14.0 FEMIS UNIX Server

The FEMIS UNIX server software provides notification between servers, the transfer of data between FEMIS and EMIS, the capability to gather meteorological data, and the ability for PCs to use the server resources for large mathematical model/simulation codes. The software on the UNIX server consists of the FEMIS host Notification Service, the FEMIS command server, the FEMIS Met application suite, and the FEMIS Data Exchange Interface (DEI). These services, combined with the UNIX COTS applications, provide the structure for the FEMIS software.

14.1 Maintenance of the FEMIS UNIX Server

Consistent server maintenance is essential for FEMIS operation. The following steps should be taken regularly to monitor and maintain the server.

14.1.1 Monitor Oracle and FEMIS

The UNIX FEMIS Monitor and/or FEMIS AutoRecovery can be used to monitor critical FEMIS functions. These functions include the FEMIS Notification Service, the FEMIS Command Server, the FEMIS DEI, the number of Oracle PC connections, the Oracle Listener, and Oracle replication. For more information on the FEMIS Monitor, see Section 2.0, FEMIS Monitoring Tools, and for Oracle maintenance, see Section 13.1.3, Oracle Database Backups.

14.1.2 Perform System Backups

System backups are critical to data recovery. It is highly recommended that each EOC establish backup procedures. For more information on Oracle backups, see Section 13.1.3, Oracle Database Backups, and for server backups, see Section 13.1.1, Full File System Backups.

14.2 Troubleshooting the FEMIS UNIX Server

The following items are provided for the System Administrator to aid in the administration of FEMIS. For more information on the COTS products, please refer to the documentation provided by the vendor.

14.2.1 FEMIS Troubleshooting

If FEMIS processes are down the following commands may be used to stop and restart all FEMIS processes.

```
# sh /etc/init.d/femis stop
# sh /etc/init.d/femis start
```

14.2.2 NFS Services

PCs may receive the following error when trying to connect to the server.

```
Network Timeout or HCLNFSD/PCNFSD not running on Host.
```

This error message typically occurs for one of the following reasons:

1. The mountd daemon is not running on the UNIX server. To resolve, start the mountd daemon.

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

2. The HCLNFSD daemon is not running on the UNIX server.

3. The NFS locking daemon is hung on the UNIX server.

For Steps 2 and 3, stop the NFS Maestro daemon, if it is running.

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

Restart the daemon

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

If the error continues, you may need to stop and restart the server locking daemon. Stop the NFS Maestro daemon, if it is running.

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

Stop lockd

```
# sh /etc/init.d/nfs.client stop
```

Restart lockd

```
# sh /etc/init.d/nfs.client start
```

Restart the NFS Maestro daemon

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

14.2.3 Samba Services

Samba is a software package for UNIX that allows interconnectivity with Microsoft Windows and Windows NT platforms. The advantage of its use is that it allows Windows platforms to communicate via native protocols to access resources (file and print) on a UNIX system. UNIX uses NFS (Network

File System) as its native format, which Windows platforms do not support as a bundled operating system capability. This situation requires the addition of a COTS package to provide NFS services to the PC, such as NFS Maestro or Solstice NFS. With the capability now on the server with Samba, a COTS package is no longer required on the client PC systems in order to access server resources. One other advantage of Samba is that it now allows encrypted user authentication to a variety of Microsoft authentication mechanisms making it much more secure and incorporable in the PC environment.

Samba, as released with FEMIS, is configured to work within the inetd framework. If you have an earlier version installed, it may have been run in stand-alone daemon mode – meaning that port monitoring was accomplished by the Samba daemon instead of the inetd daemon. Running Samba under inetd control, rather than the stand-alone daemon mode, means it may be a little more difficult to diagnose when problems arise; however, inetd has mechanisms in place to prevent runaway process replication on port driven services making it safer to use within the Solaris environment.

