

## 2.0 FEMIS Monitoring Tools

The FEMIS decision support system uses a networked, client/server architecture that requires the management of multiple servers, LAN and WAN networks, replicated relational databases, and onpost-to-offpost communications. As such, System Administrators must have a suite of tools at their disposal that will allow them to effectively identify and resolve problems as they arise in the extended FEMIS architecture.

Interruptions in FEMIS services can result from network problems, such as

- Unpredicted events (power failures) may result in server shutdowns
- Critical functions including the Oracle databases may cease to operate
- Communication services provided by other servers (such as Met, DEI, or EMIS) may be inactive.

Distributed processing in FEMIS relies on all EOC servers working properly and the network interconnecting them being reliable. As a result, the system should be monitored regularly to detect any abnormal conditions and to avoid problems.

This section describes the tools provided to assist the FEMIS System Administrator in supporting the extended FEMIS architecture. These tools assist in monitoring the system, notifying the FEMIS System Administrator that a problem exists, and, if applicable, automatic repair of system problems. These tools include the following:

### **AutoRecovery**

AutoRecovery is a UNIX tool, run as a cron job, that monitors the status of the extended FEMIS architecture and can intrusively notify the System Administrator when there is a significant problem. Where applicable, AutoRecovery will identify and fix problems automatically. AutoRecovery provides both a log and notifications on the status of extended FEMIS architecture.

### **UNIX FEMIS Monitor**

The UNIX FEMIS Monitor provides the status of the FEMIS and database UNIX processes. This UNIX FEMIS monitoring subsystem is secure and will not allow outside access to the FEMIS network via the monitoring subsystem.

### **FEMISMon Watcher (FWATCH.EXE)**

FEMISMon Watcher or FWATCH is a PC application that receives notifications from AutoRecovery and graphically displays the status of key FEMIS system components. FWATCH has triggers that will evoke alarms to notify the System Administrator if AutoRecovery detects a significant problem.

### **FEMIS Monitor PC (FMONPC.EXE)**

FEMIS Monitor PC is a PC application that checks FEMIS database replication and displays a graphic representation of replication status.

### **Network Monitor (WS\_WATCH.EXE)**

Network Monitor is a PC application that graphically depicts the status of the FEMIS network.

## **2.1 AutoRecovery**

The FEMIS AutoRecovery system is an integrated system that monitors the extended FEMIS architecture, notifies your System Administrator if significant problems arise, and fixes problems that can be automatically repaired. Figure 2-1 illustrates the flow of the monitoring, notification, and recovery effort.

The AutoRecovery system was developed to reduce the involvement of the FEMIS System Administrator in maintaining the system, aid in the identification of problems when they arise, and keep the system up and operating with fewer interruptions.

With AutoRecovery, the ability to repair and/or restart FEMIS processes has been provided along with increased identification capabilities.

It is recommended that AutoRecovery be installed (see Section 2.12, Installing the FEMIS AutoRecovery System, in the *Installation Guide for FEMIS Version 1.5*) on each of the servers in the FEMIS network. When that has been completed, the status of all processes tracked by AutoRecovery is recorded in a log on each of the servers every time AutoRecovery executes. Whenever an anomalous event occurs (e.g., database shuts down, network crashes) a log entry is made and an E-mail message is sent to all AutoRecovery custodians (See Sections 2.1.3, FEMIS Logging, 2.1.4, FEMIS Log File Archive, and 2.1.5, Sending E-mail) if so configured. Included in the E-mail message is AutoRecovery's attempt at fixing the problem, if AutoRecovery has been configured to correct the specific problem. For example, when the database listener goes down, AutoRecovery attempts to restart it. It reports that it tried to restart it and reports whether or not it successfully did so.

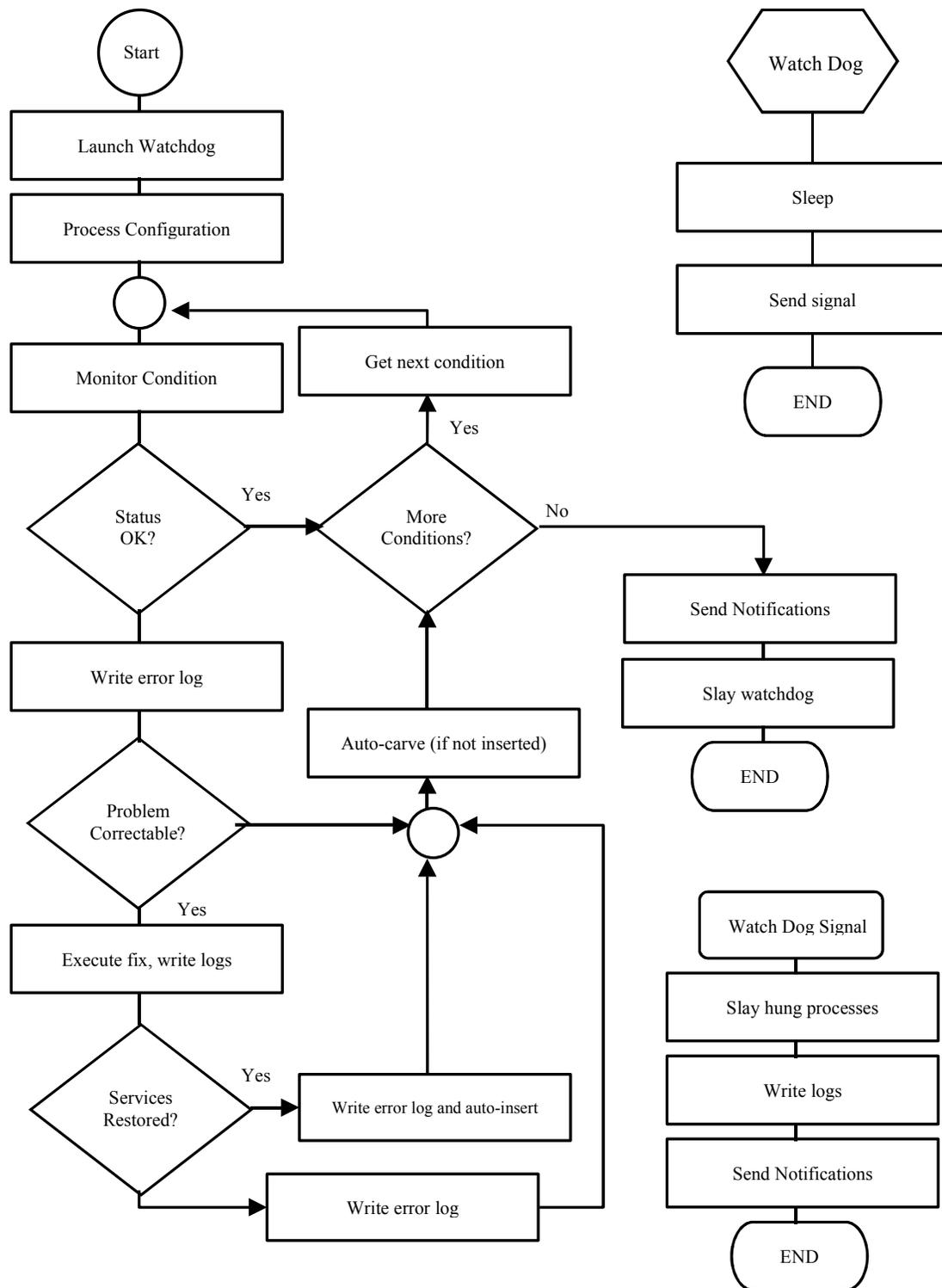
### **2.1.1 How to Execute AutoRecovery**

