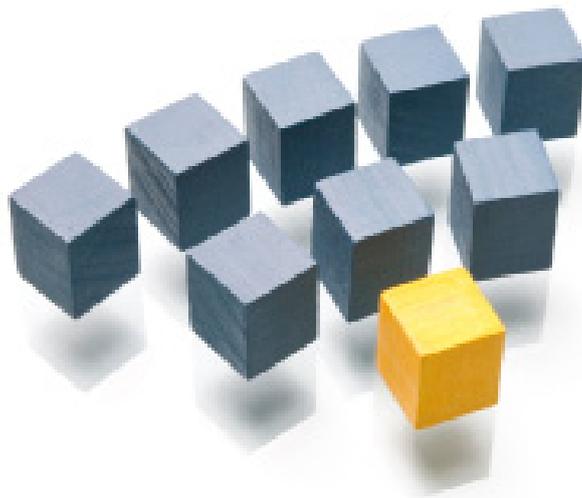


Reflex 80:20

Technical Guide





Document Tracking

Reflex Version:	4.8E
Issue Date:	APR, 2018

Document History

Date	Version	Details
13/04/07	4.7J	Technical Guide , containing Document Tracking and History tables and details of FIXSBJH utility.
13/04/07	4.7J	Amended Spooler Autodiscovery section to remove RUN command from SPAD.
21/06/07	4.7J	Amendments to License files installation.
18/09/07	4.7K	Updated Transit file table.
23/11/07	4.7K	Included FUP RELOAD commands for FIXSBJH utility.
31/12/07	4.7K	Amendments to ALTPMON, RFRECONQ utilities.
31/12/07	4.7K	New sections for Pathway Monitoring and Individual Disk Monitoring (% Full) modules.
21/01/08	4.7K	Additional file - ACTCOMM - added to files which can be updated by RFLXINTG utility.
21/05/08	4.7K	Additional information for Report 13 for ACTEXPF messages. New section for ACTEXPF utility.
14/10/08	4.7L	Updated ACTEXPF utility. New section for FIXNUMOB utility. Re-ordered Utilities section.
30/09/09	4.7M	New sections for Individual Disk Monitoring (I/O times) and File-Metrics Monitoring, amendments to Pathway Servers and Admin tables and general text changes.
30/12/09	4.7M	Additional parameters for TCP/IP M-State monitoring.
06/01/10	4.7M	Included reference to REFLEX-PWAY-MON in Pathway Monitoring section.
29/07/10	4.7M1	New PMON-INITIAL-INTERVAL parameter. FIPR-POLL-INTERVAL parameter value changed.
28/02/11	4.7N	New utility - RFUSERHK. Amendments to RFIMEX event table, Pathway Server Config, new event ranges, Admin parameters, HBIMEX TRANSIT file rec length.
03/10/11	4.7N1	Additional event ranges, new parameters, amendments to SPAD utility, typographic fixes.
11/07/12	4.7P	New Heap and PFS monitoring parameters. New Specific Process Monitoring module.



Document History (Continued)

Date	Version	Details
15/04/14	4.8	New MEASURE parameters and MEASURE serverclass descriptions for use with Reflex performance monitoring. Updates to NT alerting. Obsolete references included. General document maintenance and improvement.
10/10/14	4.8	Additional entries for MEASUREMENT-xxx-ARRAY-SIZE parameter.
01/06/15	4.8C	Chapter on FILE EXISTENCE MONITORING, typo fixes, new TRANSIT File for time sync events, general improvements to guide.
14/10/15	4.8C	Changed edit file reference for use with ALTPMON, from PROCLIST to ALTPLIST. Update to threshold flags in Admin Parameters to cater for TCP/IP via CLIM.
31/05/16	4.8C	TCPIPAD updated to include a reference to performing a FULL Warmboot in Overdrive Setup, after autodiscovering an HPE NonStop TCP/IP stack.
09/09/16	4.8D	Removed ISO9001:2008 and TickITplus references from Company Information. Updated parameter section concerning use of DEFAULT-GUARDIAN-USER.
11/04/18	4.8E	<p>Update to Transit File list.</p> <p>New Admin parameter - PFS-CAPTURE-ENABLED - to enable/disable the capturing of PFS metrics for Processes by Dashboard and the Specific Process Monitoring module.</p> <p>Email alerting updated to include Critical as the Severity choice if the resultant email is to be marked with a High Importance flag.</p> <p>Amended HP to HPE.</p> <p>VERSIONINFO chapter included.</p> <p>File Existence attributes changed from 'File not Open' to 'File is Open' and from 'EOF Not Zero' to 'File Empty'.</p> <p>New File Existence attributes for monitoring the 'Age of a File' and the 'Modification Age' of a file.</p> <p>Change to building name in Company Information in last page.</p>

**Contents**

1. Introduction
2. Utilities
3. Individual Disk Monitoring (% Full)
4. Individual Disk Monitoring (I/O Times)
5. Specific Process Monitoring
6. File Existence Monitoring
7. File Metrics Monitoring
8. Pathway Monitoring
9. Autodiscovery
10. SNMP Gateway
11. Windows Services
12. Administration Parameters
13. Installation and Configuration Issues
14. Currently Delivered Reaction Event Ranges
15. Reflex 80:20 PATHWAY Server Configuration
16. Reflex 80:20 PATHWAY Server Descriptions
17. Reflex 80:20 Non PATHWAY processes
18. Reflex 80:20 Facilities and their Abbreviations
19. OMF Conversion Facilities
20. Configuring Multiple Console Servers
21. Reflex Database Integrity Program
22. Reflex ONE24
23. Product Version Utility

Company Information



1. Introduction

This Technical Guide covers various issues which are not covered in the Installation, GUI Online Help and the Quick Start guide.

Throughout this guide, the Reflex 80:20 subvolumes and SQL Catalog may occasionally be referred to as follows:

- Object subvolume: **RFLXOBJ**
- Database subvolume: **RFLXDAT**
- Data-Dictionary subvolume: **RFLXDDL**
- SQL Catalog: **RFLXCAT**

The NonStop node and disk volume may not be referred to in some examples, as assumptions are made that users will be on the correct node and volume for the Reflex 80:20 environment.

Users should change the above to meet their requirements.





Introduction

Reflex 80:20 is supplied with additional utilities that are accessed via a TACL session.

These utilities allows a user to perform various administration functions such as run database reports, start a Gateway streamer process, warmboot facilities, insert Heartbeat processes, insert entries for File-Metrics monitoring, copy EMS events between different Reflex environments.

A summary of each Reflex utility is listed below with a full description of each utility being provided on subsequent pages.

UTILITY	Description
ACTEXPF	Report on and / or resolve expired Action Groups.
ACTFLAGS	Alter Sentra flags for Action Groups.
ACTPDEL	Delete entries from Heartbeat Module - 'Process Monitor' - database.
ACTPINS	Insert entries into Heartbeat Module - 'Process Monitor' - database.
ALTPMON	Start / Stop monitoring of Heartbeat Module - 'Process Monitor' - entries.
ALTTASKO	Alter ownership of Tasks configured in the Tasks Module.
AUDTASK	Report on the usage of Reflex Tasks.
EMSEXTRACT	Convert identical EMS events, e.g. convert identical HPE NonStop OSS events into distinct events.
FILECLNU	Resolve invalid Status Monitor formats as configured within Action Groups.
FIMETINS	Insert entries into Heartbeat Module - 'File-Metrics' - database.
FIXNUMOB	Report on and / or fix GROUP_NUM_OBJECTS value in Reflex SQL database.
FIXSBJH	Integrity check for Subject_History and Subject_Control SQL tables.
FMIMEX	Import / Export for Heartbeat Module - 'File-Metrics' - entries.
GATEWAY STREAMER	Create new EMS tokenised events.
HBIMEX	Import / Export for Heartbeat Module - 'Process Monitor' - entries.
RFADDUSR	Create a Security Profile for a nominated Guardian group.user name.



UTILITY	Description
RFIMEX	Import / Export for Action Groups, including use of pre-delivered EMS events ranges via Reflex transit files and also the import of NetBatch events and creation of associated NetBatch Status Monitor objects.
RFIMEXQ	Import / Export of data between Reflex SQL tables.
RFLXCOM	Command line utility, providing a range of facilities, e.g. warmboot, filter compile & generate, archive.
RFRECONQ	Modify node references in Reflex database. Generally used following a site-swap.
RFUSERHK	Review the Reflex security database and optionally report on or delete obsolete GUARDIAN user ids.
SERVICE MONITOR REPORTS	Print contents of Reflex Service Monitor database.
STATCOLL	Report on EMS statistics for a NonStop node, showing the range and number of SSID's and event numbers.
TASKIMEX	Import / Export for Reflex Tasks.
XRPTMENU	Report on contents of the Reflex database, e.g. Process Monitor entries, Action Groups, Security Profiles, EMS event Custom Detail.
XRPTMENU - REPORT13	Report on relationship between Action Groups and Status Monitor objects.



ACTEXPF

On running the SMON Reactions Report 13 (See XRPTMENU - REPORT 13 facility), there is a possibility that the following may be displayed in the report:

1. Reaction records may be found that are using Cover Periods which utilise two digit years, e.g. 99. Reflex will correctly handle these reactions but it is recommended that they are amended to use four digit years for consistency, e.g. 1999.
2. Reaction records may be found whose Cover Period will expire soon. Once expired, the reactions will no longer be acted upon; therefore, such reactions should be amended.

In either case, the ACTEXPF utility will resolve these issues. All Cover Period records will be amended to use four digit years and any Cover Periods that are due to expire will be extended by 10 years.

Note: It is recommended that the utility is executed when Reflex is shutdown since it will lock ACTEVE records.

The format of running the RFLXOBJ.ACTEXPF utility is:

```
RUN ACTEXPF / In <dataconf> / [preview]
```

Dataconf represents the name of the data configuration file which is found in the Reflex data subvolume, e.g. RFLXDAT.DATACONF.

Preview is an optional parameter. If specified, the ACTEXPF utility will run in 'preview' mode where it will determine if there are any problems in the ACTEVE file but not make any amendments.

Examples of running the ACTEXPF utility:

```
$LIVE RFLXOBJ 79> run actexpf /in $dev.rflxdat.dataconf , name $ACTE/ preview
File Open error 48 in file \ITLTECH.$DEV.RFLXDAT.ACTEVE.
0 Acteve records have been read.
0 Acteve records found that have two digit years.
0 Acteve records found that are due to expire.
No Acteve records have been updated.
```

```
$LIVE RFLXOBJ 80> run actexpf
Aborting because DATACONF not supplied as IN parameter.
Usage: ACTEXPF /IN <dataconf> / [Preview]
0 Acteve records have been read.
0 Acteve records found that have two digit years.
0 Acteve records found that are due to expire.
No Acteve records have been updated.
```

```
$LIVE RFLXOBJ 81> run actexpf /in $live.rflxdat.dataconf , name $ACTL/ preview
ACTEXPF Running in Preview Mode ... Please wait.
232 Acteve records have been read.
13 Acteve records found that have two digit years.
1 Acteve records found that are due to expire.
No Acteve records have been updated.
```

```
$LIVE RFLXOBJ 82> run actexpf /in $live.rflxdat.dataconf , name $ACTE/
ACTEXPF Running in Update Mode ... Please wait.
232 Acteve records have been read.
13 Acteve records found that have two digit years.
1 Acteve records found that are due to expire.
14 Acteve records have been updated.
```

Note: The ACTEXPF utility will only extend the cover period of reactions that are due to expire within the current year, **OR** the first six months of the following year. If reactions are configured that have expired more than one year ago, they will be reported upon but NOT amended; such reactions should be manually checked to determine if they are still relevant.



ACTFLAGS

ACTFLAGS is a command line utility program which allows the user to change certain flag settings of ACTEVE records without going through the GUI screen.

The utility can change the flags: Send-to-Sentra and the Send-Critical.

Actflags can operate on a single record or a group of records. When operating on groups of records, we can group by a common attribute such as Action Group, Owner etc.

ACTFLAGS uses the following commands:

```
HELP
FC
DISPLAY
SHOW
SET
RESET
UPDATE
EXIT
```

Starting the ACTFLAGS utility

To start ACTFLAGS the following must be defined if not already done so:

```
ADD DEFINE =INSIDER_REFLEX_DATACONF, FILE \node.$volume.RFLXDAT.DATACONF
```

where \node.\$volume.RFLXDAT.DATACONF is the full pathname of the Reflex 80:20 dataconf file, e.g. \ITLTECH.\$LIVE.RFLXDAT.DATACONF.

then enter the following at a TACL prompt, to start the ACTFLAGS utility:

```
RUN RFLXOBJ.ACTFLAGS
```

where RFLXOBJ is the Reflex 80:20 object subvolume.

The following information will be displayed upon successful startup:

```
Reflex 80:20 Acteve File Flag Set Utility 12/07/2012 06:37
Use HELP ALL for list of commands and syntax
```

then the command prompt:

```
ACTFLAGS>
```

will be displayed allowing the commands to be entered.

The ACTFLAGS utility is now ready to accept commands.



ACTFLAGS Commands

HELP

Use the HELP command to list the syntax of the ACTFLAGS commands.

```
HELP <help-options>
    <help-options>
        { <command-name> | ALL }
```

command-name

is the name of an ACTFLAGS command whose syntax you want to see.

ALL

lists the names of all ACTFLAGS commands with their syntax.

Examples

Enter HELP to display the names of all ACTFLAGS commands:

```
ACTFLAGS> HELP
EXIT          HELP          SET          FC          SHOW          UPDATE
DISPLAY      RESET
```

Enter HELP SET to display the syntax of the SET command:

```
SET <set-options>
    <set-options>
        { OWNER {<SSID owner> | *} }
        { SSID_VALUE {<SSID value>} }
        { RANGE {<event value>|<event from value> TO <event to value> } }
        { ACTION_GROUP {<action group>} }
        { MATCH {Y|N} }
        { FLAGS {EVENTS|CRITICAL|ALL} {Y|YES|N|NO} }
```

FC

Allows editing of last command entered.

```
e.g > ACTFLAGS> fc
    ACTFLAGS> HELP
        .      all
ACTFLAGS> HELP all
```

EXIT

Use the EXIT command to stop the current ACTFLAGS process and return to the TACL prompt.

```
EX[IT]
```

You can enter EX or EXIT to run the EXIT command, i.e.:

```
ACTFLAGS> exit
Exiting from ACTFLAGS
```

Simultaneously pressing the CTRL and Y keys at the terminal will stop ACTFLAGS after it displays EOF!

SET

Use the SET command to change one or more attribute rule settings before you update any ACTEVE records.



Use the SHOW command to display the current attribute rule settings.

You can also restore the attributes to their default settings by using the RESET command, e.g.:

```
ACTFLAGS> set owner insider
ACTFLAGS> show owner
> Owner          : INSIDER
```

This rule states that all only records with the owner of "INSIDER" will be updated.

```
ACTFLAGS> set owner *
```

This rule states that all records for all owners will be updated.

An action group may be terminated by the asterisk (*) wildcard character, e.g.:

```
ACTFLAGS> set match y
ACTFLAGS> set action_group insider*
```

This match rule states that action groups with an action group starting with "INSIDER" will be matched. i.e. "INSIDER-GROUP", "INSIDER-DISK" etc will all be matched.

If match was set to 'N' then action groups terminating with the wildcard character will NOT be treated as a wildcard search.

A warning will be displayed in this situation.

If the action group does not terminate with the wildcard character then the match setting will have no affect.

If match is set to 'Y' and there is no terminating wildcard character in the action group then only that exact action group will be matched, e.g.:

```
ACTFLAGS> set match n
ACTFLAGS> set action_group insider
```

This match rule states that only the action group "INSIDER" will be matched.

SHOW

Use THE SHOW command to display the current ACTFLAGS settings of the attributes.

```
SHOW <show-options>
    <show-options>
        [ <attribute-name> | ALL ]
<attribute-name>
    { OWNER|SSID_VALUE|RANGE|ACTION_GROUP|MATCH|FLAGS }
```

Examples

```
ACTFLAGS> show all
> Current Settings
> Action Group   : insider-up
> Match          : NO
> Flags          : EVENT Y
> Owner          : Insider
> SSID Value     : 0006
> Range          : 00409 To 00000
```

Display current owner setting

```
ACTFLAGS> SHOW OWNER
> Owner : Insider
```



RESET

Use the RESET command to restore the rule settings back to their default values:

```
RESET <reset-options>

  <reset-options>
    [ <attribute-name> | ALL ]

  <attribute-name>
    { OWNER|SSID_VALUE|RANGE|ACTION_GROUP|MATCH|FLAGS }
```

EXAMPLES

Reset all attribute settings to default values:

(Equivalent to entering RESET with no parameters)

```
ACTFLAGS> RESET ALL
```

Reset Owner attribute to default setting:

```
ACTFLAGS> reset owner
ACTFLAGS> show owner
> Owner          : Not defined
```

DISPLAY

Use this command to display all records satisfying the rules of the parameters to the command. These rules are independent of the attribute rule settings.

```
DISPLAY <display-options> |<display-options><extra action group option>

  <display-options>
    [<attribute-name> <setting>| ALL]

  <attribute-name>
    { OWNER|SUBSYSTEM|SUBSYSTEM<SSID subsystem><range attribute>|
      ACTION_GROUP }
```

The owner attribute may be followed by an action group or action group prefix to narrow down the set of records displayed.

The subsystem attribute may be on its' own or it may be followed by other attributes to narrow down the set of records displayed.

The extra attributes may be a From event on its' own, an event range, an action group or a matching action group prefix.

```
<range attribute>
  { RANGE <from value>|RANGE <from value> TO <to value> }
```

A range may consist of a From Event on its' own or a From and To event.

```
<extra action group option>
  { ACTION_GROUP <action group name/prefix> }
```

This may follow an OWNER or SUBSYSTEM subcommand and displays records with a particular action group or matching a particular action group prefix as well as a particular owner, SSID value or range.

EXAMPLES:

```
ACTFLAGS> display owner insider

Owner      Value From   To      Action Group
```



```
SendCritical SendToSentra
```

```
INSIDER 0006 +00409 +00000 EVENT-TIMER ALERT
NO          YES
```

```
ACTFLAGS> DISPLAY SUBSYSTEM INSIDER.0006
```

```
Owner      Value From To      Action Group
SendCritical SendToSentra
```

```
INSIDER 0006 +00409 +00000 EVENT-TIMER ALERT
NO          NO
```

```
ACTFLAGS> display subsystem insider.0006 range 00409
```

```
Owner      Value From To      Action Group
SendCritical SendToSentra
```

```
INSIDER 0006 +00409 +00000 EVENT-TIMER ALERT
NO          YES
```

```
ACTFLAGS> display action_group busy processes
```

```
Owner      Value From To      Action Group
SendCritical SendToSentra
```

```
INSIDER 0050 +00229 +00000 BUSY PROCESSES
NO          YES
```

```
INSIDER 0050 +02559 +00000 BUSY PROCESSES
NO          YES
```

UPDATE

Use the UPDATE command to perform flag setting changes to values and ACTEVE records satisfying the rule settings.

(Some rule settings may be ignored whenever the user is given the option), e.g.:

```
ACTFLAGS> show all
> Current Settings
> Action Group   : Not defined
> Match          : NO
> Flags          : EVENT Y
> Owner          : Not defined
> SSID Value     : 0000
> Range         : 00000 To 00000
```

```
ACTFLAGS> set owner insider
ACTFLAGS> set ssid_value 6
ACTFLAGS> set range 409
```

```
ACTFLAGS> show all
> Current Settings
> Action Group   : Not defined
> Match          : NO
> Flags          : EVENT Y
> Owner          : INSIDER
> SSID Value     : 0006
> Range         : 409 To 00000
```

```
ACTFLAGS> update
Updates successfully performed.
```



e.g. Choose to ignore the setting for the SSID value and/or range:

```
show all
> Current Settings
> Action Group   : Not defined
> Match          : NO
> Flags          : EVENT Y
> Owner          : Not defined
> SSID Value     : 0000
> Range         : 00000 To 00000

ACTFLAGS> set owner insider
ACTFLAGS> show owner
> Owner         : INSIDER

update
SSID value is a default. Ignore the setting? y/n.
?y
Range value is a default. Ignore the setting? y/n.
?y
Updates successfully performed.
```

In some cases no updates will be performed. The following message will then be returned:

```
ACTFLAGS> update
No updates made.
```

To update Action Groups for sending events to Sentra for MIS reports, utilise the following parameters/values:

To pass **ALL** events to Sentra - **>SET FLAGS EVENTS Y**

To pass only **CRITICAL** events to Sentra - **>SET FLAGS CRITICAL Y**

To pass **NO** events to Sentra - **>SET FLAGS ALL N**



ACTPDEL

This utility is designed to allow Reflex 80:20 users to delete process entries from the Heartbeat - Process Monitoring - database via an edit input file, instead of deleting them via the GUI. By using an edit file, single or multiple Reflex 80:20 environments can be easily amended without the need to manually make changes via the GUI.

Note: This utility will not delete any entries from the SQL Object database, nor will it delete any Reaction configurations. This ensures that no required monitoring will be removed, e.g. the event ranges for the deleted process may be used by another monitored process.

To execute this utility, enter the following command at a TACL prompt:

```
RUN RFLXOBJ.ACTPDEL / IN <process list> , OUT <dataconf> /
```

Where:

<process list> is a file containing the names of the NonStop processes that will be deleted from the Reflex 80:20 ACTPROC Enscribe database file. The <process list> file must exist and it must be an edit type file, code 101 and should contain a list of named processes with one process per line, e.g.:

```
\STANDBY.$APP1
\LIVE.$APP1
$ARCH
```

Note: Node prefixes are optional for 'local' processes. If a node prefix is not specified, then ACTPDEL will attempt to delete the process configured in the local node, i.e. if ACTPDEL is running in the node \LIVE, then in the example above, ACTPDEL would delete \LIVE.\$ARCH. If a 'remote' node process needs to be deleted, then its node must be specified as in the above example, e.g. \STANDBY.\$APP1.

<dataconf> is the standard Reflex Dataconf file for the nominated Reflex 80:20 environment, which will be used to locate the ACTPROC file.

Once the utility has completed, a Warmboot of the Reaction servers is required to activate the changes. ACTPDEL will display a summary of how many processes have been deleted, along with reminder messages, e.g.:

```
Successfully removed 003 processes from the ACTPROC file.
GUI views should be refreshed to see the revised process monitoring list.
Warmboot the Reaction Servers to activate the changes.
```

During processing, any non-critical errors will be displayed on the home terminal with execution continuing. Non-critical errors include issues such as badly formatted process names in the <process list> edit file. Examples of non-critical errors are:

```
"ACTPROC record was not found for process \DEV      $TEST - skipping."
```

This error means that the reported process could not be found in the ACTPROC file that contains the Heartbeat process list.

```
"Invalid processname found in the process list file on line 11.101 - skipping."
```

This error means that a named process could not be located on the displayed line in the process list file. This could be due to a blank line, or some sort of comment.

```
"Invalid processname read from the process list file: $ThisIsTooLong."
```

This error means that a string starting with a \$ character was found but it was not a valid process name.



ACTPINS

This utility is designed to allow Reflex 80:20 users to update the HeartBeat - Process Monitoring - database with configuration information held in an edit input file rather than submit this same information through the configuration screens. This configuration file could be applied to several Reflex 80:20 databases, thereby reducing the amount of manual configuration required.

To execute this utility, enter the following at a TAQL prompt:

```
RUN ACTPINS / IN <edit-configuration-commands>, OUT <DATACONF> /
<OBJECTQ-update-param>, <OBJECTQ-Initial-status>, <EMS-event-specification>
```

Where:

<edit-configuration-commands> is the edit file that contains the names of the NonStop processes that will be added into the Reflex 80:20 ACTPROC database file. The file must exist and it must be an edit file, code 101.

The file has the format of: <Process-name> , <start-time>, <end-time>, <description>

<Process-name> - The process name to be inserted in the ACTPROC database. The name should start with a "\$" and not be prefixed with a node name, e.g. \$ZTC0.

<start-time> - This value is optional, the default is 00:00. The format is HH:MM for hours and minutes. This field signifies the time that monitoring is to commence.

<end-time> - This value is optional, the default is 23:59. The format is HH:MM for hours and minutes. This field signifies the time that monitoring is to end.

<description> - This value is optional; the default is that there is no description required.

Some examples:

```
$ZTC0, 00:00, 23:59, TCP/IP process
$SPLS , , , Spooler Supervisor
$BMON
```

<dataconf> - Is the DATACONF file for the nominated Reflex 80:20 system. DATACONF is used to locate the files that make up the Reflex 80:20 database. In this instance, the ACTPROC file will be accessed by the ACTPINS program. The DATACONF file must exist.

<OBJECTQ-update-param> - By default, a process HeartBeat entry will always be created in the ACTPROC database. This parameter determines whether an entry will be created in the OBJECTQ SQL table. This table can then be viewed by Reflex 80:20 Users and used to build a Status Monitor display. Valid values are Y or N. The default is N.

<OBJECTQ-Initial-status> - This parameter determines the initial status field of objects added to the OBJECTQ SQL table. Valid values are IN or UP. The default is "IN".

When UP is specified, the process object will be set to an UP state in Reflex.

When IN is specified, Reflex will investigate the process to determine if it is running and then set an appropriate state.

<EMS-event-specification> - This parameter provides details of the down and up events that must be generated when a process is detected as executing or not executing.

The format of the parameter is "SSID-Owner.Value.Version.DOWN-event.UP-event", e.g.: **INSIDER.51.0.1001.1002**.

Validation: The values must conform to the standard EMS ranges.



ALTPMON

This utility will allow users to switch off / on, Process Monitoring performed by the HeartBeat module. The utility can be configured as a Reflex reaction to an event, executed via a Reflex Task, or embedded in obey files that load or shutdown an application.

Note: Only processes that are monitored 24 hours (00:00 to 23:59 for example), can have their monitoring period switched off or on. If unsure which processes ALTPMON should modify, check the Process 'Monitoring Period' details in the Heartbeat module. See also option 7 in XRPTMENU which can print out configuration details for all Heartbeat processes.

To execute this utility, enter the following at a TACL prompt:

```
RUN ALTPMON / IN <edit-configuration-file>,OUT DATACONF / <START | STOP>,
<Update-objectQ-database>, [ABORT]
```

Where:

<edit-configuration-file> is a file containing the names of the HPE NonStop processes for which monitoring will be stopped or started. The process can be prefixed with a node name. If no node name is specified, then local node name is assumed. The file must exist and it must be an edit file, code 101.

The edit-configuration-file contents have a format of **<process-name>**

<process-name> - the process as name held in the ACTPROC database. The name should start with a "\$" and optionally, prefixed with a node name.

Some examples are:

\$ZTC0 (this will assume a local node prefix)

\LIVE.\$XBK1

DATACONF is the DATACONF file for the nominated Reflex 80:20 system. DATACONF is used to locate the files that make up the Reflex 80:20 database. In this instance, the ALTPMON program will locate and access the ACTPROC file, via a DATACONF lookup. The DATACONF file must exist.

START | STOP The parameter that actions the starting or stopping of monitoring. One of these options must be supplied.

If START is selected, then the initial status is set to IN (for INvestigate). Status Monitor will investigate the process status during warmboots.

if STOP is selected, then the initial status is set to UP. No checks will be performed by Status Monitor during a warmboot.

<Update-objectQ-database> - This parameter determines whether the initial status field of the corresponding objectQ entry will be updated. Valid values are Y or N. The default is Y.

[ABORT] This is an optional parameter that will cause ALTPMON to abort and back out all updates if an error occurs. If ABORT is not specified, then the default behaviour is performed which will skip any entries in the edit-configuration-file that cause an error, i.e. all valid updates are performed and errors are ignored.



Example results

Running ALTPMON without an ABORT parameter

An ALTPLIST edit file has been created, containing an entry for a non-existent process called \$NONE.

All valid updates are performed and an error message is produced for the process in error.

```
RUN RFLXOBJ.ALTPMON / IN ALTPLIST, OUT RFLXDAT.DATACONF / START, Y
```

Output:

```
Missing Abort parameter. Defaulting to ignoring errors.  
Error 011 reading ACTPROC for processname: $NONE  
ACTPROC records successfully updated; 0001 entries skipped.  
All OBJECTQ database records successfully updated.
```

Running ALTPMON with ABORT parameter

The same ALTPLIST edit file is used as in the above example.

The utility abends and all updates are backed out - this is the same behaviour as the pre 4.7K version of ALTPMON.

```
RUN RFLXOBJ.ALTPMON / IN ALTPLIST, OUT RFLXDAT.DATACONF / START, Y, ABORT
```

Output:

```
Error 011 reading ACTPROC for processname: $NONE
```



ALTTASKO

This utility is designed to reduce the amount of configuration carried out in the Reflex 80:20 GUI. It will allow nominated users to be given ownership of specified Tasks or have ownership revoked without the need to make multiple changes via the GUI.

To execute this utility, enter the following at a TACL prompt:

```
RUN RFLXOBJ.ALTTASKO / IN <subvol>.<editfile>, OUT RFLXDAT.DATACONF/ ADD |  
DELETE <taskname>
```

Where:

<subvol>.<editfile> is an edit file that contains a list of user ids:

Each user id may be in alpha format <usergroup>.<member name>, or numeric format <group number>.<user number>.

<user group number>, <member number>.

Note: Leading / trailing spaces will be ignored.

Example of edit file contents:

```
develop.team  
1,175  
live.app
```

Each line in the edit file may have up to one user only. The file must exist and it must be an edit file, code 101.

RFLXDAT.DATACONF is the location of the Reflex 80:20 DATACONF file for the nominated Reflex system. DATACONF is used to locate the files that make up the Reflex database. In this instance, the ALTTASKO program will access the TASKOWNR and TASKCONF files. The DATACONF file must exist.

ADD When the ADD keyword is specified ownership is given to the specified task **<taskname>** to all user id's nominated in the edit file **<subvol>.<editfile>**.

DELETE When the DELETE keyword is specified ownership is revoked to the specified task **<taskname>** to all user id's nominated in the edit file **<subvol>.<editfile>**.

<taskname> is the name of the task for which the bulk user ownership should be added or deleted. This parameter is mandatory and the task should exist in the TASKCONF file.



AUDTASK

The Task Audit Reports utility provides a mechanism for printing off a report detailing the use of the Reflex Tasks facility.

Entering the following at the TACL prompt runs the Task Audit Report utility:

```
RUN RFLXOBJ.AUDTASK /IN <dataconf file>, NAME <$your choice>, OUT $S /
```

The **IN** file must be the DATACONF which provides the file assignments used by Reflex 80:20. This is a **compulsory parameter**.

The **OUT** file is the destination for the report, typically a spooler location for a printer.

After issuing the run command, the following menu is displayed:

```
Reflex 80:20 Tasks Audit Report
Please Select the type of report required:
1. Report on a Specific User Id
2. Report on a Specific Terminal
3. Report on a Specific Facility
4. Report on all Task Changes (default)
X. Exit
?
```

Reporting on a specific User Id will allow a report to be produced detailing the entire Task related work carried out by a particular Reflex User.

Reporting on a specific Terminal will allow a report to be produced detailing the entire Task related work carried out on a particular Terminal.

Reporting on a specific Facility will allow a report to be produced detailing all of the work carried out using a particular Facility. Facilities supported are:

```
TTU  Task Type Update
RTA  Change of Task Configuration
RPU  Change of Program Configuration
RTO  Change of Task Owner
```

Once a type of report has been selected, the Start and End periods for the report may be entered:

```
Please Enter a FROM date (DD/MM/YYYY,HH:MM) OR X to Exit.
```

```
The default date is the START of the Audit Log.
```

```
?
```

```
Please Enter a TO date (DD/MM/YYYY,HH:MM) OR X to Exit.
```

```
The default date is the END of the Audit Log.
```



The report will then be created and written to the destination supplied in the start-up parameter OUT. Once complete a summary message will be displayed:

The report completed Successfully. 000173 records found.

An excerpt from a report print is shown below:

```

** INSIDER TECHNOLOGIES LTD. ** REFLEX 80:20  AUDIT DETAIL PRINT **
-----
TIMESTAMP: 13:05:08 15-APR-13  NAME:      STPSRV      TYPE: PATHWAY
TERMINAL:   DSHIELDS              SUBTYPE:  SERVER              CLASS: LIST
USER-ID:    DEMO.REFLEX
FACILITY:   TTU
ACTION:     INSERT
TIMESTAMP: 13:05:52 15-APR-13  NAME:      STRSRV      TASK-USER-ID: SUPER.SUPER
TERMINAL:   DSHIELDS              TERMINAL:  DSHIELDSSTRSRVV
USER-ID:    DEMO.REFLEX           TASK-DESC:
FACILITY:   RTA
ACTION:     INSERT                PROGRAM:   *****  WAIT:

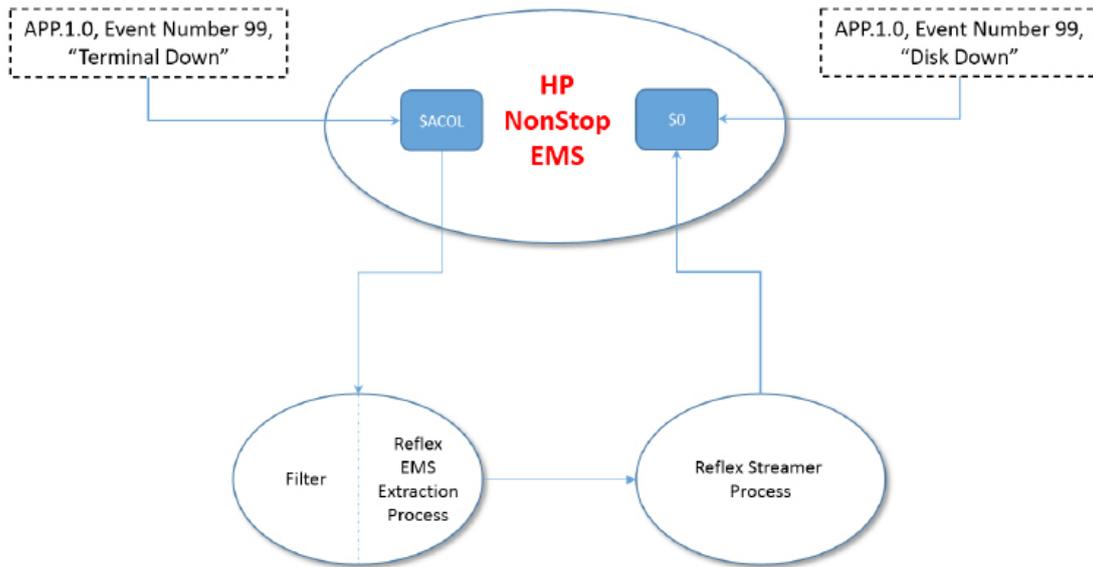
TIMESTAMP: 13:06:07 15-APR-13  NAME:      STRSRV      TYPE: PATHWAY
TERMINAL:   DSHIELDS              SUBTYPE:  SERVER              CLASS: LIST
USER-ID:    DEMO.REFLEX
FACILITY:   TTU
ACTION:     INSERT
TIMESTAMP: 13:25:50 15-APR-13  PROGRAM:   SCFRETRY   PROCESS:  $SCFR
TERMINAL:   DSHIELDS              OBJECT:    $SYSTEM.SYSTEM.TACL
USER-ID:    DEMO.REFLEX           IN-FILE:  $LIVE.RFLXOBJ.SCFRETRY
FACILITY:   RPU                   OUT-FILE:  $$.#SCF

```

EMS EXTRACTION PROCESS

The aim of the EMS Extraction Process is to cater for identical event numbers that log two different scenarios. The extraction layer retrieves the event and performs first level event number conversion; a message is then sent to a Streamer process, which will either translate and create a second unique event, or ignore it.

An example situation would be OSS, which only supports a limited number of possible events via the Syslog mechanism. The extraction process could be used to generate unique event numbers for identical OSS events.



Streamer behaviour when handling events from the EMS Extraction process.

The EMS Extraction process will send log messages to the Streamer process. Streamer will recognise these messages as coming from the EMS Extraction process and process them depending upon the Streamer start-up parameters. The table below details this behaviour.

	Ignore	Resubmit	Neither
Translated log message from the EMS Extraction Process.	A translated EMS event is generated.	A translated EMS event is generated.	An exception EMS event is generated and a log message written to the non^config file.
Non-translated log message from the EMS Extraction Process	The event is ignored. No EMS events are issued & the log message is not written to the non^config file.	The default EMS event is generated.	An exception EMS event is generated and a log message written to the non^config file.
Log messages sent from any other source. i.e. NOT the EMS Extraction process.	An exception EMS event is generated and a log message written to the non^config file.	An exception EMS event is generated and a log message written to the non^config file.	An exception EMS event is generated and a log message written to the non^config file.



The default EMS event is structured as follows:

SSID: INSIDER^50^4

Subject: Eventstreamer

Event No: 2304

Text: will contain the original event text and a suffix of the original SSID and event number. For example a suffix of:

```
"[Resubmitted from 'TANDEM.00143' Event 00009]"
```

An exception EMS event is structured as follows:

SSID: INSIDER^50^4

Subject: Eventstreamer

Event No: 2000

Text: will have a prefix of "Reflex 80:20 : 999 : No streamer record found " and a suffix of the original event text.





Starting the EMS Extraction Process

The EMS Extraction process is used to extract events from an EMS collector and forward them to a Reflex Streamer process. Prior to forwarding the events, the SSID and Event number may be converted so that a different event can be generated.

The EMS Extraction process runs as a NonStop process pair.

To start the EMS Extraction process the following must be entered at a TACL prompt:

```
RUN RFLXOBJ.EMSEXTRA / IN <dataconf file>, NAME <$your choice>, NOWAIT /
COLLECTOR <$ems collector process> STREAMER <$streamer process>
TRANSLATE <Y/N> FILTER <compiled filter file>
```

The **IN** file must be the DATACONF file which provides the file assignments used by Reflex 80:20. This is a **compulsory parameter**.

The **COLLECTOR** process is the EMS Collector process from which we will extract events. This is a **compulsory parameter**.

Note: Specifying \$0 as the EMS Collector is not recommended because doing so will result in events being extracted from \$0 by the EMS Extraction process and potentially being sent back as new messages to \$0 by the Streamer process. This would result in \$0 being flooded with messages.

The **STREAMER** process is the destination for the extracted events. This is a **compulsory parameter** and it is recommended that the High Pin version of Streamer (STREAMHI) be used with the EMS Extraction process.

The **TRANSLATE** value determines if we wish to translate any of the extracted events. Valid values are Y or N, with the default value being N.

The **FILTER** file is a compiled EMS filter to be used to filter EMS events from the EMS Collector.

Translating Events with the EMS Extraction Process

The EMS Extraction process will attempt to translate events if the TRANSLATE startup parameter was supplied with a value of Y or if it was Warmbooted with the TRANSLATE parameter.

To perform the translation, a translation file containing before and after details will be used.

The translation file to be used is defined in the Reflex Admin module under the File Alias tab as EMSTRANS. The default translation file is RFLXDAT.EMSTRANS.

The details specified in the translation file are Event SSID (Event Owner, Value and Version) and the Event number for each event. For example:

Extracted event (Before)				Extracted event (After)			
Owner	Value	Version	EventNumber	Owner	Value	Version	EventNumber
TANDEM	00143	17438	00006	APP	00012	17448	00020

This translation will take the event TANDEM.143.D30 event 6 (i.e. OSS User Alert) and translate it to APP.12.D40 event 20

The Owner, Value and Version of the NonStop subsystems can be found by looking in the relevant subsystem file, e.g. \$SYSTEM.ZSPIDEF.ZOSSTACL, which will show the Owner, Value and Version of OSS (TANDEM.143 17438).



Amending the EMS Translation File

The default EMS translation File - EMSTRANS - can be found in the the database subvolume. This key sequenced file contains the contents of the EMSTRANT tedit file i.e.:

```
INSIDER      0005000000100512FIRST      001230067811111
INSIDER      0005000000500512SECOND  003210087622222
TANDEM       001431743800006TANDEM      000121744800512
```

To amend the translation file follow these TACL commands:

1. VOLUME RFLXDAT
2. FUP
SET LIKE EMSTRANS
CREATE NEWTRANS
EXIT
3. Use TEDIT to create a file containing the Translation records required. The TEDIT file 'EMSTRANT' may be used as a template.

Note: Value, Version and Event Number fields **must** be 0 padded and the owner should have trailing spaces to pad to 8 characters.

4. FUP COPY the tedit file to the NEWTRANS file, i.e.:
FUP COPY <tedit-file>, NEWTRANS
5. Use the REFLEX GUI to Amend the EMSTRANS alias in ADMIN/FILE ALIAS to point to NEWTRANS.
6. Finally, Warmboot the EMS Extraction process via the RFLXCOM utility to force the EMS extraction process into using the new translation file:

```
RUN RFLXCOM  
WARMBOOT EMS_EXTRACT <ems extraction process> TRANSLATE.
```



FILECLNU

On running the SMON Reactions Report 13 (See XRPTMENU Utility), there is a possibility that the following may occur in the report:

1. Poor formatting of the "Map To Status Monitor Object", "S" and "R" fields. This is due to null terminated characters stored in the Action Groups field of the ACTEVE Enscribe file.
2. An error message of "Invalid Data - Run FILECLNU Utility!" in the "Map to Status Monitor Object" field. This is due to invalid characters passed in the "Pass-Manager" field of Watchdog. The "Pass-Manager" for the Action Group will be defaulted to "Subject"

In either case the FILECLNU utility will remove these issues from the respective data files.

Execute the following command at a TACL prompt:

```
RUN RFLXOBJ.FILECLNU / IN RFLXDAT.DATACONF, OUT $$.#FLCLN, NAME $FLCLN /
```

Where DATACONF represents the name of the data configuration file, \$\$.#FLCLN represents the output which will receive the formatted results and RFLXOBJ represents your Reflex 80:20 Object subvolume.





FIMETINS

This utility is designed to allow users to update the File Metrics monitoring database table with configuration information held in an edit input file rather than submitting this same information through the configuration screens. This configuration file could be applied to several Reflex 80:20 databases, thereby reducing the amount of manual configuration required.

To execute this utility, enter the following at a TACL prompt:

```
RUN FIMETINS/IN <edit-configuration-commands>/<OBJECTQ-update-param>, &
<EMS-event-specification>
```

Where:

<edit-configuration-commands> is the edit file that contains NonStop file names that are added into the Reflex 80:20 ACTFIMEQ SQL table. This file must exist and it must be an edit type file, code 101.

The NonStop file name entry has a format of: *<filename>*,*<percent-full>*,*<poll-period>*

<filename> - the file name to be inserted in the ACTFIMEQ database table. The filename should not contain the node name and it should be in the format *<vol>*.*<subvolume>*.*<filename>*

<percent-full> - The Reflex 80:20 monitoring software will emit an EMS event if the file in question exceeds this *<percent-full>* value. Valid values are 0 through 100. If no value is supplied then the default is 80.

<poll-period> - This value represents how often the file metrics for the nominated file are retrieved and analysed. The valid values are:

- D - Daily, i.e. every 24 hours
- T - Every Twelve Hours, i.e. Half-Daily
- H - Hourly
- C - Critical

The default is H.

Example contents of the edit-configuration-commands file:

```
$DEV.RFLXDAT.ACTEVE,95,H
$TEST.ARCH.FILETXFR
$LIVE.MBATDAT.AUDDT,70
$DEV.APPL.ACCOUNTA, ,C
```

<OBJECTQ-update-param>. By default, a HeartBeat File-Metrics entry will always be created in the ACTFIMEQ SQL table. This parameter determines whether an entry will also be created in the 'OBJECTQ' SQL table, which can then be viewed via Overdrive Setup and be used to help build a Status Monitor display. Valid values are Y or N. The default is N.

<EMS-event-specification>. This parameter provides details of the UP, DOWN and VULNERABLE events that must be generated when the file metrics do not meet the configured values.

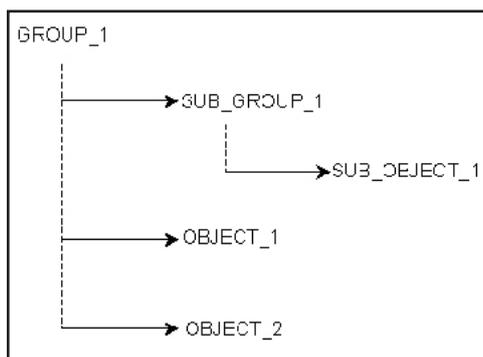
The format of the parameter is: "SSID-Owner.Value.Version.Down-event.Up-event.Vulnerable-event". e.g. INSIDER.51.0.100.200.300

Validation: The value must exist and the separate values must conform to the standard EMS ranges.

FIXNUMOB

Each group that is configured in Reflex Status monitor stores a count of the number of Groups and Objects found in the SQL tables. For example, in this tree structure:

- The number of entries below GROUP_1 would be **3** (Sub_Group_1, Object_1 and Object_2)
- The number of entries below SUB_GROUP_1 is **1** (Sub_Object_1).



These counts of the number of Groups and Objects on the first level below a Group are held in the Reflex SQL database 'GROUP' table row GROUP_NUM_OBJECTS.

The GROUP_NUM_OBJECTS row is used to speed up access through tree levels in Reflex; if the value stored is incorrect then it can lead to several issues, such as:

- The GUI reporting "Unable to find any Groups to list"
- Some objects not appearing in the GUI
- The Reflex Status Monitor Pathway serverclass crashing

To report on these counts and optionally fix any errors, the FIXNUMOB utility has been created.

It is run as follows:

```
RUN FIXNUMOB [update]
```

[update] is an optional parameter. If specified, FIXNUMOB will update all of the GROUP_NUM_OBJECTS counts so that they are correct. It is recommended that 'update' mode is only used when Reflex is shutdown, thereby avoiding any problems such as records being locked.

If the [update] parameter is not specified, then FIXNUMOB will run in 'report' mode and will not perform any updates.



Examples of running the FIXNUMOB utility:

RUN FIXNUMOB

FIXNUMOB utility running in REPORT mode.

```

Counts from counting Group Link Elements:
Count for group: CPUS                ver: S is: 00002
Count for group: CPUS                ver: L is: 00002
Count for group: DISKS               ver: L is: 00017
Count for group: DISKS               ver: S is: 00017
Count for group: FILES               ver: L is: 00002
Count for group: FILES               ver: S is: 00002
Count for group: PATHWAY             ver: P is: 00001
Count for group: PROCS               ver: S is: 00001
Count for group: PROCS               ver: L is: 00001
Count for group: SPOOLERS            ver: L is: 00004
Count for group: SPOOLERS            ver: S is: 00004
Count for group: SUBVOLS              ver: L is: 00003
Count for group: SUBVOLS              ver: S is: 00003
Count for group: TCP/IP              ver: S is: 00005
Count for group: TCP/IP              ver: L is: 00005
Count for group: TEMPORARY TEST      ver: S is: 00001
ACTUAL count for TEMPORARY TEST      ver: S is: 00003
Count for group: X25 LINES            ver: S is: 00001
Count for group: X25 LINES            ver: L is: 00001
Count for group: \ITLTECH.$HDMB      ver: P is: 00003
Count for group: \ITLTECH.$HDMB.PROGRAM ver: P is: 00002
Count for group: \ITLTECH.$HDMB.SERVERCLASS ver: P is: 00018
Count for group: \ITLTECH.$HDMB.TCP  ver: P is: 00001

Groups with counts but NO matching Group Links:
Count for group: COLLECTOR           ver: L is: 00002
Count for group: COLLECTOR           ver: S is: 00002
Count for group: DEVICE               ver: L is: 00002
Count for group: DEVICE               ver: S is: 00002
Count for group: PRINT                ver: L is: 00002
Count for group: PRINT                ver: S is: 00002

Total number of groups is: 00022
Actual number of elements in groups is: 000100
Expected number of elements in groups is: 00098
Total number of unlinked groups: 00006
Total number of groups updated: 00000

```



Description of example output:

The 'Counts from counting Group Link Elements' section details the counts for each individual Group. If the actual value of Group_Num_Objects for a particular Group differs from what the count was found to be, then the problem is listed e.g.

```
Count for group: TEMPORARY TEST ver: S is: 00001
ACTUAL count for TEMPORARY TEST ver: S is: 00003
```

The total of the Group_Num_Objects values and the expected value from totalling the actual count is highlighted in the summary. A difference between these values indicates a problem.

```
Actual number of elements in groups is: 000100
Expected number of elements in groups is: 00098
```

The report also highlights problems caused by Groups that have a non-zero Group_Num_Objects value but nothing in the tree below them, e.g.

```
Groups with counts but NO matching Group Links:
Count for group: COLLECTOR ver: L is: 00002
```

All of these problems are resolved by using FIXNUMOB in update mode. For example:

```
RUN FIXNUMOB UPDATE

FIXNUMOB utility running in UPDATE mode.

Counts from counting Group Link Elements:
Count for group: CPUS                ver: S is: 00002
Count for group: CPUS                ver: L is: 00002
Count for group: DISKS               ver: L is: 00017
Count for group: DISKS               ver: S is: 00017
Count for group: FILES               ver: L is: 00002
Count for group: FILES               ver: S is: 00002
Count for group: PATHWAY              ver: P is: 00001
Count for group: PROCS               ver: S is: 00001
Count for group: PROCS               ver: L is: 00001
Count for group: SPOOLERS            ver: L is: 00004
Count for group: SPOOLERS            ver: S is: 00004
Count for group: SUBVOLS              ver: L is: 00003
Count for group: SUBVOLS              ver: S is: 00003
Count for group: TCP/IP              ver: S is: 00005
Count for group: TCP/IP              ver: L is: 00005
Count for group: TEMPORARY TEST      ver: S is: 00001
Count for group: X25 LINES            ver: S is: 00001
Count for group: X25 LINES            ver: L is: 00001
Count for group: \ITLTECH.$HDMB      ver: P is: 00003
Count for group: \ITLTECH.$HDMB.PROGRAM ver: P is: 00002
Count for group: \ITLTECH.$HDMB.SERVERCLASS ver: P is: 00018
Count for group: \ITLTECH.$HDMB.TCP  ver: P is: 00001

Total number of groups is: 00022
Actual number of elements in groups is: 000098
Expected number of elements in groups is: 00098
Total number of unlinked groups: 00000
Total number of groups updated: 00007
```



FIXSBJH

The FIXSBJH utility provides the ability to run an integrity check against the Subject History and Subject History Control tables that store history about the events that have been processed for each object configured in Reflex. In addition, the utility can be used to re-size the amount of history that can be stored for each object.

Note: During SQL compilation of the utility, several warnings with code 4058 and 4060 will be produced. These warnings can be ignored since they are referring to SQL tables that are created dynamically whilst the utility is running.

Also note that during processing, EMS events regarding dynamic SQL re-compilation with error 8210 will be produced. These can be ignored since they are just indicating that the utility is being re-compiled after the temporary tables have been dynamically created.

The command syntax for the utility is:

```
RUN FIXSBJH / IN <DATACONF> / [MAX-HISTORY] <max-history> [SUBVOLUME] <subvol>
```

Where:

<**DATACONF**> is the DATACONF file for the nominated Reflex environment. It is used to find the location of the PARACONF file. This value is mandatory.

[**MAX-HISTORY**] is an optional parameter used to specify the maximum number of history records <**max-history**> that can be stored per object. If no value is specified then SUBJECT-HISTORY-SIZE from Paraconf will be used. The supplied value must be in the range 1 to 1000.

[**SUBVOLUME**] is an optional parameter used to specify a subvolume <**subvol**> where an archive file containing any deleted History will be stored. The filename is in the format SMddmmyy.

Performing an integrity check

An integrity check can be performed by running the utility without specifying a value for the MAX-HISTORY parameter. A SUBVOLUME may optionally be supplied. For example:

```
RUN FIXSBJH / IN <DATACONF> /
```

In this situation the utility will perform a check based upon the current Reflex SUBJECT-HISTORY-SIZE parameter value.

If any problems are found they will be reported to the home terminal, e.g. :

```
00014 objects in the Subject History Table HAVE more than 00025 entries.
Action required.
```

```
00014 objects in the Subject Control Table HAVE more than 00025 entries.
Action required.
```

At this point, if any problems need to be fixed then a prompt will be issued, e.g. :

```
Do you want to fix the problems? (Y/N):
```

Note: Reflex MUST be closed to perform any changes. If Reflex is currently running the following message will be displayed:

```
Reflex environment <Reflex Pathmon process> is still running.
Please stop Reflex and re-run FIXSBJH to fix the problems.
```



If any redundant history is found, for example if the SUBJECT-HISTORY-SIZE is set to 30 but a particular object has 50 rows of history, then the 20 oldest history rows will be archived. The filename of the archive file will be in the form SMddmmyy.

The location of the archive file will either be the location specified using the SUBVOLUME parameter or the default location of the current subvolume. Note that the utility will display the name of the archive file that has been used, for example:

```
Creating archive file \ITLTECH.$DEV.RFOB047.SM201206
```

Details of all the objects who have their history amended is displayed on the home terminal, e.g. :

```
Fixing history for object: \ITLTECH.CPU00
```

Re-sizing the amount of history stored per object:

The amount of history stored can be amended by running the utility with a value for the MAX-HISTORY parameter. The MAX-HISTORY value must be in the range 1 to 1000 and it may be larger or smaller than the previous value. A SUBVOLUME may optionally be supplied. For example:

```
RUN FIXSBJH / IN <DATACONF> / MAX-HISTORY 50
```

In this situation the utility will perform any required updates necessary to set the amount of history that can be stored per object to 50. The following message will be displayed:

```
The SUBJECT-HISTORY-SIZE of <previous value>, from Paraconf and the
supplied MAX-HISTORY differ. The MAX-HISTORY value of 0050 will be used.
```

As with the Integrity check, any problems that need an action will be displayed, e.g. :

```
00010 objects found using serial numbers that have wrapped around.
Action required.
```

At this point if any problems need to be fixed then a prompt will be issued, e.g. :

```
Do you want to fix the problems? (Y/N):
```

Note: Reflex MUST be closed to perform any changes. If Reflex is currently running the following message will be displayed:

```
Reflex environment <Reflex Pathmon process> is still running.
Please stop Reflex and re-run FIXSBJH to fix the problems.
```

If any redundant history is found, for example, if the SUBJECT-HISTORY-SIZE was set to 60 and a particular object had 60 rows of history that now need to be reduced to 50, the 10 oldest history rows will be archived.

The filename of the archive file will be in the form SMddmmyy. The location of the archive file will either be the location specified using the SUBVOLUME parameter or the default location of the current subvolume. Note that the utility will display the name of the archive file that has been used, for example:

```
Creating archive file \ITLTECH.$DEV.RFOB047.SM201213
```

Details of all the objects who have their history amended is displayed on the home terminal, e.g. :

```
Fixing history for object: \ITLTECH.CPU00
```

When the amount of history is being re-sized, the Reflex SUBJECT-HISTORY-SIZE parameter value is updated with the new value supplied via the MAX-HISTORY parameter.

```
Updating the PARACONF SUBJECT-HISTORY-SIZE record.
```



Clean-up

Note that whatever mode the utility is used in, all temporary tables will be removed after they have been used.

In addition, if no history needed to be archived then the archive file will also be purged. The utility will issue messages for these actions, e.g. :

```
Purging the archive file \ITLTECH.$DEV.RFOB047.SM201213 since no history
needed to be archived.
```

```
Dropping temporary SQL table, SBJTEMP
```

```
Dropping temporary SQL table, HISTTEMP
```

Free up Slack Space

Any slack space left in the Subject History table (SBJHISTQ) following deletions by FIXSBJH, can be freed up by running a FUP RELOAD command, e.g.:

```
FUP RELOAD RFLXDAT.SBJHISTQ
```

Archived history

If history was archived, an indication of the amount of history that has been archived will be displayed, e.g. :

```
00081 history records have been archived to \ITLTECH.$LIVE.RFLXDAT.SM201213
```

The archived history can be viewed using ENABLE as described in the "Using Enable to view Archived files" section.



FMIMEX

This utility is designed to reduce the amount of configuration carried out via the Reflex 80:20 GUI.

It will allow selected entries in the Heartbeat File Metrics database to be imported/exported between multiple Reflex environments. In addition, entries can also be translated at export time to substitute volume and subvolume names with those of a different environment.

The use of this utility will allow File Metrics entries to be moved to another Reflex 80:20 database without the need to re-key the details.

To execute this utility, enter the following at a TACL prompt:

```
RUN RFLXOBJ.FMIMEX / IN RFLXDAT.DATACONF, OUT <spooler> / <operation> <Edit file>,
TRANSIT <filename> [, RESET] [IGNORE|INSERT]
```

Where:

RFLXDAT.DATACONF is the location of the Reflex 80:20 DATACONF file

<spooler> is a valid spooler location where output will be directed e.g. \$S.#FM

Valid values for the **<operation>** parameter are :

EXPORT is used to extract File Metrics records from the Reflex database to a transit file.

IMPORT is used to read records in a transit file and import them into a File_Metrics SQL table in a Reflex database.

HELP is used to display Help text.

<edit file> is the name of an edit file detailing a list of files to export and any translation rules to apply. This is an optional parameter.

<filename> is the name of the transit file used to hold File Metrics information that has been exported or is to be imported.

RESET is an optional parameter that if specified will erase previous data from the transit file before commencing to export.

INSERT is an optional parameter, which if specified, will add entries to the SQL Object table for all files that are imported. In the situation where the addition of an object entry results in a duplicate row error, the whole transaction is aborted and all changes are backed out. This option is only applicable for imports.

IGNORE is an optional parameter which if specified will perform the same functionality as the INSERT option but if a duplicate row is found the error is ignored and the transaction will continue. This option is only applicable for imports.

Note: When extracting File_Metrics entries from a table, the edit file, if supplied, is used to determine which filenames to export and any translation rules to apply.

This **edit file** will have the same fixed format rules as the RFDEFS file where fields should start at particular column positions, i.e. first field at column 1, second field at column 9 and third field at column 17.

A line in this edit file will start with one of the keywords *VOLUME*, *SUBVOL*, *FILE* or *WILDCARD*.

The second and third fields for the *VOLUME* and *SUBVOL* keywords will be FROM and TO fields used as translation rules.



When using the keyword of *FILE* or *WILDCARD*, an entry is required in the second field (column 9) that will be the name of a file to export or a wildcard template.

When using a wildcard template only entries that match the template will be exported. For example a wildcard of \$DEV.* means export any file with a volume of \$DEV.

Note: Subvolume entries in the File Metrics database can be exported using the standard FILE keyword. For example a FILE of \$DEV.SUBVOLA.* means export a subvolume entry of \$DEV.SUBVOLA.*.

If no *VOLUME* or *SUBVOL* records exist then there is no translation to carry out. If no *FILE* or *WILDCARD* records exist then all File Metrics records will be exported.

If the edit file parameter is not supplied then all filenames will be exported with no translations.

Column	Column	Column	17
1	9		
↓	↓	↓	
VOLUME	\$DEV	\$D	
SUBVOL	SUBVOLA	SUBVOLB	
FILE	\$DEV.SUBVOL.	FILE	
FILE	\$DEV.SUBVOLC.	*	
WILDCARD	\$DEV.*		

When processing the above example the following actions will take place:

- Translate the volume \$DEV to \$D during export.
- Translate the subvolume SUBVOLA to SUBVOLB during export.
- Export the File Metrics record for the file entry \$DEV.SUBVOL.FILE.
- Export the File Metrics record for the subvolume entry \$DEV.SUBVOLC.*.
- Export all file metrics records where the file/subvolume starts with \$DEV.

The fields will be validated and if validation fails the utility will display an error message indicating the text and line number where the error occurred and stop.

A limit of 10 volumes and 10 subvolumes to use as the translation rules can be specified in the edit file.



GATEWAY STREAMER

The Gateway Streamer process takes the place of the application log and uses the translation rules built in the Gateway Module to translate log messages written to it, into EMS events.

Any log message that the Streamer Process does not recognise will result in an EMS event being generated which gives the details of the text. These records can also be written to a non^config file which can be used in a later Streamer session. The Streamer process runs as a NonStop process pair. The process can also act as a home terminal for your application, processing COBOL library errors and handling INSPECT and DEBUG prompts.

If a DEBUG prompt is detected, the trapped program is stopped. If an INSPECT prompt is detected then a SAVEABEND file is created and the trapped program is stopped. In both cases an EMS event is generated giving details of the trap.

To start the Streamer Process the following must be entered at a TACL prompt:

```
RUN RFLXOBJ.STREAM / NAME $<process id>, CPU<n>...IN <config>, &
OUT <collector> / BACKUP^CPU <n>, NON^CONFIG <filename>, &
DATACONF <dataconf-file> [, IGNORE | RESUBMIT]
```

The **IN** file is the Streamer configuration file created via the Gateway Process Editor tabbed view.

The **OUT** <collector> run option may be specified, if desired, to send events to an alternate collector - rather than \$0 - which is used by default.

The **BACKUP^CPU** value is the target CPU for the backup process of the Streamer Process. The process will **always** run as a NonStop process pair. The default value is "highest available CPU" which is also adopted if the BACKUP^CPU value is invalid.

The **NON^CONFIG** file is the destination for any records which the Streamer has no translation rule for. It must be Entry Sequenced and 255 bytes long; if this is not the case then the Streamer abends and an appropriate EMS diagnostic is produced. If the file does not exist then one is created. The default condition is that no mismatched records are dumped to the NON^CONFIG file.

The **DATACONF** file contains the file assignments required by Reflex 80:20 - this is a **compulsory parameter**.

If **BACKUP^CPU** and **NON^CONFIG** are defaulted, then the parameter string must be:

```
" , , DATACONF <dataconf-file>".
```

The parameters are in fixed positions. If the **BACKUP^CPU** parameter is defaulted then the parameter string must be:

```
" , NON^CONFIG <filename>, DATACONF <dataconf-file>".
```

IGNORE and **RESUBMIT** are optional parameters that are used in conjunction with the EMS Extraction process.

If both RESUBMIT and IGNORE are specified then the first parameter entered will be used, for example, " **IGNORE, RESUBMIT**" would result in **IGNORE** being used.

A high-pin version of the streamer object is available. It can be found in the RFLXOBJ subvolume and is named **STREAMHI**. Both versions operate in the same way.



Gateway Streamer Utilities

The Gateway Streamer module comes supplied with two useful utilities:

- PRINTCNF
- REMUPRT

PRINTCNF

This utility may be used to generate a formatted print of a specified streamer configuration file. To execute this utility, enter the following at a TAACL prompt:

```
RUN RFLXOBJ.PRINTCNF / IN RFLXDAT.DEMOCONF, OUT $S.#CONFIG /
```

where DEMOCONF represents the name of the Streamer configuration file and \$S.#CONFIG represents the output which will receive the formatted printout.

REMUPRT

If the log file that is loaded into the user interface for conversion contains unprintable characters, then the results of the user interface will be unpredictable. This will affect the Create Streamer and List, Amend, Delete Streamer dialogs.

This utility may be used to remove unprintable characters from the LOG file. Execute the following steps at a TAACL prompt:

```
ASSIGN OLDLOG, <existing-log-file>
ASSIGN NEWLOG, <newly-created-log-file>
RUN RFLXOBJ.REMUPRT
```

Any unprintable characters will be converted to a ? character and the new log record written to NEWLOG.

Additional Gateway Streamer administration functions are available via the **RFLXCOM** utility.



HBIMEX

Reflex 80:20 Heartbeat Process Import / Export utility.

This utility is designed to reduce the amount of configuration carried out in the Reflex 80:20 GUI. It will allow for the Heartbeat – Process Monitoring - database to be updated with new Heartbeat processes, or where selected Heartbeat processes can be copied to another Reflex 80:20 database without the need to re-key the details.

To execute this utility, enter the following at a TACL prompt:

```
RUN RFLXOBJ.HBIMEX / IN RFLXDAT.DATACONF, OUT $S / <operation> [<config file>] ,
[TRANSIT <filename>] [RESET] INSERT / IGNORE]
```

Where:

RFLXDAT.DATACONF is the name of the Reflex 80:20 DATACONF database that contains the location of the Heartbeat process file, ACTPROC.

The available **<operation>** values are:

EXPORT - Export processes from the Reflex 80:20 database into a Transit file.

IMPORT - Import processes from the Transit file into a Reflex 80:20 database.

HELP - Displays a summary of the command syntax.

<configfile> Edit file containing names of processes to be exported. The process names need to be entered on separate lines, e.g.:

```
$TEST
$PROC
$ARCH
```

Combination of process names with or without node prefixes can also be specified, e.g.:

```
\LIVE.$ARCH
$PROC
\TEST.$ARCH
```

<filename> - TRANSIT file to hold the data, e.g. TRANSIT **RFLXDAT.TRANSHB**.

'Export' notes:

1) Node prefixes are optional for 'local' processes. If a node prefix is not specified, then HBIMEX will attempt to Export the process or processes configured in the local node, i.e. if HBIMEX is running in the node \DEV, then in the example above, HBIMEX would Export \DEV.\$PROC. If a 'remote' node process needs to be exported, then its node must be specified as in the above example, e.g. \TEST.\$ARCH.

2) If the specified TRANSIT file does not exist, then one will be created automatically with a REC Length of 346 and type Entry Sequenced. A file name **must** be specified, even if it does not exist.

3) Check Spooler for results.

Descriptions for the remaining parameters - [RESET] INSERT / IGNORE] - are continued on the next page.



RESET - If specified, will erase previous data from the TRANSIT file before exporting processes.

INSERT - If specified, this option will add entries to the 'OBJECTQ' SQL table for all processes that are imported. In the situation where the addition of an object entry results in a duplicate row error, the whole transaction is aborted and all changes are backed out. This option is only available for imports.

IGNORE - This option performs the same functionality as the INSERT option but if a duplicate 'OBJECTQ' SQL row is found, then the error is ignored and the transaction will continue. This option is only available for imports.

'Import' notes:

1) The Import option for HBIMEX does not make use of a <configfile>. All contents of the transit file are selected for import.

2) When importing Heartbeat processes into a new database, the RFDEFS file in the destination database subvolume must contain 'Old' and 'New' node names. For example, if you have exported processes from node **\TEST** and you wish to import them into node **\LIVE**, then the RFLXDAT.RFDEFS file on node **\LIVE** should look like the following:

```
NODE      \TEST  \LIVE
```

3) The first node name **must** start in column 9; the second node name **must** start in column 17.

4) Check Spooler output for all Import results.

5) After importing processes into ACTPROC and if required, the SQL 'OBJECTQ' table, reminder messages will be issued after the end of the transaction to warmboot the appropriate servers and refresh the GUI views to see the changes.

6) Various conditions can exist which will cause the Import to either skip or backout the transaction. See spooler and hometerm for results. Examples provided below:

6.1) Process already exists in ACTPROC Enscribe file and SQL OBJECTQ table. The INSERT option has not been specified. Spooler results show:

```
ACTPROC   : Process \LIVE$ARCH already exists.
Skipping import of: \LIVE$ARCH
```

6.2) Process already exists in ACTPROC Enscribe file and OBJECTQ SQL table. The INSERT option has been specified. Spooler results show:

```
ACTPROC   : Process \LIVE$ARCH already exists.
Skipping import of: \LIVE$ARCH
```

6.3) Process does not exist in the ACTPROC Enscribe file but does exist in the OBJECTQ SQL table. The INSERT option has not been specified. Spooler results show:

```
Process Details: \TEST$PROC successfully added to ACTPROC
ACTPROC   : Record found and imported successfully
```



6.4) Process does not exist in ACTPROC Enscribe file but does exist in the OBJECTQ SQL table.

The INSERT option has been specified. Spooler results show:

```
Process Details: \LIVE$PROC successfully added to ACTPROC
SQL Error : -08227 on insert of \LIVE$PROC to OBJECT table
Object row already exists for process \LIVE$PROC
Aborting import of: \LIVE$PROC
```

The hometerm will also display the following:

```
ACTPROC records successfully imported
Transit file used: <Transit filename>
Some updates were backed out due to SQL errors such as duplicate entries.
Review the report sent to the OUTPUT destination.
GUI views should be refreshed to see the revised process monitoring list.
Warmboot the Reaction Servers to activate the changes.
```

In the above example, the whole transaction has been backed out, resulting in the ACTPROC entry being removed.

6.5) Process does not exist in the ACTPROC Enscribe file but does exist in the OBJECTQ SQL table. The **IGNORE** option has been specified. Spooler results show:

```
Process Details: \LIVE$PROC successfully added to ACTPROC
SQL Error : -08227 on insert of \LIVE$PROC to OBJECT table
Object row already exists for process \LIVE$PROC
Ignoring SQL update error for \LIVE$PROC
```

The hometerm will also display the following:

```
ACTPROC records successfully imported
Transit file used: <Transit filename>
Some SQL errors occurred but they were IGNORED.
Review the report sent to the OUTPUT destination.
GUI views should be refreshed to see the revised process monitoring list.
Warmboot the Reaction Servers to activate the changes.
```

6.6) A process is to be imported into the ACTPROC and OBJECT SQL table on node \LIVE but the exported process's node (\DEV) is no longer accessible on the network.

The \LIVE RFLXDAT.RFDEFS file also does not contain an 'Old' node reference for this process (\DEV), meaning that it will not be converted from \DEV.\$AAAA to \LIVE.\$AAAA. The INSERT option has been specified.

```
ERROR - Remote node \DEV is not accessible and has no RFDEFS translation.
Skipping import of: \DEV $AAAA
```



RFADDUSR

Users can logon to the Reflex GUI via the use of a Guardian group.user id, or a Guardian alias name, e.g. demo.reflex, or demorflx respectively. However, when logging on with an alias name, the associated group.user id is only allowed to be configured via the Reflex GUI – an alias name cannot be configured within the Reflex GUI, only the corresponding group.user id.

Note: The user id's password is not stored in Reflex. Reflex will check the user id and associated password via the HPE NonStop Safeguard facility.

Once logged on, then access to the various GUI facilities is controlled by a Security Profile. This Security Profile is a combination of the Guardian group.user id and a Security Class (the Class determines which GUI facilities this user can use).

When the Reflex 80:20 NonStop software is first installed, the database Security Profile file, e.g. RFLXDAT.SECPROFL is empty. The database Security Class file, e.g. RFLXDAT.SECCLASS is supplied with a default Class name of ALLFACIL.

This RFADDUSR utility adds an initial Guardian group.user name into SECPROFL and associates this user with the default permissions defined in the Security Class (SECCLASS) file. Once successfully completed, the user can then logon to the Reflex GUI via the original group.user name, or an associated alias name logon.

The syntax is:

```
VOLUME <Reflex Object subvolume>, e.g. RFLXOBJ  
RUN RFADDUSR / IN <Reflex Database>.DATACONF / <USER-ID>, ALLFACIL
```

Where:

<USER-ID> must be an existing Guardian user id, not a Safeguard alias, in the format group.user name.

ALLFACIL is a supplied Security Class stored in the Reflex database SECCLASS file.

For example:

```
RUN RFADDUSR / IN RFLXDAT.DATACONF / demo.reflex, ALLFACIL
```

If no parameters are supplied, i.e. only RUN RFADDUSR is executed, then a Help page is displayed.

Note: The Reflex database SECPROFL file must be empty otherwise it will fail with an error message. All diagnostics are written to the home terminal.

If the validation is successful then RFADDUSR will:

Create a SECPROFL record for user <USER-ID>, associated with Security Class "ALLFACIL"

Create an audit summary and detail record for Security Class facility "ADU".

Write a summary message to the screen; e.g. "User <USER-ID> created for security class ALLFACIL".



RFIMEX

Reflex 80:20 Import / Export Enscribe

The RFIMEX utility enables Enscribe data (EMS events configured in Reflex) to be 'imported' into or 'exported' from different Reflex event databases, i.e. copy EMS event configurations (Action Groups) between 'test' and 'live' environments without the need to duplicate the effort required.

Note: When inserting events into a 'new' database, the RFDEFS file in the destination database subvolume (RFLXDAT) must contain 'old' and 'new' node prefixes. For example, if you have EXPORTED EMS events from node \A and you wish to IMPORT them into node \B, then the RFDEFS file on node \B should look like:

```
NODE      \A      \B
```

Reflex 80:20 must not be running when using this utility except when the report option is being used.

The RFIMEX utility is run by entering the following at the TAFL prompt:

```
RUN RFLXOBJ.RFIMEX /IN RFLXDAT.DATACONF,OUT $$.#LOC/<operation> <params>
[TRANSIT <transit file>] [RESET]
```

The operations available are:

EXPORT	Export events from database.
IMPORT	Import events into database.
REPORT	Report about the events in the transit file.
HELP	Displays a summary of the command syntax.

The params could be

```
<owner>.<value>.<event number>
```

The Owner, Value or Event number may be replaced by a wildcard *.

TRANSIT <transit-file> is the location of the file that will hold the data imported or exported from the Reflex 80:20 structured files. If omitted, the location of DATACONF is used with a filename of TRANSIT.

The RESET option is used to erase the previous data from the transit file before exporting.

The following are five examples of how to use the **RFIMEX** utility:

- Export All Events to a TRANSIT file


```
RUN RFLXOBJ.RFIMEX / IN RFLXDAT.DATACONF,OUT $$.#LOC / EXPORT
*.*.* TRANSIT $DATA02.RFLXDAT.TRANSIT
```
- Import all Expand events within Transit file TRANSEXP


```
RUN RFLXOBJ.RFIMEX / IN RFLXDAT.DATACONF,OUT $$.#LOC / IMPORT
*.*.* TRANSIT $DATA02.RFLXDAT.TRANSEXP
```
- Exporting specific events, e.g. all TANDEM.PATHWAY events


```
RUN RFLXOBJ.RFIMEX / IN RFLXDAT.DATACONF,OUT $$.#LOC / EXPORT
TANDEM.*.* TRANSIT $DATA02.RFLXDAT.TRANSPAT
```
- Importing specific events, e.g. ACI events


```
RUN RFLXOBJ.RFIMEX / IN RFLXDAT.DATACONF,OUT $$.#LOC / IMPORT
ACI.*.* TRANSIT $DATA02.RFLXDAT.TRANSACI
```



- Reporting All Events in the Transit File

```
RUN RFLXOBJ.RFIMEX / IN RFLXDAT.DATACONF, OUT $$.#LOC / REPORT
*.*.* TRANSIT $DATA02.TRANSIT.TRANNBAT
```

Note: The output file is optionally placed in the spooler. This contains a report of the operations carried out by RFIMEX.

A series of transit files are supplied within your Reflex 80:20 database subvolume, the contents of which can be imported into the Reflex 80:20 database.

A list of transit files are provided in a table on the next page.

The 'Status Monitor Attributes' column shows how the various events contained with each transit file are mapped to Status Monitor icons.

For example:

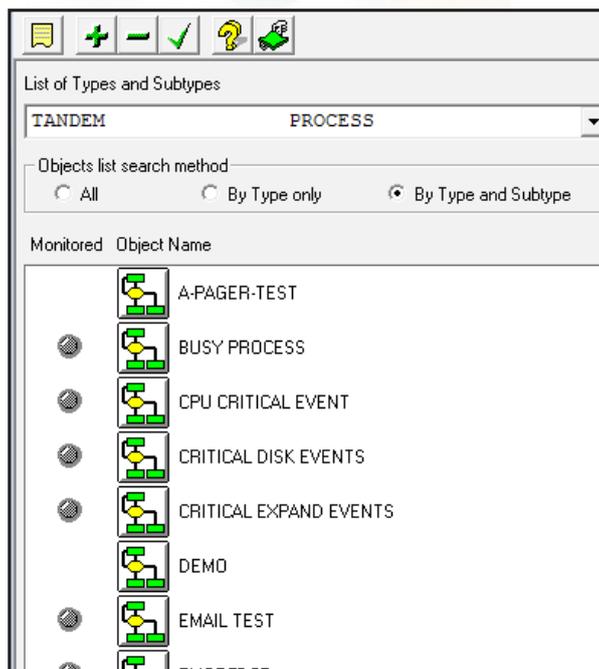
TRANEMGR transit file contains Reflex Enterprise Manager alert events which are forwarded to an icon called EMGRFDCP. This icon needs to be configured in Overdrive Setup in order to receive these events.

TRANNBAT transit file contains NetBatch events which will utilise NetBatch jobs names (~nbjobname~) for forwarding to an equivalent NetBatch named icon in Status Monitor.

TRANSMB transit file contains MultiBatch events which will utilise BMON Manager process (~man16~) and the MultiBatch Step Name (~subject~) for forwarding to an autodiscovered MultiBatch Step icon in Status Monitor. Other generic MultiBatch events can be forwarded to an icon called MULTIBAT VULN, which also needs to be configured in Status Monitor.

Suitable Icons for generic Format String icons, such as EMGRFDCP, MULTIBAT VULN.

