Unicenter

NetMaster File Transfer Management Implementation, Administration, and Operations Guide

10th edition - update 1

P01-196

Booklist

Computer Associates
The Software That Manages eBusiness

Edition	Publication Number	Product Version	Min. MS Level	Publish Date
10th Edition—Update 1	P01-196	Version 5.0	MS 5.0	April 2002

This documentation and related computer software program (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by Computer Associates International, Inc. ("CA") at any time.

This documentation may not be copied, transferred, reproduced, disclosed or duplicated, in whole or in part, without the prior written consent of CA. This documentation is proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of this documentation for their own internal use, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the confidentiality provisions of the license for the software are permitted to have access to such copies.

This right to print copies is limited to the period during which the license for the product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to return to CA the reproduced copies or to certify to CA that same have been destroyed.

To the extent permitted by applicable law, CA provides this documentation "as is" without warranty of any kind, including without limitation, any implied warranties of merchantability, fitness for a particular purpose or noninfringement. In no event will CA be liable to the end user or any third party for any loss or damage, direct or indirect, from the use of this documentation, including without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised of such loss or damage.

The use of any product referenced in this documentation and this documentation is governed by the end user's applicable license agreement.

The manufacturer of this documentation is Computer Associates International, Inc.

Provided with "Restricted Rights" as set forth in 48 C.F.R. Section 12.212, 48 C.F.R. Sections 52.227-19(c)(1) and (2) or DFARS Section 252.227-7013(c)(1)(ii) or applicable successor provisions.

© 2002 Computer Associates International, Inc. (CA)

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Table of Contents

Part I General Information

Chapter 1 Introduction 1-1

What the Product Offers 1-2

Features and Benefits..... 1-3
- Knowledge Base..... 1-4
  - File Transfer Rules..... 1-5
  - File Transfer Schedules..... 1-5
  - CA-XCOM Resources 1-5
  - CONNECT:Direct Resources 1-6
  - CONNECT:Mailbox Resources..... 1-7
  - File Transmission Services (FTS) Resources 1-7
  - File Transfer Protocol (FTP) Resources 1-8
  - Other Supporting File Transfer Resources 1-8
  - System Images 1-8
  - Templates..... 1-9
- Message Visibility..... 1-9
- Monitors 1-10
  - Active File Transfer Monitor 1-10
  - Alert Monitor 1-10
  - Status Monitor..... 1-10

File Transfer Resource Control 1-10
CA-XCOM Resources 1-10
CONNECT:Direct Resources 1-11
CONNECT:Mailbox Resources..... 1-11
FTS Resources 1-11
FTP Resources 1-12
Other Supporting Resources 1-12
Automation Engine 1-13
Multisystem Support 1-13
Focal Point Regions 1-13
Subordinates..... 1-14
Agents 1-14
File Transfer Logs 1-14
Automatic Problem Recording..... 1-14
Automatic Generation of SNMP Traps 1-14
Reporting Function..... 1-15
FTP Function Policy Control 1-15

About this Guide..... 1-15

What You Should Know Already..... 1-16

Chapter 2 File Transfer Management Resources 2-1

What Are File Transfer Management Resources?..... 2-2

File Transfer Rules 2-2
Criteria..... 2-2
Actions 2-3

File Transfer Schedules 2-3

Chapter 3 File Transfer Application Resources..... 3-1

What Are File Transfer Resources?..... 3-2
File Transfer Manager..... 3-2
File Transfer Monitors 3-2

Operational Relationship Between a File Transfer Monitor and Its Manager 3-2
Owned Resource Names 3-3

What Is a CA-XCOM Resource? 3-3
CA-XCOM File Transfer Manager..... 3-3
CA-XCOM File Transfer Monitors 3-4

The CA-XCOM File Transfer Manager Definitions 3-4
CA-XCOM Manager Templates for Jobs and Started Tasks..... 3-4

The CA-XCOM File Transfer Monitor Definitions 3-5
Transfer Request Monitor Templates..... 3-5
Stalled Transfer Monitor Templates 3-6
TCP/IP Listener Task Monitor Template..... 3-6
TCP/IP Connections Monitor Template..... 3-7
Remote Node Monitor Template 3-7

Event Flow from a CA-XCOM File Transfer Service..... 3-8

What Is a CONNECT:Direct Resource? 3-9
CONNECT:Direct File Transfer Manager..... 3-9
CONNECT:Direct File Transfer Monitors 3-10

The CONNECT:Direct File Transfer Manager Definitions 3-10
CONNECT:Direct Manager Templates for Jobs and Started Tasks 3-10
CONNECT:Direct Manager Template for Distributed Systems Applications 3-11

The CONNECT:Direct File Transfer Monitor Definitions 3-11
Process Queue Monitor Templates 3-11
Process Status Monitor Templates 3-12
Transfer Monitor Templates 3-12
TCP/IP Listener Task Monitor Template..... 3-13
TCP/IP Connections Monitor Template..... 3-13
Remote Node Monitor Template 3-13

Event Flow from a CONNECT:Direct File Transfer Service 3-14
MVS or OS/390 System..... 3-14
Distributed Systems 3-15

What Is a CONNECT:Mailbox Resource..... 3-17
CONNECT:Mailbox VSAM File Server..... 3-17
CONNECT:Mailbox Manager..... 3-17
CONNECT:Mailbox Monitors..... 3-18

CONNECT:Mailbox VSAM File Server Definitions..... 3-18
VSAM File Server Template 3-18

CONNECT:Mailbox Manager Definitions..... 3-18
The CONNECT:Mailbox Manager Template..... 3-19

CONNECT:Mailbox Monitor Definitions..... 3-19
Auto Connect Queue Monitor Template..... 3-19
BSC Line Monitor Template..... 3-19
Stalled SNA Session Monitor Template 3-20

Event Flow from CONNECT:Mailbox 3-21

What Is an FTS Resource? 3-22
FTS File Transfer Manager 3-22
FTS File Transfer Monitors 3-22

The FTS File Transfer Manager Definitions 3-23
FTS Manager Templates for Jobs and Started Tasks 3-23
FTS Manager Template for Remote Regions 3-23

The FTS File Transfer Monitor Definitions 3-23
INMC Link Monitor Template 3-24

Event Flow from an FTS File Transfer Service 3-24

What Is an FTP Resource? 3-25
FTP File Transfer Manager 3-25
FTP File Transfer Monitors 3-25

The FTP File Transfer Manager Definitions 3-26
FTP Manager Templates for Jobs and Started Tasks 3-26
Customizing TCPaccess FTP Server Templates 3-26

The FTP File Transfer Monitor Definitions 3-26
TCP/IP Listener Port Monitor Template 3-27
TCP/IP Connections Monitor Template 3-27
Remote Node Monitor Template 3-28

Event Flow from an FTP File Transfer Service 3-29

Chapter 4 Supporting File Transfer Resources 4-1

What Are the Supporting File Transfer Resources? 4-2

The IBM TCP/IP Resource Definitions 4-2
Communications Server Resource Templates 4-2

The TCPaccess Resource Definition 4-3
TCPaccess Resource Template 4-3

The DASD and Tape Resource Definitions 4-3
DASD and Tape Resource Templates 4-3

Part II Implementation and Administration

Chapter 5 Implementing the Product Region 5-1

Gather Information Now 5-2

Task 1—Logging On for First-time Customization 5-2
- Specifying the CONNECT:Direct Interface Parameters 5-6
- Specifying the CONNECT:Mailbox Interface Parameters 5-10
- Implementing the TCP/IP Interface 5-11
  - TCP/IP Client Program Configuration Dataset 5-12
- Dealing with Initialization Failures 5-13
  - Using the Initialization In Progress Dialog 5-14
- Generating an INI Procedure 5-15
  - Using an INI Procedure to Propagate Customized Parameter Group Records to Other Regions 5-16

Task 2—Defining Resources to Your Region 5-16

Task 3—Defining the Administrator 5-18

Task 4—Implementing Your Template System 5-19

Task 5—Implementing Printers 5-20

Task 6—Implementing Logging 5-21
- Subtask 6.1—Implementing File Transfer Logging 5-22
  - Allocating File Transfer Log Files 5-22
  - Disabling File Transfer Logging 5-24
- Subtask 6.2—Customizing Activity Log Settings 5-24
  - Controlling Operating System Message or Command Logging 5-25
  - Allocating Activity Log Files 5-25
- Subtask 6.3—Enabling File Transfer Schedule Logging 5-26

Task 7—Customizing the Managed File Transfer Regions 5-27
Subtask 7.1—Customizing the Managed CA-XCOM Regions..... 5-28
Subtask 7.2—Customizing the Managed CONNECT:Direct Regions..... 5-29
Subtask 7.2.1—Implementing Statistics Exits in the Managed CONNECT:Direct Regions 5-29
Subtask 7.2.2—Customizing CONNECT:Direct Initialization Parameters..... 5-31
Subtask 7.2.3—Defining the NetMaster for File Transfer Region as a CONNECT:Direct User 5-32
Customizing the $RFXPRMS NCL Procedure..... 5-33
Subtask 7.3—Customizing the Managed CONNECT:Mailbox Regions..... 5-34
Subtask 7.3.1—Implementing the Log Exit in the Managed CONNECT:Mailbox Regions..... 5-35
Subtask 7.3.2—Customizing CONNECT:Mailbox Initialization Parameters 5-36
Subtask 7.4—Customizing the Managed FTS Regions..... 5-36
Subtask 7.4.1—Defining the Link to the NetMaster for File Transfer Region 5-36
Subtask 7.4.2—Defining the NetMaster for File Transfer Region as an FTS User 5-37
Subtask 7.4.3—Installing the FTS Message Handler 5-37

Task 8—Implementing the FTP Event Flow..... 5-38
Subtask 8.1—Setting Up TCP/IP to Generate SMF Records 5-39
Setting Up Communications Server to Generate SMF Records 5-40
Setting Up TCPaccess to Generate SMF Records..... 5-41
Subtask 8.2—Implementing the SMF Exit for the FTP Receiver . 5-42
Implementing the SMF Exit for IBM’s TCP/IP 5-42
Subtask 8.3—Customizing FTPCNTL Parameter Group (Non-TCPaccess FTP) 5-42
Subtask 8.4—Setting Up SAF Access for Maintaining Policy Rule Sets..... 5-44
Defining $SOLVE.FTP.CONTROL to Your Security System 5-44
Subtask 8.5—Customizing FTPCNTL Parameter Group (TCPaccess FTP)..... 5-45

Task 9—Enabling the Interface Between NetMaster for File Transfer and TCP/IP 5-47
Enabling the Interface to Communications Server 5-47
Authorizing the Started Task User ID 5-48
Authorizing the Interface Between NetMaster for File Transfer and Communications Server 5-49
Enabling Access to SNMP Data in Communications Server ... 5-50
Enabling Name Resolution 5-51
Enabling the Interface to TCPaccess..... 5-51
Reviewing the Parameter Data Set 5-52
Enabling Access to SNMP Data in TCPaccess..... 5-53
Setting Up DNR Members..... 5-53

Task 10—Implementing a SOLVE:Problem Automatic Problem Recording Environment..... 5-54
Subtask 10.1—Copying the $RMPB07S NCL Procedure..... 5-54
Subtask 10.2—Authorizing Users in the SOLVE:Problem Region 5-54
Subtask 10.3—Defining Links..... 5-54

Task 11—Implementing the Alert Monitor Problem Ticket Interface. 5-55
Defining a Problem Ticket Interface..... 5-56
Defining an E-mail Problem Ticket Interface..... 5-56
Defining a Custom Problem Ticket Interface 5-58
Setting up the Problem Ticket Data Definition..... 5-59

Task 12—Implementing Alert Forwarding 5-60
Implementation 5-60
The SNMP Trap Definition..... 5-60
$AMEVFWD 5-61
Function 5-61
Use 5-61
Operands 5-61
Notes 5-64

Task 13—Implementing Event Recording and Reporting 5-65

Task 14—Implementing the NetMaster Reporter Interface 5-68
Subtask 14.1—Defining the Data Warehouse Server 5-68
Subtask 14.2—Logging Events to the Data Warehouse 5-69

What to Do Next 5-69

Chapter 6 Implementing Security 6-1

About Security 6-2
Controlling Access to Functions and Resources 6-3
Network Partitioning Facility (NPF) 6-3
External Security Options 6-5

Security Considerations for Existing Users 6-7
Checking Existing User Group Definitions 6-7
Customizing Existing Background User Definitions 6-8

Defining NetMaster for File Transfer Users 6-9

Managing Users in a Multisystem Environment 6-10
Implementing User Definition Synchronization Across Linked Regions 6-11
Synchronization Report 6-12
Troubleshooting 6-12

External Security Packages 6-13

Chapter 7 Administering Multisystem Operations 7-1

Multisystem Operation 7-2
Links in a Multisystem Environment 7-4
Multisystem Support in Sysplex 7-5
Multisystem Implementation Considerations 7-6
Establishing Your Multisystem Environment 7-6

Linking NetMaster for File Transfer Regions 7-7
Linking and Synchronizing Regions 7-8
Monitoring the Synchronization Procedure 7-13
Background User Considerations 7-14

Keeping Track of Linked Regions 7-15

Unlinking Regions 7-16

Transmitting Records 7-17

Chapter 8 Maintaining the Product 8-1

Starting a NetMaster for File Transfer Region 8-2

Shutting Down a NetMaster for File Transfer Region 8-3
Shutting Down a Region in an Orderly Manner 8-3
Shutting Down a Region Immediately 8-3
Bringing Down the SOLVE SSI Started Task 8-3

Maintaining the Activity Logs 8-4

Backing Up the Knowledge Base 8-5
Non-production Regions 8-5
Production Regions 8-6

Part III Operations

Chapter 9 Getting Started 9-1

Accessing and Leaving the NetMaster for File Transfer Region 9-2
Logging On 9-2
If Region Initialization Is Still in Progress 9-2
If the System Image Is Still Being Loaded 9-3
Logging Off 9-3

Changing Your Password 9-3

The Menus 9-5

Accessing Functions 9-7
Selecting an Option 9-7
Selecting a Function Directly—Using Shortcuts 9-8
Accessing a Function by Using /*shortcut-name* 9-8
Accessing a Function by Using =/*shortcut-name* *9-8*
Accessing a Function That Does Not Have a Shortcut 9-9
Selecting a Function Directly—Skipping Panels 9-9
Accessing a Panel That Is Lower in the Panel Hierarchy 9-9
Accessing a Panel That Is Higher in the Panel Hierarchy 9-9
Accessing a Panel That Requires Input Data 9-9

Using Lists 9-10
Scrolling 9-10
Scrolling Vertically 9-11
Scrolling Horizontally 9-11
Searching for an Item in Retrieved Information 9-12
Using the F5 (Find) Function Key 9-12
Using the LOCATE Command 9-13

Using Data Entry Panels 9-13
Switching to UPDATE Mode 9-13
Entering Data 9-14
Prompted Fields with List of Valid Values 9-14
Validating and Filing Data 9-14
Moving Between Panels 9-15
Selecting All Panels 9-15
Selecting Specific Panels from the Panel Display List 9-15
Selecting a Panel from Another Panel 9-15
Selecting a Panel from the Index Menu 9-16
Saving a Sequence of Definition Panels for Repeated Access . 9-16

Working with Definitions in the Knowledge Base 9-17
Adding a Definition 9-17
Browsing Definitions 9-18
Updating Definitions 9-18
Copying Definitions 9-19
Deleting Definitions 9-19

Getting Help 9-20
Using the Tip of the Day 9-20
Getting Help About a Panel 9-20
Getting Help About a Message 9-20

Working in Two Windows 9-22
Splitting a Screen 9-22
Returning a Split Screen to Single Window Display 9-22
Swapping Windows 9-22

Chapter 10 Building the Environment to Manage Your File Transfer Services 10-1

Building the Environment 10-3

Defining a System Image 10-4

Defining File Transfer Rules 10-6
Defining a File Transfer Rule Set 10-6
Adding File Transfer Rules to a Rule Set 10-6
Loading a Rule Set on Demand 10-9
Considerations—Case Sensitive Values 10-10
Considerations—Overlapping Rules 10-10
Considerations—CA-XCOM File Transfers 10-11
Considerations—CONNECT:Direct File Transfers 10-11
Considerations—CONNECT:Mailbox File Transfers 10-12
Considerations—FTP File Transfers 10-13
Considerations—FTS File Transfers 10-14
Considerations—FTS Staging Data Sets 10-16
Using a Filter Expression to Specify Rule Criteria—Example 10-17

Defining File Transfer Schedules 10-18
Specifying a Schedule 10-20
Schedule Definition—Example 10-22
Schedule Status Changes 10-23

Defining Resources for File Transfer Products 10-24
Defining CA-XCOM Resources 10-24
Creating a CA-XCOM Manager 10-25
Creating CA-XCOM Monitors 10-27
Defining CONNECT:Direct Resources 10-29
Creating a CONNECT:Direct Manager 10-29
Using the Auto Populate Facility to Create Resources for Partner CONNECT:Direct Applications 10-32
Creating CONNECT:Direct Monitors 10-34
Creating a Custom-built CONNECT:Direct Monitor Resource Definition 10-37
Defining CONNECT:Mailbox Resources 10-38
Creating a CONNECT:Mailbox Manager 10-38
Creating CONNECT:Direct Monitors 10-39
Defining FTS Resources 10-40
Defining FTP Resources 10-43

Defining TCP/IP Resources 10-48

Auto-populating a System Image with DASD and Tape Resource Definitions 10-51
Using the Auto Populate Facility to Define DASD and Tape Resources 10-51

Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on an AS/400 System 10-53

Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on a Tandem System 10-54

Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on a UNIX System 10-55
Multisystem Considerations 10-55

Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on a Windows NT System .. 10-57

Defining Rules, Schedules, and Resources to Manage a Remote FTS Region 10-58

Loading, Checking, and Automating Your File Transfer Management Environment 10-58
Loading the System Image and File Transfer Rule Set..... 10-59
Checking the Built Environment..... 10-61
Setting the Built Environment to Automated Operation..... 10-62

Chapter 11 Monitoring and Managing Alerts 11-1

What Is Displayed on the Alert Monitor?..... 11-2

Accessing the Alert Monitor..... 11-2
Changing Your Alert Monitor Profile..... 11-5

Working with Alerts 11-6
Viewing the Details of an Alert 11-6
Accessing the Status Monitor from the Alert Monitor..... 11-6
Accessing the Transient Log from the Alert Monitor..... 11-7
Raising a Problem Ticket for an Alert 11-7
Adding Operator Notes to an Alert 11-7
Closing an Alert 11-8

Displaying Alert History..... 11-8

Chapter 12 Monitoring Active File Transfers 12-1

Monitoring Active File Transfers 12-2
Displaying the Estimated Completion Time 12-3
Filtering File Transfers..... 12-4
Applying a Filter to the File Transfer Monitor 12-4
Creating a New File Transfer Monitor Filter..... 12-5
Sorting a List of Active File Transfers..... 12-6
Changing the List Format..... 12-6
Applying a List Format to the File Transfer Monitor 12-6
Creating a New List Format..... 12-7
Setting Up the File Transfer Monitor in Your User Profile 12-9

Chapter 13 Monitoring and Managing File Transfer Resources 13-1

Monitoring File Transfer Resources 13-2
Accessing the File Transfer Status Monitor 13-2
Displaying Resources 13-3
Listing Monitors Associated With a Specific Manager 13-3
Changing Your View of Displayed Resources 13-4
Changing the Type of Displayed Information 13-5
Displaying Information About File Transfer Resources 13-5

Monitoring File Transfer Schedules 13-8
Acknowledging a Failure Status 13-8
Displaying the Next Time a Schedule Starts Monitoring 13-8
Display Selective Schedules on the File Transfer Status Monitor. 13-9

Interpreting the Status of File Transfer Schedules 13-9

Interpreting the Status of Supporting File Transfer Resources 13-10
Interpreting File Transfer Status Monitor Fields 13-11
Interpreting Extended Display Messages 13-11
Interpreting Colored Resources and Messages 13-12

Displaying Information About a CA-XCOM Region 13-12
Displaying a CA-XCOM Control Library Member 13-12
Displaying the MAXLOC, MAXREM, and MAXTASK Parameters 13-12

Listing and Managing CA-XCOM Transfer Requests 13-12
Listing Transfer Requests 13-13
Managing Transfer Requests 13-13

Displaying Information About a CONNECT:Direct Region 13-14
CONNECT:Direct Security Considerations 13-14
Confirming Your CONNECT:Direct Signon Details 13-15
Clearing Your CONNECT:Direct Signon Details 13-16
Displaying a CONNECT:Direct Network Map 13-16
Displaying the Initialization Parameters of a CONNECT:Direct Region 13-18

Listing and Managing CONNECT:Direct Processes 13-19
Listing Processes 13-20
Managing Processes 13-22

Listing and Managing TCP/IP Connections 13-23
Dropping a TCP/IP Connection 13-24

Listing and Managing CONNECT:Mailbox Batches 13-24
Initiating an Auto Connect 13-26

Monitoring CONNECT:Mailbox Resources 13-27
Listing and Managing Queued Auto Connects 13-27
Listing and Managing CONNECT:Mailbox BSC Lines 13-28
Listing CONNECT:Mailbox SNA Sessions 13-28

Listing and Managing CONNECT:Mailbox VSAM Batch Files..... 13-28
Maintaining VSAM Batch Files Using the Assisted REORG Facility 13-30

Displaying Logs..... 13-32
Displaying the File Transfer Log 13-33
Browsing the File Transfer Log Online 13-34
Suppressing Messages Logged to the File Transfer Log 13-34
Accessing Activity Log from the File Transfer Log..... 13-34
Displaying the Activity Log..... 13-35
Browsing the Activity Log Online..... 13-35
Suppressing Messages Logged to the Activity Log..... 13-35
Displaying the Transient Log..... 13-36
Setting the Criteria to Display Logged Messages Selectively.. 13-37
Obtaining Help on a Logged Message..... 13-37
Printing a Transient Log 13-37
Resetting a Transient Log 13-37
Accessing the Activity Log from the Transient Log 13-38
Merging Transient Logs..... 13-39

Activating and Inactivating a File Transfer Resource 13-40
Activating a File Transfer Resource 13-40
Inactivating a File Transfer Resource 13-40

Issuing Commands to a File Transfer Resource 13-41

Issuing UNIX Shell Commands to a Remote UNIX Host 13-43

Monitoring Your File Transfer Environment by Using the Graphical Monitor 13-44

Chapter 14 Controlling the System Image..... 14-1

Changing the Global Operation Mode..... 14-2

Loading a System Image 14-3
Performing Cold and Warm Loads 14-5

Shutting Down the Resources in a Loaded System Image 14-6
Shutting Down Automated Resources 14-7
Shutting Down a Manual Resource 14-8
Shutting Down All Resources..... 14-8

Restarting the Resources in a Loaded System Image..... 14-9

Chapter 15 Customizing the Environment That Manages File Transfer Resources 15-1

Customizing CA-XCOM Monitor Criteria..... 15-2
Customizing How Often the Monitor Status Is Updated 15-2
Customizing the Heartbeat Intervals of Transfer Request Monitors..... 15-3
Customizing the Heartbeat Interval of Other Monitors 15-4
Customizing Criteria for Monitoring CA-XCOM Transfer Requests 15-5
Customizing the Criteria for Monitoring Stalled CA-XCOM Transfers..... 15-6
Customizing the Criteria for Monitoring CA-XCOM TCP/IP Connections..... 15-7
Customizing the Criteria for Monitoring a CA-XCOM Remote Node 15-8

Customizing CONNECT:Direct Monitor Criteria..... 15-9
Customizing How Often the Monitor Status Is Updated 15-9
Customizing Criteria for Monitoring CONNECT:Direct Queues . 15-10
Customizing the Criteria for Monitoring CONNECT:Direct Transfers..... 15-11
Customizing the Criteria for Monitoring a CONNECT:Direct TCP/IP Listener Task..... 15-12
Customizing the Criteria for Monitoring CONNECT:Direct TCP/IP Connections..... 15-13
Customizing the Criteria for Monitoring a CONNECT:Direct Remote Node..... 15-14

Customizing CONNECT:Mailbox Monitor Criteria 15-15
Customizing How Often the Monitor Status Is Updated 15-15
Customizing the Criteria for Monitoring Auto Connect Queues ... 15-16
Customizing the Criteria for Monitoring BSC Lines..... 15-17
Customizing the Criteria for Monitoring SNA Sessions..... 15-18

Customizing FTS Monitor Criteria..... 15-19

Customizing FTP Monitor Criteria..... 15-21
Customizing How Often the Monitor Status is Updated 15-21
Customizing the Criteria for Monitoring FTP TCP/IP Connections..... 15-22
Customizing the Criteria for Monitoring an FTP Remote Node.... 15-23

Specifying the Availability of Supporting File Transfer Resources..... 15-24
Displaying the Availability Map..... 15-25
Specifying Map Details..... 15-27
Specifying Timer Details 15-28
Timer Details—Example 15-28

Raising a Problem Ticket 15-29
Specifying the PROBSOLV Process in the State Change Exits Panel 15-29
Specifying the PROBSOLV Process for a Message Rule 15-32

Using Processes to Perform Complex Operations 15-33
Defining a Process 15-34
Checking the Availability of a Destination CONNECT:Direct Node 15-35
Specifying the PINGCD Macro 15-35
Issuing CONNECT:Direct Commands from a Process 15-37
Specifying the CDAPI Macro 15-37
Using the SNMP Trap Exit 15-39
Creating an SNMP Trap in a Process 15-39
Generating an Exception Report from a NetMaster for File Transfer Process 15-42
Specifying the FTCHECK Macro 15-42

Customizing the Manager Resource Definition 15-44

Customizing Monitor Resource Definitions 15-46

Customizing the Supporting Resource Definition 15-48

Chapter 16 Logging Messages Selectively 16-1

Logging Selected Messages to the Activity Log 16-2
Defining a Rule Set 16-2
Defining a Message Rule 16-4
Adding a Rule Set to the System Image 16-6

Logging Selected CONNECT:Direct Messages to the File Transfer Log 16-6

Chapter 17 Defining and Maintaining Calendars 17-1

Using Calendars 17-2

Creating a Calendar 17-3

Creating a Calendar Keyword 17-4

Associating a Calendar Keyword with a Date 17-4

Creating a Calendar Criteria Definition 17-7
Specifying the Criteria Expression—Example 17-7

Chapter 18 Producing Reports 18-1

About Reports 18-2

Viewing Reports and Searching the Database 18-3
Viewing Predefined Reports for File Transfer Events 18-4
Viewing All File Transfer Events 18-5
Viewing Failed File Transfer Events 18-5
Viewing the Final Results of File Transfers 18-6
Viewing Summarized Reports 18-6
Viewing Predefined Reports for Schedules 18-7
Viewing Schedules 18-8

Generating Exception Reports 18-9
Defining Exception Report Filters 18-9
Generating Exception Reports 18-10

Searching the Events Database 18-10
Searching for File Transfer Events 18-11
Searching for File Transfer Schedules 18-12
Performing a Custom Search 18-13
Examples of Custom Searches 18-14
Actions on the NCL/EF : Database Search Criteria Panel 18-15

Printing Reports 18-16
Printing Reports for File Transfer Events 18-16
Printing Reports for File Transfer Schedules 18-17
Checking the Print Queue 18-17

Extracting Data to a File 18-18

Defining Printed Reports 18-20
Defining Search Criteria (Optional) 18-20
Defining Report Details 18-21

Troubleshooting for the Reporting Facility 18-22
If the EVNTDB Database Has Not Been Allocated 18-22
If the EVNTDB Database Is Full 18-22
If the Automatic Reorganization Fails 18-22
Fixing a Failed Reorganization via a Batch Job 18-23
Fixing a Failed Reorganization via the EVENTLOG Parameter Group 18-24

Chapter 19 Advanced Features 19-1

Using the $RMDBAPI Procedure to Manage File Transfer Resource Definitions 19-2
Copying Resource Definitions—Example 19-2
Considerations 19-2

Working with Externally Updateable Schedules 19-3
Defining a CTL File to a Schedule 19-4
Viewing a CTL File 19-4
Checking a CTL File 19-5
Considerations 19-5

Chapter 20 Controlling the Use of FTP 20-1

About File Transfers Using FTP 20-2

About the TCPaccess FTP Server 20-2
Policy Control 20-3

About TCPaccess FTP Policy Rule Sets 20-3

Task 1—Defining a Policy Rule Set 20-6

Task 2—Adding Policy Rules to a Rule Set 20-6

Task 3—Activating a Policy Rule Set 20-8
Loading a Policy Rule Set 20-9
Setting Policy Mode for an Active Policy Rule Set 20-10

Viewing the Loaded Policy Rule Set 20-10

Copying the Loaded Policy Rule Set 20-11
Using Policy Rule Sets Across Linked Regions 20-11

FTP SAF Rule Considerations 20-12
Checking FTP SAF Rules 20-13
Example of Using FTP SAF Rules for an Incoming File Transfer 20-14
Example of Using FTP SAF Rules for an Outgoing File Transfer 20-14

Setting Up Your SAF Qualifier 20-14
Setting Up Your SAF Qualifier Under RACF 20-15
Setting Up Your SAF Qualifier Under ACF2 20-16
Setting Up Your SAF Qualifier Under Top Secret 20-17
Examples of Using Your SAF Qualifier 20-18
Example 1 20-18
Example 2 20-18
Example 3 20-19
Example 4 20-19

Part IV Reference

Appendix A Panel Paths for Accessing NetMaster for File Transfer Functions A-1

Panel Path Specifications A-1

Appendix B Parameter Groups B-1

List of Parameter Groups B-2

Appendix C Security Settings C-1

Security Settings for $RMADMIN C-2

Security Settings for $RMOPER C-3

Security Settings for $RMNOPER C-4

Security Settings for $RMMON C-5

Security Settings for $RMBUSER C-6

Appendix D File Transfer Variables D-1

Variables D-2

Appendix E File Transfer Events Mapping E-1

Appendix F Application Program Interface F-1

$RFCALL F-2

$RMDBAPI SERVICE={ACTIVATE | INACTIVATE} F-5

Example F-6

$RMDBAPI SERVICE={CREATE | DELETE | GET | LIST | SET} . F-7

ResourceView Definition Field Names F-7

Resource Fields F-8

File Transfer Rule Set Fields F-12

File Transfer Rule Fields F-13

Appendix G Form for Gathering Information Required During Implementation G-1

Glossary

Index

Figures and Tables

Figure 1-1. Operating Environment 1-2
Figure 1-2. Definitions in the Knowledge Base 1-4
Figure 3-1. CA-XCOM Resources 3-3
Figure 3-2. Event Flow From CA-XCOM on an MVS or OS/390 System to NetMaster for File Transfer 3-8
Figure 3-3. CONNECT:Direct Resources 3-9
Figure 3-4. Event Flow From CONNECT:Direct on an MVS or OS/390 System to NetMaster for File Transfer 3-14
Figure 3-5. Event Flow From CONNECT:Direct on a Distributed System to NetMaster for File Transfer 3-15
Figure 3-6. CONNECT:Mailbox Resources..... 3-17
Figure 3-7. Event Flow from CONNECT:Mailbox to NetMaster for File Transfer 3-21
Figure 3-8. FTS Resources 3-22
Figure 3-9. Event Flow From FTS to NetMaster for File Transfer 3-24
Figure 3-10. FTP Resources 3-25
Figure 3-11. Event Flow From an FTP Server to NetMaster for File Transfer Not Using TCPaccess FTP Server..... 3-29
Figure 3-12. Event Flow From an FTP Server to NetMaster for File Transfer Using TCPaccess FTP Server..... 3-30
Figure 5-1. Specifying the CONNECT:Direct Interface Parameters 5-9
Figure 5-2. TCP/IP Software Type and Interface..... 5-11
Figure 5-3. TCP/IP Management Interface for IBM TCP/IP Software..... 5-12
Figure 5-4. TCP/IP Management Interface for TCPaccess Software..... 5-12
Figure 5-5. Selecting the Resource Definition Option 5-17
Figure 5-6. Making a Copy of the Distributed Templates..... 5-19
Figure 5-7. The File Transfer Log Parameter Group..... 5-23

Figure 5-8. Allocating a File Transfer Log File 5-23
Figure 5-9. Allocating an Activity Log File 5-25
Figure 5-10. The Schedule File Specifications Parameter Group 5-26
Figure 5-11. Customizing the FTPCNTL Parameter Group (Without TCPaccess FTP)..... 5-43
Figure 5-12. Customizing the FTPCNTL Parameter Group (TCPaccess FTP) 5-46
Figure 5-13. Alert Monitor : Administration Menu..... 5-55
Figure 5-14. Alert Monitor : Interface Definition Panel..... 5-56
Figure 5-15. Alert Monitor : Email a Trouble Ticket Panel 5-57
Figure 5-16. Alert Monitor : Custom Trouble Ticket Panel..... 5-58
Figure 5-17. Alert Monitor : Trouble Ticket Data Entry Definition Panel ... 5-59
Figure 5-18. Implementing Event Recording and Reporting 5-66
Figure 6-1. Relationship between UAMS and NPF 6-3
Figure 6-2. Relationship Between UAMS and SAF 6-5
Figure 6-3. User Description Panel 6-9
Figure 6-4. UAMS Update Report..... 6-12
Figure 7-1. Multisystem Operation 7-3
Figure 7-2. Multisystem Link Configurations 7-5
Figure 7-3. Linking NetMaster for File Transfer Regions 7-8
Figure 7-4. Multi-System Support Menu..... 7-9
Figure 7-5. Linking NetMaster for File Transfer Regions 7-10
Figure 7-6. Confirm Database Synchronization Panel 7-11
Figure 7-7. Monitoring the Progress of Knowledge Base Synchronization 7-12
Figure 7-8. Multisystem Support—Administration Task Log 7-13
Figure 7-9. Linked Regions Panel 7-15
Figure 7-10. Browsing a System Link Definition 7-15
Figure 7-11. Confirming a Region Unlink Operation 7-16
Figure 7-12. Transmitting NetMaster for File Transfer Knowledge Base Records 7-17
Figure 8-1. Confirming an Activity Log Swap..... 8-4
Figure 9-1. The Primary Menu 9-2
Figure 9-2. User Password Maintenance Panel 9-4
Figure 9-3. Locating a Record in a List..... 9-13
Figure 10-1. ResourceView : System Image Definition Panel..... 10-5
Figure 10-2. System Image List Panel..... 10-5
Figure 10-3. FTS Management Environment..... 10-15
Figure 10-4. FTS Staging Mode Operation 10-16
Figure 10-5. Specifying File Transfer Rule Criteria—Example 10-17
Figure 10-6. File Transfer Schedule 10-21
Figure 10-7. File Transfer Schedule—Example..... 10-22
Figure 10-8. Entering Details for the XCMGR 10-25
Figure 10-9. Generating CA-XCOM Monitor Resources 10-27

Figure 10-10. Selecting CA-XCOM Monitor Templates 10-27
Figure 10-11. Entering CA-XCOM Monitor Details 10-28
Figure 10-12. Entering Details for the CDMGR 10-30
Figure 10-13. Auto Populate Selection List Panel..... 10-33
Figure 10-14. Generating CONNECT:Direct Monitor Resources 10-34
Figure 10-15. Selecting CONNECT:Direct Monitor Templates..... 10-35
Figure 10-16. Entering CONNECT:Direct Monitor Details 10-35
Figure 10-17. Generating CONNECT:Mailbox Monitor Resources..... 10-39
Figure 10-18. Entering CONNECT:Mailbox Monitor Details..... 10-39
Figure 10-19. Entering Details for the FTSMGR..... 10-41
Figure 10-20. Generating FTS Monitor Resources 10-42
Figure 10-21. Entering FTS Monitor Details 10-42
Figure 10-22. Entering Details for the FTPMGR..... 10-44
Figure 10-23. Generating FTP Monitor Resources 10-46
Figure 10-24. Selecting FTP Monitor Templates..... 10-46
Figure 10-25. Entering FTP Server Monitor Details..... 10-47
Figure 10-26. Entering Details for a TCP/IP Resource 10-48
Figure 10-27. Updated Started Task General Description Panel..... 10-50
Figure 10-28. List of Defined Resources..... 10-50
Figure 10-29. Auto Populate Selection List Panel..... 10-52
Figure 10-30. Backup System Image for Remote File Transfer Products..... 10-56
Figure 10-31. Initialization Parameters Panel 10-60
Figure 10-32. File Transfer Resources Status Monitor 10-61
Figure 10-33. Global Command Parameter Specification Panel..... 10-63
Figure 10-34. Command Confirmation Panel 10-63
Figure 11-1. Alert Monitor Screens..... 11-3
Figure 11-2. Alert Monitor Profile Panel 11-5
Figure 12-1. File Transfer Monitor Panel..... 12-2
Figure 12-2. ETA Monitoring in Progress..... 12-3
Figure 12-3. File Transfer Monitor Filter List..... 12-4
Figure 12-4. File Transfer Monitor with Filter Applied..... 12-4
Figure 12-5. Example File Transfer Monitor Filter..... 12-5
Figure 12-6. List Format Panel..... 12-7
Figure 12-7. Completed List Format Panel 12-8
Figure 12-8. File Transfer Monitor Profile Panel..... 12-9
Figure 13-1. Status Monitor : File Transfer Resources 13-2
Figure 13-2. Listing Resources..... 13-3
Figure 13-3. Changing a Filter..... 13-4
Figure 13-4. Confirming Signon Details for a CONNECT:Direct Command..... 13-15
Figure 13-5. Specify A NETMAP Node Name Panel..... 13-16
Figure 13-6. Displaying the Network Map..... 13-17
Figure 13-7. Displaying CONNECT:Direct Initialization Parameters..... 13-18

Figure 13-8. Displaying a CONNECT:Direct Process Queue Monitor 13-20
Figure 13-9. Queued Processes List 13-21
Figure 13-10. Displaying TCP/IP Connections 13-23
Figure 13-11. Dropping a TCP/IP Connection 13-24
Figure 13-12. Mailbox Batch List 13-25
Figure 13-13. File Transfer Auto Connect 13-26
Figure 13-14. Displaying CONNECT:Mailbox Monitors 13-27
Figure 13-15. VSAM File Statistics 13-29
Figure 13-16. Deallocate Confirmation Panel 13-30
Figure 13-17. Summary of Execution Status Panel 13-30
Figure 13-18. Assisted REORG Facility 13-31
Figure 13-19. File Transfer Log 13-33
Figure 13-20. Transient Log 13-36
Figure 13-21. Accessing the Activity Log from the Transient Log 13-38
Figure 13-22. Issuing CONNECT:Direct Commands 13-42
Figure 14-1. Global Command Parameter Specification Panel 14-2
Figure 14-2. Confirming the Change to Global Operation Mode 14-3
Figure 14-3. Load Command Parameter Specification 14-4
Figure 14-4. Confirming the System Image Load 14-5
Figure 14-5. Confirming the Execution of the SHUTSYS Command 14-7
Figure 15-1. Customizing the Heartbeat Criterion of CA-XCOM Transfer Request Monitors 15-3
Figure 15-2. CA-XCOM Transfer Request Monitor Details 15-5
Figure 15-3. CA-XCOM Stalled Transfer Monitor Details 15-6
Figure 15-4. CA-XCOM TCP/IP Connection Monitor Details 15-7
Figure 15-5. CA-XCOM Remote Node Monitor Details 15-8
Figure 15-6. Customizing the Heartbeat Criterion of a CONNECT:Direct Monitor 15-9
Figure 15-7. Process Queue or Status Monitor Details 15-10
Figure 15-8. CONNECT:Direct Transfer Monitor Details 15-11
Figure 15-9. CONNECT:Direct TCP/IP Listener Monitor Details 15-12
Figure 15-10. CONNECT:Direct TCP/IP Connection Monitor Details 15-13
Figure 15-11. CONNECT:Direct Remote Node Monitor Details 15-14
Figure 15-12. Customizing the Heartbeat Criterion of a CONNECT:Mailbox Monitor 15-15
Figure 15-13. Auto Connect Queue Monitor Details 15-16
Figure 15-14. BSC Line Monitor Details 15-17
Figure 15-15. SNA Session Monitor Details 15-18
Figure 15-16. Customizing the Heartbeat Criterion of an FTS Monitor 15-19
Figure 15-17. Monitor Details Panel—FTSMON Class Resource 15-19
Figure 15-18. Customizing the Heartbeat Criterion of an FTP Monitor 15-21
Figure 15-19. FTP TCP/IP Connection Monitor Details 15-22
Figure 15-20. FTP Remote Node Monitor Details 15-23

Figure 15-21. Resource Definition 15-25
Figure 15-22. Specifying the Availability of a Resource 15-26
Figure 15-23. Availability Map 15-26
Figure 15-24. Creating an Availability Map..... 15-27
Figure 15-25. Completed Timer Details Window 15-28
Figure 15-26. State Change Exits Panel 15-30
Figure 15-27. State Change Exits Panel 15-31
Figure 15-28. Specifying the ACB Name for the PROBSOLV Process..... 15-31
Figure 15-29. Status Monitor Message Details Panel 15-32
Figure 15-30. Displaying the Define Event Exits Panel..... 15-33
Figure 15-31. Process List Panel 15-34
Figure 15-32. Process Definition Panel 15-34
Figure 15-33. Specifying PINGCD Macro Parameters 15-36
Figure 15-34. PINGCD Macro Parameter Definition Panel—Example 15-36
Figure 15-35. Specifying CDAPI Macro Parameters 15-37
Figure 15-36. CDAPI Macro Parameter Definition Panel—Example 15-38
Figure 15-37. Specifying SNMPTRAP Macro Parameters..... 15-40
Figure 15-38. SNMP Trap Macro Parameter Definition Panel—Example..... 15-42
Figure 15-39. Specifying FTCHECK Macro Parameters..... 15-43
Figure 16-1. EventView : Ruleset Description..... 16-2
Figure 16-2. Specifying the Rule Set..... 16-3
Figure 16-3. The EventView : Message Filter..... 16-4
Figure 16-4. Specifying the Message Filter..... 16-5
Figure 16-5. Specifying Message Delivery 16-5
Figure 16-6. Specifying the Message Suppression Rule Set 16-6
Figure 16-7. Initialization Parameters Panel 16-7
Figure 17-1. Calendar 17-3
Figure 17-2. Creating a Calendar Keyword..... 17-4
Figure 17-3. Associating a Keyword with a Date (Sheet 1 of 2)..... 17-5
Figure 17-4. Calendar with Associated Keyword..... 17-6
Figure 17-5. Calendar Criteria—Example..... 17-7
Figure 18-1. The History Data Menu 18-3
Figure 18-2. Selection List for File Transfer Events Reports and Searches.. 18-4
Figure 18-3. File Transfer : All Events Panel..... 18-5
Figure 18-4. Summary Reports..... 18-6
Figure 18-5. Selection List for File Transfer Events Reports and Searches.. 18-7
Figure 18-6. NetMaster for File Transfer : Completed Schedules Panel 18-8
Figure 18-7. Exception Report 18-10
Figure 18-8. Search Criteria Panel..... 18-11
Figure 18-9. The Schedules Search Criteria Panel 18-12
Figure 18-10. NCL/EF : Database Search Criteria Panel 18-13
Figure 18-11. Custom Search of File Transfer Events—Example 1 18-14
Figure 18-12. Custom Search of File Transfer Events—Example 2 18-15

Figure 18-13. File Transfer Events Printed Reports List 18-16
Figure 18-14. File Transfer Schedule History Printed Reports List 18-17
Figure 18-15. Extracts List Panel 18-18
Figure 20-1. How NetMaster for File Transfer and TCPaccess FTP Server Implement FTP Policy Rules 20-5
Figure D-1. Using File Transfer Variables—Example D-2

Table 6-1. NPF Members—Samples 6-4
Table 9-1. Primary Menu Hierarchy 9-5
Table 9-2. Valid Scroll Amounts For Scrolling Vertically 9-11
Table 10-1. Status Changes of a File Transfer Schedule 10-23
Table 13-1. Actions for CA-XCOM Transfer Requests 13-13
Table 13-2. Actions for CONNECT:Direct Queued Processes 13-22
Table A-1. Useful Panel Paths A-2
Table B-1. Initialization Parameter Groups B-2
Table C-1. Security Settings for $RMADMIN C-2
Table C-2. Security Settings for $RMOPER C-3
Table C-3. Security Settings for $RMNOPER C-4
Table C-4. Security Settings for $RMMON C-5
Table C-5. Security Settings for $RMBUSER C-6
Table D-1. File Transfer Variables D-2
Table E-1. File Transfer Event Field Mappings E-1
Table E-2. Data Available for Start Events—CD and CM E-3
Table E-3. Data Available for Start Events—CA-XCOM, FTS, and FTP E-3
Table E-4. Data Available for End Events—CD and CM E-4
Table E-5. Data Available for End Events—CA-XCOM, FTS, and FTP E-4
Table F-1. Resource Field Names Used in the $RMDBAPI Procedure F-8
Table F-2. File Transfer Rule Set Field Names Used in the $RMDBAPI Procedure F-12
Table F-3. File Transfer Rule Field Names Used in the $RMDBAPI Procedure F-13

Part I

General Information

1

Introduction

This chapter introduces the Unicenter NetMaster File Transfer Management (also known as NetMaster for File Transfer) product.

The chapter contains the following topics:

- What the Product Offers
- Features and Benefits
- About this Guide
- What You Should Know Already

What the Product Offers

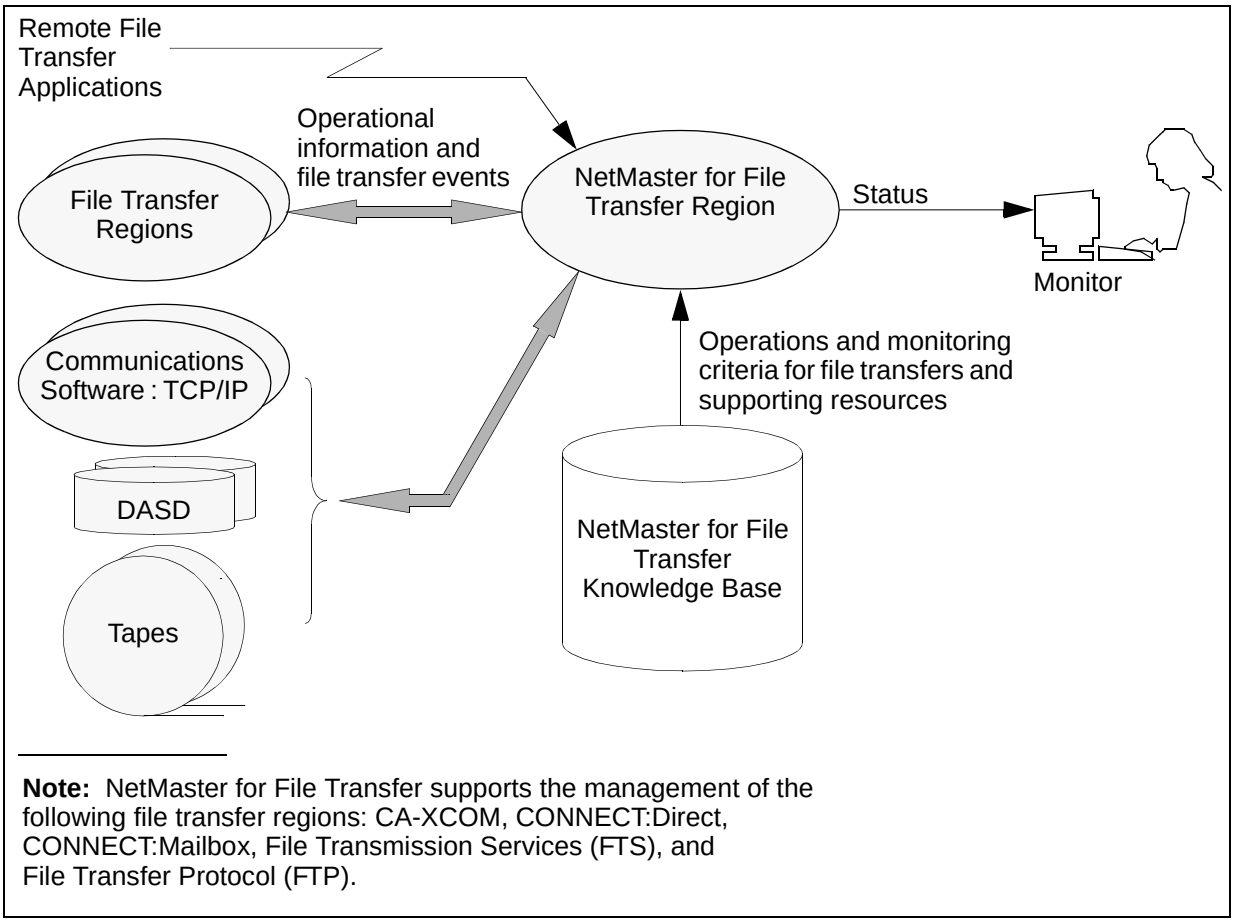
The product enables you to monitor and manage the following components in a file transfer service:

- File transfers
- Resources that support the file transfers, which include the applications that perform the transfers and the communications software that supports them

It receives events from file transfer applications and supporting resources. It uses 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 the events.

Figure 1-1 shows the typical operating environment.

Figure 1-1. Operating Environment



Through the monitor, NetMaster for File Transfer alerts you to problems that have occurred or are likely to occur in your file transfer service. In an environment where your file transfer service is provided by several file transfer regions on different systems, NetMaster for File Transfer can be configured such that a single monitor provides visibility to all these regions, by using multisystem support.

Features and Benefits

NetMaster for File Transfer provides the following features:

- Knowledge base
- Visibility of file transfer messages
- File transfer monitors
- File transfer resource control
- Automation engine
- Multisystem support
- File transfer logs
- Automatic problem recording
- Automatic generation of Simple Network Management Protocol (SNMP) traps
- Reporting facility
- FTP function policy control, if you are using the Unicenter TCPaccess FTP server

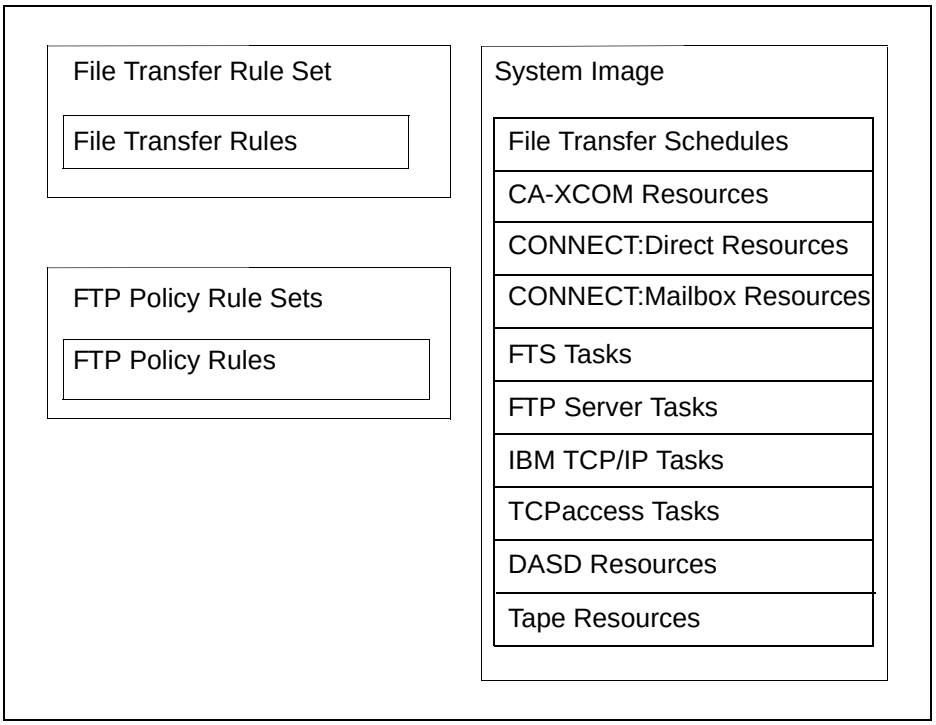
Knowledge Base

In the NetMaster for File Transfer knowledge base, you store the operations and monitoring criteria for the file transfers and the supporting resources you want to manage. Using the stored information, the NetMaster for File Transfer region is able to monitor their status and alert you when problems occur. The alert is displayed on an alert monitor. The alert may also manifest itself on a status monitor as a change in the status of the affected resources, providing you with immediate feedback of the problem area.

You define file transfer rule sets, rules, system images, and resources in the knowledge base to store the operational policies and methods of your file transfer service. The definitions you create contain information about how you want to manage the file transfers and supporting resources. For the supporting resources, templates are provided to help you create the information in the knowledge base.

Figure 1-2 shows the definitions you create to monitor your file transfer service. The following sections briefly describe these definitions.

Figure 1-2. Definitions in the Knowledge Base



File Transfer Rules

If you want to monitor individual file transfers, define file transfer rules.

The file transfer rules contain information about which files to monitor, the monitoring criteria, and what actions to take when certain conditions occur. If a monitored file transfer event occurs, the NetMaster for File Transfer region can send an alert to the alert monitor.

File Transfer Schedules

If you want to monitor whether a group of files arrives or is sent by a certain time, define file transfer schedules.

A file transfer rule enables you to monitor what is happening with individual transferred files. It does not tell you if a required file has not been transferred. If you want to monitor whether one or more files is transferred in a scheduled time interval, you have to define the schedules.

By using a schedule, you can specify the files to monitor, when the transfer should complete, and what actions to take when certain conditions occur. The NetMaster for File Transfer region will reflect any deviations from the schedule as state changes on the status monitor.

CA-XCOM Resources

NetMaster for File Transfer supports the following classes of resources to manage your CA-XCOM for MVS applications:

- CA-XCOM file transfer manager for a CA-XCOM application:

  By using these resources, you can automate the starting, stopping, and recovery of CA-XCOM for MVS regions. By the use of an availability map, you can specify when a region should start and stop.

- CA-XCOM file transfer monitors for:

  - Transfer requests
  - Stalled transfers
  - TCP/IP listener task
  - TCP/IP connections
  - Remote nodes

  By using these resources, you can specify the monitoring criteria. The NetMaster for File Transfer region will reflect any deviations from these criteria as state changes on the status monitor.

CONNECT:Direct Resources

NetMaster for File Transfer supports the following classes of resources to manage your CONNECT:Direct applications:

- CONNECT:Direct file transfer manager for a CONNECT:Direct application:
  - On MVS and OS/390 systems (job or started task)—by using these resources, you can automate the starting, stopping, and recovery of CONNECT:Direct regions. By the use of an availability map, you can specify when a region should start and stop.
  - On AS/400, Tandem, UNIX, and Windows NT systems—by using these resources, you can monitor the file transfers occurring on the remote system and issue commands to them.
- CONNECT:Direct file transfer monitors for:
  - Process queues
  - Process status
  - Transfers
  - TCP/IP listener task
  - TCP/IP connections
  - Remote node

  By using these resources, you can specify the monitoring criteria. The NetMaster for File Transfer region will reflect any deviations from these criteria as state changes on the status monitor.

CONNECT:Mailbox Resources

NetMaster for File Transfer supports the following classes of resources to manage your CONNECT:Mailbox for MVS applications:

- CONNECT:Mailbox file transfer manager for a CONNECT:Mailbox application:

  By using these resources, you can automate the starting, stopping, and recovery of CONNECT:Mailbox for MVS regions. By the use of an availability map, you can specify when a region should start and stop.

- CONNECT:Mailbox file transfer monitors for:

  - BSC lines
  - SNA sessions
  - Queued Auto Connects

  By using these resources, you can specify the monitoring criteria. The NetMaster for File Transfer region will reflect any deviations from these criteria as state changes on the status monitor.

- Started task resource for the CONNECT:Mailbox file server:

  By using this resource you can automate starting, stopping, and recovery of the CONNECT:Mailbox file server. By the use of an availability map, you can specify when a CONNECT:Mailbox file server should start and stop.

File Transmission Services (FTS) Resources

NetMaster for File Transfer supports the following classes of resources to manage your FTS regions:

- FTS file transfer manager for an FTS job or started task:

  - On the local system—by using these resources, you can automate the starting, stopping, and recovery of FTS regions. By the use of an availability map, you can specify when a region should start and stop.
  - On another system—by using these resources, you can monitor the file transfers occurring in remote regions.

- FTS file transfer monitors for the links between FTS regions:

  By using these resources, you can specify the monitoring criteria. The NetMaster for File Transfer region will reflect any deviations from these criteria as state changes on the status monitor.

File Transfer Protocol (FTP) Resources

NetMaster for File Transfer supports the following classes of resources to manage your FTP regions:

- FTP file transfer manager for an FTP server application on the local system. By using these resources, you can automate the starting, stopping, and recovery of FTP server regions. By using an availability map, you can specify when a region should start and stop.

  If you use the TCPaccess FTP server, then the file transfer manager displays a message when either of the following becomes active or inactive:

  - SOLVE Subsystem Interface (SSI)
  - Data Space Manager

- FTP file transfer monitors for the FTP application:

  - TCP/IP listener port
  - TCP/IP connections
  - Remote node

  By using these resources, you can specify the monitoring criteria. The NetMaster for File Transfer region will reflect any deviations from these criteria as state changes on the status monitor.

Other Supporting File Transfer Resources

Besides providing support for the management of file transfer applications, NetMaster for File Transfer also supports the management of the following resources:

- TCP/IP provider, which can be TCPaccess or IBM's Communications Server
- Direct access storage devices (DASD)
- Tapes

By including these resources in your file transfer management environment, you have visibility of all the components that make up your file transfer service.

System Images

A system image represents a specific environment (for example, a file transfer subsystem, and all the resources and event rules required for it to function). You define the system image in the knowledge base, and you define local resources to the system image. The image holds the information about how you want the region to manage the defined resources. The region manages the resources local to the system.

You can create different images to reflect the different ways you want to manage the resources on a system. During operation, you change the management methods by loading an appropriate image.

Only one system image can be active in a region at any one time. In a multisystem environment, each region must run a different system image. Operators can monitor the status of a resource defined to the active system image.

Templates

A template contains predefined operational information about a particular type of resource (for example, a CONNECT:Direct TCP/IP listener task monitor). Templates are grouped under their own special system image, $TEMPLAT.

The NetMaster for File Transfer product includes sample resource templates that you can use to create your CA-XCOM, CONNECT:Direct, CONNECT:Mailbox, FTP, FTS, and other supporting resource definitions. You can modify the sample templates or create your own templates. You can create templates for the different resource types in each class of resource.

You can maintain several versions of templates as different $TEMPLAT system images.

Message Visibility

A NetMaster for File Transfer region can monitor the following messages:

- CA-XCOM messages—by using the SOLVE subsystem interface (SSI) event delivery facility
- CONNECT:Direct messages—by using the SSI event delivery facility (for CONNECT:Direct applications on OS/390 systems) or TCP/IP links (for CONNECT:Direct applications on distributed systems such as UNIX)
- CONNECT:Mailbox messages—by using the SSI event delivery facility
- FTS messages—by using INMC links
- System messages—by using the Automation Services subsystem interface
- FTP messages—by using one of the following:
  - FTP file transfers *not* using the TCPaccess FTP server produce no messages, so the region generates messages based on information intercepted from FTP SMF records by using the SSI event delivery facility.
  - For FTP file transfers using the TCPaccess FTP server, messages are received directly from the server through the SSI event delivery facility.

Monitors

NetMaster for File Transfer provides an active file transfer monitor, an alert monitor, and a status monitor.

The monitors provide you with immediate feedback about the file transfers and the supporting resources you are managing. In a multisystem environment, you have visibility of all the managed transfers and resources (both local and remote) from a single monitor.

Active File Transfer Monitor

The active file transfer monitor displays information about the transfers as they happen. You can define filters to select what you want to display. You can terminate transfers.

Alert Monitor

The alert monitor displays alerts that warn you of any file transfer problems that have occurred.

Status Monitor

The status monitor displays the status of the managed file transfer resources. You can define filters to select what you want to display. The monitor:

- Warns you of any problems that have occurred or might occur.
- Enables you to manually control the managed resources.

File Transfer Resource Control

You can control the managed file transfer resources from the status monitor. In a multisystem environment, the monitor provides you with a single point of control for all the managed resources (both local and remote).

CA-XCOM Resources

NetMaster for File Transfer provides commands that you can use to control CA-XCOM resources. By using these commands you can:

- Start or stop a CA-XCOM region
- Control transfer requests
- Terminate a TCP/IP connection

CONNECT:Direct Resources

NetMaster for File Transfer provides commands that you can use to control CONNECT:Direct resources:

For a CONNECT:Direct application on …	You can …
An OS/390 system	• Start or stop a CONNECT:Direct file transfer region • Control the queued CONNECT:Direct processes • Terminate a TCP/IP connection
An AS/400, Tandem, UNIX, or Windows NT system	• Start or stop the link to the CONNECT:Direct application • Control the queued CONNECT:Direct processes

CONNECT:Mailbox Resources

NetMaster for File Transfer provides commands that you can use to control CONNECT:Mailbox resources. By using these commands you can:

- Start or stop a CONNECT:Mailbox region
- Start or stop a BSC line
- Delete a queued Auto Connect
- Initiate a transmission via $$CONNECT
- View a list of CONNECT:Mailbox batches and perform selected CONNECT:Mailbox functions on the listed batches
- Perform maintenance functions on CONNECT:Mailbox VSAM files

FTS Resources

NetMaster for File Transfer provides commands that you can use to control FTS resources:

- You can start or stop a local FTS file transfer region.
- You can start or stop the INMC link between the NetMaster for File Transfer region to a remote FTS file transfer region.

FTP Resources

NetMaster for File Transfer provides commands that you can use to control FTP resources:

For an FTP application on …	You can …
IBM's Communications Server	• Start or stop a local FTP server region • Terminate a TCP/IP connection either automatically or manually
TCPaccess	• Start or stop a local TCPaccess region • Terminate a TCP/IP connection manually
TCPaccess FTP server	• Start or stop a local TCPaccess FTP server • Terminate a TCP/IP connection automatically or manually

Other Supporting Resources

NetMaster for File Transfer provides commands that you can use to start or stop the other supporting resources. For a list of the supported resources, see the section, *Other Supporting File Transfer Resources*, on page 1-8.

Automation Engine

The automation engine enables the NetMaster for File Transfer region to control the managed file transfer resources according to the information stored in the knowledge base. You can use an availability map to specify when a resource should become active and when it should become inactive.

The automation engine reacts to events occurring in the NetMaster for File Transfer region to ensure that the managed file transfer resources are in their desired states.

It relieves you of routine operational tasks so that you can concentrate on abnormal operational conditions.

It also minimizes the impact of a failure to the users of a file transfer service. If a failure occurs while the service is idle, the service is recovered automatically before a user requires that service. That is, the users are unaware of the failure and see the service as continuously available.

During normal operation, if the operation mode of a resource is AUTOMATED, the automation engine takes control. If a problem occurs that cannot be handled by automation, you can change the operation mode to MANUAL to allow manual intervention.

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 NetMaster for File Transfer regions together to provide you with an enterprise view of the managed file transfer service.

In a multisystem environment where each region manages the resources defined to its own active 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 NetMaster for File Transfer environment can consist of focal point regions, subordinates, and agents.

Focal Point Regions

From a focal point region, you have visibility of all the managed file transfers and supporting resources.

Subordinates

From a subordinate, 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 environment.

Agents

Agents do not provide a presentation space. An agent monitors the local file transfers and supporting resources, and sends the information to the NetMaster for File Transfer region that has established a link with it. It also receives commands from the region and acts on them.

NetMaster for File Transfer supports agents that provide the interface to CONNECT:Direct applications on AS/400, Tandem, UNIX, and Windows NT systems.

File Transfer Logs

By using the file transfer log, you have a log that is devoted to the file transfer service. All file transfer events and messages are recorded in this single log. In a multisystem environment, you can view the logs in the linked regions from a focal point region.

Automatic Problem Recording

If you are running the SOLVE:Problem application on the system, you can tell NetMaster for File Transfer to raise a record in the SOLVE:Problem region when a problem occurs.

Automatic Generation of SNMP Traps

You can tell NetMaster for File Transfer to raise an SNMP trap when a specific event occurs.

Reporting Function

You can use the NetMaster for File Transfer reporting function to view your file transfer activities from a historical perspective.

The reporting function allows you to:

- Record file transfer events to an events database
- Display and print predefined reports on the recorded data
- Generate reports based on various search criteria
- Generate exception reports based on exception filters or file transfer schedule filters to report on expected events that are not found in the events database
- Generate custom reports
- Archive data to a sequential file as character-separated values (CSV)
- Extract data to a sequential file as character-separated values on an ad hoc basis for transfer to a PC file and processing by other data analysis and reporting tools

You can also use the NetMaster Reporter product to report on these file transfer activities.

FTP Function Policy Control

If your site uses the TCPaccess FTP server, you can maintain policies for the FTP file transfers.

About this Guide

This guide describes the NetMaster for File Transfer product. The guide explains how you can use the product to manage your file transfer service.

The guide enables a user to:

- Understand what this product can do
- Implement and administer the product
- Monitor and manage file transfers, schedules, and supporting resources

What You Should Know Already

This guide is for:

- System programmers and administrators who need to implement and administer the product
- Operations analysts and operators who need to manage the file transfer service

You should already be familiar with the products that support your file transfer service and with the operational requirements of the file transfer service at your site.

2

File Transfer Management Resources

This chapter describes the resources that you create in the knowledge base to manage file transfers.

The chapter contains the following topics:

- What Are File Transfer Management Resources?
- File Transfer Rules
- File Transfer Schedules

What Are File Transfer Management Resources?

File transfer management resources are definitions in the knowledge base that help you manage individual file transfers.

File transfer management can be divided into the following categories:

- Management of individual transfers as they occur (reactive management)
- Management of transfers that are scheduled to be completed at a certain time (proactive management)

To help you manage the file transfers in these ways, NetMaster for File Transfer provides the following:

- File transfer rules to provide reactive management
- File transfer schedules to provide proactive management.

File Transfer Rules

A file transfer rule contains the following types of information:

- Criteria that determine which file transfers are monitored
- Actions to perform when a file transfer satisfies the rule

Criteria

The primary criteria that a file transfer rule uses to screen file transfers are the transfer status and the transfer details. The transfer details can be CA-XCOM transfer IDs, CONNECT:Direct processes, CONNECT:Mailbox IDs, FTP server names, FTS transmission definitions, incoming files (target), or outgoing files (source). You can use the rule to detect the start, completion, or failure of a transfer.

When a transfer satisfies the primary criteria, you can differentiate it further by using the following secondary criteria:

- Time window that the rule is monitoring
- System from which the transfer originates
- System to which the transfer is destined
- ID of the user that performs the transfer
- Limits on the transferred number of bytes
- Limits on the transfer rate

Actions

By default, NetMaster for File Transfer generates an alert each time a file transfer satisfies the criteria of a rule. The severity of the alert is specified in the rule itself.

You can specify additional rule actions that are performed when a file transfer satisfies the rule criteria. These actions include generating a problem record and executing an Automation Services process. For example, for rules that monitor failed transfers, you might want to include an action that records the problem in your problem management application.

File Transfer Schedules

A file transfer rule does not tell you if a required transfer has not started. If you want to know whether one or more transfers complete successfully by a certain time, define a file transfer schedule for them in the knowledge base.

A file transfer schedule contains the following information to help you manage a file transfer:

- Time window within which the monitored file transfer should start and end
- Files in the transfer
- Actions to perform according to the status of the transfer (for example, for a status that indicates a problem, you might want to include a NetMaster for File Transfer process that records the problem in your problem management application)

3

File Transfer Application Resources

This chapter describes the resources that you create in the knowledge base to manage CA-XCOM, CONNECT:Direct, CONNECT:Mailbox, FTS, and FTP file transfer regions.

The chapter contains the following topics:

- What Are File Transfer Resources?
- Operational Relationship Between a File Transfer Monitor and Its Manager
- What Is a CA-XCOM Resource?
- The CA-XCOM File Transfer Manager Definitions
- The CA-XCOM File Transfer Monitor Definitions
- Event Flow from a CA-XCOM File Transfer Service
- What Is a CONNECT:Direct Resource?
- The CONNECT:Direct File Transfer Manager Definitions
- The CONNECT:Direct File Transfer Monitor Definitions
- Event Flow from a CONNECT:Direct File Transfer Service
- What Is a CONNECT:Mailbox Resource
- CONNECT:Mailbox VSAM File Server Definitions
- CONNECT:Mailbox Manager Definitions
- CONNECT:Mailbox Monitor Definitions
- Event Flow from CONNECT:Mailbox
- What Is an FTS Resource?
- The FTS File Transfer Manager Definitions
- The FTS File Transfer Monitor Definitions
- Event Flow from an FTS File Transfer Service
- What Is an FTP Resource?
- The FTP File Transfer Manager Definitions
- The FTP File Transfer Monitor Definitions
- Event Flow from an FTP File Transfer Service

What Are File Transfer Resources?

In NetMaster for File Transfer, a file transfer resource is an entity being managed by your region. It has associated with it operational information that is stored in the knowledge base.

A file transfer product such as CA-XCOM, CONNECT:Direct, CONNECT:Mailbox, FTS, or FTP is represented by two types of file transfer resources: a manager and its monitors.

File Transfer Manager

A file transfer manager represents a file transfer application. It can be a job, a started task, or a CONNECT:Direct AS/400, Tandem, UNIX, or Windows NT application.

The manager is deemed to be the owner of the file transfer monitors. In operation, the manager controls the file transfer region and reflects the status of the monitors.

File Transfer Monitors

The file transfer monitors are owned resources, with the file transfer manager as the owner. They monitor the operational states that affect the performance of the file transfer service.

Operational Relationship Between a File Transfer Monitor and Its Manager

In NetMaster for File Transfer, a file transfer monitor and its manager have the following operational relationships:

- A monitor becomes active when its manager is started.
- A monitor becomes inactive when its manager is shut down.

Also, if a monitor finds that an operational state is degrading the performance of the file transfer service, the condition is reflected in its owner, the manager.

Owned Resource Names

NetMaster for File Transfer manages an owned file transfer resource in relation to the file transfer manager that owns it. The owned resource is known to the region as *owner-name.resource-name*, where:

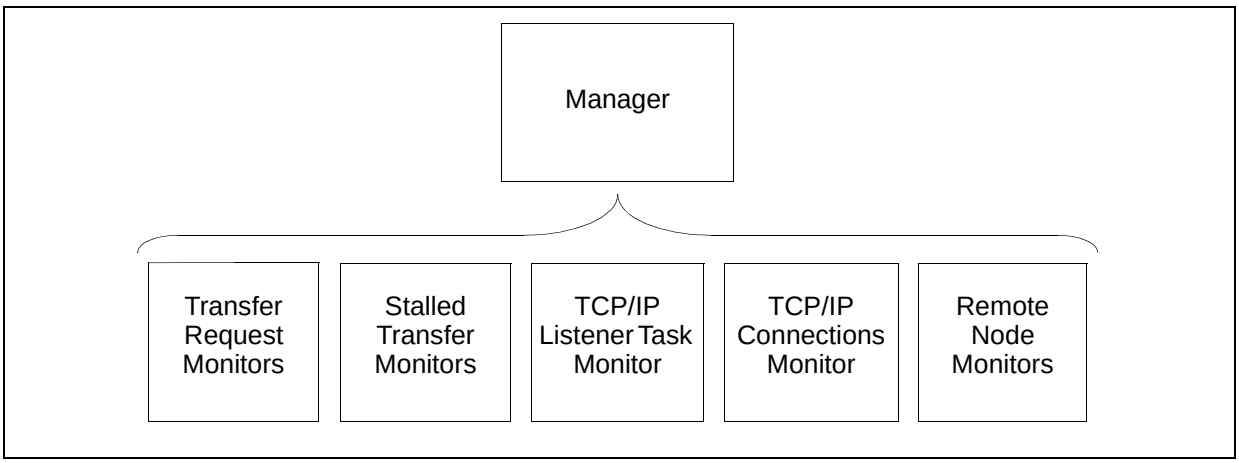
- *owner-name* is the name of the manager that owns the resource
- *resource-name* is the name of the owned resource

For example, if a file transfer region (the manager), SYDCD1, owns a monitor, EXECQ, the monitor is known to the region as SYDCD1.EXECQ.

What Is a CA-XCOM Resource?

In NetMaster for File Transfer, a CA-XCOM resource is an entity being managed by the region. It has associated with it operational information that is stored in the knowledge base. Figure 3-3 shows the supported CA-XCOM resources and their relationships.

Figure 3-1. CA-XCOM Resources



CA-XCOM File Transfer Manager

The CA-XCOM file transfer manager represents a CA-XCOM for MVS application. It can be a job or a started task.

CA-XCOM File Transfer Monitors

The CA-XCOM file transfer monitors are owned resources, with the CA-XCOM file transfer manager as the owner. They monitor the operational states that affect the performance of a CA-XCOM file transfer service. These states are monitored by the respective monitors as follows:

CA-XCOM Operational State	Monitors
The number of transfer requests in a CA-XCOM region exceeds a user-defined threshold.	Transfer request monitors for active, held, inactive, and suspended requests
A transfer in progress has been idle for too long, indicating a possible stalled condition.	Stalled transfer monitors
The CA-XCOM TCP/IP listener task is not available.	TCP/IP listener task monitor
A CA-XCOM TCP/IP data transfer connection has been idle for too long, indicating a possible hung condition.	TCP/IP connections monitor
A remote file transfer partner is not available.	Remote node monitors

The CA-XCOM File Transfer Manager Definitions

The CA-XCOM region provides a file transfer service. You may have more than one CA-XCOM region on a system to provide that service. NetMaster for File Transfer manages these regions through the information in the CA-XCOM file transfer manager resource definitions.

A manager can be defined for a job or a started task.

CA-XCOM Manager Templates for Jobs and Started Tasks

Templates are provided for defining CA-XCOM managers in the knowledge base. The templates contain the following information to help you manage a CA-XCOM region:

- System commands that activate, inactivate, and retrieve status information about the CA-XCOM region.
- System and CA-XCOM messages, and CA-XCOM monitor resource events that change the actual state of the region. For messages that indicate a problem, you might want to include a NetMaster for File Transfer process that takes certain actions (for example, to record the problem in your problem management application).

The CA-XCOM File Transfer Monitor Definitions

NetMaster for File Transfer uses the information in the CA-XCOM file transfer monitor resource definitions to monitor the operational states that affect the performance of the file transfer service.

Transfer Request Monitor Templates

Templates are provided for defining the following CA-XCOM transfer request monitors in the knowledge base:

- Active transfer monitor
- Held transfer monitor
- Inactive transfer monitor
- Suspended transfer monitor

The templates contain the following information to help you monitor a transfer request:

- A timer that solicits information about the request at regular intervals.
- A threshold for the number of CA-XCOM requests in the monitored status—if the threshold is exceeded (indicating that too many requests are in the monitored status), the state of the monitor resource changes to DEGRADED and the extended display shows the reason. A resource event is raised to indicate the condition.
- CA-XCOM monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a NetMaster for File Transfer process that takes certain actions when an undesired condition occurs (for example, to record the problem in your problem management application).

Stalled Transfer Monitor Templates

A template is provided for defining the CA-XCOM transfer monitors in the knowledge base. The template contains the following information to help you monitor executing processes:

- A timer that solicits information about the transfers at regular intervals.
- A stalled time limit that indicates that a transfer might be stalled—if no data is transferred by the time limit, the state of the monitor resource changes to DEGRADED. A resource event is raised to indicate the condition.
- A stalled time limit that indicates that a transfer can be terminated.
- CA-XCOM monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a NetMaster for File Transfer process that takes certain actions when an undesired condition occurs (for example, to record the problem in your problem management application and raise an SNMP trap).

TCP/IP Listener Task Monitor Template

A template is provided for defining the CA-XCOM TCP/IP listener task monitor in the knowledge base. The template contains the following information to help you monitor the listener task:

- A timer that solicits information about the listener task at regular intervals. If the task is not found, the state of the monitor resource changes to DEGRADED. A resource event is raised to indicate the condition.
- CA-XCOM monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a NetMaster for File Transfer process that takes certain actions when an undesired condition occurs (for example, to record the problem in your problem management application and raise an SNMP trap).

TCP/IP Connections Monitor Template

A template is provided for defining the CA-XCOM TCP/IP connections monitor in the knowledge base. The template contains the following information to help you monitor the connections:

- A timer that solicits information about the connections at regular intervals.
- An idle time limit that indicates that a connection might be hung—if the limit is exceeded, the state of the monitor resource changes to DEGRADED. A resource event is raised to indicate the condition.
- An idle time limit that indicates that a connection can be dropped (terminated).
- CA-XCOM monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a NetMaster for File Transfer process that takes certain actions when an undesired condition occurs (for example, to record the problem in your problem management application and raise an SNMP trap).

Remote Node Monitor Template

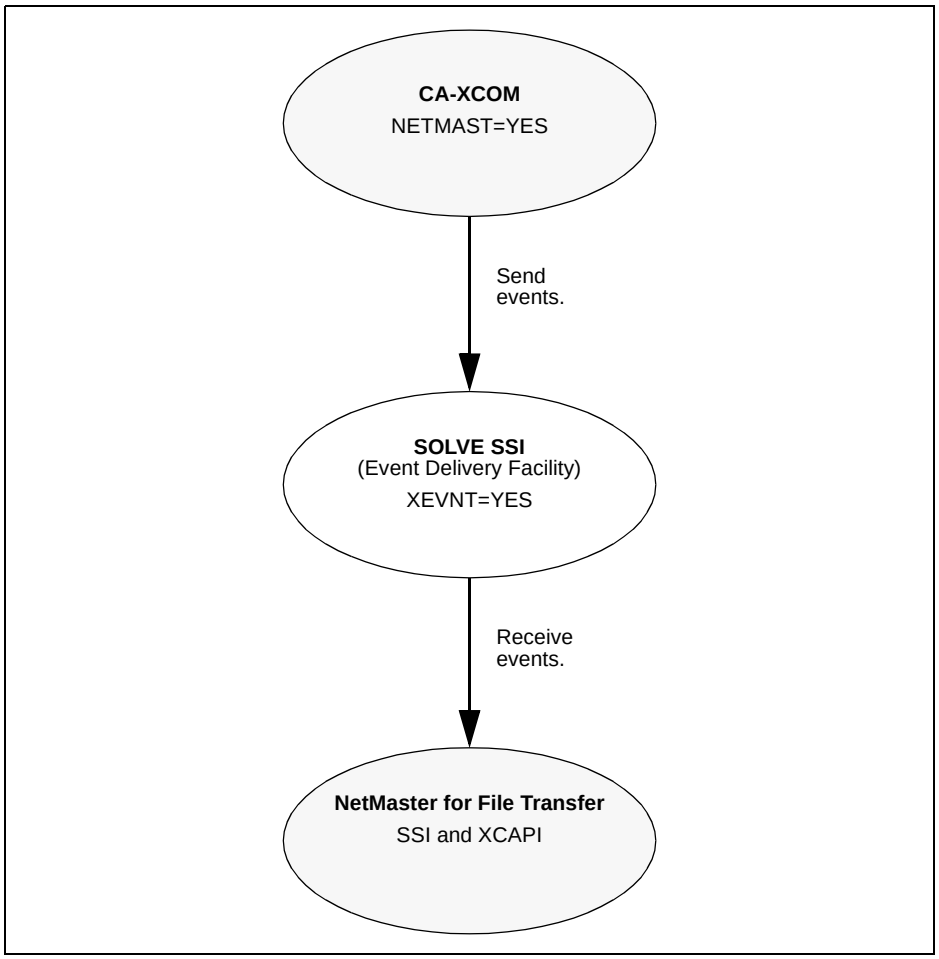
A template is provided for defining the CA-XCOM remote node monitors in the knowledge base. The template contains the following information to help you monitor a file transfer partner:

- A timer that solicits information about the partner at regular intervals. If the partner is not available, the state of the monitor resource changes to DEGRADED. A resource event is raised to indicate the condition.
- CA-XCOM monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a NetMaster for File Transfer process that takes certain actions when an undesired condition occurs (for example, to record the problem in your problem management application and raise an SNMP trap).

Event Flow from a CA-XCOM File Transfer Service

Event flow from a CA-XCOM region uses the SOLVE SSI event delivery facility. Figure 3-4 shows the flow of events from CA-XCOM on an MVS or OS/390 system to NetMaster for File Transfer.

Figure 3-2. Event Flow From CA-XCOM on an MVS or OS/390 System to NetMaster for File Transfer



NetMaster for File Transfer provides a CA-XCOM exit, NM000FXX. The exit sends CA-XCOM events to a receiver by using the event delivery facility. NetMaster for File Transfer listens to that receiver (specified in the XCAPI parameter group) for the events.

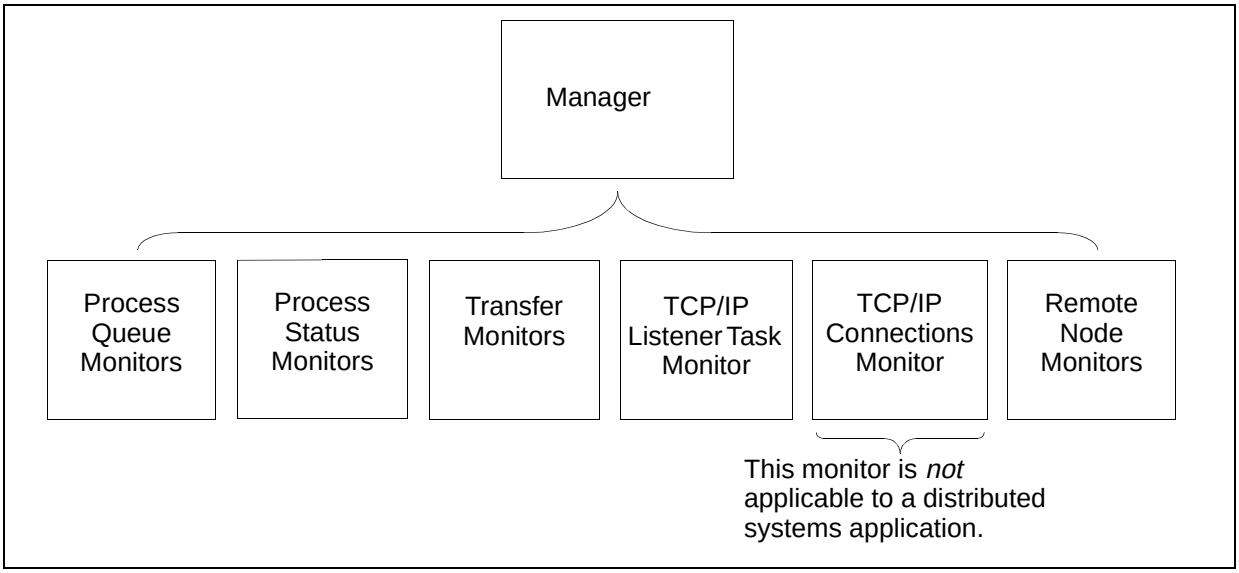
The SOLVE SSI task that provides the event delivery facility is specified in the NetMaster for File Transfer SSI parameter group.

For information about how to implement the event flow, see the section, *Subtask 7.1—Customizing the Managed CA-XCOM Regions*, on page 5-28.

What Is a CONNECT:Direct Resource?

In NetMaster for File Transfer, a CONNECT:Direct resource is an entity being managed by the region. It has associated with it operational information that is stored in the knowledge base. Figure 3-3 shows the supported CONNECT:Direct resources and their relationships.

Figure 3-3. CONNECT:Direct Resources



CONNECT:Direct File Transfer Manager

The CONNECT:Direct file transfer manager represents a CONNECT:Direct application. It can be a job, a started task, or an application on a distributed system such as UNIX.

CONNECT:Direct File Transfer Monitors

The CONNECT:Direct file transfer monitors are owned resources, with the CONNECT:Direct file transfer manager as the owner. They monitor the operational states that affect the performance of a CONNECT:Direct file transfer service. These states are monitored by the respective monitors as follows:

CONNECT:Direct Operational State	Monitors
The number of processes in a CONNECT:Direct queue exceeds a user-defined threshold.	Process queue monitors for the Exec, Hold, Timer, and Wait queues
The number of processes in a CONNECT:Direct queue that are in a particular state exceeds a user-defined threshold.	Process status monitors
A transfer in progress has been idle for too long, indicating a possible stalled condition.	Transfer monitors
The CONNECT:Direct TCP/IP listener task is not available.	TCP/IP listener task monitor
A CONNECT:Direct TCP/IP data transfer connection has been idle for too long, indicating a possible hung condition.	TCP/IP connections monitor
A remote file transfer partner is not available.	Remote node monitors

The CONNECT:Direct File Transfer Manager Definitions

The CONNECT:Direct region provides a file transfer service. You can have more than one CONNECT:Direct region (at the same version level) on a system to provide that service. NetMaster for File Transfer manages these regions through the information in the CONNECT:Direct file transfer manager resource definitions.

A manager can be defined for a job, a started task, or an application on a distributed system such as UNIX.

CONNECT:Direct Manager Templates for Jobs and Started Tasks

Templates are provided for defining CONNECT:Direct managers in the knowledge base. The templates contain the following information to help you manage a CONNECT:Direct region:

- System commands that activate, inactivate, and retrieve status information about the CONNECT:Direct region.
- System and CONNECT:Direct messages, and CONNECT:Direct monitor resource events that change the actual state of the region. For messages that indicate a problem, you might want to include a NetMaster for File Transfer process that takes certain actions (for example, to record the problem in your problem management application).

CONNECT:Direct Manager Template for Distributed Systems Applications

Templates are provided for defining managers for the following CONNECT:Direct applications in the knowledge base:

- CONNECT:Direct for OS/400
- CONNECT:Direct for Tandem
- CONNECT:Direct for UNIX
- CONNECT:Direct for Windows NT

The templates contain the NetMaster for File Transfer processes that activate, inactivate, and retrieve status information about the communication path to the remote system.

The CONNECT:Direct File Transfer Monitor Definitions

NetMaster for File Transfer uses the information in the CONNECT:Direct file transfer monitor resource definitions to monitor the operational states that affect the performance of the file transfer service.

Process Queue Monitor Templates

Templates are provided for defining the following CONNECT:Direct process queue monitors in the knowledge base:

- Exec queue monitor
- Hold queue monitor
- Timer queue monitor
- Wait queue monitor

The templates contain the following information to help you monitor a process queue:

- A timer that solicits information about the queue at regular intervals.
- A threshold for the number of CONNECT:Direct processes in the queue—if the threshold is exceeded (indicating that too many processes are being queued), the state of the monitor resource changes to DEGRADED and the extended display shows the reason. A resource event is raised to indicate the condition.
- CONNECT:Direct monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a NetMaster for File Transfer process that takes certain actions when an undesired condition occurs (for example, to record the problem in your problem management application).

Process Status Monitor Templates

Templates are provided for defining the following CONNECT:Direct process status monitors in the knowledge base:

- A monitor that looks for processes in the Hold queue that are in the WC (Wait for Connection) state
- A monitor that looks for processes in the Timer queue that are in the RE (Retry) state

The templates are extensions of the queue monitor templates. They contain an additional parameter, the CONNECT:Direct process state to monitor. You might want to monitor the state because a process in that state can indicate a degradation in the performance of the file transfer service (for example, a process with the WC state in the Hold queue).

If the number of processes in the queue that are in the specified state exceeds the threshold, the state of the monitor resource changes to DEGRADED. A resource event is raised to indicate the condition.

Transfer Monitor Templates

A template is provided for defining the CONNECT:Direct transfer monitors in the knowledge base. The template contains the following information to help you monitor executing processes:

- A timer that solicits information about the processes at regular intervals.
- A stalled time limit that indicates that a transfer might be stalled—if no data is transferred by the time limit, the state of the monitor resource changes to DEGRADED. A resource event is raised to indicate the condition.
- A stalled time limit that indicates that a process can be flushed (terminated).
- CONNECT:Direct monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a NetMaster for File Transfer process that takes certain actions when an undesired condition occurs (for example, to record the problem in your problem management application and raise an SNMP trap).

TCP/IP Listener Task Monitor Template

A template is provided for defining the CONNECT:Direct TCP/IP listener task monitor in the knowledge base. The template contains the following information to help you monitor the listener task:

- A timer that solicits information about the listener task at regular intervals. If the task is not found, the state of the monitor resource changes to DEGRADED. A resource event is raised to indicate the condition.
- CONNECT:Direct monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a NetMaster for File Transfer process that takes certain actions when an undesired condition occurs (for example, to record the problem in your problem management application and raise an SNMP trap).

TCP/IP Connections Monitor Template

A template is provided for defining the CONNECT:Direct TCP/IP connections monitor in the knowledge base. The template contains the following information to help you monitor the connections:

- A timer that solicits information about the connections at regular intervals.
- An idle time limit that indicates that a connection might be hung—if the limit is exceeded, the state of the monitor resource changes to DEGRADED. A resource event is raised to indicate the condition.
- An idle time limit that indicates that a connection can be dropped (terminated).
- CONNECT:Direct monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a NetMaster for File Transfer process that takes certain actions when an undesired condition occurs (for example, to record the problem in your problem management application and raise an SNMP trap).

Remote Node Monitor Template

A template is provided for defining the CONNECT:Direct remote node monitors in the knowledge base. The template contains the following information to help you monitor a file transfer partner:

- A timer that solicits information about the partner at regular intervals. If the partner is not available, the state of the monitor resource changes to DEGRADED. A resource event is raised to indicate the condition.
- CONNECT:Direct monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a NetMaster for File Transfer process that takes certain actions when an undesired condition occurs (for example, to record the problem in your problem management application and raise an SNMP trap).

Event Flow from a CONNECT:Direct File Transfer Service

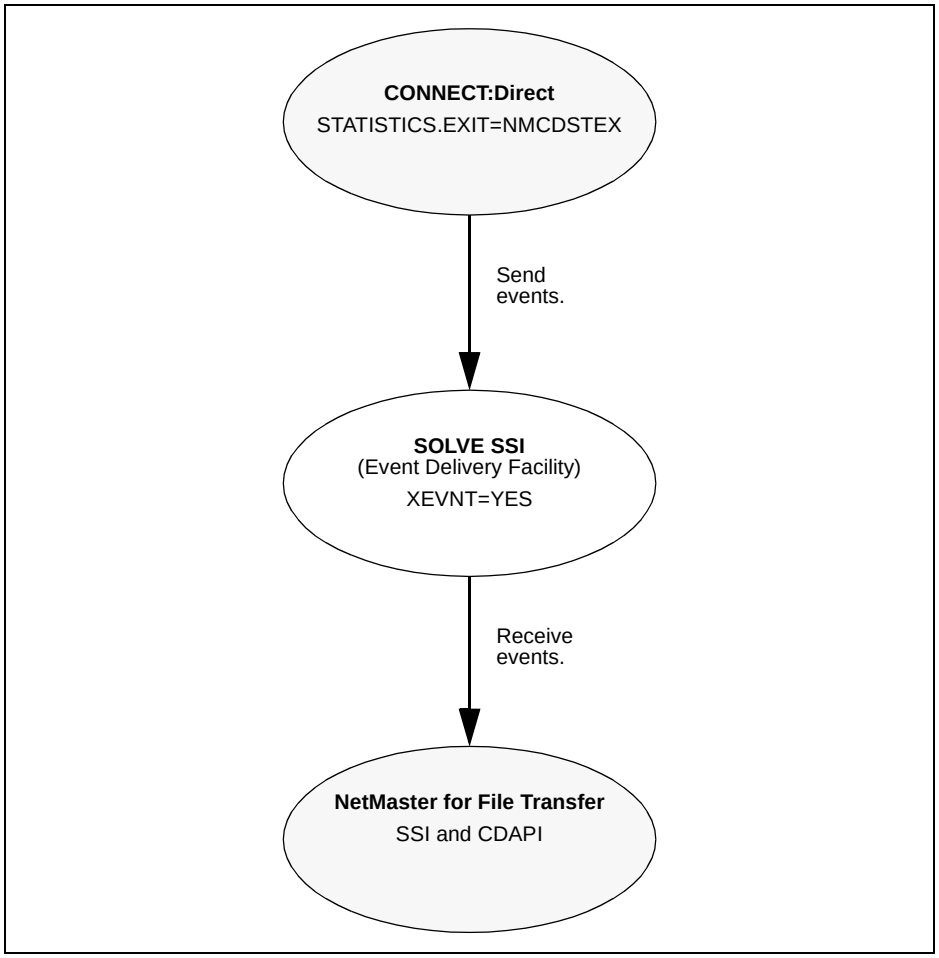
Event flow from CONNECT:Direct uses the following mechanisms:

- For CONNECT:Direct on an MVS or OS/390 system, the mechanisms are the CONNECT:Direct statistics exit and SOLVE SSI event delivery facility
- For CONNECT:Direct on a distributed system such as UNIX, the mechanisms are the NetMaster for File Transfer agent and the TCP/IP link.

MVS or OS/390 System

Figure 3-4 shows the flow of events from CONNECT:Direct on an MVS or OS/390 system to NetMaster for File Transfer.

Figure 3-4. Event Flow From CONNECT:Direct on an MVS or OS/390 System to NetMaster for File Transfer



NetMaster for File Transfer provides a CONNECT:Direct statistics exit, NMCDSTEX. The exit sends CONNECT:Direct events to a receiver by using the event delivery facility. NetMaster for File Transfer listens to that receiver (specified in the CDAPI parameter group) for the events.

