CA NetMaster® File Transfer Management

Administration Guide

Release 12.1

CA Technologies Product References

This document references the following CA Technologies products:

- CA NetMaster® File Transfer Management (CA NetMaster FTM)
- CA NetMaster® Network Management for SNA (CA NetMaster NM for SNA)
- CA SOLVE:FTS
- CA XCOM™ Data Transport® for z/OS (CA XCOM Data Transport for z/OS)
- CA Network and Systems Management (CA NSM)
- CA Service Desk for z/OS (CA Service Desk)
- CA SOLVE:Central™ Service Desk for z/OS (CA SOLVE:Central). Includes SOLVE:Problem
- CA TCPaccess™ Communications Server for z/OS (CA TCPaccess CS for z/OS)
- CA TCPaccess™ FTP Server for z/OS (CA TCPaccess FTP Server for z/OS)
- CA ACF2™ for z/OS (CA ACF2 for z/OS)
- CA Top Secret® for z/OS (CA Top Secret for z/OS)
- CA Automation Point (CA AP)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 4: Implementing Logging 39

Chapter 5: Controlling the System Image 55

Chapter 19: Implementing Services 249

Chapter 20: Producing Reports 261

Chapter 32: Implementing Print Services 403

Appendix A: File Transfer Variables 415

Appendix B: File Transfer Events Mapping 419

Appendix C: Application Programming Interface 421

Chapter 1: Introduction

This section contains the following topics:

Intended Audience

This guide is intended for technical personnel responsible for the planning, setup, and maintenance of your product's functions and services.

Typographic Conventions

This table explains the conventions used when referring to various types of commands and when indicating field attributes.

Convention	Description
Commands	Commands such as SYSPARM and SHUTDOWN are shown in uppercase.
User Entries	Information to enter onto panels is displayed in **bold** text.
Cross-References	Cross-reference links to other sections of the book are displayed as underlined blue text.
Shortcuts	Shortcuts to menus or options are displayed in **bold**, for example, **/PARMS**.

Chapter 2: Starting and Stopping a Region

This section contains the following topics:

Start SOLVE SSI

To start the SOLVE SSI, issue the following command:

```
S ssiname,REUSASID=YES
```

For a region to connect to SOLVE SSI, it must first know the SSID to connect to. To identify the SSID, specify the SSID JCL parameter or use Customizer parameter groups. When this connection is complete, authorized region users can issue SOLVE SSI commands.

The region can use the SSID JCL parameter to establish an early connection to SOLVE SSI during initialization.

This parameter has the following format:

```
SSID={ NO | * | name }
```

NO

(Default) Does not attempt to connect to SOLVE SSI. The connection is only started (or attempted) after a SYSPARMS SSID command is issued.

*****

Starts or attempts a connection to an SSID with the first four characters of the region job name.

name

Starts or attempts a connection to the specified SSID.

If asterisk (*) or *name* is specified, an attempt to connect to the SSI is immediately made. If it fails, it retries every *n* seconds, depending on the default value of the SSI retry interval.

Note: To change the value of the SSID to connect at any time, update the SSI parameter group (enter **/PARMS**). You can use this parameter group to change the SSID value or to specify an SSI retry interval.

Stop SOLVE SSI

To stop SOLVE SSI, use *one* of the following methods:

- Enter the following command:

  ```
  SSI STOP
  ```

- Enter the following operating system STOP (P) command:

  ```
  P ssiname
  ```

Note: If you use cross memory services but have not specified REUSASID=YES when you start SOLVE SSI, the address space running SOLVE SSI terminates and is not available until after the next IPL.

Start a Region

To start a region, you run it as a job or a started task. A started task has been set up during the installation process.

To start a region, issue the following command:

```
S rname,REUSASID=YES
```

Users log on to a region by using the user IDs and passwords specified in their UAMS (or external security package) records.

WTOR Confirmation Message

If you have implemented region startup confirmation, the RMIWTO06 WTOR message is displayed and startup pauses.

The WTOR message enables you to change the startup parameters. If a reply to the message is not made in 120 seconds, startup continues.

Note: For information about startup confirmation, see the online help for the AUTOIDS parameter groups.

Continue Startup with No Change

To continue startup with no change to the parameters, reply as follows:

```
R n,U
```

n is the identification number of the WTOR message.

Continue Startup with Changes

To continue startup with changes to the parameters, reply as follows:

```
R n,parameter-1=value-1[,parameter-2=value-2[,…[,parameter-n=value-n]]]
```

You can use the following parameters in your reply. The parameters change the field values in the AUTOIDS parameter group specification panel that affects the loading of the system image.

SYSTEM

Corresponds to the System Image Name field.

VERSION

Corresponds to the Version field.

MODE

Corresponds to the Automation Mode field.

COLD

Corresponds to the Cold Start on Next Restart? field.

If you reply to change parameters, you are asked to confirm your changes. You can then make additional changes or accept the displayed values.

Example: Load a Different System Image

This example reply changes the system image to load to PROD version 2:

```
R n,SYSTEM=PROD,VERSION=2
```

Stop a Region

If you have the necessary authority, you can shut down the region.

To stop a region, issue the operating system STOP (P) command.

You can also stop a region by issuing *one* of the following commands: **SHUTDOWN** or **FSTOP**.

SHUTDOWN Command

The SHUTDOWN command 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.

You can issue the SHUTDOWN command from OCS or Command Entry. Alternatively, you can issue it as a z/OS MODIFY command.

Note: For more information about the SHUTDOWN command, see the online help.

FSTOP Command

The FSTOP command immediately disconnects user sessions and shuts down the region.

Restrict the use of the FSTOP command.

You can issue the FSTOP command from OCS or Command Entry. Alternatively, you can issue it as a z/OS MODIFY command.

Important! If you are running another product in the same region, it also stops if the FSTOP command is issued.

Note: For more information about the FSTOP command, see the online help.

Start NMFTP Monitor Region

To start the NMFTP monitor, issue the following command:

S *nmftname*

nmftname

Specifies the name of the NMFTP monitor.

Stop NMFTP Monitor Region

To stop the NMFTP monitor, issue the following command:

F *nmftname*, FSTOP

nmftname

Specifies the name of the NMFTP monitor.

How You Preserve Data When Region Stops and Restarts

You can preserve some data when a region stops so that this data is available when the region restarts. You can use global variables to preserve data. You can save global variables that the region reloads when it restarts. Saved global variables are known as persistent global variables.

To preserve data, create global variables with data you want to preserve and save them, for example:

- Use the Persistent Variables Administration option (access shortcut is /PVARS).
- Call the $CAGLBL procedure using the SAVE option.

  Note: For information about the $CAGLBL procedure, see the *Network Control Language Reference Guide*.
- Use the SETVARS and GLBLSAVE macros in a process definition.

Create Persistent Global Variables Using the User Interface

You can create persistent global variables from the Persistent Variables List panel. The panel also lets you maintain those variables, for example, update, purge, or reload them.

To create a persistent global variable using the user interface

1. Enter the **/PVARS** panel shortcut.

   The Persistent Variables List panel appears.
2. Press F4 (Add).

   The Persistent Variable - Add panel appears.
3. Specify the name of the variable (without its global prefix) and its value. Press F3 (File).

The variable is saved so that it can be loaded the next time the region starts up.

Prevent the Reloading of Preserved Data

If problems occur during region startup because of invalid data being loaded, you can disable the reloading of the preserved data.

To prevent the reloading of preserved data, enter the following command when you start the region:

```
S rname,PARM='XOPT=NOPVLOAD'
```

The region starts without reloading the preserved data.

About self-test

You can use self-test to display the major configuration details of your CA NetMaster region. Self-test looks at the following areas:

- IP socket interface
- SSI communication and Packet Analyzer status
- USS (UNIX System Services) interface
- Region authority and other details

Messages are displayed at the successful completion of each test. If errors are found, appropriate messages are displayed. For help about error messages, place the cursor on the error message and press F1 (Help).

Access Self-test

To access Self-test

1. Enter the **SELFTEST** command on the OCS panel.

To access online help about the SELFTEST command

1. Enter **SELFTEST ?** on the OCS panel.

Chapter 3: Configuring a Region

This section contains the following topics:

Region Configuration

After you have completed installation and startup, your region is operational at a basic level; however, you must configure it to suit your requirements.

How You Use JCL Parameters to Configure a Region

JCL parameters enable you to configure a region. You use JCL parameters to set region information. This information includes, for example, the names of your INIT and READY procedures, and the types of security exit to use in your region.

This information is supplied by the PPREF statements in the RUNSYSIN member.

You can also pass this information in the START command using the JCL PARM field. If you specify multiple parameters, separate each with a comma.

Note: For more information, see the *Reference Guide*.

How You Display and Change JCL Parameter Settings

You can display the current settings of all the JCL parameters with the SHOW PARMS command from OCS or Command Entry. To change any of these parameters, specify their new values in the RUNSYSIN member and then restart the region.

Note: For more information about JCL parameters, see the *Reference Guide*.

How You Identify the Region to Users

If you have multiple regions or communicate with other regions, you can set the domain ID and put titles on the panels.

How You Identify Domains and Panels

The NMDID JCL parameter identifies the domain ID for each region. If you have multiple regions, specify a different domain ID for each one.

Note: For more information about the NMDID parameter, see the *Reference Guide*.

You can use the SYSTEMID (System Identifications) parameter group in Customizer to help identify your regions. This parameter group specifies a system identifier that is used when you link to other regions. Specify a different system identifier for each of your regions.

This parameter group also specifies the titles to display on the logon panel and the OCS console panel. These titles help users to identify the region that they have logged on to.

Note: The system ID parameter takes effect when the region is initialized.

Region Customizer

Customizer lets you review and update parameter groups.

You use Customizer to initialize and customize your region. Customizer is an initialization facility that lets you implement a region rapidly and easily. Also, Customizer enables you to customize parameters easily at a later stage.

When you first install a product, you set various parameters to get the product up and running. Customizer helps you set up these parameters. An initial dialog is supplied for the first time user, to walk you through the customization process. You are prompted to supply required and optional parameter values.

To access the parameter groups, enter **/PARMS**.

What Are Parameter Groups?

System parameters are grouped by category (such as Security) in logical parameter groups, to simplify the process of initializing and customizing a region.

Groups of individual parameters translate into one or more of the following:

- SYSPARMS that determine how your region functions
- Global variables that various NCL applications use to control their functions
- Local parameters that define how to implement actions associated with parameter groups

System Parameters

Most customization of your region is performed by using Customizer.

You can also use the SYSPARMS command to customize your region. Each operand of the SYSPARMS command lets you specify options to change and customize the way your region works. For ease of maintenance, you can use the Display/Update SYSPARMS panel, which is accessible by using the /SYSPARM panel shortcut.

Notes:

- SYSPARMS set by Customizer parameter groups can only be updated using Customizer.
- For SYSPARMS without a corresponding parameter group, set the SYSPARMS in the INIT and READY procedures so that they are applied when the region starts. You can update them dynamically using the SYSPARMS command.
- For more information about SYSPARMS operands, see the *Reference Guide*.

Use the SYSPARMS Command

To change a SYSPARMS operand with the SYSPARMS command, enter the following command at the OCS command line:

```
SYSPARMS operand=value operand=value ...
```

Example: Display Time on OCS Title Line

This example sets the time display at the beginning of the OCS title line using the following command:

```
SYSPARMS OCSTIME=YES
```

Initialization Operands

There are some SYSPARMS command operands that cannot be changed while the region is operational. These operands must be included in your INIT procedure so that they are executed during initialization.

Note: For a complete list of SYSPARMS commands, see the *Reference Guide*.

If you specify new values for these initialization operands, the new values do not take effect until the region is initialized. All other SYSPARMS can be changed during region operation by authorized users.

Capture Messages Not Handled by Rules

If you want to capture certain messages missed by your resource definitions and message rules, use the Unmatched Message Alerting (UMA) feature. By capturing these messages, you can review them later to create rules for them.

To capture messages not being handled by your resource definitions and message rules

1. Enter the **/PARMS** panel shortcut.

   The Parameter Groups panel appears.

2. Enter **F MSGAWARENESS**.

   The cursor locates the MSGAWARENESS parameter group.

3. Enter **U** next to the group.

   The group opens for updating.

4. Specify **ACTIVE** in the Unmatched Message Alerting field, and customize the parameters to capture the type of messages you require.

   Unmatched Message Alerting Filter

   Specifies the type of messages you want to capture.

   Unmatched Message Alerting Options

   Specifies how you want to be notified of the captured messages. The notification can be by one or all of the following methods:

   - Raise alerts.
   - Log the occurrences of the messages.
   - Issue EDS events.

   Press F6 (Action).

   The region starts to capture the specified messages.

5. (Optional) Press F3 (File) if you want to make the changes permanent.

   The group is updated with the changes.

Transient Log Tuning

A *transient log* is a log of activities associated with a resource that is monitored. One transient log exists for each resource definition loaded in a region and exists as long as the definition remains loaded in the region. You can specify the age over which logged activities are deleted to keep their number down. When the default size parameters do not suit your requirements, you can customize them. You can also change the size of the transient logs for selected resources.

Customize Tuning Parameters

The AUTOTABLES parameter group contains the tuning parameters for transient logs. The parameters control the default and maximum sizes, and the deletion of logged activities that are over a specified age. For example, when overflows occur in the logs, you can lower the maximum size while you investigate the cause of the problem.

To customize the tuning parameters for transient logs

1. Enter the **/PARMS** panel shortcut.

   The Parameter Groups panel appears.

2. Enter **F AUTOTABLES**.

   The cursor locates the AUTOTABLES parameter group.

3. Enter **U** beside the group.

   The group opens for updating.

4. Customize the parameters for transient logs to suit your requirements. Press F6 (Action).

   The changes are applied in the region.

5. (Optional) Press F3 (File) if you want to make the changes permanent.

   The group is updated with the changes.

Resize Selected Transient Logs

After your region operates for a while, you may find that you need to tune the size of some transient logs. You may also find that you need to change the resource definition templates to suit your requirements.

Important! Resizing a transient log updates the resource definition. It is recommended that if a resource needs a large transient log size, it should be updated individually. If you have a large system image and you set all resource transient logs to the maximum size, there could be system performance degradation and storage issues.

To resize selected transient logs

1. Access the list of system images that contain the resources for which you want to resize logs. For example, enter /RADMIN.I.L to access the list of local system images.

   A System Image List panel appears.

2. Enter **STL** beside the required image.

   A Set TLog Size Specification panel appears.

3. Select the required resources using the Resource Class and Resource Name fields, specify the required size for their logs, and then press F6 (Action).

   A message appears, indicating the number of resource definitions affected.

4. Press F6 (Action).

   The resource definitions are updated with the specified size. If the image is active, the affected logs are also resized.

Note: For active system images, you can also resize the transient logs from the monitors using the SETTLOG command.

Resize Multiple Transient Logs in an Image

If the transient logs for certain resources become full, you can resize them from a resource monitor.

Important! Resizing a transient log updates the resource definition. It is recommended that if a resource needs a large transient log size, it should be updated individually. If you have a large system image and you set all resource transient logs to the maximum size, there could be system performance degradation and storage issues.

To resize multiple transient logs in an image from a resource monitor

1. Enter **SETTLOG** at the Command prompt.

   You are prompted to select the image that contains the resources whose logs you want to resize.

2. Enter **S** beside the required image.

   A Set TLog Size Specification panel appears.

3. Select the required resources using the Resource Class and Resource Name fields, specify the required size for their logs, and then press F6 (Action).

   A message appears, indicating the number of resource definitions affected.

4. Press F6 (Action).

   The resource definitions are updated with the specified size, and the affected logs are resized.

Chapter 4: Implementing Logging

This section contains the following topics:

Log Types

CA NetMaster FTM provides file transfer logs and activity logs.

File transfer logs record messages from the following:

- CA XCOM Data Transport for z/OS
- CA SOLVE:FTS
- CONNECT:Direct
- CONNECT:Mailbox
- FTP
- Generic Data Transfer API

Allocate File Transfer Data Sets

During initialization, the region is allocated three log data sets. Complete this task to allocate up to seven data sets.

Note: The log file IDs are of the form RFTLOG*nn* and the data set names are of the form *dsnpref.rname*.RFTLOG*nn*.

To allocate file transfer log files

1. Define additional log data sets.
2. Enter **/PARMS** at the prompt.

   The list of parameter groups appears.
3. Enter **U** beside the FTLOGS parameter group.

   The Initialization Parameters panel appears.
4. Press F8 (Forward).

   The next panel appears.
5. Complete the fields for each file you want to make available. For more information about completing the panel, press F1 (Help).
6. To allocate more files, press F8 (Forward) again.
7. Press F6 (Action).

   The files are allocated and opened.
8. When the parameter group completes 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 OS/390 event messages. You specify the suppression parameters in the CDEVENTS parameter group.

Disable File Transfer Logging

To disable file transfer logging

1. Enter **/PARMS** at the prompt.

   The list of parameter groups appears.

2. Enter **U** beside the FTLOGS parameter group.

   The Initialization Parameters panel appears.

3. Complete the following field:

   Is Logging Required?

   Enter **NO**.

4. Press F3 (File).

   The system saves the changes.

Enable File Transfer Schedule Recovery

By logging file transfer schedule events you can retain active schedule details across a system outage or when a new system image (see page 57) is loaded.

To enable file transfer schedule logging

1. Enter **/PARMS** at the prompt.

   The list of parameter groups appears.

2. Enter **U** beside the FTSCHD parameter group.

   The Initialization Parameters panel appears

3. Complete the required fields. For more information about completing the panel, press F1 (Help).

4. Press F6 (Action).

   The new settings are activated.

5. Press F3 (File).

   The system saves the changes.

Activity Logs

The activity logging facility records all the activity in your region. You can use the activity logs to help determine the cause of problems.

Two separate activity log formats exist:

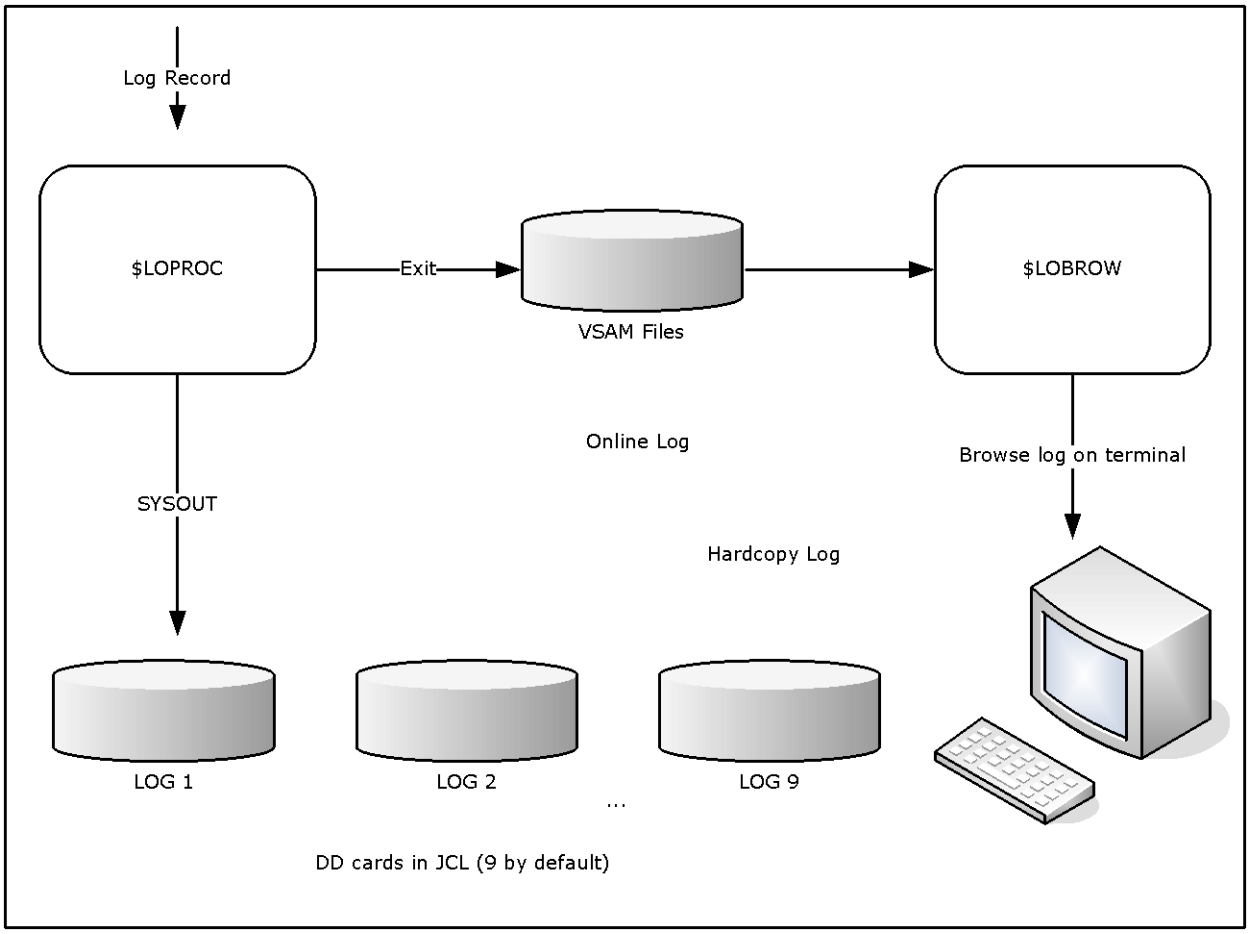
- Online
- Hardcopy

Log records are written to both formats.

By default, activity logs contain the following information:

- All commands entered
- All responses to commands entered
- Any unsolicited messages received from VTAM or the operating system, provided the related interfaces are available
- All messages explicitly written to the log by NCL procedures

The following illustration shows the path that the log record takes in the system.



The online activity log is supplied by the distributed procedure $LOPROC. The $LOPROC procedure writes log data to VSAM files (three by default). The VSAM files are accessed by a second procedure, $LOBROW, which allows online browsing of the log.

Note: $LOPROC and $LOBROW are the default procedure names. You can change these names by using the LOGFILES parameter group in Customizer (**/PARMS**).

Customize Activity Log Settings

By customizing the LOGFILES parameter group, you can do the following:

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

To customize activity log settings

1. Enter **/PARMS** at the prompt.

   The list of parameter groups appears.

2. Enter **U** beside the LOGFILES parameter group.
3. Complete the following fields:

   Log Operating System Messages?

   Set to **YES** to enable message logging.

   Log Commands?

   Set to **YES** to enable command logging.

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

4. Press F3 (File).

   The system saves the changes.

Administer Online Activity Log Files

From the Activity Log : Administration menu, you can do the following:

- Swap active activity logs
- List all days contained in log files and browse logs for a particular date
- List all log files and browse a particular file

To administer online activity log files, enter **/LOADMIN** at the prompt.

The Activity Log : Administration menu appears.

Note: For information about the options available on this menu, press F1 (Help).

Increase the Number of Activity Log Files

During initialization, the region is allocated three log data sets; however, you can allocate up to seven data sets.

Note: As supplied, the log file IDs and data set names are respectively NMLOG*nn* and *dsnpref.rname*.NMLOG*nn*.

To increase the number of activity log files

1. Enter **/PARMS** at the prompt.

   The list of parameter groups appears.

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

   The Parameter Group panel appears

3. Create new activity log files. Press F8 (Forward) to scroll through the panels.

   Note: For more information about completing the panel, press F1 (Help).

4. Press F6 (Action).

   The new settings are activated.

5. Press F3 (File).

   The system saves the changes.

Swap the Online Log

The online activity log automatically swaps to a fresh VSAM file when each file fills up.

You can manually swap your currently active VSAM file if you want to free a particular log file (for example, for backups).

Important! Swapping the current VSAM log causes the $LOPROC procedure to write all subsequent activity log records to the next VSAM log. If this log was previously used, it is reset. Therefore, you can no longer browse the old records that it contained.

To swap the online activity log

1. Enter **/LOGSWAP** at the prompt.

   The Activity Log Services : Confirm Swap Log panel appears.

2. Press F6 to request the log swap, or F12 to cancel your request.

   Note: If the $LOPROC procedure encounters a VSAM error when it is logging activity to an online log file, it automatically swaps to the next log file.

Online Log Exit

You can create an NCL procedure to intercept, analyze, and react to the messages that are sent to the activity log.

Use the LOGFILES parameter group in Customizer to specify the name of your exit.

The exit is executed every time a message is sent to the log. Using the exit to perform complex functions can degrade the performance of the region.

Note: Ensure that your log exit procedure is well-tested before you put it into production.

Variables Available to the Activity Log Exit

The following variables are available to the activity log exit:

&#LO$RECORD

Contains records of the following formats:

time_generated user_id terminal_id message_text

The text of the message starts at the fourth word of the record.

arrival_time origin region* $$AOMTIME$$ *aom_time message_text

The text of the message starts at the sixth word of the record. This format lets you identify AOM-sourced messages.

You can change the contents of this variable. To suppress the message from the log, set the variable to NOLOG.

Note: For more information, see the &LOGREAD verb in the *Network Control Language Reference Guide*.

$LOG

Specifies a Mapped Data Object (MDO) that contains the message attributes. The MDO is mapped by the $MSG map.

You can use the &ASSIGN verb to query the MDO.

Note: For information about querying MDO components and additional variables, see the *Network Control Language Programming Guide*.

Example: Remove Messages from the NCL Log

The following shows an example procedure:

```
&CONTROL
-*-----------------------------------------------*
-* TO REMOVE IKJ56247I MESSAGES FROM THE NCL LOG. *
-*-----------------------------------------------*
&PARSE DELIM=' ' VARS=#LO$WORD* DATA=&#LO$RECORD
&IF .&#LO$WORD4 EQ .IKJ56247I &THEN +
        &#LO$RECORD = NOLOG
```

Enable the Log Exit

To enable the log exit

1. Enter **/PARMS** at the prompt.

   The Customizer : Parameter Groups list appears.

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

   The Customizer : Parameter Group panel for the LOGFILES parameter group appears.

3. Enter the name of your activity log exit in the Log Exit Name field.

4. Press F6 (Action).

   The changes are applied.

5. Press F3 (File).

   The changes are saved.

Online Logging Procedure

The default online logging procedure is $LOPROC. This procedure is designed to work with the online browsing procedure $LOBROW.

You can replace the $LOPROC and $LOBROW procedures with your own customized NCL procedures. Alternatively, you can write a customized log browsing procedure to present the supplied data files (from $LOPROC) in your own format.

Structure of Supplied Log Files

The supplied log files (NMLOG01, NMLOG02, and NMLOG03) have the following physical file structure:

- The record key has the following format:

  YYYYMMDDHHMMSSHS*nnnn*

  nnnn=1000 + (reset every 100th of a second) and key length=20 bytes

- A record has the following contents

  ORIGIN

  Contains the terminal name.

  REGION

  Contains the user ID.

  TEXT

  Contains the message text to display in the activity log.

  MSGATTR

  Contains the 2-byte color/highlight indicator. Colors are R=red, Y=yellow, W=white, B=blue, G=green, T=turquoise, or P=pink. Highlight values are R=reverse, B=blink, U=underscore, or N=none.

  ORIGTIM

  Contains the time at the remote domain.

  ORIGDMN

  Contains the name of the originating domain.

  ORIGSRC

  Contains the ID of the remote terminal.

Note: For more information, see the following references:

- The description of the &FILE OPEN verb in the *Network Control Language Reference Guide*.
- The *Network Control Language Programming Guide*.

How You Write Logging and Browsing Procedures

To write your own customized NCL procedure to replace $LOBROW, use the &FILE OPEN statement with FORMAT=DELIMITED.

You can store your log records in whatever file format you want. Your log browsing procedure must match this file format.

Note: For more information, see the descriptions of the following verbs in the *Network Control Language Reference Guide*:

- &LOGREAD
- &LOGCONT
- &LOGDEL

Implement Logging and Browsing Procedures

After you write your own browsing procedure or your own logging and browsing procedures, you implement them for use.

To implement your procedures

1. Enter **U** next to the LOGFILES parameter group in Customizer.
2. Update the relevant fields.
3. Press F6 (Action).

   Your procedures are used for logging and browsing.
4. Press F3 (File).

   Your changes to the parameter group are saved.

Hardcopy Activity Log

A region can have more than one hardcopy activity log, of which only one is open for logging.

Your region can be configured to perform logging to disk, tape, or hard copy. From one to nine logs can be specified by including the required number of DD statements in the execution JCL. Logging can be specified to wrap when the last log is full or is swapped.

To obtain the status of these logs, use the SHOW LOGS command.

Note: When logging to disk the following DCB attributes should be used:

```
DSORG=PS,RECFM=VBA,LRECL=137,BLKSIZE=15476
```

Format of Logged Information

Each entry recorded on the log has the following format:

```
12.04.23.12   SMITH      TERM54     +V NET,ACT,ID=NCP001
```

This entry consists of the following information:

- A time stamp in the format *hh.mm.ss.hs* (where *hh* is the hour, *mm* is the minute, *ss* is the second, and *hs* is the hundredth of a second)
- The user ID that entered the command or logged the message
- The terminal from which the command was entered or to which a message is sent
- The text of the message or command

Commands are highlighted with a plus sign (+) prefixed to the text to make it easier to distinguish commands from messages when browsing the log. If the command entered is an unsolicited VTAM command, it is highlighted and prefixed with an equals sign (=).

Format of Logged Timer-initiated Commands

Commands executed as the result of a timer-initiated command are prefixed by a plus sign, followed by the identity number of the timer command responsible. This identity number has the following format: #*nnnn*.

Example: Logged Timer-initiated Command

This example shows the log record of a command initiated by a timer:

```
15.00.00.01   NETOPER   CNTL01    +#0005 D BFRUSE
```

Format of Logged Commands Executed in Background Environments

Commands executed under the control of background environments are identified by the following keywords in the user ID field for the command text and any resulting messages:

BG-SYS

Background System Processor

BG-MON

Background Monitor

BG-LOG

Background Logger

Format of Logged Commands from NCL Procedure-dependent Environment

If a command is executed from an NCL procedure-dependent environment (&INTCMD), the node field on the log contains the NCL ID of the process issuing the command.

Format of Log After Time Change

If a time change causes the time to go backward, the activity log differentiates the records that overlap in time by adding a plus sign (+) after the time for the newer records. The feature is only available when you are viewing the log in the default or NORMAL format.

Format of the Hardcopy Log

The hardcopy log data set has the following format:

- A heading on each page—contains the day and date on which the log was created and the system identifier (NMID) of the originating region.
- A log identifier on the right side of the page. The log identifier is the ddname under which the log was created. This log identifier assists log collation after printing.
- 60 lines on each page—this format can be altered to suit your requirements using the SYSPARMS LOGPAGE operand.

  Note: For information about LOGPAGE, see the *Reference Guide*.

Swap the Hardcopy Log

Swapping the current log frees the log for immediate printing. Swapping the log is possible only when another unused log remains to which logging can continue. You can specify up to nine logs. Logs do not need to be consecutive.

To swap the log, enter the LOGSWAP command.

When a log is swapped, the log status, the requesting user ID, and the reason for the swap are recorded. You can display these details with the SHOW LOGS command.

Each of the logs is identified in the JCL member by the LOG*n* ddname. *n* is in the range one to nine.

Example: Log Name

This example defines the LOG4 ddname:

```
//LOG4 DD SYSOUT=A,FREE=CLOSE
```

Mixing of device types is valid. Inclusion of FREE=CLOSE prints the log when it is released by the LOGSWAP command.

Reuse of Hardcopy Log Data Sets

Wrapping lets you reuse a LOG data set when all of the available LOG data sets have been used.

The LOGWRAP SYSPARM determines whether log data set wrapping is allowed. You set the value of this SYSPARM in the Are Activity Logs to Wrap? field when you customize the LOGFILES parameter group in Customizer (**/PARMS**).

If you specify NO (the default) in the Are Activity Logs to Wrap? field, then wrapping is not permitted. When all the LOG data sets have been used due to successive LOGSWAP commands, the previous LOG data sets cannot be reused. After the last LOG data set is used, any further LOGSWAP commands are rejected.

If you specify YES in the Are Activity Logs to Wrap? field, log wrapping is allowed according to the following rules:

- If you direct your LOG data sets to SYSOUT, then, as each LOG*n* DD statement is used, the data set is unallocated because FREE=CLOSE. In this case, you can reissue an ALLOC command to reallocate another SYSOUT file under the same ddname. For example:

  ```
  ALLOC DD=LOG3 SYSOUT=A FREE=CLOSE
  ```

  This ddname is now available for use as another LOG data set. Subsequent LOGSWAP operations can now reuse this LOG data set rather than rejecting the command when the last LOG data set is used.
- If the LOG DD statements point to sequential data sets, log wrapping overwrites the earlier LOG data held in these data sets. Archive the existing data before allowing the wrap to occur.

Cross-Reference of Hardcopy Logs

To help operations staff to piece the full log together, certain information is recorded on the last and first lines of swapped LOG data sets.

The first line of a new log contains the reason for the swap, or the initiating user ID.

The last message printed on a swapped log is the ddname of the new log. Also printed at the start of the new log is the ddname or logical ID for the previous log.

I/O Errors on the Hardcopy Log

If an I/O error occurs on a log, the log is closed and the next available log is automatically swapped to, if one is available, and logging continues. This also applies to data set full conditions when logging to disk.

If the I/O error occurs on the last available log, a warning message is sent to all monitor terminals informing them that logging has ceased. The STATUS command also includes a warning message if logging is stopped. All log messages are passed to LOGPROC for analysis even if no log output is possible.

Write to the System Log

You can use the SYSPARMS SYSLOG operand to write all logged output or all VTAM PPO messages received to the system log.

To write all logged output to the system log also, enter the **SYSPARMS SYSLOG=YES** command.

To write all VTAM PPO messages to the system log also, enter the **SYSPARMS SYSLOG=PPO** command.

Note: For more information about the SYSPARMS SYSLOG operand, see the *Reference Guide*.

Chapter 5: Controlling the System Image

This section contains the following topics:

Define a System Image

A system image must be defined for your CA NetMaster FTM 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 CA NetMaster FTM region, of which only one can be active at any one time.

Note: One system image is required for each CA NetMaster FTM region. If you are defining a system image for a subordinate, use the name assigned during the multisystem linking process.

To define a system image

1. Enter **/RADMIN.I** at the command prompt.

   The System Image List appears.

2. Press F4 (Add).

   The ResourceView : System Image Definition appears.

3. Complete the following fields:

   System Name

   Specifies the name of the system image.

   Database Version

   Specifies the version number allocated to the system image definition.

   Home System

   Specifies the name of the system on which the image can be loaded.

   Short Description

   Briefly describes the system image.

   EventView Ruleset to Activate

   Specifies the ruleset to activate when the system image becomes active.

   Press F3 (File).

   The system image is added to the knowledge base.

Load a System Image

You define the operations requirements of the resources to be managed on a system in a system image. You must create a system image definition before you can define the resources you want to manage.

The region loads a system image during region initialization. During operation, you may need to change the system image by loading another image.

Note: When you request to load a system image, the $RMEXSTR exit NCL procedure is executed before the starting process. This procedure may be customized at your site to perform any required tasks before any automated resources are started. The starting process cannot proceed if the exit sets a non-zero return code.

For products that use desired state automation, resources are started according to any relationships defined in the system image, and subject to resource availability.

To load a system image

1. Enter **/RADMIN.I** at the prompt.

   The ResourceView : System Image List appears.

2. Enter **L** beside the system image that you want to load.

   The LOAD Command Parameter Specification panel appears.

3. Complete the following fields:

   SysName to be Loaded

   Enter **?** and select a system image from the displayed prompt list.

   Global Automation Mode

   Specify the global operation mode for your system image.

   Perform COLD Start?

   If the Checkpoint Restart Status field is set to ACTIVE, you can enter NO in the Perform COLD Start? field to specify a warm load.

4. Press F6 (Action) to load the system image.

   The Command Confirmation panel appears.

5. Enter **CONFIRM** in the Response field.

   The system image is loaded.

Important! Resources that are monitored by the region are defined to the system image. Loading a system image affects all users of this region and may influence the resources in the system image.

Checkpoint Restart Function

The checkpoint restart function lets you preserve manual overrides across system restarts.

When checkpoint restart is active, any override placed on a resource is stored in the resource definition as checkpoint data. This checkpoint data is applied automatically to the resource when you load the system image with a Warm Start, restoring previously placed overrides.

When checkpoint restart is inactive, any override placed on a resource is not stored as checkpoint data; however, previously stored data is retained. With checkpoint restart inactive, a Warm Start does not apply any stored checkpoint data.

Note: Setting checkpoint restart inactive does not clear the stored checkpoint data. If you later set checkpoint restart to active, then a Warm Start applies the previously stored checkpoint data.

If you no longer want to restore previously placed overrides, load the system image with a Cold Start. All checkpoint data is cleared from the resource definitions, and the resources are loaded without overrides.

Cold Start also clears checkpoint data from the following resources:

- Resources in shared system images (both active and inactive) that satisfy the following conditions:
  - The resource has the local system as the home system.
  - The resource is not active on another system.
- Resources in z/VM system images where the z/VM system image has the local system as the home system

Note: The local system is where the system image is being loaded.

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 setting of the global operation mode limits the control of all resources defined to a system image. For example, if the global operation mode is MANUAL and the resource operation mode is AUTOMATED, the resource can run in the MANUAL operation mode only. If the global mode is changed to AUTOMATED, then that resource runs in its assigned mode.

You can issue a GLOBAL command from the resource monitor to set the global operation mode. For example, you have finished testing a system image on a development system in the MANUAL operation mode and you want to change the global operation mode to AUTOMATED. If you are experiencing severe problems on a production system, you can change the global operation mode from AUTOMATED to MANUAL.

Important! 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, verify that all resources are defined correctly before the change.

Set Global Operation Mode

To set the global operation mode

1. From the status monitor, enter **GLOBAL** at the prompt.

   A Global Command Parameter Specification panel appears.

2. Enter **AUTOMATED** or **MANUAL** in the Global Automation Mode field and press F6 (Action).

   A confirmation panel appears.

3. Enter **CONFIRM** in the Response field.

   The region changes the operation mode of all resources.

Example: Set Global Operation Mode

If the region is running in the MANUAL operation mode and you want to test the effects of automation on the resources in the system, set the global operation mode to AUTOMATED.

Enter the following command at the prompt of the monitor:

```
GLOBAL MODE=AUTOMATED
```

The Execute GLOBAL Command panel is displayed. Enter **S** next to the required system image. The region sets all of the resource operation modes to their normal value. This normal value is the mode defined in the resource or set by an override.

Shut Down Resources in a Loaded System Image

You can use the following commands to shut down the resources defined to a loaded system image:

SHUTSYS

Shuts down all resources with an operation mode of AUTOMATED.

SHUTFORCE

Shuts down all resources.

Shut Down Automated Resources

Note: This procedure is valid only if the global operation mode is set to AUTOMATED.

To shut down resources that are in an operation mode of AUTOMATED

1. Enter **SHUTSYS** at the prompt on the status monitor.

   If the region is linked to other regions, the Execute SHUTSYS Command panel appears listing the loaded system images in all linked regions. Go to Step 2.

   If the region is a standalone region, the Command Confirmation panel appears. Go to Step 3.

2. Enter **S** next to the system image you want to shut down.

   The Command Confirmation panel appears.

   Important! Issuing the SHUTSYS command shuts down all resources that are in the AUTOMATED mode.

3. Enter **CONFIRM** in the Response field.

   All automated resources defined to the system image are shut down.

Shut 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** beside the resource to stop it manually.

Shut Down All Resources

To shut down all resources in a system image

1. Enter **SHUTFORCE** at the prompt on the status monitor.

   If the region is linked to other regions, the Execute SHUTFORCE Command panel appears listing the loaded system images in all linked regions. Go to Step 2.

   If the region is standalone region, the Command Confirmation panel appears. Go to Step 3.

2. Enter **S** next to the system image you want to shut down.

   The Command Confirmation panel appears.

3. Enter **CONFIRM** in the Response field.

   The resources defined to the system image are shut down.

Restart Resources in a Loaded System Image

You can restart resources defined to a loaded system image that were shut down using the SHUTSYS or SHUTFORCE commands:

To restart the resources in a loaded system image:

1. Enter **STARTSYS** at the prompt on the status monitor.

   If the region is linked to other regions, the Execute STARTSYS Command panel appears listing the loaded system images in all linked regions. Go to Step 2.

   If the region is standalone, the Command Confirmation panel appears. Go to Step 3.

2. Enter **S** beside the system image that you want to restart.

   The Command Confirmation panel appears.

3. Enter **CONFIRM** in the Response field.

   The resources in the loaded system image start.

Back Up the Knowledge Base

The method you select for backing up the knowledge base depends on the configuration of your product regions and your operations requirements.

Note: The knowledge base is a data set named *dsnpref*.RAMDB, which is a VSAM data set.

Backup methods depend on whether your regions are:

- Nonproduction 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.

Create a Backup Region

To create a backup region

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.

2. From the backup region, enter **/RADMIN.I** at the prompt.

   The System Image List panel appears.

3. Press F4 (Add) to create a system image definition, and then enter **L** beside it to load the empty image.

4. Enter **/PARMS** at the prompt.

   The parameter groups appear.

5. In the AUTOIDS parameter group, complete the following fields:

   System Image Name

   Specifies the name of the empty system image.

   Version

   Specifies the version of the empty system image.

6. In the FTLOGS parameter group, complete the following field:

   Is Logging Required?

   Specify **NO** to disable logging of file transfer events.

7. In the EVENTLOG parameter group, complete the following field:

   Enable Event Logging

   Specify **NO** to disable recording of file transfer events in the EVNTDG database

8. In the FTPCNTL parameter group, complete the following field:

   Enable FTP Event Receivers

   Specify **NO** to disable the FTP event flow.

9. Enter **/MADMIN** at the prompt.

   The Multi-System Support Menu appears.

10. Select SD.

    The Remote System Identification panel appears.

11. Complete the following fields:

    Primary Name

    Specify the ACB name of a production region to link to.

    Role in Multi-System Operation

    Specify FOCAL to link this region as a focal point. Specify SUBORDINATE to link this region as a subordinate point.

    Work Dataset

    Specify the name of a VSAM data set that can be used as the work data set to reduce the synchronization time.

12. Press F6 (Action).

    The system copies the production regions' knowledge base to the backup region's knowledge base, creating a snapshot copy that you can retain for back up.

13. Enter **/MADMIN.U.**

    The backup region is unlinked from the production region.

14. Shut down the backup region and save the *dsnpref*.RAMDB data set.

    Important! Remember that this is a snapshot of the production knowledge base.

Chapter 6: Implementing Resource Templates

This section contains the following topics:

Resource Templates

Important! The supplied INTNL class resource templates are required for the region to function properly. Do not modify these templates.

After you have defined a system image, you can define resources in it. Your product includes sample resource templates, which you can use to define commonly used resources. The templates supply values for certain resource definition fields, and simplify the task of creating your own specific 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. Each version can contain, in addition to the resource templates, the availability maps and processes used by resource templates.

USRCLS Class Template

No sample USRCLS class templates are supplied. However, you can create your own templates to facilitate the definition of similar resources. The templates provide the methods for operating USRCLS class resources (if supported by your product).

Set Up Your Template System

Templates are defined in a $TEMPLAT system image. Your template system may contain different versions of templates. Group each version in a different $TEMPLAT system image.

Before you work on templates, copy the supplied templates to a different $TEMPLAT version. Start with version 0010; versions 0001 through 0009 are reserved for software updates.

To copy a $TEMPLAT system image

1. Enter **/RADMIN.T.I** at the prompt.

   The Template System Image List panel appears.

2. Enter **C** beside the system image you want to copy.

   The System Image Definition panel opens.

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.

4. Press F3 (File).

   The System Image Copy panel appears advising you of the status of the copying process. When the copying process is complete, the System Image List panel appears.

5. Set up one $TEMPLAT system image version for general use. Review the templates to ensure that they are suitable for the resources on your system. The version to use is set in the OPSYSIDS parameter group under the NAMES category during region initialization. Enter the **/PARMS** shortcut to access the Customizer : Parameter Groups panel that enables you to access the parameter for update.

$TEMPLAT System Image for Multiple Products

Each product supplies its own templates for the supported resource classes. If you want to run different products in the same region, merge the $TEMPLAT system images that contain those templates.

Note: For information about how to merge system images, see the *Reference Guide*.

Make the Template Available

To make the new copy of the template system image available for use

1. Enter **/PARMS** at the prompt.

   The list of parameter groups appears.

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

   The Customizer : Parameter Group panel appears.

3. Complete the following field:

   Active Template Image Version

   Specifies the version number of the image .

4. Press F6 (Action).

   The images are available for use.

5. Press F3 (File).

   The system saves the changed value.

   The image is made available automatically the next time the region starts up.

Associate a Template to a Resource Class

To associate a template to a resource class

1. Enter **/RADMIN.T.R** at the prompt.

   The Resource Template Definition List appears.

2. Enter **S** next to the resource class to which you want to associate the template.

   A list of templates associated with the resource class appears.

3. Enter **AP** in front of the template.

   The Automation Services : Apply Template panel appears.

4. Define how you want to apply the template and press F6 (Action).

   The ResourceView : System Image List appears.

5. Select the system image to which you want to apply the template.

   The Automation Services : Messages List panel appears with details of the process.

6. Press F3 (File).

   All resources on the selected images that are associated with the template are updated.

Resource Template Definitions

Note: The name of a template must contain alphanumeric, @, #, $, ., :, -, (, and) characters only. It must not be a number.

The panels used to add a resource template definition for a particular resource class are the same as the panels that you use when you add a resource definition for that class. You can define any information that will be used generically by a specific resource.

Variables

You can use a variable to supply the value for a field in the resource template definition.

Disable Substitution of Variables

Variables in a template are substituted by their values when you apply the template to a resource definition. You can disable variable substitution—that is, you want the variable to appear in the resource definition, *not* the value of the variable.

To disable the substitution of a variable during application, replace the ampersand (&) in front of the variable name by the underline character (_).

For example, if you specify _ZMSGTEXT in a template and apply the template to a resource definition, _ZMSGTEXT becomes &ZMSGTEXT in the resource definition.

Specify a Variable to Represent a Left-justified Fixed-length Field

Some messages contain left-justified fixed-length fields for resource names. If the name is not of the maximum length, the name is left justified. You cannot use normal variables because they do not provide padding.

To handle left-justified fixed-length fields, use less-than signs (<).

Each < represents one character. For example, <<<<< represents a five-character field with left justification.

Specify a Variable to Represent a Right-justified Fixed-length Field

Some messages contain right-justified fixed-length fields for resource names. If the name is not of the maximum length, the name is right justified. You cannot use normal variables because they do not provide padding.

To handle right-justified fixed-length fields, use greater-than signs (>).

Each > represents one character. For example, >>>>> represents a five-character field with right justification.

Maintenance of Resource Template Definitions

You can browse, update, copy, and delete resource template definitions. You can copy a resource template definition between or in $TEMPLAT system images.

Apply Updated Templates

You may have defined a number of resources by using a template and that template has since been updated. You can use the AP action code to reapply the template to update those resource definitions.

To apply updated templates

1. From the templates list, enter **AP** beside a template.

   The Apply Template panel appears.

2. Specify how the updates are performed.
3. Press F6 (Action).

   A list of system images appears.

4. Enter **S** beside the system images that contain the resource definitions that you want to update and then press Enter to apply the template to the included definitions.

Availability Maps in a Template System Image

You can define availability maps in a $TEMPLAT system image. You can then use these maps with resources built from the templates.

The procedures for creating and maintaining maps for resource templates are similar to the procedures for creating and maintaining maps for resource definitions.

Access Map Definitions in a Template System Image

To access the map definitions in a $TEMPLAT system image

1. Enter **/RADMIN.T** at the prompt.

   The Template Definition Menu appears.

2. Enter **A** at the prompt.

3. (Optional) If you want to use a different version of the $TEMPLAT system image, change the value in the Template Version field and then press Enter.

   The relevant map list panel appears. The panel lists all the maps in the selected $TEMPLAT system image.

Define and Maintain Processes in a Template System Image

You can use the processes in a $TEMPLAT system image in a resource template belonging to the same image. You can create new processes or change existing processes.

The procedures for creating and maintaining processes for resource templates are similar to the procedures for creating and maintaining processes for resource definitions (see page 213).

Access the Process Definitions in a Template System Image

To access the processes in a $TEMPLAT system image

1. Enter **/RADMIN.T** at the prompt.

   The Template Definition Menu appears.

2. Enter **P** at the prompt and, if you want to use a different version of the $TEMPLAT system image, change the value in the Version field.

   The Process List panel appears. The panel lists the processes in the selected $TEMPLAT system image.

Convert a Resource Definition into a Resource Template

You can convert a resource definition into a resource template to facilitate future definition of similar resources. After you are satisfied that a resource definition is working correctly, you can convert the definition into a template.

To convert a resource definition into a resource template

1. Use the Copy action to create another copy of the definition.
2. Change the system name on the General Description panel to $TEMPLAT, and specify the version of the $TEMPLAT image into which you want to copy the definition in the Database Version field.
3. Name the template on the General Description panel.
4. Replace the resource names on the other definition panels by *one* of the following:
   - &ZRMDBNAME if the name field is not of fixed length
   - Less-than signs (<) if the name field is of fixed length with left justification—this typically occurs in the message text
   - Greater-than signs (>) if the name field is of fixed length with right justification—this typically occurs in the message text

   Note: Keeping the name length to less than the maximum number of characters enables you to easily recognize the fixed length name fields in a message. For example, a seven-character name is displayed with an extra space in an eight-character fixed length field.
5. Replace the ampersand (&) in front of a variable by the underline character (_).
6. File the definition. Any associated availability map and processes are also copied if they do not exist already in the specified $TEMPLAT system image.

Chapter 7: File Transfer Management Resources

This section contains the following topics:

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, the following are provided:

- 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 Data Transport for z/OS transfer IDs, CONNECT:Direct processes, CONNECT:Mailbox IDs, FTP server names, CA SOLVE:FTS transmission definitions, generic data transfer APIs, 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, CA NetMaster FTM 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 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 may want to include a CA NetMaster FTM process that records the problem in your problem management application)

Chapter 8: File Transfer Application Resources

This section contains the following topics:

File Transfer Resources

A file transfer resource is an entity managed by your region. It has associated with it operational information that is stored in the knowledge base.

Two types of file transfer resources (a manager and its monitors) represent a file transfer product such as CA XCOM Data Transport for z/OS, CONNECT:Direct, CONNECT:Mailbox, CA SOLVE:FTS, or FTP.

File Transfer Manager

A file transfer manager represents a file transfer application. It can be a job, a started task, or a Windows 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

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.

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

CA NetMaster FTM 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.

CA XCOM Data Transport for z/OS Resources

A CA XCOM Data Transport for z/OS resource represents the CA XCOM Data Transport for z/OS application. In CA NetMaster FTM, this is called a *manager resource*.

Each manager resource has a set of monitor resources that represent the internal state of the manager resource.

For CA XCOM Data Transport for z/OS, the manager resource is the CA XCOM Data Transport for z/OS application. The monitor resources are as follows:

- Transfer Request Monitor
- Stalled Transfer Monitor
- TCP/IP Listener Task Monitor
- TCP/IP Connections Monitor
- Remote Node Monitor

CA XCOM Data Transport for z/OS File Transfer Monitors

The CA XCOM Data Transport for z/OS file transfer monitors represent the operational states that affect the performance of a CA XCOM Data Transport for z/OS file transfer service as follows:

CA XCOM Data Transport for z/OS Operational State	Monitors
The number of transfer requests in a CA XCOM Data Transport for z/OS 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 Data Transport for z/OS TCP/IP listener task is not available.	TCP/IP listener task monitor
A CA XCOM Data Transport for z/OS 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

CA XCOM Data Transport for z/OS Definitions

The CA XCOM Data Transport for z/OS region provides a file transfer service. You may have more than one region on a system to provide that service. CA NetMaster FTM manages these regions through the information in the CA XCOM Data Transport for z/OS file transfer manager resource definitions.

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

CA XCOM Data Transport for z/OS Manager Templates for Jobs and Started Tasks

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

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

CA XCOM Data Transport for z/OS File Transfer Monitor Definitions

CA NetMaster FTM uses the information in the CA XCOM Data Transport for z/OS 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 Data Transport for z/OS 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 Data Transport for z/OS 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.
- CA XCOM Data Transport for z/OS monitor resource events that change the actual state of the monitor resource to indicate a problem—you may want to include a CA NetMaster FTM 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 Data Transport for z/OS 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 stalled time limit that indicates that a transfer can be terminated.
- CA XCOM Data Transport for z/OS monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a CA NetMaster FTM 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 Data Transport for z/OS 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.
- CA XCOM Data Transport for z/OS monitor resource events that change the actual state of the monitor resource to indicate a problem—you may want to include a CA NetMaster FTM 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 Data Transport for z/OS 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.
- An idle time limit that indicates that a connection can be dropped (terminated).
- CA XCOM Data Transport for z/OS monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a CA NetMaster FTM 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).

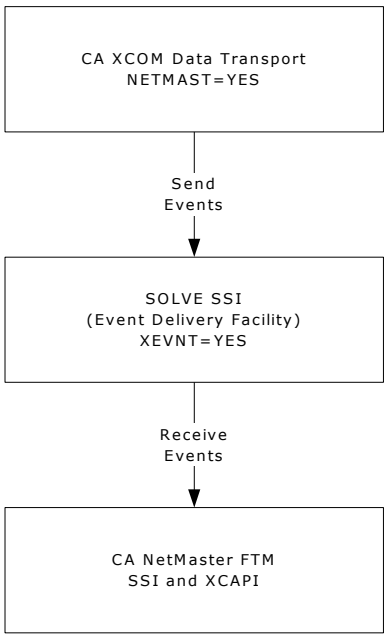
Remote Node Monitor Template

A template is provided for defining the CA XCOM Data Transport for z/OS 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.
- CA XCOM Data Transport for z/OS monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a CA NetMaster FTM 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 Data Transport for z/OS Service

Event flow from a CA XCOM Data Transport for z/OS region uses the SOLVE Subsystem Interface (SSI) event delivery facility. The following diagram shows the flow of events from CA XCOM Data Transport for z/OS on an MVS system to CA NetMaster FTM:



CA XCOM Data Transport for z/OS provides an exit that sends CA XCOM Data Transport for z/OS events to a receiver by using the event delivery facility. CA NetMaster FTM 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 CA NetMaster FTM SSI parameter group.

Note: For information about how to implement the event flow, see the *Installation Guide*.

CONNECT:Direct Resources

A CONNECT:Direct resource represents the CONNECT:Direct application. In CA NetMaster FTM, this is called a *manager resource*.

Each manager resource has a set of monitor resources that represent the internal state of the manager resource.

