

---

**Discussion Topics**

- General Discussion on basic system care for Ir1
- In addition to the discussion of issues that follows, weekly conference calls will be set up to discuss problems at each site

## M&O Documentation



- **DID 609 - IR1 Maintenance and Operations Procedures**
- **DID 611- IR1 Operator's Manual for the ECS Project**

520-TD-001-002 M&O 3-2

### Discussion Topics

**During this course, you will hear references to two primary documents. DID 609 and DID 611.**

**DID 609:** provides an operations overview that:

- supports the development of detailed science software integration and test procedures by the ECS Science Office
- supports TRMM interface testing, and
- supports the use of the system by M&O staff.

Specifically, DID 609 includes:

- an overview
- lists related documents
- describes physical components and organization of IR1
- describes purpose and operation of the TRMM interface, SSI&T, and IR1 infrastructure test tools
- lists system error and status messages

**DID 611:** details the major operations procedures and operations instructions that M&O System Administrators need to know to support the objectives of IR1:

- Operations Procedures - the step by step commands or on-line procedures needed to perform a function
- Operations Instructions - off-line procedures or directives for performing administrative, operations, management or operations support activities.

## Perform Backup/Restore



---

- **COTS Tool: Networker**
  - On-site incremental backup
  - On-site complete system backup
  - Restore selected files
  - Complete system restore

520-TD-001-002
M&O 3-3

### Discussion Topics

**Incremental and complete system backups** of files that are on the ECS system for that site, **restoral of selected files** on the system and **complete system restore** from backup tapes at that site:

- While ECS equipment is not being used, the M&O staff will perform weekly incremental backups and monthly complete system backups.
- During testing, the M&O staff will perform daily incremental backups and weekly complete system backups.
- A copy of the backups will be stored at an off site facility provided by the DAACs.
- The M&O staff shall maintain five incremental backups, and complete system backups before reusing tapes.
- For questions regarding supplies (e.g., tapes), call Tom Hickey (301) 925-0391
- Non-scheduled backups can be requested at any time through the DAAC engineering liaison with DAAC management approval.
- The backup procedures are established by DAACs and should be scripted where possible.
- Networker tool was not intended for use in recovery from system crashes (see documentation)
- Backup by Networker or Epic: ClearCase requires that the transaction log is locked up for backup of the VOB

The only time a complete system restore should have to be performed is in the event of a system crash with the loss of data, and the only way to get the system back up and running in a timely fashion is to restore the system from a previous backup. The result of this action will be that any updates to the system, (e.g. files), from the time of the last backup to the restore will be lost. The senior M&O person will get approval for the restore from the DAAC manager or their designee.

- The complete recovery of the system from a backup is the result of a trouble shooting exercise.
- The developers at the EDF must be contacted in order to verify that a complete restore of the system is the only way to resolve problem.
- After it has been decided that it is necessary to perform a complete restore of the system, the DAAC Manager or their designee are informed of the action and the results of such an action.
- All problems are documented and logged in the operator's log book.

## System Shutdown/Startup



- **Cold Startup**
  - cold boot (powering machine on)
- **Warm Startup**
  - Sybase and Autosys
  - ClearCase startup script locations
    - » SUN Solaris 2.4            /etc/rc2.d/S77atria
    - » DEC OSF1 V3.0            /sbin/init.d/atria
    - » SGI IRIX 5.3                /etc/init.d/atria
    - » HP UX 9.05                 /etc/rc.atria
- **Normal Shutdown**
  - Sun 4: /usr/etc/shutdown
  - Sun 5: /usr/sbin/shutdown and /usr/ucb/shutdown
    - » /usr/sbin/shutdown -y -g0 -i0 where  
 -y = pre-answer all questions as “yes”; -g = grace period of “0”seconds before shutdown; -i = init state (enter state “0” to stop operating system)
  - Sun 5: ( Solaris )
- **Emergency Shutdown**
  - /etc/halt

### Discussion Topics

Check with authority prior to performing the following procedures. Follow procedures for each individual site. Document all shutdowns and startups, and notify users when the system is being rebooted.

