

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 and utilities 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, such as power failures resulting 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 not be active.

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 avoid problems.

This section describes the tools and utilities 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

A UNIX tool, run as a cron job, that monitors the status of the extended FEMIS system and can intrusively notify the System Administrator when there is a significant problem. Where applicable, AutoRecovery will identify problems that can be automatically fixed and fix them. AutoRecovery will provide 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 servers and databases. 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)

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)

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

Network Monitor (WS_WATCH.EXE)

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 2.6, FEMIS AutoRecovery System Description and Installation, in the *FEMIS Installation Guide*) 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.

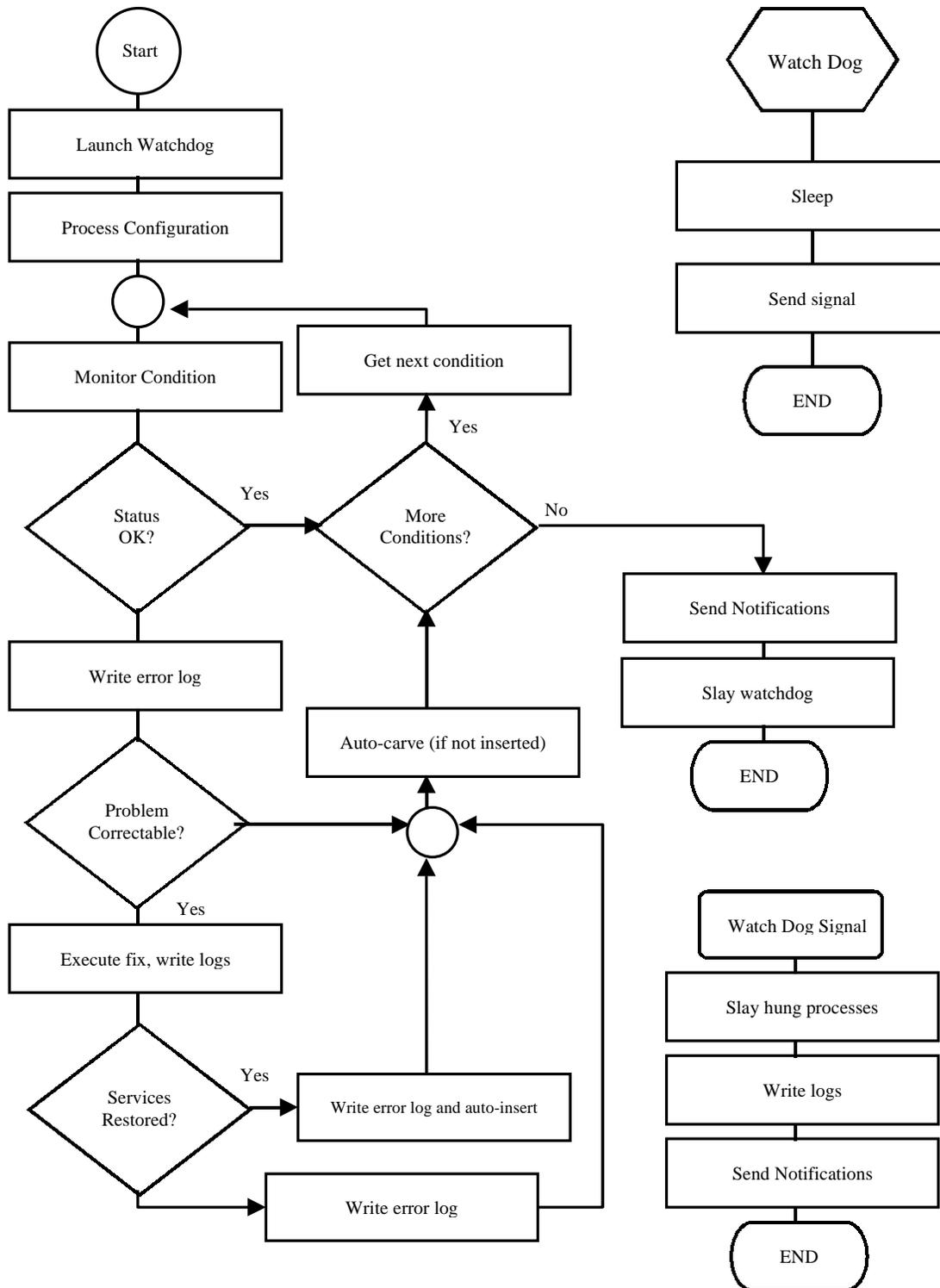
2.1.1 How to Execute AutoRecovery

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



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. 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 Dynamic Insertion/Deletion of Remote Server in Replication

The database design in FEMIS v1.4.7 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
$ac_threshold = 5;  # Defined in terms of number of AutoRecovery runs
# Auto Insert threshold - meaningless if $auto_insert is not defined
$ai_threshold = 1;  # 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 `$ac_threshold` of AutoRecovery runs. For example, on the sixth 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 second successful run of good status, it will be reinserted back into the database replication push configuration.

