2.0 FEMIS UNIX Installation

The UNIX server is the primary data and information storage and distribution component. Its primary software elements consist of the Oracle database management system (DBMS); the Evacuation SIMulation (ESIM) model with supporting processes; the Notification Service; the command server; the meteorology (Met) data receiver; the FEMIS/EMIS Data Exchange Interface (DEI); and the sockets communications service.

The programs discussed require the UNIX environment on a Sun computer running Solaris 7[(a)] and utilizing standard Berkeley or Berkley-like Sockets.

The FEMIS UNIX software installation consists of six major parts:

- Installing the UNIX Commercial-Off-The-Shelf (COTS)
- Installing the FEMIS UNIX Software
- Installing the FEMIS GIS and Database
- Checking the FEMIS Startup
- Utility to Add FEMIS User Account to the Database
- FEMIS AutoRecovery System.

The release media consists of files distributed on CDs, 8mm cartridge tapes, and on occasion, floppy disks. The release material contains the necessary scripts and data to perform an initial installation or to upgrade existing FEMIS software to the current version. The Release Notes should be read before proceeding with the UNIX installation.

The FEMIS package consists of the following:

- COTS CD
- FEMIS application tape
- Suite of FEMIS documentation.

In addition to the FEMIS package, the Sun Solaris 7 (SunOs 5.7) and Oracle media are necessary to complete the UNIX installation of FEMIS.

This guide is written assuming that your EOC is using local host network files. If your EOC is using some other facility, i.e., NIS/NIS+, then those facility-specific commands must be used.

(a) Per Sun's Release Notes (5/99), Solaris has changed the name of their latest release to Solaris 7 (SunOs 5.7) instead of Solaris 2.7. The FEMIS Bill of Materials (BOM), released on March 3, 2000, listed Solaris v2.7 as required server software. For more information, see Sun's web site – http://docs.sun.com:80/ab2/coll.385.1/@Ab2CollView?Ab2Lang=C&Ab2Enc=iso-8859-1

2.1 Installing and Configuring the UNIX COTS

It is important to coordinate the UNIX group numbers between FEMIS and other software applications that are administered with NIS+. Possible conflicts may result in the FEMIS /etc/group file. To see which group numbers are currently used for NIS+, use the following command while logged in as root:

```
niscat group.org_dir
```

If you are installing from a pre-existing NT account, then the corresponding UNIX account must be a member of the UNIX femisrun group on the server. Also, when using the NIS/NIS+ dB, be sure the /etc/nsswitch.conf file is properly configured to consult files as well as NIS. FEMIS may still have portions that expect entries in the host files. Primarily, these are FEMIS specific entries in the /etc/passwd file and its components (shadow). The /etc/group file is not specifically consulted, but any group membership changes done for the current install user need to be done according to how the nsswitch.conf is configured.

The following sections describe the installation of the UNIX COTS.

2.1.1 Installing the Operating System

S T O P

Those sites using the Sun Volume Manager or Disksuite software to manage disk arrays, that wish to maintain array configuration and data throughout the Operating System (OS) upgrade, may need to follow special instructions PRIOR to upgrading Solaris.

For upgrading the Volume Manager Software to the current VERITAS Volume Manager, specific instructions have been provided in Section 2.1.2, Upgrading Sun Volume Manager Software.

For Sun Disksuite, consult your vendor supplied documentation prior to the OS upgrade.

For installation or upgrade instructions, see the documentation provided with the operating system. Additional installation information is available on the FEMIS Web site at http://www.pnl.gov/femis under the Technical and User Support section.

Follow the instructions included with the Solaris 7 documentation. Section 2.1.1.1, Installing or Upgrading Solaris 7, provides additional information regarding the Solaris 7 installation process. If the quantity of server customizations is considered large, the upgrade option is recommended. If server clean up is preferred, then the new install option can be taken instead of upgrading an existing installation.

Note: Installing operating system patches will require relinking the Oracle software. See Section 2.3.3.4, Relinking the Oracle Software.

Solaris Versions, Maintenance Updates, and Patch Clusters

FEMIS was tested on a Solaris 7 5/99 release with patch cluster updates noted below. Solaris 7 field installations are encouraged to be the 5/99 release or later.

FEMIS was not tested on any particular Maintenance Update of Solaris 7. If a site desires to install a current stable Maintenance Update, conflicts with Solaris Maintenance Updates and FEMIS are not anticipated.

We have tested FEMIS v1.4.7 using the March 2000 patch cluster. Because all operating systems require patches to improve security and fix bugs, PNNL strongly recommends installing Sun's Solaris 7 patch cluster. The Solaris 7 patch cluster does not always include all patches that may be preferred for complete system functionality. Individual patch README files contain additional information regarding related patches that may be desired for complete fixes to reported problems. Additionally, certain hardware platforms may require specific patches that are not included in the patch cluster. Please consult Sun Solaris documentation, specifically installation release notes and ***Solaris™ 7 … Release Notes Supplement for Sun™ Hardware*** and/or Sun's Web site http://sunsolve.sun.com for further information. The patch cluster is strongly recommended as a minimum patch set for each system. This cluster is typically updated twice a month by Sun Microsystems. Refresh installations of the patch cluster are recommended on a periodic basis particularly for security enhancements.

If the patch cluster is not available, the following five patches **must be installed** for FEMIS v1.4.7. Use showrev –p to list your existing patches.

Kernel patch – 106541-10 or greater (requires quiescent system – see README)
Patchadd/patchrm patch – 107171-05
Cron patch – 107451-02
fsck patch – 107544-03
X Input & Output Method patch - 107636-03 or greater

Note: Check our web site (www.pnl.gov/femis/) for updates on patches that we have tested.

Volume Manager/Storage Array Firmware

PNNL is currently using VERITAS Volume Manager v3.0.2.

VERITAS Volume Manager v3.0.2 requires the Sun libthread patch 106980-05 (-10 is the latest at the time this was written) and the Sun kernel patch 106541 (-10 is the latest at the time this was written). The 106980 patch must be downloaded and installed separately after the cluster upgrade is completed as it is not part of the Solaris 7 patch cluster.

Solaris 7 requires SPARC Storage Array (SSA) firmware to be at v3.12. To verify your current version, use ssaadm display <controller> (where <controller> is the controller number, such as c1).

If the SSA firmware is not at v3.12, it **must be upgraded**. This can be accomplished during the Solaris 7 upgrade process, after the upgrade is complete, but **before rebooting** the new Solaris 7 kernel.

If the boot disk is a SSA disk, see the ***Solaris 7 … Sun™ Hardware Platform Guide*** section titled "Installing the Solaris Operating Environment With the SPARCstorage Array" for further information.

To upgrade the SSA firmware,

1. Enter the following command:

   ssaadm download –f /usr/lib/firmware/ssa/ssafirmware <controller>)

   where <controller> is the controller number, such as c1)

   Note: DO NOT INTERRPUT THE ABOVE COMMAND FOR ANY REASON!

2. Halt the system with /usr/sbin/init 0.

3. Click the SYS OK button on the back of the SSA(s) to reset.

4. Wait for the SSA to complete POST.

5. Boot the system by typing boot at the system ok prompt.

Patch Locations

Those patches discussed above and other patches are available from SunSolve Online at http://sunsolve.sun.com/ or the SunService Public Patch Page at ftp:// metalab.unc.edu /pub/sun-info/sun-patches.

2.1.1.1 Installing or Upgrading Solaris 7

For those sites desiring to do new installs of Solaris 7, rather than upgrading the existing Solaris v2.6, **and** upgrading the current FEMIS installation, rather than doing a new FEMIS install, several steps must be taken prior to the Operating System Installation to allow the upgrading of FEMIS later.

To accomplish the FEMIS upgrade, the FEMIS and various other packages must be removed prior to the Operating System upgrade. The skeleton directories left must be preserved prior to the Solaris 7 new install, and then restored to the system after the Solaris 7 install so that the FEMIS upgrade can be completed.

AutoRecovery and AutoRecovery Web reporting (if installed) must be removed. You may wish to save the /opt/local/bin/femis_watch.conf file for configuration of the new AutoRecovery package later. If the /opt/local/bin/femis_watch.conf is saved for later, please be aware that it **is not a drop-in replacement** for the femis_watch.conf file in the new package. It is to be used for reference only.

To remove AutoRecovery, complete the following steps.

1. Login as root, and enter the following command.

   # pkgrm FEMISar

To remove AutoRecovery Web Reporting, see Section 2.7.2.1 Removing the AutoRecovery Web Reporting Package.

To continue preparing your system for a new installation of Solaris 7 and the upgrading of your current version of FEMIS, complete the following steps.

1. Complete **only** Section 2.2.2, Upgrading the FEMIS Application. Make sure the <backupdir> created in this step will be in an area or on a device unaffected by the Operating System installation.

2. Save what is left of the /home/femis directory tree to another disk or device that will be unaffected by the Operating System installation. Use tar or ufsdump to save the image so file times are preserved.

3. Remove the Perl package. See Section 2.1.6.1 Removing the Perl Package.

4. Save the /var/opt/oracle directory tree to another disk or device that will be unaffected by the Operating System installation. You may wish to preserve the /apps/oracle tree (minus the product directory) if it is on a partition that may be affected by the Operating System installation.

5. Complete the new Solaris 7 per the vendor's documentation.

6. Restore the trees saved in Steps 3 and 5 above as appropriate.

For those sites where an Operating System upgrade will occur, rather than a new installation of Solaris 7, PNNL recommends the following method for disk partitioning and preserving data while running the installation/upgrade program for Solaris 7.

1. Use ufsdump to backup your file systems relating to the Operating System prior to upgrading.

2. Edit the /etc/vfstab file and comment out any entries relating to swap files (not swap partitions) and storage array file systems.

3. Boot the Solaris 7 CD-ROM which launches the interactive installer.

4. Follow the prompts and/or instructions to install/upgrade. Select no network unless you are upgrading from a remote install/jumpstart server or booting from the network, then the server needs to be considered networked.

5. Check if the 64-bit button has been selected. If so, this indicates your system can support running the 64-bit kernel. It will not be selected on systems where greater performance may not be realized, and it will be grayed out (not selectable) on systems where the 64-bit kernel can not be run at all. Selection, as allowed, is up to the installer.

   Selecting the 64-bit support only means that the 64-bit support (i.e., for 64-bit application development) will be installed. Even with 64-bit kernel support installed, the default kernel booted will be the one supported by your hardware (as determined by the bootstrap software).

If the current partitions are sized correctly for Solaris 7 and the requested packages, then the installation will complete without interruption.

If disk partitions are not large enough according to the interactive installer program's calculations, then the More Space Needed window will display.

1. Select the Auto-layout button, and allow it to calculate the necessary new sizes. If Auto-layout requires constraints to be changed, continue using it as a tool to plan the correct layout and sizes.

   Note: Do not allow Auto-layout to make partition backups and new layouts.

2. Make a note of the current partition size(s) and recommended new size(s). Exit the interactive installation program at this time.

3. Open a command window and dismount the affected volumes that were mounted by installation program.

3. Repartition and resize the disk layout or partitions using the command-line format tool (see the man page on *format*) as recommended by the previously suggested sizes in Step 1.

4. Adjustment the swap partition, if desired.

5. Create new file systems on the affected partitions and remount the new partitions back on to the installation file system.

6. Use ufsrestore –rf <dumpfile> to restore the affected file systems (backup previously created) onto the new disk partitions.

7. Mount or go to the partition containing the actual system's root file system. Edit the vfstab file to reflect any device changes made in Steps 3–6.

8. Remove any restoresymtable files created by ufsrestore, and dismount all file systems under the /a path.

9. Right click in the background workspace area, and select Restart Install. Proceed through the installation process as prompted. You may have to start from the beginning again, however, if disk space partitions were correctly assigned, the upgrade should continue without error.

Partitioning

Separate partitions are not absolutely necessary for /, /usr, /var, and /opt. They can be combined into one / partition or split into various subsets. The /usr is static and does not usually contain dynamic data; /var is used for logging and temporary areas, so it grow considerably; and /opt is for optional software package installations, so its size depends on the planned usage of the server.

The following packages are not functionally required in case of space limitations:

- Packages pertaining to manuals, especially developer manuals and/or software.
- DHCP server if not used by clients.
- developer profiled libraries
- Unnecessary device drivers (this may not be easily determined, use discretion).
- Documentation tools
- International locale and font support
- Font server software (if not used)
- NIS support (if not used – basic packages can not be deselected)
- demos (binaries and software)
- PCMCIA support (if not used)
- Point-to-point protocol (if not used)
- Power management utilities (if not used)
- Programming tools and libraries
- WEBNFS (if not used)
- others (site dependant and based on Installer experience)

All packages not installed at upgrade time can be installed later if desired using a variety of package management tools/software.

Patching and Patching Order (see Array notes above)

The following patches must be installed.

- 106541 — requires quiescent system
- 107171-05 — is necessary to correct certain patch order problems when installing cluster patches.

32/64-bit Kernel and Firmware Updates

Flash Prom updates apply only to the following systems (output from `uname –i`):

- SUNW, Ultra-1
- SUNW, Ultra-2
- SUNW, Ultra-4
- SUNW, Ultra-Enterprise

Prom version level can be determined with `prtconf –V`.

If a Flash Prom update is required, Solaris 7 will prompt you upon boot-up. Special steps to write-enable the Flash Prom are required, and the procedure to do this differs between hardware platforms. In the Solaris 7 documentation, ***Solaris 7 … Sun™ Hardware Platform Guide***, see the section entitled "Updating the Flash Prom on the Ultra 1, Ultra 2, Ultra 450, and Sun Enterprise 450 Systems" (Chapter 4 in 5/99 release documentation).

Utilities

Solaris 7 now incorporates traceroute and zip as bundled utilities. traceroute used to be added to the system during installation. The PC utility called PK-Zip was re-written and released for multi-platform usage. All patches for Solaris 7+ will be shipped in Zip archive format.

2.1.1.2 Automounting and FEMIS

Note: Using the automounter is optional, but strongly recommended by PNNL.

If FEMIS v1.4.5 or higher has successfully been installed, then the automount points should have been set up. Review this section to verify they were set up correctly.

This section is intended to be an overview of automounting. Specific automounting instructions are located in the following sections.

FEMIS uses the automounter scheme to automatically and transparently mount file system resources for both home and application directories. The automounter uses a series of maps to define the file resources to be mounted. Setting up the automounter consists of defining the maps and starting the automounter program.

Master Map

The master map is located at /etc/auto_master. This file provides a list of all maps on the system. It is read by the automounter daemon at system startup. The map for FEMIS looks similar to the following.

```
/net        -hosts          -nosuid,nobrowse
/home       auto_home
/apps       auto_apps
/xfn        -xfn
```

Indirect Maps

Indirect maps are used to mount file resources under a common directory. FEMIS needs two indirect maps for automounting: 1) /etc/auto_apps and 2) /etc/auto_home. The map, /etc/auto_home, contains the entries of the UNIX user login accounts to be mounted under /home. The indirect map for /etc/auto_home must look similar to the following.

Note: The current site map should list users and directory paths at your site. Remember to replace system# with the name of your server. The hostname localhost may also be used as the server name for directory structures collocated on the same server[a].

```
femis     -intr,rw,nosuid     system1:/files3/home:&
femx      -intr,rw,nosuid     system1:/files3/home:&
usera     -intr,rw,nosuid     system1:/files5/home:&
userb     -intr,rw,nosuid     system1:/files5/home:&
userc     -intr,rw,nosuid     system1:/files5/home:&
userd     -intr,rw,nosuid     system1:/files5/home:&
usere     -intr,rw,nosuid     system2:/files5/home:&
```

The /etc/auto_home map gives us a consistent view of home directories across a network. All home directories, whether remote or local, are mounted under each server's /home directory. As an example, a UNIX account for usere, which has a directory on system2 on partition /files5/home/usere, is mounted at /home/usere on the current system.