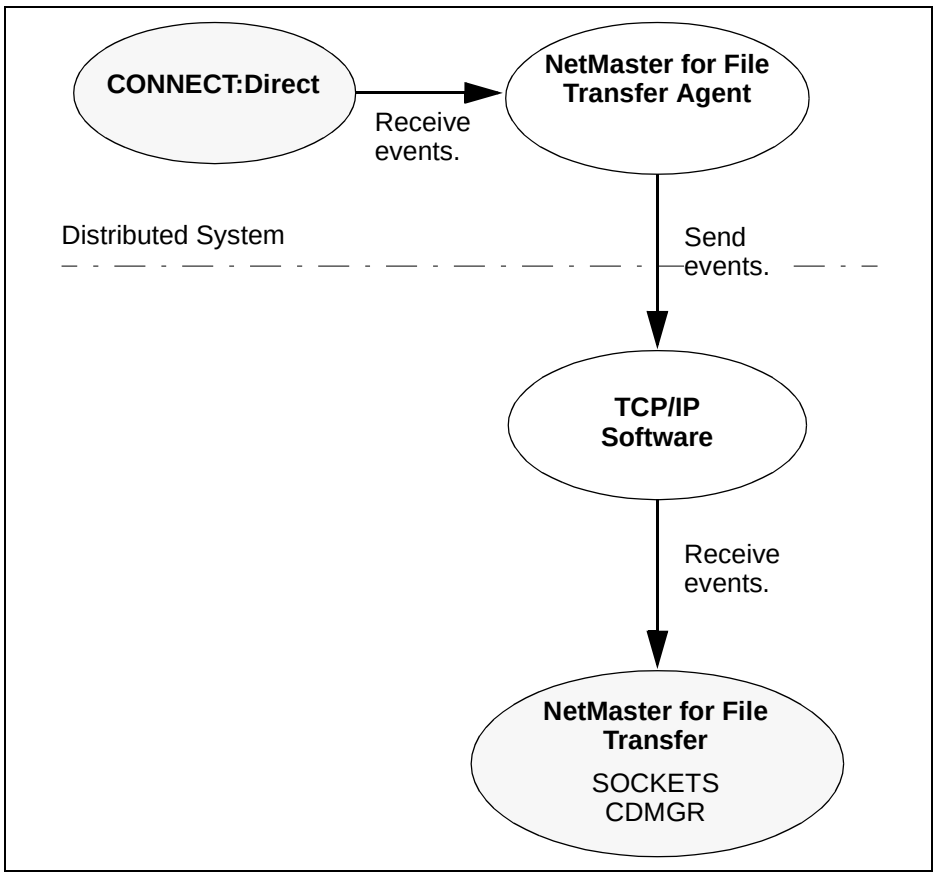
The SOLVE SSI task that provides the event delivery facility is specified in the NetMaster for File Transfer SSI parameter group.

For information about how to implement the event flow, see the section, *Subtask 7.2—Customizing the Managed CONNECT:Direct Regions*, on page 5-29.

Distributed Systems

Figure 3-5 shows the flow of events from CONNECT:Direct on a distributed system such as UNIX to NetMaster for File Transfer.

Figure 3-5. Event Flow From CONNECT:Direct on a Distributed System to NetMaster for File Transfer



NetMaster for File Transfer provides agents for the following systems: AS/400, Tandem, UNIX, and Windows NT. The agent forwards CONNECT:Direct events to the corresponding CONNECT:Direct manager (CDMGR) in your region.

The TCP/IP interface is implemented in the NetMaster for File Transfer SOCKETS parameter group.

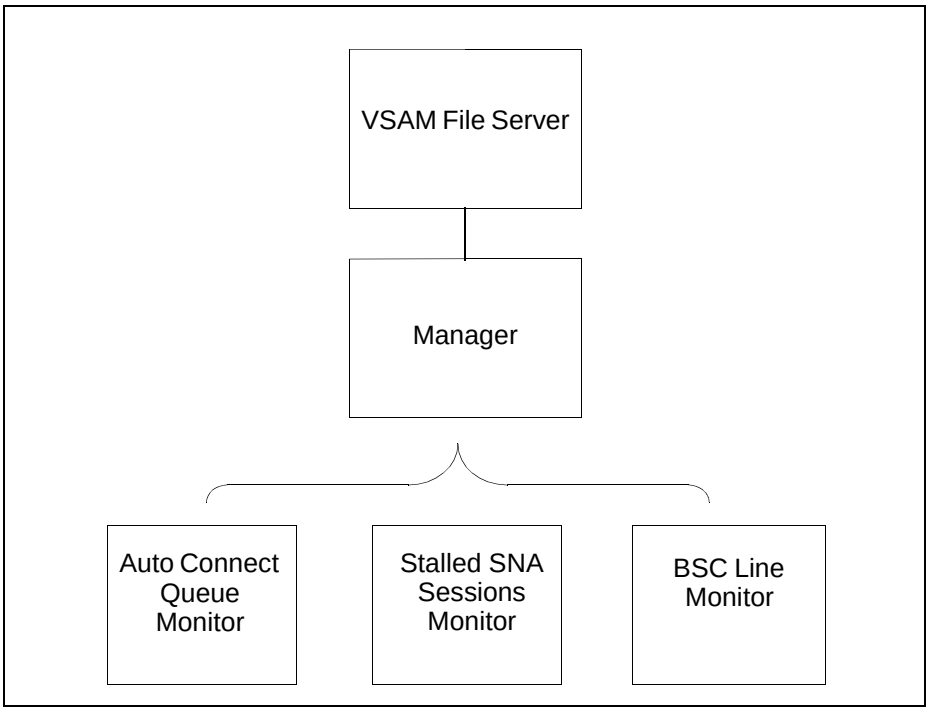
For information about how to implement the event flow, see the following:

For information about how to implement the…	**See the…**
Agents	*SOLVE:Operations for File Transfer Agent - CONNECT:Direct Installation and Administration Guide*.
TCP/IP interface	Section, *Implementing the TCP/IP Interface*, on page 5-11, and the section, *Task 9—Enabling the Interface Between NetMaster for File Transfer and TCP/IP*, on page 5-47.
CONNECT:Direct manager	Section, *Defining CONNECT:Direct Resources*, on page 10-29.

What Is a CONNECT:Mailbox Resource

In NetMaster for File Transfer, a CONNECT:Mailbox resource is an entity being managed by the region. It has associated with it operational information that is stored in the knowledge base. Figure 3-6 shows the supported CONNECT:Mailbox resources and their relationships.

Figure 3-6. CONNECT:Mailbox Resources



CONNECT:Mailbox VSAM File Server

The CONNECT:Mailbox VSAM file server started task resource represents the CONNECT:Mailbox VSAM file server.

CONNECT:Mailbox Manager

The CONNECT:Mailbox manager represents a CONNECT:Mailbox application.

CONNECT:Mailbox Monitors

The CONNECT:Mailbox monitors are owned resources, with the CONNECT:Mailbox manager as the owner. They monitor the operational states that affect the performance of a CONNECT:Mailbox application. These states are monitored by the respective monitors as follows:

CONNECT:Mailbox Operational State	Monitor
The number of queued Auto Connects exceeds a user-defined threshold.	Auto Connect queue monitor
A BSC line is not available.	BSC line monitor
An SNA session has been idle for too long, indicating a possible stalled condition.	Stalled SNA session monitor

CONNECT:Mailbox VSAM File Server Definitions

The CONNECT:Mailbox VSAM file server handles all VSAM input and output for the CONNECT:Mailbox application. The CONNECT:Mailbox VSAM file server has a parent-child relationship with the CONNECT:Mailbox manager.

VSAM File Server Template

A template is provided for defining the CONNECT:Mailbox VSAM file server started task in the knowledge base. The template contains the following information to manage the CONNECT:Mailbox VSAM file server started task:

- Start, stop, and display commands
- Monitored messages

CONNECT:Mailbox Manager Definitions

The CONNECT:Mailbox region provides a file transfer service. You can have more than one CONNECT:Mailbox region on a system to provide that service. NetMaster for File Transfer manages these regions through the information in the CONNECT:Mailbox manager resource definitions.

A manager can be defined for a CONNECT:Mailbox region running as a started task.

The CONNECT:Mailbox Manager Template

A template is provided for defining CONNECT:Mailbox managers in the knowledge base. The template contains the following information to help you manage a CONNECT:Mailbox region:

- System commands that activate, inactivate, and retrieve status information about the CONNECT:Mailbox region.
- System and CONNECT:Mailbox messages, and CONNECT:Mailbox monitor resource events that change the actual state of the region. For messages that indicate a problem, you might want to include a NetMaster for File Transfer process that takes certain actions (for example, to record the problem in your problem management application).

CONNECT:Mailbox Monitor Definitions

NetMaster for File Transfer uses the information in the CONNECT:Mailbox monitor resource definitions to monitor the operational states that affect the performance of the file transfer service.

Auto Connect Queue Monitor Template

A template is provided for defining an Auto Connect queue monitor in the knowledge base. The template contains the following information to help you monitor the Auto Connect function:

- A timer that solicits information about the Auto Connect queue at regular intervals
- A threshold for the number of queued Auto Connects—if the threshold is exceeded, the state of the monitor resource changes to degraded and an alert is raised to indicate the condition
- CONNECT:Mailbox monitor resource events that change the actual state of the monitor resource to indicate a problem

BSC Line Monitor Template

A template is provided for defining a BSC line monitor in the knowledge base. The template contains information to help you monitor BSC lines:

- A timer that solicits information about BSC lines at regular intervals
- CONNECT:Mailbox monitor resource events that change the actual state of the monitor resource to indicate a problem

Stalled SNA Session Monitor Template

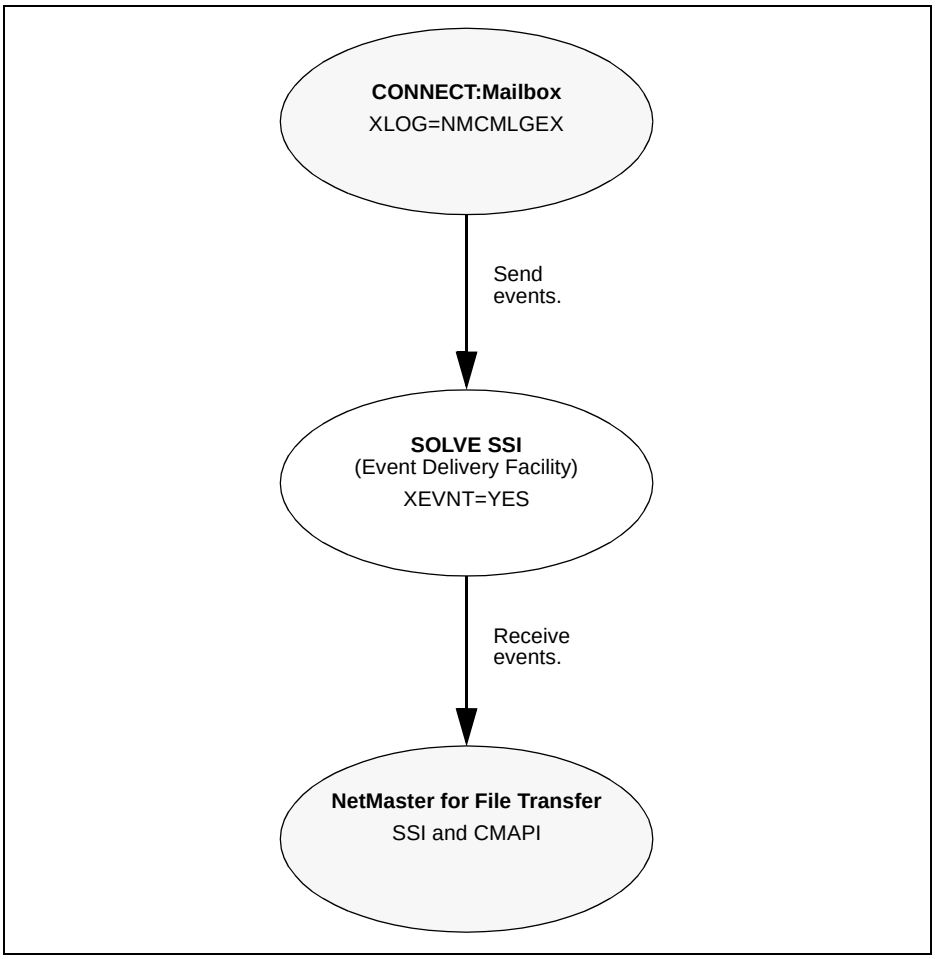
A template is provided for defining a stalled SNA session monitor in the knowledge base. The template contains the following information to help you monitor SNA sessions:

- A timer that solicits information about SNA sessions at regular intervals
- An idle time limit that indicates an SNA session might be stalled. If the time limit is exceeded, the state of the monitor resource changes to degraded and an alert is raised to indicate the condition
- CONNECT:Mailbox monitor resource events that change the actual state of the monitor resource to indicate a problem

Event Flow from CONNECT:Mailbox

Figure 3-7 shows the flow of events from CONNECT:Mailbox to NetMaster for File Transfer.

Figure 3-7. Event Flow from CONNECT:Mailbox to NetMaster for File Transfer



NetMaster for File Transfer provides a log exit, NMCMLGEX. The exit sends CONNECT:Mailbox events to a receiver by using the event delivery facility. NetMaster for File Transfer listens to that receiver (specified in the CMAPI parameter group) for the events.

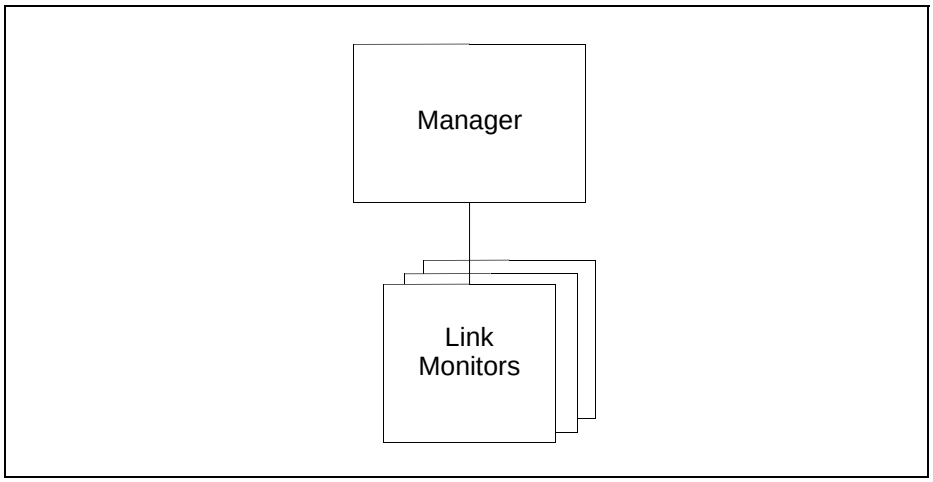
The ID of the SOLVE SSI task that provides the event delivery facility is specified in the NetMaster for File Transfer SSI parameter group.

For information about how to implement the event flow, see the section, *Defining CONNECT:Mailbox Resources*, on page 10-38.

What Is an FTS Resource?

In NetMaster for File Transfer, an FTS resource is an entity being managed by the region. It has associated with it operational information that is stored in the knowledge base. Figure 3-8 shows the supported FTS resources and their relationships.

Figure 3-8. FTS Resources



FTS File Transfer Manager

The FTS file transfer manager represents an FTS region. It can be either a job or a started task. You must define a manager for an FTS region before you can manage the file transfers to and from that region.

You can also define a manager for an FTS region on another system. However, the manager only enables the monitoring of the communications path to the region and the file transfers. It does not manage the region itself.

FTS File Transfer Monitors

The FTS file transfer monitors are owned resources, with the FTS file transfer manager as the owner. They monitor the operational states of the FTS INMC links.

The FTS File Transfer Manager Definitions

The FTS region provides a file transfer service. You can have more than one FTS region on a system to provide that service. NetMaster for File Transfer manages these regions through the information in the FTS file transfer manager resource definitions.

A manager can be defined for either a job, a started task, or a remote region, depending on whether the region is established by a job or a started task, or is on another system.

FTS Manager Templates for Jobs and Started Tasks

Templates are provided for defining managers for FTS jobs and started tasks in the knowledge base. The templates contain the following information to help you manage an FTS region:

- System commands that activate, inactivate, and retrieve status information about the FTS region.
- System and FTS messages, and FTS monitor resource events that change the actual state of the region. For messages that indicate a problem, you might want to include a NetMaster for File Transfer process that takes certain actions (for example, to record the problem in your problem management application).

FTS Manager Template for Remote Regions

A template is provided for defining managers for remote FTS regions in the knowledge base. The template contains the following information to help you manage an FTS region:

- NetMaster for File Transfer processes that activate, inactivate, and retrieve status information about the INMC link to the remote region.
- FTS monitor resource events that change the actual state of the manager. For messages that indicate a problem, you might want to include a NetMaster for File Transfer process that takes certain actions (for example, to record the problem in your problem management application).

The FTS File Transfer Monitor Definitions

NetMaster for File Transfer uses the information in the FTS file transfer monitor resource definitions to monitor the operational states that affect the links between the FTS file transfer regions.

INMC Link Monitor Template

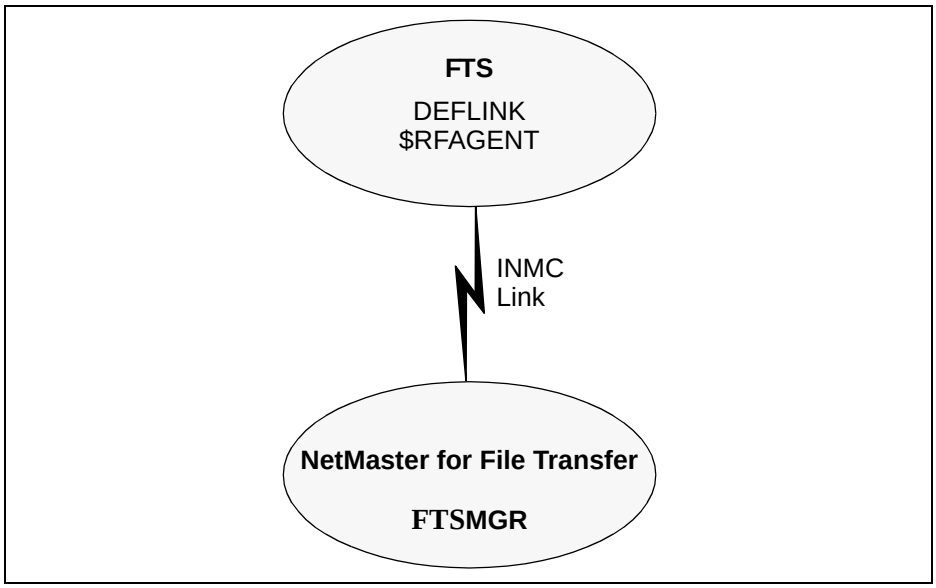
A template is provided for defining the FTS INMC link monitors in the knowledge base. You define one monitor for each link. The template contains the following information to help you monitor a link:

- A timer that solicits information about the link at regular intervals.
- FTS monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a NetMaster for File Transfer process that takes certain actions when an undesired condition occurs (for example, to record the problem in your problem management application).

Event Flow from an FTS File Transfer Service

Figure 3-9 shows the flow of events from FTS to NetMaster for File Transfer.

Figure 3-9. Event Flow From FTS to NetMaster for File Transfer



NetMaster for File Transfer provides an FTS message handler, $RFAGENT. The handler processes FTS events before they are sent to the corresponding FTS manager (FTSMGR) in the NetMaster for File Transfer region by using an INMC link.

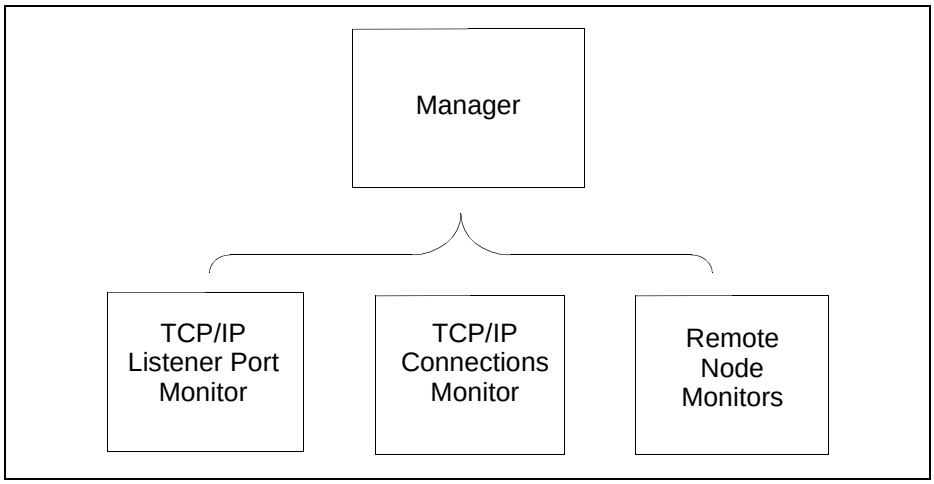
The INMC link is provided by a DEFLINK command in the FTS region.

For information about how to implement the event flow, see the section, *Subtask 7.4—Customizing the Managed FTS Regions*, on page 5-36.

What Is an FTP Resource?

In NetMaster for File Transfer, an FTP resource is an entity being managed by the region. It has associated with it operational information that is stored in the knowledge base. Figure 3-10 shows the supported FTP resources and their relationships.

Figure 3-10. FTP Resources



FTP File Transfer Manager

The FTP file transfer manager represents an FTP server application. It can be a job or a started task.

FTP File Transfer Monitors

The FTP file transfer monitors are owned resources, with the FTP file transfer manager as the owner. They monitor the operational states that affect the performance of an FTP file transfer service. These states are monitored by the respective monitors as follows:

FTP Operational State	Monitored by the…
The FTP listener port is not available.	TCP/IP listener port monitor.
An FTP data transfer connection has been idle for too long, indicating a possible hung condition.	TCP/IP connections monitor.
A remote FTP server is not available.	Remote node monitors

The FTP File Transfer Manager Definitions

The FTP server region provides a file transfer service. You can have more than one FTP server region on a system to provide that service.

Note

Each of these FTP server regions must be on the same type of TCP/IP stack, for example, Communications Server *or* TCPaccess.

NetMaster for File Transfer manages these regions by using the information in the FTP file transfer manager resource definitions

A manager can be defined for a job or a started task.

FTP Manager Templates for Jobs and Started Tasks

Templates are provided for defining FTP managers in the knowledge base. The templates contain the following information to help you manage an FTP server region:

- System commands and NetMaster for File Transfer processes that activate, inactivate, and retrieve status information about the FTP server region.
- System and FTP messages, and FTP monitor resource events that change the actual state of the region. For messages that indicate a problem, you might want to include a NetMaster for File Transfer process that takes certain actions (for example, to record the problem in your problem management application).

Customizing TCPaccess FTP Server Templates

The TCPaccess FTP server resources in templates $TEMPLAT001 and $TEMPLAT002 are SFTPJOB and SFTPSTC. These resources support the sample procedure for a started task, distributed with the TCPaccess FTP Server product. If you customize the batch job JCL for this distributed sample procedure, then you need to check the SFTPJOB template resource for consistency.

The FTP File Transfer Monitor Definitions

NetMaster for File Transfer uses the information in the FTP file transfer monitor resource definitions to monitor the operational states that affect the performance of the file transfer service.

TCP/IP Listener Port Monitor Template

A template is provided for defining the FTP TCP/IP listener port monitor in the knowledge base. The template contains the following information to help you monitor the listener port:

- A timer that solicits information about the listener port at regular intervals. If the port is not found, the state of the monitor resource changes to DEGRADED. A resource event is raised to indicate the condition.
- FTP monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a NetMaster for File Transfer process that takes certain actions when an undesired condition occurs (for example, to record the problem in your problem management application and raise an SNMP trap).

TCP/IP Connections Monitor Template

A template is provided for defining the FTP TCP/IP connections monitor in the knowledge base. The template contains the following information to help you monitor the connections:

- A timer that solicits information about the connections at regular intervals
- An idle time limit that indicates that a connection might be hung—if the limit is exceeded, the state of the monitor resource changes to DEGRADED. A resource event is raised to indicate the condition.
- An idle time limit that indicates that a connection can be dropped (terminated)
- FTP monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a NetMaster for File Transfer process that takes certain actions when an undesired condition occurs (for example, to record the problem in your problem management application and raise an SNMP trap)

Note

FTPMON monitors FTP data connections only. It does not monitor FTP control connections, but you can view them by using the D command from the status monitor.

Remote Node Monitor Template

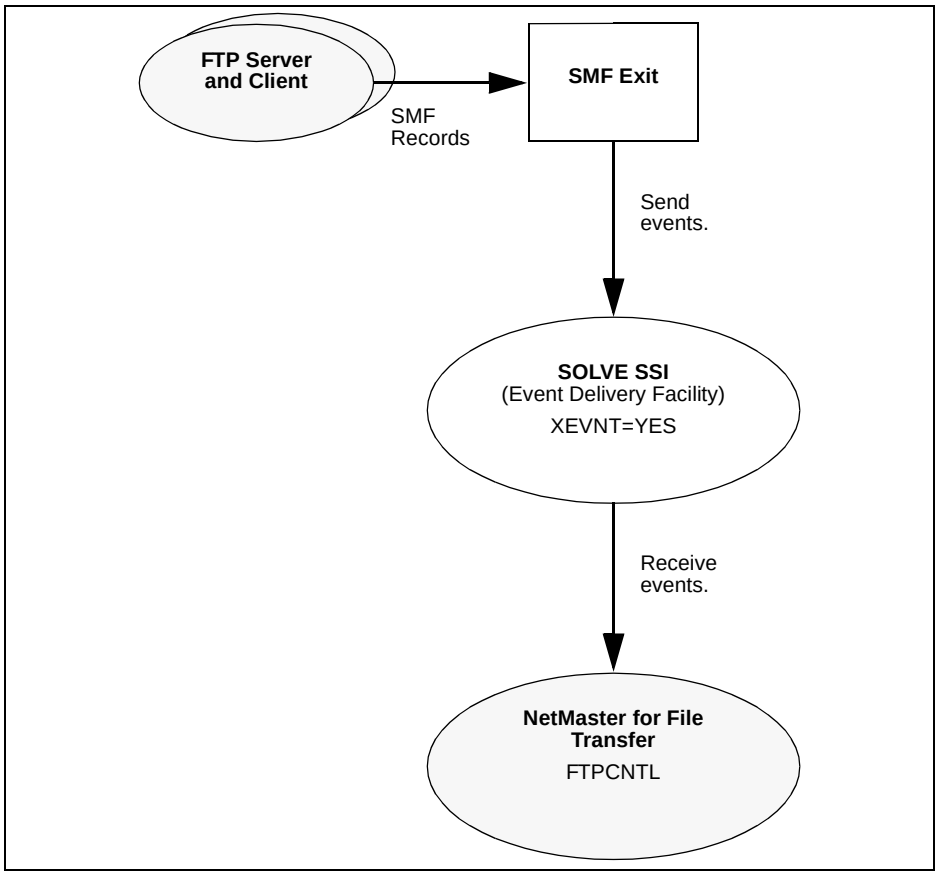
A template is provided for defining the FTP remote node monitors in the knowledge base. The template contains the following information to help you monitor a remote FTP server:

- A timer that solicits information about the remote FTP server at regular intervals. If the server is not available, the state of the monitor resource changes to DEGRADED. A resource event is raised to indicate the condition.
- FTP monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a NetMaster for File Transfer process that takes certain actions when an undesired condition occurs (for example, to record the problem in your problem management application and raise an SNMP trap).

Event Flow from an FTP File Transfer Service

Figure 3-11 shows the flow of events from an FTP server to NetMaster for File Transfer if you are *not* using a TCPaccess FTP server.

Figure 3-11. Event Flow From an FTP Server to NetMaster for File Transfer Not Using TCPaccess FTP Server



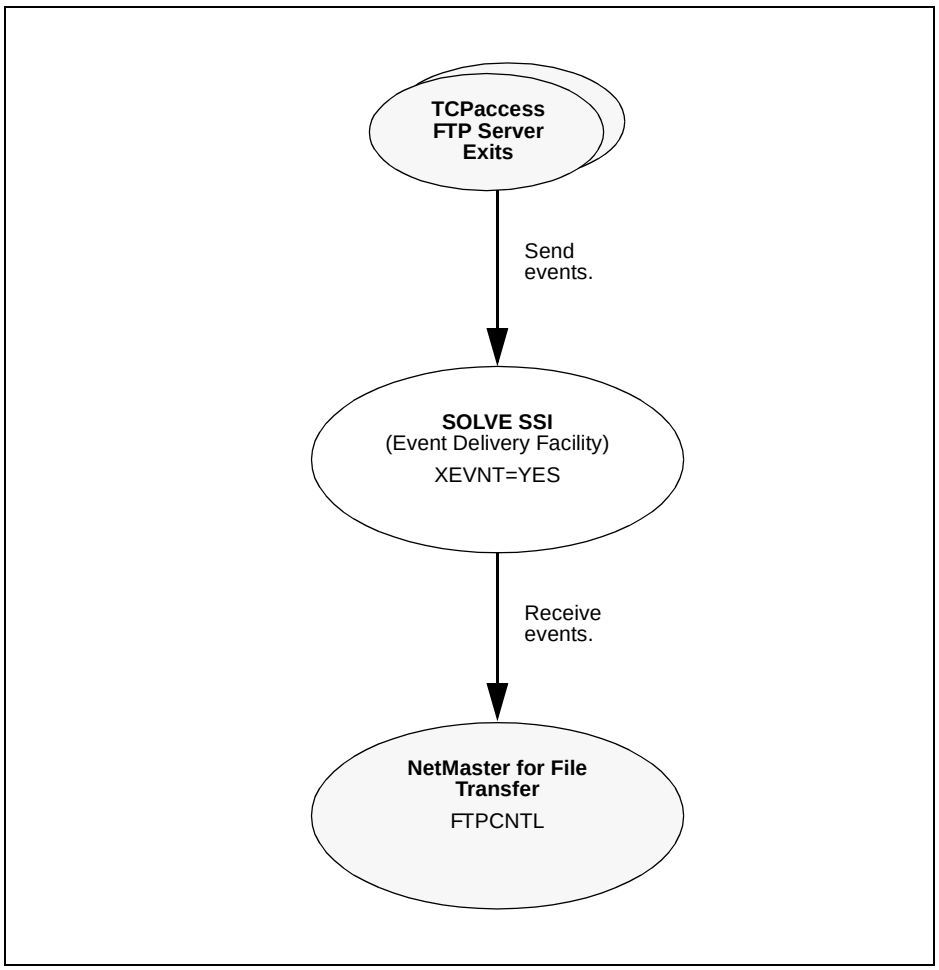
NetMaster for File Transfer provides an SMF exit, IPSMFEX. The exit forwards FTP events to a receiver by using the event delivery facility. NetMaster for File Transfer listens to that receiver for the events. The FTPCNTL parameter group controls whether that receiver is enabled.

The SOLVE subsystem interface (SSI) task that provides the event delivery facility is specified in the NetMaster for File Transfer SSI parameter group.

For information about how to implement the event flow, see the section, *Task 8—Implementing the FTP Event Flow,* on page 5-38.

Figure 3-12 shows the flow of events from the FTP server to NetMaster for File Transfer if you are using a TCPaccess FTP server.

Figure 3-12. Event Flow From an FTP Server to NetMaster for File Transfer Using TCPaccess FTP Server



The TCPaccess FTP server forwards FTP events to a receiver by using the event delivery facility. NetMaster for File Transfer listens to that receiver for the events. The FTPCNTL parameter group controls whether that receiver is enabled.

The SOLVE subsystem interface (SSI) task that provides the event delivery facility is specified in the NetMaster for File Transfer SSI parameter group.

The TCPaccess FTP server policy rule sets and rules enable you to control the use of FTP functions. A rule set containing the policy rules must be defined for your NetMaster for File Transfer region and loaded into your data space.

For information about how to implement the event flow, see the section, *Task 8—Implementing the FTP Event Flow*, on page 5-38. For information about TCPaccess FTP server policy rules, see Chapter 20, *Controlling the Use of FTP*.

4

Supporting File Transfer Resources

This chapter describes the knowledge base definitions that you create to manage the supporting file transfer resources, which include TCP/IP provider, DASD, and tapes.

The chapter contains the following topics:

- What Are the Supporting File Transfer Resources?
- The IBM TCP/IP Resource Definitions
- The TCPaccess Resource Definition
- The DASD and Tape Resource Definitions

What Are the Supporting File Transfer Resources?

The supporting file transfer resources are definitions in the knowledge base that help you manage the entities that provide the file transfer mechanisms and storage.

NetMaster for File Transfer can manage the following resources:

- IBM TCP/IP tasks
- TCPaccess tasks
- DASD
- Tapes

The IBM TCP/IP Resource Definitions

Communications Server provides the TCP/IP mechanism by which files can be transferred. NetMaster for File Transfer manages this TCP/IP started task through the information in the Communications Server resource definition.

Note

Communications Server refers to eNetwork Communications Server and OS/390 SecureWay Communications Server.

Communications Server Resource Templates

Templates are provided for defining Communications Server started task in the knowledge base. Each template contains the following information to help you manage a TCP/IP task:

- System commands that activate, inactivate, and retrieve status information about the tasks.
- System messages that change the actual state of the task. For messages that indicate a problem, you might want to include a NetMaster for File Transfer process that takes certain actions (for example, to record the problem in your problem management application).

The TCPaccess Resource Definition

TCPaccess is another product that can provide the TCP/IP mechanism by which files can be transferred. NetMaster for File Transfer manages a TCPaccess region through the information in the TCPaccess resource definition.

TCPaccess Resource Template

A template is provided for defining a TCPaccess started task in the knowledge base. The template contains the following information to help you manage a TCPaccess region:

- System commands that activate, inactivate, and retrieve status information about the TCPaccess region.
- System messages that change the actual state of the region. For messages that indicate a problem, you might want to include a NetMaster for File Transfer process that takes certain actions (for example, to record the problem in your problem management application).

Note

If TCPaccess is your FTP server, you may have defined an FTPMGR resource for your TCPaccess region. If so, it is not necessary to define a TCPaccess resource as well.

The DASD and Tape Resource Definitions

DASD and tapes provide storage for the files in a file transfer. NetMaster for File Transfer manages these resources through the information in the DASD and tape resource definitions.

DASD and Tape Resource Templates

Templates are provided for defining DASD and tape resources in the knowledge base. The templates contain the following information to help you manage a DASD or tape resource:

- System command that displays the status of the DASD or tape resource.
- System messages that change the actual state of the resource. For messages that indicate a problem, you might want to include a NetMaster for File Transfer process that takes certain actions (for example, to record the problem in your problem management application).

Part II

Implementation and Administration

5

Implementing the Product Region

To perform the tasks in this chapter, you must have completed the tasks in the *Unicenter Mainframe Installation and Setup Instructions* manual. This chapter describes the tasks you must complete to implement the NetMaster for File Transfer region.

The chapter contains the following topics:

- Task 1—Logging On for First-time Customization
- Task 2—Defining Resources to Your Region
- Task 3—Defining the Administrator
- Task 4—Implementing Your Template System
- Task 5—Implementing Printers
- Task 6—Implementing Logging
- Task 7—Customizing the Managed File Transfer Regions
- Task 8—Implementing the FTP Event Flow
- Task 9—Enabling the Interface Between NetMaster for File Transfer and TCP/IP
- Task 10—Implementing a SOLVE:Problem Automatic Problem Recording Environment
- Task 11—Implementing the Alert Monitor Problem Ticket Interface
- Task 12—Implementing Alert Forwarding
- Task 13—Implementing Event Recording and Reporting
- Task 14—Implementing the NetMaster Reporter Interface
- What to Do Next

Note

Unless indicated otherwise, when CONNECT:Direct is mentioned in these tasks, it means CONNECT:Direct for MVS or CONNECT:Direct for OS/390. For information about implementing the agents for monitoring CONNECT:Direct on distributed systems, see the *Unicenter NetMaster File Transfer Management Agent - CONNECT:Direct Installation and Administration Guide*.

Gather Information Now

During implementation you need to provide certain information. To streamline your tasks, gather the required information before you start. The form in Appendix G, *Form for Gathering Information Required During Implementation*, can help you gather the information.

Task 1—Logging On for First-time Customization

Note 1

Before proceeding with the tasks provided in this chapter, ensure that user IDs have been defined as specified in the *Unicenter Mainframe Installation and Setup Instructions*.

Note 2

If you have set up your NetMaster for File Transfer region using a pre-existing User ID Access Maintenance Subsystem (UAMS) database in which the background users are already defined for your region, you might not be able to action your changes during customization. If this is the case, you must update the background user definitions (see the section, *Security Considerations for Existing Users*, on page 6-7). Proceed as follows:

1. Enter **$UAMS** at the Command ===> prompt.
2. Update the background user definitions.
3. Exit back to the customization dialog, and continue the customization process.

As part of the installation and setup tasks, you should have defined an initial user in the NetMaster for File Transfer region.

To perform first time customization, log on to the region as that user as follows:

Step 1. Enter **LOGON APPLID(***acb-name***)**, using the ACB name of the region.

The logon panel is displayed.

Step 2. Enter the user ID and password. You are prompted to change your password.

Step 3. Change your password.

After your password is changed, the initial System Parameters Customization dialog is presented.

Step 4. Select the Fast Setup Customization Parameters option to review and customize the following parameter groups. These parameter groups *must* be updated before the System Parameters Customization dialog is complete:

- CDAPI (applicable only if you want to manage CONNECT:Direct and have included it in the RUNSYSIN member)
- CMAPI (applicable only if you want to manage CONNECT:Mailbox and have included it in the RUNSYSIN member)
- OPSYSIDS
- SOCKETS
- SYSTEMID

To customize a parameter group, proceed as follows:

a. Enter **U** beside it.

b. Press F3 (File) to indicate that you have reviewed the group.

If you update a group, you must press F6 (Action) to action the changes immediately, then press F3 (File) to save your changes to ensure that they are actioned on subsequent restarts of the region.

Review the parameter groups as follows:

- CDAPI—specify the user ID and password for signing on to CONNECT:Direct, and specify the CONNECT:Direct output and PROCESS files (see the section, *Specifying the CONNECT:Direct Interface Parameters*, on page 5-6).

  Note

  The CONNECT:Direct output file name defaults to the prefix defined for local VSAM files during the installation of NetMaster for File Transfer with DMPRINT as the suffix.

- CMAPI—specify the VSAM administration file to enable the region to retrieve help for CONNECT:Mailbox failure codes and messages.
- OPSYSIDS—if required, change the AOM subsystem ID to that assigned during setup. If the system uses the JES3 job entry subsystem, update the information about the job entry subsystem. For details on the AOM subsystem ID, see the *Unicenter Mainframe Installation and Setup Instructions*.

  Key Concept

  AOM is a subsystem interface that enables system message flow to the NetMaster for File Transfer region.

- SOCKETS—identify the TCP/IP software being used in your environment (see the section, *Implementing the TCP/IP Interface*, on page 5-11).
- SYSTEMID—you might want to change the title of the logon panel.

Step 5. When you finish with the parameter groups, press F3 (Exit) twice, to display the AutoAssist Setup panel.

Note

The region has other parameter groups that you can customize. To view the list of parameter groups, enter the **/ICS** shortcut at the ===> prompt. For a brief description of the parameter groups, see Table B-1 on page B-2.

You can now proceed to the next task (see the section, *Task 2—Defining Resources to Your Region*, on page 5-16). However, before doing so, review the following reference information:

- *Specifying the CONNECT:Direct Interface Parameters*, on page 5-6

  This section describes how to enable communication between NetMaster for File Transfer and CONNECT:Direct, by customizing the CDAPI parameter group.

- *Specifying the CONNECT:Mailbox Interface Parameters*, on page 5-10

  This section describes how to enable communication between NetMaster for File Transfer and CONNECT:Mailbox, by customizing the CMAPI parameter group.

- *Implementing the TCP/IP Interface*, on page 5-11

  This section describes how to implement the TCP/IP interface by customizing the SOCKETS parameter group.

- *Dealing with Initialization Failures*, on page 5-13

  This section provides initialization recovery information.

- *Generating an INI Procedure*, on page 5-15

  This section describes how to store parameter group records in sequential or partitioned datasets.

Specifying the CONNECT:Direct Interface Parameters

Caution

Each NetMaster for File Transfer region can only manage CONNECT:Direct applications of the same version. A NetMaster for File Transfer region cannot manage different versions of CONNECT:Direct at the same time.

You can, however, create separate regions to manage the different versions of CONNECT:Direct.

To enable communications between the NetMaster for File Transfer and the managed CONNECT:Direct regions, you must specify the following parameters in the CDAPI parameter group:

- User ID and password that allows the NetMaster for File Transfer region to sign on to the CONNECT:Direct regions.
- Dataset name of a work file that is used for CONNECT:Direct output (as defined by the DMPRINT DD name).
- Concatenation of CONNECT:Direct PROCESS files (as defined by the DMPUBLIB DD statements in the CONNECT:Direct startup JCL procedures).

Specify the parameters as follows:

Step 1. Enter the **/ICS** shortcut to display the list of parameter groups. (This step is not required when performing initial customization.)

Step 2. Enter **U** beside the CDAPI parameter group, under the NAMES category.

Step 3. Complete the fields as follows:

a. Ensure that the value in the Enable CONNECT:Direct Event Receiver field is YES to enable the region to collect CONNECT:Direct events.

b. Choose whether you want to use a different receiver ID or leave the CONNECT:Direct Event Receiver ID field at its default value.

This default value is used in the CONNECT:Direct statistics exit supplied by the NetMaster for File Transfer product. For information about how to implement the statistics exit, see the section, *Subtask 7.2.1—Implementing Statistics Exits in the Managed CONNECT:Direct Regions*, on page 5-29.

If, on the same system, you plan to implement one NetMaster region to manage one CONNECT:Direct region and another NetMaster region to manage a separate CONNECT:Direct region, ensure that you use a different event receiver ID for each SOLVE-CONNECT:Direct pair.

Note

If the region that manages a CONNECT:Direct region also manages a CA-XCOM region, a CONNECT:Mailbox region, and a TCPaccess FTP server, then you can do either of the following:

- Share the default event receiver ID between these regions.
- Use a specific event receiver ID for any combination of these regions. If you change the ID, then you must change it for each of these regions.

c. Enter the user ID and password, which allow signon to the CONNECT:Direct regions, in the CONNECT:Direct Background User ID and the CONNECT:Direct Background Password fields.

A possible user ID is that of one of the NetMaster for File Transfer background users, for example, *xxxx*BMON or *xxxx*BSYS.

Note

You can use the SHOW USERS command to find the ID of the background monitor. Enter **CMD** at the Command ===> prompt to access the Command Entry panel. Then, enter **SHOW USERS** to list the logged on users.

Key Concept 1

The user ID and password must be defined in all the CONNECT:Direct regions that are to be managed by this NetMaster for File Transfer region. You will need this user ID to complete *Subtask 7.2.3—Defining the NetMaster for File Transfer Region as a CONNECT:Direct User*, on page 5-32.

Key Concept 2

To enable automatic password update, the following conditions must be met:

- The user must be defined to the security product.
- The NetMaster for File Transfer region and the CONNECT:Direct regions must have security exits to the security product.
- The user must be defined to UAMS.

Warning

When the CDAPI User ID password is automatically updated, the new password will be unknown to the system administrator.

d. Choose whether you want the CDAPI User ID password to be automatically updated by the NetMaster for File Transfer region when the password expires. If you do not choose automatic update, you need to update the password manually and update the CDAPI parameter group with the new password.

e. Verify the dataset name of the work file in the CONNECT:Direct Output File field. The name is *dsnpref*.*rname*.DMPRINT, where *dsnpref* is the dataset prefix used during the installation of NetMaster for File Transfer and *rname* is the name of this NetMaster for File Transfer region.

f. Enter the dataset names of the PROCESS files that are used by the managed CONNECT:Direct regions in the CONNECT:Direct Process Libs fields (as defined by the DMPUBLIB DD statements in the CONNECT:Direct startup JCL procedures).

Figure 5-1 shows an example of the completed panel.

Figure 5-1. Specifying the CONNECT:Direct Interface Parameters

```
SOLVPROD-------------- ICS : Initialization Parameters -------------Page 1 of 1
Command ===>                                                  Function=Update

.- CDAPI - CONNECT:Direct Interface -----------------------------------------.
| Enable CONNECT:Direct Event Receiver . YES       (Default is YES)           |
| CONNECT:Direct Event Receiver ID ..... $RFFTEVR  (Default is $RFFTEVR)      |
| CONNECT:Direct Background User ID .... ALCDBMON                             |
| CONNECT:Direct Background Password ...           (This is not displayed)    |
| CONNECT:Direct Automatic Password .... NO_       (For Background User)      |
| CONNECT:Direct Output File ... ALSO0.SOLV17.DMPRINT_________________________ |
| CONNECT:Direct Process Libs... CD.ALCD1.PROCESS______________________________ |
|                             ... ____________________________________________ |
|                             ... ____________________________________________ |
|                             ... ____________________________________________ |
|                             ... ____________________________________________ |
'-----------------------------------------------------------------------------'
```

Step 4. When you have completed all the fields, press F6 (Action) to set the specified values.

Step 5. When the parameter group has completed its actions, press F3 (File) to save the specified values.

Specifying the CONNECT:Mailbox Interface Parameters

To enable communication between NetMaster for File Transfer and CONNECT:Mailbox you must specify the following parameters:

- CONNECT:Mailbox event receiver ID
- ISPF VSAM administration file

Specify the parameters as follows:

Step 1. Enter the **/ICS** shortcut to display the list of parameter groups. (This step is not required when performing initial customization.)

Step 2. Enter **U** beside the CMAPI parameter group, under the NAMES category.

Step 3. Complete the fields as follows:

a. Ensure that the value in the Enable CONNECT:Mailbox Event Receiver field is YES to enable the region to collect CONNECT:Mailbox events.

b. Choose whether you want to use a different receiver ID or leave the CONNECT:Mailbox Event Receiver ID field at its default value.

This default value is used in the CONNECT:Mailbox log exit supplied by the NetMaster for File Transfer product. For information about how to implement the log exit, see the section, *Subtask 7.3.1—Implementing the Log Exit in the Managed CONNECT:Mailbox Regions*, on page 5-35.

If, on the same system, you plan to implement one NetMaster region to manage one CONNECT:Mailbox region and another NetMaster region to manage a separate CONNECT:Mailbox region, ensure that you use a different event receiver ID for each NetMaster-CONNECT:Mailbox pair.

Note

If the region that manages a CONNECT:Mailbox region also manages a CA-XCOM region, a CONNECT:Direct region, and a TCPaccess FTP server, then you can do either of the following:

- Share the default event receiver ID between these regions.
- Use a specific event receiver ID for any combination of these regions. If you change the ID, then you must change it for each of the affected regions.

c. Enter the dataset name of the VSAM administration file. If this field is left blank, message help for CONNECT:Mailbox messages and codes will not be available.

Step 4. When you have completed all the fields, press F6 (Action) to set the specified values.

Step 5. When the parameter group has completed its actions, press F3 (File) to save the specified values.

Implementing the TCP/IP Interface

Implement the TCP/IP interface as follows:

Step 1. Enter the **/ICS** shortcut to display the list of parameter groups. (This step is not required when performing initial customization.)

Step 2. Enter **U** beside the SOCKETS parameter group, under the NAMES category.

The panel that specifies the type of TCP/IP software being used in your environment is displayed (see Figure 5-2 for an example). It also allows you to change the IP port number which this NetMaster for File Transfer region uses to listen for connection requests. The region needs a unique port number if you want to link the region with other SOLVE regions by using TCP/IP.

Figure 5-2. TCP/IP Software Type and Interface

```
SOLVPROD--------------- ICS : Initialization Parameters ------------Page 1 of 2
Command ===>                                                  Function=Update

.- SOCKETS - TCP/IP Sockets Interface ----------------------------------------.
|                                                                             |
| TCP/IP Software Type ......... IBM______ (IBM, TCPACCESS or NONE)           |
|                                                                             |
| Inbound Connections Port ..... 2636_     (NONE, 257 to 65535)               |
|                                                                             |
| Web Interface Port ........... NONE_     (NONE, 1 to 65535)                 |
| Web Access URL ..............                                               |
| Web User Timeout ............. 01.00     (hh.mm)                            |
|                                                                             |
| Retry Interval ..............            (Blank or time as hh.mm.ss)        |
```

Step 3. Tab to the TCP/IP Software Type input field, and enter the required value. Only one type of TCP/IP software can work with NetMaster for File Transfer on the same system.

Step 4. The Inbound Connections Port field contains a default port number. If another region on this system is already using that number, tab to the field and change it. *The port number must be unique on a system.*

Note

The default port number is 2636. This number is registered with the Internet Assigned Numbers Authority (IANA). For further information, see *ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers*.

Step 5. Press F8 (Forward) to review additional interface details. The details depend on whether you are using the IBM TCP/IP software or the TCPaccess software.

- Figure 5-3 shows the details for the IBM TCP/IP software. Review the details, and update as required.

Figure 5-3. TCP/IP Management Interface for IBM TCP/IP Software

```
SOLVPROD--------------- ICS : Initialization Parameters ------------Page 2 of 2
Command ===>                                                   Function=Update

.- SOCKETS - TCP/IP Sockets Interface ----------------------------------------.
|                                                                              |
| Interface Information:                                                       |
|   TCPIP.DATA DSN ............. TCPIP.DATA.PO(DATAD1)_______________________ |
|   Dataset Prefix ............. TCPIP                                        |
```

- Figure 5-4 shows the details for the TCPaccess software. Review the details, and update as required.

  If you are unsure of the TCPaccess subsystem ID, access the TCPaccess startup procedure and check the value of the subsystem name parameter (SSN).

Figure 5-4. TCP/IP Management Interface for TCPaccess Software

```
SOLVPROD--------------- ICS : Initialization Parameters ------------Page 2 of 2
Command ===>                                                   Function=Update

.- SOCKETS - TCP/IP Sockets Interface ----------------------------------------.
|                                                                              |
| Interface Information:                                                       |
|   TCPaccess SSID ............. ACSS     (Default is ACSS)                   |
|   TCPaccess Job Name .........                                               |
```

Step 6. When you have completed all the fields, press F6 (Action) to set the specified values and start the interface.

Step 7. When the parameter group has completed its actions, press F3 (File) to save the specified values.

You can check your TCP/IP implementation by entering the SHOW TCPIP command from a command entry panel.

TCP/IP Client Program Configuration Dataset

The TCPIP.DATA dataset name at your site might be called something like TCPIP.V3R2.TCPIP.DATA or SYS1.TCPPARMS(DATA). This dataset is what Communications Server refers to as the client configuration dataset. It contains information about how the sockets interface works with NetMaster for File Transfer (for example, how name lookup works). See the section, *Enabling Name Resolution*, on page 5-51 for further information about name lookup.

Dealing with Initialization Failures

If you log on to a region that has not completed initialization, the Initialization In Progress dialog is displayed to indicate progress and to assist you in identifying and rectifying any problems.

Fatal errors occur (for example, you are unable to log on) if either, or both, of the following are unavailable:

- Panel libraries
- Managed Object Development Services (MODS) control files

Key Concept

The MODS control files contain information that is required for the operation of the NetMaster for File Transfer region. The information includes menus, messages, and online help.

When you are performing customization, it is important to correctly identify all the relevant datasets. You must also ensure that the panel libraries and MODS control files created during installation contain the supplied panels and records.

You can identify the problems by referring to the job log for information related to the PANEL and MODS datasets.

Region startup is also inhibited if there are JCL errors or missing libraries in either your startup JCL or RUNSYSIN member.

Using the Initialization In Progress Dialog

The Initialization In Progress dialog shows you the current initialization status and whether actions associated with the parameter groups have failed.

The Initialization In Progress dialog enables you to:

- List only failed parameter groups
- List all outstanding parameter groups; that is, those that have failed, are queued to be applied, or are in the process of being applied
- List all parameter groups, including those that have run successfully
- View the messages in the initialization and customization log

The parameter group lists are dynamic action lists. You can apply the following actions to listed parameter groups:

Note

An action can only be performed against an already completed parameter group or a failed parameter group.

- **AC** (Action) to action a parameter group
- **H** (Help) to get help about a parameter group
- **I** (Ignore failure) to indicate to the region that it should ignore a failed parameter group and proceed to run dependent parameter groups

  Note

  Ignoring parameter groups is not recommended. It might affect the operation of the region. Consider carefully before applying this action.

- **L** (ILog) to view the messages, in the initialization and customization log, that relate to the selected parameter group
- **S**, ***l***, or **B** (Browse) to browse parameter group details
- **U** (Update) to update parameter group details

See the online help for additional information.

When you correct an error by updating an incorrect parameter group record, you have to action that parameter group before processing can continue (unless you apply the Ignore action). Action the parameter group in one of the following ways:

- By pressing F6 (Action) when you finish updating the parameter group
- By applying the **AC** (Action) action after you file the parameter group

Generating an INI Procedure

Parameter group records store information about parameters that have been changed by customization. Customized parameter group records are stored in the Virtual File Services (VFS) dataset.

Key Concept

The VFS dataset is a VSAM dataset. The NetMaster for File Transfer region uses this dataset for internal processing activities and as a general database.

If you want to store the information in the form of a partitioned dataset, you need to generate an INI procedure. You can use a generated INI procedure to propagate customized parameter group records to other regions (for example, from a test to a production region).

When you generate an INI procedure, the customized parameter group records are converted into procedural code, which is exported to the nominated partitioned or sequential dataset.

To generate an INI procedure, complete these steps:

Step 1. Enter the **/INIT.G** path to display the Generate INI Procedure panel.

Step 2. Enter the output dataset member name.

Step 3. Press F6 (Action) to generate the procedure. The generated procedure is displayed for you to review.

Step 4. Press F6 (Confirm) to save the procedure to the nominated output dataset.

Caution

You can edit an INI procedure by using an external package such as TSO/ISPF, but *only the customized values* contained in this procedure should be updated.

If updating, always create a backup member.

Using an INI Procedure to Propagate Customized Parameter Group Records to Other Regions

To propagate customized parameter group records to other regions:

- Ensure that the generated INI procedure is saved in a PDS that is allocated by the COMMANDS DD statements in the RUNSYSIN member.
- Specify the name of the member where the procedure is saved, as the value of the INIFILE parameter in your RUNSYSIN member.

Note

If a valid INI procedure is specified as the INIFILE parameter when system initialization occurs, the customization values contained in the nominated procedure override the customization values stored in the VFS dataset. The VFS dataset is also permanently updated to reflect the values specified in the INI procedure.

Note

If you use an initialization INI procedure to start up your region and you changed the settings of a parameter group, you must regenerate the procedure if you want the changes applied at subsequent startups of the region.

Task 2—Defining Resources to Your Region

Note

This task partially builds your file transfer management environment. If you wish, you can skip this task and proceed to the next task (see the section, *Task 3—Defining the Administrator*, on page 5-18) to continue implementing your NetMaster for File Transfer region.

To build your file transfer management environment after you have implemented your region, see Chapter 10, *Building the Environment to Manage Your File Transfer Services.*

If you are using NetMaster for File Transfer for the first time, we recommend that you utilize the File Transfer Assisted Resource Definition Facility.

The Assisted Resource Definition Facility also provides default parameter values which determine how and when automation will operate.

To access the Assisted Resource Definition Facility, proceed as follows:

Step 1. At the AutoAssist Setup panel, enter **S** beside the File Transfer Assisted Resource Definition option, as shown in Figure 5-5.

Note

If you are using a model 2 screen, you will need to press F8 to scroll forward before you can select the File Transfer Assisted Resource Definition option.

Figure 5-5. Selecting the Resource Definition Option

```
SOLVPROD------- NetMaster for File Transfer : AutoAssist Setup -----Page 2 of 2
Command ===>



                 .-------------------------------------------.
              ___ | File Transfer Assisted Resource Definition |
                 '-------------------------------------------'
```

The Assisted Resource Definition panel is displayed.

Note

If you have exited the initial System Parameters Customization dialog, you will not see the option in Figure 5-5. To access the Assisted Resource Definition Facility, enter the **/RADMIN.AD** path.

Step 2. Define the file transfer resources. For more information about how to define resources, see the following sections:

To define …	**See the section,**
CA-XCOM resources	*Defining CA-XCOM Resources*, on page 10-24
CONNECT:Direct resources	*Defining CONNECT:Direct Resources*, on page 10-29
CONNECT:Mailbox resources	*Defining CONNECT:Mailbox Resources*, on page 10-38
FTS resources	*Defining FTS Resources*, on page 10-40
FTP resources	*Defining FTP Resources*, on page 10-43
DASD and tape resources	*Auto-populating a System Image with DASD and Tape Resource Definitions*, on page 10-51

Note

When you have completed the implementation and administrative tasks described in Part II, *Implementation and Administration*, you should complete the building of your file transfer management environment (see Chapter 10, *Building the Environment to Manage Your File Transfer Services*).

You can now proceed to the next task (see the next section, *Task 3—Defining the Administrator*).

Task 3—Defining the Administrator

Change the security details of the initial user to that of an administrator, which you will use for subsequent logons, as follows:

Note

If you are using a pre-existing UAMS database, see the section, *Security Considerations for Existing Users*, on page 6-7 for considerations.

Step 1. Enter the **/ASADMIN.UP** path to display the User Profile List panel.

Step 2. Press F4 (Add) to add a new user profile. The action presents you with the first panel in the user profile definition, the User Description panel.

Step 3. Enter the ID of the initial user. The panel is refreshed with the existing information about the user.

Step 4. Enter $RMADMIN in the Group ID field to give the user administrative authority.

Step 5. Press F3 (File) to save the record.

Step 6. Enter **CMD** at the Command ===> prompt, then enter **SIGNON** on the displayed Command Entry panel to make the changes immediately available to the current user.

You can now proceed to the next task (see the section, *Task 4—Implementing Your Template System*, on page 5-19).

You can use a similar procedure to define other users (see the section, *Defining NetMaster for File Transfer Users*, on page 6-9).

Task 4—Implementing Your Template System

Templates are defined in a $TEMPLAT system image. The distributed templates are in the image, $TEMPLAT version 0001.

Copy the distributed templates to a different $TEMPLAT version. Start with version 0010. Versions 0001 through 0009 are reserved for distributed templates. By creating a copy of the image, you can, if required, customize it to suit your requirements without disturbing the distributed image.

Copy the distributed $TEMPLAT system image as follows:

Step 1. Enter the **/RADMIN.T.I** path to access the list of $TEMPLAT system images. The System Image List panel is displayed.

Step 2. Enter **C** beside $TEMPLAT 0001. The System Image Definition panel is displayed (see Figure 5-6).

Figure 5-6. Making a Copy of the Distributed Templates

```
SOLVPROD------------ ResourceView : System Image Definition -------------------
Command ===>                                                     Function=COPY


System Name ......... $TEMPLAT
Database Version .... 0001 ——— Change version number to 10 or above.
```

Step 3. Change the value in the Database Version field to uniquely identify the new copy (for example, 0010), and update the description fields as required.

Step 4. Press F3 (File) to start the copying process. The System Image Copy panel is displayed on your screen to advise you of the status of the copying process. When the copying process is complete, the System Image List panel is redisplayed.

Step 5. Make this new copy of the template system image available for use as follows:

a. Enter the **/ICS** shortcut to access the list of parameter groups.

b. Enter **U** beside the OPSYSIDS parameter group under the NAMES category.

c. Enter the version number of the image in Template System Image Version field.

d. Press F6 (Action) to make the image available for use.

e. Press F3 (File) to save the changed value, insuring that the image is made available automatically the next time the region starts up.

You can now proceed to the next task (see the section, *Task 5—Implementing Printers*, on page 5-20).

Task 5—Implementing Printers

To enable printing from the NetMaster for File Transfer region, you need to define printers to it. You also need to define the forms the printers use.

Determine your printing requirements, then proceed as follows. (If you require more information about how to complete the panels in the following steps, see the online help.)

Step 1. Enter the **/PSM** shortcut to display the primary menu of the Print Services Manager (PSM).

Step 2. Define the forms to be used by your printers:

a. Enter **F.A** to display the Form Definition panel.
b. Define a form.
c. Save the form definition:

If you …	**Press …**
Want to define an additional form	F4 (Save) to keep the Form Definition panel open. Then repeat Step b.
Have finished defining all the required forms	F3 (File) to exit to the Form Definition menu.

Step 3. From the Form Definition menu, press F3 (Exit) to return to the PSM primary menu.

Step 4. Define the printers:

a. Enter **P.A** to display the Printer Definition panel.
b. Define a printer.
c. Save the printer definition. Repeat Step b for additional printers.

You can now proceed to the next task (see the section, *Subtask 6.1—Implementing File Transfer Logging*, on page 5-22).

Task 6—Implementing Logging

The NetMaster for File Transfer product provides file transfer and activity logs:

- File transfer logs record CA-XCOM, CONNECT:Direct, CONNECT:Mailbox, FTP, and FTS messages.
- Activity logs record SOLVE and system events.

To implement logging, perform the following subtasks:

- Subtask 6.1—Implementing File Transfer Logging
- Subtask 6.2—Customizing Activity Log Settings, if required
- Subtask 6.3—Enabling File Transfer Schedule Logging, if required

Subtask 6.1—Implementing File Transfer Logging

Implement file transfer logging as follows:

1. Allocate file transfer log files. (You do not need to perform this step if you are happy with three log files, which is the default.)
2. Enable the event flow as follows:

If you want to manage the file transfer service provided by …	**You should …**
CA-XCOM regions	Customize them as described in the section, *Subtask 7.1—Customizing the Managed CA-XCOM Regions*, on page 5-28.
CONNECT:Direct regions	Implement the NetMaster for File Transfer statistics exit in each of the regions as described in the section, *Subtask 7.2.1—Implementing Statistics Exits in the Managed CONNECT:Direct Regions*, on page 5-29.
CONNECT:Mailbox regions	Customize them as described in the section, *Subtask 7.3—Customizing the Managed CONNECT:Mailbox Regions*, on page 5-34.
FTS regions	Customize them as described in the section, *Subtask 7.4—Customizing the Managed FTS Regions*, on page 5-36.
FTP	Implement the flow of FTP events as described in the section, *Task 8—Implementing the FTP Event Flow*, on page 5-38.

If you want to disable file transfer logging after you have implemented it, see the section, *Disabling File Transfer Logging*, on page 5-24.

Allocating File Transfer Log Files

During initialization, the region is allocated three file transfer log files. However, you can allocate up to seven files.

Note

The log file IDs are of the form RFTLOG*nn* and the dataset names are of the form *dsnpref.rname*.RFTLOG*nn*. (*dsnpref* is the dataset prefix used during the installation of the NetMaster for File Transfer product and *rname* is the name of the region.)

If you want to make more than three files available to the region, customize the FTLOGS parameter group as follows:

Step 1. Define additional logging data sets.

Step 2. Enter the **/ICS** shortcut to display the list of parameter groups.

Step 3. Enter **U** beside the FTLOGS parameter group. The Initialization Parameters panel is displayed (see Figure 5-7).

Figure 5-7. The File Transfer Log Parameter Group

```
SOLVPROD-------------- ICS : Initialization Parameters -------------Page 1 of 3
Command ===>                                                  Function=Update

.- FTLOGS - Log File Specifications -----------------------------------------.
|                                                                            |
| Is logging required? ......... YES       (default is YES)                  |
|                                                                            |
| Log File ID 1 ................ RFTLOG01  (default is RFTLOG01)             |
|   Log Dataset Name 1 ......... ALSO0.SOLV17.RFTLOG01_______________________ |
|                                (default is AUDE0.DENM13.RFTLOG01)          |
|   File Disposition 1 ........+ SHR  (default is SHR)                       |
|   Log File VSAM Options 1 ...+ LSR SIS DEFER_______________________________ |
|                                (default is LSR SIS DEFER)                  |
|                                                                            |
'----------------------------------------------------------------------------'
```

Step 4. From the displayed Initialization Parameters panel, press F8 (Forward) to display the next panel.

Step 5. Complete the fields for each file you want to make available. Figure 5-8 shows an example.

Figure 5-8. Allocating a File Transfer Log File

```
SOLVPROD-------------- ICS : Initialization Parameters -------------Page 2 of 3
Command ===>                                                  Function=Update

.- FTLOGS - Log File Specifications -----------------------------------------.
|                                                                            |
| Log File ID 2 ................ RFTLOG02                                  |
|   Log File Dataset Name 2 .... ALSO0.SOLV17.RFTLOG02_______________________ |
|   File Disposition 2 ........+ SHR                                         |
|   Log File VSAM Options 2 ...+ LSR SIS DEFER_______________________________ |
|                                                                            |
| Log File ID 3 ................ RFTLOG03                                  |
|   Log File Dataset Name 3 .... ALSO00.SOLV17.RFTLOG03______________________ |
|   File Disposition 3 ........+ SHR                                         |
|   Log File VSAM Options 3 ...+ LSR SIS DEFER_______________________________ |
|                                                                            |
| Log File ID 4 ................ RFTLOG04                                  |
|   Log File Dataset Name 4 .... ALSO00.SOLV17.RFTLOG04______________________ |
|   File Disposition 4 ........+ SHR                                         |
|   Log File VSAM Options 4 ...+ LSR SIS DEFER_______________________________ |
```

Step 6. To allocate more files, press F8 (Forward) again.

Step 7. When you have specified the required number of log files, press F6 (Action) to allocate and open the files.

Step 8. When the parameter group has completed its actions, press F3 (File) to save the changed information.

Note

For file transfer logs, you can suppress the logging of certain types of CONNECT:Direct for MVS or CONNECT:Direct for OS/390 event messages. You specify the suppression parameters in the CDEVENTS parameter group.

You can now proceed to the next task (see the section, *Task 7—Customizing the Managed File Transfer Regions*, on page 5-27).

Disabling File Transfer Logging

If you want to disable file transfer logging, change the value of the Is logging required? field of the FTLOGS parameter group to **NO** and action the group.

Subtask 6.2—Customizing Activity Log Settings

By customizing the LOGFILES parameter group, you can:

- Control the logging of operating system messages or commands.
- Allocate additional activity log files.

To customize the LOGFILES parameter group, proceed as follows:

Step 1. Enter the **/ICS** shortcut to display the list of parameter groups.

Step 2. Enter **U** beside the LOGFILES parameter group.

Step 3. Complete the required fields (see the following sections, *Controlling Operating System Message or Command Logging* and *Allocating Activity Log Files*).

Step 4. When you have specified the required values, press F6 (Action) to activate the new settings.

Step 5. When the parameter group has completed its actions, press F3 (File) to save the changed information.

Controlling Operating System Message or Command Logging

By default, system messages and commands received by the region are suppressed from the activity log:

If you want to enable system …	Set the value in the …
Message logging	Log Operating System Messages? field to **YES**.
Command logging	Log Commands? field to **YES**.

Allocating Activity Log Files

During initialization, the region is allocated three activity log files. However, you can allocate up to seven files.

Note

As supplied, the log file IDs and dataset names are respectively NMLOG*nn* and *dsnpref*.*rname*.NMLOG*nn*. (*dsnpref* is the dataset prefix used during the installation of the NetMaster for File Transfer product and *rname* is the name of the region.)

To make more than three files available to the region, proceed as follows:

Step 1. Define additional logging data sets.

Step 2. After the first Initialization Parameters panel is displayed, press F8 (Forward) to display the next panel.

Step 3. Complete the fields for each file you want to make available. Figure 5-9 shows an example.

Figure 5-9. Allocating an Activity Log File

```
.- LOGFILES - Log File Specifications ----------------------------------------.
|                                                                             |
| Log File ID 2 ................ NMLOG02_                                  |
|   Log File Dataset Name 2 .... ALSO00.SOLV17.NMLOG02_______________________ |
|   File Disposition 2 ........+ SHR                                          |
|   Log File VSAM Options 2 ...+ LSR SIS DEFER________________________________ |
|                                                                             |
| Log File ID 3 ................ NMLOG03_                                  |
|   Log File Dataset Name 3 .... ALSO00.SOLV17.NMLOG03_______________________ |
|   File Disposition 3 ........+ SHR                                          |
|   Log File VSAM Options 3 ...+ LSR SIS DEFER________________________________ |
|                                                                             |
| Log File ID 4 ................ NMLOG04_                                  |
|   Log File Dataset Name 4 .... ALSO00.SOLV17.NMLOG04_______________________ |
|   File Disposition 4 ........+ SHR                                          |
|   Log File VSAM Options 4 ...+ LSR SIS DEFER________________________________ |
```

Step 4. To allocate more files, press F8 (Forward) again.

Subtask 6.3—Enabling File Transfer Schedule Logging

By logging file transfer schedule events you can retain active schedule details across a system outage or when a new system image is loaded.

To enable the logging of file transfer schedule events, proceed as follows:

Step 1. Enter the **/ICS** shortcut to display the list of parameter groups.

Step 2. Enter **U** beside the FTSCHD parameter group. The Initialization Parameters panel is displayed (see Figure 5-10).

Figure 5-10. The Schedule File Specifications Parameter Group

```
SOLVPROD------------- ICS : Initialization Parameters --------------Page 1 of 1
Command ===>                                                  Function=Update

.- FTSCHD - Schedule File Specifications -------------------------------------.
|                                                                              |
| Enable Schedule Logging? ..... YES                                           |
| File ID ...................... RFTSCHD                                     |
| Dataset Name ................. ALSO0.SOLV17.RFTSCHD_______________________  |
| Delete File Records? ......... YES                                           |
|                                                                              |
'------------------------------------------------------------------------------'


.- Notes ---------------------------------------------------------------------.
| This file is used to save non-ended schedule details and to reload them     |
| after a system outage or an IPL. The contents of the file will be           |
| cleared when disabling this function if Delete File Records? is set to      |
| YES.                                                                         |
'------------------------------------------------------------------------------'
```

Step 3. Complete the required fields.

Step 4. When you have specified the required values, press F6 (Action) to activate the new settings.

Step 5. When the parameter group has completed its actions, press F3 (File) to save the changed information.

Task 7—Customizing the Managed File Transfer Regions

NetMaster for File Transfer can manage the following file transfer services:

If you want to manage …	See …
A CA-XCOM region	*Subtask 7.1—Customizing the Managed CA-XCOM Regions*, on page 5-28.
A CONNECT:Direct region	*Subtask 7.2—Customizing the Managed CONNECT:Direct Regions*, on page 5-29.
A CONNECT:Mailbox region	*Subtask 7.3—Customizing the Managed CONNECT:Mailbox Regions*, on page 5-34.
An FTS region	*Subtask 7.4—Customizing the Managed FTS Regions*, on page 5-36.
A TCPaccess FTP server	*Subtask 8.3—Customizing FTPCNTL Parameter Group (Non-TCPaccess FTP)*, on page 5-42

Note

If you want to manage FTP file transfers, you need to implement the FTP event flow (see *Task 8—Implementing the FTP Event Flow*, on page 5-38).

Subtask 7.1—Customizing the Managed CA-XCOM Regions

Warning

This subtask requires you to apply user modification (USERMOD) in the CA-XCOM region. *Ensure that the region is at the required version and maintenance level* (see the *Unicenter Mainframe Installation and Setup Instructions*).

Note

Besides performing the tasks here to implement the flow of CA-XCOM events, you also need to ensure that the SOLVE SSI event delivery facility is available to the region. The facility requires the following:

- Started task member for a SOLVE SSI includes the JCL parameter, XEVNT=YES. (This should have been done during region setup. See the *Unicenter Mainframe Installation and Setup Instructions*.)
- SSI parameter group specifies the subsystem ID of the above SOLVE SSI started task (see Step 4, on page 5-3, in the section, *Task 1—Logging On for First-time Customization*).

To customize a CA-XCOM region to work with NetMaster for File Transfer, perform the following steps:

Step 1. Ensure that the values of the following parameters in the CA-XCOM Default Options Table are as indicated:

```
NETMAST=YES,
RECVRID=xcom-event-receiver-id
```

The value of the RECVRID parameter must match the CA-XCOM event receiver ID specified in the NetMaster XCAPI parameter group. If the parameter is not specified, it assumes the value $RFFTEVR.

You should also use a low value for the ERRINTV parameter to ensure that accurate transfer request status is displayed on the monitors. Either let the parameter default or use a lower value.

Step 2. If you make changes to the default parameters, you must reassemble and link the Default Options Table.

Step 3. Copy the *dsnpref*.FT500.FTSAMP(XCUSRMOD) job member to the *dsnpref.rname*.TESTEXEC data set, where *dsnpref* is the data set prefix used during the installation of the product and *rname* is the name of the NetMaster for File Transfer region. The job applies user modification (USERMOD) to include the NetMaster for File Transfer exit in the CA-XCOM region.

Step 4. Review the comments in the copy, and update the variables that start with the question mark (?).

Step 5. Submit the customized job.

Step 6. Restart the CA-XCOM region.

Subtask 7.2—Customizing the Managed CONNECT:Direct Regions

Note

Besides performing the tasks here to implement the flow of CONNECT:Direct events, you also need to ensure that the SOLVE SSI event delivery facility is available to the region. The facility requires the following:

- Started task member for a SOLVE SSI includes the JCL parameter, XEVNT=YES. (This should have been done during region setup. See the *Unicenter Mainframe Installation and Setup Instructions*.)
- SSI parameter group specifies the subsystem ID of the above SOLVE SSI started task (see Step 4, on page 5-3, in the section, *Task 1—Logging On for First-time Customization*).

To customize a CONNECT:Direct region to work with NetMaster for File Transfer, perform the following subtasks.

Subtask 7.2.1—Implementing Statistics Exits in the Managed CONNECT:Direct Regions

Note

TheNetMaster for File Transfer statistics exit in each managed CONNECT:Direct region must be current for the version of NetMaster for File Transfer you are running. For example, if you are upgrading from SOLVE:Operations for File Transfer 2.2 to NetMaster for File Transfer 5.0, you must update the statistics exit in the CONNECT:Direct regions.

Implement the NetMaster for File Transfer statistics exit in each of the managed CONNECT:Direct regions as follows:

Step 1. Include the supplied APF-authorized FTLOAD library in the STEPLIB DD statements of the CONNECT:Direct startup JCL procedure. (The library should have been set up as *dsnpref*.FT500.FTLOAD, where *dsnpref* is the data set prefix used during the installation of the NetMaster for File Transfer product.)

Step 2. Check the following CONNECT:Direct initialization parameters:

If the value of ALLOC.STORAGE is ABOVE, STATISTICS.EXIT is not specified, and STAT.EXCLUDE is not specified, proceed to Step 5. Otherwise proceed to Step 3.

Step 3. Depending on your current CONNECT:Direct setup, you might need to copy the *dsnpref*.FT500.FTSAMP(NMCDSTEX) statistics exit to the *dsnpref.rname*.TESTEXEC data set and update the following statement:

```
$RFCDSTX AMODE=31,USREXIT=NONE,EPSRCVR=$RFFTEVR,
EXCLUDE=NONE
```

If you …	**You need to …**
Have specified BELOW for the CONNECT:Direct initialization parameter, ALLOC.STORAGE	Specify **AMODE=24** to indicate 24-bit addressing mode.
Are already using a CONNECT:Direct statistics exit	Specify the load module name of your exit in the USREXIT parameter.
Are excluding records from the CONNECT:Direct statistics file	Copy the list of excluded record types to the EXCLUDE parameter and remove STAT.EXCLUDE from the CONNECT:Direct initialization parameter.

Ensure that the value of the EPSRCVR parameter matches the CONNECT:Direct event receiver ID specified in the CDAPI parameter group.

Note

The NMCDSTEX member also contains comments that provide additional background information.

Step 4. If you updated the NMCDSTEX statistics exit, proceed as follows:

a. Copy the ASMCDSTX job from the *dsnpref*.FT500.FTSAMP library to the *dsnpref.rname*.JCL library.

b. Customize the ASMCDSTX job in the *dsnpref.rname*.JCL library, following the instructions provided by the comments in the file.

c. Submit the customized job to assemble and link-edit the exit.

Step 5. Change the value of the CONNECT:Direct initialization parameter, STATISTICS.EXIT, to **NMCDSTEX**.

NMCDSTEX is the default statistics exit name. The statistics exit name you specify must match the exit name specified in the ASMCDSTX job. If you are monitoring multiple CONNECT:Direct regions you need a unique statistics exit name and receiver ID for each CONNECT:Direct region.

You need to restart the CONNECT:Direct region to bring into effect the changes to the startup JCL procedure and the STATISTICS.EXIT initialization parameter. However, you might want to wait until you have updated one other initialization parameter as indicated in the next section, *Subtask 7.2.2—Customizing CONNECT:Direct Initialization Parameters.*

Subtask 7.2.2—Customizing CONNECT:Direct Initialization Parameters

Note

Your NetMaster for File Transfer region uses the CONNECT:Direct interface program, DMCHLAPI, to interface with a CONNECT:Direct region and must sign on to that region.

Because CONNECT:Direct places limits on the number of batch users that may be signed on concurrently, you should increase this limit to allow the extra NetMaster for File Transfer signon.

Customize each managed CONNECT:Direct region as follows:

Step 1. Increase the value of the MAXBATCH or the MAXUSERS initialization parameter to accommodate NetMaster for File Transfer.

If the current value of MAXBATCH is …	Add 1 to the value of …
Zero	MAXUSERS.
Not zero	MAXBATCH.

Step 2. Ensure that the CONNECT:Direct startup JCL procedure and the STATISTICS.EXIT initialization parameter are updated (see the section, *Subtask 7.2.1—Implementing Statistics Exits in the Managed CONNECT:Direct Regions*, on page 5-29).

Step 3. Restart the CONNECT:Direct region.

You can now continue on to define the NetMaster for File Transfer region as a CONNECT:Direct user (see the section, *Subtask 7.2.3—Defining the NetMaster for File Transfer Region as a CONNECT:Direct User*, on page 5-32).

Subtask 7.2.3—Defining the NetMaster for File Transfer Region as a CONNECT:Direct User

To enable the NetMaster for File Transfer region to execute commands in the managed CONNECT:Direct regions, define it as a user in each of the CONNECT:Direct regions. Use the user ID and password specified in the NetMaster for File Transfer parameter group, CDAPI.

Ensure that the defined user is authorized for the following functions:

- Change, delete, flush, select, and suspend processes
- Select the network map
- Other functions that you want to be able to perform from the NetMaster for File Transfer region

For example, with CONNECT:Direct for MVS or CONNECT:Direct for OS/390, you can use the following suggestion when specifying the authority of a user:

```
CHANGE=Y
DELPR=Y
FLUSH=Y
SELNET=Y
SELPR=Y
SELSTAT=Y
SUBMITTER.CMDS=(Y Y Y Y Y)
```

For more information about how to specify the authority of a CONNECT:Direct user, see the *CONNECT:Direct for MVS Installation and Administration Guide* or the *CONNECT:Direct for OS/390 Installation and Administration Guide.*

Customizing the $RFXPRMS NCL Procedure

NetMaster for File Transfer uses the INQUIRE INITPARMS command to derive the NETMAP and MSGFIL data set names, and the TCP/IP port number that CONNECT:Direct is using. For this to work, you require the CONNECT:Direct for MVS or CONNECT:Direct for OS/390 operator interface, which requires an MCS user ID. If you do not have a CONNECT:Direct MCS user ID, you need to customize the $RFXPRMS NCL procedure:

Step 1. Copy the $RFXPRMS NCL procedure from *dsnpref*.FT500.FTTEXEC to *dsnpref.rname*.TESTEXEC in the NetMaster for File Transfer region.

Note

The FTTEXEC and TESTEXEC data sets are prefixed with *dsnpref*.FT500 and *dsnpref.rname* respectively, where *dsnpref* is the data set prefix specified during the installation of the NetMaster for File Transfer product, and *rname* is the name of the region.

Step 2. Customize the $RFXPRMS NCL procedure to specify the following information of each CONNECT:Direct resource:

- *Manager resource name*—specifies the name of the manager resource defined for each CONNECT:Direct application. Specify the CONNECT:Direct Node Name.
- *NETMAP DSN*—specifies the data set names in which the network map of the CONNECT:Direct application is located.
- *MSGFIL DSNs*—the data set name in which the message file of the CONNECT:Direct application is located.
- *IBM TCP/IP Address*—the IBM TCP/IP address specified in the manager resource defined for CONNECT:Direct for OS/390 only.
- *Port number*—specifies the port number the CONNECT:Direct application uses for TCP/IP access.

For details on how to customize the $RFXPRMS NCL procedure read the comments provided in the file.

Caution

When you upgrade your version of CONNECT:Direct, ensure that you perform either of the following:

- Remove its definition from the $RFXPRMS procedure.
- Update the $RFXPRMS procedure to reflect the upgraded version.

Subtask 7.3—Customizing the Managed CONNECT:Mailbox Regions

Note

Besides performing the tasks here to implement the flow of CONNECT:Mailbox events, you also need to ensure that the SOLVE SSI event delivery facility is available to the region. The facility requires the following:

- Started task member for a SOLVE SSI includes the JCL parameter, XEVNT=YES. (This should have been done during region setup. See the *Unicenter Mainframe Installation and Setup Instructions*.)
- SSI parameter group specifies the subsystem ID of the above SOLVE SSI started task (see Step 4, on page 5-3, in the section, *Task 1—Logging On for First-time Customization*).

To customize a CONNECT:Mailbox region to work with NetMaster for File Transfer, perform the following subtasks.

Subtask 7.3.1—Implementing the Log Exit in the Managed CONNECT:Mailbox Regions

Implement the CONNECT:Mailbox log exit in each of the managed CONNECT:Mailbox regions as follows:

Step 1. Include the supplied APF-authorized FTLOAD library in the STEPLIB DD statements of the CONNECT:Mailbox startup JCL procedure. (The library should have been set up as *dsnpref*.FT500.FTLOAD, where *dsnpref* is the data set prefix used during the installation of the NetMaster for File Transfer product.)

Step 2. Complete the following steps if:

- You are already using a log exit.
- The default EPS receiver ID is not suitable.

Copy the *dsnpref*.FT500.FTSAMP(NMCMLGEX) log exit to the *dsnpref.rname*.TESTEXEC and update the following parameters:

Update …	**If …**
`USREXIT=`*`userexit`*	You want to use an existing log exit
`EPSRCVR=`*`newid`*	The default receiver ID is not suitable

Ensure that the value of the EPSRCVR parameter matches the CONNECT:Mailbox event receiver ID specified in the CMAPI parameter group.

Step 3. If you updated the NMCMLGEX log exit in Step 2, proceed as follows:

a. Copy the ASMCMLGX job from the *dsnpref*.FT500.FTSAMP library to the *dsnpref.rname*.JCL library.

b. Customize the ASMCMLGX job in the *dsnpref.rname*.JCL library, following the instructions provided by the comments in the file.

c. Submit the customized job to assemble and link-edit the exit.

Subtask 7.3.2—Customizing CONNECT:Mailbox Initialization Parameters

To enable the NetMaster for File Transfer region to execute commands and retrieve messages in the managed CONNECT:Mailbox regions, specify the following *OPTIONS definitions in the CONNECT:Mailbox ODF file:

```
MODIFY=RESP
XLOG=NMCMLGEX
```

NMCMLGEX is the default log exit. The log exit name you specify in the ODF file must match the exit name specified in the ASMCMLGX job.

Subtask 7.4—Customizing the Managed FTS Regions

To customize an FTS region to work with NetMaster for File Transfer, perform the following subtasks.

Subtask 7.4.1—Defining the Link to the NetMaster for File Transfer Region

The NetMaster for File Transfer and FTS regions communicate by using an INMC link. In each managed FTS region, define a link to the NetMaster for File Transfer region as follows:

Step 1. Log on to the FTS region, and select Operator Console Services.

Step 2. Enter the following DEFLINK command to enable the dynamic creation of an INMC link:

`DEFLINK LUNAME=`*`acb-name`* `LINK=`*`link-name`*

acb-name is the ACB name of the NetMaster for File Transfer region to which the FTS region is to establish a link, and *link-name* is a name that identifies the link.

Step 3. Enter **SHOW LINK=DYNAMIC** to check that the allowed number of dynamic links will not be exceeded. You can increase the number by issuing the following command:

`SYSPARMS DYNLMAX=`*`number`*

number sets the number of allowed dynamic links.

Step 4. Ensure that the DEFLINK and the SYSPARMS commands are included in the NMREADY procedure for the FTS region to enable the automatic execution of the commands during region startup.

Subtask 7.4.2—Defining the NetMaster for File Transfer Region as an FTS User

To enable the NetMaster for File Transfer region to execute commands in the managed FTS regions, define its BSYS background user in each of the FTS regions by copying its user ID definition, *xxxx*BSYS.

Note

You can use the SHOW USERS command to find the ID of the BSYS background user. In the NetMaster for File Transfer region, enter **CMD** at a ===> prompt to access the Command Entry panel. Then, enter **SHOW USERS** to list the users who are currently logged on to the region.

Subtask 7.4.3—Installing the FTS Message Handler

The FTS message handler, $RFAGENT, processes FTS events before they are sent to the NetMaster for File Transfer region.

To install the handler, copy it from the *dsnpref*.FT500.FTTEXEC data set to the NCL procedures library (normally TESTEXEC) in the FTS region. (*dsnpref* is the data set prefix used during the installation of the NetMaster for File Transfer product.)

Note

The $RFAGENT message handler must be present in each FTS region that you want to monitor.

Task 8—Implementing the FTP Event Flow

Before you can manage FTP transfers, you need to implement the flow of FTP events to your region.

Note

Besides performing the tasks here to implement the flow of FTP events, you also need to ensure that the SOLVE SSI event delivery facility is available to the region. The facility requires the following:

- Started task member for a SOLVE SSI includes the JCL parameter, XEVNT=YES. (This should have been done during region setup. See the *Unicenter Mainframe Installation and Setup Instructions*.)
- SSI parameter group specifies the subsystem ID of the above SOLVE SSI started task (see Step 4, on page 5-3, in the section, *Task 1—Logging On for First-time Customization*).

Implementing the FTP event flow requires different subtasks, depending on whether you are licensed for using the TCPaccess FTP server. To implement the FTP event flow, perform the following subtasks:

If you are …	**You must …**
Not licensed	Set up TCP/IP to generate SMF records (see *Subtask 8.1—Setting Up TCP/IP to Generate SMF Records*, on page 5-39).
	Implement the SMF exit for the FTP receiver (see *Subtask 8.2—Implementing the SMF Exit for the FTP Receiver*, on page 5-42).
	Customize the FTPCNTL parameter group (see *Subtask 8.3—Customizing FTPCNTL Parameter Group (Non-TCPaccess FTP)*, on page 5-42).
Licensed	Set up the SAF access for maintaining policy rule sets (see *Subtask 8.4—Setting Up SAF Access for Maintaining Policy Rule Sets*, on page 5-44).
	Customize the FTPCNTL parameter group (see *Subtask 8.5—Customizing FTPCNTL Parameter Group (TCPaccess FTP)*, on page 5-45).
	Define policy rules for the TCPaccess FTP server (see Chapter 20, *Controlling the Use of FTP*).

After you have implemented the FTP event flow, proceed to the next task (see the section, *Task 9—Enabling the Interface Between NetMaster for File Transfer and TCP/IP*, on page 5-47).

Subtask 8.1—Setting Up TCP/IP to Generate SMF Records

The subtask that you perform in this section is determined by the TCP/IP software that you have:

- For Communications Server, see the section, *Setting Up Communications Server to Generate SMF Records*, on page 5-40.
- For TCPaccess, see the section, *Setting Up TCPaccess to Generate SMF Records*, on page 5-41.

Note

If you do not have Communications Server, skip this subtask.

The configuration members for Communications Server include parameters that do the following:

- Specify which SMF records are created.
- Identify the SMF subtypes.

Step 1. Check the PROFILE.TCPIP configuration member for FTP client record creation.

Ensure that the SMFCONFIG statement includes the FTPCLIENT parameter for FTP client records, for example:

```
SMFCONFIG FTPCLIENT
```

Caution

Client record generation also relies on the client being able to extract the name of the procedure that starts the local TCP/IP stack. The name is extracted from the TCPIPJOBNAME statement by searching, in order:

- The /etc/resolv.conf UNIX file
- A TCPIP.DATA data set, which may require a SYSTCPD DD statement in the client JCL procedure.

For more information about the search order of configuration files for TCP/IP applications, see the IBM *Communications Server IP Configuration* manual.

Step 2. Check the FTP.DATA configuration member for FTP server record creation. It is recommended that you set SMF to STD.

FTP server record creation for NetMaster for File Transfer is controlled by the following SMF statements:

- SMF—all FTP server records
- SMFAPPE—FTP server append records
- SMFRETR—FTP server retrieve records
- SMFSTOR—FTP server store and store unique records

Each of these records specifies the SMF record subtype value to be used for the specific events.

The SMF statement can be used to set the default values for all types as follows:

```
SMF     STD
```

Step 3. If you have made any changes in Step 2, restart the FTP server started task. If you have made any changes in Step 1, restart the TCP/IP started task.

Note

If you do not have TCPaccess, skip this subtask.

Note

If you are using the TCPaccess 5.2 software, you must apply PTFs TP07334, TP07350, and TP07387.

Implement the software for the NetMaster for File Transfer region as follows:

Step 1. Check the IJTCFG*xx* configuration member to ensure that all of the subtypes that you require will be generated.

The SMF TYPE parameter identifies whether or not SMF records are created.

Note

If your SMF statement does not specify SUBTYPE or has SUBTYPE(ALL), you can skip this step.

The SMF statement includes a SUBTYPE parameter. This allows specific subtypes to be selected or suppressed. If the parameter is set to:

- ALL—leave it as it is.
- NONE—set it to ALL or a list the subtypes that you require.
- A list of subtypes—set it to ALL or a list of the subtypes that you require.

The following subtype is used by NetMaster for File Transfer:
SUBTYPE 20—FTP data set transfer completion (RETR, STOR, and APPE).

Step 2. Copy the NMDSPAXS load module supplied in *dsnpref*.MS*vvv*.MSLOAD to a library accessible to TCPaccess, for example a library in the TCPaccess started task STEPLIB.

Step 3. Define NMDSPAXS as a TCPaccess exit by adding the following statement to IJTCFG*xx* member:

```
EXIT PROGRAM (NDMSPAXS)
```

Note

Insert the NMDSPAXS definition in the first position of the exit list. This ensures that the exit is always called.

Step 4. Restart TCPaccess to bring the changes into effect.

Note

If you have TCPaccess 5.2 and are running FTP separately, you need to restart your FTP started task instead of your TCPaccess started task.

Subtask 8.2—Implementing the SMF Exit for the FTP Receiver

If you are using the Communications Server, then in order to intercept FTP file transfer events, you need to implement the SMF exit and ensure that this is called as a result of FTP client and server activity on your system.

Note

TCPaccess 5.2 and above do not require an SMF exit; the TCPaccess exit NMDSPAXS includes this functionality. Go to *Subtask 8.3—Customizing FTPCNTL Parameter Group (Non-TCPaccess FTP)*, on page 5-42.

The task that you perform in this section is determined by your TCP/IP stack.

Implementing the SMF Exit for IBM's TCP/IP

For IBM's Communications Server, the SMF exit module is provided in *dsnpref*.MS*vvv*.MSLOAD(NMSMFIBM).

Step 1. Copy the NMSMFIBM executable module to a load library in the link list.

Step 2. Issue an LLA refresh.

Note

A copy of this exit might already be installed on your system if you have installed the NetMaster for TCP/IP or NetSpy software.

If you have installed NetMaster for TCP/IP 5.0 or earlier, a copy of the IPSMFEX exit might be installed. You need to replace this exit with the NMSMFIBM exit.

Subtask 8.3—Customizing FTPCNTL Parameter Group (Non-TCPaccess FTP)

The FTPCNTL parameter group enables you to do the following for file transfers not using the TCPaccess FTP server:

- Specify whether to enable the receipt of FTP events. The default is to enable receipt of events.
- Change the static name for FTP transfers. The default is FTPXFER. The name enables you to filter on FTP transfers as a group in file transfer rules and schedules. You can use this name as the transfer ID when you set up rules and schedules (see, for example, *Adding File Transfer Rules to a Rule Set*, on page 10-6).

You need to customize this group only if the defaults are not suitable.

Customize the FTPCNTL parameter group as follows:

Step 1. Enter the **/ICS** shortcut to access the Customization Parameters panel, and enter **U** beside the $RF FTPCNTL parameter group.

The Initialization Parameters panel for FTP Control is displayed (see Figure 5-11).

Figure 5-11. Customizing the FTPCNTL Parameter Group (Without TCPaccess FTP)

```
SOLVPROD-------------- ICS : Initialization Parameters -------------Page 1 of 1
Command ===>                                                  Function=Update

.- FTPCNTL - FTP Control -------------------------------------------------.
| For TCPaccess FTP Server                                                |
|   Enable FTP Event Receiver ........ NO         (default is YES)        |
|   Enable Receiver ID ............... $RFFTEVR   (default is $RFFTEVR)   |
|   Enable SOLVE Data Space Monitoring NO         (default is YES)        |
|                                                                         |
| For Non TCPaccess FTP Server                                            |
|   Enable FTP Event Receiver ........ YES        (default is YES)        |
|   FTP Transfer ID .................. FTPXFER    (Optional. See note below.) |
|                                                 (default is FTPXFER)    |
'-------------------------------------------------------------------------'


.- Notes ----------------------------------------------------------------.
| Non TCPaccess FTP Server                                                |
|            Specifies whether FTP file transfer events will be received. |
|            The FTP Transfer ID will be assigned to FTP transfers.       |
'-------------------------------------------------------------------------'

 F1=Help      F2=Split      F3=File      F4=Save      F5=ILog      F6=Action
                            F9=Swap
```

Step 2. Under the heading For Non TCPaccess FTP Server, do the following:

a. To enable or disable the receipt of FTP events, enter **YES** (the default) or **NO** in the Enable FTP Event Receiver field.

b. If you want to use a different static name for FTP transfers, change the FTP Transfer ID (default FTPXFER).

