CA NetMaster® File Transfer Management

Overview Guide

Release 12.1

CA Technologies Product References

This document references the following CA Technologies products:

- CA NetMaster® File Transfer Management (CA NetMaster FTM)
- CA XCOM™ Data Transport® (CA XCOM Data Transport)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction

This section contains the following topics:

Product Overview

In today's business world, file transfer is critical to a company's competitive success. An essential aspect of business strategy is an information technology (IT) department's ability to manage and deliver reliable file transfers. With the redefining of the z/OS system as the enterprise server, file transfers have become an integral ingredient in this strategy.

CA NetMaster FTM helps you to ensure the timely delivery of files that support business critical applications by closely monitoring and automating key transfers. It enables you to increase the reliability of transfers from a variety of file transfer products on multiple systems from a single view. Automation serves to speed notification and resolution of problems for scheduled and unscheduled file transfers.

CA NetMaster FTM can help you unify and simplify the management of your IT environment for greater business results by letting you perform the following tasks:

- Monitor and manage file transfers, including the applications and infrastructure software that support them.
- Use operational information stored in a knowledge base to determine how to monitor the condition of the file transfer service and how to react to the different conditions indicated by events.
- Raise alerts to problems that have occurred or are likely to occur in your file transfer service.
- Monitor several file transfer regions on different systems from one terminal.

What You Can Manage

You can manage the following components of your site's file transfer service:

- File transfer applications that perform the transfers

  You can define application manager and monitor resources to monitor and manage the status and operation of the following file transfer applications:

  - CA SOLVE:FTS
  - CA XCOM Data Transport
  - CONNECT:Direct
  - File Transfer Protocol (FTP) server

- Files transferred or being transferred

  - You can define schedule monitor resources to monitor and manage transfers that are scheduled to start and be completed at a certain time (proactive management).
  - You can define file transfer rules to manage individual transfers as they occur (reactive management).

  CA NetMaster FTM monitors transfers initiated by the supported file transfer applications. Transfers by other methods (for example, IBM's Bulk Data Transfer (BDT) transfers) can be made available to CA NetMaster FTM using the generic data transfer application program interface (API).

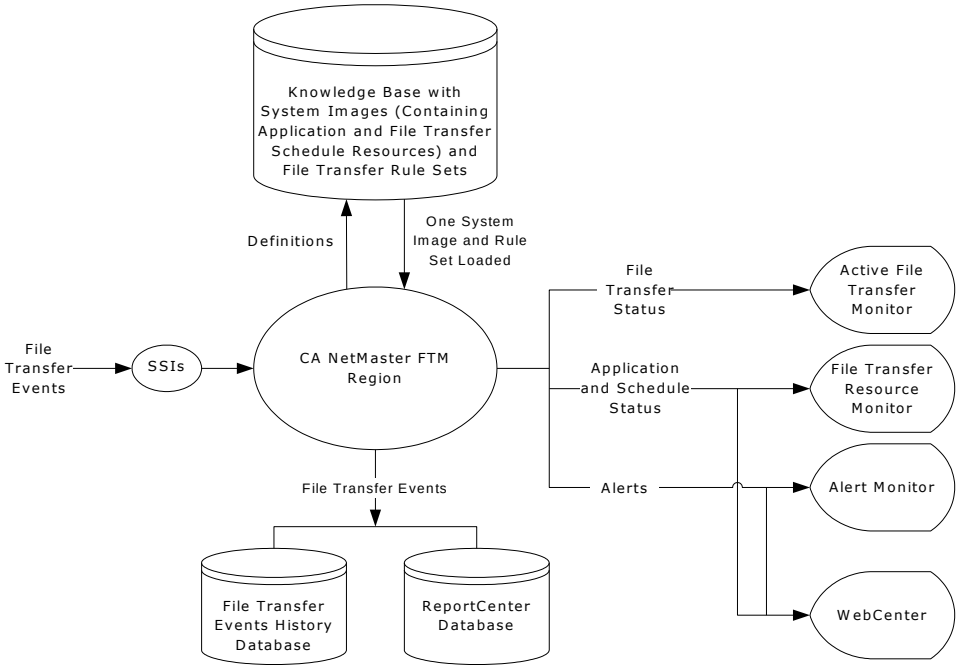
  Note: For information about how to use the generic data transfer API, see the *Administration Guide*.

