CA NetMaster® Network Management for TCP/IP

Implementation 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® Network Management for SNA (CA NetMaster NM for SNA)
- CA SOLVE:Operations® Automation (CA SOLVE:Operations Automation)
- CA Top Secret® for z/OS (CA Top Secret for z/OS)
- CA ACF2™ for z/OS (CA ACF2 for z/OS)
- CA Common Services™ for z/OS (CA Common Services for z/OS)
- CA OPS/MVS® (CA OPS/MVS)
- CA Service Desk for z/OS (CA Service Desk)
- CA TCPaccess™ Communications Server for z/OS (CA TCPaccess CS)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Introduction

This section contains the following topics:

About This Guide

After you have completed the tasks in the *Installation Guide*, you should have a working CA NetMaster NM for TCP/IP region, with a minimum of configuration tasks performed.

This guide describes the tasks that you can perform to configure the system to suit your requirements. You do not have to configure your entire system at one time; in fact, some tasks you may never do. If you do perform the tasks described, we recommend that you perform the tasks in the same order as they appear in this guide.

We recommend that you configure one region at a time, and ensure that the region is configured and working correctly before you link it or deploy it on additional regions.

Chapter 2: Configuring IP Node Monitoring

This section contains the following topics:

IP Nodes

An IP node is any host that can be reached from the z/OS host using IP. It includes routers, servers, workstations, other LPARs, and interfaces. Other LPARs can also be Enterprise Extender (EE) remote hosts. Every node has a unique network address.

An IP node definition is attached to the system image.

Note: A system image is a collection of resources. System images have unique names, generally the system ID and a version number, for example, SYS1-0001.Only one system image is loaded by a CA NetMaster NM for TCP/IP region at one time. For more information about system images, see the *Administration Guide*.

You can monitor IP nodes. Monitoring is determined by the information specified in the IP node definition. You can also include the definition in a monitoring map (see page 59).

Display IP Nodes

When you set up a region for the first time, Express Setup automatically discovers your IP nodes. To discover your IP nodes, Express Setup uses the addresses in the routing tables of your primary IP stack. The discovery radiates one hop with a time limit of 2 minutes (by default).

To display all IP nodes, enter **/IPNODE** from the command prompt.

Delete an IP Node

Express Setup usually finds a lot of IP nodes very close to the host; however, it may find nodes that you do not want to monitor. You should review all of the nodes discovered and delete the ones that you do not want to monitor.

Important! Do not monitor large numbers of non-critical nodes unnecessarily because this increases CPU usage and increases the number of alerts raised.

To delete an IP node

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

   The IP Node Monitor appears.

2. Enter **DEL** beside the IP node that you want to delete, and then press Enter.

   The IP node is deleted.

Add an IP Node

Express Setup (by default) does not find IP nodes that are further than two or three hops; therefore, if you want to monitor one of these nodes, you must add it manually.

Note: If you want to discover more IP nodes with Express Setup, you can edit *dsnpref.rname*.TESTEXEC($RMEXPR6), which is distributed in CC2DEXEC. For more information, see the *Installation Guide*.

Use descriptive and meaningful IP node names. The IP node name is used only by the IP node monitor and does not need to be the same as the IP address or IP host name. Choose IP node names that everyone recognizes. Express Setup often uses the IP address as the IP node name; however, you can rename these.

To add an IP node

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

   The IP Node Monitor appears.

2. Press F4 (Add).

   The System Image List appears.

3. Type **S** beside the system image to which the node belongs.

   The IP Node General Description panel appears.

4. Complete the following fields:

   IP Node Name

   Specifies the name of the IP node that you want to add.

   IP Addr/Host Name

   Specifies the IP address to monitor.

   Monitor by Host Name

   Specifies whether to use the IP address or host name during monitoring. If you select YES, the host name is resolved to an IP address each time the IP node is monitored. Use this option if the node's IP address may change, for example, if DHCP is used, or for IPv6 hosts.

   Group Name

   Specifies the name of the monitor group.

   Note: Enter a question mark (?) to obtain a list of existing monitor groups.

   Short Description

   Briefly describes the IP node.

   Press F4 (Save).

   The IP node definition is saved.

Organize IP Nodes

When you define an IP node, you also attach it to an IP node monitor group. The monitor group defines the checks performed and the attributes monitored. These are then used by all IP nodes that belong to that monitor group. A monitor group can define the following:

- How often the nodes are checked
- The SNMP performance attributes monitored, as well as PINGRTT and NETSTATUS
- The alerts raised and the actions performed

You can set up IP node monitor groups for different device types, and the same device type can also have multiple different groups. Some groups can do more performance monitoring, more frequent checking, or different actions when problems occur.

The following IP node monitor groups are provided:

Standard

Checks the network status (NETSTATUS) and performs a PING every 10 minutes. An alert is raised if the status is TIMEOUT or ERROR.

LowLevel

Checks the network status (NETSTATUS) and performs a PING every hour. No alerts are raised.

CiscoPerfIntens

Monitors the general availability of Cisco routers. The group checks the network status and performs a PING every 10 minutes. If the status is TIMEOUT or ERROR, an alert is raised. It monitors SNMP interface in (IfInDiscards) and interface out (InOutDiscards) discards, and the CPU 5-minute average (CiscoavgBusy5).

CiscoMonIntens

Performs the same functions as CiscoPerfIntens, plus monitors interface in (IfInErrors) and interface out (IfOutErrors), packet rates in (CiscoifInPkts) and packet rates out (CiscoifOutPkts), and router memory usage (CiscobuffNoMem).

Express Setup places all the IP nodes that it finds in the Standard group; however, you can assign them to another group.

Add an IP Node Monitor Group

If you do not want to use one of the IP node monitor groups provided, you can define your own. You can set up an IP node monitor group based on function, hardware type, importance, geographical location of hosts, and so on.

To add an IP node monitor group

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

   The IP Node Monitor Group List appears.

2. Press F4 (Add).

   The Monitor Group Details panel appears.

3. Complete the following fields:

   Name

   Specifies the name of the monitor group.

   Description

   Briefly describes the monitor group.

   Press F4 (Add).

   The Selectable Attributes List appears.

4. Enter **S** beside the attribute that you want to monitor.

   The attribute is added to the Monitor Group Details panel.

5. Enter **U** beside the attribute.

   The Alert Control Details panel appears.

6. Enter **U** beside the Alert Type that you want to apply to this attribute.

   The Alert Details panel appears.

7. Enter the alert details.

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

   If you want to add an automated action (see page 17), go to step 8.

   If you do not want to add an automated action, go to step 10.

8. (Optional) Press F5 (Actions).

   The Alert Automated Actions panel appears.

9. (Optional) Press F4 (Add) and define the automatic action.

10. Press F3 (OK).

    The IP node monitor group is added.

Alert Conditions

An alert is a notification of a fault, which you can view on the alert monitor. You can define the alert conditions on IP nodes through an IP node monitor group. Alert conditions are set separately for each IP node monitor group; therefore, the same attribute can have different alert conditions in different groups.

Numeric attributes, such as PINGRTT, have the following alert conditions:

- Above and below a threshold (absolute value)
- Above and below a baseline (moving average)

Note: Because IP nodes are sampled regularly and often at short intervals, HourOfDay is usually a suitable baseline type for IP nodes.

Each single alert condition can raise one of five different alerts. These alerts are of varying severity and text, which is based on the threshold value or baseline percentage. For example, when PINGRTT of a node in the FTPSERVERS group is greater than 5000, you raise a severity 1 alert with the text:

This node is extremely slow.

Also, when PINGRTT of a node in the FTPSERVERS group is greater than 100, you raise a severity 4 alert with the text:

This node is slightly slow.

You can also suppress alerting when an alert condition is satisfied. This feature enables you to trigger actions without sending an alert. To suppress alerting, specify **0** for the alert severity.

More information:

Alerts (see page 65)

Automatic Actions

You can set up the following actions to run automatically when an alert condition is satisfied.

Notify

Sends a user notification. This notification can be delivered in the following ways:

- Broadcast message
- TSO message
- Electronic mail
- Your own exit (NCL) routine

Command

Issues a system command.

Execute NCL

Runs an NCL procedure.

Note: You can execute a REXX procedure from an NCL procedure.

Trouble Ticket

Creates a trouble ticket that is based on the characteristics of the alert. You would usually set this action up to send a request using electronic mail.

Automation Services Process

Runs an Automation Services process to perform one or more actions, for example, write to the activity log.

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

Example: Define an IP Node Monitor Group

This example shows how to create an IP node monitor group named PING, raise a severity 3 alert when a PING takes longer than 1 second, and send an email trouble ticket to notify the operator.

To define the IP node

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

   The IP Node Monitor Group List appears.

2. Press F4 (Add).

   The Monitor Group Details panel appears.

3. Enter a Name and Description for the monitor group, and whether you want to send the performance data to ReportCenter.

   Note: For more information about ReportCenter, see the *ReportCenter Guide*.

   Press F4 (Add).

   The Selectable Attributes List appears.

4. Select PING.

   The Monitor Group Details panel appears, similar to the following:

```
PROD------------ Automation Services : Monitor Group Details ------------------
Command ===>                                                  Scroll ===> CSR

Name ........................ PING
Description ................. PING EXCESSIVE
Collection Status ........... ACTIVE            (Active or Inactive)
Send to ReportCenter? .........NO              (Yes or No)

                                                          S/U=Update R=Remove
     Attribute             Alert Summary                              Rate
     PING                                                            01:00
    **END**









 F1=Help      F2=Split     F3=Ok        F4=Add                  F6=Refresh
 F7=Backward  F8=Forward   F9=Swap               F11=Right    F12=Cancel
```

5. Enter **U** beside the PING attribute.

   The PING Alert Control Details panel appears.

6. Enter **U** beside the alert type RTT High Value.

   The High Alert Details panel appears.

7. Complete the fields, similar to the following:

```
PROD---------------- Monitor Attribute : High Alert Details --------------------
 Command ===>                                                  Function=UPDATE

 Resource ......... -                                  Group ... PING
 Attribute ........ PINGRTT
 Description ...... PING Round Trip Time (ms)
 Qualifier ........

 Å High Value Alert
 … Alert when value            Sev Alert Description
 … is greater than 1000         3  PING EXCESSIVE

 …            or >

 …            or >

 …            or >

 …            or >

 … Clear Alert when value is equal to or below



  F1=Help      F2=Split     F3=Ok                    F5=Actions
                            F9=Swap                F11=EditText F12=Cancel
```

8. Press F5 (Actions).

   The Available Actions panel appears.

9. Select AUTO_TROUBLE_TICKET.

   The Auto Trouble Ticket Details panel appears.