Step 3. Press F6 (Action) to implement your FTP initialization parameters.

Step 4. Press F3 (File) to save your changes.

Subtask 8.4—Setting Up SAF Access for Maintaining Policy Rule Sets

To maintain policy rule sets, the user ID attempting to update the rule set must be associated with a new SAF facility, $SOLVE.FTP.CONTROL, that must be defined to your security system.

The user's access to this facility determines the user's access to policy rule sets:

- Read access allows the user to view policy rule sets.
- Update access allows the user to both view and maintain policy rule sets.

The following sequence of events illustrates how the facility and a user ID are associated:

1. You define user FTPUSER to your security system.
2. You define a SAF facility to your security system.
3. You associate user FTPUSER to the SAF facility and give the user update access.
4. When FTPUSER user accesses the FTP policy rule set list panel a SAF call is made to ensure that FTPUSER has access to the $SOLVE.FTP.CONTROL facility and then to determine the authority of the user. In this example, the user has update authority.

Defining $SOLVE.FTP.CONTROL to Your Security System

The steps to define $SOLVE.FTP.CONTROL depend on your security system. They are described in the following sections.

Defining $SOLVE.FTP.CONTROL to RACF

Define $SOLVE.FTP.CONTROL to RACF by issuing the following command:

```
RDEFINE FACILITY $SOLVE.FTP.CONTROL  UACC(NONE)
PE $SOLVE.FTP.CONTROL CLASS(FACILITY) ID(userid or group)
ACCESS(UPDATE)
SETROPTS GENERIC(FACILITY) REFRESH
```

Defining $SOLVE.FTP.CONTROL to ACF2

To define $SOLVE.FTP.CONTROL to ACF2, compile the following rule to authorize users to maintain policy rules:

Note

Rule lines after the $KEY line must be in column 2.

If you compile this rule in TSO, you must enter a blank line after the last rule line entry and before the STORE command.

```
ACF
COMP *
$KEY($SOLVE.FTP.CONTROL) TYPE(FAC)
 UID(uid_string) SERVICE(UPDATE) ALLOW

STORE
END
```

Defining $SOLVE.FTP.CONTROL to Top Secret

To define $SOLVE.FTP.CONTROL to Top Secret, complete the following steps:

Step 1. To define ownership of the SAF facility, enter the following command:

```
TSS ADD(department-id) IBMFAC($SOLVE.FTP.CONTROL)
```

Step 2. To allow access to policy maintenance functions, enter the following command:

```
TSS PER(userid) IBMFAC($SOLVE.FTP.CONTROL) ACC(WRITE)
```

Subtask 8.5—Customizing FTPCNTL Parameter Group (TCPaccess FTP)

The FTPCNTL parameter group enables you to do the following for file transfers using the TCPaccess FTP server (if you are licensed for the TCPaccess FTP feature):

- Specify whether to enable the receipt of FTP events. The default is to enable receipt of events.
- Change the name of the event receiver ID. The default is $RFFTEVR.
- Specify whether to monitor the data space. The default is to monitor the data space.

  Note

  The data space is monitored through the FTPMGR, which displays a message to indicate the status of the data space.

You need to customize this group only if the defaults are not suitable.

Customize the FTPCNTL parameter group for the TCPaccess FTP server as follows:

Step 1. Enter the **/ICS** shortcut to access the Customization Parameters panel, and enter **U** beside the $RF FTPCNTL parameter group.

The Initialization Parameters panel for FTP Control is displayed (see Figure 5-12).

Figure 5-12. Customizing the FTPCNTL Parameter Group (TCPaccess FTP)

```
SOLVPROD--------------ICS : Initialization Parameters --------------Page 1 of 1
Command ===>                                                  Function=Update

.- FTPCNTL - FTP Control -------------------------------------------------.
|                                                                          |
| For TCPaccess FTP Server                                                 |
|   Enable FTP Event Receiver ......... YES       (default is YES)         |
|   Event Receiver ID ................. $RFFTEVR  (default is $RFFTEVR)    |
|   Enable SOLVE Data Space Monitoring  YES       (default is YES)         |
|                                                                          |
| For Non TCPaccess FTP Server                                             |
|   Enable FTP Event Receiver ......... NO        (default is YES)         |
|   FTP Transfer ID ................... FTPXFER   (Optional. See note below.) |
|                                                 (default is FTPXFER)     |
'--------------------------------------------------------------------------'


.- Notes ----------------------------------------------------------------.
| Non TCPaccess FTP Server                                                 |
|            Specifies whether FTP file transfer events will be received.  |
|            The FTP Transfer ID will be assigned to FTP transfers.        |
'--------------------------------------------------------------------------'

 F1=Help      F2=Split      F3=File      F4=Save      F5=ILog      F6=Action
                            F9=Swap
```

Step 2. Under the heading For TCPaccess FTP server, do the following:

a. To enable or disable the receipt of FTP events, enter **YES** (the default) or **NO** in the Enable FTP Event Receiver field.

b. If you want to use a different receiver ID name for FTP transfers, change the Receiver ID (default $RFFTEVR). This value must be the same as that configured in the TCPaccess FTP server.

c. To enable or disable the monitoring of the data space, enter **YES** (the default) or **NO** in the Enable SOLVE Data Space Monitoring field.

Step 3. Press F6 (Action) to implement your FTP initialization parameters.

Step 4. Press F3 (File) to save your changes.

Task 9—Enabling the Interface Between NetMaster for File Transfer and TCP/IP

NetMaster for File Transfer is used with IBM's Communications Server or the TCPaccess product. If you plan to use functions that require TCP/IP (for example, monitoring CA-XCOM file transfers, CONNECT:Direct file transfers on distributed systems or FTP file transfers), you need to enable the interface between them.

If you are using …	**See the section …**
Communications Server	*Enabling the Interface to Communications Server*, on this page.
TCPaccess	*Enabling the Interface to TCPaccess*, on page 5-51.

Enabling the Interface to Communications Server

You need to ensure that Communications Server can support NetMaster for File Transfer. This is done by:

1. Authorizing the started task User IDs. This enables the NETSTAT interface and the sockets interface (see the section, *Authorizing the Started Task User ID*, on page 5-48)
2. Authorizing the interface between NetMaster for File Transfer and your Communications Server product (see the section, *Authorizing the Interface Between NetMaster for File Transfer and Communications Server*, on page 5-49)
3. Enabling access to SNMP data (see the section, *Enabling Access to SNMP Data in Communications Server*, on page 5-50)
4. Enabling name resolution (see the section, *Enabling Name Resolution*, on page 5-51)

After you enable the interface, proceed to the next task (see the section, *Task 10—Implementing a SOLVE:Problem Automatic Problem Recording Environment*, on page 5-54).

Authorizing the Started Task User ID

The sockets interface allows NetMaster for File Transfer to perform TCP/IP related functions.

The NETSTAT and sockets interfaces both require an Open Edition security definition, referred to as an OMVS segment. You can use a default OMVS segment, or define a specific one, for the region started task user ID and the SOLVE SSI started task user ID.

The NETSTAT interface also requires the SOLVE SSI startup parameter UNIX=YES. For more information, see the *Unicenter Mainframe Installation and Setup Instructions*.

To authorize your started task user ID, complete the following steps:

Step 1. Set up an Open Edition security definition, which is also known as an OMVS segment.

To set up an OMVS segment, complete the following steps:

a. Identify the region started task user ID and the SOLVE SSI started task user ID that you want to authorize.

Note

These can be the same user ID, or they can be different ones.

b. Choose an OMVS UID number to associate with each started task user ID. Your security administrator may have a policy for assigning OMVS UID numbers. If not, then simply use a unique number; for example, 123.

For further information about OMVS UID numbers, see your IBM documentation.

c. Choose a home directory to associate with each started task user ID. Ensure that it exists and that the UID has at least read access to it.

You can use the UNIX root directory (/), or you can use a customized home directory name.

For example, to set up a directory called /u/solve for the user ID solve, you can issue the following commands:

mkdir /u/solve
chown solve /u/solve
chmod +777 /u/solve

You can then confirm the owner and access to the directory by using the command:

ls -l -d /u/solve

Step 2. For a user ID *uuuuuu* and UID number *nnn*, define the OMVS segment to your security system as follows:

For RACF systems, enter:
ALU *uuuuuu* OMVS(UID(*nnn*) HOME(/) PROGRAM(/bin/sh))

For ACF2 systems, enter:
SET PROFILE(USER) DIV(OMVS)
INSERT *uuuuuu* UID(*nnn*) HOME(/) PROGRAM(/bin/sh)

For Top Secret systems, enter:
TSS ADD(*uuuuuu*) HOME(/) OMVSPGM(/bin/sh) UID(*nnn*) GROUP(OMVSGRP)

Step 3. Ensure that you have completed this process for each started task user ID that you want to authorize. To confirm the contents of the OMVS segment, do this:

For RACF systems, enter:
LISTUSER *uuuuuu* OMVS NORACF

For ACF2 systems, enter:
SET PROFILE(USER) DIV(OMVS)
LIST *uuuuuu*

For Top Secret systems, enter:
TSS LIS(*uuuuuu*) DATA(ALL)

Authorizing the Interface Between NetMaster for File Transfer and Communications Server

To give NetMaster for File Transfer the correct authority, you must give it specific RACF access privileges. If you are using a different security product to RACF, make the necessary changes to the instruction.

To enable the Drop function for TCP/IP connections, authorize the user ID of the NetMaster for File Transfer region in RACF to access the MVS.VARY.TCPIP.DROP resource in the OPERCMDS class.

Note

When you start NetMaster for File Transfer, your security system assigns a user ID to the started task.

The assigned user ID is displayed in message IEF695I, which is written to the system log when the task is started. For a batch job, the assigned user ID is specified on the job card.

Caution

If you are using a security exit that returns user tokens and you are using AOM user level security which gives individual users different OS/390 command authority levels, you must set individual authority privileges.

Enabling Access to SNMP Data in Communications Server

Some NetMaster for File Transfer functions access information about Communications Server, using SNMP.

Note

This applies only if you are using NetMaster for File Transfer CONNECT:Direct agents.

To enable these functions, do this:

Step 1. Activate the SNMP Agent (OSNMPD) by following the instructions in IBM's *Communications Server IP Configuration* manual.

Step 2. Set up the TCP/IP sub-agent in the PROFILE data set by following the instructions in IBM's *Communications Server IP Configuration* manual. For example:

```
SACONFIG COMMUNITY public AGENT 161
SACONFIG ENABLED SETSENABLED
```

Note

The word `public` must be in lower case.

Step 3. Configure a community name for use by the local host IP address in the *prefix*.PW.SRC data set. Community names are case sensitive, the default community name is `public` in lower case.

Example—multiple IP addresses. If Communications Server has the IP addresses 172.24.8.1 and 172.24.1.2, then your PW.SRC data set could contain something like `public 172.24.0.0 255.255.0.0`

Example—single IP address. If Communications Server has the IP addresses 172.24.0.1, then your PW.SRC data set could contain something like `public 172.24.0.1 255.255.255.255`

See IBM's *Communications Server IP Configuration* manual for further information about configuring the SNMP Agent and configuring community names.

Key Concept

Name lookup allows translation between IP addresses and host names. NetMaster for File Transfer name lookup reads the TCPIP.DATA data set and looks for NSINTERADDR statements which contain the IP addresses of name servers.

TCP/IP tries to resolve the host name through a name server, if one is present. If the name cannot be resolved, the system uses the *prefix*.HOSTS.LOCAL data set. For more information about the data set, see IBM's *Communications Server IP Configuration* manual.

To ensure that name resolution is enabled, check that the TCPIP.DATA and *prefix*.HOSTS.LOCAL data sets are configured to suit your requirements.

The data set prefix value, *prefix*, is determined from the DATASETPREFIX statement in the TCPIP.DATA data set that you specify. This prefix is used to generate default names for Communications Server data sets.

Note

The data set prefix is used to locate the *prefix*.HOSTS.LOCAL data set. NetMaster for File Transfer must have read access to this data set.

Enabling the Interface to TCPaccess

You need to ensure that TCPaccess can support NetMaster for File Transfer. This is done by:

1. Reviewing the TCPaccess parameter data sets (see the next section, *Reviewing the Parameter Data Set*)
2. Enabling access to SNMP data (see the section, *Enabling Access to SNMP Data in TCPaccess*, on page 5-53)
3. Enabling name resolution (see the section, *Setting Up DNR Members*, on page 5-53)

Note

If you have TCPaccess 5.2, you must apply PTFs TP07334 and TP07350.

To ensure that the NetMaster for File Transfer region has the appropriate authority, access the TCPaccess PARM data set, and do the following:

Step 1. Review the TCPCFG*xx* member to ensure that a RAW protocol statement is present. This statement enables the ping and traceroute functions, for example:

```
RAW MAXLTSND(9000) MAXLTRCV(9000)  MAXQSEND(8) MAXQRECV(8)
```

Step 2. Copy the NMDSPAXS load module supplied in *dsnpref*.MS*vvv*.MSLOAD to a library accessible to TCPaccess, for example a library in the TCPaccess started task STEPLIB.

Step 3. Define NMDSPAXS as a TCPaccess exit by adding the following statement to IJTCFG*xx* member:

```
EXIT PROGRAM (NDMSPAXS)
```

Note

Insert the NMDSPAXS definition in the first position of the exit list. This ensures that the exit is always called.

Step 4. Restart TCPaccess to bring the changes into effect.

Step 5. Check the TCPaccess job log and the SYSLOG for the presence of these two messages:

```
T00EX004I NMDSPAXS: N6XA01 SOLVE log message interface
initialized
```

```
T00EX04I NMDSPAXS: N6XA02 Receiver ID $IPXssid will monitor
messages from the Sterling stack
```

where ssid is the SSID of the TCPaccess job.

These messages are passed to your region during the TCPaccess initialization. Their presence indicates that the system has been setup correctly.

Enabling Access to SNMP Data in TCPaccess

Some NetMaster for File Transfer functions access information about TCPaccess, using SNMP.

To enable this, you must activate the SNMP agent, by updating the SNMCFG*xx* member in the TCPaccess PARM data set. Make sure that you have a community value statement which includes the community name `public`.

For more information about updating the SNMCFG*xx* member, see the *TCPaccess Customization Guide*.

Setting Up DNR Members

Ensure that your TCPaccess Domain Name Resolver (DNR) members can translate the TCPaccess subsystem name into an IP address and a fully qualified host name. To do this:

Step 1. Enable translation from subsystem name to fully qualified domain name.

For example, if your TCPaccess subsystem name is ACSS and its fully qualified domain name is MVS.SITE1.COM., enter a line like the following into your DNRALC*xx* member:

```
ACSS MVS.SITE1.COM.
```

Note

Specify the domain name (rather than an IP address), and end it with a period (.).

Step 2. Enable local translation of the fully qualified host name to an IP address.

For example, if the IP address of MVS.SITE1.COM. is 172.24.140.117, enter a line like the following into your DNRHSTxx member:

```
MVS.SITE1.COM. 172.24.140.117
```

Note

This DNR configuration is recommended in the *TCPaccess Customization Guide*, which contains further details about the ACPCFG*xx*, TCPCFG*xx*, and DNRALC*xx* members of the TCPaccess PARM data set.

You need to ensure that the HOSTTABLE statement in the DNRCFG*xx* member points to the correct DNRHST*xx* member.

You do not need to restart TCPaccess to introduce changes to the DNR tables, you can restart DNR—for example:

F TCPICS,STOP DNR
F TCPICS,START DNR

Task 10—Implementing a SOLVE:Problem Automatic Problem Recording Environment

The NetMaster for File Transfer region can add problem records to a SOLVE:Problem application.

If you want to enable automatic recording of specified NetMaster for File Transfer problems in SOLVE:Problem, perform the following subtasks:

- Subtask 10.1—Copying the $RMPB07S NCL Procedure
- Subtask 10.2—Authorizing Users in the SOLVE:Problem Region
- Subtask 10.3—Defining Links

After you have implemented automated problem recording, you can proceed to the next task (see the section, *Task 11—Implementing the Alert Monitor Problem Ticket Interface*, on page 5-55).

Subtask 10.1—Copying the $RMPB07S NCL Procedure

Copy the $RMPB07S NCL procedure from the *dsnpref*.AS500.ASTEXEC data set to the NCL procedures library (normally TESTEXEC) in the region in which the SOLVE:Problem application is running. (*dsnpref* is the data set prefix used during the installation of the NetMaster for File Transfer product.)

Subtask 10.2—Authorizing Users in the SOLVE:Problem Region

Authorize the following user IDs in the SOLVE:Problem region:

- NetMaster for File Transfer BSYS background user ID *xxxx*BSYS, where *xxxx* is the domain ID of the NetMaster for File Transfer region
- IDs of the users who may raise problem tickets manually from the alert monitor in the NetMaster for File Transfer region

Subtask 10.3—Defining Links

In the SOLVE:Problem region, define a link to each NetMaster for File Transfer region from which you want to receive problem tickets as follows:

```
DEFLINK TYPE=APPC LUNAME=acb-name LINK=link-name
```

acb-name is the ACB name of the NetMaster for File Transfer region, and *link-name* is a name that identifies the link.

Task 11—Implementing the Alert Monitor Problem Ticket Interface

The alert monitor provides an interface that enables you to raise problem tickets for alerts.

The alert monitor supports the following two interfaces for raising problem tickets:

- Electronic mail, where an e-mail describing the problem can be sent to a problem management application or to a particular person. This method can be used to send tickets to multiple problem management applications.
- Custom, where you can write your own NCL code to deliver the ticket to an application by whatever means you choose.

To implement this feature, define the problem ticket interface between your NetMaster for File Transfer region and the alert monitor (see the section, *Defining a Problem Ticket Interface*, on page 5-56).

If you want the operator to supply information when requesting the creation of a ticket, you also need to set up the problem ticket data entry definition (see the section, *Setting up the Problem Ticket Data Definition*, on page 5-59).

To perform these tasks, enter the **/ALADMIN** shortcut to display the Administration Menu (see Figure 5-13).

Figure 5-13. Alert Monitor : Administration Menu

```
SOLVPROD------------Alert Monitor : Administration Menu --------------/ALADMIN
Select Option ===>

   I   - Define Trouble Ticket Interface
   D   - Define Trouble Ticket Data Entry
   H   - Set Alert History Logging Parameters
   F   - Define Filters
   L   - Define List Formats
   X   - Exit
```

Defining a Problem Ticket Interface

To define a problem ticket interface between your NetMaster for File Transfer region and the alert monitor, complete the following steps:

Step 1. On the alert monitor Administration Menu, select option **I** - Define Trouble Ticket Interface to display the Alert Monitor : Interface Definition panel (see Figure 5-14).

Figure 5-14. Alert Monitor : Interface Definition Panel

```
SOLVPROD------------- Alert Monitor : Interface Definition --------------------
Command ===>




Press F6 to confirm the Interface type

Interface Type ..........+ ____________________
```

Step 2. In the Interface Type field, specify the type of interface that you want to define.

To obtain a selection list of valid values, enter **?** in this field.

Step 3. Press F6 (Action). A panel is displayed where you can define your interface. The type of panel displayed varies, depending on the interface type that you specified. For further details, see the section, *Defining an E-mail Problem Ticket Interface*, on page 5-56 and the section, *Defining a Custom Problem Ticket Interface*, on page 5-58.

Defining an E-mail Problem Ticket Interface

If you specified **EMAIL** as the interface type on the Alert Monitor : Interface Definition panel, pressing F6 (Action) displays the Alert Monitor : Email a Trouble Ticket panel.

To define your e-mail interface, complete the following steps:

Step 1. Enter values in the input fields in the top section of the panel.

You can use F1 (Help) to obtain information about completing these fields.

Step 2. Complete the Enter Mail Text Below section of the panel, which is free format.

You can use F1 (Help) to obtain information about completing this section.

Figure 5-15 shows an example of a completed panel. The &$USRNAME variable, together with a data entry definition, enables you to prompt users to enter the address of the mail receiver. (For information about how to create the data entry definition, see the section, *Setting up the Problem Ticket Data Definition*, on page 5-59.)

For information about the file transfer variables, see help or Appendix D, *File Transfer Variables*.

Figure 5-15. Alert Monitor : Email a Trouble Ticket Panel

```
SOLVPROD------------ Alert Monitor : Email A Trouble Ticket ----Columns 001 074
Command ===>                                    Function=Update Scroll ===> PAGE

Mail Address                &$USRNAME_____________________________________________
Host Name      (IBM)        ALMVS1__
SMTP Node Name (IBM)        ALMVS1__
SMTP Job Name  (IBM)        SMTP32__
SMTP DEST Id (TCPaccess)    ________
Exit Procedure Name         ________
Subject                     &$AMDESC______________________________________________

                               Enter Mail Text Below

**** ****************************** TOP OF DATA ******************************
0001 Alert Creation Date      : &$AMDATE
0002 Alert Creation Time      : &$AMTIME
0003 Source Name              : &ZRFSRCFNAME
0004 Target Name              : &ZRFTGTFNAME
0005
0006 Severity                 : &$AMSEVERITY
**** ***************************** BOTTOM OF DATA ****************************


 F1=Help      F2=Split     F3=File      F4=Save      F5=Find      F6=Change
 F7=Backward  F8=Forward   F9=Swap     F10=Left     F11=Right    F12=Cancel
```

Step 3. Press F3 (File) to save your interface definition and return to the Alert Monitor Administration menu.

Note

For e-mail to be delivered, the SMTP job specified here must be active.

If you specified **CUSTOM** as the interface type on the Alert Monitor : Interface Definition panel, pressing F6 (Action) displays the Alert Monitor : Custom Trouble Ticket panel.

To define your custom interface, complete the following steps:

Step 1. In the Procedure Name input field, enter the name of your NCL procedure for delivering tickets.

Step 2. In the Enter Parameters Below section of the panel, specify any parameters that you want the NCL procedure to receive. This section is free format.

You can use F1 (Help) to obtain information about completing this section.

Figure 5-16 shows an example of an interface that uses the distributed SOLVE:Problem exit, $RMPB06S, to send tickets to a SOLVE:Problem region with the ACB name SOLVPROB. (For more information about the SOLVE:Problem interface, see the section, *Task 10—Implementing a SOLVE:Problem Automatic Problem Recording Environment*, on page 5-54.)

Figure 5-16. Alert Monitor : Custom Trouble Ticket Panel

```
SOLVPROD------------- Alert Monitor : Custom Trouble Ticket ----Columns 001 074
Command ===>                                  Function=Update Scroll ===> CSR

Procedure Name  $RMPB06S

                            Enter Parameters Below

**** ****************************** TOP OF DATA ******************************
0001 ACBNAME=solvprob
**** ****************************** BOTTOM OF DATA ***************************
```

Step 3. Press F3 (File) to save your interface definition and return to the Alert Monitor Administration menu.

Setting up the Problem Ticket Data Definition

If you want the operator to supply information when requesting the creation of a problem ticket, you need to set up the ticket data entry definition as follows:

Step 1. On the alert monitor Administration Menu, select option **D** - Define Trouble Ticket Data Entry to display the Alert Monitor : Trouble Ticket Data Entry Definition panel.

Step 2. In the free-format data entry section of the panel, enter the data entry definition for the panel that the operator will use when creating a ticket.

You can use F1 (Help) to obtain information about completing this section.

Figure 5-17 shows an example of a definition that prompts the operator to identify the receiver of the ticket.

Figure 5-17. Alert Monitor : Trouble Ticket Data Entry Definition Panel

```
SOLVPROD----- Alert Monitor : Trouble Ticket Data Entry Definition ------------
Command ===>                                  Function=Update Scroll ===> PAGE

**** ****************************** TOP OF DATA ******************************
0001 FIELD NAME=$USRNAME
0002  VALUE="Problem@sydney.enterprise.com"
0003  DESC="Send Email to:"
0004  COMMENT="(name for e-mail)"
0005  REQUIRED=YES
0006  LENGTH=40
**** ***************************** BOTTOM OF DATA ****************************
```

Step 3. Press F3 (File) to save your trouble ticket data entry definition and return to the alert monitor Administration Menu.

Task 12—Implementing Alert Forwarding

Alerts are normally displayed on the alert monitor. However, you can also forward them to other platforms:

- Unicenter TNG Event Console
- UNIX platforms as SNMP traps
- NetMaster for SNA (NEWS) or NetView (TME10) systems, as Generic Alert NMVTs

You can apply filter criteria to forward different types of alerts to different platforms.

Implementation

To enable alert forwarding, execute the $AMEVFWD command. This command has two groups of parameters:

- Those which describe the destination platform
- Those which supply the filtering criteria

To implement alert forwarding you need to execute an $AMEVFWD command for each combination of platform and filtering parameters. It is recommended that you include these commands in your NMREADY procedure so that they are enabled at region initialization and remain in effect while the region is running.

See the section, *$AMEVFWD*, on page 5-61 for the syntax of the $AMEVFWD command.

The SNMP Trap Definition

The MIB definition for alerts forwarded as SNMP traps is provided in member $AMTRAP, supplied in the *dsnpref*.MS*nnn*.INSTAL data set. You can download this member to your UNIX system and compile it.

Note

When copying this member to your UNIX system, you may wish to rename it to avoid problems on some UNIX systems where the $ sign has special meaning.

The supplied MIB defines two traps with the following object identifiers:

- $AMTRAP = 1.3.6.1.4.1.1126.1.2.1.2 (for an alert)
- $AMTRAPC = 1.3.6.1.4.1.1126.1.2.1.3 (when an alert is cleared)

$AMEVFWD

Function

To implement alert forwarding.

```
$AMEVFWD      DESTTYPE={ NMVT | SNMPTRAP | TNGTRAP}
               DESTADDR=ipaddr
              [DESTPORT=ipport ]
              [COMMNAME=community ]
              [NETVALRT=ppiname ]
              [FILTER=filtername | (APPLID=app
               CLASSID=class SYSTEMID=system )]
              [CLEAR={ YES|NO } ]
              [ALERTS={ NEW | ALL } ]
              [IPINACT={ WAIT | IGNORE } ]
```

Use

The $AMEVFWD command is used to implement alert forwarding.

Operands

The destination platform is specified by the DESTTYPE, DESTADDR, DESTPORT, COMMNAME, and NETVALRT parameters.

The filtering criteria are specified by either the FILTER parameter or a combination of the APPLID, CLASSID, and SYSTEMID parameters. Only alerts which meet these criteria are forwarded.

Destination Details

There are two choices of destination, either reformatted as generic alert NMVTs or as SNMP traps.

To send as NMVTs:

DESTTYPE=NMVT

NMVTs are queued to the NETVALRT PPI receiver queue and are then processed by either NetMaster for SNA (NEWS) or NetView. There are no other (destination) parameters needed. For further details, see *Notes*, on page 5-64.

NETVALRT=*ppiname*

The default name for the NETVALRT PPI receiver is NETVALRT. If you have used a different name, use this operand to specify the name.

To forward alerts as SNMP traps:

DESTTYPE=SNMPTRAP
DESTADDR=*ipaddr*
[DESTPORT=*ipport*]
[COMMNAME=*community*]
[IPINACT={ WAIT | IGNORE }]

For SNMP traps, specific destination details are required, as follows:

DESTADDR=*ipaddr*

This is mandatory. It specifies the destination (IP) address as either a valid IP address in dotted notation (for example, 123.45.6.78) or a host name address (for example, network.operations.com).

DESTPORT=*ipport*

This is optional. It specifies the port number (at the destination address). If specified, it must be a number in the range 1 to 65535. If omitted, it defaults to 162.

COMMNAME=*community*

This is optional. It specifies the community name (at the destination address). If omitted, it defaults to `public` (in lower case).

Community names are case-sensitive. When a value is specified, ensure that the value is in the correct case.

If the procedure is started from another procedure, for example within the READY procedure, ensure that the statement remains case-sensitive at execution time. By default, NCL procedures such as the READY procedure convert data to upper case during assignment. Disable upper case translation over the $AMEVFWD procedure invocation with the &CONTROL UCASE|NOUCASE statement. For example:

```
&CONTROL NOUCASE
START $AMEVFWD DESTTYPE=SNMPTRAP DESTADDR=xxx +
  DESTPORT=162 COMMNAME=public
&CONTROL UCASE
```

IPINACT={WAIT|IGNORE}

This parameter controls how the alert forwarder behaves when alerts are forwarded as SNMP traps (which requires TCP/IP services) but the TCP/IP interface is not active.

If set to WAIT, when the TCP/IP interface is inactive, alert forwarding is suspended until the interface becomes active.

If set to IGNORE, when the TCP/IP interface is inactive, any alerts are discarded.

To forward alerts as SNMP traps to a Unicenter TNG Event Console, the destination details are similar to those for SNMP traps except that DESTTYPE=TNGTRAP.

Filtering Details

There are four options for filtering. You can:

- Apply a named filter using FILTER=*filtername*.
- Apply filter criteria using the APPLID, CLASSID, and SYSTEMID parameters.
- Apply filtering criteria with the CLEAR and ALERTS operands—these can be applied regardless of the destination details. Both are optional.
- Not apply a filter.

Applying a Named Filter

FILTER=*filtername*
This specifies the name of the filter to apply. If a filter is specified, the named filter must exist.

Applying Filter Criteria

If a defined filter is not specified, you can use a combination of the APPLID, CLASSID, and SYSTEMID operands.

APPLID=*app*
This is the SOLVE application ID, for example, $RF. This defaults to all application IDs if omitted.

CLASSID=*class*
This is the Alert Monitor Class ID. This is shown as Alert Class when an alert is displayed. This defaults to all class IDs if omitted.

SYSTEMID=*system*
This is the system ID of the region where the alert originated. This defaults to the local system if omitted.

Predefined Filter Criteria

CLEAR=YES|NO

This parameter relates to alerts that are cleared. If set to YES, alerts for cleared alert events are forwarded.

ALERTS=NEW|ALL

This parameter controls how alerts generated before alert forwarding is enabled are handled.

If set to NEW—only new alerts are forwarded. This option is normally used if alert forwarding is restarted.

If set to ALL—current alerts, and new alerts as they arrive, are forwarded. Use this option to make the alert forwarding function behave the same as the Alert Monitor option at a terminal. This option is normally used when the alert monitor is started during initialization of the region.

Notes

These notes apply to forwarding alerts as NMVTs.

Forwarding to NetMaster for SNA (NEWS Component)

To receive alerts, you must have the PPI receiver active. This is normally started by the following statement, which is included in the NEWS section of the distributed $NSINIT procedure:

```
SUBMIT BMON START $NWPPIAR
```

The forwarded alerts do not appear on the Dynamic Attentions panel but are recorded as Operator Notification Events for the specific resource, identified as the primary ACB name (PRI JCL parameter) of the region which forwarded the alert.

Forwarding to NetView

To receive alerts in a NetView region, you must have the CNMCALRT task defined and active. To do this:

Step 1. Check the DSIDMN (or DSIDMNB) member in the DSIPARM PDS.

Step 2. Ensure that the CNMCALRT task is included and is initialized (INIT=Y). For example:

```
TASK  MOD=CNMCALRT,TSKID=CNMCALRT,PRI=6,INIT=Y
```

Note

This statement is necessary for the OS/390 software alert forwarding function.

The alerts are formatted as Operator Notification generic alerts.

Examples

To send all alerts from SOLVE5 as NMVTs:

```
START $AMEVFWD DESTYPE=NMVT SYSTEMID=SOLVE5
```

Task 13—Implementing Event Recording and Reporting

NetMaster for File Transfer provides a reporting function. The reporting function provides online and printed reports based on information in the event database. If you want to use the reporting function, you must activate the recording of file transfer events into the events database.

Note

If you want to use the default values of the event logging parameters, you do not need to perform this task.

The reporting function also allows you to extract the data for analysis by exporting it in character separated value (CSV) format for use by other data analysis and reporting tools.

To implement event recording, complete the following steps:

Step 1. Enter the **/ICS** shortcut to access the Customization Parameters panel, and enter **U** beside the $RF EVENTLOG parameter group.

The Initialization Parameters panel for event logging is displayed.

Figure 5-18. Implementing Event Recording and Reporting

```
SOLVPROD-------------- ICS : Initialization Parameters -------------Page 1 of 2
Command ===>                                                Function=Update

.- EVENTLOG - Event Logging -------------------------------------------------.
|                                                                             |
| Enable Event Logging ......... YES                                          |
| EVNTDB Database Name ......... AUDE0.DENM13.EVNTDB ________________________ |
| Time of Day to Delete ........ 18.05                                        |
| Number of Days to Keep ....... 4__ (0=Delete ALL Records)                   |
| EVNTARC Archive Dataset ...... AUDE0.DENM13.EVNTARC.TMP(+1)_______________ |
| Field Separator Character .... ,                                            |
| EVNTSEQ Reorg Dataset ........ AUDE0.DENM13.EVNTSEQ________________________ |
'-----------------------------------------------------------------------------'
```

Step 2. Ensure that Enable Event Logging is set to Yes.

Step 3. In the EVNTDB Database Name field, enter the data set name to which events are to be logged, or use the default. This VSAM data set was created by the setup process. See the *Unicenter Mainframe Installation and Setup Instructions* for details.

Events are retained in this database for the number of days that you specify on this panel.

Note

You should monitor the size of the EVNTDB database. When the EVNTDB database reaches the file size limit, automatic reorganization occurs. During this time no records are written to the EVNTDB database.

The utilization of data and index blocks is shown in message N13522 in the activity log when the region is initialized.

Step 4. In the EVNTARC Archive Dataset field, enter the name of the data set (which can be a data set in a generation data group (GDG)) to which events are to be archived, or leave the field at its default value. The default is a sequential data set that was created by the setup process. See the *Unicenter Mainframe Installation and Setup Instructions* for details.

Note

If you use a generation data set, use a relative generation number of +1 (for example, *gdg-name*(+1)). You must also complete the next panel. For more information about the fields, see the online help.

Note

If you need to increase the size of the EVNTDB database, ensure that the size of the EVNTARC data set is also increased, so that EVNTARC does not fill up during the archiving process.

If the archiving process fails, the records are still cleared from EVNTDB.

If you omit the event archive data set name, then old records are simply deleted when they expire.

Step 5. In the Field Separator Character field, specify the character you want to separate archived events. The default is comma (,).

Note

Events are written to the event archive data set as character separated values, which can be processed by PC-based reporting tools. As well as having data from the log periodically archived in this way, you can also extract data from the EVNTDB database on an ad hoc basis for processing and analysis. For instructions on extracting data to an external file, see the section, *Extracting Data to a File*, on page 18-18.

Step 6. In the Number of Days to Keep field, specify the number of days (between 0 and 30; default 7) for which reported events are to be kept in the EVNTDB database

Zero will cause all events to be deleted. A value between 1 and 30 will cause events from the previous 1 to 30 calendar days to be retained in the EVNTDB database.

Note

Keeping a lot of data online impacts the time to search for events.

Step 7. In the Time of Day to Delete field, specify the time of day (in the format *hh.mm*; default 00.15) at which reported events are to be deleted from the database and, if an EVNTARC archive data set is specified, archived to that data set.

Note

If the region is not active at the specified time, deletion does not occur.

Step 8. In the EVNTSEQ Reorg Dataset field, enter the name of the sequential data set that is to be used for backup during reorganization of the EVNTDB, or leave the default. The default was created by the setup process. See the *Unicenter Mainframe Installation and Setup Instructions* for details.

Step 9. Press F6 (Action) to implement your initialization parameters for reporting.

Task 14—Implementing the NetMaster Reporter Interface

If you use the NetMaster Reporter 2.0 product, you can send file transfer events to it for reporting. For information about NetMaster Reporter, see the *Working with NetMaster Reporter* guide.

To implement the interface, perform the following subtasks:

- Subtask 14.1—Defining the Data Warehouse Server
- Subtask 14.2—Logging Events to the Data Warehouse

Subtask 14.1—Defining the Data Warehouse Server

The data warehouse enables file transfer events to be logged and then extracted for reporting by the NetMaster Reporter software. If this region is not also the Report Center, you must define the data warehouse server in the region as follows. The region must also be linked to the Report Center. For information about how to link regions, see Chapter 7, *Administering Multisystem Operations*.

Step 1. Enter the **/ICS** shortcut to display the list of parameter groups.

Step 2. Enter **FIND REPORTER**, and then enter **U** beside the REPORTER parameter group.

Step 3. In the Report Center Link Name field on the displayed Reporter Interface window, specify the ACB name of the Report Center region. Leave the other fields blank.

Step 4. Press F6 (Action) to define the server, and then press F3 (File) to save the change.

Subtask 14.2—Logging Events to the Data Warehouse

To log file transfer events to the data warehouse, proceed as follows:

Step 1. Enter the **/ICS** shortcut to display the list of parameter groups.

Step 2. Enter **F EVENTLOG**, and then enter **U** beside the EVENTLOG parameter group.

Step 3. In the Send Statistical Data to NetMaster Reporter? field, enter **YES**.

Step 4. Press F6 (Action) to start logging and then F3 (File) to save the change.

What to Do Next

You have completed the implementation for your NetMaster for File Transfer region. You can now use the product to complete the building of the environment to manage your file transfer resources.

To …	You need to …
Add new users	Create additional user profiles (see the section, *Defining NetMaster for File Transfer Users*, on page 6-9).
Manage file transfer resources on more than one system	Implement NetMaster for File Transfer regions on those systems and link them together (see the section, *Linking NetMaster for File Transfer Regions*, on page 7-7). Where possible, implement your multisystem environment before you build the resource management environment for each region.
Build your file transfer resource management environment	Create file transfer rules and define the resources you want to manage (see Chapter 10, *Building the Environment to Manage Your File Transfer Services*).
Load your system image, check the operation of your defined resources, and optionally automate your resources	Perform the tasks provided in the section, *Loading, Checking, and Automating Your File Transfer Management Environment*, on page 10-58.
Define policies for use with a TCPaccess FTP server	Create policy rules (see Chapter 20, *Controlling the Use of FTP*).

6

Implementing Security

This chapter describes how to implement security in the NetMaster for File Transfer region.

The chapter contains the following topics:

- About Security
- Security Considerations for Existing Users
- Defining NetMaster for File Transfer Users
- Managing Users in a Multisystem Environment
- External Security Packages

About Security

Access to a NetMaster for File Transfer region is controlled by the User ID Access Maintenance Subsystem (UAMS).

NetMaster for File Transfer supplies sample group definitions that are generated during installation. These groups and their characteristics are described below:

- $RMADMIN—administrator—this group of users has access to all NetMaster for File Transfer administrative functions, such as adding users. An administrator has access to all the menu options and is authorized to delete database records.
- $RMOPER—operator—this group of users has access to a restricted subset of NetMaster for File Transfer functions. An operator does not have access to all the menu options and is not authorized to delete database records.
- $RMNOPER—network operator—this group of users has similar access to NetMaster for File Transfer functions as an operator. Network operators can manage network operations but are not authorized to manage system operations.
- $RMMON—monitor—this group of users has access to a restricted subset of NetMaster for File Transfer functions. A monitor user does not have access to all the menu options, and can browse but not update or delete database records.
- $RMBUSER—background user—this group of users has region or engine component authorization.

Warning

Do not modify the supplied $RMBUSER group definition, because this could impede the operation of the automation engine.

Controlling Access to Functions and Resources

Access to the functions and resources is controlled using the Network Partitioning Facility (NPF), your external security package, or both.

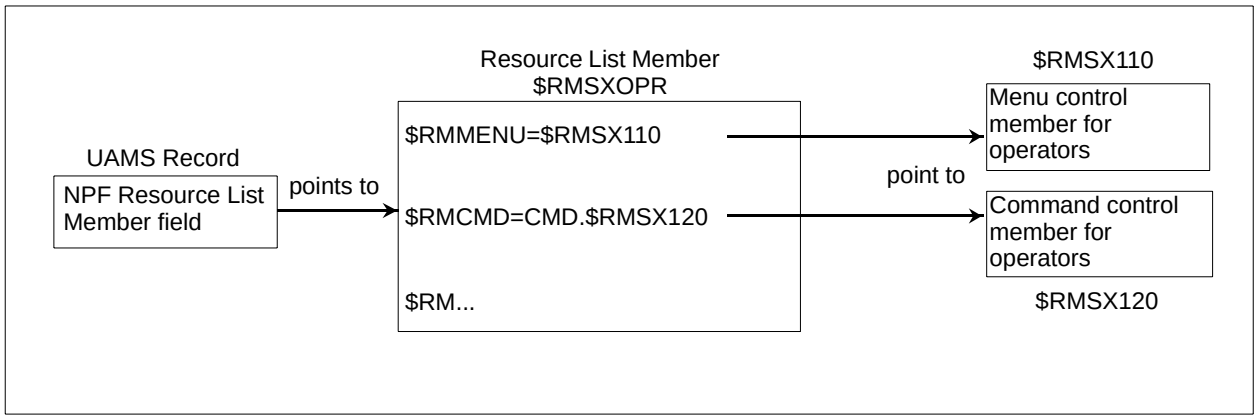
Network Partitioning Facility (NPF)

The facility contains the access permissions for user's requests to menus, resources, or commands. This is enabled when an NPF resource list member is specified in a UAMS ID definition.

By specifying structured strings, access can be restricted or allowed to menu options, databases, system images, commands, and initialization and customization parameter groups. These strings are stored in resource tables and referenced by the NPF resource list members.

Figure 6-1 shows the relationship between UAMS and NPF.

Figure 6-1. Relationship between UAMS and NPF



Your product provides sample NPF members that contain predefined tables that permit or restrict access for different groups of user. These NPF members and their content are shown in Table 6-1. For more information about these members, see the comments within the members.

Caution

The NPF members must have names that start with $RMSX. If you rename a member, ensure that its name has the correct prefix.

Table 6-1. NPF Members—Samples

NPF Member	Content
$RMSXADM	Permissions for administrators
$RMSXOPR	Permissions for operators
$RMSXNOP	Permissions for network operators
$RMSXMON	Permissions for monitors
The following members (with names prefixed by $RMSXS) require an external security package:	
$RMSXSAF	Special indicator—NPF is to be bypassed in favor of an external security package
$RMSXSAD	Permissions for administrators—combined NPF and external security package
$RMSXSOP	Permissions for operators—combined NPF and external security package
$RMSXSNO	Permissions for network operators—combined NPF and external security package
$RMSXSMO	Permissions for monitors—combined NPF and external security package

When a user accesses a menu or tries to issue a command, NPF is called. The region checks the NPF member specified in the user ID definition and its corresponding permissions. The region then responds by showing particular menu options, or allowing or disallowing the command.

By using NPF, you can also restrict certain users to certain groups of resources. For example, one operator can influence all the resources in REGION1 only, while another operator can influence all the resources in REGION2. Any attempt by the first operator to influence the resources in REGION2 will be rejected. The same restriction can apply to the messages from these regions.

Note

The region does not perform read access controls; that is, all users are able to browse all data. Users who attempt to update data they are not authorized to update are presented with a warning message, and the data is not modified.

For more information, see the *Automation Services Administrator Guide*.

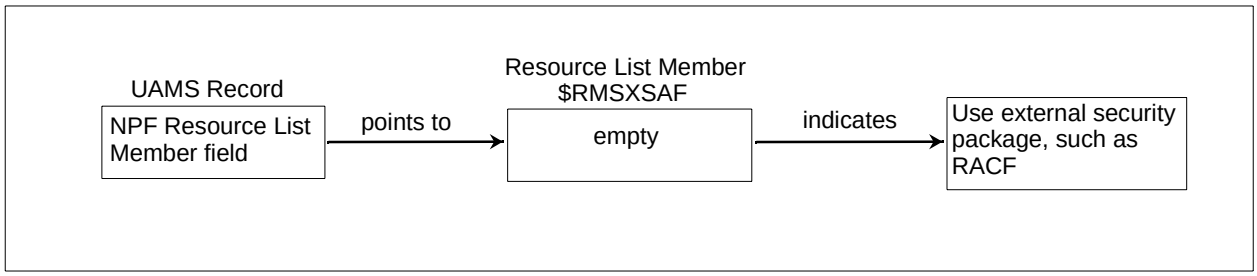
External Security Options

Your external security package can enhanced product security if it supports SAF. It can provide security on its own or in conjunction with NPF. (For more information about external security, see the section, *External Security Packages*, on page 6-13.

SAF contains the access permissions for user's requests to menus, resources, and commands. This is enabled when $RMSXS-prefixed member is specified in the NPF Resource List Member field of a UAMS ID definition.

Figure 6-2 shows the relationship between UAMS and SAF within an external security package. The $RMSXS-prefixed member can either be empty (as shown in the figure) or contain NPF statements. Sample members are listed in Table 6-1 on page 6-4.

Figure 6-2. Relationship Between UAMS and SAF



Sample security profiles are provided for each of the supported external security packages in the *dsnpref*.AS*vvv*.ASSAMP data set, as shown below. *dsnpref* is the data set prefix and *vvv* is the version of Automation Services used by the product. You can copy, customize, and integrate the appropriate profile into your security package.

Security Profile	Content
$RMSXACF	Permissions for all groups of users for CA-ACF2 versions earlier than Version 6
$RMSXAC6	Permissions for all groups of users for CA-ACF2 Version 6 and later
$RMSXRCF	Permissions for all groups of users for RACF
$RMSXTSS	Permissions for all groups of users for CA-Top Secret versions earlier than Version 5
$RMSXTS5	Permissions for all groups of users for CA-Top Secret Version 5 and later

Your external security package is called when a user accesses a menu or tries to issue a command. The region then passes the associated structured string to your external security package as a SAF formatted call. The security package responds by showing specified menu options, or allowing or disallowing the command.

For more information, see the *Automation Services Administrator Guide*.

Security Considerations for Existing Users

If you are using a pre-existing UAMS database, perform the following tasks to ensure that users are properly authorized to operate in the region:

Step 1. Ensure that the group definitions are authorized for TCP/IP.

Step 2. Ensure that the background users are defined by using the $RMBUSER group definition.

Checking Existing User Group Definitions

Ensure that the group definitions are authorized for TCP/IP as follows:

Step 1. Enter the **/UAMS** shortcut to access the UAMS maintenance function.

Step 2. Type **L** at the Select Option ===> prompt and **$RM** in the User field, then press ENTER to list the group definitions.

Step 3. Update each of the $RMADMIN, $RMOPER, $RMNOPER, $RMMON, and $RMBUSER definitions to ensure that the following fields are specified correctly:

Field	Value
Network Management field on the Access Authorities panel (3rd panel)	Y
TCP/IP field on the Network Management Details panel (8th panel)	2

Customizing Existing Background User Definitions

The $RMBUSER group definition for background regions is defined when a NetMaster for File Transfer region starts the first time. The following UAMS background user definitions (where *xxxx* is the domain ID) are also generated and linked to the UAMS group:

User ID	Description
*xxxx*AOMP	AOM procedure
*xxxx*BLOG	Logger
*xxxx*BMON	Monitor
*xxxx*BSVR	Server
*xxxx*BSYS	System
*xxxx*LOGP	Log procedure

Note

The domain ID of the region is specified in the RUNSYSIN member during setup.

If you set up your operations region by using a pre-existing UAMS database in which the background users are already defined for your region, those background user definitions are not replaced. To enable the new region to work correctly, you must update those background user definitions by associating the definitions to the $RMBUSER group ID. You can do this by completing the following steps:

Step 1. Enter the **/UAMS** shortcut to access the UAMS maintenance function.

Step 2. Type **L** at the Select Option ===> prompt and *xxxx* in the User field, then press ENTER to list the background user definitions.

Step 3. Update a required background user ID by entering $RMBUSER in the Group ID field.

Step 4. Press F3 (File) to file the change.

Step 5. Repeat step Step 3 and step Step 4 for each of the background users.

Step 6. After you finish updating the user definitions, enter **CMD** at the Command ===> prompt to access the Command Entry panel, then enter the SUBMIT USER=*background-user-id* SIGNON command for each of the background users to invoke the changes.

The following example invokes the changes for the background logger:

```
SUBMIT USER=xxxxBLOG SIGNON
```

Defining NetMaster for File Transfer Users

Define users in a NetMaster for File Transfer region through the user profiles.

To add a user profile, complete the following steps:

Step 1. Enter the **/ASADMIN.UP** path to display the User Profile List panel.

Step 2. Press F4 (Add) to add a new user profile. The action presents you with the first panel in the user profile definition, the User Description panel.

Step 3. Enter the user ID, password, and name, and assign the user to a security group. See the section, *About Security,* on page 6-2 for a list of the supplied groups.

Note

If you assign a user to a security group, then when you save the profile, a UAMS user ID definition is automatically created.

Figure 6-3 shows an example of a completed panel.

Figure 6-3. User Description Panel

```
SOLVPROD------------Automation Services : User Description --------------------
Command ===> file                                            Function=ADD

. User Description -------------------------------------------------------.
|                                                                          |
| User ID ............ BROWNP__                                           |
| Initial Password ...                                                     |
|                                                                          |
| User Name .......... Peter Brown________                                 |
| User Location ...... Operations_________                                 |
| Telephone Number ... Ext 222_____                                        |
|                                                                          |
| Group ID ..........+ $RMOPER_                                            |
| Group Name ......... Operator Group                                      |
```

Step 4. Press F3 (File) or F4 (Save) to save the new record. (Pressing F3 saves the profile and exits the profile definition. Pressing F4 saves the profile but leaves the definition open so that another profile can be added.)

Note

Once you have defined one user profile, you can use the **C** (Copy) action to duplicate an existing user profile and change the values for another user in the copied record as required.

Managing Users in a Multisystem Environment

If you have implemented a multisystem environment, where several NetMaster for File Transfer regions are linked together, you can define a user in one region and have the user definition copied to the other linked regions.

To enable this feature, you have to customize the SECSHIPPING parameter group.

Implementing User Definition Synchronization Across Linked Regions

To synchronize UAMS records across all active linked regions, you need to enable the automatic propagation facility in all those regions. Do not use this facility if the linked regions share a single UAMS database.

Synchronization depends on whether you make an update from a focal point region or a subordinate region as follows:

If the update is in a …	The update is synchronized across …
Focal point region	All active linked regions that are enabled for this feature.
Subordinate region	Only those active linked focal point regions that are enabled for this feature.

Enabling or disabling the synchronization of UAMS records across multiple regions is the function of the parameter group, SECSHIPPING. Synchronization occurs only between the linked regions in which synchronization is enabled.

To update the parameter group, proceed as follows:

Step 1. Enter the **/ICS** shortcut to display the Customization Parameters panel.

Step 2. Enter **U** (Update) beside the SECSHIPPING parameter group, which is located under the SECURITY category.

Step 3. With the SECSHIPPING - Ship UAMS Maintenance panel displayed, the following settings can be made:

- Respond **YES** to both questions to allow all add, update, delete, *and* password change operations for UAMS records to be propagated to linked regions.
- Respond **NO** to both questions to disable user definition synchronization. If an update is requested from a remote region through this facility, it is refused.

Note

If you respond YES to the question Ship to Linked Systems? and NO to the question Including Password Changes?, password changes are not synchronized. (This setting is for regions that do not share a UAMS database but use the RACF distributed password update facility.)

Synchronization Report

The UAMS database is updated when you update the User Description panel of a user profile and save it. If user definition synchronization is enabled, UAMS updates are sent to the linked regions immediately. A UAMS update report is displayed immediately, indicating the success or failure of those updates. Figure 6-4 shows a sample report.

Figure 6-4. UAMS Update Report

```
SOLVPROD---------- Automation Services : UAMS Update Report -------------------
Command ===>                                  Function=Browse Scroll ===> PAGE

               A UAMS update request was sent to all linked
           regions for user BROWNP with the following results:

Region    Message

SOLV13    RM350008 UAMS ADD PROCESSED SUCCESSFULLY
SOLV14    RM350403 UAMS ADD PROCESSED SUCCESSFULLY
SOLV15    RM350403 UAMS ADD PROCESSED SUCCESSFULLY

****************************** BOTTOM OF DATA ********************************
```

Troubleshooting

Possible reasons for a remote region update not working include the following:

- The region is not profiled for remote updates. To profile it for remote updates, specify **YES** in the Ship to Linked Systems? field of its SECSHIPPING parameter group.
- The link or remote region is not active. (Because UAMS update records are not written to a staging file, no record of the update is retained, and the UAMS record in the remote region is not updated.)
- The user does not have UAMS administration authority on the remote region.
- The record or database is locked.
- The UAMS record does not exist. This condition occurs when you update a user profile record, without providing a new initial password, and there is no associated UAMS record in a remote region. Remedy this by supplying an initial password. This results in the automatic generation of a UAMS record for the remote region, and resets the users password across the other regions.
- You based the user access on a customized user group that does not exist in the remote region.

External Security Packages

External security packages, such as RACF or CA-ACF2, can provide minimal or full security checking.

If your organization has an external security package, access to that package is provided through one of the following types of exit:

- *Partial security exit*—password and logon access maintenance is controlled by the external security package while UAMS stores the user definitions.
- *Full security exit*—all security functions are maintained and stored by your external security package.

The following sample security exits are provided with NetMaster for File Transfer and can be found in the following libraries:

- The SMP target zone library, *dsnpref*.INSTAL
- The SMP distribution zone library, *dsnpref*.BASE.INSTALL

Sample Exit	Description
CCRACFFX	Full security exit for RACF
CCACF2FX	Full security exit for CA-ACF2
NMSAFPX	SAF partial security exit

The NMSAFPX partial security exit is a SAF based security exit that supports UTOKENS. SAF is the IBM System Authorization Facility and is the agreed standard for the encoding of requests that require security checking.

Note

SAF is documented in the IBM *External Security Interface (RACROUTE) Macro Reference for MVS and VM* manual. You should refer to the documentation for your security package to see whether the package supports SAF-formatted calls.

For OS/390 systems, it is recommended that you use the NMSAFPX partial security exit as it supports RACF and CA-ACF2 security packages.

When the exit has been written, link it to create a load module. Place the module in the load library, or another library concatenated to the load library through the STEPLIB DD statement in the started task JCL. Change the JCL parameters to include the SEC={ *load-module-name* } parameter.

See Appendix C, *Security Settings*, for information about the minimum security settings for different types of users.

For further information, see the following manuals:

- The *Management Services Administrator Guide* for information about the security exit support provided by a NetMaster region.
- The *Automation Services Administrator Guide* for information about using SAF samples and NPF.

7

Administering Multisystem Operations

This chapter describes how to establish and maintain your NetMaster for File Transfer multisystem environment.

The chapter contains the following topics:

- Multisystem Operation
- Linking NetMaster for File Transfer Regions
- Keeping Track of Linked Regions
- Unlinking Regions
- Transmitting Records

Multisystem Operation

The NetMaster for File Transfer product provides focal point management to support multisystem operation (that is, management at a focal point with subordinates and agents feeding information to it) as follows:

- Peer-to-peer architecture—supports full connectivity between multiple regions. NetMaster for File Transfer regions linked in this way are known as focal point regions. (A standalone region is also regarded as a focal point region.)

  When regions are communicating with each other, authorized users can monitor and control all managed resources from any terminal connected to any region.

- Subordinate—enables you to reduce the amount of traffic in your multisystem environment. You link subordinates to focal point regions that provide central monitoring and control. A subordinate has visibility and control of the locally managed file transfers and supporting resources only.

- Agent—enables you to manage file transfers and supporting resources on a remote system without having to establish a NetMaster for File Transfer region on that system. A region on another system can manage them through the agent. NetMaster for File Transfer supports agents for AS/400, Tandem, UNIX, and Windows NT systems.

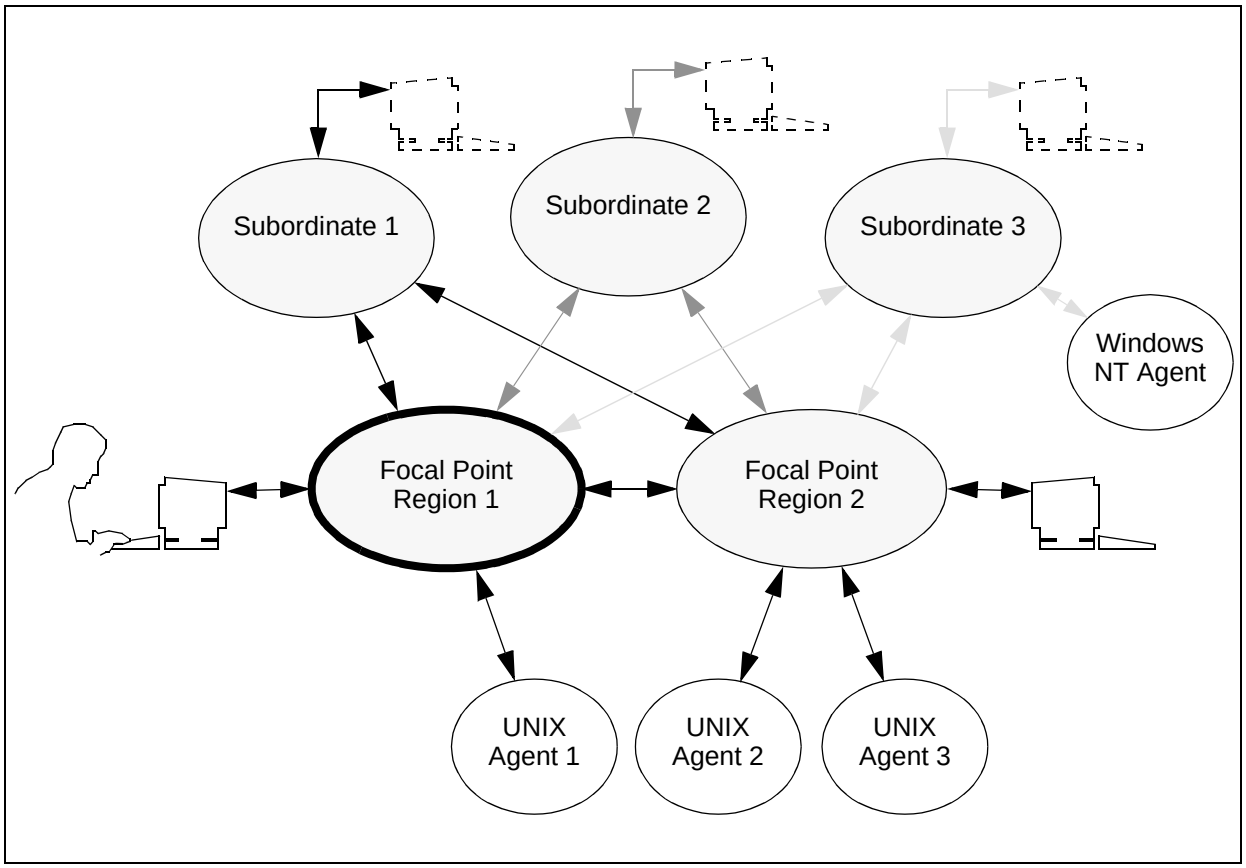
In a multisystem environment, each NetMaster for File Transfer region can run independently of the other regions. If no communication links are available, each region still provides full monitoring, control, and automation of its own managed resources.

To link a focal point region to another focal point region, or to link a subordinate to a focal point region, you need to perform the procedure described in the section, *Linking and Synchronizing Regions*, on page 7-8. To link in an agent, you need to define a file transfer manager resource as described in the section, *Defining CONNECT:Direct Resources*, on page 10-29.

Figure 7-1 shows an example of a multisystem environment, where Focal Point Region 1 is the main monitoring region and Focal Point Region 2 is a secondary region that can serve as a backup. Note the following:

- A focal point region links to all other focal point regions and subordinates.
- A subordinate links to focal point regions but does not link to another subordinate.
- A file transfer agent links to the region that manages the CONNECT:Direct applications with which it interfaces.

Figure 7-1. Multisystem Operation



Links in a Multisystem Environment

The link established between two NetMaster for File Transfer regions in a multisystem environment is an INMC link. The link is used to pass knowledge base updates, status change notification, and other information between the two regions. The link can use any combinations of the following communication access methods: EPS, VTAM, and TCP/IP.

For each region, the communication access methods available to it are specified by the MULTISYS parameter group. By default, the group enables VTAM only. (To access the MULTISYS parameter group, enter the **/ICS** shortcut.)

Note

When a region is linked in a multisystem environment, you cannot change the access methods in its MULTISYS parameter group without first unlinking the region.

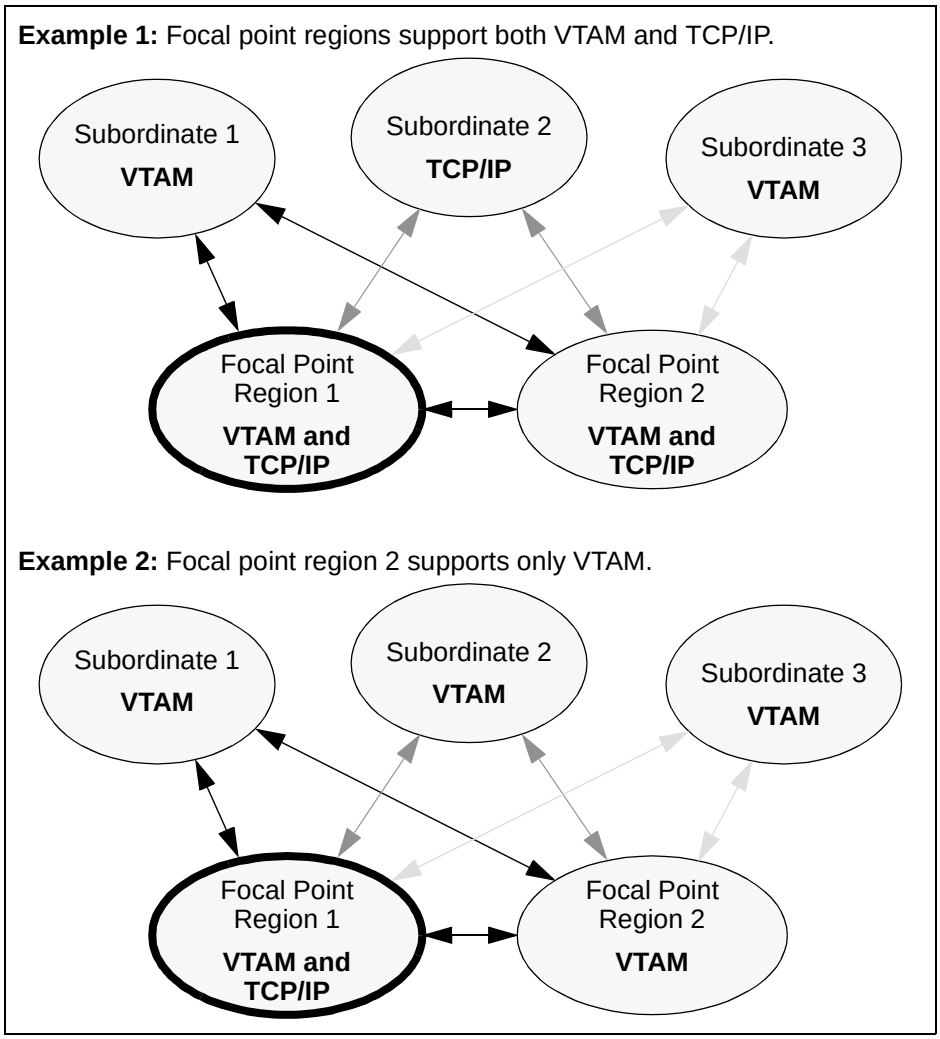
The INMC link between any two regions uses the access methods enabled by *both* regions (that is, the intersection of the two MULTISYS parameter groups). When multiple access methods are enabled, the link can use all these methods. This improves reliability because the link will function so long as one of the enabled methods is available.

When you plan your multisystem environment, you must ensure the following:

- All focal point regions must support at least one common type of access method.
- A subordinate region must support an access method that is also supported in all the focal point regions.

Figure 7-2 shows some examples.

Figure 7-2. Multisystem Link Configurations



Multisystem Support in Sysplex

With the EPS access method, you can use the Sysplex cross-system coupling facility (XCF) to implement your multisystem environment.

Note

To support the EPS access method, a SOLVE SSI region must be active in each of the cooperating systems and must be registered to XCF.

To register the SOLVE SSI region to XCF, add the XCF=YES parameter to the SOLVE SSI.

All participating NetMaster for File Transfer and SOLVE SSI regions must also include the Sysplex feature (INC=(SYSPLEX)) in their RUNSYSIN and started task members respectively.

Multisystem Implementation Considerations

When you implement your multisystem environment, consider the following:

- Ensure that the link requirements are satisfied for the planned multisystem environment (see the section, *Links in a Multisystem Environment*, on page 7-4).
- When you link two regions, the knowledge base in one region overwrites the knowledge base in the other region. Implement your multisystem environment before building up your knowledge base.
- You can link a region to a focal point only. The focal point can be either a standalone region or part of a multisystem environment.
- You can only link a standalone region into a multisystem environment. You cannot link two multisystem environments together.
- For active file transfer monitoring of FTS resources both remote and local background user IDs must be defined to the FTS region.

Establishing Your Multisystem Environment

When NetMaster for File Transfer is installed in your environment, two databases, which form the knowledge base, are downloaded. These databases, which can be tailored to suit your requirements, are:

- An icon panel database, where icon panel definitions are stored
- A database where system image, resource, availability map, process, macro, command, and other definitions are stored (the RAMDB)

Populate these databases with definitions specific to your environment. These definitions may include the system image definitions for any other regions to be installed in your environment in the near future.

As you establish other regions, link the new regions to the first region by using the Link Region and Synchronize Database option. (See the section, *Linking NetMaster for File Transfer Regions*, on page 7-7.) Once the regions are linked, future knowledge base synchronization is automatic. You can make changes to the knowledge base in one region and the changes are sent to the knowledge base in the linked regions.

Note

Synchronization does *not* apply to the NCL procedures represented by the registered commands and macros. Changes to these NCL procedures are *not* automatically reflected in the linked regions.

Linking NetMaster for File Transfer Regions

To build a multisystem environment, you start by linking two regions, then continue on to link in any other regions. The linking process also synchronizes the knowledge bases of these regions.

Note

For linked focal point regions, synchronization is complete and the focal point knowledge bases duplicate each other.

For linked subordinates, synchronization is complete only to the extent of the relevant definitions in the knowledge base. For example, a subordinate knowledge base does not contain all system images. A subordinate knowledge base contains only those images that represent the environment the subordinate is managing.

When you link two regions, the local region in which you perform the link operation receives the knowledge base from the remote region you want to link to, which must also be a focal point region. When you link a region into an existing multisystem environment, that region must be a standalone region.

During the linking and synchronization process, the knowledge base in the local region is overwritten by the knowledge base in the remote region.

Warning

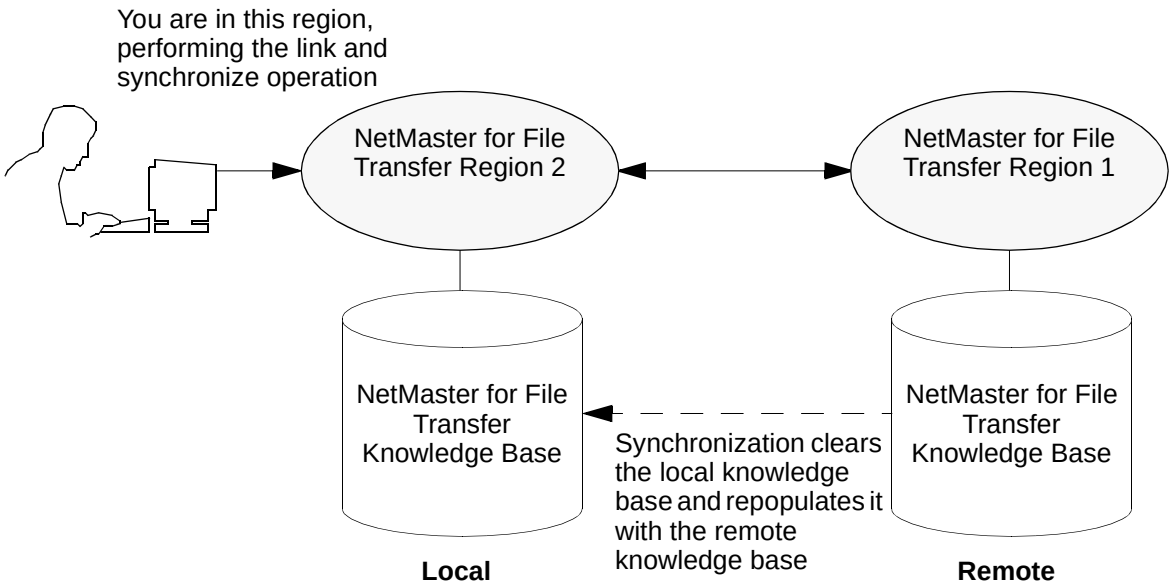
If the local knowledge base has been customized and contains definitions that you want to retain in the synchronized knowledge bases, you must transmit these definitions to the remote knowledge base before you link the regions. See the section, *Transmitting Records*, on page 7-17, for information about how to transmit definitions stored in the knowledge base.

Note

If, for whatever reason, the local region terminates during the linking and synchronization process, the local knowledge base can become corrupted and you might not be able to restart the region. Replace the corrupted knowledge base with your backup. For information about how to back up a knowledge base, see the section, *Backing Up the Knowledge Base*, on page 8-5.

Figure 7-3 shows the link and synchronize operation.

Figure 7-3. Linking NetMaster for File Transfer Regions



Note: The local region can be linked as either focal point or subordinate; the remote region must be a focal point.

After you link the regions, the knowledge bases in them are synchronized and will remain synchronized. If you make changes to the knowledge base in one region, the changes are propagated to the other regions.

Linking and Synchronizing Regions

Caution

Do not add, update, or delete knowledge base records in any linked regions while synchronization is in progress. These changes might not be propagated to the new region.

The procedure for linking and synchronizing the regions is as follows:

Step 1. Log on to the region to be synchronized with the source (remote) region. The source region contains the knowledge base you want.

Step 2. Enter the **/MADMIN** shortcut to display the Multi-System Support Menu. An example is shown in Figure 7-4.

Figure 7-4. Multi-System Support Menu

```
SOLVPROD------- Automatio                                  Menu --------$RM031
Select Option ===>

   TI  - Transmit System
   TS  - Transmit Services
   TC  - Transmit Common Components
   TR  - Transmit Ruleset
   TF  - Transmit File Transfer Ruleset
   LR  - List Linked Regions
   SD  - Link Region and Synchronize Database
   U   - Unlink Region SOLVPROD
   L   - View Task Log
   X   - Exit
```

Enter **SD** here to initiate the link and synchronize operation.

Step 3. Select option **SD** to establish a link between the local region and another region, and to update the knowledge base of the current region.

A Remote System Identification panel is displayed.

Step 4. Supply the details for the operation as follows:

a. Specify the ACB name (primary name) of the remote focal point region to which you want to link this region.

Note

The ACB name of a NetMaster for File Transfer region is specified during the setup of the product (refer to the *Unicenter Mainframe Installation and Setup Instructions*). You can use the SHOW PARMS command to determine the name (refer to the online help).

b. Specify whether this region is a focal point region or a subordinate region. If it is to be a subordinate, specify the name of the system image that is to be used by it. For example, you can use the system ID in the SYSTEMID parameter group as the system image name.

Key Concept

Each subordinate is assigned a unique system image name, and it can use an image by that name only. When you build your file transfer management environment for a subordinate, you must build the environment under the system image name specified during the linking operation.

Focal points cannot use a system image that belongs to a subordinate.

For information about how to define a system image, see the section, *Defining a System Image*, on page 10-4.

c. Enter ***dsnpref.rname*.RAMDB.WORK** in the Work Dataset field, where *dsnpref* is the dataset name prefix you used during the installation of the NetMaster for File Transfer software and *rname* is the name of the local region. Using this dataset speeds up processing significantly.

d. Specify the communication access methods to be used by the INMC link to be established between the regions. You can select any combination of the access methods; however, you can select an access method only if it is allowed in the MULTISYS parameter group.

Figure 7-5 shows an example of a completed panel.

Figure 7-5. Linking NetMaster for File Transfer Regions

```
SOLVPROD------- Automation Services : Remote System Identification ------------
Command ===>                                                Function=SYNCHRONIZE

Identify the Remote Region:
   Primary Name ................. SOLV3       (Must be a FOCAL system)

Role in Multi-System Operation .. SUBORDINATE (Specify FOCAL or SUBORDINATE)
Subordinate System Image Name ... SOLVPROD

Work Dataset .................... ALSO0.SOLVPROD.RAMDB.WORK

Specify the Communication Access Methods to be used by this system:
   Use VTAM? ................... YES
   Use EPS? .................... NO
   TCP/IP Host Name/Addr ........ ALMVS3.AL.XYZ.COM
      Port Number ............... 2636
```

Step 5. After you have specified the details, press F6 (Action) to initiate the linking process.

A confirmation panel is displayed, as shown in Figure 7-6.

Caution

To cancel the synchronization procedure, press F12 (Cancel) now.

Figure 7-6. Confirm Database Synchronization Panel

```
SOLVPROD----- Automation Services : Confirm Database Synchronization ----------


                     SYNCHRONIZE SOLVE:Operations DATABASES

     .-------------------------------------------------------------------.
     |  WARNING: THIS OPTION WILL ERASE ALL DATA IN THE SOLVE:Operations  |
     |    DATABASE AND REPLACE IT WITH DATA FROM THE NOMINATED REGION     |
     |                                                                   |
     |              The SOLVE:Operations database includes:               |
     |                                                                   |
     |                 * The resource definition database                |
     |                 * The ICOPANL panel library                       |
     |                                                                   |
     |    PROCEDURES CURRENTLY ACCESSING THIS DATABASE WILL BE FLUSHED    |
     '-------------------------------------------------------------------'

     Press Confirm key to confirm request, Cancel key to cancel the request



 F1=Help      F2=Split                                          F6=Confirm
                           F9=Swap                             F12=Cancel
```

Step 6. Press F6 (Confirm) to initiate region linking and knowledge base synchronization.

A status panel, shown in Figure 7-7, is displayed.

Figure 7-7. Monitoring the Progress of Knowledge Base Synchronization

```
SOLVPROD-------- Automation Services : Database Synchronization Status --------
Command ===>

  Status .................. ENDED         Task Number .... 0018
  Remote Primary Name ..... SOLV3         Started By ..... USER01
                                          Start Time ..... 13.52.52 07-JAN-1998
                                          End Time ....... 13.55.30 07-JAN-1998
Message


. Icon Panel Library  -------------------------------------------------------.
| Processed Successfully .. 1                                                |
| In Error ............... 0                                                |
'----------------------------------------------------------------------------'

. SOLVE:Operations Database -------------------------------------------------.
| Processed Successfully .. 647           Total Records ........... 647      |
| In Error ............... 0             Percent Complete ........ 100      |
|                                                                            |
| 0                 25                50                75               100 |
|  __________________________________________________________________________ |
| |__________________________________________________________________________| |
'----------------------------------------------------------------------------'
 F1=Help      F2=Split     F3=Exit
                           F9=Swap
```

You can press F3 (Exit) to exit the status panel at any time without affecting the link and synchronize procedure. If you exit early, note the task number for later reference.

Monitoring the Synchronization Procedure

While the synchronization procedure is in progress, the Synchronize Database Status panel is refreshed automatically every 10 seconds, keeping you informed of the progress. This panel can be refreshed manually at any time by pressing the ENTER key.

If you exited the status panel and want to check the status of the synchronization, proceed as follows:

Step 1. From the Multi-System Support Menu, select option **L** to view the administration task log. An example is shown in Figure 7-8.

Step 2. Enter **S** beside the appropriate entry from the log to view the status of the task.

The administration task log may contains up to 50 entries at any given time. Each task is allocated a sequential task number (between 1 and 50) as it commences. When the maximum task number is reached, allocation restarts from one and the oldest status records are overwritten. To delete a completed or failed task from the log, apply the **D** (Delete) action.

Figure 7-8. Multisystem Support—Administration Task Log

```
SOLVPROD----------Automation Services : Administration Task Log ---------------
Command ===>                                                   Scroll ===> PAGE

                                                              S=Select D=Delete
    Task ACB Name Type     Status   % Done Start Time         End Time
    0019 SOLV3    SYNC     RUNNING  50     13.52 07-FEB-1998
    0018 SOLV3    SYNC     ENDED    100    13.52 07-JAN-1998  13.55 07-JAN-1988
    0017 SOLV9    TRAN-CMP ENDED    100    15.44 06-JAN-1998  15.45 06-JAN-1998
    0015 SOLV1    TRAN-CMP ENDED    100    13.53 05-JAN-1998  13.54 05-JAN-1998
    0014 SOLV11   SYNC     ENDED    100    10.02 31-DEC-1997  10.03 31-DEC-1997
    **END**









 F1=Help      F2=Split     F3=Exit                   F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap
```

Background User Considerations

When you establish a region, a UAMS background system user (BSYS) ID for that region is automatically defined. The ID comprises the 4-byte region domain ID, followed by the characters BSYS. For fully functioning communication links to be established between regions, the BSYS user ID of each region must be duplicated in each linked region.

During a link and synchronize procedure, any required BSYS user IDs are defined automatically, provided that the following conditions apply:

- You have UAMS maintenance authority on all the linked regions.
- The linked regions are all working when the request is made.

If either of these conditions does not apply, then any required BSYS user IDs must be defined manually. The simplest way to do this is to copy the BSYS user ID for the current region from the UAMS User Definition List and update the user ID. (To access the UAMS maintenance functions, enter the **/UAMS** shortcut.)

The link and synchronize request is rejected if both of the following apply:

- You do not have UAMS maintenance authority on either the local or the remote region. (The user ID of the person who requests the link and synchronize procedure must be defined on both the local and remote regions.)
- The required BSYS user IDs are not defined on the local or the remote region.

After you perform a link and synchronize procedure, some required BSYS user IDs might not have been defined (due to regions not being active at the time or to you not having UAMS maintenance authority on all regions). Although a theoretical link exists, a true communications link has not been established between those regions that do not contain the requisite BSYS user IDs. Any subsequent updates to those regions will remain on the staging file until the necessary BSYS user IDs are defined.

Keeping Track of Linked Regions

To list the linked regions in your multisystem environment, enter the **/LISTREG** shortcut.

The Linked Regions panel displays the ACB names and brief descriptions of the linked regions (see Figure 7-9). It also displays the status of the data flow traffic managers. Press F11 (Right) to scroll right to display more information.

Figure 7-9. Linked Regions Panel

```
SOLVPROD------------ Automation Services : Linked Regions --------------------
Command ===>                                                  Scroll ===> 10

                                                            S/B=Browse U=Update

    Primary
    Name     Role         Link Name  Short Description
    SOLV13   FOCAL        SOLV13     Link Definition for Region SOLV13
    SOLV14   FOCAL        SOLV14     Link Definition for Region SOLV14
    SOLV15   SUBORDINATE  SOLV15     Link Definition for Region SOLV15
    **END**
```

You can apply the following actions to listed items:

- **B** to browse a link description (see Figure 7-10)
- **U** to update a link description or a (region identifier) message prefix

Figure 7-10. Browsing a System Link Definition

```
SOLVPROD------------ Automation Services : Link Record Details ----------------
Command ===>                                                   Function=Browse

  Primary Name ........ SOLV13         Link Name ....... ALFT
                                       Message Prefix... SV13A
  Short Description ... Link Definition for Region SOLV13
  Long Description .... This is a SOLVE:Operations for File Transfer region.



. System Details ------------------------------------------------------------.
| System Name ............ SOLV13           Version ............ 0001        |
| Role in Multi-System ... FOCAL            Subordinate Image .. -           |
| SMFID .................. AL01                                             |
| Access Methods: VTAM? .. YES         EPS? ... YES      TCP/IP? ... YES     |
|     TCP/IP Port ........ 2613                                              |
|     Host Name/Addr ... ALMVS1.AL.STATE.COM                                 |
. Traffic Status ------------------------------------------------------------.
| Data ................... ACTIVE                                           |
| Resource Events ......... ACTIVE     Service Events .......... ACTIVE      |
| Shared Events .......... -           File Transfer Events .... ACTIVE      |
'----------------------------------------------------------------------------'
 F1=Help      F2=Split     F3=Exit      F4=Edit
                           F9=Swap
```

Unlinking Regions

You might want to unlink a region from the other regions in a multisystem environment (for example, for maintenance purposes). If a region is no longer of use and you want to remove it from the system, make sure you unlink it first. An unlinked region becomes an isolated region.

Unlink a region as follows:

Step 1. Log on to the region you want to unlink.

Step 2. Enter the **/MADMIN.U** path.

The Confirm Unlink Panel is displayed (as shown in Figure 7-11).

Caution

To cancel the unlinking procedure, press F12 (Cancel) now.

Figure 7-11. Confirming a Region Unlink Operation

```
SOLVPROD-------------- Automation Services : Confirm Unlink ------------NET001


                           CONFIRM UNLINK OF SOLV13

     .-------------------------------------------------------------------.
     | WARNING: The unlinking of SOLV13 will result in its ISOLATION     |
     |          from all other regions.                                  |
     |                                                                   |
     | Once unlinked, you will not be able to monitor or control other   |
     | region's resources from this region and you will not be able to   |
     | monitor or control this region's resources from any other region. |
     |                                                                   |
     | To reconnect this region to another SOLVE:Operations region after |
     | unlinking you will need to perform database synchronization.      |
     '-------------------------------------------------------------------'

     Press the Enter key to unlink.
     Press the Cancel Key to cancel the request.

                 Press ENTER to unlink the region.

 F1=Help      F2
                           F9=Swap                              F12=Cancel
```

Step 3. Press ENTER to proceed with the unlinking procedure.

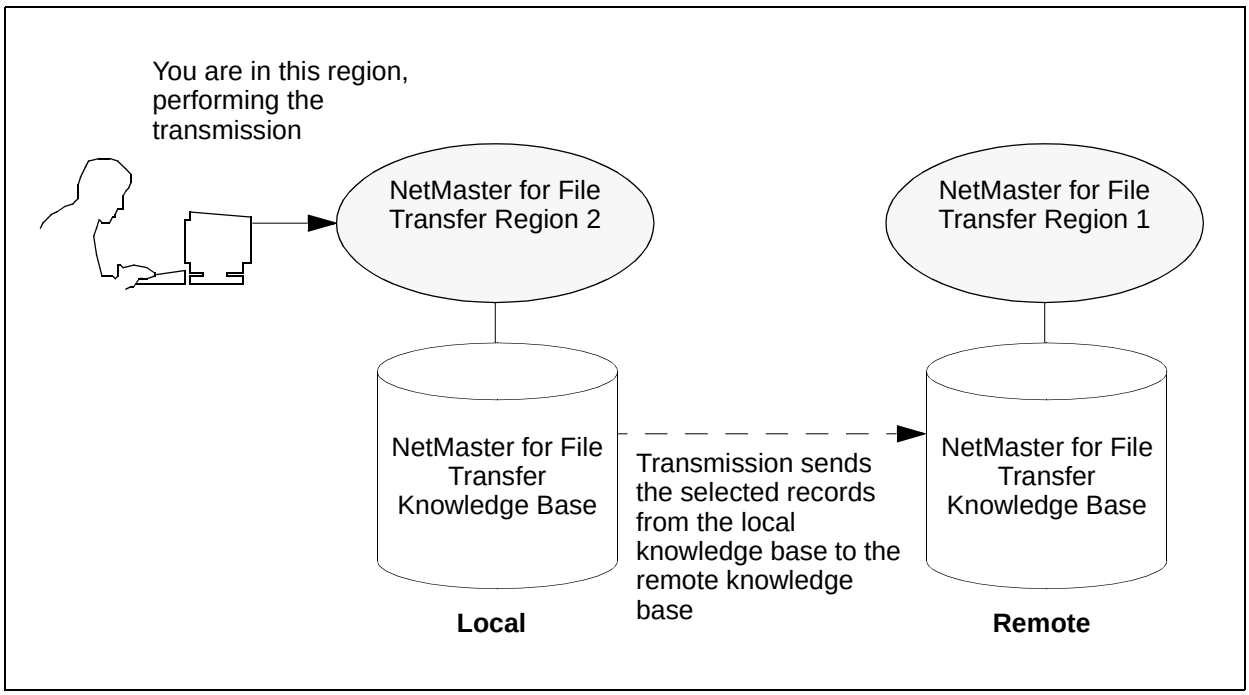
To relink a region, link that region with one of the regions in the multisystem environment. See the section, *Linking NetMaster for File Transfer Regions*, on page 7-7 for this procedure.

Transmitting Records

You can transmit (that is, copy) knowledge base records from the local region to a remote region that is *not linked* to it. You should not transmit records between linked regions because their knowledge bases are already synchronized.

Figure 7-12 shows the transmit operation.

Figure 7-12. Transmitting NetMaster for File Transfer Knowledge Base Records



Transmit knowledge base records as follows:

Step 1. Log on to the region from which you want to transmit the records.

Step 2. Enter the **/MADMIN** shortcut to display the Multi-System Support Menu.

Step 3. Specify the option you require in the Select Option ===> field.

Step 4. Press ENTER to display a Remote System Identification panel.

Step 5. Specify the ACB name (primary name) of the region to which you want to transmit records.

Step 6. If you specified the TI, TS, TR, or TF option, continue with this step. If you specified any other transmission options, go to the next step:

If you want to select the …	**Complete the …**
TI - Transmit System Image option	System Name and Version fields.
TS - Transmit Services option	Version field.
TR - Transmit Ruleset option or the TF - Transmit File Transfer Ruleset option	Ruleset Name field.

Step 7. Specify the transmission mode as follows:

If you want to …	**Specify …**
Replace a set of records, such as a system image, a rule set, *all* services, or *all elements* of a component	**REPLACE** in the Transmission Mode field.
Update a region by adding new records, without updating existing records	**MERGE** in the Transmission Mode field.
Update a region by adding new records *and* updating existing records	**OVERLAY** in the Transmission Mode field.

Step 8. Specify the communication access methods to be used for transmitting the selected records. You can enable any combination of the access methods.

Step 9. Press F6 (Action) to select the specified option. What you do next depends on the specified option and transmission mode.

Step 10. If a selection list is displayed, continue with this step. If the Confirm Transmit panel is displayed, go to Step 12.

If you selected …	**And the transmission mode is …**	**Then …**
Option **TC** - Transmit Common Components	REPLACE	A list of all the common component categories is displayed. To select all definitions in a category for transmission, enter **S** (select) beside it.
	MERGE or OVERLAY	A list of all the common component categories is displayed. To select all definitions in a category for transmission, enter **S** (Select) beside it. To select specific definitions in a category for transmission, enter **L** (List) beside the category to list the definitions, then enter **S** (Select) beside the definitions to be transmitted. After you have made your selections, press F3 (Exit) to return to the Common Component List panel.
Other transmission options	MERGE or OVERLAY	A selection list is displayed. To select all definitions for transmission, press F4 (All). To select specific definitions for transmission, enter **S** (Select) beside the definitions to be transmitted.

Step 11. When you have selected all the definitions you want to transmit, press F6 (Transmit) to request transmission.

A Confirm Transmit panel (displaying the transmission details you entered) is displayed before transmission is initiated. At this point, you have the option of confirming or cancelling your transmission request.

Step 12. Press ENTER to confirm transmission or F12 (Cancel) to cancel the transmission.

If you press ENTER to confirm transmission, a status panel is displayed, showing the progress of the transmission. If you choose to exit the status panel, you can check the status of the task subsequently by viewing the administration task log. Before you exit, note the task number for future reference. (See the section, *Monitoring the Synchronization Procedure*, on page 7-13 for information about the administration task log.)

If you press F12 (Cancel) to cancel the transmission, you are returned to the Multi-System Support menu.

8

Maintaining the Product

This chapter describes the NetMaster for File Transfer maintenance tasks.

The chapter contains the following topics:

- Starting a NetMaster for File Transfer Region
- Shutting Down a NetMaster for File Transfer Region
- Maintaining the Activity Logs
- Backing Up the Knowledge Base

Starting a NetMaster for File Transfer Region

To start the region, start your NetMaster for File Transfer started task, as implemented during the installation and setup phase of the product.

If you want to monitor CONNECT:Direct, CONNECT:Mailbox, or FTP file transfers, ensure that the SOLVE SSI that provides the event delivery facility is active. If the facility is not available, the region cannot receive those file transfer events and will be unable to monitor those transfers. For information about how to set up the event delivery facility (which uses EPS), see the *Unicenter Mainframe Installation and Setup Instructions*.

If you are using agents to pass events and commands between the region and remote systems, ensure that the agents are properly installed and configured. For information about how to install and configure an agent, see the corresponding manual for the agent.

Shutting Down a NetMaster for File Transfer Region

You can shut down a region by issuing commands from its Command Entry panel. To display the panel, enter **CMD** at a ===> prompt.

If you have the necessary authority, you can shut down the region by issuing the SHUTDOWN or FSTOP command.

Shutting Down a Region in an Orderly Manner

To shut down a region in an orderly manner, enter **SHUTDOWN** on the Command Entry panel.

The SHUTDOWN command only stops the region when the last user logs off. When you issue the SHUTDOWN command, a broadcast is issued to all users. No further logons are accepted until the region is restarted, or the SHUTDOWN CANCEL command is issued.

Shutting Down a Region Immediately

To shut down a region immediately, enter **FSTOP** on the Command Entry panel.

The FSTOP command immediately disconnects all user sessions and shuts down the region.

Bringing Down the SOLVE SSI Started Task

To shut down the SOLVE SSI started task used by the region, enter **SSI STOP** on the Command Entry panel.

Stopping the SOLVE SSI started task might cause AOM to be inactivated.

Warning

Before shutting down the SOLVE SSI started task, ensure that the SSI is not used by another region.

Maintaining the Activity Logs

The activity log records all the activities that occur within a NetMaster for File Transfer region. Your region can have more than one log file available for logging these activities. (For information about how to allocate additional log files, see the section, *Allocating Activity Log Files*, on page 5-25.)

By default, the region writes to the log files in a cyclic sequence. When the current file is full, the region starts logging to the next file, and so on (that is, files are swapped automatically). When all files are full, the first file is cleared and reused. (The LOGFILES parameter group contains information about these files.)

Under certain circumstances, you might want to direct logging to a different file before the current file is full (for example, to separate system maintenance activities from records logged during normal operation).

Swap the log files manually as follows:

Step 1. Enter the **/LOGSWAP** shortcut to clear the next file in the sequence and start logging to the new file.

A confirmation panel, shown in Figure 8-1, is displayed.

Figure 8-1. Confirming an Activity Log Swap

```
SOLVPROD------------ Automation Services : Confirm Swap Log ------------------
Command ===>

                                    SWAP LOG
.-----------------------------------------------------------------------------.
| This action will swap activity logging to the next defined log file.        |
|                                                                             |
| The new log will be emptied before swapping.  If only one log has been      |
| defined, it will also be emptied.                                           |
|                                                                             |
| Any procedure that is currently accessing the log file may be flushed by    |
| this operation.                                                             |
'-----------------------------------------------------------------------------'

  Press the Enter key to confirm the request or the Cancel key to cancel
```

Press ENTER to swap the activity log.

```
 F1=Help      F2=Split
                           F9=Swap                              F12=Cancel
```

Step 2. Press ENTER to confirm the swap.

Backing Up the Knowledge Base

The method you select for backing up the knowledge base depends on the configuration of your NetMaster for File Transfer regions and your operations requirements.

Backup methods depend on whether your regions are:

- Non-production regions
- Production regions

Non-production Regions

With non-production regions, you should be able to shut down a region to perform the backup.

Production Regions

With production regions, it is likely that you cannot shut down a region for backup. However, you can create a backup region and link it to the production regions. During the linking process, the knowledge base in the backup region is updated by the production knowledge base.

Implement the backup region as follows:

Step 1. Create the backup region.

Note

Ensure that the knowledge base of the backup region is not on the same DASD as the production knowledge bases.

Step 2. In the backup region:

a. Enter the **/RADMIN.I** path to display the System Image List panel. Press F4 (Add) to create a system image definition, then enter **L** beside it to load the empty image.

b. Enter the **/ICS** shortcut to list the parameter groups, and update them as follows:

In the …	Enter …
AUTOIDS parameter group	The name and version of the empty system image in the System Image Name and Version fields to enable the image to be loaded automatically on subsequent region startups.
FTLOGS parameter group	**NO** in the Is logging required? field to disable logging of file transfer events.
EVENTLOG parameter group	**NO** in the Enable Event Logging field to disable recording of file transfer events in the EVNTDB database.
FTPCNTL parameter group	**NO** in the Enable FTP Event Receivers field to disable the FTP event flow.

Step 3. Enter the **/MADMIN** shortcut to display the Multi-System Support Menu.

Step 4. Supply the ACB name of a production region to link to and the name of the work dataset, then select **SD** to link the backup region as a focal point to the named production region.

The backup region does not perform any automation, it just contains an up-to-date, mirror image of the production knowledge base. Therefore, you can shut down the region to back up its knowledge base. Any knowledge base updates that occur while the region is shut down are held by the staging file. These updates are sent to the region when it is restarted.

Part III

Operations

9

Getting Started

You interact with the NetMaster for File Transfer region through a user interface that comprises menus, lists, and data entry panels.

This chapter contains the following topics:

- Accessing and Leaving the NetMaster for File Transfer Region
- Changing Your Password
- The Menus
- Accessing Functions
- Using Lists
- Using Data Entry Panels
- Working with Definitions in the Knowledge Base
- Getting Help
- Working in Two Windows

Accessing and Leaving the NetMaster for File Transfer Region

You might have access to one or more regions. This depends on whether your organization has set up a single system or a multisystem environment.

To access the region, you must log on to it. The logon procedure is the same whether you are logging on in a single system or a multisystem environment. Before you can log on to a region, you need a user ID and password. Ensure that your system administrator has defined your user ID to the region and has allocated the relevant level of authority.

