CA NetMaster® Network Management for TCP/IP

Administration Guide

Release 12.1

CA Technologies Product References

This document references the following CA Technologies products:

- CA NetMaster® Network Management for TCP/IP (CA NetMaster NM for TCP/IP)
- CA NetMaster® Socket Management for CICS (CA NetMaster SM for CICS)
- CA NetSpy™ Network Performance (CA NetSpy)
- CA SOLVE:Access™ Session Management (CA SOLVE:Access)
- CA ACF2™ for z/OS
- CA Top Secret® for z/OS
- CA TCPaccess™ Communications Server for z/OS (CA TCPaccess CS for z/OS)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Introduction 13

Intended Audience 13
Typographic Conventions 13
Structure of This Guide 14

Chapter 2: Configuring a Region 15

How You Use JCL Parameters to Configure a Region 15
    How You Display and Change JCL Parameter Settings 15
How You Identify the Region to Users 15
    How You Identify Domains and Panels 16
Region Customizer 16
    What Are Parameter Groups? 16
System Parameters 17
    Use the SYSPARMS Command 17
    Initialization Operands 17
Transient Log Tuning 18
    Customize Tuning Parameters 18
    Resize Selected Transient Logs 19
    Resize Multiple Transient Logs in an Image 20

Chapter 3: Setting Up the Packet Analyzer 21

Packet Analyzer 21
Set Up the Packet Analyzer 23
Purge Packet Analysis Requests 23
Duplicate Definitions on Multiple LPARs 24
    Export Definitions 24
    Import Definitions 24
User ID Associations 25
    Modify the Supplied Exit 25

Chapter 4: Setting Up IP Event Processing 27

Event Processing and Recording 27
    Events Recorded 27
Set Up IP Event Processing and Recording 28
    Check the Setup 28

Implement Event Processing 29
Control the Amount of Data Recorded 29

Chapter 5: Setting Up CTRACE 33

About CTRACE 33
How to Enable CTRACE 33
Create an External Writer 33
Verify the Setup 35

Chapter 6: Defining a System Image 37

Define a System Image 37
Define a System Image Using Express Setup 38
Set the Default System Image 39
Load a System Image 39
Checkpoint Restart Function 41

Chapter 7: Monitoring Attributes 43

About Monitoring Attributes 43
Attribute Types 43
Baseline Types 44
Delete Baseline Data 46
Monitor MIB Attributes 46
Add MIB Attributes 47
Assign Monitored MIB Attributes to Resource Classes 48

Chapter 8: Setting Up MIB Definitions 49

About MIBinsight 49
Prepare to Compile a MIB 50
Display MIB Definitions 50
Compile a MIB Definition 51
Browse a MIB Definition 52
Display the Source of a MIB Definition 52
Recompile a MIB Definition 52
Delete a MIB Definition 53
View the Structure of a MIB Definition 53
Display Object Details 55
Set a MIB Definition to Load Automatically 56
Set a MIB Definition to Load Manually 56
Load a MIB Definition 56

Unload a MIB Definition 57
Maintain MIBs 57
Example: Using the MIBinsight Browser 58

Chapter 9: Setting Up the Initialization File 61

Generate an Initialization File 61
How You Configure the Initialization File 62
Configure a Common Initialization File 62
Configure Individual Initialization Files 63
Start Your Region from an Initialization File 64

Chapter 10: Administering a Multisystem Environment 65

Multisystem Support 65
Multisystem Operation 66
Links in a Multisystem Environment 67
Multisystem Implementation Considerations 69
How a Multisystem Environment Is Established 70
Linked Regions and Database Synchronization 70
Background User Considerations 72
Transmit Records 72
Specify Multisystem Communications Access Methods 75
Link and Synchronize Regions 75
Monitor the Synchronization Procedure 77
Knowledge Base Synchronization Maintenance 78
Display Linked Regions 78
Unlink Regions 79

Chapter 11: Implementing Status Monitor Filters 81

Implement the Status Monitor Filters 81
Access Status Monitor Filter Definitions 81
Add a Status Monitor Filter 82
Status Monitor Filter Panel 83
How You Define the Status Monitor Filter Expression 84
Maintenance of Status Monitor Filter Definitions 85

Chapter 12: Implementing Resource Templates 87

Resource Templates 87
Set Up Your Template System 88
$TEMPLAT System Image for Multiple Products 88

Resource Template Definitions 89
Set Up a Template 89
Associate a Template to a Resource Class 89
Maintenance of Resource Template Definitions 90
Apply Updated Templates 90
Define and Maintain Maps in a Template System Image 90
Access Map Definitions in a Template System Image 91
Define and Maintain Processes in a Template System Image 91
Access the Process Definitions in a Template System Image 91
Convert a Resource Definition into a Resource Template 92

Chapter 13: Implementing the Graphical Monitor 93

Graphical Monitor 93
How You Customize the Graphical Monitor 93
Resource Groups for Icons 94
Access Resource Group Definitions 94
Add a Resource Group Definition 94
Maintenance of Resource Group Definitions 97
Icons 97
Access Icon Definitions 97
Define an Icon 98
Maintenance of Icon Definitions 100
Icon Panels 100
Access Icon Panel Definitions 101
Define an Icon Panel 101
Maintenance of Icon Panel Definitions 107
How You Edit a Generated Icon Panel 108
Set Up Default Icon Panel for Your Users 109
Example: Graphical Monitor Configuration 109

Chapter 14: Implementing Processes 111

How to Implement Processes 111
Process Types 111
Access Process Definitions 112
How to Define a Process 112
Set Macro Parameters 114
How You Test a Process 115
Test a Process Interactively 115
Test a Process by Execution as a Single Task 116
How You Log Process Activities 116
Maintenance of Process Definitions 116

Back Up Global Processes 117
Update Global Process Definitions in a Backup Global Process Image 118
Restore a Global Process Definition from a Backup Global Process Image 118
Merge Two Global Process Images 119

Chapter 15: Implementing Activity Logs 121

Activity Logs 121
Implement Online Activity Logging 122
Use Additional Log Files 123
Administer Online Activity Log Files 123
Swap the Online Log 124
Online Log Exit 124
Variables Available to the Activity Log Exit 125
Enable the Log Exit 126
Online Logging Procedure 126
Structure of Supplied Log Files 126
How You Write Logging and Browsing Procedures 127
Implement Logging and Browsing Procedures 128
Hardcopy Activity Log 128
Format of Logged Information 129
Format of the Hardcopy Log 130
Swap the Hardcopy Log 131
Reuse of Hardcopy Log Data Sets 132
Cross-Reference of Hardcopy Logs 132
I/O Errors on the Hardcopy Log 133
Write to the System Log 133

Chapter 16: Implementing Print Services 135

Print Services Manager 135
Access PSM 136
Add a Printer Definition 137
List Printer Definitions 137
Add a Form Definition 137
List Form Definitions 138
Add Control Characters 138
List Control Characters 138
Add a Default Printer for a User ID 139
List Default Printers 139
Clear the Printer Spool 140
Exits to Send Print Requests to a Data Set 140
How the Procedures Process a Print Request 141

$PSDS81X and $PSDS81Z Parameters 141
Printer Exit Definition Example 144
Print-to-Email 145

Chapter 17: Implementing the NetMaster-to-NetSpy Interface 147

Customize the NetMaster-to-NetSpy Interface 147
Manage NetMaster-to-NetSpy Connections 148
Manage CA NetSpy Alerts and Monitors 148
Manage NetSpy User Alert Monitors in CA NetMaster 149
Define CA NetSpy User Alert Monitors 149
Issue CA NetSpy Commands 150

Chapter 18: Setting Up CA NetMaster SM for CICS 151

CA NetMaster SM for CICS Interface 151
Configure CA NetMaster SM for CICS 151
Customize CA NetMaster SM for CICS 151
Issue Socket Management Commands in a Command Entry Environment 152

Chapter 19: Troubleshooting 153

About self-test 153
Access Self-test 153
Display the Initialization Log 154
SNMP Data Problems 154
Commonly Encountered Errors 156
Provide Information to Technical Support 160

Appendix A: SMF Record Structure 161

Performance Monitoring SMF Record Format 161
Field Identifier 162

Appendix B: IP EDS Events 163

IP Node Monitor State Changes 163
Trap FTP, Telnet, Connection, and Message Events 164
References 166

Appendix C: Telnet Translation Tables 167

Specify Telnet Translation Tables 167

Appendix D: Health Checks 169

CA Health Checker 169
NM_ACB 170
NM_INITIALIZATION 171
NM_PA_STACKS 172
NM_SOCKETS 173
NM_SSI 174
NM_WEB 175

Index 177

Chapter 1: Introduction

This section contains the following topics:

Intended Audience (see page 13)
Typographic Conventions (see page 13)
Structure of This Guide (see page 14)

Intended Audience

After you have installed CA NetMaster NM for TCP/IP, you must configure your system by performing the tasks described in the *Implementation Guide*. The tasks described in this guide are tasks that you do not need to perform, but may want to know about.

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**.

Structure of This Guide

The chapters in this guide are arranged as follows:

Initial Administration

- Introduction
- Configuring a Region

Core Administration

- Setting Up the Packet Analyzer
- Setting Up IP Event Processing
- Setting Up CTRACE
- Defining a System Image
- Monitoring Attributes
- Setting Up MIB Definitions

Multisystem Administration

- Setting Up the Initialization File
- Administering a Multisystem Environment

Advanced Administration

- Implementing Status Monitor Filters
- Implementing Resource Templates
- Implementing the Graphical Monitor
- Implementing Processes
- Implementing Activity Logs
- Implementing Print Services

Additional Administration

- Implementing the NetMaster-to-NetSpy Interface
- Setting Up CA NetMaster SM for CICS
- Troubleshooting

Appendixes

- SMF Record Structure
- IP EDS Events
- Telnet Translation Tables
- Health Checks

Chapter 2: Configuring a Region

This section contains the following topics:

How You Use JCL Parameters to Configure a Region (see page 15)
How You Identify the Region to Users (see page 15)
Region Customizer (see page 16)
System Parameters (see page 17)
Transient Log Tuning (see page 18)

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.

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 3: Setting Up the Packet Analyzer

This section contains the following topics:

Packet Analyzer (see page 21)
Set Up the Packet Analyzer (see page 23)
Purge Packet Analysis Requests (see page 23)
Duplicate Definitions on Multiple LPARs (see page 24)
User ID Associations (see page 25)

Packet Analyzer

The Packet Analyzer is a feature of the SOLVE Subsystem Interface (SSI), which is set up during installation.

The Packet Analyzer provides the following:

Packet Tracing

The packet analyzer intercepts and stores IP packets that satisfy the trace criteria provided in a SmartTrace definition. The packets are stored in the SSI database for viewing by the region.

Note: For more information about SmartTrace definitions, see the *User Guide*.

Connection Information

The Packet Analyzer uses intercepted packets to keep track of connections. State and statistical information about each connection is stored in the SSI database. The Packet Analyzer also intercepts System Management Facility (SMF) records generated by stacks, and File Transfer Protocol (FTP) and Telnet servers to augment the connection information.

The region performs real-time query and periodic sampling of the data collected by the Packet Analyzer to produce IP connection lists.

You can enhance the connection information as follows:

- Provide rules to associate connections with a business application. The application name will be visible in connection lists, connection workload performance reports, and event recording.
- Associate user ID and LU names with the connection records through the security exits.

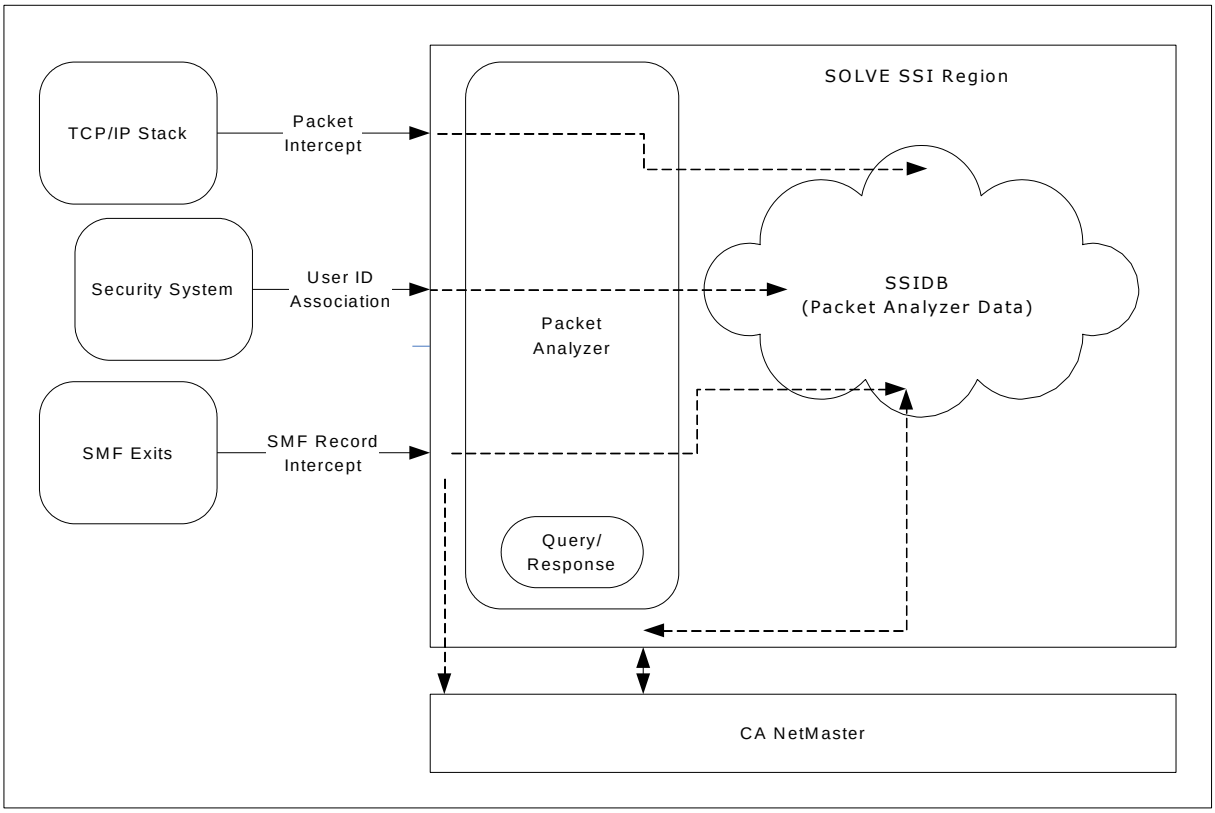
General Statistics

The Packet Analyzer intercepts packets and stores the general IP traffic and throughput statistics in the SSI database. Packet counts are maintained for interfaces, local addresses, ports, protocols, and networks.

