Oracle® Communications

EAGLE LNP Application Processor Alarms and Maintenance

Release 10.2

F38956-02

November 2021

Oracle Communications EAGLE LNP Application Processor Alarms and Maintenance, Release 10.2

F38956-02

Contents

5 Platform and Application Alarms

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

What's New in This Guide

Release 10.2.1 - November 2021

This section introduces the documentation updates for Release 10.2.1 in Oracle Communications EAGLE LNP Application Processor.

- Updated ELAP GUI images in the document.

1 Introduction

This chapter provides a brief description of this manual. This chapter also includes the scope, audience, and organization of the manual; how to find related publications; and how to contact documentation for assistance.

Overview

This manual contains the information necessary for the maintenance of the E5-APP-B that supports the EAGLE LNP Application Processor (ELAP). Included are an overview of the E5-APP-B architecture and functions, routine operational procedures, preventative maintenance techniques, and corrective maintenance procedures.

Scope and Audience

The scope of this manual covers platform and application alarms, troubleshooting and recovery procedures, and the System Healthcheck Utility, an application that generates a log file that can be provided to #unique_13 for alarm resolution. It is intended to aid maintenance personnel in resolution of ELAP alarms. When instructed by the application, use this manual to locate the platform alarm number and its recovery procedure.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1-1 Admonishments

Icon	Description
DANGER	Danger: (This icon and text indicate the possibility of *personal injury*.)
⚠ WARNING	Warning: (This icon and text indicate the possibility of *equipment damage*.)

Table 1-1 (Cont.) Admonishments

Icon	Description
⚠ CAUTION	Caution: (This icon and text indicate the possibility of *service interruption*.)
⚠ TOPPLE	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Manual Organization

This manual is organized into the following chapters:

Introduction contains general information about manual organization, scope and audience, related documentation, how to locate customer documentation on the Customer Support site, how to get technical assistance, and RMA requirements.

Maintenance provides the preventative maintenance procedures and system health checks.

Problem Detection and Reporting provides information about problem detection and reporting.

Recovery Support describes the recommended backing up of the RTDB and presents additional recovery support procedures that may be referred to by alarms recovery actions.

Platform and Application Alarms provides recovery procedures for platform and application alarms.

Field Replaceable Units (FRUs) provides instruction on replacing E5-APP-B cards and FRUs

General Procedures contains miscellaneous general procedures that are referred to within this manual.

Related Publications

For information about additional publications related to this document, refer to the Oracle Help Center site. See Locate Product Documentation on the Oracle Help Center Site for more information on related product publications.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click `Industries`.
3. Under the Oracle Communications subheading, click the `Oracle Communications documentation` link.

   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.

   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the `PDF` link, select `Save target as` (or similar command based on your browser), and save to a local folder.

2 Maintenance

This chapter provides maintenance information, problem detection description, and general recovery procedures for the E5-APP-B.

Introduction

This chapter provides preventive and corrective maintenance information. Customers perform a small number of daily preventive maintenance tasks. The ELAP application performs automatic monitoring and problem reporting.

Detailed information about recovery procedures is contained in the remaining chapters of this manual.

Preventive Maintenance

This section describes the following recommended periodic maintenance:

- Daily maintenance procedures:
  - Backing Up the RTDB
  - Transferring RTDB Backup File
  - Automatic RTDB Backup

Daily Maintenance Procedures

Use the Automatic PDB/RTDB Backup feature to backup all data stored in the PDB/RTDB. The manual backup procedures are included in this section in case the database backup needs to be performed manually. Storing database backups in a secure off-site location ensures the ability to recover from system failures.

This section describes the following recommended daily maintenance procedures:

- Backing Up the RTDB
- Transferring RTDB Backup File

Backing Up the RTDB

For ELAP 8.0 or later, a daily RTDB backup is created automatically. For automatic RTDB Backup, see Automatic RTDB Backup.

1. Log in to the ELAP**GUI** on **MPS** A as the **elapall** user.

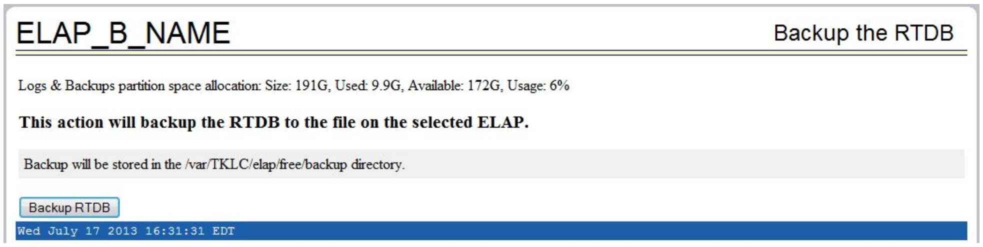
   For information about how to log in to the ELAP**GUI**, see Accessing the ELAP GUI Interface.

> **Note:**
>
> For ELAP 8.0 or later, the ELAP software can continue to operate while performing the RTDB backup.

2. From the ELAP menu, select **RTDB**, and then **Maintenance**, and then **Backup RTDB**.

   The window in Figure 2-1 is displayed.

Figure 2-1 Backup the RTDB



ELAP_B_NAME Backup the RTDB

Logs & Backups partition space allocation: Size: 191G, Used: 9.9G, Available: 172G, Usage: 6%

This action will backup the RTDB to the file on the selected ELAP.

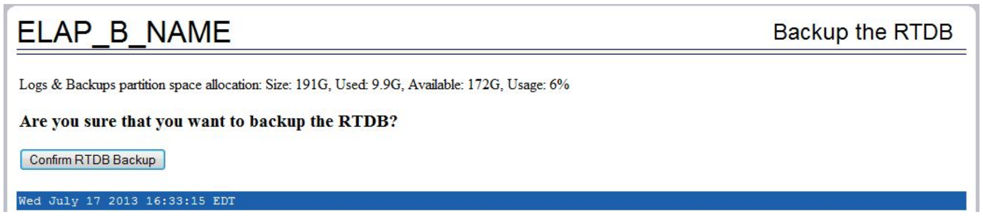
Backup will be stored in the /var/TKLC/elap/free/backup directory.

Wed July 17 2013 16:31:31 EDT

3. Click **Backup RTDB**.

   The window in Figure 2-2 displays a request for confirmation.

Figure 2-2 Backup the RTDB Confirmation



ELAP_B_NAME Backup the RTDB

Logs & Backups partition space allocation: Size: 191G, Used: 9.9G, Available: 172G, Usage: 6%

Are you sure that you want to backup the RTDB?

Wed July 17 2013 16:33:15 EDT

4. Click **Confirm RTDB Backup**.

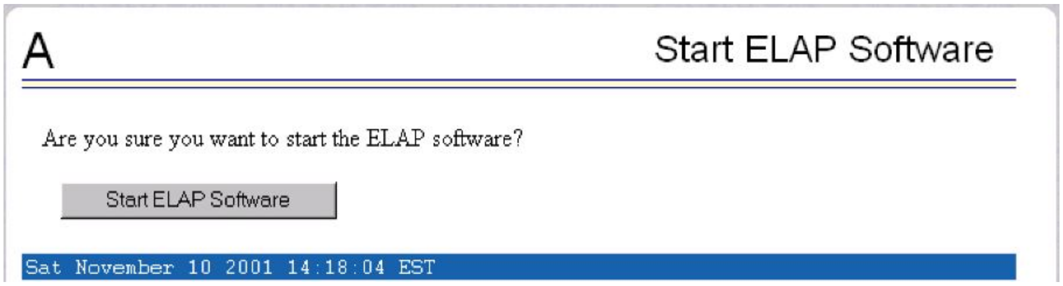
   If the backup starts successfully, the following message will scroll through the **GUI** banner:

   ```
   Backup RTDB in progress.
   ```

   After the backup completes successfully, the success window is displayed.

5. The RTDB backup procedure is complete.
6. Select **Process Control**, and then **Start Software** from the ELAP Menu.
7. On the Start ELAP Software screen as shown in Figure 2-3, click **Start ELAP Software.**

Figure 2-3 Start ELAP Software

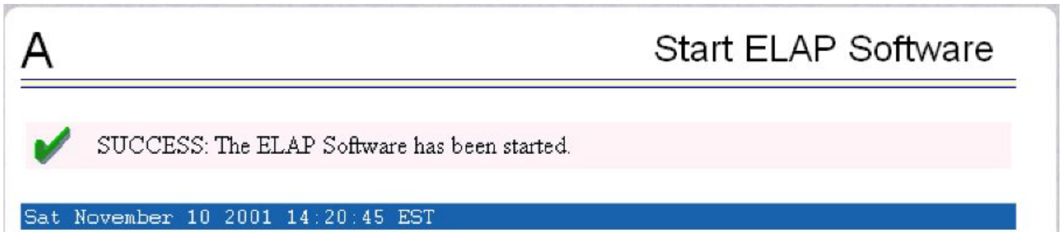


Are you sure you want to start the ELAP software?

```
Sat November 10 2001 14:18:04 EST
```

After the ELAP software has started successfully, the screen in Figure 2-4 is displayed.

Figure 2-4 Start ELAP Software - Success



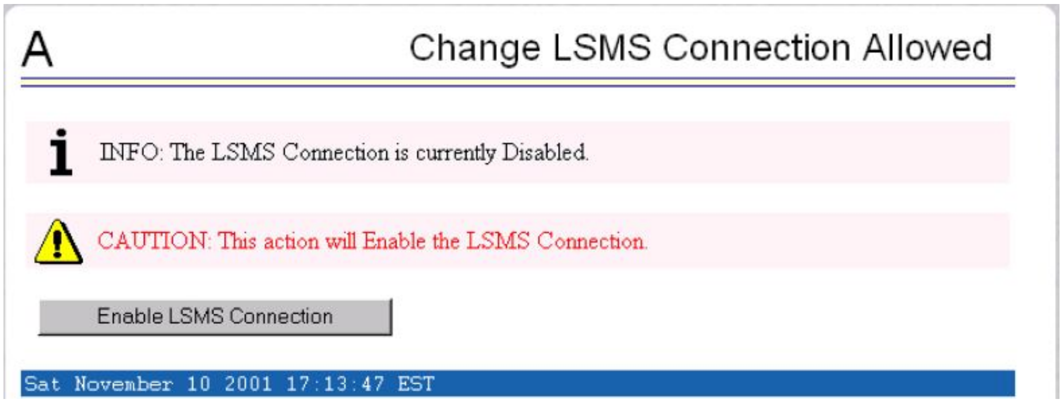
✓ SUCCESS: The ELAP Software has been started.

```
Sat November 10 2001 14:20:45 EST
```

8. Select **Maintenance**, and then **LSMS Connection**, and then **Change Allowed** from the ELAP Menu.
9. Click the **Enable LSMS Connection** button to enable the **LSMS** connection.

   Figure 2-5 shows the Change LSMS Connection Allowedwindow with the **LSMS** connection disabled.

Figure 2-5 Change LSMS Connection Allowed



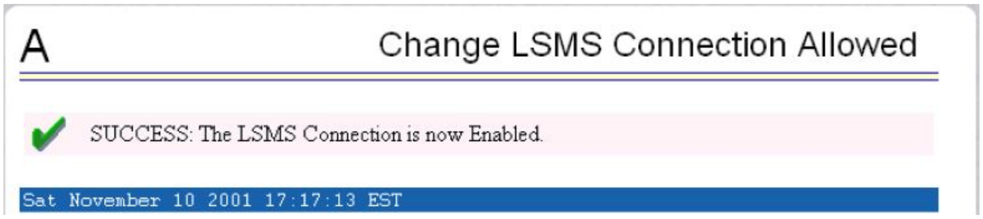
INFO: The LSMS Connection is currently Disabled.

CAUTION: This action will Enable the LSMS Connection.

```
Sat November 10 2001 17:13:47 EST
```

After the **LSMS** Connection is successfully enabled, the screen in Figure 2-6 is displayed.

Figure 2-6 Successfully Enabled LSMS Connection



A Change LSMS Connection Allowed

✓ SUCCESS: The LSMS Connection is now Enabled.

Sat November 10 2001 17:17:13 EST

Transferring RTDB Backup File

Perform this procedure once each day. The estimated time required to complete this procedure depends on network bandwidth. File sizes can be several gigabytes for the database.

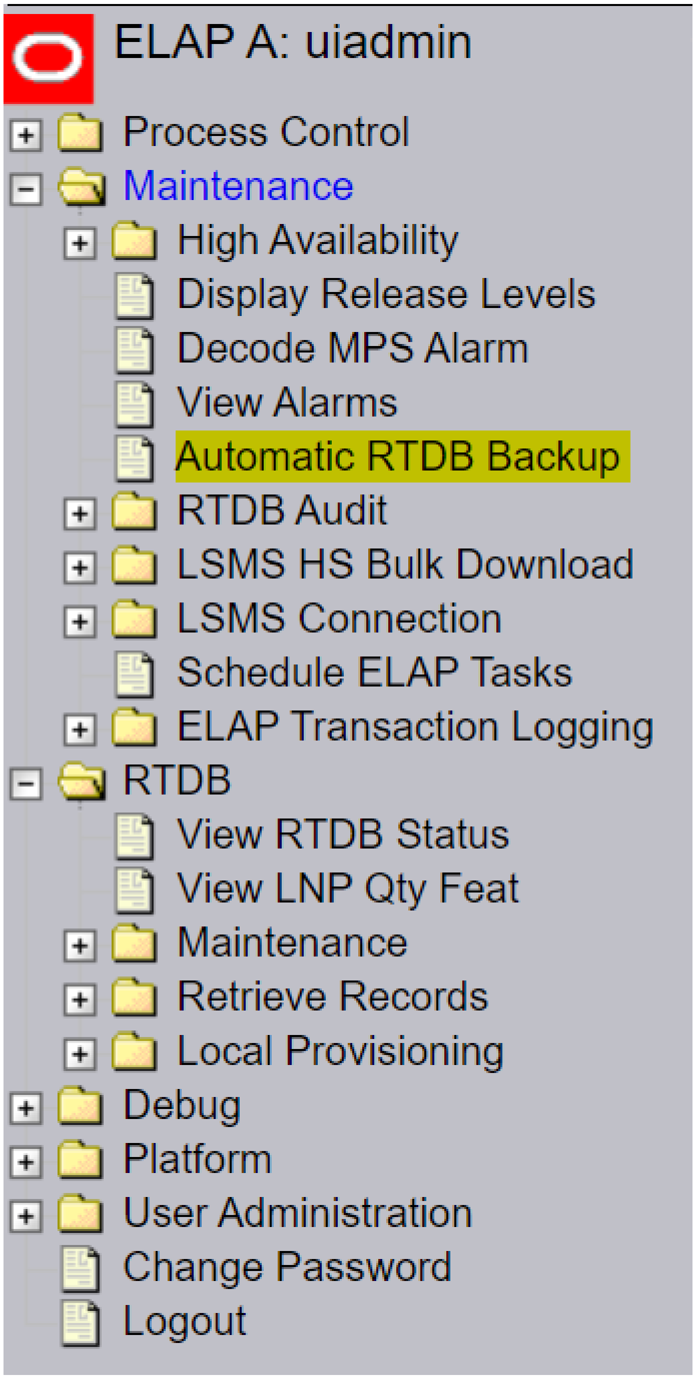
1. Log in to the ELAP command line interface with user name `elapdev` and the password associated with that name.
2. Use the Secure **File Transfer Protocol** (`sftp`) to transfer to a remote, secure location the **RTDB** backup file created by the procedure Backing Up the RTDB.

Automatic RTDB Backup

Automatic RTDB Backup can be scheduled during off-peak provisioning hours, eliminated the need for human intervention. Automatic ELAP RTDB backup intervals are scheduled at 6:a.m. every morning in the Active Server.
User Interface

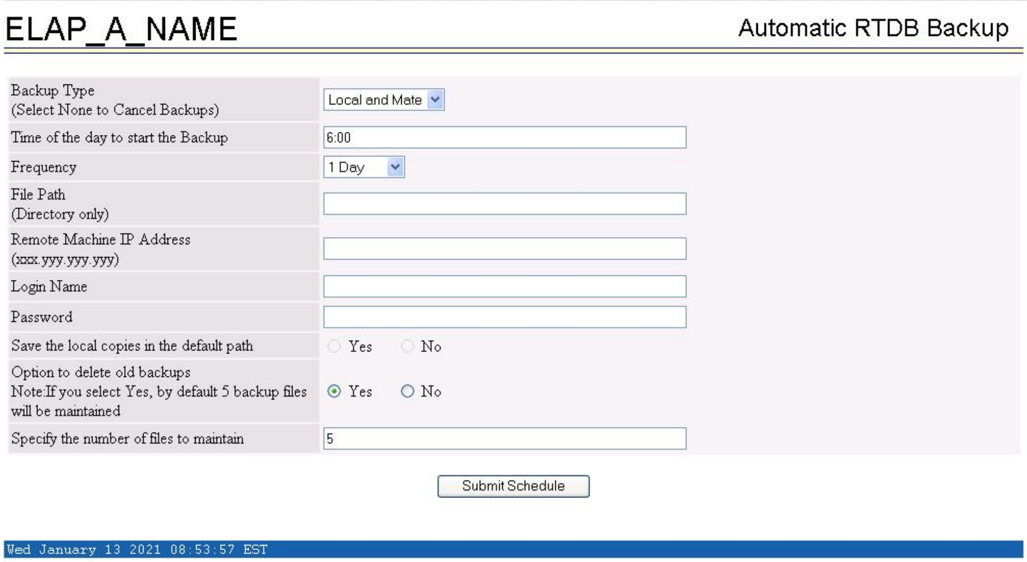
The menu item circled in #unique_28/unique_28_Connect_42_FIG_9A498360A27D40F4990F29204DFC0C32 is available on the ELAP GUI of the Active ELAP server only:

Figure 2-7   Automatic RTDB Backup Menu Item



Clicking Automatic RTDB Backup opens the page shown in Figure 2-8.

Figure 2-8 Automatic RTDB Backup GUI Screen



ELAP_A_NAME — Automatic RTDB Backup

Backup Type (Select None to Cancel Backups)	Local and Mate
Time of the day to start the Backup	6:00
Frequency	1 Day
File Path (Directory only)	
Remote Machine IP Address (xxx.yyy.yyy.yyy)	
Login Name	
Password	
Save the local copies in the default path	○ Yes ○ No
Option to delete old backups Note:If you select Yes, by default 5 backup files will be maintained	● Yes ○ No
Specify the number of files to maintain	5

Wed January 13 2021 08:53:57 EST

The Backup Type field has five options:

1. Local
2. Mate
3. Local and Mate
4. Remote
5. None

By default, backups shall be stored on both local and mate ELAP servers. If Automatic RTDB Backup is not configured, "None" option will not be available in the Backup Type field.

> **Note:**
>
> The following semantic rules must be followed:
>
> - Time of day must be in hh:mm 24-hour format. Example: 14:03
> - File path (in remote only) must be the absolute path from root
> - IP address must be in xxx.yyy.zzz.aaa format. Example: 192.168.210.111
> - Password entered will be displayed with asterisks (*)

Backup Type: Local

Selecting the Backup Type “Local” creates the backup on the same ELAP server. The user must provide the following inputs:

- Time of day to start Local Backup
- Frequency:

  - 12 hours
  - 1 day (daily)
  - 2 days
  - 3 days
  - 5 days
  - 7 days

> **Note:**
>
> Daily backup frequency is the default. Selecting an option other than 1 day prompts the user for reconfirmation of the backup frequency, as daily is the recommended frequency.

- File path where the user can provide the subdirectories created within the directory "/var/TKLC/elap/free/backup/"

> **Note:**
>
> By default, Backup file is saved in the Default File path.

- Option to delete old backups. When the user selects "yes," server will delete the old backups, except the latest number of backup files specified by the user in the "Specify the number of files to maintain" field. By default, 5 backup files are maintained. If this option is "yes," a maximum of 7 and minimum of 1 backup file may be maintained.
- Specify the number of files to maintain

Backup Type: Mate

Selecting the Backup Type "Mate" creates the backup on the local ELAP server and transfers (moves) the same backup on the mate ELAP server. The user must provide the following inputs:

- Time of day to start Backup
- Frequency (same configuration as Local)
- File path (same configuration as Local)
- Option to delete old backups (same configuration as Local)
- Specify the number of files to maintain

Backup Type: Local and Mate

Selecting the Backup Type "Local and Mate" creates the backup on the local ELAP server and transfers (moves) the same on the mate ELAP server. The user must provide the following inputs:

- Time of day to start Backup
- Frequency (same configuration as Local)
- File path (same configuration as Local)
- Option to delete old backups (same configuration as Local)

- Specify the number of files to maintain

Backup Type: Remote

Selecting the Backup Type "Remote" creates the backup on the local ELAP server and transfers (moves) the same on the remote ELAP server. The user must provide the following inputs:

- Time of day to start Backup
- Frequency (same configuration as Local)
- File path, which includes the absolute path for storing the backup file. If the user provides a non-existent directory, the directory will not be created and transfer of RTDB Backup file to the Remote Machine will fail.
- IP address of the Remote Machine
- User Login
- User Password
- Save the local copies in the default path. When the user selects "yes," the server will also save the RTDB Backup files in the local machine.

Backup Type: None

Selecting the Backup Type "None" cancels all currently scheduled backups All items on the form will be disabled except the submit button.

System Health Check Overview

The server runs a self-diagnostic utility program called `syscheck` to monitor itself. The system health check utility `syscheck` tests the server hardware and platform software. Checks and balances verify the health of the server and platform software for each test, and verify the presence of required application software.

If the `syscheck` utility detects a problem, an alarm code is generated. The alarm code is a 16-character data string in hexadecimal format. All alarm codes are ranked by severity: critical, major, and minor. Alarm Categories lists the platform alarms and their alarm codes.

The `syscheck` output can be in either of the following forms (see Health Check Outputs for output examples):

- Normal— results summary of the checks performed by `syscheck`
- Verbose—detailed results for each check performed by `syscheck`

The `syscheck` utility can be run in the following ways:

- The operator can invoke `syscheck` :
  - From the ELAP**GUI** Platform Menu (see Accessing the ELAP GUI Interface). The user can request `Normal` or `Verbose` output.
  - By logging in as a `syscheck` user (see Running syscheck Using the syscheck Login). Only `Normal` output is produced.
  - By logging in as admusr and using sudo to run syscheck on the command line (see Running syscheck from the Command line).

  - By logging into the platcfg utility and running syscheck in either Normal or Verbose mode. For more information, see 7.a.
- syscheck runs automatically by timer at the following frequencies:
  - Tests for critical platform errors run automatically every 30 seconds.
  - Tests for major and minor platform errors run automatically every 60 seconds.

Functions Checked by syscheck

Table 2-1 summarizes the functions checked by syscheck.

Table 2-1 System Health Check Operation

System Check	Function
Disk Access	Verify disk read and write functions continue to be operable. This test attempts to write test data in the file system to verify disk operability. If the test shows the disk is not usable, an alarm is reported to indicate the file system cannot be written to.
Smart	Verify that the smartd service has not reported any problems.
File System	Verify the file systems have space available to operate. Determine what file systems are currently mounted and perform checks accordingly. Failures in the file system are reported if certain thresholds are exceeded, if the file system size is incorrect, or if the partition could not be found. **Alarm** thresholds are reported in a similar manner.
Memory	Verify that 8 **GB** of **RAM** is installed.
Network	Verify that all ports are functioning by pinging each network connection (provisioning, sync, and **DSM** networks). Check the configuration of the default route.
Process	Verify that the following critical processes are running. If a program is not running the minimum required number of processes, an alarm is reported. If more than the recommended processes are running, an alarm is also reported. • sshd (**Secure Shelldaemon**) • ntpd (**NTPdaemon**) • syscheck (System Health Check **daemon**)
Hardware Configuration	Verify that the processor is running at an appropriate speed and that the processor matches what is required on the server. Alarms are reported when a processor is not available as expected.
Cooling Fans	Verifies no fan alarm is present. Fan alarm will be issued if fans are outside expected RPM.
Voltages	Measure all monitored voltages on the server main board. Verify that all monitored voltages are within the expected operating range.

Table 2-1 (Cont.) System Health Check Operation

System Check	Function
Temperature	Measure the following temperatures and verify that they are within a specified range. • Inlet and Outlet temperatures • Processor internal temperature • MCH internal temperature
MPS Platform	Provide alarm if internal diagnostics detect any other error, such as server `syscheck` script failures.

