Oracle® Communications

EAGLE Application Processor Alarms and Maintenance Guide

Release 17.0
F58685-04
February 2025

Oracle Communications EAGLE Application Processor Alarms and Maintenance Guide, Release 17.0

F58685-04

Contents

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.

Acronyms

The following table provides information about the acronyms used in the document:

Table Acronyms

Acronym	Definition
ECC	Error Correcting Code
FRU	Field Replaceable Unit
GUI	Graphical User Interface
LED	Light Emitting Diode
SFTP	Secure File Transfer Protocol
SR	Service Request
UAM	Unsolicited Alarm Message
UIM	Unsolicited Information Message
WAN	Wide Area Network

What's New in This Guide

This section introduces the documentation updates for Release 17.0 in Oracle Communications EAGLE Application Processor Alarms and Maintenance Guide.

Release 17.0 - F58685-04, February 2025

- Added the minor application alarm "6000000001000000 - NE count mismatch between PDB and RTDB" in the Alarm Categories section.
- Added the minor application alarm 6000000001000000 - NE count mismatch between PDB and RTDB.

Release 17.0 - F58685-03, October 2024

Added information about the bugs 36552163 and 36186109 in Resolution Of Known Issues.

Release 17.0 - F58685-02, June 2023

Added information about the bug 35026943 in Resolution Of Known Issues.

Release 17.0 - F58685-01, March 2023

- Added new section Resolution Of Known Issues in Appendix A.
- Updated the User Interface Screen in Accessing the EPAP GUI section in Appendix A.
- Updated Health Check Outputs section to remove commands related to `/boot` in verbose `syscheck` output.

1 Introduction

This chapter provides general information about manual organization, the scope of this manual, its targeted audience, how to get technical assistance, and how to locate customer documentation on the Customer Support site.

1.1 Overview

This manual describes all available alarms and provides their recovery procedures.

2
Problem Detection and Reporting

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

2.1 Detecting and Reporting Problems

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

The EAGLE Application B Card (E5-APP-B) 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.

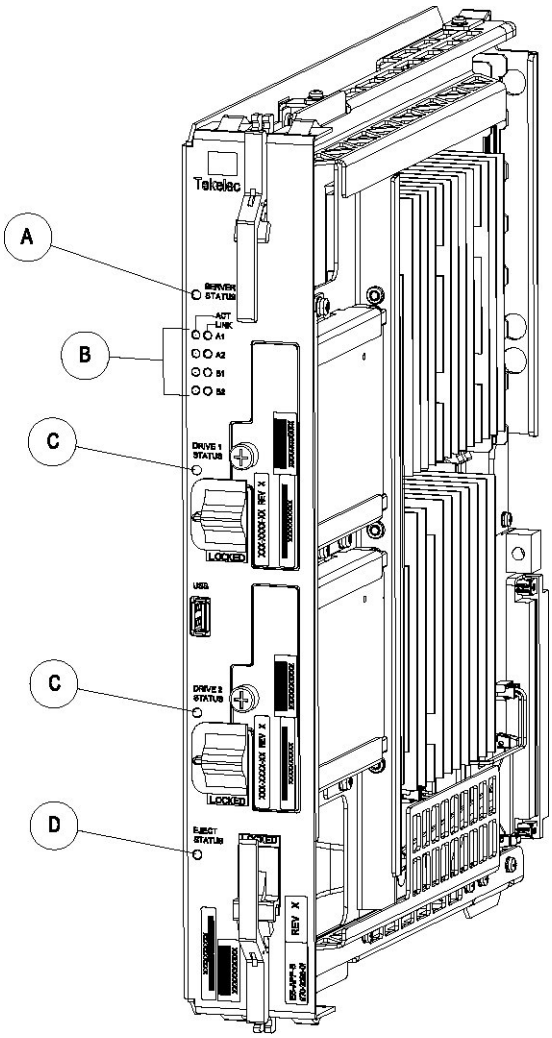
2.2 E5-APP-B Card LEDs

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

Server Panel LEDs

Figure 2-1 shows the E5-APP-B card LEDs on the front panel

Figure 2-1 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 2-1 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

Table 2-1 (Cont.) E5-APP-B LED Table

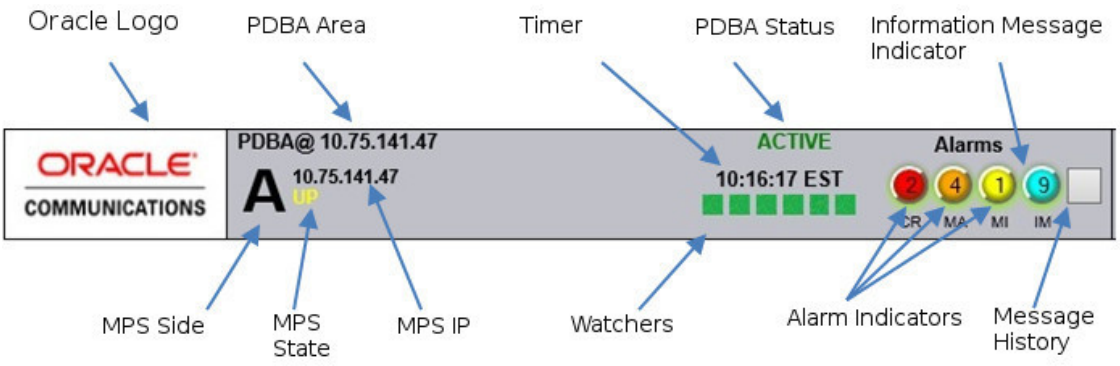
LED Name	HW/SW Controlled	Description
Drive 1 Status	SW/HW	HW: Flashing Green - Drive activity SW: Flashing Red - Impending drive removal SW: Steady red - Drive ready for removal
Drive 2 Status	SW/HW	HW: Flashing Green - Drive activity SW: Flashing Red - Impending drive removal SW: Steady red - Drive 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

2.3 Displaying Errors on EPAP GUI

If the EPAP application detects an application error or receives an alarm message from the platform layer, the EPAP application displays the error on the graphical user interface (GUI). See "EPAP GUI Main Screen" in *Administration Guide* for details on the EPAP GUI Banner.

Figure 2-2 shows the GUI banner components:

Figure 2-2 EPAP Banner Components

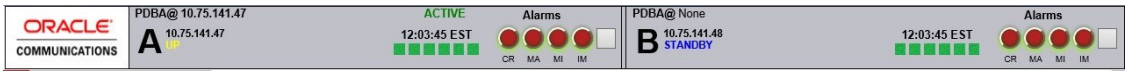


Tool tips are displayed for all EPAP banner components. Tool tips are activated when the mouse cursor (mouse-over event) is placed over the component. Each tip is unique to the banner component. The components of the EPAP Banner are displayed in Figure 2-2:

Viewing Alarm Details

The first three indicators (from left) are the alarm indicators on the EPAP GUI. These indicators displays the number of respective alarms on the EPAP. The left indicator indicates the Critical alarms; it turns red when a Critical alarm occurs. The middle indicator indicates the major alarms, and turns orange when a Major alarm is raised. The right indicator indicates the Minor alarm, and turns yellow when Minor alarm is raised. A maximum of 99 alarm counts can be displayed, considering the sum of all 3 alarm types. The indicator will remain brown if no alarm of that type is raised on the EPAP, as seen in Figure 2-3.

Figure 2-3 EPAP GUI With No Raised Alarms



Clicking on any of the alarm indicators displays the details of each prevailing alarm on the EPAP, depending on which alarm indicator is clicked, in a new window. The new window with alarm details will remain persistent until either the GUI is terminated or the user logs out of the GUI. The user will have to close all opened alarm windows manually. The details of alarm include:

1. Alarm severity and type (heading)
2. Alarm name

The individual alarm text is found in Alarm Categories. To correct the alarm condition, perform the associated procedure described in EPAP Alarm Recovery Procedures.

IPv4 and IPv6 Addresses in the EPAP GUI Banner

When the EPAP is configured as an IPv6-only node, the configured IPv6 address is reflected in both the PDB area and the MPS area. See "EPAP GUI Banner Section" in *Administration Guide* for different banner examples.

2.4 Unsolicited Alarm and Information Messages

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

- 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 Alarms.

3
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.

3.1 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
- Backing Up the PDB
- Transferring RTDB and PDB Backup Files

3.1.1 Backing Up the RTDB

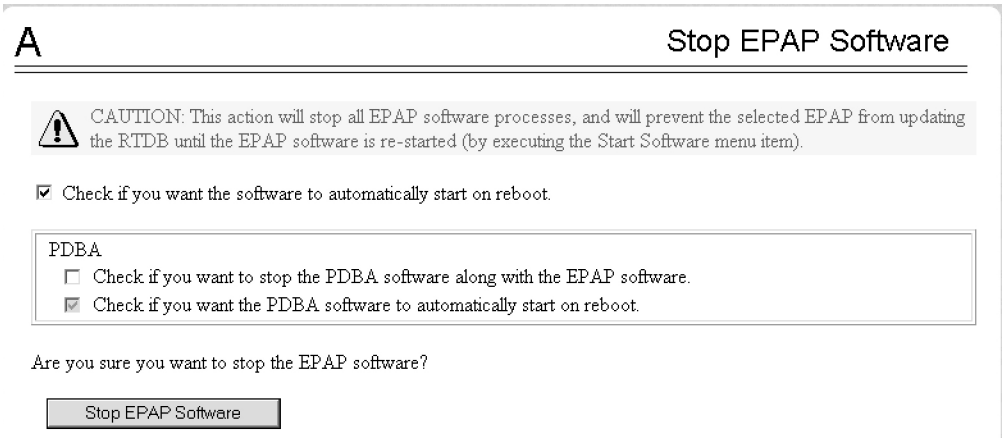
Perform this procedure once each day. The estimated time required to complete this procedure is one hour.

1. Log in to the EPAP**GUI** on server A as the **epapall** user.

   For information about how to log in to the EPAP **GUI**, refer to Accessing the EPAP GUI.
2. If you are not logged in to EPAP A, select the **Select Mate** option.
3. From the EPAP Menu, select **Process Control>Stop Software**.
4. In the Stop EPAP Software screen as shown in Figure 3-1, click **Stop EPAP Software**.

> **Note:**
>
> **DO NOT** select the option to stop the PDB along with the EPAP software.

Figure 3-1 Stop EPAP Software



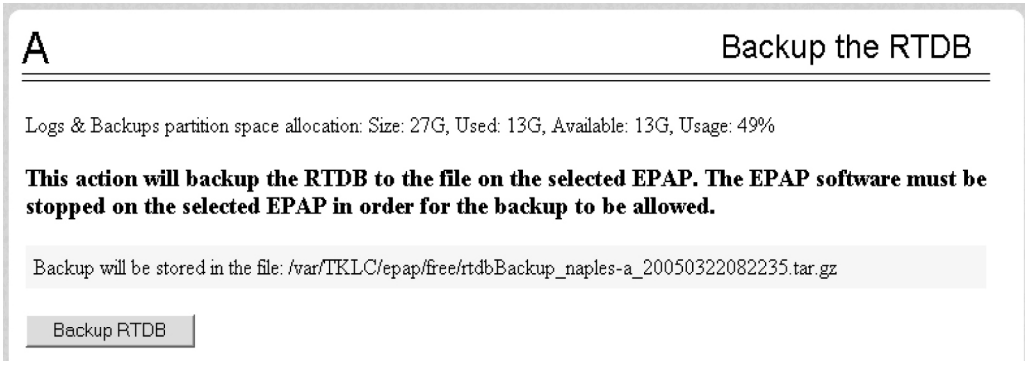
After the EPAP software has stopped successfully, the screen shown in Figure 3-2 is displayed.

Figure 3-2 EPAP Software Successfully Stopped

5. From the EPAP menu, select **RTDB>Maintenance>Backup RTDB**.

   The screen shown in Figure 3-3 is displayed.

Figure 3-3 Backup the RTDB



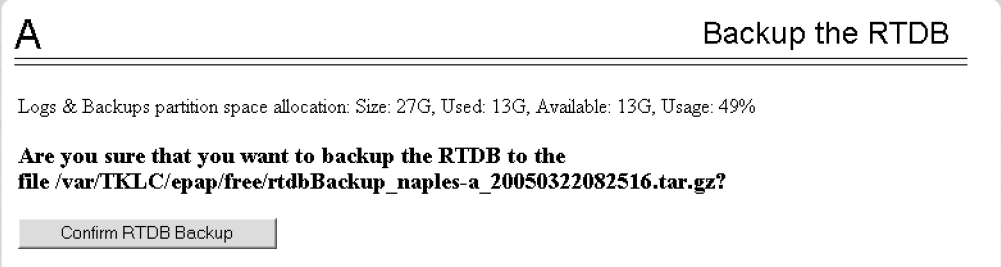
6. Record the file name as shown in this example:

   ```
   /var/TKLC/epap/free/rtdbBackup_naples-a20050322082516.tar.gz
   ```

7. Click **Backup RTDB**.

   The screen shown in Figure 3-4 displays a request for confirmation.

Figure 3-4 Backup the RTDB Confirmation



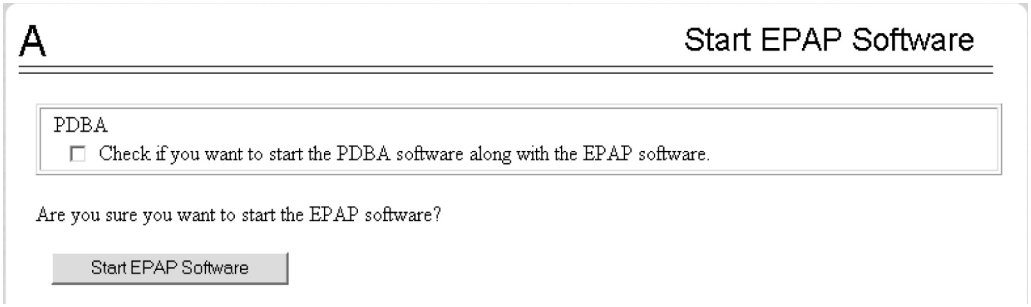
8. Click **Confirm RTDB Backup**.

   After the backup completes successfully, the screen shown in Figure 3-5 is displayed.

Figure 3-5 Backup the RTDB - Success

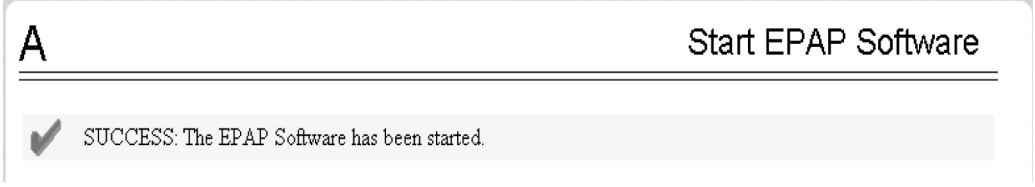
9. Select **Process Control>Start Software** from the EPAP Menu.
10. On the Start EPAP Software screen shown in Figure 3-6, click **Start EPAP Software**.

Figure 3-6 Start EPAP Software



After the EPAP software has started successfully, the screen in Figure 3-7 is displayed.

Figure 3-7 Start EPAP Software - Success



11. Continue to Backing Up the PDB.

3.1.2 Backing Up the PDB

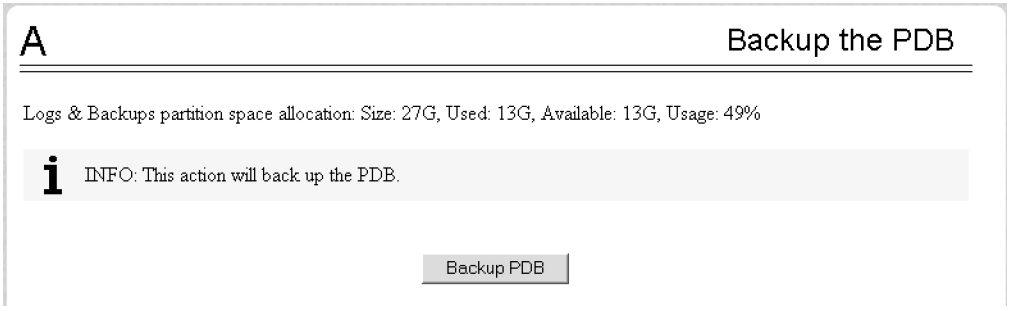
Perform this procedure once each day. The estimated time required to complete this procedure is two hours. PDB provisioning can take place while this procedure is being performed, but will extend the time required.

> **Note:**
>
> Make sure that you perform this procedure on the same server on which you performed Backing Up the RTDB. Make sure that you performed Backing Up the RTDB first so that the RTDB backup level will be lower than the associated PDB backup level.

1. Log in to the EPAP **GUI** on server A as the **epapall** user.

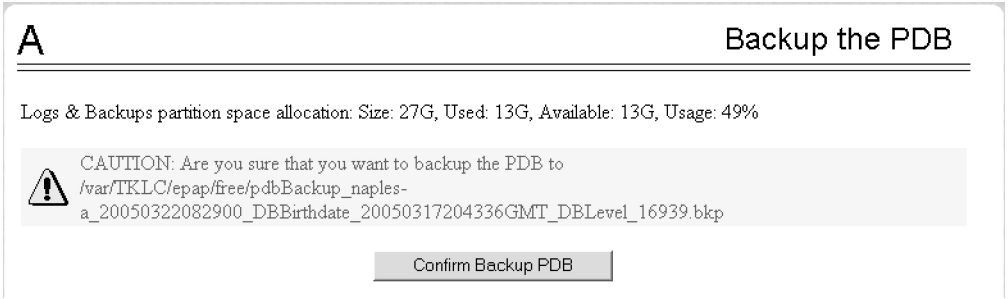
   For information about how to log in to the EPAP GUI, refer to Accessing the EPAP GUI.
2. If you are not logged in to EPAP A, select the **Select Mate** option.
3. From the EPAP Menu, select **PDBA>Maintenance>Backup>Backup the PDB**.
4. In the **Backup the PDB** screen shown in Figure 3-8, click **Backup PDB**.

Figure 3-8 Backup the PDB



The resulting screen, shown in Figure 3-9, displays a button to confirm the request to backup the PDB and the file name.

Figure 3-9 Backup PDB Confirmation



5. Record the file name.

   In this example, the file name is:

   ```
   /var/TKLC/epap/free/pdbBackup_naples-
   a_20050322082900_DBBirthdate_20050317204336GMT_DBLevel_16939.bkp
   ```

6. Click **Confirm Backup PDB**.

   After the backup completes successfully, the screen shown in Figure 3-10 is displayed:

Figure 3-10 Backup the PDB - Success

7. Continue to Transferring RTDB and PDB Backup Files .

3.1.3 Transferring RTDB and PDB Backup Files

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

1. Log in to the **EPAP** command line interface with user name `epapdev` and the password associated with that user name.
2. Use the Secure **File Transfer Protocol** (`sftp`) to transfer the following files to a remote, safe location:
   a. The **RTDB** backup file, the name of which was recorded in Backing Up the RTDB
   b. The **PDB** backup file, the name of which was recorded in Backing Up the PDB

3.2 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 OutputsHealth 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 EPAP**GUI** Platform Menu (see Accessing the EPAP GUI). 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 3-1 summarizes the functions checked by `syscheck`.

Table 3-1 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.
Swap Space	Verify that disk swap space is sufficient for efficient operation. All **TPD** installations are configured with 16 Gigabytes of swap space. The swap space is allocated between two physical disk partitions: • The first partition is 2 Gigabytes in size. It resides on a software **RAID** device, `/dev/md2`, which is a raid-1 mirror set made up of physical devices `/dev/hda2` and `/dev/hdc2`. • The second partition is 14 Gigabytes and is formatted with a filesystem. The 14 Gigabytes of space on this partition is divided into multiple 2 Gigabyte swap files. The second partition is software **RAID** device `/dev/md11`, which is a mirror set consisting of physical partitions `/dev/hda11` and `/dev/hdc11`, and is mounted under `/var/TKLC/swap`.
Memory	Verify that 8 **GB** of **RAM** is installed.

Table 3-1 (Cont.) System Health Check Operation

System Check	Function
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.
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.

3.2.1 Health Check Outputs

System health check utility `syscheck` output can be Normal (brief) or Verbose (detailed), depending on how it is initiated.