AutoRecovery is invoked via the cron facility. Entries in the root crontab file automatically invoke AutoRecovery on the following default schedule.

```
Mon thru Fri
7:00a to 6:00p - run AutoRecovery every ten minutes
6:00p to 7:00a - run AutoRecovery every half hour
Sat & Sun - run AutoRecovery hourly
```

To change the run schedule, edit the root crontab (See the man page on *crontab*).

Figure 2.1. AutoRecovery's Integration of Monitoring, Notification, and Recovery



AutoRecovery may also be run manually as a stand-alone utility. This can be done on a single command line as described below. When run manually from an interactive terminal, AutoRecovery is much more verbose about what it is doing and does include some internal (debug) information in its output. Full logging and functionality is maintained when running manually; the only difference between a cron run and manual interactive run is the output to the user when running interactively.

Be aware that running AutoRecovery manually can interfere with a background cron run of AutoRecovery. Collision detection is built into AutoRecovery so that the first process running gets to fully complete while the colliding process will merely complain and exit without doing anything except logging the collision. To avoid collisions, run AutoRecovery manually between its cron cycle (usually 5 minutes after a previous cron run is best when default times have been set). Or, disable the AutoRecovery cron entries by inserting comment characters in front of the appropriate AutoRecovery cron lines in the root crontab, and then uncomment them when the manual runs are complete.

To run AutoRecovery manually in an interactive mode

1. Log in as `root` in a Bourne shell environment (`/bin/sh`)
2. Execute the command

```
# /opt/local/bin/femis_watch
```

## 2.1.2 Messaging Service

AutoRecovery provides FEMIS system status information to the System Administrator in three ways: log files, E-mail message, and through the FEMIS Notification Service. By default the three messaging services are enabled. To disable any of the messaging services, comment out the appropriate line in the file:

```
/opt/local/bin/femis_watch.conf
```

## 2.1.3 FEMIS Logging

AutoRecovery logging is performed through the UNIX syslog message logging facility. `syslogd`, the system message logging daemon, forwards messages sent by AutoRecovery and routes them to their final destination in the `/var/log/femislog` file. In addition, AutoRecovery can be configured with different security levels. The security levels are

```
warn - log only warning messages  
notice - log warning messages and restart messages  
info - log all reported messages
```

By default, AutoRecovery uses the security level `info`.

The default log file name, location, and security levels are configurable in the `/etc/syslog.conf` file. Check for the line:

```
local7.info                /var/log/femislog
```

PNNL recommends that you do not change these default values.

## 2.1.4 FEMIS Log File Archive

Log archiving is performed by the script `/opt/local/bin/logit`. This script is run nightly from the root crontab. The default number of FEMIS log files archived is 7 days and the number of days archived can be configured by changing the value for `NUM_OF_DAYS_TO_ARCHIVE` in the `/opt/local/bin/logit` script.

## 2.1.5 Sending E-mail

When AutoRecovery discovers an error with the FEMIS configuration, it sends a warning message via E-mail. The default AutoRecovery setting sends all E-mail to the root user. You can change the default E-mail recipient or add additional E-mail recipients by editing the `/opt/local/bin/femis_watch.conf` file. Look for the `$Custodian` line and add or change any E-mail addresses between the single quotes. Note a **single space** separates each E-mail address. See the example below for clarification:

```
$Custodian = 'root femis admin@smtp.foo.com';
```

E-mail can be sent to any valid SMTP recipient. For instance, addresses can be to real users, local and remote server aliases, other mail gateways, and to files and/or programs for filtering. For syntax, and mail configurations to support expanded E-mail capability, consult your site's mail server documentation.

## 2.1.6 AutoRecovery “Watchdog” Timeout Parameter

AutoRecovery now has a configurable timeout value. In the event that AutoRecovery were to hang because of problems completing a command or spawned process, it will now force itself to abort processing if it is active for longer than the value defined in

```
$watchdog_timeout = 480;           # 480/60 = 8 minutes
```

where the value is defined in seconds.

**Note:** Setting the timeout value to something greater than the smallest crontab interval is an acceptable practice; however, subsequent AutoRecovery runs will complain about a previous run of AutoRecovery not completing and will exit if a run gets stuck. This will continue until the hung AutoRecovery process times out as defined. PNNL recommends that to avoid confusion, the value **be set less** than the smallest cron interval.