Health Check Outputs

System health check utility `syscheck` output can be either Normal (brief) or Verbose (more detailed), depending upon how `syscheck` was initiated. The following examples show Normal and Verbose output formats:

Normal Output

```
Running modules in class disk...
                                  OK
Running modules in class hardware...
                                  OK
Running modules in class net...
                                  OK
Running modules in class proc...
                                  OK
Running modules in class services...
                                  OK
Running modules in class system...
                                  OK
Running modules in class upgrade...
                                  OK
```

Verbose Output Containing Errors

If an error occurs, the system health check utility *syscheck* provides alarm data strings and diagnostic information for platform errors in its output. The following is an example of Verbose *syscheck* output:

```
Running modules in class disk...
         drbd: Checking DRBD status file, /proc/drbd
         drbd: line #1: DRBD version=[8.3.11]
         drbd: line #2 contains DRBD compilation info
         drbd: line #3: resource=[0]
         drbd: line #3: cs{0}=[Connected]
         drbd: line #3: st_self{0}=[Primary] st_peer{0}=[Secondary]
         drbd: line #3: ds_self{0}=[UpToDate] ds_peer{0}=[UpToDate]
         drbd: line #4 contains network stats
         drbd: processing alarms for resource=0
           fs: Current file space use in "/" is 43%.
           fs: Current Inode used in "/" is 14%.
           fs: Current file space use in "/boot" is 41%.
           fs: Current Inode used in "/boot" is 0%.
           fs: Current file space use in "/usr" is 57%.
           fs: Current Inode used in "/usr" is 20%.
           fs: Current file space use in "/var" is 34%.
           fs: Current Inode used in "/var" is 4%.
           fs: Current file space use in "/var/TKLC" is 40%.
           fs: Current Inode used in "/var/TKLC" is 1%.
           fs: Current file space use in "/tmp" is 0%.
           fs: Current Inode used in "/tmp" is 0%.
           fs: Current file space use in "/usr/TKLC/elap" is 6%.
           fs: Current Inode used in "/usr/TKLC/elap" is 0%.
           fs: Current file space use in "/var/TKLC/elap/drbd/mysql" is 4%.
           fs: Current Inode used in "/var/TKLC/elap/drbd/mysql" is 0%.
           fs: Current file space use in "/var/TKLC/elap/logs" is 0%.
           fs: Current Inode used in "/var/TKLC/elap/logs" is 0%.
           fs: Current file space use in "/var/TKLC/elap/free" is 3%.
           fs: Current Inode used in "/var/TKLC/elap/free" is 0%.
       hpdisk: Only HP ProLiant servers support hpdisk diagnostics.
          lsi: Could not find LSI controller. Not running test.
         meta: Checking md status on system.
         meta: md Status OK, with 3 active volumes.
         meta: Checking md configuration on system.
         meta: Server md configuration OK.
    multipath: No multipath devices configured to be checked.
          sas: Only T1200 supports SAS diagnostics.
        smart: Finished examining logs for disk: sdb.
        smart: Finished examining logs for disk: sda.
        smart: SMART status OK.
        write: Successfully read from file system "/".
        write: Successfully read from file system "/boot".
        write: Successfully read from file system "/usr".
        write: Successfully read from file system "/var".
        write: Successfully read from file system "/var/TKLC".
        write: Successfully read from file system "/tmp".
        write: Successfully read from file system "/usr/TKLC/elap".
        write: Successfully read from file system "/var/TKLC/elap/logs".
        write: Successfully read from file system "/var/TKLC/elap/free".
    Running modules in class hardware...
   cmosbattery: This hardware does not support monitoring the CMOS battery.
   cmosbattery: The test will not be ran.
          ecc: Checking ECC hardware.
          ecc: Correctible Error Count: 0
          ecc: Uncorrectible Error Count: 0
06/20/2016 05:11:30 EDT | inf | Discarding cache...
          fan: Checking Status of Server Fans.
          fan: Fan is OK. fana: 1, CHIP: FAN
          fan: Server Fan Status OK.
   fancontrol: EAGLE_E5APPB does not support Fan Controls
   fancontrol: Will not run the test.
   flashdevice: Checking programmable devices.
   flashdevice: PSOC OK.
   flashdevice: CPLD OK.
   flashdevice: BIOS OK.
   flashdevice: ALL Programmable Devices OK.
         mezz: Checking Status of Serial Mezzanine.
         mezz: Serial Mezzanine is OK. mezza: 1, CHIP: MEZZ
         mezz: Serial Mezzanine is OK. mezzb: 1, CHIP: MEZZ
         mezz: Server Serial Mezz Status OK.
        oemHW: Only Oracle servers support hwmgmt.
          psu: This hardware does not support power feed monitoring.
          psu: Will not run test.
          psu: This hardware does not support PSU monitoring.
          psu: Will not run test.
       serial: Running serial port configuration test
       serial: EAGLE_E5APPB does not support serial port configuration
monitoring
       serial: Will not run test.
         temp: Checking server temperature.
         temp: Server Temp OK. Inlet Air Temp: +25.0 C (high = +70.0
C, warn = +66 C, hyst = +75.0 C), CHIP: lm75-i2c-0-48
         temp: Server Temp OK. Outlet Air Temp: +30.0 C (high = +70.0
C, warn = +66 C, hyst = +75.0 C), CHIP: lm75-i2c-0-49
         temp: Server Temp OK. MCH Diode Temp: +41.0 C (high = +95.0
C, warn = +90 C, low = +10.0 C), CHIP: sch311x-isa-0a70
         temp: Server Temp OK. Internal Temp: +26.8 C (high = +95.0 C,
warn = +90 C, low = +10.0 C), CHIP: sch311x-isa-0a70
         temp: Server Temp OK. Core 0: +30.0 C (high = +71.0 C, crit =
+95.0 C, warn = +67 C), CHIP: coretemp-isa-0000
         temp: Server Temp OK. Core 1: +24.0 C (high = +71.0 C, crit =
+95.0 C, warn = +67 C), CHIP: coretemp-isa-0000
      voltage: Checking server voltages.
      voltage: Voltage is OK. V2.5: +2.44 V (min = +2.37 V, max =
+2.63 V), CHIP: sch311x-isa-0a70
      voltage: Voltage is OK. Vccp: +1.04 V (min = +0.85 V, max =
+1.35 V), CHIP: sch311x-isa-0a70
      voltage: Voltage is OK. V3.3: +3.27 V (min = +3.13 V, max =
+3.47 V), CHIP: sch311x-isa-0a70
      voltage: Voltage is OK. V5: +4.97 V (min = +4.74 V, max = +5.26
V), CHIP: sch311x-isa-0a70
      voltage: Voltage is OK. V1.8: +1.81 V (min = +1.69 V, max =
+1.88 V), CHIP: sch311x-isa-0a70
      voltage: Voltage is OK. V3.3stby: +3.28 V (min = +3.13 V, max =
+3.47 V), CHIP: sch311x-isa-0a70
      voltage: Voltage is OK. V3.3: +3.29 V (min = +3.13 V, max =
+3.46 V), CHIP: cy8c27x43-i2c-0-28
      voltage: Voltage is OK. V1.8: +1.81 V (min = +1.71 V, max =
+1.89 V), CHIP: cy8c27x43-i2c-0-28
      voltage: Voltage is OK. V1.5: +1.50 V (min = +1.42 V, max =
+1.57 V), CHIP: cy8c27x43-i2c-0-28
      voltage: Voltage is OK. V1.2: +1.20 V (min = +1.14 V, max =
+1.26 V), CHIP: cy8c27x43-i2c-0-28
      voltage: Voltage is OK. V1.05: +1.04 V (min = +1.00 V, max =
+1.10 V), CHIP: cy8c27x43-i2c-0-28
      voltage: Voltage is OK. V1.0: +1.00 V (min = +0.95 V, max =
+1.05 V), CHIP: cy8c27x43-i2c-0-28
      voltage: Server Voltages OK.
Running modules in class net...
   defaultroute: Checking default route(s)
   defaultroute:   Checking static default route through device eth01 to
gateway 192.168.61.250...
         ping: Checking ping hosts
         ping: prova-ip network connection OK
         ping: provb-ip network connection OK
         ping: dsmm-a network connection OK
         ping: dsmm-b network connection OK
         ping: dsmb-a network connection OK
         ping: dsmb-b network connection OK
         ping: sync-a network connection OK
         ping: sync-b network connection OK
                                  OK
Running modules in class proc...
          run: Checking RTCtimeStampd...
          run: Found 1 instance(s) of the RTCtimeStampd process.
          run: Checking ntdMgr...
          run: Found 1 instance(s) of the ntdMgr process.
          run: Checking smartd...
          run: Found 1 instance(s) of the smartd process.
          run: Checking switchMon...
          run: Found 1 instance(s) of the switchMon process.
          run: Checking atd...
          run: Found 1 instance(s) of the atd process.
          run: Checking crond...
          run: Found 1 instance(s) of the crond process.
          run: Checking snmpd...
          run: Found 1 instance(s) of the snmpd process.
          run: Checking sshd...
          run: Found 7 instance(s) of the sshd process.
          run: Checking syscheck...
          run: Found 1 instance(s) of the syscheck process.
          run: Checking rsyslogd...
          run: Found 1 instance(s) of the rsyslogd process.
          run: Checking tklcTpdCardCfgS...
          run: Found 1 instance(s) of the tklcTpdCardCfgS process.
          run: Checking alarmMgr...
          run: Found 1 instance(s) of the alarmMgr process.
          run: Checking tpdProvd...
          run: Found 1 instance(s) of the tpdProvd process.
          run: Checking trpd...
          run: Found 1 instance(s) of the trpd process.
          run: Checking prov...
          run: Found 1 instance(s) of the prov process.
          run: Checking ebdad...
          run: Found 1 instance(s) of the ebdad process.
          run: Checking hsopd...
          run: Found 1 instance(s) of the hsopd process.
          run: Checking maint...
          run: Found 1 instance(s) of the maint process.
          run: Checking exinit...
  run: Found 1 instance(s) of the syscheck process.
          run: Checking rsyslogd...
          run: Found 1 instance(s) of the rsyslogd process.
          run: Checking tklcTpdCardCfgS...
          run: Found 1 instance(s) of the tklcTpdCardCfgS process.
          run: Checking alarmMgr...
          run: Found 1 instance(s) of the alarmMgr process.
          run: Checking tpdProvd...
          run: Found 1 instance(s) of the tpdProvd process.
          run: Checking trpd...
          run: Found 1 instance(s) of the trpd process.
          run: Checking prov...
          run: Found 1 instance(s) of the prov process.
          run: Checking ebdad...
          run: Found 1 instance(s) of the ebdad process.
          run: Checking hsopd...
          run: Found 1 instance(s) of the hsopd process.
          run: Checking maint...
          run: Found 1 instance(s) of the maint process.
          run: Checking exinit...
          run: Found 1 instance(s) of the exinit process.
          run: Checking gs...
          run: Found 1 instance(s) of the gs process.
          run: Checking mysqld...
          run: Found 1 instance(s) of the mysqld process.
          run: Checking hamond...
          run: Found 1 instance(s) of the hamond process.
                                  OK
Running modules in class services...
   ha_keepalive: HA Keepalive Syscheck Test Start
   ha_keepalive: {   Broadcast        eth04              17401}: UP
   ha_keepalive: HA Keepalive Test Complete
   ha_transition: HA Transition Syscheck Test Start
   ha_transition: HA ACTIVE, no transition in progress.
   ha_transition: HA Transition Syscheck Test Complete
                                  OK
Running modules in class system...
         core: Checking for core files.
          cpu: Found "2" CPU(s)... OK
          cpu: CPU 0 is on-line... OK
          cpu: CPU 0 speed: 2660.017 MHz... OK
          cpu: CPU 1 is on-line... OK
          cpu: CPU 1 speed: 2660.017 MHz... OK
        kdump: Checking for kernel dump files.
          mem: Skipping expected memory check.
          mem: Minimum expected memory found.
          mem: 8252936192 bytes (~7871 Mb) of RAM installed.
                                  OK
Running modules in class upgrade...
    snapshots: No snapshots found. Not running test.
                                  OK
```

Running the System Health Check

The operator can run `syscheck` to obtain the operational platform status with one of the following procedures:

- Running syscheck from the Command line
- Running syscheck Through the ELAP GUI

- Running syscheck Using the syscheck Login

Running syscheck from the Command line

The admusr can use sudo to run `syscheck` from the command line. This method can be used whether an application is installed or whether the **GUI** is available.

1. Log in to the MPS as the admusr:

```
Login:  admusr
Password:  <Enter admusr password>
```

2. Run `syscheck` with any command line arguments.

```
$ sudo syscheck
```

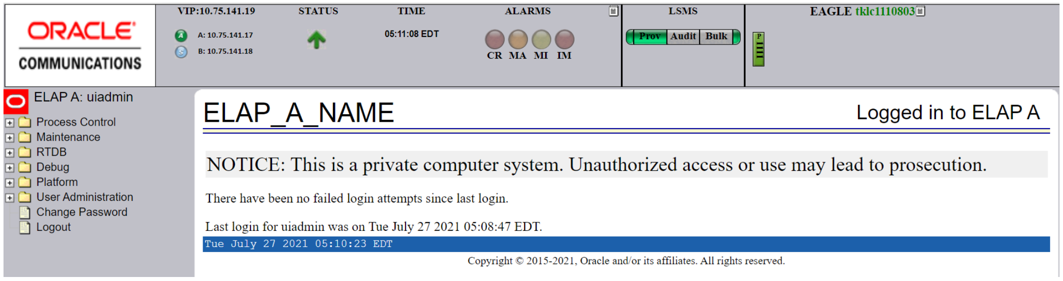
   For help on command syntax, use the `–h` option.`$ syscheck`

Running syscheck Through the ELAP GUI

Refer to *ELAP Administration and LNP Feature Activation* for more details and information about logins and permissions.

1. Log in to the User Interface of the ELAP**GUI** (see Accessing the ELAP GUI Interface).
2. Check the banner information above the menu to verify that the ELAP about which system health information is sought is the one that is logged into.

Figure 2-9 Login Window



ELAP_A_NAME

Logged in to ELAP A

NOTICE: This is a private computer system. Unauthorized access or use may lead to prosecution.

There have been no failed login attempts since last login.

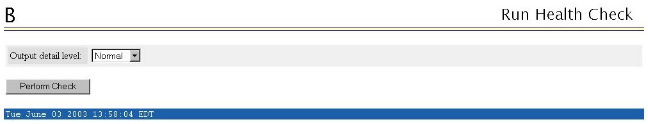
Last login for uiadmin was on Tue July 27 2021 05:08:47 EDT.

Tue July 27 2021 05:10:23 EDT

Copyright © 2015-2021, Oracle and/or its affiliates. All rights reserved.

3. If it is necessary to switch to the other ELAP, click the **Select Mate** menu item.
4. When the GUI shows you are logged into the ELAP about which you want system health information, select **Platform>Run Health Check**. as shown in the following window.

Figure 2-10 Run Health Check



Output detail level: Normal

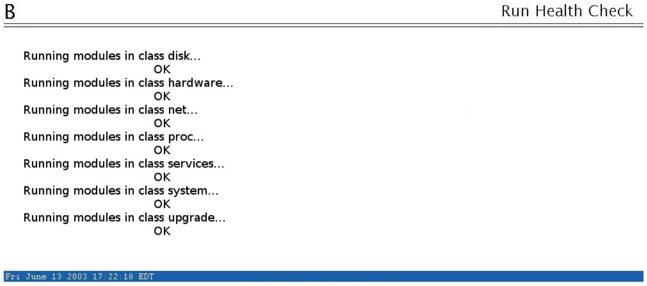
Tue June 03 2003 13:58:04 EDT

5. On the Run Health Check window, use the pull-down menu to select Normal or Verbose for the **Output detail level** desired.

6. Click the **Perform Check** button to run the system health check on the selected server.

   The system health check output data is displayed, as shown in Figure 2-11.

Figure 2-11   Displaying System Health Check on ELAP GUI



```
Running modules in class disk...
                                        OK
Running modules in class hardware...
                                        OK
Running modules in class net...
                                        OK
Running modules in class proc...
                                        OK
Running modules in class services...
                                        OK
Running modules in class system...
                                        OK
Running modules in class upgrade...
                                        OK
```

Fri June 13 2003 17:22:18 EDT

Running syscheck Using the syscheck Login

If the ELAP application has not been installed on the server or you are unable to log in to the ELAP user interface, you cannot run `syscheck` through the **GUI**. Instead, you can run `syscheck` from the `syscheck` login, and report the results to #unique_13.

1. Connect the Local Access Terminal to the server whose status you want to check (see Connecting a Local Access Terminal to Server’s Serial Port).
2. Log in as the `syscheck` user.

```
Login:  syscheck
Password:  syscheck
```

   The `syscheck` utility runs and its output is displayed to the screen.

3
Problem Detection and Reporting

This chapter provides information about problem detection and reporting by the platform operating system and the ELAP application.

Detecting and Reporting Problems

Problems are detected and reported by the platform operating system and the ELAP application.

The E5-APP-B card platform constantly monitors its operational status using the System Health Check utility `syscheck`. This utility can be initiated also by the user. For more details about `syscheck`, see System Health Check Overview.

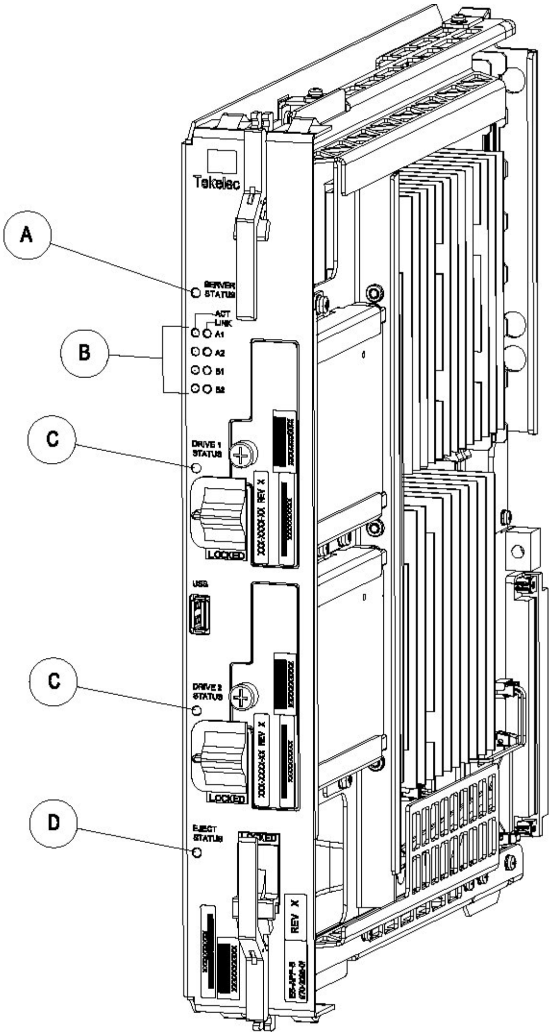
E5-APP-B Card LEDs

This section describes the LEDs found on the front face of the E5-APP-B card.

Server Panel LEDs

Figure 3-1 shows the E5-APP-B card LEDs on the front panel

Figure 3-1   E5-APP-B Card LEDs



The following light-emitting diode (**LED**) status indicators can be found on the E5-APP-B card:

- One Server Status indicator (A)
- Four E-Net link and Active LED status indicators (B)
- Two drive module status indicators (C)
- One Card Eject status indicator (D)

Table 3-1 E5-APP-B LED Table

LED Name	HW/SW Controlled	Description
Server Status	SW	Solid Red - Server is halted Flashing Red - Server is booting Solid Amber - TKLC configuration beginning Solid Green - TPD loaded/operational state Flashing Green - Server is shutting down
Drive 1 Status	SW/HW	HW: Flashing Green - Drive activity SW: Flashing Red - Impending drive removal SW: Steady red - Drive ready for removal
Drive 2 Status	SW/HW	HW: Flashing Green - Drive activity SW: Flashing Red - Impending drive removal SW: Steady red - Drive ready for removal
Eject Status	SW	Red - Card ready for extraction Flashing Red - Card preparing for extraction Off - Card is not ready for extraction
Act LED A1	HW	Flashing Green - Link Activity
Act LED A2	HW	Flashing Green - Link Activity
Act LED B1	HW	Flashing Green - Link Activity
Act LED B2	HW	Flashing Green - Link Activity
Link LED A1	HW	Green - 10/100 Link Speed Amber - 1000 Link Speed
Link LED A2	HW	Green - 10/100 Link Speed Amber - 1000 Link Speed
Link LED B1	HW	Green - 10/100 Link Speed Amber - 1000 Link Speed
Link LED B2	HW	Green - 10/100 Link Speed Amber - 1000 Link Speed

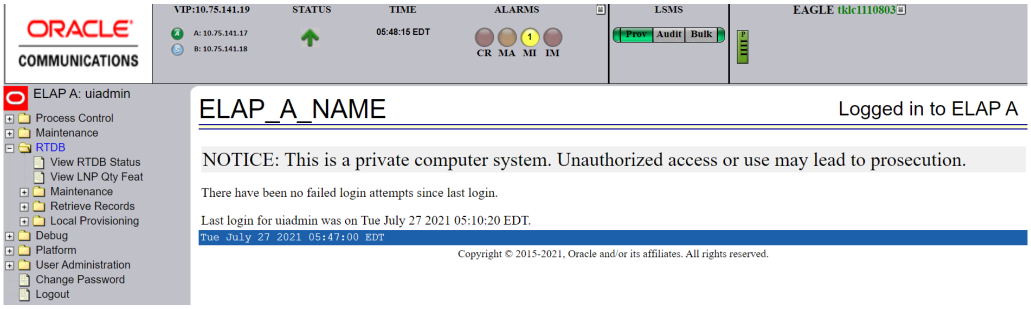
Displaying Errors on ELAP GUI

If the ELAP application detects an application error or receives an alarm message from the platform layer, the ELAP application displays the error on the graphical user interface (GUI):

- With a text message running across the banner.
- By illuminating the alarm level indicator on the GUI that corresponds to the alarm level of the error. If that alarm level indicator is already illuminated, the number shown on the indicator is incremented. For details about the alarms represented by the indicator, click the alarm button.

#unique_42/unique_42_Connect_42_V5380264 shows an example of errors displayed on the ELAP GUI.

Figure 3-2 Errors displayed on ELAP GUI



ELAP_A_NAME Logged in to ELAP A

NOTICE: This is a private computer system. Unauthorized access or use may lead to prosecution.

There have been no failed login attempts since last login.

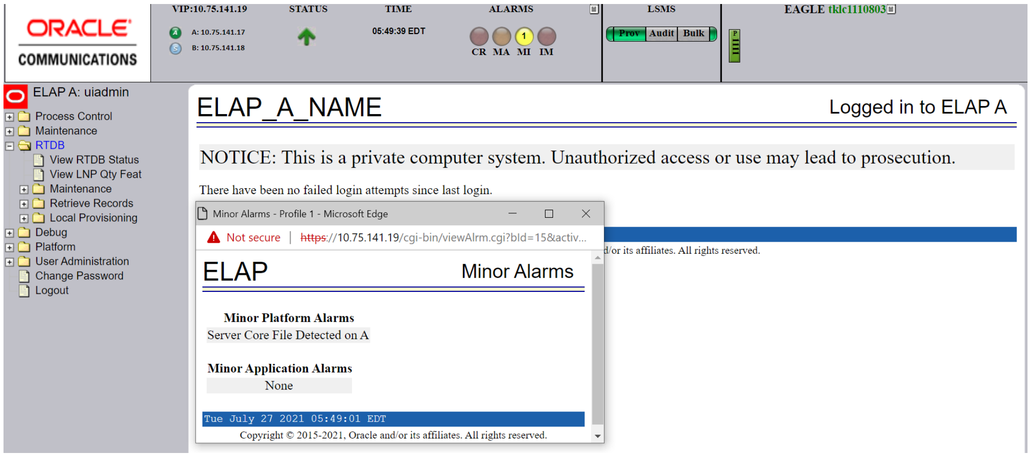
Last login for uiadmin was on Tue July 27 2021 05:10:20 EDT.

Tue July 27 2021 05:47:00 EDT

Copyright © 2015-2021, Oracle and/or its affiliates. All rights reserved.

To obtain additional information about the alarms, click any lighted alarm indicator. A pop-up window is displayed, showing the number of each type of alarm and listing the text of each existing alarm in each type. #unique_42/unique_42_Connect_42_V5380271 shows an example.

Figure 3-3 Viewing Alarm Details



ELAP_A_NAME Logged in to ELAP A

NOTICE: This is a private computer system. Unauthorized access or use may lead to prosecution.

There have been no failed login attempts since last login.

d/or its affiliates. All rights reserved.

ELAP Minor Alarms

Minor Platform Alarms
Server Core File Detected on A

Minor Application Alarms
None

Tue July 27 2021 05:49:01 EDT

Copyright © 2015-2021, Oracle and/or its affiliates. All rights reserved.

When an alarm value in the Alarm View popup window represents multiple alarms, the text of each alarm being reported is displayed. The individual alarm text is found in Alarm Categories. To correct the alarm condition, perform the associated procedure described in Recovering From Alarms.

Alarm values reported in #unique_42/unique_42_Connect_42_V5380271 may represent multiple alarms. To determine which alarms are indicated, perform Decode Alarm Strings. After determining which alarms are being reported, find the individual alarm numbers in Platform and Application Alarms.

Unsolicited Alarm and Information Messages

The EAGLE displays only one alarm per ELAP at a time based on the highest priority. If a single error is detected, the ELAP application sends an error message to the EAGLE terminal to report the active alarm category. If multiple errors are detected, the ELAP application sends an error message to the EAGLE terminal to report the most severe active alarm category.

If multiple alarms of the same severity exist and their severity is the highest alarm severity currently active, a combination alarm code is sent to the EAGLE. The EAGLE issues the appropriate **UAM** to the operator.

Errors detected in the hardware and software are reported by the following UAMs, which are described in greater detail in the EAGLE *Unsolicited Alarm and Information Messages Reference*.

- Critical Platform Alarms are reported by the EAGLE in UAM 0370.
- Critical Application Alarms are reported to the EAGLE in UAM 0371.
- Major Platform Alarms are reported to the EAGLE in UAM 0372.
- Major Application Alarms are reported to the EAGLE in UAM 0373.
- Minor Platform Alarms are reported to the EAGLE in UAM 0374.
- Minor Application Alarms are reported to the EAGLE in UAM 0375.

When all error conditions are corrected for all platform and application errors, the operator receives this UAM:

```
UAM 0250 MPS available.
```

For information about the alarm data contained in UAMs, see Platform and Application Alarms.

4

Recovery Support

The information in this section describes the recommended backing up of the RTDB and presents additional recovery support procedures that may be referred to by alarms recovery actions.

Recovering from Problems

This section describes the following recovery procedures:

- Restoring the RTDB from Backup Files
- Recovering From Alarms

Restoring the RTDB from Backup Files

This section describes the procedure for restoring the RTDB from backup files.

> **Note:**
>
> It is recommended that the **RTDB** be backed up daily (see section, Daily Maintenance Procedures). For ELAP 8.0 or later, daily backups are created automatically.

Use the following procedure to restore the RTDB from a previously prepared backup file.

> **Caution:**
>
> Contact #unique_13 before performing this procedure.

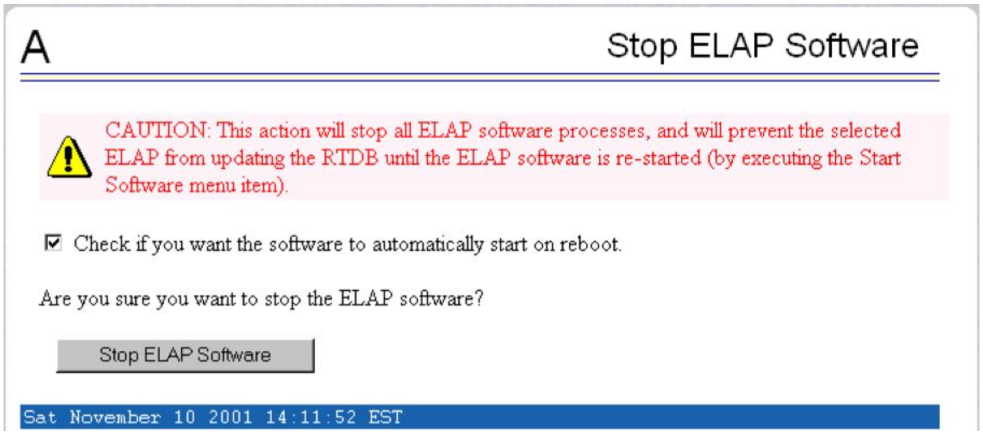
1. Contact #unique_13.
2. Log in to the ELAP command line interface with user name `elapdev` and the password associated with that user name.
3. Use the Secure **File Transfer Protocol** (`sftp`) to transfer the RTDB backup file, created by the procedure Backing Up the RTDB, to the following location:

   ```
   /var/TKLC/elap/free/backup
   ```

4. Log in to the ELAP **GUI** (see Accessing the ELAP GUI Interface).
5. Select **Process Control>Stop Software** to ensure that no other updates are occurring.

   The screen shown in Figure 4-1 is displayed.

Figure 4-1 Stop ELAP Software



A — Stop ELAP Software

CAUTION: This action will stop all ELAP software processes, and will prevent the selected ELAP from updating the RTDB until the ELAP software is re-started (by executing the Start Software menu item).

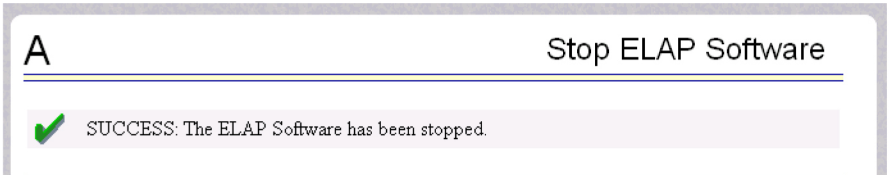
☑ Check if you want the software to automatically start on reboot.

Are you sure you want to stop the ELAP software?

Sat November 10 2001 14:11:52 EST

After the software on the selected ELAP has stopped, the screen shown in Figure 4-2 is displayed.