Logging On

Log on to a region as follows:

Step 1. Enter **LOGON APPLID(***acb-name***)**, using the ACB name of the region.

Step 2. Type your user ID and password on the displayed logon panel, and press ENTER. Figure 9-1 shows an example of the primary menu that is displayed.

Figure 9-1. The Primary Menu

```
SOLVPROD-------------- Unicenter NetMaster : Primary Menu ---------------------
Select Option ===>

   M   - Monitors                                              Userid USER01
   H   - Historical Data                                       LU     NMMAF011
   U   - User Services                                         Time   16.20.46
   O   - Operator Console Services                             WED 23-MAY-2001
   A   - Administration and Definition                         OPSYS  OS390
   X   - Terminate Window/Exit                                 Window 1









Tip of the day: Put cursor here, press F1(help) to get help on Tips of the day.

  (C) 1981,2001 Computer Associates International, Inc. All Rights Reserved.
 F1=Help      F2=Split     F3=Exit      F4=Return
                           F9=Swap
```

If Region Initialization Is Still in Progress

If the Initialization in Progress panel is displayed on your screen instead of the primary menu, the initialization of the region is still in progress. Press F3 (Exit) to exit to the primary menu.

If the System Image Is Still Being Loaded

If the local system image is still being loaded, the primary menu contains the LS option. You can select the option to monitor the loading process. You can also perform functions that do not depend on an active local system image (for example, working with knowledge base definitions).

Logging Off

To log out of the region from any panel, enter **=X** at the ===> prompt. This ends your current window.

If you are at the primary menu, enter **X** at the Select Option ===> prompt to end your current window.

Note

You can have two windows for each logon to a region. If you have two windows, repeat the procedure to end the remaining window to log off from the region.

The section, *Working in Two Windows*, on page 9-22 describes how to use the two session windows.

Changing Your Password

Your password for logging on to a region is verified by the User Access Maintenance Subsystem (UAMS).

The subsystem lets you change your password, or prompts you to change your password when it has expired after a period of time. You can change your password at any time after you log on to a region. The change becomes effective for subsequent logons.

Note

Your installation might have linked UAMS with an external security system, such as Resource Access Control Facility (RACF). If this is the case, your system administrator will tell you of any special considerations that apply when changing your password.

In a multisystem environment, the administrator might have set up the environment for the synchronization of UAMS user definitions and passwords. Changed passwords are then synchronized across linked regions.

Change your password to the region as follows:

Step 1. Enter the **=U.P** path at a => prompt to access the User Password Maintenance panel. Figure 9-2 is an example.

Figure 9-2. User Password Maintenance Panel

```
USER01---------------- UAMS : User Password Maintenance ------------Page 1 of 2
Command ===>                                                Function=Request

User ID ........................ USER01

Current Password ...............
New Password ...................
```

Type your passwords here.

Note

You can press F12 (Cancel) to cancel the operation at any time before Step 4.

Step 2. Type your current password in the Current Password field and the new password in the New Password field. The fields do not display the entered information.

Step 3. Press F3, and then reenter the new password in the displayed Re-enter New Password field.

Step 4. Press F3 (File) to file the changed password.

If UAMS synchronization is enabled, a Linked Regions UAMS Update Report panel is displayed when you save your changed password. The panel reports the success or failure of the password change in the linked regions.

If synchronization fails, ask the administrator to reset your password when the problem is corrected.

The Menus

The user interface includes several menus. The region issues an error message if you try to use a function that you are not authorized to use.

Note

In a multisystem environment, the following menus are not applicable in subordinate regions: the Service Administration menu and the System Console Consolidation menu.

Table 9-1 shows the hierarchy of the menu panels. Shortcuts to the menu options are shown in parentheses. For information about shortcuts, see the section, *Selecting a Function Directly—Using Shortcuts*, on page 9-8.

Table 9-1. Primary Menu Hierarchy

M Monitors	A	Alert Monitor (ALERTS)		
	R	Resource Monitor (RMON)		
	S	Service Monitor (SMON)		
	G	Graphical Monitor (GMON)		
	FT	File Transfer Resource Monitor (FTMON)		
	AFT	Active File Transfer Monitor (AFTMON)		
H Historical Data	A	Alert History (ALHIST)		
	F	File Transfer History (FTHIST)	B	Browse Event and Transfer Details
			P	Print Event and Transfer Details or Summaries
			EX	Extract File Transfer Events to Dataset
			BS	Browse Schedule Details
			PS	Print Schedule Details or Summaries
			ER	File Transfer Exception Reporting
	L	Activity Log		
U User Services	M	Display Product Message Help		
	P	Password Change for Your User (CHGPWD)		
	UP	Update Your User Profile		
	B	Review Broadcasts		
O Operator Console Services				

Table 9-1. Primary Menu Hierarchy

A	**Administration and Definition**	A	Alert Monitor Administration (ALADMIN)	
		R	Resource Administration (RADMIN)	R Resources
				A Availability Maps
				P Processes
				GP Global Processes
				I System Images
				T Template Definition Menu
				AD Assisted Resource Definition Menu
		S	Service Administration (SADMIN)	S Services
				A Availability Maps
				GP Global Processes
				SI Service Image
		E	Event Administration (EADMIN)	S Status
				R Rule Definition
				L Message Learning
				C System Console Consolidation
				E Event Simulation
		G	Graphical Monitor Administration (GADMIN)	I Icons
				G Resource Groups
				P Icon Panels
				E Raw Icon Panels
		M	Multi-System Support Administration (MADMIN)	
		FT	File Transfer Administration (FTADMIN)	P Maintain FTP Policies*
				R Maintain File Transfer Rulesets
				F File Transfer Monitor Filters
				L File Transfer Monitor List Formats
				E File Transfer Exception Report Filters

Table 9-1. Primary Menu Hierarchy

A	**Administration and Definition (continued)**	AS	Automation Services Administration (ASADMIN)	UP	User Profiles
				R	Reporting
				LS	View System Image Load Status
				MIG	Invoke RAMDB Migration Utility
				P	Field Prompt Lists
				A	Display Attribute Tables
				GPI	Global Processes Images
				C	Commands
				M	Macros
				S	Logon Scripts
				F	Status Monitor Filters
				L	Status Monitor List Formats
				CC	Calendar Criteria
		MS	Management Services (MS)		
		IN	Initialization and Customization Services (INIT)		

*The Maintain FTP Policies option is available only if you are licensed for the TCPaccess FTP feature.

Accessing Functions

You access functions in the region through the user interface menus by doing one of the following:

- Selecting an option from each menu that leads to the function
- Specifying the shortcut to go to the function directly
- Specifying the path to go to the function directly

The difference between accessing a function by using an option and by using the other methods is this: an option can be entered only on the menu on which you see it, whereas a path or shortcut can be entered from other panels—the primary menu, the menu it appears on (in which case it is exactly equivalent to accessing the function by using its option), or a panel on which it does not appear.

Selecting an Option

You select an option by typing the option code at the Select Option ===> prompt and pressing ENTER. For example, typing **A** at the Select Option ===> prompt on the primary menu and pressing ENTER takes you to the Administration primary menu.

Selecting a Function Directly—Using Shortcuts

You can jump to the panel of a function directly by using shortcuts. You can specify the shortcut at an ===> prompt in one of the following ways:

- Specify /*shortcut-name* to retain the current panel on return (panels nested).
- Specify =/*shortcut-name* to close the current panel and return to the primary menu on return.

Table 9-1 on page 9-5 summarizes the functions provided by the product. Each entry in the list is preceded by a one- to three-letter option, and may be followed optionally by a shortcut.

If you do not remember a shortcut, enter / or =/ to list the shortcuts from which you can select one.

Accessing a Function by Using /*shortcut-name*

Caution

If your current panel does automatic updates and you no longer need this information, use =/*shortcut-name* rather than a nested shortcut. This saves storage and resources because the region does not need to maintain a display that you no longer need.

To select the function you want, enter its corresponding shortcut, preceded by the slash (/) character, at a ===> prompt, and press ENTER.

For example, to access the Resource Administration menu, type **/RADMIN** at the ===> prompt on your current panel, and press ENTER. When you have finished with the menu, press F3 to redisplay your previous panel.

When you access a function by using its shortcut, your current panel is retained. When you press F3 to exit out of the function, this panel, with any updates, is restored. By using shortcuts, panels can be nested to a maximum of 64 levels.

Accessing a Function by Using =/*shortcut-name*

Whenever you have finished with your current panel, you can access the next function by prefixing the shortcut call with the equals (=) sign. This goes directly to the function without retaining the current panel and closes all other nested panels in this window.

For example, to access the Resource Administration menu without retaining the current panel, type **=/RADMIN** at the ===> prompt on your current panel, and press ENTER. When you have finished with the menu, press F3 to display the primary menu.

Accessing a Function That Does Not Have a Shortcut

You can combine a shortcut with option codes to form a path to access a function that does not have a shortcut itself. For example, to access the list of resource definitions, you can enter the /RADMIN.R path.

Selecting a Function Directly—Skipping Panels

You can jump to the panel of a function directly by specifying the exact path to that panel. Construct the path by linking the options you need with periods. Depending on which panel you start from, you specify the panel path in one of the ways described in the following sections.

Accessing a Panel That Is Lower in the Panel Hierarchy

If you start from a menu and want to access a panel lower in the panel hierarchy, specify the path as it is. For example, if you are at the primary menu and want to access the Resource Administration menu, type **A.R** at the Select Option ===> prompt and press ENTER.

Accessing a Panel That Is Higher in the Panel Hierarchy

If you want to access a panel that requires you to pass through a panel higher up in the panel hierarchy, you must precede the path specification with the equals sign (=). The = character brings you back to the primary menu and then to the required panel. You can specify such a path at any ===> (or =>) prompt. For example, if you are at the resource monitor and want to access the Resource Administration menu, type **=A.R** at the Command ===> prompt and press ENTER.

For a list of useful panel paths, see Table A-1 on page A-2.

To return to the primary menu, enter **==**.

Accessing a Panel That Requires Input Data

If you want to access a panel that requires you to enter data, you can enter the data by separating them from the path by a semicolon (;). For example, if you are at the primary menu and want to access the resource definitions in Version 1 of the FT1 system image, type **A.R.R;FT1;1** at the Select Option ===> prompt and press ENTER.

Using Lists

Lists comprise a series of items from which you can make a selection, or against which you can apply actions. The fourth line on a panel describes the actions that can be applied to the listed items.

There are four types of lists:

- Action lists allow you to apply *actions* to one or more listed items. Enter the required action code beside the appropriate records.
- Single select lists allow you to select one item from a list (for example, the list of valid values for a data entry field) by:
  - Entering the **S** (Select) action code beside the item
  - Moving the cursor to a position anywhere in the line containing the item you want to select and pressing ENTER
- Multiple select lists allow you to select one or more items in a list.
- Numbered lists allow you to select a single item from the list by entering the appropriate number at the ===> prompt.

If a list is longer or wider than one panel, you can scroll vertically or horizontally, as appropriate.

Scrolling

When the listed information cannot fit onto the screen, use scrolling to access the off-screen information. You can scroll vertically and horizontally.

Scrolling Vertically

Use the F8 (Forward) or F7 (Backward) function key to scroll the displayed information forward or backward by the amount displayed at the Scroll ===> prompt. Table 9-2 shows the valid scroll amounts.

Table 9-2. Valid Scroll Amounts For Scrolling Vertically

Scroll Amount	Action
C (or CSR)	If scrolling forward, the line on which the cursor is currently positioned is moved to the top of the screen. If scrolling backward, the line on which the cursor is currently positioned is moved to the bottom of the screen.
D (or DATA)	The display is scrolled one full page, less one row, in the specified direction. If scrolling forward, the last line of the current page is displayed as the first line on the next page. If scrolling backward, the first line on the current page is displayed as the last line on the next page.
H (or HALF)	The display is moved half a page in the specified direction.
M (or MAX)	The display is moved to the beginning or the end of the displayed information, depending on the function key (F8 or F7) used.
P (or PAGE)	The display is moved one full page in the specified direction.
n	The display is moved *n* lines in the specified direction.

You can also enter a temporary scroll amount at the Command ===> prompt (for example, Command ===> 5). When you press the F8 (Forward) or the F7 (Backward) function key, the displayed information is scrolled by the specified value *once only.*

Scrolling Horizontally

Use the F11 (Right) or F10 (Left) function key to scroll the displayed information to the right or to the left.

Searching for an Item in Retrieved Information

You can search for specific items in the retrieved information by using the F5 (Find) function key or the LOCATE command.

Using the F5 (Find) Function Key

The F5 (Find) function key enables you to find a particular occurrence of text in the retrieved information. Enter the text you want to find, and press F5. If the text contains more than one word, enclose the text in quotation marks. For example, to find the text, LISTENER TASK, enter **'LISTENER TASK'**, then press F5.

You can press F5 again to find the next instance of the text, and so on.

You can also use the FIRST or LAST operand to enable you find the first or last occurrence of the specified text. For example, to find the last occurrence of the text, LISTENER TASK, enter **'LISTENER TASK' LAST**, then press F5.

Expanding the Scope of the Find Function

To expand the scope of the Find function so that the search extends beyond the columns currently displayed, use the following commands:

- FMODE ALL—sets Find to search columns to the left and right of the columns displayed.
- FMODE DEFAULT—restores the standard Find function.
- FMODE—displays the current settings.

Changing the Frequency of the Records Searched Prompting

To change the frequency of the records searched prompting, use the following commands:

- FPROMPT—displays the current setting.
- FPROMPT NO—suppresses the prompt.
- FPROMPT DEFAULT—restores the prompt to its default setting.
- FPROMPT *nnnn*—displays the prompt when the number of records searched exceeds *nnnn*.

Restoring the Default Find Function

To restore the default values, use the following commands:

- RESET ALL—restores the default values of FMODE and FPROMPT.
- RESET FMODE—restores the default value of FMODE.
- RESET FPROMPT—restores the default value of FPROMPT.

The LOCATE command enables you to locate a particular record in a list. Enter **LOCATE** or **L** followed by the first few characters of the record name. The command locates the first record name in the sort field that starts with those characters. Figure 9-3 shows you how to locate a record in a list where the XCMON Name value starts with the letter P.

Figure 9-3. Locating a Record in a List

```
SOLVPROD----------------- ResourceView : XCOM Monitor List ------------------18
Command ===> L P   Press ENTER.                                Scroll ===> PAGE

. System Image -------------------------------------------------------------.
| System Name ...+ SOLVPROD     Version ...+ 0001                            |
'------------------------------------------------------------------------------'
. Resources ----------------------------------------------------------------.
|                                       S/B=Browse U=Update C=Copy D=Delete |
|     XCMON Name         Description                                        |
|     ALXC1.IPLISTEN     TCP/IP listener task monitor - AL                  |
|     ALXC1.STALLED      Stalled transfer monitor - AL                      |
```

```
SOLVPROD----------------- ResourceView : XCOM Monitor List ------------------18
Command ===>                                                   Scroll ===> PAGE

. System Image -------------------------------------------------------------.
| System Name ...+ SOLVPROD     Version ...+ 0001                            |
'------------------------------------------------------------------------------'
. Resources ----------------------------------------------------------------.
|                                       S/B=Browse U=Update C=Copy D=Delete |
|     XCMON Name         Description                                        |
|     PAXC1.IPLISTEN     TCP/IP listener task monitor - PA                  |
|     PAXC1.STALLED      Stalled transfer monitor - PA                      |
|     PAXC1.SUSPEND      Suspended transfer monitor - PA                    |
```

Using Data Entry Panels

Each record in the NetMaster for File Transfer knowledge base is displayed and maintained through a sequence of panels on which you enter the data for that record.

Switching to UPDATE Mode

Many definition panels enable authorized users to switch from the BROWSE mode to the UPDATE mode by pressing F4 (Edit). You can then edit the displayed information.

Entering Data

On a color screen, mandatory fields that you must complete are colored white. Optional fields, which you can complete as and when required, are colored turquoise. Both types of fields can be prompted fields that provide you with a list of valid values, from which you can choose one.

Prompted Fields with List of Valid Values

Many fields on the data entry panels are linked to lists containing the values that you can choose for the field. These fields are called prompted fields. Most, but *not* all, prompted fields are identified by a plus sign (+).

Enter **?** in a prompted field to display the value list, which could be either a numbered list or a single select list.

You can prefix the question mark (?) with one or more characters. The displayed list is then restricted to values that start with those characters. For example, S? displays a list of values that start with S.

Validating and Filing Data

During data entry, you can press ENTER to validate your data. Validation also occurs when you try to:

- Access another panel (for example, when you press F8 (Forward) to access the next panel)
- Save your entered data (for example, when you press F3 (File) to save a definition)

When you have finished entering data, you can do one of following:

- Press F3 (File) to save the data and return to the previous panel.
- Press F4 (Save) to save the data and remain on the panel. When adding definitions, this enables you to quickly create other similar definitions, minimizing the typing required.
- If you do *not* want to save the data, press F12 (Cancel) to return to the previous panel.

Moving Between Panels

Some functions lead to a series of data entry panels (for example, when you update a resource definition).

You can use one of the methods described in the following sections to move through these panels, depending on what you need to do.

Selecting All Panels

You might want to access every panel. All the panels are listed on a panel display list (for example, the panel that lists the resource definition panels). Enter **S** beside the name of the panel you want to access first, or enter the number that identifies that panel in the panel sequence at the Command ===> prompt (for example, 1 for the first panel). The selected panel is displayed.

Press F8 (Forward) to scroll forward to the next panel; press F7 (Backward) to scroll backward to the previous panel.

When you finish entering the data, press F3 (File) to save the data. Press F12 (Cancel) if you decide not to save the data.

Selecting Specific Panels from the Panel Display List

You might want to access certain panels only (for example, when you want to update only certain parts of a resource definition). All the panels required for a definition are listed on a panel display list. Type **S** beside the names of the panels you want to access. Once you have made all your selections, press ENTER to display the first panel you selected. Then press F8 (Forward) to scroll forward through the panels you selected. Press F7 (Backward) to scroll backward through the panels you selected.

When you finish entering the data, press F3 (File) to save the data. Press F12 (Cancel) if you decide not to save the data.

Selecting a Panel from Another Panel

If you want to skip to a panel that is not next in the sequence, and you know the sequence number of the panel you want, enter that number at the Command ===> prompt. The required panel is displayed.

Selecting a Panel from the Index Menu

From some data entry panel, you can press F11 (Panels) to display the Index Menu panel. This menu lists all the panels available for the current function. Use the Index menu if you want to jump to a panel but do not know its place in the panel sequence.

Note

If you have selected two or more panels previously, pressing F11 (Panels) displays a list of the selected panels only. You can press F6 (AllPanel or SelPanel) to switch between the full list and the partial list.

Saving a Sequence of Definition Panels for Repeated Access

On a definition list panel, you can select more than one definition. You can then work on the selected definitions in sequence. Each definition can contain a number of definition panels. Normally, the list of panels is displayed on your screen for you to select each time you access a new definition. However, if you want to browse or update the same panels for each selected definition, you can save the list of panels you want, as shown in the following procedure.

As you move through the sequence of selected definitions, the panels appear on your screen according to the saved list. You do *not* have to select the panels again when you move on to the next definition.

The following procedure uses the resource definition panels as examples:

Step 1. Enter the **/RADMIN.R.STC** path to access the list of started task definitions. The Started Task List panel is displayed.

Step 2. Type **B** (Browse) or **U** (Update) beside the definitions you want to access. You can use the F7 (Backward) or F8 (Forward) function keys to scroll through the list.

Step 3. Press ENTER to select the definitions. The Panel Display List window is displayed, listing the resource definition panels.

Step 4. Type **S** next to the panels you want, and press F4 (SaveSeq) to save the list of selected panels.

Step 5. Press ENTER to bring up the first selected panel.

When you finish with one resource definition, the panels for the next definition are displayed in the same sequence.

Working with Definitions in the Knowledge Base

You can add, browse, update, copy, and delete the definitions in the knowledge base.

If you have several regions linked together, changes to the knowledge base in one region are automatically propagated to the knowledge bases in the other regions (that is, the knowledge bases are synchronized).

Caution

You should restrict the update of a definition to a single focal point region. Updating the same definition from more than one region may cause the linked knowledge bases to become unsynchronized.

The activity log contains an audit trail of definition maintenance activities, identifying the time an activity occurs and the user responsible for that activity. The information is also displayed on the definition list panels. You can press F11 (Right) to view the information.

Adding a Definition

Add a definition as follows:

Step 1. Access the list that displays the type of definitions you want to add.

For example, if you want to add a definition for a started task, you can enter the **/RADMIN.R.STC** path to access the list of started task definitions.

Step 2. Add the definition in one of the following ways:

- Use the F4 (Add) function key.
- Update a copy of another definition.

Step 3. To see the new definition, press F6 (Refresh) to update the list. You might also need to scroll the list to bring the new addition into view.

Browsing Definitions

Browse the details of a definition in read-only mode as follows:

Step 1. Access the list of definitions.

Step 2. Enter **B** beside the definition you want to browse.

If you wish to edit the definition, press F4 (Edit).

Step 3. When you finish browsing the definition, press F3 (Exit) to exit the BROWSE panel.

To browse more than one definition in sequence, type **B** beside all the definitions you want to browse and press ENTER. If you select multiple definitions, pressing F3 (Exit) when viewing a definition exits the current definition and calls up the next definition.

Updating Definitions

Update a definition as follows:

Step 1. Access the list of definitions.

Step 2. Enter **U** beside the definition you want to update.

Note

You can press F12 (Cancel) to cancel the operation any time before Step 4.

Step 3. Update the required fields.

Step 4. Press F3 (File) to file the updated definition when you complete the update.

To update more than one definition in sequence, type **U** beside all the definitions you want to update and press ENTER.

Copying Definitions

Copy a definition if you want to create a similar definition. Copy a definition as follows:

Step 1. Access the list of definitions.

Step 2. Enter **C** beside the definition you want to copy.

> **Note**
> You can press F12 (Cancel) to cancel the operation any time before Step 4.

Step 3. Change the value in the field that uniquely identifies the new copy, and update the other fields as required.

Step 4. Press F3 (File) to file the new definition when you finish updating the copy.

> **Note**
> When you are making a copy of a definition, the F4 (Save) function key enables you to continue creating independent copies of that definition. In Step 4, instead of pressing F3, press F4. The definition will remain open, and you can perform Step 3 again to define a new copy.

To copy more than one definition in sequence, type **C** beside all the definitions you want to copy and press ENTER.

Deleting Definitions

Delete definitions that are no longer needed as follows:

Step 1. Access the list of definitions.

Step 2. Type **D** beside the definitions you want to delete, and press ENTER. You are prompted for confirmation by either a panel or a message.

> **Caution**
> If the confirmation prompt is a message, only one confirmation message is displayed even if you are deleting more than one definition.

> **Caution**
> If you wish to cancel the operation, you must press F12 (Cancel) before the next step.

Step 3. Press ENTER to delete the selected definitions.

Getting Help

Online help is provided for panels and messages.

Online help is context-sensitive and available at different levels. When you are viewing a help panel, pressing F1 (Help) takes you to the next available higher level of help. Pressing F3 (Exit) takes you back to the previous level of help, or exits help and returns you to the application. Pressing F4 (Return) exits help and returns you to the application immediately.

Using the Tip of the Day

The region displays a tip about using the product at the bottom of the primary menu. To display the detailed tip, place the cursor on the tip and press F1 (Help).

Getting Help About a Panel

Panel-based online help includes information about what each panel is used for, how to complete the fields, the actions you can perform, and the use of available function keys. Use this online help to supplement the information in this guide while you are working in the region.

Press F1 (Help) to retrieve the online help for a given panel. When you are viewing a help panel, you can press F6 (HelpHelp) to find out how to use the help facility.

If the block of help text you require splits across two panels, use the arrow keys to move the cursor to the top or the bottom of the block and press F8 (Forward) or F7 (Backward) to bring the block into view.

Getting Help About a Message

While you are working in the region, you receive messages that advise you of various events. These messages might be providing information only (for example, informing you that an update has been successful). They might also alert you to errors (for example, if you try to enter an action that is not valid for a resource).

Each message has detailed online help text associated with it. Access the help text for a particular message in one of the following ways:

- If you are viewing an activity or file transfer log, move the cursor to the required product, CONNECT:Direct, or CONNECT:Mailbox message, and press F1 (Help).
- If you are viewing a transient log, enter **H** beside the message.
- If you are at a panel and a message is displayed in red on the third line of that panel, move the cursor to that line and press F1 (Help).
- If you are using a Command Entry panel or the Operator Console Services (OCS) (also known as the message monitor), you can do one of the following:
  - Move the cursor to the line displaying the product message, and press F1 (Help).
  - Type the product message ID at the => prompt, and press F1 (Help).
- Enter the **/CODES** shortcut to display the Messages and Codes Menu panel that enables you to obtain help on product messages and on miscellaneous error codes.
- If you are using a Command Entry panel or the OCS, type **NETINFO** at the => prompt, and press F1 (Help) to display the NETINFO : Browse Utility File panel that enables you to obtain help on product messages and on miscellaneous error codes.
- From the command line of any panel, enter the **CDMSG** command to display the CONNECT:Direct Message Selection List panel that enables you to obtain help on the CONNECT:Direct for MVS or CONNECT:Direct for OS/390 messages.
- From the command line of any panel, enter the **CMMSG** command to display the CONNECT:Mailbox Message Selection List panel that enables you to obtain help on the CONNECT:Mailbox messages.

  Note

  To enable the region to retrieve CONNECT:Mailbox messages and failure codes, you must specify a VSAM administration file in the CMAPI initialization parameter. For further information see the section, *Specifying the CONNECT:Mailbox Interface Parameters*, on page 5-10.

- From the command line of any panel, enter the **CMFC** command to display the CONNECT:Mailbox Connection Failure Codes panel.

Working in Two Windows

You can divide your screen into two logical windows. Each window operates independently of the other, enabling you to perform multiple functions concurrently.

Open a second window by using the F2 (Split) or F9 (Swap) function key.

Splitting a Screen

Using the F2 (Split) function key, you can:

- Split your screen horizontally and have one window above the other.

  To split your screen horizontally, move the cursor to a line where you want the split to occur and press F2 (Split).

- Split your screen vertically and have two windows side by side.

  To split your screen vertically, move the cursor to a column on the bottom line and press F2 (Split).

Returning a Split Screen to Single Window Display

You can return a split screen to single window display in one of the following ways:

- Move the cursor to the first line on your screen, and press F2 (Split) to minimize the window. The window containing the cursor disappears, and the other window expands to full size.
- Enter **=X** to exit one of the windows. Your session with that window ends.

Swapping Windows

Using the F9 (Swap) function key, you can:

- Reverse the dimensions of the windows if you have two windows open and both are visible on the screen, and toggle between them
- Open a second full-screen window if you are currently operating with a single window open, and then toggle between them

10

Building the Environment to Manage Your File Transfer Services

After you have completed the implementation of your NetMaster for File Transfer region, you can start building the environment to manage your file transfer services. This chapter describes how to build, load, and check the environment that monitors and manages those services.

This chapter contains the following topics:

- Building the Environment
- Defining a System Image
- Defining File Transfer Rules
- Defining File Transfer Schedules
- Defining Resources for File Transfer Products
- Defining TCP/IP Resources
- Auto-populating a System Image with DASD and Tape Resource Definitions
- Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on an AS/400 System
- Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on a Tandem System
- Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on a UNIX System
- Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on a Windows NT System
- Defining Rules, Schedules, and Resources to Manage a Remote FTS Region
- Loading, Checking, and Automating Your File Transfer Management Environment

Building the Environment

NetMaster for File Transfer helps you manage:

- File transfers
- File transfer schedules
- CA-XCOM, CONNECT:Direct, CONNECT:Mailbox, FTS, and FTP server file transfer applications
- Communications Server and TCPaccess file transfer mechanisms
- DASD and tape storage devices

You create definitions in the knowledge base to store the management information. To manage all of the above, except for file transfers, you also need to create a system image (see the section, *Defining a System Image*, on page 10-4).

To manage …	**Create …**
File transfers	File transfer rules (see the section, *Defining File Transfer Rules*, on page 10-6).
File transfer schedules	FTSCHD resource definitions (see the section, *Defining File Transfer Schedules*, on page 10-18).
CA-XCOM regions	XCMGR and XCMON resource definitions (see the section, *Defining CA-XCOM Resources*, on page 10-24).
CONNECT:Direct regions	CDMGR and CDMON resource definitions (see the section, *Defining CONNECT:Direct Resources*, on page 10-29).
CONNECT:Mailbox regions	STC, CMMGR, and CMMON resource definitions (see the section, *Defining CONNECT:Mailbox Resources*, on page 10-38).
FTS regions	FTSMGR and FTSMON resource definitions (see the section, *Defining FTS Resources*, on page 10-40).
Non-TCPaccess FTP servers	FTPMGR and FTPMON resource definitions (see the section, *Defining FTP Resources*, on page 10-43).
TCPaccess FTP servers	FTPMGR and FTPMON resource definitions (see the section, *Defining FTP Resources*, on page 10-43) and policy rules (see Chapter 20, *Controlling the Use of FTP*).
Communications Server or TCPaccess	An STC resource definition (see the section, *Defining TCP/IP Resources*, on page 10-48).
DASD and tapes	DASD and TAPE resource definitions (see the section, *Auto-populating a System Image with DASD and Tape Resource Definitions*, on page 10-51).

To manage …	Create …
CONNECT:Direct file transfer service on an AS/400 system	File transfer rules, and FTSCHD, CDMGR, and CDMON resource definitions (see the section, *Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on an AS/400 System*, on page 10-53).
CONNECT:Direct file transfer service on a Tandem system	File transfer rules, and FTSCHD, CDMGR, and CDMON resource definitions (see the section, *Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on a Tandem System*, on page 10-54).
CONNECT:Direct file transfer service on a UNIX system	File transfer rules, and FTSCHD, CDMGR, and CDMON resource definitions (see the section, *Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on a UNIX System*, on page 10-55).
CONNECT:Direct file transfer service on a Windows NT system	File transfer rules, and FTSCHD, CDMGR, and CDMON resource definitions (see the section, *Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on a Windows NT System*, on page 10-57).
FTS file transfer service on a remote system	File transfer rules, and FTSCHD, FTSMGR, and FTSMON resource definitions (see the section, *Defining Rules, Schedules, and Resources to Manage a Remote FTS Region*, on page 10-58).

After you define a system image and associated resources, you can load the system image, check the built environment, and automate your resources, as described in the section, *Loading, Checking, and Automating Your File Transfer Management Environment*, on page 10-58.

Defining a System Image

A system image must be defined for your NetMaster for File Transfer region. All resources that are monitored and controlled by your region are defined to the system image. You can define many versions of system images in your NetMaster for File Transfer region, of which only one can be active at any one time.

To define a system image, proceed as follows:

Note

One system image is required for each NetMaster for File Transfer region. If you are defining a system image for a subordinate, you must use the name assigned during the multisystem linking process (see the section, *Linking and Synchronizing Regions*, on page 7-8).

Step 1. After initial logon to the NetMaster for File Transfer region, the primary menu is displayed.

At the Select Option ===> prompt, enter **/RADMIN.I**. The System Image List is displayed.

Step 2. Press F4 (Add) to add a system image.

The ResourceView : System Image Definition is displayed.

Step 3. You must specify the name of the system image, its version, the system on which the image can be loaded, and a short description of the image in this panel, as shown in Figure 10-1.

Figure 10-1. ResourceView : System Image Definition Panel

```
SOLVPROD----------- ResourceView : System Image Definition --------------------
Command ===>                                                   Function=ADD


System Name ......... FT1
Database Version .... 1
Home System ......... FT1       (...where this Image will load)

Short Description ... SYSTEM01 file transfer image
Long Description ....
```

Step 4. With the information entered, press F3 (File) to file the image.

You are returned to the System Image List panel, and a message is displayed indicating that the system image has been successfully added to the knowledge base, as shown in Figure 10-2.

Figure 10-2. System Image List Panel

```
SOLVPROD------------- ResourceView : System Image List ------------------------
Command ===>                                              Scroll ===> PAGE
RMPD0003 ADD COMPLETED SUCCESSFULLY
    S/B=Browse U=Update C=Copy D=Delete R=Resources GRT=Graphic Rsc Tree L=Load
    System                                          EventView  Home
    Name      Vers.  Short Description              Ruleset    System
    FT1       0001   SYSTEM01 file transfer image               FT1
```

Defining File Transfer Rules

The NetMaster for File Transfer region uses file transfer rules to raise alerts and perform actions in response to events associated with file transfers. If a transfer matches a rule, the region displays an alert on the alert monitor.

Caution

If you want to use file transfer rules for FTS transfers, you must define the FTS managers for the appropriate FTS regions (see the section, *Defining FTS Resources*, on page 10-40). The managers enable the NetMaster for File Transfer region to detect FTS file transfer events.

Similarly, if you want to use file transfer rules for CONNECT:Direct transfers on distributed systems such as UNIX, you must define the CONNECT:Direct managers (see the section, *Defining CONNECT:Direct Resources*, on page 10-29).

To create a set of file transfer rules, you need to perform the following tasks:

1. Define a file transfer rule set.
2. Add file transfer rules to the rule set.

Defining a File Transfer Rule Set

To define a file transfer rule set, proceed as follows:

Step 1. Enter the **/FTADMIN.R** path to display the File Transfer Ruleset List panel.

Step 2. Press F4 (Add) to create a rule set definition.

The File Transfer Ruleset panel is displayed.

Step 3. Name the rule set and provide a brief description.

Step 4. Press F3 (File) to create the definition in the knowledge base.

Adding File Transfer Rules to a Rule Set

During operation, only one rule set is active in a NetMaster for File Transfer region. Add all the file transfer rules that are to be used by a region in the same rule set. You can use different rule sets for different regions.

To add a file transfer rule to a rule set, proceed as follows:

Step 1. If you are not already displaying the File Transfer Ruleset List panel, enter the **/FTADMIN.R** path to display it.

Step 2. Enter **R** beside the rule set to which you want to add rules.

The File Transfer Rules panel is displayed.

Note

If active rules have the same criteria, the rule with the name that occurs first alphabetically, is applied.

Step 3. Press F4 (Add) to add a rule.

The File Transfer Rule Filter panel is displayed.

Step 4. In the Filter Definition window, provide the following information:

In the …	**Specify …**
Rule Name field	The name of the rule.
Rule Status field	Whether the rule is ACTIVE or INACTIVE. You can use this field to switch the rule on or off.
Description field	A brief description for the rule.
Source/Target/ TransferID field	A value to identify the event(s) that the rule monitors. This value may be case sensitive. For more information, see the section, *Considerations—Case Sensitive Values*, on page 10-10. The values can be: • CA-XCOM transfer ID • CONNECT:Direct processes • CONNECT:Mailbox IDs or batch IDs • FTP transfer ID • FTS transmission definitions • Files (or data set members) For more information about transfer IDs, see help. You can use a mask to allow matching of more than one process, definition, or file. The wildcard characters are percent (%), representing zero or more characters, and underline (_), representing a single character.

In the …	Specify …
Type field	What the value in the Source/Target/TransferID field indicates. Valid values are: • ID—for CA-XCOM transfer IDs, CONNECT:Direct processes, FTP transfers, FTS transmission definitions, or CONNECT:Mailbox IDs • SOURCE—for outgoing files or CONNECT:Mailbox batch IDs • TARGET—for incoming files or CONNECT:Mailbox batch IDs
Transfer Status field	The file transfer status that the rule should monitor: start of the transfer (START), end of the transfer (END), or failure of the transfer (FAILURE).
Alert Severity field	The severity of the alert that is raised when the rule is triggered.
Alert Autoclear field	Whether you want a generated alert to be closed automatically. If you specify YES: • START alert will be closed by a subsequent FAILURE or END status event for the same transfer. The subsequent alert includes a counter in its description to indicate how many times it has been raised. • FAILURE alert will be closed by a subsequent FAILURE or END status event for the same transfer. The subsequent alert displays a counter to indicate how many times it has been raised. You can specify an alert timeout whereby an alert is closed only after the specified period of time. **Note** An END alert can be closed automatically only by a timeout.

Step 5. In the Filter Expression window, specify any secondary criteria to further restrict the transfers that the rule should monitor. Use Boolean operators to form your expressions. You can use the question mark (?) in the Field and Opr fields to list the valid values.

To see the online help, press F1 (Help). For an example, see the section, *Using a Filter Expression to Specify Rule Criteria—Example*, on page 10-17.

Step 6. To specify the actions to perform when a file transfer satisfies the rule, press F10 (Actions).

The Alert Automated Actions panel is displayed.

Step 7. Press F4 (Add) to add an action.

The actions you can specify include raising a problem record, notifying selected users, issuing a command, and running a process (see the online help).

Step 8. Repeat Step 7 until you have specified all the required actions, then press F3 (Exit) to exit the list of specified actions.

Step 9. To override the default alert definition, press F11 (Alert).

The Alert Definition for File Transfer Rule panel is displayed.

Step 10. Complete the Resource Name, Alert Text, Alert Description, and Alert Recommended Action fields. If you want to use the default value of a field, leave the field blank.

See the online help for a list of valid variables that can be used to customize alerts.

Step 11. Press F3 (File) to save the alert definition.

Step 12. When you are satisfied with the rule, press F3 (File) to save it in the knowledge base.

Note

Before the rules can be triggered by file transfer events, you must load the rule set that contains them. If the rule set is loaded when you add a rule, then the rule becomes active immediately.

Loading a Rule Set on Demand

To load a rule set, at the File Transfer Ruleset List panel, enter **L** beside the rule set you want to load. The rule set is loaded for the session, replacing the rule set previously loaded. The default rule set defined in the AUTOIDS parameter is not changed by this load action. If you want to change the default rule set you need to change the parameter group. For further information see *Loading, Checking, and Automating Your File Transfer Management Environment*, on page 10-58.

Considerations—Case Sensitive Values

The values that you enter for FileName/TransferID and for the node name and user ID secondary criteria are case sensitive:

If you are specifying a value for …	**Specify the value in …**
CA-XCOM transfers	Any case; case sensitivity is not supported.
Transfers associated with an AS/400, Tandem, UNIX, or Windows NT system	Mixed case and special characters as required. Note that the percent sign (%) and the underline (_) are not recognized as characters in their own right; file transfer rules and schedules recognize them as wildcard characters for file names and IDs.
Transfers associated with an OS/390 system	Upper case only.

Considerations—Overlapping Rules

If a file transfer event matches more than one rule, only the most restrictive rule is triggered.

For example, an active rule set contains two rules, A and B, that have the same criteria except for file name criterion, which are, respectively, ALSO0.HYPL.CARD(%) and ALSO0.HYPL.CARD(USER01). The results of the rules being matched are as follows:

If a file transfer event is received for …	**Then rule …**
ALSO0.HYPL.CARD(USER01)	B is triggered.
ALSO0.HYPL.CARD(*x*), where *x* is *not* USER01	A is triggered.

Considerations—CA-XCOM File Transfers

A NetMaster for File Transfer region identifies a CA-XCOM transfer by *xcom-transfer-id*(*request-number*). If a transfer does not have an ID, *xcom-transfer-id* takes on the following values. Similarly, if the user ID of a transfer is not known, the user ID takes on the following values.

Systems	*xcom-transfer-id*	**User ID**
AS/400	AS400-XFR	AS400-USER
Data General	DG-XFR	DG-USER
DEC	DEC-XFR	DEC-USER
DOS	DOS-XFR	DOS-USER
MVS	MVS-XFR	MVS-USER
PC	PC-XFR	PC-USER
SYS/36	SYS36-XFR	SYS36-USER
SYS/38	SYS38-XFR	SYS38-USER
SYS/88/STRAT	SYS88-XFR	SYS88-USER
Tandem	TANDEM-XFR	TANDEM-USER
UNIX or Windows NT	UNIX-XFR	UNIX-USER
Unknown	UNKNOWN	UNKNOWN-USER
VM	VM-XFR	VM-USER
WANG	WANG-XFR	WANG-USER

Considerations—CONNECT:Direct File Transfers

When you identify CONNECT:Direct file transfers, consider the information in the following sections.

Note

NetMaster for File Transfer does not receive an event at the start of a file transfer for either of the following:

- CONNECT:Direct for Windows NT 3.3
- CONNECT:Direct for UNIX

Identifying CONNECT:Direct File Transfers by Data Set Names

With CONNECT:Direct file transfers, a NetMaster for File Transfer region cannot monitor the transfer of specific data set members. Do not identify members when you specify the file name or transfer ID criterion.

However, even though the region cannot distinguish between the members, it reacts to each transferred member. For example, the transfer of the data sets, ALSO0.HYPL.CARD(AL1) and ALSO0.HYPL.CARD(AL2), is seen by the region as two separate transfers, although the region cannot identify the actual members transferred.

Identifying CONNECT:Direct File Transfers by Process Names

A NetMaster for File Transfer region identifies a CONNECT:Direct process by *process-name*(*process-number*).

Identify CONNECT:Direct processes in the form of a mask. For example, to identify process PR01, specify PR01(%); to identify processes with names that start with PR01, specify PR01%.

Identifying CONNECT: Direct for OS/400 Transfer by Data Set Names

The start events passed from the OS/400 agent do not include the source and target data set names. If a rule is triggered by a start event, you cannot specify target or source data set names as filtering criteria for file transfer rules. If you specify source and target data set names in schedules for CONNECT:Direct for OS/400, the schedule only reacts to the end event. If you do not specify a source name in the schedule, the schedule reacts to both start and end events.

Considerations—CONNECT:Mailbox File Transfers

A NetMaster for File Transfer region identifies a CONNECT:Mailbox transfer by *mailbox-id*(*batch-number*).

Identify CONNECT:Mailbox transfers in the form of a mask. For example, to identify transfer MB01, specify MB01(%); to identify transfers with IDs that start with MB01, specify MB01%.

The region does not receive an event at the start of a host initiated Auto Connect batch transfer.

Considerations—FTP File Transfers

When you identify FTP file transfers, consider the information in the following sections.

Information Available

File transfer rules are triggered by file transfer events. There are some restrictions on the information available to NetMaster for File Transfer from FTP events. You need to consider these restrictions when setting up a file transfer rule, as a rule cannot be triggered if the required information is not available.

Note

For FTP file transfers using the TCPaccess FTP server, these restrictions do not apply.

The restrictions on the information available from FTP events are as follows:

- NetMaster for File Transfer does not receive an event at the start of an FTP file transfer.
- Only local data set names are provided in the event.
- For transfers using TCPaccess, no FTP client events are issued. However, because TCPaccess operates by using a three-party FTP model, FTP server events are issued for all transfers.

Identifying FTP File Transfers

For FTP file transfers using a TCPaccess FTP server, the transfer ID is in the format *server-name*(*transfer-number*).

Identify TCPaccess FTP server transfers in the form of a mask. For example, to identify all transfers from the server PR01, specify PR01(%); to identify transfers to and from servers with names that start with PR01, specify PR01%.

For FTP file transfers not using a TCPaccess FTP server, there is no transfer ID. Only local data set names are available for identifying FTP transfers.

You can assign a static name to all FTP transfers not using a TCPaccess FTP server, by using the FTPCNTL parameter group (see the section, *Subtask 8.3—Customizing FTPCNTL Parameter Group (Non-TCPaccess FTP)*, on page 5-42). This allows you to set up a rule that includes all such FTP transfers.

Status of FTP File Transfers

When you build your FTP file management environment and if you are not using a TCPaccess FTP server, consider the following:

- The START status is not available for FTP file transfers.
- NetMaster for File Transfer cannot distinguish between a successfully completed transfer or a transfer aborted by the client. It reports both as successful.

Key Concept

The NetMaster for File Transfer region determines the success or failure of an FTP file transfer by checking the value of the last FTP reply code, and 226 is one of many codes that the region interprets as successful.

When an FTP file transfer is aborted by the client, the last reply code is 226, indicating that the transfer is successfully aborted, and the region displays the transfer status as successful.

The TCPaccess FTP server uses a sub-reply code to differentiate between successful and aborted file transfers.

Considerations—FTS File Transfers

When you identify FTS file transfers, consider the information in the following sections.

Identifying FTS File Transfers

It is recommended that you identify FTS file transfers by the transmission definitions.

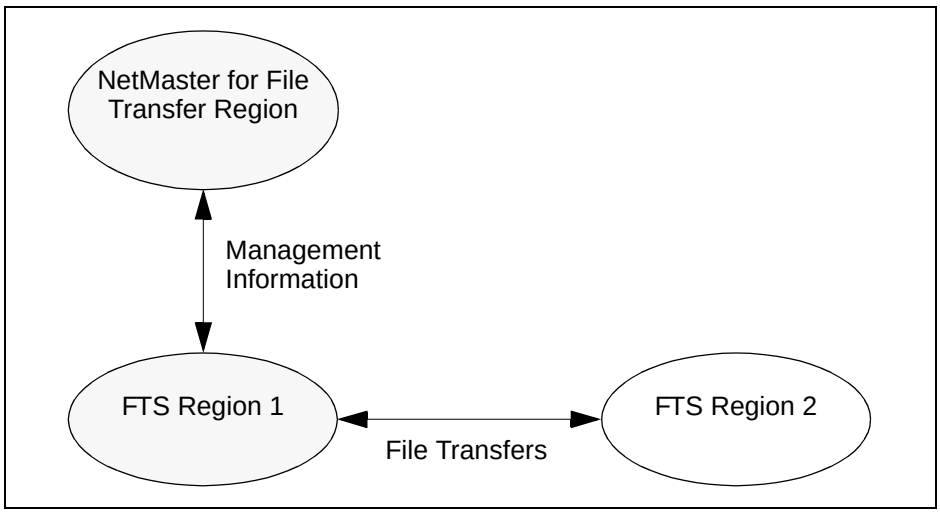
If you identify transfers by data set names, some transfer failures might be missed (for example, allocation problems at the start of a transfer or a file not empty condition).

Identifying FTS File Transfers by Transmission Definition Names

If a NetMaster for File Transfer region is monitoring multiple FTS regions, it is possible that transmission definitions with duplicate names are used. If you want to monitor such a definition, specify additional criteria to identify it uniquely.

A NetMaster for File Transfer region monitors the file transfers between FTS regions, which may or may not be managed by it. Figure 10-3 shows an example where FTS region 1 is managed and FTS region 2 is not managed.

Figure 10-3. FTS Management Environment



If an FTS transmission definition specifies a DD name that points to a data set in region 2 and NetMaster for File Transfer is not authorized in region 2, NetMaster for File Transfer will be unable to resolve the data set name and cannot monitor the data set.

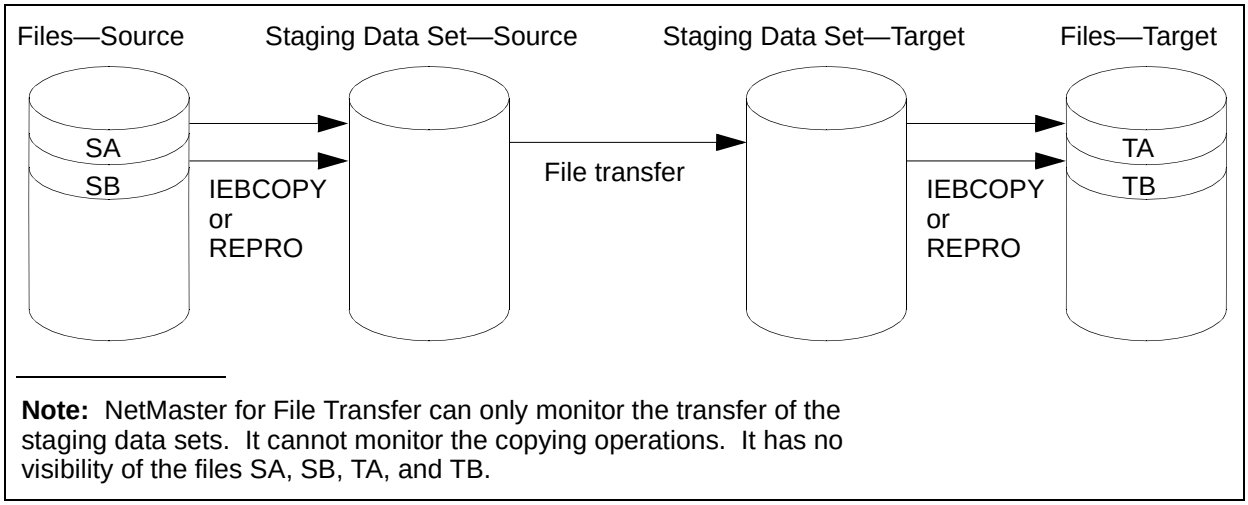
To resolve this problem, perform either of the following:

- Define the NetMaster for File Transfer BSYS background user in FTS region 2 (see the section, *Subtask 7.4.2—Defining the NetMaster for File Transfer Region as an FTS User*, on page 5-37).
- Use data set names in transmission definitions.

Considerations—FTS Staging Data Sets

An FTS region can perform a file transfer by using staging data sets. Data from different sources are copied into the source data set for transfer. When the transfer is complete, data are copied out into the different target files. Figure 10-4 shows the staging mode operation.

Figure 10-4. FTS Staging Mode Operation



Note: NetMaster for File Transfer can only monitor the transfer of the staging data sets. It cannot monitor the copying operations. It has no visibility of the files SA, SB, TA, and TB.

When staging mode operation is used, NetMaster for File Transfer can only monitor the transfer of the staging data sets. It has no visibility of the files that were copied into that data set. For this type of file transfer, ensure that your file name criterion specifies the staging data sets and not the copied files.

Using a Filter Expression to Specify Rule Criteria—Example

You want to check that any ALSO0.HYPL.CARD data set members being transferred from the local system between 6 p.m. and 7 p.m. are transferred at a minimum rate of 9,600 bytes per second. Figure 10-5 shows the file transfer rule that satisfies your requirements.

Figure 10-5. Specifying File Transfer Rule Criteria—Example

```
SOLVPROD--------- File Transfer : File Transfer Rule Filter -----------Func=ADD
Command ===>                                                  Scroll ===> CSR

. Filter Definition -------------------------------------------------------.
| Ruleset Name ...... CARDS                                                |
| Rule Name ......... FTCARDRULE                                           |
| Rule Status ....... ACTIVE     (ACTIVE or INACTIVE)                      |
| Description ....... Credit data file transfer rule                       |
| Source/Target/XfrID ALSO0.HYPL.CARD(%)                                   |
| File Type ......... SOURCE     (SOURCE,TARGET or ID)                     |
| Transfer Status ... END        (START,END, or FAILURE)                   |
| Alert Severity .... 3          (default is 4 - LOW )                     |
| Alert Autoclear ... YES        (YES,NO or hh.mm - default is YES)        |
'--------------------------------------------------------------------------'
. Filter Expression -------------------------------------------------------.
|                                                                          |
|                                                D=Delete I=Insert R=Repeat |
|      "(" Field   Opr Value                                Gen ")" Bool   |
|          TIME    GE  18.00.00                                     AND   |
|          TIME    LE  19.00.00                                     AND   |
|          TRATE   LT  9600                                                |
|  F1=Help     F2=Split    F3=File     F4=Save                             |
|  F7=Backward F8=Forward  F9=Swap    F10=Actions F11=Alert   F12=Cancel   |
'--------------------------------------------------------------------------'
```

If the transfer is slower than the minimum rate, NetMaster for File Transfer displays an alert on the alert monitor.

Defining File Transfer Schedules

The NetMaster for File Transfer region uses file transfer schedule resource definitions to monitor the status of scheduled file transfers. The region displays the schedules on the status monitor. If a scheduled file transfer does not complete successfully, the corresponding schedule on the status monitor changes status to reflect the condition.

Caution

If you want to use file transfer schedules for FTS transfers, you must define the FTS managers for the appropriate FTS regions (see the section, *Defining FTS Resources*, on page 10-40). The managers enable the NetMaster for File Transfer region to detect FTS file transfer events.

Similarly, if you want to use file transfer schedules for CONNECT:Direct transfers on distributed systems such as UNIX, you must define the CONNECT:Direct managers (see the section, *Defining CONNECT:Direct Resources*, on page 10-29).

To define a file transfer schedule in a system image, proceed as follows:

Step 1. Enter the **/RADMIN.R.FTSCHD** path to display the File Transfer Schedule List panel.

Step 2. Identify the system image to which this schedule belongs in the System Name and Version fields.

Step 3. Press F4 (Add) to create a schedule resource definition.

The File Transfer Schedule General Description panel is displayed.

Step 4. Identify the schedule by name and description in the File Transfer Schedule Name and Short Description fields.

Step 5. Press F8 (Forward) to display the Schedule panel, and specify the schedules. The file transfer schedule resource definition can contain more than one schedule. For more information about file transfer schedules, see the section, *Specifying a Schedule*, on page 10-20.

Caution

Do not overlap schedule entries. If an entry has a start time before or equal to the end of an earlier entry, the later entry is ignored.

Step 6. Press F8 (Forward) to display the File Filters panel. Identify the transfers to be monitored in the schedule. If you specify a mask, you should also specify the number of files represented by the mask.

See the following sections for special considerations:

- *Considerations—Case Sensitive Values*, on page 10-10
- *Considerations—CA-XCOM File Transfers*, on page 10-11
- *Considerations—CONNECT:Direct File Transfers*, on page 10-11
- *Considerations—CONNECT:Mailbox File Transfers*, on page 10-12
- *Considerations—FTS File Transfers*, on page 10-14
- *Considerations—FTS Staging Data Sets*, on page 10-16
- *Considerations—FTP File Transfers*, on page 10-13

Note

NetMaster for File Transfer provides extended filtering criteria that can help you identify the transfers. These criteria include the file transfer regions to and from which a transfer is made, and the size of the transfer.

To use these criteria, enter **E** beside an entry.

For information about how to specify these criteria, see the online help.

For information about specifying filters in a CTL file, see Chapter 19, *Advanced Features*.

Step 7. If you want the region to perform some actions when the schedule changes state, press F8 (Forward) to display the State Change Exits panel.

For information about these state changes, see the section, *Schedule Status Changes*, on page 10-23. For information about how to specify these actions, see the online help.

Step 8. When you are happy with the definition, press F3 (File) to save it in the knowledge base.

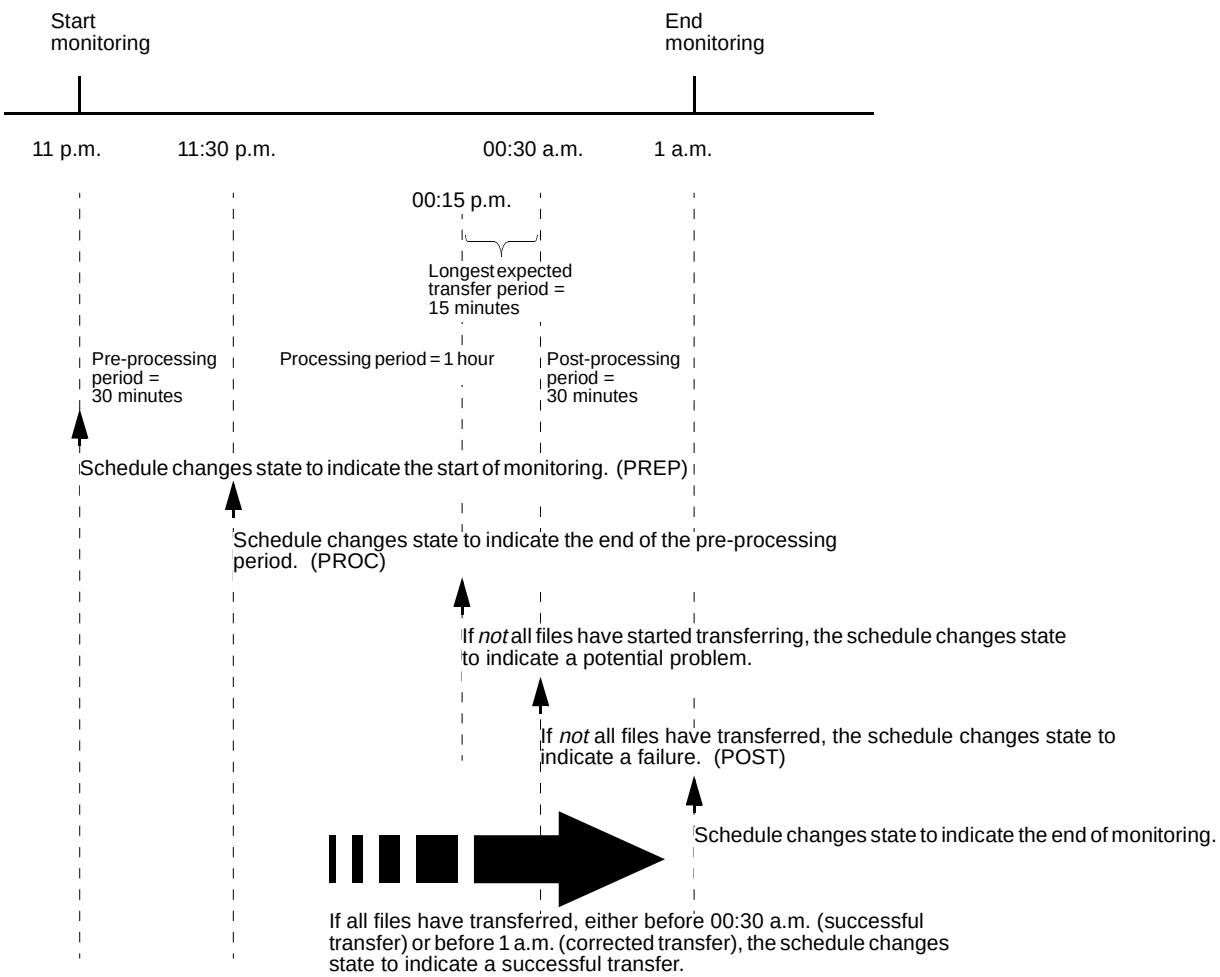
Specifying a Schedule

You can specify the following times in a file transfer schedule:

Times	Description
Day or date	Specifies the day or date when a schedule entry starts. You can use calendar criteria to identify the day. For information about how to define calendars and criteria, see Chapter 17, *Defining and Maintaining Calendars.*
Start time	Specifies the time, *hh.mm*, when the region starts to monitor for the specified file transfers. The schedule changes state to reflect this condition on the status monitor.
Pre-processing period	Specifies any required period, *hh.mm*, during which you can perform actions to prepare for the transfer.
Processing period	Specifies the period, *hh.mm*, during which the files are expected to be transferred. The schedule changes state to reflect the start of this period on the status monitor. During this period, the schedule reflects the success or failure of the transfer on the status monitor.
Post-processing period	Specifies the period, *hh.mm*, during which you can perform additional actions, if required, after the processing period. For example, you can perform actions to recover from a failure. If all failures are corrected, the schedule will indicate on the status monitor that the transfer is successful. At the end of this period, the region stops monitoring for the specified files. The schedule changes state to reflect this condition on the status monitor.
Longest expected transfer period	Specifies the expected duration of the longest file transfer in *hh.mm*. If at this duration before the end of processing, not all transfers have begun, the schedule will reflect a degraded condition on the status monitor. If you do not want to use this feature, do not specify this period. **Note** For FTP transfers that are not handled by a TCPaccess FTP server, and for host-initiated CONNECT:Mailbox Auto Connect transfers, the region is not notified when a transfer starts, but only when it ends. In this case, setting the longest expected transfer period may not be useful. If it is set, then the schedule shows degraded in the final monitoring period unless all transfers have already completed.

Figure 10-6 shows an example of a file transfer schedule.

Figure 10-6. File Transfer Schedule



Note: For information about the state changes, see Table 10-1 on page 10-23.

Schedule Definition—Example

Figure 10-7 shows an example of a file transfer schedule. The schedule expects nine ALSO0.HYPL.CARD data set members to be transferred according to the times indicated in Figure 10-6 on page 10-21.

Figure 10-7. File Transfer Schedule—Example

```
SOLVPROD--------- ResourceView : FTSCHD CARDSCHEDULE Schedule ---------FT1-0001
Command ===>

.- Schedule Entries -------------------------------------------------------.
|                                                                           |
| Day/Date or   Start  Pre-Processing  Processing  Post-Processing  Longest |
| Criteria Name Time   Period          Period      Period           Transfer |
| SUNDAY______  23.00  00.30           01.00       00.30            00.15   |
| ____________  _____  _____           _____       _____            _____   |
```

```
SOLVPROD------- ResourceView : FTSCHD CARDSHEDULE File Filters --------FT1-0001
Command ===>

.- File Filters -----------------------------------------------------------.
|                                                                           |
|                                                        E=Extended Filter |
|     File Name/Transfer ID (Case Sensitive)                   Type Number |
|     ALSO0.HYPL.CARD(%)_____________________________________ SRC  9__     |
|     ___________________________________________________ ___  ___         |
```

Schedule Status Changes

Table 10-1 shows the operation modes and states of a file transfer schedule resource as its status changes.

Table 10-1. Status Changes of a File Transfer Schedule

Time	Operation Mode	Desired State	Actual State
Before starting for the first time	MANUAL	INACTIVE	INACTIVE
Start of schedule	IGNORED	ACTIVE	INACTIVE
Start of processing	MANUAL	ACTIVE	STARTING
Transfer completed	MANUAL	ACTIVE	ACTIVE
Potential problem indicated	MANUAL	ACTIVE	DEGRADED
Transfer failure	MANUAL	ACTIVE	FAILED
Transfer recovered	MANUAL	ACTIVE	ACTIVE
End of schedule	MANUAL	INACTIVE	INACTIVE (if the schedule is satisfied) or FAILED (if the schedule is not satisfied)

You can view these states on the status monitor by entering the EXTDISP OFF command. To return to the original display mode, use the EXTDISP ON command.

To view the corresponding logical states, enter **/ASADMIN.A** and select the Manual Mode Attributes Table panel.

Key Concept

The types of operation modes are as follows:

- MANUAL—the resource can be controlled manually, and the region monitors but does *not* control the resource.
- IGNORED—this mode is the same as the MANUAL mode except that the logical state is always OK.

Defining Resources for File Transfer Products

To build an environment to manage CA-XCOM, CONNECT:Direct, CONNECT:Mailbox, FTS, and FTP resources, you define the following:

- *Manager Resources (XCMGR, CDMGR, CMMGR, FTPMGR, and FTSMGR)*—You must define manager resources to your system image. This resource class is used to define your file transfer applications to the knowledge base. This is an owning resource.
- *Monitor Resources (XCMON, CDMON, CMMON, FTPMON, and FTSMON)*—You define monitor resources to your manager resource. This resource class is used to define resources that monitor the file transfer application. These are owned resources—you define various monitors for the manager.

See the following sections for information about how to use the Assisted Resource Definition Facility to define these resources to a system image:

- *Defining CA-XCOM Resources*, on this page
- *Defining CONNECT:Direct Resources*, on page 10-29
- *Defining CONNECT:Mailbox Resources*, on page 10-38
- *Defining FTS Resources*, on page 10-40
- *Defining FTP Resources*, on page 10-43

Defining CA-XCOM Resources

A NetMaster for File Transfer region can manage CA-XCOM applications on the local system. To enable the region to perform this management function, define managers and monitors for these applications in the system image as follows:

Step 1. Use the Assisted Resource Definition Facility to create a manager for a CA-XCOM application (see the section, *Creating a CA-XCOM Manager*, on page 10-25).

Step 2. Generate monitors for the created managers (see the section, *Creating CA-XCOM Monitors*, on page 10-27).

Creating a CA-XCOM Manager

Create the resource to manage your CA-XCOM for MVS region as follows:

Step 1. Enter the **/RADMIN.AD.XC** path.

If you have …	Then …
Already defined the system image	Enter **S** beside the system image on the displayed System Image List panel.
Not yet defined your system image	Press ENTER at the Confirm System Image Add panel to add a system image. For information about how to create a system image definition, see the section, *Defining a System Image*, on page 10-4.

The XCOM Manager General Description panel is displayed.

Step 2. Enter a CA-XCOM manager name in the XCOM Manager Name field.

Note

You define a manager resource for each CA-XCOM application you want to be managed by this region.

The manager name identifies the CA-XCOM resource that is the subject of this definition. The manager name must be the same as that used for the CA-XCOM application (for example, DEXC1 (see Figure 10-8)).

Figure 10-8. Entering Details for the XCMGR

```
SOLVPROD------- ResourceView : XCOM Manager General Description -------FT1-0001
Command ===>                                                     Function=ADD

System Name ..+ FT1        Database Version ..+ 0001
XCOM Manager Name ............................ DEXC1
XCOM Manager Type ...........................+ STC

ACB Name ............


Operation Mode .....+ AUTOMATED
Short Description ... CA-XCOM started task
Long Description ....
```

Step 3. Enter the manager type in the Manager Type field.

If the CA-XCOM application is …	Enter …
Initialized as a started task	**STC** as the manager type.
Initialized as a job	**JOB** as the manager type.

Step 4. Enter **AUTOMATED** or **MANUAL** in the Operation Mode field (see Figure 10-8 on page 10-25).

Key Concept

The two types of operation mode are as follows:

- AUTOMATED—the resource is monitored and controlled (activated and inactivated) by the region.
- MANUAL—the resource can be controlled manually, and the region monitors but does *not* automatically control the resource.

Step 5. Briefly describe this resource in the Short Description field (for example, CA-XCOM started task (see Figure 10-8 on page 10-25)).

Step 6. Press F3 (File) to file the manager resource definition.

Note

If you want to create multiple manager resource definitions, press F4 (Save) to save the current definition and update the definition for a new manager resource. Repeat this process until a manager resource is defined for each CA-XCOM application on this system. When all manager resources are defined, press F3 (File) to file the last resource and proceed with the Assisted Resource Definition dialog.

The ResourceView : XCOM Manager List panel is displayed.

Note

If you specified that the CA-XCOM application was initiated by a job, you should ensure that the message text on the resource definition Display and Heartbeat Details panel is valid for your job. To do this, enter **S** beside the listed manager resource and select the Display and Heartbeat Details Panel from the displayed list.

This newly created resource will manage your CA-XCOM application. You can modify it at a later stage, as described in Chapter 15, *Customizing the Environment That Manages File Transfer Resources.*

You have completed the CA-XCOM manager resource definition and can now define monitor resources for the manager, as described in the next section, *Creating CA-XCOM Monitors*.

Creating CA-XCOM Monitors

Generate monitors for the created CA-XCOM managers as follows:

Step 1. Enter **G** beside a manager resource definition to generate monitor resources for the manager resource, as shown in Figure 10-9.

Figure 10-9. Generating CA-XCOM Monitor Resources

```
SOLVPROD----------------- ResourceView : XCOM Manager List -------------------1
Command ===>                                                   Scroll ===> PAGE

. System Image ------------------------------------------------------------------.
| System Name ...+ FT1          Version ...+ 0001                               |
'-------------------------------------------------------------------------------'
. Resources ---------------------------------------------------------------------.
|        S/B=Browse U=Update C=Copy D=Delete G=Generate MON=Monitors R=Relate |
|     CDMGR Name         Description                                            |
|  G  DEXC1              CA-XCOM started task                                   |
|     **END**                                                                   |
```

A list of the available monitor resource types is displayed.

Step 2. Enter **S** beside each type of monitor you want to generate for your manager resource definition, as shown in Figure 10-10.

Figure 10-10. Selecting CA-XCOM Monitor Templates

```
SOLVPROD---------------- ResourceView : XCOM Monitor List --------------------8
Command ===>                                                   Scroll ===> CSR

                                      Use 'S' to Select Monitor(s) to Generate
    XCMON Name         Description
S   ACTIVE             Active Transfer Monitor
S   CONNECTIONS        XCOM Connections Monitor
S   HELD               Held Transfer Monitor
S   INACTIVE           Inactive Transfer Monitor
S   LISTENER           Listener Monitor
S   REMOTENODE         Remote Node Monitor
S   STALLED            Stalled Transfer Monitor
S   SUSPENDED          Suspended Transfer Monitor
    **END**
```

Step 3. With your monitor types selected, a panel for each monitor is displayed. Enter the name of each monitor, and optionally, a long description of the monitor, as shown in Figure 10-11.

Figure 10-11. Entering CA-XCOM Monitor Details

```
SOLVPROD--------- ResourceView : XCOM Monitor General Description -----FT1-0001
Command ===>                                                       Function=ADD

System Name ..+ FT1        Database Version ..+ 0001
XCOM Monitor Name ............................ ACTIVE__
XCOM Monitor Type ...........................+ REQUEST-MON_


XCOM Manager Name .......................+ DEXC1___

Operation Mode .....+ MANUAL_____
Short Description ... Active Transfer Monitor_______
Long Description .... This XCMON monitors active file transfer requests_______
                      ____________________________________________________________
                      ____________________________________________________________
                      ____________________________________________________________
```

Step 4. Press F8 (Forward) to display the Monitor Details panel, and review the settings.

Note

If the monitor type is REQUEST-MON, the heartbeat interval is specified on the Monitor Details panel of the owning XCMGR definition.

Step 5. Press F3 (File) to file the monitor resource definition.

Step 6. When you have filed the details for all selected monitors, you are returned to the ResourceView : XCOM Manager List panel. You can enter **G** beside any remaining manager resources and repeat Step 2 through Step 5 to define monitor resources for the manager resources.

Step 7. Press F3 (Exit) to exit the ResourceView : XCOM Manager List panel.

You can customize the resource definitions created by the Assisted Resource Definition Facility. See Chapter 15, *Customizing the Environment That Manages File Transfer Resources*, for information about customizing resource definitions.

Defining CONNECT:Direct Resources

A NetMaster for File Transfer region can manage CONNECT:Direct applications on the local system and on distributed systems such as UNIX. To enable the region to perform this management function, define managers and monitors for these applications in the system image as follows:

Note

To manage CONNECT:Direct applications on a distributed system such as UNIX, you must have implemented the appropriate agent for NetMaster for File Transfer on that system.

Step 1. Use the Assisted Resource Definition Facility to create a manager for a CONNECT:Direct application (see the section, *Creating a CONNECT:Direct Manager*, on page 10-29).

Step 2. Use the Auto Populate Facility to create the managers for its partner CONNECT:Direct applications on distributed systems (see the section, *Using the Auto Populate Facility to Create Resources for Partner CONNECT:Direct Applications*, on page 10-32).

Step 3. Generate monitors for the created managers (see the section, *Creating CONNECT:Direct Monitors*, on page 10-34).

Creating a CONNECT:Direct Manager

Use the following steps to create resources to manage CONNECT:Direct for MVS or CONNECT:Direct for OS/390. (The two names are used interchangeably in this guide.) Although you can use the same steps to create resources to manage CONNECT:Direct on distributed systems, you might want to use the Auto Populate Facility to create those resources that are partners of a CONNECT:Direct for MVS region (see the section, *Using the Auto Populate Facility to Create Resources for Partner CONNECT:Direct Applications*, on page 10-32).

Step 1. Enter the **/RADMIN.AD.CD** path.

If you have …	Then …
Already defined the system image	Enter **S** beside the system image on the displayed System Image List panel.
Not yet defined your system image	Press ENTER at the Confirm System Image Add panel to add a system image. For information about how to create a system image definition, see the section, *Defining a System Image*, on page 10-4.

The C:D File Transfer Manager General Description panel is displayed.

Step 2. Enter a CONNECT:Direct manager name in the C:D File Transfer Manager Name field.

Note

You define a manager resource for each CONNECT:Direct application you want to be managed by this region.

The manager name identifies the CONNECT:Direct resource that is the subject of this definition. For CONNECT:Direct for MVS, the manager name must be the same as that used for the CONNECT:Direct application (for example, DECD1 (see Figure 10-12)). For CONNECT:Direct on a distributed system, the manager name must match the distributed system host name. For more information on the distributed system host name, see the *NetMaster for File Transfer Agent - Connect:Direct Installation and Administration Guide*.

Figure 10-12. Entering Details for the CDMGR

```
-------- ResourceView : C:D File Transfer Manager General Description ---------
Command ===>                                                   Function=ADD

System Name ..+ FT1        Database Version ..+ 0001
C:D File Transfer Manager Name ................ DECD1
C:D File Transfer Manager Type ...............+ STC
ACB Name ........... DECD1
TCP/IP Host Name/Addr .......
Agent Port Number ..........

Operation Mode .....+ AUTOMATED
Short Description ... CONNECT:Direct started task
Long Description ....
```

Step 3. Enter the manager type in the Manager Type field, and either the ACB name of the CONNECT:Direct application or the TCP/IP details of the distributed systems agent.

If the CONNECT:Direct application is …	Enter …
Initialized as a started task	**STC** as the manager type and its ACB name.
Initialized as a job	**JOB** as the manager type and its ACB name.
On an AS/400 system	**OS400** as the manager type and the TCP/IP details of the agent.
On a Tandem system	**TANDEM** as the manager type and the TCP/IP details of the agent.
On a UNIX system	**UNIX** as the manager type and the TCP/IP details of the agent.
On a Windows NT system	**NT** as the manager type and the TCP/IP details of the agent.

Step 4. Enter **AUTOMATED** or **MANUAL** in the Operation Mode field (see Figure 10-12).

Key Concept

The two types of operation mode are as follows:

- AUTOMATED—the resource is monitored and controlled (activated and inactivated) by the region.
- MANUAL—the resource can be controlled manually, and the region monitors but does *not* automatically control the resource.

Step 5. Briefly describe this resource in the Short Description field (for example, CONNECT:Direct started task (see Figure 10-12 on page 10-30)).

Step 6. Press F3 (File) to file the manager resource definition.

Note

If you want to create multiple manager resource definitions, press F4 (Save) to save the current definition and update the definition for a new manager resource. Repeat this process until a manager resource is defined for each CONNECT:Direct application to be managed by this region. When all manager resources are defined, press F3 (File) to file the last resource and proceed with the Assisted Resource Definition dialog.

The ResourceView : C:D File Transfer Manager List panel is displayed.

Note

If you specified that the CONNECT:Direct application was initiated by a job, you should ensure that the message text on the resource definition Display and Heartbeat Details panel is valid for your job. To do this, enter **S** beside the listed manager resource and select the Display and Heartbeat Details Panel from the displayed list.

This newly created resource will manage your CONNECT:Direct application. You can modify it at a later stage, as described in Chapter 15, *Customizing the Environment That Manages File Transfer Resources.*

You have completed the CONNECT:Direct manager resource definition, and can now define the partner resources for the manager, as described in the next section, *Using the Auto Populate Facility to Create Resources for Partner CONNECT:Direct Applications*.

Using the Auto Populate Facility to Create Resources for Partner CONNECT:Direct Applications

The Auto Populate Facility uses the network map of a CONNECT:Direct for MVS region to list the partner CONNECT:Direct applications. You can then select the required applications and create the manager resources for them.

To use the Auto Populate Facility to define resources for CONNECT:Direct, you must satisfy the following:

- You have defined the CONNECT:Direct for MVS manager.
- The system image that contains the manager is active.
- The CONNECT:Direct for MVS region that owns the network map is active.
- You are an authorized user in the CONNECT:Direct for MVS region.

Proceed as follows:

Step 1. Enter the **/RADMIN.AD.A** path to access the Auto Populate Facility. The Auto Populate menu is displayed.

Step 2. Type **CD** at the Select Option ===> prompt.

Step 3. Complete the fields on the panel as follows:

- Identify the system image (to which you want to add the definitions for the local resources) in the System Name and Version fields. Autopopulation puts resources for CONNECT:Direct for MVS and its partners in the same image.
- Identify the template to be used to create the definitions in the Template field. Type **?** in the field to ask for a list of valid templates.
- If required, use the Resource Mask field to restrict the list of resources that will be displayed for which you can build definitions. Use the asterisk (*) as the wildcard character. A leading or embedded * represents a single character; a trailing * represents any number of characters. For example, **A0 includes 00A0, 01A0, … while 09* includes 09A0, 09A1, 09A2, …
- Identify the manager for the CONNECT:Direct for MVS region for which you want to discover the partners.

Step 4. After you complete the fields, press ENTER. The C:D File Transfer Manager Template List panel is displayed.

Step 5. Enter **S** beside the required template to list the type of resources you selected. If you are accessing the specified CONNECT:Direct for MVS region from the NetMaster for File Transfer region for the first time, you are prompted to confirm your signon details. Enter your password and check that the other details are correct, then press F6 (Confirm). (For more information about accessing a CONNECT:Direct region, see the section, *Confirming Your CONNECT:Direct Signon Details*, on page 13-15.)

The Auto Populate Selection List panel is displayed. Figure 10-29 is an example for CONNECT:Direct for UNIX resources.

Figure 10-13. Auto Populate Selection List Panel

```
SOLVPROD------- AutoAssist : Auto Populate Selection List ---------------------
Command ===>                                                   Scroll ===> CSR

                                        S=Select Resource  U=Unselect Resource
    Name                Template     Description
    NSW00001            CDUNIX       UNIX CDMGR - NSW00001
    NSW00002            CDUNIX       UNIX CDMGR - NSW00002
    NT000001            CDUNIX       UNIX CDMGR - NT000001
    NT000002            CDUNIX       UNIX CDMGR - NT000002
    QLD00001            CDUNIX       UNIX CDMGR - QLD00001
    QLD00002            CDUNIX       UNIX CDMGR - QLD00002
    SA000001            CDUNIX       UNIX CDMGR - SA000001
    TAS00001            CDUNIX       UNIX CDMGR - TAS00001
    VIC00001            CDUNIX       UNIX CDMGR - VIC00001
    WA000001            CDUNIX       UNIX CDMGR - WA000001
    **END**





 F1=Help      F2=Split                                          F6=Action
 F7=Backward  F8=Forward   F9=Swap                             F12=Cancel
```

Step 6. Type **S** next to the resources for which you want to build definitions. To select all the displayed resources, enter **ALL S** at the Command ===> prompt.

You can press ENTER to validate your selections. The selections are tagged as selected. If you want to unselect a selected resource, enter **U** beside the resource. If you want to unselect all selected resources, enter **ALL U** at the Command ===> prompt.

Note

You can, if necessary, change the templates for individual resources.

Caution

If you want to cancel the operation, you must press F12 (Cancel) before the next step.

Step 7. Press F6 (Action) to build the resource definitions.

Step 8. When the building process is complete, enter the **/RADMIN.R.CDMGR** path to display the C:D File Transfer Manager List panel, which should show the newly created managers.

Note

If you have changed the default port number of the agents, review and update the TCP/IP details of the agents in the manager definitions.

Step 9. Define monitor resources for these managers (see the section, *Defining CONNECT:Direct Resources*, starting from Step 1 on page 10-34).

You have completed the CONNECT:Direct manager resource definitions, and can now define monitor resources for the managers, as described in the next section, *Creating CONNECT:Direct Monitors*.

Creating CONNECT:Direct Monitors

Generate monitors for the created CONNECT:Direct managers as follows:

Step 1. Enter **G** beside a manager resource definition to generate monitor resources for the manager resource, as shown in Figure 10-14.

Figure 10-14. Generating CONNECT:Direct Monitor Resources

```
SOLVPROD------- ResourceView : C:D File Transfer Manager List ----------------1
Command ===>                                                   Scroll ===> PAGE

. System Image -----------------------------------------------------------------.
| System Name ...+ FT1          Version ...+ 0001                               |
'-------------------------------------------------------------------------------'
. Resources --------------------------------------------------------------------.
|        S/B=Browse U=Update C=Copy D=Delete G=Generate MON=Monitors R=Relate |
|     CDMGR Name         Description                                           |
|  G  DECD1              CONNECT:Direct started task                           |
|     **END**                                                                  |
```

A list of the available monitor resource types is displayed.

Note

The list consists of the types for which templates are provided. If you want to create a resource that is not listed (for example, for a different CONNECT:Direct process status), see the section, *Creating a Custom-built CONNECT:Direct Monitor Resource Definition*, on page 10-37.

Step 2. Enter **S** beside each type of monitor you want to generate for your manager resource definition, as shown in Figure 10-15.

Note

The TCP/IP connections monitor is not available to a distributed systems (for example, UNIX) type manager.

Figure 10-15. Selecting CONNECT:Direct Monitor Templates

```
SOLVPROD------- ResourceView : C:D File Transfer Monitor List ---------------10
Command ===>                                                   Scroll ===> PAGE

                                        Use 'S' to Select Monitor(s) to Generate
    CDMON Name         Description
S   CONNECTIONS        C:D TCP/IP Connection Monitor
S   EXECQ              C:D Exec Queue Monitor
S   HOLDQ              C:D Hold Queue Monitor
S   HOLDQWC            C:D Hold Queue with WC Status
S   LISTENER           C:D TCP/IP Listener Task Mon.
S   REMOTENODE         C:D Remote Node Monitor
S   TIMERQ             C:D Timer Queue Monitor
S   TIMERQRETRY        C:D Timer Queue - Retry Status
S   TRANSFER           C:D Transfer Monitor
S   WAITQ              C:D Wait Queue Monitor
    **END**
```

Step 3. With your monitor types selected, a panel for each monitor is displayed. Enter the name of each monitor, and optionally, a long description of the monitor, as shown in Figure 10-16.

Figure 10-16. Entering CONNECT:Direct Monitor Details

```
-------- ResourceView : C:D File Transfer Monitor General Description ---------
Command ===>                                                    Function=ADD

System Name ..+ FT1        Database Version ..+ 0001
C:D File Transfer Monitor Name ............... TCPCONN
C:D File Transfer Monitor Type ..............+ TCP-CONNECT_


C:D File Transfer Manager Name ............... DECD1___

Operation Mode .....+ MANUAL_____
Short Description ... C:D TCP/IP Connection Monitor_
Long Description .... This monitors TCP/IP connections_________________________
                      ______________________________________________________________
                      ______________________________________________________________
                      ______________________________________________________________
```

Step 4. Press F8 (Forward) to display the Monitor Details panel, and review the settings.

If you are defining a TCP/IP listener task monitor for a CONNECT:Direct application that resides on a distributed system, specify the TCP/IP port number of the application and, if required, an SNMP community name defined on the distributed system. The default name is `public`. The specified community must include the IP addresses of the local OS/390 system.

Note

For the TCP/IP listener task monitor to work, the SNMP agent must be active.

For the TCP/IP connections monitor to work, NETSTAT must be working.

Step 5. Press F3 (File) to file the monitor resource definition.

Step 6. When you have filed the details for all selected monitors, you are returned to the ResourceView : C:D File Transfer Manager List panel. You can enter **G** beside any remaining manager resources and repeat Step 1 through Step 3 to define monitor resources for the manager resources.

Step 7. Press F3 (Exit) to exit the ResourceView : C:D File Transfer Manager List panel.

You can customize the resource definitions created by the Assisted Resource Definition Facility. See Chapter 15, *Customizing the Environment That Manages File Transfer Resources*, for information about customizing resource definitions.

Creating a Custom-built CONNECT:Direct Monitor Resource Definition

To create a definition for which a template has not been provided, proceed as follows:

Step 1. Enter the **/RADMIN.R.CDMON** path to display the C:D File Transfer Monitor List panel.

Step 2. Ensure that the system image is the one you want.

Step 3. Enter **C** beside the definition on which you want to base the new definition.

Step 4. Rename the definition, and update the other fields as required.

For example, if you want to create a monitor for a different process status, update the Process Status field on the Monitor Details panel.

Step 5. When you have completed your updates, press F3 (File) to create the definition.

Note

You can also create your own custom-built templates in the same manner. Use the panel path specification **/RADMIN.T.R.CDMON**.

Defining CONNECT:Mailbox Resources

A NetMaster for File Transfer region can manage CONNECT:Mailbox applications on the local system. To enable the region to perform this function, define managers and monitors for these applications in the system image.

Creating a CONNECT:Mailbox Manager

To define a CONNECT:Mailbox manager, do this:

Step 1. Enter the **/RADMIN.AD.CM** path**.**

If you have …	**Proceed as follows:**
Already defined the system image	Enter **S** beside the system image on the displayed System Image List panel.
Not yet defined your system image	Press ENTER at the Confirm System Image Add panel to add a system image. For information about how to create a system image definition, see the section, *Defining a System Image*, on page 10-4.

The ResourceView : C:Mailbox Resource Group Definition panel is displayed.

Step 2. Enter a file server started task name in the File Server Started Task Name field.

The started task name specifies the name of the CONNECT:Mailbox VSAM file server started task that is the subject of this definition. The VSAM file server is automatically defined as the parent of the CONNECT:Mailbox manager.

Step 3. Enter a CONNECT:Mailbox manager name in the Manager Name field.

The manager name specifies the CONNECT:Mailbox started task that is the subject of this definition.

Step 4. Enter an ACB name in the ACB Name field.

This field is optional. If an ACB name is specified, NetMaster for File Transfer activates the ACB during resource activation.

Step 5. Press F3 (File) to file the resource definition.

The ResourceView : C:Mailbox Manager List panel is displayed.

This newly created resource will manage or monitor your CONNECT:Mailbox application. You can modify it at a later stage, as described in Chapter 15, *Customizing the Environment That Manages File Transfer Resources*.

You have completed the CONNECT:Mailbox manager resource definition. To define monitor resources for the manager, do this:

Step 1. Enter **G** beside a manager resource definition to generate monitor resources for the manager resource, as shown in Figure 10-17.

Figure 10-17. Generating CONNECT:Mailbox Monitor Resources

```
SOLVPROD----------- ResourceView : C:Mailbox Manager List --------------------2
Command ===>                                                   Scroll ===> PAGE

. System Image -------------------------------------------------------------.
| System Name ...+ HYSYSIMG     Version ...+ 0001                            |
'------------------------------------------------------------------------------'
. Resources ----------------------------------------------------------------.
|        S/B=Browse U=Update C=Copy D=Delete G=Generate MON=Monitors R=Relate |
|     CMMGR Name         Description                                        |
| G   CMMGR1             C:Mailbox MANAGER                                  |
|     **END**                                                               |
```

A list of the available monitor resource types is displayed.

Step 2. Enter **S** beside each type of monitor you want to generate for your manager resource definition.

Step 3. With your monitor types selected, a panel for each monitor is displayed. Enter the name of each monitor, and optionally, a long description of the monitor, as shown in Figure 10-18.

Figure 10-18. Entering CONNECT:Mailbox Monitor Details

```
SOLVPROD---- ResourceView : C:Mailbox Monitor General Description -----CD1-0001
Command ===>                                                   Function=ADD

System Name ..+ FTI        Database Version ..+ 0001
C:Mailbox Monitor Name ........................ ACQ_____
C:Mailbox Monitor Type .......................+ ACQUEUE_____


C:Mailbox Manager Name .......................+ CMSTC___

Operation Mode .....+ MANUAL_____
Short Description ... Queued Auto Connect Monitor___
Long Description .... ____________________________________________________________
                      ____________________________________________________________
                      ____________________________________________________________
                      ____________________________________________________________
```

Step 4. Press F8 (Forward) to display the Monitor Details panel, and review the settings.

Step 5. Press F3 (File) to save the monitor resource definition.

Step 6. When you have filed the details for all selected monitors, you are returned to the ResourceView : C:Mailbox Manager List panel. You can enter **G** beside another manager resource and repeat Step 2 through Step 5 to define its monitor resources.

Step 7. Press F3 (Exit) to exit the ResourceView : C:Mailbox File Transfer Manager List panel.

You can customize the resource definitions created by the Assisted Resource Definition Facility. See Chapter 15, *Customizing the Environment That Manages File Transfer Resources*, for information about customizing resource definitions.

Defining FTS Resources

A NetMaster for File Transfer region can manage FTS applications on the local system and monitor FTS applications on remote systems. To enable the region to perform these functions, define managers and monitors for these applications in the system image.

Proceed as follows:

Step 1. Enter the **/RADMIN.AD.FTS** path.

If you have …	**Proceed as follows:**
Already defined the system image	Enter **S** beside the system image on the displayed System Image List panel.
Not yet defined your system image	Press ENTER at the Confirm System Image Add panel to add a system image. For information about how to create a system image definition, see the section, *Defining a System Image*, on page 10-4.

The FTS File Transfer Manager General Description panel is displayed.

Step 2. Enter an FTS manager name in the FTS File Transfer Manager Name field.

Note

You define a manager resource for each FTS application you want to manage or monitor in this system domain.

The manager name identifies the FTS resource that is the subject of this definition. The specified name must be the same as that used for the FTS started task or job (see Figure 10-19).

Figure 10-19. Entering Details for the FTSMGR

```
-------- ResourceView : FTS File Transfer Manager General Description ---------
Command ===>                                                   Function=ADD

System Name ..+ FT1        Database Version ..+ 0001
FTS File Transfer Manager Name ................ DEFTS1
FTS File Transfer Manager Type ...............+ STC

ACB Name ............ DEFTS1


Operation Mode .....+ AUTOMATED
Short Description ... FTS started task
Long Description ....
```

Step 3. Enter the manager type in the Manager Type field.

If the FTS application is initialized …	Enter …
As a started task	**STC** as the manager type.
As a job	**JOB** as the manager type.
On another system	**REMOTE** as the manager type.

Step 4. Enter **AUTOMATED** or **MANUAL** in the Operation Mode field.

Step 5. Briefly describe this resource in the Short Description field (for example, FTS started task).

Step 6. Press F3 (File) to file the manager resource definition.

The ResourceView : FTS File Transfer Manager List panel is displayed.

Note

If you specified that the FTS application was initiated by a job, you should ensure that the message text on the resource definition Display and Heartbeat Details panel is valid for your job. To do this, enter **S** beside the listed manager resource and select the Display and Heartbeat Details Panel from the displayed list.

This newly created resource will manage or monitor your FTS application. You can modify it at a later stage, as described in Chapter 15, *Customizing the Environment That Manages File Transfer Resources.*

You have completed the FTS manager resource definition, and can now define monitor resources for the manager, as described in the following steps.

Step 7. Enter **G** beside a manager resource definition to generate monitor resources for the manager resource, as shown in Figure 10-20.

Figure 10-20. Generating FTS Monitor Resources

```
SOLVPROD------- ResourceView : FTS File Transfer Manager List ----------------1
Command ===>                                                   Scroll ===> PAGE

. System Image -------------------------------------------------------------.
| System Name ...+ FT1          Version ...+ 0001                            |
'------------------------------------------------------------------------------'
.- Resources ---------------------------------------------------------------.
|        S/B=Browse U=Update C=Copy D=Delete G=Generate MON=Monitors R=Relate |
|     FTSMGR Name        Description                                         |
|  G  DEFTS1             FTS started task                                    |
|     **END**                                                                |
```

The panel for defining an FTS file transfer monitor is displayed.

Step 8. Enter the name of the monitor and a brief description of the monitor, as shown in Figure 10-21.

Figure 10-21. Entering FTS Monitor Details

```
-------- ResourceView : FTS File Transfer Monitor General Description ---------
Command ===>                                                   Function=ADD

System Name ..+ FT1        Database Version ..+ 0001
FTS File Transfer Monitor Name ............... LINKFTS2
FTS File Transfer Monitor Type ..............+ LINK________


FTS File Transfer Manager Name ............... DEFTS1__

Operation Mode .....+ MANUAL_____
Short Description ... FTS link monitor______________
Long Description .... ______________________________________________________
                      ______________________________________________________
                      ______________________________________________________
                      ______________________________________________________
```

Step 9. Press F8 (Forward) to display the Monitor Details panel.

Step 10. Specify the name of an INMC link defined in the managed FTS region (for example, the name of an FTS-to-FTS INMC link).

Step 11. Press F4 (Save) to save the monitor resource definition.

Step 12. Repeat Step 8 through Step 11 to define resources for each INMC link you want to monitor. You should define a monitor resource for each INMC link that is used for file transfers.

Step 13. When you have defined all your FTS file transfer monitors, press F3 (File) and you are returned to the ResourceView : FTS File Transfer Manager List panel. You can enter **G** beside any manager resource and repeat Step 8 through Step 12 to define monitor resources for the manager resources.

Step 14. Press F3 (Exit) to exit the ResourceView : FTS File Transfer Manager List panel.

You can customize the resource definitions created by the Assisted Resource Definition Facility. See Chapter 15, *Customizing the Environment That Manages File Transfer Resources*, for information about customizing resource definitions.

Defining FTP Resources

A NetMaster for File Transfer region can manage FTP server applications on the local system and monitor the health of FTP connections. To enable the region to perform these functions, define managers and monitors for these applications in the system image.

Note

For TCPaccess FTP managers, the data space (subject to the FTCNTL parameter group setting) and SOLVE SSI are also monitored by this resource.

Proceed as follows:

Step 1. Enter the **/RADMIN.AD.FTP** path.

If you have …	**Proceed as follows:**
Already defined the system image	Enter **S** beside the system image on the displayed System Image List panel.
Not yet defined your system image	Press ENTER at the Confirm System Image Add panel to add a system image. For information about how to create a system image definition, see the section, *Defining a System Image*, on page 10-4.

The FTP Server Manager General Description panel is displayed.

Step 2. Enter an FTP manager name in the FTP Server Manager Name field.

Note

You define a manager resource for each FTP server application you want to manage or monitor in this system domain.

The manager name identifies the FTP server resource that is the subject of this definition (see Figure 10-22). The specified name must be as follows:

For …	Ensure that the manager name is the …
Communications Server FTP server	FTP background daemon name (usually, FTPD1).
TCPaccess server	Server name.
TCPaccess FTP server	FTP server started task or batch job name

Figure 10-22. Entering Details for the FTPMGR

```
---------- ResourceView : FTP Server Manager General Description -SOLVPROD-0001
Command ===>                                                     Function=ADD

System Name ..+            Database Version ..+ 0001
FTP Server Manager Name ....................... FTPSRVR_
FTP Server Manager Type .....................+ STC_________




Operation Mode .....+ AUTOMATED__
Short Description ... FTP server started task____
Long Description .... ____________________________________________________________
                      ____________________________________________________________
                      ____________________________________________________________
                      ____________________________________________________________

.- Template Selection -------------------------------------------------------.
|                                M=Merge O=Override R=Reset S/B=Browse L=List  |
|      TemplateName        Copy AvailMap   Copy Process                       |
| ___  MCSSTC______        _______         _______                            |
-------------------------------------------------------------------------------
 F1=Help      F2=Split     F3=File      F4=Save
                           F9=Swap                                F12=Cancel
```

Step 3. Enter the manager type in the Manager Type field.