Samba is a very diverse and flexible package, which translates to an over-all complexity. The Samba package released with the FEMIS has been configured to specifically run a particular way. It already has predefined resources and global parameters that were obtained from field experience with non-FEMIS released versions of Samba in use at EOCs prior to this release. If your site is using schemes for PC integration that were not anticipated in the FEMIS packaged release of Samba, a few very minor edits to the configuration file may need to be done to set the site specific parameters. In these cases, a thorough review of the Samba configuration file man page is recommended to understand the different Samba configuration parameters. Basic editing of the smb.conf file is all that is typically necessary to get Samba working. If the source was installed at the package installation time, there is a whole directory tree of Samba documentation and notes available regarding specific topics that can be reviewed and/or searched.

14.2.3.1 Samba User Authentication

FEMIS Samba authentication is assumed to be provided via a primary domain controller. This requires the server to register/authenticate itself with the domain controller via the smbpasswd –j <domain_name> -r <primary domain controller> command before anything will work. This also assumes that all FEMIS client PCs are under the same domain control as the server is joining.

If domain services are not in use at a site, Samba also allows authentication via several other secure mechanisms. Samba will even allow authentication via the UNIX password on the server (although this is not recommended as it forces clear-text passwords on the network wire, and requires a special configuration of the Windows client to allow clear-text passwords to be sent). Other forms of authentication are NT server authentication, the smbpasswd file (located in /etc/samba/private), and UNIX user password authentication. The smbpasswd authentication is a fallback if user authentication fails to a domain server. This means that if a non-domain defined user logs onto a domain (or non-domain) PC, they can gain seamless access to Samba resources without having a domain account if they have a smbpasswd entry on the server. Documentation for use of the smbpasswd mechanism and file can be found in the source documentation directory in the two files ENCRYPTION.txt and DOMAIN_CONTROL.txt as well as the *smbpasswd* UNIX man page.

Some common problems that can occur with user authentication are

- No UNIX account exists for the PC user. All Samba users must have as a minimum, a UNIX account defined on the system. Samba **does not require** that the account have a valid password (unless UNIX authentication is in use) nor does it require the user to have user space (a home directory) defined on the system. The user **must be defined** to the UNIX system (in the password/shadow mechanism) or Samba will fail the request for resources. A failed request shows up on the PC as a request for username and password to gain access to the resource. Very little information is given to the client PC user as to what is failing, other than the username/password window. This is what makes Samba connectivity particularly difficult to diagnose. All diagnostic methods must be done on the server side since the PC simply is rejected without any logged reason on the PC itself.

- The user has not been added to a UNIX group required for access to a share in the smb.conf file. The default shares defined in the FEMIS smb.conf file require users to be a member of the UNIX group femisrun.

14.2.3.2 NFS and Samba Interaction

Samba and NFS services can coexist on a UNIX server and client PC; however, the PC has no real way of forcing which service is used in any particular case, even with network access orders defined to be a fixed order (see the Network Neighborhood properties pane). Usually, the differences between the NFS share names and the Samba based share names are enough for the PC to distinguish which service to use in connecting. There are occasions where the client seems to get locked into using the NFS protocol instead of the SMB Samba protocol to attach to a resource. In these cases, the method that has experienced the best success in forcing the SMB protocol use is to specify the server's host name as a raw IP address instead of a host name. For example, instead of specifying a resource name as \\anca-eoc\user, the share name would be expressed as \\131.92.35.11\user. To experience the least amount of connection problems; however, it is simply best to not install COTS NFS services on the PC if NFS will not be used.

14.2.3.3 FEMIS Samba Directory Structure

The FEMIS Samba directory structure is somewhat spread out to allow the serving of the Samba binaries and static files to multiple UNIX hosts, while maintaining server specific configuration and logging uniquely on each separate UNIX host. The directory tree is as follows:

- Static files: binaries, man pages, source tree located by default in /apps/samba.

- Configuration files: smb.conf, domain account files, and smbpasswd located in /etc/samba and /etc/samba/private.

- Log files, locks directory, and browse lists located in /var/adm/samba.