Normal Output

The following example is an output in Normal format:

```
[admusr@EPAP17 ~]$ sudo syscheck
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

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

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 example is an output in Verbose format:

```
[admusr@Salta-a ~]$ sudo syscheck -v
Running modules in class disk...
          fs: Current file space use in "/" is 31%.
          fs: Current Inode used in "/" is 10%.
          fs: Current file space use in "/usr" is 57%.
          fs: Current Inode used in "/usr" is 19%.
          fs: Current file space use in "/var" is 30%.
          fs: Current Inode used in "/var" is 4%.
          fs: Current file space use in "/var/TKLC" is 31%.
          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 "/var/TKLC/epap/db" is 88%.
          fs: Current Inode used in "/var/TKLC/epap/db" is 0%.
          fs: Current file space use in "/var/TKLC/epap/logs" is 3%.
          fs: Current Inode used in "/var/TKLC/epap/logs" is 0%.
          fs: Current file space use in "/var/TKLC/epap/free" is 7%.
          fs: Current Inode used in "/var/TKLC/epap/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 2 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 "/var/TKLC/epap/db".
       write: Successfully read from file system "/var/TKLC/epap/logs".
       write: Successfully read from file system "/var/TKLC/epap/free".
```

```
                                                                OK

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
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: +24.5 C (high = +70.0 C, warn =
+66 C, hyst = +75.0 C), CHIP: lm75-i2c-0-48
        temp: Server Temp OK. Outlet Air Temp: +27.5 C (high = +70.0 C, warn
= +66 C, hyst = +75.0 C), CHIP: lm75-i2c-0-49
        temp: Server Temp OK. MCH Diode Temp: +38.9 C (high = +95.0 C, warn =
+90 C, low = +10.0 C), CHIP: sch311x-isa-0a70
        temp: Server Temp OK. Internal Temp: +25.1 C (high = +95.0 C, warn =
+90 C, low = +10.0 C), CHIP: sch311x-isa-0a70
        temp: Server Temp OK. Core 0: +32.0 C (high = +71.0 C, crit = +95.0
C, warn = +67 C), CHIP: coretemp-isa-0000
        temp: Server Temp OK. Core 1: +32.0 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: +1.08 V (min = +0.85 V, max = +1.35 V),
CHIP: sch311x-isa-0a70
     voltage: Voltage is OK. V3.3: +3.28 V (min = +3.13 V, max = +3.47 V),
CHIP: sch311x-isa-0a70
     voltage: Voltage is OK. V5: +4.93 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: +3.29 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.
                                OK

Running modules in class net...
  defaultroute: Checking default route(s)
  defaultroute:   Checking static default route through device eth01 to
gateway fe80::226:98ff:fe1a:9ac1...
  defaultroute:   Checking static default route through device eth01 to
gateway 192.168.61.250...
  defaultroute:   Checking auto-configured default route through device eth04
to gateway fe80::226:98ff:fe1a:9ac1...
        ping: Checking ping hosts
        ping: prova-ip 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 sshd...
         run: Found 3 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 alarmMgr...
         run: Found 1 instance(s) of the alarmMgr process.
         run: Checking tpdProvd...
         run: Found 1 instance(s) of the tpdProvd process.
         run: Checking maint...
         run: Found 1 instance(s) of the maint process.
         run: Checking pdba...
         run: Found 1 instance(s) of the pdba 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 2 instance(s) of the mysqld process.
            run: Checking httpd...
            run: Found 12 instance(s) of the httpd process.
            run: Checking epapSnmpAL...
            run: Found 1 instance(s) of the epapSnmpAL process.
            run: Checking epapSnmpAgent...
            run: Found 1 instance(s) of the epapSnmpAgent process.
            run: Checking epapSnmpHBS...
            run: Found 1 instance(s) of the epapSnmpHBS process.
            run: Checking snmpd...
            run: Found 1 instance(s) of the snmpd process.
                                 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: 2660.018 MHz... OK
            cpu: CPU 1 is on-line... OK
            cpu: CPU 1 speed: 2660.018 MHz... OK
          kdump: Checking for kernel dump files.
            mem: Skipping expected memory check.
            mem: Minimum expected memory found.
            mem: 8252940288 bytes (~7871 Mb) of RAM installed.
                                 OK

Running modules in class upgrade...
   snapshots: No snapshots found. Not running test.
                                 OK

LOG LOCATION: /var/TKLC/log/syscheck/fail_log
[admusr@Salta-a ~]$
```

> **Note:**
>
> For information on alarm codes in the alarm strings and procedures to respond to alarms, see the section Alarm Categories.

3.3 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 EPAP GUI
- Running syscheck Using the syscheck Login

3.3.1 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
```

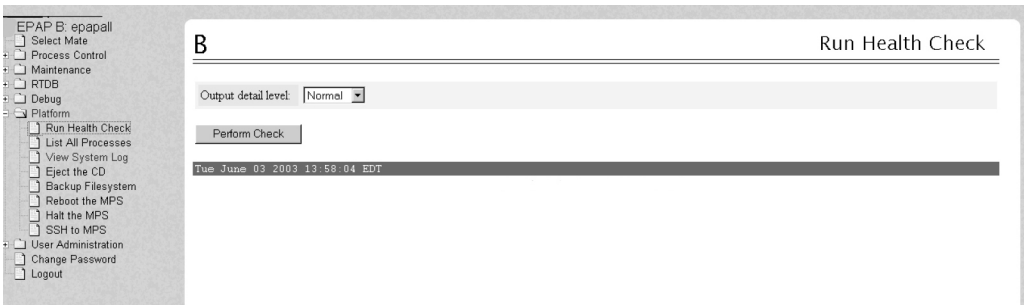
For help on command syntax, use the `-h` option.`$ syscheck`

3.3.2 Running syscheck Through the EPAP GUI

Refer to *Administration Guide* for more details and information about logins and permissions.

1. Log in to the User Interface of the EPAP **GUI** (see Accessing the EPAP GUI).
2. Check the banner information above the menu to verify that the EPAP about which system health information is sought is the one that is logged into.
3. If it is necessary to switch to the other EPAP, click the **Select Mate** menu item.
4. When the GUI shows you are logged into the EPAP about which you want system health information, select **Platform > Run Health Check** as shown in the following window.

Figure 3-11 Run Health Check



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. The example shown in Figure 3-12 shows Normal output with errors.

Figure 3-12 Displaying System Health Check on EPAP GUI

3.3.3 Running syscheck Using the syscheck Login

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

1. Connect the Local Access Terminal to the server whose status you want to check (see *Administration Guide*).
2. Log in as the `syscheck` user.

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

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

3.4 Restoring Databases from Backup Files

This section describes how restore the RTDB or PDB or both from backup files.

Restoring the RTDB from Backup Files

To restore the EPAP's RTDB from a backup file, contact My Oracle Support.

> **Note:**
>
> Back up the RTDB daily (see Backing Up the RTDB).

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

> **Caution:**
>
> Contact My Oracle Support before performing this procedure.

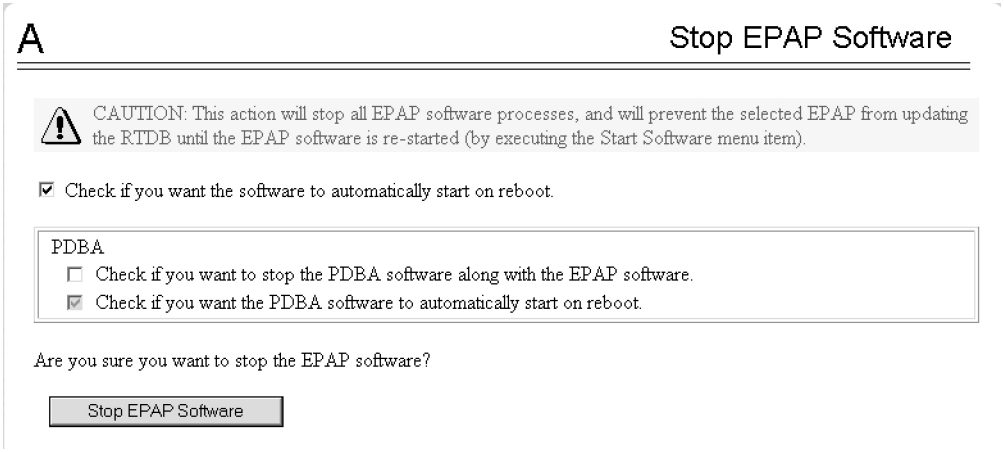
1. Log into the EPAP command line interface with user name `epapdev` and the password associated with that name.

2. Use the Secure File Transfer Protocol (`sftp`) to transfer the RTDB backup file (whose name was recorded in Restoring Databases from Backup Files) to the following location:

   ```
   /var/TKLC/epap/free/
   ```

3. Log into the EPAP **GUI** (see Accessing the EPAP GUI).
4. Select **Process Control>Stop Software** to ensure that no other updates are occurring. The screen in Figure 3-13 displays:

Figure 3-13 Stop EPAP Software

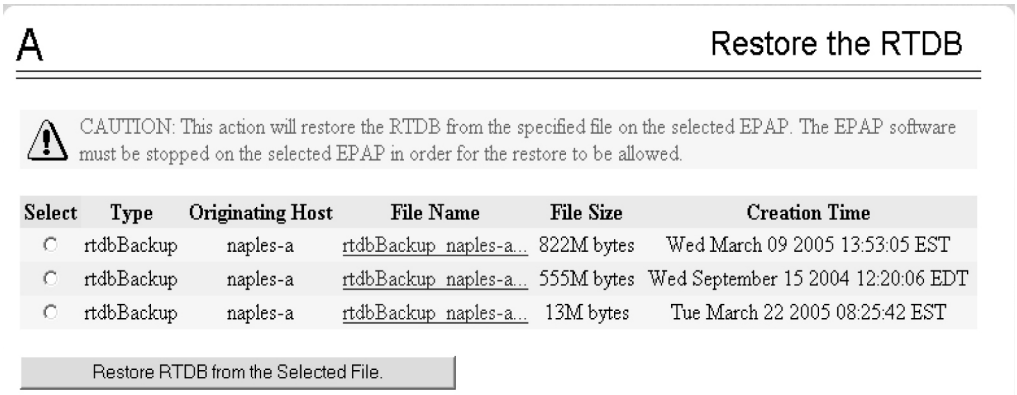


5. When you stopped the software on the selected EPAP, the screen in Figure 3-14 displays:

Figure 3-14 Stop EPAP Software - Success

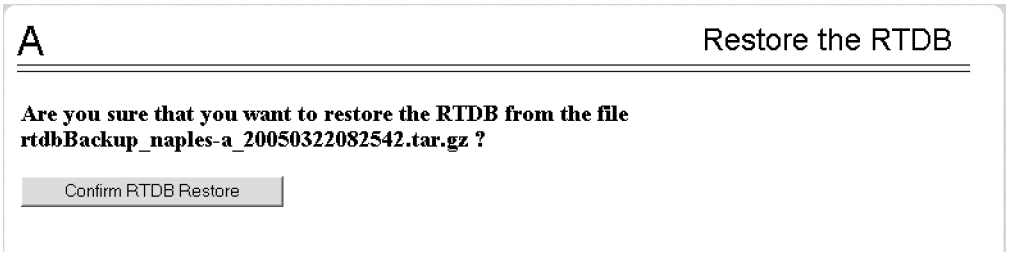
6. Select **RTDB>Maintenance>Restore** . The screen shown in Figure 3-15 displays:

Figure 3-15 Restoring the RTDB



7. On the screen shown in Figure 3-15, select the file that was transferred in Figure 3-15. Click **Restore the RTDB from the Selected File**.
8. To confirm restoring a file, click **Confirm RTDB Restore** shown in the screen for RTDB in Figure 3-16:

Figure 3-16 Restore the RTDB Confirm



9. When restoring the file is successful, the screen shown in Figure 3-17 displays:

Figure 3-17 Restore the RTDB - Success

10. This procedure is complete.

Restoring the PDB from Backup Files

To restore the EPAP's PDB from a backup file, contact Technical Services and Support, see My Oracle Support.

> **Note:**
>
> Back up the PDB daily (see Backing Up the PDB).

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

> **Caution:**
>
> Contact My Oracle Support before performing this procedure.

Text inset.

1. Log into the EPAP command line interface with user name `epapdev` and the password associated with that name.

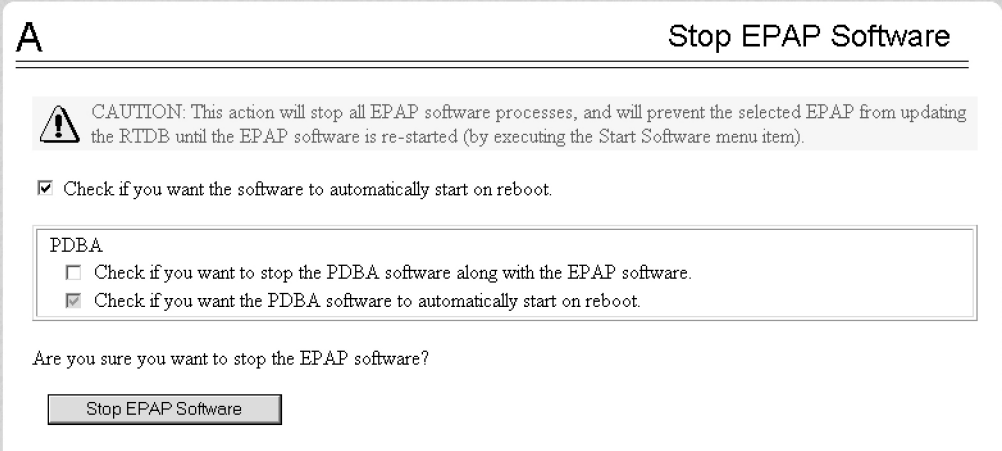
2. Use the Secure File Transfer Protocol (`sftp`) to transfer the PDB backup file (whose name was recorded in 4) to the following location:

   `/var/TKLC/epap/free/`

3. Log into the EPAP**GUI** (see Accessing the EPAP GUI).
4. Select **Process Control>Stop Software** to ensure that no other updates are occurring.

   The screen in Figure 3-18 displays:

Figure 3-18 Stop EPAP Software



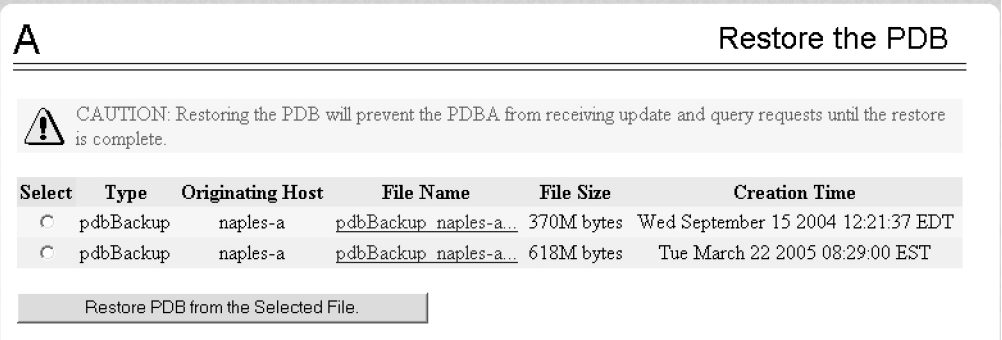
5. When you stopped the software on the selected EPAP, the screen in Figure 3-19 displays:

Figure 3-19 Stop EPAP Software - Success

6. Select **PDBA>Maintenance>Backup>Restore the PDB**.

   The screen shown in Figure 3-20 displays:

Figure 3-20 Restoring the PDB



7. On the screen shown in 6, select the file that was transferred in Restoring Databases from Backup Files.

   Click **Restore the PDB from the Selected File**.

8. Click **Confirm PDB Restore**.
9. When restoring the file is successful, a message displays informing you that the procedure was successful.

3.5 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 My Oracle Support.

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

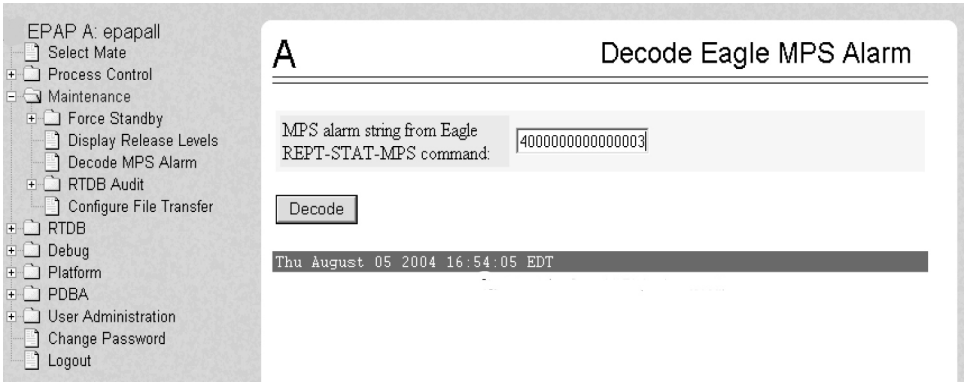
- If the problem being investigated **is no longer displayed** on the EPAP GUI, perform the following:
  1. Procedure Decode Alarm Strings
  2. Procedure Determine Alarm Cause
  3. Recovery procedure to which you are directed by procedure Determine Alarm Cause
- If the problem being investigated **is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

3.5.1 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 EPAP **GUI** (see Accessing the EPAP GUI).
2. After logging in to the EPAP, select **Maintenance>Decode MPS Alarm** from the menu.
3. Enter the 16-digit alarm string into the window on the **Decode MPS Alarm** screen, as shown in Figure 3-21.

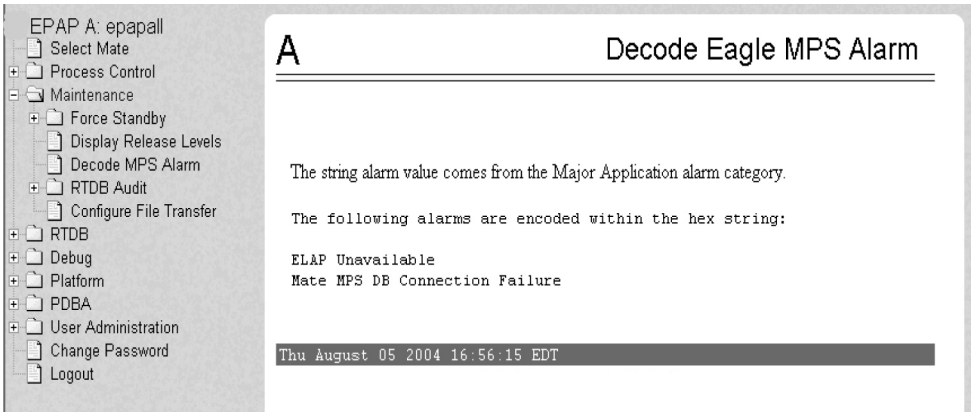
Figure 3-21 Decode MPS Alarm Screen



4. Click the **Decode** button.

The system returns information on the Alarm Category (Critical Application, Major Platform) and error text, as shown in Figure 3-22.

Figure 3-22 Decoded MPS Alarm Information



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

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

3.5.2 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 EPAP**GUI** , or as decoded from Decode Alarm Strings.
2. Run `syscheck` in Verbose mode (see Running the System Health Check).
3. Examine the `syscheck` output for specific details about the alarm.
4. Find the recovery procedure for the alarm in the procedures shown in EPAP Alarm Recovery Procedures. 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 (**FRU**s) in Recovering From Alarms if instructed by an alarm recovery procedure to replace a **FRU**.
   - Refer to general procedures used in a number of alarm recovery procedures in General Procedures
5. If the alarm persists after performing the appropriate procedure, call My Oracle Support.

4
Alarms

This chapter provides recovery procedures for platform and application alarms.

4.1 Alarm Categories

This chapter describes recovery procedures to use when an alarm condition or other problem occurs on the server. 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 Table 4-1. The procedures for correcting alarm conditions are described in Recovering From 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 4-1 shows the alarm numbers and alarm text for all alarms generated by the platform and the EPAP application. The order within a category is not significant.

