC 间一对一 IM 过程中传输的文件位于以下目录：`/opt/mftFileStore/node_1/files/im/20140811/15/file_name`

  2014 年 8 月 11 日 16:00 到 16:59 UTC 间永久群聊过程中传输的文件位于以下目录：`/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`
- 2014 年 8 月 11 日 16:00 到 16:59 UTC 间临时聊天过程中传输的第 1001 个文件位于以下目录：`/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- 如果一小时内未发生文件传输，则没有为该时间段创建的目录。

注释 M and Presence 服务和文件服务器间的流量已使用 SSHFS 加密，但写入到文件服务器的文件内容采用未加密形式。

外部文件服务器用户验证

IM and Presence Service 使用 SSH 密钥验证自身和文件服务器：

- IM and Presence Service 公钥存储于文件服务器上。
- 连接过程中，SSHFS 将验证 IM and Presence Service 私钥。 这样可确保所有文件的内容均已加密。
- 文件服务器公钥存储于 IM and Presence Service 上。 这可让 IM and Presence Service 确保其连接到配置的文件服务器，并最大程度减少中间人攻击。

注释 节点公钥将在节点分配删除后失效。 如果重新分配节点，系统将自动生成一个新的节点公钥，且必须在外部文件服务器上重新配置密钥。

外部文件服务器要求

设置外部文件服务器时，请遵循以下原则：

- 根据文件服务器容量的不同，每个 IM and Presence Service 节点都要求有其唯一的 Cisco XCP 文件传输管理器文件服务器目录，但是不同的节点可共享相同的物理文件服务器安装。
- 文件服务器必须支持 ext4 文件系统、SSHv2 和 SSH 工具。
- 文件服务器必须支持 4.9、6.x 和 7.x 的 OpenSSH 版本。

重要事项 此备注适用于 14SU3 及更高版本。

注释 从版本 14SU3 开始支持 OpenSSH 版本 8.x。

- IM and Presence Service 与外部文件服务器之间的网络吞吐量必须大于每秒 60 兆字节。

  启用托管文件传输之后，您可以使用 `show fileserver transferspeed` CLI 命令来确定您的文件服务器传输速度。 请注意，如果在系统繁忙时运行此命令，可能会影响该命令返回的值。 如需有关此命令的更多详细信息，请单击此链接查阅《*Cisco Unified Communications* 解决方案的命令行界面指南》。

外部文件服务器的分区建议

思科建议您创建一个或多个单独的文件传输存储专用的分区，因此服务器上运行的其他应用程序不会对其写入数据。 应在这些分区上创建所有文件存储目录。

请考虑以下方面：

- 在创建分区时，请务必注意 IM and Presence Service 的默认文件大小设置 (0) 允许传输的最大文件容量为 4GB。 此设置可在您设置托管文件传输时降低。
- 考虑每天上传的数量和平均文件大小。
- 确保分区拥有足够的磁盘空间承载预期文件容量。
- 例如，12000 名用户每小时传输 2 个文件，每个文件的平均大小为 100KB，则一天 8 小时的总容量为 19.2GB。

外部文件服务器目录结构

发生首个文件传输时，系统将按照本示例中所描述的自动创建带有时间戳的子目录：

- 我们会在 IM and Presence Service 节点上创建路径 `/opt/mftFileStore/node_1/`。
- 目录 `/files/` 会自动生成。
- 三个 `/chat_type/` 目录（`im`、`persistent`、`groupchat`）会自动生成。
- 日期目录 `/YYYYMMDD/` 会自动生成。
- 小时目录 `/HH/` 会自动生成。 如果一小时内传输超过 1,000 个文件，则将创建一个额外的翻转目录 `/HH.n/`。
- 系统将采用自动生成的编码资源名称保存文件，以下称为 `file_name`。

在此示例中，文件的完整路径为：`/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name`

使用我们的示例路径：

- 2014 年 8 月 11 日 15:00 到 15:59 UTC 间一对一 IM 过程中传输的文件位于以下目录：`/opt/mftFileStore/node_1/files/im/20140811/15/file_name`