If the FTP server is initialized as a …	Enter …
Started task	**STC** as the manager type.
Job	**JOB** as the manager type.

Step 4. Enter **AUTOMATED** or **MANUAL** in the Operation Mode field.

Key Concept

The two types of operation mode are as follows:

- AUTOMATED—the resource is monitored and controlled (activated and inactivated) by the region.
- MANUAL—the resource can be controlled manually, and the region monitors but does *not* control the resource.

Step 5. Briefly describe this resource in the Short Description field (for example, FTP server started task).

Step 6. Position your cursor in the first input field of the Template Selection window, and enter **L**.

The ResourceView : FTP Server Manager Template List is displayed.

Step 7. Depending on the resource for which you are defining an FTPMGR, enter **M** beside the corresponding template name, as shown in the table.

Server or Region	Job or Started Task	Template Name
Communications Server FTP server	Started task	ECSSTC
TCPaccess server	Job	AXS52JOB or AXS53JOB
TCPaccess server	Started task	AXS52STC or AXS53STC
TCPaccess FTP server	Job	SFTPJOB
TCPaccess FTP server	Started task	SFTPSTC

A message is displayed to confirm that the template values have been assigned to the resource definition.

Key Concept

Applying the M (Merge) action merges the values defined in the template with your resource definition.

You can apply O (Override) or R (Reset) for the same effect as the resource definition has no values incorporated at this stage.

See the online help for additional information about these actions.

Step 8. Continue as follows:

If you are defining …	Proceed as follows:
An Communications Server FTP server manager	On the Activation Details panel, ensure that the name in the Sys Cmd/JCL Mem field matches the FTP server started task name, and then go to Step 9.
A manager for an FTP application initiated by a job	On the Display and Heartbeat Details panel, ensure that the message text is valid for your job, and then go to Step 9.
Other managers	Go to Step 9.

Step 9. Press F3 (Exit) and then F3 (File) to file the manager resource definition.

The ResourceView : FTP Server Manager List panel is displayed.

This newly created resource will manage and monitor your FTP server application. You can modify it at a later stage, as described in Chapter 15, *Customizing the Environment That Manages File Transfer Resources.*

You have completed the FTP manager resource definition, and can now define monitor resources for the manager, as described in the following steps.

Step 10. Enter **G** beside a manager resource definition to generate monitor resources for the manager resource, as shown in Figure 10-23.

Figure 10-23. Generating FTP Monitor Resources

```
SOLVPROD------- ResourceView : FTP File Transfer Manager List ----------------1
Command ===>                                                   Scroll ===> PAGE

. System Image -------------------------------------------------------------.
| System Name ...+ FT1          Version ...+ 0001                           |
'----------------------------------------------------------------------------'
. Resources ----------------------------------------------------------------.
|        S/B=Browse U=Update C=Copy D=Delete G=Generate MON=Monitors R=Relate |
|     FTPMGR Name        Description                                        |
|  G  DEFTP1             FTP server                                         |
|     **END**                                                               |
```

A list of FTP server monitors is displayed.

Step 11. Enter **S** beside each type of monitor you want to generate for your manager resource definition, as shown in Figure 10-24.

Figure 10-24. Selecting FTP Monitor Templates

```
SOLVPROD---------- ResourceView : FTP Server Monitor List --------------------3
Command ===>                                                   Scroll ===> PAGE

                                      Use 'S' to Select Monitor(s) to Generate
    FTPMON Name        Description
S   CONNECTIONS        FTP TCP/IP Connections Monitor
S   IPLISTEN           FTP Listener Port Monitor
S   REMOTENODE         FTP Remote Node Monitor
    **END**
```

Step 12. With your monitor types selected, a panel for each monitor is displayed. Enter the name of each monitor, and optionally, a long description of the monitor, as shown in Figure 10-25.

Figure 10-25. Entering FTP Server Monitor Details

```
------------ ResourceView : FTP Server Monitor General Description ------------
Command ===>                                                     Function=ADD

System Name ..+ FT1        Database Version ..+ 0001
FTP Server Monitor Name ................ TCPCONN
FTP Server Monitor Type ...............+ TCP-CONNECT_


FTP Server Manager Name ................ FTP1____

Operation Mode .....+ MANUAL_____
Short Description ... FTP TCP/IP Connection Monitor_
Long Description .... This monitors TCP/IP connections_____________________
```

Step 13. Press F8 (Forward) to display the Monitor Details panel, and review the settings.

If you are defining a TCP/IP listener port monitor, specify, if required, an SNMP community name. The default name is `public`. The specified community must include the IP addresses of the local OS/390 system.

If you are defining a TCP/IP listener port monitor for a TCPaccess application, you *must* also specify the TCP/IP port number used by the FTP server.

Step 14. Press F3 (File) to file the monitor resource definition.

Step 15. When you have filed the details for all selected monitors, you are returned to the ResourceView : FTP Server Manager List panel. You can enter **G** beside any remaining manager resources and repeat Step 3 to Step 6 to define monitor resources for the manager resources.

Step 16. Press F3 (Exit) to exit the ResourceView : FTP Server Transfer Manager List panel.

You can customize the resource definitions created by the Assisted Resource Definition Facility. See Chapter 15, *Customizing the Environment That Manages File Transfer Resources*, for information about customizing resource definitions.

Defining TCP/IP Resources

This section describes how you add your IBM TCP/IP or TCPaccess resources to a system image. The definition enables a NetMaster for File Transfer region to manage the TCP/IP resources.

Note

If TCPaccess is your FTP server, you may have defined an FTPMGR resource for your TCPaccess region. If so, it is not necessary to define a TCPaccess resource as well.

To define the resource to your system image, proceed as follows:

Step 1. Enter the **/RADMIN** shortcut to display the Resource Administration menu.

Step 2. Identify the system image to which this resource belongs in the System Name and Version fields, then enter **R.STC** to display the Started Task List panel.

Step 3. Press F4 (Add) to create a resource definition.

The Started Task General Description panel is displayed.

Step 4. Enter a name in the Started Task Name field to identify the resource.

Caution

For TCP/IP started task class (STC) resources, the specified name must be the same as that used for the started task.

Figure 10-26. Entering Details for a TCP/IP Resource

```
SOLVPROD------- ResourceView : Started Task General Description -------FT1-0001
Command ===>                                                     Function=ADD

System Name ..+ FT1        Database Version ..+ 0001
Started Task Name ............................ TCPIPMVS
Started Task Type ...........................+ ____________


ACB Name ............ ________

Operation Mode .....+ AUTOMATED__
Short Description ... Communications Server_________
 Long Description .... ____________________________________________________________
                       ____________________________________________________________
                       ____________________________________________________________
                       ____________________________________________________________

. Template Selection -------------------------------------------------------------.
|                                M=Merge O=Override R=Reset S/B=Browse L=List |
|      TemplateName         Copy AvailMap   Copy Process                      |
| L__  ____________         YES____         YES____                           |
'----------------------------------------------------------------------------'
 F1=Help      F2=Split     F3=File      F4=Save      F5=Related
              F8=Forward   F9=Swap                  F11=Panels   F12=Cancel
```

Step 5. Enter **AUTOMATED** or **MANUAL** in the Operation Mode field (see Figure 10-26).

Step 6. Enter a short description that describes this resource in the Short Description field (for example, Communications Server as shown in Figure 10-26).

Step 7. Position your cursor in the first input field of the Template Selection window, and enter **L**.

The ResourceView : Started Task Template List is displayed.

Step 8. Depending on the resource you are defining, proceed as follows:

If you are defining a …	**Enter** M **beside the template name …**
Communications Server resource	COMSERVER.
TCPaccess resource	TCPAXS52 or TCPAXS53.

A message is displayed to confirm that the template values have been assigned to the resource definition.

Key Concept

Applying the M (Merge) action merges the values defined in the template with your resource definition.

You can apply O (Override) or R (Reset) for the same effect, because the resource definition has no values incorporated at this stage.

See the online help for additional information about these actions.

Step 9. Press F3 (Exit) to exit from the displayed panel.

The ResourceView : Started Task General Description is displayed with updated fields. Figure 10-27 shows an example.

You can scroll through the resource definition panels by pressing F8 (Forward). See Chapter 15, *Customizing the Environment That Manages File Transfer Resources* for additional information about customizing resource definitions.

Figure 10-27. Updated Started Task General Description Panel

```
SOLVPROD------- ResourceView : Started Task General Description -------FT1-0001
Command ===>                                                     Function=ADD

System Name ..+ FT1        Database Version ..+ 0001
Started Task Name ............................ TCPIPMVS
Started Task Type ...........................+ TCPIPMVS____


ACB Name ............ ________

Operation Mode .....+ AUTOMATED__
Short Description ... Communications Server_________
Long Description .... ____________________________________________________________
                      ____________________________________________________________
                      ____________________________________________________________
                      ____________________________________________________________

. Template Selection -------------------------------------------------------.
|                              M=Merge O=Override R=Reset S/B=Browse L=List |
|      TemplateName         Copy AvailMap   Copy Process                    |
| ___  COMSERVER___         YES____         YES____                         |
'----------------------------------------------------------------------------'
 F1=Help      F2=Split     F3=File      F4=Save      F5=Related
              F8=Forward   F9=Swap                  F11=Panels   F12=Cancel
```

Step 10. Press F3 (File) to file the resource definition.

The ResourceView : Started Task List panel is displayed with the STC resource listed. Figure 10-28 shows an example.

Figure 10-28. List of Defined Resources

```
SOLVPROD-------------- ResourceView : Started Task List ----------------------1
Command ===>                                                 Scroll ===> CSR
RMPD0003 ADD COMPLETED SUCCESSFULLY
. System Image -------------------------------------------------------------.
| System Name ...+ FT1_____     Version ...+ 0001                           |
'----------------------------------------------------------------------------'
. Resources ----------------------------------------------------------------.
|           S/B=Browse U=Update C=Copy CCC=Cross Class Copy D=Delete R=Relate |
|     STC Name           Description                                       |
|     TCPIPMVS           Communications Server                             |
|     **END**                                                              |
```

Step 11. Repeat Step 3 through Step 10 to add other STC resources.

These newly created resources will manage the tasks for which they are defined. You can modify them at a later stage, as described in Chapter 15, *Customizing the Environment That Manages File Transfer Resources*.

Auto-populating a System Image with DASD and Tape Resource Definitions

The AutoAssist Auto Populate Facility enables you to select particular DASD and tape resources you want to define to the system image.

Use the Auto Populate Facility to quickly create definitions in a system image for specific current resources on the local system. You can then customize the definitions individually or add definitions not reflected in the local current resource list. The facility does not overwrite existing definitions.

Using the Auto Populate Facility to Define DASD and Tape Resources

To use the Auto Populate Facility, proceed as follows:

Step 1. Enter the **/RADMIN.AD.A** path to access the Auto Populate Facility. The Auto Populate menu is displayed.

Note

If a system image does not already exist in the knowledge base, NetMaster for File Transfer will prompt you to create an image definition. For information about how to create a system image definition, see the section, *Defining a System Image*, on page 10-4.

Step 2. Type the option code for the class of resources you want to build at the Select Option ===> prompt as follows:

If you want to build …	Type …
DASD resources	D
Tape resources	T

Step 3. Complete the fields on the panel as follows:

- Identify the system image (to which you want to add the definitions for the local resources) in the System Name and Version fields.
- Identify the template to be used to create the definitions in the Template field as follows:

For …	**Type …**
DASD resources	DASD
Cartridge resources	STDCART
3420 type tape resources	STDTAPE
3480 type tape resources	TAPE

- Use the Resource Mask field to restrict the list of resources that will be displayed for which you can build definitions. Use the asterisk (*) as the wildcard character. A leading or embedded * represents a single character; a trailing * represents any number of characters. For example, **A0 includes 00A0, 01A0, … while 09* includes 09A0, 09A1, 09A2, …
- Indicate whether you want to create definitions for online resources only in the On Line Only? field. If you specify NO, all configured resources of the selected class (whether online or not) are retrieved for you to select.

After you complete the fields, press ENTER to access the current list of the class of resources you selected. The Auto Populate Selection List panel is displayed. Figure 10-29 is an example for DASD resources.

Figure 10-29. Auto Populate Selection List Panel

```
SOLVPROD------- AutoAssist : Auto Populate Selection List ---------------------
Command ===>                                                   Scroll ===> CSR

                                        S=Select Resource  U=Unselect Resource
    Name                Template     Description
    09A0                DASD         DASD 09A0 - VOLSER PGM003
    09A1                DASD         DASD 09A1 - VOLSER DEV007
    09A2                DASD         DASD 09A2 - VOLSER SSSMS1
    09A3                DASD         DASD 09A3 - VOLSER OS3SRS
    09A4                DASD         DASD 09A4 - VOLSER OS3SCT
    09A5                DASD         DASD 09A5 - VOLSER OS3SDL
    09B0                DASD         DASD 09B0 - VOLSER TST003
    09B1                DASD         DASD 09B1 - VOLSER PKG004
    09B2                DASD         DASD 09B2 - VOLSER OS4SRS
    09B3                DASD         DASD 09B3 - VOLSER OS4SCT
    09B4                DASD         DASD 09B4 - VOLSER OS4SDL
    09B5                DASD         DASD 09B5 - VOLSER OS4TMP
    0927                DASD         DASD 0927 - VOLSER IBM927
    098A                DASD         DASD 098A - VOLSER SAP001
    098B                DASD         DASD 098B - VOLSER SAN001
    098C                DASD         DASD 098C - VOLSER MSTSP1
    098D                DASD         DASD 098D - VOLSER WORKS1
 F1=Help      F2=Split                                          F6=Action
 F7=Backward  F8=Forward   F9=Swap                             F12=Cancel
```

Step 4. Type **S** next to the resources for which you want to build definitions. If you want to select all the displayed resources, enter **ALL S** at the Command ===> prompt.

You can press ENTER to validate your selections. The selections are tagged as selected. If you want to unselect a selected resource, enter **U** beside the resource. If you want to unselect all selected resources, enter **ALL U** at the Command ===> prompt.

Note

You can, if necessary, change the templates for individual resources.

Caution

If you want to cancel the operation, you must press F12 (Cancel) before the next step.

Step 5. Press F6 (Action) to build the resource definitions.

Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on an AS/400 System

You can define file transfer rules, schedules, and resources to enable your NetMaster for File Transfer region to manage a CONNECT:Direct for OS/400 file transfer service on an AS/400 system.

Note

To manage a CONNECT:Direct file transfer service on an AS/400 system, you must have implemented the AS/400 agent for NetMaster for File Transfer.

To enable communications between the region and the CONNECT:Direct application on the AS/400 system, you must define a CONNECT:Direct manager for the application.

For information about how to define …	See the section …
File transfer rules	*Defining File Transfer Rules*, on page 10-6.
File transfer schedules	*Defining File Transfer Schedules*, on page 10-18.
CONNECT:Direct managers and monitors	*Creating a CONNECT:Direct Manager*, on page 10-29.

Considerations for managing CONNECT:Direct for OS/400 products in a multisystem environment are similar to those for managing remote CONNECT:Direct for UNIX products (see the section, *Multisystem Considerations*, on page 10-55).

Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on a Tandem System

You can define file transfer rules, schedules, and resources to enable your NetMaster for File Transfer region to manage a CONNECT:Direct for Tandem file transfer service on a Tandem system.

Note

To manage a CONNECT:Direct file transfer service on a Tandem system, you must have implemented the Tandem agent for NetMaster for File Transfer.

To enable communications between the region and the CONNECT:Direct application on the Tandem system, you must define a CONNECT:Direct manager for the application.

For information about how to define …	See the section …
File transfer rules	*Defining File Transfer Rules*, on page 10-6.
File transfer schedules	*Defining File Transfer Schedules*, on page 10-18.
CONNECT:Direct managers and monitors	*Creating a CONNECT:Direct Manager*, on page 10-29.

Considerations for managing CONNECT:Direct for Tandem products in a multisystem environment are similar to those for managing remote CONNECT:Direct for UNIX products (see the section, *Multisystem Considerations*, on page 10-55).

Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on a UNIX System

You can define file transfer rules, schedules, and resources to enable your NetMaster for File Transfer region to manage a CONNECT:Direct for UNIX file transfer service on a UNIX system.

Note

To manage a CONNECT:Direct file transfer service on a UNIX system, you must have implemented the UNIX agent for NetMaster for File Transfer.

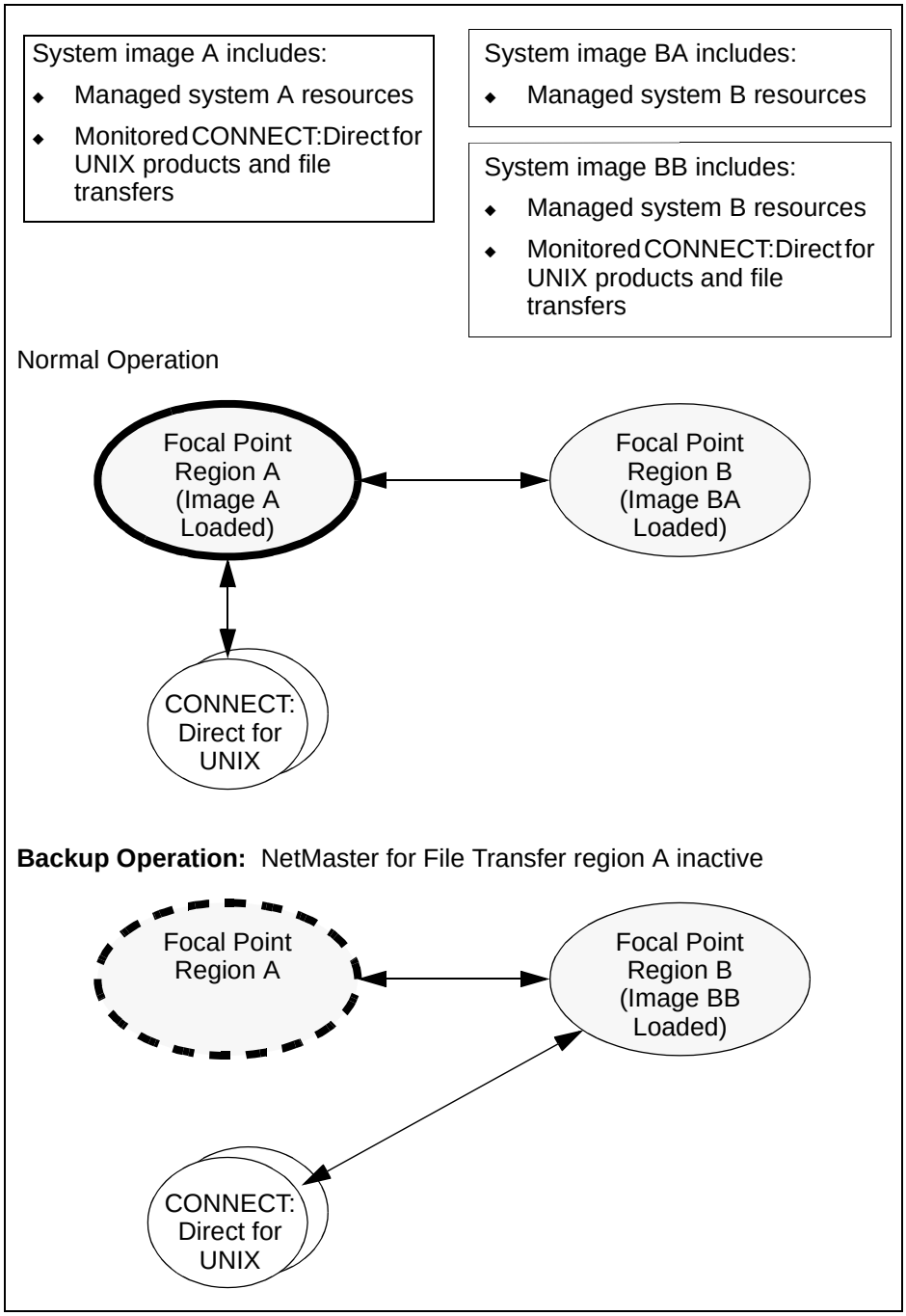
To enable communications between the region and the CONNECT:Direct application on the UNIX system, you must define a CONNECT:Direct manager for the application.

For information about how to define …	See the section …
File transfer rules	*Defining File Transfer Rules*, on page 10-6.
File transfer schedules	*Defining File Transfer Schedules*, on page 10-18.
CONNECT:Direct managers and monitors	*Creating a CONNECT:Direct Manager*, on page 10-29.

Multisystem Considerations

In a multisystem environment, you decide which NetMaster for File Transfer regions should monitor the remote CONNECT:Direct products on your UNIX systems. You can switch the monitoring functions between the different regions. Figure 10-30 shows an example in which you create a backup system image, BB, for the monitored CONNECT:Direct for UNIX products.

Figure 10-30. Backup System Image for Remote File Transfer Products



During normal operation, all defined resources are monitored. If NetMaster for File Transfer region A becomes inactive (for example, stopped for system maintenance), all resources (including the CONNECT:Direct for UNIX products) defined to system image A cannot be monitored.

However, if a backup system image has been defined for NetMaster for File Transfer region B that includes the CONNECT:Direct for UNIX products, it can be loaded when region A becomes inactive. During backup operation, region B monitors the CONNECT:Direct for UNIX products in addition to system B resources.

Note

You can also build your system images such that you can use the MV command to switch the management of the CONNECT:Direct for UNIX products between different NetMaster for File Transfer regions (see the online help).

Defining Rules, Schedules, and Resources to Manage a CONNECT:Direct File Transfer Service on a Windows NT System

You can define file transfer rules, schedules, and resources to enable your NetMaster for File Transfer region to manage a CONNECT:Direct for Windows NT file transfer service on a Windows NT system.

Note

To manage a CONNECT:Direct file transfer service on a Windows NT system, you must have implemented the Windows NT agent for NetMaster for File Transfer.

To enable communications between the region and the CONNECT:Direct application on the Windows NT system, you must define a CONNECT:Direct manager for the application.

For information about how to define …	See the section …
File transfer rules	*Defining File Transfer Rules*, on page 10-6.
File transfer schedules	*Defining File Transfer Schedules*, on page 10-18.
CONNECT:Direct managers and monitors	*Creating a CONNECT:Direct Manager*, on page 10-29.

Considerations for managing CONNECT:Direct for Windows NT products in a multisystem environment are similar to those for managing remote CONNECT:Direct for UNIX products (see the section, *Multisystem Considerations*, on page 10-55).

Defining Rules, Schedules, and Resources to Manage a Remote FTS Region

You can define file transfer rules, schedules, and resources to enable your NetMaster for File Transfer region to manage an FTS file transfer service on a remote system. You can communicate with the remote region, but you cannot control the remote region itself.

Note

To manage the file transfers in a remote FTS region, you must have customized the remote region according to the section, *Subtask 7.4—Customizing the Managed FTS Regions*, on page 5-36.

To enable communications between the NetMaster for File Transfer region and the remote FTS region, you must define an FTS manager for the application. The manager type is REMOTE.

For information about how to define …	See the section …
File transfer rules	*Defining File Transfer Rules*, on page 10-6.
File transfer schedules	*Defining File Transfer Schedules*, on page 10-18.
FTS managers and monitors	*Defining FTS Resources*, on page 10-40.

Considerations for managing remote FTS regions in a multisystem environment are similar to those for managing remote CONNECT:Direct for UNIX products (see the section, *Multisystem Considerations*, on page 10-55).

Loading, Checking, and Automating Your File Transfer Management Environment

This section describes how to:

- Load a system image and a file transfer rule set
- Check your built environment
- Set your NetMaster for File Transfer region to AUTOMATED

Loading the System Image and File Transfer Rule Set

The system image and file transfer rule set that you have defined must be loaded into your NetMaster for File Transfer region before you can monitor your file transfer service.

Note

You can load a rule set independently of the system image. For further information see *Loading a Rule Set on Demand*, on page 10-9.

To load the system image and the rule set, proceed as follows:

Step 1. At the Command ===> prompt, enter **/ICS.**

Note

You must have the required authority to access the Initialization Parameters panel. Ask your system administrator to either give you the required access authority or perform this task for you.

The Customization Parameters panel is displayed.

Step 2. Enter **F AUTOIDS** to find the AUTOIDS parameter group, and then enter **U** beside it.

The Initialization Parameters panel for the parameter group is displayed.

Step 3. Enter the name of the system image defined in the section, *Defining a System Image*, on page 10-4.

Step 4. Ensure that the Automation Mode field is set to MANUAL.

This field sets the global operation mode. Setting the mode to MANUAL ensures that all resources operate in the MANUAL mode. This allows you to familiarize yourself with the product before automating the management of your file transfer service.

Step 5. Enter **YES** in the Perform Action in Manual Mode? field, as shown in Figure 10-31.

Figure 10-31. Initialization Parameters Panel

```
SOLVPROD-------------- ICS : Initialization Parameters -------------Page 1 of 1
Command ===>                                                   Function=Update

.- AUTOIDS - Automation Identifiers ----------------------------------------.
|                                                                           |
| System Image Name (1) .............+ FT1______                           |
| Version (1) .......................+ 0001                               |
| Automation Mode (1) ............... MANUAL___ (Automated or Manual)      |
| Default Desired State ............. ACTIVE__  (Active or Inactive)       |
| Perform Action in Manual Mode? ..... YES_      (Yes or No)                |
| Active Ruleset for File Transfer...+ CARDS___                             |
| Checkpoint Restart Status .......... ACTIVE__  (Active or Inactive)       |
| Cold Start on Next Restart? (1) .... NO__      (Yes or No)                |
|                                                                           |
| Confirm via WTOR at Startup? ....... NO_       (No or Yes to confirm values |
|                                                 of fields denoted by (1) ) |
| Role in Multi-system Operation ..... FOCAL                                |
'---------------------------------------------------------------------------
'

.- Notes -------------------------------------------------------------------.
| Warning: If actioned the specified System Image will be reloaded.         |
'---------------------------------------------------------------------------
'
 F1=Help      F2=Split     F3=File      F4=Save      F5=ILog      F6=Action
                           F9=Swap                                F12=Cancel
```

Step 6. Enter the name of the file transfer rule set defined in the section, *Defining File Transfer Rules*, on page 10-6.

If no rule set is specified, no rules are triggered.

Step 7. Press F6 (Action) to action the parameter group.

The system image and the file transfer rule set are loaded, and a message is displayed indicating that the $RM AUTOIDS parameter group has been set.

Note

A loaded image or rule set is displayed with highlight on the System Image List or the File Transfer Ruleset List panel. You can use these lists to determine which image or rule set is loaded.

Step 8. Press F3 (File) to file the change.

When the NetMaster for File Transfer region is next started, the specified system image and file transfer rule set are automatically loaded.

You have now loaded your system image and are ready to check if the environment you built manages the file transfer service as required, as described in the following section.

Key Concept

After you have loaded an image, you can define additional resources to it and the defined resources will immediately become available to the region. Similarly, you can add rules to a loaded file transfer rule set and the rules will immediately become available to the region.

Checking the Built Environment

Enter the **/FTMON** shortcut at the Command ===> prompt to display the file transfer status monitor.

Figure 10-32 shows an example that displays the status of file transfer resources defined for the loaded system image.

Note

If the displayed resource names are truncated, enter **FORMAT LONGNAME** to increase their display width.

Figure 10-32. File Transfer Resources Status Monitor

```
SOLVPROD----------- Status Monitor : File Transfer Resources ----------FT1-0001
Command ===>                                                   Scroll ===> PAGE

                  S=Status L=Log D=Display A=Act T=Term DB=Database ?=List Cmds
    System   Class Resource          Desired  Actual    Mode      Logical   Ovr
    FT1      CDMGR ALCDUNX1          ACTIVE   ACTIVE    MANUAL    OK
    FT1      CDMGR DECD1             ACTIVE   ACTIVE    MANUAL    OK
    FTI      CDMON DECD1.ALCDUNX1    ALCDUNX1 AVAILABLE AT 09.33
    FT1      CDMON DECD1.HOLDQ       QUEUE(HOLD) STATUS(ANY) CNT(10) AT 14.20
    FT1      CDMON DECD1.LISTENER    LISTENER TASK FOUND AT 14.34
    FT1      CDMON DECD1.RETRYQ      QUEUE(TIMER) STATUS(RETRY) CNT(1) AT 14.34
    FT1      CDMON DECD1.TCPCON      0 CONNECTIONS CHECKED. ALL OK AT 14.39
    FT1      CDMON DECD1.TIMERQ      QUEUE(TIMER) STATUS(ANY) CNT(0) AT 14.04
    FTI      CDMON DECD1.TRANSFER    NO TRANSFERS FOUND AT 14.36
    FT1      FTPMG FTPSVR            ACTIVE   ACTIVE    MANUAL    OK
    FT1      FTPMO FTPSVR.LISTENER   LISTENER TASK FOUND AT 14.53
    FT1      FTPMO FTPSVR.TCPCON     0 CONNECTIONS CHECKED. ALL OK AT 15.53
    FT1      FTSCH ALCARDSCHEDL      PROC 14.30 REQ:0069 COMP:0001 FAIL:0000
    FT1      FTSMG CAFTS1            UNABLE TO COMMUNICATE WITH CAFTS1 14.50
    FT1      FTSMO CAFTS1.CAAR       UNABLE TO COMMUNICATE WITH CAFTS1 14.50
    FT1      XCMGR XC3000            ACTIVE   ACTIVE     MANUAL     OK
    FT1      XCMON XC3000.STALL      NO TRANSFERS FOUND AT 14.05
 F1=Help      F2=Split     F3=Exit      F4=Add       F5=Find
 F7=Backward  F8=Forward   F9=Swap                   F11=Right
```

You should ensure that the state of the displayed resources reflects the state of the resources that you have defined to your system image.

Various commands are available to you that can be issued against listed resources. These commands enable you to perform actions against a resource or display information about a resource, such as:

- Activating a resource
- Terminating a resource
- Displaying resources owned by a manager
- Listing CONNECT:Direct processes

To display the list of commands, enter **?** beside a resource. The list of commands is displayed along with a description of each command.

If you are satisfied that your resources have been defined correctly, you can set your global operation mode to AUTOMATED, as described in the section, *Setting the Built Environment to Automated Operation*, on page 10-62.

Setting the Built Environment to Automated Operation

To set the file transfer management environment to automated operation, you must set your global operation mode to AUTOMATED. This enables the control of resources defined in your system image to be automated.

Key Concept

The *default* desired state of the defined resource(s) is specified by your system administrator in the $RM AUTOIDS parameter group. The default state is either ACTIVE or INACTIVE.

If you set the global operation mode to AUTOMATED and the default resource desired state is set to ACTIVE, the region will attempt to automatically start all automated resources.

For a resource such as a CONNECT:Direct region, you can specify the desired state of the resource and the times you require the resource to be active or inactive, by using the availability map in the resource definition. See the section, *Specifying the Availability of Supporting File Transfer Resources*, on page 15-24, for additional information about customizing availability maps.

To set the global operation mode to AUTOMATED, proceed as follows:

Step 1. Enter **GLOBAL** at the Command prompt.

Step 2. The Global Command Parameter Specification panel is displayed.

Step 3. Enter **AUTOMATED** in the Global Automation Mode field, and press F6 (Action), as shown in Figure 10-33.

Figure 10-33. Global Command Parameter Specification Panel

```
SOLVPROD-------------  GLOBAL Command Parameter Specification -----------------
Command ===>

.- Global Command Parameter ---------------------------------------------------.
|                                                                               |
|  ACB Name .................. DECD1                                          |
|                                                                               |
|  Current SysName ........... FT1                                            |
|  Current Version ........... 0001                                           |
|                                                                               |
|  Current Automation Mode ... MANUAL                                           |
|                                                                               |
|  Global Automation Mode .... AUTOMATED (Automated or Manual)                  |
|                                                                               |
'-------------------------------------------------------------------------------'
```

Press F6 to action the GLOBAL command.

A confirmation panel is displayed.

Step 4. Enter **CONFIRM** in the Response field, as shown in Figure 10-34.

Figure 10-34. Command Confirmation Panel

```
SOLVPROD-------- Automation Services : Command Confirmation -------------NET001


OpSys    OS390                                                  Userid USER01
                                                                LU     NMMAF022
                                                                FRI 20-JUN-1997
                                                                Time   17.17.00

WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING
WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING
***                                                                         ***
***     Command to Confirm .... GLOBAL                                      ***
***     SysName and Version ... FT1 0001                                    ***
***     User Supplied Parms ... MODE=AUTOMATED                              ***
***                                                                         ***
***     Enter CONFIRM to continue                                           ***
***     Enter CANCEL or press PF12 to terminate                             ***
***                                                                         ***
WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING
WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING

Response ... CONFIRM  ( CONFIRM / CANCEL )
 F1=Help      F2=Split
                          F9=Swap                              F12=Cancel
```

You are returned to the file transfer status monitor. Your NetMaster for File Transfer region is now in AUTOMATED mode and automatically controlling the resources defined in the loaded system image.

If you are satisfied that your resources are operating correctly in the AUTOMATED mode, you can update the $RM AUTOIDS parameter group and set the Automated Mode field to AUTOMATED. This sets the mode of the system image to AUTOMATED each time it is loaded at region startup and enables the resources defined to the system image to be controlled by the NetMaster for File Transfer region.

11

Monitoring and Managing Alerts

This chapter describes how to use the alert monitor to keep track of problems or impending problems in file transfer operations.

This chapter contains the following topics:

- What Is Displayed on the Alert Monitor?
- Accessing the Alert Monitor
- Working with Alerts
- Displaying Alert History

What Is Displayed on the Alert Monitor?

The alert monitor warns you of the following events:

- A file transfer rule being triggered
- State changes in defined resources

Accessing the Alert Monitor

The alert monitor provides an integrated, correlated event notification system that indicates to operators that a problem has been detected and that some action needs to be taken. Only alerts of the current date that are active for the current region startup are displayed. You can, however, access the other alerts in the history log (see the section, *Displaying Alert History*, on page 11-8).

In a multisystem environment, you can monitor active alerts from all linked regions in a focal point region. You can monitor only local active alerts in a subordinate region.

To access the alert monitor, enter the **/ALERTS** shortcut. The monitor displays all alerts that require operator attention.

Figure 11-1 shows an example of an alert monitor screen.

Figure 11-1. Alert Monitor Screens

```
SOLVPROD (11.33.01)-------- Alert Monitor : Alerts ------------Link: *MULTIPLE*
Command ===>                                                  Scroll ===> PAGE
AMDISP01 ACTIVITY HAS OCCURRED OFFSCREEN (ABOVE) FOR A SEVERITY 2 ALERT
           S/B=Browse T=Track N=Notes A=Analyze TT=TroubleTicket C=Close ?=More
    Time     Description                                Resource          Track
    22.38.44 XCMGR XC3000 on system FT1-0001 require XC300
    22.36.00 FTSCHD DBALLOK on system DECD1-0001 req DBALLOK
    21.39.51 CDMON NNDEA1.WAITQMON on system DECD1-0 NNDEA1.WAITQMON
    21.39.51 CDMON NNDEA1.TMRQUEUE on system DECD1-0 NNDEA1.TMRQUEUE
    21.39.49 CDMON NNDEA1.LISTENER on system DECD1-0 NNDEA1.LISTENER
    21.39.48 CDMON NNDEA1.CDTRMON on system DECD1-00 NNDEA1.CDTRMON
    21.39.48 CDMON NNDEA1.DECD1 on system DECD1-0001 NNDEA1.DECD1
    21.39.47 CDMON NNDEA1.EXECQ on system DECD1-0001 NNDEA1.EXECQ
    21.29.37 CMMGR CMSTC on system DECD1-0001 requir CMSTC
    21.29.36 FTPMGR TCPIP on system DECD1-0001 requi TCPIP
    21.29.32 FTPMGR FTPSRV3A on system DECD1-0001 re FTPSRV3A
    21.29.30 FTPMGR FTPD1 on system DECD1-0001 requi FTPD1
    21.28.58 FTSMGR STNMA on system DECD1-0001 requi STNMA
    21.28.50
    21.28.45
    21.28.36
 F1=Help      F2=Split     F3=Exit      F4=History   F5=Find      F6=Hold
 F7=Backward  F8=Forward   F9=Swap                   F11=Right
```

To display additional information, press F11.

```
SOLVPROD (11.55.49)-------- Alert Monitor : Alerts ------------Link: *MULTIPLE*
Command ===>                                                  Scroll ===> PAGE

           S/B=Browse T=Track N=Notes A=Analyze TT=TroubleTicket C=Close ?=More
    Time     Description                                     S Elapsed Occur
    22.38.44 XCMGR XC3000 on system FT1-0001 requires operator  3         1
    22.36.00 FTSCHD DBALLOK on system DECD1-0001 requires opera 3         1
    21.39.51 CDMON NNDEA1.WAITQMON on system DECD1-0001 require 3         1
    21.39.51 CDMON NNDEA1.TMRQUEUE on system DECD1-0001 require 3         1
    21.39.49 CDMON NNDEA1.LISTENER on system DECD1-0001 require 3         1
    21.39.48 CDMON NNDEA1.CDTRMON on system DECD1-0001 requires 3         1
    21.39.48 CDMON NNDEA1.DECD1 on system DECD1-0001 requires o 3         1
    21.39.47 CDMON NNDEA1.EXECQ on system DECD1-0001 requires o 3         1
    21.29.37 CMMGR CMSTC on system DECD1-0001 requires operator 3         1
    21.29.36 FTPMGR TCPIP on system DECD1-0001 requires operato 3         1
    21.29.32 FTPMGR FTPSRV3A on system DECD1-0001 requires oper 3         1
    21.29.30 FTPMGR FTPD1 on system DECD1-0001 requires operato 3         1
    21.28.58 FTSMGR STNMA on system DECD1-0001 requires operato 3         1
    21.28.50 FTSMGR QANM3 on system DECD1-0001 requires operato 3         1
    21.28.45 CDMGR VENUS on system DECD1-0001 requires operator 3         1
```

```
SOLVPROD (11.36.12)-------- Alert Monitor : Alerts ------------Link: *MULTIPLE*
Command ===>                                                  Scroll ===> PAGE

           S/B=Browse T=Track N=Notes A=Analyze TT=TroubleTicket C=Close ?=More
    Time     Description                                 1st Time System
    22.38.44 XCMGR XC3000 on system FT1-0001 requires ope 22.38.44 SOLVPROD
    22.36.00 FTSCHD DBALLOK on system DECD1-0001 requires 22.36.00 SOLVPROD
    21.39.51 CDMON NNDEA1.WAITQMON on system DECD1-0001 r 21.39.51 SOLVPROD
    21.39.51 CDMON NNDEA1.TMRQUEUE on system DECD1-0001 r 21.39.51 SOLVPROD
    21.39.49 CDMON NNDEA1.LISTENER on system DECD1-0001 r 21.39.49 SOLVPROD
    21.39.48 CDMON NNDEA1.CDTRMON on system DECD1-0001 re 21.39.48 SOLVPROD
    21.39.48 CDMON NNDEA1.DECD1 on system DECD1-0001 requ 21.39.48 SOLVPROD
    21.39.47 CDMON NNDEA1.EXECQ on system DECD1-0001 requ 21.39.47 SOLVPROD
    21.29.37 CMMGR CMSTC on system DECD1-0001 requires op 21.29.37 SOLVPROD
    21.29.36 FTPMGR TCPIP on system DECD1-0001 requires o 21.29.36 SOLVPROD
    21.29.32 FTPMGR FTPSRV3A on system DECD1-0001 require 21.29.32 SOLVPROD
    21.29.30 FTPMGR FTPD1 on system DECD1-0001 requires o 21.29.30 SOLVPROD
    21.28.58 FTSMGR STNMA on system DECD1-0001 requires o 21.28.58 SOLVPROD
    21.28.50 FTSMGR QANM3 on system DECD1-0001 requires o 21.28.50 SOLVPROD
    21.28.45 CDMGR VENUS on system DECD1-0001 requires op 21.28.45 SOLVPROD
    21.28.36 CDMGR TITAN on system DECD1-0001 requires op 21.28.36 SOLVPROD
```

Alerts are color coded by severity. They are sorted in order of severity, then time—the most severe alerts are listed first, then, in each category of severity, the most recent of the alerts are listed first.

You can change the information displayed on the alert monitor by using the following commands:

- SORT—to change the sort order
- LOCATE—to locate an alert by the sorted fields
- FILTER *filter-name*—to display alerts that match the criteria specified in the filter
- FORMAT *format-name*—to change the way the information is displayed

Note

You can display a selection list of filters and formats by entering the FILTER or FORMAT command.

The monitor refreshes your screen each time an alert arrives. If alert activities are causing interruptions to what you are doing, press F6 (Hold) to disable screen refresh. To resume display of new alerts, press F6 (Resume) again.

For an explanation of the information displayed by the alert monitor and available commands, see the online help.

Changing Your Alert Monitor Profile

You can use your monitor profile to customize the type of information displayed when you access the alert monitor. This profile specifies the following:

- Filter to use when you first enter the alert monitor
- The display format to use when you first enter the alert monitor

There are several ways to change your monitor profile:

- Use the FILTER *filter-name* SAVE command. The filter is saved to your user profile.
- Use the FORMAT *format-name* SAVE command. The format is saved to your user profile.
- Change your alert monitor profile by using the User Profile Menu.

To change your alert monitor profile by using the User Profile Menu, do this:

Step 1. Enter **=U.UP** from any panel. The Panel Display List is displayed.

Step 2. Enter **S** beside Alert Monitor Profile. The Alert Monitor Profile panel is displayed (see Figure 11-2).

Figure 11-2. Alert Monitor Profile Panel

```
SOLVPROD-------- Automation Services : Alert Monitor Profile ------------USER01
Command ===>                                                   Function=UPDATE

. Alert Monitor Display Control -------------------------------------------------.
|                                                                                |
| Monitor List Filter ............+ ____________                               |
|                                                                                |
| Monitor List Format ............+ ________                                   |
|                                                                                |
'--------------------------------------------------------------------------------'
```

Enter a question mark (?) to display lists of defined filters and formats.

Step 3. Enter an existing filter name in the Monitor List Filter field.

Step 4. Enter an existing format name in the Monitor List Format field.

Step 5. Press F3 (File) to save the changes to your user profile.

Working with Alerts

The alert monitor displays the alert when it arrives. Alerts may be closed automatically by the region or manually by the operator. When an alert is closed, it is removed from the alert monitor and is retained in the alert history log.

Typically, when an alert arrives, you would proceed as follows:

Step 1. Browse the alert to find out whether any suggested recommended actions are provided (see the next section, *Viewing the Details of an Alert*, on page 11-6).

If the alert is generated by the region on behalf of a defined resource, you can access the file transfer status monitor to work on that resource (see the section, *Accessing the Status Monitor from the Alert Monitor*, on page 11-6).

Step 2. To respond to an alert, you should indicate to other users that you will be working on it.

Enter **T** beside the alert. Your user ID is displayed in the Track column.

Step 3. Perform any necessary actions to remove the alert condition.

Step 4. Record notes that provide future reference information about this alert in the alert definition (see the section, *Adding Operator Notes to an Alert*, on page 11-7).

Step 5. After the alert condition is resolved, close the alert (if required) (see the section, *Closing an Alert*, on page 11-8).

Viewing the Details of an Alert

Enter **B** beside an alert to view its details. An alert comes with the following information:

- General information such as severity level, the source of the alert, and update history
- Possible causes of the alert and any recommended actions

To print the details, enter **PRINT** at the Command ===> prompt.

Accessing the Status Monitor from the Alert Monitor

If an alert is generated by the region on behalf of a defined resource, you can access the status monitor to work on that resource.

To access the status monitor, enter **A** beside the alert.

For information about how to use the status monitor, see Chapter 13, *Monitoring and Managing File Transfer Resources*.

Accessing the Transient Log from the Alert Monitor

If an alert is generated by the region on behalf of a defined resource, you can access the corresponding transient log.

To access the log, enter **TL** beside the alert.

For information about how to use the transient log, see the section, *Displaying the Transient Log*, on page 13-36.

Raising a Problem Ticket for an Alert

If your system administrator has implemented the interface for raising a problem ticket, you can apply the **TT** action at the Alert Monitor panel.

The TT action produces a request for a problem ticket as defined to your region.

For information about how to implement the problem ticket interface, see the section, *Task 11—Implementing the Alert Monitor Problem Ticket Interface*, on page 5-55.

Adding Operator Notes to an Alert

You can add notes to an alert for future reference. For example, you might want to leave the next operator some notes about an alert that has not yet been closed. Notes are also added automatically to provide a history of the actions performed on the alerts.

To add notes to an alert, proceed as follows:

Step 1. Enter **N** beside the alert to display the Alert Notes panel.

Step 2. Press F4 (Add) to enable you to add notes.

Step 3. Enter your notes about the alert. Refer to the online help about how to use the editor.

Step 4. When you finish entering your notes, press F3 (File) to save the notes with the alert.

Closing an Alert

Alerts may be closed automatically by the region, or manually.

For example, an alert might be generated because a resource entered a degraded state. When the degraded condition is corrected, the alert is closed automatically. Another alert might be a reminder alert and needs to be closed manually.

To close an alert, enter **C** beside the alert to close it.

Displaying Alert History

The alert history lists all alerts, both active and closed, that occurred during a predefined period.

To view the alert history, press F4 (History). The alerts for the current date are displayed. If you want to display the alerts for the other dates, use the DATE command. For more information about the command, refer to the online help.

To view the history of actions performed on an alert, enter **N** beside it.

Note

To customize how long an alert is retained in the alert history log, enter the **/ALADMIN.H** path to display the History Logging Parameters Definition panel.

12

Monitoring Active File Transfers

This chapter describes how to monitor active file transfers.

This chapter contains the following topics:

- Monitoring Active File Transfers
- Displaying the Estimated Completion Time
- Filtering File Transfers
- Sorting a List of Active File Transfers
- Changing the List Format
- Setting Up the File Transfer Monitor in Your User Profile

Monitoring Active File Transfers

The active file transfer monitor enables you to view all of the active file transfers in your environment. The file transfers are displayed as a list. From this list you can:

- Select a specific file transfer and:
  - Display the details of the transfer
  - Exclude the file transfer from the list
  - Display the estimated completion time with ETA monitoring
  - Terminate the transfer (CA-XCOM, CONNECT:Direct, or TCPaccess FTP server transfers only)

    Note

    Users belonging to the following user groups cannot terminate a transfer: $RMBUSER and $RMMON.

  Note

  Transfer termination and ETA monitoring require the definition of the manager for the region that provides the file transfer events.

- Filter transfers so that only those that meet specific criteria are listed
- Sort the listed transfers
- Change the list format to suit your specific needs
- Define a monitoring profile to suit your specific needs

Note

Active file transfer monitoring is not available for host-initiated CONNECT:Mailbox Auto Connect transfers or FTP transfers (except those using the TCPaccess FTP server) because there is no information available for start events.

To monitor active file transfers, enter the **/AFTMON** shortcut.

The File Transfer Monitor panel is displayed (see Figure 12-1).

Figure 12-1. File Transfer Monitor Panel

```
            M=ETA Monitor MO=ETA Monitor Off S=Show Event X=Exclude T=Terminate
    Transfer ID       Started  Source Node     Source Data
    F41982SL01(1520)  08:39:48 XC3000          DS001.RFNMFT.LARGE.FILE
    QXLT0001(106)     08:40:29 CD400           CDLIB/CDBIGFILE(TEST02)
    QXLT0001(107)     08:41:15 CD400           CDLIB/CDBIGFILE(TEST02)
```

Displaying the Estimated Completion Time

The ETA monitor displays the progress of a selected file transfer. To display the estimated completion time for a file transfer, do this:

Step 1. On the File Transfer Monitor panel, enter **M** in front of the active file transfer.

The display is updated to acknowledge that ETA monitoring has been requested. This is followed by confirmation that it has started.

Step 2. If the monitor does not know the size of the file being transferred, you will be prompted for the size. Enter the estimated size of the file in the units of measurement used by the file transfer.

Caution

If you are monitoring a compressed file, specify its estimated compressed size.

If the estimated size is exceeded, the monitor will display 99% until the transfer is completed. If this occurs, turn the monitor off, re-enter the file size, and start monitoring again.

Figure 12-2 shows that ETA monitoring is in progress for F42322SL01(1525) and QXLT0004(113).

Figure 12-2. ETA Monitoring in Progress

```
            M=ETA Monitor MO=ETA Monitor Off S=Show Event X=Exclude T=Terminate
    Transfer ID       Started  Source Node     Source Data
    F42322SL01(1525)  10:43:28 139.00K Bytes in 00h 00m 12s 01% ETA 00h 19m 48s
    QXLT0002(111)     10:43:31 CD400           CDLIB/CDBIGFILE(TEST02)
    QXLT0004(113)     11:06:51 CD400           CDLIB/CDBIGFILE(TEST02)
    QXLT0005(114)     11:06:51 CD400           CDLIB/CDBIGFILE(TEST02)
    QXLT0004(113)     11:06:54   14.6K Blks in 00h 03m 30s 15% ETA 00h 19m 50s
```

The ETA displays:

- The number of bytes, blocks, or records transferred
- The time taken on the transfer so far
- The percentage completed
- The estimated time for the transfer to complete
- An optional graphic fuel gauge of the transfer's progress (set by the $RF FTMONITOR parameter group)

Filtering File Transfers

You can filter the file transfers so that only those that meet the criteria you set will be listed. You can apply an existing filter or create a new one.

Applying a Filter to the File Transfer Monitor

To apply a file transfer monitor filter, use the FILTER command. The format of the FILTER command is FILTER *filtername*.

For example, to apply a filter called PRODSOURCE, use the command FILTER PRODSOURCE.

Applying a File Transfer Monitor Filter from a List

To select and apply a filter from a list of file transfer monitor filters, do this:

Step 1. Enter **FILTER** at the File Transfer Monitor panel command prompt.

The File Transfer Monitor Filter List panel is displayed (see Figure 12-3).

Figure 12-3. File Transfer Monitor Filter List

```
SOLVPROD-------- File Transfer : File Transfer Monitor Filter List ------------
Command ===>                                                   Scroll ===> HALF

                                            S/B=Browse U=Update C=Copy D=Delete
    Filter Name   Description
    MORNING       Started before 09:00.
    NONE          All File Transfers
    PRODSOURCE    Source node is production.
    SALES         User has sales ID.
    **END**
```

Step 2. Select the required filter, and press ENTER.

The File Transfer Monitor panel is displayed showing the name of the applied filter (see Figure 12-4).

Figure 12-4. File Transfer Monitor with Filter Applied

```
SOLVPROD------ File Transfer : File Transfer Monitor ------Filter(PRODSOURCE)
Command ===>                                                Scroll ===> HALF
RFFT0004 Monitor Filter SET TO (PRODSOURCE)
          M=ETA Monitor MO=ETA Monitor Off S=Show Event X=Exclude T=Terminate
    Transfer Id       Started  Source Node     Source Data
    COMPNT(14)        12:36:22 PRODUCTION      PROD.USER01.PROCESS
    **END**
```

Creating a New File Transfer Monitor Filter

To create a new file transfer monitor filter, do this:

Step 1. From the primary menu, enter **/FTADMIN.F**.

The File Transfer Monitor Filter List panel is displayed.

Step 2. Press F4 (Add).

The File Transfer Monitor Filter panel is displayed.

Step 3. Enter the name and description of the filter in the Filter Definition section of the panel (see Figure 12-5).

Step 4. Create the filter in the Filter Expression section of the panel (see Figure 12-5).

To determine the valid values for a field, type **?** in the field and press ENTER. For more information on creating a filter expression, press F1 (Help).

Step 5. Press F3 (File) to save the filter.

Figure 12-5. Example File Transfer Monitor Filter

```
SOLVPROD-------- File Transfer : File Transfer Monitor Filter --------Func=ADD
Command ===>                                                  Scroll ===> HALF

| Filter Definition -------------------------------------------------------|
| Name ......... PRODSOURCE                                                |
| Description .. Source node is production and user is not USER02          |
| Last Updated at          on WED 08-DEC-1999 by USER01                    |
-----------------------------------------------------------------------------|
| Filter Expression -------------------------------------------------------|
|                                                                          |
|                                                D=Delete I=Insert R=Repeat|
|      "(" Field   Opr Value                                Gen ")" Bool |
|      ___ SRCADDR EQ  "PRODUCTION"_____________________  ______ _ AND  |
|      ___ USER    NE  "USER02"_________________________  ______ _ ____ |
|      ___ ______  __  ________________________________  ______ _ ____ |
|                                                                          |
|                                                                          |
|                                                                          |
|                                                                          |
|                                                                          |
|                                                                          |
|  F1=Help     F2=Split    F3=File     F4=Save                             |
|  F7=Backward F8=Forward  F9=Swap                            F12=Cancel   |
|---------------------------------------------------------------------------|
```

Sorting a List of Active File Transfers

You can sort the list of file transfers to three levels. The fields you can sort on are:

- JOBNAME—the file transfer product job name
- PRODUCT—the file transfer product
- SRCADDR—the source address or node
- SRCFNAME—the source data name
- STARTTIME—the start time
- SYSTEM—the NetMaster region which originated the event
- TGTADDR—the target address or node
- TGTFNAME—the target data name
- USER—the initiating user ID
- XFRID—the file transfer ID

To sort the contents of the list, use the SORT command. The format of the SORT command is SORT *field*, *field*, *field*.

For example, to do a primary sort on the source address, with a secondary sort on the time that the transfer started, use the command:
SORT SRCADDR, STARTTIME

The default sort order is by STARTTIME.

Changing the List Format

The list format specifies the appearance of the active file transfer monitor. You can use the default list format, apply an existing list format, or create a new one. The default list format is:

- Active file transfers are displayed in green.
- File transfers that fail are displayed in red and remain visible for 30 minutes.
- Completed file transfers are displayed in blue and remain visible for 2 minutes.

Note

To change the amount of time file transfers remain visible, you need to customize the FTMONITOR parameter group.

Applying a List Format to the File Transfer Monitor

To apply a list format, use the FORMAT command. The syntax of the FORMAT command is FORMAT *formatname*

For example, to apply a list format called OPER01, use the command FORMAT OPER01.

Applying a List Format from a Selection List

To select and apply a list format from a list, do this:

Step 1. Enter **FORMAT** at the File Transfer Monitor panel command prompt.

The Lists panel is displayed.

Step 2. Select the required format from the list of formats.

The File Transfer Monitor panel is displayed in the new list format.

Creating a New List Format

To create a new list format, do this:

Step 1. From the primary menu enter **/FTADMIN.L**.

The List Definition List panel is displayed.

Step 2. Press F4 (Add).

The List Description panel is displayed.

Step 3. Enter your values into the List Name, Description, and Service Procedure fields.

Figure 12-6 shows an example of a completed panel.

Figure 12-6. List Format Panel

```
SOLVPROD-------------------- CAS : List Description ---------------Page 1 of 4
Command ===>                                                       Function=Add

Appl ID .............+ $RF
List Type ............ PRIVATE   (PUBLIC or PRIVATE)
Userid ............... FTMON     (Userid if PRIVATE)
List Name ............ OPERLIST01
Description ........... Used by operations.
Title ................
Status ................ ACTIVE          Group .............+
Service Procedure ..... OPS             Data Source .........
Get All Entries? ...... YES             Exit Name ...........
Add Allowed? .......... YES             Help Name ...........
Default Mnemonic ...... B               Select Mnemonic ..... S
Entry Msg Position .... 2               Entry Msg Length ....
Present Empty List? ... YES             Auto Refresh Rate ...
                                        Heading Sub Char ....
Comments .............




 F1=Help      F2=Split     F3=File      F4=Save
              F8=Forward   F9=Swap                                F12=Cancel
```

Step 4. Press F8 (Forward) three times.

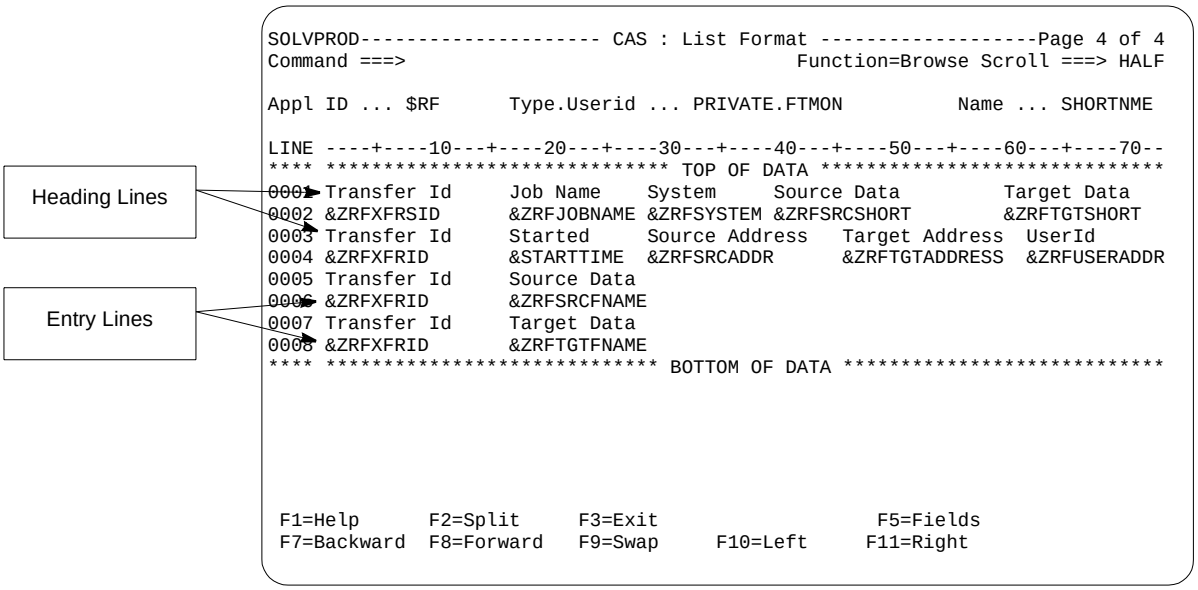
The List Format panel is displayed.

Step 5. Specify the headings as you would like them to appear on the monitor. These lines are the heading lines (see Figure 12-7).

Step 6. Specify the corresponding variables beneath the headings. Specify the variables in a single line. These lines are the entry lines. See the online help for a list of valid variables.

A completed List Format panel is shown in Figure 12-7.

Figure 12-7. Completed List Format Panel



Step 7. Press F3 (Exit) to save the list format.

Setting Up the File Transfer Monitor in Your User Profile

You can specify your default monitor filter, the list format, and the sort criteria for the active file transfers in your user profile.

To update your profile for the active file transfer monitor, do this:

Step 1. Enter **PROFILE** at the File Transfer Monitor panel command prompt.

The File Transfer Monitor Profile panel is displayed (see Figure 12-8).

Figure 12-8. File Transfer Monitor Profile Panel

```
SOLVPROD---- Automation Services : File Transfer Monitor Profile -------USER01
Command ===>                                                     Function=UPDATE


- File Transfer Monitor Display Control -------------------------------------
|                                                                            |
| File Transfer Monitor Filter ...+                                          |
|                                                                            |
| Monitor List Format ............+                                          |
|                                                                            |
| Transfer Sort Criteria .........+                                          |
|                                 +                                          |
|                                 +                                          |
|                                                                            |
-----------------------------------------------------------------------------





 F1=Help      F2=Split     F3=File      F4=Save
                           F9=Swap                                F12=Cancel
```

Step 2. Enter the name of the filter in the File Transfer Monitor Filter field. To select from a list of filters, enter **?**.

Step 3. Enter the name of the format in the Monitor List Format field. To select from a list of formats, enter **?**.

Step 4. Enter the fields on which the list is to be sorted in the Transfer Sort Criteria fields. The fields are listed in sort order. To select from a list of fields, enter **?**.

Step 5. Press F3 (File) to apply the profile.

The File Transfer Monitor panel is displayed with the monitor filter, the list format, and the sort criteria applied. The monitor defaults to these values each time it is started.

13

Monitoring and Managing File Transfer Resources

This chapter describes how to use the file transfer status monitor to view the status of the file transfer schedules and resources.

This chapter contains the following topics:

- Monitoring File Transfer Resources
- Monitoring File Transfer Schedules
- Interpreting the Status of File Transfer Schedules
- Interpreting the Status of Supporting File Transfer Resources
- Displaying Information About a CA-XCOM Region
- Listing and Managing CA-XCOM Transfer Requests
- Displaying Information About a CONNECT:Direct Region
- Listing and Managing CONNECT:Direct Processes
- Listing and Managing TCP/IP Connections
- Listing and Managing CONNECT:Mailbox Batches
- Monitoring CONNECT:Mailbox Resources
- Listing and Managing CONNECT:Mailbox VSAM Batch Files
- Displaying Logs
- Activating and Inactivating a File Transfer Resource
- Issuing Commands to a File Transfer Resource
- Issuing UNIX Shell Commands to a Remote UNIX Host
- Monitoring Your File Transfer Environment by Using the Graphical Monitor

Monitoring File Transfer Resources

This section describes how you monitor the file transfer resources defined to your system image on the file transfer status monitor. The following sections explain how to perform the following:

- Access the file transfer status monitor
- Display resources
- Change your file transfer status monitor profile

Accessing the File Transfer Status Monitor

The file transfer status monitor displays the status of the resources defined in the loaded system image. After initial logon to the NetMaster for File Transfer region, the Primary Menu panel is displayed.

To access the file transfer status monitor, enter **/FTMON** at the Select Option ===> prompt.

The file transfer status monitor, as shown in Figure 13-1, displays the status of the resources.

Key Concept

The resources displayed on the panel are dependent on the filter selected for the file transfer status monitor. The default filter (FILETRANSFER), displays all the file transfer resources defined in your region, as shown in Figure 13-1.

Figure 13-1. Status Monitor : File Transfer Resources

```
SOLVPROD----------- Status Monitor : File Transfer Resources ----------FT1-0001
Command ===>                                                   Scroll ===> PAGE

                  S=Status L=Log D=Display A=Act T=Term DB=Database ?=List Cmds
    System   Class    Resource     Desired  Actual     Mode       Logical   Ovr
    FT1      CDMGR    ALCDUNX1     ACTIVE   ACTIVE     MANUAL     OK
    FT1      CDMGR    DECD1        ACTIVE   ACTIVE     MANUAL     OK
    FTI      CDMON    DECD1.ALCDUN ALCDUNX1 AVAILABLE AT 09.33
    FT1      CDMON    DECD1.HOLDQ  QUEUE(HOLD) STATUS(ANY) CNT(10) AT 14.20
    FT1      CDMON    DECD1.LISTEN LISTENER TASK FOUND AT 14.34
    FT1      CDMON    DECD1.RETRYQ QUEUE(TIMER) STATUS(RETRY) CNT(1) AT 14.34
    FT1      CDMON    DECD1.TCPCON 0 CONNECTIONS CHECKED. ALL OK AT 14.39
    FT1      CDMON    DECD1.TIMERQ QUEUE(TIMER) STATUS(ANY) CNT(0) AT 14.04
    FTI      CDMON    DECD1.TRANSF NO TRANSFERS FOUND AT 14.36
    FT1      FTPMGR   FTPSVR       ACTIVE   ACTIVE     MANUAL     OK
    FT1      FTPMON   FTPSVR.LISTE LISTENER TASK FOUND AT 14.53
    FT1      FTPMON   FTPSVR.TCPCO 0 CONNECTIONS CHECKED. ALL OK AT 15.53
    FT1      FTSCHD   ALCARDSCHEDL PROC 14.30 REQ:0069 COMP:0001 FAIL:0000
    FT1      FTSMGR   CAFTS1       UNABLE TO COMMUNICATE WITH CAFTS1 14.50
    FT1      FTSMON   CAFTS1.CAAR  UNABLE TO COMMUNICATE WITH CAFTS1 14.50
    FT1      XCMGR    XC3000       ACTIVE   ACTIVE     MANUAL     OK
    FT1      XCMON    XC3000.STALL NO TRANSFERS FOUND AT 14.05
 F1=Help      F2=Split     F3=Exit      F4=Add       F5=Find
 F7=Backward  F8=Forward   F9=Swap                   F11=Right
```

Displaying Resources

This section describes how to:

- List the monitors associated with a specific manager
- Change your view of the displayed resources
- Change the type of displayed information
- Display information about the resources

Listing Monitors Associated With a Specific Manager

NetMaster for File Transfer allows you to view those resources associated with a resource manager (owner resource).

For example, to list resources associated with a CA-XCOM Manager resource (XCMGR), enter **Z** beside a listed XCMGR resource.

All resources associated with the XCMGR resource are listed, as shown in Figure 13-2.

Figure 13-2. Listing Resources

```
SOLVPROD----------- Status Monitor : File Transfer Resources ----------FT1-0001
Command ===>                                                   Scroll ===> PAGE

                 S=Status L=Log D=Display A=Act T=Term DB=Database ?=List Cmds
    System   Class    Resource     Desired  Actual     Mode       Logical   Ovr
    FT1      CDMGR    ALCDUNX1     ACTIVE   ACTIVE     MANUAL     OK
Z   FT1      XCMGR    XC3000       ACTIVE   ACTIVE     MANUAL     OK
    **END**
```

Enter the Zoom Command.

```
SOLVPROD---------------- Status Monitor : Owner(XC3000) ---------------FT1-0001
Command ===>                                                   Scroll ===> PAGE

                 S=Status L=Log D=Display A=Act T=Term DB=Database ?=List Cmds
    System   Class    Resource     Desired  Actual     Mode       Logical   Ovr
    FT1      XCMGR    XC3000       ACTIVE   ACTIVE     MANUAL     OK
    FT1      XCMON    XC3000.CONNECT  2 CONNECTIONS CHECKED. ALL OK AT 11.55
    FT1      XCMON    XC3000.HELD  STATUS(HELD) CNT(1) AT 11.52
    FT1      XCMON    XC3000.LISTE LISTENER TASK FOUND AT 11.53
    FT1      XCMON    XC3000.INACT STATUS(INACTIVE) CNT(0) AT 11.52
    FT1      XCMON    XC3000.STALL NO TRANSFERS FOUND AT 11.53
    FT1      XCMON    XC3000.SUSPE STATUS(SUSPENDED) CNT(0) AT 11.52
    **END**

 F1=Help      F2=Split     F3=Exit      F4=Add       F5=Find
 F7=Backward  F8=Forward   F9=Swap                   F11=Right
```

Key Concept

You can change your view of displayed resources by using a temporary file transfer status monitor filter. The file transfer status monitor filter determines which resources are displayed on the monitor. The filter that you select remains valid for the current monitor session only. When you next return to the file transfer status monitor, the default FILETRANSFER filter is used.

To select a file transfer status monitor filter and change the view of displayed resources, proceed as follows:

Step 1. At the file transfer status monitor Command ===> prompt, enter **FILTER**.

A list of filters is displayed, as shown in Figure 13-3.

Note

You can also enter FILTER *name* to select a filter (for example, FILTER CD).

Figure 13-3. Changing a Filter

```
SOLVPROD----------- Status Monitor : File Transfer Resources ----------FT1-0001
Command ===> FILTER                                            Scroll ===> CSR

                 S=Status                    =Act T=Term DB=Database ?=List Cmds
SOLVPROD------ Automation                    Monitor Filter List ---------------
Command ===>                                                   Scroll ===> CSR

                                          Use 'S' to select the required Filter
    Filter Name   Description
    XC            XCOM Managers and Monitors
    XCMGR         XCOM Managers
S   XCMON         XCOM Monitors

  F1=Help      F2=Split     F3=Exit      F4=Return    F5=Find      F6=Refresh
  F7=Backward  F8=Forward   F9=Swap
```

Enter the FILTER Command.

Selecting a filter

Step 2. Move the cursor to the desired filter, and enter **S**.

The resources, as specified in the filter, are displayed.

Changing the Type of Displayed Information

The file transfer status monitor displays fields or extended messages. The fields display resource state and mode of operation information. Whereas, extended messages display information *about* the state of a resource—extended display messages are specified in the definition of a resource.

To remove the display of all extended display messages from your file transfer status monitor, enter **EXTDISP OFF** at the Command ===> prompt.

To redisplay extended display messages, enter **EXTDISP ON** at the Command ===> prompt.

Displaying Information About File Transfer Resources

NetMaster for File Transfer allows you to display information about a selected resource. The information that is displayed depends on the type of the selected resource.

To display information about a resource, enter **D** beside the resource. If a Signon Details panel is displayed, see the section, *CONNECT:Direct Security Considerations*, on page 13-14.

The following table lists the information displayed for a particular resource type.

Resource Type	Information Displayed
CA-XCOM manager (XCMGR class)	The Command Entry panel is displayed. It displays the version of the selected CA-XCOM region.
CA-XCOM transfer request monitor (XCMON class)	A panel is displayed that lists the requests with the monitored status, and which allows you to issue commands against those requests. See the section, *Listing and Managing CA-XCOM Transfer Requests*, on page 13-12.
CA-XCOM stalled transfer monitor (XCMON class)	A panel is displayed that lists the active transfer requests, and which allows you to issue commands against those requests. See the section, *Listing and Managing CA-XCOM Transfer Requests*, on page 13-12.
CA-XCOM TCP/IP connections monitor (XCMON class)	An action list is displayed for the monitored TCP/IP connections. See the section, *Listing and Managing TCP/IP Connections*, on page 13-23.
CA-XCOM TCP/IP listener task monitor (XCMON class)	Status details are displayed for the monitored TCP/IP listener task.

Resource Type	Information Displayed
CA-XCOM remote node monitor (XCMON class)	Status information is displayed for the monitored remote nodes.
CONNECT:Direct manager (CDMGR class)	The Command Entry panel is displayed. This panel displays information about a managed local CONNECT:Direct for MVS or CONNECT:Direct for OS/390 region, or about the link to a managed remote CONNECT:Direct application. The display action that is executed when you enter the D command is defined in your resource definition.
CONNECT:Direct queue and status monitor (CDMON class)	A panel is displayed that lists the processes associated with the selected queue, and which allows you to issue commands against those processes. See the section, *Listing and Managing CONNECT:Direct Processes*, on page 13-19.
CONNECT:Direct transfer monitor (CDMON class)	A panel is displayed that lists the processes associated with the Exec queue, and which allows you to issue commands against those processes. See the section, *Listing and Managing CONNECT:Direct Processes*, on page 13-19.
CONNECT:Direct TCP/IP connections monitor (CDMON class)	An action list is displayed for the monitored TCP/IP connections. See the section, *Listing and Managing TCP/IP Connections*, on page 13-23.
CONNECT:Direct TCP/IP listener task monitor (CDMON class)	Status details are displayed for the monitored TCP/IP listener task.
CONNECT:Direct remote node monitor (CDMON class)	The log of the process that checks the availability of the node is displayed.
CONNECT:Mailbox VSAM file server (STC class)	The Command Entry panel is displayed. This panel displays information about a managed local CONNECT:Mailbox VSAM file server application. The display action that is executed when you enter the D command is defined in your resource definition.
CONNECT:Mailbox (CMMGR)	The Command Entry panel is displayed. This panel displays information about a managed local CONNECT:Mailbox application. The display action that is executed when you enter the D command is defined in your resource definition.

Resource Type	Information Displayed
CONNECT:Mailbox Auto Connect Queue monitor (CMMON)	A panel is displayed listing any queued Auto Connects.
CONNECT:Mailbox BSC Line monitor (CMMON)	A panel is displayed listing BSC lines used by CONNECT:Mailbox file transfer sessions.
CONNECT:Mailbox SNA Sessions monitor (CMMON)	A panel is displayed listing the batches in CONNECT:Mailbox SNA file transfer sessions with the monitored remote sites.
DASD (DASD class)	The Command Entry panel is displayed. This panel displays information about the DASD. The display command that is executed when you enter the D command is defined in your resource definition.
FTP manager (FTPMGR class)	The Command Entry panel is displayed. This panel displays information about a managed FTP server region. The display action that is executed when you enter the D command is defined in your resource definition.
FTP connections monitor (FTPMON class)	An action list is displayed for the monitored TCP/IP connections. See the section, *Listing and Managing TCP/IP Connections*, on page 13-23.
FTP listener monitor (FTPMON class)	Status details are displayed for the monitored TCP/IP listener port.
FTP remote node monitor (FTPMON class)	The results of the check on the availability of the node is displayed.
File transfer schedule (FTSCHD class)	A list of monitored files that have completed or failed transfer is displayed.
FTS manager (FTSMGR class)	The Command Entry panel is displayed. This panel displays information about a managed local FTS region or about the link to a managed remote FTS region. The display action that is executed when you enter the D command is defined in your resource definition.
FTS link monitor (FTSMON class)	The Command Entry panel is displayed. This panel displays information about the link.
Started task (STC class)	The Command Entry panel is displayed. This panel displays information about the started task. The display command that is executed when you enter the D command is defined in your resource definition.

Resource Type	Information Displayed
Tape (TAPE class)	The Command Entry panel is displayed. This panel displays information about the tape unit. The display command that is executed when you enter the D command is defined in your resource definition.

Monitoring File Transfer Schedules

File transfer schedules are FTSCHD class resources. For information about how a schedule changes its status, see Figure 10-6 on page 10-21.

The display of these resources on the status monitor is color coded. Typically, green indicates that files are arriving according to the schedule, while yellow or red suggests problems that require your attention.

If the status of a schedule indicates a problem, enter **L** beside the schedule to display its transient log for more information. From the transient log, you can also enter S beside a message to display the NetMaster for File Transfer activity log, which can provide you with extra information about the problem. For more information about logs, see the section, *Displaying Logs*, on page 13-32.

Acknowledging a Failure Status

If the status of a schedule is displayed in red and you know that it is no longer a problem, enter **OK** beside it to set its status color to green.

Displaying the Next Time a Schedule Starts Monitoring

Enter **NXT** beside a schedule to find out when it will next start monitoring.

Display Selective Schedules on the File Transfer Status Monitor

You can display only those schedules you want to monitor as follows:

If you want to display …	Enter …
All file transfer schedules only	**FILTER FTSCHD** at the Command ===> prompt.
Active schedules only	**FILTER ACTSCHEDS** at the Command ===> prompt.
All active and failed schedules	**FILTER SCHEDULEMON** at the Command ===> prompt.

If you want to remove a particular schedule from your monitor, enter **OFF** beside it. The schedule is removed from the monitor but will reappear at its next start time.

Interpreting the Status of File Transfer Schedules

NetMaster for File Transfer uses extended display messages to indicate the status of file transfer schedules. The format of the message is as follows:

```
xxxx hh.mm REQ:nnnn COMP:nnnn FAIL:nnnn
```

xxxx	displays the following stages of file transfer monitoring: PREP—pre-processing PROC—processing POST—post-processing END—end of monitoring For information about these stages, see the section, *Specifying a Schedule*, on page 10-20.
hh.mm	displays the time of the last status update.
REQ:*nnnn*	displays the required number of files to be transferred for the schedule.
COMP:*nnnn*	displays the number of completed transfers.
FAIL:*nnnn*	displays the number of failed transfers.

Interpreting the Status of Supporting File Transfer Resources

Supporting file transfer resources include the following classes of resources:

- CDMGR and CDMON (CONNECT:Direct manager and monitor)
- CMMGR and CMMON (CONNECT:Mailbox manager and monitor)
- DASD (DASD)
- FTPMGR FTPMON (FTP manager and monitor)
- FTSMGR and FTSMON (FTS manager and monitor)
- STC (Communications Server tasks, TCPaccess tasks, and CONNECT:Mailbox VSAM file server)
- TAPE (tape units)
- XCMGR and XCMON (CA-XCOM manager and monitor)

The status of resources is displayed in the following ways:

- File transfer status monitor fields
- Extended display messages
- Colored resources and messages

Interpreting File Transfer Status Monitor Fields

The status of a resource can be determined by observing the displayed status fields. To display the status fields, at the file transfer status monitor Command ===> prompt, enter **EXTDISP OFF**. The default status fields for NetMaster for File Transfer are as follows:

Desired

This field displays the desired state of the file transfer resource. The desired states can be ACTIVE or INACTIVE.

Actual

This field displays the actual state of the file transfer resource. The actual state of the resource can be ACTIVE, STARTING, STOPPING, INACTIVE, DEGRADED, FAILED, or UNKNOWN.

Mode

This field displays the mode in which the resource is operating. The modes can be AUTOMATED, MANUAL, or IGNORED. When in AUTOMATED mode, the resource is controlled by the NetMaster for File Transfer region. When in MANUAL or IGNORED mode, the resource is controlled by you.

Logical

This field specifies the logical state of the region. The displayed logical state is determined by the state of the Desired, Actual, and Mode fields for the file transfer resource. The logical state can be UNKNOWN, INERROR, FAILED, ATTENTION, DEGRADED, PENDING, STARTING, STOPPING, or OK.

Note

The determination of a logical state can be customized by your system administrator. To view the method used in determining the logical state of the resources in your NetMaster for File Transfer region, enter **/ASADMIN.A** at the Command ===> prompt and view the mode attributes tables.

Interpreting Extended Display Messages

When the state of a resource changes, an extended display message may be displayed. The message that is displayed, when a resource changes state, is stored in the resource definition. You can view the extended display messages by accessing the status monitor message details panel of the resource definition and entering **ED** beside a listed status monitor message. See the sections, *Customizing the Manager Resource Definition*, on page 15-44, and *Customizing Monitor Resource Definitions*, on page 15-46, for information about how to access and customize manager and monitor resource definitions.

Interpreting Colored Resources and Messages

Each file transfer resource is displayed in a color which reflects its logical state. Resources that are displayed in the color of green are in a logical state of OK. The color in which extended messages are displayed is specified in the resource definition. Extended messages overwrite the status monitor fields. If resources are displayed in a color other than green, they may require your attention. To view the colors assigned to particular states, enter **/ASADMIN.A** at the Command ===> prompt and view the logical state attributes table.

Displaying Information About a CA-XCOM Region

NetMaster for File Transfer allows you to display information about a CA-XCOM region, such as:

- Control library member
- MAXLOC, MAXREM, and MAXTASK

For more information about commands for CA-XCOM resources, see help.

Displaying a CA-XCOM Control Library Member

To display the control library member of a CA-XCOM region, enter **LST** beside the XCMGR resource.

Also, you can use the DIS and ENA commands to disable and enable control library members.

Displaying the MAXLOC, MAXREM, and MAXTASK Parameters

To display the parameters, enter **INQ** beside the XCMGR resource.

If you want to change these parameters, enter **DFT** beside the resource.

Listing and Managing CA-XCOM Transfer Requests

You can display the transfer requests in a CA-XCOM region on the file transfer status monitor. The requests displayed are those associated with the monitored request status.

The following sections describe how to list and manage these requests.

Listing Transfer Requests

You can list the CA-XCOM transfer requests that are monitored by the NetMaster for File Transfer product.

To list the requests, enter **D** beside an XCMON transfer request monitor.

To refresh the list, press F6 (Refresh).

You can also enter any of the following commands beside an XCMGR resource to list its transfer requests:

Command	Transfer Requests Displayed
VA	All requests
VAC	Requests that are active
VH	Requests that are held
VI	Requests that are inactive
VS	Requests that are suspended

Managing Transfer Requests

You can manage the listed CA-XCOM requests by using the actions described in Table 13-1.

Table 13-1. Actions for CA-XCOM Transfer Requests

Action	Description
A (Alter)	Use this action to modify the details of a request.
D (Delete)	Use this action to delete a request.
H (Hold)	Use this action to hold a pending transfer.
R (Release)	Use this action to release a held transfer.
R (Resume)	Use this action to resume a suspended transfer.
SP (Suspend)	Use this action to suspend an active transfer.
T (Terminate)	Use this action to stop and purge an active transfer immediately.
V (View) or S	Use this action to display a panel which provides details of a request.

Displaying Information About a CONNECT:Direct Region

NetMaster for File Transfer allows you to display information about a CONNECT:Direct region, such as:

- Network maps
- Initialization parameters (INITPARMS)

CONNECT:Direct Security Considerations

When you use any function in NetMaster for File Transfer that requires authorized access to CONNECT:Direct, you need to confirm your CONNECT:Direct signon details.

Note

This is necessary only once during each session for each CDMGR defined.

However, if you use the CLR command to clear your security access, you will need to reconfirm your signon details the next time you want to use one of these functions.

See the section, *Clearing Your CONNECT:Direct Signon Details*, on page 13-16 for information about using the CLR command.

Confirming Your CONNECT:Direct Signon Details

The first time (within a session) you enter a command needing security confirmation, a Signon Details panel is displayed, as shown in Figure 13-4.

Figure 13-4. Confirming Signon Details for a CONNECT:Direct Command

```
.- CONNECT:Direct Signon Details ---------------------------------------------.
|                                                                              |
|  User ID ................. USER1                                            |
|                                                                              |
|  Password ................                                                   |
|                                                                              |
|  Case Sensitive ........... NO        (Yes/No)                               |
|                                                                              |
|  Press F6 to Confirm or F12 to Cancel                                        |
|                                                                              |
'------------------------------------------------------------------------------'
```

To confirm your signon details, proceed as follows:

Step 1. Complete the fields on this panel.

Note

If your details are defined to CONNECT:Direct as case sensitive, ensure that you do both of the following:

- Enter your user ID and password in the correct case.
- Check that the value in the Case Sensitive field is YES.

For further information about this panel, press F1 (Help).

Step 2. Press F6 (Confirm) to confirm your CONNECT:Direct signon details.

You can then continue your processing.

Clearing Your CONNECT:Direct Signon Details

Once you have confirmed your CONNECT:Direct signon details for a particular CDMGR resource during a session, you retain your security access to that CDMGR for the whole of the session. However, if you do not want to leave your CONNECT:Direct security access available, you can clear it.

To clear your CONNECT:Direct security access, enter **CLR** (Clear) next to the CDMGR for which you have confirmed your signon details. A message is displayed, confirming that your signon details have been cleared.

Note

If you clear your security access, you will be prompted to confirm your signon details again the next time you want to use a function requiring authorized access to CONNECT:Direct.

Displaying a CONNECT:Direct Network Map

To display the network map of a CONNECT:Direct region, proceed as follows:

Step 1. At the file transfer status monitor, enter **NM** beside a CDMGR resource. The Specify A NETMAP Node Name panel is displayed, as shown in Figure 13-5.

Figure 13-5. Specify A NETMAP Node Name Panel

```
SOLVPROD--------- File Transfer : Specify A NETMAP Node Name ------------------
Command ===>                                                   Function=UPDATE

.- Specify Node Name -------------------------------------------------------.
|                                                                            |
|  Node Name ............. *______________                                  |
```

Step 2. You can display the network map entries for all nodes, a range of nodes, or a specific node, as follows:

If you want to …	**Then enter …**
Display all nodes in the network map for this manager resource	***** in the Node Name field and press F6 (Action).
Display a range of nodes that have the same prefix in the network map for this manager resource	*prefix******,in the Node Name field and press F6 (Action) (for example, DEC*).
Display a specific node contained in the network map for this manager resource	The known node name Node Name field and press F6 (Action) (for example, DECD1 as shown in Figure 13-6).

Figure 13-6. Displaying the Network Map

```
SOLVPROD--------- File Transfer : Specify A NETMAP Node Name ---------------
Command ===>                                                  Function=UPDATE

.- Specify Node Name -------------------------------------------------------.
|                                                                           |
|  Node Name ............. DECD1__________                                |
|                                                                           |
```

```
SOLVPROD--------- File Transfer : 'SELECT' Command Results -----Columns 001 079
Command ===>                                                  Scroll ===> PAGE

********************************* TOP OF DATA *********************************
SAFL000I Netmap record(s) SELECTed from the Network Map
=========================================================
                    SELECT NETWORK MAP
=========================================================

Node Name   : DECD1               VTAM Applid   : DECD1L
Max Parsess : 255                 Def Ses Class : 16
Session Type: SNA                 Environment   :
Node Status : INTERNAL, SEND, RECEIVE
_____________________________________________________
RFCDCMD07 COMMAND PROCESSING COMPLETED
****************************** BOTTOM OF DATA *******************************
```

Step 3. Press F3 (Exit) to return to the file transfer status monitor.

Displaying the Initialization Parameters of a CONNECT:Direct Region

To display the initialization parameters of a CONNECT:Direct region, proceed as follows:

Note

The IIP command is valid only for CONNECT:Direct Version 2.1.1 or later, as Version 1.8 does not support the INQUIRE INITPARMS command.

Step 1. At the file transfer status monitor, enter **IIP** beside the desired CDMGR resource.

The INQUIRE INITPARMS panel is displayed, as shown in Figure 13-7.

Figure 13-7. Displaying CONNECT:Direct Initialization Parameters

```
SOLVPROD------------- File Transfer : INQUIRE INITPARMS -------Columns 001 079
Command ===>                                                   Scroll ===> PAGE

********************************* TOP OF DATA ********************************
SGNQ000I INQUIRE command processing complete.
==============================================================================
DECD1             *INQUIRE INITPARM*  DATE: 07/17/97  TIME: 12:01:38
==============================================================================

CKPT.MODE               => (RECORD  BLOCK   PDS     NOPDS   VSAM    VSAM    )
CKPT.DAYS               => 4
CONNECT.WAIT            => 3
ESTAE                   => YES
MAX.TAPE                => 10
MAXPRIMARY              => 6
MAXSECONDARY            => 6
MAXRETRIES              => 10
MAXBATCH                => 4
MAXUSERS                => 6
MAXPROCESS              => 12
MCS.SIGNON              => SIGNON (DISPLAY SUPPRESSED)
NDM.NODE                => 1
 F1=Help      F2=Split     F3=Exit                   F5=Find
 F7=Backward  F8=Forward   F9=Swap     F10=Left     F11=Right
```

Step 2. Press F3 (Exit) to return to the file transfer status monitor.

Listing and Managing CONNECT:Direct Processes

You can display processes for a CONNECT:Direct resource on the file transfer status monitor. The processes displayed are those associated with the monitored CONNECT:Direct queue. The following CONNECT:Direct queues are monitored by your region:

Queue Name	Platform
Wait queue	All
Hold queue	All
Timer queue	All
Exec queue	All except OS/400
Bad queue	Tandem
Call queue	Tandem
Initial queue	Tandem
Retain queue	Tandem
Suspend queue	Tandem
X-R&T queue	Tandem
Active queue	OS/400
Start queue	OS/400

NetMaster for File Transfer also allows you to monitor processes of a particular status within a specific queue type. The process status type is specified in the resource definition. See the section, *Customizing Criteria for Monitoring CONNECT:Direct Queues*, on page 15-10 for additional information on customizing queue monitor resources.

Listing processes and managing processes are discussed in the following sections.

Note

When you use any function in NetMaster for File Transfer that requires authorized access to CONNECT:Direct, you need to confirm your CONNECT:Direct signon details (see the section, *Confirming Signon Details for a CONNECT:Direct Command*, on page 13-15 for further details).

This confirmation is necessary only once in each session.

Listing Processes

You can list processes within CONNECT:Direct queues that are monitored by the NetMaster for File Transfer product.

To list CONNECT:Direct processes, enter **D** beside a CDMON process queue monitor (see Figure 13-8).

Figure 13-8. Displaying a CONNECT:Direct Process Queue Monitor

```
SOLVPROD----------------- Status Monitor : Owner(DECD1) ---------------FT1-0001
Command ===>                                                  Scroll ===> PAGE

                 S=Status L=Log D=Display A=Act T=Term DB=Database ?=List Cmds
    System   Class    Resource     Desired  Actual     Mode       Logical   Ovr
    FT1      CDMGR    DECD1        ACTIVE  ACTIVE     AUTOMATED  OK
    FT1      CDMON    DECD1.IPLIST LISTENER TASK FOUND AT 16.42
    FT1      CDMON    DECD1.MIPCON 1 CONNECTIONS CHECKED. ALL OK AT 16.38
    FT1      CDMON    DECD1.MSNASE NO SESSIONS EXCEED IDLE TIME LIMIT AT 16.38
    FT1      CDMON    DECD1.QEXEC  QUEUE(EXEC) STATUS(ANY) CNT(0) AT 16.33
 D  FT1      CDMON    DECD1.QHOLD  QUEUE(HOLD) STATUS(ANY) CNT(0) AT 16.33
                 ON    DECD1.                          ANY) CNT(0) AT 16.33
                 ON    DECD1.                          ANY) CNT(0) AT 16.33
    FT1      CDMON    DECD1.SHOLDW QUEUE(HOLD) STATUS(WC) CNT(0) AT 16.33
    FT1      CDMON    DECD1.SRETRY QUEUE(TIMER) STATUS(RETRY) CNT(0) AT 16.33
    **END**

 F1=Help      F2=Split     F3=Exit      F4=Return    F5=Find
 F7=Backward  F8=Forward   F9=Swap
```

D command

Resource type is QUEUE

You can also enter any of the following commands beside a CDMGR resource to list its queued processes:

Command	Queued Process Displayed
VA	All queued processes
VAC	Processes in the Active queue
VB	Processes in the Bad queue
VC	Processes in the Call queue
VE	Processes in the Exec queue
VH	Processes in the Hold queue
VI	Processes in the Initial queue
VR	Processes in the Retain queue
VST	Processes in the Start queue
VSU	Processes in the Suspend queue
VT	Processes in the Timer queue
VW	Processes in the Wait queue
VXR	Processes in the Retain-Timer queue

A list of processes is displayed, as shown in Figure 13-9.

Figure 13-9. Queued Processes List

```
SOLVPROD---------- Automation Services : DECD1 HOLD Queue ---------------------
Command ===>                                                   Scroll ===> PAGE

                                   S/V=View C=Change D=Delete H=Hold R=Release
    Prc Name    Prc Num Stat   Queue Sub Node         Other Node       User Id
    HOLDQ01           1 HI     HOLD  DECD1            QACD1            user1
    HOLDQ02           2 HI     HOLD  DECD1            QACD1            user1
    HOLDQ03           3 HI     HOLD  DECD1            QACD1            user1
    HOLDQ04           4 HI     HOLD  DECD1            QACD1            user1
    HOLDQ05           5 HI     HOLD  DECD1            QACD1            user1
    HOLDQ06           6 HI     HOLD  DECD1            QACD1            user1
    HOLDQ07           7 HI     HOLD  DECD1            QACD1            user1
    HOLDQ11           8 HI     HOLD  DECD1            QACD1            user1
    HOLDQ02           9 HI     HOLD  DECD1            QACD1            user1
    **END**
```

To refresh the list, press F6 (Refresh).

Managing Processes

You can manage the listed CONNECT:Direct processes by using the actions described in Table 13-2.

Table 13-2. Actions for CONNECT:Direct Queued Processes

Action	Description
C	Use the C (Change) action to modify the parameters of a nonexecuting process. You can also release a held process or restart a failed process using this command.
D	Use the D (Delete) action to delete a nonexecuting process from the queue.
DF	Use the DF (Delete/Force) action to forcibly terminate and delete the process from the Exec queue.
DH	Use the DH (Delete/Hold) action to terminate a process on the CONNECT:Direct for NT executing queue and move it to the hold queue.
FP	Use the FP (Flush Process) action to terminate an executing process.
FPF	Use the FPF (Flush Process Force) action to force terminate an executing process.
H	Use the H (Hold) action to place a nonexecuting process on the Hold queue.
R	Use the R (Release) action to release a held process.
SP (not applicable to processes on distributed systems)	Use the SP (Suspend Process) action to terminate execution and place an executing process on the Hold queue.
SPF (not applicable to processes on distributed systems)	Use the SPF (Suspend Process Force) action to force terminate an executing process and place that process on the Hold queue.
V	Use the V (View) action to display a panel which provides details of the selected process. An F6 (Refresh) function key is available on that panel for you to refresh the displayed information.

Listing and Managing TCP/IP Connections

The TCP/IP : Connection List panel displays information about the current state of active connections for the monitored CA-XCOM, CONNECT:Direct, or FTP region on an OS/390 system. You can investigate problems occurring on any listed connection by using the actions displayed on the TCP/IP : Connection List panel, shown in Figure 13-10. These actions can be used as tools in the investigation of a file transfer problem.

You can display a list of TCP/IP connections in either of the following ways:

- Enter **D** beside a TCP/IP connections monitor resource. Figure 13-10 shows an example.
- Enter **VIP** beside a XCMGR, CDMGR, or FTPMGR resource.

Press F1, to access online help for additional information on the fields displayed on the TCP/IP : Connection List panel.

Figure 13-10. Displaying TCP/IP Connections

```
SOLVPROD---------------- Status Monitor : Owner(XC3000) ---------------FT1-0001
 Command ===>                                                   Scroll ===> PAGE

                 S=Status L=Log D=Display A=Act T=Term DB=Database ?=List Cmds
    System   Class    Resource     Desired  Actual     Mode       Logical   Ovr
    FT1      XCMGR    XC3000       ACTIVE   ACTIVE     MANUAL     OK
 D  FT1      XCMON    XC3000.CONNE 2 CONNECTIONS CHECKED. ALL OK AT 11.55
    FT1      XCMON    XC3000.LISTE LISTENER TASK FOUND AT 11.53
    FT1      XCMON    XC3000.INACT STATUS(INACTIVE) CNT(0) AT 11.52
```

```
SOLVPROD---------------- TCP/IP : Connection List --------------Stack: TCPIP38
 Command ===>                                                   Scroll ===> CSR

    Line 1 of 3                                   Refresh Every ...      Seconds
                                            P=Ping T=TraceRoute NL=Lookup Z=Drop
                                                                            L=Log
    Foreign Host     Port Local Host       LPort LU name  User ID  TaskName
    172.16.123.22    8044 192.168.110.25    1835                    XC3000
    *                   * *                 8044                    XC3000
    172.16.123.22    8044 192.168.110.25    1808                    XC3000
    **END**

 F1=Help      F2=Split     F3=Exit                                F6=Refresh
 F7=Backward  F8=Forward   F9=Swap                 F11=Right
```

Dropping a TCP/IP Connection

Where an error condition exists (for example, the connection seems to have stalled), it might be necessary to drop that connection and have CA-XCOM, CONNECT:Direct, or FTP reconnect.