Figure 4-2 Stop ELAP Software - Success



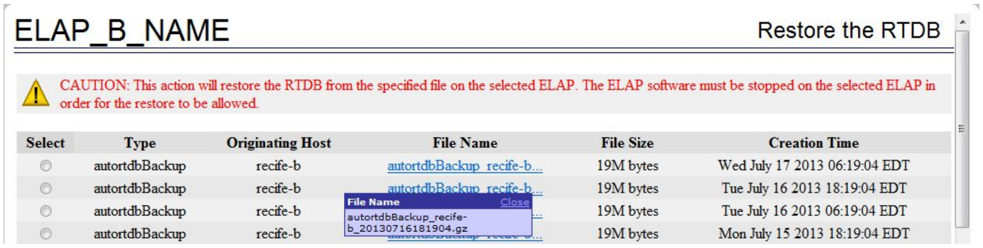
A — Stop ELAP Software

SUCCESS: The ELAP Software has been stopped.

6. Select **RTDB>Maintenance>Restore RTDB**.

   The screen shown in Figure 4-3 is displayed.

Figure 4-3 Restoring the RTDB



ELAP_B_NAME — Restore the RTDB

CAUTION: This action will restore the RTDB from the specified file on the selected ELAP. The ELAP software must be stopped on the selected ELAP in order for the restore to be allowed.

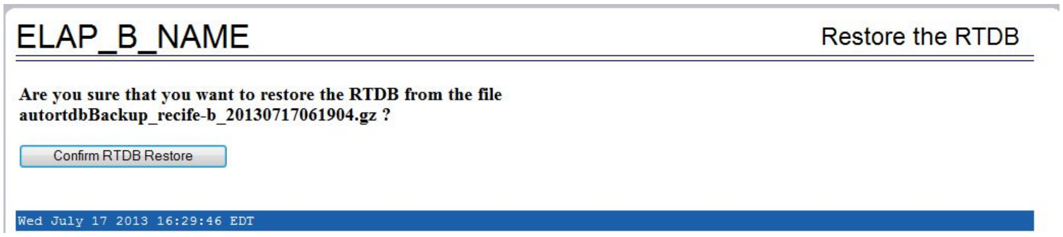
Select	Type	Originating Host	File Name	File Size	Creation Time
○	autortdbBackup	recife-b	autortdbBackup_recife-b...	19M bytes	Wed July 17 2013 06:19:04 EDT
○	autortdbBackup	recife-b	autortdbBackup_recife-b...	19M bytes	Tue July 16 2013 18:19:04 EDT
○	autortdbBackup	recife-b	...	19M bytes	Tue July 16 2013 06:19:04 EDT
○	autortdbBackup	recife-b	...	19M bytes	Mon July 15 2013 18:19:04 EDT

File Name — Close

autortdbBackup_recife-b_20130716181904.gz

7. On the screen shown in Figure 4-3 , select the file that was transferred in 3. Click **Restore the RTDB from the Selected File**.
8. To confirm restoring a file, click **Confirm RTDB Restore** shown in Figure 4-4.

Figure 4-4 Restore the RTDB Confirm



ELAP_B_NAME

Restore the RTDB

Are you sure that you want to restore the RTDB from the file autortdbBackup_recife-b_20130717061904.gz ?

Wed July 17 2013 16:29:46 EDT

After the file is successfully restored, the success screen is displayed.

Recovering From Alarms

Alarms are resolved in order of severity level from highest to lowest. When combination alarms are decoded into their individual component alarms, the customer can decide in which order to resolve the alarms because all alarms are of equal severity. For assistance in deciding which alarm to resolve first or how to perform a recovery procedure, contact #unique_13.

Evaluate the following problems to find the appropriate recovery procedure as follows:

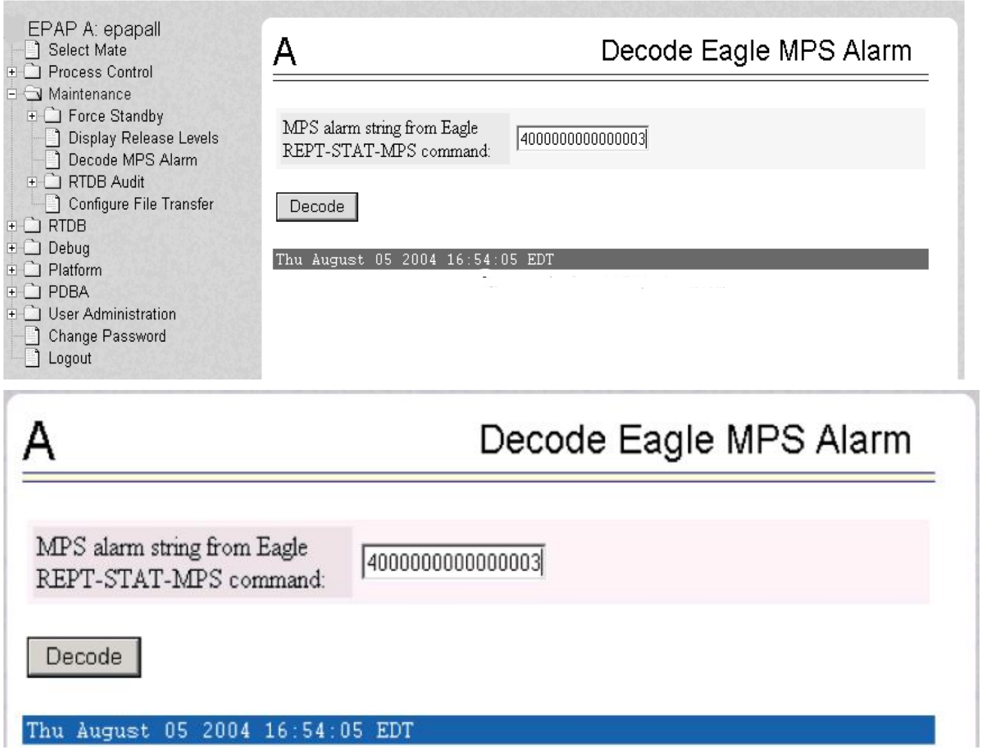
- If the problem being investigated **is no longer displayed** on the ELAP GUI, perform the following:
  1. Procedure Decode Alarm Strings
  2. Procedure Determine Alarm Cause
  3. Recovery procedure to which you are directed by procedure Determine Alarm Cause
- If the problem being investigated **is being reported currently** on the ELAP GUI, perform the following:
  1. Procedure Decode Alarm Strings

Decode Alarm Strings

Use the following procedure to decode alarm strings that consist of multiple alarms.

1. Log in to the **User Interface** screen of the ELAP **GUI** (see Accessing the ELAP GUI Interface).
2. After logging in to the ELAP, select **Maintenance>Decode MPSAlarm** from the menu.
3. Enter the 16-digit alarm string into the window on the **Decode MPSAlarm** screen, as shown in Figure 4-5.

Figure 4-5   Decode MPS Alarm Screen



MPS alarm string from Eagle REPT-STAT-MPS command: 4000000000000003

Thu August 05 2004 16:54:05 EDT

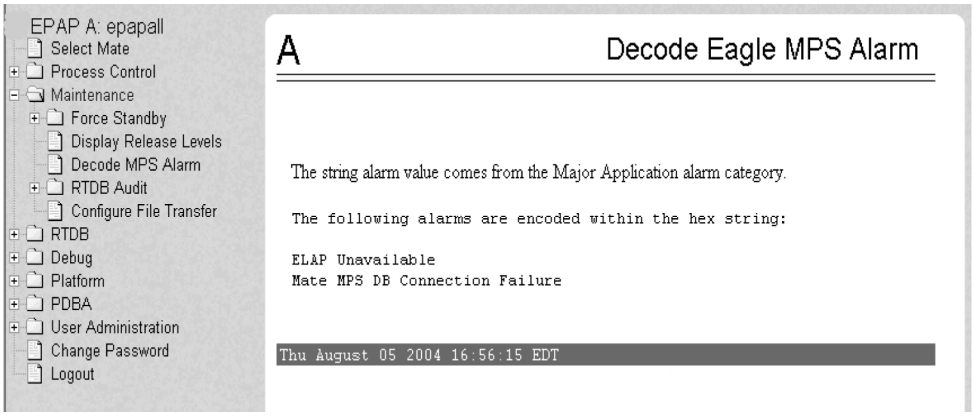
MPS alarm string from Eagle REPT-STAT-MPS command: 4000000000000003

Thu August 05 2004 16:54:05 EDT

4. Click the **Decode** button.

   The system returns information on the **Alarm** Category (Critical Application, Major Platform) and error text, as shown in Figure 4-6.

Figure 4-6   Decoded MPS Alarm Information

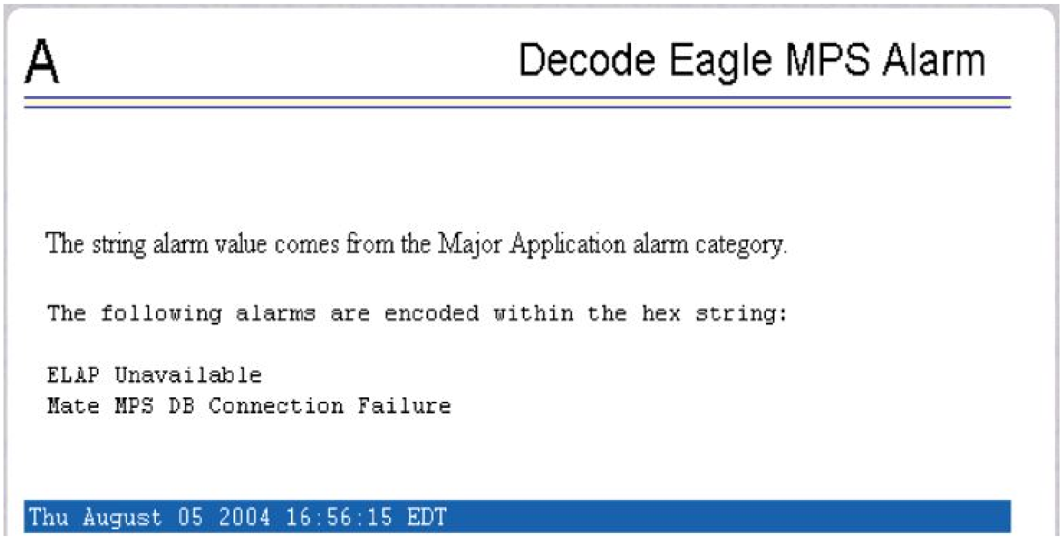


The string alarm value comes from the Major Application alarm category.

```
The following alarms are encoded within the hex string:

ELAP Unavailable
Mate MPS DB Connection Failure
```

Thu August 05 2004 16:56:15 EDT



The string alarm value comes from the Major Application alarm category.

```
The following alarms are encoded within the hex string:

ELAP Unavailable
Mate MPS DB Connection Failure
```

Thu August 05 2004 16:56:15 EDT

5. Find the alarm text string shown on the **GUI** in Table 5-1. Note the corresponding alarm number change. Perform procedure Determine Alarm Cause.

> **Note:**
>
> For combination errors, multiple procedures may be required to resolve the problem.

Determine Alarm Cause

Use this procedure to find information about recovering from an alarm.

1. Record the alarm data string shown in the banner or the **Alarm** View on the ELAP**GUI** , or as decoded from Decode Alarm Strings.
2. Run `syscheck` in Verbose mode (see Running syscheck Through the ELAP GUI).
3. Examine the `syscheck` output for specific details about the alarm.
4. Find the recovery procedure for the alarm in the procedures shown in Platform and Application Alarms. The alarms are ordered by ascending alarm number.

   Other procedures may be required to complete an alarm recovery procedure:

   - Refer to procedures for replacing Field Replaceable Units (**FRUs**) in Field Replaceable Units if instructed by an alarm recovery procedure to replace a **FRU**.
   - Refer to general procedures used in a number of alarm recovery procedures in Platform and Application Alarms
5. If the alarm persists after performing the appropriate procedure, call #unique_13.

5

Platform and Application Alarms

This chapter provides recovery procedures for platform and application alarms related to the E5-APP-B.

Alarm Categories

This chapter describes recovery procedures to use when an alarm condition or other problem exists on the MPS system. For information about how and when alarm conditions are detected and reported, see Detecting and Reporting Problems.

When an alarm code is reported, locate the alarm in Platform and Application Alarms. The procedures for correcting alarm conditions are described in Platform and Application Alarms.

> **Note:**
>
> Sometimes the alarm string may consist of multiple alarms and must be decoded in order to use the **Alarm** Recovery Procedures in this manual. If the alarm code is not listed, see Decode Alarm Strings.

Platform and application errors are grouped by category and severity. The categories are listed from most to least severe:

- Critical Platform Alarms
- Critical Application Alarms
- Major Platform Alarms
- Major Application Alarms
- Minor Platform Alarms
- Minor Application Alarms

Table 5-1 shows the alarm numbers and alarm text for all alarms generated by the MPS platform and the ELAP application. The order within a category is not significant. Some of the alarms described in this chapter are not available with specific configurations.

Table 5-1 Platform and Application Alarms

Alarm Codes and Error Descriptor	UAM Number
Critical Platform Alarm(There are no critical EPAP Platform Alarms)	
1000000000002000 - Uncorrectable ECC Memory Error	0370
1000000000008000 – Server NTP Daemon lost NTP synchronization for extended time	0370
1000000000010000 – Server's time has gone backwards	0370

Table 5-1 (Cont.) Platform and Application Alarms

Alarm Codes and Error Descriptor	UAM Number
Critical Application Alarms(There are no critical EPAP Application Alarms)	
2000000000000001 - LSMS DB Maintenance Required	0371
Major Platform Alarms	
3000000000000001 – Server fan failure	0372
3000000000000002 - Server Internal Disk Error	0372
3000000000000008 - Server Platform Error	0372
3000000000000010 - Server File System Error	0372
3000000000000020 - Server Platform Process Error	0372
3000000000000080 - Server Swap Space Shortage Failure	0372
3000000000000100 - Server provisioning network error	0372
3000000000000200 – Server Eagle Network A error	0372
3000000000000400 – Server Eagle Network B error	0372
3000000000000800 – Server Sync network error	0372
3000000000001000 - Server Disk Space Shortage Error	0372
3000000000002000 - Server Default Route Network Error	0372
3000000000004000 - Server Temperature Error	0372
3000000000008000 - Server Mainboard Voltage Error	0372
3000000000010000 - Server Power Feed Error	0372
3000000000020000 - Server Disk Health Test Error	0372
3000000000040000 - Server Disk Unavailable Error	0372
3000000000080000 - Device Error	0372
3000000000100000 - Device Interface Error	0372
3000000000200000 - Correctable ECC Memory Error	0372
3000000400000000 - Multipath device access link problem	0372
3000000800000000 – Switch Link Down Error	0372
3000001000000000 - Half-open Socket Limit	0372
3000002000000000 - Flash Program Failure	0372
3000004000000000 - Serial Mezzanine Unseated	0372
3000000008000000 - Server HA Keepalive Error	0372
3000000010000000 - DRBD block device can not be mounted	0372
3000000020000000 - DRBD block device is not being replicated to peer	0372
3000000040000000 - DRBD peer needs intervention	0372

Table 5-1 (Cont.) Platform and Application Alarms

Alarm Codes and Error Descriptor	UAM Number
3000020000000000 - Server NTP Daemon never synchronized	0372
Major Application Alarms	
4000000000000001 - Mate ELAP Unavailable	0373
4000000000000004 - Congestion	0373
4000000000000008 - File System Full	0373
4000000000000010 - Log Failure	0373
4000000000000040 - Fatal Software Error	0373
4000000000000080 - RTDB Corrupt	0373
4000000000000100 - RTDB Inconsistent	0373
4000000000000200 - RTDB Incoherent	0373
4000000000000800 - Transaction Log Full	0373
4000000000001000 - RTDB 100% Full	0373
4000000000002000 - RTDB Resynchronization In Progress	0373
4000000000004000 - RTDB Reload Is Required	0373
4000000000400000 - LVM Snapshot detected that is too old	0373
4000000000800000 - LVM Snapshot detected that is too full	0373
4000000001000000 - LVM Snapshot detected with invalid attributes	0373
4000000002000000 - DRBD Split Brain	0373
4000000010000000 - An instance of Snapmon already running	0373
Minor Platform Alarms	
1000000000000001 – Breaker panel feed unavailable	0374
5000000000000001 - Server Disk Space Shortage Warning	0374
5000000000000002 - Server Application Process Error	0374
5000000000000004 - Server Hardware Configuration Error	0374
5000000000000020 - Server Swap Space Shortage Warning	0374
5000000000000040 - Server Default Router Not Defined	0374
5000000000000080 – Server temperature warning	0374
5000000000000100 - Server Core File Detected	0374
5000000000000200 - Server NTP Daemon Not Synchronized	0374
5000000000000800 - Server Disk Self Test Warning	0374
5000000000001000 - Device Warning	0374
5000000000002000 - Device Interface Warning	0374

Table 5-1 (Cont.) Platform and Application Alarms

Alarm Codes and Error Descriptor	UAM Number
5000000000004000 - Server Reboot Watchdog Initiated	0374
5000000000008000 - Server HA Failover Inhibited	0374
5000000000010000 - Server HA Active To Standby Transition	0374
5000000000020000 - Server HA Standby To Active Transition	0374
5000000000080000 - NTP Offset Check Failure	0374
5000000000100000 - NTP Stratum Check Failure	0374
5000000020000000 – Server Kernel Dump File Detected	0374
5000000040000000 – TPD Upgrade Failed	0374
5000000080000000– Half Open Socket Warning Limit	0374
5000000000800000 - DRBD failover busy	0374
5000000400000000 – NTP Source Server is not able to provide correct time	0374
Minor Application Alarms	
4000000000020000 - Automatic RTDB Backup is not configured	0375
6000000000000010 - Minor Software Error	0375
6000000000000200 - RTDB Backup Failed	0375
6000000000000400 - Automatic RTDB Backup Failed	0375
6000000000000800 - Automatic Backup cron entry modified	0375
6000000000002000 - Configurable Quantity Threshold Exceeded	0375
6000000000020000 - Automatic RTDB Backup is not configured	0375
NOTE: The order within a category is not significant.	

MPS Alarm Recovery Procedures

This section provides recovery procedures for the MPS and ELAP alarms, listed by alarm category and **Alarm** Code (alarm data string) within each category.

Critical Platform Alarms

Critical platform alarms are issued if uncorrectable memory problems are detected.

1000000000002000 - Uncorrectable ECC Memory Error

This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the Error-Correcting Code (**ECC**) circuitry in the memory is unable to correct.

Recovery

- Contact #unique_13 to request hardware replacement.

1000000000008000 – Server NTP Daemon lost NTP synchronization for extended time

Alarm Type: TPD

Description: This alarm indicates that a TPD syscheck test determined that the time last synchronized with an NTP server has exceeded the critical threshold (LAST_SYNCHRONIZED_TIME_PERIOD_CRITICAL), as configured by the application.

Severity: Critical

Alarm ID: TKSPLATCR16

Recovery

Contact #unique_13.

1000000000010000 – Server's time has gone backwards

Alarm Type: TPD

Description: This alarm indicates that syscheck determined that a server's time has gone backwards.

Severity: Critical

Alarm ID: TKSPLATCR17

Recovery

Contact #unique_13.

Critical Application Alarms

This section describes the critical application alarms.

2000000000000001 - LSMS DB Maintenance Required

This alarm indicates that database maintenance is required.

Recovery

- Call #unique_13 for assistance.

Major Platform Alarms

Major platform alarms involve hardware components, memory, and network connections.

3000000000000001 – Server fan failure

Alarm Type: TPD

Description: This alarm indicates that a fan on the application server is either failing or has failed completely. In either case, there is a danger of component failure due to overheating.

Description: This alarm indicates that a fan in the EAGLE fan tray in the EAGLE shelf where the E5-APP-B is "jacked in" is either failing or has failed completely. In either case, there is a danger of component failure due to overheating.

Severity: Major

OID: TpdFanErrorNotify 1.3.6.1.4.1.323.5.3.18.3.1.2.1

Alarm ID: TKSPLATMA13000000000000001

Recovery

> **Note:**

1. Run syscheck in Verbose mode to verify a fan failure using the following command:

```
[admusr@hostname1351690497 ~]$ sudo syscheck -v hardware fan
Running modules in class hardware...
         fan: Checking Status of Server Fans.
*          fan: FAILURE:: MAJOR::3000000000000001 -- Server Fan
Failure. This test uses the leaky bucket algorithm.
*          fan: FAILURE:: Fan RPM is too low, fana: 0, CHIP: FAN
One or more module in class "hardware" FAILED

LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

2. Refer to the procedure for determining the location of the fan assembly that contains the failed fan and replacing a fan assembly in the appropriate hardware manual. After you have opened the front lid to access the fan assemblies, determine whether any objects are interfering with the fan rotation. If some object is interfering with fan rotation, remove the object.
3. Run "syscheck -v hardware fan" (see Running syscheck Through the ELAP GUI)
   - If the alarm has been cleared (as shown below), the problem is resolved

```
[admusr@hostname1351691862 ~]$ sudo syscheck -v hardware fan
Running modules in class hardware...
Discarding cache...
         fan: Checking Status of Server Fans.
         fan: Fan is OK. fana: 1, CHIP: FAN
         fan: Server Fan Status OK.
                                 OK
```

   - If the alarm has not been cleared (as shown below) continue with the next step

```
[admusr@hostname1351690497 ~]$ sudo syscheck -v hardware fan
Running modules in class hardware...
         fan: Checking Status of Server Fans.
```

```
*          fan: FAILURE:: MAJOR::3000000000000001 -- Server Fan Failure.
This test uses the leaky bucket algorithm.
*          fan: FAILURE:: Fan RPM is too low, fana: 0, CHIP: FAN
One or more module in class "hardware" FAILED

LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

4. Contact #unique_13.

3000000000000002 - Server Internal Disk Error

This alarm indicates that the server is experiencing issues replicating data to one or more of its mirrored disk drives. This could indicate that one of the server disks has failed or is approaching failure.

Recovery

1. Run `syscheck` in Verbose mode.
2. Call #unique_13 and provide the system health check output.
3. Run `syscheck` in verbose mode.
4. The syscheck output will indicate which of the possible failures have been detected.

   Depending on which failure was detected, go to the step shown as follows:

   a. If both the md status check and the md configuration check failed, go to .
   b. If only the md status check failed, go to .
   c. If only the md configuration check failed, go to .
5. Check to see if an md resynch is in-progress on the server:

   a. Log in as `root` to the server that is generating the alarm.

   ```
   Login:  root
   Password: <Enter root password>
   ```

   b. Examine the file `/proc/mdstat` using the command:`# more /proc/mdstat`If any lines are printed that indicate an md group is resynching, wait up to two hours to allow the system to finish resyncing.

      If the resyncing has not completed in this time, proceed to . When an md group is in the process of resynching, its entry in `/proc/mdstat` will look similiar to the following:

   ```
   md2 : active raid1 hdc2[2] hda2[0]
         538112 blocks [2/1] [U_]
         [>....................]  recovery =  3.6% (20088/538112)
   finish=0.4min speed=20088K/sec
   ```

   c. After waiting the required amount of time, rerun `syscheck`.

      If the alarm has been cleared, the problem is solved. If the alarm has not been cleared, go to the next step.

6. If the syscheck output contains the text:

   ```
   md status check failed
   ```

   or

   ```
   Both the md status check and the md configuration check failed
   ```

   a. Log in as `root` to the server that is generating the alarm.

      ```
      Login:  root
      Password: <Enter root password>
      ```

   b. Check the status of the md mirrors: `# syscheck -v disk meta`

   c. For each md group that is detected to have problems an entry will appear in the output similiar to the following:

      ```
      meta: Number of active devices for md2 does not match expected.
      meta: md2 is reporting faulty status, "_U".
      meta: "md2" is in error state ->
      meta: md2 : active raid1 hdc2[1]
      meta: 538112 blocks [2/1] [_U]
      ```

      This indicates which md group has a problem. In the example above, md group #2 is reporting failure and the information reported indicates that the group is still active on device hdc2, but 2 devices were expected and only 1 is functional. **NOTE**: The `syscheck` output shown only lists the devices in the md group that are currently functional and doesn’t explicitly indicate that a particular device has failed. Proceed to the next sub-step to determine which of the server’s disks has issues.

   d. The server is always configured with each disk drive mastering one of the system’s **IDE** channels.

      This means the logical device names for the disk drives will always be consistant, (see). The disk connected to the primary **IDE** channel will always be `/dev/hda` and the drive on the secondary channel is always `/dev/hdc`. Referring back to the syscheck output shown in the previous sub-step, the device hdc2 is reported to be still active, so the problem is obviously with the `/dev/hda` (Primary Master) device. Now that the device name is known, proceed to the next sub-step to attempt to correct this issue.

Table 5-2 Logical Disk Name Matrix

Physical Disk	Logical Name
Primary Master	`/dev/hda`
Secondary Master	`/dev/hdc`

e. In order to determine if this disk requires replacing it is very important to keep a record of every reported occurance of the alarm.

   With this in mind, create a record of this incident making note of the date and time, hostname of server, and device name determined in the previous sub-step. If this is the first reported problem with this particular disk drive, execute "Procedure 6-2: Creating or Repairing Mirrors on a Disk Drive" to attempt to repair the disk mirroring on the drive. If any previous occurances of the alarm have been recorded for this disk, the drive must be replaced. Follow Procedure 6-1, “Replacing a Faulty Disk Drive with a New Disk Drive to replace the disk.

7. If the output from syscheck contains the text:

```
md configuration check failed
```

   a. Log in as `root` to the server that is generating the alarm.

```
Login:  root
Password: <Enter root password>
```

   b. Check validity of the `/etc/raidtab` file.

      `# more /etc/raidtab`Scan through the output to ensure that there are no duplicate entries and that each of the md groups active on the server is listed. (To get an idea which md groups are currently active on the server look at the file `/proc/mdstat`.) Each md group active on the server should have one and only one entry in the `/etc/raidtab` file that looks similar to:

```
raiddev              /dev/md2
raid-level                   1
nr-raid-disks                2
chunk-size                   64k
persistent-superblock        1
nr-spare-disks               0
    device           /dev/hda2
    raid-disk      0
    device           /dev/hdc2
    raid-disk      1
```

      If any discrepancies are found between `/etc/raidtab` and the `/proc/mdstat` file, make note of them and proceed to .

8. Run `savelogs` to gather all application logs, (see Saving Logs Using the ELAP **GUI**).

9. Run `savelogs_plat` to gather system information for further troubleshooting, (see Saving Logs Using the ELAP **GUI**), and contact Tekelec Platform Engineering.

3000000000000008 - Server Platform Error

This alarm indicates a major platform error such as a corrupt system configuration or missing files, or indicates that `syscheck` itself is corrupt.

Recovery

1. Run `syscheck` in Verbose mode.
2. Call #unique_13 and provide the system health check output.
3. Log in as `root` to the server that is generating the alarm.

   ```
   Login:  root
   Password: <Enter root password>
   ```

4. Reconfigure syscheck: `# syscheck -reconfig`

   By running this command syscheck will rewrite its configuration files.
5. Exit from root shell: `# exit`
6. Run `syscheck`.
   1. If the alarm has been cleared, the problem is resolved.
   2. If the alarm has not been cleared, continue with the next step.
7. Run `savelogs` to gather all application logs, (see Saving Logs Using the ELAP **GUI**).
8. Run `savelogs_plat` to gather system information for further troubleshooting, (see Saving Logs Using the ELAP **GUI**), and contact Tekelec Platform Engineering.

