マネージド ファイル転送の設定

マネージド ファイル転送の概要

マネージド ファイル転送（MFT）を使用すると、Cisco Jabber などの IM and Presence サービス クライアントは他のユーザ、アドホック グループ チャット ルーム、および永続的なチャット ルームにファイルを転送できます。ファイルは外部ファイル サーバのリポジトリに保存され、トランザクションが外部データベースのログに記録されます。

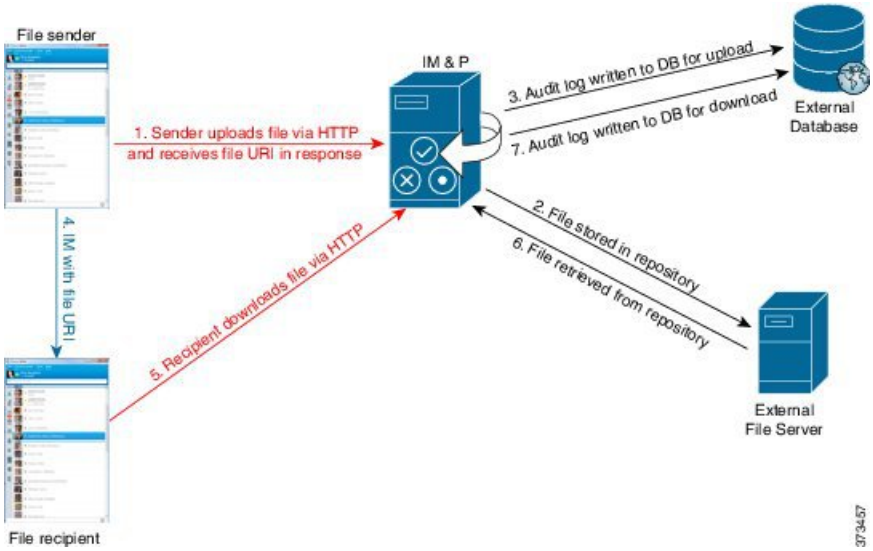
マネージド ファイル転送機能を展開するには、次のサーバも展開する必要があります。

- **外部データベース** - すべてのファイル転送は外部データベースに記録されます。
- **外部ファイルサーバ** - 転送された各ファイルのコピーは、外部ファイルサーバのリポジトリに保存されます。

（注） この設定はファイル転送に固有な設定であり、法規制コンプライアンスのためのメッセージ アーカイバ機能には影響しません。

使用例については、 マネージド ファイル転送の通話フロー （2 ページ）

マネージド ファイル転送の通話フロー



1. 送信者はHTTP経由でファイルをIM and Presenceサービス サーバにアップロードし、サーバはファイルのURIを応答として返します。
2. IM and Presenceサービスサーバは、ファイルをファイルサーバリポジトリに送信して保存します。
3. IM and Presenceサービスは外部データベース ログ テーブルに、アップロードを記録する項目を書き込みます。
4. 送信者が受信者にIMを送信します。IMにはファイルのURIが含まれています。
5. 受信者は、IM and Presence Serviceにファイルの HTTP 要求を送信します。IM and Presenceサービスはリポジトリからファイルを読み取り（6）、ログ テーブルにダウンロードを記録（7）した後で、ファイルを受信者に送信します。

グループ チャットや常設チャット ルームにファイルを転送するためのフローもこれと類似していますが、異なる点として送信者はチャットルームにIMを送信し、チャットルームの各参加者は個別にファイル ダウンロード要求を送信します。

（注） ファイルのアップロードが発生すると、そのドメインで使用可能な企業内のすべてのマネージドファイル転送サービスの中からマネージドファイル転送サービスが選択されます。ファイルアップロードは、このマネージドファイル転送サービスを実行しているノードに関連付けられた外部データベースと外部ファイルサーバのログに記録されます。あるユーザがこのファイルをダウンロードすると、この2番目のユーザのホームがどこかにあるかには関係なく、同じマネージドファイル転送サービスがその要求を処理して、同じ外部データベースおよび同じ外部ファイル サーバのログに記録します。

マネージド ファイル転送の前提条件

- 外部データベースと外部ファイルサーバも配置する必要があります。
- すべてのクライアントが、割り当てられている IM and Presence Service ノードの完全な FQDN を解決できることを確認してください。これはマネージドファイル転送が機能するために必要です。