To drop a TCP/IP connection for the monitored region, proceed as follows:

Step 1. Enter **Z** beside the connection on the TCP/IP Connection List.

A confirmation message is displayed.

Note

With TCPaccess, you are prompted to supply a user ID and password. Ensure that you are authorized to issue the SYSSTAT command.

Step 2. Press ENTER to confirm. A message informing you that the connection has been successfully dropped is displayed, and the connection is highlighted on the connection list, as shown in Figure 13-11.

Figure 13-11. Dropping a TCP/IP Connection

```
SOLVPROD---------------- TCP/IP : Connection List --------------Stack: TCPIP38
Command ===>                                                  Scroll ===> PAGE
IPCALL62 Connection id 0000D575 dropped successfully
    Line 1 of 2                                   Refresh Every ...      Seconds
                                            P=Ping T=TraceRoute NL=Lookup Z=Drop
                                                                            L=Log
    Foreign Host     Port Local Host       LPort LU name  User ID  TaskName
    *                  * *                  8044                    XC3000
    172.16.123.22   ***DROPPED***
    **END**
```

Listing and Managing CONNECT:Mailbox Batches

You can list and manage CONNECT:Mailbox batches from the file transfer status monitor.

To display a list of batches:

Step 1. Enter **DIR** beside a CMMGR resource.

Step 2. Enter the required mailbox ID.

Step 3. Press F6 (Action). The Mailbox Batch List is displayed.

Figure 13-12. Mailbox Batch List

```
SOLVPROD--------- Automation Services : Mailbox Batch List --------------DE1REM
Command ===>                                                   Scroll ===> PAGE

     I=Invoke C=Connect S=StatFlags expand   StatFlag changes (set on): R=Ready
     D=Deleted T=Transmitted E=Extracted M=Multiple   (set off): NR ND NT NE NM
     Number User Batch ID            Date        Time  Recs/Blks StatFlags  VBQ
        813 PCAND1  Q1U9054833-S01   30-MAR-2000 15:14       101  A NTU       1
        814 PCAND1  Q1U9054833-S02   30-MAR-2000 15:14       101  A NTU       1
        815 PCAND1  Q1U9054833-S03   30-MAR-2000 15:14       101  A NTU       1
        816 PCAND1  Q1U9054833-S04   30-MAR-2000 15:14       101  A NTU       1
        817 PCAND1  Q1U9054833-S05   30-MAR-2000 15:15       101  A NTU       1
        818 PCAND1  Q1U9054833-S06   30-MAR-2000 15:16       101  A NTU       1
        819 PCAND1  Q1U9054833-S07   30-MAR-2000 15:16       101  A NTU       1
        820 PCAND1  Q1U9054833-S08   30-MAR-2000 15:17       101  A NTU       1
        821 PCAND1  Q1U9054833-S09   30-MAR-2000 15:18       101  A NTU       1
        822 PCAND1  Q1U9054833-S10   30-MAR-2000 15:19       101  A NTU       1
        823 PCAND1  Q1U9054833-S11   30-MAR-2000 15:19       101  A NTU       1
        826 PCAND1  Q1U9054833-S14   30-MAR-2000 15:20       101  A NTU       1
    **END**
```

To manage CONNECT:Mailbox batches you can issue the following line commands against one or more batches:

Command	Description
I	Invokes an end of batch agent request
C	Initiates an Auto Connect request
S	Provides an explanation of the status flags
R	Sets the status flag to allow the batch to be requested by a remote site, or transmitted by a host-initiated Auto Connect
D	Sets the status flag to show the batch has been deleted
T	Sets the status flag to indicate that the batch has been transmitted
E	Sets the status flag to indicate that the batch was extracted by the EXTRACT utility
M	Sets the status flag to indicate that the batch is available for multiple transmissions

The following commands turn the corresponding status flags off:

NR ND NT NE NM

To issue any of these line commands against all listed batches, at the command prompt enter **All *x***, where *x* is one of the following commands:

R D T E M

Initiating an Auto Connect

You can start a host-initiated Auto Connect from the file transfer status monitor. By using the CON command you can override the *CONNECT record parameters specified in your Options Definitions File (ODF).

To initiate an Auto Connect do this:

Step 1. Enter **CON** beside a CMMGR resource.

The File Transfer : CON panel is displayed (see Figure 13-13).

Figure 13-13. File Transfer Auto Connect

```
SOLVPROD-------------------- File Transfer : CON ------------------SOLVPROD:CM1
Command ===>

List Name .......
Mailbox ID ......
User Batch ID ...                                  Generic
Batch Number ....
OneBatch ........ NO        (YES or NO, default is NO)
ACQueue .........           (YES or NO)
Compress ........           (YES or NO)
Truncate ........           (YES or NO)
Batch Separator +

For SNA only
   Media .......+

For BSC only
   Mode ........+
   Transparent...           (YES or NO)
   Block ........           (1-99)
   Line ID ......           (Switched lines only)

 F1=Help      F2=Split     F3=Exit      F4=Save      F5=Load      F6=Action
                           F9=Swap
```

You must enter a value in the List Name field.

The list name must be specified in the ODF.

Save the criteria for later use by pressing F4 (Save).

Step 2. Complete the panel and press F6 (Action).

Batches are transmitted as follows:

If you specified …	**Then …**
List name only	Batches appropriately flagged are transmitted
Mailbox ID	Batches appropriately flagged in this mailbox are transmitted
User batch ID	Batches matching this ID are transmitted

Step 3. Press F3 to exit the panel.

You can also issue the CON command from the Mailbox Batch List command line. The NetMaster for File Transfer : CON panel is displayed with the Mailbox ID field prefilled.

Monitoring CONNECT:Mailbox Resources

You can display CONNECT:Mailbox monitors via the status monitor (see Figure 13-14). The CONNECT:Mailbox monitors are:

- ACQUEUE—Auto Connect queue
- SNASESS—Stalled SNA sessions
- BSCLINES—BSC Lines

Figure 13-14. Displaying CONNECT:Mailbox Monitors

```
SOLVPROD---------- Status Monitor : File Transfer Resources -----------FT1-0001
Command ===>                                                   Scroll ===> PAGE

                 S                                  T=Term DB=Database ?=List Cmds
    System   Class                                l     Mode       Logical   Ovr
    FT1      CMMGR                                IVE   MANUAL     ATTENTION
Z   FT1      CMMGR    DECM1        ACTIVE   ACTIVE     MANUAL     OK
    FT1      CMMGR    HYCMMGR      ACTIVE   INACTIVE   MANUAL     ATTENTION
    FT1      CMMGR    QACM1        ACTIVE   ACTIVE     MANUAL     OK
    FT1      CMMGR    QACM2        ACTIVE   ACTIVE     MANUAL     OK
```

Enter Z beside the required CONNECT:Mailbox Manager to display the associated monitors

```
SOLVPROD----------------- Status Monitor : Owner(DECM1) ---------------FT1-0001
Command ===>                                                   Scroll ===> PAGE

                 S=                                 t T=Term DB=Database ?=List Cmds
    System   Class    Resource     Desired  Actual     Mode       Logical   Ovr
    FT1      CMMGR    DECM1        ACTIVE   ACTIVE     MANUAL     OK
D   FT1      CMMON    DECM1.ACQ    AUTO CONNECT QUEUE CNT(1). ALL OK AT 11.29
    FT1      CMMON    DECM1.SNASES NO STALLED SNA SESSIONS. ALL OK AT 11.29
```

Enter D beside the required CONNECT:Mailbox Monitor.

```
SOLVPROD--------- File Transfer : DECM1 Auto Connect Queue --------------------
Command ===>                                                   Scroll ===> CSR

                                                                      D=Delete
 List Name  Priority  Date         Time     Reason       Entry Number
 QACM2      0         23-JAN-2000  23:45    SESSIONS     205
 QACM1      0         23-JAN-2000  23:45    SESSIONS     206
 **END**
```

Listing and Managing Queued Auto Connects

To display the Auto Connect Queue monitor, from the Status Monitor, enter **D** beside the monitor name (see Figure 13-14). The panel lists any queued Auto Connects for the list names defined in the monitor.

Note

You can display all the queued Auto Connects associated with a CONNECT:Mailbox manager by entering **VA** beside the CONNECT:Mailbox manager.

To delete a queued Auto Connect queue, enter **D** beside the entry you want to delete.

Listing and Managing CONNECT:Mailbox BSC Lines

To display the BSC Lines monitor, from the Status Monitor, enter **D** beside the required BSC line monitor name (see Figure 13-14). The panel lists the BSC lines that are named in the monitor and shows the status of the lines.

Note

You can display all BSC lines associated with a CONNECT:Mailbox manager by entering **VB** beside the CONNECT:Mailbox manager.

You can issue the following commands against the listed lines:

- S (Start)—to start a line
- P (Stop)—to stop a line

Listing CONNECT:Mailbox SNA Sessions

To display the SNA session information, from the Status Monitor, enter **D** beside the required SNA sessions monitor name (see Figure 13-14). The panel lists the batches in CONNECT:Mailbox SNA file transfer sessions with the monitored remote sites.

Note

You can display all the SNA sessions associated with a CONNECT:Mailbox manager by entering **VS** beside the CONNECT:Mailbox manager.

Listing and Managing CONNECT:Mailbox VSAM Batch Files

As batches are added and deleted from the VSAM batch queues, it may be necessary to recover space. You can monitor and maintain VSAM files from the VSAM File Statistics panel.

To access the VSAM File Statistics, enter **VSS** beside the required CMMGR resource from the resource monitor (see Figure 13-15).

Figure 13-15. VSAM File Statistics

```
SOLVPROD---------------- Status Monitor : Owner(DECM1) ---------------FT1-0001
Command ===>                                                   Scroll ===> CSR

                  S=Status L=Log D=Display A=Act T=Term DB=Database ?=List Cmds
    System   Class    Resource     Desired  Actual     Mode       Logical   Ovr
vss DECD1    CMMGR    DECM1        ACTIVE   STARTING   MANUAL     OK
```

```
SOLVPROD--------- Automation Services : VSAM File Statistics -------------------
Command ===>                                                   Scroll ===> CSR
```

Press F11 (Right) to display more information

```
                                  A=Allocate AC=Allocate Collector D=Deallocate
                                             LC=LISTCAT Report AR=Assisted REORG
                      High-Alloc'd   High-Used
                        Relative      Relative            Offline Alloc  Collect
    File ID  %Used   Byte Address  Byte Address  Extents  Users  Status Status
    VBQ01      97        58060800      56401920     13       1   YES    CURRENT
    VBQ02     100         4147200       4147200      1       1   YES
    VBQ03     100       102021120     102021120    119       1   YES
    VBQ04     100       102021120     102021120    119       1   YES
    VBQ05     100        13271040      13271040     12       1   YES
    VCF        50         1658880        829440      1       1   YES
    VLF1        *               *             *      *       *   NO
    VLF2      100        29030400      29030400     14       1   YES    CURRENT
    VPF         1        68843520        829440      1       1   YES
    **END**
```

```
SOLVPROD--------- Automation Services : VSAM File Statistics -------------------
Command ===>                                                   Scroll ===> CSR

                                  A=Allocate AC=Allocate Collector D=Deallocate
                                             LC=LISTCAT Report AR=Assisted REORG

                                                         Offline Alloc  Collect
    File ID  Dataset Name                                 Users  Status Status
    VBQ01    AUDE0.DECM1.VBQ01                               1   YES    CURRENT
    VBQ02    AUDE0.DECM1.VBQ02                               1   YES
    VBQ03    AUDE0.DECM1.VBQ03                               1   YES
    VBQ04    AUDE0.DECM1.VBQ04                               1   YES
    VBQ05    AUDE0.DECM1.VBQ05                               1   YES
    VCF      AUDE0.DECM1.VCF                                 1   YES
    VLF1     AUDE0.DECM1.VLF1                                *   NO
    VLF2     AUDE0.DECM1.VLF2                                1   YES    CURRENT
    VPF      AUDE0.DECM1.VPF                                 1   YES
    **END**
```

The following table lists available commands and the file types the commands can be issued against:

Command	Description	File Type
A	Allocates a VSAM file to CONNECT:Mailbox	VBQ, VLF
AC	Allocates and assigns a data file as a current collection file or logging file to CONNECT:Mailbox	VBQ, VLF
D	Deallocates a file from CONNECT:Mailbox	VBQ, VLF
LC	Executes and displays the results of an IDCAMS LISTCAT report	All types
AR	Displays the Assisted REORG Facility panel	VBQ, VLF

You cannot deallocate a VBQ and VLF file if it is the current collection or log file.

To use the Assisted REORG Facility do this:

Step 1. Enter **AR** beside the required VSAM file.

If the file has not been deallocated, you are prompted to deallocate the file (see Figure 13-16). Press F6 (Confirm) to deallocate the file.

Figure 13-16. Deallocate Confirmation Panel

```
SOLVPROD---------- Automation Services : Assisted REORG Facility ------FT1-0001
Command ===>

                          Deallocate VBQ03 File
.------------------------------------------------------------------------.
| This action will deallocate VBQ03 from CONNECT:Mailbox in preparation  |
| for an Assisted REORG of the file. Batches that reside on the selected VBQ |
| file will not be available for transmission to a remote site.          |
'------------------------------------------------------------------------'

  Press the Confirm key to confirm the request or the Cancel key to cancel
```

When the file is deallocated the Summary of Execution Status panel is displayed detailing the default dataset names to be used during the reorganization (see Figure 13-17).

Figure 13-17. Summary of Execution Status Panel

```
SOLVPROD------- Automation Services : Assisted REORG Facility --------FT1-0001
Command ===>

                          Summary of Execution Status
.------------------------------------------------------------------------.
|                                                                        |
| ( Done    ) 1. Deallocate AUDE0.DECM1.VBQ03                            |
| ( Pending ) 2. Rename to  AUDE0.DECM1.VBQ03.TMP0                       |
| ( Pending ) 3. Create new dataset ( First 5 lines of IDCAMS input shown ) |
|                                                                        |
|               DEFINE CLUSTER   -                                       |
|                 (NAME(AUDE0.DECM1.VBQ03)    -                          |
|                  VOLUMES(DIP001)    -                                  |
|                  CYLINDER(10 1) -                                      |
|                  MODEL(AUDE0.DECM1.VBQ03.TMP0))                        |
|                                                                        |
| ( Pending ) 4. Copy records into new dataset and if successful, delete work |
|                dataset    AUDE0.DECM1.VBQ03.TMP0                       |
| ( Pending ) 5. Allocate   AUDE0.DECM1.VBQ03                            |
|                                                                        |
'------------------------------------------------------------------------'
  Press the Confirm key for Auto Execution or Cancel key to Update Execution
 F1=Help      F2=Split                                          F6=Confirm
                          F9=Swap                              F12=Cancel
```

Step 2. Press F6 (Confirm) to automatically execute the reorganization.

If you want to change any default information provided, press F12 (Cancel). The Assisted REORG Facility panel is displayed (see Figure 13-18). Enter **E** beside the task you want to change. When you have made the required changes press F6 (Action) to execute the task. When the task completes successfully you can choose to continue the reorganization automatically by pressing F6 (AutoExec) or manually execute each task by entering **E** (Execute) beside the next task until all tasks have completed successfully.

Figure 13-18. Assisted REORG Facility

```
SOLVPROD--------- Automation Services : Assisted REORG Facility -------FT1-0001
Command ===>                                                  Scroll ===> PAGE
RFCMV2L06 REQUEST TO SUSPEND AUTO EXECUTION HAS BEEN ACCEPTED
                                                   S/B=Browse E=Execute R=Redo
    Task Description                                             Status
    Deallocate AUDE0.DECM1.VBQ03                                 Done
    Rename AUDE0.DECM1.VBQ03                                     Pending Review
    Create new AUDE0.DECM1.VBQ03                                 Pending Review
    Copy data to AUDE0.DECM1.VBQ03                               Pending
    Allocate AUDE0.DECM1.VBQ03                                   Pending
    **END**









 F1=Help      F2=Split     F3=Exit                                F6=AutoExec
                           F9=Swap
```

As each task is completed the status field is updated and the task is highlighted. The status can be:

- Pending Review—user input required if the defaults are not acceptable
- Pending—waiting for execution
- In Progress—the task is in progress
- Error—the task ended in error and is highlighted in red
- Done—the task completed successfully and is highlighted in white

Step 3. When all tasks have completed successfully, press F3 to exit the Assisted REORG Facility.

If a task ends in error, do this:

Step 1. Enter **B** beside the task that has ended in error.

Browse the results of the task.

Step 2. Enter **R** beside the task to reset the default values of the task.

Step 3. If required, make any changes to the task.

Step 4. Press F6 to continue the reorganization automatically, or enter **E** beside the next task until all tasks have completed successfully.

A task can only be executed if the preceeding task completed successfully.

If the reorganization is stopped manually before all tasks are complete a warning message is issued indicating either the next task to be completed or the last completed task. You might need to complete the remaining tasks offline.

Displaying Logs

You can access various logs to assist in solving file transfer problems. The following logs are available to you:

- File transfer log
- Activity log
- Transient logs

Use the F7 (Backward) and F8 (Forward) keys to scroll through a displayed log. Use the F10 (Left) and F11 (Right) keys to move the displayed view of any log to the left or right, enabling you to view messages that extend across more than one panel.

Displaying the File Transfer Log

Key Concept

The file transfer log provides an historical view of the activities for the selected file transfer region. One file transfer log is created for each NetMaster for File Transfer region. This means that if multiple CA-XCOM, CONNECT:Direct, FTP server, and FTS regions are defined to a NetMaster for File Transfer system image, then all messages generated by those regions will be saved to one file transfer log.

To display the file transfer log from the file transfer status monitor, enter **FTL** beside a listed file transfer resource, or **FTLOG** at the Command ===> prompt.

Note

Entering **FTLOG** at the Command ===> prompt displays the whole file transfer log.

Entering **FTL** beside a listed resource displays the file transfer log entries for that resource.

Figure 13-19 shows an example of the file transfer log for a CONNECT:Direct region.

Figure 13-19. File Transfer Log

```
SOLVPROD----------- File Transfer Log for WED 20-SEP-2000 --------Line 1 of 135
Command ===>                                                  Scroll ===> PAGE

Time     Log Data
        ----+----10---+----20---+----30---+----40---+----50---+----60---+----7
15.09.35 RFCDEV01 PROCESS MONST01(3) SUBMITTED
15.09.35 RFCDEV03 PROCESS MONST01(3) WAS SUBMITTED BY qauser1 ON QACD1. PNODE=Q
15.09.38 SVTM055I SESSION ESTABLISHED WITH            SNODE=QACD1            (
15.09.39 SVTM055I SESSION ESTABLISHED WITH            PNODE=QACD1            (
15.09.39 SVTM036I PROCESS STARTED   MONST01 (       3) SNODE=QACD1            (
15.09.39 SVTM036I PROCESS STARTED   MONST01 (       3) PNODE=QACD1            (
15.10.26 RFCDEV19 PROCESS MONST01(3) RUN TASK ABEND1 STEP ABEND806 FAILED: CC=-
15.10.26 RFCDEV03 PROCESS MONST01(3) WAS SUBMITTED BY qauser1 ON QACD1. PNODE=Q
15.10.26 RFCDEV19 PROCESS MONST01(3) RUN TASK ABEND1 STEP ABEND806 FAILED: CC=-
15.10.26 RFCDEV03 PROCESS MONST01(3) WAS SUBMITTED BY qauser1 ON QACD1. PNODE=Q
15.10.27 SVTM052I ABEND1   RUN TASK MONST01 (       3) SNODE=QACD1            (
15.10.38 SVTM052I ABEND1   RUN TASK MONST01 (       3) PNODE=QACD1            (
15.10.40 RFCDEV11 PROCESS MONST01(3) COMPLETED
15.10.40 RFCDEV03 PROCESS MONST01(3) WAS SUBMITTED BY qauser1 ON QACD1. PNODE=Q
15.10.40 SVTM037I PROCESS ENDED     MONST01 (       3) SNODE=QACD1            (
15.10.41 SVTM037I PROCESS ENDED     MONST01 (       3) PNODE=QACD1            (
15.10.42 SVTM056I SESSION TERMINATED  WITH            PNODE=QACD1            (
 F1=Help      F2=Split     F3=Exit      F4=ActLog    F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap     F10=Left     F11=Right
```

Note

You can ignore failure messages due to a $RF* CONNECT:Direct process. These messages are the results of polling a defined CONNECT:Direct remote node (CDMON resource of type REMOTE-NODE).

Browsing the File Transfer Log Online

The following aids are available to help you use the file transfer log:

- Forward and backward scroll
- Various display formats
- Highlighting log records
- Log filter to restrict the records displayed
- Positioning by time
- Positioning by date, either absolute or relative
- Positioning by labels set in the log
- Searching for text
- Selective printing of log records

See the online help for detailed information about these aids.

Suppressing Messages Logged to the File Transfer Log

You can suppress CONNECT:Direct messages from being logged to the file transfer log. You do this by specifying which event messages generated by CONNECT:Direct regions are logged to the file transfer log. See the section, *Logging Selected CONNECT:Direct Messages to the File Transfer Log*, on page 16-6 for the procedure for selecting the messages to be logged.

Accessing Activity Log from the File Transfer Log

You can find out about other activities that were occurring at the time a file transfer message is logged by accessing the activity log as follows:

Step 1. From the file transfer log, place the cursor on the message of interest.

Step 2. Press F4 (ActLog) to display the activity log.

Step 3. When you have finished using the activity log, press F3 (Exit) to return to the file transfer log.

Displaying the Activity Log

Key Concept

The activity log provides an historical view of the system and activities monitored by the region. A region can have more than one activity log, of which only one is open for logging. The activity log is stored on DASD, so that users can access this information if necessary. You can also access the activity log from the transient log, as described in *Accessing the Activity Log from the Transient Log*, on page 13-38.

To display the activity log, proceed as follows:

Step 1. Access the primary menu.

Step 2. At the Select Option ===> prompt, enter **H**.

Step 3. On the displayed History Data : Primary Menu, enter **L**. (If you want to access the log in a linked region, identify the region in the Link Name field.).

Note

You can also enter **$LOG** at the Command ===> prompt of file transfer status monitor to display the current activity log.

An activity log appears on your screen displaying the logged activities. The log also displays the day, date, and time when the region was last initialized.

Browsing the Activity Log Online

The aids available for you to browse the activity log online are similar to those available for the file transfer log. See the section, *Browsing the File Transfer Log Online*, on page 13-34 for a list of the browsing aids. See also the help.

Suppressing Messages Logged to the Activity Log

You can suppress messages logged to the activity log. This enables you to log only those messages generated by file transfer resources. See the section, *Logging Selected Messages to the Activity Log*, on page 16-2 for the procedure for selecting the messages to be logged.

Displaying the Transient Log

Key Concept

Each file transfer resource has its own transient log. The transient log provides a real-time view of the activity associated with the selected resource. Transient logs are not kept between region restarts.

To display the transient log from the file transfer status monitor, enter **L** beside a resource.

A transient log is displayed for the selected resource, as shown in Figure 13-20.

Figure 13-20. Transient Log

```
SOLVPROD----- Automation Services :  DECD1 Transient Log Browse ---------------
Command ===>                                                   Scroll ===> CSR

                                                          S=Select H=HelpMessage
    Time     Log Event
    16.06.46 RMMF0300 SSHA004I DECD1
    16.06.46 RMSTMS44 ACTUAL STATE CHANGED FROM <ACTIVE> TO <STOPPING> BY <SSH
    16.07.02 RMSTMS44 ACTUAL STATE CHANGED FROM <STOPPING> TO <INACTIVE> BY <S
    16.07.02 SITB001I CONNECT:DIRECT FOR MVS TERMINATION COMPLETE.
    16.07.02 RMMO0120 EXECUTING PROCESS($NCL) FOR DECD1
    16.07.04 IEF404I DECD1 - ENDED - TIME=16.07.04
    16.07.05 $HASP395 DECD1    ENDED
    16.07.41 RMSTMS44 ACTUAL STATE CHANGED FROM <INACTIVE> TO <STARTING> BY <$
    16.07.41 $HASP100 DECD1    ON STCINRDR
    16.07.41 $HASP373 DECD1    STARTED
    16.07.41 IEF403I DECD1 - STARTED - TIME=16.07.41
    16.07.49 SITA001I CONNECT:DIRECT FOR MVS INITIALIZATION BEGUN.
    16.09.07 SVTJ010I - NDM APPLICATION INACTIVE ENTER 'CANCEL' OR 'GO'
    16.09.07 RMSTMS40 EXTENDED DISPLAY<*** WTOR OUTSTANDING ***> SEVERITY<1> F
    16.09.08 RMMF0010 OUTSTANDING WTOR ALERT RECEIVED
    16.13.59 RMCALL06 COMMAND(L) REQUESTED BY USERID(USER01) FOR CDMGR(DECD1)
    **END**
 F1=Help      F2=Split     F3=Exit                   F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap     F10=Left     F11=Right
```

The Transient Log Browse panel displays messages for the resource in chronological order. Messages in the transient log appear in different colors according to the severity level of the message, as follows:

Severity	Description	Color
1	Severe error	Red
2	System command	White
3	Status change	Yellow
4	Warning	Turquoise
5	Informational or user-defined log message	Blue
6	Audit trail	Pink

Setting the Criteria to Display Logged Messages Selectively

Key Concept

When you access the transient log of a resource, you are profiled to view all messages logged for that resource. You can limit the number of messages you see in the current session by profiling for certain criteria.

To set profile values, enter **PROFILE** at the Command ===> prompt. A panel appears displaying the current profile setting. Change the settings as required. See the online help for additional information about the available settings.

Obtaining Help on a Logged Message

To display the detailed help text associated with a message in the transient log, enter **H** beside the message.

Printing a Transient Log

To print a transient log, proceed as follows:

Step 1. Enter **P** beside a resource to print its transient log.

The Generate a Report panel is displayed.

Step 2. Specify your printing requirements.

Step 3. Press F6 (Confirm) to print the log report.

Resetting a Transient Log

To reset the transient log of a resource, enter **LR** beside the resource. This command clears the transient log of all messages.

Accessing the Activity Log from the Transient Log

To access the activity log from the transient log, enter **S** beside a message in the transient log (see Figure 13-21).

The activity log for the region is displayed, as shown in Figure 13-21. Notice that the activity log displays messages around the time associated with the selected transient log message.

Figure 13-21. Accessing the Activity Log from the Transient Log

```
SOLVPROD----- Automation Services :  DECD1 Transient Log Browse ---------------
Command ===>                                                   Scroll ===> PAGE

                                                          S=Select H=HelpMessage
    Time     Log Event
    *** START OF LOG ***
S   08.05.07 RMDP0007 COMMAND 'D J,DECD1' ISSUED FOR CDMGR(DECD1)
    08.05.07 RMDP0021 DECD1    DECD1    CONNECT  NSW  S
```

```
NMLOG01---- Automation Services : Log for WED 20-SEP-2000 ------Line 750 of 875
Command ===>                                                  Scroll ===> PAGE

        Initialized on WED 20-SEP-2000 at 07.00.19.73. Jobname(SOLV17)
Time     Log Data
         ----+----10---+----20---+----30---+----40---+----50---+----60---+----7
08.05.07 N11209 COMMAND ACCEPTED. PURGE ID NUMBER IS 27.
08.05.07 RMLO0099 (CDMGR:DECD1) RMDP0007 COMMAND 'D J,DECD1' ISSUED FOR CDMGR(D
08.05.07 RMLO0099 (CDMGR:DECD1) RMDP0021 DECD1    DECD1    CONNECT  NSW  S
08.05.07 RMLO0099 (CDMGR:DECD1) RMSTMS44 ACTUAL STATE CHANGED FROM <UNKNOWN> TO
08.05.07 RMLO0099 (CDMGR:DECD1) RMDM0013 STATUS INQUIRY COMPLETED RC:0 RETURNED
08.05.07 N11C04 COMMAND SUBMITTED TO BSYS REGION.
08.05.08 START $RMDM00S OBJID='FT1     000109DECD1.IPLINK' STARTBY='STARTSYS'
08.05.08 N11C04 COMMAND SUBMITTED TO BSYS REGION.
08.05.08 START $RMDM00S OBJID='FT1     000109DECD1.IPLISTNR' STARTBY='STARTSYS'
08.05.08 N11C04 COMMAND SUBMITTED TO BSYS REGION.
08.05.09 START $RMDM00S OBJID='FT1     000109DECD1.PSHOLDWC' STARTBY='STARTSYS'
08.05.09 RMLO0099 (CDMON:DECD1.IPLINK) RMDP0015 EXECUTING PROCESS '$NCL
08.05.09 N11C04 COMMAND SUBMITTED TO BSYS REGION.
08.05.09 START $RMDM00S OBJID='FT1     000109DECD1.PSRETRYQ' STARTBY='STARTSYS'
08.05.09 RMLO0099 (CDMON:DECD1.IPLISTNR) RMDP0015 EXECUTING PROCESS '$NCL
08.05.09 N11C04 COMMAND SUBMITTED TO BSYS REGION.
 F1=Help      F2=Split     F3=Exit      F4=Return    F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap     F10=Left     F11=Right
```

Merging Transient Logs

Key Concept

You can merge the transient logs of monitor resources with a manager resource. This enables you to view and print the transient log for, for example, the CONNECT:Direct manager (CDMGR) and its owned resources (CDMON). To identify the owner of a message, the merged log contains the following additional information:

- System image name and version
- Class name and the resource name

Caution

This command may take some time to execute and consume many system resources.

To display a merged transient log, enter **LC** beside a manager resource. To refresh the log, press F6 (Refresh). The log display may extend over several screens. Use the F7 (Backward) and F8 (Forward) function keys to scroll through the screens.

The size of the merged transient log is limited by the size of the transient log of the selected manager resource. The size of the transient log is specified in the Automation Log Details panel of the manager resource definition. When the merged log becomes full, the oldest messages are replaced by the new messages.

Printing a Merged Transient Log

To print a merged transient log, proceed as follows:

Step 1. Enter **PC** beside a manager resource to print its merged transient log.

The PSM : Confirm Printer panel is displayed.

Step 2. Specify your printing requirements.

Step 3. Press F6 (Confirm) to print the log report.

Activating and Inactivating a File Transfer Resource

You can manually activate or inactivate a file transfer resource. This manual activation and inactivation is available only when the defined resource is in the MANUAL operation mode. See Chapter 14, *Controlling the System Image*, for an explanation of operating modes.

To determine the mode of operation for a particular resource, observe its Mode field on the file transfer status monitor.

Note

You can activate a monitor resource only if its owner manager is active.

Activating a File Transfer Resource

To activate a resource, proceed as follows:

Step 1. Enter **A** beside the resource.

A confirmation message is displayed.

Step 2. Press ENTER to confirm the activation.

Note

The A command executes the activation command specified in the Activation Details panel of the resource definition. See the section, *Customizing the Manager Resource Definition*, on page 15-44 for additional information about resource definitions.

Inactivating a File Transfer Resource

To inactivate a resource, proceed as follows:

Step 1. Enter **T** beside the resource.

A confirmation message is displayed.

Step 2. Press ENTER to confirm the inactivation.

Note

The T command executes the inactivation command specified in the Inactivation Details panel of the resource definition. See the section *Customizing the Manager Resource Definition*, on page 15-44 for additional information about resource definitions.

Issuing Commands to a File Transfer Resource

You can use the CMD command to issue commands to the following file transfer resources from your file transfer status monitor:

- Managers
- TCP/IP provider

For example, to display the statistics of a CONNECT:Direct region, proceed as follows:

Step 1. At the file transfer status monitor, enter **CMD** beside the desired CDMGR resource.

The CONNECT:Direct Commands panel is displayed.

Note

If you enter CMD beside an AS/400, Tandem, UNIX, or Windows NT CONNECT:Direct CDMGR resource, the Command Entry panel is displayed.

To issue CONNECT:Direct commands to CONNECT:Direct running on a remote system, do the following:

1. Type the CONNECT:Direct command directly at the ===> prompt on the Command Entry panel.
2. Press ENTER to issue the command, and view the command results.

For available commands, see the user's guide for the CONNECT:Direct product to which you want to issue commands.

Step 2. At the ===> prompt, enter **CMD INQUIRE STATISTICS**.

The current status of the selected CONNECT:Direct statistics logging facility is displayed, as shown in Figure 13-22.

Figure 13-22. Issuing CONNECT:Direct Commands

```
 SOLVPROD-------- Automation Services : CONNECT:Direct Commands-----Line 1 of 41
 Modify DECD1    ===>  CMD INQUIRE STATISTICS
                 ===>

 System SOLV13        Limit 1000   Wrap OFF   Edit OFF   Scroll OFF   Async ON

1---+----10---+----20---+----30---+----40---+----50---+----60---+----70---+----
 SYSCMD F DECD1,CMD INQUIRE STATISTICS
 N86510 COMMAND PASSED TO OPERATING SYSTEM
 12:47:18 STC 2368   CD  - RC=00000000  MSG=S
 12:47:18 STC 2368   INQUIRE command processing complete.
 12:47:19 STC 2368  ==========================================================
 12:47:19 STC 2368   DECD1            *INQ STATS* DATE: 07/17/97  TIME: 12:47:18
 12:47:19 STC 2368  ==========================================================

 12:47:20 STC 2368   Status       => Enabled               Sec. Name  =>
 12:47:20 STC 2368   Return Code  => 0                     Message ID => SSTW000
 12:47:20 STC 2368   Last "S2"    => 12:05:36              Que Wait   => No
 12:47:20 STC 2368   Dsn Base     => AUDE0.DECD1.STATS
 12:47:20 STC 2368   Excluded     =>
 12:47:20 STC 2368   *****************  F I L E                          *****
 12:47:21 STC 2368   Status       => Complete
 12:47:21 STC 2368   Start Date   => 07/12/97                            /17/9
 12:47:21 STC 2368   Start Time   => 21:59:30                            :22:1
 12:47:21 STC 2368   KSDS Size    => 196608                ESDS CIS   => 4096
```

CONNECT:Direct statistics

Press F8 to scroll forward and F7 to scroll backward; press F11 to scroll right and F10 to scroll left

Note

The Commands panel is profiled to display write-to-operator (WTO) messages generated by the file transfer resource. For example, if you issue CMD against a CONNECT:Direct manager resource, the panel will update with any WTO messages generated by the CONNECT:Direct region for which the manager resource is defined.

Issuing UNIX Shell Commands to a Remote UNIX Host

You can issue UNIX shell commands from NetMaster for File Transfer to a UNIX host, as long as the host has a CDMGR resource defined in the region, and the Allow UNIX Shell Commands option within the NetMaster for File Transfer agent that is running on the target UNIX host, is enabled. To issue a UNIX shell command, proceed as follows:

Step 1. At the file transfer status monitor, locate the CDMGR resource for the desired UNIX host.

Step 2. Enter CMD beside the CDMGR resource for the desired host.

The Command Entry panel is displayed.

Step 3. On the Command Entry panel, type in the UNIX shell command you wish to issue, preceded by sys. For example, to issue the ps -ef command, enter **sys ps -ef**.

Note

UNIX shell commands are upper and lower case sensitive—be sure to use the exact command syntax. For these commands to be effective, you must enable the Allow UNIX Shell Commands option within the NetMaster for File Transfer agent that is running on the target UNIX host (see the *SOLVE:Operations for File Transfer Agent - CONNECT:Direct Installation and Administration Guide*).

Step 4. Press ENTER to send the command and view the command results.

Warning

It is possible to specify root (super-user) permission when setting the Allow UNIX Shell Commands option within the UNIX agent. Misuse of root privileges can result in serious disruptions to the UNIX system. Be sure to check with the appropriate UNIX system administrator for a complete explanation of the permissions available to you before issuing any commands.

Monitoring Your File Transfer Environment by Using the Graphical Monitor

The graphical monitor enables you to monitor file transfer resources by groups. For example, suppose you are transferring files for different organizations and you want to group these transfers by organization. You can group the transfers for each organization in a resource group and attach the group to an icon on a panel that can be displayed on the graphical monitor. The icons then enable you to monitor the file transfers by organization.

You create resource groups, icons, and icon panels from the Icon Administration menu. To access the menu, enter the **/GADMIN** shortcut. For information about how to create an icon panel, see the online help.

After you have created your icon panel, you can display it on the graphical monitor. To access the monitor, enter the **/GMON** shortcut. To display your panel, enter **PANEL** at the Command ===> prompt and select it from the displayed list. To make the panel your default, enter **PROFILE** and specify it in your user profile. For further information see the *Automation Services Common User Guide*.

14

Controlling the System Image

This chapter discusses the commands that authorized users can use from the status monitor to control a loaded system image.

This chapter contains the following topics:

- Changing the Global Operation Mode
- Loading a System Image
- Shutting Down the Resources in a Loaded System Image
- Restarting the Resources in a Loaded System Image

Changing the Global Operation Mode

The global operation mode determines the mode of operation for a loaded (active) system image. Your region can run in a global operation mode of AUTOMATED or MANUAL.

As the name global suggests, the control of all resources defined to a system image is limited by the setting of the global operation mode. For example, if the global operation mode is MANUAL and the operation mode of a resource is AUTOMATED, the resource can only run in the MANUAL operation mode. If the global mode is changed to AUTOMATED, then that resource will run in its assigned mode.

You can issue a GLOBAL command from the file transfer status monitor to set the global operation mode. For example, when you have finished testing a system image in a development system in the MANUAL operation mode, you might want to change the global operation mode to AUTOMATED. If you are experiencing severe problems in a production system, you might want to change the global operation mode from AUTOMATED to MANUAL.

To set the global operation mode to AUTOMATED or MANUAL, proceed as follows:

Step 1. At the file transfer status monitor, enter **GLOBAL** at the Command ===> prompt.

A Global Command Parameter Specification panel is displayed, as shown in Figure 14-1.

Figure 14-1. Global Command Parameter Specification Panel

```
SOLVPROD--- Automation Services : GLOBAL Command Parameter Specification ------
Command ===>

.- Global Command Parameter ---------------------------------------------------.
|                                                                               |
|  ACB Name ................. DECD1                                           |
|                                                                               |
|  Current SysName ........... FT1                                             |
|  Current Version ........... 0001                                            |
|                                                                               |
|  Current Automation Mode ... MANUAL                                           |
|                                                                               |
|  Global Automation Mode .... AUTOMATED (Automated or Manual)                  |
|                                                                               |
'-------------------------------------------------------------------------------'
```

Step 2. Enter **AUTOMATED** or **MANUAL** in the Global Automation Mode field and press F6 (Action).

A confirmation panel is displayed, as shown in Figure 14-2.

Figure 14-2. Confirming the Change to Global Operation Mode

```
SOLVPROD---------- Automation Services : Command Confirmation --------------FTI


OpSys    OS390                                                  Userid USER01
                                                                LU     NMMAF022
                                                                WED 20-JUN-2001
                                                                Time   17.17.00

WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING
WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING
***                                                                         ***
***     Command to Confirm .... GLOBAL                                      ***
***     SysName and Version ... FT1 0001                                    ***
***     User Supplied Parms ... MODE=AUTOMATED                              ***
***                                                                         ***
***     Enter CONFIRM to continue                                           ***
***     Enter CANCEL or press PF12 to terminate                             ***
***                                                                         ***
WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING
WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING

Response ... CONFIRM  ( CONFIRM / CANCEL )
 F1=Help      F2=Split
                          F9=Swap                              F12=Cancel
```

Warning

Changing the global operation mode affects all resources that are defined in the loaded system image. If you are changing the mode from MANUAL to AUTOMATED, you should ensure that all resources are defined correctly before making the change.

Step 3. Enter **CONFIRM** in the Response field.

You are returned to the monitor.

Loading a System Image

The region normally loads a user specified system image during region initialization. During operation, you may need to change the system image by loading another image (for example, if a newer image, which is defined as a separate image, needs to be used).

In a multisystem environment, if you are in a focal point region, you can change the image in a subordinate region.

To load the system image, proceed as follows:

Step 1. At the file transfer status monitor, enter **LOAD** at the Command ===> prompt.

The LOAD Command Parameter Specification panel is displayed. Figure 14-3 shows an example.

Step 2. Enter **?** in the SysName to be Loaded field, and select a system image from the displayed prompt list.

Step 3. Specify the global operation mode for your system image in the Global Automation Mode field.

Figure 14-3. Load Command Parameter Specification

```
SOLVPROD------ Automation Services : LOAD Command Parameter Specification -----
Command ===>

.- Load Command Parameters -------------------------------------------------.
|                                                                            |
|  ACB Name ................. SOLVEPROD                                    |
|  Current SysName .......... FT1                                            |
|  Current Version .......... 0001                                           |
|                                                                            |
|  SysName to be Loaded ....+ FT1_____                                       |
|  Version to be Loaded ....+ 0002                                           |
|  Global Automation Mode ... MANUAL___ (Automated or Manual)                |
|                                                                            |
|  Last Warm Start Date ........                                             |
|                  Time ........                                             |
|                  ACB Name ....                                             |
|                                                                            |
|  Checkpoint Restart Status ... ACTIVE                                      |
|  Perform COLD Start? ......... NO_                                         |
|                                                                            |
'----------------------------------------------------------------------------'

 F1=Help      F2=Split                                          F6=Action
                           F9=Swap                            F12=Cancel
```

Step 4. If the Checkpoint Restart Status field is set to ACTIVE, you can specify that a warm load be performed by entering NO in the Perform COLD Start? field. See the section, *Performing Cold and Warm Loads*, on page 14-5 for additional information about performing cold and warm loads.

Step 5. Press F6 (Action) to load the system image.

The Command Confirmation panel is displayed.

Step 6. Enter **CONFIRM** in the Response field, to confirm the system image load (see Figure 14-4).

Figure 14-4. Confirming the System Image Load

```
OpSys    OS390                                                Userid USERO1
Vtam Ver 4.8.0                                                LU     NMMAF043
Subarea  SYD1VTM1                                             MON 15-OCT-2001
                                                              Time   11.08.21

WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING
WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING
***                                                                         ***
***     Command to Confirm .... LOAD                                        ***
***     SysName and Version ... FTI 0001                                    ***
***     Parms : NEWSYS=COMP001 NEWVERS=0001 MODE=MANUAL WARM=YES            ***
***                                                                         ***
***     Enter CONFIRM to continue                                           ***
***     Enter CANCEL or press PF12 to terminate                             ***
***                                                                         ***
WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING
WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING

Response ... CONFIRM  ( CONFIRM / CANCEL )
```

Warning

Resources that are monitored by the region are defined to the system image. Loading a system image effects all users of this region.

The system image is loaded, and you are returned to the file transfer status monitor.

Performing Cold and Warm Loads

When you load a system image, you can specify that a cold or warm load be performed. This is dependent on the setting of the Checkpoint Restart Status field in the $RM AUTOIDS parameter group.

Key Concept

Cold and warm loads are described below:

Cold—when a cold load is performed, resources defined to the system image are checked, and if automated, are brought into the desired state. The system image is loaded as if this was the first time it was loaded.

Warm—when a warm load is performed, resources are placed in the state they were in when this system image was last in use. All manual overrides performed on resources defined to the system image are retained when this system image is loaded.

The Checkpoint Restart Status field displayed on the LOAD Command Parameter Specification panel, shown in Figure 14-3 on page 14-4, displays the status as specified in $RM AUTOIDS parameter group.

Shutting Down the Resources in a Loaded System Image

You can use the following commands to shut down the resource(s) defined to a loaded system image:

- SHUTSYS—shutdown of all resources with an operation mode of AUTOMATED
- SHUTFORCE—shutdown of all resources

Shutting Down Automated Resources

To shut down resources that are in an operation mode of AUTOMATED, proceed as follows:

Note

This procedure is only valid if the global operation mode is set to AUTOMATED.

Step 1. At the Command ===> prompt of the file transfer status monitor, enter **SHUTSYS**.

If the region is …	You …
Linked to other regions	Can perform SHUTSYS in other regions. The Execute SHUTSYS Command panel is displayed, listing the loaded system images in all linked regions. Enter **S** beside the system image you want to shut down.
Standalone	Perform SHUTSYS in the current region.

A Command Confirmation panel is displayed, as shown in Figure 14-5.

Figure 14-5. Confirming the Execution of the SHUTSYS Command

```
SOLVPROD------ Automation Services : Command Confirmation ------------------FT1


OpSys    MVSESA                                                 Userid USER01
                                                                LU     NMMAF056
                                                                MON 23-JUN-1997
                                                                Time   12.22.50

WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING
WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING
***                                                                         ***
***     Command to Confirm .... SHUTSYS                                     ***
***     SysName and Version ... FT1 0001                                    ***
***                                                                         ***
***                                                                         ***
***     Enter CONFIRM to continue                                           ***
***     Enter CANCEL or press PF12 to terminate                             ***
***                                                                         ***
WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING
WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING WARNING

Response ... _______  ( CONFIRM / CANCEL )
 F1=Help      F2=Split
                          F9=Swap                              F12=Cancel
```

Warning

Issuing the SHUTSYS command shuts down all resources that are in the AUTOMATED mode.

Step 2. Enter **CONFIRM** in the Response field.

All automated resources defined to the system image are shut down.

Shutting Down a Manual Resource

To shut down resources that are in the MANUAL operation mode, do one of the following:

- Enter **MA** beside the resource to change its operation mode from MANUAL to AUTOMATED before issuing the SHUTSYS command.
- Enter **T** adjacent to the resource to stop it manually.

Shutting Down All Resources

To shut down all resources in a system image, proceed as follows:

Note

This command is only valid if the global operation mode is set to AUTOMATED.

Step 1. At the Command ===> prompt of the file transfer status monitor, enter **SHUTFORCE**.

If the region is …	**You …**
Linked to other regions	Can perform SHUTFORCE in other regions. The Execute SHUTFORCE Command panel is displayed, listing the loaded system images in all linked regions. Enter **S** beside the system image you want to shut down.
Standalone	Perform SHUTFORCE in the current region.

A Command Confirmation panel is displayed.

Step 2. Enter **CONFIRM** in the Response field.

All resources defined to the system image are shut down.

Restarting the Resources in a Loaded System Image

To restart resources defined to a loaded system image that were shut down using the SHUTSYS or SHUTFORCE commands, proceed as follows:

Step 1. At the Command ===> prompt of the file transfer status monitor, enter **STARTSYS**.

If the region i …	**You …**
Linked to other regions	Can perform STARTSYS in other regions. The Execute STARTSYS Command panel is displayed, listing the loaded system images in all linked regions. Enter **S** beside the system image you want to restart.
Standalone	Perform STARTSYS in the current region.

A confirmation panel is displayed.

Step 2. Enter **CONFIRM** in the response field.

15

Customizing the Environment That Manages File Transfer Resources

In Chapter 10, *Building the Environment to Manage Your File Transfer Services*, you built the environment to manage your file transfer services. You used templates to define some of the resources you want to manage. This chapter describes how you can add your own customization to these resource definitions.

This chapter contains the following topics:

- Customizing CA-XCOM Monitor Criteria
- Customizing CONNECT:Direct Monitor Criteria
- Customizing CONNECT:Mailbox Monitor Criteria
- Customizing FTS Monitor Criteria
- Customizing FTP Monitor Criteria
- Specifying the Availability of Supporting File Transfer Resources
- Raising a Problem Ticket
- Using Processes to Perform Complex Operations
- Customizing the Manager Resource Definition
- Customizing Monitor Resource Definitions
- Customizing the Supporting Resource Definition

Customizing CA-XCOM Monitor Criteria

You can customize CA-XCOM monitor (XCMON) resource definitions to suit your requirements. This section describes how to customize the monitoring criteria for:

- Heartbeat interval
- Transfer requests
- Stalled transfers
- TCP/IP connections
- Remote nodes

Customizing How Often the Monitor Status Is Updated

The status update frequencies are set by the heartbeat interval. For transfer request monitors, the update frequency is determined by the owning manager. Other monitors have their own individual update frequencies.

Customizing the Heartbeat Intervals of Transfer Request Monitors

To customize how often the transfer request monitor status is updated, proceed as follows:

Step 1. At the file transfer status monitor, enter **DB** beside the XCMGR resource.

Step 2. On the displayed list of panels, enter **S** beside the Monitor Details panel.

The Monitor Details panel is displayed, as shown in Figure 15-1.

Figure 15-1. Customizing the Heartbeat Criterion of CA-XCOM Transfer Request Monitors

```
 . Heartbeat Details -------------------------------------------------------.
 |                                                                          |
 | Active Transfer Request Monitors                                         |
 | Heartbeat Interval ..... 00.05.00                                        |
 |                                                                          |
 | Inactive Transfer Request Monitors (Suspended, Held, and Inactive)       |
 | Heartbeat Interval ..... 00.05.00                                        |
```

Step 3. Update the interval time in the Heartbeat Interval fields.

The format is *hh.mm.ss*, where:

- *hh* is the interval time in hours and is in the range 0 through 24
- *mm* is the interval time in minutes and is in the range 0 through 59
- *ss* is the interval time in seconds and is in the range 0 through 59

For example, 00.02.00 means that the status is updated every two minutes.

Note

The minimum value allowed is one minute (00.01.00).

Step 4. With the heartbeat intervals specified, press F3 (File).

The change is filed, and you are returned to the file transfer status monitor. The new heartbeat interval is now in effect for the resource.

Customizing the Heartbeat Interval of Other Monitors

To customize how often the status of the other CA-XCOM monitors is updated, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside the required XCMON resource.

The Monitor Details panel is displayed.

Step 2. Update the interval time in the Heartbeat Interval field.

Step 3. With the heartbeat interval specified, press F3 (File).

The change is filed, and you are returned to the file transfer status monitor. The new heartbeat interval is now in effect for the resource.

Customizing Criteria for Monitoring CA-XCOM Transfer Requests

To customize criteria for a CA-XCOM transfer request monitor, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside a transfer request XCMON-class resource.

The Monitor Details panel is displayed, as shown in Figure 15-2.

Figure 15-2. CA-XCOM Transfer Request Monitor Details

```
.- Transfer Request Monitor Details ----------------------------------------.
|    Transfer Request Status.....+ ACTIVE___                                |
|    Transfer Request Threshold.... 100_                                    |
|                                                                           |
|    Transfer Request ID ............. __________                          |
|                        ............. __________                          |
|                        ............. __________                          |
|                        ............. __________                          |
|                        ............. __________                          |
|    Remote Server                                                          |
| (TCP/IP Host Name/Addr or LU Name) .. ______________________________      |
|                    ................. ______________________________      |
|                    ................. ______________________________      |
|                    ................. ______________________________      |
|                    ................. ______________________________      |
```

Step 2. You can customize the fields displayed in the Transfer Request Monitor Details window of the Monitor Details panel as follows:

If you want to change the …	Then enter …
Criteria to monitor requests with a different status	**?** in the Transfer Request Status field and select from the displayed values.
Request threshold	The new threshold value in the Transfer Request Threshold field.
Monitored CA-XCOM transfer IDs	The IDs in the Transfer Request ID fields. If you do not want to restrict the monitored IDs, leave the fields blank.
Monitored remote CA-XCOM server	The TCP/IP host name or address, or the LU name of the remote node in the Remote Server fields. If you do not want to restrict the monitored nodes, leave the fields blank.

Step 3. Press F3 (File) to file the changes and return to the file transfer status monitor.

The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customizing the Criteria for Monitoring Stalled CA-XCOM Transfers

To customize the criteria for a CA-XCOM stalled transfer monitor, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside a stalled transfer XCMON-class resource.

A Monitor Details panel is displayed, as shown in Figure 15-3.

Figure 15-3. CA-XCOM Stalled Transfer Monitor Details

```
     Heartbeat Interval ...... 00.05.00  (hh.mm.ss)

.- Stalled Monitor -------------------------------------------------------.
|    Stalled Time to Alert ...... 00.30.00    (hh.mm.ss)
|    Stalled Time to Terminate .. ________    (hh.mm.ss)
|                                                                          |
|                                                                          |
|    Transfer Request ID ............. __________                         |
|                        ............. __________                         |
|                        ............. __________                         |
|                        ............. __________                         |
|                        ............. __________                         |
|    Remote Server                                                         |
| (TCP/IP Host Name/Addr or LU Name) .. ______________________________     |
|                    .................. ______________________________     |
|                    .................. ______________________________     |
|                    .................. ______________________________     |
|                    .................. ______________________________     |
```

Step 2. You can customize the fields displayed in the Stalled Monitor Details window of the Monitor Details panel as follows:

If you want to change …	Then enter …
The time a transfer in progress can be idle before an alert is raised	The new value in the Stalled Time to Alert field.
The time a transfer in progress can remain idle before it is terminated	A new value in the Stalled Time to Terminate field.
Monitored CA-XCOM transfer IDs	The IDs in the Transfer Request ID fields. If you do not want to restrict the monitored IDs, leave the fields blank.
Monitored remote CA-XCOM server	The TCP/IP host name or address, or the LU name of the remote node in the Remote Server fields. If you do not want to restrict the monitored nodes, leave the fields blank.

Step 3. Press F3 (File) to file any changes and return to the file transfer status monitor.

The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customizing the Criteria for Monitoring CA-XCOM TCP/IP Connections

To customize the criteria for a CA-XCOM TCP/IP connections monitor, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside a TCP/IP connections XCMON-class resource.

A Monitor Details panel is displayed, as shown in Figure 15-4.

Figure 15-4. CA-XCOM TCP/IP Connection Monitor Details

```
     Heartbeat Interval ...... 00.05.00  (hh.mm.ss)

.- TCP/IP Connection Monitor Details ----------------------------------------.
|    Idle Time to Alert ...... 00.30.00 (hh.mm.ss)                           |
|    Idle Time to Drop ....... ________ (hh.mm.ss)                           |
```

Step 2. You can customize the two fields displayed in the TCP/IP Connection Monitor Details window of the Monitor Details panel as follows:

If you want to change the …	**Then enter …**
Time a TCP/IP connection can be idle before an alert is raised	The new value in the Idle Time to Alert field.
Time a connection can remain idle before it is dropped	A new value in the Idle Time to Drop field.

Step 3. Press F3 (File) to file any changes and return to the file transfer status monitor.

The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customizing the Criteria for Monitoring a CA-XCOM Remote Node

To customize the criteria for a CA-XCOM remote node monitor, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside a remote node XCMON-class resource.

A Monitor Details panel is displayed, as shown in Figure 15-5.

Figure 15-5. CA-XCOM Remote Node Monitor Details

```
Heartbeat Interval ...... 00.05.00  (hh.mm.ss)

.- Remote Node Monitor Details ---------------------------------------------.
|                                                                            |
|    Remote Node LU Name  ............. LU0001__                           |
|   (To check SNA Connectivity)                                              |
|                                                                            |
|                                                                            |
|                                                                            |
|    Remote Node TCP/IP Host Name/Addr.. ____________________________________ |
|   (To check IP Connectivity)                                               |
```

Step 2. You can change the remote file transfer partner node that you want to monitor.

Step 3. Press F3 (File) to file any changes and return to the file transfer status monitor.

The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customizing CONNECT:Direct Monitor Criteria

You can customize CONNECT:Direct monitor (CDMON) resource definitions to suit your requirements. This section describes how to customize the monitoring criteria for:

- Heartbeat interval
- Queues
- Transfers
- Listener tasks (for CONNECT:Direct applications on distributed systems)
- TCP/IP connections
- Remote nodes

Customizing How Often the Monitor Status Is Updated

To customize how often the monitor status is updated, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside the CDMON resource.

The Monitor Details panel is displayed, as shown in Figure 15-6.

Figure 15-6. Customizing the Heartbeat Criterion of a CONNECT:Direct Monitor

```
-------- Automation Services : CDMON DECD1.PSHOLDWC Monitor Details -----------
Command ===>                                                   Function=UPDATE

  Heartbeat Interval ......... 00.30.00
```

Step 2. Update the interval time in the Heartbeat Interval field.

The format is *hh.mm.ss*, where:

- *hh* is the interval time in hours and is in the range 0 through 24
- *mm* is the interval time in minutes and is in the range 0 through 59
- *ss* is the interval time in seconds and is in the range 0 through 59

For example, 00.02.00 means that the command is issued every two minutes.

Note

The minimum value allowed is one minute (00.01.00).

Step 3. With the heartbeat interval specified, press F3 (File).

The change is filed, and you are returned to the file transfer status monitor. The new heartbeat interval is now in effect for the resource.

Customizing Criteria for Monitoring CONNECT:Direct Queues

To customize criteria for a CONNECT:Direct process queue or process status monitor, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside a process queue or status CDMON resource.

The Monitor Details panel is displayed, as shown in Figure 15-7.

Figure 15-7. Process Queue or Status Monitor Details

```
-------- Automation Services : CDMON DECD1.PSHOLDWC Monitor Details -----------
Command ===>                                                     Function=UPDATE

  Heartbeat Interval ......... 00.30.00

. Queue Monitor Details -------------------------------------------------------.
|    Queue Type ............... HOLD_                                         |
|    Queue Depth Threshold ... 10__                                           |
|    Process Status .........+ WC___                                          |
|    Destination Node(s) ..... _______________                                |
|                         ..... _______________                               |
|                         ..... _______________                               |
|                         ..... _______________                               |
|                         ..... _______________                               |
|    Process Name(s) ......... ________                                       |
L - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Step 2. You can customize the fields displayed in the Queue Monitor Details window of the Monitor Details panel as follows:

If you want to change the …	**Then enter …**
Monitor queue type	One of the following in the Queue Type field: • ACTIVE • BAD • CALL • EXEC • HOLD • INITIAL • RETAIN • START • SUSPEND • TIMER • WAIT • X-R&T
Queue threshold	The new threshold value in the Queue Depth Threshold field.
Process status monitored by this resource	**?** at the Process Status field and select from the displayed prompt list.
Monitored CONNECT:Direct destination nodes	The node names in the Destination Node(s) fields.
Monitored CONNECT:Direct processes	The process names in the Process Name(s) fields.

Step 3. Press F3 (File) to file the changes and return to the file transfer status monitor.

The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customizing the Criteria for Monitoring CONNECT:Direct Transfers

To customize the criteria for a CONNECT:Direct transfer monitor, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside a transfer CDMON resource.

A Monitor Details panel is displayed, as shown in Figure 15-8.

Figure 15-8. CONNECT:Direct Transfer Monitor Details

```
-------- Automation Services : CDMON DECD1.TRANSFER Monitor Details -----------
Command ===>                                                   Function=UPDATE

     Heartbeat Interval ...... 00.05.00     (hh.mm.ss)

.- File Transfer Monitor Details ---------------------------------------------.
|    Stalled Time to Alert ... 00.30.00     (hh.mm.ss)                        |
|    Stalled Time to Flush ... 01.00.00     (hh.mm.ss)                        |
|                                                                             |
|    Destination Node(s) ..... ________________                               |
|                        ..... ________________                               |
|                        ..... ________________                               |
|                        ..... ________________                               |
|                        ..... ________________                               |
|    Process Name(s) ......... ________                                       |
|                    ......... ________                                       |
|                    ......... ________                                       |
|                    ......... ________                                       |
|                    ......... ________                                       |
'-----------------------------------------------------------------------------'
```

Step 2. You can customize the fields displayed in the File Transfer Monitor Details window of the Monitor Details panel as follows:

If you want to change …	**Then enter …**
The time an executing process can be idle before an alert is raised	The new value in the Stalled Time to Alert field.
The time an executing process can remain idle before it is flushed	A new value in the Stalled Time to Flush field.
Monitored CONNECT:Direct destination nodes	The node names in the Destination Node(s) fields.
Monitored CONNECT:Direct processes	The process names in the Process Name(s) fields.

Step 3. Press F3 (File) to file any changes and return to the file transfer status monitor.

The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customizing the Criteria for Monitoring a CONNECT:Direct TCP/IP Listener Task

These criteria are required for CONNECT:Direct applications on distributed systems only. To specify the criteria, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside a listener task CDMON resource.

A Monitor Details panel is displayed, as shown in Figure 15-9.

Figure 15-9. CONNECT:Direct TCP/IP Listener Monitor Details

```
-------- Automation Services : CDMON DECD1.IPLISTNR Monitor Details -----------
Command ===>                                                   Function=UPDATE

  Heartbeat Interval ......... 00.30.00

.- TCP/IP Listener Task Monitor Details -------------------------------------.
|    Retry Attempts .......... 2_                                            |
|    Retry Interval .......... 5_           (Seconds Between Retry Attempts)  |
|    CONNECT:Direct Port No .. _____                                         |
|    SNMP Community Name ..... ______________________________________________ |
`_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _'
```

Step 2. You can customize the fields displayed in the TCP/IP Listener Monitor Details window of the Monitor Details panel as follows:

If you want to change the …	**Then enter …**
Number of times this monitor tries to find the listener task	A new value in the Retry Attempt field.
Time interval between retry attempts	A new value in the Retry Interval field.
TCP/IP details to reflect changes to the monitored CONNECT:Direct application	New values in the CONNECT:Direct Port No and SNMP Community Name fields.

Step 3. Press F3 (File) to file any changes and return to the file transfer status monitor.

The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customizing the Criteria for Monitoring CONNECT:Direct TCP/IP Connections

To customize the criteria for a CONNECT:Direct TCP/IP connections monitor, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside a TCP/IP connections CDMON resource.

A Monitor Details panel is displayed, as shown in Figure 15-10.

Figure 15-10. CONNECT:Direct TCP/IP Connection Monitor Details

```
---------- Automation Services : CDMON DECD1.CONNECT Monitor Details ----------
Command ===>                                                   Function=UPDATE

     Heartbeat Interval ...... 00.05.00     (hh.mm.ss)

.- TCP/IP Connection Monitor Details ----------------------------------------.
|    Idle Time to Alert ...... 00.30.00   (hh.mm.ss)                         |
|    Idle Time to Drop ....... 01.00.00   (hh.mm.ss)                         |
'---------------------------------------------------------------------------'
```

Step 2. You can customize the two fields displayed in the TCP/IP Connection Monitor Details window of the Monitor Details panel as follows:

Note

If the connections are established by using TCPaccess, you cannot drop a connection automatically by using an idle time limit.

If you want to change the …	Then enter …
Time a TCP/IP connection can be idle before an alert is raised	The new value in the Idle Time to Alert field.
Time a connection can remain idle before it is dropped	A new value in the Idle Time to Drop field.

Step 3. Press F3 (File) to file any changes and return to the file transfer status monitor.

The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customizing the Criteria for Monitoring a CONNECT:Direct Remote Node

To customize the criteria for a CONNECT:Direct remote node monitor, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside a remote node CDMON resource.

A Monitor Details panel is displayed, as shown in Figure 15-11.

Figure 15-11. CONNECT:Direct Remote Node Monitor Details

```
------------ Automation Services : CDMON DECD1.PING Monitor Details -----------
Command ===>                                                   Function=UPDATE

     Heartbeat Interval ...... 00.05.00     (hh.mm.ss)

.- Remote Node Monitor Details ----------------------------------------------.
|                                                                            |
|    Remote Node Name ........ ALUNIXCD1_______                              |
|                                                                            |
'----------------------------------------------------------------------------'
```

Step 2. You can change the remote file transfer partner that you want to monitor.

Step 3. Press F3 (File) to file any changes and return to the file transfer status monitor.

The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customizing CONNECT:Mailbox Monitor Criteria

You can customize CONNECT:Mailbox monitor (CMMON) resource definitions to suit your requirements. This section describes how to customize the monitoring criteria for:

- Heartbeat interval
- Auto Connect queue
- BSC lines
- SNA sessions

Customizing How Often the Monitor Status Is Updated

To customize how often the monitor status is updated, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside the CMMON resource.

The Monitor Details panel is displayed, as shown in Figure 15-12.

Figure 15-12. Customizing the Heartbeat Criterion of a CONNECT:Mailbox Monitor

```
----------- Automation Services : CMMON DECM1.ACQ Monitor Details -------------
Command ===>                                                   Function=UPDATE

     Heartbeat Interval ...... 00.30.00     (hh.mm.ss)
```

Step 2. Update the interval time in the Heartbeat Interval field.

The format is *hh.mm.ss*, where:

- *hh* is the interval time in hours and is in the range 0 through 24
- *mm* is the interval time in minutes and is in the range 0 through 59
- *ss* is the interval time in seconds and is in the range 0 through 59

For example, 00.02.00 means that the command is issued every two minutes.

Note

The minimum value allowed is one minute (00.01.00).

Step 3. With the heartbeat interval specified, press F3 (File).

The change is filed, and you are returned to the file transfer status monitor. The new heartbeat interval is now in effect for the resource.

Customizing the Criteria for Monitoring Auto Connect Queues

To customize criteria for an Auto Connect Queue monitor, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside an Auto Connect Queue CMMON resource.

The Monitor Details panel is displayed (see Figure 15-13).

Figure 15-13. Auto Connect Queue Monitor Details

```
----------- Automation Services : CMMON DECM1.ACQ Monitor Details -------------
Command ===>                                                     Function=UPDATE

     Heartbeat Interval ...... 00.05.00     (hh.mm.ss)

.- Auto Connect Queue Monitor Details ----------------------------------------.
|    Queue Depth Threshold.... 0_______                                        |
|    List Name(s)............ ________                                        |
|                ............ ________                                        |
|                ............ ________                                        |
|                ............ ________                                        |
|                ............ ________                                        |
'------------------------------------------------------------------------------'
```

Step 2. You can customize the fields as follows:

If you want to change the …	**Then enter the …**
Queue threshold	New threshold value in the Queue Depth Threshold field.
Monitored CONNECT:Mailbox Auto Connect list names	List names in the List Name(s) fields.

Step 3. Press F3 (File) to save the changes and return to the file transfer status monitor.

Customizing the Criteria for Monitoring BSC Lines

To customize criteria for a BSC line monitor, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside a BSC line CMMON resource.

The Monitor Details panel is displayed (see Figure 15-14).

Figure 15-14. BSC Line Monitor Details

```
--------- Automation Services : CMMON DECM1.BSCLINE Monitor Details -----------
Command ===>                                                   Function=UPDATE

     Heartbeat Interval ...... 00.05.00     (hh.mm.ss)

.- BSC Line Details -------------------------------------------------------.
|    Queue Depth Threshold ... 0                                            |
|    Automatic Restart?....... NO           (YES/NO)                        |
|                                                                           |
|    Line Name(s) ............ ________                                    |
|                 ............ ________                                    |
|                 ............ ________                                    |
|                 ............ ________                                    |
`- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -'
```

Step 2. You can customize the fields as follows:

If you want to change …	**Then enter …**
Whether a BSC line is automatically restarted	YES or NO in the Automatic Restart? field.
The monitored BSC lines	The line names in the Line Name(s) fields.

Step 3. Press F3 (File) to save the changes and return to the file transfer status monitor.

Customizing the Criteria for Monitoring SNA Sessions

To customize criteria for an SNA session monitor, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside an SNA session CMMON resource.

The Monitor Details panel is displayed (see Figure 15-15).

Figure 15-15. SNA Session Monitor Details

```
--------- Automation Services : CMMON DECM1.SNASESS Monitor Details -----------
Command ===>                                                     Function=UPDATE

     Heartbeat Interval ...... 00.05.00     (hh.mm.ss)

.- SNA Session Monitor Details ---------------------------------------------.
|    Stalled Time to Alert ... 00.02.00     (hh.mm.ss)                      |
|                                                                           |
|    Remote Name(s) .......... ________                                     |
|                   .......... ________                                     |
|                   .......... ________                                     |
|                   .......... ________                                     |
|                   .......... ________                                     |
```

Step 2. You can customize the fields as follows:

If you want to change the …	Then enter the …
Amount of time an SNA session remains idle before an alert is raised	New value in the Stalled Time to Alert field.
Remote site sessions to be monitored	Remote site names in the Remote Name(s) fields.

Step 3. Press F3 (File) to save the changes and return to the file transfer status monitor.

Customizing FTS Monitor Criteria

You use FTSMON class resources to monitor the links between FTS regions. You can customize how often a monitor resource checks the status of a link. Proceed as follows:

Step 1. At the file transfer status monitor, enter **DB** beside the FTSMON resource.

A ResourceView : Panel Display List panel is displayed, as shown in Figure 15-16.

Figure 15-16. Customizing the Heartbeat Criterion of an FTS Monitor

```
SOLVPROD-------------- ResourceView : Panel Display List ----------------------
Command ===>                                                   Scroll ===> PAGE

                                      Use 'S' to select panel(s) to be displayed
    Panel Description
    FTS File Transfer Monitor General Description
S   FTSMON CAFTS1.CAAR Monitor Details
    FTSMON CAFTS1.CAAR Status Monitor Message Details
    FTSMON CAFTS1.CAAR State Change Exits
    FTSMON CAFTS1.CAAR Automation Log Details
    FTSMON CAFTS1.CAAR Owner Details
    FTSMON CAFTS1.CAAR Extended Function Exit
    **END**
```

Step 2. Enter **S** beside the listed Monitor Details panel to display it. Figure 15-17 shows an example.

This panel identifies the link being monitored and displays the heartbeat interval that determines how often the link status is checked.

Figure 15-17. Monitor Details Panel—FTSMON Class Resource

```
SOLVPROD----- ResourceView : FTSMON CAFTS1.CAAR Monitor Details -------FT1-0001
Command ===>                                                    Function=UPDATE



. Link Monitor Details -------------------------------------------------------.
|                                                                              |
|    Link Name  ............... CAAR________                                 |
|                                                                              |
|    Heartbeat Interval ...... 00.05.00                                        |
|                                                                              |
'------------------------------------------------------------------------------'
```

Step 3. Enter an interval time in the Heartbeat Interval field.

The format is *hh.mm.ss*, where:

- *hh* is the interval time in hours and is in the range 0 through 24
- *mm* is the interval time in minutes and is in the range 0 through 59
- *ss* is the interval time in seconds and is in the range 0 through 59

For example, 00.02.00 means that the status of the specified link is checked every two minutes.

Note

The minimum value allowed is one minute (00.01.00).

Step 4. With the heartbeat interval specified, press F3 (File).

The change is filed, and you are returned to the file transfer status monitor. The new heartbeat interval is now in effect for the resource.

Customizing FTP Monitor Criteria

You can customize FTP monitor (FTPMON) resource definitions to suit your requirements. This section describes how to customize the monitoring criteria for:

- Heartbeat interval
- TCP/IP connections
- Remote nodes

Customizing How Often the Monitor Status is Updated

To customize how often the monitor status is updated, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside the FTPMON resource.

The Monitor Details panel is displayed, as shown in Figure 15-18.

Figure 15-18. Customizing the Heartbeat Criterion of an FTP Monitor

```
-------- Automation Services : FTPMON FTPSVR.TCPCON Monitor Details -----------
Command ===>                                                   Function=UPDATE

  Heartbeat Interval ......... 00.30.00
```

Step 2. Update the interval time in the Heartbeat Interval field.

The format is *hh.mm.ss*, where:

- *hh* is the interval time in hours and is in the range 0 through 24
- *mm* is the interval time in minutes and is in the range 0 through 59
- *ss* is the interval time in seconds and is in the range 0 through 59

For example, 00.02.00 means that the command is issued every two minutes.

Note

The minimum value allowed is one minute (00.01.00).

Step 3. With the heartbeat interval specified, press F3 (File).

The change is filed, and you are returned to the file transfer status monitor. The new heartbeat interval is now in effect for the resource.

Customizing the Criteria for Monitoring FTP TCP/IP Connections

To customize the criteria for an FTP TCP/IP connections monitor, proceed as follows:

Note

FTPMON monitors FTP data connections only. It does not monitor FTP control connections, but you can view them by using the D command from the status monitor.

Step 1. At the file transfer status monitor, enter **U** beside a TCP/IP connections FTPMON resource.

A Monitor Details panel is displayed, as shown in Figure 15-19.

Figure 15-19. FTP TCP/IP Connection Monitor Details

```
. TCP/IP Connection Monitor Details ----------------------------------------.
|   Idle Time to Alert ...... 00.02.00  (hh.mm.ss)                          |
|   Idle Time to Drop .......           (hh.mm.ss)                          |
'---------------------------------------------------------------------------'
```

Step 2. You can customize the two fields displayed in the TCP/IP Connection Monitor Details window of the Monitor Details panel as follows:

If you want to change the …	**Then enter …**
Time a TCP/IP connection can be idle before an alert is raised	The new value in the Idle Time to Alert field.
Time a connection can remain idle before it is dropped	A new value in the Idle Time to Drop field.

Step 3. Press F3 (File) to file any changes and return to the file transfer status monitor.

The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customizing the Criteria for Monitoring an FTP Remote Node

To customize the criteria for an FTP remote node monitor, proceed as follows:

Step 1. At the file transfer status monitor, enter **U** beside a remote node FTPMON resource.

A Monitor Details panel is displayed, as shown in Figure 15-20.

Figure 15-20. FTP Remote Node Monitor Details

```
---------- Automation Services : FTPMON FTPSVR.PING Monitor Details -----------
Command ===>                                                   Function=UPDATE

     Heartbeat Interval ...... 00.05.00     (hh.mm.ss)

.- Remote Node Details -------------------------------------------------------.
|                                                                              |
|  TCP/IP Host Name/Addr ..... ______________________________________________ |
|  TCP/IP Port Number ........ 21___                                           |
|  Time Out After ........... 300                                              |
```

Step 2. You can customize the fields displayed in the Remote Node Details window of the Monitor Details panel as follows:

If you want to …	**Then enter …**
Monitor the availability of a different remote FTP server	The new values in the TCP/IP Host Name/Addr and TCP/IP Port Number fields.
Change the number of seconds to wait for the status of the remote node to be resolved	A new value in the Time Out After field.

Step 3. Press F3 (File) to file any changes and return to the file transfer status monitor.

The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Specifying the Availability of Supporting File Transfer Resources

Each resource that supports your file transfers (for example, CONNECT:Direct manager or DASD) has an availability map. This map can be customized by you to specify the automation of the resource.

Note

The availability map only activates or inactivates the resource if your resource operation mode is set to AUTOMATED and the global operation mode is also set to AUTOMATED. See the section, *Changing the Global Operation Mode*, on page 14-2, for information about setting the global operation mode.

Key Concept

A manager resource (for example, a CONNECT:Direct manager) is an owning resource. The availability of the manager resource determines the availability of its owned resources.

Displaying the Availability Map

To display the availability map, proceed as follows:

Step 1. From any panel, enter **/RADMIN.R**.

Note

The /RADMIN.R path provides a different way of accessing your resource definitions. You do not need to access the status monitor first.

The ResourceView : Resource Definition panel is displayed. You can change the displayed system image or accept the default. The last specified system image is the default system image (see Figure 15-21).

Figure 15-21. Resource Definition

```
SOLVPROD------------ ResourceView : Resource Definition -----------------------
Command ===>                                                   Scroll ===> PAGE

. System Image ------------------------------------------------------------------.
| System Name ...+ FT1_____     Version ...+ 0001                                |
'-------------------------------------------------------------------------------'
. Resource Classes --------------------------------------------------------------.
|                                       Use 'S' to Select Resource Class        |
|     Class    Description                                                      |
|     CDMGR    C:D File Transfer Manager                                        |
|     CDMON    C:D File Transfer Monitor                                        |
|     CMMGR    C:Mailbox Manager                                                |
|     CMMON    C:Mailbox Monitor                                                |
|     DASD     Direct Access Device                                             |
|     FTPMGR   FTP Server Manager                                               |
|     FTPMON   FTP Server Monitor                                               |
|     FTSCHD   File Transfer Schedule                                           |
|     FTSMGR   FTS File Transfer Manager                                        |
|     FTSMON   FTS File Transfer Monitor                                        |
|     INTNL    SOLVE:Operations Internal                                        |
|     STC      Started Task                                                     |
|     TAPE     Tape or Cartridge                                                |
|  F1=Help     F2=Split    F3=Exit     F4=Return               F6=Refresh     |
|  F7=Backward F8=Forward  F9=Swap                                              |
'-------------------------------------------------------------------------------'
```

You can change the system name and version number.

Step 2. Enter **S** beside the required resource class.

The resource list panel is displayed. This panel lists the resources defined to the specified system image.

Step 3. Enter **U** beside the resource for which you wish to define an availability map.

A list of the panels in the resource definition is displayed, as shown in Figure 15-22.

Note

You can also access the list of panels by issuing the DB command against the resource from the file transfer status monitor.

Figure 15-22. Specifying the Availability of a Resource

```
SOLVPROD------------- ResourceView : Panel Display List ---------------------
Command ===>                                                   Scroll ===> PAGE

                                      Use 'S' to select panel(s) to be displayed
    Panel Description
    C:D File Transfer Manager General Description
    CDMGR DECD1 Availability Map
    CDMGR DECD1 Activation Details
    CDMGR DECD1 Inactivation Details
    CDMGR DECD1 Force Inactivation Details
    CDMGR DECD1 Display and Heartbeat Details
    CDMGR DECD1 Status Monitor Message Details
    CDMGR DECD1 State Change Exits
    CDMGR DECD1 Automation Log Details
    CDMGR DECD1 Owner Details
    CDMGR DECD1 Extended Function Exit
    **END**
```

Step 4. Enter **S** beside the listed Availability Map panel.

The Availability Map panel is displayed, as shown in Figure 15-23.

Figure 15-23. Availability Map

```
SOLVPROD-------- ResourceView : CDMGR DECD1 Availability Map ----------FT1-0001
Command ===>                                                   Function=UPDATE

.- Map Details -------------------------------------------------------------.
| Map Name .....+ ____________                        Expire Delete ...       |
| Description ...                                                             |
| Timer Execution Control System .........+ N/A      (Service/Shared Images)  |
| Attached Resources ...+ _                                                   |
'-----------------------------------------------------------------------------'
.- Timer Details -----------------------------------------------------------.
|                                                                             |
|     Day Date        Time     SVC/Resource Name  Des.State Mode       Status |
|                                                                             |
|                                                                             |
```

Specifying Map Details

To specify availability map details, proceed as follows:

Step 1. At the Availability Map panel, enter a map name in the Map Name field.

Note

The map name identifies the map. After an availability map is created, it can be used by other resource definitions in the same system image.

Step 2. Press F10 (EditMap) to edit the map.

The availability map is displayed with an updated Description field, as shown in Figure 15-24.

Figure 15-24. Creating an Availability Map

```
SOLVPROD-------- ResourceView : CDMGR DECD1 Availability Map ----------FT1-0001
Command ===>                                                   Scroll ===> PAGE

. Map Details ---------------------------------------------------------------.
| Map Name ...... FIRST                                Expire Delete ... NO    |
| Description ... Availability Map for DECD1                                   |
| Timer Execution Control System .........+ N/A      (Service/Shared Images)  |
| Attached Resources ..                                                        |
'------------------------------------------------------------------------------'
. Timer Details -------------------------------------------------------------.
|                                                 D=Delete I=Insert R=Repeat |
```

Step 3. You can set the Expire Delete field to YES to delete timers when they expire or NO to retain all expired timers.

Key Concept

Timers are the items listed in the Timer Details window. These items specify the desired state of the resource on specified times.

Step 4. You may update the Description field, or accept the default.

Step 5. To display a list of attached resources, enter **?** in the Attached Resources field.

A list of resource definitions using this availability map is displayed.

Specifying Timer Details

To specify timer details, proceed as follows:

Step 1. At the Availability Map panel, enter the timer details in the Timer Details window.

See the online help for an explanation of the displayed fields.

Step 2. Press F3 (OK) to confirm that you have completed specifying timer details.

Step 3. Press F3 (File) to file the updated definition.

You are returned to the resource list. If the operation mode of the resource is AUTOMATED, the resource will be controlled by your NetMaster for File Transfer region as specified in the availability map.

Timer Details—Example

Figure 15-25 shows a completed availability map. For this map, the desired state of the resource(s) is as follows:

- ACTIVE from 0800 hours to 1900 hours every Monday
- INACTIVE from 1900 hours every Monday to 0800 hours every Tuesday
- ACTIVE from 0800 hours every Tuesday to 1200 hours every Sunday
- INACTIVE from 1200 hours every Sunday to 0800 hours every Monday

Figure 15-25. Completed Timer Details Window

```
.- Timer Details -----------------------------------------------------------.
|                                                                           |
|     Day Date        Time     SVC/Resource Name  Des.State Mode       Status |
|     MON             08.00.00                    ACTIVE               ON     |
|     MON             19.00.00                    INACTIVE             ON     |
|     TUE             08.00.00                    ACTIVE               ON     |
|     SUN             12.00.00                    INACTIVE             ON     |
|                                                                           |
|                                                                           |
|                                                                           |
|                                                                           |
|                                                                           |
'---------------------------------------------------------------------------'
 F1=Help      F2=Split     F3=File      F4=Save      F5=Related
```

See the online help for additional information about specifying timer details.

Raising a Problem Ticket

NetMaster for File Transfer allows you to record problems in a problem management application for a defined resource.

To achieve this, NetMaster for File Transfer provides the PROBSOLV process. This process invokes a procedure which raises a problem ticket to a SOLVE:Problem application. For further information, see *Task 10—Implementing a SOLVE:Problem Automatic Problem Recording Environment*, on page 5-54.

This process enables you to record problems as they occur, and is associated with the resource in the resource definition.

You can specify the process in either of the following resource definition panels:

- State Change Exits panel—specify the exit in this panel if you want a problem ticket to be raised based on a change in the resource state.
- Define Event Exits panel of a message rule—specify the exit in this panel if you want a problem ticket to be raised based upon receipt of a message.

Specifying the PROBSOLV Process in the State Change Exits Panel

To specify the PROBSOLV process in the State Change Exits panel, proceed as follows:

Step 1. From any panel, enter **/RADMIN.R**.

The ResourceView : Resource Definition panel is displayed. You can change the displayed system image or accept the default. The last specified system image is the default system image.

Step 2. Enter **S** beside the required resource class.

The resource list panel is displayed. This panel lists the resources defined to the specified system image.

Step 3. Enter **U** beside the resource for which you wish to specify the PROBSOLV process.

A list of the panels in the resource definition is displayed.

Note

You can also access the list of panels by issuing the DB command against the resource from the file transfer status monitor.

Step 4. Enter **S** beside the listed State Change Exits panel.

The State Change Exits panel is displayed, as shown in Figure 15-26.

Figure 15-26. State Change Exits Panel

```
SOLVPROD------ ResourceView : CDMGR DECD1 State Change Exits ----------FT1-0001
Command ===>                                                   Function=UPDATE

. State Change Exits -------------------------------------------------------.
|                      S/B=Browse U=Update I=Interactive L=List P=Parameters |
|     Invoked                     Process  Parameters                       |
| ___ BEFORE ACTIVATION            ________                                 |
|     State   Change    Change                                              |
|     Type    From      To        Process  Parameters                       |
| ___ ACTUAL_ ANY_______ FAILED___ $NCL____ $NCL=$RFCDTAB ACTION=FREE OWNER=&Z |
| ___ ACTUAL_ ANY_______ INACTIVE_ $NCL____ $NCL=$RFCDTAB ACTION=FREE OWNER=&Z |
| ___ _______ __________ _________ ________                                 |
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
```

Warning

Do not change the state change exits provided by the template.

Step 5. Enter field data as follows:

Field	Action	Input Example
State Type	Specify the State Type. You can enter ? to select from a prompt list.	ACTUAL
Change From	Specify the initial state of the resource. You can enter ? to select from a prompt list.	ANY
Change To	Specify the final state of the resource. You can enter ? to select from a prompt list.	FAILED
Process	Specify the process. Enter **PROBSOLV**.	PROBSOLV

If you enter the information as specified in the Input Example column of the above table, the PROBSOLV process will run, and a problem ticket will be raised, if the actual state of this resource changes from any actual state to a FAILED actual state. For example, if the resource state changes from ACTIVE to FAILED or UNKNOWN to FAILED, the PROBSOLV process will run, and a problem ticket will be raised.

Step 6. Enter **P** in the first input field of the line entry.

The Define Exits Parameters panel is displayed, as shown in Figure 15-27.

Figure 15-27. State Change Exits Panel

```
SOLVPROD------ ResourceView : CDMGR DECD1 State Change Exits ----------FT1-0001
Command ===>                                                   Function=UPDATE

. State Change Exits -------------------------------------------------------.
|                      S/B=Browse U=Update I=Interactive L=List P=Parameters |
|     Invoked                     Process  Parameters                       |
| ___ BEFORE ACTIVATION            ________                                 |
|     State   Change    Change                                              |
|     Type    From      To        Process  Parameters                       |
| ___ ACTUAL_ ANY_______ FAILED___ $NCL____ $NCL=$RFCDTAB ACTION=FREE OWNER=&Z |
| ___ ACTUAL_ ANY_______ INACTIVE_ $NCL____ $NCL=$RFCDTAB ACTION=FREE OWNER=&Z |
| P__ ACTUAL_ ANY_______ FAILED___ PROBSOLV                                 |
| ___ ________ __________ __________ _________                              |
|
```

```
SOLVPROD---- ResourceView : CDMGR DECD1 Define Exit Parameters --------FT1-0001
Command ===>                                                    Function=UPDATE

State Type ...... ACTUAL
Change From ..... ANY
Change To ....... FAILED
Process ......... PROBSOLV

. Parameters ---------------------------------------------------------------.
| ______________________________________________________________________ |
| ______________________________________________________________________ |
'------------------------------------------------------------------------'
```

Step 7. Enter the ACB name for your SOLVE:Problem application in the Parameters window as ACB=*acb-name* (see Figure 15-28).

Figure 15-28. Specifying the ACB Name for the PROBSOLV Process

```
SOLVPROD----- ResourceView : CDMGR DECD1 Define Exit Parameters -------FT1-0001
Command ===>                                                    Function=UPDATE

State Type ...... ACTUAL
Change From ..... ANY
Change To ....... FAILED
Process ......... PROBSOLV

. Parameters ---------------------------------------------------------------.
| ACB=SOPROB1_____________________________________________________________  |
| ______________________________________________________________________ |
'------------------------------------------------------------------------'
```

Step 8. Press F3 (OK) after you have entered the ACB name in the Parameters window.

You are returned to the State Change Exits panel.

Step 9. Press F3 (File) to file the resource definition.

Specifying the PROBSOLV Process for a Message Rule

To specify the PROBSOLV process for a message rule, proceed as follows:

Step 1. From any panel, enter **/RADMIN.R**.

The Resource Definition panel is displayed. You can change the displayed system image or accept the default. The last specified system image is the default system image.

Step 2. Enter **S** beside the required resource class.

The resource list panel is displayed. This panel lists the resources defined to the system image.

Step 3. Enter **U** beside the resource for which you wish to specify the PROBSOLV process.

A list of the panels in the resource definition is displayed.

Note

You can also access the list of panels by issuing the DB command against the resource from the file transfer status monitor.

Step 4. Enter **S** beside the listed Status Monitor Message Details panel.

The Status Monitor Messages Details panel is displayed, as shown in Figure 15-29.

Figure 15-29. Status Monitor Message Details Panel

```
--------- ResourceView : CDMGR DECD1 Status Monitor Message Details ---FT1-0001
Command ===>                                                  Function=UPDATE

.-------------------------------------------------------------------------------.
|      Activate Inactivate Messages                      Pty  Ext   Status      |
| ___  SITA036I_____________________________________ 000  NO    ACTIVE      |
| ___  SITB001I_____________________________________ 000  NO    INACTIVE    |
| ___  SITB001I_____________________________________ 000  NO    INACTIVE    |
'-------------------------------------------------------------------------------'
.-------------------------------------------------------------------------------.
|  S=LstPnls EF=ExtFilter EA=EvntAct EE=EvntExit ED=ExtDisp DOC=EvntDoc D=Del |
|      Status Monitor Messages                           Pty  Ext   Status      |
| ___  $AA-RFCONN05 DECD1___________________________ ___  YES   DEGRADED__ |
| ___  $AA-RFLSTNR04 DECD1__________________________ ___  YES   DEGRADED__ |
| ___  $AA-RFQUEUE03 DECD1__________________________ ___  YES   DEGRADED__ |
| ___  $AA-RFQUEUE05 DECD1__________________________ ___  YES   DEGRADED__ |
| ___  $AA-RFQUEUE05 DECD1__________________________ ___  YES   DEGRADED__ |
| ___  $AA-RFRESET01 DECD1__________________________ ___  YES   _________ |
| ___  $AA-RFSESS04 DECD1___________________________ ___  YES   DEGRADED__ |
| ___  $HASP100 DECD1    ON_________________________ ___  NO    STARTING__ |
| ___  $HASP373 DECD1    STARTED____________________ ___  NO    STARTING__ |
'-------------------------------------------------------------------------------'
 F1=Help      F2=Split     F3=File      F4=Save      F5=Related   F6=SortMsgs
 F7=Backward  F8=Forward   F9=Swap     F10=ScrlLst  F11=Panels   F12=Cancel
```

Step 5. Position your cursor in the first input field of any listed message, and enter **EE**.

The Define Event Exits Panel is displayed, as shown in Figure 15-30.

Key Concept

You can specify that the PROBSOLV process be performed upon receipt of any message listed in both the Activate Inactivate Messages window and the Status Monitor Messages window.

Figure 15-30. Displaying the Define Event Exits Panel

```
-------- ResourceView : CDMGR DECD1 Status Monitor Message Details ----FT1-0001
Command ===>                                                   Function=UPDATE

.------------------------------------------------------------------------------.
|      Activate Inactivate Messages                      Pty  Ext   Status     |
| EE   SITA036I_____________________________________ 000  NO    ACTIVE     |
```

```
SOLVPROD------ ResourceView : CDMGR DECD1 Define Event Exits ----------FT1-0001
Command ===>                                                   Function=UPDATE

. Extended Event Exits ----------------------------------------------------.
|                                   S/B=Browse U=Update I=Interactive L=List |
|     Exit Type    Process  Parameters                                      |
| ___ State Change ________ ______________________________________________ |
|                          ______________________________________________ |
|                                                                           |
| ___ Problem      ________ ______________________________________________ |
|                          ______________________________________________ |
|                                                                           |
| ___ General      ________ ______________________________________________ |
|                          ______________________________________________ |
|                                                                           |
'---------------------------------------------------------------------------'
```

Step 6. Enter **PROBSOLV** in the Process field for the Problem exit type.

Step 7. You must specify the ACB name for your SOLVE:Problem application in the Parameters field as ACB=*acb-name*.

Step 8. Press F3 (OK) when you have completed entering the data.

You are returned to the Define Event Exits panel.

Step 9. Press F3 (File) to file the definition.

Using Processes to Perform Complex Operations

A process is a series of steps that can be executed in sequence. Each step performs a single operation, by using a macro. The following sections describe how to use some of the macros to perform special operations. For information about other macros, see the online help.

Defining a Process

To define a process, proceed as follows:

Step 1. At an ===> prompt, enter **/RADMIN.P**.

The Process List is displayed, as shown in Figure 15-31.

Figure 15-31. Process List Panel

```
SOLVPROD------------- Automation Services : Process List ---------------------2
Command ===>                                                   Scroll ===> CSR

. System Image -------------------------------------------------------------.
| System Name .... FT1          Version ...+ 0001                            |
'----------------------------------------------------------------------------'
. Processes ----------------------------------------------------------------.
|                 S/B=Browse U=Update C=Copy D=Delete E=Execute I=Interactive |
|     Process   Description                                            Glbl |
|     PROBOIM   Create an OIM Problem Record (Supply Link,Cat,Sev,Grp,Fau Yes |
|     PROBSOLV  Create a SOLVE:Problem Problem Record (Supply ACB=)       Yes |
|     **END**                                                                |
```

Note

The process you create here is only available to the specified system image. If you want to create a process that is available to *all* definitions in the knowledge base, enter **/RADMIN.GP** as the path.

Step 2. Change, if required, the displayed system image, or accept the default. The last specified system image is the default system image (see Figure 15-31).

Step 3. Press F4 (Add) to add a process.

The Process Definition panel is displayed, as shown in Figure 15-32.

Figure 15-32. Process Definition Panel

```
SOLVPROD--------- Automation Services : Process Definition --------Function=Add
Command ===>                                                   Scroll ===> PAGE

. Process Definition -------------------------------------------------------.
| System Name .. FT1       Version .. 0001   Last Updated By                 |
| Name .........                             At           On                 |
| Description ..                                                            |
'----------------------------------------------------------------------------'
. Process Steps ------------------------------------------------------------.
|                                                                            |
|                                          D=Delete I=Insert P=Parms R=Repeat |
|                     Condition                                              |
|      StepName   Step/RC  Opr R/C   Macro    Description                    |
|                                                                            |
|                                                                            |
```

Step 4. Specify the name of your process in the Name field (for example, SNMPTRAP).

Step 5. Enter a description of your process in the Description field.

Step 6. Enter information in the fields of the Process Steps window.

Step 7. Enter **P** beside each process step, and specify the macro parameters.

Step 8. When you finish defining your process, press F3 (File) to file the definition.

You can now specify this process in a resource definition in the same manner as that discussed for the SOLVE:Problem process (see the section, *Raising a Problem Ticket*, on page 15-29).

Checking the Availability of a Destination CONNECT:Direct Node

Use the PINGCD macro to check the availability of a destination node for a CONNECT:Direct application. The return codes are as follows:

Return Code	Meaning
0	The destination node is available.
4	The destination node cannot be contacted.
8	The destination node is not defined in the network map of the CONNECT:Direct application. For example, you might have specified a wrong name.

By using the return codes, you can specify the next step to perform.

Specifying the PINGCD Macro

Specify the PINGCD macro in your process as follows:

Step 1. Add or update a process for the macro (see the section, *Defining a Process*, on page 15-34).

Step 2. Enter information in the fields of the Process Steps window, on the Process Definition panel, as follows:

Field	Action	Input Example
StepName	Specify the process step.	ONE
Macro	Specify **PINGCD** as the name of the macro.	PINGCD

Step 3. Enter **P** beside your line entry.

The PINGCD Macro Parameter Definition panel is displayed, as shown in Figure 15-33.

Figure 15-33. Specifying PINGCD Macro Parameters

```
. Process Steps ------------------------------------------------------------.
|                                                                           |
|                                          D=Delete I=Insert P=Parms R=Repeat |
|                      Condition                                            |
|      StepName   Step/RC  Opr R/C   Macro    Description                  |
| P    ONE                           PINGCD   CHECK AVAILABILITY OF DESTINATI |
|                                                                           |
```

```
SOLVPROD--- Automation Services : PINGCD Macro Parameter Definition -----------
Command ===>                                                   Function=UPDATE

.- PINGCD Parameter Details ------------------------------------------------.
|                                                                           |
| CDMGR Name .... _____________                                             |
|                                                                           |
| Remote Node ... _____________                                             |
|                                                                           |
| Wait Time .... 30__  Wait Time Expiry Return Code ... 69_                 |
'---------------------------------------------------------------------------'
```

Step 4. Enter the PINGCD macro details. For information about the fields, see the online help.

Figure 15-34. PINGCD Macro Parameter Definition Panel—Example

```
SOLVPROD--- Automation Services : PINGCD Macro Parameter Definition -----------
Command ===>                                                   Function=UPDATE

.- PINGCD Parameter Details ------------------------------------------------.
|                                                                           |
| CDMGR Name .... DECD1________                                             |
|                                                                           |
| Remote Node ... ALUNIXCD1____                                             |
|                                                                           |
| Wait Time .... 30__  Wait Time Expiry Return Code ... 69_                 |
'---------------------------------------------------------------------------'
```

In the example shown in Figure 15-34, you check the availability of the ALUNIXCD1 node of the DECD1 CONNECT:Direct region.

Step 5. With the field data entered, press F3 (OK).

You are returned to the Process Definition panel.

Issuing CONNECT:Direct Commands from a Process

Use the CDAPI macro to issue a command to a specified CONNECT:Direct application. The macro monitors the response and sets a return code. By using the return code, you can specify the next step to perform.

Specifying the CDAPI Macro

Specify the CDAPI macro in your process as follows:

Step 1. Add or update a process for the macro (see the section, *Defining a Process*, on page 15-34).

Step 2. Enter information in the fields of the Process Steps window, on the Process Definition panel, as follows:

Field	Action	Input Example
StepName	Specify the process step.	ONE
Macro	Specify **CDAPI** as the name of the macro.	CDAPI

Step 3. Enter **P** beside your line entry.

The CDAPI Macro Parameter Definition panel is displayed, as shown in Figure 15-35.

Figure 15-35. Specifying CDAPI Macro Parameters

```
. Process Steps ------------------------------------------------------------.
|                                                                           |
|                                          D=Delete I=Insert P=Parms R=Repeat |
|                     Condition                                             |
|     StepName   Step/RC  Opr R/C   Macro    Description                    |
| P   ONE                           CDAPI    ISSUE COMMAND TO CONNECT:DIRECT |
```

```
SOLVPROD--- Automation Services : CDAPI Macro Parameter Definition ------------
Command ===>                                                   Function=UPDATE

.- CONNECT:Direct Command Details ------------------------------------------.
|                                                                           |
| CDMGR Name ... ________                                                   |
|                                                                           |
| Command ...... ___________________________________________________________ |
|                ___________________________________________________________ |
|                                                                           |
| Wait Time .... 30__  Wait Time Expiry Return Code ... 69_                 |
'---------------------------------------------------------------------------'
.- Response Message Analysis -----------------------------------------------.
|                                D=Delete Extended Filter  S=Extended Filter |
|           Message Text                                    Return Extended |
|                                                           Code   Filter?  |
|   ___     ______________________________________________  ___             |
|   ___     ______________________________________________  ___             |
|   ___     ______________________________________________  ___             |
|   ___     ______________________________________________  ___             |
|   ___     ______________________________________________  ___             |
'---------------------------------------------------------------------------'
 F1=Help      F2=Split     F3=OK
                           F9=Swap                                F12=Cancel
```

Step 4. Enter the CDAPI macro details. For information about the fields, see the online help.

In the example shown in Figure 15-36, you look for the HOLDQ01 CONNECT:Direct process in the DECD1 region and test that the process exists. You can then use the return code to decide on the next step to take. (A zero return code means a successful operation.)

Figure 15-36. CDAPI Macro Parameter Definition Panel—Example

```
SOLVPROD--- Automation Services : CDAPI Macro Parameter Definition ------------
Command ===>                                                   Function=UPDATE

.- CONNECT:Direct Command Details ---------------------------------------------.
|                                                                               |
| CDMGR Name ... DECD1___                                                       |
|                                                                               |
| Command ...... SELECT PROCESS WHERE (QUEUE=HOLD)_____________________________ |
|                ______________________________________________________________ |
|                                                                               |
| Wait Time .... 30__  Wait Time Expiry Return Code ... 69_                     |
'-------------------------------------------------------------------------------'
.- Response Mess-------------------------------------------------------------.
|                                                                               |
|          Mess                                                                 |
|                                                                               |
|   S__     PRC_____________________________________________                    |
|   ___     ________________________________________________                    |
```

Enter **S** to specify extended filter for HOLDQ01.