3000000000000010 - Server File System Error

This alarm indicates that `syscheck` was unsuccessful in writing to at least one of the server file systems.

Recovery

- Call #unique_13 for assistance.

3000000000000020 - Server Platform Process Error

This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.

Recovery

- Contact #unique_13 for recovery procedures.

3000000000000080 - Server Swap Space Shortage Failure

This alarm indicates that the server’s swap space is in danger of being depleted. This is usually caused by a process that has allocated a very large amount of memory over time.

Note:

In order for this alarm to clear, the underlying failure condition must be consistently undetected for a number of polling intervals. Therefore, the alarm may continue to be reported for several minutes after corrective actions are completed.

Recovery

- Call #unique_13 for assistance.

3000000000000100 - Server provisioning network error

Alarm Type: TPD

Description: This alarm indicates that the connection between the server’s eth01ethernet interface and the customer network is not functioning properly. The eth01 interface is at the upper right port on the rear of the server on the EAGLE backplane.

Note:

The interface identified as eth01 on the hardware is identified as eth91 by the software (in syscheck output, for example).

Severity: Major

OID: TpdProvNetworkErrorNotify 1.3.6.1.4.1.323.5.3.18.3.1.2.9

Alarm ID: TKSPLATMA93000000000000100

Recovery

1. Perform the following substeps to verify that the network configuration is correct.
   a. Log in as `elapconfig` on the E5-APP-B server.

      Enter option `1`, `Display Configuration`, from the ELAP Configuration Menu.

```
 /-----ELAP Configuration Menu----------\
/----------------------------------------\
|  1 | Display Configuration             |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                     |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys        |
|----|-----------------------------------|
|  5 | Change Password                   |
|----|-----------------------------------|
|  6 | Platform Menu                     |
|----|-----------------------------------|
|  7 | Configure NTP Server              |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/
Enter Choice:  1
```

Output similar to the following is displayed. The network configuration information related to the provisioning network is highlighted in bold.

```
MPS Side A:  hostname: bahamas-a  hostid: a8c0ca3d
             Platform Version: 2.0.2-4.0.0_50.26.0
             Software Version: ELAP 1.0.1-4.0.0_50.31.0
             Wed Sep  7 15:05:55 EDT 2005
ELAP A Provisioning Network IP Address = 192.168.61.202
ELAP B Provisioning Network IP Address = 192.168.61.203
Provisioning Network Netmask = 255.255.255.0
Provisioning Network Default Router = 192.168.61.250
ELAP A Backup Prov Network IP Address  = Not configured
ELAP B Backup Prov Network IP Address  = Not configured
Backup Prov Network Netmask            = Not configured
Backup Prov Network Default Router     = Not configured
ELAP A Sync Network Address            = 192.168.2.100
ELAP B Sync Network Address            = 192.168.2.200
ELAP A Main DSM Network Address        = 192.168.120.100
ELAP B Main DSM Network Address        = 192.168.120.200
ELAP A Backup DSM Network Address      = 192.168.121.100
ELAP B Backup DSM Network Address      = 192.168.121.200
ELAP A HTTP Port                       = 80
ELAP B HTTP Port                       = 80
ELAP A HTTP SuExec Port                = 8001
ELAP B HTTP SuExec Port                = 8001
ELAP A Banner Connection Port          = 8473
ELAP B Banner Connection Port          = 8473
ELAP A Static NAT Address              = Not configured
ELAP B Static NAT Address              = Not configured
ELAP A LSMS Connection Port            = 7483
ELAP B LSMS Connection Port            = 7483
ELAP A EBDA Connection Port            = 1030
ELAP B EBDA Connection Port            = 1030
Time Zone                              = America/New_York

Press return to continue...
```

b. Verify that the provisioning network **IP** address, netmask, and network default router **IP** address for the server reporting this alarm are correct.

   If configuration changes are needed, refer to the *Administration and LNP Feature Activation Guide* for ELAP.

2. Verify that a customer-supplied cable labeled TO CUSTOMER NETWORK is securely connected to the appropriate server. Follow the cable to its connection point on the local network and verify this connection is also secure.

3. Test the customer-supplied cable labeled TO CUSTOMER NETWORK with an Ethernet Line Tester. If the cable does not test positive, replace it.

4. Have your network administrator verify that the network is functioning properly.
5. If no other nodes on the local network are experiencing problems and the fault has been isolated to the server or the network administrator is unable to determine the exact origin of the problem, contact #unique_13.

3000000000000200 – Server Eagle Network A error

Alarm Type: TPD

Description: This alarm is generated by the MPS syscheck software package and is not part of the TPD distribution.

Description:

> **Note:**
>
> If these three alarms exist, the probable cause is a failed mate server.
>
> - 3000000000000200-Server Eagle Network A Error
> - 3000000000000400-Server Eagle Network B Error
> - 3000000000000800-Server Sync Network Error

This alarm indicates an error in the Main **SM** network, which connects to the SM A ports. The error may be caused by one or more of the following conditions:

- One or both of the servers is not operational.
- One or both of the switches is not powered on.
- The link between the switches is not working.
- The connection between server A and server B is not working.

Some of the connections between the servers of the **SM** networks (main and backup).

- The **eth01** interface (top ethernet port on the rear of the server) connects to the customer provisioning network.
- The **eth02** interface (2nd from top ethernet port on the rear of the server) connects to port 3 of switch A.
- The **eth03** interface (2nd from bottom ethernet port on the rear of the server) connects to port 3 of switch B.
- The **eth04** interface (bottom ethernet port on the rear of the server) connects to port 5 of switch A
- The interfaces on the switch are ports 1 through 20 (from left to right) located on the front of the switch.
- Ports 1 and 2 of switch A connect to ports 1 and 2 of switch B.
- Ports 7 to 24 of switch A and ports 5 through 24 of switch B can be used for links to the Main SM ports (SM A ports) on the EAGLE.

Severity: Major

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.10

Alarm ID: TKSPLATMA103000000000000200

Recovery

1. Perform the following:
   a. Verify that both servers are powered on by ensuring that the **POWER LEDs** on both servers are illuminated green.
   b. Verify that the Ethenet hubs or switches are powered on.
   c. Verify that no fault lights on the Ethenet hubs or switches are illuminated.
2. Perform the following substeps to verify that the network configuration is correct.
   a. Log in as `elapconfig` on the E5-APP-B server.

      Enter option `1`, `Display Configuration`, from the ELAP Configuration Menu.

```
/-----ELAP Configuration Menu----------\
/----------------------------------------\
|  1 | Display Configuration             |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                     |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys        |
|----|-----------------------------------|
|  5 | Change Password                   |
|----|-----------------------------------|
|  6 | Platform Menu                     |
|----|-----------------------------------|
|  7 | Configure NTP Server              |
|----|-----------------------------------|
|  8 | Mate Disaster Recovery            |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/
Enter Choice:  1
```

Output similar to the following is displayed. The network configuration information related to the **EAGLE** Network A (the Main DSM network) is highlighted in bold.

```
MPS Side A:  hostname: bahamas-a  hostid: a8c0ca3d
             Platform Version: 2.0.2-4.0.0_50.26.0
             Software Version: ELAP 1.0.1-4.0.0_50.31.0
             Wed Sep  7 15:05:55 EDT 2005

ELAP A Provisioning Network IP Address = 192.168.61.202
ELAP B Provisioning Network IP Address = 192.168.61.203
Provisioning Network Netmask           = 255.255.255.0
Provisioning Network Default Router    = 192.168.61.250
ELAP A Backup Prov Network IP Address  = Not configured
ELAP B Backup Prov Network IP Address  = Not configured
Backup Prov Network Netmask            = Not configured
Backup Prov Network Default Router     = Not configured
ELAP A Sync Network Address            = 192.168.2.100
ELAP B Sync Network Address            = 192.168.2.200
ELAP A Main DSM Network Address = 192.168.120.100
ELAP B Main DSM Network Address = 192.168.120.200
ELAP A Backup DSM Network Address      = 192.168.121.100
ELAP B Backup DSM Network Address      = 192.168.121.200
ELAP A HTTP Port                       = 80
ELAP B HTTP Port                       = 80
ELAP A HTTP SuExec Port                = 8001
ELAP B HTTP SuExec Port                = 8001
ELAP A Banner Connection Port          = 8473
ELAP B Banner Connection Port          = 8473
ELAP A Static NAT Address              = Not configured
ELAP B Static NAT Address              = Not configured
ELAP A LSMS Connection Port            = 7483
ELAP B LSMS Connection Port            = 7483
ELAP A EBDA Connection Port            = 1030
ELAP B EBDA Connection Port            = 1030
Time Zone                              = America/New_York

Press return to continue...
```

b. Verify that the Main DSM Network **IP** address for the server reporting this alarm is correct.

   If configuration changes are needed, refer to the *Administration and LNP Feature Activation Guide* for ELAP.

3. Verify that both servers are powered on by confirming that the **POWER** LEDs on both servers are illuminated green.
   a. Verify that the switch is powered on.
   b. Verify that the switch does not have any fault lights illuminated.
   c. Verify that the **eth01** cable is securely connected to the top port on the server that is reporting the error.
   d. Trace the **eth01** cable to the switch. Verify that the **eth01** cable is securely connected at correct point of the customer uplink.
   e. Verify that the cable connecting the switches is securely connected at both switches.
4. Run `syscheck`.
   a. If the alarm is cleared, the problem is resolved.
   b. If the alarm is not cleared, continue with the next step.
5. Verify that the cable from **eth01** to the switch tests positive with an Ethernet Line Tester. Replace any faulty cables.
6. If the problem persists, call #unique_13.
7. Perform general **IP** troubleshooting.

   The `syscheck` utility reports this error when it tries to `ping` hosts dsmm-a and dsmm-b a set number of times and fails. This failure could mean any number of things are at fault on the network, but general **IP** troubleshooting will usually resolve the issue. The `platcfg` utility can be used to help isolate the problem. To access the `platcfg` utility:

a. Log in as `platcfg` to the server that is generating the alarm.

```
Login:  platcfg
Password: <Enter platcfg password>
```

b. To display various network information and statistics, select menu options:`Diagnostics->Network Diagnostics->Netstat`

c. To `ping` the dsmb-a and/or dsmb-b select menu options:`Diagnostics->Network Diagnostics->Ping`

d. To verify no routing issues exist, select menu options:`Diagnostics->Network Diagnostics->Traceroute`

8. Run `savelogs` to gather all application logs.
9. Run `savelogs_plat` to gather system information for further troubleshooting, and contact #unique_13.

3000000000000400 – Server Eagle Network B error

Alarm Type: TPD

Description: This alarm is generated by the MPS syscheck software package and is not part of the TPD distribution.

Description:

> **Note:**
>
> If these three alarms exist, the probable cause is a failed mate server.
>
> - 3000000000000200-Server Eagle Network A Error
> - 3000000000000400-Server Eagle Network B Error
> - 3000000000000800-Server Sync Network Error

This alarm indicates an error in the Backup **SM** network, which connects to the SM B ports. The error may be caused by one or more of the following conditions:

- One or both of the servers is not operational.
- One or both of the switches is not powered on.
- The link between the switches is not working.
- The connection between server A and server B is not working.

Some of the connections between the servers of the **SM** networks (main and backup).

- The **eth01** interface (top ethernet port on the rear of the server) connects to the customer provisioning network.

- The **eth02** interface (2nd from top ethernet port on the rear of the server) connects to port 4 of switch A.
- The **eth03** interface (2nd from bottom ethernet port on the rear of the server) connects to port 4 of switch B.
- The **eth04** interface (bottom ethernet port on the rear of the server) connects to port 6 of switch A.
- The interfaces on the switch are ports 1 through 20 (from left to right) located on the front of the switch.
- Ports 1 and 2 of switch A connect to ports 1 and 2 of switch B.
- Ports 7 to 24 of switch A and ports 5 through 24 of switch B can be used for links to the Main SM ports (SM A ports) on the EAGLE.

Severity: Major

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.11

Alarm ID: TKSPLATMA113000000000000400

Recovery

1. Perform the following:
   a. Verify that both servers are powered on by ensuring that the **POWER LEDs** on both servers are illuminated green.
   b. Verify that the Ethernet hubs or switches are powered on.
   c. Verify that no fault lights on the Ethernet hubs or switches are illuminated.
2. Perform the following substeps to verify that the network configuration is correct.
   a. Log in as `elapconfig` on the E5-APP-B server.

      Enter option `1`, `Display Configuration`, from the ELAP Configuration Menu.

```
/-----ELAP Configuration Menu----------\
/-----------------------------------------\
|  1 | Display Configuration              |
|----|------------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|------------------------------------|
|  3 | Set Time Zone                      |
|----|------------------------------------|
|  4 | Exchange Secure Shell Keys         |
|----|------------------------------------|
|  5 | Change Password                    |
|----|------------------------------------|
|  6 | Platform Menu                      |
|----|------------------------------------|
|  7 | Configure NTP Server               |
|----|------------------------------------|
|  8 | Mate Disaster Recovery             |
|----|------------------------------------|
|  e | Exit                               |
\-----------------------------------------/
Enter Choice:  1
```

Output similar to the following is displayed. The network configuration information related to the **EAGLE** Network B (the Backup **DSM** network) is highlighted in bold.

```
MPS Side A:  hostname: bahamas-a  hostid: a8c0ca3d
             Platform Version: 2.0.2-4.0.0_50.26.0
             Software Version: ELAP 1.0.1-4.0.0_50.31.0
             Wed Sep  7 15:05:55 EDT 2005

ELAP A Provisioning Network IP Address = 192.168.61.202
ELAP B Provisioning Network IP Address = 192.168.61.203
Provisioning Network Netmask           = 255.255.255.0
Provisioning Network Default Router    = 192.168.61.250
ELAP A Backup Prov Network IP Address  = Not configured
ELAP B Backup Prov Network IP Address  = Not configured
Backup Prov Network Netmask            = Not configured
Backup Prov Network Default Router     = Not configured
ELAP A Sync Network Address            = 192.168.2.100
ELAP B Sync Network Address            = 192.168.2.200
ELAP A Main DSM Network Address        = 192.168.120.100
ELAP B Main DSM Network Address        = 192.168.120.200
ELAP A Backup DSM Network Address = 192.168.121.100
ELAP B Backup DSM Network Address = 192.168.121.200
ELAP A HTTP Port                       = 80
ELAP B HTTP Port                       = 80
ELAP A HTTP SuExec Port                = 8001
ELAP B HTTP SuExec Port                = 8001
ELAP A Banner Connection Port          = 8473
ELAP B Banner Connection Port          = 8473
ELAP A Static NAT Address              = Not configured
ELAP B Static NAT Address              = Not configured
ELAP A LSMS Connection Port            = 7483
ELAP B LSMS Connection Port            = 7483
ELAP A EBDA Connection Port            = 1030
ELAP B EBDA Connection Port            = 1030
Time Zone                              = America/New_York

Press return to continue...
```

b. Verify that the Backup DSM Network **IP** address for the server reporting this alarm is correct.

   If configuration changes are needed, refer to *Administration and LNP Feature Activation Guide* for ELAP.

3. Verify that both servers are powered on by confirming that the **POWER** LEDs on both servers are illuminated green.

   a. Verify that the switch is powered on.

   b. Verify that the switch does not have any fault lights illuminated.

   c. Verify that the **eth01** cable is securely connected to the top port of the server that is reporting the error.

   d. Trace the **eth01** cable to the switch. Verify that the **eth01** cable is securely connected to the correct point of the customer uplink.

   e. Verify that the cable connecting the switches is securely connected at both switches.

4. Run `syscheck`.
   a. If the alarm is cleared, the problem is resolved.
   b. If the alarm is not cleared, continue with the next step.
5. Verify that the cable from **eth01** to the hub tests positive with an Ethernet Line Tester. Replace any faulty cables.
6. If the problem persists, call #unique_13 for assistance.
7. Perform general **IP** troubleshooting.

   The `syscheck` utility reports this error when it tries to `ping` hosts dsmb-a and dsmb-b a set number of times and fails. This failure could mean any number of things are at fault on the network, but general **IP** troubleshooting will usually resolve the issue. The `platcfg` utility can be used to help isolate the problem. To access the `platcfg` utility:

   a. Log in as `platcfg` to the server that is generating the alarm.

   ```
   Login:  platcfg
   Password: <Enter  platcfg
    password>
   ```

   b. To display various network information and statistics, select menu options:`Diagnostics->Network Diagnostics->Netstat`
   c. To `ping` the dsmm-a and/or dsmm-b select menu options:`Diagnostics->Network Diagnostics->Ping`
   d. To verify no routing issues exist, select menu options:`Diagnostics->Network Diagnostics->Traceroute`
8. Run `savelogs` to gather all application logs, (see Saving Logs Using the ELAP **GUI**).
9. Run `savelogs_plat` to gather system information for further troubleshooting, (see Saving Logs Using the ELAP **GUI**), and contact #unique_13.

3000000000000800 – Server Sync network error

Alarm Type: TPD

Description: This alarm is generated by the MPS syscheck software package and is not part of the TPD distribution.

Description:

> **Note:**
>
> If these three alarms exist, the probable cause is a failed mate server.
>
> - 3000000000000200-Server Eagle Network A Error
> - 3000000000000400-Server Eagle Network B Error
> - 3000000000000800-Server Sync Network Error

This alarm indicates that the **eth03** connection between the two servers is not functioning properly. The **eth03** connection provides a network path over which the servers synchronize data with one another. The **eth03** interface is the 2nd from the bottom ethernet port on the rear of the server.

> **Note:**
>
> The sync interface uses **eth03** and goes through switch B. All pairs are required.

Severity: Major

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.12

Alarm ID: TKSPLATMA12300000000000800

Recovery

1. Verify that both servers are booted up by ensuring that the **POWER LED**s on both servers are illuminated green.
2. Perform the following substeps to verify that the network configuration is correct.
   a. Log in as `elapconfig` on the E5-APP-B server.

      Enter option `1`, `Display Configuration`, from the ELAP Configuration Menu.

```
/-----ELAP Configuration Menu----------\
/----------------------------------------\
|  1 | Display Configuration              |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                      |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys         |
|----|-----------------------------------|
|  5 | Change Password                    |
|----|-----------------------------------|
|  6 | Platform Menu                      |
|----|-----------------------------------|
|  7 | Configure NTP Server               |
|----|-----------------------------------|
|  8 | Mate Disaster Recovery             |
|----|-----------------------------------|
|  e | Exit                               |
\----------------------------------------/
Enter Choice:  1
```

Output similar to the following is displayed. The network configuration information related to the Sync Network is highlighted in bold.

```
MPS Side A:  hostname: bahamas-a  hostid: a8c0ca3d
             Platform Version: 2.0.2-4.0.0_50.26.0
             Software Version: ELAP 1.0.1-4.0.0_50.31.0
             Wed Sep  7 15:05:55 EDT 2005
ELAP A Provisioning Network IP Address = 192.168.61.202
ELAP B Provisioning Network IP Address = 192.168.61.203
Provisioning Network Netmask           = 255.255.255.0
Provisioning Network Default Router    = 192.168.61.250
ELAP A Backup Prov Network IP Address  = Not configured
ELAP B Backup Prov Network IP Address  = Not configured
Backup Prov Network Netmask            = Not configured
Backup Prov Network Default Router     = Not configured
ELAP A Sync Network Address = 192.168.2.100
ELAP B Sync Network Address = 192.168.2.200
ELAP A Main DSM Network Address        = 192.168.120.100
ELAP B Main DSM Network Address        = 192.168.120.200
ELAP A Backup DSM Network Address      = 192.168.121.100
ELAP B Backup DSM Network Address      = 192.168.121.200
ELAP A HTTP Port                       = 80
ELAP B HTTP Port                       = 80
ELAP A HTTP SuExec Port                = 8001
ELAP B HTTP SuExec Port                = 8001
ELAP A Banner Connection Port          = 8473
ELAP B Banner Connection Port          = 8473
ELAP A Static NAT Address              = Not configured
ELAP B Static NAT Address              = Not configured
ELAP A LSMS Connection Port            = 7483
ELAP B LSMS Connection Port            = 7483
ELAP A EBDA Connection Port            = 1030
ELAP B EBDA Connection Port            = 1030
Time Zone                              = America/New_York

Press return to continue...
```

b. Verify that the Sync Network **IP** address for the server reporting this alarm is correct.

   If configuration changes are needed, refer to *ELAP Administration and LNP Feature Activation*.

3. If the problem persists, contact #unique_13.

3000000000001000 - Server Disk Space Shortage Error

This alarm indicates that one of the following conditions has occurred:

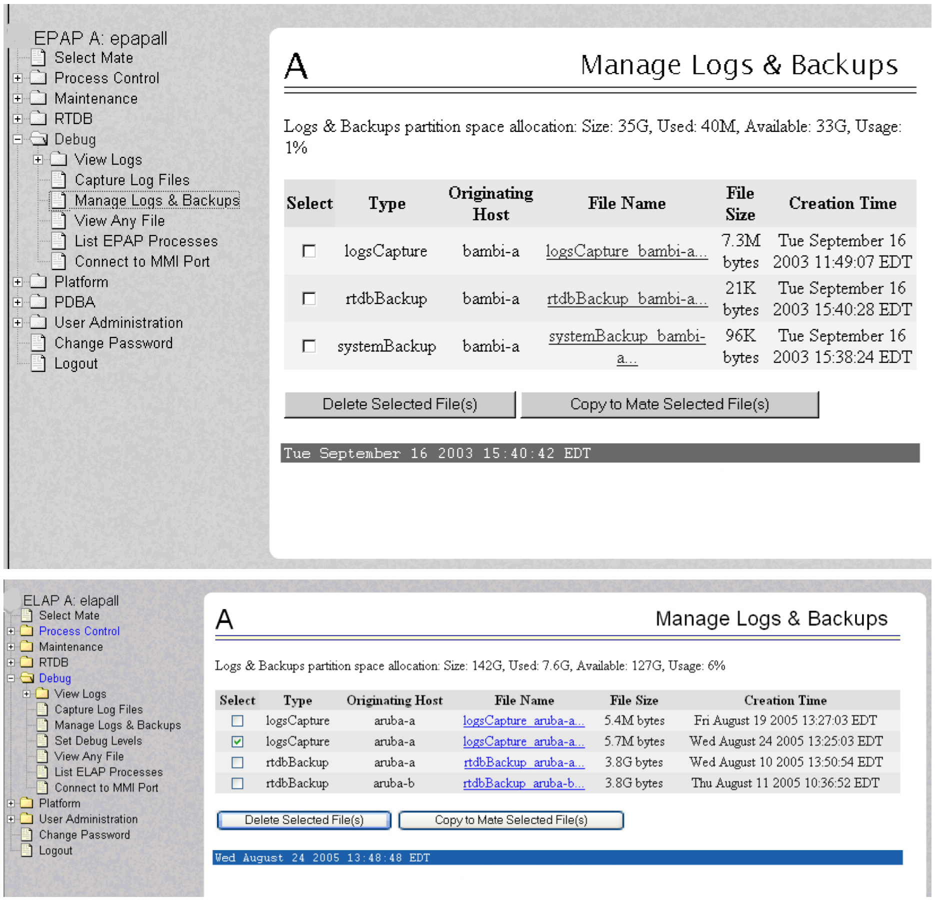
- A file system has exceeded a failure threshold, which means that more than 90% of the available disk storage has been used on the file system.
- More than 90% of the total number of available files have been allocated on the file system.
- A file system has a different number of blocks than it had when installed.

Recovery

1. Run `syscheck` (see Running syscheck Through the ELAP GUI).
2. Examine the syscheck output to determine if the file system `/var/TKLC/epap/free/var/TKLC/elap/free` is low on space. If it is, continue to the next step; otherwise go to 4.
3. If possible, recover space on the free partition by deleting unnecessary files:
   a. Log in to the ELAP **GUI** (see Running syscheck Through the ELAP GUI).
   b. Select **Debug>Manage Logs & Backups**.

      A screen similar to Figure 5-1 is displayed. This screen displays information about the total amount of space allocated for and currently used by logs and backups. The display includes logs and backup files which might be selected for deletion to recover additional disk space.

Figure 5-1 Manage Logs and Backups



Logs & Backups partition space allocation: Size: 35G, Used: 40M, Available: 33G, Usage: 1%

Select	Type	Originating Host	File Name	File Size	Creation Time
□	logsCapture	bambi-a	logsCapture_bambi-a...	7.3M bytes	Tue September 16 2003 11:49:07 EDT
□	rtdbBackup	bambi-a	rtdbBackup_bambi-a...	21K bytes	Tue September 16 2003 15:40:28 EDT
□	systemBackup	bambi-a	systemBackup_bambi-a...	96K bytes	Tue September 16 2003 15:38:24 EDT

Tue September 16 2003 15:40:42 EDT

Logs & Backups partition space allocation: Size: 142G, Used: 7.6G, Available: 127G, Usage: 6%

Select	Type	Originating Host	File Name	File Size	Creation Time
□	logsCapture	aruba-a	logsCapture_aruba-a...	5.4M bytes	Fri August 19 2005 13:27:03 EDT
☑	logsCapture	aruba-a	logsCapture_aruba-a...	5.7M bytes	Wed August 24 2005 13:25:03 EDT
□	rtdbBackup	aruba-a	rtdbBackup_aruba-a...	3.8G bytes	Wed August 10 2005 13:50:54 EDT
□	rtdbBackup	aruba-b	rtdbBackup_aruba-b...	3.8G bytes	Thu August 11 2005 10:36:52 EDT

Wed August 24 2005 13:48:48 EDT

   c. Click the checkbox of each file to be deleted, then click **Delete Selected File(s)**.
4. Call #unique_13 for assistance.

3000000000002000 - Server Default Route Network Error

This alarm indicates that the default network route of the server is experiencing a problem. Running `syscheck` in Verbose mode will provide information about which type of problem.

> **Caution:**
>
> When changing the network routing configuration of the server, verify that the modifications will not impact the method of connectivity for the current login session. The route information must be entered correctly and set to the correct values. Incorrectly modifying the routing configuration of the server may result in total loss of remote network access.

Recovery

1. Run `syscheck` in Verbose mode (see Running the System Health Check).

   The output should indicate one of the following errors:

   - `The default router at <IP_address> cannot be pinged.`

     This error indicates that the router may not be operating or is unreachable. If the `syscheck` Verbose output returns this error, go to 2 .

   - `The default route is not on the provisioning network.`

     This error indicates that the default route has been defined in the wrong network. If the `syscheck` Verbose output returns this error, go to 3.

   - `An active route cannot be found for a configured default route.`

     This error indicates that a mismatch exists between the active configuration and the stored configuration. If the `syscheck` Verbose output returns this error, go to 4.

   > **Note:**
   >
   > If the `syscheck` Verbose output does not indicate one of the errors above, go to step 5.

2. Perform the following substeps when `syscheck` Verbose output indicates:

   ```
   The default router at <IP_address> cannot be pinged
   ```

   a. Verify that the network cables are firmly attached to the server, network switch, router, Ethernet switch or hub, and any other connection points.

   b. Verify that the configured router is functioning properly.

Request that the network administrator verify the router is powered on and routing traffic as required.

c. Request that the router administrator verify that the router is configured to reply to pings on that interface.

d. Run `syscheck`.