外部データベースの前提条件

ヒント　常設チャットやメッセージアーカイブを展開している場合は、すべての機能に同じ外部データベースとファイルサーバを割り当てることができます。サーバの容量を判断する際には、見込まれる IM トラフィック、ファイル転送数、およびファイル サイズを考慮するようにします。

外部データベースをインストールし、設定します。サポートされているデータベースを含む詳細については、*IM and Presence* サービスのデータベース設定ガイドをご覧ください。

さらに、次の注意事項に従ってください。

- IM and Presence サービス クラスタ内の各 IM and Presence サービス ノードに対して 1 つの固有の論理外部データベース インスタンスが必要です。
- 外部データベースは、仮想化プラットフォームと非仮想化プラットフォームの両方でサポートされています。
- ログに記録されるメタデータの完全なリストについては、『*Database Setup for IM and Presence Service on Cisco Unified Communications Manager*』の『外部データベースツール』にある AFT_LOG テーブルを参照してください。
- IPv6 を使用して外部データベースに接続している場合は、IPv6 の設定に関する詳細をIPv6 タスク フローの設定で確認してください。

外部ファイル サーバの要件

外部ファイルサーバをセットアップするときには、次のガイドラインに従ってください。

- ファイル サーバの容量に応じて、各 IM and Presence Service ノードは自身の Cisco XCP ファイル転送ディレクトリを必要としますが、複数のノードで同じ物理ファイル サーバ インストールを共有できます。
- ファイル サーバは ext4 ファイル システム、SSHv2、および SSH ツールをサポートする必要があります。
- ファイルサーバは、4.9 ～ 6.x 間の OpenSSH バージョンをサポートする必要があります。

- IM and Presence Service と外部ファイル サーバの間のネットワーク スループットは、1 秒間に 60 MB を超えている必要があります。

  ファイル サーバの転送スピードを判別するために、マネージド ファイル転送を有効化した後で、show fileserver transferspeed CLI コマンドを使用できます。なお、システムの稼動率が高いときにこのコマンドを実行すると、コマンドから返される値に影響を与えることがあります。このコマンドの詳細については、「*Command Line Interface Guide for Cisco Unified Communications Solutions*」をこのリンクで参照してください。

外部ファイルサーバに対するパーティションの推奨事項

サーバ上で稼動している他のアプリケーションが書き込まないように、ファイル転送ストレージ専用の別のパーティションを1つ以上作成することをシスコでは推奨しています。すべてのファイル ストレージ ディレクトリを、これらのパーティションに作成してください。

次の点に注意してください。

- パーティションを作成する場合、IM and Presence Service のデフォルト ファイル サイズ（0）を設定すると、最大 4 GB までファイルを転送できることに注意してください。マネージドファイル転送をセットアップするときには、この設定を低い値にすることができます。
- 1 日あたりのアップロード数と平均ファイル サイズを考慮してください。
- 予想されるファイル容量を保持するのに十分なディスク領域がパーティションにあることを確認します。
- たとえば 12000 人のユーザが 1 時間あたり平均 100 KB のファイルを 2 つ転送すると、1 日 8 時間では 19.2 GB になります。

外部ファイルサーバのディレクトリ構造

次の例に示すように、最初のファイル転送が発生すると、タイムスタンプ付きのサブディレクトリが自動生成されます。

- IM and Presence Service ノード上にパス `/opt/mftFileStore/node_1/` を作成します。
- ディレクトリ `/files/` が自動生成されます。
- 3 つの `/chat_type/` ディレクトリ（`im`、`persistent`、`groupchat`）が自動的に生成されます。
- 日付のディレクトリ `/YYYYMMDD/` が自動生成されます。
- 時間のディレクトリ `/HH/` が自動生成されます。1 時間以内に 1,000 個を超えるファイルが転送されると、追加のロールオーバー ディレクトリ `/HH.n/` が作成されます。
- ファイルは、自動生成されたエンコード リソース名付きで保存されます（これ以降、`file_name` と表します）。

この例では、ファイルの完全パスは `/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name` となります。

この例のパスを使用すると：

- 2014 年 8 月 11 日 15.00 ～ 15.59 UTC に 1 対 1 IM で転送されたファイルは、次のディレクトリに配置されます。`/opt/mftFileStore/node_1/files/im/20140811/15/file_name`

  2014 年 8 月 11 日 16.00 ～ 16.59 UTC に常設グループチャットで転送されたファイルは、次のディレクトリに配置されます。`/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`