- File transfer infrastructure that supports the file transfer service

  You can define infrastructure resources to monitor and manage the status and operation of TCP/IP stacks, direct access storage devices (DASDs), and tape devices.

How the Product Works

CA NetMaster FTM is a VTAM application program that runs as an MVS started task on a z/OS system. A running instance (an MVS address space) is called a region (file transfer management region). The following illustration shows the main product components and the flow of data:



File transfer events are processed as follows:

1. Two subsystem interfaces (SSIs) are available to process events before the events are passed to the region: SOLVE SSI and NMFTP Monitor SSI. The SSIs are separate address spaces that run on the same system. Depending on the application that performs the transfer, an event may be processed by none, one, or both of these SSIs. For example, events from CA SOLVE:FTS go to the region directly, while FTP file transfer events from IBM's Communications Server are processed by both SSIs.

   Note: For more information about file transfer event flows, see the *Administration Guide*.

2. When the region receives the file transfer events (and system events), it acts on them according to the definitions in the loaded system image and file transfer rule set. A system image contains resource definitions such as file transfer application managers and file transfer schedule monitors; a rule set contains file transfer rules. You can define multiple system images and file transfer rule sets in the region's knowledge base, but only one of each is loaded and active.

3. Based on the information in the events, the region presents the health of your file transfer service on various displays. You can define filters to select what you want to display.
   - The Active File Transfer Monitor shows the status and details of individual transfers (for example, a transfer has started and is in progress). You can terminate transfers from this display.
   - The File Transfer Resource Monitor shows the status of managed applications and file transfer schedules (for example, the time when a schedule will start).
   - The Alert Monitor shows alerts that warn you of any problems or critical activities (for example, an alert indicating a transfer failure generated by a file transfer rule because the rule criteria are satisfied).
   - WebCenter provides a web-based display for application and schedule status, and alerts.
4. The region stores start, completion, and failure event records in a history database and, if ReportCenter is configured, in the ReportCenter database. These databases let you report on file transfer activities, which can help you plan your file transfer service. Reports on the history database are 3270-based; while reports on the ReportCenter database are web-based, using WebCenter, and provide a richer presentation with graphs.

Multisystem Support

Multisystem support provides you with a single point of visibility for all the managed file transfers and supporting resources that you want to manage.

You can link file transfer management regions together to provide an enterprise view of the managed file transfer service. These linkages are not restricted by a sysplex.

In a multisystem network where each region manages the resources defined to its own loaded system image, failure of one region does not affect the automated operation of resources on the other systems, and you can still have an enterprise view of the resources managed on those systems.

A multisystem network can consist of the following:

- Focal point regions—you have visibility of all the managed file transfers and supporting resources.
- Subordinate regions—you have visibility of the locally managed file transfers and supporting resources only. By using subordinates, you reduce the amount of traffic in the multisystem network.

Note: For more information about multisystem support, see the *Administration Guide*.

How Product Deployment Works

Typically, product deployment consists of the following stages:

1. Install CA NetMaster FTM. The process installs the product using SMP/E.
   a. Transfer the software to your system.
   b. Use Install Utility to install the software.
2. Set up the product for a system. The process sets up the started tasks and configures other software to work with CA NetMaster FTM.
   a. Use Install Utility to set up the following region and interfaces:
      - A management region that monitors and lets you manage your file transfer service
      - A SOLVE SSI that provides communication between the region and other software
      - (Only if you are using IBM's Communications Server) An NMFTP Monitor SSI that obtains FTP file transfer-related system management facilities (SMF) records
   b. Use Install Utility to create VTAM definitions and tables for the access method control blocks (ACBs) required by the management region.
   c. Configure the management region, interfaces, and your communications server to enable the flow of FTP events to CA NetMaster FTM.
   d. Configure other file transfer applications to enable the flow of application events to CA NetMaster FTM.
3. Start the interfaces.
4. Start the management region, and perform initial customization.

5. Implement your file transfer management environment.

   a. Define resources and rules.

      - Determine the applications that perform the file transfers you want to monitor and manage, create a system image, and define resources for those applications in the system image.
      - Determine the scheduled file transfers you want to monitor and manage, and define resources for the schedules in the system image.
      - Determine the file transfers you want to monitor and manage, create a rule set, and define rules for them.

   b. Load the rule set and system image.

   The management region starts to monitor your file transfer service based on the defined rules and resources. You can use the displays (such as the Active File Transfer Monitor for individual transfers and the File Transfer Resource Monitor for application resources) to view their status.