10. Complete the fields, similar to the following:

```
PROD------------ Alert Monitor : Auto Trouble Ticket Details ------------------
Command ===>

Short Description ... PING EXCESSIVE
EMAIL ADDRESS#1 ..... operator@company.com
EMAIL ADDRESS #2 ....



 F1=Help      F2=Split     F3=File
                           F9=Swap                                F12=Cancel
```

11. Press F3 (File) until the PING Alert Control Details panel appears. The details look similar to the following:

```
PROD---------- Monitor Attribute : PING Alert Control Details -----------------
Command ===>                                                  Scroll ===> CSR

Resource ......... -                                 Group ... PING
Attribute ........ PING
Description ...... Check Network Connectivity
Qualifier ........ ____________________
Baseline Type ...+ _________ (Daily, DayOfWeek or HourOfDay)
Three Strike Alert NO_       (YES or NO)
Rate ............. 60        (minutes)
PING Packet Size . 256__     (64-65519 bytes)
     Count ....... 3_        (1-10)
     Wait ........ 5_        (Timeout in seconds)
                             S/U=Update A=Actions C=Clear Actions R=Reset Alert
                                                 Max
    Alert Type          Summary                  Sev  Act#  Alert Text
    RTT High Value      Sev:3 >1000               3     1  PING EXCESSIVE
    RTT Low Value                                 -     -
    RTT Above Baseline                            -     -
    RTT Below Baseline                            -     -
    Unreachable Host                              -     -
    **END**
 F1=Help      F2=Split     F3=Ok                              F6=Refresh
 F7=Backward  F8=Forward   F9=Swap                           F12=Cancel
```

12. Press F3 (OK).

    The details are saved.

13. Press F3 (OK).

    The monitor group is created.

Chapter 3: Configuring Event Monitoring

This section contains the following topics:

Event Detectors

An *event detector* defines the network and systems events that you want to monitor, and what to do when the event occurs.

You can define an alert to raise, and you can define the wording of the alert. You can also define an automatic action (see page 17) to run.

Sample event detector definitions are supplied. Each type of event is represented in the samples. Use these definitions as examples when you create your own event detectors.

The following types of event detectors are available:

CCTN3270

Monitors Cisco channel card TN3270 log messages.

CONNECT

Monitors connections.

CONNSTAT

Monitors the status of TCP connections.

CONSOLE

Monitors system console messages.

CUSTOM

Monitors custom events.

FRAGMENT

Monitors IP packet fragmentation.

FTPFAIL

Monitors FTP failures.

ICMP

Monitors ICMP messages.

LISTENER

Monitors listening ports.

NOLISTEN

Monitors connection attempt failures due to a listener port not being active.

RTPRED5M

Monitors RTP pipe congestion.

SSLHFAIL

Monitors Secure Sockets Layer (SSL) handshake failures.

SVRRESET

Monitors TCP connections that a server resets.

TCPEND

Monitors the end of TCP connections by reason codes.

TCPSTART

Monitors the start of TCP connections.

Note: The CONNECT and LISTENER detectors operate by polling, as determined by the IPTIMING parameter group.

Define an Event Detector

To specify the type of event that you want to monitor, define an event detector.

Follow these steps:

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

   The Event Detectors Controls List appears.

2. Press F4 (Add).

   The Valid Value List appears.

3. Select a type (see page 21) from the list, and press Enter.

   The corresponding detector definition panel appears.

4. Complete the following fields:

   Short Description

   Briefly describes the event detector. This description appears on the Event Detector Controls List. Use this description in your own documentation.

   Status

   Specifies whether this rule detects events. Making a detector inactive means that you can keep a definition, but not have it checked.

5. Press F4 (Criteria) and define the criteria (see page 23) for events that you want to monitor.

6. Press F5 (Alert) and define the alert (see page 24).

7. (Optional) Press F6 (Actions) to define any action (see page 24) that you want the system to take in response to a triggering event.

8. Press F3 (File).

   The new detector is added.

Define Event Criteria

Event criteria define the conditions that trigger the alert, the actions, or both.

Follow these steps:

1. From the detector definition panel, press F4 (Criteria).

   The corresponding criteria panel appears.

2. Complete the fields on the criteria panel.

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

3. Press F3 (OK).

   The event criteria are saved.

Define an Alert

After you define the conditions that cause the alert, define the actual alert, for example, the type and severity. If you do not want to raise an alert, specify 0 for severity.

Follow these steps:

1. From the detector definition panel, press F5 (Alert).

   The Alert Definition panel appears.

   Note: For some detector types, this panel contains only the Description and Severity fields.

2. Complete the fields.

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

3. Press F3 (OK).

   The alert details are saved.

Define an Automatic Action

After you define the alert criteria and the alert, you can define an action (see page 17) that happens automatically when the event criteria is satisfied.

Follow these steps:

1. From the detector definition panel, press F6 (Actions).

   The Available Actions panel appears.

2. Select the action to use.

   An action-specific details panel appears.

3. Complete the action-specific details on the panel.

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

4. Press F3 (File).

   The selected action is added.

5. Press F3 (File).

   The details are saved.

IP Connection Events

You can set up event detectors to poll connection information at defined intervals and to create alerts according to the criteria that you define.

Use IP connection event detectors to detect long-running problems, such as connections that have been idle or in a wait state for a long time.

Note: IP connection detectors do not detect every connection in real time. They run a NETSTAT command at regular intervals and scan the output for connections that match your criteria. Because this uses a polling mechanism, connections may start and end between each polling interval; therefore, some connections are not found.

You can use combinations of any of the following as criteria for a connection detector to create an alert:

- A task name—as for the Taskname column on connection lists
- TCP status—as for the Status column on connection lists, except that connections with Listen status are not monitored
- Byte count—bytes in and bytes out on connection lists
- A full or generic local IP address or local port number—must match connection list values
- A full or generic remote IP address or remote port number—must match connection list values
- Idle or elapsed time threshold

Define an IP Connection Detector

To define an IP connection detector, you perform the steps to define an event detector and select CONNECT as the Alert Detector Type.

Note: Before you set up an event detector for connections, use the TCP/IP : Connections Menu to find the connection that you want to monitor, and note the values displayed in the various columns.

Example: Define an IP Connection Detector

This example shows how to define an event detector that drops FTP data connections that have been idle for more than 10 minutes.

To define the IP connection detector

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

   The Event Detectors Controls List appears.

2. Press F4 (Add).

   The CAS : Valid Value List appears.

3. Enter **S** next to CONNECT.

   The Connection Detector panel appears.

4. Complete the following fields:

   Short Description

   Briefly describes the event detector.

   Note: This description appears on the Event Detector Controls List. Use this in your own documentation.

   Status

   Specifies whether this rule detects events.

5. Press F4 (Criteria).

   The TCP/IP : Connection Criteria panel appears.

6. Complete the panel as follows:

```
PROD---------------------- TCP/IP : Connection Criteria -----------------------
Command ===>


Short Description  Drop FTP Data Connections                  Status ACTIVE

Task Name ........ FTPSRV
TCP Status .......
Bytes In+Out Over

Foreign Host .....
Foreign Port .....
Local Host .......
Local Port ....... 21
Idle Time Over ... 00:10            (hh:mm)


Note: Generic values may be used. Field values are as shown on connection list


 F1=Help      F2=Split     F3=OK
                           F9=Swap                                F12=Cancel
```

7. Press F3 (OK).

   The TCP/IP : Connection Detector panel appears.

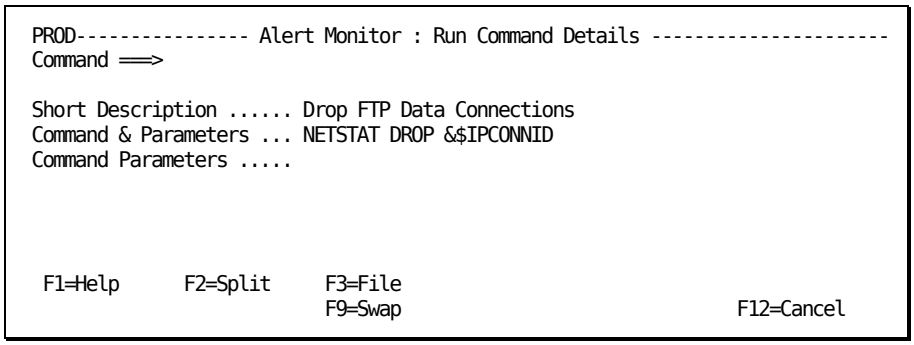
8. Press F6 (Actions).

   The Available Actions panel appears.

9. Enter **S** next to RUN_COMMAND.

   The Run Command Details panel appears.

10. Complete the panel as follows:



11. Press F3 (File).

    The Alert Automated Actions panel appears, with RUN-COMMAND added to the list of actions.

12. Press F3 (OK).

    The TCP/IP : Connection Detector panel appears.

13. Press F3 (File).

    The IP connection detector is saved.

Monitor FTP Failure Events

FTP failures detected by the FTP logging function can be declared as alerts. An FTP is considered to have failed if there is a response code of other than 0 or 250 in the FTP client or server event.

You can detect FTP failures that match the following conditions:

- A specific FTP command (Retr, Stor, Appe,Delete, Rename), or any command
- Remote IP address
- Data set name
- FTP server job name

Define an FTP Failure Detector

To define an FTP failure detector, you perform the steps to define an event detector and select FTPFAIL as the Alert Detector Type.

Example: Define an FTP Failure Detector

This example shows how to create an alert if the receipt of a production data set fails.

To define an FTP Failure detector

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

   The Event Detectors Controls List appears.

2. Press F4 (Add).

   The CAS : Valid Value List appears.

3. Enter **S** beside FTPFAIL

   The FTP Failure Detector panel appears.

4. Complete the following fields:

   Short Description

   Briefly describes the event detector.

   Note: This description appears on the Event Detector Controls List. Use this in your own documentation.

   Status

   Specifies whether this rule detects events.

5. Press F4 (Criteria).

   The FTP Failure Criteria panel appears.

6. Complete the panel as follows:

```
PROD------------------- TCP/IP : FTP Failure Criteria -------------------------
Command ===>

Short Description ..... FTP Failure                          Status ACTIVE

FTP Command ........... STOR          (*, Retr, Stor, Appe, Delete, Rename)

Remote IP Address .....

Dataset Name(Member) .. PROD.ERROR.LOG

Server Job Name .......


 F1=Help      F2=Split     F3=OK
                           F9=Swap                              F12=Cancel
```

7. Press F3 (OK).

   The FTP Failure Detector panel appears.

8. Press F5 (Alert).

   The Alert Definition panel appears.

9. Enter the severity of the alert that you want to create and press F3 (OK).

   The FTP Failure Detector panel appears.

10. Press F3 (File).

    The details are saved.

Monitor Console Messages

CA NetMaster NM for TCP/IP can detect z/OS console messages issued by a specific job name, generic job name, or the TCP/IP stack. You can specify extended message text matching, not only the message number.

You can update or replace alerts, as well as raising a new alert each time a message is received.