  2014 年 8 月 11 日 16:00 到 16:59 UTC 间永久群聊过程中传输的文件位于以下目录：`/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`
- 2014 年 8 月 11 日 16:00 到 16:59 UTC 间临时聊天过程中传输的第 1001 个文件位于以下目录：`/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- 如果一小时内未发生文件传输，则没有为该时间段创建的目录。

注释 M and Presence 服务和文件服务器间的流量已使用 SSHFS 加密，但写入到文件服务器的文件内容采用未加密形式。

外部文件服务器用户验证

IM and Presence Service 使用 SSH 密钥验证自身和文件服务器：

- IM and Presence Service 公钥存储于文件服务器上。
- 连接过程中，SSHFS 将验证 IM and Presence Service 私钥。 这样可确保所有文件的内容均已加密。
- 文件服务器公钥存储于 IM and Presence Service 上。 这可让 IM and Presence Service 确保其连接到配置的文件服务器，并最大程度减少中间人攻击。

注释 节点公钥将在节点分配删除后失效。 如果重新分配节点，系统将自动生成一个新的节点公钥，且必须在外部文件服务器上重新配置密钥。

外部文件服务器的分区建议

思科建议您创建一个或多个单独的文件传输存储专用的分区，因此服务器上运行的其他应用程序不会对其写入数据。 应在这些分区上创建所有文件存储目录。

请考虑以下方面：

- 在创建分区时，请务必注意 IM and Presence Service 的默认文件大小设置 (0) 允许传输的最大文件容量为 4GB。 此设置可在您设置托管文件传输时降低。
- 考虑每天上传的数量和平均文件大小。
- 确保分区拥有足够的磁盘空间承载预期文件容量。
- 例如，12000 名用户每小时传输 2 个文件，每个文件的平均大小为 100KB，则一天 8 小时的总容量为 19.2GB。

外部文件服务器用户验证

IM and Presence Service 使用 SSH 密钥验证自身和文件服务器：

- IM and Presence Service 公钥存储于文件服务器上。
- 连接过程中，SSHFS 将验证 IM and Presence Service 私钥。 这样可确保所有文件的内容均已加密。
- 文件服务器公钥存储于 IM and Presence Service 上。 这可让 IM and Presence Service 确保其连接到配置的文件服务器，并最大程度减少中间人攻击。

注释 节点公钥将在节点分配删除后失效。 如果重新分配节点，系统将自动生成一个新的节点公钥，且必须在外部文件服务器上重新配置密钥。

外部文件服务器目录结构

发生首个文件传输时，系统将按照本示例中所描述的自动创建带有时间戳的子目录：

- 我们会在 IM and Presence Service 节点上创建路径 `/opt/mftFileStore/node_1/`。
- 目录 `/files/` 会自动生成。
- 三个 `/chat_type/` 目录（`im`、`persistent`、`groupchat`）会自动生成。
- 日期目录 `/YYYYMMDD/` 会自动生成。
- 小时目录 `/HH/` 会自动生成。 如果一小时内传输超过 1,000 个文件，则将创建一个额外的翻转目录 `/HH.n/`。
- 系统将采用自动生成的编码资源名称保存文件，以下称为 `file_name`。

在此示例中，文件的完整路径为：`/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name`

使用我们的示例路径：

- 2014 年 8 月 11 日 15:00 到 15:59 UTC 间一对一 IM 过程中传输的文件位于以下目录：`/opt/mftFileStore/node_1/files/im/20140811/15/file_name`

  2014 年 8 月 11 日 16:00 到 16:59 UTC 间永久群聊过程中传输的文件位于以下目录：`/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`
- 2014 年 8 月 11 日 16:00 到 16:59 UTC 间临时聊天过程中传输的第 1001 个文件位于以下目录：`/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- 如果一小时内未发生文件传输，则没有为该时间段创建的目录。