The indirect map for /etc/auto_apps should look similar to following.

```
oracle      -intr,rw,nosuid     system1:/files2/app:&
```

Automounter Map Availability

Changes to indirect maps are available right away. Changes to the /etc/auto_master are effective only by restarting the automount daemon.

```
# /etc/init.d/autofs stop
# /etc/init.d/autofs start
```

([a]) The term localhost must be used carefully when the automount map is distributed via NIS/NIS+ in a multiple server configuration, or where PC clients can interpret NIS automount map information.

Note: Automount cannot reflect new file systems in cases where the currently automounted file system is moved out from underneath an actively automounted file system in lieu of a replacement file system. To replace a mapped automount file system, make sure no processes are active in the automount tree by using fuser -nc <auto_mount_path>, and that automount has released the mount point before changing an automounted file system.

FEMIS Users

Note: Actual UNIX user accounts are created as needed. Steps are provided to create accounts for Oracle and the FEMIS application in their respective installation sections.

If the automounter is being used, an entry is necessary in /etc/auto_home, for each new FEMIS user added to the system. See Indirect Maps section above for more information. For additional information on automounting and automount maps, see the man page on *automount* and the Solaris documentation.

2.1.1.3 Creating Users and Groups

This section provides an overview on guidelines and instructions for creating FEMIS UNIX user accounts and groups on your server. Specific instructions are supplied in the Section 2.2.1, Creating UNIX Accounts on the Server.

The following information is required to create a UNIX user account:

Username
User Identification Number
Group Identification Number or Name
User's home directory location (usually /home/<user>)
Preferred user shell (usually /bin/csh)
Password

Usernames

Note: The UNIX username **must be the same** as the corresponding Windows NT username.

Usernames, or login names, will allow the user to access the server with the appropriate access privileges. A username should be

Unique within the organization
Contain two to eight letters or digits
One character must be lower case
First character must be a letter
May not contain a space or a new line (\n).

User Identification Numbers

A user identification (UID) number is assigned to each username. It identifies the user to the system and controls access to files and directories. UIDs have several requirements:

UIDs must be unique for each user.
UIDs must be whole numbers between 100 and MAXUID (defined in /sys/param.h>).

Since many employers assign employees with unique employee numbers, System Administrators can use or manipulate employee numbers to get unique UIDs in the appropriate range. UIDs, along with the rest of the username data, is stored in the /etc/passwd file.

Password

Note: PNNL recommends that the UNIX password **be the same** as the corresponding Windows NT password if NFS Maestro or SUNWpcnfd are being used at your site. This is not a requirement if Samba is being used on the UNIX server, and it is authenticating to the same domain/NT server as the PC (assuming domain and/or Windows NT server authentication is in use).

Each username must be assigned a password. Passwords have a big impact on systems security so follow these minimum conventions when creating passwords. Passwords should

Be six to eight characters in length
Include at least one digit or special character such as $, &, #
Differ from the user login name
Be changed often
Avoid proper nouns, or any word a person could guess by knowing you
Avoid words found in the dictionary
Avoid Social Security numbers, phone numbers, and car license numbers.

Group Identification Numbers

A group is a collection of users who share files and other resources. Each group has a group name, a group identification (GID) number, and a list of usernames that belong to the group. A primary group is the group the operating system will assign to files created by the user. Each user belongs to one primary group. The primary group must already exist when adding a new user.

User Home Directory

The user's home directory is the space on the disk that is allocated for a user. Use the full path name or see Section 2.1.1.2, Automounting and FEMIS, if automounting home directories.

Creating FEMIS User Accounts

All FEMIS accounts must be members of the UNIX group femisrun. The femisrun should already exist prior to adding users. See Section 12.1, Operating System Security, in the ***FEMIS System Administration Guide*** for more information.

Note: The user ID listed below is an example only. Select a user ID that is unique for your EOC.

1. Create the UNIX user account.

   # /usr/sbin/useradd -u NEWUID -g femisrun -c “A Name”-d login_directory_path -s /bin/csh login_name

   Example:

   # /usr/sbin/useradd -u 4000 -g femisrun -c “John Doe” -d /files1/home/jdoe -s /bin/csh jdoe

   If automounting, the login directory path should be /home/login-name.

2. Create the appropriate home directories for the newly created accounts.

   # mkdir -p login_directory_path
   # chown login_name:femisrun login_directory_path

3. Set the account password.

   # passwd login_name

If you are using the automounter, make the appropriate entry in the /etc/auto_home file. See Section 2.1.1.2, Automounting and FEMIS, for more information.

For additional information on UNIX user accounts and groups, see the man pages on *useradd*, *groupadd*, and *passwd*, as well as the Solaris documentation.

S T O P

If AutoRecovery has previously been installed on the server and FEMIS, Oracle, or UNIX COTS software will be installed or upgraded, AutoRecovery MUST be stopped until the UNIX installation is complete.

To stop AutoRecovery, edit the root crontab file and comment out the lines pertaining to AutoRecovery.

1. Login as root.

2. Enter the following:

   crontab -e

3. Comment out the lines following ##FEMISar.

   Example:

```
##FEMISar
#0 * * * * LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/files2/app/oracle/product/8.1.6/lib; export
LD_LIBRARY_PATH; /opt/local/bin/femis_watch > /dev/null 2>&1 #FEMISar
#30 * * * 1-5 LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/files2/app/oracle/product/8.1.6/lib; export
LD_LIBRARY_PATH; /opt/local/bin/femis_watch > /dev/null 2>&1 #FEMISar
#10,20,40,50 7-18 * * 1-5
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/files2/app/oracle/product/8.1.6/lib; export
LD_LIBRARY_PATH; /opt/local/bin/femis_watch > /dev/null 2>&1 #FEMISar
#0 0 * * * sh /opt/local/bin/logit > /dev/null 2>&1 #FEMISar
```

When you have completed the UNIX installation process (upgrade or fresh install), be sure the lines in the crontab file are uncommented and updated according to new paths. AutoRecovery is the last UNIX item to be installed/upgraded. Installation and upgrading instructions for AutoRecovery are in Section 2.6, FEMIS AutoRecovery System Description and Installation.

2.1.2 Upgrading Sun Volume Manager Software

Note: Start the process of obtaining licensing (lead-time up to 5 working days). Current Sun Volume Manager 2.5 license should move across, but a hardcopy version of the license is prudent in case the system needs to ever be rebuilt from scratch. See instructions in ***VERITAS Volume Manager for Solaris Installation Guide*** section titled "Obtaining a License Key" for further information. The VERITAS product information (software serial number) is packaged separately in a sealed envelope.

This section only includes instructions for upgrading Sun Volume Manager v2.5 software on Solaris v2.6 to VERITAS Volume Manger v3.0.2 on Solaris 7. For new installations and setup of the VERITAS software or differing Operating System requirements, see the documentation and licensing supplied with VERITAS.

Note: The instructions below **must also be done prior** to upgrading from Solaris v2.6 to Solaris 7.

To upgrade Sun Volume Manager v2.5 software on Solaris v2.6 to VERITAS Volume Manger v3.0.2 on Solaris 7, complete the following steps.

1. Backup the data on your system in single user mode, particularly the data located on the Storage Array and /usr/lib.

2. Backing up the complete system using ufsdump to preserve file times.

3. Make sure that at least one plex for each of these volumes (if any of the file systems /, /usr, /var, or /opt are defined on volumes) is formed from a single subdisk that begins on a cylinder boundary. See ***VERITAS Volume Manager for Solaris Installation Guide*** section titled "Upgrading to VxVM 3.0.X and Solaris 2.5.1/2.6/7" for further information.

4. Load and mount the CD-ROM installation media. SPARC1000 (and possibly other older) server CD-ROM drives may not read the VERITAS v3.0.2 CD. In these cases it may be necessary to read and dump the installation CD to some other medium (network or removable) from a system with a newer CD-ROM drive, which is done to gain access to the installation software.

5. Run the upgrade_start script to prepare the previous release of the Volume Manager for removal. upgrade_start is locate at <installation software path>/scripts/upgrade_start.

6. Change directories to /var/sadm/patch. Using the ls command, determine if you have any versions of patch number 105463-xx are installed on the system. If they have been installed, they **must be removed**. If multiple versions of the same patch exist, they must all be removed. Remove the highest numbered revision first, then the next, and so on.

7. Reboot to single user mode using the command init S.

8. Remove the following packages, if they are installed:

   SUNWassa, SUNWvmman, , SUNWvxvm, SUNWvmdev, SUNWasevm

   This can be accomplished on a single pkgrm line:

   # pkgrm SUNWassa SUNWvmman SUNWvxva SUNWvmdev SUNWasevm

9. Edit the /etc/vfstab file, and comment out any storage array lines under Volume Management control.

10. Reboot to the Solaris 7 installation media, and proceed with the Solaris 7 installation/upgrade.

11. Reboot to single user mode using the command init S.

12. Access/mount the VERITAS installation software, and add the VxVM 3.0.2 package:

    # pkgadd –d <installation software path>/<OS_version>/pkgs VRTSvxvm

    If this returns warnings that include the string /etc/vx, ignore them and continue.

13. Complete the upgrade by entering:

    # <installation software path>/scripts/upgrade_finish

14. Edit the /etc/vfstab file, and uncomment the previously commented lines from Step 9.

15. Reboot to multi-user mode. Note any errors during reboot regarding drv/atf and drv/ses. If any errors occur, edit the /etc/system file once the system is booted, and comment the lines at the end of the file regarding the drivers that had errors. In /etc/system, a comment line begins with an asterisk (*). Be sure to comment **only** those lines in the file relating to the force load errors recorded during boot. These devices may be necessary for functionality beyond the scope of this section that is added and configured at a later date. If this situation is planned, the lines can be uncommented later, or left as is until the VERITAS configuration is complete.

16. Using pkgadd, install any or all of the additional packages VRTSvmsa, VRTSvmdoc, VRTSvmman, and VRTSvmdev.

    Note: Importing a pre-3.x Volume Manager disk group does not automatically upgrade the disk group version to the VxVM 3.x level. You may need to manually upgrade each of your disk groups following a VxVM upgrade. See the section on disk tasks in the ***VERITAS Command Line Interface Administrator's Guide*** for information on how to upgrade a disk group.

17. Follow the instructions in the ***VERITAS Volume Manager for Solaris Installation Guide*** for "Setting Up and Starting the Storage Administrator".

2.1.3 Installing and Configuring Samba

Note: Disable and/or remove any previous versions of Samba from the system. Save the old configuration file for reference.

Samba may exist on a system in one of two forms.

- It can be launched in a stand-alone mode in which case it is initially started by /etc/init.d startup scripts. To disable in this case, simply remove or rename the Samba startup scripts, and kill all smbd and nmbd processes.

- The other form is launched from the inetd daemon. In this case, the startup lines must be temporarily commented out of the /etc/inetd.conf file, and inetd signaled to reread its configuration file with a kill –HUP <inetd pid>. Then kill all smbd and nmbd processes on the system to disable.

The location of the original configuration file can then be determined either from the startup scripts or the inetd.conf file. The smbd and nmbd binaries usually reside in a bin directory under the Samba main installation root. The old configuration file will be typically located under the lib portion of this tree and is called smb.conf. There may be additional information worth saving in the lib branch, so saving this entire directory for future reference is recommended.

Be sure to create an automount location entry for /apps/samba. For example: in /etc/auto_apps:

```
samba        -intr,rw,nosuid        localhost:/vol02/app:&
```

Note: Be sure /vol02/app/samba exists. Create it, if necessary.

2.1.3.1 Installing Samba

Note: When installing a FEMIS package from the spool directory, it is possible to receive a Sun Package installation error, Broken Pipe. This error happens when the last package in the list is not selected for installation. This error will not cause any problems with the FEMIS installation. Continue with the installation.

To install Samba v2.0.6, complete the following steps.

1. Login as root, and insert the FEMIS application tape into the tape drive.

2. Create a temporary spool directory.

   ```
   # mkdir /<dir>/spool
   # chmod 755 /<dir>/spool
   ```

3. Spool the installation package from the 8mm tape using the Solaris software installation utility.

   ```
   # pkgadd -s /<dir>/spool -d /dev/rmt/??
   ```

   where ?? is the device number of the tape drive. Select the packages desired and run the pkgadd utility to install the FEMIS package.

   ```
   # pkgadd -d /<dir>/spool
   ```

4. Select the Samba application for installation.

5. Answer the questions as prompted:

   - The source is the original Samba source tree (unconfigured).

- The Windows NT Domain will only apply to those sites using NT Domain services. Enter anything if your site is not using this capability.

- The WINS address is an IP address of a WINS server. Enter d if you are not using this capability at your site.

- Enter the actual absolute path name for the automounted location of /apps/samba. For example: /vol02/app/samba as taken from the automount entry example above.

6. Select y to continue when the following prompt displays: This package contains scripts which will be executed with super-user permission during the process of installing this package.

7. Select q to quit after installing the Samba package.

8. Use pkgchk to verify the package was installed correctly.

   # pkgchk -n SAMBA

   If you only see the above output or get a prompt with no output, the package installed successfully. Continue with the installation by configuring Samba.

2.1.3.2 Configuring Samba

Samba configuration can get quite complex because of the flexibility the software offers. Please refer to the man page on smbd.conf for other options and combinations. A template configuration file is provided by the package installation which will set up basic parameters and define basic FEMIS shares. However, manual configuration is inevitable in order to bring the prior version's definitions into place for compatibility.

1. View the /etc/samba/smb.conf file. Edit the template as necessary according to your site specific requirements. If you need to bring in configuration from a previous version of Samba, do that here. Pay particular attention to the values for the following parameters:

   - hosts allow is set according to your site's subnet configuration.

   - security and password server are set according to the authentication method in use at your site (domain, NT server, local smbpasswd, or UNIX). Edits done at this time will override entries requested by the package install scripts. This will allow EOC customization beyond what the default package installation deals with.

   - Uncomment the interfaces line if you are running more than one interface on your server (machine is a router) if you want Samba to present itself on all interfaces. The device designation le0…n is assumed, but can be changed to hme0...n (hme*) for those sites so configured.

- Be sure the share entries for femis, femis_user, and user reflect the correct path for your site. The rest of the configuration for these entries is recommended to remain as shipped.

2. Test the configuration by running the Samba testparm program.

   This program will report on the currently defined configuration. It will point out any configuration errors, and report assumed default values for the whole configuration. If this program does not return errors, proceed to the next step. If it does, review and correct the configuration file and re-run testparm.

   ```
   # /apps/samba/bin/testparm
   Load smb config files from /etc/samba/smb.conf
   Processing section "[homes]"
   Processing section "[printers]"
   Processing section "[femis]"
   Processing section "[femis_user]"
   Processing section "[user]"
   Loaded services file OK.
   WARNING: You have some share names that are longer than 8 chars
   These may give errors while browsing or may not be accessible
   to some older clients
   Press enter to see a dump of your service definitions
   ```

3. Join your Windows NT domain (if applicable):

   To join an existing NT domain, an entry containing the NetBIOS name of the server must be added to the NT domain on the Primary Domain Controller using Server Manager for Domains.

   Once the above is complete, enter the following command on the Samba server:

   ```
   /apps/samba/bin/smbpasswd –j <domain_name> -r <primary domain controller>
   ```

   You should receive the following response:

   ```
   <date/time stamp>: change_trust_account_password: Changed password for domain
   <domain_name>.
   Joined domain <domain_name>.
   ```

4. Enable Samba via the /etc/inetd.conf configuation file. The package installation will have added new lines to the /etc/inetd.conf file which specifies the Samba daemon startup. Signal inetd to reread its configuration file to launch Samba.

   ```
   # ps –ef | grep inetd
   # kill –HUP <inetd pid>
   ```

5. Verify client connectivity by attempting to connect to one of the default new shares defined in the smb.conf file from a PC.

Samba source files are distributed with this installation and are located at /apps/samba/source if installed. Under /apps/samba/source/docs is useful information regarding Samba operation and use, especially in integrating with Microsoft Windows environments. In addition, Samba provides detailed UNIX manual pages on its primary components which are included with the package and are located under the default path /apps/samba/man. Further information and up-to-date news regarding Samba can be obtained from the Samba Web site: http://www.samba.org/ (locate a close mirror site from there).