Note: For an example of how to clear an alert when a corresponding OK message is detected, see the SAMPLE: SYSVIEW... console detectors.

Define a Console Message Detector

To define a console message detector, you perform the steps to define an event detector and select CONSOLE as the Alert Detector Type.

Example: Define a Console Message Detector

This example shows how to create a severity 4 alert when message M123 PROCESSING COMMAND occurs for commands VARY and STATUS, for jobname TCPIP1.

To define a console message detector

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

   The Event Detectors Controls List appears.

2. Press F4 (Add).

   The CAS : Valid Value List appears.

3. Enter **S** beside CONSOLE.

   The Console Message Detector panel appears.

4. Complete the following fields:

   Short Description

   Briefly describes the event detector.

   Note: This description appears on the Event Detector Controls List. Use this in your own documentation.

5. Press F4 (Criteria).

   The Console Message Criteria panel appears.

6. Complete the panel as follows:

```
PROD---------------- TCP/IP : Console Message Criteria ----------------------
Command ===>

Short Description ..... PROCESSING COMMAND_____________       Status ACTIVE__

Console Message Details
Text... M123 PROCESSING COMMAND:_____________________________________________

Jobname TCPIP1__          (Enter * for TCPIP Started Task)

Extended Message Filtering

  Strt Word      Scan
  Pos  Num  Opr  Text
1 1__  4__  EQ_  VARY_____________________________________________________
2 15_  5__  EQ_  STATUS___________________________________________________
3 ___  ___  ___  _____________________________________________________
4 ___  ___  ___  _____________________________________________________
5 ___  ___  ___  _____________________________________________________

Expression ..... ____________________________________  e.g. 1 and (2 or 3)

 F1=Help      F2=Split     F3=OK
                           F9=Swap                              F12=Cancel
```

7. Press F3 (OK).

   The Console Message Detector panel appears.

8. Press F5 (Alert).

   The Alert Definition panel appears.

9. Enter **4** in the Severity field and press F3 (OK).

   The Console Message Detector panel appears.

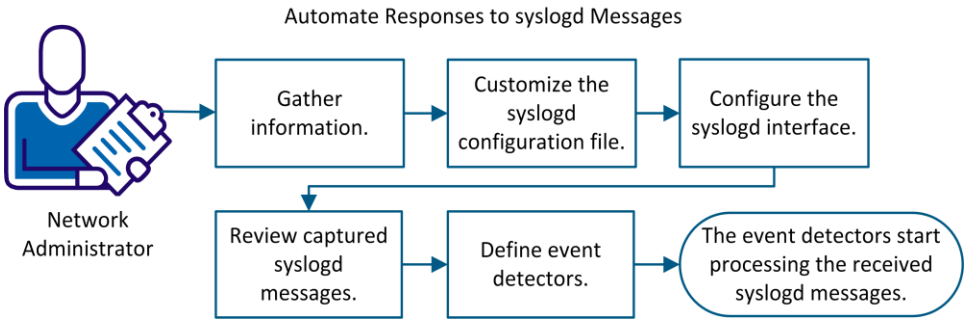
10. Press F3 (File).

    The console message detector is saved.

How You Automate Responses to syslogd Messages in UNIX System Services

As a network administrator, you want to automate responses to certain syslogd messages. Through the SYSLOGD parameter group, the region can become a destination for selected syslogd messages. You can then define event detectors to automate responses to these messages.

The following illustration provides an overview of the process:



The process has the following tasks:

1. Gather information (see page 32).
2. Customize the syslogd configuration file (see page 32).
3. Configure the syslogd interface (see page 33).
4. Review captured syslogd messages (see page 34).
5. Define event detectors (see page 34).

At the end of the process, the event detectors process your messages and respond according to your specification.

Gather Information

Before you start, determine the logging rules that select the messages that you want syslogd to pass to the region.

A facility name and a priority code define a logging rule. For locally generated messages, the rule can include the user ID and job name of the program that generated the message. For messages arriving over the network, the rule can include the IP address or host name of the sender. The logging rule forms part of a syslogd rule configuration statement.

This rule configuration statement has the following format:

`[(host).|user_id.job_name.]facility.priority pipe_path_name`

pipe_path_name

Specifies the destination to which syslogd passes the messages. The region uses a UNIX System Services (USS) named pipe (or first-in-first-out (FIFO) special file) for this purpose. You can use the region default or can use your own pipe. The parameter specifies the absolute path name of the pipe.

Default: /etc/nmtcpip.*region_acb_name*.syslogd.pipe (*region_acb_name* is the name of the primary ACB for the region.)

Note: For information about syslogd rule configuration statements, see IBM *z/OS Communications Server IP Configuration Reference*.

Example: Pass Internet Key Exchange (IKE) Daemon Messages

This example tells syslogd to pass IKE daemon messages with a priority of notice or higher to the REGION01 region:

```
local4.notice /etc/nmtcpip.REGION01.syslogd.pipe
```

Customize the syslogd Configuration File

The syslogd configuration file specifies the messages to pass to a particular destination. To pass the required messages to the region, customize the file using the rule configuration statements that you determine in the previous task.

Configure the syslogd Interface

The SYSLOGD parameter group configures the region as a destination for selected messages from the local syslogd. syslogd passes selected messages to the region using a USS named pipe (or FIFO special file).

Follow these steps:

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

   The list of parameter groups appears.

2. Find the SYSLOGD parameter group, and enter **U** next to it.

3. Specify the field values:

   a. In the Enable SYSLOGD Interface field, specify **YES**.

   b. In the Log Messages field, specify **YES** to write the messages to the activity log.

      Note: The logged messages help you define your event detectors.

   c. In the Named Pipe field, specify the absolute path name of the pipe that you specify in the syslogd configuration file.

4. Press F6 (Action).

   The region creates the named pipe, starts a pipe receiver, and *reinitializes* syslogd. The region starts to receive the selected syslogd messages.

5. Press F3 (File).

   You save the parameter group. At a region startup, the saved group tells the region to start the pipe receiver and *reinitialize* syslogd.

Review Captured syslogd Messages

The SYSLOGD parameter group enables the logging of captured syslogd messages in the region. The RMSL0105 identifies the captured messages. After you action the parameter group for the first time, wait for the region to capture the messages. Review these messages to determine which ones you want to detect.

Follow these steps:

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

   The region activity log appears.

2. Use the **F RMSL0105** command to find an instance of the message. Enter **FILTER RMSL0105** to display only the RMSL0105 messages.

   Note: For information about the message syntax, place the cursor on a message and press F1 (Help).

3. Review the messages, and note the ones that you want to detect.

   You create a list of messages for which you want to define event detectors.

Define Event Detectors

You want to automate responses to the syslogd messages that the region receives. The SYSLOGD event detectors enable you to detect specific messages, raise alerts, and perform actions.

Follow these steps:

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

   The Event Detector Controls List panel appears.

2. Press F4 (Add), and enter **S** next to the SYSLOGD event detector type.

   A panel appears for you to define the detector.

   Note: For information about the panels and fields, press F1 (help).

3. Describe the detector, and set the status to ACTIVE.

   Note: You can also activate or inactivate a detector from the Event Detector Controls List panel.

4. Specify the criteria for the message you want to detect:

   a. Press F4 (Criteria).

   b. Specify the criteria, and press F3 (OK).

      The Event Detector Controls List panel appears with the criteria information.

   The detector triggers on messages that satisfy the specified criteria.

5. Define the alert that you want to raise:

   a. Press F5 (Alert).

   b. Define the alert, and press F3 (OK).

      The Event Detector Controls List panel appears with the alert information.

   When the detector is triggered, it raises the defined alert.

6. (Optional) Specify the actions that you want to perform:

   a. Press F6 (Actions).

   b. Select the type of action.

   c. Specify the action, and press F3 (File).

      The Alert Automated Actions panel appears.

   d. If you want to specify more actions, press F4 (Add). Repeat Step b and Step c.

      If you have finished specifying your actions, press F3 (OK). The Event Detector Controls List panel appears with the action information.

   When the detector is triggered, it performs the specified actions.

7. Press F3 (File).

   You save the detector. The detector is active and starts processing received syslogd messages.

Example: Detect EZD1125I Messages

This example shows the criteria to detect an EZD1125I message. You review the region activity log and note the following message that has IKE as the source:

```
22.12.25 RMSL0105 276.1 Aug  7 02:12:25 USILCO31 IKE: EZD1125I SERVAUTH check for user
JOHNDOE  and profile EZB.NETMGMT.CO31.TCPIP.IPSEC.DISPLAY failed during an NMI
request
```

The message indicates that a user attempted to issue a Network Management Interface (NMI) request but was refused. The user does not have READ access to the security resource required to display IPSec information. You want to define an event detector to alert you on such events. The following panel shows the criteria to detect such messages:

```
Short Description ..... EZD1125I_____________________       Status ACTIVE__

USS Syslog Daemon Message Details
Text... EZD1125I_____________________________________________________________

Source  IKE_____

Extended Message Filtering

  Strt Word      Scan
  Pos  Num  Opr  Text
1 ___  9__  EQ_  EZB.NETMGMT.*.TCPIP.IPSEC.DISPLAY_____________________________
2 ___  ___  ___  _____________________________________________________________
```

Example: Detect a Message That Does Not Begin With a Message ID

This example shows the criteria to detect an EZD0917I message that follows a qualifying text string:

```
11.57.07 RMSL0105 4177.1 Dec  6 16:57:07 BADEVL IKE: Message instance 384: EZD0917I
Could not find applicable KeyExchangeRule - LocalIp : 192.168.21.1 RemoteIp :
192.168.21.5 LocalID :  Any RemoteID : ID_DER_ASN1_DN
CN=dept001.comp001.com,OU=Mainframe,O=COMP001 Data
```

The following panel shows the criteria to detect such a message:

```
Short Description ..... EZD0917I_____________________       Status ACTIVE__

USS Syslog Daemon Message Details
Text... Message instance_____________________________________________________

Source  IKE_____

Extended Message Filtering

  Strt Word      Scan
  Pos  Num  Opr  Text
1 ___  4__  EQ_  EZD0917I_____________________________________________________
2 ___  ___  ___  _____________________________________________________________
```

Configure Connection Event History Recording

CA NetMaster NM for TCP/IP stores and records details of all IP, FTP, and Telnet connections in the IPLOG database for the last seven days. This data is useful for problem determination and planning. It can also be useful for audit and security purposes.

Important! To record connection events, you must ensure that your server is set up to generate SMF records. For more information, see the *Installation Guide*.

To configure connection event history recording to suit your requirements, you must do the following:

1. Define the connection event history data set details (see page 38).
2. Define the stack event processing options (see page 39).

Define the Connection Event History Data Set

This procedure defines the data set where the connection events are stored, how long they are retained, and the time of day that expired events are deleted.