2.1.8 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	mounted
hclnfsd	nfsd	rpcbind	sendmail
statd	syslogd	utmpd	xntpd/ntpd

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 8).

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:

```
$femis_event_restart_command = 'su - femis -c "$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. Determines 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 SYSTEM tablespace threshold from 85% to 90%, change

```
SYSTEM => 85, to SYSTEM => 90,
```

The default threshold for all Oracle tablespaces is 85%.

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

There are two Oracle components that make up replication. The components 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.

4. Checks the status of the remote database listeners.
5. Checks remote systems for Oracle and FEMIS process status to determine remote database connectivity.

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, nor 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 field to `!= 0`.

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.

6. Determines auto-insert and auto-carve lists based on whether the above Process 3 and Process 6 Steps 4 and 5 were successful.
7. If no errors in Processes 1 and 5 and Process 6 Steps 4 and 5 were detected, and replication was configured; but either the remote replication push was disabled or the database listener (update) mechanism was disabled; and at least one remote host is available, attempt repairs on either mechanism or both depending on the detected failure.
8. auto-insert and/or auto-carve hosts based on the lists built throughout the run.

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.

2.1.9 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.

2.1.10 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 fi1 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 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 v1.4.7, so the “snapshot status” event messages currently generated by AutoRecovery are based on other system criteria (not actual snapshot time/updates).

2.1.11 AutoRecovery Error Messages

This section includes AutoRecovery error messages, the problem that caused the error message to display, and possible solutions to resolve the error message.

Table 2.1. AutoRecovery Error Messages

Error Message	Problem	Solution
AutoRecovery attempted to run during system init change: ...	AutoRecovery was launched from cron during a system boot phase. It should only be considered a problem if it occurs successively, multiple times.	No action required if only received once. If received multiple successive times, then a boot phase process is hung. Locate the hung process and correct.
AutoRecovery running without watchdog!	The watchdog timeout process could not be launched.	AutoRecovery could not fork a process. This may be caused by system resources being exhausted. Examine resource usage and correct.
Could not status system processes.	The system process table defined in femis_watch.conf was empty or undefined.	Check /opt/local/femis_watch.conf for the table containing the @sys_proc definition. Make sure it has entries and no syntax errors. Syntax errors may not be in the table definition itself, but could also be in lines around the definition, particularly in front of it.
Could not status swap space.	The swap threshold is not defined in the configuration file.	Check /opt/local/femis_watch.conf for a line containing “\$swap = ...;”. Make sure it has no syntax errors. Syntax errors may not be in the threshold definition itself, but could also be in lines around the definition, particularly in front of it.
Could not status network connections.	The network host table is not defined in the configuration file.	Check /opt/local/femis_watch.conf for the table containing the @network definition. Make sure it has entries and no syntax errors. Syntax errors may not be in the table definition itself, but could also be in lines around the definition, particularly in front of it.

Error Message	Problem	Solution
Could not status Oracle processes.	At least one of the required Oracle processes is not executing correctly and a review of the Oracle system is recommended.	If this check could not be completed then there is most likely a more serious problem with the database. If there are no other symptoms, then your Database Administrator should diagnose why this database query failed and shutdown and restart Oracle if necessary.
Local listener is down.	The Oracle listener on the local server has stopped working.	Check the /var/log/femislog or the remainder of the E-mail message to indicate if AutoRecovery was successful in restarting the listener. If the listener was not restarted, check the Oracle alert log for any anomalies and restart the listener (command: lsnrctl start).
Could not retrieve push fi list, defaulting to regular site definitions.	The replication push list could not be retrieved from the local Oracle database, even though the local Oracle database could be connected to.	This would typically indicate an internal Oracle problem with the FEMIS database. It could also be a problem with the Perl – Oracle interface, but would be accompanied by other such errors if this is the case. Your Database Administrator should be consulted for correction.
Could not status Oracle tablespaces.	AutoRecovery attempted to measure the amount of data in the Oracle tablespaces but was unable to complete the status check.	If this check could not be completed, then there is most likely a more serious problem with the database. If there are no other symptoms, then your Database Administrator should diagnose why this database query failed and, if necessary, shutdown and restart Oracle.
Database ... may not be available.	The thresholds and process checks defined in the configuration file for remote system checks failed for a particular remote server.	The message does not absolutely indicate that the remote database is not available but that the criteria set in the configuration file for the remote check failed. See the @femismon_proc definition in the /opt/local/bin/femis_watch.conf file. This may not be a correctable situation on the local EOC; however, the threshold values can be adjusted as necessary on the local side to keep

Error Message	Problem	Solution
		<p>AutoRecovery from complaining. Make this change carefully, since it may lead to false indications of a good remote system.</p>
<p>The host “servername” was not stasured or is unavailable, skipping database “database user name”.</p>	<p>This is a warning that AutoRecovery cannot access the remote server and will skip the remote database check. You should also see Connect refused to “servername” port 23.</p>	<p>This message generally occurs when the network or remote server is not operating correctly. Check the status of the network across the site.</p> <ol style="list-style-type: none"> 1. Try the ping –sRv command to check the server for yourself. If this is successful, also attempt a telnet session to the remote host. AutoRecovery requires that both a ping and a telnet attempt be successful before saying the host is reachable. 2. If you have the traceroute command on your system, use it to track the source of the problem. See the man page on <i>traceroute</i> for more information. <p>If the network is working correctly, then your Database Administrator at the remote EOC should be contacted in order to resolve the problem.</p>
<p>The host “servername” was not stasured or is unavailable, skipping listener fi#.</p>	<p>This is a warning that AutoRecovery cannot access the remote server and will skip the remote listener check. You should also see Connect refused to “servername” port 23.</p>	<p>This message generally occurs when the network or remote server is not operating correctly. Check the status of the network across the site.</p> <ol style="list-style-type: none"> 1. Try the ping –sRv command to check the server for yourself. If this is successful, also attempt a telnet session to the remote host. AutoRecovery requires that both a ping and a telnet attempt be successful before saying the host is reachable. 2. If you have the traceroute command on your system, use it to track the source of the problem.

Error Message	Problem	Solution
		<p>See the man page on <i>traceroute</i> for more information.</p> <p>If the network is working correctly then your Database or System Administrator at the remote EOC should be contacted in order to resolve the problem.</p>
<p>Local replication is not running.</p> <p>Trying to fix broken replication (push).</p> <p>Broken replication (push) was fixed!</p>	<p>This is an indication that either the local Oracle replication push mechanism was not enabled or had failed, but it was restarted (corrected) automatically.</p>	<p>No action is required, since the problem was repaired. However, if the message occurs consecutively and frequently, then your Database Administrator should be contacted in order to resolve the issue.</p>