Where events are mapped to generic icons, then it is recommended that an object type_subtype of TANDEM_PROCESS is utilised, e.g.:





Reflex TRANSIT files

Transit file	SSID	Description	Status Monitor Attributes(s)
TRANBBOX	ETINET.1	ETINET BackBox	(1) Format String: WARNING EVENTS (2) Format String: DOWN EVENTS
TRANCACT	INSIDER.50	Disk Cache	Subject
TRANCPUT	INSIDER.50	CPU	Subject
TRANDIO	INSIDER.50	Disk I/O	Subject
TRANEMGR	INSIDER.50	Enterprise Manager	Format String: EMGRFDCP
TRANMHS	TANDEM.45	MHS	~procdesc~.~mhs~.~subject~
TRANMMON	ITLTASK.4	Mount-Monitor	Format String: MOUNTMON.
TRANNBAT	TANDEM.9	NetBatch	~nbjobname~
TRANPING	INSIDER.50	Reflex PING	Format String: REFLEX WORKSTATION
TRANPWYM	INSIDER.50	Pathway monitoring utility	~manager~.~subject~
TRANSACI	ACI.328	ACI BASE24	(1) P1A^GATE.~subject~ (2) P1B^GATE.~subject~
TRANSAFE	SAFECOM.1	SAFEGUARD	Format String: SAFEGUARD
TRANSASY	TANDEM.12	Async terminal	Subject
TRANSCLK	TANDEM.66	CLOCK events	Format String: SYSCLOCK
TRANSCPU	TANDEM.15	CPU events	Format String: CPU CRITICAL EVENTS
TRANSDSH	INSIDER.50	Dash-Metrics events	Subject
TRANSDSK	TANDEM.31	Disk events	(1) ~procdesc~ (2) Format String: CRITICAL DISK EVENTS
TRANSENV	TANDEM.238	Envoy events	Subject
TRANSETI	INSIDER.6	MultiBatch Event-Timer events	(1) ~man16~.~subject~ (2) Format String: EVENT-TIMER ALERTS



Transit file	SSID	Description	Status Monitor Attributes(s)
TRANSEXP	TANDEM.30	Expand events	Format String: CRITICAL EXPAND EVENTS
TRANSFSP	TANDEM.240	Fast Spooler	Subject
TRANSIPC	TANDEM.203	Kernel OS Message System	Format String: CPU CRITICAL EVENT
TRANSJS	INSIDER.51	JOBLOTS monitoring utility events	Subject
TRANSKMS	TANDEM.183	KMSF events	Format String:KMSF SWAPFILES PROBLEM
TRANSLAN	TANDEM.19	LAN events	Subject
TRANLSA	TANDEM.192	ServerNet LAN System	Subject
TRANSMB	MULTIBAT.1	MultiBatch events	(1) ~man16~.~subject~ (2) Format String: MULTIBAT VULN
TRANSMEM	INSIDER.50	Heap and PFS alerting events.	Format String: HEAP-USE-INCREASING PFS-USE-INCREASING
TRANSMF	TANDEM.168	SMF events	Subject
TRANSMQ	IBM.99	WebSphere MQ	~mq-qmgr~.~mq-channelname~ ~mq-qmgr~ ~mq-qmgr~.~mq-qname~
TRANSNSC	TANDEM.204	NSC	Subject
TRANSOMF	TANDEM.127	OMF events	Subject
TRANSOSM	TANDEM.250	OSM events	Format String: HPE OSM EVENTS
TRANSOSS	TANDEM.143	OSS events	Format String: OSS ALERTS
TRANSPAT	TANDEM.8	Pathway events	~manager~.~subject~
TRANSPO	TANDEM.57	Spooler error events	Subject
TRANSRDF	INSIDER.1	RDF monitoring utility events	Format String: RDFAGENT



Reflex TRANSIT files

Transit file	SSID	Description	Status Monitor Attributes(s)
TRANSSPL	INSIDER.50	AGENT-SPOOLER events	Subject
TRANSSTO	TANDEM.189	Storage events	Subject
TRANSTAP	TANDEM.4	Tape events	Subject
TRANSTCP	INSIDER.50	TCP/IP events	Subject
TRANSTIM	TANDEM.273 TANDEM.66	Time Sync, Clock sync events	Format String: TIMESYNC
TRANSTIV	TIVOLI.1	TIVOLI	Remote Alert
TRANSTMF	TANDEM.10	TMF events	Format String: (1) TMF CRITICAL EVENTS (2) TMF DOWN EVENTS (3) TMF VULN EVENTS
TRANTMFA	INSIDER.200	TMF monitoring utility events	Subject
TRANSTSK	Not applicable	Contains Tasks for importing via the TASKIMEX utility	Not applicable
TRANSVHS	TANDEM.138	VHS	Subject
TRANSWAN	TANDEM.176	WAN	Subject
TRANTFDS	TANDEM.151	TFDS (DMP)	Format String: TFDS SWITCH
TRANX25T	INSIDER.50	X.25 monitoring events	Subject
TRNTHRS	INSIDER.50	Action Group Threshold events	Format String: ACTION GROUP THRESHOLD



RFIMEX - Import and configuration of NetBatch events

The RFIMEX Transit file - TRANNBAT - contains a sample of NetBatch EMS events which can be imported into the Reflex database.

The range of NetBatch EMS events contained within the 'TRANNBAT' transit file are:

```
TANDEM.9.102
TANDEM.9.202
TANDEM.9.203
TANDEM.9.204
TANDEM.9.301
```

When these are imported into the Reflex database via RFIMEX, the following Action Group entries will automatically be configured:

```
NETBATCH-JOB-START
NETBATCH-JOB-NORMAL-STOP
NETBATCH-JOB-ABNORM-STOP
NETBATCH-JOB-OVER-LIMIT
NETBATCH-JOB-START-ERROR
```

To ensure the Reflex Event-Monitor process is monitoring these NetBatch EMS events, execute all three steps via the Reaction Module red exclamation mark "Warmboot the Modified Servers" .

Note: There is no auto-discovery module to populate the Reflex object database. Therefore, individual objects need to be configured in the Reflex SQL object database, via the 'OD Setup' module.

An example is provided below on how to configure a Status Monitor object in OD Setup for a NetBatch job called DISKS-ADMIN.

Batchcom status

```
1} S *
NETBATCH SERVER - T9190D30 - (29JUN2005-ADH) Time: 20SEP05 14:34:49
JOB STATUS
JOB  JOBNAME                USERID  LOG  STATE        CLASSNAME
-----
285  DISKS-ADMIN             255,255  440  21SEP06      SYSADMIN
```

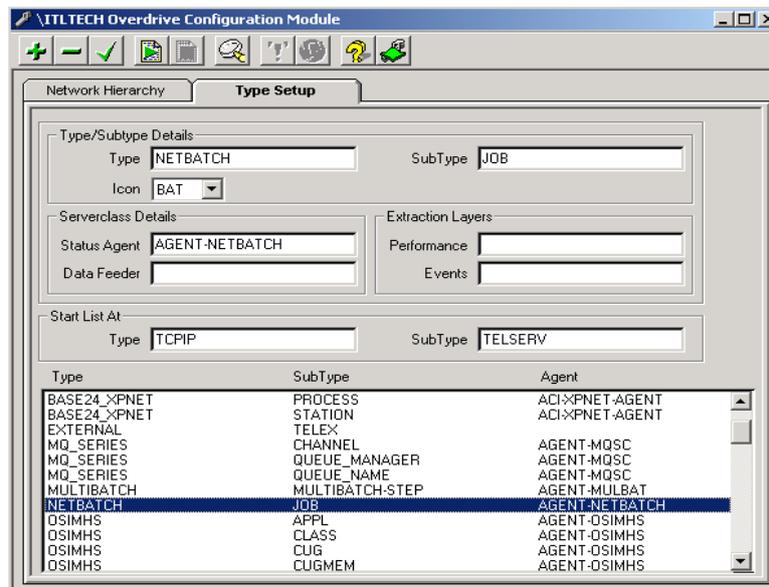
NetBatch Object configuration

The Status Monitor object for the NetBatch job - DISKS-ADMIN - now needs to be configured in OD Setup. See instructions on the following page.

NetBatch Type / Subtype

Before a NetBatch object can be configured in OD Setup, ensure a Type / Subtype for NETBATCH JOB exists, or is setup.

Via the Reflex 80:20 GUI, drop-down 'Monitor' menu, select the "Type/Subtype Setup" window to provide the following display.



Ensure Type / Subtype Details for NETBATCH JOB respectively is configured, utilising the Reflex Status Agent: "AGENT-NETBATCH".

OD Setup Object Configuration

Using the OD Setup Module, add a user-defined NETBATCH JOB object via the "Status Monitor Setup - Objects List" window.

In the "Objects Detail Dialog", ensure the following is set:

Manager Node and **Process** is specified, e.g. \ITLTECH \$ZBAT
(Where \$ZBAT is the NetBatch Manager Process)

List of Types and **Subtypes** is selected for NETBATCH JOB

Initial Status is set to UP

Add this object into the Object database and drag and drop into an appropriate Status Monitor tree structure.



RFIMEXQ

Reflex 80:20 Import/Export SQL Tables

The RFIMEXQ utility enables data from Reflex 80:20 SQL tables to be managed as follows:

- Export data from SQL tables into an entry-sequenced file.
- Transfer data from an entry-sequenced file into SQL tables.
- Read data from an unstructured file into SQL tables.

This utility allows data to be transferred between different Reflex 80:20 SQL databases, e.g. between the Test and Live environments.

Reflex 80:20 must not be running when using this utility.

The RFIMEXQ utility is run by entering the following at the TACL prompt:

```
RUN RFLXOBJ.RFIMEXQ / IN RFLXDAT.DATACONF,OUT $$.#RFIMQ / <operations>
<table-params> [params] TRANSIT <transit file> [SEPARATE]
```

The <operations> options are:

EXPORT - Transfers data from the defines tables to the transit file in the current subvolume.

IMPORT - Transfers data to the currently defined tables from the transit.

HELP - Displays a summary of the command syntax.

The <tables-params> options are:

STATUS-MONITOR - If used with the TYPICAL parameter then the following tables will be imported / exported: Group Table, Group Link Table, Object Table. If COMPLETE is specified then the previously mentioned tables and the Device Type Table, Object Type Table, Status Agent Tables will also be imported / exported.

SERVICE-MONITOR - If used with the TYPICAL parameter then the following tables will be imported / exported: Cal Holidays Table, Cal Time Handle Table, Serv Group Link Table, Serv Group Table, Rule Def Parts Table, Rule Def Event Table, Rule Definition Table, Service Objects Table. If COMPLETE is specified then the previously mentioned tables and the Rules Data Def Table, Data Def Obj Link Table, Data Elements Table will also be imported / exported.

NETWORK - The Network Hierarchy Table will be imported / exported if this parameter is used.

HISTORY - The Subject History Table and the Subject Control Table will be imported / exported if this parameter is used.

REACTION - The following tables will be imported / exported if this parameter is used: Tap Param Table, Command Post Config Table, Active Command Post Table, File Presence Table, File Metrics Table, File Poll Check Table.

ALL - If TYPICAL parameter is specified then all SERVICE-MONITOR and STATUS-MONITOR typical tables will be imported / exported. If COMPLETE parameter is specified then all SERVICE-MONITOR and STATUS-MONITOR complete tables will be imported / exported.

The [params] options are:

TYPICAL

COMPLETE



Details of these parameters is described above

Note: This parameter is optional. If it is not specified then TYPICAL is assumed to be the default.

TRANSIT - <transit-file> is the location of the file, or files that will hold the data imported or exported from the tables.

SEPARATE - is an optional parameter. If specified the data from each table is written to a separate transit file. The transit files will be in the location specified by the previous parameter. If this parameter is not specified then it is assumed that all data will be written to a single transit file.

The following are four examples of how to use the RFIMEXQ utility:

Export data into a single file

```
RUN RFLXOBJ.RFIMEXQ/IN RFLXDAT.DATACONF,OUT $$.#RFIMEXQ/EXPORT
STATUS-MONITOR TYPICAL TRANSIT $DATA02.TRANSIT.TXFILE
```

Importing data from a single file

```
RUN RFLXOBJ.RFIMEXQ/IN RFLXDAT.DATACONF,OUT $$.#RFIMEXQ/IMPORT
STATUS-MONITOR TYPICAL TRANSIT $DATA02.TRANSIT.TXFILE
```

Exporting data into multiple files

```
RUN RFLXOBJ.RFIMEXQ/IN RFLXDAT.DATACONF,OUT $$.#RFIMEXQ/EXPORT ALL COMPLETE
TRANSIT $DATA02.TRANSIT.Q
```

Importing data from multiple files

```
RUN RFLXOBJ.RFIMEXQ/IN RFLXDAT.DATACONF,OUT $$.#RFIMEXQ/IMPORT ALL COMPLETE
TRANSIT $DATA02.TRANSIT.Q
```

Note: The output file is optionally placed in the spooler. This contains a report of the operations carried out by RFIMEXQ.



RFLXCOM

This utility provides several administration facilities, including those for Streamer processes.

RFLXCOM is a command line interface program which allows the user to perform various functions via the command line.

Via RFLXCOM, the user is able to Cancel Radiopaging requests, Enable and Disable radiopager dialling and display information about streamer processes. It is also able to warmboot various Reflex servers without having to use the Reflex GUI.

The following options have been added to RFLXCOM:

```
WARMBOOT EMS_EXTRACT
HOUSEKEEP
ARCHIVE
FILTER
ACTIVATE
```

WARMBOOT EMS_EXTRACT allows you to change the EMS Filter file or Translation file that is to be used.

HOUSEKEEP clears down the Subject Control and/or Subject History Tables.

ARCHIVE will move Audit & Status Monitor History data from the Reflex environment to archive files in a specified subvolume.

FILTER will generate and compile EMS Filter files.

ACTIVATE allows a paging process to be restarted and to reset thresholds for an Action Group. e.g. `ACTIVATE REACT $EMON TANDEM.8.1048 PATHWAY-TERM-SUSP`. Where `$EMON` is `<Reflex evtmon-process>`, `TANDEM.8.1048` is `<event-id>` and `PATHWAY-TERM-SUSP` is `<Action-Group>`.

Running RFLXCOM

To run RFLXCOM the following define must first be added to your TACL session:

```
ADD DEFINE =INSIDER_REFLEX_DATACONF, FILE <VOL>.RFLXDAT.DATACONF
```

Execute RFLXCOM, via the following command:

```
RUN RFLXOBJ.RFLXCOM
```

Note: If a `FILTER COMPILE` is to be performed then RFLXCOM must be run as a named:

```
RUN RFLXOBJ.RFLXCOM / NAME $<process-name> /
```

The command prompt `RFLX>` will be displayed allowing the commands to be entered.

```
Cancel Paging -> DELETE PAGE
Enable Paging -> ACTIVATE PAGE
Disable Paging -> SUSPEND PAGE
REFRESH -> WARMBOOT STREAMER
```

The RFLXCOM commands can also be executed within the same command line. For example, to display help information without using the RFLXCOM interface, enter the following command:

```
RUN RFLXOBJ.RFLXCOM HELP SYNTAX
```



Archiving

When Archiving Audit files and if no parameters are passed, i.e. the command ARCHIVE AUDIT is entered, then ALL records for BOTH of the Reflex 80:20 Audit files (<Reflex Database svol>.AUDDDET & AUDLOG) will be archived to the current logged on subvolume.

Note: The Archiving SMON command that was used for the archiving of Status Monitor History has been superseded by the FIXSBJH utility.

Archive files will be created by RFLXCOM. If Archived Audit files exist in the specified subvol for the day of the archive, they will be appended to.

Archived Audit files will be named as follows:

Archived AUDDDET file: ADddmmyy

Archived AUDLOG file: ALddmmyy

Archived files may be viewed using the HPE NonStop utility ENABLE as described in the "Using Enable to view Archived files" section.

Using Enable to view Archived files

ENABLE source files are supplied to generate the ENABLEs for the Archived AUDLOG and Archived Status Monitor History files. The source files are named ENBAUDL and ENBSBJHS, located in the Reflex Data dictionary subvolume (RFLXDDL).

The ENABLE source files will need some minor alterations so that they use the relevant DATAFILE and DICTIONARY for your environment. You may also want to change the name of the Pathway environment and SCOBOL object files, which will be created.

Once the ENABLE files have been amended for your environment, they need to be generated using the ENABLE command as follows:

```
ENABLE / IN <enable-source>, OUT <outfile>/
```

If the ENABLE is generated successfully, SCOBOL object files and Pathway configuration files will have been generated. Each ENABLE program may be used by starting up the Pathway environment and running the ENABLE program.

Example obey files, RUNARCHA and RUNARCHS are supplied to show the commands that are required to start up the pathway environment and run the ENABLE program. These files may need amending to work in your environment.

Once generated the ENABLES can be modified to process different archived files by amending the file ASSIGN statement in the Pathway configuration files.

Example of Viewing Archived Status Monitor History data

To view archived Status Monitor History data, carry out the following steps:

Edit / tedit the ENABLE source file: **ENBSBJHS** and amend the *DICTIONARY* and *DATAFILE* locations for your Reflex 80:20 environment, e.g.:

- **DICTIONARY** \$DATA02.RFLXDDL
- **DATAFILE** \$DATA02.MYSUBVOL.SM280103

*The DICTIONARY value should point to your Reflex 80:20 DDL subvolume.
The DATAFILE value should point to the 'Status Monitor History' archived file created earlier.*

Once amended, execute command: **ENABLE / IN ENBSBJHS , OUT \$\$.#SPOOL /**



Peruse contents should show results similar to:

```

ENABLE - T9155D40 - (09SEP96)          SYSTEM \INSIDER
- ENABLE source file to generate the enable program SBJ-HISTORY-PROG
- Use this file as an input file to ENABLE
- i.e. ENABLE /IN ENBSBJHS, OUT $$.#SPOOL/
- Enable will generate SCOBOL objects in AOBJ files (AOBJCOD & AOBJDIR) and
- a PATHWAY configuration file ARCHPTH3
- Note that the DATAFILE and DICTIONARY parameters will need tailoring to
- your specific requirements
SET BOX RECORD arch-Subject-history-rec
ADD BOX arch-Subject-history-rec , DELETE OFF, INSERT OFF, UPDATE OFF,
DICTIONARY $DATA02.RFLXDDL, DATAFILE $DATA02.MYSUBVOL.SM280103
Box added:          ARCH-SUBJECT-HISTORY-REC
SET APPL TREE (01 arch-subject-history-rec )
SET APPL PATHCOMFILE archpth3
SET APPL SCOBOBJECT AOBJ
ADD APPL Sbj-hist-prog
Application added:  SBJ-HIST-PROG
- Generate the applications here
GENERATE sbj-hist-prog
Generating program: SBJ-HIST-PROG
Please wait...
Program generated:  SBJ-HIST-PROG
Programs generated: 1
Errors detected: 0

```

Within the Reflex 80:20 DDL subvolume, e.g. RFLXDDL, obey the following file:

- **RUNARCHS**

NB. This file may need amending first, to avoid process name conflicts.

An example of 'RUNARCHS' contents is provided below:

```

CREATE archlog
ASSIGN PATHCTL, archctl
PATHMON / NAME $arch, NOWAIT,CPU 0, OUT archlog /
PATHCOM / IN archpth3 / $arch
PATHCOM $arch; RUN sbj-hist-prog
PATHCOM $arch; SHUTDOWN, WAIT

```

Obeying this file will start a Pathway interface with the following screen being immediately displayed (see next page):



```

SBJ-HIST-PROG
Page 1/1
* SUBJECT-HISTORY-KEY
  HISTORY-OBJECT-NAME _____
  HISTORY-NODE-NAME   _____
  HISTORY-SERIAL      _____
  HISTORY-OBJECT-TYPE _____
  HISTORY-OBJECT-SUBTYPE _____
  HISTORY-STATE       _____
  HISTORY-CHANGE-TIME _____
  HISTORY-CHANGE-TEXT _____

  _____

  HISTORY-OWNER       _____
  HISTORY-VALUE       _____
  HISTORY-VERSION     _____
  HISTORY-EVENT-NUMBER _____
  HISTORY-TIMESTAMP   _____

Ready for input          F3 for Help, shift F16 to Exit

BLOCK

```

To display examples of the various function key, select F3.

To select a record, using 'approximate', enter a possible value in the first field, i.e. HISTORY-OBJECT-NAME and execute F6. This will obtain the first record from the table using the specified value as a starting point.

For example, if you need to obtain EMS event history for object starting with \$ZTC0, enter this value in the HISTORY-OBJECT-NAME field and select F6. This will display the first EMS event record which fulfills this search criterion. From here, you can then use F5 to display next record(s).



Viewing Archived Auddet files

An ENABLE cannot be generated for AUDDDET. Attempting to generate and ENABLE will produce the error "DDL record exceeds 2046 bytes"

To circumvent this problem, take the generated ENABLE SCOBOL for AUDLOG and modify it for your needs. The SCOBOL source for the AUDLOG ENABLE can be generated by adding the command SET APPL SCOBOLSOURCE <scobol-source> to the ENABLE source.

Using the method described above, the SCOBOL source file SCOBAUDD was produced.

The main changes required to SCOBAUDD are:

- Replace AUDLOG record structure with AUDDDET record structure.
- Amend Checksum values to those of AUDDDET.
- Remove redundant alternate key definitions and the code that used them.
- Amend record and key sizes to reflect those of AUDDDET.
- Introduce new overlays & paging code to handle the field AUDDDET-DETAIL.

Once the SCOBOL changes are made and the program compiled, the Pathway configuration must be produced. The easiest way to create the Pathway configuration file is to take a copy of the AUDLOG Pathway configuration file and amend it. The following changes are required:

- Set the TCP params MAXTERMDATA and MAXREPLY to 29000. This is required to handle the size of the AUDDDET record.
- Set the TCP param TCLPROG to point to the location of the SCOBOL object files where the SCOBAUDD file was compiled into e.g. \$DISK.SUBVOL.AOBJ.
- Amend the SET PROGRAM TYPE and ADD PROGRAM commands to refer to the new AUDDDET-PROG.
- Amend the ASSIGN of AUDDDET-REC to point to the required file.

Further information about ENABLE, SCOBOL and PATHWAY can be found in the appropriate HPE NonStop documentation.



RFRECONQ

RFRECONQ is a utility which allows node name references to be modified within SQL tables and Enscribe files. Volume and subvolume references in the Enscribe files may also be modified.

To modify the node, subvolume and volume references, the utility will read 'Production' and 'Backup' references from a RFDEFS file. [Note: The RFDEFS file is found in the same subvolume as that specified for the DATACONF location; see example RUN command below]. The utility will ignore any process references in the RFDEFS file. The central column in the RFDEFS file will represent 'Production' details and the rightmost column will represent 'Backup' details:

	Production	Backup
NODE	\PROD	\BACK
VOLUME	\$LIVE	\$DEV
SUBVOL	APP	TESTAPP

To start RFRECONQ enter the following at a TAQL prompt:

```
RUN RFRECONQ / IN RFLXDAT.DATACONF, OUT <output location> / <files> <direction>
<service> <location>
```

Where the files options available are:

ALL - Reconciles node names in Reflex 80:20 SQL tables and Enscribe files. Also reconciles volume and subvolume names in the enquire files.

ENSCRIBE - Reconciles node, volume and subvolume names in Reflex 80:20 Enscribe files. The following files are modified: DATACONF, PARACONF, ACTPROC, ACTCOMM, PROGCONF and STRMCONF.

SQL-ALL - Reconciles node names in Reflex 80:20 SQL tables.

SQL-TYPICAL - Reconciles node names in Reflex 80:20 SQL tables, but not all node name references are updated in the object table.

SQL-OBJECT - Reconciles node names in Reflex 80:20 Object Table only.

SQL-SUBJECT-HISTORY - Reconciles node names in Reflex 80:20 Subject History and Subject Control Tables - 'SBJHISTQ' and 'SBJCTRLQ' respectively.

NETWORK HIERARCHY - Reconciles node names in Reflex 80:20 Network Hierarchy Table only.

The direction option can either be:

PRODUCTION-TO-BACKUP - Changes all production references to backup references in SQL tables and Enscribe files, e.g. \PROD to \BACK

BACKUP-TO-PRODUCTION - Changes all backup references to production references in SQL tables and Enscribe files, e.g. \BACK to \PROD



The Service options are:

SWAP-SERVICE - If duplicate key values are found when updating the Reflex 80:20 SQL tables the remaining field values are swapped over.

NOSWAP-SERVICE - The opposite of swap service in that the fields are not swapped over.

Note: If this parameter is omitted the default is assumed to be Swap-Service.

The location is either:

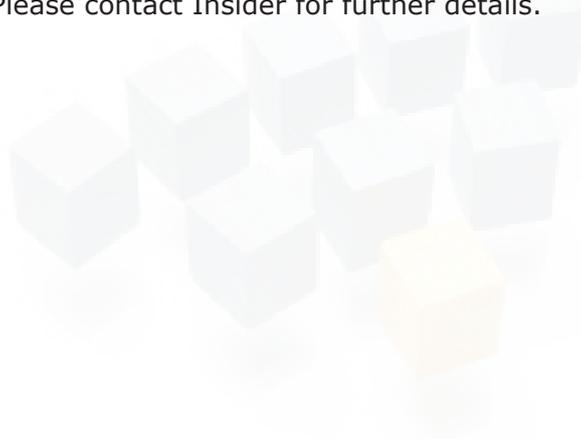
INSIDER - If the utility is being executed at Insider then this option is to be used. This option processes the contents of the DATACONF file last.

ON-SITE - When using the utility on a Customer site this option should be used. This option processes the contents of the DATACONF file first.

Note: Both of these parameters depend on whether you are performing a site-swap to your Production or Backup nodes. If this parameter is omitted the default is assumed to be On-Site.

The RFRECONCQ utility is primarily used for a Disaster Recovery situation.

Insider Technologies have procedures which can assist with a client's Reflex 80:20 Disaster Recovery environment. Please contact Insider for further details.





RFUSERHK

RFUSERHK allows a user to review the Reflex security database and optionally report on or delete obsolete GUARDIAN user ids from within the Reflex environment.

RFUSERHK will review the following four files:

- TASKCONF - Contains the name and configuration details of a Reflex Task record. This includes an optional requirement to specify the user id that programs within the task will execute as.
- TASKOWNR - Tasks have to be owned by one or more nominated user ids before that user can execute the task. The task / user id relationship is stored within this file.
- CONSFILT - The Console module is equipped with an extended filtering facility. This will allow the events retrieved from EMS by the Console module to be subjected to a further level of filtering before being buffered and relayed to the Reflex GUI for display. The extended filtering settings are stored in the CONSFILT file and this includes the ability to filter by the user id that created, or did not create the original EMS event.
- SECPROFL - Contains Reflex Security Profiles, which provides a correlation between a Security Class and a user. This Security Profile needs to be in place for the user to logon.

To start RFUSERHK, enter the following at a TACL prompt:

```
RUN RFUSERHK / IN RFLXDAT.DATACONF,OUT <LISTING FILE> / A,B,C,D UPDATE | PREVIEW
```

Where the options are:

<LISTING FILE> - Specify a listing file to receive the results. The default is the user's home terminal.

A - Enter Y or N to review the TASKCONF file. Default is N

B - Enter Y or N to review the TASKOWNR file. Default is N

C - Enter Y or N to review the CONSFILT file. Default is N

D - Enter Y or N to review the SECPROFL file. Default is N

UPDATE - Delete records

PREVIEW - Preview and report but don't delete records

Default = PREVIEW

Note: The utility will never delete any records from the TASKCONF, TASKOWNR or CONSFILT files, even when UPDATE mode is selected.

Manual changes via the Reflex GUI will always be required to correct any issues highlighted in the report.

Obsolete users discovered in the SECPROFL file will result in the associated record being deleted when UPDATE mode is selected.

Syntax errors will be reported to the <LISTING FILE> and not to EMS.



SERVICE MONITOR REPORTS

The Service Monitor Reports utility gives the user the ability to print the contents of the Service Monitor files, providing an overview of the current configuration. This provides a mechanism to locate any problems with the Service Monitor tree.

To run the reports utility, the following must be entered at a TACL prompt.

```
RUN RFLXOBJ.SERVPTS
```

The following menu will then be displayed allowing the user to select the required options.

```
Node : \INSIDER   Reflex Service Reports Menu           16/04/2013 16:26
1. Service Rules Report
2. Service Links Validation Report
9. Alter Spooler Location ($S) `
0. Exit Menu
```

Selecting an invalid option will display one of the following messages dependant on the input given.

```
*** Error : Invalid option, must be 0,1,2 or 9 ***
*** Error : Option must be a numeric value ***
```

To alter the current spooler location (default \$S) select option 9, the following prompt is then displayed allowing the user to amend the location. If no input is given, the value will remain the same.

```
Enter new Spooler Location (e.g $S)
```

Option 1: Service Rules Report

Selecting option 1 will display the following message and produce a print of the currently defined Services along with the Rules attached to the service.

```
Printing Service Rules Report...
Report completed.
Press a key.
```




Option 2 : Service Links Report

Selecting option 2 will display the following message and produce a print of all the links currently defined in Service Monitor.

Printing Service Links Report...

Report completed.

Press a key.

```

+-----+
| Service Name : ITLTECH |
+-----+

+-----+
|0001| Platform : \ITLTECH | Link Type : Object |
+-----+
|   FILES | Found | |
|   | |-----|
|   +--- $DATA99.TESTSUBV.ABCDEFGH | Found |
+-----+

+-----+
|0002| Platform : | Link Type : Group |
+-----+
|   ITLTECH | Found | |
|   | |-----|
|   +--- FILES | Found |
+-----+

+-----+
|0003| Platform : | Link Type : Group |
+-----+
|   ITLTECH | Found | |
|   | |-----|
|   +--- MULTIBATCH | Found |
+-----+

+-----+
|0004| Platform : \ITLTECH | Link Type : Object |
+-----+
|   MULTIBATCH | Found | |
|   | |-----|
|   +--- $BMON | Found |
+-----+

+-----+
|0005| Platform : \ITLTECH | Link Type : Object |
+-----+
|   MULTIBATCH | Found | |
|   | |-----|
|   +--- CSPL.AA.01 | Found |
+-----+

Node : \ITLTECH          Reflex Service Links Validation Report          28/0

+-----+
| Service Name : \INSIDER |
+-----+

+-----+
|0001| Platform : \ITLTECH | Link Type : Object |
+-----+
|   \INSIDER | Found | |
|   | |-----|
|   +--- \INSIDER.$X2520 | Missing |
+-----+

+-----+
| End of Report |
+-----+
    
```



STATCOLL

The STATCOLL Utility reads through a nominated EMS collector or log file and creates a report giving statistics by:

- (a) Event Number
- (b) Subsystem

Output is identical to that displayed via the Reflex 80:20 GUI - Discovery Module.

```
RUN RFLXOBJ.STATCOLL / IN RFLXDAT.DATACONF, ..standard run options../ param, param...
```

where params can be:

COLLECTOR - \$0 (default) or EMS Alternate Collector Name.

LOGFILE - Name of an EMS logfile (default: \$0 Collector).

STARTTIME - Format DD/MM/YYYY/HH:MM:SS (default: 00:00:00 today).

ENDTIME - Format DD/MM/YYYY/HH:MM:SS (default: 23:59:99 today).

STATSFIL - Output for statistics (default: \$S.#STATS).

FILTER - Name of EMS filter to allow statistics to be collected for a subset of events (default: all events).

Note: Entering RUN STATCOLL at a TACL session will display the above syntax, in addition to two further parameters (see below), the functions of which are no longer supported.

DICTSVOL - Subvolume containing the Data Dictionary for PCFILE layout, used by PCFORMAT program (default: no PCFORMAT output file produced).

PCFILE - CSV file containing statistics for exporting to PC spreadsheet (default: no PC output file produced).

Example:

```
RUN RFLXOBJ.STATCOLL / IN RFLXDAT.DATACONF / COLLECTOR $0 , ENDTIME &  
04/04/2017/15:00:00 , STATSFIL $S.#STATS
```



TASKIMEX

The TASKIMEX utility enables Reflex Tasks to be 'Imported' into or 'Exported' from different Reflex 80:20 databases, i.e. transfer Tasks between 'Test' and 'Live' environments without the need to duplicate the effort required.

Note : When inserting Tasks in a new database, the RFDEFS file in the destination database subvolume must contain 'Old' and 'New' node names.

For example, if you have exported tasks from node **\TEST** and you wish to import them into node **\LIVE**, then the RFLXDAT.RFDEFS file on node **\LIVE** should look like the following:

```
NODE      \TEST  \LIVE
```

The first node name **must** start in column 9; the second node name **must** start in column 17.

Note:The Reflex application must not be running when using this or any other Import / Export utility.

The TASKIMEX utility is run by entering the following at a TACL prompt.

```
RUN RFLXOBJ.TASKIMEX / IN RFLXDAT.DATACONF, OUT $$ / <operation> <taskname>
[TRANSIT <transit-file>] [RESET]
```

The available **<operation>** values are:

EXPORT – Export tasks from a Reflex Database.

IMPORT – Import tasks into a Reflex Database.

HELP – Displays a summary of the command syntax.

<taskname> - Can be the name of a specific task, e.g. BACKUP, or if you wish to Export or Import All Tasks, then utilise the wildcard symbol '*'.

[TRANSIT <transit-file>] - Location of the file that will hold the data Exported from the Reflex 80:20 database. If omitted, then the subvolume location of the Dataconf file is used, using a default filename of **'TRANSIT'**.

[RESET] - This option is used to erase any previous data in the transit file before performing an Export operation.

The following are examples of how to use the TASKIMEX utility:

Export All Tasks (*)

```
RUN RFLXOBJ.TASKIMEX / IN RFLXDAT.DATACONF, OUT $$ / EXPORT * TRANSIT
$DATA.RFLXDAT.TRANIMEX
```

Import All Tasks (*)

```
RUN RFLXOBJ.TASKIMEX / IN RFLXDAT.DATACONF, OUT $$ / IMPORT * TRANSIT
$DATA.RFLXDAT.TRANIMEX
```

Export a Specific Task (BACKUP)

```
RUN RFLXOBJ.TASKIMEX / IN RFLXDAT.DATACONF, OUT $$ / EXPORT BACKUP TRANSIT
$DATA.RFLXDAT.TRANIMEX
```

Import a Specific Task (BACKUP)

```
RUN RFLXOBJ.TASKIMEX / IN RFLXDAT.DATACONF, OUT $$ / IMPORT BACKUP TRANSIT
$DATA.RFLXDAT.TRANIMEX
```



XRPTMENU - Reflex 80:20 Reports

The Reflex 80:20 Reports utility provides a mechanism for printing the contents of the following Reflex 80:20 system files.

Reactions - Prints details of EMS events stored in Reaction Module and Action Groups.

Tasks and Programs - Prints contents of configured Task Names and their associated Task Programs.

Monitored Objects - Prints details of configured Status Monitor Objects.

Network Hierarchy - Prints details of Reflex 80:20 Networked NonStop nodes.

Parameters - Prints details of Database Parameters.

Process Monitoring - Prints details of configured Heartbeat Processes.

File List - Details of Reflex 80:20 files are listed, including brief description of each.

Security Profiles - Displays details of Security Profiles, associated Security Classes and User ID's.

Programs - Provides details of Programs configured in the TASKS module.

Streamer - Lists contents of each Streamer configuration.

Custom Details - Display EMS events with any user-configured 'Probable Cause & Recommended Action' details.

SMON Reactions - Details which Reaction events, where appropriate, map to which graphical icons on the Status Monitor display (See **REPORT13** section in this manual for further details).

These files provide a valuable overview of the system by displaying all the information in the database for each selected type of report. For example selecting Hardware Monitoring will provide a print out showing all the devices currently configured for monitoring including any descriptions, object icons, classes etc. used to display each hardware device on the status monitoring screen.

The Reflex 80:20 Reports Utility is run by entering the following at a TACL prompt:

```
RUN XRPTMENU
```

Next, you will be prompted to enter the location of the subvolume where your DATACONF file resides, e.g.:

```
$LIVE.RFLXDAT
```

You will then be prompted to enter the location of the print spooler, e.g.:

```
$S (within this spooler, the reports will be created in the location #RFLXnn where nn is the number of the report selected).
```

You will then be prompted whether a CSV file version of 'Report13' is required. There are three options: "Y", "N" and "E".

If "Y" is selected then a CSV file version will be output to the location of the Reflex DATACONF subvolume as follows:

```
RPNNMMDD where NN = menu option number/report number, MM = month and DD = day.
```

Note: If a report is run more than once in a day the the file will be overwritten each time.

After entering this information, the Reflex 80:20 Reports Menu will be displayed.



```
insider reflex
REFLEX - Reports Utility
Date 07/03/2014

1. Reactions
2. Tasks and Programs
3. Monitored Objects
5. Network Hierarchy
6. Parameters
7. Process Monitoring
8. File List
9. Security Profiles
10. Programs
11. Streamer
12. Custom Details
13. SMON Reactions Report

A. Run All Reports
R. Run Marked Reports
E. Exit Menu

Select option
?
```

You can select one or more report types from the menu and send them to the selected print spooler as follows:

1. Enter the number corresponding to the report you want to print and press enter. This will 'mark' the selected report in the menu.
2. Continue by selecting any other reports you wish to print. If you want to print all the reports, you may enter A at the prompt. If you make a mistake and mark the wrong report, simply enter its number again to de-select it.

```
insider reflex
REFLEX - Reports Utility
Date 07/03/2014

x 1. Reactions
x 2. Tasks and Programs
x 3. Monitored Objects
5. Network Hierarchy
6. Parameters
x 7. Process Monitoring
8. File List
9. Security Profiles
10. Programs
11. Streamer
12. Custom Details
x 13. SMON Reactions Report

A. Run All Reports
R. Run Marked Reports
E. Exit Menu

Select option
?
```

3. When you have marked all the reports you want to print, enter R at the prompt. The selected reports will be sent to the spooler and an acknowledgement message will be displayed. When all the reports have been sent, the utility will terminate and you will be returned to the TAFL prompt.



XRPTMENU - REPORT13 facility

An option in XRPTMENU is to product 'Report13' which provides Action Group to Status Monitor object relationships.

The XRPTMENU steps for producing 'REPORT13' results are provided below:

1. Volume: RFLXOBJ
2. Enter TACL command: RUN XRPTMENU
3. In the XRPTMENU utility, enter the location of the Reflex 80:20 DATACONF file, e.g. \$DATA.RFLXDAT
Note: The DATACONF file is used as a 'look-up' for the location of the Reflex 80:20 database.
4. Enter location of spooler, e.g. \$S
5. Enter Y to the question "Do you require a CSV version of the report"?
6. Enter 13 in the 'Select Option'
7. Enter R in the 'Select Option' (to Run Marked Reports)

Upon completion of REPORT 13, results are in Spooler under location #RFLX13 with a CSV file also being created in the database subvolume, e.g. RFLXDAT.

The naming convention for the CSV file is: RP13mmdd.

Upload this file to your PC, specifying ASCII option and once uploaded, add a suffix to the filename of CSV, e.g. RP130603.CSV.

If required, this file can now be imported into a Excel spreadsheet, or other documentation.

Examples of output from Report 13

Subsystem ID	Event Number	Reaction From	Cover To	Period S R	Action Group	Map
MAKE.0001	+00100	04-05-10:0000	04-05-20:2359	U N	MAKE-BLDG-UP	\$BLDLG
MAKE.0001	+00200	04-05-10:0000	04-05-20:2359	D N	MAKE-BLDG-DOWN	\$BLDLG
MAKE.0001	+00300	04-05-10:0000	04-05-20:2359	U N	MAKE-MCPTERM-UP	\$BHOME
MAKE.0001	+00400	04-05-10:0000	04-05-20:2359	D N	MAKE-MCPTERM-DOWN	\$BHOME

In the above example:

MAKE.0001.00100 & 000200 events are mapped to S.M. object \$\$BLDLG.

The 'S' column indicates the following:

N = Not graphically monitored, U = UP event, D = Down event, V = Vuln event

The 'R' column indicates the following:

N = Event not sent to Sentra, Y = Event sent to Sentra



Subsystem ID	Event Number	Reaction From	Cover To	Period S R	Action Group	Map
INSIDER.0051	+00100	09-08-04:0000	09-08-14:2359		INSIDER-DOWN	NoHG
=\$ZZWAN						

In the above example:

INSIDER.0051 event is associated with Process Monitoring but the object of \$ZZWAN is not present in Status Monitor, as indicated by text "NoHG=\$\$ZZWAN". ("NoHG" represents "No Heartbeat Graphic to Map to.").

Subsystem ID	Event Number	Reaction From	Cover To	Period S R	Action Group	Map
IBM.0099	+00002	01-01-97:0000	01-01-50:2359		MQ-CHANNEL-DOWN	~mq-
qmgr~.~mq-channelname~						
IBM.0099	+00003	01-01-97:0000	01-01-50:2359		MQ-QM-DOWN	~mq-
qmgr~						
IBM.0099	+00004	01-01-97:0000	01-01-50:2359		MQ-QM-QUEUE-DOWN	~mq-
qmgr~.~mq-qname~						
IBM.0099	+00005	01-01-97:0000	01-01-50:2359		MQ-QM-CH-INACTIVE	~mq-
qmgr~.~mq-channelname~						
Vulnerable Events					=	000001
Down Events					=	000003
Up Events					=	000000
Not configured to be monitored graphically					=	000000
With no corresponding graphic for mapping					=	000000
Total number of action groups					=	000004
Cover Periods Not Covering Current Period					=	000000
Events Relayed to Sentra					=	000000
Processes with no action groups configured					=	000000
No ACTWDOG record					=	000000
Total events monitored for subsystem id					=	000004

In the above example:

IBM.0099.00002 is mapped to a Status Monitor object, which matches the MQ Q-Manager and MQ-Channelname issued by the EMS event.

IBM.0099.00004 will map to the MQ Q-Manager object.

Subsystem ID	Event Number	Reaction From	Cover To	Action Group	Map To Status Monitor Object	S R
TANDEM.0041	+00006	09-09-94:0000	31-12-20:2359	X25-RAISED	Invalid Data - Run FILECLNU Utility!	U N
TANDEM.0041	+00007	09-09-94:0000	31-12-20:2359	X25-RESTART	Invalid Data - Run FILECLNU Utility!	D N
Vulnerable Events					=	000000
Down Events					=	000001
Up Events					=	000001
Not configured to be monitored graphically					=	000000
With no corresponding graphic for mapping					=	000000
Total number of action groups					=	000002
Cover Periods Not Covering Current Period					=	000000
Events Relayed to Sentra					=	000000
Processes with no action groups configured					=	000000
No ACTWDOG record					=	000000
Total events monitored for subsystem id					=	000002

On some occasions, an error message of "Invalid Data - Run FILECLNU Utility!" occurs in the "Map To Status Monitor Object" field. This is due to invalid characters (ie not N/Y/F/ space) passed in the "Pass-Manager" field of Watchdog.

See example on the next page which, obtained via the FUP command:

```
FUP COPY RFLXDAT.ACTWDOG, , A, SHARE.
```



```

$DEV.RFDA047.ACTWDOG RECORD 58 LEN 220
 0: X25-RAISED
 35: U7LINE UP
 70: X25X25..AP1X25.. .. ..
105:

$DEV.RFDA047.ACTWDOG RECORD 59 LEN 220
 0: X25-RESTART
 35: D7Line DOWN
 70: .. .. .. ..
105:

$DEV.RFDA047.ACTWDOG RECORD 60 LEN 220
 0: X25-SU-DOWN N
 35: DN
 70: .. .. .. ..
105:
    
```

The '7' character represents the 'Manager' field in the Status Monitor attribute; if this field is not used, then it should be represented with a 'N'.

The 3rd record shows a valid 'N' stored.

Reflex 4.7 provides a 'file clean-up' facility called FILECLNU to remove invalid characters such as this.

```
RUN RFLXOBJ.FILECLNU/IN RFLXDAT.DATACONF, OUT $S.#FLCLN, NAME $FLCLN/
```

where DATACONF represents the name of the data configuration file; \$S.#FLCLN represents the output which will receive the formatted print out, and RFLXOBJ represents your Reflex 80:20 object subvolume.

Subsystem ID	Event Number	Reaction From	Cover Period To	Action Group	Map To Status Monitor Object	S	R
TANDEM.0008	+01043	20-03-96:0000	20-03-20:2359	PATHWAY-OBJ-STARTED-UP	~manager-~subject~	U	N
TANDEM.0008	+01047	20-03-96:0000	20-03-20:2359	PATHWAY-OBJ-TCPTERM-VULN	~manager-~subject~	V	N
TANDEM.0008	+01064	20-03-96:0000	20-03-20:2359	PATHWAY-FREEZE-THAW-VULN	~manager-~subject~	V	N
TANDEM.0008	+01065	20-03-96:0000	20-03-20:2359	PATHWAY-FREEZE-THAW-VULN	~manager-~subject~	V	N
Vulnerable Events				=	000003		
Down Events				=	000000		
Up Events				=	000001		
Not configured to be monitored graphically				=	000000		
With no corresponding graphic for mapping				=	000000		
Total number of action groups				=	000003		
Cover Periods Not Covering Current Period				=	000000		
Events Relayed to Sentra				=	000000		
Processes with no action groups configured				=	000000		
No ACTWDOG record				=	000000		
Total events monitored for subsystem id				=	000004		

In the above example:

TANDEM.0008 events are mapped to a Status Monitor object, which matches the Manager and Subject token issued by the EMS event.

As these are HPE NonStop Pathway events (TANDEM.8 SSID), the Manager could be \$RFLX (Pathmon process) and the subject could be SMON-PROCESSING (server name).



Subsystem ID	Event Number	Reaction From	Cover Period To	Action Group	Map
AABB.0010	+00010	08-10-03:0000	08-10-23:2359	INSIDER-UP-FILE	!! EMS Event Subject !! ,U,N
AABB.0010	+00020	08-10-03:0000	08-10-23:2359	INSIDER-DOWN-FILE	!! Not Graphically Monitored !! ,N,Y
AABB.0010	+00030	08-10-03:0000	08-10-23:2359	INSIDER-VULN-FILE	!! EMS Event Subject !! ,V,N
AABB.0010	+00030	08-10-03:0000	08-10-23:2359	INSIDER-VULN-FILE	!! 2 DIGIT COVER PERIODS - RUN ACTEXPF !!
AABB.0010	+00040	08-10-03:0000	08-10-23:2359	INSIDER-UP-FILE	!! EMS Event Subject !! ,U,N
AABB.0010	+00040	08-10-03:0000	08-10-23:2359	INSIDER-VULN-FILE	!! COVER PERIODS DUE TO EXPIRE RUN ACTEXPF !!

On some occasions, an error message of "2 DIGIT COVER PERIODS - RUN ACTEXPF" or "COVER PERIODS DUE TO EXPIRE RUN ACTEXPF" occurs in the "Map to Status Monitor Object" fields. This is due to problems found in the Cover Period of a configured reaction.

Reactions that have been created with two digit years will be processed correctly by Reflex but for consistency, it is recommended that they are converted to four digit years.

Any reaction whose cover period has expired will no longer be processed, therefore it is important to know if any reactions will soon expire. The cover periods of reactions can be easily amended using the Reflex GUI, however, it could be a laborious task if there are many reactions that are due to expire at the same time.

Both of these problems can be resolved by using the ACTEXPF utility program. This program will amend any reaction records which are using two digit years, to now use four digit years. The program will also extend the cover period of reactions that are due to expire by a further 10 years.





3. Individual Disk Monitoring (% Full)

Monitoring Individual % Full Values

Monitoring of individual disks with differing % full values can be configured and alerted if thresholds per disk are broken, e.g. alert if \$SYSTEM is greater than (>) 90% full and also alert if \$ARCH is less than (<) 85% full.

If required, monitoring can be disabled for individual disks, e.g. \$DATA is always a certain % full and therefore monitoring is not required for this particular disk.

To use this facility, the following configuration is required.

1. Within the Reflex Admin Module, File Alias tab, configure a new DISKFULL file alias that points to an edit file.

Alias	Filename
CONSCONF	\INSIDER.\$LIVE.RFLXDAT.CONSCONF
CONSFILT	\INSIDER.\$LIVE.RFLXDAT.CONSFILT
CONSGATE	\INSIDER.\$LIVE.RFLXDAT.CONSGATE
CPUMONIT	\INSIDER.\$LIVE.RFLXDAT.CPUMONIT
DATADEFQ	\INSIDER.\$LIVE.RFLXDAT.DATADEFQ
DATAEQ	\INSIDER.\$LIVE.RFLXDAT.DATAEQ
DATCACHQ	\INSIDER.\$LIVE.RFLXDAT.DATCACHQ
DDEFQ	\INSIDER.\$LIVE.RFLXDAT.DDEFQ
DEVICEQ	\INSIDER.\$LIVE.RFLXDAT.DEVICEQ
DISKFULL	\INSIDER.\$LIVE.RFLXDAT.DISKFULL
DISKIO	\INSIDER.\$LIVE.RFLXDAT.DISKIO
EMONCOLO	\INSIDER.\$O
EMONCOL1	\INSIDER.\$ZLOG
EMSTRANS	\INSIDER.\$LIVE.RFLXDAT.EMSTRANS
EVENTCX	\INSIDER.\$LIVE.RFLXDAT.EVENTCX
EVENTDR	\INSIDER.\$LIVE.RFLXDAT.EVENTDR

2. Enter individual disk entries into the DISKFULL edit file in the format:

```
<disk name> <%full value> [<operator>]
```

The **disk name** can be any valid, local physical disk name, e.g. \$SYSTEM.

The **%full value** can be any number in the range 0 to 100, or it can be one of the special values of -1 or 999:

Value of -1 - disables ALL disk threshold monitoring for the individual disk

Value of 999 - disables % full monitoring for the individual disk but still performs monitoring for other disk metrics such as Cache Read Hits.

The **operator** is an optional operator value of < or >. The default value if no operator is specified as >.

Disks that are not listed in the DISKFULL tedit file will use the default % Full check, as configured in the Reflex Admin - Parameter 'DISK-FULL-THRESHOLD'.



Individual Disk Monitoring (% Full)

Each disk entry must be on a separate line.

The maximum number of individual disk entries that can be monitored is controlled by the Admin parameter - MAX-DISKS - and the highest value that the MAX-DISKS parameter can have specified is 1500.

Example contents of the DISKFULL edit file are:

```
$SYSTEM 80 >  
$ARCH 85 <  
$DEV 999  
$TEST -1  
$DATA 90 >
```

3. To activate monitoring, either stop, then restart Reflex OR freeze, stop, thaw and start the Pathway Serverclass DASH-THRESH.

Example EMS event raised by the DASH-THRESH server for Individual Disk Monitoring (% Full):

```
12:28 13DEC07 000,01,316 REFLEX 80:20 : DASHBOARD - Disc $ARCH is 80% full.  
Threshold (< 85%) has been exceeded.
```





4. Individual Disk Monitoring (I/O Times)

Monitoring of Individual Disk I/O

Individual Disk I/O can be monitored and each Disk can be monitored against specific values. This type of monitoring is provided via the REFLEX-DISKIO serverclass.

REFLEX-DISKIO will obtain the count of timings that I/O took on each Disk at regular polling intervals as defined in the Admin Parameter DISKIO-POLL-INTERVAL.

The timings of each I/O are counted into 'time buckets' of 0-50ms, 51-100ms, 101-200ms, 201ms-1sec, 1-2secs and 2-5secs.

Timings are obtained for each Disk Path i.e. the Primary, Backup, Mirror and Mirror Backup paths.

For example, using a DISKIO-POLL-INTERVAL of 600 (seconds) the timing counts obtained are:

Poll at 09:00:

I/O Times:						
Path	0-50ms	51-100ms	101-200ms	201ms-1sec	1-2secs	2-5secs
P	0	0	0	0	0	0
B	1897410	2	0	0	0	0
M	0	0	0	0	0	0
MB	36668	2	1	0	0	0

Poll at 09:10:

I/O Times:						
Path	0-50ms	51-100ms	101-200ms	201ms-1sec	1-2secs	2-5secs
P	0	0	0	0	0	0
B	1899410	3	0	0	0	0
M	0	0	0	0	0	0
MB	40000	2	1	0	0	0

The difference between the counts obtained during the previous and current polls for each disk path is calculated and is used in the monitoring checks, i.e. using the example above, the monitoring check will be made against the Backup Disk Path 0-50ms value being greater than or equal to 2000 (1899410 - 1897410).

If the specified monitoring count is exceeded then an EMS event is issued. When the specified monitoring count is no longer exceeded a different EMS event is issued.

The 3 new events issued by the REFLEX-DISKIO serverclass are:

DOWN (6052) - The DOWN event is only issued if a Primary Disk Path exceeds its I/O threshold

VULNERABLE (6051) - The VULNERABLE event is issued if any non-Primary Disk Path exceeds its I/O threshold

UP (6050) - The UP event is only issued if all Disk Paths return I/O levels back to below the threshold

These events / reactions are provided in a transit file named TRANDIO which can be imported via the RFIMEX utility.



Individual Disk Monitoring (I/O Times)

To use this facility, the following configuration amendments are required.

1. Within the Reflex Admin Module (File Alias tab), configure a new DISKIO file alias that points to an edit file containing Disk I/O monitoring rules. A default configuration is shipped that uses an edit file named DISKIO which is located in the Reflex Data subvolume (e.g. RFLXDAT.DISKIO).
2. A maximum number of Disk entries that can be monitored is controlled by the Admin Parameter DISKIO- MAX-DISKS. The default value is 500. Amend as required.
3. The frequency of EMS events issued by the DISK I/O monitoring program is controlled by the Admin Parameter DISKIO-MSG-FREQ. The default value is 3, i.e. notify on every 3rd poll if the state of the Disk hasn't changed. Amend as required.
4. The Admin Parameter DISKIO-POLL-INTERVAL controls how often the DISKIO modules polls to obtain DISK I/O Timing counts. The default value is for 10 minutes. Amend as required.
5. Enter individual Disk I/O monitoring entries into the DISKIO edit file in the format:

```
<disk name> <0-50ms count><51-100ms count><101-200ms count>
<201ms-1sec count><1-2secs count><2-5secs count>
```

The disk name can be the any valid, local physical disk name e.g. \$SYSTEM.

Each count can be a value in the range 0 to 100000 (do not include any commas).

Only Disks that are configured in the DISKIO file will be monitored. Each disk entry must be on a separate line, with a single space between each value.

Example contents of the DISKIO file are:

```
$SYSTEM 1000 750 500 100 1 1
$DEV    1000 750 500 100 1 1
$BAD    1000 750 500 100 1 1
$OSS    1000 750 500 100 1 1
```

Note: Any amended Disk I/O parameters and associated monitoring rules are only detected when the REFLEX-DISKIO serverclass is started. Therefore, any amendments will only become active once the serverclass has been frozen, stopped, thawed and re-started.



5. Specific Process Monitoring

This is a polling module that obtains process metrics for a set of configured processes and polls them at regular intervals.

The Specific Process Monitoring module can be used to keep track of any 'problem' processes that are not busy enough to appear in the top 10 busiest processes within the CPU they are using.

The process metrics that are obtained are displayed in the Reflex Dashboard GUI.

This module uses two Admin Parameters to control the polling and an additional Admin Parameter to control the frequency of Busy alerts if the optional Busy monitoring is used. See the "Admin Params" section for details on PROCBABY-BUSY-FREQ, PROCBABY-INTERVAL and PROCBABY-PRIORITY parameters.

An edit file - PROCLIST - is used to specify which processes are to be monitored along with optional Busy threshold values and event numbers.

The Specific Process Monitoring module uses the serverclass PROC-MASTER, configured within the Reflex PWCONF file and is started automatically via the STARTSRV file; both of these files are located in the RFLXOBJ subvolume. The PROC-MASTER serverclass launches PROCBABY processes in each available CPU.

The Specific Process Monitoring module can optionally raise EMS alerts if processes breach a configured Busy threshold. Individual Busy thresholds can be configured within the edit file - PROCLIST. Individual Up and Down events numbers can also be configured which will be used to raise events using an SSID of INSIDER.52.4.

As mentioned previously, the processes to monitor are specified in the PROCLIST edit file but the contents must adhere to the following limits:

- A maximum of 1000 entries can be read from the PROCLIST file.

- Each entry in the PROCLIST edit file must be specified on a separate line.

- Each entry can be a process name or an object filename.

- A single trailing wildcard character (*) may also be used.

Notes: If an object filename is specified then all processes running against the object filename will be monitored.

An optional Busy % threshold along with Up and Down event numbers can be specified. In this situation, if the Busy % value is breached then an EMS alert is raised using SSID INSIDER.52.4 along with the Down event number. When the process returns below the Busy % threshold an EMS alert is raised using SSID INSIDER.52.4 and the Up event number.

The Busy threshold events also include a subject token that is set to the process name of the offending process. It is recommended that any Up / Down events are configured in ranges such as an Up event range of 1 - 999 and a Down event range of 1000 - 1999 since this would allow single reactions to be configured for the Up and Down alerting.



Specific Process Monitoring

The PROCLIST edit file must reside in the same subvolume as the PROCBABY object code.

Example PROCLIST file contents:

```
object file / process name <Busy % value> <Up event> <Down event>
$DISK.SVOL.OBJECT
$APP
$LI*
$DISK.APPOBJ.*
$SYSTEM.SYSTEM.TACL           2           10           1010
```

An example PROCLIST edit file is shipped in the Reflex object subvolume, typically RFLXOBJ.

When processing the PROCLIST edit file contents, any entry that doesn't contain a process name / object file is ignored.

In addition, if an entry has a valid process name / object file but invalid busy monitoring values then standard monitoring is performed but no Busy threshold monitoring is performed.

Finally, EMS alert messages are raised for any violations, such as:

```
14-03-22 14:29:10 \INSIDER.$X0476 INSIDER.REFLEX.4 002000 REFLEX 80:20
    PROCBABY - Problem in PROCLIST file, line
    3. One (or more) alerting parameters
    missing.

14-03-22 14:29:10 \INSIDER.$X0476 INSIDER.REFLEX.4 002000 REFLEX 80:20
    PROCBABY - Problem in PROCLIST file, line
    4. The Up and Down event numbers Must be
    different
```



6. File Existence Monitoring

The File Existence Monitoring facility can be found within the Reflex Heartbeat module and can be used to monitor files that are delivered from remote platforms to the HPE NonStop system, or for files that already exist on HPE NonStop.

Various file attributes can be monitored and if a monitored file is not in an expected state, e.g. 'File is Open' is selected and the monitored file is in an open state, then an EMS event can be raised.

Monitored files can have a Status Monitor object and Action Groups (EMS Events) associated, so that if Reflex finds there is a deviation from any of the configured attributes for that file, then an EMS Event will be issued and the object state changed.

When the File Existence tab is opened, the view displays the file existence record in the database for which monitoring has been set-up. A list of all configured file existence records is displayed on the left along with the Calendar Period configured for the monitoring of that file. The right hand side of the tabbed view displays the detail associated with any selected file existence record.

The various check boxes and fields in the right hand area of the File Existence view control which attributes of the file are to be verified and checked once the assigned calendar period has started. Any deviation from any check boxes ticked for the file will result in a vulnerable EMS alert being raised.

The FILE-PRES-MONIT serverclass performs the file existence monitoring.

As of Reflex v4.8B, the behaviour of the File Existence / Calendaring has changed. In previous releases, the Calendar and polling periods were strictly adhered to with potentially detrimental effect to the File Existence monitoring. Take for example a situation where there are a large number of files being monitored, e.g. 10,000 files, with a poll period configured for every minute. If only 7,500 files could be monitored every minute then the remaining 2,500 files would be left unmonitored when the next poll period kicks in.

From v4.8B, the monitoring of files now takes precedence over any Calendar / poll periods. Therefore in the example above, all 10,000 files would be monitored and the next poll period would be delayed; in this situation an EMS event will be raised, such as:

```
15-02-16 10:35:22 \INSIDER.$R8FM INSIDER.REFLEX.4 005137 File
File Existence Monitoring for Calendar
Period FILEMETRIC-HALFDAILY-CHECK has
been delayed since Monitoring for
Calendar Period PEAK-TIME is still
in progress.
```

In addition, if monitoring is still being performed then any incoming Calendar messages will be delayed until the monitoring is complete; in this situation an EMS event will be raised, such as:

```
15-02-16 10:35:22 \INSIDER.$R8FM INSIDER.REFLEX.4 005137 File
Existence Monitoring: A calendar START
message for Calendar Period
FILEMETRIC-HALFDAILY-CHECK has
been delayed since Monitoring for
Calendar Period PEAK-TIME is still
in progress.
```

**Check File Attributes area**

- **Timestamp Current** - checking this box will result in an EMS vulnerable alert being raised if the file being monitored does not have a timestamp that is today's timestamp.
- **File Empty** - checking this box will result in an EMS vulnerable alert being raised if the file being monitored is empty.
- **File is Open** - checking this box will result in an EMS vulnerable alert being raised if the file being monitored is open for write access.
- **Corrupt** - checking this box will result in an EMS vulnerable alert being raised if the file being monitored is marked as corrupt.
- **Broken** - checking this box will result in an EMS vulnerable alert being raised if the file being monitored is marked as broken.
- **Security** - the Use Security check box allows for the file existence monitoring software to verify the Read/Write/Execute/Purge settings and that the Guardian User ID is as expected. Any deviation from the entered values will result in a vulnerable alert being generated.
- **File Age** - the File Age Use box allows for the file existence monitoring software to check the age of a file. When a non-zero value is entered in the minutes box then a vulnerable alert will be raised if the file is older than the specified file age. If the minutes value is set to 0 then the value specified for the Event Value will be used as the File Age. For example, if the File Age is set to 0 and the event to be issued is TEST.10.0, then the File Age used would be 10 minutes.
- **Modification Age** - the Modification Age Use box allows for the file existence monitoring software to check the age of the last modification to a file. When a non-zero value is entered in the minutes box then a vulnerable alert will be raised if the file is not modified within the specified amount of minutes. If this minutes value is set to 0 then the value specified for the Event Value will be used as the Modification Age. For example, if the Modification Age is 0 and the event to be issued is TEST.10.0, then the Modification Age used would be 10 minutes.



File Existence Monitoring

Monitor Files area

- **Specific File** - this check box is checked if a specific file name is monitored at a given time. The file name cannot be wildcarded. Examples are: '\$DATA02.REMOTE.TRXSFILE', '\$D.DELIVER.PAYMENTS'.
- **First File With Prefix** - this check box is checked if only one file with a particular prefix should be monitored within a given subvolume at a given time. Only the first file with the given prefix will be checked for. Examples are: '\$DATA02.RFDA35.DA*' would check the first file with a prefix of 'DA', '\$SYSTEM.REMOTE.P*' would check the first file with a prefix of 'P'.
 - Note: At least one character should be specified as the prefix followed by a wildcard as in the last example.
- **All Files With Prefix** - this check box is checked if all files with a particular prefix should be monitored within a given subvolume at a given time. All files with the given prefix will be checked for. Examples are: '\$DATA02.RFDA36.PY*' which would check all files with a prefix of 'PY', while '\$BOS.DELIVER.T*' would check all files with a prefix of 'T'.
 - Note: At least one character should be specified as the prefix followed by a wildcard as in the last example. This method is useful if delivered files have a numeric suffix which is changeable on a daily basis, for example: '\$DATA02.REMOTE.PAY00001', '\$DATA02.REMOTE.PAY00002'.

Filename area

This field is used to enter the filename the user wishes to monitor for existence at an assigned calendar period.

All filenames should be fully qualified with both volume and subvolume references. HPE NonStop files are only monitored locally to the node running a licensed copy of the Reflex 80:20 application.

Entering a node reference in this field, e.g. \INSIDER.\$DATA02.REMOTE.TRXS0001, will result in the node reference being stripped from the filename entered. A wildcarded filename can be entered in this field and the effect of entering a wildcard is dependent upon the 'Monitor Files' area at the bottom of the Reflex GUI screen.

Note: Only an asterisk wildcard '*' can be used. This can only be used in the filename portion of the fully qualified filename, e.g. \$DATA02.RFDA36.T*, \$DATA02.TRSMIT.S*Q. There needs to be at least one character prefix in the filename as shown. The '?' character cannot be specified.

Calendar Period area

This field is used to assign a calendar period for which the file entered will be monitored. These calendar periods are taken from the Admin module / Calendar tabbed view.

Typically, files are delivered from remote systems at set times during the day or in the evening for processing on the HPE NonStop system. An example would be, monitor \$DATA02.REMOTE.TRXSFILE for existence or changes on weekdays but not weekends and bank holidays, between 20:00 and 20:30. Assigning a calendar period with these settings would result in the above file being monitored at those times and any deviation within this period would result in an EMS alert.

Note: Any calendar period record available cannot be deleted from the Admin module / Calendar Tabbed view if it is referred to in the File Existence module.



7. File-Metrics Monitoring

The File Metrics Monitoring facilities can be found within the Reflex Heartbeat module.

Numerous file attributes can be monitored and rules configured so that EMS events can be raised if the file is not in a 'healthy' state. For example, a rule could be configured to alert if the file is not Licensed or is greater than 90% full.

From release v4.7M, several enhancements have been made to allow increased flexibility, improve memory management and also negate the need for separate 'satellite' environments to cater for the monitoring of a large number (> 10,000) of files.

Files can be monitored at several polling intervals of:

- Critical Monitoring, i.e. user specified polling period (15 to 1800 seconds)
- Hourly Monitoring
- Half Daily Monitoring, i.e. every 12 hours
- Daily Monitoring, i.e. every 24 hours

In addition, entire subvolumes can be monitored on a daily polling basis.

Each of these monitoring periods use a single Reflex Pathway serverclass to perform their monitoring. These serverclasses are:

- FILE-METS-CRIT
- FILE-METS-HOUR
- FILE-METS-HALFD
- FILE-METS-DAILY
- FILE-METS-SVOL

By separating the monitoring in this way, it is possible to leave the serverclasses frozen for the monitoring periods that are not required. For example, if only Subvolume monitoring is required then the serverclasses FILE-METS-CRIT, FILE-METS-HOUR, FILE-METS-HALFD and FILE-METS-DAILY could be left frozen without impacting the Subvolume monitoring.

The STARTSRV file (located in the Object subvolume, e.g. RFLXOBJ) should be edited to specify which (if any) File Metrics serverclasses should be thawed and started. In the example extract below, only the Subvolume monitoring serverclass is thawed and started:

```
THAW SERVER REFLEX-CALMON

[ THAW SERVER FILE-METS-DAILY           ; START SERVER FILE-METS-DAILY
[ THAW SERVER FILE-METS-HALFD          ; START SERVER FILE-METS-HALFD
[ THAW SERVER FILE-METS-HOUR           ; START SERVER FILE-METS-HOUR
[ THAW SERVER FILE-METS-CRIT           ; START SERVER FILE-METS-CRIT
THAW SERVER FILE-METS-SVOL             ; START SERVER FILE-METS-SVOL

THAW SERVER FILE-MON-SET-UP
```

Each serverclass / polling interval has several configuration options that control how they run. With the exception of Subvolume monitoring each serverclass can run with up to 5 processes, to enable a larger number of files to be monitored than was previously available with earlier Reflex releases.

The number of files that each monitoring process can cater for is specified by the serverclass Startup parameter MAX-FILES. Valid values for MAX-FILES range from 500 to 10,000. Therefore with a maximum configuration of 5 processes each monitoring 10,000 files, it is possible for each monitoring period to monitor up to 50,000 files.



File-Metrics Monitoring

To determine, how many processes to configure for each file monitoring serverclass, an understanding of how many files to be monitored is required. In addition some scope should be factored in for increased future requirements; this is particularly important if wildcard filenames are being monitored, since in the future, more files may match the specified wildcard. The maximum number of files that can be monitored can be determined from the equation:

Number of processes running in the serverclass * MAX-FILES startup parameter

Note that the Subvolume Monitoring serverclass, FILE-METS-SVOL, only runs as a single process. Any attempts to configure additional Subvolume Monitoring processes will result in those processes stopping automatically.

When running in a multiple process configuration, the first process that starts in the serverclass acts as the 'controlling' process with additional processes acting as 'standby' processes. The 'controlling' process is responsible for initially allocating the shared extended memory segment, handling communications with other Reflex modules and generally controlling the 'standby' processes.

The number of processes that can be used for a File Metrics Monitoring serverclass is controlled by the usual Serverclass parameters MAXSERVERS and NUMSTATIC, in conjunction with a Reflex Admin Parameter FIME-MAX-STANDBY-**xxx** where **xxx** is a serverclass identifier of CRITICAL, DAILY, HDAILY, or HOURLY.

The Reflex FIME-MAX-STANDBY-**xxx** Admin Parameter controls the maximum number of 'standby' processes that the serverclass can use; i.e. the number of additional processes to the initial 'controlling' process.

For example, if the **MAXSERVERS** and **NUMSTATIC** Pathway settings for the FILE-METS-HOUR serverclass were set to 3 and the Reflex Admin Parameter FIME-MAX-STANDBY-HOURLY was set to 2, then the serverclass would run with 3 processes: 1 'controlling' process and 2 'standby' processes.

```
=INFO FILE-METS-HOUR
SERVER FILE-METS-HOUR
PROCESSTYPE GUARDIAN
AUTORESTART 0
CREATEDELAY 1 MINS
DEBUG OFF
DELETEDELAY 10 MINS
HIGHPIN ON
HOMETERM $ZHOME
IN $LIVE.RFLXDAT.DATACONF
LINKDEPTH 3
MAXLINKS 3
MAXSERVERS 3
NUMSTATIC 3
OWNER \ITLTECH.1,17
PARAM SERVNAME "FILE-METS-HOUR"
PRI 139
PROCESS $FHOU1 (CPUS 2:3,PRI 150)
PROCESS $FHOU2 (CPUS 2:3,PRI 150)
PROCESS $FHOU3 (CPUS 2:3,PRI 150)
PROGRAM $LIVE.RFLXOBJ.FIMEMONQ
SECURITY "N"
STARTUP "MAX-FILES 500 INFO-EVENTS Y TYPE 3"
TIMEOUT 100 MINS
TMF ON
```

A simple equation to determine the configuration is:

```
Serverclass MAXSERVERS = FIME-MAX-STANDBY-xxx + 1
Serverclass NUMSTATIC = FIME-MAX-STANDBY-xxx + 1
```



File-Metrics Monitoring

Please be aware that if the Pathway configuration was configured to use more processes than the amount catered for by the FIME-MAX-STANDBY-xxx parameter, then the additional processes would be automatically stopped.

IMPORTANT: Since the monitoring processes for a particular period share an extended segment of memory, they **MUST** be configured to use the same primary & backup CPUs, i.e. **ALL** processes in a File Metrics serverclass **MUST** use the same primary and backup CPUs.

When the 'Standby' monitoring process(es) start up, a delay is used to allow the 'controlling' process time to determine the size of the extended segment to allocate it (based on the actual number of file monitoring entries) and to determine how many 'standby' processes are running. This delay is configurable using the Admin Parameter FIME-METS-DELAY but under normal circumstances it should not be altered.

When the File Metrics serverclasses are running, any 'standby' processes will only be activated if there are more files than can be monitored by the 'controlling' process. For example, in a configuration where the serverclass has 2 processes running (1 'controller' and 1 'standby') and has a MAX-FILES value of 500 then when there are only 450 files to monitor the 'standby' process will perform no processing and it will be waiting for the 'controlling' process to wake it.

If an additional 51 files require monitoring (either due to new file definitions being entered in the GUI and a warmboot being performed, OR from new files matching a wildcard entry) then the 'controlling' process will send a wake message to the 'standby' process. The 'standby' process will then start to monitor the 501st file. The 'controlling' process will dynamically use any configured 'standby' process as required; it will also tell 'controlling' processes to sleep if they are no longer required.

If the File Metrics serverclass processes are stopped outside of the Pathway environment, i.e. with a TACL STOP command, or if they abend, then configuration details for the processes will be left over in the SQL table file_poll_check_table. These configuration details can prevent new instances of the processes from starting. Therefore, a TACL routine named CLRFIMET has been created to clear this configuration information. The TACL routine is used as follows:

```
LOAD / KEEP 1 / CLRFIMET
```

Two routines: CODE and CLRFIMET will be loaded, i.e.:

```
Loaded from $LIVE.RFLXOBJ.CLRFIMET:
```

```
CODE CLRFIMET
```

Issuing the command CLRFIMET will start the routine, provide a menu and display the file that will be updated:

```
CLRFIMET
--- Insider Technologies: Reflex 80:20 ---
--- File Metrics SQL Table Reset Routine ---
--- Reset Options:
(1) Critical Monitoring period
(2) Hourly Monitoring period
(3) Half Daily Monitoring period
(4) Daily Monitoring period
(5) Subvolume Daily period
(6) All Monitoring periods
(X) Exit

SQL Table that will be updated is: \ITLTECH.$DEV.RFDA047.ACTFIPLQ

Please select the Reset option_
```



File-Metrics Monitoring

Once the selected Reset option has been entered, the result will be displayed, e.g.:

```
Resetting Hourly period entries
- 5 row(s) updated.
End of SQLCI Session
```

Note This routine should ONLY be used for File Metrics monitoring periods that have NO processes running. If it is used against a monitoring period that has processes running then those processes may crash.

File-Metrics Monitoring: Ease of Configuration

To ease the configuration of the File Metrics module, a TAACL routine CNFFIMET has been created. This routine will allow the number of File Metrics processes, their process names and primary/backup CPUs to be specified.

The maximum number of files that each File Metrics process can monitor and whether they issue informational EMS events can also be configured. In addition the routine will update the Pathway configuration file (PWCONF), the Pathway start-up file (STARTSRV) and the Reflex Admin parameter file (PARACONF). Where possible, the routine will use default values if the enter key is used to answer any questions. If the number of process to be used for a monitoring period is supplied as 0, then monitoring for that period is disabled.

The TAACL routine is used as follows:

```
LOAD / KEEP 1 / CNFFIMET
```

Nineteen routines will be loaded, i.e.:

```
Loaded from $LIVE.RFLXOBJ.CNFFIMET:
CODE          VALIDATE          VALIDATE_NUM      VALIDATE_FLAG
VALIDATE_NUM2 VALIDATE_CPU       UPDATE_PWCONF     UPDATE_STARTSRV
GET_PROCNAME  GET_PROCNUM       GET_DATACONF      GET_CPUS
GET_MAXFILES  GET_INFO          SQL_UPDATE        CHECK_PWAY
READ_PARACONF READ_DATACONF     CNFFIMET
```

Issuing the command CNFFIMET will start the routine, provide a menu and display the SQL table that will be updated:

```
CNFFIMET
----- Insider Technologies: Reflex 80:20 -----
----- File Metrics configuration Routine -----

----- Configuration Options:

(1) Critical Monitoring period
(2) Hourly Monitoring period
(3) Half Daily Monitoring period
(4) Daily Monitoring period
(5) Subvolume Daily period

(X) Exit

SQL Table that will be updated is: \ITLTECH.$LIVE.RFLXDAT.ACTFIPLQ
Please select the Configuration option:
```

Once the configuration option has been entered, the location of the Dataconf file will be prompted for, e.g. after entering 1:

```
Enter the Dataconf location
or press enter to use the default value of RFLXDAT.DATACONF
Please enter the location of the Dataconf file:
```



File-Metrics Monitoring

Once the Dataconf location has been entered e.g. RFLXDAT.DATACONF, the file will be opened to determine the location of the Paraconf file. The Paraconf will then be read to obtain the name of the Reflex Pathmon process. The Reflex Pathway will also be checked to ensure that the serverclass to be updated is not in use.

```
The Dataconf location was entered as : RFLXDAT.DATACONF
Attempting to read the Dataconf file to obtain Paraconf location
Determined Reflex Paraconf file to be: \ITLTECH.$LIVE.RFLXDAT.PARACONF
Attempting to read the Paraconf file to obtain Pathmon Process name.
Determined Reflex Pathmon process to be: $RFLX
Checking if serverclass FILE-METS-CRIT is running in Pathway $RFLX
No running processes were found for serverclass FILE-METS-CRIT.
Proceeding with configuration.
```

Assuming that there were no running processes for the serverclass running, the number of processes to configure is then prompted for:

```
Enter number of processes for Critical monitoring or
press enter to use default of 2. (N.B. use 0 to disable monitoring)
New number of processes required (0-5) :
```

Once the number of processes has been entered, e.g. 3, it is then validated.

The prefix for the file metrics process(es) is then prompted for:

```
The number of processes entered was : 3
Number of processes : 3 - Valid
Enter 4 char process prefix or press enter to use default of $FCRI
New process prefix :
```

Once the process prefix is entered, it is validated. In the example above, the enter key was pressed, causing a default prefix to be used.

The Primary and Backup CPUs are then requested:

```
Using the default process prefix of : $FCRI
Enter CPUs to use or press enter to use CPUs 0:1
Enter Primary CPU to use for serverclass processes (0-1) :
Enter Backup CPU to use for serverclass processes (0-1) :
```

Once the Primary and Backup CPUs have been supplied, they are validated. In this example, CPUs 1 and 0 were supplied.

The maximum number of files that can be monitored by each process is then requested:

```
The Primary CPU entered was : 1
CPU number : 1 - Valid
The Backup CPU entered was : 0
CPU number : 0 - Valid
Enter Maximum Number of Files to monitor or
press enter to use default of 5000.
New Maximum number of Files to Monitor (500-10000) :
```



File-Metrics Monitoring

After a value for the maximum number of files to monitor has been entered, it is then validated. In this example, a maximum number of files to monitor of 1500 was entered.