- 2014 年 8 月 11 日 16.00 ～ 16.59 UTC にアドホックチャットで転送された1001番目のファイルは、次のディレクトリに配置されます。`/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`

- 1 時間単位の中でファイル転送が発生しない場合、その期間にはディレクトリが作成されません。

（注） IM and Presence Service とファイル サーバの間のトラフィックは SSHFS を使用して暗号化されますが、ファイルの内容は、暗号化されていない形式でファイル サーバに書き込まれます。

外部ファイルサーバのユーザー認証

IM and Presence Service は、次のように SSH キーを使用して自身とファイル サーバを認証します。

- IM and Presence Service のパブリック キーはファイル サーバに保存されます。
- SSHFS は、接続中に IM and Presence Service のプライベート キーを検証します。これにより、すべてのファイルの内容が確実に暗号化されます。
- ファイル サーバのパブリック キーは、IM and Presence Service に格納されます。これにより IM and Presence Service は設定済みのファイル サーバに確実に接続し、中間者攻撃を最小限に抑えることができます。

（注） ノードの公開キーはノードの割り当てが解除されると無効になります。ノードが再び割り当てられると、新しいノード公開キーが自動的に生成されます。このキーを外部ファイルサーバで再設定する必要があります。

マネージド ファイル転送のタスク フロー

IM and Presence サービスでマネージドファイル転送機能を設定し、外部ファイルサーバを設定するには、次の作業を完了してください。

始める前に

マネージドファイル転送用に外部データベースと外部ファイルサーバの両方を設定します。要件については、

- 外部データベースの前提条件 （3 ページ）
- 外部ファイル サーバの要件 （3 ページ）

外部データベースの設定方法については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.htmlで*IM and Presence* サービスの外部データベース設定ガイドを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	外部データベースの接続の追加 （7 ページ）	IM and Presence サービスからの外部データベースへの接続を設定します。
ステップ 2	外部ファイル サーバのセットアップ （8 ページ）	ファイル サーバ上でユーザ、ディレクトリ、所有、権限、および他のタスクを設定する前に、外部サーバーをセットアップします。
ステップ 3	外部ファイルサーバーのユーザの作成 （9 ページ）	外部ファイルサーバーのユーザのセットアップ
ステップ 4	外部ファイル サーバのディレクトリを設定 （10 ページ）	外部ファイルサーバの最上位ディレクトリ構造を設定します。
ステップ 5	外部ファイルサーバの公開鍵を取得する （11 ページ）	外部ファイルサーバーの公開鍵を取得します。
ステップ 6	IM and Presence Service での外部ファイル サーバのプロビジョニング （12 ページ）	外部ファイル サーバの次の情報を取得します。
ステップ 7	Cisco XCP ファイル転送マネージャのアクティベーションの確認 （15 ページ）	マネージドファイル転送が有効になっている各ノードで、Cisco XCP File Transfer Manager サービスがアクティブである必要があります。

	コマンドまたはアクション	目的
ステップ 8	マネージド ファイル転送の有効化 （15 ページ）	IM and Presence サービスでのマネージド ファイル転送の有効化
ステップ 9	外部サーバーステータスの確認 （18 ページ）	外部データベースの設定と外部ファイル サーバの設定に問題がないことを確認します。

外部データベースの接続の追加

IM and Presence サービスからの外部データベースへの接続を設定します。マネージドファイル転送では、各 IM and Presence Service ノードに対して 1 つの固有の論理外部データベース インスタンスが必要です。

始める前に

各外部データベースをセットアップします。詳細は、*IM and Presence* サービスの外部データベース設定ガイドを参照してください。

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

手順

ステップ 1 [Cisco Unified CM IM and Presence 管理（Cisco Unified CM IM and Presence Administration）]から、**[メッセージ（Messaging）]** > **[外部サーバ設定（External Server Setup）]** > **[外部データベース（External Databases]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 **[データベース名（Database Name）]** フィールドに、外部データベースインスタンスの名前を入力します。

ステップ 4 **データベースの種類**ドロップダウンリストから、展開する外部データベースの種類を選択します。

ステップ 5 データベースの**ユーザ名**と**パスワード情報**を入力します。

ステップ 6 **[Hostname]** フィールドにホストのデータベースのホスト名または IP アドレスを入力します。

ステップ 7 **外部データベース設定**ウィンドウの残りの設定を完了します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