2.1.4 Installing the NFS Authentication Services Daemon

For FEMIS v1.4.7, either NFS Maestro v 6.1 or Sun PC NFS v1.2 can be installed as the authentication service daemon. The following sections provide installation instructions for both NFS packages.

Note: If you have an older version of the NFS Maestro or Sun PC NFS package on your server, you **must remove** it. If the NFS software was installed manually (no packages were used), determine from the entries in /etc/init.d the location of the software and remove it along with its start/stop scripts in /etc/init.d and/or /etc/rd#.d directories.

2.1.4.1 Determining Version of NFS Daemon

If you do not know if NFS Maestro or Sun PC NFS has been installed as a package on your server, enter the following commands:

```
# pkginfo -l HCLNFS
# pkginfo -l SUNWpcnfd
```

2.1.4.2 Removing Previous NFS Daemon

To remove the old version of the NFS Maestro or Sun PC NFS package, enter the following commands:

```
# pkgrm HCLNFS
# pkgrm SUNWpcnfd
```

2.1.4.3 Installing Hummingbird NFS Daemon

Note: When installing the FEMIS package from the spool directory, it is possible to receive a Sun Package installation error, Broken Pipe. This error happens when the last package in the list is not selected for installation. This error will not cause any problems with the FEMIS installation. Continue with the installation.

The Hummingbird NFS Daemon (NFS Maestro v6.1) has been included with FEMIS v1.4.7. To install the NFS Daemon, complete the following steps.

1. Login as root, and insert the FEMIS application tape into the tape drive.

2. Create a temporary spool directory.

   ```
   # mkdir /<dir>/spool
   # chmod 755 /<dir>/spool
   ```

   Spool the installation package from the 8mm tape using the Solaris software installation utility.

   ```
   # pkgadd -s /<dir>/spool -d /dev/rmt/??
   ```
   where ?? is the device number of the tape drive. Select the packages desired and run the pkgadd utility to install the FEMIS package.

   ```
   # pkgadd -d /<dir>/spool
   ```

3. Select the HCLNFS application for installation.

4. Select y to continue when the following prompt displays: "This package contains scripts which will be executed with super-user permission during the process of installing this package."

5. Select q to quit after installing the HCLNFS package.

6. Use pkgchk to verify the package was installed correctly.

   ```
   # pkgchk -n HCLNFS
   ```

7. Ignore the following errors:

   ```
   ERROR: /etc/init.d/hclnfs
       Permission <0755> expected <0744> actual
       Group name <other> expected <sys> actual
   ```

   If you only see the above output, or you get a prompt with no output, the package installed successfully.

8. Enter the following command to start the Hummingbird NFS daemon:

   ```
   # sh /etc/init.d/hclnfs start
   ```

2.1.4.4 Installing Sun PC NFS Daemon

The Sun PC NFS Daemon (SUNWpcnfd) has been included with FEMIS v1.4.7. To install the Sun PC NFS Daemon, complete the following steps.

1. Login as root, and insert the FEMIS application tape into the tape drive.

2. Create a temporary spool directory.

   ```
   # mkdir /<dir>/spool
   # chmod 755 /<dir>/spool
   ```

   Spool the installation package from the 8mm tape using the Solaris software installation utility.

   ```
   # pkgadd -s /<dir>/spool -d /dev/rmt/??
   ```

   where ?? is the device number of the tape drive. Select the packages desired and run the pkgadd utility to install the FEMIS package.

   ```
   # pkgadd -d /<dir>/spool
   ```

3. Select the SUNWpcnfd application for installation.

4. Select y to continue when the following prompt displays: This package contains scripts which will be executed with super-user permission during the process of installing this package.

5. Select q to quit after installing the SUNWpcnfd package.

6. Use pkgchk to verify the package was installed correctly.

   ```
   # pkgchk -n SUNWpcnfd
   ```

7. Ignore errors like the following:

   ```
   ERROR: /etc/init.d/SUNWpcnfd
   Permission <0755> expected <0744> actual
   Group name <other> expected <sys> actual
   ```

   If you only see the above output, or you get a prompt with no output, the package installed successfully.

8. Enter the following command to start the Solstice NFS daemon:

   ```
   # sh /etc/init.d/SUNWpcnfd start
   ```

2.1.5 Installing an E-mail Package

Install your E-mail package according to documentation provided by the vendor.

2.1.6 Installing Perl v5.004-04

If you are upgrading FEMIS, you will have a previous version of the Perl package that **must be removed**, prior to installing Perl v5.004-04.

2.1.6.1 Removing the Perl Package

1. Login as root.

2. Enter the following

   ```
   # pkgrm Perl
   ```

3. Select y to continue when the following prompt displays: Do you want to remove this package?

4. Also select y for this prompt: Removing installed package instance <Perl>. This package contains scripts that will be executed with super-user permission during the process of removing this package. Do you want to continue with the removal of this package [y,n,?,q].

5. Verify that the package was removed successfully.

2.1.6.2 Installing the Perl Package

The Perl application will require 15MB of disk space for a spool directory. To install Perl, which has been included with FEMIS v1.4.7, complete the following steps.

1. Login as root, and insert the FEMIS application tape into the tape drive.

2. Create a temporary spool directory.

   ```
   # mkdir /<dir>/spool
   # chmod 755 /<dir>/spool
   ```

3. Spool the installation package from the 8mm tape using the Solaris software installation utility.

   ```
   # pkgadd -s /<dir>/spool -d /dev/rmt/??
   ```

   where ?? is the device number of the tape drive.

4. Run the pkgadd utility to install the Perl package.

   ```
   # pkgadd -d /<dir>/spool
   ```

5. Select the Perl application for installation.

6. Select y to continue when the following prompt displays: The following files are already installed on the system and are being used by another package: /opt/local/bin <attribute change only> * - conflict with a file which does not belong to any package. Do you want to install these conflicting files.

7. Select y to continue when the following prompt displays: This package contains scripts which will be executed with super-user permission during the process of installing this package.

8. Select q to quit after installing the Perl package.

9. Use pkgchk to verify that Perl installed correctly.

   #pkgchk -n Perl

   Note: The packages installed successfully if no error output is displayed. Report any errors to PNNL.

10. Remove the spool directory.

    # rm -r /<dir>/spool

11. Logout.

2.2 Installing the FEMIS UNIX Software

Before configuring the FEMIS UNIX software on the server, you **must determine** the FEMIS home directory

Example: /home/femis

Using the Solaris software installation utility, pkgadd, the FEMIS application and support files will be installed to the Sun server.

2.2.1 Creating UNIX Accounts on the Server

Note: If you have successfully installed FEMIS v1.4.5 or higher, then skip this section.

You will need to create several new UNIX accounts on the server to prepare for the FEMIS package installation.

1. Login as root.

2. Create the following accounts (numeric IDs are for example only):

   # /usr/sbin/groupadd -g 30510 femisrun
   # /usr/sbin/useradd -u 30508 -g femisrun -c “FEMIS Account” -d /home/femis -s /bin/csh femis

If you are running DEI, create the following account **only on the onpost server**:

```
# /usr/sbin/useradd -u 30509 -g femisrun -c "FEMX Account" -d /home/femx -s /bin/csh femx
```

3. Create the appropriate home directories for the newly created accounts. Make sure each directory has the correct owner and group.

```
# mkdir -p /<file system>/home/femis
# chown femis:femisrun /<file system>/home/femis
```

Note: Creating the femx directory should only be done on the onpost server.

```
# mkdir -p /<file system>/home/femx
# chown femx:femisrun /<file system>/home/femx
```

4. Set the account password.

```
# passwd femis
```

Note: Setting the femx password should only be done for the onpost server.

```
# passwd femx
```

5. Edit /etc/auto_home and add entries for both the femis and femx accounts, if your system uses automount maps. The entries must look similar to the following:

```
femis      -intr,rw,nosuid      systemname:path:&
femx       -intr,rw,nosuid      systemname:path:&
```

Example:

```
femis      -intr,rw,nosuid      mysystem:/<file system>/home:&
femx       -intr,rw,nosuid      mysystem:/<file system>/home:&
```

The colon and ampersand (:&) in the above examples may also have a /<map_key> instead. Either method of map specification is fine.

See Section 2.1.1.2, Automounting and FEMIS, for more information.

6. Add the following line to the /etc/dfs/dfstab file, unless Samba is being exclusively used for FEMIS:

```
share -F nfs -o rw /<disk>/home/femis
```

where <disk> is whichever device /home/femis is on.

Note: To restrict NFS access, see the man pages on *share* and *share_nfs* in your Solaris documentation.

If you do not have any other entries in the dfstab file, you will need to start the NFS server process. If you do not start the NFS server process, you will see errors like "RPC: Program not registered" when entering the shareall command (see below). To start the NFS server process, type the following:

```
# /etc/init.d/nfs.server start
```

To make the /<disk>/home/femis directory available to NFS authentication services (daemon) type

```
# shareall
```

To check that the directory is available to NFS Maestro type

```
# share
```

You should see output similar to the following:

```
# -     /<disk>/home/femis rw ""
```

2.2.2 Upgrading the FEMIS Application

Note: If you are doing a new install of FEMIS, then skip this section. If you have successfully installed FEMIS v1.4.6 or higher, then you **must complete** this section.

To prepare for the new version (an upgrade) of FEMIS, check for the existence of required user accounts, backup the FEMIS directory, and remove the old FEMIS installation.

1. Login as root.

2. Copy the site-specific directories to another location using the following commands:

   Note: The <backup> directory in the following represents a file system of your choice on this server where you can save a copy of the files. You will need to restore the /home/femis/user directory at the end of the Section 2.2.3, Installing the FEMIS Package. The configd and etc directories are backed up in this step for redundancy only.

   ```
   # mkdir <backupdir>
   # cd /home/femis
   # tar cf - user configd etc pc/femtools/femis.db | (cd <backupdir>; tar xf -)
   ```

   Use these files to reference site-specific information, as needed.

3. Make sure both the femis and femisrun accounts exist, if you are installing on the onpost server. Otherwise, only the femis account needs to exist.

   # logins -m -l femis

   Your output should look similar to the following:

   femis 30508 femisrun 30510 FEMIS Account

   If your output is blank, you need to add the femis and femisrun accounts. See Section 2.2.1, Creating UNIX Accounts on the Server, to add these accounts.

   If you are running DEI, the femx account should exist.

   # logins -m -l femx
   Your output should look similar to the following:

   femx 30509 femisrun 30510 FEMIX Account

   Note: Some systems may show femx having supplemental group membership in the femis group. The femis group, as of v1.4.7, is obsolete and may be removed from the system as long as any files having femis as the group owner are changed to femisrun (or match whatever the femis account's primary group is). The exception is those **deemed sensitive for security reasons**, such as /home/femis/etc/cmdserv.conf which should have group ownership set to noaccess (see Section 12.1.6 No Access Files in the ***FEMIS System Administration Guide***).

   If your output is blank, you will need to add the femx account. See Section 2.2.1, Creating UNIX Accounts on the Server, to add this account.

4. Stop all FEMIS processes, such as DEI and Notification, before removing the FEMIS package.

   Login as femis.

   On all servers

   % stopnotify This will stop Notification.

   Onpost Only

   % femisdei -kill
   % stopdai.sh

5. Remove the FEMIS application.

Login as root.

```
# pkgrm FEMIS
```

You will most likely see warning messages about package dependencies similar to the following:

```
## Verifying package dependencies.
WARNING:
        The <FEMISgs> package depends on the package
        currently being removed.
WARNING:
        The <FEMISdb> package depends on the package
        currently being removed.
Dependency checking failed.

Do you want to continue with the removal of this package [y,n,?,q]
```

If this message appears, answer Yes by typing a y and pressing Enter.

6. Delete the site-specific directories that you backed up in Step 2.

```
# rm -r /home/femis/user
# rm -r /home/femis/configd        (The directory may not exist).
# rm -r /home/femis/etc
```

2.2.3 Installing the FEMIS Package

Note: When installing the FEMIS package from the spool directory, it is possible to receive a Sun Package installation error, Broken Pipe. This error happens when the last package in the list is not selected for installation. This error will not cause any problems with the FEMIS installation. Continue with the installation.

You will copy the FEMIS package(s) to a spool directory and install FEMIS by completing the following steps. The FEMIS application will require 82MB of disk space for a spool directory.

1. Login as root, insert the FEMIS application tape into the tape drive.

2. Enter the following command to mount the FEMIS installation directory, if you are using the automounter.

```
cd /home/femis
```

3. Create a temporary spool directory.

```
# mkdir /<dir>/spool
# chmod 755 /<dir>/spool
```

4. Spool the installation package from the 8mm tape using the Solaris software installation utility.

   # pkgadd -s /<dir>/spool -d /dev/rmt/??

   where ?? is the device number of the tape drive. Select the packages desired and run the pkgadd utility to install the FEMIS package.

5. Run the following command again if exited above:

   # pkgadd -d /<dir>/spool

6. Select the FEMIS application for installation.

   Ignore any warning messages about disk space.
   If the femx account was created prior to the installation, you will be asked if you want to install DEI. If the server will be running the FEMIS DEI, select y to install the DEI options.

   Select y to continue when the following prompt displays: This package contains scripts which will be executed with super-user permission during the process of installing this package.

7. Select q to quit, after the FEMIS application has been installed.

8. Use pkgchk to verify the FEMIS package has installed correctly.

   #pkgchk -n FEMIS

   Ignore the following errors:

   ERROR: /etc/init.d/femis
   permissions <0644> expected <0744> actual group name <other> expected <sys> actual
   ERROR: /home/femis
   permissions <0755> expected <0775> actual owner name <femis> expected <femx> actual

   If you only see the above output, or you get a prompt with no output, the package installed successfully.

9. Remove the spool directory, **unless you will be installing AutoRecovery or AutoRecovery Web.**

   # rm -r /<dir>/spool

10. Restore only the FEMIS application user directories in the /home/femis/user directory and the femis.db file from the backup you made in Section 2.2.2, Upgrading the FEMIS Application (Step 2), if you are upgrading the FEMIS application.

```
# cd /home/femis/pc/femtools
# mv femis.db femis_orig.db
# cp –p <backupdir>/pc/femtools/femis.db  .
# cd <backupdir>/user
# tar cf – `find . –type d  \!  -name . –prune` | (cd /home/femis/user; tar xf -)
```

11. Set the setgid bit for the /home/femis/user directory.

    ```
    # find /home/femis/user –type d –exec chmod g+xs {} \;
    ```

12. Remove the FEMIS application tape from the drive.

2.2.4 Installing Network Time Protocol (NTP)

This section describes the steps required to remove the Network Time Protocol (NTP) package bundled with previous versions of FEMIS, and it steps you through configuring the NTP software bundled with the Solaris operating system.

If you have any version of the FEMIS NTP package on your server, you will need to remove it. If you do not know if NTP is installed as a package on your server, enter the following command:

```
# pkginfo | grep XNTPD
```

A result similar to the following means the NTP package is installed on your server.

```
application   XNTPD    Network Time Protocol
```

Note: If you do not received a response to the above command, skip to Configuring NTP below.

If you know you are already running the bundled Solaris NTP, proceed to Step4 under Configuring NTP.

Removing the Old Version of NTP

1. Stop the NTP daemon.

   ```
   # sh /etc/init.d/ntp stop
   ```

2. Save the old ntp.conf file for reference.

   ```
   # cp /etc/ntp.conf /etc/ntp.conf.old
   ```

3. Enter the following command to remove the old version of the NTP package.

   ```
   # pkgrm XNTPD
   ```

4. Select y to continue when the following prompt displays: "Do you want to remove this package?"

5. Also select y for this prompt: "Removing installed package instance <XNTPD>. This package contains scripts that will be executed with super-user permission during the process of removing this package. Do you want to continue with the removal of this package [y,n,?,q]"

Configuring NTP

Note: You do not need to configure NTP if you already have the Solaris version of NTP configured.

NTP is included with the Solaris operating system. To configure NTP complete the following steps.