For CONNECT:Direct, the manager resource is the CONNECT:Direct application. The monitor resources are as follows:

- Process Queue Monitor
- Process Status Monitor
- Transfer Monitor
- TCP/IP Listener Task Monitor
- Remote Node Monitor

Note: The TCP/IP Listener Task Monitor does not apply to a distributed systems application.

CONNECT:Direct File Transfer Monitors

The CONNECT:Direct file transfer monitors represent the operational states that affect the performance of a CONNECT:Direct file transfer service. These states are monitored 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

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. CA NetMaster FTM 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 Windows.

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 CA NetMaster FTM 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 CONNECT:Direct for Windows in the knowledge base.

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

CONNECT:Direct File Transfer Monitor Definitions

CA NetMaster FTM 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.
- CONNECT:Direct monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a CA NetMaster FTM 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.

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 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 CA NetMaster FTM 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.
- CONNECT:Direct monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a CA NetMaster FTM 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.
- 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 CA NetMaster FTM 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: The template is not available on distributed systems.

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.
- CONNECT:Direct monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a CA NetMaster FTM 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).

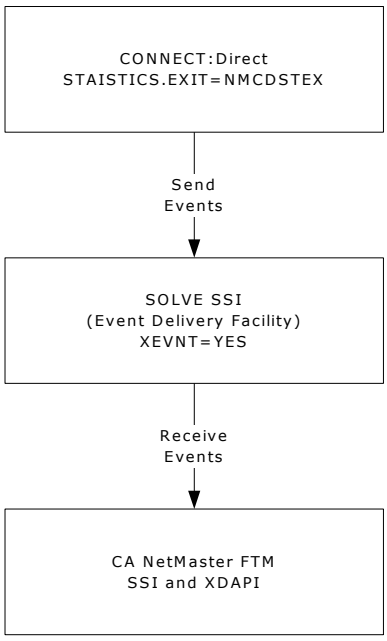
Event Flow from a CONNECT:Direct File Transfer Service

Event flow from CONNECT:Direct uses the following mechanisms:

- For CONNECT:Direct on a z/OS system, the mechanisms are the CONNECT:Direct statistics exit and SOLVE SSI event delivery facility
- For CONNECT:Direct on a distributed system such as Windows, the mechanisms are the CA NetMaster FTM agent and the TCP/IP link

z/OS System

The following diagram shows the flow of events from CONNECT:Direct on a z/OS system to CA NetMaster FTM:

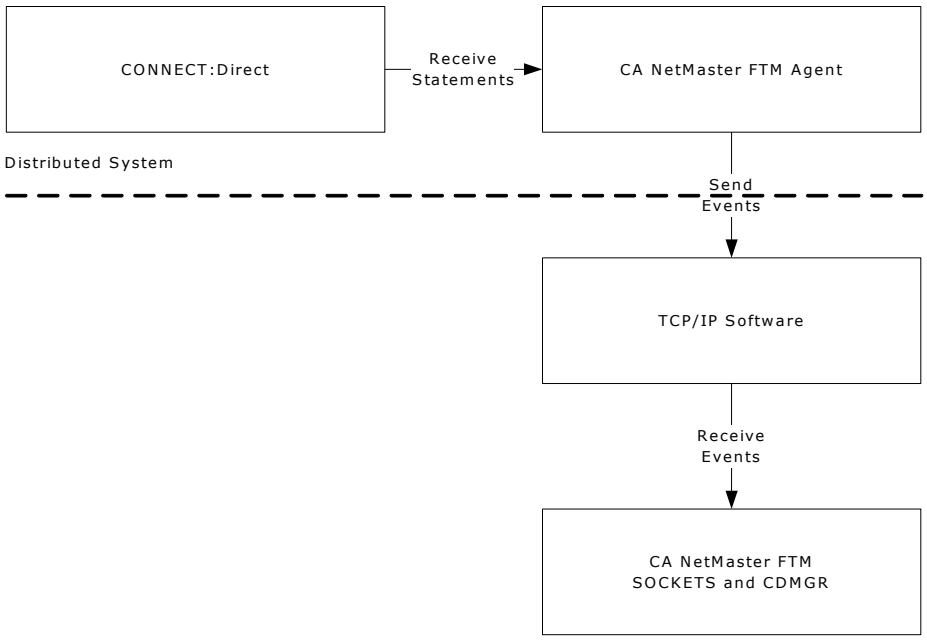


CA NetMaster FTM provides a CONNECT:Direct statistics exit, NMCDSTEX. The exit sends CONNECT:Direct events to a receiver by using the event delivery facility. CA NetMaster FTM listens to that receiver (specified in the CDAPI parameter group) for the events.

The SOLVE SSI task that provides the event delivery facility is specified in the CA NetMaster FTM SSI parameter group.

Distributed Systems

The following diagram shows the flow of events from CONNECT:Direct on Windows to CA NetMaster FTM:



CA NetMaster FTM provides agents for Windows systems. The agent forwards CONNECT:Direct events to the corresponding CONNECT:Direct manager (CDMGR) in your region.

The TCP/IP interface is implemented in the SOCKETS parameter group.

Notes:

- For information about how to implement the agent, see the *CA NetMaster File Transfer Management Agent—CONNECT:Direct Installation and Administration Guide.*
- For information about how to implement the TCP/IP interface, see the *CA NetMaster NM for TCP/IP Administration Guide*.
- For information about how to implement the CONNECT:Direct manager, see How to Define CONNECT:Direct Resources (see page 130).

CONNECT:Mailbox Resources

A CONNECT:Mailbox resource represents the CONNECT:Mailbox application. In CA NetMaster FTM, this is called a *manager resource*.

Each manager resource has a set of monitor resources that represent the internal state of the manager resource.

For CONNECT:Mailbox, the manager resource is the VSAM file server of CONNECT:Mailbox. The monitor resources are as follows:

- Auto Connect Queue Monitor
- Stalled SNA Sessions Monitor
- BSC Line Monitor

CONNECT:Mailbox Monitors

The CONNECT:Mailbox monitors represent the performance of a CONNECT:Mailbox application. These states are monitored 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. CA NetMaster FTM 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.

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 CA NetMaster FTM process that takes certain actions (for example, to record the problem in your problem management application).

CONNECT:Mailbox Monitor Definitions

CA NetMaster FTM 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.
- 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

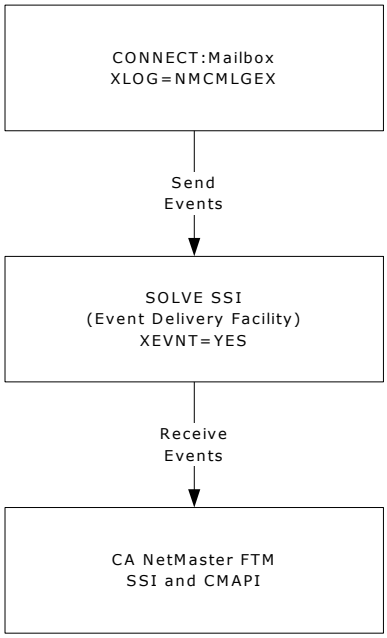
Stalled SNA Session Monitor Template

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.
- CONNECT:Mailbox monitor resource events that change the actual state of the monitor resource to indicate a problem.

Event Flow from CONNECT:Mailbox

The diagram below shows the flow of events from CONNECT:Mailbox to CA NetMaster FTM:



CA NetMaster FTM provides a log exit, NMCMLGEX. The exit sends CONNECT:Mailbox events to a receiver by using the event delivery facility. CA NetMaster FTM 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 CA NetMaster FTM SSI parameter group.

FTS Resources

An FTS resource represents the CA SOLVE:FTS application. In CA NetMaster FTM, this is called a *manager resource*.

Each manager resource has a set of monitor resources that represent the internal state of the manager resource.

For CA SOLVE:FTS, the manager resource is the CA SOLVE:FTS application. The monitor resources represent defined INMC Link Monitors.

FTS File Transfer Manager

CA SOLVE:FTS can be in the same or a separate region as CA NetMaster FTM. You must define a manager for a CA SOLVE:FTS instance before you can manage the file transfers to and from that instance.

- If CA SOLVE:FTS is in the same region, the manager enables the monitoring of file transfers. It does not manage the region itself.
- If CA SOLVE:FTS is in a separate region on the same system, the manager (as managing either a job or started task) enables the monitoring of file transfers. It also manages that separate region.
- If CA SOLVE:FTS is on another system, the manager enables the monitoring of the communications path to the remote region and the file transfers. It does not manage the remote region itself.

FTS File Transfer Manager Definitions

CA SOLVE:FTS provides a file transfer service. You can have more than one region on a system to provide that service. CA NetMaster FTM interacts with these regions through the information in the FTS file transfer manager resource definitions.

FTS Manager Template for Local Region

A template is provided for defining a manager for CA SOLVE:FTS in the local CA NetMaster FTM region. The template contains the following information to help you manage file transfers to and from the region:

- Processes that activate, inactivate, and retrieve status information about file transfer monitoring in the 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 process that takes certain actions (for example, to record the problem in your problem management application).
- A state change exit that activates the manager (and thus file transfer monitoring) when the system image is loaded (specifically, when its actual state changes from UNKNOWN to INACTIVE during the loading).

FTS Manager Templates for Jobs and Started Tasks

Templates are provided for defining managers for CA SOLVE:FTS jobs and started tasks. The templates contain the following information to help you manage a CA SOLVE:FTS region:

- System commands that activate, inactivate, and retrieve status information about the region.
- System and 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 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 CA SOLVE:FTS regions. The template contains the following information to help you manage a remote region:

- 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 process that takes certain actions (for example, to record the problem in your problem management application).

FTS File Transfer Monitor Definitions

CA NetMaster FTM uses the information in the FTS file transfer monitor resource definitions to monitor the operational states that affect the links between the CA SOLVE:FTS file transfer regions.

INMC Link Monitor Template

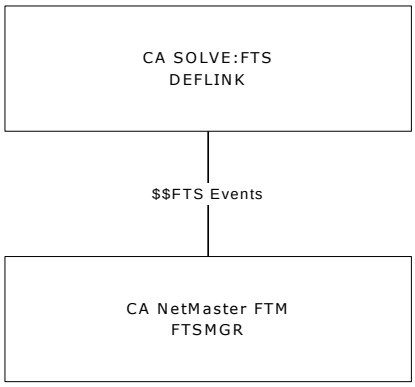
A template is provided for defining the FTS INMC link monitors in the knowledge base. You define one monitor for each link. The template contains the following information to help you monitor a link:

- 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 may want to include a CA NetMaster FTM 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

The FTS manager (FTSMGR) monitors file transfers through $$FTS events. When CA SOLVE:FTS and CA NetMaster FTM are in the same region, the event flow is within the region.

When CA SOLVE:FTS is in another region, the event flow is depicted by the following diagram:



The INMC link is provided by a DEFLINK command in the remote CA SOLVE:FTS region.

Note: For information about how to implement the event flow, see the *Installation Guide*.

For remote back-level CA SOLVE:FTS regions, you can continue to use the $RFAGENT message handler. The handler processes events before they are sent to the corresponding FTS manager in the CA NetMaster FTM region by using an INMC link.

FTP Resources

An FTP resource represents the FTP application. In CA NetMaster FTM, this is called a *manager resource*.

Each manager resource has a set of monitor resources that represent the internal state of the manager resource.

For FTP, the manager resource is the FTP application. The monitor resources are as follows:

- TCP/IP Port Monitor
- TCP/IP Connections Monitor
- Remote Node Monitor

FTP File Transfer Monitors

The FTP file transfer monitors represent the operational states that affect the performance of an FTP file transfer service. These are monitored 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

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, IBM's Communications Server *or* CA TCPaccess CS for z/OS.

CA NetMaster FTM 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 CA NetMaster FTM 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 CA NetMaster FTM process that takes certain actions (for example, to record the problem in your problem management application).

Customize CA TCPaccess FTP Server for z/OS Templates

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

FTP File Transfer Monitor Definitions

CA NetMaster FTM 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.
- FTP monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a CA NetMaster FTM 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.
- 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 CA NetMaster FTM 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.
- FTP monitor resource events that change the actual state of the monitor resource to indicate a problem—you might want to include a CA NetMaster FTM 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).

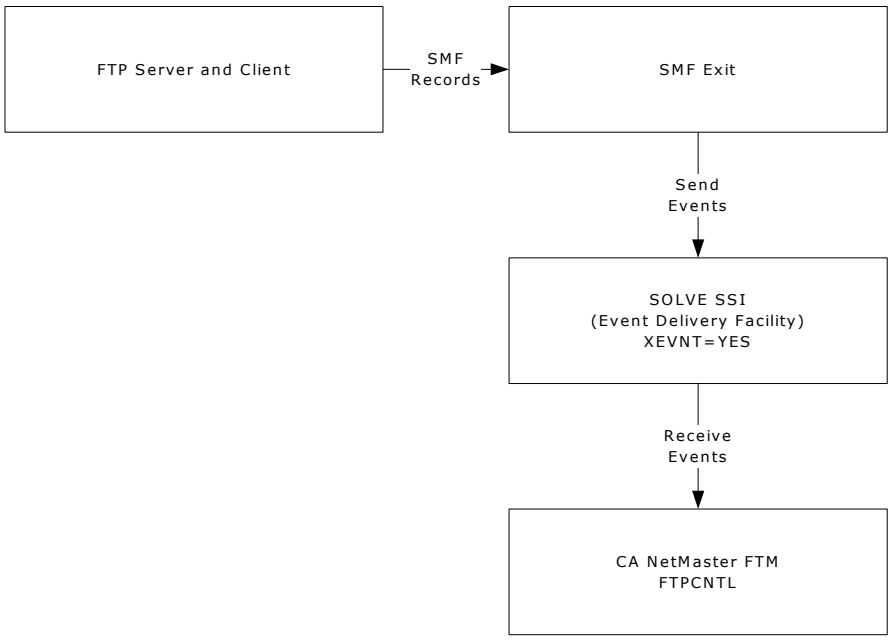
Event Flow from an FTP File Transfer Service

How events flow from an FTP server to CA NetMaster FTM depends on the underlying TCP/IP mechanism:

- CA TCPaccess CS for z/OS
- CA TCPaccess FTP Server for z/OS
- IBM's Communications Server

Event Flow from CA TCPaccess CS for z/OS

The following diagram shows the flow of events from an FTP server on CA TCPaccess CS for z/OS to CA NetMaster FTM if you are *not* using CA TCPaccess FTP Server for z/OS:

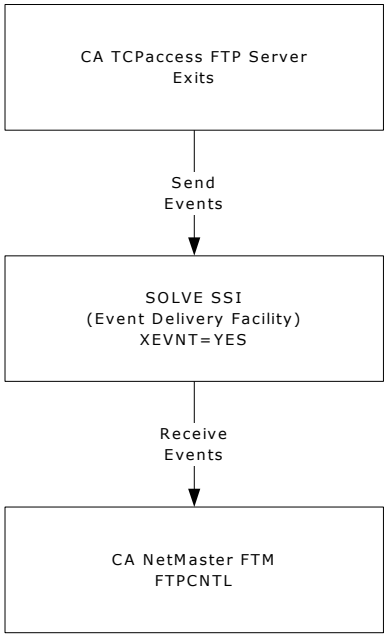


CA NetMaster FTM provides an SMF exit, IPSMFEX. The exit forwards FTP events to a receiver by using the event delivery facility. CA NetMaster FTM listens to that receiver for the events. The FTPCNTL parameter group controls whether that receiver is enabled.

The SOLVE SSI task that provides the event delivery facility is specified in the CA NetMaster FTM SSI parameter group.

Event Flow from CA TCPaccess FTP Server for z/OS

The following diagram shows the flow of events from the CA TCPaccess FTP Server for z/OS to CA NetMaster FTM if you are using CA TCPaccess FTP Server for z/OS:



CA TCPaccess FTP Server for z/OS forwards FTP events to a receiver by using the event delivery facility. CA NetMaster FTM listens to that receiver for the events. The FTPCNTL parameter group controls whether that receiver is enabled.

The SOLVE SSI task that provides the event delivery facility is specified in the CA NetMaster FTM SSI parameter group.

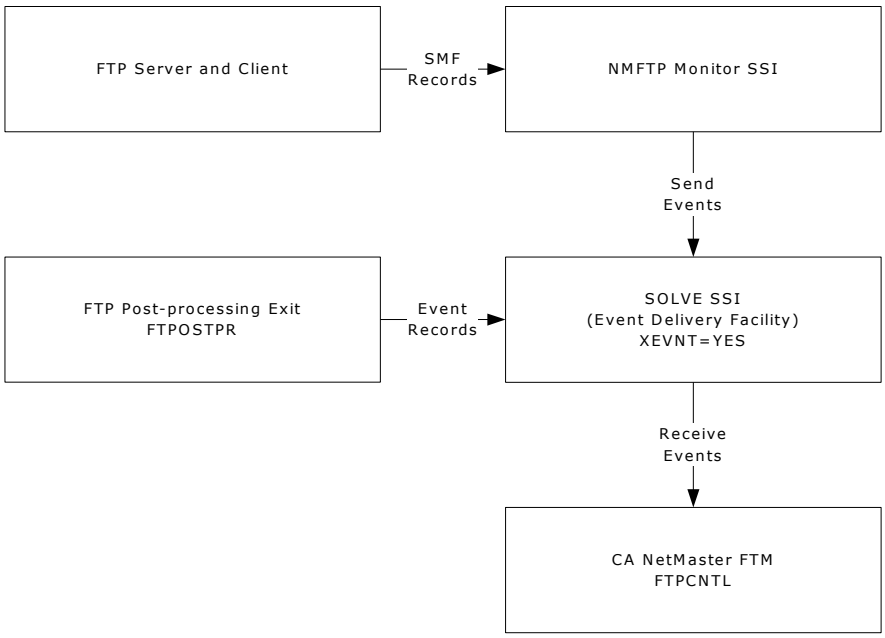
The CA TCPaccess FTP Server for z/OS policy rule sets and rules let you control the use of FTP functions. A rule set containing the policy rules must be defined for your CA NetMaster FTM region.

More information:

CA TCPaccess FTP Server for z/OS Policy Rule Sets (see page 153)

Event Flow from IBM's Communications Server

The following diagram shows the flow of events on IBM's Communications Server to CA NetMaster FTM:



CA NetMaster FTM provides an NMFTP Monitor SSI. The SSI exploits IBM's network management interface to obtain FTP file transfer-related SMF records and forwards the events to a receiver by using the event delivery facility. CA NetMaster FTM listens to that receiver for the events.

Note: The FTPCNTL parameter group controls whether the receiver is enabled.

The network management interface does not recognize termination failures if the file transfer does not start; therefore, the FTP post-processing exit, FTPOSTPR, is used to provide these missing events.

The SOLVE SSI task that provides the event delivery facility is specified in the CA NetMaster FTM SSI parameter group.

Chapter 9: Supporting File Transfer Resources

This section contains the following topics:

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.

CA NetMaster FTM can manage the following resources:

- IBM TCP/IP tasks
- CA TCPaccess FTP Server for z/OS and CA TCPaccess CS for z/OS tasks
- DASD
- Tapes

IBM TCP/IP Resource Definitions

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

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 CA NetMaster FTM process that takes certain actions (for example, to record the problem in your problem management application).

CA TCPaccess CS for z/OS Resource Definition

CA TCPaccess CS for z/OS can provide the TCP/IP mechanism by which files can be transferred. CA NetMaster FTM manages a CA TCPaccess CS for z/OS region through the information in the CA TCPaccess CS for z/OS resource definition.

CA TCPaccess CS for z/OS Resource Template

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

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

Note: If CA TCPaccess CS for z/OS is your FTP server, you may have defined an FTPMGR resource for your CA TCPaccess CS for z/OS region. If so, it is not necessary to define a CA TCPaccess CS for z/OS resource as well.

DASD and Tape Resource Definitions

DASD and tapes provide storage for the files in a file transfer. CA NetMaster FTM 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 CA NetMaster FTM process that takes certain actions (for example, to record the problem in your problem management application).

Chapter 10: Building the Management Environment

This section contains the following topics:

Build the Environment

CA NetMaster FTM helps you manage the following:

- File transfers
- File transfer schedules
- CA XCOM Data Transport for z/OS, CONNECT:Direct, CONNECT:Mailbox, CA SOLVE:FTS, and FTP server file transfer applications
- IBM's Communications Server and CA TCPaccess CS for z/OS 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.

To manage...	Create...
File transfers	File transfer rules
File transfer schedules	FTSCHD resource definitions
CA XCOM Data Transport for z/OS regions	XCMGR and XCMON resource definitions
CONNECT:Direct regions	CDMGR and CDMON resource definitions
CONNECT:Mailbox regions	STC, CMMGR, and CMMON resource definitions
CA SOLVE:FTS regions	FTSMGR and FTSMON resource definitions
IBM's Communications Server or CA TCPaccess CS for z/OS	FTPMGR and FTPMON resource definitions

To manage...	Create...
CA TCPaccess FTP Server for z/OS	FTPMGR and FTPMON resource definitions and policy rules
IBM's Communications Server or CA TCPaccess CS for z/OS	An STC resource definition
DASD and tapes	DASD and TAPE resource definitions
CONNECT:Direct file transfer service on a Windows system	CDMGR and CDMON resource definitions
FTS file transfer service on a remote system	FTSMGR and FTSMON resource definitions
Generic API	File transfer rules and schedule resources

After you define a system image and associated resources, you can load the system image, check the built environment, and automate your resources.

Define File Transfer Rules

The CA NetMaster FTM 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.

Important! To use file transfer rules for FTS transfers, define the FTS managers for the appropriate CA SOLVE:FTS regions. The managers enable the CA NetMaster FTM region to detect FTS file transfer events. To use file transfer rules for CONNECT:Direct transfers on distributed systems such as UNIX, define the CONNECT:Direct managers. Define CONNECT:Direct for OS/390 resources to enable access to the CONNECT:Direct messages.

To create a set of file transfer rules:

1. Define a file transfer rule set.
2. Add file transfer rules to the rule set.

Define a File Transfer Rule Set

To define a file transfer rule set

1. Enter **/FTADMIN.R** at the command prompt.

   The File Transfer Ruleset List appears.

2. Press F4 (Add).

   The File Transfer Ruleset panel appears.

3. Complete the following fields:

   Ruleset Name

   Specifies the name of the file transfer ruleset.

   Limits: 8 characters

   Description

   Briefly describes the file transfer ruleset.

   Press F3 (File).

   The definition is created in the knowledge base.

Add File Transfer Rules to a Rule Set

During operation, only one rule set is active in a CA NetMaster FTM 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

1. Enter **/FTADMIN.R** at the command prompt.

   The File Transfer Ruleset List appears.

2. Enter **R** beside the rule set to which you want to add rules.

   The File Transfer Rules panel appears.

   Note: If active rules have the same criteria, the rule with the name that occurs first alphabetically, is applied.

3. Press F4 (Add).

   The File Transfer Rule Filter panel appears.

4. Complete the following fields:

   Rule Name

   Specifies the name of the rule.

Rule Status

Specifies whether the rule is ACTIVE or INACTIVE. You can use this field to switch the rule on or off.

Description

Specifies a brief description for the rule.

Source/Target/XfrID

Identifies the events that the rule monitors. This value can be case sensitive.

- CA XCOM Data Transport for z/OS transfer ID
- Generic data transfer API product ID
- CONNECT:Direct processes
- CONNECT:Mailbox IDs or batch IDs
- FTP transfer ID
- CA SOLVE:FTS transmission definitions
- Files (or data set members)

Note: 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.

Type

Specifies the value that the Source/Target/TransferID field should monitor:

- **ID** applies to CA XCOM Data Transport for z/OS transfer IDs, CONNECT:Direct processes, FTP transfers, CA SOLVE:FTS transmission definitions, Generic API, or CONNECT:Mailbox IDs.
- **SOURCE** applies to outgoing files or CONNECT:Mailbox batch IDs.
- **TARGET** applies to incoming files or CONNECT:Mailbox batch IDs.

Transfer Status

Specifies the file transfer status that the rule should monitor:

- **START** monitors start of the transfer.
- **END** monitors end of the transfer.
- **FAILURE** monitors failure of the transfer.

Alert Severity

The severity of the alert that is raised when the rule is triggered.

Alert Autoclear

Specifies whether to close a generated alert automatically. If you specify YES:

- START alert is 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 is 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 time out whereby an alert is closed only after the specified period of time.

5. 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.

   Press F10 (Actions).

   The Alert Automated Actions panel appears.

6. Press F4 (Add).

   The Available Actions panel appears.

7. Select the actions to perform when a file transfer satisfies the rule.

   The actions you can specify include raising a problem record, notifying selected users, issuing a command, and running a process (see the online help).

8. Repeat step 6 until you have specified all the required actions, then press F3 (Exit) to exit the list of specified actions.

9. Press F11 (Alert) to override the default alert definition.

   The Alert Definition for File Transfer Rule panel appears.

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.

11. Press F3 (File).

    The definition is saved.

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.

Load a Rule Set on Demand

To load a rule set

1. Enter **/FTADMIN.R** at the command prompt.

   The File Transfer Ruleset List appears.

2. Enter **L** beside the rule set you want to load.

   The rule set is loaded for the session, replacing the rule set previously loaded.

Note: The default rule set defined in the AUTOIDS parameter group is not changed by this load action. If you want to change the default rule set you need to change the parameter group.

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 specify a value for transfers associated with a UNIX, Generic API, or Windows system, you must specify it in mixed case and special characters.

Note: The percent sign (%) and the underline (_) are not recognized as characters; file transfer rules and schedules recognize them as wildcard characters for file names and IDs.

If you specify a value for transfers associated with a z/OS system, you must specify it in upper case.

Note: This does not apply to HFS files.

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 Data Transport for z/OS File Transfers

A CA NetMaster FTM region identifies a CA XCOM Data Transport for z/OS 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
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	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.

Notes:

- CA NetMaster FTM does not receive an event at the start of a file transfer for CONNECT:Direct for Windows versions supported by CA NetMaster FTM.
- In CONNECT:Direct systems, if you run a job on a remote system and start monitoring after the request, the job file name is not returned with the end event notification.

Identify CONNECT:Direct File Transfers by Data Set Names

With CONNECT:Direct file transfers, a CA NetMaster FTM region cannot monitor the transfer of specific data set members. Do not identify members when you specify the file name or transfer ID criterion.

The region reacts to each transferred member. For example, the region sees the transfer of the data sets, ALSO0.HYPL.CARD(AL1) and ALSO0.HYPL.CARD(AL2), as two separate transfers, although it cannot identify the actual members transferred.

Identify CONNECT:Direct File Transfers by Process Names

A CA NetMaster FTM 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%.

Considerations: CONNECT:Mailbox File Transfers

A CA NetMaster FTM 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 CA NetMaster FTM 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.

Information available from FTP events has the following restrictions:

- Only local data set names are provided in the event.
- For transfers using CA TCPaccess CS for z/OS:
  - CA NetMaster FTM does not receive an event at the start of an FTP file transfer.
  - No FTP client events are issued; however, because CA TCPaccess CS for z/OS operates by using a three-party FTP model, FTP server events are issued for all transfers.

Identify FTP File Transfers

For FTP file transfers using CA TCPaccess FTP Server for z/OS, the transfer ID is in the format *server-name*(*transfer-number*).

Identify the 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 CA TCPaccess FTP Server for z/OS, no transfer ID is available. Only local data set names are available for identifying FTP transfers. However, you can assign a static name to all FTP transfers not using CA TCPaccess FTP Server for z/OS by using the FTPCNTL parameter group.

Status of FTP File Transfers

When you build your FTP file management environment and if you are using CA TCPaccess CS for z/OS, consider the following:

- CA NetMaster FTM cannot distinguish between a successfully completed transfer and a transfer aborted by the client. It reports both as successful.

  Note: This does not apply to IBM Communications Server when you use the FTP post-processing exit FTPOSTPR.

- The START status is not available for FTP file transfers.

The CA NetMaster FTM 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.

CA TCPaccess FTP Server for z/OS uses a sub-reply code to differentiate between successful and aborted file transfers.

Considerations: FTS File Transfers

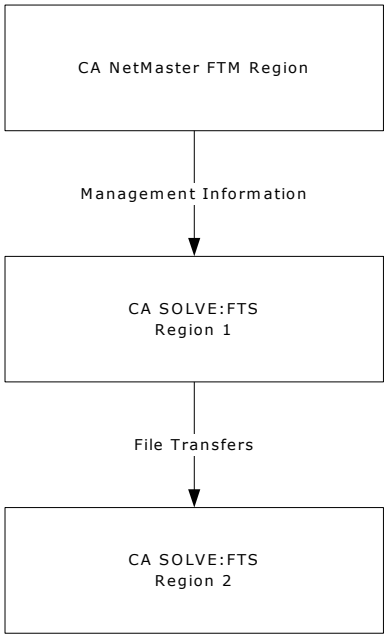
When you identify FTS file transfers, consider the information in the following sections.

Identify FTS File Transfers by Transmission Definition Names

If a CA NetMaster FTM region is monitoring multiple CA SOLVE: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.

Handle Transmission Definitions That Specify DD Names

A CA NetMaster FTM region monitors the file transfers between CA SOLVE:FTS regions, which may or may not be managed by it. The following diagram shows an example where FTS Region 1 is managed and FTS Region 2 is not managed:



If a CA SOLVE:FTS transmission definition specifies a DD name that points to a data set in Region 2 and CA NetMaster FTM is not authorized in Region 2, CA NetMaster FTM will be unable to resolve the data set name and cannot monitor the data set.

To resolve this problem, perform *one* of the following:

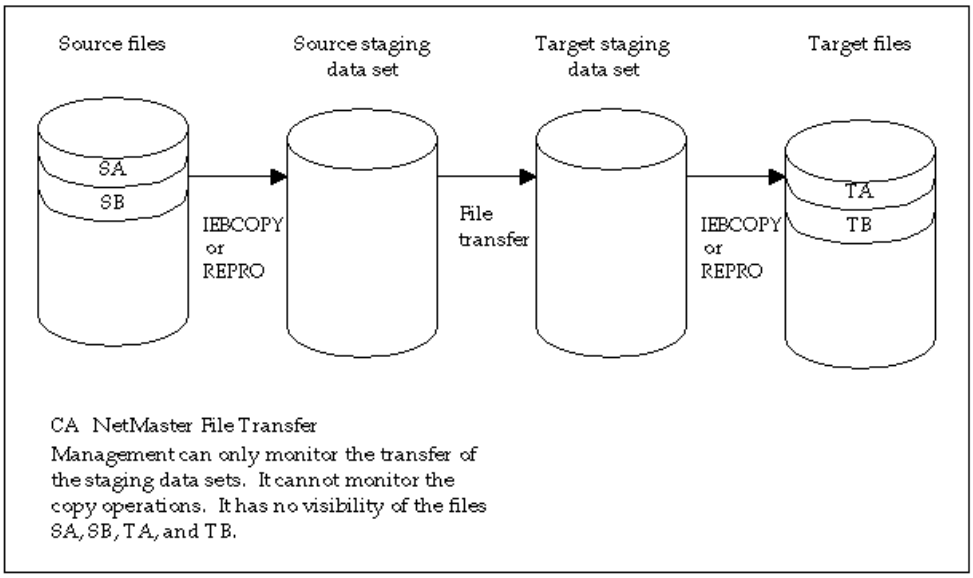
- Define the CA NetMaster FTM BSYS background user in FTS Region 2

  Note: For more information, see the *Installation Guide*.

- Use data set names in transmission definitions.

Considerations: Staging Data Sets

A CA SOLVE: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. The following diagram shows the staging mode operation:



When staging mode operation is used, CA NetMaster FTM 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.

Define File Transfer Schedules

The CA NetMaster FTM 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 state to reflect the condition.

Important! To use file transfer schedules for FTS transfers, define the FTS managers for the appropriate CA SOLVE:FTS regions. The managers enable the CA NetMaster FTM region to detect FTS file transfer events. Similarly, to use file transfer schedules for CONNECT:Direct transfers on distributed systems such as UNIX, define the CONNECT:Direct managers.

To define a file transfer schedule in a system image

1. Enter **/RADMIN.R** at the command prompt.

   The ResourceView : Resource Definition panel appears.

2. Enter **S** beside the FTSCHD file transfer schedule resource class.

   The File Transfer Schedule List appears.

3. Complete the following fields:

   Important! Ensure that you add the schedule to the correct system image.

   System Name

   Specifies the name of the system image to which this schedule belongs.

   Version

   Specifies the version number of the system image to which this schedule belongs.

   Press F4 (Add).

   The File Transfer Schedule General Description panel appears.

4. Complete the following fields:

   File Transfer Schedule Name

   Specifies the name of the file transfer schedule.

   Short Description

   Briefly describes the file transfer schedule

   Press F8 (Forward).

   The Schedule panel appears.

5. Complete the following fields:

Day/Date or Criteria Name

Specifies the day or date when a schedule entry starts. You can define calendar criteria (see page 167) to identify the day.

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 Transfer

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: File transfer schedule resource definition can contain more than one schedule.

Important! Do not overlap schedule entries.

Press F8 (Forward).

The File Filters panel appears.

6. 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.

   Note: CA NetMaster FTM 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.

   Note: For information about how to specify these criteria, see the online help.

   Press F8 (Forward).

   The State Change Exits panel appears.

7. (Optional) If you want the region to perform some actions when the schedule changes state (see page 122), complete this panel.

   Note: For information about how to specify these actions, see the online help.

   Note: Specifying an exit prevents the corresponding default alert from being raised by the region. The exit takes over this responsibility.

8. Press F3 (File).

   The schedule is saved to the knowledge base.

More information:

Schedule Control Files (see page 447)

Schedule Status Changes

The operation modes and states of a file transfer schedule resource as its status changes are shown in the following table:

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.

The following types of operation modes are available:

- 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.

Schedule Event Exits

You can specify an exit process for the following conditions:

- All the specified file transfers for the schedule have started

  Important! A transfer restart is counted as a normal start.
- All the specified file transfers for this schedule have successfully completed
- A specified file transfer for this schedule has failed

The exit process is executed when the condition is met. For example, you can take some action and set the schedule as COMPLETED rather than wait for the End of Processing period. You can use the STARTNCL macro to start the following API to force completion:
`$RFCALL ACTION=FORCEEND NAME=`*`schedule-name`*

Another example is to use the SHDCALL macro to send a command to CA 7 WA to submit a job at the completion of the schedule.

For Transfer Failures, the specified process is executed for every transfer failure until the number of successful transfers has reached the expected transfer count.

Variables Available for the Failure Process

In addition to the schedule knowledge base variables, the following variables are available to the transfer failure event process:

Variable	Description
&ZRFXFRID	The Transfer ID
&ZRFPRODUCT	The Data Transfer product
&ZRFJOBNAME	The Data Transfer STC or JOBNAME
&ZRFUSER	The ID of the user that performed the transfer
&ZRFSRCADDR	The address or node name of the source of the transfer
&ZRFSRCFNAME	The name of the source data in the transfer
&ZRFTGTADDR	The address or node name of the target of the transfer
&ZRFTGTFNAME	The name of the target data in the transfer
&ZRFABENDCODE	The ABEND code
&ZRFFAILCODE	The FAILURE Code
&ZRFFAILDESC	The FAILURE Description

Add Extra Fields

You may need to associate schedule specific information that cannot be currently accommodated with the SCHEDULE Owner Details panel. You can specify up to 16 extra fields (of 70 characters each). The additional details are available through knowledge base variables &ZRMDBADDET1 to &ZRMDBADDET16.

Schedule Resource Definition List

File Transfer schedules do not support the definitions of relationships with other resources. Use one of the various File Transfer Schedule exits to establish dependencies.

FTSCHD - Schedule File Specifications

The Schedule Recovery is optional; the default is YES (Schedule Recovery ON). The schedule file (FTSCHD) is required even if Schedule Recovery is set to NO.

Automation Table Controls

To reduce virtual storage use with a large number of schedules, you can set the Transient Log Table Size to zero. If the Transient Log Limit in AUTOTABLES is set to 0, then NO transient logs are allocated for any resource.

Note: If the Transient Log Limit in AUTOTABLES is set to a value greater than 0, individual resource definition can be changed dynamically to a lesser value (including 0).

Specify Event Exits

To specify event exits for a file transfer schedule

1. Enter **/RADMIN.R** at the command prompt.

   The ResourceView : Resource Definition panel appears.

2. Enter **S** beside the FTSCHD file transfer schedule resource class.

   The File Transfer Schedule List appears.

3. Enter **U** beside the schedule to which you want add exits.

   The Panel Display List appears.

4. Enter **5** at the Command prompt.

   The Event Exits panel appears.

5. Enter **?** in the Process field for the event condition.

   The Automation Services : Process List panel appears with a list of processes.

6. Enter **S** beside the required process.

   You are returned to the Event Exits panel with the name of the process.

   Note: If the process requires parameters, apply the P action.

7. Repeat steps 5 and 6 for each event condition for which you want to specify an exit. After you specify your exits, press F4 (Save).

   The schedule is saved with the event exits.

Chapter 11: Building Resources for File Transfer Products

This section contains the following topics:

Define Resources for File Transfer Products

To build an environment to manage CA XCOM Data Transport for z/OS, 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.

Note: File transfer product resources are not available for the Generic data transfer API.

How to Define CA XCOM Data Transport for z/OS Resources

A CA NetMaster FTM region can manage CA XCOM Data Transport for z/OS applications on the local system. To enable the region to perform this management function, you must define managers and monitors for these applications in the system image.

To define CA XCOM Data Transport for z/OS resources

1. Use the Assisted Resource Definition Facility to create a manager for a CA XCOM Data Transport for z/OS application.
2. Generate monitors for the created managers.

Create a CA XCOM Data Transport for z/OS Manager

To create the resource to manage your CA XCOM Data Transport for z/OS region

1. Enter **/RADMIN.AD.XC** at the command prompt and do *one* of the following:
   - If you have defined the system image, enter **S** beside the system image on the displayed System Image List panel.
   - If you have not defined your system image, press Enter at the Confirm System Image Add panel to add a system image.

   The XCOM Manager General Description panel appears.
2. Complete the following fields:

   XCOM Manager Name

   Specifies the name of the CA XCOM Data Transport for z/OS manager.

   Note: You define a manager resource for each application you want to be managed by this region. The manager name identifies the CA XCOM Data Transport for z/OS resource that is the subject of this definition. The manager name must be the same as that used for the CA XCOM Data Transport for z/OS application.

   Manager Type

   Specifies the type of the manager:

   - **STC** specifies that the application is initialized as a started task.
   - **JOB** specifies that the application is initialized as a job.

   ACB Name

   (Optional) Specifies the name of the VTAM ACB that must be active before this resource can start successfully.

   Operation Mode

   Specifies the type of operation:

   - **AUTOMATED** specifies that the resource is monitored and controlled (activated and inactivated) by the region.
   - **MANUAL** specifies that the resource can be controlled manually, and the region monitors but does *not* automatically control the resource.

   Short Description

   Briefly describes this resource.

   Press F3 (File).

   The manager resource definition is filed.

3. (Optional) Press F4 (Save) to save the current definition and update the definition for a new manager resource if you want to create multiple manager resource definitions. Repeat this process until a manager resource is defined for each CA XCOM Data Transport for z/OS application on this system.

   Press F3 (File).

   The ResourceView : XCOM Manager List panel appears.

4. (Optional) If you specified that the CA XCOM Data Transport for z/OS application was initiated by a job, 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 manages your CA XCOM Data Transport for z/OS application. You can modify it at a later stage.

You have completed the CA XCOM Data Transport for z/OS manager resource definition and can now define monitor resources for the manager (see page 129).

Create CA XCOM Data Transport for z/OS Monitors

To generate monitors for the created CA XCOM Data Transport for z/OS managers

1. Enter **G** beside a manager resource definition.

   A list of the available monitor resource types appears.

2. Enter **S** beside each type of monitor you want to generate for your manager resource definition.

   A panel for each monitor appears.

3. Enter the name of each monitor, and optionally, a long description of the monitor.

   Press F8 (Forward).

   The Monitor Details panel appears.

4. Review the settings and press F3 (File).

   When you have filed the details for all selected monitors, the ResourceView : XCOM Manager List appears.

   Note: If the monitor type is REQUEST-MON, the heartbeat interval is specified on the Monitor Details panel of the owning XCMGR definition.

5. (Optional) Enter **G** beside any remaining manager resources and repeat steps 2 through 4 to define monitor resources for the manager resources.
6. Press F3 (Exit).

   The monitor is created.

You can customize the resource definitions created by the Assisted Resource Definition Facility.

How to Define CONNECT:Direct Resources

A CA NetMaster FTM region can manage CONNECT:Direct applications on the local system and on distributed systems such as Windows. To enable the region to perform this management function, define managers and monitors for these applications in the system image.

Note: To manage CONNECT:Direct applications on a distributed system such as Windows, you must have implemented the appropriate agent for CA NetMaster FTM on that system.

To define CONNECT:Direct Resources

1. Use the Assisted Resource Definition Facility to create a manager for a CONNECT:Direct application.
2. Use the Auto Populate Facility to create the managers for its partner CONNECT:Direct applications on distributed systems.
3. Generate monitors for the created managers.

Create a CONNECT:Direct Manager

You can use the same steps to create resources to manage CONNECT:Direct on distributed systems; however, you may want to use the Auto Populate Facility to create those resources that are partners of a CONNECT:Direct for OS/390 region.

To create resources to manage CONNECT:Direct for OS/390

1. Enter **/RADMIN.AD.CD** at the command prompt and do *one* of the following:
   - If you have defined the system image, enter **S** beside the system image on the displayed System Image List panel.
   - If you have not defined your system image, press Enter at the Confirm System Image Add panel to add a system image.

   The C:D File Transfer Manager General Description panel appears.

2. Complete the following fields:

C:D File Transfer Manager Name

Specifies the name of the CONNECT:Direct manager.

Define a manager resource for each CONNECT:Direct application to be managed by this region.

Note: The manager name identifies the CONNECT:Direct resource that is the subject of this definition. For CONNECT:Direct for OS/390, the manager name must be the same as that used for the CONNECT:Direct application. For CONNECT:Direct on a distributed system, the manager name must match the distributed system host name.

Note: For more information about the distributed system host name, see the *CA NetMaster File Transfer Management Agent—CONNECT:Direct Installation and Administration Guide*.

C:D File Transfer Manager Type

Specifies the type of manager. Enter ? to display a list of valid values.

If the CONNECT:Direct application is …	Enter …
Initialized as a started task	STC as the manager type and, optionally, its ACB name.
Initialized as a job	JOB as the manager type and, optionally, its ACB name.
On a Windows system	Windows as the manager type and the TCP/IP details of the agent.

ACB Name

(Optional) Specifies the name of the VTAM ACB that must be active before this resource can start successfully.

TCP/IP Host Name/Addr

Specifies the TCP/IP details of the distributed systems agent.

Operation Mode

Specifies the type of operation:

- **AUTOMATED** specifies that the resource is monitored and controlled (activated and inactivated) by the CA NetMaster FTM region.
- **MANUAL** specifies that the resource can be controlled manually, and the CA NetMaster FTM region monitors but does *not* automatically control the resource.

Short Description

Briefly describes this resource.

Press F3 (File).

The manager resource definition is filed.

3. (Optional) 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.
4. Press F3 (File).

   The ResourceView : C:D File Transfer Manager List panel appears.
5. (Optional) If you specified that the CONNECT:Direct application was initiated by a job, 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 manages your CONNECT:Direct application. You can modify it at a later stage.

You have completed the CONNECT:Direct manager resource definition, and can now define the partner resources for the manager (see page 133).

Use 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 an z/OS 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 OS/390 manager.
- The system image that contains the manager is active.
- The CONNECT:Direct for OS/390 region that owns the network map is active.
- You are an authorized user in the CONNECT:Direct for OS/390 region.

To create resources for partner Connect:Direct applications

1. Enter **/RADMIN.AD.A** at the command prompt.

   The Auto Populate Menu appears.

2. Type **CD** at the prompt and complete the following fields:

   System Name and Version

   Specifies the name and version of the system image (to which you want to add the definitions for the local resources). Auto population puts resources for CONNECT:Direct for OS/390 and its partners in the same image.

   Template

   Specifies the template to use to create the definitions. Type **?** in the field to display a list of valid templates.

   Resource Mask

   Restricts the list of resources that appear 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, …

   CDMGR Name

   Specifies the manager for the CONNECT:Direct for OS/390 region for which you want to discover the partners.

   Press Enter.

   The C:D File Transfer Manager Template List panel appears.

3. Enter **S** beside the required template to list the type of resources you selected.

   If you are accessing the specified CONNECT:Direct for OS/390 region from the CA NetMaster FTM 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).

   The Auto Populate Selection List panel appears.

4. Type **S** beside the resources for which you want to build definitions.

   Note: To select all the displayed resources, enter **ALL S** at the command prompt.

   Press Enter to validate your selections.

   The selections are tagged as selected.

   Note: To deselect a selected resource, enter **U** beside the resource. To deselect all selected resources, enter **ALL U** at the command prompt. You can, if necessary, change the templates for individual resources. To cancel the operation, press F12 (Cancel) before the next step.

5. Press F6 (Action).

   The resource definitions are built.

6. Enter **/RADMIN.R.CDMGR** at the prompt.

   The C:D File Transfer Manager List appears with the newly-created managers.

7. (Optional) 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.

   Define monitor resources for these managers.

You have completed the CONNECT:Direct manager resource definitions, and can now define monitor resources for the managers.

Create CONNECT:Direct Monitors

To generate monitors for the CONNECT:Direct managers

1. Enter **G** beside a manager resource definition.

   A list of the available monitor resource types appears.

2. Enter **S** beside each type of monitor you want to generate for your manager resource definition.

   A panel for each monitor appears.

   Note: The TCP/IP connections monitor is not available to a distributed systems (for example, Windows) type manager.

3. Enter the name of each monitor, and optionally, a long description of the monitor.

   Press F8 (Forward).

   The Monitor Details panel appears.

4. Review the settings and press F3 (File).

   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 system.

   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.

5. (Optional) Enter **G** beside any remaining manager resources and repeat steps 2 through 4 to define monitor resources for the manager resources.

6. Press F3 (Exit).

   The monitor is created.

You can customize the resource definitions created by the Assisted Resource Definition Facility.

How to Define CONNECT:Mailbox Resources

A CA NetMaster FTM 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.

Create a CONNECT:Mailbox Manager

To define a CONNECT:Mailbox manager

1. Enter **/RADMIN.AD.CM** at the prompt**.**

   The System Image List appears.

2. Do *one* of the following:

   - If you have defined the system image, enter **S** beside the system image.
   - If you have not defined your system image, press Enter at the Confirm System Image Add panel to add a system image (see page 56).

   The ResourceView : C:Mailbox Resource Group Definition panel appears.

3. Complete the following fields:

   File Server 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.

   Manager Name

   Specifies the CONNECT:Mailbox started task that is the subject of this definition.

   ACB name

   (Optional) Specifies the ACB Name. If an ACB name is specified, CA NetMaster FTM activates the ACB during resource activation.

   Press F3 (File).

   The ResourceView : C:Mailbox Manager List appears.

This resource manages or monitors your CONNECT:Mailbox application. You can modify it at a later stage.

Create CONNECT:Mailbox Monitors

To define monitor resources for the manager

1. Enter **G** beside a manager resource definition on the ResourceView : C:Mailbox Manager List.

   The C:Mailbox Monitor List appears.

2. Enter **S** beside each type of monitor you want to generate for your manager resource definition.

   The ResourceView: C:Mailbox Monitor General Description panel appears for each monitor.

3. Enter the name of each monitor, and optionally, a long description of the monitor.

   Press F8 (Forward).

   The Monitor Details panel appears.

4. Review the settings and press F3 (File).

   The monitor resource definition is saved.

You can customize the resource definitions created by the Assisted Resource Definition Facility.

How to Define FTS Resources

To enable the region to manage CA SOLVE:FTS file transfers, define managers and monitors for the CA SOLVE:FTS applications in the system image.

Define Managers

To define managers for CA SOLVE:FTS applications in the system image

1. Enter **/RADMIN.AD.FTS** at the prompt.

   The System Image List appears.

2. Do *one* of the following:

   - If you have defined the system image, enter **S** beside the system image.
   - If you have not defined the system image, press Enter at the Confirm System Image Add panel to add a system image (see page 56).

   The FTS File Transfer Manager General Description panel appears.

3. Complete the following fields:

   FTS File Transfer Manager Name

   Specifies the FTS manager name.

   Note: Define a manager resource for each 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.

   Manager Type

   Specifies the manager type:

   - **SELF** specifies that the application is in this region.
   - **STC** specifies that the application is initialized as a started task as another region on this system. The specified manager name must be the same as that used for the started task.
   - **JOB** specifies that the application is initialized as a job as another region on this system. The specified name must be the same as that used for the job.
   - **REMOTE** specifies that the application is initialized on another system.

   Operation Mode

   Specifies the operation mode:

   - **AUTOMATED** specifies that the region maintains monitors and controls the resource.
   - **MANUAL** specifies that the resource is controlled manually; the region monitors but does *not* control the resource.

   Short Description

   Briefly describes the resource, for example, FTP started task.

4. Press F3 (File).

   The resource definition is saved and the ResourceView : FTS File Transfer Manager List panel appears.

   Note: If you specified that the application was initiated by a job, 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.

You can modify the newly-created resource at a later stage.

Define Monitors

To define managers for CA SOLVE:FTS applications in the system image

1. Enter **G** beside a manager resource definition on the ResourceView : FTS File Transfer Manager List.

   The FTS File Transfer Monitor General Description panel appears.

2. Complete the following fields:

   FTS File Transfer Monitor Name

   Specifies the name of the monitor.

3. Press F8 (Forward).

   The FTSMON Monitor Details panel appears.

4. Complete the following field:

   Link Name

   Specifies the name of an INMC link defined in the managed CA SOLVE:FTS region (for example, the name of an FTS-to-FTS INMC link).

   Press F4 (Save).

   The monitor resource definition is saved.

5. Repeat steps 2 to 4 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.

6. Press F3 (File).

   The ResourceView : FTS File Transfer Manager List appears.

7. Enter **G** beside any manager resource and define monitor resources for the manager resources.

8. Press F3 (Exit).

   The monitor definition is saved.

You can customize the resource definitions created by the Assisted Resource Definition Facility.

How to Define FTP Resources

A CA NetMaster FTM 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 managers of CA TCPaccess FTP Server for z/OS, the transfer policy rule set (subject to the FTPCNTL parameter group setting) and SOLVE SSI are also monitored by this resource.

Define Managers

To define managers for FTP server applications in the system image

1. Enter **/RADMIN.AD.FTP** at the prompt.

   The System Image List appears.

2. Do *one* of the following:

   - If you have defined the system image, enter **S** beside the system image.
   - If you have not defined your system image, press Enter at the Confirm System Image Add panel to add a system image (see page 56).

   The FTP Server Manager General Description panel appears.

3. Complete the following fields:

   FTP Server Manager Name

   Specifies the FTP server resource that is the subject of this definition. You define a manager resource for each FTP server application you want to manage or monitor in this system domain. The following rules apply:

   - For Communications Server FTP server, ensure that the manager name is the FTP background daemon name (usually, FTPD1).
   - For CA TCPaccess CS for z/OS, ensure that the manager name is the server name.
   - For CA TCPaccess FTP Server for z/OS, ensure that the manager name is the FTP server started task or batch job name.

   FTP Server Manager Type

   Specifies the manager type:

   - **STC** specifies that the FTP server is initialized as a started task
   - **JOB** specifies that the FTP server is initialized as a job.

Operation Mode

Specifies the operation mode:

- **AUTOMATED** specifies that the region maintains monitors and controls the resource.
- **MANUAL** specifies that the resource is controlled manually, and the region monitors but does *not* control the resource.

Short Description

Briefly describes the resource, for example, FTS started task.

Position your cursor in the first input field of the Template Selection window, and enter **L**.

The ResourceView : FTP Server Manager Template List appears.

4. Enter **M** beside the corresponding template name, as shown in the following table:

Server or Region	Job or Started Task	Template Name
Communications Server FTP server	Started task	CSFTPSRV
CA TCPaccess CS for z/OS	Job	AXS52JOB, AXS53JOB, or AXSJOB
CA TCPaccess CS for z/OS	Started task	AXS52STC, AXS53STC, or AXSSTC
CA TCPaccess FTP Server for z/OS	Job	SFTPJOB
CA TCPaccess FTP Server for z/OS	Started task	SFTPSTC

A confirmation message appears.

Note: 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.

5. Do *one* of the following:
   - If you are defining 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 continue to the next step.
   - If you are defining 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 continue to the next step.
   - If you are defining other managers, continue to the next step.
6. Press F3 (Exit) and then F3 (File).

   The manager resource definition is saved and the ResourceView : FTP Server Manager List panel appears.

This newly created resource manages and monitors your FTP server application. You can modify it at a later stage.

Define Monitors

To define monitors for FTP server applications in the system image

1. Enter **G** beside a manager resource definition on the ResourceView : FTP Server Manager List.

   The FTP Server Monitor List appears.
2. Enter **S** beside each type of monitor you want to generate for your manager resource definition.

   The FTP Server Monitor General Description panel appears.
3. Complete the following fields:

   FTP Server Monitor Name

   Specifies the name of the monitor.

   Press F8 (Forward).

   The FTPMON Monitor Details panel appears.
4. Review the settings and press F3 (File).

   The monitor definition is saved.
5. Enter **G** beside any remaining manager resources to define monitor resources for the manager resources.
6. Press F3 (Exit).

   The ResourceView : FTP Server Manager List appears.

You can customize the resource definitions created by the Assisted Resource Definition Facility.

Define TCP/IP Resources

You add your IBM TCP/IP or CA TCPaccess CS for z/OS resources to a system image. The definition enables a CA NetMaster FTM region to manage the TCP/IP resources.

Note: If CA TCPaccess CS for z/OS is your FTP server, you may have defined an FTPMGR resource for your CA TCPaccess CS for z/OS region. If so, it is not necessary to define a CA TCPaccess CS for z/OS resource as well.

To define the resource to your system image

1. Enter **/RADMIN** at the prompt.

   The Resource Administration menu appears.

2. Complete the following fields:

   System Name

   Specifies the name of the system image to which this resource belongs.

   Version

   Specifies the version of the system specified in System Name.

   Enter **R.STC** at the prompt.

   The Started Task List appears.

3. Press F4 (Add).

   The Started Task General Description panel appears.

4. Complete the following fields:

   Started Task Name

   Specifies the name of the started task.

   Important! For TCP/IP started task class (STC) resources, the specified name must be the same as that used for the started task.

   Operation Mode

   Specifies the operation mode:

   - **AUTOMATED** specifies that the region maintains monitors and controls the resource.
   - **MANUAL** specifies that the resource is controlled manually, and the region monitors but does *not* control the resource.

Short Description

Briefly describes the resource.

Position your cursor in the first input field of the Template Selection window, and enter **L**.