Note: Connection events from a busy network can occur in large numbers and at high rates. This results in high VSAM activity and high file record and space requirements. IPLOG does reorganize itself using the IPLOGSEQ data set. However, if you have a large or busy network, we recommend that you review the space and extent allocations of IPLOG and IPLOGSEQ.

To define the connection event history data set

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

   The Customizer : Parameter Groups panel appears.

2. Enter **U** beside the IPFILES parameter group in the FILES category.

   The IPFILES - TCP/IP File Specifications panel appears.

3. Complete the following fields:

   IPLOG Event History Dataset

   Defines the database to which the events are logged.

   Keep IPLOG data for

   Specifies the number of days to retain the events in the IPLOG database.

   Range: 0-7 days

   Delete expired IPLOG data at

   Specifies the time of day when the IPLOG data that is older than the specified retention period is deleted.

   IPLOGSEQ Reorg Dataset

   Defines the sequential data set used by the IPLOG reorganization process.

4. Press F6 (Action).

   The details are applied (but not saved).

5. Press F3 (File).

   The details are saved.

Define Stack Event Processing

This procedure defines the type of events to log in the activity log and the type of events to save in the IPLOG database.

Note: If you do not intend to look for these events on the activity log or in the event history, do not perform this procedure because it can consume CPU resources.

To define stack event processing

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

   The Customizer : Parameter Groups panel appears.

2. Enter **U** beside the IPEVENT parameter group in the MONITORS category.

3. Specify YES for each type of event that you want to log or save, or both.

4. Press F6 (Action).

   The details are applied (but not saved).

5. Press F3 (File).

   The details are saved.

Chapter 4: Configuring Application Workload Monitoring

This section contains the following topics:

Activate Stack Connection Workload Monitoring

CA NetMaster NM for TCP/IP connection workload monitoring and its ConBytes, ConConnects, and ConActive attributes are used to monitor all IP, FTP, and Telnet application workload. The business application names that you add are used to qualify the attributes.

To activate stack connection workload monitoring

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

   The IP resource monitor appears.

2. Enter **UM** next to the stack for which you want to activate monitoring.

   The ResourceView: Stack Monitoring Definition panel appears.

3. Enter **U** next to Connection Workload Monitoring.

   The Monitoring Definition panel appears.

4. Press F4 (Add).

   The Selectable Attributes List appears.

   Note: Only attributes not selected already appear in the Selectable Attributes List.

5. Ensure that the following attributes are selected. To select the attribute, type **S** next to it.

   ConActive

   Specifies the total number of active connections when connection workload was last sampled, by application for this stack.

   ConBytes

   Specifies the bytes transferred during the last sample period (expressed as an hourly rate), by application for this stack.

   ConConnects

   Specifies the number of connections during the last sample period (expressed as an hourly rate), by application for this stack.

   ConTotalActive

   Specifies the total number of active connections for this stack when connection workload was last sampled.

   ConTotalBytes

   Specifies the total number of bytes transferred during the last sample period for all connections for this stack.

   ConTotalConnects

   Specifies the total number of connections started during the last sample period for this stack.

   Press Enter.

   The attributes are added to the Monitoring Definition panel.

   Note: If you want to break down the total connections by remote network or stack home address, add the Con*ByNet and Con*ByIf attributes.

6. Press F3 (OK).

   The ResourceView: Stack Monitoring Definition panel appears.

7. Complete the following fields:

   Monitor Rate

   Defines how often this monitoring is performed (in minutes).

   Send to ReportCenter

   Specifies whether to send an hourly summary of data to ReportCenter for this type of monitoring.

8. Press F3 (File).

   The details are saved.

Business Application Names

You can group IP connections and define them with a *business application name*. The Packet Analyzer detects and examines all IP connections for each monitored stack, and groups them into your business application name.

Multiple groupings can be defined with the same business application name. The definitions are sequenced as a set of rules. The first rule that satisfies the connection criteria determines the name to which the connection belongs.

If you set up CA NetMaster NM for TCP/IP to monitor IP, FTP, and Telnet application workload, the monitoring attributes are qualified by the business application names that you add.

The business application name is then used to describe the IP connections on the following:

- Graphical reporting tools such as ReportCenter
- Connection lists
- Connection workload monitoring displays
- Performance history and workload monitoring displays

By grouping your connections and workload data in this way, you can produce more meaningful reports. You can also raise an alert for a business application name.

Note: Connection events are recorded in the event history data set (IPLOG) or written to the activity log, as specified in the IPEVENT Customizer parameter group. For more information, see the *Administration Guide*.

Important! To record connection events and group them into business application names, you must ensure that your server is set up to generate SMF records. For more information, see the *Installation Guide*.

Analyze Business Application Names

If you choose to create business application names automatically when you run Express Setup, a business application name is created for discovered address spaces. The name allocated is the address space name, and the ports are those ports that are active when it is discovered. However, if you set up your business application names manually, you can define more meaningful names. Only you know who uses the applications, how they are used, and which ones are the most relevant to your business.

Before you define a business application name, you should analyze your environment and decide what you want to monitor. Business application names let you measure more than merely the traffic to one port/protocol or address space. The following examples give you some ideas of what you can define.

Example 1: Break Workload Down by Location and Department

You want to break down the Telnet workload at a location or departmental level. You define the following rules:

- Local port 23 and remote IP address 10.20.30.1 to 10.20.30.199 as application TN-Factory
- Local port 23 and remote IP address 10.20.30.200 to 10.20.30.229 as application TN-Admin
- Local port 23 and remote IP address 10.20.30.230 to 10.20.30.255 as application TN-IT
- Local port 1023 as application TN-IT

With these rules, you separate the Telnet workload for your factory, administration, and IT groups.

Example 2: Show Port Use by Application

You want to see what applications use what ports. You define the following rules:

- Local port 1414 as application WebSphereMQ
- Local ports 8080-8443 as application Tomcat
- Task name ACCTS and port 12300 as application AcctsUpd
- Task name ACCTS and port 12301 as application AcctsAdm

Example 3: Show Remote Addresses or Ports by Location

You want to display remote addresses and ports by office location. You define the following rules:

- Remote address X and port 24 as PerthOffice
- Remote address V and port 26 as SydneyOffice

Business Application Names and Address Spaces

Business application names can specify an address space name, port, and stack in their criteria; however, you can name them independently of any address space.

Business application name setup is not bound by address spaces. A business application name does not need any knowledge of the address spaces used by a connection. For example, a business application name can be defined as the following:

- A subset of connections to one address space
- All connections to a single address space
- All connections to multiple address spaces
- A subset of the connections to multiple address spaces

Define a Business Application Name

To make the most of the monitoring capabilities and to produce valuable reports, it is important that you define some business application names for your environment.

To define a business application name

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

   The Business Applications menu appears.

2. Select option A - List and Define Business Applications.

   The Application Name Definition List appears.

3. Press F4 (Add).

   The Application Name Definition panel appears.

4. Complete the following fields:

   Order

   Specifies the order in which the definition is processed.

   Note: A connection can pass the criteria of many different names. To control this, specify the order in which the definition is processed. Define the most specific applications early in the order.

   Range: 0 through 32767

   Default: 32767

   Application Name Base

   Specifies the base name given to the application. The value in the Generate Name field is appended to this base.

   Note: Use caution when specifying a Generate Name of JOBNAME, REMOTEADDR, or REMOTEPORT because these values can result in many application entries, which cause high CPU.

5. Complete the Connection Match Criteria.

   Note: Press F1 (Help) for information about the fields.

6. Complete the Processing Options.

   Note: Press F1 (Help) for information about the fields.

7. Press F3 (File)

   The business application name is saved and added to the definition list.

Define Alert Conditions for Application Workload

Connection workload monitoring provides byte throughput, connection rates, and concurrent active connections. For non-critical applications, connection monitoring is often performed to get trend data; however, you can set alert conditions on these criteria.

Note: For all numeric counter and total attributes, alert conditions are checked after each individual sample, based on its equivalent hourly rate. If the rate would exceed the alert condition, the alert is raised immediately without waiting for the hour to pass.

To set alert criteria on a business application name

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

   The IP resource monitor appears.

2. Enter **UM** beside the stack for which you want to update monitoring.

   The ResourceView: Stack Monitoring Definition panel appears.

3. Enter **U** beside Connection Workload Monitoring.

   The Monitoring Definition panel appears.

4. Type **S** beside the ConBytes or ConConnects attribute and press Enter.

   The Alert Control Details panel appears.

5. Enter the name of the business application name for which you want to define alert conditions in the Qualifier field.

6. Define the alert conditions.

7. Press F3 (OK).

   The alert conditions are saved.

Telnet and FTP Workload

A STACK resource's FTP workload monitoring and Telnet workload monitoring are based on connection completed SMF events. CA NetMaster NM for TCP/IP is notified when the FTP transfer or Telnet connection ends, then records the entire byte count of the transmission in the ending interval.

Compared to real-time figures, the accuracy of the SMF end-based traffic figures depends on the length of the transfers and connections. Generally, we recommend that you monitor FTP and Telnet traffic using connection workload monitoring because it provides superior real-time FTP and Telnet workload data.

To see FTP and Telnet byte and transfer counts in real time, in the intervals in which they occur, use connection workload monitoring. Set up suitable FTP and Telnet business application names.

Use FTP workload monitoring to monitor FTP failure rates or to gain performance data for individual FTP users. You can also use FTP workload monitoring if you use ReportCenter because of its long time frames and reporting intervals.

Define FTP-related Business Application Names

Default business application name definitions, or those created by Express Setup, tend to group all FTP connections together and call them FTP. When you define business application names for FTP transfers, use more granular names, for example:

- Name groups of FTP transfers according to server or location
- Name groups of FTP transfers according to who is at the receiving end of the transfer

You can set separate performance alerting criteria for each different name. One group of FTP transfers would have much stricter controls than others.

Define Telnet-related Business Application Names

Default business application name definitions, or those created by Express Setup, tend to group Telnet connections together and call them Telnet.

When you define business application names for Telnet connections, use more meaningful names, for example:

- Telnet application
- Logical function or geographical location of the users
- Type or location of the Telnet servers
- Security requirements of connections

Activate FTP Stack Failure Rate Monitoring

To raise an alert when large numbers of FTP transfers fail in an interval, you can monitor FTP failure rates.

To activate FTP stack failure rate monitoring

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

   The IP resource monitor appears.

2. Enter **UM** beside the stack for which you want to activate monitoring.

   The ResourceView: Stack Monitoring Definition panel appears.

3. Enter **U** beside FTP Workload Monitoring.

   The Monitoring Definition panel appears.

4. Press F4 (Add).

   The Selectable Attributes List appears.

5. Add and remove attributes until only the following appear:

   FTPFailures

   Specifies the number of FTP failures by user ID.

   FTPFailuresByNet

   Specifies the number of FTP failures by network.

   FTPTotalFailures

   Specifies the number of FTP failures for this host.