ステップ 8 **[保存（Save）]** をクリックします。

ステップ 9 この手順を繰り返して、各外部データベースインスタンスへの接続を作成します。

外部ファイル サーバのセットアップ

ファイルサーバ上でユーザ、ディレクトリ、所有、権限、および他のタスクを設定する前に、外部サーバーをセットアップします。

始める前に

外部ファイルサーバの設計上の推奨事項を確認してください。詳細については、外部ファイル サーバの要件 （3 ページ）を参照してください。

手順

ステップ 1 サポート対象のバージョンの Linux をインストールします。

ステップ 2 次のいずれかのコマンドを root として入力し、ファイル サーバが SSHv2 および OpenSSH 4.9 以降をサポートしていることを確認します。

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

または

```
# 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
...
```

ステップ 3 プライベート/パブリック キーの認証を許可するには、`/etc/ssh/sshd_config` ファイルで以下のフィールドが はい に設定されていることを確認します。

- RSAAuthentication はい
- PubkeyAuthentication はい

ファイル内でこれらの行をコメント アウトした場合、設定をそのまま保持することが可能です。

ヒント また、セキュリティを強化するために、ファイル転送ユーザ（この例では *mftuser*）に対してパスワード ログインを無効にすることもできます。これにより、必ず SSH のパブリック/プライベート キー認証によってログインされるようになります。

ステップ 4 サーバ上で稼動している他のアプリケーションが書き込まないように、ファイル転送ストレージ専用の別のパーティションを1つ以上作成することをシスコでは推奨しています。すべてのファイル ストレージ ディレクトリを、これらのパーティションに作成してください。

次のタスク

外部ファイルサーバーのユーザの作成 （9 ページ）

外部ファイルサーバーのユーザの作成

外部ファイルサーバーのユーザのセットアップ

始める前に

外部ファイル サーバのセットアップ （8 ページ）

手順

ステップ 1 root としてファイルサーバ上で、マネージド ファイル転送機能のユーザを作成します。このユーザは、ファイル ストレージのディレクトリ構造（この例では*mftuser*を使用）を所有し、ホーム ディレクトリを強制的に作成します（**-m**）。

```
# useradd -m mftuser
# passwd mftuser
```

ステップ 2 マネージド ファイル転送ユーザに切り替えます。

```
# su mftuser
```

ステップ 3 *~mftuser* ホーム ディレクトリの下に、キー ストアとして使用する `.ssh` ディレクトリを作成します。

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

ステップ 4 `.ssh`ディレクトリの下に`authorized_keys`ファイルを作成します。このファイルは、マネージド ファイル転送が有効になっている各ノードについて、パブリック キーを保持するのに使われます。

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

ステップ 5 パスワードを使用しない SSH が機能するように、正しい権限を設定します。

```
$ chmod 700 ~mftuser (directory)
$ chmod 700 ~/.ssh (directory)
$ chmod 700 ~/.ssh/authorized_keys (file)
```

（注） いくつかの Linux システムでは、SSH の設定によってこれらの権限が異なることがあります。

次のタスク

外部ファイル サーバのディレクトリを設定 （10 ページ）

外部ファイル サーバのディレクトリを設定

外部ファイルサーバの最上位ディレクトリ構造を設定します。

任意のディレクトリ名を付けて、任意のディレクトリ構造を作成することができます。マネージドファイル転送が有効になっている各ノード用にディレクトリを必ず作成してください。後で、IM and Presence Service でマネージド ファイル転送を有効にするときに、各ディレクトリをノードに割り当てる必要があります。

重要 マネージドファイル転送が有効になっている各ノード用に1つのディレクトリを作成する必要があります。

（注） ファイルサーバのパーティション/ディレクトリは、ファイルの格納に使用される IM and Presence Service ディレクトリにマウントされます。

始める前に

外部ファイルサーバーのユーザの作成 （9 ページ）

手順

ステップ 1 root ユーザーに切り替えます。

```
$ exit
```

ステップ 2 マネージド ファイル転送が有効になっている IM and Presence Service のすべてのノードのディレクトリを格納するために、最上位のディレクトリ構造（この例では `/opt/mftFileStore/`）を作成します。

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

ステップ 3 `/opt/mftFileStore/` の占有者として *`mftuser`* を指定します。

```
# chown mftuser:mftuser /opt/mftFileStore/
```