<p>Local replication is not running.</p> <p>Trying to fix broken replication (push).</p> <p>Broken replication (push) could not be fixed.</p>	<p>This is an indication that either the local Oracle replication push mechanism was not enabled, or had failed. An attempt to run the Oracle stored procedure to fix the mechanism was made but was not successful.</p>	<p>This is an indication of a serious problem with the FEMIS Oracle replication mechanism. This problem should be corrected as soon as possible since this will directly affect replication data from your EOC to other remote EOCs. Your Database Administrator should be contacted in order to resolve the issue.</p>
<p>Remote replication is NOT configured!</p>	<p>The remote replication mechanism (<code>remote_update</code>) is not configured.</p>	<p>This indicates a FEMIS Oracle database configuration problem. Your Database Administrator should be contacted in order to resolve the issue.</p>
<p>Local replication is NOT configured!</p>	<p>The local push replication mechanism (<code>push_local</code>) is not configured.</p>	<p>This indicates a FEMIS Oracle database configuration problem. Your Database Administrator should be contacted in order to resolve the issue.</p>
<p>Remote replication is not running.</p> <p>Trying to fix broken replication (update).</p> <p>Broken replication (update) was fixed.</p>	<p>This is an indication that either the local Oracle replication update mechanism was not enabled or had failed, but it was restarted (corrected) automatically.</p>	<p>No action is required, since the problem was repaired. However, if the message occurs consecutively and frequently, then your Database Administrator should be contacted in order to resolve the issue.</p>

Error Message	Problem	Solution
<p>Remote replication is not running. Trying to fix broken replication (update). Broken replication (update) could not be fixed.</p>	<p>This is an indication that either the local Oracle replication update mechanism was not enabled or had failed. An attempt to run the Oracle stored procedure to fix the mechanism was made but was not successful.</p>	<p>This is an indication of a serious problem with the FEMIS Oracle replication mechanism. This problem should be corrected as soon as possible since this will directly affect the ability of your EOC to receive data from other remote EOCs. Your Database Administrator should be contacted in order to resolve the issue.</p>
<p>Not attempting to fix replication.</p>	<p>Replication problems were encountered, but other errors prevented AutoRecovery from safely attempting to correct the problem.</p>	<p>This message must be understood in context with other errors that AutoRecovery has reported. Research and correct the other errors, and then automatic correction will occur.</p>
<p>Replication error not found when indicated (Notifications)! Software error, please report.</p>	<p>Indicates an internal software logic error.</p>	<p>This is an internal AutoRecovery software error and should never be seen. Contact PNNL if this error occurs. It could also indicate serious corruption of the femis_watch script, the femis_watch.conf file, or other hardware related corruption scenarios.</p>
<p>fi* (servername) is being added back to replication push. (* represents Oracle instance number).</p>	<p>The remote server has become good again, and is being added back into the Oracle replication push list.</p>	<p>This is a message indication of a corrected situation and requires no action.</p>
<p>fi * (servername) is being removed from replication push because of errors. (* represents Oracle instance number).</p>	<p>The remote server indicated by the instance number has experienced problems for one run plus the defined threshold amount defined in the configuration file and is being removed from the Oracle replication push list.</p>	<p>This message will be preceded by some number (as defined in the configuration file) of previous AutoRecovery runs indicating a problem(s) with a remote server. If problems occur consecutively for a remote site, and auto_carve is enabled, then the remote host that is causing the problems will be removed from the Oracle push replication list to protect your local Oracle job queue from hanging up. This message indicates an automatic action taken by AutoRecovery and will not generally require intervention. However, once a site is removed from the push list,</p>

Error Message	Problem	Solution
		<p>local Oracle data will no longer be replicated to the remote database. Intervention may be required to correct the situation, which would typically be a problem on the remote EOC's server.</p>
<p>Could not connect to local Oracle.</p>	<p>The AutoRecovery system was not able to connect with the local database.</p>	<ol style="list-style-type: none"> 1. Your Database Administrator should attempt to diagnose why the local database is inaccessible and the exact condition of the database. The database may only be partially shutdown. A complete manual shutdown and startup of Oracle will most likely be required. 2. Check the Oracle tablespace. This message can occur when Oracle is running low on tablespace.
<p>Could not send FEMIS notification.</p>	<p>AutoRecovery has determined that the FEMIS notification daemon is not running.</p>	<p>Check the <code>/var/log/femislog</code>, or the remainder of the E-mail message to determine whether or not AutoRecovery was successful in restarting notification. If it was not successful, this could indicate a larger problem. If logging is enabled, check the log files. Double check your FEMIS notification installation/configuration. See Section 3.0, FEMIS Notification Service, for more information. If the problem persists, call the IEM Help Desk.</p>
<p>Unable to remove existing history file, statistics not saved!</p>	<p>The history file was not able to be unlinked for new updates. Historical statistics affecting auto-insert and auto-carve will be lost.</p>	<p>This will generally be an indication of a file permissions problem either on the file <code>/var/tmp/.autorecovery.run</code> or the <code>/var/tmp</code> directory itself. This is an error that should not occur unless some other process has been touching the run file or the <code>/var/tmp</code> directory during or between an AutoRecovery run.</p>

Error Message	Problem	Solution
Can't open file <filename>: <error description>.	The history file could not be opened for new updates. Historical statistics affecting auto-insert and auto-carve will be lost	This will generally be an indication of a file permissions problem either on the file /var/tmp/.autorecovery.run or the /var/tmp directory itself. This is an error that should not occur unless some other process has been touching the run file or the /var/tmp directory during or between an AutoRecovery run.
<p>There are ___ “daemon name” daemons. The range is set from ___ to ___.</p> <p><i>See the following messages for information on femisdei, oracle processes, and tnslnr daemons.</i></p>	The number of named daemons is outside the threshold identified by AutoRecovery.	<ol style="list-style-type: none"> 1. Check the rest of the message to see if AutoRecovery corrected the problem. 2. Check the system for other problem associated with the daemon. 3. Change the threshold values for the daemon in /opt/local/bin/femis_watch.conf.
<p>There are 0 tnslnr daemons. The range is set from 1 to 1.</p> <p>Trying to restart the tnslnr daemon.</p>	The Oracle listener on the local server has stopped working.	Check the /var/log/femislog or the remainder of the E-mail message to determine if AutoRecovery was successful in restarting the listener. If the listener was not restarted, check the Oracle alert log for any anomalies and restart the listener (command: lsnrctl start).
Trying to restart the ... daemon.		This is an informative message and requires no action by itself.
Could not attempt to restart ..., ntpdate is still running.	Sun’s current implementation of starting NTP launches a ntpdate process prior to starting ntpd. ntpdate can hang if a good connection to the time server is not established.	Verify connectivity to the remote time server and that time services are running properly. If remote time services are up and available, then kill the offending ntpdate process and allow AutoRecovery to attempt another NTP restart or restart manually with the command /etc/init.d/xntpd start. If ntpdate still hangs, there may be network issues causing the problem. Resolve and correct, then attempt restart after killing the ntpdate process again.

Error Message	Problem	Solution
<p>Restart failed. There are ... daemons. The range is set from ... to ...</p>	<p>The attempt to restart a restartable process failed.</p>	<p>Verify that the process does indeed not exist in the process table. Also, verify the AutoRecovery configuration to be sure this is a process that can be stasured and restarted.</p> <p>If the above conditions are true, then try running the restart command defined in the configuration file for the offending process manually (as the root user). If this fails, resolve and correct for the specific situation. If it is successful, then check for syntax errors on the restart command in the configuration file.</p>