6. Set up user security for the management region.
7. Deploy the product on each system where you want to manage file transfers. You can then link CA NetMaster FTM on those systems together to provide a multisystem view of your file transfer activities from a single management region.

Note: Details about how to complete the stages are in the following guides:

- For steps 1 to 4, see the *Installation Guide*.
- For steps 5 and 7, see the *Administration Guide*.
- For step 6, see the *Security Guide*.

More information:

How You Define File Transfer Application Resources (see page 19)

How You Implement Your File Transfer Management Environment

Implementation consists of analyzing, and the definition of resources and rules to manage your file transfer service. Typically, the process consists of the following stages:

1. Identify what can impact the service (for example, the file transfer applications used by the service and the file transfer schedules that need to be met to satisfy service-level agreements (SLAs)).
2. Define the relevant application and schedule monitor resources.
3. After the initial implementation has been running for a period, review the historical data to identify problems and statistics:
    a. Adjust your file transfer service in response to the problems and statistics.
    b. Update the application and schedule monitor resources to reflect the adjustments you make to your file transfer service, and in response to perceived problems.
    c. Define file transfer rules in response to perceived problems.
4. Repeat Step 3 to improve your implementation continuously.

More information:

How You Define File Transfer Application Resources (see page 19)
How You Manage Scheduled File Transfers (see page 25)
How You Use Historical Data for Planning (see page 23)

Chapter 2: Monitoring File Transfers

This section contains the following topics:

How You Monitor File Transfers

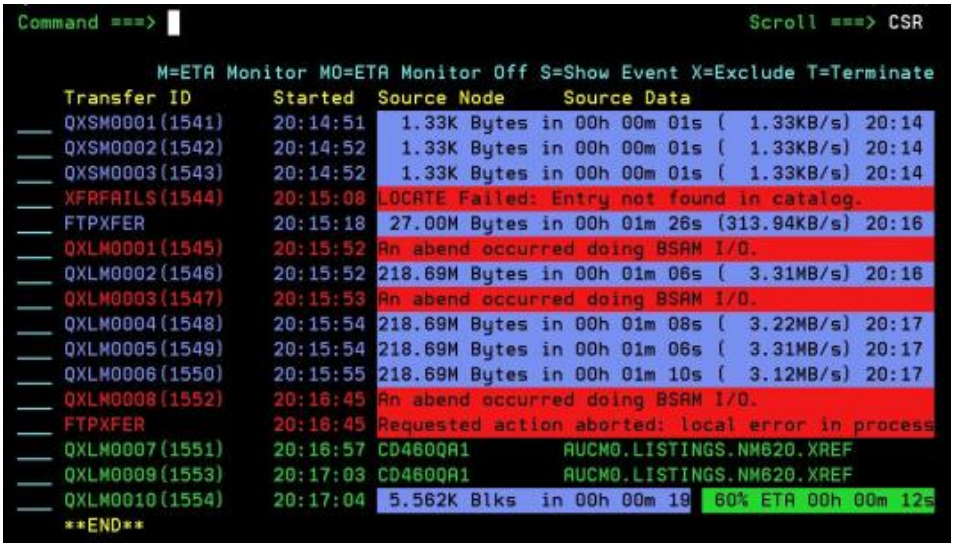
The Active File Transfer Monitor is where you can monitor the status and view the details of file transfers as they occur, and are detected by the region. You access the monitor using the /AFTMON panel shortcut.

You should be able to see the FTP transfers immediately. To see transfers by a supported application such as CA SOLVE:FTS and CONNECT:Direct, you must define a manager resource for it in the loaded system image. To see transfers by other methods, you must use the generic data transfer API.

Failed or completed transfers are removed from the monitor after a period specified in the FTMONITOR region parameter group, but you can still view their details in the history database.

Example: Active File Transfer Monitor Display

The following illustration shows an example of the information displayed on the monitor. You can press F11 to scroll to the right to display additional information such as information about the target (the recipient of a transfer).



The example shows sample transfers with various statuses:

- Transfers that have failed, for example:

  ```
  XFRFAILS(1544)    20:15:08 LOCATE Failed: Entry not found in catalog.
  ```

  These transfers are displayed in red.

- Transfers that have completed, for example:

  ```
  QXSM0001(1541)    20:14:51   1.33K Bytes in 00h 00m 01s (  1.33KB/s) 20:14...
  ```

  These transfers are displayed in blue.