1. Login as root.

2. Enter the following:

   cd /home/femis/install

3. Run the following script to configure an ntp.conf file in the /etc/inet directory and start the NTP daemon (xntpd). You may need information from the ntp.conf.old file in the /etc directory before running this script. Then you may remove the ntp.conf.old file.

   sh ntp_config

   The installation will ask if the server will get time from another server; select y if yes, otherwise select n.

   If you selected y above, the installation will prompt for the NTP server's Internet Protocol (IP) address. Make sure the NTP server is accessible (available on the network) as the installation will attempt to ping the NTP server.

   The message: "/etc/inet/ntp.conf already exists. It will not be reconfigured," means the script found an existing /etc/inet/ntp.conf file and exited without making any changes to the /etc/inet/ntp.conf file.

4. Check your NTP configuration.

   ntptrace <servername>

   It may take awhile before your output shows a traceback other than a "timeout". Once the traceback information displays correctly, NTP is configured.

For additional information on NTP see the Section 11.0, Server Network Time Protocol (NTP) Set Up, in the ***FEMIS System Administration Guide***.

Note: If the server is not synching with any time source, you **must change** the file so NTP will work. See Section 11.0, Server Network Time Protocol (NTP) Set Up, in the ***FEMIS System Administration Guide*** for instructions.

2.3 Installing the FEMIS GIS and Database

If this is a new installation of FEMIS, you will need to install both the Oracle software (v8.1.6) and the FEMIS GIS and database packages.

If you are upgrading to a new version of FEMIS, you will have to upgrade Oracle to v8.1.6 and install the appropriate FEMIS GIS and database package from the tape, if FEMIS v1.4.6 has not previously been installed.

In FEMIS, database topologies are defined either as NxN or NxM, which are number pairs that indicate the number of EOC databases and the number of servers. For example, a 3x3 (or NxN) configuration indicates three EOCs on three servers. Likewise, an 8x4 (or NxM) configuration represents eight EOCs on four servers.

On each server, Oracle schemas are created to store the EOC data. The schemas are broken into two groups: 1) data owner schema or 2) snapshot owner schema. A data owner schema has the database tables that store the data for an EOC. A snapshot owner schema has a set of specialized snapshot tables that are created to support the replication of data.

On every NxN configuration, there is exactly one data owner and N-1 snapshot owners per server. By definition, NxM configurations have more than one data owner on at least one of the M servers in the configuration.

The terms data owner and snapshot owner will be used frequently throughout this section and as the installation is performed. You will need to know which server has which data owner within your configuration.

To properly complete the installation for your site, follow the instructions in the Section 2.3.1, Installing the GIS and Oracle Database through Section 2.3.5.7, Setting Up the Oracle Backups.

2.3.1 Installing the GIS and Oracle Database

Note: Complete this section only if you are installing a new FEMIS GIS and database package. If you are upgrading the existing database skip to the next section.

Oracle Release v8.1.6 requires a minimum of 128MB of RAM; if you do not have this much memory installed, **do not attempt** to install Oracle v8.1.6. To check the amount of memory available, issue the following command:

```
# /usr/sbin/prtconf | grep size
```

To install the GIS and database package, complete the following steps.

1. Insert the GIS and database tape into the tape drive.

   This installation may require considerable disk space for a spool directory. To create a temporary spool directory, run the following commands but only if you did not create the spool when you installed the FEMIS package.

   # mkdir /<dir>/spool

   Spool the installation package from the 8mm tape using the Solaris software installation utility.

   # pkgadd -s /<dir>/spool -d /dev/rmt/??

   where ?? is the device number of the tape drive. Select the packages desired, and run the pkgadd utility to install the GIS and database package.

   # pkgadd -d /<dir>/spool
2. Select the numbers corresponding to your site's GIS and database using commas as separators.

3. Select q to quit, after the GIS and database have been installed.

4. Use pkgchk to verify the packages were installed correctly.

   #pkgchk -n <package name>

   No output is expected as a result of this command.

5. Remove the spool directory.

   # rm -r /<dir>/spool

6. Remove the tape from the drive.

2.3.2 Database Cleanup Tasks

The following tasks describe how to prepare your existing database for an upgrade. Check each subsection to see if it pertains to your site.

2.3.2.1 Dropping Database Objects and Exporting Data Owners

Note: Complete this section only if you have a previous version of FEMIS installed. If you do not have a previous version installed, skip this section and go to Section 2.3.2.2, Removing Current Oracle Installation.

1. Drop all the non-table objects. If you are upgrading on an NxM or NxN system, the master drop script will drop objects from all servers in the configuration and only needs to be performed on one server.

   As oracle user:

   ```
   % svrmgrl
   SVRMGR>connect internal          (system response should be Connected.)
   SVRMGR>shutdown immediate        (system response should be Oracle instance shut down.)
   SVRMGR>startup                   (system response should be "Oracle instance started...")
   SVRMGR>exit
   ```

   As femis user:

   ```
   % cd /home/femis/database/eocdba
   % sqlplus /nologin
   SQL> @master_dr
   ```

   Watch the progress of the master_dr.sql script. If you do not have any problems, press Enter after each Pause statement is encountered.

2. Perform an export of all FEMIS data owners on each server. The export files created in this step will be re-imported later if you need to reinstall Oracle. If you are not going to reinstall or upgrade Oracle, then export this data as a safety precaution.

   Note: To determine the "data owner" schemas, review the /home/femis/etc/eoclist.dat file. The first column lists all EOCs for your site. The third column lists the server where the EOC is a data owner. Perform an export for every EOC whose server matches your server.

   ```
   % cd $/home/femis/database/exports/<site name>
   % exp userid=<EOC_name>/<data owner password> file=<EOC_name>_<date (yyyymmdd)>.dmp
   log=<EOC_name>_<date>.log
   ```

3. Repeat this export command for each data owner schema that resides on this server. For example, if you have eight EOCs at your site but only three EOC databases reside on this server, then you will make three database exports on this server. You must then export the remaining data owners from each of the other servers in the configuration.

2.3.2.2 Removing Current Oracle Installation

Note: The following tasks are only required if you are upgrading to Oracle v8.1.6. If you are installing Oracle for the first time or if you already have Oracle v8.1.6 installed, then skip this section.

1. Login as oracle user and enter the following to shutdown the old database, shutdown the listener, and delete the old Oracle files.

   ```
   % svrmgrl
   SVRMGR>connect internal
   SVRMGR>shutdown immediate
   SVRMGR>exit
   % lsnrctl
   LSNRCTL>stop
   LSNRCTL>exit
   ```

   Note: Before removing the Oracle Product directory, confirm that all Oracle Instances (some facilities have multiple instances running) have been shutdown. Use the ps and grep commands to identify the Oracle processes. For example ps -ef |grep oracle | sort.

2. Identify the location of the Oracle data and log files, and delete them.

   ```
   % cd
   % ls /*/app/oracle/oradata/*
   % rm –rf /*/app/oracle/oradata/fi<#>/*
   % cd $ORACLE_HOME
   % cd ..
   % rm -rf <oracle_directory>
   ```

   The oracle_directory is named after the version number, for example, for Oracle v7.3.3 the directory is named 7.3.3. To confirm the removal of this directory, enter

   ```
   ls
   ```

3. Save the current configuration files in /var/opt/oracle.

   ```
   % cd /var/opt/oracle
   % mkdir bkp
   % cp *.ora ./bkp
   ```

4. Comment out all database instances in the /var/opt/oracle/oratab file. This is important; otherwise you will have difficulty in creating a new instance with the same name as the old one.

2.3.3 Installing Oracle Software or Relinking Oracle

Note: If you do not have Oracle v8.1.6 (the version required for FEMIS v1.4.7) installed, carefully review each of the following sections and determine which sections pertain to your site.

If you already have the Oracle v8.1.6 installed, you may need to relink the Oracle software. To determine if relinking is necessary, go to Section 2.3.3.4, Relinking the Oracle Software, and skip Sections 2.3.3.1, 2.3.3.2, and 2.3.3.3.

Before beginning the Oracle v8.1.6 installation, you should review the installation guide provided by Oracle, ***Oracle8i Installation Guide Release 2 (8.1.6) for Sun SPARC Solaris***. The following steps are required to install Oracle and identify specific parameter settings required by FEMIS.

2.3.3.1 Creating the UNIX Environment for Oracle

Note: Numeric IDs in this section are for example only.

To create the UNIX environment for Oracle v8.1.6, complete the following steps.

1. Select a drive on which to install Oracle (this will be referred to as <install_drive>). The drive must have a minimum of 1000MB available. Select two additional drives on which to locate the FEMIS database files (these will be referred to as <driveA> and <driveB>). Each of these drives should have a minimum of 500MB available. It is recommended that all drives used are RAID volumes. For complete information on server drives, see the ***FEMIS Bill of Materials (BOM)*** or on the FEMIS web site at http://www.pnl.gov/femis. The following command will allow you to view the drives and their available storage space.

   ```
   % df –k –F ufs
   ```

2. Login in as root.

   Check if there is a group named dba and a group named oinstall in the /etc/group file, and also determine if oracle is a member of the dba and the oinstall group.

   ```
   # egrep '^dba|^oinstall' /etc/group
   ```

   Verify that output from the above command resembles the following:

   ```
   dba:*:26001:oracle
   oinstall::26002:oracle
   ```

   If you do not the get the output above, use the following command to add a dba and/or an oinstall group, as necessary:

   ```
   # /usr/sbin/groupadd -g 26001 dba
   # /usr/sbin/groupadd -g 26002 oinstall
   ```

Note: You may select any number for your group identification (GID) number that is not currently being used. Be sure to check for the existence of a GID in both the /etc/group file and NIS+ (if your site uses NIS+).

Edit the /etc/group file, and add oracle to the group oinstall, as necessary.

3. Check if an oracle account already exists.

   # logins –m –l oracle

   The following is an example of output from the above command.

   ```
   oracle      300   dba          26001    Oracle Account
                     oinstall     26002
   ```

   If the line does not exist, use the following command to add the oracle user assigned to the dba group:

   # /usr/sbin/useradd -u 300 -g dba -c “Oracle Account” -d /<install_drive>/app/oracle -s /bin/csh oracle

   Set the Oracle password to your desired value using the UNIX passwd process.

   #passwd oracle

   If an Oracle account already exists, verify that the login directory is correct. Change the password, if desired.

4. Create the following directories, if they do not already exist.

   ```
   % su -
   # mkdir -p /<install_drive>/app/oracle
   # chown oracle:dba /<install_drive>/app/oracle
   # chmod 755 /<install_drive>/app/oracle
   # mkdir -p /<driveA>/app/oracle
   # chown oracle:dba /<driveA>/app/oracle
   # chmod 755 /<driveA>/app/oracle
   # mkdir -p /<driveB>/app/oracle
   # chown oracle:dba /<driveB>/app/oracle
   # chmod 755 /<driveB>/app/oracle
   ```

5. Set up the automount map. If your system uses automount maps, edit /etc/auto_apps and add the following line:

   ```
   oracle   -intr,rw,nosuid   systemname:path
   ```

Example:

```
oracle   -intr,rw,nosuid  Mysystem:/<install_drive>/app/oracle
```

See Section 2.1.1.2, Automounting and FEMIS, for more information.

6. Make sure there is adequate shared memory. Examine the following parameters in the /etc/system file.

```
set shmsys:shminfo_shmmax=4294967295
set shmsys:shminfo_shmmin=1
set shmsys:shminfo_shmmni=400
set shmsys:shminfo_shmseg=36
set semsys:seminfo_semmni=256
set semsys:seminfo_semmsl=600
set semsys:seminfo_semmns=1800
set semsys:seminfo_semopm=100
set semsys:seminfo_semvmx=32767
```

If there are no parameters, copy them from the template. As root, set them to the recommended values shown above or as high as possible for the operating system.

A copy of the recommended values can be found in

/home/femis/install/oracle_template/kernel_parms.dat

Note: If any of these parameters are changed, you must reboot the server (as root, use the init 6 command to reboot) before proceeding.

7. Verify there is at least two times (preferably three) as much swap space as physical RAM (a minimum of 400MB is recommended). If additional swap space is required, see your System Administrator.

To determine how much physical RAM you have, enter the following command:

```
# prtconf | grep size
```

Note: At least 128MB of RAM are required for Oracle v8.1.6 installation.

To determine the available swap space, enter the following command:

```
# /usr/sbin/swap –s
```

8. Verify that the necessary Solaris 7 patches and packages are installed prior to installing Oracle.

   Solaris 7 107636-01

   #> showrev -p | grep 107636

   Packages

   #> pkginfo -i SUNWarc SUNWbtool SUNWhea SUNWlibm SUNWlibms SUNWsprot SUNWtoo

   If any of the patches and/or packages above are not displayed as installed, then install them.

9. Verify there is a local bin directory /usr/local/bin. If the directory does not exist, then it should be created as root.

10. Create the /var/opt/oracle directory, if it does not exist.

    ```
    #> mkdir -p /var/opt/oracle
    #> chown -R oracle /var/opt/oracle
    #> chgrp -R dba /var/opt/oracle
    #> chmod -R 755 /var/opt/oracle
    ```

11. Log completely off and back onto the server as oracle.

12. Copy the template files to the admin directory.

    ```
    % cp -r /home/femis/install/oracle_template/* /<install_drive>/app/oracle/admin
    % chown -R oracle /<install_drive>/app/oracle/admin
    % chgrp -R dba /<install_drive>/app/oracle/admin
    % chmod -R 755 /<install_drive>/app/oracle/admin
    ```

13. Create the product directories, if they do not exist.

    ```
    % mkdir -p /<install_drive>/app/oracle/product/8.1.6
    % chown -R oracle /<install_drive>/app/oracle/product
    % chgrp -R dba /<install_drive>/app/oracle/product
    % chmod -R 755 /<install_drive>/app/oracle/product
    ```

14. Copy the new Oracle UNIX setup file to the installation directory.

    Note: If you previously had FEMIS installed, you should compare your existing configuration files with the new ones. If your existing files have been customized, then do not overwrite them but perform Step 14 to make sure the values are still correct for this server.

```
% cd /<install_drive>/app/oracle/admin
% cp -p oracle.mycshrc /<install_drive>/app/oracle/.mycshrc
% cp -p oracle.cshrc /<install_drive>/app/oracle/.cshrc
% cp -p oracle.oraclerc /<install_drive>/app/oracle/.oraclerc
% cp -p oracle.login /<install_drive>/app/oracle/.login
```

15. Make sure the following environment variables are correct in .oraclerc file.

```
ORACLE_TERM (set it to match the xterm for the given keyboard: xsun or xsun5)
ORACLE_BASE = /<install_drive>/app/oracle
ORACLE_HOME = /$ORACLE_BASE/product/8.1.6
PATH includes:
    $ORACLE_HOME/bin
    /etc
    /usr/local/bin
    /bin
    /usr/bin
    /usr/ccs/bin
ORACLE_SID = fi<x>
ORACLE_DOC = $ORACLE_BASE/doc
CLASSPATH = $ORACLE_HOME/JRE:$ORACLE_HOME/jlib
LD_LIBRARY_PATH = /usr/lib:/usr/dt/lib:/usr/ucblib:/usr/openwin/lib:$ORACLE_HOME/lib
ORACLE_EXPORT = /<driveA>/app/oracle/admin/fi<x>/exp
ORACLE_LOGS  = /<driveA>/app/oracle/admin/fi<x>/logs
ORACLE_FULL = /<driveB>/app/oracle/admin/fi<x>/full
ORACLE_COLD = /<driveB>/app/oracle/admin/fi<x>/cold
```

16. Create the directories that Oracle uses for database backups.

```
% source .oraclerc
% cd /<install_drive>/app/oracle/admin
% ./dbbackup_setup
```

This executable will check on needed environment variables and then create directories. If any errors are reported, correct them and then rerun the setup process.

17. Patch the dbstart script with the following commands (assumes you are still in /<install_drive>/app/oracle/admin):

```
% cp dbstart $ORACLE_HOME/bin
```

2.3.3.2 Installing the Oracle Software

Complete the following steps to install the Oracle v8.1.6 software.