- **ECS Cold Startup** - start the system with no subsystems previous running - cold boot
- **ECS Warm Startup** - restart subsystems while not affecting others (e.g. autosys/sybase, ClearCase)
- **ECS Normal Shutdown** - shutdown the system with no loss of data.
  - The time of shutdown must be coordinated with the Resource Manager (M&O person)
  - Once a time of least impact has been determined, the DAAC Manager is notified and must approve the shutdown/resource schedule change before it can take place.
  - When shutting down, make sure ClearCase is shut off
  - Everything is tied into the DCE server at the EDF; it has the potential to hangup so give EDF a call to find DCE personnel. Shutdown is very slow when DCE is either not working right or the server is unavailable.
  - All activities associated with the shutdown will be logged in the operator's logbook.
- **ECS Emergency Shutdown** - shut down system in emergency situations with minimal loss of data
  - The senior M&O person at the site is responsible for determining the problem and making the decision to perform an emergency shutdown. Whenever possible the DAAC Manager should be consulted prior to system shutdown. Shutdown may be a complete system shutdown or possibly only a subsystem shutdown.
  - If the entire system is locked up then a complete system shutdown is required and the emergency shutdown and start-up procedures should be executed immediately. The DAAC Manager is notified after the system has been brought back up.
  - If major subsystems are locked up, the entire system should also be brought down and the emergency shutdown and start-up procedures should be executed immediately.
  - If one or only a few of the subsystems are experiencing problems, and only some of the users are impacted, do the following:
    - » try to resolve the problems with the subsystems (consult with EDF)
    - » if a shutdown is necessary, then try to shutdown the problem subsystems first
    - » try not to impact users that are still using the system
    - » notify the DAAC Manager if the problem is not immediate
    - » document the problem, generate a problem report, log all activities in operator's logbook.

## Add/Delete Users



- Adding UNIX Users
- Deleting UNIX Users

520-TD-001-002 M&O 3-5

### Discussion Topics

Describe the commands that M&O staff will use to add and delete UNIX users to the systems located at the sites

- In order for anyone to have a user account on any of the computers that make up ECS, the user must provide to the DAAC Management a detailed justification for why they should have an account on the system.
- Once the application is approved, the M&O person at the site where the user is requesting an account will add the new user. It's important that this process is standardized. Al Ward will provide a custom script that will be passed on to the DAACs for adding new accounts.
- The same approval process will be used for deleting a user, changing privileges, and changing affiliations.
- Unless it is indicated on the form, the user will be added to all UNIX systems at a particular site.
- For questions concerning adding/deleting ClearCase users, see Dave Compton (301) 925-1097
- The DAAC manager will authorize deletion of user accounts from the ECS system. Before deleting a user, make sure all user files have been successfully backed up before deleting a home directory.

## Adding Users



---

**User Registration Request Form**

User Name: \_\_\_\_\_

Date of Request: \_\_\_\_\_

UNIX ID: \_\_\_\_\_

Home Directory: \_\_\_\_\_

Group: \_\_\_\_\_

Organization: \_\_\_\_\_

Site: \_\_\_\_\_

Approval: \_\_\_\_\_ Date: \_\_\_\_\_

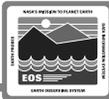
520-TD-001-002 M&O 3-6

### Discussion Topics

User's must submit request for account form (see slide) to the DAAC management. Some information on the form may be completed by the M&O staff.

- The DAAC management will then approve or disapprove the application. Upon approval the DAAC management will give the form to the DAAC ECS System Engineering liaison.
- The ECS System Engineering liaison then gives the form(s) to the M&O person so that they may take the appropriate action (add the user, delete the user, change privileges or change affiliations). Unless indicated on the form the action will take place for all systems at a particular site. A separate form must be submitted for each site.
- M&O personnel then follow the appropriate procedure for the action.
- For adding new users, the M&O person will phone the new password to the user with the temporary password. The password will be set to expire as soon as the user logs on, forcing them to change their password. In the event a user forgets their password, a new password will be issued in the same format.
- Keep UNIX user id convention consistent
- The M&O person then sends email message to the people listed in the Ops procedures when the action has been completed.
- This action, as all changes to the ECS system, will be logged in the Operators log book.

