Managed File Transfer Administration

- Managed File Transfer Administration Overview, on page 1
- Managed File Transfer Administration Prerequisites, on page 2
- Managed File Transfer Administration Task Flow, on page 2

Managed File Transfer Administration Overview

As the IM and Presence Service administrator , you are responsible for managing file storage and disk usage for the Managed File Transfer feature. Use this chapter to monitor the levels of file storage and disk usage and to set counters and alerts to let you know when the levels exceed your defined thresholds.

Managing External File Server and Database Server

When managing external database size, you can combine queries with shell scripting so that files get purged from the database automatically, according to your specifications. To create your queries use file transfer metadata. This includes transfer type, file type, timestamp, absolute path on the file server to the file, and other information.

When choosing how to handle file transfers within IM and group chat, consider that one-to-one IM and group chat are probably transient so transferred files may be deleted promptly. However, keep in mind that:

- IMs delivered to offline users may trigger a delayed request for a file.
- Persistent chat transfers may need to be longer lived.

Note

- Do not purge files that were created during the current UTC hour.
- After the file server is assigned, you can change the name of the file server configuration, but not the file server itself.
- If managed file transfer is configured and you change settings, restarting the Cisco XCP Router service restarts the managed file transfer feature.
- If you change settings without changing them on the file server itself, file transfer stops working and you receive a notification to restart the Cisco XCP Router service.
- If a database or file server failure occurs, a message is generated that specifies the failure. However, the error response does not distinguish between the database, file server, or some other internal failure. The Real-Time Monitoring Tool also generates an alarm when there is a database or file server failure. This alarm is independent of whether a file transfer is occurring.

Managed File Transfer Administration Prerequisites

Configure the Managed File Transfer feature.

Managed File Transfer Administration Task Flow

Procedure

	Command or Action	Purpose
Step 1	AFT_LOG Table Example Query and Output , on page 3	The following procedure provides an example of a query that you can run on the `AFT_LOG` table and how to use the output to purge unwanted files from the file server.
Step 2	Set Service Parameter Thresholds, on page 4	Configure the Managed File Transfer service parameters to define the threshold at which an RTMT alarm is generated for the external file server disk space.
Step 3	Configure XCP File Transfer Manager Alarms, on page 5	Configure alarms for Managed File Transfer to let you know when defined thresholds have been reached.
Step 4	Clean External Database for Managed File Transfer, on page 7	Optional. Use the External Database Cleanup Utility to configure jobs that monitor the external database and delete expired records. This will ensure that there is always enough disk space for new records.

AFT_LOG Table Example Query and Output

The following procedure provides an example of a query that you can run on the `AFT_LOG` table and how to use the output to purge unwanted files from the file server.

This query returns records for every uploaded file after the specified date.

Note For sample SQL commands, see External Database Disk Usage, on page 3.

Procedure

Step 1 In the External Database, enter the following command:

```
SELECT file_path
FROM aft_log
WHERE method='Post' AND timestampvalue > '2014-12-18 11:58:39';
```

The command generates the following output:

```
/opt/mftFileStore/node_1/files/im/20140811/15/file_name1
/opt/mftFileStore/node_1/files/im/20140811/15/file_name2
/opt/mftFileStore/node_1/files/im/20140811/15/file_name3
/opt/mftFileStore/node_1/files/im/20140811/15/file_name4
...
/opt/mftFileStore/node_1/files/im/20140811/15/file_name99
/opt/mftFileStore/node_1/files/im/20140811/15/file_name100
```

Step 2 Write a script that uses the `rm` command and this output to purge the above files from the external file server. For sample SQL queries, see *Database Setup for IM and Presence Service on Cisco Unified Communications Manager*.

Note
Files that have not been purged from the external file server can still be accessed or downloaded even if records relating to those files have been purged from the external database.

What to do next

Set Service Parameter Thresholds, on page 4

External Database Disk Usage

You must ensure that the disks or tablespaces do not become full, otherwise the managed file transfer feature may stop working. Following are sample SQL commands that you can use to purge records from the external

database. For additional queries, see the *Database Setup for IM and Presence Service on Cisco Unified Communications Manager*.

Note Files that have not been purged from the external file server can still be accessed or downloaded even if records relating to those files have been purged from the external database.

Action	Sample Command

Remove all records of files that were uploaded.	`DELETE`
	`FROM aft_log`
	`WHERE method = 'Post';`

Remove records of all files that were downloaded by a specific user.	`DELETE`
	`FROM aft_log`
	`WHERE jid LIKE '<userid>@<domain>%' AND method = 'Get';`

Remove records of all files that were uploaded after a specific time.	`DELETE`
	`FROM aft_log`
	`WHERE method = 'Post' AND timestampvalue > '2014-12-18 11:58:39';`

In addition, there are counters and alarms that can help you manage database disk usage. For details, see Alarms and Counters for Managed File Transfer, on page 5.

Set Service Parameter Thresholds

Configure the Managed File Transfer service parameters to define the threshold at which an RTMT alarm is generated for the external file server disk space.

Procedure

Step 1 In Cisco Unified CM IM and Presence Administration, choose **System** > **Service Parameters**.

Step 2 Choose the **Cisco XCP File Transfer Manager** service for the node.

Step 3 Enter values for the following service parameters.

- **External File Server Available Space Lower Threshold**— If the percentage of available space on the external file server partition is at or below this value, the XcpMFTExtFsFreeSpaceWarn alarm is raised. The default value is 10%.
- **External File Server Available Space Upper Threshold**— If the percentage of available space on the external file server partition reaches or exceeds this value, the XcpMFTExtFsFreeSpaceWarn alarm is cleared. The default value is 15%.