1. Log completely off and back onto the server as oracle with the group set to oinstall.

   % newgrp oinstall
   % id should return something like uid=26000(oracle) gid=26002(oinstall)

2. Insert the Oracle8 Server v8.1.6 CD into the CD drive.

3. Mount the CD

   $ cd /cdrom/oracle8i

4. Run the installer.

   ./runInstaller &

5. Install the Oracle products. After the Universal Installer comes up, perform the following operations at the indicated windows.

   WELCOME — Click Next.

   FILE LOCATIONS —Verify Destination path settings, then click Next.

   UNIX GROUP NAME —Type in oinstall in the space provided. (This window may not display.)

   AVAILABLE PRODUCTS — Select the Oracle 8i Enterprise Edition 8.1.6.0.0, then click Next.

   INSTALLATION TYPES — Select Custom, then click Next.

   AVAILABLE PRODUCTS COMPONENTS — Select the following components (a check mark indicates a selected product); the plus (+) and minus (–) signs expand or contract the upper level menus:

   – ☑ Oracle 8I Enterprise Edition 8.1.6.0.0
   – Product Options
   – ☑ Oracle 8i Server 8.1.6.0.0
   – Optional
   ☑ Oracle Database Configuration Assistant 8.1.6.0.0
   ☐ Oracle Data Migration Assistant 8.1.6.0.0
   ☐ Oracle Database Demos 8.1.6.0.0
   ☑ Advanced Replication 8.1.6.0.0
   ☐ Legato Storage Manager 8.1.6.0.0
   ☐ Migration Utility 8.1.6.0.0
   ☑ Oracle Intelligent Agent 8.1.6.0.0
   ☐ Oracle Partitioning 8.1.6.0.0
   ☑ Heterogeneous Services ODBC Connectivity 8.1.6.0.0

–☐ Oracle Product Options 8.1.6.0.0
- ☐ Oracle Time Series 8.1.6.0.0
- ☐ Oracle Visual Information Retrieval 8.1.6.0.0 0
- –☐ Oracle Spatial 8.1.6.0.0
  - +Optional
- ☐ Oracle Advanced Security 8.1.6.0.0
- –☐ Oracle interMedia 8.1.6.0.0
  - +Optional

–☑ Net 8 Products 8.1.6.0.0
- ☑ Net 8 Client 8.1.6.0.0
- ☑ Net 8 Server 8.1.6.0.0
- ☐ Oracle Names 8.1.6.0.0
- ☑ Oracle Connection Manager 8.1.6.0.0
- ☐ External Naming: NIS 8.1.6.0.0
- ☑ Oracle Protocol Support 8.1.6.0.0

-☑ Oracle Utilities 8.1.6.0.0
- ☑ Oracle Database Utilities 8.1.6.0.0
- ☑ SQL*Plus 8.1.6.0.0

-☑ Oracle Configuration Assistants 8.1.6.0.0
- ☐ Oracle Database Migration Assist 8.1.6.0.0
- ☑ Oracle Database Configuration Assistant 8.1.6.0.0

-☑ Development Tools 8.1.6.0.0
- ☑ Oracle Call Interface (OCI) 8.1.6.0.0
- ☑ Object Type Translator 8.1.6.0.0

-☑ Oracle Java Products 8.1.6.0.0
- ☑ Oracle JDBC Drivers 8.1.6.0.0
  - ☑ Oracle JDBC/OCI Driver for JDK 1.18.1.6.0.0
  - ☑ Oracle JDBC/OCI Driver for JDK 1.28.1.6.0.0
  - ☑ Oracle Thin Driver for JDK 1.18.1.6.0.0
  - ☑ Oracle Thin Driver for JDK 1.28.1.6.0.0
- ☑ Oracle SQLJ 8.1.6.0.0
- ☑ Oracle Java Tools 8.1.6.0.0

+☐ Oracle Enterprise Manager Products 8.1.6.0.0

–☑ Oracle Installation Products 8.1.6.0.0
- ☑ Oracle Universal Installer 1.7.0.18.0A

☑ Solaris Documentation 8.1.6.0.0

Click Next.

COMPONENT LOCATIONS — Click Next.

PRIVILEGED OPERATING SYSTEM GROUPS (change to dba) — Click Next.

CREATE DATABASE — Select NO, then click Next.

ORACLE PROTOCOL SUPPORT — Click Next.

SUMMARY — Review your selections. You will probably see more products than you selected (some are required to support your selections), but as a minimum, you should see the products that were originally selected. Click the Install button if your selections are correct. If they need to be revised, then click on the Previous button and revise selections.

Edit the root.sh file. Comment with a # any lines containing the text "$CHOWN root" and "$CHMOD 6??? or 4???" (where ??? = three permission digits).

As root, execute the root.sh. When prompted by the following: Enter the full pathname of the local bin directory, accept the default path. When prompted, dismiss the Setup Privileges window.

CONFIGURATION TOOLS — auto-defaults to NET8 CONFIGURATION ASSISTANT — Click Cancel and confirm Yes.

ERROR (Triggered from the previous step – ignore) — Click OK.

CONFIGURATION TOOLS — Click Next, then Exit, and confirm Yes.

6. Create the database using the Database Creation Assistant.

   At the O/S prompt, verify that you are part of the dba group by typing id and enter.

   ```
   % newgrp dba
   % id should return uid=26000(oracle) gid=26001(dba)
   ```

   Then change directory to the new ORACLE_HOME and run the Database Creation Assistant.

   ```
   cd $ORACLE_HOME/bin
   ./dbassist &
   ```

7. After the Database Creation Assistant comes up, perform the following operations at the indicated windows:

   ORACLE DATABASE CONFIGURATION ASSISTANT
   - Select Create a database, and click Next.
   - Select Custom, and click Next.
   - Select Multipurpose, and click Next.
   - Change Concurrently connected users to 35, and click Next.
   - Select Dedicated Server Mode, and click Next.
   - Verify a box is checked for each of the following: Oracle JServer, Advanced Replication, SQL*Plus Help
   - Click Next to continue.

Enter the Global Database Name, and click Next.

Example: fi1

Note: If an Alert window regarding an instance is already in use, choose another instance name. Acknowledge the Alert by clicking OK. Edit the /var/opt/oracle/oratab file to remove the offending instance line, and click Next. Then, you may get the Alert window described below.

If an Oracle Database Configuration Assistant Alert window appears, click the Yes button and proceed. This removes the old folder with the same instance name in the $ORACLE_BASE/admin directory allowing the same instance name to be recreated.

Change the ControlFiles so that each control file has a different number in the /filesX line whereX = 0....n.

Example: /files0, /files1, /files2

Click Next.

Create tablespaces, for each tabbed tablespace input the following parameters (Create file locations based on your best judgement of space available and disk usage).

SYSTEM

Size (MB):	400
File:	(Verify the File Location)
Autoextend:	YES
Next (KB):	1000
Min Extent (KB):	1000
% Increase:	0
Initial (KB):	100
Next (KB):	100
Min:	1
Max:	Check “Unlimited”

TOOLS

Size (MB):	50
File:	(Verify the File Location)
Autoextend:	YES
Next (KB):	1000
Min Extent (KB):	1000
% Increase:	0
Initial (KB):	100
Next (KB):	100
Min:	1
Max:	Check “Unlimited”

USERS

Size (MB):	5
File:	(Verify the File Location)
Autoextend:	OFF
Min Extent (KB):	1000
% Increase:	0
Initial (KB):	100
Next (KB):	100
Min:	1
Max:	Check “Unlimited”

ROLLBACK

Size (MB):	200
File:	(Verify the File Location)
Autoextend:	OFF
Min Extent (KB):	1000
Initial (KB):	1000
Next (KB):	1000
Min:	2
Max:	Check “Unlimited”

INDEX

Size (MB):	(Accept the default)
File:	(Accept the default)
Autoextend:	(Accept the default)
Next (KB):	(Accept the default)
Min Extent (KB):	(Accept the default)
% Increase:	(Accept the default)
Initial (KB):	(Accept the default)
Next (KB):	(Accept the default)
Min:	(Accept the default)
Max:	(Accept the default)

TEMPORARY

Size (MB):	50
File:	(Verify the File Location)
Autoextend:	OFF
Min Extent (KB):	1000
Initial (KB):	500
Next (KB):	500

Note: SYSTEM, ROLLBACK, and TEMPORARY should be on different disk devices to distribute I/O.

Click Next.

Ignore the Redo Log settings (these will be updated by post-generation modifications.), and click Next.

Ignore the Checkpoint settings, leave the Enable Archive Log box unchecked, and click Next.

Change the following parameters as indicated:

Block Buffers 8192
Processes 300
Block Size 4096

Click Next.

Leave the Trace File Directory settings intact and click Next.

Select the Save information to a shell script setting, and click Finish. In the _popup window, accept the default location and enter the file in the format of <sid>master.sh (Example: fi1master.sh). Click OK to save the file. Acknowledge the alert windows that indicate the status of the file creations.

8. Change directory to the location of the saved scripts generated in the previous step:

```
% cd $ORACLE_HOME/assistants/dbca
% ls -l fi*.sh
```

This should produce a listing of scripts as per the example below:

```
% ls -la fi*.sh
-rwxr-xr-x   1 oracle   dba        214 Feb 10 20:22 fi1alterTablespace.sh
-rwxr-xr-x   1 oracle   dba        639 Feb 10 20:22 fi1java.sh
-rwxr-xr-x   1 oracle   dba        548 Feb 10 20:22 fi1master.sh
-rwxr-xr-x   1 oracle   dba        253 Feb 10 20:22 fi1replicate.sh
-rwxr-xr-x   1 oracle   dba        682 Feb 10 20:22 fi1run.sh
-rwxr-xr-x   1 oracle   dba       4004 Feb 10 20:22 fi1run1.sh
-rwxr-xr-x   1 oracle   dba        452 Feb 10 20:22 fi1run2.sh
-rwxr-xr-x   1 oracle   dba        188 Feb 10 20:22 fi1sqlplus.sh
```

9. Review and edit the scripts that are displayed in Step 8 above; make changes as indicated below to the named scripts:

- fi*run.sh

Add the following under maxlogfiles 32.

maxlogmembers 4

Add the following text MAXSIZE 800M to the end of the line DATAFILE '<file>' SIZE 400M AUTOEXTEND ON NEXT 1000K.

Replace the LOGFILE component with the following change, editing for the correct file and instance names.

```
logfile
  GROUP 1 ('/<install_drive>/app/oracle/oradata/fi9/redo01a.log',
    '/<driveA:>/app/oracle/oradata/fi9/redo01b.log' ,
    '/<driveB:>/app/oracle/oradata/fi9/redo01c.log') SIZE 10M,
  GROUP 2
    ('/<install_drive>/app/oracle/oradata/fi9/redo02a.log',
    '/<driveA:>/app/oracle/oradata/fi9/redo02b.log' ,
    '/<driveB:>/app/oracle/oradata/fi9/redo02c.log') SIZE 10M;
```

- fi*run1.sh

Make the following changes to the fi*run1.sh file:

1) Add the following text “MAXSIZE 200M” to the end of the line “CREATE TABLESPACE TOOLS DATAFILE ‘<file>’ SIZE 50M REUSE AUTOEXTEND ON NEXT 1000K”.
2) Limit rollback segments to 6 (RBS0 - RBS5); delete others

10. Verify the ORACLE_SID entry. If it is not set, set it appropriately (instance name), change directory to the pfile directory for the instance and review/change the init.ora script, as per the example below.

```
% setenv ORACLE_SID  <fi#>
% cd $ORACLE_BASE/admin/$ORACLE_SID/pfile
% mv init<SID#>.ora init<SID#>.org
```

Then copy the sample init.ora file and edit per the following example:

```
% cp /<install_drive>/app/oracle/admin/initfix.ora  ./initfi<SID#>.ora
% vi init<SID#>.ora
```

where <SID#> is the instance number.

Edit the init.ora file to replace instance, and file specific values that are different from the original file. Verify that rollback segment, and control file names and locations are correct. Update the path for the log_archive_dest_1 parameter (it should match $ORACLE_LOGS/arch).

Note: The control file disk spindles in the init.ora file **must match** the ones that were specified in the Database Creation Assistant (dbassist). To verify they match, check the init<SID#>.org file that you created above.

11. Verify that all database file directories exist before executing the database creation script.

```
% ls -la /*/app/oracle/oradata/$ORACLE_SID
% ls -la $ORACLE_BASE/admin/$ORACLE_SID (check for bdump, cdump, udump)
```

12. Change directory to the location of the database creation scripts and execute the master script, as per the example below:

    Note: This is a time consuming task and may take up to several hours, depending upon the speed of your system. You may see many ORA-04132 errors regarding nonexistent objects. These will be created and are normal output.

    ```
    % cd $ORACLE_HOME/assistants/dbca
    % ./<SID>master.sh
    ```

    Note: If during the process of creating the database, the orapwd file is corrupt or missing it will need to be recreated. To recreate the orapwd file, enter the following commands:

    ```
    cd $ORACLE_HOME/dbs
    orapwd file=orapw<SID> password=<create a password>  entries=<a number>
    ```

    You will have to re-execute the master script at the beginning of Step 12.

13. Review database creation log files for errors.

    ```
    % cd $ORACLE_BASE/admin/$ORACLE_SID/create
    % ls -lat *.log
    % grep ORA- *.log | more
    ```

14. Change the password for the SYS and SYSTEM accounts, via svrmgrl, as per the example below:

    ```
    SVRMGR> connect internal
    SVRMGR> alter user sys identified by dba<SID#>;     (for example for fi6 use dba6)
    SVRMGR> alter user system identified by dba<SID#>;     (for example for fi6 use dba6)
    ```

15. Create an oracle user account to permit scheduled exports, using svrmgrl, by copying and pasting the following text into the svrmgrl session:

    ```
    SVRMGR> connect internal
    SVRMGR> CREATE USER "ORACLE"  PROFILE "DEFAULT"
    2> IDENTIFIED EXTERNALLY
    3> DEFAULT TABLESPACE "USERS"
    4> TEMPORARY TABLESPACE "TEMP"
    5> QUOTA UNLIMITED ON TEMP
    6> QUOTA UNLIMITED ON USERS
    7> ACCOUNT UNLOCK;
    SVRMGR > GRANT "CONNECT" TO "ORACLE";
    SVRMGR > GRANT "EXP_FULL_DATABASE" TO "ORACLE";
    SVRMGR > ALTER USER "ORACLE" DEFAULT ROLE  ALL;
    ```

16. Edit the oratab, as oracle, in /var/opt/oracle and change the third field from no (N) to yes (Y) so that the database is brought up when the server is rebooted. Also make sure that the path is preceded by ORACLE_SID parameter followed by a colon as shown below (the example is for a database instance with ORACLE_SID = fi1).

    fi1: /<install_drive>/app/oracle/product/8.1.6:Y

17. Login in as root and copy a file named dbora into the /etc/init.d directory, if it does not already exist.

    ```
    # cp /<install_drive>/app/oracle/admin/dbora /etc/init.d/dbora
    # ls –la /etc/init.d/dbora
    ```

18. Link dbora by entering the following:

    ```
    % ln -s /etc/init.d/dbora /etc/rc0.d/K10dbora
    % ln -s /etc/init.d/dbora /etc/rc2.d/S99dbora
    ```

19. Remove any previous versions of Oracle startup scripts by completing the following:

    ```
    # cd /etc/init.d
    # rm  oracle
    # cd  ..
    # rm -i rc?.d/[KS]*oracle
    ```

20. Reserve a port for the Net8 listener by making the following entry in the /etc/services file (insert this in port number sequence).

    ```
    listener_name 1521/tcp        # Net8 listener
    ```

21. Copy the original SQL*Net files (sqlnet.ora, listener.ora, tnsnames.ora) from /var/opt/oracle to the $ORACLE_HOME/network/admin directory (they are compatible with Net8).

    ```
    % cd $ORACLE_HOME/network/admin
    % cp /var/opt/oracle/*.ora .
    ```

    Change the hostname, instance name, and $ORACLE_HOME path to the correct identity for the server that you are working on.