```
D=Delete Extended Filter  S=Extended Filter |
                            Return Extended |
                            Code   Filter?  |
                            02_             |
                            ___             |
```

```
SOLVPROD----- Automation Services : Extended Message Filtering ----------------
Command ===>                                                     Function=UPDATE

. Extended Filter Definition -------------------------------------------------.
|                                                                               |
| Message Text .......... PRC_____________________________________________      |
|                                                                               |
| Wildcard Character .... *_                                                    |
'-------------------------------------------------------------------------------'
. Message Text Analysis ------------------------------------------------------.
|                                                                               |
|   Strt Word      Scan                                                         |
|   Pos  Num  Opr  Text                                                         |
| 1 001  001  EQ_  PRC___________________________________________________       |
| 2 001  002  EQ_  NAME__________________________________________________       |
| 3 001  004  EQ_  HOLDQ01_______________________________________________       |
| 4 ___  ___  ___  ______________________________________________________       |
| 5 ___  ___  ___  ______________________________________________________       |
|                                                                               |
| Expression e.g (1 and (2 or 3)) 1 AND 2 AND 3__________________________       |
'-------------------------------------------------------------------------------'

 F1=Help      F2=Split     F3=OK
                           F9=Swap                                F12=Cancel
```

Step 5. With the field data entered, press F3 (OK).

You are returned to the Process Definition panel.

Using the SNMP Trap Exit

NetMaster for File Transfer allows you to generate SNMP traps. An SNMP trap can be used to inform a remote system of a resource state change.

The SNMPTRAP macro is supplied with your NetMaster for File Transfer product. To generate an SNMP trap, you define an NetMaster for File Transfer process that uses this macro.

Creating an SNMP Trap in a Process

To create an SNMP trap, proceed as follows:

Step 1. Add or update a process for the trap (see the section, *Defining a Process*, on page 15-34).

Step 2. Enter information in the fields of the Process Steps window, on the Process Definition panel, as follows:

Field	Action	Input Example
StepName	Specify the process step.	ONE
Macro	Specify SNMPTRAP as the name of the macro.	SNMPTRAP

Step 3. Enter **P** beside your line entry.

The SNMPTRAP Macro Parameter Definition panel is displayed, as shown in Figure 15-37.

Figure 15-37. Specifying SNMPTRAP Macro Parameters

```
. Process Steps ------------------------------------------------------------.
|                                                                           |
|                                          D=Delete I=Insert P=Parms R=Repeat |
|                      Condition                                            |
|      StepName   Step/RC  Opr R/C   Macro    Description                  |
|  P   ONE                           SNMPTRAP ISSUE AN SNMPTRAP ON BEHALF OF |
|
```

```
------------ Automation Services : SNMPTRAP Macro Parameter Definition --------
Command ===>                                                   Function=UPDATE

. SNMP Trap Details --------------------------------------------------------.
|                                                                           |
| Text ..... ______________________________________________________________ |
|            ______________________________________________________________ |
|            ______________________________________________________________ |
|            ______________________________________________________________ |
|            ______________________________________________________________ |
|            ______________________________________________________________ |
|                                                                           |
| Destinations Dataset ...... ____________________________________________  |
|           or                                                              |
| Destination Address(es) ... ____________________________________________ |
|                                                                           |
| Enterprise Id ............. 1.3.6.1.4.1.11.2.17.1_____________________ |
|                                                                           |
| Specific Trap Number ...... 59047936_______________________________________ |
|                                                                           |
| Community Name ............ public_____________________________________ |
'---------------------------------------------------------------------------'
 F1=Help      F2=Split     F3=OK
                           F9=Swap                                F12=Cancel
```

Step 4. Enter the SNMP trap details as follows (see Figure 15-38 on page 15-42 for an example screen):

Field	Action	Input Example
Text	Enter the text to send with the trap.	See Figure 15-38 on page 15-42.
Destinations Dataset or	Specify the dataset name (DSN) in which the address(es) of remote system(s) are located. Enter the DSN.	SOPS.REMOTE.ADDR
Destination Address(es)	Specify the destination address(es) of the remote system(s). Enter an address, or multiple addresses by using a comma or a space as the delimiting character.	172.24.170.23
Enterprise ID	Together with the specific trap number, specify the format of the trap. The format identified by this field is determined by your open platform administration.	1.3.6.1.4.1.11.2.17.1
Specific Trap Number	Together with the enterprise ID, specify the format of the trap. The format identified by this field is determined by your open platform administration.	59047936
Community Name	Specify the community for which the trap is destined. This field is *case sensitive* and can be left with its default of `public`.	PUBLIC

Figure 15-38. SNMP Trap Macro Parameter Definition Panel—Example

```
--------- Automation Services : SNMPTRAP Macro Parameter Definition -----------
Command ===>                                                   Function=UPDATE

. SNMP Trap Details -------------------------------------------------------.
|                                                                          |
| Text ..... SOLVE1_____________________________________________________ |
|            SOLVE2_____________________________________________________ |
|            SOLVE3_____________________________________________________ |
|            FT1-0001___________________________________________________ |
|            CONNECT:DIRECT(C:D-NAME)___________________________________ |
|            FT1-0001 HAS NO C:D-NAME LISTENER TASK_____________________ |
|                                                                          |
| Destinations Dataset ...... ____________________________________________ |
|           or                                                             |
| Destination Address(es) ... 172.24.170.23_____________________________ |
|                                                                          |
| Enterprise Id ............. 1.3.6.1.4.1.11.2.17.1_____________________ |
|                                                                          |
| Specific Trap Number ...... 59047936__________________________________ |
|                                                                          |
| Community Name ............ PUBLIC_____________________________________ |
'--------------------------------------------------------------------------'
 F1=Help      F2=Split     F3=OK
                           F9=Swap                              F12=Cancel
```

In the example shown in Figure 15-38, the remote system at the specified address is sent this SNMP trap when the CONNECT:Direct listener task is lost. This process would be specified in the manager resource definition for CONNECT:Direct (C:D-NAME) and processed as an exit upon receipt of a message which indicated that the CONNECT:Direct region did not have a listener task.

Step 5. With the field data entered, press F3 (OK).

You are returned to the Process Definition panel.

Generating an Exception Report from a NetMaster for File Transfer Process

The FTCHECK macro generates a file transfer exception report based on a specified filter. If a return code of 4 is received, further information is available in the returned variables which can be checked further by the process to perform other actions. For more information, see the online help.

Specifying the FTCHECK Macro

Specify the FTCHECK macro in your process as follows:

Step 1. Add or update a process for the macro (see the section, *Defining a Process*, on page 15-34).

Step 2. Enter information in the fields of the Process Steps window, on the Process Definition panel, as follows (see Figure 15-39):

Field	Action	Input Example
StepName	Specify the process step.	ONE
Macro	Specify FTCHECK as the name of the macro.	FTCHECK

Step 3. Enter **P** beside your line entry.

The FTCHECK Macro Parameter Definition panel is displayed, as shown in Figure 15-39.

Figure 15-39. Specifying FTCHECK Macro Parameters

```
 . Process Steps ------------------------------------------------------------.
 |                                                                           |
 |                                          D=Delete I=Insert P=Parms R=Repeat |
 |                     Condition                                             |
 |      StepName   Step/RC  Opr R/C   Macro    Description                  |
 | P    ONE                           FTCHECK  GENERATE EXCEPTION REPORT    |
```

```
SOLVPROD ---- Automation Services : FTCHECK Macro Parameter Definition --------
Command ===>                                                   Function=UPDATE

.- Report Definition Details ------------------------------------------------.
| Exception Report Filter ..+ ____________                                   |
| OR                                                                         |
| FTSCHD  System Image + ________ Version + ____  Name + ________________    |
'----------------------------------------------------------------------------'

.- Period to Check ----------------------------------------------------------.
| From Date ................. ___________  From Time ... ________          |
| To Date.................... ___________  To Time ..... ________          |
| OR                                                                         |
| Within the last ........... _____  (1 to 10000 Hours)                     |
'----------------------------------------------------------------------------'

.- Print Exception Report Results (Optional) --------------------------------.
| Printer Name ..+ ___________                                               |
| Copies ......... ___  (Range 1 to 255)                                     |
| Hold? .......... ___  (YES or NO)                                          |
| Keep? .......... ___  (YES or NO)                                          |
'----------------------------------------------------------------------------'
 F1=Help      F2=Split     F3=OK
                           F9=Swap                              F12=Cancel
```

Step 4. Enter the FTCHECK macro details. For information about the fields, press F1 (Help) to view the online help.

Step 5. With the field data entered, press F3 (OK).

You are returned to the Process Definition panel.

Customizing the Manager Resource Definition

The manager resource templates you use when you define manager resources provide sufficient information for you to manage the CA-XCOM CONNECT:Direct, CONNECT:Mailbox, FTP, and FTS regions. You can, however, customize the defined manager resources to suit your special requirements.

To customize or view a manager resource definition, proceed as follows:

Step 1. Enter the **/RADMIN.R.*resource-class-name*** path to access the list of defined resources.

For example, to access the list of defined CA-XCOM managers, enter the **/RADMIN.R.XCMGR** path.

Step 2. Identify the system image that contains the manager you want to customize in the System Name and Version fields.

Step 3. Enter **U** beside the manager you want to customize.

The list of panels in the resource definition is displayed.

Step 4. To display a panel, enter **S** beside it.

Note

You can also enter a number at the Command ===> prompt to display a panel. For example, to display the first panel, enter **1**.

Warning

The supplied templates ensure that your file transfer resources are monitored correctly. When customizing a manager resource definition, ensure that you do not change the following:

- State change exits specified by the template
- Display processes specified by the template
- Operations commands specified by the template
- Message rules specified by the template

The manager resource definition comprises the following panels:

Panel Name	Description
General Description	This panel allows you to specify general information about the resource (for example, the operation mode).
Availability Map	This panel allows you to specify the schedule that activates or inactivates the resource.
Activation Details	This panel allows you to specify how the region starts the resource.
Inactivation Details	This panel allows you to specify how the region stops the resource normally.
Force Inactivation Details	This panel allows you to specify how the region stops the resource immediately.
Display and Heartbeat Details	This panel allows you to specify how to retrieve status information about the resource.
Status Monitor Message Details	This panel allows you to specify rules which react to unsolicited messages. *Do not change those rules specified by the template*.
State Change Exits	This panel allows you to specify exit processes which are executed as a result of a resource state change. *Do not change the information specified by the template*. You can add exits (for example, the SOLVE:Problem exit).
Automation Log Details	This panel allows you to customize log attributes such as the size of the transient log, where messages are logged, and what messages are logged.
Owner Details	This panel allows you to specify particulars of the person(s) responsible for the resource.
Extended Function Exit	This panel allows you to extend the function of NetMaster for File Transfer by specifying a user procedure.

Step 5. Press F12 (Cancel) to exit the resource definition without saving any changes, or press F3 (File) to exit the resource definition and file the changes.

Customizing Monitor Resource Definitions

The monitor resource templates you use when you define monitor resources provide sufficient information for you to monitor the resources used by the file transfer regions. You can, however, customize the defined monitor resources to suit your special requirements.

To customize or view a monitor resource definition, proceed as follows:

Step 1. Enter the **/RADMIN.R.*resource-class-name*** path to access the list of defined resources.

For example, to access the list of defined CA-XCOM monitors, enter the **/RADMIN.R.XCMON** path.

Step 2. Identify the system image that contains the monitor you want to customize in the System Name and Version fields.

Step 3. Enter **U** beside the monitor you want to customize.

The list of panels in the resource definition is displayed.

Step 4. To display a panel, enter **S** beside it.

Note

You can also enter a number at the Command ===> prompt to display a panel. For example, to display the first panel, enter **1**.

Warning

The supplied templates ensure that your file transfer resources are monitored correctly. When customizing a monitor resource definition, ensure that you do not change the following:

- Message rules specified by the template
- State change exits specified by the template

The monitor resource definition comprises the following panels:

Panel Name	Description
General Description	This panel allows you to specify general information about the resource (for example, the operation mode).
Monitor Details	This panel allows you to specify monitoring criteria pertinent to the monitor type (for example, the idle time of a TCP/IP connection).
Status Monitor Message Details	This panel allows you to specify rules which react to unsolicited messages. *Do not change those rules specified by the template*.
State Change Exits	This panel allows you to specify exit processes which are executed as the result of a resource state change. *Do not change the information specified by the template*. You can add exits (for example, a SOLVE:Problem exit).
Automation Log Details	This panel allows you to customize log attributes such as the size of the transient log, where messages are logged, and what messages are logged.
Owner Details	This panel allows you to specify particulars of the person(s) responsible for the resource.
Extended Function Exit	This panel allows you to extend the function of NetMaster for File Transfer by specifying a user procedure.

Step 5. Press F12 (Cancel) to exit the resource definition without saving any changes, or press F3 (File) to exit the resource definition and file the changes.

Customizing the Supporting Resource Definition

The resource templates you use when you define supporting resources (such as TCPaccess and DASDs) provide sufficient information for you to manage those resources. You can, however, customize the defined resources to suit your special requirements.

To customize or view a supporting resource definition, use the following menu paths to access the required definitions, then follow the procedure used for customizing manager resources (see the section, *Customizing the Manager Resource Definition*, on page 15-44):

If you want to access the resource definitions for …	**Enter the …**
DASDs	**/RADMIN.R.DASD** path.
TCPaccess tasks, Communications Server, or CONNECT:Mailbox VSAM file server	**/RADMIN.R.STC** path.
Tapes	**/RADMIN.R.TAPE** path.

16

Logging Messages Selectively

You can control which messages are logged in a NetMaster for File Transfer region by suppressing the unwanted messages from being delivered to the logs.

This chapter contains the following topics:

- Logging Selected Messages to the Activity Log
- Logging Selected CONNECT:Direct Messages to the File Transfer Log

Logging Selected Messages to the Activity Log

By default, the activity log contains only messages generated by the NetMaster for File Transfer region.

However, you can include system messages in the activity log by using the LOGFILES parameter group. To enable logging of system messages, specify **YES** in the Log Operating System Messages? field (see the section, *Controlling Operating System Message or Command Logging*, on page 5-25). This enables logging of *all* system messages.

If you want to log certain system messages only, you must first define an EventView rule set containing message rules and associate the rule set with the system image, as described in the following sections.

Defining a Rule Set

To define a rule set, proceed as follows:

Step 1. Enter the **/EADMIN.R.R** path.

The EventView : Ruleset List panel is displayed.

Step 2. Press F4 (Add) to add a rule set to the knowledge base.

The EventView : Ruleset Description panel is displayed, as shown in Figure 16-1.

Figure 16-1. EventView : Ruleset Description

```
SOLVPROD--------------- EventView : Ruleset Description -----------------------
Command ===>                                                     Function=ADD

Ruleset Name ........ ________                     Ruleset Status ...+ ACTIVE__
Short Description ... ______________________________

. Control Options -------------------------------------------------------------.
|                                                                              |
| Default Message Delivery ....+ YES  (if no rule for message)                 |
| Perform Message Modification?  YES                                           |
| Perform Action? ............. YES                                           |
| Log Ruleset Activity? ........ NO_                                           |
|                                                                              |
| Collect Statistics? .......... YES                                           |
```

Step 3. Specify the name of the rule set in the Ruleset Name field (for example, FT11).

Step 4. Provide a short description in the Short Description field (for example, File transfer logging).

Step 5. Enter **IGN** in the Default Message Delivery field.

This ensures that no messages are logged to the activity log unless they are defined to the rule set.

Note

If a rule in the rule set has a different message delivery option, this overrides the message delivery option specified in the rule set.

Step 6. Enter **NO** in the Collect Statistics? field.

The collect statistics feature is not required for the management of file transfers.

Step 7. Enter **NO** in the Learn New Messages? field.

The learn new messages feature is not required for the management of file transfers.

Figure 16-2 shows an example of a completed rule set definition.

Figure 16-2. Specifying the Rule Set

```
SOLVPROD--------------- EventView : Ruleset Description -----------------------
Command ===>                                                     Function=ADD

Ruleset Name ........ FT11____                    Ruleset Status ...+ ACTIVE__
Short Description ... File transfer logging_________

. Control Options ---------------------------------------------------------.
|                                                                          |
| Default Message Delivery ....+ NO_  (if no rule for message)             |
| Perform Message Modification?  YES                                       |
| Perform Action? ............. YES                                       |
| Log Ruleset Activity? ........ NO_                                       |
|                                                                          |
| Collect Statistics? .......... NO                                        |
| Learn New Messages? .......... NO                                        |
|                                                                          |
'--------------------------------------------------------------------------'




 F1=Help      F2=Split     F3=File      F4=Save
              F8=Forward   F9=Swap                  F11=Panels   F12=Cancel
```

Step 8. Press F3 (File) to file the rule set.

You are returned to the EventView : Ruleset List panel, and the defined rule set is added to that list.

You will now define a message rule(s) that allows messages to be delivered to the activity log.

Defining a Message Rule

To define a message rule that delivers messages from a specified region to the activity log, proceed as follows:

Note

You should define a message rule for each managed file transfer or supporting region whose messages are to be logged.

Step 1. At the EventView : Ruleset List panel, enter **M** beside the rule set defined in the previous section.

The EventView : Message Rule List panel is displayed.

Step 2. Press F4 (Add) to add a message rule.

The EventView : Message Filter panel is displayed, as shown in Figure 16-3.

Figure 16-3. The EventView : Message Filter

```
SOLVPROD----------------- EventView : Message Filter ----------------------FT11
Command ===>                                                   Function=ADD

Ruleset Name ........ FT11                           Rule Status ...+ ACTIVE__
Short Description ... ______________________________

. Expected Message -------------------------------------------------------------.
|                                        S=ListPanels E=ExtFilter T=TestVars |
|      Message Text  ( WildChar = * )                                   ExtFlt |
| ___  ____________________________________________________________________ NO     |
'----------------------------------------------------------------------------'
. Execution Conditions ---------------------------------------------------------.
|                                                                              |
| Job Name .... ________   Rule Priority ........... __   (1 is best)         |
| Job Type ...+ _______    Execute If Not Best Fit?  ___                       |
```

Step 3. Enter a short description of the message rule (for example, CONNECT:Direct messages).

Step 4. Enter ***** in the Message Text field.

An asterisk (*) specifies that all messages are accepted.

Step 5. Enter the job name of a managed region in the Job Name field (for example, DECD1).

The name ensures that only messages generated by the specified job are logged in the activity log.

Step 6. Enter the job type in the Job Type field: STC for a started task and JOB for a batch job.

Figure 16-4 shows an example of a completed Message Filter panel.

Figure 16-4. Specifying the Message Filter

```
SOLVPROD----------------- EventView : Message Filter ----------------------FT11
Command ===>                                                   Function=ADD

Ruleset Name ........ FT11                          Rule Status ...+ ACTIVE__
Short Description ... CONNECT:Direct messages_______

. Expected Message -------------------------------------------------------------.
|                                          S=ListPanels E=ExtFilter T=TestVars |
|      Message Text  ( WildChar = * )                                   ExtFlt |
| ___  *_____________________________________________________________ NO      |
'--------------------------------------------------------------------------------'
. Execution Conditions ---------------------------------------------------------.
|                                                                                |
| Job Name .... DECD1___   Rule Priority ........... __   (1 is best)           |
| Job Type ...+ STC____    Execute If Not Best Fit?  ___                         |
|                                                                                |
|         Mon Tue Wed Thu Fri Sat Sun       Time       Start       End          |
| On Days ___ ___ ___ ___ ___ ___ ___       Range1 ... ________    ________    |
|                                           Range2 ... ________    ________    |
|                                                                                |
'--------------------------------------------------------------------------------'

 F1=Help      F2=Split     F3=File      F4=Save
              F8=Forward   F9=Swap                 F11=Panels   F12=Cancel
```

Step 7. Press F8 (Forward) to scroll to the Message Delivery panel, and enter **YES** in the Deliver Field, as shown in Figure 16-5.

Figure 16-5. Specifying Message Delivery

```
SOLVPROD--------------- EventView : * Message Delivery --------------------FT11
Command ===>                                                   Function=ADD

Deliver ............+ YES


. Threshold --------------------------------------------------------------------.
|                                                                                |
| Maximum Number .... ____                                                       |
| Time Interval ..... ________                                                   |
```

Step 8. Press F3 (File) to file the message rule.

You are returned to the Message Rule List panel, and the message rule is listed. Press F11 (Right) to display additional details.

Step 9. To define message rules for other regions defined to a system image, repeat Step 2 through Step 8.

Step 10. Press F3 (Exit) to exit the EventView : Message Rule List panel.

Adding a Rule Set to the System Image

To enable a rule set to be loaded, you need to associate it with an active system image (that is, a system image that is loaded in the NetMaster for File Transfer region).

To associate a rule set with a system image, proceed as follows:

Step 1. Enter the **/RADMIN.I** path.

The ResourceView : System Image List panel is displayed.

Step 2. Enter **U** beside the system image to which you wish to associate the message suppression rule set.

The ResourceView : System Image Definition panel is displayed.

Step 3. Enter the name of the defined rule set in the EventView Ruleset to Activate field (for example, enter FT11, as shown in Figure 16-6).

Figure 16-6. Specifying the Message Suppression Rule Set

```
SOLVPROD----------- ResourceView : System Image Definition --------------------
Command ===>                                                     Function=UPDATE


System Name ......... FT1
Database Version .... 0001
Home System ......... COMP001_

Short Description ... SYSTEM01 file transfer image__
Long Description .... ____________________________________________________________
                      ____________________________________________________________
                      ____________________________________________________________
                      ____________________________________________________________

EventView Ruleset to Activate ...+ FT11____
```

Step 4. Press F3 (File) to file the changes to your system image.

If you updated the active system image, your message suppression rule set is now in effect.

Logging Selected CONNECT:Direct Messages to the File Transfer Log

You can restrict the CONNECT:Direct event messages to be recorded in the file transfer log by suppressing unwanted messages. You do this by specifying which event messages generated by CONNECT:Direct regions, defined to the active system image, are logged in the file transfer log.

To specify which messages are logged to the file transfer log, proceed as follows:

Step 1. Enter the **/ICS** shortcut to display the Customization Parameters panel.

Step 2. At the Command ===> prompt, enter **F CDEVENTS** to find the CDEVENTS parameter group.

The parameter group list is scrolled to display the $RF CDEVENTS parameter group.

Step 3. Enter **U** beside the listed $RF CDEVENTS parameter group.

The Initialization Parameters panel for the parameter group is displayed, as shown in Figure 16-7.

Figure 16-7. Initialization Parameters Panel

```
SOLVPROD-------------- ICS : Initialization Parameters -------------Page 1 of 1
Command ===>                                                   Function=Update

.- CDEVENTS - CONNECT:Direct Event Log Options -------------------------------.
|                                                                              |
| Are the following CONNECT:Direct events to be logged:                        |
|   WTOs? ...................... NO_       (default is YES)                   |
|   Successful Steps? .......... YES       (default is YES)                   |
| Are the following additional messages to be logged:                          |
|   Submit Details?             NO         (default is YES)                   |
'------------------- Notes Window ----------------------------------------------'

.- Notes ---------------------------------------------------------------------.
| These options allow you to limit the type of CONNECT:Direct events written  |
| to the file transfer log.  They are effective only if file transfer         |
| logging is enabled in the FTLOGS parameter group.                            |
|  WTOs specifies if CONNECT:Direct WTOs are to be included.                   |
|  Successful Steps specifies if process steps that complete with a zero       |
|  return code are to be included.                                             |
|  Submit Details specifies if message RFCDEV03 is to be generated.  This      |
|  message contains process submission information for other process related  |
|  events (such as Copy Step Ended, Process Ended, and so on).                 |
'------------------------------------------------------------------------------'
 F1=Help      F2=Split     F3=File      F4=Save      F5=ILog      F6=Action
                           F9=Swap                                F12=Cancel
```

Step 4. See the Notes window for a description of the fields, and make changes accordingly.

Step 5. With the changes made, perform one of the following:

If you want to action the changes …	Press …
Immediately	F6 (Action). The changes are not saved, and are not in effect the next time the region is started.
Immediately and also every time the region starts up	F6 (Action), then press F3 (File) to save the changes.
Only on subsequent startups of the region	F3 (File) to save the changes.

17

Defining and Maintaining Calendars

You use a calendar to define date criteria that you can use to specify file transfer schedules.

The chapter contains the following topics:

- Using Calendars
- Creating a Calendar
- Creating a Calendar Keyword
- Associating a Calendar Keyword with a Date
- Creating a Calendar Criteria Definition

Using Calendars

You can create different calendars for different purposes. Within each calendar, you can associate keywords to particular dates. By using keywords, you can create complex date criteria (for example, all public holidays except when it falls on a Tuesday).

Use calendars to create date criteria by completing the following tasks:

1. Enter the **/ASADMIN.CC** path to access the Calendar Criteria menu.
2. From the Calendar Criteria Menu, enter **C** to display the Calendar List panel, from which you can create your calendars (see the section, *Creating a Calendar*, on page 17-3).
3. From the Calendar Criteria Menu, enter **K** to display the Keyword List panel, from which you can create calendar keywords (see the section, *Creating a Calendar Keyword*, on page 17-4).
4. After you created a keyword, you can associate the keyword to particular dates of a calendar (see the section, *Associating a Calendar Keyword with a Date*, on page 17-4).
5. From the Calendar Criteria Menu, enter **CR** to display the Calendar Criteria List panel, from which you can create date criteria (see the section, *Creating a Calendar Criteria Definition*, on page 17-7).

Creating a Calendar

Create a calendar as follows:

Step 1. Enter the **/ASADMIN.CC.C** path to display the Calendar List panel.

Step 2. Press F4 (Add) to display the Calendar Definition panel.

Step 3. Specify the name of the calendar and provide a short description for the calendar.

Step 4. Press F3 (File) to create the calendar.

To view the calendar, enter **V** beside it. Your calendar will look like the example in Figure 17-1.

Figure 17-1. Calendar

```
SOLVPROD----- Automation Services : Calendar Year Display --------$CALNDAR-0000
Command ===>                                                   Scroll ===> CSR

                                                                      S/=Select
     Calendar Name ... AUCALENDAR - Calendar for Australia
     Year ............ 1997
                                1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 3 3
    Month      1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    ---------  -------------------------------------------------------------
    January    . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    February   . . . . . . . . . . . . . . . . . . . . . . . . . . .
    March      . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    April      . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    May        . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    June       . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    July       . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    August     . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    September  . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    October    . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    November   . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    December   . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    **END**
 F1=Help      F2=Split     F3=Exit                   F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap     F10=PrevYear F11=NextYear
```

The calendar is displayed as a grid, with the months forming the rows, or horizontal lines, and the dates forming the columns, or vertical lines. Weekends are highlighted on monochrome terminals, or are shown in a different color to weekdays.

The panel also provides the S action code, and the F10 (PrevYear) and F11 (NextYear) function keys. Try them and see what happens.

Creating a Calendar Keyword

You use a calendar keyword to represent one or more dates in a calendar. For example, you can create a keyword, PUBHOLNA, for public holidays.

Create a calendar keyword as follows:

Step 1. If you are not yet on the Keyword List panel, enter the **/ASADMIN.CC.K** path to display the panel.

Step 2. Press F4 (Add) to display the Keyword Definition panel.

Step 3. Specify the name of the keyword and provide a short description for the keyword.

Figure 17-2 shows an example.

Figure 17-2. Creating a Calendar Keyword

```
SOLVPROD------- Automation Services : Keyword Definition ---------$CALNDAR-0000
Command ===>                                                      Function=ADD


Keyword Name ......... PUBHOLNA

Short Description .... National public holiday_______
Long Description ..... ____________________________________________________________
                       ____________________________________________________________
```

Step 4. Press F3 (File) to create the keyword.

Associating a Calendar Keyword with a Date

Associate a calendar keyword with a date in a calendar as follows:

Step 1. If you are not yet on the Keyword List panel, enter the **/ASADMIN.CC.K** path to display the list of defined keywords.

Step 2. Enter **R** beside the keyword you want to associate with a date.

The Keyword References for Year panel is displayed.

Step 3. To associate a keyword to a date, follow the steps shown in the example in Figure 17-3. The steps associate the PUBHOLNA keyword to 25 December 2000 on the AUCALENDAR calendar.

Figure 17-3. Associating a Keyword with a Date (Sheet 1 of 2)

```
SOLVPROD-- Automation Services : Keyword References for Year -----$CALNDAR-0000
Command ===>                                                   Scroll ===> CSR

                                                                      S/=Select
     Keyword ... PUBHOLNA - National public holiday
     Year ...... 2000
                                1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 3 3
    Month      1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    ---------  -------------------------------------------------------------
    January    . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    February   . . . . . . . . . . . . . . . . . . . . . . . . . . .
    March      . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    April      . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    May        . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    June       . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    July       . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    August     . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    September  . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    October    . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    November   . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
S   December   . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    **END**
 F1=Help      F2=Split     F3=Exit      F4=Return    F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap      F10=PrevYear F11=NextYear
```

Enter **S** beside the required month.

```
SOLVPROD-- Automation Services : Keyword References for Month ----$CALNDAR-0000
Command ===> L 25                                              Scroll ===> CSR

                                                         S/U=Update B=Browse
     Keyword ... PUBHOLNA - National public holiday
     Year ...... 1997
     Month ..... December

      Day   Julian  Cnt  Calendars 1 to 4
     01 MON   335    0
     02 TUE   336    0
     03 WED   337    0
     04 THU   338    0
     05 FRI   339    0
     06 SAT   340    0
     07 SUN   341    0
     08 MON   342    0
     09 TUE   343    0
     10 WED   344    0
     11 THU   345    0
     12 FRI   346    0
     13 SAT   347    0
 F1=Help      F2=Split     F3=Exit      F4=Return    F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap                   F11=Right
```

Enter **L 25** to locate the date.

```
SOLVPROD-- Automation Services : Keyword References for Month ----$CALNDAR-0000
Command ===>                                                   Scroll ===> CSR

                                                         S/U=Update B=Browse
     Keyword ... PUBHOLNA - National public holiday
     Year ...... 1997
     Month ..... December

      Day   Julian  Cnt  Calendars 1 to 4
U    25 THU   359    0
     26 FRI   360    0
     27 SAT   361    0
     28 SUN   362    0
```

Enter **U** beside the date.

Figure 17-3. Associating a Keyword with a Date (Sheet 2 of 2)

```
SOLVPROD--- Automation Services : Keyword References for Day -----$CALNDAR-0000
Command ===>                                                   Scroll ===> CSR

                                                   S/R=Reference Switch B=Browse
     Keyword     PUBHOLNA - National public holiday
     Day ....... THU 25

     Calendar Name   Description
R    AUCALENDAR      Calendar for Australia
```

Enter **R** beside the calendar to which you want to associate the keyword.

```
SOLVPROD--- Automation Services : Keyword References for Day -----$CALNDAR-0000
Command ===>                                                   Scroll ===> CSR

     Keywor
     Year .
     Month ..... December
     Day ....... THU 25

     Calendar Name   Description
     AUCALENDAR      Calendar for Australia          **REFERENCED**
    **END**
```

The keyword is associated with the date in the selected calendar, as indicated by **REFERENCED**. (You can dissociate the keyword from the calendar by applying the R action again.)

To view the calendar with the associated keyword, enter **/ASADMIN.CC.C** at the Command ===> prompt, then enter **V** beside the calendar. Your calendar will look like the example in Figure 17-4. Any date that has a keyword entered against it has a Y instead of a dot.

Figure 17-4. Calendar with Associated Keyword

```
SOLVPROD----- Automation Services : Calendar Year Display --------$CALNDAR-0000
Command ===>                                                   Scroll ===> CSR

                                                                   S/=Select
     Calendar Name ... AUCALENDAR - Calendar for Australia
     Year ........... 1997
                                 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 3 3
    Month      1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    ---------  -------------------------------------------------------------
    January    . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    February   . . . . . . . . . . . . . . . . . . . . . . . . . . .
    March      . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    April      . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    May        . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    June       . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    July       . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    August     . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    September  . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    October    . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    November   . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    December   . . . . . . . . . . . . . . . . . . . . . . . . . Y . . . . . .
    **END**
 F1=Help      F2=Split     F3=Exit                   F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap     F10=PrevYear F11=NextYear
```

Creating a Calendar Criteria Definition

You use calendar criteria to define complex date or day requirements. For an example, see the next section, *Specifying the Criteria Expression—Example*.

Create a calendar criteria definition as follows:

Step 1. If you are not yet on the Calendar Criteria List panel, enter the **/ASADMIN.CC.CR** path to display the panel.

Step 2. Press F4 (Add) to display the Calendar Criteria panel.

Step 3. Specify the name of the criteria, provide a short description for the criteria, and identify the calendar on which the criteria is based.

Step 4. Specify the expression that defines your criteria. You can enter a question mark (?) to list the valid values for the fields.

Step 5. Press F3 (File) to create the criteria definition.

Specifying the Criteria Expression—Example

Figure 17-5 shows a criteria definition that selects Mondays as long as it is not a public holiday, as identified by the PUBHOLNA keyword.

Figure 17-5. Calendar Criteria—Example

```
SOLVPROD--------- Automation Services : Calendar Criteria ---------Function=ADD
Command ===>                                                  Scroll ===> CSR

. Calendar Criteria Definition ----------------------------------------------.
| Name ......... MONNOTPUBHOL                                                |
| Description .. Mondays but not public holidays                             |
| Calendar ..... AUCALENDAR    Calendar for Australia                        |
'----------------------------------------------------------------------------'
. Calendar Criteria Expression ----------------------------------------------.
|                                                D=Delete I=Insert R=Repeat |
|      "(" Keyword  Opr Keyword Value                              ")" Bool  |
|          DAY      EQ  'MON'                                          AND   |
|          PUBHOLNA EQ  'N'                                                  |
```

18

Producing Reports

Reporting enables you to extract information about the logged file transfer activities.

The chapter contains the following topics:

- About Reports
- Viewing Reports and Searching the Database
- Generating Exception Reports
- Searching the Events Database
- Printing Reports
- Extracting Data to a File
- Defining Printed Reports
- Troubleshooting for the Reporting Facility

About Reports

NetMaster for File Transfer has a reporting function, which allows you to view your file transfer activity from a historical perspective.

The reporting function allows you to:

- Record file transfer events to an events database
- Display and print predefined reports on the recorded data
- Generate reports based on various search criteria
- Generate custom reports
- Generate exception reports to identify expected events that are not found in the events database
- Archive data to a sequential file as character-separated values (CSV)
- Extract data to a sequential file as character-separated values on an ad hoc basis for transfer to a PC file and processing by other data analysis and reporting tools

To enable NetMaster for File Transfer to collect the events, use the Initialization Parameters panel (see the section, *Task 13—Implementing Event Recording and Reporting*, on page 5-65 for details).

Viewing Reports and Searching the Database

The reporting options available from the History Menu allow you to view reports currently defined to your region. The following predefined reports are available:

- Event reports
  - All file transfer events
  - Failed file transfers
  - File transfer results
  - Summary reports
- Schedule reports
  - Completed schedules
  - Failed schedules

The search facility also allows you to define your own search criteria to obtain specific information from the events database. The following options are available for searching:

- Perform Custom Search
- Search File Transfers
- Search Schedules

The reporting and search options for file transfer events and schedules are accessed through different options on the History Data menu (see Figure 18-1).

Figure 18-1. The History Data Menu

```
Select Option ===>

   B  - Browse Event and Trans
   P  - Print Event and Transfer Details or Summaries
   EX - Extract File Transfer Events to Dataset
   BS - Browse Schedule Details
   PS - Print Schedule Details o
   ER - File Transfer Exception
   X  - Exit

Extract Dataset ... ____________________________________________ ( Opt EX )
                    Dataset must be sequential with RECFM=VB & LRECL>=600
                    Extract to use ( , ) as field separator
```

To view reports or perform searches for file transfer events select Option B

To view reports or perform searches for file transfer schedules select Option BS

Viewing Predefined Reports for File Transfer Events

To access file transfer event reports and searches, perform the following steps:

Step 1. Enter the **/FTHIST** shortcut.

The History Data menu is displayed (see Figure 18-1 on page 18-3).

Step 2. At the Select Option ===> prompt, enter **B**.

A selection list is displayed (see Figure 18-2).

Figure 18-2. Selection List for File Transfer Events Reports and Searches

```
Command ===>                                                Scroll ===> PAGE

                                                         S/=Select I=Information
    Description
    List All File Transfer Events
    List Failed File Transfers
    List File Transfer Results
    Perform Custom Search
    Search File Transfers
    Transfers by Mailbox ID
    Transfers by Source Address
    Transfers by Target Address
    Transfers by Transfer ID
    Transfers by User ID
    **END**
```

The following predefined reports are available:

- All File Transfer Events report lists all events (that is, all START, END, and FAILURE events).
- Failed File Transfers report lists failed events (that is, all FAILURE events).
- File Transfer Results report lists the final results of the transfers (that is, all END and FAILURE events, but excluding those failures that were subsequently retried).
- Transfers by … reports list the last transfer events summarized:
  - Mailbox ID
  - Source Address
  - Target Address
  - Transfer ID
  - User ID

To generate these reports, enter **S** beside the predefined report type that you require. The corresponding type of report is displayed.

See the following sections for further details of these reports.

Viewing All File Transfer Events

If you selected All File Transfer Events, then the File Transfer : All Events panel is displayed (see Figure 18-3). To display additional information for an event, press F11 (Right). Alternatively, enter **S** beside an event to display further details for that event. You can then use the F5 (Previous) and F6 (Next) keys to scroll to the previous and next events in the list. Press F1 (Help) for information about these details.

You can sort events by a specific criterion by entering SORT at the Command ===> prompt. Select the criterion to form the full command, then press ENTER again to start sorting.

Figure 18-3. File Transfer : All Events Panel

```
SOLVPROD---------------- File Transfer : All Events ----------------1121/1926
Command ===>                                                  Scroll ===> PAGE

                                                                   S/=Select
    Event    Event        Transfer        Step                     Duration
    Time     Date         ID              Name     Status     Bytes  (seconds)
    11:26:28 13-APR-2000  FTI1BSC(901)             FAILURE
    11:26:10 13-APR-2000  FTPXFER                  END      11.890K         1
    10:57:44 13-APR-2000  FTI1BSC(916)             END      16.530K        57
    10:56:47 13-APR-2000  FTI1BSC(916)             START
    10:48:26 13-APR-2000  FTI1BSC(914)             FAILURE
    10:47:44 13-APR-2000  FTI1BSC(914)             START
    10:25:24 13-APR-2000  FTPXFER                  END       2.880K         1
    09:31:44 13-APR-2000  FTI1BSC(901)             FAILURE
    08:15:51 13-APR-2000  QXLU0003(27)    CPYLF    FAILURE
    08:15:46 13-APR-2000  QXLU0003(24)    CPYLF    FAILURE
    08:15:45 13-APR-2000  QXLU0002(23)    CPYLF    FAILURE
    08:12:35 13-APR-2000  QXLU0002(23)    CPYLF    START
    08:12:35 13-APR-2000  QXLU0001(22)    CPYLF    START
    06:52:11 13-APR-2000  FTPXFER                  END      24.720K         1
    06:52:01 13-APR-2000  FTPXFER                  END      25.338K         1
    06:51:30 13-APR-2000  FTPXFER                  END      91.840K         1
    06:51:28 13-APR-2000  FTPXFER                  END      43.760K         1
    22:36:16 12-APR-2000  FTI1BSC(901)             FAILURE
    22:35:08 12-APR-2000  QXLU0003(44)    CPYLF    FAILURE
    22:25:48 12-APR-2000  QXLU0002(43)    CPYLF    FAILURE
    22:25:47 12-APR-2000  QXLU0003(44)    CPYLF    START
 F1=Help      F2=Split     F3=Exit                  F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap                  F11=Right
```

Viewing Failed File Transfer Events

If you selected Failed File Transfers, then the File Transfer : Failed File Transfers panel is displayed. The report on this panel is in the same format as that on the NetMaster for File Transfer : All Events panel (see Figure 18-3).

You can sort events by a specific criterion by entering SORT at the Command ===> prompt. Select the criterion to form the full command, then press ENTER again to start sorting.

Viewing the Final Results of File Transfers

If you selected File Transfer Results, then the File Transfer : File Transfer Results panel is displayed. The report on this panel is in the same format as that on the File Transfer : All Events panel (see Figure 18-3).

You can sort events by a specific criterion by entering SORT at the Command ===> prompt. Select the criterion to form the full command, then press ENTER again to start sorting.

Viewing Summarized Reports

If you selected any of the Transfers by… reports, the Transfers by… panel is displayed. The information displayed depends on the report you select. The transfers are summarized by either mailbox ID, Source Address, Target Address, Transfer ID, or User ID (See Figure 18-4).

Figure 18-4. Summary Reports

```
SOLVPROD-------- File Transfer : Transfers by Source Address ------------------
Command ===>                                                   Scroll ===> PAGE

                                                 S/=Transfers F=Failed R=Results
    Source Address         Last Event              Last Event Type
    BARTOK                 29-MAR-2000 16:28:55    FAILURE
    CD320DE1               28-MAR-2000 12:52:54    FAILURE
    CD320QA1               28-MAR-2000 11:24:08    FAILURE
    CD320QA1.A11           26-MAR-2000 16:23:00    END
    CD400                  28-MAR-2000 16:41:26    FAILURE
    CD410DE1               29-MAR-2000 08:15:05    END
    CD410DE1.CRA           23-MAR-2000 12:17:08    FAILURE
    CD410QA1               27-MAR-2000 16:37:27    END
    DECM1                  29-MAR-2000 12:24:54    END
    DE1P1                  27-MAR-2000 13:44:47    END
    **END**
```

You can issue commands against a line item to display more information. The commands display panels filtered for the selected Source Address, Target Address, Transfer ID, or User ID. The commands are:

- S—displays the List All File Transfer panel
- F—displays the List Failed File Transfers panel
- R—displays the List File Transfer Results panel

Viewing Predefined Reports for Schedules

To access file transfer event reports and searches, do this:

Step 1. Enter the **/FTHIST** shortcut to display the History Data menu (see Figure 18-1 on page 18-3).

Step 2. At the Select Option ===> prompt, enter **BS**.

A selection list is displayed (see Figure 18-5).

Figure 18-5. Selection List for File Transfer Events Reports and Searches

```
Command ===>                                                  Scroll ===> PAGE

                                                        S/=Select I=Information
    Description
    List Schedules : Completed
    List Schedules : Failed
    Search Schedules
    **END**
```

The following predefined reports are available:

- Schedules : Completed report lists all completed schedules
- Schedules : Failed report lists all failed schedules

If you selected Schedules : Completed, the File Transfer : Completed Schedules panel is displayed (see Figure 18-6). The display shows a summary report of all completed schedules in the current system, including failed schedules. If you want to see a list of failed schedules only, select Schedules : Failed from the list of reports.

Figure 18-6. NetMaster for File Transfer : Completed Schedules Panel

```
SOLVPROD -------------- File Transfer : Completed Schedules -------------71/143
Command ===>                                                   Scroll ===> PAGE

                                                        S/=Transfers F=Filters
    Event    Event        Schedule                 Total    Total   Total
    Time     Date         Name              Status Required Failed  Completed
    13:16:00 16-APR-2000  DBLANK            FAIL   170      0       0
    04:00:10 15-APR-2000  FTFR              OK     1        0       1
    04:00:05 15-APR-2000  FTFR1             OK     1        0       1
    18:02:40 14-APR-2000  FTPIN             FAIL   100      0       50
    18:02:21 14-APR-2000  FTPALL            OK     100      12      100
    18:02:09 14-APR-2000  FTPOUT            FAIL   100      0       50
    12:01:01 14-APR-2000  KBFTFR3           OK     2        0       2
    11:55:00 14-APR-2000  KBFTFR2           FAIL   999      0       0
    11:41:00 14-APR-2000  DLC               FAIL   2        0       0
    18:07:40 13-APR-2000  FTPALL            OK     100      0       100


 F1=Help      F2=Split     F3=Exit                   F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap                  F11=Right
```

To view the file transfer events associated with a particular schedule:

Step 1. Enter **S** beside the required schedule. The File Transfer : File Transfer Events panel is displayed.

Step 2. Enter **S** beside the required file transfer event to view details of the event in one screen display.

To view the filters associated with a particular schedule:

Step 1. Enter **F** beside the required schedule. The File Transfer : File Filters panel is displayed.

Step 2. Enter **S** beside the required filter to display the file transfer events monitored by this filter.

Step 3. Enter **S** beside the required file transfer event to view details of the event in one screen display.

Generating Exception Reports

The ER - File Transfer Exception Reporting option on the History Data menu allows you to generate exception reports to identify expected events that are not found in the events database.

Exception reports are based on predefined filters. The filter can be an existing FTSCHD file filter or an exception report filter.

Defining Exception Report Filters

To define an exception file filter do this:

Step 1. Enter the **/FTHIST.ER.F** path. The Exception Report Filter List is displayed.

You can also define exception report filters through the Administration Menu (/FTADMIN.E).

Step 2. Press F4 (Add). The Exception Report Filter panel is displayed.

Step 3. Name the filter and provide a brief description.

Step 4. In the Filter window specify the expected transfers.

As with schedules, filters can be stored in a CTL file. For information about specifying filters in a CTL file, see the section, *Defining a CTL File to a Schedule*, on page 19-4.

You can view CTL files directly from Exception Report Filter panel.

Step 5. When you have completed the definition, press F3 (File) to save it to the knowledge base.

Generating Exception Reports

To generate an exception report, do this:

Step 1. Enter the **/FTHIST.ER** path to access the Exception Reporting Menu.

Step 2. Select the appropriate option for the type of filter you want to use for your report:

Select Option …	To List …
F	Exception report filters
S	FTSCHD file filters

Step 3. Enter **E** beside the appropriate filter. The Exception Report Confirmation panel is displayed.

Step 4. Enter the appropriate time period and press F6 (Confirm) to generate the report (see Figure 18-7).

An exception report is generated only if the expected events are not found in the events database.

Figure 18-7. Exception Report

```
SOLVPROD-------------- File Transfer : Exception Report ----Columns 00001 00079
Command ===>                                                   Scroll ===> PAGE

********************************** TOP OF DATA **********************************
Exception Report:
=================
Interval Checked:
From................... 30-MAR-2000 08:04
To .................... 30-MAR-2000 11:04
------
Exception Details:
==================
FILTER                                                    TYPE   REQD   DONE
                                                                  CNT    CNT
SYS1.DAE                                                  SRC     100      0
****************************** BOTTOM OF DATA ******************************
```

Searching the Events Database

The search facility allows you to define your own search criteria to obtain specific information from the EVNTDB events database. The following options are available for searching:

- Perform Custom Search
- Search File Transfers
- Search Schedules

See the following sections, *Searching for File Transfer Events*, on page 18-11 and *Performing a Custom Search*, on page 18-13 for further details of these reports.

Searching for File Transfer Events

To search for file transfer events, perform the following steps:

Step 1. Enter the **/FTHIST.B** path. A selection list of reports and searches is displayed (see Figure 18-2).

Step 2. Select Search File Transfers.

The Search Criteria panel is displayed (see Figure 18-8), with entry fields for the predefined search criteria.

Figure 18-8. Search Criteria Panel

```
SOLVPROD------------- File Transfer : Search Criteria -------------------------
Command ===>                                                     Function=Search

Transfer Status ........... _______  (START, END or FAILURE)
From Date ................. ___________  From Time ... ________
To Date ................... ___________  To Time ..... ________

Byte Count Over ........... __________  (Bytes)
          Under ........... __________  (Bytes)
Duration Over ............. _____  (Seconds)
Show Retries .............. _  (Y/N - Default is Y)

The following search fields are Case-Sensitive...

User ID ................... ________________________________
Transfer ID ............... __________________

Source Node/Address ........ ________________
Source File Name ........... ______________________________________________

Target Node/Address ........ ________________
Target File Name ........... ______________________________________________
 F1=Help      F2=Split     F3=Exit      F4=Save      F5=Load      F6=Action
                           F9=Swap
```

Step 3. Enter values for your search of the database, or press F5 (Load) to retrieve previously saved criteria.

Note

Press F1 (Help) for information about any of these fields.

Step 4. Press F6 (Action).

The NetMaster for File Transfer : Event Search panel is displayed. The report on this panel is in the same format as that on the NetMaster for File Transfer : All Events panel (see Figure 18-3).

Note

The most recent search criteria values are retained and can be used if you want to print a report. You can also save the criteria by pressing F4 (Save) from the Search Criteria panel. You can save multiple search criteria and retrieve them later for use.

Searching for File Transfer Schedules

To search for file transfer schedules, follow these steps:

Step 1. Enter the **/FTHIST.BS** path. A selection list of reports and searches is displayed.

Step 2. Select Search Schedules from the selection list of reports.

The Search Criteria panel is displayed as shown in Figure 18-9.

Figure 18-9. The Schedules Search Criteria Panel

```
SOLVPROD------------- File Transfer : Search Criteria -------------------------
Command ===>                                                   Function=Search




System Name ...............+ ________
Version ...................+ ____
Schedule Name .............+ _____________  ( Name or Mask )
Schedule Status ...........+ ____          ( OK, FAIL or ALL )

From Date ................. ___________
     Time ................. _____
  To Date ................. ___________
     Time ................. _____



 F1=Help      F2=Split     F3=Exit      F4=Save      F5=Load      F6=Action
                           F9=Swap
```

Step 3. Enter values for your search, or press F5 to select a previously saved search criteria. The default values for System Name and Version are the values for the current system image.

Note

Press F1 (Help) for information about any of these fields.

Step 4. Press F6 to start the search.

The NetMaster for File Transfer : Schedules Search Result panel is displayed.

Note

The most recent search criteria values are retained. You can also save the criteria by pressing F4 (Save) from the Search Criteria panel. You can save multiple search criteria and retrieve them later for use.

Performing a Custom Search

The Perform Custom Search option enables you to define your own search criteria by using the fields in the events database.

To search for file transfer events by specifying your own search criteria, do this:

Step 1. On the selection list for reports and searches (see Figure 18-2), select Perform Custom Search.

The NCL/EF : Database Search Criteria panel is displayed (see Figure 18-10).

Figure 18-10. NCL/EF : Database Search Criteria Panel

```
                                                    D=Delete I=Insert R=Repeat
   "("   Field          Opr  Value                              Gen ")"   Bool
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
   ___ + ____________ + ___  ________________________________ + ___ ___ + ___
F1=Help      F2=Split     F3=Exit      F4=Save      F5=Load      F6=Action
                          F9=Swap
```

Note

You can list the fields in the events database by entering **?** in the Field field on the NCL/EF : Database Search Criteria panel. The format of the valid values for these fields can be found in an off-loaded CSV archive of the events database.

The following fields are case-sensitive: $RFFAILDESC, $RFSRCADDR, $RFSRCFNAME, $RFTGTADDR, $RFTGTFNAME, $RFUSER, and $RFXFRID.

Step 2. Complete the columns for as many criteria as you need, or press F5 (Load) to retrieve previously saved criteria.

Step 3. Press F6 (Action) to perform the search.

The NetMaster for File Transfer : EVNTDB Search panel is displayed. The report on this panel is in the same format as that on the NetMaster for File Transfer : All Events panel (see Figure 18-3).

Note

If you want to save the criteria, press F4 (Save) from the Search Criteria panel. You can save multiple search criteria and retrieve them later for use.

Examples of Custom Searches

The following examples could help you customize your own searches of the events database.

Example 1

This is an example of search criteria that produced a list of all CONNECT:Direct file transfers that abended with abend code XCPR01.

Figure 18-11. Custom Search of File Transfer Events—Example 1

```
SOLVPROD----------------- NCL/EF : Database Search Criteria ------------------
Command ===>                                                   Function=Search

                                                     D=Delete I=Insert R=Repeat
    "("   Field          Opr  Value                             Gen ")"  Bool
        + $RFPRODUCT   + EQ   CD                              +         + AND
        + $RFABENDCODE + EQ   XCPR01                          +         +
        +              +                                      +         +
        +              +                                      +         +
        +              +                                      +         +
        +              +                                      +         +
        +              +                                      +         +
```

Example 2

This is an example of search criteria that produced a list of file transfers, started between 3:00 p.m. and 4:00 p.m. on 18th May 1998, that abended with abend code XCPR01.

Figure 18-12. Custom Search of File Transfer Events—Example 2

```
SOLVPROD ---------------- NCL/EF : Database Search Criteria ------------------
Command ===>                                                   Function=Search

                                                        D=Delete I=Insert R=Repeat
    "("   Field          Opr  Value                            Gen ")"   Bool
        + $RFSTARTTIME + GE   150000                          +         + AND
        + $RFSTARTTIME + LE   160000                          +         + AND
        + $RFSTARTDATE + EQ   18-MAY-1998                     +         + AND
        + $RFABENDCODE + EQ   XCPR01                          +         +
        +              +                                      +         +
```

Actions on the NCL/EF : Database Search Criteria Panel

For information about the actions available on this panel, press F1 (Help).

Printing Reports

The reporting options allow you to print reports currently defined to your region.

Caution

Generating a printed report may consume a lot of CPU resources. Where possible, perform this action when the system is not busy.

Printing Reports for File Transfer Events

To display a list of predefined reports and print a selected report for file transfer events, complete the following steps:

Step 1. From the History Data menu, select **P** (see Figure 18-1 on page 18-3).

The Reports List is displayed (see Figure 18-13).

Figure 18-13. File Transfer Events Printed Reports List

```
SOLVPROD----------------- File Transfer : Reports List ----------------------18
Command ===>                                                   Scroll ===> PAGE

                                                          S/=Select I=Information
    Description
    List All File Transfer Events: Detailed
    List All File Transfer Events: Summary
    List All Transfers by field: Detailed
    List All Transfers by field: Summary
    List Failed File Transfers: Detailed
    List Failed File Transfers: Summary
    List Failed Transfers by field: Detailed
    List Failed Transfers by field: Summary
    List File Transfer Results: Detailed
    List File Transfer Results: Summary
    List Transfer Results by field: Detailed
    List Transfer Results by field: Summary
    Perform Custom Search: Detailed
    Perform Custom Search: Summary
    Search File Transfers: Detailed
    Search File Transfers: Summary
    **END**
```

Step 2. Enter **S** beside the listed report that you want to print.

The PSM : Confirm Printer panel is displayed. For information about setting up printers, see *Task 5—Implementing Printers*, on page 5-20.

Step 3. Press F6 (Confirm) to confirm the details of the print job.

You are returned to the Report Writer : Report List panel, where a message is displayed indicating that the print job has been submitted to the print queue.

Note

You can add your own report definitions to this list. For details of how to do this, see *Defining Printed Reports*, on page 18-20.

Printing Reports for File Transfer Schedules

To display a list of predefined reports and print a selected report for file transfer schedules, complete the following steps:

Step 1. From the History Data menu, select **PS** (see Figure 18-1 on page 18-3).

The Reports List is displayed (see Figure 18-14).

Figure 18-14. File Transfer Schedule History Printed Reports List

```
SOLVPROD---------------- File Transfer : Reports List -----------------------6
Command ===>                                                   Scroll ===> PAGE

                                                          S/=Select I=Information

    Description
    List Schedules Completed : Detailed
    List Schedules Completed : Summary
    List Schedules Failed : Detailed
    List Schedules Failed : Summary
    Search Schedules : Detail
    Search Schedules : Summary
    **END**
```

Step 2. Enter **S** beside the listed report that you want to print.

The PSM : Confirm Printer panel is displayed.

Step 3. Press F6 (Confirm) to confirm the details of the print job.

You are returned to the Report Writer : Report List panel, where a message is displayed indicating that the print job has been submitted to the print queue.

Note

You can add your own report definitions to this list. For details of how to do this, see *Defining Printed Reports*, on page 18-20.

Checking the Print Queue

To check the print queue, at the Command ===> prompt on the Report Writer : Report List panel, enter **PQ**.

The PSM : Output Queue is displayed.

Actions available on this panel enable you to browse a report output, release a held report, or delete a print job from the printer queue.

For more information about using Report Writer functions, see the *Management Services Report Writer User's Guide.*

Extracting Data to a File

The EVNTDB events database contains the file transfer activity data. This database can be periodically archived in a character separated values (CSV) format for processing by external analysis and reporting tools. The period of time that data is kept online is defined by your system administrator. For more information, see the section, *Task 13—Implementing Event Recording and Reporting*, on page 5-65.

You can analyze file transfer activity and trends by reading the data extracted from the database in any standard analysis and reporting tool on a PC.

To extract the file transfer data on an ad hoc basis for purposes of analysis, complete the following steps:

Step 1. Allocate a sequential dataset with the following attributes:

RECFM	VB
LRECL	600
BLKSIZE	greater than or equal to 604

Step 2. Access the History Data menu (see Figure 18-1 on page 18-3).

Step 3. At the Select Option ===> prompt, type **EX** and, in the Extract Dataset field, specify the dataset name that you have just defined. Press ENTER.

The Extracts List is displayed (see Figure 18-15).

Figure 18-15. Extracts List Panel

```
SOLVPROD --------------- File Transfer : Extracts List ------------------------
Command ===>                                                   Scroll ===> PAGE

              Extract Destination DSN: AUDE0.DENM13.EVNTARC.TMP(+1)
                                                                  S/=Select
    Description
    Extract All File Transfer Events
    Extract Failed File Transfers
    Extract File Transfer Results
    Perform Custom Extract
    Search & Extract File Transfers
    **END**
```

Step 4. Select an extract option. Use the following table to help you decide which option to select:

To select fields to be extracted from …	Then select …
All file transfer events	Extract All File Transfer Events
Failed file transfers only	Extract Failed File Transfers
File transfer results only	Extract File Transfer Results
File transfers based on your own search criteria of the fields in the events database	Perform Custom Extract (See *Performing a Custom Search*, on page 18-13 for details on defining your own search.)
File transfers based on entry fields for predefined search criteria	Search and Extract File Transfers (See *Searching for File Transfer Events*, on page 18-11 for details on defining a search.)

The Fields List is displayed. By default, all fields are selected.

Step 5. Enter **U** beside the fields you want to exclude from the extract.

Alternatively, deselect all fields by entering **All U** at the Command ===> prompt, then enter **S** beside the fields you want to include in the extract.

Note

Commands you enter at the prompt override any other entries. You should execute any commands you enter at the prompt before making any other entries beside the field names.

Step 6. Press F6 (Action) to perform the extract.

Automation Services extracts the relevant records from the events database, EVNTDB, to the defined dataset, and presents them as CSV fields with a header.

Step 7. Transfer the defined dataset to your PC, and save it with a .TXT extension.

Step 8. Open the .TXT file by using your preferred PC application (for example, Microsoft Excel), and import this file as a .CSV file.

Step 9. Analyze your data by applying facilities such as graphs and charts, tables, and macros.

Note

Extraction copies but does *not* clear the records from the EVNTDB database.

Defining Printed Reports

To set up your own reports to print, you must define them to the NetMaster for File Transfer region.

There are two possible stages involved in defining these reports:

- Defining search criteria (optional)
- Defining report details

Defining Search Criteria (Optional)

If you want to define specific search criteria in addition to those available on the Report Writer : Report Description panel (see Step 2 in the next section, *Defining Report Details*, on page 18-21), complete the following steps:

Step 1. At an ===> prompt, enter **/CASCRIT**.

The CAS : Criteria Definition Menu is displayed.

Note

For details about using the CAS : Criteria Definition Menu, press F1 (Help) for online help. To file your definitions, press F3 (File).

Step 2. Specify your search criteria, and press F3 (File) to save your criteria.

Note

You use these criteria in Step 5 of the next section, *Defining Report Details*, on page 18-21.

Defining Report Details

To define your report details, complete the following steps:

Step 1. At an ===> prompt, enter **/REPORT.R.L;$RF** to list all printed reports defined to NetMaster for File Transfer.

The Report Writer : Report Definition List is displayed.

Step 2. Identify a listed report that has a format similar to the report you want to set up, and enter **C** beside it to make a copy.

The Report Writer : Report Description panel is displayed.

Step 3. In the Report Name field, enter your own report name.

Step 4. In the Description field, enter your report description.

Step 5. So that the report you are setting up will be available for use, ensure that the Group field has the value $RFREPORTING. Also ensure that the Report Exit field has the value $RFLORWX.

Step 6. If you have defined any specific search criteria (see the previous section, *Defining Search Criteria (Optional)*, on page 18-20), enter your values in the Criteria fields.

Step 7. Press F3 (File).

The Report Writer : Report Definition Component Menu is displayed, with a message that your report has been added.

Step 8. Change the title of your report by doing this:

a. Select the **RH** – Report Header option and press ENTER.

The Report Writer : Edit Report Header Layout panel is displayed.

b. To file the changes, press F3 (File).

The Report Writer : Report Definition Component Menu is displayed, with a message that your header has been updated.

c. Press F3 (Exit) until you reach the Report Writer : Report Definition Menu.

d. Select **R** - Reset Report Cache to immediately activate the new report definition.

Troubleshooting for the Reporting Facility

The reporting facility is dependent on the events database, EVNTDB. It cannot operate in either of the following cases:

- The EVNTDB database has not been allocated.
- The EVNTDB database is full.

In either case an error message is displayed.

If the EVNTDB Database Has Not Been Allocated

If the error message says that the EVNTDB database has not been allocated, then you need to allocate this database before reselecting a reporting option.

See the section, *Task 13—Implementing Event Recording and Reporting*, on page 5-65 for information about allocating the EVNTDB database.

If the EVNTDB Database Is Full

If the error message says that logging has stopped, this may be because the EVNTDB database is full. If automatic reorganization is not set, you need to complete the following steps:

Step 1. Check the activity log (**=H.L**) for further messages about what is happening.

Step 2. Extract the data currently in the EVNTDB database.

Step 3. If the EVNTDB database is full, delete and redefine the EVNTDB database.

See the message help (F1) for details of how to perform these steps.

If the Automatic Reorganization Fails

If the error message says that the automatic reorganization has failed, you may need to redo the reorganization. The reorganization occurs in two phases, an unload phase and a reload phase. The error message gives details of where the reorganization failed and the required action.

There are two ways to fix a failed reorganization: by using a batch job or by using the EVENTLOG parameter group. These methods are described below.

Fixing a Failed Reorganization via a Batch Job

To fix a failed reorganization via a batch job, follow these steps:

Step 1. From the error message determine the phase of the reorganization when the failure occurred.

Step 2. Issue the command:

```
DEALLOC DD=EVNTDB
```

If the failure occurred during the UNLOAD phase complete Step 3, otherwise skip this step and go to Step 4.

Step 3. Submit a batch job that executes an IDCAMS REPRO, for example:

```
REPRO INDATASET(EVNTDB dataset name)
      OUTDATASET(Reorg dataset name)
```

For information about the dataset attributes, see the *Unicenter Mainframe Installation and Setup Instructions*.

Note

Allocate enough space for the REORG dataset to contain all the records from the EVNTDB.

Step 4. Submit a batch job to define a new EVNTDB database (optionally giving it more space). For information about the datatset attributes, see the *Unicenter Mainframe Installation and Setup Instructions*.

Step 5. Submit a batch job that executes an IDCAMS REPRO, for example:

```
REPRO INDATASET(EVNTSEQ dataset name from UNLOAD phase)
      OUTDATASET(new EVNTDB dataset name)
```

For information about the datatset attributes, see the *Unicenter Mainframe Installation and Setup Instructions*.

Step 6. When the batch jobs complete successfully, update the EVENTLOG parameter group from the Customization Parameters panel (/ICS shortcut) specifying the following parameters:

a. In the Enable Event Logging field, enter **YES.**

b. In the EVNTDB Database Name field, enter the EVNTDB dataset name used in Step 5.

c. Leave the EVNTSEQ Reorg Dataset field blank.

Step 7. Press F6 (Action) to apply the changes, clear the reorganization lock, and reinitialize the event logging environment.

Step 8. If you require automatic reorganization, specify a dataset name in the EVNTSEQ Reorg Dataset field and press F3 (File) to save the parameter settings.

Fixing a Failed Reorganization via the EVENTLOG Parameter Group

To fix a failed reorganization via the EVENTLOG parameter group, follow these steps:

Step 1. From the error message determine the phase of the reorganization when the failure occurred.

If the failure occurred during the UNLOAD phase complete Step 2, otherwise go straight to Step 3.

Step 2. Update the EVENTLOG parameter group from the Customization Parameters panel (/ICS shortcut) specifying the following parameters:

a. In the Enable Event Logging field, enter **NO**
b. In the EVNTDB Database Name field, enter the EVNTDB dataset name
c. In the EVNTSEQ Reorg Dataset field, enter the EVNTSEQ dataset name

Note

Allocate enough space for the reorganization dataset to contain all the records from the EVNTDB database.

Press F6 (Action) to unload the EVNTDB database to the EVNTSEQ reorganization dataset.

Step 3. Submit a batch job to define a new EVNTDB database (optionally giving it more space). For information about the datatset attributes, see the *Unicenter Mainframe Installation and Setup Instructions*.

Step 4. Update the EVENTLOG parameter group from the Customization Parameters panel (/ICS shortcut) specifying the following parameters:

a. In the Enable Event Logging field, enter **YES**.

b. In the EVNTDB Database Name field, enter the new EVNTDB dataset name defined in Step 3.

c. In the EVNTSEQ Reorg Dataset field, enter the ENVTSEQ dataset name from the UNLOAD phase.

Press F6 (Action) to reload the EVNTSEQ from the EVNTDB, clear the reorganization lock, and reinitialize the event logging environment

Step 5. Press F3 (File) to save the current parameter settings.

19

Advanced Features

This chapter describes advanced features of the NetMaster for File Transfer product.

The chapter contains the following topics:

- Using the $RMDBAPI Procedure to Manage File Transfer Resource Definitions
- Working with Externally Updateable Schedules

Using the $RMDBAPI Procedure to Manage File Transfer Resource Definitions

You can use the $RMDBAPI procedure to manage your file transfer resource definitions. The $RMDBAPI allows you to:

- Create resource definitions
- Delete resource definitions
- Copy resource definitions
- Retrieve information about resource definitions
- Activate file transfer rules
- Inactivate file transfer rules

The API can be used within an NCL procedure or as a command. For information regarding the syntax of the API, press F1 (Help), then press F11 (Index) to access the API online help.

Copying Resource Definitions—Example

You can copy a resource definition using the SERVICE=GET and SERVICE=CREATE operands. Use the GET operand to retrieve information about a resource definition. The retrieved values are stored in the &ZRMDB-prefixed variables. To copy the resource definition, use the CREATE operand and specify a new name for the definition.

Considerations

You cannot directly update existing resource definitions using the API. You can create a new resource, including any updates required, then delete the old resource.

If you delete a ruleset, the rules within the ruleset are also deleted. If the ruleset is active, the request is rejected.

Working with Externally Updateable Schedules

A control file (CTL file) is a dataset that contains file filter definitions used in a schedule to monitor file transfers. The CTL file can be created in any text editor and can be stored as an MVS PDS member or a sequential dataset. When specified in a schedule, the CTL file is read when the schedule is activated and is used to externally build the file filters. For information about specifying filters to schedules, see *Defining File Transfer Schedules*, on page 10-18.

By using a CTL file you can:

- Externally update file filters before a schedule is activated
- Share common filters by specifying the CTL file to more than one schedule
- Easily maintain common filters by updating the filters in one CTL file

The syntax of a CTL file is as follows:

```
FILTER NAME=Filename/Transfer ID(Required.  Case Sensitive)
       TYPE=SRC | TGT | ID(Required)
       NUMBER=1 | n (Optional n=999 (max) )
       TGTNODE=target node(Optional)
       SRCNODE=source node(Optional)
       MINSIZE=n (Optional  n=9999999999 (max) )
       MAXSIZE=n(Optional n=9999999999 (max) )
```

A CTL file must comply with these rules:

- The file should have a record length of 80 bytes.
- The file is not case sensitive except for the value of NAME= .
- To start a new filter entry, FILTER should be the first word on a new line. Any occurrence of the word FILTER that is not the first word of a line will be treated as a comment until the next valid FILTER is encountered.
- Any attribute that is repeated within a filter takes on the value of the last attribute specified. For example:

  ```
  FILTER NAME=X TYPE=SRC  MINSIZE=10 MAXSIZE=20 MINSIZE=15
  ```

  The value of MINSIZE is 15.

Defining a CTL File to a Schedule

When you create a CTL file you have to define it to a schedule. To define a CTL file to a schedule follow these steps:

Step 1. Enter the **/RADMIN.R.FTSCHD** path. The File Transfer Schedule List is displayed.

Step 2. Enter **U** beside the appropriate schedule name. The Panel Display List is displayed.

Step 3. Enter **S** beside File Filters. The File Filters panel for the schedule is displayed.

Step 4. Enter the name of the CTL file in the File Name/Transfer ID field.

Step 5. Enter CTL in the Type field.

Step 6. Press F3 (File) to save the changes to the schedule.

Viewing a CTL File

To view the contents of a CTL file follow these steps:

Step 1. Enter the **/RADMIN.R.FTSCHD** path. The File Transfer Schedule List is displayed.

Step 2. Select the required FTSCHD name. The Panel Display List is displayed.

Step 3. Select the FTSCHD File Filters panel description. The File Filters panel is displayed.

Step 4. Enter V beside the CTL file you want to view. The CTL file is displayed.

Checking a CTL File

When you have created the CTL file and specified it in a schedule, you can check the syntax and view the contents of the file. To check the syntax of a CTL file, follow these steps:

Step 1. Enter the **/RADMIN.R.FTSCHD** path to display the File Transfer Schedule List panel.

Step 2. Select the required FTSCHD name. The Panel Display List is displayed.

Step 3. Select the FTSCHD File Filters panel description. The File Filters panel is displayed.

Step 4. Enter **CHK** beside any file of type CTL. The syntax of the file is checked.

You should check the syntax of the file before a schedule is activated, as an invalid CTL file will prevent a schedule from being activated.

Note

It is recommended that you limit access to CTL files to authorized personnel only.

To view the contents of a CTL file, follow the steps described above to display the ResourceView : FTSCHD File Filters panel. Enter **V** beside the required file. The CTL file is displayed in the CAS : TEXT EDITOR.

Considerations

Filters are uniquely defined by all attributes. Duplicate filters are ignored. You can specify multiple instances of a filter in a CTL file with different attributes. If the multiple instances of the filter have the same attributes, the instances are considered duplicates and only the first instance of the filter is used.

20

Controlling the Use of FTP

This chapter describes how to control the use of FTP by using TCPaccess FTP server (previously known as the Network*IT* FTP server) and NetMaster for File Transfer policy rules.

The chapter contains the following topics:

- About File Transfers Using FTP
- About the TCPaccess FTP Server
- About TCPaccess FTP Policy Rule Sets
- Task 1—Defining a Policy Rule Set
- Task 2—Adding Policy Rules to a Rule Set
- Task 3—Activating a Policy Rule Set
- Viewing the Loaded Policy Rule Set
- Copying the Loaded Policy Rule Set
- FTP SAF Rule Considerations
- Setting Up Your SAF Qualifier

About File Transfers Using FTP

NetMaster for File Transfer manages and monitors various types of file transfer, including those using FTP.

Information must be provided to NetMaster for File Transfer by the monitored FTP server and/or client. The IBM server and client and the TCPaccess server and client provide only limited information. This limits the management and monitoring functionality that can be provided for FTP transfers using these servers and clients.

The TCPaccess FTP Server product is an FTP server and client that is specifically designed to work in conjunction with NetMaster for File Transfer. NetMaster for File Transfer provides a complete management and monitoring interface for FTP transfers that use a TCPaccess FTP server, with none of the limitations that apply to FTP transfers using other FTP servers and clients.

About the TCPaccess FTP Server

Note

A separate license is required to use the TCPaccess FTP feature of NetMaster for File Transfer.

The TCPaccess FTP Server product is an FTP server and client that you can use instead of or in conjunction with the FTP server supplied with your TCP/IP stack. Together with NetMaster for File Transfer, it provides the following functions:

- Monitoring the resources used by TCPaccess FTP file transfers
- Monitoring START, END, and FAILURE events for TCPaccess FTP file transfers
- Tracking progress of TCPaccess FTP file transfers through the Active File Transfer monitor
- The ability to terminate TCPaccess FTP file transfers from the Active File Transfer monitor
- Visibility of all TCPaccess FTP file transfers performed by the TCPaccess FTP server

Policy Control

NetMaster for File Transfer with TCPaccess FTP offers another unique feature to help you manage your FTP environment. This is the ability to control FTP transfers in line with a defined policy. Using a defined policy, you can allow or restrict transfers based on any combination of file names, user ID, IP addresses, and time of day.

You set up the policy for your TCPaccess FTP server transfers by defining a policy rule set in NetMaster for File Transfer.

About TCPaccess FTP Policy Rule Sets

TCPaccess FTP policy rule sets, together with your security package (for example, RACF), enable you to control the transfer of files using FTP. A rule set is a grouping of rules.

A TCPaccess FTP policy rule set contains the following criteria to match the rule to FTP file transfer requests:

- File names
- Users
- Transfer direction
- Local server IP address and port
- Remote IP addresses
- Time of day and day of week

You can define a rule set containing TCPaccess FTP policy rules on your NetMaster for File Transfer region and load it into your data space, as described in the following tasks. You can define many rule sets of policy rules on your NetMaster for File Transfer region. However, only one of the rule sets can be in the data space at any one time.

Note

For more information about the data space, see the *Management Services Administrator Guide*.

The TCPaccess FTP policy rule sets are stored in the NetMaster for File Transfer knowledge base, and you can maintain them in this region. Rule set maintenance has no effect on the loaded policy rule set; to change the loaded rule set, you need to reload it into the data space.

To activate a policy rule set, you must load a copy of the rule set into the data space.

The loaded policy rule set is enforced as long as the data space is active and policy mode has been set to ON. It does not depend on the NetMaster for File Transfer region once it is loaded. Rule set maintenance has no effect on the loaded policy rule set; to change the loaded rule set, you need to reload it into the data space.

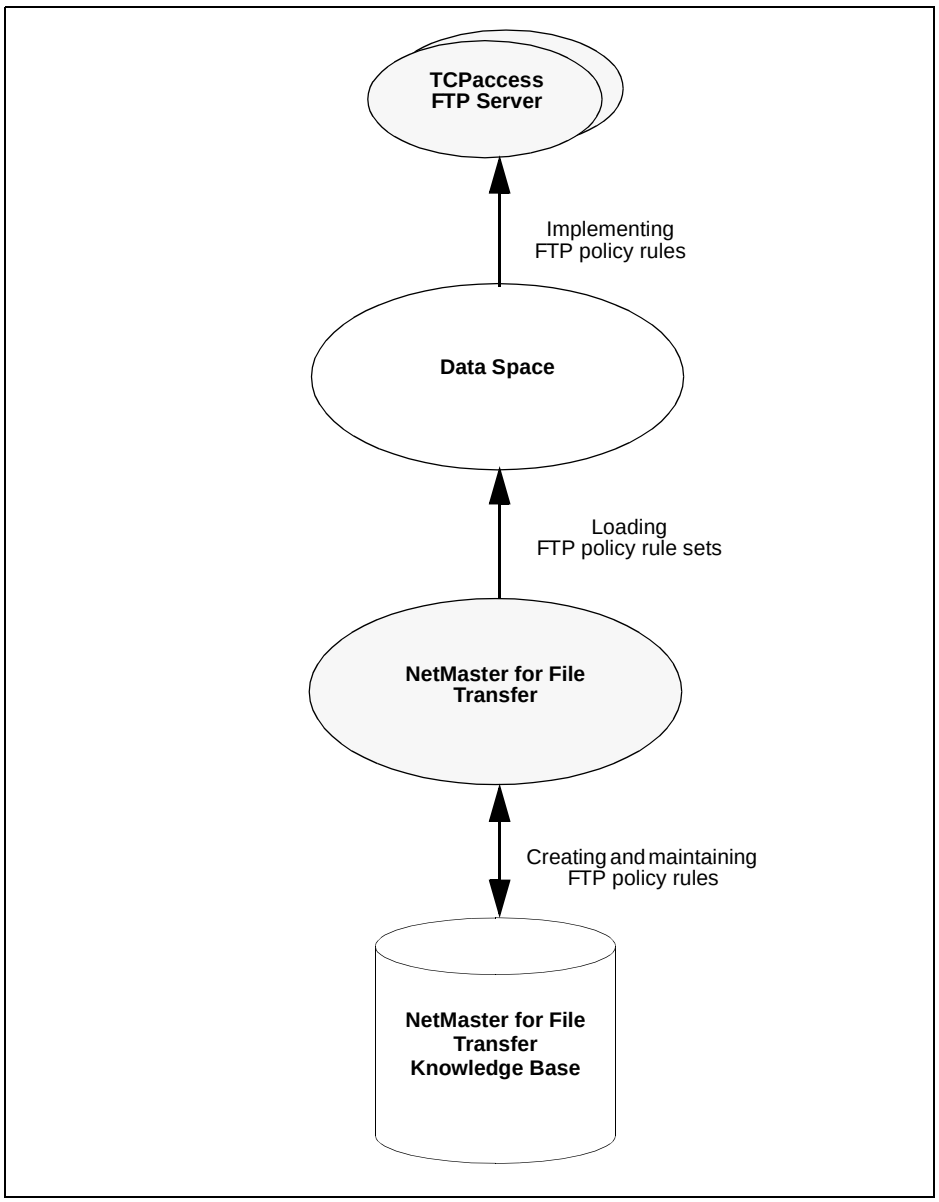
The user of the loaded policy rule set is the TCPaccess FTP server.

To implement a set of TCPaccess FTP policy rules, you need to perform the following tasks:

1. Define a policy rule set.
2. Add policy rules to the rule set.
3. Activate the policy rule set.

These tasks are described in the following sections.

Figure 20-1. How NetMaster for File Transfer and TCPaccess FTP Server Implement FTP Policy Rules



Task 1—Defining a Policy Rule Set

To define a policy rule set, proceed as follows:

Step 1. Enter the **/FTADMIN.P.M** path to display the FTP Policy Ruleset List panel.

Step 2. Press F4 (Add) to create a rule set definition.

The FTP Policy Ruleset panel is displayed.

Step 3. Name the rule set and provide a brief description.

Step 4. Press F3 (File) to create the definition in the knowledge base.

Task 2—Adding Policy Rules to a Rule Set

During operation, only one rule set can be loaded into the data space. Combine into the same rule set all the TCPaccess FTP policy rules that are to be used together. You can create different rule sets to:

- Load at a future time
- Load into the data space on another LPAR

To add a policy rule to a rule set, proceed as follows:

Step 1. If you are not already displaying the File Transfer Ruleset List panel, enter the **/FTADMIN.P.M** path to display it.

Step 2. Enter **R** beside the rule set to which you want to add rules.

The FTP Policy Rule List panel is displayed.

Note

Policy rules are evaluated in the order that they appear in the list, until a match is made. To change the position of a rule on the FTP Policy Rule List panel, type **M** (Move) next to it, type **B** or **A** next to the rule that you want to move it before or after, and press ENTER.

Step 3. Press F4 (Add) to add a rule.

The FTP Policy Rule panel is displayed.

Step 4. In the Rule Definition window, provide the following information:

In the …	Specify …
Description field	A brief description of the rule.
Status field	Whether the rule will be used (ACTIVE) or not used (INACTIVE) when it is loaded.
Allow Request? field	Whether the rule allows matched FTP requests: • NO disallows matched requests. • YES allows matched requests.
Log field	Whether messages are logged for matched FTP requests in the TCPaccess FTP server: • FAIL logs messages for requests disallowed by SAF security when the Allow Request? field is YES and a SAF qualifier is specified. • NO logs no messages, except when the policy mode is WARN. • YES logs messages for all matched requests.
SAF Qualifier field	A value that can be used to support SAF security. If Allow Request? is YES, then you can use this value to perform further checking of a matched FTP request. The resource that can be checked is as follows: FTP.*saf-qualifier.remote-ip-address.filename*. The default SAF class is $FTP. However, you can change the class by specifying the SAFFTP initialization parameter of the Data Space Manager. This parameter is in the DSPSYSIN member.

Note

See the section, *FTP SAF Rule Considerations*, on page 20-12 for further information about the SAF class.

See the section, *Setting Up Your SAF Qualifier*, on page 20-14 for details of JCL to define the SAF class.

See the *Management Services Administrator Guide* for further information about the SAFFTP initialization parameter for the Data Space Manager.

Step 5. In the Matching Criteria window, provide the following information:

In the …	Specify …
File Name field	The names of files to match. You can use a mask to allow matching of more than one file. The specified value is not case sensitive. The wildcard characters are %, representing zero or more characters, and _, representing a single character.
User List field	User List specifies the user IDs to match. You can specify a list of IDs separated by comma (,). You can use masks. The specified value is not case sensitive. The wildcard characters are %, representing zero or more characters, and _, representing a single character.
Transfer Direction field	Whether the rule matches inbound (IN) or outbound (OUT) file transfers.
Local Server IP Address field	A TCPaccess FTP server on the local system to match.
Local Server Port field	A TCPaccess FTP server on the local system to match.
Remote IP Address fields	The range of remote IP addresses to match. To match a single address, leave the High field blank.
Time of Day fields	The time period to match. If the first time is later than the second time, then the period spans midnight.
Day of Week fields	The days of the week to match.

Step 6. When you are satisfied with the rule, press F3 (File) to save it in the knowledge base.

Task 3—Activating a Policy Rule Set

When a rule set is complete, you can activate it by loading it into the data space.

Note

Only one rule set can be active at any time.

If the data space is not active, then start it by entering the following operating system command:

```
S solvedsp
```

where *solvedsp* is the name of your Data Space Manager.

See the *Management Services Administrator Guide* for further information about starting your Data Space Manager.

Loading a Policy Rule Set

To load a policy rule set into the data space, proceed as follows:

Step 1. Enter the **/FTADMIN.P.M** path to display the FTP Policy Ruleset List panel.

Step 2. Type **L** beside the name of the rule set definition to be loaded.

The FTP Policy Ruleset panel is displayed, showing the name of the rule set definition to be loaded.

Step 3. In the Load Ruleset window, identify the policy mode to be used:

- ON to allow access according to rules
- OFF to disable rules and allow access always
- WARN to allow access and log matches according to rules

Step 4. Press F6 (Confirm) to load the FTP policy rule set into the data space.

Each rule in the rule set is loaded into the data space table according to its sequence number.

Once you have loaded a policy rule set, it is highlighted in white in the rule set list. If you have made any changes to the rule set since it was loaded, then ** MODIFIED ** is displayed to the right of its name.

Note

If you make changes to the loaded rule set, they do not take effect until you reload the rule set.

Setting Policy Mode for an Active Policy Rule Set

To set the policy mode for an active policy rule set, proceed as follows:

Step 1. Enter the **/FTADMIN.P.S** path.

The FTP Policy Ruleset panel is displayed.

Step 2. Change the Policy Mode field to the required value:

- ON to allow access according to rules
- OFF to disable rules and allow access always
- WARN to allow access and log matches according to rules

Step 3. Press F6 (Confirm) to change the policy mode in the data space.

Note

You can also view the currently loaded rule set and policy mode by issuing the following system command:

`F SOLVDSP,display`

where *SOLVDSP* is the name of your Data Space Manager.

Viewing the Loaded Policy Rule Set

To view the loaded policy rule set, proceed as follows:

Step 1. Enter the **/FTADMIN.P** path to display the FTP Policy Maintenance menu.

Step 2. Type **V** in the Select Option ===> field.

The FTP Policy Ruleset panel is displayed, showing the Loaded Ruleset Definition.

Copying the Loaded Policy Rule Set

You can copy the loaded policy rule set to use it as the basis of a new rule set. To copy the loaded policy rule set, proceed as follows:

Step 1. Enter the **/FTADMIN.P** path to display the FTP Policy Maintenance menu.

Step 2. Type **C** in the Select Option ===> field.

The FTP Policy Ruleset panel is displayed.

Step 3. In the Ruleset Definition window, provide the following information:

In the …	**Specify …**
Name field	The name of the new rule set to be copied from the loaded rule set.
Description field	A brief description of the rule set.

Step 4. Press F3 (File) to copy the rule set and its rules.

Using Policy Rule Sets Across Linked Regions

If you have linked regions, then any policy rule sets that you create are visible on all those regions. If the regions are on different LPARs, then you can load the same rule set into the data spaces of different LPARs. To do this, you need to log on to a region running on the LPAR where you want to load the rule set.

You can use option TC – Transmit Common Components on the Multi-System Support Menu to link regions (see the section, *Linking NetMaster for File Transfer Regions*, on page 7-7).

FTP SAF Rule Considerations

When you request a file transfer to or from the TCPaccess FTP server, the server compares the request to the rules in the data space until a criteria match is found. The actions in the matching rule (allow request, log, check SAF) are then performed.

Note

If no rules match or the data space is not active, then the request is allowed.

To default to disallowing requests, define the last rule in the rule set as having no criteria (matches all requests) and Allow Request?=NO.

If your network environment is using a firewall and performing address translation, then you should determine the translated address of the remote and specify this address in the rule.

Checking FTP SAF Rules

FTP SAF rules are checked only if the matching FTP rule does both of the following:

- Mentions a *saf_qualifier*.
- Allows access.

Note

To check that the new SAF class has been activated and that SAF profiles have been set up, refer to your security administrator.

The SAF resource checked has a CLASS value as specified by the SAFFTP parameter in the data space parameters; otherwise it defaults to $FTP. The profile name is FTP.*saf-qualifier.remote-ip-address.filename*.

The first 44 bytes of the file name are used. MVS file names have a maximum of 44 bytes, so no truncation occurs. However, HFS file names can be much longer. The remote IP address is trimmed of leading zeroes. Member names for PDS files are not used in the profile name.

Note

HFS file names can be in mixed case, but all file names are converted to upper case before calling the SAF exit.

The level of access required depends on whether the transfer is outgoing or incoming:

- Outgoing transfers (in which the server reads the file name and transmits it to a remote destination) require read access in your SAF profile.
- Incoming transfers (in which the server receives a file being sent from a remote destination and stores it on the host) require update access in your SAF profile.

This is similar to normal dataset access security checks.

Note

For incoming new file allocations, the normal dataset security call checks for alter access. However, for FTP SAF calls, the call is incoming, so the SAF rule access is update. The FTP SAF rule does not distinguish between new files and existing file replacement.

Example of Using FTP SAF Rules for an Incoming File Transfer

A remote client at IP address 100.200.10.400 issues a PUT transfer request output to PDS dataset DEPT1.USER.FILE1(MEMBER1). This indicates an incoming transfer. The FTP matching rule specifies a SAF qualifier of DEPTUSER. A SAF check is then performed on the following SAF profile:

FTP.DEPTUSER.100.200.10.400.DEPT1.USER.FILE1

Update access is required for the transfer to proceed.

Note

You can use masking in rules in the normal manner for your security package; for RACF, for example, FTP.DEPTUSER.100.200.*.*.DEPT1.** would match the previous SAF check. Similarly for other security packages.

The normal security check for accessing the dataset is still performed. The FTP SAF check is in addition to the normal security call for dataset access.

Example of Using FTP SAF Rules for an Outgoing File Transfer

A user issues a PUT request for an HFS file called /usr/var/DevProc.log from the local host to host 100.200.10.222. The matching FTP policy rule has a SAF qualifier of DEVFILES. The security facility is called with the following SAF profile:

FTP.DEVFILES.100.200.10.222./USR/VAR/DEVPROC.LOG

The user requires read access for this resource for the transfer to proceed.

Setting Up Your SAF Qualifier

The following sections describe how to set up your SAF qualifier under the following security packages:

- RACF
- ACF2
- Top Secret

Setting Up Your SAF Qualifier Under RACF

To set up your SAF qualifier class and profiles under RACF, complete the following steps:

Step 1. Define the SAF class to the RACF Class Descriptor Table by using one of the JCL members in your *dsnpref.rname*.SS400.SSSAMP library:

- DEFRACFA (for non-SMP/E)
- DEFRACFS (for SMP/E)

Note

The class provided in the JCL is $FTP. You can stipulate anything you like here, as long as it conforms to RACF standards. If you use another name, ensure that you code the SAFFTP=*yourname* statement in the SOLVEDSP startup deck.

Note

An IPL is required for changes to the RACF Class Descriptor Table to take effect.

Step 2. Set up profiles for the SAF class, as follows:

RDEFINE $FTP FTP.*saf-qualifier.remote-ip-address.filename* UACC(NONE)
PE FTP.*saf-qualifier.remote-ip-address.filename* CLASS($FTP) ID(*userid or group*) ACCESS(READ)
SETROPTS GENERIC($FTP) REFRESH

These profiles are in the format FTP.*saf-qualifier.remote-ip-address.filename*, where:

- FTP is a constant.
- *saf-qualifier* is a name that you determine and enter in the SAF Qualifier Field when defining your policy rule.
- *remote-ip-address* is the standard dotted decimal notation of an IP address (* wildcard allowed).
- *filename* is an OS/390 dataset (* wildcard allowed).

Step 3. Make the profiles available to specific users or groups of users, with access attributes of either read or write, as shown in the section, *Examples of Using Your SAF Qualifier*, on page 20-18.

Setting Up Your SAF Qualifier Under ACF2

To set up your SAF qualifier under ACF2, complete the following steps:

Step 1. Define an FTP rule type.