注释 M and Presence 服务和文件服务器间的流量已使用 SSHFS 加密，但写入到文件服务器的文件内容采用未加密形式。

托管文件传输任务流程

完成以下任务以在 IM and Presence Service 上设置托管文件传输功能，并设置外部文件服务器。

开始之前

为托管文件传输设置外部数据库和外部文件服务器。有关要求，请参阅

- 外部数据库前提条件，第 3 页
- 外部文件服务器要求，第 3 页

有关如何配置外部数据库的详细信息，请参阅《*IM and Presence Service* 外部数据库设置指南》，网址：https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。

过程

	命令或操作	目的
步骤 1	添加外部数据库连接，第 9 页	从 IM and Presence Service 配置与外部数据库的连接。
步骤 2	设置外部文件服务器，第 10 页	在文件服务器上设置用户、目录、所有权、权限和其他任务前，设置外部文件服务器。
步骤 3	为外部文件服务器创建用户，第 11 页	为外部文件服务器设置用户。
步骤 4	设置外部文件服务器目录，第 12 页	设置外部文件服务器的顶级目录结构。
步骤 5	获取外部文件服务器公钥，第 13 页	获取外部文件服务器的公钥。
步骤 6	在 IM and Presence Service 上设置外部文件服务器，第 14 页	获取外部文件服务器的以下信息：
步骤 7	验证 Cisco XCP 文件传输管理器激活，第 16 页	Cisco XCP 文件传输管理器服务必须在启用了托管文件传输的各个节点上处于活动状态。
步骤 8	启用托管文件传输，第 17 页	在 IM and Presence Service 上启用托管文件传输。
步骤 9	验证外部服务器状态，第 18 页	验证并确保外部数据库设置和外部文件服务器设置不存在任何问题。

添加外部数据库连接

从 IM and Presence Service 配置与外部数据库的连接。使用托管文件传输时，您需要为每个 IM and Presence Service 群集节点提供唯一的逻辑外部数据库实例。

开始之前

设置每个外部数据库。有关详细信息，请参阅《*IM and Presence Service* 外部数据库设置指南》，网址：

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

过程

步骤 1 在 Cisco Unified CM IM and Presence 管理中，选择**消息** > **外部服务器设置** > **外部数据库**。
步骤 2 单击**新增**。
步骤 3 在**数据库名称**字段中，输入外部数据库实例的名称。
步骤 4 在**数据库类型**下拉列表中，选择您要部署的外部数据库的类型。
步骤 5 输入数据库的**用户名**和**密码信息**。
步骤 6 在**主机名**字段中，输入数据库的主机名和 IP 地址。
步骤 7 完成**外部数据库设置**窗口的剩余设置。有关这些字段及其设置的帮助，请参阅联机帮助。
步骤 8 单击**保存**。
步骤 9 重复此程序以创建到每个外部数据库实例的连接。

设置外部文件服务器

在文件服务器上设置用户、目录、所有权、权限和其他任务前，设置外部文件服务器。

开始之前

查看对外部文件服务器的设计建议。 有关详细信息，请参阅外部文件服务器要求，第 3 页。

过程

步骤 1 安装支持的 Linux 版本。
步骤 2 以根用户输入以下命令，验证文件服务器是否支持 SSHv2 和 OpenSSH 4.9 或更高版本：

```
# telnet localhost 22
Trying ::1...
Connected to localhost.
Escape character is '^]'.
SSH-2.0-OpenSSH_5.3
```

或者

```
# ssh -v localhost
OpenSSH_5.3p1, OpenSSL 1.0.0-fips 29 Mar 2010
debug1: Reading configuration data /root/.ssh/config ...
...debug1: Local version string SSH-2.0-OpenSSH_5.3
```

...