    If the copy command above fails, enter the following commands:

    ```
    % cd /<install_drive>/app/oracle/admin
    % cp -p listener.ora tnsnames.ora sqlnet.ora $ORACLE_HOME/network/admin
    ```

    Modify the files in the destination path to match your site's server and database instance names. Be sure to include listener definitions for the whole site in the tnsnames.ora file.

22. Verify the listener status.

    % lsnrctl
    LSNRCTL>status

    If the response to the status command lists a summary of approximately 10 parameters, and one of these is uptime, then the listener is running. Exit by typing:

    lsnrctl>exit

    If the listener is not working, then start it by typing:

    lsnrctl>start

23. Switch user to femis and link the oracle environment parameter file to the femis home directory to preserve environment file setting integrity.

    % su - femis
    % ln –s ~oracle/.oraclerc

24. Switch user to oracle, and put the database in archive mode.

    % su - oracle
    % svrmgrl
    SVRMGR> connect internal
    SVRMGR> shutdown immediate
    SVRMGR> startup mount;
    SVRMGR> alter database archivelog;
    SVRMGR> archive log list;
    SVRMGR> shutdown immediate
    SVRMGR> startup
    SVRMGR> exit

2.3.3.3 Installing and Using Oracle Documentation

Note: The following application are required to view the Oracle documentation:

HTML: Netscape Navigator 3.0 (or higher) or Microsoft Internet Explorer 3.0 (or higher).
PDF: Acrobat Reader 3.0 (or higher) or PDFViewer Web browser plug-in 1.0 (or higher).

Complete the following steps to install the Oracle v8.1.6 software.

1. Log completely off and back onto the server as oracle with the group set to oinstall.

   % id should return something like uid=26000(oracle) gid=26002(oinstall)

2. Insert the Oracle8i On-Line Generic Documentation CD into the CD drive.

3. Mount the CD

   $ cd /cdrom/816_docs

4. Run the installer. Click Next on the Welcome window.

   runInstaller &

5. Select a product to install, when prompted by the installer, navigate to the CD-ROM, and locate the file /INSTALL/docs_816.jar. Select this file as your source.

   Install the documentation into the $ORACLE_DOCS directory that exists if a previous version of Oracle has been installed. If the directory does not exist, see Step 3 in Section 2.3.3.5, Configuring Existing Oracle for Latest Version of FEMIS. If $ORACLE_DOCS is set, the documentation will be installed there regardless of the destination setting specified in this window.

   Click Next to verify the product list is correct.

   Click Install on the Verification window.

To view the HTML and PDF documentation from a local installation or from the CD-ROM, follow these steps:

1. Use your browser to open the top-level index.htm file within the installed documentation directory.

   Note: If you do not wish to launch the Information Navigator Java applet, open the file products.htm instead of index.htm.

2. Click on the category of documentation you wish to view (Server and Data Warehousing, Application Development, Networking and Security, Parallel Server, interMedia, Java, or WebDB).

3. Click on the HTML or PDF link, on the resulting product-level index file, corresponding to the book you wish to view. Clicking the HTML link takes you to the table of contents for that book; clicking the PDF link displays the appropriate document using your installed Acrobat products or your browser's Acrobat plug-in.

2.3.3.4 Relinking the Oracle Software

Note: If you have Oracle v8.1.6 installed but were required to install, upgrade, or patch the operating system, then complete this section to relink the Oracle software.

If you just completed the steps in Section 2.3.3.2, Installing the Oracle Software, then skip this section because Oracle has already been relinked.

1. Shutdown Oracle by logging in to UNIX as the oracle user and complete the following:

   ```
   % svrmgrl
   SVRMGR>connect internal
   SVRMGR>shutdown immediate
   SVRMGR>exit
   ```

2. Relink the Oracle software.

   ```
   % cd $ORACLE_HOME/bin
   % relink all
   ```

   This process may take several minutes to complete. It will produce a large amount of output, which is normal. Some error output will occur regarding portions of Oracle that are not installed, which is normal. As long as the last messages prior to link completion do not indicate fatal errors, you can assume the link was successful.

3. Restart Oracle.

   ```
   % svrmgrl
   SVRMGR>connect internal
   SVRMGR>startup
   SVRMGR>exit
   ```

2.3.3.5 Configuring Existing Oracle for Latest Version of FEMIS

Note: If you already had Oracle v8.1.6 installed and are upgrading FEMIS, then you **must complete** this section.

If you have just installed Oracle per the steps in Section 2.3.3, Installing Oracle or Relinking Oracle, then skip this section, and go to Section 2.3.4, Defining the Database Topology.

1. Copy the template files to the admin directory.

   ```
   % cp -r /home/femis/install/oracle_template/* /<install_drive>/app/oracle/admin
   % chown -R oracle /<install_drive>/app/oracle/admin
   % chgrp -R dba /<install_drive>/app/oracle/admin
   % chmod -R 755 /<install_drive>/app/oracle/admin
   ```

2. Copy the new Oracle UNIX setup files to the installation directory.

   Note: If you previously had FEMIS installed, you should compare your existing configuration files with the new ones. If your existing files have been customized, then **do not overwrite** them but complete Step 3 to make sure the values are still correct for this server.

```
% cd /<install_drive>/app/oracle/admin
% cp -p oracle.mycshrc /<install_drive>/app/oracle/.mycshrc
% cp -p oracle.cshrc /<install_drive>/app/oracle/.cshrc
% cp -p oracle.oraclerc /<install_drive>/app/oracle/.oraclerc
% cp -p oracle.login /<install_drive>/app/oracle/.login
```

3. Make sure the following environment variables are correct. Also make sure that all directories specified by the parameters exist and have their owner, group owner, and mode set to oracle, dba, and 755 respectively. These can be set using the chown, chgrp, and chmod commands.

```
ORACLE_TERM (set it to match the xterm for the given keyboard: xsun or xsun5)
ORACLE_BASE = /<install_drive>/app/oracle
ORACLE_HOME = /$ORACLE_BASE/product/8.1.6
PATH includes:
    $ORACLE_HOME/bin
    /usr/local/bin
    /bin
    /usr/bin
    /usr/ccs/bin
ORACLE_SID = fi<x>
ORACLE_DOC = $ORACLE_HOME/doc
LD_LIBRARY_PATH=/usr/lib:/usr/dt/lib:/usr/ucblib:/usr/openwin/lib:/$ORACLE_HOME/lib
        /usr/openwin/lib:
ORACLE_EXPORT = /<driveA>/app/oracle/fi<x>/export
ORACLE_LOGS  = /<driveA>/app/oracle/fi<x>/logs
ORACLE_FULL = /<driveB>/app/oracle/fi<x>/full
ORACLE_COLD = /<driveB>/app/oracle/fi<x>/cold
CLASSPATH = $ORACLE_HOME/JRE:$ORACLE_HOME/jlib
```

4. Switch user to femis and copy the oracle environment parameter file to the femis home directory.

```
% su - femis
% cd ~oracle
% cp .oraclerc /home/femis/.oraclerc
```

2.3.3.6 Modifying the Initialization Parameter

Due to changes in FEMIS, one of the Oracle initialization parameters may need updating. To determine if changes are necessary, log into UNIX as the oracle user and check the following:

```
%  su - oracle
%  cd $ORACLE_BASE/admin/$ORACLE_SID/pfile
% vi  init<$ORACLE_SID>.ora
```

Look for an entry in this file, e.g., initfi2.ora, like open_cursors = 800. If this line is not present, add it; or if the line exists but the number is less than 800, change the value to 800. If changes are made, the database must be shutdown and restarted (using the following commands) to make the change active.

```
% svrmgrl
SVRMGR> connect internal
SVRMGR> shutdown immediate    Wait until the database is down, then:
SVRMGR> startup
SVRMGR> exit
```

2.3.4 Defining the Database Topology

Note: This section **must be completed** regardless if this is a new or upgrade installation of FEMIS.

Six configuration files are used to define a topology:

/home/femis/etc/eoclist.dat	EOC List	general topology
/home/femis/etc/grplist.dat	Group List	snapshot groups
/home/femis/etc/seqlist.dat	Sequence List	sequence Ids
/home/femis/etc/tablist.dat	Table List	Table privileges
/home/femis/etc/vuelist.dat	View List	Views
/home/femis/etc/eocnum.dat	EOC Numbers	for this site

The primary configuration file is the EOC List file, ./etc/eoclist.dat, which is used by many of the FEMIS shell scripts. The other configuration files are used only by the Make Configuration (makecfg.sh) code generator.

The EOC List file consists of one record for each EOC database. Each record consists of eight space-separated columns. Except for the Yes/No flag in column five, nothing should be uppercase.

1: EOC name	name of the EOC and Oracle user account
2: Password	initial password for the Oracle user account
3: Server	server where the data is located
4: Listener	Oracle listener name for the account
5: Onpost	Y=onpost database, N=offpost database
6: EOC #	EOC number used for sequence IDs
7: Port	FEMIS notification port
8: Other EOCs	Comma-separated list of other EOCs on this server, w/o white space. If none, then 0 is used.
9: Remote EOCs	Comma-separated list of remote EOCs, w/o white space. If none, then 0 is used.

The Group List file is used to define the database replication setup. It indicates which tables go in which replication groups, plus which tables must have what kind of snapshots. It contains N major sections, the first one normally for just the one onpost EOC (e.g., tead), and the remaining ones for the offpost EOCs (e.g., ctoo and utst). The onpost section is different from the offpost sections, which are alike except for the EOC name in the first column.

The Sequence List file is used to define the Oracle sequence IDs in the database, which are used to generate unique keys when inserting records into the database.

The tablist.dat file controls table privileges for database users. It has one row for each table in the database. It is possible to modify this file at the time of this installation but extreme care must be taken. See Section 4.5, Security Provisions, in the ***FEMIS Data Management Guide*** for a description of the format of this file.

The View List file is used to define which views are created on which tables. The views combine data from other EOCs into a site-wide version of shared tables. For example, the S_FACILITY view is a combination of the Facility tables in each of the EOC databases.

The eocnum.dat file is the basic file that determines the names of the EOCs at a site and assigns an EOC number to each. This file is used by the Build Topology Program, bldtopo.sh and is placed into the /home/femis/etc directory as part of the initial installation of a site's database package. It is preserved throughout the installation of the FEMIS package (Section 2.2.2, Upgrading the FEMIS Application, Step 2).

2.3.4.1 Running the Build Topology Program

To define a topology, you must create the configuration files and put them in a standard location using the Build Topology program.

1. Login as femis.

2. Copy the eocnum.dat file if you have never installed a database package.

   % cp /home/femis/database/exports/<site name>/eocnum.dat /home/femis/etc

3. Create the configuration files, and place the files in a standard location.

   %cd ~femis/etc
   % ~femis/database/dba/bldtopo.sh

The Build Topology program prompts you for information to define the general topology–the EOC List file. If at any point you do not specify something, the program will exit.

How many servers? ==>

Enter the number of servers in the topology. For example, for a 3x1, enter 1; for a 6x6, enter 6; or for a 8x4 enter 4.

The build topology program reads the eocnum.dat file and displays the information back to the window.

Enter server name for <eoc_name> ==>

Each time you get this prompt, you must enter the name of the Sun server where the FEMIS database for the EOC that is listed will reside. For example, for the CTOO database, enter tcemsun.

```
Enter listener for <eoc_name>       ==>
```

Enter the Oracle listener name for that server. For example, fi3.

The loop then repeats, asking for the next server and listener until you have supplied all of them. If you have specified an Nx1 topology, then the script will ask you for the server and listener name only once.

After you answer all the prompts, the Build Topology program creates the remaining topology files automatically.

2.3.4.2 Setting Up the EOC DBA Directory (as femis)

As released, FEMIS contains a ~femis/database directory that has a number of subdirectories, none of which should be changed. However, for your own use, you need a working copy of some of the files. Plus, you need to generate brand new SQL scripts that are specific to your database topology. When you have completed the following steps, you will have your own ~femis/database/eocdba directory with all the scripts you will need to manage your FEMIS database.

1. Login as femis.

2. Create a working directory, eocdba, for your own use.

   ```
   % cd ~femis/database/dba
   % mkeocdba.sh
   ```

3. Generate the scripts used to load the stored procedures.

   ```
   % cd ~femis/database/eocdba
   % makeproc.sh
   ```

   This shell script creates the driver scripts to create (master_cr_procedures.sql) and drop (master_dr_procedures.sql) the stored procedures in all the FEMIS EOC database schemas. The shell script also creates all the actual server-specific files, cr_procedures_SERVER.sql and dr_procedures_SERVER.sql.

4. Generate the scripts used to manage and control the database.

   ```
   % cd ~femis/database/eocdba
   % makecfg.sh
   ```

This shell script creates a very large number of SQL scripts.

Note: It is essential that all FEMIS servers use the same database topology. Be sure to copy the eocdba and etc directories to all servers in the configuration since every server needs the same files.

2.3.5 Creating or Updating the FEMIS Database

Complete the following sections to create or update the FEMIS database.

2.3.5.1 Creating the Database Schemas

The following steps **must be completed** on each server in the site configuration. **Verify that the files in both the /home/femis/etc and /home/femis/database/eocdba directories were copied to all servers** (See Section 2.3.4.1, Running the Build Topology Program). Complete the following steps to create the database schemas.

1. Login as femis.

2. Change to the ~femis/database/eocdba directory.

   % cd ~femis/database/eocdba

3. Skip this step if you are updating the database; the tablespaces already exist.

   To place the files in the desired directory(s), edit the cr_db_ts_<sever name>.sql file. If possible, place the fmain and findex tablespaces on different disk drives. Place the fsnapshot and fsnaplog tablespaces on different disk drives as well. For example:

fmain.dbf	/<driveA>/app/oracle/oradata/fi<x>	300M
findex.dbf	/<driveB>/app/oracle/oradata/fi<x>	400M
fsnapshot.dbf	/<driveA>/app/oracle/oradata/fi<x>	500M
fsnaplog.dbf	/<driveB>/app/oracle/oradata/fi<x>	200M

   Note: An Nx1 configuration will not have the last two shapshot definition lines above.

4. Run the Master Create Database script for either a new installation or an update.

   Note: Before continuing, this script **must be executed** at each server in the configuration while logged onto the server locally as femis.

   This script creates the new tablespaces and schemas. If you are performing an update, then you will receive error messages stating that the tablespaces and some of the data schemas already exist. Disregard these messages during the update.

Note: In FEMIS v1.4.7, **Oracle's sys schema is required to run the master_cr_db script**. In some previous versions, the system schema was required to run this script.

```
% sqlplus /nologin
SQL> @master_cr_db_<server name>.sql
```

Enter <Sys Password> when prompted.

2.3.5.2 Loading Data (as femis)

Note: Depending on what installation steps you have previously completed, you will either update the data in your database, or import data from one of two places and perform the update. Please review this section carefully.

If you installed Oracle v8.1.6 and had a previous version of FEMIS installed, then you will want to import the data that was exported in Step 2 of Section 2.3.2.1, Dropping Database Objects and Exporting Data Owners.

If you did not have a previous version of FEMIS and have installed the GIS and database package (Section 2.3.1, Installing the GIS and Oracle Database), then you will want to import the data found in the /home/femis/database/exports/<site name> directory.

Note: Remember that you need to know where each of the N data owners are for your NxN or NxM database configuration. You will import the data for each data owner exactly one time across all the servers at your site. If you have an NxN configuration, you will perform one import on each server; but for an NxM configuration, some servers will have more than one data owner. You will not import any data into any of the snapshot owners.

1. Login as femis.

2. Complete the Oracle import function.

```
% cd /home/femis/database/exports/<site name>
% imp <USER1>/<PASSWORD> file=<EOC_name>_<EOC_date>.dmp log=<USER1_today's
date>.log
% imp <USER2>/<PASSWORD> file=<EOC_name>_<EOC_date>.dmp log=<USER2_today's
date>.log
...and so on
```

The actual name of the .dmp files will be specific for your site and may contain a date stamp, e.g., anad_19961210.dmp.