  - If the alarm is cleared, the problem is resolved and this procedure is complete.
  - If the alarm is not cleared, go to 5.

3. Perform the following substeps when `syscheck` Verbose output indicates:

```
The default route is not on the provisioning network
```

a. Obtain the proper Provisioning Network netmask and the **IP** address of the appropriate Default **Route** on the provisioning network.

   This information is maintained by the customer network administrators.

b. Log in to the **MPS** with user name `elapconfig`.

   The server designation at this site is displayed as well as **hostname**, **hostid**, **Platform Version**,
   Software Version, and the date. Verify that the side displayed is the MPS that is reporting the problem. In this example, it is MPS A. Enter option `2`, `Configure Network Interfaces Menu`, from the ELAP Configuration Menu.

```
MPS Side A:  hostname: mpsa-d1a8f8  hostid: 80d1a8f8
             Platform Version: x.x.x-x.x.x
             Software Version: ELAP x.x.x-x.x.x
             Wed Jul 17 09:51:47 EST 2005
/-----ELAP Configuration Menu----------\
/--------------------------------------\
|  1 | Display Configuration             |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                     |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys        |
|----|-----------------------------------|
|  5 | Change Password                   |
|----|-----------------------------------|
|  6 | Platform Menu                     |
|----|-----------------------------------|
|  7 | Configure NTP Server              |
|----|-----------------------------------|
|  8 | Mate Disaster Recovery            |
|----|-----------------------------------|
|  e | Exit                              |
\-----------------------------------------/
Enter Choice:  2
```

c. Enter option `1`, `Configure Provisioning Network`, from the Configure Network Interfaces Menu.

   The submenu for configuring communications networks and other information is displayed.

```
/-----Configure Network Interfaces Menu-\
/-----------------------------------------\
|  1 | Configure Provisioning Network     |
|----|------------------------------------|
|  2 | Configure DSM Network              |
|----|------------------------------------|
|  3 | Configure Forwarded Ports          |
|----|------------------------------------|
|  4 | Configure Static NAT Addresses     |
|----|------------------------------------|
|  e | Exit                               |
\-----------------------------------------/

Enter choice:  1
```

   This warning is displayed.

```
ELAP software is running. Stop it? [N] Y
```

d. Type `Y` and press **Enter**.

e. If the **LSMS** Connection has not been previously disabled, the following prompt is displayed. Type `Y` and press **Enter**.

```
The LSMS Connection is currently enabled. Do you want to disable it?
[Y]  Y
```

   This confirmation is displayed.

```
The LSMS Connection has been disabled.
```

   The ELAP A provisioning network IP address is displayed.

```
Verifying connectivity with mate ...
Enter the ELAP A provisioning network IP Address [192.168.61.90]:
```

f. Press **Enter** after each address is displayed until the Default **Route** address displays.

```
Verifying connectivity with mate ...
```

```
Enter the ELAP A provisioning network IP Address
[192.168.61.90]: Enter the ELAP B provisioning network IP
Address [192.168.61.91]: Enter the ELAP provisioning network
netmask [255.255.255.0]:
Enter the ELAP provisioning network default router IP Address:
192.168.61.250
```

g. If the default router IP address is incorrect, type the correct address and press **Enter**.

h. After the Provisioning Network configuration information is verified and corrected, type `e` to return to the Configure Network Interfaces Menu.

i. Type `e` again to return to the ELAP Configuration Menu.

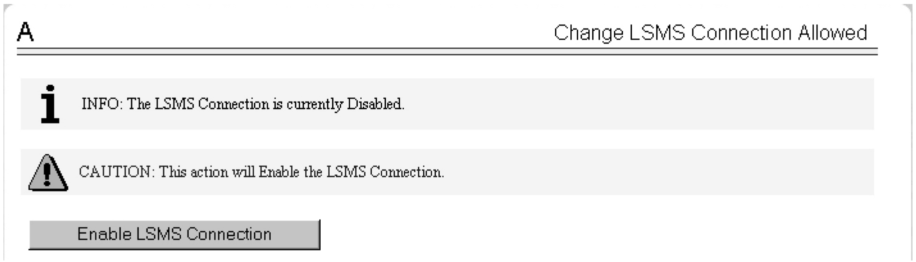
j. Run `syscheck`.

   - If the alarm is cleared, the problem is resolved. Restart the ELAP software and enable the connection to the **LSMS** as described in 3.k, 3.l, and 3.m.
   - If the alarm is not cleared, go to 5.

k. Restart the ELAP software.

l. Select **Maintenance>LSMS Connection>Change Allowed**: a window similar to the example shown in Figure 5-4 displays.

Figure 5-2   Enable LSMS Connection Window



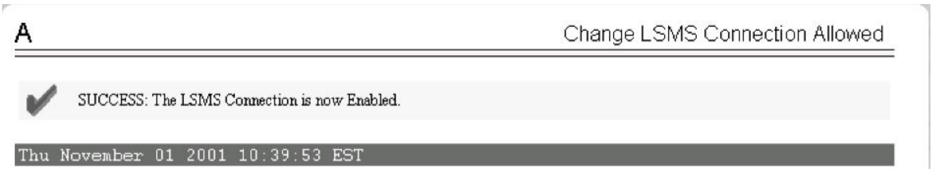
INFO: The LSMS Connection is currently Disabled.

CAUTION: This action will Enable the LSMS Connection.

m. Click the **Enable LSMS Connection** button.

After the connection is enabled, the workspace displays the information shown in Figure 5-3.

Figure 5-3   LSMS Connection Enabled



SUCCESS: The LSMS Connection is now Enabled.

Thu November 01 2001 10:39:53 EST

This procedure is complete.

4. Perform the following substeps to reboot the server if the `syscheck` Verbose output indicates the following error:

```
An active route cannot be found for a configured default route, . .
```

   a. Log in as `elapconfig` on the E5-APP-B server.

      Enter option `6`, `Platform Menu`, from the ELAP Configuration Menu.

```
 /-----ELAP Configuration Menu----------\
/----------------------------------------\
|  1 | Display Configuration             |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                     |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys        |
|----|-----------------------------------|
|  5 | Change Password                   |
|----|-----------------------------------|
|  6 | Platform Menu                     |
|----|-----------------------------------|
|  7 | Configure NTP Server              |
|----|-----------------------------------|
|  8 | Mate Disaster Recovery            |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/
Enter Choice: 6
```

   b. Enter option `2`, `Reboot MPS`, from the ELAP Platform Menu.

      At the prompt, enter the identifier of the MPS to which you are logged in (`A` or `B`); in this example, `A` is used.

```
/-----ELAP Platform Menu-\
/--------------------------\
|  1 | Initiate Upgrade    |
|----|---------------------|
|  2 | Reboot MPS          |
|----|---------------------|
|  3 | MySQL Backup        |
|----|---------------------|
|  4 | RTDB Backup         |
|----|---------------------|
|  e | Exit                |
\--------------------------/
Enter Choice:  2

Are you sure you want to reboot the MPS?
```

```
Reboot MPS A, MPS B or BOTH? [BOTH]:  A
Reboot local MPS...
```

c. Wait for the reboot to complete.

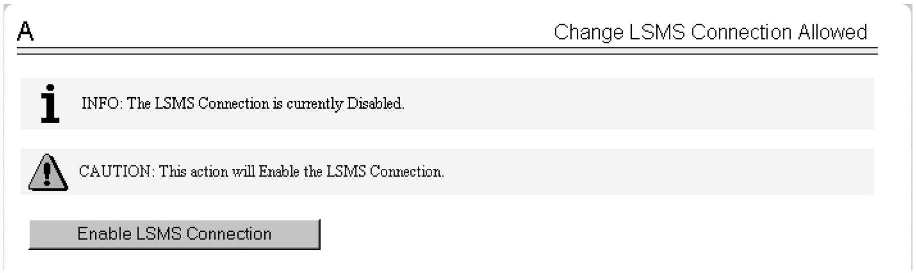
d. Run `syscheck`.

   - If the alarm is cleared, the problem is resolved. Restart the ELAP software and enable the connection to the **LSMS** as described in 4.e, 4.f, and 4.g.
   - If the alarm is not cleared, go to 5.

e. Restart the ELAP software.

f. Select **Maintenance>LSMS Connection>Change Allowed**: a window similar to the example shown in Figure 5-4 displays.

Figure 5-4 Enable LSMS Connection Window



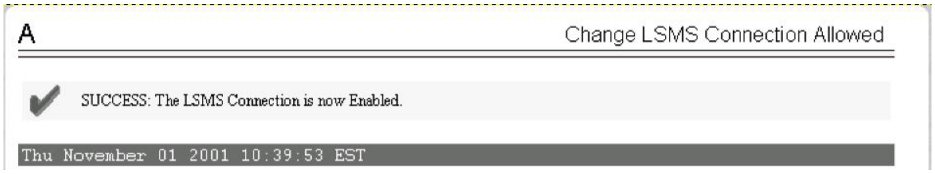
INFO: The LSMS Connection is currently Disabled.

CAUTION: This action will Enable the LSMS Connection.

g. Click the Enable **LSMS** Connection button.

   After the connection is enabled, the workspace displays the information shown in Figure 5-5.

Figure 5-5 LSMS Connection Enabled



SUCCESS: The LSMS Connection is now Enabled.

Thu November 01 2001 10:39:53 EST

This procedure is complete.

5. Contact #unique_13 for further assistance. Provide the `syscheck` output collected in the previous steps.

3000000000004000 - Server Temperature Error

Alarm Type: TPD

Description: The internal temperature within the server is unacceptably high.

Severity: Major

OID: TpdTemperatureErrorNotify 1.3.6.1.4.1.323.5.3.18.3.1.2.15

Alarm ID: TKSPLATMA153000000000004000

Recovery

1. Ensure that nothing is blocking the fan's intake. Remove any blockage.
2. Verify that the temperature in the room is normal with the following table. If it is too hot, lower the temperature in the room to an acceptable level.

Table 5-3 Server Environmental Conditions

Ambient Temperature	Operating: 5 degrees C to 40 degrees C Exceptional Operating Limit: 0 degrees C to 50 degrees C Storage: -20 degrees C to 60 degrees C
Ambient Temperature	Operating: 5° C to 35° C Storage: -20° C to 60° C
Relative Humidity	Operating: 5% to 85% non-condensing Storage: 5% to 950% non-condensing
Elevation	Operating: -300m to +300m Storage: -300m to +1200m
Heating, Ventilation, and Air Conditioning	Capacity must compensate for up to 5100 BTUs/hr for each installed frame. Calculate HVAC capacity as follows: Determine the wattage of the installed equipment. Use the formula: watts x 3.143 = BTUs/hr

> **Note:**
>
> Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. The alarm may take up to five minutes to clear after conditions improve. It may take about ten minutes after the room returns to an acceptable temperature before syscheck shows the alarm cleared.

3. Verify that the temperature in the room is normal. If it is too hot, lower the temperature in the room to an acceptable level.

> **Note:**
>
> Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. It may take about ten minutes after the room returns to an acceptable temperature before the alarm cleared.

4. Run syscheck Check to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.

5. Run syscheck Check to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.
6. Replace the filter (refer to the appropriate hardware manual).

> **Note:**
>
> Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. The alarm may take up to five minutes to clear after conditions improve. It may take about ten minutes after the filter is replaced before syscheck shows the alarm cleared.

7. Run syscheck.
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.
8. If the problem has not been resolved, contact #unique_13.

3000000000008000 - Server Mainboard Voltage Error

This alarm indicates that at least one monitored voltages on the server mainboard is not within the normal operating range.

Recovery

- Contact #unique_13 for assistance.

3000000000010000 - Server Power Feed Error

This alarm indicates that one of the power feeds to the server has failed.

Recovery

1. Locate the server supplied by the faulty power feed. Verify that all connections to the power supply units are connected securely. To determine where the cables connect to the servers, see the Power Connections and Cables page of the ELAP E5-APP-B Interconnect.
2. Run `syscheck` (see Running syscheck Through the ELAP GUI).
   a. If the alarm is cleared, the problem is resolved.
   b. If the alarm is not cleared, go to 3.
3. Trace the power feed to its connection on the power source.

   Verify that the power source is on and that the power feed is properly secured.
4. Run `syscheck` (see Running syscheck Through the ELAP GUI).
   a. If the alarm is cleared, the problem is resolved.
   b. If the alarm is not cleared, go to 5.
5. If the power source is functioning properly and all connections are secure, request that an electrician check the voltage on the power feed.

6. Run `syscheck` (see Running syscheck Through the ELAP GUI).
   a. If the alarm is cleared, the problem is resolved.
   b. If the alarm is not cleared, go to 7.
7. If the problem is not resolved, call #unique_13 for assistance.
8. Run `savelogs_plat` to gather system information for further troubleshooting, (see Saving Logs Using the ELAP **GUI**), and contact #unique_13.

3000000000020000 - Server Disk Health Test Error

This alarm indicates that the hard drive has failed or failure is imminent.

Recovery

- Immediately contact #unique_13 for assistance with a disk replacement.

3000000000040000 - Server Disk Unavailable Error

This alarm indicates that the `smartd` service is not able to read the disk status because the disk has other problems that are reported by other alarms. This alarm appears only while a server is booting.

Recovery

- Perform the recovery procedures for the other alarms that accompany this alarm.

3000000000080000 - Device Error

This alarm indicates that the offboard storage server has a problem with its disk volume filling.

Recovery

- Call #unique_13 for assistance.

3000000000100000 - Device Interface Error

This alarm indicates that the IP bond is either not configured or not functioning.

Recovery

- Call #unique_13 for assistance.

3000000000200000 - Correctable ECC Memory Error

This alarm indicates that chipset has detected a correctable (single-bit) memory error that has been corrected by the Error-Correcting Code (**ECC**) circuitry in the memory.

Recovery

- No recovery necessary.

  If the condition persists, contact #unique_13 to request hardware replacement.

3000000400000000 - Multipath device access link problem

Alarm Type: TPD

Description: One or more "access paths" of a multipath device are failing or are not healthy, or the multipath device does not exist.

Severity: Major

OID: TpdMpathDeviceProblemNotify1.3.6.1.4.1.323.5.3.18.3.1.2.35

Alarm ID: TKSPLATMA353000000400000000

Recovery

1. #unique_13 should do the following:
   a. Check in the MSA administration console (web-application) that correct "volumes" on MSA exist, and read/write access is granted to the blade server.
   b. Check if multipath daemon/service is running on the blade server: service multipathd status. Resolution:
      i. start multipathd: service multipathd start
   c. Check output of "multipath -ll": it shows all multipath devices existing in the system and their access paths; check that particular /dev/sdX devices exist. This may be due to SCSI bus and/or FC HBAs haven't been rescanned to see if new devices exist. Resolution:
      i. run "/opt/hp/hp_fibreutils/hp_rescan -a",
      ii. "echo 1 > /sys/class/fc_host/host*/issue_lip",
      iii. "echo '- - -' > /sys/class/scsi_host/host*/scan"
   d. Check if syscheck::disk::multipath test is configured to monitor right multipath devices and its access paths: see output of "multipath -ll" and compare them to "syscheckAdm disk multipath - -get - -var=MPATH_LINKS" output. Resolution:
      i. configure disk::multipath check correctly.
2. Contact #unique_13.

3000000800000000 – Switch Link Down Error

This alarm indicates that the switch is reporting that the link is down. The link that is down is reported in the alarm. For example, port 1/1/2 is reported as 1102.

Recovery Procedure:

1. Verify cabling between the offending port and remote side.
2. Verify networking on the remote end.
3. If problem persists, contact #unique_13 to verify port settings on both the server and the switch.

3000001000000000 - Half-open Socket Limit

Alarm Type: TPD

Description: This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.

Severity: Major

OID: tpdHalfOpenSocketLimit 1.3.6.1.4.1.323.5.3.18.3.1.2.37

Alarm ID: TKSPLATMA37 3000001000000000

Recovery

- Contact #unique_13.

3000002000000000 - Flash Program Failure

Alarm Type: TPD

Description: This alarm indicates there was an error while trying to update the firmware flash on the E5-APP-B cards.

Severity: Major

OID: tpdFlashProgramFailure 1.3.6.1.4.1.323.5.3.18.3.1.2.38

Alarm ID: TKSPLATMA383000002000000000

Recovery

- Contact #unique_13.

3000004000000000 - Serial Mezzanine Unseated

Alarm Type: TPD

Description: This alarm indicates the serial mezzanine board was not properly seated.

Severity: Major

OID: tpdSerialMezzUnseated 1.3.6.1.4.1.323.5.3.18.3.1.2.39

Alarm ID: TKSPLATMA393000004000000000

Recovery

- Contact #unique_13.

3000000008000000 - Server HA Keepalive Error

This alarm indicates that heartbeat process has detected that it has failed to receive a heartbeat packet within the timeout period.

Recovery

1. Determine if the mate server is currently operating. If the mate server is not operating, attempt to restore it to operation.
2. Determine if the keepalive interface is operating.
3. Determine if heartbeart is running (service TKLCha status).

4. Call #unique_13 for assistance.

3000000010000000 - DRBD block device can not be mounted

This alarm indicates that DRBD is not functioning properly on the local server. The DRBD state (disk state, node state, or connection state) indicates a problem.

Recovery

- Call #unique_13 for assistance.

3000000020000000 - DRBD block device is not being replicated to peer

This alarm indicates that DRBD is not replicating to the peer server. Usually this alarm indicates that DRBD is not connected to the peer server. A DRBD Split Brain may have occurred.

Recovery

1. Determine if the mate server is currently operating.
2. Call #unique_13 for assistance.

3000000040000000 - DRBD peer needs intervention

This alarm indicates that DRBD is not functioning properly on the peer server. DRBD is connected to the peer server, but the DRBD state on the peer server is either unknown or indicates a problem.

Recovery

- Call #unique_13 for assistance.

3000020000000000 - Server NTP Daemon never synchronized

Alarm Type: TPD

Description: This alarm indicates that the NTP sync file (/var/TKLC/log/syscheck/ntp_sync_config) and the NTP last known good time file (/var/TKLC/log/syscheck/ntp_last_good_time) have not been synchronized.

Severity: Major

Alarm ID: TKSPLATMA42

Recovery

Contact #unique_13.

Major Application Alarms

The major application alarms involve the ELAP software, **RTDBs**, file system, and logs.

4000000000000001 - Mate ELAP Unavailable

One ELAP has reported that the other ELAP is unreachable.

Recovery

1. Log in to the ELAP**GUI** (see Accessing the ELAP GUI Interface).
2. View the ELAP status on the banner.
   - If the mate ELAP status is **DOWN**, go to 4 .
   - If the mate ELAP status is **ACTIVE** or **STANDBY**, go to 7.
3. Select the **Select Mate** menu item to change to the mate ELAP.
4. Select **Process Control>Start Software** to start the mate ELAP software.
5. View the ELAP status on the banner.
   - If the mate ELAP status is **ACTIVE** or **STANDBY**, the problem is resolved.
   - If the mate ELAP status is still **DOWN**, continue with 6.
6. Select the **Select Mate** menu item to change back to the side that reported the alarm.
7. Stop and start the software on the side that is reporting the alarm (see Restarting the ELAP Software).
8. If the problem persists, run `savelogs` to gather system information for further troubleshooting (see Saving Logs Using the ELAP **GUI**), and contact #unique_13.

4000000000000002 - RTDB Mate Unavailable

The local ELAP cannot use the direct link to the Standby for **RTDB** database synchronization.

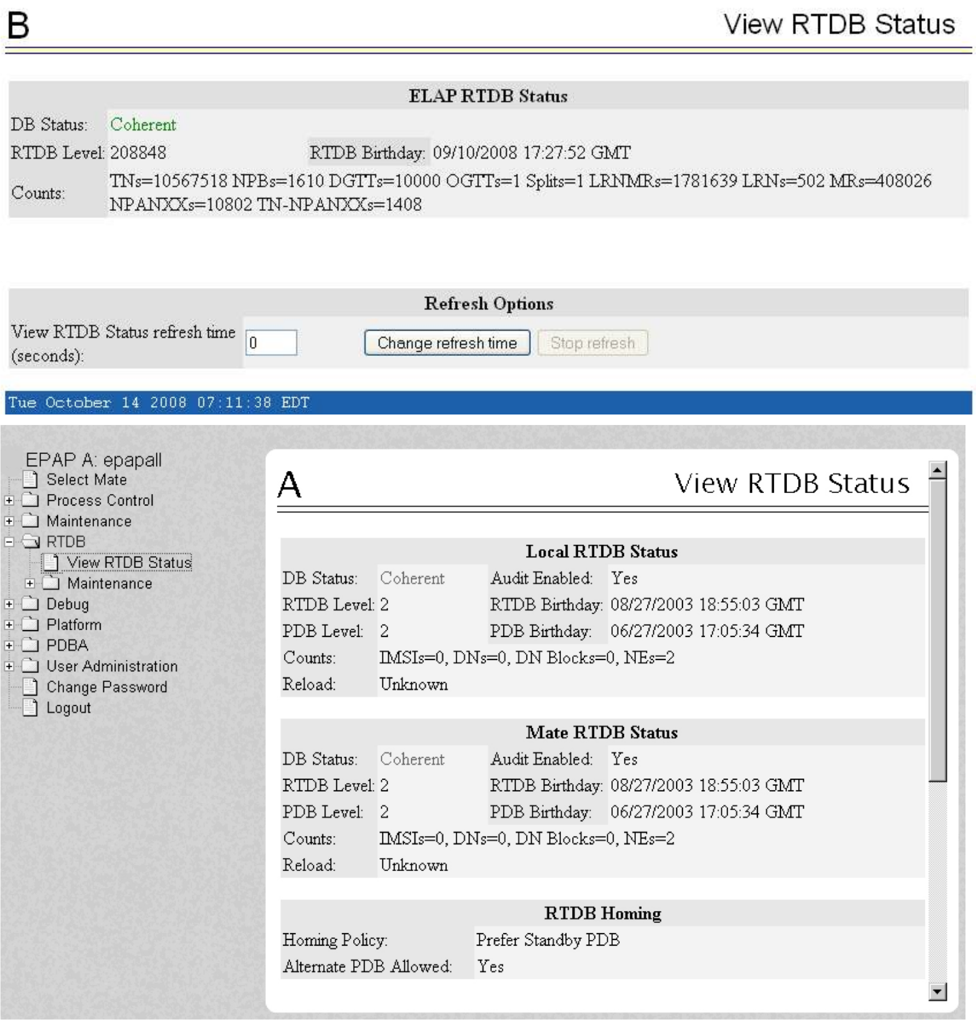
Recovery

1. Log in to the ELAP**GUI** (see Accessing the ELAP GUI Interface).
2. View the ELAP status on the banner.
   - If the mate ELAP status is **DOWN**, go to 4.
   - If the mate ELAP status is **ACTIVE** or **STANDBY**, go to 7.
3. Select the **Select Mate** menu item to change to the mate ELAP.
4. Select **Process Control>Start Software** to start the mate ELAP software.
5. Determine whether the alarm has cleared by verifying whether it is still being displayed in the banner or in the **Alarm** View window.
   - If the alarm has cleared, the problem is resolved.
   - If the alarm has not yet cleared, continue with 6.
6. Ensure that you are logged into the side opposite from the side reporting the alarm.

   If it is necessary to change sides, select the **Select Mate** menu item to change to the side opposite the side that reported the alarm.
7. Stop and start the software on the side that is reporting the alarm (see Restarting the ELAP Software).

8. Select **RTDB>View RTDB Status** to verify that the **RTDB** status on both sides is coherent, as shown in Figure 5-6.

Figure 5-6 Coherent RTDB Status



B View RTDB Status

ELAP RTDB Status			
DB Status:	Coherent		
RTDB Level:	208848	RTDB Birthday:	09/10/2008 17:27:52 GMT
Counts:	TNs=10567518 NPBs=1610 DGTTs=10000 OGTTs=1 Splits=1 LRNMRs=1781639 LRNs=502 MRs=408026 NPANXXs=10802 TN-NPANXXs=1408		

Refresh Options	
View RTDB Status refresh time (seconds):	0

Tue October 14 2008 07:11:38 EDT

A View RTDB Status

Local RTDB Status			
DB Status:	Coherent	Audit Enabled:	Yes
RTDB Level:	2	RTDB Birthday:	08/27/2003 18:55:03 GMT
PDB Level:	2	PDB Birthday:	06/27/2003 17:05:34 GMT
Counts:	IMSIs=0, DNs=0, DN Blocks=0, NEs=2		
Reload:	Unknown		

Mate RTDB Status			
DB Status:	Coherent	Audit Enabled:	Yes
RTDB Level:	2	RTDB Birthday:	08/27/2003 18:55:03 GMT
PDB Level:	2	PDB Birthday:	06/27/2003 17:05:34 GMT
Counts:	IMSIs=0, DNs=0, DN Blocks=0, NEs=2		
Reload:	Unknown		

RTDB Homing	
Homing Policy:	Prefer Standby PDB
Alternate PDB Allowed:	Yes

9. If the problem persists, run `savelogs` to gather system information for further troubleshooting (see Saving Logs Using the ELAP **GUI**), and contact #unique_13.

4000000000000004 - Congestion

The ELAP **RTDB** database record cache used to keep updates currently being provisioned is above 80% capacity.

Recovery

1. At the EAGLE input terminal, enter the `rept-stat-mps` command to verify the status.

   Refer to *Commands User's Guide* to interpret the output.

2. If the problem does not clear within 2 hours with an "ELAP Available" notice, capture the log files on both ELAPs (see Saving Logs Using the ELAP **GUI**) and contact #unique_13.

4000000000000008 - File System Full

This alarm indicates that the server file system is full.

Recovery

- Call #unique_13 for assistance.

4000000000000010 - Log Failure

This alarm indicates that the system was unsuccessful in writing to at least one log file.

- Call #unique_13 for assistance.

4000000000000040 - Fatal Software Error

A major software component on the ELAP has failed.

Recovery

1. Perform Restarting the ELAP Software
2. Capture the log files on both ELAPs (see Saving Logs Using the ELAP **GUI**) and contact #unique_13.

4000000000000080 - RTDB Corrupt

A real-time database is corrupt. The calculated checksum did not match the checksum value stored for one or more records.

Recovery

- Capture the log files on both ELAPs (see Saving Logs Using the ELAP **GUI**) and contact #unique_13.

4000000000000100 - RTDB Inconsistent

The real-time database for one or more Service Module cards is inconsistent with the current real-time database on the Active ELAP fixed disks.

Recovery

- Capture the log files on both ELAPs (see Saving Logs Using the ELAP **GUI**) and contact #unique_13.

4000000000000200 - RTDB Incoherent

This message usually indicates that the **RTDB** database download is in progress.

When the download is complete, the following **UIM** message will appear:

```
0452 - RTDB reload complete
```

Recovery

1. If this alarm displays while an **RTDB** download is in progress, no further action is necessary.
2. If this alarm displays when an **RTDB** download is not in progress, capture the log files on both ELAPs (see Saving Logs Using the ELAP **GUI**) and contact #unique_13.

4000000000000800 - Transaction Log Full

The transaction log is full.

Recovery

- Contact #unique_13.

4000000000001000 - RTDB 100% Full

The **RTDB** on the ELAP is at capacity. The ELAP **RTDB** is not updating.

You may be able to free up space by deleting unnecessary data in the database. The ELAP must be upgraded in order to add disk capacity.

Recovery

- Contact #unique_13 for assistance.