## 2.1.7 AutoRecovery Database Monitoring Parameters

AutoRecovery possesses the capability to monitor the internal Oracle replication processes. It does this by monitoring the status of Oracle jobs. Several parameters are available to tune this capability. The default values for these parameters are hard-coded into the source script so that if they are removed from the configuration file, the monitoring of Oracle jobs will still be able to complete without internal errors. Any values specified in the configuration file over-ride the hard-coded defaults. These parameters are as follows with their default values:

```
$hung_job_time = 35 minutes  
$late_job_time = 30 minutes  
$late_job_fail_count = 8 failures
```

### Definitions

**Hung [Oracle] job:** An Oracle job that has been active (running) for a period longer than it “normally” takes to complete its prescribed function.

**Late [Oracle] job:** An Oracle job that has failed at least once and meets either of the following additional requirements:

1. Its failure count exceeds a nominal value that considers sporadic network anomalies.
2. The time since it was last run (submitted to the job queue) has matched or exceeded a nominal time that considers network anomalies and Oracle job queue processing in the FEMIS environment.

The `$hung_job_time` parameter defines the word “normally” in the hung job definition. If an Oracle job run time exceeds this threshold, it means the job has been active (running) for longer than the defined `$hung_job_time` threshold. Correction is accomplished automatically in AutoRecovery by stopping the Oracle snapshot process handling the job’s function. Oracle then respawns a new process to handle the job.

If the job’s failure count has been incremented, the late jobs can occur in two different situations and do not indicate a stuck snapshot process. No automated corrections are ever done on late jobs until they finally break (16 retries as defined by Oracle). At that point AutoRecovery attempts correction by applying an ordered set of processing rules to repair the situation. Only informational messages are given regarding late jobs. The parameter `$late_job_fail_count` defines the “nominal value” in

condition 1 of the late job definition. The parameter `$late_job_time` defines the “nominal time” of the late job definition in condition 2 above.

Most FEMIS Oracle jobs run in a very short amount of time (usually a few minutes); however, large data transfers on slow or troubled networks may take longer. The default times were selected to be substantially large considering field experience at most EOCs. Alterations of these values are not usually necessary from the defaults but may be done in situations where network data transfers are extremely slow or sporadic.

## 2.1.8 Dynamic Insertion/Deletion of Remote Server in Replication

The database design in FEMIS v1.5 now allows AutoRecovery to dynamically remove and reinsert remote servers in a site configuration “on the fly”. This insertion and deletion primarily affects replicated database data but also affects messages that AutoRecovery sends out. Four parameters in `femis_watch.conf` control how these functions behave. They are

```
$auto_carve = 1;          # Allow auto_carve if defined
$auto_insert = 1;        # Allow auto reinsertion if defined

# Auto Carve threshold - meaningless if $auto_carve is not defined
$sac_threshold = 6;      # Defined in terms of number of AutoRecovery runs
# Auto Insert threshold - meaningless if $auto_insert is not defined
$ai_threshold = 3;       # Defined in terms of number of AutoRecovery runs
```

`auto_carve` and `auto_insert` define whether each respective feature is enabled. This is controlled with a zero (disabled) or one (greater than zero – enabled) value. The threshold values define the number of AutoRecovery runs required **before** the specific action occurs and are defined in terms of AutoRecovery runs. Zero can be valid values for either threshold, although it is not highly recommended to use this value. Generally, the values shown are recommended.

`auto_carve` will remove a host from database push replication if the host is down (not reachable, or experiences listener and/or database process errors) for the number defined in `$sac_threshold` of AutoRecovery runs. For example, on the seventh consecutive failed run with the above set definitions, AutoRecovery will remove the problem server from push replication.

Conversely, as soon as the host becomes available again, on the fourth successful run of good status, it will be reinserted back into the database replication push configuration.

## 2.1.9 AutoRecovery Events/Actions

Every time AutoRecovery is executed (from the root crontab), it goes through the following set of events and actions.

**Process 1**—AutoRecovery monitors for and verifies that certain system processes are running. The monitored processes are defined in `/opt/local/bin/femis_watch.conf` and include as a default

```
inetd      lockd      lpsched    *mountd    smbd
*hclnfsd   *nfsd     rpcbind    sendmail    nmbd
statd      syslogd   utmpd      xntpd/ntpd
```

\* Indicates that the default lower limit is set to 0 on these processes (ignoring their “non-existence”) because Samba is in use at most EOCs and NFS has been disabled for security reasons on depot servers.

The format is as follows: daemon name, minimum number of processes, maximum number of processes, time value, restartable flag, and restart command. The time value field represents a “time to wait” before checking if the restart command worked, and it only applies to the processes that can be restarted by AutoRecovery.

**Note:** To effectively disable process monitoring (which is not recommend), set `min` to 0, and `max` to a high number, such as 500.

**Process 2**—AutoRecovery monitors disk and swap space. AutoRecovery reports to the System Administrator when either disk or swap thresholds have been exceeded. Disk and swap thresholds can be customized for each server. The threshold values are defined in `/opt/local/bin/femis_watch.conf`. To change the threshold values for disks, check the “@disks = (” section. To change the threshold for swap space, check the `$swap =` section.

**Process 3**—AutoRecovery checks connectivity only for hosts configured in the `/opt/local/bin/femis_watch.conf` file. To configure AutoRecovery for remote connectivity checks, look for the following line.

```
@network = ( 'system1', 'system2' )
```

Change the system names to reflect the name of your system (optional for NxM – but required for AutoRecovery to work in an Nx1 configuration. The term `localhost` may also be used for the local host name) and all remote systems in your FEMIS configuration. Add as many entries as necessary, making sure the system names are quoted and separated by commas.

During the connectivity check, if a host is not reachable, it is added to the `auto-carve` list if `auto-carve` is enabled, and the `auto-carve` threshold has been exceeded for this site. The problem host will not actually get removed unless local Oracle connectivity is accomplished (see Process 6 Step 12).