<p>A previous run of ./femis_watch did not complete. Please check the following processes</p> <pre> PID COMMAND process id(s) process name(s) **** Exiting ./femis_watch **** </pre>	<p>There is another version of AutoRecovery (femis_watch) that has not completed or is hung.</p>	<p>The AutoRecovery message includes a list of processes that are associated with an earlier run of AutoRecovery. Has the same process been hung for several cycles of Auto-Recovery?</p> <p>If not, then the \$watchdog_timeout value in the configuration file may be set too high relative to the AutoRecovery cron interval. Adjust the value as necessary.</p> <p>If so, then the watchdog timeout may not be working properly. Verify that there were no watchdog launch problems or that the \$watchdog_timeout is defined in the configuration file.</p>

Error Message	Problem	Solution
<p>There are 0 femisdei daemons. The range is set from 1 to 1.</p> <p>Trying to restart the femisdei daemon.</p> <p>Restart failed. There are 0 femisdei daemons. The range is set from 1 to 1</p> <p>FEMIS notification could not be sent, * errors.</p>	<p>femisdei could not be restarted.</p>	<p>Consult the <i>FEMIS System Administration Guide</i>, or the <i>FEMIS Installation Guide</i> for proper configuration of the FEMIS DEI system.</p>
<p>FEMIS event is not running on port 9021.</p> <p>FEMIS event is not running on port 9022.</p> <p>FEMIS event is not running on port 9023.</p> <p>Trying to restart FEMIS event.</p> <p>Restart FEMIS event failed.</p>	<p>This is a combination message indicating the femis_event process was not running, and a restart was attempted but failed. The FEMIS event server controls notification messages and is an integral part of the FEMIS software. Resolution of the problem is necessary.</p>	<p>This could indicate a larger problem. If logging is enabled, check the log files. Double check your FEMIS notification installation/configuration. See Section 3.0, FEMIS Notification Service, for more information on FEMIS Notification. If the problem persists, contact the IEM Help Desk.</p>
<p>Trying to restart FEMIS event.</p>		<p>This is an informative message by itself and does not require intervention.</p>
<p>FEMIS event is not running on port 9021.</p> <p>FEMIS event is not running on port 9022.</p> <p>FEMIS event is not running on port 9023.</p> <p>Trying to restart FEMIS event.</p> <p>Restart FEMIS event successful.</p>	<p>This is a combination message indicating the femis_event process was not running, and a restart was attempted and was successful.</p>	<p>No further intervention is required unless the problem occurs consecutively and frequently.</p> <p>If it does occur consecutively and frequently, then this could indicate a larger problem. If logging is enabled, check the log files. Double check your FEMIS notification installation/configuration. See Section 3.0, FEMIS Notification Service, for more information on FEMIS Notification. If the problem persists, contact the IEM Help Desk.</p>
<p>FEMIS event is not running on port "port #".</p>	<p>AutoRecovery has determined that the FEMIS notification daemon is not running.</p>	<p>Check the /var/log/femislog, or the remainder of the E-mail message to indicate whether or not AutoRecovery was successful in restarting notification. If it was not successful, this could indicate a larger problem.</p>

Error Message	Problem	Solution
		<p>If logging is enabled, check the log files. Double check your FEMIS notification installation/configuration. See Section 3.0, FEMIS Notification Service, for more information on FEMIS Notification. If the problem persists, contact the IEM Help Desk.</p>
<p>Cannot connect to Oracle.</p>	<p>The AutoRecovery system was not able to connect with the local database.</p>	<ol style="list-style-type: none"> 1. Your Database Administrator should attempt to diagnose why the local database is inaccessible and the exact condition of the database. The database may only be partially shutdown. A complete manual shutdown and startup of Oracle will most likely be required. 2. Check the Oracle tablespace. This message can occur when Oracle is running low on tablespace.
<p>Listener fi* is down (* represents Oracle instance number).</p>	<p>The Oracle listener on a remote server has stopped responding or is unreachable at this time.</p>	<p>No local action may be necessary unless this is a local networking issue. Contact the remote server System Administrator that hosts the listener.</p>
<p>swap is __% full, __kb used.</p>	<p>Swap space has exceeded the threshold configured in /opt/local/bin/femis_watch.conf.</p>	<p>The swap threshold is set to 80 by default. You can increase this in /opt/local/bin/femis_watch.conf by changing swap = 80 to a higher value. Monitor the system. A high value for swap can be a symptom of other problems.</p>
<p>Disk space on “disk” is __% full, __kb used.</p>	<p>The disk space on “disk” has exceeded the threshold configured in /opt/local/bin/femis_watch.conf.</p>	<p>The disk threshold is set to 80 by default. You can increase this in /opt/local/bin/femis_watch.conf by changing the disk threshold to a higher value.</p> <p>Look for any files or directories that can be deleted. Be on the lookout for any core files that can be deleted.</p> <p>If the disk in question has Oracle export, log or other Oracle files associated with it and check to make sure the Oracle cleanup script is run</p>

Error Message	Problem	Solution
		<p>every week. The cleanup script will not run if the full system backup script fails to complete. If a backup failure is confirmed, rerun the full backup script and delete some of the older oracle export and log files.</p>
<p>Connect refused to “servername” port 23.</p>	<p>AutoRecovery could not ping the named server. AutoRecovery will skip all other system and database checks on a system it cannot ping.</p>	<ol style="list-style-type: none"> 1. Your network, router, or server could be experiencing problems. Check with your network or System Administrator for the server mentioned in the message. 2. Try the ping –sRv command to check the server for yourself. 3. If you have the traceroute command on your system, use it to track the source of the problem. See the man page on <i>traceroute</i> for more information.
<pre>##### Processing SIGALRM Interrupt! Level 2: Killing: user = root, pid = 29800, ppid = 29799, comm = /files2/app/oracle/product/8.1.6/bi n/lsnrctl status fi6.world Trying TERM... process 29800 sucessfully signaled. Level 1: Killing: user = root, pid = 29799, ppid = 29768, comm = sh -c /files2/app/oracle/product/8.1.6/bi n/lsnrctl status fi6.world 2>&1</pre>	<p>The watchdog timer (timeout) expired for an AutoRecovery run.</p>	<p>This message indicates the process cleanup of a hung AutoRecovery process. The processes listed indicate the active process tree (parent – child relationship) that was killed in order to get AutoRecovery to exit gracefully.</p> <p>This message may also occur with out the action messages indicating attempts to kill with an actual kill signal. When this occurs, the timeout occurred, but the offending processes exited gracefully on their own while the timeout interrupt was being processed.</p> <p>This message may also occur with an empty body indicating that a timeout occurred, but the offending processes exited on their own before the</p>

Error Message	Problem	Solution
		<p>interrupt routine could determine what was hanging up AutoRecovery.</p> <p>No action is required unless this occurs consecutively and frequently. If this is the case, then there may be problems with the specific subsystem that is hanging up. Resolve the issue based on the hung process information in the messages and the specific case those message refer to.</p>
<p>Remote check on “database code” found 0 Ora* process(es). The range is set from __ to __. (* represents the Oracle process name).</p>	<p>This message occurs in combination with messages stating that a remote database may not be available. It is the specific indication of why AutoRecovery believes that the remote database may not be available.</p>	<p>The message does not absolutely indicate that the remote database is not available but that the criteria set in the configuration file for the remote check failed. See the @femismon_proc definition in the /opt/local/bin/femis_watch.conf file. This may not be a correctable situation on the local EOC; however, the threshold values can be adjusted as necessary on the local side to keep AutoRecovery from complaining. Make this change carefully, since it may lead to false indications of a good remote system.</p>

2.2 UNIX FEMIS Monitor

The UNIX FEMIS Monitor provides the status of the FEMIS servers and databases. 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 utility 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 How to Detect System Problems

As necessary, the System Administrator can observe the UNIX FEMIS Monitor output on the server monitor. The monitor can be started by logging in as femis and typing femismon.sh. The monitor periodically (default is every minute) checks the status of major system interfaces, including the database, on each server. When done reviewing the monitor output, type <Ctrl>C to end the monitor session. An example of typical output generated by the monitor under normal operating conditions is shown below.