Table 4-1 Platform and Application Alarms

Alarm Codes and Error Descriptor	UAM Number
Critical Platform Alarms	
1000000000002000 - Uncorrectable ECC Memory Error	0370
Major Platform Alarms	
32300 3000000000000001 – Server Fan Failure	0372
32301 3000000000000002 - Server Internal Disk Error	0372
32303 3000000000000008 - Server Platform Error	0372
32304 3000000000000010 - Server File System Error	0372
32305 3000000000000020 - Server Platform Process Error	0372

Table 4-1 (Cont.) Platform and Application Alarms

Alarm Codes and Error Descriptor	UAM Number
32307 3000000000000080 - Server Swap Space Shortage Failure	0372
32308 3000000000000100 - Server Provisioning Network Error	0372
32309 3000000000000200 – Server Eagle Network A Error	0372
32310 3000000000000400 – Server Eagle Network B Error	0372
32311 3000000000000800 – Server Sync Network Error	0372
32312 3000000000001000 - Server Disk Space Shortage Error	0372
32313 3000000000002000 - Server Default Route Network Error	0372
32314 3000000000004000 - Server Temperature Error	0372
32315 3000000000008000 – Server Mainboard Voltage Error	0372
32317 3000000000020000 - Server Disk Health Test Error	0372
32318 3000000000040000 - Server Disk Unavailable Error	0372
32321 3000000000200000 – Correctable ECC Memory Error	0372
32334 3000000400000000 - Multipath Device Access Link Problem	0372
3000000800000000 – Switch Link Down Error	0372
32336 3000001000000000 - Half-open Socket Limit	0372
32337 3000002000000000 - Flash Program Failure	0372
32338 3000004000000000 - Serial Mezzanine Unseated	0372
Major Application Alarms	
4000000000000001 - Mate EPAP Unavailable	0373
4000000000000002 - RTDB Mate Unavailable	0373
4000000000000004 - Congestion	0373
4000000000000008 - File System Full	0373
4000000000000010 - Log Failure	0373
4000000000000020 - RMTP Channels Down	0373
4000000000000040 - Fatal Software Error	0373
4000000000000080 - RTDB Corrupt	0373
4000000000000100 - RTDB Inconsistent	0373
4000000000000200 - RTDB Incoherent	0373
4000000000001000 - RTDB 100% Full	0373
4000000000002000 - RTDB Resynchronization In Progress	0373
4000000000004000 - RTDB Reload Is Required	0373
4000000000008000 - Mate PDBA Unreachable	0373
4000000000010000 - PDBA Connection Failure	0373
4000000000020000 - PDBA Replication Failure	0373
4000000000040000 - RTDB DSM Over-Allocation	0373
4000000000080000 - RTDB Maximum Depth Reached	0373
4000000000100000 - No PDBA Proxy to Remote PDBA Connection	0373
4000000000200000 - DSM Provisioning Error	0373
4000000000800000 - EPAP State Changed to UP	0373

Table 4-1 (Cont.) Platform and Application Alarms

Alarm Codes and Error Descriptor	UAM Number
4000000004000000 - RTDB Overallocated	0373
4000000020000000 - Mysql Lock Wait Timeout Exceeded	0373
Minor Platform Alarms	
32500 5000000000000001 – Server Disk Space Shortage Warning	0374
32501 5000000000000002 – Server Application Process Error	0374
5000000000000004 - Server Hardware Configuration Error	0374
32506 5000000000000040 – Server Default Router Not Defined	0374
32507 5000000000000080 – Server Temperature Warning	0374
32508 5000000000000100 – Server Core File Detected	0374
32509 5000000000000200 – Server NTP Daemon Not Synchronized	0374
32511 5000000000000800 – Server Disk Self Test Warning	0374
32514 5000000000004000 – Server Reboot Watchdog Initiated	0374
32518 5000000000040000 – Platform Health Check Failure	0374
32519 5000000000080000 – NTP Offset Check Failed	0374
32520 5000000000100000 – NTP Stratum Check Failed	0374
325295000000020000000 – Server Kernel Dump File Detected	0374
325305000000040000000 – TPD Upgrade Failed	0374
325315000000080000000– Half Open Socket Warning	0374
5000000100000000 – Server Upgrade Pending Accept/ Reject	0374
Minor Application Alarms	
6000000000000001 - RMTP Channel A Down	0375
6000000000000002 - RMTP Channel B Down	0375
6000000000000008 - RTDB 80% Full	0375
6000000000000010 - Minor Software Error	0375
6000000000000020 - Standby PDBA Falling Behind	0375
6000000000000040 - RTDB Tree Error	0375
6000000000000080 - PDB Backup failed	0375
6000000000000100 - Automatic PDB Backup failed	0375
6000000000000200 - RTDB Backup failed	0375
6000000000000400 - Automatic RTDB Backup failed	0375
6000000000001000 - SSH tunnel not established	0375
6000000000002000 - RTDB 90% Full	0375
6000000000004000 - PDB 90% Full	0375
6000000000008000 - PDB 80% Full	0375
6000000000010000 - PDB InnoDB Space 90% Full	0375
6000000000040000 - RTDB Client Lagging Behind	0375
6000000000080000 - Automatic Backup is not configured	0375
6000000000100000 - EPAP QS Replication Issue	0375

Table 4-1 (Cont.) Platform and Application Alarms

Alarm Codes and Error Descriptor	UAM Number
6000000000200000 - EPAP QS Lagging Behind	0375
6000000000400000 - License capacity is not configured	0375
6000000000800000 - Long wait on write for PDBI update	0375
6000000001000000 - NE count mismatch between PDB and RTDB	0375
NOTE: The order within a category is not significant.	

4.2 EPAP Alarm Recovery Procedures

This section provides recovery procedures for platform and application alarms. The alarm categories are listed by severity.

4.3 Critical Platform Alarms

4.3.1 1000000000002000 - Uncorrectable ECC Memory Error

Alarm Type: TPD

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

Severity: Critical

OID: 1.3.6.1.4.1.323.5.3.18.3.1.1.14TpdFanErrorNotifyTpdEccUncorrectableError

Alarm ID: TKSPLATCR141000000000002000

Recovery

- Contact My Oracle Support to request hardware replacement.

4.4 Critical Application Alarms

No critical **EPAP** alarms are generated.

4.5 Major Platform Alarms

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

4.5.1 32300 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: TpdFanErrorNotifyTpdFanErrorNotify 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 EPAP 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 My Oracle Support.

4.5.2 32301 3000000000000002 - Server Internal Disk Error

Alarm Type: TPD

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

Severity: Major

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.2TpdFanErrorNotifyTpdIntDiskErrorNotify

Alarm ID: TKSPLATMA23000000000000002

Recovery

1. Run syscheck in Verbose mode (see procedure Running the System Health Check.).
2. Contact the My Oracle Support and provide the system health check output.

> **Note:**
>
> Refer to *Hardware and Installation Guide* for E5-APP-B, *Field Replaceable Units (FRUs)* section for information about installing a hard disk drive.

3. Contact My Oracle Support.

4.5.3 32303 3000000000000008 - Server Platform Error

Alarm Type: TPD

Description: This alarm indicates an error such as a corrupt system configuration or missing files, or indicates that syscheck itself is corrupt.

Severity: Major

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.4TpdFanErrorNotifyTpdPlatformErrorNotify

Alarm ID: TKSPLATMA43000000000000008

Recovery

1. Run syscheck in Verbose mode (see procedure Run Syscheck Manually).).
2. Contact My Oracle Support and provide the system health check output.

4.5.4 32304 3000000000000010 - Server File System Error

Alarm Type: TPD

Description: This alarm indicates that syscheck was unsuccessful in writing to at least one of the server's file systems.

Severity: Major

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.5TpdFanErrorNotifyTpdFileSystemErrorNotify

Alarm ID: TKSPLATMA53000000000000010

Recovery

- Contact My Oracle Support.

4.5.5 32305 3000000000000020 - Server Platform Process Error

Alarm Type: TPD

Description: 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.

Severity: Major

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.6TpdFanErrorNotifyTpdPlatProcessErrorNotify

Alarm ID: TKSPLATMA63000000000000020

Recovery

1. Rerun syscheck in verbose mode (see procedure Running the System Health Check).
   - If the alarm has been cleared, the problem is solved.
   - If the alarm has not been cleared, contact My Oracle Support.
2. Contact My Oracle Support.

4.5.6 32307 3000000000000080 - Server Swap Space Shortage Failure

Alarm Type: TPD

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

Severity: Major

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.8TpdFanErrorNotifyTpdSwapSpaceShortageErrorNotify

Alarm ID: TKSPLATMA83000000000000080

Recovery

- Contact My Oracle Support.

4.5.7 32308 3000000000000100 - Server Provisioning Network Error

Alarm Type: TPD

Description: This alarm indicates that the connection between the server's eth1ethernet interface and the customer network is not functioning properly. The eth1 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: TpdFanErrorNotifyTpdProvNetworkErrorNotify 1.3.6.1.4.1.323.5.3.18.3.1.2.9

Alarm ID: TKSPLATMA93000000000000100

Recovery

1. Verify that a customer-supplied cable labeled TO CUSTOMER NETWORK is securely connected to the upper right port on the rear of the server on the EAGLE backplane.to the appropriate server. Follow the cable to its connection point on the local network and verify this connection is also secure.
2. Test the customer-supplied cable labeled TO CUSTOMER NETWORK with an Ethernet Line Tester. If the cable does not test positive, replace it.
3. Have your network administrator verify that the network is functioning properly.
4. 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 My Oracle Support.

4.5.8 32309 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 A) connects to the customer provisioning network.
- The **eth02** interface (2nd from top ethernet port on the rear of the server A) connects to port 3 of switch A.
- The **eth03** interface (2nd from bottom ethernet port on the rear of the server A) connects to port 3 of switch B.
- The **eth04** interface (bottom ethernet port on the rear of the server A) is an optional connection to the backup customer provisioning network.
- 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 5 through 21 of switch A 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. Refer to MPS-specific documentation for information regarding this alarm.
2. Contact My Oracle Support.
3. Perform the following:
   a. Verify that both servers are powered on by confirming that the **POWER** LEDs on both servers are illuminated green.
   b. Verify that the switch is powered on.
   c. Verify that the switch does not have any fault lights illuminated.
   d. Verify that the **eth01** cable is securely connected to the top port on the server that is reporting the error.
   e. Trace the **eth01** cable to the switch. Verify that the **eth01** cable is securely connected at correct point of the customer uplink.
   f. Verify that the cable connecting the switches is securely connected at both switches.
4. Run `syscheck` (see Running syscheck Through the EPAP GUI).
   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 My Oracle Support.
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, (see Saving Logs Using the EPAP **GUI**).
9. Run `savelogs_plat` to gather system information for further troubleshooting, (see Saving Logs Using the EPAP **GUI**), and contact My Oracle Support.

4.5.9 32310 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 B) connects to the customer provisioning network.
- The **eth02** interface (2nd from top ethernet port on the rear of the server B) connects to port 4 of switch A.

- The **eth03** interface (2nd from bottom ethernet port on the rear of the server B) connects to port 4 of switch B.
- The **eth04** interface (bottom ethernet port on the rear of the server B) is an optional connection to the customer backup provisioning network.
- 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 5 through 21 of switch B can be used for links to the Backup SM ports (SM B 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. Refer to MPS-specific documentation for information regarding this alarm.
2. Contact My Oracle Support.
3. Perform the following:
   a. Verify that both servers are powered on by confirming that the **POWER** LEDs on both servers are illuminated green.
   b. Verify that the switch is powered on.
   c. Verify that the switch does not have any fault lights illuminated.
   d. Verify that the **eth01** cable is securely connected to the top port of the server that is reporting the error.
   e. Trace the **eth01** cable to the switch. Verify that the **eth01** cable is securely connected to the correct point of the customer uplink.
   f. Verify that the cable connecting the switches is securely connected at both switches.
4. Run `syscheck` (see Running syscheck Through the EPAP GUI).
   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 My Oracle Support 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 EPAP **GUI**).
9. Run `savelogs_plat` to gather system information for further troubleshooting, (see Saving Logs Using the EPAP **GUI**), and contact My Oracle Support.

4.5.10 32311 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: TKSPLATMA123000000000000800

Recovery

1. Refer to MPS-specific documentation for information regarding this alarm.
2. Contact My Oracle Support.
3. Verify that both servers are powered on by confirming that the **POWER** LEDs on both servers are illuminated green.

4. Verify that the **eth03** cable is securely connected to the 2nd from bottom ethernet port on both Server A and Server B.
5. Test the **eth03** cable with an Ethernet Line Tester that is set to test a straight-through cable.
6. If the cable does not test positive, replace it.
7. If the problem persists, call My Oracle Support for assistance. Switch B may have failed.
8. Perform general **IP** troubleshooting.

   The `syscheck` utility reports this error when it tries to `ping` hosts sync-a and sync-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 sync-a and/or sync-b select menu options:`Diagnostics->Network Diagnostics->Ping`

   d. To verify no routing issues exist, select menu options:`Diagnostics->Network Diagnostics->Traceroute`
9. Run `savelogs` to gather all application logs (see Saving Logs Using the EPAP **GUI**).
10. Run `savelogs_plat` to gather system information for further troubleshooting, (see Saving Logs Using the EPAP **GUI**), and contact Platform Engineering.

4.5.11 32312 3000000000001000 - Server Disk Space Shortage Error

Alarm Type: TPD

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

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

Severity: Major

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.13

Alarm ID: TKSPLATMA133000000000001000

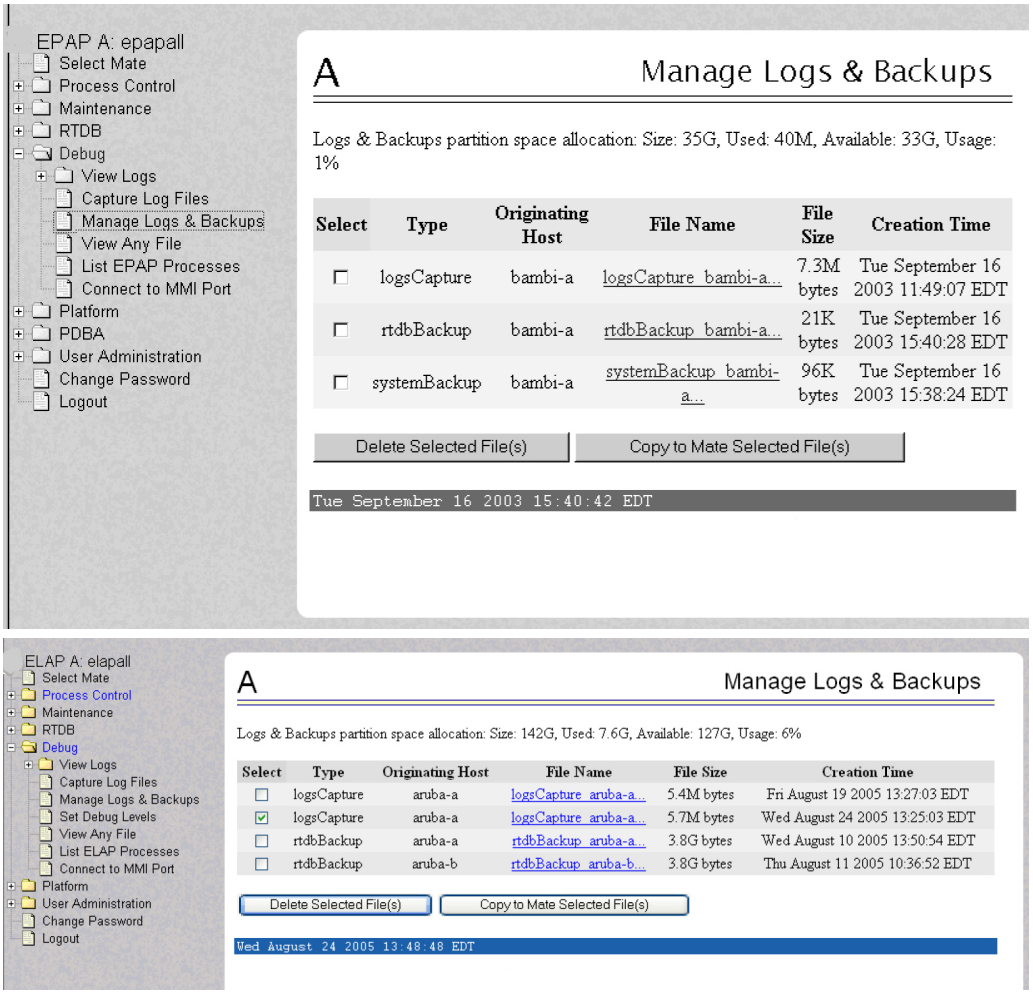
Recovery

1. Run `syscheck`.
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 EPAP **GUI**.
   b. Select **Debug>Manage Logs & Backups**.

      A screen similar to Figure 4-1 is displayed. This screen displays the 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 4-1 Manage Logs and Backups



   c. Click the checkbox of each file that you want to delete and then click **Delete Selected File(s)**.

4. If the file system mounted on `/var/TKLC/epap/logs/var/TKLC/elap/logs` is the file system that syscheck is reporting to be low on space, execute the following steps:
   a. Log into the server generating the alarm as the admusr:

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

b. Change to the `/var/TKLC/epap/logs` directory:

```
$ cd /var/TKLC/epap/logs
```

c. Confirm that you are in the `/var/TKLC/epap/logs` directory:

```
$ pwd
/var/TKLC/epap/logs
```

d. When the `pwd` command is executed, if `/var/TKLC/epap/logs` is not output, go back to sub-step b.

e. Look for files that you want to delete and execute an `rm` command for each:

```
$ sudo rm <filename>
```

where `<filename>` is replaced by the name of the file to be deleted.

f. Re-run `syscheck`.

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

5. If syscheck has determined inodes have been depleted or a file system has a different number of blocks, skip to 11.

6. Execute the following steps to collect and remove any core files from the server.

Core files can occupy a large amount of disk space and may be the cause of this alarm:

a. Log into the server generating the alarm as the admusr:

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

b. To list core files on the server, execute the following command, where `<mountpoint>` is the file system's mount point:

```
$ sudo find <mountpoint> -name core.[0-9]\* -print -exec gzip -9 {} \;
```

> **Note:**
>
> The find command shown above will list any core files found and then compress and rename the file adding a ".gz" extension.

If any core files are found, transfer them off of the system and save them aside for examination by Oracle. Once a copy of a compressed file has been saved it is safe to delete it from the server.

c. Re-run `syscheck`.

- If the alarm has been cleared, the problem is resolved.
- If the alarm has not been cleared, proceed to 7.

7. Execute the following steps if the file system reported by syscheck is `/tmp`, otherwise skip to 11.
   a. Log into the server generating the alarm as the admusr:

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

   b. Change to the `/tmp` directory:

      ```
      $ cd /tmp
      ```

   c. Confirm that you are in the `/tmp` directory:

      ```
      $ pwd
      /tmp
      ```

   d. When the `pwd` command is executed, if `/tmp` is not output, go back to 5.
   e. Look for possible candidates for deletion:

      ```
      $ ls *.iso *.bz2 *.gz *.tar *.tgz *.zip
      ```

   f. If any files that can be deleted exist, the output of the `ls` will show them. For each of the files listed, execute the `rm` command to delete the file:

      ```
      $ sudo rm <filename>
      ```

   g. Run `syscheck`.
      - If the alarm is cleared, the problem is solved.
      - If the alarm is not cleared, go to the next step.
   h. Upon a reboot the system will clean the `/tmp` directory.

      To reboot the system, issue the following command:

      ```
      $ sudo shutdown -r now
      ```

   i. Re-run `syscheck`.
      - If the alarm has been cleared, the problem is resolved.
      - If the alarm has not been cleared, proceed to the next step.
8. Execute the following steps if the file system reported by syscheck is `/var`, otherwise skip to 11.
   a. Log into the server generating the alarm as the admusr:

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

   b. Change to the `/var/tmp` directory:

      ```
      $ cd /var/tmp
      ```

c. Confirm that you are in the `/var/tmp` directory:

```
$ pwd
/var/tmp
```

d. When the `pwd` command is executed, if `/var/tmp` is not output, go back to 6.

e. Since all files in this directory can be safely deleted, execute the `rm *` command to delete all files from the directory:

```
$ sudo rm -i *
```

f. Re-run `syscheck`.

- If the alarm is cleared, the problem is solved.
- If the alarm is not cleared, go to 11.

9. Execute the following steps if the file system reported by syscheck is /var/TKLC, otherwise skip to 11.

a. Log into the server generating the alarm as the admusr:

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

b. Change to the `/var/TKLC/upgrade` directory:

```
$ cd /var/TKLC/upgrade
```

c. Confirm that you are in the `/var/TKLC/upgrade` directory:

```
$ pwd
/var/TKLC/upgrade
```

d. When the `pwd` command is executed, if `/var/TKLC/upgrade` is not output, go back to 6.

e. Since all files in this directory can be safely deleted, execute the `rm *` command to delete all files from the directory:

```
$ sudo rm -i *
```

f. Run `syscheck`.

- If the alarm is cleared, the problem is solved.
- If the alarm is not cleared, go to 11.

10. For any other file system, execute the following command, where `<mountpoint>` is the file system's mount point:

```
$ sudo find <mountpoint> -type f -exec du -k {} \; | sort -nr > /tmp/
file_sizes.txt
```

This will produce a list of files in the given file system sorted by file size in the file `/tmp/file_sizes.txt`.

> **Note:**
>
> The `find` command noted above could possibly take a few minutes to complete if the given mountpoint contains many files.

Do not delete any file unless you know for certain that it is not needed. Continue to 11 .

11. Run `savelogs` to gather all application logs (see Saving Logs Using the EPAP **GUI**).
12. Run `savelogs_plat` to gather system information for further troubleshooting, (see Saving Logs Using the EPAP **GUI**), and contact My Oracle Support.
13. Run syscheck in Verbose mode.
14. Contact My Oracle Support.

4.5.12 32313 3000000000002000 - Server Default Route Network Error

Alarm Type: TPD

Description: 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 is occurring.

> **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.

Severity: Major

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.14

Alarm ID: TKSPLATMA143000000000002000

Recovery

1. Run `syscheck` in Verbose mode.

   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 4.

   - `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 4.

- `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 5.

2. Run `syscheck` in Verbose mode.

   If the output should indicates:

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

   Go to 3, otherwise go to 4.

3. Perform the these substeps:

   a. Verify the network cables are firmly attached to the server, network switch, router, 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. If the alarm is cleared, the problem is resolved.

4. 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 server with username `epapconfig`.

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

   ```
   MPS Side A:  hostname: mpsa-d1a8f8  hostid: 80d1a8f8
                Platform Version: x.x.x-x.x.x
                Software Version: EPAP x.x.x-x.x.x
                Wed Jul 17 09:51:47 EST 2002
    /-------EPAP 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 | PDB Configuration Menu            |
|----|-----------------------------------|
|  9 | Security                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
|  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 Sync Network               |
|----|--------------------------------------|
|  3 | Configure DSM Network                |
|----|--------------------------------------|
|  4 | Configure Backup Provisioning Network |
|----|--------------------------------------|
|  5 | Configure Forwarded Ports            |
|----|--------------------------------------|
|  6 | Configure Static NAT Addresses       |
|----|--------------------------------------|
|  7 | Configure Provisioning VIP Addresses |
|----|--------------------------------------|
|  e | Exit                                 |
\-------------------------------------------/
Enter choice:  1
```

d. Enter option `1`, `IPv4 Configuration` (or `2` for `IPv6 Configuration`), from the Configure Provisioning Network Menu.

```
MPS Side A:  hostname: EPAP17  hostid: f80a110f
             Platform Version: 6.0.2-7.0.3.0.0_86.45.0
             Software Version: EPAP 161.0.28-16.1.0.0.0_161.28.0
             Wed Jun 15 01:33:56 EDT 2016

/-----Configure Provisioning Network Menu-\
/-----------------------------------------\
|  1 | IPv4 Configuration                 |
|----|------------------------------------|
|  2 | IPv6 Configuration                 |
|----|------------------------------------|
|  e | Exit                               |
\-----------------------------------------/

Enter Choice:  1
```

e. The following warning is displayed. Type `Y` and press **Enter**.

```
EPAP software and PDBA are running. Stop them? [N]  Y
```

f. The EPAP A provisioning network **IP** address is displayed.