**Process 4**—AutoRecovery monitors and, by default, attempts to restart the following FEMIS processes:

```
femisevent : FEMIS event notification
femisdei   : FEMIS Data Exchange Interface (only if onpost)
```

If these FEMIS processes should not be restarted, comment out the following lines in the `/opt/local/bin/femis_watch.conf` file. The DEI restart command only applies to depot servers. When running on an off-post server, DEI is ignored altogether by AutoRecovery:

```
$femis_event_restart_command = 'su - femis -c  
"$ENV{$FEMIS_HOME}/bin/stopnotify;  
$ENV{$FEMIS_HOME}/bin/startnotify "';  
  
$femis_dei_restart_command = 'su - femis -c  
"$ENV{$FEMIS_HOME}/bin/femisdei" ';
```

**Process 5**—AutoRecovery checks the following Oracle Processes and attempts to restart the Oracle Listener (`tnslsnr`) process if it is not running.

```
ora_ckpt_fi#      ora_reco_fi#      ora_smon_fi#      ora_arch#_fi#  
ora_dbwr#_fi#    ora_pmon_fi#    ora_lgwr_fi#    ora_snp#_fi#
```

The monitored processes are defined in `/opt/local/bin/femis_watch.conf`. The format is as follows: daemon name, minimum number of processes, maximum number of processes, status flag, restartable flag, and restart command. The status flag represents a “time to wait” before checking if the restart command worked. The status flag applies only to the Oracle Listener, since it is the only Oracle process with a restart command.

**Process 6**—AutoRecovery monitors Oracle’s ability to login to the local Oracle database. If successful, it:

1. Reprocesses the site configuration information based on Oracle Replication push list.
2. Checks the percentage full for Oracle tablespaces.

To configure the reporting threshold of the Oracle tablespaces, look for the `%oracle_tablespaces =` line in the `/opt/local/bin/femis_watch.conf` file. You can adjust the reporting threshold by changing the value for the Oracle tablespace of interest. For example, to increase the Oracle `FINDEX` tablespace threshold from 85% to 90%, change

```
FINDEX => 85, to FINDEX => 90,
```

The default threshold for all Oracle tablespaces is 85%, except `SYSTEM` and `TOOLS` which are set to 100% because `Auto-Extend` is set on these tables.

3. Checks for hung and late Oracle jobs. See definitions in Section 2.1.7, AutoRecovery Database Monitoring Parameters.

4. Checks for broken Oracle jobs.

Broken Oracle jobs are those internal Oracle jobs that have failed 16 times. Oracle attempts retries on any job that fails to execute successfully up to 16 times. If on the 16<sup>th</sup> retry the job fails again, it is considered “broken” and is not resubmitted to the Oracle job queue from that point forward. Jobs can break when network connectivity to remote hosts is disabled for a period of time. This time varies with FEMIS client use that submits requests to the extended FEMIS system for replicated data. AutoRecovery will attempt to resubmit the broken job to the Oracle job queue if EOC conditions are good; thereby allowing the broken job to complete in most cases.

5. Checks the status of the remote database listeners if the site configuration includes remote databases.

6. Checks remote systems for Oracle and FEMIS process status to determine remote database connectivity if the site configuration includes remote databases.

AutoRecovery now has the capability to determine if a remote system is “good” or “bad” based on the processes running on that remote system. There is a new section in the `femis_watch.conf` file that defines thresholds and values of processes on remote systems for determining if a remote system is good or not. The definition table is called `@femismon_proc`. This table must not have the entry order changed or any entries removed. Ignoring a particular process altogether is accomplished with an `ignore_flag` that is set or cleared in the array definition. The table columns are defined as follows:

```
<descriptive daemon name>, ignore_flag, min, max
```

To ignore an entry, set the `ignore_flag` to not equal zero.

For example, `[ "OraArch", 1, 1, 1 ]`, defines the eighth row in the `@femismon_proc` array. The `ignore_flag` is greater than zero, so this value will be ignored when determining if a remote server is good or not. If it were not ignored, an error would be generated if there were less than or greater than one remote `OraArch` processes, and the remote server would not have been considered available. The string `OraArch` has no bearing in this array on how the remote search is conducted. It is merely just a descriptive string name for output in the error message.

7. Determines `auto-insert` and `auto-carve` lists if the site configuration includes remote databases. These lists are based on whether Process 3 and Steps 5 and 6 in this process were successful.

8. If no errors in were detected Processes 1 and 5 and Step 1 in this process and at least one remote host is available, then AutoRecovery attempts to repair hung Oracle jobs by stopping the affected Oracle snapshot processes (UNIX processes). Check if the hung job was corrected after waiting 60 seconds.

9. Monitors the FEMIS database replication if the configuration is other than an Nx1.

There are two Oracle mechanisms that make up replication. The mechanisms are `push_local`, which sends data changes to remote servers, and `update_remote`, which receives and processes data change requests. AutoRecovery will attempt to fix these replication components, if all other AutoRecovery system checks complete successfully. Otherwise, an error notification is generated.

10. If no errors were detected in Processes 1 and 5 and Steps 5 and 6 of this process and replication was configured; but either the remote replication push mechanism failed or the database listener (update) mechanism failed; and at least one remote host is available, then AutoRecovery attempts to repair either mechanism or both depending on the detected failure.
11. If corrections were attempted in Step 10, then AutoRecovery rechecks for broken Oracle jobs.
12. If the site configuration includes remote databases, then `auto-insert` and/or `auto-carve` hosts are based on the lists built throughout the run. Verify that the insertions and/or deletions took place.
13. If no errors were detected in Processes 1 and 5 and Step 1 in this process and at least one remote host is available, AutoRecovery attempts to repair broken Oracle jobs. Verify that broken jobs were corrected.
14. (This step conditionally follows Step 4 above.) If the EOC does not include any remote databases (Nx1 configuration), and if no errors were detected in Processes 1 and 5 and Step 1 in this process, AutoRecovery attempts to repair hung Oracle jobs by stopping the affected Oracle snapshot processes (UNIX processes). After waiting 60 seconds, verify the hung job was corrected.
15. (This step follows Step 14 which conditionally follows Step 4 above.) If the EOC does not include any remote databases (Nx1 configuration), and if no errors were detected in Processes 1 and 5 and Step 1 in this process, then AutoRecovery attempts to repair broken Oracle jobs. Verify that broken jobs were corrected.