The following is an example for an 8x8 Alabama configuration on a server with the ANAD data owner schema and seven snapshot owner schemas.

```
% imp anad/anad file=anad_19961210.dmp log=anad_<today's date>.log
```

2.3.5.3 Upgrading Database from Previous Versions of FEMIS

S T O P

Before continuing, make sure that the imports for all EOCs have been completed.

Note: Perform the following upgrade only if you had FEMIS v1.4.6 installed, and you are upgrading to v1.4.7. When these upgrade scripts are executed the database structure will be modified for all EOCs at your site. Therefore this upgrade process **only needs to be performed once** at one EOC.

1. Run the update structure/data scripts to update all the owner schemas and create the scripts for the upgrade from FEMIS v1.4.6 to v1.4.7. All databases must be up and available during this operation.

```
% su - femis
% cd /home/femis/database/upd/V1.4.6_V1.4.7
% makerun.sh
```

Note: If you prefer to run the update in its entirety and review it later for errors, then you can use the makerun_nopause.sh script to create the update scripts without any pause statements.

2. Run the master_run.sql script when you are sure the makerun.sh script executed successfully. The update scripts will now be run one at a time. There are pause statements scattered liberally throughout the scripts. Watch closely for errors as each script is run.

```
% sqlplus /nologin
SQL> @master_run
```

Note: If you used the nopause shell script and find errors, you may have to start your build process over from the time of the imports.

2.3.5.4 Creating Objects that Share Data (as femis)

S T O P

Before continuing, make sure all servers are online, and the databases for all EOCs are configured for FEMIS v1.4.7.

At this point, you should have schemas on all servers and have loaded the data. You are now ready to create views, snapshots, synonyms, and other replication-support items.

Note: This create process **needs to be performed once**, but it **must be done** on the server that hosts the onpost EOC.

The Master Create SQL script (master_cr.sql) runs scripts that create the following:

sequence numbers	(All)
alternate views	(All)
snapshot logs	(NxN, NxM)
snapshots	(NxN, NxM)
snapshot groups	(NxN, NxM)
synonyms for onpost tables	(All)
site views	(All)
replication tables and code	(NxN, NxM)

To run the Master Create SQL script, which can take hours to complete on a multi-server configuration, complete the following:

1. Login as femis.

```
% cd ~femis/database/eocdba
% sqlplus /nologin @master_cr.sql
```

You need to watch its progress and occasionally press Enter when prompted. If errors occur, use Ctrl-C to stop the script so you can determine what caused the errors.

2.3.5.5 Creating FEMIS Schema Synonyms

The Oracle FEMIS schema at each instance in the database configuration requires a set of synonyms. Upon the successful running of the master_cr.sql script in the previous section, these synonyms have been created for the onpost server only. For each of the offpost servers, complete the following instructions once for each server.

1. Login as femis.

```
% cd ~femis/database/eocdba
%sqlplus /
SQL> @cr_femis_<eoc code>_syn.sql
SQL> exit
```

where the <eoc code> is any one of the data owners located at the server being used.

2.3.5.6 Fixing the EOC Table (as femis)

Run the following script once for all EOCs. It will change the Notify port, the UNIX port, the Server name, and EOC number to match the EOC List file. This process needs to be performed once at one EOC to change the EOC data for all EOCs.

1. Login as femis.

   ```
   % cd ~femis/database/eocdba
   % fixeoc.sh -fix
   ```

2.3.5.7 Setting Up the Oracle Backups

Note: The following **needs to be performed once** on all servers.

To set up the crontabs to perform automatic database backups and exports, complete Steps 1 and 2. To perform a full cold backup, complete Step 3.

1. Switch to the femis user, and enter the following:

   ```
   su – femis
   % cd ~oracle/admin
   % crontab femis.crontab
   ```

   Edit the crontab to replace $HOME with /apps/oracle.

2. Switch to the oracle user.

   ```
   su - oracle
   % cd ~oracle/admin
   % crontab oracle.crontab
   ```

3. Perform a full backup to another directory by entering the following commands:

   ```
   % cd /<install_drive>/app/oracle/admin
   % dbbackup_cold
   ```

For more information on the Oracle backups, see Section 13.0, Backup Strategy for FEMIS, in the ***FEMIS System Administration Guide***.

2.3.5.8 Starting Replication (as femis)

Since neither an NxN nor an NxM configuration store data for all EOCs on each server, the data must be replicated by Oracle to make all of the data accessible to all servers. The following script starts the replication process for your configuration.

If you have an Nx1 database configuration, then skip this step.

Note: The following **only needs to be performed once** at one EOC.
Do not start replication until all the FEMIS databases have been installed and configured on all servers at the site.

To start replication, run the Master Start Replication script.

1. Login as femis

```
% cd ~femis/database/eocdba
% sqlplus /nologin
SQL> @master_rep_start.sql
```

2.3.6 Configuring the FEMIS Files (as root)

Note: The following **needs to be performed once** on all servers.

This section explains how to configure the FEMIS files to accommodate the database topology by running the FEMIS configuration script. Before you run this script, you will need to determine some site-specific values.

Determine the Oracle settings

ORACLE_SID	(Example: fi4)
ORACLE_BASE	(Example: /files1/app/oracle)
ORACLE_HOME	(Example: /files1/app/oracle/product/8.1.6)

The above values can be determined from the Oracle account environment file /apps/oracle/.oraclerc, or by logging into the Oracle account briefly and running the env command.

If DEI was installed, decide upon the following items

FEMX Home Directory	(Default: /home/femx)
EMIS Host Computer	(Example: teadsun)
EMIS User-Name	(Default: femx)
EMIS Password	(Example: femxfer)

The FEMIS configuration script uses the /home/femis/etc/eoclist.dat, system settings, the /home/femis/install/femis_info file, and Oracle database settings to create the FEMIS configuration files, which will be placed in the ./home/femis/etc and /home/femis/configd directories.

Note: Before configuring FEMIS files, you **must know** the EOC name, the EMIS transfer account password, and your UNIX server netmask.

To configure the FEMIS files:

1. Login as root.

2. Change the directory to the FEMIS install directory, usually /home/femis/install.

3. Edit the femis_info file so the values match the system setup.

   The Oracle environment variables should be set to match the values given in the ~oracle/.oraclerc file.

   Note: You must include the explicit file path for the Oracle directories listed in this file. Automount points will not work in this context.

   The FEMIS DEI variables only need to be set, if the server will be running DEI.

   EMIS_HOST should be set to the server name and the EMIS_USER **must be set to emisx.**

4. Change the directory to /home/femis/install/femis_template/etc.

5. Edit the femisdei.cfg file. Remove or comment out (by placing a "#" character at the beginning of the line) the line that starts with ORACLE_USER.

6. Change the directory back to /home/femis/install.

7. Execute the ./configure_files.sh script. Follow the install prompts for EOC name(s), EMIS transfer account password, UNIX server netmask, and whether Samba paths are generated instead of NFS file paths.

2.3.7 Copying files to the /home/femis/user directory

Several files located on the shared directory that PCs map to the M:\ drive are used to patch files and update the Oracle data sources on each PC.

To set this up, you must copy the following files from /home/femis/configd to /home/femis/user.

fupdate.tpl

Also, you must copy the following files from /home/femis/pc/femmisc to /home/femis/user.

odbcsub.vbs
pfemis.vbs

Rename fupdate.tpl to fupdate.bat. When logging in, the FEMIS startup script will execute the FUPDATE.BAT batch file. FUPDATE.BAT can be used to update any file(s) on all FEMIS PCs such as the HOST file or GIS data files. View FUPDATE.BAT for specific instructions.

2.3.8 Correcting Group Ownership

Verify the group ownership is correct on the /home/femis, /home/femis/user, and /home/femis/pc/femtools and that they are in the femisrun group. If it is not correct, enter the following command at the UNIX prompt logged in as root.

```
# chgrp femisrun /home/femis /home/femis/user /home/femis/pc/femtools
```

Verify user account directories group membership with the following command.

```
# find /home/femis/user \! –group femisrun –ls | more
```

Typically, this command should not return anything. If it does, then the return will be a list of files and directories that do not have femisrun group membership. This situation may be occurring by design to protect data in certain accounts. Consult the local administrator to determine if this is the case. If this situation was not intended, then correct with the following command.

```
# find /home/femis/user \! –group femisrun –exec chgrp femisrun {} \;
```

To correct individual users or groups of users use an argument list and/or wildcard notation for the directory list argument(s) to find. For example, to just correct files belonging to the FEMIS users *info* and *train*, the following command would work.

```
# find /home/femis/user/info /home/femis/user/train \! –group femisrun –exec chgrp femisrun {} \;
```

2.3.9 Verifying the Configuration Files (as femis)

Having run the FEMIS configuration script (Section 2.3.6, Configuring the FEMIS Files), you must now verify whether the configuration files it created are correct.

1. Login as femis.

2. Check that the femis account is setup correctly.

```
% env
    USER=femis
    HOME=/home/femis
    SHELL=/bin/csh
    FEMIS_HOME=<full path>
    LD_LIBRARY_PATH=/usr/lib:/$FEMIS_HOME/lib:/usr/ucblib
```

Note: Because of the integration of the contents of .oraclerc file into the femis environment, some paths may be duplicated in LD_LIBRARY_PATH, or PATH (below). The duplication does not cause any known problems and can be left as is. What is critical is that the /usr/lib path be before any /usr/ucblib paths, particularly in the LD_LIBRARY_PATH environment variable.

The ORACLE_SID and ORACLE_HOME environment variables must be set. The values for these are site/server dependent. The ORACLE_SID should be set to the string "fi" followed by a server-specific number. The ORACLE_HOME environment variable will point to the home directory of your Oracle installation.

The PATH environment variable, as a minimum, includes the following:

.:/home/femis:/bin:/usr/bin:/usr/sbin:/$ORACLE_HOME/bin:/etc:/usr/ccs/bin:$FEMIS_HOME/bin:$FEMIS_HOME/database/dba

Note: The PATH variable may include /usr/local/bin on those sites where this directory exists so that remote Secure Shell utilities will work for the femis UNIX account.

3. Verify your have the following files if this is an onpost installation.

   /home/femis/etc/femisdei.cfg
   /home/femis/etc/femisdei.prf

4. Validate the /home/femis/configd/hosts file: The HOSTS file should be configured with the correct host names and IP addresses. This file should be a copy of /etc/hosts on the UNIX system.

5. Validate the /home/femis/configd/addodbc.bat file: FEMIS uses the home/femis/configd/addodbc.bat batch file to add all the necessary ODBC (Open Data Base Connectivity) values. Verify that the mapping from EOC code to listener ID is correct in each line. Copy good version of addodbc.bat to /home/femis/user.

   See Section 4.2.8, Validating I:\USER Directory, for instructions on copying this file so that all the FEMIS PCs are setup with the correct ODBC values.

6. Validate the /home/femis/pc/xntp/ntp.conf file: the ntp.conf file should be configured with the correct IP address for the time server.

   The line beginning with “server” must have the correct IP address of the NTP server, which should be one of the UNIX servers on the WAN.

7. Check the system files to verify the FEMIS entries were added.

   /etc/services
   /etc/inetd.conf

   In the /etc/services file, you should see a service named femis setup for port 1776. In the /etc/inetd.conf file, you should see a femis entry pointing at the full file path of the femisd executable.

8. Check the FEMIS startup/shutdown script.

   /etc/init.d/femis

9. Check the FEMIS dot files.

   /home/femis/.femisrc
   /home/femis/.oraclerc

2.3.10 Setting Up the Command Server Configuration File

The access block in the command server configuration file needs to be set up. This set up **is not done automatically** during installation and needs to be set up manually. If this step is not performed and completed correctly, FEMIS Evacuation and any other program needing the command server will terminate with an Access Denied error.

During FEMIS UNIX installation, the command server configuration file cmdserv.conf is copied to /home/femis/etc. Verify that this file exists.

In the cmdserv.conf file, locate the access block. This block begins with [ACCESS] and ends with [END]. The required directives within the access block are deny and allow. Each directive can contain an IP address and an IP subnet mask. These arguments define the range of IP addresses that are to be allowed or denied access to the command server. Also refer to Section 4.0, FEMIS Command Server, in the ***FEMIS System Administration Guide*** for details on command server syntax.

The correct set up is to deny access by clients on all IP addresses except the ones that specifically are to be allowed. To accomplish this, the first directive should be deny 0.0.0.0, and the remaining directives should be combinations of allow and deny to establish the allowed IP address ranges.

The installer needs to obtain the IP address and subnet mask of the LAN on which the UNIX server was installed, along with the same information for all other LANs on the Wide Area Network (WAN).

As an example, the following block is valid for the Oregon/Washington network:

```
[ACCESS]
Deny        0.0.0.0                         # deny all except
Allow       198.176.0.0     255.255.248.0   # oregon
Allow       199.233.108.0   255.255.255.0   # benton county
Allow       199.47.32.0     255.255.255.0   # washington
Allow       131.92.39.0     255.255.255.0   # umcd
[END]
```

The above example access block is used on all six Oregon/Washington WAN servers.

To allow additional ranges of IP address to access the command server, simply add the appropriate allow directives in the access block.

Do not copy this file from host-to-host, as the file contains host/site dependent fields, such as host name, site name, Oracle instance name, and full Oracle path. Instead, edit each cmdserv.conf file on each host one at a time.

2.3.11 Setting Up femis_event

Note: If all of the UNIX hosts in your WAN have one and only one IP address, then this section can be disregarded. However, if any of the UNIX hosts have dual ethernet interfaces (i.e., they perform router functions, or have multiple IP addresses), then pay special attention to the following workaround.

Interconnections between notification servers are accomplished by including the service port and UNIX host name on the startup command line, e.g., A> femis_event -c 9020@B 9020@C where A, B, and C are names of UNIX hosts. For this example of setting up femis_event, assume that host B has multiple IP addresses, and that all such addresses are included in the /etc/hosts files on A and other nodes on the network.

First determine which IP addresses for B, and all multiple IP address hosts in the network, is the primary IP address for host B. Log into B's femis account, and run femis_event with only the -i option. You should get a response such as the following:

```
B% femis_event -i
Last build ……..… Thu Oct 17 11:54:08 PST 1996
Host name is ..... B
IP address is ….. 111.111.111.111
Port number is ... 9020
```

Next, on all nodes where notification servers are to be executed, ensure there is a unique name in the /etc/hosts which resolves to the IP address reported above. For example:

```
A% grep B /etc/hosts
111.111.111.111 B
111.111.222.222 B
```

Be sure to substitute the actual host names for A, B, and C. Edit and modify the host's file, adding a host, e.g., BB, name which resolves to a unique IP address. For example:

```
A% grep BB /etc/hosts
111.111.111.111 BB
```

From this step forward, you should always refer to the server with multiple IP addresses by the unique name associated with the IP address found in the femis_event-i command. In this example, BB is the IP address name.

Note: Failing to implement the above workaround for UNIX hosts having multiple IP addresses can have disastrous results. Under some conditions, a femis_event process can terminate with a bus error after running out of file descriptors if this workaround is not implemented as described.

2.4 Checking the FEMIS Startup

To check the FEMIS startup, you will need to reboot the server and verify the FEMIS programs are running.

2.4.1 Rebooting the Server (as root)

To activate some of the system-level changes that the FEMIS UNIX Installation script makes, complete the following steps to reboot the server.

Note: If you have an Nx1 database configuration, then skip Steps 1 and 4.

1. Login as femis, and stop master replication.

   ```
   %cd /home/femis/database/eocdba
   %sqplus /nologin @master_rep_stop.sql
   ```

2. Login as root.

3. Enter the following on a Solaris machine:

   ```
   # /etc/init 6
   ```

   As the server reboots, note the status messages during the startup of the FEMIS processes.

4. Login as femis, and start replication.

   ```
   %cd /home/femis/database/eocdba
   %sqplus /nologin @master_rep_start.sql
   ```

2.4.2 Verifying the FEMIS Programs (as femis)

After the server has rebooted, verify that the FEMIS programs are running.

Login as femis.