The requirement for Informational EMS messages is then prompted for:

```
The maximum number of files to monitor was : 1500
Maximum Number of Files : 1500 - Valid
Enter Info Events flag or press enter to use the default of N
Are Info Events required (Y/N) :
```

After the Informational Events value has been entered and validated (in the example below, a Y was entered), the main processing is then performed.

The SQL table FILE_POLL_CHECK_TABLE is updated to correspond with the number of processes that are required. If the number of processes was previously entered as 0, then no entries will exist in the SQL table for the monitoring period being configured, i.e. it is disabled.

```
Info Events Flag : Y - Valid
SQL Conversational Interface - T9191G07 - (01AUG05)
(C) 1987 COMPAQ (C) 2004 Hewlett Packard Development Company, L.P.
Removing old entries from the =file_poll_check_table
- 4 row(s) deleted.
Adding 3 entries to the =file_poll_check_table
- 1 row(s) inserted.
- 1 row(s) inserted.
- 1 row(s) inserted.
End of SQLCI Session
```

The Pathway configuration file PWCONF is then updated, based upon the required configuration.

```
Updating the serverclass FILE-METS-CRIT in the PWCONF file
Purging old PWCONF2
$LIVE.RFLXOBJ.PWCONF2 Purged
Copying existing PWCONF to PWCONF2
FILES DUPLICATED: 1
```

The Reflex Pathway startup-file STARTSRV is then updated based upon the required configuration. If the number of processes was previously entered as 0, then the File Metrics serverclass is left frozen.

```
Purging old STRTSRV2
$LIVE.RFLXOBJ.STARTSRV2 Purged
Copying existing STARTSRV to STRTSRV2
FILES DUPLICATED: 1
Updating the serverclass FILE-METS-CRIT in the STARTSRV file
```



File-Metrics Monitoring

Finally, the Reflex Admin Parameter file - PARACONF - is updated so that the correct number of File Metrics Standby processes are configured.

```
Updating the Reflex Admin param FIME-MAX-STANDBY-CRITICAL to 0002
```

```
Successfully updated the Paraconf file.
```

```
Configuration changes successfully completed.
```

If any problems or validation errors occur, the TAACL routine will stop. In the example below, a request has been made to configure the File Metrics for the Hourly Monitoring period which still has processes running:

```
7> CNFFIMET
7..
— Insider Technologies: Reflex 80:20 —
— File Metrics configuration Routine —
— Configuration Options:
(1) Critical Monitoring period
(2) Hourly Monitoring period
(3) Half Daily Monitoring period
(4) Daily Monitoring period
(5) Subvolume Daily period
(X) Exit
SQL Table that will be updated is: \ITLTECH.$DEV.RFDA047.ACTFIPLQ
Please select the Configuration option : 2
Enter the Dataconf location
or press enter to use the default value of RFLXDAT.DATACONF
Please enter the location of the Dataconf file : RFDA047.DATACONF
The Dataconf location was entered as : RFDA047.DATACONF
Attempting to read the Dataconf file to obtain Paraconf location
Determined Reflex Paraconf file to be: \ITLTECH.$DEV.RFDA047.PARACONF
Attempting to read the Paraconf file to obtain Pathmon Process name.
Determined Reflex Pathmon process to be: $RQST
Checking if serverclass FILE-METS-HOUR is running in Pathway $RQST
Serverclass FILE-METS-HOUR has 2 processes running.
Please Freeze and Stop this serverclass before attempting reconfiguration.
Configuration changes aborted.
```



8. Pathway Monitoring

PATHWAY MONITORING (PWYMON)

This is a polling module that checks the status of nominated Pathway serverclasses at regular intervals.

It utilises a **File Alias** and two **Parameters**, both of which are configured via the Reflex Admin module; further details are provided on the next page.

Reflex Pathway Monitoring uses a serverclass **REFLEX-PWAY-MON**, configured within the Reflex PWCONF file and is started automatically via the STARTSRV file; both of these files are located in the RFLXOBJ subvolume.

Pathway Monitoring can also be used to alert on situations which will produce a DOWN event or a VULNERABLE event. An UP event will be issued for when the the situation has been resolved.

DOWN event situations

- The serverclass is running with less than the minimum number of processes, e.g. alert if the serverclass is running with less than 2 processes.
- The serverclass has debug enabled.
- The home terminal configured for the serverclass does not exist.
- The object that the serverclass is configured to use does not exist.

VULNERABLE event situations

- The serverclass is running against a ZZBI object.
- The serverclass is in a frozen state.

When the state returns back to an acceptable state then a corresponding **UP** event will be issued.

EMS event range

SSID:	INSIDER.50.0
UP event:	6000
VULNERABLE event:	6001
DOWN event:	6002

A Reflex Transit file - TRANPWYM - is provided for the above events.

The Reaction for all events utilises a format string value of `~manager~.~subject~`, which relates to the EMS event tokens for 'Pathmon Process' and 'Pathway Server' respectively.

The contents of the transit file can be imported via the RFIMEX utility.



Monitoring Pathway ServerClasses

The Pathway serverclasses that are to be monitored are listed in a PWYLIST file. There can be a maximum of 10 PWYLIST files, which are named PWYLIST0 to PWYLIST9. Each file can have multiple serverclasses declared for monitoring.

These files are standard EDIT type files (filecode 101) and are typically stored in the Reflex data subvolume (RFLXDAT).

The contents of the PWYLIST files follow a strict format as follows:

?	PATHMON	Server Name	Min	DEBUG	HT	PROG	ZZBI	FRZN
Y	\$RFLX	REFLEX-ADMIN	0	Y	Y	Y	Y	Y
Y	\$RFLX	REFLEX-SMON	1	Y	Y	Y	Y	Y
Y	\$RFLX	SMON-PROCESSING	1	Y	Y	Y	Y	Y
Y	\$RFLX	FILE-METS-MONIT	5	Y	Y	Y	Y	Y

Column references

- Any lines that have a ? in column 0 are treated as a comment.
- A Y in column 0 means that the declaration on that line is enabled; any other character means that the declaration is disabled.
- Column 2 is used to declare the Pathmon in which the serverclass is configured.
- Column 10 is used to declare the serverclass name.
- Column 31 is used to specify the minimum number of processes that the serverclass should have running.
- Column 41 is used to specify if debug alerting is required; values allowed are Y/N.
- Column 46 is used to specify if valid home terminal alerting is required; values allowed are Y/N.
- Column 51 is used to specify if valid program alerting is required; values allowed are Y/N.
- Column 56 is used to specify if ZZBI alerting is required; values allowed are Y/N.
- Column 61 is used to specify if frozen serverclass alerting is required; values allowed are Y/N.

An example file - PWYLIST0 - can be found in the Reflex data subvolume (RFLXDAT).

Reflex Admin / File Alias configuration

Each PWYLIST file that is to be used must be declared in the Admin / File Alias screen of Reflex, which shows the contents of the Reflex DATACONF file. The File Aliases specified must be in the range PWYLIST0 to PWYLIST9.

Reflex Admin / Parameters configuration

The Admin / Parameters screen contains configuration details that are used by the Pathway Monitoring module, which are:

- PWYMON-INTERVAL - specifies the time interval in seconds, between monitoring polls to the specified Pathway serverclasses.
- PATHMON-PROCESS - specifies the Pathmon that Reflex is running under.



Autodiscovery Modules

In order to keep user-input to a minimum when populating the Object database, several Autodiscovery modules are available which will automatically detect:

- NonStop Peripherals
- MultiBatch batch schedules
- Pathway objects
- X.25 Lines and SUs
- Async terminals
- Spooler objects
- OMF objects
- WebSphere MQ objects
- TCP/IP objects

These modules may be run from a TACL session or configured to run as Reflex Tasks.

NonStop Peripherals

The HPE NonStop Autodiscovery module automatically retrieves a list of all the logical peripheral devices and CPUs attached to your node.

The Autodiscovery utility is initiated by entering the following at a TACL prompt:

```
RUN RFLXOBJ.AUTODISC / IN RFLXDAT.DATACONF, OUT <OUTFILE> /
```

where RFLXOBJ is the Reflex 80:20 Object subvolume and RFLXDAT is the location of the Reflex 80:20 database configuration file.

Note: The "out <outfile>" parameter is optional. If it is not specified, then output will be returned to the terminal.

While the utility is running, a report similar to the example shown below will be generated:

```
Auto Discovery started successfully.....
Can't find Device no. 001 for object $0
Can't find Device no. 0021 for object $TMP
Can't find Device no. 0050 for object $ZA000
Auto Discovery completed successfully.....
```

Any devices that cannot be found by Autodiscovery are listed, which are devices that when checked against the Reflex SQL Device Type table are deemed not to be relevant.



MultiBatch

Users running MultiBatch can utilise the Reflex 80:20 MultiBatch Autodiscovery module to populate the MultiBatch stack programmatically within Reflex Status Monitor.

The following files are supplied as part of the MultiBatch installation object subvolume:

MBATAD - Autodiscovery Module for MultiBatch Version 8 and 9.

MULTIBGnn - MultiBatch Status Agent for various versions, e.g. MULTIBG93 which will operate with MultiBatch version 9.3.

Note: The MULTIBGnn objects can run as High or Low-pin.

Autodiscovery Module - MultiBatch Systems

Introduction

The MultiBatch Auto-Discovery utility is designed to easily scan and load MultiBatch BMON components into the Reflex 80:20 Status Monitor Database.

MBATAD supports the loading of the following BMON components:

- Jobs
- Segments
- Units
- Steps

Before you can Autodiscover your BMON, the following pre-requisites are required (described in the SET command):

- The MultiBatch Prepare Name, e.g. EOD-PREP
- The location of the MultiBatch Dataconf subvol (where the above Prepare name resides)
- Specify either: BUILD ALL (automatically place BMON objects into 'Live' Overdrive Status Monitor), or BUILD OBJECTS (placing BMON STEP objects into OD SETUP, from where tree structures can be built manually)

When the above three pre-requisites have been specified, execute the CREATE command to autodiscover your BMON.

Note: If you utilise the DELETE command, then only objects previously autodiscovered via SET BUILD ALL command are deleted; BMON objects resident in OD SETUP are not deleted.



Starting the MBATAD Utility

Before the MBATAD Utility can be started, the following define must be added at the TACL prompt:

```
ADD DEFINE =INSIDER_REFLEX_DATACONF, FILE <dataconf-file>
```

<dataconf-file> being the subvolume and name of the REFLEX 80:20 DATACONF file.

e.g. `ADD DEFINE =INSIDER_REFLEX_DATACONF, FILE $DATA.RFLXDAT.DATACONF.`

When the define has been added, type `RUN MBATAD` at the TACL prompt to start the MBATAD Utility. The following information will be displayed upon successful startup.

```
MultiBatch Auto-Discovery Utility 18/04/2014 21:45
```

```
Use HELP ALL for list of commands and syntax
```

```
MBATAD>
```

The MBATAD Utility is now ready to accept commands.

MBATAD Commands

HELP

Use the HELP command to list the syntax of the MBATAD commands.

```
HELP [ command-name | ALL ]
```

command-name is the name of a MBATAD command whose syntax you want to see.

ALL lists the names of all MBATAD commands with their syntax.

Examples

Enter HELP to display the names of all MBATAD commands :

```
MBATAD> HELP
```

```
EXIT HELP SET FC SHOW
```

```
CREATE DELETE RESET
```

Enter HELP DELETE to display the syntax of the DELETE command:

```
DELETE <delete-options>
```

```
<delete-options>
```

```
{ $<bmon-name>.<job-name>.<segment-name> | * | }
```



SET

This command is used to configure the following:

- MultiBatch **Dataconf** location (DATACONF <subvol-name>)
- MultiBatch **Prepare** Name (PREPARE <prepare-name>)
- **Build** BMON, either for including into 'Live' Overdrive (**ALL**), or for placing into Overdrive Setup (**OBJECTS**)

Enter HELP SET to display the syntax of the SET command:

```
SET <set-options>
```

```
<set-options>
```

```
{ DATACONF <subvol-name> } This is the location of the MultiBatch dataconf file.
{ PREPARE <prepare-name> } This is the Prepare name for the BMON you're
Autodiscovering
{ BUILD { ALL | OBJECTS } } Specify 'ALL' if you wish to place your
Autodiscovered BMON into Overdrive, i.e. 'Live'
Status Monitor.
```

NB. A Warmboot is performed automatically. Specify 'BUILD OBJECTS' if you only wish to place your Autodiscovered objects into OD SETUP. A Warmboot is then required after your BMON has been manually built within Overdrive Setup.

Note: If you do specify 'BUILD OBJECTS', then only OBJECTS for the BMON 'STEPS' will be placed into OD SETUP, e.g. \$TEST.JOBA.AA.01.* (Jobs and Segments are not Autodiscovered!) Your own tree structure can then be created.

CREATE

Use the CREATE command to build the MultiBatch tree and Objects.

Example

Create objects only

```
MBATAD> CREATE
> Removing current tree and objects
> Tree and objects removed
> Building job records
> Building segment records
> Building step records
> Building links
> Create completed
```



Examples

Setting the MultiBatch DATACONF file.

```
MBATAD> SET DATACONF $DATA.MBDATA.DATACONF
```

Setting the MultiBatch PREPARE name.

```
MBATAD> SET PREPARE EOD-PREP
```

SHOW

Use the SHOW command to display the current MBATAD settings.

```
SHOW [ attribute-name | ALL ]
```

attribute-name

```
{ DATACONF | PREPARE }
```

Examples

Display all current attribute settings. (Equivalent to entering SHOW with no parameters)

```
MBATAD> SHOW ALL
> Current Settings
> Dataconf Name : \INSIDER.$DATA.MBDATA.DATACONF
> Prepare Name : EOD-PREP
> BUILD MODE: ALL
```

Display current DATACONF setting.

```
MBATAD> SHOW DATACONF
> Dataconf Name : \INSIDER.$DATA.MBDATA.DATACONF
```

RESET

Use the RESET command to restore the MBATAD settings back to the default values.

```
RESET [ attribute-name | ALL ]
```

attribute-name

```
{ DATACONF | PREPARE }
```

Examples

Reset all attribute settings to default values. (Equivalent to entering RESET with no parameters)

```
MBATAD> RESET ALL
```

Reset DATACONF attribute to default setting

```
MBATAD> RESET DATACONF
```



DELETE

Use the DELETE command to remove current MultiBatch tree entries from the database.

```
DELETE <delete-options>
      <delete-options>
      { <$bmon>.<job-name>.<segment-name> | * | }
```

Note: Currently, only one wildcard character is allowed and must be at the end of the wildcard string.

This facility will only delete BMON objects which have previously been Autodiscovered via use of the SET BUILD ALL command set, i.e. Autodiscovered into the 'Live' database.

If BMON objects exist in the OD SETUP environment and grouped accordingly, then the tree structure will not be deleted - a manual removal is required.

Examples

Delete any jobs starting with JOB within the BMON process \$TES10.

```
MBATAD> DELETE $TES10.JOB*
```

Delete the BMON process \$TES10.

```
MBATAD> DELETE $TES10
```

Delete any BMON processes starting with \$TES.

```
MBATAD> DELETE $TES*
```

Delete jobs within BMON \$TES10 starting with BBB and have a segment name of QQ

```
MBATAD> DELETE $TES10.BBB*.QQ
```

EXIT

Use the EXIT command to stop the current MBATAD process and return to the TACL prompt.

```
EX[IT]
```

You can enter EX or EXIT to run the EXIT command.

Simultaneously pressing the CTRL and Y keys at the terminal will stop MBATAD after it has displayed EOF!



PATHWAY

Users can utilise the Pathway Autodiscovery module to populate the Pathway programmatically within Reflex Status Monitor.

The following files are supplied as part of the Pathway installation object subvolume:

PATHAD - Pathway Autodiscovery utility

PATHAG - Status Agent for Pathway objects

Autodiscovery Module - Pathway Systems

The Reflex 80:20 Pathway Auto-Discovery utility is designed to easily scan and load various user-definable Pathway components for a nominated Pathway system.

PATHAD supports the loading of the following PATHWAY components:

- Servers
- Terminals
- Programs
- TCP's

Starting the PATHAD Utility

Before the PATHAD Utility can be started, the following define must be added at the TACL prompt:

```
ADD DEFINE =INSIDER_REFLEX_DATACONF, FILE <dataconf-file>
```

<dataconf-file> being the subvolume and name of the REFLEX 80:20 DATACONF file.

e.g. `ADD DEFINE =INSIDER_REFLEX_DATACONF, FILE $DATA.RFLXDAT.DATACONF.`

When the define has been added, type `RUN PATHAD` at the TACL prompt to start the PATHAD Utility.

The following information will be displayed upon successful startup.

```
Reflex 80:20 Pathway Auto-Discovery Utility 15/02/2014 16:13
Use HELP ALL for list of commands and syntax
```

PATHAD>

The PATHAD Utility is now ready to accept commands.

HELP

Use the HELP command to list the syntax of the PATHAD commands.

```
HELP [ command-name | ALL ]
```

command-name is the name of a PATHAD command whose syntax you want to see.

ALL lists the names of all PATHAD commands with their syntax.

Examples

Enter HELP to display the names of all PATHAD commands:

```
PATHAD> HELP
EXIT          HELP          SET           FC            SHOW
CREATE       RESET         DELETE
```



Enter HELP SET to display the syntax of the SET command :

```
SET <set-options>
<set-options>
    {TOPLVL  { YES | NO } }
    {BUILD   { ALL | OBJECTS } }
    {STATE   { UP | DOWN | IN[VESTIGATE] } }
    {INCLUDE { ALL | TCP | SERV[ER] | TERM[INAL] | PROG[RAM] } }
    {ALIAS   <alias-name> }
    {MATCH   <match-string> }
    {PATHWAY <$pathway-process> }
```

EXIT

Use the EXIT command to stop the current PATHAD process and return to the TACL prompt.

EX[IT]

- You can enter EX or EXIT to run the EXIT command.
- Simultaneously pressing the CTRL and Y keys at the terminal will stop PATHAD after it displays EOF!

SET

Use the SET command to change one or more PATHAD attributes before you create any objects or groups. Use the SHOW command to display the current PATHAD attributes. You can also restore the attributes to their default settings by using the RESET command.

```
SET  { TOPLVL  { YES | NO } }
     { BUILD   { ALL | OBJECTS } }
     { STATE   { UP | DOWN | IN[VESTIGATE] } }
     { INCLUDE { ALL | TCP | SERV[ER] | TERM[INAL] | PROG[RAM] } }
     { ALIAS   <alias-name> }
     { MATCH   <match-string> }
     { PATHWAY <$pathway-process> }
```

```
TOPLVL { YES | NO }
```

specifies whether the Pathway tree will be created under its own Top-Level icon on the Status Monitor screen (YES) or under the "PATHWAY" Group. Default is "NO".

```
BUILD { ALL | OBJECTS }
```

specifies whether both the objects and the entire Pathway tree will be created or only the objects. Default is "ALL".

Note: If 'OBJECTS' is selected, then the 'TOPLVL' and 'ALIAS' settings are ignored and reset to their default values when the 'CREATE' command is called.

```
STATE { UP | DOWN | IN[VESTIGATE] }
```

sets the initial state assigned to each object that is created. Default is "INVESTIGATE".



```
INCLUDE { ALL | TCP | SERV[ER] | TERM[INAL] | PROG[RAM] }
```

specifies which Pathway components are to be created. Default is "ALL".

Examples

- Include only SERVER components.
PATHAD> SET INCLUDE SERVER
- Include ALL components.
PATHAD> SET INCLUDE TCP SERVER TERM PROGRAM
- Include SERVER and PROGRAM components.
PATHAD> SET INCLUDE SERVER PROG

ALIAS <alias-name>

specifies an alternative name for the group under which the Pathway components are created when building a tree. A maximum of 40 characters is allowed for the name. To specify an alias name with space characters, place it within quotations. The alias name can be reset by specifying a NULL string i.e. "". Default is "".

Note: The Alias name will be ignored if 'TOPLVL' is set to 'YES', as Top-Level groups cannot be renamed.

Examples

- Set Alias name to SALFORD-QUAYS.
PATHAD> SET ALIAS SALFORD-QUAYS
- Set Alias name to SALFORD QUAYS
PATHAD> SET ALIAS "SALFORD QUAYS"
- Clear the Alias name
PATHAD> SET ALIAS ""

MATCH <match-string>

used when building one type of Pathway component. Allows component names to be searched by specifying a wildcard search string. A maximum of 40 characters is allowed for the match string each of which can only be alphanumeric, wildcard characters (& and *) or '-'. The default match string is "".

Note: The Match string will be ignored if the 'INCLUDE' setting specifies more than one component type as searches are only done on one type.

Examples

- Set the match string to search for components ending with "SETUP".
PATHAD> SET MATCH *SETUP
- Set the match string to search for components starting with "REFLEX-".
PATHAD> SET MATCH REFLEX-*
- Reset the match string.
PATHAD> SET MATCH ""



SHOW

Use the SHOW command to display the current PATHAD settings.

```
SHOW [ attribute-name | ALL ]
      attribute-name
      { STATE | BUILD | INCLUDE | TOPLVL | MATCH | ALIAS
        PATHWAY }
```

Examples

- Display all current attribute settings. (Equivalent to entering SHOW with no parameters)


```
PATHAD> SHOW ALL
> Current Settings
> Pathway Name   : "\INSIDER.$RDEV"
> Alias Name     : "SALFORD QUAYS"
> Match String   : Not defined
> Top Level      : NO
> Initial State  : INVESTIGATE
> Build Mode     : ALL
> Include Types  : ALL
```
- Display current PATHWAY settings


```
PATHAD> SHOW PATHWAY
> Pathway Name   : "\INSIDER.$RDEV"
```

CREATE

Use the CREATE command to build the Pathway tree and/or Objects.

Examples

- Create objects only


```
PATHAD> CREATE
> Removing current tree entries...
> Deleting current objects...
> Searching for "SERVER" entries.
> Found 59 entries.
> Searching for "TCP" entries.
> Found 1 entry.
> Searching for "TERMINAL" entries.
> No entries found.
> Searching for "PROGRAM" entries.
> Found 1 entry.
> Create completed
```
- Create tree with only SERVER components using wildcard search "REFLEX*"


```
PATHAD> CREATE
> Deleting current objects...
> Searching for "SERVER" entries.
> Found 59 entries of which 25 entries match the search criteria.
> Create completed
```

Note: If you set BUILD ALL in Pathway Autodiscovery then a full warmboot will automatically be carried out and objects will *not* be visible in Overdrive Setup.



RESET

Use the RESET command to restore the PATHAD settings back to the default values.

```
RESET [ attribute-name | ALL ]
      attribute-name
          { STATE | BUILD | INCLUDE | TOPLVL | MATCH | ALIAS |
            PATHWAY }
```

Examples

- Reset all attribute settings to default values
(Equivalent to entering RESET with no parameters)
PATHAD> RESET ALL
- Reset PATHWAY attribute to default setting
PATHAD> RESET PATHWAY

DELETE

Use the DELETE command to remove current PATHWAY tree entries from the database.

```
DELETE <delete-options>
<delete-options>
{ PATHWAY
  { SERV[ER]    [<match-string>] }
  { PROG[RAM]  [<match-string>] }
  { TCP        [<match-string>] }
  { TERM[INAL] [<match-string>] }
```

Note: The PATHWAY parameter must be set to the required Pathway system e.g. \$RDEV prior to using the DELETE command. The <match-string> will allow wildcards to be entered to delete multiple entries.

Examples

- Delete any servers ending with "-SETUP"
PATHAD> DELETE SERVER *-SETUP
- Delete all servers
PATHAD> DELETE SERVER
- Delete entries PATHWAY system
PATHAD> DELETE PATHWAY

In order for Reflex 80:20 to monitor a Pathway system dynamically, the Pathway will need to be configured to log status change events to \$0 (or an Alternative Collector and monitored by Reflex 80:20. See EMANCOLn File Alias).

This is achieved by accessing the Pathway System via Pathcom and altering either LOG1 or LOG2 to use the following comand:

```
LOGn $0, EVENTFORMAT, STATUS
```

It is recommended that the above command is added to the Pathway configuration files for all of your Reflex monitored Pathway systems.



X25

The Reflex 80:20 X25 Auto-Discovery utility is designed to easily scan and load X25 lines and Sub-Devices.

Starting the X25AD Utility

Before the X25AD Utility can be started, the following define must be added at the TACL prompt.

```
ADD DEFINE =INSIDER_REFLEX_DATACONF, FILE <dataconf-file>
```

<dataconf-file> being the subvolume and name of the Reflex 80:20 DATACONF file.

e.g. \$DATA.RFLXDAT.DATACONF.

When the define has been added, type RUN X25AD at the TACL prompt to start the X25AD Utility. The following information will be displayed upon successful startup.

```
Reflex 80:20 X25 Auto-Discovery Utility          10/12/2013  11:14
Use HELP ALL for list of commands and syntax
X25AD>
```

The X25AD Utility is now ready to accept commands.

X25AD Commands

HELP

Use the HELP command to list the syntax of the X25AD commands.

```
HELP [ command-name | ALL ]
```

command-name - is the name of an X25AD command whose syntax you want to see.

ALL - lists the names of all X25AD commands with their syntax.

Examples

Enter HELP to display the names of all X25AD commands:

```
X25AD> HELP
EXIT          HELP          SET          FC          SHOW
CREATE       RESET
```

Enter HELP SET to display the syntax of the SET command:

```
X25AD> HELP SET
SET <set-options>

<set-options>
  { TOPLVL  { YES | NO }
  { BUILD   { ALL | OBJECTS }
  { STATE   { UP | DOWN | IN[VESTIGATE] }
  { MATCH   <match-string>
```



EXIT

Use the EXIT command to stop the current X25AD process and return to the TACL prompt.

EX[IT]

- You can enter EX or EXIT to run the EXIT command.
- Simultaneously pressing the CTRL and Y keys at the terminal will stop X25AD after it displays EOF!

SET

Use the SET command to change one or more X25AD attributes before you create any objects or groups. Use the SHOW command to display the current X25AD attributes. You can also restore the attributes to their default settings by using the RESET command.

```
SET { TOPLVL      { YES | NO }
      { BUILD      { ALL | OBJECTS }
      { STATE      { UP | DOWN | IN[VESTIGATE] }
      { MATCH      <match-string> }
```

```
TOPLVL { YES | NO }
```

specifies whether the X25 line group will be created under its own Top-Level icon on the Status Monitor screen (YES) or under the "X25 LINES" Group. Default is "NO".

```
BUILD { ALL | OBJECTS }
```

specifies whether both the objects and the entire X25 tree will be created or only the objects. Default is "ALL".

Note: If 'OBJECTS' is selected, then the 'TOPLVL' setting is ignored and reset to its default value when the 'CREATE' command is called.

```
STATE { UP | DOWN | IN[VESTIGATE] }
```

sets the initial state assigned to each object that is created. Default is "INVESTIGATE".

```
MATCH <match-string>
```

allows X25 lines to be searched by specifying a wildcard search string. A maximum of 40 characters is allowed for the match string each of which can only be alphanumeric, wildcard characters (& and *). The first character must always be a '\$'. The default match string is "".

Examples

- Set the match string to search for X25 lines ending with "20".

```
X25AD> SET MATCH $*20
```

- Set the match string to search for X25 lines starting with "\$X25".

```
X25AD> SET MATCH $X25*
```

- Reset the match string. (N.b. can also use RESET MATCH)

```
X25AD> SET MATCH ""
```



SHOW

Use the SHOW command to display the current X25AD settings.

```
SHOW [ attribute-name | ALL ]
      attribute-name
      { STATE | BUILD | TOPLVL | MATCH }
```

Examples

- Display all current attribute settings
(Equivalent to entering SHOW with no parameters)
X25AD> SHOW ALL
> Current Settings
> Match String : Not defined
> Top Level : NO
> Initial State : INVESTIGATE
> Build Mode : ALL
- Display current STATE setting
X25AD> SHOW STATE
> Initial State : INVESTIGATE

CREATE

Use the CREATE command to build the X25 tree and/or Objects.

```
CREATE
```

Examples

- Create X25 line groups and objects
X25AD> CREATE
> Removing current tree entries...
> Deleting current objects...
> Searching for X25 lines and sub-devices
> Found 3 sub-device(s) for X25 line \$X2520
> Found 1 X25 line
> Create completed successfully

RESET

Use the RESET command to restore the X25AD settings back to their default values.

```
RESET [ attribute-name | ALL ]

      attribute-name
      { STATE | BUILD | TOPLVL | MATCH }
```

Examples

- Reset all attribute settings to default values
(Equivalent to entering RESET with no parameters)
X25AD> RESET ALL
- Reset STATE attribute to default setting
X25AD> RESET STATE



ASYNCD

The Reflex 80:20 ASYNCD Auto-Discovery utility is designed to easily scan and load ASYNCD lines.

Starting the ASYNCD Utility

Before the ASYNCD Utility can be started, the following define must be added at the TACL prompt:

```
ADD DEFINE =INSIDER_REFLEX_DATACONF, FILE <dataconf-file>
<dataconf-file> being the subvolume and name of the Reflex 80:20 DATACONF file.
e.g. $DATA.RFLXDAT.DATACONF.
```

When the define has been added, type RUN ASYNCD at the TACL prompt to start the ASYNCD Utility. The following information will be displayed upon successful startup:

```
Reflex ASYNCD line Auto-Discovery Utility          22/04/2014  15:53
Use HELP ALL for list of commands and syntax
```

ASYNCD>

The ASYNCD Utility is now ready to accept commands.

ASYNCD Commands

HELP

Use the HELP command to list the syntax of the ASYNCD commands.

```
HELP [ command-name | ALL ]
```

command-name is the name of a ASYNCD command whose syntax you want to see.

ALL

lists the names of all ASYNCD commands with their syntax.

Examples

- Enter HELP to display the names of all ASYNCD commands:

```
ASYNCD> HELP
EXIT          HELP          SET          FC          SHOW
CREATE       RESET
```

- Enter HELP SET to display the syntax of the SET command:

```
ASYNCD> HELP SET
SET <set-options>
<set-options>
  { TOPLVL  { YES | NO }  }
  { MATCH  <match-string> }
```



EXIT

Use the EXIT command to stop the current ASYNCAD process and return to the TACL prompt.

EX[IT]

- You can enter EX or EXIT to run the EXIT command.
- Simultaneously pressing the CTRL and Y keys at the terminal will stop ASYNCAD after it displays EOF!

SET

Use the SET command to change one or more ASYNCAD attributes before you create any objects or groups. Use the SHOW command to display the current ASYNCAD attributes. You can also restore the attributes to their default settings by using the RESET command.

```
SET { TOPLVL { YES | NO } }
    { MATCH <match-string> }
```

```
TOPLVL { YES | NO }
```

specifies whether the ASYNC line group will be created under its own Top-Level icon on the Status Monitor screen (YES) or under the "ASYNC LINES" Group. Default is "NO".

```
MATCH <match-string>
```

allows ASYNC lines to be searched by specifying a wildcard search string. A maximum of 40 characters is allowed for the match string each of which can only be alphanumeric, wildcard characters (& and *). The first character must always be a '\$'. The default match string is "".

Examples

Set the match string to search for ASYNC lines starting with "\$TM*":

```
ASYNCAD> SET MATCH $TM*
```

SHOW

Use the SHOW command to display the current ASYNCAD settings.

```
SHOW [ attribute-name | ALL ]
      attribute-name
      { TOPLVL | MATCH }
```

Examples

- Display all current attribute settings
(Equivalent to entering SHOW with no parameters)

```
ASYNCAD> SHOW ALL
> Current Settings
> Match String : Not defined
> Top Level    : NO
```

- Display current TOPLVL setting

```
ASYNCAD> SHOW TOPLVL
> Top Level    : NO
```



CREATE

Use the CREATE command to build the ASYNC tree and/or Objects.

Examples

- Create ASYNC groups and objects

```
ASYNCAD> CREATE
> Deleting current tree entries...
> Searching for ASYNC lines
> Found 4 ASYNC lines.
> Create completed successfully
```

RESET

Use the RESET command to restore the ASYNCAD settings back to their default values.

```
RESET [ attribute-name | ALL ]
```

```
attribute-name
  { TOPLVL | MATCH }
```

Examples

- Reset all attribute settings to default values
(Equivalent to entering RESET with no parameters)

```
ASYNCAD> RESET ALL
```

- Reset TOPLVL attribute to default setting

```
ASYNCAD> RESET TOPLVL
```



SPOOLER

The Reflex 80:20 Spooler Auto-Discovery utility is designed to easily scan and load nominated Spooler components into the Reflex 80:20 Object database.

Spooler AutoDiscover (SPAD) supports the following Spooler components

- Supervisors
- Collectors
- Print Processes
- Devices

The autodiscovery tool will not build a graphical representation of the nominated Spooler environment; this view needs to be created manually via the Reflex OverDrive Setup facility.

SPAD Pre-requisites

The Spooler Auto-Discovery utility has been implemented as a TACL macro.

Before loading and executing this macro, the following pre-requisites must be reviewed.

- The macro will attempt to access the supplied 'SPINI' file to determine the names of the Supervisor processes to be interrogated. A copy of this file must be located on the current subvolume when the macro is executed.
- The Supervisor process names must be entered into the 'SPINI' file, one per line, e.g.:

```
$SPLS
$SPLD
```

- To discover the names of the Spooler collectors, Print processes and Devices, a SPOOLCOM command will be executed via the 'SPAD' macro.

By default this has been set to \$SYSTEM.SYSTEM.SPOOLCOM. If this is not the case, edit the 'SPAD' macro file and alter the setting of the **spoolcom_loc** variable.

SPAD LOAD and execution

To load the SPAD TACL macro:

```
LOAD / KEEP 1 / SPAD
```

The SPAD macro supports two parameters: SPINTYP and AGENT.

The SPAD can be executed using one, both, or none of these parameters.

```
SPAD [SPINTYP] [AGENT]
```

If the SPINTYP parameter is specified then Object Type table inserts are placed in a file named SPINTYP instead of being placed alongside all of the inserts for discovered Spooler objects into the SPIN file.

If the AGENT parameter is specified then the Status Agent for Spooler objects, AGENT-SPL, is included in the Object Type Table inserts. If this parameter is used then please ensure that the serverclass AGENT-SPL is thawed.

If there is an error while SPAD is processing, a Completion Code of 4 is returned.



SPAD SQLCI Processing

The SPAD macro creates two files in your current subvolume: SPIN and SPDEL. If the SPINTYP parameter was specified then a SPINTYP file is also created:

- SPIN contains the SQL script that needs to be executed to update the Object database table. If the SPINTYP parameter was not specified then the SPIN file also contains SQL script to update the Object Type database table.

The previous version of this file will be held in SPIN2.

- Optional SPINTYP file contains an SQL script to update the Object Type database table.

The previous version of this file will be held in SPINTYP2.

- SPDEL contains the SQL script that can be used to remove the Spooler components from the Reflex object database.

The previous version of this file will be held in SPDEL2.

To create the object database:

```
VOLUME RFLXOBJ
```

```
Load up the SQL defines: RUN RSQLDEFS
```

```
SQLCI / IN SPIN /
```

```
If the SPINTYP parameter was specified: SQLCI / IN SPINTYP /
```

If the SPINTYP parameter was not specified then the first four insert commands in the SPIN file will attempt to create object type and subtype records for Spooler Supervisors, Collectors, Print processes and Devices. If the SPINTYP parameter was specified then these four insert commands will be placed in the SPINTYP file.

If SPAD has been executed previously then these four insert commands will fail as these rows will already exist. These errors can be ignored.

Once the database has been updated by the SPAD utility, you will need to:

- Create a graphical tree to depict the Spooler hierarchy, using OverDrive Setup.
- FREEZE / STOP / THAW / START the Reflex Pathway server 'AGENT-SPOOLER' to allow spooler monitoring to start.
- If the AGENT parameter was specified then ensure that the 'AGENT-SPL' serverclass is THAWed to allow detailed spooler information to be obtained by the Status Monitor.

The SPDEL obey file can be used to delete the Spooler object information from the Reflex SQL database.

To delete the spooler object database:

```
VOLUME RFLXOBJ
```

```
Load up the SQL Defines: RUN RSQLDEFS
```

```
SQLCI / IN SPDEL /
```

```
To ensure that the Object counts in the Group table entries are correct:
```

```
RUN FIXNUMOB UPDATE
```

Note: The SPDEL file only removes Object table entries and Group Link relationships to those Object table entries. SPDEL will not remove any Group table entries and Group Link relationships created in the OverDrive Set-up facility.

These database entries will have to be manually deleted in OverDrive Set-up after the SPDEL obey file has been executed.



Example output after running SPAD

```

*
** Executing the Insider Technologies Spooler AutoDiscovery Facility **
*
** Checking for a valid SPOOLCOM file
*
** Checking for old SPIN and SPDEL files
*
** SPIN2 does not exist
*
** SPDEL2 does not exist
*
** Deleting old Work files
*
** Starting up the Editor and creating new SPIN & Work files
*
** Processing the SPINI file
*
** Retrieving the Spooler Collector information
*
* Supervisor process $<Supervisor-1> discovered
* Collector $<Collector-1> discovered
* Collector $<Collector-2> discovered
* etc.....
* Print Process $<Print-Process -1> discovered
* Print Process $<Print-Process -2> discovered
* etc...
* Device $<Device-1> discovered
* Device $<Device-2> discovered
* etc...
* Supervisor process $<Supervisor-2> discovered
* etc...

** Closing Down the Editor
*
** Deleting old Work files
*
$<currentvol>.<currentsubvol>.SPCOLOUT Purged
$<currentvol>.<currentsubvol>.SPPRTOUT Purged
$<currentvol>.<currentsubvol>.SPDEVOUT Purged
$<currentvol>.<currentsubvol>.SPDUMMY Purged
*
** Spooler AutoDiscovery Complete
*
** To complete the Reflex Spooler install
* a) Load up the SQL defines; RUN RSQLDEFS
* b) Execute an SQLCI / IN SPIN / command
*

```



Spooler Agent Processes

Spooler Agent

The Spooler Agent process periodically monitors the health of a system's spooler processes.

The interval between health checks is based on the Reflex 80:20 'SPOOLER-INTERVAL' parameter which is held in the PARACONF file; see Reflex GUI - Admin Module - Parameters tab. If no parameter is present, a default of 1 minute will be used.

The process will load the list of Spoolers to be monitored by reading these from the Reflex 80:20 object database; only those with a 'LIVE' status will be monitored.

The current usage of the Spooler Collector will be compared to the 'SPOOLER-THRESHOLD' parameter; if not present, a value of 80% is used as a default.

EMS events are issued by the Spooler-Agent when certain conditions occur; a list is provided below. To configure these in Reflex, see the RFIMEX Utility section and IMPORT the events contained in the supplied TRANSIT file: **TRANS SPL**.

Once the events have been imported, click on the RED exclamation ! mark in the Reaction Module and follow through the Generate and Compile Filter steps, followed by a Warmboot

```
5050 SPOOLAGENT : Monitoring of Spoolers starting.
5060 SPOOLAG : Spooler <supervisor> active
5061 SPOOLAG : Spooler <supervisor> DRAIN
5062 SPOOLAG : Spooler <supervisor> warm starting
5063 SPOOLAG : Spooler <supervisor> cold starting

5070 SPOOLAG : Collector <collector> belonging to <supervisor> active
5071 SPOOLAG : Collector <collector> user <supervisor> over threshold
5072 SPOOLAG : Collector <collector> belonging to <supervisor> full
5073 SPOOLAG : Collector <collector> belonging to <supervisor> drain
5074 SPOOLAG : Collector <collector> belonging to <supervisor> dormant

5080 SPOOLAG : Print process <print> belonging to <supervisor> active
5081 SPOOLAG : Pint process <print> belonging to <supervisor> dormant

5090 SPOOLAG : Device <device> belonging to <supervisor> waiting
5091 SPOOLAG : Device <device> belonging to <supervisor> busy
5092 SPOOLAG : Device <device> belonging to <supervisor> offline
5093 SPOOLAG : Device <device> belonging to <supervisor> printing
```



TCP/IP

The Reflex TCP/IP Auto-Discovery utility is designed to easily scan and load TCP/IP objects.

The utility will detect the following TCP/IP objects: Process, Subnet, Route, Compatibility Process (Parallel TCP/IP), Compatibility Subnet (Parallel TCP/IP), Compatibility Route (Parallel TCP/IP), Listner, and Telserv process.

Important: If the HPE NonStop TCP/IP stack configuration is amended after it has been autodetected by a previous run of the TCPIPAD program, then the TCPIPAD program will detect the new configuration. In this situation however, it is necessary to perform a FULL Warmboot of the Overdrive Setup as this is required to ensure any redundant tree structures are removed from the Overdrive display.

Starting the TCPIPAD Utility

Before the TCPIPAD Utility can be started, the following define must be added at the TACL prompt.

```
ADD DEFINE =INSIDER_REFLEX_DATACONF, FILE <volume>.RFLXDAT.DATACONF
```

When the define has been added, type RUN TCPIPAD at the TACL prompt to start the TCPIPAD Utility. The following information will be displayed upon successful startup.

```
Reflex TCP/IP Auto-Discovery Utility          20/05/2016 14:51
Use HELP ALL for list of commands and syntax
TCPIPAD>
```

The TCPIPAD Utility is now ready to accept commands.

TCPIPAD Commands

HELP

Use the HELP command to list the syntax of the TCPIPAD commands.

```
HELP [ command-name | ALL ]
command-name
    is the name of an TCPIPAD command whose syntax you want to see.
ALL
    lists the names of all TCPIPAD commands with their syntax.
```

Examples

- Enter HELP to display the names of all TCPIPAD commands :

```
TCPIPAD> HELP
EXIT          HELP          SET          FC          SHOW
CREATE       RESET
```

- Enter HELP SET to display the syntax of the SET command :

```
TCPIPAD> HELP SET
SET <set-options>
    <set-options>
    {TOPLVL { YES | NO } }
    {BUILD { ALL | OBJECTS } }
    {STATE { UP | DOWN | IN[VESTIGATE] } }
    { MATCH <match-string> }
```



EXIT

Use the EXIT command to stop the current TCPIPAD process and return to the TACL prompt. EX[IT]

- You can enter EX or EXIT to run the EXIT command.
- Simultaneously pressing the CTRL and Y keys at the terminal will stop TCPIPAD after it displays EOF!

SET

Use the SET command to change one or more TCPIPAD attributes before you create any objects or groups. Use the SHOW command to display the current TCPIPAD attributes. You can also restore the attributes to their default settings by using the RESET command.

```
SET { TOPLVL { YES | NO } }
    { BUILD { ALL | OBJECTS } }
    { STATE { UP | DOWN | IN[VESTIGATE] } }
    { MATCH <match-string> }
```

```
TOPLVL { YES | NO }
```

specifies whether the TCP/IP process group will be created under its own Top-Level icon on the Status Monitor screen (*YES*) or under the "TCP/IP" Group. Default is "NO".

```
BUILD { ALL | OBJECTS }
```

specifies whether both the objects and the entire TCP/IP tree will be created or only the objects. Default is "ALL".

Note : If 'OBJECTS' is selected, then the 'TOPLVL' setting is ignored and reset to its default value when the 'CREATE' command is called.

```
STATE { UP | DOWN | IN[VESTIGATE] }
```

sets the initial state assigned to each object that is created. Default is "INVESTIGATE".

```
MATCH <match-string>
```

allows TCP/IP processes to be searched by specifying a wildcard search string. A maximum of 40 characters is allowed for the match string each of which can only be alphanumeric, wildcard characters (& and *). The first character must always be a '\$'. The default match string is "".

Examples

- Set the match string to search for TCP/IP processes lines ending with "2".
TCPIPAD> SET MATCH \$*2
- Set the match string to search for TCP/IP processes starting with "\$ZTC".
TCPIPAD> SET MATCH \$ZTC*
- Reset the match string. (*N.b. can also use RESET MATCH*)
TCPIPAD> SET MATCH ""

SHOW

Use the SHOW command to display the current TCPIPAD settings.

```
SHOW [ attribute-name | ALL ]
attribute-name
{ STATE | BUILD | TOPLVL | MATCH }
```



Examples

- Display all current attribute settings
(Equivalent to entering *SHOW* with no parameters)
TCPIPAD> SHOW ALL>
Current Settings
> Match String : Not defined
> Top Level : NO
> Initial State : INVESTIGATE
> Build Mode : ALL
- Display current STATE setting
TCPIPAD> SHOW STATE
> Initial State : INVESTIGATE

CREATE

Use the CREATE command to build the TCP/IP tree and/or Objects.

```
CREATE
```

Examples

- Create TCP/IP line groups and objects
TCPIPAD> CREATE
> Deleting TCP/IP tree entries...
> Removing TCP/IP objects...
> Searching for TCP/IP objects
> Found 2 subnet(s) for TCP/IP process \$ZTC0
> Found 3 route(s) for TCP/IP process \$ZTC0
> Found 1 listner(s) for TCP/IP process \$ZTC0
> Found 1 telser(s) for TCP/IP process \$ZTC0
> Found 1 TCP/IP process
> Create completed successfully

Important: If the HPE NonStop TCP/IP stack configuration is amended after it has been autodetected by a previous run of the TCPIPAD program, then the TCPIPAD program will detect the new configuration. In this situation however, it is necessary to perform a FULL Warmboot of the Overdrive Setup as this is required to ensure any redundant tree structures are removed from the Overdrive display.

RESET

Use the RESET command to restore the TCPIPAD settings back to their default values.

```
RESET [ attribute-name | ALL ]
attribute-name
{ STATE | BUILD | TOPLVL | MATCH }
```

Examples

- Reset all attribute settings to default values
(Equivalent to entering *RESET* with no parameters)
TCPIPAD> RESET ALL
- Reset STATE attribute to default setting
TCPIPAD> RESET STATE



WebSphere MQ

The Reflex 80:20 MQSeries Auto-Discovery utility is designed to easily scan and load various user definable MQSeries components into the Reflex 80:20 Object database.

MQAD supports the following components

- Queue Managers
- Queues
- Channels

In addition the autodiscovery tool will build a graphical representation of the nominated MQ environments.

MQAD Pre-requisites

The MQSeries Auto-Discovery utility has been implemented as a TACL macro.

Before loading and executing this macro, the following pre-requisites must be reviewed.

- The macro will attempt to access the MQSINI file to determine the names of the Queue Managers. A copy of this file must be located on the "current" subvolume when the macro is executed.
- To discover the names of the MQSeries channels and queues, the RUNMQSC command line utility must be executed. By default this has been set to \$SYSTEM.SYSTEM.RUNMQSC. If this is not the case, edit the MQAD file and alter the setting of the mqsc_loc variable.
- In some installations, the RUNMQSC command is restricted to a secure UserID. Ensure that your current User can execute this command and access the nominated queue manager, and that the user can create files on your current volume.
- The graphical tree will be placed in the MQS class within the Reflex 80:20 Status Monitor. If this is not appropriate, then edit the MQAD file and alter the setting of the class_icon variable. The new class name must be 3 characters in length.

MQAD LOAD and Execution

To load the MQAD TACL macro:

```
LOAD / KEEP 1/ MQAD
```

If the MQ PARAMS have not been loaded by your TACLCSTM, then the following command is required:

```
PARAM MQDEFAULTPREFIX $<Your-MQ-Database-Volume>
```

To execute the autodiscovery utility, execute the macro:

```
MQAD (no parameters are required)
```

The next page shows an example of the journal which will be displayed on your home terminal:



```
*
** Executing the Insider Technologies MQSeries AutoDiscovery Facility **
*
** Checking for a valid RUNMQSC file
*
** Checking for old MQSQLIN and MQSQLDEL files
```

At this point in the flow, if the old files exist, they will be deleted and the current files renamed to the old file name.

```
*
** Deleting old Work files
*
** Starting up the Editor and creating new MQSQLIN & Work files
*
** Inserting Reflex 80:20 Status Monitor MQ Groups and Links
*
** Processing the MQSINI file
*
** Removing the duplicate Queue Managers
*
** Retrieving the MQ Queue and Channel information
*
*   Manager Process x discovered
*       Queue y discovered
*       etc....
*       Channel z discovered
*       etc....
** Closing Down the Editor
*
** Deleting old Work files
*
```

At this point in the flow, if the work files exist, they will be deleted.

```
*
** MQSeries AutoDiscovery Complete
*
** To complete the Reflex 80:20 MQSeries install
*   a) Load up the SQL defines; RUN RSQLDEFS
*   b) Execute an SQLCI / IN MQSQLIN / command
```



MQAD SQLCI Processing

The MQAD macro creates two files in your "current" subvolume.

Note: If you have logged on as a Secure User to allow MQAD to execute RUNMQSC, please ensure that this user has write access to the Reflex 80:20 Database.

Alternatively, re-secure the MQSQLIN file to the owner of the Reflex 80:20 database and then logon as that user.

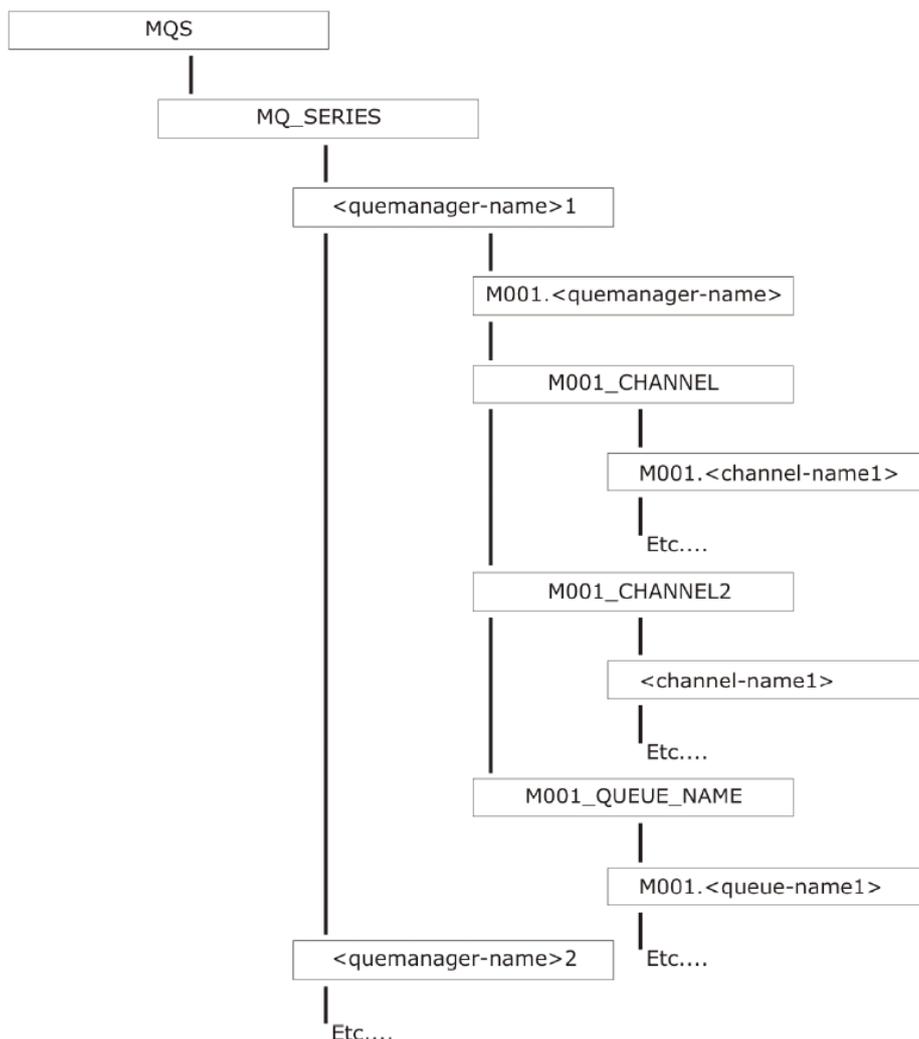
MQSQLIN contains the SQL script that needs to be executed to create the Object database and the Status Monitor tree. The previous version of this file is held in MQSQLIN2.

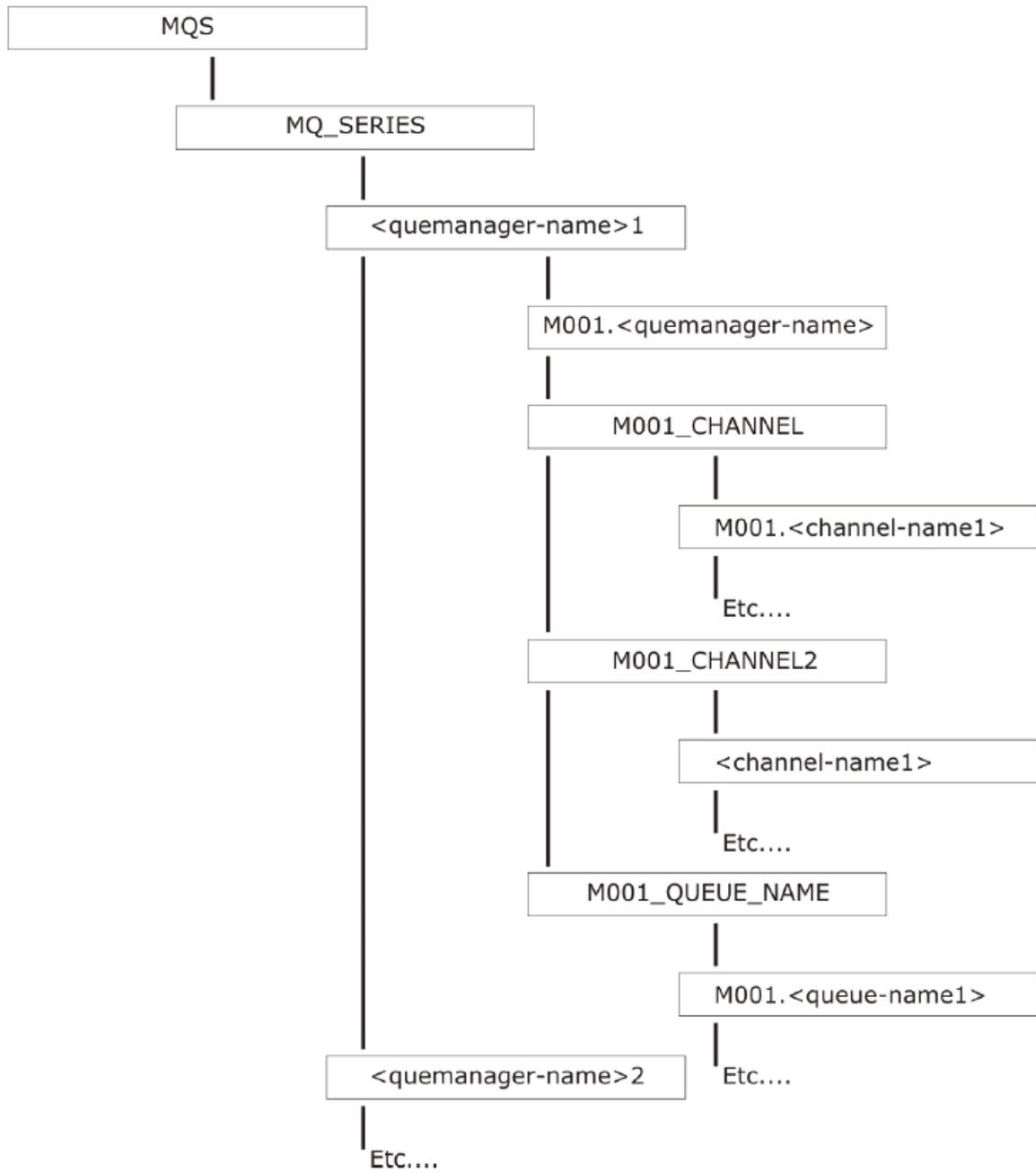
MQSQLDEL contains the SQL script that can be used to remove MQSERIES Objects and the graphical tree. To create the object database:

- Load up the SQL Defines: RUN RSQLDEFS
- SQLCI / IN MQSQLIN /

Once the database has been updated by the MQAD utility, a warmboot of the Status Monitor facilities is required. This can be achieved through the GUI or the RFLXCOM utility.

The graphical tree that is created will be displayed in the following format:







10. SNMP Gateway

SNMP Gateway

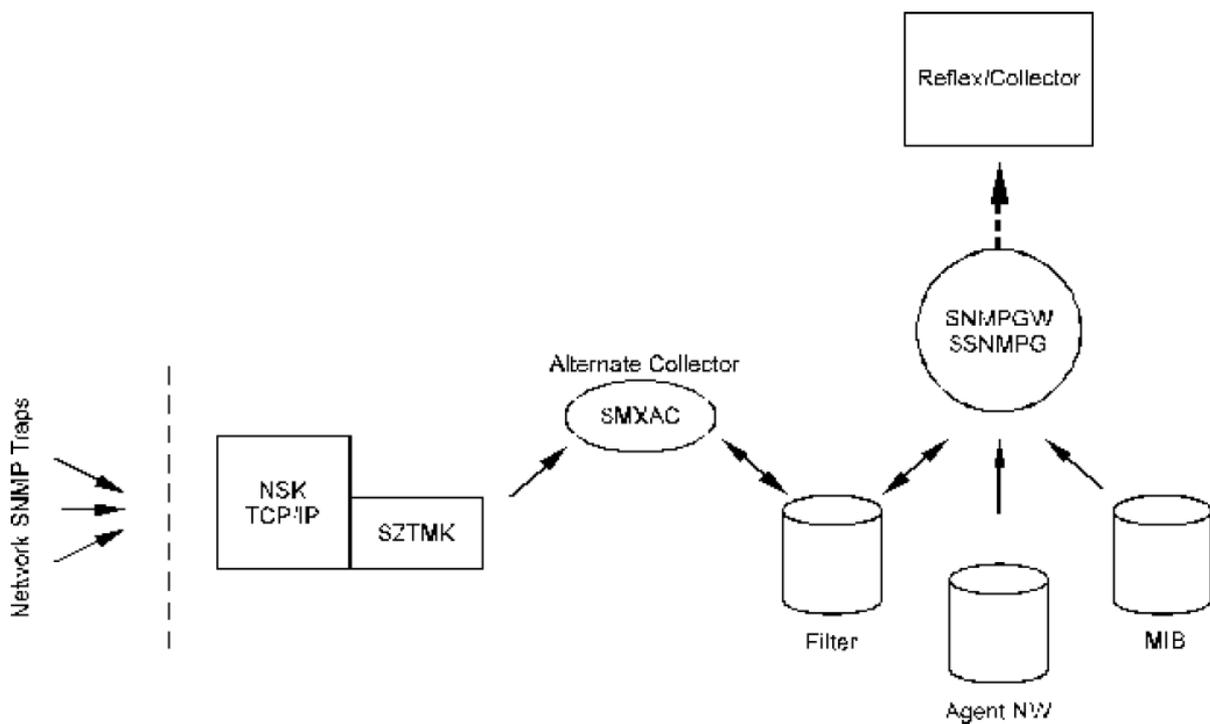
This section described defines the installation and configuration procedures for the SNMPGW product.

The application requires D30 OS or above, TCP/IP subsystems, SNMP Agent and SNMP Multiplexor software to be available.

The SNMP Gateway translates the SNMP events generated by HPE NonStop's SNMP MUX application into more meaningful Reflex 80:20 supplied EMS events.

Central to the application is an ASN.1 parser which translates OID's against an enterprise MIB and variable information (Label, Description and Values). The SNMPGW application will also substitute verbose descriptions for internet addresses to allow operators to swiftly identify which agent is emitting a particular trap.

The application during start-up, first reads in a nominated agent file containing locations of the required MIB definitions. The application then waits for writes to a specified alternate collector (\$MXAC in the diagram below). The translated events are reported to the Primary Collector \$0. NonStop subsystems are decoded and associated descriptions and variable names are parsed from a loaded MIB file.



SNMPGW Process Interaction



Installation

The software is delivered on two sub-volumes:

1. **SNMPGWV11** - The application and initialisation files, containing the following files:
 - SNMPGW SNMP - Gateway application
 - RUNTPD - Start-up script for SNMPGW
 - HOSTS - Example format hosts file
 - FILTOBJ - Sample filter object file
 - FILTSRC - Sample filter SRC file
 - FILTMAC - Sample filter macro file
2. **GWMIBSV11** - MIB loading and control subvolume, containing the following file:
 - GATEWAY MIB definition file

ZTCPIP Services File

RFC1155	MIB File
RFC1213	MIB II definitions messages
EVENTGW	SNMPGW customised text file

The trap multiplexor collects traps on port 162.

It should be checked that the following entry is available in the services file. This would usually be '\$SYSTEM.ZTCPIP.SERVICES'.

snmp	162/udp
------	---------

Agents Host File

The SNMPGW application uses entries in either the system host file or a duplicate file as a first point of reference to add an internet host description. The file is read in the same format as the systems hosts file '\$SYSTEM.ZTCPIP.HOSTS' and can substitute descriptions held as comments in a file similar to the TCP/IP hosts file.

An existing system hosts file can be copied to the default SNMPG disk volume.

Up to 25 characters of text can be used to describe the network device emitting the trap. If no text comment is available then the original internet address will be used. If the host file is not specified then the application will attempt to use native internet resolving methods. This will use either the usual hosts file '\$system.ztcip.hosts' or DNS where the service is set up.

The define TCPIP^HOST^FILE must be set to alias the system hosts file. This can be checked by typing the PARAM command in the start-up TACL. If the variable TCPIP^HOST^FILE is set the value will be displayed.



SNMP OUT

Reflex has the ability to translate EMS messages to SNMP traps. This translation and forwarding to the SNMP agent is controlled by Reflex 80:20. SNMP Trap messages are used to inform the management applications of events occurring on the managed systems. The managed resources are represented by data which held in a logical Management Information Base (MIB) on the managed systems.

The MIB also describes the Trap messages which can be generated by the managed systems. The MIB is partitioned into different types of data. A number of standard MIB definitions describe standard managed resources, such as the Internet protocol handlers. Proprietary definitions are described in an "enterprise" specific area of the MIB. Each enterprise is allocated an "enterprise identifier" which defines a sub-tree of the MIB in which the enterprise can define its own data and traps.

The main elements of the SNMP Trap message are

Component	Description
<i>PDU type</i>	Identifies the PDU (Protocol Data Unit) as a TRAP PDU
<i>enterprise</i>	Identifies where the TRAP is defined in the MIB. This is a SNMP OID (Object Identifier) for a node in the MIB.
<i>agent-addr</i>	The internet address of the object which generated the TRAP.
<i>generic-trap</i>	A number indicating the generic type of the TRAP. May be one of: coldStart, warmStart, linkDown, linkUp, authenticationFailure, egpNeighborhoodLoss, enterpriseSpecific. This field will always be enterpriseSpecific in the TRAP PDUs generated by SNMP/Out.
<i>specific-trap</i>	A number identifying the type of TRAP within the specific trap class. In the case of an enterpriseSpecific TRAP this will be relative to the enterprise identifier.
<i>time-stamp</i>	A time stamp of the time the TRAP was generated.
<i>variable-bindings</i>	A set of variables. The variables are defined in the definition of the TRAP in the MIB. A variable consists of a SNMP OID representing the name and type of the variable, plus the value of the variable.

The *variable-bindings* for the SNMP/Out traps are defined as follows:

```
VARIABLES {
    trapOwner,
    trapValue,
    trapSubject,
    trapProcess,
    trapGenerationTime,
    trapCritical,
    trapMgrName,
    trapText }
```

where the SNMP variables correspond to the equivalent EMS event tokens.



These variables have the following types:

trapOwner	DisplayString (SIZE (1..10))
trapValue	DisplayString (SIZE (1..6))
trapSubject	DisplayString (SIZE (1..50))
trapProcess	DisplayString (SIZE (1..50))
trapGenerationTime	DisplayString (SIZE (19))
trapCritical	DisplayString (SIZE (1..14))
trapMgrName	DisplayString (SIZE (1..32))
trapText	DisplayString (SIZE (1..1000))

where DisplayString is an SNMP macro used to define strings which may be displayed in a user interface.

A MIB has been defined for EMS events in the Insider Technologies Limited part of the MIB. Sub-branches of this part of the MIB are used to identify the subsystem generating the EMS events.

The function of the SNMP/Out module is to translate selected EMS events into Trap messages which are sent to the SNMP management application. The SNMP Trap messages identify the subsystems originating the EMS events. The Trap's specifictrap field identifies the type of EMS event. Selected EMS tokens are translated to SNMP variables in the Trap messages.

The HPE NonStop SNMP Agent must be installed and configured on the system. See the SNMP Agent manual for details.

The alias SNMPAGNT must be assigned to the name of the SNMP Agent process. This can be accomplished using the File Alias view in the Reflex Admin module.

SNMP/Out generates SNMP Traps from EMS events by translating the EMS Subsystem Name to a branch in the EMS event sub-tree of the MIB. The branches are identified by a unique number between 1 and 32000. The translation is accomplished by associating the unique integer with the subsystem's name in the SNMPDET file. This file is pre-configured with the most common subsystem names and associated integers. However if the user wishes to generate traps from EMS events generated by subsystems not included in the table then it is necessary for the user to carry out the following procedure:

1. Allocate a unique integer for the new subsystem.
2. Modify the SNMPDET file to contain the subsystem's name and the integer assigned to it. This is carried out by using the SNMP Trap tabbed view in the Admin module.



MIB File

The MIB Gateway file is used to map specific MIBs to EMS identifiers. The file must exist and always contain entries for 'SMI' and 'MIBII' which are defaults. The following is an example of a MIB file:

```
// ITL SNMP Gateway Version 1
// _____
// 12/9/1996
// This file defines the initialization parameters for
// the SNMP gateway.
// Statements of the form
// <MIB-name> <file-name> { <Enterprise OId> <MIB Value> }
// define files containing MIB definitions. The statements are
// terminated by a new line, and the fields of the statements are
// separated by spaces. { <Enterprise OId> <EMS Value> } is optional.
// Where these fields are in a statement they assign an EMS value to
// the associated Enterprise Object Identifier. Comments can be
// included by using "//". The remainder of the line will be ignored.

SMI $D.GWMIBS.RFC1155
MIB-II $D.GWMIBS.RFC1213
MultiTech $D.GWMIBS.Multi1 1.3.6.1.4.1.995 1
Cubix-BC-MIB $D.GWMIBS.Bc 1.3.6.1.4.1.708.1.6 2
Cubix-Ies-MIB $D.GWMIBS.Ies2 1.3.6.1.4.1.708.1.7 3
LAN-MGR2-MIB $D.GWMIBS.Lmmib2 1.3.6.1.4.1.77.1 4
ISOCOR-MIB $D.GWMIBS.Isosmtp 1.3.6.1.4.1.1427 5
WINDOWS-MIB $D.GWMIBS.Wins 1.3.6.1.4.1.311.2 6
MS-DHCP-MIB $D.GWMIBS.Dhcp 1.3.6.1.4.1.311.3 7
```

The loading of MIB files is reported at the operator console.

Where a MIB file is not available an error message is output to EMS.

Note: that Reflex 80:20 uses the EMS value and EMS event number to identify uniquely the event generated by the SNMP Gateway. Therefore it is essential that the EMS MIB value in the GATEWAY file is the same as for the Reflex 80:20 event database.

Preparing the Filter

Filters provide a means of limiting the EMS messages read from the HPE NonStop Trap Multiplexor. A filter can be compiled to only enable specific tokens to be read. An example of a filter follows:

```
Filter trapmux^filt;

BEGIN

    IF ZSPI^TKN^SSID = SSID (TANDEM.185.0) and ZTMX^TKN^TRAP^ENTERPRISE =
    "1.3.6.1.4.1.995"

    THEN PASS;

END;
```

This filter will only pass on buffers that are from the Trap MUX and have an enterprise value of 995.



MIB File

The filter is compiled by loading in the DDL definition used by the filter.

For example:

```
LOAD / keep 1 / $SYSTEM.ZSPIDEF.ZSPITACL
LOAD / keep 1 / $SYSTEM.ZSPIDEF.ZEMSTACL
LOAD / keep 1 / $SYSTEM.ZSPIDEF.ZTMXTACL
EMF / in FILTSRC/ SNMPFO
```

where:

FILTSRC is the filter source code and SNMPFO is the filter object file.

Alternate Collector

An alternate collector is required for the HPE NonStop Multiplexor to write tokenised events to and for the SNMPGW process to read events from.

The alternate collector is generated by defining a sub volume for log files and issuing the following command:

```
EMSACOLL /NOWAIT, NAME $MXAC/ LOGSUBVOL $DISK.AVOL.SNMPACOL, SECURITY "NNNN"
```

Reflex 80:20 EventCX Configuration

The SNMPGW product is distributed with a customised text file that can be appended to the usual Reflex 80:20 EventCX file. The following describes how this is achieved.

Go to the Reflex 80:20 'OBJECT' subvolume:

If the 'EVENTCX' file is not in an opened state it may be updated by:

```
>FUP COPY EVENTGW, EVENTCX
```

This may be checked via the command 'FUP LISTOPENS EVENTCX'.

Alternatively, when the file is open the following applies:

```
>OBEY STOPRFLX
```

Stops the Reflex 80:20 environment

```
>FUP COPY EVENTGW, EVENTCX
```

Appends the SNMPGW distributed customised text file to the Reflex 80:20 customised text file.

```
>OBEY RUNRFLX
```

Starting the SNMPAgent

Prior to starting the trap multiplexor the agent should be running. To start the SNMP agent the following command can be used:

```
RUN SNMPAGT / NAME $ZSNMP, NOWAIT/
```



Starting the SNMP Multiplexor

A complete explanation of how to start the trap is given by the Trap Multiplexor manual.

The following example command starts the trap multiplexor using the standard SNMP port for receiving traps. The multiplexor must be started as a member of the super user group (255,*).

```
RUN SNMPTMUX / NAME $ZTMX, NOWAIT / -a $ZSNMP -t $ZTCO -c $MXAC
```

Configuration Arguments:

-a	The SNMP agent process
-t	If it is required to monitor from. If it was required to monitor from two TCP/IP processes then the argument would be: -t (\$ZTC0, \$ZTC1)
-c	The EMS collector process to receive events generated by the SNMP Multiplexor.

Starting the SNMPGW Application

To run the application the following command line is issued:

```
RUN SNMPGW -c collector name -f filter name -d debuglevel -h inetagentfile -m $D.MIBGW
```

Once the application is running, EMS messages from the NonStop Trap Multiplexor will be translated and output to the primary collector \$0.

Argument	Description	Optional	Default
-c	Multiplexor collector	N	\$MXAC
-f	Compiled filter	N	FILTOBJ
-d	Debug level 0 to 4	Y	0
-h	Hosts file	Y	HOSTS
-m	Gateway file location. The default is the current sub-volume	Y	GATEWAY

Start-up messages are written to the system console and \$0.

OID Translation Rules

ASN.1 OID references are decoded to the last OID digit. Where the last OID digit is an index into a table or is the value 0 the parent node details is used.



Reflex SNMP Traps

The SNMP-OUT Pathway Server provides the Reflex user with the ability to report events occurring in a Reflex managed system to an alien System Management regime, such as HPE OpenView.

SNMP-OUT provides connectivity to the widest possible range of Management systems by using the SNMP (Simple Network Management Protocol) standard.

SNMP-OUT provides this facility by giving the Reflex user the ability to specify which EMS events will generate SNMP Trap messages. The events selected by the user are sent to the SNMP-OUT process, which translates the EMS event to a corresponding SNMP Trap message.

Before any SNMP Traps can be fired, the SNMP-OUT Pathway Server needs to be running in the Reflex Pathway environment. If it's not currently running, it will need to be started by issuing the command '**START SERVER SNMP-OUT**' in the Pathway environment.

Note: The server may well be frozen as standard. If so, then thaw and start it in the STARTSRV file, located in the RFLXOBJ subvolume.

The SNMP Trap tabbed view in the Administration Module displays information on subsystems that currently have an SNMP trap assigned. The SNMP Trap screen allows a unique number to be assigned to each subsystem owner name for which SNMP Traps are to be generated from Reflex. This is necessary as the name itself cannot be used as a branch in the Trap MIB (Management Information Block).

The user should set up a unique number for each subsystem owner on the HPE NonStop system that the user intends to generate traps from, for example:

```
TANDEM = 1           INSIDER = 2           ITLTECH = 3
```

This is necessary, as the alphabetic name itself cannot be used as a numeric branch in the Trap MIB.

Selecting the SNMP Trap radio button in the Reaction Module marks an Action Group for SNMP forwarding. When the event associated with the SNMP Trap mapping occurs, it will be forwarded to the trap destination endpoint defined by the HPE NonStop SNMP agent.

If SNMP Traps are no longer required for a particular Action Group then selecting the SNMP Trap radio button and selecting the 'Yes' option followed by a Warmboot will turn the Traps off.



11. Windows Services

Overview

This section concerns itself with specific alerts being relayed to TIVOLI, BMC Patrol, email, SMS, Sentra, or HPE Openview. In order for this alerting mechanism to be enabled, a Reflex 80:20 service should be installed on a nominated Windows server. The software is included in the GUI Client installation script and appropriate licences need to be in place in the Reflex 80:20 application in order for each alert type to be used.

REGISTRY SETTINGS

Server Installation/operation

The Reflex 80:20 Server and the Reflex 80:20 TEC Event Adapter are implemented as Windows Services.

They may be installed via the Reflex 80:20 Installation Script. Following installation they may be started/stopped via the Windows Control Panel Services applet. Default settings are written to the Registry. These settings may be subsequently altered by the customer and any altered settings are only activated when the service is restarted.

Reflex 80:20 Windows Server Registry Settings

TIVOLI specific settings

Some important Tivoli-specific settings for the Reflex 80:20 Windows server are described below (unless otherwise specified, values are 1 = On, 0 = Off):

HKEY_LOCAL_MACHINE:SYSTEM: CurrentControlSet:Services:RflxNTServSvc:

SERVER_ACTIONS

MONITOR_CLIENT_ACTIONS - specifies whether to generate client status events (connected, disconnected, heartbeat_missed, heartbeat_resumed).

MONITOR_SERVER_ACTIONS - specifies whether to generate server status events (running, stop_pending).

PERFORM_TIVOLI_LOGFILE_WRITE - specifies whether to generate events for TEC.

SERVER_SETTINGS

MAX_HEARTBEAT_INTERVAL_SECS - specifies number of seconds between events before it is deemed that the client heartbeat has been missed (causing a heartbeat_missed event to be generated).

MAX_NUM_MISSED_HEARTBEATS - specifies how many consecutive heartbeats should be missed before a further heartbeat_missed event is to be generated.

PORT_NUMBER - specifies the port number upon which the RflxNTServSvc will listen for client connections (default 4913).

TIVOLI_EVENT_MAPFILE_SETTINGS

PATH - specifies path to MAP file (see Event Class Mapping below); default value is INSTALL\TivoliConfig\RFLXMAP, where INSTALL is the directory into which Reflex 80:20 is installed. * See footnote

TIVOLI_LOGFILE_SETTINGS

PATH - specifies path to logfile; default value is INSTALL\TivoliConfig\RFLXLOG, where INSTALL is the directory into which Reflex 80:20 is installed. * See footnote

* For 32-bit machines, this is C:\Program Files\Reflex\<version> and on 64-bit machines, this is C:\Program Files (x86)\Reflex\<version>. For example: C:\Program Files (x86)\Reflex\v4.8.



ROLLOVER_SIZE(KB) - specifies the size at which the logfile will be "rolled over", i.e. will be renamed with the next available suffix e.g. RFLXLOG.0, RFLXOG.1 etc. and a new RFLXLOG file will be generated.

ROLLOVER_MAX_INSTANCES - specifies the maximum number of rollovers that can occur; if value is 0 then rollover feature is disabled; if value is > 0, then when the maximum number of rollovers has occurred, the RFLXLOG file will continue to grow rather than being rolled over.

Reflex 80:20 TEC Event Adapter Registry Settings

The Reflex 80:20 TEC Event Adapter comes in three flavours:

NonTMEReflexAdapterSvc.exe (NonTME)

TMEReflexAdapterSvc (TME-Endpoint)

MNReflexAdapterSvc.exe (TME-ManagedNode)

Refer to the Tivoli Enterprise Console Adapter's Guide for an explanation of the distinction between these flavours.

The user may select any combination of flavours during the execution of the Reflex 80:20 Install Script.

The settings for the various flavours of Reflex 80:20 TEC Event Adapter are similar to those of the Reflex 80:20 Windows Service described before, except that there are no **TIVOLI_LOGFILE** settings and there is an additional **SERVER_SETTINGS** value as described below:

HKEY_LOCAL_MACHINE:SYSTEM:CurrentControlSet:Services:NonTMEReflexAdapterSvc:

SERVER_SETTINGS

CONFPATH - specifies path to .conf file. The default value is: INSTALL\TivoliConfig\NonTMEReflexAdapterSvc.conf, where INSTALL is the directory into which Reflex 80:20 is installed. * See footnote.

See the Tivoli Enterprise Console Adapter's Guide for a description of the settings which may be contained in a .conf file.