Your region performs real-time query and periodic sampling of the data collected by the Packet Analyzer to produce the following:

- IP summary displays
- Performance monitoring for port throughput, address spaces, and stacks
- IP history displays for FTP and Telnet connections

The following diagram shows the flow of information through the Packet Analyzer:



Set Up the Packet Analyzer

To enable the Packet Analyzer, one active SSI on the system must have PKTANALYZER=YES. The SSI is set up during installation. For more information, see the *Installation Guide*.

JCL parameters in the SOLVE SSI region can be used to modify the size of the Packet Analyzer database and set limits on trace sizes, and so on. For more information, see the *SOLVE Subsystem Interface Guide*.

To check the status of the Packet Analyzer, enter the **SELFTEST** command.

Purge Packet Analysis Requests

When a STACK-class resource is loaded for the first time, the region requests the Packet Analyzer to collect packet information for the resource. The request remains active until you delete the resource.

Under some circumstances, you may want to purge a request without deleting the corresponding STACK resource specifically. For example, you may have deleted a region or moved a region to a different LPAR, but you did not delete the individual STACK resources beforehand, causing the corresponding requests to remain when they are not required.

To purge packet analysis requests

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

   The Packet Analysis Request List appears.

2. Enter **P** beside the requests you want to purge.

   Note: You cannot purge the blue color requests, which are associated with the STACK resources in the current local system image.

   For more information, press F1 (Help).

Duplicate Definitions on Multiple LPARs

Each LPAR has only one Packet Analyzer. This means that multiple regions on the same LPAR use the same application name definitions.

If you want to duplicate definitions on multiple LPARs, you can export and import definitions to and from other LPARs using the Packet Analyzer Utilities Menu.

You can export application name definitions to a physical sequential data set (DSORG=PS) or a member of a partitioned data set (DSORG=PO), with 80-byte fixed-length records. You can then import the definitions in the data set to other LPARs. This enables you to easily implement applications at your site that are common on more than one LPAR.

Export Definitions

To export definitions

1. Ensure that a sequential data set exists to hold the exported definitions.
2. Enter **/IPAUTIL** at the prompt.

   The Packet Analyzer Utilities Menu appears.
3. Complete the following field:

   Data Set Name

   Identifies the data set that you want to export.

   Select the **EA** option.

   The definitions are exported.

Import Definitions

To import the definitions in a data set

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

   The Packet Analyzer Utilities Menu appears.
2. Complete the following field:

   Data Set Name

   Identifies the data set that you want to import.

   Select the **IA** option.

   The definitions are imported. When the process completes, a report appears summarizing the result of the process.

User ID Associations

A security exit associates user IDs with IP connections. This association makes it easier to diagnose problems because a user is more likely to know their mainframe user ID than their IP address.

User ID associations are collected from the following connections:

- Telnet connections—if CA SOLVE:Access is used
- Telnet connections—if installation exits are used
- FTP connections on CA TCPaccess CS for z/OS
- FTP connections after a file transfer (GET/PUT) on an IBM TCP/IP stack

Note: To obtain the user ID information, the exit must know the LU name that is associated with a Telnet connection. Not all applications pass the LU name to the exit. In which case, no user ID correlation can be accomplished.

Modify the Supplied Exit

The product comes with a security exit for each of CA ACF2 for z/OS, CA Top Secret for z/OS, and RACF. Each exit has a modifiable stub. If you have an existing exit, merge it into the corresponding supplied exit.

To modify the supplied exit

1. Select the appropriate stub in the CC2DSAMP data set:
   - NMIPUSRX for CA ACF2 for z/OS or RACF
   - NMIPUSTX for CA Top Secret for z/OS
2. Create a user modification (USERMOD) with your additions for the selected stub.

   The USERMOD contains the functions from your existing exit.
3. Install the USERMOD.

   The supplied exit is modified.

Chapter 4: Setting Up IP Event Processing

This section contains the following topics:

Event Processing and Recording (see page 27)
Set Up IP Event Processing and Recording (see page 28)

Event Processing and Recording

You can specify whether you want to save or log FTP, Telnet, and connection events. The receipt of an SMF record that was created by your stack, Telnet server, or FTP server triggers these events.

Events Recorded

The type of TCP/IP stack that you are using determines the events passed to your system.

The following table shows what events are available with each stack.

Event	IBM TCP/IP	CA TCPaccess CS for z/OS
FTP Server Logon fail	Yes	No
FTP Server End of transfer	Yes	Yes
FTP Client End of transfer	Yes	No
Telnet Server Start of session	Yes	Yes
Telnet Server End of session	Yes	Yes
Telnet Client Start of session	Yes	No
Telnet Client End of session	Yes	No
TCP Connection start	Yes	Yes
TCP Connection end	Yes	Yes

Set Up IP Event Processing and Recording

Setting up event processing enables you to specify whether you want to log or save FTP, Telnet, and connection events.

To set up event processing

1. Check the setup.
2. Implement event processing.
3. Customize event recording for business applications.
4. Control the data retention period.
5. Run self-test.

Check the Setup

To check the setup

1. Ensure that the SOLVE SSI was implemented during installation and setup.
2. Ensure that your TCP/IP stack is enabled to generate SMF events. For more information, see the *Installation Guide*.

Implement Event Processing

For FTP events, Telnet events, and connection events, you can specify the following options:

Log Events

Writes individual event details to the activity log. They can be accessed using the standard log browse facility. Logging is useful if you want to relate events to other concurrent activity in the region.

Save Events

Saves individual event details in the Event History data set (IPLOG). You can display event details online, or print them using the **/IPHIST** shortcut. You can also export them to sequential files for reporting with external reporting tools, for audit purposes.

To specify event processing options

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

   The Customizer : Parameter Groups panel appears. This panel lists all the parameter groups that set up the characteristics of the region.

2. Press F8 (Forward) until the parameter group IPEVENT appears.

3. Enter **U** in front of the parameter group.

   The Customizer : Parameter Group panel appears.

4. Specify **YES** or **NO** in each of the event processing fields. For a description of the fields, press F1 (Help).

5. Press F6 (Action).

   The settings are applied.

6. Press F3 (File).

   The settings are saved.

Control the Amount of Data Recorded

A large volume of IP events can be collected. To limit the amount of recorded data, you can do the following:

- Enable delivery of connection event records to specific business applications

  Note: Business applications are groups of IP connections that correspond to your organization's usage and business requirements.

- Specify an appropriate data retention period

Customize Event Recording for Business Applications

If you indicate in the IPEVENT parameter group that you want to log or save connection events, then, by using the application name definitions, you can specify to log or save only events for certain business applications.

The TCP/IP : Application Name Definition panel lets you specify processing options. These options include the Deliver Records field that identifies which event records are delivered to your region. The field is applicable to connection events only. Telnet and FTP events are always delivered.

To limit the amount of recorded data

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

   The Application Name Definition List appears.

2. Press F4 (Add).

   The Application Name Definition panel appears.

3. Determine the business applications for which you want to save connection events and enable delivery for those applications.

4. Specify the type of connection events you want: initiation, termination, or both.

   To prevent the delivery of connection events for the application, specify **NONE** (the default) in this field. For information about the values in this field, press F1 (Help).

   Review your application name definitions to ensure that the value of the Deliver Records field matches your requirements. For those connections that do not match any definition, the default definition applies. The default definition is the last definition in the list.

Control the Data Retention Period

On a busy system, event recording can produce a large amount of data. When you enable event saving, the data is stored in the IPLOG file.

To specify how long you want to keep the data

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

   The Customizer : Parameter Groups panel appears.

2. Enter **U** next to the IPFILES parameter group.

   The IPFILES - TCP/IP File Specifications panel appears. This panel specifies the following:

   - The storage details for your TCP/IP data
   - SMF configuration

   The data sets on this panel were created during the setup process.

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

3. Review the fields, and specify your values. For information about the fields, press F1 (Help).

4. Press F6 (Action).

   The changes are applied.

5. Press F3 (File).

   The changes are saved.

Chapter 5: Setting Up CTRACE

This section contains the following topics:

About CTRACE (see page 33)
How to Enable CTRACE (see page 33)

About CTRACE

IBM's Component Trace (CTRACE) is a packet tracing facility, which is useful for debugging network problems. CA NetMaster simplifies the process of initiating, formatting, and viewing packet traces captured using CTRACE.

Note: You can also perform packet traces using SmartTrace. For information about setting up SmartTrace, see the *Implementation Guide*.

How to Enable CTRACE

To enable CTRACE

1. Create an external writer.
2. Verify the Setup.

Create an External Writer

CTRACE collects trace data from your server. For packet tracing to work, you need to create source JCL that invokes a CTRACE external writer. The external writer is used to write trace data to a data set each time packet tracing is used.

The external writer must use only single data sets for recording trace data. This is because CA NetMaster NM for TCP/IP reads only one trace data set.

To create an external writer

1. Edit the following example JCL to suit your specific requirements. The JCL procedure should be added to your SYS1.PROCLIB system library.

```
//PTTCP PROC
//*
//* CTRACE External writer for TCP/IP Packet Tracing
//*
//IEPROC EXEC PGM=ITTTRCWR,TIME=1440
//*
//*TRCOUT01 DD DSN=TCPIP.PTRACE.PTRACE,DISP=OLD
//
//TRCOUT01 DD DSN=TCPIP.PTTRACE.PTRACE,DISP=(NEW,CATLG),
//            VOL=SER=????,UNIT=SYSDA,DSORG=PS,
//            SPACE=(4096,(100,10))
```

   PTTCP is the name of the external writer. You can change this to suit your installation; it must be between one and seven characters long.

   Do *one* of the following:

   - Create a trace data set with the attributes DSORG=PS, RECFM=27994, and LRECL=VB.
   - Leave DSORG, RECFM, and LRECL unspecified and allow the program to determine their values.

   After the trace data set is allocated, do *one* of the following:

   - Modify the JCL so that TRCOUT01 is specified with DISP=OLD.
   - Delete or rename the TRCOUT01 data set before rerunning the procedure.

2. Determine the command that you are going to use to start the CTRACE external writer. You must specify this command on the CTRACE panel when you start CTRACE for the first time from your region. For example:

   TRACE CT,WTRSTART=PTTCP,NOWRAP

   where:

   - TRACE is the MVS TRACE command.
   - CT indicates that it is a component trace.
   - PTTCP is the name of the external writer that you specified in Step 1.

   For more information, see the IBM's *MVS Diagnosis: Tools and Service Aids* guide.

Verify the Setup

To verify the setup, you must start a CTRACE trace.

To start a trace

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

   The CTRACE Packet Tracing Menu appears.

2. Enter **PT** at the prompt.

   The Start CTRACE panel appears.

3. Complete the following field:

   Command to Start CTRACE

   Specifies the command to use to start CTRACE.

4. Press F6 (Action).

   The trace starts.

To stop a trace

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

   The CTRACE Packet Tracing Menu appears.

2. Enter **PTC** at the prompt.

   The Confirm Trace Stop panel appears.

3. Press F6 (Confirm).

   The trace stops.

Chapter 6: Defining a System Image

This section contains the following topics:

Define a System Image (see page 37)
Set the Default System Image (see page 39)
Load a System Image (see page 39)

Define a System Image

You can use express setup (see page 38) to define a system image to your region automatically or you can build one manually.

To define a system image manually

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

   The System Image List panel appears. This panel lists the system images defined to your system.

2. Press F4 (Add).

   The System Image Definition panel appears.

3. Specify the name of the system image, the version number, and a short description of the system image.

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

4. Press F3 (File).

   The System Image List appears and a message appears indicating that the system image has been successfully added to the knowledge base.

Define a System Image Using Express Setup

Express setup defines a system image to your region at installation; however, you can use express setup at any time to build a new system image. Express setup discovers resources and nodes automatically.

Note: The time taken to complete this process is determined by your site's configuration.

To define a system image using express setup

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

   The Automation Services : Confirm Express Setup panel appears.

2. Specify values in the System Image and Version fields.

   These default to the local z/OS system name and the next available version number.

3. Configure the $RMEXPR6 control member. Perform the following steps:

   a. Copy *dsnpref*.NMC1.CC2DEXEC($RMEXPR6) into *dsnpref.rname*.TESTEXEC.

   b. Update the *dsnpref.rname*.TESTEXEC($RMEXPR6) specifications. For example, comment out the resources you do not need to discover.

   c. Rename $RMEXPR6 and use this in the Control Member field.

      The $RMEXPR6 Control Member defaults to discover all of your resources.

4. Set Load Image? to YES.

   This system image is loaded after the discovery has completed.

5. Set the Create Application Name Definitions? field to YES.

   Application name definitions are automatically created for each address space discovered.

6. Press F6 (Action).

   The Automation Services : Express Setup Status panel appears. This panel reports the progress of the resource discovery and the number of resources successfully discovered.

Set the Default System Image

The region loads a system image during initialization. The system image loaded when the region is initialized is controlled by the AUTOIDS parameter group.

To set up the system image to load on restart

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

   The Customizer : Parameter Groups panel appears.

2. Enter **U** beside the $RM AUTOIDS parameter group.

   The AUTOIDS - Automation Identifiers panel appears.

3. Enter **?** in the System Image Name field.

   The ResourceView : System Image List panel appears.

4. Select the System Image that you want to load at restart and press F6 (Action).

   Important! F6 (Action) replaces the currently-loaded system image. If you do not want to load the system image now, skip this step.

5. Press F3 (File).

   The system image loads each time the region starts.

Load a System Image

The region loads a system image during region initialization. The system image loaded when the region is initialized is controlled by the AUTOIDS parameter group. When you create a system image and its associated resources, the default system image can be replaced by a temporary system image. During operation, you may need to change the system image by loading another temporary image.

Subordinate regions can load only system images whose name is associated to the subordinate region during the link and synchronization process.

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.

To load a system image

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

   The System Image Definition Menu appears.

2. Select the type of system image that you want to load.

   The System Image List appears.

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

   The LOAD Command Parameter Specification panel appears.

4. 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.

   Note: Operation Mode applies only to products that perform Desired State Management.

   Perform COLD Start?

   Specifies whether to perform a cold start. Valid values are:

   YES

   Deletes any preserved manual overrides used by the Checkpoint Restart facility.

   NO

   Retains preserved manual overrides and re-applies them to resources if Checkpoint Restart is ACTIVE.

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

   The Command Confirmation panel appears.

6. 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.

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.

Chapter 7: Monitoring Attributes

This section contains the following topics:

About Monitoring Attributes (see page 43)
Monitor MIB Attributes (see page 46)

About Monitoring Attributes

Monitoring attributes are defined to every IP resource. Monitoring attributes let you test the performance of a resource against a value or a calculated baseline to trigger alerts and actions.

Note: If you specify a type of baseline alerting, it is based on the hourly rate for total and counters.