## AutoSys Database Maintenance



- **Data Base Maintenance**
  - **Script**  
`$AUTOSYS/bin/DBMaint`
  
  - **Maintenance Command**  
`% archive_events -A -n 4`
  
  - **Tuning Commands**  
`update statistics`  
`sp_recompile`

520-TD-001-002 M&O 3-7

### Discussion Topics

Once every 24 hours, AutoSys goes into a database maintenance cycle. It does not process any events until this cycle is completed. The time that the maintenance cycle begins can be set using the **DBMaintTime** parameter.

During the maintenance cycle, AutoSys executes the script **\$AUTOSYS/BIN/DBMaint**. This script:

- archives and removes old events from the database
- updates the database's execution plans and indexes
- recompiles the stored procedures that use the database tables
- checks the available space in the database

The functions performed by the maintenance script can also be executed individually from the UNIX prompt.

- The **archive\_events** command can be used to archive all events older than a specified number of days. It first archives the events in an archive directory, then it deletes these events from the database.
- The **update statistics** command can be used to update the indexing statistics for a particular table(s), in order to optimize the performance of the database.
- The **sp\_recompile** command is used to recompile the procedures that use the table(s), so that they will be able to utilize the updated index statistics.

Additional details about database maintenance are contained in Chapter 14 of the AutoSys User Manual.

## Database Administration



- **Sybase Roles**
  - System Administrator (sa)
  - System Security Officer (SSO)
  - Operator
  - Database Owner (DBO)

520-TD-001-002
M&O 3-8

### Discussion Topics

Sybase Roles (see Chapter 2 in the System Administrator's Guide for details). These roles are not currently set up in the IR1 PDPS database -- it is up to the sites to determine if they want to set up these roles.

- **System Administrator (sa)**
  - The sa login is initially assigned three special roles and can execute all SQL commands. To divide responsibility and increase accountability, you can assign these roles to separate logins and then lock the sa login
    - » System Administrator - administrative tasks
    - » System Security Officer - security tasks
    - » Operator - can backup and load all databases and transaction logs.
  - owns the *master* database
  - is treated as database owner in every database
  - has access to all databases and objects
  - manage disk storage
  - drop, modify, and lock logins
  - grant/revoke SA role
  - create user databases and grant ownership of them
  - grant certain permissions to SQL server users
  - diagnose system problems
  - fine-tune SQL server
  - shut down SQL server
  - monitor recovery
- **System Security Officer (SSO)** performs security tasks.
  - create logins
  - lock logins
  - administer passwords
  - grant and revoke SSO and OPER roles
  - manage the audit system
- **Database Owner (DBO)** owns the database and performs certain database-specific administrative functions to maintain it
  - create tables another objects
  - add users and groups; define privileges
  - backup and restore the database and transaction log

## Database Administration (cont'd)



- **Sybase failure**
  - System
  - Media
- **Backup procedures**
  - dump database
  - dump transaction
  - automatic

520-TD-001-002
M&O 3-9

### Discussion Topics

**Database Failures.** There are two different kinds of database failures.

- In the case of system failure, such as power outages or SQL Server failure, as long as the Sybase startup script is entered into the automatic startup sequence (a one-time entry into the startup file), recovery is automatic and requires no DBA intervention.
  - If the Sybase startup script is not manually entered into the automatic startup sequence, then the server will not be restarted upon boot up.
  - If there is a SQL server failure, the DBA will need to determine what brought the server down; the System Administrator may be required to bring the SQL server back up.
- If there is a media failure, DBA intervention is required. In order for the DBA to recover the database to the point in time of failure, the database must have been configured, and the data in the database must have been backed up to support such a recovery.
- To ensure that a full recovery can be done, the *master* database and the log tables (syslogs) must be mirrored to a second disk. If there is a loss of one of the disks, the mirrored files can be used for recovery. Also, a good backup strategy should include frequent backups of the *master* database, the *master* log, the model database, and all databases and associated transaction logs on the Server. The "dbcc" (database consistency checker) program should be run prior to backups to verify the integrity of the databases.