The ResourceView : Started Task Template List appears.

5. Do *one* of the following:
   - If you are defining a Communications Server resource, enter **M** beside the template COMSERVER.
   - If you are defining a CA TCPaccess CS for z/OS resource, enter **M** beside the template TCPAXS52, TCPAXS53, or TCPAXS60.

   A confirmation message appears.

   Note: 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 action.
6. Press F3 (Exit).

   The ResourceView : Started Task General Description appears with updated fields.
7. Press F3 (File).

   The ResourceView : Started Task List panel appears with the STC resource listed.
8. (Optional) Repeat steps 3 to 8 to add other STC resources.

These newly created resources manage the tasks for which they are defined. You can modify them at a later stage.

Auto-populate a System Image with DASD and Tape Resource Definitions

The AutoAssist Auto Populate Facility lets you select particular DASD and tape resources that 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.

Define DASD and Tape Resources Using Auto Populate

To define DASD and tape resources using the Auto Populate Facility

1. Enter **/RADMIN.AD.A** at the prompt.

   The Auto Populate menu appears.

   Note: If a system image does not already exist in the knowledge base, CA NetMaster FTM prompts you to create an image definition (see page 56).

2. Enter the option code for the class of resources you want to build at the prompt.

3. Complete the following fields:

   System Name

   Specifies the system image to which you want to add the definitions for the local resources.

   Version

   Specifies the version of the System Name.

   Template

   Specifies the template to use to create the definitions. Enter **?** to display a list of valid templates.

   Resource Mask

   (Optional) Restricts the list of resources displayed. 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, …

   Online Only?

   Specifies whether you want to create definitions for online resources only. If you specify NO, all configured resources of the selected class (whether online or not) are retrieved for you to select.

   Press Enter.

   The Auto Populate Selection List appears.

4. Type **S** next to the resources for which you want to build definitions, and press Enter.

   Note: To select all the displayed resources, enter **ALL S** at the command prompt. To deselect a selected resource, enter **U** beside the resource. To deselect all selected resources, enter **ALL U** at the command prompt. You can change the templates for individual resources. To cancel the operation, you must press F12 (Cancel) before the next step.

5. Press F6 (Action).

   The resource definitions are built.

Manage a CONNECT:Direct File Transfer Service on a Windows System

You can define file transfer rules, schedules, and resources to enable your CA NetMaster FTM region to manage a CONNECT:Direct for Windows file transfer service on a Windows system.

Note: To manage a CONNECT:Direct file transfer service on a Windows system, you must have implemented the Windows agent for CA NetMaster FTM.

To enable communications between the region and the CONNECT:Direct application on the Windows system, you must define a CONNECT:Direct manager for the application.

Considerations for managing CONNECT:Direct for Windows products in a multisystem environment are similar to those for managing remote CONNECT:Direct for UNIX products.

More information:

Define File Transfer Rules (see page 108)
Define File Transfer Schedules (see page 119)
How to Define CONNECT:Direct Resources (see page 130)

Manage a Remote CA SOLVE:FTS Region

You can define file transfer rules, schedules, and resources to enable your CA NetMaster FTM 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 customize it according to the *Installation Guide.*

To enable communications between the CA NetMaster FTM region and the remote FTS region, you must define an FTS manager for the application. The manager type is REMOTE.

Considerations for managing remote FTS regions in a multisystem environment are similar to those for managing remote CONNECT:Direct for UNIX products.

More information:

Define File Transfer Rules (see page 108)
Define File Transfer Schedules (see page 119)
How to Define FTS Resources (see page 137)

Load 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 CA NetMaster FTM region before you can monitor your file transfer service.

Note: You can load a rule set independently of the system image.

To load the system image and the rule set

1. Enter **/PARMS** at the command prompt.

   The Customizer : Parameter Groups panel appears.

   Note: You must have the required authority to access the panel. Ask your system administrator to give you the required access authority or perform this task for you.

2. Enter **F AUTOIDS** to find the AUTOIDS parameter group, and then enter **U** beside it.

   The Initialization Parameters panel for the parameter group appears.

3. Complete the following fields:

   System Image Name

   Specifies the name of the defined system image.

   Automation Mode

   Specifies the global operation mode. Set this field to **MANUAL**.

   Note: Setting the mode to MANUAL ensures that all resources operate in the MANUAL mode. This lets you familiarize yourself with the product before automating the management of your file transfer service.

   Perform Action in Manual Mode?

   Specifies how actions are performed. Enter **YES** in the field.

   Active Ruleset for File Transfer

   Specifies the name of the file transfer rule set. If no rule set is specified, no rules are triggered.

4. Press F6 (Action).

   The parameter group is actioned. The system image and the file transfer rule set are loaded, and a message indicates that the $RM AUTOIDS parameter group is set.

   Note: A loaded image or rule set appears 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.

5. Press F3 (File).

   The changes are filed.

   When the CA NetMaster FTM 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 the environment you built (see page 148) to ensure that it manages the file transfer service as required.

Note: After you have loaded an image, you can define additional resources to it, and the defined resources are available to the region immediately. Similarly, you can add rules to a loaded file transfer rule set and the rules are available to the region immediately.

Check the Built Environment

To check the status of your environment

1. Enter **/FTMON** at the command prompt.

   The file transfer status monitor appears.

2. 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 appears with a description of each command.

If you are satisfied that your resources are defined correctly, you can set your global operation mode to AUTOMATED (see page 149).

Set 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.

Important! The default desired state of the defined resources is specified by your system administrator in the $RM AUTOIDS parameter group. The default state is ACTIVE or INACTIVE.

If you set the global operation mode to AUTOMATED and the default resource desired state is set to ACTIVE, the region attempts to start all automated resources automatically.

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.

To set the global operation mode to AUTOMATED

1. Enter **GLOBAL** at the command prompt on the File Transfer Status Monitor.

   The Global Command Parameter Specification panel appears.

2. Enter **AUTOMATED** in the Global Automation Mode field, and press F6 (Action).

   A confirmation panel appears.

3. Enter **CONFIRM** in the Response field.

   The File Transfer Status Monitor appears.

Your CA NetMaster FTM region is now in AUTOMATED mode and automatically controls the resources defined in the loaded system image.

Note: 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 CA NetMaster FTM region.

Chapter 12: Controlling the Use of FTP

This section contains the following topics:

File Transfers Using FTP

CA NetMaster FTM manages and monitors various types of file transfer, including those using FTP.

The monitored FTP server and client must provide information to CA NetMaster FTM. The CA TCPaccess CS for z/OS and client provides only limited information; therefore, this limits the management and monitoring functionality provided for FTP transfers using this server and client.

CA TCPaccess FTP Server for z/OS is an FTP server and client that is specifically designed to work in conjunction with CA NetMaster FTM. CA NetMaster FTM provides a complete management and monitoring interface for FTP transfers that use CA TCPaccess FTP Server for z/OS, with none of the limitations that apply to FTP transfers using other FTP servers and clients.

CA TCPaccess FTP Server for z/OS

Note: CA TCPaccess FTP Server for z/OS is a separate product and requires its own license.

CA TCPaccess FTP Server for z/OS 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 CA NetMaster FTM, it provides the following functions for CA TCPaccess FTP Server for z/OS file transfers:

- Monitoring the resources used
- Monitoring START, END, and FAILURE events
- Tracking progress through the Active File Transfer monitor
- Terminates transfers from the Active File Transfer monitor
- Visibility of all transfers performed by CA TCPaccess FTP Server for z/OS

Policy Control

CA NetMaster FTM with CA TCPaccess FTP Server for z/OS lets you 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 CA TCPaccess FTP Server for z/OS transfers by defining a policy rule set in CA NetMaster FTM.

CA TCPaccess FTP Server for z/OS Policy Rule Sets

CA TCPaccess FTP Server for z/OS policy rule sets, together with your security package, let you control the transfer of files using FTP. A rule set is a grouping of rules.

An 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 FTP policy rules on your CA NetMaster FTM region and load it. You can define many rule sets of policy rules on your CA NetMaster FTM region; however, only one of the rule sets can be loaded at any one time.

The FTP policy rule sets are stored in the CA NetMaster FTM knowledge base and you can maintain them in this region. Rule set maintenance does not effect the loaded policy rule set; to change the loaded rule set, you need to reload it.

To activate a policy rule set, you must load a copy of the rule set.

The loaded policy rule set is enforced if an active SOLVE SSI has set PKTANALYZER=YES and the policy mode is ON. It does not depend on the CA NetMaster FTM region once it is loaded.

The user of the loaded policy rule set is CA TCPaccess FTP Server for z/OS.

Define a Policy Rule Set

To define a policy rule set

1. Enter **/FTADMIN.P.M** at the command prompt.

   The FTP Policy Ruleset List panel appears.

2. Press F4 (Add).

   The FTP Policy Ruleset panel appears.

3. Complete the following fields:

   Name

   Specifies the name of the rule set.

   Description

   Briefly describes the rule set.

4. Press F3 (File).

   The definition is saved in the knowledge base.

Add Policy Rules to a Rule Set

During operation, only one rule set can be loaded; therefore, you should combine all the CA TCPaccess FTP Server for z/OS policy rules that are to be used together into the same rule set. You can create different rule sets to do the following:

- Load at a future time
- Load on another LPAR

To add a policy rule to a rule set

1. Enter **/FTADMIN.P.M** at the command prompt.

   The File Transfer Ruleset List appears.

2. Enter **R** beside the rule set to which you want to add rules.

   The FTP Policy Rule List appears.

   Note: Policy rules are evaluated in the order that they appear in the list, until a match is made.

3. Press F4 (Add).

   The FTP Policy Rule panel appears.

4. Complete the following fields:

Description

Briefly describes the rule.

Status

Specifies whether the rule is used when it is loaded.

Allow Request?

Specifies whether the rule allows matched FTP requests.

Log

Specifies whether messages are logged for matched FTP requests in CA TCPaccess FTP Server for z/OS:

- **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

Used to support SAF security. If Allow Request? is YES, 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 through the FTPCNTL parameter group.

File Name

Specifies 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

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

Specifies whether the rule matches inbound or outbound file transfers.

Local Server IP Address

Specifies the CA TCPaccess FTP Server for z/OS on the local system to match.

Local Server Port

Specifies the CA TCPaccess FTP Server for z/OS on the local system to match.

Remote IP Address

Specifies the range of remote IP addresses to match. To match a single address, leave the High field blank.

Time of Day

Specifies the period to match. If the first time is later than the second time, then the period spans midnight.

Day of Week

Specifies the days of the week to match.

Press F3 (File).

The rules are saved in the knowledge base.

More information:

FTP SAF Rule Considerations (see page 159)
How to Set Up a SAF Qualifier Under CA ACF2 for z/OS (see page 162)
How to Set Up a SAF Qualifier Under CA Top Secret for z/OS (see page 163)
How to Set Up a SAF Qualifier Under RACF (see page 164)

Load a Policy Rule Set

When a rule set is complete, you can activate it by loading it.

Note: Only one rule set can be active at any time.

To load a policy rule set

1. Enter **/FTADMIN.P.M** at the command prompt.

   The FTP Policy Ruleset List appears.

2. Type **L** beside the name of the rule set definition to load.

   The FTP Policy Ruleset panel appears, showing the name of the rule set definition to be loaded.

3. Complete the following field:

   Policy Mode

   Specifies the policy mode to use:

   - **ON** permits access according to rules.
   - **OFF** disables rules and always permits access.
   - **WARN** permits access and logs matches according to rules

   Press F6 (Confirm).

   The FTP policy rule set is loaded.

Note: After 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 ** appears to the right of its name. If you make changes to the loaded rule set, they do not take effect until you reload the rule set.

Set Policy Mode for an Active Policy Rule Set

To set the policy mode for an active policy rule set

1. Enter **/FTADMIN.P.S** at the command prompt.

   The FTP Policy Ruleset panel appears.

2. Complete the following field:

   Policy Mode

   Specifies the policy mode to use:

   - **ON** permits access according to rules.
   - **OFF** disables rules and always permits access.
   - **WARN** permits access and logs matches according to rules

   Press F6 (Confirm).

   The policy mode is saved.

View the Loaded Policy Rule Set

To view the loaded policy rule set

1. Enter **/FTADMIN.P** at the command prompt.

   The FTP Policy Maintenance menu appears.

2. Type **V** at the prompt.

   The FTP Policy Ruleset panel displays the loaded rule set definition.

Copy 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

1. Enter **/FTADMIN.P** at the command prompt.

   The FTP Policy Maintenance menu appears.

2. Type **C** at the prompt.

   The FTP Policy Ruleset panel appears.

3. Complete the following fields:

   Name

   Specifies the name of the new rule set to be copied from the loaded rule set.

   Description

   Briefly describes the rule set.

   Press F3 (File).

   The rule set and its rules are copied.

Use 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 on 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.

FTP SAF Rule Considerations

When you request a file transfer to or from CA TCPaccess FTP Server for z/OS, the server compares the request to the loaded rules 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 no active SOLVE SSIs have PKTANALYZER=YES, 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.

Check 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 in the FTPCNTL parameter group. The default is $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 zeros. 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 data set access security checks.

Note: For incoming new file allocations, the normal data set 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: Use FTP SAF Rules for an Incoming File Transfer

A remote client at IP address 192.168.10.255 issues a PUT transfer request output to PDS data set 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.192.168.10.400.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 packages.

The normal security check for accessing the data set is still performed. The FTP SAF check is in addition to the normal security call for data set access.

Example: Use 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 172.24.10.222. The matching FTP policy rule has a SAF qualifier of DEVFILES. The security facility is called with the following SAF profile:

```
FTP.DEVFILES.172.24.10.222./USR/VAR/DEVPROC.LOG
```

The user requires read access for this resource for the transfer to proceed.

How to Set Up a SAF Qualifier Under CA ACF2 for z/OS

To set up a SAF qualifier under CA ACF2 for z/OS

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 CA ACF2 for z/OS resource type of FTP. It also sets a maximum length for profile names.

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)
    saf-qualifier1.- UID(uid_string) SERVICE(READ) ALLOW
    saf-qualifier2.- UID(uid_string) SERVICE(UPDATE) ALLOW
    saf-qualifier3.- UID(uid_string) SERVICE(READ) PREVENT
    saf-qualifier4.- UID(uid_string) SERVICE(UPDATE) PREVENT
    saf-qualifier5.10.11.12.13.filename UID(uid_string) SERVICE(UPDATE) ALLOW

   STORE
   END
   ```

More information:

Examples of Using Your SAF Qualifier (see page 165)

How to Set Up a SAF Qualifier Under CA Top Secret for z/OS

To set up a SAF qualifier under CA Top Secret for z/OS

1. Define the class.

   Note: $FTP is the default class name for FTP SAF rules. If you have used a different class name in the FTPCNTL parameter group, 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*).

2. Define ownership.

   TSS ADD(*department-id*) $FTP(FTP.)

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.saf-qualifier.10.11.12.13.filename) 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.saf-qualifier1.) ACCESS(WRITE)
   ```

How to Set Up a SAF Qualifier Under RACF

To set up a SAF qualifier class and profiles under RACF

1. Define the SAF class to the RACF Class Descriptor Table by using one of the JCL members in your *dsnpref*.NMC1.CC17SAMP library:

   - DEFRACFA (for non-SMP/E)
   - DEFRACFS (for SMP/E)

   Note: The default class name for FTP SAF rules is $FTP. You can stipulate any value that conforms to RACF standards. If you use another name, ensure that you specify it in the FTPCNTL parameter group.

   Note: An IPL is required for changes to the RACF Class Descriptor Table to take effect.

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 have the following format:

   FTP.*saf-qualifier*.*remote-ip-address*.*filename*

   FTP

   Is a constant.

   saf-qualifier

   Specifies the name that you determine and enter in the SAF Qualifier Field when defining your policy rule.

   remote-ip-address

   Specifies the standard dotted decimal notation of an IP address (* wildcard allowed).

   filename

   Specifies the name of a data set (* wildcard allowed).

3. Make the profiles available to specific users or groups of users, with access attributes of either read or write.

More information:

Examples of Using Your SAF Qualifier (see page 165)

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.172.24.215.17.FTP.DATA.FILE
```

1. Connect this sample profile to user ID FTPUSER with read access in your security system.
2. Define a policy rule allowing FTP transfers to the users you want, with the SAF qualifier coded as SAFSAMP.

If FTPUSER requests a transfer to open a connection to 172.24.215.17 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.172.24.215.17.**
```

1. Connect this sample profile to user ID FTPUSER with read access in your security system.
2. Define a policy rule allowing FTP transfers to the users you want, 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 172.24.215.17; however, FTPUSER can send any file out to this IP address.

Example 3

```
FTP.SAF SAMP.*.**
```

1. Connect this sample profile to user ID FTPUSER with read access in your security system.
2. Define a policy rule allowing FTP transfers to the users you want, 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
```

1. Connect this sample profile to user ID FTPUSER with write access in your security system.
2. Define a policy rule allowing FTP transfers to the users you want, 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.

Chapter 13: Defining and Maintaining Calendars

This section contains the following topics:

How to Use Calendars to Create Date Criteria

You use a calendar to define date criteria that you can use to specify file transfer schedules.

You can create different calendars for different purposes. In 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).

To use calendars to create date criteria

1. Enter **/ASADMIN.CC**.

   The Calendar Criteria menu appears.

2. Select option **C** to add your calendar.
3. Enter **K** at the Calendar Criteria Menu to create calendar keywords.
4. Associate the keyword to particular dates of a calendar.
5. Enter **CR** from the Calendar Criteria Menu to create date criteria.

Create a Calendar

To create a calendar

1. Enter **/ASADMIN.CC.C**.

   The Calendar List appears.

2. Press F4 (Add).

   The Calendar Definition panel appears.

3. Complete the following fields:

   Calendar Name

   Specifies the name of the calendar.

   Short Description

   Briefly describes the calendar.

4. Press F3 (File).

   The calendar is created.

Calendar Format

The calendar appears 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.

From a calendar, you can also display the previous year and next year.

Create 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.

To create a calendar keyword

1. Enter **/ASADMIN.CC.K.**

   The Keyword Panel List appears.

2. Press F4 (Add).

   The Keyword Definition panel appears.

3. Complete the following fields:

   Keyword Name

   Specifies the name of the keyword.

   Short Description

   Briefly describes the keyword.

4. Press F3 (File).

   The keyword is created.

Associate a Calendar Keyword with a Date

To associate a calendar keyword with a date in a calendar

1. Enter **/ASADMIN.CC.K** at the command prompt.

   The Keyword List appears.

2. Enter **R** beside the keyword you want to associate with a date.

   The Keyword References for Year panel appears.

3. Enter **S** beside the month that you want to associate with the keyword, and enter **L** *nn* at the command prompt, where *nn* is the date that you want to associate with the keyword.

   The Keyword References for Month panel appears.

4. Enter **U** beside the date that you want to associate with the keyword.

   The Keyword References for Day panel appears.

5. Enter **R** beside the calendar that you want to associate with the keyword.

   REFERENCED appears beside your selection.

View a Calendar with Associated Keyword

To view the calendar with the associated keyword

1. Enter **/ASADMIN.CC.C** at the command prompt.

   The Keyword Panel List appears.

2. Enter **V** beside the calendar.

   Any date that has a keyword entered against it displays **Y** instead of a dot.

Create a Calendar Criteria Definition

You can use calendar criteria to define complex date or day requirements.

To create a calendar criteria definition

1. Enter **/ASADMIN.CC.CR**.

   The Calendar Criteria List appears.

2. Press F4 (Add).

   The Calendar Criteria panel appears.

3. Complete the following fields:

   Name

   Specifies the name of the calendar criteria in use.

   Description

   Briefly describes the calendar criteria.

   Calendar

   Specifies the related calendar to use when the criteria expression is evaluated.

4. Specify the expression that defines your criteria. Press F1 (Help) for more information.

   Note: Enter a question mark (?) to list the valid values for the fields.

   Press F3 (File).

   The criteria definition is created.

Example: Specify the Criteria Expression

This following example shows a criteria definition that selects Mondays as long as it is not a public holiday, as identified by the PUBHOLNA keyword.

```
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'                                                    |
```

Chapter 14: Implementing Availability Maps

This section contains the following topics:

Availability Maps

An availability map enables you to define the availability requirements for a service or resource. An availability map also enables you to schedule the execution of processes. You can add an availability map at any time. The map becomes effective as soon as you attach services or resources to it.

How You Implement Availability Maps

The desired state information specified in a service or a resource definition determines its status. The definition can include an availability map that schedules changes to the default availability. Timers activate these changes.

Note: The default desired state determines the default availability of a service or resource. The state is set in the AUTOIDS parameter group during region initialization. The Customizer : Parameter Groups panel lists the region parameter groups. Enter the **/PARMS** shortcut to access the panel.

Availability maps enable you to schedule changes to the default availability requirements of one or more services or resources. The service image and each system image have its own set of availability maps. You define an availability map (for example, MAP1) and attach as many services or resources to the map as required. Because availability maps are not limited to a seven-day cycle, you can define changes to the availability requirements that apply daily, on the same day every week, on the same date every month, for a specific date and time, and so on. You can also suppress changes temporarily and update timer information at any time.

An availability map has two parts: a map definition and a timer definition. The map definition contains information about the map itself. The timer definition contains information about when to change the desired state of the services or resources that use this map. The timer definition can also contain information about when to change the operation mode and when to start processes to perform special tasks.

Creating an availability map has the following two stages:

1. Creating an availability map.
2. Attaching services or resources to a map.

Note: For information about how availability and resource relationships affect operations, see the *Reference Guide*.

Rules for Availability Map Definitions

The following rules apply to availability maps:

- If the timer definition is blank, it means that default availability requirements apply to all the services or resources attached to that map.
- A map only applies to the service image or the system image for which it is defined.
- Map names must be unique in the image to which the map applies.

Access Availability Map Definitions

You can define as many maps for a system image as you want. After the map is defined, you can define timer information and attach services or resources to the map. Use the Availability Maps option to create and maintain availability map definitions.

The service image and each system image have its own set of availability maps.

To access service availability map definitions

1. Enter **/SADMIN.A** at the prompt.

   The Availability Map List appears.

To access resource availability map definitions

1. Enter **/RADMIN** at the prompt.

   The Resource Administration menu appears.

2. Enter **A** at the prompt and the name and version of the system image that owns the maps you want to create or access, and then press Enter.

   The Availability Map List panel appears. This panel lists the availability maps for the specified service or system image.

Note: To display the maps owned by another system image or resource, you can enter another name (resources only) or version number at the top of this panel.

Temporary Availability Maps

A temporary availability map is an availability map created from the status monitor to override the current map attached to a service or resource. A temporary map has an expiry time when the map is deleted automatically. You can use a temporary map as any other map, remembering that it has a defined life time.

Create an Availability Map

To create an availability map

1. Press F4 (Add) from the Availability Map List panel.

   The Availability Map panel appears.

2. Specify the timer information that sets the availability requirements. For information about the fields, press F1 (Help).

How You Define Timers

You can define two types of timer information:

- For all services or resources, define the timer, leaving the SVC/Resource Name field blank. This timer information applies to any services or resources attached to the map.
- For a specific service or resource, define the timer with the name of the service or resource in the SVC/Resource Name field. This timer information applies to the named service or resource if the service or resource is attached to the map.

You can use the action codes to repeat or delete rows of information, or to insert blank lines.

Use the following values in the Day field to simplify data entry:

*****

Repeats the timer for all days (that is, Monday through Sunday).

W/D

Repeats the timer for weekdays (that is, Monday through Friday).

W/E

Repeats the timer for weekends (that is, Saturday and Sunday).

Leave the Day field blank if you fill in the Date field. If the Mode field is left blank, you do not override the operation mode.

Scheduling of Processes

If you want the map to start processes at defined times, press F11 (Right) to display the fields for specifying processes.

Manual Overrides

You can use a timer to reset manual desired state and operation mode overrides. Specify RESET in the Des.State and in the Mode fields.

When a manual override exists, the scheduled change to the overridden parameter cannot be made. If you want to help ensure that the scheduled changes are made, reset the overrides first.

Note: For more information about how to perform manual overrides, see the *User Guide*.

Availability Map Example

This example describes how to define an availability map for services.

In this example, you define a map for the defined services to schedule such things as availability during holidays and when system maintenance is required. The map is named MAP1.

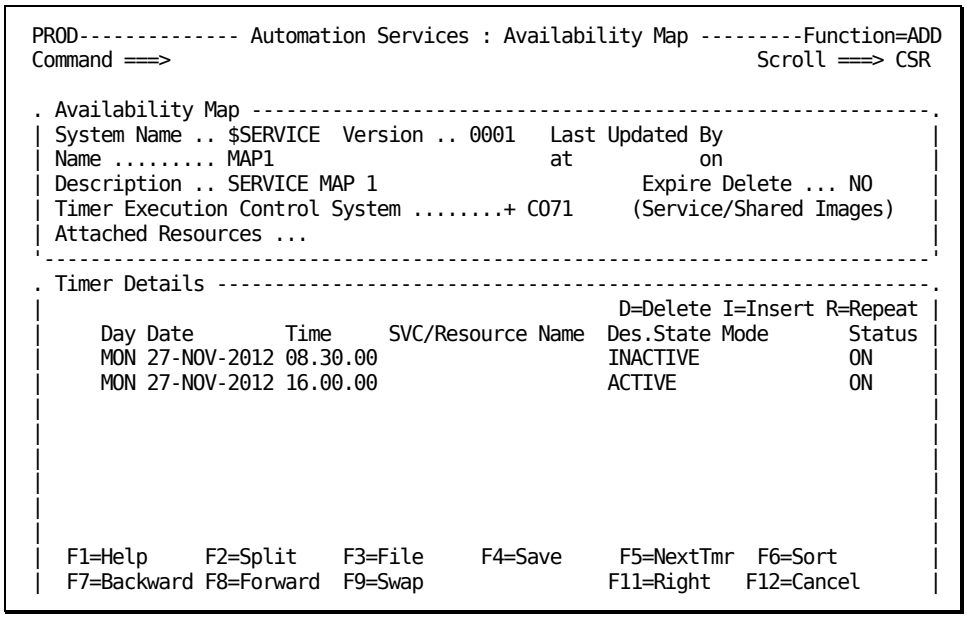
Use the **/SADMIN.A** path and the F4 (Add) function key to access the Availability Map panel. On the panel, you type the following values:

- **MAP1** in the Name field
- A description in the Description field
- **N** in the Expire Delete field to retain expired timer events (These events occur on specific dates.)

You can now specify timer details.

You want to stop all services on 27 November 2012 at 0830 hours for system maintenance and reactivate all services at 1600 hours on the same day. (Resources that belong to the services have a scheduled INACTIVE desired state for all times. That is, the services control the availability of those resources by using the ACTIVE desired state overrides.)

In the Timer Details box, type the information about the date, the time, the change to the status, and whether to process this change. To have a change processed, specify **ON** in the Status column. The following shows the completed Availability Map panel.



Timer Information

The Next Timers Execution Time panel lists information about upcoming changes to availability. You can obtain different views of this timer information by:

- Viewing the timer information in all availability maps for the services or in a system image
- Viewing the timer information in one availability map

The views list the next invocation of the defined timers. For example, a timer that executes every Monday is listed once only.

View All Timer Information

You can view a list of the upcoming changes scheduled in all maps defined in the service image or in a system image. The changes are listed in chronological order.

To view this information from the Availability Maps List panel, press F12 (NextTmr).

A Next Execution Time panel appears, listing the upcoming changes for all the maps.

View the Timer Information in One Availability Map

You can view a list of the upcoming changes scheduled in an individual map. The changes are listed in chronological order.

To view the timer information in an availability map

- From the Availability Map List panel, enter **N** next to an availability map to select the NextTimers action.
- From an Availability Map panel (while you are working on an availability map definition, a resource definition, or a service definition), press F5 (NextTmr).

A Next Execution Time panel appears, listing the upcoming changes for the selected map.

Attach a Service or Resource Definition to an Availability Map

After a map is defined, you can attach service or resource definitions by using:

- The Availability Map List
- The service or resource definition panels

To attach a service or resource definition to an availability map from the Availability Map List

1. Enter **AR** next to the availability map to which you want to add a resource or service.

   The Attach Resources panel appears.

2. Enter **S** next to the resource or service that you want to add to the availability map.

   The Attach Resources Results panel appears, which tells you whether the operation was successful.

3. Press F3 (File).

   The Availability Map List appears.

   Note: To display the resources or services that are attached to an availability map, enter **LR** next to the availability map in the list.

To attach a service or resource to a map while you are working on the definition

1. Select the General Description panel.
2. Enter the name of the availability map in the Availability Map field, and press F3 (File).

   The details are saved.

Detach Service or Resource Definitions from an Availability Map

You can detach service or resource definitions from an availability map (for example, if you want to change a resource definition and test it separately).

You can detach a service or a resource from an availability map by using:

- The Availability Map List
- The service or resource definition panels

To detach a service or resource from an availability map from the Availability Map List

1. Enter **/SADMIN.A** (for services) or the **/RADMIN.A** (for resources) at the prompt.

   The Availability Map List panel appears.

2. Enter **LR** next to the map from which you want to detach services or resources.

   A list of the attached services or resources appears.

3. Enter **DT** next to the services or resources that you want to detach from the map and press Enter.

   The services or resources are detached from the map.

To detach a service or a resource from a map while you are working on the definition

1. Select the General Description panel.
2. Remove the name of the availability map from the Availability Map field and press F3 (File).

   The service or resource is detached from the map.

Maintenance of Availability Map Definitions

You can browse, update, copy, and delete timer information and availability map definitions from the Availability Map List panel.

Chapter 15: Implementing Status Monitor Filters

This section contains the following topics:

Status Monitor

The status monitor displays the status of defined services and the status of defined resources in the currently-active system images. The display is in the form of a list. You can customize the status monitor to display only the services and resources of interest.

You customize a status monitor by using status monitor filters. You can selectively view different groups of services and resources by swapping filters.

Implement the Status Monitor Filters

You use filters to customize a Status Monitor panel. For example, you can define a filter that causes the Status Monitor to display only those resources that are applicable to a subset of your network.

A Status Monitor filter uses a Boolean expression, which you define on the Status Monitor Filter panel, to determine what to display on the monitor. You restrict the display by using the resource attributes such as names and status.

When you save a filter definition in the knowledge base, the definition propagates automatically to all the connected regions—that is, the definition is global.

Access Status Monitor Filter Definitions

Status Monitor filters let you configure your view of monitored resources to suit your requirements. You can selectively view different groups of resources by swapping filters.

To access Status Monitor filter definitions, enter **/ASADMIN.F** at the prompt.

The Status Monitor Filter List appears.

The panel displays the list of filter definitions in the knowledge base. You can add a new definition, or browse, update, copy or delete an existing definition.

Add a Status Monitor Filter

To add a Status Monitor filter definition

1. Access the Status Monitor Filter List.
2. Press F4 (Add).

   The Status Monitor Filter panel appears.

   Note: If you change your mind and do not want to add the filter, press F12 (Cancel) to cancel the operation any time before Step 5.
3. Complete the Name and Description fields in the Filter Definition window to identify the new filter.

   Note: Press F1 (Help) for a description of the fields.
4. Specify a Boolean expression (see page 184) in the Filter Expression window to define the filter.
5. Press F3 (File).

   The new definition is saved.

Status Monitor Filter Panel

The Status Monitor Filter panel specifies the details of a Status Monitor filter. The operation you are performing is displayed at the top right of the panel, for example, Function=UPDATE.

The panel displays two windows. The Filter Definition window identifies the filter by name and description, and the Filter Expression window specifies the Boolean expression that defines the filter.

Example: Status Monitor Filter Panel

```
PROD-------- Automation Services : Status Monitor Filter -------Function=UPDATE
Command ===>                                                    Scroll ===> 10

+ Filter Definition ------------------------------------------------------------+
| Name ......... ATTENTION                                                     |
| Views ........                                                               |
| Description .. RESOURCES THAT ARE IN ATTENTION STATE                         |
| Last Updated at 22.09.04 on WED 24-MAY-2006 by USER01                        |
+------------------------------------------------------------------------------+
+ Filter Expression -------------------------------------------------------------+
|                                                                               |
|                                                 D=Delete I=Insert R=Repeat    |
|      "(" Field   Opr Value                                      Gen ")" Bool  |
|          LOGSTAT =   "ATTENTION"                                              |
|     **END**                                                                   |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|  F1=Help     F2=Split    F3=File     F4=Save                                  |
|  F7=Bkwd     F8=Forward  F9=Swap                              F12=Cancel      |
+------------------------------------------------------------------------------+
```

Status Monitor Views

A view customizes your Status Monitor for the specific purpose of monitoring certain classes of objects. Each view has associated with it a selected set of filters and display formats.

To see the supported views, enter **?** in a View field.

How You Define the Status Monitor Filter Expression

Use the Filter Expression window on the Status Monitor Filter panel to specify the Boolean expression that defines the filter. The expression uses resource attributes as criteria to determine what to display on the Status Monitor.

To display the list of valid values for a field, enter a question mark (?) in the field.

Use the following action codes to help you enter the expression:

D

Deletes the selected line.

I

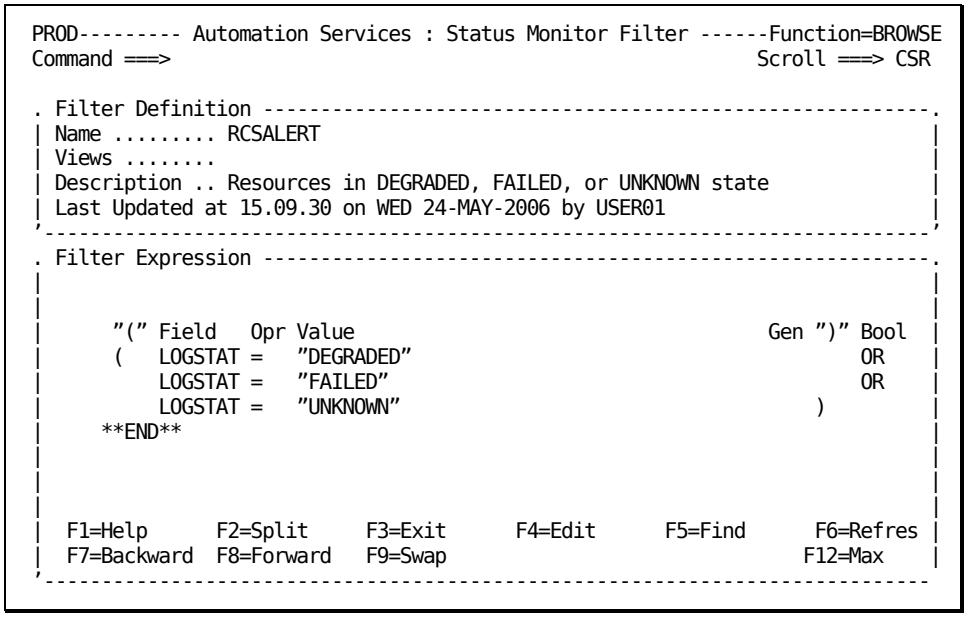
Inserts a blank line after the selected line.

R

Repeats a selected line.

Example: Define a Status Monitor Filter

This example defines a filter named RSCALERT that enables an operator to monitor resources that have a DEGRADED, FAILED, or UNKNOWN logical state. The following panel shows the completed filter.



The filter expression causes a Status Monitor to display only services that have the DEGRADED, FAILED, or UNKNOWN logical state.

Example: Define Status Monitor Filter Expression

In this example, you define a filter called SERVICEALERT that enables an operator to monitor services that have a DEGRADED, FAILED, or UNKNOWN logical state. The following diagram shows the completed Status Monitor Filter panel.

```
PROD--------- Automation Services : Status Monitor Filter ------Function=BROWSE
Command ===>                                                  Scroll ===> CSR

. Filter Definition ------------------------------------------------------------.
| Name ......... SERVICEALERT                                                   |
| Views ........                                                                |
| Description .. Services in DEGRADED, FAILED, or UNKNOWN state                 |
| Last Updated at 15.09.30 on WED 28-MAY-1997 by USER01                         |
'-------------------------------------------------------------------------------'
. Filter Expression ------------------------------------------------------------.
|                                                                               |
|                                                                               |
|      "(" Field   Opr Value                                    Gen ")" Bool    |
|          CLSNAME =   "SVC"                                          AND       |
|      (   LOGSTAT =   "DEGRADED"                                     OR        |
|          LOGSTAT =   "FAILED"                                       OR        |
|          LOGSTAT =   "UNKNOWN"                                  )             |
|     **END**                                                                   |
|                                                                               |
|                                                                               |
|                                                                               |
|  F1=Help      F2=Split     F3=Exit      F4=Edit      F5=Find      F6=Refres   |
|  F7=Backward  F8=Forward   F9=Swap                               F12=Max      |
'-------------------------------------------------------------------------------
```

The filter expression causes a status monitor to display only services that have the DEGRADED, FAILED, or UNKNOWN logical state.

Maintenance of Status Monitor Filter Definitions

You can browse, update, copy, and delete filter definitions from the Status Monitor Filter List panel.

If the Filter Expression window does not fully display the Boolean expression while you are browsing a definition, press F12 (Max) to expand the window.

Note: After you update a filter definition, an operator who is already using that filter does not see the update. To use the updated filter, the operator must enter the REFILTER command.

Chapter 16: Customizing the Environment That Manages Resources

This section contains the following topics:

Manager Resource Definition

The manager resource templates you use when you define manager resources provide sufficient information for you to manage your regions; however, you can customize the defined manager resources to suit your special requirements.

The manager resource definition comprises the following panels:

General Description

Specifies general information about the resource, for example, the operation mode

Availability Map

Specifies the schedule that activates or inactivates the resource

Activation Details

Specifies how the region starts the resource.

Inactivation Details

Specifies how the region stops the resource normally.

Force Inactivation Details

Specifies how the region stops the resource immediately.

Display and Heartbeat Details

Specifies how to retrieve status information about the resource.

Resource Monitor Message Details

Specifies rules that react to unsolicited messages. *Do not change those rules specified by the template*.

State Change Exits

Specifies exit processes that are executed because of a resource state change. *Do not change the information specified by the template*. You can add exits, for example, the CA SOLVE:Central exit.

Automation Log Details

Customizes log attributes such as the size of the transient log, where messages are logged, and what messages are logged.

Owner Details

Specifies particulars of the persons responsible for the resource.

Extended Function Exit

Extends functions by specifying a user procedure.

The supplied templates ensure that your 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

Customize Manager Resource Definition

To customize or view a manager resource definition

1. Enter the **/RADMIN.R.resource-class-name** path.

   The list of defined resources appears.

2. Complete the following fields:

   System Name

   Specifies the system image that contains the manager you want to customize.

   Version

   Specifies the version of the system image that contains the manager you want to customize.

3. Enter **U** beside the manager you want to customize.

   The list of panels in the resource definition appears.

4. Enter **S** beside the panel you want to display.

   Note: You can also enter a number at the prompt to display a panel. For example, to display the first panel, enter 1

5. Customize the definition, as required.

6. Press F3 (File).

   The system saves your changes.

Monitor Resource Definition

The monitor resource templates you use when you define monitor resources provide sufficient information for you to monitor the resources used by your regions; however, you can customize the defined monitor resources to suit your special requirements.

The supplied templates ensure that your file transfer resources are monitored correctly.

The monitor resource definition comprises the following panels:

General Description

Specifies general information about the resource, for example, the operation mode.

Monitor Details

Specifies monitoring criteria pertinent to the monitor type, for example, the idle time of a TCP/IP connection.

Resource Monitor Message Details

Specifies rules that react to unsolicited messages. *Do not change those rules specified by the template*.

State Change Exits

Specifies exit processes that 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 CA SOLVE:Central exit.

Automation Log Details

Customizes log attributes such as the size of the transient log, where messages are logged, and what messages are logged.

Owner Details

Specifies particulars of the person responsible for the resource.

Extended Function Exit

Extends functions by specifying a user procedure.

Important! 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

Customize a Monitor Resource Definition

To customize a monitor resource definition

1. Enter **/RADMIN.R**.*resource-class-name* at the prompt. For example, to access the list of defined CA XCOM Data Transport for z/OS monitors, enter **/RADMIN.R.XCMON**.

   The list of defined resources appears.

2. Complete the following fields:

   System Name

   Specify the system image that contains the monitor you want to customize.

   Version

   Specify the version of the system image that contains the monitor you want to customize.

3. Enter **U** beside the monitor you want to customize.

   The list of panels in the resource definition appears.

4. To display a panel, enter **S** beside it.

   Note: You can also enter a number at the prompt to display a panel. For example, to display the first panel, enter 1.

5. Complete the monitor resource definition panels.

   For more information about completing the panels, press F1 (Help).

6. Press F3 (File).

   The system files the changes.

Customize the Supporting Resource Definition

The resource templates you use when you define supporting resources provide sufficient information for you to manage those resources; however, you can 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:

To access the resource definitions for...	Enter the...
DASDs	**/RADMIN.R.DASD**
Tapes	**/RADMIN.R.TAPE**

Customize CA XCOM Data Transport for z/OS

You can customize CA XCOM Data Transport for z/OS monitor resource definitions to suit your requirements. This section describes how to customize the monitoring criteria for the following:

- Heartbeat interval
- Transfer requests
- Stalled transfers
- TCP/IP connections
- Remote nodes

Customize the Heartbeat Interval

The status update frequencies are set by the heartbeat interval. For transfer request monitors, the owning manager determines the update frequency. Other monitors have their own individual update frequencies.

Important! Defining too many resources with short heart beat values increases CPU usage.

To customize the heartbeat interval

1. From the file transfer resource monitor, do *one* of the following:
   - Enter **U** beside the required XCMON resource. Go to Step 3.
   - Enter **DB** beside the XCMGR resource. Go to Step 2.

   Note: In the default view, the Class column is abbreviated; therefore, ensure that you select the correct class.
2. (Optional) Enter **S** beside the Monitor Details panel.

   The Monitor Details panel appears.
3. Complete the following field:

   Heartbeat Interval

   Defines how often the region retrieves status information in the format hh.mm.ss. The minimum interval is 1 minute.

   hh

   Defines the interval time in hours.

   Limits: 24 hours

   mm

   Defines the interval time in minutes.

   Limits: 59 minutes

   ss

   Defines the interval time in seconds.

   Limits: 59 seconds
4. Press F3 (File).

   The system files the changes and the file transfer resource monitor appears. The new heartbeat interval is now in effect for the resource.

Customize Transfer Requests

To customize criteria for a CA XCOM Data Transport for z/OS transfer request monitor

1. From the file transfer resource monitor, enter **U** beside a transfer request XCMON-class resource.

   The Monitor Details panel appears.

2. Complete the following fields:

   Transfer Request Status

   Defines the status of requests to monitor.

   Transfer Request Threshold

   Defines the threshold for the number of CA XCOM Data Transport for z/OS transfer requests with the specified status.

   Transfer Request ID

   Restricts monitoring to specific IDs. If you want to monitor all IDs, leave the fields blank.

   Remote Server

   Restricts monitoring to a specific TCP/IP host name or address, or LU name of a remote node. If you want to monitor all nodes, leave the fields blank

3. Press F3 (File).

   The system files the changes and the file transfer resource monitor appears. The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customize Stalled Transfers

To customize the criteria for a CA XCOM Data Transport for z/OS stalled transfer monitor

1. From the file transfer resource monitor, enter **U** beside a stalled transfer XCMON-class resource.

   The Monitor Details panel appears.

2. Complete the following fields:

   Stalled Time to Alert

   Defines the time a transfer in progress remains idle before an alert is raised.

   Stalled Time to Terminate

   Defines the time a transfer in progress remain idle before it terminates.

   Transfer Request ID

   Restricts monitoring to specific IDs. If you want to monitor all IDs, leave the fields blank.

   Remote Server

   Restricts monitoring to a specific TCP/IP host name or address, or LU name of a remote node. If you want to monitor all nodes, leave the fields blank

3. Press F3 (File).

   The system files the changes and the file transfer resource monitor appears. The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customize TCP/IP Connections

To customize the criteria for a CA XCOM Data Transport for z/OS TCP/IP connections monitor

1. From the file transfer resource monitor, enter **U** beside a TCP/IP connections XCMON-class resource.

   The Monitor Details panel appears.

2. Complete the following fields:

   Idle Time to Alert

   Defines the time a TCP/IP connection can be idle before an alert is raised.

   Idle Time to Drop

   Defines the Time a connection can remain idle before it is dropped.

3. Press F3 (File).

   The system files your changes and the file transfer resource monitor appears. The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customize Remote Nodes

To customize the criteria for a CA XCOM Data Transport for z/OS remote node monitor

1. From the file transfer resource monitor, enter **U** beside a remote node XCMON-class resource.

   The Monitor Details panel appears.

2. Change the remote file transfer partner node that you want to monitor.

3. Press F3 (File).

   The system files your changes and the file transfer resource monitor appears. The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customize CONNECT:Direct

You can customize CONNECT:Direct monitor resource definitions to suit your requirements. This section describes how to customize the monitoring criteria for the following:

- Heartbeat interval
- Queues
- Transfers
- Listener tasks (for CONNECT:Direct applications on distributed systems)
- TCP/IP connections
- Remote nodes

Customize the Heartbeat Interval

To customize how often the monitor status is updated

1. From the file transfer resource monitor, enter **U** beside the CDMON resource.

   The Monitor Details panel appears.

2. Complete the following field:

   Heartbeat Interval

   Defines how often the region retrieves status information in the format hh.mm.ss.

   hh

   Defines the interval time in hours.

   Limits: 24 hours

   mm

   Defines the interval time in minutes.

   Limits: 59 minutes

   ss

   Defines the interval time in seconds.

   Limits: 59 seconds

3. Press F3 (File).

   The system files the changes and the file transfer resource monitor appears. The new heartbeat interval is now in effect for the resource.

Customize Queues

To customize criteria for a CONNECT:Direct process queue or process resource monitor

1. From the file transfer resource monitor, enter **U** beside a process queue or status CDMON resource.

   The Monitor Details panel appears.

2. Complete the following fields:

   Queue Type

   Defines the logical CONNECT:Direct Transmission Control Queue that this resource monitors.

   Note: The options available are platform-dependent.

   Queue Depth Threshold

   Defines the number of CONNECT:Direct processes that can accumulate in the specified queue.

   Process Status

   Defines the process status monitored by this resource.

   Destination Node

   Restricts monitoring to specific CONNECT:Direct nodes. If you want to monitor all nodes, leave the fields blank.

   Process Name

   Restricts monitoring to specific CONNECT:Direct processes. If you want to monitor all processes, leave the fields blank.

3. Press F3 (File).

   The system files the changes and the file transfer resource monitor appears. The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customize Transfers

To customize the criteria for a CONNECT:Direct transfer monitor

1. From the file transfer resource monitor, enter **U** beside a transfer CDMON resource.

   The Monitor Details panel appears.

2. Complete the following fields:

   Stalled Time to Alert

   Defines the time an executing process is idle before an alert is raised.

   Stalled Time to Flush

   Defines the time an executing process is idle before it is flushed.

   Destination Node

   Restricts monitoring to specific CONNECT:Direct nodes. If you want to monitor all nodes, leave the fields blank.

   Process Name

   Restricts monitoring to specific CONNECT:Direct processes. If you want to monitor all processes, leave the fields blank.

3. Press F3 (File).

   The system file the changes and the file transfer resource monitor appears. The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customize Listener Tasks

These criteria are required for CONNECT:Direct applications on distributed systems only.

To customize the criteria for monitoring a CONNECT:Direct TCP/IP Listener Task:

1. From the file transfer resource monitor, enter **U** beside a listener task CDMON resource.

   The Monitor Details panel appears.

2. Complete the following fields:

   Retry Attempt

   Defines the number of times this monitor attempts to find the listener task.

   Retry Interval

   Defines the time interval between retry attempts.

   CONNECT:Direct Port No

   Restricts monitoring to specific CONNECT:Direct ports. If you want to monitor all ports, leave the fields blank.

   SNMP Community Name

   Restricts monitoring to specific CONNECT:Direct community names. If you want to monitor all names, leave the fields blank.

3. Press F3 (File).

   The system files the changes and the file transfer resource monitor appears. The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customize TCP/IP Connections

To customize the criteria for a CONNECT:Direct TCP/IP connections monitor

1. From the file transfer resource monitor, enter **U** beside a TCP/IP connections CDMON resource.

   The Monitor Details panel appears.

2. Complete the following fields:

   Idle Time to Alert

   Defines the time a TCP/IP connection remains idle before an alert is raised.

   Idle Time to Drop

   Defines the time a connection remains idle before it is dropped.

   Note: If the connections are established using CA TCPaccess FTP Server for z/OS, you cannot drop a connection automatically by using an idle time limit

3. Press F3 (File).

   The system files the changes and the file transfer resource monitor appears. The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customize Remote Nodes

To customize the criteria for a CONNECT:Direct remote node monitor

1. From the file transfer resource monitor, enter **U** beside a remote node CDMON resource.

   The Monitor Details panel appears.

2. Complete the following field:

   Remote Node Name

   Defines the remote file transfer CONNECT:Direct node that you want to monitor.

3. Press F3 (File).

   The system files the changes and the file transfer resource monitor appears. The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customize CONNECT:Mailbox

You can customize CONNECT:Mailbox monitor (CMMON) resource definitions to suit your requirements. This section describes how to customize the monitoring criteria for the following:

- Heartbeat interval
- Auto Connect queue
- BSC lines
- SNA sessions

Customize the Heartbeat Interval

To customize how often the monitor status is updated

1. From the file transfer resource monitor, enter **U** beside the CMMON resource.

   The Monitor Details panel appears.

2. Complete the following field:

   Heartbeat Interval

   Defines how often the region retrieves status information in the format hh.mm.ss.

   hh

   Defines the interval time in hours.

   Limits: 24 hours

   mm

   Defines the interval time in minutes.

   Limits: 59 minutes

   ss

   Defines the interval time in seconds.

   Limits: 59 seconds

3. Press F3 (File).

   The system files the change and the file transfer resource monitor appears. The new heartbeat interval is now in effect for the resource.

Customize Auto Connect Queues

To customize criteria for an Auto Connect Queue monitor

1. From the file transfer resource monitor, enter **U** beside an Auto Connect Queue CMMON resource.

   The Monitor Details panel appears.

2. Complete the following fields:

   Queue Depth Threshold

   Defines the number of CONNECT:Mailbox connections that can accumulate in the Auto Connect queue.

   List Name

   Restricts monitoring to specific CONNECT:Mailbox Auto Connect list names. If you want to monitor all names, leave the fields blank.

3. Press F3 (File).

   The system saves the changes and the file transfer resource monitor appears.

Customize BSC Lines

To customize criteria for a BSC line monitor

1. From the file transfer resource monitor, enter **U** beside a BSC line CMMON resource.

   The Monitor Details panel appears.

2. Complete the following fields:

   Automatic Restart?

   Defines whether a BSC line is automatically restarted.

   Line Name

   Defines the BSC lines to monitor.

3. Press F3 (File).

   The system saves the changes and the file transfer resource monitor appears.

Customize SNA Sessions

To customize criteria for an SNA session monitor

1. From the file transfer resource monitor, enter **U** beside an SNA session CMMON resource.

   The Monitor Details panel appears.

2. Complete the following fields:

   Stalled Time to Alert

   Defines the time an SNA session remains idle before an alert is raised.

   Remote Name

   Defines the remote site sessions to monitor.

3. Press F3 (File).

   The system saves the changes and the file transfer resource monitor appears.

Customize CA SOLVE:FTS

You use FTSMON class resources to monitor the links between CA SOLVE:FTS regions.

To customize how often a monitor resource checks the status of a link

1. From the file transfer resource monitor, enter **DB** beside the FTSMON resource.

   The ResourceView : Panel Display List panel appears.

2. Enter **S** beside the listed Monitor Details panel.

   This panel identifies the link being monitored and displays the heartbeat interval that determines how often the link status is checked.

3. Complete the following fields:

   Heartbeat Interval

   Defines how often the region retrieves status information in the format hh.mm.ss.

   hh

   Defines the interval time in hours.

   mm

   Defines the interval time in minutes.

   ss

   Defines the interval time in seconds.

4. Press F3 (File).

   The system files the changes and the file transfer resource monitor appears. The new heartbeat interval is now in effect for the resource.

Customize FTP Monitor

You can customize FTP monitor resource definitions to suit your requirements. This section describes how to customize the monitoring criteria for the following:

- Heartbeat interval
- TCP/IP connections
- Remote nodes

Customize the Heartbeat Interval

To customize how often the monitor status is updated

1. From the file transfer resource monitor, enter **U** beside the FTPMON resource.

   The Monitor Details panel appears.

2. Complete the following field:

   Heartbeat Interval

   Defines how often the region retrieves status information in the format hh.mm.ss.

   hh

   Defines the interval time in hours.

   Limits: 24 hours

   mm

   Defines the interval time in minutes.

   Limits: 59 minutes

   ss

   Defines the interval time in seconds.

   Limits 59 seconds

3. Press F3 (File).

   The system files the changes and the file transfer resource monitor appears. The new heartbeat interval is now in effect for the resource.

Customize TCP/IP Connections

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 resource monitor.

To customize the criteria for an FTP TCP/IP connections monitor

1. From the file transfer resource monitor, enter **U** beside a TCP/IP connections FTPMON resource.

   The Monitor Details panel appears.

2. Complete the following fields:

   Idle Time to Alert

   Defines the time a TCP/IP connection remains idle before an alert is raised.

   Idle Time to Drop

   Defines the time a connection remains idle before it is dropped.

3. Press F3 (File).

   The system files the changes and the file transfer resource monitor appears. The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Customize FTP Remote Nodes

To customize the criteria for an FTP remote node monitor

1. From the file transfer resource monitor, enter **U** beside a remote node FTPMON resource.

   The Monitor Details panel appears.

2. Complete the following fields:

   TCP/IP Host Name/Addr

   Defines the host name or address of the remote FTP server to monitor.

   TCP/IP Port Number

   Defines the port number of the remote FTP server to monitor.

   Time Out After

   Defines the number of seconds to wait for the status of the remote node to be resolved.

3. Press F3 (File).

   The system files the changes and the file transfer resource monitor appears. The region issues a CHK command to recheck the status of the updated monitor, using the new values.

Use 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 more information about other macros, see the online help.

Define a Process

To define a process

1. Enter **/RADMIN.P** at the prompt.

   The Process List appears.

   Note: The process you create here is available to the specified system image only. To create a process that is available to *all* definitions in the knowledge base, enter **/RADMIN.GP** as the path.

2. (Optional) Change the displayed system image. The last specified system image is the default system image.

3. Press F4 (Add).

   The Process Definition panel appears.

4. Complete the following fields:

   Name

   Specifies the name of the process (for example, SNMPTRAP).

   Description

   Describes your process.

5. Complete the fields of the Process Steps window. For more information about the fields, press F1 (Help).

6. Enter **P** beside each process step and specify the macro parameters.

7. Press F3 (File).

   The system files the definition.

You can now specify the process in a resource definition for any action that requires more complex processing.

Check 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.

Specify the PINGCD Macro

To specify the PINGCD macro in your process

1. Add or update a process for the macro.
2. Complete the following fields on the Process Definition panel:

   Step Name

   Specify the process step.

   Macro

   Specify **PINGCD** as the name of the macro.
3. Enter **P** beside your line entry.

   The PINGCD Macro Parameter Definition panel appears.
4. Enter the PINGCD macro details. For more information about the fields, see the online help.
5. Press F3 (OK).

   The Process Definition panel appears.

Issue 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.

Specify the CDAPI Macro

To specify the CDAPI macro in your process

1. Add or update a process for the macro.
2. Complete the following fields from the Process Definition panel:

   Step Name

   Specifies the process step.

   Macro

   Specifies the name of the macro. Enter **CDAPI**.
3. Enter **P** beside your line entry.

   The CDAPI Macro Parameter Definition panel appears.
4. Enter the CDAPI macro details. For more information about the fields, see the online help.
5. Press F3 (OK).

   The system saves your changes and the Process Definition panel appears.

Use the SNMP Trap Exit

You can generate SNMP traps to inform a remote system of a resource state change.

The SNMPTRAP macro is supplied. To generate an SNMP trap, you define a process that uses this macro.

Create an SNMP Trap in a Process

To create an SNMP trap

1. Add or update a process for the trap.
2. Complete the following fields on the Process Definition panel:

   Step Name

   Specifies the process step.

   Macro

   Specifies the name of the macro. Enter **SNMPTRAP.**
3. Enter **P** beside your line entry.

   The SNMPTRAP Macro Parameter Definition panel appears.
4. Complete the following fields:

   Text

   Specifies the text to send with the trap.

   Destinations Dataset

   (Optional) Specifies the data set name (DSN) in which the addresses of remote systems is located

   Destination Address(es)

   (Optional) Specifies the destination addresses of the remote systems.

   Enterprise ID

   Specifies the format of the trap.

   Note: The format identified by this field is determined by your open platform administration

   Specific Trap Number

   Specifies the trap number.

   Community Name

   Specifies the community for which the trap is destined.
5. Press F3 (OK).

   The system saves the details and the Process Definition panel appears.

Generate an Exception Report from a Process

The FTCHECK macro generates a file transfer exception report based on a specified filter. If a return code of 4 is received, more 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.

Specify the FTCHECK Macro

To specify the FTCHECK macro in your process

1. Add or update a process for the macro.
2. Complete the following fields from the Process Definition panel.

   Step Name

   Specifies the process step.

   Macro

   Specifies the name of the macro. Enter **FTCHECK**.
3. Enter **P** beside your line entry.

   The FTCHECK Macro Parameter Definition panel appears.
4. Enter the FTCHECK macro details. For more information about the fields, press F1 (Help) to view the online help.
5. Press F3 (OK).

   The settings are saved and the Process Definition panel appears.

Chapter 17: Implementing Processes

This section contains the following topics:

How to Implement Processes

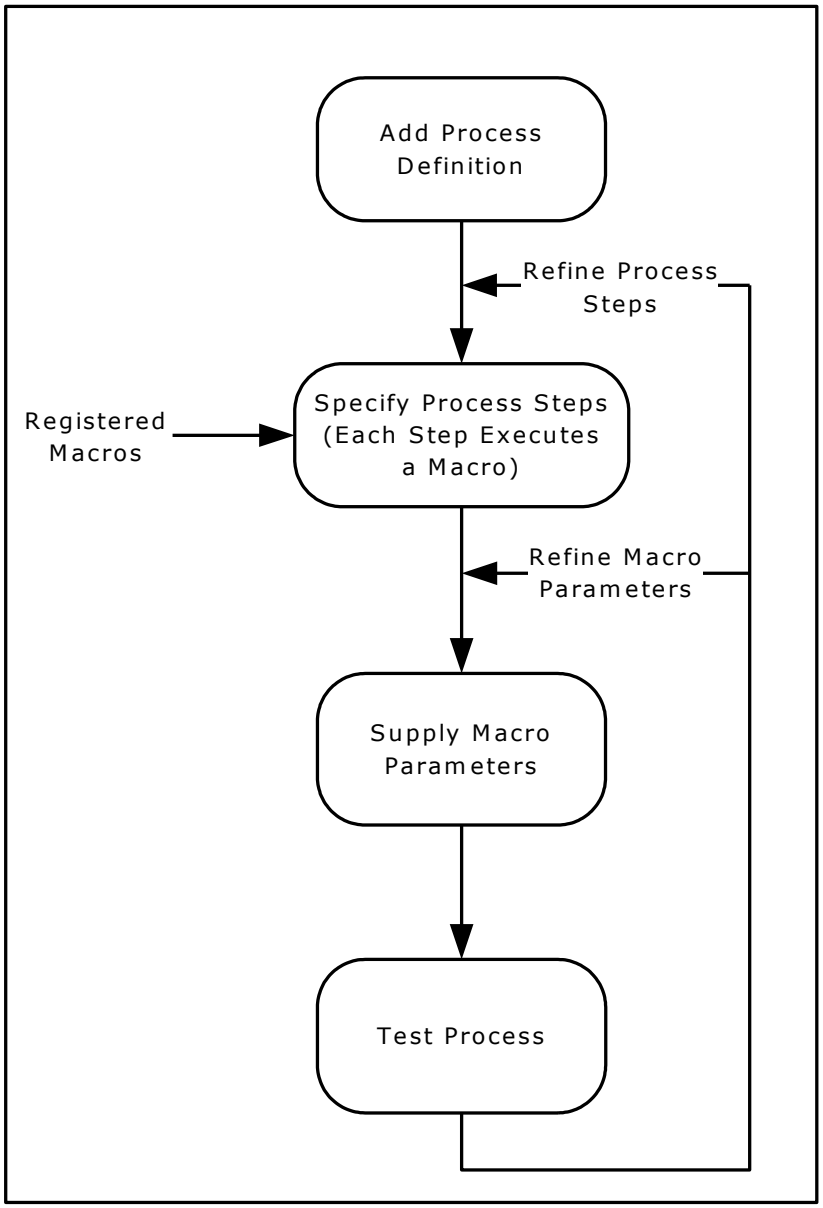
A process is a series of steps that can be executed in sequence to perform complex processing.

You define processes to automate complex operations tasks.

Processes can be executed as follows:

- From a resource definition—you can specify a process in a resource definition. The process is invoked when required for that resource.
- From an availability map—you can specify a process in an availability map (for example, to perform tasks at particular times).
- From an event rule—you can specify a process in an event rule. The process is invoked when an event triggers the rule.
- As a single task—you can run a process as a single, independent task. Use this feature to debug processes or as a quick way of executing a process manually.
- Interactively—you can run a process in the INTERACTIVE mode. Use this feature to check the results of processing single steps, or of processing a sequence of steps one at a time. You can display individual step logs and, if required, change the step parameters.

The following illustration shows the typical stages in defining a process.



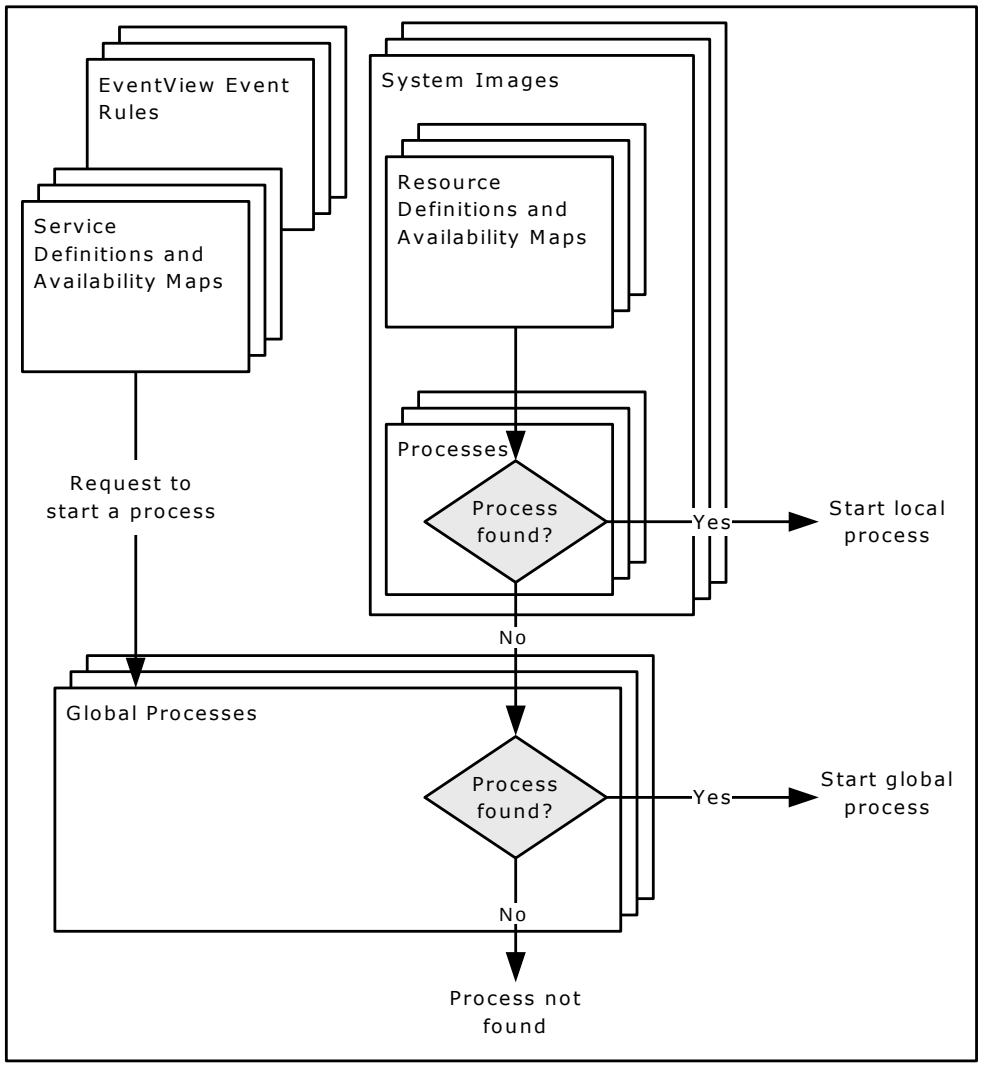
Process Types

A process can be global (available to all components) or local (available to a specific system image only). A global process is available to all components; however, a local process is available only if it belongs to the local active image.

ServiceView and EventView components can use global processes only. ResourceView components can use both types of processes, according to the following rules:

- If a process is required and one exists in the local active system image, that process is used.
- If the required process does not exist in the active system image, the global process of the same name is used.

The following illustration shows how processes are searched for execution.



Access Process Definitions

Each system image has its own set of processes and access to global processes belonging to the $PROCESS 0001 system image.

To access the local process definitions in a system image

1. Enter **/RADMIN**.

   The Resource Administration menu appears.

2. Type the option code **P**, and the name and version of the system image, and press Enter.

   The Process List panel appears. This panel lists the processes in the system image and the global processes (displayed in blue on a color terminal).

To access the global process definitions

1. Enter **/RADMIN.GP**.

   The Process List panel appears. This panel lists the global processes.

How to Define a Process

From the Process List panel, press F4 (Add) to add a process definition. A Process Definition panel is displayed.

To define a process, first decide what you want the process to do, then break it down into steps, each step representing an action. Specify a macro for each step. A macro is an NCL procedure that performs the processing for that step. Authorized users can use the Register Macros option to register new macros.

Step processing can be conditional on the processing result of an earlier step. In the following example, STEP2 runs if STEP1 processing returns a code of 0. STEP3 runs if STEP1 processing returns a code greater than 0.