4000000000002000 - RTDB Resynchronization In Progress

This message indicates that the **RTDB** resynchronization is in progress.

Recovery

- No further action is necessary.

4000000000004000 - RTDB Reload Is Required

This message indicates that the **RTDB** reload is required because the transaction logs did not contain enough information to resynchronize the databases (the transaction logs may be too small).

> **Caution:**
>
> If both sides are reporting this error, contact #unique_13.

If only one side is reporting this error, use the following procedure.

Recovery

1. Log in to the User Interface screen of the ELAP (see Accessing the ELAP Text Interface).

2. Refer to *LNP Database Synchronization* for the correct procedures.
3. If the problem persists, contact #unique_13.

4000000000400000 - LVM Snapshot detected that is too old

> **Note:**
>
> LVM alarms are valid for ELAP 8.0 and later.

This alarm indicates that an LVM snapshot has been present on the system for longer than 30 minutes. LVM snapshots should not exist for longer than 15 minutes or performance may be degraded as the LVM snapshot overfills with data.

The **Logical Volume Manager** (**LVM**) creates read-only snapshots of the database. These LVM snapshots are present when an audit of the LSMS database is active and when the database is being downloaded to EAGLE. An LVM snapshot provides rollback and recovery capability to the active database. All LVM snapshots are removed when no longer needed, or are removed and recreated when in continuous use such as during an LSMS audit which may last several hours.

Recovery

- Contact #unique_13.

4000000000800000 - LVM Snapshot detected that is too full

This alarm usually occurs when an LVM snapshot has remained in existence too long and has a higher full percentage than expected; however, the alarm may occur also if an unusually large number of updates, distributed evenly across the entire database, have been received.

The **Logical Volume Manager** (**LVM**) creates read-only snapshots of the database. These LVM snapshots are present when an audit of the LSMS database is active and when the database is being downloaded to EAGLE. An LVM snapshot provides rollback and recovery capability to the active database. All LVM snapshots are removed when no longer needed, or are removed and recreated when in continuous use such as during an LSMS audit which may last several hours.

Recovery

- Contact #unique_13.

4000000001000000 - LVM Snapshot detected with invalid attributes

An LVM snapshot has been detected with invalid attributes. This alarm may occur if an LVM snapshot cannot be removed completely due to an error in the LVM subsystem. Restarting the ELAP software may clear this condition.

Recovery

- Contact #unique_13.

4000000002000000 - DRBD Split Brain

This alarm occurs when the ELAP A and B servers have simultaneous outages or if the three heartbeat paths are lost between the two servers. If either condition occurs, neither server can determine which server has the most recent copy of the database. The first system to recover becomes the HA active system. Manual action is required to determine which copy of the shared data is valid and to resynchronize with the other system.

Recovery

- Contact #unique_13.

4000000010000000 - An instance of Snapmon already running

This is an indication that the ELAP snapshot monitoring of LVM snapshots is in progress. The monitoring is done every 10 minutes via snapmon cron job. The following lnpdb snapshots are monitored:

- prov1snap
- prov2snap
- auditsnap
- backupsnap

Recovery

- Contact #unique_13

Minor Platform Alarms

Minor platform alarms involve disk space, application processes, **RAM**, and configuration errors.

1000000000000001 – Breaker panel feed unavailable

Alarm Type: TPD

Description: This alarm is generated by the MPS syscheck software package and is not part of the **TPD** distribution. Refer to MPS-specific documentation for information regarding this alarm.

Severity: Critical

OID: 1.3.6.1.4.1.323.5.3.18.3.1.1.1

Alarm ID: TKSPLATCR1

Recovery

1. See 910-5129-001 Rev. A, PM&C/T5100 Platform Troubleshooting Guide.
2. Contact #unique_13.

5000000000000001 - Server Disk Space Shortage Warning

This alarm indicates that one of the following conditions has occurred:

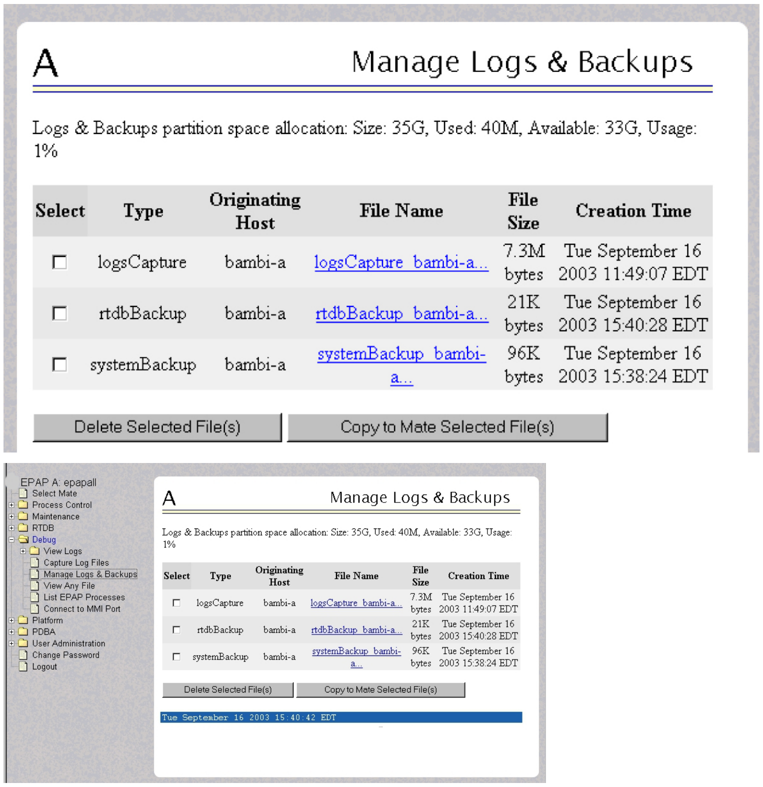
- A file system has exceeded a warning threshold, which means that more than 80% (but less than 90%) of the available disk storage has been used on the file system.
- More than 80% (but less than 90%) of the total number of available files have been allocated on the file system.

Recovery

1. Run `syscheck` (see Running syscheck Through the ELAP GUI)
2. Examine the `syscheck` output to determine if the file system `/var/TKLC/epap/free/var/TKLC/elap/free` is the one that is low on space. If the file system is low on disk space, continue to 3; otherwise go to 4.
3. You may be able to free up space on the free partition by deleting unnecessary files, as follows:
   a. Log in to the ELAP**GUI** (see Accessing the ELAP GUI Interface)
   b. Select **Debug>Manage Logs & Backups**.

      A screen similar to Figure 5-7 is displayed. This screen displays information about the total amount of space allocated for and currently used by logs and backups. The display includes logs and backup files which might be selected for deletion to recover additional disk space.

Figure 5-7   Manage Logs and Backups



A

Manage Logs & Backups

Logs & Backups partition space allocation: Size: 35G, Used: 40M, Available: 33G, Usage: 1%

Select	Type	Originating Host	File Name	File Size	Creation Time
□	logsCapture	bambi-a	logsCapture_bambi-a...	7.3M bytes	Tue September 16 2003 11:49:07 EDT
□	rtdbBackup	bambi-a	rtdbBackup_bambi-a...	21K bytes	Tue September 16 2003 15:40:28 EDT
□	systemBackup	bambi-a	systemBackup_bambi-a...	96K bytes	Tue September 16 2003 15:38:24 EDT

A

Manage Logs & Backups

Logs & Backups partition space allocation: Size: 35G, Used: 40M, Available: 33G, Usage: 1%

Select	Type	Originating Host	File Name	File Size	Creation Time
□	logsCapture	bambi-a	logsCapture_bambi-a...	7.3M bytes	Tue September 16 2003 11:49:07 EDT
□	rtdbBackup	bambi-a	rtdbBackup_bambi-a...	21K bytes	Tue September 16 2003 15:40:28 EDT
□	systemBackup	bambi-a	systemBackup_bambi-a...	96K bytes	Tue September 16 2003 15:38:24 EDT

Tue September 16 2003 15:40:42 EDT

c. Click the checkbox of each file to be deleted, then click **Delete Selected File(s)**.

4. Call #unique_13 for assistance.

5000000000000002 - Server Application Process Error

This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.

Recovery

1. If a 3000000000000020 - Server Platform Process Error alarm is also present, execute the recovery procedure associated with that alarm before proceeding.
2. Log in to the User Interface screen of the ELAP**GUI** (see Accessing the ELAP GUI Interface)
3. Check the banner information above the menu to verify that you are logged into the problem ELAP indicated in the **UAM**.

   If it is necessary to switch to the other side, select **Select Mate**.
4. Open the Process Control folder, and select the **Stop Software** menu item.
5. Open the Process Control folder, and select the **Start Software** menu item.
6. Capture the log files on both ELAPs (see Saving Logs Using the ELAP **GUI**) and contact #unique_13.

5000000000000004 - Server Hardware Configuration Error

This alarm indicates that one or more of the server's hardware components are not in compliance with proper specifications (refer to *Application B Card Hardware and Installation Guide*.
Recovery

1. Run `syscheck` in verbose mode.
2. Call #unique_13 for assistance.

5000000000000008 - Server RAM Shortage Warning

This alarm indicates one of two conditions:

- Less memory than the expected amount is installed.
- The system is swapping pages in and out of physical memory at a fast rate, indicating a possible degradation in system performance.

This alarm may not clear immediately when conditions fall below the alarm threshold. Conditions must be below the alarm threshold consistently for the alarm to clear. The alarm may take up to five minutes to clear after conditions improve.

Recovery

- Call #unique_13 for assistance.

5000000000000020 - Server Swap Space Shortage Warning

This alarm indicates that the swap space available on the server is less than expected. This is usually caused by a process that has allocated a very large amount of memory over time.

> **Note:**
>
> In order for this alarm to clear, the underlying failure condition must be consistently undetected for a number of polling intervals. Therefore, the alarm may continue to be reported for several minutes after corrective actions are completed.

Recovery

- Call #unique_13 for assistance.

5000000000000040 - Server Default Router Not Defined

This alarm indicates that the default network route is either not configured or the current configuration contains an invalid **IP** address or hostname.

> **Caution:**
>
> When changing the server's network routing configuration it is important to verify that the modifications will not impact the method of connectivity for the current login session. It is also crucial that this information not be entered incorrectly or set to improper values. Incorrectly modifying the server's routing configuration may result in total loss of remote network access.

Recovery

1. Perform the following substeps to define the default router:
   a. Obtain the proper Provisioning Network netmask and the **IP** address of the appropriate Default **Route** on the provisioning network.

      These are maintained by the customer network administrators.
   b. Log in to the **MPS** with username elapconfig (see Accessing the ELAP Text Interface).

      The server designation at this site is displayed as well as **hostname**, **hostid**, **Platform Version**, **Software Version**, and the date. Ensure that the side displayed is the **MPS** that is reporting the problem. In this example, it is **MPS** A. Enter option 2, Configure Network Interfaces Menu, from the ELAP Configuration Menu.

```
MPS Side A:  hostname: mpsa-d1a8f8  hostid: 80d1a8f8
             Platform Version: x.x.x-x.x.x
             Software Version: ELAP x.x.x-x.x.x
             Wed Jul 17 09:51:47 EST 2005
```

```
/-----ELAP Configuration Menu----------\
/----------------------------------------\
|  1 | Display Configuration             |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                     |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys        |
|----|-----------------------------------|
|  5 | Change Password                   |
|----|-----------------------------------|
|  6 | Platform Menu                     |
|----|-----------------------------------|
|  7 | Configure NTP Server              |
|----|-----------------------------------|
|  8 | Mate Disaster Recovery            |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/
Enter Choice:  2
```

c. Enter option `1`, Configure Provisioning Network from the Configure Network Interfaces Menu.

This displays the submenu for configuring communications networks and other information.

```
/-----Configure Network Interfaces Menu-\
/-----------------------------------------\
|  1 | Configure Provisioning Network     |
|----|------------------------------------|
|  2 | Configure DSM Network              |
|----|------------------------------------|
|  3 | Configure Forwarded Ports          |
|----|------------------------------------|
|  4 | Configure Static NAT Addresses     |
|----|------------------------------------|
|  e | Exit                               |
\-----------------------------------------/
Enter choice:  1
```

The following warning appears:
ELAP software is running. Stop it?

d. Type `Y` and press Enter.

If the **LSMS** Connection has not been previously disabled, the following prompt appears:

```
The LSMS Connection is currently enabled. Do you want to disable
it? [Y]  Y
```

e. Type `Y` and press Enter.

   The following confirmation appears:

```
The LSMS Connection has been disabled.
```

   The ELAP A provisioning network IP address displays:

```
Verifying connectivity with mate ...
Enter the ELAP A provisioning network IP Address [192.168.61.90]:
```

f. Press Enter after each address is displayed until the Default **Route** address displays:

```
Verifying connectivity with mate ...
Enter the ELAP A provisioning network IP Address [192.168.61.90]:
Enter the ELAP B provisioning network IP Address [192.168.61.91]:
Enter the ELAP provisioning network netmask [255.255.255.0]:
Enter the ELAP provisioning network default router IP Address:
192.168.61.250
```

g. If the default router **IP** address is incorrect, correct it, and press Enter.

h. After vverifying or correcting the Provisioning Network configuration information, enter `e` to return to the Configure Network Interfaces Menu.

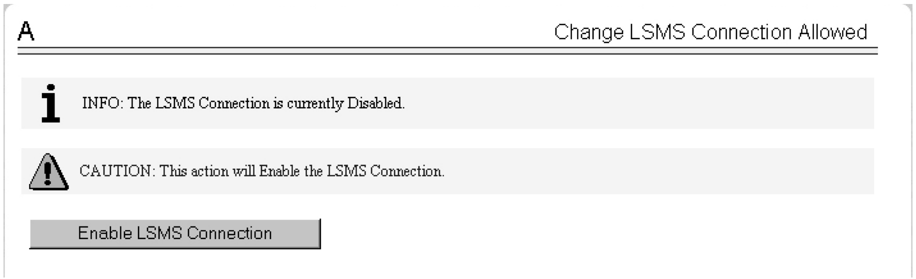
i. Enter `e` again to return to the ELAP Configuration Menu.

2. Rerun `syscheck`.
   - If the alarm has not been cleared, contact #unique_13 for further assistance. Make the `syscheck` output available to them. This procedure is complete.
   - If the alarm has been cleared, the problem is solved, and you can restart the ELAP software and enable the connection to the **LSMS** as described in .
3. Perform the following substeps to restart the ELAP and enable the **LSMS** connection.

   a. Restart the ELAP software (see Restarting the ELAP Software).

   b. Select **Maintenance>LSMS Connection>Change Allowed**: a window similar to the example shown in Figure 5-8 displays.

Figure 5-8 Enable LSMS Connection Window



A

Change LSMS Connection Allowed

INFO: The LSMS Connection is currently Disabled.

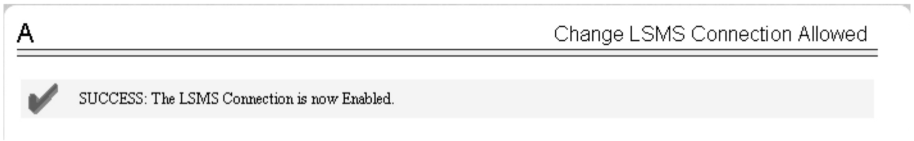
CAUTION: This action will Enable the LSMS Connection.

   c. Click the Enable **LSMS** Connection button.

When the connection has been enabled, the workspace displays the information shown inFigure 5-9.sw

.

Figure 5-9 LSMS Connection Enabled



A Change LSMS Connection Allowed

✓ SUCCESS: The LSMS Connection is now Enabled.

5000000000000080 – Server temperature warning

Alarm Type: TPD

Description: This alarm indicates that the internal temperature within the server is outside of the normal operating range. A server Fan Failure may also exist along with the Server Temperature Warning.

Severity: Minor

OID: tpdTemperatureWarningNotify 1.3.6.1.4.1.323.5.3.18.3.1.3.8

Alarm ID: TKSPLATMI85000000000000080

Recovery

1. Ensure that nothing is blocking the fan's intake. Remove any blockage.
2. Verify that the temperature in the room is normal. If it is too hot, lower the temperature in the room to an acceptable level.

Table 5-4 Server Environmental Conditions

Ambient Temperature	Operating: 5 degrees C to 40 degrees C Exceptional Operating Limit: 0 degrees C to 50 degrees C Storage: -20 degrees C to 60 degrees C
Relative Humidity	Operating: 5% to 85% non-condensing Storage: 5% to 950% non-condensing
Elevation	Operating: -300m to +300m Storage: -300m to +1200m
Heating, Ventilation, and Air Conditioning	Capacity must compensate for up to 5100 BTUs/hr for each installed frame. Calculate HVAC capacity as follows: Determine the wattage of the installed equipment. Use the formula: watts x 3.143 = BTUs/hr

> **Note:**
>
> Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. The alarm may take up to five minutes to clear after conditions improve. It may take about ten minutes after the room returns to an acceptable temperature before syscheck shows the alarm cleared.

3. Verify that the temperature in the room is normal. If it is too hot, lower the temperature in the room to an acceptable level.

   > **Note:**
   >
   > Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. It may take about ten minutes after the room returns to an acceptable temperature before the alarm cleared.

4. Run syscheck to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.
5. Replace the filter (refer to the appropriate hardware manual).

   > **Note:**
   >
   > Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. It may take about ten minutes after the filter is replaced before the alarm cleared.

6. Run syscheck to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, contact #unique_13 and provide the system health check output.

5000000000000100 - Server Core File Detected

This alarm indicates that an application process has failed and debug information is available.

Recovery

1. Run `savelogs` to gather system information (see Running syscheck Through the ELAP GUI”)
2. Contact #unique_13.

   They will examine the files in `/var/TKLC/core` and remove them after all information has been extracted.

5000000000000200 - Server NTP Daemon Not Synchronized

This alarm indicates that the **NTP daemon** (background process) has been unable to locate a server to provide an acceptable time reference for synchronization.

Severity: Minor

Alarm ID: TKSPLATMI10

Recovery

- Contact #unique_13.

5000000000000400 - Server CMOS Battery Voltage Low

The presence of this alarm indicates that the **CMOS** battery voltage has been detected to be below the expected value. This alarm is an early warning indicator of **CMOS** battery end-of-life failure which will cause problems in the event the server is powered off.

Recovery

- Contact #unique_13.

5000000000000800 - Server Disk Self Test Warning

A non-fatal disk issue (such as a sector cannot be read) exists.

Recovery

- Contact #unique_13.

5000000000001000 - Device Warning

This alarm indicates that either a `snmpget` cannot be performed on the configured SNMP OID or the returned value failed the specified comparison operation.

Recovery

1. Run `syscheck` in Verbose mode. (See Running the System Health Check.)
2. Call #unique_13 for assistance.

5000000000002000 - Device Interface Warning

This alarm can be generated by either an SNMP trap or an IP bond error. If `syscheck` is configured to receive SNMP traps, this alarm indicates that a SNMP trap was received with the *set* state. If `syscheck` is configured for IP bond monitoring, this alarm can mean that a slave device is not operating, a primary device is not active, or `syscheck` is unable to read bonding information from interface configuration files.

Recovery

1. Run `syscheck` in Verbose mode. (See Running the System Health Check.)

2. Call #unique_13 for assistance.

5000000000004000 - Server Reboot Watchdog Initiated

This alarm indicates that the server has been rebooted due to a hardware watchdog.

Recovery

- Contact #unique_13.

  This condition should never happen.

5000000000008000 - Server HA Failover Inhibited

This alarm indicates that the server has been inhibited and HA failover is prevented from occurring.

Recovery

- Call #unique_13 for assistance.

5000000000010000 - Server HA Active To Standby Transition

This alarm indicates that the server is in the process of transitioning HA state from Active to Standby.

Recovery

- Call #unique_13 for assistance.

5000000000020000 - Server HA Standby To Active Transition

This alarm indicates that the server is in the process of transitioning HA state from Standby to Active.

Recovery

- Call #unique_13 for assistance.

5000000000040000 - Platform Health Check Failure

This alarm indicates a `syscheck` configuration error.

Recovery

- Call #unique_13 for assistance.

5000000000080000 - NTP Offset Check Failure

This alarm indicates that time on the server is outside the acceptable range or offset from the NTP server. The alarm message provides the offset value of the server from the NTP server and the offset limit set for the system by the application.

Alarm Type: TPD

Severity: Minor

Alarm ID: TKSPLATMI20

Recovery

- Call #unique_13 for assistance.

5000000000100000 - NTP Stratum Check Failure

This alarm indicates that NTP is syncing to a server, but the stratum level of the NTP server is outside the acceptable limit. The alarm message provides the stratum value of the NTP server and the stratum limit set for the system by the application.

Recovery

- Call #unique_13 for assistance.

5000000020000000 – Server Kernel Dump File Detected

Alarm Type: TPD

Description: This alarm indicates that the kernel has crashed and debug information is available.

Severity: Minor

OID: 1.3.6.1.4.1.323.5.3.18.3.1.3.30

Alarm ID: TKSPLATMI305000000020000000

Recovery

1. Run syscheck in Verbose mode (see Running the System Health Check).
2. Contact #unique_13.

5000000040000000 – TPD Upgrade Failed

Alarm Type: TPD

Description: This alarm indicates that a TPD upgrade has failed.

Severity: Minor

OID: tpdServerUpgradeFailDetectedNotify 1.3.6.1.4.1.323.5.3.18.3.1.3.31

Alarm ID: TKSPLATMI315000000040000000

Recovery

1. Run the following command to clear the alarm.

   ```
   /usr/TKLC/plat/bin/alarmMgr —clear TKSPLATMI31
   ```

2. Contact #unique_13.

5000000080000000– Half Open Socket Warning Limit

Alarm Type: TPD

This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.

Severity: Minor

OID: tpdHalfOpenSocketWarningNotify1.3.6.1.4.1.323.5.3.18.3.1.3.32

Alarm ID: TKSPLATMI325000000080000s000

Recovery

1. Run syscheck in verbose mode (see Running the System Health Check).
2. Run `syscheck` (see Running syscheck Using the syscheck Login)
3. Contact #unique_13 and provide the system health check output.

5000000000200000 - SAS Presence Sensor Missing

This alarm indicates that the server drive sensor is not working.
Recovery

- Call #unique_13 for assistance with a replacement server.

5000000000400000 - SAS Drive Missing

This alarm indicates that the number of drives configured for this server is not being detected.

Recovery

- Call #unique_13 to determine if the alarm is caused by a failed drive or failed configuration.

5000000000800000 - DRBD failover busy

This alarm indicates that a DRBD sync is in progress from the peer server to the local server. The local server is not ready to bethe primary DRBD node because its data is not current.

Recovery

1. Wait for approximately 20 minutes, then check if the DRBD sync has completed. A DRBD sync should take no more than 15 minutes to complete.
2. If the alarm persists longer than this time interval, call #unique_13 for assistance.

5000000001000000 - HP disk resync

This alarm indicates that the HP disk subsystem is currently resyncing after a failed or replaced drive, or after another change in the configuration of the HP disk subsystem. The output of the message will include the disk that is resyncing and the percentage complete.

This alarm eventually clears after the resync of the disk is completed. The time to clear is dependant on the size of the disk and the amount of activity on the system..

Recovery

1. Run `syscheck` in Verbose mode.
2. If the percent recovering is not updating, wait at least 5 minutes between subsequent runs of `syscheck`, then call #unique_13 with the `syscheck` output.

5000000400000000 – NTP Source Server is not able to provide correct time

This alarm indicates that an NTP server was not able to provide a good time.

Severity: Minor

Alarm ID: TKSPLATMI35

Recovery

Contact #unique_13.

Minor Application Alarms

Minor application alarms involve **RTDB** capacity and software errors.

4000000000020000 - Automatic RTDB Backup is not configured

This is an indication that the Automatic RTDB Backup is not configured on the system, i.e., the Backup Type is "None."

Recovery

- Configure the Automatic RTDB backup with backup type other than None. Refer to Automatic RTDB Backup for details on how to configure the Automatic RTDB Backup.

6000000000000010 - Minor Software Error

A minor software error has been detected.

Recovery

1. Run `syscheck`.
2. Contact #unique_13.

   Have the system health check data available.

6000000000000200 - RTDB Backup Failed

This alarm indicates that the system was unable to complete an RTDB backup.

Recovery

- Call #unique_13 for assistance.

6000000000000400 - Automatic RTDB Backup Failed

This alarm indicates that the system was unable to complete an automatic RTDB backup.

Recovery

- Call #unique_13 for assistance.

6000000000000800 - Automatic Backup cron entry modified

This alarm indicates that the `cron` entry for automatic backups has been modified. No further action is required.

6000000000002000 - Configurable Quantity Threshold Exceeded

This alarm indicates that the RTDB file system has reached the user-configured threshold.

Recovery

1. If the user-configurable threshold is set to less than 90%, then the user may increase the threshold to a higher value.
    a. Log in to the User Interface of the ELAP GUI. See Accessing the ELAP GUI Interface.
    b. Select **User Administration**, and then **Modify Defaults** to change the threshold value (1-99). See *ELAP Administration and LNP Feature Activation* for additional information.
2. If the user-configurable threshold is set to 90% or higher, call #unique_13 for assistance.

6000000000020000 - Automatic RTDB Backup is not configured

This is an indication that the Automatic RTDB Backup is not configured on the system, i.e., the Backup Type is "None."

Recovery

- Configure the Automatic RTDB backup with backup type other than None. Refer to Automatic RTDB Backup for details on how to configure the Automatic RTDB Backup.

6

Field Replaceable Units

This chapter describes the components of an E5-APP-B card that can be replaced in the field and includes procedures for replacing each type of field replaceable unit (**FRU**).

Introduction

Oracle Communication EAGLE Application B Cards (E5-APP-B) are complete application server platforms and are designed for the high-availability environments required by telephony networks. They are installed in an EAGLE shelf.

Even with the advanced reliability of the E5-APP-B design, hardware failures may still occur. The E5-APP-B card is designed for easy maintenance when replacements are needed.

This chapter highlights the E5-APP-B card components that are field replaceable units (**FRU**) and provides procedures for replacing them.

This chapter explains how to remove a card from the EAGLE. The procedures include the administrative commands required to take a card out of service and place it back into service.

In the event a numbered event message is encountered, refer to the appropriate procedure in the *Unsolicited Alarm and Information Messages Reference*.

Additional information about each command can be found in the EAGLE *Commands User's Guide*.

Safety Information

Safety icons and text are used throughout this manual to warn the reader of the potential of personal injury, service interruption, and equipment damage. For information about what each of the icons mean, see Documentation Admonishments.

Before beginning any procedure described in this manual, make sure that you are familiar with each of the following safety admonishments. Additional safety admonishments may be included, or repeated, for specific procedures.

> ⚠ **Caution:**
>
> All personnel associated with the installation of these systems must adhere to all safety precautions and use required protection equipment, to avoid the possibility of injury to personnel, service degradation, and/or service interruption.

> ⚠ **Caution:**
>
> Always wear a wrist strap or other electrostatic protection when handling an E5-APP-B card.

Caution:

Always place removed cards into an electrostatic protection bag before sending to Oracle or storing in inventory (unless the card is being stored in the optional spare card storage shelf).

E5-APP-B Card FRUs and Part Numbers

The following **E5-APP-B** card components can be replaced in the field:

- **E5-APP-B** cards (P/N 870-3096-01 and P/N 870-3096-02)
- Drive modules (P/N 870-3097-01 and P/N 870-3097-02)

Removing and Replacing E5-APP-B Cards

This section gives procedures on removing and replacing the E5-APP-B card and drive modules.

