

EOSDIS Maintenance and Development Project

Release 7.20 Mission Operation Procedures for the EMD Project

Revision -

July 2007

Raytheon Company
Upper Marlboro, Maryland

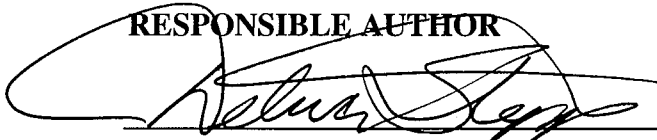
Release 7.20 Mission Operation Procedures for the EMD Project

Revision -

July 2007

Prepared Under Contract NAS5-03098
CDRL Item 23

RESPONSIBLE AUTHOR

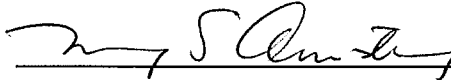


Debra Stepp, Lay'wan Gamble, & Ken Prickett
EOSDIS Maintenance and Development Project

Date

July 31, 2007

RESPONSIBLE OFFICE



Mary Armstrong, Program Manager
EOSDIS Maintenance and Development Project

Date

July 31, 2007

Raytheon Company
Upper Marlboro, Maryland

This page intentionally left blank.

Preface

This document is a formal contract deliverable. It requires Government review and approval within 45 business days. Changes to this document will be made by document change notice (DCN) or by complete revision.

Any questions should be addressed to:

Data Management Office
The EMD Project Office
Raytheon Company
1616 McCormick Drive
Upper Marlboro, Maryland 20774-5301

Revision History

| Document Number | Status/Issue | Publication Date | CCR Number |
|-----------------|--------------|------------------|------------|
| 611-EMD-100 | Original | July 2007 | 07-0390 |

This page intentionally left blank.

Abstract

This document, Mission Operation Procedures for the EMD Project, provides DAAC procedures that assign and describe operators, engineers, operations support, administration and management staff actions required to configure, maintain and operate the ECS applications at maturity. The DAAC portion of this document contains system-level standard procedures that can be modified at the DAACs during subsequent training, operations exercises and procedure review activities to reflect desired uniqueness. The objectives of the current release of the system are to provide capability to support the ingest and archive of raw data obtained from instruments on Earth Observing System (EOS) satellites [e.g., the EOS AM Mission spacecraft 1, morning equator crossing spacecraft series (Terra (AM-1)), EOS PM Mission spacecraft 1 and the afternoon equator crossing spacecraft series (Aqua (PM-1))]. Other capabilities provided by the current release include processing the data obtained, distributing raw or processed data as requested, quality assurance of processed data, supporting communication networks, and systems monitoring via interfaces with the ECS operations staff.

This page intentionally left blank.

Contents

Preface

Abstract

1. Introduction

| | | |
|-------|---|-----|
| 1.1 | Identification..... | 1-1 |
| 1.2 | Scope..... | 1-1 |
| 1.2.1 | On-Site Procedures Tailoring Guide..... | 1-1 |
| 1.3 | Purpose..... | 1-1 |
| 1.4 | Status and Schedule | 1-2 |
| 1.5 | Organization..... | 1-2 |

2. Related Documentation

| | | |
|-------|--|-----|
| 2.1 | Parent Documents | 2-1 |
| 2.2 | Applicable Documents..... | 2-1 |
| 2.3 | Information Documents | 2-1 |
| 2.3.1 | Information Documents Referenced | 2-1 |
| 2.3.2 | Information Documents Not Referenced | 2-3 |

3. System Administration

| | | |
|-------|------------------------------|-----|
| 3.1 | Overview..... | 3-1 |
| 3.2 | Secure Access to DAACs | 3-1 |
| 3.3 | Setting Up SSH..... | 3-1 |
| 3.3.1 | Initiating SSHSETUP | 3-2 |
| 3.4 | Remote SSH Access | 3-2 |

| | | |
|--------|---|------|
| 3.4.1 | Setting Up Remote Access SSH | 3-2 |
| 3.5 | Changing Your Passphrase | 3-3 |
| 3.5.1 | Changing Your Passphrase | 3-3 |
| 3.6 | Logging in to System Hosts | 3-4 |
| 3.6.1 | Log in to System Hosts | 3-4 |
| 3.7 | System Startup and Shutdown | 3-5 |
| 3.7.1 | Cold Startup By Subsystem | 3-6 |
| 3.7.2 | Warm Startup | 3-7 |
| 3.7.3 | Updating leapsec.dat and utcpole.dat Files..... | 3-8 |
| 3.7.4 | Normal Shutdown | 3-9 |
| 3.7.5 | Emergency Shutdown | 3-10 |
| 3.7.6 | System Shutdown by Server | 3-12 |
| 3.8 | Checking the Health and Status of the System | 3-12 |
| 3.9 | WhatsUp Professional 2006 (Premium Edition) – Removed | 3-12 |
| 3.10 | Whazzup??? | 3-12 |
| 3.10.1 | Starting EcMsWz-Whazzup..... | 3-13 |
| 3.10.2 | Host Status | 3-15 |
| 3.10.3 | Verify Mode..... | 3-15 |
| 3.10.4 | Performance Management | 3-15 |
| 3.11 | ECS Health Check GUI | 3-23 |
| 3.11.1 | Starting and Using the ECS Health Check GUI | 3-26 |
| 3.12 | ECS Assistant and ECS Monitor | 3-28 |
| 3.12.1 | Starting ECS Assistant..... | 3-28 |
| 3.12.2 | Using the ECS Assistant Server Monitor | 3-31 |
| 3.12.3 | Using EcCsIdPingServers to Determine Server Status..... | 3-31 |
| 3.13 | Tape Operations | 3-33 |
| 3.13.1 | Networker Administrator Screen | 3-33 |
| 3.13.2 | Labeling Tapes..... | 3-35 |
| 3.13.3 | Indexing Tapes..... | 3-37 |
| 3.14 | System Backups and Restores | 3-42 |
| 3.14.1 | Incremental Backup | 3-43 |
| 3.14.2 | Full System Backup | 3-46 |
| 3.14.3 | Single or Multiple File Restore..... | 3-48 |

| | | |
|---------|--|------|
| 3.14.4 | Complete System Restore | 3-52 |
| 3.15 | User Administration..... | 3-56 |
| 3.15.1 | Screening Personnel..... | 3-56 |
| 3.15.2 | Screening Procedures..... | 3-57 |
| 3.15.3 | Adding a New User..... | 3-58 |
| 3.15.4 | Deleting a User | 3-58 |
| 3.15.5 | Changing a User's Account Configuration..... | 3-60 |
| 3.15.6 | Changing User Access Privileges | 3-60 |
| 3.15.7 | Changing a User Password | 3-61 |
| 3.15.8 | Checking a File/Directory Access Privilege Status | 3-61 |
| 3.15.9 | Changing a File/Directory Access Privilege..... | 3-62 |
| 3.15.10 | Moving a User's Home Directory | 3-65 |
| 3.16 | Commercial Off-the-Shelf (COTS) Software Administration..... | 3-65 |
| 3.16.1 | Installation | 3-65 |
| 3.16.2 | LOG FILES..... | 3-65 |
| 3.16.3 | COTS Configuration..... | 3-66 |
| 3.17 | Security | 3-66 |
| 3.17.1 | Generating Security Reports..... | 3-66 |

4. Database Administration

| | | |
|-------|---|------|
| 4.1 | System Overview | 4-4 |
| 4.1.1 | Information Model | 4-4 |
| 4.1.2 | Subsystems..... | 4-7 |
| 4.1.3 | Databases | 4-8 |
| 4.1.4 | Commercial Off-the-Shelf (COTS) Databases | 4-10 |
| 4.1.5 | Flat Files | 4-10 |
| 4.1.6 | Resident Databases | 4-11 |
| 4.1.7 | Database Directory Locations..... | 4-12 |
| 4.2 | Database Management..... | 4-13 |
| 4.2.1 | Database Management Model | 4-13 |
| 4.2.2 | Database Management Implementation..... | 4-15 |
| 4.2.3 | Hardware, Software, and Database Mapping | 4-18 |
| 4.3 | Database Administrator | 4-18 |

| | | |
|--------|---|------|
| 4.3.1 | DBA Tasks and Procedures | 4-19 |
| 4.4 | Starting and Stopping Database Servers | 4-21 |
| 4.4.1 | Start Adaptive Server Enterprise (ASE) Servers | 4-22 |
| 4.4.2 | Start the ASE Backup Server | 4-23 |
| 4.4.3 | Start the ASE Monitor Server | 4-23 |
| 4.4.4 | Stop the ASE Monitor Server | 4-25 |
| 4.4.5 | Stop the ASE Backup Server | 4-26 |
| 4.4.6 | Stop the ASE Server | 4-27 |
| 4.5 | Creating Database Devices | 4-27 |
| 4.5.1 | Create a Database Device | 4-27 |
| 4.6 | Installing Databases and Patches | 4-31 |
| 4.6.1 | Perform a Database Build Procedure (Example Only) | 4-31 |
| 4.6.2 | Install a Database Patch (Example) | 4-34 |
| 4.6.3 | COTS Databases | 4-35 |
| 4.7 | Configuring Databases | 4-35 |
| 4.7.1 | Configure the ASE Server Parameters | 4-35 |
| 4.7.2 | Configuration Parameters and the Configuration Registry | 4-40 |
| 4.7.3 | Configuration Registry | 4-40 |
| 4.7.4 | Use the following procedure to display configuration parameters | 4-40 |
| 4.8 | Working with Indexes, Segments, and Caches | 4-43 |
| 4.8.1 | Delete an Index | 4-43 |
| 4.8.2 | Create Database Segments (Example) | 4-44 |
| 4.8.3 | Create Database Segments (Example) | 4-45 |
| 4.8.4 | Caches | 4-47 |
| 4.9 | Backing Up and Recovering Data | 4-47 |
| 4.9.1 | Perform Automatic Backups | 4-48 |
| 4.9.2 | Performing Automatic Backups | 4-48 |
| 4.9.3 | Perform Manual Backups | 4-50 |
| 4.9.4 | Perform a User Database Recovery (Order of Procedures) | 4-52 |
| 4.9.5 | Perform a User Database Recovery (Example) | 4-53 |
| 4.9.6 | Create a User Database (Example) | 4-54 |
| 4.10 | Establishing Database Security | 4-56 |
| 4.10.1 | Grant or Revoke Database Access Privileges | 4-58 |

| | | |
|--------|--|------|
| 4.10.2 | Create an ASE Server Login..... | 4-59 |
| 4.10.3 | Change a Password..... | 4-62 |
| 4.10.4 | Perform Auditing..... | 4-62 |
| 4.10.5 | EMD Security Directive..... | 4-63 |
| 4.11 | Copying, Replicating, and Extracting Data..... | 4-64 |
| 4.11.1 | Copying a Database (Example)..... | 4-64 |
| 4.12 | Bulk Copying..... | 4-65 |
| 4.12.1 | Perform Bulk Copying..... | 4-65 |
| 4.13 | Replication System Administration..... | 4-66 |
| 4.13.1 | Replication System Administrator Tasks..... | 4-67 |
| 4.13.2 | DAAC DBA Replication Roles and Tasks..... | 4-67 |
| 4.13.3 | Database Replication..... | 4-68 |
| 4.14 | Performance Monitoring, Tuning, and Problem Reporting..... | 4-69 |
| 4.14.1 | Monitoring..... | 4-69 |
| 4.14.2 | Tuning..... | 4-70 |
| 4.15 | Ensuring Database Quality..... | 4-71 |
| 4.15.1 | Integrity Monitoring..... | 4-71 |
| 4.16 | Sybase Troubleshooting..... | 4-72 |
| 4.16.1 | Space Usage..... | 4-72 |
| 4.16.2 | Troubleshoot Chronic Deadlock..... | 4-72 |
| 4.17 | Oracle Procedures – Removed..... | 4-74 |

5. Security Services

| | | |
|-------|---|------|
| 5.1 | Scanning Network Vulnerabilities..... | 5-1 |
| 5.2 | Ensuring Password Integrity..... | 5-1 |
| 5.2.1 | Detecting Weak Passwords..... | 5-2 |
| 5.2.2 | ANLpasswd..... | 5-7 |
| 5.3 | Aging Passwords..... | 5-11 |
| 5.4 | Secure Access through Secure Shell..... | 5-12 |
| 5.4.1 | Installation of SSH..... | 5-12 |
| 5.4.2 | The SSH Encryption Mechanism..... | 5-13 |
| 5.4.3 | Using Secure Shell..... | 5-13 |

| | | |
|-------|---|------|
| 5.4.4 | A Layer of Convenience | 5-14 |
| 5.4.5 | Multiple Connections..... | 5-15 |
| 5.4.6 | Secure FTP..... | 5-15 |
| 5.4.7 | Other Notes | 5-15 |
| 5.4.8 | Configuration of Secure Shell..... | 5-15 |
| 5.4.9 | Administration of Secure Shell..... | 5-17 |
| 5.5 | Controlling Requests for Network Services (TCP Wrappers)..... | 5-18 |
| 5.5.1 | Installation, Configuration, and Testing for Wrappers | 5-18 |
| 5.6 | Monitoring File and Directory Integrity (Tripwire) | 5-20 |
| 5.6.1 | Installation of Tripwire | 5-21 |
| 5.6.2 | Updating the Tripwire Database | 5-21 |
| 5.6.3 | Configuring the tw.config File..... | 5-22 |
| 5.7 | Reporting Security Breaches | 5-23 |
| 5.8 | Initiating Recovery from Security Breaches..... | 5-23 |

6. Network Administration

| | | |
|-------|--|-----|
| 6.1 | Network Documentation..... | 6-1 |
| 6.2 | Network Monitoring | 6-1 |
| 6.2.1 | Big Brother - Better Than Free Edition | 6-1 |
| 6.2.2 | WhatsUp Professional 2006 Premium (WhatsUp Professional) -Removed..... | 6-1 |
| 6.3 | DAAC LAN Topology Overview..... | 6-1 |
| 6.4 | Network Hardware Components..... | 6-2 |
| 6.4.1 | Portus Firewall..... | 6-2 |
| 6.4.2 | VLAN Ethernet Switch..... | 6-2 |
| 6.4.3 | GigE Switch..... | 6-3 |
| 6.5 | Domain Name Service (DNS) Structure..... | 6-3 |
| 6.6 | Host Names | 6-4 |
| 6.7 | Network Security | 6-4 |
| 6.7.1 | Network Connectivity..... | 6-4 |
| 6.7.2 | Troubleshooting - Verifying Connectivity | 6-4 |

7. System Monitoring

| | | |
|-------|---|-----|
| 7.1 | Overview | 7-1 |
| 7.2 | Checking the Health and Status of the Network | 7-1 |
| 7.2.1 | Big Brother | 7-1 |
| 7.3 | Using WhatsUp Professional Reports - Removed | 7-2 |
| 7.4 | Starting and Using the ECS Health Check GUI | 7-2 |
| 7.4.1 | Starting ECS Health Check | 7-2 |
| 7.5 | Monitoring and Managing Server Applications | 7-4 |
| 7.5.1 | Whazzup?? | 7-5 |
| 7.5.2 | ECS Assistant and ECS Monitor | 7-5 |

8. Problem Management

| | | |
|-------|--|------|
| 8.1 | The Problem Resolution Process — An Overview | 8-2 |
| 8.1.1 | Internal Process | 8-2 |
| 8.2 | Problem Management Procedures | 8-3 |
| 8.3 | Using the Trouble Ticket System | 8-5 |
| 8.3.1 | Accessing the Trouble Ticket System | 8-7 |
| 8.3.2 | Submitting a Trouble Ticket | 8-12 |
| 8.3.3 | Reviewing and/or Modifying Open Trouble Tickets | 8-13 |
| 8.3.4 | Moving Trouble Tickets Through Lifecycle State of Events | 8-15 |
| 8.3.5 | Adding Users to TestTrack Pro | 8-15 |
| 8.3.6 | Privileges in TestTrack Pro | 8-16 |
| 8.3.7 | Modifying TestTrack Pro's Configuration | 8-20 |
| 8.3.8 | Generating Trouble Ticket Reports | 8-20 |
| 8.4 | Emergency Fixes | 8-21 |

9. Configuration Management

| | | |
|-------|--|-----|
| 9.1 | Configuration Identification Procedure | 9-2 |
| 9.1.1 | Purpose | 9-2 |
| 9.1.2 | Applicability | 9-2 |

| | | |
|-------|--|------|
| 9.1.3 | References..... | 9-2 |
| 9.2 | Configuration Change Control Procedures..... | 9-3 |
| 9.2.1 | Purpose..... | 9-3 |
| 9.2.2 | Applicability | 9-3 |
| 9.2.3 | References..... | 9-3 |
| 9.2.4 | Procedures..... | 9-3 |
| 9.3 | Configuration Status Accounting Procedures..... | 9-17 |
| 9.3.1 | Purpose..... | 9-17 |
| 9.3.2 | Applicability | 9-18 |
| 9.3.3 | References..... | 9-18 |
| 9.3.4 | Procedures..... | 9-18 |
| 9.4 | Configuration Audits | 9-19 |
| 9.4.1 | Purpose..... | 9-19 |
| 9.4.2 | Applicability | 9-19 |
| 9.4.3 | References..... | 9-20 |
| 9.4.4 | Procedures..... | 9-20 |
| 9.5 | Archiving Procedures for the SW CM Manager (ClearCase) | 9-20 |
| 9.5.1 | Purpose..... | 9-20 |
| 9.5.2 | Applicability | 9-21 |
| 9.5.3 | References..... | 9-21 |
| 9.5.4 | Definitions | 9-21 |
| 9.5.5 | General..... | 9-21 |
| 9.5.6 | Procedures..... | 9-22 |
| 9.6 | Software Delivery and Installation | 9-22 |
| 9.6.1 | Purpose..... | 9-22 |
| 9.6.2 | Applicability | 9-22 |
| 9.6.3 | References..... | 9-22 |
| 9.6.4 | Procedures..... | 9-22 |
| 9.7 | Baseline Manager | 9-24 |
| 9.7.1 | Overview..... | 9-24 |
| 9.7.2 | Baseline Terms and Concepts..... | 9-24 |
| 9.7.3 | Baseline Manager (BLM) Outputs Useful at the Sites | 9-28 |
| 9.7.4 | Procedure for Retrieving Baseline Reports | 9-29 |

10. Metadata Administration

| | | |
|--------|---|------|
| 10.1 | ESDT Descriptor Files..... | 10-2 |
| 10.1.1 | Generating Descriptor Files..... | 10-3 |
| 10.1.2 | Verifying Descriptor Files | 10-4 |
| 10.2 | Preparation of Earth Science Data Types | 10-4 |
| 10.2.1 | Definitions | 10-4 |
| 10.2.2 | Process | 10-6 |
| 10.3 | Metadata Population | 10-7 |
| 10.3.1 | Collection-Level Metadata | 10-7 |
| 10.3.2 | Granule-Level Metadata | 10-7 |
| 10.3.3 | Product-Specific Metadata..... | 10-8 |
| 10.4 | Testing and Validation..... | 10-8 |

11. Production Rules – Removed

12. Resource Planning – Removed

13. Production Planning – Removed

14. Production Processing – Removed

15. Quality Assurance

| | | |
|--------|--|------|
| 15.1 | Using the QA Monitor | 15-1 |
| 15.1.1 | Configure QAMUT..... | 15-4 |
| 15.1.2 | Populate DsQAMUTESDTSite Table | 15-8 |
| 15.1.3 | Update QA Metadata Flags Using QAMUT | 15-9 |

16. Ingest

| | | |
|------|---------------------------------|-----|
| 16.1 | Ingest Process | 6-1 |
| 16.2 | Logging in to System Hosts..... | 6-4 |

| | | |
|----------|--|-------|
| 16.2.1 | Log in to System Hosts | 6-4 |
| 16.3 | Monitoring the Ingest System..... | 6-5 |
| 16.3.1 | DPL Ingest GUI | 6-6 |
| 16.3.1.1 | Launching the DPL Ingest GUI | 6-10 |
| 16.3.2 | Monitoring Requests Status | 6-11 |
| 16.3.3 | Viewing Historical Requests | 6-22 |
| 16.3.4 | Provider Status | 6-27 |
| 16.3.5 | File System Status | 6-31 |
| 16.3.6 | Transfer Host Status..... | 6-34 |
| 16.3.7 | Viewing ECS Service Status..... | 6-36 |
| 16.4 | Interventions & Alerts | 6-39 |
| 16.4.1 | Open Intervention | 6-39 |
| 16.4.2 | Viewing System Alerts | 6-48 |
| 16.5 | DPL Ingest Configuration..... | 6-53 |
| 16.5.1 | Data Provider Configuration..... | 6-54 |
| 16.5.2 | Data Type Configuration | 6-64 |
| 16.5.3 | Transfer Host Configuration..... | 6-67 |
| 16.5.4 | File System Configuration | 6-75 |
| 16.5.5 | ECS Service Configuration..... | 6-76 |
| 16.5.6 | Global Tuning Configuration..... | 6-87 |
| 16.5.7 | Configure Volume Groups..... | 6-93 |
| 16.5.8 | Operator Configuration..... | 6-103 |
| 16.6 | Reports | 6-107 |
| 16.6.1 | Reports | 6-107 |
| 16.6.2 | Viewing the Volume Groups History Page | 6-110 |
| 16.7 | Help Pages and Context Help | 6-112 |
| 16.8 | Data Pool Maintenance GUI..... | 6-113 |
| 16.8.1 | Data Pool Maintenance GUI..... | 6-113 |
| 16.8.2 | Managing Data Pool Collection Groups..... | 6-116 |

17. Archive Management/DataPool Maintenance

| | | |
|------|-----------------------------------|------|
| 17.1 | Archive Management Overview | 17-1 |
| 17.2 | Archive Hardware | 17-1 |

| | | |
|---------|---|-------|
| 17.3 | Archive Software | 17-2 |
| 17.4 | Starting and Stopping StorNext | 17-2 |
| 17.4.1 | Starting the StorNext Application..... | 17-3 |
| 17.4.2 | Stopping the StorNext Application..... | 17-5 |
| 17.4.3 | Rebooting the StorNext MetaData Servers..... | 17-6 |
| 17.5 | Loading and Removing Archive Media..... | 17-7 |
| 17.5.1 | Loading Archive Media | 17-7 |
| 17.6 | Deleting Granules | 17-13 |
| 17.6.1 | Generating a GeoID File to Be Used as Input to the Bulk Delete Utility or the Bulk Undelete Utility..... | 17-15 |
| 17.6.2 | Deleting Granules, Phase 1: Running the Bulk Delete Utility | 17-19 |
| 17.6.3 | Deleting Granules, Phase 2: Running the Deletion Cleanup Utility | 17-24 |
| 17.6.4 | Deleting Granules, Phase 3: Running the Archive Batch Delete Utility | 17-34 |
| 17.6.5 | “Undeleting” Granules from the Archive and Inventory | 17-40 |
| 17.7 | Backing Up the StorNext Application | 17-44 |
| 17.7.1 | Executing a StoreNext Backup | 17-46 |
| 17.7.2 | Scheduling a StorNext Backup | 17-48 |
| 17.8 | ACSLs Procedures | 17-49 |
| 17.8.1 | Entering the Archive After StorNext is Started | 17-51 |
| 17.8.2 | Backing Up the ACSLS Database | 17-52 |
| 17.8.3 | Restoring the ACSLS Database..... | 17-52 |
| 17.8.4 | Checking Cleaning Cartridges | 17-53 |
| 17.9 | Data Pool Maintenance Tasks..... | 17-54 |
| 17.9.1 | Features of the Data Pool Maintenance GUI | 17-54 |
| 17.9.2 | Data Pool File Systems | 17-57 |
| 17.9.3 | Cloud Cover | 17-60 |
| 17.9.4 | Batch Summary..... | 17-63 |
| 17.9.5 | List Insert Queue..... | 17-64 |
| 17.9.6 | Configuration Parameters | 17-66 |
| 17.9.7 | Aging Parameters..... | 17-67 |
| 17.9.8 | Collection Groups | 17-68 |
| 17.9.9 | Themes..... | 17-75 |
| 17.9.10 | Help..... | 17-77 |

| | | |
|----------|--|--------|
| 17.10 | Procedures for Using the Data Pool Maintenance GUI | 17-79 |
| 17.10.1 | Launching and Shutting Down the DPM GUI..... | 17-80 |
| 17.10.2 | Monitoring Data Pool Active Insert Processes and Insert Actions..... | 17-82 |
| 17.10.3 | Managing Data Pool File Systems Using the DPM GUI..... | 17-84 |
| 17.10.4 | Managing Cloud Cover Information Using the DPM GUI | 17-88 |
| 17.10.5 | Checking the Status of Batch Inserts | 17-91 |
| 17.10.6 | Checking the Data Pool Insert Queue and Canceling a Data Pool Insert Action | 17-92 |
| 17.10.7 | Managing Data Pool Configuration Parameters and Data Pool Tuning | 17-94 |
| 17.10.8 | Managing Data Pool Collection Groups | 17-100 |
| 17.10.9 | Managing Data Pool Collections within Collection Groups | 17-106 |
| 17.10.10 | Managing Themes Using the DPM GUI | 17-113 |
| 17.11 | Working with Data Pool Scripts | 17-118 |
| 17.11.1 | Extending the Period of Retention for Granules in the Data Pool..... | 17-120 |
| 17.11.2 | Running the Data Pool Cleanup Utility | 17-124 |
| 17.11.3 | Running the Data Pool Access Statistics Utility..... | 17-132 |
| 17.11.4 | Using the Batch Insert Utility | 17-140 |
| 17.11.5 | Running the Bulk Metadata Generation Tool (BMGT)..... | 17-142 |
| 17.11.6 | Running the Bulk URL Utility..... | 17-147 |
| 17.11.7 | Running the Most Recent Data Pool Inserts Utility | 17-149 |
| 17.11.8 | Running the Data Pool Collection-to-Group Remapping Utility | 17-151 |
| 17.11.9 | Running the Data Pool QA Update Utility | 17-152 |
| 17.11.10 | Running the Data Pool Move Collections Utility..... | 17-153 |
| 17.11.11 | Running the Data Pool Hidden Scrambler Utility in Rename Mode..... | 17-155 |

18. Distribution Concepts

| | | |
|--------|---|-------|
| 18.1 | OMS/Distribution Overview..... | 18-1 |
| 18.2 | Changes to OMS/Distribution since Release 7.20..... | 18-2 |
| 18.3 | Order Manager Subsystem (OMS) | 18-6 |
| 18.4 | Logging in to System | 18-8 |
| 18.4.1 | Logging into ECS | 18-8 |
| 18.5 | Launching the Order Manager GUI..... | 18-9 |
| 18.5.1 | Launch the Order Manager GUI..... | 18-12 |

| | | |
|---------|--|--------|
| 18.6 | Monitoring/Controlling Order Manager Operations | 18-14 |
| 18.7 | Viewing Open Intervention Information on the OM GUI | 18-15 |
| 18.7.1 | Viewing Open Intervention Information on the OM GUI | 18-15 |
| 18.7.2 | Setting Refresh Options on OM GUI Pages | 18-21 |
| 18.7.3 | Responding to an Open Intervention | 18-23 |
| 18.8 | Monitoring/Controlling Distribution Request Information on the OM GUI..... | 18-33 |
| 18.8.1 | Monitoring/Controlling Distribution Request Information on the OM GUI... | 18-37 |
| 18.8.2 | Filtering Data Displayed on the Distribution Requests Pages..... | 18-48 |
| 18.8.3 | Changing the Priority of a Distribution Request Using the OM GUI | 18-53 |
| 18.8.4 | Suspending, Resuming, Canceling, Resubmitting, or Stopping a Distribution Request Using the OM GUI..... | 18-56 |
| 18.8.5 | Viewing Processing Services Requests | 18-60 |
| 18.8.6 | Editing Values Assigned to FtpPush Parameters..... | 18-65 |
| 18.8.7 | Annotating a Physical Media Distribution (PMD) Request from the Distribution Request Details Page | 18-67 |
| 18.8.8 | Viewing Open HEG Intervention Information on the OM GUI..... | 18-68 |
| 18.8.9 | Responding to an Open HEG Intervention | 18-74 |
| 18.8.10 | Viewing Pending HEG Granules | 18-78 |
| 18.8.11 | Viewing Operator Alerts on the OM GUI | 18-82 |
| 18.8.12 | Viewing Completed Operator Actions and Interventions on the OM GUI | 18-86 |
| 18.9 | Historical Distribution Requests on the OM GUI | 18-94 |
| 18.9.1 | Viewing Historical Distribution Requests on the OM GUI..... | 18-94 |
| 18.21.2 | Viewing Historical Processing Requests on the OM GUI..... | 18-96 |
| 18.10 | Viewing and Responding to Suspended FTP/SCP Push Distribution Destinations | 18-99 |
| 18.10.1 | Suspended Destinations | 18-99 |
| 18.10.2 | Viewing and Responding to Destination Details on the OM GUI | 18-103 |
| 18.11 | Checking/Modifying OM Queue Status | 18-107 |
| 18.11.1 | Checking/Modifying OM Queue Status | 18-107 |
| 18.11.2 | Checking/Modifying HEG Order Status..... | 18-112 |
| 18.11.3 | Checking Staging Status | 18-114 |
| 18.12 | Checking/Modifying Values Assigned to OM Configuration Parameters | 18-118 |
| 18.12.1 | Checking/Modifying Values Assigned to Aging Parameters | 18-119 |

| | | |
|----------|---|--------|
| 18.12.2 | Checking/Modifying Values Assigned to OMS Server or Database Parameters | 18-122 |
| 18.12.3 | Checking/Modifying Values Assigned to Media Parameters | 18-127 |
| 18.12.4 | Checking/Modifying Values Assigned to Media Creation Parameters ... | 18-132 |
| 18.12.5 | Checking or Modifying ODL Metadata Users Configuration | 18-135 |
| 18.12.6 | External Subsetting Configuration | 18-138 |
| 18.12.7 | Checking/Modifying FTP Push/SCP Policy Configuration | 18-141 |
| 18.12.8 | Adding Destinations to the Frequently Used Destinations List | 18-148 |
| 18.13 | Using OM GUI Help | 18-158 |
| 18.14 | Viewing the OM GUI Log | 18-159 |
| 18.14.1 | Viewing the OM GUI Log | 18-159 |
| 18.15 | Viewing PMD Open Intervention Information on the OM GUI | 18-163 |
| 18.15.1 | Viewing PMD Open Intervention Information on the OM GUI | 18-163 |
| 18.15.2 | Responding to a PMD Open Intervention | 18-171 |
| 18.15.3 | Checking/Modifying PMD Device Configuration | 18-178 |
| 18.15.4 | Filtering Data Displayed on the PMD Device Configuration Page | 18-190 |
| 18.15.5 | Checking/Modifying PMD Printer Configuration | 18-191 |
| 18.15.6 | Checking/Modifying PMD Module Configuration | 18-195 |
| 18.15.7 | Checking PMD Reports | 18-200 |
| 18.15.8 | Monitoring/Controlling PMD Media Creation Using the OM GUI | 18-202 |
| 18.15.9 | Activating PMD Requests | 18-211 |
| 18.15.10 | Failing a PMD Request | 18-218 |
| 18.15.11 | Annotating a PMD Action | 18-221 |
| 18.15.12 | Mounting Media for PMD Production | 18-224 |
| 18.15.13 | Confirming Mount Media for PMD | 18-225 |
| 18.15.14 | Failing Mount Media for PMD | 18-228 |
| 18.15.15 | Collecting Media for PMD QC | 18-231 |
| 18.15.16 | Confirming Media Collection Complete for PMD | 18-232 |
| 18.15.17 | Failing PMD Media Collection | 18-235 |
| 18.15.18 | Activating Media for QC | 18-239 |
| 18.15.19 | Mounting Media for PMD QC | 18-243 |
| 18.15.20 | Assembling PMD Packages | 18-243 |
| 18.15.21 | Marking PMD Request Shipped | 18-244 |
| 18.15.22 | Confirming PMD Media Dismounted | 18-247 |

| | | |
|----------|---|--------|
| 18.15.23 | Confirming PMD Package Assembled | 18-251 |
| 18.15.24 | Marking PMD Package Not Assembled | 18-254 |
| 18.15.25 | Printing PMD Outputs | 18-258 |
| 18.16 | Using the Order Manager Command Line Utility | 18-261 |
| 18.16.1 | Order Manager Command Line Utility | 18-261 |
| 18.16.2 | Running the OM Command Line Utility | 18-261 |
| 18.16.3 | Running the OM Command Line Utility | 18-269 |
| 18.16.4 | OMS Configuration Script (OMS Configuration CI) Activities | 18-271 |
| 18.16.5 | Configuring How Long Order-Tracking Information is Kept in the OMS Database | 18-276 |
| 18.16.6 | Getting OMS Configuration CI Help | 18-281 |
| 18.17 | Tuning Order Manager Subsystem and Data Pool Parameters | 18-282 |
| 18.17.1 | Throttling Archive Staging for Output Devices and FTP Connections ... | 18-283 |
| 18.17.2 | Ensuring the Staging of Low-Priority Requests at a Reasonable Pace ... | 18-283 |
| 18.17.3 | Ensuring That High-Priority Requests Are Expedited | 18-285 |
| 18.18 | OMS Database Cleanup Guidelines | 18-287 |
| 18.18.1 | Removal of Completed OMS Actions, Interventions and Notifications . | 18-287 |
| 18.18.2 | Removal of Order-Tracking Information for Completed Orders | 18-288 |
| 18.18.3 | Fault Recovery | 18-288 |
| 18.18.4 | Fault Handling | 18-289 |
| 18.18.5 | Client Crash and Restart | 18-290 |
| 18.18.6 | Server Crash and Restart | 18-291 |
| 18.18.7 | Request Resubmission | 18-291 |
| 18.19 | Troubleshooting a Order Manager GUI Failure | 18-292 |
| 18.19.1 | Checking the Science Data Server Log Files | 18-304 |
| 18.19.2 | Checking the Archive Server Log Files | 18-308 |
| 18.19.3 | Checking the Staging Disk | 18-309 |
| 18.19.4 | Checking the Staging Disk ALOG File | 18-310 |
| 18.19.5 | Checking the Space Available in the Staging Area | 18-310 |
| 18.19.6 | Checking Log Files | 18-311 |
| 18.19.7 | Checking Database Connections | 18-314 |
| 18.19.8 | Recovering from Order Manager Failures | 18-318 |
| 18.19.9 | Determining the Permissions for Creating an Ftp Pull Subdirectory | 18-323 |
| 18.19.10 | HEG Failures | 18-324 |

| | | |
|----------|--|--------|
| 18.19.11 | Checking HEG Server Log Files | 18-342 |
| 18.19.12 | Checking Files in the HEG Tempfiles Directory..... | 18-353 |

19. User Services – Removed

20. Library Administration

| | | |
|--------|--|------|
| 20.1 | EMD Library Administration Overview..... | 20-1 |
| 20.1.1 | Data Management (DM) | 20-1 |
| 20.2 | Configuration Management (CM) Overview | 20-3 |
| 20.2.1 | Configuration Management (CM) | 20-3 |
| 20.3 | Systems Monitoring Center (SMC) System Overview..... | 20-4 |
| 20.3.1 | Systems Monitoring Center (SMC) System | 20-4 |
| 20.4 | On-Site Documentation Overview..... | 20-4 |
| 20.4.1 | On-Site COTS Document and Software Maintenance | 20-4 |

21. COTS Hardware Maintenance

| | | |
|--------|--|------|
| 21.1 | Overview..... | 21-1 |
| 21.2 | COTS Hardware Maintenance - General..... | 21-1 |
| 21.2.1 | Corrective Maintenance | 21-2 |
| 21.2.2 | Preventive Maintenance..... | 21-2 |
| 21.2.3 | Configuration Management | 21-2 |
| 21.2.4 | COTS Hardware Maintenance Safety..... | 21-2 |
| 21.3 | COTS Hardware Maintenance - Contract Information..... | 21-2 |
| 21.3.1 | COTS Hardware Maintenance Contract | 21-3 |
| 21.3.2 | Information Required to Obtain COTS Hardware Maintenance | 21-3 |
| 21.4 | Hardware Repairs – Standard | 21-3 |
| 21.4.1 | Hardware Problem Reporting | 21-4 |
| 21.4.2 | Hardware Corrective Maintenance Actions..... | 21-4 |
| 21.4.3 | Contract On-Site Hardware Maintenance..... | 21-6 |
| 21.4.4 | Return-to-Depot Support | 21-8 |

| | | |
|--------|---|-------|
| 21.5 | Maintenance Spares | 21-8 |
| 21.5.1 | Use of Maintenance Spares..... | 21-9 |
| 21.5.2 | Return of Failed LRUs..... | 21-9 |
| 21.6 | Non-Standard Hardware Support..... | 21-9 |
| 21.6.1 | Escalation of COTS Hardware Support Problem | 21-9 |
| 21.6.2 | Low Cost Equipment – Not Repaired..... | 21-10 |

22. Software Maintenance

| | | |
|--------|--|------|
| 22.1 | Introduction..... | 22-1 |
| 22.2 | COTS Software Maintenance | 22-1 |
| 22.2.1 | Management of COTS Software Maintenance Contracts..... | 22-2 |
| 22.2.2 | Management of COTS Software Licenses..... | 22-2 |
| 22.2.3 | COTS Software Installation and Upgrades..... | 22-3 |
| 22.2.4 | Obtaining COTS Software Support | 22-3 |
| 22.2.5 | COTS Software Problem Reporting | 22-4 |

23. Property Management

| | | |
|--------|---|------|
| 23.1 | Receipt of Equipment and Software from Vendor | 23-1 |
| 23.2 | Receipt of Equipment and Software from the ILS Property Administrator | 23-3 |
| 23.3 | Equipment Tagging..... | 23-4 |
| 23.4 | Property Records and Reporting..... | 23-5 |
| 23.4.1 | Maintaining Property Records | 23-5 |
| 23.4.2 | Reporting Loss, Theft, Damage or Destruction | 23-5 |
| 23.5 | Equipment Relocation..... | 23-6 |
| 23.5.1 | Intra-Site Relocation | 23-6 |
| 23.5.2 | Inter-Site Relocation | 23-6 |
| 23.5.3 | External Transfers..... | 23-6 |
| 23.6 | Inventories and Audits | 23-7 |
| 23.7 | Storage | 23-7 |
| 23.7.1 | Segregation Requirements | 23-7 |
| 23.7.2 | Stock Rotation..... | 23-8 |

| | | |
|--------|---|------|
| 23.7.3 | Physical Security..... | 23-8 |
| 23.8 | Packing and Shipping | 23-8 |
| 23.9 | Electrostatic Discharge (ESD) Program | 23-8 |

24. Installation Planning

| | | |
|------|--|------|
| 24.1 | Overview..... | 24-2 |
| 24.2 | Responsibilities..... | 24-2 |
| 24.3 | Process Description..... | 24-2 |
| 24.4 | Maintenance of Hardware Diagrams | 24-3 |

25. COTS Training

| | | |
|------|---|------|
| 25.1 | Requesting COTS Training | 25-1 |
| 25.2 | Coordinating COTS Training | 25-2 |
| 25.3 | Canceling/Rescheduling COTS Training | 25-3 |
| 25.4 | Contractor COTS Training Funds Accounting | 25-3 |

26. System Science Integration & Test – Removed

27. Inventory Logistical Management (ILM)

| | | |
|--------|---|-------|
| 27.1 | ILM [Inventory, Logistics and Maintenance (ILM) Manager]..... | 27-1 |
| 27.2 | Remedy User Tool Overview | 27-6 |
| 27.2.1 | Navigating Remedy User Tool | 27-6 |
| 27.2.2 | Defining Search Criteria | 27-8 |
| 27.2.3 | ILM Predefined Reports | 27-13 |
| 27.3 | Property Management..... | 27-14 |
| 27.3.1 | ILM-EIN GUI | 27-14 |
| 27.3.2 | ILM-EIN Structure GUI | 27-42 |
| 27.3.3 | ILM-EIN Transaction GUI | 27-43 |
| 27.3.4 | ILM-Transaction Log | 27-60 |
| 27.3.5 | ILM-OEM Parts | 27-64 |

| | | |
|---------|--------------------------------------|--------|
| 27.3.6 | ILM-Vendor-MFR GUI | 27-66 |
| 27.3.7 | ILM-HwSw Codes GUI | 27-67 |
| 27.3.8 | ILM-Status Codes GUI | 27-69 |
| 27.3.9 | ILM-Maint Contract GUI | 27-70 |
| 27.3.10 | ILM-Sites GUI | 27-75 |
| 27.3.11 | ILM-Inventory Location GUI | 27-76 |
| 27.4 | Maintenance Management | 27-77 |
| 27.4.1 | ILM-MWO GUI | 27-77 |
| 27.4.2 | ILM-MWO Line Item GUI | 27-90 |
| 27.5 | License Management | 27-102 |
| 27.5.1 | ILM-License Products GUI | 27-103 |
| 27.5.2 | ILM-License Entitlement GUI | 27-106 |
| 27.5.3 | ILM-License GUI | 27-112 |
| 27.5.4 | ILM-License Mapping GUI | 27-125 |
| 27.5.5 | ILM-Additional Host GUI | 27-127 |
| 27.6 | System Administrator Functions | 27-128 |
| 27.6.1 | ILM-System Parameters | 27-128 |
| 27.6.2 | User GUI | 27-130 |
| 27.6.3 | Remedy's Admin Tool GUI | 27-132 |
| 27.6.4 | Databases | 27-134 |
| 27.6.5 | Special Constraints | 27-134 |
| 27.6.6 | Event and Error Messages | 27-134 |

28. Maintenance of Configuration Parameters

| | | |
|--------|--|------|
| 28.1 | Parameter Change Control Procedure | 28-1 |
| 28.2 | Overview of Configuration Parameter Files | 28-2 |
| 28.3 | Overview of Configuration Registry | 28-2 |
| 28.3.1 | Registry Deployment and Baseline Maintenance | 28-3 |
| 28.3.2 | How to Run a Mkcfg | 28-4 |
| 28.3.3 | Registry | 28-4 |
| 28.3.4 | How to Apply a Registry Patch | 28-4 |
| 28.3.5 | How to Run the Registry Population Tool | 28-4 |

| | | |
|--------|--|------|
| 28.4 | Configuration Registry Procedures..... | 28-6 |
| 28.4.1 | Registry Preparation Procedure | 28-6 |
| 28.4.2 | Registry Database Backup Procedure..... | 28-7 |
| 28.4.3 | Registry Patch Procedure..... | 28-7 |
| 28.4.4 | Display Parameters Using the Configuration Registry GUI..... | 28-8 |