Event Class Mapping

Successful Event Class Mapping (i.e. the mapping of Reflex 80:20 HPE NonStop events to instances of Event Classes that can be monitored by TEC), depends upon the following:

1. The definition of Tivoli Reactions – refer to the earlier part of this appendix.
2. The ability of the Reflex 80:20 TEC Adapter (or Reflex 80:20 Windows server) to recognise the events relayed to it by Reflex 80:20 as a result of those Reactions – refer to Map File.
3. If Reflex 80:20 Windows server is used, the ability of the TEC Logfile adapter to understand the Reflex 80:20 logfile – refer to Logfile and Logfile Format File.
4. The ability of the TEC Console to recognise the events forwarded to it by the Reflex 80:20 TEC Adapter (or the TEC Logfile adapter) – refer to Baroc File.

Baroc File

The event classes used in Reflex 80:20 TEC Integration are defined in the RFLX.BAROC file which is installed in the directory INSTALL\TivoliConfig\ where INSTALL is the directory into which Reflex 80:20 is installed. * See footnote.

* For 32-bit machines, this is C:\Program Files\Reflex\



The basic event classes used in Reflex 80:20 TEC Integration fall into two categories:

- *Events describing the status of the Reflex 80:20 Windows server or Reflex 80:20 TEC Adapter and the connection status of its Reflex 80:20 NonStop client(s).* These events are self-explanatory and are mapped to event classes derived from the hierarchical classes RFLX_EVENT_SVRADAP_STATUS_Base and RFLX_EVENT_SVRADAP_CLIENT_STATUS_Base.

Note: generation of these events may be optionally enabled/disabled via the Reflex 80:20 Windows server or Reflex 80:20 TEC Adapter Registry settings.

- *Events incoming from Reflex 80:20 NonStop client(s).* These events all have the same basic structure and are mapped to event classes derived from the hierarchical class RFLX_EVENT_Base. An essential feature of these events is the presence of the following "event tokens": ssid_owner, ssid_subsystem, event_number. These tokens are important, since taken together they allow an event to be categorised.

Map File

The Reflex 80:20 Windows server or Reflex 80:20 TEC Adapter, maps events incoming from Reflex 80:20 NonStop client(s) to specific event classes.

To do this, it uses mappings derived by reading at startup the event mappings file RFLXMAP which is installed in the directory INSTALL\TivoliConfig\, where INSTALL is the directory into which Reflex 80:20 is installed. * See footnote.

Each line in the **RFLXMAP** file maps a combination of ssid_owner, ssid_subsystem, event_number values (* represents a wildcard) to a specific event class in the RFLX.BAROC file.

Note: the columns are tab-separated.

Logfile and Logfile Format File

The Reflex 80:20 Windows server implementation generates a logfile, which by default is called RFLXLOG. The file RFLX.FMT contains format specifications enabling the TEC Logfile Adapter to read the logfile and pass the events to TEC.

Note: "long" and "short" format specifications are given for each class. This is because the user has the option, when initially configuring the Event via the Reflex 80:20 GUI, to nominate a "short" event (in which case certain tokens are not used) or a "long" event (in which case those tokens are used).

RFLXLOG and **RFLX.FMT** are, respectively, generated and installed in the directory INSTALL\TivoliConfig\ where INSTALL is the directory into which Reflex 80:20 is installed. * See footnote.

Customer-specific Event Specialisation

Customer-specific Event Specialisation may be achieved by amending (or replacing) the RFLX.BAROC, RFLX.FMT, and RFLXMAP files.

Note: if the name/location of the MAP file to be used is other than the default, then it will be necessary to update the Reflex 80:20 Windows Server/Reflex Adapter registry settings.

The Reflex 80:20 Windows Server/Reflex Adapter must be stopped and restarted in order to use the new/amended mappings.

The new/amended BAROC (and FMT file if used) must be re-imported/distributed to the Tivoli environment – see Tivoli documentation.

* For 32-bit machines, this is C:\Program Files\Reflex\<version> and on 64-bit machines, this is C:\Program Files (x86)\Reflex\<version>. For example: C:\Program Files (x86)\Reflex\v4.8.



Auto-generation of Event Specialisation Files

The Reflex 80:20 GUI's Tivoli Event Class Definition dialogue facilitates the auto-generation of BAROC, FMT, and MAP files tailored to the user's specific needs. See the Reaction module within the GUI on-line help for a breakdown of these files.

Manual Amendments

Minor amendments, such as the additional definition of a new Event Class, may be performed manually by using a text editor.

Note: Any new Event Class must be appended to the BAROC file, must be derived from the RFLX_EVENT_Base, must not introduce new slots and requires that corresponding entries be appended to the MAP file (and FMT file if using the TEC NT Logfile Adapter). The structure of the format specifications in the FMT file may not be altered.

For example, suppose a new Tivoli Reaction had been configured for the following Event and it was desired to add a corresponding new Event Specialisation.

```
SSID_Owner    INSIDER
SSID_Subsystem 50
Event Number  2553
```

First, choose a meaningful, unique name for the event, e.g. RFLX_CPUPercentBusyThresholdExceeded

The following line should then be added to the RFLX.MAP file (note that in this file the columns are tab-separated):

```
RFLX_CPUPercentBusyThresholdExceeded  INSIDER 50 2553
```

The following lines should be appended to the RFLX.BAROC file

Note: Tivoli requires there to be a blank line after the ';' and also after the 'END'

```
) ;
#RFLX_CPUPercentBusyThresholdExceeded
TEC_CLASS :
RFLX_CPUPercentBusyThresholdExceeded ISA RFLX_Event_Base;
END
```

If the TEC Logfile Adapter is to be used, then the following lines should be appended to the RFLX.FMT file.

```
FORMAT RFLX_CPUPercentBusyThresholdExceeded FOLLOWS RFLX_Event_Base_Short
%t %s %s %s %s short %s %s %s %s
RFLX_CPUPercentBusyThresholdExceeded %s*
END
FORMAT RFLX_CPUPercentBusyThresholdExceeded FOLLOWS RFLX_Event_Base_Long
%t %s %s %s %s long %s %s %s %s %t %s %s
RFLX_CPUPercentBusyThresholdExceeded %s*
END
```



SMS Alerts

This section details both the Windows server front end and NonStop backend requirements for enabling SMS (Short Message Service) alerts from Reflex 80:20. These SMS alerts will be raised as a result of Reflex 80:20 Reaction configured EMS events which have been nominated as requiring further investigation by IT personnel. In order to activate SMS paging, a number of basic steps need to be carried out.

What follows are instructions for installing the SMS module on a Windows server. Also included are the configuration instructions for the HPE NonStop node and within the Reflex 80:20 GUI.

The SMS module contains a distributable licensed product called Message Master™ which houses the various protocols that can be selected for communicating with recognised mobile phone service providers as well as normal pagers.

Prior to configuring your SMS workstation software, ensure that the Reflex 80:20 environment on your HPE NonStop system is configured to alert to an Enterprise Manager. This information is contained within your RUNEMON file (located in your Reflex 80:20 object subvolume, e.g. RFLXOBJ).

Edit your RUNEMON file and ensure the RUN evntmon command line contains parameter ENT-MGR - see example below:

```
RUN evntmon / name [emon_name] , nowait, IN [home_term],      &
OUT [home_term] / backup^cpu 0, PAGEGEN [pagegen_name] ,    &
CEGEN [cegen_name] , SERVER^QUEUE 5000,                    &
ENT-MGR REMOT-BMC-REACT
```

The above RUN command is contained at the end of the RUNEMON file.

IMPORTANT: The SMS/Paging product used by Reflex 80:20 is called MessageMaster and can cause intermittent windows dialog lockout problems, e.g. unable to close certain dialogs, slow start-up of certain windows dialogs. The software does not affect running processes on the Windows Server. It is necessary that this software is run on a Windows server that has been nominated as one which does not run applications/programs critical to the operation. A dedicated Windows server or one which runs non-critical applications should be the elected choice for SMS/Paging via Reflex 80:20.

IMPORTANT: You need 'Administrator Level' access to install/start 'RflxNTServSvc'.

Windows Server Installation and Considerations

The user will have received an '.exe' file on a supplied Reflex 80:20 CD-ROM. This will have a name of 'XFPddmm.EXE', where 'ddmm' represents the day and the month of the release.

This '.exe' file contains both the Reflex 80:20 GUI and the SMS alerting module.

Preliminary steps for enabling SMS alerting:

1. If not done already, on the nominated Windows server for SMS alerting, go to Control Panel\Modems to configure a modem to dial externally. A V.90 modem is recommended.

Note: Ensure your modem is configured with appropriate drivers to ensure 'handshaking' via Message Master™ is successful. It may also be worthwhile to initially set your modem speed to 9600bps.

2. Double click on this XFP '.exe' file.
3. The user may be prompted with the following message 'Version Vn.n of Reflex 80:20 is already installed. Do you wish to overwrite this version?'. Click '**OK**' to this message.



Windows Services

4. Click '**Next >**' to proceed to the next stage of the installation script.
5. Select the 'Destination Directory' for installing the SMS alerting module and proceed to the next step by clicking '**Next >**'.
6. **Uncheck** the install box for 'Reflex 80:20 Client GUI using Fastpipe'.
7. **Check** the install box for 'Reflex 80:20 Windows Services' and proceed to the next step by clicking '**Next >**'.
8. Select **SMS** from the RflxNTServSvc Actions screen then proceed to the next step by clicking '**Next >**'.
9. Select **GSM** then proceed to the next step by clicking '**Next >**'.
10. Click '**Next >**' again to begin the install.
10. Click '**Finish**' to end the install.
11. Restart the Windows server by clicking '**OK**'.

The Reflex 80:20 Windows service for receiving SMS alerts from the NonStop node has now been activated. To confirm that this is the case, carry out the following steps:

1. Navigate to the Services applet for the Windows platform.
2. Scroll down the services list on the left side of the window to find the service 'RflxNTServSvc', which should have a status of 'STARTED' and a start-up set to 'AUTOMATIC'. If the service is not started, select 'RflxNTServSvc' and select 'Start'.

See example below:

Service Name	Description	Status	Start Type	Path
Protected Storage	Provides protecte...	Started	Manual	Local Syste..
Quality Windows Audio Vi...	Quality Windows ...		Manual	Local Servic...
ReflexNTServSvc	Reflex: Provides m...	Started	Automatic	Local Syste..
Remote Access Auto Conn...	Creates a connecti...		Manual	Local Syste..
Remote Access Connectio...	Manages dial-up ...		Manual	Local Syste..
Remote Desktop Configura...	Remote Desktop ...	Started	Manual	Local Syste..

3. Closedown the Services applet using the 'CLOSE' button.

Within the Windows directory into which the SMS module was installed will be an executable with the following name: 'MMCfg.exe'. Carry out the following steps:

1. Double click the Message Master configuration utility (MMCfg.exe) from the appropriate directory. * See footnote.
2. Click on 'Message-Master Modem/ISDN' and select Configuration.

* For 32-bit machines, this is C:\Program Files\Reflex\<>version> and on 64-bit machines, this is C:\Program Files (x86)\Reflex\<>version>. For example: C:\Program Files (x86)\Reflex\v4.8.



Windows Services

3. In the **Dial parameters and modem device** dialog tab, select your modem from the Device list, ensuring it matches that installed on your Windows platform.
4. Select the **Send Options** dialog tab and change the retries value to 5.
5. In the **Send Options** tab, ensure "Check Messages for Invalid Characters" and "Replace invalid characters automatically" are selected. This allows the NonStop EMS event manager tokens to be issued to SMS. If this option is not selected, then Message Master™ will not forward EMS event manager tokens. **Note:** If selected, then the backslash from the manager token is not included, e.g. \INSIDER.\$ABCD is sent to SMS as INSIDER.\$ABCD (This is due to a Message Master™ restriction).
6. After updating the **Send Options** tab, click on apply.
7. A list of pre-defined services can be viewed via the 'Defined Services' tab. Details of your particular SMS provider can be viewed by selecting the 'Properties' tab. If however, you wish to add in a new subscriber, execute the following steps:
 - a) Stop "RflxNTServSvc" Service.
 - b) Click on New.
 - c) Enter the name of your provider.
 - d) Select 'Protocol Type' from the drop down list. NB: Message Master only supports certain protocols, e.g. TAP, UCF.
 - e) Select 'Additional' tab and enter in the service provider bureau number (see other pre-defined services for examples and for examples of other values in other tabs)
 - f) After entering all details, click on apply.

To check that your new service provider has been registered, access the registry settings, search for 'Derdack', check under its 'Message-Master Services' folder, then select your new service provider.

8. If a new service provider has been added, then update your Reflex 80:20 SMSSERVICE.ini file, located in your Reflex 80:20 SMS server directory to include this new provider. An example is provided below (Vodafone (SMS) UK service provider has been added to this file):

[Vodafone SMS (UK)]
AppearInList=Y

By entering new details in SMSSERVICE.ini file, it ensures they appear in the Action Group 'Remote Alert' SMS Service list.

9. Select **OK** and **Close** to exit the Message Master configuration utility.
10. Start the "RflxNTServSvc" Windows Service.

The port number that the Windows server uses is '4913'. If this needs to be changed due to the fact that other software is using this port, then the registry should be edited as follows:

1. Click on 'Start' on the main windows toolbar.
2. Click on 'Run'.
3. Type 'regedit' and then press Return.
4. Navigate down to the following directory:

```
My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RflxNTServSvc\Parameters\SERVER_SETTINGS
```

5. Change the port number after double clicking on it.



Windows Services

6. Exit from the Registry Editor.
7. Having carried out the steps above, navigate to the Services applet for the Windows platform.
8. Stop and Start the 'RflxNTServSvc' Windows service and then close the application.

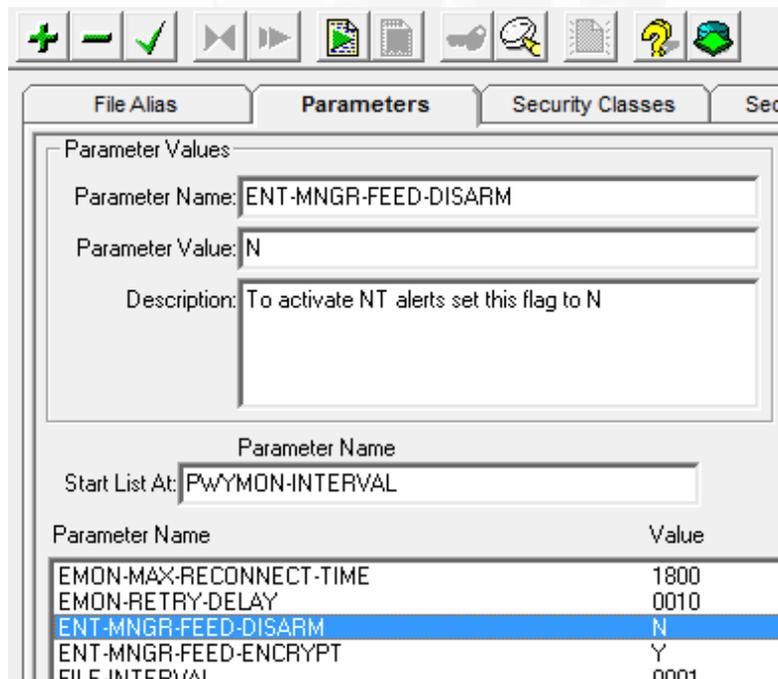
Note: For ISDN modems the number of retries is configurable in MessageMaster using mmcfg.exe. Use mmcfg.exe to set number of retries under the **SEND** option.

Before setting the number of retries, the RflxNTServSvc Windows service must be stopped and then started after the setting has been changed.

HPE NonStop Considerations

This section details the way in which an incoming EMS event on the HPE NonStop node can be configured to cause a Windows alert to be sent to the appropriate TCP/IP address and subsequently into the 'RflxNTServSvc' for the purposes of raising an SMS message. Carry out the following steps:

1. Logon to Reflex 80:20 using an assigned Guardian user.
2. Click on the Administration button on the main toolbar.
3. Navigate to the Parameters tab, double-click the ENT-MNGR-FEED-DISARM parameter and ensure the value is set to N. If changing the value from Y to N then ensure you click on the amend (green tick) button.



4. Staying in the Parameters tab, double click the 'SELECT-REMOTE- ALERT' parameter.



- Set the third and fourth flags to 'YY' to allow SMS alerts to be raised. Amend the record.

File Alias	Parameters	Security Classes	Se
Parameter Values			
Parameter Name:	SELECT-REMOTE-ALERT		
Parameter Value:	NNYYNNN		
Description:	Parameter to set the destination of remote alerts: Tivoli NT, Tivoli Tec.BMC Patrol, SMS, Sentra, Email, hpOpenView		

Note: Sites using SMS alerts will require the 3 letter mnemonic 'MME' as part of their Reflex 80:20 licence files.

- Warmboot Status Monitor by clicking on 'OD Setup' icon on the main toolbar and subsequently clicking either of the '!' icons. Acknowledge the return message by clicking 'Ok'.
- Logoff the GUI and re-login to read the new SMS setting.
- Click on the 'Configuration' drop-down menu and select 'Specify Remote Platforms', followed by the 'Reflex 80:20 NT Alerting' option.

Reflex NT Alerting

TCP/IP Port Settings (Mandatory)

Default IP Address/Port Primary Backup

Primary IP Address/Port

Backup IP/Address/Port

Switch to Backup Port if Primary fails

Optional Settings (Not applicable for SMS/Tivoli/hp OpenView Reactions)

Alert Length

Version No Previous

Version No

System Name

Manager Name

Host Type

Company Name

Provider Location

NT Server Name

Event ID

- In the basic configuration of having one Windows server with SMS alerting installed, enter in the 'Primary IP Address / Port', the address of the nominated workstation, e.g. 192.9.200.20.4913, where the last value is the port number of the workstation that you nominated earlier for the SMS service. Amend the record.

Note: If using a non-stop approach to alerting, specify a second TCP/IP address.port number and check the 'Switch to Backup Port if Primary Fails' option. Ensure that the SMS software is installed on a second Windows server.

You can also select whether to make the Primary or Backup Address / Port Number the default, e.g. if the Primary becomes unavailable for a length of time, then modify this field to make the Backup the default address / port.



Windows Services

10. The alert length field represents the length of the text message that can be sent to a mobile phone. In the case of SMS, the alert length cannot exceed 160. This value can only be amended to an appropriate value within Reflex via the use of SQLCI. In order to do this, logon as the owner of the Reflex 80:20 Pathway. Navigate to the Reflex 80:20 object subvolume and run the 'RSQLDEFS' file to load the defines.
11. The table is =CMND_POST_CONFIG_TABLE and the field to be amended is 'SCCALERT_LENGTH'. Set this field value to '160'. For more detailed instructions on how to do this, please contact Insider Technologies Limited.
11. If the SMS software has been installed and activated as a service on the appropriate Windows server then proceed with the next steps.
12. Click on the 'Reaction' button on the main toolbar.
13. Warmboot the software by clicking on the '!' on the top of this dialog and then click on the 'Warmboot Reaction Servers'.
14. Click on the Console button to view the EMS messages resulting from the warmboot operation. A message stating that a successful connection to the nominated workstation should appear on the EMS log.

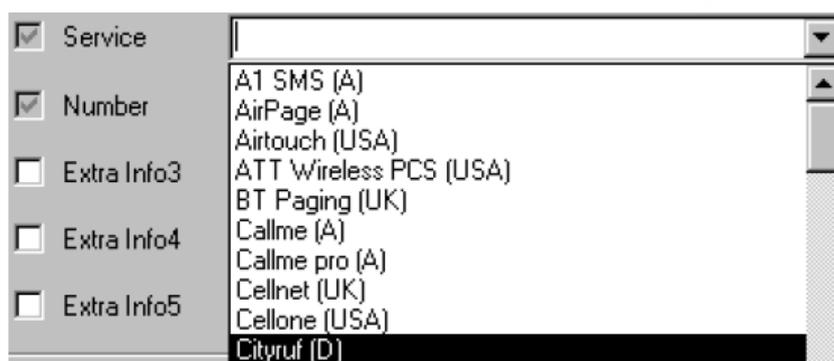
Connectivity between the HPE NonStop node and the Windows server has now been achieved.





What follows next, are instructions to set-up nominated EMS events to alert to a specified network provider.

1. With an appropriate EMS event in context within the Reflex 80:20 GUI dialog, navigate to the Action Group tab within the Reaction module.
2. Enter an **Action Group** name for your SMS reaction.
3. Click on the 'Remote Platform' attribute.
4. Click on any tokens you wish to appear in the resulting SMS message. Remember that only 160 characters of your chosen text will be displayed. Click on a check box and enter any free text you wish to appear in the SMS message.
5. It is imperative that '**SERVICE**' and '**NUMBER**' are entered as follows:
 - 5.1. **SERVICE** should be the exact name of the network provider nominated in the Windows Message Master software, e.g. Vodafone SMS (UK). It is important that this name takes account of the appropriate case and spacing specified in MessageMaster.
 - 5.2. The **NUMBER** field should contain the number of the mobile that should be called.



6. Add this record with the '+' icon at the top of this dialog.
7. Exit this SMS dialog and add the underlying Reaction record using the '+' icon.
8. In order to activate this SMS alert, click on the '!' icon on the Reaction toolbar and follow through the Generate and Compile Filter steps followed by the Warmboot. The SMS alert can be tested using the Event Test tab in the Reaction dialog.



Tivoli Alerts

This section details both the Windows front end and HPE NonStop backend requirements for enabling TIVOLI Enterprise Console (TEC) alerts from Reflex 80:20. These TEC alerts will be raised as a result of Reflex 80:20 Reaction configured EMS events which have been nominated as requiring further investigation by IT personnel by way of reporting to a TIVOLI TEC Console. In order to activate TEC alerting, a number of basic steps need to be carried out.

What follows are instructions for installing the Insider Technologies TIVOLI Adapter module on a Windows workstation. Also included are the configuration instructions for the HPE NonStop node and for the Reflex 80:20 GUI.

Windows Server Considerations

You will have received an '.exe' file on a supplied Reflex 80:20 CD-ROM. This will have a name of 'XFPddmm.EXE', where 'ddmm' represents the day and the month of the release.

This '.exe' file contains both the Reflex 80:20 GUI and the TIVOLI TEC alerting module.

Preliminary steps for enabling TIVOLI TEC alerting:

1. Double click on the XFP '.exe' file.
2. The user may be prompted with the following message 'Version Vn.n of Reflex 80:20 is already installed. Do you wish to overwrite this version?'. Click '**OK**' to this message.
3. Click '**Next>**' to proceed to the next stage of the installation script.
4. Select the 'Destination Directory' for installing the alerting module and proceed to the next step by clicking '**Next>**'.
5. **Uncheck** the install box for the 'Reflex 80:20 Client GUI using Fastpipe.'

TIVOLI Logfile approach

6. The following method is for alerting to TIVOLI, using the Reflex/ TIVOLI logfile approach by way of the TIVOLI logfile adapter (TIVOLI software), which is configured to monitor the logfile written to a Windows server.
7. Check the install box for ' Reflex 80:20 Windows Services' and proceed to the next step by clicking '**Next>**'.
7. Uncheck all check boxes on the 'RflxNTServSvc Actions' screen leaving only the '**TIVOLI**' check box selected then proceed to the next step by clicking '**Next>**'.
8. Click '**Next>**' again to begin the install.

TIVOLI TEC Adapter approach

9. If using the 'ReflexAdapterSvc', then the options '**TivoliNonTME**' and '**TIVOLI TME (Endpoint)**' will be requested. Click on the appropriate solution for your preferred configuration.

See later pages in this Technical Guide for a discussion on the two types of Reflex 80:20 TEC adapter usage.



10. Click '**Finish**' to end the install.
11. Restart the Windows server by clicking 'OK'.

The Reflex 80:20 Windows service for receiving TIVOLI alerts from the HPE NonStop node has now been activated. To confirm that this is the case, carry out the following steps:

1. Having carried out the steps above, navigate to the Services applet for the Windows platform.
2. Scroll down the services list on the left side of the window to find the service 'RflxNTServSvc', which should have a status of 'STARTED' and a start-up set to 'AUTOMATIC'. If the service is not started, select 'RflxNTServSvc' and select 'Start'.

See example below:

Program Compatibility Ass...	This service provi...	Started	Automatic	Local System...
Protected Storage	Provides protecte...		Manual	Local System...
Quality Windows Audio Vi...	Quality Windows ...		Manual	Local Service...
ReflexNTServSvc	Reflex: Provides m...	Started	Automatic	Local System...
Remote Access Auto Conn...	Creates a connecti...		Manual	Local System...
Remote Access Connectio...	Manages dial-up ...		Manual	Local System...
Remote Desktop Configura...	Remote Desktop	Started	Manual	Local Service...

3. Closedown the application using the 'CLOSE' button.

The port number that the Windows server uses is '4913'. If this needs to be changed due to the fact that other software is using this port, then the registry should be edited as follows:

1. Click 'Start' on the main Windows toolbar.
2. Click on 'Run'.
3. Type 'regedit' and then press return.
4. Navigate down to the following directory:

```
My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RflxNTServSvc\Parameters\SERVER_SETTINGS
```

5. Change the port number after double clicking on it.
6. Exit from the Registry Editor.
7. Having carried out the steps above, navigate to the Services applet for the Windows platform.
8. Stop and Start the 'RflxNTServSvc' Windows service and then close the application.

HPE NonStop Considerations

This section details the way in which an incoming EMS event on the NonStop node can be configured to cause a Windows alert to be sent to the appropriate TCP/IP address and subsequently into the '**RflxNTServSvc**', for the purposes of raising a TIVOLI alert message.

Prior to configuring your Tivoli workstation software, ensure that the Reflex 80:20 environment on your NonStop node is configured to alert to an Enterprise Manager. This information is contained within your RUNEMON file (located in your Reflex 80:20 object subvolume, e.g. RFLXOBJ).

Edit your RUNEMON file and ensure the RUN evtmon command line contains parameter ENT-MGR - see example below:

```
RUN evtmon / name [emon_name] , nowait, IN [home_term], &
OUT [home_term] / backup^cpu 0, PAGEGEN [pagegen_name] , &
CEGEN [cegen_name] , SERVER^QUEUE 5000, &
ENT-MGR TIVOLI-REACT
```



Carry out the following steps:

1. Logon to Reflex 80:20 using an assigned Guardian user.
2. Click on the Administration button on the Main toolbar.
3. Navigate to the Parameters tab (the second tab along) and double click on the **'SELECT-REMOTE-ALERT'** parameter.
4. Set the first flag to 'Y' to allow TIVOLI alerts to be raised. Amend the record.

5. Warmboot Status Monitor by clicking on 'OD Setup' icon on the main toolbar and subsequently clicking either of the '!' icons. Acknowledge the return message by clicking 'Ok'.
6. Logoff the GUI and re-login in order to read the new TIVOLI setting.
7. Click on **'Specify Platforms'** and select the **'Reflex NT Alerting'** option.

8. In the basic configuration of having one Workstation workstation with TIVOLI alerting installed, enter in the 'Primary IP Address / Port ', the address of the nominated workstation, e.g. 192.9.200.180.4913, where the last value if the port number of the workstation you nominated earlier for the TIVOLI service. Amend the record.

Note: If using a non-stop approach to alerting, specify a second TCP/IP address.port number and check the 'Switch to Backup Port if Primary Fails' option. Ensure that the TIVOLI software is installed on a second Windows server.

You can also select whether to make the Primary or Backup Address / Port Number the default, e.g. if the Primary becomes unavailable for a length of time, then modify this field to make the Backup the default address / port.



9. The alert length field represents the length of the text message that can be sent to TIVOLI. This value can only be amended in an SQLCI session on the HPE NonStop node to an appropriate value.

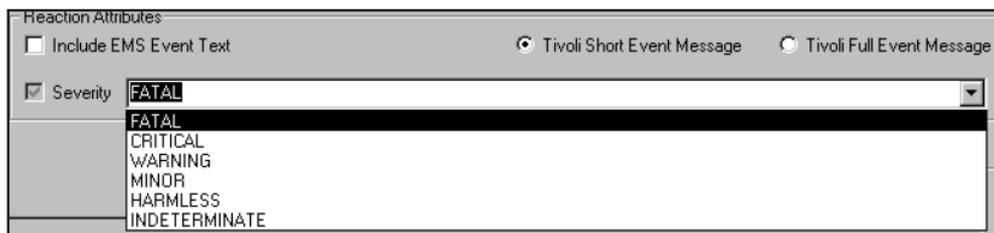
In order to do this, logon as the owner of the Reflex 80:20 Pathway. Navigate to the Reflex 80:20 object subvolume and run the **'RSQLDEFS'** file. The table is =CMND_POST_CONFIG_TABLE and the field to be amended is **'SCCALERT_LENGTH'**. Set this field value to **'1000'**. For more detailed instructions on how to do this, contact Insider Technologies Limited.

10. If the TIVOLI software has been installed and activated as a service on the appropriate Windows server then proceed with the next steps.
11. Click on the **Administration** button on the main Reflex 80:20 toolbar.
12. Navigate to the Parameters tab (the second tab along) and double click on the **'ENT-MNGR-FEED-DISARM'** parameter.
13. Set the flag to 'N' to allow TIVOLI alerts to be raised via the remote feeder mechanism. Amend the record.
14. Click on the **'Reaction'** button on the main toolbar.
15. Warmboot the software by clicking on the '!' on the top of this dialog and then click on the **'Warmboot Reaction Servers'**.
16. Click on the Console button to view the EMS messages resulting from the warmboot operation. A message stating that a successful connection to the nominated workstation should appear in the EMS log.



Connectivity between the HPE NonStop node and the Windows server has now been achieved. What follows are instructions to set-up nominated EMS events to alert to a Remote Platform.

1. With an appropriate EMS event in context within the Reflex 80:20 GUI dialog, navigate to the Action Group tab within the Reaction module.
2. Enter an Action Group name for your TIVOLI reaction.
3. Click on the 'REMOTE PLATFORM' attribute.
4. Click on whether using the short or the long message configuration.
5. Click on a severity value for the event.



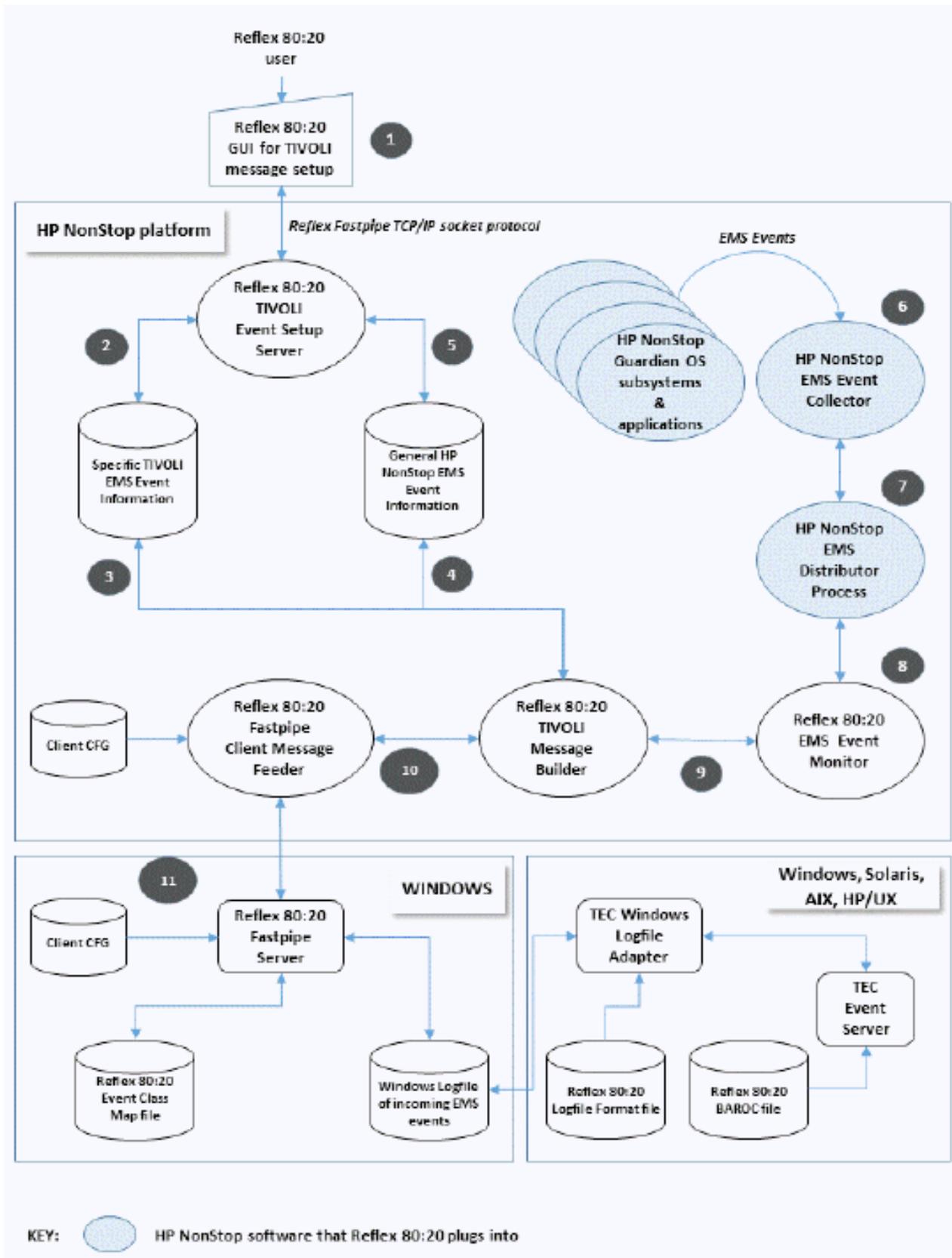
6. Leave this REMOTE PLATFORM dialog and add the underlying reaction record using the '+' icon.
7. In order to activate this REMOTE PLATFORM alert, click on the '!' icon on the reaction toolbar and follow through the Generate, Compile filter steps followed by the warmboot.

The REMOTE PLATFORM alert can be tested using the Event Test tab in the Reaction dialog.

The next few pages provides an overview of the TIVOLI integration architecture and the alternative approaches to using a TIVOLI Logfile or a TIVOLI TEC Adapter.



Tivoli Integration Architecture - Approach One





Approach One - Tivoli using a Logfile

Here is a description of the information flow in the first diagram showing the logfile approach for TEC integration:

1. The user configures which events should be reacted to via a GUI screen which talks directly to the HPE NonStop node across TCP/IP.
2. The event configuration information is written to the Reflex 80:20 database. It consists of general header data to be written in the message to Tivoli, e.g. platform name, location etc., and event specific information e.g. CPU down, Disk Path down, X25 line down and so forth.
3. Two SQL tables will hold this Tivoli event information.
4. Reflex 80:20 is continually monitoring EMS event messages logged by the various subsystems which make up the Guardian operating system, as well as other applications.
5. These events are written to an HPE NonStop Collector process and a distributor process programmatically started by the Reflex 80:20 Event Monitor is used to receive the EMS events into the event monitor process.
6. The Reflex 80:20 event monitor is the junction point to incoming events and this process ascertains which reaction has been configured for this incoming event.
7. If this EMS event is to be formatted and sent to the Tivoli TEC, then it is sent to the Tivoli message builder which extracts the required information from the SQL tables.
8. This message is then sent to a process that contains the TCP/IP socket protocol to talk to a remote platform. This process is responsible for just taking the message and relaying it to a Windows server. The protocol is proprietary, is written by Insider Technologies and is called Fastpipe™.
9. The Windows platform is executing a server which receives the incoming message. This server also contains the TCP/IP socket protocol Fastpipe™. Using files prepared for event formatting, the server writes the message in the required format to the logfile. The TEC Logfile Adapter is then used to forward those events to the TEC console via the TEC Event Server.

Approach Two - Tivoli using an Reflex 80:20 TEC Event Adapter

Here is a description of the information flow in the second diagram showing the Reflex 80:20 TEC Event Adapter approach for Tivoli integration (foundation level):

1. Steps 1 through 8 are as above.
2. This message is then sent to a process that contains the TCP/IP socket protocol to talk to a remote platform. This process is responsible for just taking the message and relaying it to the Reflex 80:20 TEC Event Adapter. The protocol is proprietary and is written by Insider Technologies and is called Fastpipe™.
3. The events received by the Reflex 80:20 TEC Event Adapter are written to the TEC Event Server.



BMC Patrol Alerts

This section details both the Windows front end and HPE NonStop backend requirements for enabling BMC Patrol alerts from Reflex 80:20. These alerts will be raised as a result of Reflex 80:20 Reaction configured EMS events which have been nominated as requiring further investigation by IT personnel by reporting to the BMC Patrol console. In order to activate these particular alerts, a number of basic steps need to be carried out.

What follows are instructions for installing the BMC Patrol module on a Windows server. Also included are the configuration instructions on the HPE NonStop node and within the Reflex 80:20 GUI.

Windows Server Installation and Considerations

The user will have received an '.exe' file on a supplied Reflex 80:20 CD-ROM. This will have a name of 'XFPddmm.EXE', where 'ddmm' represents the day and the month of the release.

This '.exe' file contains both the Reflex 80:20 GUI and the BMC Patrol alerting module.

Preliminary steps for enabling BMC Patrol alerting:

1. Double click on this XFP '.exe' file.
2. The user may be prompted with the following message 'Version Vn.n of Reflex 80:20 is already installed. Do you wish to overwrite this version?'. Click '**OK**' to this message.
3. Click '**Next >**' to proceed to the next stage of the installation script.
4. Select the 'Destination Directory' for installing the BMC Patrol alerting module and proceed to the next step by clicking '**Next >**'.
5. **Uncheck** the install box for the 'Reflex 80:20 Client GUI using Fastpipe'.
6. **Check** the install box for 'Reflex 80:20 Windows Services' and proceed to the next step by clicking '**Next >**'.
7. **Uncheck** all check boxes on the 'RflxNTServSvc Actions' screen leaving only the 'PATROLCLI' check box checked then proceed to the next step by clicking '**Next >**'.
8. You will be presented with the 'Configure PatrolCli Settings' screen with the following fields:
 - Home:** Host name where the PATROL Agent is running, e.g. test03.itl.co.uk
 - User Name:** The user name used to open a session with a PATROL Agent, e.g. ITL\Administrator
 - Password:** The password used to open a session with a PATROL Agent
 - Path:** This is the path to the PATROLCLI executable that is invoked when a BMC Patrol alert is generated, e.g. C:\Program Files\BMC Software\Patrol3\bin.

Note: a trailing backslash should **not** be added to the end of the path).
9. Click '**Next >**' again to begin the install.
10. Click '**Finish**' to end the install.
11. Restart the Windows server by clicking '**OK**'.



Windows Services

To confirm that this is the case, carry out the following steps:

1. Having carried out the steps above, navigate to the Services applet for the Windows platform.
2. Scroll down the services list on the left side of the window to find the service 'RflxNTServSvc', which should have a status of 'STARTED' and a start-up set to 'AUTOMATIC'. If the service is not started, select 'RflxNTServSvc' and select 'Start'.

See example below:

Program Compatibility Ass...	This service provi...	Started	Automatic	Local System...
Protected Storage	Provides protecte...		Manual	Local System...
Quality Windows Audio Vi...	Quality Windows ...		Manual	Local Service...
RflxNTServSvc	Reflex: Provides m...	Started	Automatic	Local System...
Remote Access Auto Conn...	Creates a connecti...		Manual	Local System...
Remote Access Connectio...	Manages dial-up ...		Manual	Local System...
Remote Desktop Configura...	Remote Desktop ...	Started	Manual	Local System...

3. Closedown the application using the 'CLOSE' button.

The port number that the Windows server uses is '4913'. If this needs to be changed due to the fact that other software is using this port, then the registry should be edited as follows:

1. Click 'Start' on the main Windows toolbar.
2. Click on 'Run'.
3. Type 'regedit' and then press Return.
4. Navigate down to the following directory:

```
My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RflxNTServSvc\Parameters\SERVER_SETTINGS
```

5. Change the port number after double clicking on it.
6. Exit from the Registry Editor.
7. Having carried out the steps above, navigate to the Services application for the Windows platform.
8. Stop and Start the 'RflxNTServSvc' service and then close the application.



HPE NonStop Considerations

This appendix details the way in which an incoming EMS event on the HPE NonStop node can be configured to cause a Windows alert to be sent to the appropriate TCP/IP address and subsequently into the 'RflxNTServSvc', for the purposes of raising a BMC Patrol message.

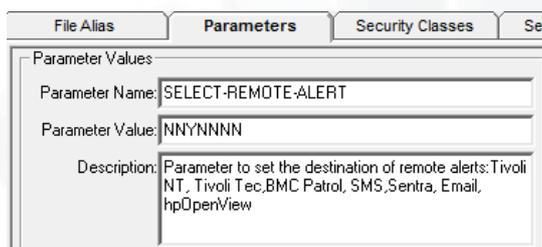
Note: It is required to tell \$EMON to send messages to REMOT-BMC-REACT. This is carried out by stopping \$EMON, setting the ENT-MGR flag in the RUNEMON file and then restarting \$EMON.

Edit your RUNEMON file and ensure the RUN evntmon command line contains parameter ENT-MGR - see example below:

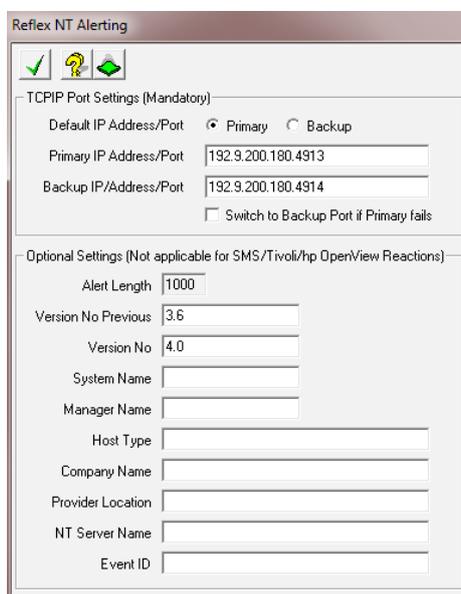
```
RUN evntmon/ name [emon_name], nowait, IN [home_term], OUT [home_term] / &
backup^cpu 0, PAGEGEN [pagegen_name] , CEGEN [cegen_name] , &
SERVER^QUEUE 5000, ENT-MGR REMOT-BMC-REACT
```

Carry out the following steps:

1. Logon to Reflex 80:20 using an assigned Guardian user.
2. Click on the Administration button on the Main toolbar.
3. Navigate to the Parameters tab (the second tab along) and double click on the 'SELECT-REMOTE-ALERT' parameter.
4. Set the third flag to 'Y' to allow BMC Patrol alerts to be raised. Amend the record.



5. Warmboot Status Monitor by clicking on 'OD Set-up' icon on the main toolbar and subsequently clicking on the '!' icon. Acknowledge both return messages by clicking 'OK' to both.
6. Logoff the GUI and Re-logon to read the new BMC Patrol setting.
7. Click on 'Specify Platforms' and select the 'Reflex NT Alerting' option.





Note: In the basic configuration of having one Workstation workstation with BMC Patrol alerting installed, enter in the 'Primary IP Address / Port ', the address of the nominated workstation, e.g. 192.9.200.180.4913, where the last value is the port number of the workstation you nominated earlier for the TIVOLI service. Amend the record.

If using a non-stop approach to alerting, specify a second TCP/IP address.port number and check the 'Switch to Backup Port if Primary Fails' option. Ensure that the BMC Patrol software is installed on a second Windows server.

You can also select whether to make the Primary or Backup Address / Port Number the default, e.g. if the Primary becomes unavailable for a length of time, then modify this field to make the Backup the default address / port.

If the BMC Patrol software has been installed and activated as a service on the appropriate Windows server then proceed with the next steps.

8. Click on the **Administration** button on the Main toolbar.
9. Navigate to the Parameters tab (the second tab along) and double click on the '**ENT-MNGR-FEED- DISARM**' parameter.
10. Set the flag to '**N**' to allow alerts to be raised via the remote feeder mechanism. Amend the record.
11. Click on the '**Reaction**' button on the main toolbar.
12. Warmboot the software by clicking on the '!' on the top of this dialog and then click on the '**Warmboot Reaction Servers**'.
13. Click on the Console button to view the EMS messages resulting from the warmboot operation. A message stating that a successful connection to the nominated workstation should appear on the EMS log.

Connectivity between the HPE NonStop and the Windows server has now been achieved. What follows are instructions to set-up nominated EMS events to be alerted to.

1. With an appropriate EMS event in context within the Reflex 80:20 GUI dialog, navigate to the Action Group tab within the Reaction module.
2. Enter an Action Group name for your BMC Patrol reaction.
3. Click on the green '**REMOTE ALERT**' attribute.
4. Click on any tokens you wish to appear in the resulting BMC Patrol message. Click on a check box and enter any free text you wish to appear in the BMC Patrol message.



5. Add this record with the '+' icon at the top of this dialog.
6. Exit this BMC Patrol dialog and add the underlying reaction record using the '+' icon.
7. In order to activate this BMC Patrol alert, click on the '! icon on the reaction toolbar and follow through the Generate and Compile Filter steps followed by the warmboot. The BMC Patrol alert can be tested using the Event Test tab in the reaction dialog.

Installing BMC Patrol

The BMC Patrol software will need to be installed on the same Windows server that you installed the RflxNTServSvc service on. Please see the relevant notes/documents to install the BMC Patrol software.

Running BMC Patrol Event Manager

From the 'START' menu, locate the 'BMC Patrol' menu then select the 'Operator Console'. After a short while, the BMC Operator Console will be displayed. Now, from the 'Tools' menu, select the 'Event Manager' item.

The 'PATROL Event Manager' will be started and displayed. Patrol events raised by Reflex will appear in this view.

Diagnosing Problems

There may be occasions when Events are not being received by the PATROL Event Manager, this is usually due to a configuration issue with the Reflex and/or PATROL software. Following are some checks that can be carried out to help diagnose any issues found.

1. Checking the Windows Services

The passing of Events to the PATROL Event Manager relies on both the RflxNTServSvc and the PATROL Agent services being up and running on the same PC. To check if these services are running perform the following checks:

- 1.1. Navigate to the Services applet for the Windows platform.
- 1.2. When the appropriate window has opened and the list of Services displayed, scroll down the list and find the PATROL Agent and RflxNTServSvc entries. Both these entries should have the 'Status' set to 'Running' and the 'Startup' set to 'Automatic'. If this is not the case then refer to the Reflex Technical Guide for instructions on Installing and Configuring the Services.



2. Checking the Logfile

Another thing to check is the logfile produced by the PatrolCli application. This file can be found in the Reflex directory on the PC and will be named '**PatrolCli_Log.txt**'. View this file to check if any error information is displayed that may help diagnose the problem.

3. Manually running

Another option is to manually run the PatrolCli script file to check for any problems. This can be done as follows.

- Open a Command Prompt on the Windows PC.
- Change to the BMC Patrol directory on the PC, e.g. CD C:\Program Files\BMC Software\
- Now change to the directory that contains the PatrolCli executable, e.g. CD Patrol3\bin\
- Enter the following command to run the script file:

```
PatrolCli.exe -f C:\Program Files\Reflex\PatrolScript.txt
```

Note: The location of the script is the directory where Reflex was installed on the PC

- Check any messages displayed at the Command Prompt.
- Check the PATROL Event Manager to see if the Event Details have been displayed.



Email Alerts

This section details both the Windows front end and HPE NonStop back end requirements for enabling email alerts from Reflex 80:20. These email alerts will be raised as a result of Reflex 80:20 Reaction configured EMS events which have been nominated as requiring further investigation by IT personnel. In order to activate email alerts, a number of basic steps need to be carried out.

What follows are instructions for installing the email module on a Windows server or server. Also included are the configuration instructions for the HPE NonStop platforms and for within the Reflex 80:20 GUI.

Prior to configuring your email alerting, ensure that the Reflex 80:20 environment on your HPE NonStop system is configured to alert to an Enterprise Manager. This information is contained within your RUNEMON file (located in your Reflex 80:20 object subvolume, e.g. RFLXOBJ).

Edit your RUNEMON file and ensure the RUN evtmon command line contains parameter ENT-MGR - see example below:

```
RUN evtmon / name [emon_name], nowait, IN [home_term], OUT [home_term] /      &
backup^cpu 0, PAGEGEN [pagegen_name] , CEGEN [cegen_name] ,                &
SERVER^QUEUE 5000, ENT-MGR REMOT-BMC-REACT
```

The above RUN command is contained at the end of the RFLXOBJ.RUNEMON file.

Windows Server Installation and Considerations

The user will have received an '.exe' file on a supplied Reflex 80:20 CD-ROM. This will have a name of 'XFPddmm.EXE', where 'ddmm' represents the day and the month of the release.

This '.exe' file contains both the Reflex 80:20 GUI and the Email alerting module.

Preliminary steps for enabling Email alerting:

1. Double click on this XFP '.exe' file.
2. The user may be prompted with the following message 'Version Vn.n of Reflex 80:20 is already installed. 'Do you wish to overwrite this version?'. Click '**OK**' to this message.
3. Click '**Next >**' to proceed to the next stage of the installation script.
4. Select the 'Destination Directory' for installing the email alerting module and proceed to the next step by clicking '**Next >**'.
5. **Uncheck** the install box for the Reflex 80:20 Client GUI using Fastpipe™.
6. **Check** the install box for 'Reflex 80:20 Windows Services' and proceed to the next step by clicking '**Next >**'.
7. Select the email option from the RflxNTServSvc Actions screen then proceed to the next step by clicking '**Next >**'.

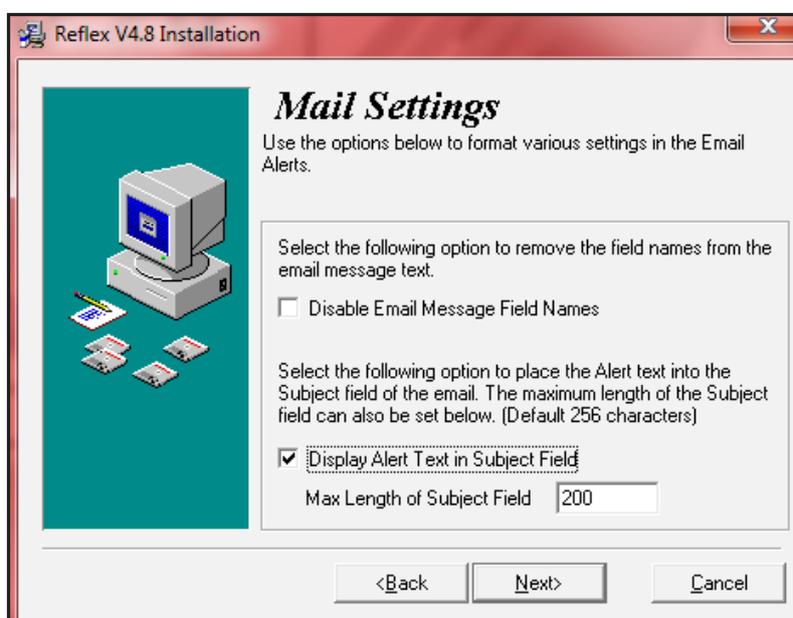


8. Configuring RflxNTServSvc to use SMTP Email:

- SMTP_ADDRESS - Enter a valid SMTP User Address to use as the Originator Address (e.g. reflex.alert@company.co.uk).
- SMTP_SERVER - Enter the DNS Name or TCP/IP address of mail server (e.g. mail.company.co.uk or xxx.xxx.xxx.xxx).
- SMTP_PORT - A default value of 25 is supplied.

Leave the User Name and Password fields blank.

9. **Note:** If you wish the HPE NonStop EMS Event Text to form part of the email Subject Line, then select 'Display Alert Text in Subject Field' option with a 'Max Length of Subject Field' value set to 200, as in the example below:



10. Click '**Next >**'
11. Click '**Next >**' again
12. Click '**Finish**' to end the install.
13. Restart the Windows server by clicking 'OK'.



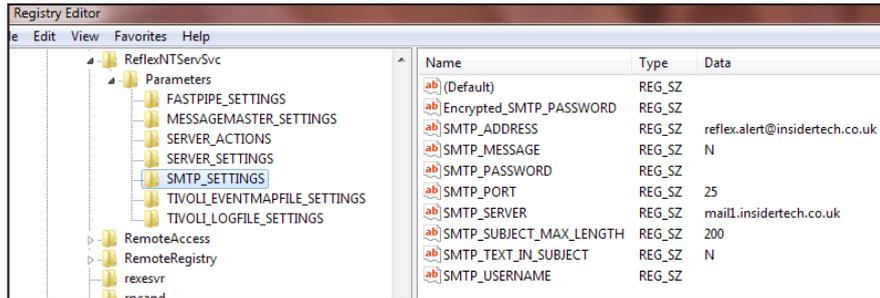
Windows Services

The results of the configuration are stored in the registry and can be obtained via clicking the 'Start' button and selecting the 'run' option.

1. Enter 'REGEDIT' into the edit box.
2. Using the tree on the left-hand side, navigate to the following entry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RflxNTServSvc\Parameters\SMTP_SETTINGS.

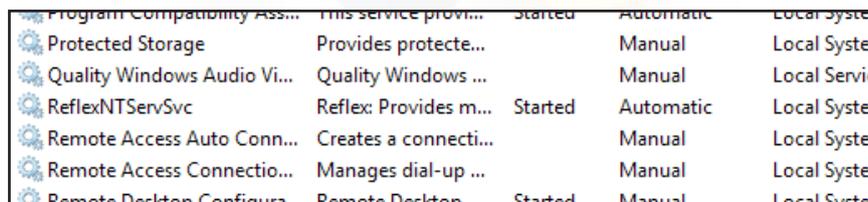
Example regedit results on completion:



The Reflex 80:20 Windows service for receiving email alerts has now been activated. To confirm that this is the case, carry out the following steps:

1. Having carried out the steps above, navigate to the Services application for the Windows platform.
2. Scroll down the services list on the left side of the window to find the service 'RflxNTServSvc', which should have a status of 'STARTED' and a start-up set to 'AUTOMATIC'. If the service is not started, select 'RflxNTServSvc' and select 'Start'.

See example below:





Setting-up the Port Number

The Reflex 80:20 software now needs to know the Port number where the RflxNTServSvc is situated.

Establishing the Port Number

1. Click on the 'Start' button and select the 'Run' option.
2. Enter 'REGEDIT' into the edit box and click the 'Okay' button.
3. Using the tree on the left-hand side, navigate to the following entry
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RflxNTServSvc\Parameters\SERVER_SETTINGS`
4. On the right-hand side will be displayed an entry for 'PORT_NUMBER', make a note of its value e.g. "4913".
5. Start up the Reflex 80:20 GUI and select the 'Configuration' Menu. From there, select 'Specify Remote Platforms' followed by 'Reflex 80:20 NT Alerting'. The Reflex 80:20 NT Alerting dialog will now be displayed:

6. Enter the email server's TCP/IP address, and Port number as stored in the registry, into the 'Primary IP Address / Port' field.
7. Note: A Primary IP Address / Port Number and Backup IP Address / Port Number can be specified, so that if the '**Switch to Backup Port if Primary Fails**' tickbox is selected and the Primary IP Address / Port Number is unavailable, Reflex email alerting will take place via the Backup address / port.

You can also select whether to make the Primary or Backup Address / Port Number the default, e.g. if the Primary becomes unavailable for a length of time, then modify this field to make the Backup the default address / port.

8. The alert length field represents the length of the text message that can be sent in an email. This value is set to 1000 by default but if required, can be amended via an SQLCI session on the HPE NonStop. Logon as the owner of the Reflex 80:20 Pathway.

Navigate to the Reflex 80:20 object subvolume and run the 'RSQLDEFS' file. The table is =CMND_POST_CONFIG_TABLE and the field to be amended is 'SCCALERT_LENGTH'. Set this field value to your new value. For more detailed instructions on how do this, contact Insider Technologies Limited.



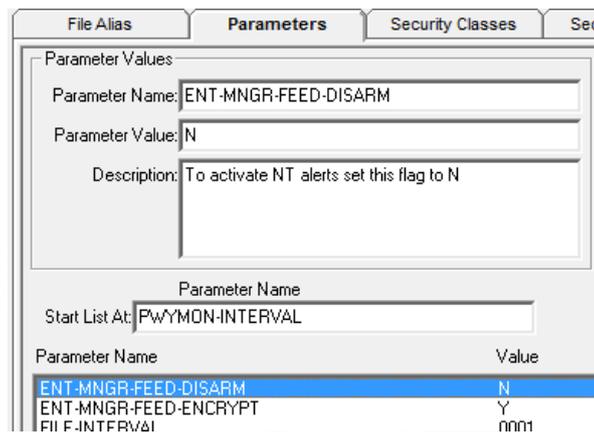
Windows Services

9. Click the 'Amend' button to update the settings, then close down the 'Reflex 80:20 NT Alerting' dialog.
10. In order to make active the TCP/IP details specified in this window, warmboot the Reflex 80:20 software using the Reaction module.

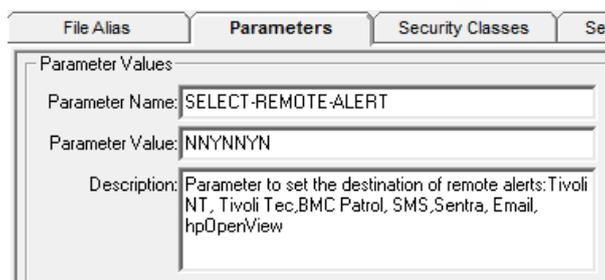
HPE NonStop Considerations

This section details the way in which an incoming EMS event on the HPE NonStop platform can be configured to cause a Windows alert to be sent to the appropriate TCP/IP address and subsequently into the 'RflxNTServSvc' for the purposes of raising an Email message. Carry out the following steps:

1. Logon to Reflex 80:20 using an assigned Guardian user.
2. Click on the Administration button on the Reflex 80:20 toolbar.
3. Navigate to Parameters tab and double-click on the ENT-MNGR-FEED-DISARM and ensure the value is set to N. If changing the value from Y to N then ensure you click on the amend button.



4. Staying in the Parameters tab, double click on the 'SELECT-REMOTE-ALERT' parameter.
5. Set the third and sixth flags to 'YY' to allow Email alerts to be raised. Amend the record.



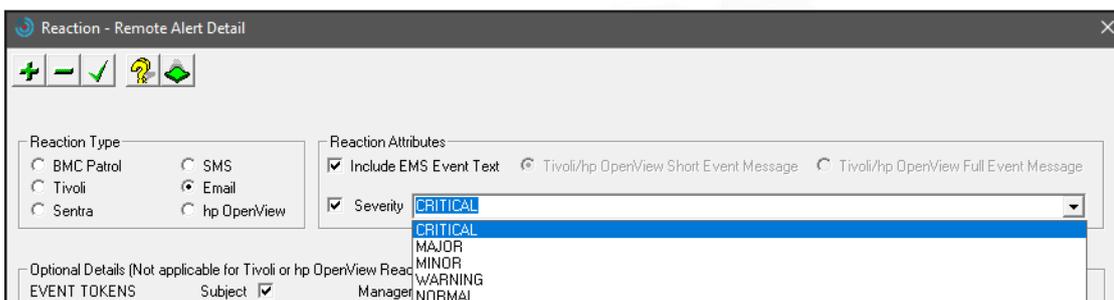


Windows Services

- Warmboot Status Monitor by clicking on 'OD Set-up' icon on the main toolbar and subsequently clicking either of the '!' icons. Acknowledge the return message by clicking 'Ok'.
- Click on the Console button to view the EMS messages resulting from the warmboot operation. A message stating that a successful connection to the nominated workstation should appear on the EMS log.

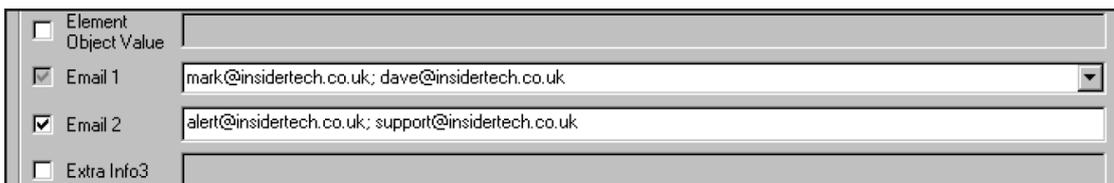
Connectivity between the HPE NonStop and the Windows server has now been achieved. What follows are instructions to set-up nominated EMS events to alert to via an email.

- With an appropriate EMS event in context within the Reflex 80:20 GUI dialog, navigate to the Action Group tab within the Reaction module.
- Enter an **Action Group** name for your Email reaction.
- Click on the green attribute that contains an 'Remote Platform' descriptor next to it.
- Click on any tokens you wish to appear in the resulting Email message. Click on a check box and enter any free text in the 'Extra Info' fields you wish to appear in the email message.
- If you wish the resultant email to be marked with a High Importance flag, then select the Severity as either a Critical or Major.



Use the Email fields to enter the Email addresses required. Multiple Email addresses can be entered by using a semi colon as a separator e.g. mark@insidertech.co.uk; dave@insidertech.co.uk.

- Add this record with the '+' icon at the top of this dialog.
- Leave this Email dialog and add the underlying reaction record using the '+' icon.
- In order to activate this Email alert, click on the '!' icon on the reaction toolbar and follow through the generate and compile filter steps followed by the warmboot. The Email alert can be tested using the Event Test tab in the Reaction dialog.





HPE OpenView Alerts

This section details both the Windows front end and HPE NonStop back end Server requirements for enabling HPE OpenView Alerts from Reflex 80:20.

It is assumed that the OVO 7 for Windows server is up-and-running and that a suitable Windows server has been configured as a "Managed Node".

Note: The Managed Node will host the Windows Service "RflxNTServSvc" which is used to relay NonStopServer events to the OpenView Server via the OpenMessageInterface API.

In order to activate HPE OpenView Alerting a number of basic steps need to be carried out.

NonStop Server Considerations

This section details the way in which an incoming EMS event on the NonStop Server platform can be configured to cause a Windows alert to be sent to the appropriate TCP/IP address and subsequently into the 'RflxNTServSvc' for the purposes of raising a HPE Openview alert message.

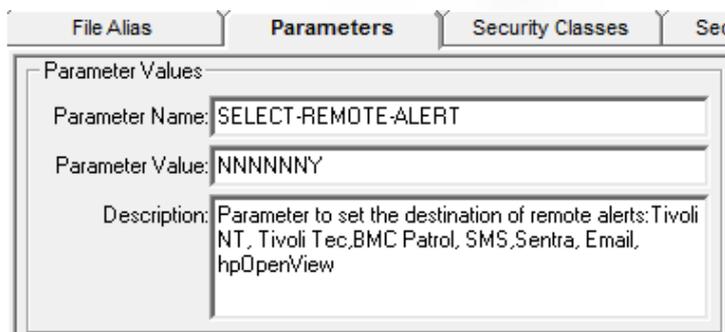
Note: It is required to tell Event-Monitor to send messages to OPENVIEW-REACT This is carried out by stopping \$EMON, setting the ENT-MGR flag in the RUNEMON file and the restarting \$EMON.

Edit your RUNEMON file and ensure the RUN evntmon command line contains parameter ENT-MGR - see example below:

```
RUN evntmon/ name [emon_name], nowait, IN [home_term], OUT [home_term] / &
backup^cpu 0, PAGEGEN [pagegen_name] , CEGEN [cegen_name] , &
SERVER^QUEUE 5000, ENT-MGR OPENVIEW-REACT
```

Carry out the following steps:

1. Logon to Reflex 80:20 using an assigned Guardian user.
2. Click on the Administration button on the Main toolbar.
3. Navigate to the Parameters tab (the second tab along) and double click on the '**SELECT-REMOTE-ALERT**' parameter.
4. Set the seventh flag of seven to 'Y' to allow HPE Openview alerts to be raised. Amend the record.





Windows Services

5. Warmboot Status Monitor by clicking on 'OD Setup' icon on the main toolbar and subsequently clicking either of the '!' icons. Acknowledge the return message by clicking 'Ok'.
6. Logoff the GUI and re-login to read the new HPE OpenView setting.
7. Click on '**Select Remote Platforms**' and select the '**Reflex 80:20 NT Alerting**' option.

8. From this dialog, make sure the 'Default IP Address / Port' has been selected.
9. Enter the email server's TCP/IP address, and Port number as stored in the registry, into the 'Primary IP Address / Port' field.
10. Note: A Primary IP Address / Port Number and Backup IP Address / Port Number can be specified, so that if the '**Switch to Backup Port if Primary Fails**' tickbox is selected and the Primary IP Address / Port Number is unavailable, Reflex NT alerting will take place via the Backup address / port.

You can also select whether to make the Primary or Backup Address / Port Number the default, e.g. if the Primary becomes unavailable for a length of time, then modify this field to make the Backup the default address / port.



Windows Services

Connectivity between the HPE NonStop platform and Managed Node has now been configured. What follows are instructions to set-up nominated EMS events to alert to a Remote Platform.

1. With an appropriate EMS event in context within the Reflex 80:20 GUI dialog, navigate to the **Action Group** tab within the Reaction module.
2. Enter an **Action Group** name for your REMOTE PLATFORM reaction.
3. Click on the Remote Alert attribute.

Note: this might be abbreviated if allowing other reactions to use the same Windows mechanism, e.g. SMS, BMC Patrol.

4. Click on whether using the short or the long message configuration.
5. Click on a severity value for the event.

6. Leave this REMOTE PLATFORM dialog and add the underlying reaction record using the '+' icon.
7. In order to activate this REMOTE PLATFORM alert, click on the '!' icon on the reaction toolbar and follow through the generate and compile filter steps followed by the warmboot. The REMOTE PLATFORM alert can be tested using the Event Test tab in the reaction dialog.



Managed Node Considerations

You will have received a .msi file on the supplied Reflex 80:20 CD ROM.

The RflxNTServSvc is installed via execution of this .msi file on the Managed Node.

Please read at least Installation prerequisites, Installation Custom Actions and Manual Configuration following Installation before continuing with the installation of the ReflexSPI.

Installation Prerequisites

Prior to installation ensure that:

1. The OVO 7 for Windows server (henceforth referred to as "OpenView Server") is configured and up-and-running.
2. A Designated Managed Node has been configured. Note that the Designated Managed Node and OpenView Server may be one and the same.

Note: The Designated Managed Node will host the Windows Service "RflxNTServSvc" which is used to relay NonStopServer events to the OpenView Server via the OpenMessageInterface API.

3. Reflex 80:20 is up-and-running on the HPE NonStop Server. Make a note of the following properties as they are needed during installation:

Pathmon Name (e.g. \$RFLX)

Fastpipe Listener IP Address (e.g. 192.9.200.151)

Fastpipe Listener Port Number (e.g. 5611)

Node Name (e.g. \ITLTECH)

4. Reflex 80:20 has been configured for HPE OpenView Alerts.
5. The Remote Platform for RflxNT Alerting has been configured with the IP address of the Designated Managed Node. The Port Number will normally be 4913.
6. The desired HPE OpenView reactions have been configured in Reflex 80:20.

Note: It is advisable to close the OpenView Console for the duration of the installation.

Installation Launch Conditions

Installation will not proceed in the absence of the following registry keys:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\HP OpenView\InstallDir
```

and

```
HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\HP OpenView\DataDir
```

These keys should exist on an OpenView Server or Managed Node.

Installation Folder

All delivered files are placed under <InstallDir>\SPI-share\ReflexSPI, where <InstallDir> is given by the registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\HP OpenView\InstallDir.
```

<InstallDir> typically will have the value "C:\Program Files\HPE OpenView".



Delivered Files

The following files are delivered:

```
DASH.INI
MessageMaster.dll
ReflexObjUp.wav
AUTOACKMAP.txt
PCTREE32.DLL
CONSOLE.INI
Dash.exe
RflxNTServSvc.exe
FastPipe.dll
zlib.dll
ServerIniTemplate.txt
MMICOM.dll
ReflexObjDown.wav
Reflex.exe
OpenViewNonStopSPITasks.exe
NETMONINITEMPLATE.txt
REFLEX.INI
ITLUTL.dll
ReflexOnlineHelp.reg
REFLEX.CHM
itl_db_util.dll
ReflexObjVuln.wav
Server.ini
NETMON.INI
reflexhelpinstall.bat
<DIR> HPOpenviewConfig
    NonStopServerPol.data
    ReflexServices.mof
    NonStopServerPol.header
    MofTypeSubtypeTemplate.txt
    RflxNTServSvcuninstall.bat
    NonStopServerPol.bat
    RflxNTServSvcinstall.bat
    NonStopServerPolConfig.mm
    NonStopServerPol
    ReflexPolicy.bat
    AUTOACKMAP.txt
    MofHeader.txt
    NonStopServer_tools.mof
    reflexservices.bat
    NonStopServerPolDataTemplate.txt
    RflxNTServSvc.reg
    ReflexSPIReadMe.rtf
    MofNodeTemplate.txt
    NonStopServer_toolsMofTemplate.txt
```



Installation Custom Actions

The following Installation Custom Actions are offered during execution of the ReflexSPI.msi:

1. Install RflxNTServSvc
This action will automatically stop and uninstall any existing RflxNTServSvc, install the new RflxNTServSvc, apply appropriate registry settings (see Registry Settings below) and start the RflxNTServSvc.
2. AutoDiscover Services and Generate ReflexServices.mof file
This action will query Reflex servers on the HPE NonStop platform in order to discover the nodes and distinct types/subtypes of all objects currently being monitored. It will then generate a ReflexServices.mof file in which each node/type/subtype has a corresponding OpenView "Service" definition.
3. Upload ReflexServices.mof file
This action will upload the ReflexServices.mof file into OpenView. When OpenView Console is subsequently re-opened the Service tree will now include the auto-discovered services.
4. Upload Policy Files (NonStopServerPol, NonStopServer_tools.mof)
This action will upload the NonStopServerPol file into OpenView. When OpenView Console is subsequently re-opened the Policy management tree will now include the NonStopServer policy group. This action will also upload the NonStopServer_tools.mof file into OpenView. When OpenView Console is subsequently re-opened the Tools tree will now include the NonStopServer tools group.

Custom Action 1 should be selected only when installing on the Designated Managed Node.

Custom Actions 2 through 4 should be selected only when installing on the OpenView Server.

Should the OpenView Server and Designated Managed Node be one and the same then all Custom Actions 1 through 4 should be selected.

Manual Configuration following Installation

Following installation it is necessary to deploy the NonStopServer Policy to the Designated Managed Node. This can be done via the OpenView Console. The policy will be located in the policy tree: Policy management/Policy groups/NonStopServer/NonStopServer.

Uninstallation

Prior to uninstallation, the following tasks must be performed manually (via the OpenView Console):

- uninstall NonStopServer Policy from Managed Node (or Server)
- delete NonStopServer Policy Group
- delete the Service/Systems Infrastructure/NonStopServer and Service/Systems/SystemsInfrastructure/RflxNTServSvc service trees
- delete the Tools/NonStopServer/Reflex 80:20 GUI

To uninstall re-run the ReflexSPISetup.msi or use Add/Remove Programs.

During uninstallation the RflxNTServSvc (if selected during installation) will be stopped and uninstalled and the corresponding Registry Settings removed. The delivered files will be removed.



Following uninstallation, the following registry branch should be removed:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Insider Technologies Ltd\Reflex\  
ContextSensitiveHelp\CONTEXT_SENSITIVE_HELP_IDS
```

Custom Actions via Reflex 80:20 GUI

Note: the following Installation Custom Actions can also be carried out via the Reflex 80:20 GUI Tool on the OpenView Server.

1. AutoDiscover Services and Generate ReflexServices.mof file
2. Upload ReflexServices.mof file
3. Generate and Upload Policy Files (i.e. NonStopServerPol file and NonStopServer_tools.mof file)

The "AutoDiscover Services and Generate ReflexServices.mof file" and "Upload ReflexServices.mof file" actions should be used whenever new types/subtypes of object become monitored by Reflex.

It is not necessary to perform those actions when new objects of existing type/subtype become monitored by Reflex.

Note: It is advisable to close the OpenView Console when uploading policy or .mof files.

Auto-acknowledgement

The NonStopServerPol policy rules support "auto-acknowledgement" whereby an existing message in the "Active Messages" view is automatically acknowledged (and therefore moved to the "Acknowledged Messages" view) upon receipt of a corresponding "Acknowledging" message.

Auto-acknowledgement is supported for three distinct varieties of message:

- i) Status Events generated by RflxNTServSvc:
 - ReflexNTServer Running - ReflexNTServer Stop Pending
 - Client Heartbeat Resumed - Client Heartbeat Missed
 - Client Disconnected - Client Connected

- ii) Reflex Action Needed - Action Clear events

- iii) Mapped Events

These are events appearing in the user-configurable AUTOACKMAP.txt file (see below).

AUTOACKMAP.txt

This file is used by the RflxNTServSvc to tag those events (other than RflxNTServSvc Status Events and Action Needed/Action Clear Events) which are deemed to be auto-acknowledged upon the receipt of specific subsequent events. The tagging enables the NonStopServerPol rules to perform the auto-acknowledgement.

The default AUTOACKMAP.txt file caters for pre-configured "Dashboard" events e.g. "DiskPercentFullThresholdExceeded / DiskPercentFullThresholdNoLongerExceeded".

The Reflex 80:20 GUI facilitates tailoring of the AUTOACKMAP.txt file via the menu item:

Reactions->Define HPE OpenView Auto-acknowledge Map.



User-defined events may be identified and added to the AUTOACKMAP.txt file via the Reflex 80:20 GUI.

Note: for the changes in the AUTOACKMAP.txt file to take effect, it is necessary to perform the following steps on the Designated Managed Node:

- i) Stop the RflxNTServSvc
- ii) Copy the new AUTOACKMAP.txt file to the location specified by the registry key:

```
HKEY_LOCAL_MACHINES\SYSTEM\CurrentControlSet\Services\RflxNTServSvc\
Parameters\OPENVIEW_AUTOACKMAPFILE_SETTINGS\PATH
```

- iii) Restart the RflxNTServSvc

Note: auto-acknowledgement of Mapped Events may be disabled by setting to 0 the value of the registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RflxNTServSvc\
Parameters\OPENVIEW_AUTOACKMAPFILE_SETTINGS\USE_OPENVIEW_AUTOACKMAPFILE
```

RflxNTServSvc Registry Settings

Default settings for the RflxNTServSvc are written to the Windows Registry during the execution of the ReflexSPI.msi. The default settings can be altered by the customer. Altered settings are activated only when the service is restarted.

Some important HPE OpenView-specific settings for the Reflex 80:20 Windows server are described below (unless otherwise specified, values are 1 = On, 0 = Off):

HKEY_LOCAL_MACHINE:SYSTEM: CurrentControlSet:Services:RflxNTServSvc:

SERVER_ACTIONS

MONITOR_CLIENT_ACTIONS - specifies whether to generate client status events (connected, disconnected, heartbeat_missed, heartbeat_resumed)

MONITOR_SERVER_ACTIONS - specifies whether to generate server status events (running, stop_pending)

PERFORM_OPENVIEW_CALLS - specifies whether to forward events to the OpenView Server via the OpenMessage API

SERVER_SETTINGS

MAX_HEARTBEAT_INTERVAL_SECS - specifies number of seconds between events before it is deemed that the client heartbeat has been missed (causing a heartbeat_missed event to be generated)

MAX_NUM_MISSED_HEARTBEATS - specifies how many consecutive heartbeats should be missed before a further heartbeat_missed event is to be generated

PORT_NUMBER - specifies the port number upon which the RflxNTServSvc will listen for client connections (default 4913)

OPENVIEW_AUTOACKMAPFILE_SETTINGS

USE_OPENVIEW_AUTOACKMAPFILE - specifies whether to enable the Auto-acknowledgement facility.

PATH - specifies path to AUTOACKMAP.txt file (see Auto-acknowledgement of Events above)



RflxNTServer Service Installation

RflxNTServer Service Installation used in TIVOLI/BMC PATROL/SENTRA/SMS/e-mail alerting

The RflxNTServer is installed as a Service on a Windows server simply by executing the supplied installation script,

The advantages of a Windows service are as follows:

- it will continue running even when the user logs off
- if the machine is restarted then the service will be among the first applications to be restarted when the logon screen is shown

Starting

Following installation the RflxNTServer Windows service may be started by any of the following methods:

- restart the machine
- press the Start Button in the Services Applet with RflxNTServer highlighted
- issue the command line RflxNTServer -s

Stopping

Pressing the Stop button on the Services Applet will cause RflxNTServer Windows service to quit irrespective of whether it has any connected clients.

Command line parameters

The following parameters may be passed on the RflxNTServer command line:

- i will install the service
- n will uninstall the service
- s will start the service

The following command is the most common way of creating the service:

```
RflxNTServer -n -i
```

This first uninstalls a service called RflxNTServer if it exists and then creates a new service called RflxNTServer.

To start the above service, type RflxNTServer -s or press the Start Button in the Services Applet with RflxNTServer highlighted.