Upon completion of monitoring for all the above events, AutoRecovery then

- Sends the FEMIS notifications to be picked up by the PC.
- Saves AutoRecovery statistical information.
- E-mails the results, if warranted, to AutoRecovery custodians.
- Logs the results to the `/var/log/femislog` file.

## 2.1.10 Detecting System Problems with AutoRecovery

AutoRecovery attempts to identify and fix, when possible, the root cause of a problem. For example, the AutoRecovery software running onpost identifies that a remote database listener is not running. It notifies the onpost System Administrator of the situation but cannot restart the remote listener. If `auto-carve` is enabled and then if the remote listener continues to remain down on subsequent AutoRecovery runs, a message is sent to the onpost System Administrator indicating the problem is continuing until the `auto-carve` threshold is exceeded. Once exceeded, the remote site where the listener has been down is removed from the onpost replication push mechanism to protect the onpost Oracle job queue. A message indicating the remote problem with the listener, in addition to the removal of the remote host from the push list, is sent to the onpost System Administrator. The reverse is true once the remote listener is re-enabled and is able to be connected to by the onpost server and `auto-insert` is enabled.

Other situations are detected and corrected as configured in the configuration file. These are typically local FEMIS/system process checks and process restarts.

## 2.1.11 Using AutoRecovery

The System Administrator can monitor progress of the FEMIS AutoRecovery by monitoring the log file. To monitor progress on the server console, use the following command:

```
tail -f /var/log/femislog.
```

A typical (no problems found) report will show a set of messages similar to the following:

```
May 23 00:30:02 somehost.outthere.mil /opt/local/bin/femis_watch: **** Beginning FEMIS Check
****
May 23 00:30:03 somehost.outthere.mil /opt/local/bin/femis_watch: System processes are running
May 23 00:30:03 somehost.outthere.mil /opt/local/bin/femis_watch: Swap space status is okay
May 23 00:30:03 somehost.outthere.mil /opt/local/bin/femis_watch: Disk space status is okay
May 23 00:30:03 somehost.outthere.mil /opt/local/bin/femis_watch: Network connections are
reachable
May 23 00:30:03 somehost.outthere.mil /opt/local/bin/femis_watch: FEMIS event is running
May 23 00:30:03 somehost.outthere.mil /opt/local/bin/femis_watch: Oracle processes are running
May 23 00:30:04 somehost.outthere.mil /opt/local/bin/femis_watch: Local listener is up
May 23 00:30:10 somehost.outthere.mil /opt/local/bin/femis_watch: Connected to local Oracle
May 23 00:30:10 somehost.outthere.mil /opt/local/bin/femis_watch: Oracle tablespaces are within
limits
May 23 00:30:11 somehost.outthere.mil /opt/local/bin/femis_watch: Bi-directional replication is
running
May 23 00:30:11 somehost.outthere.mil /opt/local/bin/femis_watch: Listener fil is up
May 23 00:30:15 somehost.outthere.mil /opt/local/bin/femis_watch: Oracle database anad is
available
May 23 00:30:15 somehost.outthere.mil /opt/local/bin/femis_watch: Oracle database aema is
available
May 23 00:30:15 somehost.outthere.mil /opt/local/bin/femis_watch: Oracle database ctal is
available
May 23 00:30:15 somehost.outthere.mil /opt/local/bin/femis_watch: Oracle database cstc is
available
```

```
May 23 00:30:19 somehost.outthere.mil /opt/local/bin/femis_watch: FEMIS notification was sent
May 23 00:30:19 somehost.outthere.mil /opt/local/bin/femis_watch: **** FEMIS Check Complete
****
```

When problems are detected, the `/var/log/femislog` file will have error messages similar to the following:

```
May 23 21:53:42 somehost.outthere.mil ./femis_watch: **** Beginning FEMIS Check ****
May 23 21:53:42 somehost.outthere.mil ./femis_watch: System processes are running
May 23 21:53:42 somehost.outthere.mil ./femis_watch: Swap space status is okay
May 23 21:53:42 somehost.outthere.mil ./femis_watch: Disk space status is okay
May 23 21:53:42 somehost.outthere.mil ./femis_watch: Network connections are reachable
May 23 21:53:43 somehost.outthere.mil ./femis_watch: FEMIS dei processes are running
May 23 21:53:43 somehost.outthere.mil ./femis_watch: FEMIS event is running
May 23 21:53:43 somehost.outthere.mil ./femis_watch: Local listener is up
May 23 21:53:43 somehost.outthere.mil ./femis_watch: Connected to local Oracle
May 23 21:53:44 somehost.outthere.mil ./femis_watch: Oracle tablespaces are within limits
May 23 21:53:44 somehost.outthere.mil ./femis_watch: Bi-directional replication is running
May 23 21:53:46 somehost.outthere.mil ./femis_watch: Oracle database ccal is available
May 23 21:53:46 somehost.outthere.mil ./femis_watch: Oracle database ccla is available
May 23 21:53:46 somehost.outthere.mil ./femis_watch: Oracle database ceto is available
May 23 21:53:46 somehost.outthere.mil ./femis_watch: Oracle database ccle is available
May 23 21:54:09 somehost.outthere.mil ./femis_watch: FEMIS notification was sent
May 23 21:54:10 somehost.outthere.mil ./femis_watch: There are 0 ora_arc[0-9]+_fi daemons. The
range is set from 1 to 1.
May 23 21:54:10 somehost.outthere.mil ./femis_watch: Listener fi2 is down
May 23 21:54:10 somehost.outthere.mil ./femis_watch: fi2 (otherhost) is being removed from
replication push because of errors.
May 23 21:54:10 somehost.outthere.mil ./femis_watch: **** FEMIS Check Complete ****
```

In addition to the `/var/log/femislog` file, the AutoRecovery custodians will receive E-mail. Examples of E-mail messages are as follows:

For the above bad case...

```
There are 0 ora_arc[0-9]+_fi daemons. The range is set from 1 to 1.
Listener fi2 is down
```

```
fi2 (otherhost) is being removed from replication push because of errors.
```

AutoRecovery works in conjunction with the PC application FEMISMon Watcher (FWATCH). As AutoRecovery examines that status of the FEMIS architecture, it not only sends messages to the log as described above, but it also sends messages to the FEMIS Notification Services. These notifications are picked up by FWATCH. FWATCH will then give a graphical view of the status of key FEMIS components for the site. FWATCH can be set to sound alarms that will intrusively interrupt the System Administrator or whoever is logged onto the PC where FWATCH is running.