步骤 3 为允许私钥/公钥验证，请确保您在 `/etc/ssh/sshd_config` 文件中将以下字段设置为是。

- RSAAuthentication *yes*
- PubkeyAuthentication *yes*

如果文件中已对此加以注释，则可忽略这些设置。

提示 为增强安全性，您也可为文件传输用户禁用密码日志（在我们的示例中为 *mftuser*）。这将仅允许使用 SSH 公钥/私钥身份验证登录。

步骤 4 思科建议您创建一个或多个单独的文件传输存储专用的分区，因此服务器上运行的其他应用程序不会对其写入数据。 应在这些分区上创建所有文件存储目录。

下一步做什么

为外部文件服务器创建用户，第 11 页

为外部文件服务器创建用户

为外部文件服务器设置用户。

开始之前

设置外部文件服务器，第 10 页

过程

步骤 1 在作为根的文件服务器上，为托管文件传输功能创建用户。 此用户拥有文件存储目录结构 (示例使用 *mftuser*）并强制创建主目录 (**-m**)。

```
# useradd -mmftuser
# passwdmftuser
```

步骤 2 切换到托管文件传输用户。

```
# sumftuser
```

步骤 3 在用作密钥库的 *~mftuser* 主目录下创建 `.ssh` 目录。

```
$ mkdir~mftuser/.ssh/
```

步骤 4 在用于为每个启用托管文件传输的节点保存公钥文本的 `.ssh` 目录下创建 `authorized_keys` 文件。

```
$ touch~mftuser/.ssh/authorized_keys
```

步骤 5 为无密码 SSH 设置适当的权限，以让其正常运行。

```
$ chmod 700 ~mftuser（目录）
$ chmod 700 ~/.ssh（目录）
$ chmod 700 ~/.ssh/authorized_keys（文件）
```

注释 在一些 Linux 系统上，这些权限可能根据您 SSH 配置的不同而有所差异。

下一步做什么

设置外部文件服务器目录，第 12 页

设置外部文件服务器目录

设置外部文件服务器的顶级目录结构。

您可使用任何目录名称创建您希望创建的任何目录结构。确保为每个启用了托管文件传输的节点创建一个目录。稍后，当您在 IM and Presence Service 上启用托管文件传输时，必须为每个节点分配一个目录。

重要事项 您必须为启用了托管文件传输的各个节点创建一个目录。

注释 文件服务器分区/目录安装于用于存储文件的 IM and Presence Service 目录中。

开始之前

为外部文件服务器创建用户，第 11 页

过程

步骤 1 切换回根用户。

```
$ exit
```

步骤 2 创建一个顶级目录结构（示例中使用 `/opt/mftFileStore/`）来为启用了托管文件传输的所有 IM and Presence Service 节点托管目录。

```
# mkdir -p /opt/mftFileStore/
```

步骤 3 授予 *mftuser* 对 `/opt/mftFileStore/` 目录的唯一所有权。

```
# chownmftuser:mftuser /opt/mftFileStore/
```

步骤 4 授予 *mftuser* 对 `mftFileStore` 目录的唯一权限。

```
# chmod 700 /opt/mftFileStore/
```

步骤 5 切换到 *mftuser*。

```
# su mftuser
```

步骤 6 在 /opt/mftFileStore/ 下为每个启用了托管文件传输的节点创建一个子目录。（稍后，当您启用托管文件传输时，您将为节点分配各个目录。）

```
$ mkdir /opt/mftFileStore/{node_1,node_2,node_3}
```

注释

- 当您在 Cisco Unified CM IM and Presence 管理中设置文件服务器时，这些目录和路径将在您配置的**外部文件服务器目录**字段中使用。
- 如果您有多个写入到此文件服务器的 IM and Presence Service 节点，则您必须为各个节点定义目标目录，就像我们在示例中为三个节点 {*node_1*,*node_2*,*node_3*} 所做的一样。
- 在每个节点的目录中，传输类型子目录（im、groupchat 和 persistent）由 IM and Presence Service 自动创建，所有后续目录也是如此。