List of Figures

| | | |
|----------------|---|------|
| Figure 3.10-1. | ECS Whazzup Initial Display | 3-14 |
| Figure 3.10-2. | Host Status Pop-Up Display | 3-16 |
| Figure 3.10-3. | Host Status Data Display | 3-17 |
| Figure 3.10-4. | Mode Status Pop-Up Display..... | 3-18 |
| Figure 3.10-5. | Mode Status Data Display..... | 3-19 |
| Figure 3.10-6. | Verify Mode Pop-Up Display | 3-20 |
| Figure 3.10-7. | Verify Mode Data Display..... | 3-21 |
| Figure 3.10-8. | Performance Management Selection Display | 3-22 |
| Figure 3.10-9. | Performance Management Data Display | 3-23 |
| Figure 3.11-1. | ECS Health Check GUI at Startup..... | 3-24 |
| Figure 3.11-2. | ECS Health Check GUI Having Detected an Error | 3-25 |
| Figure 3.12-1. | ECS Assistant GUI Manager Windows | 3-29 |
| Figure 3.12-2. | ECS Monitor GUI | 3-30 |
| Figure 3.13-1. | Networker Administrative Main Screen | 3-34 |
| Figure 3.13-2. | Jukebox Labeling Window | 3-36 |
| Figure 3.13-3. | Tape Index Following the Initial Inventory | 3-38 |
| Figure 3.13-4. | Tapes Changed But Not Re-Inventoried..... | 3-39 |
| Figure 3.13-5. | Index is Updated after Re-Inventory..... | 3-40 |
| Figure 3.13-6. | Jukebox Mounting Window..... | 3-41 |
| Figure 3.14-1. | Networker Schedules Window..... | 3-44 |
| Figure 3.14-2. | Networker Backup Window | 3-47 |
| Figure 3.14-3. | Networker Recovery Window..... | 3-50 |

| | |
|--|------|
| Figure 3.14-4. Tapes Required for Full System Restore | 3-52 |
| Figure 3.14-5. Networker Administrator's Window | 3-54 |
| Figure 3.15-1. /etc/passwd.yp File Fields | 3-59 |
| Figure 3.15-2. /etc/group File | 3-59 |
| Figure 3.15-3. Access Permissions | 3-63 |
| Figure 4.1-1. Earth Science Information Model | 4-5 |
| Figure 4.1-2. An Example of Data Product Levels..... | 4-6 |
| Figure 4.1-3. Database Replication..... | 4-12 |
| Figure 4.2-1. Sybase Central..... | 4-18 |
| Figure 4.5-1. Example of an add_devices.sql File for Creation of a Database Device | 4-29 |
| Figure 4.7-1. Example of sp_configure Output | 4-38 |
| Figure 4.7-2. Configuration Registry | 4-41 |
| Figure 4.7-3. Configuration Registry Attributes Pop-Up Window | 4-42 |
| Figure 4.8-1. Example of Creation of a Database Segment Template File | 4-46 |
| Figure 4.9-1. Sample template.sql File for Creation of a Database..... | 4-55 |
| Figure 4.9-2. Completed Create Database Script | 4-56 |
| Figure 4.10-1. Sample template.sql File for New Database User Login | 4-61 |
| Figure 8.3-1. Main TestTrack Pro Trouble Ticket GUI | 8-8 |
| Figure 8.3-2. TestTrack Pro Log Server GUI..... | 8-11 |
| Figure 8.3-3. Add Trouble Ticket GUI..... | 8-12 |
| Figure 8.3-4. TestTrack Pro WEB Login GUI | 8-14 |
| Figure 8.3-5. TestTrack Pro PC Client Login GUI..... | 8-15 |
| Figure 8.3-6. License Server Admin Utility GUI | 8-16 |
| Figure 8.3-7. Users GUI | 8-18 |
| Figure 9.2-1. Configuration Change Request (CCR) Form..... | 9-4 |
| Figure 9.2-2. TestTrack Pro Workflow of Events | 9-6 |
| Figure 9.2-3. EMD CCR Impact Analysis (1 of 2)..... | 9-9 |
| Figure 9.2-4. Workflow Diagram for EMD CM Administrator | 9-13 |

| | |
|--|-------|
| Figure 9.2-5. Workflow Diagram for Site-level CM Administrator..... | 9-16 |
| Figure 9.7-1. EMD Baseline Concept from a Design (CIL/CAL) View | 9-26 |
| Figure 9.7-2. EMD Baseline Concept from an Operational (Network) View | 9-27 |
| Figure 9.7-3. EMD Baseline Concept from an Operational (Subsystem) View..... | 9-27 |
| Figure 9.7-4. Sample EBIS Page | 9-31 |
| Figure 10.2-1. The ESDT Generation Process | 10-5 |
| Figure 10.2-2. Steps in ESDT Development | 10-7 |
| Figure 15.1-1. Sample Metadata QA Update Request..... | 15-4 |
| Figure 16.1-1. Data Pool Ingest High Level Architecture..... | 6-2 |
| Figure 16.3-1. Data Pool Ingest GUI Intro Screen | 6-8 |
| Figure 16.5-1. Dynamic and Static Configuration Icons | 6-88 |
| Figure 16.5-2. Volume Groups Configuration (listing page) | 6-93 |
| Figure 16.5-3. Operator Configuration Page | 6-104 |
| Figure 16.6-1. Report Setup Page..... | 6-108 |
| Figure 16.7-1. Help – General Topics | 6-112 |
| Figure 17.9-1. Security Login Prompt..... | 17-55 |
| Figure 17.9-2 DPM GUI Home Page | 17-56 |
| Figure 17.9-3. Data Pool File System Information Page..... | 17-58 |
| Figure 17.9-4. Add New File System Page..... | 17-59 |
| Figure 17.9-5. Modify File System Information Page..... | 17-60 |
| Figure 17.9-6. Cloud Cover Information Page | 17-61 |
| Figure 17.9-7. Add New Cloud Cover Information Page..... | 17-62 |
| Figure 17.9-8. Modify Source Description Page | 17-63 |
| Figure 17.9-9. Batch Summary Page | 17-64 |
| Figure 17.9-10. List Insert Queue Page | 17-65 |
| Figure 17.9-11. Sample DPM GUI Pages for .XML File Path and Content | 17-66 |
| Figure 17.9-12. List of Configuration Parameters Page | 17-67 |
| Figure 17.9-13. Aging Parameters Page | 17-68 |

| | |
|---|--------|
| Figure 17.9-14. Collection Groups Page | 17-69 |
| Figure 17.9-15. Collection Group Detail Page | 17-70 |
| Figure 17.9-16. Collection Detail Page | 17-71 |
| Figure 17.9-17. Modify Collection Page | 17-72 |
| Figure 17.9-18. Collections Not in Data Pool Page..... | 17-73 |
| Figure 17.9-19. Add New [ECS] Collection Page..... | 17-74 |
| Figure 17.9-20. Modify Collection Group Page | 17-75 |
| Figure 17.9-21. Detailed List of Data Pool Themes Page | 17-76 |
| Figure 17.9-22. Add New Theme Page | 17-77 |
| Figure 17.9-23. Modify Theme Page..... | 17-78 |
| Figure 17.9-24. Help Page | 17-79 |
| Figure 17.11-1. The Data Pool Cleanup Utility Uses Expiration Date, Retention Priority, and/or Theme Association to Qualify Granules, Marked with X, for Deletion | 17-125 |
| Figure 18.2-1. System Context Diagram | 18-4 |
| Figure 18.2-2. Order Manager Subsystem (OMS) Context Diagram | 18-5 |
| Figure 18.5-1. Security Login Prompt | 18-13 |
| Figure 18.5-2. Order Manager Page | 18-14 |
| Figure 18.7-1. Open Interventions Page | 18-16 |
| Figure 18.7-2. ECS Order Page | 18-18 |
| Figure 18.7-3. Open Intervention for Request Page | 18-19 |
| Figure 18.7-4. Close Confirmation for intervention (FTP/SCP Push) | 18-28 |
| Figure 18.7-5. Close Confirmation (PMD)..... | 18-29 |
| Figure 18.7-6. Close Confirmation Page Showing Additional E-Mail Text Box..... | 18-31 |
| Figure 18.7-7. Intervention Disposition Page..... | 18-32 |
| Figure 18.8-1. Distribution Requests Page | 18-34 |
| Figure 18.8-2. Staging Distribution Requests Page..... | 18-35 |
| Figure 18.8-3. FtpScpPush Distribution Requests Page..... | 18-36 |
| Figure 18.8-4. Distribution Request Detail (DISTRIBUTION REQUEST X) Page (Physical Media)..... | 18-41 |

| | |
|---|--------|
| Figure 18.8-5. Distribution Request Detail (DISTRIBUTION REQUEST X) Page (Non-Physical Media)..... | 18-42 |
| Figure 18.8-6. Distribution Requests Filters Pop-Up Window | 18-49 |
| Figure 18.8-7. Destination Details Page (Ftp Push Monitor – Suspended Destination Name OTHER) | 18-55 |
| Figure 18.8-8. Suspend Request Dialogue Box..... | 18-57 |
| Figure 18.8-9. Resume Request Confirmation Dialogue Box | 18-58 |
| Figure 18.8-10. Cancel Request Confirmation Dialogue Box..... | 18-59 |
| Figure 18.8-11. Resubmit Request Confirmation Dialogue Box..... | 18-59 |
| Figure 18.8-12. Processing Services Requests | 18-63 |
| Figure 18.8-13. Processing Services Requests Filter..... | 18-64 |
| Figure 18.8-14. Edit FtpPush Parameters Page | 18-66 |
| Figure 18.8-15. Open HEG Interventions Page..... | 18-69 |
| Figure 18.8-16. Open HEG Intervention Detail (Intervention for Request X) Page | 18-72 |
| Figure 18.8-17. Processing Instructions Window..... | 18-73 |
| Figure 18.8-18. Close Confirmation Page for HEG Intervention..... | 18-77 |
| Figure 18.8-19. Pending HEG Granules Page | 18-80 |
| Figure 18.8-20. Operator Alerts Page..... | 18-83 |
| Figure 18.8-21. Suspended Host Detail Page | 18-87 |
| Figure 18.8-22. Completed Operator Actions and Interventions Page..... | 18-88 |
| Figure 18.8-23. Completed Intervention/Action Detail (Completed Operator Intervention/Action for Request X) Page | 18-91 |
| Figure 18.9-1. Historical Distribution Requests Page | 18-95 |
| Figure 18.9-2. Historical Processing Requests | 18-97 |
| Figure 18.9-3. Historical Processing Requests Filter | 18-98 |
| Figure 18.10-1. Suspended Destinations Monitor | 18-100 |
| Figure 18.11-1. OM Queue Status Page | 18-107 |
| Figure 18.11-2. OM Queue Status Page - Text-Only Version..... | 18-110 |
| Figure 18.11-3. HEG Order Status Page..... | 18-113 |
| Figure 18.11-4. Staging Status by Media Type Page | 18-116 |

| | |
|---|--------|
| Figure 18.11-5. Staging Status by FTP Push/SCP Destination Page..... | 18-117 |
| Figure 18.12-1. Aging Parameters Page | 18-120 |
| Figure 18.12.-2. OMS Server and Database Configuration Page..... | 18-123 |
| Figure 18.12-3. Media Configuration Page | 18-128 |
| Figure 18.12-4. “Remember Values” Confirmation Dialogue Box..... | 18-131 |
| Figure 18.12-5. Media Creation Configuration Page | 18-133 |
| Figure 18.12-6. ODL Metadata File Users Configuration..... | 18-136 |
| Figure 18.12-7. Add a Metadata User..... | 18-137 |
| Figure 18.12-8. Delete Metadata User..... | 18-138 |
| Figure18.12-9. External Subsetting Configuration..... | 18-140 |
| Figure 18.27-10. Add External Subsetting Configuration..... | 18-141 |
| Figure 18.12-11. FTP Push/SCP Policy Configuration Page | 18-142 |
| Figure 18.12-12. FTP Push/SCP Destination Details Page | 18-145 |
| Figure 18.12-13. Add New Destination Page | 18-148 |
| Figure 18.12-14. “Done” Confirmation Dialogue Box..... | 18-152 |
| Figure 18.13-1. Example of HelpOnDemand | 18-159 |
| Figure 18.14-1. OM GUI Help Page..... | 18-160 |
| Figure 18.14-2. OM GUI Log Viewer Page | 18-161 |
| Figure 18.14-2. Example of OM GUI Log Contents | 18-163 |
| Figure 18.15-1. Open Physical Media Interventions Page | 18-164 |
| Figure 18.15-2. PMD Open Intervention Detail (Intervention for Request X) Page | 18-169 |
| Figure 18.15.3. Granule List for Volume Y of Request X | 18-174 |
| Figure 18.15-4. PMD Device Configuration Page | 18-179 |
| Figure 18.15-5. Pop-Up Dialogue Box for Changing the On-Line/Off-Line Status of a Device | 18-181 |
| Figure 18.15-6. Add New Device Page | 18-183 |
| Figure 18.15-7. Add New Device Page with Device Type Radio Buttons | 18-184 |
| Figure 18.15-8. Add New Device Page - QC | 18-185 |
| Figure 18.15-9. Add New Device Page – Production and QC | 18-186 |

| | |
|--|--------|
| Figure 18.18-10. Add New Device Page – Production (Luminex) | 18-187 |
| Figure 18.15-11. Add New Device Page – Production (Tape) | 18-188 |
| Figure 18.15-12. PMD Printer Configuration Page | 18-192 |
| Figure 18.15-13. PMD Printer Configuration Page with Edit Parameters Area..... | 18-193 |
| Figure 18.15-14. PMD Production Module Configuration Page..... | 18-196 |
| Figure 18.15-15. Add New Production Module Table (PMD Production Module Configuration Page..... | 18-198 |
| Figure 18.15-16. PMD Report Summary Page..... | 18-200 |
| Figure 18.15-17. Media Creation Actions Page | 18-203 |
| Figure 18.15-18. Activate Request Dialogue Box for Tape Media | 18-215 |
| Figure 18.15-19. Activate Request Dialogue Box for Disk Media | 18-216 |
| Figure 18.15-21. Fail Request Page..... | 18-219 |
| Figure 18.15-22. Annotate Action Page | 18-222 |
| Figure 18.15-23. Confirm Mount Media Page | 18-225 |
| Figure 18.15-24. Fail Mount Media Page..... | 18-229 |
| Figure 18.15-25. Media Collection Complete Page | 18-233 |
| Figure 18.15-26. Fail Media Collection Page..... | 18-237 |
| Figure 18.15-27. Activate QC Dialogue Box | 18-240 |
| Figure 18.15-28. Mark Request Shipped Page | 18-245 |
| Figure 18.15-29. Confirm Media Dismounted Page..... | 18-249 |
| Figure 18.15-30. Confirm Package Assembled Page | 18-252 |
| Figure 18.15-31. Package Not Assembled Page..... | 18-255 |
| Figure 18.15-32. Print Outputs Page | 18-259 |
| Figure 18.15-33. Print Outputs Page for Tape Media..... | 18-259 |
| Figure 18.16-1. OMS Configuration CI Main Menu..... | 18-275 |
| Figure 18.16-2. Configure Order Tracking Data Menu..... | 18-277 |
| Figure 20-1. The EDHS Home Page, the EMD Baseline Information Home Page, and the Systems Monitoring Center Home Page..... | 20-1 |
| Figure 23.3-1. EMD Property Tags (Actual Size)..... | 23-4 |

| | |
|--|-------|
| Figure 27.2.1-1. Open GUI..... | 27-6 |
| Figure 27.2.2.1-1. Search by Example..... | 27-8 |
| Figure 27.2.2.2-1. Using the Advanced Search Bar | 27-10 |
| Figure 27.3.1-1. ILM-EIN (Part Info and Location & Purchasing Info) GUI..... | 27-15 |
| Figure 27.3.1-2. ILM-EIN (Maintenance & Other Info.) GUI | 27-16 |
| Figure 27.3.1-3. ILM-EIN (Components) GUI | 27-17 |
| Figure 27.3.1-4. ILM-EIN (Maintenance Contract) GUI | 27-18 |
| Figure 27.3.1-5. ILM-EIN (History) GUI..... | 27-19 |
| Figure 27.3.1.1-1. ILM-EIN Reports GUI..... | 27-24 |
| Figure 27.3.1.1-2. ILM-DIA Reports GUI | 27-30 |
| Figure 27.3.1.1-3. Report To File GUI | 27-30 |
| Figure 27.3.1.1-4. Text Import Wizard GUI..... | 27-31 |
| Figure 27.3.1.1-5. Enter Parameter Values GUI..... | 27-31 |
| Figure 27.3.1.1-6. Install/Receipt Report GUI | 27-32 |
| Figure 27.3.1.1-7. Installation Report GUI..... | 27-33 |
| Figure 27.3.1.1-8. Purchase Order Cost Report GUI..... | 27-34 |
| Figure 27.3.1.1-9. Parent EIN Report GUI..... | 27-35 |
| Figure 27.3.1.1-10. Parent EIN & Total System Cost Report GUI | 27-36 |
| Figure 27.3.1.1-11. Inventory Report GUI | 27-37 |
| Figure 27.3.1.1-12. Quarterly Property Management Report GUI..... | 27-38 |
| Figure 27.3.1.1-13. Cost – Selected ECS Managed Report GUI..... | 27-39 |
| Figure 27.3.1.1-14. EIN Transaction History Report | 27-40 |
| Figure 27.3.1.1-15. Spare Equipment Report GUI | 27-41 |
| Figure 27.3.2-1. ILM-EIN Structure GUI..... | 27-42 |
| Figure 27.3.3-1. ILM-EIN Transaction GUI (Install/Move/Ship/RTS) | 27-44 |
| Figure 27.3.3-2. ILM-EIN Transaction GUI (Relocation) | 27-45 |
| Figure 27.3.3-3. ILM-EIN Transaction GUI (Archive)..... | 27-46 |
| Figure 27.3.3-4. ILM-TRS Dialog GUI..... | 27-57 |

| | |
|--|--------|
| Figure 27.3.3.1-1. ILM-Process Component GUI | 27-58 |
| Figure 27.3.4-1. ILM-Transaction Log GUI..... | 27-60 |
| Figure 27.3.4-3. ECS Shipping Report GUI..... | 27-63 |
| Figure 27.3.5-1. ILM-OEM Parts GUI | 27-64 |
| Figure 27.3.6-1. ILM-Vendor-MFR GUI | 27-66 |
| Figure 27.3.7-1. ILM-HwSw Codes GUI | 27-68 |
| Figure 27.3.8-1. ILM-Status Codes GUI | 27-69 |
| Figure 27.3.9-1. ILM-Maint Contract GUI..... | 27-70 |
| Figure 27.3.9-3. Maintenance Contract Report GUI | 27-74 |
| Figure 27.3.10-1. ILM-Sites GUI | 27-75 |
| Figure 27.3.11-1. ILM-Inventory Location GUI | 27-76 |
| Figure 27.4.1-1. ILM-MWO GUI – Parent Information | 27-78 |
| Figure 27.4.1-2. ILM-MWO GUI - Failure and Vendor Contact..... | 27-79 |
| Figure 27.4.1-3. ILM-MWO GUI – ALDT | 27-80 |
| Figure 27.4.1-4. ILM-MWO GUI - Total Down Time..... | 27-81 |
| Figure 27.4.1-5. ILM-MWO GUI - Failed & Replacement Components | 27-82 |
| Figure 27.4.1-6. Work Order Verification Report GUI..... | 27-88 |
| Figure 27.4.1-7. RMA Report GUI..... | 27-89 |
| Figure 27.4.2-1. ILM-MWO Line Item GUI | 27-90 |
| Figure 27.5.1-1. ILM-License Products GUI | 27-104 |
| Figure 27.5.2-1. ILM-License Entitlement GUI..... | 27-106 |
| Figure 27.5.2-4. License Entitlement Status Report GUI..... | 27-112 |
| Figure 27.5.3-1. ILM-License GUI | 27-113 |
| Figure 27.5.3-3. ILM-DIA-Lic Report GUI | 27-122 |
| Figure 27.5.3-4. License Allocation By Host Report GUI | 27-123 |
| Figure 27.5.3-5. License Allocation By Product Report GUI | 27-124 |
| Figure 27.5.4-1. ILM-License Mapping GUI..... | 27-125 |
| Figure 27.5.5-1. ILM-Additional Host GUI | 27-127 |

| | |
|--|--------|
| Figure 27.6.1-1. ILM-System Parameters GUI | 27-129 |
| Figure 27.6.2-1. User GUI | 27-131 |
| Figure 27.6.3-1. Admin Tool GUI | 27-133 |

List of Tables

| | |
|--|------|
| Table 3.3-1. SSH - Activity Checklist | 3-2 |
| Table 3.6-1. Login to System Hosts - Activity Checklist | 3-4 |
| Table 3.7-1. System Startup and Shutdown - Activity Checklist | 3-6 |
| Table 3.10-1. Whazzup - Activity Checklist | 3-13 |
| Table 3.11-1. ECS Health Check - Activity Checklist | 3-24 |
| Table 3.12-1. ECS Assistant - Activity Checklist | 3-28 |
| Table 3.13-1. Tape Operations - Activity Checklist | 3-33 |
| Table 3.14-1. System Backup and Restores - Activity Checklist | 3-43 |
| Table 3.15-1. User Administration - Activity Checklist | 3-56 |
| Table 3.17-1. Security - Activity Checklist | 3-67 |
| Table 4.1-1. Data Product Level Definitions | 4-7 |
| Table 4.1-2. Subsystem Functions | 4-8 |
| Table 4.1-3. Custom Databases | 4-9 |
| Table 4.1-4. Flat Files | 4-11 |
| Table 4.1-5. Resident Databases | 4-12 |
| Table 4.1-6. Location of Principal Database Components | 4-14 |
| Table 4.2-1. Sybase Adaptive Server Enterprise (ASE) Components | 4-17 |
| Table 4.3-1. DBA Tasks Performed on a Regular Basis | 4-21 |
| Table 4.4-1. Starting and Stopping Database Servers - Activity Checklist | 4-22 |
| Table 4.5-1. Creating Database Devices - Activity Checklist | 4-28 |
| Table 4.6-1. Installing Databases and Patches - Activity Checklist | 4-32 |
| Table 4.7-1. Configuring Databases - Activity Checklist | 4-36 |
| Table 4.8-1. Working with Indexes, Segments, and Caches - Activity Checklist | 4-44 |

| | |
|---|------|
| Table 4.9-1. Backing Up and Recovering Data - Activity Checklist | 4-48 |
| Table 4.9-2. Automatic Backup Files | 4-49 |
| Table 4.9-3. Files That Need to Be Modified before Running Scripts | 4-51 |
| Table 4.9-4. Automatic Backup Components | 4-51 |
| Table 4.10-1. Roles and Privileges | 4-58 |
| Table 4.10-2. Establishing Database Security - Activity Checklist | 4-59 |
| Table 4.12-1. Bulk Copying - Activity Checklist | 4-66 |
| Table 4.13-1. Replication System Administrator Tasks | 4-68 |
| Table 4.13-2. DAAC DBA Replication Roles and Tasks | 4-69 |
| Table 4.14-1. Tuning Options | 4-72 |
| Table 4.16-1. Sybase Troubleshooting - Activity Checklist | 4-73 |
| Table 5.2-1. Crack - Activity Checklist | 5-2 |
| Table 5.2-2. ANLpasswd - Activity Checklist | 5-8 |
| Table 5.4-1. Secure Access through Secure Shell - Activity Checklist | 5-12 |
| Table 5.5.1-1. Operator Functions | 5-19 |
| Table 7.2-1. Common functions performed by Big Brother | 7-1 |
| Table 7.4-1. ECS Health Check - Activity Checklist | 7-2 |
| Table 7.5-1. Monitoring and Managing Server Applications - Activity Checklist | 7-4 |
| Table 8.3-1. Trouble Ticket Priority/NCR Severity | 8-6 |
| Table 8.3-2. Trouble Ticket System - Activity Checklist | 8-7 |
| Table 8.3-3. TestTrack Pro Trouble Tickets MAIN GUI Field Description | 8-9 |
| Table 8.3-4. Trouble Ticket TAB Description | 8-10 |
| Table 8.3-5. Edit TestTrack Pro Server GUI's Field Descriptions | 8-11 |
| Table 8.3-6. Table of Access Control Groupings | 8-18 |
| Table 8.3-7. Report Types in TestTrack Pro | 8-21 |
| Table 8.4-1. Example of Emergency Change Procedure | 8-23 |
| Table 9.2-1. State Table Composition in TestTrack Pro Format | 9-5 |
| Table 10.1-1. ESDT Descriptor - Activity Checklist | 10-2 |

| | |
|---|-------|
| Table 15.1-1. Using the QAMUT - Activity Checklist | 15-2 |
| Table 15.1-2. Configuration File Parameters for QAMUT (1 of 2) | 15-5 |
| Table 15.1-2. Configuration File Parameters for QAMUT (2 of 2) | 15-6 |
| Table 15.1-3. Populate DsQAMUTESDTSite Table..... | 15-8 |
| Table 16.2-1. Login to System Hosts - Activity Checklist..... | 6-4 |
| Table 16.3-1. Monitoring DPL Ingest | 6-7 |
| Table 16.3-2. Home Page Field Descriptions | 6-9 |
| Table 16.3-3. Request Status Page Column Descriptions | 6-11 |
| Table 16.3-4. Ingest Request Status Allowed Actions | 6-12 |
| Table 16.4-1. Interventions & Alerts | 6-39 |
| Table 16.5-1. Modifying DPL Ingest Configuration | 6-53 |
| Table 16.5-2. Data Provider Configuration Parameter Descriptions..... | 6-54 |
| Table 16.5-3. Polling Location Detail Page Field Descriptions | 6-57 |
| Table 16.5-4. Data Type Configuration Page Field Descriptions..... | 6-64 |
| Table 16.5-5. SCP/FTP Host Page Field Descriptions | 6-68 |
| Table 16.5-6. Archive File Systems Configuration Page Field Descriptions..... | 6-75 |
| Table 16.5-7. ECS Services Configuration Field Description..... | 6-77 |
| Table 16.5-8. ECS Services Configurable Field Descriptions..... | 6-77 |
| Table 16.5-9. Global Tuning Parameter Descriptions | 6-89 |
| Table 16.5-10. Volume Groups Configuration Page Field Descriptions..... | 6-94 |
| Table 16.5-11. Add Volume Group Page Field Description | 6-94 |
| Table 16.5-12. Volume Group Naming | 6-96 |
| Table 16.6-1. Reports..... | 6-107 |
| Table 16.6-2. Volume Groups History Page Field Description..... | 6-110 |
| Table 16.8-1. Data Pool Maintenance | 6-113 |
| Table 17.4-1. Starting and Stopping StorNext..... | 17-3 |
| Table 17.5-1. Loading and Removing Archive Media - Activity Checklist..... | 17-7 |
| Table 17.6-1. Deleting Granules - Activity Checklist | 17-14 |

| | |
|--|--------|
| Table 17.7-1. StorNext Backup Procedures - Activity Checklist | 17-46 |
| Table 17.8-1. ACSLS Command Reference | 17-49 |
| Table 17.8-2. ACSLS Utilities | 17-50 |
| Table 17.8-3. ACSLS Procedures - Activity Checklist | 17-51 |
| Table 17.10-1. Data Pool Maintenance Tasks - Activity Checklist | 17-79 |
| Table 17.11-1. Data Pool Scripts - Activity Checklist | 17-120 |
| Table 18.4-1. ESDT Descriptor - Activity Checklist | 18-8 |
| Table 18.5-1. ESDT Descriptor - Activity Checklist | 18-11 |
| Table 18.7-1. Open Interventions - Activity Checklist | 18-15 |
| Table 18.8-1. Monitoring/Controlling Distribution Requests - Activity Checklist | 18-37 |
| Table 18.9-1. Historical Distribution Requests - Activity Checklist | 18-94 |
| Table 18.9-1. Suspended FTP/SCP Push Distribution Destinations - Activity Checklist | 18-99 |
| Table 18.11-1. Checking/Modifying OM Queue Status - Activity Checklist | 18-108 |
| Table 18.12-1. Checking/Modifying Values Assigned to OM Configuration Parameters - Activity Checklist | 18-120 |
| Table 18.12-2. External Processing Parameters | 18-139 |
| Table 18.15-1. Viewing PMD Open Intervention - Activity Checklist | 18-164 |
| Table 18.16-1. Using Order Manager Command Line Utility - Activity Checklist | 18-262 |
| Table 18.19-1. Order Manager GUI User Messages | 18-293 |
| Table 18.19-2. Troubleshooting Order Manager GUI Failure - Activity Checklist | 18-305 |
| Table 18.19-3. Recovering from Order Manager Failures | 18-318 |
| Table 18.19-4. Troubleshooting HEG Problems | 18-326 |
| Table 21.4-1. DAAC Hardware Problem Reporting Procedures | 21-4 |
| Table 21.4-2. Hardware Corrective Maintenance Actions | 21-5 |
| Table 21.4-3. Obtaining On-Site Hardware Maintenance Support | 21-6 |
| Table 21.4-4. Procedure for Return to Depot (Advance Replacement and Return before Replacement) | 21-8 |
| Table 21.6-1. Procedure for Time and Material Support | 21-9 |
| Table 22.2-1. COTS Maintenance - Activity Outline | 21-2 |

| | |
|---|-------|
| Table 23.1-1. Procedure for the Receipt of Property | 23-2 |
| Table 23.1-2. Procedure for Completion of the Inventory Worksheet | 23-2 |
| Table 23.1-3. Procedure for Completion of the Non Conforming Product Report | 23-3 |
| Table 23.1-4. Receiving Process Checklist | 23-3 |
| Table 23.2-1. LMC Actions for Property Received from the ILS Property Administrator.... | 23-4 |
| Table 24.3-1. Installation Planning Activity Outline..... | 24-3 |
| Table 25.1-1. COTS Training - Activity Checklist | 25-1 |
| Table 27.1-1. Common Operator Functions Performed with ILM..... | 27-2 |
| Table 27.1-2. Remedy-ILM Groups Description..... | 27-3 |
| Table 27.2.2.1-1. Relational Operators Used in the Query Window..... | 27-9 |
| Table 27.2.2.2-1. Operators Used in the Advanced Search Bar | 27-11 |
| Table 27.2.2.2-2. Wildcard Symbols | 27-12 |
| Table 27.2.2.2-3. Using Keywords | 27-12 |
| Table 27.2.3-1. ILM Pre-Defined Reports..... | 27-13 |
| Table 27.3.1-1. ILM-EIN Form Field Description | 27-20 |
| Table 27.3.1-2. Add New Inventory Item..... | 27-22 |
| Table 27.3.1-3. Modifying EIN Record..... | 27-23 |
| Table 27.3.1.1-1. ILM-EIN Pre-Defined Reports..... | 27-25 |
| Table 27.3.1.1-2. Procedures to Generate ILM-EIN Predefined Reports..... | 27-26 |
| Table 27.3.2-1. ILM-EIN Structure Field Descriptions..... | 27-43 |
| Table 27.3.3-1. ILM-EIN Transaction Form Field Descriptions..... | 27-47 |
| Table 27.3.3-2. Procedures to Perform EIN Transactions | 27-49 |
| Table 27.3.3.1-1. ILM-Component to Process Field Descriptions..... | 27-59 |
| Table 27.3.4-1. ILM-Transactions Field Descriptions | 27-61 |
| Table 27.3.4-2. Procedures to Generate EIN Shipment Report..... | 27-62 |
| Table 27.3.5-1. ILM-OEM Parts Field Descriptions | 27-65 |
| Table 27.3.6-1. ILM-Vendor-MFR Field Descriptions | 27-67 |
| Table 27.3.7-1. ILM-HwSw Codes Field Descriptions | 27-68 |

| | |
|---|--------|
| Table 27.3.8-1. ILM-Status Codes Field Descriptions | 27-69 |
| Table 27.3.9-1. ILM-Maint Contract Field Descriptions | 27-73 |
| Table 27.3.9-2. Procedures to Generate Maintenance Contract Report | 27-73 |
| Table 27.3.10-1. ILM-Sites Field Descriptions | 27-75 |
| Table 27.3.11-1. ILM-Inventory Location Field Descriptions | 27-77 |
| Table 27.4.1-1. ILM-MWO Field Descriptions..... | 27-83 |
| Table 27.4.1-2. Procedure to Add a New Work Order | 27-86 |
| Table 27.4.1-2. Procedure to Add a New Work Order | 27-86 |
| Table 27.4.1-3. Procedures to Generate ILM-MWO Predefined Reports | 27-87 |
| Table 27.4.2-1. ILM-MWO Line Item Field Descriptions | 27-93 |
| Table 27.4.2-2. Effects on Property Records by MWO Line Item Processing..... | 27-95 |
| Table 27.4.2-3. Procedure to Add Work Order Line Items | 27-99 |
| Table 27.5.1-1. ILM-License Products Field Descriptions | 27-105 |
| Table 27.5.2-1. ILM-Entitlement Field Descriptions | 27-109 |
| Table 27.5.2-2. Procedure to Add New License Entitlement | 27-110 |
| Table 27.5.2-2. Procedures to Generate ILM-License Entitlement Predefined Reports | 27-111 |
| Table 27.5.3-1. ILM-License Field Descriptions | 27-117 |
| Table 27.5.3-2. Procedure to Add New License and Allocate It to a Machine | 27-119 |
| Table 27.5.3-3. Procedures to Generate ILM-License Predefined Reports..... | 27-121 |
| Table 27.5.4-1. ILM-License Mapping Field Descriptions | 27-126 |
| Table 27.5.5-1. ILM-Additional Host Field Descriptions | 27-128 |
| Table 27.6.1-1. ILM-System Parameters Field Descriptions | 27-130 |
| Table 27.6.2-1. User Form Field Descriptions | 27-132 |
| Table 27.6.3-1. Admin Tool GUI, Workflow Object Descriptions | 27-133 |
| Table 27.6.6-1. Non System-Failure Related Error Messages | 27-134 |
| Table 28.4-1. Configuration Registry - Activity Checklist | 28-6 |

Abbreviations and Acronyms

1. Introduction

This document, Release 7.20 Mission Operation Procedures for the Earth Observing System Data and Information System (EOSDIS) Maintenance and Development (EMD) Project, provides procedures to configure, maintain and operate the EOSDIS Core System (ECS).

1.1 Identification

This document meets the milestone specified as Contract Data Requirements List (CDRL) Item 23, under contract NAS5-03098. It reflects the system as delivered at Release 7.20.

1.2 Scope

The scope of this document is directed to Distributed Active Archive Center (DAAC) operations activities to support the Release 7.20 ECS system. Both procedures and instructions are identified. Operations procedures are defined as the step-by-step commands or on-line procedures needed to perform a function. The Operations Instructions are the off-line procedures or directives for performing administrative, operations, management, or operations support activities (e.g., Configuration Management, Problem Management, or Quality Assurance).

1.2.1 On-Site Procedures Tailoring Guide

Each DAAC may modify these procedures and instructions to accommodate site-specific operations requirements. Such documentation should be versioned and dated in MS Word format with a master copy forwarded to the following address:

EMD Training
The EMD Project Office
Raytheon Company
1616 McCormick Drive
Upper Marlboro, MD 20774-5301

For specifics on authoring, formatting, importing, exporting and maintenance of procedures and instructions see Chapter 20, Library Administration.

1.3 Purpose

The purpose of this document is to identify the procedures and instructions to operate and maintain Release 7.20 systems. In addition, DAAC staff responsibilities are identified. The DAAC operations staff is comprised of operators, engineers, as well as operations support, administration and management staff personnel.

This document will also be used as a training aid for operations staff who are located at the sites. The operations procedures and operations instructions were derived from, and are intended to be

consistent with, the system functions and capabilities specified in the system design specifications.

1.4 Status and Schedule

This document is to be delivered on an annual basis. Updates are made to reflect new system releases. Changes are submitted through established configuration management procedures, such as configuration change requests or published revisions known as interim updates published to the web site at <http://edhs1.gsfc.nasa.gov/> at an “Interim Updates” link on the abstract page for this document (611-EMD-100).

1.5 Organization

The contents subsequent to this first section are presented as follows:

- Section 2 **Related Documentation.** Lists documents that drive, support or expand on the material in this manual.
- Section 3 **System Administration.** Identifies the operations procedures and/or operations instructions for system administration activities, such as backup and restore, log maintenance, user account administration, and workstation installation.
- Section 4 **Database Administration.** Identifies the operations procedures and/or operations instructions for database administration activities, such as product installation, disk storage management, login and privileges administration, database validation, backup and recovery, database configuration, tuning and performance monitoring.
- Section 5 **Security Services.** Identifies the operations procedures and/or operations instructions for security services activities, such as user authentication and authorization, data access control, network services monitoring, password protection, file modification monitoring.
- Section 6 **Network Administration.** Identifies the operations procedures and/or operations instructions for network administration activities, such as network and system configuration monitoring, and network services monitoring.
- Section 7 **System Monitoring.** Identifies the operations procedures and/or operations instructions for network system monitoring, such as problem monitoring and resolution.
- Section 8 **Problem Management.** Identifies the operations procedures and/or operations instructions for submitting, processing and resolving Troubleshooting tickets.

- Section 9 **Configuration Management.** Identifies the operations procedures and/or operations instructions for configuration management activities, such as Configuration Control Board (CCB) support, configuration item identification, submission and processing of configuration change requests (CCRs), configuration status accounting, configuration audits, data management, operational database maintenance, software transfer and installation.
- Section 10 **Metadata Administration.** Identifies the operations procedures and/or operations instructions for metadata administration activities, such as establishing collections, populating the database, and specifying Earth Science Data Type (ESDT) services.
- Section 11 **Production Rules.** This section has been retired.
- Section 12 **Resource Planning.** This section has been retired.
- Section 13 **Production Planning.** This section has been retired.
- Section 14 **Production Processing.** This section has been retired.
- Section 15 **Quality Assurance.** Identifies the operations procedures and/or operations instructions to perform DAAC manual non-science quality assurance activities, such as visualization of science data products and updating quality assurance metadata.
- Section 16 **Data Pool Ingest.** Identifies the operations procedures and/or operations instructions to support data acquisition.
- Section 17 **Archive Procedures.** Identifies the operations procedures and/or operations instructions for archiving activities, such as archive repository maintenance, fault monitoring and notification, and temporary data storage.
- Section 18 **Data Distribution.** Identifies the operations procedures and/or operations instructions to support data distribution activities, such as media operations and product shipment.
- Section 19 **User Services.** This section has been removed.
- Section 20 **Library Administration.** Identifies the operations procedures and/or operations instructions to support librarian administration activities, such as change package preparation and distribution, master document control and maintenance.
- Section 21 **COTS Hardware Maintenance.** Identifies the operations procedures and/or operations instructions for preventive and corrective maintenance activities of commercial off-the-shelf (COTS) hardware for the EMD project.

- Section 22 **Software Maintenance.** Identifies the operations procedures and/or operations instructions to support maintenance activities for COTS software, custom software, and science software.
- Section 23 **Property Management.** Identifies the operations procedures and/or operations instructions for the receipt, control, and accountability of EMD property at all affected sites.
- Section 24 **Installation Planning.** Identifies the operations procedures and/or operations instructions to support installation planning activities for conducting site surveys, ensuring that site preparations/coordination are completed on schedule, facilitating receipt and installation of the hardware.
- Section 25 **COTS Training.** Identifies the operations procedures and/or operations instructions to support COTS training activities, such as training request processing, training coordination, training scheduling, and training record maintenance.
- Section 26 **Science Software Integration and Test (SSI&T).** This section has been removed.
- Section 27 **Inventory Logistical Management (ILM).** ILM helps the operations staff at the DAACs, EOC, and SMC to maintain records that describe all inventory components and their assembly structures and interdependencies. The database maintained by this tool keeps chronological histories (a record of the transactions) of receipt, installation, and relocation of inventory items. There is a license management section and general updates to work order processes, forms, and report formats.
- Section 28 **Maintenance of Configuration Parameters.** These procedures describe the overall maintenance of the system configuration parameters baseline for custom software and hardware, including patches, database, operating systems, COTS software, and networks.
- **Abbreviations and Acronyms.** Identifies abbreviations and acronyms used throughout this document.

2. Related Documentation

2.1 Parent Documents

The parent documents are the documents from which the Mission Operation Procedures' scope and content are derived.

| | |
|-----------|---|
| 423-41-01 | Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work |
| 423-46-03 | EMD Task 201 Statement of Work for ECS SDPS Maintenance |
| 423-46-02 | Contract Data Requirements Document for EMD Task 201 ECS SDPS Maintenance |

2.2 Applicable Documents

The following documents are referenced within the Mission Operation Procedures document, or are directly applicable, or contain policies or other directive matters that are binding upon the content of this volume.

| | |
|-----------|---|
| 420-05-03 | Goddard Space Flight Center, Earth Observing System (EOS) Performance Assurance Requirements for the EOSDIS Core System (ECS) |
| 423-41-02 | Goddard Space Flight Center, Functional and Performance Requirements Specification for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS F&PRS) |
| 423-46-01 | Goddard Space Flight Center, Functional and Performance Requirements Specification for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS) Science Data Processing System (EMD F&PRS) |

2.3 Information Documents

2.3.1 Information Documents Referenced

The following documents are referenced herein and amplify or clarify the information presented in this document. These documents are not binding on the content of the Mission Operation Procedures for the EMD Project.

| | |
|-------------|---|
| 105-EMD-001 | Property Management Plan for the EMD Project |
| 110-EMD-001 | Configuration Management Plan for the EMD Project |
| 170 EMD 003 | A Data Formatting Toolkit for Extended Data Providers to NASA's Earth Observing System Data and Information System (V5.0) |

| | |
|---------------|---|
| 500-EMD-001 | Terra Spacecraft Ephemeris and Attitude Data Preprocessing |
| 500-EMD-002 | Aqua Spacecraft Ephemeris and Attitude Data Preprocessing |
| 500-EMD-003 | Aura Spacecraft Ephemeris and Attitude Data Preprocessing |
| 609-EMD-100 | Release 7.20 Operations Tools Manual for the EMD Project |
| 910-TDA-003 | COTS Software Version Baseline Report |
| 910-TDA-005 | Site-Host Map Report |
| 910-TDA-021 | SYBASE SQLServer 11.0.x ALL DAAC Database Configurations |
| 910-TDA-022 | Custom Code Configuration Parameters for ECS |
| 910-TDA-023 | Critical COTS Software List |
| 910-TDA-030 | COTS [Software] Where Used Report |
| 914-TDA-337 | Whats Up Professional 2006 Maintenance Upgrade for the EMD Project: Release Notes |
| 914-TDA-370 | AMASS to StorNext |
| 914-TDA-376 | Luminex Physical Media |
| 921-TDx-001 | DAAC LAN Topology |
| 921-TDx-002 | [DAAC] Hardware/Network Diagram |
| 921-TDx-003 | IP Address Assignment (DAAC Hosts) |
| 921-TDx-004 | IP Address Assignment (DAAC Network Hardware) |
| 921-TDx-005 | Dual-Homed Host Static Routes |
| CM-004 | EMD Project Instruction: CCB Change Control Process |
| CM-1-032-1 | EMD Project Instruction: COTS and Custom Software Preparation and Delivery |
| CM-045 | EMD Project Instruction: EMD Software Build Process |
| DM-002 | EMD Project Instruction: Data Identification Numbering |
| MIL-HDBK-263B | Electrostatic Discharge Control Handbook for Protection of Electrical and Electronic Parts, Assemblies, and Equipment (Excluding Electrically Initiated Explosive Devices) (Metric) |
| MIL-STD-1686C | Department of Defense Standard Practice: Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices) |

2.3.2 Information Documents Not Referenced

The following documents, although not referenced herein and/or not directly applicable, do amplify or clarify the information presented in this document. These documents are not binding on the content of the Mission Operation Procedures for the EMD Project.

| | |
|-------------|---|
| 290-004 | Goddard Space Flight Center, Internet Protocol Operational Network (IONet) Access Protection Policy and Requirements |
| 423-10-21 | Earth Science Data and Information System Project Configuration Management Procedures |
| 423-16-01 | Data Production Software and Science Computing Facility (SCF) Standards and Guidelines |
| 305-EMD-100 | Release 7.20 Segment/Design Specification for the EMD Project |
| 311-EMD-100 | Release 7.20 INGEST (INS) Database Design and Schema Specifications for the EMD Project |
| 311-EMD-101 | Release 7.20 Science Data Server Database Design and Schema Specifications for the EMD Project |
| 311-EMD-102 | Release 7.20 Storage Management and Data Distribution Subsystems Database Design and Database Schema Specifications for the EMD Project |
| 311-EMD-103 | Release 7.20 Systems Management Subsystem Database Design and Schema Specifications for the EMD Project |
| 311-EMD-104 | Release 7.20 Order Manager Database Design and Database Schema Specifications for the EMD Project |
| 311-EMD-105 | Release 7.20 Spatial Subscription Server (SSS) Database Design and Schema Specifications for the EMD Project |
| 311-EMD-106 | Release 7.20 Data Pool Database Design and Schema Specifications for the EMD Project |
| 508-EMD-001 | ACRONYMS for the EOSDIS Maintenance and Development (EMD) Project |
| 905-TDA-001 | EMD System Baseline Specification |
| 914-TDA-331 | Solaris_8_OS_patches_0905 |
| 920-TDx-001 | Hardware-Design Diagram |
| 920-TDx-002 | Hardware-Software Map |
| 905-TDA-002 | ECS Host Naming Convention |
| 920-TDx-009 | DAAC HW Database Mapping |
| 920-TDx-019 | Hosts' Custom Code Baseline |

| | |
|--------------------|--|
| 152-TP-003 | Glossary of Terms for the EOSDIS Core System (ECS) Project |
| FB9401V2 | EOSDIS Core System Science Information Architecture |
| NPR 1600.1 | NASA Procedural Requirements: NASA Security Program Procedural Requirements |
| NPR 2810.1 | NASA Procedural Requirements: Security of Information Technology |
| OMB Circular A-130 | Office of Management and Budget, Management of Federal Information Resources |

3. System Administration

3.1 Overview

Secure Shell (ssh) is an application that greatly improves network security. Secure Shell is the standard for remote logins, solving the problem of hackers stealing passwords. Secure Shell secures connections by encrypting passwords and other data. Once launched, it provides transparent, strong authentication and secure communications over any IP-based connection. The SSH Secure Shell application is virtually invisible during day-to-day use. It provides a provides an extensive library of features for securing and authenticating terminal connections, file transfers or almost any other type of connection might be created over an IP network. Secure Shell is to be used for communication among system platforms and among the DAACs.

3.2 Secure Access to DAACs

The Local Area Network (LAN) that has been implemented at the DAACs is more secure than most other LANs. From the Internet, it is not possible to directly connect with all hosts at a DAAC. There is a set of hosts that are dual-homed to a user LAN that is connected on one side to the Internet and to the DAAC production LAN on the other side. This will require an interactive user to first use SSH to access a dual homed host and then use ssh to access a production host. In order to minimize the impact on the user, a single login has been implemented.

3.3 Setting Up SSH

SSH programs have client and server components much like other network programs. The user only needs to be concerned with the client configuration as the server side is set up by a systems administrator. The amount of effort that it takes to get SSH going depends on how many different home directories the user has. At Landover, for instance, there are separate directories for the EDF and the VATC.

Most users will start from the same host whether from an X terminal, a UNIX workstation or a PC. Prior to executing **ssh** commands, use **setenv DISPLAY <IP address>:0.0** at your local host. To ensure system security, do not use the **setenv DISPLAY** command on subsequent hosts accessed via **ssh**. The process is started by running the **SSH setup (sss)** script, which will enable **ssh** to other hosts from which one may use the same home directory. The only thing you need to do before executing the script is to pick a good passphrase of at least 10 characters. You can, and should, use spaces and multiple words with numbers and misspellings and special characters. Note that passwords are NOT echoed back to the screen.

Table 3.3-1 contains the activity checklist for setting up SSH.

Table 3.3-1. SSH - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|------------------------------|-----------|-----------|
| 1 | SA | Initializing SSHSETUP | (P) 3.3.1 | |
| 2 | SA | Setting Up Remote Access SSH | (P) 3.4.1 | |
| 3 | SA | Changing Your Passphrase | (P) 3.5.1 | |

3.3.1 Initiating SSHSETUP

- 1 Log in into your normal UNIX workstation where your home directory resides.
 - 2 Initiate Secure Shell setup by typing **sss** then press the **Return/Enter** key.
 - You will see an information statement:
Use a passphrase of at least 10 characters which should include numbers or special characters and MAY include spaces
 - 3 At the **New passphrase:** prompt type *passphrase* then press the **Return/Enter** key.
 - 4 At the **Retype new passphrase:** prompt type *passphrase* then press the **Return/Enter** key.
 - You will then see:
Initializing random number generator...
Generating p: Please wait while the program completes ...
%
 - This establishes the .ssh sub-directory in your <username>/home directory, creates the local ssh key, and creates the necessary files.
-

3.4 Remote SSH Access

If you need to access a host with a different home directory, you will need to run the **sshremote** script. This script sets up the destination host with the new set of keys and transfers the source (local) key to the destination and the destination key to the source. You must have an existing account on the remote host.

3.4.1 Setting Up Remote Access SSH

- 1 Log in into your normal Unix workstation where your home directory resides.

2 Initiate Secure Shell remote setup by typing **ssr** then press the **Return/Enter** key.

- You will see the following prompt: Remote user name: (Default: <name>):

NOTE: User must first have an account on the remote system.

You have a local passphrase. Do you want to setup for:

- 1 VATC
 - 2 EDF
 - 3 GSFC DAAC
 - 4 SMC
 - 5 GSFC M and O
 - 6 LP DAAC
 - 7 LP M and O
 - 8 LaRC DAAC
 - 9 LaRC M and O
 - 10 NSIDC DAAC
 - 11 NSIDC M and O
 - x Exit from script
- Select:**

3 At the **Select:** prompt, type in the corresponding number to the desired host then press the **Return/Enter** key.

- You will receive a message similar to the following:

Enter the password for the remote system: <password>

4 At the prompt **Enter existing passphrase for remote system:** type *<passphrase>* then press the **Return/Enter** key.

- A prompt similar to the following will be displayed:

Working...

NOTE: The ssh keys at remote sites can be different from the local host ssh key.

3.5 Changing Your Passphrase

Another script has been developed to change your passphrase on the local host and then transfer the key to the other environments. The **ssh** keys for remote hosts will have to be changed separately. Use the following procedure to change your passphrase:

3.5.1 Changing Your Passphrase

1 Log in to your normal Unix workstation where your home directory resides.

- Initiate passphrase change by typing **ssp** then press the **Return/Enter** key.

- You will see an information statement:

Use a passphrase of at least 10 characters which should include numbers or special characters and MAY include spaces

- At the **Old passphrase:** prompt type *old_passphrase* then press the **Return/Enter** key.
- At the **New passphrase:** prompt type *new_passphrase* then press the **Return/Enter** key.
- At the **Retype new passphrase:** prompt type *new_passphrase* then press the **Return/Enter** key.

- You will then see an information prompt similar to the following:

ssh-keygen will now be executed. Please wait for the prompt to Return!
/home/userid/.ssh/authorized_keys permissions have already been set.
%

3.6 Logging in to System Hosts

Logging in to system hosts is accomplished from a UNIX command line prompt. It is an initial set of steps that is performed when accomplishing many other tasks.

Logging in to system hosts starts with the assumption that the applicable hosts are operational and the operator has logged in to a workstation or X-term that has access to the applicable network in the system.

Table 3.6-1 contains the activity checklist for Login to System Hosts.

Table 3.6-1. Login to System Hosts - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|------------------------|-----------|-----------|
| 1 | SA | Log in to System Hosts | (P) 3.6.1 | |

3.6.1 Log in to System Hosts

NOTE: Commands in Steps 1 and 2 are typed at a UNIX system prompt.