6. Press F3 (OK).

   The details are saved.

Chapter 5: Configuring IP Resource Monitoring

This section contains the following topics:

IP Resources

CA NetMaster NM for TCP/IP supports the following IP resources:

- z/OS IP Stacks
- Open Systems Adapters (OSAs)
- Address Spaces
- Enterprise Extender (EE)
- APPN/HPR
- Virtual IP Addresses (VIPAs)
- Cisco Channel Cards
- Communications Storage Manager (CSM)

You can view your IP resources from the IP resource monitor. The IP resource monitor regularly checks the IP resources, samples and stores performance data, and raises alerts when they violate performance triggers. You can perform diagnostic functions from the IP resource monitor or through a network diagnosis menu.

Unlike IP nodes, IP resources are defined individually, not as members of groups.

Display IP Resources

When you set up a region for the first time, Express Setup automatically discovers the important IP resources that are present and active at the time.

To display all IP resources, enter **/IPMON** from the command prompt.

Note: After initial setup, resources are not updated automatically.

Delete an IP Resource

Express Setup usually finds a lot of IP resources; however, it may find IP resources that you do not want to monitor. You should review all of the IP resources discovered and delete the ones that you do not want to monitor.

Important! Do not monitor large numbers of non-critical resources unnecessarily because this increases CPU usage and increases the number of alerts raised.

To delete an IP resource

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

   The IP resource monitor appears.

2. Enter **DEL** beside the IP resource that you want to delete, and then press Enter.

   The IP resource is deleted.

IP Resource Definitions

The IP resource definition is attached to the system image and monitoring is activated when the system image is loaded.

Note: A system image is a collection of resources. System images have unique names, generally the system ID and a version number, for example, SYS1-0001. Only one system image is loaded by a CA NetMaster NM for TCP/IP region at one time. For more information about system images, see the *Administration Guide*.

IP resource definitions are qualified by the following:

- The system image name and version
- The resource name and class

The IP resource classes are as follows:

APPN/HPR

Defines APPN/HPR.

ASMON

Defines an Address Space Monitor.

Note: You can define an external Telnet server using this option.

CIP

Defines a Cisco Channel card.

CSM

Defines a Communication Storage Manager.

EE

Defines an Enterprise Extender.

OSA

Defines an Open Systems Adapter.

ROUTER

Defines an IBM 2216 Routers.

STACK

Defines a TCP/IP Stack.

VIPA

Defines a Virtual IP Address.

Note: If you set the field Create VIPA Resources to YES when you create a STACK resource, a VIPA resource is created automatically for each active dynamic VIPA when the system image is loaded. To define the way in which the VIPA resource is created, you can apply a VIPA resource template. The VIPA resource is built from a template. To change the way in which the VIPA resource is created, you can modify the default VIPA resource template, or create a new one. For more information about resource templates, see the *Administration Guide*.

How to Add an IP Resource

If Express Setup does not define all of your resources, you must add them manually.

To define your IP resources, you must complete the following panels:

General Description

Defines the IP resource to your region and determines if monitoring is active.

Monitoring Definition

Determines which attributes are monitored as well as the frequency and level of monitoring. Monitoring attributes let you test the performance of a resource against a value or a calculated baseline to trigger alerts and actions.

You can define automation rules using the following panels:

Status Monitor Message Details

Defines an action when a specific system console message occurs.

Automation Log Details

Controls the resource transient log.

Owner Details

Describes the owner of the resource.

Note: For this initial implementation, we recommend that you use the default settings. When you are more familiar with CA NetMaster NM for TCP/IP, you can use these panels to define more advanced automation.

When you define a resource, a template is applied based on the type of resource that you select. You can modify the settings to suit your requirements or accept the defaults. You can also edit the template.

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

Add an IP Resource

The general procedures for defining different classes of IP resources are similar. This procedure shows you how to add a resource from the Resource Definition list. You can also add a resource from the IP Resource Monitor using the F4 (Add) function key.

To add an IP resource

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

   The Resource Definition panel appears.

2. Enter **S** next to the resource class that you want to add.

   The *resource* list appears.

3. Press F4 (Add).

   The General Description panel appears.

4. Complete the fields:

   a. Identify the resource. For example, specify the job name of an address space in the Address Space Monitor Name field of an ASMON resource.

   b. Enter **L** in the action field in the Template Selection box.

      The templates available for the resource class are listed.

   c. Enter **M** next to the template you want to apply.

      The definition is populated with values from the template, and the panel is refreshed with any incomplete mandatory fields highlighted.

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

   d. Complete the highlighted fields.

5. Press F8 (Forward).

   The Monitoring Definition panel appears with the default attributes listed.

6. Ensure that all the attributes that you want to monitor are listed. To edit the list, press F10 (EditLst).

7. Review the following fields, and update the values if necessary:

   Monitor Rate

   Specifies how often to perform this monitoring.

   Range: 5 through 60 minutes

   Send to ReportCenter

   Specifies whether to send an hourly summary of data to ReportCenter.

8. Press F3 (File).

   The resource is added.

Performance Alerts

You can configure the CA NetMaster NM for TCP/IP region to raise alerts on any performance attribute samples when certain criteria are met. The alert is then displayed on the alert monitor.

Alerts can be raised on a performance attribute when the following occurs:

- A sample value is above or below an absolute threshold value, for example, PINGRTT for IP host SERVER01 exceeds 2000ms
- A sample value differs from a moving average by more or less than a specified percentage, for example, ConBytes for IP application APPL01 is more than 80% above what it usually is for this hour of this day
- An enumerated value is or is not a specified character value, for example, NETSTATUS=SNMPERROR

Performance data attributes generally fall into the following categories:

Availability, Stability, and Reliability

Specifies whether the resource is active, reachable, and responsive.

Throughput

Specifies how many bytes, packets, datagrams, segments went through, in an interval.

Errors

Specifies how many errors occurred in an interval.

Response Time

Specifies the actual response time. Possibly the lowest, highest, average, in an interval.

Workload

Specifies how much work an application user did in an interval.

Capacity and Utilization

Specifies how much of its internal resources a device is using.

Resource Usage

Specifies how much of the external system resources a device is using.

Configuration

Specifies device and environmental configuration.

Define a Performance Alert

You can define a performance alert after you have defined performance monitoring. The process is the same for stack resources and other IP resources; however, the procedure to access the Monitoring Definition list differs.

To define a performance alert

1. From the Monitoring Definition list, enter **U** beside the attribute for which you want to raise an alert.

   The Alert Control Details panel appears.

2. Enter **U** beside the type of alert that you want to raise.

   The Alert Details panel appears.

3. Enter the details of the alert and then press F3 (OK).

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

4. Press F3 (OK).

   The details are saved.

Example: Define a Performance Alert

This example shows how to raise a severity 3 alert when the total number of FTP failures on STACK01 exceeds 100 per hour. You want the text on the alert monitor to say, *Excessive FTP Failures*.

To define the alert

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

   The IP resource monitor appears.

2. Enter **UM** beside the stack for which you want to define monitoring.

   The Monitoring Definition panel appears.

3. Enter **U** beside FTP Workload Monitoring.

   The Monitoring Definition List appears.

4. Press F4 (Add).

   The Selectable Attributes List appears.

5. Enter **S** beside FTPTotalFailures.

   The Monitoring Definition List appears.

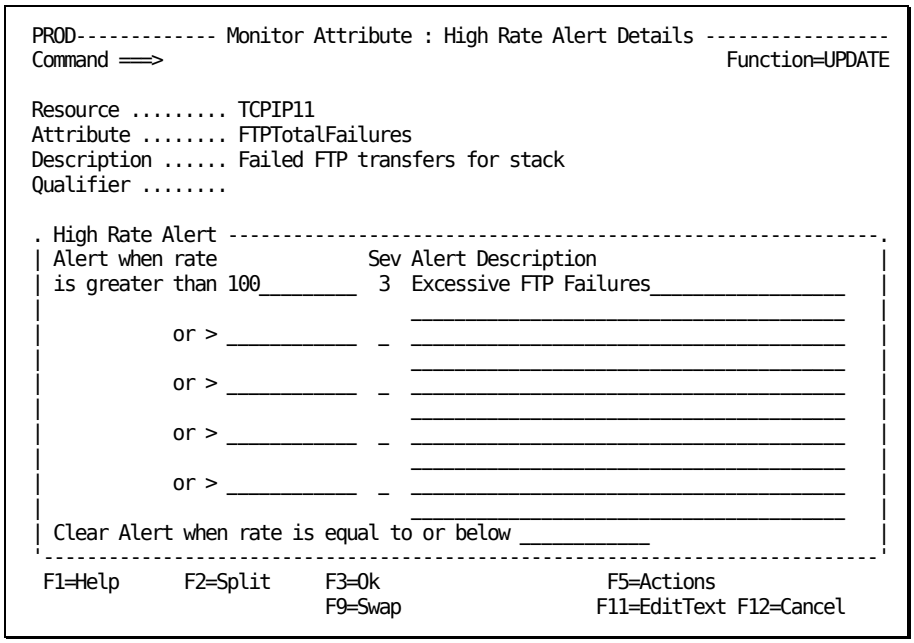
6. Enter **U** beside FTPTotalFailures.

   The Alert Control Details panel appears.

7. Enter **U** beside High Rate Alert.

   The High Rate Alert Details panel appears.

8. Enter the alert details as follows:



9. Press F3 (OK).

   The alert details are saved.

Monitoring Maps

The information in a resource definition determines how the resource is monitored. The definition can include a monitoring map, which schedules changes to the default monitoring. Timers activate these changes.

You can use monitoring maps to do the following:

- Automatically change the monitoring status of a resource
- Raise alerts at set times only, for example, during peak processing

Each system image has its own set of monitoring maps. You define a monitoring map, for example, MAP1 and attach as many resources to the map as required. Because monitoring maps are not limited to a seven-day cycle, you can define changes to the monitoring requirements that apply daily, on the same day every week, on the same date every month, for a specific date and time, and so on. You can also suppress changes temporarily and update timer information at any time.

A monitoring map has two parts—a map definition and a timer definition. The map definition contains information about the monitoring activity. The timer definition contains information about when to change the monitoring activity of the resources that use the map. The timer definition can contain information about when to change the status of alerts and when to start processes to perform special tasks.

The following rules apply to monitoring maps:

- If the timer definition is blank, default monitoring requirements apply to all resources attached to that map.
- A map applies only to the system image for which it is defined.
- Map names must be unique in the image to which the map applies.

Define a Monitoring Map

You can define as many maps for a system image as you want. When the map is defined, you can attach resources to the map.

To define a monitoring map

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

   The Resource Administration panel appears.

2. Type **M**, and the name and version of the system image that owns the maps you want to create or access, and then press Enter.

   The Monitoring Map List appears. This panel lists the monitoring maps for the specified system image.

3. Press F4(Add).

   The Monitoring Map panel appears.