**Note:** FWATCH is currently designed to reflect notification messages based on snapshot status. Snapshot status is no longer directly checked in AutoRecovery in FEMIS v1.5, so the “snapshot status” event messages currently generated by AutoRecovery are based on other system criteria (not actual snapshot time/updates).

To troubleshoot AutoRecovery error messages or other problems, see the AutoRecovery help topics by selecting `Help` → `Troubleshooting Guide` on the Workbench or opening the `TSG.HLP` file in your FEMIS directory.

## 2.2 UNIX FEMIS Monitor

The UNIX FEMIS Monitor provides the status of the FEMIS and database UNIX processes. This UNIX FEMIS monitoring subsystem is secure and will not allow outside access to the FEMIS network via the monitoring subsystem. Significant effort was made to ensure that only a privileged FEMIS System Administrator could start, halt, or otherwise alter the execution of the FEMIS support applications.

### 2.2.1 Background

The `FEMISMON` tool was the first automated monitoring tool provided with FEMIS. Its intended use now is to complement the AutoRecovery application and is to be run on an “as needed” basis. Also, AutoRecovery invokes the FEMIS Monitor Daemon (`femismond`) to obtain counts of various process names.

`femismond` counts processes of various types using one of two methods. First, `femismond` can invoke a series of `ps` and `grep/egrep` commands and finally using `grep -c` to send a number on standard output. Second, `femismond` can invoke a script to perform actions more complicated than simple `ps` and `grep`. Typically, the scripts invoke an `awk` command to perform some convoluted counting operations.

### 2.2.2 UNIX FEMIS Monitor Configuration File

The FEMIS Monitor configuration file is copied to `/home/femis/etc` as part of the FEMIS installation process. This configuration file (`cmdserv.conf`) contains instructions to the command server daemon program. The contents of this configuration file: 1) define the path for two shell commands, `ps` and `egrep`, and 2) define the process names of five processes.

The keyword, `solaris`, indicates conditions for the Sun Solaris operating system. The keyword, `allhost`, indicates a command for any and all operating systems. Other platform dependent keywords include `aix` and `linux`.

Command name/path lines found in the FEMIS Monitor configuration files are

```
Command platform PS path
Command platform EGREP path
Command platform SH path
Command platform EGREP path
```

Process name/path lines found in the FEMIS Monitor configuration file are

```
Femisd process femisd
FemdCmd process femisd -- 9015
FemdEve process femisd -- 902
FemdMon process femisd -- 9040
Fevent process femis_event
Fcommand process cmdservd
Fdei process femisdei
OracleFi process oraclefi
OraCkpt process ora_ckpt_
OraLgwr process ora_lgwr_
OraPmon process ora_pmon_
OraReco process ora_reco_
OraSmon process ora_smon_
OraArch process +++
OraDbwr process +++
OraSnap process +++
```

Script name/path lines found in the FEMIS Monitor configuration file are (paths are relative to the FEMIS home directory /<device name>/home/femis/).

```
Femisd script bin/femismon-ps-1
FemdCmd script bin/femismon-ps-3
FemdEve script bin/femismon-ps-3
FemdMon script bin/femismon-ps-3
Fevent script bin/femismon-ps-1
Fcommand script bin/femismon-ps-1
Fdei script bin/femismon-ps-1
OracleFi script bin/femismon-ps-2
OraCkpt script bin/femismon-ps-2
OraLgwr script bin/femismon-ps-2
OraPmon script bin/femismon-ps-2
OraReco script bin/femismon-ps-2
OraSmon script bin/femismon-ps-2
OraArch script bin/femismon-ps-OraArch
OraDbwr script bin/femismon-ps-OraDbwr
OraSnap script bin/femismon-ps-OraSnap
```

All processes counted by femismond now utilize scripts.

The ps command arguments found in the FEMIS Monitor configuration file are (these are the options passed to the ps command in the scripts.)

```
Femisd psargs -o comm
FemdCmd psargs -o args
FemdEve psargs -o args
FemdMon psargs -o args
Fevent psargs -o comm
Fcommand psargs -o comm
Fdei psargs -o comm
OracleFi psargs -o args
OraCkpt psargs -o comm
```

```
OraLgwr psargs -o comm
OraPmon psargs -o comm
OraReco psargs -o comm
OraSmon psargs -o comm.
OraArch psargs -o comm
OraDbwr psargs -o comm
OraSnap psargs -o comm
```

An extra `grep` is performed in some of the scripts. Lines `exgrep` define the strings searched for by the extra `grep`. An asterisk (\*) denotes no extra `grep`. Three plus signs (+++) denotes undefined.

```
Femisd exgrep *
FemdCmd exgrep *
FemdEve exgrep *
FemdMon exgrep *
Fevent exgrep *
Fcommand exgrep *
Fdei exgrep *
OracleFi exgrep LOCAL=no
OraCkpt exgrep *
OraLgwr exgrep *
OraPmon exgrep *
OraReco exgrep *
OraSmon exgrep *
OraArch exgrep +++
OraDbwr exgrep +++
OraSnap exgrep +++
```

### 2.2.3 UNIX FEMIS Monitor Scripts

Scripts are now utilized to perform process counting, rather than a string of `ps` and `grep`s. There are three standard scripts, and all are located in `/home/femis/bin/`. They are `femismon-ps-1`, `femismon-ps-2`, and `femismon-ps-3`. Also in `/home/femis/bin`, there are several non-standard scripts. They are `femismon-ps-Fcommand`, `femismon-ps-Fdei`, `femismon-ps-Femisd`, `femismon-ps-Fevent`, `femismon-ps-OraDbwr`, and `femismon-ps-OraSnap`. Only two of these scripts are currently in use: `OraDbwr` and `OraSnap`. The others are not being used. The ones not in use are there in case FEMIS is ported to a platform where the standard scripts will not work or return the correct process count. In that case, the non-standard scripts for `Fcommand`, `Fdei`, `Femisd`, and `Fevent` can be modified as needed.