- In the terminal window (at the command line prompt) start the log-in to the appropriate host by typing **ssh <hostname>** then press the **Return/Enter** key.
 - The **-l** option can be used with the ssh command to allow logging in to the remote host (or the local host for that matter) with a different user ID. For example, to log in to x0ins01 as user cmops enter:

/ssh -l cmops x0dpl01

- Depending on the set-up it may or may not be necessary to include the path (i.e., /usr/local/bin/) with the ssh command. Using ssh alone is often adequate. For example:

```
ssh x0dpl01
```

- or -

```
ssh -l cmops x0dpl01
```

- Examples of Sun Consolidation External Server host names include **e0dpl01**, **g0dpl01**, **l0dpl01**, and **n0dpl02**.
 - Examples of Sun Consolidation Internal Server host names include **e0oml11**, **g0oml11**, **l0oml03**, and **n0oml04**.
 - If you receive the message, “**Host key not found from the list of known hosts. Are you sure you want to continue connecting (yes/no)?**” enter **yes** (“y” alone will not work).
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Passphrase for key '<user@localhost>'** appears; continue with Step 3.
 - If you have not previously set up a secure shell passphrase, go to Step 4.
- 2** If a prompt to **Passphrase for key '<user@localhost>'** appears, type your **<passphrase>** then press the **Return/Enter** key.
- If a command line prompt is displayed, log-in is complete.
 - If the passphrase is unknown, press the **Return/Enter** key, which should cause a **<user@remotehost>'s password:** prompt to appear (after the second or third try if not after the first one), then go to Step 4.
 - If the passphrase is entered improperly, a **<user@remotehost>'s password:** prompt should appear (after the second or third try if not after the first one); go to Step 4.
- 3** If a prompt for **<user@remotehost>'s password:** appears, type your **password** then press the **Return/Enter** key.
- A command line prompt is displayed.
 - Log-in is complete.
-

3.7 System Startup and Shutdown

Starting or shutting down a computer system may involve nothing more than turning a power switch to the on or off position. However, the interdependency of the various servers may require the System Administrator to startup or shutdown the servers in a particular order. Depending on the situation, the entire computer system may be started or stopped (cold) or only

selected servers may be started or stopped (warm). The next sections cover the procedures and details of cold and warm startups and shutdowns.

A complete system startup and shutdown should only need to occur approximately once in three or four months during the early stages of system implementation due to the inherent instability of new systems. After the system stabilizes, it is estimated that complete system startups and shutdowns will occur only about once a year. Partial shutdowns and restarts will be performed as needed due to maintenance concerns.

Table 3.7-1 contains the activity checklist for System Startup and Shutdown.

Table 3.7-1. System Startup and Shutdown - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|--|-------------|-----------|
| 1 | SA | Performing Cold Subsystem Startup | (P) 3.7.1.1 | |
| 2 | SA | Performing Warm Subsystem Startup | (P) 3.7.2.1 | |
| 3 | SA | Updating leapsec.dat and utcpole.dat Files | (P) 3.7.3.1 | |
| 4 | SA | Performing Normal Shutdown by Subsystem | (P) 3.7.4.1 | |
| 5 | SA | Performing Emergency Shutdown | (P) 3.7.5.1 | |

3.7.1 Cold Startup By Subsystem

A cold startup is indicated when there are no subsystems currently running, e.g., when the system is to be turned on for the first time, following a system maintenance operation that requires all power to be turned off, or following a power failure. In most situations a cold startup is also indicated by the power switch being in the OFF position.

3.7.1.1 Performing Cold Subsystem Startup

- 1 Determine which machines perform the following functions (some machines may perform multiple functions).
 - Domain Name Server (DNS) Master
 - Name Information Server (NIS) Master
 - Mail Hub Server(s)
 - Automount Servers
 - ClearCase Server
 - Communication Subsystem (CSS)
 - Other License Servers

- Sybase ASE Servers
 - Client Subsystem (CLS)
- 2 Startup the DNS Master, the NIS Master, and the CSS server.
 - Once that system has booted without error, proceed to Step 3.
 - 3 Power on the ClearCase server(s).
 - Once the systems(s) have booted without error, proceed to Step 4.
 - 4 Power on the Interface server(s).
 - Once the system(s) have booted without error, proceed to Step 5.
 - 5 Power on the MSS server(s).
 - Once the system(s) have booted without error, proceed to Step 6.
 - 6 Power on the DPL_Ingest server(s).
 - Once the system(s) have booted without error, proceed to Step 7
 - 7 Power on the Client and Data Management server(s).
-

3.7.2 Warm Startup

A warm startup is indicated when there are some subsystems currently running while others have been shutdown either due to operator intervention or an external malfunction. The subsystems not actively running need to be started without interfering with the current active operations. In some instances, a warm startup may require some active subsystems to be shutdown and restarted so that their interaction and connectivity will be properly resumed.

3.7.2.1 Performing Warm Subsystem Startup

- 1 Determine which machines perform the following functions:
 - Domain Name Server (DNS) Master
 - Name Information Server (NIS) Master
 - Mail Hub Server(s)
 - Automount Servers
 - ClearCase Server
 - Communication Subsystem (CSS)
 - Other License Servers

- System Management Subsystem
 - Sybase ASE Servers
 - Client Subsystem (CLS)
- 2 Determine which machine is currently down.
 - 3 Determine the interoperability dependencies among the machines.
 - 4 Turn on machines in an order consistent with the dependencies.
-

3.7.3 Updating leapsec.dat and utcpole.dat Files

In order to ensure proper operation of Product Generation Executives (PGEs), two files must be updated weekly with data transferred from the U.S. Naval Observatory. These files are **`${PGSHOME}/database/common/TD/leapsec.dat`** and **`${PGSHOME}/database/common/CSC/utcpole.dat`**. The updating of these files is accomplished by executing **`leapsec_update.sh`** and **`utcpole_update.sh`** in the **`/usr/ecs/OPS/CUSTOM/TOOLKIT/toolkit/bin/sgi64_daac_f77`** directory on each Science Processor with root privileges. If the tasks have not been set up to be accomplished via cron job, they must be done manually.

3.7.3.1 Updating leapsec.dat and utcpole.dat Files

NOTE: The user account performing the update must have write permission in the Toolkit directories.

- 1 Log in to one of the xx4spl01 machines.
 - 2 Type **`cd /usr/ecs/MODE/CUSTOM/TOOLKIT/toolkit/bin/sgi64_daac_f77`** then press the **Return/Enter** key.
 - 3 Type **`source pgs-env.csh`** then press the **Return/Enter** key.
 - 4 Type either **`update_leapsec.sh`** (to update the leap seconds file) or **`update_utcpole.sh`** (to update the leap seconds file) as appropriate then press the **Return/Enter** key.
 - 5 Type responses to program prompts as appropriate.
 - 6 Repeat Steps 4 and 5 to update the other file.
 - 7 Repeat Steps 1 through 6 for each additional Science Processor host (if any).
-

3.7.4 Normal Shutdown

A normal shutdown occurs when the operator is required to turn off the power to the entire system or any of the component subsystems. The Resource Manager schedules normal shutdowns (with prior approval of DAAC management) at a time that minimizes disruption to system users, e.g., during off-hours. No loss of data is anticipated from a normal shutdown. All subsystems are shut down in a routine fashion.

The system shutdown procedure is performed by the System Administrator at the discretion of the Network Administrator, usually for the purpose of repair. The system shutdown is normally performed in reverse order of the system startup as previously described. Prior to a normal shutdown, the System Administrator sends broadcast messages to all Computer Operators on the system at Shutdown Minus 30 minutes, Shutdown Minus 15 minutes, and Shutdown Minus one minute. At the scheduled shutdown time, the System Administrator blocks all incoming requests from the gateway and allows active jobs to complete (unless it is anticipated that they will take longer than 10 minutes, in which case the System Administrator will terminate the processes and notify the originator). The System Administrator then begins to shut down all subsystems in the order prescribed in the procedure below.

When all subsystems have been successfully shutdown, the UNIX prompt appears on the console screen. Total time from shutdown initiation to completion may be as long as 45 minutes.

3.7.4.1 Performing Normal Shutdown by Subsystem

Steps 1 through 7 below are preliminary steps to shutting down each subsystem and are repeated (as necessary) for each subsystem.

- 1 Log in to the server as **root**.
- 2 Type **root_password** then press the **Return/Enter** key.
- 3 Type **wall** then press the **Return/Enter** key.
- 4 Type This machine is being shutdown for *reason*. Please save your work and log off now. We are sorry for the inconvenience. then press the **Ctrl** and **D** keys simultaneously.
- 5 Wait at least five minutes.
- 6 At the UNIX prompt type **shutdown -g0 -i0** or **shutdown now -i0** then press the **Return/Enter** key.
- 7 Power off all peripherals and the CPU.
- 8 Determine which machines perform the following functions:
 - DNS Master
 - NIS Master
 - Mail Hub Server(s)

- Automount Server
 - ClearCase Server
 - CSS
 - CLS
 - Other License Servers
 - MSS including Sybase ASE Servers
 - Ingest
- 9 Power off the CLS server by following Steps 1 through 7 above for the machine.
 - Once the system(s) have shutdown without error, proceed to Step 10.
 - 10 .1 Power off the Ingest server(s) by following Steps 1 through 7 above for each machine.
 - Once the system(s) have shutdown without error, proceed to Step 11
 - 11 Power off the DSS server(s) by following Steps 1 through 7 above for each machine.
 - Once the system(s) have shutdown without error, proceed to Step 12.
 - 12 Power off the MSS server(s) by following Steps 1 through 7 above for each machine.
 - Once the system(s) have shutdown without error, proceed to Step 13.
 - 13 Power off the Interface server(s) by following Steps 1 through 7 above for each machine.
 - Once the system(s) have shutdown without error, proceed to Step 14.
 - 14 Power off the ClearCase server(s) by following Steps 1 through 7 above for each machine.
 - Once the system(s) have shutdown without error, proceed to Step 15.
 - 15 Power off the CSS server, the NIS Master and the DNS Master by following Steps 1 through 7 above for each machine
-

3.7.5 Emergency Shutdown

An emergency shutdown is indicated when the System Administrator determines that the entire system or a component subsystem requires immediate maintenance. Indications that an emergency shutdown is in order include:

- The system or subsystem is locked up and users are unable to access or maneuver through the system
- An impending or actual power failure

- An actual system or subsystem hardware or software failure

Every effort should be made to minimize loss of data during an emergency shutdown by informing users to save files and log off if at all possible. However, circumstances may be such that a large-scale loss of data is unavoidable. In such instances, data will be restored from the most recent backup tapes and temporary backup files provided by the system (if applicable).

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 on line.

If major subsystems are locked up, 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 on line.

If one or only a few of the subsystems are experiencing problems and only some of the users are affected, the subsystem problem(s) should be resolved first. If the System Administrator determines that all efforts to resolve the subsystem problems are exhausted and a shutdown is necessary, only the affected subsystems should be shutdown. Only if these steps provide no relief should the entire system be brought down. In any case, every effort should be made to accommodate users that are still on the system and to minimize data loss.

3.7.5.1 Performing Emergency Shutdown

- 1 Log in to the server as root.
- 2 Type **root_password** at the UNIX prompt then press the **Return/Enter** key.
- 3 Type **sync** at the UNIX prompt then press the **Return/Enter** key.
 - The **sync** command causes all information in memory that should be on disk to be written out including modified super blocks, modified inodes, and delayed block I/O. If the system is to be stopped, **sync** must be called to insure file system integrity.
- 4 Type **sync** (again) at the UNIX prompt then press the **Return/Enter** key.
- 5 Type **halt** at the UNIX prompt then press the **Return/Enter** key.
- 6 Shutdown all client workstations.
- 7 Determine which machines perform the following functions (some machines may perform multiple functions).
 - Sybase ASE/Rep
 - AutoSys
 - ClearCase
 - Automount
 - Mail Hub

- NIS
 - DNS
- 8 Power off the Sybase ASE/Rep server(s).
 - Once the system has shutdown without error, proceed to Step 9.
 - 9 Power off the AutoSys server(s).
 - Once the system has shutdown without error, proceed to Step 10.
 - 10 Power off the ClearCase server(s).
 - Once the system has shutdown without error, proceed to Step 11.
 - 11 Power off the Automount server(s).
 - Once the system has shutdown without error, proceed to Step 12.
 - 12 Power off the NIS server(s).
 - Once the system has shutdown without error, proceed to Step 13.
 - 13 Power off the DNS server(s).
-

3.7.6 System Shutdown by Server

In situations where only a single server requires maintenance, the System Administrator will need to determine if and how the faulty server affects other servers on the network. One server may be able to be shutdown without affecting the rest of the network, or several dependent servers may have to be shutdown in addition to the target server. Because of these interdependencies, each case will have to be uniquely evaluated.

3.8 Checking the Health and Status of the System

The system is heavily dependent on the use of computer networks. Graphical tools available to monitor system status include a COTS program, **WhatsUp Professional 2006 Premium Edition (WhatsUp Professional)**; three custom software programs, **ECS Assistant/ECS Monitor**, **EcMs-Whazzup??**, and the **ECS Health Check GUI**; and a script, **EcCsIdPingServers**, that permits an operator to ping all servers. These programs provide system monitors with real-time status of the system and indications of potential problem areas.

3.9 WhatsUp Professional 2006 (Premium Edition) - Removed

3.10 Whazzup???

A powerful COTS program that has been modified for monitoring the system is EcMsWz - Whazzup. It is a web-accessed program that provides a graphical display of Host Status, Mode

Status, Mode Verification and Performance Management. Figure 7 shows the initial Whazzup display.

These functions of Whazzup provide graphical displays of host and software-server status in real-time mode. When used in conjunction with ECS Assistant, System Administrators can acquire a comprehensive knowledge of the system's status.

Table 3.10-1 contains the activity checklist for Whazzup.

Table 3.10-1. Whazzup - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|-------------------------|------------|-----------|
| 1 | SA | Starting EcMsWz-Whazzup | (P) 3.10.1 | |

To start EcMsWz-Whazzup, execute the following procedure:

3.10.1 Starting EcMsWz-Whazzup

- 1 Log in to a host machine.
- 2 At the UNIX prompt on the host from which Whazzup is to be run, type **setenv DISPLAY <hostname>:0.0** press the **Return/Enter** key.
 - **Note:** If the host has been remotely accessed via ssh then do not use the **setenv DISPLAY** command again. Doing so will compromise system security.
 - **hostname** is the name of the machine on which Whazzup is to be displayed, i.e., the machine you are using.
 - To verify the setting, type **echo \$DISPLAY** then press the **Return/Enter** key.
- 3 At the UNIX prompt, using secure shell, log on to the Whazzup host, xxdpl0x. Type **ssh xxdpl0x** then press the **Return/Enter** key.
- 4 Type **Passphrase** then press the **Return/Enter** key.
 - You are logged into the Whazzup host machine.
- 5 To start the Netscape web browser type **netscape &** then press the **Return/Enter** key.
 - You are in the web browser on the Whazzup host xxins0x.
- 6 In the **Location** field of the Netscape browser type the URL for Whazzup (e.g., **http://xxdpl0x:5150**) then press the **Return/Enter** key.
 - The Whazzup intro screen appears (Figure 3.10-1).

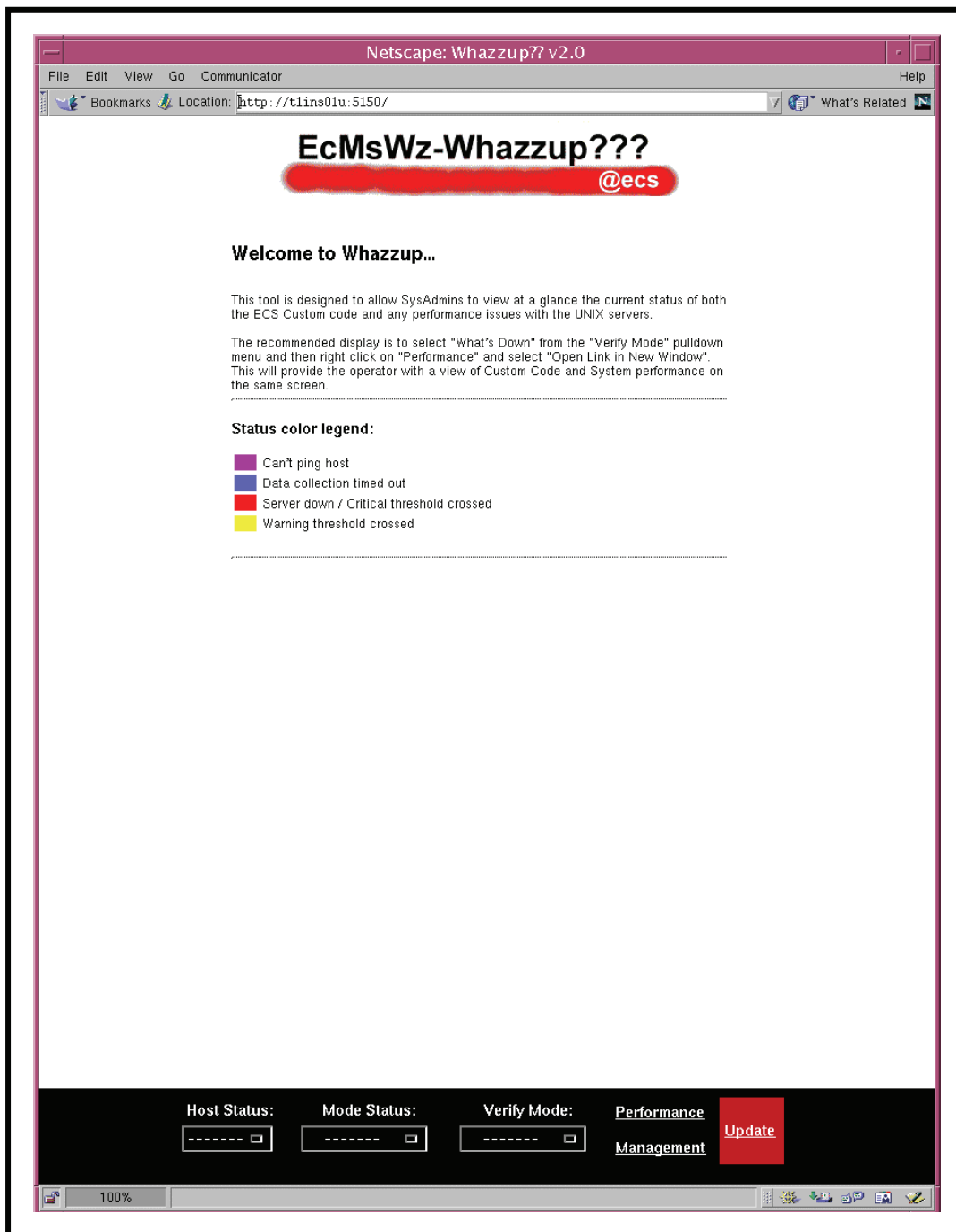


Figure 3.10-1. ECS Whazzup Initial Display

- 7 Select a monitoring function:
- **Host Status** to determine individual host parameters.
 - **Mode Status** to determine “up” servers for the selected Mode.
 - **Verify Mode** to determine status of all servers for a selected Mode.
 - **Performance Management** to determine the performance status of all hardware/software servers for all modes.
-

3.10.2 Host Status

Selecting Host Status provides a pop-up box (Figure 3.10-2) from which to choose a specific host to determine its status.

Host Status data include percent of CPU used, Swap Free space, Memory Free space, and Server information (Figure 3.10-3).

Selecting Mode Status (Figure 3.10-4) enables a pop-up window showing Modes available. Subsequent to selecting the desired Mode, a display of “up” system servers is provided as shown in Figure 3.10-5.

3.10.3 Verify Mode

Selecting **Verify Mode** and choosing a desired mode (Figure 3.10-6) will provide a thorough display of system server status, by host, for the mode (Figure 3.10-7). Alternatively, selecting **What’s Down** will provide a display indicating all down system servers, by mode, by host.

3.10.4 Performance Management

Following recommended monitoring procedures, the optimum method of system monitoring is to select **What’s Down** from **Verify Mode** and then **Right Click** on **Performance Management** (Figure 3.10-8) and open the link in a new window (Figure 3.10-9).

Having these two displays active simultaneously will provide the Systems Administrator the status of “down” system servers and the performance status of individual hosts.

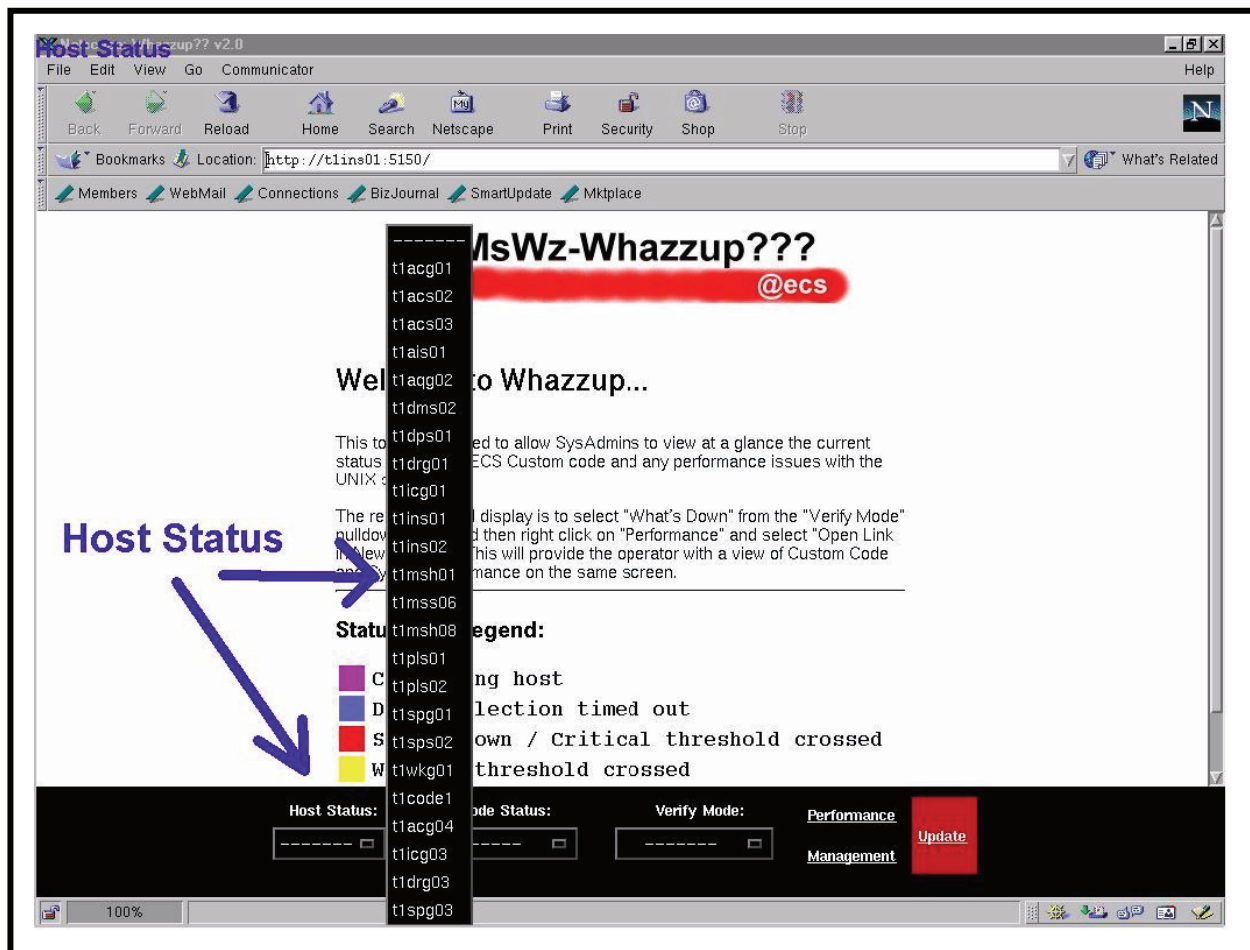


Figure 3.10-2. Host Status Pop-Up Display

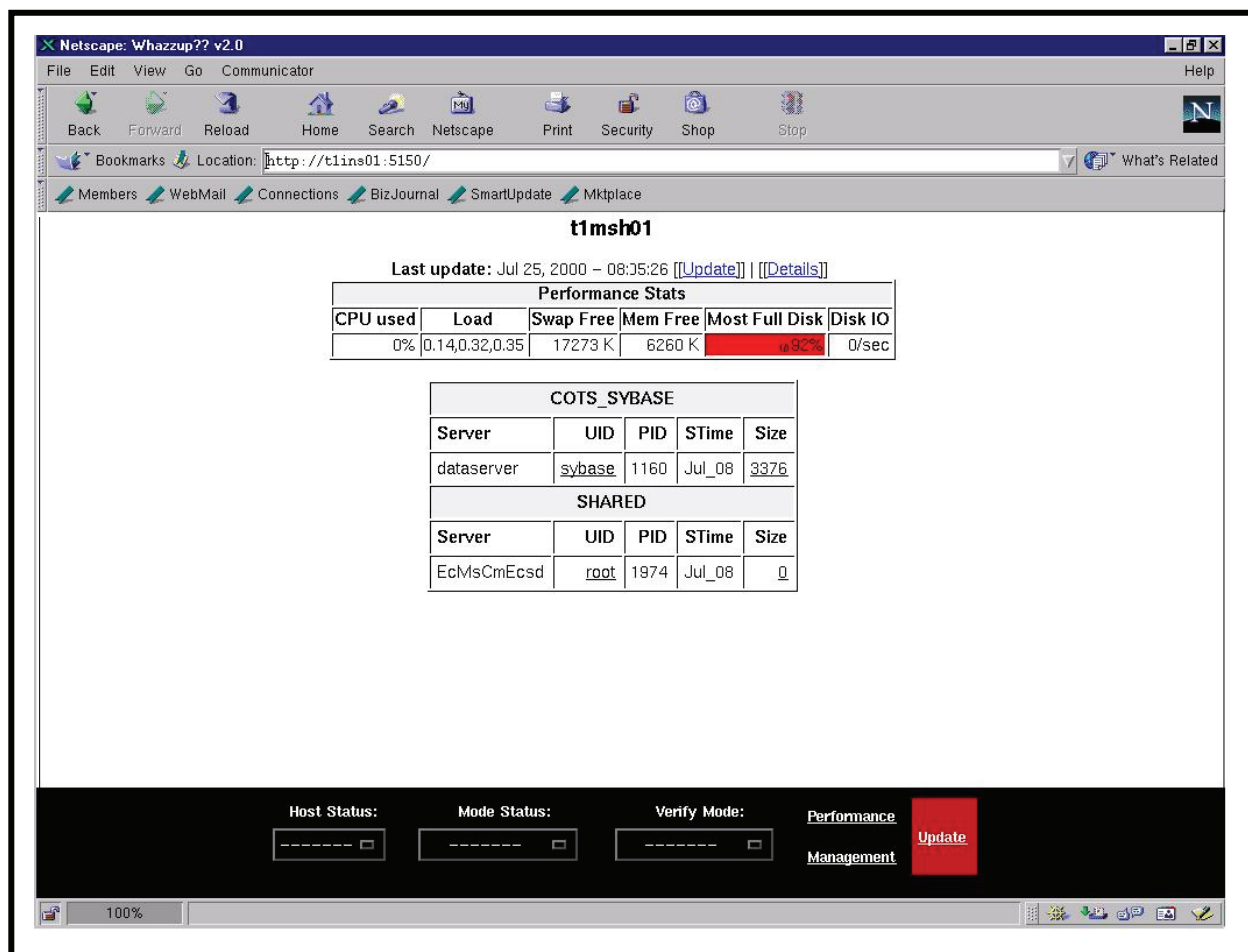


Figure 3.10-3. Host Status Data Display

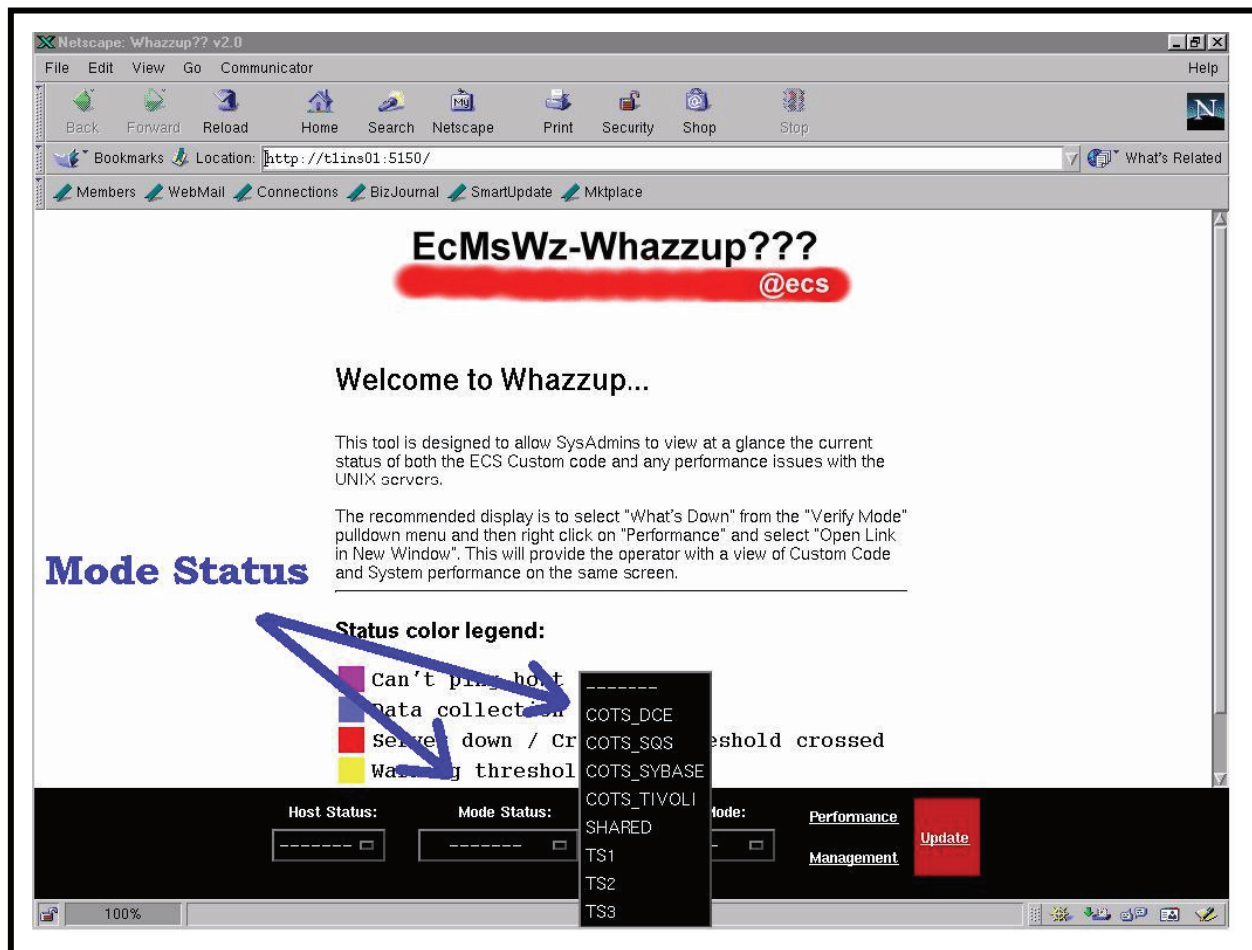


Figure 3.10-4. Mode Status Pop-Up Display

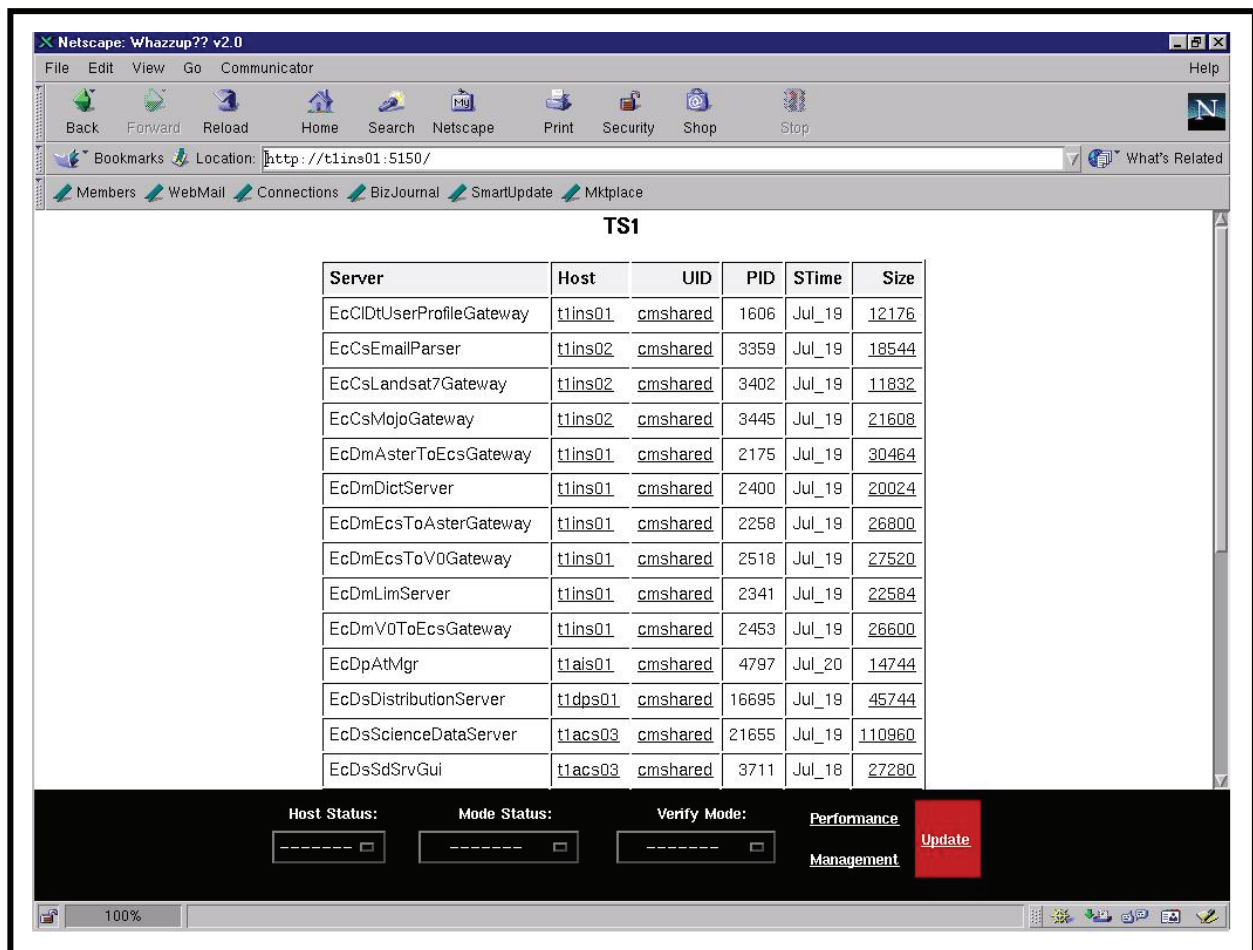


Figure 3.10-5. Mode Status Data Display

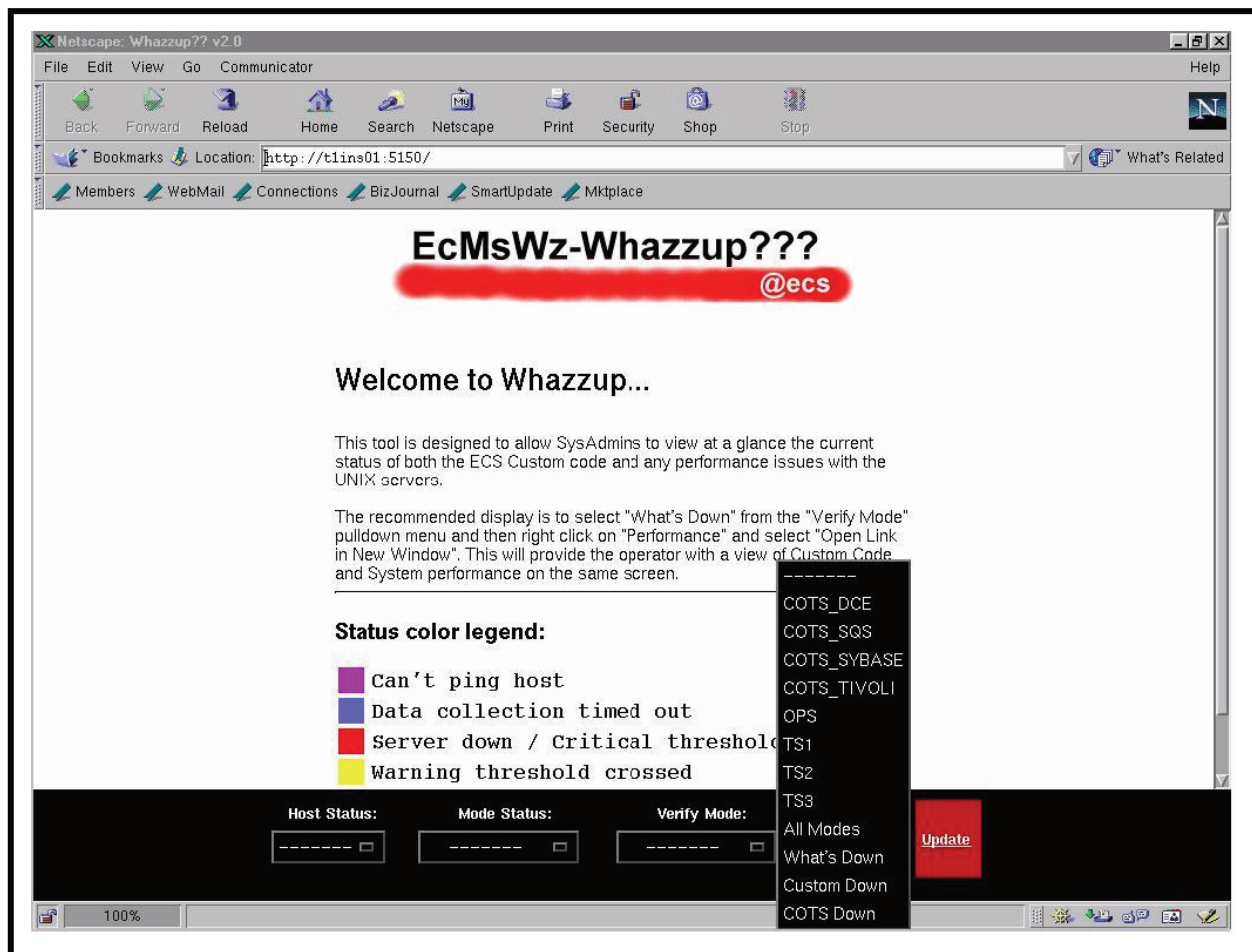


Figure 3.10-6. Verify Mode Pop-Up Display

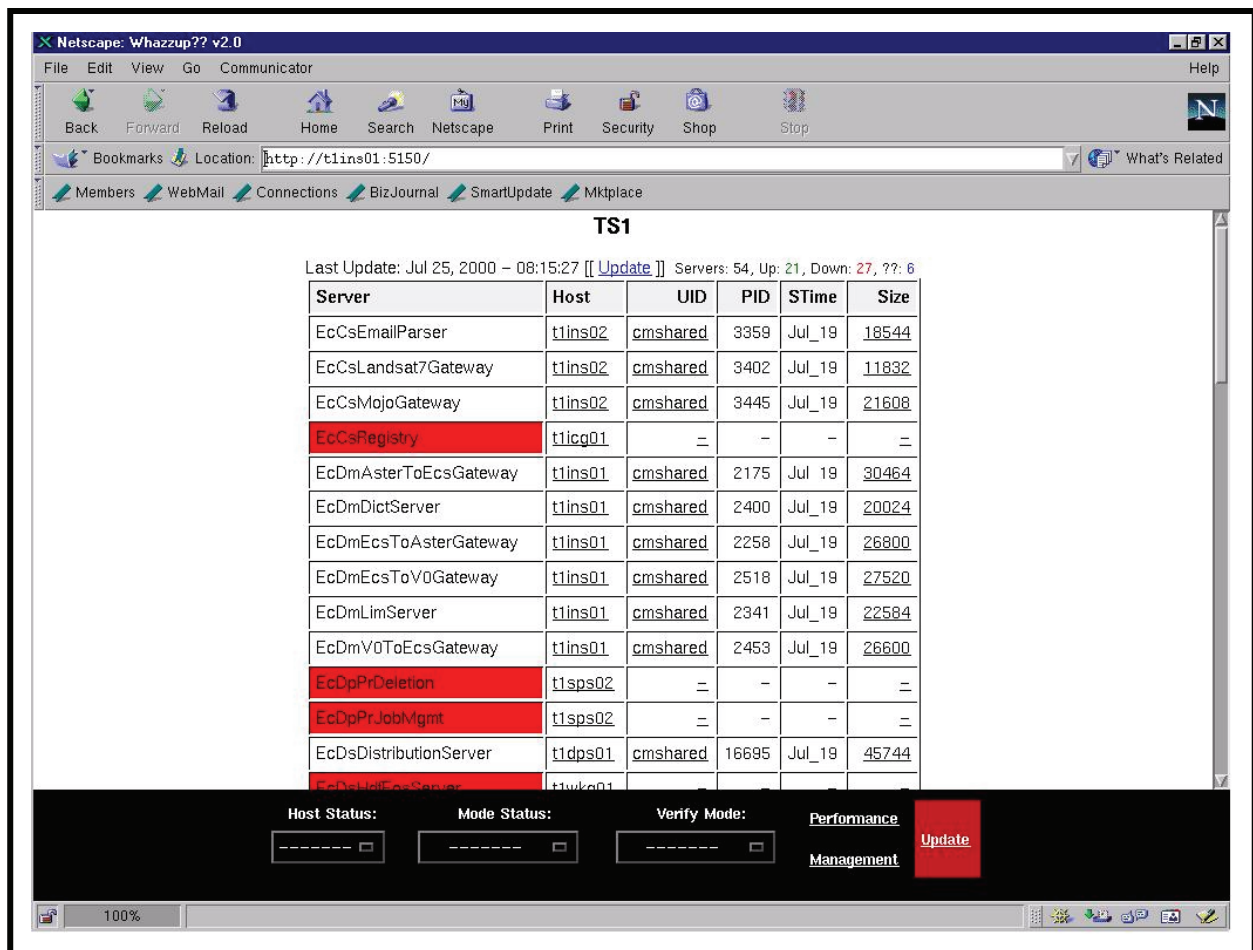


Figure 3.10-7. Verify Mode Data Display

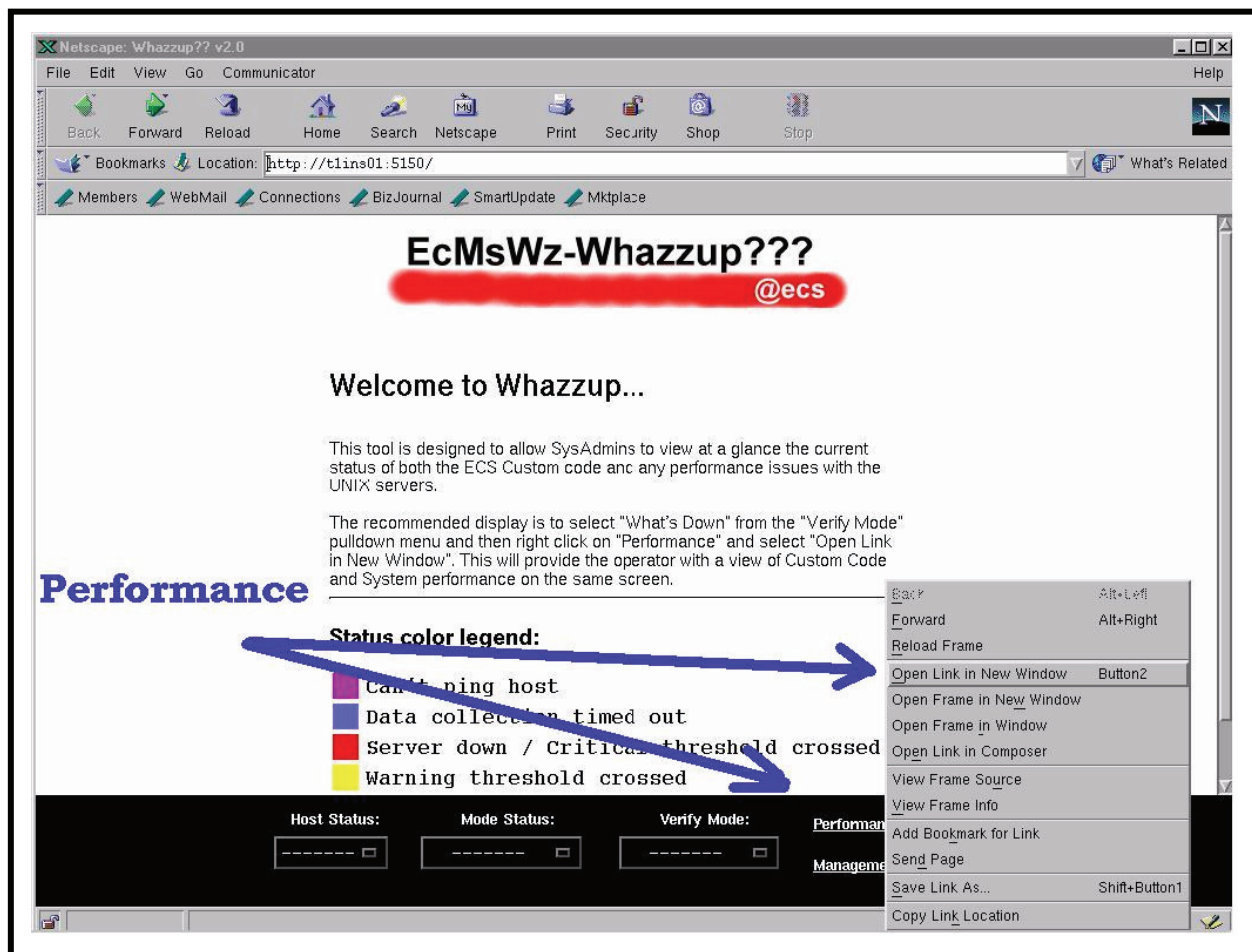


Figure 3.10-8. Performance Management Selection Display

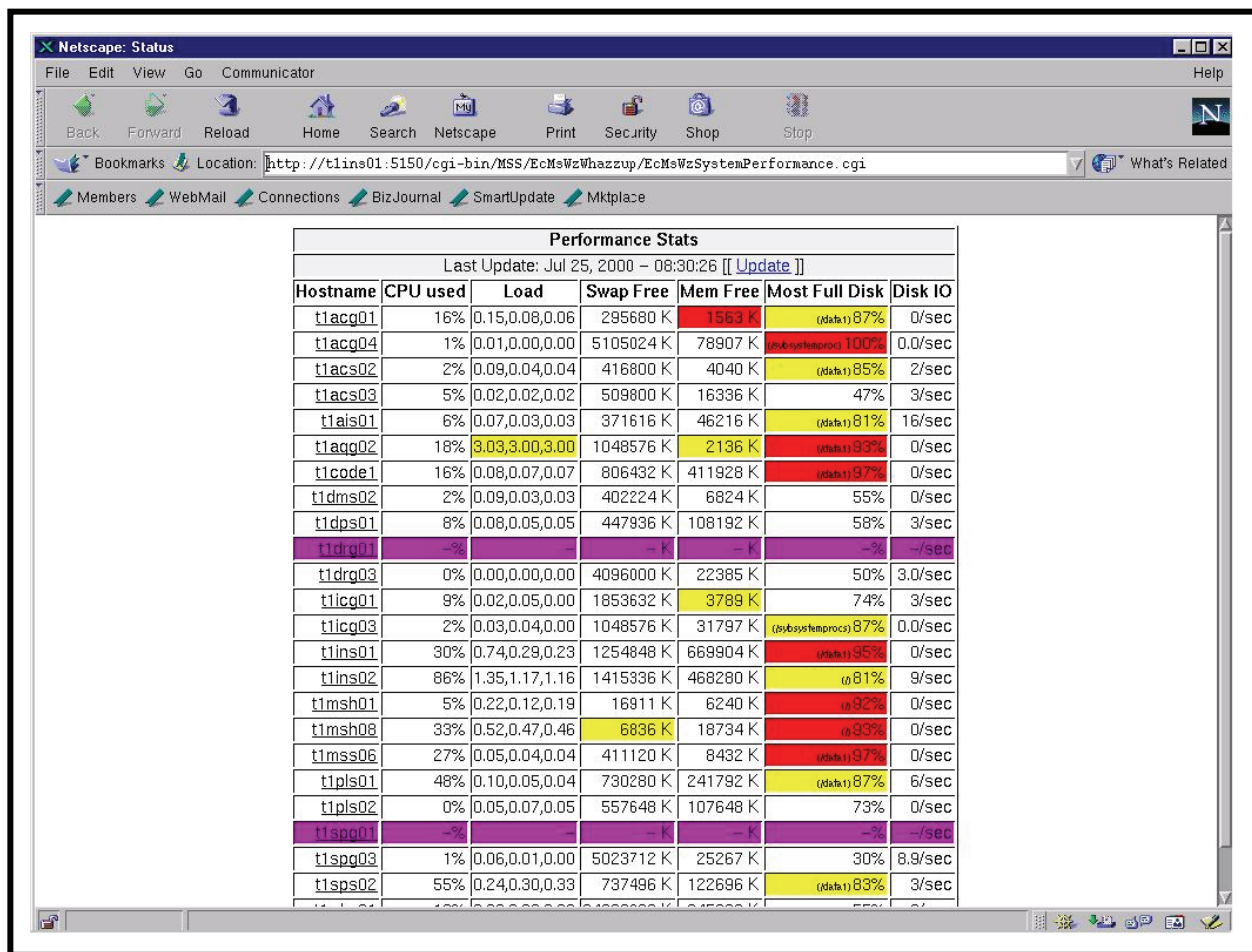


Figure 3.10-9. Performance Management Data Display

3.11 ECS Health Check GUI

The ECS Health Check GUI (Figures 3.11-1 and 3.11-2) indicates the status of the EcDmV0ToEcsGateway and Data Pool drill-down search engine. At a specified rate it sends inventory searches to the EcDmV0ToEcsGateway and/or submits granule search requests to the Data Pool. It provides warnings by the following means when a failure is registered by the GUI during the current search:

- Visual warning (including details about the time and nature of the error).
- Audible alarm (when implemented).
- E-mail message.