Attribute Types

An attribute can be *one* of the following types:

GAUGE

Displays a numeric value that may increase or decrease in an allowable range. For example, processor memory usage varies between zero and the physical limit of the hardware.

COUNTER

Displays the rate of increase in units per hour in a sample period. The rate is derived from sample data, which is an accumulated count that increases in value over time (for example, bytes received). This type is also referred to as COUNT.

ENUMERATED

Displays the value from a defined set of discrete values. For example, the state of a device can be ACTIVE or INACTIVE. Multiple values are aggregated so that a percentage of a particular value over time is available. This type is also referred to as ENUM.

TOTAL

Displays the rate of increase in units per hour in a sample period. The rate is derived from sample data, which is the total increase in value in a sample period.

Baseline Types

Baselines are sliding averages of hourly values. You can use them to monitor network activity more easily.

If you use sampled data, the region calculates baselines for numeric type attributes—gauges, counters, and totals. You can use these baselines for alerting. When you specify a resource's monitoring, you can update the alert details and specify the type of baseline to alert on.

When individual samples are taken, they are compared to the baseline value as follows:

Counter and Total Attribute Sample Values

The equivalent hourly rate is calculated and compared to the baseline value. If the equivalent hourly rate differs from the baseline value by more than the specified percentage, an alert is raised.

Gauge Attribute Sample Values

The original sample value is compared to the baseline value. If the sample value differs from the baseline value by more than the specified percentage, an alert is raised.

When samples are summarized for each hour, the region recalculates the baseline as a moving average and stores the updated baseline value.

All baselines are averages of hourly summary values. The hourly summary values that are averaged depend on the baseline type.

The following baseline types are available:

Hour Of Day

Averages the hourly summary value for one specific hour of one specific day name, for up to the last ten weeks, for example, Friday at 17:00.

This type is the most granular baseline because you are comparing only the same specific time of the week.

One hundred and sixty eight hour-of-day baselines exist, one for each hour of each day name (24 hours a day, 7 days a week).

Day Of Week

Averages the hourly summary value for all hours in a specific day name (that is, Monday, Tuesday, and so on) for up to the last ten weeks.

Day of week is not as precise as the hour of day baseline. Every hour on Tuesday is averaged together. No account is taken for the fact that some hours, for example, working hours, frequently have different workloads than others (for example, late shift or off peak hours).

Seven day-of-week baselines exist, one for each day.

Daily

Averages the hourly summary value for all hours in the day, for each day up to the last 30 days.

Daily is the least precise baseline. This baseline does not account for the workload characteristics of different hours. Also, it disregards the different daily workload patterns.

One daily baseline exists.

Note: Baseline values become available after the first hourly summary of an attribute; however, when you start performance monitoring for the first time, baselines are calculated on few hourly summaries. To avoid spurious alerting, we recommend that you collect baseline date for a few days or weeks before you use it for alerting.

Delete Baseline Data

This option lets you delete baseline data for an individual attribute and qualifier, thus resetting the baseline values to null. You may want to do this after atypical network activity or when changing a region from testing to production.

Important! Deleting the baseline data affects the current monitoring for the attribute and may stop alerts from being automatically reset. We recommend that you manually close any open alerts for the selected attribute and qualifier.

To delete baseline data

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

   The Security and System Services : Primary Menu appears.

2. Enter **BL** at the prompt.

   The Data Framework : Baselined Resources panel appears.

3. Enter **D** beside the resource name that you want to delete.

   A confirmation message appears.

4. Press Enter.

   The baseline data for the selected resource is deleted.

Monitor MIB Attributes

MIB attribute monitoring lets you select an SNMP MIB attribute to monitor. When you define a monitor group, you have a list of predefined attributes that you can monitor. For the following resources, you can additionally choose one or more MIB attributes to monitor:

- TCP/IP Stacks
- CIPs
- Routers
- IP nodes

Add MIB Attributes

To monitor a MIB attribute, you must add it to the list of monitoring attributes.

To add MIB attributes

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

   The Monitoring Attributes panel appears.

2. Press F4 (Add).

   The Attribute Application Controls panel appears.

3. Press F10 (MibAttr).

   The list of available MIBs appears.

4. Enter **S** next to the MIB that contains the attributes you want.

   The MIBinsight Structure Viewer appears. The attributes are in green.

5. Enter **S** next to the required attribute.

   The Attribute Definition panel appears with the fields populated with values associated with the selected attribute. For fields that are not populated, specify your own values.

   Note: The TOTAL type is not applicable to user-defined attributes.

   If the attribute you have added is *not* a table entry, you do not have to qualify it. Go to Step 8.

6. (Optional) Press F11 (MibQual) to select a qualifier.

   The MIBinsight Structure Viewer appears.

   This procedure identifies the index of the entry whose attribute you want to monitor. You can qualify attributes in a table. Attributes not in a table have an index of 0 and do not require a qualifier.

7. Enter **S** next to the required qualifier.

   The Attribute Definition panel appears with the Qualifier Name and Qualifier ID fields populated.

8. Review the values. You can change some of the values.

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

9. Press F4 (Save).

   The definition is saved.

Assign Monitored MIB Attributes to Resource Classes

You can specify the classes of resources that can monitor a particular MIB attribute. When you specify the monitoring requirements for a resource definition, only the assigned MIB attributes are listed. After a MIB attribute is added to a resource class, you can monitor that attribute.

To assign monitored MIB attributes to resource classes

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

   The Monitoring Attributes panel appears.

2. Enter **U** beside the required attribute.

   The Attribute Definition panel appears.

3. Press F5 (Classes).

   The list of resource classes appears.

4. Enter **I** beside the required classes that you want to include. To remove an included class, enter **E** beside it.

5. Press F3 (Exit).

   The Attribute Definition panel appears.

6. Press F3 (Save).

   The details are saved.

Chapter 8: Setting Up MIB Definitions

This section contains the following topics:

About MIBinsight (see page 49)
Prepare to Compile a MIB (see page 50)
Display MIB Definitions (see page 50)
Display Object Details (see page 55)
Set a MIB Definition to Load Automatically (see page 56)
Set a MIB Definition to Load Manually (see page 56)
Load a MIB Definition (see page 56)
Unload a MIB Definition (see page 57)
Maintain MIBs (see page 57)
Example: Using the MIBinsight Browser (see page 58)

About MIBinsight

MIBinsight is a component that allows you to manage SNMP Management Information Bases (MIBs). MIBinsight comprises a MIB maintenance facility and a browser, and provides the ability to monitor MIB attributes.

MIBs identify data using Object Identifiers (OIDs). OIDs are a string of numbers (usually long); they are not user-friendly. MIBinsight translates these numbers into a more intelligible, human-readable format and allows you to view the knowledge of the resource in a user-friendly way.

To use the MIBinsight browser, your product accesses MIB definitions. A database of MIB definitions is supplied with your product. The supplied MIB definitions include standard MIBs defined by RFCs, and vendor-specific MIBs defined by IBM and Cisco. The MIB definitions are stored in source form, and compiled form, in the MODSDIS VSAM file.

These supplied MIB definitions enable you to use the MIBinsight browser to view MIBs associated with your Communications Server stack, and MIBs in many routers and other network devices. However, you can have a device with a MIB whose definition is not included in the supplied set. If you have access to the MIB definition, you can compile it into your product using the MIBinsight compiler, making it available for use with the MIBinsight browser, and attribute monitoring.

For the MIBinsight browser to use the MIB definitions, they must be loaded into storage. You can flag definitions for automatic loading, or you can load them manually.

You can compile, administer, and load MIB definitions using the MIBinsight maintenance facility. You can also monitor (see page 46) MIB attributes. For information about browsing MIBs using the MIBinsight browser, see the *User Guide*.

Prepare to Compile a MIB

The MIB import/export file is used to store exported items and resolve imports during a MIB compile. Before you can compile a MIB that contains import statements, you must populate the import/export file with the required components.

Some precompiled MIB definitions and an empty import/export file are provided. If you want to add and compile any other MIB definitions, you must recompile all distributed MIB definitions to populate this file. The easiest way to recompile all MIB definitions is to use the MIBinsight batch compiler. The batch compiler is submitted to the background system region and compilation messages are written to the activity log.

To run the batch compiler

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

   The TCP/IP : Administration Menu appears.

2. Enter **MC** (Run MIBinsight Batch Compiler) at the prompt.

   The compiler starts.

Display MIB Definitions

The MIBinsight : Defined MIBs panel displays all MIBs defined to the system. From this panel, you can perform the following tasks:

- Add a MIB definition (and compile it)
- Browse a MIB definition
- Delete a MIB definition
- Browse the source for a MIB definition
- Compile a MIB definition (from an external source)
- Recompile a MIB definition (from the internal source)
- View the structure of a MIB definition
- Flag a MIB definition for automatic loading
- Flag a MIB definition for manual loading
- Load a MIB definition
- Unload a MIB definition

To access MIB definitions, enter **/MIBD** at the prompt.

The MIBinsight : Defined MIBs panel appears.

Note: Loaded MIBs are displayed in white.

Compile a MIB Definition

You can compile a MIB definition from an external source.

Note: Before you perform this task, you must populate the import/export file (see page 50).

To compile a MIB definition

1. From the MIBinsight : Defined MIBs panel, enter **CM** next to the MIB definition that you want to compile.

   The MIBinsight : MIB Definition Panel appears.

2. Complete the fields on the panel. For a description of the fields, press F1 (Help).

   Note: The compiler provides the MIB name, for example, SNMPv2TC-v1.

3. Press F5 (Options).

   The MIBinsight : Compiler Options panel appears.

4. Enter **YES** next to the options that you want to ignore. For a description of the fields, press F1 (Help).

5. If you want to import definitions from another MIB, which was compiled with a different name, enter the name in the Import Rename field.

   For example, if the MIB you are compiling imports definitions from MIB1, but MIB1 has been compiled and exported under the name MIB2, then you can specify MIB1=MIB2 in the Import Rename field to enable the compiler to find the requested definitions.

6. Press F3 (File)

   The MIBinsight : MIB Definition panel appears.

   Do *one* of the following:

   - If you want to compile the MIB definition as defined, go to Step 8.
   - If you want to compile the MIB definition from a different external source file, go to Step 7.

7. (Optional) If you want to compile the MIB definition from a different external source file, enter the name of the file in the external source file, and a short description.

8. Press F6 (Compile)

   The MIB definition is compiled.

Browse a MIB Definition

You can display the details of a MIB definition that has been defined and compiled.

To browse a MIB definition

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

   The MIBinsight : Defined MIBs panel appears.

2. Enter **BD** next to the MIB definition that you want to browse.

   The MIBinsight : MIB Definition panel appears with the details of the MIB definition.

Display the Source of a MIB Definition

You can display the source records of a compiled MIB definition.

To display the source records of a MIB definition

1. Enter **/MIBD** at the prompt.
2. The MIBinsight : Defined MIBs panel appears.
3. Enter **B** next to the MIB definition that you want to browse.

   The MIBinsight : MIB Source panel appears.

Recompile a MIB Definition

You can recompile a MIB definition from internal source, to repopulate the import/export file.

To recompile a MIB definition (from internal source)

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

   The MIBinsight : Defined MIBs panel appears.

2. Enter **R** next to the MIB definition that you want to recompile.

   The MIBinsight : MIB Definition Panel appears.

   Note: The compiler provides the MIB name, for example, SNMPv2TC-v1.

3. Press F5 (Options).

   The MIBinsight : Compiler Options panel appears.

4. Enter **YES** next to the options that you want to enable. For a description of the fields, press F1 (Help).
5. (Optional) To import definitions from another MIB definition, which was compiled with a different name, enter the name in the Import Rename field.

6. Press F3 (File)

   The MIBinsight : MIB Definition panel appears.

7. Press F6 (Compile)

   The MIB definition is recompiled.

Delete a MIB Definition

You can delete a MIB definition from the database.

Note: This deletes only MIB definitions from MODSUSR. The distributed MIB definitions in MODSDIS cannot be deleted.

To delete a MIB definition

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

   The MIBinsight : Defined MIBs panel appears.

2. Enter **D** next to the MIB definition that you want to delete.

   A confirmation message appears.

3. Press Enter.

   The MIB definition is deleted.

View the Structure of a MIB Definition

You can display the structure of a MIB definition as a tree. From here you can do the following:

- Expand and collapse the tree to display the entire MIB structure
- Display the full details of an object
- Display the enumerated values of an object
- Display the objects that make up an index entry of an object

Display MIB Definition Structure

To display the structure of a MIB definition

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

   The MIBinsight : Defined MIBs panel appears.

2. Enter **V** next to the MIB definition that you want to view.

   The MIBinsight : Structure Viewer appears.

3. To display the full object names, OIDs, and descriptions, press F11 (Right).

Expand and Collapse the Tree

Objects that have subordinate objects in the MIB definition and therefore expandable, are preceded with a rectangle.

To expand an object

1. Enter **E** (Expand) next to the object.

To collapse an object

1. Enter **C** (Collapse) next to the object.

You can toggle between global expand and global collapse by pressing F4 (Expand/Collapse).

Display Enumerated Values

If a MIB object is an enumerated value, press F6 (ViewEnum) to display the list of all possible values.

```
PROD------------------ MIBinsight : Enumerated Values ------------------------
Command ===>                                                 Scroll ===> CSR

     MIB Name ........ SNA-NAU-MIB
     Object Name ..... snaLuSessnOperState
     Minimum Value ... 1
     Maximum Value ... 4

    Enum  Value
       1  unbound
       2  pendingBind
       3  bound
       4  pendingUnbind
    **END**


 F1=Help      F2=Split     F3=Exit      F4=Return    F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap
```

If the MIB object has an index structure, press F6 (ViewIndx) to display the details.

```
PROD----------------------- MIBinsight : Indexes -----------------------------
Command ===>                                                 Scroll ===> CSR

     MIB Name ........ SNA-NAU-MIB
     Object Name ..... snaLuSessnEntry

    Name                              Object ID                          Impl
    snaNodeAdminIndex                 1.3.6.1.2.1.34.1.1.1.1.1           No
    snaLuAdminLuIndex                 1.3.6.1.2.1.34.1.2.1.1.1           No
    snaLuSessnRluIndex                1.3.6.1.2.1.34.1.2.3.1.1           No
    snaLuSessnIndex                   1.3.6.1.2.1.34.1.2.3.1.2           No
    **END**


 F1=Help      F2=Split     F3=Exit      F4=Return    F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap
```

Display Object Details

To display the full details of an object

1. Position your cursor next to the object, and then press Enter.

   The MIBinsight : Object Details panel appears.

Note: To display the MIB definition source details from here, press F5 (BrowSrc).

Set a MIB Definition to Load Automatically

This option enables the AutoLoad flag for a MIB definition. If the AutoLoad flag is enabled, the MIB definition is loaded into the lookup table when the region is initialized.

