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することができます。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。

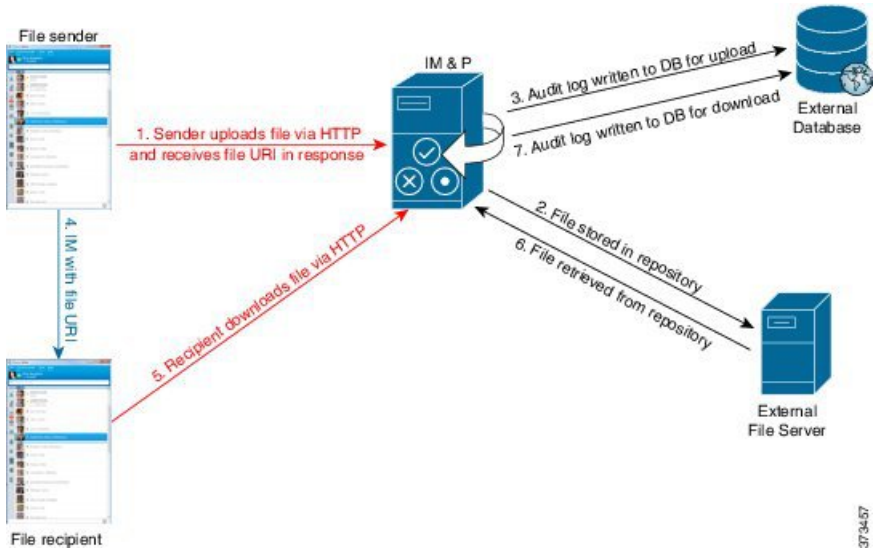
マネージド ファイル転送機能を展開するには、以下のサーバも配置する必要があります。

- **外部データベース**：すべてのファイル転送が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を外部ファイル サーバ上のリポジトリに保存します。

（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。

ユース ケースついての参照先 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. 送信者がHTTP 経由でファイルを IM and Presence Service 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 Service サーバがファイルをストレージ用のファイル サーバ リポジトリに送信します。
3. IM and Presence Service が、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. 送信者は、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、このファイルの IM and Presence Service に HTTP 要求を送信します。IM and Presence Service が、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、ファイルが受信者にダウンロードされます。

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 ファイル転送の要件

- 外部データベースおよび外部ファイル 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 ファイル転送の動作のために必要とされます。

外部データベースの要件

ヒント　また、常設チャットやメッセージ アーカイバを導入している場合は、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 サイズを考慮する必要があります。

外部データベースをインストールして設定します。サポートされるデータベースを含む詳細は、*IM and Presence* データベース セットアップ ガイド を参照してください。

さらに、以下のガイドラインに従ってください。

- 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、*Cisco Unified Communications Manager* での *IM and Presence Service* のデータベース設定ガイドの「外部データベースツール」の 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する場合は、IPv6 のセットアップの詳細について IPv6 の設定タスク フロー を確認してください。

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際は、以下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 ノードは独自の Cisco XCP File Transfer Manager ファイル サーバ ディレクトリを必要とします。ただし、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することもできます。
- 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。
- ファイルサーバーは、4.9、6.x、and 7.x の OpenSSH バージョンをサポートする必要があります。

重要 このノートは、リリース 14SU3 以降に適用されます。

（注） OpenSSH バージョン 8.x は、リリース 14SU3 以降でサポートされています。

- 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、このリンクの *Cisco Unified Communications Solutions* コマンドライン インタフェイス ガイド を参照してください。

外部ファイル サーバのパーティション

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。

次の例をご覧ください。

- 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 の IM で転送されたファイルは、以下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、以下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、以下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。これで、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。

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際は、以下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 ノードは独自の Cisco XCP File Transfer Manager ファイル サーバ ディレクトリを必要とします。ただし、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することもできます。
- 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。
- ファイルサーバーは、4.9、6.x、and 7.x の OpenSSH バージョンをサポートする必要があります。

重要 このノートは、リリース 14SU3 以降に適用されます。

（注） OpenSSH バージョン 8.x は、リリース 14SU3 以降でサポートされています。

- 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、このリンクの *Cisco Unified Communications Solutions* コマンドライン インタフェイス ガイド を参照してください。