Table 3.11-1 contains the activity checklist for ECS Health Check.

Table 3.11-1. ECS Health Check - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|--|--------------|-----------|
| 1 | SA | Start and Use the ECS Health Check GUI | (P) 3.11.1.1 | |

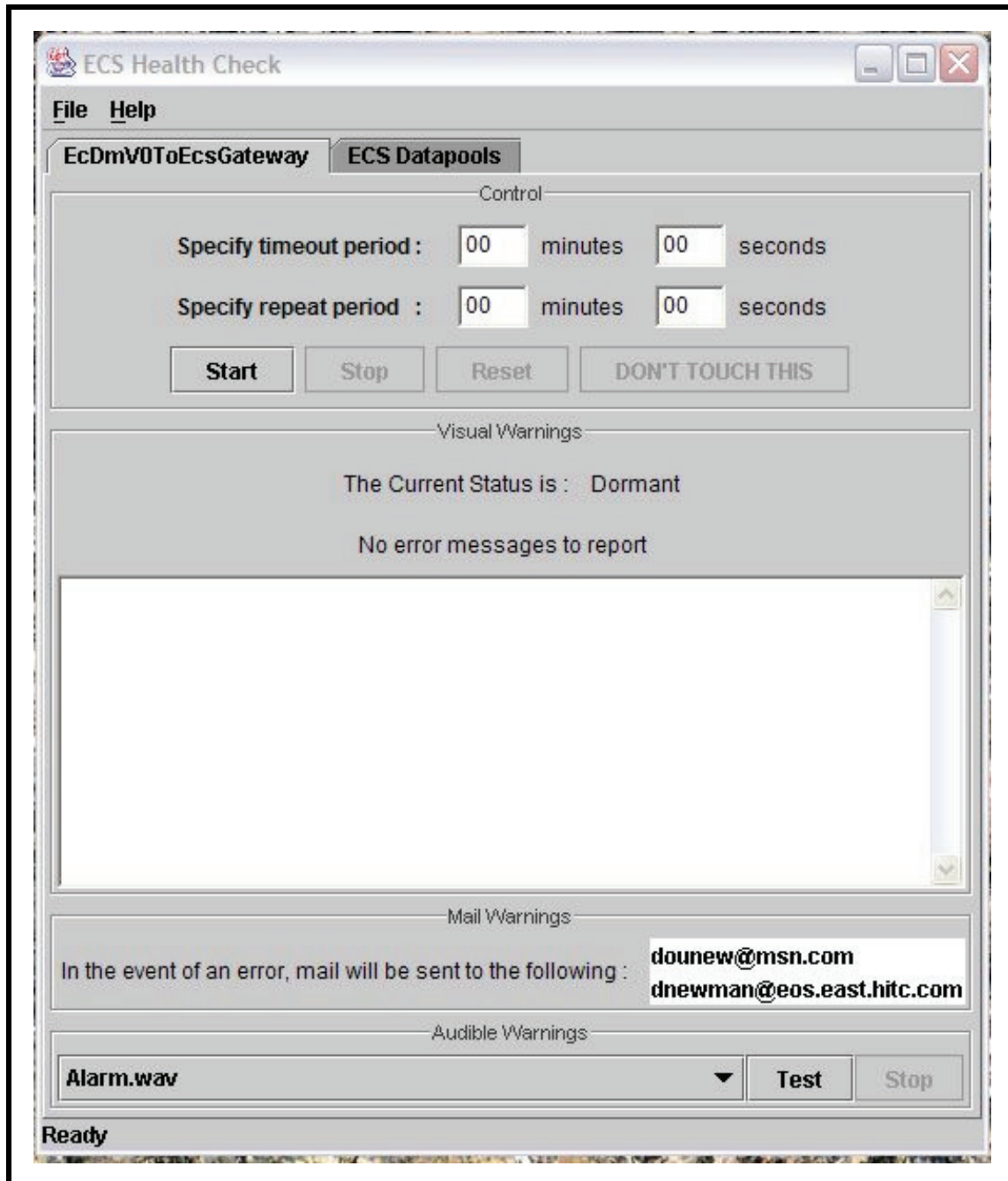


Figure 3.11-1. ECS Health Check GUI at Startup

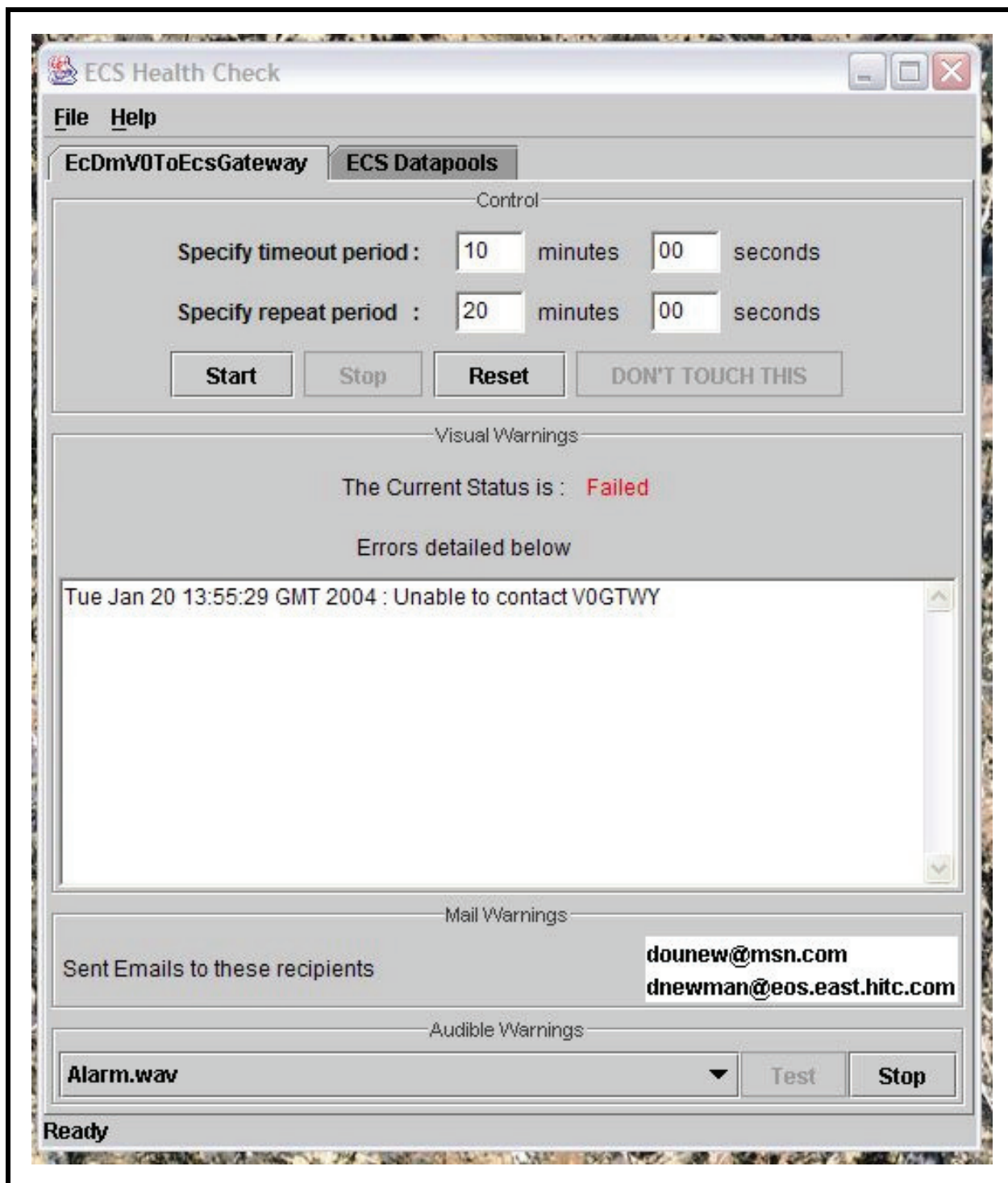


Figure 3.11-2. ECS Health Check GUI Having Detected an Error

3.11.1 Starting and Using the ECS Health Check GUI

The ECS Health Check GUI is accessible on the Sun Consolidation Internal Server host. To access the tool and view the current status of the EcDmV0ToEcsGateway and/or Data Pool use the procedure that follows.

3.11.1.1 Start and Use the ECS Health Check GUI

- 1 Log in to the Sun Consolidation Internal Server host as cmshared.
 - The EcCsHealthCheckStart script must be run by cmshared.
 - Examples of Sun Consolidation Internal Server hosts include **g00ml11**, **e00ml11**, **l00ml03**, and **n00ml04**.
 - For detailed instructions refer to the **Log in to System Hosts** procedure (previous section of this lesson).
- 2 At the UNIX prompt type **cd /usr/ecs/<MODE>/CUSTOM/bin/CSS** and then press the **Return/Enter** key.
 - Change to the directory containing the start script (i.e., EcCsHealthCheckStart) for the ECS Health Check GUI.
 - The location is different from that of most other start scripts because the COTS dependency on the V0ImClientSimulator application requires that the parent application be run in the same directory as the V0ImClientSimulator binary.
- 3 At the UNIX prompt type **EcCsHealthCheckStart <MODE>** and then press the **Return/Enter** key.
 - The ECS Health Check GUI is displayed.
- 4 Click on the appropriate tab for the area to be monitored.
 - The following choices are available:
 - **EcDmV0ToEcsGateway.**
 - **ECS Datapools.**
- 5 In the **Specify timeout period: minutes** and **seconds** text entry boxes type the number of minutes and seconds (respectively) before timeout.
 - **Timeout period** specifies how long the GUI will wait for a response from the current search before flagging an error.

- 6 In the **Specify repeat period: minutes** and **seconds** text entry boxes type the number of minutes and seconds (respectively) before repeating a search.
 - **Repeat period** specifies how often the GUI sends an inventory search to the area being monitored.
- 7 Click on the **Start** button in the **Control** pane to start checking the selected area.
 - The ECS Health Check GUI starts sending inventory searches to the selected area at the frequency specified in the **Specify repeat period** text boxes.
 - **The Current Status is:** (as displayed on the GUI) changes from **Dormant** to **Running**.
- 8 Repeat Steps 4 through 7 to set up inventory searches of the other area (if applicable).
- 9 Observe information displayed in the **Visual Warnings** pane of the ECS Health Check GUI and listen for audible warnings (if enabled).
 - Nothing much will appear to happen unless an error occurs in an inventory search sent to the EcDmV0ToEcsGateway/Data Pool, in which case the following indications will be evident:
 - **The Current Status is:** (as displayed on the GUI) changes from **Running** to **Failed** (in red).
 - Details concerning the time and nature of the error are displayed in the **Visual Warnings** text pane.
 - The **Mail Warnings** pane indicates that mail has been sent successfully to the recipients in the list.
 - A repeating audible alarm sounds (if enabled).
 - If an error occurs in a search sent to the EcDmV0ToEcsGateway/Data Pool, no further inventory searches will be sent to the selected area unless restarted using the **Start** button in the **Control** pane (refer to Step 13).
 - When an error occurs in an inventory search sent to the EcDmV0ToEcsGateway/Data Pool a detailed, time stamped description of the error is recorded in the EcCsHealthCheck.ALOG file in the /usr/ecs/*MODE*/CUSTOM/logs directory.
- 10 To stop an audible alarm (when applicable) click on the **Stop** button in the **Audible Warnings** pane.
 - The alarm stops sounding.
- 11 To clear error information from the ECS Health Check GUI (when applicable) click on the **Reset** button in the **Control** pane.
 - The error information is cleared from the ECS Health Check GUI.

- 12 To stop inventory searches of the selected area (when applicable) click on the **Stop** button in the **Control** pane.
 - The GUI goes to a Dormant state.
 - 13 To restart inventory searches of the selected area (when applicable) return to Step 7 (click on the **Start** button in the **Control** pane).
 - The GUI goes to a dormant state.
 - 14 To exit from the ECS Health Check GUI (when applicable) select **File → Exit** from the pull-down menu.
 - The ECS Health Check GUI is dismissed.
-

3.12 ECS Assistant and ECS Monitor

The Whazzup tool provides a quick look capability to note whether any servers are down. The ECS Assistant and ECS Monitor tools provide additional easy-to-use tools that offer a server monitoring and ping capability (ECS Monitor) as well as a capability to start and stop servers (ECS Assistant). Figure 3.10-1 shows the ECS Assistant GUI for access to manager functions, the ECS Assistant subsystem manager GUI, and an example of a confirmation dialog.

Table 3.12-1 contains the activity checklist for ECSAssistant.

Table 3.12-1. ECS Assistant - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|---|------------|-----------|
| 1 | SA | Starting ECS Assistant | (P) 3.12.1 | |
| 2 | SA | Using the ECS Assistant Server Monitor | (P) 3.12.2 | |
| 3 | SA | Using EcCslIdPingServers to Determine Server Status | (P) 3.12.3 | |

3.12.1 Starting ECS Assistant

- 1 Log in to one of the host machines.
- 2 At the UNIX prompt on the host from which the ECS Assistant is to be run, type **setenv ECS_HOME /usr/ecs** then press the **Return/Enter** key.
 - To verify the setting, type **echo \$ECS_HOME** then press the **Return/Enter** key.

- 3 At the UNIX prompt, type **cd /tools/common/ea** then press the **Return/Enter** key. Then type **EcCoAssist /tools/common/ea &** then press the **Return/Enter** key.
 - **/tools/common/ea** is the path where ECS Assistant is installed, and also where EcCoScriptlib may be found.
 - The ECS Assistant GUI is displayed.
- 4 At the ECS Assistant GUI, click the **Subsystem Manager** pushbutton.
 - The Subsystem Manager GUI is displayed.
- 5 Select a mode by clicking on the down arrow at the right end of the **Mode** field and then on the desired mode name in the resulting list.
 - The selected mode is displayed in the **Mode** field and colored indicators show the installation status for components in that mode on the host; the legend for the color indications is at the lower right on the Subsystem Manager window.
- 6 In the list of subsystems, double click on the name of the subsystem of interest.
 - One or more component groups appear below the selected subsystem name.

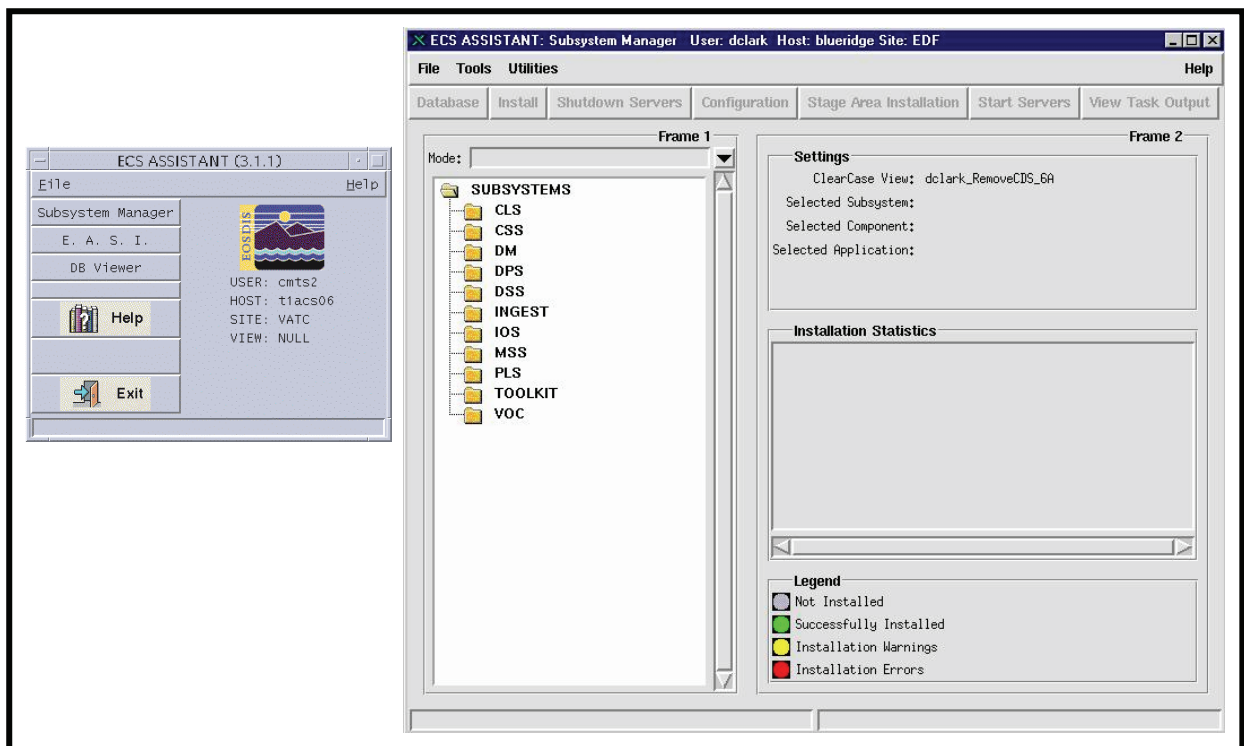


Figure 3.12-1. ECS Assistant GUI Manager Windows

- 7 Double click on the name of a component group.
 - One or more application groups appear below the selected component group name.
 - 8 Double click on the name of the application group of interest.
 - The applications or servers in the selected group are listed below the name of the group.
 - 9 Single click on the name of an application or server of interest.
 - The selected application or server is highlighted.
 - Detailed installation information is displayed in the **Installation Statistics** window.
-

ECS Monitor provides a convenient way to monitor the status of the servers by listing their up/down condition. The ECS Monitor GUI is shown in Figure 3.12-2; the status flag for a server is up or down indicating whether or not that server is running, and for a server that is running, the window shows the process ID (PID), the user ID, and the start time. There is a script that works with a *Sweeper* binary to ping the servers and clients in a mode to determine their status.

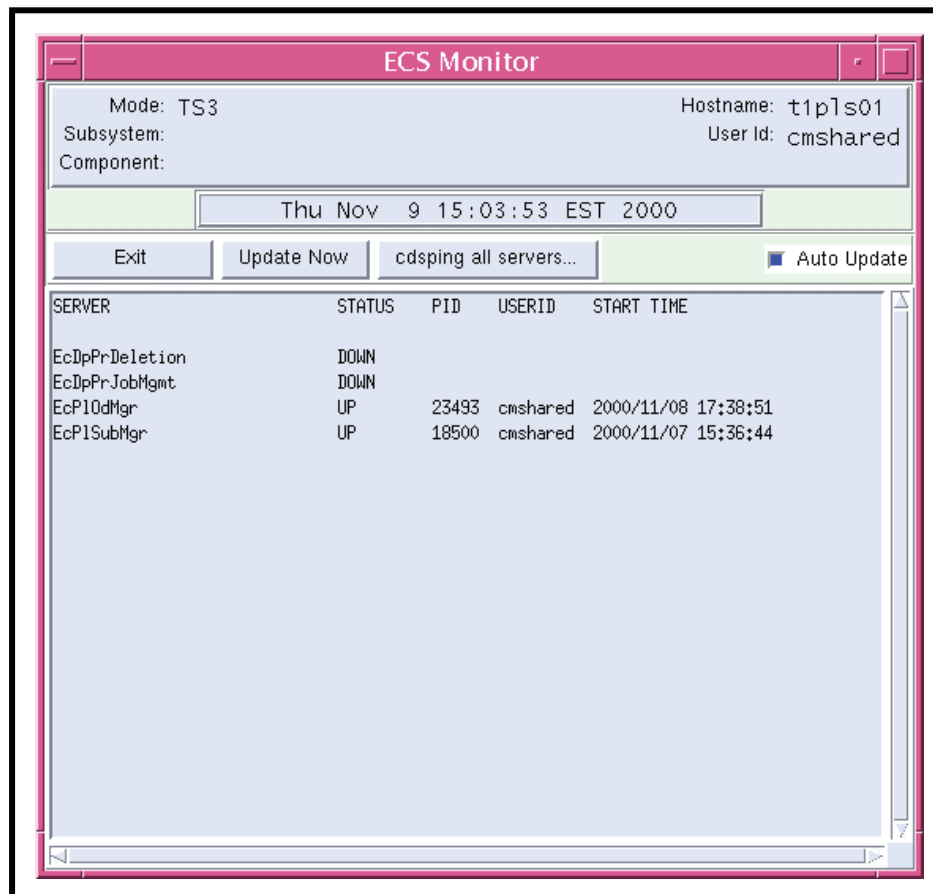


Figure 3.12-2. ECS Monitor GUI

3.12.2 Using the ECS Assistant Server Monitor

- 1 Log in to one of the host machines.
 - 2 At the UNIX prompt on the host from which the ECS Assistant is to be run, type **setenv ECS_HOME /usr/ecs** then press the **Return/Enter** key.
 - To verify the setting, type **echo \$ECS_HOME** then press the **Return/Enter** key.
 - 3 At the UNIX prompt, type **cd /tools/common/ea** then press the **Return/Enter** key.
 - **/tools/common/ea** is the path where ECS Monitor is installed.
 - 4 Type **EcCoMonitorGui /tools/common/ea <MODE> &**, then press **Return/Enter** key.
 - **/tools/common/ea** is the path where EcCoScriptlib may be found.
 - The **ECS Monitor GUI** is displayed, showing the status (**UP** or **DOWN**) of the servers on the current host in the mode specified in the command, as indicated near the top left corner of the window.
 - The status “**UP/DOWN**” indicates whether a listed server is running.
 - 5 To update the **Server Monitor** GUI click the **update** button in the GUI.
 - This causes the list to update to the current status.
 - 6 To monitor other servers, log in to other hosts and launch the ECS Monitor GUI in the desired mode, as in Steps 2 through 4.
 - To exit, click the **EXIT** button. This terminates display of the monitor GUI.
-

Use the following procedure to ping servers.

3.12.3 Using EcCsIdPingServers to Determine Server Status

- 1 Log in to one of the host machines.
- 2 At the UNIX prompt, type **cd /usr/ecs/MODE/CUSTOM/utilities** then press the **Return/Enter** key.
 - The prompt reflects a change to directory **cd /usr/ecs/MODE/CUSTOM/utilities**, where **MODE** is likely to be **OPS**, **TS1**, or **TS2**.

3 Then type **EcCsIdPingServers** *MODE* then press the **Return/Enter** key.

- The result should appear similar to the following:

```
/usr/ecs/DEV03/CUSTOM/bin/CSS/Sweeper -nsh dss2 -nsp 22822
FoSwSweeper application started...
We made a connection with EntryId =g0icg01:17871:12451240 ---
EcSrTransportEcInGranServer
We made a connection with EntryId =g0ins02:22336:6737528 --- DsHrQuitIDL
We made a connection with EntryId =g0pls02:35211:25637 --- PLOdMsgDObj
We made a connection with EntryId =g0dis02:48315:18311 ---
DsDdRequestMgrIDL
We made a connection with EntryId = g0ins02:17862:12461267 ---
InAutoIngestIF
We made a connection with EntryId = g0dis02:49473:13375 --- DsStReqMgrIDL
We made a connection with EntryId = g0ins02:41566:13071 --- IoAdRpc
We made a connection with EntryId = g0ins02:18139:12460808 ---
InRequestMgrIF
We made a connection with EntryId =g0dms03:42000:13266 ---
EcSrTransportDDICT
We made a connection with EntryId = g0pls02:22359:6737528 ---
    DsHrNonConfIDL681ab65e-60bc-1024-8e70-08006902a6d6
We made a connection with EntryId = g0pls02:22346:6737528 ---
    DsHrConformantIDL681ab65d-60bc-1024-8e70-08006902a6d6
We made a connection with EntryId =g0mss21:64657:8006 --- EcAcOrderMgr
We made a connection with EntryId =g0mss11:41449:22898 ---
EcSrTransportDarServer
We made a connection with EntryId = g0icg02:17724:12445092 --- EcRgRegistry
We made a connection with EntryId =g0mss11:41278:22739 ---
InDDNTransferPkt
We made a connection with EntryId =g0psl02:35085:25466 --- Deletion
We made a connection with EntryId =g0pls02:35168:25584 ---
SubscriptionQueue
We made a connection with EntryId =g0mss21:64700:8059 ---
MsAcUsrRequestMgr
We made a connection with EntryId =g0mss21:64690:8059 ---
MsAcRegUserMgr
We made a connection with EntryId =g0mss21:64695:8059 ---
MsAcUsrProfileMgr
We made a connection with EntryId =g0pls02:35127:25527 ---
DpPrSchedulerDObj
We made a connection with EntryId =g0ins02:22364:6738409 ---
    DsHrNonConfIDL681ab654-60bc-1024-8e70-08006902a6d6
We made a connection with EntryId =g0ins02:22353:6738409 ---
    DsHrConformantIDL681ab653-60bc-1024-8e70-08006902a6d6
We made a connection with EntryId =g0ins02:22342:6738409 --- DsHrQuitIDL
```

3.13 Tape Operations

In this lesson you will learn how Networker Administrative software and the Exabyte tape drive work together to administer the use of tapes for system backups and file restorations. Functions such as how to label a new tape, how to index a tape cartridge, and how to perform backups and restores are covered.

Table 3.13-1 contains the activity checklist for Tape Operations.

Table 3.13-1. Tape Operations - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|--------------------------|--------------|-----------|
| 1 | SA | Performing Tape Labeling | (P) 3.13.2.1 | |
| 2 | SA | Indexing Tape | (P) 3.13.3.1 | |

Terms:

- **Cartridge** - A hardware device that is part of the Exabyte tape drive. It holds up to 10 tapes that are automatically selected by Networker.
- **Drive** - Hardware device into which the tape or tape cartridge is inserted that performs the actual recording of data.
- **Index** - A list of the labeled tapes currently stored in the jukebox.
- **Inventory** - The action of making an index.
- **Jukebox** - A hardware device that stores more than one tape used for system backups and restores. Working in conjunction with specialized software, it can automatically select the proper tape, load the tape into the tape drive, and return it to its appropriate slot upon completion of the task.
- **Label** - A unique name assigned to a tape by Networker.
- **Volume** - A recording medium; in the case of this course, a volume and a tape are synonymous.

3.13.1 Networker Administrator Screen

The main Networker Administrator screen (Figure 3.13-1), which is displayed after typing **nwadmin** at a UNIX prompt, contains four main sections:

- The menu bar at the top of the screen, which displays all of the possible capabilities of Networker Admin.
- The **speedbar**, which can be customized, displays icons that execute the most common procedures.

- Current configuration information, including the current Networker server, the available backup devices (tape drives, file systems, CD-ROMs, etc.).
- Current status windows, which display in real time the actual activity on the various devices, and progress and error messages.



Figure 3.13-1. NetWorker Administrative Main Screen

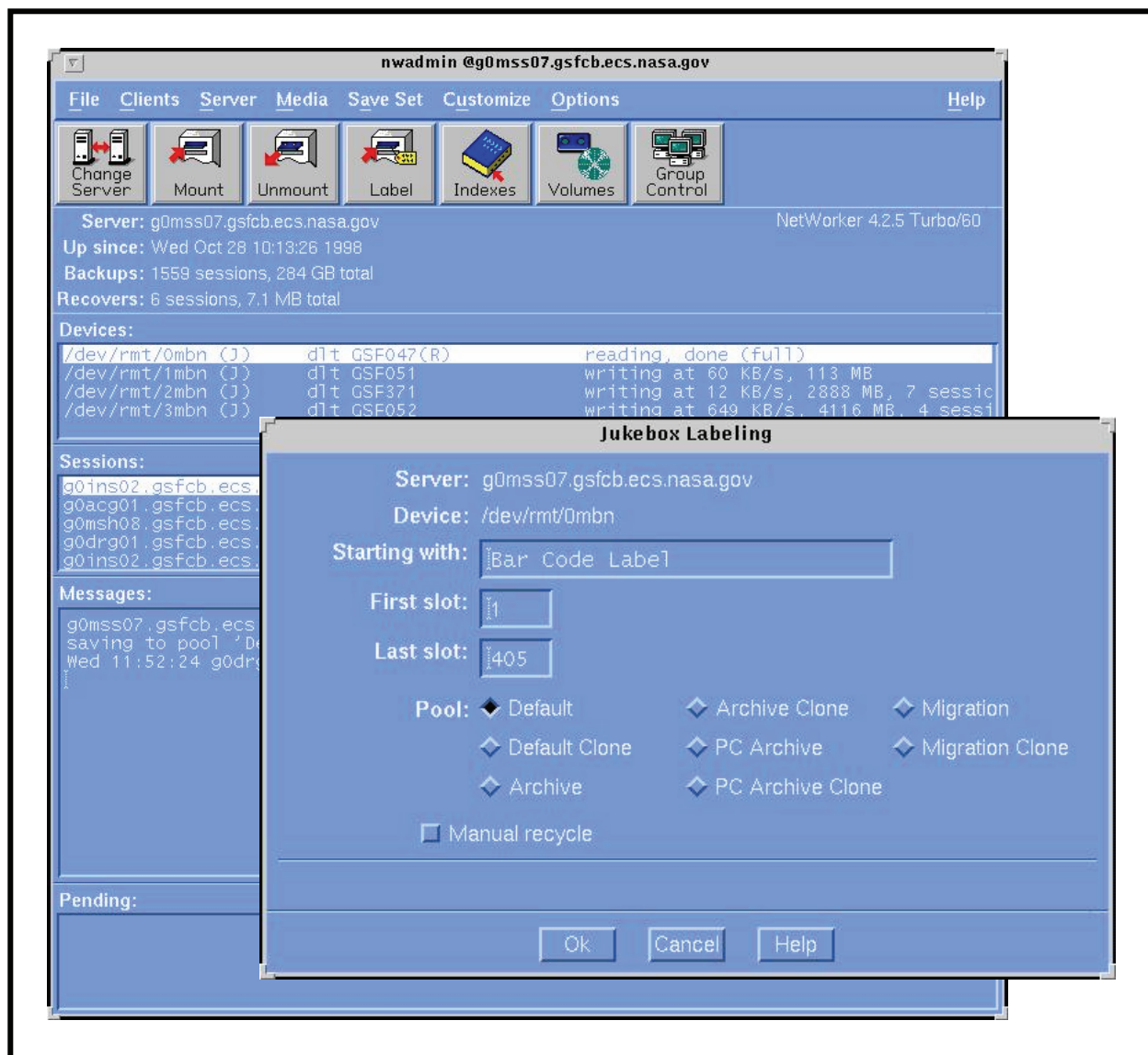
3.13.2 Labeling Tapes

Files and directories have unique names that are assigned by the user to identify them. In much the same manner, tapes are given unique names, or labels. This allows such programs as Networker and such hardware devices such as the Exabyte jukebox to automate the tape selection process when performing system backups and restores. When a tape is initialized, Networker assigns it a label. Networker then stores the tape's label with a file that is written to the tape so that when a file restoration request is received, Networker will know exactly which tape to select from the jukebox.

3.13.2.1 Performing Tape Labeling

- 1 Log in to a system terminal.
- 2 To set the display to the current terminal type **setenv DISPLAY <IPNumber>:0.0** then press the **Return/Enter** key.
- 3 To start the log-in to the Backup client server type **ssh BackupServerName** in the second window and then press the **Return/Enter** key.
 - If you have previously set up a secure shell passphrase and executed **ssr (sshremote)**, a prompt to **Enter Passphrase for key '<user@localhost>'** appears; continue with Step 3.
 - If you have not previously set up a secure shell passphrase, go to Step 4.
- 4 If a prompt to **Enter Passphrase for key '<user@localhost>'** appears, type your **Passphrase** and then press the **Return/Enter** key. Go to Step 5.
- 5 At the **<user@remotehost>'s password:** prompt, type your **Password** and then press the **Return/Enter** key.
- 6 To start the log-in as root type **su** then press the **Return/Enter** key.
 - A password prompt is displayed.
- 7 At the password prompt enter **RootPassword** then press the **Return/Enter** key.
 - Remember that the password is case sensitive.
 - You are authenticated and returned to the UNIX prompt.
- 8 At the UNIX prompt, type **nwadmin** then press the **Return/Enter** key.
 - A window opens for the Networker Administrative program.
- 9 Insert the blank tape(s) in the jukebox's cartridge.
 - Remove any non-blank tapes from the cartridge or else they will be re-labeled and the data on the tapes will be lost.
- 10 Install the cartridge in the jukebox.

- 11 Click the **Label** button.



- The **Jukebox Labeling** window opens (Figure 3.13-2).

Figure 3.13-2. Jukebox Labeling Window

- 12 In the field marked **Starting with**, type the tape label you wish to use for the first tape in the sequence.
- Tape labels are named by using the host name (e.g., **x00ml01**), a dot or period, and a sequential number (e.g., **001**, **002**).

- By default, the system will prompt you with the next label in the sequence (e.g., **x0oml01.011**).
- 13** In the **First Slot** field, enter **1** or the slot containing the first volume to be labeled; in the **Last Slot** field, enter **10** or the slot containing the last volume to be labeled.
 - Slot 1 is at the top of the cartridge and 10 at the bottom.
 - Slot 11 is the non-removable slot within the jukebox. This usually contains a cleaning tape.
 - It is OK to leave empty slots.
 - 14** Click on the **OK** button.
 - A status message indicating the progress of the tape labeling procedure appears and updates.
 - Labeling a full cartridge of tapes takes about 15 minutes.
 - 15** When the status in the **Jukebox Labeling** window reads **finished**, click on the **Cancel** button.
 - The **Jukebox Labeling** window closes.
 - 16** Select **File → Exit** from the pull-down menu.
 - The **nwadmin** program terminates and you are returned to the UNIX prompt.
 - 17** At the UNIX prompt for the backup server, type **exit** then press the **Return/Enter** key.
 - **Root** is logged out.
 - 18** Type **exit** again then press the **Return/Enter** key.
 - You are logged out of and disconnected from the backup server.
 - 19** Put an identifying sticker on the outside of each tape cassette.
-

3.13.3 Indexing Tapes

Labeled tapes are loaded in a tape cartridge that is inserted into the Exabyte tape drive, also referred to as the jukebox. Networker needs to know the location of each tape in the jukebox. To do this, Networker uses a process called **inventory**, which prepares an index by matching a tape label to the cartridge slot that holds that tape (Figure 3.13-3). Then, when a request to recover a file or a set of files is received, *Networker* locates the tape based on the information in its memory.

CAUTION

If you move a tape from its position in the cartridge, Networker will not know where to find it. You must re-index the cartridge by performing these procedures again for Networker to select the correct tape.

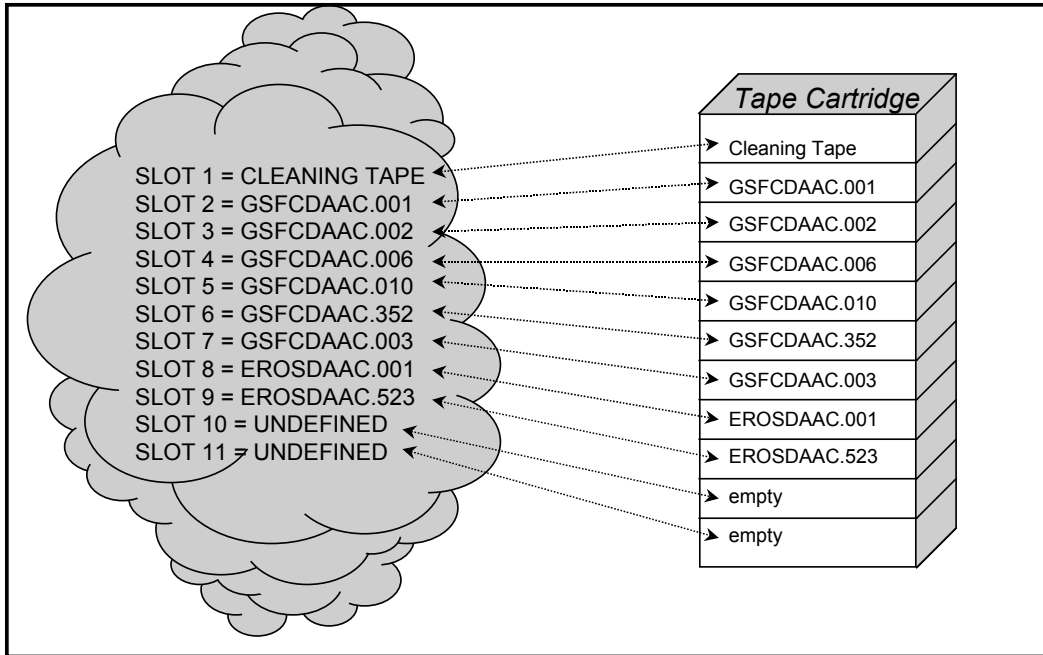


Figure 3.13-3. Tape Index Following the Initial Inventory

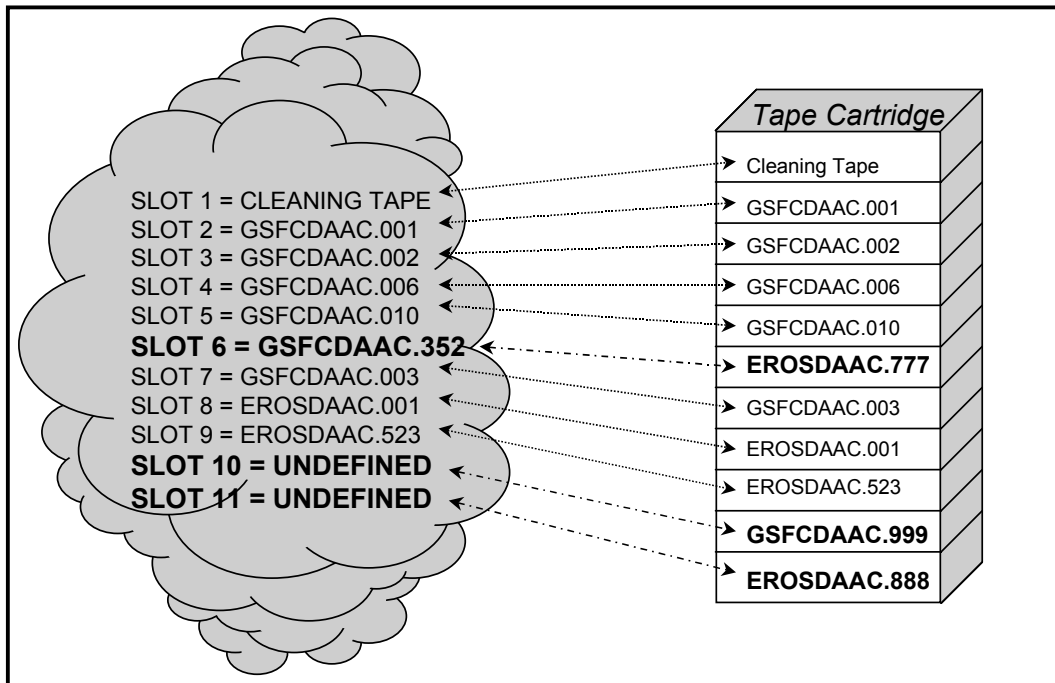


Figure 3.13-4. Tapes Changed But Not Re-Inventoried

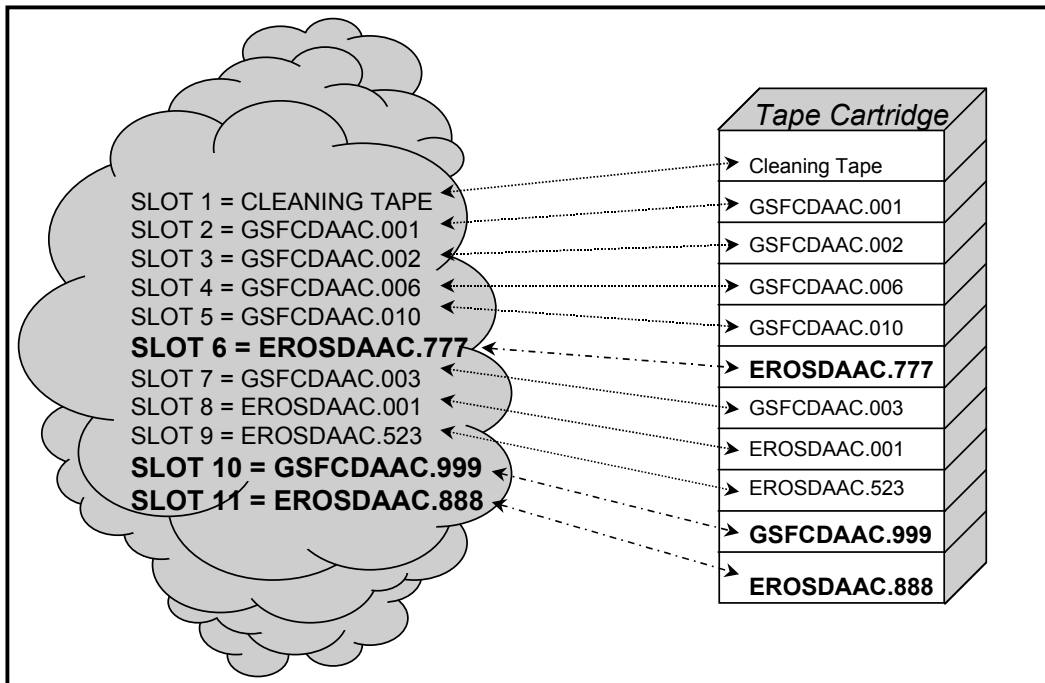


Figure 3.13-5. Index is Updated after Re-Inventory

3.13.3.1 Indexing Tape

- 1 Login to a system terminal.
- 2 Set display to current terminal by typing: **setenv DISPLAY <IPNumber>:0.0** then press the **Return/Enter** key.
- 3 Start the log-in to the Backup client server by typing **ssh BackupServerName** in the second window and then press the **Return/Enter** key.
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter Passphrase for key '<user@localhost>'** appears; continue with Step 3.
 - If you have not previously set up a secure shell passphrase, go to Step 4.
- 4 If a prompt to **Enter Passphrase for key '<user@localhost>'** appears, type your **Passphrase** and then press the **Return/Enter** key. Go to Step 5.
- 5 At the **<user@remotehost>'s password:** prompt, type your **Password** and then press the **Return/Enter** key.

- 6 Log in as root by typing **su** then press the **Return/Enter** key.
 - A password prompt is displayed.
- 7 Enter the **RootPassword** then press the **Return/Enter** key.
 - You are authenticated as root and returned to the UNIX prompt.
- 8 At the UNIX prompt, type **nwadmin** then press the **Return/Enter** key.
 - A window opens for the **Networker Administrative** program.
- 9 Click the **Mount** button, or select **Media -> Mount** from the menu.
 - The **Jukebox Mounting** window opens (Figure 3.13-6) and displays a list of the tapes that Networker is currently aware of.
 - When you are finished with this window, click the **Cancel** button.