Note: Only MIBs that have one or more OBJECT-TYPE definitions can be loaded into the lookup table.

To automatically load a MIB at initialization

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

   The MIBinsight : Defined MIBs panel appears.

2. Enter **A** (Auto Load) next to the MIB definition that you want to load.

Set a MIB Definition to Load Manually

This option disables the AutoLoad flag for a MIB definition, so that the MIB definition is not loaded into the lookup table automatically when the region is initialized. If you want to load the MIB definition, you will have to do it manually.

To disable the AutoLoad flag for a MIB definition

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

   The MIBinsight : Defined MIBs panel appears.

2. Enter **M** next to the MIB definition that you want to load under manual control.

Load a MIB Definition

This option manually loads a MIB definition into the lookup table so that the MIBinsight browser and MIBinsight attribute monitoring can use it.

To load a MIB definition

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

   The MIBinsight : Defined MIBs panel appears.

2. Enter **L** next to the MIB definition that you want to load.

Unload a MIB Definition

This option removes a MIB definition from the lookup table.

Follow these steps:

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

   The MIBinsight : Defined MIBs panel appears.

2. Enter **U** next to the MIB definition that you want to unload.

Maintain MIBs

You can copy, move, or delete a MIB in a file in the Managed Object Development Services (MODS) concatenation.

Follow these steps:

1. Enter the **/MODSAD.MIB** panel shortcut.

   The MIB Utility Menu appears.

2. Select the required option with appropriate field values.

   Note: For information about the fields, press F1 (Help).

   The MIBs in the specified MODS file are listed.

3. Enter **S** next to the required MIB.

   The selected option executes.

Example: Using the MIBinsight Browser

In this example, the enterprise has a PC called Uluru running a mission-critical Windows application. You want to monitor the overall CPU consumption of this PC and the CPU utilization of the application. If there is poor response you may need to remotely diagnose what is happening on this PC. Providing the Windows SNMP service is started on this PC, you can interrogate it using the MIBinsight browser. Among the many management objects implemented by the Windows SNMP service are objects defined in the HOST-RESOURCES-MIB definition. These objects include overall processor load (CPU percentage) and CPU and memory use for each software item running on the PC.

To monitor the CPU consumption and utilization of the application

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

   The TCP/IP : Network Diagnostics Functions menu appears.

2. Enter the IP address of the PC that you want to diagnose in the Host Name/Addr field.

   The MIBinsight : User Security Details panel appears.

3. Specify the SNMP version and security information you need to access the SNMP agent on the PC, and press F3 (File).

   The MIBinsight : Loaded MIBs list appears. This list lets you select the MIB definitions with which to prime your browser

   Note: These details default to SNMP Version 2C, with GET and SET Community Names set to public.

4. Select the HOST-RESOURCES-MIB.

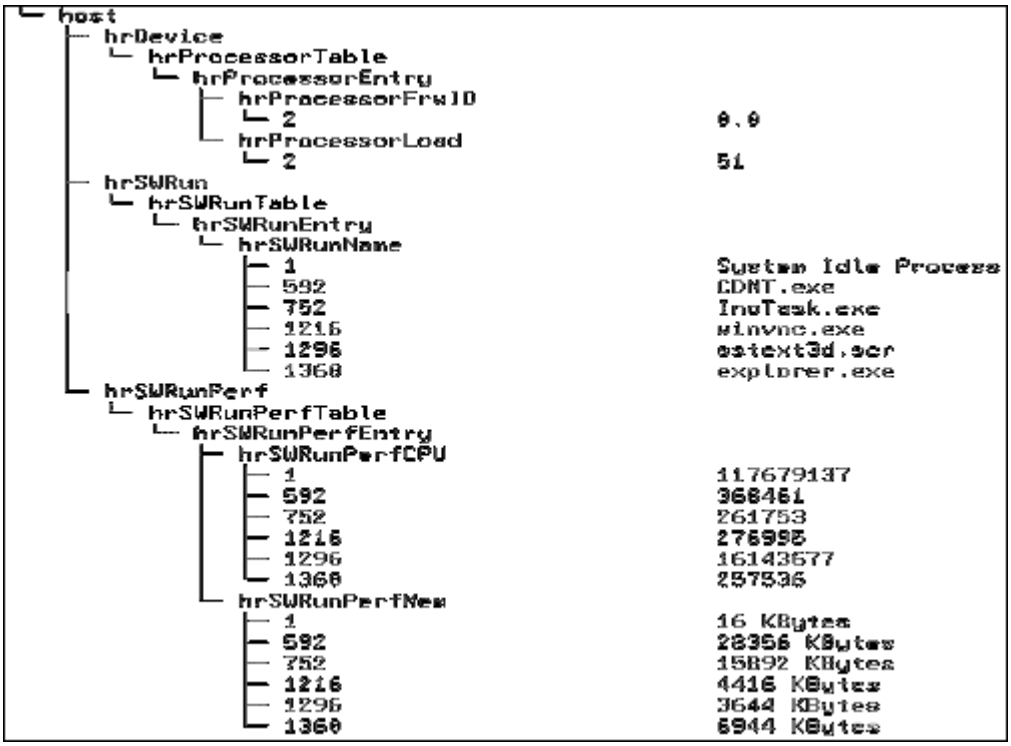
   The MIBinsight browser appears.

   To view the values for a particular object enter G (Get) beside the object. To delete objects from the MIB browser that are not relevant to your current inquiry, enter D (Delete) next to the object. To populate a table of objects, use the T (GetTable) command.

5. Get the values for the system objects sysDescr, sysObjectID, sysUpTime, sysName and sysServices, and populate the host resource tables hrProcessorTable, hrSWRunTable and hrSWRunPerfTable. Delete all other object definitions loaded into the MIB browser.

The following shows the result of the browsing:

The following provides a more detailed view of the host section:



Example: Results

The hrSWRunTable and the hrSWRunPerfTable use the same index, hrSWRunIndex. This index corresponds with the Process ID displayed in the Processes List of the Windows Task Manager display. There were more than six tasks running on Uluru at the time but only the six tasks listed were selected. Likewise, all attributes have been deleted from the hrSWRunTable except for hrSWRunName.

The previous display shows that the overall CPU usage on the PC at present is 51% utilization - nothing to worry about. The display also indicates that the task with the highest CPU utilization is the System Idle Process, which has used 117,679,137 centiseconds (13.62 days) of CPU since the PC was booted over 23 days ago (sysUpTime). The second highest user of CPU is task ID 1296 - sstext3d.scr - the screen-saver. The third highest CPU user is task ID 592 - CDNT.exe. This task has used a total of 368,461 centiseconds (61 minutes). It is also the highest user of memory, currently consuming 28,356 Kilobytes. This may be the application we are interested in monitoring. Enter G (Get) next to the 592 index for hrSWRunPerfCPU and hrSWRunPerfMem to display the latest CPU and memory figures for this task, enabling you to monitor its current utilization.

If this application is critical to the enterprise, it would be advisable to define Uluru as an IP node and monitor it. It would also be advisable to define hrSWRunPerfCPU and hrSWRunPerfMem as Data Sampling Framework attributes to monitor, optionally filtering both attributes for task 592. After they are defined, you can monitor these attributes for the Uluru IP Node and issue alerts when the CPU or memory utilization for this task exceeds or falls under a defined threshold.

The screen width is 120 characters. The MIBinsight browser is designed to use the maximum screen width available to your 3270 session. If you have a session defined as 160 characters wide, the MIBinsight browser uses this full width. This is useful when displaying long OIDs and their associated values. It is also useful when displaying the full SNMP tree.

The MIBinsight Browser default view is a flat view with only tables, table entries, and tabulated objects nested; however, to the full SNMP structure (as in the above example), enter the TREE ON command at the command line.

The default sort order for tabulated objects is indexes in attributes (by Attribute), and this is the order displayed. For example, the display shows all indexed values for hrSWRunPerfCPU before displaying all indexed values for hrSWRunPerfMem. This is also the order in which objects are accessed from a MIB. However, the MIBinsight browser lets you resort tabulated objects to display them by Index. This is useful when you want to see all attributes and their values for each table entry. You can toggle the sort order between by Attribute and by Index using F12.

Press F6 (Walk) to continue walking through a MIB. As new objects are browsed they are dynamically added to the MIBinsight browser display.

Chapter 9: Setting Up the Initialization File

This section contains the following topics:

Generate an Initialization File (see page 61)
How You Configure the Initialization File (see page 62)
Start Your Region from an Initialization File (see page 64)

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 10: Administering a Multisystem Environment

This section contains the following topics:

Multisystem Support (see page 65)
Multisystem Operation (see page 66)
Linked Regions and Database Synchronization (see page 70)
Display Linked Regions (see page 78)
Unlink Regions (see page 79)

Multisystem Support

If you have regions on different systems, you can link them together to form a multisystem configuration.

A multisystem configuration enables you to log onto your local region, and view and control the resources of linked regions. You can do things such as:

- View a single monitor display of the resources or nodes in all the linked regions
- Display the alerts raised from all the linked regions
- Display a consolidated list of IP connections across multiple stacks and regions

Multisystem configurations are set up and administered from the Automation Services : Multi-System Support Menu. To access this menu, enter the shortcut **/MADMIN**.

For more information, press F1 (Help).

Multisystem Operation

Your product provides focal point management to support multisystem operation. Management is at a focal point with subordinates and other focal points feeding information to it, as follows:

Focal

Supports full connectivity between multiple regions. Regions linked in this way are known as focal point regions.

When regions are communicating with each other, authorized users can monitor and control all managed resources from any terminal connected to any region.

All focal point regions have the knowledge base synchronized.

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 resources that belong to the local system image only.

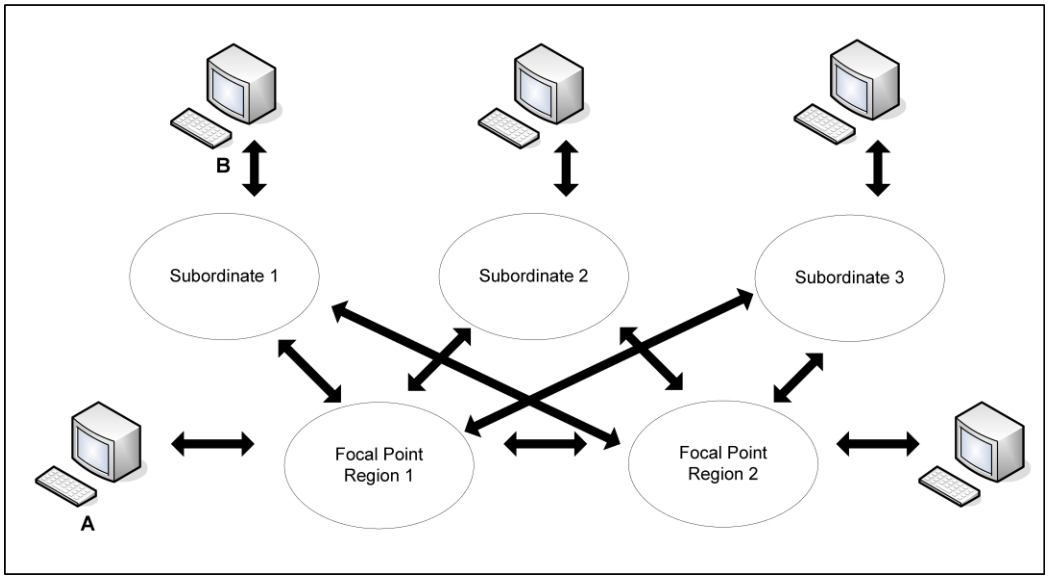
In a multisystem environment, each region runs independently of the other regions. If no communication links are available, each region still provides full monitoring, control, and automation of its own managed resources.

To link a focal point region to another focal point region, or to link a subordinate to a focal point region, you link and synchronize the regions.

Notes:

- You can link as focal points only those regions that are configured for the same products. For a subordinate-focal point link, the products configured in the subordinate region can be a subset of the products configured in the focal point region.
- Subordinate regions assume a system image name that cannot be used for any other region in the multisystem environment. We recommend that you use a unique system image name for subordinate regions running on the same LPAR. If you use express setup, the system image name defaults to the SMF ID.

The following diagram shows an example of a multisystem environment. Logging on to Console A allows visibility to all resources. Logging on to Console B allows visibility to the subordinate system image only.



Notes:

- A focal point region links to all other focal point regions and subordinates.
- A subordinate links to focal point regions but does not link to other subordinates.

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.

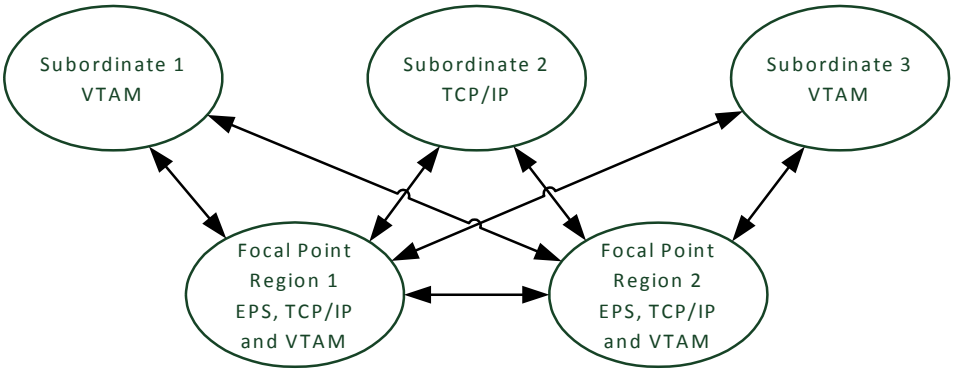
The INMC link between any two regions uses the access methods enabled by *both* regions (that is, the intersection of the two MULTISYS parameter groups). When multiple access methods are enabled, the link can use all these methods. This improves reliability because the link functions when one of the 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.

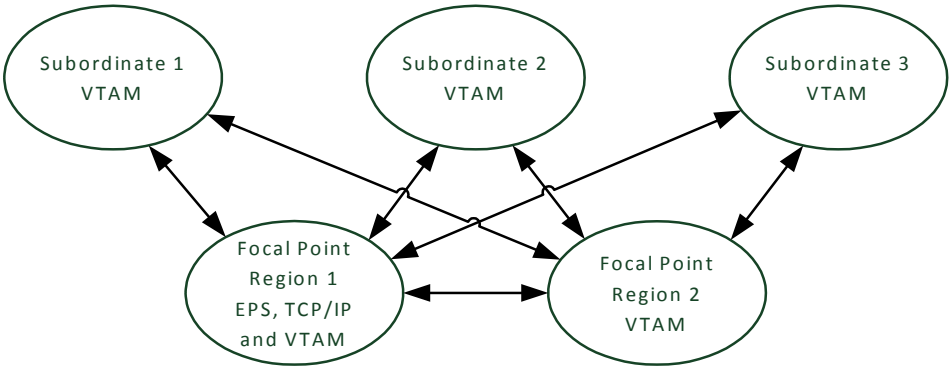
Example: Focal Point Regions Support All Access Methods

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 a Sysplex

With the EPS access method, you can use the sysplex cross-system coupling facility (XCF) to implement your multisystem environment.