*The following values are contained in the file registry

```
[SERVER SETTINGS]
```

```
PORT_NUMBER=4913
```

```
//port number which RflxNTServer will "listen on"
```

```
[FASTPIPE SETTINGS]
```

```
FASTPIPE_TIMEOUT_MSECS=15000
```

```
//fast pipe timeout - not currently implemented
```

```
[SERVER_ACTIONS]
```



```
PERFORM_PATROLCLI_CALLS=1
```

```
//indicates whether RflxNTServer should make PatrolCli calls when BMC Patrol messages are sent from the client
```

```
//(default value 1 = yes, may also be set to 0 = no)
```

```
PERFORM_DATABASE_DUMP=0
```

```
//indicates whether RflxNTServer should perform database dumps when //BMC Patrol messages are sent from the client
```

```
//(default value 0 = no, may also be set to 1 = yes)
```

```
NB this value should be set to 0 unless the RflxNTServer is to be configured for
```

```
//SENTRA (contact Insider Technologies for details)
```

If the registry setting 'PERFORM_PATROL_CALLS' is set to 1 then the following registry keys and values will be created:

[PatrolCli_Settings]

PATH=PATROL

This is the path to the PATROLCLI executable that is invoked when a BMC Patrol alert is generated.

HOST=ITLTECH

Host name where the PATROL Agent is running.

USER_NAME=user_name

The user name used to open a session with a PATROL Agent

PASSWORD=password

The password used to open a session with a PATROL Agent

Multiple Services/Configurations

A disadvantage of services is that they must have unique names. However, you could circumvent this by copying RflxNTServer.exe to, say, RflxNTServer2.exe and installing that as a service by issuing the following command line:

```
RflxNTServer2 -I
```

Thus it would be possible for different HPE NonStop nodes to connect to different RflxNTServers, which could be configured to pass alerts to the same or different Enterprise Managers.



12. Administration Params

ADMIN PARAMS SETTINGS

This section describes the use and value settings for each of the parameters configurable in the Reflex 80:20 product. A list of these parameters can be viewed by accessing the Administration module and clicking on the Parameters tab.

The table on the following pages provide a brief explanation of the prime function of each Administration Parameter.

Where a 'Partial' and 'Full' warmboot is mentioned in the table, then the following description will assist in determining which warmboot to perform:

PARTIAL Warmboot

The Partial Warmboot causes a message to be sent to several serverclasses to re-read the configuration information which has been amended, such as polling intervals and threshold limits. In addition, if there has been a change to a tree structure in OD Setup (Status Monitor setup), e.g. a new object has been added, then that individual tree is refreshed so that the change can take effect.

The Partial Warmboot was introduced in later releases of Reflex as an alternative to the more process intensive Full Warmboot.

FULL Warmboot

The Full Warmboot performs all of the functions of the Partial Warmboot **BUT** every Status Monitor tree and object is refreshed. Therefore, if there are many trees and objects configured in the Status Monitor view, then the Full Warmboot can take considerably longer to complete, when compared to a Partial Warmboot.

Deciding on which warmboot option to use really depends on the number of changes that are to be activated but generally, a Partial Warmboot should be all that is required. Performing a Full Warmboot will just take longer, as every tree and object will be refreshed.



Administration Params

Parameter Name	Value(s)	Warmboot	Description of Use
ACTION-GROUP-DOWN	INSIDER-DOWN	Stop/Start Reflex	Can be modified with any 30 character value you desire; INSIDER-DOWN is the default. This can be set to a generic value which is more site-specific, e.g. ACTION-APP-DOWN or BANK-DOWN-EVENT-REACTION. This parameter is usually set-up at the beginning of using the product. It is used as a file key to embrace all down messages sent to the Status Monitor graphical display for both processes and files which have been setup using the Heartbeat module. If the user wants the product to automatically set-up a graphical reaction to a process down or file not present situation, the reaction key in the Reaction module will be set to the value given here.
ACTION-GROUP-UP	INSIDER-UP	Stop/Start Reflex	As above but for the 'UP' graphical reactions relating to Heartbeat configured processes and files.
ACTION-GROUP-VULN	INSIDER-VULN	Stop/Start Reflex	As above but for the 'VULNERABLE' graphical reaction cases relating to Heartbeat monitored files. Note: Whereas a process can either be up or down in the Reflex context, a file can be present or not present but also have an offending attribute, e.g. file corrupt, file broken, file full and so forth, each of which represent vulnerable scenarios.
ALLOW-MEASURE	Y, N. Default - N		This parameter is used to determine if the use of Measure is permitted.
AUDIT-FLAG	Y, N Default - Y	Stop/Start Reflex	If this flag is set to 'Y' then all of the configuration carried out in the Reflex GUI screens will be audited and any actions carried out written to the AUDLOG file. This file is accessible from the Administration module and the contents can be ordered by timestamp, facility, Guardian User ID and terminal ID. The AUDLOG file can also be archived; details of how to perform this are contained in this guide (see the RFLXCOM utility section).



Administration Params

<p>CACHE-READ-HITS-THRESH-OPERAND</p>	<p>LT, GT Default: GT</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used to determine the type of threshold check to be used when checking Disk Cache Read hits. A value of GT informs the threshold engine to perform a greater than (>) check, whereas a value of LT informs the threshold engine to perform a less than (<) check.</p> <p>This parameter is used in conjunction with the parameter DISK-CACHE-READ-HITS-THRESHOLD, i.e. if CACHE-READ-HITS-THRESH-OPERAND is set to LT and DISK-CACHE-READ-HITS-THRESHOLD is set to 90, then a threshold event will be raised when the Cache Read Hits is less than (<) 90.</p>
<p>CONSOLE-ALERTS-FLAG</p>	<p>0(None), 1(Critical), 2(Action), 3 (Critical & Action) Default - 0</p>	<p>Freeze, Stop, Thaw & Start the Reflex CONSOLE Pathway server</p>	<p>This flag enables any Critical or Action needed EMS events not currently configured in Reflex to be monitored, to still be passed to the status monitor graphical alerting screen. This is achieved by attaching the inverse compiled filter (ECALFOB2) to the Primary View in CONSOLE. Icons can then be set-up in Status Monitor to catch the alerts 'rejected' by Console. Events issued: 2602 for Critical events and 2603 for Action needed events. These events are pre-delivered and associated with graphical alerting as a default.</p>
<p>CPU-BUSY-THRESHOLD</p>	<p>0 through 99 Default - 70</p>	<p>Stop/Start Reflex (alternatively warm-boot via Status Monitor set-up (!) icon and Freeze, Stop Thaw & Start the Reflex DASH-THRESH Pathway server)</p>	<p>This parameter controls two functions within Reflex:</p> <p>The first is the CPU threshold as observed in the Dashboard module of Reflex. Any breach of threshold will render the appropriate graph or the CPU summary, with a red colour indicating the threshold has been compromised.</p> <p>The second effect of this parameter is to control the EMS messages ('exceeded' event - 2553) and ('no longer exceeded' event - 2561) which corresponds to threshold breached and threshold no longer breached, respectively. These events are pre-delivered and associated with graphical alerting as a default.</p>



Administration Params

<p>CPU-DASH-MSG-FREQ</p>	<p>1 through 99 Default - 10</p>	<p>Stop/Start Reflex (alternatively warm-boot via Status Monitor set-up (!) icon and Freeze, Stop Thaw & Start the Reflex DASH-THRESH Pathway server)</p>	<p>This parameter is used in conjunction with all the other Dashboard parameters. It controls how often to output a CPU threshold breached message. An example would be, if the CPU-POLL-INTERVAL is set to 15 seconds and CPU-DASH-MSG-FREQ set to 5 then a CPU busy message would only be output if the CPU was seen to be busy 15 x 5 seconds (1 minute 15 seconds). At this point, a CPU Busy EMS message would be raised by Dashboard.</p>
<p>CPU-POLL-INTERVAL</p>	<p>15 through 3600 (seconds) Default - 30</p>	<p>Warmboot via the Status Monitor set-up (!) icon. Note that the new interval will ONLY become active once the next poll of the current poll period is complete, i.e. if the poll interval was set to 10 minutes and is then changed to 2 minutes, the change to 2 minutes will only take place after the current 10 minute poll is activated. If such a delay is a problem, then it can be forced by a freeze, stop, thaw and then start of the DASH-THRESH Pathway server, following the warmboot.</p>	<p>This parameter is used in conjunction with all the other Dashboard parameters. It controls how often to issue a CPU threshold breached message. An example would be if the CPU-POLL-INTERVAL is set to 15 seconds and CPU-DASH-MSG-FREQ set to 5 then a CPU busy message would only be output if the CPU was seen to be busy 15 x 5 seconds (1 minute 15 seconds). At this point, a CPU Busy EMS message would be raised by Dashboard.</p>
<p>CPU-QUEUE-THRESHOLD</p>	<p>0 through 50 Default - 20</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Partial Warm-boot (!) icon.</p>	<p>The parameter represents how many queued processes are allowed in a CPU before a threshold message is raised. The appropriate graph in the Dashboard will show red for the appropriate CPU when the threshold is compromised. Queue threshold exceeded EMS event - 2555 Queue threshold no longer exceeded EMS event - 2563</p>



Administration Params

DASH-CACHE-SUPPRESS	<p>3 Y/N values referring to:</p> <p>disk cache read hits,</p> <p>disk cache faults,</p> <p>disk cache audits</p> <p>Default: YYY</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used to control whether the various cache threshold events are suppressed.</p> <p>If set to Y the events are not generated.</p>
DASH-RESTRICT-PROC-BUSY-OS	<p>Y, N</p> <p>Default: N</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>When set to Y, this parameter instructs Dashboard to ignore processes running against the following object codes:</p> <p>OSIMAGE, OVDP and TSYS DP2.</p> <p>Therefore, this parameter can be used to prevent Busy messages from being produced by system processes such as Disk processes.</p>
DASH-RESTRICT-PROC-BUSY-PRI	<p>Y, N</p> <p>Default: N</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>When set to Y, this parameter instructs Dashboard to only perform checks against processes that have a Priority below 200. Therefore, this parameter can be used to prevent Busy messages and Change of Priority messages from being produced by system processes such as Disk processes.</p>
DASH-SUSPECT-INTERVAL	<p>1 through 99</p> <p>Default - 1</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter controls how often a suspect process is reported on by Dashboard.</p> <p>An example would be if the CPU-POLL-INTERVAL is set to 15 seconds and the DASH-SUSPECT-INTERVAL parameter is set to 5, then a suspect process EMS message would only be output if the process was seen to be suspect 15 x 5 seconds (1 minute 15 seconds).</p> <p>At this point, a suspect process EMS message would be raised by Dashboard. Current suspect states are as follows:</p> <p>SUSPENDED/ DEBUG BREAKPOINT/ DEBUG TRAP/ DEBUG REQUEST/ INSPECT MEM ACCESS BREAKPOINT/ INSPECT BREAKPOINT/ INSPECT TRAP/ INSPECT REQUEST/ SAVEABEND/ TERMINATING.</p>



Administration Params

<p>DASH-SUSPECT-SUPPRESS</p>	<p>Y, N Default - N</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter does NOT stop the suspect process EMS messages from being emitted but controls whether they are seen in normal EMS viewing consoles like CONSOLE, Viewpoint™ and View + Point™. This is achieved by Reflex placing a suppress token in the EMS event to make it invisible on the system. The purpose of this is to allow the event to be seen in the Reflex graphical status monitor display where important events have been consolidated rather than adding more 'noise' to the EMS collectors on the HPE NonStop node.</p>
<p>DASH-THRESH-SUPP-ARP-LAYER</p>	<p>4 Y/N values referring to: In ARP Requests In ARP Replies Out ARP Requests Out ARP Replies Default: YYYY</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used to control whether the various TCP/IP Layer threshold events are suppressed. If set to Y the events are not generated. Note: When TCP/IP is being used via a CLIM, then these suppression flags should be set to 'Y' since the metrics being monitored are not available from the CLIM.</p>
<p>DASH-THRESH-SUPP-ICMP-LAYER</p>	<p>6 Y/N values referring to: Bad Checksum In Dest Unreachable In Source Quench Out Source Quench Invalid Header Size Packets too short Default - YYYYYY</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used to control whether the various TCP/IP ICMP Layer threshold events are suppressed. If set to Y the events are not generated. Note: When TCP/IP is being used via a CLIM, then these suppression flags should be set to 'Y' since the metrics being monitored are not available from the CLIM.</p>
<p>DASH-THRESH-SUPP-IP-LAYER</p>	<p>9 Y/N values referring to: Bad Checksum Bad Packet Size Fragments Input Fragments Dropped Fragments Timed Out Invalid Header Size Packets Cant Forward Packets Too Small Short Packets Default: YYYYYYYYY</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used to control whether the various TCP/IP IP Layer threshold events are suppressed. If set to Y the events are not generated. Note: When TCP/IP is being used via a CLIM, then these suppression flags should be set to 'Y' since the metrics being monitored are not available from the CLIM.</p>



Administration Params

<p>DASH-THRESH-SUPP-IP-STATS</p>	<p>5 Y/N values referring to:</p> <ul style="list-style-type: none"> Bad Route Dynamic Redirects New Gateway Redirects Wildcard Matches Unreachable <p>Default: YYYYY</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used to control whether the various TCP/IP IP Routing Stats threshold events are suppressed.</p> <p>If set to Y the events are not generated.</p> <p>Note: When TCP/IP is being used via a CLIM, then these suppression flags should be set to 'Y' since the metrics being monitored are not available from the CLIM.</p>
<p>DASH-THRESH-SUPP-TCP-LAYER</p>	<p>10 Y/N values referring to:</p> <ul style="list-style-type: none"> Bad Checksum Bad Offest Invalid Header Size Retransmitted Packets Connections Timouts Connections Closed Connections Dropped No Ports for Pockets Established Connects Keep-Alive Dropped <p>Default: YYYYYYYYYY</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used to control whether the various TCP/IP IP Layer threshold events are suppressed.</p> <p>If set to Y the events are not generated.</p> <p>Note: When TCP/IP is being used via a CLIM, then these suppression flags should be set to 'Y' since the metrics being monitored are not available from the CLIM.</p>
<p>DASH-THRESH-SUPP-TCP-IP</p>	<p>3 Y/N values referring to:</p> <ul style="list-style-type: none"> Route Usage Subnet Errors (input/output) Subnet Packets (input/output) <p>Default: YYY</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used to control whether the various TCP/IP IP Route and Subnet threshold events are suppressed.</p> <p>If set to Y the events are not generated.</p> <p>Note: When TCP/IP is being used via a CLIM, then these suppression flags should be set to 'Y' since the metrics being monitored are not available from the CLIM.</p>
<p>DASH-THRESH-SUPP-UDP-LAYER</p>	<p>3 Y/N values referring to:</p> <ul style="list-style-type: none"> Bad Checksum Bad Packet Size Invlaid Header Size <p>Default: YYY</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used to control whether the various TCP/IP UDP Layer threshold events are suppressed.</p> <p>If set to Y the events are not generated.</p> <p>Note: When TCP/IP is being used via a CLIM, then these suppression flags should be set to 'Y' since the metrics being monitored are not available from the CLIM.</p>



Administration Params

<p>DASH-THRESH-SUPPRESS</p>	<p>16 Y/N values referring to:</p> <ul style="list-style-type: none"> CPU Busy CPU Queue Length CPU Page Faults Disk Full Process Busy Process Priority Disk Fragment ZZBI Processes CPU Memory Pressure CPU Memory Queue Len CPU PCBs Lowpin CPU PCBs Highpin CPU TLEs CPU Disk I/O's CPU Disk Hits % Free Memory Pages <p>Default: NNNNNNNNNNNNNNNN (16 N's)</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used to control whether the various Disk/CPU threshold events are suppressed.</p> <p>If set to Y the events are not generated.</p>
<p>DASH-THRESH-SUPPRESS-X25</p>	<p>11 Y/N values referring to:</p> <ul style="list-style-type: none"> Line Quality SU In Use Modem Error Frame Sent RNR Frame Sent REJ Frame Received RNR Frame Received REJ Packet Sent RNR Packet Sent Restart Packet Received RNR Packet Received Restart <p>Default: YYYYYYYYYYY (11 Y's)</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used to control whether the various X25 threshold events are suppressed.</p> <p>If set to Y the events are not generated.</p>
<p>DASHBABY-PRIORITY</p>	<p>50 - 190</p> <p>Default:100</p>	<p>Via Status Monitor s et-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>The priority that the DASHBABY processes (created by the Dash-Master Server) will run at in each CPU.</p>
<p>DATA-ANALYSIS-TRACE-FLAG</p>	<p>Y, N</p> <p>Default - N</p>	<p>Warm-boot Service Monitor set-up using the (!) icon.</p>	<p>This parameter controls whether unrecognised APIs forwarded into the service monitor module are written to a trace file (TRACEFIL) in the data subvolume. These will be any APIs not set-up in the data definition dialog under the configuration menu of Reflex 80:20.</p> <p>See Reflex on-line help for more details.</p>



Administration Params

DEFAULT-GUARDIAN-USER	<group-name>. <user-name>, e.g. BUS.USER Default: REFLEX.OPS	Stop/Start Reflex	This parameter can be set-up if you wish to supply users with a direct connection with Reflex without the need for a logon ID. This is typical of where business users just require to access the service level state of objects for viewing but cannot actually change any details in Reflex. The Guardian user ID specified here would normally be associated with a 'READONLY' Security Class in the Administration module of Reflex 80:20. See next parameter.
DEFAULT-GUARDIAN-USER-ENABLED	Y, N Default - N	Stop/Start Reflex	<p>This flag is used in conjunction with the previous parameter for controlling whether users have access to the Reflex Pathway without the need for a Guardian user ID.</p> <p>In practice, only a Reflex administrator would have access to the parameters screen for updating these parameters. The Security Class facility ID for this function is 'DPU'.</p> <p>Once the DEFAULT-GUARDIAN-USER and DEFAULT-GUARDIAN-USER-ENABLED parameters have been configured, a 'business' user can logon to the GUI by selecting the "Auto Logon as Default User" option from the GUI Configuration drop-down menu.</p> <p>To de-activate the 'Auto Logon' facility, amend the AUTO_LOGON value from 1 to 0, within the REFLEX.INI file located in PC folder: C:\Users\<Name>\AppData\Roaming\ITL\Reflex\<Version>.</p>
DISK-AUDIT-FORCES-THRESHOLD	1 - 32767 default: 1000	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by dashboard to determine the number of Audit Forces that need to occur before Reflex flags a warning.</p> <p>An EMS event will be raised for the offending audit force block.</p> <p>Audit forces block size 512 exceeded EMS event - 5265 Audit forces block size 512 not exceeded EMS event - 5264 Audit forces block size 1024 exceeded EMS event - 5267 Audit forces block size 1024 not exceeded EMS event - 5266 Audit forces block size 2048 exceeded EMS event - 5269 Audit forces block size 2048 not exceeded EMS event - 5268 Audit forces block size 4096 exceeded EMS event - 5271 Audit forces block size 4096 exceeded EMS event - 5270</p>
DISK-FULL-THRESHOLD	1 - 99 Default 95	Stop/Start Reflex (Alternatively warm-boot Status Monitor set-up (!) icon and Freeze, Stop Thaw & Start the Reflex DASH-THRESH Pathway server)	<p>Dashboard will periodically poll (based on the DISK-POLL-INTERVAL) on the amount of disk space that is being used (based as a percentage). This will then be used to highlight any disks in Dashboard that have breached the threshold and subsequently colour the appropriate disk red on a graph or in the disk summary.</p> <p>Disk Threshold exceeded EMS event - 2556 Disk Threshold no longer exceeded EMS event - 2564</p>



Administration Params

<p>DISK-HITS-THRESHOLD</p>	<p>0 - 20000 Default - 2000</p>	<p>Via the Status Monitor set-up module, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used by dashboard to determine the number of Disk Cache Hits per second that are allowed during a CPU poll interval, before Reflex flags a warning.</p> <p>An EMS event will be raised for the offending CPU.</p> <p>Disk Cache Hits exceeded EMS event - 2581</p> <p>Disk cache Hits not exceeded EMS event - 2580</p>
<p>DISK-CACHE-FAULTS-THRESHOLD</p>	<p>1 - 32767 Default: 1000</p>	<p>Via the Status Monitor set-up module, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used by dashboard to determine the number of Cache Faults that need to occur before Reflex flags a warning.</p> <p>An EMS event will be raised for the offending cache faults block.</p> <p>Cache faults block size 512 exceeded EMS event - 5257</p> <p>Cache faults block size 512 not exceeded EMS event - 5256</p> <p>Cache faults block size 1024 exceeded EMS event - 5259</p> <p>Cache faults block size 1024 not exceeded EMS event - 5258</p> <p>Cache faults block size 2048 exceeded EMS event - 5261</p> <p>Cache faults block size 2048 not exceeded EMS event - 5260</p> <p>Cache faults block size 4096 exceeded EMS event - 5263</p> <p>Cache faults block size 4096 exceeded EMS event - 5262</p>



Administration Params

<p>DISK-CACHE-POLL-INTERVAL</p>	<p>60 - 28800 Default: 1800</p>	<p>Via the Status Monitor set-up module, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is the Cache poll interval that is used in Dashboard to poll at the configured number of seconds the Cache status.</p>
<p>DISK-CACHE-READ-HITS-THRESHOLD</p>	<p>0 - 100 Default: 95</p>	<p>Via the Status Monitor set-up module, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine what percentage of Cache Reads were 'Cache Read Hits' during a disk cache poll interval, before Reflex flags a warning on the Cache Faults block.</p> <p>An EMS event will be raised for the offending Cache Read Hits block.</p> <p>Cache Read Hits block size 512 exceeded EMS event - 5249 Cache Read Hits block size 512 not exceeded EMS event - 5248 Cache Read Hits block size 1024 exceeded EMS event - 5251 Cache Read Hits block size 1024 not exceeded EMS event - 5250 Cache Read Hits block size 2048 exceeded EMS event - 5253 Cache Read Hits block size 2048 not exceeded EMS event - 5252 Cache Read Hits block size 4096 exceeded EMS event - 5255 Cache Read Hits block size 4096 exceeded EMS event - 5254</p> <p>This parameter is used in conjunction with the parameter CACHE-READ-HITS-THRESH-OPERAND. i.e. if CACHE-READ-HITS-THRESH-OPERAND is set to LT and DISK-CACHE-READ-HITS-THRESHOLD is set to 90 then a threshold event will be raised when the Cache Read Hits is less than (<) 90.</p>
<p>DISK-DASH-MSG-FREQ</p>	<p>1 - 99 Default - 1</p>	<p>Stop/Start Reflex (Alternatively warm-boot Status Monitor set-up (!) icon and Freeze, Stop Thaw & Start the Reflex DASH-THRESH Pathway server)</p>	<p>This parameter is used in conjunction with all the other dashboard disk parameters. It controls 'how often' to output a DISK threshold breached message. An example would be, if the DISK-POLL-INTERVAL is set to 15 seconds and DISK-DASH-MSG- FREQ set to 5 then a DISK full message would only be output if the DISK was seen to be busy 15 x 5 seconds (1 minute 15 seconds). At this point, a DISK full EMS message would be raised by Dashboard.</p>
<p>DISK-FRAGMENT-THRESHOLD</p>	<p>1 - 99999 Default - 1500</p>	<p>Stop/Start Reflex (Alternatively warm-boot Status Monitor set-up (!) icon and Freeze, Stop Thaw & Start the Reflex DASH-THRESH Pathway server)</p>	<p>The parameter represents how many DISK FRAGMENTS are allowed on a DISK before a threshold message is raised.</p> <p>The appropriate graph in the Dashboard will show red for the appropriate disk when the threshold is compromised.</p> <p>Fragment threshold exceeded EMS event - 2566 Fragment threshold no longer exceeded EMS event - 2567</p>



Administration Params

DISKIO-MAX-DISKS	500 - 1000 Default: 500	Stop / Start the REFLEX-DISKIO serverclass	This parameter is used to specify the maximum number of individual disks that can be monitored by the Disk I/O module
DISKIO-MSG-FREQ	1 - 99 Default: 3	Stop / Start the REFLEX-DISKIO serverclass	This parameter is used to specify the frequency of EMS events issued by the Disk I/O module if a Disk remains in the same Down / Vulnerable state
DISKIO-POLL-INTERVAL	60 - 28800 seconds Default: 600	Stop / Start the REFLEX-DISKIO serverclass	This parameter is used to specify how often the Disk I/O module polls for updated I/O
DISKIOS-THRESHOLD	0 - 10000 Default: 500	Via the Status Monitor set-up module, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by dashboard to determine the number of Disk I/O's per second that are allowed during a CPU poll interval, before reflex flags a warning.</p> <p>An EMS event will be raised for the offending CPU:</p> <p>Disk I/O's exceeded EMS event - 2579</p> <p>Disk I/O's not exceeded EMS event - 2578</p>



Administration Params

<p>DISK-POLL-INTERVAL</p>	<p>60 through 28 800 seconds - maximum 8 hours Default: 60</p>	<p>Warmboot via the Status Monitor set-up (!) icon. Note that the new interval will ONLY become active once the next poll of the current poll period is complete, i.e. if the poll interval was set to 10 minutes and is then changed to 2 minutes, the change to 2 minutes will only take place after the current 10 minute poll is activated. If such a delay is a problem, then it can be forced by a freeze, stop, thaw and then start of the DASH-THRESH Pathway server, following the warmboot.</p>	<p>This is the disk poll interval which is used by Dashboard to poll at the configured number of seconds to check disk status.</p>
<p>EMON-MAX-PATHSEND-RETRIES</p>	<p>0-99 Default: 3</p>	<p>Warmboot the Reaction Module by executing the <i>third</i> step under the (!) icon ("Warmboot Reaction Servers")</p>	<p>This parameter is used to specify the maximum number of times that Eventmon will attempt a Pathsend to Status Monitor, following a previous Pathsend error. A delay will occur before each attempt to re-send; this delay is controlled by the EMON-RETRY-DELAY parameter.</p>
<p>EMON-MAX-RECONNECT-TIME</p>	<p>60 through 1800 minutes Default: 1800</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used to determine the maximum time in the past that the EVNTMON process will re-connect to the EMS Distributor following a backup takeover of their primary process. Note that if the last processed log-time from the primary process is less than the value of EMON-MAX-RECONNECT-TIME, then the log time used following a backup takeover will be the last processed logtime plus 1 microsecond.</p>
<p>EMON-RETRY-DELAY</p>	<p>1-60 Default: 10</p>	<p>Warmboot the Reaction Module by executing the <i>third</i> step under the (!) icon ("Warmboot Reaction Servers")</p>	<p>This parameter is used to specify how long to wait (in seconds) before attempting to re-send a failed Pathsend. During the delay, no new EMS events will be processed but existing I/O from previous Pathsends will be completed. The number of retries that the delay / attempt to re-send occurs is controlled by the EMON-MAX-PATHSEND-RETRIES parameter.</p>



Administration Params

ENT-MNGR-FEED-DISARM	Y, N Default: Y	Warmboot the Reaction Module by executing the <i>third</i> step under the (!) icon ("Warmboot Reaction Servers")	This parameter controls whether alerts are sent to a nominated TCP/IP address and then onto an allocated Enterprise Manager. or to allow SMS paging. or to ITL SENTRA (Windows monitoring). The ENT-MNGR-FEEDER Pathway server in the Reflex 80:20 Pathway is a Fastpipe client responsible for relaying Enterprise Manager alerts. Setting this flag to a value of 'N' will enable this relaying of alerts.
ENT-MNGR-FEED-ENCRYPT	Y, N Default: Y	Warmboot the Reaction Module by executing the <i>third</i> step under the (!) icon ("Warmboot Reaction Servers")	This parameter is used to enable Blowfish encryption for the Enterprise Manager Feeder serverclass 'ENT-MNGR-FEED'. A value of Y enables encryption and a value of N disables encryption.
FILE-INTERVAL	1 - 3600 Default: 1	Stop/Start the file agent.	The use of this parameter has been superceded by the FIME and FIPR prefixed parameters listed lower down. It is used by the FILEAGNT code in the object subvolume which monitors any files referenced in the object table for percent full at the configured interval. See the Reflex 80:20 user manual for more details. The Heartbeat module takes over from this monitoring as of release 4.0 onwards.
FILE-THRESHOLD	0 - 99 Default: 1	Stop/Start the file agent.	The use of this parameter has been superceded by the FIME and FIPR prefixed parameters listed lower down. It is used by the FILEAGNT code in the object subvolume which monitors any files referenced in the object table for percent full at the configured interval.



Administration Params

FIME-MAX-STANDBY -CRITICAL	0 - 4 Default: 1	Stop / Start the FILE-METS-CRIT serverclass	This parameter is used to specify how many Standby processes are allowed to run for the File Metrics Critical period monitoring
FIME-MAX-STANDBY -DAILY	0 - 4 Default: 1	Stop / Start the FILE-METS-DAILY serverclass	This parameter is used to specify how many Standby processes are allowed to run for the File Metrics Daily period monitoring
FIME-MAX-STANDBY -HDAILY	0 - 4 Default: 1	Stop / Start the FILE-METS-HALFD serverclass	This parameter is used to specify how many Standby processes are allowed to run for the File Metrics Half Daily period monitoring
FIME-MAX-STANDBY -HOURLY	0 - 4 Default: 1	Stop / Start the FILE-METS-HOURLY serverclass	This parameter is used to specify how many Standby processes are allowed to run for the File Metrics Hourly period monitoring



Administration Params

FIME-METS-DELAY	120 - 600 secsnds Default: 120	Warmboot the Reaction Module by executing the <i>third</i> step under the (!) icon ("Warmboot Reaction Servers")	This parameter controls the delay between the Controlling and Standby File Metrics processes, accessing their shared memory segment
FIME-METS-SUPPRESS	Y, N Default: N	Warmboot the Reaction Module by executing the <i>third</i> step under the (!) icon ("Warmboot Reaction Servers")	This parameter does NOT stop the File Monitoring EMS messages from being emitted but controls whether they are seen in normal EMS viewing consoles like CONSOLE, Viewpoint™ and View + Point™. This is achieved by Reflex placing a suppress token in the EMS event to make it invisible on the system. The purpose of this is to allow the event to be seen in the Reflex graphical status monitor display where important events have been consolidated rather than adding more noise to the collectors on the HPE NonStop node.
FIME-MSG-FREQUENCY	1 - 99 Default: 1	Warmboot the Reaction Module by executing the <i>third</i> step under the (!) icon ("Warmboot Reaction Servers")	This parameter controls the frequency that the same state is reported by way of an EMS event message. For instance, if a file is found to be corrupt, an EMS message will be generated. If it is found to be corrupt <i>N</i> seconds (FIME-POLL-INTERVAL) later, it will not be reported until this frequency parameter is reached. If it is set to '1' then it will be reported constantly until the file problem is resolved.



Administration Params

FIME-POLL-INTERVAL	15 - 1800 seconds Default: 60	Warmboot the Reaction Module by executing the third step under the (!) icon ("Warmboot Reaction Servers")	This parameter is used by the File Metrics monitoring software within the Heartbeat module of Reflex. It only relates to the CRITICAL period of monitoring and can be set to 15 seconds through to 1800 seconds (30 minutes). Any files being monitored at a CRITICAL rate will be assigned this period.
FIPR-MSG-FREQUENCY	1 - 99 Default: 1	Warmboot the Reaction Module by executing the third step under the (!) icon ("Warmboot Reaction Servers")	This parameter is used by the File Existence monitoring software and controls the frequency that the same state is reported, by way of an EMS event message. For instance, if a file is found to be corrupt an EMS message will be generated. If it is found to be corrupt N seconds (FIPR-POLL-INTERVAL) later, it will not be reported until this frequency parameter is reached. If it is set to '1' then it will be reported constantly until the file problem is resolved.
FIPR-POLL-INTERVAL	15 - 3600 seconds Default: 60	Warmboot the Reaction Module by executing the third step under the (!) icon ("Warmboot Reaction Servers")	This parameter is used by the File Existence monitoring software within the Heartbeat module of Reflex. It can be set to 15 seconds through to 3600 seconds (60 minutes), depending on the user assigned requirement. A file will be checked for existence between an assigned calendar period at the interval specified.
FIPR-PRES-SUPPRESS	Y, N Default: N	Warmboot the Reaction Module by executing the third step under the (!) icon ("Warmboot Reaction Servers")	This parameter does NOT stop the File Existence monitoring EMS messages from being emitted but controls whether they are seen in normal EMS viewing consoles like CONSOLE, Viewpoint™ and View + Point™. This is achieved by Reflex placing a suppress token in the EMS event to make it invisible on the system. The purpose of this is to allow the event to be seen in the Reflex graphical status monitor display where important events have been consolidated rather than adding more noise to the collectors on the HPE NonStop node.



Administration Params

<p>HEAP-ALERT-FREQ</p>	<p>1 through 99 Default: 3</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Warmboot (!) icon ("Perform Partial Warmboot of the Server").</p>	<p>This parameter is used in conjunction with other HEAP Dashboard and CPU-POLL-INTERVAL parameters. It controls how often to output a Heap threshold breached message.</p> <p>An example would be if HEAP-ALERT-INCREASE-COUNT is set to 3, HEAP-ALERT-POLL-COUNT is set to 12, HEAP-ALERT-FREQ is set to 3 and the CPU-POLL-INTERVAL parameter is set to 30. When these parameters have been set to these values, then the Process metrics are retrieved every 30 seconds and if the Heap usage increases at least 3 (HEAP-ALERT-INCREASE-COUNT) times in a range of 12 polls, then an alert is raised; any further alerts for the same process will only occur after increasing Heap usage has been detected by more than 3 (HEAP-ALERT-FREQ) times.</p>
<p>HEAP-ALERT-DN-FREQ</p>	<p>1 through 99 Default: 1</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Warmboot (!) icon ("Perform Partial Warmboot of the Server").</p>	<p>This parameter is used in conjunction with other HEAP Dashboard and CPU-POLL-INTERVAL parameters. It controls how often to output a Heap threshold breached message. It controls the frequency at which a Down alert is raised when a process uses increasing amounts of Heap.</p> <p>An example would be if HEAP-ALERT-DN-FREQ is set to 1, HEAP-ALERT-INCREASE-COUNT is set to 3, HEAP-ALERT-POLL-COUNT is set to 12, HEAP-ALERT-FREQ is set to 3 and the CPU-POLL-INTERVAL parameter is set to 30. When these parameters have been set to these values, then the Process metrics are retrieved every 30 seconds and if the Heap usage increases at least 3 (HEAP-ALERT-INCREASE-COUNT) times in a range of 12 polls, then a Vulnerable alert is raised; if Heap usage increases for a further (HEAP-ALERT-DN-FREQ x HEAP-ALERT-INCREASE-COUNT) times, i.e. 3 more times, then a Down alert is raised.</p>
<p>HEAP-ALERT-UP-FREQ</p>	<p>1 through 99 Default: 3</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Warmboot (!) icon ("Perform Partial Warmboot of the Server").</p>	<p>This parameter is used in conjunction with other HEAP Dashboard and CPU-POLL-INTERVAL parameters. It controls the frequency at which an Up alert is raised when a process continues to use the same amount of Heap.</p> <p>An example would be if the HEAP-ALERT-UP-FREQ is set to 3, HEAP-ALERT-INCREASE-COUNT is set to 3, HEAP-ALERT-POLL-COUNT is set to 12, HEAP-ALERT-FREQ is set to 3 and the CPU-POLL-INTERVAL is to 30. When these parameters have been set to these values, then the Process metrics are retrieved every 30 seconds and if the Heap usage increases at least 3 (HEAP-ALERT-INCREASE-COUNT) times in a range of 12 polls, then a Vulnerable alert is raised.</p> <p>If Heap usage remains the same for a further (HEAP-ALERT-POLL-COUNT x HEAP-ALERT-UP-FREQ) times, i.e. 36 more times, then an Up alerts is raised. Note that an Up alert is raised immediately if Heap usage decreases.</p>



Administration Params

HEAP-ALERT-INCREASE-COUNT	1 through 99 Default: 3	Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Warmboot (!) icon ("Perform Partial Warmboot of the Server").	<p>This parameter is used in conjunction with other HEAP Dashboard and CPU-POLL-INTERVAL parameters. It is used to specify how many times the Heap usage of a process must increase within HEAP-ALERT-POLL-COUNT polls before an alert is raised.</p> <p>For example, HEAP-ALERT-INCREASE-COUNT is set to 3, HEAP-ALERT-POLL-COUNT is set to 12 and the CPU-POLL-INTERVAL is set to 30, then the Process metrics are retrieved every 30 seconds and if the Heap usage increases at least 3 (HEAP-ALERT-INCREASE-COUNT) times in a range of 12 polls, then an alert is raised.</p>
HEAP-ALERT-POLL-COUNT	1 through 99 Default: 12	Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Warmboot (!) icon ("Perform Partial Warmboot of the Server").	This parameter is used in conjunction with other HEAP Dashboard and CPU-POLL-INTERVAL parameters. It controls how many polls of Process metrics are examined when checking for increasing amounts of Heap usage.
HEAP-ALERT-SUPPRESS	Y, N Default: N	Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Warmboot (!) icon ("Perform Partial Warmboot of the Server").	This parameter is used to suppress Heap usage alert messages. A value of Y enables suppression and a value of N disables suppression.



Administration Params

HEARTBEAT-EMS-SUPPRESS	Y, N Default: N	Warmboot the Reaction Module by executing the third step under the (!) icon ("Warmboot Reaction Servers")	<p>This parameter does NOT stop the Heartbeat process monitoring EMS messages from being emitted but controls whether they are seen in normal EMS viewing consoles like CONSOLE, Viewpoint™ and View + Point™. This is achieved by Reflex placing a suppress token in the EMS event to make it invisible on the system.</p> <p>The purpose of this is to allow the event to be seen in the Reflex graphical status monitor display where important events have been consolidated rather than adding more 'noise' to the collectors on the HPE NonStop node.</p>
MAX-DISCS	500 - 1500 Default: 1200	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is used to determine the maximum number of disks that can be configured in Reflex.
MEASURE-SUBVOL	A valid subvolume Default: \$DEV.RFLXMEAS		This is the subvolume that is used to store the Measure Data file.
MEASUREMENT-DURATION	30 - 300 seconds Default - 30		This parameter is the Measurement duration in seconds which will be used.



Administration Params

MEASUREMENT-CPU-ARRAY-SIZE	16 Range: 2 to 16 Default: 16	Stop and restart the MEAS-CPU-CLI serverclass	The array size value determines how many entries to store in an internal array used to store previous Measurement results. This array is used when determining if a Rate threshold has been breached. The array size should be large enough to store the maximum number of Measurements that will be returned.
MEASUREMENT-CPU-CATCHUP-RATE	0 - 30 seconds Default: 0	Stop and restart the MEASURE-CPU serverclass	This controls the interval value to return to the client when there is a backlog of Measurement data available, i.e. if there is a backlog of Measurement data, then tell the client how often to request data earlier than the MEASUREMENT-CPU-INTERVAL so that processing can catch up to the current time.
MEASUREMENT-CPU-DURATION	0 or 30 - 300 seconds Default: 0	Stop and restart the MEASURE-CPU serverclass	This is the Measurement duration (in seconds) for CPU measurements. Note that a value of 0 indicates that 'continual measurements' are to be used.
MEASUREMENT-CPU-FILE-LIFE	600 - 43200 seconds (10 minutes to 12 hours). Default: 21600 (6 hours)	Stop and restart the MEASURE-CPU serverclass	When using 'continual measurements', this is the duration of each individual Measurement file in seconds.
MEASUREMENT-CPU-HOUSEKEEP	24 - 168 hours Default: 24	Stop and restart the MEASURE-CPU serverclass	This specifies the interval, in hours, between the Housekeeping routine being used.
MEASUREMENT-CPU-INTERVAL	10 - 600 seconds Default: 30	Stop and restart the MEASURE-CPU serverclass	This is the interval, in seconds, between each measurement.
MEASUREMENT-CPU-INTV-PER-RQST	1 - 100 Default: 1	Stop and restart the MEASURE-CPU serverclass	This controls how many Measurement Intervals will be grouped into a reply to a client request. For example, if MEASUREMENT-CPU-INTV-PER-RQST is set to 40 and MEASUREMENT-CPU-INTERVAL is set to 30 then Measurement results will be available every 20 minutes (40 x 30 seconds). If the Measurement was being performed on a 2 CPU node then there will be 80 Measurements available.



Administration Params

MEASUREMENT-CPU-IO-BUFFSIZE	32 - 4096 Default: 48	Stop and restart the MEASURE-CPU serverclass	This specifies the size of the i/o buffer in kb to use in replies to the client. Larger sizes will use more memory but will enable a reduced number of serverclass_sends. Note that sizes above 32k are only supported on Integrity / Integrity Blade nodes using TS/MP 2.5 or later.
MEASUREMENT-CPU-READ-ALL	Y/N Default: N	Stop and restart the MEASURE-CPU serverclass	Control whether to measure ALL entities or only those configured in the Reflex database.
MEASUREMENT-CPU-SUBVOL	A valid subvolume Default: \$DEV. MEASCPU	Stop and restart the MEASURE-CPU serverclass	This is the subvolume that is used to store Measure Data files and control files. Note that the subvolume should only be used by a single Measurement feed.
MEASUREMENT-DISK-ARRAY-SIZE	400 Range: 40 to 10000 Default: 400 NB: 400 = 100 x 4 disk paths.	Stop and restart the MEAS-DISK-CLI serverclass	The array size value determines how many entries to store in an internal array used to store previous Measurement results. This array is used when determining if a Rate threshold has been breached. The array size should be large enough to store the maximum number of Measurements that will be returned. Note that the Disk Measurement will return Measurement results for each Disk Path; therefore for each physical disk, there may be 4 sets of Measurement results returned for the primary, backup, mirror and mirror backup paths.
MEASUREMENT-DISK-CATCHUP-RATE	0 - 30 seconds Default: 0	Stop and restart the MEASURE-DISK serverclass	This controls the interval value to return to the client when there is a backlog of Measurement data available, i.e. if there is a backlog of Measurement data, then tell the client how often to request data earlier than the MEASUREMENT-DISK-INTERVAL so that processing can catch up to the current time.
MEASUREMENT-DISK-DURATION	0 or 30 - 300 seconds Default: 0	Stop and restart the MEASURE-DISK serverclass	This is the Measurement duration (in seconds) for DISK measurements. Note that a value of 0 indicates that 'continual measurements' are to be used.



Administration Params

MEASUREMENT-DISK-FILE-LIFE	600 - 43200 seconds (10 minutes to 12 hours). Default: 21600 (6 hours)	Stop and restart the MEASURE-DISK serverclass	When using 'continual measurements', this is the duration of each individual Measurement file in seconds.
MEASUREMENT-DISK-HOUSEKEEP	24 - 168 hours Default: 24	Stop and restart the MEASURE-DISK serverclass	This specifies the interval, in hours, between the Housekeeping routine being used.
MEASUREMENT-DISK-INTERVAL	10 - 600 seconds Default: 30	Stop and restart the MEASURE-DISK serverclass	This is the interval, in seconds, between each measurement.
MEASUREMENT-DISK-INTV-PER-RQST	1 - 100 Default: 1	Stop and restart the MEASURE-DISK serverclass	This controls how many Measurement Intervals will be grouped into a reply to a client request. For example, if MEASUREMENT-DISK-INTV-PER-RQST is set to 40 and MEASUREMENT-DISK-INTERVAL is set to 30 then Measurement results will be available every 20 minutes (40 x 30 seconds). If the Measurement was being performed against 1 DISK (Primary and Backup) then there will be 80 Measurements available.
MEASUREMENT-DISK-IO-BUFFSIZE	32 - 4096 Default: 48	Stop and restart the MEASURE-DISK serverclass	This specifies the size of the i/o buffer in kb to use in replies to the client. Larger sizes will use more memory but will enable a reduced number of serverclass_sends. Note that sizes above 32k are only supported on Integrity / Integrity Blade nodes using TS/MP 2.5 or later.
MEASUREMENT-DISK-READ-ALL	Y/N Default: N	Stop and restart the MEASURE-DISK serverclass	Control whether to measure ALL entities or only those configured in the Reflex database.
MEASUREMENT-DISK-SUBVOL	A valid subvolume Default:\$DEV. MEASDISK	Stop and restart the MEASURE-DISK serverclass	This is the subvolume that is used to store Measure Data files and control files. Note that the subvolume should only be used by a single Measurement feed.



Administration Params

MEASUREMENT-FILE-ARRAY-SIZE	4000 Range: 500 to 10000 Default: 4000	Stop and restart the MEAS-FILE-CLI serverclass	The array size value determines how many entries to store in an internal array used to store previous Measurement results. This array is used when determining if a Rate threshold has been breached. The array size should be large enough to store the maximum number of Measurements that will be returned.
MEASUREMENT-FILE-CATCHUP-RATE	0 - 30 seconds Default: 0	Stop and restart the MEASURE-FILE serverclass	This controls the interval value to return to the client when there is a backlog of Measurement data available, i.e. if there is a backlog of Measurement data, then tell the client how often to request data earlier than the MEASUREMENT-FILE-INTERVAL so that processing can catch up to the current time.
MEASUREMENT-FILE-DURATION	0 or 30 - 300 seconds Default: 0	Stop and restart the MEASURE-FILE serverclass	This is the Measurement duration (in seconds) for FILE measurements. Note that a value of 0 indicates that 'continual measurements' are to be used.
MEASUREMENT-FILE-FILE-LIFE	600 - 43200 seconds (10 minutes to 12 hours). Default: 21600 (6 hours)	Stop and restart the MEASURE-FILE serverclass	When using 'continual measurements', this is the duration of each individual Measurement file in seconds.
MEASUREMENT-FILE-HOUSEKEEP	24 - 168 hours Default: 24	Stop and restart the MEASURE-FILE serverclass	This specifies the interval, in hours, between the Housekeeping routine being used.
MEASUREMENT-FILE-INTERVAL	10 - 600 seconds Default: 30	Stop and restart the MEASURE-FILE serverclass	This is the interval, in seconds, between each measurement.



Administration Params

MEASUREMENT-FILE-INTV-PER-RQST	1 - 100 Default: 1	Stop and restart the MEASURE-FILE serverclass	<p>This controls how many Measurement Intervals will be grouped into a reply to a client request.</p> <p>For example, if MEASUREMENT-FILE-INTV-PER-RQST is set to 40 and MEASUREMENT-FILE-INTERVAL is set to 30 then Measurement results will be available every 20 minutes (40 x 30 seconds).</p> <p>If the Measurement was being performed against 2 FILES then there will be 80 Measurements available.</p>
MEASUREMENT-FILE-IO-BUFFSIZE	32 - 4096 Default: 48	Stop and restart the MEASURE-FILE serverclass	<p>This specifies the size of the i/o buffer in kb to use in replies to the client. Larger sizes will use more memory but will enable a reduced number of serverclass_sends.</p> <p>Note that sizes above 32k are only supported on Integrity / Integrity Blade nodes using TS/MP 2.5 or later.</p>
MEASUREMENT-FILE-READ-ALL	Y/N Default: N	Stop and restart the MEASURE-FILE serverclass	Control whether to measure ALL entities or only those configured in the Reflex database.
MEASUREMENT-FILE-SUBVOL	A valid subvolume Default: \$DEV.MEASFILE	Stop and restart the MEASURE-FILE serverclass	This is the subvolume that is used to store Measure Data files and control files. Note that the subvolume should only be used by a single Measurement feed.



Administration Params

MEASUREMENT-OCPU-ARRAY-SIZE	16 Range: 2 to 16 Default: 16	Stop and restart the MEAS-OCPU-CLI serverclass	The array size value determines how many entries to store in an internal array used to store previous Measurement results. This array is used when determining if a Rate threshold has been breached. The array size should be large enough to store the maximum number of Measurements that will be returned.
MEASUREMENT-OCPU-CATCHUP-RATE	0 - 30 seconds Default: 0	Stop and restart the MEASURE-OCPU serverclass	This controls the interval value to return to the client when there is a backlog of Measurement data available, i.e. if there is a backlog of Measurement data, then tell the client how often to request data earlier than the MEASUREMENT-OCPU-INTERVAL so that processing can catch up to the current time.
MEASUREMENT-OCPU-DURATION	0 or 30 - 300 seconds Default: 0	Stop and restart the MEASURE-OCPU serverclass	This is the Measurement duration (in seconds) for OCPU measurements. Note that a value of 0 indicates that 'continual measurements' are to be used.
MEASUREMENT-OCPU-FILE-LIFE	600 - 43200 seconds (10 minutes to 12 hours). Default: 21600 (6 hours)	Stop and restart the MEASURE-OCPU serverclass	When using 'continual measurements', this is the duration of each individual Measurement file in seconds.
MEASUREMENT-OCPU-HOUSEKEEP	24 - 168 hours Default: 24	Stop and restart the MEASURE-OCPU serverclass	This specifies the interval, in hours, between the Housekeeping routine being used.
MEASUREMENT-OCPU-INTERVAL	10 - 600 seconds Default: 30	Stop and restart the MEASURE-OCPU serverclass	This is the interval, in seconds, between each measurement.



Administration Params

MEASUREMENT-OCPU-INTV-PER-RQST	1 - 100 Default: 1	Stop and restart the MEASURE-OCPU serverclass	<p>This controls how many Measurement Intervals will be grouped into a reply to a client request.</p> <p>For example, if MEASUREMENT-OCPU-INTV-PER-RQST is set to 40 and MEASUREMENT-OCPU-INTERVAL is set to 30 then Measurement results will be available every 20 minutes (40 x 30 seconds).</p> <p>If the Measurement was being performed on a 2 CPU node then there will be 80 Measurements available.</p>
MEASUREMENT-OCPU-IO-BUFFSIZE	32 - 4096 Default: 48	Stop and restart the MEASURE-OCPU serverclass	<p>This specifies the size of the i/o buffer in kb to use in replies to the client. Larger sizes will use more memory but will enable a reduced number of serverclass_sends.</p> <p>Note that sizes above 32k are only supported on Integrity / Integrity Blade nodes using TS/MP 2.5 or later.</p>
MEASUREMENT-OCPU-READ-ALL	Y/N Default: N	Stop and restart the MEASURE-OCPU serverclass	Control whether to measure ALL entities or only those configured in the Reflex database.
MEASUREMENT-OCPU-SUBVOL	A valid subvolume Default:\$DEV. MEASOCPU	Stop and restart the MEASURE-OCPU serverclass	This is the subvolume that is used to store Measure Data files and control files. Note that the subvolume should only be used by a single Measurement feed.



Administration Params

MEASUREMENT-OSNS-ARRAY-SIZE	40 Range: 2 to 100 Default: 40	Stop and restart the MEAS-OSNS-CLI serverclass	The array size value determines how many entries to store in an internal array used to store previous Measurement results. This array is used when determining if a Rate threshold has been breached. The array size should be large enough to store the maximum number of Measurements that will be returned.
MEASUREMENT-OSNS-CATCHUP-RATE	0 - 30 seconds Default: 0	Stop and restart the MEASURE-OSNS serverclass	This controls the interval value to return to the client when there is a backlog of Measurement data available, i.e. if there is a backlog of Measurement data, then tell the client how often to request data earlier than the MEASUREMENT-OSNS-INTERVAL so that processing can catch up to the current time.
MEASUREMENT-OSNS-DURATION	0 or 30 - 300 seconds Default: 0	Stop and restart the MEASURE-OSNS serverclass	This is the Measurement duration (in seconds) for OSNS measurements. Note that a value of 0 indicates that 'continual measurements' are to be used.
MEASUREMENT-OSNS-FILE-LIFE	600 - 43200 seconds (10 minutes to 12 hours). Default: 21600 (6 hours)	Stop and restart the MEASURE-OSNS serverclass	When using 'continual measurements', this is the duration of each individual Measurement file in seconds.
MEASUREMENT-OSNS-HOUSEKEEP	24 - 168 hours Default: 24	Stop and restart the MEASURE-OSNS serverclass	This specifies the interval, in hours, between the Housekeeping routine being used.
MEASUREMENT-OSNS-INTERVAL	10 - 600 seconds Default: 30	Stop and restart the MEASURE-OSNS serverclass	This is the interval, in seconds, between each measurement.



Administration Params

MEASUREMENT-OSNS-INTV-PER-RQST	1 - 100 Default: 1	Stop and restart the MEASURE-OSNS serverclass	<p>This controls how many Measurement Intervals will be grouped into a reply to a client request.</p> <p>For example, if MEASUREMENT-OSNS-INTV-PER-RQST is set to 40 and MEASUREMENT-OSNS-INTERVAL is set to 30 then Measurement results will be available every 20 minutes (40 x 30 seconds).</p> <p>If the Measurement was being performed against 2 OSS Nameservers then there will be 80 Measurements available.</p>
MEASUREMENT-OSNS-IO-BUFFSIZE	32 - 4096 Default: 48	Stop and restart the MEASURE-OSNS serverclass	<p>This specifies the size of the i/o buffer in kb to use in replies to the client. Larger sizes will use more memory but will enable a reduced number of serverclass_sends.</p> <p>Note that sizes above 32k are only supported on Integrity / Integrity Blade nodes using TS/MP 2.5 or later.</p>
MEASUREMENT-OSNS-SUBVOL	A valid subvolume Default:\$DEV. MEASOSNS	Stop and restart the MEASURE-OSNS serverclass	<p>This is the subvolume that is used to store Measure Data files and control files. Note that the subvolume should only be used by a single Measurement feed.</p>



Administration Params

MEASUREMENT-PROC-ARRAY-SIZE	4000 Range: 500 to 10000 Default: 4000	Stop and restart the MEAS-PROC-CLI serverclass	The array size value determines how many entries to store in an internal array used to store previous Measurement results. This array is used when determining if a Rate threshold has been breached. The array size should be large enough to store the maximum number of Measurements that will be returned.
MEASUREMENT-PROC-CATCHUP-RATE	0 - 30 seconds Default: 0	Stop and restart the MEASURE-PROC serverclass	This controls the interval value to return to the client when there is a backlog of Measurement data available, i.e. if there is a backlog of Measurement data, then tell the client how often to request data earlier than the MEASUREMENT-PROC-INTERVAL so that processing can catch up to the current time.
MEASUREMENT-PROC-DURATION	0 or 30 - 300 seconds Default: 0	Stop and restart the MEASURE-PROC serverclass	This is the Measurement duration (in seconds) for PROC measurements. Note that a value of 0 indicates that 'continual measurements' are to be used.
MEASUREMENT-PROC-FILE-LIFE	600 - 43200 seconds (10 minutes to 12 hours). Default: 21600 (6 hours)	Stop and restart the MEASURE-PROC serverclass	When using 'continual measurements', this is the duration of each individual Measurement file in seconds.
MEASUREMENT-PROC-HOUSEKEEP	24 - 168 hours Default: 24	Stop and restart the MEASURE-PROC serverclass	This specifies the interval, in hours, between the Housekeeping routine being used.
MEASUREMENT-PROC-INTERVAL	10 - 600 seconds Default: 30	Stop and restart the MEASURE-PROC serverclass	This is the interval, in seconds, between each measurement.



Administration Params

MEASUREMENT-PROC-INTV-PER-RQST	1 - 100 Default: 1	Stop and restart the MEASURE-PROC serverclass	<p>This controls how many Measurement Intervals will be grouped into a reply to a client request.</p> <p>For example, if MEASUREMENT-PROC-INTV-PER-RQST is set to 40 and MEASUREMENT-PROC-INTERVAL is set to 30 then Measurement results will be available every 20 minutes (40 x 30 seconds).</p> <p>If the Measurement was being performed against 2 PROCESSES then then there will be 80 Measurements available.</p>
MEASUREMENT-PROC-IO-BUFFSIZE	32 - 4096 Default: 48	Stop and restart the MEASURE-PROC serverclass	<p>This specifies the size of the i/o buffer in kb to use in replies to the client. Larger sizes will use more memory but will enable a reduced number of serverclass_sends.</p> <p>Note that sizes above 32k are only supported on Integrity / Integrity Blade nodes using TS/MP 2.5 or later.</p>
MEASUREMENT-PROC-READ-ALL	Y/N Default: N	Stop and restart the MEASURE-PROC serverclass	Control whether to measure ALL entities or only those configured in the Reflex database.
MEASUREMENT-PROC-SUBVOL	A valid subvolume Default:\$DEV. MEASPROC	Stop and restart the MEASURE-PROC serverclass	This is the subvolume that is used to store Measure Data files and control files. Note that the subvolume should only be used by a single Measurement feed.



Administration Params

MEASUREMENT-SQLP-ARRAY-SIZE	4000 Range: 500 to 10000 Default: 4000	Stop and restart the MEAS-SQLP-CLI serverclass	The array size value determines how many entries to store in an internal array used to store previous Measurement results. This array is used when determining if a Rate threshold has been breached. The array size should be large enough to store the maximum number of Measurements that will be returned.
MEASUREMENT-SQLP-CATCHUP-RATE	0 - 30 seconds Default: 0	Stop and restart the MEASURE-SQLP serverclass	This controls the interval value to return to the client when there is a backlog of Measurement data available, i.e. if there is a backlog of Measurement data, then tell the client how often to request data earlier than the MEASUREMENT-SQLP-INTERVAL so that processing can catch up to the current time.
MEASUREMENT-SQLP-DURATION	0 or 30 - 300 seconds Default: 0	Stop and restart the MEASURE-SQLP serverclass	This is the Measurement duration (in seconds) for SQLP measurements. Note that a value of 0 indicates that 'continual measurements' are to be used.
MEASUREMENT-SQLP-FILE-LIFE	600 - 43200 seconds (10 minutes to 12 hours). Default: 21600 (6 hours)	Stop and restart the MEASURE-SQLP serverclass	When using 'continual measurements', this is the duration of each individual Measurement file in seconds.
MEASUREMENT-SQLP-HOUSEKEEP	24 - 168 hours Default: 24	Stop and restart the MEASURE-SQLP serverclass	This specifies the interval, in hours, between the Housekeeping routine being used.
MEASUREMENT-SQLP-INTERVAL	10 - 600 seconds Default: 30	Stop and restart the MEASURE-SQLP serverclass	This is the interval, in seconds, between each measurement.



Administration Params

MEASUREMENT-SQLP-INTV-PER-RQST	1 - 100 Default: 1	Stop and restart the MEASURE-SQLP serverclass	<p>This controls how many Measurement Intervals will be grouped into a reply to a client request.</p> <p>For example, if MEASUREMENT-SQLP-INTV-PER-RQST is set to 40 and MEASUREMENT-SQLP-INTERVAL is set to 30 then Measurement results will be available every 20 minutes (40 x 30 seconds).</p> <p>If the Measurement was being performed against 2 SQL PROCESSES then there will be 80 Measurements available.</p>
MEASUREMENT-SQLP-IO-BUFFSIZE	32 - 4096 Default: 48	Stop and restart the MEASURE-SQLP serverclass	<p>This specifies the size of the i/o buffer in kb to use in replies to the client. Larger sizes will use more memory but will enable a reduced number of serverclass_sends.</p> <p>Note that sizes above 32k are only supported on Integrity / Integrity Blade nodes using TS/MP 2.5 or later.</p>
MEASUREMENT-SQLP-READ-ALL	Y/N Default: N	Stop and restart the MEASURE-SQLP serverclass	Control whether to measure ALL entities or only those configured in the Reflex database.
MEASUREMENT-SQLP-SUBVOL	A valid subvolume Default:\$DEV. MEASSQLP	Stop and restart the MEASURE-SQLP serverclass	This is the subvolume that is used to store Measure Data files and control files. Note that the subvolume should only be used by a single Measurement feed.



Administration Params

MEASUREMENT-SQLS-ARRAY-SIZE	4000 Range: 500 to 10000 Default: 4000	Stop and restart the MEAS-SQLS-CLI serverclass	The array size value determines how many entries to store in an internal array used to store previous Measurement results. This array is used when determining if a Rate threshold has been breached. The array size should be large enough to store the maximum number of Measurements that will be returned.
MEASUREMENT-SQLS-CATCHUP-RATE	0 - 30 seconds Default: 0	Stop and restart the MEASURE-SQLS serverclass	This controls the interval value to return to the client when there is a backlog of Measurement data available, i.e. if there is a backlog of Measurement data, then tell the client how often to request data earlier than the MEASUREMENT-SQLS-INTERVAL so that processing can catch up to the current time.
MEASUREMENT-SQLS-DURATION	0 or 30 - 300 seconds Default: 0	Stop and restart the MEASURE-SQLS serverclass	This is the Measurement duration (in seconds) for SQLS measurements. Note that a value of 0 indicates that 'continual measurements' are to be used.
MEASUREMENT-SQLS-FILE-LIFE	600 - 43200 seconds (10 minutes to 12 hours). Default: 21600 (6 hours)	Stop and restart the MEASURE-SQLS serverclass	When using 'continual measurements', this is the duration of each individual Measurement file in seconds.
MEASUREMENT-SQLS-HOUSEKEEP	24 - 168 hours Default: 24	Stop and restart the MEASURE-SQLS serverclass	This specifies the interval, in hours, between the Housekeeping routine being used.
MEASUREMENT-SQLS-INTERVAL	10 - 600 seconds Default: 30	Stop and restart the MEASURE-SQLS serverclass	This is the interval, in seconds, between each measurement.



Administration Params

MEASUREMENT-SQLS-INTV-PER-RQST	1 - 100 Default: 1	Stop and restart the MEASURE-SQLS serverclass	<p>This controls how many Measurement Intervals will be grouped into a reply to a client request.</p> <p>For example, if MEASUREMENT-SQLS-INTV-PER-RQST is set to 40 and MEASUREMENT-SQLS-INTERVAL is set to 30 then Measurement results will be available every 20 minutes (40 x 30 seconds).</p> <p>If the Measurement was being performed against an SQL PROCESS that uses 2 SQL STATEMENTS then there will be 80 Measurements available.</p>
MEASUREMENT-SQLS-IO-BUFFSIZE	32 - 4096 Default: 48	Stop and restart the MEASURE-SQLS serverclass	<p>This specifies the size of the i/o buffer in kb to use in replies to the client. Larger sizes will use more memory but will enable a reduced number of serverclass_sends.</p> <p>Note that sizes above 32k are only supported on Integrity / Integrity Blade nodes using TS/MP 2.5 or later.</p>
MEASUREMENT-SQLS-READ-ALL	Y/N Default: N	Stop and restart the MEASURE-SQLS serverclass	Control whether to measure ALL entities or only those configured in the Reflex database.
MEASUREMENT-SQLS-SUBVOL	A valid subvolume Default:\$DEV. MEASSQLS	Stop and restart the MEASURE-SQLS serverclass	This is the subvolume that is used to store Measure Data files and control files. Note that the subvolume should only be used by a single Measurement feed.



Administration Params

MEM-FREE-PAGES-THRESHOLD	1 - 100 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine % of Free Memory Pages at which to highlight a problem.</p> <p>An EMS event will be raised for the offending CPU.</p> <p>% Free Memory Pages has reached the threshold EMS event - 5600</p> <p>% Free Memory Pages is above the threshold EMS event - 5550</p>
MEM-PRESSURE-THRESHOLD	0 - 7 Default: 7	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine the frequency of Page Faults on a CPU during a CPU poll interval, before Reflex flags a warning.</p> <p>An EMS event will be raised for the offending CPU.</p> <p>Memory Pressure exceeded EMS event - 2569</p> <p>Memory Pressure not exceeded EMS event - 2568</p>
MEM-Q-LEN-THRESHOLD	0 - 100 Default: 85		<p>Indicates the number of processes waiting for a Page Fault to be serviced before being highlighted on Dashboard.</p> <p>An EMS event will be raised for the offending CPU.</p> <p>Memory Queue Length exceeded EMS event - 2571</p> <p>Memory Queue length not exceeded EMS event - 2570</p>
MULTIBATCH-INVESTIGATE	Y, N Default: N	Warmboot the Reaction Module by executing the third step under the (!) icon ("Warmboot Reaction Servers")	<p>This parameter is used in conjunction with Insider Technologies MultiBatch, Nonstop batch scheduler product.</p> <p>If you have autodetected a MultiBatch schedule (using the MBATAD utility), the resulting object tree will consist of jobs, segments and units.</p> <p>When a Status Monitor warmboot takes place, each job will not be investigated for status using the MultiBatch agent (AGENT-MULBAT). Instead, the MultiBatch environment will be interrogated using the same agent for failed jobs only at the end of the warm-boot. This will speed up the warm-boot operation for large scheduling environments.</p>



Administration Params

MQDEFAULTPREFIX	Free Text Default: \$SYSTEM		This is the MQ Series default Queue prefix as used by the Reflex MQSC process.
MQNSKOPTPATH	Free Text Default: /opt/mqm	Stop / Start the AGENT-MQSC serverclass	This parameter is required to allow access to WebSphere MQ v5.3.
MQNSKVARPATH	Free Text Default: /var/mqm	Stop / Start the AGENT-MQSC serverclass	This parameter is required to allow access to WebSphere MQ v5.3.
MQSC-CPU	0 - 15 Default: 0		This is the CPU that the MQSC process resides in.
MQSC-LOCATION	Free Text Default: \$SYSTEM.SYSTEM.RUNMQSC		This is the location of the MQ Series utility MQSC.
MQSC-PRIORITY	50-190 Default: 50		This is the priority that the MQ Series MQSC process will use.
MQSC-PROCESS	Free Text Default: \$RFMQ		This is the name of the MQ Series MQSC process.
MQVOLUME	Free Text Default: \$SYSTEM		This is the MQ Series Queue Manager Default Volume as used by the MQSC process.



Administration Params

NUM-TRXS-PER-TMF	0 - 500 Default: 100	Stop/Start Reflex	This parameter determines how many SQL database record changes are allowed to take place (delete, insert, amend) before the changes are committed to the Reflex database. The default is usually recommended.
OPENINFO-DASH-TCPIP-PREFIX	A 4 character process name prefix Default: \$TOP	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This is the prefix to use for OPENINFO processes as used by the Reflex TCP/IP Dashboard. A 2 digit number will be appended.
OPENINFO-PROCESS-AGENT-PREFIX	A 4 character process name prefix Default: \$POP	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This is the prefix to use for OPENINFO processes as used by the Reflex Process Status Agent. A 2 digit number will be appended.
OPENINFO-PROCESS-TCPIPAD-PREFIX	A 4 character process name prefix Default: \$XOP	N/A	This is the prefix to use for OPENINFO processes as used by the Reflex TCP/IP Autodetect. A 2 digit number will be appended.
PAGE-FAULT-THRESHOLD	0 - 999 Default: 500		Number of Page Faults per second permitted before Dashboard highlights the problem.



Administration Params

PASS-FROZEN-OBJECT-TO-SENTRA	Y, N Default: N		This parameter is used to determine if Reflex passes events to Sentra for those objects where Status Monitor monitoring is 'frozen'.
PATHMON-PROCESS	The name of the Reflex Pathmon process Default: \$RFLX Max 6 characters including the '\$' sign.	Stop/Start Reflex	This parameter should be set-up at the beginning of a product install of Reflex. It is the name of the Pathway process. It should not exceed 5 characters which includes the '\$' sign. It is used by HPE NonStop processes for internal message sending to appropriate servers within the Reflex application. For multiple networked Reflex environments, this process name should be the same on all HPE NonStop nodes and owned by the same Guardian user, with the user id utilising the same 'remote' passwords.
PCBS-HI-PIN-THRESHOLD	0 - 9000 Default: 3000	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is used by Dashboard to determine the number of High Pin Process Control Blocks in the processor that are in use during a CPU poll interval, before Reflex flags a warning. An EMS event will be raised for the offending CPU. PCBs high pin exceeded EMS event - 2575 PCBs high pin not exceeded EMS event - 2574
PCBS-LOW-PIN-THRESHOLD	0 - 255 Default: 200	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is used by Dashboard to determine the number of Low Pin Process Control Blocks in the processor that are in use during a CPU poll interval, before Reflex flags a warning. An EMS event will be raised for the offending CPU. PCBs Low pin exceeded EMS event - 2573 PCBs Low pin not exceeded EMS event - 2572
PFS-CAPTURE-ENABLED	Y, N Default: N	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is used to control whether PFS metrics are captured for processes by the Dashboard and Specific Process Monitoring modules. Note: Capturing PFS metrics may cause the NMONITOR system process to go busy.



Administration Params

<p>PFS-ALERT-FREQ</p>	<p>1 through 99 Default: 3</p>	<p>Warm-boot Dashboard by going into status monitor set-up and clicking the leftmost partial warm-boot (!) icon.</p>	<p>This parameter is used in conjunction with other PFS Dashboard and CPU-POLL-INTERVAL parameters. It controls how often to output a PFS threshold breached message.</p> <p>An example would be if the PFS-ALERT-INCREASE-COUNT is set to 3, PFS-ALERT-POLL-COUNT is set to 12, PFS-ALERT-FREQ is set to 3 and the CPU-POLL-INTERVAL is set to 30. When these parameters have been set to these values, then Process metrics are retrieved every 30 seconds and if the PFS usage increases at least 3 (PFS-ALERT-INCREASE-COUNT) times in a range of 12 polls, then an alert is raised; any further alerts for the same process will only occur after increasing PFS usage has been detected by more than 3 (PFS-ALERT-FREQ) times.</p>
<p>PFS-ALERT-DN-FREQ</p>	<p>1 through 99 Default: 1</p>	<p>Warm-boot Dashboard by going into status monitor set-up and clicking the leftmost partial warm-boot (!) icon.</p>	<p>This parameter is used in conjunction with other PFS Dashboard and CPU-POLL-INTERVAL parameters. It controls the frequency at which an Down alert is raised when a process continues to use increasing amounts of PFS.</p> <p>An example would be if the PFS-ALERT-DN-FREQ is set to 1, PFS-ALERT-INCREASE-COUNT is set to 3, PFS-ALERT-POLL-COUNT is set to 12, PFS-ALERT-FREQ is set to 3 and CPU-POLL-INTERVAL is set to 30.</p> <p>When these parameters have been set to these values, then the Process metrics are retrieved every 30 seconds and if the PFS usage increases at least 3 (PFS-ALERT-INCREASE-COUNT) times in a range of 12 polls, then a Vulnerable alert is raised. If PFS usage increases for a further (PFS-ALERT-DN-FREQ x PFS-ALERT-INCREASE-COUNT) times, i.e. 3 more times, then a Down alert is raised.</p>
<p>PFS-ALERT-UP-FREQ</p>	<p>1 through 99 Default: 3</p>	<p>Warm-boot Dashboard by going into status monitor set-up and clicking the leftmost partial warm-boot (!) icon.</p>	<p>This parameter is used in conjunction with other PFS Dashboard and CPU-POLL-INTERVAL parameters. It controls the frequency at which an Up alert is raised when a process remains using the same amount of PFS.</p> <p>An example would be if the PFS-ALERT-UP-FREQ is set to 3, PFS-ALERT-INCREASE-COUNT is set to 3, PFS-ALERT-POLL-COUNT is set to 12, PFS-ALERT-FREQ is set to 3 and CPU-POLL-INTERVAL is set to 30. When these parameters have been set to these values, then the Process metrics are retrieved every 30 seconds and if the PFS usage increases at least 3 (PFS-ALERT-INCREASE-COUNT) times in a range of 12 polls, then a Vulnerable alert is raised. If PFS usage remains the same for a further (PFS-ALERT-POLL-COUNT x PFS-ALERT-UP-FREQ) times, i.e. 36 more times, then an Up alert is raised. Note that an Up alert is raised immediately if PFS usage decreases.</p>



Administration Params

PFS-ALERT-IN-CREASE-COUNT	1 through 99 Default: 3	Warm-boot Dashboard by going into status monitor set-up and clicking the leftmost partial warm-boot (!) icon.	<p>This parameter is used in conjunction with other PFS Dashboard and CPU-POLL-INTERVAL parameters. It is used to specify how many times the PFS usage of a process must increase within PFS-ALERT-POLL-COUNT polls before an alert is raised.</p> <p>An example would be if PFS-ALERT-IN-CREASE-COUNT is set to 3, PFS-ALERT-POLL-COUNT is set to 12 and CPU-POLL-INTERVAL is set to 30. When these parameters have been set to these values, then the Process metrics are retrieved every 30 seconds and if the PFS usage increases at least 3 times in a range of 12 polls, then an alert is raised.</p>
PFS-ALERT-POLL-COUNT	1 through 99 Default: 12	Warm-boot Dashboard by going into status monitor set-up and clicking the leftmost partial warm-boot (!) icon.	<p>This parameter is used in conjunction with the other PFS Dashboard and CPU-POLL-INTERVAL parameters. It controls how many polls of Process metrics are examined when checking for increasing amounts of PFS usage.</p>
PFS-ALERT-SUPPRESS	Y, N default: N	Warm-boot Dashboard by going into status monitor set-up and clicking the leftmost partial warm-boot (!) icon.	<p>This parameter is used to suppress PFS usage alert messages. A value of Y enables suppression and a value of N disables suppression.</p>



Administration Params

PMON-INITIAL-INTERVAL	0, or 30-120 Default: 0 (off)	Warmboot the Reaction Module by executing the third step under the (!) icon ("Warmboot Reaction Servers")	This is the time in seconds before the initial Process Monitor checks are performed following a warmboot. Supported values are 0, or 30 to 120 seconds. A value of 0 means that the Process Monitor is to use the PMON-POLL-INTERVAL parameter value.
PMON-MSG-FREQUENCY	1 - 99 Default: 10	Warmboot the Reaction Module by executing the third step under the (!) icon ("Warmboot Reaction Servers")	<p>This parameter controls how often the same EMS event is output if a process is found to be in the same state. For example, if a process is in a DOWN state then Reflex will generate a down EMS event (as configured by the user in the next section).</p> <p>If the process is down the next time it polls then the process monitor will not raise another EMS message until it has polled 'PMON-MSG-FREQUENCY' times at which point, it will raise the down EMS message again. This is to cut down on EMS event pollution on the EMS logs.</p>
PMON-POLL-INTERVAL	15 - 1800 Default: 30	Warmboot the Reaction Module by executing the third step under the (!) icon ("Warmboot Reaction Servers")	<p>This is the poll interval in seconds that the Reflex 80:20 non-stop process monitor will check the configured processes as to their UP/DOWN status.</p> <p>This is used in conjunction with the 'PMON-MSG-FREQUENCY' parameter. The defaults are a frequency of '10' and a poll interval of '30' seconds. The result here would be that a process down would not be re-reported until '10 x 30' seconds later, i.e. 5 minutes.</p>



Administration Params

PROCBABY-BUSY-FREQ	1 through 99 Default: 3	Warm-boot Dashboard by going into status monitor set-up and clicking the left-most partial warm-boot (!) icon.	<p>This parameter is used in conjunction with the optional Busy value which is used when performing Specific Process monitoring. It controls how often to output a Busy message for a specific process being monitored.</p> <p>An example would be, if PROCBABY-BUSY-FREQ is set to 3, then following the initial occurrence of a specific process breaching its busy threshold value and if the subsequent 3 polls found that the process was still busy, no alerts would be generated but an alert would be generated on the 4th poll.</p>
PROCBABY-INTERVAL	15 through 3600 seconds Default: 60	Warm-boot Dashboard by going into status monitor set-up and clicking the left-most partial warm-boot (!) icon.	<p>This parameter is used to control the interval between collection of Specific Process Metrics.</p> <p>Note: If the Interval Value has been changed, then the new interval will ONLY become active once the next poll of the current period is complete, e.g. if the poll interval was set to 10 minutes and the interval value is then changed to 2 minutes, then the change to 2 minutes will only take place after the current 10 minute poll interval has expired.</p>
PROCBABY-PRIORITY	50 through 190 Default: 100	Warm-boot Dashboard by going into status monitor set-up and clicking the left-most partial warm-boot (!) icon.	<p>This parameter controls the priority that the PROCBABY process (created by the PROC-MASTER serverclass) will run at in each CPU.</p>
PROCESS-BUSY-THRESHOLD	0 - 99 Default: 30	Stop/Start Reflex (alternatively warm-boot via Status Monitor set-up (!) icon and Freeze, Stop Thaw & Start the Reflex DASH-THRESH Pathway server)	<p>This parameter is used by Dashboard module to determine when a process should be flagged as being unusually busy for a particular HPE NonStop node. This will result in an EMS message being raised to the EMS log which can optionally be used to drive a graphical icon in the status monitor screen.</p> <p>Exceeded threshold event - 2559</p> <p>No longer exceeded threshold event - 2565</p>



Administration Params

PWYMON-INTERVAL	60 - 28800 Default: 90	Start / Stop REFLEX-PWAY-MON Server-class	This parameter is used to specify the interval in seconds between monitoring polls to the pathway serverclasses.
REFLEX-CATALOG	A valid SQL Catalog subvolume Default \\ITLTECH.\$DEV. RFCATnnn	Stop Reflex. ReSQLCOMPILE and restart Reflex	This parameter is set up at the beginning of a full Reflex 80:20 installation to instruct the SQL compiler to register any Reflex SQL embedded objects with the catalog named here. Once a Reflex SQL catalog is created it should not be touched!
REFLEX-FEEDER-FLAG (This Admin Parameter is obsolete as of version 4.8)	Y, N Default: N	Start/Stop Reflex	This parameter determines whether or not CPU, Disk, File and Status Monitor metrics are relayed to a Fastpipe client on the NonStop node, which then forwards them to a nominated Windows server. The node will affix a timestamp to each record sent. On the Windows machine, the data is written to an ODBC database where it can be accessed for graphing and trending for management reporting. For more information on this aspect of Reflex, contact Insider Technologies. Note: The feeder mechanism requires licensing. The AVAILAB-FEEDER server configuration within PWCONF should be amended with the appropriate details.
REMOTE-SYSTEM-MONIT	Y, N Default: N	Start/Stop Reflex	It is possible (with the aid of EMS forwarding distributors) to send events to a central Reflex 80:20 application where they can be used to drive graphical icons on the Status Monitor screen. If this flag is set to 'Y' then the system check within the Reflex 80:20 ECALLFLT filter (compiled filter - ECALFOBJ) will be taken out and all events from all HPE NonStop platforms with the same SSID and event number will be processed if they have been configured in the local Reaction engine.
RUNTASK-LOCATION	Free text Default: \$DEV. RFOBnnn. RUNTASK	Stop/Start Reflex	This parameter informs the TASKMASTER module of the location of the RUNTASK code. This code is used to initiate any programs configured in the Tasks module of the Reflex GUI.