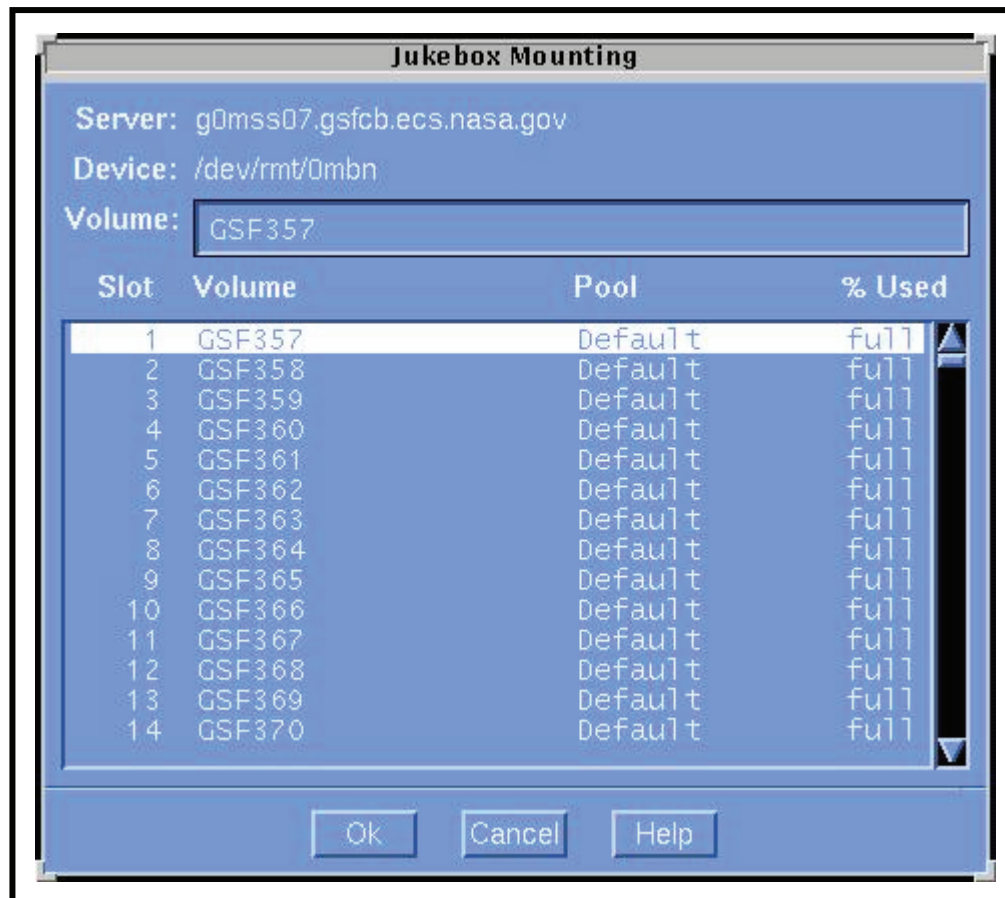


Figure 3.13-6. Jukebox Mounting Window

- 10 Insert the required tape(s) in the jukebox's cartridge then install the cartridge in the jukebox.
 - Refer to the jukebox's documentation for detailed instructions on installing the cartridge.
 - 11 Select **Media** from the menu bar then select **Inventory**.
 - The **Jukebox Inventory** window opens.
 - 12 In the **First Slot** field, enter **1** or the slot containing the first volume to be labeled; in the **Last Slot** field, enter **10** or the slot containing the last volume to be labeled.
 - Slot 1 is at the top of the cartridge and 10 at the bottom.
 - Slot 11 is the non-removable slot within the jukebox. This usually contains a cleaning tape.
 - It is OK to leave empty slots or slots with previously inventoried tapes.
 - 13 Click the **OK** button.
 - A status message indicating the progress of the tape indexing procedure appears and updates.
 - Inventorying a full cartridge of tapes takes between 20 and 30 minutes.
 - 14 When the **Jukebox Inventory** status reads **finished**, click the **Cancel** button.
 - 15 Click the **Mount** button to verify that the indexing worked.
 - The **Jukebox Mounting** window opens.
 - The **required tape(s)** should be shown. If not, repeat this procedure from Step 9.
 - 16 Click the **Cancel** button.
 - The **Jukebox Mounting** window closes.
 - 17 From the menu bar, select **File** then select **Exit**.
 - 18 At the UNIX prompt for the *BackupServer*, type **exit** then press the **Return/Enter** key.
 - 19 At the next UNIX prompt type **exit** again then press the **Return/Enter** key.
-

3.14 System Backups and Restores

Performing regular and comprehensive backups is one of the most important responsibilities a System Administrator has. Backups are the insurance that essentially all of the system data is always available. If the system crashes and all disks are damaged, the System Administrator should be able to restore the data from the backup tapes depending on backup method (e.g., full or partial).

Table 3.14-1 contains the activity checklist for System Backup and Restores.

Table 3.14-1. System Backup and Restores - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|--|--------------|-----------|
| 1 | SA | Performing On-Demand Incremental Backup | (P) 3.14.1.1 | |
| 2 | SA | Performing Full Backup | (P) 3.14.2.1 | |
| 3 | SA | Performing Single or Multiple File Restore | (P) 3.14.3.1 | |
| 4 | SA | Performing Full System Restore | (P) 3.14.4.1 | |

3.14.1 Incremental Backup

An incremental backup copies to tape all files on a system or subsystem that were created or modified since the previous incremental backup regardless of the backup level. The purpose of an incremental backup is to insure that the most recent edition of a file is readily available in case user error or disastrous system failure causes the file to become corrupt. Incremental backups are scheduled at a time that causes minimal disruption to the users. Copies of all incremental backup tapes are stored offsite for five weeks before they are reused.

Incremental backups are performed automatically according to the schedule setup in the Networker. Schedules windows (Figure 3.14-1). Incremental backups can also be requested at unscheduled times by completing the **Incremental Backup Request Form** and submitting it to the DAAC manager.

3.14.1.1 Performing On-Demand Incremental Backup

- 1 Log in to a system terminal.
- 2 To set the display to the current terminal type **setenv DISPLAY <IPNumber>:0.0** then press the **Return/Enter** key.
- 3 To start the log-in to the Backup client server type **ssh BackedUpSystemName** in the second window and then press the **Return/Enter** key.
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter Passphrase for key '<user@localhost>'** appears; continue with Step 3.
 - If you have not previously set up a secure shell passphrase, go to Step 4.
- 4 If a prompt to **Enter Passphrase for key '<user@localhost>'** appears, type your **Passphrase** and then press the **Return/Enter** key. Go to Step 5.
- 5 At the **<user@remotehost>'s password:** prompt, type your **Password** and then press the **Return/Enter** key.

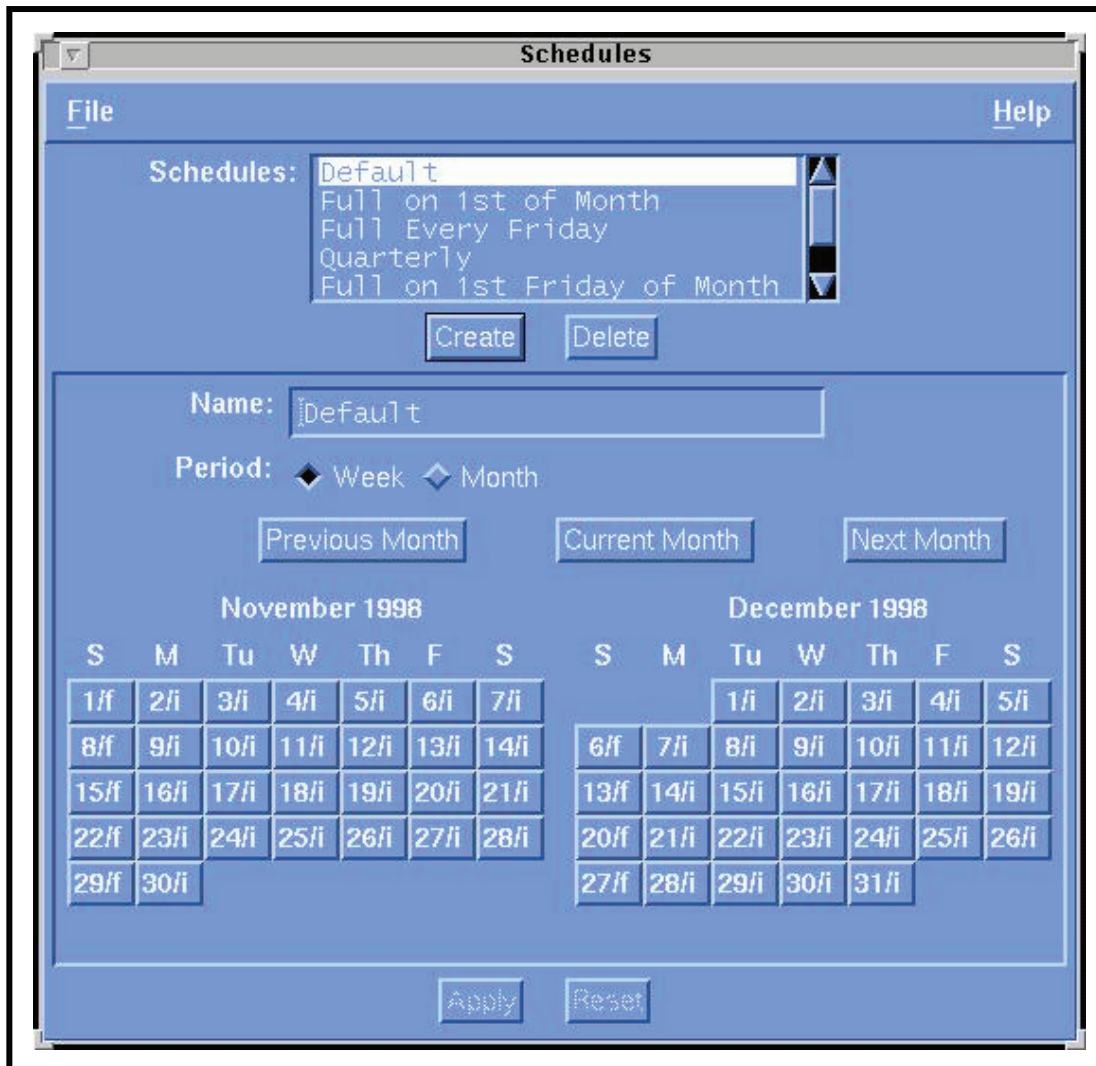


Figure 3.14-1. Networker Schedules Window

- 6 Log in as root by typing **su** then press the **Return/Enter** key.
 - A password prompt is displayed.
- 7 Enter the **RootPassword** then press the **Return/Enter** key.
 - You are authenticated as root and returned to the UNIX prompt.
- 8 At the UNIX prompt, type **nwadmin** then press the **Return/Enter** key.
 - A window opens for the Networker Administrative program.

- 9 Select **Customize → Schedules** from the pull-down menu.
 - The **Schedules** window opens.
- 10 Look at the button for today and note the letter on that day. If there is an **i** next to the date on this button, go to Step 11.
 - The **i** stands for incremental; **f** stands for full. Whichever is on the button for today is what kind of backup that will be done, unless it is overridden.
- 11 Click and hold the button for today, select **Overrides** from the resulting menu, select **Incremental** from the next resulting menu.
- 12 Click on the **Apply** button.
- 13 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.
- 14 Click the **Group Control** button.
 - The **Group Control** window opens.
- 15 Click on the **Start** button.
 - A **Notice** window opens.
- 16 Click on the **OK** button.
 - The **Notice** window closes. The regularly scheduled backup will still run (even though we are now doing a backup).
- 17 Close the **Group Control** window by clicking in the upper left corner of the **Group Control** window and selecting **Close** from the resulting menu.
 - Status updates appear in the **nwadmin** window.
 - When the backup is complete, a **Finished** message will appear.
- 18 If the button for today in Step 10 had an **i** on it, go to Step 22.
- 19 Select **Customize → Schedules** from the pull-down menu.
 - The **Schedules** window opens.
- 20 Click and hold the button for today, select **Overrides** from the resulting menu, and select **Full** from the next resulting menu.
- 21 Click on the **Apply** button.
- 22 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.
- 23 To quit the Networker Administrative program select **File → Exit** from the pull-down menu.
 - The **nwadmin** window closes.

- 24 At the UNIX prompt for the machine to be backed up, type **exit** then press the **Return/Enter** key.
 - Root is logged out.
 - 25 Type **exit** again then press the **Return/Enter** key.
 - You are logged out and disconnected from the machine to be backed up.
-

3.14.2 Full System Backup

A full system backup is a snapshot of the data on the entire system as of a particular date. The data is stored on tapes that are used to recreate the system in the event of a total system failure. The full system backup is run by the System Administrator on a regular schedule, usually weekly. Full system backup tapes are stored offsite for security reasons.

3.14.2.1 Performing Full Backup

- 1 Log in to a system terminal.
- 2 To set the display to the current terminal type **setenv DISPLAY <IPNumber>:0.0** then press the **Return/Enter** key.
- 3 To log in to the machine to be backed up type **ssh *BackedUpSystemName*** then press the **Return/Enter** key.
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter Passphrase for key '<user@localhost>'** appears; continue with Step 3.
 - If you have not previously set up a secure shell passphrase go to Step 4.
- 4 If a prompt to **Enter Passphrase for key '<user@localhost>'** appears, type your **Passphrase** and then press the **Return/Enter** key. Go to Step 5.
- 5 At the **<user@remotehost>'s password:** prompt, type your **Password** and then press the **Return/Enter** key.
- 6 To log in as root type **su** then press the **Return/Enter** key.
 - A password prompt is displayed.
- 7 Type the **RootPassword** then press the **Return/Enter** key.
 - You are authenticated as root and returned to the UNIX prompt.

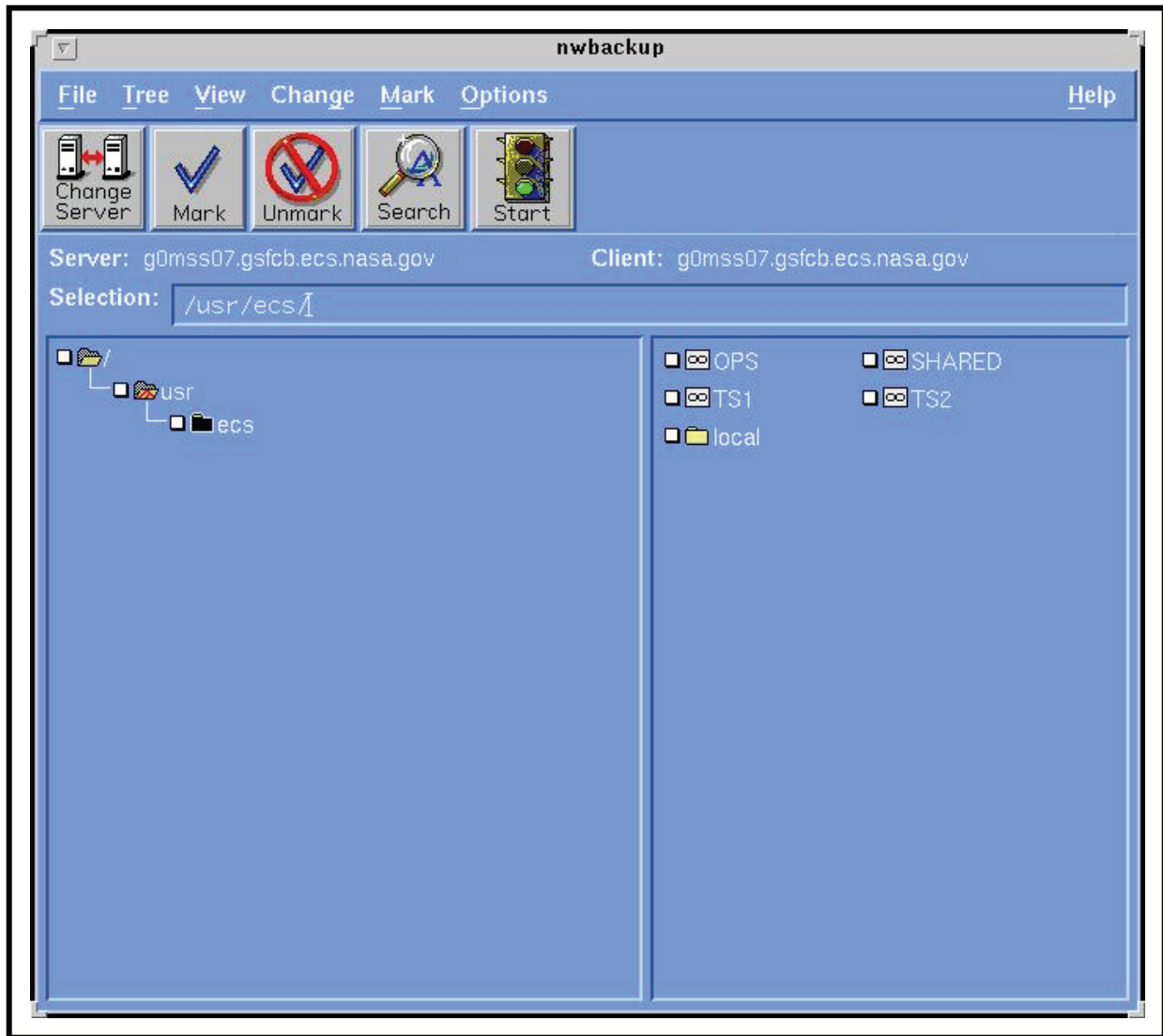


Figure 3.14-2. Networker Backup Window

- 8 To execute the Networker Backup program type **nwbackup** then press the **Return/Enter** key.
 - A Networker Backup window opens (Figure 3.14-2). You are now able to perform a full backup.
- 9 If no **files/directories to be backed up** were provided by the requester, i.e. the whole machine is to be backed up, then type / in the **Selection** field and click the **Mark** button.
 - / is designated for backup and has a check next to it.

- 10 If **files/directories to be backed up** were provided, then select the **files/directories to be backed up** in the directory display and click the **Mark** button.
 - Drag scroll bar with the mouse to scroll the list up and down.
 - Double-click on directory name to list its contents.
 - To move up a directory level, type the path in the **Selection** field.
 - Clicking the **Mark** button designates the file for backup and puts a check next to it.
 - 11 Click on the **Start** button.
 - A **Backup Options** window opens.
 - 12 Click on the **OK** button.
 - The **Backup Options** window closes.
 - The **Backup Status** window opens providing updates on the backup's progress.
 - 13 After the **Backup Completion Time** message appears in the **Backup Status** window, click the **Cancel** button.
 - The **Backup Status** window closes.
 - The backup is complete.
 - 14 To quit the Networker Backup program select **File** → **Exit** from the pull-down menu.
 - The Networker Backup window closes.
 - 15 At the UNIX prompt for the **machine to be backed up**, type **exit** then press the **Return/Enter** key.
 - Root is logged out.
 - 16 Type **exit** again then press the **Return/Enter** key.
 - You are logged out and disconnected from the machine to be backed up.
-

3.14.3 Single or Multiple File Restore

From time to time individual files or groups of files (but not all files) will have to be restored from an incremental backup tape due to operator error or system failure.

In order to perform the procedure, the System Administrator must have obtained the following information from the requester:

- Name of machine to be restored.
- Name of file(s) to be restored.
- Date from which to restore.

- User ID of the owner of the file(s) to be restored.
- Choice of action to take when conflicts occur. Choices are:
 - Rename current file
 - Keep current file
 - Write over current file with recovered file

3.14.3.1 Performing Single or Multiple File Restore

- 1 Log in to a system terminal.
- 2 To set the display to the current terminal type **setenv DISPLAY <IPNumber>:0.0** then press the **Return/Enter** key.
- 3 To log in to the machine to be restored type **ssh <host name> *Machine Restored*** then press the **Return/Enter** key.
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter Passphrase for key '<user@localhost>'** appears; continue with Step 3.
 - If you have not previously set up a secure shell passphrase, go to Step 4.
- 4 If a prompt to **Enter Passphrase for key '<user@localhost>'** appears, type your **Passphrase** and then press the **Return/Enter** key. Go to Step 5.
- 5 At the **<user@remotehost>'s password:** prompt, type your **Password** and then press the **Return/Enter** key.
- 6 To log in as root type **su** then press the **Return/Enter** key.
 - A password prompt is displayed.
- 7 Type the **RootPassword** then press the **Return/Enter** key.
 - You are authenticated as root and returned to the UNIX prompt.
- 8 To log in as the user type **su UserID**.
 - You are authenticated as the owner of the file(s) to be restored.
- 9 To execute the Networker Recovery program type **nwrecover** then press the **Return/Enter** key.
 - A window opens for the **Networker Recovery** program (Figure 3.14-3). You are now able to restore files.

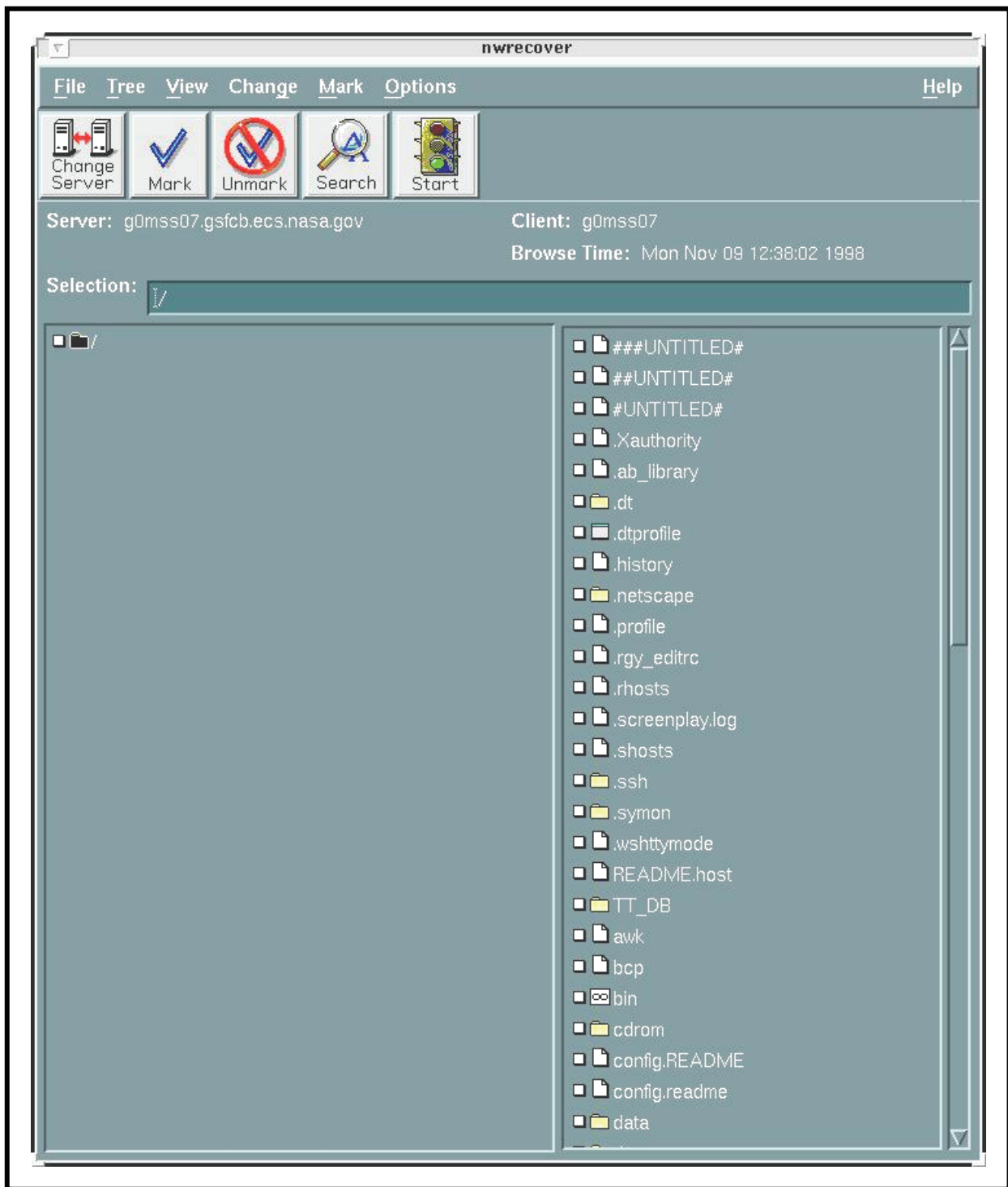


Figure 3.14-3. Networker Recovery Window

- 10 Select **file(s) to be restored** and click the **Mark** button.
 - Drag scroll bar with the mouse to scroll the list up and down.
 - Double-click on directory name to list its contents.
 - Clicking on the **Mark** button designates the file for restore and puts a check next to it.
- 11 Select **Change → Browse Time** from the pull-down menu.
 - The **Change Browse Time** window opens.
- 12 Select the **date from which to restore**.
 - Networker will automatically go to that day's or a previous day's backup which contains the file.
- 13 Click on the **Start** button.
 - The **Conflict Resolution** window opens.
- 14 In response to the question "Do you want to be consulted for conflicts" click on the **yes** button.
- 15 Click on the **OK** button.
 - If prompted with a conflict, choices of action will be: rename current file, keep current file, or write over current file with recovered file.
 - Select the requester's **choice of action to take when conflicts occur**.
 - The **Recover Status** window opens providing information about the to be restored.
 - If all the required tapes are not in the drive, a notice will appear.
 - Click on the **OK** button in the notice window.
- 16 When a **recovery complete** message appears, click on the **Cancel** button.
- 17 Select **File → Exit** from the pull-down menu.
 - The Networker Recovery program quits.
- 18 Type **exit** then press the **Return/Enter** key.
 - The owner of the file(s) to be restored is logged out.
- 19 Type **exit** again then press the **Return/Enter** key.
 - Root is logged out

20 Type **exit** one last time then press the **Return/Enter** key.

- You are logged out and disconnected from the **machine to be restored**.
-

3.14.4 Complete System Restore

A complete system restore is an emergency procedure that should be performed only in the event of a system crash with the loss of data. 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 between the last backup and the time of the restore will be lost. The System Administrator will determine which complete backup tape(s) to use (Figure 3.14-4). Depending on the frequency of complete system backups and incremental backups, data loss can be minimized.

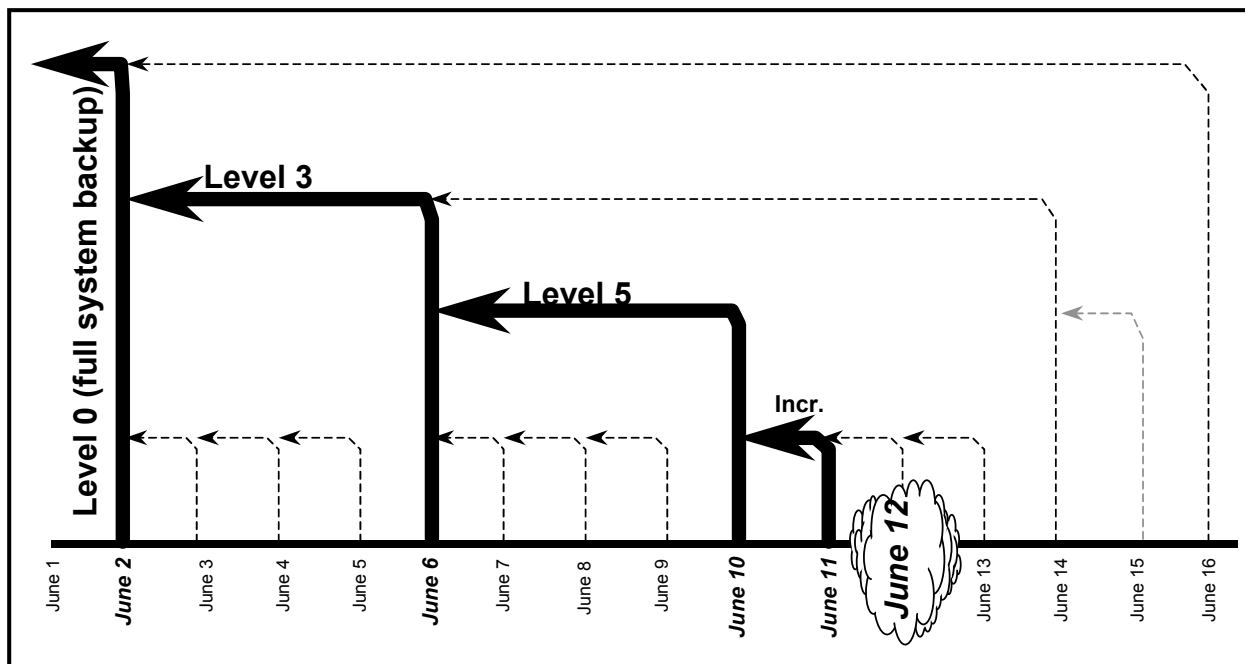


Figure 3.14-4. Tapes Required for Full System Restore

A complete system restore involves restoring a number of tapes depending upon the particular situation. For example, should a system failure occur immediately after a full system backup was performed, only the tapes used in that backup will be required to restore the system to its usable state. However, if there was a period of time between the last full system backup and the system failure, tapes from the last full system backup as well as partial and incremental backups will have to be restored. This may become a time consuming process depending on the server affected, how much data is to be recovered, and how many tapes need to be restored. Additionally, the System Administrator may determine that only one or two of the many

partitions need to be restored to make the system whole again. Therefore, these procedures will have to be mixed and matched to determine the proper restoration procedure for a given situation.

To perform the procedure, the SA must have the following information about the requester:

- Name of system to be restored
- Date from which to restore

3.14.4.1 Performing Full System Restore

- 1 To log in to the backup server type `/tools/bin/ssh BackupServerName` then press the **Return/Enter** key.
- 2 To set the display to the current terminal type `setenv DISPLAY <IPNumber>:0.0` then press the **Return/Enter** key.
- 3 To log in to the machine to be restored type `/tools/bin/ssh MachineToRestore` then press the **Return/Enter** key.
 - If you have previously set up a secure shell passphrase and executed `ssr`, a prompt to **Enter Passphrase for key '<user@localhost>'** appears; continue with Step 3.
 - If you have not previously set up a secure shell passphrase, go to Step 4.
- 4 If a prompt to **Enter Passphrase for key '<user@localhost>'** appears, type your *Passphrase* and then press the **Return/Enter** key. Go to Step 5.
- 5 At the `<user@remotehost>'s password:` prompt, type your *Password* and then press the **Return/Enter** key.
- 6 To log in as root type `su` then press the **Return/Enter** key.
 - A password prompt is displayed.
- 7 Type the *RootPassword* then press the **Return/Enter** key.
 - You are authenticated as root and returned to the UNIX prompt.
- 8 To set the display to the current terminal type `setenv DISPLAY <IPNumber>:0.0` or `setenv DISPLAY BackupServerName:0.0` then press the **Return/Enter** key.
- 9 To log in as the user type: `su UserID` then press the **Return/Enter** key.
 - You are authenticated as the owner of the file(s) to be restored.
- 10 To set the display to the current terminal type `setenv DISPLAY IPNumber:0.0` or `setenv DISPLAY MachineRestored:0.0` then press the **Return/Enter** key.

11 To execute the Networker Administrator program type **nwadmin** then press the **Return/Enter** key.

- A window opens for the Networker Administrator program (Figure 3.14-5).
- You are now able to perform restores of partitions.



Figure 3.14-5. Networker Administrator's Window

- 12 Select **Save Set** → **Recover Set** from the pull-down menu.
 - The **Save Set Recover** window opens.
- 13 Select the **Name of system to be restored** (referred to as **System** in the rest of this procedure) in the **Client** field's menu.
 - The **Save Set** listing updates. This is a listing of partitions on the **System**.
 - At this time, note the partitions listed for the **System**. To do a complete system restore, this procedure needs to be performed for each partition listed.
- 14 Select the **Save Set**/partition from the listing.
 - The **Instance** listing updates.
- 15 Select the appropriate **Instance**.
 - An **Instance** is a particular Networker client backup. A listing of **Instances** is a report detailing the Networker client backups that have occurred.
 - Select an **Instance** based upon the **Date from which to restore** (referred to as **Date** in the rest of this procedure) and of an appropriate level:
 - To determine a base **Date**, you must consider the time of day that backups occur. For example, if the backup occurs at 02:00 each morning then a system corrupted at noon on June 6 would require a restoration of the June 6 backup. However, if the system corruption took place around the time of the backup, it would be more prudent to use the backup from June 5.
 - If the backups are full or incremental, perform the following actions:
 - Select the most recent full backup that occurred on or prior to the **Date** and perform a partition restore. If the date of this full backup is not the same as the **Date**, perform a partition restore using each incremental backup, in chronological order, between this full backup and the day after the **Date**.
 - If the backups are of different numerical levels, follow these steps:
 - First select the most recent level 0/full backup prior to or on the **Date** and perform a restore of the partition. If a level 0/full backup did not occur on the **Date**, select the most recent backup of the next highest level occurring after this level 0 and prior to or on the **Date**.
 - Perform a restore of the partition. Continue to select the most recent backup of the next highest level occurring between the last used **Instance** and the day after the **Date** until reaching an instance on the **Date**.
 - You can double click an **Instance** to see which tape is required.
- 16 Click on the **Recover** button.
 - The **Save Set Recover Status** window opens.

- To show which tapes are required click on the **Volumes** button.
 - 17 Click on the **Options** button.
 - The **Save Set Recover Options** window opens.
 - 18 Set Duplicate file resolution to Overwrite the existing file by clicking its radio button.
 - 19 Make sure that the **Always prompt** checkbox is **not** checked.
 - 20 Click on the **OK** button.
 - The **Save Set Recover Options** window closes.
 - 21 Click on the **Start** button in the **Save Set Recover Status** window.
 - Status messages appear in the **Status** box.
 - A **recovery complete** message appears when recovery is complete.
 - 22 Click on the **Cancel** button after the **recovery complete** message appears.
 - The **Save Set Recover Status** window closes.
 - 23 If additional partition restores are required, go to Step 12. Otherwise, select **File → Exit** from the pull-down menu to quit the Networker Administrator program.
 - 24 At the UNIX prompt for the backup server, type **exit** then press the **Return/Enter** key.
 - 25 Type **exit** again then press the **Return/Enter** key.
-

3.15 User Administration

3.15.1 Screening Personnel

Table 3.15-1 contains the activity checklist for User Administration.

Table 3.15-1. User Administration - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|--|--------------|-----------|
| 1 | SA | Checking File/Directory Access Privileges | (P) 3.15.8.1 | |
| 2 | SA | Changing a File/Directory Access Privilege | (P) 3.15.9.1 | |

3.15.1.1 Screening Criteria

Some positions require special access privileges in order to do the assigned job or duties. These are called public trust positions because they can affect the integrity, efficiency, or effectiveness of the system to which they have been granted privileged access. Screening for suitability, prior

to being granted access, is required. This screening, National Agency Check (NAC), is required to ensure that granting any special access privileges to someone would not cause undue risk to the system for which that employee has these privileges. Line Management is responsible for requesting suitability screening for the employees in their respective organizations.

OMB Circular A-130, Appendix III and NPR 2810.1 require the following employees to undergo personnel screening:

- All employees who require privileged access or limited privileged access to a Federal computer system or network.
- Privileged access – Can bypass, modify, or disable the technical or operational system security controls.
- Limited privileged access – Can bypass, modify or disable security controls for part of a system or application but not the entire system or application.

Internet Protocol Operational Network (IONet) Access Protection Policy and Requirements (290-004) requires the following employees to undergo suitability screening:

- All employees who require privileged access, limited privileged access, or access to the Closed Segment of the Internet Protocol Operational Network (IONet) (formerly NASCOM).
- All employees having access to IONet network control devices.

NPR 1600.1 requires that all employees granted unescorted access to a NASA Resource Protection (NRP) facility or area and/or a NASA-designated Limited Area undergo screening.

3.15.2 Screening Procedures

The line manager will submit NASA Form 531 containing the following information for each employee needing suitability screening.

- Full name (first, middle initial and last)
- Goddard badge number if badged employee
- Reason for requesting screening
- Type and date of any previous security investigation or clearance if known
- Phone number and email address

The request should be sent to the EDF Security Administrator. The GSFC Security Office (GSO) will search the personnel security database to determine if a current NAC has been performed. If not the employee will be contacted to obtain additional information. The GSO will report a favorable or unfavorable result back to the EDF Security Administrator upon completion of the suitability screening.

3.15.3 Adding a New User

Adding a user to the system is accomplished through a series of steps that may be performed as a suite from the command line or by use of a script. The procedure below outlines the individual steps that are required to completely set up a new user on the system. The scripts will accomplish these steps in an interactive manner.

The requester fills out a User Registration Request Form and submits it to the requestor's supervisor. The requester's supervisor reviews the request, and if s/he determines that it is appropriate for the requester to have an account, forwards the request to the System Administrator. If the requester requires a National Agency Check (NAC) before access is granted, the supervisor will forward the request to the Security System Engineer, who will then ensure that proper procedures are followed before the request is sent to the System Administrator (SA). The System Administrator verifies that all required information is contained on the form. If it is, s/he forwards the request to the approval authority, the DAAC Manager. Incomplete forms are returned to the requester's supervisor for additional information. If the request for the accounts fits within policy guidelines, the DAAC Manager approves the request and returns the request form to the System Administrator to implement.

The System Administrator should be familiar with a UNIX text editor and the files **/etc/passwd.y** (Figure 3.15-1), **/etc/group** (Figure 3.15-2), and **/etc/auto.home**.

The System Administrator (SA) creates a new user account with command-line/script entries. As an example, The Goddard Space Flight Center DAAC uses a script, *Newuser*, to add new users to the system. The script, which is available to other DAACs, walks the System Administrator through data input of user information, checks for the same user in other systems, creates a User ID, synchronizes password files and creates home directories for new users.

3.15.4 Deleting a User

The Deleting a User process begins when the requester has determined that no useful files remain in the user's home directory and submits a request to delete the user's account to his/her supervisor. The supervisor approves or denies the request. Once approved, the request is forwarded to the OPS Super. The OPS Super reviews the request and forwards it to the SA who deletes the user's account. When the user has been deleted, the SA notifies the requester, supervisor and OPS Super.

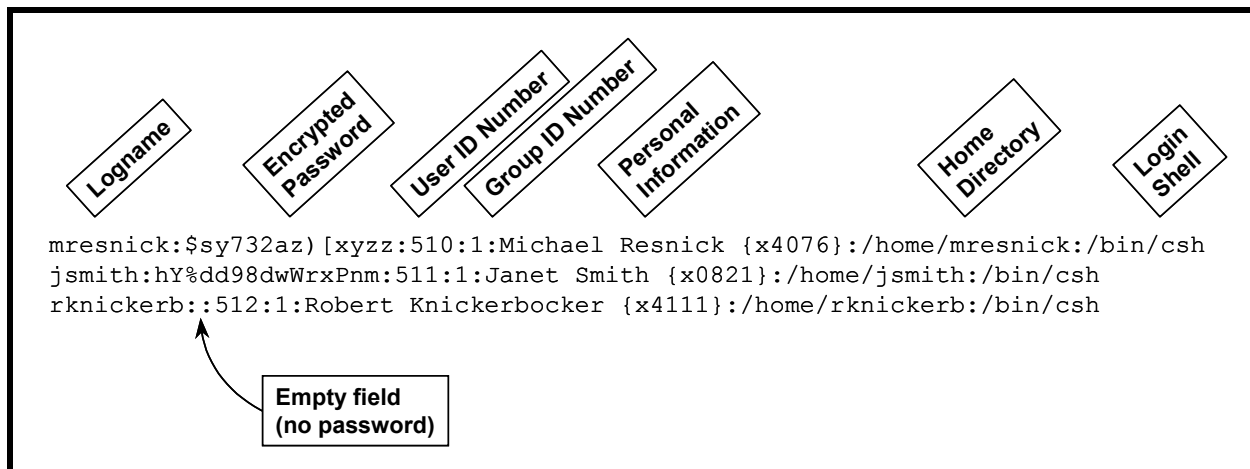


Figure 3.15-1. /etc/passwd.y File Fields

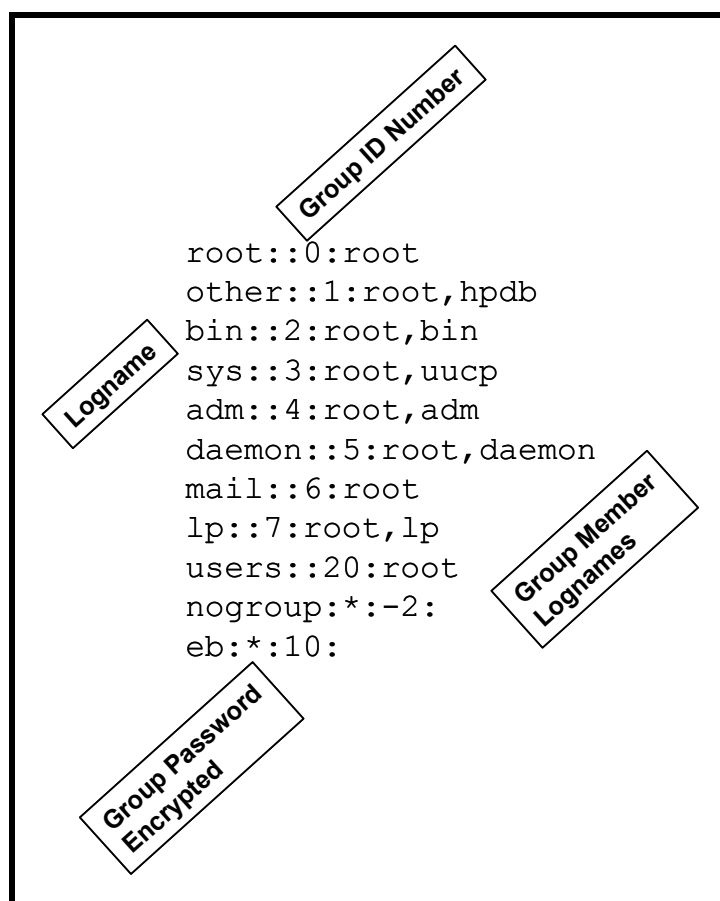


Figure 3.15-2. /etc/group File

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for deleting a user has already been approved by DAAC Management. In order to perform the procedure, the SA must have obtained the following information from the requester:

- **UNIX login of the user to be deleted**
- **Role(s) of the user to be deleted**

The System Administrator deletes a user with command-line/script entries. As an example, The Goddard Space Flight Center DAAC uses a script, *Lockdown*, to lock, unlock and delete user accounts. This script, which is available to other DAACs, walks the System Administrator through the steps necessary to delete a user account. It assists the System Administrator in locating the correct user account for deletion and deletes the user account and all associated file references. It also enables the System Administrator to lock or unlock accounts.

3.15.5 Changing a User's Account Configuration

Account configuration is accomplished through command line and script. The DAAC manager must authorize changes to user accounts.

The Changing a User Account Configuration process begins when the requester submits a request to the OPS Super detailing what to change about the account configuration and the reason for the change. Requests for changes to privileged accounts shall be sent to the Security System Engineer. The OPS Supervisor or the Security System Engineer reviews the request and forwards it to SA who changes the user's account configuration. When the changes are complete the SA notifies the requester and OPS Supervisor.

In order to perform the procedure, the System Administrator must have obtained the following information from the requester:

- What to change and new settings. Can be any of:
 - New Real User Name
 - New Office Number
 - New Office Phone Number
 - New Home Phone Number
 - New UNIX Group
 - New Login Shell
- Current UNIX Login of the User

3.15.6 Changing User Access Privileges

The Changing User Access Privileges process begins when the requester submits a request to his/her supervisor. Requests for changes to privileged accounts shall be sent to the Security

System Engineer. The supervisor or the Security System Engineer approves or denies the request. Once approved, the request is forwarded to the OPS Super. The Ops Super reviews the request and forwards it to the SA who changes the user's access privileges. When the changes are complete the SA notifies the requester, supervisor and Ops Super.

In order to perform the procedure, the System Administrator must have obtained the following information about the requester:

- Role(s) to which the user is to be added
- Role(s) from which the user is to be removed
- UNIX login of the user

3.15.7 Changing a User Password

The Changing a Users Password process begins when the requester submits a request to the SA. The System Administrator verifies that the requester is who s/he claims to be. Once verified, the SA changes the user's password. When the change is complete the SA notifies the requester.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing a user password has already been approved by DAAC Management. In order to perform the procedure, the SA must have obtained the following information about the requester:

- UNIX login of the user
- New password for the user

To change a user password for the requester, execute the command line or script procedure steps that have been developed.

3.15.8 Checking a File/Directory Access Privilege Status

3.15.8.1 Checking File/Directory Access Privileges

- 1 At a UNIX prompt, type **cd *Path*** then press the **Return/Enter** key.
 - The ***Path*** is the full path up to but not including the file/directory on which access privilege status is needed. For example, if the requester wants access privileges status on directory /home/jdoe, type **cd /home** then press the **Return/Enter** key.
- 2 From the UNIX prompt, type **ls -la**. The output from the command should appear as follows:

| | | | | | | |
|------------|----|----------|----------|-------|--------------|----------|
| drwxrwxrwx | 3 | mresnick | training | 8192 | Jun 14 08:34 | archive |
| drwxr-xr-x | 11 | mresnick | training | 4096 | Jul 03 12:42 | daacdata |
| -rw-rw-rw- | 1 | mresnick | training | 251 | Jan 02 1996 | garbage |
| lrw-r--r-- | 2 | jjones | admin | 15237 | Apr 30 20:07 | junk |
| -rwxr--rw- | 1 | mresnick | training | 5103 | Oct 22 1994 | trash |

- The first column of output is the file access permission level for the file (see Figure 33 below for a description of file permissions).
 - The next column to the right is the number of links to other files or directories.
 - The third column is the file owner's user ID
 - The fourth column is the group membership of that owner.
 - The fifth column shows file size in bytes.
 - The sixth column displays the date and time of last modification (if the date is more than six months old, the time changes to the year)
 - The last column displays the file name.
-

3.15.9 Changing a File/Directory Access Privilege

File and directory access privileges are displayed in the first output column of the **ls -l** command and consist of ten characters, known as **bits**. Each bit refers to a specific permission. The permissions are divided into four groupings shown and briefly described in Figure 3.15-3.

In order to perform the procedure, the System Administrator must have obtained the following information about the requester:

- Full path of the file/directory on which access privileges will be changed.
- New access privileges to set on the file/directory. Can be any of:
 - New owner
 - New group
 - New user/owner privileges (read, write and/or execute)
 - New group privileges (read, write and/or execute)
 - New other privileges (read, write and/or execute)

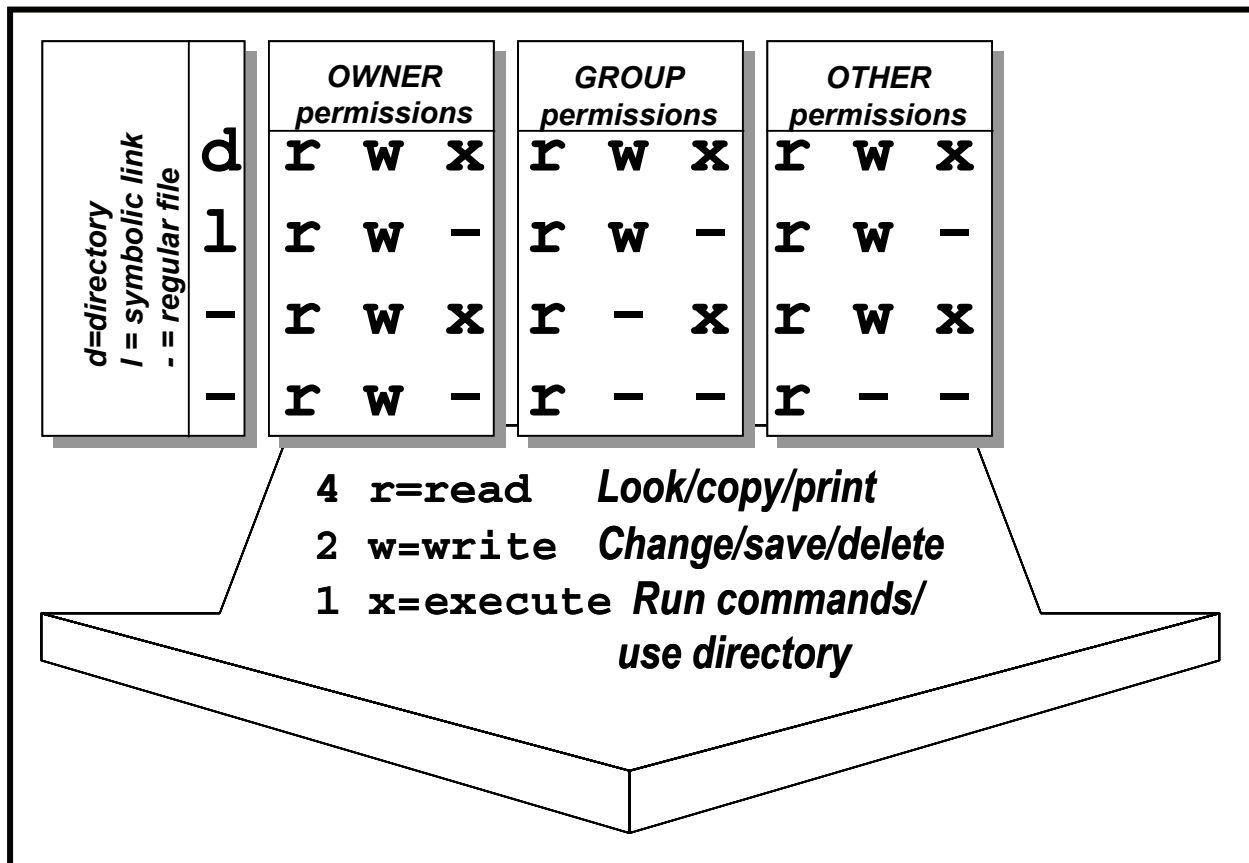


Figure 3.15-3. Access Permissions

3.15.9.1 Changing a File/Directory Access Privilege

- 1 At the UNIX prompt type **su** then press the **Return/Enter** key.
- 2 At the **Password** prompt, type **RootPassword** then press the **Return/Enter** key.
 - Remember that **RootPassword** is case sensitive.
 - You are authenticated as root.
- 3 Type **cd Path** then press the **Return/Enter** key.
 - The **Path** is the full path up to but not including the file/directory on which access privileges will be changed. For example, if the requester wants access privileges changed on directory /home/jdoe type **cd /home** then press the **Return/Enter** key.