外部ファイル サーバのパーティション

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。

次の例をご覧ください。

- 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 の IM で転送されたファイルは、以下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、以下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、以下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。これで、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。

外部ファイル サーバのパーティション推奨

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。

次の例をご覧ください。

- 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 サーバのユーザ認証

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。これで、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。

外部ファイル サーバ 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 の IM で転送されたファイルは、以下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、以下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、以下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。

マネージド ファイル転送のタスク フロー

これらのタスクを完了して、IM and Presence Serviceのマネージド ファイル転送機能を設定し、外部ファイル サーバを設定します。

始める前に

マネージドファイル転送用の外部データベースと外部ファイルサーバを設定します。要件については、以下を参照してください。

- 外部データベースの要件 （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の詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.htmlの *IM and Presence Service* 外部データベース セットアップ 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
Step 1	外部データベース接続の追加 （11 ページ）	IM and Presence Serviceから外部データベースへの接続を設定します。
Step 2	外部ファイル サーバのセットアップ （11 ページ）	ファイル サーバ上でユーザ、ディレクトリ、帰属、権限、および他のタスクを設定する前に、以下の手順を実行します。
Step 3	外部ファイル サーバのユーザの作成 （13 ページ）	外部ファイル サーバのユーザを作成します。
Step 4	外部ファイルサーバのディレクトリのセットアップ （14 ページ）	外部ファイルサーバの最上位レベルのディレクトリ構造を設定します。
Step 5	外部ファイル サーバの公開キーの取得 （15 ページ）	外部ファイル サーバ 公開キーを取得します。
Step 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 （16 ページ）	外部ファイル サーバに関する以下の情報を取得します。
Step 7	Cisco XCP File Transfer Manager のアクティベーションの確認 （18 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 サービスが有効化されていなければなりません。

	コマンドまたはアクション	目的
Step 8	マネージド ファイル転送の有効化 （19 ページ）	IM and Presence Serviceでのマネージド ファイル転送を有効にします。
Step 9	外部サーバのステータスの確認 （21 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。

外部データベース接続の追加

IM and Presence Serviceから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の設定詳細については、以下の *IM and Presence Service* 外部データベース セットアップ 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

Step 1 Cisco Unified CM IM and Presence 管理で、**メッセージング** > **外部サーバの設定** > **外部データベース**を選択します。

Step 2 **[新規追加]** をクリックします。

Step 3 **データベース名** フィールドに、データベースの名前を入力します。

Step 4 **データベース タイプ** ドロップダウンから、導入する外部データベースのタイプを選択します。

Step 5 データベースの **ユーザ名** および **パスワード情報** を入力します。

Step 6 **ホスト名** フィールドにホストの DNS ホスト名または IP アドレスを入力します。

Step 7 **外部データベースの設定** ウィンドウで残りの設定を入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

Step 8 [保存（Save）] をクリックします。

Step 9 この手順を繰り返して、外部データベース インスタンスへの各接続を作成します。

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、帰属、権限、および他のタスクを設定する前に、以下の手順を実行します。

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ます。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

Step 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。

Step 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
...
```

Step 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 *yes* に設定されていることを確認します。

- RSAAuthentication *yes*
- PubkeyAuthentication *yes*

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。

Step 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 サーバのユーザの作成 （13 ページ）

外部ファイル サーバのユーザの作成

外部ファイル サーバのユーザを作成します。

始める前に

外部ファイル サーバのセットアップ（11 ページ）

手順

Step 1 ファイル サーバ上で root として、マネージド ファイル転送機能用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を所有し（この例では *mftuser* を使用）、強制的にホーム ディレクトリを作成します（**-m**）。

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

Step 2 マネージド ファイル転送ユーザに切り替えます。

```
# su mftuser
```

Step 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/
```

Step 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
```

Step 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のセットアップ（14 ページ）

外部ファイル サーバのディレクトリのセットアップ

外部ファイル サーバの最上位レベルの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。必ず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作成してください。後に、IM and Presence Service でマネージド ファイル転送を有効にする際には、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 サーバのユーザの作成（13 ページ）

手順

Step 1 root ユーザーに切り替えます。

```
$ exit
```

Step 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/
```

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

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

Step 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/
```

Step 5 *mftuser* に切り替えます。