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

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

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

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

i. After you have verified or corrected the `Provisioning Network configuration information`, enter `e` to return to the Configure Network Interfaces Menu.

j. Enter `e` again to return to the EPAP Configuration Menu.

k. Go to 6.

5. Perform the following substeps to reboot the server if the `syscheck` output indicates the following error. Otherwise, go to 6:

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

a. Log in as `epapconfig` on the server console.

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

```
 /-------EPAP 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 | PDB Configuration Menu            |
|----|-----------------------------------|
|  9 | Security                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/
Enter Choice:  6
```

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

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

```
MPS Side A:  hostname: EPAP17  hostid: f80a110f
             Platform Version: 6.0.2-7.0.3.0.0_86.45.0
             Software Version: EPAP 161.0.28-16.1.0.0.0_161.28.0
             Wed Jun 15 01:34:39 EDT 2016

/-----EPAP Platform Menu-\
/-------------------------\
|  1 | Initiate Upgrade   |
|----|--------------------|
|  2 | Reboot MPS         |
|----|--------------------|
|  3 | MySQL Backup       |
```

```
|----|--------------------|
|  4 | RTDB Backup        |
|----|--------------------|
|  5 | PDB Backup         |
|----|--------------------|
|  e | Exit               |
\-------------------------/


Enter Choice:  2
Reboot MPS A, MPS B or BOTH? [BOTH]:  A
Reboot local MPS...
```

c. Wait for the reboot to complete.

d. Go to 6.

6. Run `syscheck`.
   - If the alarm is cleared, the problem is resolved.
   - If the alarm is not cleared, go to the next step.
7. Contact My Oracle Support with the `syscheck` output collected in the previous steps.
8. Run `savelogs` to gather all application logs (see Saving Logs Using the EPAP **GUI**).
9. Run `savelogs_plat` to gather system information for further troubleshooting (see Saving Logs Using the EPAP **GUI**), and contact My Oracle Support.
10. Run `syscheck` in Verbose mode.

    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 4.

    - `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, contact My Oracle Support.

    - `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, contact My Oracle Support.
11. Perform the following substeps when `syscheck` Verbose output indicates:

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

a. Verify the network cables are firmly attached to the server, network switch, router, 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. Rerun syscheck:

- If the alarm has been cleared, the problem is solved.
- If the alarm has not been cleared, contact My Oracle Support.

12. Contact My Oracle Support.

4.5.13 32314 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 (see the following table). If it is too hot, lower the temperature in the room to an acceptable level.

Table 4-2 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 (see Running the System Health Check).
   - 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 My Oracle Support.

4.5.14 32315 3000000000008000 – Server Mainboard Voltage Error

Alarm Type: TPD

Description: This alarm indicates that one or more of the monitored voltages on the server mainboard have been detected to be out of the normal expected operating range.

Severity: Major

OID: TpdMainboardVoltageErrorNotify 1.3.6.1.4.1.323.5.3.18.3.1.2.16

Alarm ID: TKSPLATMA163000000000008000

Recovery

- Contact My Oracle Support.

4.5.15 32317 3000000000020000 - Server Disk Health Test Error

Alarm Type: TPD

Description: Either the hard drive has failed or failure is imminent.

Severity: Major

OID: TpdDiskHealthErrorNotify 1.3.6.1.4.1.323.5.3.18.3.1.2.18

Alarm ID: TKSPLATMA183000000000020000

Recovery

1. Immediately contact My Oracle Support for assistance with a disk replacement.
2. Perform the recovery procedures for the other alarms that accompany this alarm.
3. If the problem has not been resolved, contact My Oracle Support.

4.5.16 32318 3000000000040000 - Server Disk Unavailable Error

Alarm Type: TPD

Description: 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.

Severity: Major

OID: TpdDiskUnavailableErrorNotify 1.3.6.1.4.1.323.5.3.18.3.1.2.19

Alarm ID: TKSPLATMA193000000000040000

Recovery

- Contact My Oracle Support.

4.5.17 32321 3000000000200000 – Correctable ECC Memory Error

Alarm Type: TPD

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

Severity: Major

OID: TpdEccCorrectableErrorNotify 1.3.6.1.4.1.323.5.3.18.3.1.2.22

Alarm ID: TKSPLATMA223000000000200000

Recovery

- No recovery necessary. If the condition persists, contact My Oracle Support to request hardware replacement.

4.5.18 32334 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. My Oracle Support 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 My Oracle Support.

4.5.19 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 My Oracle Support to verify port settings on both the server and the switch.

4.5.20 32336 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 My Oracle Support.

4.5.21 32337 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 My Oracle Support.

4.5.22 32338 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 My Oracle Support.

4.6 Major Application Alarms

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

4.6.1 4000000000000001 - Mate EPAP Unavailable

One EPAP has reported that the other EPAP is unreachable.

Recovery

1. Log in to the EPAP**GUI** (see Accessing the EPAP GUI).
2. View the EPAP status on the banner.
   - If the mate EPAP status is **DOWN**, go to 3 .
   - If the mate EPAP status is **ACTIVE** or **STANDBY**, go to 4.
3. Select the **Select Mate** menu item to change to the mate EPAP.
4. Select **Process Control > Start Software** to start the mate EPAP software.
5. View the EPAP status on the banner.
   - If the mate EPAP status is **ACTIVE** or **STANDBY**, the problem is resolved.
   - If the mate EPAP 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 EPAP Software).
8. If the problem persists, run `savelogs` to gather system information for further troubleshooting (see Saving Logs Using the EPAP **GUI**), and contact My Oracle Support.

4.6.2 4000000000000002 - RTDB Mate Unavailable

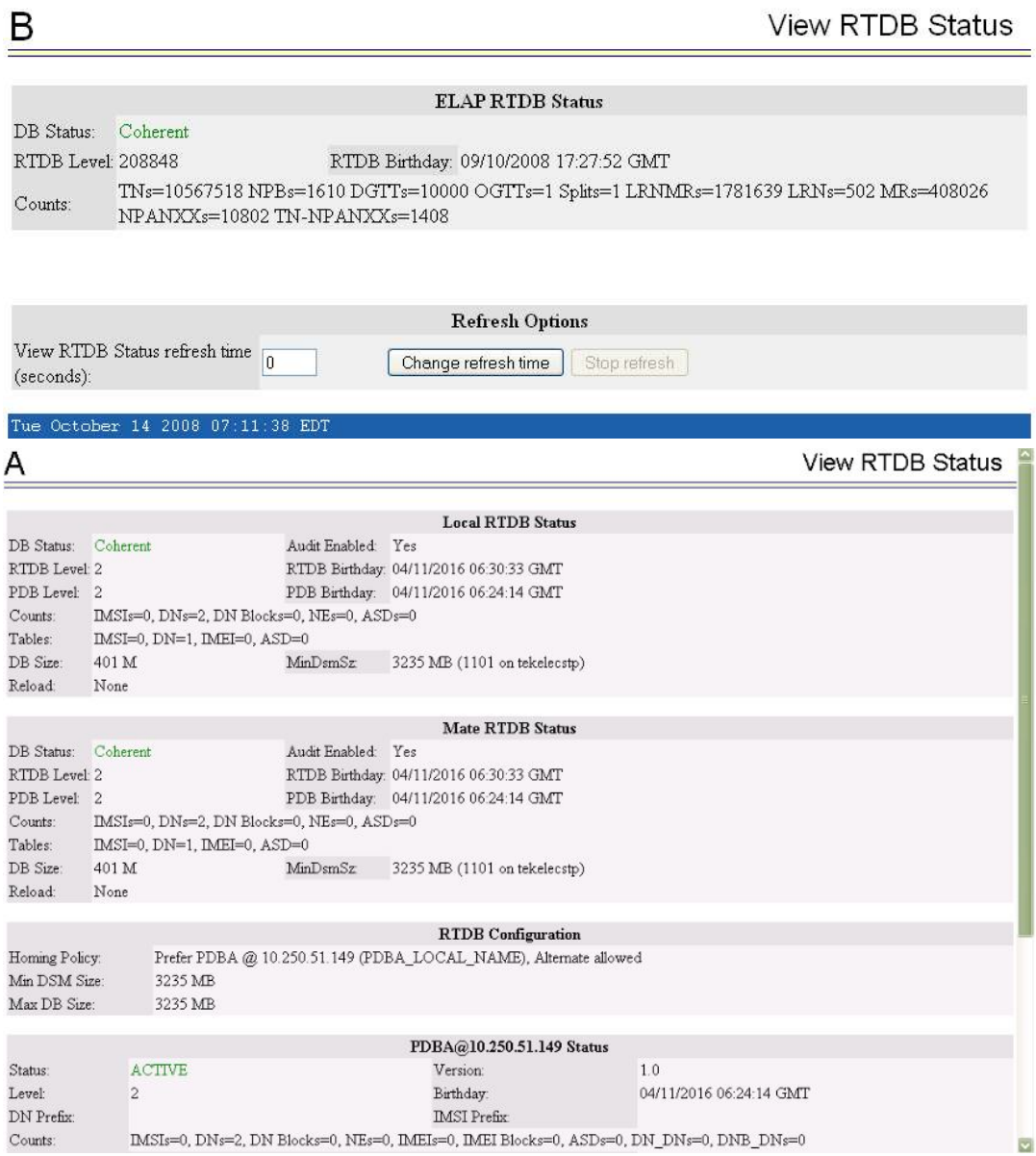
The local EPAP cannot use the direct link to the Standby for RTDB database synchronization.

Recovery

1. Log in to the EPAP**GUI** (see Accessing the EPAP GUI).
2. View the EPAP status on the banner.
   - If the mate EPAP status is **DOWN**, go to 3.
   - If the mate EPAP status is **ACTIVE** or **STANDBY**, go to 4.
3. Select **Process Control > Start Software** to start the mate EPAP software.
4. Select the **Select Mate** menu item to change to the mate EPAP.
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. Make sure 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 EPAP Software).
8. Select **RTDB>View RTDB Status** to verify that the RTDB status on both sides is coherent, as shown in Figure 4-2.

Figure 4-2 Coherent RTDB Status



9. If the problem persists, run `savelogs` to gather system information for further troubleshooting (see Saving Logs Using the EPAP **GUI**), and contact My Oracle Support.

4.6.3 4000000000000004 - Congestion

The EPAP **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 "EPAP Available" notice, capture the log files on both EPAPs (see Saving Logs Using the EPAP **GUI**) and contact My Oracle Support.

4.6.4 4000000000000008 - File System Full

This alarm indicates that the server file system is full.

Recovery

- Call My Oracle Support for assistance.

4.6.5 4000000000000010 - Log Failure

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

- Call My Oracle Support for assistance.

4.6.6 4000000000000020 - RMTP Channels Down

Both **IP** multicast mechanisms are down.

Recovery

1. Check the physical connections between the local server and the **Service Module** cards on the EAGLE.

   Make sure the connectors are firmly seated.
2. Stop and restart the software on the side that is reporting the alarm (see Restarting the EPAP Software).
3. Capture the log files on both EPAPs (see Saving Logs Using the EPAP **GUI**) and contact My Oracle Support.

4.6.7 4000000000000040 - Fatal Software Error

A major software component on the EPAP has failed.

Recovery

1. Restart EPAP software. See Restarting the EPAP Software
2. Capture the log files on both EPAPs (see Saving Logs Using the EPAP **GUI**) and contact My Oracle Support.

4.6.8 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 EPAPs (see Saving Logs Using the EPAP **GUI**) and contact My Oracle Support.

4.6.9 4000000000000100 - RTDB Inconsistent

This message indicates one or more of the following conditions:

- The real-time database for one or more **Service Module** cards is inconsistent with the current real-time database on the Active EPAP fixed disks
- **RTDB**s detect that it is ahead of an **ACTIVE**PDBA that it just connected to (probably a PDBA switchover has occurred, or a restore from a backup of PDB with a previous db level)
- **RTDB** timestamp of most recent level does not match the **PDBA**s record of that timestamp.

Recovery

1. Log in to the User Interface screen of EPAP A (see Accessing the EPAP GUI)
2. Check the banner information above the menu to verify that you are logged into the EPAP A that is reporting the problem.

   If it is necessary to switch to EPAP B, click the **Select Mate** menu item.
3. From the menu, select **RTDB>View RTDB Status** to display status information about the **RTDB**s.

   Figure 4-3 shows an example of two Inconsistent RTDBs.

Figure 4-3 Inconsistent RTDB Status

If one RTDB is inconsistent and the other is coherent in a mated pair setup, proceed to 4. If both RTDBs on an EPAP paired setup are inconsistent, reload from the nearest EPAP site with a coherent RTDB. If all RTDBs are inconsistent, additional steps may be required to reload one RTDB from PDB and backup the new RTDB, then restore the remaining RTDBs.

4. Verify the PDB information on the RTDB Status view is correct before continuing.

5. Before attempting to copy the RTDB, the EPAP A software must be stopped by doing the following:

> **Caution:**
>
> If the software is not stopped as directed in 5.a through 5.c, the RTDB will become corrupted.

   a. Select **Process Control>Stop Software** to stop the software.

      The following warning appears:

```
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).
```

   b. On the **Stop EPAP Software** screen, make sure the following item on the screen is checked: **Check if you want the software to automatically start on reboot.**

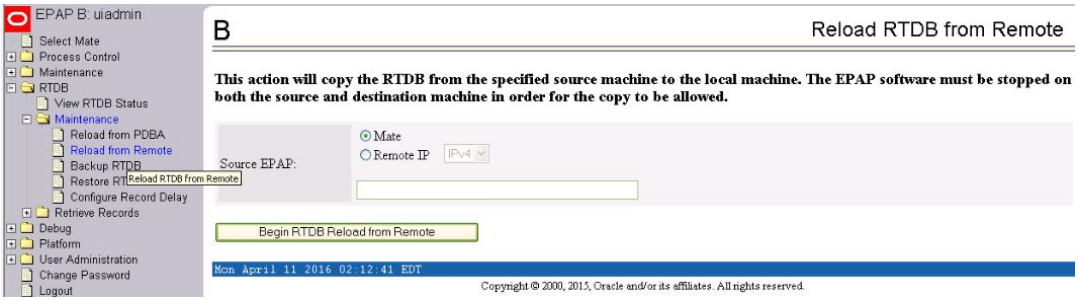
   c. Select the **Stop EPAP Software** button to stop the software.

   d. Select **Select Mate** from the menu to return to the EPAP that is reporting the problem.

6. Select **RTDB>Maintenance>Reload from Remote**.

   The screen shown in Figure 4-6 shows this function.

Figure 4-4 Reload RTDB from Mate EPAP



7. Make sure that the Mate radio button is filled in, as shown in Figure 4-6 and click the **Begin RTDB Reload from Remote** button.

8. Click the **Reload** button as shown in Figure 4-6.

9. When the reload has completed, start the software on EPAP A by doing the following:

   a. Select **Process Control > Start Software** to start the software again.

      Make sure the following item on the screen is checked:

      Check if you want to start the PDBA software along with the EPAP software

   b. Select the **Start EPAP Software** button to start the software.

10. If the problem persists, capture the log files on both EPAPs (see Saving Logs Using the EPAP **GUI**) and contact My Oracle Support.

4.6.10 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 EPAPs (see Saving Logs Using the EPAP **GUI**) and contact My Oracle Support.

4.6.11 4000000000001000 - RTDB 100% Full

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

You may be able to free up space by deleting unnecessary data in the database.

This error can result from one of the following conditions on the EAGLE:

- The EPAP Data Split feature is not ON
- The epap240m STP option is not ON (E5-SM8G-B card required)
- The 120M DN and 120M IMSIs via split database feature is OFF at EPAP and OFF at Eagle
- The 120M DN and 120M IMSIs via split database feature is OFF at EPAP and ON at Eagle

Recovery

1. On the EAGLE, turn ON the optional EPAP Data Split feature to allow more room for the provisioned data.
2. On the EAGLE, turn ON the epap240m STP option (E5-SM8G-B card required) to allow more room for the provisioned data.
3. Turn ON the optional 120M DN and 120M IMSIs via Split database feature on the EPAP and Eagle to allow more room for the provisioned data.
4. Contact My Oracle Support for assistance.

4.6.12 4000000000002000 - RTDB Resynchronization In Progress

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

Recovery

- No further action is necessary.

4.6.13 4000000000004000 - RTDB Reload Is Required

This message indicates that the RTDB reload is required for one of the following reasons:

- The PDB Birthday on the EPAP reporting the error does not match the mate EPAP's PDB Birthday.
- 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 My Oracle Support.

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

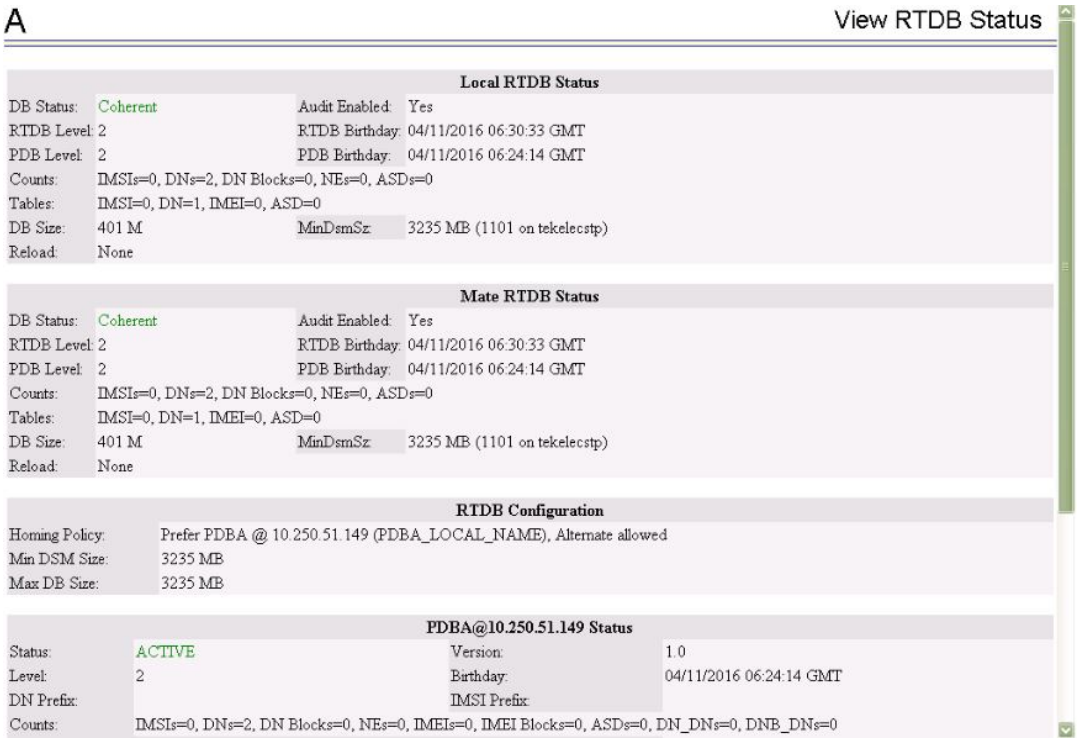
Recovery

1. Log in to the User Interface screen of the EPAP (see 4000000000004000 - RTDB Reload Is Required)
2. Check the banner information above the menu to verify that you are logged into the EPAP that is reporting the problem.

   If it is necessary to switch to the problem **EPAP**, click the **Select Mate** menu item.
3. From the menu, select **RTDB>View RTDB Status** to display status information about the **RTDBs**.

   Figure 4-5 shows an example.

Figure 4-5 RTDB Status



4. If the RTDB birthdays for both the local RTDB and the mate RTDB are the same, you can copy the mate's RTDB to the local RTDB.

   If the RTDB birthdays are not the same, go to step 5.

5. Before attempting to copy the RTDB, you must stop the software on both sides by doing the following:

> **Caution:**
>
> If you do not stop the software on both sides, as directed in substeps 5a through 5c, the **RTDB**s will become corrupted.

   a. Select **Process Control > Stop Software** to stop the software.

      The following warning appears:

```
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).
```

   b. On the **Stop EPAP Software** screen, make sure the following item on the screen is checked:

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

   c. Select the **Stop EPAP Software** button to stop the software.

   d. Select **Select Mate** from the menu.

   e. Repeat substeps 5.a through 5.c on the other side.

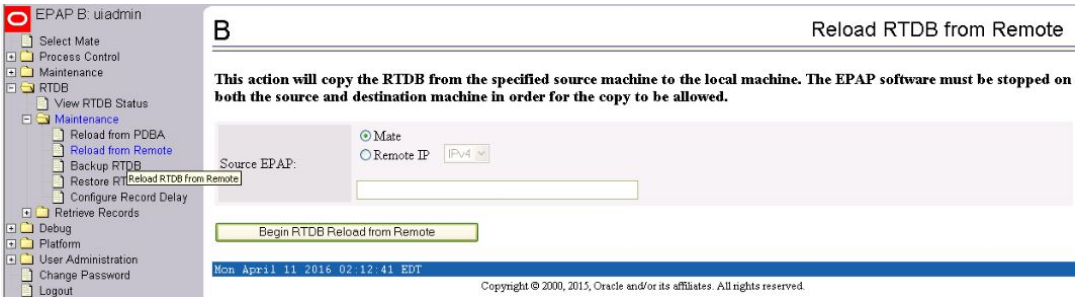
   f. Select **Select Mate** from the menu to return to the EPAP that is reporting the problem.