- Transfers that are in progress, for example:

  ```
  QXLM0007(1551)    20:16:57 CD460QA1        AUCM0.LISTINGS.NM620.XREF
  ```

  These transfers are displayed in green.

  If estimated-time-of-arrival (ETA) monitoring is enabled for a transfer, it shows both the bytes transferred so far and the estimated time for the transfer to complete, as indicated by the last transfer listed in the illustration.

  Note: For more information about ETA monitoring, see the *User Guide*.

Display File Transfer Details

You can display the details of a file transfer on the Active File Transfer Monitor. For example, if a transfer has failed, you want to find out about it so that the failure can be corrected.

To display the details of a file transfer, enter **S** next to it.

Example: Details of a Failed CONNECT:Direct File Transfer

The following illustration shows the details of the failed file transfer (ID XFRFAILS(1544)) that was initiated by the CD460 CONNECT:Direct region. It identifies the affected transfer, and shows the failure and ABEND codes.

```
FILE TRANSFER DETAILS:
======================
     File Transfer Product ....... CONNECT:Direct
     Task Name ................... CD460
     User Name ................... USER01
     Status ...................... FAILURE
     Transfer ID ................. XFRFAILS(1544)

     Source Data ................. CODE0.LISTINGS.NM620.FILE
            System/Node .......... CD460
     Target Data ................. CODE0.USER01.CD460.Q5201501.DSRFXF1
            System/Node .......... CD460

     Failure Code ................ TRANFAIL
     Abend Code .................. SDE1708I
     Retried (Y/N) ............... N
     Failure Reason .............. LOCATE Failed: Entry not found in catalog.

     Start Date .................. 14-MAY-2008
          Time ................... 20:15:08
          GMT Offset ............. -0400
       End Date .................. 14-MAY-2008
          Time ................... 20:15:08
          GMT Offset ............. -0400

     Step name of COPY ........... CPY
--------------------------------------------------------------------------------
EVENT DETAILS:
==============
     Event Issue Date ............ 14-MAY-2008
                 Time ............ 20:15:09
```

Example: Details of a Completed FTP File Transfer

The following illustration shows the details of the completed FTP file transfer (ID FTPXFER). It identifies the transfer, and shows the volume and rate of the transfer.

```
FILE TRANSFER DETAILS:
======================
     File Transfer Product ....... IPSERVER
     Task Name ................... FTPD311
     User Name ................... OMVS
     Status ...................... END
     Transfer ID ................. FTPXFER
     Transfer Duration ........... 86  (00.01.26)
     Bytes Transferred ........... 27000000  (27.000M)
     Transfer Rate (Bytes/sec) ... 313.940K
     Compression (%) ............. None

     Source Data ................. ( -- Not Available -- )
            System/Node .......... 172.24.138.151
     Target Data ................. /u/users/opsdev/help/shared/portal_tab_selec
            System/Node .......... 192.168.65.31

     Start Date .................. 14-MAY-2008
           Time .................. 20:15:18
           GMT Offset ............ -0400
       End Date .................. 14-MAY-2008
           Time .................. 20:16:44
           GMT Offset ............ -0400

     Local TCP Port Number ....... 20
     Remote TCP Port Number ...... 4446
     Data Transfer Operation Type  STORE
     FTP Stack Name .............. TCPIP31
     Data Set Type ............... HFS
     Data Type ................... BINARY
     Transmission Mode ........... STREAM
--------------------------------------------------------------------------------
EVENT DETAILS:
==============
     Event Issue Date ............ 14-MAY-2008
                 Time ............ 20:16:53
```

Customize Your Active File Transfer Monitor

You can customize how information is displayed on the Active File Transfer Monitor to make it more manageable. For example, you can create a filter and use it to exclude certain types of file transfers, use the X action to exclude specific transfers, and sort the displayed transfers in a certain way. If you want to use the same filter and sort order whenever you access the monitor, you can add them to your profile.

To create a filter, enter the **/FTADMIN.F** panel path to access the list of Active File Transfer Monitor filters and add it there. For example, you can limit the display to only those transfers that have failed.

To apply a filter to the monitor, enter **FILTER** and select the required filter from the displayed list.

To exclude a displayed transfer, enter **X** next to it. For example, you may want to exclude a transfer that you know is of no consequence to your business.

To sort your display, enter **SORT** and select the column you want to sort on. You can enter SORT *sort_column_1*, *sort_column_2*, *sort_column_3* to sort your display on up to three columns.