Note

Do not configure the lower threshold value to be greater than the upper threshold value. Otherwise the Cisco XCP File Transfer Manager service will not start after you restart the Cisco XCP Router service.

Step 4 Click **Save**.

Step 5 Restart the Cisco XCP Router service:

a) From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.
b) From the **Server** drop-down select the IM and Presence publisher and click **Go**.
c) Under **IM and Presence Services**, select **Cisco XCP Router**, and click **Restart**.

What to do next

Configure XCP File Transfer Manager Alarms, on page 5

Configure XCP File Transfer Manager Alarms

Configure alarms for Managed File Transfer to let you know when defined thresholds have been reached.

Procedure

Step 1 Sign in to **Cisco Unified IM and Presence Serviceability**.

Step 2 Choose **Alarm** > **Configuration**.

Step 3 From the **Server** drop-down, choose the server (node), and click **Go**.

Step 4 From the **Service Group** drop-down list, choose **IM and Presence Services** and click **Go**.

Step 5 From the **Service** drop-down list, choose **Cisco XCP File Transfer Manager (Active)** and click **Go**.

Step 6 Configure the preferred alarm settings. For help with the fields and tehhir settings, refer to the online help.

Step 7 Click **Save**.

What to do next

For more information on the available alarms and counters, see Alarms and Counters for Managed File Transfer, on page 5

Alarms and Counters for Managed File Transfer

With Managed File Transfers, the transferred files get delivered to users only after they are successfully archived to the external file server, and after the file metadata is logged to the external database. If an IM and Presence Service node loses its connection to the external file server or external database, IM and Presence Service does not deliver the file to the recipient.

Alarms for Managed File Transfer

To ensure that you are notified if a connection is lost, verify that the following alarms are properly configured in the Real-Time Monitoring Tool.

Note Any files that were uploaded before the connection to the external file server was lost and which were in the process of being downloaded to the recipient, fail to be downloaded. However, there is a record of the failed transfer in the external database. To identify these files, the external database fields file_size and bytes_transferred do not match.

Table 1: Alarms for Managed File Transfers

Alarm	Problem	Solution
XcpMFTExtFsMountError	Cisco XCP File Transfer Manager has lost its connection to the external file server.	Check the External File Server Troubleshooter for more information. Check that the external file server is running correctly. Check if there is any problem with the network connectivity to the external file server.
XcpMFTExtFsFreeSpaceWarn	Cisco XCP File Transfer Manager has detected that the available disk space on the external file server is low.	Free up space on the external file server by deleting unwanted files from the partition used for file transfer.
XcpMFTDBConnectError	Cisco XCP data access layer was unable to connect to the database.	Check the System Troubleshooter for more information. Check that the external database is running healthy and if there is any problem with the network connectivity to the external database server.
XcpMFTDBFullError	Cisco XCP File Transfer Manager cannot insert or modify data in the external database because either the disk or tablespace is full.	Check the database and assess if you can free up or recover any disk space. Consider adding additional database capacity.

Counters for Managed File Transfer

To help you administer managed file transfer, you can monitor the following counters via the Real-Time Monitoring Tool. These counters are saved in the Cisco XCP MFT Counters folder.

Table 2: Counters for Managed File Transfers

Counter	Description
MFTBytesDownloadedLastTimeslice	This counter represents the number of bytes downloaded during the last reporting interval (typically 60 seconds).

Counter	Description
MFTBytesUpoadedLastTimeslice	This counter represents the number of bytes uploaded during the last reporting interval (typically 60 seconds).
MFTFilesDownloaded	This counter represents the total number of files downloaded.
MFTFilesDownloadedLastTimeslice	This counter represents the number of files downloaded during the last reporting interval (typically 60 seconds).
MFTFilesUploaded	This counter represents the total number of files uploaded.
MFTFilesUploadedLastTimeslice	This counter represents the number of files uploaded during the last reporting interval (typically 60 seconds).

Clean External Database for Managed File Transfer

Configure jobs that monitor the external database and delete expired records. This will ensure that there is always enough disk space for new records.

To clean database tables for Managed File Transfer, make sure to select the **Managed File Transfer (MFT)** feature under **Feature Tables**.

Procedure

Step 1 Log into Cisco Unified CM IM and Presence Administration on the database publisher node.

Step 2 Choose **Messaging** > **External Server Setup** > **External Database Jobs**.

Step 3 Click **Clear External DB**.

Step 4 Do one of the following:

- For manual cleanup of an external database that connects to the publisher node, select **Same Cup Node**.
- For manual cleanup of an external database that connects to a subscriber node, select **Other Cup Node** and then select the external database details.
- If you are configuring the system to monitor and clean the external database automatically, check the **Automatic Clean-up** radio button.

Note
We recommend that you run a manual cleanup prior to setting up the automatic cleanup.

Step 5 Set the **Number of Days** that you want to go back for file deletion. For example, if you enter 90, the system deletes records that are older than 90 days.

Step 6 Click **Update Schema** to create the Indexes and stored procedures for the database.

Note
You need to update the schema only the first time that you run the job.

Step 7 Set the **Number of Days** that you want to go back for file deletion. For example, if you enter **90**, the system deletes records that are older than 90 days.

Step 8 In the **Feature Tables** section, select each feature for which you want to clean records:

- **Text Conference (TC)**—Select this option to clean database tables for the Persistent Chat feature.
- **Message Archiver (MA)**—Select this option to clean database tables for the Message Archiver feature.
- **Managed File Transfer (MFT)**—Select this option to clean database tables for the Managed File Transfer feature

Step 9 Click **Submit Clean-up Job**.

Note
If you have the **Automatic** option enabled, and you want to disable it, click the **Disable Automatic Clean-up Job** button.