4. Complete the following fields:

   Name

   Defines the name of the monitoring map.

   Description

   Describes the monitoring map.

5. Specify the timer information (see page 61).

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

6. Press F3 (File).

   The details are saved.

Timer Definitions

You can define the following types of timer information:

For all Resources

Defines the timer, leaving the Resource Name field blank. This timer information applies to any resources attached to the map.

For a Specific Resource

Defines the timer with the name of the resource in the Resource Name field. This timer information applies to the named resource if the resource is attached to the map.

You can use the action codes to repeat or delete rows of information, or to insert blank lines.

You can use the following values in the Day field to simplify data entry:

*****

Repeats the timer for all days (that is, Monday through Sunday).

W/D

Repeats the timer for weekdays (that is, Monday through Friday).

W/E

Repeats the timer for weekends (that is, Saturday and Sunday).

Example: Define a Monitoring Map

In this example, you define a map named MAP02. You want to stop monitoring all resources and the raising of alerts on 20 October 2007 at 0830 hours. You want to reactivate all services at 1600 hours on the same day.

To define the monitoring map

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

   The Resource Administration panel appears.

2. Type **M**, and the name and version of the system image that owns the maps you want to create or access, and then press Enter.

   The Monitoring Map List appears. This panel lists the monitoring maps for the specified system image.

3. Press F4(Add).

   The Monitoring Map panel appears.

4. Complete the details as follows:

```
PROD--------------- Automation Services : Monitoring Map ----------Function=ADD
Command ===>                                                 Scroll ===> CSR

Å Monitoring Map
… System Name .. SYS1                        Last Updated By
… Version ...... 0001                        at           on
… Name ......... MAP02
… Description .. RESOURCE MAP 02                    Expire Delete ... NO
… Attached Resources ...

Å Timer Details
…                                                  D=Delete I=Insert R=Repeat
…     Day Date        Time     Resource Name       Mon.Activity Alerts Status
…     SAT 20-OCT-2007 08.30.00                     INACTIVE     N      ON
…     SAT 20-OCT-2007 16.00.00                     ACTIVE       Y      ON



…     **END**


…  F1=Help     F2=Split    F3=File     F4=Save     F5=NextTmr  F6=Sort
…  F7=Backward F8=Forward  F9=Swap               F11=Right   F12=Cancel
```

Attach a Resource Definition

After you have defined your resources and a map, you can attach resource definitions to the map.

Note: If your maps are already defined, you can perform this task when you are adding a resource.

To attach a resource definition

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

   The Monitoring Map List appears.

2. Enter **AR** next to the monitoring map to which you want to add a resource.

   The Attach Resources panel appears.

3. Enter **S** next to the resource that you want to add to the monitoring map.

   The Attach Resources Results panel appears, which tells you if the operation was successful.

4. Press F3 (File).

   The details are saved.

Chapter 6: Configuring the Alert Monitor

This section contains the following topics:

Alerts

An alert is a notification of a fault. Alerts can come from multiple LPARs, different CA NetMaster products, and external products. The alert monitor provides a consolidated, dynamic display of alerts. From the alert monitor, you can close and update alerts, and obtain details about affected resources.

When you implement your product, you must decide how you want to be notified of an alert. You can do the following:

- Watch the alert monitor and manually administer the alert, for example, close the alert, change the severity, raise a trouble ticket.
- Watch the IP node monitor and IP resource monitor and when you see that a node or a resource has an alert, use the **AL** line command to display it.
- Send an alert to an external product.
- Send alert details to an email address, to an NCL procedure, a TSO or CA NetMaster broadcast message, or to a WTO.

Alert Sources

Alerts can come from the following sources:

IP Node Monitor and IP Resource Monitor

Raises alerts based on the performance of specified attributes of IP resources. The alerts can be:

- Enumerated attributes equal to a specific value
- Numeric attributes above or below a specified constant threshold
- Numeric attributes differing from a baseline by more than a specified percentage

IP Event Detectors

Raises alerts based on an event, for example, a particular port listener becomes active or an FTP transfer matching specified criteria fails.

User-written NCL Procedures

Raises alerts defined by user-written NCL procedures, using supplied NCL API calls.

CA NetMaster Internals

Raises alerts concerning the conditions that affect the operation of the CA NetMaster NM for TCP/IP region, for example, VSAM errors on critical files.

CA OPS/MVS

Raises alerts specific to CA OPS/MVS.

Define Alert Filters

You can filter the alerts displayed on the alert monitor by applying a set of criteria to each of the fields in the alert. The filters that you create can be named and stored for later use. By defining an alert filter, you can restrict the alerts sent to a particular destination and restrict the number of alerts displayed on the alert monitor.

When you define alert filters, consider where you want to send the resulting alerts. Also, consider which of your alerts belong together and should be sent to the same destination. You may want to send every alert to the same destination. Alternatively, you can send them to different destinations. For example, you can send an IP alert to email address A, write a WTO about certain FTP failures, or pass details of IP connections to NCL procedure N.

To define alert filters

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

   The Alert Monitor : Filter Definition List panel appears.

2. Press F4 (Add).

   The Alert Filter panel appears.

3. Complete the following fields:

   Name

   Specifies the name of the filter.

   Description

   Describes the filter.

   Filter Expression

   Specifies the Boolean expression that determines what alerts to pass.

   Note: For more information about creating Boolean expressions, press F1 (Help).

4. Press F3 (File).

   The alert monitor filter is saved.

Alert Monitor Display Format

The alert monitor display format determines the information displayed for the alerts on the alert monitor, for example, the columns and the order in which they appear.

For each type of information you want to display on the alert monitor, you need to specify the following:

- A static heading
- A variable that contains the required information

You can create a multiscreen alert monitor display with up to 10 screens, which lets you display more information on the monitor. To access the screens, press F11 (Right) or F10 (Left).

The variable contains the information you want to display. The name of a variable can sometimes be longer than the data to display. You can enter a shorter name and then make that shorter name an alias of the actual name.

Create the Alert Monitor Display Format

The alert monitor display format determines the information displayed for the alerts on the alert monitor.

To create the alert monitor display format

1. Enter **/ALADMIN.L** at the prompt.

   The List Definition List appears.

2. Enter **C** beside the DEFAULT display format definition.

   A copy of the List Description panel appears.

3. Enter a new value in the List Name field to identify the new definition, and update the Description and Title fields.

   Press F8 (Forward) three times.

   The List Format panel appears.

4. Enter column headings and variables using the text editor to specify the information to display on the alert monitor.

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

5. (Optional) Press F5 (Fields) to create aliases.

6. Press F3 (File).

   The details are saved.

Alert Monitor Trouble Ticket Interface

The alert monitor provides an interface that lets you send alert information in the form of a trouble ticket to another interface automatically or manually.

The alert monitor supports the following interfaces for raising trouble tickets:

Electronic Mail

Sends an email describing the problem to a problem management application or a particular person. This method can be used to send tickets to multiple problem management applications.

Custom

Lets you write your own NCL procedure to deliver the trouble ticket to an application by whatever means you choose. For example, you can do the following:

- Invoke a REXX procedure and pass alert variables.
- Send to any external interface, for example, problem management product.
- Send to z/OS system facilities, for example, system console, data sets, SMF user records, batch jobs.
- Invoke applications, for example, FTP.

Service Desk

Creates a new CA Service Desk request from the alert details.

Note: If your CA Service Desk installation is configured with the optional ITIL application, incidents are created instead of requests.

Note: You can choose one interface only.

If you want the operator to supply information when creating a ticket, you also need to set up the trouble ticket data entry definition.

Define an Email Trouble Ticket Interface

This option sends an email describing the problem to a problem management application or a particular person.

Note: To enable this option, you must ensure that your z/OS Systems Programmer enables SMTP support on this region's TCP/IP stack.

To define an email trouble ticket interface

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

   The Alert Monitor : Trouble Ticket Interface Definition panel appears.

2. Enter **EMAIL** in the Interface Type field and press F6 (Action).

   The Email a Trouble Ticket panel appears.

3. Complete the following fields:

   Mail Address

   Specifies the email address of the trouble ticket system to which you want to send the message.

   Note: The &$USRNAME variable works with the default trouble ticket data entry definition (see page 73). If you do not want operators to change the address, specify an address in this field and delete the fields in the data entry definition.

   Host Name

   Specifies the host name of this system. This value is usually the NJE node name.

   Note: Applies to IBM's Communications server only.

   SMTP Node Name

   Specifies the NJE node name on which the SMTP server runs. This name usually has the same value as the Host Name.

   Note: Applies to IBM's Communications server only.

   SMTP Job Name

   Specifies the name of the address space in which SMTP runs. This name is usually SMTP.

   Note: Applies to IBM's Communications server only.

   SMTP DEST Id

   Specifies the destination ID in the REMOTE (...) parameter of the SMTP statement in member APPCFG*xx* of the PARM data set.

   Note: Applies to CA TCPaccess CS only.

   Exit Procedure Name

   Specifies the name of an NCL exit routine, in which you can customize the email message sent by this trouble ticket. Enables you to send a trouble ticket to multiple email addresses. (see page 75)

   Subject

   Specifies the heading to display as the subject of the email message.

   Enter Mail Text Below

   Specifies the mail message text. Press F1 (Help) for information about variables.

   Press F3 (File).

   The definition is saved.

Define a Custom Trouble Ticket Interface

This option lets you write your own NCL procedure to deliver the trouble ticket to an application by whatever means you choose.

To define a custom trouble ticket interface

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

   The Alert Monitor : Trouble Ticket Interface Definition panel appears.

2. Enter **CUSTOM** in the Interface Type field and press F6 (Action).

   The Custom Trouble Ticket panel appears.

3. Complete the following fields:

   Procedure Name

   Specifies the name of your NCL procedure for delivering tickets.

   Note: NCL must be in the CA NetMaster NM for TCP/IP COMMANDS concatenation. To list the concatenation, enter **/DATASET.A**.

   Enter Parameters Below

   Specifies any parameters that you want the NCL procedure to receive.

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

Example: Execute a REXX Procedure

The following example shows an NCL statement that executes a REXX procedure in your environment:

```
REXX rexx_procedure parm_1...parm_n
```

Define a CA Service Desk Trouble Ticket Interface

This option creates CA Service Desk request from the alert details.

To define a CA Service Desk trouble ticket interface

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

   The Alert Monitor : Trouble Ticket Interface Definition panel appears.

2. Enter **SERVICEDESK** in the Interface Type field and press F6 (Action).

   The Custom Trouble Ticket panel appears.

3. Complete the following fields:

   CA Service Desk Server Web Services HTTP URL

   Specifies the HTTP URL of the web services definitions on the target CA Service Desk server.

   Default: If left blank, the CA Common Services for z/OS CAISDI/soap component chooses the default server.