```
                Condition
StepName    Step/RC  Opr RC
STEP1       STEP1
STEP2       STEP1     =   0
STEP3       STEP1     >   0
```

When you define a process on the Process Definition panel, complete the following fields:

- Name and Description fields to identify the process
- StepName and Macro fields to define each step

If you want to find out what macros are available, enter **?** in a Macro field to display the list of available macros.

Important! $NCL is the name of a special process definition. Do not use this name when you add process definitions.

Conditions are optional. Use relational operators in the Opr fields to set the conditions. Enter **?** in an Opr field to identify the valid relational operators.

You can repeat and delete steps, and insert blank lines.

Press F11 (Right) to display the parameters for each step.

The return code from a process is the return code from the last executed process step.

Example: Issue Multiple System Commands

The following shows an example of a process that issues multiple system commands.

```
PROD----------- Automation Services : Process Definition ----------Function=Add
Command ===>                                                  Scroll ===> PAGE

+ Process Definition ------------------------------------------------------------+
| System Name .. PROD      Version .. 0001   Last Updated By                     |
| Name ......... TEST PROC                   at           on                    |
| Description .. ISSUE SYSTEM COMMANDS                                           |
+--------------------------------------------------------------------------------+
+ Process Steps ------------------------------------------------------------------+
|                                                                                |
|                                       D=Delete I=Insert P=Parms R=Repeat       |
|                    Condition                                                   |
|      StepName   Step/RC  Opr RC    Macro    Description                        |
|      STEP1                         SYSCMD   EXECUTE A COMMAND                  |
|      STEP2      STEP1    =   0     SYSCMD   EXECUTE A COMMAND                  |
|      STEP3      STEP2    =   0     SYSCMD   EXECUTE A COMMAND                  |
|      STEP4      STEP1    =   99    SYSCMD   EXECUTE A COMMAND                  |
|                                                                                |
|                                                                                |
|                                                                                |
|                                                                                |
|  F1=Help     F2=Split    F3=File     F4=Save                                   |
|  F7=Bkwd     F8=Forward  F9=Swap               F11=Right   F12=Cancel        |
+--------------------------------------------------------------------------------+
```

If STEP1 completes successfully, STEP2 executes the next shutdown command. If STEP2 completes successfully, STEP3 issues the final shutdown command.

If STEP1 fails, STEP4 executes and issues a CANCEL command.

Set Macro Parameters

When you select a macro, it contains either no parameters or default parameters.

To set the parameters for a macro

1. Enter **P** next to the process step.

   A Macro Parameter Definition panel appears.

2. Change the parameters as required and press F3 (OK). The parameters required by each macro depend on the purpose of the macro.

Example: Set Macro Parameters

The following shows the parameters set for Step 1 in the previous example.

```
PROD----- Automation Services : SYSCMD Macro Parameter Definition -------------
Command ===>                                                  Function=UPDATE

+- System Command ------------------------------------------------------------+
|                                                                             |
| Command ..... F CA7T,/LOGON MASTER_____________________________________     |
|                                                                             |
| Jobname ..... ________                                                      |
|                                                                             |
| Wait Time ... 30__  Wait Time Expiry Return Code ... 99_                    |
+-----------------------------------------------------------------------------+
+- Response Message Analysis --------------------------------------------------+
|                                D=Delete Extended Filter  S=Extended Filter  |
|           Message Text                                    Return Extended   |
|                                                           Code   Filter?    |
|   ___     CA-7.023 - V3.0 (9106) OPERATOR IS LOGGED ON_   0__    NO         |
|   ___     ____________________________________________    ___               |
|   ___     ____________________________________________    ___               |
|   ___     ____________________________________________    ___               |
|   ___     ____________________________________________    ___               |
|                                                                             |
+-----------------------------------------------------------------------------+
 F1=Help      F2=Split     F3=OK
                           F9=Swap                              F12=Cancel
```

The parameters include:

- The system command issued
- The text of the expected response
- A processing return code of 0
- A wait time of 30 seconds
- A time-out return code of 99

You can also specify an extended filter for the analysis of the response message text. For example, a response can contain variable information and you want to accept the message only if it contains specific values.

Variable as a Macro Parameter

You can use a variable to hold the value of a macro parameter. You pass the value of any variables required by a process as parameters when you specify the process, for example, in a resource definition.

Important! Do *not* specify variable names that start with #, $, or Z.

Example: Use a Variable as a Macro Parameter

You have defined a process that contains the SYSCMD macro which issues the $DU,&PRT command. When you use the process, you supply the value of the &PRT variable by specifying the following parameter: PRT=*printer-name*. Specify the name of the variable only (without the &).

Generic Processes Using Resource Variables

You can define generic processes that perform functions that are dependent on how they are initiated by using resource variables. These variables contain information about a resource that is defined to the knowledge base. They are useful for building automated paging, standardized startup for CICS regions, and many other tasks where a uniform solution is required. Using a generic process reduces any overhead associated with building individual processes for individual resources.

Note: For information about knowledge base variables, see the *Reference Guide*.

Example: Use Process to Page Support

Service level agreements require that appropriate support personnel are pageable if any production CICS region is under stress. CA AP is available at your site to monitor the condition and provide the paging function. Different CICS regions have different support personnel assigned.

You implement the following method in the CICS resource definitions:

1. Specify details of the support personnel.
2. Identify and specify the message to trigger automated paging.
3. Specify an event-related action for this message using the following generic process:

	Condition					
	StepName	Step/RC	Opr	RC	Macro	Description
	S1				WTOR	WTOR TO L1 SUPPORT
	S2	S1	EQ	32	WTOR	TIMED OUT - CALL L2
	S1OK	S1	EQ	0	SETSTATE	L1 RESPONDED - SET EXT. DISPLAY
	S2OK	S2	EQ	0	SETSTATE	L2 RESPONDED - SET EXT. DISPLAY
	S3	S2	NE	0	GENALERT	NO SUPPORT - RAISE ALERT
	S4	S2	NE	0	SETSTATE	NO SUPPORT - SET EXT. DISPLAY

   a. At Step S1, the resource sends a WTOR message, using knowledge base variables (for example, &ZRMDBREOPAG1 that contains the pager number) to provide details of the support personnel responsible for the failing resource.

      CA AP or by an operator intercepts the WTOR message, and the indicated first-level support person is paged. Response to the message indicates the success or failure of paging.

   b. If paging of the first-level person is successful, Step S1OK sets the extended display of the resource to indicate that the support person has acknowledged the paging.

      If no reply is received within a specified period, Step S2 sends another WTOR message to invoke paging of the second-level support person.

   c. If paging of the second-level person is successful, Step S2OK sets the extended display of the resource to indicate that the support person has acknowledged the paging.

      If paging fails, Step S3 raises an alert and Step S4 sets the extended display of the resource to indicate that no support personnel have responded.

Processes to Generate Alerts

You can use a process in a ResourceView resource definition or an EventView message rule to generate alerts in response to problems occurring in a resource.

The GENALERT macro enables you to generate an alert from a process.

Example: Generate Alert on Security Violation

The DFHAC2003 message indicates that a CICS security violation has occurred. You may want to be warned of these violations. The following panels show the message rule definition that generates an alert under this condition by using the SECALERT process definition:

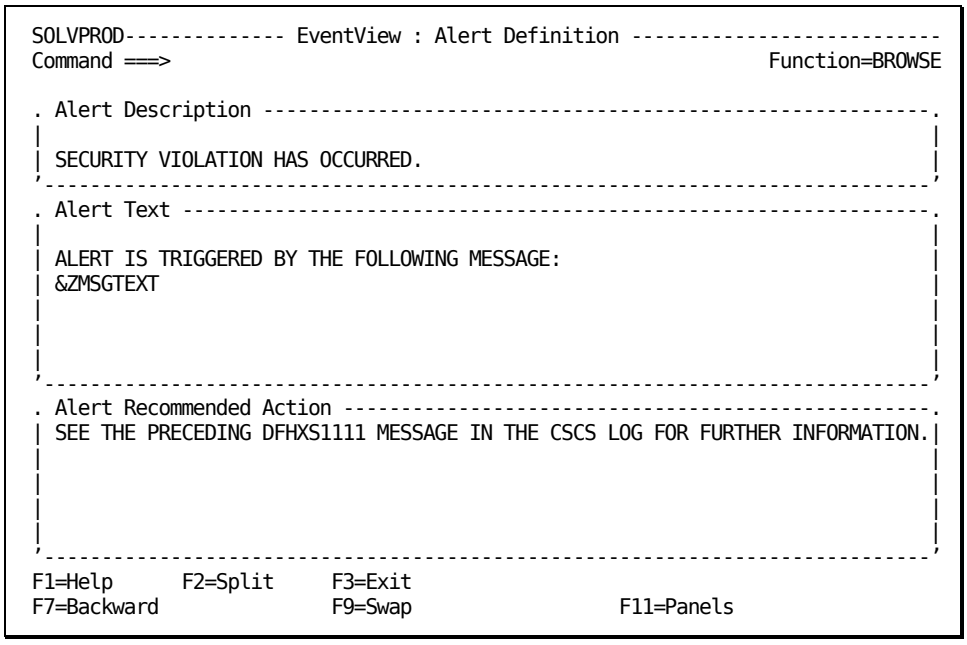
```
SOLVPROD--------------- EventView : Message Filter -------------------CICSSEC--
Command ===>                                                  Function=BROWSE

Ruleset Name ........ CICSSEC                       Rule Status .... ACTIVE
Short Description ... CICS security alerts

. Expected Message ------------------------------------------------------------.
|                                    S=ListPanels E=ExtFilter T=TestVars |
|      Message Text  ( WildChar = * )                                ExtFlt |
| ___  DHFAC2003                                                     NO     |
```

```
SOLVPROD---------- EventView : DHFAC2003 Message Actions ------------CICSSEC--
Command ===>                                                  Function=BROWSE

Reply Text .......

System Command ...

MS Command .......


. Automation Actions ----------------------------------------------------------.
|                                                  S/B=Browse U=Update L=List |
|      Process     Parameters                                                 |
| ___  SECALERT                                                               |
```

The following panels show the SECALERT process definition and the parameters used by the GENALERT macro:

```
SOLVPROD------- Automation Services : Process Definition -------Function=Browse
Command ===>                                                  Scroll ===> CSR

. Process Definition ------------------------------------------------------.
| System Name .. $PROCESS  Version .. 0001   Last Updated By USER01         |
| Name ......... SECALERT                    At 16.21.13  On WED 24-JUL-1996 |
| Description .. CICS security violation alert generator                    |
'---------------------------------------------------------------------------'
. Process Steps -----------------------------------------------------------.
|                                                                           |
|                                                                  P=Parms  |
|                    Condition                                              |
|      StepName   Step/RC  Opr RC    Macro    Description                   |
| P    A                             GENALERT GENERATE AN EVENTVIEW ALERT   |
|     **END**                                                               |
```

```
SOLVPROD-------------- EventView : Alert Attributes --------------------------
Command ===>                                                  Function=BROWSE

. Alert Reference Key -----------------------------------------------------.
|                                                                          |
| Reference ... CICS_SECURITY_ALERT_&ZMSGWORD20                            |
|                                                                          |
'--------------------------------------------------------------------------'
. Alert Attributes --------------------------------------------------------.
|                                                                          |
| Severity .... 2                                                          |
| Type ........ DEFAULT                                                    |
| Origin ...... ALERTMACRO                                                 |
```



How You Test a Process

After you have defined a process, you can test it by executing it as a single task or by executing it in the interactive mode.

Test a Process Interactively

From the Process List panel, enter **I** beside a process to execute it in the interactive mode. The Process Definition panel for that process appears. You can:

- Enter **E** beside a step to execute only that step irrespective of the condition.
- Use F12 (Step) to execute a number of steps in sequence. Pressing F12 (Step) executes the next step in the sequence. The execution of each step depends on the condition specified for the step.
- Enter **L** beside an executed step to see the processing log. The log display is positioned at the latest entries relating to the selected step.
- Enter **P** beside a step to view the macro parameters.

To interactively edit and test the process steps

1. Press F4 (Edit) to access the Interactive Edit function to edit the process steps.
2. Modify the steps, as required.
3. When you complete the modifications, press F4 (OK) to return to the INTERACTIVE mode. You can also press F3 (File) to return to that mode. Pressing F3 (File) saves the modifications.
4. Test the modified process.
5. Press F3 (Exit) and F3 (File) again to save the modified steps.

   If the test is not satisfactory, restart from Step 1.

Test a Process by Execution as a Single Task

To test a process by execution as a single task

1. From the Process List panel, enter **E** beside a process.

   The task is executed as a single, independent task. The Optional Process Parameter Specification panel appears.

   Note: When you use the E action code to execute a process, the process is executed under the BSYS background user ID.
2. Supply any parameters required by the process in the Parameters field, then press F6 (Action).

   When the process has executed, a processing log appears. This log contains the processing results.

How You Log Process Activities

Process activities are written to the activity log while you are testing a process. However, you can control the logging when a process is executed, for example, from a resource definition. Use the $LOG process parameter to control the logging as follows:

$LOG=BOTH

Logs activities in full and summary form.

$LOG=FULL

Logs activities in full.

$LOG=NO

(Default) Does not log activities.

$LOG=SUMM

Logs activities in summary form only.

Maintenance of Process Definitions

You can browse, update, copy, and delete process definitions from the Process List panel.

Back Up Global Processes

To assist you with the maintenance of your global processes, you can create backup versions of your global process image. By creating a backup version of your global process image, you can perform the following:

- Update global process definitions in any version of a global process image.
- Restore a global process definition from a backup global process image.
- Merge two versions of a global process image.

To create a backup version of a global process image

1. Enter **/ASADMIN.GPI** at the prompt.

   The Global Process Image List appears.

   Note: If you have not created a backup before, there is only one global process image listed: $PROCESS 0001. The active global process image can only be $PROCESS 0001. $PROCESS 0001 cannot be deleted.

2. Enter **C** beside the global process image you want to copy.

   The Global Process Image Definition panel appears.

3. Enter a new Database Version, Short Description, and Long Description.

4. Press F3 (File).

   The backup version of the global process image is saved. A copy in progress panel appears while the copy occurs. The Global Process Image List appears with the backup version displayed in the list.

   If the global process image you have specified already exists, the Confirm System Image Merge panel appears.

Update Global Process Definitions in a Backup Global Process Image

You can access a list of all the global process definitions in any version of a global process image. From this list you can update any global process definition contained in the global process image.

To update a global process definition in the $PROCESS 0002 backup image created above

1. Enter **L** (List Processes) beside the $PROCESS 0002 global process image in the Global Process Image List.

   The Global Process List panel appears showing all of the global process definitions in that global process image.

   Note: You can access the list of global processes for another version of the global process image by changing the version number on the Global Process List panel and pressing Enter.

2. Enter **U** beside the global process definition that you want to update.

   The Process Definition panel appears for that global process definition.

3. Update the global process definition, as required.

4. Press F3 (File).

   The changes are saved and the Global Process List appears.

Restore a Global Process Definition from a Backup Global Process Image

If you have made changes to a global process definition and you are having trouble with its implementation, you can restore it from a previous version of the definition.

To restore global process definition $PROC01 from $PROCESS 0002 to $PROCESS 0001

1. Enter **C** beside $PROC01 in the global process list.

   The Process Definition panel appears.

2. Change the Database Version from 0002 to 0001 and press F3 (File).

   The changes are saved. Because there is already a copy of the global process in the target global process image, the Confirm Copy Replace panel appears.

3. Press Enter to confirm the replace or F12 (Cancel) to cancel the request.

   The Global Process List appears.

Change a Global Process to a Local Process

You can change a global process to a local process while performing a copy on any global process in the global process selection list.

To change global process PROC01 to a local process in the SYS01 system image

1. Enter **C** beside PROC01 in the Global Process List.

   The Process Definition panel appears.

2. Change the System Name to SYS01 and press F3 (File).

   The Global Process List appears.

   To view the new local process, access the list of processes for the system image that you copied it to.

Merge Two Global Process Images

You can merge two global process images and replace the active global process image with a backup version.

To merge global process images $PROCESS 0002 and $PROCESS 0001

1. Enter **C** beside the $PROCESS 0002 on the Global Process Image List.

   The Global Process Image Definition panel appears.

2. Change the Database Version number to 0001 and press F3 (File).

   The Confirm System Image Merge panel appears.

3. Enter **YES** in the input field if you want to overlay like-named components.
4. Press F6 (Confirm).

   The global process images are merged.

Chapter 18: Implementing the Graphical Monitor

This section contains the following topics:

Graphical Monitor

The graphical monitor presents the status of resources in icons on an icon panel.

You customize the graphical monitor by using icon panels. You can change the icon panel to obtain a different view of the monitored systems and networks. By zooming (Z) in on an icon, you can selectively view the group of resources that it contains.

The graphical monitor monitors groups of resources as a single entity.

How You Customize the Graphical Monitor

To customize the graphical monitor, you define resource groups, icons, and icon panels. You arrange icons on icon panels and attach resource groups to the icons so that each icon on the panel represents a group of resources. After you generate an icon panel, an operator can use that panel to customize the graphical monitor.

You generate an icon panel as follows:

1. Define the required resource groups.
2. Define the icons to use on an icon panel.
3. Define the icon panel.
4. Place the defined icons on the panel and attach resource groups to them.

When you save a resource group, icon, or icon panel definition, or generate an icon panel description file, it propagates to all the connected regions. That is, the definition of the generated icon panel is global.

Resource Groups for Icons

A resource group represents a group of resources that you have defined in the knowledge base. To define a resource group, use *one* of the following methods:

- **Specify an Icon Panel**

  The panel displays icons representing other resource groups. Use the Zoom Icon Panel Definition panel to specify the icon panel.

- **Specify a Group of Resources**

  You can identify up to 16 resources by class and name. Thus, the identified resources are independent of system images. In a multisystem environment, the specified class and name points to resources in all the system images that are loaded in the linked regions. You can, however, specifically exclude remote resources. Use the Resource Filter Definition panel to specify the resources to group.

- **Specify a Resource Group Filter**

  A resource group filter uses a Boolean expression to define a group of resources. You group the resources by their static attributes such as names and parent system images. Use the Resource Group Filter Definition panel to define the Boolean expression.

Access Resource Group Definitions

The Resource Groups List displays the list of resource group definitions in the knowledge base. You can add a new definition, or browse, update, copy or delete an existing definition.

To access resource group definitions, enter **/GADMIN.G** at the command prompt.

The Resource Group List appears.

Add a Resource Group Definition

To add a resource group definition

1. Enter **/GADMIN.G** at the prompt.

   The Resource Group List appears.

2. Press F4 (Add) to add a group definition.

   The Resource Group Definition panel appears.

   Note: If you change your mind and do not want to add the group, press F12 (Cancel) to cancel the operation any time before Step 6.

3. Complete the Name and Description fields to identify the new group.
4. Select *one* of the following options to define the group:
   - Select option A to specify an icon panel.

     The Zoom Icon Panel Definition panel appears. Proceed to Step 5a.
   - Select option B to specify a group of resources by class and name.

     The Resource Filter Definition panel appears. Proceed to Step 5b.
   - Select option C to specify a resource group filter.

     The Resource Group Filter Definition panel (see page 232) appears. Proceed to Step 5c.

   Note: Options B and C are related. You can use option B to specify the services and resources in the group directly. If you then select option C, the specification defined by using option B is expanded into a Boolean expression.
5. Depending on the option you select, proceed as follows:
   a. Specify the name of a generated icon panel in the Zoom Icon Panel Name field. You can enter a question mark (?) in the field to access the icon panel prompt list from which you can select the required panel.

      After you specify the name, proceed to Step 6.
   b. Identify the resources by class and name in the ClassDsc and Resource Name fields. You can enter a question mark (?) in the fields to access the resource class and resource name prompt lists from which you can select the required class and name.

      If you want to exclude the resources from remote systems, specify **Y** (yes) in the Exclude Remote System Resource field. The default is NO.

      After you identify the resources, proceed to Step 6.
   c. Press F10 (EditFltr) to edit the filter. See the online help for a description of the fields.

      Specify the Boolean expression (see page 232) in the Filter Expression window to define the filter.

      Press F3 (OK) to exit the edit mode, then proceed to Step 6.
6. Press F3 (File) to file the new definition when you finish defining the group.

Resource Group Filter Definition Panel

The Resource Group Filter Definition panel specifies the details of a resource group.

The panel displays two windows. The Filter Definition window identifies the filter, and the Filter Expression window specifies the Boolean expression of the filter.

Example: Resource Group Filter Definition Panel

This example defines a group that contains all started tasks except those resources with a name of PCICS1.

```
PROD1------ Automation Services : Resource Group Filter Definition ------------
Command ===>                                                    Function=UPDATE

. Filter Definition ------------------------------------------------------------.
| Name ......... $ICRSRC                                                       |
| Description .. RESOURCE GROUP "RSRC" DIRECT FILTERING                        |
| Last Updated at 17.11.27 on SUN 06-FEB-2011 by USER01                        |
'------------------------------------------------------------------------------'
. Filter Expression ------------------------------------------------------------.
|                                                                              |
|      "(" Field    Opr Value                                  Gen ")" Bool    |
|      (   CLSNAME  EQ  "STC"                                          AND     |
|          NAME     NE  "PCICS1"                                   )           |
|     **END**                                                                  |
```

Resource Group Filter Expression

Use the Filter Expression window on the Resource Group Filter Definition panel to specify the Boolean expression that defines the filter. The expression uses resource attributes to determine what belongs to the group.

Use the following action codes to help you enter the expression:

D (Delete)

Deletes the selected line.

I (Insert)

Inserts a blank line after the selected line.

R (Repeat)

Repeats a selected line.

Maintenance of Resource Group Definitions

You can browse, update, copy, and delete group definitions from the Resource Group List panel.

Note: During an update, if the resources in the resource group are specified by using option C, you have no access to option B.

Except as noted above, you can change the method of definition during an update. Saving a definition by a new method automatically overrides the definition by the current method.

Icons

An icon is a graphic that you can use to represent resource groups on the graphical monitor. You use icons to build icon panels. You position one or more icons on a panel and attach resource groups to the icons, one group for each icon. When used, an icon displays a status determined by the status of the underlying group members. An operator can zoom in on an icon using the Z (Zoom) command. This action displays another icon panel or a group of resources in the Status Monitor, as determined by the attached resource groups. Use the Icon Editor to define an icon.

Access Icon Definitions

To access icon definitions, enter **/GADMIN.I** at the prompt.

The Icon List panel appears.

The panel displays the list of icon definitions in the knowledge base. You can add a new definition, or browse, update, copy or delete an existing definition. You can also edit a definition from the Icon Panel Generator panel.

Define an Icon

You use icons to build the panel for your graphical monitor.

To define an icon

1. Enter **/GADMIN.I** at the prompt.

   The Icon List panel appears.

2. Press F4 (Add).

   The Icon Editor panel appears.

3. Complete the following fields:

   Name

   Specifies the name of the icon.

   Description

   Describes the icon.

   Icon Height

   Specifies the height of the icon in lines.

   Icon Width

   Specifies the width of the icon in characters.

   Note: If you change the default size, press Enter to update the shape of the icon in the Edit Area window.

   Specify the values you want to display (see page 236) on the icon.

4. Press F3 (File).

   The new definition is saved.

Icon Editor Panel

The Icon Editor panel specifies the details of an icon. The operation you are performing is displayed at the top right of the panel, for example, Function=UPDATE.

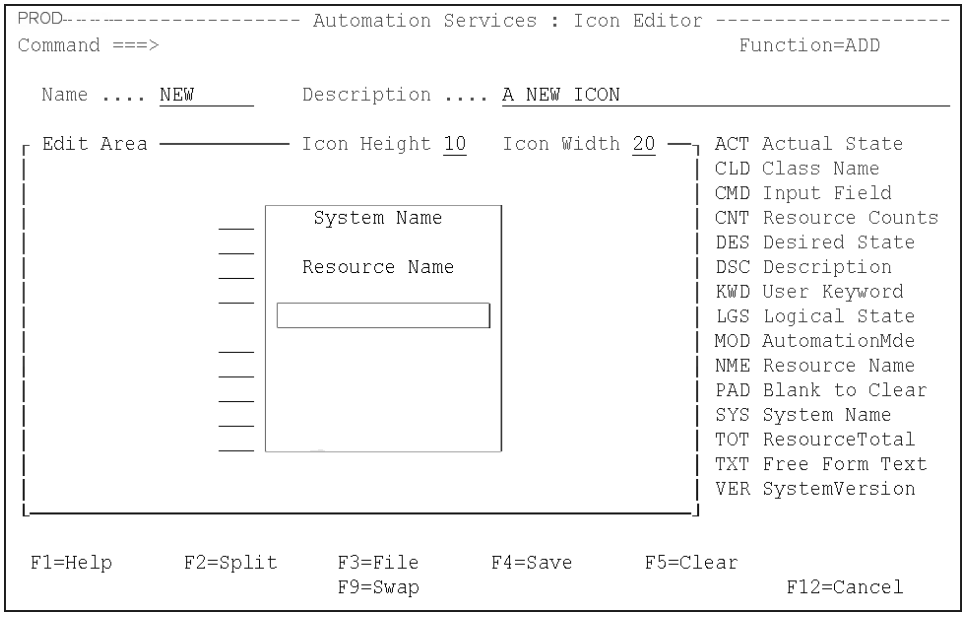
The panel specifies the following information:

- Name and description of the icon
- Size of the icon (height and width)
- Actual icon representation

The Edit Area window specifies the values you want to display on the icon.

Example: Icon Editor Panel

This example defines a resource icon.



How You Edit the Icon

Use the Edit Area window on the Icon Editor panel to specify what you want to display on the icon.

The icon contains the number of lines specified in the Icon Height field. Use the three-character codes listed to the right of the Edit Area window to specify the values you want displayed on the icon. To use a code, enter the code in a line field. You can use the code on any line, irrespective of whether the line is blank or not. Except for the TXT code, executing a code on a line overrides what is already there.

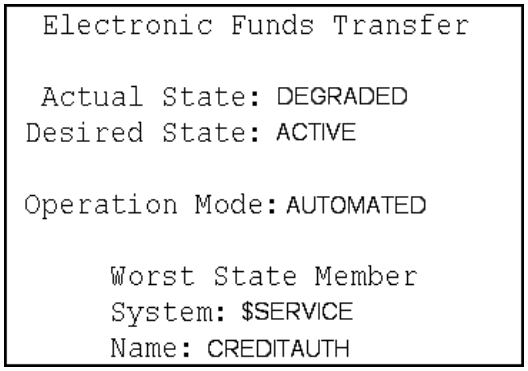
You can type codes in more than one line field, then press Enter to execute the codes.

Pressing F5 (Clear) clears the icon. Use the PAD code to clear a line.

Note: For information about the codes, see the online help.

Icon Definition Example

In this example, an icon, EFTPOS, is defined for the group of services and resources that support electronic funds transfer. The finished icon as it appears to an operator is shown in the following figure:



To define the icon

1. Enter **/GADMIN.I** at the prompt.

   The Icon List panel appears.

2. Press F4 (Add).

   The Icon Editor panel appears.

3. Enter **EFTPOS** in the Name field and a description in the Description field, for example, Electronic funds transfer.

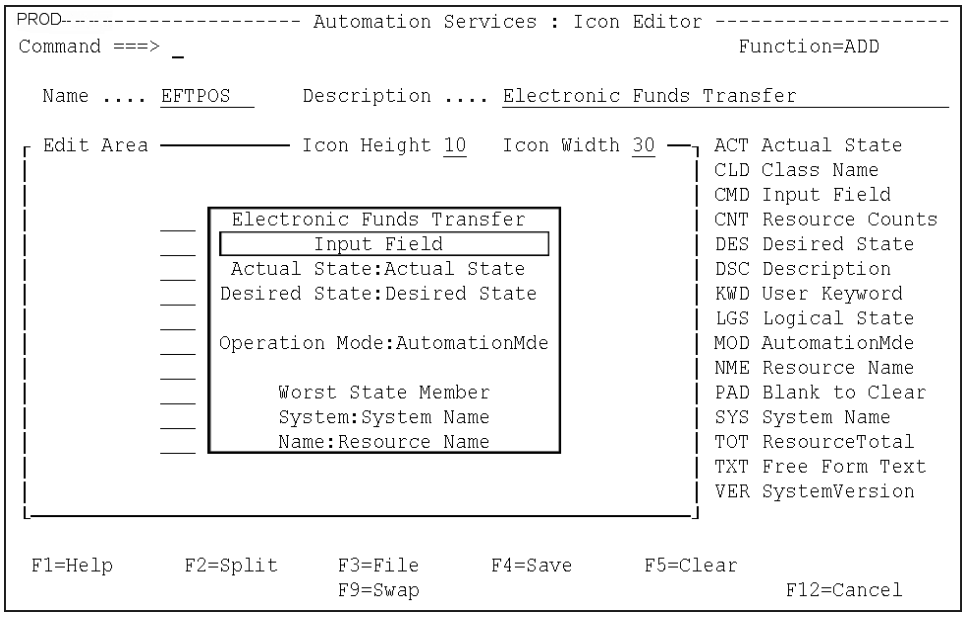
4. You want the icon size to be 10 lines by 30 characters. Change the icon width to 30, and press Enter to update the shape of the icon.

5. Enter **TXT** in the first line field. A text field appears in the icon.

6. Enter **ELECTRONIC FUNDS TRANSFER** in the text field.
7. Enter **CMD** in the second line field to create the command entry field.
8. Enter **ACT** in the third line field.
9. To add the description to the field, enter **TXT** in the line field. Enter **Actual State** in the displayed text field. A colon is inserted automatically after the entered text.
10. Repeat steps 8 and 9, using the appropriate codes, for the following information:
    - Desired state (line 4)
    - Operation mode (line 6)
    - Identity of the group member that has the worst logical state (lines 9 and 10)

    Use steps 5 and 6 to enter the Worst State Member label (line 8).
11. Press F3 (File) to file the definition when you finish with the panel.

The following shows the completed Icon Editor panel.



Icon Panels

An icon panel defines what is displayed on the graphical monitor. You arrange icons on the panel and attach resource groups to the icons.

You can define your own icon panel or select one of the predefined panels provided with your product.

When you create an icon panel, you create an icon panel definition and the icon panel description file. An operator uses the panel to customize the graphical monitor. You can generate an icon panel (that is, the description file) only if all the icons on the icon panel definition have attached resource groups. Use the Icon Panel Generator to define and generate the icon panel.

Important! Icon panels defined on a 3270 Model 4 or equivalent terminal cannot be used on Model 3 and Model 2 terminals. Icon panels defined on a Model 3 terminal cannot be used on Model 2 terminals.

Access Icon Panel Definitions

To access icon panel definitions, enter **/GADMIN.P** at the prompt.

The Icon Panel Definition List panel appears. The panel displays the list of icon panel definitions in the knowledge base. You can add a new definition, or browse, update, copy, or delete an existing definition.

Define an Icon Panel

When you define an icon panel, you can create a new panel or select a pre-defined panel. A default panel is distributed for your product; however, if you have installed more than one product in your environment, $RMDYNAMIC is your default icon panel.

Note: $RMDYNAMIC is the default icon panel when more than one product is present in a region. It dynamically displays one icon per product found on the region. As such, it is different to other icon panels and should not be edited or regenerated by users. If it is regenerated in error, panel $RMDYNAMICBU is available in the ICOPANL data set to use to recover $RMDYNAMIC.

To define an icon panel

1. Enter **/GADMIN.P** at the prompt.

   The Icon Panel Definition List panel appears.

2. Do *one* of the following:

   - Press F4 (Add) to add a new icon panel definition.

     The Icon Panel Generator Initial Help panel appears.

   - Select one of the pre-defined defaults for your product.

     The Icon Panel Generator Initial Help panel appears.

   Note: Pressing F4 (Remove Help Screen) exits and removes permanently the help panel. That is, the help panel does not appear the next time you work on an icon panel definition.

3. When you finish reading the help text, press Enter.

   The Icon Panel Generator panel appears.

   If you selected one of the pre-defined defaults, go to Step 5.

   If you are defining a new icon panel, go to Step 4.

4. Complete the following fields:

   Name

   Specifies the name of the icon panel.

   Description

   Describes the icon panel.

5. Use the function keys to create or edit your panel. The left limit of the icon placement area is column 2, and the top limit of the icon placement area is row 5. The right and bottom limits are dependent on the size of your screen and the width and height of the icon.

6. Press F3 (File).

   The new icon panel is generated.

   Note: If an icon in the panel definition does not have an attached resource group, you cannot generate the new panel. A message is displayed on your screen to this effect. You can either attach any missing resource groups so that you can generate the panel or press F3 (File) again to file the definition without generating the panel.

Icon Panel Generator Panel

The Icon Panel Generator panel specifies the details of an icon panel. The operation you are performing is displayed at the top right of the panel.

The panel specifies the following information:

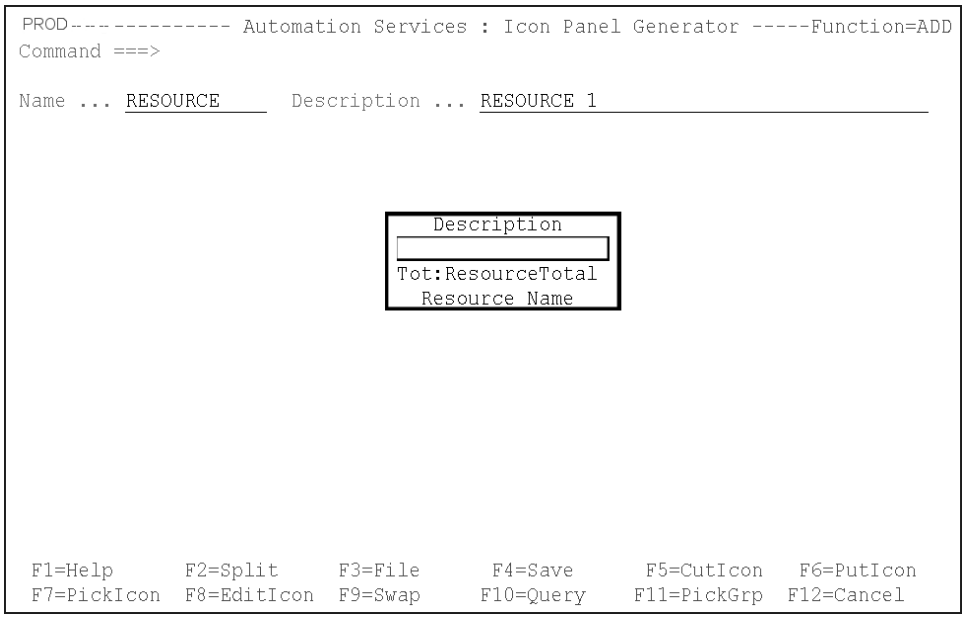
- Name and description of the icon panel
- Actual icon panel representation

The area from Column 2 to the right and from Row 5 down contains the icons you want to display on the graphical monitor.

Use the function keys on the Icon Panel Generator panel to specify what you want to display on the graphical monitor.

Example: Icon Panel Generator Panel

This example defines a panel with one icon.



Add an Icon to the Icon Panel

To build an icon panel for your graphical monitor, you add icons to the panel.

To add an icon to the icon panel

1. Move the cursor to fix the position of the top left corner of your icon. You must place the cursor in an area not already occupied by another icon.
2. Press F7 (PickIcon) to display the list of defined icons.

   The Icon List panel appears.
3. Enter **S** beside the icon you want to add to the icon panel.

   The Icon Panel Generator panel appears. The selected icon is positioned with its top left corner at the cursor.

   Note: After you pick an icon, you can move the cursor to another position and press F6 (PutIcon) to duplicate the icon on the icon panel. You can thus quickly position multiple icons with the same attributes on the panel.
4. Press F11 (PickGrp) to attach a resource group to the icon.

   The Resource Groups List panel appears.
5. Enter **S** beside the group you want to attach to the icon.

   The Icon Panel Generator panel appears. You have added an icon with an attached resource group to the icon panel.

Attach a Resource Group to an Icon on the Icon Panel

You can attach resource groups to icons on the Icon Panel Generator panel. You can change a resource group attachment by attaching another group to the icon.

To attach a resource group to an icon on the icon panel

1. Move the cursor in the icon to which you want to attach a resource group.
2. Press F11 (PickGrp).

   The Resource Groups List panel appears.
3. Enter **S** beside the group you want to attach to the icon.

   The Icon Panel Generator panel appears.

Duplicate an Icon on the Icon Panel

Note: Duplicating an icon on the icon panel copies only the icon, not the attached resource group.

To duplicate an icon on the icon panel

1. Move the cursor inside the icon you want to duplicate.
2. Press F7 (PickIcon).

   The icon is highlighted
3. Position the cursor to where you want to place a copy of the icon and press F6 (PutIcon).

   The icon is placed at the cursor.

   Note: The cursor position fixes the top left corner of the duplicate icon.

Move an Icon on the Icon Panel

To move an icon to another position on the icon panel

1. Move the cursor in the icon you want to move.
2. Press F5 (CutIcon).

   The selected icon is no longer displayed.
3. Move the cursor to fix the position of the top left corner of the icon being moved and press F6 (PutIcon).

   The icon appears at the position of the cursor.

Edit an Icon on the Icon Panel

You can edit an icon from the Icon Panel Generator panel. Editing enables you to update the original icon or create a new copy of the icon.

Updating an icon from the Icon Panel Generator panel updates the icon definition in the knowledge base and the selected icon only. If there are other icons in the panel definition that use the same icon definition, these other icons are not updated as long as you remain in the panel definition. You can, therefore, have several versions of the same icon in the panel definition. When you generate the icon panel, the panel reflects these different versions of the icon (even though there is only one version of the icon definition).

Note: Although a generated icon panel can retain different versions of the same icon, the icon panel definition cannot. The next time you access the panel definition, the definition reflects the latest version of the icon.

To edit an icon on the icon panel

1. Position the cursor in the icon you want to edit.
2. Press F8 (EditIcon).

   The Icon Editor panel appears.
3. Edit the icon, as required.

   Note: If you want to create a new copy of the icon, change the value in the Name field.
4. Press F3 (File).

   The updated definition is saved and the Icon Panel Generator panel appears.

Display Information About an Icon on the Icon Panel

You can display the name of and the resource group attached to an icon on the icon panel.

To display the information, press F10 (Query).

A message displays the required information.

The following example identifies the icon as CVNEW with an attached resource group named ACREC:

```
RM810017 ICON=CVNEW RESOURCE GROUP=ACREC
```

Delete an Icon from the Icon Panel

To delete an icon from the icon panel

1. Position the cursor in the icon you want to delete.
2. Press F5 (CutIcon).

   The selected icon is deleted.

   Note: The CutIcon action temporarily stores the icon that is removed from the icon panel; however, the icon is lost if you use the F7 (PickIcon) or F5 (CutIcon) function key on another icon.

Maintenance of Icon Panel Definitions

You can browse, update, copy, and delete icon panel definitions from the Icon Panel Definition List panel.

Note: You cannot update the definition of an icon panel that a graphical monitor is using.

If an icon in the panel definition does not have an attached resource group, you cannot generate the panel. A message is displayed on your screen to advise you of the fact. You can either attach any missing groups so that you can generate the panel or press F3 (File) again without generating the panel.

How You Edit a Generated Icon Panel

To update an icon panel, you can regenerate the panel by using an updated definition or you can edit the panel description file directly.

Enter the **/GADMIN.E** path to access the list of icon panels. The Panel List panel appears.

The panel displays the list of icon panels in the knowledge base. Some of these panels are generated using icon panel definitions; some of these panels are created by users (for example, by using the Copy or Rename action). If an icon panel definition generates the panel, the Name and Description columns reflect the name and description of the definition.

Consider the following when you edit an icon panel description file:

- If you regenerate an icon panel by using the P - Define Icon Panels option, you lose whatever editing you did in the description file. Use the R action to rename the panel before editing.
- The first line in a description file is the panel description, as displayed on the panel list.
- The #NOTE #ICON statement in a description file associates the specified resource groups with the icon panel.

Note: For information about panels and panel statements, see the *Network Control Language Programming Guide*.

Set Up Default Icon Panel for Your Users

You can add an icon panel to a user profile so that it is displayed automatically each time that user accesses the graphical monitor.

To add an icon panel to a user profile

1. Enter **/ASADMIN.UP** at the prompt.

   The User Profile List appears.

2. Select the user profile.

   The Panel Display List appears.

3. Select Graphical Monitor Profile.

   The Graphical Monitor Profile panel appears.

4. Complete the following field:

   Panel Name

   Specifies the name of the icon panel that you want to appear.

   Note: You can enter ? to display a selection list of icon panels.

5. Press F3 (File).

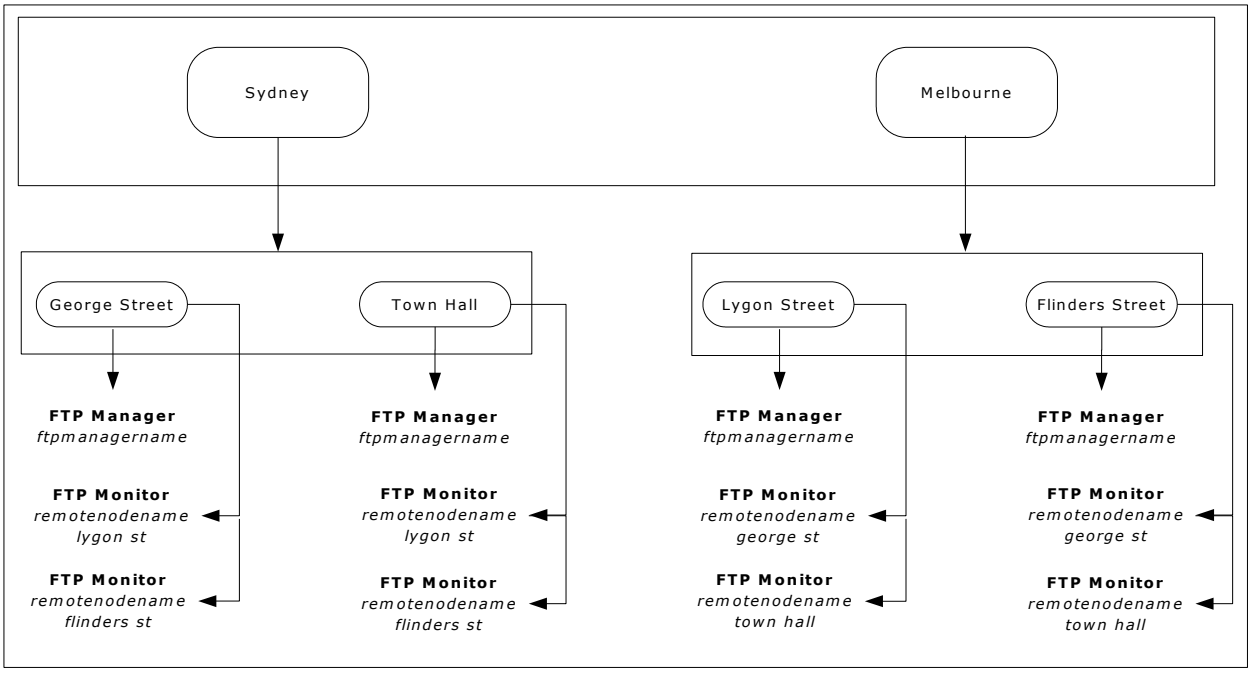
   The details are saved.

Example: Graphical Monitor Configuration

The Rich Bank provides banking services in Australia. In Sydney it has branches at George Street and Town Hall, and in Melbourne it has branches at Lygon Street and Flinders Street.

You want to monitor the file transfers between the Sydney and Melbourne offices.

The following diagram illustrates this structure:



To create this structure, you need the following:

- Two icon templates (which can be used for the six icons)
- six resource groups - one each for Sydney, Melbourne, and all of the branches
- Three icon panels

Chapter 19: Implementing Services

This section contains the following topics:

Services

A service is a collection of resources that support a business or operations function. After you have defined the resources, you group relevant resources in service definitions. You use service definitions to specify the service availability requirements of your organization.

Note: You can define and manage services from focal point regions only. Services are not visible in subordinate regions, but you can include resources managed by a subordinate region in a service.

Access Service Definitions

Service definitions are stored in the knowledge base in a structure similar to that of resource definitions. Service definitions belong to the service system image, $SERVICE. Version 0001 of this image is always active. The definitions have a class of SVC.

To access service definitions, enter **/SADMIN.S** at the prompt.

The ServiceView : Service List panel appears. The panel lists the services in the knowledge base.

Note: To assist with maintenance of your service definitions you can create backup versions of the $SERVICE 0001 service image.

Service Definition Panels

You can use variables as data in a service definition.

To add a service definition, press F4 (Add) from the Service List panel. A Service General Description panel appears. You define the service by entering data on the following panels:

Service General Description

You must complete this panel. The panel enables you to identify the service, specify the service operation mode, and define the availability requirements for the service.

Service Filters

Complete this panel. The panel enables you to select members for the service and specify how important a member is to the service.

State Thresholds

The panel enables you to define how the statuses of the service members affect the status of the service.

State Change Exits

The panel enables you to specify state change exit processes that are invoked if the service changes to a given state.

Automation Log Details

The panel enables you to change the logging requirements.

Owner Details

The panel enables you to identify up to two people who can be contacted if the service has operational problems.

Extended Function Exit

The panel enables you to specify an exit NCL procedure that can be used to extend the service functions provided in the region.

General Description

The Service General Description panel specifies the service name, the operation mode, a description of the service, and the availability map to apply.

Operation Modes

Specify an operation mode of AUTOMATED, IGNORED, MANUAL, OFF, or STARTAUTO. During operation, the global operation mode can restrict the mode specified in the Operation Mode field.

The operation modes have the following effects on a service:

AUTOMATED

Specifies that the region monitors and automates the control of the service.

When the desired state of the service is set to ACTIVE, the service places an ACTIVE desired state override on its members. The region then determines the actual state of the service from the actual states of the members.

When the desired state of the service is set to INACTIVE, the service removes the ACTIVE desired state overrides from its members. The service acquires an INACTIVE actual state immediately.

IGNORED or MANUAL

Specifies that the region monitors but relinquishes control of the service to the operators. A service in the IGNORED mode always appears green on your monitors.

When the desired state of the service is set to ACTIVE, the service does not place the ACTIVE desired state overrides on its members. The overrides occur only when an operator starts the service manually by using the A(ctivate) command.

Similarly, setting the desired state of the service to INACTIVE does not affect the members. The members are affected only when an operator stops the service manually by using the T(erminate) command.

OFF

Specifies that the region does not monitor or control the service. The definition remains in the knowledge base, but the service does not appear on your monitors.

STARTAUTO

Specifies that the region starts the service in the AUTOMATED mode. As the service achieves its desired state, the region switches the service to MANUAL mode.

Define the Availability of the Service

You can use an availability map to define the changes to the normal availability of the service.

In a multisystem environment, you specify a system as the service automation focal point system and the scheduled times refer to the local times on that system. If the map schedules the starting of processes, the processes are started in the region on that system only.

To attach an existing map, enter the name of the map in the Availability Map field. Press F10 (Edit Map) to update the timer details.

Leave the Availability Map field blank if you want to use the default desired state, which can be either ACTIVE or INACTIVE (as set in the AUTOIDS parameter group during region initialization).

The availability of a service overrides the availability of its members. If the service is always a member of another service, let the other service handle the availability of this service. Define the desired state of the service to be always inactive.

Note: You can create a new map from the service definition. You can name a new map and define it, or access an existing map, change the name, and update the copy. The map is created in the knowledge base when you save the definition.

Select Service Members

To select service members

1. From the General Description panel, press F8 (Forward).

   The Service Filters panel appears. This panel defines the filters that select the members of the service.

2. Define the filters by specifying the following criteria:

   - The service class (SVC, if the member is another service) or resource class in the Class field.
   - The name of the member in the Name field. You can use the following wildcard characters:
     - The underline character (_) represents a single character. For example, PROD_X3A matches PROD1X3A, PROD2X3A, …
     - The percent character (%) represents zero or more characters. For example, PROD%X3A matches PRODX3A, PROD1X3A, PROD2X3A, …
     - You can also use the asterisk (*) as a wildcard character. An asterisk behaves the same way as the % character, but you cannot have the * at the beginning of or embedded in the specified value. For example, * and PROD* are valid values.
   - The SMF ID of the system that owns the member in the SMF ID field. The default is the SMF ID of the local system.

     When you have resources with the same identification defined on different systems and you want to include all those resources as members, specify ***** in the SMF ID field.
   - The type of resource (as specified in the resource definition) in the Type field. You can use the asterisk (*) wildcard character by itself or at the end of the specified value.

     Note: The Type field is irrelevant for a service. Leave the value to the default.
   - A weight that indicates how important the member is to the service in the Weight field.
   - The type of weight in the Weight Type field.

   You can define up to 97 lines of members.

Weight of a Service Member

The weight indicates how important a member is to the service. The valid values are 0 percent through 100 percent.

If the weight is 100 percent, the actual state of the member affects the actual state of the service directly. For example, if the member fails, the service fails.

If the weight is 0 percent, the member has no effect on the service.

If the weight is between 0 percent and 100 percent, the effect of the member on the service depends on the state thresholds (see page 255).

You can apply the following types of weights to service members:

Fixed Weight

With a fixed weight, every member included in a line entry has the weight specified in the Weight field.

In the following examples, the weight is 100 percent fixed:

- If the line entry includes only one member (for example, the PRODA started task on the EASTTEST 0001 system), the member has 100 percent weighting.
- If the line entry includes more than one member (for example, the PRODA started tasks on all the connected systems (SMF ID=*)), each member has 100 percent weighting.

Proportional Weight

You can use the proportional type of weight when the line entry includes more than one member. With a proportional weight, every member included in the line entry has an equal proportion of the weight specified in the Weight field. For example, if the weight is 100 percent proportionally applied to two members, each member has 50 percent weighting in the service.

View the Service as Defined by the Service Filters

The service filters select the members for a service. Only members defined in active system images are selected. The members can change if the active system images change (for example, when a connected region has a different system image loaded).

To view the members in a service, press the F5 (Model) function key.

Merge Two Service Images

You can merge two service images and replace the active image with a backup version.

To merge service images $SERVICE 0002 and $SERVICE 0001

1. Enter **C** beside the $SERVICE 0002 on the ServiceView : Service Image List panel.

   The ServiceView : Service Image Definition panel appears.

2. Change the Database Version number to 0001and press F3 (File).

   The Confirm System Image Merge panel appears.

3. Enter **YES** in the input field if you want to overlay like-named components.

4. Press F6 (Confirm).

   The service images are merged.

State Thresholds

From the Service Filters panel, press F8 (Forward) to go to the State Thresholds panel. Use this panel to define how the actual states of the members affect the actual state of the service.

The actual state of a service can be *one* of the following:

- UNKNOWN
- FAILED
- ACTIVE
- STARTING
- DEGRADED

You must assign a threshold to the first four states.

Thresholds are evaluated in the order shown. The service takes on the state of the first threshold equaled or exceeded, irrespective of whether other thresholds are Equaled or exceeded. For each actual state, you specify a percentage threshold value that, if equaled or exceeded, causes the service to take on that state (unless a state of higher severity has also satisfied its threshold requirement). This threshold is expressed as a combined weight of the members required to deliver the service.

Each member of the service has a weight associated with it. The weight expresses the level of impact the individual resource has on the threshold calculation for the actual state of the service.

If members are not ACTIVE, you can use their logical state to calculate the threshold for the actual state of the service. In this case, if a member has a logical state of OK, its weight is added to the combined weight for the ACTIVE state. If a member has a logical state of UNKNOWN or STARTING, their weight is added to the combined weight for the corresponding actual state. If a member has any other logical state, their weight is added to the combined weight for the FAILED actual state.

Note: If a service filter finds no members, the weight specified in the Weight column on the Service Filters panel is added to the combined weight for the UNKNOWN state.

Using the logical state rather than the actual state to calculate the threshold has advantages. For example, you can shut down a resource that is part of a service without affecting the service. The service sees a logical state of OK, even though the resource is INACTIVE, and treats it as though it is ACTIVE. Alternatively, when a resource fails and you set it to IGNORED, the service sees the resource as ACTIVE (OK), and the service continues unaffected.

State Change Exits

From the State Thresholds panel, press F8 (Forward) to scroll forward to the State Change Exits panel. This panel lets you specify the following types of exit processes:

- A process that executes before the service is started. By using this feature, you can add your own preactivation tasks to the internal service starting method.
- Processes that execute on specified state changes. For example, if a service fails, you can invoke a procedure that writes a problem report. You can specify a process to execute on changes to the actual state, the desired state, or the logical state of the service.

In a multisystem environment, you can specify whether the processes are executed in a specific region only or in all connected regions.

Define the Logging Details

From the State Change Exits panel, press F8 (Forward) to scroll forward to the Automation Log Details Panel. This panel contains the following information:

- Size of the temporary log for the service (known as a *transient log*)
- Destination of the logged information
- Type of information logged

Owner Details

From the Automation Log Details panel, press F8 (Forward) to scroll forward to the Owner Details panel. This panel lets you identify up to two people who can be contacted if this service has operational problems.

Extended Function Exit

From the Owner Details panel, press F8 (Forward) to scroll forward to the Extended Function Exit panel. The panel lets you provide additional operator functions. Specify the exit NCL procedure that provides these functions. The procedure is invoked when an operator issues the XF command against the service.

The extended function exit NCL procedure has access to variables that contain all of the service details with the prefix ZRM.

Maintenance of Service Definitions

You can browse, update, copy, and delete service definitions from the Service List panel.

Note: If you only want to hide a service definition from the region, set the operation mode to OFF. The definition remains in the knowledge base but is not used.

Back Up Service Definitions

To assist you with the maintenance of your service definitions, you can create backup versions of your service image. By creating a backup version of your service image or definitions, you can perform the following:

- Update service definitions in any version of a service image
- Restore a service definition from a backup service image
- Merge two versions of a service image

To create a backup version of a service image

1. Enter **/SADMIN.SI** at the prompt.

   The service image list appears.

   Note: If you have not created a backup before, there is only one service image listed: $SERVICE 0001.The active service image can be $SERVICE 0001 only. $SERVICE 0001 cannot be deleted.

2. Enter **C** next to the service image you want to copy.

   The ServiceView : Service Image Definition panel appears.

3. Enter a new Database Version, Short Description, and (optionally) a Long Description.
4. Press F3 (File).

   A copy in progress panel opens while the copy occurs. The Service Image List appears with the backup version displayed in the list.

Update Service Definitions in a Backup Service Image

You can access a list of all the service definitions in any version of a service image. From this list you can update any service definitions contained in the service image.

To update a service definition in the $SERVICE 0002 backup image

1. Enter **L** (List Services) beside the $SERVICE 0002 service image in the Service Image List.

   The ServiceView : Service List panel appears showing the service definitions in that service image.

   Note: You can access the list of service definitions for another version of the service image by changing the version number on the Service Image List panel and pressing Enter.
2. Enter **U** beside the service definition that you want to update.

   The ServiceView : Panel Display List appears for that service definition.
3. Update the service definition, as required.
4. Press F3 (File) to save the changes.

   The ServiceView : Service List panel appears.

Restore a Service Definition from a Backup Service Image

If you have made changes to a service definition and you are having trouble with its implementation, you can restore it from a previous version of the definition.

To restore service definition SERV01 from $SERVICE 0002 service image to $SERVICE 0001

1. Enter **C** beside SERV01 in the ServiceView : Service List.

   The ServiceView : Service Image Definition panel appears.

2. Change the Database Version from 0002 to 0001 and press F3 (File).

   Because there is already a copy of the service in the target service image, the Confirm Copy Replace panel appears.

3. Press Enter to confirm the replace or F12 (Cancel) to cancel the request.

   The ServiceView : Service List panel appears.

Chapter 20: Producing Reports

This section contains the following topics:

About Reports

CA NetMaster FTM has a reporting function, which lets you view your file transfer activity from a historical perspective.

The reporting function lets you do the following:

- 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

Note: To enable CA NetMaster FTM to collect the events, you must configure them using the Initialization Parameters panel.

View Reports and Search the Database

The reporting options available from the History Menu let you view reports currently defined to your region. The following predefined reports are available:

- Event reports
  - All file transfer events (all START, END, and FAILURE events)
  - Failed file transfers (all FAILURE events)
  - File transfer results (all END and FAILURE events, but excluding those failures that were subsequently retried)
  - Summary reports (by Mailbox ID, Source Address, Target Address, Transfer ID, or User ID)
- Schedule reports
  - Completed schedules
  - Failed schedules

The search facility also lets you 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.

View Predefined Reports for File Transfer Events

To access file transfer event reports and searches

1. Enter **/FTHIST** at the command prompt.

   The History Data menu appears.

2. Enter **B** at the command prompt.

   A display list appears.

3. Enter **S** beside the predefined report type that you want.

   The corresponding type of report appears.

Note: You can sort events by a specific criterion by entering SORT and the sort criterion at the command prompt (does not apply to summary reports).

View Predefined Reports for Schedules

To access file transfer event reports and searches

1. Enter **/FTHIST**.

   The History Data menu appears.

2. Enter **BS** at the command prompt.

   A display list appears.

3. Enter **S** beside the predefined report type that you want.

   The corresponding type of report appears.

View Events Associated with a Schedule

To view the file transfer events associated with a particular schedule:

1. Enter **S** beside the required schedule.

   The File Transfer : File Transfer Events panel appears.

2. Enter **S** beside the required file transfer event.

   The details of the event appear.

View Filters Associated with a Schedule

To view the filters associated with a particular schedule

1. Enter **F** beside the required schedule.

   The File Transfer : File Filters panel appears.

2. Enter **S** beside the required filter.

   The file transfer events monitored by this filter are displayed.

3. Enter **S** beside the required file transfer event.

   The details of the event are displayed.

Generate Exception Reports

The File Transfer Exception Reporting option on the History Data menu lets you 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.

Define Exception Report Filters

To define an exception file filter:

1. Enter **/FTHIST.ER.F** at the command prompt.

   The Exception Report Filter List appears

   Note: You can also define exception report filters through the Administration Menu **(/FTADMIN.E**)

2. Press F4 (Add).

   The Exception Report Filter panel appears.

3. Complete the following fields:

   Name

   Specifies the name of the exception report filter.

   Description

   Briefly describes the filter.

   Specify the expected transfers in the Filter window. For more information, press F1 (Help).

   Note: Filters can be stored in a CTL file. You can view CTL files directly from Exception Report Filter panel.

   Press F3 (File).

   The exception file filter is saved to the knowledge base.

Generate Exception Reports

To generate an exception report:

1. Enter **/FTHIST.ER** at the command prompt.

   The Exception Reporting Menu appears.

2. Select *one* of the following options:

   F

   Lists exception report filters.

   S

   Lists FTSCHD file filters.

3. Enter **E** beside the appropriate filter.

   The Exception Report Confirmation panel appears.

4. Enter the appropriate time period and press F6 (Confirm) to generate the report.

   An exception report is generated only if the expected events are not found in the events database.

Search 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:

- Search File Transfers
- Search Schedules
- Perform Custom Search

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 from the Search Criteria panel. You can save multiple search criteria and retrieve them later for use.

Search for File Transfer Events

To search for file transfer events

1. Enter **/FTHIST.B** at the command prompt.

   A selection list of reports and searches appears.

2. Select Search File Transfers.

   The Search Criteria panel appears.

3. Do *one* of the following:

   - Enter your search criteria. For information about the fields, press F1 (Help).
   - Press F5 (Load) to retrieve previously saved criteria.

4. Press F6 (Action).

   The File Transfer : File Transfer Search panel appears.

   Note: The report on this panel is in the same format as that on the File Transfer : All Events panel.

Search for File Transfer Schedules

To search for file transfer schedules

1. Enter **/FTHIST.BS** at the command prompt.

   A selection list of reports and searches appears.

2. Select Search Schedules from the selection list of reports.

   The Search Criteria panel appears.

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.

   Press F1 (Help) for information about any of these fields.

4. Press F6 to start the search.

   The File Transfer : Schedules Search Result panel appears.

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.

Perform a Custom Search

The Perform Custom Search option lets you define your own search criteria by using the fields in the events database.

Note: The following fields are case-sensitive:

- $RFFAILDESC
- $RFSRCADDR
- $RFSRCFNAME
- $RFTGTADDR
- $RFTGTFNAME
- $RFUSER
- $RFXFRID

To search for file transfer events by specifying your own search criteria

1. Select Perform Custom Search from the File Transfer : Display List.

   The Network Database : Search Criteria panel appears.

2. Complete the columns for as many criteria as you need, or press F5 (Load) to retrieve previously saved criteria. For information about the actions available on this panel, press F1 (Help).

   Note: List the fields in the events database by entering **?** in the Field field. The format of the valid values for these fields can be found in an off-loaded CSV archive of the events database.

3. Press F6 (Action).

   The File Transfer : EVNTDB Search panel appears.

   Note: The report on this panel is in the same format as that on the File Transfer : All Events panel.

4. Press F4 (Save).

   The data is saved.

Print Reports

The reporting options let you print reports currently defined to your region.

Generating a printed report may consume a lot of CPU resources. Where possible, perform this action when the system is not busy.

Print Reports for File Transfer Events

To display a list of predefined reports and print a selected report for file transfer events:

1. Enter **/FTHIST** at the command prompt.

   The History Data menu appears.

2. Select **P**.

   The Reports List appears.

3. Enter **S** beside the listed report that you want to print.

   The PSM : Confirm Printer panel appears.

4. Press F6 (Confirm) to confirm the details of the print job.

   The Reports List appears. A message also appears indicating that the print job was submitted to the print queue.

Print Reports for File Transfer Schedules

To display a list of predefined reports and print a selected report for file transfer schedules

1. Enter **/FTHIST** at the command prompt.

   The History Data menu appears.

2. Select **PS**.

   The Reports List appears.

3. Enter **S** beside the listed report that you want to print.

   The PSM : Confirm Printer panel appears.

4. Press F6 (Confirm) to confirm the details of the print job.

   The Reports List appears. A message also appears indicating that the print job was submitted to the print queue.

Check the Print Queue

To check the print queue

1. Enter **/FTHIST** at the command prompt.

   The History Data menu appears.

2. Enter **PQ**.

   The PSM : Output Queue appears.

3. Select the required action to browse a report output, release a held report, or delete a print job from the printer queue.

Extract 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. Your system administrator defines the period of time that data is kept online.

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 for analysis

1. Allocate a sequential data set with the following attributes:

Attribute	Value
RECFM	VB
LRECL	600
BLKSIZE	Greater than or equal to 604

2. Enter **/FTHIST** at the command prompt.

   The History Data menu appears.

3. Enter **EX** at the prompt and specify the data set name that you have just defined in the Extract Dataset field.

   The Extracts List appears.

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
File transfers based on entry fields for predefined search criteria	Search and Extract File Transfers

   The Fields List appears.

   Note: By default, all fields are selected.

5. Do *one* of the following*:*

   - Enter **U** beside the fields you want to exclude from the extract.
   - Enter **All U** at the command prompt to deselect all fields, 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.

6. Press F6 (Action).

   The system extracts the relevant records from the events database, EVNTDB, to the defined data set, and presents them as CSV fields with a header.

7. Transfer the defined data set to your PC, and save it with a .TXT extension.
8. Open the .TXT file by using your preferred PC application (for example, Microsoft Excel), and import this file as a .CSV file.
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.

Define Printed Reports

To set up your own reports to print, you must define them to the CA NetMaster FTM region.

There are two possible stages involved in defining these reports:

- Defining search criteria (optional)
- Defining report details

Define Search Criteria (Optional)

To define specific search criteria in addition to those available on the Report Writer : Report Description panel

1. Enter **/CASCRIT** at the command prompt.

   The CAS : Criteria Definition List appears.

2. Define your search criteria. For more information, press F1 (Help) for online help.
3. Press F3 (File).

   Your criteria are saved.

Define Report Details

To define your report details

1. Enter **/RWDEFN.L;$RF** at the command prompt.

   All defined reports appear on the Report Writer : Report Definition List.

2. Enter **C** beside a listed report that has a format similar to the report you want to set up.

   The Report Writer : Report Description panel appears.

3. Complete the following fields:

   Report Name

   Specifies your own report name.

   Description

   Describes your report.

   Note: To make the report you are setting up available, ensure that the Group field has the value $RFREPORTING. Also ensure that the Report Exit field has the value $RFLORWX.

   (Optional) If you have defined any specific search criteria, enter your values in the Criteria fields.

   Press F3 (File).

   The Report Writer : Report Definition Component Menu appears, with a message that your report has been added.

4. Select **RH** from the Report Writer : Report Definition Component Menu.

   The Report Writer : Edit Report Header Layout panel appears.

5. Edit the header, as required, and press F3 (File).

   The Report Writer : Report Definition Component Menu appears, with a message that your header has been updated.

6. Press F3 (Exit) until the Report Writer : Report Definition Menu appears.

7. Select **R** .

   The new definition is activated.

Troubleshoot the Reporting Facility

The reporting facility is dependent on the events database, EVNTDB. It cannot operate if the following conditions apply:

- The EVNTDB database has not been allocated.
- The EVNTDB database is full.

In either case an error message appears.

If the EVNTDB Database Is Not Allocated

If the error message says that the EVNTDB database is not allocated, then you need to allocate this database before reselecting a reporting option.

If the EVNTDB Database Is Full

If the error message says that logging has stopped, the EVNTDB database may be full. If automatic reorganization is not set, complete the following steps:

1. Check the activity log (**=H.L**) for more messages about what is happening.
2. Extract the data currently in the EVNTDB database.
3. If the EVNTDB database is full, delete and redefine the EVNTDB database.

Note: For information about how to perform these steps, see the message help.

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.

Fix a Failed Reorganization by Using a Batch Job

To fix a failed reorganization using a batch job

1. Determine the phase of the reorganization when the failure occurred.
2. Issue the following command:

   DEALLOC DD=EVNTDB

   If the failure occurred during the UNLOAD phase, complete step 3; otherwise, skip this step and go to step 4.
3. (Optional) Submit a batch job that executes an IDCAMS REPRO, for example:

   REPRO INDATASET(EVNTDB dataset name) OUTDATASET(Reorg dataset name)

   Note: Allocate enough space for the REORG data set to contain all the records from the EVNTDB.
4. Submit a batch job to define a new EVNTDB database (optionally giving it more space).
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)
   ```
6. Update the EVENTLOG parameter group from the Customization Parameters panel (**/PARMS**) specifying the following parameters:

   Enable Event Logging

   Enter **YES.**

   EVNTDB Database Name

   Enter the EVNTDB data set name used in step 5.

   EVNTSEQ Reorg Dataset

   Leave blank.
7. Press F6 (Action).

   The changes are applied.
8. (Optional) If you require automatic reorganization, specify a data set name in the EVNTSEQ Reorg Dataset field and press F3 (File).

   The parameter settings are saved.

Fix a Failed Reorganization via the EVENTLOG Parameter Group

To fix a failed reorganization using the EVENTLOG parameter group

1. Determine the phase of the reorganization when the failure occurred.

   If the failure occurred during the UNLOAD phase, complete step 2; otherwise, go to step 3.

2. Update the EVENTLOG parameter group from the Customization Parameters panel **(/PARMS**) specifying the following parameters:

   Enable Event Logging

   Enter **NO**.

   EVNTDB Database Name

   Enter the EVNTDB data set name.

   EVNTSEQ Reorg Dataset

   Enter the EVNTSEQ data set name.

   Note: Allocate enough space for the reorganization data set to contain all the records from the EVNTDB database.

3. Press F6 (Action).

   The EVNTDB database is unloaded to the EVNTSEQ reorganization data set.

4. Submit a batch job to define a new EVNTDB database (optionally giving it more space).

5. Update the EVENTLOG parameter group from the Customization Parameters panel **(/PARMS**) specifying the following parameters:

   Enable Event Logging

   Enter **YES**.

   EVNTDB Database Name

   Enter the new EVNTDB data set name defined in step 4.

   EVNTSEQ Reorg Dataset

   Enter the ENVTSEQ data set name from the UNLOAD phase.

6. Press F6 (Action).

   The changes are applied.

7. Press F3 (File).

   The current parameter settings are saved.

Chapter 21: Implementing EventView

This section contains the following topics:

EventView

EventView performs automation at the event level. It provides event level automation and control, and can handle timed events.

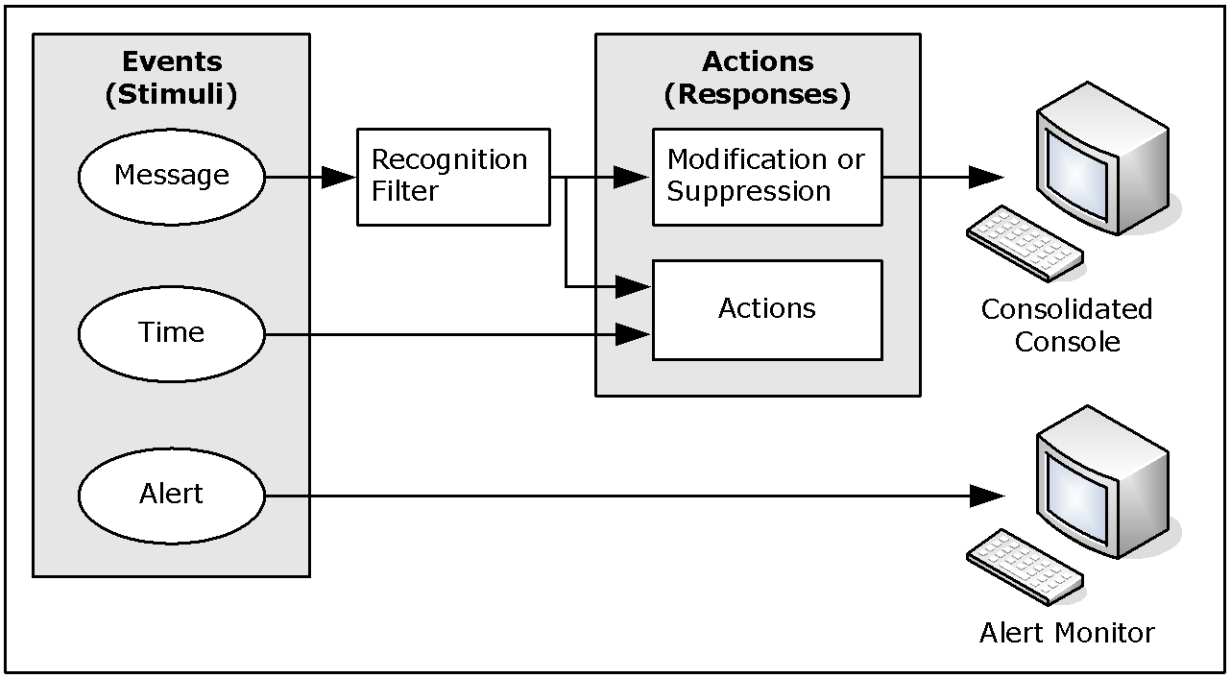
Successful event management relies on the recognition of significant events from the mass of messages generated by a system and the appropriate responses to these events.

EventView Functions

EventView provides the following functions:

- Event-based automation, which relies on the following:
  - The creation of appropriate rules and rule sets
  - The processing of messages
  - The processing of EventView timers
  - Message generation
- Console message consolidation
- Alert generation

The following illustration shows how EventView works.



Event-based Automation

You can define event rules to do the following:

- Suppress messages
- Change message text
- Enhance message presentation (for example, highlighting)
- Set route and descriptor codes
- Perform actions

Rules are grouped logically into rule sets, which define how an event is processed and what actions are taken in response to an event that is *not* related to a resource. (Resource-based events are handled by ResourceView.) An event can be a message or a specified time.

Sample Message Suppression Rule Sets

EventView provides the following samples of message suppression rule sets:

- AGRSUPP, which is based on the aggressive list of suppressible messages recommended by IBM
- CONSUPP, which is based on the conservative list of suppressible messages recommended by IBM

Note: For the IBM recommended lists, see IBM's *MVS Initialization and Tuning Reference* guide.

Console Message Consolidation

You can monitor message flows from multiple systems on a single screen—the consolidated console. Console consolidation controls the way you see messages on the console. In addition, messages displayed on the consolidated console are affected by EventView processing.

For example, message text and message presentation can be modified by EventView, and the consolidated console user sees the modified message. If EventView suppresses a message, that message is not displayed on the consolidated console.

You can define message profiles that customize the view of the message flow. Different users can have different sets of message profiles to suit the functions they perform.

Message profiles enable the meaningful grouping of messages based on criteria such as system, message ID, job name, and system codes.

Benefits of Using EventView

EventView benefits your organization in the following ways:

- Reduces system console message rates; you can filter messages received and suppress unwanted messages
- Produces a standardized response to events or problems
- Enables you to schedule actions to occur at specific times or at regular intervals
- Gathers useful statistics for messages and timers
- Able to learn messages
- Enables you to monitor message flows to multiple consoles on a single screen
- Enables you to generate alerts to remind operators of significant events

Message Monitoring

Besides responding to resource status, you need to respond to events not handled by resource automation.

The Automation Services components that affect message display are the EventView message rules and the console message consolidation facility. To use the latter facility, you define message profiles.

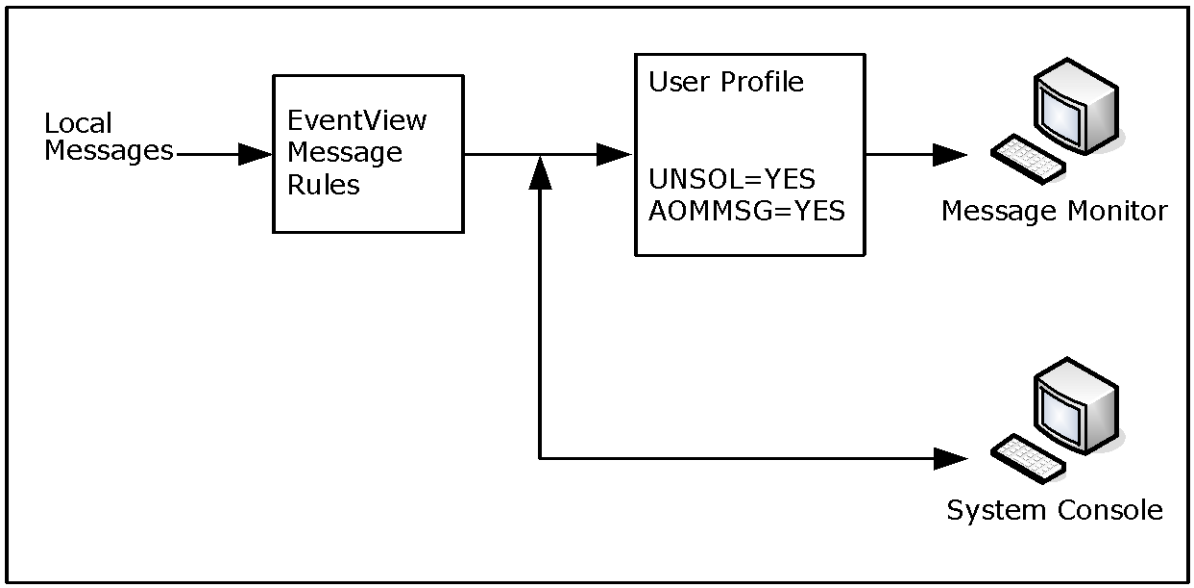
Typically, you use both components and you can monitor messages from multiple systems. However, if you do not want to define message profiles, you can disable the message consolidation facility. In this case, only messages from the local system can be monitored. You control the availability of the facility by using the CCONSOLIDATN parameter group.

Note: For more information about parameter groups, see the *Reference Guide*.

Console Consolidation Disabled

Without the console consolidation facility, you are able to monitor local messages only. Remote messages are not routed to this region, and messages from this system are not routed to remote regions.

The following illustration shows how messages arrive at the message monitor.

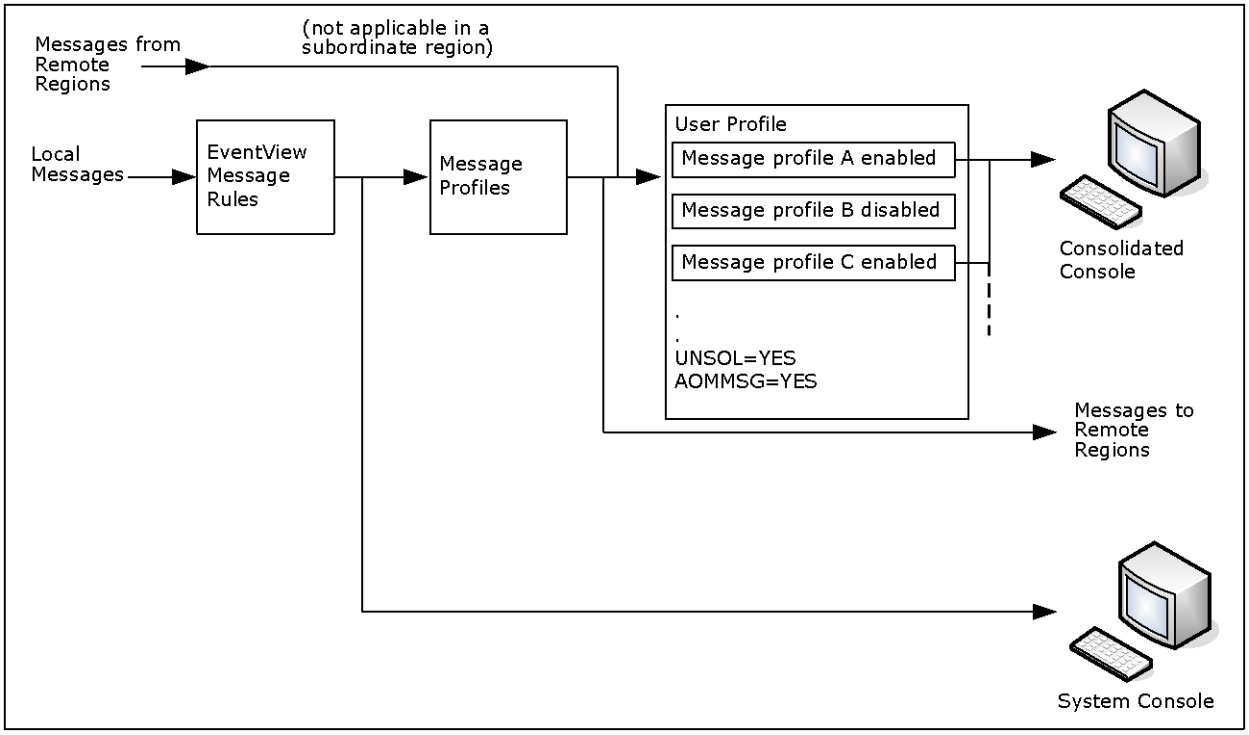


Console Consolidation Enabled

With message consolidation enabled, the message monitor becomes a consolidated console. Using the console consolidation facility, an operator is able to monitor messages from one or more systems on the consolidated console.

You use EventView message rules to preprocess the messages, for example, suppressing or highlighting the messages. You can then use message profiles to select the type of processed information to display on the consolidated console. For example, you can define a message profile that selects messages from a particular system. You can selectively enable profiles to customize the view of monitored events, for example, VTAM messages only.

The following illustration shows how messages arrive at the consolidated console.



How You Implement Message Profiles

Typical stages in implementing message profiles are as follows:

1. Analyze the message flow and the operations tasks to determine the different message views that are required.
2. Create EventView rules to suppress unwanted messages.
3. Create the message profiles, and assign each operator the appropriate message profile IDs in the user definition and user profile.
4. Activate the message profiles.

Alert Generation

Alerts are displayed on the alert monitor. Alerts can be generated from EventView rules. Generate alerts through user-defined processes by using the following macros:

- GENALERT enables a process to generate an alert of a specified severity.
- DELALERT enables a process to remove an alert from the alert monitor.

Use alerts to warn operators of significant events (for example, reminding the operator to perform tasks that cannot be automated).

Chapter 22: Implementing EventView Rule Sets

This section contains the following topics:

EventView Rule Sets

EventView rule sets consist of various members that define how an event is processed and what actions are taken in response to the event. An EventView rule set can include the following:

- Initial actions
- Message rules
- Message group rules
- Timer rules
- Other rule sets

You can create an EventView rule set for each area of responsibility. For example, you can create a CICS rule set, a VTAM rule set, and so on, to organize your rules in logical and manageable groups.

Note: Specify automation that deals with the status of resources in the resource definition, *not* in a message rule.

To activate an EventView rule set, it must be associated with an active system image.

Note: For information about system images, see the *Reference Guide.*

Only one EventView rule set, known as the primary rule set, is associated with a system image. If you want to activate more than one EventView rule set, include the other rule sets in the rule set associated with the active image. For example, you could create a master EventView rule set into which all other EventView rule sets are included.

Add an EventView Rule Set

You must add an EventView rule set before you can add the associated members.

To add an EventView rule set

1. Enter **/EADMIN.R.R** at the prompt.

   The Ruleset List panel appears.

2. Press F4 (Add).

   The Ruleset Description panel appears.

3. Complete the panel, adding comments on the Comments panel if required. See the online help for field descriptions.

   Note: An EventView rule set can be activated only if it has an ACTIVE status.

Specify Control Options for Testing

The control options for the primary EventView rule set override those options specified for the included EventView rule sets.

When setting up an EventView rule set, you can test it without actually triggering any rules.

To set up a rule set for testing, specify the following values:

- **NO** for the Perform Message Modification? and Perform Action? options
- **YES** for the Log Ruleset Activity? option

You can then see from the entries in the general activity log (marked as TEST) what activity would take place if the EventView rule set was, in reality, working as intended.

Example: Messages Logged in Test Mode

This example shows some messages logged in test mode.

```
09.04.49 RE0113 RULESET ACTIVITY LOGGING STARTED
09.04.58 RE0130 (TEST) RULE FOR TESTMSG SET ATTRIBUTES: DELIVER=NO
09.05.12 RE0114 RULESET ACTIVITY LOGGING STOPPED
```

Monitor EventView Rule Set Status

To view the status of the active EventView rule set and all its included rule sets on the current system, enter **/EADMIN.S.R** at the prompt.

The EventView : Ruleset Status panel appears. This panel displays the same information as the Ruleset Description panel, plus it lists loaded EventView rule sets. The primary EventView rule set is the first EventView rule set listed, followed by its included EventView rule sets. Each level of further inclusion is indicated by indentation.

Note: If an EventView rule set has a status of inactive, its included EventView rule sets are not processed.

Statistics

If you specify YES in the Collect Statistics? field on the Ruleset Description panel, then EventView collects statistics relating to messages received and timer schedule items executed. You can use these statistics to measure the effectiveness of your EventView rules.

If the SMFDATA region parameters are configured, the statistics are output to SMF at a user-defined interval.

Note: For information about the SMF record format, see the *Reference Guide*.

Change the EventView Rule Set Associated with a Local System Image

You can change the EventView rule set associated with a local system image. Update the EventView Ruleset to Activate field on the System Image Definition panel.

Note: The associated rule set is activated when the system image is loaded initially. If you change the rule set associated with the system image later, you do not have to reload the system image. The rule set takes effect immediately when the system image definition is saved.

To change the EventView rule set associated with a local system image

1. Enter **/RADMIN.I.L** at the prompt.

   The Local System Image List appears.

2. Enter **U** (Update) next to the system image that you want to update.

   The Local System Image Definition panel appears.

3. Enter the new EventView rule set name in the EventView Ruleset to Activate field.

   Note: You can select an EventView rule set from the prompted field value list.

4. Press F3 (File).

   The updated record is saved.

   Note: By default, EventView rule actions are not executed if the system image is operating in the MANUAL global operation mode. The actions, however, can be enabled by using the Perform Action in Manual Mode? field of the AUTOIDS region parameter group.

Add Associated Rules

After you have created an EventView rule set, you can add associated message, message group, or timer rules.

To add a rule

1. From the Ruleset List, apply the appropriate action, such as **M** (Message List), to the EventView rule set with which you want to associate the new rule.
2. Press F4 (Add).
3. Complete the fields on the initial panel displayed, and on any subsequent panels as required. Press F1 (Help) for help about the fields.

Message Rules

Message rules contain some or all of the following information:

- Message text and filtering criteria
- Message delivery and suppression details
- Required message modification details
- Which actions a message triggers
- Which message groups the current message rule is related to
- User-defined EventView variables

How You Add Message Rules

Message rules are added (see page 289) in the same way as other EventView rule set members. You apply the **M** (Message List) action to the EventView rule set with which you want to associate the new message rule.

Important! Message Text is a mandatory field. If you enter the wildcard character in this field, *all* messages are tested against this rule, which can degrade performance.

Message Execution Conditions

You can specify execution conditions (see page 319). The rule executes only if all of the given conditions apply.

Message Groups

If a message on its own is not significant, but another message increases its significance, create a message group to associate these messages.

Note: The order in which the grouped messages occur is not important, as long as all arrive in the specified time interval.

Message group rules contain the following information:

- The maximum time interval in which all messages in the group must be received, to trigger the rule
- Message text for up to ten messages, on the Message Group Details panel (displayed automatically when a message is associated with a message group (see page 290))
- The text of a message to issue if the group rule is triggered, and where and how to display this message
- The action or actions to perform when a group rule is triggered
- User-defined EventView variables, which you can set to the specified values before or after other rule actions

How You Add Message Group Rules

Message group rules are added in the same way as other EventView rule set members. You apply the **G** (Group) action to the EventView rule set with which you want to associate the new message group.

Associate Message Rules with Message Group Rules

To establish a relationship between a message rule and a message group rule, you must add an entry on the Related Message Group panel (the fifth panel in the sequence of Message Rule panel). The message rule is in turn added on the Message Group Details panel of the message group rule definition. The same message rule can be associated with up to five message group rules.

To associate a message rule with a message group rule

1. Enter **5** from within the message rule definition, for example:

```
PROD----------------- EventView : Message Filter ---------------------TAPEMON
Command ===> 5                                                Function=UPDATE

Ruleset Name ........ TAPEMON                       Rule Status ...+ ACTIVE__
Short Description ... Mount request processing_____

. Expected Message ------------------------------------------------------------.
|                                        S=ListPanels EV=ExtFilter TV=TestVars |
|      Message Text  ( WildChar = * )                                   ExtFlt |
| ___  IEC501A                                                          NO     |
'-------------------------------------------------------------------------------'
```

   The Related Message Group panel appears.

2. Add the message group rule. Optionally, specify a correlation key for precise recognition purposes.

   The following panel shows an example:

```
PROD---------------- EventView : IEC501A Related Message Group ---------TAPEMON
Command ===>                                                  Function=UPDATE

. Message Group Table ---------------------------------------------------------.
|                                                                              |
| MsgGroupID   CorrelationKey                                                  |
| GROUP1_____ &ZMSGJOBNM_____________________________________________________ |
```

3. Press F3 (File).

   The message rule is updated and added to the message group rule definition, for example:

```
PROD---------------- EventView : Message Group Details -----------------TAPEMON
Command ===>                                                  Function=UPDATE

Ruleset Name ......... TAPEMON
Message Group Name ... GROUP1                       Rule Status ...+ ACTIVE__
Short Description .... Tape mount group_____________
Interval ............. 00.10.00

. Expected Message ------------------------------------------------------------.
|                                                      S/B=Browse U=Update     |
|      Message Rule Text                                                       |
| ___ IEC501A                                                                  |
| ___ IEC509A                                                                  |
| ___                                                                          |
```

The correlation key enables one message group rule to cover numerous different situations, saving you from having to create numerous different rules. The rule is not triggered unless the values of the correlation keys in each of the grouped messages match.

For example, the correlation key as shown in the example, is the name of the variable that contains the job name. The group rule is triggered only if the messages associated with the group:

- All arrived in the specified interval (10 minutes)
- Were all generated by the same job

Timers

If you want a rule triggered on a particular day of the week (or year) and at a particular time, you need to add a timer rule. Timer rules contain the following information:

- Whether the timer rule applies to a specific system
- Up to 99 detailed schedule items
- Which actions are triggered by a timer
- User-defined EventView variables

How You Add Timers

Timer rules are added (see page 289) in the same way as other EventView rule set members. You apply the **T** (Timer) action to the EventView rule set with which you want to associate the new timer.

Initial Actions

Initial actions are actions performed when an EventView rule set is activated (that is, when the associated system image becomes active), and before message processing commences.

How You Add Initial Actions

You add initial actions from the Ruleset List by applying the **IA** (Initial Actions) action to the nominated EventView rule set.

Set variables that are essential to the functioning of an EventView rule set in the initial action rules.

Note: If an EventView rule set has associated included EventView rule sets, the initial actions specified for those EventView rule sets are also performed when the primary EventView rule set becomes active.

If you want to set any EventView variables before or after any of the initial actions are performed (to pass parameter values, for example), press F8 (Forward) to go to the Set Variables panel.

On the Set Variables panel, you supply a name for each EventView variable that you want to set, plus the required variable value. When you use the variable subsequently, you prefix the name with &ZREV, which is the EventView variable identifier.

Example: Log Rule Set Activation Message

This example logs a message to indicate that an EventView rule set is activated.

```
PROD------------------- EventView : Initial Action ----------------------BACKUP
Command ===> forward                                            Function=UPDATE

Ruleset Name ........ BACKUP
Initial Action Name   NOTIFY                          Rule Status ...+ ACTIVE
Short Description ... Log a startup message

System Command ... ____________________________________________________________
                   ____________________________________________________________
MS Command .......... LOG RULESET BACKUP IS NOW ACTIVE
```

How Initial Actions Are Executed

When an EventView rule set is activated, the associated initial actions are executed. When you load a system image that contains an EventView rule set that is already active, the region does not reactivate that EventView rule set and the associated initial actions are not executed (for example, when you switch images that use the same EventView rule set).

If you have several system images that use the same EventView rule set and you want the initial actions associated with the EventView rule set executed every time you load one of those images, you can create a primary EventView rule set for each of the images. Each primary EventView rule set includes the actual EventView rule set you want. Because the primary EventView rule sets are different, it is activated every time you switch between the images, thus executing the initial actions.

Include EventView Rule Sets in Other Rule Sets

To include an EventView rule set in another rule set

1. From the Ruleset List, apply the **IR** (Include) action to the EventView rule set in which you want to include another EventView rule set.

   The Include Ruleset List appears. This list is blank if there is no EventView rule sets included in the current EventView rule set.

2. Press F4 (Add).

   The Eligible Ruleset List appears.

3. Select the EventView rule set to include in the current EventView rule set.

   The selected EventView rule set is added to the Included Ruleset List for the current EventView rule set. This means that the included EventView rule set is active when the parent EventView rule set is active.

Note: Only the control options of the EventView rule set associated to the system image are used. The control options of included rule sets are ignored.

Maintenance of EventView Rule Sets

You can browse, update, copy, and delete EventView rule set definitions from the Ruleset List panel.

The C and the D action codes enable you to copy and to delete an *entire* EventView rule set. To copy or delete the EventView rule set definition only, use the CO or DO action codes. You can use the DO action code to delete an EventView rule set only if it is empty—that is, it contains no rules.

EventView Variables

The ability to set and use EventView variables in rules lets you create dynamic rules that depend on conditions identified by other rules and EventView rule sets. That is, you use EventView variables to control rule execution.

EventView variables can be used for the following:

- To pass information and data between rules
- To obtain more information about the environment in which the rule is executing
- To record system states

EventView variables can be set on the Set Variables panel of a message rule, a timer rule, or a group rule. Here, you can set values for up to six variables. These values can be literal or you can specify a substitution variable as the source of the variable value for a message rule.

EventView variables can be used by:

- *Rules*, to do the following:
  - Provide a correlation key value to match on the Message Delivery panel and the Related Message Group panel.
  - Provide a value for insertion in replacement text. Replacement text specified on the Message Modification, Set Variables and Test Variables panels can include EventView variable names.
- *Processes*, where the macros EVVARGET and EVVARSET can be used to get and set the values of EventView variables. Variable names can be specified in the Parameters field on the Rule Action panel, as well as on other panels where processes are invoked (see page 213).
- *NCL procedures*, where the $RECALL application program interface (API) can be used to get and set the values of EventView variables. For more information about $RECALL API, see the *Reference Guide*.

You must remember to add the EventView variable indicator prefix, &ZREV, to a variable name when it is specified for evaluation.

View EventView Variables

To view all EventView variables that have been set, enter **/EADMIN.S.V** at the prompt.

The EventView : Active Variables panel appears.

Chapter 23: Configuring Timers

This section contains the following topics:

Timer Rules

A timer rule enables you to schedule an action or actions to perform at a specific time or times of the day, week, month, or year.

A timer rule contains the following information:

- The action or actions to perform
- A schedule that defines when the action or actions are performed
- Whether catchup is required, if the system running the timer is unavailable when the timer is due to be activated

A timer schedule is similar to the availability map used by resources controlled by the region. You can specify up to 99 schedule items per timer rule, each containing the following information:

- The day of the week, date, and time when the action or actions are performed
- Whether the action or actions are performed once only, or at regular intervals during a given time period

Add Timers

If you want to add a timer rule that is very similar to an existing one, you can save yourself having to retype details by copying the existing timer and updating the copy as appropriate.

To add a timer rule

1. Enter **/EADMIN.R**.

   The Define Event Rules panel appears.

2. Type **T** at the prompt and complete the following field:

   Ruleset

   Specifies the name of the rule set with which you want to associate the timer rule.

   Press Enter.

   The Timer Rule List for the specified rule set appears.

3. Press F4 (Add).

   The Timer Description panel appears.

4. Complete the fields on this and subsequent timer rule panels, as required.

   Note: For more information, press F1 (Help).

   Note: If you enter YES in the Delete on Expiry? field, schedule items that have a full date specified are deleted when they pass their expiry date and time.

Note: You can also add or update timers from the Active Timer Display List (**/EADMIN.S.T**).

How Catchup Works

When you define a timer, you specify whether catchup is required if a region running the timer is unavailable when the timer is due to be activated.

Note that if you enter YES in the Catchup Required? field on the Timer Schedule panel, catchup applies to all schedule items entered for this timer.

- If you specify YES, then the scheduled action or actions are performed when the region becomes available, provided that the time specified in the Window field has not elapsed, with the exception of the situation noted below.
- If you specify NO, no belated processing occurs for that timer.

Note: In the case of timers that define actions that are repeated, catchup can be requested. If the specified end time has passed by the time the region running the timer becomes available, the specified action or actions are still performed once. If the region running the timer becomes available part way through the specified time period, the specified action or actions continue at the specified intervals until the specified end time.

Catchup Window

If you specify that catchup is required, you can identify the window in which catchup is performed. You can specify a value between one minute and 24 hours. If the region running the timer becomes available before the catchup window ends, catchup is performed.

Timer Schedule Items

You can enter up to 99 schedule items for a timer. Enter schedule details according to the following definitions:

Day

Specifies the days of the week when the timer is activated. As well as the abbreviated versions, you can enter shorthand values asterisk (*), W/D, or W/E in this field. If an asterisk is entered, an individual schedule item is created for each of the seven days of the week, with all other values duplicated. If you enter W/D, an individual schedule item is created for each of the five working days of the week. Entering W/E results in the creation of individual schedule items for Saturday and Sunday.

Note: The validation procedure does not accept a value in both the Day and the Date fields; enter a value in one of these fields only.

Date

Specifies the date when the timer is activated. If you specify a numeric value between 1 and 31 in this field, the timer is activated on that day of the month each month. For example, if you specify 1, it is activated on the first day of each month. If, in addition to specifying a day, you also specify the first three characters of a month in the format *dd-mmm*, the timer is activated on that day of that month each year. If, in addition to specifying a day and a month, you also specify a four-character year value in the format *dd-mmm-yyyy*, the timer is activated on that day of that month and that year. If you entered YES in the Delete on Expiry? field, schedule items that have a full date specified are purged after execution.

Time

Specifies the time when the action or actions associated with the timer are performed or, if the Every field also contains a value, the time when the action or actions associated with the timer are first performed.

Every

Specifies the period if you want the action or actions associated with the timer performed at regular intervals. If you enter a value in this field, you must also enter a value in either the Num or the End Time field. When you complete one of these fields, the other is calculated automatically when validation occurs.

The first time the action or actions associated with the timer are performed is specified in the Time field—see the preceding field description. To calculate the time when the second occurrence of the action or actions associated with the timer are performed, the value in the Every field is added to the value in the Time field, and so on.

Num

Specifies the number of times that the action or actions associated with the timer are performed. When you enter a value in this field, the value in the End Time field is automatically calculated.

End Time

Specifies the last permissible time when the regular action or actions associated with the timer are performed. When you enter a value in this field, the value in the Num field is automatically calculated.

Status

Specifies the status of a timer schedule item: ACTIVE or INACTIVE. You can disable an individual timer schedule item by changing the status of that item from ACTIVE to INACTIVE.

Add Further Schedule Items

When you have completed the first seven entry lines on the static list displayed initially, you can add further schedule items.

To add further schedule items

1. Press F10 (Scrllst).

   Note: If you are using a 24-line screen, you can type MAX at the prompt to maximize screen use and to display the schedule list only.

2. To add a line to the schedule, apply the **R** (Repeat) action to a listed item.

3. Overtype the repeated line with the new schedule item details.

View the Next Execution of Timer Schedule Items

To view the next execution of the time schedule items, press the F5 (NextTmr) function key on the Timer Schedule panel.

The Next Execution Display panel appears.