ステップ 4 *mftuser* に、mftFileStore ディレクトリに対する占有権を付与します。

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

ステップ 5 *mftuser* に切り替えます。

```
# su mftuser
```

ステップ 6 マネージドファイル転送が有効になっている各ノードに関して、/opt/mftFileStore/ の下にサブディレクトリを作成します（後で、マネージドファイル転送を有効にするときに各ディレクトリを 1 つのノードに割り当てます）。

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

（注）
- これらのディレクトリとパスは、**外部ファイルサーバ ディレクトリ**フィールドで使用され、Cisco Unified CM IM and Presence Administration でファイルサーバをプロビジョニングするときに設定します。
- 複数の IM and Presence Service ノードがこのファイル サーバに書き込む場合は、前述の例で 3 つのノード {*node_1*,*node_2*,*node_3*} に設定したように、各ノードのターゲット ディレクトリを定義する必要があります。
- 各ノードのディレクトリ内では、転送タイプのサブディレクトリ（im、groupchat、および persistent）が IM and Presence Service によって自動的に作成されます。その後のすべてのディレクトリも同様です。

次のタスク

外部ファイルサーバの公開鍵を取得する （11 ページ）

外部ファイルサーバの公開鍵を取得する

外部ファイルサーバーの公開鍵を取得します。

始める前に

外部ファイル サーバのディレクトリを設定 （10 ページ）

手順

ステップ 1 ファイル サーバのパブリック キーを取得するには、次のように入力します。

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

host はファイル サーバのホスト名、FQDN、または IP アドレスです。

警告

- ファイル サーバのパブリック キーをスプーフィングする「中間者攻撃」を防ぐには、**ssh-keyscan -t rsa** *host* コマンドで返されるパブリック キーの値が、ファイル サーバの実際のパブリック キーであることを確認する必要があります。
- ファイル サーバで、（このシステムでは `/etc/ssh/` の下にある）`ssh_host_rsa_key.pub` ファイルの場所に移動し、パブリック キー ファイルの内容と、**ssh-keyscan -t rsa** *host* コマンドで返されたパブリック キー値を比べて、ホスト以外の部分が一致することを確認してください（ファイル サーバの `ssh_host_rsa_key.pub` ファイルにはホストが存在しません）。

ステップ 2 `ssh_host_rsa_key.pub` ファイルの内容ではなく、**ssh-keyscan -t rsa** *host* コマンドの結果をコピーします。サーバのホスト名、FQDN、またはIPアドレスから最後まで、キー値全体を必ずコピーしてください。

（注） ほとんどの場合、サーバのキーはホスト名または FQDN で始まりますが、IP アドレスで始まることもあります。

たとえば、次の内容をコピーします。

hostname ssh-rsa AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs...

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

（... を追加）。

ステップ 3 **ssh-keyscan -t rsa** *host* コマンドの結果をテキスト ファイルに保存します。これは、「*IM and Presence Service* での外部ファイル サーバの展開」の手順でファイル サーバを設定するときに必要になります。

ステップ 4 作成した `authorized_keys` ファイルを開き、開いたままにしておきます。後で、IM and Presence サービスでファイルサーバをプロビジョニングするときに、必要になります。

（注） 公開鍵を取得できない場合は、外部ファイルサーバと公開キーのトラブルシューティング （19 ページ）で詳細なヘルプを参照してください。

次のタスク

IM and Presence Service での外部ファイル サーバのプロビジョニング （12 ページ）

IM and Presence Service での外部ファイル サーバのプロビジョニング

マネージド ファイル転送を有効にするクラスタ内の各ノードについて、1 つの外部ファイル サーバ インスタンスを設定する必要があります。

外部ファイル サーバ インスタンスは、外部ファイル サーバの物理インスタンスである必要はありません。ただし、ある 1 つのホスト名に関して、それぞれの外部ファイル サーバ インスタンス用に一意の外部ファイルサーバディレクトリ パスを指定する必要があります。同じノードから、すべての外部ファイル サーバ インスタンスを設定できます。

始める前に

外部ファイルサーバの公開鍵を取得する （11 ページ）

外部ファイル サーバの次の情報を取得します。

- ホスト名、FQDN、または IP アドレス
- パブリック キー
- ファイル ストレージ ディレクトリへのパス
- ユーザ名（User name）

手順

ステップ 1 **[Cisco Unified CM IM and Presence 管理（Cisco Unified CM IM and Presence Administration）]** で、**[メッセージ（Messaging）] > [外部サーバ設定（External Server Setup）] > [外部ファイル サーバー（External File Servers）]** を選択します。