6. Verify that you are logged in to the side that is reporting the problem.

7. Select **RTDB>Maintenance>Reload from Remote**.

   The screen shown in Figure 4-6 shows this function.

Figure 4-6 Reload RTDB from Mate EPAP



8. Make sure that the Mate radio button is filled in, as shown in Figure 4-6 and click the **Begin RTDB Reload from Remote** button.

9. When the reload has completed, start the software on both sides by doing the following:

   a. Select **Process Control > Start Software** to start the software again.

      Make sure the following item on the screen is checked (this item applies only if performing this procedure on Side A):

      Check if you want to start the PDBA software along with the EPAP software.

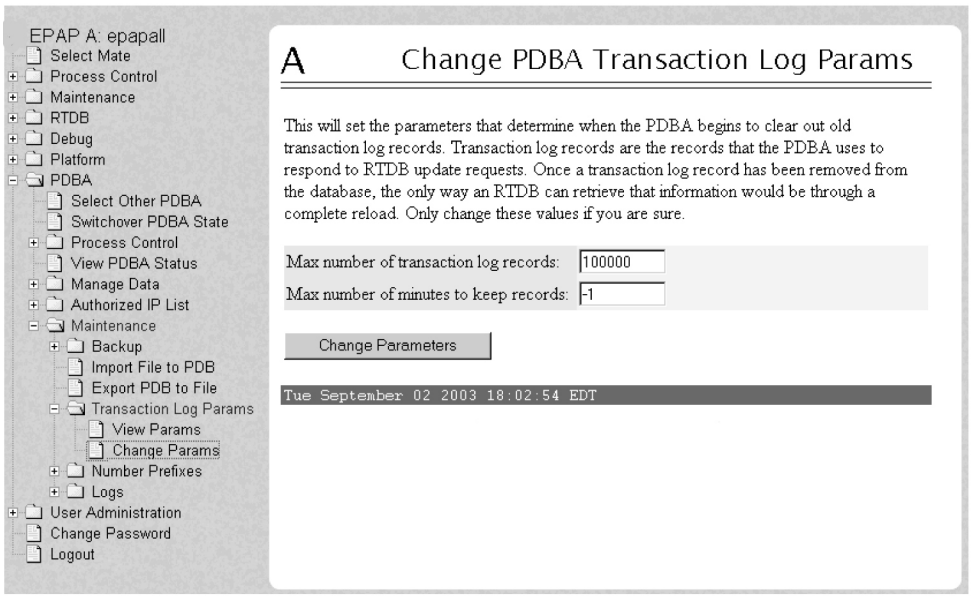
b. Select the **Start EPAP Software** button to start the software.

c. Select **Select Mate** from the menu.

d. Repeat substeps 9.a and 9.b on the other side.

10. If you wish to increase the size of the transaction logs, select **PDBA> Maintenance > Transaction Log Params > Change Params** as shown in Figure 4-7.

Figure 4-7 Changing Transaction Log Parameters



11. If the problem persists, contact My Oracle Support.

4.6.14 4000000000008000 - Mate PDBA Unreachable

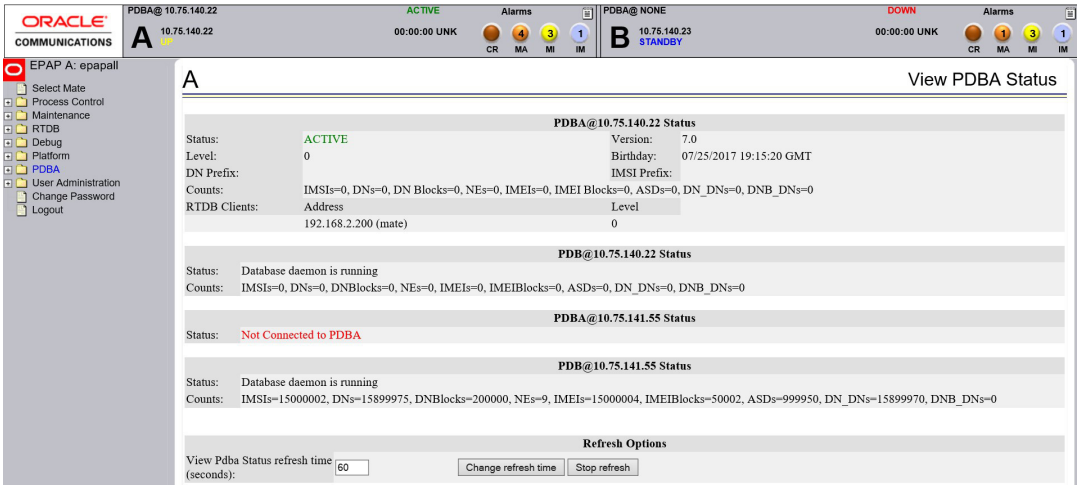
This message indicates that the other PDBA is unreachable.

Recovery

1. Log in to the **User Interface** screen of the EPAP **GUI** (see Accessing the EPAP GUI).
2. Check the banner information above the menu for the PDBA status.
   a. If neither PDBA status is **DOWN**, go to 3.
   b. If status of one of the **PDBA**s is **DOWN**, continue with 4.

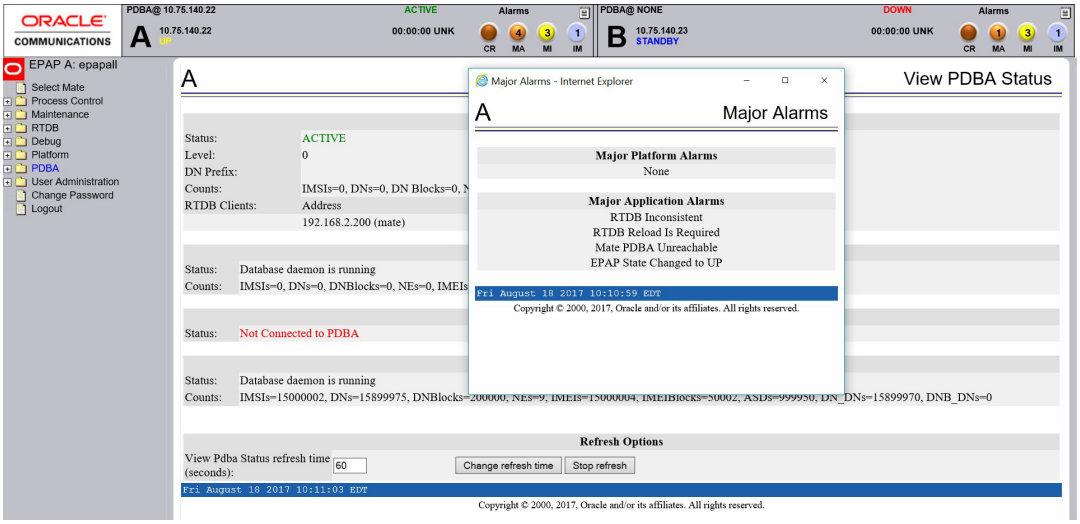
   Figure 4-8 shows an example in which the PDBA on EPAP B is **DOWN**.

Figure 4-8 PDBA Down



3. View Tool Tips to verify the alarm and to verify that you are logged into the EPAP whose PDBA is **DOWN**.

Figure 4-9 Alarms Details

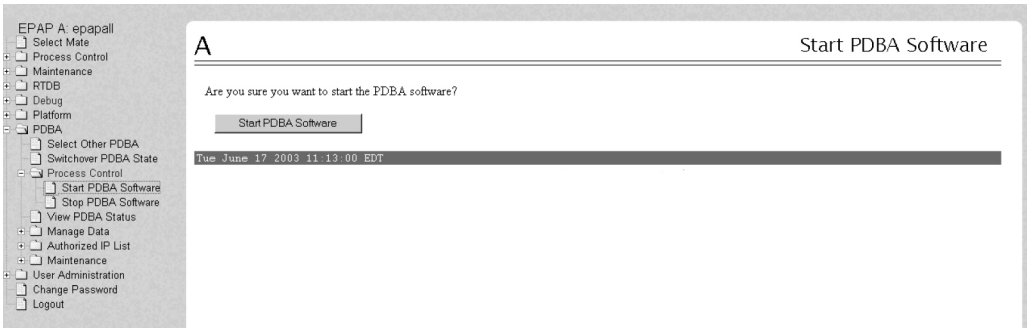


If it necessary to switch to the other PDBA, select PDBA>Select Other PDBA.

4. Attempt to start the PDBA by selecting **PDBA> Process Control > Start** PDBA Software.

The window shown in Figure 4-10 is displayed.

Figure 4-10 Start PDBA



5. Click the **Start PDBA Software** button.
6. When the PDBA software has been started, the window shown in Figure 4-11 displays, and within moments the banner will show the PDBA status as **ACTIVE** or **STANDBY**.

   If the status does not change to **ACTIVE** or **STANDBY**, continue to 7.

Figure 4-11 PDBA Started

7. Check the status of the provisioning network.

   If problems exist in the provisioning network, fix them.
8. If the problem persists, run `savelogs` (see Saving Logs Using the EPAP **GUI**), and contact My Oracle Support.

4.6.15 4000000000010000 - PDBA Connection Failure

The local EPAP RTDB process cannot connect to the local PDBA.

Recovery

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

   Select **Select Mate** if necessary to switch to the problem EPAP.
3. Perform Restarting the EPAP and PDBA.
4. Select **RTDB>View RTDB Status** and determine the homing policy for the PDBA.

   In the example shown in Figure 4-12, the Homing Policy shows that the Standby PDB is preferred for homing.

Figure 4-12 Determining the Homing Policy

5. At the EPAP indicated by the Homing Policy, repeat 3 and 5 to restart the PDBA.
6. If the problem persists, run `savelogs` (see Saving Logs Using the EPAP **GUI**), and contact My Oracle Support.

4.6.16 4000000000020000 - PDBA Replication Failure

Provisioning data is no longer being exchanged from the Active **PDB** to the Standby **PDB**.

1. Run `savelogs` (see Saving Logs Using the EPAP **GUI**).
2. Contact My Oracle Support.

4.6.17 4000000000040000 - RTDB DSM Over-Allocation

At least one **Service Module** card in the attached EAGLE has insufficient memory to provision the **RTDB** entry. No more provisioning will be allowed to the **RTDB** until this issue is resolved.

Recovery

1. Install Service Module cards in the attached EAGLE with sufficient memory to accommodate the expected size of the RTDB.
2. Contact My Oracle Support for assistance.

4.6.18 4000000000080000 - RTDB Maximum Depth Reached

For ELAP 7.0 or earlier, this alarm indicates that the maximum depth has been reached for a tree. If the alarm was initiated during a data update, the update will continually fail until there is manual intervention. RTDB data is stored as inverse tree structures. The trees have a maximum depth allowed.

This alarm indicates that the maximum depth has been reached for a tree. If the alarm was initiated during a data update, the update will continually fail until there is manual intervention. RTDB data is stored as inverse tree structures. The trees have a maximum depth allowed.

Recovery

- Contact My Oracle Support.

4.6.19 4000000000100000 - No PDBA Proxy to Remote PDBA Connection

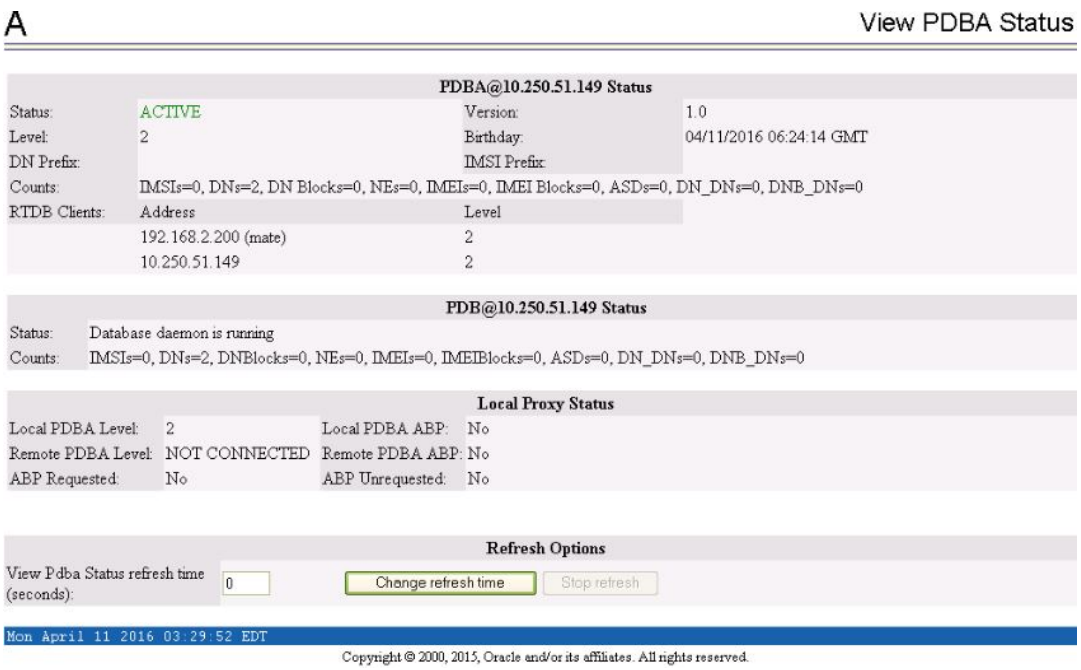
This message indicates that the PDBA Proxy feature is disabled or the software is down.

Recovery

1. Log in to the User Interface screen of EPAP A (see Accessing the EPAP GUI)
2. Refer to the **LNP** *Database Synchronization Manual* for the correct procedures.
3. Select **PDBA>View PDBA Status** to verify that the PDBA proxy feature is enabled.

   The Local Proxy Status items only appear if the PDBA Proxy feature is enabled (See Figure 4-13).

Figure 4-13 View PDBA Status Screen



4. Refer to Restarting the EPAP and PDBA to restart the PDBA.
5. If the problem persists, capture the log files on both EPAPs (see Saving Logs Using the EPAP **GUI**) and contact My Oracle Support.

4.6.20 4000000000200000 - DSM Provisioning Error

A coherent **SM RTDB** is more than 1000 levels behind the **EPAP RTDB**.

Recovery

- Monitor this situation.

  If it does not improve, contact My Oracle Support for guidance.

4.6.21 4000000000800000 - EPAP State Changed to UP

The standby EPAP state was changed from STANDBY to UP.

Recovery

1. Restart the EPAP software.

   See Restarting the EPAP Software.

2. If the standby EPAP state is not changed back to STANDBY, capture the log files on both EPAPs (see Saving Logs Using the EPAP **GUI**) and contact My Oracle Support.

4.6.22 4000000004000000 - RTDB Overallocated

At least one Service Module card in the attached EAGLE has insufficient memory to provision the RTDB entry. No more provisioning will be allowed to the RTDB until this issue is resolved.

This error can result from one of the following conditions on the EAGLE:

- The EPAP Data Split feature is not ON
- The epap240m STP option is not ON (E5-SM8G-B card required)
- The 120M DN and 120M IMSIs via split database feature is OFF at EPAP and OFF at Eagle
- The 120M DN and 120M IMSIs via split database feature is OFF at EPAP and ON at Eagle

Recovery

1. On the EAGLE, turn ON the optional EPAP Data Split feature to allow more room for the provisioned data.
2. On the EAGLE, turn ON the epap240m STP option (E5-SM8G-B card required) to allow more room for the provisioned data.
3. Turn ON the optional 120M DN and 120M IMSIs via Split database feature on the EPAP and Eagle to allow more room for the provisioned data.
4. Contact My Oracle Support for assistance.

4.6.23 4000000020000000 - Mysql Lock Wait Timeout Exceeded

If MySQL is not able to get a lock to write to the PDB table, then an alarm is raised after 15 minutes when the lock wait timeout is exceeded.

Occasionally, a transaction can hang for a longer time, particularly in a multi-threaded environment, and also due to some underlying hardware failure on the disk, kernel bugs, and so on.

Recovery

Restart the PDB software.

4.7 Minor Platform Alarms

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

4.7.1 32500 5000000000000001 – Server Disk Space Shortage Warning

Alarm Type: TPD

Description: 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.

Severity: Minor

OID: 1.3.6.1.4.1.323.5.3.18.3.1.3.1

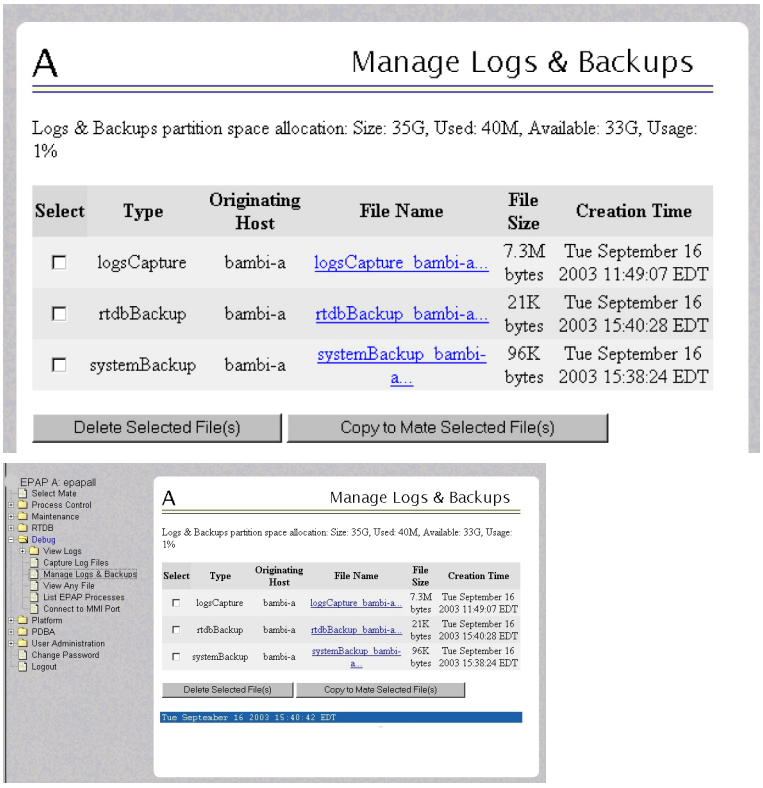
Alarm ID: TKSPLATMI15000000000000001

Recovery

1. Examine the syscheck output to determine if the file system `/var/TKLC/epap/free/var/TKLC/elap/free` is low on space. If so, continue to step 2a; otherwise skip to step 3.
2. Delete unnecessary files, as follows, to free up space on the free partition:
   a. Log in to the EPAP **GUI** (see Accessing the EPAP GUI)
   b. Select **Debug>Manage Logs & Backups**.

      A screen similar to Figure 4-14 displays. This screen displays the information about the total amount of space allocated for, and the amount of space currently used by logs and backups, and it lists logs and backup files that you might choose to delete, freeing up additional disk space.

Figure 4-14 Manage Logs and Backups



c. Click the checkbox of each file that you want to delete and then click **Delete Selected File(s)**.

3. Contact My Oracle Support, and provide the system health check output.

4.7.2 32501 5000000000000002 – Server Application Process Error

Alarm Type: TPD

Description: 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.

Severity: Minor

OID: 1.3.6.1.4.1.323.5.3.18.3.1.3.2

Alarm ID: TKSPLATMI25000000000000002

Recovery

1. Run syscheck in verbose mode (see procedure Run Syscheck Manually)
2. Contact My Oracle Support, and provide the system health check output.
3. Contact My Oracle Support.
4. If a 32305 3000000000000020 - Server Platform Process Error alarm is also present, execute the recovery procedure associated with that alarm before proceeding.
5. Log in to the User Interface screen of the EPAP**GUI** (see Accessing the EPAP GUI)
6. Check the banner information above the menu to verify that you are logged into the problem EPAP indicated in the **UAM**.

If it is necessary to switch to the other side, select **Select Mate**.

7. Open the Process Control folder, and select the **Stop Software** menu item.
8. Open the Process Control folder, and select the **Start Software** menu item.
9. Capture the log files on both EPAPs (see Saving Logs Using the EPAP **GUI**) and contact My Oracle Support.

4.7.3 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 My Oracle Support for assistance.

4.7.4 32506 5000000000000040 – Server Default Router Not Defined

Alarm Type: TPD

Description: 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.

Severity: Minor

OID: 1.3.6.1.4.1.323.5.3.18.3.1.3.7

Alarm ID: TKSPLATMI75000000000000040

Recovery

1. Run syscheck in verbose mode (see procedure Running the System Health Check).
2. Contact My Oracle Support, and provide the system health check output.
3. 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 server with username `epapconfig` (see Accessing the EPAP GUI).