For an NxN configuration, there should be one FEMIS Notification Server process running. For an Nx1 configuration, there should be N of them running. For an NxM, there should be one FEMIS Notification Server process for each EOC per server in the configuration.

```
% ps -ef | grep femis_event
```

If it is not running, restart it with logging turned on.

```
% startnotify -log
```

Then use the Show Notify utility.

```
% shownotify aux
```

Refer to Section 3.0, FEMIS Notification Service, in the ***FEMIS System Administration Guide*** for more information.

If DEI should be running, check it also.

```
% ps -ef | grep femisdei
```

If it is not running, check the log file home/femis/log/femisdei.log, to see what happened. The most common problem occurs when DEI cannot connect to Oracle. Check the configuration file, /home/femis/etc/femisdei.cfg, and restart DEI by typing femisdei. Refer to Section 7.0, FEMIS Data Exchange Interface (DEI), in the ***FEMIS System Administration Guide*** for more information.

2.5 Utility to Add FEMIS Login Account to the Database

The adduser utility enables you to add a FEMIS login account for a FEMIS user to the database. To use the utility, follow the procedure in the example, substituting the new login account name for wayne.

> **Note:** The adduser.sh script will try to add an account to each database specified using the database password found in /home/femis/etc/eoclist.dat. The second column in this file is the password column. If the database password has been changed for security or other reasons, then this file is kept deliberately out of date. If you need to run adduser.sh against a particular database that has changed its password, temporarily update the /home/femis/etc/eoclist.dat file to contain the proper database password in the second column before actually running the adduser.sh script. After running the script, restore the /home/femis/etc/eoclist.dat to its original condition.

To create a FEMIS login account for wayne, complete the following steps.

1. Login as femis.

2. Run the adduser.sh script with the appropriate command line parameters.

   To add a login account for a specific EOC, run

   ```
   % adduser.sh -user wayne -eoc <eocname> -run
   ```

   where <eocname> must be in lower case.

or

To add a login account on all EOCs in the configuration, run

```
% adduser.sh -user wayne -all -run
```

This script will create and run an SQL script to add the user to the database and give the new user all privileges. It takes a long time to run.

The script does the following:

- Adds a mostly empty record for the user to the PERSON table.
- Adds a record to the FEMIS_USER table.
- Adds many records (>200) to the USER_MODE_PRIV table.

You should then be able to login to FEMIS on the PC as the new user (wayne) with the password femis.

2.6 FEMIS AutoRecovery System Description and Installation

Note: You must have the FEMIS Perl package installed to use AutoRecovery, see Section 2.1.6, Installing Perl v5.004-04.

The FEMIS AutoRecovery system is used to monitor the FEMIS server and application.

The following files are used, generated, or they indirectly affect the FEMIS AutoRecovery system:

/opt/local/bin/femis_watch
/opt/local/bin/femis_watch.conf (typical path)
/opt/local/bin/logit
/var/log/femislog[1-7]
/tmp/.auto.debug
/tmp/.autorecovery.pid
/var/tmp/.autorecovery.run
/home/femis/etc/eoclist.dat
/etc/syslog.conf

The two files, femis_watch and femis_watch.conf, are Perl scripts that comprise the heart of the FEMIS AutoRecovery system.

The FEMIS AutoRecovery system is run by cron. The run schedule is set in the root crontab. The default schedule is

```
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 UNIX man page on *crontab* before proceeding.

```
% su -
# crontab -e
```

2.6.1 Messaging Service

The AutoRecovery system uses three messaging services: logging, E-mail, and 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
```

For example, to disable syslog messages, comment out the following line:

```
$syslog_it = 1;
```

To disable E-mail messages, comment out the following line:

```
$mail_it = 1;
```

To disable notification through the FEMIS Notification Service, comment out the following line:

```
$notify_it = 1;
```

2.6.2 Logging

AutoRecovery logging is performed through syslog and can be configured with the following levels:

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

The default log level is info.

To log both warning and restart messages, complete the following steps.

1. Edit /etc/syslog.conf and change:

   local7.info to: local7.notice

   Log archiving is performed by the script /opt/local/bin/logit. This script is run nightly from the root crontab. The default number of logs archived is 7 days. 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.

   The log file is set in /etc/syslog.conf. The default log file is /var/log/femislog. The log file can be changed by editing /etc/syslog.conf and /opt/local/bin/logit.

2. Restart syslogd.

   ```
   % su -
   # sh /etc/init.d/syslog stop
   # sh /etc/init.d/syslog start
   ```

2.6.3 Sending E-mail

AutoRecovery sends all warning messages via E-mail to the root user by default. This configuration can be changed or added to by editing the file /opt/local/bin/femis_watch.conf and changing or adding E-mail addresses to the $Custodian line. 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.

2.6.4 Running Processes

AutoRecovery verifies certain processes are running. The 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, time value, restartable flag, and restart command.

The following line is the default configuration for the syslog daemon. The line defines the syslog daemon process syslogd. A minimum of one process is to be running, and not more than three. Also, the time value specifies a one second wait before attempting to verify that a restart of the daemon was successful. The daemon is restartable, and the restart command is "sh /etc/init.d/syslog start".

```
[ "syslogd",    1, 3, 1, 1, "sh /etc/init.d/syslog start" ],
```

The following line is the default configuration for only one NFS Maestro daemon, and it will restart the daemon if the number of processes is less than one.

[“hclnfsd”,1, 1, 1, 1, “sh /etc/init.d/hclnfs stop; sh /etc/init.d/hclnfs start”],

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

The time value, mentioned above did not have functionality in previous versions of FEMIS (formerly known as the status flag). In this version the value specifies a time to wait (in seconds) before verification of a process restart is attempted. This applies to all so-defined restartable processes.

2.6.5 Monitoring Swap and Disk Space

AutoRecovery monitors used disk and swap space. The thresholds are defined in /opt/local/bin/femis_watch.conf and can be customized for each server.

The following are two examples of configuration changes.

1. Complete the following steps to change the swap space monitoring to report 60% full instead of 80% full:

   Edit /opt/local/bin/femis_watch.conf

   Change $swap = 80; to $swap = 60;

2. Complete the following steps to change the disk space monitoring to report when / (root file system) is 90% full:

   Edit /opt/local/bin/femis_watch.conf.

   Look for the “@disks = (“ section.

   Edit the line by changing [“/” , 80], to [“/” , 90],

2.6.6 Remote Host Auto-Carve and Auto-Insert

The database design in FEMIS version 1.4.7 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.

Please refer to Section 2.1, AutoRecovery, in the ***FEMIS System Administration Guide*** for further information.

2.6.7 Remote Process Monitoring

Previous versions of AutoRecovery did not allow any configuration to determination if a remote system was good or bad based on the processes running on that system. This version now has a section in the femis_watch.conf file which 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 which 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 ignore_flag 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.

2.6.8 AutoRecovery's 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.

2.6.9 Installing AutoRecovery

Remove the previous version of the AutoRecovery package.

```
# pkgrm FEMISar
```

The FEMIS AutoRecovery system has been included with the FEMIS software distribution. FEMIS AutoRecovery requires the FEMIS packaged Perl version 5.004 to run. To install, see Section 2.1.6, Installing Perl v5.004-04. To install FEMIS AutoRecovery, you will need to create a spool directory that will require approximately 1MB of disk space.

1. Login in as root.

2. Insert the FEMIS tape into the tape drive, and enter the following commands as root:

   ```
   # mkdir /<dir>/spool
   # chmod 755 /<dir>/spool
   ```

3. Spool the installation package from the 8mm tape.

   ```
   # pkgadd -s /<dir>/spool -d /dev/rmt/??
   ```

   where ?? is the device number of the tape drive.

   Select FEMISar from the available package list.

4. Run the pkgadd utility to install the FEMISar package.

   # pkgadd -d /<dir>/spool

   Select FEMISar and follow the prompts through the installation.

5. Use pkgchk to verify that FEMISar were installed correctly.

   #pkgchk -n FEMISar

   Note: The packages installed successfully if no error output is displayed. Report any errors to PNNL.

6. Remove the spool directory.

   # rm -r /<dir>/spool

7. Logout.

2.6.10 Configuring AutoRecovery

To configure FEMIS AutoRecovery, complete the following steps.

1. Login as femis.

2. Edit the AutoRecovery configuration file /opt/local/bin/femis_watch.conf. Example:

   % chmod u+w femis_watch.conf
   % vi /opt/local/bin/femis_watch.conf

   Enable/disable Auto-Carve/Auto-Insert as desired and set appropriate thresholds, if necessary.

   Verify the restart commands are correct for all restartable processes.

   Add additional $Custodians to receive E-mail when a problem is detected.

   Verify the $ENV{FEMIS_HOME} variable points to the FEMIS installation directory.

   Verify the $ENV{ORACLE_HOME} variable points to the Oracle installation directory.

   Modify disk thresholds and default disk names; add disks as necessary.

   Replace the host entries in the @network list with the other servers at your site.

Verify the two lines in the %oracle_tablespaces definition match the following:

```
SYSTEM    =>  100,
TOOLS     =>  100,
```

Save and exit the file.

Enter chmod u-w femis_watch.conf.

3. Edit the FEMISar lines in the root crontab.

```
% su -
# crontab -e
```

Change volXX in the LD_LIBRARY_PATH = $LD_LIBRARY_PATH : /volXX/ environment variable to reflect the correct Oracle path.

Uncomment the FEMISar execution lines.

The FEMIS AutoRecovery should start running at the next scheduled FEMIS AutoRecovery (femis_watch) cron event. To verify it is running, check the log file for recent entries.

```
% tail /var/log/femislog
```

2.7 AutoRecovery Web Reporting Application

AutoRecovery monitors the FEMIS server and reports any errors to your System Administrator, using a standard E-mail message. Your System Administrator must log into E-mail and examine the messages to determine is a server has a problem. PNNL developed the AutoRecovery Web Reporting application to provide a more generic way for your System Administrator to examine the status of their systems.

Using the AutoRecovery Web Reporting application, messages can be sent to a central E-mail account. The E-mail is processed by AutoRecovery Web Reporting and displayed by a web server. Your System Administrator can view the status of your server using any browser application. AutoRecovery Web Reporting can be expanded to receive E-mail from each EOC. Using this capability allows all System Administrators to status their EOC server messages without installing a web server at each EOC.

2.7.1 Software Requirements

AutoRecovery Web Reporting requires the following applications:

- FEMIS AutoRecovery v2.2
- PERL v5.004-04

- MailTools v1.13 (a PERL extension included in the FEMIS PERL package)
- Apache Web Server v1.3.12

FEMIS AutoRecovery and PERL are packaged separately. The Apache Web Server, and the AutoRecovery Web Reporting scripts are included in the FEMISarw package.

2.7.2 AutoRecovery Web Reporting

If you are upgrading FEMIS, you must remove the previous version of the AutoRecovery Web Reporting package.

2.7.2.1 Removing the AutoRecovery Web Reporting Package

1. Login as root.

2. # pkgrm FEMISarw

   Select y to continue when the following prompt displays: Do you want to remove this package?

   Also select y for this prompt: Removing installed package instance <FEMISarw>. This package contains scripts that will be executed with super-user permission during the process of removing this package. Do you want to continue with the removal of this package [y,n,?,q].

3. Verify that the package was removed successfully.

2.7.2.2 Installing AutoRecovery Web Reporting

Note: This package has dependencies on the Perl 5.004. The Perl package must be installed before you can install AutoRecovery Web Reporting.

To install AutoRecovery Web Reporting, which has been included with FEMIS v1.4.7, complete the following steps.

1. Login as root.

2. Insert the FEMIS application tape into the tape drive.

   To create a temporary spool directory, run the following:

   ```
   # mkdir /<dir>/spool
   # chmod 755 /<dir>/spool
   ```

Spool the installation package from the 8mm tape using the Solaris software installation utility.

```
# pkgadd -s /<dir>/spool -d /dev/rmt/??
```

where ?? is the device number of the tape drive. Select the packages desired and run the pkgadd utility to install the FEMISarw package.

```
# pkgadd -d /<dir>/spool
```

3. Select the FEMISarw application for installation.

4. Select y to continue when the following prompt displays: This package contains scripts which will be executed with super-user permission during the process of installing this package.

5. After installing the FEMISarw package select q to quit.

6. Use pkgchk to verify the package was installed correctly.

   ```
   # pkgchk -n FEMISarw
   ```

7. Ignore the following or similar errors:

   ```
   ERROR: /etc/init.d/apache
       Permission <0700> expected <0744> actual
   ```

   Note: If you only see the above output or your system prompt appears with no output, the package installed successfully.

8. Remove the spool directory.

   ```
   # rm -r /<dir>/spool
   ```

9. Remove the tape from the drive.

2.7.3 Configuring AutoRecovery Web Reporting

To configure AutoRecovery Web Reporting, complete the following steps.

1. Login as root.

   Two new users, femisar and www (if they do not already exist), are created with the installation of the FEMISarw package.

2. **Be sure to set the femisar password**. Example: passwd femisar.

3. Edit /opt/local/apache/htdocs/index.html. Change YOUR_SYSTEM_NAME_HERE to your servername (e.g., tornado.pnl.gov).

4. Edit /opt/local/apache/conf/httpd.conf. Change the Server Admin variable to reflect the E-mail address of your System Administrator.

5. Edit /opt/local/apache/htdocs/femis/mb/index.pl. Change root\@localhost to the System Administrator's E-mail address (e.g., admin\@pnl.gov).

6. Edit /opt/local/apache/home/femisar/bin/mail.pl. Change root@localhost to the System Administrator's E-mail address (e.g., admin@pnl.gov).

7. Edit all html files in the /opt/local/apache/htdocs/femis/help directory. Change http://tornado.pnl.gov to http://YOURSERVERNAME.YOURDOMAIN. Change the E-mail address from root@localhost to the System Administrator's E-mail address.

8. Run /opt/local/apache/bin/setup_femisarw. When prompted, enter the name of each server that will send AutoRecovery E-mail messages. The script will create a directory for each server with the appropriate permissions.

9. Start the web server.

   sh /etc/init.d/apache start

10. Test the application with a web browser. The address should be http://YOURSERVERNAME.YOURDOMAIN (e.g., http://tornado.pnl.gov).

11. Edit the /opt/local/bin/femis_watch.conf on each server from which you will receive AutoRecovery E-mail, and add femisar to the Custodian list. (e.g., $Custodian = 'femisar@yoursystem.yourdomain').

AutoRecovery Web Reporting is now available for you to use.

2.7.4 Customizing AutoRecovery Web Reporting

To customize AutoRecovery Web Reporting, complete the following sections.

2.7.4.1 Setting the $retainFlag Variable

The variable $retainFlag in /opt/local/apache/home/femisar/bin/clean.pl is used to control how old messages are removed from the MessageBase. The string is comprised of three parts. The first part is a single letter that specifies what method to use to remove the messages.

- If the letter is a p (pruned), then messages that are older than the current date minus the specification in the next two parts are removed.

- If the letter is a t (truncated), messages are removed at a time that is a multiple of the unit specification and modulus of the unit specification. In other words, if the span and unit specification is a 1d (1 day), then the messages that are older than midnight GMT of the previous day would be removed.

The next two parts are the number of units and the type of the unit. The number must be a positive whole number or 0. The unit code may be one of the following: s, m, h, d, or w, which stand for seconds, minutes, hours, days, or weeks. These number and type of units could be used in a specification, such as t0d that would remove all messages before the current day (GMT).

The default is set to p24h.

2.7.4.2 Changing the Refresh Rate

To change the refresh rate of the AutoRecovery Web Reporting application, edit /opt/local/apache/htdocs/femis/mb/index.pl. The default is set to 60 seconds. To change the default value, change content="60" to your preferred refresh rate.

2.7.4.3 Accurate System Time

Proper operation of a public web server requires accurate time keeping, since elements of the HTTP protocol are expressed as the time of day.

2.7.4.4 Customizing the Apache Web Server

For additional information on customizing the Apache Web Server, see the online manual at http://YOURSERVERNAME/manual or go the Apache Web Page at http://www.apache.org.