ステップ 2 **[新規追加（Add New）]** をクリックします。
[外部ファイルサーバ（External File Servers）] ウィンドウが表示されます。

ステップ 3 サーバの詳細を入力します。フィールドとその設定オプションの詳細については、外部ファイル サーバ フィールド （13 ページ）を参照してください。

ステップ 4 **[保存（Save）]**をクリックします。

ステップ 5 マネージドファイル転送が有効になっているクラスタノードごとに別々の外部ファイルサーバ インスタンスを作成するまで、この手順を繰り返します。

次のタスク

Cisco XCP ファイル転送マネージャのアクティベーションの確認 （15 ページ）

外部ファイル サーバ フィールド

フィールド	説明
名前（Name）	ファイル サーバの名前を入力します。すぐに識別できるよう、サーバ名はできるだけ説明的な名前にしてください。 最大文字数は 128 文字です。使用できる文字は英数字、ダッシュ、および下線文字です。

フィールド	説明
ホスト/IP アドレス（Host/IP Address）	ファイル サーバのホスト名または IP アドレスを入力します。 （注） • [ホスト/IPアドレス（Host/IP Address）] フィールドに入力する値は、下記の [外部ファイルサーバパブリックキー（External File Server Public Key）] フィールドで指定するキーの先頭部分と一致する必要があります。 • この設定を変更した場合は、Cisco XCP Router サービスを再起動する必要があります。
外部ファイルサーバパブリックキー（External File Server Public Key）	ファイル サーバのパブリック キー（テキスト ファイルに保存するよう指示されたキー）を、このフィールドに貼り付けます。 キーを保存しなかった場合は、次のコマンドを実行してファイルサーバからそれを取得できます。 `$ ssh-keyscan -t rsa host`（ファイル サーバ上で）*host* は、ファイル サーバの IP アドレス、ホスト名、または FQDN です。 ホスト名、FQDN、または IP アドレスから始まって末尾まで、キーのテキスト全体をコピー/ペーストする必要があります。たとえば、次の内容をコピーします。 extFileServer.cisco.com ssh-rsa AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs... ...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/sdug+/+N9MQ== （... を追加）。 **重要** この値は必ず、[ホスト/IPアドレス（Host/IP Address）] フィールドに入力したホスト名、FQDN、または IP アドレスで始まる必要があります。たとえば [ホスト/IPアドレス（Host/IP Address）] フィールドで extFileServer が使用されている場合は、このフィールドの先頭部分は extFileServer となり、その後に rsa キー全体が続きます。
外部ファイルサーバディレクトリ（External File Server Directory）	ファイル サーバ ディレクトリ階層の最上位のパス（例：`/opt/mftFileStore/node_1/`）。
ユーザ名（User Name）	外部ファイル サーバ管理者のユーザ名。

Cisco XCP ファイル転送マネージャのアクティベーションの確認

マネージドファイル転送が有効になっている各ノードで、Cisco XCP File Transfer Manager サービスがアクティブである必要があります。

このサービスが開始可能なのは、外部データベースと外部ファイルサーバがすでに割り当てられており、しかもサービスがデータベースに接続してファイルサーバをマウントできる場合だけです。

始める前に

IM and Presence Service での外部ファイル サーバのプロビジョニング （12 ページ）

手順

ステップ 1 クラスタ内のいずれかのノードで [Cisco Unified IM and Presenceのサービスアビリティ（Cisco Unified IM and Presence Serviceability）] ユーザ インターフェイスにログインします。

ステップ 2 **[ツール（Tools）] > [サービス アクティベーション（Service Activation）]** を選択します。

ステップ 3 **サーバ**ドロップダウンから、マネージド ファイル転送が有効になっているノードを選択し、**[移動（Go）]**をクリックします。

ステップ 4 **Cisco XCP ファイル転送マネージャ**サービスの**アクティベーションステータス**が**起動済**であることを確認します。

ステップ 5 サービスが無効になっている場合は、**Cisco XCP ファイル転送マネージャ**チェックボックスをチェックして、**保存する**をクリックします。

ステップ 6 マネージド ファイル転送が有効になっているすべてのノードで、この手順を繰り返します。

次のタスク

マネージド ファイル転送の有効化 （15 ページ）

マネージド ファイル転送の有効化

IM and Presence サービスでのマネージド ファイル転送の有効化

手順

ステップ 1 **Cisco Unified CM IM and Presence Administration** にサインインし、**[メッセージング（Messaging）] > [ファイル転送（File Transfer）]** を選択します。**[ファイル転送（File Transfer）]** ウィンドウが開きます。