Shell commands for `ps`, `awk`, and `grep/egrep` are passed to the scripts in environment variables – `FM_PS`, `FM_AWK`, and `FM_GREP` – for that purpose. These environments are constructed by combining `Commands` and `psargs` above. For example, `FM_PS` might contain `/bin/ps -ef -o comm`.

There are four arguments to the standard scripts `$1`, `$2`, `$3`, and `$4` as follows: `$1` is the extra string to `grep` for (i.e. `LOCAL=no`), `$2` is the file name string to `grep` for, `$3` is the first argument of `FILE`, and `$4` is the second argument to `FILE`.

Standard script #1 performs `PS | AWK | GREP $XGREP | GREP -c $LEN $FILE`. The AWK program outputs the first non-path file item plus its length. Script #1 is used for counting `Fcommand`, `Femisd`, `Fevent`, and `Fdei`.

Standard script #2 performs `PS | AWK | GREP $XGREP | GREP -c "1 $FILE $FILE"`. The AWK program outputs the non-path file item twice plus its position. Script #2 is used for counting OracleFi processes.

Standard script #3 performs `PS | AWK | GREP $XGREP | GREP $2 $3 $4 | GREP -v grep | GREP -cv TheScriptName`. Script #3 is used for counting some of the OraXxxx processes.

Scripts `femismon-ps-OraArch`, `femismon-ps-OraDbwr`, and `femismon-ps-OraSnap` are custom non-standard scripts for those situations. Generally, nothing is passed into the non-standard scripts. They must do everything internally.

## 2.2.4 UNIX FEMIS Monitor Daemon Program

The FEMIS Monitor daemon program is copied to `/home/femis/bin` as part of the FEMIS installation process. This executable (`femismond`) is invoked whenever a socket connection request comes in on service port 9040, or whenever protocol 9040 has been parsed by the FEMIS contact daemon (`femisd`) on service port 1776.

The FEMIS Monitor daemon performs the following tasks: 1) reads the configuration file; 2) uses the `ps`, `awk`, and `grep` commands to count the number of certain processes; 3) counts `femis_event`, `cmdservd`, `femisdei`, `oracle`, and `femisd` processes; and 4) then sends process count information to the client program at the other end of the socket connection, i.e., `femismon`.

## 2.2.5 UNIX FEMIS Monitor Client Program

The FEMIS Monitor client program is copied to `/home/femis/bin` as part of the FEMIS installation process. This executable (`femismon`) is the FEMIS monitor client program. It communicates with the UNIX FEMIS Monitor Daemon.

Usage is: `femismon [-v] [-a] [-u] [-esdofDB] [port] host`

Option `-a` invokes all options `-esdof`. Option `-v` reports version identifier. Option `-u` forces use of unregistered service port (9040). Option `-D` turns on diagnostic messages. Option `-B` instructs `femismon` to report in brief format. The port is the service port number (default = 9040). The host is the remote computer name.

## 2.3 FEMISMon Watcher (FWATCH.EXE)

The FEMISMon Watcher or FWATCH (FWATCH.EXE) program is a PC program that watches for notifications sent by the UNIX `AutoRecovery` and/or `femismon` programs. This program shows the status of all the databases, replication snapshots, and other information for each server. It is designed to graphically notify you of a problem. For FWATCH.EXE to provide valid results, `femis_event` and either `AutoRecovery` or `femismon` **must be running** on the server. You will only be notified if errors occur. To install FEMISMon Watcher, select System Tools on the Custom Setup window during the PC installation.

### 2.3.1 Notification Status

All of the servers for the site are listed across the top of the spreadsheet. The server containing your default EOC will be in uppercase. Down the left of the spreadsheet are all the EOC databases for the site and rows for UNIX server status (SRV), `femisdei` (DEI) status, and `femis_event` (FEV) status.

As this program gets notifications, it fills in cells on the spreadsheet.

If the item is running correctly, OK is displayed in the cell, and it is colored green.

If the item is not running correctly, the cell is colored either yellow or red (depending on the severity of the error) and contains the text which indicates the error:

```
ERR:DB - if the database is down
ERR:SNP - if the snapshots are broken
ERR:DEI - if femisdei is not running
ERR:FEV - if femis_event is not running
ERR:SRV - if the server may be down.
```

Clicking on a cell will indicate when the last message for that cell was received and how many minutes ago it was received.

### 2.3.2 Menu Options

The colors will fade to white as the time since a message was received increases to indicate that the information may be out of date. This feature can be turned on or off using the `Fade Colors` under `Options` menu.

As messages are received, the program can beep, flash the window, or display a message to the user. You can choose the notification methods under the `Notifications` menu. Also under the `Notifications` menu, you can choose to be notified about messages from all EOCs and servers or just your own EOC and server.

**Note:** It is highly recommended that you **do not use** the message option for replication errors because many messages may appear if there are replication problems from one server.

If you have indicated that you want to be notified by a flashing window, the window will flash until you click the `Stop Flashing` menu item under the `Options` menu.

The `Clear Spreadsheet` option under the `Options` menu allows you to blank out the current view.

The `Show Messages` menu under the `Options` menu will either show or hide a list box of all the actual messages received from the server.

All the selections for the menu items are stored on the PC in the `FEMIS.INI` file so they will be the same the next time you start the program.

## 2.4 FEMIS Monitor PC (FMONPC.EXE)

The FEMIS Monitor PC tool (`FMONPC.EXE`) checks the FEMIS database replication status and does not require any user privileges to run (does not ask for a user login). To install FEMIS Monitor PC, select `System Tools` on the `Custom Setup` window during the PC installation.