This panel displays the next scheduled execution time and date of each timer schedule item in the order that they fall due, as well as all the schedule item details specified in the schedule map.

```
PROD--------------- EventView : Next Execution Display -----------------------
Command ===>                                                  Scroll ===> PAGE

    Item NextDate     NextTime  Day  Date        Time      Every  Num  EndTime
      2  08-AUG-1995  16.00.00  TUE             16.00.00  00.10  12   18.00.00
      3  09-AUG-1995  16.00.00  WED             16.00.00  00.10  12   18.00.00
      4  10-AUG-1995  16.00.00  THU             16.00.00  00.10  12   18.00.00
      5  11-AUG-1995  16.00.00  FRI             16.00.00  00.10  12   18.00.00
      6  12-AUG-1995  16.00.00  SAT             16.00.00  00.30  4    18.00.00
      7  13-AUG-1995  16.00.00  SUN             16.00.00  00.30  4    18.00.00
      1  14-AUG-1995  16.00.00  MON             16.00.00  00.10  12   18.00.00
    **END**

  F1=Help      F2=Split     F3=Exit                  F5=Find      F6=Refresh
  F7=Backward  F8=Forward   F9=Swap
```

Delete Timer Schedule Items

To delete a timer schedule item, apply the **D** (Delete) action to the item.

Timer Actions

On the Timer Actions panel, you can specify what response is made when a scheduled timer item is triggered. You can specify the following:

- System command text, such as: START STC1
- Command text, such as:

  ```
  LOG TEST TIMER RULE EXECUTED
  ```

- A process selected from the list of valid processes—enter a question mark in the field to display a list of valid processes
- An Automation Services command selected from the list of valid commands—enter a question mark in the field to display a list of valid commands

Example: Send Warning Message

The TSO resource is defined to stop automatically at 1900 on weekdays. To warn users of the impending shutdown, you can define a timer that sends a warning message to the users at 1845 on the weekdays.

```
PROD------------------ EventView : GRTIMER1 Rule Actions -------------FOGRULE1
Command ===>                                                    Function=COPY

System Command ... SEND 'TSO WILL BE STOPPED IN 15 MINUTES - PLEASE LOG OFF'
                   ____________________________________________________________
OCS Command ...... ____________________________________________________________
                   ____________________________________________________________
```

Display Active Timer Rules

To display active timer rules

1. Enter **/EADMIN**.

   The Event Administration Menu appears.

2. Enter **S.T**.

   The Active Timer Display appears.

   The displayed list shows the date and time of the next scheduled execution of all timer rules that have a status of active and are associated with the active rule set. If you scroll to the right, the schedule item details, as specified on the schedule map, appear.

   You can browse, update, copy, or delete listed timers.

Chapter 24: Setting Up Event Monitoring

This section contains the following topics:

Implement Event Recording and Reporting

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 lets you 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

1. Enter **/PARMS** at the prompt.

   The Customization Parameters panel appears.

2. Enter **U** beside the $RF EVENTLOG parameter group.

   The Initialization Parameters panel for event logging appears.

3. Complete the following fields:

   Enabled Event Logging

   Ensure this field is set to Yes.

   EVNTDB Database Name

   Enter the data set name to which events are to be logged, or use the default. The setup process created this VSAM data set. For more information, see the *Installation Guide*.

   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.

   The utilization of data and index blocks is shown in message N13522 in the activity log when the region is initialized.

Time of Day to Delete

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.

Number of Days to Keep

Specify the number of days (between 0 and 30; default 7) for which reported events are to be kept in the EVNTDB database.

Zero deletes all events. A value between 1 and 30 retains events from the previous 1 to 30 calendar days in the EVNTDB database.

Note: Keeping a lot of data online impacts the time to search for events.

EVNTARC Archive Dataset

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. For more information, see the *Installation Guide*.

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.

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.

Field Separator Character

Specify the character you want to separate archived events. The default is comma (,).

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.

EVNTSEQ Reorg Dataset

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 setup process created the default. For more information, see the *Installation Guide*.

4. Press F6 (Action) to implement your initialization parameters for reporting.

Implement the ReportCenter Interface

If you use ReportCenter, you can send file transfer events to it for reporting.

For more information about implementing ReportCenter, see the *ReportCenter Guide.*

Log Event Rates to the Data Warehouse

To log event rates to the data warehouse

1. Enter **/PARMS** at the prompt.

   The list of parameter groups appears.
2. Enter **U** beside the EVENTLOG parameter group.

   The Parameter Group panel appears.
3. Press F8 (Forward).
4. In the Send Event Rate Data to ReportCenter? field, enter **YES**.
5. Press F6 (Action).

   Logging starts.
6. Press F3 (File).

   The system saves the changes.

Implement CA SOLVE:Central Problem Records

If you have CA SOLVE:Central you can set up your region to add problem records to it.

To implement an automatic problem recording environment

1. Copy the $RMPB07S NCL procedure from the *dsnpref*.NMC1.CC2DEXEC data set to the NCL procedures library (normally TESTEXEC) in the region in which CA SOLVE:Central is running.

2. Authorize the following user IDs in the problem management region:
   - The BSYS background user ID *xxxx*BSYS, where *xxxx* is the domain ID of the CA NetMaster FTM region
   - IDs of the users who may raise trouble tickets manually from the Alert Monitor
3. In the problem management region, define a link to each CA NetMaster FTM region from which you want to receive trouble tickets as follows:

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

   acb-name is the ACB name of the CA NetMaster FTM region, and *link-name* is a name that identifies the link.

Chapter 25: Processing Messages

This section contains the following topics:

Message Rules

You use EventView message rules to process messages.

How You Specify Message Filtering Criteria

The text of a received message is compared with the scan text specified on the Message Filter panel. For example, if you specify TESTMSG1 as the scan text, any message starting with those eight characters is considered a match, including TESTMSG12 and TESTMSG1 TESTING.

Note: If you want to capture a message that has leading blanks, do not specify the leading blanks on the message filter panel. However, on the Extended Message Filter panel, absolute position is important so leading blanks must be counted when using start position of text.

This message text can include wildcard characters. The default is the asterisk (*). You can specify the message text that triggers the rule if the execution conditions are met. You can also specify additional filters on further panels to check for various different conditions. To access those panels, enter **E** next to the message text (as shown in the following illustration).

```
PROD------------------ EventView : Message Filter ----------------------TAPEMON
Command ===>                                                    Function=UPDATE

Ruleset Name ........ TAPEMON                        Rule Status ...+ ACTIVE
Short Description ... Mount request processing

. Expected Message ------------------------------------------------------------.
|                                      S=ListPanels E=ExtFilter T=TestVars |
|      Message Text  ( WildChar = * )                                  ExtFlt |
| e    IEC501A                                                         NO     |
'-----------------------------------------------------------------------------'
```

```
PROD----------------- EventView : Extended Message Filter ---------------------
Command ===>                                                    Function=UPDATE

Message Text ......... IEC501A
Wildcard Character ... _
Descriptor Code .....+ ____________
Route Code ..........+ ____________
Message ID ........... ____________ (of major line)
System Name .......... ________

. Message Text Analysis -------------------------------------------------------.
|   Strt Word      Scan                                                       |
|   Pos  Num  Opr  Text                                                       |
| 1 ___  ___  ___  ___________________________________________________________ |
| 2 ___  ___  ___  ___________________________________________________________ |
| 3 ___  ___  ___  ___________________________________________________________ |
| 4 ___  ___  ___  ___________________________________________________________ |
| 5 ___  ___  ___  ___________________________________________________________ |
|                                                                             |
| Expression ..... ____________________________________ e.g. (1 and (2 or 3)) |
'-----------------------------------------------------------------------------'

 F1=Help      F2=Split     F3=OK
              F8=Forward   F9=Swap                 F11=Panels   F12=Cancel
```

Use Wildcards in Message Text

Typically, you can simply specify enough message text to identify the messages you want the message rule to process.

You can also use wildcard characters to insert character patterns in the message text. If you use a wildcard character, you must also add a wildcard character to the end of the message text if necessary.

The following examples show the correct use of wildcard characters:

EC501A
IEC50*A*
IEC5**A*

The number of characters represented by a wildcard character is dependent on its position in the message text as follows:

- If the wildcard character is at the beginning of, or embedded in the message text, it represents one character.
- If the wildcard character is at the end of the message text, it represents any number of characters.

Extended Filtering Criteria

The Extended Message Filter panel lets you specify precise criteria to match:

Wildcard Character

Specifies a value other than the default value of an asterisk (*). This change is reflected in the Wildcard Character field on the Message Filter panel when you save the extended filtering criteria. This feature is useful if the message actually contains an asterisk.

Descriptor Code

Specifies one or more descriptor codes. A descriptor code determines the color that the operating system uses to display the message on a color console. The code also determines whether the message is a non-roll delete message. The descriptor codes assigned to a message are tested against the specified descriptor codes. A message matches if it contains any of the specified descriptor codes.

Route Code

Specifies one or more route codes. The operating system uses the route code to control message delivery. The route codes assigned to a message are tested against the specified route codes. A message matches if it contains any of the specified route codes.

Message ID

Specifies the first word of the message text (disregarding any flag characters, such as an asterisk, in position 1 or 2). When a secondary line of a multiline WTO message is filtered, the message ID for the line is the same as the ID for the primary line.

System Name

Specifies the name of the system from which the message originated. This field is useful if the local system reissues messages received from other systems. Messages are reissued if the system is part of a sysplex environment.

Message Text Analysis

You can analyze the text of the current message by word, phrase, or string, by specifying any combination of start position, word number, and permitted operator (such as equals, is greater than, and so on). You can specify up to five tests to perform on the message text and link these tests in an expression.

Note: EventView comparisons are *text-based*, that is, they are performed character by character, starting from the leftmost character of the extracted text. Text checking is done using the EBCDIC codes. Numbers are regarded as text. For example, the character string 100 is less than 99.

Message Text Analysis Criteria

You specify the message text analysis criteria on the following panels:

- Define Extended Filter Definitions panel (for a resource definition)
- Extended Message Filter panel (for a message action rule).

The panels enable you to analyze the text of the received message by specifying values in the Strt Pos, Word Num, and Opr fields. You can specify up to five tests, which are then linked in a defined, logical relationship that you specify in the Expression field.

For example, the Expression field has the entry 1 AND (2 OR 3). For the rule to be valid, Test 1 must be true and either Test 2 *or* Test 3 must be true.

A message consists of words. A word is a string of characters delimited by either a space or a comma. You have the option of specifying a word or part of a word for testing, or of extracting a substring for testing.

Important! ResourceView handles numeric comparisons; EventView always performs character comparisons.

Strt Pos

Specifies a position in the message where the text comparison is to start. The presence or absence of a value in the Word Num field determines the actual starting position.

If the start position is 2 and the Word Num field is blank, the comparison is on the partial message starting at the second character.

If the Strt Pos field is blank but the Word Num field has a value, then only that word is compared to the scan text. If the Strt Pos *and* the Word Num field are blank, the entire message is compared to the scan text.

If both Strt Pos and Word Num fields have values, the comparison narrows to a start position in a single word of the message text. The text used for comparison is the partial word. For example, if the word number is 8 and the start position is 2, the comparison starts from the second character of the eighth word.

For example, the following message arrives:

```
AAA100A THIS IS A MESSAGE NUMBERED MESSAGE 100
```

- If the Strt Pos field has a value of 2, the string tested is as follows:

  ```
  AA100A THIS IS A MESSAGE NUMBERED MESSAGE 100
  ```

- If the Word Num field has a value of 5, the string tested is as follows:

  ```
  MESSAGE
  ```

- If the Strt Pos field has a value of 2 and the Word Num field has a value of 5, the string tested is as follows:

  ```
  ESSAGE
  ```

Default: 1

Values: 1 through 999

Lne Num

Specifies a particular line in a multiline WTO or WTOR. If blank, any value in the Word Num field is treated as if all lines in the multiline message are joined as one string.

Values: Blank and 1 through 999

Note: Lne Num is not supported in EventView message rules; it is supported in ResourceView only.

Word Num

Specifies a particular word in a specific position in the message text string. If this field is blank, the entire message text that occurs after the specified start position is compared to the scan text. If this field contains a value but the Strt Pos field is blank, only the specified word is compared to the scan text. Spaces or commas delimits words.

Values: Blank and 1 through 999

Opr

Specifies a valid operator to control the type of comparison to perform if you enter a value in the Strt Pos or the Word Num field. The following operators are valid:

- CT (ConTain)
- EQ (EQual to)
- GE (Greater than or Equal to)
- GT (Greater Than)
- LE (Less than or Equal to)
- LT (Less Than)
- NE (Not Equal to).

If you enter a question mark (?) in this field, the list of valid operators is displayed.

Scan Text

Specifies the actual text (scan text) you want to test against the message text. You must have a match in the specified position or word for the comparison to be true. If you specify either CT or EQ as the operator, you can use the wildcard in or at the end of the Scan Text field. (You cannot use the wildcard character with the other operators.)

CT Operator

The CT operator tests whether the extracted message text (after the Strt Pos and Word Num fields have been applied) contains the specified scan text. If the Strt Pos and Word Num fields are blank, then the comparison is true if the scan text appears anywhere in the message.

Example: Use CT to Test a Message

This example uses the CT operator to test the following message:

```
AAA100A THIS IS A MESSAGE NUMBERED MESSAGE 100
```

The following table shows the result of the tests:

Strt Pos	Word Num	Scan Text	Extracted Text	Result
3	5	AGE	SSAGE	TRUE
1	2	THIS	THIS	TRUE

EQ Operator

The EQ operator tests for an exact match. That is, the (extracted) message text string must match the scan text exactly for the test to succeed.

A wildcard can be either in the scan text or at the end of the scan text.

If, for example, the message text is FREDERICK and the scan text is FRED, the test fails. If, however, the scan text is FRED*, the test succeeds.

Example: Use EQ to Test a Message

This example uses the EQ operator to test the following message:

```
AAA100A THIS IS A MESSAGE NUMBERED MESSAGE 100
```

The following table shows the result of the tests:

Strt Pos	Word Num	Scan Text	Extracted Text	Result
4	5	SAG	SAGE	FALSE
4	5	SAGE	SAGE	TRUE
1	8	10	100	FALSE
1	8	100	100	TRUE

GE Operator

The GE operator tests whether the value of the (extracted) message text is greater than or equal to that of the scan text. For ResourceView, if the characters to test are numeric, a numeric comparison is executed.

Example: Use GE to Test a Message

This example uses the GE operator to test the following message:

```
AAA100A THIS IS A MESSAGE NUMBERED MESSAGE 100
```

The following table shows the result of the tests:

Strt Pos	Word Num	Scan Text	Extracted Text	Result
1	8	99	100	TRUE (ResourceView)
1	8	99	100	FALSE (EventView)
1	8	100	100	TRUE
4	Blank	99	100A THIS …	FALSE
4	5	LAGE	SAGE	TRUE
4	5	TAGE	SAGE	FALSE

GT Operator

The GT operator tests whether the value of the (extracted) message text string is greater than the value of the scan text. For ResourceView, if the characters to test are numeric, a numeric comparison is executed.

Example: Use GT to Test a Message

This example uses the GT operator to test the following message:

```
AAA100A THIS IS A MESSAGE NUMBERED MESSAGE 100
```

The following table shows the result of the tests:

Strt Pos	Word Num	Scan Text	Extracted Text	Result
1	8	99	100	TRUE (ResourceView)
1	8	99	100	FALSE (EventView)
1	8	100	100	FALSE
4	Blank	99	100A THIS …	FALSE
4	5	LAGE	SAGE	TRUE
4	5	TAGE	SAGE	FALSE

LE Operator

The LE to operator tests whether the value of the (extracted) message text string is less than or equal to that of the scan text. For ResourceView, if the characters to test are numeric, a numeric comparison is executed.

Example: Use LE to Test a Message

This example uses the LE operator to test the following message:

```
AAA100A THIS IS A MESSAGE NUMBERED MESSAGE 100
```

The following table shows the result of the tests:

Strt Pos	Word Num	Scan Text	Extracted Text	Result
1	8	99	100	FALSE (ResourceView)
1	8	99	100	TRUE (EventView)
1	8	100	100	TRUE
4	Blank	99	100A THIS …	TRUE
4	5	LAGE	SAGE	FALSE
4	5	TAGE	SAGE	TRUE

LT Operator

The LT operator tests whether the value of the (extracted) message text string is less than the value of the scan text. For ResourceView, if the characters to test are numeric, a numeric comparison is executed.

Example: Use LT to Test a Message

This example uses the LT operator to test the following message:

```
AAA100A THIS IS A MESSAGE NUMBERED MESSAGE 100
```

The following table shows the result of the tests:

Strt Pos	Word Num	Scan Text	Extracted Text	Result
1	8	99	100	FALSE (ResourceView)
1	8	99	100	TRUE (EventView)
1	8	100	100	FALSE
4	Blank	99	100A THIS …	TRUE
4	5	LAGE	SAGE	FALSE
4	5	TAGE	SAGE	TRUE

NE Operator

The NE to operator tests for a mismatch between the (extracted) message text string and the scan text.

Example: Use NE to Test a Message

This example uses the NE operator to test the following message:

```
AAA100A THIS IS A MESSAGE NUMBERED MESSAGE 100
```

The following table shows the result of the tests:

Strt Pos	Word Num	Scan Text	Extracted Text	Result
1	8	99	100	TRUE
1	8	100	100	FALSE
4	Blank	99	100A THIS …	TRUE
4	5	LAGE	SAGE	TRUE
4	5	TAGE	SAGE	TRUE

Expression To Link Tests

The tests you specify in the Text Analysis box are linked in a defined relationship in the Expression field. The Boolean operators AND, OR, and NOT link the tests.

For example, you specify 1 and (2 or 3) in the Expression field. This expression indicates that the following conditions must be satisfied before the rule can be triggered:

- Test 1 must always be true.
- Either Test 2 or Test 3 must be true.

Note: If you leave the Expression field blank, all specified conditions must be true.

EventView Variables

You can use the values of EventView variables as a condition to trigger a rule. You specify the values on the Test EventView Variables panel (the second panel in the extended filter sequence). These values are compared with the values of the predefined EventView variables when the rule is validated. To trigger the rule, they must match.

Execution Conditions

If the message text passes the filtering process, further validation is performed to see whether the message received meets the specified execution conditions.

All the execution conditions specified on the Message Filter panel must be met before the message rule can be triggered. The following shows an example.

```
. Execution Conditions ------------------------------------------------------.
|                                                                             |
| Job Name ....            Rule Priority ...........      (1 is best)        |
| Job Type ....            Execute If Not Best Fit?                           |
|                                                                             |
|         Mon Tue Wed Thu Fri Sat Sun       Time       Start       End       |
| On Days NO  NO  YES NO  NO  NO  NO        Range1 ...                         |
|                                           Range2 ...                         |
|                                                                             |
'-----------------------------------------------------------------------------'
```

Important! If you want to detect a message from a started task that runs under the master scheduler (that is, by using the SUB=MSTR operand), do not use the Job Name and Job Type fields.

Overlapping Rules

You need to take into consideration that there may be more than one rule that applies to the same message.

EventView selects and executes the rule considered to be the best fit. This decision is based on how specific the filtering and execution conditions are; the more specific the rule (for example, the more message text specified), the better the fit.

You can override this determination of the best fit by entering a value (in the range 1 to 99) in the Rule Priority field, to indicate the order of importance. Top priority rules are given a ranking of 1, while the least important rule can be ranked 99.

You may want to trigger multiple rules for one message. The Execute if Not Best Fit? field, which can be set to Yes or to No, functions as follows:

- If set to NO (the default), the rule is not executed unless it is the best fit.
- If set to YES, the rule actions are executed whenever validation is successful.

Message Delivery

When a message satisfies the filtering criteria of a rule that is the best fit, the rule controls how the message is delivered. Specify the delivery criteria on the Message Delivery panel.

Set the Deliver Flag

To set the Deliver flag on the Message Delivery panel, specify *one* of the following values:

- YES (the default), if you want to deliver the message to the operating system and the consolidated console, and to log to the system log (SYSLOG) and the activity log
- IGN, if you want the region to ignore the message, but deliver it to the operating system and log it to the system log (SYSLOG)
- LOG, if you want the message logged to SYSLOG and the activity log, but not displayed on the console
- NO, if you want the message suppressed everywhere with the exception of SYSLOG
- Z, if you want the message suppressed everywhere, including SYSLOG

Note: Delivery of system messages to the activity log can be suppressed by the LOGFILES parameter group.

Delivery Thresholds

Thresholds determine what actions are taken when multiple messages trigger the rule in a given time period.

You set thresholds on the Message Delivery panel. You can request that the action associated with the rule be performed before these thresholds are reached, after they are reached, or whenever the rule is triggered, by entering a valid value in the Do Action field.

Note: When a threshold is reached, the value of the Deliver flag is effectively reversed. For example, if the flag is set to NO, messages to which the rule applies are suppressed until the threshold is reached, then delivered to the console. If the flag is set to YES, messages are delivered to the console until the threshold is reached, then suppressed. If the flag is set to LOG, messages are sent to the log until the threshold is reached, then delivered to the console.

How You Use Thresholds When Deliver Flag Is YES

You can specify that you do not want to see the same message more than a given number of times within a certain time interval.

For example, if you do not want to see the same message more than ten times within one minute, you enter the following values:

- **10** in the Maximum Number field
- **00.01.00** in the Time Interval field.

How You Use Thresholds When Delivery Flag Is NO

You can specify that you only want a message displayed if it starts occurring more frequently than usual. You enter a value in the Time Interval field. If more messages of the same kind than the number specified in the Maximum Number field are received in the specified time interval, the messages are displayed. Otherwise, the messages are not displayed.

For example, you want to see every fifth occurrence of a message. You set the Maximum Number field to four and leave the Time Interval field blank (or set to 0). This setting specifies that, no matter how long the interval between occurrences of this message, every fifth occurrence of the message is displayed. All other occurrences of the message are suppressed.

Correlation Key

To avoid creating separate rules for different versions of the same message, you can specify a correlation key on the Message Delivery panel. The rule keeps separate threshold counts for each instance of the correlation key. The separate counts avoid the possible suppression of important but uncommon versions of a message.

The correlation key can include the following:

- A user-defined EventView variable
- A reference to a ZMSG system variable, such as &ZMSGWORD3

Note: For more information about the system variables, see the *Network Control Language Reference Guide*.

Example: Specify a Correlation Key

This example limits the number of messages (from a given job) that trigger the rule to ten for every hour:

```
PROD------------------ EventView : Message Delivery --------------------TAPEMON
Command ===>                                                    Function=UPDATE

Deliver ..........+ YES

. Threshold ------------------------------------------------------------------.
|                                                                              |
| Maximum Number .. 10                                                         |
| Time Interval ... 01.00.00                                                   |
| Do Action ......+ _____                                                      |
| Correlation Key   &ZMSGJOBNM                                                 |
|                                                                              |
'------------------------------------------------------------------------------'









 F1=Help      F2=Split     F3=File      F4=Save
 F7=Backward  F8=Forward   F9=Swap                 F11=Panels    F12=Cancel
```

Message Modification

Message presentation and message text can be modified by specifying the requirements on the Message Modification panel.

Message Text Replacement

Using the Replacement Text field on the Message Modification panel, you can replace the entire message text with an alternative text string. The text can include system variables.

Note: For more information about the system variables, see the *Network Control Language Reference Guide*.

System Message Presentation Parameters

To alter how a message is displayed to a system console user, specify the message descriptor code in the Set Descriptor Code field. This code determines the color that the system uses to display the message on a color console, and whether the message is non-roll deletable.

To change the message route code, specify a value in the Set Route Code field, which the system uses to control message delivery.

OCS Message Presentation Parameters

By completing the appropriate fields in the lower box on the Message Modification panel, you can alter how a message is displayed to a user. You can also specify whether a console alarm is sounded when the message is delivered, and whether the message is delivered to monitor class users. The monitor status of a user is set in the user definition and profile.

Example: Sound Alarm on Message Delivery

This example specifies that the console alarm is sounded when the messages that trigger the rule are delivered.

```
PROD-------------------- EventView : Message Modification --------------TAPEMON
Command ===>                                                    Function=UPDATE

Replacement Text ____________________________________________________________
                 ____________________________________________________________

. Message Presentation ------------------------------------------------------.
|                                                                            |
| Set Descriptor Code ....+ ____________                                     |
| Set Route Code .........+ ____________                                     |
|                                                                            |
'----------------------------------------------------------------------------'

. SOLVE Message Presentation ------------------------------------------------.
|                                                                            |
| Color ......+ _________  Highlight ...+ _______  Intensity ...+ ______     |
| Monitor? .... ___        Alarm? ....... YES      NRD? ......... ____       |
| Message Code  __                                                           |
|                                                                            |
'----------------------------------------------------------------------------'


 F1=Help      F2=Split     F3=File      F4=Save
 F7=Backward  F8=Forward   F9=Swap                F11=Panels    F12=Cancel
```

Actions to Take in Response to Messages

Important! Do *not* capture a WTO message and then, using a process or other means, reissue the same WTO message. Reissuing a captured WTO message causes a loop.

On the Message Actions panel, you can specify what response is made to a message. Apart from reply text, you can specify the following:

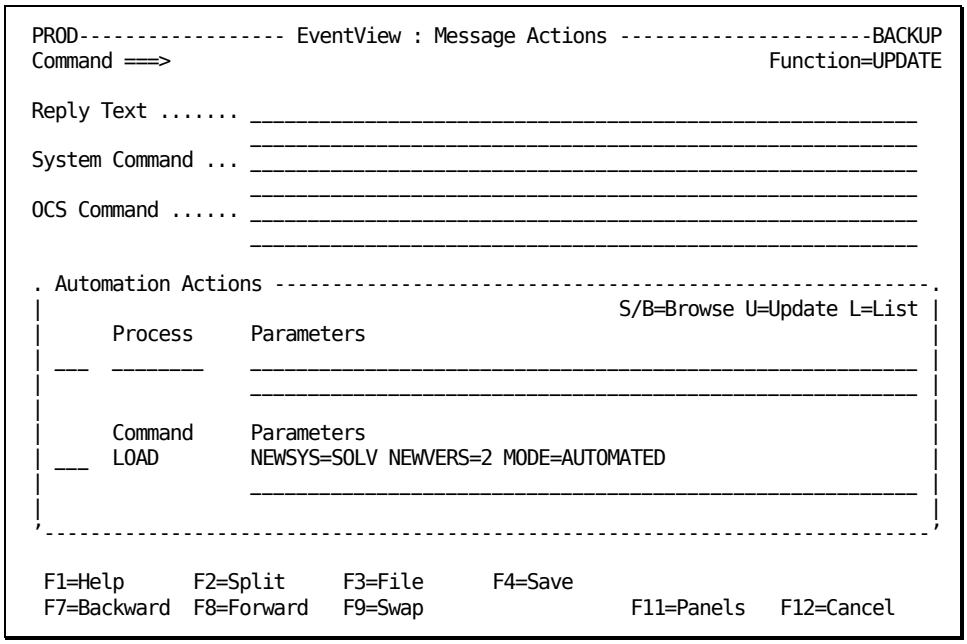
- System command text, such as: START STC1.
- OCS Command text, such as:

  LOG TEST MSG1 ENCOUNTERED-WORD5=&ZMSGWORD5

- A process selected from the list of valid processes—enter a question mark in the field to display a list of valid processes.
- An Automation Services command selected from the list of valid commands—enter a question mark in the field to display a list of valid commands.

Example: Load System Image on Rule Trigger

This example loads a new system image in the local region when the rule is triggered.



How You Suppress Messages

You can reduce message traffic to the system and the consolidated console by suppressing messages that operators do not require to perform their tasks. Message suppression does not affect the automated resource monitoring and control functions performed by ResourceView and ServiceView.

Use the following methods to suppress messages:

- Set the Deliver flag from the Message Delivery panel of a message rule. For example, you can specify LOG to suppress messages that trigger the rule from the consoles but enables them to be logged.
- Use the threshold criteria on the Message Delivery panel to suppress redundant messages when multiple messages trigger the rule in a specified time.
- When you have implemented rules for all relevant messages, you can suppress all other messages. To suppress these messages, specify NO or Z in the Default Message Delivery field on the Ruleset Description panel.

  Use the message-learning facility to identify any new messages that have been suppressed. You can then decide whether to create rules for them.

Log 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

1. Enter **/PARMS** at the prompt.

   The Customization Parameters panel appears.

2. At the prompt, enter **F CDEVENTS** to find the CDEVENTS parameter group.

   The parameter group list scrolls to display the $RF CDEVENTS parameter group.

3. Enter **U** beside the listed $RF CDEVENTS parameter group.

   The Initialization Parameters panel for the parameter group appears.

   See the Notes window for a description of the fields, and make changes accordingly.

4. Perform *one* of the following:

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.

Chapter 26: Message Learning

This section contains the following topics:

About Message Learning

The message-learning facility records messages seen by EventView. The facility provides you with a list of all messages encountered during system operation. After you review the initial set of messages, you can reset the new message indicator. Then, when new software is installed, you can easily learn about the new messages.

The facility allows you to do the following:

- List all learnt messages, or all *new* learnt messages
- Display formatted information about listed messages
- Create a message rule from a learnt message
- Use the learnt message list as a prompt list when specifying messages for resource definitions. For more information, see the *Reference Guide*.

Normally, only the first message that starts with a particular word is learnt. However, since some programs issue diverse messages with the same first word, EventView allows for this possibility. EventView also allows you to learn the minor lines of a multiline message. You can enable these features by entering YES in the Learn Multiple Messages? field on the Message Details panel of a learnt message.

Control Message Learning

Message learning can be enabled only if an EventView rule set is loaded with your system image. You control the facility by using the Learn New Messages? field on the Ruleset Description panel of the rule set definition.

To enable message learning for a rule set

1. Enter **/EADMIN.R.R** at the prompt.

   The Ruleset List panel appears.

2. Enter **U** next to the rule set for which you want to enable message learning.

   The panels for rule set definition are listed.

3. Enter **S** next to Ruleset Description.

   The Ruleset Description panel appears.

4. Specify **YES** in the Learn New Messages? field, and press F3 (File).

   Message learning is enabled for the rule set.

Browse and Update Learnt Messages

You can browse and update learnt messages by applying the appropriate action to a listed message.

To display learnt messages

1. Enter **/EADMIN** at the prompt.

   The Event Administration panel appears.

2. Select **L** - Message Learning.

3. Select either **L** - Learnt Messages (to list all learnt messages) or **N** - New Learnt Messages.

4. Apply the **B** (Browse) action to a message you want to browse, or the **U** (Update) action to a message you want to update.

   For example, you may want to update the Learn Multiple Messages? field on the Message Details panel, to indicate that you want EventView to learn multiple messages with the same ID.

5. Select the panel you want to browse or update. Press F1 (Help) for definitions of the fields on the panels.

Generate a Rule for a Learnt Message

If you want to suppress further instances of a message, or to automate the response to the message, you can generate an associated message rule.

To generate a rule for a learnt message

1. From the Learnt Message List, apply the **GR** (Generate Rule) action to a listed item.

   The Ruleset List panel appears.

2. Select the rule set to which you want to add the message rule.

   The initial panel of the generated message rule appears in Add mode. All details stored in the learnt message record that are relevant to message rules have been copied to the message rule record and are displayed in the appropriate fields.

3. Complete the mandatory Short Description field, and complete or update other fields as required.

4. Save the new message rule.

Reset New Message Indicators

If you want to differentiate between messages learnt before and after a certain date, you can reset the new message indicators. You may also want to reset the new message indicators after you review and create rules for the current learnt messages.

Later, you can select the New Learnt Messages option from the Event Message Learning menu to list only those messages that are learnt since you reset the new message indicators (for example, since the last review).

If you list all learnt messages, an asterisk (*) identifies the messages that are flagged as new messages.

To reset new message indicators

1. Enter the **/EADMIN.L** panel path.

   The Event Message Learning menu appears.

2. Select the **R** option.

   The Confirm Database RESET panel appears.

3. Press Enter.

   The new message indicators are reset.

Delete All Learnt Messages

To avoid accumulating too many messages, you can purge all messages after you have viewed those messages that interest you and generated appropriate rules.

Important! Purged messages cannot be recovered.

The AUTOTABLES parameter group controls the size of the table that stores the learnt messages.

To delete all learnt messages, select the **D** option from the Event Message Learning menu.

All learnt messages are purged from the Message Learning database.

Chapter 27: Implementing Message Profiles

This section contains the following topics:

Consolidated Console

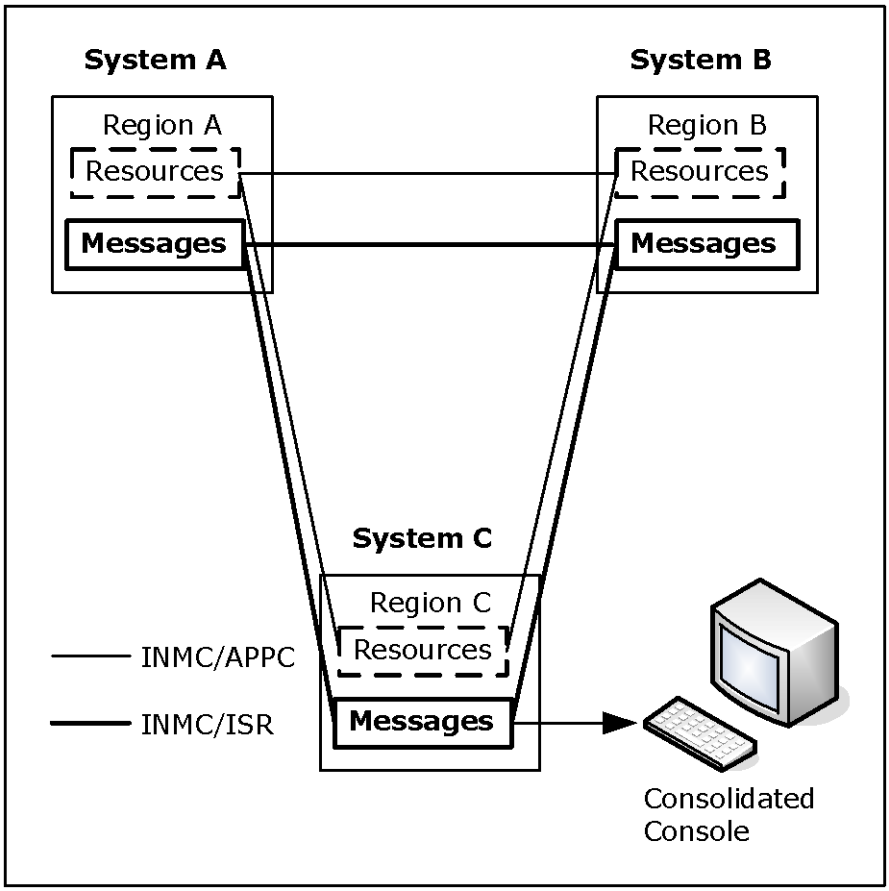
The console consolidation facility consolidates console message traffic from multiple systems onto a single panel (known as a *consolidated console*). Operators can thus view those messages from a single console. You create *message profiles* that contain criteria to identify and classify messages. If a user requests messages for a given message profile, all messages that match the criteria of that profile are displayed on that user's consolidated console.

Note: Multisystem message visibility is available only at consolidated consoles in focal point regions. In subordinate regions, only local messages are visible.

How Console Consolidation Works in a Multisystem Environment

Multisystem support at the message level provides for the distribution of messages to consolidated consoles in focal point regions in the multisystem environment.

The following illustration shows how each region communicates with other connected regions by using Inter-Network Management Connection (INMC)/Inter-System Routing (ISR) links.



Each region has an ISR link manager. The ISR link manager is started up as part of region initialization. The ISR link is active but disabled until a user starts console consolidation. The ISR link manager enables message flow across the link based on requests from users for messages that match specific message profiles.

The user profile determines the messages seen on a consolidated console. The ISR link manager suppresses those messages that are not required, thus reducing the amount of message flow. A user who has not been assigned message profiles or has all the assigned message profiles disabled sees no messages on the consolidated console.

Message Profiles

You can define profiles that capture different types of messages. When you create or change a message profile, the data is automatically distributed to the knowledge bases in connected regions.

Note: You can define message profiles in focal point regions only; however, the defined profiles are available to subordinate regions through knowledge base synchronization.

A message profile contains the following criteria types that determine which messages a consolidated console receives:

- The system from which the message comes
- The ID (or the first word) of the message
- The job for which the message is generated
- The message routing and descriptor codes
- The message types and levels, and the types and classes of job for which the message is generated

A message profile must use at least one criterion from the last four criteria types.

Each profile has a status that determines whether it can be activated for use. Profiles must be activated, either by you or automatically during region startup, before they can be used. After you define the profiles, you activate them for use by the operators.

Rules for Defining and Using Message Profiles

This section contains rules about entering data on panels and about how to get the best results when defining message profiles.

Create New Message Profiles in a Single System First

Create a new message profile to select messages from one system only, using selection criteria that are unique to that system. For example, if each system uses different message classes, specify a message class that is unique to your system. When this profile is working successfully in one system, you can copy it into a new profile for other systems whose messages you want to monitor.

Unique Message Profile Names and IDs

Unique profile names and IDs identify message profiles. When messages are captured, they are associated with a specific profile ID. The profiles replace the message routing codes corresponding to the IDs as the means for the region to direct relevant messages to operators. An operator who wants to receive specific messages on a consolidated console enables the relevant profiles. Alternatively, if the operator always wants to see consolidated messages for certain profiles, the operator can specify this information in the user profile (see page 333).

Important! A profile acts on messages after they are processed by EventView message rules. For example, if a rule changes the routing code and you want to capture the message, use a profile ID that corresponds to the changed routing code.

You cannot include special characters (for example, _, -, (,), and ~) or spaces in a profile name.

Wildcards

Use wildcard characters to represent character patterns at particular positions in a character string. The supported wildcard characters are as follows:

- *, representing any character as follows:
  - If the * is at the beginning of or embedded in a character string, it represents one character.
  - If the * is at the end of a character string, it represents any number of characters.

  You *cannot* use an * by itself. In the following example, messages are selected for any system that starts with the letters EAST:

  Systems to Include
  EAST*
- #, representing one numeric character. In the following example, messages are selected for systems EAST0 through EAST9:

  Systems to Include
  EAST#
- @, representing one alpha character. In the following example, messages are selected for systems EAST0A through EAST9Z:

  Systems to Include
  EAST#@

Type as many characters as necessary to select the required information.

If you want to use a wildcard character in the literal sense, precede the character by a backslash (\), for example:

- ABC### matches any value that starts with ABC followed by three numeric characters.
- ABC##\# enables you to match a value that starts with ABC followed by two numeric characters and ending in a # character.

Ranges

Use a colon (:) to specify ranges.

The character strings on each side of the colon must be of equal length.

Note: The backslash (\) is regarded as one character when the length of the string is calculated.

The asterisk (*) wildcard character can only be used at the end of a string.

Example: Select Messages in a Range of Systems

This example selects messages for systems EAST0, EAST1, and EAST2.

```
Systems to be Included
EAST0:EAST2
```

Inclusion and Exclusion Criteria

In each profile, you specify the criteria that determine the messages to display on the consolidated console. Most panels have *inclusion fields* and *exclusion fields*, or allow you to specify N(o) or Y(es), according to whether you want to include or exclude messages with certain attributes. The rules for including and excluding messages are as follows:

- If you leave all the fields on a panel blank, the criteria specified on the other panels determine what messages are displayed. For example, if you leave the System Specification panel blank, messages from all connected regions are potentially available for display.

  However, if you do *not* specify any criteria (that is, if you leave the criteria fields on all the panels blank), the profile receives *no* messages.

- If you specify inclusion and exclusion values for a particular criterion, the inclusion values take priority. The exclusion values are then applied to the resulting set of included messages.

  For example, using message ID as a criterion, if you want to include all message IDs except the IDs starting with AAA111, you can use the following values:

  - A*:9* as inclusion values
  - AAA111* as exclusion values

- Messages are selected for display only if they meet the criteria specified on all panels. For example, YES in the Sess field on the Message Job Specification panel specifies that only SESS type messages are displayed, even if messages of other types meet the criteria specified on the other panels.
- Items selected with N or Y have an OR relationship. For example, if you include routing codes 1, 2, and 11, messages that have a routing code of 1 *or* 2 *or* 11, *or* a combination of these codes, are displayed if they satisfy the other criteria.
- If you complete an exclusion field or specify N, a message that meets this criterion is not displayed, even if it satisfies all the inclusion criteria.

Note: The consolidated console does not receive messages suppressed by EventView rules.

Access the Message Profile Definitions

To access the message profile definitions, enter **/EADMIN.C.M** at the prompt.

The Message Profiles panel appears.

This panel lists all the message profiles in the knowledge base. You can enter action codes to perform actions on existing message profiles, or press F4 (Add) to add a new profile.

How You Define a Message Profile

To add a message profile, press F4 (Add) from the Message Profiles panel. You define the profile by using the following panels:

Profile Details

Enables you to identify the profile. Complete this panel.

System Specification

Enables you to use the system associated with a message as a selection criterion.

Message Specification

Enables you to use the message ID as a selection criterion.

Job Name Specification

Enables you to use the job associated with a message as a selection criterion.

OS Codes Specification

Enables you to use the routing and descriptor codes associated with a message as selection criteria.

Message Job Specification

Enables you to use the message type and level, and the job type and class associated with a message as selection criteria.

You can create a profile to capture particular messages (for example, tape mount messages) or messages for particular jobs (for example, production CICS jobs). You do not need to complete every panel for most profile definitions. However, complete at least one of the criteria panels. If you leave all the criteria panels blank, the profile blocks all messages.

Profile Details

Use the Profile Details panel to identify the message profile. Specify the profile name, ID, and description. All profile panels contain this information.

Note: You cannot use the value 2 as the profile ID.

Only profiles that have IDs corresponding to those set for a parameter in the CCONSOLIDATN parameter group are available for use in the local region. The parameter can exclude certain IDs. To display the value of the parameter, enter the **/PARMS** shortcut to access the list of parameter groups and browse the CCONSOLIDATN parameter group.

The Profile Details panel also contains the following information:

- Profile status
- Whether to profile for solicited messages
- History of when the profile was created and last updated

Only profiles with an ACTIVE status can be activated for use.

System Criteria

From the Profile Details panel, press F8 (Forward) to display the System Specification panel. You can specify the systems for which messages are captured.

The values you use in the Systems to be Included or Excluded fields are the system management facilities (SMF) ID or the region domain ID. The value type is indicated at the bottom of the panel as SMFID or NMDID respectively, and is set in the CCONSOLIDATN parameter group.

The criteria can be specific, generic, or in a range.

Leave the fields blank to allow messages for all the connected systems to be captured. These messages are captured only if other criteria are specified in the profile and the messages satisfy those criteria.

Message ID Criteria

From the System Specification panel, press F8 (Forward) to display the Message Specification panel. You can specify the IDs (or generic IDs, for example, $HASP*) of the messages you want to capture. The message ID is the first word of a message.

The values can be specific, generic, or in a range.

Leave the fields blank to capture messages with any ID. These messages are captured only if other criteria are specified in the profile and the messages satisfy those criteria.

Job Criteria

From the Message Specification panel, press F8 (Forward) to display the Job Name Specification panel. You can name the jobs (and started tasks) for which messages are captured.

The values can be specific, generic, or in a range.

Leave the fields blank to capture messages for all jobs. These messages are captured only if other criteria are specified in the profile and the messages satisfy those criteria.

System Codes Criteria

From the Job Name Specification panel, press F8 (Forward) to display the OS Codes Specification panel. You can specify the route and descriptor codes assigned to messages that are captured. Messages can contain one or a combination of the codes you specify. If a message contains codes that you exclude specifically, the message is not selected.

You can exclude certain codes by typing **N** under the codes, include certain codes by typing **Y** under the codes, and leave the other code fields blank. A message containing any of the included codes is selected unless the message also contains an excluded code.

Leave the fields blank to capture messages that contain any route and descriptor codes. If other criteria are specified in the profile and the message satisfies those criteria, the message is displayed on the consolidated console.

Message Type, Level, and Job Criteria

From the OS Codes Specification panel, press F8 (Forward) to display the Message Job Specification panel. You can specify the message types, and message levels, job types, and job classes assigned to messages that are captured.

You can include or exclude certain items in each criteria type, but not both (except for the Broadcast field under Message Levels). For example, if you want to accept immediate action messages but not broadcast messages, specify Y in the Immediate Action field and N in the Broadcast field.

Leave the fields blank to allow messages of any type, level, job type, or job class. If other criteria are specified in the profile and the message satisfies those criteria, the message is displayed on the consolidated console.

Job Classes

The job class is assigned by the CLASS parameter of the JOB JCL statement.

Message Types

Message types correspond to the operands of the MONITOR or STOPMN system commands. For example, messages generated because of the MONITOR SESS command have the SESS type.

Message Levels

Message levels indicate the relative importance of a message.

Note: The broadcast level has precedence over all other message criteria. If broadcast messages are allowed, the message profile passes all broadcast messages irrespective of the other criteria.

Job Types

Job types are as follows:

Job

Indicates a batch job.

STC

Indicates a started task.

In a JES3 environment, a started task has a job type of Job.

TSU

Indicates a TSO user.

Unknown

Indicates a job type that is not one of the previous types.

Example: Profile Specific Messages

In this example, the organization has two branches: an eastern branch and a western branch. You want to create a profile to capture all tape mount messages for all the production systems running in the eastern data center, but do not want to capture messages for development jobs. The job classes assigned to tape mount requests are 1, 2, and 3.

From the Message Profiles panel, press F4 (Add) to add a profile. A Profile Details panel appears. You can press F8 (Forward) to scroll forward through the panels or enter the panel index number at the Command prompt to select a specific panel. (Pressing F11 (Panels) displays of a list of panels and panel index numbers.)

Use the following panels in this example:

- Profile Details
- System Specification
- Message Specification
- Job Name Specification
- Message Job Specification

On the Profile Details panel, type a unique profile name (TAPEMOUNTS), a unique ID (127), a description of the profile (Tape Mounts for Eastern Production Jobs), and assign a status. Assign a status of ACTIVE so that the profile can be activated.

The following panel shows the completed Profile Details.

```
PROD------------------- EventView : Profile Details -------------MCPROFIL-0000
Command ===>                                                  Function=UPDATE

+---------------------- Message Classification Profile ----------------------+
| Name ... TAPEMOUNTS       ID ..... 127 (1 - 128)                           |
| Description .... Tape Mounts for Eastern Production Jobs_____________________ |
+-------------------------------------------------------------------------------+
+ Profile Status ------------------------------------------------------------+
| Profile Status ... ACTIVE__ (Active/Inactive)                              |
+-------------------------------------------------------------------------------+
+ Include Solicited Messages? -----------------------------------------------+
| Solicited Type ... NO___    (No, Other, Nothr, Yes, All)                   |
+-------------------------------------------------------------------------------+

+ History -------------------------------------------------------------------+
|                                                                            |
| Profile Created           Profile Last Updated      Profile Status Updated |
| Userid  USER01            Userid                    Userid                 |
| Date .. THU 25-MAY-2006   Date ..                   Date ..                |
| Time .. 14.48.27          Time ..                   Time ..                |
+-------------------------------------------------------------------------------+

 F1=Help      F2=Split     F3=File      F4=Save
              F8=Forward   F9=Swap                 F11=Panels    F12=Cancel
```

Press F8 (Forward) to scroll forward to the System Specification panel. You do not want to capture messages for any western branch systems, so you complete the exclusion fields. All western branch systems start with the letters WST, so WST* is typed to exclude all western branch systems.

The following panel shows the completed System Specification.

```
PROD---------------- EventView : System Specification -----------MCPROFIL-0000
Command ===>                                                  Function=UPDATE

+---------------------- Message Classification Profile ----------------------+
| Name ... TAPEMOUNTS       ID ..... 127 (1 - 128)                           |
| Description .... Tape Mounts for Eastern Production Jobs                   |
+----------------------------------------------------------------------------+
+-----------------------------------+ +-----------------------------------+
| Systems to be Included            | | Systems to be Excluded            |
+-----------------------------------+ +-----------------------------------+
| ________________ ________________ | | WST*_____________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
+-----------------------------------+ +-----------------------------------+

Note : Identify the systems by using SMFID


 F1=Help      F2=Split     F3=File      F4=Save
 F7=Backward  F8=Forward   F9=Swap                 F11=Panels    F12=Cancel
```

Press F8 (Forward) to scroll forward to the Message Specification panel. You only want to display IEF233A messages, which are requests for tape mounts, so you complete the inclusion fields.

The following panel shows the completed Message Specification.

```
PROD---------------- EventView : Message Specification -----------MCPROFIL-0000
Command ===>                                                  Function=UPDATE

+---------------------- Message Classification Profile ----------------------+
| Name ... TAPEMOUNTS       ID ..... 127 (1 - 128)                           |
| Description .... Tape Mounts for Eastern Production Jobs                   |
+----------------------------------------------------------------------------+
+-----------------------------------+ +-----------------------------------+
| Message IDs to be Included        | | Message IDs to be Excluded        |
+-----------------------------------+ +-----------------------------------+
| IEF233A__________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
+-----------------------------------+ +-----------------------------------+




 F1=Help      F2=Split     F3=File      F4=Save
 F7=Backward  F8=Forward   F9=Swap     F10=Scrllst  F11=Panels    F12=Cancel
```

Press F8 (Forward) to scroll forward to the Job Name Specification panel. You do not want to capture messages for development jobs. All development jobs in the eastern branch start with the letters DEV, so DEV* is typed in an exclusion field.

The following panel shows the completed Job Name Specification.

```
PROD---------------- EventView : Job Name Specification ----------MCPROFIL-0000
Command ===>                                                  Function=UPDATE

+---------------------- Message Classification Profile -----------------------+
| Name ... TAPEMOUNTS       ID ..... 127 (1 - 128)                            |
| Description .... Tape Mounts for Eastern Production Jobs                    |
+-----------------------------------------------------------------------------+
+-----------------------------------+ +-----------------------------------+
| Job Names to be Included          | | Job Names to be Excluded          |
+-----------------------------------+ +-----------------------------------+
| ________________ ________________ | | DEV*_____________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
+-----------------------------------+ +-----------------------------------+



 F1=Help      F2=Split     F3=File      F4=Save
 F7=Backward  F8=Forward   F9=Swap     F10=Scrllst  F11=Panels   F12=Cancel
```

Enter **6** at the prompt to display the Message Job Specification panel. Here you want to capture messages for jobs only, in job classes 1 (for jobs that need one tape mounted), 2 (for jobs that need two tapes mounted), and 3 (for jobs that need three tapes mounted).

The following panel shows the completed Message Job Specification.

```
PROD-------------- EventView : Message Job Specification ---------MCPROFIL-0000
Command ===>                                                  Function=UPDATE

+---------------------- Message Classification Profile -----------------------+
| Name ... TAPEMOUNTS       ID ..... 127 (1 - 128)                            |
| Description .... Tape Mounts for Eastern Production Jobs                    |
+-----------------------------------------------------------------------------+
+-----------------------------------------------------------------------------+
| Message Types        ( Y =Include, N =Exclude, Blank =Don't care )           |
|  Jobnames .. ___   Status .. ___   Active .. ___   Sess .. ___              |
|                                                                             |
| Message Levels       ( Y =Include, N =Exclude, Blank =Don't care )           |
|      WTOR .. ___  Immediate Action .. ___  Critical Eventual .. ___         |
|  Eventual .. ___     Informational .. ___          Broadcast .. ___         |
|                                                                             |
| Job Types            ( Y =Include, N =Exclude, Blank =Don't care )           |
|       Job .. YES   STC .. ___   TSU .. ___   Unknown .. ___                 |
|                                                                             |
| Job Classes          ( Y =Include, N =Exclude, Blank =Don't care )           |
|              ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789                           |
| (A-Z,0-9) ..                          YYY                                   |
+-----------------------------------------------------------------------------+
 F1=Help      F2=Split     F3=File      F4=Save
 F7=Backward              F9=Swap                 F11=Panels    F12=Cancel
```

Example: Profile Messages for Specific Jobs

In this example, you want to create a profile to capture messages for certain CICS jobs on the production systems in the eastern and the western branches. The branches use only one test system, ETST. You assign a status of INACTIVE, as you do not want the profile to be used immediately. You only want to capture messages that have routing codes of 1, 2, or 11.

From the Message Profiles panel, you press F4 (Add) to add a profile. A Profile Details panel appears. You can press F8 (Forward) to scroll forward through the panels or enter the panel index number at the Command prompt to select a specific panel. (Pressing F11 (Panels) displays a list of panels and panel index numbers.)

Use the following panels in this example:

- Profile Details
- System Specification
- Job Name Specification
- OS Codes Specification

The following panels show the completed message profile:

```
PROD------------------- EventView : Profile Details -------------MCPROFIL-0000

Command ===>                                                  Function=UPDATE

+---------------------- Message Classification Profile -----------------------+
| Name ... CICSMESSAGES     ID ..... 126 (1 - 128)                            |
| Description .... Messages for all production CICS Jobs_____________________ |
+-------------------------------------------------------------------------------+

+ Profile Status ------------------------------------------------------------+
| Profile Status ... INACTIVE (Active/Inactive)                              |
```

```
PROD----------------- EventView : System Specification -----------MCPROFIL-0000
Command ===>                                                  Function=UPDATE

+---------------------- Message Classification Profile -----------------------+
| Name ... CICSMESSAGES     ID ..... 126 (1 - 128)                            |
| Description .... Messages for all production CICS Jobs                      |
+-------------------------------------------------------------------------------+
+-----------------------------------+ +-----------------------------------+
| Systems to be Included            | | Systems to be Excluded            |
+-----------------------------------+ +-----------------------------------+
| _______________ _______________ | | ETST_____________ _______________ |
```

```
PROD---------------- EventView : Job Name Specification ----------MCPROFIL-0000
Command ===>                                                  Function=UPDATE

+---------------------- Message Classification Profile -----------------------+
| Name ... CICSMESSAGES     ID ..... 126 (1 - 128)                            |
| Description .... Messages for all production CICS Jobs                      |
+-------------------------------------------------------------------------------+
+-----------------------------------+ +-----------------------------------+
| Job Names to be Included          | | Job Names to be Excluded          |
+-----------------------------------+ +-----------------------------------+
| CICSPRD1:CICSPRD9 CICSTST*________ | | CICSPRD4_________ _______________ |
```

```
PROD--------------- EventView : OS Codes Specification -----------MCPROFIL-0000
Command ===>                                                  Function=UPDATE

+---------------------- Message Classification Profile -----------------------+
| Name ... TAPEMOUNTS       ID ..... 127 (1 - 128)                            |
| Description .... Messages for all production CICS Jobs                      |
+-------------------------------------------------------------------------------+
+-------------------------------------------------------------------------------+
| Routing Codes    ( Y =Include, N =Exclude, Blank =Don't care )               |
|                    1         2         3         4         5         6      |
|           12345678901234567890123456789012345678901234567890123456789012345  |
|   1-64 => YY        Y                                                       |
```

Example: Profile All Messages

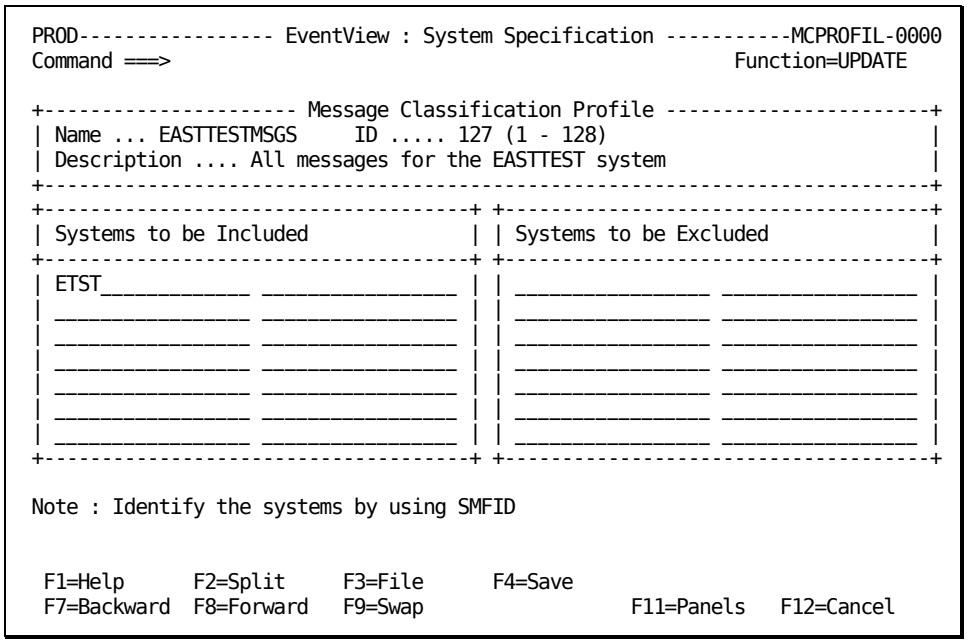
Note: This example is for illustration only. In a multisystem environment, if you have not implemented EventView message rules to provide a high level of message suppression, using this message profile can result in a very high volume of message flow to the consolidated console.