下一步做什么

获取外部文件服务器公钥，第 13 页

获取外部文件服务器公钥

获取外部文件服务器的公钥。

开始之前

设置外部文件服务器目录，第 12 页

过程

步骤 1 要检索文件服务器的公钥，请输入：

```
$ ssh-keyscan -t rsa host
```

其中 *host* 是文件服务器的主机名、FQDN 或 IP 地址。

警告

- 为避免中间人攻击（此时文件服务器公钥具有欺骗性），您必须确认通过 **ssh-keyscan -t rsa***host* 命令返回的公钥值是文件服务器的实际公钥。
- 在文件服务器上，转到 ssh_host_rsa_key.pub 文件的位置（在我们的系统中，其位于 /etc/ssh/ 下），并确认公钥文件的内容减去主机（主机不在文件服务器上的 ssh_host_rsa_key.pub 文件中）与命令 **ssh-keyscan -t rsa***host* 返回的公钥值相匹配。

步骤 2 复制 **ssh-keyscan -t rsa***host* 命令的结果，而不是 ssh_host_rsa_key.pub 文件中的值。 确保复制整个密钥值，从服务器主机名、FQDN 或 IP 地址一直到最后。

注释 在大多数情况中，服务器密钥以主机名或 FQDN 开始，但其也有可能以 IP 地址开始。

例如，应复制：

hostname ssh-rsa AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs...

...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/sdug+/+N9MQ==

（使用了省略号）。

步骤 3 将 **ssh-keyscan -t rsa***host* 命令的结果保存到一个文本文件。 您在 *IM and Presence Service* 上部署外部文件服务器时需要用到该文件。

步骤 4 打开您创建的 authorized_keys 文件并将其保持打开状态。 当您稍后在 IM and Presence Service 上设置文件服务器时需要用到它。

注释 如果您不能检索公钥，请参阅排查外部文件服务器公钥和私钥， 第 19 页获得进一步的帮助。

下一步做什么

在 IM and Presence Service 上设置外部文件服务器， 第 14 页

在 IM and Presence Service 上设置外部文件服务器

您必须为将启用托管文件传输的群集中的每个节点配置一个外部文件服务器实例。

外部文件服务器实例不必是外部文件服务器的物理实例。 但是请注意，对于给定主机名，您必须为各个外部文件服务器实例指定唯一的外部文件服务器目录路径。 您可从一个相同的节点配置所有外部文件服务器实例。

开始之前

获取外部文件服务器公钥， 第 13 页

获取外部文件服务器的以下信息：

- 主机名、FQDN 或 IP 地址
- 公钥
- 文件存储目录的路径
- 用户名

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**消息** > **外部服务器设置** > **外部文件服务器**。

步骤 2 单击**新增**。
此时将显示**外部文件服务器**窗口。

步骤 3 输入服务器详细信息。 有关这些字段及其配置选项的帮助，请参阅外部文件服务器字段 ， 第 15 页。

步骤 4 单击**保存**。

步骤 5 重复此过程，直到为启用托管文件传输的每个群集节点创建了单独的外部文件服务器实例。

下一步做什么

验证 Cisco XCP 文件传输管理器激活 ， 第 16 页

外部文件服务器字段

字段	说明
名称	输入文件服务器的名称。 理想的情况下，服务器名称应具有足够的描述性，从而能立即识别。 最大字符数：128。允许的值包括字母数字、连字符和下划线。
主机/IP 地址	输入文件服务器的主机名或 IP 地址。 **注释** • 为主机/IP 地址字段所输入的值必须与为“外部文件服务器公钥”字段（随后）所输入的密钥开端匹配。 • 如果您更改此设置，则您必须重启 Cisco XCP 路由器服务。

字段	说明
外部文件服务器公钥	将文件服务器公钥（您按桌面保存为文本文件的密钥）粘贴到此字段。 如果您未保存密钥，您可通过在文件服务器上运行以下命令从文件服务器检索该密钥： `$ ssh-keyscan -t rsa`*host*（在文件服务器上）。 其中 *host* 是文件服务器的 IP 地址、主机名或 FQDN。 您必须复制和粘贴从主机名、FQDN 或 IP 地址开始一直到最后的整个密钥文本。 例如，应复制： extFileServer.cisco.com ssh-rsa AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs... ...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/sdug+/+N9MQ== （使用了省略号）。 **重要事项** 此值必须以您为“主机/IP 地址”字段所输入的主机名、FQDN 或 IP 地址开始。 例如，如果在“主机/IP 地址”字段使用了 extFileServer，则该字段必须以 extFileServer 开始，其后跟整个 rsa 密钥。
外部文件服务器目录	文件服务器目录分层顶部的路径。 例如 `/opt/mftFileStore/node_1/`
用户名	外部文件服务器管理员的用户名。