   Note: This URL points to the web services definitions that CAISDI/soap invokes to create the requests. This URL is not the same as the URL that is used to log on to CA Service Desk. Contact your CA Service Desk Administrator for the URL.

   CCI Sysid

   Specifies the CA Common Services for z/OS CCI system ID of the z/OS LPAR where the CAISDI/soap task is active. This ID is the SYSID name specified in the CAICCI startup JCL.

   Default: If left blank, the local CAICCI on this LPAR locates a suitable CAISDI/soap task.

   Request Description Format

   Specifies whether the SD Request Description field is produced with HTML formatting or in plain text (TEXT).

   Default: HTML

   Note: In most cases, you can leave the CA Service Desk Server Web Services HTTP URL and CCI Sysid fields blank. Leaving the fields blank allows the CAISDI/soap component to use its default values.

   Press F3 (File)

   The definition is saved.

Set Up the Trouble Ticket Data Definition

If you want the operator to supply information when creating a trouble ticket, you need to set up the ticket data entry definition.

To set up the trouble ticket data definition

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

   The Alert Monitor : Administration Menu appears.

2. Select option **D** - Define Trouble Ticket Data Entry.

   The Trouble Ticket Data Entry Definition panel appears.

3. In the free-format data entry section of the panel, enter the data entry definition for the panel that the operator will use when creating a ticket.

Notes:

- For more information about completing this section, press F1 (Help).
- You can create multiple field names by replicating the key variables linked by default.

Example1 : Trouble Ticket Data Definition

This example shows a definition that prompts the operator to identify the receiver of the ticket.

```
PROD-------- Alert Monitor : Trouble Ticket Data Entry Definition -------------
Command ===>                                    Function=Update Scroll ===> CSR

****** ***************************** TOP OF DATA ******************************
000001 FIELD NAME=$USRNAME
000002  VALUE="Problem@sydney.enterprise.com"
000003  DESC="Send Email to:"
000004  COMMENT="(name for email)"
000005  REQUIRED=YES
000006  LENGTH=40
****** **************************** BOTTOM OF DATA ****************************


 F1=Help      F2=Split     F3=File      F4=Save      F5=Find      F6=Change
 F7=Backward  F8=Forward   F9=Swap     F10=Left     F11=Right    F12=Cancel
```

Example 2: Data Entry Definition

To make the panel more user-friendly, you can change this panel by creating a trouble ticket data entry definition.

```
PROD-------- Alert Monitor : Trouble Ticket Data Entry Definition -------------
 Command ===>                                      Function=Update Scroll ===> CSR
 AMTTDED08 TROUBLE TICKET DATA ENTRY DEFINITION SAVED
 ****** ***************************** TOP OF DATA ******************************
 000001 FIELD NAME=$USRX
 000002  VALUE=
 000003  DESC="Press F6 to send the ticket"
 000004  COMMENT=
 000005  REQUIRED=NO
 000006  LENGTH=0
 ****** **************************** BOTTOM OF DATA ****************************


  F1=Help      F2=Split     F3=File      F4=Save      F5=Find      F6=Change
  F7=Backward  F8=Forward   F9=Swap     F10=Left     F11=Right    F12=Cancel
```

```
PROD---------------- Alert Monitor : Trouble Ticket Details -------------------
Command ===>

Press F6 to send the ticket ..
```

Implement Trouble Ticket Interface for Multiple Email Addresses

You can use an exit procedure, together with the trouble ticket interface and data entry definitions, to implement an interface that prompts operators for more than one email address to which they can send a trouble ticket.

To implement a trouble ticket interface for multiple email addressees

1. Create an NCL procedure with the following statements, and save it to your TESTEXEC:

```
&IF .&$USRNAME1 NE . &THEN +
&$AMTADDRESS1 = &$USRNAME1
&IF .&$USRNAME2 NE . &THEN +
&$AMTADDRESS2 = &$USRNAME2
...
```

   Note: The number of &IF statements sets up the number of addresses you want to provide.

2. Update the trouble ticket data entry definition (see page 73) with the following fields:

```
FIELD NAME=$USRNAME1
VALUE="&$AMTADDRESS1"
DESC="EMAIL ADDRESS #1"
COMMENT=""
REQUIRED=NO
LENGTH=40
FIELD NAME=$USRNAME2
VALUE=""
DESC="EMAIL ADDRESS #2"
COMMENT=""
REQUIRED=NO
LENGTH=40
...
```

   Notes:

   - The number of fields corresponds to the number of email addresses in the procedure you created.
   - The value &$AMTADDRES1 must be specified.

3. Define the email trouble ticket interface (see page 69) specifying a default address in the Mail Address field and the name of the procedure in the Exit Procedure Name field.

   The trouble ticket interface prompts operators for email addresses when they enter TT next to an alert.

Example: Implement a Trouble Ticket Interface for Two Email Addresses

To create an NCL procedure called EXAMPLE that sends emails to two addresses

1. Create an NCL procedure called EXAMPLE with the following statements, and save it to the TESTEXEC:

```
&IF .&$USRNAME1 NE . &THEN +
&$AMTADDRESS1 = &$USRNAME1
&IF .&$USRNAME2 NE . &THEN +
&$AMTADDRESS2 = &$USRNAME2
...
```

2. Enter **/ALADMIN** at the prompt.
3. Select option **D** - Define Trouble Ticket Data Entry.
4. Complete the panel as follows:

```
PROD-------- Alert Monitor : Trouble Ticket Data Entry Definition ------------
Command ===>                                    Function=Update Scroll ===> CSR

****** ***************************** TOP OF DATA ******************************
000001 FIELD NAME=$USRNAME1
000002  VALUE="&$AMTADDRESS1"
000003  DESC="EMAIL ADDRESS#1"
000004  COMMENT=""
000005  REQUIRED=NO
000006  LENGTH=40
000007 FIELD NAME=$USRNAME2
000008  VALUE=""
000009  DESC="EMAIL ADDRESS #2"
000010  COMMENT=""
000011  REQUIRED=NO
000012  LENGTH=40
****** **************************** BOTTOM OF DATA ****************************
```

5. Enter **/ALTTI** at the prompt.
6. Enter **EMAIL** in the Interface Type field and press F6 (Action).
7. Complete the panel as follows:

```
PROD--------------- Alert Monitor : Email A Trouble Ticket -Columns 00001 00072
Command ===>                                    Function=Update Scroll ===> CSR

Mail Address              defaultaddress@tt.com_____________________________
Host Name      (IBM)      HOSTNAME
SMTP Node Name (IBM)      NODENAME
SMTP Job Name  (IBM)      SMTP____
SMTP DEST Id (TCPaccess)  ________
Exit Procedure Name       EXAMPLE_
Subject                   &$AMDESC_____________________________________________

                             Enter Mail Text Below

****** ***************************** TOP OF DATA ******************************
```

Result

When an operator enters **TT** next to an alert, they are prompted for an email address as follows:

```
PROD--------------- Alert Monitor : Trouble Ticket Details --------------------
Command ===>


Email Address #1 ... defaultaddress@tt.com
Email Address #2 ...
```

Enable Alerts from External Applications

You can generate alerts (to view on the alert monitor) from external applications such as CA OPS/MVS.

Note: To use this feature, the SOLVE SSI must be active.

To enable alerts from external applications

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

   The Customizer : Parameter Groups list appears.

2. Enter **U** next to the $NM ALERTS parameter group in the Interfaces category.

   The ALERTS - Alert Monitor Interface panel appears.

3. Enter **YES** in the Enable External Alerts? field.

4. Press F6 (Action).

   The details are activated immediately.

5. Press F3 (File).

   The details are saved.

Forward Alerts

Alerts are normally displayed on the alert monitor; however, you can define them so that they are forwarded automatically to the following platforms:

- EM Console in CA NSM NetMaster Option
- UNIX platforms as SNMP traps
- CA NetMaster NM for SNA or Tivoli NetView (TME10) systems, as generic alert NMVTs
- CA Service Desk servers, as CA Service Desk requests or incidents

You can apply filter criteria to forward different types of alerts to different platforms.

Implement Alert Forwarding

You implement alert forwarding by using Customizer parameter groups.

Note: TNGTRAP and SERVICEDESK do not have clear alert events. Only active alerts and considerations are forwarded.

To implement alert forwarding

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

   The Customizer : Parameter Groups list appears.

2. Enter **U** beside the $NM ALERTS parameter group in the Interfaces category.

   The ALERTS - Alert Monitor Interface panel appears.

3. Complete the following field:

   Dest Type

   Specifies the type of alert forwarding to use.

   When you press Enter, the fields dynamically change to match the specified destination type.

4. (Optional) Press F8 (Forward) and repeat step 3 for each Definition ID, as required.

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

5. Press F6 (Action).

   The details are applied.

6. Press F3 (File).

   The details are saved.

Forward to CA NSM NetMaster Option

To receive alerts on CA NSM NetMaster Option, you must load the rules to reformat the alert messages for display on the EM Console.

To forward alerts to the EM Console in CA NSM NetMaster Option

1. Use FTP to download the message definition rules in binary mode from the UNIEMMSG member of your CC2DSAMP data set created at installation. For example, using the Windows FTP client from the prompt:

```
>ftp myhost
Connected to myhost.mycompany.com.
User (myhost.mycompany.com:(none)): user01
331 Send password please.
Password: xxxxxxxx
230 USER01 is logged on. Working directory is "/u/users/user01".
ftp>cd "prefix.NMC1.CC2DSAMP"
250 The working directory "prefix.NMC1.CC2DSAMP" is a partitioned data set
ftp>binary
200 Representation type is Image
ftp> get uniemmsg uniemmsg.txt
200 Port request OK.
125 Sending data set prefix.NMC1.CC2DSAMP(UNIEMMSG) FIXrecfm 80
250 Transfer completed successfully.
ftp: 3200 bytes received in 0.67Seconds 4.77Kbytes/sec.
ftp>quit
```

2. From a Windows prompt on the destination CA NSM NetMaster Option EM Server, load the message definition rules from the downloaded file. Enter the following command at the prompt to define the rules to event management:

```
cautil -f "uniemmsg.txt"
```

3. Enter the following command to load the rules:

```
oprcmd opreload
```

4. On CA NetMaster NM for TCP/IP, set the alert forwarding destination to TNGTRAP.

Forward as an SNMP Trap Definition

The MIB definition for alerts forwarded as SNMP traps is provided in member $AMTRAP, supplied in the *dsnpref*.NMC1.CC2SAMP data set. You can download this member to your UNIX system and compile it.

Note: When copying this member to your UNIX system, you can rename it to avoid problems on some UNIX systems where the $ sign has special meaning.

The supplied MIB defines two traps with the following object identifiers:

- $AMTRAP = 1.3.6.1.4.1.1126.1.2.1.2 (for an alert)
- $AMTRAPC = 1.3.6.1.4.1.1126.1.2.1.3 (when an alert is cleared)

Forward to CA Service Desk

Before you can forward alert details to CA Service Desk to create requests, you must implement CA Service Desk Integration. For more information, see the *CA Common Services for z/OS CA Service Desk Integration Guide*.