      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 server that is reporting the problem. In the following example, it is server A.

c. Enter option `2`, `Configure Network Interfaces Menu`, from the EPAP `Configuration Menu`.

```
MPS Side A:  hostname: mpsa-d1a8f8  hostid: 80d1a8f8
             Platform Version: x.x.x-x.x.x
             Software Version: EPAP x.x.x-x.x.x
             Wed Jul 17 09:51:47 EST 2002
 /-------EPAP 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 | PDB Configuration Menu            |
|----|-----------------------------------|
|  9 | Security                          |
|----|-----------------------------------|
| 10 | SNMP Configuration                |
|----|-----------------------------------|
| 11 | Configure Alarm Feed              |
|----|-----------------------------------|
| 12 | Configure Query Server            |
|----|-----------------------------------|
| 13 | Configure Query Server Alarm Feed |
|----|-----------------------------------|
| 14 | Configure SNMP Agent Community    |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/
Enter Choice:  2
```

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

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

```
MPS Side A:  hostname: EPAP17  hostid: f80a110f
             Platform Version: 6.0.2-7.0.3.0.0_86.45.0
             Software Version: EPAP 161.0.28-16.1.0.0.0_161.28.0
             Wed Jun 15 01:33:55 EDT 2016

/-----Configure Network Interfaces Menu----\
/-------------------------------------------\
|  1 | Configure Provisioning Network       |
```

```
|----|---------------------------------------|
|  2 | Configure Sync Network                |
|----|---------------------------------------|
|  3 | Configure DSM Network                 |
|----|---------------------------------------|
|  4 | Configure Backup Provisioning Network |
|----|---------------------------------------|
|  5 | Configure Static NAT Addresses        |
|----|---------------------------------------|
|  6 | Configure Provisioning VIP Addresses  |
|----|---------------------------------------|
|  e | Exit                                  |
\----------------------------------------/

Enter choice:  1
```

e. Enter option `1`, `IPv4 Configuration` (or option `2`, `IPv6 Configuration`), from the `Configure Network Interfaces Menu`.

```
MPS Side A:  hostname: EPAP17  hostid: f80a110f
             Platform Version: 6.0.2-7.0.3.0.0_86.45.0
             Software Version: EPAP 161.0.28-16.1.0.0.0_161.28.0
             Wed Jun 15 01:33:56 EDT 2016

/-----Configure Provisioning Network Menu-\
/----------------------------------------\
|  1 | IPv4 Configuration                |
|----|-----------------------------------|
|  2 | IPv6 Configuration                |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/

Enter Choice:  1
```

The following warning appears:

```
EPAP software and PDBA are running. Stop them? [N]
```

f. Type `Y` and press Enter.

The EPAP A provisioning network IP address displays:

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

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

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

```
Enter the EPAP provisioning network default router IP Address:
192.168.61.250
```

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

i. After you have verifying or correcting the Provisioning Network configuration information, enter **e** to return to the `Configure Network Interfaces Menu`.

j. Enter **e** again to return to the EPAP Configuration Menu.

4. Run `syscheck` again. If the alarm has not been cleared, go to 6

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

6. Contact My Oracle Support.

4.7.5 32507 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 4-3 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
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. 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 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.
7. If the problem has not been resolved, contact My Oracle Support and provide the system health check output.
8. If the problem has not been resolved, contact My Oracle Support.

4.7.6 32508 5000000000000100 – Server Core File Detected

Alarm Type: TPD

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

Severity: Minor

OID: tpdCoreFileDetectedNotify 1.3.6.1.4.1.323.5.3.18.3.1.3.9

Alarm ID: TKSPLATMI95000000000000100

Recovery

1. Run syscheck in verbose mode.
2. Run `savelogs` to gather system information (see Saving Logs Using the EPAP **GUI**)
3. Contact Customer Care Center.

Note:

There is a special case of heartbeat process aborting and producing core file not as a result of a bug, but as an expected and intentional response of the process to unexpected activity on the network connecting the cluster nodes. Example of such activity could be switch configuration being performed during the time cluster nodes are trying to, or already are coupled together. To recognize such a case, the investigator first needs to find out if the core file was produced by the heartbeat process:

a. Inspect syscheck verbose output, and look for "core" module. The output would be similar to following:

```
     core: Checking for core files.     core: There are core
files on the system:     core:     CORE DIR: /var/TKLC/
core     core:         CORE: core.heartbeat.<pid>
core:         CORE: core.heartbeat.<pid>.bt *     core:
FAILURE:: MINOR::5000000000000100 -- Server Core File Detected
```

There, investigator finds out there is a core file named `core.heartbeat.<pid>`, where <pid> is the process ID of the failed heartbeat process.

b. If heartbeat core file was found, the investigator must get the backtrace of the process from the core file by running command:

```
gdb /usr/lib/hearbeat/heartbeat /var/TKLC/core/
core.heartbeat.<pid>
```

Once in gdb shell, entering `bt`. The output would be similar to the following:

```
(gdb) bt #0 0x00002b872c2c0215 in raise () from /lib64/
libc.so.6 #1 0x00002b872c2c1cc0 in abort () from /lib64/
libc.so.6 #2 0x000000000040b20c in update_ackseq () #3
0x000000000040d225 in send_cluster_msg () #4
0x000000000040d8d7 in send_local_status () #5
0x000000000040da63 in hb_send_local_status () #6
0x00002b872b2733d7 in Gmain_timeout_dispatch (src=0x13b66bc8,
func=0x40da40 , user_data=0x0) at GSource.c:1570 #7
0x00002b872b8bbdb4 in g_main_context_dispatch () from /lib64/
libglib-2.0.so.0 #8 0x00002b872b8bec0d in ?? () from /lib64/
libglib-2.0.so.0 #9 0x00002b872b8bef1a in g_main_loop_run ()
from /lib64/libglib-2.0.so.0 #10 0x000000000040e8de in
initialize_heartbeat () #11 0x000000000040f235 in main ()
```

The investigator is concerned in lines beginning with #0 through #5, where, in the fourth column, after the word "in", are listed function names called within the heartbeat process. If the order of called functions is the same as in the example above (i.e., raise on line #0) then abort, update_ackseq, send_cluster_msg, send_local_status, and hb_send_local_status on line #5, it is likely that the special case occurred. If such a case was recognized, the investigator can safely delete files `/var/TKLC/core/core.heartbeat.<pid>` and `/var/TKLC/core/`

> core.heartbeat.<pid>.bt and then clear the alarm itself by calling alarmMgr - -clear TKSPLATMI9.

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

4.7.7 32509 5000000000000200 – Server NTP Daemon Not Synchronized

Alarm Type: TPD

Description: 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

OID: tpdNTPDeamonNotSynchronizedNotify 1.3.6.1.4.1.323.5.3.18.3.1.3.10

Alarm ID: TKSPLATMI105000000000000200

Recovery

- Contact My Oracle Support.

4.7.8 32511 5000000000000800 – Server Disk Self Test Warning

Alarm Type: TPD

Description: A non-fatal disk issue exists.

Severity: Minor

OID: tpdSmartTestWarnNotify 1.3.6.1.4.1.323.5.3.18.3.1.3.12

Alarm ID: TKSPLATMI125000000000000800

Recovery

- Contact My Oracle Support.

4.7.9 32514 5000000000004000 – Server Reboot Watchdog Initiated

Alarm Type: TPD

Description: This alarm indicates that the hardware watchdog was not strobed by the software and so the server rebooted the server. This applies to only the last reboot and is only supported on a T1100 application server.

Severity: Minor

OID: tpdWatchdogRebootNotify 1.3.6.1.4.1.323.5.3.18.3.1.3.15

Alarm ID: TKSPLATMI155000000000004000

Recovery

- Contact My Oracle Support.

4.7.10 32518 5000000000040000 – Platform Health Check Failure

Alarm Type: TPD

Description: This alarm is used to indicate a syscheck configuration error.

Severity: Minor

OID: tpdPlatformHealthCheckFailedNotify 1.3.6.1.4.1.323.5.3.18.3.1.3.19

Alarm ID: TKSPLATMI195000000000040000

Recovery

- Contact My Oracle Support.

4.7.11 32519 5000000000080000 – NTP Offset Check Failed

Alarm Type: TPD

Description: This minor alarm indicates that time on the server is outside the acceptable range (or offset) from the NTP server. The Alarm message will provide the offset value of the server from the **NTP** server and the offset limit that the application has set for the system.

Severity: Minor

OID: ntpOffsetCheckFailedNotify 1.3.6.1.4.1.323.5.3.18.3.1.3.20

Alarm ID: TKSPLATMI205000000000080000

Recovery

- Contact My Oracle Support.

4.7.12 32520 5000000000100000 – NTP Stratum Check Failed

Alarm Type: TPD

Description: This alarm indicates that NTP is syncing to a server, but the stratum level of the NTP server is outside of the acceptable limit. The Alarm message will provide the stratum value of the NTP server and the stratum limit that the application has set for the system.

Severity: Minor

OID: NtpStratumCheckFailedNotify 1.3.6.1.4.1.323.5.3.18.3.1.3.21

Alarm ID: TKSPLATMI215000000000100000

Recovery

- Contact My Oracle Support.

4.7.13 32529500000020000000 – 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 My Oracle Support.

4.7.14 32530500000040000000 – 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 My Oracle Support.

4.7.15 32531500000080000000– Half Open Socket Warning

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

Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdHalfOpenSocketWarningNotify1.3.6.1.4.1.323.5.3.18.3.1.3.32

Alarm ID: TKSPLATMI325000000080000000

Recovery

- Contact My Oracle Support.

4.7.16 5000000100000000 – Server Upgrade Pending Accept/Reject

Alarm Type: TPD

Description: This alarm is generated if an upgrade is not accepted or rejected after the upgrade.

Severity: Minor

OID: 1.3.6.1.4.1.323.5.3.18.3.1.3.33

Alarm ID: TKSPLATMI33

Alarm Value: 5000000100000000

Recovery

To clear this alarm, the upgrade should be accepted/rejected via the platcfg menu.

4.7.17 5000004000000000 - Platform Data Collection Error

Alarm Type: TPD

Description: Platform Data Collection Error

Severity: Minor

OID: tpdPdcError

Alarm ID: 5000004000000000

Recovery

- Contact My Oracle Support.

4.8 Minor Application Alarms

Minor application alarms involve the EPAP **RMTP** channels, **RTDB** capacity, and software errors.

4.8.1 6000000000000001 - RMTP Channel A Down

Channel A of the **IP** multicast mechanism is not available.

Recovery

1. Check the physical connections between the local EPAPs, and the EPAPs and the **Service Module** cards on the EAGLE. Make sure that the connectors are firmly seated.
2. Run `syscheck` (see Running the System Health Check)

   If you cannot log in, go to 3.
3. Perform Restarting the EPAP Software.
4. Capture the log files on both EPAPs (see Saving Logs Using the EPAP **GUI**")
5. Contact My Oracle Support.

4.8.2 6000000000000002 - RMTP Channel B Down

Channel B of the **IP** multicast mechanism is not available.

Recovery

1. Check the physical connections between the local EPAPs, and the EPAPs and the **Service Module** cards on the EAGLE.

   Make sure the connectors are firmly seated.
2. Run `syscheck` (see Running the System Health Check).

   If you cannot log in, go to 4.
3. Perform Restarting the EPAP Software.
4. Capture the log files on both EPAPs (see Saving Logs Using the EPAP **GUI**).
5. Contact My Oracle Support.

4.8.3 6000000000000008 - RTDB 80% Full

For ELAP 7.0 or earlier, the RTDB on the EPAP or DSM is approaching capacity (80%).

The RTDB on the EPAP or DSM is approaching capacity (80%).

This error can result from one of the following conditions on the EAGLE:

- The EPAP Data Split feature is not ON
- The epap240m STP option is not ON (E5-SM8G-B card required)
- The 120M DN and 120M IMSIs via split database feature is OFF at EPAP and OFF at Eagle
- The 120M DN and 120M IMSIs via split database feature is OFF at EPAP and ON at Eagle

Recovery

1. On the EAGLE, turn ON the optional EPAP Data Split feature to allow more room for the provisioned data.
2. On the EAGLE, turn ON the epap240m STP option (E5-SM8G-B card required) to allow more room for the provisioned data.
3. Turn ON the optional 120M DN and 120M IMSIs via Split database feature on the EPAP and Eagle to allow more room for the provisioned data.
4. Contact My Oracle Support for assistance.

4.8.4 6000000000000010 - Minor Software Error

A minor software error has been detected.

Recovery

1. Run `syscheck`.
2. Contact My Oracle Support.

   Have the system health check data available.

4.8.5 6000000000000020 - Standby PDBA Falling Behind

This is an indication that there is a congestion condition affecting updates to the standby PDBA. The amount of time between an update being committed in the Active PDB and the same update being committed in the Standby PDB has reached an unacceptable level.

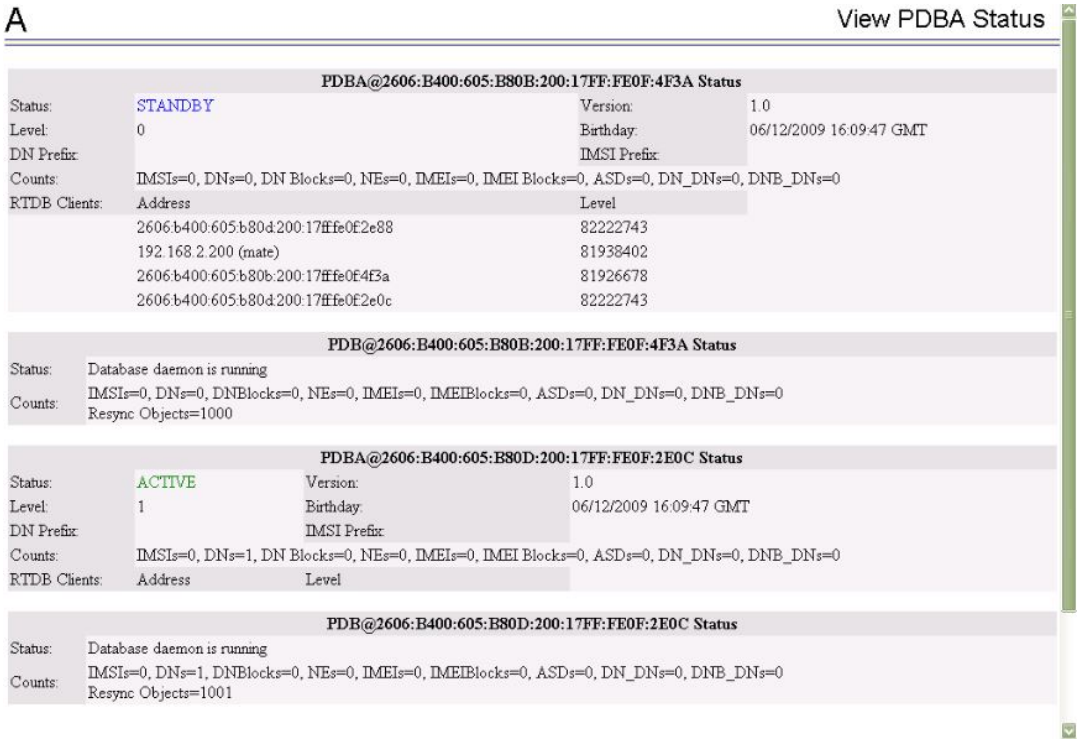
The EPAP attempts to automatically recover from this situation. This error can result from one of the following conditions:

- Provisioning activity is very heavy
- The provisioning network is experiencing errors or latency
- Server maintenance functions (such as backups, restores, imports, exports, etc) are occurring

Recovery

1. Periodically, verify that the level of the standby PDBA is catching up by selecting **PDBA>View** PDBA Status and comparing the Level of the Standby PDBA (on EPAP A in the example shown in Figure 4-15) to the Level of the Active PDBA (on EPAP B in the example).

Figure 4-15 View PDBA Status


A

View PDBA Status

PDBA@2606:B400:605:B80B:200:17FF:FE0F:4F3A Status

Status:	STANDBY	Version:	1.0
Level:	0	Birthday:	06/12/2009 16:09:47 GMT
DN Prefix:		IMSI Prefix:	
Counts:	IMSIs=0, DNs=0, DN Blocks=0, NEs=0, IMEIs=0, IMEI Blocks=0, ASDs=0, DN_DNs=0, DNB_DNs=0		
RTDB Clients:	Address	Level	
	2606:b400:605:b80d:200:17fffe0f2e88	82222743	
	192.168.2.200 (mate)	81938402	
	2606:b400:605:b80b:200:17fffe0f4f3a	81926678	
	2606:b400:605:b80d:200:17fffe0f2e0c	82222743	

PDB@2606:B400:605:B80B:200:17FF:FE0F:4F3A Status

Status:	Database daemon is running
Counts:	IMSIs=0, DNs=0, DNBlocks=0, NEs=0, IMEIs=0, IMEIBlocks=0, ASDs=0, DN_DNs=0, DNB_DNs=0 Resync Objects=1000

PDBA@2606:B400:605:B80D:200:17FF:FE0F:2E0C Status

Status:	ACTIVE	Version:	1.0
Level:	1	Birthday:	06/12/2009 16:09:47 GMT
DN Prefix:		IMSI Prefix:	
Counts:	IMSIs=0, DNs=1, DN Blocks=0, NEs=0, IMEIs=0, IMEI Blocks=0, ASDs=0, DN_DNs=0, DNB_DNs=0		
RTDB Clients:	Address	Level	

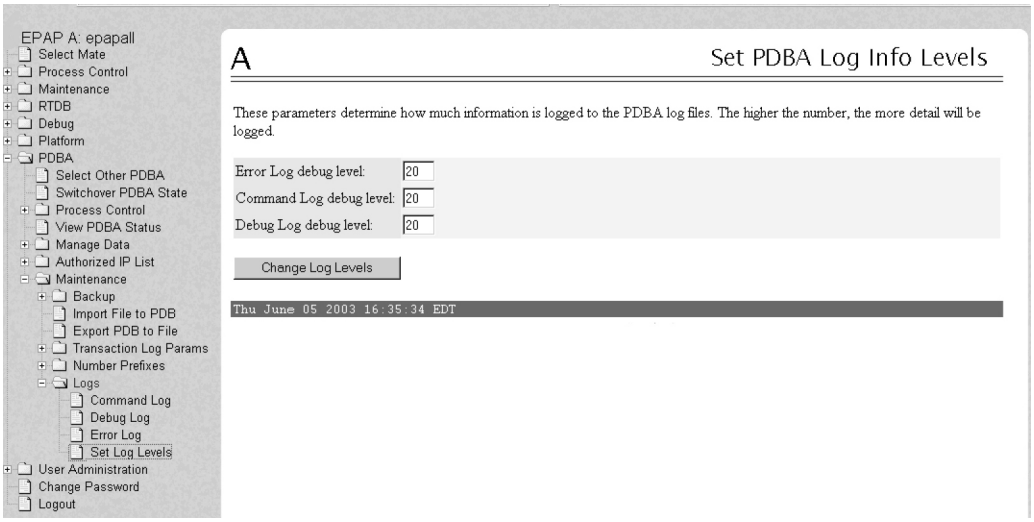
PDB@2606:B400:605:B80D:200:17FF:FE0F:2E0C Status

Status:	Database daemon is running
Counts:	IMSIs=0, DNs=1, DNBlocks=0, NEs=0, IMEIs=0, IMEIBlocks=0, ASDs=0, DN_DNs=0, DNB_DNs=0 Resync Objects=1001

2. If the problem persists for more than two hours, run `savelogs` (see Saving Logs Using the EPAP **GUI**), and contact My Oracle Support for assistance.
3. Login to the User Interface screen of the EPAP **GUI** as any user who has permission to use the **Set Log Levels** menu item.
4. Select **PDBA> Maintenance> Logs> Set Log Levels.**

   The Set PDBA Log Info Levels screen displays, as shown in Figure 4-16.

Figure 4-16 Set PDBA Log Info Levels



5. Verify that the Log Levels match the Log Levels of the MPS on the mated EAGLE STP.

   Figure 4-16 shows the usual settings. Correct log levels if necessary.

6. If adjustments are necessary, it is recommended that the `Command Log debug level` and the `Debug Log debug level` are lowered before adjusting the `Error Log debug level`.

4.8.6 6000000000000040 - RTDB Tree Error

For ELAP 7.0 or earlier, this alarm indicates either that the depth is greater than the theoretical maximum or that some other general problem has been found with a tree. RTDB data is stored as inverse tree structures. The trees have maximum theoretical depths based on the number of records in the tree.

This alarm indicates either that the depth is greater than the theoretical maximum or that some other general problem has been found with a tree. RTDB data is stored as inverse tree structures. The trees have maximum theoretical depths based on the number of records in the tree.

Recovery

- Contact My Oracle Support.

4.8.7 6000000000000080 - PDB Backup failed

The **PDB** backup failed because of at least one of the following conditions:

- A manual backup script was not able to create **PDB** backup successfully
- A **PDB** backup was already in progress when Automatic **PDB** backup attempted to start
- A **PDB** restore was in progress when the Automatic **PDB** backup attempted to start

To verify the exact failure condition, refer to the error string in the log file.

> **Note:**
>
> This alarm will also clear if the Automatic **PDB/RTDB** backup executes successfully during the next scheduled backup time.

Recovery

- To clear this alarm immediately, perform one of the following:
  - Cancel the Automatic **PDB** / **RTDB** backup via the **EPAP GUI** as follows:

    > **Note:**
    >
    > Automatic **PDB** / **RTDB** Backup will have to be rescheduled if it is cancelled.

    1. Log in to the User Interface screen of the EPAP **GUI** (see Accessing the EPAP GUI).
    2. From the menu, select **Maintenance>Automatic PDB/RTDB Backup** to display the automatic backup screen.
    3. From the **Automatic PDB/RTDB Backup** screen, select **None** as the **Backup Type.**
    4. Select the **Schedule Backup** button to complete the cancellation.

       Automatic **PDB**/**RTDB** Backup will have to be rescheduled. Refer to *Administration Guide* to reschedule the Automatic **PDB** / **RTDB** Backup.
  - Perform a manual backup via the **EPAPGUI** (see Backing Up the PDB).