Removing an E5-APP-B Card

Procedure - Remove E5-APP-B card

Note:

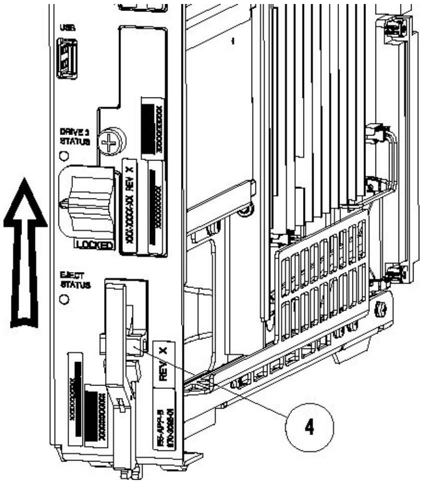
The `shutdown`, `init 6` or `halt` commands will not shut down the E5-APP-B card.

1. On the E5-APP-B card, slide the Ejector switch (4) up to the UNLOCKED position (see Figure 6-1).

   Caution:

   When the Ejector switch goes from locked to unlocked and the E5-APP-B card is in service, the card will halt.

Figure 6-1 E5-APP-B Card Eject Hardware Switch, UNLOCKED



2. WAIT for the E5-APP-B Eject Status LED to go from blinking red to a steady red.

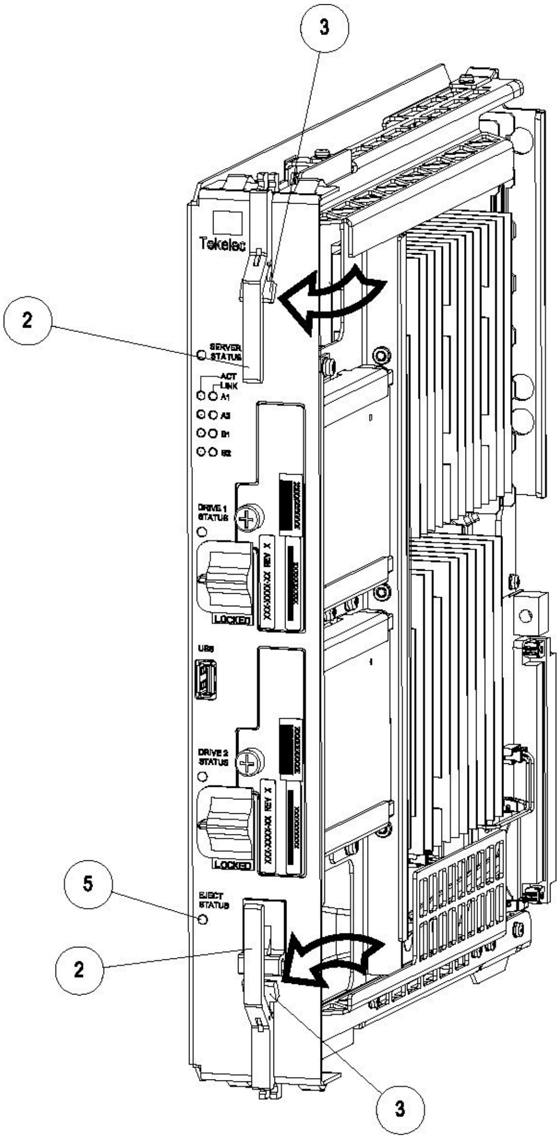
   When the Eject Status LED is steady red, the E5-APP-B card is in shutdown state.

   If the Ejector switch is put into the LOCKED position now, the E5-APP-B card will reboot.

3. Grasp the upper and lower card Inject/Eject (I/E) lever release (3) just underneath the I/E lever, and press it to meet the I/E lever. This is the mechanical interlock for the card.

   See Figure 6-2

Figure 6-2   E5-APP-B Card UNLOCKED



4. While holding the I/E interlock and lever, pull the levers (2) away from the shelf until they are parallel to the floor.
5. Remove the E5-APP-B card from the EAGLE shelf.

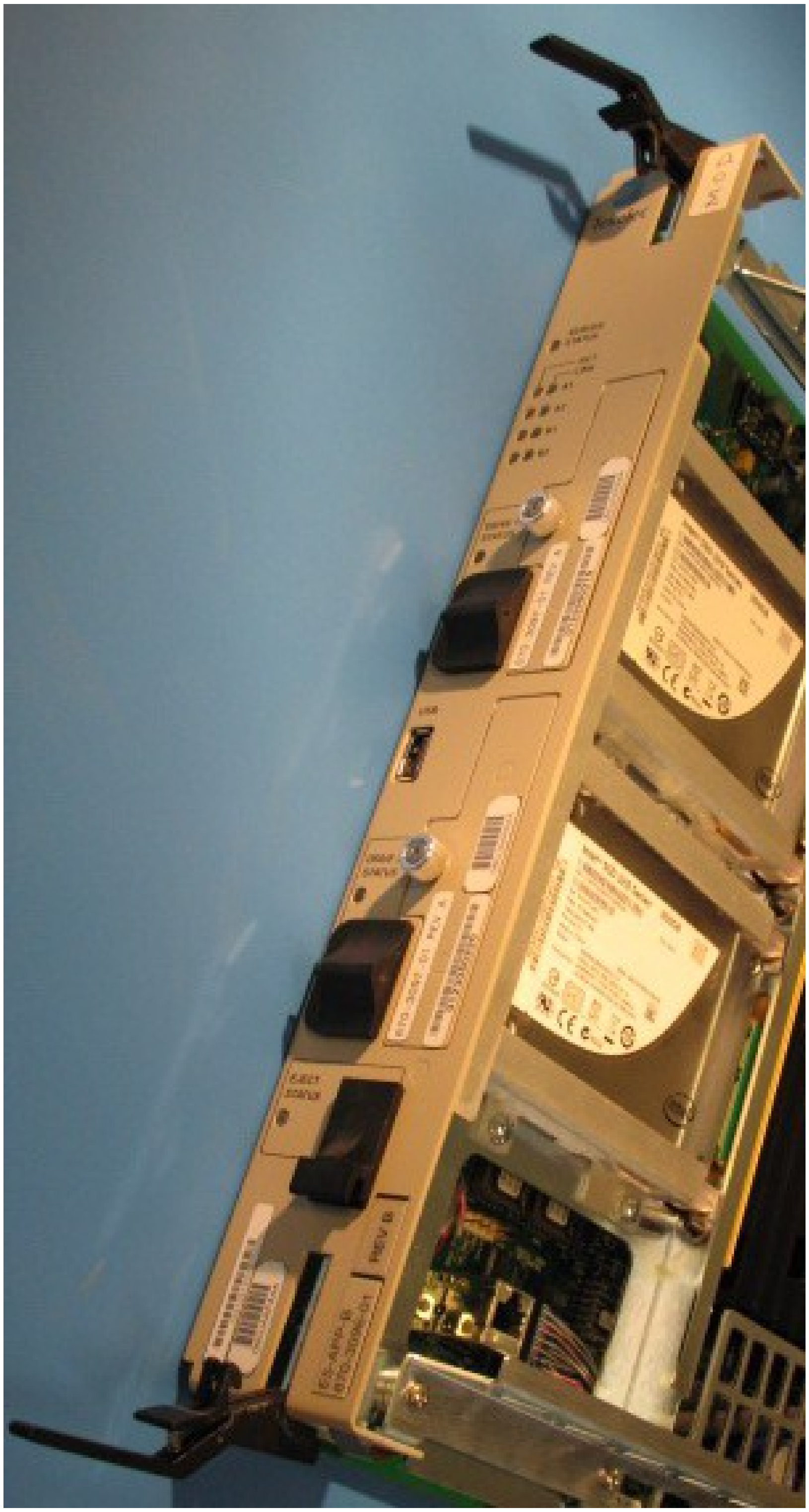
Replacing an E5-APP-B Card

Procedure - Replace E5-APP-B card

1. While holding the I/E interlock and lever, pull the levers (2) away from the card until they are parallel to the floor.

   Figure 6-3 illustrates the angle of the interlocks and levers just before inserting E5-APP-B Card into the EAGLE shelf.

Figure 6-3 E5-APP-B Card UNLOCKED

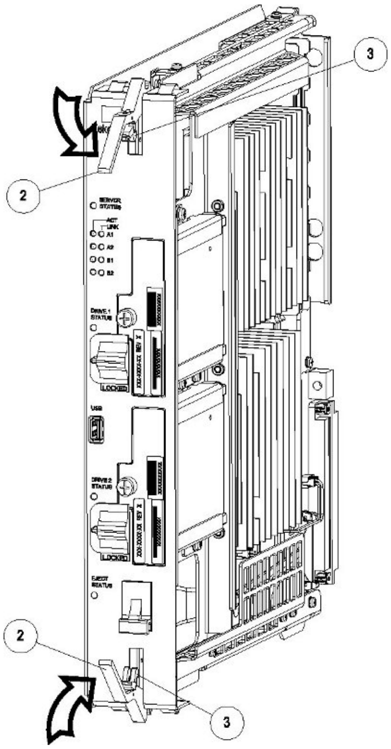


2. Insert the E5-APP-B card into the EAGLE shelf.

   Carefully align the edges of the card with the top and bottom card guides. Then, push the card along the length of the card guides until the rear connectors on the card engage the mating connectors on the target shelf backplane.

3. Push in the top and bottom inject/eject clamps (see Figure 6-4).

Figure 6-4   E5-APP-B Card Inject Levers

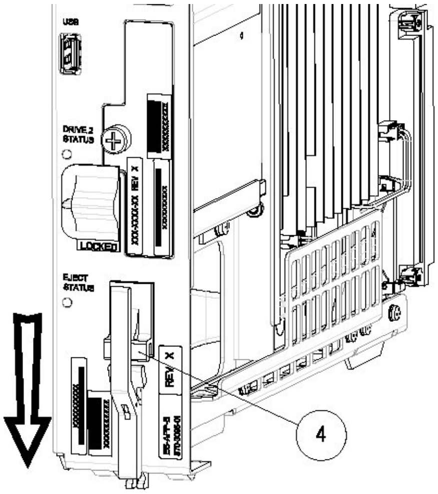


This locks the card in place and ensures a strong connection with the pins on the target shelf backplane.

4. Slide the E5-APP-B Ejector switch (4) down to the LOCKED position (see Figure 6-5).

> **Note:**
>
> When the Ejector switch goes from UNLOCKED to LOCKED, the E5-APP-B Eject Status LED blinks red as the E5-MASP card goes online.

Figure 6-5   E5-APP-B Card Inject Hardware Switch, LOCKED



5. WAIT for the E5-APP-B Eject Status LED to go from blinking red to off.

Removing and Replacing a Drive Module Assembly

E5-APP-B cards are designed for high-availability environments, but even with the advanced reliability of the E5-APP-B card, hardware failures can occur. The E5-APP-B card is designed for easy maintenance when drive module replacement is needed. Since there are two drive modules configured with RAID in an E5-APP-B card, if one becomes corrupt the other drive continues to function. No down time is required to replace a drive module as this procedure can be used on a setup that is up and running.
Oracle now provides 480G drive modules that allow for a larger data capacity. When upgrading from 300G to 480G drive modules, both drive modules should be replaced one after the other.

Procedure - Remove and Replace a Drive Module Assembly

1. Use the `smartd` command to verify the drive module names.

   ```
   $ ls /var/TKLC/log/smartd
   lock log.sda log.sdb sda sdb
   ```

   In this example, the drive module names are sda and sdb.

2. Use the `mdstat` command to determine whether a drive module is corrupt:

   ```
    $ sudo cat /proc/mdstat
   ```

   - On a healthy system where both drive modules (sda and sdb) are functioning properly, the `mdstat` output will include both drive modules:

     ```
      $ sudo cat /proc/mdstat
     Personalities : [raid1]
     md2 : active raid1 sda2[0] sdb2[1]
           26198016 blocks super 1.1 [2/2] [UU]
           bitmap: 1/1 pages [4KB], 65536KB chunk
     ```

```
md1 : active raid1 sda3[0] sdb3[1]
      262080 blocks super 1.0 [2/2] [UU]

md3 : active raid1 sdb1[1] sda1[0]
      442224640 blocks super 1.1 [2/2] [UU]
      bitmap: 1/4 pages [4KB], 65536KB chunk

unused devices: <none>
```

- On a system where one of the drive modules is healthy and one is corrupt, only the healthy drive module is displayed:

  ```
   $ sudo cat /proc/mdstat
  Personalities : [raid1]
  md2 : active raid1 sdb2[1]
        26198016 blocks super 1.1 [2/1] [_U]
        bitmap: 1/1 pages [4KB], 65536KB chunk

  md1 : active raid1 sdb3[1]
        262080 blocks super 1.0 [2/1] [_U]

  md3 : active raid1 sdb1[1]
        442224640 blocks super 1.1 [2/1] [_U]
        bitmap: 3/4 pages [12KB], 65536KB chunk

  unused devices: <none>
  ```

  In this example, the `mdstat` output shows only sdb, which indicates that sda is corrupt.

3. Log in as admusr and run the `failDisk` command to mark the appropriate drive module to be replaced.

   If you are replacing a healthy drive module with a higher capacity drive module, the `force` option is required. The `force` option is not required when replacing a corrupt drive module.

   - Replacing a corrupt drive module:

     ```
     $ sudo /usr/TKLC/plat/sbin/failDisk <disk to be removed>
     ```

     For example:

     ```
     $ sudo /usr/TKLC/plat/sbin/failDisk /dev/sda
     ```

   - Replacing a healthy drive module with a higher capacity drive module:

     ```
     $ sudo /usr/TKLC/plat/sbin/failDisk --force <disk to be removed>
     ```

     For example:

     ```
     $ sudo /usr/TKLC/plat/sbin/failDisk --force /dev/sda
     ```

4. After `failDisk` runs successfully, remove the drive module assembly.

See Removing a Drive Module Assembly.

5. Insert the new drive module assembly.

   See Replacing a Drive Module Assembly.

6. If you are replacing a 300G drive module with a 480G drive module, repeat these steps to replace the other 300G drive module with a 480G drive module.

Removing a Drive Module Assembly

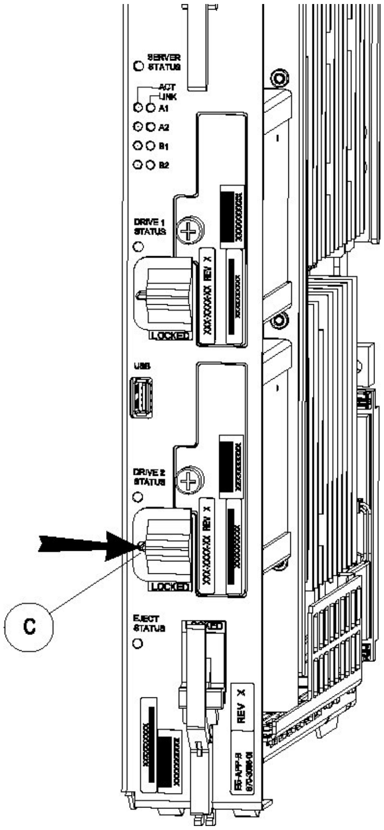
Procedure - Remove Drive Module Assembly

1. Verify that the drive module is locked in position and in use.

   The switch lock release (C) is in the LOCKED position and the Status LED on the E5-APP-B card is OFF.

   Move the switch lock release (C) to the "released" position by pressing in the direction indicated. Refer to Figure 6-6.

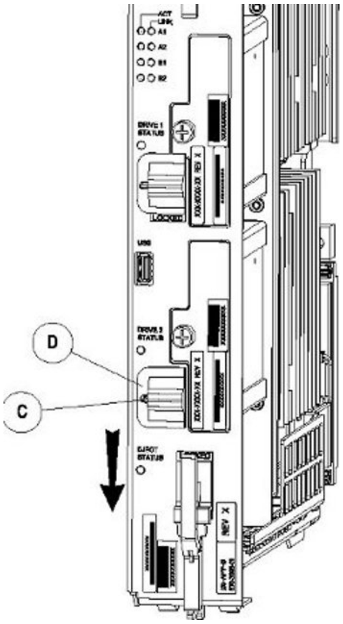
Figure 6-6 Drive Module Released



2. Move drive module locking switch (D) from the LOCKED to the unlocked position and wait for the LED (B) to indicate a steady red state. See Figure 6-7 and Figure 6-8, respectively.

   When drive module locking switch (D) is transitioned from locked to unlocked, the LED will flash red to indicate the drive is unlocked and in process of shutting down.

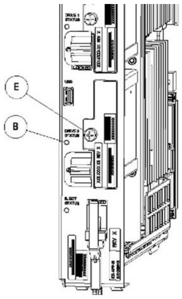
Figure 6-7   Drive Module UNLOCKED



Caution:

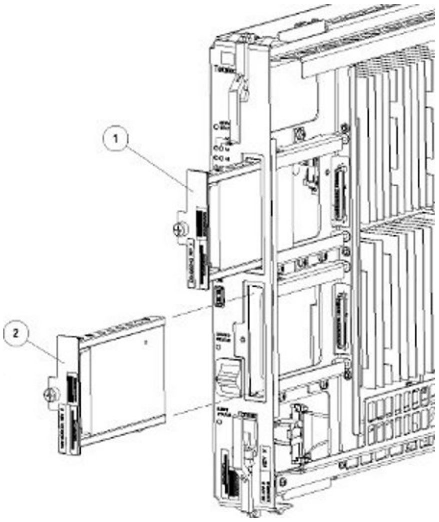
Removal of the drive prior to the LED indicating steady red could result in drive corruption.

Figure 6-8   Drive Module Status



3. When the LED indicates a steady red, the drive module can be safely removed.
4. Loosen the drive module screw (E) (see Figure 6-8).
5. Grasp the screw (E) and pull the drive out slowly until it is free from the card (see Figure 6-9).

Figure 6-9   Drive Module Removal

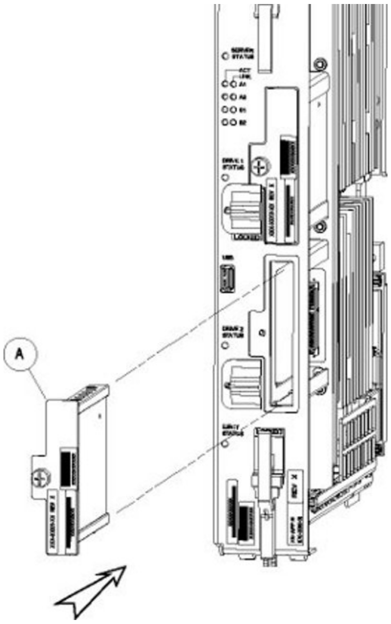


Replacing a Drive Module Assembly

Procedure - Replace Drive Module Assembly

1. Slide a new drive(s) module into the drive slot on the card (see Figure 6-10).

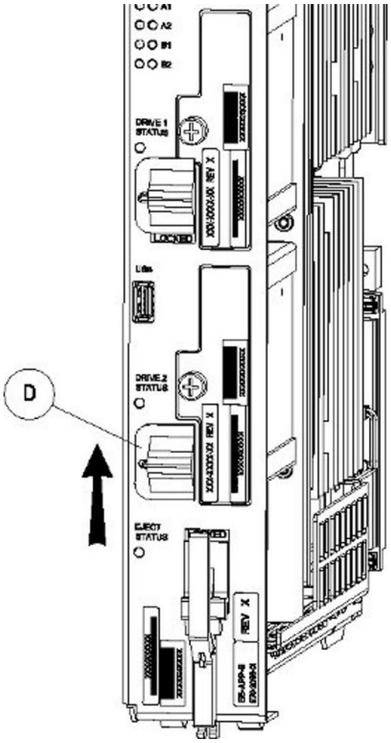
Figure 6-10   Drive Module Replacement



2. Gently push the drive (A) in slowly until it is properly seated.
3. Tighten the mounting screw until the Drive Status LED is in a steady red state ((B), from Figure 6-8).
4. Move the drive module locking switch (D) from the unlocked to the LOCKED position.

When drive module locking switch (D) is transitioned from unlocked to locked, the LED will flash red to indicate the drive is locked and in process of coming online (see Figure 6-11).

Figure 6-11 Drive Module Locked



5. When the LED turns off, log in as admusrroot and run the `cpDiskCfg` command to copy the partition table from the good drive module to the new drive module.

```
$ sudo /usr/TKLC/plat/sbin/cpDiskCfg <source disk> <destination
disk>
```

```
# /usr/TKLC/plat/sbin/cpDiskCfg <source disk> <destination disk>
```

   For example:

```
$ sudo /usr/TKLC/plat/sbin/cpDiskCfg /dev/sdb /dev/sda
```

```
# /usr/TKLC/plat/sbin/cpDiskCfg /dev/sdb /dev/sda
```

6. After successfully copying the partition table, use the `mdRepair` command to replicate the data from the good drive module to the new drive module.

```
$ sudo /usr/TKLC/plat/sbin/mdRepair
```

```
# /usr/TKLC/plat/sbin/mdRepair
```

This step takes 45 to 90 minutes and runs in the background without impacting functionality.

Sample output of the command:

```
[admusr@recife-b ~]$ sudo /usr/TKLC/plat/sbin/mdRepair
SCSI device 'sdb' is not currently online
probing for 'sdb' on SCSI 1:0:0:0
giving SCSI subsystem some time to discover newly-found disks
Adding device /dev/sdb1 to md group md1...
md resync in progress, sleeping 30 seconds...
md1 is 0.0% percent done...

This script MUST be allowed to run to completion.  Do not exit.


bgRe-installing master boot loader(s)

Adding device /dev/sdb2 to md group md3...
Adding device /dev/sdb9 to md group md5...
Adding device /dev/sdb7 to md group md4...
Adding device /dev/sdb6 to md group md7...
Adding device /dev/sdb8 to md group md6...
Adding device /dev/sdb3 to md group md2...
Adding device /dev/sdb5 to md group md8...
md resync in progress, sleeping 30 seconds...
md3 is 3.6% percent done...

This script MUST be allowed to run to completion.  Do not exit.


md resync in progress, sleeping 30 seconds...
md5 is 27.8% percent done...

This script MUST be allowed to run to completion.  Do not exit.

md resync in progress, sleeping 30 seconds...
md4 is 8.9% percent done...

This script MUST be allowed to run to completion.  Do not exit.

md resync in progress, sleeping 30 seconds...
md4 is 62.5% percent done...

This script MUST be allowed to run to completion.  Do not exit.

md resync in progress, sleeping 30 seconds...
md7 is 14.7% percent done...

This script MUST be allowed to run to completion.  Do not exit.

md resync in progress, sleeping 30 seconds...
md7 is 68.3% percent done...

This script MUST be allowed to run to completion.  Do not exit.
```

```
md resync in progress, sleeping 30 seconds...
md8 is 0.3% percent done...

This script MUST be allowed to run to completion.  Do not exit.

md resync in progress, sleeping 30 seconds...
md8 is 1.1% percent done...

This script MUST be allowed to run to completion.  Do not exit.

md resync in progress, sleeping 30 seconds...
md8 is 2.0% percent done...
```

7. Use the `cat /proc/mdstat` command to confirm whether RAID repairs are successful.

   After the RAID is repaired successfully, output showing both drive modules is displayed:

```
Personalities : [raid1]
md1 : active raid1 sdb2[1] sda2[0]
      262080 blocks super 1.0 [2/2] [UU]

md2 : active raid1 sda1[0] sdb1[1]
      468447232 blocks super 1.1 [2/2] [UU]
      bitmap: 1/4 pages [4KB], 65536KB chunk

unused devices: <none>


Personalities : [raid1]
md2 : active raid1 sda2[0] sdb2[1]
      26198016 blocks super 1.1 [2/2] [UU]
      bitmap: 1/1 pages [4KB], 65536KB chunk

md1 : active raid1 sda3[0] sdb3[1]
      262080 blocks super 1.0 [2/2] [UU]

md3 : active raid1 sdb1[1] sda1[0]
      442224640 blocks super 1.1 [2/2] [UU]
      bitmap: 1/4 pages [4KB], 65536KB chunk

unused devices: <none>
```

   Output of `cat /proc/mdstat` prior to re-mirroring:

```
[admusr@recife-b ~]$ sudo cat /proc/mdstat
Personalities : [raid1]
md1 : active raid1 sda1[0]
      264960 blocks [2/1] [U_]

md3 : active raid1 sda2[0]
      2048192 blocks [2/1] [U_]
```

```
md8 : active raid1 sda5[0]
      270389888 blocks [2/1] [U_]

md7 : active raid1 sda6[0]
      4192832 blocks [2/1] [U_]

md4 : active raid1 sda7[0]
      4192832 blocks [2/1] [U_]

md6 : active raid1 sda8[0]
      1052160 blocks [2/1] [U_]

md5 : active raid1 sda9[0]
      1052160 blocks [2/1] [U_]

md2 : active raid1 sda3[0]
      1052160 blocks [2/1] [U_]

unused devices: <none>
```

Output of `cat /proc/mdstat` during re-mirroring process:

```
[admusr@recife-b ~]$ sudo cat /proc/mdstat
Personalities : [raid1]
md1 : active raid1 sdb1[1] sda1[0]
      264960 blocks [2/2] [UU]

md3 : active raid1 sdb2[1] sda2[0]
      2048192 blocks [2/2] [UU]

md8 : active raid1 sdb5[2] sda5[0]
      270389888 blocks [2/1] [U_]
      [=====>...............]  recovery = 26.9% (72955264/270389888)
finish=43.8min speed=75000K/sec

md7 : active raid1 sdb6[1] sda6[0]
      4192832 blocks [2/2] [UU]

md4 : active raid1 sdb7[1] sda7[0]
      4192832 blocks [2/2] [UU]

md6 : active raid1 sdb8[1] sda8[0]
      1052160 blocks [2/2] [UU]

md5 : active raid1 sdb9[1] sda9[0]
      1052160 blocks [2/2] [UU]

md2 : active raid1 sdb3[2] sda3[0]
      1052160 blocks [2/1] [U_]
      resync=DELAYED
```

Output of `cat /proc/mdstat` upon successful completion of re-mirror:

```
[admusr@recife-b ~]$ sudo cat /proc/mdstat
Personalities : [raid1]
md1 : active raid1 sdb1[1] sda1[0]
      264960 blocks [2/2] [UU]

md3 : active raid1 sdb2[1] sda2[0]
      2048192 blocks [2/2] [UU]

md8 : active raid1 sdb5[1] sda5[0]
      270389888 blocks [2/2] [UU]

md7 : active raid1 sdb6[1] sda6[0]
      4192832 blocks [2/2] [UU]

md4 : active raid1 sdb7[1] sda7[0]
      4192832 blocks [2/2] [UU]

md6 : active raid1 sdb8[1] sda8[0]
      1052160 blocks [2/2] [UU]

md5 : active raid1 sdb9[1] sda9[0]
      1052160 blocks [2/2] [UU]

md2 : active raid1 sdb3[1] sda3[0]
      1052160 blocks [2/2] [UU]

unused devices: <none>
```

A
General Procedures

This chapter includes general procedures for the E5-APP-B.

Introduction

This chapter contains miscellaneous general procedures that are referred to within this manual.