**Backup Procedures.** There must be a Backup Server running on the same system as the SQL Server which performs the backup task. Networker will not do this type of backup.

- The "dump" command is used to back up an entire database and the transaction log. The file output as a result of this command can then be backed up using an operating system backup.
  - The "dump database" command can be run while users are actively using the database. Sybase recommends that the database be in single user mode to run a dbcc and backup the database.
  - The "dump transaction" command is the command used to back up the transaction log only. This is the command used for incremental backups. Unlike the "dump database" command, the "dump transaction" command causes the transaction log to get pruned (i.e., cleans out committed transactions).
- There are a couple of ways to set up backups to be done automatically. UNIX scripts can be set up to run the database scripts to do the dumps or the backups can be executed through a threshold manager. If a threshold is crossed, the SQL Server suspends writes to the logs, placing an error in the error log for all suspended transactions, and executes a stored procedure "sp\_thresholdaction", which will perform a "dump transaction".

## Database Administration (cont'd)



- **Recovery procedures**
  - load database
  - load transaction
  - buildmaster program

520-TD-001-002 M&O 3-10

### Discussion Topics

**Recovery Procedures. The following should be practiced at the individual sites.**

- The "load database" command is the command used to replace existing contents in a database with data from a dumped image created with the "dump database" command. There can be no active users at the time of the load. The current rdb image must match the image of the database that is contained in the dump file. If the databases are incompatible, the load will fail.
- The "load transaction" command reads a previously backed up copy of the transactions log into the current transactions log as a means of recovery. The transaction log backups must be loaded in the order that they were done.
- If the master database gets damaged, it can be rebuilt using the "buildmaster" program, if you have current backups. This program needs to be run in a single-user mode, with the SQL Server down. The "dbcc" program should always be run on each database after running "buildmaster" to ensure the consistency of the database.

## Additional Administrative Activities



- **Managing Disk Space**
  - /tmp
  - /usr/tmp
  - /usr/adm
- **General Reporting**
  - HP OpenView
  - netstat -nr where
    - n = show network addresses as numbers
    - r = show routing tables
- **Security**
- **DNS**
- **ClearCase**
  - Atria support
    - » phone: (617) 676-2450
    - » email: support@atria.com

520-TD-001-002
M&O 3-11

## Discussion Topics

- **Managing/freeing disk space.**
  - monitor /tmp and /usr/tmp directories, clean them out on a weekly basis; you can always grab a file off the system at the EDF
  - remove user/adm crash directories(on SGI) after backup
  - the #1 problem for DAACs will be keeping user's home directories uncluttered which causes stress on Networker
  - Mail: User must maintain their own mail directory, the SA cannot clean up these individual directories; encourage users to keep mail left on server to a minimum
  - need to leave 1 Gig per VOB created because they will grow
- **General Reporting -- All reports will be generated using the HP OpenView (network monitoring) capability**
  - If there are problems with the network, you can also use netstat -nr command to obtain additional information/statistics
- **Security**
  - System Administrators can use a SUDO file which allows developers to execute root commands without knowing the root password (it will use an individual's password). SUDO can track time, what the command is, and can limit commands. Located in usr/local/bin
  - Eliminate unused accounts/beware of sharing of accounts and passwords
  - If you suspect hackers, contact the router/network person to see if they are having the same problem
  - COPS, CRACK, wrappers (no hardcopy log host)
  - DCE server at EDF controls certain access at the sites
- **Dynamic Name Service (DNS) - resolving IP addresses to name of system**
  - can get out of sync, which causes wrong IP addresses
  - determine who is local DNS administrator and who their backup is
  - can be used as a part of the troubleshooting process
- **ClearCase - don't remove a View using UNIX commands**
  - there are two reference manuals available. The Atria support numbers listed in them are incorrect. See slide for correct numbers.