In this example, you want to create a profile to capture the messages for all connected systems. You allow all messages by excluding a system that is not part of the network. The following shows an example where DMMY is the excluded system.

```
PROD---------------- EventView : System Specification -----------MCPROFIL-0000
Command ===>                                                  Function=UPDATE

+---------------------- Message Classification Profile -----------------------+
| Name ... ALLMESSAGES      ID ..... 127 (1 - 128)                            |
| Description .... All messages                                               |
+-----------------------------------------------------------------------------+
+-----------------------------------+ +-----------------------------------+
| Systems to be Included            | | Systems to be Excluded            |
+-----------------------------------+ +-----------------------------------+
| ________________ ________________ | | DMMY____________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
| ________________ ________________ | | ________________ ________________ |
+-----------------------------------+ +-----------------------------------+

Note : Identify the systems by using SMFID


 F1=Help      F2=Split     F3=File      F4=Save
 F7=Backward  F8=Forward   F9=Swap                 F11=Panels   F12=Cancel
```

Example: Profile Messages for a Particular System

In this example, you want to create a profile to capture the messages for a particular system. The following shows an example where ETST is the system whose messages you want to monitor.



Change the Activation Status of a Message Profile

A message profile must have an ACTIVE status before it can be activated for use. If you only want to change the Profile Status Field for a profile, change the value directly from the Message Profiles panel.

To change the value to ACTIVE, type **A** next to all the profiles you want to update and press Enter.

The value in the Status column for the profiles changes to ACTIVE.

To change the value to INACTIVE, type **I** next to all the profiles you want to update and press Enter.

The value in the Status column for the profiles changes to INACTIVE.

Activate Message Profiles

Note: The message profile activation process can halt the region for a short period of time. After this period, the region continues from where it left off, without loss of control or data. However, delays might occur in responses to system activities. Unless the activation of the message profiles is of a high priority, perform this task when the system is not busy.

After you have created or updated message profiles, you must activate (load) them in each of the linked regions before they can be used.

To activate message profiles, use *one* of the following methods:

- Select the **A** option on the System Console Consolidation panel, or enter the **/EADMIN.C.A** path (available to focal point regions only).
- Enter **ACTIVATE** at the prompt on the Message Profiles panel (available to focal point regions only). To display the panel, enter the **/EADMIN.C.M** path.
- Action the CCONSOLIDATN parameter group (available to focal point and subordinate regions). To display the list of parameter groups, enter the **/PARMS** shortcut.

A region only activates profiles with a status of ACTIVE.

Profiles with a status of ACTIVE also become active automatically whenever the region is started. Profiles with a status of INACTIVE are not activated when the region is started.

Message Profile Size Considerations

If the total size of the profiles loaded is too large, activation of message profiles can fail. If the problem occurs, a message is generated to indicate by how much the size should be reduced. The ID of the message is either RMCCST11 or RMINWI36.

Note: For information about how to correct the problem, see the message online help.

Maintenance of Message Profile Definitions

In a focal point region, you can browse, update, copy, and delete message profile definitions from the Message Profiles panel.

Note: For information about how to assign message profiles to individual users, see the *Security Guide*.

Monitor Messages Using Consolidated Console

The console message consolidation facility enables authorized users to view console message traffic from multiple systems on a single console (referred to as a *consolidated console*). An authorized user can create *message profiles* that contain criteria to identify and classify messages. When you use a consolidated console, you use message profiles to select the messages for viewing. All messages that match the criteria of the profiles are displayed on your consolidated console.

Note: The facility is fully functional in focal point regions only. In subordinate regions, only local console message traffic is visible.

Message Monitor

The message monitor is based on Operator Console Services (OCS).

Prefix Messages with the System Name

Use the following command to specify whether you want your messages prefixed with the originating system name:

```
PROFILE AOMPRFSN={NO | YES}
```

For example, to prefix the displayed messages with the system name, enter PROFILE AOMPRFSN=YES.

The changed value is valid for the current session only. If you want to specify a value to use whenever you access the message monitor as a consolidated console, specify the value at the Message Monitor Message Formatting panel of your user profile.

Consolidated Console Setup Requirements

To use the consolidated console, you must be authorized to use OCS and AOM, and authorized to receive AOM messages. This information is specified in your user ID definition.

In addition, your user profile must be set up to receive the relevant messages.

Authorization Requirements

Your authority for using the consolidated console should be set up by the administrator.

If the User Access Maintenance Subsystem (UAMS) is used to manage authorization, enter the **/UAMS.B** path to browse your user ID definition.

The authorization requirements are as follows:

UAMS Panel (Page Number)	Field	Value
Access Authorities (3)	Operations Management	Y
	Operator Console Services	Y
OCS Details (5)	Initial OCS Command	-$RMCCOCS
AOM General Details (10)	AOM Message Receipt	Y
	Console Routing Codes	ALL
	Message Level Screening	ALL

Profile Requirements

To enable you to receive messages on a consolidated console, ensure that the following fields on the Message Monitor Message Receipt panel of your user profile have the values Y:

- Receive Unsolicited Messages
- Receive System Messages

To access your user profile, enter the **=U.UP** path.

Access the Consolidated Console

From the primary menu, enter **O** to access OCS. If the lower right of your screen is not displaying CC ON or CC PND, enter **CCON** to change the monitor to a consolidated console. If an RMCCOC07 message is displayed or if the status is CC PND, your console is unable to receive system messages because your profile is not suitable for the consolidated console.

The console starts displaying the messages that match the message profiles available to you. You must have at least one message profile enabled to view any message.

Notes:

- If console consolidation is disabled, you can monitor local messages only. (Message consolidation is enabled or disabled in the CCONSOLIDATN parameter group. For information about parameter groups, see the *Reference Guide*.
- You can also use the Command Entry facility as a consolidated console. To access the Command Entry panel, type **CMD** at a prompt, or press F5 from OCS. Enter **CCON** to turn on console message consolidation. The Command Entry facility keeps the messages that scroll off the panel, that is, you can bring those messages back onto the panel by pressing the F7 or F8 scroll function keys.

If the Console Does Not Display System Messages

If the console does not display system messages, use the following procedure to investigate the cause and correct the problem. You may not need to complete all of the steps if the problem is corrected before the end of the procedure.

1. Enter **PROFILE CC** and ensure that at least one of your message profiles is enabled.

   If a defined message profile is not accessible, check its status. When you load the profiles, only those with an ACTIVE status are loaded.

2. Enter **PROFILE** to display your console profile. Ensure that the values of the following profile parameters are as indicated:

   UNSOL

   Set to YES.

   AOMMSG

   Set to YES.

   AOMMSGLV

   Set to other than NONE.

   You can correct the value by issuing the following command for each relevant parameter:

   PROFILE *profile-parameter=parameter-value*

   The changed value is valid for the current session only. If you want to change a value permanently, change it in your user profile.

   If the AOMMSG and AOMMSGLV parameters are not displayed or if the AOMMSGLV parameters cannot be changed, you need to update your user ID definition according to the guidelines in the next step; otherwise, proceed to Step 4.

   Note: If you are not authorized to correct errors found in the following steps, report the errors to the administrator.

3. Enter the **/UAMS.B** path to browse your user ID definition. Ensure that your AOM General Details panel displays the following values:

   AOM Message Receipt

   Set to Y.

   Console Routing Codes

   Set to ALL.

   Message Level Screening

   Set to ALL.

   When these values are correct, you can then update the corresponding profile parameters as indicated in the previous step.

   You should also ensure that the Initial OCS Command field on your OCS Details panel has the value $RMCCOCS. This command ensures that the message monitor is always presented to you as a consolidated console.

   Ensure that console consolidation is activated by the CCONSOLIDATN region parameter group.

Use Message Profiles to Select the Messages to Monitor

In a consolidated console, you can use predefined message profiles to select the messages you want to monitor.

To access your list of message profiles, issue the **PROFILE CC** command. The Private Message Profile Control panel displays the list of message profiles that you can use to profile your consolidated console.

The initial status of the message profiles are as follows:

- If you disabled the message profile in your user profiles, the profile appears with a status of DISABLED.
- If you enabled the message profile in your user profiles, the profile appears with a status of ENABLED or PENDING.

Use the **D** or **E** action codes to disable or enable selected profiles for this session with your consolidated console. Enabled profiles have a status of PENDING if your monitoring environment cannot receive the requested messages (for example, if the UNSOL profile parameter has a value of NO indicating that you cannot receive unsolicited messages).

You can use the F10 (MsgFlow) function key to switch the value of the AOMMSG profile parameter between NO and YES. This parameter indicates whether you can receive AOM messages. The value must be YES for you to receive messages at your consolidated console.

Use the F11 (LstSort) function key to sort the list of message profiles by name or by ID. The initial sort is by name.

Reply to a WTOR Message From the Consolidated Console

Note: You can reply to resource or service related WTOR messages from the status or graphical monitor by using the W command.

Use the following command to reply to a local WTOR message:

```
SYSCMD REPLY wtor-id,reply-text
```

Use the following command to reply to a remote WTOR message:

```
ROUTE DOMAIN=domain-id SYSCMD REPLY wtor-id,reply-text
```

The value of *domain-id* is the domain ID of the region that sends the remote WTOR message. The ID appears as a prefix to the message if the value of your PREFSYS profile parameter is YES.

For information about the SYSCMD and ROUTE commands, see the online help.

Note: You can use the EQUATE command to reduce the typing required when issuing a command. For example, you can equate text as follows:

```
EQUATE / SYSCMD REPLY+
EQUATE domain-id ROUTE DOMAIN=domain-id SYSCMD REPLY+
```

You can then use the following commands to reply respectively to a local or a remote WTOR message:

```
/ wtor-id,reply-text
domain-id wtor-id,reply-text
```

For information about the EQUATE command, see the online help.

To ensure that the required text strings are always equated in the region, specify the EQUATE commands in the EQUATES parameter group.

Exit the Consolidated Console

Exit your consolidated console in one of the following ways:

- To exit the consolidated console and remain in OCS or your Command Entry panel, issue the **CCOFF** command. You can use the CCON command to return to the consolidated console.
- To exit the consolidated console and return to the previous panel, press F3.

Chapter 28: Configuring the Event Simulator

This section contains the following topics:

Event Simulator

The event simulator enables you to correctly assess the impact of a loaded system image on the operations of the local system. The MSGAWARENESS parameter group controls the availability of the simulator.

By using the simulator, you can generate simulated events and review the returned results. A simulated event returns the expected results. It does not invoke the actual actions. The results of the simulation identify the following affected active definitions:

- Resource definitions
- EventView rules
- Consolidated console message profiles
- Other product-specific definitions and records

Generate Simulated Events

To generate simulated events

1. Enter **/EADMIN.E** at the prompt.

   The Simulated Events List appears.

2. Do *one* of the following:

   - If the required event definition is not on the list, press F4 (Add) to define and generate the event.
   - If the required event definition is on the list, do one of the following:
     - Use the SV or SI action code to simulate one or more defined events.
     - Enter **ALL SI** at the prompt to simulate all defined events.

Define a Simulated Event

To define a simulated event

1. From the Simulated Event List, enter **/EADMIN.E** at the prompt.
2. The simulated event definitions appear.
3. Press F4 (Add). You can also use the C action code to open a copy of an existing definition that you can modify.

   The Simulate Message panel appears.
4. Specify the message you want to simulate and the type of information you want returned.

   You can enter a question mark (?) in the Message Text field to display the list of messages learned by the region. If you select a message from the list, the panel is automatically updated for any associated job name, routing codes, and descriptor codes.
5. Do *one* of the following:

   - If you want to generate the simulated event, press F6 (Simulate). To save the results, press F3 (File) or F4 (Save).
   - If you do not want to generate the simulated event now, press F3 (File) to save the definition for later use.

   Note: Filed message definitions are *not* retained across region restarts.

Results of Event Simulation

The results of event simulation are returned on the Simulation Results List panel.

```
PROD-------- Automation Services : Simulation Results List --------------------
Command ===>                                                 Scroll ===> CSR

                 S/B=Browse Definition U=Update Definition C=Collapse E=Expand
    Simulated Message Details:
     Message Text ... $HASP170 PRT1     INTERRUPTED
     Jobname ........ JES2           Jobtype ....... JOB  Message Type ... WTO
     Route Codes .... 7              Desc. Codes ... 4

    ************************** Simulation Results ****************************
    Dflt EventView Ruleset ..... $$$$$URS
         Default ruleset processing performed as per:
            Message Delivery ... YES           Perform Mods.? .. YES
            Perform Actions? ... YES           Log Activity? ... NO
            Collect Statistics?  YES           Learn New Msgs?   NO

    Miss No Consolidated Console profiles hit for the following reason:
            No Consolidated Console Profiles Hit

    Hit  PRT Resource Name ..... PRT1         JES Printer PRT1
         Monitor Message ....... $HASP170 PRT1*
         Extended Actions:
```

For the previous example, the results indicate that the:

- Messages are passed on by the $$$$$URS rule set but no rules are triggered
- PRT1 resource becomes degraded but no actions are invoked

If the results are not satisfactory for a displayed definition, you can use the U action code to update it. For example, if you enter U next to the PRT resource line, the Status Monitor Message Details panel displays. You can then update the appropriate resource message rule.

Summarize the Results

When a simulated event affects many definitions, the results are displayed over several panels; however, you can summarize the results.

To summarize the results, enter **ALL C** at the prompt.

The results appear as a list of affected definitions.

Note: You can use the ALL E command to display all details of all the results. You can use the C and E action codes to change the view of selected results.

Maintenance of Simulated Event Definitions

You can browse, update, copy, and delete simulated event definitions. To delete all definitions, enter **ALL D** at the prompt.

Note: If you update the message attributes, you are creating a message. Previously stored simulation results are not retained.

Chapter 29: Setting Up the Alert Monitor

This section contains the following topics:

Access Alert Administration

Alert Monitor administration lets you define Alert Monitor interfaces, filters, and formats that apply to all users.

You perform Alert Monitor administration functions from the Alert Monitor : Administration Menu.

To access Alert Monitor administration functions, enter **/ALADMIN** at the prompt.

The Alert Monitor : Administration Menu appears.

```
PROD---------------- Alert Monitor : Administration Menu --------------/ALADMIN
 Select Option ===>

    I   - Define Trouble Ticket Interface                    ALTTI
    D   - Define Trouble Ticket Data Entry                   -
    F   - Define Filters                                     ALFILT
    L   - Define List Formats                                -
    MIF - Invoke Alert Filter Migration Utility              -
    ST  - Alert Monitor Self Test                            ALTEST
    X   - Exit
```

Alert Monitor Trouble Ticket Interface

The Alert Monitor provides an interface that lets you send alert information in the form of a *trouble ticket* to another interface automatically or manually.

The Alert Monitor supports the following interfaces for raising trouble tickets:

Electronic Mail

Sends an email describing the problem to a problem management application or a particular person. This method can be used to send tickets to multiple problem management applications.

Custom

Lets you write your own NCL procedure to deliver the trouble ticket to an application by whatever means you choose. For example, you can do the following:

- Invoke a REXX procedure, and pass alert variables.
- Send to any external interface, for example, problem-management product.
- Send to MVS system facilities, for example, system console, data sets, SMF user records, or batch jobs.
- Invoke applications, for example, FTP.

Service Desk

Creates a new CA Service Desk request from the alert details.

Note: If your CA Service Desk installation is configured with the optional ITIL application, incidents are created instead of requests.

Note: You can choose one interface only.

If you want the operator to supply information when requesting the creation of a ticket, you also need to set up the trouble ticket data entry definition.

Define a Trouble Ticket Interface

If you want to enable operators to raise trouble tickets on alerts, you must define the trouble ticket interface.

To define a trouble ticket interface between the Alert Monitor and another application

1. From the Alert Monitor Administration Menu, select option **I** - Define Trouble Ticket Interface.

   The Alert Monitor : Interface Definition panel appears.

2. Enter the type of interface that you want to define in the Interface Type field.

   Note: To obtain a selection list of valid values, enter **?** in this field.

3. Press F6 (Action).

   A panel appears where you can define an email (see page 363), custom (see page 365), or CA Service Desk (see page 366) interface. The type of panel displayed varies, depending on the interface type that you specified.

Define an Email Trouble Ticket Interface

This option enables alert details to be sent using email.

Note: To enable this option, you must ensure that your Systems Programmer enables SMTP support on this region's TCP/IP stack.

To define an email trouble ticket interface

1. Enter **/ALADMIN** at the prompt.

   The Alert Monitor : Administration Menu appears.

2. Select option **I** - Define Trouble Ticket Interface.

   The Alert Monitor : Trouble Ticket Interface Definition panel appears.

3. Enter **EMAIL** in the Interface Type field, and press F6 (Action).

   The Email a Trouble Ticket panel appears.

4. Leave the &$USRNAME variable in the Mail Address field. The variable works with the default trouble ticket data entry definition (see page 368) to specify the email address of the trouble ticket system to which you want to send the message. The data entry definition lets operators specify the address.

   If you do not want operators to be able to change the address, specify the address in the Mail Address field and delete the fields in the data entry definition.

   Complete the other fields:

   Host Name

   (IBM's Communications server only) Specifies the host name of this system. This is usually the NJE node name.

   SMTP Node Name

   (IBM's Communications Server only) Specifies the NJE node name on which the SMTP server runs. This is usually the same value as the Host Name.

   SMTP Job Name

   (IBM's Communications server only) Specifies the name of the address space in which SMTP runs. This is usually SMTP.

   SMTP DEST Id

   (CA TCPaccess CS for z/OS only) Specifies the destination ID in the REMOTE parameter of the SMTP statement in member APPCFG*xx* of the PARM data set.

   Exit Procedure Name

   Specifies the name of an NCL exit routine, in which you can customize the email message sent by this trouble ticket.

   Subject

   Specifies the heading to display as the subject of the email message.

   Enter Mail Text Below

   Specifies the mail message text. Press F1 (Help) for information about variables.

   Press F3 (File).

   The definition is saved.

Define a Custom Trouble Ticket Interface

You use the custom interface if you want to use your own procedure to send trouble tickets.

To define a custom trouble ticket interface

1. Enter **/ALADMIN** at the prompt.

   The Alert Monitor : Administration Menu appears.

2. Select option **I** - Define Trouble Ticket Interface.

   The Alert Monitor : Trouble Ticket Interface Definition panel appears.

3. Enter **CUSTOM** in the Interface Type field, and press F6 (Action).

   The Custom Trouble Ticket panel appears.

4. Complete the following fields:

   Procedure Name

   Specifies the name of your NCL procedure for delivering tickets.

   Important! The NCL procedure must be in the COMMANDS concatenation for your region. To list the concatenation, enter **/ALLOC**.

   Enter Parameters Below

   Specifies any parameters that you want the NCL procedure to receive. Press F1 (Help) for information about variables.

Example: Define a Custom Trouble Ticket Interface

This example shows an interface that uses the distributed CA SOLVE:Central exit, $RMPB06S, to send tickets to a CA SOLVE:Central region with the ACB name SOLVPROB and other required values.

```
PROD----------------- 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
         parm1=value1
         parm2=value2
**** ***************************** BOTTOM OF DATA ******************************
```

Example: Invoke a REXX procedure

This example shows how you can use the NCL procedure to execute a REXX procedure.

The NCL statement that executes a REXX procedure in your environment has the following format:

REXX *rexx_procedure parm_1 … parm_n*

Define a CA Service Desk Trouble Ticket Interface

The CA Service Desk integration (see page 379) feature must be implemented before you can send alert trouble tickets to it; otherwise, all alert forwarding requests fail.

Note: For more information, see the *CA Common Services for z/OS Service Desk Integration Guide*.

To define a CA Service Desk trouble ticket interface

1. Enter **/ALADMIN** at the prompt.

   The Alert Monitor : Administration Menu appears.

2. Select option **I** - Define Trouble Ticket Interface.

   The Alert Monitor : Trouble Ticket Interface Definition panel appears.

3. Enter **SERVICEDESK** in the Interface Type field, and press F6 (Action).

   The Service Desk Trouble Ticket Setup panel appears.

4. Complete the following fields:

   CA Service Desk Server Web Services HTTP URL

   Specifies the HTTP URL of the web services definitions on the target CA Service Desk server.

   Default: If left blank, the CA Common Services CAISDI/soap component chooses the default server.

   Note: This URL points to the web services definitions that CAISDI/soap invokes to create the requests. This is not the same as the URL that is used to log on to CA Service Desk. Contact your CA Service Desk administrator for the URL.

   CCI Sysid

   Specifies the CCI system ID of the LPAR where the CAISDI/soap task is active. This is the SYSID name specified in the CAICCI startup JCL.

   Default: If left blank, the local CAICCI on this LPAR locates a suitable CAISDI/soap task.

   Request Description Format

   Specifies whether the USD Request Description field is produced with HTML formatting or in plain text (TEXT).

   Default: HTML

   Note: In most cases, leaving the CA Service Desk Server Web Services HTTP URL and CCI Sysid fields blank will suffice. This lets the CAISDI/soap component use its default values.

   Press F3 (File)

   The definition is saved.

Set Up the Trouble Ticket Data Entry Definition

If you want the operator to supply information when creating a trouble ticket, you need to set up the ticket data entry definition.

To set up the trouble ticket data entry definition

1. Enter **/ALADMIN** at the prompt.

   The Alert Monitor : Administration Menu appears.

2. Select option **D** - Define Trouble Ticket Data Entry.

   The Trouble Ticket Data Entry Definition panel appears.

3. 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 create multiple field names by replicating the key variables linked by default.

   Note: For more information about completing this section, press F1 (Help).

Example: Data Entry Definition to Prompt Operators for Email Address

The following example shows a definition that prompts the operator to identify the receiver of the ticket.

```
PROD--------- 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 email)"
0005  REQUIRED=YES
0006  LENGTH=40
**** ***************************** BOTTOM OF DATA ****************************
```

Considerations

To make the panel more user-friendly, you can change this panel by creating a trouble ticket data entry definition.

Example: Data Entry Definition

Here is an example of the data entry definition.

```
PROD--------- Alert Monitor : Trouble Ticket Data Entry Definition ------------
Command ===>                                    Function=Update Scroll ===> CSR
AMTTDED08 TROUBLE TICKET DATA ENTRY DEFINITION SAVED
**** ****************************** TOP OF DATA *******************************
0001 FIELD NAME=$USRX
0002  VALUE=
0003  DESC="Press F6 to send the ticket"
0004  COMMENT=
0005  REQUIRED=NO
0006  LENGTH=0
**** ***************************** BOTTOM OF DATA ******************************
```

```
PROD---------------- Alert Monitor : Trouble Ticket Details -------------------
Command ===>

Press F6 to send the ticket ..
```

Implement Trouble Ticket Interface for Multiple Email Addressees

You can use an exit procedure, together with the trouble ticket interface and data entry definitions, to implement an interface that prompts operators for more than one email address.

To implement a trouble ticket interface for multiple email addressees

1. Create an NCL procedure with the following statements, and save it to your TESTEXEC:

   ```
   &IF .&$USRNAME1 NE . &THEN +
   &$AMTADDRESS1 = &$USRNAME1
   &IF .&$USRNAME2 NE . &THEN +
   &$AMTADDRESS2 = &$USRNAME2
   ...
   ```

   Note: The number of &IF statements sets up the number of addresses you want to provide.

2. Update the trouble ticket data entry definition (see page 368) with the following fields:

   ```
   FIELD NAME=$USRNAME1
   VALUE="&$AMTADDRESS1"
   DESC="EMAIL ADDRESS #1"
   COMMENT=""
   REQUIRED=NO
   LENGTH=40
   FIELD NAME=$USRNAME2
   VALUE=""
   DESC="EMAIL ADDRESS #2"
   COMMENT=""
   REQUIRED=NO
   LENGTH=40
   ...
   ```

   Notes:

   - The number of fields corresponds to the number of email addresses in the procedure you created.
   - The value &$AMTADDRESS1 must be specified.

3. Define the email trouble ticket interface (see page 363) specifying a default address in the Mail Address field and the name of the procedure in the Exit Procedure Name field.

   The trouble ticket interface prompts operators for email addresses when they enter TT next to an alert.

Example: Implement a Trouble Ticket Interface for Two Email Addresses

To create an NCL procedure named EXAMPLE that sends emails to two addresses

1. Create an NCL procedure named EXAMPLE with the following statements, and save it to the TESTEXEC:

```
&IF .&$USRNAME1 NE . &THEN +
&$AMTADDRESS1 = &$USRNAME1
&IF .&$USRNAME2 NE . &THEN +
&$AMTADDRESS2 = &$USRNAME2
...
```

2. Enter **/ALADMIN** at the prompt.
3. Select option **D** - Define Trouble Ticket Data Entry.
4. Complete the panel as follows:

```
PROD-------- Alert Monitor : Trouble Ticket Data Entry Definition ------------
Command ===>                                    Function=Update Scroll ===> CSR

****** ***************************** TOP OF DATA ******************************
000001 FIELD NAME=$USRNAME1
000002  VALUE="&$AMTADDRESS1"
000003  DESC="EMAIL ADDRESS#1"
000004  COMMENT=""
000005  REQUIRED=NO
000006  LENGTH=40
000007 FIELD NAME=$USRNAME2
000008  VALUE=""
000009  DESC="EMAIL ADDRESS #2"
000010  COMMENT=""
000011  REQUIRED=NO
000012  LENGTH=40
****** **************************** BOTTOM OF DATA ****************************
```

5. Enter **/ALTTI** at the prompt.
6. Enter **EMAIL** in the Interface Type field and press F6 (Action).
7. Complete the panel as follows:

```
PROD--------------- Alert Monitor : Email A Trouble Ticket -Columns 00001 00072
Command ===>                                    Function=Update Scroll ===> CSR

Mail Address              defaultaddress@tt.com_____________________________
Host Name      (IBM)      HOSTNAME
SMTP Node Name (IBM)      NODENAME
SMTP Job Name  (IBM)      SMTP____
SMTP DEST Id (TCPaccess)  ________
Exit Procedure Name       EXAMPLE_
Subject                   &$AMDESC_____________________________________________

                             Enter Mail Text Below

****** ***************************** TOP OF DATA ******************************
```

Result

When an operator enters **TT** next to an alert, they are prompted for an email address as follows:

```
PROD--------------- Alert Monitor : Trouble Ticket Details --------------------
Command ===>

Email Address #1 ... defaultaddress@tt.com
Email Address #2 ...
```

Define Alert Monitor Filters

You can filter the alerts displayed on the Alert Monitor by applying a set of criteria to each of the fields in the alert. The filters that you create can be named and stored for later use, using the FILTER command.

To define an Alert Monitor filter

1. Enter **/ALFILT** at the prompt.

   The Alert Monitor : Filter Definition List panel appears.

2. Press F4 (Add).

   The Alert Filter panel appears.

3. Complete the following fields:

   Name

   Specifies the name of the filter.

   Description

   Describes the filter.

   Filter Expression

   Specifies the Boolean expression that determines what alerts are passed by the filter. For more information about creating Boolean expressions, press F1 (Help).

   Press F3 (File)

   The Alert Monitor filter is saved.

Alert Monitor Display Format

The Alert Monitor display format determines the information displayed for the alerts on the Alert Monitor, for example, the columns and the order in which they appear.

You specify the Alert Monitor display format on the List Format panel.

For each type of information you want to display on the Alert Monitor, you need to specify two items: a static heading and a variable that contains the required information.

You can create a multiscreen Alert Monitor display with up to 10 screens, enabling you to display more information on the monitor. The screens can be accessed by pressing the F11 (Right) or F10 (Left) function keys from the monitor.

The variable contains the information you want to display. The name of a variable can sometimes be longer than the data to display. You can enter a shorter name and then make that shorter name an alias of the actual name.

Create the Alert Monitor Display Format

You can create format definitions that can be used to customize the information displayed on the Alert Monitor.

To create the Alert Monitor display format

1. Enter **/ALADMIN.L** at the prompt.

   The List Definition List appears.

2. Enter **C** beside the DEFAULT display format definition.

   A copy of the List Description panel appears.

3. Enter a new value in the List Name field to identify the new definition, and update the Description and Title fields.

   Press F8 (Forward) three times.

   The List Format panel appears.

4. Enter column headings and variables using the text editor to specify the information to display on the Alert Monitor.

   Note: For more information about the text editor, press F1 (Help).

5. (Optional) Press F5 (Fields) to create aliases.

6. Press F3 (File).

   The details are saved.

Enable Alerts from External Applications

You can generate alerts (to view on the Alert Monitor) from external applications such as CA OPS/MVS.

Note: To use this feature, the SOLVE SSI must be active.

Follow these steps:

1. Enter **/PARMS** at the prompt.

   The Parameter Groups list appears.

2. Enter **U** next to the $NM ALERTS parameter group in the Interfaces category.

   The ALERTS - Alert Monitor Interface panel appears.

3. Enter **YES** in the Enable External Alerts? field.

4. Press F6 (Action).

   The changes are activated immediately.

5. Press F3 (File).

   The settings are saved.

Alert Forwarding

Alerts are displayed on the Alert Monitor; however, you can also forward them to the following platforms:

- EM Console in CA NSM
- UNIX platforms as SNMP traps
- CA NetMaster NM for SNA or Tivoli NetView (TME10) systems, as generic alert NMVTs
- CA Service Desk servers (see page 379), as CA Service Desk requests or incidents

You can apply filter criteria to forward different types of alerts to different platforms.

Alert forwarding does not require manual intervention; it occurs automatically when the alert is created.

Implement Alert Forwarding

You implement alert forwarding by using Customizer parameter groups.

Note: TNGTRAP and SERVICEDESK do not have clear alert events. Only alert open and considerations are forwarded.

To implement alert forwarding

1. Enter **/PARMS** at the prompt.

   The Customizer : Parameter Groups list appears.

2. Enter **U** in front of the ALERTS parameter group in the Interfaces category.

   The parameter group opens for update.

3. Complete the following field:

   Dest Type

   Specifies the type of alert forwarding to use.

   Press Enter.

   The fields dynamically change to match the specified destination type.

4. Review the fields, and update as required.

   (Optional) Press F8 (Forward), and repeat Step 3 for each Definition ID.

   Note: Press F1 (Help) for information about the fields.

5. Press F6 (Action).

   The changes are applied.

6. Press F3 (File).

   The settings are saved.

SNMP Trap Definition

The MIB definition for alerts forwarded as SNMP traps is provided in member $AMTRAP, supplied in the CC2DSAMP data set. You can download this member to your UNIX system and compile it.

Note: When copying this member to your UNIX system, you can 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)

Forward to Tivoli NetView

To receive alerts in a Tivoli NetView region, the CNMCALRT task must be defined and active. The alerts are formatted as Operator Notification generic alerts.

To forward alerts to Tivoli NetView

1. Check the DSIDMN (or DSIDMNB) member in the DSIPARM PDS. DSIPARM.PDS is allocated by the Tivoli NetView started task.
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 z/OS software alert forwarding function.

Forward to CA NSM

To format the traps sent to a CA NSM management platform, you must load the rules to reformat the alert messages for display on the EM Console.

To forward alerts to the EM Console in CA NSM

1. Use FTP to download the message definition rules in binary mode from the UNIEMMSG member of your CC2DSAMP data set created at installation. For example, using the Windows FTP client from the prompt:

   ```
   >ftp myhost
   Connected to myhost.mycompany.com.
   User (myhost.mycompany.com:(none)): user01
   331 Send password please.
   Password: xxxxxxxx
   230 USER01 is logged on. Working directory is "/u/users/user01".
   ftp>cd "prefix.ppvv.CC2DSAMP"
   250 The working directory "prefix.ppvv.CC2DSAMP" is a partitioned data set
   ftp>binary
   200 Representation type is Image
   ftp> get uniemmsg uniemmsg.txt
   200 Port request OK.
   125 Sending data set prefix.ppvv.CC2DSAMP(UNIEMMSG) FIXrecfm 80
   250 Transfer completed successfully.
   ftp: 3200 bytes received in 0.67Seconds 4.77Kbytes/sec.
   ftp>quit
   ```

2. From a Windows prompt on the destination CA NSM EM Server, load the message definition rules from the downloaded file. Enter the following command at the prompt to define the rules to event management:

   ```
   cautil -f "uniemmsg.txt"
   ```

3. Enter the following command to load the rules:

   ```
   oprcmd opreload
   ```

4. In your region, set the alert forwarding destination to TNGTRAP.

Alert Forwarding to CA Service Desk

Before you can forward alert details to CA Service Desk to create requests, you implement CA Service Desk Integration.

Note: For more information, see the *CA Common Services for z/OS Service Desk Integration Guide.*

Do not forward any alerts to CA Service Desk until integration is completely and correctly implemented; otherwise, all alert forwarding requests to CA Service Desk fail.

Suppress State Change Alerts

The region automatically generates an alert for a resource that changes state. You can suppress the alerts for selected state changes. You can also specify the severity levels of the generated state change alerts.

To suppress automatically generated state change alerts

1. Enter the **/PARMS** panel shortcut.

   The Parameter Groups panel appears.

2. Enter **F STATECHANGE**.

   The cursor locates the STATECHANGE parameter group.

3. Enter **U** beside the group.

   The group opens for updating.

4. Blank out the fields for the states you want to suppress alerting. For example, if you want to suppress alerting for state changes to UNKNOWN, blank out the Unknown field.

   Press F6 (Action).

   The region stops generating alerts for those state changes.

5. Press F3 (File).

   The group is updated with the changes.

State Change Alerts

State change alerts are based on RMAM001*xx* messages. These messages are defined in CAS, and you can customize them.

You can maintain messages from the Message Definition List panel. The shortcut to the panel is /CASMSG.

Note: For information about how to maintain messages, see the *Managed Object Development Services Guide*.

CA Service Desk Integration

The CA Service Desk Integration feature creates CA Service Desk requests from forwarded alerts and alert trouble tickets, or both.

You can define multiple forwarding destinations to CA Service Desk, with each one pointing to a different CA Service Desk server.

Note: If your CA Service Desk installation is configured with the optional ITIL application, incidents are created instead of requests.

Many CA Technologies mainframe products use this feature to consolidate their problem notification on a specified CA Service Desk server. The feature uses W3C SOAP (Simple Object Access Protocol) to invoke web services provided by CA Service Desk.

Software Requirements

CA Service Desk Integration has the following software requirements:

- CA Service Desk r11 or r11.1
- CA Common Services for z/OS r11, specifically the CAICCI and CAISDI/soap components

How Requests Are Created

To create a CA Service Desk request from an alert, the following internal steps are performed:

1. The CA Common Services for z/OS CAICCI component is used to pass the request to the CA Common Services for z/OSCAISDI soap component. CAISDI/soap is a z/OS-hosted SOAP client.
2. CAISDI/soap sets up an IP connection with the CA Service Desk server, then uses HTTP/HTTPS requests to invoke the necessary web services on the CA Service Desk server to create the new request or incident.
3. The request or incident number is returned and annotated in the alert.

Request Assignment

By default, CA Service Desk requests created by your region appear as *assigned* requests, with an assignee and an end user of System_NetMaster_User.

Your CA Service Desk administrator can customize the product templates to change these assignments to suit your organization.

Request Updating

A CA Service Desk request created from an alert is static. It reflects the alert details that were current at the time it was created.

Note: A CA Service Desk request is not subsequently updated with any changes to the alert, nor closed when the corresponding alert is closed.

Requests are intended for initial problem notification to a wider and more general data center audience. CA Service Desk Integration complements the functions of the Alert Monitor; it does not replace the Alert Monitor.

Every request (if HTML format is used) contains hyperlinks to various WebCenter pages, including the Alert Monitor. You should use the Alert Monitor for real-time dynamic alerting functions.

For recurring alerts, a request is created for the first occurrence only.

Other Ways to Create Requests or Incidents

In addition to Alert Monitor forwarding and trouble tickets, CA Service Desk requests or incidents can also be created from the following functions:

- Operator Console Services (OCS)
- MVS console

Operator Console Services

The OCS command SDCREATE can be used to create a CA Service Desk request from the OCS command line, for example:

```
SDCREATE Problem xxx has occurred
```

This attempts to open a request on the default CA Service Desk server. The request will have a severity of 4, and a summary and description of *Problem xxx has occurred*. Like other requests raised, it is assigned to System_NetMaster_User.

Use the SDTEST command to check if a default server is implemented.

MVS Console

As with any product command, you can also issue SDCREATE from the MVS system console, for example:

```
F rname,SDCREATE Problem xxx has occurred
```

Request Description Format

By default, your region generates CA Service Desk request description content in HTML format.

By default, CA Service Desk does not render embedded HTML directives in the request description field. To support this, you must customize your CA Service Desk server. This task involves customizing the detail_cr.htmpl form to add keeptags and keeplinks support.

Note: For more information, see the *Service Desk Modification Guide*.

Implement the Alert History Function

The Alert Monitor retains data in an alert history file. You can define the time period that alerts are retained.

To specify the time period that alerts are retained

1. Enter **/PARMS** at the prompt.

   The Customizer : Parameter Groups list appears.

2. Enter **U** in front of the $NM ALERTHIST parameter group in the Files category.

   The ALERTHIST - Alert History File Specification panel appears.

3. Complete the following fields:

   Days to Retain Alerts

   Specifies the number of days that you want to retain alerts in the history file.

   Limits: 999 days

   Default: 7 days

   Time of Day for Alert Purge

   Specifies the time of day (in the format hh.mm) at which alerts older than the value in the Days to Retain Alerts field are deleted from the history file.

   Press F6 (Action).

   The changes are applied.

4. Press F3 (File).

   The settings are saved.

Reorganize Files and Monitor Space Usage

Over time, the alert history file can become fragmented. You can reorganize the file to improve its efficiency.

To reorganize the Alert History database for optimum space usage

1. Copy (REPRO) the alert history file to a backup file.
2. Delete and redefine the original file.

Use the same attributes that were used when the file was defined at region setup. See the generated S01LCALC member in your INSTALL.JCL data set; this member has the original VSAM definition JCL for the file.

Monitor the amount of disk space used by the data set to estimate the optimal file size and optimal frequency of reorganization.

Example: Back Up Alert History File

This example backs up an alert history file.

```
//BKALERTH EXEC PGM=IDCAMS
//SYSPRINT DD   SYSOUT=*
//IN       DD   DSN=?prefix.ALERTH,DISP=SHR
//OUT      DD   SN=?prefix.ALERTH.BACKUP.SEQ,DISP=OLD
//SYSIN    DD   *
 REPRO INFILE(IN) OUTFILE(OUT)
/*
```

The sequential backup file has the following format:

```
DSORG=PS,RECFM=VB,LRECL=32756,BLKSIZE=32760
```

Extract Alert Data for Reporting

You can extract alert data from the Alert History database in a character separated values (CSV) format for processing by external reporting and analysis tools. The default field separator character is comma (,). You can change it in the ALERTHIST parameter group.

To extract alert data for reporting and analysis

1. Allocate a sequential data set with the following attributes:
   - LRECL is greater than or equal to 300 bytes.
   - RECFM is VB.
2. Enter **/ALHIST**.

   The History Menu appears.
3. Type **EX** at the prompt, and specify the data set name that you have allocated in the Extract DSN field.

   (Optional) If you want to limit the extracted data, select an Alert Monitor filter (see page 372) through the Filter Name field.

   Press Enter.

   The data is extracted to the specified data set.
4. Transfer the data set to your personal computer (PC) in ASCII format, and save it with an appropriate extension. (For example, if you plan to use Microsoft Excel to process the data, use the .csv extension.)

   The extracted data is saved in a text file.
5. Open the text file by using your preferred PC application.

   The extracted data is presented in your preferred format for analysis.
6. Analyze your data by applying facilities such as graphs and charts, tables, and macros.

Chapter 30: Setting Up the Initialization File

This section contains the following topics:

Generate an Initialization File

If you are deploying multiple regions, each region must be configured for its local environment. When you have configured your first region, you can build an initialization file from that region and then configure it for use with your other regions. This removes the need to customize each region with Customizer.

The tasks outlined below show how to configure a region from an initialization file. The initialization file is produced from a running region for your product.

To generate an initialization file

1. From the Primary Menu, enter **/CUSTOM**.

   The Customizer panel appears.

2. Select option G - Generate INI Procedure.

   The Customizer : Generate INI Procedure panel appears.

3. Enter the data set name and the member name of the file in the Generate INI File Details section.

   Note: The data set must be in the commands concatenation of the RUNSYSIN member for the region in which it is used.

4. Ensure that the member name and data set name are correct. Enter **YES** in the Replace Member? field if you are replacing an existing member.

5. Press F6 (Action).

   The initialization file is generated.

6. Make a note of the data set and member names and press F6 (Confirm).

   The details are saved.

How You Configure the Initialization File

The initialization file must be configured before it can be used for other regions. You can perform this configuration as follows:

- Configure an individual initialization file for each region.
- Configure a common initialization file for multiple regions.

You can use system variables and static system variables with both of these methods. The variables substitute for the initialization parameters in the INI file.

Configure a Common Initialization File

You can customize an initialization file using variables so that it can be used for multiple regions.

To configure a common initialization file

1. Create a data set that is available to every region to be initialized from the common initialization file, for example, PROD.INIFILES.
2. Add the newly created data set to the COMMANDS concatenation of the RUNSYSIN member to every region to be initialized from the common initialization file.

   Note: RUNSYSIN is located in TESTEXEC.
3. Copy the initialization file generated into the new INIFILES data set.
4. Use your TSO editing tool to open the initialization file in edit mode.
5. Replace the relevant generated variables in the initialization file with the following system variables:

   &ZDSNQLCL

   The local VSAM data set qualifier.

   &ZDSNQSHR

   The shared VSAM data set qualifier.

   &ZACBNAME

   The primary VTAM ACB name used by the region.

   &ZDSNQLNV

   The local non-VSAM data set qualifier.

   &ZDSNQSNV

   The shared non-VSAM data set qualifier.

   &ZNMDID

   The domain identifier.

&ZNMSUP

The system user prefix.

6. Replace the relevant generated variables in the initialization file with the z/OS static system symbols as follows:

   &SYSCLONE

   The short name for the system.

   &SYSNAME

   The name of the system.

   &SYSPLEX

   The name of the sysplex.

   &SYSR1

   The IPL VOLSER.

7. Save the changes to the initialization file.

Configure Individual Initialization Files

You can customize an initialization file generated from one region so that it can be used for another region.

To configure an individual initialization file for each region

1. Use your TSO editing tool to open the initialization file in edit mode.
2. Substitute the parameters in the initialization file with *one* of the following:
   - Hard-coded data set names for the region in which the file is used
   - System variables

   This enables the initialization file to work in regions with different data sets than the region in which it was generated.
3. Save the changes to the initialization file.
4. Copy the initialization file to the region's TESTEXEC or one of the other libraries in the COMMANDS concatenation.
5. Repeat steps 1 to 4 for each initialization file needed.

Note: The region from which the original initialization file was generated should have the same product sets as the destination regions that will use that initialization file.

Start Your Region from an Initialization File

The name of the initialization file must be specified by the INIFILE parameter in the RUNSYSIN member.

Updating your RUNSYSIN member causes your region to set its initialization parameters from the initialization file. All Customizer parameter settings are overwritten.

To update your RUNSYSIN member

1. Use a text editor to open your RUNSYSIN member.
2. Insert the line PPREF='INIFILE=*membername*' into your RUNSYSIN member.
3. Save the member.

Chapter 31: Administering a Multisystem Environment

This section contains the following topics:

Multisystem Operation

Your 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. 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 region on that system.

In a multisystem environment, each 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 link and synchronize the regions.

Links in a Multisystem Environment

The link established between two 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 combination of the following communications protocols: VTAM, TCP/IP, and EPS. VTAM is the default.

For each region, the MULTISYS parameter group specifies the available communication access methods. If TCP/IP is used, ensure that the SOCKETS parameter group is activated.

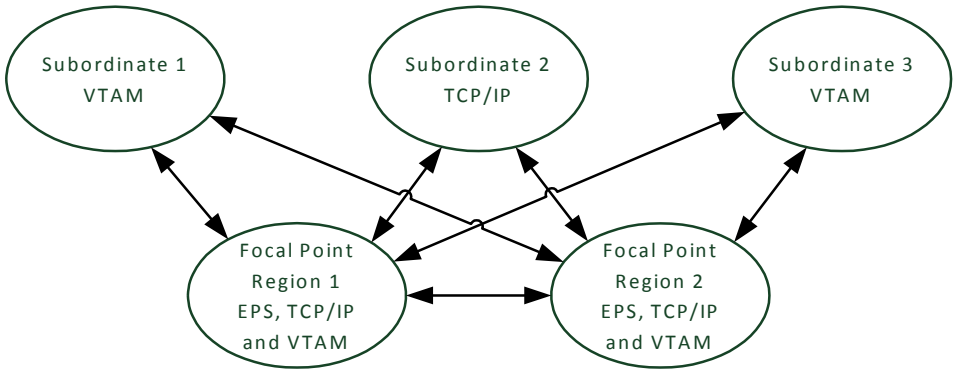
The INMC link between any two regions uses the access methods enabled by *both* regions (that is, the intersection of the two MULTISYS parameter groups). When multiple access methods are enabled, the link can use all these methods. This improves reliability because the link functions when one of the enabled methods is available.

When you plan your multisystem environment, 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.

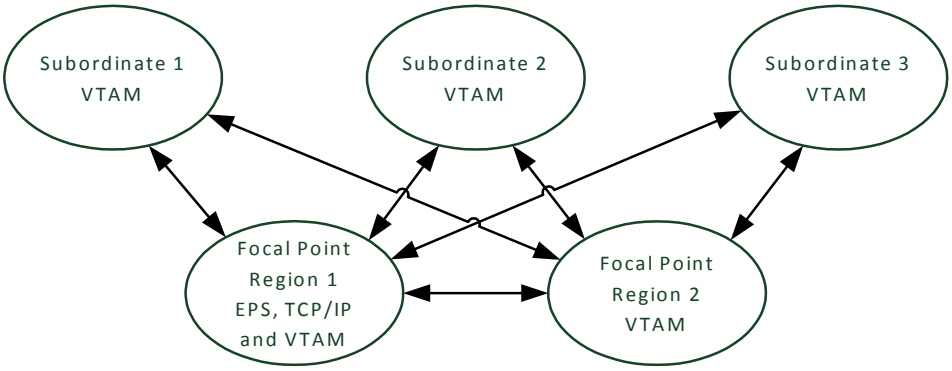
Example: Focal Point Regions Support All Access Methods

This example shows a multisystem link configuration when the focal point regions support ESP, TCP/IP, and VTAM. The subordinate regions can support any one of these access methods.



Example: One Focal Point Region Supports VTAM Only

This example shows a multisystem link configuration when a focal point region supports VTAM only. The subordinate regions must support VTAM.



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 CA NetMaster FTM 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
- When you link two regions, the knowledge base in the linking region is replaced by the knowledge base in the region to which you link. 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 link a standalone region into a multisystem environment only. 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.

How a Multisystem Environment Is Established

When you install your product, two databases are downloaded. These databases, which can be customized to suit your requirements, are:

- An icon panel database, where icon panel definitions are stored for the graphical monitor
- The RAMDB, where system image, resource, availability map, process, macro, command, and other definitions are stored

Together, these databases form the knowledge base.

Populate these databases with definitions specific to your environment. These definitions can include the system image definitions for any other regions that you want to install in your environment in the future.

As you establish regions, link the new regions to the first region by using the Link Region and Synchronize Database (see page 393) option. When databases are linked, future synchronization is automatic. Changes to the database in one region are sent to the databases in the linked regions that have visibility to those resources and system images.

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.

In a multisystem environment, you can monitor and control the resources in all linked regions from a single focal point.

Linked Regions and Database Synchronization

When the first region is created in your environment, two databases are downloaded and can be customized for your environment. Together, these two databases (the Automation Services database and the icon panel library) form the knowledge base.

To build a multisystem environment, you start by linking two regions, and then continue to link in any other regions. The linking process also synchronizes the knowledge bases of these regions.

Notes

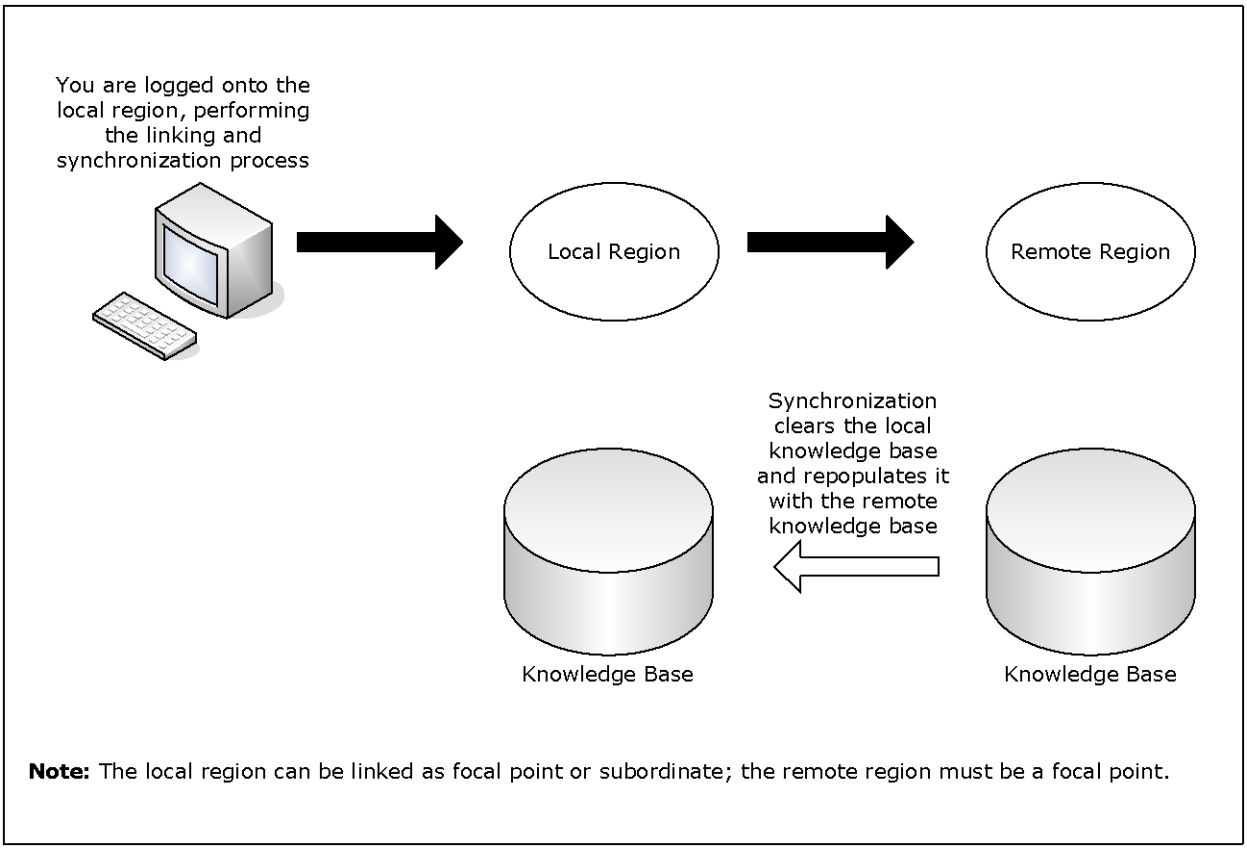
- For linked focal point regions, synchronization is complete and the focal point knowledge bases are identical.
- For linked subordinates, synchronization is complete only to the extent of the relevant definitions in the knowledge base. For example, a subordinate knowledge base does not contain all 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. This remote region must be a focal point region. When you link a region into an existing multisystem environment, that region must be a stand-alone region.

Important! During the linking and synchronization process, the knowledge base in the local region is overwritten by the knowledge base from the remote focal region. If the local knowledge base has customized definitions that you want to retain, transmit these definitions to the remote knowledge base before you link the regions. Otherwise, the local knowledge base definitions are overwritten and lost.

Note: If the local region terminates during the linking and synchronization process, the local knowledge base can become corrupted and you cannot restart the region. Replace the corrupted knowledge base with your backup, restart the region, and resynchronize the knowledge base. For more information about backups, see the *Reference Guide*.

The following illustration shows the link and synchronization operation.



Note: The local region can be linked as focal point or subordinate; the remote region must be a focal point.

After you link the regions, the knowledge bases are synchronized and remain synchronized. If you change the knowledge base in one region, the changes are propagated to the other regions.

Background User Considerations

When you establish a region, a UAMS background system (BSYS) user ID for that region is automatically defined. The background user ID comprises the four-byte region domain ID, followed by the characters BSYS. To establish fully-functioning communication links 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 to UAMS, provided that the following conditions apply:

- You have UAMS maintenance authority on *all* the linked regions.
- The existing multisystem linked regions are active when the request is made.

If either of these conditions does not apply, then any required BSYS user IDs must be defined manually to UAMS. 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 in the local or the remote region. (The user ID of the person who requests the link and synchronize procedure must be defined in the local and remote regions.)
- The required BSYS user IDs are not defined in the local or the remote region.

Important! If you use an external security system, you must manually define the BSYS user IDs of the remote systems to your external security system.

Link and Synchronize Regions

Important! Do not add, update, or delete knowledge base records in any linked regions while synchronization is in progress. These changes may not be propagated to the new region. Before you perform synchronization, ensure that you back up the knowledge base.