Administration Params

SMON-GRP-HEALTH	Y, N Default - N	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter dictates whether an EMS event is generated if a top-level group changes status. This event could be used to generate an appropriate reaction for forwarding to an Enterprise Manager. The Events generated are 2457 through 2459.
SMON-GRP-HEALTH-SUPP	Y, N Default - Y	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter does NOT stop the Status Monitor group level monitoring EMS messages from being emitted but controls whether they are seen in normal EMS viewing consoles like CONSOLE, Viewpoint™ and View + Point™. This is achieved by Reflex placing a suppress token in the EMS event to make it invisible on the system. The purpose of this is to allow the event to be seen in the Reflex graphical status monitor display where important events have been consolidated rather than adding more noise to the collectors on the HPE NonStop node.
SMON-RESYNC	Y, N Default :Y	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This flag is used to determine if resync messages are sent between Status Monitor serverclasses. If set to Y, then regular top level group status is sent to ensure that the top level group status is consistent.
SMON-RESYNC-FREQ	60 - 600 Default : 60	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This determines the frequency at which resync messages are sent (in seconds) between the Status Monitor serverclasses.



Administration Params

SPOOLER-FREQUENCY	1 - 99 Default: 1	Stop/Start Agent-Spooler server in the Reflex 80:20 Pathway	This parameter controls the frequency that the same state is reported by way of an EMS event message. For instance, if a spooler component is found to be in error or other offending state, an EMS message will be generated. If it is found to be in the same state <i>N</i> seconds (SPOOLER-INTERVAL) later, it will not be reported until this frequency parameter is reached. If it is set to '1' then it will be reported constantly until the spooler problem is resolved.
SPOOLER-INTERVAL	5 - 720 Default: 5	Stop/Start Agent-Spooler server in the Reflex 80:20 Pathway	This is the poll in minutes that the Reflex 80:20 spooler monitor will check the configured spooler components as to their UP/DOWN/VULNERABLE status. This is used in conjunction with the 'SPOOLER-FREQUENCY' parameter. The defaults are a frequency of 1 and a poll interval of 5 minutes. The result here would be that a spooler component in an offending state would not be re-reported until '1 x 5' minutes later.
SPOOLER-REPORT-EMPTY-FILE	Y,N Default: N	Stop/Start Agent-Spooler server in the Reflex 80:20 Pathway	This parameter is used to control whether 'empty file' messages are produced by the Spooler Agent process. In circumstances where there are no results from a SPOOLCOM command, e.g. SPOOLCOM \$SPLS;DEV, then the results file will be empty which could lead to error messages being generated. On backup nodes where there are no spooler devices configured, this generation of error messages is undesirable.
SPOOLER-SUPPRESS	Y, N Default - N	Stop/Start Agent-Spooler server in the Reflex 80:20 Pathway	This parameter does NOT stop the spooler monitoring EMS messages from being emitted but controls whether they are seen in normal EMS viewing consoles like CONSOLE, Viewpoint™ and View + Point™. This is achieved by Reflex placing a suppress token in the EMS event to make it invisible on the system. The purpose of this is to allow the event to be seen in the Reflex graphical status monitor display where important events have been consolidated rather than adding more 'noise' to the collectors on the HPE NonStop node.
SPOOLER-THRESHOLD	0 - 99 Default: 70	Stop/Start Agent-Spooler server in the Reflex 80:20 Pathway	This is the threshold at which an EMS event will be generated for a spooler collector should it become close to full. The events raised are: 5071 (over threshold) 5072 (spooler full).



Administration Params

STATS-COLLECTOR	Free Text Default: \$DEV. RFOBnnn. STATCOLL	Stop/Start Reflex	Consumer Distributor that collects and tabulates statistics to be output to a printer, disc file or PC Format file. This parameter represents the location of the object file which collects the EMS events for the nominated time window.
STATS-DICT	Free Text Default: \$DEV. RFDDnnn	Stop/Start Reflex	A Reflex 80:20 sub-volume that contains the REFLEX Data Dictionary. The PCFORMAT program used by the Discovery module uses the dictionary to produce a CSV file for the PC. PCFORMAT is supplied by HPE NonStop in earlier release of the K series operating system.
STATS-PROCESS	Valid process name Default: \$STAT	Stop/Start Reflex	When Discovery is selected and a request submitted to graph the various EMS alerts that have occurred within the given time period, the discovery program specified by STATS-COLLECTOR will be given the process name specified here. Only 1 of these processes can be running at any one time.
SUBJECT-HISTORY-SIZE	1 - 1000 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Partial Warmboot (!) icon.	This parameter represents the number of EMS messages held for a particular Status Monitor object. For example, if 5 were selected, then up to 5 events would be held before the oldest event was replaced by the newest. This value can ONLY be amended using the FIXSBJH utility, while Reflex is shut down. For example RUN FIXSBJH /IN <dataconf>/MAX-HISTORY 500 will amend the SUBJECT-HISTORY-SIZE value to 500 and update the SQL tables accordingly.
TASK-Q-LEN	Default: 5	Stop/Start Reflex	The number of tasks of the same name which will be queued for action by TaskMaster.



Administration Params

TCPIP-ARP-LAY-THRESH-INTERVAL	1 - 1440 Default: 60	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is the interval that is used by the Dashboard to check if a TCP/IP ARP Layer threshold has been exceeded.
TCPIP-LISTNER-MSG-FREQ	1-99 Default: 1	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is used in conjunction with the TCPIP-LISTNER-POLL-INTERVAL parameter. It controls 'how often' to output a Listner Down event.
TCPIP-LISTNER-POLL-INTERVAL	60 to 28800 Default: 300	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is the poll interval which is used by Dashboard to poll at the configured number of seconds to check that the TCP/IP Listner process is running.
TCPIP-LISTNER-PROC-SUPPRESS	Y/N Value Default: Y	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon	This parameter is used to control whether the events are suppressed if a TCP/IP Listner process is not running. If set to Y, then the events are not generated.



Administration Params

TCPIP-MSTATE-MSG-FREQ	1 - 99 Default: 2	Via Status Monitor set-up, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is used in conjunction with the TCPIP-SUBNET-POLL-INTERVAL paramter. It controls 'how often' to output an M-State Down message. (See the X25-DASH-MSG-FREQ parameter for an example).
TCPIP-MSTATE-SUPPRESS	Y/N Value Default: N	Via Status Monitor set-up, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is used to control whether the events are suppressed if a TCP/IP v6 Subnet's M-State is in a DOWN state. If set to Y, then events are not generated.
TCPIP-NO-LISTNER-SUPPRESS	Y/N Value Default: N	Via Status Monitor set-up, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is used to control whether the events are suppressed if a TCP/IP process has no Listner process running against it. If set to Y the events are not generated.





Administration Params

TCPIP-PROCESS-POLL-INTERVAL	60 - 28800 Default: 60	Warmboot via the Status Monitor set-up (!) icon. Note that the new interval will ONLY become active once the next poll of the current poll period is complete, i.e. if the poll interval was set to 10 minutes and is then changed to 2 minutes, the change to 2 minutes will only take place after the current 10 minute poll is activated. If such a delay is a problem, then it can be forced by a freeze, stop, thaw and then start of the DASH-THRESH Pathway server, following the warmboot.	This parameter is the poll interval which is used by Dashboard to poll at the configured number of seconds for TCP/IP Process status (includes all TCP/IP layers).
TCPIP-ROUTE-POLL-INTERVAL	60 - 28800 Default: 60	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is the poll interval which is used by Dashboard to poll at the configured number of seconds for TCP/IP Route status.
TCPIP-SUBNET-POLL-INTERVAL	60 - 28800 Default: 60	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is the poll interval which is used by Dashboard to poll at the configured number of seconds for TCP/IP Subnet status.



Administration Params

TCPIP-ROUTE-THRESHOLD-INTERVAL	1 - 1440 Default: 60	Via Status Monitor set-up, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is the interval that is used by the Dashboard to check if a TCP/IP Route threshold has been exceeded.
TCPIP-SUB-THRESHOLD-INTERVAL	1 - 1440 Default: 60	Via Status Monitor set-up, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is the interval that is used by the Dashboard to check if a TCP/IP Subnet threshold has been exceeded.
TCPIP-ICMP-LAY-THRESH-INTERVAL	1 - 1440 Default: 60	Via Status Monitor set-up, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is the interval that is used by the Dashboard to check if a TCP/IP ICMP Layer threshold has been exceeded.
TCPIP-IP-LAY-THRESH-INTERVAL	1 - 1440 Default: 60	Via Status Monitor set-up, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is the interval that is used by the Dashboard to check if a TCP/IP IP Layer threshold has been exceeded.
TCPIP-IP-STATS-THRESH-INTERVAL	1 - 1440 Default: 60	Via Status Monitor set-up, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is the interval that is used by the Dashboard to check if a TCP/IP Process IP Routing Stats threshold has been exceeded.
TCPIP-TELSERV-MSG-FREQ	1-99 Default: 1	Via Status Monitor set-up, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is used in conjunction with the TCPIP-TELSERV-POLL-INTERVAL parameter. It controls 'how often' to output the Telserv Down event.
TCPIP-TELSERV-POLLINTERVAL	60 to 28800 Default: 300	Via Status Monitor set-up, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is the poll interval which is used by Dashboard to poll at the configured number of seconds to check that the TCP/IP Telserv processes are running.
TCPIP-TELSERV-PROCSUPPRESS	Y/N Default: Y	Via Status Monitor set-up, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is used to control whether the events are suppressed if a TCP/IP Telserv process is not running. If set yo Y, then the events are not generated.



Administration Params

TCPIP-UDP-LAY-THRESH-INTERVAL	1 - 1440 Default: 60	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is the interval that is used by the Dashboard to check if a TCP/IP Process UDP Layer threshold has been exceeded.
TCPIP-TCP-LAY-THRESH-INTERVAL	1 - 1440 Default: 60	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is the interval that is used by the Dashboard to check if a TCP/IP Process TCP Layer threshold has been exceeded.
TCPIP-DASH-MSG-FREQ	1 - 99 Default: 2	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is used in conjunction with all the other TCP/IP Dashboard parameters. It controls 'how often' to output a TCP/IP threshold breached message. (see X25-DASH-MSG-FREQ for example)
TCPIP-NO-LISTNER-MSG-FREQ	1 - 99 Default: 2	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is used in conjunction with TCP/IP-PROCESS-POLL-INTERVAL Parameters. It controls 'how often' to output a No Listner message. (see X25-DASH-MSG-FREQ for example)
TCPIP-ARP-IN-REPLY-THRESH	0 - 32768 Default: 200	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is used by Dashboard to determine how many Reply Packets are received at the TCP/IP ARP layer during a TCPIP-ARP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process. An EMS event will be raised for the offending TCP/IP process. Received ARP Replys exceeded EMS event - 5503 Received ARP Replys no longer exceeded EMS event - 5443



Administration Params

TCPIP-ARP-IN-REQUEST-THRESH	0 - 32768 Default: 4000	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Request Packets are received at the TCP/IP ARP layer during a TCPIP-ARP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Received ARP Requests exceeded EMS event - 5502</p> <p>Received ARP Requests no longer exceeded EMS event - 5442</p>
TCPIP-ARP-OUT-REPLY-THRESH	0 - 32768 Default: 200	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Request Packets are sent at the TCP/IP ARP layer during a TCPIP-ARP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Sent ARP Requests exceeded EMS event - 5505</p> <p>Received ARP Requests no longer exceeded EMS event - 5445</p>
TCPIP-ARP-OUT-REQUEST-THRESH	0 - 32768 Default: 200	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Request Packets are sent at the TCP/IP ARP layer during a TCPIP-ARP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Received ARP Replys exceeded EMS event - 5504</p> <p>Received ARP Replys no longer exceeded EMS event - 5444</p>
TCPIP-ICMP-BAD-CHECK-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Bad Checksums are received at the TCP/IP ICMP layer during a TCPIP-ICMP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Bad Checksum exceeded EMS event - 5496</p> <p>Bad Checksum no longer exceeded EMS event - 5436</p>



Administration Params

TCPIP-ICMP-IN-QUENCH-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Source Quench messages are received at the TCP/IP ICMP layer during a TCPIP-ICMP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Source Quench Received exceeded EMS event - 5498</p> <p>Source Quench Received no longer exceeded EMS event - 5438</p>
TCPIP-ICMP-OUT-QUENCH-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Source Quench messages are sent at the TCP/IP ICMP layer during a TCPIP-ICMP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Source Quench Sent exceeded EMS event - 5498</p> <p>Source Quench Sent no longer exceeded EMS event - 5438</p>
TCPIP-ICMP-INV-HEADER-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Invalid Headers are received at the TCP/IP ICMP layer during a TCPIP-ICMP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Invalid Headers Received exceeded EMS event - 5500</p> <p>Invalid Headers Received no longer exceeded EMS event - 5440</p>
TCPIP-ICMP-TOO-SHORT-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Packets that are Too Short are received at the TCP/IP ICMP layer during a TCPIP-ICMP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Packets Too Short exceeded EMS event - 5501</p> <p>Packets Too Short no longer exceeded EMS event - 5441</p>



Administration Params

TCPIP-IP-FRAG-INPUT-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warmboot (!) icon.	<p>This parameter is used by Dashboard to determine how many Fragmented Packets are received at the TCP/IP layer during a TCPIP-ICMP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Fragmented Packets exceeded EMS event - 5484</p> <p>Fragmented Packets no longer exceeded EMS event - 5424</p>
TCPIP-IP-FRAG-TIMEOUT-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warmboot (!) icon.	<p>This parameter is used by Dashboard to determine how many Fragment Timeouts are received at the TCP/IP layer during a TCPIP-ICMP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Fragment Timeouts exceeded EMS event - 5486</p> <p>Fragment Timeouts no longer exceeded EMS event - 5426</p>
TCPIP-IP-INV-HEADER-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warmboot (!) icon.	<p>This parameter is used by Dashboard to determine how many Invalid Headers are received at the TCP/IP layer during a TCPIP-ICMP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Invalid Headers exceeded EMS event - 5487</p> <p>Invalid Headers no longer exceeded EMS event - 5427</p>
TCPIP-IP-PACK-CANT-FWD-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warmboot (!) icon.	<p>This parameter is used by Dashboard to determine how many Packets Can't be Forwarded at the TCP/IP layer during a TCPIP-ICMP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Packets Can't Forward exceeded EMS event - 5488</p> <p>Packets Can't Forward no longer exceeded EMS event - 5428</p>
TCPIP-IP-PACK-TOO-SMALL-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warmboot (!) icon.	<p>This parameter is used by Dashboard to determine how many Packets are received that are Too Small at the TCP/IP layer during a TCPIP-ICMP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Packets Too Small exceeded EMS event - 5488</p> <p>Packets Too Small no longer exceeded EMS event - 5428</p>



Administration Params

<p>TCPIP-IP-SHORT-PACKET-THRESH</p>	<p>0 - 32768 Default: 10</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine how many Short Packets are received at the TCP/IP layer during a TCPIP-ICMP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Short Packets exceeded EMS event - 5490</p> <p>Short Packets no longer exceeded EMS event - 5430</p>
<p>TCPIP-IP-BAD-ROUTE-THRESH</p>	<p>0 - 32768 Default: 10</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine how many Bad Route Redirects are received at TCP/IP IP Routing during a TCPIP-IP-STATS-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Bad Route Redirects exceeded EMS event - 5491</p> <p>Bad Route Redirects no longer exceeded EMS event - 5431</p>
<p>TCPIP-IP-DYNAMIC-THRESH</p>	<p>0 - 32768 Default: 10</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine how many Dynamic Redirects are received at TCP/IP IP Routing during a TCPIP-IP-STATS-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Dynamic Redirects exceeded EMS event - 5492</p> <p>Dynamic Redirects no longer exceeded EMS event - 5432</p>
<p>TCPIP-IP-UNREACHABLE-THRESH</p>	<p>0 - 32768 Default: 10</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine how many Unreachable Routes are received at TCP/IP IP Routing during a TCPIP-IP-STATS-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Unreachable Routes exceeded EMS event - 5495</p> <p>Unreachable Routes no longer exceeded EMS event - 5435</p>



Administration Params

<p>TCPIP-ICMP-UNREACHABLE-THRESH</p>	<p>0 - 32768 Default: 10</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine how many Destination Unreachable messages are received at the TCP/IP ICMP layer during a TCPIP-ICMP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Destination Unreachable exceeded EMS event - 5497</p> <p>Destination Unreachable no longer exceeded EMS event - 5437</p>
<p>TCPIP-IP-BAD-CHECK-THRESH</p>	<p>0 - 32768 Default: 10</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine how many Bad Checksum are received at the TCP/IP layer during a TCPIP-ICMP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Bad Checksum exceeded EMS event - 5482</p> <p>Bad Checksum no longer exceeded EMS event - 5422</p>
<p>TCPIP-IP-BAD-PACKET-THRESH</p>	<p>0 - 32768 Default: 10</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine how many Bad Packets are received at the TCP/IP layer during a TCPIP-ICMP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Bad Packets exceeded EMS event - 5483</p> <p>Bad Packets no longer exceeded EMS event - 5423</p>
<p>TCPIP-IP-FRAG-DROPPED-THRESH</p>	<p>0 - 32768 Default: 10</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine how many Dropped Fragments are received at the TCP/IP layer during a TCPIP-ICMP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Dropped Fragments exceeded EMS event - 5485</p> <p>Dropped Fragments no longer exceeded EMS event - 5425</p>



Administration Params

<p>TCPIP-IP-WILDCARD-THRESH</p>	<p>0 - 32768 Default: 10</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine how many Wildcard Matches are received at TCP/IP IP Routing during a TCPIP-IP-STATS-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Wildcard Matches exceeded EMS event - 5495</p> <p>Wildcard Matches no longer exceeded EMS event - 5435</p>
<p>TCPIP-IP-NEW-GATEWAY-THRESH</p>	<p>0 - 32768 Default: 10</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine how many New Gateway Redirects are received at TCP/IP IP Routing during a TCPIP-IP-STATS-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>New Gateway Redirects exceeded EMS event - 5493</p> <p>New Gateway Redirects no longer exceeded EMS event - 5433</p>
<p>TCPIP-ROUTE-USAGE-THRESHOLD</p>	<p>0 - 900000 Default: 70000</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine the Route Usage during a TCPIP-ROUTE-THRESHOLD-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP route.</p> <p>An EMS event will be raised for the offending TCP/IP route.</p> <p>Route Usage exceeded EMS event - 5360</p> <p>Route Usage no longer exceeded EMS event - 5350</p>
<p>TCPIP-SUBNET-ERRORS-THRESHOLD</p>	<p>0 - 32768 Default: 10</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine the number of Subnet Errors during a TCPIP-SUB-THRESHOLD-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP subnet.</p> <p>An EMS event will be raised for the offending TCP/IP subnet.</p> <p>Subnet Received Errors exceeded EMS event - 5392</p> <p>Subnet Sent Errors exceeded EMS event - 5393</p> <p>Subnet Received Errors no longer exceeded EMS event - 5372</p> <p>Subnet Sent Errors no longer exceeded EMS event - 5373</p>



Administration Params

<p>TCPIP-SUBNET-PACKET-THRESHOLD</p>	<p>0 - 900000 Default: 70000</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine the number of Subnet Packets Sent/Received during a TCPIP-SUB-THRESHOLD-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP subnet.</p> <p>An EMS event will be raised for the offending TCP/IP subnet.</p> <p>Subnet Packets Received exceeded EMS event - 5391</p> <p>Subnet Packets Sent exceeded EMS event - 5390</p> <p>Subnet Packets Received no longer exceeded EMS event - 5371</p> <p>Subnet Packets Sent no longer exceeded EMS event - 5370</p>
<p>TCPIP-TCP-BAD-CHECK-THRESH</p>	<p>0 - 32768 Default: 10</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine how many Bad Checksums are received at the TCP/IP TCP layer during a TCPIP-TCP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Bad Checksum exceeded EMS event - 5470</p> <p>Bad Checksum no longer exceeded EMS event - 5410</p>
<p>TCPIP-TCP-BAD-OFF-THRESH</p>	<p>0 - 32768 Default: 10</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine how many Bad Offsets are received at the TCP/IP TCP layer during a TCPIP-TCP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Bad Offsets exceeded EMS event - 5471</p> <p>Bad Offsets no longer exceeded EMS event - 5411</p>



Administration Params

TCPIP-TCP-CONN-CLOSED-THRESH	0 - 32768 Default: 5000	Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Closed Connections are at the TCP/IP TCP layer during a TCPIP-TCP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Closed Connections exceeded EMS event - 5471</p> <p>Closed Connections no longer exceeded EMS event - 5411</p>
TCPIP-TCP-CONN-DROPPED-THRESH	0 - 32768 Default: 20	Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Dropped Connections are at the TCP/IP TCP layer during a TCPIP-TCP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Dropped Connections exceeded EMS event - 5476</p> <p>Dropped Connections no longer exceeded EMS event - 5416</p>
TCPIP-TCP-CONN-TIME-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Times Out Connections are at the TCP/IP TCP layer during a TCPIP-TCP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Timed Out Connections exceeded EMS event - 5474</p> <p>Timed Out Connections no longer exceeded EMS event - 5414</p>
TCPIP-TCP-EST-CONN-THRESH	0 - 32768 Default: 2000	Via Status Monitor set-up, warmboot Dashboard by clicking the left-most Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Established Connections are at the TCP/IP TCP layer during a TCPIP-TCP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Established Connections exceeded EMS event - 5477</p> <p>Established Connections no longer exceeded EMS event - 5417</p>



Administration Params

TCPIP-TCP-INV-HEADER-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Invalid Headers are received at the TCP/IP TCP layer during a TCPIP-TCP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Invalid Headers exceeded EMS event - 5472</p> <p>Invalid Headers no longer exceeded EMS event - 5412</p>
TCPIP-TCP-KEEP-ALIVE-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Keep Alive Messages are Dropped at the TCP/IP TCP layer during a TCPIP-TCP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Keep Alive Dropped exceeded EMS event - 5472</p> <p>Keep Alive Dropped no longer exceeded EMS event - 5412</p>
TCPIP-TCP-NO-PORT-PACK-THRESH	0 - 32768 Default: 100	Via Status Monitor set-up, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many packets are received that have No Port at the TCP/IP TCP layer during a TCPIP-TCP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>No Ports Dropped exceeded EMS event - 5506</p> <p>No Ports Dropped no longer exceeded EMS event - 5446</p>
TCPIP-TCP-RETRANS-PACK-THRESH	0 - 32768 Default: 200	Via Status Monitor set-up, warm-boot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many packets are Retransmitted at the TCP/IP TCP layer during a TCPIP-TCP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Retransmitted Packets exceeded EMS event - 5473</p> <p>Retransmitted Packets no longer exceeded EMS event - 5413</p>



Administration Params

TCPIP-UDP-BAD-CHECK-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Bad Checksums are received at the TCP/IP UDP layer during a TCPIP-UDP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Bad Checksums exceeded EMS event - 5479</p> <p>Bad Checksums no longer exceeded EMS event - 5419</p>
TCPIP-UDP-BAD-PACKET-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Packets with a Bad Size are received at the TCP/IP UDP layer during a TCPIP-UDP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Bad Packet Size exceeded EMS event - 5480</p> <p>Bad Packet Size no longer exceeded EMS event - 5420</p>
TCPIP-UDP-INV-HEADER-THRESH	0 - 32768 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Invalid Headers are received at the TCP/IP UDP layer during a TCPIP-UDP-LAY-THRESH-INTERVAL Threshold interval, before Reflex flags a warning on the TCP/IP process.</p> <p>An EMS event will be raised for the offending TCP/IP process.</p> <p>Invalid Headers exceeded EMS event - 5480</p> <p>Invalid Headers no longer exceeded EMS event - 5420</p>
TIME-OUT	>= 120 seconds. Default: 3600 seconds	Legacy	Used previously for the Reflex 'green screen' time out, if the session was not used after a period of time. The 'green screen' interface is no longer supported.
TITLE	Free text default: '.'	Legacy	Used for the Title bar in 'green screen' version of Reflex. This interface is no longer supported.
TLES-CURRENT-THRESHOLD	0 - 1250 Default: 1000	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine the number of Time List Elements in the Processor that are in use during a CPU poll interval, before Reflex flags a warning.</p> <p>An EMS event will be raised for the offending CPU:</p> <p>TLEs exceeded - 2577</p> <p>TLEs no longer exceeded - 2576</p>



Administration Params

TREE-PROCESSING-QUEUE	0 - 100 Default: 70	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	Used between the Event Monitor and Status Monitor during a warmboot so that events are not lost when this is being executed.
X25-DASH-MSG-FREQ	1 - 99 Default: 2	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used in conjunction with all the other Dashboard parameters. It controls 'how often' to output a X25 threshold breached message.</p> <p>An example would be, if the X25-POLL-INTERVAL is set to 15 seconds and X25-DASH-MSG-FREQ set to 5 then a X25 SU not started message would only be output if the SU was seen to be not started for 15 x 5 seconds (1 minute 15 seconds). At this point, a X25 SU not started EMS message would be raised by Dashboard.</p>
X25-FRAME-RECV-REJ-THRESHOLD	0 - 1000 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Rejects were received at the Frame Level, during a Frame Level Threshold interval, before Reflex flags a warning on the X25 line.</p> <p>An EMS event will be raised for the offending X25 line.</p> <p>Received Rejects at Frame Level exceeded EMS event - 2597</p> <p>Received Rejects at Frame Level no longer exceeded EMS event - 2596</p>
X25-FRAME-RECV-RNR-THRESHOLD	0 - 1000 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many RNR's were received at the Frame Level, during a Frame Level Threshold interval, before Reflex flags a warning on the X25 line.</p> <p>An EMS event will be raised for the offending X25 line.</p> <p>Received RNR's at Frame Level exceeded EMS event - 2595</p> <p>Received RNR's at Frame Level no longer exceeded EMS event - 2594</p>
X25-FRAME-SENT-REJ-THRESHOLD	0 - 1000 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Rejects were sent at the Frame Level, during a Frame Level Threshold interval, before Reflex flags a warning on the X25 line.</p> <p>An EMS event will be raised for the offending X25 line.</p> <p>Sent Rejects at Frame Level exceeded EMS event - 2593</p> <p>Sent Rejects at Frame Level no longer exceeded EMS event - 2592</p>



Administration Params

X25-FRAME-SENT-RNR-THRESHOLD	0 - 1000 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many RNR's were sent at the Frame Level, during a Frame Level Threshold interval, before Reflex flags a warning on the X25 line.</p> <p>An EMS event will be raised for the offending X25 line.</p> <p>Sent Rejects at Frame Level exceeded EMS event - 2591</p> <p>Sent Rejects at Frame Level no longer exceeded EMS event - 2590</p>
X25-FRAME-THRESHOLD-INTERVAL	1 - 1440 Default: 60	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This is the interval that is used by the Dashboard Threshold code to check if a X25 Frame Level threshold has been exceeded.
X25-LINE-QUALITY-THRESHOLD	0 - 100 Default: 90	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine the percentage of line quality before Reflex flags a warning on the X25 line.</p> <p>An EMS event will be raised for the offending line:</p> <p>Note that this parameter is a MINIMUM value, i.e. when the line quality is below the specified parameter value, then the line quality is exceeded.</p> <p>Line quality exceeded - 2586</p> <p>Line quality no longer exceeded - 2585</p>
X25-MODEM-ERR-THRESH-INTERVAL	1 - 1440 Default: 60	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	This parameter is the interval that is used by the Dashboard to check if the Modem Error threshold has been exceeded.
X25-MODEM-ERROR-THRESHOLD	0 - 1000 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many modem errors occur during a modem error threshold interval before Reflex flags a warning on the X25 line.</p> <p>An EMS event will be raised for the offending X.25 line:</p> <p>Modem errors exceeded - 2588</p> <p>Modem errors no longer exceeded - 2587</p>
X25-NUMBER-OF-SU-TO-MONITOR	0 - 1000 Default: 50	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to allocate memory for an internal table holding the state of the SU's we will monitor.</p> <p>It should be large enough to accommodate the number of SU's on all X25 lines that are configured for monitoring by Reflex.</p>



Administration Params

X25-PACKET-RECV-REST-THRESHOLD	0 - 1000 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Restarts were received at the Packet Level, during a Packet Level Threshold interval, before Reflex flags a warning on the X25 line.</p> <p>An EMS event will be raised for the offending X25 line.</p> <p>Received Restarts at Packet Level exceeded EMS event - 5244</p> <p>Received Restarts at Packet Level no longer exceeded EMS event - 5245</p>
X25-PACKET-RECV-RNR-THRESHOLD	0 - 1000 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many RNR's were received at the Packet Level, during a Packet Level Threshold interval, before Reflex flags a warning on the X25 line.</p> <p>An EMS event will be raised for the offending X25 line.</p> <p>Received RNR's at Packet Level exceeded EMS event - 5243</p> <p>Received RNR's at Packet Level no longer exceeded EMS event - 5242</p>
X25-PACKET-SENT-REST-THRESHOLD	0 - 1000 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many Restarts were sent at the Packet Level during a Packet Level Threshold before Reflex flags a warning on the X25 line.</p> <p>An EMS event will be raised for the offending X25 line.</p> <p>Sent Restarts at Packet Level exceeded EMS event - 5240</p> <p>Sent Restarts at Packet Level no longer exceeded EMS event - 5241</p>
X25-PACKET-SENT-RNR-THRESHOLD	0 - 1000 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is used by Dashboard to determine how many RNR's were sent at the Packet Level, during a Packet Level Threshold interval, before Reflex flags a warning on the X25 line.</p> <p>An EMS event will be raised for the offending X25 line.</p> <p>Sent RNR's at Packet Level exceeded EMS event - 2599</p> <p>Sent RNR's at Packet Level no longer exceeded EMS event - 2598</p>
X25-PACKET-THRESHOLD-INTERVAL	1 - 1440 Default: 10	Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.	<p>This parameter is the interval that is used by the Dashboard to check if a X25 Packet Level threshold has been exceeded.</p>



Administration Params

<p>X25-POLL-INTERVAL</p>	<p>60 - 28800 Default: 60</p>	<p>Warmboot via the Status Monitor set-up (!) icon. Note that the new interval will ONLY become active once the next poll of the current poll period is complete, i.e. if the poll interval was set to 10 minutes and is then changed to 2 minutes, the change to 2 minutes will only take place after the current 10 minute poll is activated. If such a delay is a problem, then it can be forced by a freeze, stop, thaw and then start of the DASH-THRESH Pathway server, following the warmboot.</p>	<p>This parameter is the X25 poll interval which is used by Dashboard to poll at the configured number of seconds for X25 status.</p>
<p>X25-SU-IN-USE-THRESHOLD</p>	<p>0 - 100 Default 70</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used by Dashboard to determine the percentage of how many SU's are in use (started) out of the available SU's before Reflex flags a warning on the X25 line.</p> <p>An EMS event will be raised for the offending X25 line.</p> <p>SU in use exceeded EMS event - 2584</p> <p>SU in use no longer exceeded EMS event - 2583</p>
<p>X25-SU-NOT-STARTED-SUPPRESS</p>	<p>Y, N Default: N</p>	<p>Via Status Monitor set-up, warmboot Dashboard by clicking the leftmost Partial Warm-boot (!) icon.</p>	<p>This parameter is used to control whether events are suppressed for any X25 SU's that are not started on a line that is being monitored.</p>



13. Installation and Configuration Issues

Overview

This section covers extra installation and configuration issues that are not covered in the Installation Guide. It is recommended that you work through the Installation and Quick Start Guides before referring to this section.

Activating your HPE NonStop SQL Licence

Read the HPE NonStop manual 'NonStop SQL/MP Installation and Management Guide', section 'Initialising SQL/MP'.

Execute all of the steps in this section to initialise your HPE NonStop SQL software.

Merging Reflex 80:20 EMS Templates Reference

This section is only a guide to be used in conjunction with the HPE NonStop manuals referred to elsewhere.

Installing the Reflex 80:20 EMS templates for the HPE NonStop Integrity or Blade series platforms:

Note: It is worth replacing specific references below to your own site-specific references first before attempting to merge the Reflex 80:20 EMS templates into your current set.

1. Logon as SUPER.SUPER onto your Reflex 80:20 HPE NonStop system.

2. At a TACL prompt type:

```
>SCF          [return]
```

3. Once in SCF, type the following:

```
1-> ASSUME SUBSYS $ZZKRN          [return]
```

```
2-> INFO                          [return]
```

```
NonStop KERNEL - Info SUBSYS  \ITLTECH.$ZZKRN
```

```
Current Settings
```

```
*DAYLIGHT_SAVING_TIME ..... TABLE
*NONRESIDENT_TEMPLATES..... $SYSTEM.SYS02.TEMPLATE
*POWERFAIL_DELAY_TIME..... 30
*RESIDENT_TEMPLATES..... $SYSTEM.SYS02.RTEMPLATE
  SUPER_SUPER_IS_UNDENIABLE..... OFF
*SYSTEM_NAME..... \ITLTECH
*SYSTEM_NUMBER..... 100
  SYSTEM_PROCESSOR_TYPE ..... NSR-W
*TIME_ZONE_OFFSET..... +00:00
```

```
Pending Changes (will take effect at next system load)
```

```
None
```

A display similar to the text above will be shown. This output shows where the resident and non-resident EMS template files are located on your HPE NonStop system.

4. Exit from SCF by typing 'EXIT [return]'.
5. At a TACL prompt, type the following (replace the references given with your own site-specific references retrieved with your SCF commands).

```
> FUP DUP $system.sys02.template, $system.sys10.zztempla [return]
```



Installation and Configuration Issues

6. Type the following command (using your own file references):

```
>TEMPLI $system.sys02.rtplate, $system.sys02.template [return]
```

Note: Having entered TEMPLI, take a note of the output file produced so that we can use it in a later step, e.g. ZZTP0000

7. Once in TEMPLI, type the following command (using your own file references):

```
> FILE ZZtempla [return]
> FILE $<your Reflex 80:20 volume>.RFLXDDL.NRESTEMP [return]
> FILE $system.system.EVENTTD [return]
> FILE <other third-party product templates> [return]
> EXIT [return]
```

where RFLXDDL is your Reflex 80:20 Dictionary sub-volume and EVENTTD are your TANDEM templates (usually on \$system).

Note: An example method of finding the location of 'EVENTTD' on your HPE NonStop system would be to enter the following command at a TACL prompt:

```
> PATHCOM $ZVPT [return]
> INFO ZVPT-EVNT-DETL [return]
```

where \$ZVPT is the PATHWAY name for your own Viewpoint PATHWAY.

The name and location of the EVENTTD file will be displayed in the returned details of the INFO command above.

8. After the build has taken place, type the following (with your own references):

```
> alter define =_ems_templates, file $system.sys02.template [return]
```

9. Type the following commands (with your own references):

```
> FUP RENAME $system.sys02.template, $system.sys02.ZZTEMPLA [return]
> FUP RENAME $system.sys02.ZZTP0000, $system.sys02.template [return]
```

where the ZZTP0000 is the name of the file produced in step [6].

10. Type the following command:

```
> SCF [return]
```

11. Once in SCF, type the following commands (with your own references):

```
> ASSUME SUBSYS $ZZKRN [return]
> INFO ALLPROCESSORS [return]
> ALTER SUBSYS $ZZKRN, RESIDENT $system.sys02.rtplate, NONRESIDENT
$system.sys02.template [return]
> EXIT [return]
```

Note: If both the resident and non-resident template files point to '\$system.system' then this 'alter' command does not need to be carried out. This is because any 'sysnn' template inclusions are resolved. If the names you are using for your filenames are different however then the alter command will be required.



Installation and Configuration Issues

12. At a TACL prompt, type the following commands (with your own references):

```
> FUP SECURE $system.sys02.template, "NNOO" [return]
> FUP SECURE $system.sys02.rtplate, "NNOO" [return]
```

These commands allow applications to see the template files. Amend your 'rwp' security in line with your security settings for the HPE NonStop system.

Note: In order to view the Reflex 80:20 "Cause", "Effect" and "Recovery" fields in Viewpoint™, you must also merge the Reflex 80:20 NRESTEMP file into the Viewpoint EVENTTD templates file using the TEMPLI command as follows:

Shutdown Viewpoint Pathway

```
1> PATHCOM $ZVPT
= SHUTDOWN2, MODE IM (Using appropriate user id)
```

2> Logon super.super

```
> VOLUME to location of the EVENTTD file, e.g. $SYSTEM.SYSTEM
> FUP LISTOPENS EVENTTD – check for any other processes which have EVENTTD open.
  These will need to be stopped.
> FUP DUP EVENTTD, OEVENTTD (Take backup as a precaution)
```

3> TEMPLI ZZRES, \$<DISK>.<SUBVOL>.EVENTTD

Specify a *temporary subvolume* for EVENTTD. **Do not** specify the current EVENTTD file, e.g. \$SYSTEM.SYSTEM.EVENTTD!

TEMPLI will then provide a prompt >

Within the TEMPLI interface, enter the following:

```
> FILE $SYSTEM.SYSTEM.EVENTTD
> FILE $DISK.RFLXDDL.NRESTEMP (Reflex 80:20 template file, located within the DDL
  subvolume)
> FILE (specify any other third party EMS templates)
> FILE (specify any other third party EMS templates)
> EXIT
```

You should now start to receive output from TEMPLI similar to below:

For file \$SYSTEM.SYSTEM.EVENTTD:

```
TANDEM.ODP (2) (???) - formatting version: D20 (01 JAN 01 00:00) TANDEM.TAPE (4)
(???) - formatting version: F40 (01 JAN 01 00:00)
TANDEM.DNS (5) (???) - formatting version: D20 (01 JAN 01 00:00)
TANDEM.PUP (7) (???) - formatting version: D30 (01 JAN 01 00:00)
TANDEM.PATHWAY (8) (???) - formatting version: D42 (01 JAN 01 00:00) TANDEM.BAT (9)
(???) - formatting version: D30 (01 JAN 01 00:00)
TANDEM.TMF (10) (???) - formatting version: D05 (01 JAN 01 00:00)
TANDEM.EMS (12) (???) - formatting version: F40 (01 JAN 01 00:00)
```

etc...

```
TANDEM.SPR (206) (???) - formatting version: G03 (01 JAN 01 00:00)
15114 templates added, 0 templates replaced.
```



Installation and Configuration Issues

Etc...

For file \$DISK.RFLXDDL.NRESTEMP:

```
INSIDER.REFLEX (50) (RFX) - formatting version: Reflex 80:20 Version n.n  
(date & time)
```

number templates added, 0 templates replaced.

For output templates:

```
INSIDER.REFLEX (50) (RFX) - formatting version: Reflex 80:20 Version n.n  
(date & time)
```

etc...

Once TEMPLI has completed the merge, you will be presented with output similar to below:

```
Resident templates file: $SYSTEM.SYSTEM.ZZRES
```

```
Nonresident templates file: <Temporary disk.subvolume>.EVENTTD
```

```
Templates: 16380
```

```
Resident templates: 97
```

```
Resident size (bytes): 12288
```

```
Warnings: 0
```

```
Errors: 0
```

4> VOLUME <Temporary disk.subvolume>

5> FUP DUP EVENTTD, \$SYSTEM.SYSTEM.*, PURGE, SAVEALL

Start Viewpoint Pathway again and any other applications which accessed this system template file.



Installation and Configuration Issues

Viewpoint - Copying EMS Events into Reflex 80:20

Note: This section is included for completeness but the Reflex 80:20 module CONSOLE can be used exclusively to copy EMS events into the Reflex 80:20 database. From here the EMS event can be configured to invoke the appropriate Reflex 80:20 reaction.

Reflex 80:20 CONSOLE (also available as ITL's View + Point product) includes the most useful aspects of Viewpoint and HPE NonStop EMSA (EMS Analyser).

If you have Viewpoint on the HPE NonStop system where Reflex 80:20 has been installed, then there is a further facility available which enables Viewpoint events to be placed in the Reflex 80:20 database. This is done using the Viewpoint "EXTRAS" function key (SF15) provided as standard with Viewpoint.

In order to make use of this facility the following conditions must be satisfied:

You must have Viewpoint on your HPE NonStop system

The file supplied by Insider Technologies (ZVPT-EXTRAS) which is called by the SF15=EXTRAS function key in Viewpoint must be in the Viewpoint PATHWAY. This is done (while logged on with sufficient security privilege to modify Viewpoint) as follows:

```
> SCUP COPY RFLXOBJ.POBJ (ZVPT-EXTRAS (*)),
<Viewpoint Sub-Volume>.POBJ [return]
```

where RFLXOBJ is your Reflex 80:20 object sub-volume

The Viewpoint PATHWAY must be modified to include the Insider Technologies supplied server, REFLEX-CONTEXT.

Note: Edit/Tedit the Reflex 80:20 supplied file 'VWPTSERV' which is located in your Reflex 80:20 object sub-volume. Change the sub-volume references, home-term, CPUs, process name to your own preferred site-specific references.

Carry out the following command after the above edit:

```
> PATHCOM/in RFLXOBJ.VWPTSERV/$<Viewpoint PATHMON Process>[return]
```

where RFLXOBJ is your Reflex 80:20 object sub-volume

Note: The location of the Viewpoint Marked Events file (EVNTMKRD) may also need to be changed if it has not been done using RFINSTAL and RFDEFS. The logical name of the file is EVNTMKRD. Logon to the Reflex 80:20 GUI and click on the ADMIN button on the main toolbar. Scroll down the list of file records until EVNTMKRD is seen and subsequently double-click on this record. Change the record to point to the actual location of the EVNTMKRD file and then click on the AMEND key (the tick icon on the dialog toolbar). Refer to Chapter [3] of the Reflex 80:20 User Manual.



Unpak and Load the Reflex 80:20 Licence Files

The license files will be supplied in a PAK file and will contain the following 4 files:

- FACILDB - the Reflex 80:20 facilities that can be used in an installation.
- LICENCE - the nodes upon which Reflex 80:20 can be installed and loaded.
- RFLXFAC - an edit version of the FACILDB file which can be extended and reloaded with assistance from Insider Technologies.
- RFLXLIC - an edit version of the LICENCE file which can be extended and reloaded with assistance from Insider Technologies.

Note: It is important to shutdown the Reflex environment before any new licence files are installed, as the 'old' licence files may be open by user sessions.

1. Logoff all Reflex GUI sessions.
2. Volume to the Reflex Object subvolume, e.g. RFLXOBJ and shutdown Reflex:

```
RFLXOBJ>OBEY STOPRFLX
```

3. Via the Reflex Database subvolume, e.g. RFLXDAT, rename the current versions of the above files; for example:

```
RFLXDAT>FUP RENAME FACILDB, OFACILDB
```

4. Using FTP, download the PAK file as a binary file to a temporary subvolume, e.g. RFLXTEMP.

5. Alter the code of the PAK file to 800, i.e.:

```
RFLXTEMP>FUP ALTER <licence PAK file>, CODE 800
```

6. Run the PAK file to restore the licence files to your database subvolume:

```
RUN <licence PAK file>, $*.*.* , MAP NAMES &
($*.*.* TO $<volume>.RFLXDAT), &
LISTALL, OPEN, AUDITED, MYID
```

7. Volume to the Reflex Object subvolume and restart Reflex:

```
RFLXOBJ>OBEY RUNRFLX
```



Monitoring Reflex 80:20 GUI Client Connectivity with Reflex 80:20 Ping

It is not unheard of in the PC world, for PC workstations (or GUIs) to become frozen or locked out in some manner. If more than one PC is being configured with the Reflex 80:20 GUI client, then it will be useful to implement some workstation monitoring. In this regime, one workstation looks out for the interests of another.

How it works:

To activate the 'pulses' from the workstation, the following parameter needs to be added to the 'REFLEX.ini' file under [APPLICATIONS].

Workstation Ping = n

n = 1 – Ping Activated

n = 0 – Ping Deactivated

The PC workstation where the Reflex 80:20 GUI client is installed can be configured to send a pulse message to the HPE NonStop at minute intervals. To configure this to occur for your Reflex 80:20 client, edit the 'REFLEX.ini' file on your Reflex 80:20 PC directory (as shown below) and change the flag 'Workstation Ping' to a value of '1'.

If this parameter is not present in the 'REFLEX.ini' file then Ping Deactivated is assumed.

```
[WORKBENCH]
Large Buttons=1
Sounds=0

[APPLICATIONS]
DASHBOARD=.\DASH.EXE
WorkStation Ping=1

[POSITIONS]
Network Monitor=7 7 292 292
Status Monitor=23 38 1028 449
Admin=6 5 955 606
Discovery=0 0 689 359
Task
.
.
.
.
```

If the ping server 'REFLEX-PING' does not receive a pulse message for more than a 2 minutes then it raises an EMS message. This is a parameter set-up in your own 'REFLEX.ini' file. The ping server takes the decision that the PC is no longer operational.

The EMS message produced has the following format '**INSIDER.50.2650**'. This message can then be seen on an operators EMS viewing console (or can be configured to alert to the Status Monitor graphical display – see later – for another Reflex 80:20 GUI client to flash as critical).

The manager token of this EMS message is set to the 'REFLEX-PING' process and subject token set to the TERM name of your PC workstation stated in your 'SERVER.ini' file.



14. Currently Delivered Reaction Event Ranges

This section describes the pre-delivered Reaction module database that can be seen by clicking on the Reaction button on the main toolbar of Reflex 80:20, maximising the Reaction window and then clicking on the Reaction List tab to display the list of currently set-up event ranges.

If any of these events are not required to be alerted on, amend the cover period for the event range by double clicking on the event and subsequently going into the Action Group tab to amend the cover period. After this, warm-boot the reaction servers by clicking on the '!' icon and carrying out the third option. For a description of the cause, effect and recovery texts (for the 'INSIDER.50' events), edit the TEMPLATE file in your Reflex 80:20 DDL dictionary sub-volume and search on the event numbers.

Several of the reactions detailed in the table below are pre-installed in the Reflex Database. Reactions that are not pre-installed can be imported using the RFIMEX utility. Please see the RFIMEX utility section for further details.

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
CLOCKMON.01	+00001 - +00999	01/01/1997 00:00	01/01/2050 23:59	CLOCKMON-ALERTS	MultiBatch clockmon alert events generated when a unit is not started by a specific time.
INSIDER.6	+00409	20/3/1996 00:00	20/3/2020 23:59	EVENT-TIMER-ALERT	MultiBatch Event-Timer event. "ETI job held in BMON"
INSIDER.50	+00001	20/03/1996 00:00	20/03/2020 23:59	TAP-PROTOCOL-EXAMPLE	This is an example of a typical set-up for paging to a modem plugged into the back of the HPE NonStop node. Cover period not active for this event range.
INSIDER.50	+02553 - +02556	20/03/1996 00:00	20/03/2020 23:59	DASHBOARD-SYSTEM-METS1	These events are threshold exceeded messages for CPUs and disks; CPU busy, > Page Faults, > CPU Queue and > disk space respectively.
INSIDER.50	+02558 - +02560	20/03/1996 00:00	20/03/2020 23:59	DASHBOARD-SYSTEM-METS2	Suspect process Messages; non-running state, > % busy, priority changed respectively.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
INSIDER.50	+02561 - +02565	20/03/1996 00:00	20/03/2020 23:59	DASHBOARD-SYSTEM-METS3	These events are threshold NO LONGER exceeded messages for CPUs and disks: CPU not busy, < Page Faults, < CPU Queue and < disk space respectively.
INSIDER.50	+02566	20/03/1996 00:00	20/03/2020 23:59	DASHBOARD-SYSTEM-METS4	Disk fragmentation parameter has been exceeded.
INSIDER.50	+02567	20/03/1996 00:00	20/03/2020 23:59	DASHBOARD-SYSTEM-METS5	Disk fragmentation parameter is no longer exceeded.
INSIDER.50	+02568	01/01/1997 0:00	01/01/2050 23:59	CPU-UP	CPU Memory pressure UP
INSIDER.50	+02569	01/01/1997 0:00	01/01/2050 23:59	CPU-VULN	CPU Memory pressure VULNERABLE
INSIDER.50	+02570	01/01/1997 0:00	01/01/2050 23:59	CPU-UP	CPU Memory Queue Length UP
INSIDER.50	+02571	01/01/1997 0:00	01/01/2050 23:59	CPU-VULN	CPU Memory Queue Length VULNERABLE
INSIDER.50	+02572	01/01/1997 0:00	01/01/2050 23:59	CPU-UP	CPU Lowpin PCB UP



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
INSIDER.50	+02573	01/01/1997 0:00	01/01/2050 23:59	CPU-VULN	CPU Lowpin PCB VULNERABLE
INSIDER.50	+02574	01/01/1997 0:00	01/01/2050 23:59	CPU-UP	CPU Highpin PCB UP
INSIDER.50	+02575	01/01/1997 0:00	01/01/2050 23:59	CPU-VULN	CPU Highpin PCB VULNERABLE
INSIDER.50	+02576	01/01/1997 0:00	01/01/2050 23:59	CPU-UP	CPU TLE UP
INSIDER.50	+02577	01/01/1997 0:00	01/01/2050 23:59	CPU-VULN	CPU TLE VULNERABLE
INSIDER.50	+02578	01/01/1997 0:00	01/01/2050 23:59	CPU-UP	CPU Disk I/O's UP
INSIDER.50	+02579	01/01/1997 0:00	01/01/2050 23:59	CPU-VULN	CPU Disk I/O's VULNERABLE
INSIDER.50	+02580	01/01/1997 0:00	01/01/2050 23:59	CPU-UP	CPU Cache Hits UP
INSIDER.50	+02581	01/01/1997 0:00	01/01/2050 23:59	CPU-VULN	CPU Cache Hits VULNERABLE
INSIDER.50	+02583	01/01/1997 0:00	01/01/2050 23:59	X25-UP	X.25 SU's In Use UP
INSIDER.50	+02584	01/01/1997 0:00	01/01/2050 23:59	X25-VULN	X.25 SU's In Use VULNERABLE



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
INSIDER.50	+02585	01/01/1997 0:00	01/01/2050 23:59	X25-UP	X.25 Line Quality OK UP
INSIDER.50	+02586	01/01/1997 0:00	01/01/2050 23:59	X25-VULN	X.25 Line Quality OK VULNERABLE
INSIDER.50	+02587	01/01/1997 0:00	01/01/2050 23:59	X25-UP	X.25 Modem Error UP
INSIDER.50	+02588	01/01/1997 0:00	01/01/2050 23:59	X25-VULN	X.25 Modem Error VULNERABLE
INSIDER.50	+02590	01/01/1997 0:00	01/01/2050 23:59	X25-UP	X.25 Frame RNR Sent UP
INSIDER.50	+02591	01/01/1997 0:00	01/01/2050 23:59	X25-VULN	X.25 Frame RNR Sent VULNERABLE
INSIDER.50	+02592	01/01/1997 0:00	01/01/2050 23:59	X25-UP	X.25 Frame REJ Sent UP
INSIDER.50	+02593	01/01/1997 0:00	01/01/2050 23:59	X25-VULN	X.25 Frame REJ Sent VULNERABLE
INSIDER.50	+02594	01/01/1997 0:00	01/01/2050 23:59	X25-UP	X.25 Frame RNR Received UP



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
INSIDER.50	+02595	01/01/1997 0:00	01/01/2050 23:59	X25-VULN	X.25 Frame RNR Received VULNERABLE
INSIDER.50	+02596	01/01/1997 0:00	01/01/2050 23:59	X25-UP	X.25 Frame REJ Received UP
INSIDER.50	+02597	01/01/1997 0:00	01/01/2050 23:59	X25-VULN	X.25 Frame REJ Received VULNERABLE
INSIDER.50	+02598	01/01/1997 00:00	01/01/2050 23:59	X25-UP	X.25 Packet RNR Sent UP.
INSIDER.50	+02599	01/01/1997 00:00	01/01/2050 23:59	X25-VULN	X.25 Packet RNR Sent VULNERABLE.
INSIDER.50	+02602	20/03/1996 00:00	20/03/2020 23:59	CONSOLE-ALERT-CRITIC	<p>It is possible to have Reflex spot any CRITICAL token EMS events that have not been configured in the reaction database for graphical reporting.</p> <p>With this event, any critical event can be sent to an icon in Status Monitor to flash an icon red thereby indicating to an operator that a critical event may need to be included in the general Reflex configuration.</p>
INSIDER.50	+02603	20/03/1996 00:00	20/03/2020 23:59	CONSOLE-ALERT-VULN	As above but for ACTION NEEDED events.
INSIDER.50	+05060	20/03/1996 00:00	20/03/2020 23:59	SPOOLER-OBJECT-UP	Spooler supervisor active message.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
INSIDER.50	+05061 - +05064	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT- DOWN	In order: Spooler Drain Spooler is Warm Starting Spooler is Cold Starting Spooler has a PROC ERROR
INSIDER.50	+05066	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT- DOWN	Reflex 80:20 configured spooler not found. A spooler is present in a Status Monitor object tree but is not present in the SPOOLCOM configuration.
INSIDER.50	+05070	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT-UP	Spooler Collector active.
INSIDER.50	+05071	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT- VULN	Spooler Collector is over threshold.
INSIDER.50	+05072 - +05073	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT- DOWN	In order: Collector is full Collector is draining
INSIDER.50	+05074	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT-UP	Collector is dormant.
INSIDER.50	+05075	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT- DOWN	Collector has a PROC ERROR.
INSIDER.50	+05077	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT- DOWN	Reflex 80:20 configured collector not found. A collector is present in a Status Monitor object tree but is not present in the SPOOLCOM configuration.
INSIDER.50	+05080 - +05081	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT-UP	In order: Print process is active Print process is dormant
INSIDER.50	+05082	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT- DOWN	Print process has a PROC ERROR.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
INSIDER.50	+05084	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT- DOWN	Reflex 80:20 configured print process not found. A print process is present in a Status Monitor object tree but is not present in the SPOOLCOM configuration.
INSIDER.50	+05090 - +05091	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT-UP	In Order: Device is waiting Device is busy
INSIDER.50	+05092	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT- DOWN	Device is OFFLINE.
INSIDER.50	+05093	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT-UP	Device is printing.
INSIDER.50	+05095 - +05096	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT- DOWN	In Order: Device has a DEVICE ERROR Device has a PROC ERROR
INSIDER.50	+05098	20/03/1996 00:00	20/03/2020 23:59	SPOOLER- OBJECT- DOWN	Reflex 80:20 configured device not found. A device is present in a Status Monitor object tree but is not present in the SPOOLCOM configuration.
INSIDER.50	+05110	20/03/1996 00:00	20/03/2020 23:59	FILE-AGENT- UP	This action group is no longer required as at release 4.0 of Reflex 80:20.
INSIDER.50	+05111 - +05112	20/03/1996 00:00	20/03/2020 23:59	FILE-AGENT- DOWN	As above.
INSIDER.50	+05246	20/03/1996 0:00	20/03/2020 23:59	X25-SU- DOWN	X.25 Subnet DOWN event



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
INSIDER.50	+05247	20/03/1996 0:00	20/03/2020 23:59	X25-SU-UP	X.25 Subnet UP event
INSIDER.50	+05248	01/01/1997 00:00	01/01/2050 23:59	DISK-CACHE-UP	Disk Cache Read Hits 512 UP.
INSIDER.50	+05249	01/01/1997 00:00	01/01/2050 23:59	DISK-CACHE-VULN	Disk Cache Read Hits 512 VULN.
INSIDER.50	+05280 - +05299	20/03/1996 0:00	20/03/2020 23:59	TCPIP-LISTNER-UP	TCP/IP Listner UP events
INSIDER.50	+05300 - +05319	20/03/1996 0:00	20/03/2020 23:59	TCPIP-LISTNER-DOWN	TCP/IP Listner DOWN events
INSIDER.50	+05350 - +05359	20/03/1996 0:00	20/03/2020 23:59	TCPIP-ROUTE-UP	TCP/IP Route UP events
INSIDER.50	+05360 - +05369	20/03/1996 0:00	20/03/2020 23:59	TCPIP-ROUTE-DOWN	TCP/IP Route DOWN events
INSIDER.50	+05370 - +05389	20/03/1996 0:00	20/03/2020 23:59	TCPIP-SUB-NET-UP	TCP/IP Subnet UP events
INSIDER.50	+05390 - +05409	20/03/1996 0:00	20/03/2020 23:59	TCPIP-SUB-NET-DOWN	TCP/IP Subnet DOWN events



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
INSIDER.50	+05410 - +05469	20/03/1996 0:00	20/03/2020 23:59	TCPIP-PROC- ESS- UP	TCP/IP Process UP events
INSIDER.50	+05470 - +05529	20/03/1996 0:00	20/03/2020 23:59	TCPIP-PROC- ESS- DOWN	TCP/IP Process DOWN events
INSIDER.50	+05530 - +05539	01/01/1997 0:00	01/01/2050 23:59	TCPIP-TEL- SERV-UP	TCP/IP Telserv UP events
INSIDER.50	+05540 - +05549	01/01/1997 0:00	01/01/2050 23:59	TCPIP-TEL- SERV-DOWN	TCP/IP Telserv DOWN events
INSIDER.50	+05550 - +05599	20/03/1996 0:00	20/03/2020 23:59	DASHBOARD- SYSTEM- METS7	Threshold events for CPU UP states, including % Free Memory Pages
INSIDER.50	+05600 - +05649	20/03/1996 0:00	20/03/2020 23:59	DASHBOARD- SYSTEM- METS7	Threshold events for CPU VULN states, including % Free Memory Pages
INSIDER.50	+05650	29/09/2000 0:00	29/09/2030 23:59	HEAP-USE- INCREASING- DOWN	Heap use has continued increasing for a specific process and a down state has been reached.
INSIDER.50	+05651	29/09/2000 0:00	29/09/2030 23:59	HEAP-USE- INCREASING- VULN	Heap use has increased for a specific process and a vulnerable state has been reached.
INSIDER.50	+05652	29/09/2000 0:00	29/09/2030 23:59	HEAP-USE- INCREASING- UP	Heap use has either decreased or remained the same for a specific process and an up state has been reached.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
INSIDER.50	+05660	29/09/2000 0:00	29/09/2030 23:59	PFS-USE-IN-CREASING-DN	PFS use has continued increasing for a specific process and a down state has been reached.
INSIDER.50	+05661	29/09/2000 0:00	29/09/2030 23:59	PFS-USE-INCREASING-VULN	PFS use has increased for a specific process and a vulnerable state has been reached.
INSIDER.50	+05662	29/09/2000 0:00	29/09/2030 23:59	PFS-USE-IN-CREASING-UP	PFS use has either decreased or remained the same for a specific process and an up state has been reached.
INSIDER.50	+06000	20/03/1996 00:00	20/03/2020 23:59	PWYMON-UP	Pathway Monitor UP event
INSIDER.50	+06001	20/03/1996 00:00	20/03/2020 23:59	PWYMON-VU	Pathway Monitor VULNERABLE event
INSIDER.50	+06002	20/03/1996 00:00	20/03/2020 23:59	PWYMON-DOWN	Pathway Monitor DOWN event



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
MULTIBAT.1	+00003 - +00006	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-UP	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00010	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00011 - +00012	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-DOWN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
MULTIBAT.1	+000015	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-UP	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+000017 - +000018	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-DOWN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+000020	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+000021	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
MULTIBAT.1	+000022	01/01/1997 0:00	01/01/2050 23:59	MULTI-BAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+000023	01/01/1997 0:00	01/01/2050 23:59	MULTI-BAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
MULTIBAT.1	+000024	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-UP	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00026 - +00028	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-DOWN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor. This Action Group also has 'Exclude Events From' set for +00027.
MULTIBAT.1	+00031 - +00032	01/01/1997 0:00	01/01/2050 23:59	MBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
MULTIBAT.1	+00035 - +00037	01/01/1997 0:00	01/01/2050 23:59	MBAT.VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00038 - +00039	01/01/1997 0:00	01/01/2050 23:59	MBAT-DOWN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00040 - +00043	01/01/1997 0:00	01/01/2050 23:59	MBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Auto-discovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor. This Action Group also has 'Exclude Events From' set for +00041.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
MULTIBAT.1	+00041	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-DOWN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor
MULTIBAT.1	+00044	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-UP	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor
MULTIBAT.1	+00045	01/01/1997 0:00	01/01/2050 23:59	MBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
MULTIBAT.1	+00046	01/01/1997 0:00	01/01/2050 23:59	MBAT-DOWN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor
MULTIBAT.1	+00050 - +00052	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-DOWN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor
MULTIBAT.1	+00054	01/01/1997 0:00	01/01/2050 23:59	MBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
MULTIBAT.1	+00055	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00056	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-DOWN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00058 - +00059	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-DOWN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
MULTIBAT.1	+00060	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00061 - +00062	01/01/1997 0:00	01/01/2050 23:59	MBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00063	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00066 - +00067	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
MULTIBAT.1	+00066 - +00067	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-UP	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00072	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-DOWN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00079 - +00080	01/01/1997 0:00	01/01/2050 23:59	MBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00081	01/01/1997 0:00	01/01/2050 23:59	MBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
MULTIBAT.1	+00083 - +00085	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00086	01/01/1997 0:00	01/01/2050 23:59	MBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00087	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-DOWN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
MULTIBAT.1	+00089	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00090	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00092 - +00093	01/01/1997 0:00	01/01/2050 23:59	MBAT-VULN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
MULTIBAT.1	+00095	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-DOWN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.
MULTIBAT.1	+00900 - +00999	01/01/1997 0:00	01/01/2050 23:59	MULTIBAT-DOWN	MultiBatch events issued for a variety of conditions, e.g. Job started, Abended, Complete, etc. NB. These events are mapped to either MultiBatch steps 'Autodiscovered' within Status Monitor, using Manager & Subject tokens, or to 'format string' Status Monitor objects, e.g. MULTIBAT-VULN, MULTIBAT-DOWN. See the "Status Monitor" reaction within each Action Group to check how the event 'maps' onto Status Monitor.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
TANDEM.4	+00291	01/01/1995 0:00	20/03/2020 23:59	TAPE-DOWN	HPE NonStop Tape Drive Down
TANDEM.4	+00406	01/01/1995 0:00	20/03/2020 23:59	TAPECHANGE	HPE NonStop tape change event.
TANDEM.8	+01043	20/03/1996 0:00	20/03/2020 23:59	PATHWAY-OBJ-STARTED	Pathway server has been started within an application Pathway. Note that Pathway events are only written to the EMS log if activated.
TANDEM.8	+01047	20/03/1996 0:00	20/03/2020 23:59	PATHWAY-OBJ-TCPTERM	Pathway TCP Terminal aborted.
TANDEM.8	+01064 - +01065	20/03/1996 0:00	20/03/2020 23:59	PATHWAY-FREEZE-THAW	Freeze and Thaw operations on servers being carried out.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
TANDEM.4	+00406	01/01/1995 0:00	20/03/2020 23:59	TAPECHANGE	HPE NonStop tape change event.
TANDEM.8	+01043	20/03/1996 0:00	20/03/2020 23:59	PATHWAY-OBJ-STARTED	Pathway server has been started within an application Pathway. Note that Pathway events are only written to the EMS log if activated.
TANDEM.8	+01047	20/03/1996 0:00	20/03/2020 23:59	PATHWAY-OBJ-TCPTERM	Pathway TCP Terminal aborted.
TANDEM.8	+01064 - +01065	20/03/1996 0:00	20/03/2020 23:59	PATHWAY-FREEZE-THAW	Freeze and Thaw operations on servers being carried out.
TANDEM.10	+00074 - +00076	01/01/1994 0:00	01/12/2020 23:59	TMF-DOWN-EVENT	TMP: audittrail issues, TMF shutdown event
TANDEM.10	+00077 - +00078	01/01/1994 0:00	01/12/2020 23:59	TMF-VULNERABLE-EVENT	TMP: audit flush, begin transaction failed
TANDEM.10	+00079	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-TMF-EVENTS	TMP: audit error
TANDEM.10	+00080 - +00086	01/01/1994 0:00	01/12/2020 23:59	TMF-VULNERABLE-EVENT	TMP: audit trail issues
TANDEM.10	+00089 - +00090	01/01/1994 0:00	01/12/2020 23:59	TMF-DOWN-EVENT	TMP: audit trail, audit disk issues
TANDEM.10	+00093	01/01/1994 0:00	01/12/2020 23:59	TMF-VULNERABLE-EVENT	TMP: file transition error
TANDEM.10	+00104	01/01/1994 0:00	01/12/2020 23:59	TMF-VULNERABLE-EVENT	TMP: audit trail vol - invalid file
TANDEM.10	+00109	01/01/1994 0:00	01/12/2020 23:59	TMF-VULNERABLE-EVENT	TMP: audittrail cannot roll



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
TANDEM.10	+00111	01/01/1994 0:00	01/12/2020 23:59	TMF- DOWN-EVENT	TMP: stopped before rollover
TANDEM.10	+00114 - +00117	01/01/1994 0:00	01/12/2020 23:59	TMF- VULNERABLE- EVENT	TMP: audittrail volumes, files issues
TANDEM.10	+00118	01/01/1994 0:00	01/12/2020 23:59	TMF- DOWN-EVENT	TMP: audittrail is format2
TANDEM.10	+00122 - +00123	01/01/1994 0:00	01/12/2020 23:59	CRITICAL- TMF-EVENTS	TMP: TMF is stopping, stopped
TANDEM.10	+00124 - +00125	01/01/1994 0:00	01/12/2020 23:59	TMF- DOWN-EVENT	TMP: file system errors
TANDEM.10	+00128	01/01/1994 0:00	01/12/2020 23:59	TMF- DATAVOL- DOWN	TMP: disable datavol issued
TANDEM.10	+00131	01/01/1994 0:00	01/12/2020 23:59	TMF- DATAVOLS- STARTED	TMP: datavol started
TANDEM.10	+00134	01/01/1994 0:00	01/12/2020 23:59	TMF- DATAVOL- DIS-CLEAN	TMP: datavol disabled
TANDEM.10	+00135	01/01/1994 0:00	01/12/2020 23:59	TMF- DATAVOL- ENABLED	TMP: datavol enabled
TANDEM.10	+00136	01/01/1994 0:00	01/12/2020 23:59	TMF- DATAVOL- DELETED	TMP: datavol deleted
TANDEM.10	+00137 - +00146	01/01/1994 0:00	01/12/2020 23:59	TMF- DOWN-EVENT	TMP: various TMF configuration, volume, backup issues
TANDEM.10	+00147	01/01/1994 0:00	01/12/2020 23:59	TMF- VULNERABLE- EVENT	TMP: backup TMP taking over



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
TANDEM.10	+00150	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-TMF- EVENTS	TMP: file system error, when accessing TMF config file
TANDEM.10	+00151	01/01/1994 0:00	01/12/2020 23:59	TMF- VULNERABLE- EVENT	TMP: wrong version in TMF config file
TANDEM.10	+00152	01/01/1994 0:00	01/12/2020 23:59	TMF- DOWN-EVENT	TMP: extended seg allocation failed
TANDEM.10	+00157	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-TMF- EVENTS	TMP: file system error
TANDEM.10	+00159	01/01/1994 0:00	01/12/2020 23:59	TMF- VULNERABLE- EVENT	TMP: unexpected error from a DP
TANDEM.10	+00168 - +00178	01/01/1994 0:00	01/12/2020 23:59	TMF- VULNERABLE- EVENT	REC: Various recovery event messages
TANDEM.10	+00180 - +00184	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-TMF- EVENTS	MON: Various TMF failure messages
TANDEM.10	+00186	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-TMF- EVENTS	TMP: TMF cannot stop until RDF does
TANDEM.10	+00190 - +00194	01/01/1994 0:00	01/12/2020 23:59	TMF- VULNERABLE- EVENT	REC: Various file entry messages
TANDEM.10	+00197	01/01/1994 0:00	01/12/2020 23:59	TMF- VULNERABLE- EVENT	REC: File recovery event



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
TANDEM.10	+00202	01/01/1994 0:00	01/12/2020 23:59	TMF- DOWN-EVENT	DMP: Dump/ restore error
TANDEM.10	+00203	01/01/1994 0:00	01/12/2020 23:59	TMF- VULNERABLE- EVENT	DMP: Dump/ restore warning
TANDEM.10	+00204	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-TMF- EVENTS	DMP: fatal tape error
TANDEM.10	+00205	01/01/1994 0:00	01/12/2020 23:59	TMF- DOWN-EVENT	DMP: tape warning
TANDEM.10	+00206	01/01/1994 0:00	01/12/2020 23:59	TMF- VULNERABLE- EVENT	DMP: tape mount error
TANDEM.10	+00207	01/01/1994 0:00	01/12/2020 23:59	TMF- VULNERABLE- EVENT	DMP: tape mount warning
TANDEM.10	+00209	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-TMF- EVENTS	DMP: Dump/ restore other error
TANDEM.10	+00221	01/01/1994 0:00	01/12/2020 23:59	TMF- VULNERABLE- EVENT	DMP: Dump/ restore other warning
TANDEM.10	+00229	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-TMF- EVENTS	DMP: file not found in online dump



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
TANDEM.10	+00258	01/01/1994 0:00	01/12/2020 23:59	TMF- VULNERABLE- EVENTS	TMP: audit dumping disabled
TANDEM.10	+00263 - +00264	01/01/1994 0:00	01/12/2020 23:59	TMF- VULNERABLE- EVENTS	TMP: audit dump - not all copies made, audit dump failed
TANDEM.10	+00266	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-TMF- EVENTS	TMP: error on source file for audit overflow copy
TANDEM.10	+00267 - +00268	01/01/1994 0:00	01/12/2020 23:59	TMF- VULNERABLE- EVENTS	TMP: audit overflow copying failures
TANDEM.10	+00270 - +00274	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-TMF- EVENTS	TMP: audit dump, overflow issues
TANDEM.10	+00283	01/01/1994 0:00	01/12/2020 23:59	TMF-DOWN- EVENT	TMP: TMF Catalog process error
TANDEM.10	+00284	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-TMF- EVENTS	TMP: TMF Catalog deleted
TANDEM.10	+00288 - +00289	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-TMF- EVENTS	TMP: Transaction aborted events
TANDEM.10	+00401 - +00402	01/01/1997 0:00	01/12/2020 23:59	TMF- VULNERABLE- EVENTS	TMP: file rec, volume rec completed



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
TANDEM.12	+00007	01/01/1994 0:00	01/12/2020 23:59	ASYNCDOWN	Asynchronous line is down.
TANDEM.15	+00100	10/05/1995 0:00	10/05/2020 23:59	INSIDER-UP	CPU up event.
TANDEM.15	+00101	20/03/1996 0:00	20/03/2020 23:59	INSIDER-DOWN	CPU down event.
TANDEM.15	+00102	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-CPU-EVENT	CPU Power On
TANDEM.15	+00200	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-CPU-EVENT	CPU DIVER DOWN
TANDEM.15	+00312	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-CPU-EVENT	Uncorrectable Memory Error
TANDEM.15	+00326	01/01/1997 0:00	01/12/2050 23:59	CPU-MICROCODE-FAILURE	Millicode Halt
TANDEM.31	+05001 - +05002	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05005	09/03/1994 0:00	31/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05008	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05010	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05010	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05014	01/01/1994 0:00	01/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05015	09/03/1995 0:00	31/12/2020 23:59	DISK-DOWN	HPE NonStop disk down event.
TANDEM.31	+05018	09/03/1995 0:00	31/12/2020 23:59	DISK-UP	HPE NonStop disk up event.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
TANDEM.31	+05026	09/03/1995 0:00	31/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05028 - +05029	09/03/1995 0:00	31/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05032 - +05033	09/03/1995 0:00	31/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05040	09/03/1995 0:00	31/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05042	09/03/1995 0:00	31/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05044	09/03/1995 0:00	31/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05051	09/03/1995 0:00	31/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05052	09/03/1995 0:00	31/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05058	09/03/1995 0:00	31/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05071	09/03/1995 0:00	31/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05078	09/03/1995 0:00	31/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05082 - +05083	09/03/1995 0:00	31/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.
TANDEM.31	+05086 - +05087	09/03/1995 0:00	31/12/2020 23:59	CRITICAL-DISK-EVENTS	HPE NonStop disk down event.



Currently Delivered Reaction Event Ranges

Subsystem ID	Event Number Range	Cover Period From	Cover Period To	Action Group Name	Description
TANDEM.41	+00006	09/09/1994 0:00	31/12/2020 23:59	X25-RAISED	X25 line started.
TANDEM.41	+00007	09/09/1994 0:00	31/12/2020 23:59	X25-DOWN	X25 line down.
TANDEM.41	+00044	09/09/1994 0:00	31/12/2020 23:59	X25-LINE_READY	X25 network ready
TANDEM.41	+00045	09/09/1994 0:00	31/12/2020 23:59	X25-LINE_READY	X25 not network ready
TANDEM.41	+000116	09/09/1994 0:00	31/12/2020 23:59	X25-LINE_READY	X25 CLEAR Failure.
TANDEM.45	+00009	20/03/1996 0:00	20/03/2020 23:59	MHS-STATE-PLUS-NINE	X400 messaging component down.
TANDEM.45	- 00003	20/03/1996 0:00	20/03/2020 23:59	MHS-STATE-MINUS-THREE	X400 messaging component is up.



15. Reflex 80:20 Pathway Server Configuration

This section categorises the various servers that execute within the Reflex 80:20 PATHWAY in terms of their functional areas. The process names are given although the prefix of '\$RX' may have been changed to avoid clashes with your own environment.

Server Name	Process	Object	SQL	Pathway Params	GUI Administration Parameters (PARACONF)
ADMINISTRATION					
REFLEX-ADMIN	\$RXAD	SRVADMIN	No		Time-out, audit-flag, title, NB: validates all entered parameters.
REFLEX-AUDITLOG	\$RXAU	SRVALL	No		
STATUS MONITOR					
AGENT-DISK	\$RXDS	DISKAG	No		
AGENT-FILE	\$RXFI	FILEAG	No		
AGENT-MULBAT	\$RXMB	MULTBG92, MULTBG93	No		
AGENT-NETBATCH	\$RXNB	NBATCHAG	No		
AGENT-OSIMHS (OBSOLETE AS OF V4.8)	\$RXOS	OSIMHSAG	No		
AGENT-PATH	\$RXPA	PATHAG	No		
AGENT-PROC	\$RXAP	PROCAG	No		OPENINFO-PROCESS-AGENT-PREFIX
AGENT-SPL	\$RXSL	SPLAG	No		
AGENT-TANDEM-HW	\$RXHW	TANHWAG	No		
REFLEX-SMON	\$RXSM	SRVSMOQ	Yes	Interval	Num-trxs-perf-tmf, pathmon-process, subject-history-size, smon-grp-health, smon-grp-health-supp, select-remote-alert
CER-EXTRACT	\$RCER	SRVCER	NO		
PROC-MASTER	\$RPRO	SRVPROC	YES		procbaby-interval, procbaby-priority, procbaby-busy-freq, pathmon-process



Reflex 80:20 Pathway Server Configuration

Server Name	Process	Object	SQL	Pathway Params	GUI Administration Parameters (PARACONF)
STATUS MONITOR					
REFLEX-SMON-DB	\$RXSD	SRVS MDB	Yes		Action-group-down, action-group-up, audit-flag.
SMON-SETUP	\$RXSE	SRVSETUP	Yes		Audit-flag, num-trxs-per-tmf, pathmon-process.
SMON-PROCESSING	\$RXPM	SRVS MPQ	Yes	Interval	Num-trxs-per-tmf, pathmon-process, subject-history-size, smon-grp-health, smon-grp-health- supp, MultiBatch-investigate, select-remote-alert, tree-processing-queue.
STATUS-QUEUE	\$RXQU	SRVQUECO	Yes	Max-queue	Reflex-smon, pathmon-process.
SERVICE MONITOR					
DATA-ANALYSIS	\$RXDT	SRVDAACO	Yes		Pathmon-process, num-trxs-per-tmf, data-analysis-trace-flag.
DATA-DEF-SETUP	\$RXDF	SRVDDEFQ	Yes		Audit-flag.
DATA-FORWARDING	\$RXFW	SRVFWDCO	Yes	Errorinterval, Heart-interval	Pathmon-process.
RULES-ANALYSIS	\$RXRA	SRVRUACO	Yes		Pathmon-process, num-trxs-per-tmf.
RULES-BID-SETUP	\$RXRB	SRVSMRCO	Yes		Audit-flag.
SERVICE-DISPLAY	\$RXDP	SRVDISMQ	Yes		
SERVICE-SETUP	\$RXS1	SRVSEMSC	Yes		Pathmon-process, Audit-flag.