Notes:

- To support the EPS access method, a SOLVE SSI region must be active in each of the co-operating systems and must be registered to XCF.
- To register the SSI region to XCF, ensure that XCF=YES is set in the SSI parameters member of the SSIPARM data set. This is the default setting at installation.

Multisystem Implementation Considerations

When you implement your multisystem environment, consider the following:

- Ensure that the link requirements (see page 67) are satisfied for the planned multisystem environment.
- When you link two regions, the knowledge base in one region overwrites the knowledge base in the other region. *You must transmit all system images used by the local region to the target focal point region prior to synchronization.*
- You can only link a region to a focal point region. The focal point region can be a stand-alone region or part of a multisystem environment.
- You can only link a stand-alone region into a multisystem environment.

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 70) 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

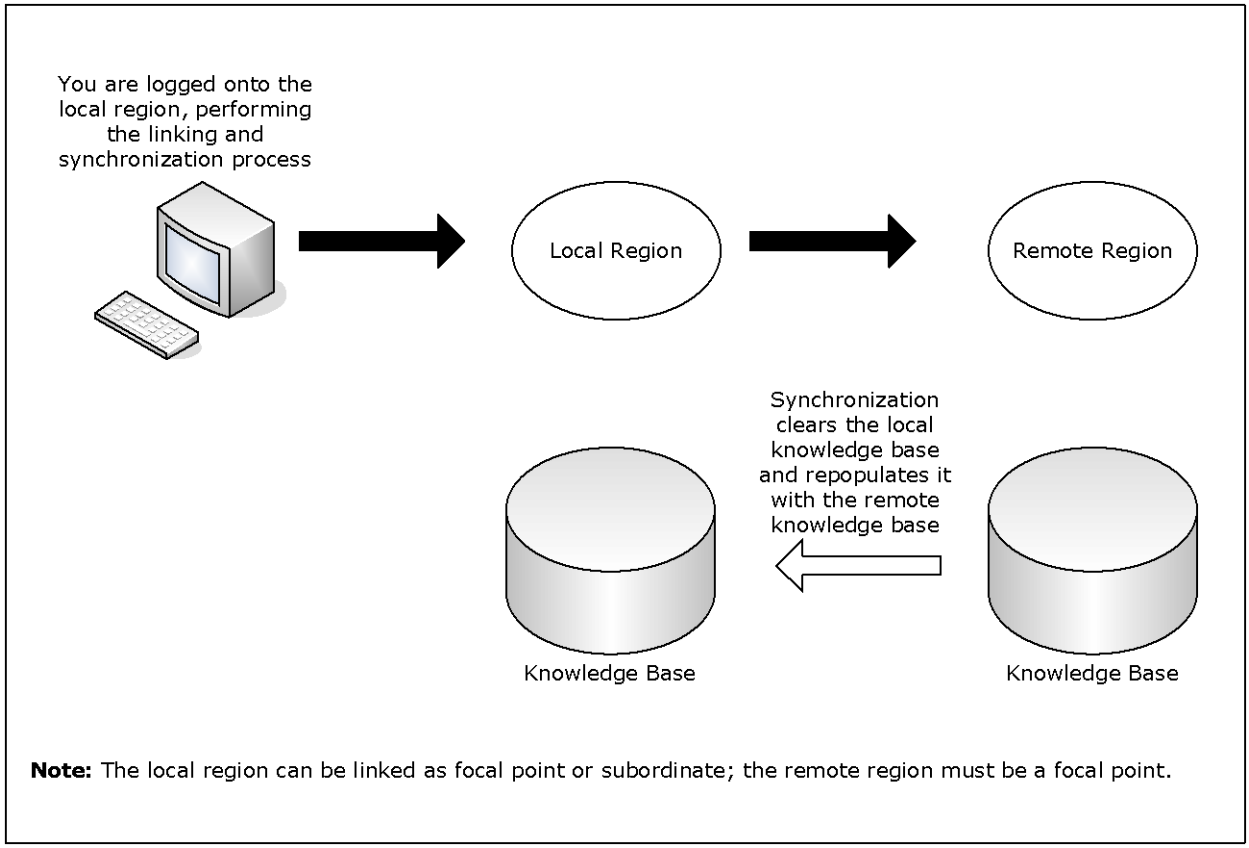
- For linked focal point regions, synchronization is complete and the focal point knowledge bases are identical.
- For linked subordinates, synchronization is complete only to the extent of the relevant definitions in the knowledge base. For example, a subordinate knowledge base does not contain all 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.

Transmit 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.

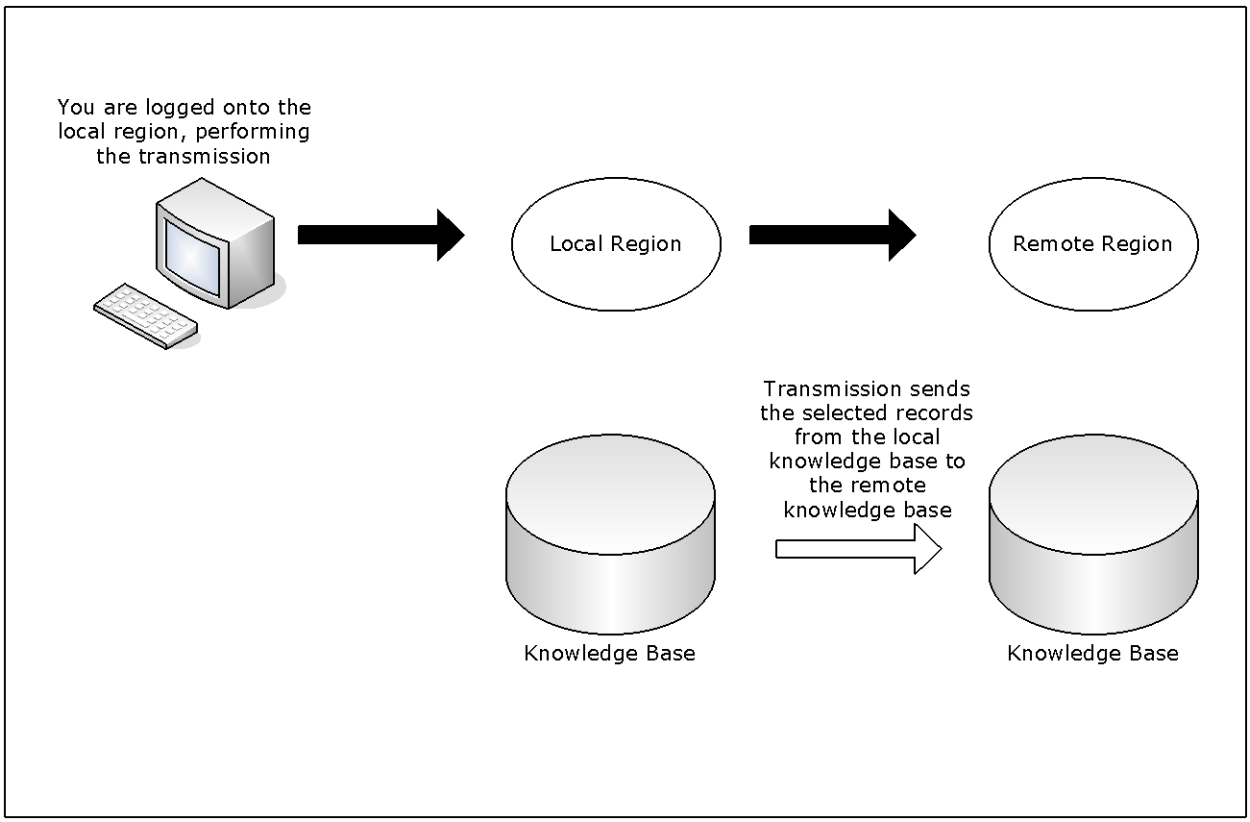
By specifying the appropriate transmission mode on the Remote System Identification panel, you can specify how to update the records in the remote region.

The following transmission modes are available:

- Replace (R) deletes any existing remote records, then transmits the local records.
- Overlay (O) replaces existing remote records with the same name, adds records that do not already exist, but does not delete any records in the remote knowledge base.
- Merge (M) adds records that do not already exist, but does not have any affect on existing records in the remote knowledge base.

Transmission Procedure

This diagram 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 type of system data that you want to transmit 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 option, go to step 5. If you specified any other transmission options, go to Step 6.
5. Complete the System Name and Version fields.

   Note: For information about the fields, press F1 (Help)

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** beside the categories that you want to transmit.
   - If you selected option TC with a transmission mode of MERGE or OVERLAY, enter **S** beside the categories that you want to transmit.
     To select specific definitions in a category for transmission, enter **L** (List) beside the category to list the definitions, then enter **S** beside the definitions to transmit.
   - If you selected other transmission options with a transmission mode of MERGE or OVERLAY, press F4 (All) to transmit all definitions or enter **S** beside 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 choose to exit the status panel, you can check the status of the task by viewing the administration task log **(MADMIN.L)**. Before you exit, note the task number for future reference.

Specify Multisystem Communications Access Methods

This procedure specifies the access methods that the region uses for communications. You can only enable a method if it is supported on your system.

To specify the communications access methods

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

   The Customizer : Parameter Groups panel appears.

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

   The MULTISYS - Multi-System Options panel appears.

3. Complete the following fields:

   VTAM?

   Specifies whether the region uses the VTAM access method.

   EPS?

   Specifies whether the region uses the EndPoint Services access method.

   TCP/IP?

   Specifies whether the region uses the TCP/IP access method.

   Link Establishment Timeout Period

   Specifies the time to wait for a link to be established.

   Default: 60 seconds

   Press F6 (Action).

   The communications access methods are activated.

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.

Chapter 11: Implementing Status Monitor Filters

This section contains the following topics:

Implement the Status Monitor Filters (see page 81)
Access Status Monitor Filter Definitions (see page 81)
Add a Status Monitor Filter (see page 82)
Maintenance of Status Monitor Filter Definitions (see page 85)