- 4 If there is a **New owner** then type **chown *NewOwner FileOrDirectoryName*** then press the **Return/Enter** key.
- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe type **chown *NewOwner jdoe*** then press the **Return/Enter** key.
- 5 If there is a **New group** then type **chgrp *NewGroup FileOrDirectoryName*** then press the **Return/Enter** key.
- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe type **chgrp *NewGroup jdoe*** then press the **Return/Enter** key.
- 6 If there are **New user/owner privileges** type **chmod *u=NewUserPrivileges FileOrDirectoryName*** then press the **Return/Enter** key.
- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe type **chmod *u=NewUserPrivileges jdoe*** then press the **Return/Enter** key.
 - The ***NewUserPrivileges*** are “r” for read, “w” for write, and “x” for execute. For example, to give the user/owner read, write and execute privileges, type **chmod *u=rwx FileOrDirectoryName*** then press the **Return/Enter** key.
- 7 If there are **New group privileges** type **chmod *g=NewGroupPrivileges FileOrDirectoryName*** then press the **Return/Enter** key.
- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe type **chmod *g=NewGroupPrivileges jdoe*** then press the **Return/Enter** key.
 - The ***NewGroupPrivileges*** are “r” for read, “w” for write, and “x” for execute. For example, to give the group read and execute privileges, type **chmod *g=rx FileOrDirectoryName*** then press the **Return/Enter** key.
- 8 If there are **New other privileges** then type **chmod *o=NewOtherPrivileges FileOrDirectoryName*** then press the **Return/Enter** key.
- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe type **chmod *o=NewOtherPrivileges jdoe***, then press the **Return/Enter** key.

- The *NewOtherPrivileges* are “r” for read, “w” for write, and “x” for execute. For example, to give others read privileges, type **chmod o=r *FileOrDirectoryName*** then press the **Return/Enter** key.

9 Type **exit** then press the **Return/Enter** key.

- Root is logged out.
-

3.15.10 Moving a User’s Home Directory

The process of moving a user's home directory begins when the requester submits a request to the Ops Supervisor. The Ops Supervisor approves or denies the request. Once approved, the request is forwarded to the SA who moves the user’s home directory. When the changes are complete the SA notifies the requester and Ops Supervisor.

3.16 Commercial Off-the-Shelf (COTS) Software Administration

The EMD organization provides maintenance for EMD hardware, software, and firmware systems delivered under the EMD contract to the EMD sites.

Commercial off-the-shelf (COTS) software and hardware are maintained in accordance with the current *EMD COTS Deployment Plan*, (335-EMD-series document). The project maintenance philosophy for software is to provide EMD centralized support for developed items and vendor support for COTS software.

3.16.1 Installation

EMD Project software consists of COTS, custom-developed, and science software.

Software maintenance includes:

- Right to us COTS software products..
- Access to software vendor telephone support
- Access to vendors on-line and email support
- Receive patches and upgrades
- The DAAC maintenance activity includes: software configuration management (CM) including support for change control, configuration status accounting, audit activities, and software quality assurance (QA). Each site is the CM authority over its own resources subject to ESDIS delegation of roles for EMD management.

3.16.2 LOG FILES

Log files must be maintained documenting all COTS installations and modifications. These files delineate manufacturer, product, installation date, modification date and all other pertinent configuration data available.

3.16.3 COTS Configuration

The COTS software upgrades are subject to CCB approval before they may be loaded on any platform. EMD Sustaining Engineering notifies the CCB of the upgrade that has been received. The COTS SW Librarian distributes the COTS software upgrade as directed by the CCB. The site Software Maintenance Engineer, Network Administrator, and the System Administrator are responsible for upgrading the software on the host machine and providing follow-up information to the Configuration Management Administrator (CMA. The site Local Maintenance Coordinator will notify the appropriate personnel (Release Installation Team, System Administrator, Network Administrator, Software Maintenance Engineer) when the COTS software is received and approved by the CCB for installation.

COTS software patches may be provided by the COTS software vendor in response to a DAAC's call requesting assistance in resolving a COTS software problem. The problem may or may not exist at other locations. When a COTS software patch is received directly from a COTS software vendor (this includes downloading the patch from an on-line source), the DAAC's CCB will be informed via CCR prepared by the requesting Operator, System Administrator, Network Administrator, or site Software Maintenance Engineer. It is the responsibility of the Operator, System Administrator, Network Administrator, or site Software Maintenance Engineer to notify the CCB of the patch's receipt, purpose, and installation status and to comply with the CCB decisions. The Operator, System Administrator, Network Administrator, or site Software Maintenance Engineer installs COTS software patches as directed by the CCB.

In addition to providing patches to resolve problems at a particular site, the software vendor will periodically provide changes to COTS software to improve the product; these changes are issued as part of the software maintenance contract. Upgrades are issued to licensees of the basic software package. Therefore, the COTS software upgrades will be shipped to the ILS Property Administrator (PA), who receives and enters them into inventory.

3.17 Security

System security architecture must meet the requirements for data integrity, availability, and confidentiality. Security Services meet these requirements by incorporating a variety of mechanisms to establish and verify user accounts, issue and verify passwords, audit user activity, and verify and protect data transfer. To monitor and control access to network services, Security Services use the public domain tool, TCP Wrappers (Note: All DAACs, except for NSIDC do not use TCP Wrappers). Other public domain COTS products — ANLpasswd and Crack— provide additional password protection for local system and network access. The tool Tripwire monitors changes to files and flags any unauthorized changes.

This section defines step-by-step procedures for System Administrators to run the Security Services tools. The procedures assume that the requester's application for a Security process has already been approved by DAAC Management.

3.17.1 Generating Security Reports

Table 3.17-1 contains the activity checklist for Security.

Table 3.17-1. Security - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|--------------------|--------------|-----------|
| 1 | SA | User Activity Data | (P) 3.17.1.1 | |

A log is created to keep track of unsuccessful attempts to log into the computer. After a person makes five consecutive unsuccessful attempts to log in, all these attempts are recorded in the file `/var/adm/loginlog`. The procedures assume that the file has been created and the operator has logged on as root.

3.17.1.1 User Activity Data

- 1 At the UNIX prompt type `/usr/bin/logins [-admopstux] [-g group...] [-l login...]` then press the **Return/Enter** key.
 - **-a** Adds two password expiration fields to the display. The fields show how many days a password can remain unused before it automatically becomes inactive, and the date that the password will expire.
 - **-d** Selects logins with duplicate uids.
 - **-m** Displays multiple group membership information.
 - **-o** Formats output into one line of colon-separated fields.
 - **-p** Selects logins with no passwords.
 - **-s** Selects all system logins.
 - **-t** Sorts output by login instead of by uid.
 - **-u** Selects all user logins.
 - **-x** Prints an extended set of information about each selected user. The extended information includes home directory, login shell and password aging information, each displayed on a separate line. The password information consists of password status (“PS” for password, “NP” for no password or “LK” for locked). If the login is passworded, status is followed by the date the password was last changed, the number of days required between changes, and the number of days allowed before a change is required. The password aging information shows the time interval that the user will receive a password expiration warning message (when logging on) before the password expires.
 - **-g group** Selects all users belonging to group, sorted by login. Multiple groups can be specified as a comma-separated list. When the **-l** and **-g** options are combined, a user will be listed only once, even if the user belongs to more than one of the selected groups.

- **-l login** Selects the requested login. Multiple logins can be specified as a comma-separated list. Depending on the nameservice lookup types set in `/etc/nsswitch.conf`, the information can come from the `/etc/passwd` and `/etc/shadow` files and other nameservices. When the **-l** and **-g** options are combined, a user will be listed only once, even if the user belongs to more than one of the selected groups.
- 2 Type **logins -x -l username** then press the **Return/Enter** key.
 - Displays login status for a user.
 - 3 Type **/var/adm/loginlog** then press the **Return/Enter** key.
 - To enable login Logging, this creates the log file **loginlog**.
 - 4 Type **chmod 600 /var/adm/loginlog** then press the **Return/Enter** key.
 - This sets read and write permissions for root on the file.
 - 5 Type **chgrp sys /var/adm/loginlog** then press the **Return/Enter** key.
 - This sets the group to **sys**.
-

3.17.1.1 User Audit Trail Information

The **audit_startup** script is used to initialize the audit subsystem before the audit daemon is started. This script is configurable by the System Administrator, and currently consists of a series of **auditconfig** commands to set the system default policy, and to download the initial events to class mapping. Type the following command to initialize the audit subsystem:

/etc/security/audit_startup

The audit command is the general administrator's interface to the audit trail. The audit daemon may be notified to read the contents of the `audit_control` file and re-initialize the current audit directory to the first directory listed in the `audit_control` file or to open a new audit file in the current audit directory specified in the `audit_control` file as last read by the audit daemon. The audit daemon may also be signaled to close the audit trail and disable auditing. The audit commands are input as shown:

3.17.1.2 Audit Commands

audit -n then press the **Return/Enter** key.

- Signals audit daemon to close the current audit file and open a new audit file in the current audit directory.

audit -s then press the **Return/Enter** key.

- Signals audit daemon to read the current audit file. The audit daemon stores the information internally.

audit -t then press the **Return/Enter** key.

- Signals audit daemon to close the current audit file, disable audit and die.

praudit -sl *filename* then press the **Return/Enter** key.

- Displays audit output. The print audit command converts the binary audit records into a variety of formats, depending on the options used with the commands. The format of audit files is included in the file `/usr/include/sys/audit.h`. By default, user IDs (UID) and group IDs (GID) are converted to their ACSII representation.

This page intentionally left blank.

4. Database Administration

4.1 System Overview

The general system design of the Database Administration system is to receive data from external sources; save data in either long-term or permanent storage; produce from the data higher-level data products; and provides data access support to scientist and other registered clients.

4.1.1 Information Model

The Earth Science Information Model characterizes earth science data as a data pyramid consisting of broad, multi-layered data categories as shown in Figure 4.1-1. Logical collections of data, based on their expected relationships, are developed to capture the variability in remote sensing instruments, science disciplines, and other characteristics of the earth science community. For example, some products have related properties (e.g., cloud type and cloud drop size) while other products are dissimilar (e.g., land vegetation indices and ocean productivity), which suggest certain logical groupings. Characteristics are often similar across a particular science discipline and across products generated from a given instrument but different among the various provider sites because of differing science disciplines focus and organizational autonomy.

Metadata. *Metadata are data about data that are provided to the system by the external data provider or the generating algorithm.* They describe characteristics of data origin, content, format, quality, and condition. They also provide information to process and interpret data. Metadata are required for access to all data in the system.

An earth science metadata model supports the data standardization necessary for total system interoperability within a heterogeneous, open systems environment. (Refer to the latest version of the *Earth Science Data Model*; e.g., 420-EMD-001, Implementation Earth Science Data Model for the EMD Project.) The data model includes diagrams that illustrate the relationships of classes, the attributes contained within the classes, the characteristics of the relationships between classes, and the attribute specifications.

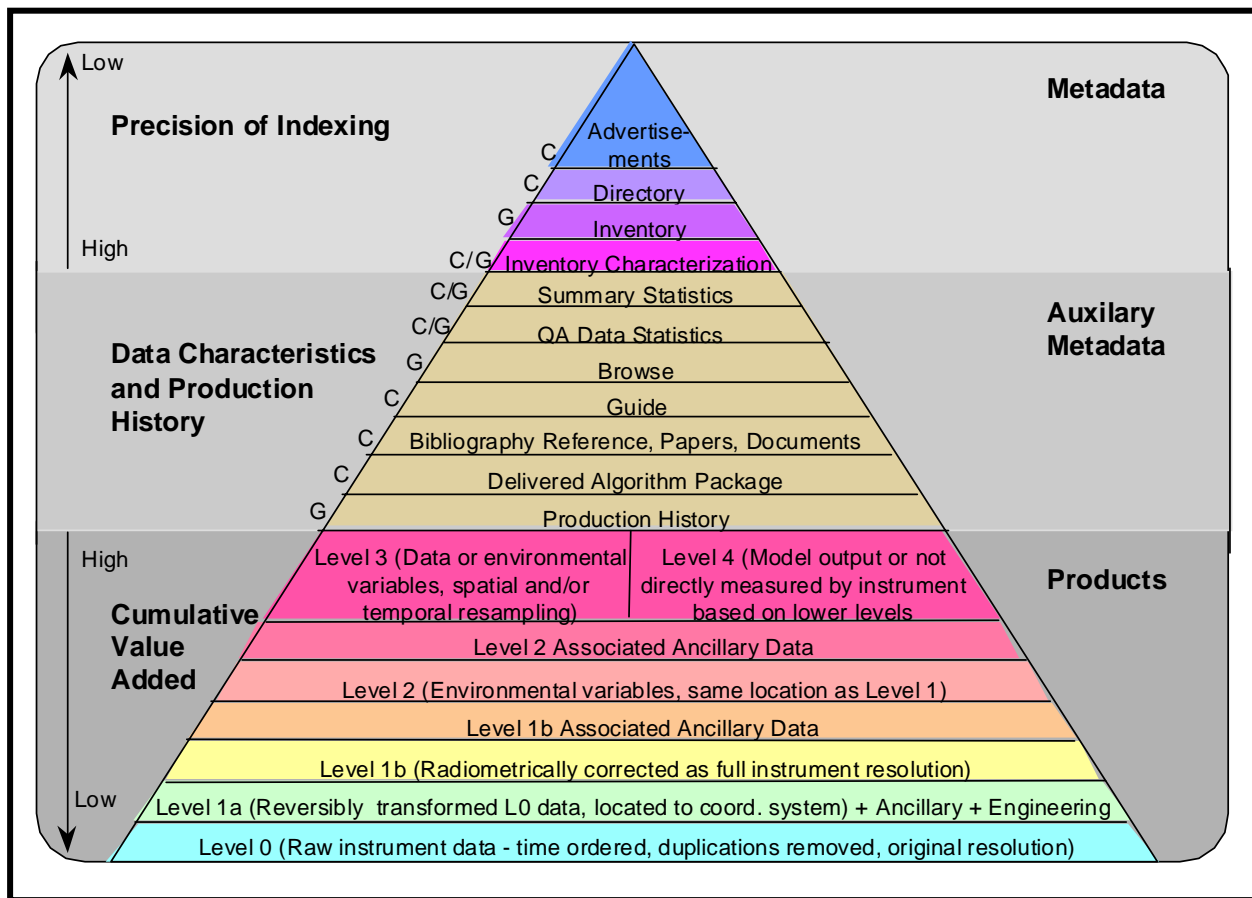


Figure 4.1-1. Earth Science Information Model

Attributes are descriptors of data populating searchable database fields, enabling finite classification of data residing in the system. Attributes can either be collection-level or granule-level attributes and either core or product-specific attributes. A collection is a grouping of related science data. A granule is the smallest aggregation of data that is independently managed (i.e., ingested, processed, stored, or retrieved) by the system. The majority of attributes in the data model are collection-level attributes, which means that they apply to all granules in the collection.

Data Products. *Data products are a processed collection of one or more parameters packaged with associated ancillary and labeling data and formatted with uniform temporal and spatial resolution, e.g., the collection of data distributed by a data center or subsetted by a data center for distribution.* There are two types of data products:

- Standard, which is a data product produced at a DAAC by a community consensus algorithm for a wide community of users.
- Special, which is a data product produced at a science computing facility by a research algorithm for later migration to a community consensus algorithm and can be archived and distributed by a DAAC.

Data products are categorized by levels, which are described in shown in Figure 4.1-2 and described in Table 4.1-1.

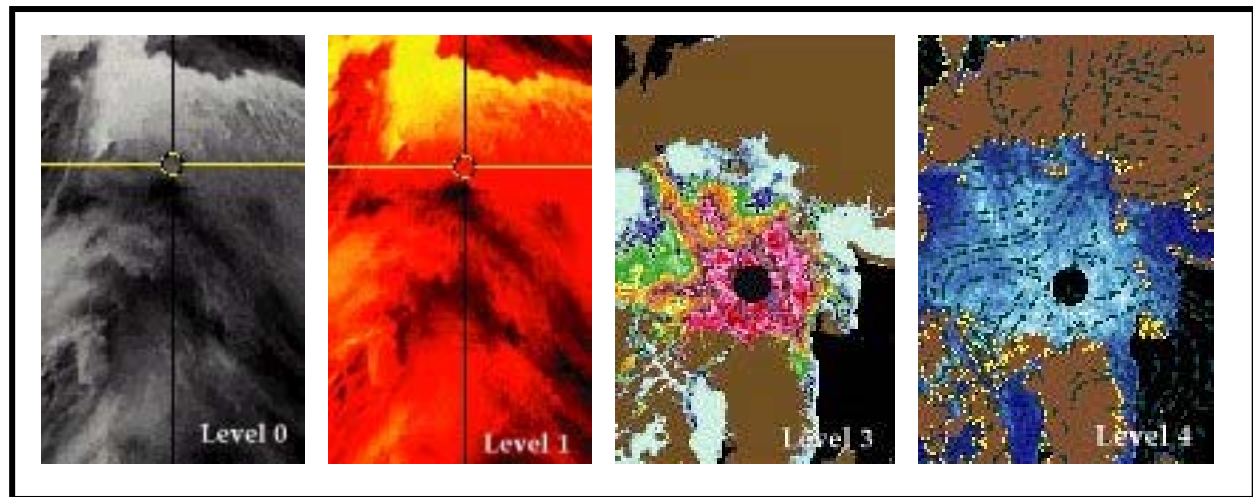


Figure 4.1-2. An Example of Data Product Levels

Table 4.1-1. Data Product Level Definitions

| Level | Definition |
|-------|--|
| 0 | Reconstructed, unprocessed instrument/payload data at full resolution; any and all communications artifacts (e.g., synchronization frames, communications headers, duplicate data removed) |
| 1A | Reconstructed unprocessed instrument data at full resolution, time-referenced, and annotated with ancillary information, including radiometric and geometric calibration coefficients and geo-referencing parameters (e.g., platform ephemeris computed and appended but no applied to the Level 0 data) |
| 1B | Level 1A data that have been processed to sensor units (not all instruments will have a Level 1B equivalent) |
| 2 | Derived geophysical variables at the same resolution and location as the Level 1 source data |
| 3 | Derived geophysical variables mapped on uniform space-time grid scales, usually with some completeness and consistency |
| 4 | Model output or results from analyses of lower-level data (e.g., variables derived from multiple measurements) |

4.1.2 Subsystems

The system is comprised several subsystems, see table 4.1-2. More detailed information can be found in the *Segment/Design Specification for the EMD Project* (305-EMD-100). The primary functions of the remaining subsystems can be grouped into the following four categories:

- **Data Ingest.** Ingest is accomplished by means of the Data Pool-Ingest Subsystem (DPL), which interfaces with external applications and provides data staging capabilities and storage for an approximately 1-year buffer of Level 0 data so that reprocessing can be serviced from local storage.
- **Data Storage and Management.** Data storage and management is provided by the Data Server Subsystem (DSS), which can archive science data, search for and retrieve archived data, manage the archives, and stage data resources needed as input to science software or resulting as output from their execution. The Data Server Subsystem provides access to earth science data in an integrated fashion through an application programming interface (API) that is common to all layers.
- **Information Search and Data Retrieval.** Search and retrieval is accomplished by the science user interface functions in the Client Subsystem (CLS), and by information search support functions in the Data Management Subsystem (DMS).

Table 4.1-2. Subsystem Functions (1 of 2)

| Subsystem | | Functions |
|--------------------|-----|---|
| Client | CLS | The client part of the client-server access paradigm through graphical user interface and data/service access tools, as well as application program interface (API) libraries to system services |
| Internetworking | ISS | Provides networking services based on protocols and standards corresponding to the lower four layers of the Open Systems Interconnection (OSI) reference model: the transport layer's TCP and UDP protocol, the network layer's IP protocol, and the physical/data link layer's Ethernet, FDDI, and Gigabit Ethernet protocols. |
| Data Management | DMS | System wide distributed search and access services with multiple science discipline views of data collections and "one-stop shopping" with location transparent access to those services and data. |
| Data Server | DSS | Locally optimized search, access, archive and distribution services with a science discipline view of data collections and an extensible Earth Science Data Type and Computer Science Data Type view of the archive holdings |
| DPL Ingest Service | DPL | Clients for importing data (science products, ancillary, correlative, documents, etc.) into system data repositories (data servers) on an <i>ad hoc</i> or scheduled basis and deals with external system interfaces |

Table 4.1-2. Subsystem Functions (2 of 2)

| Subsystem | | Functions |
|-----------------------------|-----|--|
| Management | MSS | Functions for system startup/shutdown, resource management, performance monitoring, error logging, system and science software configuration management, and resource accounting |
| Communications | CSS | The distributed computing infrastructure that enables intra- and inter-site communications between the subsystems. From a scientist user's perspective, the system infrastructure appears as services, and interfaces to services, which are displayed on the user's workstation desktop. This perspective is similar to the view of the World Wide Web (WWW) servers as seen through a local client such as Netscape. |
| Data Pool Ingest | DPL | Provides on-line access for browsing and FTP download of selected granules, metadata, and browse data. |
| Spatial Subscription Server | SSS | Permits creation and management of subscriptions for data distribution/notification and Data Pool insert |
| Order Manager | OMS | Manages orders from EDG and other sources and either distributes the data through the Data Pool (either electronically or on hard media) or dispatches requests to appropriate system services (e.g., SDSRV, PDS). |

4.1.3 Databases

Custom Databases. The custom databases described in Table 4.1-3 encompass the majority of the subsystem persistent data requirements. Other data requirements are met through the use of flat files, which are described below. With the exception of the PDS databases, which are implemented using Oracle, all custom databases are implemented using Sybase.

Table 4.1-3. Custom Databases (1 of 3)

| Database Name | Document Number | DB Software | Logical Categories |
|---------------------------------------|-----------------|-------------|------------------------------|
| Science Data Server Subsystem (SDSRV) | 311-EMD-101 | Sybase | Database Version Information |
| | | | System Management Data |
| | | | Collection, Granule Metadata |
| | | | DAP Metadata |
| | | | Spatial Metadata |
| | | | Data Originator Metadata |
| | | | Granule Metadata |
| | | | Contact Metadata |
| | | | Collection Metadata |
| | | | Temporal Metadata |
| | | | Planning Data |
| | | | Data Processing Data |

Table 4.1-3. Custom Databases (2 of 3)

| Database Name | Document Number | DB Software | Logical Categories |
|---|-----------------|-------------|------------------------------|
| Storage Management and Database Distribution Subsystems (STMGT & DDIST) | 311-EMD-102 | Sybase | Database Version Information |
| | | | Data Distribution |
| | | | Archive Services |
| | | | Request Handling |
| | | | Server Configuration |
| | | | Cache Management |
| | | | Media Operations |
| | | | FTP Services |
| | | | Staging Disk Operations |
| | | | GR Cleanup |
| Ingest Subsystem (INS) | 311-EMD-100 | Sybase | Database Version Information |
| | | | Datatype Information |
| | | | Configuration Data |
| | | | Active Requests |
| | | | Validation Data |
| | | | Table Locking Information |
| Systems Management Subsystem (MSS) | 311-EMD-103 | Sybase | Database Version Information |
| | | | Order Information |
| | | | Site Information |
| | | | Validation Data |
| | | | User Data |
| Data Pool (DPL) | 311-EMD-106 | Sybase | Collection Metadata |
| | | | Granule Metadata |
| | | | Insert Action Data |
| Order Manager Server (OMS) | 311-EMD-104 | Sybase | Queue/Status Information |
| | | | Request Information |
| | | | Intervention Information |

Table 4.1-3. Custom Databases (3 of 3)

| Database Name | Document Number | DB Software | Logical Categories |
|-----------------------------------|-----------------|-------------|------------------------------|
| Spatial Subscription Server (SSS) | 311-EMD-105 | Sybase | Database Version Information |
| | | | Subscription Information |
| | | | Event Information |
| | | | Action Information |

4.1.4 Commercial Off-the-Shelf (COTS) Databases

There are several important databases resident in system COTS product. Remedy and TestTrack Pro provides a means of reporting, classifying, and tracking defects. Remedy is being used, in this capacity within a limited client environment. XRP-II is a baseline manager used to maintain records of baselined operational system configurations. Database descriptions can be obtained by consulting the relevant vendor documentation.

4.1.5 Flat Files

A flat file is an operating system file that is read and written serially. Flat file data are fairly static and have no explicit relationship to other data in the enterprise. There are cases when the implementation of certain persistent data is better suited to a flat file than to a database, e.g., system configuration data, external interface data, log files. Flat files used in the system are described in Table 4.1-4.

Table 4.1-4. Flat Files (1 of 2)

| Database | Flat File Attributes | | | |
|---------------|----------------------|--|---|---|
| | Usage | Types | Formats | Descriptions |
| TestTrack Pro | Yes | Linux flat file | Variable length | Log files, configuration files; portability |
| SDSRV | Yes | UNIX flat file; ELF 32-bit MSB dynamic lib SPARC Version 1, dynamically linked | Variable length, Dynamic Link Library (DLL) | Log files, configuration files, template used to validate ESDTs on installation, uniquely named ESDT file descriptors, generic to ESDT-specific processing capabilities |
| DMS | Yes | UNIX flat file | Variable length | Log files, configuration files |
| STMGT & DDIST | Yes | UNIX flat file | Variable length | Disk index files, staging data information, resource lists |
| INS | Yes | UNIX flat file | Variable length | Log files, configuration files, data delivery records |
| REGIST | No | | | |

Table 4.1-4. Flat Files (2 of 2)

| Database | Flat File Attributes | | | |
|----------|----------------------|---------------|---|---|
| | Usage | Types | Formats | Descriptions |
| MSS | Yes | ASCII, binary | Single line records, one/two fields; EcAgEvent objects; MsAgMgmtHandle object; integers; string lists | Accountability component files, subagent component files |
| NM | No | | | |
| DPL | Yes | ASCII | Variable length | For Data Pool Access Statistics Utility, temporary storage of data to be exported to database |
| OMS | No | | | |
| SSS | No | | | |

4.1.6 Resident Databases

Table 4.1-5 shows the custom and COTS databases that are resident at the SMC and the DAACs. Each resident database is individually installed and maintained.

Table 4.1-5. Resident Databases

| Databases | SMC | DAAC | | |
|---|-----|----------------------------|---------|-------|
| | | LaRC | LP DAAC | NSIDC |
| Custom | | | | |
| Science Data Server Subsystem (SDSRV) | | ✓ <input type="checkbox"/> | ✓ | ✓ |
| Data Management Subsystem (DMS) | ✓ | ✓ <input type="checkbox"/> | ✓ | ✓ |
| Storage Management and Database Distribution Subsystems (STMGT & DDIST) | | ✓ <input type="checkbox"/> | ✓ | ✓ |
| Registry (REGIST [MSS]) | ✓ | ✓ <input type="checkbox"/> | ✓ | ✓ |
| Systems Management Subsystem (MSS) | ✓ | ✓ <input type="checkbox"/> | ✓ | ✓ |
| Subscription Server (SUBSRV) | | ✓ <input type="checkbox"/> | ✓ | ✓ |
| NameServer (NM) | ✓ | ✓ <input type="checkbox"/> | ✓ | ✓ |
| Product Distribution System (PDS) | | ✓ <input type="checkbox"/> | ✓ | ✓ |
| Data Pool Ingest (DPL_INS) | | ✓ <input type="checkbox"/> | ✓ | ✓ |
| Order Manager Subsystem (OMS) | | ✓ <input type="checkbox"/> | ✓ | ✓ |
| Spatial Subscription Server (SSS) | | ✓ <input type="checkbox"/> | ✓ | ✓ |
| Replication Server System Database (RSSD) | | ✓ <input type="checkbox"/> | ✓ | ✓ |
| COTS | | | | |
| Remedy (MSS) | ✓ | ✓ <input type="checkbox"/> | ✓ | ✓ |

Replicated Databases. In the system design, the System Monitoring Center SMC database is the primary database for all records. This means that all user account requests, profile creation, and profile modification activities must take place at the SMC. Sybase replication capabilities automatically send committed database changes from the SMC to the other sites. This significantly decreases the elapsed time from when a change is made to when that change is propagated to other sites. Figure 4.1-3 illustrates replication for the User Profile database.

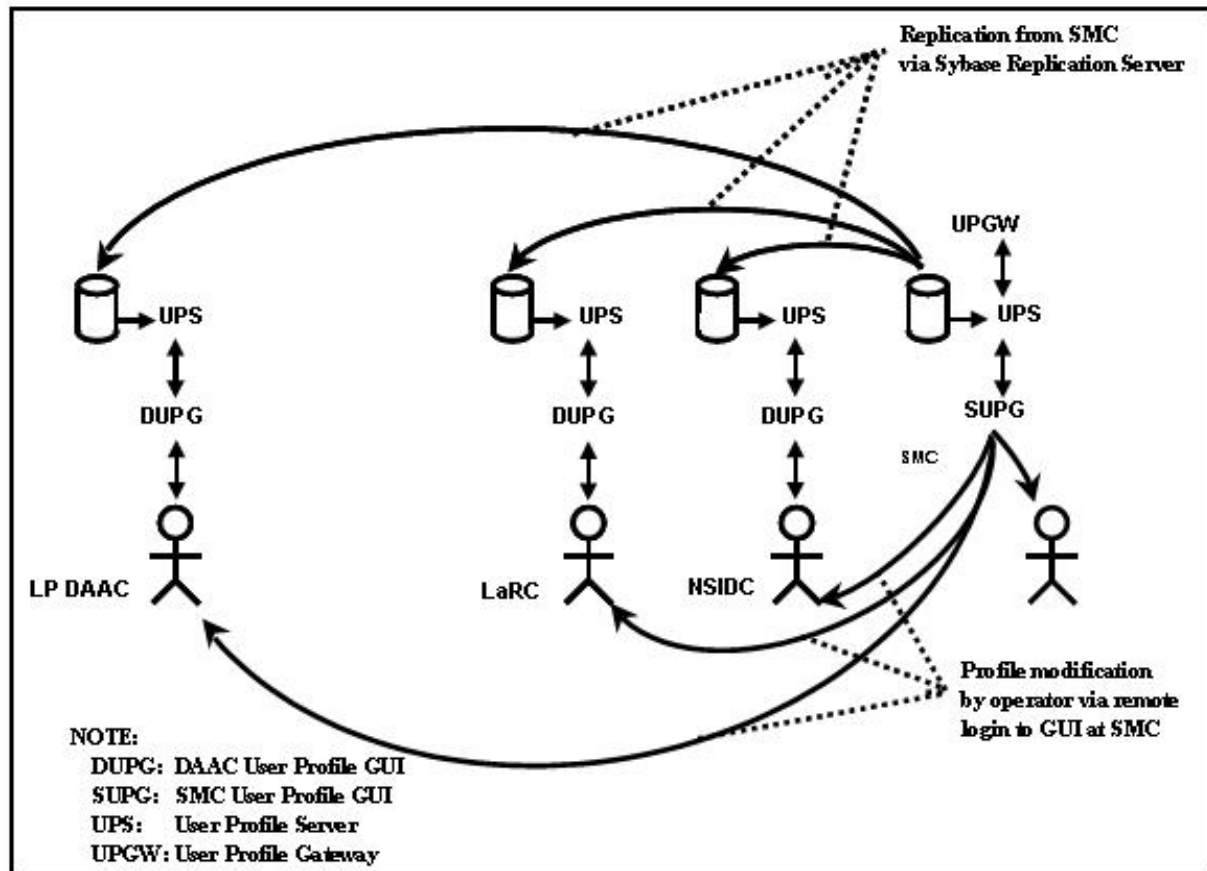


Figure 4.1-3. Database Replication

4.1.7 Database Directory Locations

Locations of principal database components are shown in Table 4.1-6.

Table 4.1-6. Location of Principal Database Components

| Name | Variant | Vendor | Principal Directory | Comments |
|---|-----------------|-------------|-----------------------------|---|
| Software Developer's Kit (formerly Open Client) | PC | Sybase | c:\windows\system | |
| Software Developer's Kit (formerly Open Client) | LINUX | Sybase | /tools/sybOCv12.5.1 | Just utilities, not libraries |
| Software Developer's Kit (formerly Open Client) | LINUX | Sybase | /tools/sybOCv12.5.1 | |
| Red Hat Enterprise Linux 4 | Red Hat | Linux | | |
| Replication Server | SUN, SGI, LINUX | Sybase | /usr/ecs/OPS/COTS/rep125 | |
| Replication Server Manager | SUN, SGI, LINUX | Sybase | /usr/ecs/OPS/COTS/rep125 | |
| ASE Server Monitor Client/Svr | SUN, SGI, LINUX | Sybase | /usr/ecs/<mode>/COTS/sybase | At DAAC discretion/ required for launch |
| Spatial Query Server (SQS) | SGI | Autometrics | /usr/ecs/OPS/COTS/sqs_342 | |
| Sybase Adaptive Server | SUN, SGI, LINUX | | /usr/ecs/OPS/COTS/sybase | /usr/ecs/OPS/COTS/sybase_125 or sybase125 is an acceptable install dir. |
| Sybase Adaptive Svr Enterprise | SUN, SGI, LINUX | Sybase | /usr/ecs/OPS/COTS/sybase | /usr/ecs/OPS/COTS/sybase_125 or sybase125 is an acceptable install dir. |
| Sybase Adaptive Svr Enterprise | SGI, SUN, LINUX | Sybase | /usr/ecs/OPS/COTS/sybase | |
| Sybase Adaptive Svr Enterprise | SGI, SUN, LINUX | Sybase | /usr/ecs/OPS/COTS/sybase | /usr/ecs/OPS/COTS/sybase_125 or sybase125 is an acceptable install dir. |
| Sybase Central | PC | Sybase | TBI | |

4.2 Database Management

4.2.1 Database Management Model

The concept that forms the basis of database management is described in *EOSDIS Core System Science Information Architecture* (FB9401V2). The EMD database management model is a variant of the ISO Data Management Reference Model (ISO 10032:1994). The variation is in the local (site) data management. The ISO reference model does not provide a structure for local data management. EMD defines local data management as being provided by a local information manager and a collection of data servers.

The model permits the following services and requests:

- *Client is a program requesting data management services.* A client can be an application program, such as a science algorithm, or a user interface, for example, an interface for formulating database queries and displaying query results. The client may use a data dictionary or vocabulary to assist in the formulation of database requests.

- *Data Server is an instance of a service that is capable of executing data access, query, and manipulation requests against a collection of data.* Data server actually refers to a service provider at a logical level. The data server may actually be constructed from multiple physical servers implementing various aspects of the data server's functionality. Data servers use lower layers of data management services, which are described in the data server architecture, section 6.4. Note that a site may choose to provide access to the same data via several different data servers, perhaps supporting different data access and query languages.
- *Data Dictionary Service is a service that manages and provides access to databases containing information about data.* Each data object, data element, data relationship, and access operation available via data servers is defined and described in the dictionary databases. Data dictionaries are intended for access by users (e.g., to obtain a definition of a data item) and programs (e.g., to format a screen).
- *Vocabulary Service is a service that manages and provides access to databases containing the definition of terminology, e.g., of words and phrases.* Vocabularies are intended for access by users (e.g., to obtain the appropriate term given a meaning) and programs (e.g., to let a user identify the intended meaning of a term which has several alternative definitions).

The model identifies the following key data objects supporting these services:

- *Schema is a formal description of the content, structure, constraints, and access operations available for or relevant to a database or a collection of databases.* The reference model contains Data Server and Data Dictionary/Vocabulary schema.

The model provides for the following kinds of requests:

- *Query is a request formulated in a language offered (i.e., supported) by a data server.* It contains data search and access specifications expressed in terms defined either by the language itself, or in a schema offered by the corresponding server. In general, a query language is paired with a particular type of schema. For example, relational queries reference objects defined in a relational schema.
- *Data Access Request is a service request that invokes an operation offered by a data server on a data object or a set of data.* The object types and the operations that a given service offers for them are described in the schema used by the service.

In addition, Data Servers conform to the general interface requirements as prescribed by the Interoperability Architecture. For example, this means that Data Servers accept requests regarding the status and estimated cost of a query or data access request. The servers also use the Interoperability Services in the course of their interactions. For example, clients use request brokers in order to locate a data dictionary service.

4.2.2 Database Management Implementation

4.2.2.1 Software

As previously described, system databases are primarily based on Sybase software. Primary components include:

- **Sybase Adaptive Server Enterprise (ASE).** ASE is an integrated set of software products for designing, developing and deploying relational database applications. It consists of a high-performance relational database management system (RDBMS), which runs database servers, and a collection of applications and libraries, which run on database clients. This arrangement, consisting of servers that are accessed by multiple clients over a network, forms the basis for Sybase's client/server architecture. ASE components are described in Table 4.2-1. An illustration of the main screen of Sybase Central, which can be used to perform many of the DBA procedures described in subsequent sections of this document, is shown in Figure 4.2-1.
- **Other Sybase Components:**
 - **Spatial Query Server (SQS).** The Spatial Query Server (SQS) is a multi-threaded Sybase Open Query database engine that is used by the Science Data Subsystem (SDSRV). This product allows definition of spatial data types, spatial operators, and spatial indexing. SQS communicates with the Sybase ASE Server to process SDSRV requests to push and pull metadata. Both the SDSRV database server and the SQS server resides on the same SGI machine.
 - **Replication Server (RS).** The Sybase Replication Server is used by the Management Subsystem (MSS) to allow all science users to register only once at their specified home DAAC and be able to request data from all DAAC sites. The RS uses replication definitions for tables at the primary database and subscriptions for tables at the replication sites. The replication definitions specify the location of the primary data while the subscription specifies the location of the replicate data. The replication definition and subscriptions are specified at the table or stored procedure level. The model attempts to prevent data inconsistencies that would be created by updating and replicating copies of the same data in two databases simultaneously. It stipulates that inserts, updates, and deletes to the data can only occur at the primary database, while select statements may occur at either the primary or the replicate database. The model assumes the enforcement of data ownership using custom developed database triggers, client code, or operational procedures.

Table 4.2-1. Sybase Adaptive Server Enterprise (ASE) Components (1 of 2)

| Type | Component | Description | Sub-Components and Features |
|--------|---|---|---|
| Client | Sybase Central | A Windows application for managing Sybase databases. Helps manage database objects and perform common administrative tasks. | Connecting to, disconnecting from, and stopping servers |
| | | | Troubleshooting Adaptive Server problems |
| | | | Managing data caches |
| | | | Managing Adaptive Server physical resources |
| | | | Creating, deleting, backing up, and restoring databases |
| | | | Creating and deleting Adaptive Server logins, creating and deleting database users and user groups, administering Sybase roles, and managing object and command permissions |
| | | | Monitoring Adaptive Server performance data and tuning performance parameters |
| | Sybase Central Plug-Ins | Each server product is managed by a service provider plug-ins that coexists with other service providers in the Sybase Central framework. | ASE Plug-In Replication Server Manager (RSM). Provides the ability to manage, monitor, and troubleshoot most replication system components (primary and replicate database servers, Replication Servers, Replication Agents, and database gateways). |
| Client | Software Developer's Kit (formerly Open Client) | | CS-Library, which contains a collection of utility routines used by all client applications. |
| | | | Client-Library and DB-Library, which contains a collection of routines that are specific to the programming language being used in an application |
| | | | Net-Library, which contains network protocol services that support connections between client applications and Adaptive Server. |
| | | | Utilities: isql – an interactive query processor that sends commands to the RDBMS from the command line. bcp – a program that copies data from a database to an operating system file, and vice versa. defncopy - a program that copies definitions of database objects that from a database to an operating system file and vice-versa. |

Table 4.2-1. Sybase Adaptive Server Enterprise (ASE) Components (2 of 2)

| Type | Component | Description | Sub-Components and Features |
|--------|-------------------------|--|--|
| Server | Adaptive Server (ASE) | Sybase's high-performance RDBMS | |
| | Backup Server(TM) | A server application that runs concurrently with Adaptive Server to perform high-speed on-line database dumps and loads. | |
| | Adaptive Server Monitor | Monitor Server | Allows capture, display, and evaluation of Adaptive Server performance data and tune Adaptive Server performance |
| | | Historical Server | Writes the data to files for offline analysis |

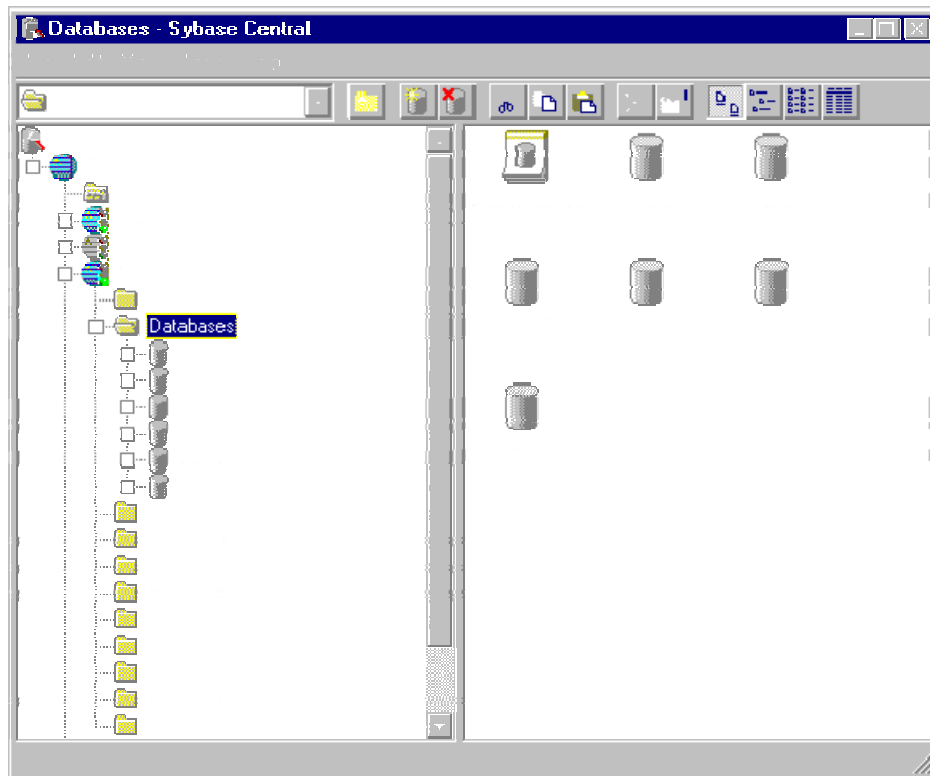


Figure 4.2-1. Sybase Central

4.2.3 Hardware, Software, and Database Mapping

Currently, user database reside on SUN SGI and Linux machines. They can be managed using PCs (Sybase Central only). Mapping documents for the DAACs are available on the web at <http://cmdm-ldo.raytheon.com/baseline/>, through the **Technical Documents** link. The hardware layout diagrams are available in documents 920-TDx-001, *Hardware-Design Diagram*. Hardware to software mappings are available in documents 920-TDx-002 *Hardware-Software Map*. The hardware database mappings are available in document 920-TDx-009 *DAAC HW Database Mapping*.

4.3 Database Administrator

The Database Administrator (DBA) is the individual responsible for the installation, configuration, update/upgrade, maintenance, and overall integrity, performance and reliability of system databases. In general, the DBA is concerned with the availability of the server, the definition and management of resources allocated to the server, the definition and management of databases and objects resident on the server, and the relationship between the server and the operating system. Basic DBA responsibilities include:

- Performing the database administration utilities such as database backup, maintenance of database transaction logs, and database recovery.
- Monitoring and tuning the database system (e.g., the physical allocation of database resources).
- Maintaining user accounts for the users from the external system. The DAAC database administrator creates user registration and account access control permissions in the security databases.
- Creating standard and *ad hoc* security management reports of stored security management data using the Sybase report generator.
- Working with EMD sustaining engineering and DAAC system test engineers to set up a test environment as needed.
- Working with the data specialist on information management tasks involving databases, data sets, and metadata management.
- Consolidating event reports into a site event history database for reporting activities to the SMC on a regular basis.
- Performing daily database synchronization.
- Administering the Replication Server System Database (RSSD).

4.3.1 DBA Tasks and Procedures

Basic DBA tasks and procedures are described in the following sections. Table 4.3-1 shows DBA tasks that have to be done on a regular basis and the section where they are addressed in this document.

Table 4.3-1. DBA Tasks Performed on a Regular Basis

| Time Period | Task | Importance | Found In ... |
|--------------------------------|---------------------------------|--|--|
| Daily | Capture database configurations | Absolutely necessary for database recovery if problems occur | Configuring Databases |
| | Reclaim disk space | | /usr/ecs/OPS/CUSTOM/dbms/COMDBAdmin/EcCoDbSyb_Reorg compact |
| | Run after reorg compact | only necessary if you want statistics for non-leading columns of the index | /usr/ecs/OPS/CUSTOM/dbms/COMDBAdmin/EcCoDbSyb_CustomizedDbStat |
| | Remove old dump files. | Keeping tack of seven (7) days worth of retrievable data or can specify another value. | /usr/ecs/OPS/CUSTOM/dbms/COMDBAdmin/EcCoDbSyb_CleanupDumps |
| Weekly | Monitor Sybase disk usage | | Monitoring and Tuning Databases |
| | Clean up old files | | |
| Monthly | Reboot | | Starting and Stopping Servers |
| Before and After Installations | Run DbVerify scripts | | Installing Databases and Patches |

Subsequent sections related to Database Administration address the following topics:

- **Section 4.4** An overview of the process and step-by-step procedures for starting and stopping database servers.
- **Section 4.5** An overview of the process and step-by-step procedures for creating database devices.
- **Section 4.6** An overview of the process and step-by-step procedures for installing databases and patches.
- **Section 4.7** An overview of the process and step-by-step procedures for configuring databases.
- **Section 4.8** An overview of the process and step-by-step procedures for working with indexes, segments, and caches.
- **Section 4.9** An overview of the process and step-by-step procedures for backing up and recovering data.
- **Section 4.10** An overview of the process and step-by-step procedures for establishing database security.