验证 Cisco XCP 文件传输管理器激活

Cisco XCP 文件传输管理器服务必须在启用了托管文件传输的各个节点上处于活动状态。

该服务仅在分配了外部数据库和外部文件服务器时，以及服务能够连接数据库并安装文件服务器时启动。

开始之前

在 IM and Presence Service 上设置外部文件服务器， 第 14 页

过程

步骤 1 在群集的任何节点上，登录到 **Cisco Unified IM and Presence 功能配置**用户界面。

步骤 2 选择**工具** > **服务启动**。

步骤 3 从**服务器**下拉列表中，选择一个启用了托管文件传输的节点，然后单击**前往**。

步骤 4 确认 **Cisco XCP 文件传输管理器**服务的**激活状态**是否为**已激活**。

步骤 5 如果服务禁用，则选中 **Cisco XCP 文件传输管理器**复选框，然后单击**保存**。

步骤 6 对启用了托管文件传输的所有群集节点重复此程序。

下一步做什么

启用托管文件传输，第 17 页

启用托管文件传输

在 IM and Presence Service 上启用托管文件传输。

过程

步骤 1 登录到 **Cisco Unified CM IM and Presence 管理**，选择**消息** > **文件传输**。 **文件传输**窗口将打开。

步骤 2 在“文件传输配置”区域，根据您的部署，选择**托管文件传输**或**托管和对等文件传输**。 请参阅文件传输选项，第 18 页。

步骤 3 输入最大文件大小。 如果您输入 0，则应用最大大小 (4GB)。

注释 您必须重新启动 Cisco XCP 路由器服务，此更改才能生效。

步骤 4 在“托管文件传输分配”区域，为群集中的各个节点分配外部数据库和外部文件服务器。

a) 外部数据库 - 从下拉列表选择外部数据库的名称。

b) 外部文件服务器 - 从下拉列表选择外部文件服务器的名称。

步骤 5 单击**保存**。

单击**保存**后，将显示各个分配的**节点公钥**链接。

步骤 6 对于启用了托管文件传输的群集中的各个节点，您必须将节点的整个公钥复制到外部文件服务器的 `authorized_keys` 文件。

a) 要显示节点的公钥，向下滚动到“托管文件传输分配”区域，并单击**节点公钥**链接。 复制对话框的整个内容，包括节点的 IP 地址、主机名或 FQDN。

示例：

```
ssh-rsa yc2EAAAABIwAAAQEAp2g+S2XDEzptN11S5h5nwVleKBnfG2pdW6KiLfzu/sFLegioIIqA8jBguNY/...
...5s+tusrtBBuciCkH5gfXwrsFS0O0AlfFvwnfq1xmKmIS9W2rf0Qp+A+G4MVpTxHgaonw== imp@imp_node
```

（使用了省略号）。

警告

- 如果配置了托管文件传输功能，且“文件传输类型”更改为**禁用**或**对等**，则所有托管文件传输设置都将被删除。
- 节点的密钥将在节点从外部数据库和文件服务器取消分配时失效。

b) 在外部文件服务器上，打开您在 *mftuser* 的主目录下创建的 *~mftuser*/.ssh/authorized_keys 文件（如果尚未打开），然后（在新的一行）添加每个节点的公钥。