To add the filter and sort order to your profile, enter **PROFILE** and complete the relevant fields.

How You Define File Transfer Application Resources

For the Active File Transfer Monitor to display file transfers by a supported application such as CA SOLVE:FTS, you must define an application manager resource for it in the loaded system image. Defining a manager resource also enables you to manage the file transfer application by automating responses to application events. In addition, you can define application monitor resources to look after certain internal states of the manager. For example, with CA XCOM Data Transport, you can define a monitor to alert you to stalled transfers.

Note: For more information about manager and monitor resources, see the *Administration Guide*.

You can use the following process to define your application resources:

1. CA NetMaster FTM provides an AutoAssist facility that helps you define resources. You access the facility using the /RADMIN.AD panel shortcut, which displays the Assisted Resource Definition menu.
2. The menu provides an option for each of the supported applications. For example, to define resources for CA XCOM Data Transport, you select Option XC. You are asked to create a system image for the resources if the knowledge base contains no existing images (for example, the first time you use a new region), or you are presented with a list of existing images that you can select. You must have a system image before you can define any resources.
3. After you have created or selected the image, you complete the application's Manager General Description panel to define the manager resource. One of the fields you must specify is Manager Type, which determines the template to use for defining this resource.

   A *resource template* provides predefined values for the definition of commonly-used resources. These values specify, for example, how to manage the starting and stopping of the application, and how to respond to changes in the application status. CA NetMaster FTM includes templates for various resource types.
4. After the manager resource is defined, you define the monitor resources for the manager from the application's Manager List panel using the G action. Again, the Type field in a monitor resource definition determines the template to use.
5. The AutoAssist facility helps you define your resources by using distributed templates. You can review these defined resources and, if required, update them to suit your environment. An application's Manager List panel lets you access the manager definitions, and the MON action on that panel lets you access the monitor resources defined for a manager. You can access the list of managers at any time through the /RADMIN.R panel shortcut.
6. For the region to use the defined resources, you must load the image that contains them. You can do this from the File Transfer Resource Monitor using the LOAD command. To enable loading to occur automatically when the region starts, you must specify it in the AUTOIDS region parameter group. (You can access the list of parameter groups using the /PARMS panel shortcut.)

How You Monitor File Transfer Applications

You can monitor and act on file transfer application resources in a loaded system image from the File Transfer Resource Monitor. You access the monitor using the /FTMON panel shortcut.

Example: File Transfer Resource Monitor

The following illustration shows an example of monitored file transfer resources.

```
PROD12#11------------- File Transfer Resource Monitor ----------------CO11-0002
Command ===>                                                 Scroll ===> PAGE

        S=Status L=Transient Log D=Display A=Act T=Term DB=Database ?=List Cmds
    System   Class  Resource       Desired  Actual     Mode       Logical   Ovr
    CO11     FTPMGR FTPD111        ACTIVE   ACTIVE     MANUAL     OK
    CO11     FTPMON FTPD111.CO31   SERVCO31 AVAILABLE AT 01.19
    CO11     FTPMON FTPD111.CONNEC 0 CONNECTIONS CHECKED. ALL OK AT 00.51
    CO11     FTPMON FTPD111.LISTEN LISTENER TASK FOUND AT 00.48 PORT 21
    CO11     XCMGR  XC300DE2       XC300DE1 NOT AVAILABLE AT 00.51
    CO11     XCMON  XC300DE2.ACTIV STATUS(ACTIVE) CNT(0) AT 00.47
    CO11     XCMON  XC300DE2.CONNE 0 CONNECTIONS CHECKED. ALL OK AT 00.51
    CO11     XCMON  XC300DE2.HOLD  STATUS(HELD) CNT(0) AT 00.47
    CO11     XCMON  XC300DE2.INACT STATUS(INACTIVE) CNT(0) AT 00.47
    CO11     XCMON  XC300DE2.LISTE LISTENER TASK FOUND AT 00.51 PORT 8745
    CO11     XCMON  XC300DE2.STALL NO TRANSFERS FOUND AT 00.51
    CO11     XCMON  XC300DE2.SUSPE STATUS(SUSPENDED) CNT(0) AT 00.47
    CO11     XCMON  XC300DE2.XC300 XC300DE1 NOT AVAILABLE AT 00.51
    **END**
```

The example shows the status of an FTP manager resource (FTPD111), a CA XCOM Data Transport manager resource (XC300DE2), and associated monitor resources:

- The FTPD111 FTP manager resource monitors the status of the FTP server. It owns the following monitor resources:
  - FTPD111.CO31, which monitors a remote FTP server (a file transfer partner)
  - FTPD111.CONNECT, which monitors file transfer connections to the server
  - FTPD111.LISTEN, which monitors the listener
- The XC300DE2 CA XCOM Data Transport manager resource monitors the status of the CA XCOM Data Transport application. It owns the following monitor resources:
  - XC300DE2.ACTIVE, which monitors active file transfer requests
  - XC300DE2.CONNECT, which monitors the file transfer connections
  - XC300DE2.HOLD, which monitors held requests
  - XC300DE2.INACTIVE, which monitors inactive requests
  - XC300DE2.LISTEN, which monitors the listener
  - XC300DE2.STALLS, which watches for stalled file transfers
  - XC300DE2.SUSPEND, which monitors suspended requests
  - XC300DE2.XC300DE1, which monitors a remote CA XCOM Data Transport application (a file transfer partner)

The example indicates that all the monitored resources are in their normal operating state, except for the CA XCOM Data Transport remote node monitor (XC300DE2.XC300DE1), which indicates that the XC300DE1 file transfer partner is not available.

How You Use Historical Data for Planning

You can see the file transfers in action on the Active File Transfer Monitor and can react to them as problems occur. Historical data, on the other hand, helps you minimize future problems. There are two sources of historical data: the history database and the ReportCenter database.

You access the history database through the History Data menu, using the /FTHIST panel shortcut. You can search the database and generate reports using predefined or your own criteria. You can also use Report Writer (accessible using the /RW panel shortcut) to design your own 3270-based reports.

The following examples show how you can use historical data:

- If the data indicates that critical transfers are failing for the same reason, you can define rules to provide automated recovery for those failures.
- You can identify expected transfers that do not occur, which you can define schedule resources to monitor.
- You can identify FTP transfers to unauthorized sites and define rules to provide automated alerting.

Note: The history database is cleared periodically as specified in the EVENTLOG region parameter group. However, you can specify that the data be archived before clearance.

If you have implemented ReportCenter, you can generate predefined web-based reports on transfers stored in the ReportCenter database over time, for example:

- If you have implemented multisystem file transfer management, you can compare the load (for example, total bytes transferred and average transfer rate) between systems.
- You can show where transfers are busiest by source and destination.

Example: Storage Problems

Your business is impacted by file transfer storage problems at a certain destination. You want to find out the cause so you can plan for future occurrences of these problems.

1. You use ReportCenter to generate a File Transfer Address Analysis report for the destination to find out about its file transfer activities. You notice that occasionally there are a large amount of inbound bytes. You suspect that occasional transfer of huge files may be taking up the storage space, thus impacting some more critical transfers.
2. You know that all critical transfers to that destination are below a certain size. So, to confirm your suspicion, you search the history database using the destination and byte count as criteria. You find a number of transfers that match the criteria. They are unscheduled transfers from various users and are not critical.
3. You decide to move these huge files somewhere else as they arrive to free up storage for the critical transfers and notify the users who perform the transfers. You can automate these actions using a file transfer rule (see page 31).

Chapter 3: Managing Scheduled File Transfers

This section contains the following topics:

How You Manage Scheduled File Transfers

The Active File Transfer Monitor tells you if a file transfer is in progress, has completed, or has failed. The monitor does not alert you if an expected transfer does not occur or arrive within a scheduled period. To manage scheduled file transfers, you can define schedule monitor resources in the loaded system image.

In a schedule monitor resource definition, you can specify the following criteria and actions:

- The schedule within which transfers occur

  A schedule can have multiple transfer instances repeated at specific times. You can divide the time allocated for each instance into a preprocessing period, a processing period, and a post-processing period. This division enables you to perform some action for each period to support the transfers.

  For example, at the start of preprocessing, you can specify that the resource checks that required files are ready for transfer and raises an alert if the files are not ready. The alert lets you take corrective action before the transfer instance starts.

- The files scheduled to be transferred
- The recovery action for failed transfers, enabling them to be corrected within the scheduled period

You can monitor and act on these resources from the File Transfer Resource Monitor.