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 84) 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.

```
PROD--------- Automation Services : Status Monitor Filter ------Function=BROWSE
Command ===>                                                  Scroll ===> CSR

. Filter Definition ------------------------------------------------------------.
| Name ......... RCSALERT                                                      |
| Views ........                                                               |
| Description .. Resources in DEGRADED, FAILED, or UNKNOWN state               |
| Last Updated at 15.09.30 on WED 24-MAY-2006 by USER01                        |
'------------------------------------------------------------------------------'
. Filter Expression ------------------------------------------------------------.
|                                                                              |
|                                                                              |
|      "(" Field   Opr Value                                    Gen ")" Bool   |
|      (   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 12: Implementing Resource Templates

This section contains the following topics:

Resource Templates (see page 87)
Set Up Your Template System (see page 88)
Resource Template Definitions (see page 89)
Maintenance of Resource Template Definitions (see page 90)
Define and Maintain Maps in a Template System Image (see page 90)
Define and Maintain Processes in a Template System Image (see page 91)
Convert a Resource Definition into a Resource Template (see page 92)

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.

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*.

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.

Set Up a Template

To set up a template

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

   The ResourceView : Resource Template Definition panel appears. This panel lists the resource classes that you can use templates with.

2. Enter **S** beside the required class, for example STACK.

   The TCP/IP Stack List appears.

3. Press F4 (Add).

   The General Description panel appears.

4. Complete the fields on each of the definition panels.

   For more information about completing the panels, press F1 (Help).

   After completing the definition panels, the ResourceView : TCP/IP Stack List appears with the new template.

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.

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.

Define and Maintain Maps in a Template System Image

You can define monitoring 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 **M** 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 111).

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 13: Implementing the Graphical Monitor

This section contains the following topics:

Graphical Monitor (see page 93)
How You Customize the Graphical Monitor (see page 93)
Resource Groups for Icons (see page 94)
Icons (see page 97)
Icon Panels (see page 100)
How You Edit a Generated Icon Panel (see page 108)
Set Up Default Icon Panel for Your Users (see page 109)
Example: Graphical Monitor Configuration (see page 109)

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 96) 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 96) 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 100) 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.

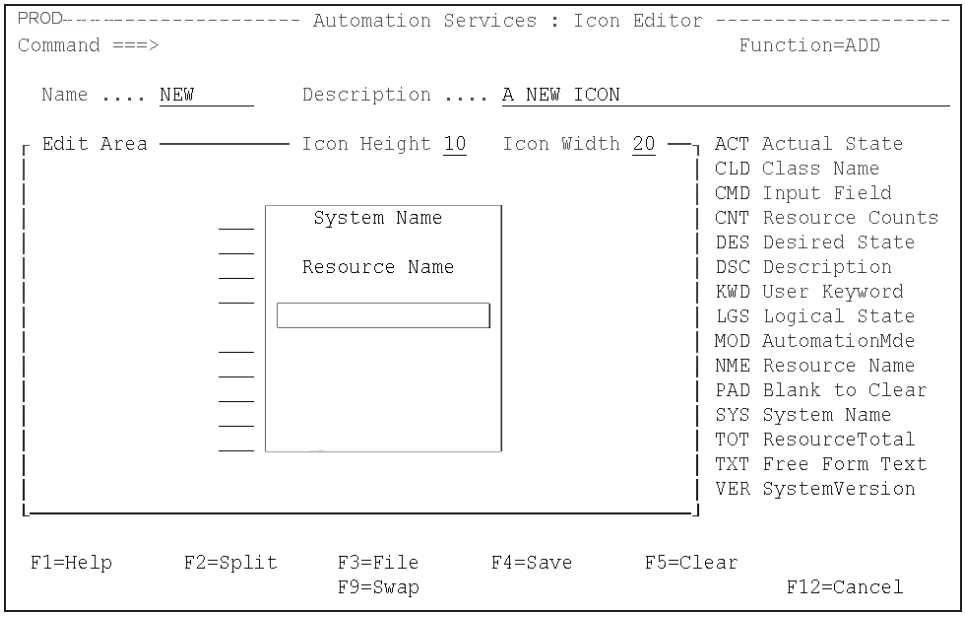
The panel specifies the following information:

- 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.

Maintenance of Icon Definitions

You can browse, update, copy, and delete icon definitions from the Icon List 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:

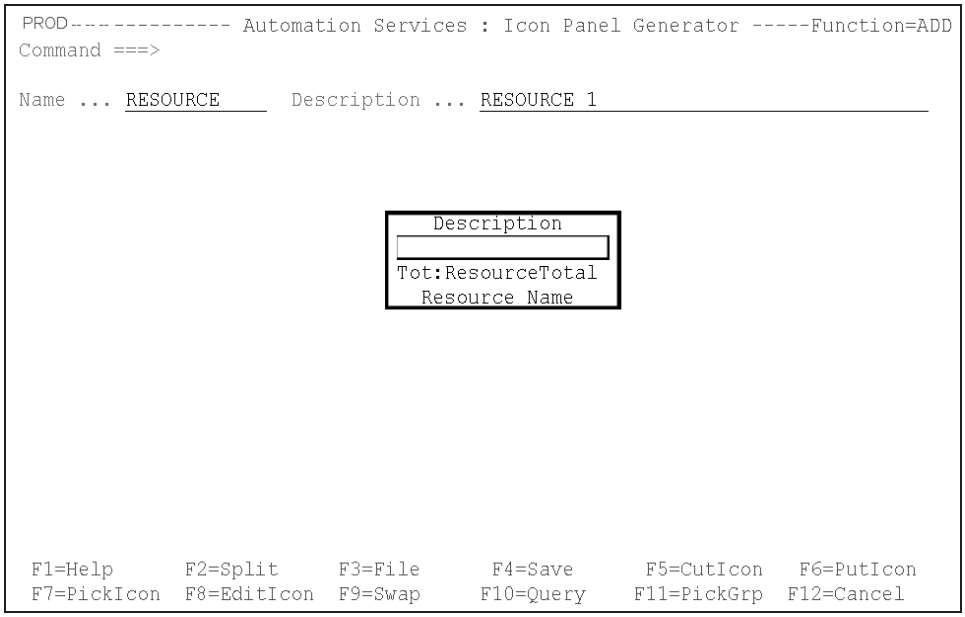
- Name and description of the icon panel
- Actual icon panel representation

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.

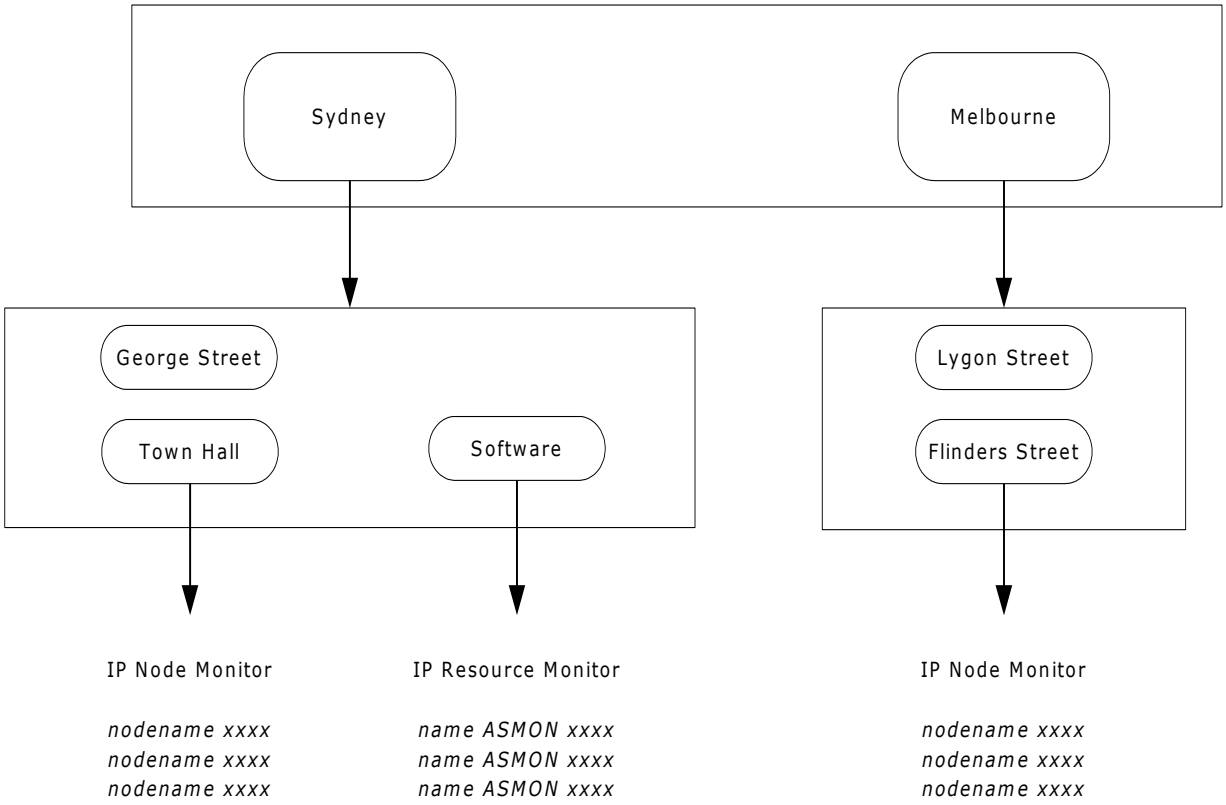
Example: Graphical Monitor Configuration

The Rich Finance Company provides financial 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. The company also has a department in Sydney that performs back-office processing in a small data center.

You want to monitor the key IP nodes in the Sydney and Melbourne offices, and the following address spaces on the Sydney LPAR:

- Individual CICS applications
- Subsystem
- Mainframe printing application

The following diagram illustrates this structure:



To create this structure, you need the following:

- Two icon templates (which can be used for the seven icons)
- Seven resource groups - one each for Sydney, Melbourne, and all of the branches
- Seven icons - one each for Sydney, Melbourne, and all of the branches
- Three icon panels

Chapter 14: Implementing Processes

This section contains the following topics:

[How to Implement Processes](#) (see page 111)
[Access Process Definitions](#) (see page 112)
[How to Define a Process](#) (see page 112)
[How You Test a Process](#) (see page 115)
[How You Log Process Activities](#) (see page 116)
[Maintenance of Process Definitions](#) (see page 116)
[Back Up Global Processes](#) (see page 117)

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 event detector—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.

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.

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 &).

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 15: Implementing Activity Logs

This section contains the following topics:

Activity Logs (see page 121)
Implement Online Activity Logging (see page 122)
Administer Online Activity Log Files (see page 123)
Swap the Online Log (see page 124)
Online Log Exit (see page 124)
Online Logging Procedure (see page 126)
Hardcopy Activity Log (see page 128)
Swap the Hardcopy Log (see page 131)
Reuse of Hardcopy Log Data Sets (see page 132)
Cross-Reference of Hardcopy Logs (see page 132)
I/O Errors on the Hardcopy Log (see page 133)
Write to the System Log (see page 133)

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:

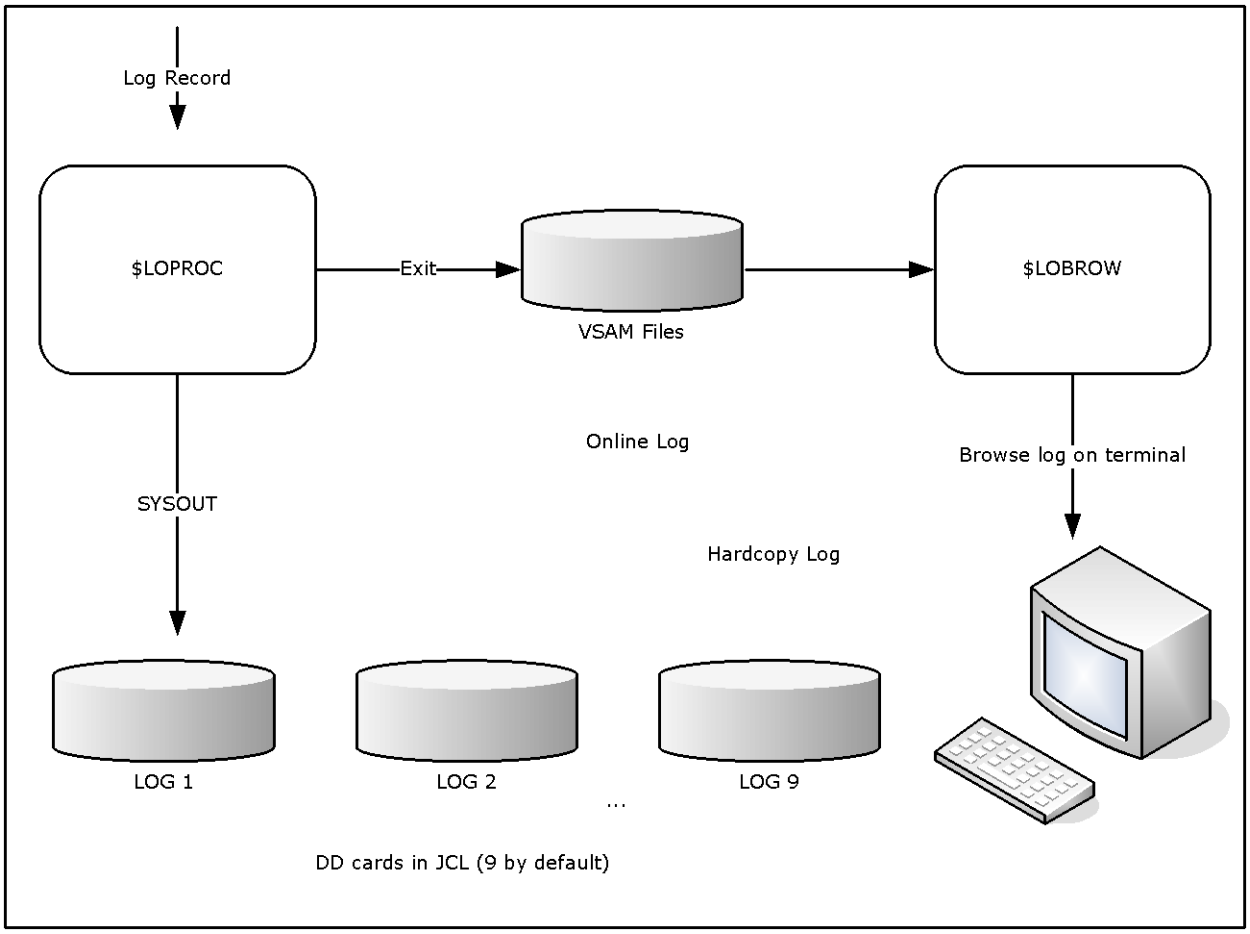
- Online
- Hardcopy

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**).

Implement Online Activity Logging

During initialization, the region allocates, by default, three VSAM log files for online logging. However, you can allocate up to seven files.

Note: The log file IDs are of the form NMLOG*nn* and the data set names are of the form *dsnpref.rname*.NMLOG*nn*. (*dsnpref* is the data set prefix used during product installation and *rname* is the name of the region.)

Use Additional Log Files

If you want to make more than three files available to the region, define the new VSAM files and then customize the LOGFILES parameter group by defining additional logging data sets.

To customize the LOGFILES parameter group

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. Press F8 (Forward) to display the next page.

4. Complete the fields for each file you want to make available. To allocate more files, press F8 (Forward) again.

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

6. Press F6 (Action).

   The changes are applied.

7. Press F3 (File).

   The changes are saved.

Note: For more information about using this panel, press F1 (Help).

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).

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 16: Implementing Print Services

This section contains the following topics:

Print Services Manager (see page 135)
Access PSM (see page 136)
Add a Printer Definition (see page 137)
List Printer Definitions (see page 137)
Add a Form Definition (see page 137)
List Form Definitions (see page 138)
Add Control Characters (see page 138)
List Control Characters (see page 138)
Add a Default Printer for a User ID (see page 139)
List Default Printers (see page 139)
Clear the Printer Spool (see page 140)
Exits to Send Print Requests to a Data Set (see page 140)
Print-to-Email (see page 145)

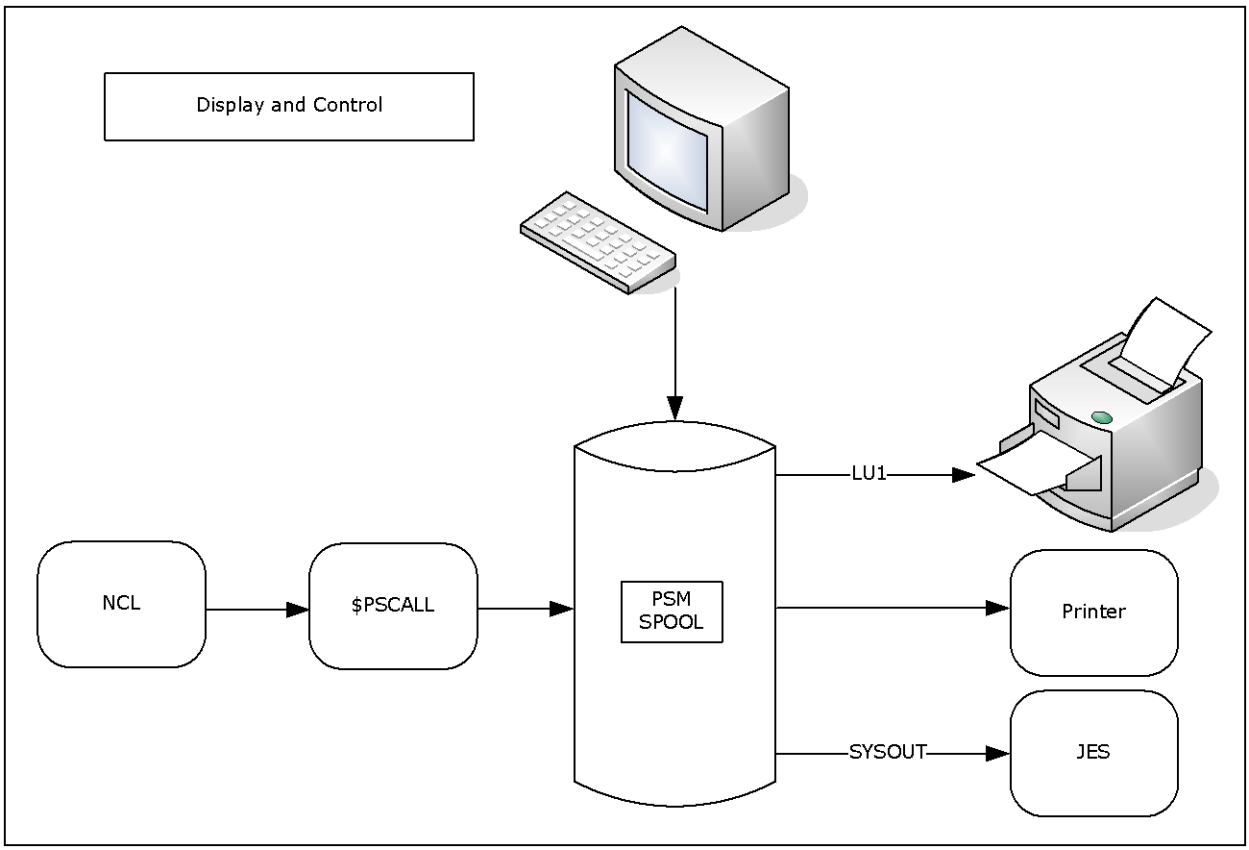
Print Services Manager

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*.

Chapter 17: Implementing the NetMaster-to-NetSpy Interface

This section contains the following topics:

Customize the NetMaster-to-NetSpy Interface (see page 147)
Manage NetMaster-to-NetSpy Connections (see page 148)
Manage CA NetSpy Alerts and Monitors (see page 148)
Issue CA NetSpy Commands (see page 150)

Customize the NetMaster-to-NetSpy Interface

If you use CA NetSpy, you can define an interface to it to perform some CA NetSpy functions from your CA NetMaster region.

To customize the interface, update the NETSPYLINKS parameter group in Customizer.

To update the NETSPYLINKS parameter group

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

   The Customizer : Parameter Groups list appears.

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

   The NETSPYLINKS - Links to NetSpy Applications panel appears.

3. In the Connections fields, specify the values of the NSYXNAME parameter in the INITPRM member of the CA NetSpy that you want to link to your region.

4. Enter a value in each field that you require.

   For more information about completing this panel, press F1 (Help).

5. Press F6 (Action).

   The changes are actioned.

6. Press F3 (File).

   The changes are saved.

   Note: The Enable NetSpy Alert Processing field in the NETSPYLINKS parameter group lets you switch off the receipt of all alerts from CA NetSpy. Normally, you should leave the field to its default value of YES; however, you may want to enter **NO** to switch the alerts off under abnormal conditions (for example, when the region is flooded by these alerts).

Manage NetMaster-to-NetSpy Connections

Your region provides a control for the NetMaster-to-NetSpy interface. From this interface you can do the following:

- Activate and inactivate connections to CA NetSpy.

  Note: These connections are defined in the NETSPYLINKS parameter group.

- Use the console command interface to modify control parameters for CA NetSpy.
- Stop the interface to CA NetSpy.

To control connections to CA NetSpy

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

   The NetSpy Connections panel appears. This panel displays the status of defined links to CA NetSpy.