- **Section 4.11** An overview of the process and step-by-step procedures for copying individual databases.
- **Section 4.12** An overview of the process and step-by-step procedures for bulk copying.
- **Section 4.13** An overview of the process and step-by-step procedures for replication system administration.
- **Section 4.14** An overview of the process and step-by-step procedures for performance monitoring, tuning, and problem reporting.
- **Section 4.15** An overview of the process and step-by-step procedures for ensuring database quality.
- **Section 4.16** An overview of the process and step-by-step procedures for Sybase troubleshooting.

4.4 Starting and Stopping Database Servers

Each procedure outlined has an **Activity Checklist** table that provides an overview of the task to be completed. The outline of the **Activity Checklist** is as follows:

Column one - **Order** shows the order in which tasks could be accomplished.

Column two - **Role** lists the Role/Manager/Operator responsible for performing the task.

Column three - **Task** provides a brief explanation of the task.

Column four - **Section** provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found.

Column five - **Complete?** is used as a checklist to keep track of which task steps have been completed.

Table 4.4-1, below, provides an Activity Checklist for starting and stopping database servers.

Table 4.4-1. Starting and Stopping Database Servers - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|------------------------------|-------------|-----------|
| 1 | DBA | Start ASE Servers | (P) 4.4.1.1 | |
| 2 | DBA | Start the ASE Backup Server | (P) 4.4.2 | |
| 3 | DBA | Start the ASE Monitor Server | (P) 4.4.3 | |
| 4 | DBA | Stop the ASE Monitor Server | (P) 4.4.4 | |
| 5 | DBA | Stop the ASE Backup Server | (P) 4.4.5 | |
| 6 | DBA | Stop the ASE Server | (P) 4.4.6 | |

4.4.1 Start Adaptive Server Enterprise (ASE) Servers

A server process is started manually when a new server is installed or after a system outage. In order to perform the procedure, the DBA must know the database server name and be assigned `sa_role` (refer to Section 4.10, Establishing Database Security). The following procedures are applicable.

4.4.1.1 Start ASE Servers

- 1 Log in to a local host.
 - 2 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY ServerName:0.0**, then press the **Return/Enter** key.
 - 3 Log into the server on which the ASE Server Process is to be started by typing: **/tools/bin/ssh ServerName**, then press the **Return/Enter** key.
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 4.
 - If you have not previously set up a secure shell passphrase, go to Step 5.
 - 4 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your *Passphrase* and then press the **Return/Enter** key.
 - Go to step 6.
 - 5 At the **<user@remotehost>'s password:** prompt, type your *Password* and then press the **Return/Enter** key.
 - 6 Log into the server as sybase, type, **su – sybase** and press the **Return/Enter** key.
 - A password prompt is displayed.
 - 7 Enter *sybase password*, then press the **Return/Enter** key.
 - You are authenticated as yourself and returned to the UNIX prompt.
 - 8 At the UNIX prompt, type **cd /ASE-12_5/install** and then press the **Return/Enter** key.
 - 9 At the UNIX prompt, type **./RUN_servername &** then press the **Return/Enter** key.
 - 10 At the UNIX prompt, type **showserver**, then press the **Return/Enter** key.
 - This displays a listing of the ASE Server processes that are running.
-

4.4.2 Start the ASE Backup Server

NOTE: This procedure should be done after ASE Server is up and running

- 1 Log in to a local host.
- 2 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY ServerName:0.0**, then press the **Return/Enter** key.
- 3 Log into the server on which the ASE Server Process is to be started by typing: **/tools/bin/ssh ServerName**, then press the **Return/Enter** key.
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 4.
 - If you have not previously set up a secure shell passphrase, go to Step 5.
- 4 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your **Passphrase** and then press the **Return/Enter** key.
 - Go to step 6.
- 5 At the **<user@remotehost>'s password:** prompt, type your **Password** and then press the **Return/Enter** key.
- 6 Log into the server as sybase, type, **su – sybase** and press the **Return/Enter** key.
 - A password prompt is displayed.
- 7 Enter **sybase password**, then press the **Return/Enter** key.
 - You are authenticated as yourself and returned to the UNIX prompt.
- 8 Type **cd /ASE-12_5/install** and press the **Return/Enter** key.
- 9 Type, **./RUN_backupservername &** and press the **Return/Enter** key.

NOTE: You may have to hit the **Return/Enter** key one more time

4.4.3 Start the ASE Monitor Server

NOTE: This procedure is be done on an as needed basis and after the ASE Server is up and running

- 1 Log in to a local host.

- 2 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY ServerName:0.0**, then press the **Return/Enter** key.
 - 3 Log into the server on which the ASE Server Process is to be started by typing: **/tools/bin/ssh ServerName**, then press the **Return/Enter** key.
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 4.
 - If you have not previously set up a secure shell passphrase, go to Step 5.
 - 4 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your *Passphrase* and then press the **Return/Enter** key. Go to step 6.
 - 5 At the **<user@remotehost>'s password:** prompt, type your *Password* and then press the **Return/Enter** key.
 - 6 Log into the server as sybase, type, **su – sybase** and press the **Return/Enter** key.
 - A password prompt is displayed.
 - 7 Enter *sybase password*, then press the **Return/Enter** key.
 - You are authenticated as yourself and returned to the UNIX prompt.
 - 8 Type **cd /ASE-12_5/install** and press the **Return/Enter** key.
 - 9 Type **./ RUN_monitor_srvr** and press the **Return/Enter** key.
-

Servers are stopped by the DBA when the system needs to be brought down. Servers are brought down in an order that is the reverse of the start-up order. The **shutdown** command issued from within isql shuts down the server where you are logged in. It allows for the completion of any current processes and blocks the start of any new processes before the server is shutdown.

When you issue a **shutdown** command, the server:

- Disables all logins except the sa's.
- Performs a checkpoint in each database, moving changed pages from memory to disk.
- Waits for currently executing SQL statements or procedures to finish.

Adding a **nowait** option to the command immediately terminates all processes and shuts down the server. The **nowait** option should be used sparingly because it may cause data loss and complicate recovery.

4.4.4 Stop the ASE Monitor Server

NOTE: This procedure should be done before the ASE Server is shutdown

- 1 Log on to a local host.
- 2 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY ServerName:0.0**, then press the **Return/Enter** key.
- 3 Log into the server on which the ASE Server Process is to be stopped by typing: **/tools/bin/ssh ServerName**, then press the **Return/Enter** key.
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 4.
 - If you have not previously set up a secure shell passphrase, go to Step 5.
- 4 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your *Passphrase* and then press the **Return/Enter** key.
 - Go to step 6.
- 5 At the **<user@remotehost>'s password:** prompt, type your *Password* and then press the **Return/Enter** key.
- 6 Log into the server as sybase, type, **su – sybase** and press the **Return/Enter** key.
 - A password prompt is displayed.
- 7 Enter *sybase password*, then press the **Return/Enter** key.
 - You are authenticated as yourself and returned to the UNIX prompt.
 - Your new home directory is **/usr/ecs/OPS/COTS/sybase** and all required environment variables have been set.

NOTE: Environment and DS queary are set when you use **su – sybase**, if not use **\$SYBASE/bin/** in command line.

- 8 Type **isql –Usa** and press the **Return/Enter** key.
 - 9 Type the *sa-password* when prompted for it and press the **Return/Enter** key.
 - 10 Type **sms_shutdown** at “1>” prompt and press the **Return/Enter** key.
 - 11 Type **go** at “2>” prompt and press the **Return/Enter** key.
-

4.4.5 Stop the ASE Backup Server

NOTE: This procedure should be done before shutting down the ASE Server

- 1 Log on to a local host.
- 2 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY ServerName:0.0**, then press the **Return/Enter** key.
- 3 Log into the server on which the ASE Server Process is to be stopped by typing: **/tools/bin/ssh ServerName**, then press the **Return/Enter** key.
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 4.
 - If you have not previously set up a secure shell passphrase, go to Step 5.
- 4 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your *Passphrase* and then press the **Return/Enter** key.
 - Go to step 6.
- 5 At the **<user@remotehost>'s password:** prompt, type your *Password* and then press the **Return/Enter** key.
- 6 Log into the server as sybase, type, **su – sybase** and press the **Return/Enter** key.
 - A password prompt is displayed.
- 7 Enter *sybase password*, then press the **Return/Enter** key.
 - You are authenticated as yourself and returned to the UNIX prompt
 - Your new home directory is **/usr/ecs/OPS/COTS/sybase** and all required environment variables have been set.

NOTE: GDAAC implementation has a sybsetup.csh file (type source sybsetup.csh).

- 8 Type, **isql –U<username>** and press the **Return/Enter** key.
 - 9 Type the *password* when prompted for it and press the **Return/Enter** key.
 - 10 Type **shutdown SYB_BACKUP** at the “1>” prompt and press the **Return/Enter** key.
 - 11 Type **go** at the “2>” prompt and press the **Return/Enter** key.
-

4.4.6 Stop the ASE Server

-
- 1 Use **shutdown** to bring the server to a halt.
 - This command can only be issued by the Sybase System Administrator (sa).
 - If you do not give a server name, shutdown shuts down the ASE Server you are using.
 - Syntax:
1> shutdown [with] [wait] [with nowait]
2> go
 - 2 To see the names of the backup servers that are accessible from your ASE Server, execute **sp_helpserver**.
 - Use the value in the name column in the shutdown command.
 - You can only shut down a Backup Server that is:
 - Listed in **syssservers** on your ASE Server
 - Listed in your local interfaces file
-

4.5 Creating Database Devices

Table 4.5-1, below, provides an Activity Checklist for creating database devices.

Table 4.5-1. Creating Database Devices - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|--------------------------|-------------|-----------|
| 1 | DBA | Create a Database Device | (P) 4.5.1.1 | |

4.5.1 Create a Database Device

Database devices store the objects that make up databases. The term “device” can refer to either a physical or a logical device. Logical devices include any portion of a disk, such as a *partition* or a *file* in the file system used to store databases and their objects. A database device can be created when the System Administrator determines that new disk space is available for database use or as part of the recovery process. The System Administrator makes a request to the Data Base Administrator (DBA), who creates the new database device and notifies the System Administrator when the device has been created.

In order to create a new device, the DBA must have the following:

- The name of database device to be created
- A physical device on which to place database device
- The device size in megabytes

- The name of the mirror device, if one is in effect

*The creation of a database device is the mapping of physical space to a logical name and virtual device number (**vdevno**) contained in the master database. The **disk init** command is used to initialize this space. **Disk init** syntax is:*

```
name = device_name
physname = physicalname
vdevno = virtual_device_number (optional: will use the next available number)
size = number_of_blocks
[vstart = virtual_address
cntrltype = controller_number] (optional)
```

Before you run **disk init**, see the server installation and configuration guide for your platform for information about choosing a database device and preparing it for use with the server. You may want to repartition the disks on your computer to provide maximum performance for your databases. **Disk init** divides the database devices into allocation units of 256 2K pages, a total of 1/2MB. In each 256-page allocation unit, the **disk init** command initializes the first page as the allocation page, which will contain information about the database (if any) that resides on the allocation unit.

Once initialization is complete, the space described by the physical address is available to the server for storage and a row is added to the **sysdevices** table in the master database. The initialized database can be:

- Allocated to the pool of space available to a user database
- Allocated to a user database and assigned to store a specific database object or objects
- Used to store a database's transaction logs

NOTE: Unless you are creating a small or non-critical database, always place the log on a separate database device.

After you run the **disk init** command, be sure to use **dump database** to dump the master database. This makes recovery easier and safer in case master is damaged. If you add a device and fail to back up master, you may be able to recover the changes with **disk reinit**.

4.5.1.1 Create a Database Device

NOTE: This procedure will assist in creating a database device.

- 1 Log on to a local host.
- 2 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY ServerName:0.0**, then press the **Return/Enter** key.

- 3 Log into the server on which the new database device is to be created by typing: **/tools/bin/ssh <ServerName>**, then press the **Return/Enter** key.
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 4.
 - If you have not previously set up a secure shell passphrase, go to Step 5.
- 4 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your **Passphrase** and then press the **Return/Enter** key.
 - Go to step 6.
- 5 At the **<user@remotehost>'s password:** prompt, type your **Password** and then press the **Return/Enter** key.

NOTE: For each database device to be created, perform Steps 6 through 9.

- 6 Using the text editor of your choice, edit **DeviceName.sql** and make changes to information enclosed in brackets (including the brackets) as appropriate:
 - An example of an **add_devices.sql** file for creation of a database device is shown in Figure 4.5-1.

```

/*****
/* name: [add_devices.sql]
/* purpose:
/* written:
/* revised:
/* reason:
*****/
disk init name = [device name],
physname = "/dev/[device name]",
vdevno = [#],
size = [size]
go
sp_helpdevice [device name]
go

```

Figure 4.5-1. Example of an add_devices.sql File for Creation of a Database Device

- In the area delimited by **/* */**, enter an appropriate description of the script including the file name, date written and person who wrote the script, its

purpose, and any other information deemed appropriate. Be sure to enclose each line of the comment between `/* */`.

- The **disk init name** is the *DeviceName* is used in Step 8 above. You may not use spaces or punctuation except the underscore character (`_`) in *DeviceName*. Remember that the name you assign is case-sensitive. Be sure there is a comma after *DeviceName*
- The physname is the *FullPath_to_DeviceName*. Be sure to enclose *FullPath_to_DeviceName* in double quotes. Be sure to place a comma after *FullPath_to_DeviceName* but outside the double quotes.
- The **vdevno**, an optional command in this current version of ASE, is the **VirtualDeviceNumber**. **vdevno** is a unique identifying number for the database device. It is unique among all the devices used by ASE Server and is never reused. Device number 0 represents the device named **d_master** that stores the system catalogs. Legal numbers are between 1 and 255, but the highest number must be one less than the number of database devices for which your system is configured. For example, for a system with the default configuration of 10 devices, the legal device numbers are 1-9. The default of 10 devices can be changed using **sp_configure**. If a number is specified, ASE assigns the next available virtual device number. This feature helps to eliminate the possibility of using an existing number, which Sybase will usually return the message, “device activation error.” The next available number can be determined by looking at the output from the **sp_helpdevice** command and selecting the next number in sequence.
- The **size** is the *DeviceSize* in blocks. To compute the number of blocks, multiply the device size in megabytes by 512; e.g., a 1,000 Mb device has 512,000 blocks

7 After the changes have been made, save the file according to the rules of your text editor.

8 At the UNIX prompt, type **isql -Username -SServerName -iDeviceName.sql -oDeviceName.out** then press the **Return/Enter** key.

- *ServerName* is the name of the server on which the database device will be created.
- *DeviceName.sql* is the name of the script file you created in step 8.
- *DeviceName.out* is the filename of the script’s output for confirmation and/or troubleshooting purposes.)
- The system will prompt you for a password.

9 At the **Password:** prompt, type the *<password>* then press the **Return/Enter** key.

- When the UNIX prompt is again displayed the process is complete.

10 At the UNIX prompt, type **more DeviceName.out**, then press the **Return/Enter** key.

- This allows you to view the *DeviceName.out* file to confirm that the device has been created or to check for device creation errors.

4.6 Installing Databases and Patches

Table 4.6-1, below, provides an Activity Checklist for installing databases and patches.

Table 4.6-1. Installing Databases and Patches - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|------------------------------------|-------------|-----------|
| 1 | DBA | Perform a Database Build (Example) | (P) 4.6.1.1 | |
| 2 | DBA | Install a Database Patch (Example) | (P) 4.6.2.1 | |

4.6.1 Perform a Database Build Procedure (Example Only)

The ECS Assistant is a custom application that simplifies the process of installing, testing and managing system software. The **Subsystem Manager** screen is used in the operational environment. The **Database** option is used to install, drop, patch, and update subsystem-specific databases. The **Install** option is used to install custom software in a particular mode. The **Configuration** option is used to create CFG, ACFG and PCFG files for selected components. The **Stage Area Installation** option is used to input the staging location where the delivered software is stored. The **View Task Output** option is used to view results as the specified task is executing. A detailed description of ECS Assistant use can be found in 609-EMD-001, *Release 7.11 Operations Tools Manual for the EMD Project*.

To perform a database build follow the steps included in the documentation (e.g., release notes) that specifies performing the build. The following steps are an example of a database that was built and populated with data from the version of the database that the new database was replacing. Unless otherwise specified, the scripts that were run are located in the `/usr/ecs/<MODE>/CUSTOM/dbms/<SUBSYSTEM>` directory.

4.6.1.1 Performance Database Build (Example)

- 1 Create new db logins for new servers.
 - For example:

```
# EcDsStDb6ALogins <MODE> <dbo_user_name> <dbo_user_password>  
<server_name> <DBNAME>
```
- 2 Run the database verification script on the existing database.
 - For example:

```
# EcStDbVerify5B <MODE> <USERNAME> <SERVER> <DBNAME>
```
 - The script is located in the `/usr/ecs/<MODE>/CUSTOM/dbms/COM/DBAdmin` directory. The output from this script is located in

/usr/ecs/<MODE>/CUSTOM/logs and is named
EcStDbVerify5B.<DBSERVER>.<DBNAME>.<DATETIME>.

- 3 Bulk copy data out of the existing database:
 - For example:
**# EcDsStBulkCopyOut5B <MODE> <USERNAME> <PASSWORD>
<SERVER> <DBNAME>**
 - The output from this script is saved as
/usr/ecs/<MODE>/CUSTOM/logs/EcDsStBulkCopy.log.
- 4 Build the database using **ECS Assistant**.
 - Using the **SubSystem Manager**, execute the **DbBuild** function to build the database.
 - Enter the appropriate parameters in the **Database Script Parameters** dialogue box.
- 5 Execute the **EcDbDDMUpdateVersionTable.sql** script file that is under the directory **/usr/ecs/{MODE}/CUSTOM/dbms/COM/DBAdmin**.
 - The parameters to be passed are **MODE USERNAME DSQUERY DBNAME**.
 - You will be prompted for the password.
- 6 Review the file **EcMsDbBuild.log** in **/usr/ecs/<MODE>/CUSTOM/logs** for any error or warning messages.
- 7 Have the DBA verify the database changes through the **DbDesc** script for this subsystem.
- 8 Verify that the database version identifiers are correct.
 - For example:
**# isql -S <server_name> -U <db_user_name> -P <db_user_password>
use <database>_<MODE>
go
select * from EcDbDatabaseVersions where EcDbCurrentVersionFlag=" Y"
go**
- 9 Run a database transition upgrade script.
 - For example:
**# EcDsStDbSybaseUpgrade. ksh <MODE> <USERNAME> <PASSWORD>
<SERVER> <DBNAME>**
- 10 Run a script to create all of the new tables required for transition into the new database.
 - For example:
**# EcDsStCreate5BTranTables <USERNAME> <PASSWORD> <SERVER>
<DBNAME>**

- 11** Bulk copy data in the old tables into the new database.
- For example:
EcDsStBulkCopyIn5B <MODE> <USERNAME> <PASSWORD> <SERVER> <DBNAME>
 - The output from this script is saved as
/usr/ecs/<MODE>/CUSTOM/logs/EcDsStBulkCopy.log.
- 12** Run the Transition Script.
- For example:
EcDsStTransition5Bto6A <MODE> <USERNAME> <PASSWORD> <SERVER> <DBNAME>
- NOTE:** You will need to have the secure shell passphrase and install login password ready to enter when prompted.
- The output from this script is saved as
/usr/ecs/<MODE>/CUSTOM/logs/EcDsStTransition.log.
- 13** Run the database verification script (script is located in the **/usr/ecs/<MODE>/CUSTOM/dbms/COM/DBAdmin** directory).
- For example:
EcStDbVerify6A <MODE> <USERNAME> <SERVER> <DBNAME>
 - The output from this script is saved as
/usr/ecs/<MODE>/CUSTOM/logs/EcStDbVerify6A.<DBSERVER>.<DBNAME>.<DATETIME>.
- 14** Check the differences between the database verification script output logs for the old database and the new database:
- For example:
diff -w EcStDbVerify5B.<DBSERVER>.<DBNAME>.<DATETIME> EcStDbVerify6A.<DBSERVER>.<DBNAME>.<DATETIME>
- 15** Compare the output of this statement with the differences expected based on information in the reference document.
- 16** Run a script to remove all tables required for transition into the new database:
- For example:
EcDsStDrop5BTranTables <USERNAME> <PASSWORD> <SERVER> <DBNAME>
-

4.6.2 Install a Database Patch (Example)

To install a database patch follow the steps included in the documentation (e.g., release notes) that specifies installing the patch. To install database patches, perform the following steps for all subsystems/components and then perform the appropriate subsystem/component-specific procedures.

4.6.2.1 Install a Database Patch (Example)

- 1 Verify the current version of the database being patched.

```
# isql -S <server_name> -U <db_user_name> -P <db_user_password>
# use <db_name>[_<MODE>]
# go
# select * from EcDbDatabaseVersions where EcDbCurrentVersionFlag=" Y"
# go
```
- 2 Compare the current database version against the appropriate version listed in the table provided in the patch instructions.
 - If the current version is greater than or equal to the appropriate version listed in the table, continue with the database patch.
 - If the current version is less than the appropriate version listed in the table, stop and patch the deficient database.
- 3 From the **ECS Assist Subsystem Manager** select the appropriate mode, subsystem, and component from the main window.
- 4 From the **ECS Assist Subsystem Manager** select **DbPatch** from the **Database** menu.
 - A **File Selection** window appears.
- 5 From the **ECS Assist Subsystem Manager** (in the **File Selection** window) select **.dbparms** and **OK**.
- 6 Follow subsystem-specific installation instructions included in the documentation (e.g., release notes) that specifies installing the patch to complete the database patch process.
 - For example:
 - 1 Logon to the host where the subsystem database package is installed.
 - 2 Start ECS Assist's Subsystem Manager, select the appropriate mode, subsystem, and component.
 - 3 Select **DbPatch** from the **Database** menu. A **File Selection** window appears.
 - 4 In the "**File Selection**" window, select "**.dbparms**" and then "**Ok**". The "**Configurable Database Parameters**" dialog box appears.

- 5 Verify the patch number (referring to the table in the patch instructions). If it is not correct, correct it, enter the required information and select **Ok**.
-

4.6.3 COTS Databases

AutoSys and Remedy have Sybase databases. COTS installation is performed by the auto-install applications in the `/usr/ecs/OPS/COTS` directory. The results of the installation are stored in the appropriate subdirectories, e.g., an **autosys_install.scr** file located in the AutoSys home directory (`/use/ecs/OPS/COTS/autosys`).

4.7 Configuring Databases

Table 4.7-1, below, provides an Activity Checklist for configuring databases.

Table 4.7-1. Configuring Databases - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|----------------------------------|-------------|-----------|
| 1 | DBA | Configure the ASE Server | (P) 4.7.1.1 | |
| 2 | DBA | Display Configuration Parameters | (P) 4.7.4 | |

4.7.1 Configure the ASE Server Parameters

Configuration parameters are user-defined settings that control various aspects of a database server's behavior. The server supplies default values for all configuration parameters. However, some of the configuration parameters need to be customized (refer to *SYBASE SQLServer 11.0.x: ALL DAAC Database Configurations*, 910-TDA-021).

Configuration parameters are grouped according to the area of server behavior that they affect. This makes it easier to identify all parameters that may need to be tuned in order to improve a particular area of ASE Server performance. The groups are:

- Backup/Recovery.
- Cache Manager.
- Component Integration Services
- DTM Administration
- Diagnostics
- Disk I/O
- Error Log
- Extended Stored Procedure
- General Information
- Java Services
- Languages
- Lock Manager

- Memory Use
- Meta Data Cache
- Monitoring
- Network Communications
- Operating System Resources
- Parallel Query
- Physical Memory
- Physical Resources
- Processors
- Red Agent Tread Administration
- SQL Server Administration
- Security Related Unicode
- User Environment

While each parameter has a primary group to which it belongs, many have secondary groups to which they also belong. For instance, the parameter number of remote connections belongs primarily in the Network Communications group, but also secondarily in the SQL Server Administration group and the Memory Use group. This reflects the fact that some parameters have implications for a number of areas of ASE Server behavior.

The configuration parameters are divided between two tables:

- Sybase Configuration Parameter Table
- DAAC-Specific Configuration Parameter Table.

The Sybase Configuration Parameter Table groups the configuration parameters by functionality. It provides a list of configurable parameters under each functional group, and provides recommended values for these parameters:

The following type of information is captured in the Sybase Configuration Parameter Table:

- Group Name.
- Group Description.
- Parameter Name (for each group).
- Parameter Description.
- Command Line.
- Status (Static or Dynamic parameter).
- Recommended Value.
- Range (Minimum and maximum parameter value).
- Display Level (Basic, Intermediate, Comprehensive).
- Impact (Brief description of type of impact when a parameter value is configured).
- Controlling Authority (Entity responsible for controlling changes to a configuration parameter).
- Comments (This will include suggestions and examples).

Configuration parameters can be set or changed in one of two ways:

- By executing the system procedure **sp_configure** with the appropriate parameters and values.
- By hand-editing your configuration file and then invoking **sp_configure** with the configuration file option.

Configuration parameters are either dynamic or static. *Dynamic parameters go into effect as soon as **sp_configure** is executed. Static parameters require the ASE server to reallocate memory and take effect only after ASE Server has been restarted.*

The roles required for using **sp_configure** are as follows:

- Any user can execute **sp_configure** to display information about parameters and their current values.
- Only System Administrators and System Security Officers can execute **sp_configure** to modify configuration parameters.
- Only System Security Officers can execute **sp_configure** to modify values for allow updates, audit queue size and remote access.

The system procedure **sp_configure** displays and resets configuration parameters. One can restrict the number of parameters **sp_configure** displays by using **sp_displaylevel** to set the display level to one of the three values: Basic, Intermediate, or Comprehensive.

Figure 4.7-1 shows a sample **sp_configure** output. **Name** column is the description of the variable. The **minimum** column is the minimum allowable configuration setting. **Maximum** is the theoretical maximum value to which the configuration option can be set. The actual maximum value is dependent on the specific platform and available resources to the ASE server. **Config_value** reflects the current system default values. **Run_value** reflects the values the system is currently using, which may be different from the default values.

SQL Server configuration can be done either interactively by using **sp_configure** or non-interactively by invoking **sp_configure** with a configuration file. Configuration files can be used for several reasons:

- To replicate a specific configuration across multiple servers by using the same configuration file.
- To use a configuration file as a baseline for testing configuration values on your server.
- To use a configuration file to do validation checking on parameter values before actually setting the values.
- To create multiple configuration files and to switch between them as your resource needs change.

Previous releases of ASE Server required that **reconfigure** be executed after executing **sp_configure**. This is no longer required. The **reconfigure** command still exists, but it no longer has any effect.

| name | minimum | maximum | config value | run value |
|------------------------------|---------|------------|--------------|-----------|
| recovery interval | 1 | 32767 | 0 | 5 |
| allow updates | 0 | 1 | 0 | 0 |
| user connections | 5 | 2147483647 | 0 | 25 |
| memory | 3850 | 2147483647 | 0 | 5120 |
| open databases | 5 | 2147483647 | 0 | 12 |
| locks | 5000 | 2147483647 | 0 | 5000 |
| open objects | 100 | 2147483647 | 0 | 500 |
| procedure cache | 1 | 99 | 0 | 20 |
| fill factor | 0 | 100 | 0 | 0 |
| time slice | 50 | 1000 | 0 | 100 |
| database size | 2 | 10000 | 0 | 2 |
| tape retention | 0 | 365 | 0 | 0 |
| recovery flags | 0 | 1 | 0 | 0 |
| nested triggers | 0 | 1 | 1 | 1 |
| devices | 4 | 256 | 0 | 10 |
| remote access | 0 | 1 | 1 | 1 |
| remote logins | 0 | 2147483647 | 0 | 20 |
| remote sites | 0 | 2147483647 | 0 | 10 |
| remote connections | 0 | 2147483647 | 0 | 20 |
| pre-read packets | 0 | 2147483647 | 0 | 3 |
| upgrade version | 0 | 2147483647 | 1002 | 1002 |
| default sortorder id | 0 | 255 | 50 | 50 |
| default language | 0 | 2147483647 | 0 | 0 |
| language in cache | 3 | 100 | 3 | 3 |
| max online engines | 1 | 32 | 1 | 1 |
| min online engines | 1 | 32 | 1 | 1 |
| engine adjust interval | 1 | 32 | 0 | 0 |
| cpu flush | 1 | 2147483647 | 200 | 200 |
| i/o flush | 1 | 2147483647 | 1000 | 1000 |
| default character set id | 0 | 255 | 1 | 1 |
| stack size | 20480 | 2147483647 | 0 | 28672 |
| password expiration interval | 0 | 32767 | 0 | 0 |
| audit queue size | 1 | 65535 | 100 | 100 |
| additional netmem | 0 | 2147483647 | 0 | 0 |
| default network packet size | 512 | 524288 | 0 | 512 |
| maximum network packet size | 512 | 524288 | 0 | 512 |
| extent i/o buffers | 0 | 2147483647 | 0 | 0 |
| identity burning set factor | 1 | 9999999 | 5000 | 5000 |
| allow sendmsg | 0 | 1 | 0 | 0 |
| sendmsg starting port number | 0 | 65535 | 0 | 0 |

Figure 4.7-1. Example of sp_configure Output

Configuration files are not automatically backed up when you back up your master database. As they are part of the operating system files, they should be backed up in the same way other operating system files are backed up.

In order to perform the following procedure, the DBA must have obtained the following information:

- Name of server to be configured
- New values for configuration variables.

To set ASE Server configuration variables, the DBA must have **sa_role** (ASE Server) permissions. To set ASE Server configuration variables **allow updates**, **audit queue size**, **password expiration interval**, or **remote access**, **sso_role** (ASE Server) is also required.

Some parameter values take effect as soon as you reset the value. Others, which involve memory reallocation, do not change until you reset the value and then reboot ASE Server.

4.7.1.1 Configure the ASE Server

- 1 Log into the server that will be reconfigured by typing: **telnet *ServerName*** or **ssh *ServerName***, then press **Return**.
 - 2 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.
 - A password prompt is displayed.
 - 3 Enter ***YourPassword*** then press **Return**.
 - You are authenticated as yourself and returned to the UNIX prompt.
 - 4 Set display to current terminal by typing: **setenv DISPLAY *IPNumber:0.0*** or **setenv DISPLAY *ServerName:0.0***, then press **Return**.
 - 5 Begin the ASE session by typing at the UNIX prompt **isql -S*ServerName*** then press **Return**.
 - 6 Type **sp_configure** then press **Return**.
 - 7 Type **go**, then press **Return**.
 - A list of the configurable parameters, their maximum and minimum values, the current setting and the default values is displayed.
 - 8 After determining which parameter(s) to reset, type: **sp_configure "*ParameterName*", *NewValue***, then press **Return**.
 - ***ParameterName*** is the name from the list displayed in Step 7 above.
 - Be sure to enclose the name in double quotes.
 - ***NewValue*** is the numeric value that you want to assign to ***ParameterName***.
 - 9 Type **go**, then press **Return**.
 - 10 Repeat Steps 7 through 9 for each parameter you want to reconfigure.
 - 11 When complete, type **quit** at the isql prompt, then press **Return**.
 - You are returned to the UNIX prompt.
-

4.7.2 Configuration Parameters and the Configuration Registry

There are many configurable parameters associated with the custom software. Some of them are set by default to values that may be appropriate for most operating conditions. Others may be set to values that may or may not be appropriate for the requirements of operations at a particular DAAC. Some parameters may be changed using system Graphical User Interfaces (GUIs) specifically designed to monitor and control functions related to particular subsystems. Others may require changes to a configuration file or database.

NOTE: Before changing any configuration parameter, make certain either that it is not under configuration control or that you have obtained any necessary approval specified in local Configuration Management policies and procedures.

4.7.3 Configuration Registry

Configuration parameters for custom software are managed by the Configuration Registry. The Configuration Registry Server provides a single interface to retrieve configuration attribute-value pairs for servers from the Configuration Registry Database, via a Sybase Server. The Configuration Registry Server maintains an internal representation of the tree in which configuration attribute-value pairs are stored. General configuration parameters used by many servers are stored in higher nodes in the tree. Parameters specific to a single server are contained in the leaf nodes of the tree. A script tool is available for loading the Configuration Registry database from data in configuration files. This loading is a one-time event to populate the Registry database with the information contained in **.cfg** files. Once the Configuration Registry is loaded, if the configuration files are moved or otherwise made inaccessible to the software, the software goes to the Configuration Registry to obtain needed configuration parameters. There is also a Configuration Registry application that can be used to view and edit configuration data in the database. Changes to the Configuration Registry typically are under the control of Configuration Management and the Database Administrator.

Data in the Registry database are stored hierarchically, sorted by hostnames. An application may have multiple entries, each under a different hostname where it runs. The application queries the database directly. The application shows the Attribute Tree on the left. It displays parameters and their values in the Attribute Listing on the right. It provides the operator with capability to create, read, update, and delete database entries. A click on a parameter name in the Attribute Listing displays a pop-up window, permitting the user to update or delete the parameter.

4.7.4 Use the following procedure to display configuration parameters.

- 1 On workstation **x0dms##**, in a terminal window, type **/usr/ecs/*mode*/CUSTOM/utilities/EcCsRegistryGUIStart *mode* &** at a UNIX command prompt and then press the **Return/Enter** key (where *mode* is likely to be **TS1**, **TS2**, or **OPS**).
 - The **x** in the workstation name is a letter designating your site: **g** = GSFC, **m** = SMC, **l** = LaRC, **e** = EDC, **n** = NSIDC, **o** = ORNL, **a** = ASF, **j** = JPL; the **##** is an identifying two-digit number (e.g., **g0dms03** indicates a data management subsystem workstation at GSFC). If you access the workstation through a secure shell remote

login (ssh), you must enter **setenv DISPLAY <local_workstation IP address>:0.0** prior to the ssh before entering the command after the ssh. The *<ipaddress>* is the ip address of **x0mss##**, and **xterm** is required when entering this command on a Sun terminal.

- The Database Login window is displayed with entries filled in for **User Id:** (e.g., **EcCsRegistry**), **Server:** (e.g., **x4dpl02_srvr**), and **DB Name:** (e.g., **EcCsRegistry_mode**). (See Figure 4.7-2 below.)

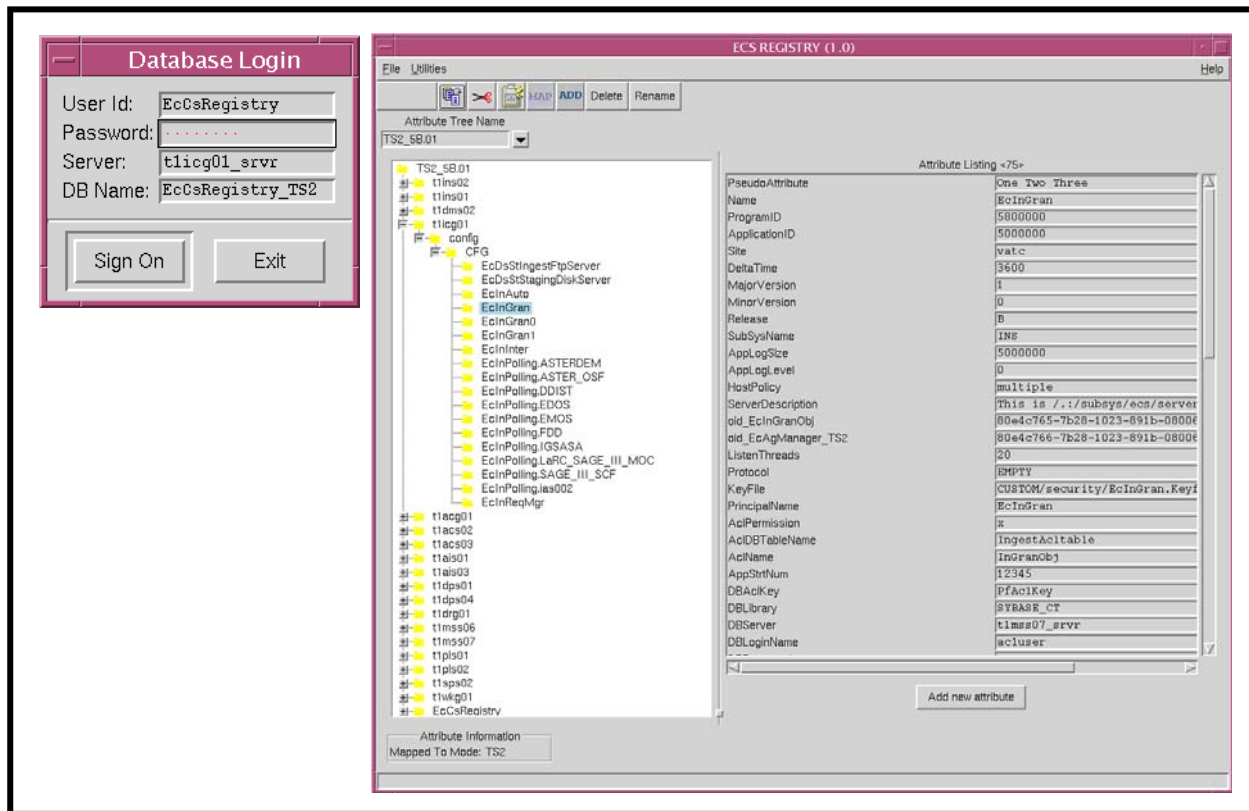


Figure 4.7-2. Configuration Registry

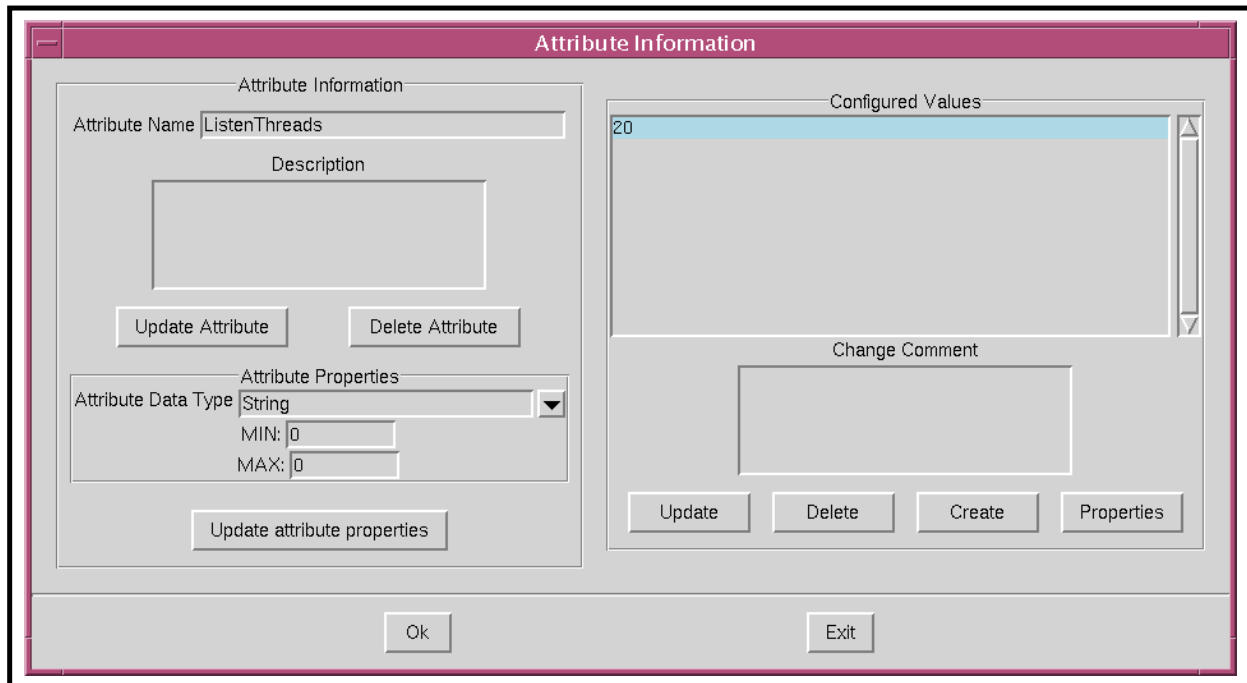


Figure 4.7-3. Configuration Registry Attributes Pop-Up Window

- 2 In the Database Login window click in the **Password:** field and type the password.
 - The typed password is not displayed (dots are displayed in place of the password).
- 3 Click on the **Sign On** button.
 - The Database Login window is closed and the Configuration Registry GUI is displayed.
- 4 On the tree showing system hosts displayed on the left side of the GUI, click on the "+" sign next to one of the hosts for which parameters are to be displayed.
 - The tree displays a **config** branch.
- 5 Click on the "+" next to **config**.
 - The tree displays a **CFG** branch.
- 6 Click on the "+" next to **CFG**.
 - The tree displays the computer software components for the selected host.
- 7 Click on one of the listed components (or its folder icon).
 - The **Attribute Listing** field displays the configuration parameters associated with the selected component. (See Figure 4.7-3.)
 - If there are a large number of parameters, the right side of the window will have a scroll bar that may be used to scroll down the list.

- 8 Click on one of the listed parameters.
 - The **Attribute Information** pop-up window for the selected parameter is displayed, showing detailed information concerning the parameter.
 - If you are logged in with an account authorized with appropriate permissions, the **Attribute Information** window permits changing or deleting the parameter.
 - 9 To exit from the Configuration Registry GUI, follow menu path **File→Exit**.
-

4.8 Working with Indexes, Segments, and Caches

Table 4.8-1, below, provides an Activity Checklist for working with indexes, segments, and caches.

Table 4.8-1. Working with Indexes, Segments, and Caches - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|------------------------------------|-------------|-----------|
| 1 | DBA | Delete an Index | (P) 4.8.1.1 | |
| 2 | DBA | Create Database Segments (Example) | (P) 4.8.3 | |

4.8.1 Delete an Index

An index provides a means of locating a row in a database table based on the value of a specific column(s), without having to scan all data in the table. When properly implemented, indexes can significantly decrease the time it takes to retrieve data, thereby increasing performance. Sybase allows the definition of two types of indexes:

- *Clustered index, where the rows in a database table are physically stored in sequence determined by the index.* The ASE Server continually sorts and re-sorts the rows of a table so that their physical order is always the same as their logical (or indexed) order. Clustered indexes are particularly useful when data are frequently retrieved in sequential order. Only one clustered index can be defined for a table.
- *Non-clustered indexes differ from their clustered counterpart in that the physical order of rows is not necessarily the same as their indexed order.* Each non-clustered index provides access to the data in its own sort order, giving the appearance of data in that physical order. Up to 249 non-clustered indexes can be defined for one table.

Clustered indexes allow faster searches than non-clustered indexes. Clustered indexes are often called the primary key of the table. If you don't specify which type of index you want, it will be a non-clustered index by default.

There are a lot of options for creating an index, but the most commonly used one is unique. Both clustered and non-clustered indexes can be unique. *A unique index prohibits duplicate values in*

the column that the index is on. They cannot be created on text or image datatypes because those datatypes cannot reliably be declared unique.

Index keys need to be differentiated from logical keys. Logical keys are part of the database design, defining the relationships between tables: primary keys, foreign keys, and common keys. *When you optimize your queries by creating indexes, these logical keys may or may not be used as the physical keys for creating indexes.* You can create indexes on columns that are not logical keys, and you may have logical keys that are not used as index keys.

Tables that are read-only or read-mostly can be heavily indexed, as long as your database has enough space available. If there is little update activity, and high select activity, you should provide indexes for all of your frequent queries. Be sure to test the performance benefits of index covering.

Also, remember that with each insert, all non-clustered indexes have to be updated, so there is a performance price to pay. The leaf level has one entry per row, so you will have to change that row with every insert.

4.8.1.1 Delete an Index:

- 1** To delete an index, type **drop index**.
 - 2** Type the table name that has the index, a period, and the index name that you want to delete.
 - 3** Type **go** then press **Enter**.
-

4.8.2 Create Database Segments (Example)

Segments are named subsets of the database devices available to a particular ASE Server database. A segment can best be described as a label that points to one or more database devices.

Segmenting can increase ASE Server performance and give the SA or DBA increased control over placement, size and space usage of specific database objects. For example:

- If a table is placed on one device and its non-clustered indexes on a device on another disk controller, the time required to read or write to the disk can be reduced since disk head travel is usually reduced.
- If a large, heavily used table is split across devices on two separate disk controllers, read/write time may be improved.
- The ASE Server stores the data for text and image columns on a separate chain of data pages. By default, this text chain is placed on the same segment as the table. Since reading a text column requires a read operation for the text pointer in the base

table and an additional read operation on the text page in the separate text chain, placing the text chain on a separate physical device can improve performance.

Segments are created within a particular database from the database devices already allocated to that database. Each ASE Server database can contain up to 32 segments. The database devices must first be initialized with **disk init** and then be made available to the database with a **create database** or **alter database** statement segment names can be assigned.

When a database is first created, the ASE Server creates three segments in the database:

- System, which stores the database's system tables.
- Logsegment, which stores this database's transaction log.
- Default, which initially stores all other database objects.

Additional segments can be created. Subsystem databases, for example, consist of the following:

- Default data segment used if no other segment specified in the create statement.
- SYSLOGS, transaction logs.
- System tables and indexes.
- OPS mode data and index segments.
- TS1 mode data and index segments.
- TS2 mode data and index segments.

If tables and indexes are placed on specific segments, those database objects cannot grow beyond the space available to the devices represented by those segments, and other objects cannot contend for space with them. Segments can be extended to include additional devices as needed. Thresholds can be used to provide warnings when space becomes low on a particular database segment.

In the following example procedure, the DBA receives a request to create a segment for the storage of the SubServer table indexes in the t1ins01_svr database on a separate physical disk. Two devices, **subserver_data** and **subserver_index**, have already been created and are located on different physical disks.

In order to perform the procedure, the DBA must have obtained the following information:

- Name of database
- Database device extents
- Space on the database allocated to the Database device

To create a database, the DBA must have **sa_role**:

4.8.3 Create Database Segments (Example)

- 1 At the UNIX prompt, type **cd ASE-12_5/scripts** and then press **Return**.
- 2 Using the text editor of your choice, edit **segment.sql** and make changes to information enclosed in brackets (including the brackets) as appropriate.
- 3 After the changes have been made, save the file according to the rules of the text editor.

- 4 At the UNIX prompt, type: **isql -U<username> -S<ServerName> -iSegment.sql -oSegment.out** and then press **Return**.
 - The system will prompt you for a password.
 - 5 At the **Password:** prompt, type the *<password>*, then press **Return**.
 - When the UNIX prompt is again displayed the process is complete.
 - 6 At the UNIX prompt, type **more Segment.out** , then press **Return**.
 - This allows you to view the *Segment.out* file to confirm that the device has been created or to check for database creation errors.
-

Figure 4.8-1 shows an example of creation of a database segment template file.

```
/* **** */
/* name: [segment.sql] */
/* purpose: */
/* written: */
/* revised: */
/* reason: */
/* **** */

sp_addsegment [seg_name], [DBname],[Device Name]
```

Figure 4.8-1. Example of Creation of a Database Segment Template File

After the segment has been defined in the current database, the **create table** or **create index** commands use the optional clause “**on segment_name**” to place the object on a particular segment. Syntax:

```
create table table_name (column_name datatype ...) [on segment_name]
create [clustered | nonclustered] index index_name on table_name (columns)
```

Use **sp_helpdb** database_name to display the segments defined for that database.