Do not forward any alerts to CA Service Desk until CA Service Desk integration is completely and correctly implemented; otherwise, all alert forwarding requests to CA Service Desk fail.

Suppress State Change Alerts

The region automatically generates an alert for a resource that changes state. You can suppress the alerts for selected state changes, and specify the severity levels of the generated state change alerts.

Note: State change alerts are based on RMAM001*xx* messages. These messages are defined in CAS, and you can customize them. For more information about how to maintain messages, see the *Managed Object Development Services Guide*.

To suppress automatically generated state change alerts

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

   The Parameter Groups panel appears.

2. Enter **U** next to the STATECHANGE parameter group in the Monitors category.

   The group opens for updating.

3. Blank out the fields for the states for which you want to suppress alerting. For example, if you want to suppress alerting for state changes to UNKNOWN, blank out the Unknown field.

4. Press F6 (Action).

   The region stops generating alerts for those state changes.

5. Press F3 (File).

   The group is updated with the changes.

Example: Monitor Listener Port

You are monitoring an address space that runs a critical IP application server and you want to raise a severity 1 alert if the listener port 3333 on TCP/IP stack STACK01 is not in a status of LISTEN, and clear the alert when the status becomes LISTEN. Port 3333 is associated with ASMON resource INETD7.

To raise an alert on a listener port

1. Enter **/IPMON** from the command prompt.

   The IP resource monitor appears.

2. Enter **UM** beside an application server ASMON resource.

   The Monitoring Definition panel appears.

3. Press F10 (EditLst).

   A list of attributes appears.

4. Enter **S** beside the PortStatus attribute.

5. Enter **?** in the Qualifier field and select the port number.
6. Enter **U** beside Value Alert.

   The Value Alert Details panel appears.
7. Complete the details as follows:

```
PROD--------------- Monitor Attribute : Value Alert Details -------------------
Command ===>                                                  Function=UPDATE

Resource ......... INETD7
Attribute ........ PortStatus
Description ...... Listening port state
Qualifier ........ TCPIP11-TCP(3333)
Å Value Alert
… Alert when value           Sev  Alert Description
…   is =

…   or =

…   or =

…   or =

… or NOT LISTEN               1

… Clear Alert when value is LISTEN
…                    or NOT UNKNOWN



 F1=Help      F2=Split     F3=Ok                    F5=Actions
                           F9=Swap                F11=EditText F12=Cancel
```

8. Press F3 (OK).

   The details are saved.

Implement Alert History

The alert monitor retains data in an alert history file. You can define the time period that alerts are retained.

To specify the time period that alerts are retained

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

   The Customizer : Parameter Groups list appears.

2. Enter **U** next to the $NM ALERTHIST parameter group in the Files category.

   The ALERTHIST - Alert History File Specification panel appears.

3. Complete the following fields:

   Days to Retain Alerts

   Specifies the number of days that you want to retain alerts in the history file.

   Limit: 999 days

   Default: 7 days

   Time of Day for Alert Purge

   Specifies the time of day (in the format *hh.mm*) at which alerts older than the value in the Days to Retain Alerts field are deleted from the history file.

   Press F6 (Action).

   The changes are applied.

4. Press F3 (File).

   The settings are saved.

Chapter 7: Configuring Packet Tracing

This section contains the following topics:

SmartTrace

SmartTrace is a real-time packet tracing facility that lets you do the following:

- Initiate a trace and view the results in real-time
- Define packet trace criteria, using a simple panel interface
- Export trace data to LIBPCAP or CTRACE format, which allows you to use the trace data with other packet tracing viewers
- Analyze a trace using IBM's Interactive Problem Control System (IPCS) trace reports

Configure SmartTrace

SmartTrace is implemented in the Packet Analyzer; therefore, the Packet Analyzer must be enabled to use SmartTrace. This configuration is done when you set up your product.

Default settings are defined; however, the settings are customizable when you run the following packet traces in your region:

- Traces that are started using the PT line command against a resource or connection
- User-defined traces, unless overridden in the trace definition

The default settings are customizable through the SMARTTRACE Customizer parameter group. During Express Setup, the group is populated with discovered ports associated with DB2 Distributed Relational Database Architecture (DRDA), FTP, HTTP, and Telnet for decoding packets.

Follow these steps:

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

   The Parameter Groups panel appears.

2. Select $IP SMARTTRACE from the Tuning category.

   The SMARTTRACE Customizer panel appears.

3. Complete the following fields:

   Note: For information about the Packet Analyzer parameters, see *SOLVE Subsystem Interface Guide*.

   Trace Limit

   Specifies the number of packets that are retained for a trace. When the limit is exceeded, the oldest packet is discarded.

   Limits: 10 through the value specified in the PAMMTTSIZE Packet Analyzer parameter in SOLVE SSI

   Trace Expiry

   Specifies the length of time that the trace is retained in memory before it is discarded.

   This value has the following format:

   hhh:*mm*

   Limits: 000:02 through the value specified in the PAMFZKPTIME Packet Analyzer parameter in SOLVE SSI

   Example: 100:10 (100 hours and 10 minutes)

   Initial Packets Traced

   Specifies the number of packets that are retained at the start of a TCP connection when you create a multiple TCP connection trace.

   Limits: 3 through the value specified in the PAMITTSIZE Packet Analyzer parameter in SOLVE SSI

   Maximum Connections Traced

   Specifies the limit on the number of TCP connection traces generated per stack when you create a multiple TCP connection trace. This limit does not include expired connection traces. When exceeded, any new TCP connections are ignored.

   Limits: 1 through the value specified in the PAMTCCCRLIM Packet Analyzer parameter in SOLVE SSI

   Press F8 (Forward).

   Page 2 of the group appears.

4. Review the ports to decode packets, and update the fields if necessary.

   Press F6 (Action).

   The details are applied.

5. Press F3 (Exit).

   The details are saved.

SmartTrace Security

SmartTrace lets you view IP packets as they flow into and out of a z/OS system, and provides instant access to the IP packet data.

Because IP packets can contain sensitive data, access to the data portion (that is, the data after the IP, TCP, and UDP headers) should be restricted to only those users who need to view the data in an IP packet.

To ensure that access to this data is correctly secured, CA NetMaster NM for TCP/IP utilizes the capabilities of the z/OS security package that is installed on your system (for example, CA ACF2 for z/OS, CA Top Secret for z/OS, or RACF).

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

Chapter 8: Configuring the DB2 Network Information Center

This section contains the following topics:

Overview

The DB2 Network Information Center provides functions essential to DB2 database administrators (DBAs) and other data center roles responsible for remote application connections to DB2 for z/OS. Before you can use some of these functions, a few one-time setup tasks are required. These tasks ensure that the region correctly monitors the DB2 Distributed Data Facility (DDF) address spaces on this system.

These tasks should be done by a person with the responsibility and authority to configure your CA NetMaster NM for TCP/IP regions.

How You Configure the Center in a New Region

The first time a new region starts, a program named Express Setup runs. Express Setup discovers all active DB2 for z/OS DDF address spaces on the system. (The discovery considers a DDF address space to be one that has a program name of DSNYASCP and an address space name ending in DIST.)

When Express Setup finds a DDF address space, it does these things:

- Define the DDF address space as a resource to the IP Resource Monitor. This resource definition ensures that the region collects throughput and performance data for the address space, and that you can run IP packet traces on the address space.
- Add the DDF TCP port numbers to the SMARTTRACE parameter group as DRDA ports. The identification of these ports ensures that when you view a DDF TCP/IP packet trace, SmartTrace does DRDA-specific decoding and formatting to make the trace a lot easier for you to understand.
- Add the traffic from the DDF address space to a DB2 business application name (see page 43). The name enables the region to add all DDF traffic together to make it easier to compare the total DB2 TCP/IP traffic with other TCP/IP traffic.

Express Setup only discovers DDF address spaces that were active when it ran. If a DB2 subsystem or its DDF address spaces was not active or had not yet opened a socket when Express Setup ran, you can define them to the region manually.

After Express Setup has run, you check what is discovered and customize the configuration to suit your requirements:

- You can use the IP Resource Monitor to see the defined DDF address spaces (ASMON resources). Enter the FILTER DB2 command to list the address spaces. (DB2 is a distributed monitor filter.) Add any missing DDF address spaces that you want to monitor as ASMON resources of Type DB2 (see page 55).
- Review the DRDA ports specified in the SMARTTRACE parameter group (see page 85). Add any missing ports.
- Review that the defined DB2 business application name meets your requirements. After you become familiar with all the DB2 diagnostics and traffic displays, you can replace the DB2 application name with more granular custom names of your choice. For example, you can group your traffic by DB2 subsystem version, function, geography, user, and so on).

How You Configure the Center in an Existing Region

In general, Express Setup is not rerun in upgraded regions because these regions have existing monitoring specifications that must be kept unchanged. Normal region upgrade retains all DB2 DDF address spaces that the IP Resource Monitor monitors previously.

You review and customize the existing configuration to suit your requirements:

- The DB2 Network Information Center requires that the DDF address spaces be defined as ASMON resources of Type DB2. Review the definitions, and update the type if necessary. You can use the U line command on the IP Resource Monitor to update a resource definition.
- Add any missing DDF address spaces that you want to monitor as ASMON resources of Type DB2 (see page 55).
- Update the SMARTTRACE parameter group (see page 85) for any missing DRDA ports. You can identify the ports using the IL option at the information center.

Add Traffic From a DDF Address Space to the DB2 Application Name

Sometimes, you can find that Express Setup has not added a DDF address space to the DB2 application name. You can add the address space manually by copying the name definition for an existing DDF address space.

To add a DDF address space to the DB2 application name

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

   The TCP/IP Application Name Definition List appears.

2. Find the definitions with a base application name of DB2. Press F11 (Right) until the Application Jobname column appears.

   The column shows the job name of the DDF address spaces.

3. Enter **C** next to the last DB2 entry.

   The Application Name Definition panel appears.

4. Update the Application Jobname field with the job name of the DDF address space you want to add, and press F3 (File).

   Traffic from the DDF address space is added to the DB2 application name.

Chapter 9: What's Next?

This section contains the following topics:

For More Information

Now that you have completed the tasks in this guide, you can use your CA NetMaster NM for TCP/IP region to perform useful tasks in your z/OS TCP/IP environment.

We recommend that you use the region for a while to ensure that you have configured the correct IP nodes and resources, are monitoring the most useful attributes, and so on. When you are happy with the set up, you can continue with more advanced customization.

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

When you are familiar with CA NetMaster NM for TCP/IP, you can explore its more advanced features by reading the other guides in the documentation set. These can be downloaded from Technical Support.

Note: For assistance, contact CA Support at http://ca.com/support.

Index

S

T