注释 authorized_keys 文件必须包含启用了分配到文件服务器的 IM and Presence Service 节点的各个托管文件传输的公钥。

c) 保存并关闭 authorized_keys 文件。

步骤 7 （可选）配置托管文件传输服务参数，以定义为外部文件服务器磁盘空间生成 RTMT 警报的阈值。

步骤 8 在启用了托管文件传输的所有节点上重新启动 Cisco XCP 路由器服务。请参阅“重新启动 Cisco XCP 路由器服务”。

下一步做什么

验证外部服务器状态，第 18 页

文件传输选项

您可在“文件传输”窗口中配置以下文件传输选项之一：

文件传输选项	说明
禁用	文件传输对群集禁用。
点对点	允许一对一文件传输，但不在服务器上存档或存储文件。 不支持群聊文件传输。
托管文件传输	允许一对一和组文件传输。 文件传输将记录到数据库中，传输的文件将存储于服务器。 客户端还必须支持托管文件传输，否则不允许进行文件传输。
托管和对等文件传输	允许一对一和组文件传输。 仅在客户端支持托管文件传输时，文件传输才将记录到数据库中，且传输的文件将存储于服务器。 如果客户端不支持托管文件传输，此选项等同于“对等”选项。

注释 如果在节点上配置了托管文件传输，且您将“文件传输类型”更改为**禁用**或**对等**，则请注意外部数据库和该节点外部文件服务器的映射设置将删除。 如果您为节点重新启用了托管文件传输，则数据库和文件服务器仍将处于配置状态，但是您必须重新分配它们。

在升级到 IM and Presence Service 10.5(2) 版或更高版本后，根据您预升级设置的不同，系统将选中**禁用**或**对等**选项。

验证外部服务器状态

验证并确保外部数据库设置和外部文件服务器设置不存在任何问题。

开始之前

启用托管文件传输，第 17 页

过程

步骤 1 验证外部数据库的状态：

a) 在 **Cisco Unified CM IM and Presence 管理**中，选择**消息** > **外部服务器设置** > **外部数据库**。
b) 检查“外部数据库状态”区域中提供的信息。

步骤 2 在您需要验证是否已分配外部文件服务器的 IM and Presence Service 节点上：

a) 在 **Cisco Unified CM IM and Presence 管理**中，选择**消息** > **外部服务器设置** > **外部文件服务器**。
b) 检查“外部文件服务器状态”区域中的信息，以验证连接是否无故障。

排查外部文件服务器公钥和私钥

服务器私钥/公钥对生成后，私钥通常将写入到 `/etc/ssh/ssh_host_rsa_key`

公钥将写入到 `/etc/ssh/ssh_host_rsa_key.pub`

如果这些文件不存在，则完成以下程序：

过程

步骤 1 输入以下命令：

```
$ ssh-keygen -t rsa -b 2048
```

步骤 2 复制文件服务器的公钥。

您必须复制整个公钥文本的字符串，包括主机名、FQDN 或 IP 地址（例如 *hostname* ssh-rsa AAAAB3NzaC1yc...）。 在大多数 Linux 部署中，密钥都包含服务器的主机名或 FQDN。

提示 如果 `$ ssh-keygen -t rsa -b 2048` 命令的输出不包含主机名，则使用以下命令的输出：`$ ssh-keyscan`*hostname*

步骤 3 对于每个配置为使用此文件服务器的 IM and Presence Service 节点，请将公钥粘贴到**外部文件服务器配置**窗口中的**外部文件服务器公钥**字段内。

重要事项 必须为托管文件传输功能配置无密码的 SSH。有关无密码 SSH 的完整配置说明，请参阅 SSHD 主页。

注释 在检查从发布方节点到订阅方节点的状态时，信息消息“可以从此处运行此外部文件服务器的诊断测试”将显示，反之亦然。

在日志中我们会看到"pingable": "-7"，这意味着我们正在查看未配置外部文件服务器的其他节点的状态。

我们在发布方节点上配置外部文件服务器，并在外部文件服务器的“Authorized_key”文件中共享发布方节点公钥。

管理托管文件传输

配置托管文件传输后，您需要持续管理此功能。 例如，您需要建立一个系统来管理文件服务器和数据库增长。 托管文件传输管理概述.

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。