Reflex 80:20 Pathway Server Configuration

Server Name	Process	Object	SQL	Pathway Params	GUI Administration Parameters (PARACONF)
DASHBOARD					
DASH-MASTER	\$RXDB	SRVDASH	Yes		Cache-read-hits-thresh-operand, cpu-poll-interval, disk-poll-interval, cpu-busy-threshold, cpu-queue-threshold, disk-full-threshold, disk-frag-threshold, page-fault-threshold, dash-suspect-interval, process-busy-threshold, dash-thresh-suppress, cpu-dash-msg-freq, disk-dash-msg-freq, dash-suspect-suppress
DASH-THRESH	\$RXTH	SRVTHRS	No		
REFLEX-DISKIO	\$RXDI	SRVDSKIO	No		Diskio-max-disks, Diskio-msg-freq, Diskio-poll-interval
DISCOVERY					
REFLEX-STATS	\$RXAT	SRVSTAT	No		Stats-dict, stats-collector, stats-process, audit-flag
GATEWAY					
REFLEX-S-STATS	\$RXSS	SRVSPS	No		
REFLEX-STREAM	\$RXES	SRVESTRM	No		Audit-flag
CONSOLE					
CONSOLE	\$RXCO	SRVCONS	No		Console-alerts-flag
EVENT DATABASE					
REFLEX-EC-LIST	\$RXLS	SRVRAL	No		
REFLEX-EVENTCX	\$RXCX	SRVCX	No		Audit-flag
REFLEX-EVENTDB	\$RXEV	SRVEVDB	No		Audit-flag
REFLEX-EVENTTD	\$RXTD	SRVEVT	No		



Reflex 80:20 Pathway Server Configuration

Server Name	Process	Object	SQL	Pathway Params	GUI Administration Parameters (PARACONF)
ENTERPRISE MANAGEMENT					
ENT-MNGR-SETUP	\$RXPS	SRVENTMC	Yes		Audit-flag
ENT-MNGR-FEEDER	\$RXRD	EMGRFDCP	No	RA, RD, RG, RH, RI	Ent-mngr-feed-disarm
REMOT-BMC-REACT	\$RXCR	REMBGENC	Yes	Max-cmnd-sgs	Pathmon-process, select-remote-alert
REMOTE-DELIVERY	\$RXRD	REMOTECQ	Yes	Remote, Tivoli, tcpip	Pathmon-process
OPENVIEW-REACT	\$RXOV	OPVWGENC	Yes		Pathmon-process, select-remote-alert
TIVOLI-REACT	\$RXTV	TIVOGENC	Yes	Array-entries, heartbeat, interval	Pathmon-process, select-remote-alert
TASKMASTER					
REFLEX-TASKS	\$RXTA	SRVTASK	Yes		Audit-flag, task-q-len, Pathmon-process



Reflex 80:20 Pathway Server Configuration

Server Name	Process	Object	SQL	Pathway Params	GUI Administration Parameters (PARACONF)
MISCELLANEOUS					
AVAILAB-FEEDER (OBSOLETE AS OF V4.8)	\$RXAV	RFLXFDCO	No	RA through RI	Reflex-feeder-flag
CALENDAR-SETUP	\$RXCS	SRVCALEQ	Yes		Audit-flag, num-trxs-per-tmf
DASH-DATACOL	\$RXDA	SRVDACOL	Yes		
PAGEGEN-TAPS	\$RXTS	SRVTAPS	Yes		
REFLEX-CALMON	\$RXCA	CALMON	Yes		
REFLEX-EGEN	\$RXPI	SRVEGEN	No		
REFLEX-MEASURE	\$RXME	SRVMEAS	No		Allow-Measure, Measurement-Duration, Measure-Subvol
REFLEX-PING	\$RXPI	SRVPING	No		
REFLEX-WILDCARD	\$RXAL	SRVWILD	No		



Reflex 80:20 Pathway Server Configuration

Server Name	Process	Object	SQL	Pathway Params	GUI Administration Parameters (PARACONF)
HEARTBEAT					
FILE-METS-CRIT	\$FCRI1 - 5	FIMEMONQ	Yes	Servname, Max-Files, Info-Events, Type	Fime-poll-interval, fime-msg-frequency, fime-mets-suppress, pathmon-process, fime- max-standby-critical, fime-mets-delay
FILE-METS-DAILY	\$FDAI1 - 5	FIMEMONQ	Yes	Servname, Max-Files, Info-Events, Type	Fime-poll-interval, fime-msg-frequency, fime-mets-suppress, pathmon-process, fime- max-standby-daily, fime-mets-delay
FILE-METS-HALFD	\$FHDA1 - 5	FIMEMONQ	Yes	Servname, Max-Files, Info-Events, Type	Fime-poll-interval, fime-msg-frequency, fime-mets-suppress, pathmon-process, fime- max-standby-hdaily, fime-mets-delay
FILE-METS-HOUR	\$FHOU1 - 5	FIMEMONQ	Yes	Servname, Max-Files, Info-Events, Type	Fime-poll-interval, fime-msg-frequency, fime-mets-suppress, pathmon-process, fime- max-standby-hourly, fime-mets-delay
FILE-METS-SVOL	\$FSVL1	FIMEMONQ	Yes	Servname, Max-Files, Info-Events, Type	Fime-poll-interval, fime-msg-frequency, fime-mets-suppress, pathmon-process, fime-mets-delay
FILE-MON-SET-UP	\$RXFS	SRVFMNSQ	Yes		Audit-flag, action-group-down, action-group-up, action-group-vuln.
FILE-PRES-MONIT	\$RXFM	FIPRMONQ	Yes	Max-files, Info-events	Fipr-poll-interval, fipr-msg-frequency, fipr-mets-suppress, pathmon-process.
REFLEX-PROCMON	\$RXPR	SRVRPM	Yes		Action-group-down, action-group-up, audit-flag.



Reflex 80:20 Pathway Server Configuration

Server Name	Process	Object	SQL	Pathway Params	GUI Administration Parameters (PARACONF)
REACTION					
REFLEX-C-ACTION	\$RXAE	SRVRCU	Yes		Audit-flag
REFLEX-C-CMNDS	\$RXCM	SRVRCU	No		Runtask-location, audit-flag
REFLEX-C-EVENTS	\$RXMG	SRVRDE	No		Audit-flag
REFLEX-C-OPS	\$RXOP	SRVRCM	No		Audit-flag, remote-system-monit
REFLEX-C-PAGE	\$RXPG	SRVRRP	No		Audit-flag
REFLEX-C-WDOG	\$RXWD	SRVRWA	No		Audit-flag
REFLEX-P-CANCEL	\$RXCP	SRVAPL	No		
SNMP-DETAILS	\$RXS2	SRVSNMP	No		Audit-flag
SNMP-OUT	\$RXSN	SNMPT	No		



Reflex 80:20 Pathway Server Configuration

Server Name	Process	Object	SQL	Pathway Params	GUI Administration Parameters (PARACONF)
MEASURE MONITORING					
MEASURE-CPU	\$MCPU	MEASCPU	YES		MEASUREMENT-CPU-CATCHUP-RATE MEASUREMENT-CPU-DURATION MEASUREMENT-CPU-FILE-LIFE MEASUREMENT-CPU-HOUSEKEEP MEASUREMENT-CPU-INTERVAL MEASUREMENT-CPU-INTV-PER-RQST MEASUREMENT-CPU-IO-BUFFSIZE MEASUREMENT-CPU-READ-ALL
MEASURE-DSK	\$MDSK	MEASDSK	YES		MEASUREMENT-DISK-CATCHUP-RATE MEASUREMENT-DISK-DURATION MEASUREMENT-DISK-FILE-LIFE MEASUREMENT-DISK-HOUSEKEEP MEASUREMENT-DISK-INTERVAL MEASUREMENT-DISK-INTV-PER-RQST MEASUREMENT-DISK-IO-BUFFSIZE MEASUREMENT-DISK-READ-ALL
MEASURE-FILE	\$MFIL	MEASFIL	YES		MEASUREMENT-FILE-CATCHUP-RATE MEASUREMENT-FILE-DURATION MEASUREMENT-FILE-FILE-LIFE MEASUREMENT-FILE-HOUSEKEEP MEASUREMENT-FILE-INTERVAL MEASUREMENT-FILE-INTV-PER-RQST MEASUREMENT-FILE-IO-BUFFSIZE MEASUREMENT-FILE-READ-ALL
MEASURE-OSSCPU	\$MOCP	MEASOCP	YES		MEASUREMENT-OCPU-CATCHUP-RATE MEASUREMENT-OCPU-DURATION MEASUREMENT-OCPU-FILE-LIFE MEASUREMENT-OCPU-HOUSEKEEP MEASUREMENT-OCPU-INTERVAL MEASUREMENT-OCPU-INTV-PER-RQST MEASUREMENT-OCPU-IO-BUFFSIZE MEASUREMENT-OCPU-READ-ALL



Reflex 80:20 Pathway Server Configuration

Server Name	Process	Object	SQL	Pathway Params	GUI Administration Parameters (PARACONF)
MEASURE MONITORING					
MEASURE-OSNS	\$MOSN	MEASOSN	YES		MEASUREMENT-OSNS-CATCHUP-RATE MEASUREMENT-OSNS-DURATION MEASUREMENT-OSNS-FILE-LIFE MEASUREMENT-OSNS-HOUSEKEEP MEASUREMENT-OSNS-INTERVAL MEASUREMENT-OSNS-INTV-PER-RQST MEASUREMENT-OSNS-IO-BUFFSIZE MEASUREMENT-OSNS-READ-ALL
MEASURE-PROC	\$MPR	MEASPRC	YES		MEASUREMENT-PROC-CATCHUP-RATE MEASUREMENT-PROC-DURATION MEASUREMENT-PROC-FILE-LIFE MEASUREMENT-PROC-HOUSEKEEP MEASUREMENT-PROC-INTERVAL MEASUREMENT-PROC-INTV-PER-RQST MEASUREMENT-PROC-IO-BUFFSIZE MEASUREMENT-PROC-READ-ALL
MEASURE-SQLPROC	\$MSQP	MEASSQP	YES		MEASUREMENT-SQLP-CATCHUP-RATE MEASUREMENT-SQLP-DURATION MEASUREMENT-SQLP-FILE-LIFE MEASUREMENT-SQLP-HOUSEKEEP MEASUREMENT-SQLP-INTERVAL MEASUREMENT-SQLP-INTV-PER-RQST MEASUREMENT-SQLP-IO-BUFFSIZE MEASUREMENT-SQLP-READ-ALL
MEASURE-SQLSTMT	\$MSQS	MEASSQS	YES		MEASUREMENT-SQLS-CATCHUP-RATE MEASUREMENT-SQLS-DURATION MEASUREMENT-SQLS-FILE-LIFE MEASUREMENT-SQLS-HOUSEKEEP MEASUREMENT-SQLS-INTERVAL MEASUREMENT-SQLS-INTV-PER-RQST MEASUREMENT-SQLS-IO-BUFFSIZE MEASUREMENT-SQLS-READ-ALL



Reflex 80:20 Pathway Server Configuration

Server Name	Process	Object	SQL	Pathway Params	GUI Administration Parameters (PARACONF)
CONNECTIVITY					
FASTPIPE-BACKUP	\$RXFB	FASTPIPE	No	Location of FPINI	
FASTPIPE-SERVER	\$RXFP	FASTPIPE	No	Location of FPINI2	
SPOOLER MONITORING					
AGENT-SPOOLER	\$RXSG	SPOOLAG	Yes		Spooler-interval, spooler-threshold, spooler-frequency, spooler-suppress, spooler-report-empty-file.
X25 MONITORING					
DASH-X25	\$RXDX (used in Dashboard)	SRVDAX25	Yes		X25-poll-interval, X25-dash-msg-freq, X25-su-not-started-msg-freq, X25-su-not-started-suppress, X25-number-of-su-to-monitor.
AGENT-X25	\$RX25 (used in SMON)	X25AG	No		
X25-DATACOL	\$RXDC	X25DACOL	Yes		Pathmon-process
BASE24 XPNET MONITORING (STATUS MONITOR)					
ACI-XPNET-AGENT	\$RXXP	XPNETAGC	No	XB SERVER-NCP XC 1500 XD 0 XE 0 XF 0	Pathmon-process Note: Also reads RFLXDAT.XPNETCNF for BASE24 configuration values



Reflex 80:20 Pathway Server Configuration

Server Name	Process	Object	SQL	Pathway Params	GUI Administration Parameters (PARACONF)
MQ SERIES MONITORING					
AGENT-MQSC	\$RXMQ	MQAG	Yes		MQSC-CPU, MQSC-PRIORITY, MQSC-PROCESS, MQSC-LOCATION, MQVOLUME, MQDEFAULTPREFIX, MQNSKOPTPATH, MQNSKVARPATH
TCP/IP MONITORING					
DASH-TCPIP	\$RXTC	SRV DATCP	Yes		TCPIP-PROCESS-POLL-INTERVAL, TCPIP-ROUTE-POLL-INTERVAL, TCPIP-SUBNET-POLL-INTERVAL, TCPIP-NO-LISTNER-MSG-FREQ, TCPIP-NO-LISTNER-SUPPRESS, TCPIP-MSTATE-SUPPRESS, TCPIP-MSTATE-MSG-FREQ, OPENINFO-DASH-TCPIP-PREFIX, TCPIP-LISTNER-POLL-INTERVAL, TCPIP-TELSERV-POLL-INTERVAL, TCPIP-LISTNER-PROC-SUPPRESS, TCPIP-TELSERV-PROC-SUPPRESS, TCPIP-LISTNER-MSG-FREQ, TCPIP-TELSERV-MSG-FREQ
AGENT-TCPIP	\$RXAI	TCPIPAG	No		
PATHWAY MONITORING					
REFLEX-PWAY-MON	\$RXPW	PWYMON	No		PWYMON-INTERVAL, PATHMON-PROCESS



16. Reflex 80:20 Pathway Server Descriptions

This section categorises the various servers that execute within the Reflex 80:20 PATHWAY in terms of their functional areas as well as providing a description of each.

Server Name	Process	Description
ADMINISTRATION		
REFLEX-ADMIN	\$RXAD	Takes care of the logon dialog and session of the GUI client, the maintenance of the files and parameter records and the security classes and security profiles.
REFLEX-AUDITLOG	\$RXAU	Responsible for the browsing of the Reflex 80:20 audit log by terminal, timestamp, facility and Guardian user.
STATUSMONITOR		
ACI-XPNET-AGENT	\$RXXP	Responsible for retrieving information, status and statistics of a particular BASE24 XPNET object. It is called when Detailed Information of a XPNET object is requested from the Status Monitor screen.
AGENT-DISK	\$RXDS	Allows for the return of complete and comprehensive HPE NonStop Disk details to an "Info Request" command, performed via the Overdrive - Status Monitor screen.
AGENT-FILE	\$RXFI	Allows for the passing back of complete HPE NonStop file details to the info request of the Overdrive - Status Monitor screen. It will also accept a status request which will reply with either file present or not present.
AGENT-MULBAT	\$RXMB	Allows for the passing back of complete MultiBatch job details to the info request of the Overdrive - Status Monitor screen. It will also accept a status request which will reply with either job failed or OK.
AGENT-NETBAT	\$RXNB	Allows for passing back of complete NetBatch component details to the info request of the Overdrive - Status monitor screen. It will also accept a status request which will reply with the state of the relevant NetBatch component.
AGENT-OSIMHS (OBSOLETE AS OF V4.8)	\$RXOS	Allows for the passing back of complete messaging X400 details to the info request of the Overdrive - Status Monitor screen. It will also accept a status request which will reply with either messaging component in error or otherwise.
AGENT-PATH	\$RXPA	Allows for the passing back of complete Pathway component details to the info request of the Overdrive - Status Monitor screen. It will also accept a status request which will reply with either Pathway component (e.g. server) failed or otherwise.
CER-EXTRACT	\$RCER	Returns Cause, Effect, Recovery information for a selected EMS event.
PROC-MASTER	\$RPRO	A server which plugs directly into the Dashboard display of the GUI client to display process metrics for nominated processes. The server starts a baby process per CPU to pass back Process information locally to the master process.



Reflex 80:20 Pathway Server Descriptions

Server Name	Process	Description
STATUS MONITOR		
AGENT-PROC	\$RXAP	Allows for the passing back of complete HPE NonStop process details to the info request of the Overdrive - Status Monitor screen. It will also accept a status request which will reply with either process present or not present.
AGENT-SPL	\$RXSL	Allows for passing back of complete Spooler component details to the info request of the Overdrive - Status Monitor screen.
AGENT-TANDEM-HW	\$RXHW	Allows for the passing back of HPE NonStop hardware device details to the info request of the Overdrive - Status Monitor screen. It will also accept a status request which will reply with either hardware present or not present.
AGENT-X25	\$RX25	Responsible for retrieving information, status and statistics of a particular X25 Line or X25 Sub Unit. It is called when Detailed Information of a X25 object is requested from the Status Monitor screen.
REFLEX-SMON	\$RXSM	This is the Status Monitor server which hooks up to the live Overdrive – Status Monitor screen. This server and process should always be running and is key to displaying critical, vulnerable and acknowledged objects in the drill down object trees. The Event Monitor process passes status EMS events directly to it to provide graphical status information about HPE NonStop components to operators.
REFLEX-SMON-DB	\$RXSD	Responsible for the maintenance of the Network Hierarchy SQL table (NETWHIEQ) and the maintenance of Status Monitor reactions file (ACTWDOG) for graphical alerting purposes.
SMON-SETUP	\$RXSE	Server which sets up the various trees in Status Monitor as part of the dragging and dropping of HPE NonStop object components into drill down trees. It also handles requests for Status Monitor set-up warm-boot.
SMON-PROCESSING	\$RXPM	Responsible for handling the more time consuming processing previously handled by the REFLEX-SMON server-class, for example checking the status of a tree.
STATUS-QUEUE	\$RXQU	Used only in cases where the sheer volume of HPE NonStop objects (e.g. a large Pathway tree) causes slow response times in the live Status Monitor screens after warm-boot. This process handles status requests by passing indeterminate status (orange) back to Status Monitor and subsequently chasing the actual status of a HPE NonStop component that it will feed to Status Monitor in a NOWAITed mode.



Reflex 80:20 Pathway Server Descriptions

Server Name	Process	Description
MEASURE MONITORING		
MEASURE-CPU	\$MCPU	This server is responsible for obtaining CPU Measurement information for configured CPUs and making it available for registered clients.
MEASURE-DISK	\$MDSK	This server is responsible for obtaining DISK Measurement information for configured DISKS and making it available for registered clients.
MEASURE-FILE	\$MFIL	This server is responsible for obtaining FILE Open Measurement information for configured FILES and making it available for registered clients.
MEASURE-OSSCPU	\$MOCP	This server is responsible for obtaining OSS CPU Measurement information for configured CPUs and making it available for registered clients.
MEASURE-OSSNS	\$MOSN	This server is responsible for obtaining OSS Nameserver Measurement information for configured CPUs and making it available for registered clients.
MEASURE-PROC	\$MPR	This server is responsible for obtaining Process Measurement information for configured PROCESSES and making it available for registered clients.
MEASURE-SQLPROC	\$MSQP	This server is responsible for obtaining SQL Process Measurement information for configured PROCESSES and making it available for registered clients.
MEASURE-SQLSTMT	\$MSQS	This server is responsible for obtaining SQL Statements Measurement information for configured PROCESSES and making it available for registered clients.



Reflex 80:20 Pathway Server Descriptions

Server Name	Process	Description
SERVICE MONITOR		
DATA-ANALYSIS	\$RXDT	Server that breaks up incoming APIs from the forwarding processes into their component parts based on definitions provided to it in the data definition dialogs of the Reflex client. This server then writes these individual field values to the cache table (DATCACHQ) for analysis by the RULES-ANALYSIS server.
DATA-DEF-SETUP	\$RXDF	This server is provided to allow for the setting up of data definition APIs for any APIs that require to be fed through to Service Monitor for analysis. This circumvents the necessity to hard-code API structure definitions in the Reflex product so that third party applications can plug in easily to the Server Monitor infrastructure.
DATA-FORWARDING	\$RXFW	A DATA-FORWARDING server exists on all Reflex nodes in a Service Monitor network to allow for the passing of APIs up to the parent node for rules analysis. Reflex service monitoring takes place on the nominated parent node.
RULES-ANALYSIS	\$RXRA	This server will search for any rules set-up in service monitor, which have been tagged by the DATA-ANALYSIS server as requiring a scan for status. This will be based on the fact that 1 or more field attributes referenced within the rule have changed value.
RULES-BID-SETUP	\$RXRB	A server supplied to enable the setting up of rules for the Service Monitor module. Fields within incoming APIs can be grouped and compared to various values to establish whether agreed service level agreements are about to be or are being compromised.
SERVICE-DISPLAY	\$RXDP	This server receives status information about services from the RULES-ANALYSIS server and subsequently allows for status relating to these services to be displayed on the live service screen. This server plugs directly into the live Service Monitor display.
SERVICE-SETUP	\$RXS1	Server that sets up the various trees in Service Monitor as part of the dragging and dropping of HPE NonStop object components from various HPE NonStop nodes into drill down trees. It also handles requests for Service Monitor set-up warm-boot.



Reflex 80:20 Pathway Server Descriptions

Server Name	Process	Description
DASHBOARD		
DASH-MASTER	\$RXDB	A server that plugs directly into the Dashboard display of the GUI client for displaying system metric information at configured polling intervals. This metric information relates to disks, CPUs and processes. The server starts a baby process per CPU to pass back CPU information locally to the master process.
DASH-THRESH	\$RXTH	A process responsible for comparing retrieved system metric values against agreed threshold limits. If those thresholds have been exceeded then EMS events are generated which can then be configured to cause graphical alerting of processes, CPUs and disks in the live Status Monitor screen.
DASH-X25	\$RXDX	This server is responsible for retrieving X25 metrics for use in the Dashboard screens. It also handles some of the threshold alerts based on the X25 metrics.
REFLEX-DISKIO	\$RXDI	This serverclass performs monitoring of Disk I/O. It obtains the Disk I/O timing counts at regular intervals and checks if thresholds have been exceeded.
X25-DATACOL	\$RXDC	This process plugs into the DASH-X25 server for collecting data for the Service Monitor module. It polls DASH-X25 at the same rate as for the Dashboard GUI windows to collect this data; therefore, the parameters for specifying the polling intervals apply.
DISCOVERY		
REFLEX-STATS	\$RXAT	Server used for setting up EMS analysis requests over a period of time with specified filter and collector values. The server will initiate a distributor to peruse EMS log files and pass back EMS graphical bar-chart readouts of events generated over time, from most down to least reported.
GATEWAY		
REFLEX-S-STATS	\$RXSS	This server handles requests for streamer statistics based on text event throughput through the configured streamer process.
REFLEX-STREAM	\$RXES	Handles the configuration of streamer records from streamer process through to the set-up of the translation rules for incoming text events.



Reflex 80:20 Pathway Server Descriptions

Server Name	Process	Description
CONSOLE		
CONSOLE	\$RXCO	This is the event viewing console in Reflex 80:20 which extracts EMS events and the mandatory EMS tokens from an event for display. Up to 16 user views can be configured with various filters and collectors assigned. Searches and extended filters can be configured to allow for advanced analysis of the EMS event logs for problem events.
EVENT DATABASE		
REFLEX-EC-LIST	\$RXLS	Server to pass back a list of reaction records with their corresponding reaction settings for display in the Reaction module.
REFLEX-EVENTCX	\$RXCX	This server allows for the customising of the CAUSE and RECOVERY texts seen in the detail function of the Console display. This text is substituted for the pre-delivered texts of any third-party software in the Console display only.
REFLEX-EVENTDB	\$RXEV	Individual EMS event records can be added to the Reflex event database with this server which hooks up to the Database module of the Reflex 80:20 GUI client.
REFLEX-EVENTTD	\$RXTD	This server passes back any pre-supplied CAUSE and RECOVERY HPE NonStop event texts. It is not currently in use as at release 4.1 of Reflex 80:20.
ENTERPRISE MANAGEMENT		
ENT-MNGR-SETUP	\$RXPS	This server caters for the setting up of Enterprise Manager attribute (TIVOLI, COMMAND/POST, SENTRA, SMS or E-Mail) alerts to a remote Windows platform.
ENT-MNGR-FEEDER	\$RXEM	This process is key to relaying any Enterprise Manager alerts (TIVOLI, COMMAND/POST, SENTRA, SMS or E-Mail) to a nominated Windows platform. It uses Fastpipe TCP/IP socket protocol to achieve this. The Reflex Windows Server process will need to be installed on the Windows box in order for this relay to work correctly.
OPENVIEW-REACT	\$RXOV	This server will build any event messages that required to be passed to the HPE Openview Enterprise Manager from SQL tables ACTCMDPQ and CMDPCNFQ. This will be as a result of EMS events that have been nominated as requiring an Enterprise Manager Reaction to be initiated.
REMOTE-DELIVERY	\$RXRD	This server will relay an API directly to a nominated platform. It is not currently in use as at release 4.1.
REMOT-BMC-REACT	\$RXCR	This server will build any event messages that require to be passed to the COMMAND/POST Enterprise Manager from tables ACTCMDPQ and CMDPCNFQ. This will be as a result of EMS events that have been nominated as requiring an Enterprise Manager reaction to be initiated.
TIVOLI-REACT	\$RXTV	This server will build any event messages that require to be passed to the TIVOLI Enterprise Manager from tables ACTCMDPQ and CMDPCNFQ. This will be as a result of EMS events that have been nominated as requiring an Enterprise Manager reaction to be initiated.



Reflex 80:20 Pathway Server Descriptions

Server Name	Process	Description
TASKMASTER		
REFLEX-TASKS	\$RXTA	This server plugs directly into the GUI for setting up Reflex tasks and programs in the Taskmaster module.
MISC		
AVAILAB-FEEDER (SERVER IS OBSOLETE AS OF V4.8)	\$RXAV	This process is responsible for piping time-stamped system metric data to a nominated NT workstation (Note: this nomination is carried out at the server level as a start-up parameter). The data consists of CPU, disk, file and status monitor object status data. It requires for the appropriate Windows software to be installed to provide trending using graphing software and accompanying SQL queries.
CALENDAR-SETUP	\$RXCS	This server plugs into the administration module of Reflex 80:20 for setting up both calendar time windows and year records for stating statutory and bank holidays.
DASH-DATACOL	\$RXDA	This process plugs into DASH-MASTER server for collecting data for the Service Monitor module. It polls DASH-MASTER at the same rate as for the Dashboard GUI windows in the client to collect this data so the parameters for specifying polling intervals apply.
PAGEGEN-TAPS	\$RXTS	The modification of the TAP parameter details for BT text paging can be achieved with this server. It only allows amending of the configured TAP record.
REFLEX-CALMON	\$RXCA	This server process is the Reflex calendar process for informing of started and elapsed calendar time periods. Any process can start up and register with this process for subsequently receiving calendar information for registered calendar periods. This includes third party software using Insider Technologies supplied APIs.



Reflex 80:20 Pathway Server Descriptions

Server Name	Process	Description
MISC		
REFLEX-EGEN	\$RXEG	This server allows for reactions to be tested by writing an EMS event into the GUI dialog and raising it to the event log by clicking on the client toolbar. It is useful when severe events cannot be created for testing purposes, e.g. CPU down, X25 line down.
REFLEX-MEASURE	\$RXME	This server-class is used to run a Measure on demand against a specified process or File Open(s) to provide additional diagnostic information.
REFLEX-PING	\$RXPI	For more information on this server, see appendices in this quick-start manual. It acts to monitor for workstations that have been locked up due to spurious window problems. Locked out workstations can then be reported the graphical displays of working workstations.
REFLEX-WILDCARD	\$RXAL	This serverclass enables the use of wildcards for searching on event reactions. It is a legacy server only invoked by the green-screen Pathway version of Reflex where scroll bars were not available. The green-screen version is no longer supported.
HEARTBEAT		
FILE-METS-CRIT	\$FCRI1 - 5	This server-class consists of 1 controlling process and up to 4 additional standby processes that perform file monitoring for the critical polling period
FILE-METS-DAILY	\$FDAI1 - 5	This server-class consists of 1 controlling process and up to 4 additional standby processes that perform file monitoring for the daily polling period
FILE-METS-HALFD	\$FHDA1 - 5	This server-class consists of 1 controlling process and up to 4 additional standby processes that perform file monitoring for the half daily polling period.
FILE-METS-HOUR	\$FHOU1 - 5	This server-class consists of 1 controlling process and up to 4 additional standby processes that perform file monitoring for the hourly polling period.
FILE-METS-SVOL	\$FSVL1	This server-class consists of 1 process that performs file monitoring for the daily subvolume monitoring.
FILE-MON-SET-UP	\$RXFS	This server-class enables the set-up of files to be monitored on the HPE NonStop platform at 5 configurable intervals (the fifth is for sub-volume monitoring). The intervals are critical (user configurable), hourly, half-daily and daily.
FILE-PRES-MONIT	\$RXFM	This process monitors files for their arrival at a given calendar period. In order to do this, it registers itself with the REFLEX-CALMON process to receive information about started calendar periods.
REFLEX-PROCMON	\$RXPR	This server allows for the set-up of process records in the heartbeat module of Reflex 80:20. These processes will then be monitored for their existence by the process monitor process \$PMON at the configured time window.



Reflex 80:20 Pathway Server Descriptions

Server Name	Process	Description
REACTION		
REFLEX-C-ACTION	\$RXAE	This server allows for the setting up of action groups and cover periods for events that should be reacted to by the Reflex 80:20 product.
REFLEX-C-CMND5	\$RXCM	This server allows for the entering of commands under the reaction module of Reflex 80:20. Tasks are now the preferred approach to kicking off both commands and a sequence of programs.
REFLEX-C-EVENTS	\$RXMG	This server allows for the set-up of an EMS event to be generated to the log as a result of an incoming EMS event.
REFLEX-C-OPS	\$RXOP	This server allows for the generation and compilation of an EMS HPE NonStop filter. It allows for the servicing of the request to warm boot the reaction module.
REFLEX-C-PAGE	\$RXPG	This server allows for the set-up of paging details under the reaction module by service number and a list of 10 contact pagers.
REFLEX-C-WDOG	\$RXWD	This server is well used in Reflex as it allows for the passing of EMS events from the event monitor (\$EMON) through to the Status Monitor module for graphical alerting of HPE NonStop health of configured hardware and software components.
REFLEX-P-CANCEL	\$RXCP	This server actions requests to cancel currently active pager requests. Note: these are not SMS page requests that are handled by off-line Windows Server but HPE NonStop port to modem page requests.
SNMP-DETAILS	\$RXS2	This server allows for the set-up of SSID to OID number part number for SNMP traps in Reflex 80:20. These are for outgoing SNMP traps.
SNMP-OUT	\$RXSN	This process handles SNMP trap messages which have been configured using a standard ITL message format for all Reflex SNMP traps.
CONNECTIVITY		
FASTPIPE-BACKUP	\$RXFB	This server is used only if the GUI is using a NonStop approach to TCP/IP connectivity to the Reflex 80:20 application. It acts to support connection if the primary TCP/IP stack fails. Up to 9 of these back-up servers can be configured to communicate with 9 other TCP/IP stacks.
FASTPIPE-SERVER	\$RXFP	This is the primary server to enable connectivity between the Reflex GUI client and the Reflex Pathway. It uses Insider Technologies propriety TCP/IP socket protocol - FASTPIPE.
SPOOLER MONITORING		
AGENT-SPOOLER	\$RXSG	This server allows for the monitoring of spooler entities, i.e. print processes, devices, collectors and supervisors. Events are generated to the EMS log which can be reported to the Status Monitor screen for graphical alerting.



Reflex 80:20 Pathway Server Descriptions

Server Name	Process	Description
MQ SERIES MONITORING		
AGENT-MQSC	\$RXMQ	This server is a purchasable module. It is responsible for retrieving information about MQ Series objects. It is called when Detailed Information of a MQ Series object is requested from the Status Monitor screen.
TCP/IP MONITORING		
DASH-TCPIP	\$RXTC	This server is responsible for retrieving TCP/IP metrics for use by the Dashboard Threshold server. This server also handles some threshold alerting itself.
AGENT-TCPIP	\$RXAI	This server is responsible for retrieving information, status and statistics about TCP/IP objects. It is called when Detailed Information of a TCP/IP object is requested from the Status Monitor screen.
PATHWAY MONITORING		
REFLEX-PWAY-MON	\$RXPW	This server provides monitoring of nominated pathway serverclasses at regular time intervals.



17. Reflex 80:20 Non Pathway Processes

This section categorises the various processes that execute outside the Reflex 80:20 PATHWAY. The process names are given although the names may have been changed to avoid clashes with your own environment.

Process	Object	SQL	External Params	GUI Administration Parameters (PARACONF)
\$EMON	EVNTMON	Yes	Server^queue, ent^mgr	emon-max-reconnect-time, emon-max-pathsend-retries, emon-retry-delay, emoncol0 <i>through</i> emoncol9, pathmon-process.
\$PMON	PROCMON	No	Max-processes	Pmon-poll-interval, pmon-msg-frequency, heartbeat-ems-suppress.
\$CGEN	CEGEN	No		
\$RTSK	TASKMAST			Task-q-len (RUNTASK).
\$PGEN	PAGEGEN	Yes	Call-retries, success-attempts, Backup_cpu, delay	



Reflex 80:20 Non Pathway Processes

Configuring Paging using RUNPGEN

The TACL macro RUNPGEN, located within the Reflex object subvolume is used to configure and start the Paging process.

This TACL macro can be amended to suite your individual needs.

The macro requires two site specific file locations to be specified for the DATACONF and OLCONF files. These locations are typically \$<your vol>.RFLXDAT.DATACONF and \$<your vol>.RFLXDAT.OLCONF.

The actual RUN command for the paging process can be found at the foot of the macro. The RUN command supports the following external parameters:

External Params	Function
BACKUP-CPU	Specifies the CPU in which the backup process will run. If the specified CPU is not available then a different CPU will be automatically chosen.
CALL-RETRIES	<p>This is used to determine the number of call attempts to make to each paging contact. The minimum value allowed is 0 and the maximum is 10. The default value is 3.</p> <p>A value of 0 signifies that only a single attempt to issue a page will be made to each paging contact; there will be no retries attempted.</p> <p>Note that this parameter does not apply to the fall back pager. If the fallback pager is being used then calls will be continually re-tried until a call is successful. Note that the fall back pager will be activated if no pager is configured to cover the time when the reaction event was raised or if errors occurred on the nominated pager resulting in unsuccessful calls and the re-try attempts being exceeded.</p>
DELAY	Delay is used to specify how long to pause (in seconds) between successful page calls. The default value is 300.
SUCCESS-ATTEMPTS	<p>This is used to determine the number of successful calls that will be made before the call is cancelled. The minimum value allowed is 0 and the maximum is 50. The default value is 0.</p> <p>A value of 0 signifies that the call will NEVER be cancelled and is only used for test purposes. If only a single successful call is required before the call is cancelled then a value of 1 should be used.</p> <p>(Note that success refers to a successful call to the bureau or paging service and not that the actual page has been delivered).</p>

Note: The TEST-MODE parameter is no longer supported. Using TEST-MODE will result in the paging process immediately stopping.

If the paging process needs to be started via RUNPGEN after a problem, then the evtmon process may need to be stopped first and then restarted after the paging process has started.

The RFLXCOM utility can be used to send commands to the paging process to alter its behaviour. For example, paging may be suspended. Please see the RFLXCOM section for details.



18. Reflex 80:20 Facilities and their Abbreviations

This section describes the purpose of each 3-letter abbreviation. Those that are **greyed** out are no longer used but are included for completeness. This section is useful when setting up Security Classes & Profiles for Reflex users. Using this table as a guide will enable the restriction of certain functional areas of Reflex while allowing access to others.

Note: From the following table, only the facilities with the Security Class Restriction set to Yes will be displayed in the Security Classes section of the GUI.

Abbrev	Description of use	Security Class Restriction	Checked By	Area of Reflex Product
ACF	Active Flag set utility	No	HPE NonStop	ACTFLAGS utility.
ACI	Used to licence both the Base24 XPNET status agent and the auto detection utility, XPNETAGC and XPNETADC respectively.	No	HPE NonStop	Base24 Monitoring.
ALL	Audit Screen.	No	GUI	Administration.
APL	The ability to cancel live page requests using GUI.	Yes	GUI	Reaction - Paging.
AVL	This function controls the successful start-up of the trending facility that sends CPU, DISK, SMON and File data to an NT box for graphing.	No	HPE NonStop	Insider Technologies supply an offline process for the populating of a relational database for graphing and trending the aforementioned components.
CEG	This function allows the command/ event generator process to start-up successfully.	No	HPE NonStop	This process will invoke a configured command or raise an EMS event.
CHU	The ability to add Calendar time periods.	Yes	GUI	Administration.
CML	List CPU Records – no longer used - legacy.	No		Overdrive.
CMU	Update CPU records - no longer used - legacy.	Yes		Overdrive Set-up.
CNU	This facility allows for the update of Console views - not validated.	Yes		Console.



Reflex 80:20 Facilities and their Abbreviations

Abbrev	Description of use	Security Class Restriction	Checked By	Area of Reflex Product
CON	This function is to allow for the use of the event viewing screen.	Yes	HPE NonStop & GUI	Console.
CPT	Reomte Alert set-up and alerting to NT, CP, SENTRA, Tivoli, SMS.	Yes	HPE NonStop & GUI	Reaction - Enterprise Management.
CXL	Listing customised event detail information.	No		Database.
CXM	Menu for customised event detail information - Pathway menu no longer used.	No		Database.
CXU	Update customised event detail information.	Yes	GUI	Database.
CYU	Update calendar year records.	Yes	GUI	Administration.
DAU	Update service monitor data definition records.	Yes	GUI	Service Monitor.
DBA	List Aliases for EMS Events - Pathway screen no longer used.	Yes		Database.
DBL	List Event Database Records.	No		Database.
DBM	A Pathway menu for the event database - Pathway screen no longer used.	No		Administration.
DBU	Event Database function for event add, delete and amend.	Yes	GUI	Database.



Reflex 80:20 Facilities and their Abbreviations

Abbrev.	Description of use	Security Class Restriction	Checked By	Area of Reflex Product
DCM	A Pathway menu for the files/parameters screens - Pathway screen no longer used.	No		Administration.
DDC	The function controls the successful start-up of the dashboard data collector.	No	HPE NonStop	This process passes metric data to service monitor and optionally, ITL's Windows trending software.
DEF	Pathway screen used to set event defaults - Pathway screen no longer used.	Yes		Administration.
DFL	List the file alias records in the administration module.	No	GUI	Administration.
DFU	Update the file alias records in the administration module.	Yes	GUI	Administration.
DIO	Disk I/O Time Monitoring	Yes	HPE NonStop	Disk I/O Time Monitoring
DPL	List the parameter records in the administration module.	No	GUI	Administration.
DPU	Update the parameter records in the administration module.	Yes	GUI	Administration.
EEX	Allows the EMS Extraction utility to run.	No	HPE NonStop	EMS Extra.
EMN	Allows the Event Monitor process to start-up successfully.	No	HPE NonStop	HPE NonStop platform process which acts as a junction point to all configured event reactions.
EVC	Display the customised event detail information for the EMS database.	Yes	GUI	Database.
EVD	Pathway menu screen for the database module - Pathway screen no longer used.	No		Database.



Reflex 80:20 Facilities and their Abbreviations

Abbrev.	Description of use	Security Class Restriction	Checked By	Area of Reflex Product
EVM	Display the context of an EMS message in terms of explanatory (expanded) text.	No	GUI	Discovery.
EVT	Display the event details for a HPE NonStop EMS event.	No	GUI	Database.
FMU	Configuring/Update File Monitoring entries in Heartbeat module.	Yes	HPE NonStop & GUI	Heartbeat.
LIC	Show the Reflex License details for a particular customer.	No	GUI	Miscellaneous.
HML	This is a Pathway screen to list hardware monitor records - Pathway screen no longer used.	No		Overdrive Set-up.
HMU	This is a Pathway screen to update hardware monitor records - Pathway screen no longer used.	Yes		Overdrive Set-up.
LOG	The main introduction screen in the Reflex Pathway - Pathway screen no longer used.	No		Miscellaneous.
MEN	Reflex 80:20 Pathway main menu screen - Pathway screen no longer used.	No		Miscellaneous.
MME	This function is for activating SMS alerting.	Yes	HPE NonStop	SMS Alerting.
MON	ActionView monitor function - not used.	No		Miscellaneous.
MQA	This facility allows the MQ Series Status Agent to run.	No	HPE NonStop	This process passes back status and metric information relating to WebSphere MQ Series objects.



Reflex 80:20 Facilities and their Abbreviations

Abbrev.	Description of use	Security Class Restriction	Checked By	Area of Reflex Product
NAC	Pathway green screen which displays all 3 letter facilities and their descriptions - Pathway screen no longer used.	No		Miscellaneous.
NHL	List the network hierarchy records for the HPE NonStop network.	No	GUI	Overdrive & Service Monitor.
NHU	This function allows for the update of the network hierarchy list.	Yes	GUI	Overdrive & Service Monitor.
PAD	This function controls the Pathway auto-detection facility.	No	HPE NonStop	This function builds Pathway object trees for the Status Monitor code.
PAG	This function allows for the successful start-up of the HPE NonStop port paging process.	No	HPE NonStop	This process allows for page requests to be raised via a configured HPE NonStop port.
PMO	This function code allows for the successful startup of the process monitor function.	No	HPE NonStop	This process checks at a configurable rate for HPE NonStop processes.
PSA	This function controls the successful use of the Pathway status agent.	No	HPE NonStop	This process passes back both status and metric information relating to servers and TDPs.
PSW	This is the security function that requires a user to logon with a Guardian ID.	No	GUI	Administration - LOGON.
PAL	This function allows for the list of reactions to be returned in the reaction module.	No	GUI	Reaction.
PWY	Pathway Monitoring	Yes	HPE NonStop	Pathway Monitoring



Reflex 80:20 Facilities and their Abbreviations

Abbrev.	Description of use	Security Class Restriction	Checked By	Area of Reflex Product
RAM	This is a Pathway menu screen under the Reaction module - Pathway screen no longer used.	No		Reaction
RAU	This function allows for the maintenance of Action Groups.	Yes	GUI	Reaction.
RCM	This option allows for the generating and compiling of filters and subsequent warm-boot of Reflex 80:20.	Yes	GUI	Reaction.
RCU	This function allows for the entering of command details under Action Groups.	Yes	GUI	Reaction - Command.
RDE	This function allows for the entering of event details under Action Groups.	Yes	GUI	Reaction - Event.
RED	This function controls the successful startup of the remote sending TCP/IP facility.	No	HPE NonStop	This process allows for the sending of a formatted message to a given remote platform.
REM	This is a Pathway menu controlling access to the various reaction functions - Pathway screen no longer used.	No		Reaction.
RES	This allows Status Monitor objects to be reset back to the up state.	Yes	HPE NonStop	Status Monitor.
RFA	This function allows for the freezing of reactions at object level.	Yes	GUI	Overdrive / Reaction.
RPD	This is a program definition menu - Pathway screen no longer used.	No		Tasks / Reaction.
RPM	This function allows for the setup of process monitor records.	Yes	GUI	Heartbeat - process existence.



Reflex 80:20 Facilities and their Abbreviations

Abbrev.	Description of use	Security Class Restriction	Checked By	Area of Reflex Product
RPL	This function allows for the listing of programs in the tasks function.	No	GUI	Taskmaster.
RPU	This function allows for the maintenance of programs in tasks.	Yes	GUI	Taskmaster.
RRP	This function allows for the entering of HPE NonStop port paging details under Action Groups.	Yes	GUI	Reaction - Paging.
RSM	This function allows for the setting up of SSID to OID translation rules for SNMP traps.	Yes	GUI	Administration - SNMP.
RTA	This function allows for the configuration of tasks with program records. Optionally can be set to enforce the entering of passwords for alternative startup user Ids.	Yes	GUI	Taskmaster.
RTI	Function to allow the passing back of task ownership list.	No	GUI	Taskmaster.
RTO	This function allows the adjoining of Guardian owners to tasks set up.	Yes	GUI	Taskmaster.
RTL	The function allows for the listing of Tasks.	No	GUI	Taskmaster.
RTM	This is a Pathway menu screen for the taskmaster module - Pathway screen no longer used.	No		Taskmaster.



Reflex 80:20 Facilities and their Abbreviations

Abbrev.	Description of use	Security Class Restriction	Checked By	Area of Reflex Product
RTU	This function allows for the resetting of failed Tasks in the Tasks module.	Yes	GUI	Reaction / Tasks.
RUB	This function allows for the building of rules under service trees on the parent node.	Yes	GUI	Service Monitor.
RWA	This function allows for the building of a Status Monitor reaction to an incoming event for graphical alerting.	Yes	GUI	Reaction / Overdrive.
SCL	This function allows the addition and modification of security classes.	Yes	GUI	Administration.
SEL	This function allows the listing of security classes for viewing.	No	GUI	Administration.
SEM	This function allows for the start-up of all Service Monitor processes on the parent node and some GUI control.	No	GUI	Service Monitor.
SEN	Sentra EventMon	No	HPE NonStop	HPE NonStop platform process that forwards event information to the Sentra product.
SMM	This is a Pathway Status Monitor menu - Pathway screen no longer used.	No		Overdrive Set-up.
SMN	This function allows access to the "Get Current Status" (traffic light button) and the "Acknowledge" facility (obtained separately within the 'Acknowledge or reset' Window).	No	GUI	Status Monitor



Reflex 80:20 Facilities and their Abbreviations

Abbrev.	Description of use	Security Class Restriction	Checked By	Area of Reflex Product
SMO	This function is used for Overdrive operational control - Pathway screen no longer used.	No		Live Overdrive.
SPD	This function allows for the addition of Streamer process details.	Yes	GUI	Gateway.
SPR	This function allows for the adjoining of security classes to security profiles.	Yes	GUI	Administration.
SPS	This facility allows for the display of streamer threshold information.	No	GUI	Gateway.
STA	This function allows for the display of the Discovery event statistics.	Yes	GUI	Discovery.
STI	This function allows for the addition of streamer configuration rule records in the translation tab.	Yes	GUI	Gateway.
STL	This function allows for the listing of configuration rules in the GUI.	No	GUI	Gateway.
STM	This is a Pathway screen for the various streamer functions - Pathway screen no longer used.	No		Gateway.



Reflex 80:20 Facilities and their Abbreviations

Abbrev.	Description of use	Security Class Restriction	Checked By	Area of Reflex Product
STR	This function allows for the successful start-up of any streamer processes.	No	HPE NonStop	This process allows for the conversion of basic text messages to unique tokenised EMS messages.
STU	This function allows for the update of streamer configuration rules in the translation tab.	Yes	GUI	Gateway.
TAD	This facility allows the TCP/IP Autodiscovery utility to run.	No	HPE NonStop	TCP/IP Autodiscovery utility.
TAP	This function allows for the update of streamer configuration rules in the translation tab.	No	GUI	HPE NonStop Port Paging.
TAS	This function allows for the successful start-up of the task master process.	No	HPE NonStop	This process can invoke tasks that have been set-up in Reflex.
TES	This function allows a user to raise a test event onto the EMS primary collector.	Yes	GUI	Reaction - Test.
TSL	This facility allows for the listing of both object types and subtypes.	No	GUI	Overdrive / Service Monitor / Reaction.
TSU	This facility allows for the listing of both object types and subtypes.	Yes	GUI	Overdrive / Service Monitor / Reaction.
TTL	This function allows the user to list tasks and their corresponding object types and subtypes.	No	GUI	Overdrive / Reaction.
TTU	This function allows the user to modify tasks and their corresponding object types and subtypes.	Yes	GUI	Overdrive / Reaction.
TXM	This is a Pathway menu function - Pathway screen no longer used.	No		Event Database.



Reflex 80:20 Facilities and their Abbreviations

Abbrev.	Description of use	Security Class Restriction	Checked By	Area of Reflex Product
WAR	This allows for a FULL warm-boot of the Status Monitor.	Yes	HPE NonStop	Status Monitor Setup & RFLXCOM
WIF	This function represents the overdrive interface and is no longer user.	No		Live Overdrive.
XAD	This facility allows the X25 Autodiscovery to run.	No	HPE NonStop	X25 Autodiscovery Utility
XCS	This function allows for the display of CPU metric statistics in Dashboard.	No	GUI	Dashboard.
XDS	This function allows for the display of disk metric statistics in Dashboard.	No	GUI	Dashboard.
XPD	This function allows for the display of the top 5 busy process metric statistics per CPU, in Dashboard.	No	GUI	Dashboard.



19. OMF Conversion Facilities

Introduction

This section documents the utilities that are available to Reflex 80:20 users to allow OMF template files to be converted into Reflex 80:20 database entries. The end product of the conversion will be a database that provides two forms of monitoring:

- Is a nominated process executing?
- Is a nominated file more than x% full.

Other monitoring options are available within Reflex 80:20. The conversion process will default these options and users can then use the Reflex 80:20 GUI to invoke them at a later date. The two conversion utilities are:

- ACTPINS – which converts process monitoring entries.
- FIMETINS – which converts file monitoring entries.

The two utilities can also be used by non-OMF users to spool large amounts of configuration information into the Reflex 80:20 database without having to set this up through the Reflex 80:20 screen.

The manual covers the installation, run time options and the changes that need to be made to the OMF configuration files before conversion.

ACTPINS

Introduction

The ACTPINS program reads records from an edit configuration file and inserts them into the ACTPROC Reflex 80:20 Enscribe database.

Optionally the ACTPINS program will make an entry in the OBJECTQ Reflex 80:20 SQL table for the nominated process. Users can utilise this table to build a Status Monitoring GUI.

Installation

This utility accesses SQL tables and therefore SQL compilation is required after the installation. Load the Reflex defines first via RUN RFLXOBJ.RSQLDEFS before executing the following command:

```
SQLCOMP/IN ACTPINS, OUT $$.#ACTP/CATALOG =REFLEX_CATALOG,EXPLAIN PLAN
```

Run time command

```
RUN ACTPINS / IN <edit-configuration-commands>, OUT <DATACONF>/ &  
<OBJECTQ-update-param>, <OBJECTQ-Initial-status>, <EMS-event-specification>
```

<edit-configuration-commands> - This edit file contains the names of the HPE NonStop processes that need to be added into the Reflex 80:20 Enscribe database table, ACTPROC.

<dataconf> - This file is the DATACONF file for the nominated Reflex 80:20 system. The file will contain the location of the ACTPROC database file.

<OBJECTQ-update-param> - This parameter determines whether an entry will be created in the Reflex 80:20 OBJECTQ SQL table. This will make the process names available to those Users who wish to build a graphical view of the processes in the Reflex 80:20 Status Monitor product. The value must be Y or N.

<OBJECTQ-Initial-status> - This parameter determines the initial status field of objects added to the OBJECTQ SQL table. Valid values are IN or UP. The default is "IN".

<EMS-event-specification> - This parameter provides details of the up and down events that must be generated when a process is detected as executing or not executing.

The format of the parameter is "SSID-Owner.Value.Version.Down-event.Up-event".
E.g. INSIDER.51.0.1001.1002.



Configuration Input File

The configuration file can have up to 4 fields separated by commas.

Only the first field, process name, is mandatory.

The structure of the file is:

<Process-name> , <start-time>, <end-time>, <description>

<Process-name> - the process name to be inserted in the ACTPROC database. The name should start with a "\$" and will not be prefixed with a node name. E.g. \$ZTC0.

<start-time> - This value is optional, the default is 00:00. The format is HH:MM for hours and minutes. This field signifies the time that monitoring is to commence.

<end-time> - This value is optional, the default is 23:59. The format is HH:MM for hours and minutes. This field signifies the time that monitoring is to end.

<description> - This value is optional, the default is that there is no description required.

Some examples:

```
$ZTC0, 00:00, 23:59, TCP/IP process
```

```
$SPLS , , , Spooler Supervisor
```

```
$BMON
```

OMF File Changes

A sample OMF file is shown at Section 4.

The OMF configuration file will not be in the required ACTPINS format and it will need to be edited before being processed by the ACTPINS program. Use the following instructions to achieve this:

1. Create an empty edit file.

```
EDIT <process-conversion-file>
```

2. Take a copy of the OMF template file and delete redundant data using the following repetitive edit commands:

```
*GET <OMF-file> TL
```

```
*DNB /PROCESS/A
```

```
*DNB /ADD /A
```

Note: This is ADD followed by a space character

```
*CAB/ADD PROCESS //A
```

```
*C 10:132/, 00:00, 23:59/A
```

3. Review the settings, changing any of the defaults to more appropriate settings.
4. Some OMF template files will have duplicate entries in by mistake. These can be removed using a sort. Skip this section if your file does not have duplicate entries.

Create an edit file SORTINP containing the following entries:

```
FROM <process-conversion-file>
```

```
TO <sort-output-file>
```

```
ASC 1:35
```

```
RUN, REMOVEDUPS
```



OMF Conversion Facilities

```
SORT/ IN SORTINP/
```

The output file will be entry sequenced, ACTPINS requires an edit file so convert back.

```
EDIT <process-conversion-file>2
```

```
*GET <sort-output-file> TL
```

The following warning message can be ignored:

```
INPUT RECORD LENGTH TRUNCATED TO 255 BYTES
```

ACTPINS execution

Review the PMON-MSG-FREQUENCY and PMON-POLL-INTERVAL parameter settings in the admin parameter database.

Select the event numbers that will be generated when missing processes are detected.

Execute the conversion facility. For example:

```
RUN ACTPINS/IN <process-conversion-file>, OUT DATACONF/Y, UP, INSIDER.1.0.2.3
```

If the conversion fails, then all changes will be backed out.





FIMETINS

Introduction

The FIMETINS program reads records from an edit configuration file and inserts them into the ACTFIMEQ Reflex 80:20 SQL table.

Optionally the FIMETINS program will make an entry in the OBJECTQ Reflex 80:20 SQL table for the nominated process. Users can utilise this table to build a Status Monitoring GUI.

Installation

This utility does access SQL tables and therefore SQL compilation is required after the installation.

Load the Reflex defines via RUN RFLXOBJ.RSQLDEFS before executing the following command:

```
SQLCOMP/IN FIMETINS,OUT $$.#FIME/CATALOG =REFLEX_CATALOG,EXPLAIN PLAN
```

Run time command

```
RUN FIMETINS / IN <edit-configuration-commands>/ <OBJECTQ-update-param>, &  
<EMS-event-specification>
```

<edit-configuration-commands> - This edit file contains the names of the HPE NonStop files that need to be added into the Reflex 80:20 SQL database table, ACTFIMEQ.

<OBJECTQ-update-param> - This parameter determines whether an entry will be created in the Reflex 80:20 OBJECTQ SQL table. This will make the file names available to those Users who wish to build a graphical view of the files in the Reflex Status Monitor product. The value must be Y or N.

<EMS-event-specification> - This parameter provides details of the up and down events that must be generated when a file is detected as greater than x% full.

"SSID-Owner.Value.Version.Down-event.Up-event.Vulnerable-event", e.g.:

```
INSIDER.51.0.1001.1002.1003.
```



Configuration Input File

The configuration file can have up to 3 fields separated by commas.

Only the first field - "file name" - is mandatory.

The structure of the file is: <File Name> , <percent-full>, <poll-period>

<File-name> - the file name to be inserted in the ACTFIMEQ database table. The name should not contain the node name and it should be in the format RFLXDAT.<filename>.

<percent-full> - The Reflex 80:20 monitoring software will emit an EMS event if the file in question exceeds this <percent-full> value. Valid values are 0 through 100. If no value is supplied then the default is 80.

<poll-period> - This value represents how often the file metrics for the nominated file are retrieved and analysed. The valid values are:

? D - Daily

? T - Every twelve hours, i.e. half-daily

? H - Hourly

? C - Critical

The default is H, hourly

Some examples:

```
$DEV.RFLXDAT.DATACONF, 95, H
```

```
$DEV.RFTSDAT.TEMPFILE
```

```
$DEV.TEMP.TEMPFILE, 70
```

```
$DEV.ZAPPL.TEMPFILE, , C
```



OMF Conversion Facilities

OMF File Changes

A sample OMF file is shown at Section 4.

The OMF configuration file will not be in the required FIMETINS format and it will need to be edited before being processed by the FIMETINS program. Use the following instructions to achieve this:

1. Create an empty edit file.
EDIT <file-conversion-file>
2. Take a copy of the OMF template file and delete redundant data using the following repetitive edit commands:

```
*GET <OMF-file> TL
```

```
*DNB /FILE/A
```

```
*DNB /ADD /A
```

Note: This is ADD and a space character

```
*LB/THRESHOLD/A
```

Make a note of any files that do not have the default threshold and then remove the

```
“,THRESHOLD x” clauses.
```

```
*CAB/ADD FILE //A
```

```
*C 40/, 80, C/A
```

Alter specific file thresholds by changing the 80 value back to the original threshold if required.

3. Review the settings, changing any of the defaults to more appropriate settings.
4. Some OMF template files will have duplicate entries in by mistake. These can be removed using a sort. Skip this section if your file does not have duplicate entries.

Create an edit file SORTINF containing the following entries:

```
FROM <file-conversion-file>
```

```
TO <sort-output-file>
```

```
ASC 1:35
```

```
RUN, REMOVEDUPS
```

```
SORT/ IN SORTINF/
```

The output file will be entry sequenced, FIMETINS requires an edit file so convert back.

```
EDIT <file-conversion-file>2
```

```
*GET <sort-output-file> TL
```

The following warning message can be ignored.

```
INPUT RECORD LENGTH TRUNCATED TO 255 BYTES
```

FIMETINS execution

Review the FIME-METS-SUPPRESS, FIME-MSG-FREQUENCY and FIME-POLL-INTERVAL parameter settings in the admin parameter database. Select the event numbers that will be generated when thresholded files are detected.

Execute the conversion facility. For example:

```
RUN FIMETINS / IN <file-conversion-file>/ Y, INSIDER.1.0.2.3.4
```

If the conversion fails, then all changes will be backed out.



Sample OMF Template File

```
SET CONFIRM ON
== Set values corresponding to OMF environment
SET NSSID $ZNS
SET NSSCONF $SYSTEM.SYSTEM.NSSCONF
SET SYSTEM \<node>
SET ALLOWERRORS ALL
SET ALLOWWARNINGS ALL
DELETE CPU *
DELETE PROCESS *
DELETE DISK *
DELETE FILE *
DELETE SPOOLSUPERVISOR *
DELETE SPOOLCOLLECTOR *
DELETE SPOOLPRINTPROCESS *
DELETE SPOOLDEVICE *
DELETE TMFTRANSACTION
DELETE TMFAUDITDUMP
DELETE TMFAUDITTRAIL
RESET CPU
    SET CPU SAMPLING-INTERVAL 1
    SET CPU UP-EVENT          N
    SET CPU UP-DISPLAY       N
    SET CPU ODD-EVENT        C
    SET CPU ODD-DISPLAY      N
    SET CPU DOWN-EVENT       C
    SET CPU DOWN-DISPLAY     Y
    SET CPU THRESHOLD        100
ADD CPU 00
ADD CPU 01
ADD CPU 02
```



OMF Conversion Facilities

RESET PROCESS

SET PROCESS SAMPLING-INTERVAL 1

SET PROCESS UP-EVENT N

SET PROCESS UP-DISPLAY N

SET PROCESS ODD-EVENT N

SET PROCESS ODD-DISPLAY N

SET PROCESS DOWN-EVENT C

SET PROCESS DOWN-DISPLAY Y

SET PROCESS MONITOR-PRIORITY N

SET PROCESS MONITOR-CPU N

ADD PROCESS \$A

ADD PROCESS \$B

ADD PROCESS \$C

ADD PROCESS \$D

RESET FILE

SET FILE SAMPLING-INTERVAL 5

SET FILE UP-EVENT N

SET FILE UP-DISPLAY N

SET FILE ODD-EVENT C

SET FILE ODD-DISPLAY N

SET FILE DOWN-EVENT C

SET FILE DOWN-DISPLAY N

SET FILE THRESHOLD 80

ADD FILE \$VOL.SVOL.FILEA

ADD FILE \$VOL.SVOL.FILEB

ADD FILE \$VOL.SVOL.FILEC



20. Configuring Multiple Console Servers

Pathway Configuration

To help reduce the load on an individual CPU, multiple Reflex 'Console' Pathway Serverclasses can be configured within different CPU's.

To configure multiple 'Console' Serverclasses, the Pathway Configuration file, PWCONF will need to be amended. This file will contain the default Console Serverclass called 'CONSOLE', which will always be present. You will also need to amend the STARTSRV file to include 'THAW' and 'START' commands for any new Console servers that you add. Both of these files can be found in the Reflex Object Subvolume (typically RFLXOBJ).

Using an appropriate editor, open up the PWCONF file and locate the 'CONSOLE' serverclass definition. Once located, copy the text starting at 'RESET SERVER' and finishing at 'FREEZE SERVER CONSOLE', as shown here.

```

RESET SERVER
SET SERVER HIGHPIN      ON
SET SERVER AUTORESTART  5
SET SERVER MAXSERVERS   1
SET SERVER MAXLINKS     100
SET SERVER TIMEOUT      10 MINS
SET SERVER NUMSTATIC    1
SET SERVER LINKDEPTH    5
SET SERVER TMF          ON
SET SERVER CPUS        1:0
SET SERVER PROGRAM      <OBJLOC>.SRVCONS
SET SERVER PROCESS    $<PREFIX>CO
SET SERVER IN           <DATALOC>.DATACONF
SET SERVER PRI          150
ADD     SERVER CONSOLE
FREEZE  SERVER CONSOLE

```

Then paste the text after the default 'CONSOLE' configuration. Now find the 'SET SERVER CPUS' section, and alter the Primary and Backup CPU values accordingly to spread the load across CPU's i.e. if the default 'CONSOLE' server is set as '1' for Primary and '0' for Backup, as shown above, then set the new entry to '0:1'.

Locate the 'SET SERVER PROCESS' section and amend this to '\$<PREFIX>C1'. It is recommended that for each new Console entry, you increment the process name i.e. if another entry is added, set it to '\$<PREFIX>C2' and so on.

You now need to set the name of the Serverclass by amending the following two lines. It is advisable to have the Serverclass name correspond with the Process name i.e. in this case, 'CONSOLE' should be amended to 'CONSOLE1' for '\$<PREFIX>C1'.

```

ADD SERVER CONSOLE      (Change to CONSOLE1)
FREEZE SERVER CONSOLE (Change to CONSOLE1)

```

Exit the editor, edit the 'STARTSRV' file and locate the reference to the default Console server. Insert the following text for each Console server added to the PWCONF file above, remembering to alter the Serverclass name to the appropriate name.

```

THAW SERVER CONSOLE1; START SERVER CONSOLE1

```

The Reflex pathway configuration is now set-up to run multiple Console server classes.



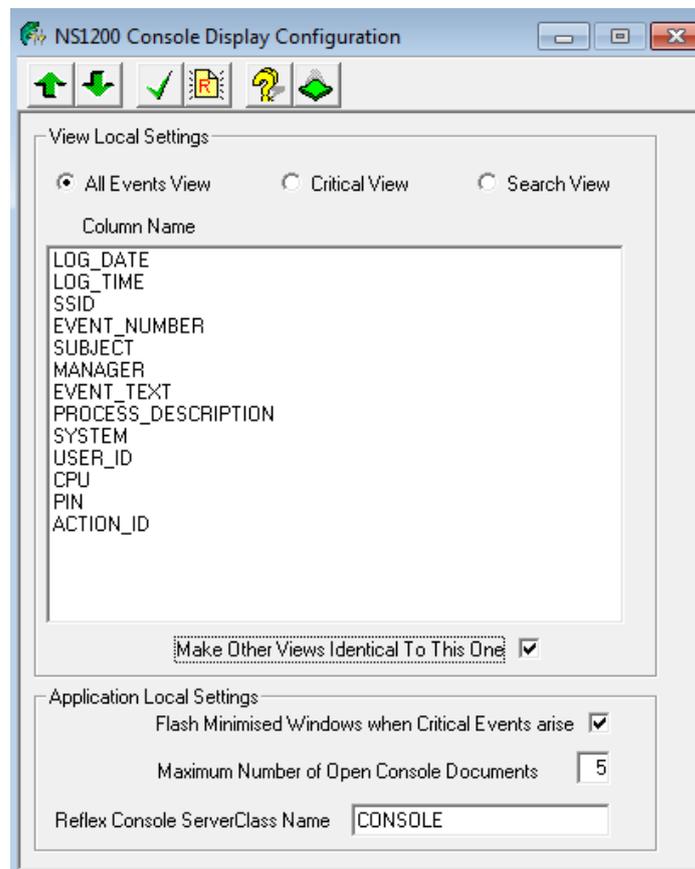
Configuring Multiple Console Servers

GUI Configuration

You now need to set-up the Reflex GUI Console to retrieve events from the appropriate Console server. Once Reflex has been started and you have logged on, select 'Console Display Configuration' from the GUI 'Configuration' drop-down menu.

When the 'Console Display Configuration' GUI is displayed (see *below*), you will see an entry at the bottom that allows the Console Serverclass name to be specified. This will be set to 'CONSOLE' by default when Reflex is installed. Change this to the Console Serverclass that you wish to use e.g. 'CONSOLE1' and click the amend icon to accept the update.

When the Console GUI is opened, it will retrieve its events from this server class.



Reflex Console Display Configuration



21. Database Integrity Program

RFLXINTG

The RFLXINTG program lets you verify the integrity of the Reflex database. The program checks, for example: any inconsistencies, event records which do not have actions assigned to them, security classes that are not used by any security profiles. You can select whether all the data files are checked, or selected files only. The program can be configured to automatically update files and records that are found to be inconsistent and a printed report can be produced.

RFLXINTG is run from the TACL prompt by navigating to the Reflex object subvolume and entering the following command:

```
RUN RFLXINTG / IN <data-subvolume>.DATACONF, OUT $$.#REPORT / params
```

where *params* are:

REPORT (produces a printed report without updating any files)

UPDATE ALL (updates all files and produces a printed report)

UPDATE ALL EXCEPT <**filename**> (updates all files except those specified by filename and produces a printed report)

UPDATE EVENTDB <**filename**> (updates only the file specified by filename and produces a printed report)

where **filename** is:

ACTCOMM, ACTEVE, ACTMESS, ACTPAGE, ACTWDOG, ALIASMAP, EVENTCX, EVETXT, PROGASS, PROGCONF, PROGPARG, SECCLASS, SECPROFL, TASKCONF, TASKOWNR, TASKPROG

The Reflex Database Integrity program checks the database in six phases as described below.

Phase 1

The event database, EVENTDB, is read. If the EVENTCX flag is set then the EVENTCX file is read to find the corresponding record. If the record does not exist, then the EVENTCX flag is reset in the event database.

The program then checks to see if any of the event flags are set (watchdog, radiopager, etc.). If any are found, the corresponding ACTEVE record is read. If this record is not found, then all the flags in the event record are reset. If the corresponding ACTEVE record is found, each flag is checked against its equivalent flag in the ACTEVE file and if any discrepancies are detected, an appropriate message is displayed and the conflicting flags are reset.

The program then checks to see if any aliases have been defined. If any are found, the ALIASMAP file is read and checked for a matching record. If a matching record is not found, then one is created and inserted into the ALIASMAP file.

Phase 2

This phase attempts to populate the event database using details found in the other database files. Records will be created if they do not already exist.

Phase 3

The program reads the Watchdog ACTWDOG, radiopager ACTPAGE, Event Command ACTCOMM and Event Message ACTMESS files and checks that for each record, a corresponding record exists in the ACTEVE file and that the appropriate flag is set. If a record is found in any of the ACT* files which does not have a corresponding ACTEVE record, it will be deleted. The ACTEVE file is again read and wherever a flag is set the program checks that a corresponding flag exists in the ACTPAGE, ACTWDOG, ACTCOMM and ACTMESS files. If no corresponding record is found then the appropriate flag is reset in the ACTEVE file and the event database.



Database Integrity Program

Phase 4

This phase reads the event database and checks if any event records exist in which all the event flags (watchdog, radiopager, etc.) are not set. If any such records are found, they are deleted from the event database.

Phase 5

This phase reads the security class file SECCLASS and checks that each security class is used by at least one entry in the security profile file SECPROFL. If not, the security class record is deleted. An additional check is made to see if the facility specified in the security class file is also specified in the facilities database FACILDB, if not, the security class record is deleted.

Phase 6

The TASKPROG file containing all the tasks and programs attached to those tasks is read. The program then reads the TASKCONF task configuration file to find a record with the same task name. If no match is found, the TASKPROG record is deleted. The file containing the program configurations PROGCONF is then checked for a matching program name. Again if no match is found, the TASKPROG record is deleted.

The TASKCONF file which contains all the task configuration records is now read and an attempt made to match each with a record in the TASKPROG task configuration file. Any task configuration record not matched is deleted.

The TASKOWNR file which lists all the task owner records is now read and an attempt made to match each with a task in the TASKCONF task configuration file. Any task owner record not matched is deleted.

Finally, EVETXT the event text file is read and records matched to those in the EVENTDB file. Records found without a corresponding match are deleted.

Shown below is a typical Reflex Database Integrity program printout.

This program will access the following files:

```
-----
| File Name                                     | access |
-----
| $S                                           | read write |
| $DATA02.SCOT DATACONF                     | read only |
| \INSIDER.$DATA02.SCOTT.EVENTDB             | read only |
| \INSIDER.$DATA02.SCOTT.EVENTCX             | read only |
| \INSIDER.$DATA02.SCOTT.ACTEVE              | read only |
| \INSIDER.$DATA02.SCOTT.ACTWDOG             | read only |
| \INSIDER.$DATA02.SCOTT.ACTPAGE             | read only |
| \INSIDER.$DATA02.SCOTT.ACTCOMM             | read only |
| \INSIDER.$DATA02.SCOTT.ACTMESS             | read only |
| \INSIDER.$DATA02.SCOTT.ALIASMAP            | read only |
| \INSIDER.$DATA02.SCOTT.FACILDB             | read only |
| \INSIDER.$DATA02.SCOTT.SECCLASS            | read only |
| \INSIDER.$DATA02.SCOTT.SECPROFL            | read only |
| \INSIDER.$DATA02.SCOTT.STRMCONF            | read only |
| \INSIDER.$DATA02.SCOTT.PROGCONF            | read only |
| \INSIDER.$DATA02.SCOTT.PROGPARG            | read only |
| \INSIDER.$DATA02.SCOTT.PROGASS             | read only |
| \INSIDER.$DATA02.SCOTT.TASKCONF            | read only |
| \INSIDER.$DATA02.SCOTT.TASKPROG            | read only |
| \INSIDER.$DATA02.SCOTT.TASKOWNR            | read only |
| \INSIDER.$DATA02.SCOTT.EVETXT              | read only |
-----
```

This program will use a TMF count of : 020.



Database Integrity Program

Starting Phase 1

```
Summary of Phase 1:  Number of missing EVENTCX records      : 00000,
                    Number of missing ACTEVE records      : 00000,
                    Number of missing STRMCONF records     : 00000,
                    Number of STRMCONF records with invalid configs : 00000,
                    Number of deleted STRMCONF records    : 00000,
                    Number of missing EVCONFIG records    : 00000,
                    Number of missing ALIASMAP records     : 00000,
                    Number of ALIASMAP records inserted   : 00000,
                    Number of EVENTDB records with incorrect info : 00000,
                    Number of updated EVENTDB records     : 00000,
```

Starting Phase 2

```
Database Inconsistency : Incompatibility between EVENTDB and ACTEVE :
                        : FOR event owner : INSIDER , event value : 0051,
                        : event number : +3106.
```

```
Database Inconsistency : Incompatibility between EVENTDB and ACTEVE :
                        : FOR event owner : INSIDER , event value : 0051,
                        : event number : +3106.
```

```
Database Inconsistency : Incompatibility between EVENTDB and ACTEVE :
                        : FOR event owner : INSIDER , event value : 0051,
                        : event number : +3106.
```

```
Database Inconsistency : Incompatibility between EVENTDB and ACTEVE :
                        : FOR event owner : INSIDER , event value : 0051,
                        : event number : +3106.
```

```
Database Inconsistency : Incompatibility between EVENTDB and ACTEVE :
```

```
Summary of Phase 2 :  Number of missing EVENTDB records : 00000,
                    Number of EVENTDB records inserted : 00000,
                    Number of EVENTDB records with incorrect info :00005,
                    Number of updated EVENTDB records : 00000,
                    Number of orphaned ALIASMAP records : 00000,
                    Number of deleted ALIASMAP records : 00000,
                    Number of STRMCONF records with invalid configs :00000,
                    Number of deleted STRMCONF records : 00000,
```

Starting Phase 3

```
Summary of Phase 3 :  Number of orphaned ACT* records : 00000,
                    Number of inconsistencies between ACT* records : 00000,
                    Number of deleted ACT* records : 00000,
                    Number of missing ACT* records : 00000,
                    Number of updated EVENTDB records : 00000,
```

Starting Phase 4

```
Summary of Phase 4 :  Number EVENTDB records with all flags set to 'N' :00000,
                    Number of deleted EVENTDB records : 00000,
```



Database Integrity Program

Starting Phase 5

```
Summary of Phase 5      : Number of unused SECCLASS records : 00000,
                        : Number of records with an invalid facility : 00000,
                        : Number of deleted SECCLASS records : 00000,
```

Starting Phase 6

```
Database inconsistency:EVETXT record exists & is not used -> Owner : INSIDER
                                                                Value : 0050
                                                                Event No : 02553
```

```
Database inconsistency:EVETXT record exists & is not used -> Owner : INSIDER
                                                                Value : 0050
                                                                Event No : 02554
```

```
Database inconsistency:EVETXT record exists & is not used -> Owner : INSIDER
                                                                Value : 0050
                                                                Event No : 02555
```

```
Database inconsistency:EVETXT record exists & is not used -> Owner : INSIDER
                                                                Value : 0050
                                                                Event No : 02556
```

```
Database inconsistency:EVETXT record exists & is not used -> Owner : TANDEM
                                                                Value : 0010
                                                                Event No : 00078
```

```
Database inconsistency:EVETXT record exists & is not used -> Owner : TANDEM
                                                                Value : 0031
                                                                Event No : 05056
```

Summary of Phase 6

```
Number of unused TASKPROG records      : 00000
Number of unused TASKCONF records      : 00000
Number of unused TASKOWNR records      : 00000
Number of unused EVETXT records        : 00006
Number of deleted TASKPROG records     : 00000
Number of deleted TASKCONF records     : 00000
Number of deleted TASKOWNR records     : 00000
Number of deleted EVETXT records       : 00000
```



Introduction

This section details the best approach to using the BASE24™/XPNET agents available within the Reflex 80:20 product.

Reflex ONE24™ manages single and multiple instances of the BASE24™ application across an entire HPE NonStop Expand network, offering tight integration within an all-encompassing graphical interface.

An XPNET automatic detection utility is available to extract a copy of the various XPNET nodes, stations, lines, links, processes and device entities using the NCP (network control point) servers of BASE24™. This detection will populate the Reflex 80:20 database with the required records to enable graphical component trees to be built up using the Reflex 80:20 GUI interface. These object trees can be tailored in any way depending upon how users wish to see the various XPNET relationships.

For instance, an object tree can be built to group a station with related lines and processes. The detection utility can also produce default trees where all like XPNET components are grouped under a single display icon for each XPNET object node, e.g. P1A^NODE STATIONS, P1B^NODE LINES.

Once an XPNET graphical tree has been built, a simple click on an individual component will provide access to information, status and statistics relating to that XPNET object. This is provided using a status agent module available within the Reflex ONE24 product, interacting with the NCP-SERVERS of the BASE24™ application. This feature enables users to make use of the integrated network display of Reflex 80:20 to access XPNET component data rather than using TACL prompts and the NCPCOM conversational interface.

Reflex 80:20 provides quiet, CPU friendly monitoring of all HPE NonStop Guardian subsystems and applications. This is achieved by taking advantage of the DSM subsystems. Reflex 80:20 can be configured with BASE24™ and XPNET EMS exception alerts that will automatically be mapped against the detected XPNET graphical trees of Status Monitor. From here, users can acknowledge events and invoke XPNET tasks to remedy problems. A default list of tasks is available in Reflex ONE24™, by way of a transit file that can be imported into the Reflex 80:20 database using a standard deliverable utility.

A list of received EMS events can be displayed for each XPNET entity providing a comprehensive history of issues and states over hours, days and weeks.

The rest of this section verifies and describes the correct set-up of your Reflex 80:20 application to make use of the BASE24™ monitoring capabilities available within the Reflex ONE24 product.



BASE24™ Set-up of Reflex ONE24

BASE24™ XPNET Version

Reflex ONE24™ agents have been engineered and tested against version 3.05 of the XPNET layer of the BASE24™ application, with integration testing being performed by Insider Technologies personnel. Check your version of XPNET before proceeding, to ensure compliance with Reflex ONE24™.

Note: Any questions on the installation of the Reflex ONE24™ product or the features currently available should be directed at Insider Technologies and not ACI.