Accessing the ELAP GUI Interface

ELAP employs a web-based user interface. It uses the typical client-server paradigm. The front end appears on an Internet browser. The back end operates on the platform. The front end is officially supported on Microsoft® Internet Explorer, versions 8.0 or 9.0, and on Mozilla® Firefox®, version 3.0.0 or later.:

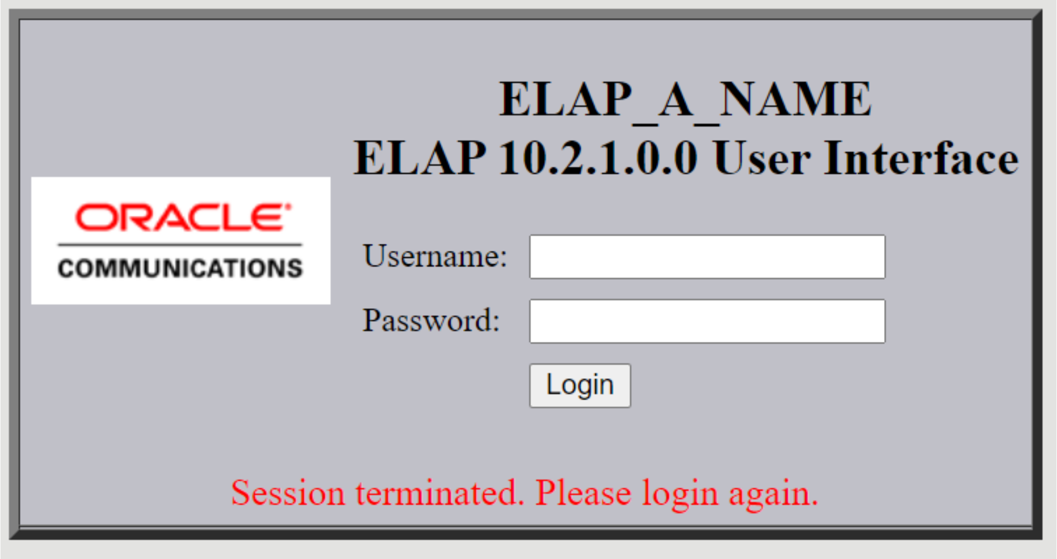
```
CAUTION: The User Interface may not function correctly with the browser you
are using.
Microsoft® Internet Explorer, versions 8.0 and 9.0, have been certified for
this application
```

Use the following procedure to access the main screen of the ELAP GUI interface.

1. Using the selected browser (Microsoft® Internet Explorer 8.0 or 9.0, or Mozilla® Firefox® 3.0.0 or later), type the **IP** address for your ELAP application into the URL field.

   The login screen shown in #unique_30/unique_30_Connect_42_V5405805 appears.

Figure A-1 ELAP User Interface Screen



ELAP_A_NAME
ELAP 10.2.1.0.0 User Interface

Username:

Password:

Session terminated. Please login again.

If using Firefox®, the following message will be displayed when logging into the ELAP GUI:

```
CAUTION: The User Interface may not function correctly with the
browser you are using.
Microsoft® Internet Explorer, versions 8.0 and 9.0, have been
certified for this application
```

> **Note:**
>
> #unique_30/unique_30_Connect_42_V5405805 does not show the release number that appears on the ELAP User Interface Login window because this manual covers multiple ELAP releases.

2. Enter the appropriate username and password.

   Specify a username that has permission to access the menu items indicated in the procedure to be performed. Table A-1 shows the default usernames. Additional usernames can be defined by selecting the User Administration menu item. For more information about assigning usernames, refer to *ELAP Administration and LNP Feature Activation*.

   Table A-1 Usernames

ELAP UI Login Name	Access Granted
epapmaintelapmaint	Maintenance menu and all sub menus
epapdebugelapdebug	Debug menu and all sub menus
epapplatformelapplatform	Platform menu and all sub menus
uiadmin	User Administration menu
epapallelapall	All of the menus in this Table

3. Continue with the procedure that invoked this procedure.

Connecting to the Server Command Line

You can connect to the ELAP server command line for the following purposes:

- Accessing the ELAP text interface (see Accessing the ELAP Text Interface)
- Running `syscheck` (see Running the System Health Check)

It is possible to connect to the ELAP server command line in any of the following ways:

- Use a secure shell (`ssh`) utility to connect to either server's **IP** address. This connection will be made through the port that is identified as **eth01** on the ELAP E5-APP-B Interconnect and is identified as **eth91** by the software. For more information, see Using ssh to Connect to the Server Command Line.
- Use a secure shell (ssh) utility to accessible ELAP server. Use command `minicom mate` to log on to the mate ELAP server's command line.
- If access to the MPS server is not available through an IP network, connect to the E5-APP-B card via the serial port:

For connecting the E5-APP-B A card, disconnect the console cable from the serial port on the E5-APP-B card's adapter. The cable should be disconnected at the point where it connects to the serial port labeled 'S1' on the E5-APP-B card's adapter and use it for serial access. Cable part numbers - 830-1220-xx.

- Connect a cable, Part Number 830-0058-xx (xx represents the cable length), to serial port ttyS0 on either the A or B server (see Connecting a Local Access Terminal to Server’s Serial Port).

Using ssh to Connect to the Server Command Line

You can log into either ELAP server from any terminal using a `ssh` (**Secure Shell**) utility.

> **Note:**
>
> If your terminal does not already have `ssh` installed, PuTTY is a free `ssh` utility for Windows that you can download from the web.

Use the following procedure to `ssh` to the server command line.

- From a command-line prompt on your terminal, enter the following command to start a secure shell session with an ELAP server: `ssh <username>@<server_IP_address>`

  where `<server_IP_address>` is the **IP** address of the server and `<username>` is either of the following:

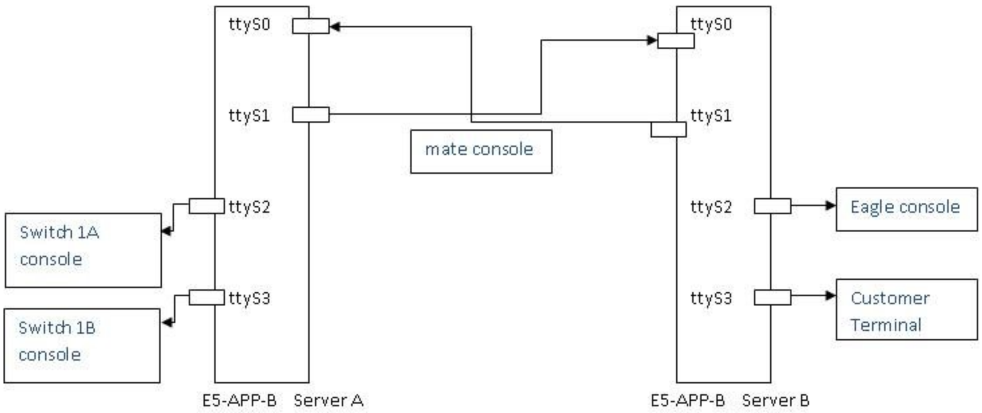
  - ELAPconfig—for accessing the ELAP text interface, enter the ELAPconfig username and the password provided by your system administrator. For more information about the ELAP text interface, see Accessing the ELAP Text Interface.
  - syscheck—for runing the `syscheck` utility, enter syscheck as the username and syscheck as the password. For more information about running syscheck from this interface, see Running syscheck Using the syscheck Login.

Connecting a Local Access Terminal to Server’s Serial Port

Port ttyS0 is the port used on both ELAP A and B servers to connect to the console.

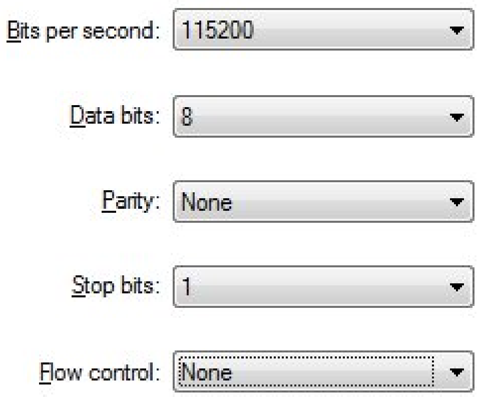
1. Connect the workstation you will use as the Local Access Terminal to Serial port ttyS0 on the server (see Figure A-2).

Figure A-2   E5-APP-B on ELAP Console Connectivity



2. Reconnect the original cables as shown in Figure A-2.
3. If using a laptop, the refer to Figure A-3 for the correct settings needed for the local console connection to the ttyS0 port:

Figure A-3   Laptop Connection Settings



Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

4. When the prompt appears on the Local Access Terminal, enter either of the following usernames and associated passwords:
   - To access the ELAP text interface, enter the ELAPconfig username and the password provided by your system administrator. For more information about the ELAP text interface, see Accessing the ELAP Text Interface.
   - To run the `syscheck` utility, enter syscheck as the username and syscheck as the password. For more information about running syscheck from this interface, see Running syscheck Using the syscheck Login

   Once a server has been installed with ELAP application and cabling has been completed, the subsequent upgrades can be done via serial connectivity from the mate ELAP server.

Accessing the ELAP Text Interface

The ELAP text-based user interface is accessed through the Local Access Terminal. The text-based user interface is used for initial configuration of the ELAP application.

Some errors described in this manual result from errors in the initial configuration, and recovery from them requires that you access the text interface.

For information about the initial configuration of the ELAP application, refer to *ELAP Administration and LNP Feature Activation*.

1. Connect the Local Access Terminal to the server you need to access (see Connecting a Local Access Terminal to Server's Serial Port).
2. Log in with username elapconfig and the password provided by your system administrator.
3. Continue with the procedure that invoked this procedure.

Saving Logs Using the ELAP **GUI**

During some corrective procedures, it may be necessary to provide Oracle with information about the ELAP for help in clearing an alarm. These log files are used to aid #unique_13 when troubleshooting the ELAP.

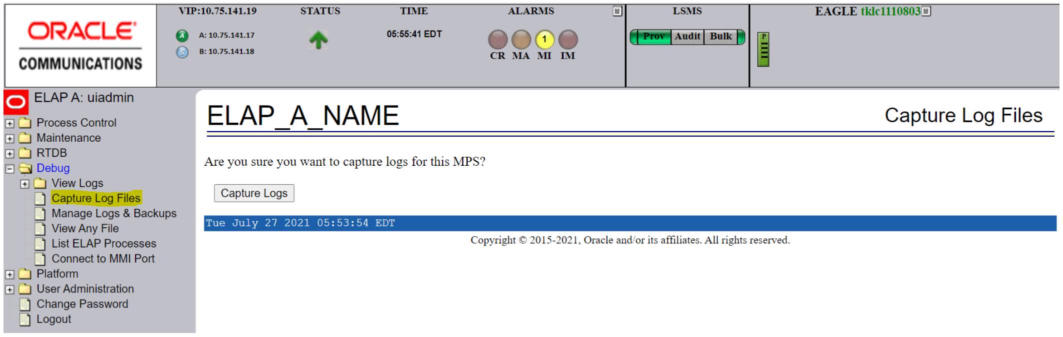
Use the following procedure to save logs using menu selections from the ELAP GUI.

1. Log in to the User Interface screen of the ELAP GUI (see Accessing the ELAP GUI Interface).
2. Check the banner information above the menu to verify that you are logged into the problem ELAP indicated in the **UAM**.

   If it is necessary to switch to the problem ELAP, click the **Select Mate** menu item.
3. From the menu, select **Debug> Capture Log Files.**
4. Deselect (if necessary) the box labeled `Check if you want to capture core files with the Logs`, as shown in #unique_134/unique_134_Connect_42_V886821.

> **Note:**
>
> Contact #unique_13 for assistance before capturing core files with the log files.

Figure A-4   Capture Logs File Screen



Are you sure you want to capture logs for this MPS?

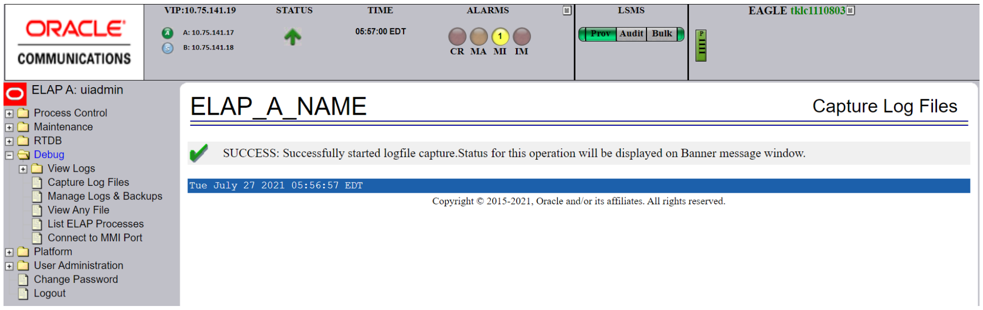
```
Tue July 27 2021 05:53:54 EDT
```

Copyright © 2015-2021, Oracle and/or its affiliates. All rights reserved.

5. Click the **Capture Logs** button to capture the log files.

   After completion, verify the following response:

Figure A-5 Capture Logs Success



ELAP_A_NAME — Capture Log Files

SUCCESS: Successfully started logfile capture.Status for this operation will be displayed on Banner message window.

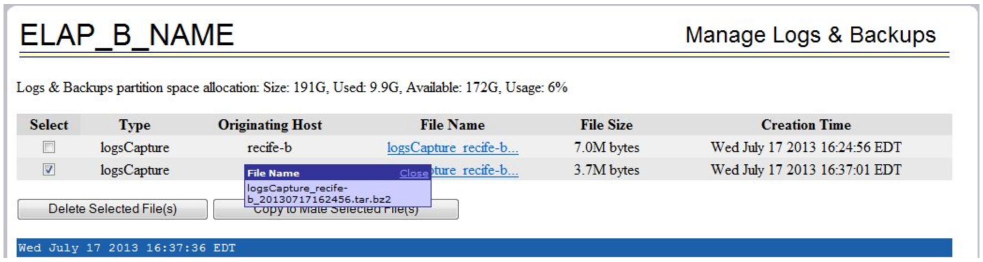
```
Tue July 27 2021 05:56:57 EDT
```

Copyright © 2015-2021, Oracle and/or its affiliates. All rights reserved.

6. Contact #unique_13 to analyze and check the log files.
7. When #unique_13 has finished analyzing the logs files, delete them from the server by selecting **Debug>Manage Logs Files and Backups** to open the **Manage Logs and Backups** Screen.
8. Click the checkboxes for the files you want to delete and then click the **Delete Selected File(s)** button.

   An example is shown in .

Figure A-6 Deleting Captured Log Files



ELAP_B_NAME — Manage Logs & Backups

Logs & Backups partition space allocation: Size: 191G, Used: 9.9G, Available: 172G, Usage: 6%

Select	Type	Originating Host	File Name	File Size	Creation Time
□	logsCapture	recife-b	logsCapture_recife-b...	7.0M bytes	Wed July 17 2013 16:24:56 EDT
☑	logsCapture		...ture_recife-b...	3.7M bytes	Wed July 17 2013 16:37:01 EDT

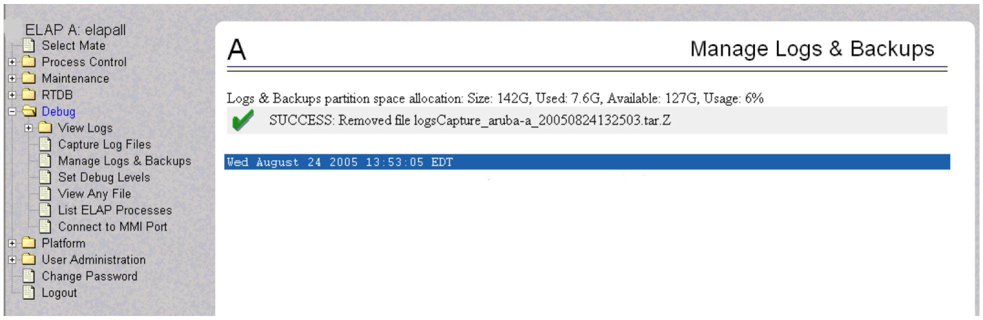
File Name — Close
logsCapture_recife-b_20130717162456.tar.bz2

```
Wed July 17 2013 16:37:36 EDT
```

.

When the log files have been deleted, the GUI displays confirmation, as shown in .

Figure A-7 Delete Log Files Success



A — Manage Logs & Backups

Logs & Backups partition space allocation: Size: 142G, Used: 7.6G, Available: 127G, Usage: 6%

SUCCESS: Removed file logsCapture_aruba-a_20050824132503.tar.Z

```
Wed August 24 2005 13:53:05 EDT
```

Restarting the ELAP Software

This procedure is used when referenced by one of the procedures in Platform and Application Alarms.

> **Caution:**
>
> Perform this procedure only when directed to by one of the procedures in Platform and Application Alarms. This is not a standalone procedure.

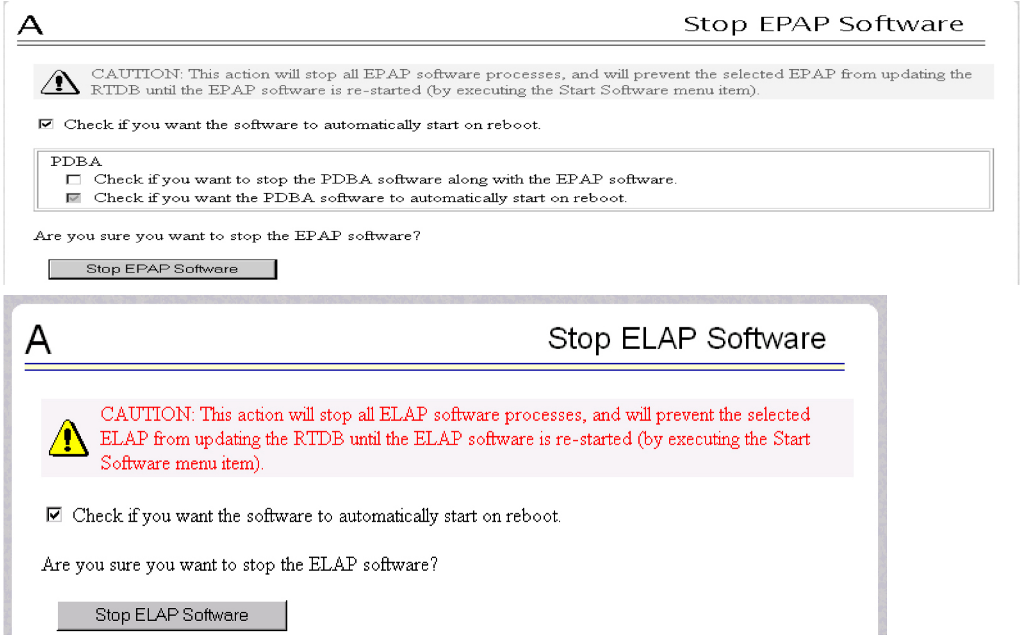
The **PDBA** items that appear in the screens in this procedure apply only to the **EPAP** application. These items will not appear for the **ELAP** application.

1. Log in to the User Interface screen of the ELAP**GUI** (see Accessing the ELAP GUI Interface).
2. Check the banner information above the menu to verify that you are logged into the problem ELAP indicated in the **UAM**.

   If it is necessary to switch to the problem ELAP, select **Select Mate**.
3. From the **elapmaint** screen, select **Process Control>Stop Software**.

   The screen shown in Figure A-8 appears:

Figure A-8 Stop Software Confirmation



CAUTION: This action will stop all EPAP software processes, and will prevent the selected EPAP from updating the RTDB until the EPAP software is re-started (by executing the Start Software menu item).

☑ Check if you want the software to automatically start on reboot.

PDBA
☐ Check if you want to stop the PDBA software along with the EPAP software.
☑ Check if you want the PDBA software to automatically start on reboot.

Are you sure you want to stop the EPAP software?

CAUTION: This action will stop all ELAP software processes, and will prevent the selected ELAP from updating the RTDB until the ELAP software is re-started (by executing the Start Software menu item).

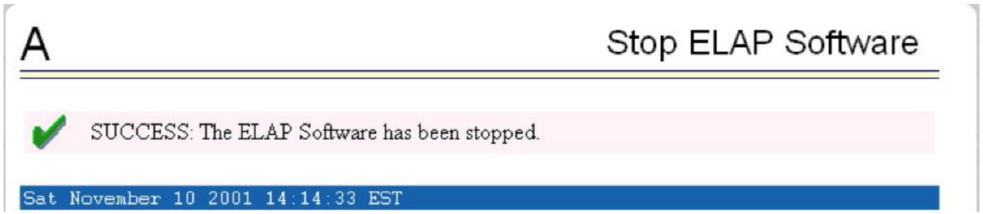
☑ Check if you want the software to automatically start on reboot.

Are you sure you want to stop the ELAP software?

4. On the **Stop ELAP Software** screen, make sure the checkboxes are is checked as shown in Figure A-9.
5. Click the **Stop ELAP Software** button to stop the software.

   The screen shown in Figure A-9 appears.

Figure A-9 Stop Software Completion Screen

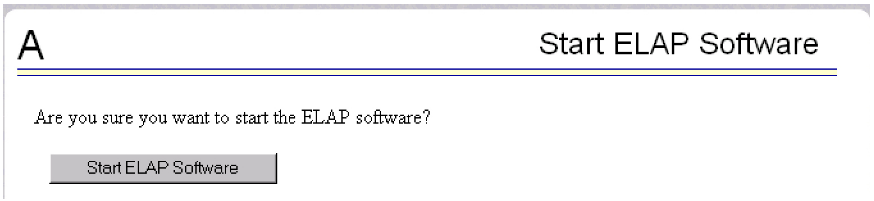


SUCCESS: The ELAP Software has been stopped.

Sat November 10 2001 14:14:33 EST

6. Select **Process Control> Start Software**.
7. From the **Start ELAP Software** screen, make sure the check boxes are checked as shown in Figure A-10:

Figure A-10 Start ELAP Software

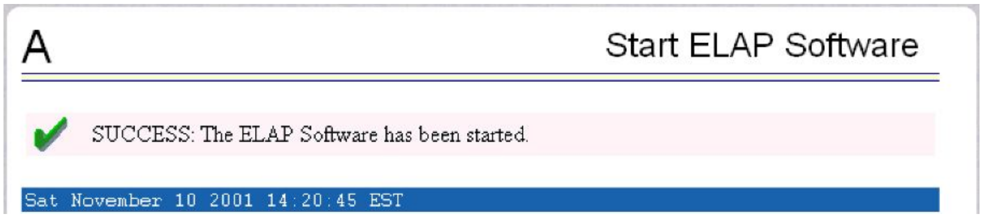


Are you sure you want to start the ELAP software?

8. Click the **Start ELAP Software** button to start the software.

   The screen shown in Figure A-11 confirms that the software has started:

Figure A-11 Start Software Completion Screen



SUCCESS: The ELAP Software has been started.

Sat November 10 2001 14:20:45 EST

Rebooting the MPS

This procedure is used when referenced by one of the procedures in Platform and Application Alarms.

> **Caution:**
>
> Perform this procedure only when directed to by one of the procedures in Platform and Application Alarms. This is not a standalone procedure.

The **PDBA** items that appear in the screens in this procedure apply only to the **EPAP** application. These items will not appear for the **ELAP** application.

1. Login to the **User Interface** screen of the ELAP**GUI** (see Accessing the ELAP GUI Interface).

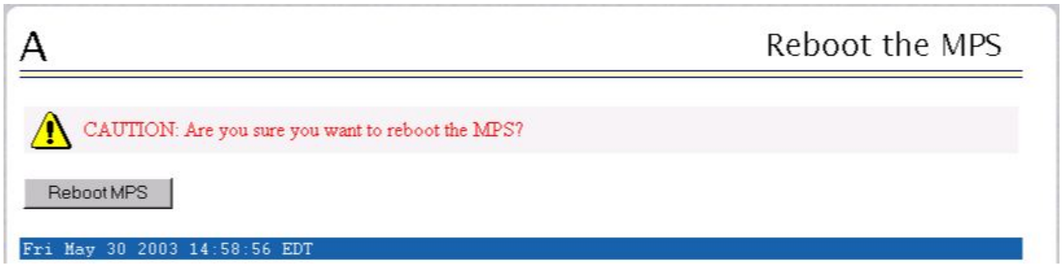
2. Check the banner information above the menu to verify that you are logged into the problem ELAP indicated in the **UAM**.

   Select **Select Mate** if necessary to switch to the problem ELAP.

3. Select **Platform> Reboot the MPS**.

   The screen shown in Figure A-12 appears:

Figure A-12 Request Reboot of the MPS



A

Reboot the MPS

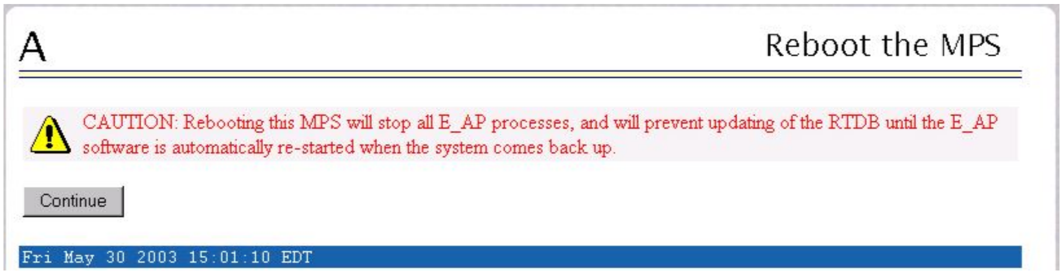
CAUTION: Are you sure you want to reboot the MPS?

Fri May 30 2003 14:58:56 EDT

4. Click the **Reboot the MPS** button to restart the **MPS**.

   The screen shown in Figure A-13 is displayed.

Figure A-13 Confirm Requested Reboot the MPS



A

Reboot the MPS

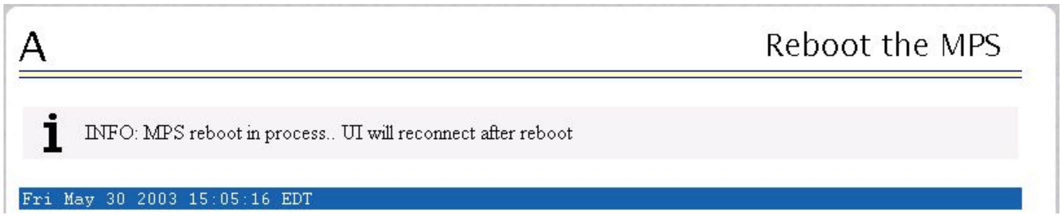
CAUTION: Rebooting this MPS will stop all E_AP processes, and will prevent updating of the RTDB until the E_AP software is automatically re-started when the system comes back up.

Fri May 30 2003 15:01:10 EDT

5. Click the **Continue** button.

   The screen shown in Figure A-14 is displayed.

Figure A-14 Reboot Information



A

Reboot the MPS

INFO: MPS reboot in process.. UI will reconnect after reboot

Fri May 30 2003 15:05:16 EDT

This will reboot the ELAP and also start the ELAP software. The connection to the ELAP will be lost.

6. At the **EAGLE** input terminal, enter the `rept-stat-mps` command to verify the status of the ELAP.

Refer to *Commands User's Guide* to interpret the output.

7. If the problem has not been resolved, contact #unique_13 for assistance.

   Have the system health check data available.

8. Return to the procedure that directed you to perform this procedure.