ステップ 2 [ファイル転送設定（File Transfer Configuration）] エリアで、展開に応じて **[マネージドファイル転送（Managed File Transfer）]** または **[マネージドおよびピアツーピアファイル転送**

（**Managed and Peer-to-Peer File Transfer**）] のいずれかを選択します。ファイル転送オプション （17 ページ）を参照してください

ステップ 3 [最大ファイルサイズ（Maximum File Size）] を入力します。0 を入力すると、最大サイズ（4 GB）が適用されます。

（注） この変更を有効にするには、Cisco XCP Router サービスを再起動する必要があります。

ステップ 4 [マネージドファイル転送の割り当て（Managed File Transfer Assignment）] エリアで、クラスタの各ノードに対して外部データベースと外部ファイル サーバを割り当てます。

a) 外部データベース：ドロップダウン リストから、外部データベースの名前を選択します。
b) 外部ファイル サーバ：ドロップダウン リストから、外部ファイル サーバの名前を選択します。

ステップ 5 [保存（Save）] をクリックします。

[保存（Save）] をクリックすると、それぞれの割り当てに対して [ノードパブリックキー（Node Public Key）] リンクが表示されます。

ステップ 6 マネージド ファイル転送が有効になるクラスタ内の各ノードについて、ノードのパブリック キー全体を外部ファイル サーバの `authorized_keys` ファイルにコピーする必要があります。

a) ノードのパブリック キーを表示するには、[マネージドファイル転送の割り当て（Managed File Transfer Assignment）] エリアをスクロール ダウンして [ノードパブリックキー（Node Public Key）] リンクをクリックします。ノードの IP アドレス、ホスト名、FQDN を含めて、ダイアログボックスの内容全体をコピーします。

例：

```
ssh-rsa
yc2EAAAABIwAAAQEAp2g+S2XDEzptN11S5h5nwVleKBnfG2pdW6KiLfzu/sFLegioIIqA8jBguNY/...

...5s+tusrtBBuciCkH5gfXwrsFS0O0AlfFvwnfq1xmKmIS9W2rf0Qp+A+G4MVpTxHgaonw== imp@imp_node
```

（... を追加）。

警告
- マネージドファイル転送機能が設定されいる場合、[ファイル転送タイプ（File Transfer Type）] が [無効（Disabled）] または [ピアツーピア（Peer-to-Peer）] に変更されると、マネージドファイル転送のすべての設定が削除されます。
- 外部データベースおよびファイル サーバからノードが割り当て解除されると、ノードのキーは無効になります。

b) 外部ファイル サーバ上で、*`mftuser`* のホームディレクトリの下に作成した `~mftuser/.ssh/authorized_keys` ファイルがまだ開いていない場合は、これを開いて、（新しい行で）各ノードのパブリック キーを付加します。

（注） `authorized_keys` ファイルには、ファイル サーバに割り当てられている、マネージド ファイル転送が有効な各 IM and Presence Service ノードのパブリック キーが含まれる必要があります。

c) `authorized_keys` ファイルを保存して閉じます。

ステップ 7 （オプション）マネージド ファイル転送サービス パラメータを設定して、外部ファイル サーバのディスク領域に関する RTMT アラートが生成されるしきい値を定義します。

ステップ 8 マネージド ファイル転送が有効になっているすべてのノード上で、Cisco XCP Router を再起動します。『Cisco XCP Router サービスの再起動』を参照してください。

次のタスク

外部サーバーステータスの確認 （18 ページ）

ファイル転送オプション

次のいずれかのファイル転送オプションを [ファイル転送（File Transfer）]ウィンドウで設定できます。

ファイル転送オプション	説明
無効	クラスタのファイル転送が無効です。
ピアツーピア	[ピアツーピア（Peer-to-Peer）]のファイル転送は許可されますが、サーバではファイルのアーカイブや保存が行われません。グループチャットのファイル転送はサポートされません。
マネージド ファイル転送	1対1およびグループのファイル転送が許可されます。ファイル転送がデータベースのログに記録され、転送されたファイルはサーバに保存されます。クライアントがマネージドファイル転送をサポートしている必要もあります。そうでない場合、ファイル転送は許可されません。
マネージド ファイル転送およびピアツーピア ファイル転送	1対1およびグループのファイル転送が許可されます。ファイル転送がデータベースのログに記録され、転送されたファイルはサーバに保存されます（ただしクライアントがマネージドファイル転送をサポートする場合のみ）。クライアントがマネージドファイル転送をサポートしていない場合、このオプションはピアツーピア オプションと同等になります。