```
ACF
SET CON(GSO)
IN CLASMAP.FTP RESOURCE($FTP) RSRCTYPE(FTP) ENTITYLN(157)
END
```

This maps $FTP SAF rules to an ACF2 resource type of FTP. It also sets a maximum length for profile names.

Step 2. Compile a rule similar to the following to allow users access to appropriate FTP SAF rules:

Note

Rule lines after the $KEY line must be in column 2.

If you compile this rule in TSO, you must enter a blank line after the last rule line entry and before the STORE command.

```
ACF
COMP *
$KEY(FTP) TYPE(FTP)
 SAFQUAL1.- UID(UID_string) SERVICE(READ) ALLOW
 SAFQUAL2.- UID(UID_string) SERVICE(UPDATE) ALLOW
 SAFQUAL3.- UID(UID_string) SERVICE(READ) PREVENT
 SAFQUAL4.- UID(UID_string) SERVICE(UPDATE) PREVENT
 SAFQUAL5.10.11.12.13.DATA.SET.NAME UID(UID_string)
SERVICE(UPDATE) ALLOW

STORE
END
```

For further information, see the section, *Examples of Using Your SAF Qualifier*, on page 20-18.

Setting Up Your SAF Qualifier Under Top Secret

To set up your SAF qualifier under Top Secret, complete the following steps:

Step 1. Define the class.

Note

$FTP is the default class name for FTP SAF rules. If you have used a different class name (by specifying the SAFFTP initialization parameter for the Data Space Manager), then use the new name instead of $FTP in the commands shown here.

TSS ADD(RDT) RESCL($FTP) RESCODE(*xx*) ACLST(WRITE,READ) ATTR(DEFPROT,LONG,GENERIC).

Note

Resource code can be a hex value from 01-3F. Select a unique value. To determine if code *xx* is already in use, you can issue the command TSS LIST(RDT) RESCODE(*xx*).

Step 2. Define ownership.

TSS ADD(*department-id*) $FTP(FTP.)

Step 3. Permit access to specific rules as required. You can permit access for a user ID, a group of users, or a user profile, as appropriate to your organization.

To permit access for a user ID:

TSS PER(*userid*) $FTP(FTP.*SAFQUAL*.10.11.12.13.*data.set.name*) ACCESS (READ)

Note

The $FTP parameter is restricted to a maximum of 44 characters.

To permit access for a user profile:

TSS PER(*profile*) $FTP(FTP.*SAFQUAL1*.) ACCESS(WRITE)

For further information, see the following section, *Examples of Using Your SAF Qualifier*.

Examples of Using Your SAF Qualifier

These examples show how you can allow specific users or groups of users to have access to various combinations of incoming and outgoing file transfers.

Example 1

FTP.SAFSAMP.208.11.215.17.FTP.DATA.FILE

Step 1. Connect this sample profile to user ID FTPUSER with read access within your security system.

Step 2. Define a policy rule allowing FTP transfers to whatever users you wish, with the SAF qualifier coded as SAFSAMP.

If FTPUSER requests a transfer to open a connection to 208.11.215.17 and put a file from there into FTP.DATA.FILE, then the request is rejected, because FTPUSER has only read access to the file as governed by your security system through the SAF qualifier.

However, if FTPUSER requests a transfer to get the FTP.DATA.FILE, the request is allowed, because FTPUSER has read access.

Example 2

FTP.SAFSAMP.208.11.215.17.**

Step 1. Connect this sample profile to user ID FTPUSER with read access within your security system.

Step 2. Define a policy rule allowing FTP transfers to whatever users you wish, with the SAF qualifier coded as SAFSAMP.

In this case, FTPUSER has read access to the above profile, and cannot download *any* file on the mainframe, from the IP address 208.11.215.17; however, FTPUSER can send *any* file out to *this* IP address.

Example 3

FTP.SAFSAMP.*.**

Step 1. Connect this sample profile to user ID FTPUSER with read access within your security system.

Step 2. Define a policy rule allowing FTP transfers to whatever users you wish, with the SAF qualifier coded as SAFSAMP.

In this case, FTPUSER has read access to the above profile, and cannot download *any* file on the mainframe, from *any* IP address; however, FTPUSER can send *any* file *out* to *any* IP address.

Example 4

FTP.SAFSAMP.*.FTP.DATA.FILE

Step 1. Connect this sample profile to user ID FTPUSER with write access within your security system.

Step 2. Define a policy rule allowing FTP transfers to whatever users you wish, with the SAF qualifier coded as SAFSAMP.

In this case, FTPUSER has write access to the above profile, and cannot download *any* file on the mainframe EXCEPT FTP.DATA.FILE from *any* IP address; however, FTPUSER can send FTP.DATA.FILE *out*, and *only* that file, to *any* IP address.

Part IV

Reference

A

Panel Paths for Accessing NetMaster for File Transfer Functions

This appendix lists some of the path specifications that you can use to access NetMaster for File Transfer functions.

Panel Path Specifications

A panel path specification enables you to jump between panels.

To jump to a panel, enter the path specification at a ===> prompt.

Table A-1 lists the paths to some of the NetMaster for File Transfer functions that you might need to use.

Table A-1. Useful Panel Paths

To access the …	Enter …	Or …
Activity log	**=H.L**	
Alert monitor Administration Menu	**=A.A**	**/ALADMIN**
Assisted Resource Definition Facility to help you build your file transfer management environment	**=A.R.AD**	**/RADMIN.AD**
Calendar Criteria menu	**=A.AS.CC**	**/ASADMIN.CC**
Customization Parameters panel to maintain the parameters that governs the characteristics of the NetMaster for File Transfer region	**=A.IN.P**	**/ICS**
File transfer Exception Reporting Menu	**=H.FT.ER**	**/FTHIST.ER**
File transfer History Data	**=H.FT**	**/FTHIST**
File Transfer Ruleset List panel to create rulesets and rules to monitor file transfers	**=A.FT.R**	**/FTADMIN.R**
FTP Policy Maintenance menu	**=A.FT.P**	**/FTADMIN.P**
Generate INI Procedure function	**=A.IN.G**	**/INIT.G**
Graphical monitor Administration Menu to create icon panels	**=A.G**	**/GADMIN**
Link Region and Synchronize Database function	**=A.M.SD**	**/MADMIN.SD**
Linked Regions panel	**=A.M.LR**	**/LISTREG**
Monitor to view the managed file transfer resources	**=M.FT**	**/FTMON**
Monitor to view the managed file transfers	**=M.AFT**	**/AFTMON**
Multi-System Support Menu	**=A.M**	**/MADMIN**
Primary Menu	**==**	
PSM Primary Menu	**=A.MS.PS**	**/PSM**
Report Writer Primary Menu	**=A.MS.R**	**/REPORT**
Ruleset List panel to add and maintain message suppression rulesets	**=A.E.R.R**	**/EADMIN.R.R**
Swap Log function to swap activity logs	**=A.MS.LA.S**	**/LOGSWAP**
System Image List panel to add an image to contain the file transfer schedules and resources you want to manage	**=A.R.I**	**/RADMIN.I**
Template System Image List panel to maintain $TEMPLAT system images	**=A.R.T.I**	**/RADMIN.T.I**
User Profile List panel to add new users	**=A.AS.UP**	**/ASADMIN.UP**

B

Parameter Groups

Region initialization parameters are grouped, by category, in logical parameter groups, to simplify the initialization and customization of a NetMaster for File Transfer region. This appendix lists the various categories of parameter groups you can set.

List of Parameter Groups

The parameter groups are listed in Table B-1.

Table B-1. Initialization Parameter Groups

Category	Parameter Group ID	Description
Files	AUTOFILES	Automation Files Specification—identifies the: • Knowledge base • Staging file • Internal reader • Default JCL library for jobs We strongly recommend that you run the RAMDB in a separate LSR pool. To do this, you need to: • Define an additional LSR pool in the LSR parameter group • Specify **LSR=? DEFER** in the Database VSAM Options field, where ? is the LSR pool that you defined
	EVENTLOG	Event Logging—enables or disables logging, and specifies the EVNTDB database, the EVNTARC archive dataset, the EVNTSEQ reorganization dataset, and other associated parameters.
	FTLOGS	Log File Specifications—specifies the file transfer log requirements.
	FTSCHD	Schedule File Specifications—enables or disables the saving and reloading of incomplete schedule details after a system outage, or after a new system image is loaded.
	LOGFILES	Log File Specifications—specifies the activity log requirements.
	MODSFILES	MODS Files Specifications—identifies the required MODS files.
	NETINFODB	NetInfo Database Specification—identifies the NETINFO file.
	PANELLIBS	Panel Libraries Specifications—specifies the panel library paths.
	PSMSPOOL	PSM Spool File Specification—identifies the PSM spool file.

(Sheet 1 of 5)

Table B-1. Initialization Parameter Groups

Category	Parameter Group ID	Description
Interfaces	CDAPI	CONNECT:Direct Interface—specifies: • Whether CONNECT:Direct file transfer events will be received. • CONNECT:Direct event receiver ID • User ID that identifies the region to CONNECT:Direct • Work file for CONNECT:Direct output (DMPRINT) • Concatenation of the CONNECT:Direct PROCESS files (DMPUBLIB)
	CMAPI	CONNECT:Mailbox Interface—specifies: • Whether CONNECT:Mailbox file transfer events will be received. • ID that identifies the event receiver that is used to collect events from CONNECT:Mailbox regions • CONNECT:Mailbox ISPF interface administration file, that the SOLVE region uses to retrieve message and connect failure code Help
	EXTAPPLS	External Applications Access—specifies the: • External applications access requirements • LU 1 logon mode for the MTO command
	FTPCNTL	FTP Control—specifies whether FTP file transfer events will be received.
	SOCKETS	TCP/IP Sockets Interface—identifies the TCP/IP software being used in the environment and specifies its interfaces.
	SSI	SOLVE Sub-System Interface—specifies the: • SOLVE subsystem interface requirements • Non-VTAM terminal requirements
	UNICENTER	Unicenter Agent Specification—specifies the requirements for working with the Unicenter Network Management Option for NetMaster software.
	WSPEER	Workstation Peer Specification—specifies the requirements for connecting to the SOLVE:Operations for IT/Operations and SOLVE:Operations for OpenView processes.
	XCAPI	CA-XCOM Interface—specifies: • Whether CA-XCOM file transfer events will be received. • CA-XCOM event receiver ID.

(Sheet 2 of 5)

Table B-1. Initialization Parameter Groups

Category	Parameter Group ID	Description
Monitors	FTMONITOR	File Transfer Monitor Options—specifies: • The amount of time ended and failed file transfers remain on the monitor • The polling period of the file transfer product • Whether the fuel gauge is used to display file transfer progress
Names	AUTOIDS	Automation Identifiers—specifies the: • System image to be loaded on startup • Default desired state • Rule actions in MANUAL operation mode • File transfer ruleset to be loaded on startup • Checkpoint requirements • Startup WTOR requirement
	OPSYSIDS	Operating System Identifiers—identifies the: • Template system image • System • JES • AOM subsystem interface and its command character • Logon mode for APPC sessions
	SYSTEMID	SOLVE System Identifications—specifies the: • Region ID • Logon panel title • Message monitor title
Security	CMDREPLS	Command Replacements—specifies the replaced Management Services commands.
	LOGONUSRDATA	Should SOLVE Accept User Data?—specifies whether to accept user data when a user logs on to the region.
	SECSHIPPING	Ship UAMS Maintenance—specifies the UAMS synchronization requirements.

(Sheet 3 of 5)

Table B-1. Initialization Parameter Groups

Category	Parameter Group ID	Description
Tuning	ABENDCMD	Command Issued if System ABENDs—specifies the system command to issue when the region ends abnormally.
	AOMQUEUES	AOM System Queue Limits—specifies the: • AOM SSI storage requirements for message traffic • Threshold that prevents message bursts from overloading the region
	AUTOTABLES	Automation Table Controls—specifies the: • Default size of a transient log • Size of the vartable for the active system image • Command cache requirements • Size of the vartable for message learning
	CDEVENTS	CONNECT:Direct Event Log Options—enables you to restrict the type of CONNECT:Direct events recorded in the file transfer log.
	CONSOLES	Console Specifications—specifies the: • Console requirements • System command processing requirements
	LSRPOOL	VSAM LSR Pool Specifications—specifies the local shared resource (LSR) pools of buffers.
	MULTISYS	Multi-System Options—specifies whether multisystem operations is supported by one or both of the following: TCP/IP and VTAM.
	NCLCONTROLS	NCL Control Parameters—specifies the NCL processing environment.
	NDBLIMITS	NDB Processing Limits—specifies the NDB scanning limits.
	NONSWAP	Does SOLVE Run Non-swappable?—specifies whether the region should ever be swapped out of memory.
	SMFDATA	SMF Recording Details—specifies the SMF recording details.
	TIMINGS	Automation Timing Controls—specifies the: • Status display timing requirements • Link processing timing requirements

(Sheet 4 of 5)

Table B-1. Initialization Parameter Groups

Category	Parameter Group ID	Description
Useability	CCONSOLIDATN	Console Consolidation Options—specifies: • Whether console consolidation is enabled • Message profile restrictions
	DISPLAYS	Presentation Controls—specifies certain characteristics of the graphical monitor and the knowledge base synchronization status display.
	EQUATES	System Equates—specifies equated strings.
	EVENTSIM	Event Simulation Options—specifies whether the event simulator is enabled.
	PMENUCONTROL	Primary Menu Control Options—specifies how the primary menu is displayed.

(Sheet 5 of 5)

C

Security Settings

This appendix specifies the recommended security settings for each of the supplied group IDs. These settings can be used if you want to create group IDs for your external security package. The settings are presented as they appear in UAMS providing the panel, field, value, and structured field for each setting.

Note

The structured field information is useful to installations that have an external security package controlling user access with a partial or full security exit. See the *Management Services Administrator Guide* for detailed information about the structured fields.

Security Settings for $RMADMIN

$RMADMIN is the group ID for administrators. The recommended security settings are given in Table C-1.

Table C-1. Security Settings for $RMADMIN

Panel (Page Number)	Field	Value	Structured Field
User Authorities (2)	Authority Level	255	50
	Multiple Signon Authority	Y	19
	Split/Swap Authority	Y	2E
	APPC Access Key	ALL	60
	APPC Access Lock	ALL	61
User Access (3)	Network Management	Y	22
	Operations Management	Y	2B
	Operator Console Services	Y	20
	Management Services	Y	511
	UAMS Maintenance	Y	2A
	Broadcast Services	Y	21
	System Support Services	Y	23
OCS Details (6)	Monitor Status	Y	51
	Message Code	FF	58
	NPF Resource List Member	$RMSXADM	5B
	Initial OCS Command	-$RMCCOCS	54
Network Management Details (8)	TCP/IP Services	2	530
AOM General Details (11)	AOM Message Receipt	Y	180
	Console Routing Codes	ALL	180B
	Message Level Screening	ALL	182
AOM MVS Details (12)	Console Authority	M	181
Print Services Manager Details (13)	Maintenance Access	2	501

Security Settings for $RMOPER

$RMOPER is the group ID for operators. The recommended security settings are given in Table C-2.

Table C-2. Security Settings for $RMOPER

Panel (Page Number)	Field	Value	Structured Field
User Authorities (2)	Authority Level	200	50
	Multiple Signon Authority	Y	19
	Split/Swap Authority	Y	2E
	APPC Access Key	ALL	60
	APPC Access Lock	ALL	61
User Access (3)	Network Management	Y	22
	Operations Management	Y	2B
	Operator Console Services	Y	20
	Management Services	Y	511
	Broadcast Services	Y	21
OCS Details (6)	Monitor Status	Y	51
	Message Code	FF	58
	NPF Resource List Member	$RMSXOPR	5B
	Initial OCS Command	-$RMCCOCS	54
Network Management Details (8)	TCP/IP Services	2	530
AOM General Details (11)	AOM Message Receipt	Y	180
	Console Routing Codes	ALL	180B
	Message Level Screening	ALL	182
AOM MVS Details (12)	Console Authority	M	181

Security Settings for $RMNOPER

$RMNOPER is the group ID for network operators. The recommended security settings are given in Table C-3.

Table C-3. Security Settings for $RMNOPER

Panel (Page Number)	Field	Value	Structured Field
User Authorities (2)	Authority Level	200	50
	Multiple Signon Authority	Y	19
	Split/Swap Authority	Y	2E
	APPC Access Key	ALL	60
	APPC Access Lock	ALL	61
User Access (3)	Network Management	Y	22
	Operator Console Services	Y	20
	Broadcast Services	Y	21
OCS Details (6)	Monitor Status	Y	51
	Message Code	FF	58
	NPF Resource List Member	$RMSXNOPR	5B
	Initial OCS Command	-$RMCCOCS	54
Network Management Details (8)	TCP/IP Services	2	530

Security Settings for $RMMON

$RMMON is the group ID for monitors. The recommended security settings are given in Table C-4.

Table C-4. Security Settings for $RMMON

Panel (Page Number)	Field	Value	Structured Field
User Authorities (2)	Authority Level	000	50
	Multiple Signon Authority	Y	19
	APPC Access Key	ALL	60
	APPC Access Lock	ALL	61
User Access (3)	Network Management	Y	22
	Operations Management	Y	2B
Network Management Details (8)	TCP/IP Services	1	530
AOM General Details (11)	AOM Message Receipt	Y	180
	Console Routing Codes	ALL	180B
	Message Level Screening	ALL	182
AOM MVS Details (12)	Console Authority	I	181

Security Settings for $RMBUSER

$RMBUSER is the group ID for background users. The recommended security settings are given in Table C-5.

Table C-5. Security Settings for $RMBUSER

Panel (Page Number)	Field	Value	Structured Field
User Authorities (2)	Authority Level	255	50
	APPC Access Key	ALL	60
	APPC Access Lock	ALL	61
User Access (3)	Network Management	Y	22
	Operations Management	Y	2B
	Operator Console Services	Y	20
	Management Services	Y	511
	Broadcast Services	Y	21
	Object Services Support	Y	605
	System Support Services	Y	23
OCS Details (6)	Monitor Status	Y	51
	NPF Resource List Member	$RMSXADM	5B
Network Management Details (8)	TCP/IP Services	2	530
AOM MVS Details (12)	Console Authority	M	181

D

File Transfer Variables

File transfer variables enable you to extract information about file transfer events.

This appendix describes these variables.

Variables

Use the variables in Table D-1 to retrieve data from a file transfer event.

You can use the variables to pass values to the following:

- E-mail problem ticket interface (see the section, *Defining an E-mail Problem Ticket Interface*, on page 5-56)
- Automated actions in a file transfer rule
- Customizing alerts

Figure D-1 shows an example of the use the variables in the text to be sent to the user, USER01, in response to an event that satisfies the file transfer rule.

Figure D-1. Using File Transfer Variables—Example

```
SOLVPROD---------- File Transfer : User Notification Details ------------------
Command ===>

Short Description .. File transfer status and source
Notify ............ USER01

Text ............... &ZRFPRODUCT,&ZRFSRCADDR,&ZRFSTATUS,&ZRFSRCNAME,&ZRFSRCTYPE
```

Table D-1. File Transfer Variables

Variables	Description
&ZRFABENDCODE	Contains the abend code.
&ZRFBLKIN	Contains the number of blocks read during the transfer.
&ZRFBLKOUT	Contains the number of blocks written during the transfer.
&ZRFCMPRPCT	Contains the compression percentage of the file transfer.
&ZRFENDDATE	Contains the date when the transfer ended.
&ZRFENDTIME	Contains the time when the transfer ended.
&ZRFFAILCODE	Contains the failure code.
&ZRFFAILDESC	Contains the failure description.
&ZRFJOBNAME	Contains the name of the file transfer application.
&ZRFLATENCY	Contains the time between the CA-XCOM transfer request and the start of the actual transfer.
&ZRFNETTYPE	Contains the type of protocol used for a CA-XCOM transfer.
&ZRFPRODUCT	Contains the type of file transfer product.
&ZRFRECIN	Contains the number of records read during the transfer.

(Sheet 1 of 2)

Table D-1. File Transfer Variables

Variables	Description
&ZRFRECOUT	Contains the number of records written during the transfer.
&ZRFRETRIES	Contains the number of times an alert has been raised for a file transfer event.
&ZRFSRCADDR	Contains the address or node name of the source of the transfer.
&ZRFSRCFNAME	Contains the ID of the data in the transfer.
&ZRFSTARTDATE	Contains the date when the transfer started.
&ZRFSTARTTIME	Contains the time when the transfer started.
&ZRFSTATUS	Contains the monitored transfer status: START, END, or FAILURE.
&ZRFSTCJOBID	Contains the ID of the TCPaccess FTP server started task or job.
&ZRFTGTADDR	Contains the address or node name of the target of the transfer.
&ZRFTGTFNAME	Contains the ID of the data in the transfer.
&ZRFUSER	Contains the ID of the user that performs the transfer.
&ZRFXFRAMT	Contains the number of bytes transferred.
&ZRFXFRDUR	Contains the time, in seconds, taken for the transfer.
&ZRFXFRID	Contains either a CA-XCOM transfer ID, CONNECT:Direct process name, a CONNECT:Mailbox ID and batch number, an FTP ID if specified in the FTPCNTL parameter group, or an FTS transmission definition name.
&ZRFXFRRATE	Contains the transfer rate in bytes per second.
&ZRFXFRTYPE	Contains the CA-XCOM transfer type (EXECUTE or SCHEDULE).

(Sheet 2 of 2)

Note

The &ZRFBLKIN and &ZRFRECIN variables are applicable to CONNECT:Direct transfers only. The &ZRFBLKOUT and &ZRFRECOUT variables are applicable to CONNECT:Direct and CONNECT:Mailbox transfers only. Whether the amount of data read or written is in blocks or records depends on the file format.

E

File Transfer Events Mapping

The information available for file transfer events for the various file transfer products is different. The following tables list the variances in the information available for each product and how it is derived.

Table E-1. File Transfer Event Field Mappings

Event Field Name	Mapping
CA-XCOM	
Transfer ID	CA-XCOM transfer ID(request number) (see also the section, *Considerations—CA-XCOM File Transfers*, on page 10-11)
Target Data	One of the following: • Name of the file that receives the transferred data • INTRDR if an internal reader receives the transferred data • SYSOUT:*class options* if a SYSOUT file receives the transferred data, where *class* is the SYSOUT class *options* identifies one or more of the following: - Destination (DEST:*destination*) - External writer name (WTR:*writer*) - Job ID (JOBID:*job-id*) - Job name (JOBNAME:*job-name*) - Report name (REP:*report*)

Table E-1. File Transfer Event Field Mappings

Event Field Name	Mapping
CONNECT:Direct	
Transfer ID	Process name(process number)
CONNECT:Mailbox	
Transfer ID	Mailbox ID(batch number) For inbound transfers Mailbox ID is extracted from $$ADD. For outbound transfers Mailbox ID is extracted from batch ADD
Source Address	Remote Connect—Remote name (SNA sessions), BSC line name (BSC lines) Auto Connect—Task name
Target Address	Remote Connect—Task name Auto Connect—Remote name
Source Data	Inbound transfers—User batch ID from $$ADD Outbound transfers—Batch ID from batch ADD
Target Data	Inbound transfers—User batch ID from $$ADD Outbound transfers—Batch ID from batch ADD
FTP not using a TCPaccess FTP server	
Transfer ID	Is null unless a transfer ID is specified in the FTPCNTL parameter group
Source Data	Available only for local transfers
Target Data	Available only for local transfers
FTP using a TCPaccess FTP server	
Transfer ID	TCPaccess FTP server started task or job name and TCPaccess FTP server allocated file transfer number; the format is *server-name(transfer-number)*, where: • *server-name* is the JES started task or job name of the TCPaccess FTP server address space • *transfer-number* is the file transfer number (in hexadecimal notation) allocated by TCPaccess FTP server
FTS	
Transfer ID	Transmission name
Source Address	Primary name of the region initiating the transfer
Target Address	Primary name of the region receiving the transfer

Table E-2 and Table E-3 list the data available for each product from a start event. In Table E-2, CD refers to CONNECT:Direct and CM refers to CONNECT:Mailbox.

Table E-2. Data Available for Start Events—CD and CM

	CD for MVS or CD for OS/390	CD for UNIX	CD for NT	CD for Tandem	CD for OS/400	CM *
Transfer ID	Yes	Yes	Yes	Yes	Yes	Yes
Source Data	Yes	Yes	Yes	Yes	No	Yes
Source Address	Yes	Yes	Yes	Yes	Yes	Yes
Target Data	Yes	Yes	Yes	Yes	No	Yes
Target Address	Yes	Yes	Yes	Yes	Yes	Yes
User ID	Yes	Yes	Yes	Yes	Yes	No

Note

* The start event is not available for a host initiated CONNECT:Mailbox Auto Connect transfer.

Table E-3. Data Available for Start Events—CA-XCOM, FTS, and FTP

	CA-XCOM	FTS	FTP not using TCPaccess FTP	FTP using TCPaccess FTP
Transfer ID	Yes	Yes	No	Yes
Source Data	Yes	Yes	No	Yes
Source Address	Yes	Yes	No	Yes
Target Data	Yes	Yes	No	Yes
Target Address	Yes	Yes	No	Yes
User ID	Yes	Yes	No	Yes

Table E-4 and Table E-5 list the data available for each product from an end event. In Table E-4, CD refers to CONNECT:Direct and CM refers to CONNECT:Mailbox

Table E-4. Data Available for End Events—CD and CM

	CD for MVS or CD for OS/390	CD for UNIX	CD for NT	CD for Tandem	CD for OS/400	CM
Transfer ID	Yes	Yes	Yes	Yes	Yes	Yes
Source Data	Yes	Yes	Yes	Yes	Yes	Yes
Source Address	Yes	Yes	Yes	Yes	Yes	Yes
Target Data	Yes	Yes	Yes	Yes	Yes	Yes
Target Address	Yes	Yes	Yes	Yes	Yes	Yes
User ID	Yes	Yes	Yes	Yes	Yes	Yes

Table E-5. Data Available for End Events—CA-XCOM, FTS, and FTP

	CA-XCOM	FTS	FTP not using TCPaccess FTP	FTP using TCPaccess FTP
Transfer ID	Yes	Yes	Yes	Yes
Source Data	Yes	Yes	Yes *	Yes *
Source Address	Yes	Yes	Yes	Yes
Target Data	Yes	Yes	Yes *	Yes *
Target Address	Yes	Yes	Yes	Yes
User ID	Yes	Yes	Yes	Yes

Note

* For all FTP transfers, either the Source Data or Target Data is available, whichever is the local data.

F

Application Program Interface

This appendix describes the use and syntax of the application programming interface (API) procedures, $RFCALL and $RMDBAPI. For additional API procedures, see the *Automation Services Administrator Guide.*

$RFCALL

$RFCALL is the API procedure used to call NetMaster for File Transfer from external sources (for example, a user-written NCL procedure).

Syntax

```
$RFCALL     ACTION=CDCOMMAND
            NAME=cd-manager-name
            [SYSNAME=system-image-name]
            [VERSION=system-image-version]
            COMMAND='cd-command-string'
            [DISPLAY={YES|NO}]
            [USERID=user-id PASSWORD=user-password]
            [CASE={YES|NO}]
```

Use

Use this call to issue CONNECT:Direct commands from NetMaster for File Transfer.

Operands

ACTION=CDCOMMAND
Indicates that a CONNECT:Direct command is to be processed.

NAME=*cd-manager-name*
Specifies the name of the CONNECT:Direct manager to which the command applies.

SYSNAME=*system-image-name*
Specifies the name of the system image in which the command is processed.

The default is the name of the local active system image.

VERSION=*system-image-version*
Specifies the version of the system image in which the command is processed.

The default is the version of the local active system image.

COMMAND=‘*cd-command-string’*
Specifies the command to be sent to the CONNECT:Direct product.

DISPLAY={YES|NO}

Specifies whether the response to the command is displayed (YES) or returned as &RFRESP*n* variables (NO), where *n* is a sequence number starting from 1 (for example, &RFRESP1). The default values are as follows:

In…	The default value is…
Full -screen mode	YES.
Background mode	NO.

USERID=*user-id*

Specifies the CONNECT:Direct signon ID of the user issuing the command. You must specify this operand if you use the API in background mode.

PASSWORD=*user-password*

Specifies the CONNECT:Direct signon password of the user. You must specify this operand if you use the API in background mode.

CASE={YES|NO}

Indicates whether the specified CONNECT:Direct signon details of the user are to be treated as case sensitive.

Returned Variables

&RFRESP*n*

Command response is returned in &RFRESP*n* variables. Each variable contains one line of the response.

&RFRESPCNT

The number of lines in the command response is returned in the &RFRESPCNT variable.

&SYSMSG

Contains the message returned by $RFCALL.

Return Codes

The following return codes indicate the success or failure of command processing:

RETCODE	Meaning
0	Processing was successful.
8	Processing failed.
16	Error occurred in call syntax.

Example

The following example shows how to issue a SELECT PROCESS command to the CONNECT:Direct region, DECD1, on the local system in full-screen mode:

```
$RFCALL ACTION=CDCOMMAND NAME=DECD1
COMMAND='SELECT PROCESS WHERE (QUEUE=HOLD)'
```

$RMDBAPI SERVICE={ACTIVATE | INACTIVATE}

Syntax

```
$RMDBAPI    SERVICE={ACTIVATE | INACTIVATE}
            RSNAME=ft-ruleset-name RMNAME=ft-rule-name
```

Use

Use this call to change the status of a file transfer rule in a NetMaster for File Transfer region to ACTIVE or INACTIVE. The region will act on the rule if the rule belongs to the loaded file transfer rule set.

Operands

SERVICE={ACTIVATE | INACTIVATE}
Indicates that status of the specified file transfer rule, *ft-rule-name*, be changed as follows:

- ACTIVATE changes the rule status to ACTIVE.
- INACTIVATE changes the rule status to INACTIVE.

RSNAME=*ft-ruleset-name*
Specifies the name of the file transfer rule set to which the specified rule, *ft-rule-name*, belongs.

RMNAME=*ft-rule-name*
Specifies the name of the file transfer rule to which the service applies.

Returned Variable

&SYSMSG
Contains the message returned by $RMDBAPI.

Return Codes

The following return codes indicate the success or failure of the status change processing:

&RETCODE	Meaning
0	Processing was successful.
8	Processing failed.
16	Error occurred in call syntax.

Example

The following example changes the status of the CD40FAIL rule in the CDFAIL file transfer rule set to ACTIVE:

```
&CALL    PROC=$RMDBAPI +
         PARMS=(SERVICE=ACTIVATE,+
                RSNAME=CDFAIL,RMNAME=CD40FAIL)
```

$RMDBAPI SERVICE={CREATE | DELETE | GET | LIST | SET}

For detailed information about the API, see the *Automation Services Administrator Guide*.

Syntax

```
$RMDBAPI    SERVICE={CREATE | DELETE | GET | LIST | SET}
            [TRUNCATE={YES|NO}]
            [{NAME=resource-name[MANNAME=manager-name]}|
             {RSNAME=ft-ruleset-name[RMNAME=ft-rule-name]}]
            CLASS=cc
            [SYSNAME=system-name]
            [VERSION=version]
            [field-name-1=field value-1]
            [field-name-2=field value-2]
            .
            .
            .
            [field-name-n=field value-n]
```

Use

Use this call to maintain ResourceView definitions in the knowledge base.

Operands

The next section lists the values for the *field-name-n* operands that are specific to the NetMaster for File Transfer product. For full details of the operands, see the *Automation Services Administrator Guide*.

ResourceView Definition Field Names

The following sections list the product specific field names.

The names are related to the corresponding field labels on the appropriate definition panels:

- Fields that are mandatory on a panel are mandatory in the API.
- Values that are valid in the panel fields are valid in the API.
- Fields that have default values inherit the values in the API.

Resource Fields

Table F-1 lists the product specific resource field names that can be used in the $RMDBAPI procedure.

Table F-1. Resource Field Names Used in the $RMDBAPI Procedure

Field Names	Field Label on Panel
General Description	
IPADDR	TCP/IP Host Name/Addr
IPPORT	Agent Port Number
Monitor Details	
HBACT	Active Transfer Request Monitors Heartbeat Interval
HBEATIN	Heartbeat Interval
HBINACT	Inactive Transfer Request Monitors Heartbeat Interval
Auto Connect Queue Monitor Details	
QDEPTH	Queue Depth Threshold
LISTNM1 to LISTNM5	List Name(s)
BSC Line Monitor Details	
QDEPTH	Queue Depth Threshold
AUTORES	Automatic Restart?
LINENM1 to LINENM5	Line Name(s)
File Transfer Monitor Details	
IDLEALT	Stalled Time to Alert
IDLEDRP	Stalled Time to Flush
QDEST1 to QDEST5	Destination Node(s)
QPNAME1 to QPNAME5	Process Name(s)

(Sheet 1 of 4)

Table F-1. Resource Field Names Used in the $RMDBAPI Procedure

Field Names	Field Label on Panel
Monitor Details (*continued*)	
Link Monitor Details	
LINKNME	Link Name
Queue Monitor Details	
QTYPE	Queue Type
QDEPTH	Queue Depth Threshold
QSTATUS	Process Status
QDEST1 to QDEST5	Destination Node(s)
QPNAME1 to QPNAME5	Process Name(s)
Remote Node Monitor Details	
RMSNNDE	Remote Node LU name (CA-XCOM)
RMIPNDE	Remote Node TCP/IP Host Name/Addr (CA-XCOM)
REMNODE	Remote Node Name (CONNECT:Direct)
IPADDR	TCP/IP Host Name/Addr (FTP)
IPPORT	TCP/IP Port Number (FTP)
TIMEOUT	Timeout After (FTP)
SNA Session Monitor Details	
IDLEALT	Stalled Time to Alert
RMTNM1 to RMTNM5	Remote Name(s)

(Sheet 2 of 4)

Table F-1. Resource Field Names Used in the $RMDBAPI Procedure

Field Names	Field Label on Panel
Monitor Details (*continued*)	
Stalled Monitor Details	
IDLEALT	Stalled Time to Alert
IDLEDRP	Stalled Time to Terminate
TRID1 to TRID5	Transfer Request ID
SERV1 to SERV5	Remote Server
TCP/IP Connection Monitor Details	
IDLEALT	Idle Time to Alert
IDLEDRP	Idle Time to Drop
TCP/IP Listener Task Monitor Details	
LRETRYA	Retry Attempts
LRETRYI	Retry Interval
IPPORT	CONNECT:Direct Port No
COMMUNE	SNMP Community Name
Transfer Request Monitor Details	
TRSTATS	Transfer Request Status
TRDEPTH	Transfer Request Threshold
TRID1 to TRID5	Transfer Request ID
SERV1 to SERV5	Remote Server

(Sheet 3 of 4)

Table F-1. Resource Field Names Used in the $RMDBAPI Procedure

Field Names	Field Label on Panel
Schedule	
CRIT1 to CRIT97	Day/Date or Criteria Name
TIME1 to TIME97	Start Time
PREP1 to PREP97	Pre-Processing Period
PROC1 to PROC97	Processing Period
POST1 to POST97	Post-Processing Period
LONG1 to LONG97	Longest Transfer
File Filters	
FILE1 to FILE97	File Name/Transfer ID
TYPE1 to TYPE97	Type
FNUM1 to FNUM97	Number
Extended File Filter	
SRC1 to SRC97	Source System/Node
TGT1 to TGT97	Target System/Node
MIN1 to MIN97	Minimum File Size (In Bytes)
MAX1 to MAX97	Maximum File Size (In Bytes)

(Sheet 4 of 4)

File Transfer Rule Set Fields

Table F-2 lists the file transfer rule set field names that can be used in the $RMDBAPI procedure.

Table F-2. File Transfer Rule Set Field Names Used in the $RMDBAPI Procedure

Field Name	Field Label on Panel
File Transfer Rule Set	
SDESC	Description

File Transfer Rule Fields

Table F-3 lists the file transfer rule field names that can be used in the $RMDBAPI procedure.

Table F-3. File Transfer Rule Field Names Used in the $RMDBAPI Procedure

Field Names	Field Label on Panel
File Transfer Rule Filter	
RSTAT	Rule Status
SDESC	Description
PFNAME	FileName/TransferID
SRCTGT	File Type
TSTAT	Transfer Status
SVRTY	Alert Severity
AUTOCLR	Alert Autoclear
L1 to L10	(
FLD1 to FLD10	Field
O1 to O10	Opr
VAL1 to VAL10	Value (field value must not contain the tilde (~) character)
G1 to G10	Gen
R1 to R10	)
B1 to B10	Bool

(Sheet 1 of 3)

Table F-3. File Transfer Rule Field Names Used in the $RMDBAPI Procedure

Field Names	Field Label on Panel
Alert Automated Actions	
Caution You must use the ALACT*n* names in sequence (for example, ALACT1, ALACT2, ALACT3, …). If you break the sequence, the names following the break are ignored. For example, if you specify ALACT1 and ALACT3 but do not specify ALACT2, ALACT3 is ignored.	
ALACT1 to ALACT99 **Note** The maximum size of an Actions record is 12500 bytes, which may reduce the actual number of actions (*n*) that can be added to a file transfer rule.	Automation_Services_Process AUTO_TROUBLE_TICKET NOTIFY RUN_COMMAND RUN_NCL
ALDSC1 to ALDSC*n*	Short Description
For Automation_Services_Process only	
ALPRC*n*	Process
ALPRS*n*	Parameters
For AUTO_TROUBLE_TICKET only	
ALUT*mn* and ALUV*mn* **Note** *m* is 1 to 9, identifying up to nine FIELD NAME-VALUE pairs for each action. You must use *m* in sequence. Use these operands to override the values already implemented in the region.	FIELD NAME= and VALUE= on Alert Monitor : Trouble Ticket Data Entry Definition panel

(Sheet 2 of 3)

Table F-3. File Transfer Rule Field Names Used in the $RMDBAPI Procedure

Field Names	Field Label on Panel
Alert Automated Actions (*continued*)	
For NOTIFY only	
ALUI1*n* to ALUI2*n*	Notify
ALTX1*n* to ALTX4*n*	Text
For RUN_COMMAND only	
ALCMD*n*	Command & Parameters
ALPR1*n*	Command Parameters
For RUN_NCL only	
ALPRN*n*	Procedure Name
ALPR1*n* to ALPR5*n*	Parameter
Alert Definition for File Transfer Rule	
Note The region assigns default values for these fields when an alert is generated. You can override these default values.	
ADRES	Resource Name
ADDESC	Alert Description
ADTXT1 to ADTXT5	Alert Text
Note The API treats ADTXT*n* and ADRACT*n* as blocks of data. If used, the values are overridden as blocks, not line by line. For example, if you specify ADTXT1 only, ADTXT2 to ADTXT5 will display as blank lines.	
ADRACT1 to ADRACT4	Alert Recommended Action

(Sheet 3 of 3)

G

Form for Gathering Information Required During Implementation

During the implementation process, you will need to provide information required by the process. To streamline your tasks, copy the form in this appendix and use it to gather the required information before you start the process.

Required Information	Value	See…
Initial user ID and password		page 5-2
Primary application name of the region		page 5-2
New password		page 5-3
Data set prefix used during installation		page 5-4
AOM subsystem ID		page 5-4
Name and version of the TCP/IP software		page 5-11
TCPIP.DATA dataset name—if you are using Communications Server TCPaccess subsystem ID—if you are using TCPaccess		page 5-11
Port number for inbound connections		page 5-11
For CA-XCOM		
Name of the CA-XCOM startup JCL procedure		page 5-28
Name of the Default Options Table		page 5-28

Required Information	Value	See…
For CONNECT:Direct		
CONNECT:Direct for MVS or CONNECT:Direct for OS/390 user ID and password for the region		page 5-4
Concatenation of CONNECT:Direct PROCESS files		page 5-6
Name of the CONNECT:Direct startup JCL procedure		page 5-29
CONNECT:Direct for MVS or CONNECT:Direct for OS/390 initialization parameters: ALLOC.STORAGE STATISTIS.EXIT Name of USEREXIT—if you are using an existing exit		page 5-29
For CONNECT:Mailbox		
Name of the CONNECT:Mailbox VSAM administration file		page 5-10
Name of the CONNECT:Mailbox startup JCL procedure		page 5-35
CONNECT:Mailbox for MVS initialization parameters: Name of USEREXIT—if you are using an existing exit Name of the ODF file		 page 5-35 page 5-36
For FTP		
Name of the PROFILE.TCPIP configuration member		page 5-40
Name of the FTP.DATA configuration member		page 5-40
Name of the PW.SRC dataset		page 5-50
Name of the TCPIP.DATA dataset		page 5-51
Name of the HOST.LOCAL dataset		page 5-51
SAF qualifier for access control		page 20-13

Glossary

ACB (access method control block)

A control block that links an application program to an access method such as VTAM.

Activity Log

A log of all important activities occurring in a region. You can use the log to assist you in determining the cause of a problem.

Actual State

The state a defined resource is actually in at any given time when a region is active. ResourceView keeps the actual state consistent with the desired state.

The valid actual states are: ACTIVE, DEGRADED, FAILED, INACTIVE, RECOVERED, STARTING, STOPPING, and UNKNOWN.

Alert

An event displayed on the alert monitor. An alert can be internally generated (for example, when a monitored resource fails) or user-defined.

AOM (Advanced Operation Management)

A management services facility that manages and controls local and remote operating systems. This is the subsystem interface to the SOLVE region. The interface enables the passage of system messages, events, and commands.

API (application program interface)

A functional interface supplied by a program. The interface enables another application, written in a high-level language, to use specific data or functions of the program.

APPC (advanced program-to-program communications)

An IBM-defined application-level protocol (which makes use of LU 6.2) that allows interconnected systems to communicate and share the processing of programs.

AUTOMATED Mode

A resource operation mode that allows you to automate many of the functions previously done by operators at consoles. Other modes of operation are OFF, MANUAL, and IGNORED.

Availability Map

When a region is implemented, a resource defined in the knowledge base can be attached to an availability map. This map indicates the time that the resource is available to the system.

Boolean

An adjective that describes a logical entity, operator, operation, or expression; named after the philosopher George Boole.

Boolean Expression

A logical expression that evaluates to either false or true.

Consolidated Console

Enables you to view messages from linked operation regions at a single monitor.

The link between regions occurs at the event level, where INMC enables one region to ship messages to another region.

DASD (direct access storage device)

A storage device in which the access time is effectively independent of the location of the data (for example, a disk drive).

Desired State

The required state of a resource. Desired state can be overridden by an availability map or manually from a monitor.

The valid values are ACTIVE and INACTIVE.

Display Attribute Tables

Tables containing display attribute values for resources and icons on the status and graphical monitors.

The logical state of a resource determines its display attributes. Authorized users can customize display attributes.

EPS (EndPoint Services)

EndPoint Services is a communications access method provided by the SOLVE subsystem interface (SSI) regions. The method provides communication by using the MVS cross-system coupling facility (XCF) in a Sysplex environment.

Exit

A user-written program or procedure that can be invoked by a SOLVE region. The exit provides data to the region and performs actions that the region does *not* directly support but that are required by the installation.

FTP (File Transfer Protocol)

Enables you to transmit data packets between systems.

FTS (File Transmission Services)

Enables you to transmit datasets between systems.

Graphical Monitor

A facility that enables you to monitor and control resources. The monitor provides an iconic view of groups of resources.

Heartbeat Feature

Enables you to specify a time interval at which the SOLVE region checks the status of the resource. You use the feature to monitor resources that are liable to change state without an accompanying message.

Icon

A graphical representation of grouped resources (for example, all printers in a system image) that is displayed on the graphical monitor. If the icon changes color, an operator can check the resources in the resource group to see what has happened and why.

Icon Panel

A predefined panel that contains icons that represent groups of resources. For example, an icon panel might contain an icon for the printers on a system, another icon for the started tasks on a system, and so on.

ICS (Initialization and Customization Services)

An AutoAssist facility that helps you set up your region parameters.

INMC (Inter-Management Services Connection)

A Management Services component that allows multiple SOLVE regions to be linked and controlled from a single location.

Internet

A collection of linked networks using TCP/IP and related protocols.

ISR (Inter-System Routing)

Enables the routing of information between regions.

Knowledge Base

A database in which you store the policies and procedures that govern the operation of your systems.

Every NetMaster for File Transfer region has its own knowledge base. The knowledge base stores, for example, system image definitions, resource definitions, process definitions, and ruleset definitions for that region.

The changes made to a definition held in a knowledge base are reflected across the knowledge bases in all linked regions, regardless of their physical location.

The fact that each region has its own knowledge base means that the region can run in isolation if the links to other regions fail.

Logical State

The state of a resource based on its actual state, desired state, and operation mode. The logical state of a resource determines its display attributes, and alerts the operator to changes in the resource state. The operator can then take action if necessary.

The valid logical states are: OK, ATTENTION, INERROR, PENDING, STARTING, STOPPING, FAILED, DEGRADED, and UNKNOWN.

LSR (local shared resource)

Local shared resource pools are used for buffering I/O to VSAM files. NCL supports this type of processing for user databases (UDBs).

LU (logical unit)

SNA introduced the concept of the logical unit (LU). The LU is a type of SNA network addressable unit (NAU) that enables end users to gain access to network resources and communicate with each other.

LU 0

An unconstrained SNA protocol that allows the selection of any set of available protocol rules, as long as the two LUs are able to communicate with each other successfully according to the rules chosen. Therefore, all LU types are an implementation of LU 0.

LU 6.2

A protocol that serves as a port into an SNA network. LU 6.2 defines a specific set of services, protocols, and formats for communication between logical processors. LU 6.2 provides presentation services for the presentation of data to the end user, transaction services for performing transaction processing on behalf of the end user, and LU services for managing the resources of the LU.

Macro

See Registered Macro.

Message Profile

A set of criteria that determines which messages are displayed on a message consolidation console.

MODS (Managed Object Development Services)

A Management Services development environment that provides tools for creating and customizing NCL applications.

MVS (Multiple Virtual Storage)

An IBM operating system.

NCL (Network Control Language)

A structured interpretive language available in a SOLVE region. The language enables you to develop logical procedures (programs) for performing specific tasks. NCL contains a wide range of logic, built-in functions, and arithmetic facilities which can be used to provide powerful monitoring and automatic control functions.

NCL Procedure

A member of the SOLVE procedures dataset comprising NCL statements. The NCL statements are executed by an EXEC or a START command specifying the name of the procedure.

NCL Process

The NCL task that is invoked by an EXEC or a START command to execute one or more NCL procedures. Each NCL process has a unique NCL process identifier.

NPF (Network Partitioning Facility)

A Management Services facility that defines the functions a user can perform.

Non-roll Delete (NRD) Message

A message on an OCS screen. The message indicates an event of critical importance and does *not* roll off the screen as the screen fills up (for example, a message that requires a reply). You remove an NRD message by deleting the message explicitly or by replying to the message.

OCS (Operator Console Services)

A Management Services facility that provides a central point of message monitoring and operational control either locally or for a network of SOLVE regions.

Operations Region

A region established by the execution of the Automation Services or NetMaster for File Transfer application. The region uses the information in a knowledge base to automate the operations processes in an organization.

Packet

A sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals and, possibly, error control information are arranged in a specific format.

Parameter Group

Contains parameters that determine the characteristics of a Management Services region.

PPI (program-to-program interface)

Enables programs to exchange data.

Process

In Automation Services or NetMaster for File Transfer, a process is a means of automating a series of commands and actions. For example, the sequence of actions involved in shutting down a resource can be translated into a series of steps in a single process. A macro performs the actions required by each step.

Prompted Field

A field that is linked to a list of values. You can select one of these values to complete the field. Authorized users can edit the lists.

PSM (Print Services Manager)

Enables you to control the physical printing of reports on JES or network printers.

RACF (Resource Access Control Facility)

An IBM-licensed program that provides for access control by identifying users to the system and verifying their authority, authorizing access to DASD data sets, logging detected unauthorized attempts to enter the system, and logging detected accesses to protected data sets.

Registered Command

A command containing instructions to the SOLVE region about the actions to take.

Registered Macro

A macro pointing to an NCL procedure that performs the actions in a process step.

Resource

An entity used to provide a function (for example, a CONNECT:Direct process queue monitor).

Resources are defined to a region as part of a system image. A resource definition contains the operations policies and methods for a resource.

Resource Group

A group representing a group of resources. You attach resource groups to icons. An operator can issue a command to look at the resources if, for example, an icon changes color. The icon might have an attached resource group that contains, for example, all the printers in a system image.

Resource Group Filter

A set of instructions that determines which resources are contained in a resource group.

Resource States

A resource defined to a region has three types of states: desired, actual, and logical. The region aims to maintain the resource at the desired state.

The logical state indicates the condition of a resource, based on its desired state, actual state, and operation mode. The logical state determines the display attributes of a resource and alerts the operator to any problems.

Resource Template

A template providing predefined values for the definition of a commonly-used resource.

SNMP (Simple Network Management Protocol)

A protocol for the management of the internet.

SOLVE

SOLVE encompasses the services provided by Management Services and Automation Services. For example, the SOLVE PPI is a service provided by the subsystem interface (SSI) in Management Services.

Status Monitor

Enables you to monitor and control individual resources. The monitor displays resource statuses in line-by-line mode. These statuses are color-coded to alert an operator to changes in resource status. Changes in color are governed by changes to the *logical state* of a resource.

Status Monitor Filter

A Boolean expression that determines which resources are to be displayed on the status monitor. For example, an operator may use a filter that only displays the printers in a system image.

System Domain

A VTAM term that describes a logical division of a network. Networks are divided into domains that are associated with the way they are controlled.

System Image

Part of the knowledge base and identifies the resources that are to be controlled by the region. Each system has its own system image.

TCP/IP (Transmission Control Protocol/Internet Protocol)

The Internet Protocol routes packets across multiple subnetworks (such as LANs and WANs). The Transmission Control Protocol is used on top of IP and provides guaranteed delivery of data across the internet.

Transient Log

A log of activities associated with a resource that is monitored by a region. One transient log exists for each resource definition loaded in a region and exists as long as the definition remains loaded in the region. The resource definition can, however, save the log entries to the activity log.

UAMS (User Access Maintenance Subsystem)

The security component of management services that enables the definition of users and the associated user authority.

Variable

Used to store data that can change. A variable is represented by a word that starts with an ampersand (&), followed by the name of the variable. For example, &A is a variable where A is the name. When &A is processed, it is replaced by the stored value.

VFS (Virtual File Services)

A service providing a VSAM dataset that is used by a SOLVE region for internal processing activities and as a general database.

WTO (write-to-operator)

A user-coded service that enables a message to be written to the system console operator, to inform the operator of errors and unusual system conditions that need correcting.

WTOR (write-to-operator with reply)

A user-coded service that enables a message to be written to the system console operator, to inform the operator of errors and unusual system conditions that need correcting, and to which a response is expected.

Index

Symbols

$RFAGENT FTS message handler, 5-37
$RFCALL API, F-2
$RMDBAPI API
    field names
        file transfer rule sets, F-12
        file transfer rules, F-13
        resources, F-8
    file transfer rule set, activating, F-5
    ResourceView definitions
        creating, F-7
        deleting, F-7
        listing, F-7
        retrieving information about, F-7
    system image definition
        field values, changing, F-7
$RMDBAPI procedure, 19-2
$RMPB07S procedure, 5-54
$TEMPLAT system image, 1-9
    setting up default version, 5-19

A

AC (Action) action, 5-14
accessing
    activity logs, 13-32
    alert monitor, 11-2
    file transfer logs, 13-32
    file transfer status monitor, 10-61, 13-2
    transient logs, 13-32
ACF2, 6-13
    sample full security exit, 6-13
    sample partial security exit, 6-13
    using SAF, 6-13
action lists
    applying action to an item, 9-10
    description, 9-10
actions for CA-XCOM requests
    A (Alter), 13-13
    H (Hold), 13-13
    R (Release), 13-13
    R (Resume), 13-13
    S (Suspend), 13-13
    T (Terminate), 13-13
    V (View), 13-13

actions for CONNECT:Direct processes
C (Change), 13-22
D (Delete), 13-13, 13-22
DF (Delete/Force), 13-22
DH (Delete/Hold), 13-22
F (Flush), 13-22
FPF (Flush Process Force), 13-22
H (Hold), 13-22
R (Release), 13-22
S (Suspend), 13-22
SPF (Suspend Process Force), 13-22
V (View), 13-22
actions for resource definitions, D (Display), 13-5
actions for templates
M (Merge), 10-45, 10-49
O (Override), 10-45, 10-49
R (Reset), 10-45, 10-49
activating resources, 13-40
active file transfer monitor, 1-10
active file transfers, monitoring, 12-2
activity logs, 8-4
allocating, 5-25
browsing online, 13-35
displaying, 13-35
file IDs, 5-25
file transfer logs, accessing from, 13-34
LOGFILES parameter group, 5-24
messages, help for, 9-21
reusing, 8-4
suppressing messages, 16-2
swapping, 8-4
Administration Task Log panel, 7-13
administrator
change initial user to administrator, 5-18
defining, 5-18
group ID, 6-2
security settings, C-2
agents, 1-14
alert forwarding, 5-60
alert history, 11-8
alert monitor, 1-10
accessing, 11-2
alerts, 11-2
user profile, 11-5
alert monitor Administration Menu, 5-55
Alert Monitor panels
Alerts, 11-3
Custom Trouble Ticket, 5-58
Email a Trouble Ticket, 5-57
Interface Definition, 5-56
Trouble Ticket Data Entry Definition, 5-59
alerts, 11-6
and status monitor, 11-6
and transient log, 11-7
associated details, 11-6
closure, 10-8, 11-8
monitoring, 11-2
operator notes, 11-7
problem tickets, 11-7
responding to, 11-6
ALL S command, 10-33, 10-53
ALL U command, 10-33, 10-53
API (application program interface), $RFCALL, F-2
application program interface. *See* API
archive data set, 5-67
AS/400
CONNECT:Direct commands, 13-41
file transfer management, 10-53
resources, CONNECT:Direct, 10-32
assisted reorganization facility, 13-30
assisted resource definition, 10-24
authorizing
functionality on Communications Server, 5-49
interface
to Communications Server, 5-47
to TCPaccess, 5-51
Auto Connect
displaying queue, 13-27
initiating, 13-26
Auto Populate Facility, 10-51
Selection List panel, 10-33, 10-52
AUTOIDS parameter group, 10-59
automatic problem recording, 1-14, 5-54
$RMPB07S procedure, 5-54
link definitions, SOLVE:Problem, 5-54
user IDs, SOLVE:Problem, 5-54
automation, 10-62
engine, 1-13
availability map, 15-25
map details, 15-27
timer details, 15-28

B

background region, user definition, 6-2
background users
  BSYS, 7-14
  group ID, 6-2
    security settings, C-6
  updating pre-existing definitions, 6-8
backups, knowledge base, 8-5
BSC lines monitor, displaying, 13-28
BSYS background user, multisystem implementation, 7-14

C

calendars, 17-2
  criteria, 17-7
  display, 17-3
  keywords, 17-4, 17-6
    dates, associating with, 17-4
canceling changes to a record, 9-14
CA-XCOM
  control library member, 13-12
  events, 3-8
  file transfers, displaying information, 13-5
  listing transfer requests, 13-13
  manager resources, 10-24
    creating, 10-25
  managing transfer requests, 13-13
  monitor resources, 10-24
    creating, 10-27
  remote node monitors, customizing criteria, 15-8
  remote nodes, displaying information, 13-6
  stalled transfer monitors, customizing criteria, 15-6
  transfer request monitors, customizing criteria, 15-5
CA-XCOM monitor template definitions
  remote node monitor, 3-7
  stalled transfer monitors, 3-6
  TCP/IP connections monitor, 3-7
  TCP/IP listener task monitor, 3-6
  transfer request monitors, 3-5
CA-XCOM monitors, customizing criteria
  monitor heartbeat, 15-2
  remote node monitor, 15-8
  stalled transfer monitor, 15-6
  TCP/IP connections monitor, 15-7
  transfer request monitors, 15-5
CA-XCOM parameters, 13-12
CA-XCOM resource definitions
  assisted resource definition, 10-24
  description, 1-5
  jobs, 3-4
  monitors, 3-5
  started tasks, 3-4
CA-XCOM resources, 3-3
  controlling, 1-10
  file transfer manager, 3-3
  file transfer monitors, 3-4
CA-XCOM, displaying information about
  control library member, 13-12
  managers, 13-5
  region, 13-12
  TCP/IP connections, 13-5
  transfer requests, 13-5, 13-12
CDAPI macro, parameter details, 15-38
CDMSG command, 9-21
changing global operation mode, 14-2
CMMSG command, 9-21
cold load, 14-5
collecting SNMP data
  from Communications Server, 5-50
  from TCPaccess, 5-53
commands
  confirming CONNECT:Direct signon details, 13-15, 13-19
  CONNECT:Direct for OS/400, 13-41
  CONNECT:Direct for Tandem, 13-41
  CONNECT:Direct for UNIX, 13-41
  CONNECT:Direct for Windows NT, 13-41
  CONNECT:Mailbox, 13-25
  display, 13-13, 13-20
  displaying CA-XCOM information, 13-12
  displaying CONNECT:Direct information, 13-14
  issuing to a file transfer region, 13-41
  listing, 10-62
  UNIX, 13-43

commands, CA-XCOM resources
DFT, 13-12
DIS, 13-12
ENA, 13-12
INQ, 13-12
LST, 13-12
VA, 13-13
VAC, 13-13
VH, 13-13
VI, 13-13
VS, 13-13
commands, CONNECT:Direct resources
CLR, 13-16
CMD, 13-41
FTL, 13-33
IIP, 13-18
NM, 13-16
VA, 13-21
VAC, 13-21
VB, 13-21
VC, 13-21
VE, 13-21
VH, 13-21
VI, 13-21
VIP, 13-23
VR, 13-21
VST, 13-21
VSU, 13-21
VT, 13-21
VW, 13-21
VXR, 13-21
commands, CONNECT:Mailbox resources
C, 13-25
CON, 13-26
D, 13-25
DIR, 13-24
E, 13-25
FTL, 13-33
I, 13-25
M, 13-25
R, 13-25
S, 13-25
T, 13-25
VSS, 13-28
commands, FTP resources
FTL, 13-33
VIP, 13-23
commands, FTS resources
FTL, 13-33
commands, specific
$LOG, 13-35
ALL S, 10-33, 10-53
ALL U, 10-33, 10-53
CDMSG, 9-21
CMD, 13-41
CMMSG, 9-21
CON, 13-26
FILTER, 13-4
FTLOG, 13-33
GLOBAL, 14-2
LOAD, 14-4
LOCATE, 9-13
PROFILE, 13-37
SHUTFORCE, 14-6
SHUTSYS, 14-6
STARTSYS, 14-6
Communications Server
authorizing, 5-49
authorizing interface to, 5-47
collecting SNMP data from, 5-50
PW.SRC data set, 5-50
SNMP agent, 5-50
specifying SNMP community names, 5-50
started tasks, 4-2
complex operations, 15-33
Confirm Database Synchronization panel, 7-11
Confirm Swap Log panel, 8-4
Confirm Unlink panel, 7-16

CONNECT:Direct
confirming signon details, 13-15, 13-19
events, 3-14
file transfers, displaying information, 13-6
initialization parameters, 13-14
MAXBATCH, 5-31
MAXUSERS, 5-31
STATISTICS.EXIT, 5-30
interface parameters, 5-6
listing processes, 13-20
manager resources, 10-24
creating, 10-29
managing processes, 13-22
message logging, selective, 16-6
monitor resources, 10-24
creating, 10-34
partner resources, creating, 10-32
process monitors, customizing criteria, 15-10
remote node monitors, customizing criteria, 15-14
remote nodes, displaying information, 13-6
security considerations, 13-14, 13-19
statistics exit, 5-29
transfer monitors, customizing criteria, 15-11

CONNECT:Direct commands, issuing from processes, 15-37

CONNECT:Direct monitor template definitions
process queue monitors, 3-11
process status monitors, 3-12
remote node monitor, 3-13
TCP/IP connections monitor, 3-13
TCP/IP listener task monitor, 3-13
transfer monitors, 3-12

CONNECT:Direct monitors, customizing criteria
listener task monitors, 15-12
monitor heartbeat, 15-9, 15-15
queue monitors, 15-10
remote node monitor, 15-14
TCP/IP connections monitor, 15-13
transfer monitor, 15-11

CONNECT:Direct resource definitions
assisted resource definition, 10-29
autopopulation, 10-32
custom-built, 10-37
description, 1-6
jobs, 3-10
monitors, 3-11
started tasks, 3-10

CONNECT:Direct resources, 3-9
confirming signon details, 13-15, 13-19
controlling, 1-11
destination nodes, checking availability, 15-35
file transfer manager, 3-9
file transfer monitors, 3-10
monitoring, 13-2

CONNECT:Direct, displaying information about
managers, 13-6
network map, 13-16
processes, 13-19
queued processes, 13-6
region, 13-14
TCP/IP connections, 13-6

CONNECT:Mailbox
batches
displaying, 13-24
managing, 13-25
interface parameters, 5-10
log exit, 5-35
manager resources, 10-24
creating, 10-38
monitor resources, 10-24
creating, 10-39

CONNECT:Mailbox events, 3-21

CONNECT:Mailbox monitor template definitions
Auto Connect queue monitor, 3-19
BSC line monitor, 3-19
SNA sessions monitor, 3-20

CONNECT:Mailbox monitors
customizing criteria
Auto Connect queue monitor, 15-16
BSC lines monitors, 15-17
hearbeat interval, 15-15
SNA sessions monitors, 15-18
displaying and managing
Auto Connect queue, 13-27
BSC lines, 13-28
SNA sessions, 13-28

CONNECT:Mailbox resource definitions
assisted resource definition, 10-38
description, 1-7
CONNECT:Mailbox resources, 3-17
controlling, 1-11
customizing criteria
Auto Connect queue monitor, 15-16
BSC lines monitors, 15-17
SNA sessions monitors, 15-18
file transfer manager, 3-18
file transfer monitor, 3-18, 3-19
manager, 3-17
VSAM file server, 3-17, 3-18
CONNECT:Mailbox, displaying information about
batches, 13-24
monitors, 13-27
VSAM batch files, 13-28
considerations
case sensitive values, 10-10
CA-XCOM file transfers, 10-11
CONNECT:Direct file transfers, 10-11
CONNECT:Mailbox file transfers, 10-12
FTP file transfers, 10-13
FTS file transfers, 10-14
FTS staging data sets, 10-16
multisystem implementation, 7-6
overlapping file transfer rules, 10-10
control file. *See* CTL file
controlling access by using NPF to
functions, 6-3
resources, 6-3
controlling FTP use, 20-1
controlling system images, 14-1
criteria for file transfer event search, 18-13
CTL file
checking syntax, 19-5
defining to schedules, 19-4
viewing, 19-4
customizing
availability map, 15-24
FTS monitor heartbeat details, 15-19
region parameters, 5-3
background user, 5-2
resource definitions, 15-1
managers, 15-44
monitors, 15-46
supporting, 15-48
customizing CA-XCOM resources
monitor heartbeat details, 15-2
remote node monitor, 15-8
stalled transfer monitor, 15-6
TCP/IP connections monitor, 15-7
transfer request monitors, 15-5
customizing CONNECT:Direct resources
listener task monitors, 15-12
monitor heartbeat details, 15-9, 15-15
queue monitors, 15-10
remote node monitor, 15-14
TCP connections monitor, 15-13
transfer monitor, 15-11
customizing CONNECT:Mailbox resources, monitor heartbeat details, 15-15
customizing FTP resources
monitor heartbeat details, 15-21
remote node monitor, 15-23
TCP connections monitor, 15-22

D

DASD
displaying information about, 13-7
monitoring, 13-2
resource definitions, 4-3
customizing, 15-48
data
case sensitive, 10-10
entering on panels, 9-14
filing, 9-14
saving, 9-14
validation, 9-14
data entry panels, 9-13
data warehouse servers, 5-68
event logging, 5-69
database searches, 18-3, 18-10
Database Synchronization Status panel, 7-12
date criteria, 17-7

defining
a file transfer rule set, 20-6
CA-XCOM resources, 10-24
CONNECT:Direct resources, 10-29
CONNECT:Mailbox resources, 10-38
DASD resources, 10-51
file transfer rule sets, 10-6, 20-6
file transfer rules, 10-6
file transfer schedules, 10-18
FTP resources, 10-43
FTS resources, 10-40
printed reports, 18-20
system images, 10-4
tape resources, 10-51
TCP/IP resources, 10-48
definitions, customizing, 15-1
DFT command, 13-12
dialogs
Initialization in Progress, 5-13
System Parameters Customization, 5-3
DIS command, 13-12
display commands, 13-5
displaying
activity log from the transient log, 13-38
activity logs, 13-35
alert history, 11-8
availability map, 15-25
CA-XCOM parameters, 13-12
CONNECT:Direct initialization parameters, 13-18
CONNECT:Direct network map, 13-14
file transfer logs, 13-33
file transfer resources, 13-3
logs, 13-32
processes
on the Exec queue, 13-19
on the Hold queue, 13-19
on the Timer queue, 13-19
on the Wait queue, 13-19
TCP/IP connections, 13-23
transient logs, 13-36
displaying information about
CA-XCOM
file transfers, 13-5
regions, 13-12
remote nodes, 13-6
transfer requests, 13-5, 13-12
CONNECT:Direct
file transfers, 13-6
processes, 13-19
queued processes, 13-6
regions, 13-14
remote nodes, 13-6
CONNECT:Mailbox
Auto Connect queue, 13-27
batches, 13-24
BSC lines monitor, 13-28
monitors, 13-27
SNA sessions monitor, 13-28
DASD, 13-7
file transfer schedules, 13-7
FTP managers, 13-7
FTP remote nodes, 13-7
FTP servers, 13-7
FTS links, 13-7
FTS managers, 13-7
started tasks, 13-7
tapes, 13-8
TCP/IP listener, 13-5, 13-6
displaying the file transfer status monitor panel, 10-61
dropping TCP/IP connections, 13-24

E

e-mail, problem tickets, 5-56
file transfer variables, D-2
ENA command, 13-12
enabling
NETSTAT interface, 5-48
sockets interface, 5-48
EndPoint Services. *See* EPS
entering data, 9-14
EPS (EndPoint Services), multisystem support in Sysplex, 7-5

event flow, NetMaster for File Transfer
CA-XCOM, 3-8
CONNECT:Direct, 3-14
distributed systems, 3-15
MVS and OS/390, 3-14
CONNECT:Mailbox, 3-21
data warehouse, 5-69
FTP, 3-29
FTS, 3-24
event recording, implementing, 5-65
events database. *See* EVNTDB database
EVNTARC data set, implementing, 5-67
EVNTDB database
error if full or unallocated, 18-22
implementing, 5-66
search criteria, 18-13
searching, 18-10
examples
file transfer schedule, 10-22
file transfer variables, D-2
exits
CONNECT:Mailbox log exit, 5-35
SMF, 5-42
statistics, 5-22
to external security packages, 6-13
external security packages
ACF2, 6-5, 6-13
calling using SAF, 6-5
exits to, 6-13
full security exit, 6-13
partial security exit, 6-13
RACF, 6-5, 6-13
Top Secret, 6-5
extracting data to a file, 18-18

F

features, 1-3
automatic problem recording, 1-14
automation engine, 1-13
CA-XCOM resource definitions, 1-5
CONNECT:Direct resource definitions, 1-6
CONNECT:Mailbox resource definitions, 1-7
file transfer rules, 1-5
file transfer schedules, 1-5
FTP function policy control, 1-15
FTP resource definition, 1-8
FTS resource definitions, 1-7
knowledge base, 1-4
monitors, 1-10
multisystem support, 1-13
reporting function, 1-15
SNMP traps, 1-14
field names
$REDBAPI, used in
file transfer rules, F-13
$RMDBAPI, used in
file transfer rule sets, F-12
resources, F-8
fields
mandatory, 9-14
optional, 9-14
file transfer events, analyzing data, 18-18
file transfer logging, implementation, 5-22
file transfer logs, 1-14, 13-33
activity log, accessing, 13-34
allocating, 5-22
browsing, 13-34
displaying, 13-33
file IDs, 5-22
suppressing messages, 13-34
file transfer managers
CA-XCOM, 3-3
CONNECT:Direct, 3-9
CONNECT:Mailbox, 3-17
FTP, 3-25
FTS, 3-22
file transfer monitors
active, 1-10
CA-XCOM, 3-4
CONNECT:Direct, 3-10
CONNECT:Mailbox, 3-18
FTP, 3-25
FTS, 3-22

File Transfer Protocol. *See* FTP
file transfer regions, issuing commands, 13-41
file transfer resources, 3-2
  activating, 13-40
  controlling, 1-10, 13-40
  inactivating, 13-40
  owners, 3-2
  specifying availability, 15-24
  supporting, 4-2
file transfer rule sets
  defining, 10-6, 20-6
  rules, adding, 10-6, 20-6
file transfer rules
  case sensitive values, 10-10
  CA-XCOM considerations, 10-11
  CONNECT:Direct transfers
    data set names, 10-12
    process names, 10-12
  CONNECT:Mailbox considerations, 10-12
  criteria, 10-17
  defining, 10-6
  description, 1-5
  filter expressions, 10-17
  FTP transfers
    information available, 10-13
    static name, 10-13
  FTS transfers
    DD names, 10-15
    name criterion, 10-14
    transmission definition names, 10-14
  overlaps, 10-10
  rule set, adding to, 10-6, 20-6
  status, 10-7
  transfer status criterion, 10-8
  wildcard characters, 10-7
file transfer schedules, 10-20
  CA-XCOM considerations, 10-11
  CONNECT:Direct transfers
    data set names, 10-12
    process names, 10-12
  CONNECT:Mailbox considerations, 10-12
  defining, 10-18
  description, 1-5
  displaying information, 13-7
  example, 10-22
  failure acknowledgment, 13-8
  FTP transfers
    information available, 10-13
    static name, 10-13
  FTS transfers
    DD names, 10-15
    name criterion, 10-14
    transmission definition names, 10-14
  monitoring, 13-2, 13-8
  next schedule display, 13-8
  selective display on status monitor, 13-9
  status changes, 10-23
  status information, 13-9
  updating externally, 19-3
file transfer status monitor
  accessing, 13-2
  filter selection, 13-4
file transfer variables, D-2
File Transmission Services. *See* FTS
filing data, 9-14
FILTER command, 13-4
filter expressions, file transfer rules, 10-17
finding information
  using the FMODE command, 9-12
  using the FRPOMPT command, 9-12
  using the LOCATE command, 9-12
focal point regions, 1-13
  knowledge base synchronization, 7-7
forwarding alerts, 5-60
FTCHECK macro, parameter details, 15-42, 15-43
FTP (File Transfer Protocol)
  considerations, 10-13
  implementing event flow, 5-38
  manager resources, 10-24
  monitor resources, 10-24
FTP events, 3-29
FTP function policy control, 1-15
FTP managers, displaying information, 13-7
FTP monitor template definitions
  remote node monitor, 3-28
  TCP/IP connections monitor, 3-27
  TCP/IP listener port monitor, 3-27
FTP monitors, customizing criteria
  monitor heartbeat, 15-21
  remote node monitor, 15-23
  TCP/IP connections monitor, 15-22
FTP policy rules, status, 20-7
FTP remote nodes, displaying information, 13-7

FTP resource definitions
assisted resource definition, 10-43
description, 1-8
jobs, 3-26
monitors, 3-26
started tasks, 3-26
FTP resources
controlling, 1-12
file transfer manager, 3-25, 3-26
file transfer monitors, 3-25, 3-26
FTP servers, displaying information, 13-7
FTP use, controlling, 20-1
FTS (File Transmission Services)
manager resources, 10-24
monitor resources, 10-24
staging data set considerations, 10-16
FTS events, 3-24
FTS links
displaying information, 13-7
to NetMaster for File Transfer, 5-36
FTS managers, displaying information, 13-7
FTS monitor template definitions, INMC link monitor, 3-24
FTS regions
INMC links, 5-36
remote, 10-58
FTS resource definitions
assisted resource definition, 10-40
description, 1-7
file transfer monitors, 3-23
jobs, 3-23
remote regions, 3-23
started tasks, 3-23
FTS resources, 3-22
controlling, 1-11
file transfer manager, 3-22
file transfer monitors, 3-22
monitoring, 13-2
functions, controlling access to, 6-3

G

GLOBAL command, 14-2
global operation mode, 10-59
AUTOMATED, 14-2
changing, 14-2
MANUAL, 14-2
setting, 10-62
graphical monitor, 13-44
group IDs
administrator, 6-2
security settings, C-2
background user, 6-2
security settings, C-6
monitor, 6-2
security settings, C-5
network operator, 6-2
security settings, C-4
operator, 6-2
security settings, C-3
pre-existing, 6-7

H

heartbeat details, 15-2, 15-9, 15-15, 15-21
help
facilities for messages, 13-37
activity log, 9-21
online, 9-20
tip of the day, 9-20
horizontal scrolling, 9-11
HOSTS.LOCAL data set, 5-51

I

I (Ignore) action, 5-14
IBM TCP/IP
monitoring, 13-2
resource definitions, 10-48
customizing, 15-48
started tasks, 4-2
icon panel database, 7-6
implementation considerations, multisystem environment, 7-6

implementation process
authorizing for TCP/IP, 5-47
customizing regions, 5-2
CA-XCOM, 5-28
CONNECT:Direct, 5-29
CONNECT:Mailbox, 5-34
file transfer, 5-27
FTS, 5-36
defining region as
CONNECT:Direct user, 5-32
FTS user, 5-37
defining the administrator, 5-18
implementing
automatic problem recording, 5-54
FTP event flow, 5-38
printers, 5-20
SMF exit for FTP receiver, 5-42
template system, 5-19
installing FTS message handler, $RFAGENT, 5-37
implementing
the FTP event flow, 5-38
the SMF exit for FTP receiver, 5-42
inactivating a resource, 13-40
Index Menu, 9-16
INI procedure
editing, 5-15
generating, 5-15
propagating parameter group records, 5-15
INIFILE JCL parameter, 5-16
initialization
dealing with failures, 5-13
listing failed parameter groups, 5-14
System Initialization in Progress dialog, 5-14
Initialization in Progress panel, 9-2
initiating an Auto Connect, 13-26
INMC links, 5-36
INQ command, 13-12
interface parameters
CONNECT:Direct, 5-6
CONNECT:Mailbox, 5-10
interface to Communications Server, authorizing, 5-47
interfaces, implementing
NetMaster Reporter, 5-68
TCP/IP, 5-11
interpreting extended display messages, 13-11
issuing commands to a file transfer application, 13-41

K

keywords
calendar, 17-4
dates, associating with, 17-4
knowledge base, 1-4
backup, 8-5
linked, 7-8
synchronization
focal point regions, 7-7
monitoring, 7-13
subordinates, 7-7
types
icon panel, 7-6
RAMDB, 7-6
knowledge base definitions, 1-8
adding, 9-17
browsing, 9-18
cancelling changes to, 9-14
copying, 9-19
deleting, 9-19
updating, 9-18

L

libraries, checking panel libraries, 5-13
Link Record Details panel, 7-15
links
multisystem support, 7-4
unlinking a region, 7-16
listing and managing
CA-XCOM transfer requests, 13-12
CONNECT:Direct processes, 13-19
TCP/IP connections, 13-23
listing commands, 10-62
lists
parameter group, 5-14
types, 9-10
loading
a file transfer rule set, 10-59
a system image, 10-59
file transfer rule set, 10-59
message rule sets, 16-6
system image, 10-59, 14-3
locating records, 9-13
log exit, NMCMLGEX, 5-35

log files, allocating, 5-22, 5-25
LOGFILES parameter group, 5-24
logging off, 9-3
logging on, 9-2
logs
activity, 8-4, 13-35
alert history, 11-8
displaying, 13-32
file transfer, 1-14, 13-33
transient, 13-36
merged, 13-39
LST command, 13-12

M

Managed Object Development Services. *See* MODS
manager resources
CA-XCOM resource definitions, creating, 10-25
CONNECT:Direct resource definitions
creating, 10-29
partners, creating, 10-32
CONNECT:Mailbox resource definitions, 10-38
creating, 10-38
customizing, 15-44
the availability map, 15-24
FTP resource definitions, 10-43
FTS resource definitions, 10-40
managing CA-XCOM transfer requests, 13-13
managing CONNECT:Mailbox resources
Auto Connect Queue, 13-27
BSC lines monitor, 13-28
SNA sessions monitor, 13-28
VSAM batch files, 13-28
managing processes, 13-22
mandatory fields, 9-14
MAXBATCH initialization parameter, 5-31
MAXUSERS initialization parameter, 5-31
menus, 9-5
merged transient log, size, 13-39
messages
delivery mechanism, 1-9
extended display messages, 13-11
help for, 9-21, 13-37
logging, selective, 16-2
rules, 16-4
suppressing, 13-34, 13-35
visibility, 1-9
MODIFY=RESP
MODS (Managed Object Development Services), checking control files, 5-13
monitor
group ID, security settings, C-5
security group ID, 6-2
monitor resources
CA-XCOM resource definitions, 3-5
creating, 10-27
CONNECT:Direct resource definitions, 3-11
creating, 10-34
CONNECT:Mailbox resource definitions, 3-19
creating, 10-39
customizing monitoring criteria
CA-XCOM, 15-2
CONNECT:Direct, 15-9
CONNECT:Mailbox, 15-15
FTP, 15-21
FTS, 15-19
customizing resource definitions, 15-46
resource definitions
FTP, 3-26
FTS, 3-23
monitoring
active alerts, 11-2
active file transfers, 12-2
monitoring and managing resources, 10-61, 13-1
monitors
alert, 1-10, 11-2
displaying information, 13-5, 13-6
file transfer, active, 1-10
graphical, 13-44
status, 1-10
multiple select lists, 9-10

multisystem support, 1-13
agents, 1-14
BSYS background user, 7-14
considerations, 7-6
focal point regions, 1-13
how it works, 7-2
links, 7-4
remote applications, 10-55
subordinates, 1-14
Sysplex, 7-5
unlinking a region, 7-16
Multi-System Support Menu, 7-9

N

name lookup, how it works in IBM TCP/IP, 5-51
names
case sensitive, 10-10
resources, 3-3
NetMaster for File Transfer
databases, 7-6
features and benefits, 1-3
introduction, 1-2
knowledge base, 7-6
multisystem operation, 7-6
NetMaster for File Transfer regions
activity logs, 8-4
CA-XCOM events, 3-8
CONNECT:Direct events, 3-14
distributed systems, 3-15
MVS, 3-14
CONNECT:Mailbox events, 3-21
customizing, 5-2
FTP events, 3-29
FTS events, 3-24
FTS links, 5-36
linked, keeping track of, 7-15
linking, 7-7
BSYS background user, 7-14
logging off, 9-3
logging on, 5-2, 9-2
unlinking, 7-16
user definition for background region, 6-2
NetMaster Reporter, 1-15
NetMaster Reporter interface, 5-68
data warehouse servers, 5-68
events, sending, 5-69
NETSTAT interface, enabling, 5-48
network map, 13-14
network operator, group ID, 6-2
security settings, C-4
network partitioning facility. *See* NPF
NMCDSTEX statistics exit, 5-30, 5-35
NMCMLGEX log exit, 5-35
NPF (network partitioning facility)
controlling access to
functions, 6-3
resources, 6-3
relationship with UAMS, 6-3
resource list members, 6-3
resource tables, 6-3
NSINTERADDR statement, 5-51
numbered lists, 9-10

O

online help, 9-20
for messages, 9-21
Open Edition security definition, 5-48
operation mode
AUTOMATED, 10-26, 10-31, 10-45
IGNORED, 10-23
MANUAL, 10-23, 10-26, 10-31, 10-45
operator group ID, 6-2
security settings, C-3
optional fields, 9-14
options definition file *See* ODF
OS/400, CONNECT:Direct commands, 13-41
owner resources, 3-2
operational relationship, 3-2

P

panel libraries, checking, 5-13
panels
customizing access sequence, 9-16
data entry, 9-13
paths to, A-1
shortcuts, 9-8

panels, alert monitor
Administration Menu, 5-55
Alert Monitor, 11-3
Custom Trouble Ticket, 5-58
Email a Trouble Ticket, 5-57
Interface Definition, 5-56
Trouble Ticket Data Entry Definition, 5-59
panels, AutoAssist
Auto Populate Selection List, 10-33, 10-52
panels, specific
Administration Task Log, 7-13
All Events, 18-5
Confirm Database Synchronization, 7-11
Confirm Swap Log, 8-4
Confirm Unlink, 7-16
Database Synchronization Status, 7-12
History Data, 18-3
Initialization In Progress, 9-2
Link Record Details, 7-15
Multi-System Support Menu, 7-9
NCL/EF : Database Search Criteria, 18-13
Search Criteria, 18-11
User Password Maintenance, 9-4
parameter groups
AUTOIDS, 10-59
CDAPI, 5-4, 5-6, 5-32
CDEVENTS, 5-24
CMAPI, 5-4
EVENTLOG, 5-66
FTLOGS, 5-22, 5-24
LOGFILES, 5-24
OPSYSIDS, 5-4
SOCKETS, 5-4, 5-11
SYSTEMID, 5-4
parameters
CA-XCOM, 13-12
GLOBAL command, 14-2
password, changing, 9-3
performing a custom search, 18-13
PINGCD macro, parameter details, 15-36
primary menu, 9-2
printers, implementing, 5-20
printing reports, 18-16
problem ticket
interface, alert monitor
custom, 5-58
defining, 5-56
e-mail, 5-56
raising, 1-14, 5-54, 15-29
raising for an alert, 11-7
SOLVE:Problem
$RMPB07S procedure, 5-54
link definitions, 5-54
user IDs, 5-54
PROBSOLV process, 15-29
processes
Automation Services, PROBSOLV, 15-29
complex operations, 15-33
CONNECT:Direct
issuing commands, 15-37
listing, 13-20
managing, 13-19, 13-22
PROFILE command, transient log, 13-37
prompted fields, 9-14

Q

queues
Active, 13-19
Bad, 13-19
Call, 13-19
Exec, 13-19
Hold, 13-19
Initial, 13-19
Retain, 13-19
Start, 13-19
Suspend, 13-19
Timer, 13-19
Wait, 13-19
X-R&T, 13-19

R

RACF, 6-13
sample security exits, 6-13
using SAF, 6-13
raising a problem ticket, 1-14, 5-54, 15-29

relationships
file transfer monitor and manager, 3-2
VSAM file server and CONNECT:Mailbox manager, 3-18
remote FTS regions, file transfer management, 10-58
reporting function, 1-15
implementing, 5-65
troubleshooting, 18-22
reports
all file transfer events, 18-5
checking print queue, 18-17
completed schedules, 18-8
defining to NetMaster for File Transfer, 18-20
failed file transfer events, 18-5
failed schedules, 18-8
final file transfer results, 18-6
NetMaster Reporter, 1-15
overview, 18-2
printing, 18-16
selection list, 18-4, 18-7
summary reports, 18-6
UAMS, user definition synchronization, 6-12
viewing, 18-3
resource definitions
DASD, 10-51
extended display messages, 13-11
file transfer managers, 10-24
file transfer monitors, 10-24
IBM TCP/IP, 10-48
tapes, 10-51
TCPaccess, 10-48
resource definitions, adding
Assisted Resource Definition Facility, by using, 10-24
Auto Populate Facility, by using, 10-32, 10-51
custom-built, 10-37
loaded system image, 10-61
resource definitions, customizing
CA-XCOM monitor details, 15-2
CONNECT:Direct monitor details, 15-9
CONNECT:Mailbox monitor details, 15-15
DASD definitions, 15-48
FTP monitor details, 15-21
FTS monitor details, 15-19
manager resource definitions, 15-44
monitor resource definitions, 15-46
panel access sequence, 9-16
tape definitions, 15-48
TCP/IP for MVS definition, 15-48
TCPaccess definition, 15-48
resource templates, 1-9
resources
controlling access to, 6-3
customizing definitions, 15-1
displaying file transfer resources, 13-3
monitoring, 10-61, 13-2
monitoring and managing, 13-1
names, 3-3
restarting, 14-9
shutting down, 14-6
all automated resources, 14-7
all resources, 14-8
specifying criteria for
CA-XCOM monitor, 15-2
CONNECT:Direct monitor, 15-9
CONNECT:Mailbox monitor, 15-15
FTP monitor, 15-21
FTS monitor, 15-19
restarting resources, 14-9
rule sets
EventView, 16-2
file transfer, 10-6, 20-6

S

SAF (System Authorization Facility)
calling an external security package, 6-5
relationship with UAMS, 6-5
sample security templates, 6-6
saving data, 9-14
scrolling, 9-10

searching
criteria, 18-13
custom, 18-13
database, 18-3, 18-10
events database, 18-10
EVNTDB database, 18-10
examples, 18-14
file transfer events, 18-10, 18-11
file transfer schedules, 18-12
security
combined NPF and external options, 6-5
CONNECT:Direct, 13-14, 13-19
external options, 6-5
for existing background users, 6-8
for existing users, 6-7
levels, 6-2
updating across linked regions, 6-11
security access, Open Edition, 5-48
security, controlling access to
functions, 6-3
resources, 6-3
security, supplied group IDs
administrator, 6-2
background user, 6-2
monitor, 6-2
network operator, 6-2
operator, 6-2
selecting panels
all panels, 9-15
using Index Menu, 9-16
using Panel Display List, 9-15
using sequence number, 9-15
setting
global operation mode, 10-62
resources to AUTOMATED, 14-8
setting resource to AUTOMATED, 14-8
shortcuts, 9-8
shutting down
all resources, 14-8
automated resources, 14-7
shutting down automated resources, 14-7
signon details, CONNECT:Direct
confirming, 13-15, 13-19
single select lists, 9-10
SMF exit for FTP receiver, 5-42
SNA sessions monitor, displaying, 13-28
SNMP trap, 1-14, 15-39
creating, 15-39
macro parameter details, 15-41
process, specifying in, 15-39
using, 15-39
SNMP, collecting data
from Communications Server, 5-50
from TCPaccess, 5-53
sockets interface, enabling, 5-48
SOLVE:Problem
automatic problem recording, 1-14, 5-54
$RMPB07S procedure, 5-54
link definitions, 5-54
user ID requirements, 5-54
specifying an exit, 15-29
specifying
availability map
map details, 15-27
timer details, 15-28
criteria
CA-XCOM monitor resources, 15-2
CONNECT:Direct monitor resources, 15-9
CONNECT:Mailbox monitor resources, 15-15
FTP monitor resources, 15-21
FTS monitor resources, 15-19
file transfer resource availability, 15-24
staging file, 7-14
started task, 10-48
displaying information, 13-7
started task, VSAM file server, 3-18
statistics exit, 5-29, 5-35
STATISTICS.EXIT initialization parameter, 5-30
status monitor, 1-10
file transfer schedules, 13-9
display, 13-9
status, file transfers
FTP consideration, 10-14
structured strings, 6-3
subordinates, 1-14
knowledge base synchronization, 7-7
supported TCP/IP software types, 5-11

suppressing messages
activity log, 13-35
associating rule sets to the system image, 16-6
defining message rules, 16-4
defining rule sets, 16-2
file transfer log, 13-34
synchronizing knowledge bases, and linking NetMaster for File Transfer regions, 7-7
system images, 10-4
Assisted Resource Definition Facility, 10-25, 10-29, 10-38, 10-40, 10-43
Auto Populate Facility, 10-51
controlling, 14-1
defining, 10-4
description, 1-8
for templates, 5-19
loading, 5-18, 14-3
cold, 14-5
warm, 14-5
resource definitions, adding, 10-61
system parameters
initial customization dialog, 5-3
listing parameter groups that failed initialization, 5-14
parameter group lists, 5-14
parameter groups, B-2
See also parameter groups

T

Tandem
CONNECT:Direct commands, 13-41
file transfer management, 10-54
resources for CONNECT:Direct, 10-32
tape resource definitions, 4-3
customizing, 15-48
tapes
displaying information, 13-8
monitoring, 13-2
TCP/IP connections
customizing criteria, 15-22
displaying information, 13-5, 13-6
dropping, 13-24
listing, 13-23
monitor, customizing criteria, 15-7, 15-13
TCP/IP data set prefix, specifying, 5-12
TCP/IP interface, 5-11
TCP/IP listener, displaying information, 13-5, 13-6
TCPaccess
collecting SNMP data from, 5-53
monitoring, 13-2
PARM data set, reviewing, 5-52
SNMCFG*xx* member, 5-53
SNMP agent, 5-53
SNMP community name, 5-53
startup procedure, 5-12
subsystem ID, 5-12
TCPCFG*xx* member, 5-52
TCPaccess resource definition, 10-48
customizing, 15-48
FTP manager consideration, 10-48
started task, 4-3
TCPCFG*xx* member, 5-52
TCPIP.DATA data set, specifying, 5-12
templates
Communications Server resource definitions, 4-2
copying $TEMPLAT system image, 5-19
DASD resource definition, 4-3
description, 1-9
distributed, 1-4
specifying version to use, 5-19
system, implementing, 5-19
tape resource definition, 4-3
TCPaccess resource definition, 4-3
versions, 5-19
templates, CA-XCOM
manager resource definitions
jobs, 3-4
started tasks, 3-4
monitor resource definitions
remote node, 3-7
stalled transfer, 3-6
TCP/IP connections, 3-7
TCP/IP listener task, 3-6
transfer requests, 3-5

templates, CONNECT:Direct
manager resource definitions
AS/400 application, 3-11
jobs, 3-10
started tasks, 3-10
Tandem application, 3-11
UNIX application, 3-11
Windows NT application, 3-11
monitor resource definitions
process queue, 3-11
process status, 3-12
remote node, 3-13
TCP/IP connections, 3-13
TCP/IP listener task, 3-13
transfer, 3-12
templates, CONNECT:Mailbox
manager resource definitions, 3-19
monitor resource definitions
Auto Connect queue, 3-19
BSC line, 3-19
SNA sessions, 3-20
VSAM file server, 3-18
templates, FTP
manager resource definitions
jobs, 3-26
started tasks, 3-26
monitor resource definitions
remote node, 3-28
TCP/IP connections, 3-27
TCP/IP listener port, 3-27
templates, FTS
INMC links monitor resource definition, 3-24
manager resource definitions
jobs, 3-23
remote region, 3-23
started tasks, 3-23
terminating a region, 13-40
tip of the day, 9-20
transfer requests
CA-XCOM
listing, 13-13
managing, 13-12, 13-13
monitor heartbeat, 15-3
transient logs, 13-36
displaying an activity log, 13-38
merged, 13-39
size, 13-39
message help, 13-37
printing, 13-37
printing merged transient logs, 13-39
resetting, 13-37
specifying what to display, 13-37
transmitting knowledge base records, 7-17
trouble tickets
interface, alert monitor
custom, 5-58
defining, 5-56
e-mail, 5-56
raising for an alert, 11-7
See also problem tickets
troubleshooting
reporting function, 18-22
user definition synchronization, 6-12

U

UAMS (User Access Maintenance Facility)
calling
NPF, 6-3
SAF, 6-5
relationship with
NPF, 6-3
SAF, 6-5
synchronizing user definitions across linked regions, 6-11
staging file, 7-14
troubleshooting, 6-12
update report, 6-12
UNIX
CONNECT:Direct commands, 13-41
file transfer management, 10-55
multisystem considerations, 10-55
resources for CONNECT:Direct, 10-32
shell commands, 13-43
unlinking a region, 7-16
UPDATE mode, switching to, 9-13
updating background user definitions, 6-8
User Access Maintenance Subsystem. *See* UAMS
user definitions
generating background users, 6-8
synchronization
report, 6-12
troubleshooting, 6-12
User Password Maintenance panel, 9-4
user profiles
alert monitor, 11-5
copying, 6-9
defining, 6-9

V

VA command, 13-13, 13-21
VAC command, 13-13, 13-21
validating data, 9-14
variables
    e-mail problem tickets, D-2
    file transfer, D-2
    file transfer rules, use in examples, D-2
VB command, 13-21
VC command, 13-21
VE command, 13-21
vertical scrolling, 9-11
VH command, 13-13, 13-21
VI command, 13-13, 13-21
viewing all file transfer events, 18-5
VR command, 13-21
VS command, 13-13
VSAM batch files
    assisted reorganization, 13-30
    displaying and managing, 13-28
    managing, 13-30
VSAM file server started task, 3-18
VST command, 13-21
VSU command, 13-21
VT command, 13-21
VW command, 13-21
VXR command, 13-21

W

warm load, 14-5
wildcard characters, 10-7
windows, 9-22
    simultaneous display of, 9-22
    swap, 9-22
Windows NT
    CONNECT:Direct commands, 13-41
    file transfer management, 10-57
    resources for CONNECT:Direct, 10-32

X

XCOM. *See* CA-XCOM