```
* * * MSG: -- FEMIS Process Monitor --
* * * MSG: /home/femis/bin/femismon.sh
* * * MSG: Fri Apr 5 13:46:38 PST 1996
* * * MSG: -----
* * * MSG: -- FEMIS Processes Status --
* * * MSG: virus
* * * MSG: femis_event : up
* * * MSG: # cmdserv : 0
* * * MSG: femisdei : up
* * * MSG: # Oracles : 51
* * * MSG: # femisd : 7
* * * MSG: -----
* * * MSG: -- Oracle Database Status --
* * * MSG: DB and Listener : ok (tead on virus)
* * * MSG: Snapshot account: ok (utst on virus)
* * * MSG: -----
* * * MSG: Sleeping...
```

The femisd count refers to the number of femisd processes currently running on the server. It is a daemon that passes all socket communication between the FEMIS PC and the FEMIS UNIX processes. The femisd daemon is started as needed so the output results are for the user's information.

The monitor first checks the status of your local server. If you use the -all command line option, all servers and databases are checked. In case a server was unavailable, a standard UNIX error message is displayed along with another warning message. These errors are due to complete network failure or server shutdown and should be uncommon. If a server failure is detected, try to determine the cause by contacting the System Administrator for the EOC. For example, if the server were down, the following messages would be displayed