For a resource to manage the scheduled file transfers, it must be defined in the loaded system image. You can define the resource from the File Transfer Resource Monitor as follows:

1. Press F4 to add a resource.
2. Select the system image to which you want to add the resource.
3. Select the FTSCHD resource class to add a schedule monitor resource.
4. Complete the definition of the resource.

Example: Account Reporting

You have an SLA to provide account reports every Monday on client data you receive the previous Friday. The data is in a number of files transferred using FTP. You decide to use a file transfer schedule monitor resource definition to help you satisfy the SLA:

1. You specify a schedule window for the transfer on the Schedule panel of the definition:
   - You specify a preprocessing period before the expected start of the transfer so that you can check that you have enough storage to receive the files.
   - You specify a post-processing period after the expected completion of the transfer so that, if failure occurs, you can correct it before reports are generated from the transferred files.
2. You identify the files to monitored within the schedule window on the File Filters panel.
3. You create the following process definitions and specify them on the State Change Exits panel to automate actions:

   Note: A *process* is a definition you can create to automate a series of actions. It uses macros (distributed with the product) to perform those actions. You define processes through the Global Process List panel, which you access using the /RADMIN.GP panel shortcut. For more information about processes, see the *Administration Guide*.

   - A process to run at the start of the schedule window to check storage space (using the SYSCMD macro) and raise an alert (using the GENALERT macro) on shortage so that corrective actions can be taken
   - A process to run at post-processing to raise an alert (using the GENALERT macro) on failure so that corrective actions can be taken
   - A process to run at the end of the schedule window to submit the reporting job (using the SUBJOB macro) so that the reports can be transferred and ready for the client on Monday
4. You create a process definition and specify it on the Event Exits panel to raise alerts on individual failed file transfers, enabling you to correct the problems before the expected completion of the transfer. However, this exit does not tell you if a file has not arrived. The process you run at post-processing can catch this failure.

To ensure that your client actually receives the reports on time, you can create another resource to monitor the scheduled transfer of the reports.

How You Monitor Scheduled File Transfers

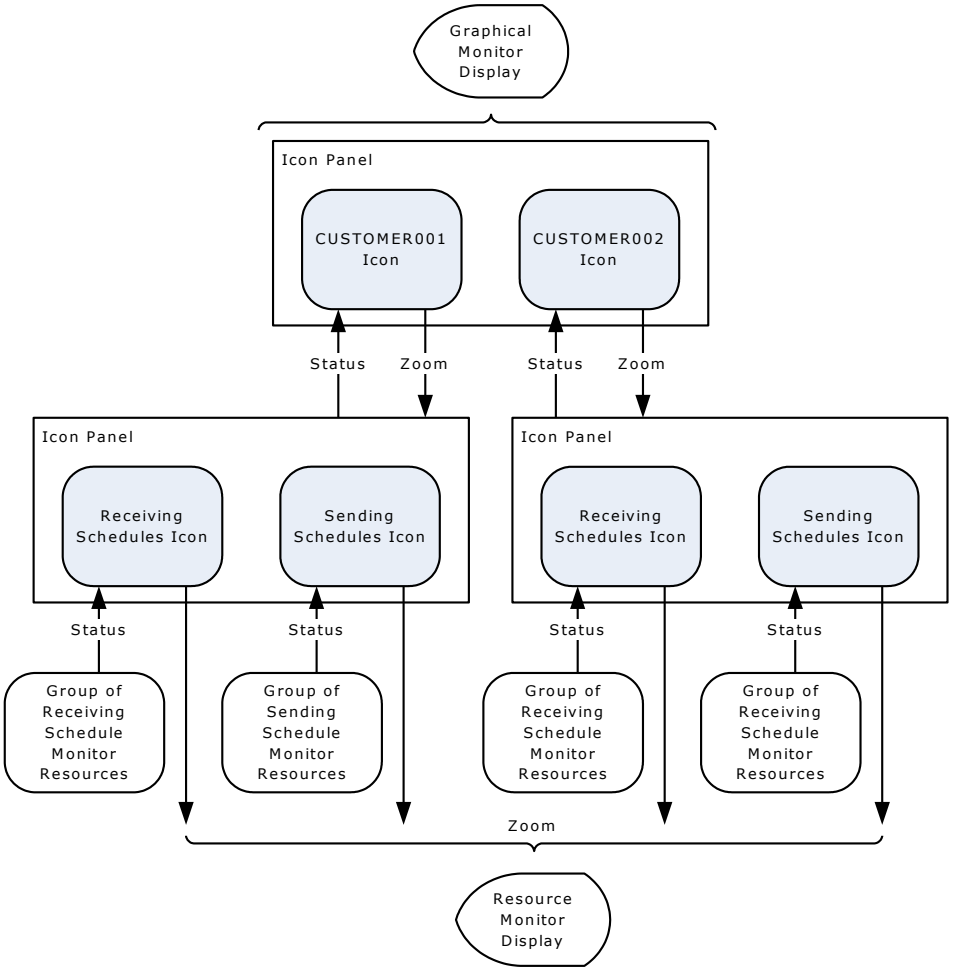
As you monitor file transfer applications (see page 21), you can monitor and act on FTSCHD-class file transfer schedule resources in a loaded system image from the File Transfer Resource Monitor.