### 2.4.1 Replication Status

The basic operation is to start the program, then click the `Check All Replication` button. The program then connects to all databases, writes a record into the `REPLICATION_TEST` replicated table, and continues to check all the databases to see if the records from the others have been replicated.

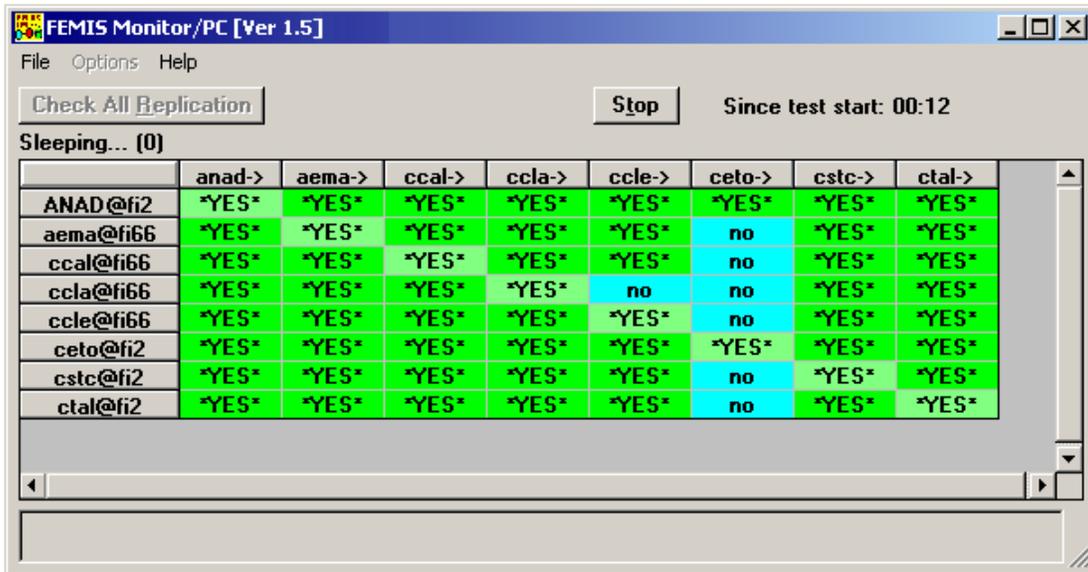
A spreadsheet of the results is shown on the FEMIS Monitor/PC window (See Figure 2-2).

- The headers across the top are `From Database XXX` (Row Header).
- The headers down the left side are `To Database XXX` (Column Header).
- The cells contains the text `*YES*` if the data has replicated from one database to the other.
- The cells contains the text `no` if the data has not appeared yet.
- If the program cannot connect to a database, `Error` is shown for the entire row for that database.
- The spreadsheet should be read `Data from database` (Column Header) has/has not replicated to database (Row Header).

- Any errors are listed in a scrollable box at the bottom of the window.

**Note:** If any of the diagonal items are `no`, then the database **has not** replicated to itself.

Figure 2.2. FEMIS Monitor/PC Window



After each check of all databases, the utility will pause for a number of seconds to reduce its network and server usage. (The number of seconds to pause may be set under the `Options` menu. The default is 10 seconds.)

This utility will stop checking:

- If all the databases have replicated and everything says `*YES*`

Or

- If a number of minutes has passed since it started to check. (Under the `Options` menu, set the number of minutes to keep checking. The default is 10 minutes.)

## 2.4.2 Options Menu

The following describes menu options.

- Show Replication Timing (approximate) – displays the approximate time it took for the data at one EOC to be replicated to another EOC, instead of putting `*YES*` in the spreadsheet. To enable this option, highlight it, and a check mark indicates it has been enabled. Replication times displayed are the times when the data was first found to be replicated at the remote EOC by `FMONPC`. It is not the time the Oracle database actually performed the replication. If you need

a more granular time measurement, configure the `Pause between checks` option to check at more frequent intervals.

- `Stop Checking Replication` – sets the length of time to continue checking. Select either 5, 10, or 30 minutes.
- `Pause Between Checks` – sets the pause length between checks. Select 5, 10, 20, or 60 seconds.
- `Check Replication To` and `Check Replication From` – bring up a list so you can select one row or one column to see if replication is working to or from a single EOC.
- `Clear Spreadsheet` – clears all entries on the spreadsheet.
- `Cleanup All DBs` – cleans up the information used by `FMONPC` in all databases in case there were network, server, database, or PC problems while `FMONPC` was running.

**Note:** Using this option while another PC is running `FMONPC` can cause items in the spreadsheet to change, such as the whole spreadsheet will change to display `no`. If `no` appears from an EOC to itself when `YES` was previously displayed, then someone else probably used this option.

- `Clear Errors` – clears the list box of errors at the bottom of the window.

Normally, the monitoring tool is installed only on the System Administrator's PC. It may be installed on a few selected PCs but should not be installed on every PC.

Figure 2-2 illustrates that most of the database replication is working except that the `CETO` database has not replicated to any other databases (except itself) and the `CCLC` database has not replicated to the `CCLA` database.

## 2.5 Network Monitor (`WS_WATCH.EXE`)

The Network Monitor tool graphically shows the network status by coloring icons that indicate the status. This tool should be installed on one PC because it uses network resources when it is running. The PC will periodically send a message (ping) to a set of computers, servers, routers, or other network equipment to see if they respond. The graphical status indicates whether or not the network equipment responded to the ping from this single PC. To install Network Monitor, select System Tools on the Custom Setup window during the PC installation.

**Note:** The status may not mean that the entire network is up and working correctly, just that some route exists from this PC to the remote equipment. It does not indicate that other points on the network can connect to each other or that the performance of the network may be unacceptably slow.

**Note:** To reduce the network resources used, **do not change** the time between checks to less than a minute. Longer durations (e.g., 5, 30, 60 minutes) between checks may be acceptable, depending on the reliability of your network.

For additional information on setting up and configuring the Network Monitor tool (`ws_watch`), click on Help on the menu bar.

This tool is freeware and distributed with FEMIS as a useful tool. Any comments or suggestions should be directed to the author of `ws_watch`.