To link and synchronize regions

1. Log on to the region to synchronize with the source (remote) region.

   The source region contains the knowledge base you want.

2. Enter **/MADMIN** at the prompt.

   The Multi-System Support Menu appears.

3. Select option **SD**.

   This establishes a link between the local region and another region, and updates the knowledge base of the current region.

   The Remote System Identification panel appears.

4. Complete the following fields:

   Primary Name

   Specifies the ACB name of the remote focal point region to which you want to link this region.

   Role in Multi-System Operation

   Specifies whether this region is a focal point region or a subordinate region. A focal point region must satisfy the following conditions:

   - The product sets in all focal point regions match.
   - At least one access method must be available.

   Subordinate System Image Name

   (Optional) If you specified subordinate, specify the name of the system image that is to be used by it.

   Important! Each subordinate is assigned a unique system image name, and it can use an image by that system image name only. When you build your environment for a subordinate, you must build the environment under the system image name specified during the linking operation.

   Subordinate regions are restricted to loading only system images with the name specified here. Different system image versions can be maintained under the system image name.

   Work Dataset

   (Optional) Specifies the VSAM data set to use to reduce the time for synchronization.

   The following fields specify the communication access methods to be used during synchronization. You can select any combination of the access methods; however, you can only select an access method if it is enabled in the MULTISYS parameter group.

   Use VTAM?

   (Optional) Specifies whether to use VTAM for communication.

   Use EPS?

   (Optional) Specifies whether to use EPS for communication.

   TCP/IP Host Name/Addr

   (Optional) Specifies the TCP/IP host name and address of the remote region.

Port Number

(Optional) Specifies the TCP/IP port number of the remote region.

5. Press F6 (Action) to initiate the linking process.

   A confirmation panel appears.

6. Press F6 (Confirm) to initiate region linking and knowledge base synchronization.

   A status panel appears.

   Note: 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.

Monitor the Synchronization Procedure

While the synchronization procedure is in progress, the Synchronize Database Status panel is refreshed automatically every 10 seconds. This panel can be refreshed manually at any time by pressing the Enter key.

To check the status of the synchronization

1. From the Multi-System Support Menu, select option L to view the administration task log.
2. Enter S beside the appropriate entry from the log to view the status of the task.

The administration task log may contain 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.

Knowledge Base Synchronization Maintenance

Automation Services maintains synchronization between linked knowledge bases by using a staging file.

When a knowledge base update occurs, information about the update is stored in the staging file as follows:

- For an update in a focal point region, a separate update record is written for each affected linked region.
- For an update in a subordinate region, a single update record is written for a linked focal point region.

A record stays in the staging file until the update is performed successfully in the destined region. If the region is inactive, the record stays in the staging file until the region is started.

Important! If the staging file becomes full, knowledge base synchronization cannot be maintained and the local region is unlinked automatically. A staging file can become full if a remote linked region remains inactive for an extended period of time. If an extended downtime is planned for a linked region, unlink the remote region before inactivation.

Display Linked Regions

To list the linked regions in your multisystem environment, enter **/LISTREG** at the prompt.

The Linked Regions panel displays the ACB names, the mode these regions are linked in, and a brief description of the linked regions. The panel also displays the status of the data flow traffic managers.

Press F11 (Right) to scroll right to display more information.

Unlink Regions

You may 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, ensure that you unlink it first. An unlinked region is a stand-alone region.

To unlink a region

1. Log on to the region you want to unlink and enter **/MADMIN.U** at the prompt.

   The Confirm Unlink Panel appears.

   Note: To cancel the unlinking procedure, press F12 (Cancel) now.

2. Press Enter to proceed with the unlinking procedure.

To relink a region, link that region with one of the regions in the multisystem environment.

Transmission of 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 cannot transmit a system image to a region in which the image is currently loaded. You cannot transmit and replace a rule set when the rule set is currently loaded in the remote (target) region.

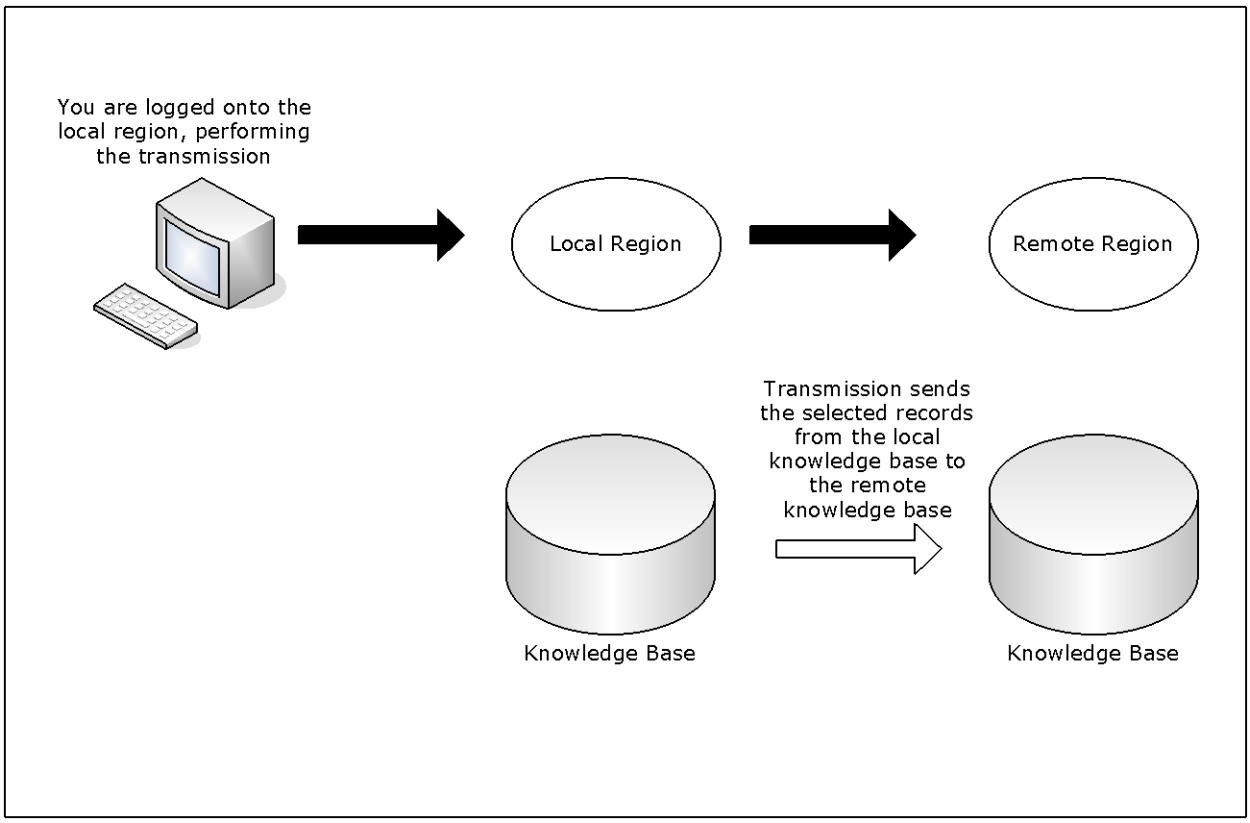
By specifying the appropriate transmission mode on the Remote System Identification panel, you can specify how to update the records in the remote region.

The following transmission modes are available:

- Replace (R) deletes any existing remote records, and then transmits the local records.
- Overlay (O) replaces existing remote records with the same name, adds records that do not exist, but does not delete any remote records.
- Merge (M) adds records that do not exist, but does not affect existing records in the remote knowledge base.

Transmit Records

The following illustration shows the transmit operation.



To transmit knowledge base records

1. Log on to the region from which you want to transmit the records.
2. Enter **/MADMIN** at the prompt.

   The Multi-System Support Menu appears.
3. Specify the option you want at the prompt and press Enter.

   A Remote System Identification panel appears.
4. Specify the ACB name (primary name) of the region to which you want to transmit records.

   If you specified the TI, TS, or TR option, go to Step 5. If you specified any other transmission options, go to Step 6.

5. Complete the following fields:

   System Name

   Specifies the name of the system to transmit. Applies to option TI only.

   Version

   Specifies the version of the system to transmit. Applies to options TI and TS only.

   Ruleset Name

   Specifies the name of the rule set to transmit. Applies to option TR only.

6. Do *one* of the following:

   - If you want to replace a set of records or all elements of a component, enter REPLACE in the Transmission Mode field.
   - If you want to update a region by adding new records without updating existing records, enter MERGE in the Transmission Mode field.
   - If you want to update a region by adding new records and updating existing records, enter OVERLAY in the Transmission Mode field.

7. Specify the communication access methods to use for transmitting the selected records. You can enable any combination of the access methods.

8. Press F6 (Action) to select the specified option.

   If a selection list appears, go to Step 9. If the Confirm Transmit panel appears, go to Step 11.

9. Do *one* of the following:

   - If you selected option TC with a transmission mode of REPLACE, enter **S** next to the categories that you want to transmit.
   - If you selected option TC with a transmission mode of MERGE or OVERLAY, enter **S** next to the categories that you want to transmit.
     To select specific definitions in a category for transmission, perform the following steps:

     a. Enter **L** (List) next to the category to list the definitions.

     b. Enter **S** next to the definitions to transmit.

   - If you selected other transmission options with a transmission mode of MERGE or OVERLAY, take *one* of the following actions:

     - To transmit all definitions, press F4 (All).
     - To transmit specific definitions, enter **S** next to the definitions that you want to transmit.

10. Press F6 (Transmit).

    A Confirm Transmit panel appears.

11. Press Enter to confirm transmission.

    A status panel appears, showing the progress of the transmission.

    Note: If you exit the status panel, you can check the status of the task by viewing the administration task log. Before you exit, note the task number for future reference.

Chapter 32: Implementing Print Services

This section contains the following topics:

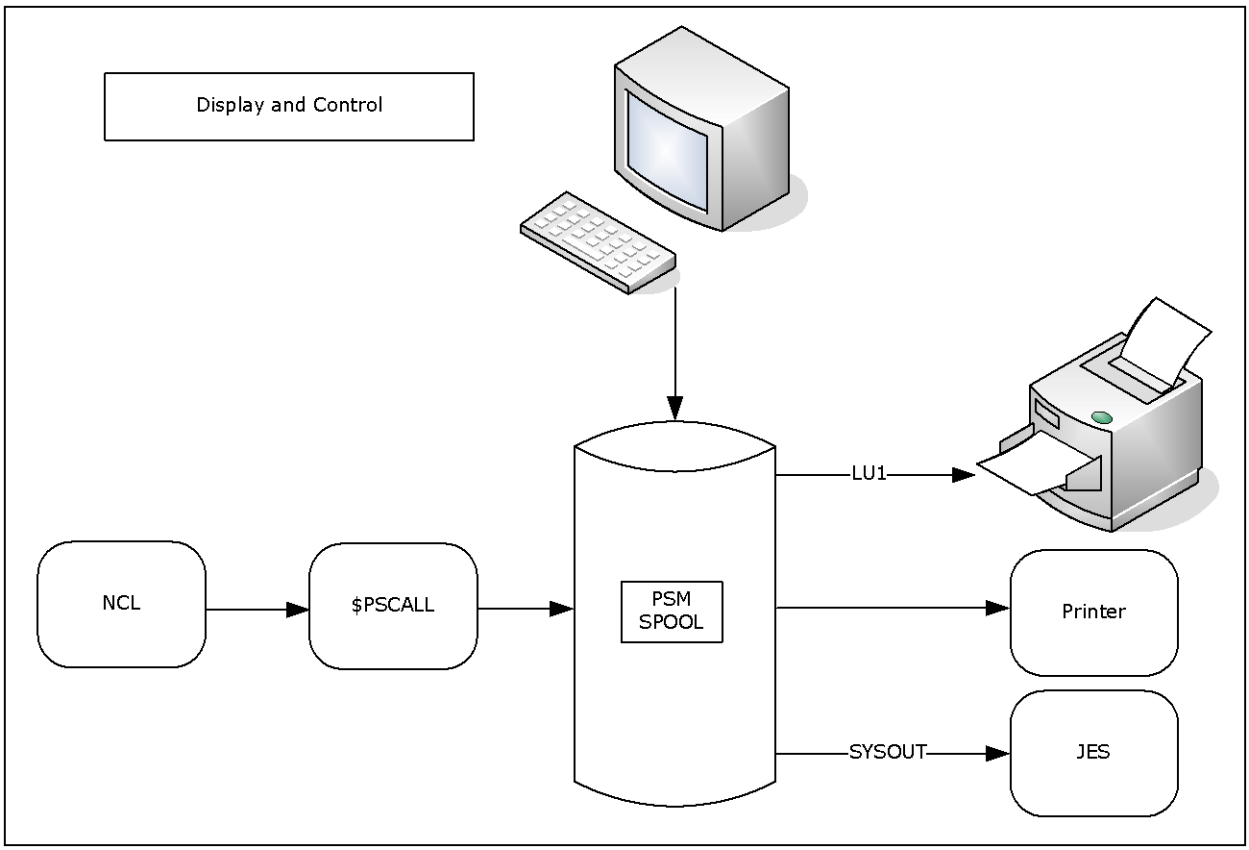
Print Services Manager

Print Services Manager (PSM) allows you to specify the format of a print request and on which printer it is printed. Print requests can be viewed online before or after printing and can be redirected to files rather than printers.

PSM provides the following features, which can be customized to suit your requirements:

- Printer definition facilities
- Form definition maintenance
- Setup definition maintenance
- Default printer assignment maintenance
- Alias printer name definitions
- Banner page customization on output
- Spooled print request browsing, retention, and redirection to a different printer
- Integration with NCL-based components

The following illustration shows the different ways that PSM can be used to control printing requirements.



Access PSM

The customizable functions of PSM are accessed from the PSM : Primary Menu.

To access PSM, enter **/PSM** at the prompt.

Note: You can also access PSM directly by invoking the $PSCALL NCL procedure from OCS or an installation written NCL procedure. The PSM NCL interface is described in the *Network Control Language Reference Guide*.

Add a Printer Definition

A printer definition defines where, how, and on what paper output is printed. A printer definition is required for each printer at which output is printed.

To add a printer definition

1. Enter **/PSMPRTR** at the prompt.

   The PSM : Printer Definition List appears.

2. Press F4 (Add).

   The PSM : Printer Definition panel appears.

3. Complete the fields, as required.

   Note: For information about the fields, press F1 (Help).

4. Press F3 (File).

   The definition is saved.

List Printer Definitions

You can display a list of all the printer definitions defined for your region. This lets you browse and perform maintenance on the listed definitions.

To list all printer definitions, enter **/PSMPRTR** at the prompt.

Add a Form Definition

A form definition is required for each type of paper on which output is printed. The Form Definition Menu is used to set up and administer these form definitions.

To add a form definition

1. Enter **/PSMFORM** at the prompt.

   The PSM : Form Definition List appears.

2. Press F4 (Add).

   The PSM : Form Definition panel appears.

3. Complete the fields and press F3 (File).

   The form definition is saved.

   Note: For information about the fields, press F1 (Help).

List Form Definitions

You can list all of the form definitions defined for your region and then browse and perform maintenance on them.

To list all form definitions, enter **/PSMFORM** at the prompt.

Add Control Characters

Control characters are sent to a printer before or after (or both) the output is printed. They are defined in setup definitions.

To add control characters

1. Enter **/PSMSET** at the prompt.

   The PSM : Setup Definition List appears.

2. Press F4 (Add).

   The PSM : Setup Definition panel appears. To access the second panel of the setup definition, press F8 (Forward).

   Complete the fields, as required.

   Note: For information about the fields, press F1 (Help).

3. Press F3 (File).

   The setup definition is saved.

List Control Characters

You can display a list of all the setup definitions defined for your region. This list lets you browse and perform maintenance on the listed definitions.

To list control characters, enter **/PSMSET** at the prompt.

Add a Default Printer for a User ID

Each user ID in your region can be assigned a default printer. Default printer assignments let you define the printer to which output is sent whenever a user ID does not specify a printer.

To add a default printer for a user ID

1. Enter **/PSMDFTP** at the prompt.

   The PSM : Default Printer Assignment List appears.

2. Press F4 (Add).

   The PSM : Default Printer Assignment panel appears.

3. Complete the following fields:

   User ID

   Specifies the User ID of the user to whom the printer is assigned a default.

   Printer Name

   Specifies the name of the printer to which this user's printing is sent.

   Press F3 (File).

   The default printer assignment is saved.

List Default Printers

You can display a list of all the default printer assignments defined for each user ID. This list lets you browse and perform maintenance on the listed definitions.

To list default printers, enter **/PSMDFTP** at the prompt.

Clear the Printer Spool

Print requests are retained on the print spool if an error occurs during printing or if HELD is specified on the PSM : Print Request panel. The PSM clear spool panel is used to clear print requests from the print queue.

Note: This function is available to authorized users only.

To clear the print spool

1. Enter **/PSMADMN** at the prompt.

   The PSM : Administration Menu appears.

2. Enter **CS** at the prompt.

   The PSM : Clear Spool panel appears.

3. Complete the following field:

   Date

   Specifies that all print requests added to the spool before or on this date are deleted.

   Press F6 (Action).

   The print requests are deleted.

Exits to Send Print Requests to a Data Set

Two printer exit procedures are distributed with your product. Each writes the output for a print request to a data set. The procedure $PSDS81X can be customized to specific site requirements. The procedure $PSDS81Z offers the same functionality with improved performance, but cannot be customized. The target data sets for both procedures can be sequential or partitioned.

Parameters that control the operation of the exit are defined in the Exit Data portion of the printer definition. Procedures that pass data to PSM for printing can override the exit data specified in the PSM printer definition.

The procedures use the parameters contained in the exit data to do the following:

- Determine the target data set
- Determine how to process a data line with a skip amount of zero
- Set the length of the lines print

How the Procedures Process a Print Request

The procedures read each line of print data and write it directly to the nominated data set. Each print line is analyzed according to skip control before processing. This continues until all lines of data for the print request have been received from PSM and written to the nominated data set.

$PSDS81X and $PSDS81Z Parameters

The $PSDS81X and $PSDS81Z exits have the following keyword parameters:

```
  DSN=datasetname
[ DISP={ SHR | OLD | NEW | MOD } ]
[ LRECL={ n | 80 } ]
[ SKIP0={ NEWLINE | DISCARD | DESTRUCTIVE |
          NONDESTRUCTIVE } ]
[ CYL= pri [,sec] [,dir] ]
[ TRK={ pri [,sec] [,dir] | 15,5 } ]
[ BLKSZ= n ]
[ STORC= storclas ]
[ MGMTC= mgmtclas ]
[ DATAC= dataclas ]
[ VOL= volser ]
[ UNIT={ unit | SYSALLDA} ]
[ RECFM={ F | FB | V | VB } ]
```

DSN=*datasetname*

Specifies the target data set name. If the data set is partitioned, the member name must be included or the data set is corrupted.

You can use the following symbolics in the *datasetname* parameter:

- &DAY is the day of the week (for example, MON).
- &YY is the two-digit representation of the year (for example, 11).
- &YYYY is the four-digit representation of the year (for example, 2011).
- &MM is the two-digit representation of the month (for example, 02).
- &MON is the three-character representation of the month (for example, JAN and FEB).
- &DD is the day of the month.
- &HHMMSS is the time.
- &HH is the hour.
- &MIN is the minute.
- &JOBID is the job ID.
- &JOBNAME is the job name.
- &NMID is the region ID.
- &NMDID is the region domain ID (DID).
- &GRPNAME is the sysplex name.
- &SYSID is the system ID.
- &SYSNAME is the system name.
- &USERID is the requesting user ID.

Symbolics are delimited by a period (.) or another symbolic (that is, &YY&MM. is the same as &YY.&MM.). Symbolics are also allowed in a member name.

Example:

```
DSN=NM.&SYSID..&USERID..D&YY&MM&DD..T&HHMMSS..DATA
```

For example, this specification can resolve to the following data set name:

```
DSN=NM.SYSA.MYUSER.D040915.T144505.DATA
```

DISP={ SHR | OLD | NEW | MOD }

Specifies the disposition of the output data set.

- SHR specifies shared use of the data set.
- OLD specifies exclusive use of the data set.
- NEW allocates a new data set.
- MOD appends the output in the file.

Default: SHR

LRECL={ *n* | 80 }

Specifies the output record length.

Limits: 1 through 250

Default: 80

SKIP0={ NEWLINE | DISCARD | DESTRUCTIVE | NONDESTRUCTIVE }

Specifies how to process a data line with a skip amount of zero.

- NEWLINE creates a line of data.
- DISCARD discards the line of data.
- DESTRUCTIVE causes the data to replace the existing data line.
- NONDESTRUCTIVE overlays the data on the existing data line, but only where blanks were present on the existing data line. No existing non-blank characters are modified.

Note: The procedures ignore the following PSM print options: NEWPAGE and USCORE.

Default: NEWLINE

The following additional parameters are applicable when DISP=NEW is specified:

CYL=*pri,sec,dir*

Specifies the primary and secondary space allocation values in cylinders. If a partitioned data set is used, the parameter specifies the number of directory blocks.

TRK=*pri,sec,dir*

Specifies the primary and secondary space allocation values in tracks. If a partitioned data set is used, the parameter specifies the number of directory blocks.

Default: TRK=15,5

BLKSZ=*blocksize*

Specifies the block size.

STORC=*storclas*

Specifies the storage class.

MGMTC=*mgmtclas*

Specifies the management class.

DATAC=*dataclas*

Specifies the data class.

VOL=*volser*

Specifies the volume serial number.

UNIT= { *unit* | SYSALLDA }

Specifies the unit.

Default: SYSALLDA if volser is specified

RECFM= { F | FB | V | VB }

Specifies the record format.

Default: FB

Printer Exit Definition Example

This example directs the output for a PSM print request, assigned to the printer named DSEXIT, to the member TEST1 in the data set PROD.PSM.DATA. The record length of this data set is 80. Overlay lines in the data are removed.

```
PROD1--------------------- PSM : Printer Definition --------------------------
Command ===>                                                  Function=BROWSE

  Printer Name ... DSEXIT
  Type ........... EXIT              (JES, VTAM, ALIAS, EXIT)
  Description .... Print to a data set
  Lower Case? .... YES               (Yes or No)
  Line Limit ..... 0                 (0 to 999999)
  Form Name .....+ FORM0
ALIAS Printer
  Real Name .....+                   (Real printer name)
JES Printer
  Destination ....                   (destid.userid)
  Output Class ...                   (A to Z, 0 to 9)
VTAM Printer
  LU Name ........
  Logmode ........
EXIT
  Exit Name ...... $PSDS81Z
  Exit Data ...... DSN=PROD.PSM.DATA(TEST1) LRECL=80
                   SKIP0=DISCARD
```

Note: Previous references to parameters WKVOL, CYL, and LIST in the exit data are no longer required. Remove them from the printer definition before using $PSDS81Z or $PSDS81X, or the print request fails.

Print-to-Email

The $PSEMAIL printer definition lets you email the output of a printing request. The request can be either an attachment or in the body of the email. When the output is sent as an attachment, the email uses the PS8803 message as its body and the PS8804 message as its salutation:

`Data attached for` *`email_subject`*

`Yours,`
`user_name`

user_name

Displays the sender name defined in UAMS.

You can maintain these messages from the Message Definition List panel. The shortcut to the panel is /CASMSG.

Note: For information about how to maintain messages, see the *Managed Object Development Services Guide*.

Appendix A: File Transfer Variables

This section contains the following topics:

Variables

File transfer variables enable you to extract information about file transfer events.You can use the variables to pass values to the following:

- Email trouble ticket interface
- FT schedules
- A failure event exit
- Automated actions in a file transfer rule
- Customizing alerts

Example: Use File Transfer Variable

The following example shows the use of variables in the text to be sent to the user, USER01, in response to an event that satisfies the file transfer rule.

```
PROD------------ File Transfer : User Notification Details --------------------
Command ===>
Short Description .. File transfer status and source
Notify ............. USER01
Text ............... &ZRFPRODUCT,&ZRFSRCADDR,&ZRFSTATUS,&ZRFSRCNAME,&ZRFSRCTYPE
```

File Transfer Variables

&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.

&ZRFDATATYPE

Contains the type of data set transferred by an IBM CS FTP server or FTP client (for example, ASCII, EBCDIC, IMAGE, DOUBLEBYTE, or UCS2).

&ZRFDSTYPE

Contains the data type transferred by an IBM CS FTP server or FTP client (for example, SEQ, PDS, or HFS).

&ZRFEDATE

Contains the date when the transfer ended in *yyyymmdd* format. See also &ZRFENDDATE.

&ZRFENDDATE

Contains the date when the transfer ended in *dd-mmm-yyyy* format. See also &ZRFEDATE.

&ZRFENDTIME

Contains the time when the transfer ended in *hh.mm.ss* format. See also &ZRFETIME.

&ZRFETIME

Contains the time when the transfer ended in *hhmmss* format. See also &ZRFENDTIME.

&ZRFFAILCODE

Contains the failure code.

&ZRFFAILDESC

Contains the failure description.

&ZRFFTPOPER

Contains the type of data transfer operation (command) handled by an IBM CS server or FTP client (for example, RETRIEVE, APPEND, STORE, or STOREUNIQUE).

&ZRFJOBNAME

Contains the name of the file transfer application.

&ZRFLATENCY

Contains the time between the CA XCOM Data Transport for z/OS transfer request and the start of the actual transfer.

&ZRFNETTYPE

Contains the type of protocol used for a CA XCOM Data Transport for z/OS transfer.

&ZRFPRODUCT

Contains the type of file transfer product.

&ZRFRECIN

Contains the number of records read during the transfer.

&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.

&ZRFSDATE

Contains the date when the transfer started in *yyyymmdd* format. See also &ZRFSTARTDATE.

&ZRFSRCADDR

Contains the address or node name of the source of the transfer.

&ZRFSRCFNAME

Contains the name of the source file.

&ZRFSTARTDATE

Contains the date when the transfer started in *dd-mmm-yyyy* format. See also &ZRFSDATE.

&ZRFSTARTTIME

Contains the time when the transfer started in *hh.mm.ss* format. See also &ZRFSTIME.

&ZRFSTATUS

Contains the monitored transfer status: START, END, or FAILURE.

&ZRFSTCJOBID

Contains the ID of the CA TCPaccess FTP Server for z/OS started task or job.

&ZRFSTIME

Contains the time when the transfer started in *hhmmss* format. See also &ZRFSTARTTIME.

&ZRFSTKNAME

Contains the TCP/IP stack name used by an IBM CS FTP server or FTP client.

&ZRFTGTADDR

Contains the address or node name of the target of the transfer.

&ZRFTGTFNAME

Contains the name of the target file.

&ZRFUSER

Contains the ID of the user that performs the transfer.

&ZRFXFRAMT

Contains the number of bytes transferred. See also &ZRFXFRDBYTES.

&ZRFXFRDBYTES

Contains the number of bytes transferred but converted to kilobytes, megabytes, gigabytes, or terabytes. See also &ZRFXFRAMT.

&ZRFXFRDRATE

Contains the transfer rate in kilobytes, megabytes, gigabytes, or terabytes per second. See also &ZRFXFRRATE.

&ZRFXFRDUR

Contains the time, in seconds, taken for the transfer.

&ZRFXFRID

Contains one of the following values:

- CA XCOM Data Transport for z/OS transfer ID
- CONNECT:Direct process name
- CONNECT:Mailbox ID and batch number
- FTP ID if specified in the FTPCNTL parameter group
- Generic data transfer ID
- CA SOLVE:FTS transmission definition name

&ZRFXFRRATE

Contains the transfer rate in bytes per second. See also &ZRFXFRDRATE.

&ZRFXFRTYPE

Contains the CA XCOM Data Transport for z/OS transfer type (EXECUTE or SCHEDULE).

&ZRFXMITMODE

Contains the transmission mode for a transfer handled by an IBM CS FTP server or FTP client (for example, BLOCKED, COMPRESSED, or STREAM.

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.

Appendix B: File Transfer Events Mapping

This section contains the following topics:

File Transfer Events

The format of the transfer identifier used for file transfer events varies between products. The mapping of the Transfer ID field is as follows:

CA XCOM Data Transport for z/OS

Transfer ID maps the CA XCOM Data Transport for z/OS transfer ID (request number).

CONNECT:Direct

Transfer ID maps the process name (process number).

CONNECT:Mailbox

Transfer ID maps the mailbox ID (batch number). For inbound transfers, Mailbox ID is extracted from $$ADD. For outbound transfers, Mailbox ID is extracted from batch ADD.

CA SOLVE:FTS

Transfer ID maps the transmission name.

CA TCPaccess FTP Server for z/OS

Transfer ID maps the CA TCPaccess FTP Server for z/OS started task or job name and CA TCPaccess FTP Server for z/OS allocated file transfer number in the following format:

server-name(*transfer-number*)

server-name

Specifies the JES started task or job name of the CA TCPaccess FTP Server for z/OS address space.

transfer-number

Specifies the file transfer number (in hexadecimal notation) allocated by CA TCPaccess FTP Server for z/OS.

CA TCPaccess CS for z/OS

Transfer ID is null unless a transfer ID is specified in the FTPCNTL parameter group.

IBM Communications Server

Transfer ID is null unless a transfer ID is specified in the FTPCNTL parameter group.

Note: For information about the fields in the event, see the online help.

Appendix C: Application Programming Interface

This section contains the following topics:

$RFCALL

$RFCALL is the API procedure used to call CA NetMaster FTM from external sources, for example, a user-written NCL procedure.

$RFCALL ACTION=CDCOMMAND

Use this call to issue CONNECT:Direct commands from CA NetMaster FTM.

This command has the following format:

```
$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}]
```

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.

Default: 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.

Default: 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 appears (YES) or returned as &RFRESP*n* variables (NO), where *n* is a sequence number starting from 1 (for example, &RFRESP1).

Default: 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:

0

Processing 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)'
```

$RFCALL ACTION=FORCEEND

Use this call to force a schedule that monitors file transfers to end.

This command has the following format:

```
$RFCALL ACTION=FORCEEND NAME=schedule-name
```

ACTION=FORCEEND

Indicates that a schedule is to be ended.

NAME=*schedule-name*

Specifies the name of the schedule resource to be ended.

Example

The following example shows how to force a schedule resource (identified by the &ZRMDBNAME knowledge base variable) to end.

```
$RFCALL ACTION=FORCEEND NAME=&ZRMDBNAME
```

Note: For more information about knowledge base variables, see the *Reference Guide.*

$RMDBAPI

You can use the $RMDBAPI procedure to manage your file transfer resource definitions. The $RMDBAPI lets you:

- 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 in an NCL procedure or as a command.

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.

You cannot directly update existing resource definitions using the API. You can create a new resource, including any updates required, and then delete the old resource. If you delete a rule set, the rules in the rule set are also deleted. If the rule set is active, the request is rejected.

$RMDBAPI SERVICE={ACTIVATE | INACTIVATE}

Use this call to change the status of a file transfer rule in a region to ACTIVE or INACTIVE. The region acts on the rule if the rule belongs to the loaded file transfer rule set.

This command has the following format:

```
$RMDBAPI SERVICE={ACTIVATE | INACTIVATE}
         RSNAME=ft-ruleset-name RMNAME=ft-rule-name
```

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:

0

Processing 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}

Use this call to maintain ResourceView definitions in the knowledge base.

This command has the following format:

```
$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]
```

Note: The next section lists the values for the *field-name-n* operands that are specific to CA NetMaster FTM. For more information about the operands, see the *Reference 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

This table lists the product specific resource field names that can be 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 Names
BSC Line Monitor Details	
QDEPTH	Queue Depth Threshold
AUTORES	Automatic Restart?
LINENM1 to LINENM5	Line Names
File Transfer Monitor Details	
IDLEALT	Stalled Time to Alert
IDLEDRP	Stalled Time to Flush
QDEST1 to QDEST5	Destination Nodes
QPNAME1 to QPNAME5	Process Names
Link Monitor Details	
LINKNME	Link Name

Field Names	Field Label on Panel
Queue Monitor Details	
QTYPE	Queue Type
QDEPTH	Queue Depth Threshold
QSTATUS	Process Status
QDEST1 to QDEST5	Destination Nodes
QPNAME1 to QPNAME5	Process Names
Remote Node Monitor Details	
RMSNNDE	Remote Node LU name (CA XCOM Data Transport for z/OS)
RMIPNDE	Remote Node TCP/IP Host Name/Addr (CA XCOM Data Transport for z/OS)
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 Names
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

Field Names	Field Label on Panel
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
FT 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)

Field Names	Field Label on Panel
State Change Exits	
STRPREX	Start of Pre-Processing
STRPRCX	Start of Processing
LNGXFRX	Longest Transfer Exceeded
ENDCMPX	End of Processing: All Transfers Complete
ENDINCX	End of Processing: All Transfers not Complete
ENDPOSX	End of Post-Processing
Define Exit Parameters	
STRPRE1 to STRPRE2	Parameters (for STRPREX)
STRPRC1 to STRPRC2	Parameters (for STRPRCX)
LNGXFR1 to LNGXFR2	Parameters (for LNGXFRX)
ENDCMP1 to ENDCMP2	Parameters (for ENDCMPX)
ENDINC1 to ENDINC2	Parameters (for ENDINCX)
ENDPOS1 to ENDPOS2	Parameters (for ENDPOSX)
Event Exits	
ASTARTEX	All Transfer Started
ACOMPLEX	All Transfer Completed
FAILUREX	Transfer Failure
Define Exit Parameters	
ASTARTP1 to ASTARTP2	Parameters (for ASTARTEX)
ACOMPLP1 to ACOMPLP2	Parameters (for ACOMPLEX)
FAILURP1 to FAILURP2	Parameters (for FAILUREX)
Additional Details	
ADDDET1 to ADDDET16	Additional Details

File Transfer Rule Set Fields

This table lists the file transfer rule set field names that can be used in the $RMDBAPI procedure.

Field Name	Field Label on Panel
File Transfer Rule Set	
SDESC	Description

File Transfer Rule Fields

This table lists the file transfer rule field names that can be 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

Field Names	Field Label on Panel
Alert Automated Actions	
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.	
	Important! 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	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*	FIELD NAME= and VALUE= on Alert Monitor : Trouble Ticket Data Entry Definition panel
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.	
	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

Field Names	Field Label on Panel
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
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.	
ADTXT1 to ADTXT5	Alert Text
ADRACT1 to ADRACT4	Alert Recommended Action

Appendix D: Generic Data Transfer Application Event Support

This section contains the following topics:

Set Up Data Transfer Products

Generic data transfer application event support lets you set up your own data transfer products to work with CA NetMaster FTM. To do this you must modify your data transfer application to collect the required event data and call the CA NetMaster FTM API code.

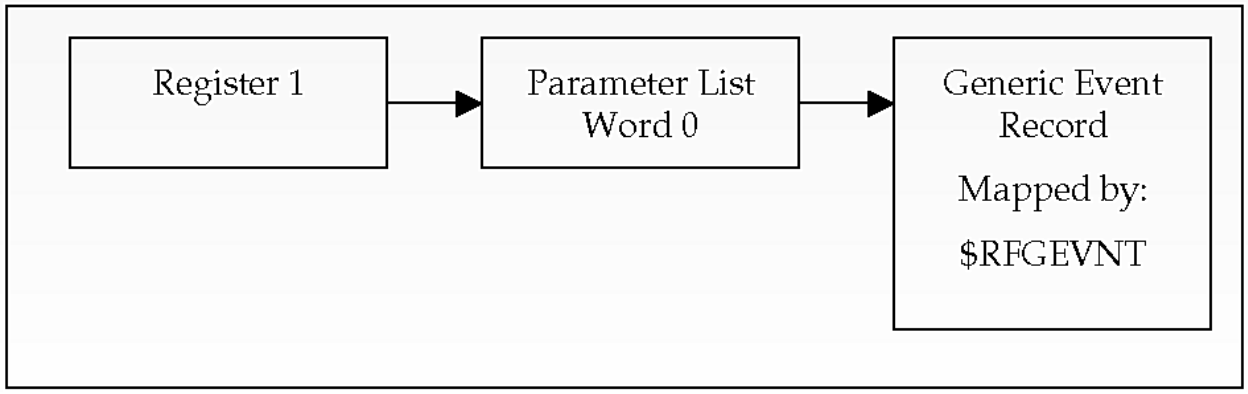
API Calling Requirements

Call NM000FGX (the API) once for each data transfer event. The standard linkage conventions apply. Ensure that NM000FGX is loaded either before the first call or by the first call.

The coding requirements are:

- Initialize the generic event (see page 439) record to spaces. The assembler macro provided generates the dummy section (DSECT) mapping the generic event.
- Set the various fields (see page 439) as needed (the Transfer Id and Event Type are mandatory).
- Place the address of the generic event record in the first and only word of a Parameter List.
- Set register 1 to point to a Parameter List.
- Call NM000FGX.
- NM000FGX returns a completion code through register 15. A return code of 0 indicates that the generic event was validated and forwarded through the Simple One-Shot Event Sender facility to the appropriate File Transfer regions. A return code other than 0 indicates an error condition.

The following diagram shows how the information is passed to the API:



Example Code

The following example shows a generic event API. You can add it to the relevant logic (for example, the exit) of your data transfer application.

Note: You can use the Browse Event and Transfer Details option on the History Data menu (/FTHIST.B) to verify that your modified application works correctly. Select List All File Transfer Events, and verify that the generic transfer events are visible.

```
*        .---------------------------------------.
*        | Event addressability                  |
*        |                                       |
*        |  Register assignments are sample only.  |
*        '---------------------------------------'
         LA    R9,EVENT
         USING GEVENT,R9
*
*        .---------------------------------------.
*        | Check if the NMFT API was Loaded      |
*        '---------------------------------------'
         L     R1,GEVTEP               Get NM000FGX entry point addr.
         LTR   R1,R1
         BNZ   BLDEVENT                Already loaded, Build event
         CLC   GEVTR15,=F'0'           Did a prior Load failed?
         BNE   ??????                    - Yes, report error (may be)
*
*        .-----------------------------------------------------.
*        |   I n i t i a l i s z a t i o n   (maybe)           |
*        |                                                     |
*        | LOAD the NMFT API module (NM000FGX)                 |
*        '-----------------------------------------------------'
         LOAD  EP=NM000FGX             LOAD
         ST    R15,GEVTR15             Save Return Code
         LTR   R15,R15                 Load failed ?
         BNZ   ??????                    - Yes, report error (may be)
         ST    R0,GEVTEP               Save Entry point
*
*        .---------------------------------------.
*        | Set NM000FGX parameter List           |
*        '---------------------------------------'
         ST    R9,GENEVTAD             Set Gen Event pointer
         OI    GENEVTAD,X'80'          Flag it as last in list
*
*        .---------------------------------------.
*        | The NMFT API was successfully Loaded  |
*        '---------------------------------------'
*        ooo      xxxxxx,xxxxxx        Whatever is required (i.e: WTO)
*        ...      ......
```

```
BLDEVENT EQU   *
*        .-------------------------------------------------.
*        |  A s s e m b l e   t h e   e v e n t   f i e l d s  |
*        |                                                 |
*        | Note: Register assignments are sample only.     |
*        '-------------------------------------------------'
*
*        .---------------------------------------.
*        | Initialise the Event record with spaces |
*        '---------------------------------------'
         LR    R4,R9
         LA    R5,GEVENTLG
         XR    R3,R3
         ICM   R3,B'1000',=C' '
         MVCL  R4,R2
*        .---------------------------------------.
*        |       Build the Event record          |
*        | Note: Only GEXFRID and GETYPE are     |
*        |       required all other fields are   |
*        |       Optional.                       |
*        '---------------------------------------'
         MVC   GEXFRID,=CL32'MYTRANSFER(00001)'       *< REQUIRED >*
         MVI   GETYPE,GESTART                         *< REQUIRED >*
         MVC   GEDXPRD,=CL24'ACME-DATASTAR Ver 06.2'
         MVC   GESRCNOD,=CL20'HEAD-OFFICE.NODE001'
         MVC   GESRCDAT,=CL256'NEW.YEARLY.RATES'
         MVC   GETRGNOD,=CL20'OVERTHERE.BRANCH'
         MVC   GETRGDAT,=CL256'/master/rates.data'
         MVC   GEUSRDAT,=CL32'Sample Start Event'
         MVC   GEUSERID,=CL16'ACCOUNTU0001'
*
CALLAPI  EQU   *                      RETURN OK
*        .-----------------------------------------------------------.
*        |  CALL the NMFT API module (NM000FGX)                      |
*        '-----------------------------------------------------------'
         LA    R1,PARMLIST             R1 -> Parameter list
         L     R15,GEVTEP              R15 -> NM000FGX
         BASSM R14,R15                 CALL EXIT MODULE
*
FGXRETRN EQU   *
         LTR   R15,R15                 Call returned in error ?
         BNZ   ??????                  - Yes, report error (may be)
*
*        ooo      xxxxxx,xxxxxx        Whatever
*        ...      ......
*
```

```
*       *--------*   D A T A   A R E A    *----------*
*       .---------------------------------------.
*       | NMFT API (NM000FGX) Parameter List      |
*       '---------------------------------------'
PARMLIST DS    0D                      NM000FGX Parameter List
GENEVTAD DS    A(0)                    Generic Event Address
*
*       .---------------------------------------.
*       | NMFT API (NM000FGX) Load control        |
*       '---------------------------------------'
GEVTEP   DC    F'0'                    NM000FGX Entry Point Address
GEVTRC   DS    0F                      RETURN CODES
GEVTR15  DC    F'0'                    - R15
GEVTR0   DC    F'0'                    - R0
*
*-------------------------------------------------------------------------*
*       Generic event                                                     *
*-------------------------------------------------------------------------*
EVENT    DS    0D
         DS    CL(GEVENTLG)' '
*
*-------------------------------------------------------------------------*
*     DSECTS                                                              *
*-------------------------------------------------------------------------*
         $RFGEVNT
```

Generic Event Record: Sample DSECT (Macro $RFGEVNT)

Build the Generic Event record before calling NM000FGX. The name (label) of the DSECT is GEVENT.

Three types of event are supported and mapped using the following distributed DSECT:

- Transfer Start (optional)
- Transfer End
- Transfer Failure

Field Name	Field Type	Usage	Hex Offset	Default	Required /Optional	Apply to Event Type
GERCVID	CL8	EPS Event Receiver ID	0000	$RFFTEVR	OPT	All
GEXFRID	CL32	Transfer ID	0008	-	REQ	All

Field Name	Field Type	Usage	Hex Offset	Default	Required /Optional	Apply to Event Type
GETYPE	CL1	Event Type S: START E: END F: FAILURE	0028	-	REQ	All
GETRACE	CL1	Trace Option T: TRACE ON N: TRACE OFF	0029	N	OPT	All
-	CL6	Spare	002A	-		
GEXBYTES	D	Bytes Transmitted	0030	-	OPT	End
GEXRECS	F	Records Transmitted	0038	-	OPT	End
GEFAILRC	F	Error Code	003C	-	OPT	Failure
GEFAILTX	CL128	Error Text	0040	-	OPT	Failure
GEDXPRD	CL24	File Transfer Product ID	00C0	STC Name	OPT	All
GEUSERID	CL16	User ID	00D8	STC Name	OPT	All
GESRCNOD	CL64	Transfer Source Node Name or Address	00E8	-	OPT	All
GESRCDAT	CL255	Transfer Source Data File	00FC	-	OPT	All
GETRGNOD	CL64	Transfer Target Node Name or Address	01FC	-	OPT	All
GETRGDAT	CL255	Transfer Target Data File	0210	-	OPT	All
GEXSTART	PL8	Transfer Start *hhmmssth*0*cyyddd*F	0310	For Start Event, set to Event Time For End/Failure event, set to 0	OPT	All
GEXEND	PL8	Transfer End *hhmmssth*0*cyyddd*F	0318	Event Time	OPT	End Failure
GEUSRDAT	CL32	User Data	0320	-	OPT	All

Notes:

- Data Transfer Start Events are optional. The Transfer ID and Event Type fields are mandatory.
- If you specify an IP address in the GESRCNOD or GETRGNOD field, it must be character-formatted.

EPS Event Receiver ID (Optional)

Applies to: All events

Default: $RFFTEVR

Validation: None

If specified, ensure consistency between calls to NM000FGX.

Transfer ID

Applies to: All events

Validation: If missing, NM000FGX forwards the event with Event Status set to XIDMISSING and returns with R15 set to 4. The transfer ID must be from 1 to 32 characters. The character set is validated and should include the following:

- A–Z
- a–z
- 0–9
- #
- @
- $
- Period “.”
- Underscore “_”
- Hyphen “-“
- Open parenthesis “(“
- Close parenthesis “)”

If the validation fails, NM000FGX forwards the event with Record Status set to XIDINVALID and return with R15 set to 8.

Event Type

Applies to: All events

Validation: The values supported are:

- S for Transfer Start
- E for Transfer End
- F for Transfer Failure

If missing or incorrect, NM000FGX forwards the event with $RFPPIMP Record Status set to TYPEINVALID and returns with R15 set to 12.

User data (Optional)

Applies to: All event

Default: None

Validation: None

Trace Option (Optional)

Applies to: All events

Default: N

Validation: The values supported are:

- T to turn on trace option for this event
- N to indicate no trace option for this event

If incorrect, N (*no trace*) is assumed.

When this field is set to T, NM000FGX issues the following message (WTO):
`RFGE01 iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii Type:t forwarded to:rrrrrrrr Status:sssssssss RC:nnnn`

where:

- *iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii* is the File Transfer ID (see Transfer ID)
- *t* is the event type (see: Event Type)
- *rrrrrrrr* is the EPS Event Receiver ID
- *sssssssss* is the event status
- *nnnn* is NM000FGX return code

Bytes Transmitted (Optional)

Applies to:	End event
Default:	None
Validation:	None

Records Transmitted (Optional)

Applies to:	End event
Default:	None
Validation:	None

Error Code (Optional)

Applies to:	Failure event
Default:	None

Specify a meaningful error code.

Error Text (Optional)

Applies to:	Failure event
Default:	None
Validation:	None

File Transfer Product ID (Optional)

Applies to:	All event
Default:	STC Name
Validation:	None

If specified, ensure its consistency between calls to NM000FGX.

User ID (Optional)

Applies to:	All event
Default:	STC Name
Validation:	None

If specified, ensure consistency between the related Start and End/Failures Events.

Transfer Source Node Name or Address (Optional)

Applies to:	All event
Default:	None
Validation:	None

If specified, ensure consistency between the related Start and End/Failures Events.

Transfer Source Data Name (Optional)

Applies to:	All event
Default:	None
Validation:	None

If specified, ensure consistency between the related Start and End/Failures Events.

Transfer Target Node Name or Address (Optional)

Applies to:	All event
Default:	None
Validation:	None

If specified, ensure consistency between the related Start and End/Failures Events.

Transfer Target Data Name (Optional)

Applies to:	All event
Default:	None
Validation:	None

If specified, ensure consistency between the related Start and End/Failures Events.

Transfer Start Time (Optional)

Applies to:	All event
Default:	For Start event—Event time For End/Failure event—None
Validation:	None

Transfer End Time (Optional)

Applies to:	End and Failure events
Default:	Event time
Validation:	None

Return Codes

NM000FGX returns the completion code through Register 15. The following table shows the settings:

R15 (Hex)	Reason	Event Forwarded	$RFPPIMP Record Status	WTO Issued
0 (00)	Normal Completion	Yes	COMPLETE	No
4 (04)	Transfer ID is missing	Yes	XIDMISSING	No
8 (08)	Transfer ID is invalid	Yes	XIDINVALID	No
12 (0C)	Event Type is invalid	Yes	TYPEINVALID	No
16 (10)	Parameter List Address (R1) is null	No	n/a	No
24 (18)	Event Address is null	No	n/a	No
32 (20)	No active SOLVE SSI with "XEVNT" support found	No	n/a	No
36 (24)	The SOLVE SSI REGION is not active	No	n/a	No
40 (28)	The SOLVE SSI is in shutdown	No	n/a	Yes
44 (2C)	Unable to send EVENT	No	n/a	Yes
64 (40)	NM000FGX abended	No	n/a	Yes
68 (44)	Unable to obtain storage - EVENT not sent	No	n/a	Yes

Appendix E: Implementing Schedule Control Files

This section contains the following topics:

Schedule Control Files

A control file (CTL file) is a data set 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 data set. When specified in a schedule, the CTL file is read when the schedule is activated and is used to externally build the file filters.

By using a CTL file you can do the following:

- 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 CTL file has the following format:

```
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 the NAME attribute.
- 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 in 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.

Define 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

1. Enter **/RADMIN.R.FTSCHD** at the command prompt.

   The File Transfer Schedule List appears.

2. Enter **U** beside the appropriate schedule name.

   The Panel Display List appears.

3. Enter **S** beside File Filters.

   The File Filters panel for the schedule appears.

4. Complete the following fields:

   Source Data or Target Data or Transfer ID

   Specifies the name of the CTL file.

   Type

   Specifies the type of file. Enter CTL.

   Press F3 (File).

   The changes to the schedule are saved.

View a CTL File

To view the contents of a CTL file

1. Enter **/RADMIN.R.FTSCHD** at the command prompt.

   The File Transfer Schedule List appears.

2. Select the required FTSCHD name.

   The Panel Display List appears.

3. Select the FTSCHD File Filters panel description.

   The File Filters panel appears.

4. Enter **V** beside the CTL file you want to view.

   The CTL file appears.

Check a CTL File

After 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

1. Enter **/RADMIN.R.FTSCHD** at the command prompt.

   The File Transfer Schedule List panel appears.

2. Select the required FTSCHD name.

   The Panel Display List appears.

3. Select the FTSCHD File Filters panel description.

   The File Filters panel appears.

4. Enter **CHK** beside any file of type CTL.

   The syntax of the file is checked.

Note: You should check the syntax of the file before a schedule is activated, because an invalid CTL file prevents a schedule from being activated.It is recommended that you limit access to CTL files to authorized personnel only.

CTL File 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.

Appendix F: Health Checks

This section contains the following topics:

CA Health Checker

The CA Health Checker provides a simple and consistent method for CA products to create health checks to run under the IBM Health Checker for z/OS. The IBM Health Checker for z/OS helps you identify potential problems in your z/OS environment by checking system or product parameters and system status against recommended settings. CA NetMaster FTM health checks are automatically activated on the target system when the product is started on a system with IBM Health Checker for z/OS installed and configured.

The CHECK_OWNER for all CA NetMaster FTM health checks is CA_NM.

Use either CA SYSVIEW or SDSF Health Checker displays to list and view the checks. View messages generated by CA health checks in the MVS System Log.

NM_ACB

Description

This CA NetMaster FTM health check checks that the primary ACB of the region is open. This check runs every 5 minutes.

Best Practice

VTAM is required to access the 3270 interface. If you primarily use the WebCenter interface to access you region, you can lower the priority of this health check.

Parameters accepted

None.

Debug Support

No.

Verbose Support

No.

Reference

None.

Non-exception Messages

The following messages can appear in health checker:

- This region's primary ACB, *acbname*, is open.
- The region is shutting down. Check is not relevant at this time.

Exception Messages

If an exception occurs, the following messages are issued as WTOs and written to the SYSLOG:

- CAH0001E The check timed out while waiting for a response to a command.
- NMH0106E This region's primary ACB, *acbname*, is not open.

NM_INITIALIZATION

Description

This CA NetMaster FTM health check checks region initialization. The check runs once at region startup. If an exception occurs, the check repeats every 5 minutes until initialization is successful.

Best Practice

Follow the Install Utility procedures in the *Installation Guide* to set up your region, and ensure that the parameters are specified correctly.

Parameters Accepted

None.

Debug Support

No.

Verbose Support

No.

Reference

See the online help for region parameter groups.

Non-exception Messages

The following messages can appear in health checker:

- The region has initialized successfully.
- The region is initializing. Check is not relevant at this time.
- The region is shutting down. Check is not relevant at this time

Exception Messages

If an exception occurs, the following messages are issued as WTOs and written to the SYSLOG:

- CAH0001E The check timed out while waiting for a response to a command.
- NMH0104E Initialization errors have occurred in region *regionname*.

NM_SOCKETS

Description

This CA NetMaster FTM health check checks that the sockets are available to support IP connections. The check runs every 15 minutes.

Best Practice

To help ensure IP connections, the port number for the connection must be specified and not in use by another task.

Parameters Accepted

None.

Debug Support

No.

Verbose Support

No.

Reference

None.

Non-exception Messages

The following messages can appear in health checker:

- Sockets are configured and active. HTTP port is *nnnn* URL is http://*nnn.nnn.nnn.nnn:nnnn*
- The region is initializing. Check is not relevant at this time.
- The region is shutting down. Check is not relevant at this time

Exception Messages

If an exception occurs, the following messages are issued as WTOs and written to the SYSLOG:

- CAH0001E The check timed out while waiting for a response to a command.
- NMH0110E TCP/IP interface is not active, status is *cccccccc*.
- NMH0111E No port number has been specified for this region.

NM_SSI

Description

This CA NetMaster FTM health check checks that the SOLVE SSI SSID is defined and connected. The check runs every 15 minutes.

Best Practice

Ensure that the following conditions are met:

- The SOLVE SSI started task is active.
- The SOLVE SSI SSID value for the region matches the SSID= parameter for the SOLVE SSI started task.
- The SOLVE SSI SSID and the AOM SSID are different.

Parameters Accepted

None.

Debug Support

No.

Verbose Support

No.

Reference

None.

Non-exception Messages

The following messages can appear in health checker:

- SOLVE SSI SSID correctly defined and connected. SSID is *ssidname*.
- The region is initializing. Check is not relevant at this time.
- The region is shutting down. Check is not relevant at this time.

Exception Messages

If an exception occurs, the following messages are issued as WTOs and written to the SYSLOG:

- CAH0001E The check timed out while waiting for a response to a command.
- NMH0108E SSID error, no SSID specified.
- NMH0108E SSID error, *ssidname* is not connected.
- NMH0108E SSID error, SSID matches AOM SSID(*ssidname*).

NM_WEB

Description

This CA NetMaster FTM health check checks that the WebCenter interface is available. This check runs every 15 minutes.

Best Practice

Use the Install Utility to set up the region. During the process, specify the web interface port.

Parameters Accepted

None.

Debug Support

No.

Verbose Support

No.

Reference

None.

Non-exception Messages

The following messages can appear in health checker:

- The region is initializing. Check is not relevant at this time.
- The region is shutting down. Check is not relevant at this time.
- The WebCenter interface is active. HTTP port is *nnnn* URL is http://*nnn.nnn.nnn.nnn:nnnn*

Exception Messages

If an exception occurs, the following messages are issued as WTOs and written to the SYSLOG:

- CAH0001E The check timed out while waiting for a response to a command.
- NMH0113E The WebCenter interface is not [active | configured].

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W