The File Transfer Resource Monitor lets you monitor defined resources individually. If you have a large number of logically related resources, you can use the graphical monitor to monitor them as a group. The monitor presents the status of resources in icons on icon panels. The status of the group icon reflects the status of the underlying resources. You can have multiple groups, each consisting of logically related resources. You customize the graphical monitor to suit your requirements through its Administration Menu panel, which you access using the /GADMIN panel shortcut.

Note: For information about how to customize the graphical monitor, see the *Administration Guide*.

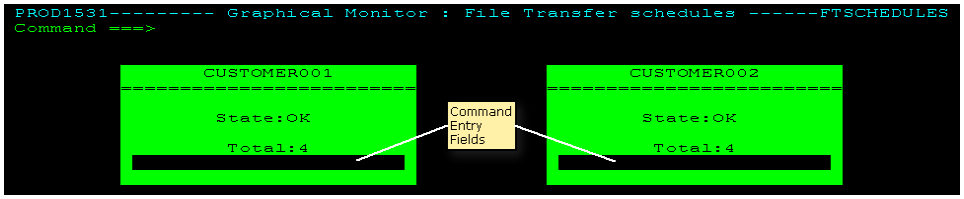
Example: Graphical Monitor

You have SLAs with two customers to provide reports on client data. To satisfy the SLA for each customer, you want to ensure that client data is received from and reports sent to the customer on time. You determine that a number of file transfer schedules must be completed and define file transfer schedule monitor resources for them. You then customize the graphical monitor using the following structure:



The status of the schedule monitor resources is passed to the graphical monitor. If a customer icon shows a problem, you can zoom into the schedule icons to determine whether the problem is with the receiving or sending of files. If, for example, there is a problem with receiving, you can zoom into the individual schedule monitor resources represented by the icon and determine which schedule is causing the problem.

The following example shows an entry panel. It shows four schedules associated with each customer and that they are currently in the OK state. Each icon provides a command entry field where you can enter the Z (Zoom) command.



Chapter 4: Managing Individual File Transfers

This section contains the following topics:

How You Manage Unscheduled File Transfers

You have seen how you can define resources to help you manage scheduled file transfers. However, there are other transfers occurring in your environment that are not scheduled. The Active File Transfer Monitor lets you monitor these transfers, but you can also manage them by defining rules to detect them and provide appropriate responses. For example, you can define rules to detect unauthorized transfers and raise alerts when they occur.

You can use the following process to define your file transfer rules:

1. Before you can define any rules, you must define a rule set to hold them. You define rule sets through the File Transfer Ruleset List panel, which you access using the /FTADMIN.R panel shortcut.
2. After you defined a rule set, you can add rules to it. The R action lets you access the File Transfer Rules panel from which you can add rules.
3. For the region to use the defined rules, you must load the rule set that contains them. You can do this from the File Transfer Ruleset List panel using the L action. To enable automatic loading when the region starts, you must specify the rule set in the AUTOIDS region parameter group.

Example: Storage Problems

Storage problems require you to move some huge transferred files to somewhere else to free up storage for critical file transfers. You decide to automate this using a file transfer rule:

- To detect the right transfers, the rule matches all completed incoming transfers with a Boolean expression of destination (TGTADDR) and byte count (XFRAMT).
- On detection of a matched transfer, the rule performs the following actions:
  - Execute a Network Control Language (NCL) procedure that moves the file. The file to be moved can be identified using the &ZRFTGTFNAME variable.

    Note: For information about NCL, see the *Network Control Language Programmer Guide* and the *Network Control Language Reference Guide*.
  - Notify the user who performed the transfer of the new location of the file. The user to be notified can be identified using the &ZRFUSER variable.

Index