```
PROD  ---------------------- NetSpy Connections -------------------------------
 Command ===>                                                 Scroll ===> CSR

                                      A=Activate I=Inactivate P=Stop F=Modify
    Link Name    ACB Name Status     System   Ver  STC      ITVL
    $ESLA31IVS40 -        FAILED     -        -    N/A         0
    $ESLCSNM21NX -        FAILED     -        -    N/A         0
    $ESLCSNM22NX CSNM22NS RUNNING    XE61     11.0 N/A        60
    $ESLQANM1NX  -        FAILED     -        -    N/A         0
    **END**
```

   Note: For more information about the information displayed and actions available on this panel, press F1 (Help).

Manage CA NetSpy Alerts and Monitors

Your region can receive alerts from CA NetSpy. CA NetMaster alerts are generated for each alert generated by CA NetSpy that is received. The following types of alerts are generated:

Alerts from EPS Services

For general Alert Monitors defined through CA NetSpy.

Alerts from the NetMaster-to-NetSpy interface

For user Alert Monitors defined through CA NetMaster.

Manage NetSpy User Alert Monitors in CA NetMaster

To manage CA NetSpy user Alert Monitors

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

   The NetSpy Monitors List appears. This panel lists the CA NetSpy user Alert Monitors defined for a resource.

   Note: For more information about the information displayed and actions available on this panel, press F1 (Help).

Define CA NetSpy User Alert Monitors

Authorized users can define, delete, and update CA NetSpy user Alert Monitors for a particular resource.

To define a CA NetSpy user Alert Monitor

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

   The NetSpy Monitors List appears.

   Note: For more information about these monitors, press F1 (Help)

2. Press F4 (Add).

   The NetSpy : Monitor Definition panel appears.

3. Complete the fields on this panel and press F3 (File).

   The definition is saved.

Issue CA NetSpy Commands

Your region supports a CA NetSpy command interface. This interface allows a subset of display commands to return information to your region.

To issue a command

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

   The NetSpy Commands panel appears. This panel lists the CA NetSpy commands that you can issue.

2. Enter **S** next to the command.

   The NetSpy : Command Arguments panel appears.

3. Enter values in the fields for any operands that you want to use.

4. Press F6 (Action).

   The command output appears.

   Note: You can also issue a command, together with any operands, by entering it directly at the command prompt on the NetSpy Commands panel. If you enter a command without any operands, it is issued with its default operands.

Chapter 18: Setting Up CA NetMaster SM for CICS

This section contains the following topics:

CA NetMaster SM for CICS Interface (see page 151)

CA NetMaster SM for CICS Interface

An interface to CA NetMaster SM for CICS is provided. When this interface is enabled, it does the following:

- Passes additional CICS information about TCP connections to your product, such as user ID, CICS transaction name, and CICS transaction number.

  This information then becomes available through central network management displays within your product.
- Allows you to monitor CICS IP resources (resource class CICMON).

For more information, see the *CA NetMaster SM for CICS Installation Guide*.

Configure CA NetMaster SM for CICS

To configure CA NetMaster SM for CICS in your region, set the PROD=SOCKETMGMT parameter in your RUNSYSIN member.

Customize CA NetMaster SM for CICS

If CA NetMaster SM for CICS is configured in your region, it is automatically enabled when you implement your region. You can then customize it if necessary.

To customize CA NetMaster SM for CICS

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

   The Customizer : Parameter Groups panel appears.
2. Select the SOCKETMGMT parameter group.

   The SOCKETMGMT - SocketMgmt Agents parameter appears.
3. Specify (YES or NO) whether the region adds resources dynamically to the system image.
4. Specify a background user ID and password.

5. Specify (YES or NO) whether to use your product's signon details for user access to CICS.
6. Press F6 (Action).

   The changes are applied.
7. Press F3 (File).

   The settings are saved.

Issue Socket Management Commands in a Command Entry Environment

To issue a Socket Management command in a Command Entry environment

1. Enter /IPMON at the prompt.

   The IP Resource Monitor appears.
2. Enter **CMD** (Command Entry - SocketMgmt) next to a CICMON resource.

   A Command Entry panel appears.
3. Enter a Socket Management command in the SocketMgmt Command field.
4. Press F4 (Execute).

   The command output appears on the Command Entry panel.

   Note: For information about the details displayed and actions available, press F1 (Help).

Chapter 19: Troubleshooting

This section contains the following topics:

About self-test (see page 153)
Display the Initialization Log (see page 154)
SNMP Data Problems (see page 154)
Commonly Encountered Errors (see page 156)
Provide Information to Technical Support (see page 160)

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. Do *one* of the following:
   - Enter **/IPTEST** at the prompt.
   - Enter the **SELFTEST** command on the OCS panel.

To access online help about the SELFTEST command

1. Enter *one* of the following commands on the OCS panel at the prompt.
   - **SELFTEST ?**
   - **SELFTEST HELP**

Display the Initialization Log

The initialization log can be used to help diagnose problems that may occur during the following:

- When your region starts
- When you update a parameter group

You can display the initialization log for all parameter groups, or by parameter group.

To display the initialization log

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

   The Customizer panel appears.

2. Enter **L** at the prompt.

   The Initialization Log appears.

To display the initialization log for a particular parameter group

1. Enter **/PARMS**.

   The Customizer : Parameter Groups panel appears.

2. Enter **L** (ILog) beside the parameter group for which you want to display the initialization log.

   The Initialization Log appears.

More information:

Region Customizer (see page 16)

SNMP Data Problems

If you receive any of the following errors, access to SNMP data may not be enabled:

- No entries in routing table
- SNMP errors returned from the stack's IP addresses
- Listener detectors always trigger

To enable access to SNMP data

1. Check that the SNMP subagent has been configured in the profile TCP data set.

2. The TCP/IP subagent must be able to connect to the SNMP agent. To do this, it uses a UNIX Stream socket represented by the file name in the dpiPathNameForUnixStream MIB object.

   To set the file name for the UNIX Stream socket, do *one* of the following:

   - Use the dpiPathNameForUnixStream statement in the OSNMPD.DATA file
   - Use the -s OSNMPD initialization parameter
   - The UNIX stream socket must be a UNIX System Services (USS) Special File. If the file exists, ensure that:
   - It has the correct file attributes
   - It has permission bits set to allow both read and write
   - If the file does not exist, but the file name is specified as described above, the SNMP agent will automatically create it.

3. To determine the file name, issue the USS command:
   ```
   osnmp  get dpiPathNameForUnixStream.0
   ```
   The file name is displayed—the default file name is /tmp/dpi_socket.

4. To determine the attributes and permissions, issue the USS command:
   ```
   ls -1 /tmp/dpi_socket
   ```
   The file attributes and permissions are displayed. For example:
   ```
   crw-r-----              1 OMVSKERN SYS1       6,  0 Jan 27 03:35 dpi_socket
   ```
   The first character (c) indicates this is a Special File. The following nine characters show permissions. The values 6 and 0 preceding the date indicate the major and minor node type. The UNIX Stream socket must be major node type 6.

5. To create the file, use the MKNOD command located in the /usr/sbin directory. For example:
   ```
   cd /usr/sbin
   mknod /tmp/dpi_socket c 6 0
   ```
   A character special file is created; major type 6, minor type 0.

For more information, see the following:

- IBM's *Communications Server IP Configuration* for more information about configuring the SNMP Agent and configuring community names
- IBM's *UNIX System Services Planning Manual* for more information about creating special files
- IBM's *UNIX System Services Command Reference* for more information on how to use and interpret USS commands

Commonly Encountered Errors

The following table describes common errors or conditions you can encounter, their probable cause, and the recommended action to take to resolve them:

Error Type or Symptom	Probable Cause	What to do...
NETSTAT or Connections List Errors:		
General Note:	Incorrect or incomplete configuration causes most of errors from NETSTAT or List Connection requests.	Ensure that all steps in the tasks for your environment have been successfully completed. **Note:** For more information, see the *Installation Guide*.
IPNS0807 UNIX SHELL OPEN REQUEST HAS FAILED, CALL=0 RC=0 RSN=0000-0000	SOLVE SSI software is out of date.	Ensure that the SOLVE SSI run-time libraries contain the latest release of security and system services.
IPNS0806 UNIX SHELL REQUEST OPEN HAS FAILED DUE TO UNIX interface not available	SOLVE SSI is not configured to act as the USS interface.	Update your SOLVE SSI configuration to include the start parameter UNIX=YES.
	The user ID associated with the SOLVE SSI started task does not have an OMVS segment.	Set up an OMVS segment in the CA ACF2 for z/OS, CA Top Secret for z/OS, or RACF profile of the user ID associated with the SOLVE SSI started task. **Note:** For more information, see the *Installation Guide*.
IPNS0809 UNIX SHELL INITIALIZATION FAILED, CALL=760 RC=129 RSN=053B-006C	The user ID associated with the SOLVE SSI started task has in its OMVS segment the name of a shell program that could not be invoked.	Ensure that this user ID has a valid shell program specified in the PROGRAM section of its OMVS segment. **Note:** For more information, see the *Installation Guide*.

Error Type or Symptom	Probable Cause	What to do...
Cannot change to the HOME directory.	The user ID associated with the SOLVE SSI started task does not have at least read access to the home directory defined in its OMVS segment.	Ensure that this user ID has at least read access to the specified home directory. **Note:** For more information, see the *Installation Guide*.
User ID not displayed in list connections, or IP address not being displayed in EASINET.	The default application for Telnet is not performing user ID registration. The following causes are possible:	
	■ SYSPARM IPCHECK is set to NONE. ■ The default application using RACF is not SOLVE:Access.	Set IPCHECK to REGISTER or VERIFY.
Errors Starting Sockets Interface		
N3B290 WARNING - UNABLE TO OBTAIN TCP/IP HOST NAME, USING 'LOCALHOST' N3B291 WARNING - UNABLE TO OBTAIN TCP/IP HOST ADDRESS USING 127.0.0.1 (LOOPBACK)	The DNRALC*xx* and DNRHST*xx* members have not been configured as specified. For example, DNRALC*xx* does not contain an entry for the CA TCPaccess CS for z/OS subsystem name.	Follow the instructions for setting up DNR in the *Installation Guide.*
TVG101 TCPAXS INTERFACE INITIALIZATION FAILURE 31 - BAD RET HOSTNAME LEN: 0 N3B220 TCPIP START (TYPE=TCPAXS) FAILED, 7 - TCPAXS MODULE NM053030 INITIALIZATION FAILURE, RC: 8	The DNRALC*xx* member contains an entry for the CA TCPaccess CS for z/OS subsystem name, which translates the name directly to an IP address, not to a host name.	Follow the instructions for setting up DNR in the *Installation Guide*.

Error Type or Symptom	Probable Cause	What to do...
Name lookup is not working.	The host that is defined as the Domain Name Server (DNS) is down or incorrectly defined.	Ping the name server host to verify that it is accessible from the system. **IBM TCP/IP:** Review the NSINTERADDR parameter specified (up to three occurrences allowable) in the TCPIP.DATA data set. This parameter contains the IP address of a DNS system. **CA TCPaccess CS for z/OS:** Review the contents of the DNRNSC*xx* member in the CA TCPaccess CS for z/OS PARM data set.
	The host's files are incorrect or out of date.	**IBM TCP/IP:** Review the contents of the *prefix*.HOSTS.LOCAL data set. If the *prefix*.HOSTS.LOCAL data set has been updated since your product was started and you want to refresh it, go to the SOCKETS parameter group.
Name lookup, ping, or traceroute is slow.	The Name Server is unreachable, inoperative, or slow.	**CA TCPaccess CS for z/OS:** Update the SOCKETS parameter group to specify DNR mode 'Local'.
IPSNPK09 No resp from &P1 – SNMP may be unauth/unavailable	The device does not support SNMP, or you are not authorized.	Define SNMP security.

Error Type or Symptom	Probable Cause	What to do...
Mail is not being sent for the Email trouble ticket.	The job name or destination on the trouble ticket interface definition is not running.	Check the trouble ticket job name.

UNIX SHELL SSI Interface Self-Test Errors:

Error Type or Symptom	Probable Cause	What to do...
General Note:	Incorrect or incomplete configuration causes most of errors from the UNIX shell SSI Interface section of the self-test.	Ensure that all steps in all tasks in this section have been successfully completed. **Note:** For more information, see the *Installation Guide*.
IPDI5227 Warning: Unexpected response from NETSTAT, see the log for details.	Netstat errors indicate various conditions, which can affect your system.	Look in the activity log for additional error messages (such as messages with a prefix of IPNS or EZA).

Provide Information to Technical Support

Sometimes problems occur that require more in-depth diagnosis. A running CA NetMaster region may contain information that helps Technical Support determine the cause of a problem; therefore, Technical Support may ask you to provide a dump of a running region.

The latest Activity Log provides a history of events. Keep all logs since the system was started, and send to Technical Support. Also, send the JES system log and the results of $$SYSPRO.

Use IBM Utility TERSE to reduce the sizes of the dumps, activity logs, and other information gathered.

To dump a CA NetMaster region

1. Ensure that the CA NetMaster JCL parameter XOPT=(option|,option,...) includes the SDUMP option.

   The SVCDUMP can be found on SYS1.DUMP, or equivalent. The NetMaster JCL parameters can be found in the RUNJCLIN member.

2. Ensure that the SDATA parameters for SDUMP contain the following options:

   ```
   (CSA,LPA,LSQA,PSA,RGN,SQA,SUM,TRT)
   ```

3. Issue the following command:

```
DUMP COMM=(Dump of NetMaster)
R nn,JOBNAME=jobname,
SDATA=(CSA,PSA,RGN,TRT,LPA,SQA,LSQA,SUM),END
```

Note: The preferred dump DSN should be blocked at LRECL 4160, BLKSIZE 24960.

Appendix A: SMF Record Structure

This section contains the following topics:

Performance Monitoring SMF Record Format (see page 161)

Performance Monitoring SMF Record Format

Position	Length in Bytes	Description
1 to 18	18	SMF record header
19 and 20	2	CA NetMaster NM for TCP/IP category ID Always X'5000'
21 to 32	12 blank padded	NMID Example: NETMASTR*bbbb* (where *b* is a blank)
33 to 34	2	Record type DS or DH (where DS is a one-off sample record and DH is the hourly roll up)
35 and 36	2	Length of data Example: X'0007' indicates that the data is 7 bytes long
37 and 38	2	Field identifier (see page 162)
39 to *n*	Varying	Data

Field Identifier

Field Identifier	Description
X'0001'	Resource application ID
X'0002'	Resource class
X'0003'	Resource group name
X'0004'	Resource ID
X'0005'	Attribute ID
X'0006'	Attribute qualifier
X'0007'	Attribute type (counter, gauge, enumerated, or total)
X'0008'	Attribute value if numeric
X'0009'	Attribute character value if not numeric
X'000A'	Minimum value (for gauge only)
X'000B'	Maximum value (for gauge only)
X'000C'	Period covered by the sample (only for enumerated attribute types in DH record types)

From the Resource Monitor, enter **H** next to a resource to display a list of attributes that can be monitored by that resource type.

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

Appendix B: IP EDS Events

This section contains the following topics:

IP Node Monitor State Changes (see page 163)
Trap FTP, Telnet, Connection, and Message Events (see page 164)

IP Node Monitor State Changes

A change in the state of an IP node monitored by the IP Node Monitor is advertised by an Event Distribution Services (EDS) event, which triggers a display update for anyone watching the device status display. The EDS event also can be picked up by any other process, which requires this information.

The EDS event created for a state change has the following attributes:

EDS Event	Attribute
Name	$IPNMON.STATE.UPD
Resource	The IP address of the node.
Ref	*oldstate - newstate*

Possible status values are:

Status Value	Description
Unknown	Ping has not completed.
OK	Ping completed successfully.
Timeout	Ping timed out.
SNMP Error	Ping completed successfully but an SNMP request has returned an error.

Trap FTP, Telnet, Connection, and Message Events

You can trap the following:

- FTP, Telnet, and connection message events from SMF exits (see page 27)
- Console and syslog messages from CA TCPaccess CS for z/OS (see page 27)

You can set up event detectors to trigger alerts and actions on receipt of events.

To trap FTP failures, use an FTPFAIL monitor. To trap other EDS events, use a CUSTOM monitor.

The EDS events that are issued when an FTP, Telnet, or connection event takes place are listed in this table.

Event	Event Name	Object	Resource	Reference	Message ID	Client/ Server
FTP Retrieve	$IP.FTPLOG.RETR	Remote IP address	Data set name	FTP server name	IPFM2103 IPFM2113	S C
FTP Store	$IP.FTPLOG.STOR	Remote IP address	Data set name	FTP server name	IPFM2103 IPFM2113	S C
FTP Store Unique	$IP.FTPLOG.STOU	Remote IP address	Data set name	FTP server name	IPFM2103 IPFM2113	S C
FTP Append	$IP.FTPLOG.APPE	Remote IP address	Data set name	FTP server name	IPFM2103 IPFM2113	S C
FTP Logon Failed	$IP.FTPLOG.LOGONF	Remote IP address		FTP server name	IPFM2102	S
FTP Delete	$IP.FTPLOG.DELETE	Remote IP address	Data set name	FTP server name	IPFM2104	S
FTP Rename	$IP.FTPLOG.RENAME	Remote IP address		FTP server name	IPFM2105	S
FTP Retrieve Failure	$IP.FTPFAIL.RETR	Remote IP address	Data set name	FTP server name	IPFM2113 IPFM2129	S C

Event	Event Name	Object	Resource	Reference	Message ID	Client/ Server
FTP Store Failure	$IP.FTPFAIL.STOR	Remote IP address	Data set name	FTP server name	IPFM2113 IPFM2129	S C
FTP Store Failure Unique	$IP.FTPFAIL.STOU	Remote IP address	Data set name	FTP server name	IPFM2113 IPFM2129	S C
FTP Append Failure	$IP.FTPFAIL.APPE	Remote IP address	Data set name	FTP server name	IPFM2113 IPFM2129	S C
FTP Delete Failure	$IP.FTPFAIL.DELETE	Remote IP address	Data set name	FTP server name	IPFM2114	S
FTP Rename Failure	$IP.FTPFAIL.RENAME	Remote IP address	Old data set name, new data set name	FTP server name	IPFM2115	S
Telnet connection started	$IP.TNLOG.START	Remote IP address	Telnet LU name	Application name	IPCM2002	S
Telnet connection started	$IP.TNLOG.START	Remote IP address	Telnet client job name	Telnet client node name	IPCM2013	C
Telnet connection stopped	$IP.TNLOG.STOP	Remote IP address	Telnet LU name	Application name	IPCM2003	S
Telnet connection stopped	$IP.TNLOG.STOP	Remote IP address	Telnet job name	Telnet client node name	IPCM2014	S
Connection started	$IP.CONNECT.START	Remote IP address	Client job name	Client job name	IPCM2311	-
Connection stopped	$IP.CONNECT.STOP	Remote IP address	Client job name	Client job name	IPCM2312	-
CA TCPaccess CS for z/OS message received	$IP.AXSLOG. MESSAGE	Severity code	CA TCPaccess CS for z/OS SSID	CA TCPaccess CS for z/OS message number	CA TCPaccess CS for z/OS message number	

References

For more information about the format of FTP records and how SMF exits are invoked, see IBM's *Communications Server IP Configuration Guide.*

For more information about FTP reply codes, see *RFC 959*, *File Transfer Protocol* .

Appendix C: Telnet Translation Tables

This section contains the following topics:

Specify Telnet Translation Tables (see page 167)

Specify Telnet Translation Tables

You can create a Telnet connection to a remote host. Telnet connections usually operate using the ASCII character set. Messages are translated between ASCII and EBCDIC when using Telnet connections from your product.

Note: You do not need to change the defaults unless you have problems with the way data is displayed on Telnet connections. For example, you may be using a national language character set.

Data translation between ASCII and EBCDIC is determined by the following:

- Translate Table Data Set—a partitioned data set containing the translation tables you want to use.
- Translate Table—a default value for the table name being used for Telnet connections. The table name is the name of the member in the partitioned data set. If you specify a data set without a table name, then your Telnet connections will use a default of TELNET.

To add your own translation tables, add a member to the data set. Each member in this data set contains two tables—the first translates from ASCII to EBCDIC, and the second from EBCDIC to ASCII. The following table formats are supported:

- Source form—used by Communications Server
- Binary form—used by Communications Server and TCPaccess Open Edition Support

Note: If you are using Communications Server, see the IBM *Communications Server Customizing and Administration Guide* for more information.

If you are using TCPaccess, you can generate the binary tables by using the TSO CONVXL8 or TSO LOADXL8 commands supplied with TCPaccess Open Edition Support.

Note: For more information about using Telnet connections, see the *User Guide*.

To specify the Telnet translation tables

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

   The Customizer : Parameter Groups panel appears.

2. Select the TELNETTRT parameter group.

   The Telnet Translate Parameter appears.

3. Specify a translate table DSN and translate table.
4. Press F6 (Action).

   The changes are applied.

5. Press F3 (File).

   The settings are saved.

Appendix D: Health Checks

This section contains the following topics:

CA Health Checker (see page 169)
NM_ACB (see page 170)
NM_INITIALIZATION (see page 171)
NM_PA_STACKS (see page 172)
NM_SOCKETS (see page 173)
NM_SSI (see page 174)
NM_WEB (see page 175)

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 NM for TCP/IP 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 NM for TCP/IP 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 NM for TCP/IP 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 NM for TCP/IP 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_PA_STACKS

Description

Checks that active stacks are known to Packet Analyzer. The check runs every 15 minutes.

For CA NetMaster NM for TCP/IP to monitor the packets flowing through an active stack, Packet Analyzer must know of the stack.

Best Practice

None.

Parameters Accepted

None.

Debug Support

No.

Verbose Support

No.

Reference

None.

Non-exception Messages

The following messages can appear in health checker:

- All active stacks are known to Packet Analyzer.
- 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.
- NMH0115E Not all active stacks are known to Packet analyzer.

NM_SOCKETS

Description

This CA NetMaster NM for TCP/IP 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 NM for TCP/IP 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 NM for TCP/IP 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

$

$LOBROW procedure • 121
$LOPROC procedure • 121
$PSDS81X printer exit for a data set • 140

&

&INTCMD verb • 130

A

activity logs
  cross referencing • 132
  deal with I/O errors • 133
  file structure • 126
  format • 129, 130
  hardcopy • 128, 130
  logged information • 121
  online swapping • 124
  swapping • 131
ALLOC command • 132
application name definitions
  event processing • 30
  exporting • 24
  importing • 24
  working with • 24
applications
  connections, and • 21, 23
attributes, types • 43
automatic log swapping • 133
Automation Services
  multisystem operation • 70
AUTOTABLES parameter group • 18

B

baselines
  types • 44
BSYS, effect on multisystem implementation • 72

C

CICS commands, issuing • 152
clear printer spool • 140
commands, SHOW
  SHOW PARMS • 15
commands, specific
  ALLOC • 132
  LOGSWAP • 132
configure multiple regions • 61
connection events, trap • 164
connections
  user ID associations • 25
considerations
  multisystem implementation • 69
contacting technical support • 3
control characters, printer
  add • 138
cross referencing logs • 132
CTRACE
  create external writer • 33
  defined • 33
  enable • 33
  verify setup • 35
customer support, contacting • 3
Customizer parameter groups • 16
  FTLOGS • 122
  SYSTEMID • 16

D

database
  icon panel • 70
database synchronization
  maintain • 78
default printers
  assign • 139
domain ID, defining • 16

E

EDS events • 164
emails of printed output • 145
EPS (EndPoint Services), multisystem support in sysplex • 68
errors in activity log • 133
events
  recorded • 27
exits
  printers • 140
  user ID associations • 25
external writer, create • 33

F

file IDs, logs • 122
focal point regions
  knowledge base synchronization • 70
form definitions • 137
  list • 138
formats
  activity log • 129
  logged information • 129
FTP, trap events • 164

G

graphical monitor
  customize • 93

H

hardcopy log, format • 130
Health Checker • 169

I

icon panel database • 70
identify your region to users • 16
implementation considerations, multisystem environment • 69
initialization files • 61
IPFILES parameter group • 31

J

JCL parameters
  customize your region • 15
  displaying current settings • 15
  specify • 15
JCL parameters, specific
  NMDID • 16

K

knowledge base
  linked • 70
  monitor synchronization • 77
  staging files • 78
  synchronize focal point regions • 70
  synchronize subordinates • 70
  update • 78

L

links
  multisystem support • 67
  unlink a region • 79
LOAD command
  checkpoint restart • 41
log data sets, wrap • 132
log file IDs • 122
LOGPAGE operand • 130
logs
  activity • 126
LOGSWAP command • 132

M

maintenance, MIBs • 57
MIB attributes
  add • 47
  monitor • 46
  resource classes • 48
MIBs maintenance • 57
monitoring
  attributes • 43
  MIB attributes • 46
multiple regions
  configure • 61
multisystem support
  considerations • 69
  how it works • 66
  multisystem support, enabling • 65
  sysplex • 68

N

NCL procedures
  $LOBROW • 121
  $LOPROC • 121
  INIT member • 15
  PSM to data set exit • 140
  READY member • 15
NMDID JCL parameter • 16

O

online activity log • 129

P

Packet Analyzer
  about • 21
  application names and connections • 21, 23
  duplicate definitions • 24
  purge requests • 23
  requests • 23

set up • 23
status • 23
panels
SocketMgmt Command Entry • 152
paper definitions
add • 137
list • 138
parameter groups
Customizer • 16
FTLOGS • 122
SYSTEMID • 16
printer definitions • 137
list • 137
Print-to-Email • 145
printer exit procedure
for writing to data set • 140
printer requirements
clear printer spool • 140
control characters • 138
setup definition • 138
printers
spool • 140
PSM
access • 136
customize • 135
facilities • 135
send print requests to data set • 140

R

regions
BSYS background user considerations • 72
define to users • 16
domain ID • 16
link • 70
linked, keeping track of • 78
resources
MIB attributes • 48
RFC 959, File Transfer Protocol • 166

S

security exit, user ID associations • 25
setup definition • 138
SHOW PARMS command • 15
SmartTrace
defined • 33
Socket Management, issue CICS commands • 152
STACK class resources
packet analysis requests • 23
staging file • 72, 78
state, change of • 163
subordinates
knowledge base synchronization • 70
support, contacting • 3
synchronize databases
link regions • 70
maintain synchronization • 78
SYSLOG operand • 133
SYSOUT • 132
SYSPARMS, general information
command format • 17
specify in INIT member • 17
system identifier • 16
system images, controlling
checkpoint restart • 41
system log • 133
PPO messages • 133
SYSTEMID parameter • 16

T

TCP/IP panels
Start CTRACE • 35
technical support, contacting • 3
Telnet, translation tables • 167
time change, effect on log format • 130
timer commands • 129
transient logs
size • 20
translate table • 167
translating between ASCII and EBCDIC • 167

U

unlink a region • 79
user ID, connections association • 25
user profiles
icon panel, adding • 109

V

verbs
&INTCMD • 130

W

wrap log data sets • 132