Use **sp_helpsegment** segment_name to list the objects on the segment and show the mapped devices.

4.8.4 Caches

A cache is a block of memory that is used by Sybase to retain and manage pages that are currently being processed. By default, each database contains three caches:

- Data caches retain most recently accessed data and index pages
- Procedure caches retain most recently accessed stored procedure pages
- User transaction log caches are transaction log pages that have not yet been written to disk for each user

The size of each of these default caches is a configurable item that must be managed on a DAAC-by-DAAC basis. These caches can be increased or decreased as needed. The data cache can be further subdivided into named caches. *A named cache is a block of memory that is named and used by the database management system (DBMS) to store data pages. The named data caches can be used only by databases or database objects that are explicitly bound to them. All objects not explicitly bound to named data caches use the default data cache.* A database, table, index, or text or image page chain can be bound to a named data cache.

Assigning a database table to named cache causes accessed pages to be loaded into memory and retained. Named caches greatly increase performance by eliminating the time associated for disk input and output (I/O).

4.9 Backing Up and Recovering Data

Database and transaction log backups and recoveries are probably the most important tasks the DBA must perform. Without regular and complete backups of databases and transaction logs, the potential for enormous amounts of data to be lost is very great. How often you back up a database depends on how frequently the data is updated and how costly it would be to lose it. Databases that are constantly being modified need to be backed up frequently; databases containing relatively static data can be backed up less frequently. You should regularly back up production databases, for example. If you experience a media failure, you can restore the data from the most recent backups the **restore** command. You do not have to shut down servers to back up or restore a database. The Backup Server makes it possible to perform online backup and restore operations while the Adaptive Server is running.

Table 4.9-1, below, provides an Activity Checklist for backing up and recovering data.

Table 4.9-1. Backing Up and Recovering Data - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|--|-------------|-----------|
| 1 | DBA | Perform Automatic Backups | (P) 4.9.2 | |
| 2 | DBA | Perform Manual Backups | (P) 4.9.3.1 | |
| 3 | DBA | Perform a User Database Recovery (Order of Procedures) | (P) 4.9.4.1 | |
| 4 | DBA | Perform a User Database Recovery (Example) | (P) 4.9.5.1 | |
| 5 | DBA | Create a User Database (Example) | (P) 4.9.6 | |

4.9.1 Perform Automatic Backups

Each DAAC is responsible for determining its own backup schedule to meet its individual requirements. It is strongly suggested that a regular schedule of database backups be established and maintained. Although the databases are included in the daily backups of the entire system, separate database backups should be performed nightly.

Database backups are run by a UNIX **cron** job which executes the **EcCoSyb_DumbDb** program located in the **\$/usr/ecs/CUSTOM/dbms/COM/DBAdmin** directory. No intervention in the automatic backup process is required by the DBA, though periodic checks of the backup subdirectories are recommended.

Manual backups can be performed at any time by the DBA and are recommended for the following situations:

- Any change to the master database, including new logins, devices, and databases.
- Any major change to user databases, such as a large ingest or deletion of data, definition of indexes, etc.
- Other mission-critical activities as defined by the DAAC operations controller.

The following are procedures and scripts files that are currently being used for Sybase backups. There are **cron** jobs running at all Sybase servers that have ASE server installed. All dump files are currently written to local machine. The site DBA is responsible for configuring the backup dump to the remote Sybase directory.

4.9.2 Performing Automatic Backups

1 Check if **crontab** is up and running.

> **crontab -l**

- The output will look something like the following:
019 * * 1-6 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_DumpDb
012 * * 1-6 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_DumpTran
021 * * 1-5 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_CkErrorLog

2 If **crontab** is not running, enter:

> **crontab /usr/ecs/OPS/COTS/sybase/run_sybcron**

- The files shown in Table 4.9-2 will be installed by ECS Assistant to the directory **/usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin**:

Table 4.9-2. Automatic Backup Files (1 of 2)

| Script | Description |
|--------------------|---|
| EcCoDbSyb_SetupKsh | This file contains the SYBASE and DSQUERY (server) environment setup. This file is called by EcCoDbSyb_DumpDb, EcCoDbSyb_DrumpTran, and EcCoDbSyb_CkErrorLog scripts. |

Table 4.9-2. Automatic Backup Files (2 of 2)

| Script | Description |
|---|---|
| EcCoDbSyb_DumpDb | This script contains the code to dump the databases. First, it checks for any DBCC error on the master database, if there is any error on the master, the script sends an email to the DBA and exits the program. If the master database dump was successful, then the rest of the databases are dumped. Each database has a DBCC check; if there is any error on the database then the database is NOT dumped and an email is sent to the DBA. At the end, a status email is sent, providing all the database names that were successfully dumped. |
| EcCoDbSyb_DumpTran | This script contains the code to dump the transaction logs. This dumps the transaction logs for each database, it checks the error log file; if the error Msg is 4207 or 4221 it does a dump of the database first, then it does the transaction dump. If there is any other error Msg then the transaction dump fails and email is sent. At the end, the status of the transaction log dumps is emailed to the DBA. |
| EcCoDbSyb_SedFile | This file contains all the databases that don't need to be dump (i.e., temp, model, etc.) |
| EcCoDbSyb_DboMail | This file contains the email list of all the DBAs. |
| EcCoDbSyb_DbStat | This script updates the index table of a database. This script is called from EcCoDbSyb_DumpDb after each successfully database dump. |
| EcCoDbSyb_CkErrorLog | This script checks for specific database error messages from the Sybase Error Log File every hour and emails the error messages to the DBAs in the EcCoDbSyb_DboMailfile. |
| EcCoDbSyb_tran_log.awk | This script matches the current hour with the hour the error messages were generated in the Error Log File. If errors found, the messages are saved in a mail file and sent to DBAs. |
| 0 0 * * 1-6 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_DumpDb 0 10,13,16 * * 1-6 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_DumpTran 0 * * * 1-6 /usr/ecs/OPS/CUSTOM/dbms/COM/DBAdmin/EcCoDbSyb_CkErrorLog NOTE: Make sure there is an OPS mode directory with all script files. | |

- 3 Modify the files shown in Table 4.9-3 before running any of the scripts shown in Table 4.9-2.

Table 4.9-3. Files That Need to Be Modified before Running Scripts

| File | Modification |
|--------------------|--|
| EcCoDbSyb_SetupKsh | Make user you have the SYBASE files under /usr/ecs/OPS/COTS/sybase |
| EcCoDbSyb_SedFile | Add any other database that might not need to be backed up. The databases that are listed in this file do not need to be backed up. |
| EcCoDbSyb_DboMail | Add/delete the email of the DBA and any other email that might need to be added/deleted. All the errors and status are sent to them. |

ASE Server backups are performed nightly by a **cron** job which runs the **sybcron** program located in the **\$SYBASE/** directory. The following table of definitions (Table 4.9-4) is used throughout the rest of this section.

Table 4.9-4. Automatic Backup Components

| Name | Function |
|------------------|--|
| sybcron | File added with the crontab -e command, contains several executable cron commands. Example: 00 19 * * 1-6 /data1/COTS/sybase/sybasedump |
| EcCoDbSyb_DumpDb | Controlling script that performs the following functions: run isql to create the Backup Statements run isql to execute the Backup Statements record the results of the Backup Statements in Backup Files copy the Backup Files to the Backup Subdirectory create the Backup Summary greps successful Dump statements along with any errors generated, sends e-mail to the DBA and writes them to the backup_summary file |
| sp | ASE Server password file - contains password for backup role |

4.9.3 Perform Manual Backups

Both the **dump database** and **dump transaction** command processing are off-loaded to the backup server and will not affect normal operations of the database. These commands are performed by the System Administrator on appropriate databases using the following syntax.

```
1> dump database master to
   "compress::/usr/ecs/OPS/COTS/sybase/sybase_dumps/dumps/dbname.dat.compress
   .MMDDHHMM"
2> go
```

4.9.3.1 Perform Manual Backups

- 1 Log on to a local host.
 - 2 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY ServerName:0.0**, then press **Return**.
 - 3 Log into the server that contains the database to be backed up by typing: **/tools/bin/ssh gsfcsparc5.gsfcmo.ecs.nasa.gov**, then press **Return**.
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 4.
 - If you have not previously set up a secure shell passphrase, go to Step 5.
 - 4 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your *Passphrase* and then press the **Enter** key.
 - Go to step 6.
 - 5 At the **<user@remotehost>'s password:** prompt, type your *Password* and then press the **Enter** key.
 - 6 Log into Sybase by typing: **su-sybase**, then press **Return**.
 - A password prompt is displayed.
 - 7 Enter *SybasePassword* then press **Return**.
 - Remember that *SybasePassword* is case-sensitive.
 - You are authenticated as yourself and returned to the UNIX prompt.
 - Your new home directory is **/usr/ecs/OPS/COTS/sybase** and all required environment variables have been set.
 - 8 At the UNIX prompt, type **isql -Usa** then press **Return**.
 - 9 To backup the database, at the isql prompt, type **dump database DBName to "compress::/BackupDirectory/DBName.dat"**, then press **Return**.
 - 10 Type **go**, then press **Return**.
 - 11 To backup the transaction log, at the isql prompt, type **dump transaction DBName to "compress::/BackupDirectory/DBName_tx.dat"**, then press **Return**.
 - 12 Type **go**, then press **Return**.
-

4.9.4 Perform a User Database Recovery (Order of Procedures)

Database recovery is performed when the Database Administrator determines that some database data is corrupt or when the System Administrator determines that a database device has failed. The System Administrator makes a request to the Database Administrator, who performs the restore and notifies the System Administrator when the restore is complete.

The symptoms of media failure are as variable as the causes. If only a single block on the disk is bad, your database may appear to function perfectly for some time after the corruption appears; this is why you should run **dbcc** commands frequently. If an entire disk or disk controller is bad, you will not be able to use a database. ASE Server marks it as suspect and displays a warning message. If the disk storing the master database fails, users will not be able to log into the server, and users already logged in will not be able to perform any actions that access the system tables in master.

4.9.4.1 Perform Database Recovery

- 1 The device failure has been verified by the System Administrator and restoration has been requested from the DBA.
 - 2 If possible, perform a dump of the current database and the current database transaction log for each database on the failed device to be restored. If this is not possible due to the damage to the database device, then the DBA will have to use the most recent database and transaction log dumps.
 - 3 If possible, the DBA examines the space usage for each database on the failed device. The same defaults should be set when the new database device(s) is (are) created.
 - 4 The DBA drops the database(s) on the failed device, then the database device itself is dropped.
 - 5 The DBA initializes a new database device. This is why it is important to keep the device creation scripts.
 - 6 The DBA recreates each user database on the new database device. This is why it is important to keep the user creation scripts.
 - 7 Each database is reloaded with data from the database backups and the transaction log backups. It is this procedure that is detailed below.
 - 8 The DBA notifies the System Administrator when the database restoration is complete.
-

In order to perform the procedure, the DBA must have obtained the following information:

- Name of database device that has failed

- Name of the replacement device
- Name of the databases that reside on the failed device
- Name of the backup volumes
- Name of the dump files on the backup volumes

Manual recovery of a user database is performed by the System Administrator by the use of the **load database** and **load transaction** commands. For issues concerning the **master** database, please consult your System Administrator's Guide for assistance. It is recommended that any user database to be recovered be dropped and created with the **for load** option. The **databasename.sql** along with any **alter.databasename.sql** scripts can be combined into one script which will re-create the user database with the **for load** option. This will insure the success of the **load database** and **load transaction** commands.

4.9.5 Perform a User Database Recovery (Example)

In the example procedures that follow, the database **UserDB** was created using the following script excerpt (stored in `home/scripts/create.databases/userdb.sql`):

```
create database UserDB on data_dev1 = 100 log on tx_log1 = 50 [with override]
```

and was modified using the following script excerpt (`home/scripts/create.databases/alteruserdb.sql`):

```
alter database UserDB on data_dev1=50
```

For the purposes of this example, the full database backup and transaction log dumps were successful and located in `/usr/ecs/OPS/COTS/UserDB.dat` and `UserDB_tx.dat`.

4.9.5.1 Perform a User Database Recovery (Example)

- 1 In the `$SYBASE/ASE-12_5/scripts/` directory, make a script file to load database and save template for future use.

- Syntax:

```
% cd /usr/ecs/OPS/COTS/sybase/scripts/,  
% cp template.sql userdb_for_load.sql.
```

NOTE: If template does not exist, vi `userdb_for_load.sql`.

- 2 Modify appropriate items so that the script file resembles the following:

```
create database UserDB on data_dev2=100 log on tx_log2=50 for load  
go  
alter database UserDB on data_dev3=50  
go
```

- 3 Save the script in `$SYBASE/ASE-12_5/scripts/create.databases/userdb_for_load.sql`

- 4 Run the script from the UNIX command prompt.
`%isql -Usa -Sservername -iuserdb_for_load.sql -ouserdb_for_load.out`
 - 5 Check the **userdb_for_load.out** file for success.
 - 6 Load the database from the full backup.
1> load database UserDB from
“compress::/usr/ecs/OPS/COTS/sybase/sybase_dumps/week1/dbname.dat.MMDDH
HMM”
2> go
 - 7 Load the transaction file from the transaction file dump.
1> load transaction UserDB
from“compress::/usr/ecs/OPS/COTS/sybase/sybase_dumps/week1/dbname.tran.MMDDH
HMM”
2> go
-

4.9.6 Create a User Database (Example)

- 1 Log on to a local host.
- 2 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY ServerName:0.0**, then press **Return**.
- 3 Log into the server on which the new database device is to be created by typing:
/tools/bin/ssh <ServerName>, then press **Return**.
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 4.
 - If you have not previously set up a secure shell passphrase, go to Step 5.
- 4 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your *Passphrase* and then press the **Enter** key. Go to step 6.
- 5 At the **<user@remotehost>'s password:** prompt, type your *Password* and then press the **Enter** key.

NOTE: For each database device to be created, perform Steps 6 through 9:

- 6 At the UNIX prompt, type **cd /ASE-12_5/** then press **Return**.
 - This place you in the directory that contains all the scripts used to create database devices.

- It is important that these scripts not be deleted from the system in case it is necessary to restore a database device following a failure (see **Restore Databases**).

7 Using the text editor of your choice, edit **DBName.sql** and make changes to information enclosed in brackets (including the brackets) as appropriate (see Figure 4.9-1).

- **DBName** is the name of the database and should describe its function succinctly.
- **DBDeviceName** is the name of the existing, approved database device on which **DBName** will reside.
- **DBSize_in_MB** is the estimated size of the database in megabytes.
- **LogDBDeviceName** is the name of the database device holding the transaction log
- **LogSize_in_MB** is the estimated size of the transaction log in megabytes.
- The **sp_helpdb** command provides feedback at the end of the script to assure that the database has been created.

```

/* ***** */
/* name: template.sql */
/* purpose: */
/* written: */
/* revised: */
/* reason: */
/* ***** */
create database database_name
on data_dev = size, /* in MB */
log on log_dev = size
go
sp_helpdb database_name
go

```

Figure 4.9-1. Sample template.sql File for Creation of a Database

8 After the changes have been made, save the file according to the rules of the text editor.

9 At the UNIX prompt, type:

isql -U<username> -S<ServerName> -iDBName.sql -oDBName.out

then press **Return**.

- **ServerName** is the name of the server on which the database device will be created.
- **DBName.sql** is the name of the script file you created in step 8.
- **DBName.out** is the filename of the script's output for confirmation and/or troubleshooting purposes. The system will prompt you for a password.

- 10 At the **Password:** prompt, type the *<password>* then press **Return**.
 - When the UNIX prompt is again displayed the process is complete.
 - 11 At the UNIX prompt, type **more DBName.out** then press **Return**.
 - This allows you to view the *DBName.out* file to confirm that the device has been created or to check for database creation errors.
-

A sample of a completed **Create Database** script is shown in Figure 4.9-2.

```
/* **** */
/* name: test_db.sql */
/* purpose: create a database for testing */
/* written: 12/19/97 */
/* revised: */
/* reason: */
/* **** */
create database test_db
on test_dev = 3
go
sp_helpdb test_db
go
```

Figure 4.9-2. Completed Create Database Script

4.10 Establishing Database Security

Permissions control access within a database. There are two types of permissions within a database: object and command. Object privileges control select, insert, update, delete, and execute permissions on tables, views, and stored procedures. Command permissions control access to the create statements for databases, defaults, procedures, rules, tables, and views. Access controls allow giving various kinds of permissions to users, groups, and roles with the **grant** command. The **revoke** command rescinds these permissions.

The ability to assign permissions for the commands is determined by each user's status (e.g., system administrator, database owner, database object owner) and by whether or not a particular user has been granted a permission with the option to grant that permission to other users.

Groups are a means of logically associating users with similar data access needs. Once a group has been defined, object and command permissions can be granted to that group. A user who is member of a group inherits all of the permissions granted to that group.

Roles provide a structured means for granting users the permissions needed to perform standard database-related activities and also provide a means for easily identifying such users. They provide a means of enforcing and maintaining individual accountability. There are six pre-defined roles shown in Table 4.10-1 that may be assigned to a user. Other unique roles can be created and granted to users, groups of users, or other roles. In addition, role hierarchies can be defined. This enables a user assigned one role to automatically have the privileges available to all other roles lower in the hierarchy. Mutually exclusive roles can also be defined. This can be done in terms of membership – a single user cannot be granted both roles – or activation – a single user can be granted two roles but cannot enable both (e.g., both cannot be enabled simultaneously).

Table 4.10-1. Roles and Privileges

| Roles | | Privileges |
|--------------------------|------------------|---|
| System Administrator | sa_role | Grant a specific user permissions needed to perform standard system administrator duties including: Installing SQL server and specific ASE server modules Managing the allocation of physical storage Tuning configuration parameters Creating databases |
| Site Security Officer | sso_role | Grant a specific user the permissions needed to maintain ASE server security including: <ul style="list-style-type: none"> • Adding server logins • Administrating passwords • Managing the audit system • Granting users all roles except the sa_role |
| Operator | oper_role | Grant a specific user the permissions needed to perform standard functions for the database including: <ul style="list-style-type: none"> • Dumping transactions and databases • Loading transactions and databases |
| Navigator | navigator_role | Grant a specific user the permissions needed to manage the navigation server |
| Replication | replication_role | Grant a specific user the permissions needed to manage the replication server |
| Sybase Technical Support | sybase_ts_role | Grant a specific user the permissions needed to execute database consistency checker (dbcc), a Sybase supplied utility supporting commands that are normally outside of the realm of routine system administrator activities |

Table 4.10-2, below, provides an Activity Checklist for establishing database security.

Table 4.10-2. Establishing Database Security - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|--|--------------|-----------|
| 1 | DBA | Grant or Revoke Database Access Privileges | (P) 4.10.1.1 | |
| 2 | DBA | Create an ASE Server Login | (P) 4.10.2.1 | |
| 3 | DBA | Change a Password | (P) 4.10.3.1 | |
| 4 | DBA | Perform Auditing | (P) 4.10.4.1 | |

4.10.1 Grant or Revoke Database Access Privileges

The DBA uses the **grant** and **revoke** statements to control permissions. The syntax for grant and revoke statements is similar:

```
grant {all [ privileges] | command_list} to {public | name_list | role_name}
revoke {all [ privileges] | command_list} from { public | name_list | role_name}.
```

4.10.1.1 Granting or Revoking Database Access Privileges

- 1 Determine the privileges that you want to grant and to which user(s).
- 2 Log on to a local host.
- 3 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY ServerName:0.0**, then press **Return**.
- 4 Log into the server where the user database resides by typing: **/tools/bin/ssh ServerName**, then press **Return**.
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 5.
 - If you have not previously set up a secure shell passphrase, go to Step 6.
- 5 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your **Passphrase** and then press the **Enter** key.
 - Go to step 7.
- 6 At the **<user@remotehost>'s password:** prompt, type your **Password** and then press the **Enter** key.
- 7 At the UNIX prompt, type **su-sybase** then press **Return**.
 - A password prompt is displayed.

- 8 Enter *SybasePassword*, then press **Return**.
 - You are authenticated as yourself and returned to the UNIX prompt.
 - Your new home directory is **/usr/ecs/OPS/COTS/sybase** and all required environment variables have been set.
- 9 At the UNIX prompt, type **isql -Usa**, then press **Return**.
- 10 At the **Password:** prompt, type the *SybaseSAPassword* then press **Return**.
 - Note: the *SybaseSAPassword* is case-sensitive.
- 11 If you are granting privileges, at the isql prompt, type **grant Privilege to LoginName** then press **Return**.
 - If more than one privilege is to be granted, repeat this step on subsequent lines.
- 12 If you are revoking privileges, at the isql prompt, type **revoke Privilege from Logname** then press **Return**.
 - If more than one privilege is to be revoked, repeat this step on subsequent lines.
- 13 When all privileges have been assigned, type **go** then press **Return**.

NOTE: It is recommended that the DBA store the privilege granting and revoking commands in **.sql** files in the **\$SYBASE/ASE-12_5/scripts/..** directory along with their results.

4.10.2 Create an ASE Server Login

A user is given a login account with a unique ID. All of that user's activity on a server can be attributed to his or her server user ID and audited. Passwords are stored in the **master..syslogins** table in encrypted form. When users log in from a client, they can choose client-side password encryption before sending the password over the network. A user can be granted the ability to impersonate another user. This proxy authorization allows administrators to check permissions for a particular user or to perform maintenance on a user's database objects. Application servers can execute procedures and commands on behalf of several users.

Providing users with access to ASE servers and their databases consists of the following steps:

- A server login account for a new user is created.
- The user is added to a database and optionally assigned to a group.
- The user or group is granted permissions on specific commands and database objects.

The user needs an ASE Server login to access the DBMS. The login is assigned to a user with the related permissions. During initial database installation, logins used by the custom code were created and permissions assigned for access to subsystem databases. In addition, special database installation logins, **<SUBSYS>_role**, were created to support database installation needs. For each login, the level of access is limited to that associated with their login, group or assigned

group/role. Object permissions are set within the installation scripts of the <SUBSYS> subsystem for each object and group/role.

In order for a user to connect to an ASE Server, a login must be created by the DBA. That login must then be assigned to particular database(s) that the user will access. All login details are stored in the syslogins table in the **master** database. Two stored procedures are required:

- The stored procedure **sp_addlogin** adds new login names to the server but does not grant access to any user database. Syntax:
sp_addlogin login_name, password, [,default database ,language, fullname]
- The stored procedure **sp_adduser** adds the user. Syntax:
sp_adduserlogin_name [username, group_name]
go

4.10.2.1 Create an ASE Server Login

- 1 Log on to a local host.
- 2 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY ServerName:0.0**, then press **Return**.
- 3 Log into the server for which a new login procedure is to be created up by typing: **/tools/bin/ssh ServerName**, then press **Return**.
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 4.
 - If you have not previously set up a secure shell passphrase, go to Step 5.
- 4 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your **Passphrase** and then press the **Enter** key. Go to step 6.
- 5 At the **<user@remotehost>'s password:** prompt, type your **Password** and then press the **Enter** key.
- 6 At the UNIX prompt, type **su-sybase** then press **Return**. A password prompt is displayed.
- 7 Enter **SybasePassword** then press **Return**.
 - Note: **SybasePassword** is case-sensitive.
 - You are authenticated as yourself and returned to the UNIX prompt.
 - Your new home directory is /usr/ecs/OPS/COTS/sybase and all required environment variables have been set.
- 8 At the UNIX prompt, type **cd ASE-12_5/scripts/server.users** then press **Return**.

- 9 Using the text editor of your choice, edit ***UserName.sql*** (see Figure 4.10-1) and make changes to information enclosed in brackets (including the brackets) as appropriate:
- 10 After the changes have been made, save the file according to the rules of the text editor.

```
/* **** */
/* name: [template.sql] */
/* purpose: */
/* written: */
/* revised: */
/* reason: */
/* **** */
    sp_addlogin [login name], [password], [default database]
go
    use [default database]
go
    sp_adduser [login name]
go
    /* the following is optional, by database */
    sp_changegroup [group name], [login name]
go
    sp_helpuser
go
```

Figure 4.10-1. Sample *template.sql* File for New Database User Login

- 11 At the UNIX prompt, type ***isql -Usa -SServerName -iUserName.sql -oUserName.out*** then press **Return**.
 - ***ServerName*** is the name of the server on which the master database is stored.
 - ***UserName.sql*** is the name of the script file you created in Step 9.
 - ***UserName.out*** is the filename of the script's output for confirmation and/or troubleshooting purposes.
 - The system will prompt you for a password.
 - 12 At the Password: prompt, type the ***SybaseSAPassword*** then press **Return**.
 - When the UNIX prompt is again displayed the process is complete.
 - 13 At the UNIX prompt, type ***more UserName.out*** then press **Return**.
 - This allows you to view the ***UserName.out*** file to confirm that the user login has been created or to check for user login creation errors.
-

4.10.3 Change a Password

One of the most common problems a DBA encounters is a user who cannot connect to an ASE Server. The following procedure is applicable.

4.10.3.1 Changing a Password

- 1 At the UNIX prompt, type **isql -Udbastudent** then press **Return**.
 - The system will prompt you for a password.
- 2 At the **Password:** prompt, type the *dbastudentpassword* then press **Return**.
- 3 At the Sybase prompt, type the following:
sp_password old-password, new-password

NOTE: The dba (or any user with sso_role) may change another user's password with the following syntax: (this is the most common activity performed)

sp_password sso_role password, new-password, login name

4.10.4 Perform Auditing

A comprehensive audit system is provided with Adaptive Server. The audit system consists of a system database called sybsecurity, configuration parameters for managing auditing, a system procedure, **sp_audit**, to set all auditing options, and a system procedure, **sp_addauditrecord**, to add user-defined records to the audit trail. When you install auditing, you can specify the number of audit tables that Adaptive Server will use for the audit trail. If you use two or more audit tables to store the audit trail, you can set up a smoothly running audit system with no manual intervention and no loss of records.

A System Security Officer manages the audit system and is the only user who can start and stop auditing, set up auditing options, and process the audit data. As a System Security Officer, you can establish auditing for events such as:

- Server-wide, security-relevant events.
- Creating, deleting, and modifying database objects.
- All actions by a particular user or all actions by users with a particular role active.
- Granting or revoking database access.
- Importing or exporting data.
- Logins and logouts.

The following statements represent examples for performing auditing:

4.10.4.1 Perform Auditing

- 1 Run **installsecurity** auditing located under **\$SYBASE/ASE-12_5/scripts**.
 - 2 Add a login for auditing:
sp_addlogin ssa, ssa_password, sybsecurity
use sybsecurity
sp_changedbowner ssa
sp_role "grant", sso_role, ssa
 - 3 Enable auditing:
sp_configure "auditing", 1
sp_audit "cmdtext", "dbo", "on"
 - 4 **You can test via these next few steps:** Create a table in a database with one field.
 - 5 Grant all on the table for the **loginname**.
 - 6 Log into isql using the **loginname**.
 - 7 **Insert a record** into the table.
 - 8 Log into isql as **ssa**.
 - 9 Select * from **sysaudits** where **loginname** = "**loginname**"
-

NOTE: Once auditing is turned on, the **sysaudit** tables will get filled up very quickly. The database option, options of **trunc log on chkpt** needs to be turned on in the **sybsecurity** database so that the **logsegment** of this database can be cleaned up upon checkpoint. This **logsegment** can also be cleaned up by means of transaction dumps if the database is installed on two separate disk devices. Also, as soon as auditing is turned on, a **cron** job needs to be turned on at the same time to **bcp** out and truncate the **sysaudit** table. This is very important.

4.10.5 EMD Security Directive

All System Administrators and Database Administrators at the sites are responsible for reasonable security measures when installing custom software. This means:

- Changing the permissions of online secure files to the minimum level required.
- Backing up secure file(s) to removable media (floppy or tape) and removal of secure files immediately after installation is complete and then keeping the removable medium in a secure location.

The following file is affected as result of this requirement on the EMD program:

```
/usr/ecs/<MODE>/CUSTOM/dbms/<SUBSYSTEM>/Ec<server>SybaseLogins.sql
```

Set permissions to 711 (user read, write, execute; group and other read only).

4.11 Copying, Replicating, and Extracting Data

To create an exact copy of a database (Individual Databases):

- Dump the existing database.
- Create a database to load with this dump.

The new database does not have to be the same size as the original. The only requirement is that the destination database must be at least as large as the dumped database and have the same beginning fragments as the original database. This information can be obtained from saved database creation scripts or by running the following command:

```
select segmap,'Size in MB'=size/512 from sysusages where dbid= db_id("database_name")
```

4.11.1 Copying a Database (Example)

A database was created with the following statement:

```
create database dbname on datadevice1 = 1000,  
log on Logdevice1 = 200  
go  
alter device dbname on datadevice2 = 500    running:  
select segmap,'Size in MB'=size/512 from sysusages  
where dbid= db_id("dbname")  
would return:segmap  Size in MB  
3    1000  
4    200  
3    500
```

You could create a 3GB database as follows and load your database into it (using **for load** option will shorten database load time):

```
create database newdatabase on datadevice3 = 1000 log on logdevice3 = 200  
for load  
go  
alter database newdatabase on datadevice 3=500 for load  
go  
alter database newdatabase on datadevice4=300 for load  
go  
alter database newdatabase on datadevice5=1000 for load  
go  
load database newdatabase from dbname_dump  
go
```

4.12 Bulk Copying

Table 4.12-1, below, provides an Activity Checklist for bulk copying.

Table 4.12-1. Bulk Copying - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|----------------------|--------------|-----------|
| 1 | DBA | Perform Bulk Copying | (P) 4.12.1.1 | |

4.12.1 Perform Bulk Copying

The bulk copy (**bcp**) utility is located in the **\$SYBASE/OCS-12_5/bin** directory and is designed to copy data to and from ASE Server databases to operating system files. You must supply the following information for transferring data to and from ASE Server:

- Name of the database and table.
- Name of the operating system file.
- Direction of the transfer (in or out).

In order to use **bcp**, you must have an ASE Server account and the appropriate permissions on the database tables and operating system files that you will use. To copy data **into** a table, you must have **insert** permission on that table. To copy data **out** to an operating system file, you must have **select** permission on the following tables:

- The table being copied:
 - **sysobjects**
 - **syscolumns**
 - **sysindexes**

bcp syntax:

```
bcp [[database_name].owner.]table_name {in | out} datafile [-e errfile] [-n] [-c]
    [-t field_terminator] [-r row_terminator] [-U username] [-S server]
```

4.12.1.1 Perform Bulk Copying

- 1 Log on to a local host.
- 2 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** or **setenv DISPLAY ServerName:0.0**, then press **Return**.

- 3 Log into the server that contains the database to be backed up by typing: **/tools/bin/ssh *ServerName***, then press **Return**.
 - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 4.
 - If you have not previously set up a secure shell passphrase, go to Step 5.
 - 4 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your **Passphrase** and then press the **Enter** key.
 - Go to step 6.
 - 5 At the **<user@remotehost>'s password:** prompt type your **Password** and then press the **Enter** key.
 - 6 Set Login as sybase and cd to **/usr/ecs/OPS/COTS/sybase/scripts/**.
 - Note: **SybasePassword** is case-sensitive.
 - You are authenticated as yourself and returned to the UNIX prompt.
 - Your new home directory is **/usr/ecs/OPS/COTS/sybase** and all required environment variables have been set.
 - 8 Modify the [table name]_out script with the correct database name, table name, direction, and login name and save.
 - 9 Run the [table name]_out script and press **Return** for each of the prompts except the last.
 - 10 At the last prompt store [your responses] in a [table name].fmt file. This creates a format file for future bulkcopy activity.
 - 11 To copy the data to another already created table, repeat Steps 6, 7, and 8 with the following changes:
 - The direction is “in”
 - Use the optional **-f [format file name]**
-

4.13 Replication System Administration

Administering the replication system is primary the role of the Replication System Administrator (RSA). The Replication System Administrator installs, configures, and administers the replication system. Given the distributed nature of the MSS implementation this role may be performed by different people at different locations. If this is the case, various tasks for administering Replication Server may require coordination between Replication System Administrators.

The Replication System Administrator has **sa** user permissions, which provides that person with the ability to execute nearly all commands in the replication system. In managing the system, the

Replication System Administrator may need to coordinate with DBAs for both local and remote databases.

Replication System Administrators should be experienced Sybase DBAs and should have taken the Sybase training classes *Replication System Administration* and *Replication Disaster Recovery Workshop*. They should also have read and understood the manuals: *Replication Server Administration Guide*, *Replication Server Configuration Guide for UNIX Platforms*, *Replication Server Reference Manual*, and *Replication Trouble Shooting Guide*.

4.13.1 Replication System Administrator Tasks

Table 4.13-1 identifies tasks required to maintain a replication system:

Table 4.13-1. Replication System Administrator Tasks

| Task | Roles |
|---|--|
| Installing Replication Server | Replication System Administrator (RSA) |
| Adding or removing a Replication Server | RSA |
| Starting up and shutting down Replication Server. | RSA |
| Configuring Replication Server | RSA |
| Maintaining Routes (Creating and modifying) | RSA |
| Managing the RSSD | RSA |
| Adding a primary and replicate database. | RSA |
| Adding login names, database users, and administering appropriate permissions | RSA |
| Adding replicated tables or changing table schemas. Creating and modifying replicated tables Creating and modifying replication definitions Creating and materializing subscriptions at replicate sites. | RSA |
| Defining data server function-string classes and function strings. | RSA |
| Applying database recovery procedures. | RSA |
| Maintaining and monitoring database connections | RSA |
| Monitoring Replication Server | RSA |
| Processing rejected transactions | RSA |
| Quiescing Replication Server | RSA |
| Reconciling database inconsistencies. | RSA |

4.13.2 DAAC DBA Replication Roles and Tasks

The Database Administrator (DBA) supports some Replication Server administrator tasks. Table 4.13-2 lists tasks that the DBA administrators perform at the local DAACs with respect to replication server administration.

Table 4.13-2. DAAC DBA Replication Roles and Tasks

| Task | Roles |
|---|-------|
| Installing Replication Server | DBA |
| Managing the RSSD | DBA |
| Adding a primary and replicate database. | DBA |
| Adding login names, database users, and administering appropriate permissions | DBA |
| Adding replicated tables or changing table schemas. Creating and modifying replicated tables Creating and modifying replication definitions Creating and materializing subscriptions at replicate sites. | DBA |
| Defining data server function-string classes and function strings. | DBA |
| Applying database recovery procedures. | DBA |
| Processing rejected transactions | DBA |
| Quiescing Replication Server | DBA |
| Reconciling database inconsistencies. | DBA |

4.13.3 Database Replication

The MSS database is the only database to use replication. This is done so user profile and order tracking data can be shared among the DAACs.

Replication begins with definitions and subscriptions. *Replication definitions specify the tables and columns that may be replicated for a data recipient. Replications subscriptions specify which definitions the data recipient wishes to receive.* In addition, the replication database and server must be configured to support the potentially large volumes of data that will be transferred between the source and recipient databases.

The MSS replication definition and subscription scripts were developed as templates for installation at DAACs and the SMC. Since peer-to-peer configuration for MsAcUserProfile is required, the template approach was decided so that only those scripts that need to be implemented at each site are configured. The template files provide the necessary generic functions needed to configure the MSS MsAcUserProfile replication environment. Unix shell scripts have been developed to allow installers to pass the appropriate site-specific information (i.e. database name, replicate replication server name, etc.) when prompted. The Unix script then customizes the template script files for the specific site. The DD&M group has created naming conventions for all replication scripts and naming conventions for the subscriptions, replication definitions, and other objects related to the replication environment. Script names consist of the following conventions:

<action>.<SUBSYS>.<Replication Object>.<Primary Site ID>.sql.<Replicate Site ID>

4.14 Performance Monitoring, Tuning, and Problem Reporting

Databases are ubiquitous in the system, and performance has been addressed from the beginning of the project. Each database has an expected performance profile, including initial size, growth rates, transaction rates, and response times. Analysis of database performance generally takes a multi-tiered approach. At the lowest level, the data access patterns are analyzed and the database physical design is tailored for these access patterns. These activities occur during the design stage of the development. During the implementation phase, actual transactions are inspected to make sure that they are efficiently coded, and are consistent with the expected use of the database. Once implemented, the performance of the database is measured under various loads; performance is tuned by modifying various configuration parameters provided by the database management system, and in some cases by modifying the database design or the data access code.

Actual performance can be assessed from a response time perspective or a capacity perspective. Response times can be measured in a variety of ways. For some of the system databases, a direct user interface is available that will provide a basis for assessing response time performance—for example, searches provided through the client. For these cases, the analytical task becomes the separation of the database component of the response time from all other contributors. Other system databases do not have a direct user interface because they serve system internal functions; an example is the Subscription database. Response time performance for these databases may be measured using test drivers or by capturing timing marks from instrumented code as test threads are run through the system. Database capacity—usually measured as the number of transactions that the database can handle per second—is usually tested with test drivers, although it can also be measured when the system is put through thread tests, operational tests, or stress tests. Sybase monitoring tools can be used to measure the throughput of the system during such tests, although they add their own overhead and reduce the maximum capacity achievable. The Sybase monitoring tool collects an enormous wealth of information about the use of Sybase resources—everything from hardware (CPUs, memory, disk channels) to Sybase internally configured resources (cache blocks, spin locks, indexes). These resources can then be tuned according to the usage patterns observed (including the possible addition of hardware).

4.14.1 Monitoring

The easiest way to monitor performance is through the Monitor Server. The Monitor Server provides specific performance data on cache usage, network traffic, device I/O, and locking activity. *Performance is the measure of efficiency of an application or multiple applications running in the same environment.* Performance is usually measured in one of two ways:

- *Response time, which is the time that a single task takes to complete.*
- Throughput, which is the volume of work completed in a fixed time period, e.g. transactions per second (tps).

Most of your tuning efforts should address the amount of time it takes for the server to respond to queries.

You can run **sp_sysmon** both before and after tuning Adaptive Server configuration parameters to gather data for comparison. You can also use **sp_sysmon** when the system exhibits the behavior you want to investigate. In many tests, it is best to start the applications, and then start **sp_sysmon** when the caches have had a chance to reach a steady state. If you are trying to measure capacity, be sure that the amount of work you give the server keeps it busy for the duration of the test. Many of the statistics, especially those that measure data per second, can look extremely low if the server is idle during part of the sample interval. In general, **sp_sysmon** produces valuable information when you use it:

- Before and after cache or pool configuration changes.
- Before and after certain **sp_configure** changes.
- Before and after the addition of new queries to your application mix.
- Before and after an increase or decrease in the number of Adaptive Server engines.
- When adding new disk devices and assigning objects to them.
- During peak periods, to look for contention.
- During stress tests to evaluate an Adaptive Server configuration for a maximum expected application load.
- When performance seems slow or the system behaves abnormally.

4.14.2 Tuning

Response time can be shortened by reducing contention and waits times, particularly disk I/O wait times; using faster components; and reducing the amount of time the resources are needed. In some cases, Adaptive Server is optimized to reduce initial response time, that is, the time it takes to return the first row to the user. This is especially useful in applications where a user may retrieve several rows with a query and then browse through them slowly with a front-end tool. Other ways of increasing performance are summarized by system level in Table 4.14-1.

Table 4.14-1. Tuning Options

| Layers | Tuning Options |
|------------------|--|
| Application | Remote or replicated processing to move decision support off machine |
| | Stored procedures to reduce compilation time and network usage |
| | Minimum locking level that meets application needs |
| Database | Transaction log thresholds to automate dumps and avoid running out of space |
| | Thresholds for space monitoring in data segments |
| | Partitions to speed loading of data |
| | Devices to avoid disk contention, take advantage of I/O parallelism |
| Server | Tuning memory, most critical configuration parameters and other parameters |
| | Configuring cache sized and I/O sizes |
| | Scheduling batch jobs and reporting for off hours |
| | Reconfiguring parameters for shifting workload patterns |
| Devices | More medium-sized devices and more controllers for better I/O throughput |
| | Distributing databases, tables, and indexes for even I/O load across devices |
| | Segments, partitions for I/O performance on large tables used for parallel queries |
| Network | Configuring packet sizes to match application needs |
| | Configuring subnets |
| | Isolating heavy network uses |
| | Configuring for multiple network engines |
| Hardware | Configuring the housekeeper task to improve CPU use |
| | Configuring multiple data caches |
| Operating System | Choosing between files and raw partitions |
| | Increasing memory size |

4.15 Ensuring Database Quality

4.15.1 Integrity Monitoring

The Database Consistency Checker (**dbcc**) is a set of utility commands for checking the logical and physical consistency of a database. Use the **dbcc** commands:

- As part of regular database maintenance (periodic checks run by the System Administrator). These checks can detect, and often correct, errors before they affect a user's ability to use ASE Server.
- To determine the extent of possible damage after a system error has occurred.
- Before backing up a database.
- Because you suspect that a database is damaged. For example, if using a particular table generates the message "Table corrupt", you can use dbcc to determine if other tables in the database are also damaged.

The integrity of the internal structures of a database depends upon the System Administrator or Database Owner running database consistency checks on a regular basis. Two major functions of dbcc are:

- Checking allocation structures (the commands checkalloc, tablealloc, and indexalloc).
- Checking page linkage and data pointers at both the page level and row level (checktable and checkdb). The next section explains page and object allocation and page linkage.

The **dbcc** command is used in the database backup scripts to determine if the database is properly configured and without errors. If errors occur, the backup will not proceed and a message is sent to the DBA with notification of the problem.

4.16 Sybase Troubleshooting

4.16.1 Space Usage

Thresholds are defined on segments to provide a free space value at which a procedure is executed to provide a warning or to take remedial action. Use **sp_addthreshold** to define your own thresholds: **sp_addthreshold database_name, segment_name, free_space, procedure_name**, where **free_space** is the number of free pages at which the threshold procedure executes; **procedure_name** is the stored procedure which the threshold manager executes when the number of free pages falls below the **free_space** value.

Table 4.16-1, below, provides an Activity Checklist for Sybase troubleshooting.

Table 4.16-1. Sybase Troubleshooting - Activity Checklist

| Order | Role | Task | Section | Complete? |
|-------|------|-------------------------------|--------------|-----------|
| 1 | DBA | Troubleshoot Chronic Deadlock | (P) 4.16.2.1 | |

4.16.2 Troubleshoot Chronic Deadlock

A deadlock (also known as a "deadly embrace") is a situation where two database processes are simultaneously attempting to lock data that the other holds. For example, two users (A and B) are updating the same table of data at the same time. User A holds a lock on Page 1 and requests a lock on Page 2. Meanwhile, user B holds a lock on Page 2 and has requested a lock on Page 1. Without intervention, these two jobs would never finish.

Sybase detects these situations, analyzes the two processes and automatically kills the process with less accumulated processor time. Sybase prints out an error message to the killed process and requests that the user re-submit the job. A Sybase error message similar to the following one is displayed:

Msg 1205, Level 13, State 1:
Server 'SERVER', Procedure 'sp_whatever', Line 123:

**Your server command (family id #0, process id #99) was deadlocked with another process and has been chosen as deadlock victim. Re-run your command.
(return status = -3)**

4.16.2.1 Troubleshoot Chronic Deadlock

- 1 Turn on deadlock printing information and **sp_configure** "print deadlock information".
- 2 Recreate the problem.
- 3 As deadlocks occur, **tail -f the \$SYBASE/ASE-12_5/install/errorlog** (or wherever the errorlog prints out to).
 - Detailed information is printed out (e.g., line numbers of code causing deadlocks, tables within Sybase).
- 4 Run **dbcc traceon(3604)** and **dbcc page(#)** on the page numbers printed by **traceflag 1204**.
 - **dbcc page** will report the tablename and the index that is being used.
 - It is helpful to see if it is a non-clustered or a clustered index.
- 5 Monitor locks and blocked processes during deadlock re-creation.
 - Use **sp_lock**, **sp_block** and **sp_blocker** to print out detailed information about locking and blocking.
- 6 Run **sp_sysmon** while re-creating the problem, and analyze the "Lock Management" section.
 - Advanced deadlock diagnosis can be conducted using:
 - **traceflags 602, 603**, which prints out information for deadlock prevention.
 - **traceflag 1205**, which puts a stack trace on the deadlock.
 - **traceflag 8203**, which displays statement and transaction locks.
 - **sp_configure** "deadlock checking period", "deadlock retries", which are configuration parameters related to deadlocking.
 - Common deadlock problems and solutions include:
 - **Contention on heap tables**. "Last page contention" problems occur where high insert rates always seem to go on the last page of a table. This creates what is known as a "heap table," which is bound to have performance problems. The end of the table (in terms of a page chain) is a hotspot of activity. If this is the cause of the deadlocks, either partition the table (which creates several insert points for data and eliminates the "heapiness") or re-create your clustered index on a field that spreads inserts along the entire page chain of the table (i.e., clustered indexes on surrogate keys as opposed to last name or something similarly random). This can be seen in **sp_sysmon** output "Last page locks on heaps."

- **Poorly written key generation schemes.** Using a "select max(col)+1" method or high rate OLTP applications generating keys from a badly configured **key_storage** table system are always deadlock candidates. Never use the "select max+1" method. If you must use a **key_storage** solution (if you can't deal with identity gaps for example), ensure that the key_storage table is configured for Row Level Locking (in Sybase 11.9.2 and above) or has max_rows_per_page=1 (in Sybase 11.5 and 11.0).
 - **Lock contention; sp_configure "number of locks".** If you have configured too few locks for the system, severe lock contention can occur and deadlocking can be common. There is an entire section of **sp_sysmon** devoted to Lock management. Large updating within multi-user applications and long running transactions will definitely lead to deadlocking. Don't issue multiple update statements within the same transaction. If you must update multiple objects within the same transaction, make sure you consistently access the objects in the same order throughout the application. Updating or deleting from tables without covering indexes cause table scans. Other options: System data Lock strategies: In 11.9.2 and above: examine whether it may be wise to go to Row Level locking or Data only locking.
 - **Hardware problems.** Slower I/O devices increase deadlock vulnerability.
 - **Cursors.** Should be avoided.
 - **Parallelism.** y using some of the parallel processing features available in later versions, deadlocking is subdued.
 - **ANSI isolation level 3** (serialization) locking. Avoid when possible.
 - **Descending scans in indexes.** Can sometimes cause deadlocks after upgrading where none previously occurred.
 - **Application-side deadlocking.** See Section 1.5.1 of the Sybase FAQ for a quick example of Application-side deadlocking and how to avoid it.
 - **Deadlocking increases with upgrade.** These deadlocks are frequently caused by the "allow backward scans" option being turned on by default. They can also be caused by differing optimizer paths with new version (after upgrade) or just the engine's sheer speed. Also recommended to increase lock escalation threshold if using RLL (defaults to 200, which is not a lot of rows).
-

4.17 Oracle Procedures – Removed

This page intentionally left blank.