4.8.8 6000000000000100 - Automatic PDB Backup failed

The **PDB** backup failed because of at least one of the following conditions:

- The mate machine was not reachable.
- The **SCP** command to transfer of PDB backup file to mate fails
- The transfer of Automatic PDB Backup to Mate fails
- The transfer of Automatic PDB Backup to mate failed due to disk space shortage on mate
- The remote machine was not reachable
- The connection to remote host failed for **SFTP** of the PDB Backup file
- The SFTP to the remote host failed for Automatic PDB Backup
- The login or password configured for the Remote machine is wrong for the configured user
- The Destination File Path to store the PDB Backup file in Remote machine configured by the user does not exist
- The transfer of the Automatic PDB Backup to the remote failed due to disk space shortage on the remote

To verify the exact failure condition, refer to the error string in the log file.

> **Note:**
>
> This alarm will clear if the Automatic PDB / RTDB backup executes successfully during the next scheduled backup time.

Recovery

To clear this alarm immediately, cancel the Automatic PDB/RTDB backup via the **EPAPGUI**, as described in 1 through 4.

> **Note:**
>
> Automatic PDB/RTDB Backup will have to be rescheduled if it is cancelled.

1. Log in to the User Interface screen of the EPAP GUI (see Accessing the EPAP GUI).
2. From the menu, select **Maintenance>Automatic PDB/RTDB Backup** to display the **Automatic PDB/RTDB Backup** screen.
3. From the **Automatic PDB/RTDB Backup** screen, select **None** as the **Backup Type.**
4. Select the **Schedule Backup** button to complete the cancellation.

> **Note:**
>
> Automatic PDB/RTDB Backup will have to be rescheduled. Refer to *Administration Guide* to reschedule the Automatic PDB/RTDB Backup.

4.8.9 6000000000000200 - RTDB Backup failed

The **RTDB** backup failed because of at least one of the following conditions:

- The manual backup script (backupRtdb.pl) was not able to create RTDB Backup successfully.
- The **EPAP** software could not be successfully stopped in order for Automatic RTDB Backup to start.
- Another user has already stopped the EPAP Software before the script stops the EPAP Software for Automatic RTDB Backup
- Another user is currently stopping the EPAP Software. The Automatic RTDB Backup script cannot stop the EPAP Software.
- The GUI Server returned an error when trying to get a lock from it for Automatic RTDB Backup.
- Not able to connect to GUI server for Automatic RTDB Backup
- The EPAP software was not running when it was to be stopped for Automatic RTDB Backup
- The mate machine is not reachable.

To verify the exact failure condition, refer to the error string in the log file.

> **Note:**
>
> This alarm will clear if the Automatic PDB/RTDB backup executes successfully during the next scheduled backup time.

Recovery

- To clear this alarm immediately, perform one of the following:
  - Cancel the Automatic PDB/RTDB backup in the EPAP GUI.

    > **Note:**
    >
    > Automatic PDB/RTDB Backup will have to be rescheduled if it is cancelled.

    1. Log in to the User Interface screen of the EPAP GUI (see Accessing the EPAP GUI).
    2. From the menu, select **Maintenance>Automatic PDB/RTDB Backup** to display the **Automatic PDB/RTDB Backup** screen.
    3. From the **Automatic PDB/RTDB Backup** screen, select **None** as the **Backup Type.**
    4. Select the **Schedule Backup** button to complete the cancellation. Automatic PDB/RTDB Backup will have to be rescheduled. Refer to *Administration Guide* to reschedule the Automatic PDB/RTDB Backup.
  - Perform a manual backup via the EPAP GUI as described in Backing Up the RTDB.

4.8.10 6000000000000400 - Automatic RTDB Backup failed

The **RTDB** backup failed because of at least one of the following conditions:

- The mate machine is not reachable.
- Automatic **RTDB** Backup file transfer to the Mate failed.
- Unable to connect to Remote host **IP Address** for Automatic RTDB Backup.
- Automatic RTDB Backup file transfer to the Remote failed.
- The incorrect login or password configured for Automatic RTDB Backup.
- The destination path does not exist in remote machine IP Address for Automatic RTDB Backup.

To verify the exact failure condition, refer to the error string in the log file.

> **Note:**
>
> This alarm will clear if the Automatic PDB/RTDB backup executes successfully during the next scheduled backup time.

Recovery

To clear this alarm immediately, cancel the Automatic **PDB** / **RTDB** backup in the EPAP GUI as described in 1 through 4.

> **Note:**
>
> Automatic PDB/RTDB Backup will have to be rescheduled if it is cancelled.

1. Log in to the User Interface screen of the EPAP **GUI** (see Accessing the EPAP GUI).
2. From the menu, select **Maintenance>Automatic PDB/RTDB Backup** to display the **Automatic PDB/RTDB Backup** screen.
3. From the **Automatic PDB/RTDB Backup** screen, select **None** as the **Backup Type.**
4. Select the **Schedule Backup** button to complete the cancellation. Automatic PDB/RTDB Backup will have to be rescheduled. Refer to *Administration Guide* to reschedule the Automatic PDB/RTDB Backup.

4.8.11 6000000000001000 - SSH tunnel not established

One or more SSH tunnels has been enabled in the past, but the cron job was not able to re-establish the SSH tunnel with all of the Authorized PDBA Client IP addresses.

Recovery

- Verify that the Customer Provisioning Application (CPA) machine is up and running.
  - If the CPA machine is not running, restart it and wait for the alarm to clear.
  - If the CPA machine is running, or if the alarm does not clear, contact My Oracle Support.
- If the alarm text is "SSH tunnel down for <IP>", verify that the port specified for SSH tunneling is not in use on the remote machine.

4.8.12 6000000000002000 - RTDB 90% Full

The RTDB on the EPAP is approaching capacity (90%).

This error can result from one of the following conditions on the EAGLE:

- The EPAP Data Split feature is not ON
- The epap240m STP option is not ON (E5-SM8G-B card required)
- The 120M DN and 120M IMSIs via split database feature is OFF at EPAP and OFF at Eagle
- The 120M DN and 120M IMSIs via split database feature is OFF at EPAP and ON at Eagle

Recovery

1. On the EAGLE, turn ON the optional EPAP Data Split feature to allow more room for the provisioned data.
2. On the EAGLE, turn ON the epap240m STP option (E5-SM8G-B card required) to allow more room for the provisioned data.
3. Turn ON the optional 120M DN and 120M IMSIs via Split database feature on the EPAP and Eagle to allow more room for the provisioned data.

4. Contact My Oracle Support for assistance.

4.8.13 6000000000004000 - PDB 90% Full

The PDB on the EPAP has exceeded 90% of purchased capacity.

Recovery

1. Log in to the EPAP CLI as epapdev.
2. Use the manageLicenseInfo utility to check the value of purchased capacity (see the "Current license capacity"):

   ```
   $ manageLicenseInfo -l
   ```

3. Purchase additional provisioning database capacity licenses as needed.
4. Use the manageLicenseInfo utility to specify the additional amount of desired PDB capacity, where "License Capacity value" is the number of additional licenses required when one license supports 0.5M data (DN, IMSI, and IMEI):

   ```
   $ manageLicenseInfo -a <License Capacity value>
   ```

For assistance or additional information, contact My Oracle Support.

4.8.14 6000000000008000 - PDB 80% Full

The PDB on the EPAP has exceeded 80% of purchased capacity.

Recovery

1. Log in to the EPAP CLI as epapdev.
2. Use the manageLicenseInfo utility to check the value of purchased capacity (see the "Current license capacity"):

   ```
   $ manageLicenseInfo -l
   ```

3. Purchase additional provisioning database capacity licenses as needed.
4. Use the manageLicenseInfo utility to specify the additional amount of desired PDB capacity, where "License Capacity value" is the number of additional licenses required when one license supports 0.5M data (DN, IMSI, and IMEI):

   ```
   $ manageLicenseInfo -a <License Capacity value>
   ```

For assistance or additional information, contact My Oracle Support.

4.8.15 6000000000010000 - PDB InnoDB Space 90% Full

The storage space in InnoDB Engine on the EPAP is approaching capacity (90%).

Recovery

1. Purchase additional provisioning database capacity licenses.
2. Contact My Oracle Support.

4.8.16 6000000000040000 - RTDB Client Lagging Behind

This alarm is generated if the RTDB was not up while provisioning was done at the PDB, or if there is latency in the network resulting in RTDBs receiving updates late.

> **Note:**
>
> This alarm may occur during import and should eventually clear when the RTDB process catches up.

Recovery

The provisioning at the PDBs can be stopped until the RTDBs reach the same level.

4.8.17 6000000000080000 - Automatic Backup is not configured

The Automatic Backup is not configured at the PDB only.

Recovery

- Contact My Oracle Support.

4.8.18 6000000000100000 - EPAP QS Replication Issue

The EPAP Query Server is not reachable, not associated, or disconnected from the EPAP.

Recovery

- Contact My Oracle Support.

4.8.19 6000000000200000 - EPAP QS Lagging Behind

The EPAP Query Server is not in synch with the EPAP and is falling behind from a threshold set by the user.

Recovery

- Contact My Oracle Support.

4.8.20 6000000000400000 - License capacity is not configured

The license capacity has never been set or the license capacity is set to 0.

By default, up to 120M can be provisioned if license capacity is not set. To use the EPAP Expansion to 480M Database Entries feature, additional capacity (i.e., Required Capacity - Current Purchased Capacity) must be purchased before adjusting the license capacity using the following procedure. For capacity over 255M, 480G drive modules are required.

Recovery

1. Log in to the EPAP CLI as epapdev.

2. Use the manageLicenseInfo utility to check the value of purchased capacity (see the "Current license capacity"):

   ```
   $ manageLicenseInfo -l
   ```

3. Use the manageLicenseInfo utility to specify the additional amount of desired PDB capacity, where `<License Capacity value>` is the number of additional licenses required when one license supports 0.5M data (DN, IMSI, and IMEI):

   ```
   $ manageLicenseInfo -a <License Capacity value>
   ```

   For example, if 120M is currently provisioned and an additional 80M is desired for a new capacity of 200M, 160 should be specified for the `<License Capacity value>`:

   ```
   manageLicenseInfo -a 160
   ```

For assistance or additional information, contact My Oracle Support.

4.8.21 6000000000800000 - Long wait on write for PDBI update

Customers should complete the following steps in order to raise the "Long Wait on Write for PDBI Update" alarm. This will ensure the user is alerted to a PDBI write connection holding for too long:

1. Issue the uiEdit command

   ```
   "PDBI_LONG_WAIT_ALARM_TIME" <time in seconds>
   ```

   where <time in seconds> is the time value that a PDBI connection is allowed to hold a write connection before triggering the alarm.

2. Investigate the alarm banner on the EPAP GUI for the alarm text "Long wait on write for PDBI update"; or, identify the alarm bit 6000000000800000 from the connected EAGLE; or, find the alarm number 45121 from the SNMP NM server.

3. If the alarm is triggered, find the PDBI connection information by issuing the grep

   ```
   "Throw alarm for connection" pdba.err.*
   ```

   command in the

   ```
   /usr/TKLC/epap/logs
   ```

   directory.

4. Clear the alarm to release the PDBI write connection in question.

4.8.22 6000000001000000 - NE count mismatch between PDB and RTDB

Customer should schedule a cron job in “/etc/cron.d/TS.EXAP” for “/usr/TKLC/appl/bin/checkNEsanity.pl” in order to raise the alarm, when there is count mismatch between PDB and RTDB for Network Entity (NE). This cron will be scheduled only on the server having RTDB, hence don’t schedule the cron on pdbonly server.

Customer can schedule the cron considering the following conditions:

- Cron should be scheduled once in a day.
- Server should not be involved in any other activity at the time when this cron is scheduled, to neglect any impact.
- It will be good to schedule the cron when the provisioning rate is very low or negligible.
- Cron should be scheduled at some specific time of the day when scheduling for once in a day.

For example: To schedule daily once at 05:00 , Sched="daily,1,05:00"

00 05 * * * epapdev /usr/TKLC/appl/bin/checkNEsanity.pl

If the alarm is observed, follow the below mentioned recovery steps:

- When the alarm is observed, savelogs (application logs) is automatically taken for the first time but the customer will have to take the platform logs manually from the platcfg menu. Also, customer can retake the application logs, if more recent logs are needed.
- If we have other RTDBs connected to the same PDB and the DB on them is good, then the customer can restore the backup from one of the other connected RTDBs on this RTDB.
- If all RTDBs connected to the same PDB are show NE mismatch then restore both PDB and RTDB from backup taken from another site having the similar database.
- If the above two options are not feasible, then do a reload from PDB on this RTDB. This will reload the database from scratch on RTDB, from the connected PDB. This process will take time depending upon the total size of the database.

Contact support for any query.

5
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**).

5.1 Introduction

E5-APP-B cards 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 *Unsolicited Alarm and Information Messages Reference*.

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

5.2 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.

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).

5.3 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)

5.4 Removing and Replacing E5-APP-B Cards

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

5.4.1 Removing an E5-APP-B Card

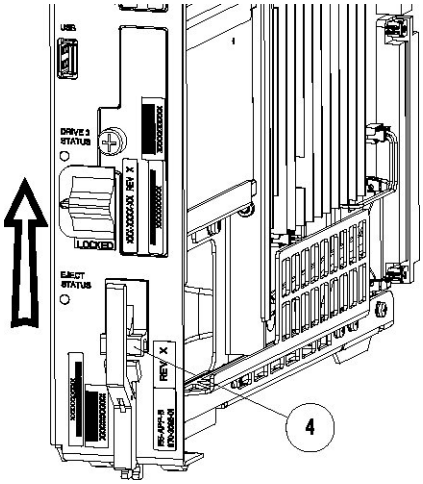
Procedure - Remove E5-APP-B card

> **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 5-1).

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

Figure 5-1 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.

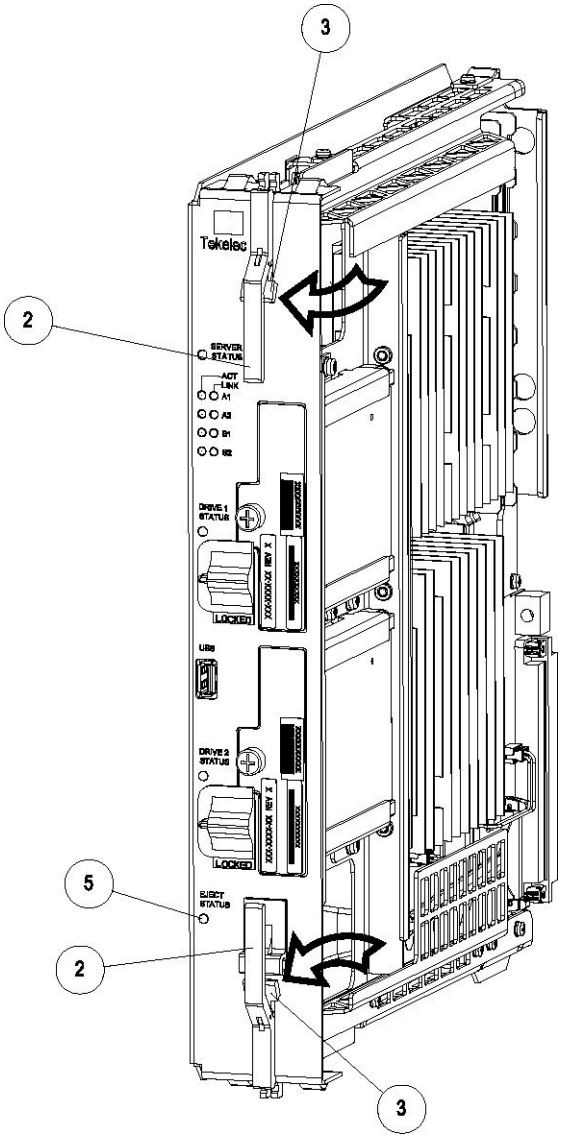
   When the Eject Status LED is steady red, the E5-APP-B card is in shutdown state.

   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 5-2

Figure 5-2 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.

5.4.2 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 5-3 illustrates the angle of the interlocks and levers just before inserting E5-APP-B Card into the EAGLE shelf.

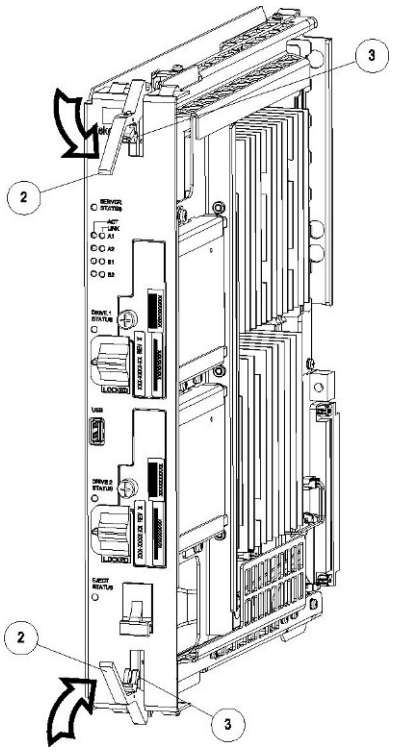
Figure 5-3 E5-APP-B Card UNLOCKED

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 5-4).

Figure 5-4 E5-APP-B Card Inject Levers

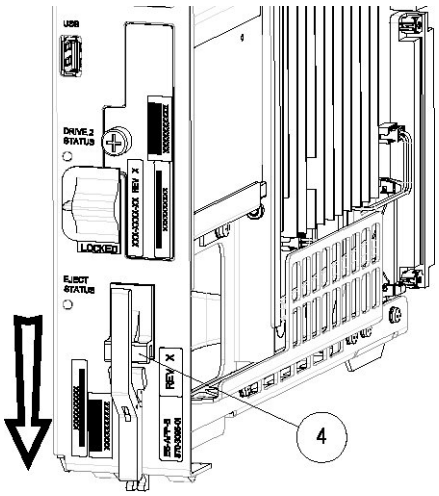


This locks the card in place and ensures a strong connection with the pins on the target shelf backplane.

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

> **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 5-5 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.

5.5 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. The 480G drive modules will support the existing data capacity and no down time is required. To take advantage of the increased storage capacity of the 480G drive modules, EPAP must be re-installed. For information about increasing the existing data capacity after upgrading to 480G drive modules, see Increasing Data Capacity with 480G Drive Modules.