（注） マネージドファイル転送がノードで設定されていて、ファイル転送タイプを**無効**または**ピアツーピア**に変更した場合は、そのノードの外部データベースと外部ファイルサーバにマップされた設定が削除されることに注意してください。データベースとファイルサーバの設定は残りますが、そのノードでマネージドファイル転送を再び有効にする場合は、データベースとファイル サーバの再割り当てが必要になります。

IM and Presence Service リリース 10.5(2) 以降にアップグレードすると、アップグレード前の設定に応じて、**無効**または**ピアツーピア**が選択されます。

外部サーバーステータスの確認

外部データベースの設定と外部ファイル サーバの設定に問題がないことを確認します。

始める前に

マネージド ファイル転送の有効化 （15 ページ）

手順

ステップ 1 外部データベースのステータスを確認するには

a) **[Cisco Unified CM IM and Presence 管理（Cisco Unified CM IM and Presence Administration）]**で、**[メッセージ（Messaging）]** > **[外部サーバ設定（External Server Setup）]** > **[外部データベース（External Databases]** を選択します。

b) [外部データベースのステータス（External Database Status）] エリアに示される情報を確認します。

ステップ 2 外部ファイル サーバが割り当てられたことを確認する必要がある IM and Presence Serviceノードで、次のようにします。

a) **[Cisco Unified CM IM and Presence 管理（Cisco Unified CM IM and Presence Administration）]**で、**[メッセージ（Messaging）]** > **[外部サーバ設定（External Server Setup）]** > **[外部ファイルサーバー（External File Servers）]** を選択します。

b) [外部ファイルサーバのステータス（External File Server Status）] エリアに示される情報を確認して、接続に問題がないことを確認します。

外部ファイルサーバと公開キーのトラブルシューティング

サーバのプライベート/パブリック キー ペアが生成されるとき、プライベート キーは通常、`/etc/ssh/ssh_host_rsa_key` に書き込まれます。

パブリック キーは `/etc/ssh/ssh_host_rsa_key.pub`に書き込まれます。

これらのファイルがない場合は、以下の手順に従ってください。

手順

ステップ 1 次のコマンドを入力します。

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

ステップ 2 ファイル サーバのパブリック キーをコピーします。

ホスト名、FQDN、またはIPアドレスから、パブリック キーのテキストの文字列全体をコピーする必要があります（例：*hostname* ssh-rsa AAAAB3NzaC1yc...）。ほとんどのLinux環境では、サーバのホスト名またはFQDNがキーに含まれています。

ヒント **$ ssh-keygen -t rsa -b 2048** コマンドの出力にホスト名が含まれていない場合は、代わりに **$ ssh-keyscan** *hostname* コマンドの出力を使用します。

ステップ 3 このファイル サーバを使用するように設定されている IM and Presence Service の各ノードについて、[外部ファイルサーバ設定（External File Server Configuration）] ウィンドウの [外部ファイルサーバパブリックキー（External File Server Public Key）] フィールドにパブリック キーを貼り付けてください。

重要 マネージドファイル転送機能には、パスワードを使用しない SSH を設定する必要があります。パスワードを使用しないSSHを設定する手順の詳細については、SSHDマニュアル ページを参照してください。

（注） パブリッシャ ノードからサブスクライバ ノードにステータスを確認するとき、および逆方向に確認するとき、「この外部ファイルサーバ用の診断テストは次から実行される場合があります（The diagnostics tests for this External File Server may be run from here.）」という情報メッセージが表示されます。

ログに「pingable」：「-7」と表示されます。これは、外部ファイルサーバが構成されていない他のノードのステータスを表示していることを意味します。

パブリッシャノードに外部ファイルサーバを設定し、パブリッシャノードの公開鍵は外部ファイルサーバの「Authorized_key」ファイルで共有されます。

マネージド ファイル転送の管理

マネージド ファイル転送を設定した後は、機能を継続的に管理する必要があります。たとえば、ファイルサーバとデータベースの増加を管理するためのシステムを整備する必要があります。マネージド ファイル転送管理の概要.