```
* * * MSG: virus
* * * ERR: Server not responding: virus *****
```

If the server is available, the monitor then checks the femis_event process, which is the notification service. If the process is operating normally, the message femis_event :ok is displayed. If problems are detected, the message femis_event : down is shown. Refer to Section 3.0, FEMIS Notification Service, for diagnosing and fixing notification problems.

The next check is on the number of FEMIS Command Service daemons running. The result is informational, and 0 is valid, which means no one is using the Evacuation module in FEMIS.

The monitor then checks on the femisdei (the FEMIS/EMIS Data Exchange Interface). The normal condition shows femisdei : ok, but errors will display femisdei : down. This check is only performed on the server that supports the FEMIS DEI interface. Refer to Section 7.0, FEMIS Data Exchange Interface (DEI), for diagnosing and fixing problems with this interface.

Next the number of current Oracle client processes is shown. If this number is over 100, serious problems have caused database sessions to abort.

The monitor's last check is on the Oracle database. The first step is to see if Oracle is running. The other items to check are the status of the local and any remote accounts for other EOCs. Normally, no errors will be present, and a listing similar to the previous example will be displayed.

After the last check has been completed, notification messages are sent via the FEV utility, which the PC Monitoring tool uses. These messages indicate whether each item checked was running properly.

If any database errors are detected, the process will attempt to identify the probable cause according to the following precedence:

1. If the local Oracle Listener process has failed on a server, the following message will be displayed:

```
* * * ERR: DB or Listener : down (tead on virus) *****  
* * * ERR:           Oracle Listener on virus down
```

2. If the local Oracle database instance has failed, the following message will be displayed:

```
* * * ERR: DB or Listener : down (tead on virus) *****  
* * * ERR:           Oracle Database on virus down
```

3. If the network is unavailable or any other types of errors are present, the following message will be displayed:

```
* * * ERR: DB or Listener : down (tead on virus) *****  
* * * ERR:           Probable Network error
```

4. If Oracle replication errors are detected, the following message will be displayed:

```
* * * ERR: Snapshot account : down (utst on virus) *****
```

5. If the data acknowledgment Oracle job is not running, the following message will be displayed:

```
* * * ERR: Data acknowledge: down (tead on virus) *****
```

When database errors are reported, contact your Database Administrator and review what the AutoRecovery has reported and/or fixed. For more information, refer to the temporary files, femismon.*, that are left in the /tmp directory. These files are especially useful for determining why replication is not working.

For site-wide monitoring, you can run the FEMIS Monitor with the -all option, which shows the status of all servers and all Oracle accounts on all servers.

2.2.3 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 /filesX/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 +++
```

2.2.4 UNIX FEMIS Monitor Scripts

Scripts are now utilized to perform process counting, rather than a string of `ps` and `greps`. 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 for that purpose, `FM_PS`, `FM_AWK`, `FM_GREP`. 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.