```
# su mftuser
```

Step 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およびパスは、Cisco Unified CM IM and Presence 管理ページでファイルサーバをプロビジョニングする際に設定する **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 サーバの公開キーの取得 （15 ページ）

外部ファイル サーバの公開キーの取得

外部ファイル サーバ 公開キーを取得します。

始める前に

外部ファイル サーバのディレクトリのセットアップ （14 ページ）

手順

Step 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）。

Step 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、必ずキー値全体を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）。

Step 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。

Step 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。後に、IM and Presence Serviceでファイル サーバをプロビジョニングする際にこれが必要となります。

（注） 公開キーを取得できない場合は、外部ファイル サーバの公開キーおよび秘密キーのトラブルシューティング （22 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 （16 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 サーバの公開キーの取得 （15 ページ）

外部ファイル サーバに関する以下の情報を取得します。

- ホスト名、FQDN、または IP アドレス
- 公開鍵
- ファイル ストレージ ディレクトリへのパス

- ユーザ名

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**メッセージング** > **外部サーバの設定** > **外部ファイル サーバ**を選択します。

Step 2 **[新規追加]** 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。

Step 3 サーバの詳細を入力します。フィールドおよび設定オプションの詳細については、外部ファイル サーバのフィールド（17 ページ）を参照してください。

Step 4 **[保存（Save）]** をクリックします。

Step 5 マネージド ファイル転送が有効化されているクラスタ ノードごとに、個別の外部ファイル 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 File Transfer Manager のアクティベーションの確認 （18 ページ）

外部ファイル サーバのフィールド

フィールド	説明
名前	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。
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。

フィールド	説明
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、次のようにコピーします。 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	外部ファイル サーバ管理者のユーザ名。

Cisco XCP File Transfer Manager 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 サービスが有効化されていなければなりません。

外部データベースおよび外部ファイル サーバがすでに割り当てられており、さらに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にのみ、このサービスが起動します。

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（16 ページ）

手順

Step 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。

Step 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。

Step 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て、**移動**をクリックします。

Step 4 **Cisco XCP File Transfer Manager** サービスの **アクティベーション ステータス** が **アクティブ済**であることを確認します。

Step 5 サービスが非アクティブ化されている場合は、**Cisco XCP File Transfer Manager** チェックボックスをオンにして、**保存**をクリックします。

Step 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クラスタ 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 （19 ページ）

マネージド ファイル転送の有効化

IM and Presence Serviceでのマネージド ファイル転送を有効にします。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**にログインし、**メッセージング** > **ファイル転送**を選択します。**ファイル転送** ウィンドウが開きます。

Step 2 ファイル転送設定エリアで、導入に応じて、**マネージド ファイル転送** あるいは **マネージド ピアツーピアファイル転送** を選択します。ファイル転送のオプション （20 ページ）を参照してください。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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 サービスを再起動します。「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

外部サーバのステータスの確認 （21 ページ）

ファイル転送のオプション

次のいずれかのオプションを [ファイル転送] ウィンドウで設定することができます。

ファイル転送オプション	説明
Disabled	ファイル転送がクラスタで無効化されています。
ピアツーピア	1 対 1 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。

アップグレード以前の設定により、IM and Presence Service リリース 10.5(2) 以降へのアップグレード後、**無効にする** あるいは **ピアツーピア** が選択されています。

外部サーバのステータスの確認

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 （19 ページ）

手順

Step 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**で、**メッセージング** > **外部サーバの設定** > **外部データベース**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。

Step 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IM and Presence Service ノードで：

a) **Cisco Unified CM IM and Presence 管理**で、**メッセージング** > **外部サーバの設定** > **外部ファイル サーバ**を選択します。

b) 外部ファイル サーバのステータス 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の公開キーおよび秘密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

Step 1 次のコマンドを入力します。

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

Step 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。

Step 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。

このログには、「-7」つまり外部ファイルサーバが設定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示す、「 ping 」が表示されます。

パブリッシャーノードでは外部ファイルサーバを設定し、パブリッシャ ノードの公開キー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、この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拡張を管理するためにシステムを導入する必要があります。マネージド ファイル転送の管理の概要。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。