The Reflex ONE24™ XPNETCNF Configuration File

This edit file contains various configuration values to be used by both the XPNET automatic detection utility 'XPNETADC' and the Reflex ONE24 status agent server ACI-XPNET-AGENT (XPNETAGC). This file will need to be modified as part of Reflex ONE24 BASE24™ monitoring.

This edit file is always contained within the Reflex 80:20 data files sub-volume, e.g.

```
\INSIDER.$DATA02.RFLXDAT.XPNETCNF
```

Note: If you have received an XPNETCNF file as part of a Reflex ONE24 BASE24™ delivery, place a copy of this in your Reflex 80:20 database subvolume, e.g. RFLXDAT. Check to see if you already have a copy of this file.

The configuration values are listed below in their respective order within the edit file.

1. **User** – represents the user portion of the key into the XPNET security system. If the security is turned off for the XPNET layer of BASE24™ then this value does not need to be supplied. If security is turned on, then an appropriate BASE24™ user needs to be supplied here, e.g. BASE24™/USER. This is currently the default. See A Read Only BASE24™ User.
2. **Sess_id** – identifies an end user session in cases where multiple openers may be logged on to the same user definition. This can be any 16-character printable ASCII value. The sess-id is logged in the command audit event. The default is 'rflx24cmdissued'.
3. **User_info** – represents information needed for user verification. This must match the password entered into the NCSS record for the user-id/node combination. This is only true if the security is turned on the XPNET layer. See A Read Only BASE24™ User.
4. **Ncp_val_abnormal** – one of the states of an XPNET component. The default is down (DN). This will show as red in Reflex ONE24™ Status Monitor if requesting exact XPNET status using the floating toolbar. If wanting to show this as green (UP) or blue for vulnerable (VU), change value appropriately. This is also true of items 5 to 10 below.
5. **Ncp_val_configured** – the default is vulnerable (VU).
6. **Ncp_val_started** – the default is up (UP).
7. **Ncp_val_starting** – the default is vulnerable (VU).
8. **Ncp_val_stopped** – the default is stopped (DN).
9. **Ncp_val_stopping** – the default is vulnerable (VU).
10. **Ncp_val_suspended** – the default is vulnerable (VU).
11. **Ncp_server** – this is the name of the BASE24™/XPNET server which is usually 'SERVER-NCP' within the BASE24™ Pathway. This is the default.
12. **Ncp_process** – this should be set to the process name of the production / live Pathway for the BASE24™ application, e.g. \$PPMN. This is the default.



A Read Only BASE24™ User

If the security for the XPNET layer of the BASE24™ application is turned to 'ON' then parameters [1] and [3] above will need to be supplied. This XPNET parameter setting can be verified by accessing the PATHCOM interface for your elected BASE24™ application and executing an info request on server 'SERVER-NCPI'. The parameter 'ENABLE-SECURITY' within this server configuration will detail whether or not the security is switched on or off.

The ENABLE-SECURITY parameter is used to enable or disable security checks within SERVER-NCP. If ENABLE-SECURITY is set to ON, the NCSP and NCSS files of BASE24™ are used to check a user's access to a node and command. Security violations result in the generation of a security violation event containing user and session information. If ENABLE-SECURITY is set to OFF, the NCSP and NCSS files are not checked. The default value for this parameter is ON.

If switched off then parameter [1] and [3] above need not be supplied and can be set to spaces or left at the default values. If switched ON then a special Reflex ONE24™ BASE24™ user needs to be set-up (or a current low security BASE24™ user utilised) within the BASE24™ application to allow read only access.

This user requires only the ability to see the BASE24™ XPNET object components, i.e. XPNET nodes, stations, lines, links, processes and devices. This ensures that the automatic detection utility and status agent can issue the following commands programmatically through the NCP servers:

- Listobjects - automatic detection - TACL
- Status - status agent - GUI
- Info - status agent - GUI
- Statistics - status agent - GUI

This is the same user and password when using the NCPCOM conversational interface when security is set to on. Update parameter [1] and [3] in the XPNETCNF file discussed in the previous section.

Remember that the password and user are case sensitive and that the XPNETCNF file needs to reflect the user set-up exactly.

XPNET Object Types and Sub-types

Every object or entity with the Reflex 80:20 application has an associated type and subtype. Here are some examples:

HPE NonStop Component	Type	Subtype
CPU	TANDEM_HARDWARE	CPU
DISK	TANDEM_HARDWARE	DISK
SERVER	PATHWAY	SERVER
PROCESS	TANDEM	PROCESS

The reason behind this type association is so that tasks, status agents and Status Monitor graphical icons can be linked with component types, such as the above. In the case of tasks, only pertinent tasks are listed in the Status Monitor window for particular component types. Some types and subtypes have a corresponding status agent. An agent can probe a component sub-system for more detailed information on that object. The component information can then be displayed in a pop up window in the Status Monitor screen.



The types and subtypes for the BASE24™ XPNET components are as follows:

XPNET Component	Type	Subtype	Status Agent
NODE	BASE24_XPNET	NODE	XPNET-AGENT
STATION	BASE24_XPNET	STATION	XPNET-AGENT
LINE	BASE24_XPNET	LINE	XPNET-AGENT
LINK	BASE24_XPNET	LINK	XPNET-AGENT
PROCESS	BASE24_XPNET	PROCESS	XPNET-AGENT
DEVICE	BASE24_XPNET	DEVICE	XPNET-AGENT

These need to be added to the list of types and subtypes delivered as standard with the Reflex 80:20 product. To do this, carry out the following (see **note** below):

1. Logon to the Reflex 80:20 application with an appropriate Guardian user who has been given set-up rights.
2. Click on the 'Monitor' option above the main toolbar, which is the sixth option along above the Gateway graphic.
3. Click on the 'Network Set-up' option to display the Overdrive Configuration Window. Maximise this window.
4. Subsequently click on the 'Type Set-up' tab to show a list of pre-delivered types and subtypes.
5. Scroll down the list to look for the above types and subtypes for the XPNET components. If they are not present then type them in exactly as specified above and click on the add button '+' on the window toolbar.

Note: if you have received an SQLINUP file as part of a Reflex ONE24™ BASE24™ delivery, the above steps are not required. Carry out the following procedure:

1. Logon to the HPE NonStop as the Guardian User who owns the Reflex 80:20 application.
2. Volume to the object sub-volume, e.g. RFLXOBJ.
3. Run the RSQLDEFS file in this sub-volume to load the Reflex 80:20 SQL defines.
4. Access the SQLCI interface by typing 'SQLCI' at a TACL prompt.
5. Obey the SQLINUP file supplied to add the XPNET component types and subtypes.
6. Exit from the SQLCI interface. The Types and Subtypes can then be viewed by carrying out steps 1 to 4 above.



Checking REFLEX ONE24 XPNET Executables

Reflex ONE24™ requires two object files to be placed in the object sub-volume before BASE24™ XPNET monitoring can proceed. These are as follows:

- XPNETADC - XPNET menu driven detection utility
- XPNETAGC - XPNET status agent to supply info, status and statistics

The XPNETADC executable can be run from a TACL prompt (see Auto-Detection of BASE24™/XPNET to provide for automatic detection of XPNET components). It does not require a Pathway server to be set-up and is a menu driven utility. The second object, XPNETAGC requires a Pathway server as discussed in section 2.5, and allows detailed information to be passed back to the Reflex 80:20 Status Monitor graphical window on user request.

Note: If you have received both XPNETADC and XPNETAGC object files as part of a Reflex ONE24™ delivery, place them in the Reflex 80:20 object sub-volume. Both files interact with the NCP servers of XPNET but the XPNETADC detection executable also populates the Reflex 80:20 SQL database. For this reason it will need SQL compiling. If required, carry out the following steps:

1. Logon to the HPE NonStop as the Guardian user who owns the Reflex 80:20 application.
2. Volume to the Reflex 80:20 object sub-volume, e.g. RFLXOBJ.
3. Run the RSQLDEFS file in this sub-volume to load the Reflex 80:20 SQL defines.
4. Type the following:

```
>SQLCOMP/IN XPNETADC,OUT $$.#XPRFLX,PRI 50,NAME $RFSQC/CATALOG =REFLEX_CATALOG
```

5. Check PERUSE to ensure the SQL compilation was successful.

Once having applied any of the amendments referred to in this section of the document, stop and start the Reflex 80:20 application to pick up the ONE24 modifications. To do this, carry out the following steps:

1. Logon to the HPE NonStop as the Guardian user who owns the Reflex 80:20 application.
2. Exit any Reflex 80:20 GUIs currently running.
3. Volume to the Reflex 80:20 object sub-volume.
4. Obey the STOPRFLX file in this sub-volume.
5. Once stopped, obey the RUNRFLX file in the same sub-volume.
6. Re-start and logon to the Reflex 80:20 GUI.



Auto-Detection of BASE24™/XPNET

The Reflex ONE24™ BASE24™ XPNETADC Detection Utility

It is recommended that this section be read in its entirety before deciding on a particular approach to graphically representing your BASE24™ XPNET components.

This utility allows for the detection and extraction of a complete copy of the XPNET components that make up a given XPNET node. These components are subsequently inserted into the Reflex 80:20 SQL database to provide easy configuration of the product for BASE24™ XPNET monitoring. To run the utility, carry out the following steps:

1. Logon to the HPE NonStop as the Guardian user who owns the Reflex 80:20 Pathway application.
2. Volume to the Reflex 80:20 object sub-volume, e.g. RFLXOBJ.
3. Type: `>RUN XPNETADC / in RFLXDAT.XPNETCNF / [return]`
4. The following menu will appear:

```
Node : \INSIDER          Reflex BASE24 XPNET Autodetect Menu

[ 1] Auto-Detect NODES          [ 7] Delete NODES
[ 2] Auto-Detect LINES          [ 8] Delete LINES
[ 3] Auto-Detect STATIONS       [ 9] Delete STATIONS
[ 4] Auto-Detect PROCESSES      [10] Delete PROCESSES
[ 5] Auto-Detect LINKS         [11] Delete LINKS
[ 6] Auto-Detect DEVICES       [12] Delete DEVICES

[13] Enter a Preferred Reflex CLASS for SMON Display
[14] Object Tree/Object Detect - Default Object Tree
[15] Autodetect Objects Outside of SMON Warm-Boot

0. Exit Menu

Option >
```

This menu allows for both the detection and deletion of XPNET components from the Reflex 80:20 database. The default detection will insert all like components under a single Status Monitor group. This will be placed below the BASE24™ class heading (B24) for a given BASE24™ XPNET node. This can be seen clearly in the following bitmap.

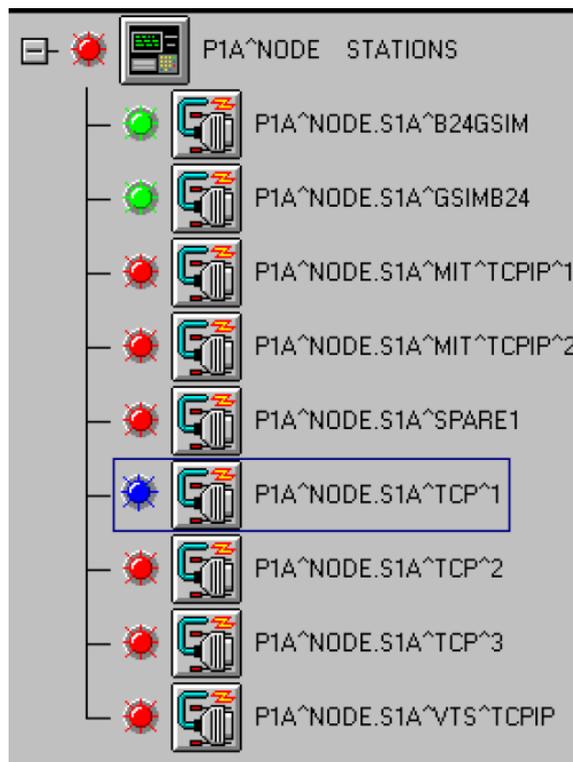


If option [3] on the menu 'Auto-Detect STATIONS', is selected, the user is prompted to enter the XPNET node to probe for station components.

```
Option > 3
```

```
Enter XPNET node for stations to be autodetected, e.g. P1A^NODE :  
XPNET Node> P1A^NODE
```

This will result in a group under the B24 class heading, called 'P1A^NODE STATIONS'. Beneath this will be placed all the stations belonging to that XPNET node. This is shown in the bitmap on the next page. **Note:** the status of components is discussed in a later section.

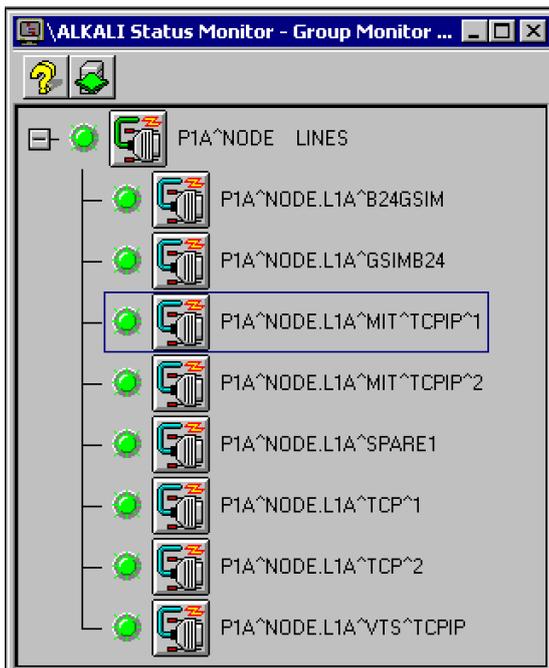


Similarly, if option [2] on the menu 'Auto-Detect LINES', is selected, the user is prompted to enter the XPNET node to probe for line components.

```
Option > 2
```

```
Enter XPNET node for lines to be autodetected, e.g. P1A^NODE:
XPNET Node> P1A^NODE
```

This will result in a group under the B24 class heading called 'P1A^NODE LINES'. Beneath this will be placed all the lines belonging to that XPNET node. This is shown in the bitmap on the next page. **Note:** the status of components is discussed in a later section.



This is the default automatic detection for all XPNET node components. The detection of the actual XPNET nodes themselves will result in all XPNET nodes for a given Pathway being placed under a top-level group called 'XPNET NODES'.

If running the XPNETADC ONE24 detection utility, the default discovery will result in all like components being placed under a group name with the XPNET node name followed by the type of component as shown above. This can be changed to provide a more tailored aesthetic look for your BASE24 XPNET layer and this discussed in the next section.

If more XPNET components are configured in the XPNET layer of BASE24™, the XPNETADC detection utility can be used to redetect and so rebuild the object trees of Reflex 80:20 Status Monitor. Before this can be done, a 'DELETE' should be carried out for the appropriate object tree (see **Note** below before doing this). In the case of the last example, 'P1A^NODE LINES', this is carried out by selecting option [8] from the menu and typing the appropriate XPNET node.

```
Option > 8

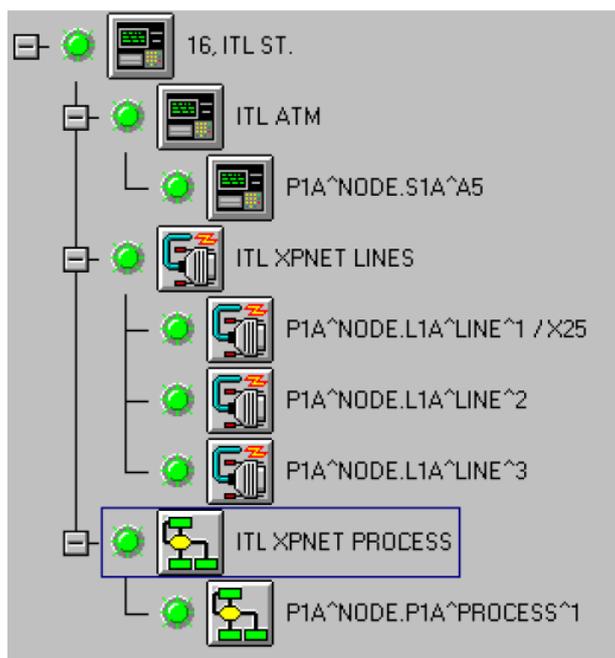
Enter XPNET node for lines to be deleted. e.g. P1A^NODE:
XPNET Node> P1A^NODE
```

Note: Detecting all of your XPNET components such that they are grouped under a main heading group name, that is 'XPNET node name' followed by type, e.g. P1A^NODE STATIONS, then performing a deletion followed by redetection can be carried out as often as required. This may not be the case if using a less grouped approach for displaying XPNET entities; e.g. every station (ATM or Point of Sale Terminal) has its own presence in a top-level Status Monitor matrix (see ATM diagram below). See next section for tailoring different graphical layouts for your XPNET components and approaches to adding to Reflex ONE24, newly configured BASE24 XPNET components.



Options Available for Tailoring Graphical Displays

Different approaches for displaying the XPNET layer of BASE24™ can be taken in Reflex ONE24™ other than the default displays talked about so far. This can be achieved by using some of the options available in the XPNETADC ONE24 detection utility but also making use of the Status Monitor set-up screens. These allow for the dragging and dropping of objects into component trees for a greater separation of business service areas or geographical locations. In the latter case, ATMs (stations) as an example, can be separated into regions, streets or most and least sensitive in terms of customer usage. Lines associated with stations can be grouped under the same heading so that relationships can be maintained graphically making troubleshooting easier. This is especially true when using tasks; see Using Reflex ONE24 Tasks to control XPNET Entities.



What follows is a discussion on the ways that Reflex ONE24™ can be used to produce the best graphical representation of the BASE24™ XPNET layer for your particular requirements. Later options may provide a more appropriate strategy for your particular on-site monitoring needs.

Option [13] – Enter a preferred Reflex ONE24™ class for SMON display

The default for any detected XPNET components is to place the resulting group of components under the 'B24' class as shown in section 3.1. Option [13] allows the user to change the class under which detected groups are stored. This can also be a totally new class name not currently seen in the Status Monitor display, e.g. NEW, ACI or XPN.

To place components belonging to say 'P1A^NODE' XPNET node under a P1A class, request option [13] from the XPNETADC detection menu and type P1A (or a preferred class) at the prompt 'CLASS Node>'.

```
CLASS Node>
```

```
Option > 13
```

```
Enter a Reflex CLASS name under which to store Autodetection:
CLASS Node>
```



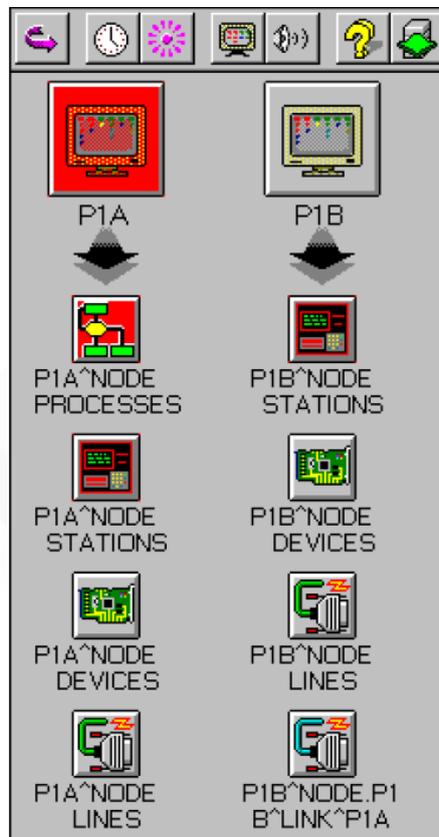
Reflex ONE24

Using options 2 to 6 on the XPNETADC detection menu, build the Reflex ONE24™ Status Monitor groups for the relevant P1A^NODE component types (or the XPNET node you are detecting for).

Note: The XPNET nodes themselves are detected and inserted under a single group and so should be placed under a generic class if using this class naming approach, e.g. XPN or B24 could be used for XPNET nodes.

If you have a second node to detect, e.g. P1B^NODE, enter option [13] once again from the XPNETADC detection menu and type 'P1B'.

Using options 2 to 6 on the XPNETADC detection menu, build the Reflex ONE24™ Status Monitor groups for the relevant P1B^NODE component types (or the XPNET node you are detecting for). The resulting display using this approach to XPNET detection will look as follows (the status is discussed in a later section):



Option [14] – Object Tree / Object Detect – Default Object Tree

Rather than building XPNET component trees using the detection menu, option [14] allows for the detection of just the XPNET objects themselves. These are inserted into the object SQL table, e.g. RFLXDAT.OBJECTQ. From here they can be dragged and dropped using a Reflex 80:20 GUI window, into groups that you have named yourself.

```
Option > 14

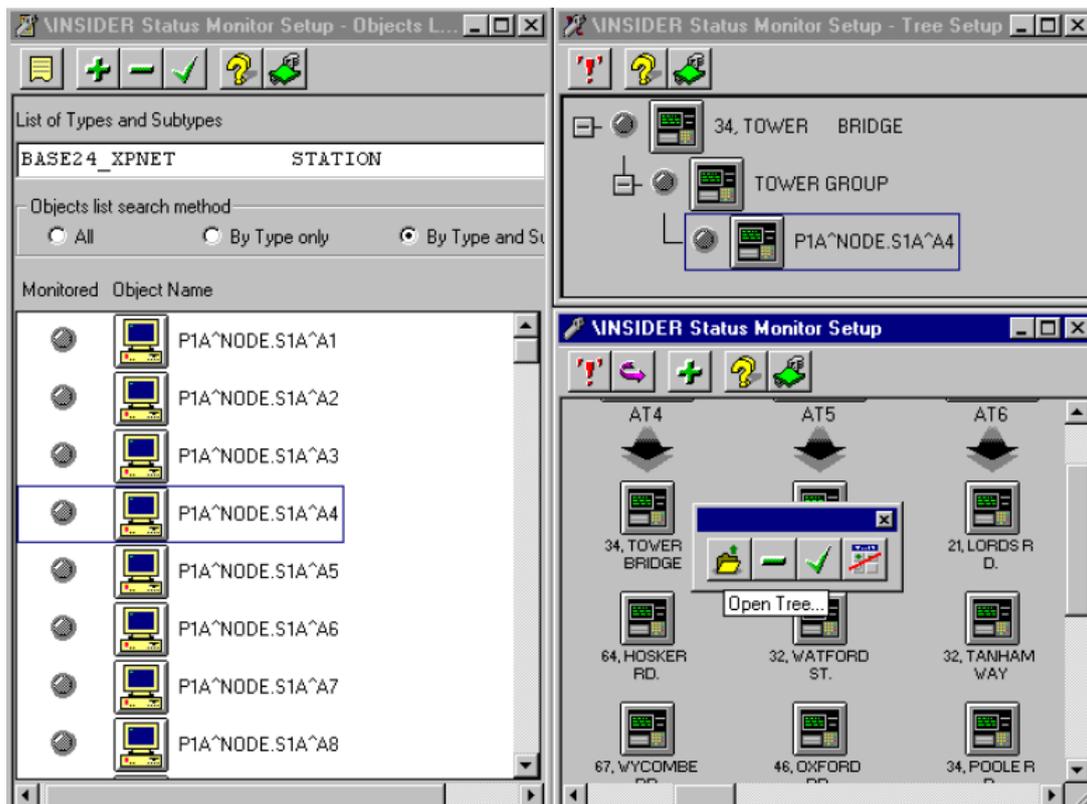
Enter 1 - Object Tree / 2 - Object Level Auto-Detection:
1 or 2>
```



Reflex ONE24

Enter 14 at the XPNETADC menu as shown above and then enter 2 to signify that you just require the raw XPNET components to be detected rather than the tree building to be performed. After this toggle has been applied, any detection that takes place using the options 1 to 6 on the detection menu will only detect the XPNET objects and not build the Status Monitor trees.

After detecting the XPNET objects, the user can access the object list window of Reflex 80:20 and drag and drop objects into appropriately named groups. This is shown in the following bitmap:



Outlined below are the steps used to create a group called '34, Tower Bridge' and drag an appropriate station (ATM) under it for monitoring.

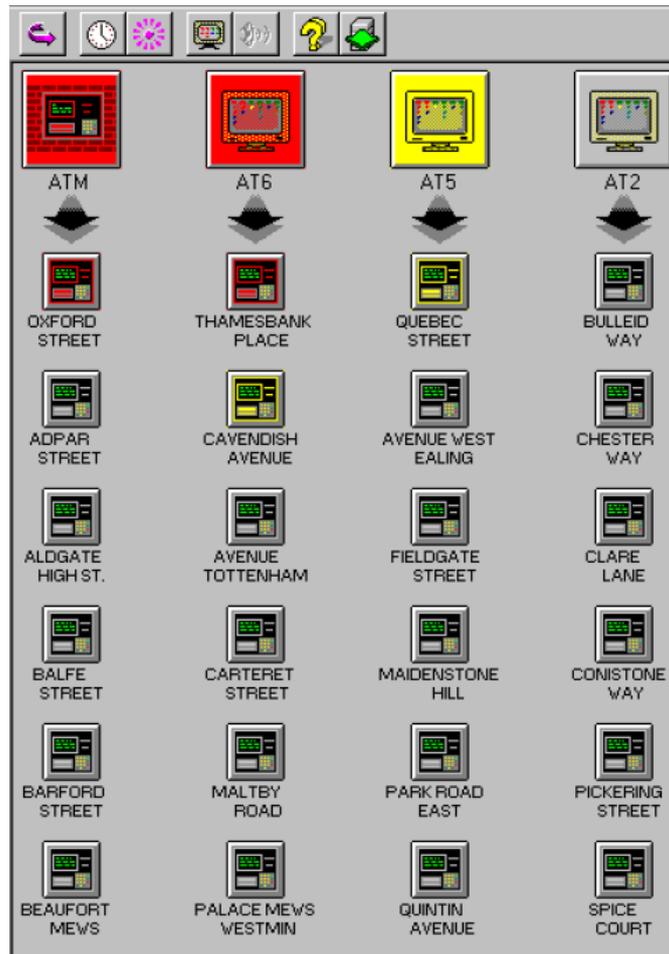
1. Logon to the HPE NonStop with the Guardian user who owns the Reflex 80:20 Pathway.
2. Volume to the Reflex 80:20 object sub-volume, e.g. RFLXOBJ.
3. Run the XPNETADC ONE24 detection utility as follows (RFLXDAT is the location of your Reflex 80:20 data files):


```
> RUN XPNETADC / IN RFLXDAT.XPNETCNF / [return]
```
4. Enter option [14] and set detection type to '2' – Object Level Auto-Detection.
5. Enter option [3] to detect XPNET stations.
6. Enter the XPNET node you wish to probe and extract a copy of the station components to insert into the Reflex 80:20 database, e.g. P1A^NODE.
7. Enter '0' to exit from the XPNETADC detection menu.
8. Logon to the Reflex ONE24™ GUI with a user who has access to Reflex 80:20 set-up facilities, e.g. a Reflex ONE24™ Administrator user.
9. Click on the 'OD set-up' icon on the main toolbar.



10. Maximise the resulting window.
11. Click on either an existing class icon, e.g. ATM, B24, BAT or click on '+' icon on the toolbar to enter a new class name, e.g. AT1, XPN, ACI. Enter the group name '34, Tower Bridge' (or your own preferred name) and choose an icon for display, e.g. ATM.
12. Click on the '+' icon on the set-up window toolbar and acknowledge the message for confirmation of the added group/class function. The screen will be refreshed and your top-level group will be displayed appropriately under the chosen class.
Note: In some cases, the text may be wrapped to the next line of the display for a group name breaking a word into 2 fragments. If this is not preferred, delete the group by left clicking on it and re-add but placing some spaces between it and the next word, e.g. '34, Tower Bridge'. This will force the set-up code to throw the next word to the next line rather than breaking it over 2 lines. **Note:** Reflex 80:20 allows up to 11 characters per line.
13. Left click on the group you added and click on the folder icon on the floating toolbar to drill down.
14. Click on the 'Window' option above the main toolbar of Reflex 80:20 and tile the display vertically. Three windows will appear. The top-level display you have just come from, the object list window and the next level set-up window.
15. Minimise the top-level window and re-tile vertically so that only the object list window and next level set-up window appears.
16. Right click on the group name icon you added and add another group name. The reason this is done is so that in your eventual display, your group name is not replaced by the object name you will eventually add since there is only one object in the group.
17. Type the name of a group and click on the '+' button to insert it.
18. On the object list window, click the pager button for listing 'By Type and Subtype'.
19. Click on the 'down arrow' under the 'List of Types and Subtypes' heading to show the current Reflex ONE24™ types and sub-types.
20. Click on the 'BASE24_XPNET STATION' type and subtype and subsequently list the objects using the note paper icon in the top left of the object list window.
21. The stations will be listed. Click and hold on the appropriate station and drag and drop it over the second group you added in next level window display.
22. Finally, click on the '!' icon on the next level window to warm-boot the set-up data to show your newly added group containing your elected station in the live Overdrive monitoring window. Click on the confirmation messages for the warm-boot and subsequently click on the 'Overdrive' icon on the main toolbar to see the result.

Repeatedly building up groups in this way allows the user to produce any desired graphical display for XPNET nodes, stations, lines, links, processes and devices. For an ATM network, repeatedly carrying out the above steps after detecting the stations, can lead to an ATM matrix similar to the one displayed below. In larger networks, ATMs can be grouped under a single group. For instance, Oxford Street in London may be home to 40 ATMs that could be dragged and dropped under an Oxford Street top-level group. Each of the stations underneath the group can then be given an alias name for the street number or sequence number.



IMPORTANT: If tailoring your own screens without using the XPNETADC ONE24 defaults of placing components all under a group then the deletion options of the XPNETADC menu should NOT be used. Instead, components should be added manually using the Reflex ONE24™ GUI. The detection facility is for bulk detection to speed up the set-up process but small modifications to the screen or new XPNET additions should be made manually.

If using the defaults of group detection under XPNET node icons, the deletion options can be used as often as required to refresh those groups.

Option [15] – Auto-detect Objects Outside of SMON Warm-Boot

This option on the XPNETADC detection menu allows for the production of a separate XPNET database. This falls outside of the warm-boot mechanism. The sum result of this mode of detection is that the resulting trees cannot be accessed using the set-up GUIs of Reflex 80:20. They can only be seen in the live Overdrive window. Choosing '2' from this option allows no user access to detected XPNET trees.

```
Option > 15

Enter 1 - Warm-Boot Detection / 2 - Outside Warm-Boot Detection:
1 or 2>
```



In large XPNET systems, this will lead to an improved warm-boot response time. The XPNET component trees are always available in the live Overdrive window with any red/blue status logged against individual XPNET components being retained. This option will be expanded in the next release of the software.

Adding XPNET Components Manually After Bulk Detection

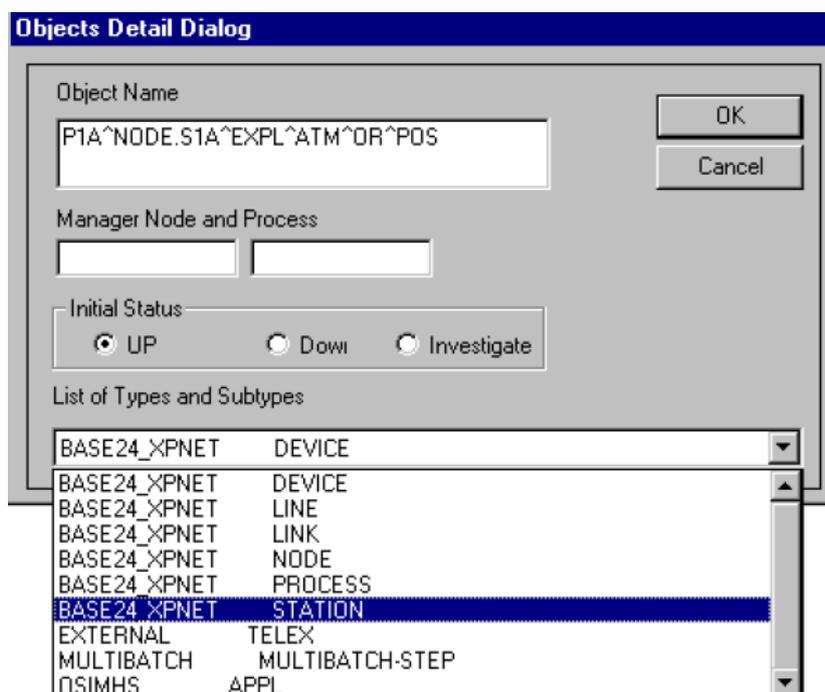
It is important that after bulk detection of XPNET components that newly configured stations, lines etc., are added manually to the Reflex 80:20 database. This is only true if not using the default detection options offered for grouping objects and opting for a more tailored Status Monitor screen.

Outlined below are the steps in adding in XPNET components manually using the GUI set-up screen:

1. Logon to the Reflex 80:20 GUI with a user who has access to Reflex 80:20 set-up facilities, e.g. a Reflex ONE24™ Administrator user.
2. Click on the 'OD set-up' icon on the main toolbar.
3. Maximise the resulting window.
4. If no appropriate XPNET groups currently exist below the class names across the top, of the screen, click on either an existing class icon, e.g. ATM, B24, BAT or click on '+' icon on the toolbar to enter a new class name, e.g. AT1, XPN, ACI. Enter a group name and choose an icon for display, e.g. ATM.
5. Click on the '+' icon on the set-up window toolbar and acknowledge the message for confirmation of the added group/class function. The screen will be refreshed and your top-level group will be displayed appropriately under the chosen class.

Note: In some cases, the text may be wrapped to the next line of the display for a group name breaking a word into 2 fragments. If this is not preferred, delete the group by left clicking on it and re-add but placing some spaces between it and the next word, e.g. '34, Tower Bridge'. This will force the set-up code to throw the next word to the next line rather than breaking it over 2 lines. **Note:** Reflex 80:20 allows up to 11 characters per line.

6. Left click on the group you added and click on the folder icon on the floating toolbar to drill down.
7. Click on the 'Window' option above the main toolbar of Reflex 80:20 and tile the display vertically. Three windows will appear. The top-level display you have just come from, the object list window and the next level set-up window.
8. Minimise the top-level window and re-tile vertically so that only the object list window and next level set-up window appears.
9. Right click on the group name icon you added and add another group name. The reason this is done is so that in your eventual display, your group name is not replaced by the object name you will eventually add since there is only one object in the group.
10. Type the name of a group and click on the '+' button to insert it.
11. On the objects list window, click on the add button '+'. The following window should appear.



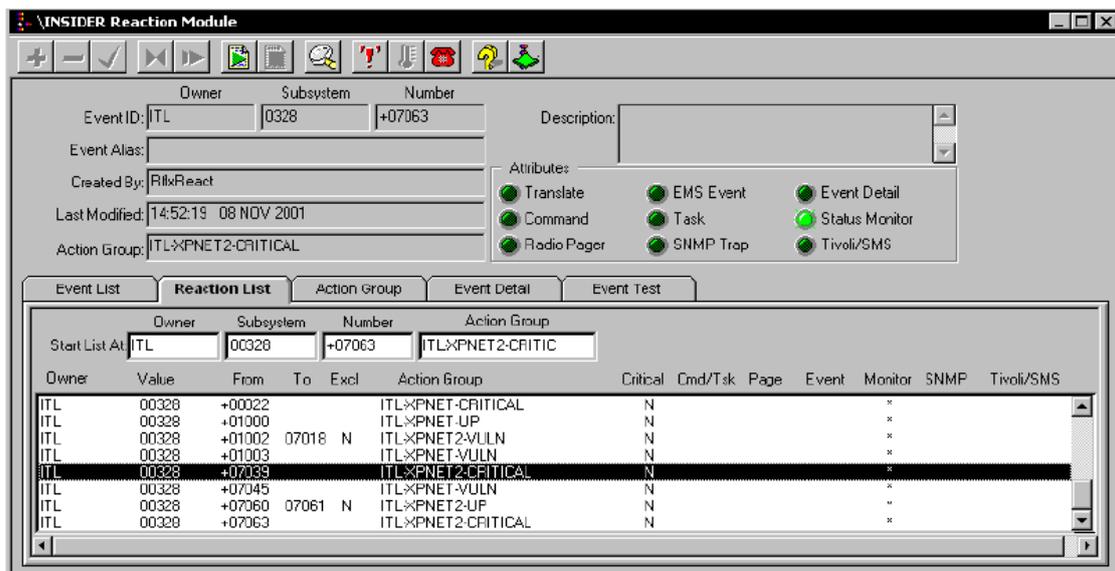
12. Add in the name of the XPNET component you wish to add in the format as shown above, e.g. P1B^NODE.S1B^EXAMPLE^STAT, where the component name is prefixed with the XPNET node name.
13. Select the appropriate type and subtype for the newly added XPNET component from the drop down list as shown above.
14. Select from the 'Initial Status' box, whether during a warm-boot, object is to be 'Investigated' (to check status of object) or automatically placed in either an 'UP' or 'DOWN' state, regardless of actual state. EMS events or users requesting status after the warm-boot has occurred will drive the icon status after the warm-boot.
15. Click on the OK button to add the XPNET object and drag and drop it into the group in the next level window. Once the object has been added it can be dragged into any group you choose or can occur in more than one group.
16. Finally, click on the '!' icon on the next level window to warm-boot the set-up data to show your newly added group containing your elected station in the live Overdrive monitoring window. Click on the confirmation messages for the warm-boot and subsequently click on the 'Overdrive' icon on the main toolbar to see the result.



Configuring BASE24™ EMS Events for Reflex ONE24

The Reflex 80:20 Reaction Module

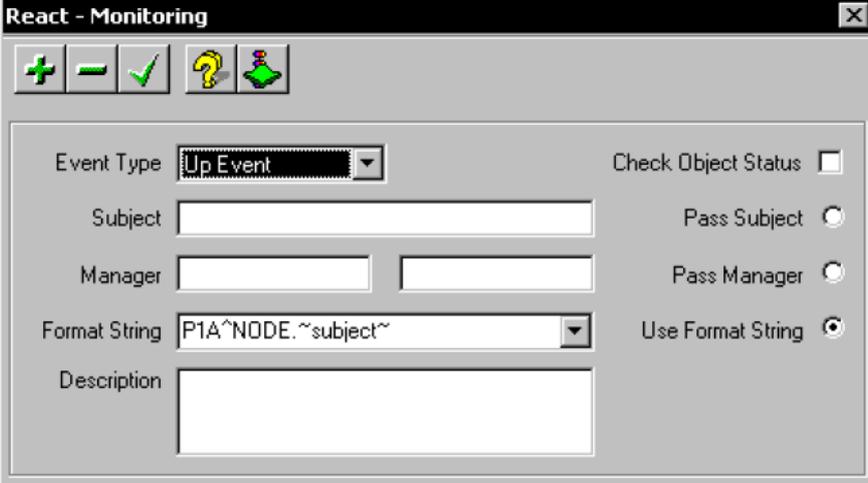
The Reflex 80:20 product allows for the monitoring of chosen EMS event ranges within the BASE24™ application. These can be system level problems or issues, such as invalid or unrecognised data passed to certain XPNET processes, right through to ATM (station) specific EMS alerts such as: hopper low, cash out, paper out, etc.



The green light 'Attributes' in the bitmap above represent all the reactions that can be carried out as a result of receiving a BASE24™ event. An event relating to any area of the BASE24™ application can be mapped either against a generic icon graphic in Status Monitor or an individual XPNET node, station, line, link, process or device.

In order to add an event (or event range), carry out the following steps:

1. Logon to the Reflex 80:20 GUI with a user who has access to Reflex 80:20 set-up facilities, e.g. a Reflex ONE24™ Administrator user.
2. Click on the Reaction module on the main toolbar of Reflex 80:20.
3. Maximise the resulting window.
4. Click on the 'Action Group' tab of the maximised window.
5. Enter the SSID of the event(s) you wish to monitor, e.g. XPNET would be ACI.328.
6. Enter the event or event range of the EMS event(s) you wish to monitor.
7. Enter an Action Group. This is a free text field used to group a reaction(s) that you wish to occur when the given EMS event(s) is passed to Reflex 80:20. This Action Group can be used again if just wishing to carry out the same reaction, e.g. toggle the colour of an XPNET component icon from one status to another. Action group 'ACI-ITL-XPNET-CRITICAL' could be used as the action group to toggle the status of a station, line or process to red (critical/down). This action group is subsequently associated with EMS events relating to XPNET components that are in a down state.
8. Enter a desired cover period.
9. Click on the Status Monitor green attribute button that is the middle right reaction. The following window will be shown:

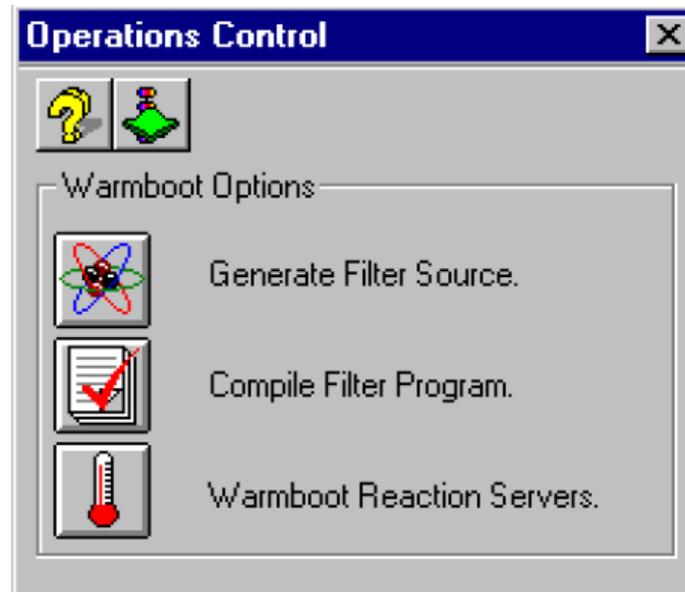


10. Enter the appropriate status you wish to reflect on the graphical Status Monitor screen, i.e. Up, Down or Vulnerable (the latter could be station or line STOPPING for instance).
11. Click on the 'Use Format String' pager button and clear the 'Check Object Status' box. In the latter case, this represents whether Reflex ONE24 function checks the physical or actual status of an XPNET object on receiving an event. This may or may not be appropriate. If an EMS event states that a station has stopped but it has physically started then you may wish to check the object status for this EMS event to be overridden. If the EMS event is informing that 'cash is low' for an ATM (station) then checking the object status will toggle the status of the ATM back to up. In this case we want to display a vulnerable condition even though we are aware of the station being physically up in XPNET. Clearing the object status box in this case, is the preferred setting.
12. Enter the format string as XPNET node suffixed by the subject string in the format shown above. In the case of most XPNET events, the subject of the event is the offending XPNET component. This will be extracted and joined to the XPNET node as entered above and subsequently mapped exactly against one of the graphical icons in the Overdrive window. In the case were the XPNET EMS event has a generic EMS subject token, create an object with a generic name (see Adding XPNET Components Manually after Bulk Detection), e.g. XPNET ISSUES and type 'XPNET ISSUES' into the format string field above. If an event is raised stating a general XPNET issue, this can be mapped directly to the graphical icon 'XPNET ISSUES'.
13. Click on the add button '+' on the window to add the record. If you are re-using the same action group in a BASE24™ event range, then the details may already exist in which case just click the tick (amend) icon to amend the record. This sets a flag on the action group screen to denote that a reaction has been set-up for the given event or event range.
14. Click on the OK confirmation box and exit the above window.
15. Click on add '+' icon on the Reaction window (or amend - tick) to record the addition or modification.



Carry out these steps for other event or event ranges that you wish to monitor. When you have completed the new event additions, carry out the following steps:

1. Click on the '?' icon on the reaction toolbar. The following floating window will be displayed.



2. Click on 'Generate Filter Source' button and wait for confirmation of completion. This generates a filter source file to pass your newly added BASE24™ events to the Reflex 80:20 event monitor.
3. Click OK on the confirmation message. Click on the 'Compile Filter Program' and then click OK to the 'compilation started' confirmation message.
4. Logon to the HPE NonStop as the Guardian user who owns the Reflex 80:20 Pathway application and check PERUSE for successful compilation listings. Alternatively, activate CONSOLE and check for successful compilation EMS messages generated by Reflex 80:20.
5. Click on the 'Warm-boot Reaction Servers' to allow the event monitor to pick up the new filter for your newly added event ranges.

Event Ranges for Multiple XPNET Nodes

If you have more than one XPNET node within your production / live BASE24™ Pathway, then multiple event ranges need to be added to map to the graphical icons of Status Monitor. This is only the case if the reaction is for Status Monitoring.

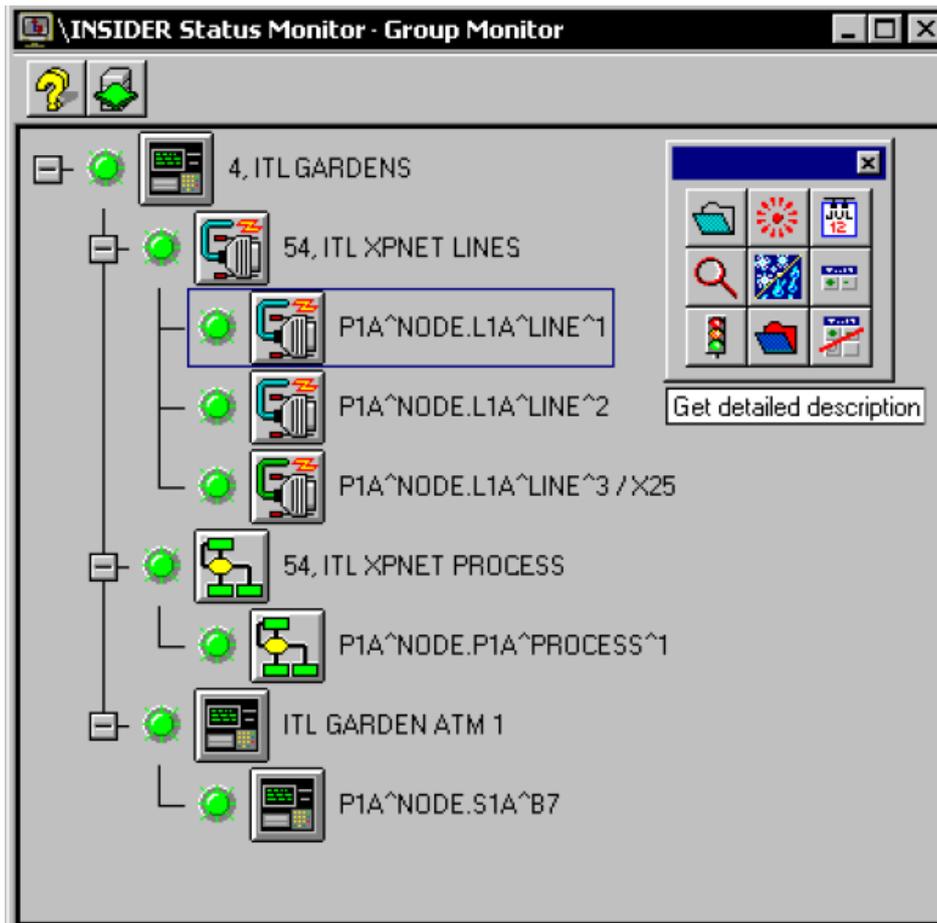
In the case of the example in The Reflex 80:20 Reaction module section, add the same event (or event range) with a different Action Group, e.g. ACI-ITL-XPNET-CRITICAL2, and assign your second node, e.g. P1B^NODE in the React – monitoring window, e.g. P1B^NODE.~subject~. This will result in 2 different action groups assigned to the same event range. This approach is only necessary for non-generic graphical icons, e.g. P1B^NODE.S1A^STATION, as opposed to 'XPNET ISSUES' as discussed in the previous section.



Reflex 80:20 GUI Display of ONE24 XPNET Information

Displaying XPNET Information, Status and Statistics

With the inclusion of the Reflex ONE24™ status agent in the Reflex 80:20 Pathway configuration (ACI-XPNET-AGENT), users are now free to click on any of the BASE24™ XPNET components for detail. The detail window that is brought up will contain detailed configuration information, status details and statistics for the appropriate object. In order to retrieve detailed information, left click on any XPNET component and the floating toolbar shown in the first bitmap below, will be displayed.



Click on the magnifying glass icon (centre left) to retrieve detailed information in the format shown for the appropriate XPNET entity:

```

TRIBUTARY OF
SYMBOLIC NAME          S1A^B24GSIM
LINE ENABLED           00001
INVALID                00000
LOGICAL ACK            OFF
SENSE STATUS Q CNT     00
FORMAT VAR CNT         00
FORMAT VAR STRING
USER DATA NAME        $TEST1.EUR1OBJ
USER DATA

S T A T U S:
-----

CURRENT STATUS         STARTED
CRTP TERM STAT.       STATUS SEL
LINE PROTOCOL          X25
LOGICAL STATE          STARTED
QUEUE COUNT            00000
QUEUE STATE            NORMAL
RETRY COUNT            00
WARMBACKUP LOGIC      WARMSTART
STATE DETAIL           STATE DETAIL

S T A T I S T I C S:
-----

ERRS                   0000000000
INPUT COUNT            0000000000
INPUT FAILURES         0000000000
LINE PROTOCOL          00019
MAX QUEUE COUNT        00000
MSGS DROPPED TTL      0000000000
MSG DROP RATE          0000000000
OUTPUT COUNT           0000000000
OUTPUT FAILURES        0000000000

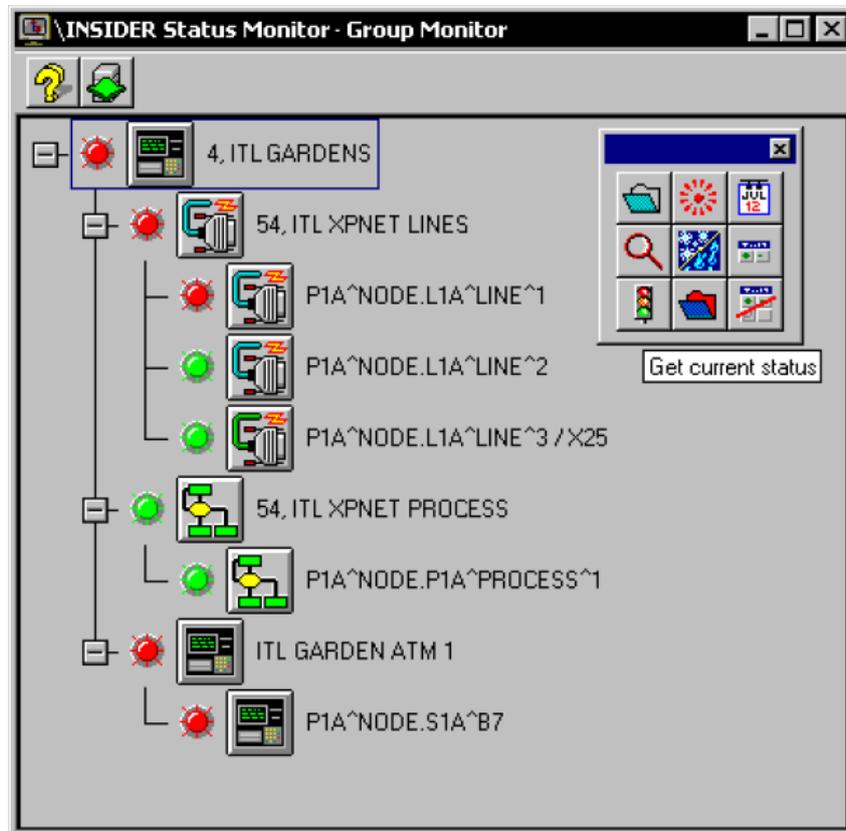
```

Getting Actual Status of an XPNET Component

Reflex ONE24™ will get the status of all XPNET components at start-up or warm-boot if configured to do so (see the Auto-Detection of BASE24™/XPNET section regarding 'Initial Status'). The XPNET graphical icons are then driven by EMS events configured to be reported to the Status Monitor screen.

This explains why Reflex 80:20 is so CPU friendly as it is not constantly probing XPNET every 'N' seconds to find out that the majority of the system is fine. This will lead to an unnecessary load on the XPNET layer of BASE24™ especially in the case of thousands of XPNET components. Instead, Reflex 80:20 listens to the rich supply of BASE24™ exception alerts. The product subsequently reports the graphical status of XPNET entities and other issues relating to other areas of the BASE24™ application.

It is possible for users, however, to request the actual XPNET status of components at any time using Reflex ONE24™. This can be done at object level or at group level. In the latter case, based on the way the objects have been dragged and dropped into groups, users can request the XPNET status of all components subordinate to a group. Left click on a group or object to display the floating toolbar and click on the traffic light graphical icon to get the status from the XPNET layer rather than an EMS event.



In this case, a line and a station are in a STOPPED state indicated by the red coloration. The user has the option of then bringing up the task window to start both the station and line. In the case where all objects are down, a task could be configured to start all XPNET components for a given ATM. See the next section for task configuration.

Edit the ONE24 XPNETCNF file in your data files sub-volume to change the colour representation of each of the 7 states. This is discussed in BASE24™ Set-up of Reflex ONE24, XPNET Object Types and Sub-types.



Using Reflex ONE24 Tasks to Control XPNET Entities

Importing ONE24 XPNET Tasks

A transit file is available that contains a number of configured tasks for each type of XPNET component. Examples of the tasks contained in this file are START, STOP and ABORT BASE24 XPNET component. This can be imported into your Reflex 80:20 environment. To do this, carry out the following:

Note: The transit file is called TRANSTSK and is contained in your Reflex 80:20 data files sub-volume. If you received a separate upgrade sub-volume for Reflex ONE24™ then copy the TRANSTSK file to your Reflex 80:20 data files sub-volume.

1. Logon to the HPE NonStop with the Guardian user who owns the Reflex 80:20 Pathway application.
2. Volume to the Reflex 80:20 object sub-volume, e.g. RFLXOBJ.
3. Run the TASKIMEX import/export utility (RFLXDAT is the location of your data files):

```
> RUN TASKIMEX / IN RFLXDAT.DATACONF / IMPORT * TRANSIT TRANSTSK
```
4. Logon to the Reflex 80:20 GUI with a user who has access to Reflex 80:20 set-up facilities, e.g. a Reflex ONE24 Administrator user.
5. Click on the 'Tasks' icon on the main toolbar.
6. Click on 'Window', 'Tile Vertical' options to show both the programs window and the tasks window of Reflex 80:20.

Since this is a transit file prepared at Insider Technologies, the node, volume and subvolume locations for the task programs should be reconciled. To do this, carry out the following still in the Reflex 80:20 GUI:

1. Maximise the 'Task Master – Program Definition' window.
2. Double-click on the first XPNET program entry – ABRTLIN.
3. Click on the 'Definition' tab (second tab in this window). See bitmap below.
4. Change the process name if required and all HPE NonStop node prefixes.
5. Change all entries in the Parameters aspect of the window to the on-site preferences. The 'INFILE' should stay as 'RFBMTASK' but the node, volume and sub-volume should be reconciled to your Reflex 80:20 object sub-volume.

Note: 'RFBMTASK' is a macro that interacts with NCPCOM (Network Control Point communication) and is contained in your Reflex 80:20 object files sub-volume. If you received a separate upgrade sub-volume for Reflex ONE24™ then copy the RFBMTASK file to your Reflex 80:20 object sub-volume.

6. All other tabs should remain as delivered for the program window. Click on the tick graphic on the program window toolbar to amend the record.
7. Repeat for all other XPNET programs. Go back to the list tab for programs and look for those with XPNET with the description.

All the tasks are owned by SUPER.SUPER and will be executed by the owner of the Reflex 80:20 Pathway application. If you require other users of Reflex 80:20 to run these tasks or you need to run the tasks as a different user in your BASE24™ environment other than the Reflex 80:20 Pathway user, e.g. 'REFLEX.OWNER' then carry out the following tasks:

1. Click on the Tasks module and maximise the Tasks Master window (as opposed to the 'Task Master – Program Definition' window).
2. Double-click on the first XPNET Task – TABRTLIN.



3. Click on the second tab 'Task Configuration' to display the program run as part of this task. Enter the 'Execution User' details and password. This will be the owner of the process when it runs up. Ensure the user has the authority to access NCPCOM and invoke the appropriate commands that make up this task.
4. Click on the tick icon to amend the details.
5. Click on the, 'Task Owners' tab (third tab from left) on this window.
6. Type the task name in the 'Task Name' field if not already there and give it to any other users of Reflex 80:20 who may need to run the task.
7. Click on the '+' icon to add this task owner record.
8. All other tabs should remain as delivered for the Task window.
9. Repeat for all other ONE24 XPNET tasks. Go back to the list tab for tasks and look for those with XPNET for the description.

The bitmap below shows the program details as delivered in the TRANSIT file TRANSTSK. These should be changed as described in the instructions above.



The RFBMTASK Macro for Initiating XPNET Tasks

Each ONE24 program (as described in the last section) has a parameters tab entry which contains four parameters as shown below.

Program Details	
Program Name:	ABRTLIN
Object Code:	\INSIDER.\$SYSTEM.SYSTEM.TACL
Process Name:	\$RXTKA
Enforce:	No

Parameter Assignments	
Parameter Name	Parameter Value
xpnet	~subject~
path	\$cpmn
command	abort
type	line

The '~subject~' parameter will be substituted with either the subject token of the incoming XPNET component EMS event or the XPNET graphic icon description of the Status Monitor screen. This will depend on whether task is started automatically or manually respectively.

The remaining 3 parameters relate to:

- The live / production BASE24 Pathway
- The command to be performed
- The XPNET component type

These parameters at run time, will be fed into the ONE24 RFBMTASK macro below. This TACL macro interacts with NCPCOM using the parameters supplied.

Note: In the case where security is switched on in the XPNET layer (see A Read Only BASE24™ User), the ONE24 macro can be amended to supply an appropriate user to allow the task command to occur (logon command as illustrated).



These parameters at run time, will be fed into the ONE24 RFBMTASK macro below. This TACL macro interacts with NCPCOM using the parameters supplied.

Note: In the case where security is switched on in the XPNET layer (see A Read only BASE24™ User), the ONE24 macro can be amended to supply an appropriate user to allow the task command to occur (logon command as illustrated).

```
?TACL ROUTINE

#FRAME
#PUSH #INFORMAT
#SET #INFORMAT TACL

#push object
#push path
#push command
#push type
#push :var

#set object [#param xpnet]
#set path [#param path]
#set command [#param command]
#set type [#param type]

#append :var logon reflex/invoke, insider
#append :var path [path]
#append :var [command] [type] [object]

ncpcom /inv :var /

#output Parameter is : [object]

#UNFRAME
```

A copy of this macro can be used if requiring wild-carded commands such that the ~subject~ could be substituted in the parameters tab with a wild-carded entry.

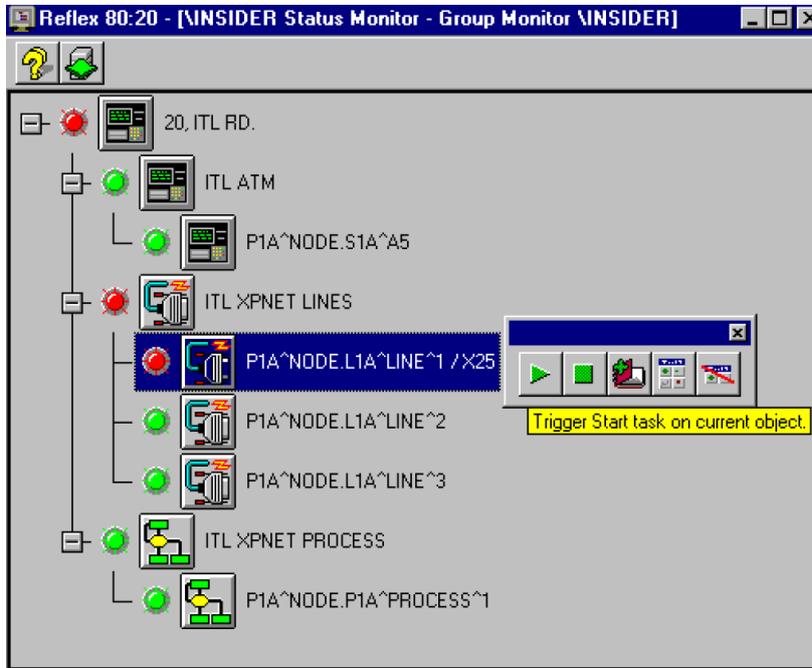
Another approach would be to change a copy of the above macro. With this approach, the NCPCOM command 'UNDER' could be used, e.g. 'start station *, under node p1a^node', 'start station *, under line ~subject~' and so forth.



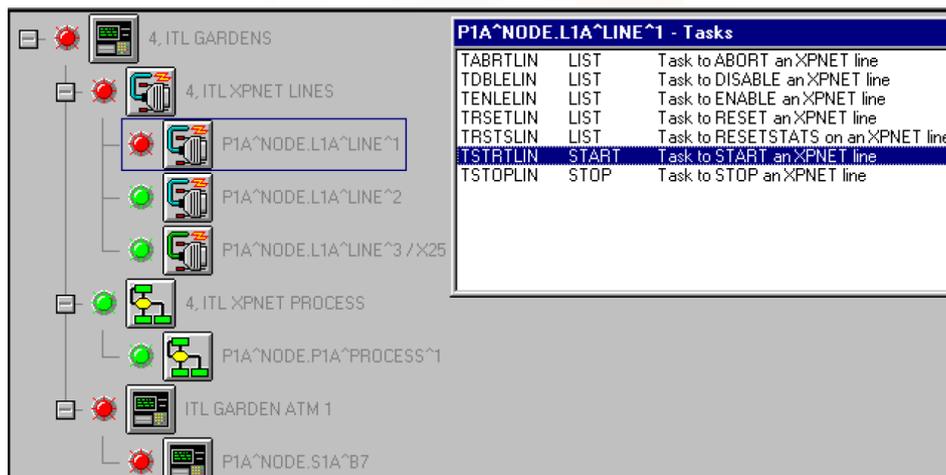
Reflex ONE24

Starting ONE24 XPNET Tasks in Reflex 80:20 Status Monitor

The Status Monitor screens of Reflex 80:20 avoid the need for users to logon to the HPE NonStop platform, get a TACL session and execute XPNET component commands via NCP.COM; this can all be achieved using the TASK functionality of Reflex ONE24™. An example of this can be seen in the following bitmap.



Clicking the arrow icon will initiate the task associated with a line start in the Tasks module discussed in the previous section. The stop button will initiate the stop task associated with a line. Click on the book graphical icon to display all tasks currently set-up, which relate to XPNET lines. This is shown below:

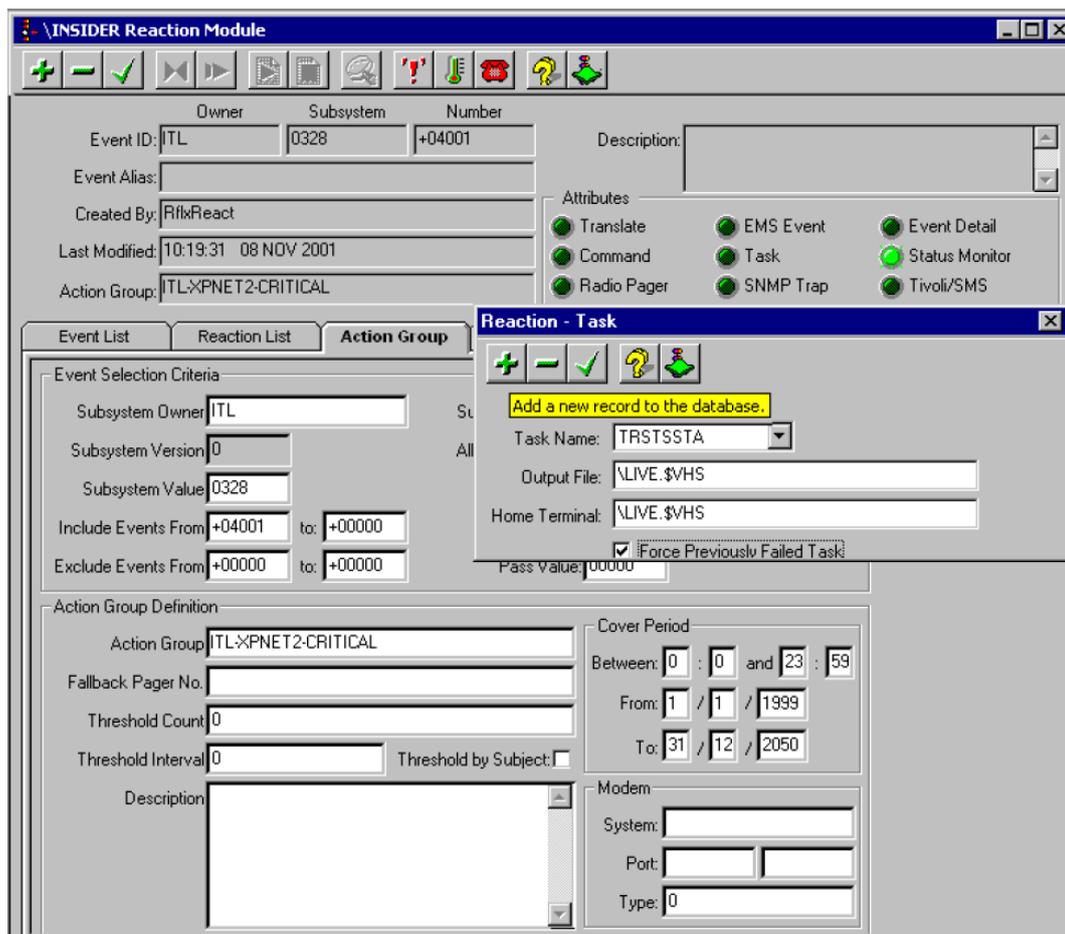


The Reflex 80:20 administrator should have given all Guardian users who require to initiate ONE24 XPNET tasks, the appropriate authority via the Reflex 80:20 GUI to invoke the task. This can be achieved within the task module of Reflex 80:20 under the Task Owners tab of the task window.



Automatic Starting of ONE24 XPNET Tasks

Rather than using the Status Monitor screen discussed in the last section, to invoke tasks, the Reaction module of Reflex 80:20 can be used to kick a task automatically on seeing a critical event. This may be especially useful when a station is stopped or aborted or a line goes down and needs to be restarted immediately. Below is a bitmap of the Reaction module and the task drop down window for associating a task with an event. A remedy for the problem is invoked without the need for operator intervention.

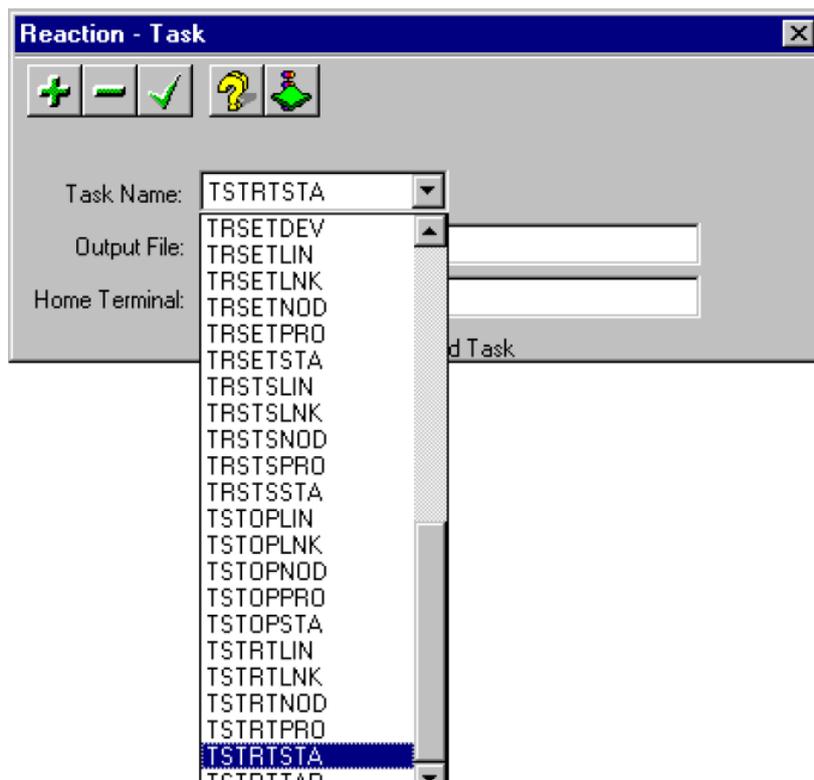


In the above example, a start station task is being associated with an event. On receiving this event from the XPNET layer of BASE24™, Reflex 80:20 will automatically start the station contained in the incoming EMS alert.

In order to add a task to an event or event range, carry out graphical monitoring:

1. Logon to the Reflex 80:20 GUI with a user who has access to Reflex 80:20 set-up facilities, e.g. Reflex ONE24™ Administrator user.
2. Click on the Reaction module on the main toolbar of Reflex 80:20.
3. Maximise the resulting window.
4. Click on the 'Action Group' tab of the maximised window.
5. Enter the SSID of the event(s) you wish to start a task for (**Note:** you can pick the BASE24 event from the previous tab also).
6. Enter the event or event range of the EMS event(s) you wish to monitor if not already listed.

7. Enter an Action Group. This is a free text field used to group a reaction(s) that you wish to occur when the given EMS event(s) is passed to Reflex 80:20. This Action Group can be used again if just wishing to carry out the same reaction, e.g. start a given XPNET station. Action group 'ACI-ITL-XPNET-START' could be used as the action group to start an XPNET station, line or process. This action group is subsequently associated with EMS events relating to XPNET stations in a down state.
8. Enter a desired cover period.
9. Click on the Task green attribute button that is the middle right reaction. The following window will be shown:

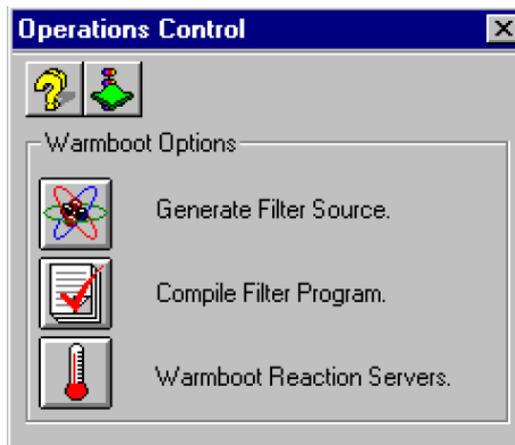


10. Use the drop down list to associate the task you wish to initiate on receiving the event or event range.
11. Enter your preferred output file and home terminal (see previous bitmap for appropriate syntax).
12. Click on the add button '+' on the window to add the record. If you are re-using the same action group in a BASE24 event range, then the details may already exist in which case just click the tick (amend) icon to amend the record. This sets a flag on the action group screen to denote that a reaction has been set-up for the given event or event range.
13. Click on the OK confirmation box and exit the above window.
14. Click on add '+' icon on the Reaction window (or amend - tick) to record the addition or modification.

Carry out these steps for other event or event ranges that you wish to initiate tasks for. When you have completed the new task additions, carry out the following steps:

Note: If just changing a task or field entry rather than an event range value, then just carry out step [10] below. This is because the filter already contains the event you are interested in from a previous generation and compilation of the filter.

1. Click on the '!' icon on the reaction toolbar. The following floating window will be displayed.



2. Click on 'Generate Filter Source' button and wait for confirmation of completion. This generates a filter file to pass your newly added BASE24™ events to the Reflex 80:20 event monitor.
3. Click OK on the confirmation message. Click on the 'Compile Filter Program' and then click OK to the 'compilation started' confirmation message.
4. Logon to the HPE NonStop as the Guardian user who owns the Reflex 80:20 Pathway application and check peruse for successful compilation listings. Alternatively, bring up CONSOLE and check for successful compilation EMS messages generated by Reflex 80:20.
5. Click on the 'Warm-boot Reaction Servers' to allow the event monitor to pick up the new filter for your newly added event ranges.



23. Product Version Utility

REFLEX PRODUCT VERSION

Within the Reflex Windows GUI installation directory, an executable called 'VersionInfo.exe' is supplied.

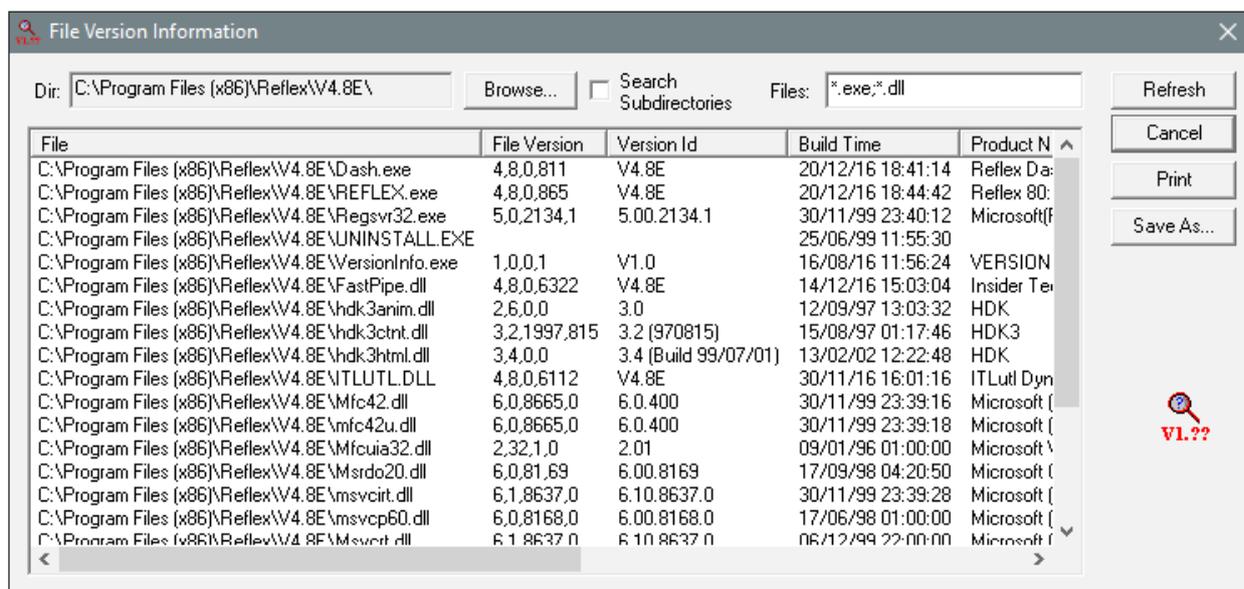
When executed, the results will be provided in a window from where the contents can be saved to a .txt file.

Info: If a customer comes across a problem with the product, Insider Technologies Helpdesk may ask for this file to be run with the contents saved and sent to Insider.

Running the VersionInfo.exe

Navigate to the location of the Reflex.exe executable which provides the Reflex GUI interface, e.g. C:\Program Files (x86)\Reflex\V4.8E.

Within this directory, execute the 'VersionInfo.exe' file to obtain following display:



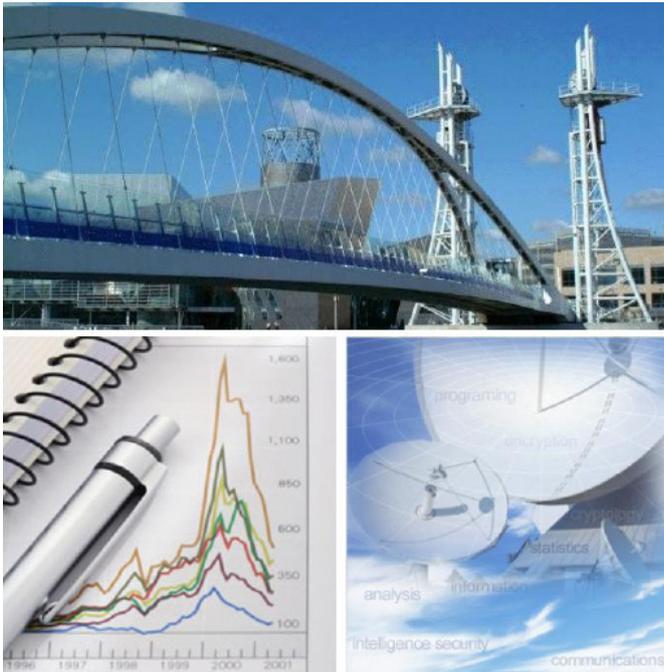
Saving the results

Click on the 'Save As' button and save the .txt file to a suitable location.

If required, email the file to Insider Technologies at support@insidertech.co.uk.



Company Information



Insider Technologies is a UK-based software and services company, operating in the Financial and Messaging markets. It provides Service Management, Tracking, Bespoke Software and Information Mediation solutions. A cross section of our customers include Banking and Financial Services, Telecommunications Providers and Government and Military Institutions.

For details about the full range of products and services available from Insider Technologies Limited, please contact our Product Development Centre at:

Insider Technologies Limited

2 City Approach
 Albert Street
 Eccles
 Manchester
 M30 0BL
 United Kingdom
 Tel: +44 (0)161 876 6606
 Fax: +44 (0)161 868 6666
 E-Mail: support@insidertech.co.uk
 Web Site: <http://www.insidertech.co.uk>



ISV/Software Solutions