2.2.5 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`.

2.2.6 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, utilized by the `femismon.sh` script to provide communication 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.

The `femismon.sh` script invokes the command `femismon -B` to collect status information from the FEMIS monitor daemon. The brief format is as follows: `E C D O F` all on one line, where `E` is the number of `femis_event` processes, `C` is the number of command servers, `D` is the number of `femisdei` processes, `O` is the number of Oracle client processes, and `F` is the number of `femisd` processes.

2.3 FEMISMon Watcher (FWATCH.EXE)

The FEMISMon Watcher (`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.

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. The server containing your default EOC will be in uppercase.

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).

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.

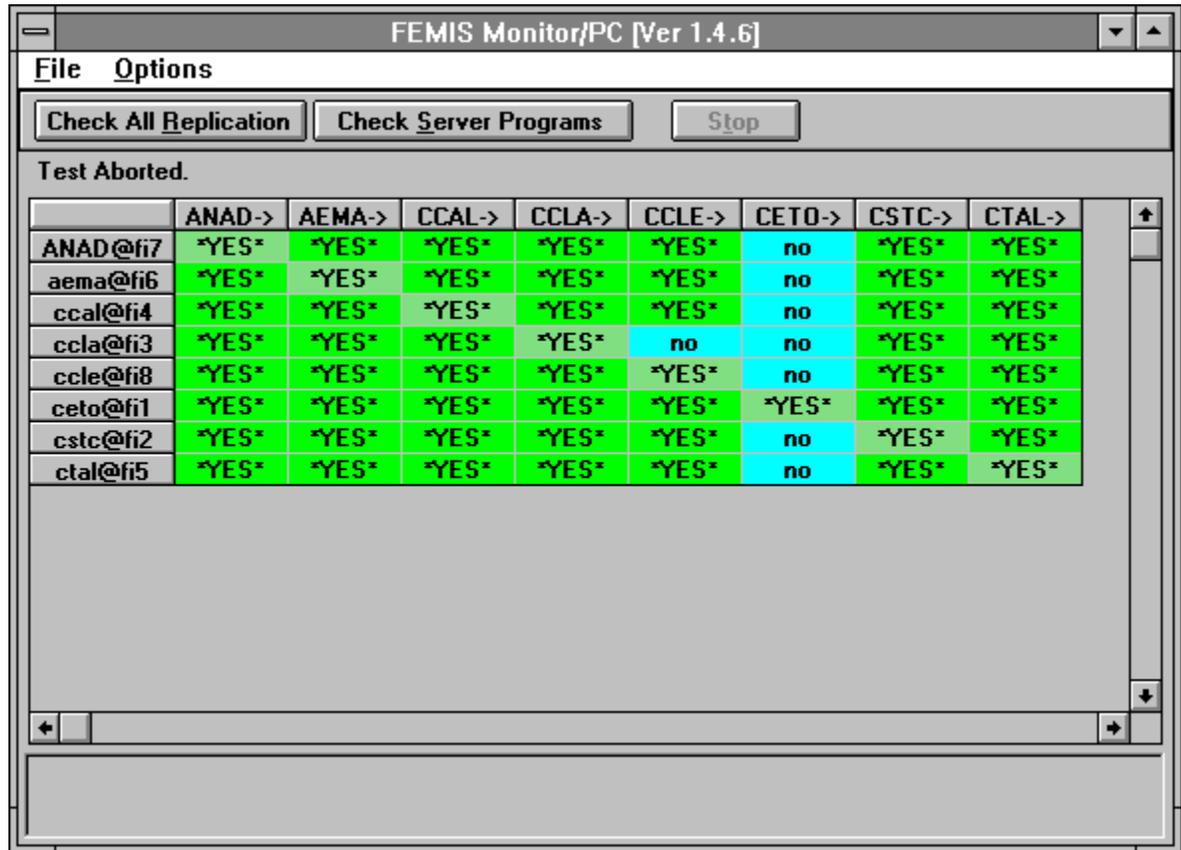
A spreadsheet of the results is shown on the FEMIS Monitor/PC window (See Figure 2-2).

- The headers across the top are From Database XXX.
- The headers down the left side are To Database XXX.
- 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.

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.)

Figure 2.2. FEMIS Monitor/PC Window



This utility will stop checking

1. If all the databases have replicated and everything says *YES*

or

2. 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 either 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 CCLE 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.

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.

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.