Procedure - Remove and Replace a Drive Module Assembly

1. Log in as admusr and 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]
md1 : active raid1 sdb2[1] sda2[0]
      262080 blocks super 1.0 [2/2] [UU]

md2 : active raid1 sda1[0] sdb1[1]
      292631552 blocks super 1.1 [2/2] [UU]
      bitmap: 2/3 pages [8KB], 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]
md1 : active raid1 sdb2[1]
      262080 blocks super 1.0 [2/1] [_U]

md2 : active raid1 sdb1[1]
      292631552 blocks super 1.1 [2/1] [_U]
      bitmap: 2/3 pages [8KB], 65536KB chunk
```

```
unused devices: <none>
```

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

3. 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.

5.5.1 Removing a Drive Module Assembly

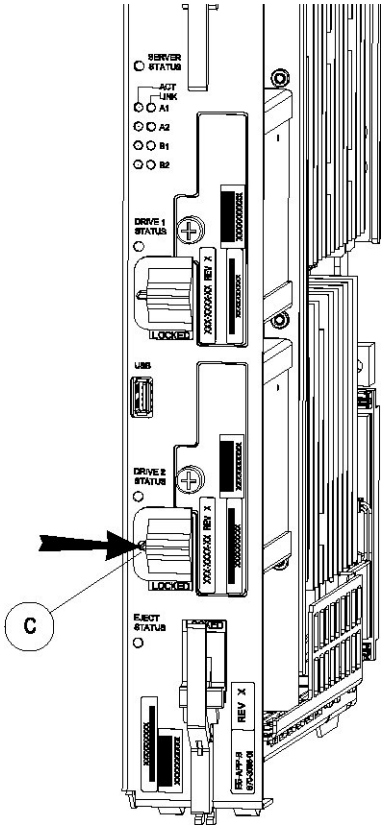
Procedure - Remove Drive Module Assembly

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 5-6.

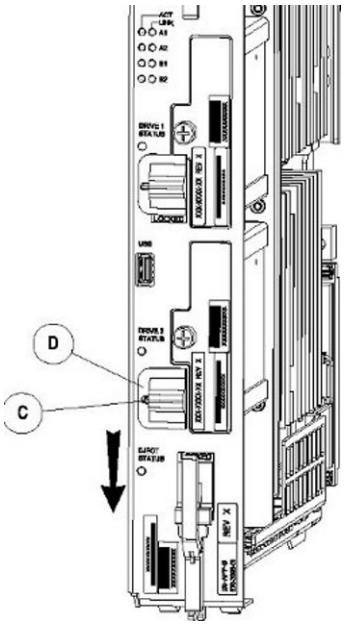
Figure 5-6 Drive Module Released



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 5-7 and Figure 5-8, respectively.

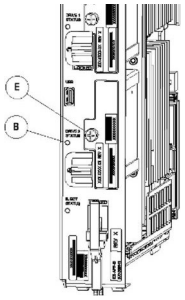
   When drive module locking switch (D) is transitioned from locked to unlocked, the LED will flash red to indicate the drive is unlocked and in process of shutting down.

Figure 5-7 Drive Module UNLOCKED



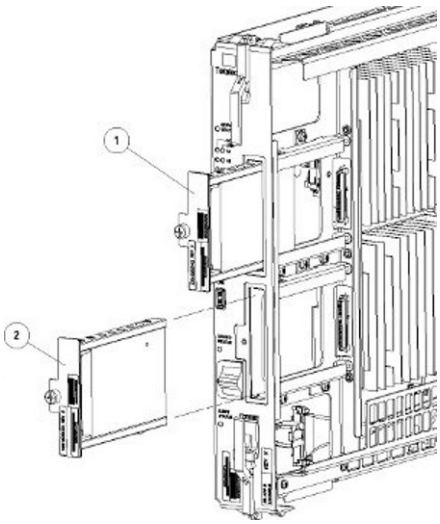
> **Caution:**
>
> Removal of the drive prior to the LED indicating steady red could result in drive corruption.

Figure 5-8 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 5-8).
5. Grasp the screw (E) and pull the drive out slowly until it is free from the card (see Figure 5-9).

Figure 5-9 Drive Module Removal

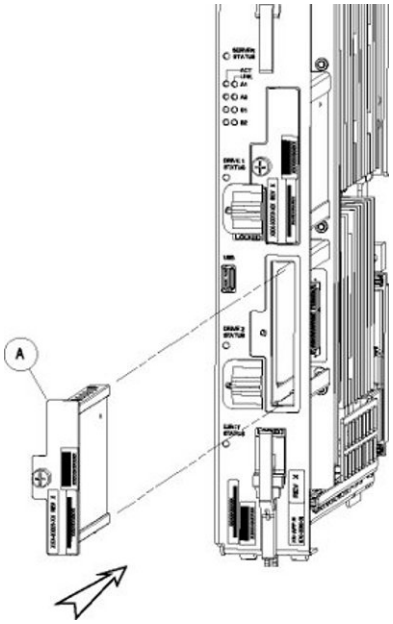


5.5.2 Replacing a Drive Module Assembly

Procedure - Replace Drive Module Assembly

1. Slide a new drive(s) module into the drive slot on the card (see Figure 5-10).

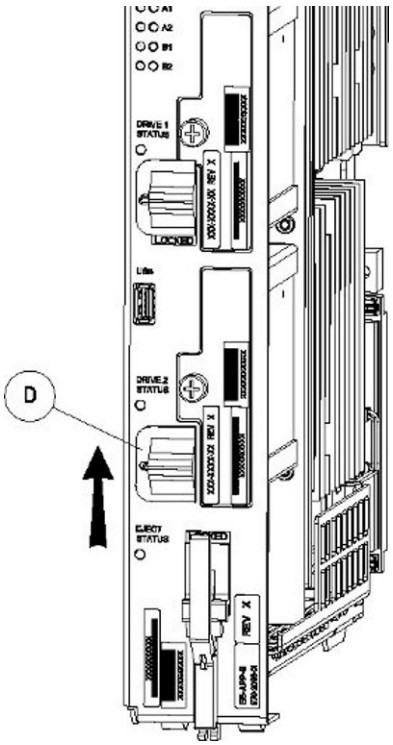
Figure 5-10 Drive Module Replacement



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 5-8).
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 5-11).

Figure 5-11 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>
```

5.6 Increasing Data Capacity with 480G Drive Modules

If 300G drive modules were in use when EPAP was installed, EPAP must be re-installed to take advantage of the additional storage capacity available on 480G drive modules.

Procedure - Increase Data Capacity with 480G Drive Modules

1. Backup the data and configurations of the existing setup.

Perform the following procedures for data backup and configurations:

- **Pre Full Upgrade Steps**
  a. SETTING UP PRE-FULL UPGRADE ENVIRONMENT
  b. CAPTURING CURRENT CONFIGURATIONS
  c. CAPTURING CURRENT CONFIGURATIONS ON STANDALONE EPAP
  d. PRE-FULL UPGRADE CHECK
- **Data Backup before Full Upgrade**
  a. SHUTTING DOWN THE PDBA AND EPAP
  b. DISABLE EPAP VIP AND DEACTIVATE PDBA PROXY FEATURE
  c. STOP ACTIVE PDBA AND VERIFY PDBA REPLICATION STATUS
  d. DISCONNECT REMOTE PDBA
  e. BACKUP EUIDB DATABASE
  f. BACKUP PDB
  g. BACKUP RTDB DATABASE
  h. STOP MYSQL SERVICE
  i. TRANSFER DATABASES TO MATE AND REMOTE

For detailed configurations of these procedures, refer *3.2 Pre Full Upgrade Steps* and *3.3 Data Backup before Full Upgrade* in *Full Upgrade Guide*.

2. If you have not already replaced both 300G drive modules with 480G drive modules, remove the 300G drive modules from the E5-APP-B card.

   See Removing a Drive Module Assembly.

3. If you have not already replaced both 300G drive modules with 480G drive modules, insert the new 480G drive modules.

   See steps 1 through 4 in Replacing a Drive Module Assembly.

4. After the drive modules are successfully replaced, IPM the drive modules with the latest TPD and install EPAP.

   Perform the following procedures for IPM and EPAP installation:

   a. PRE INSTALL CONFIGURATION
   b. EPAP INSTALLATION

   For detailed configurations of these procedures, refer *3.4 IPM and EPAP 16.1 Installation* in *Full Upgrade Guide*.

5. Perform initial configuration and data migration to complete the procedure.

   Perform the following procedures for initial configuration and data migration:

   - **Initial Configuration**
     a. CONFIGURE NETWORK INTERFACE USING PLATCFG UTILITY
     b. CONFIGURE NETWORK INTERFACES
     c. TRANSFER DATABASES
     d. RESTORE EUIDB DATABASE
     e. CONFIGURE PROVISIONING NETWORK

f. VERIFY CONFIGURATIONS
g. CONFIGURE NTP SERVERS
h. POST CONFIGURATION SYSCHECK
i. REBOOT THE MPS

- **Data Migration**
  a. RESTORE PDB
  b. RESTORE AND CONVERT RTDB
  c. VERIFY PDBA AND RTDB ARE IN SYNC
  d. RELOAD RTDB FROM MATE
  e. POINT ACTIVE PDB (2A) TO UPGRADED STANDBY PDB (1A)
  f. SET SPECIFIC RTDB HOMING
  g. POINT STANDBY PDB (1A) TO ACTIVE PDB (2A)
  h. RESTART THE PDBA AND EPAP
  i. UPDATE PDB CONFIGURATION
  j. EXCHANGE KEYS BETWEEN PROVISIONABLE AND NONPROVISIONABLE SERVERS USING SCRIPT
  k. EXCHANGE KEYS BETWEEN PROVISIONABLE AND NONPROVISIONABLE
  l. ENABLE EPAP PDBA PROXY AND EPAP VIP OPTIONAL FEATURES
  m. CONFIGURE THE AUTO BACKUP
  n. SWITCHOVER PDBA
  o. CHECK REPLICATION BETWEEN ACTIVE AND STANDBY PDBA

For detailed configurations of these procedures, refer to *3.5 Initial Configuration on EPAP* and *3.6 Data Migration* in *Full Upgrade Guide*.

A
General Procedures

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

A.1 Accessing the EPAP GUI

EPAP supports a web-based Graphical User Interface (GUI) based on the client-server paradigm. The front end appears on an Internet browser, and the back end operates on the platform. For details about the EPAP GUI setup and login, see *EAGLE Application Processor Administration Guide*. Microsoft Internet Explorer® version 11 is supported and certified for use with the EPAP Graphical User Interface (GUI). Other browsers may be partially compatible with the EPAP GUI. When using these browsers, the following message may be displayed when logging in to the EPAP GUI:

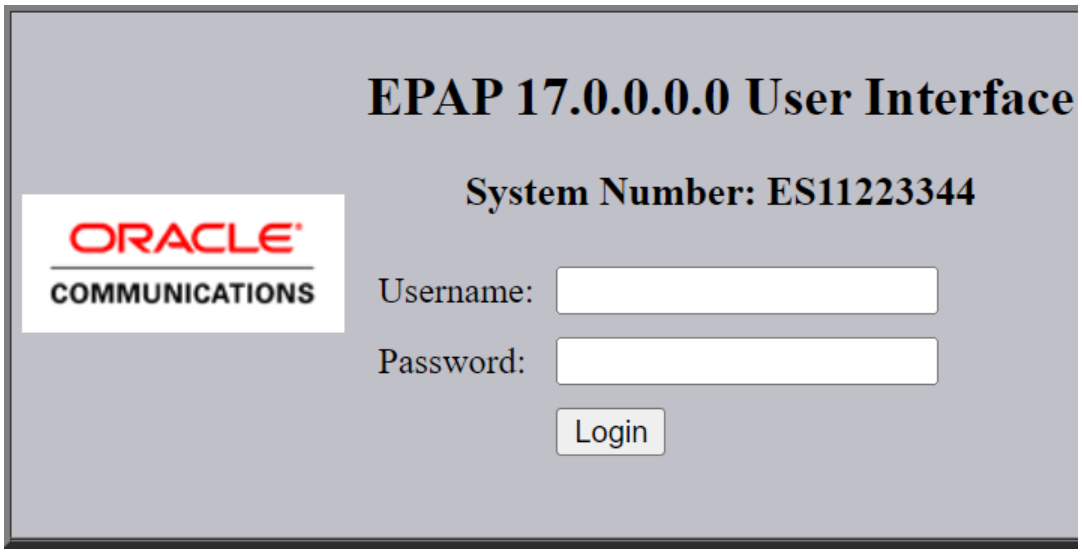
```
CAUTION: The User Interface may not function correctly with the browser you
are using.
```

Use the following procedure to access the main screen of the EPAP GUI:

1. Enter the IP address of the EPAP application in the browser URL field.

   The login screen shown in Figure A-1 appears.

Figure A-1 EPAP User Interface Screen



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 *EAGLE Application Processor Administration Guide*.

Table A-1 Usernames

EPAP GUI Login Name	Access Granted
epapmaint	Maintenance menu and all sub menus
epappdba	Database menu and all sub menus
epapdebug	Debug menu and all sub menus
epapplatform	Platform menu and all sub menus
uiadmin	User Administration menu
epapall	All of the menus in this Table

3. Continue with the procedure that invoked this procedure.

A.2 Accessing the EPAP Text Interface

The EPAP text-based user interface is accessed through the Local Access Terminal. The text-based user interface is used for initial configuration of the EPAP 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 EPAP application, refer to *Administration Guide*.

A.3 Restarting the EPAP and PDBA

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

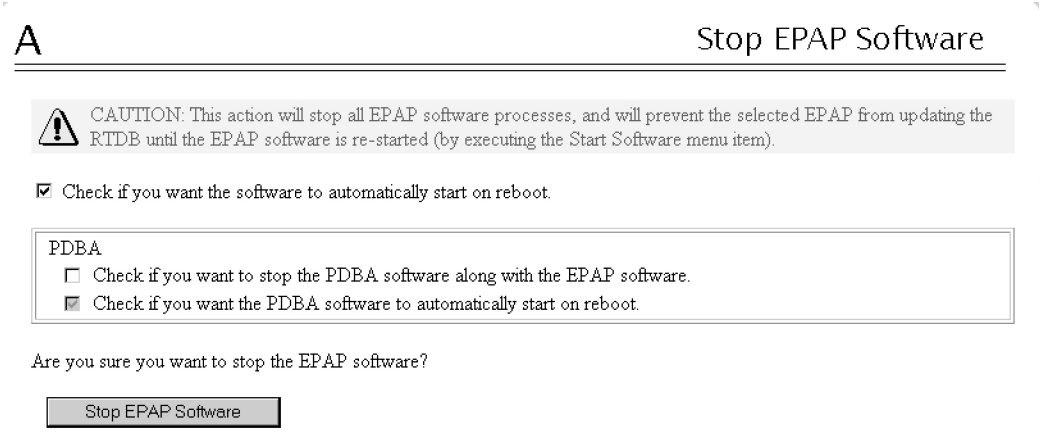
The PDBA items that appear in the screens in this procedure apply only to the EPAP application. These items will not appear for the ELAP application.

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

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

   The screen shown in Figure A-2 appears:

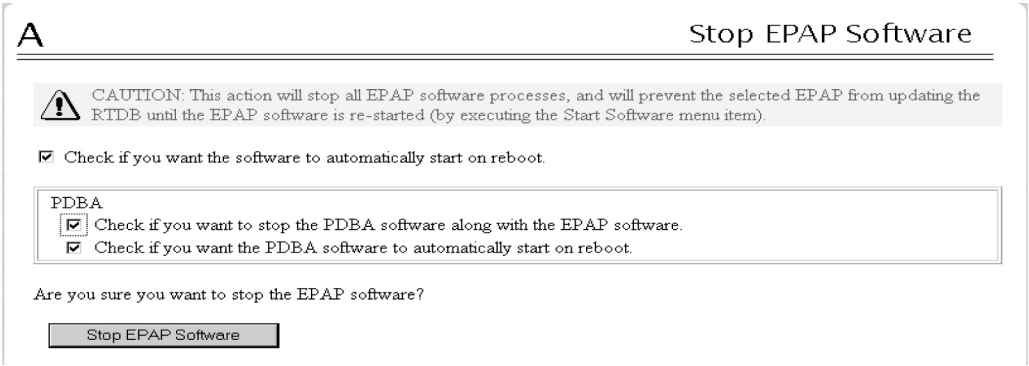
Figure A-2 Stop Software Confirmation



4. On the **Stop EPAP Software** screen, make sure the following checkboxes are all checked, so that the PDBA software is stopped along with the EPAP software and so that both the PDBA and EPAP software are automatically restarted on reboot (see Figure A-2 for an example):
   a. **Check to cause the software to automatically start on reboot**

      This checkbox causes the EPAP software to automatically reboot.
   b. **Check to stop the PDBA software along with the EPAP software**
   c. **Check to cause the PDBA software to automatically start on reboot**

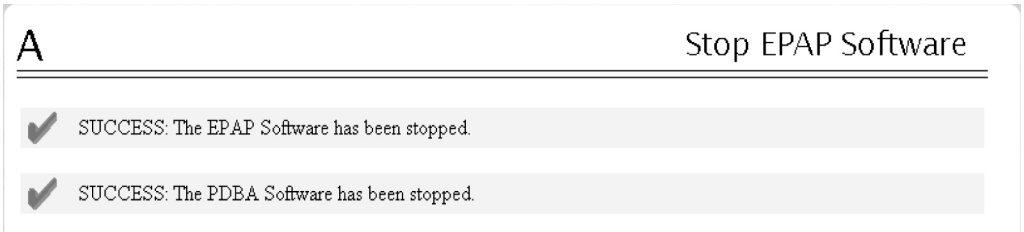
Figure A-3 Stop Software



5. Click the **Stop EPAP Software** button to stop the software.

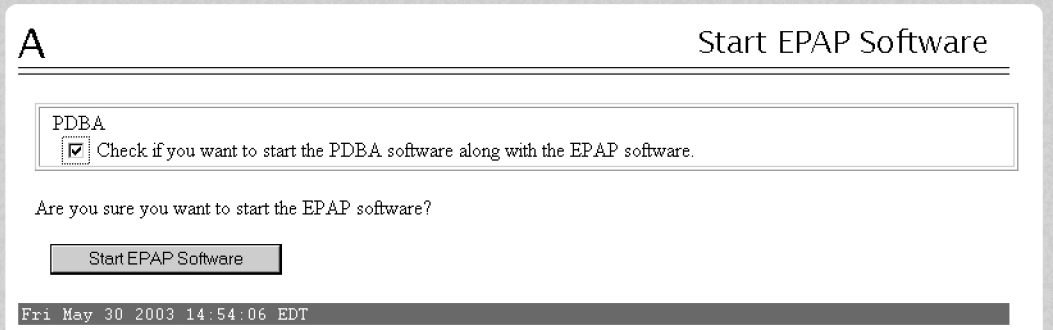
   The screen shown in Figure A-3 appears (the PDBA item appears only if performing this procedure on Side A).

Figure A-4 Stop Software Completion Screen



6. Select **Process Control > Start Software**.
7. From the **Start EPAP Software** screen, make sure the checkboxes are checked as shown in Figure A-5 (this item applies only if performing this procedure on Side A):

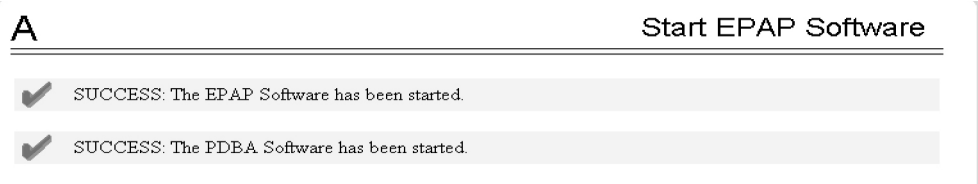
Figure A-5 Start EPAP Software



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

   The screen shown in Figure A-6 confirms that the software has started (the PDBA item appears only if performing this procedure on Side A):

Figure A-6 Start Software Completion Screen



A.4 Restarting the EPAP Software

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

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

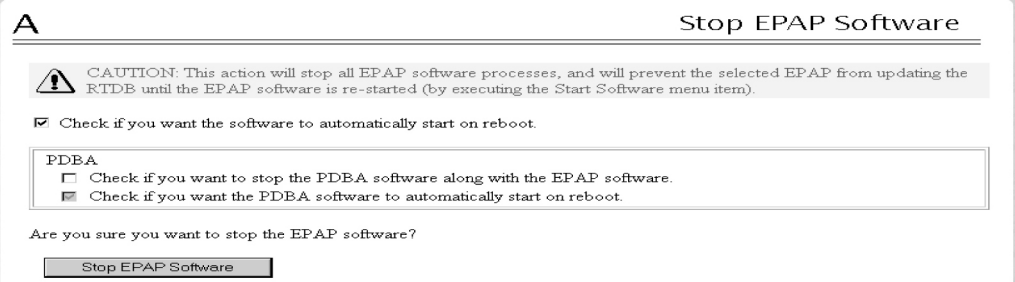
The PDBA items that appear in the screens in this procedure apply only to the EPAP application.

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

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

   The screen shown in Figure A-7 appears:

Figure A-7 Stop Software Confirmation



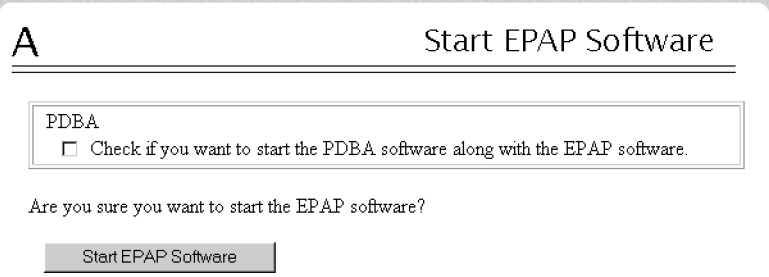
4. On the **Stop EPAP Software** screen, make sure that appropriate check boxes are checked as shown in Figure A-7.
5. Click the **Stop EPAP Software** button to stop the software.

   The screen shown in Figure A-8 appears.

Figure A-8 Stop Software Completion Screen

6. Select **Process Control > Start Software**.
7. From the **Start EPAP Software** screen, make sure that the check boxes are checked as shown in Figure A-9:

Figure A-9 Start EPAP Software



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

   The screen shown in Figure A-10 confirms that the software has started:

Figure A-10 Start Software Completion Screen

A.5 Saving Logs Using the EPAP GUI

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

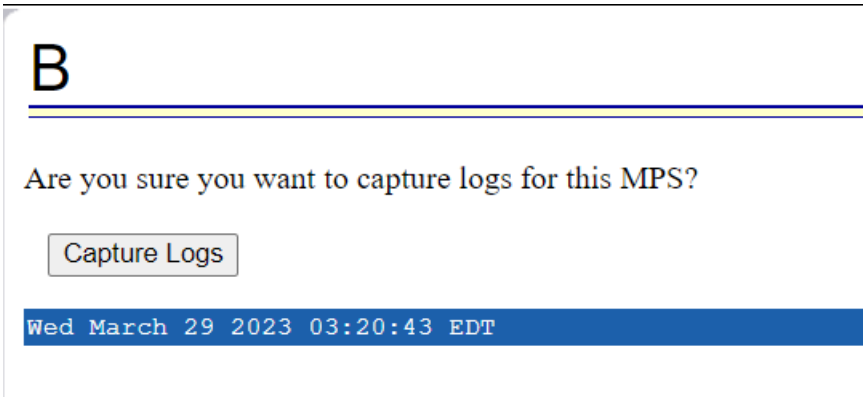
Use the following procedure to save logs using menu selections from the EPAP GUI.

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

   If it is necessary to switch to the problem EPAP, 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`.

> **Note:**
>
> Contact My Oracle Support for assistance before capturing core files with the log files.

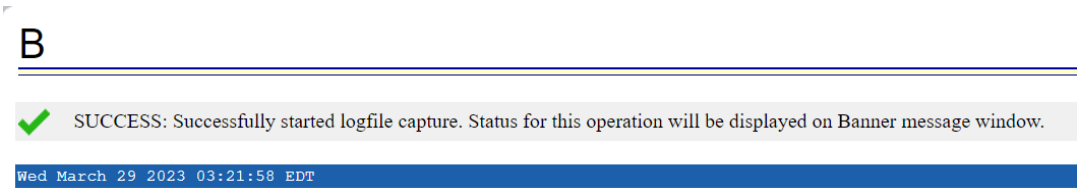
Figure A-11 Capture Logs File Screen



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

   After completion, verify the following response:

Figure A-12 Capture Logs Success

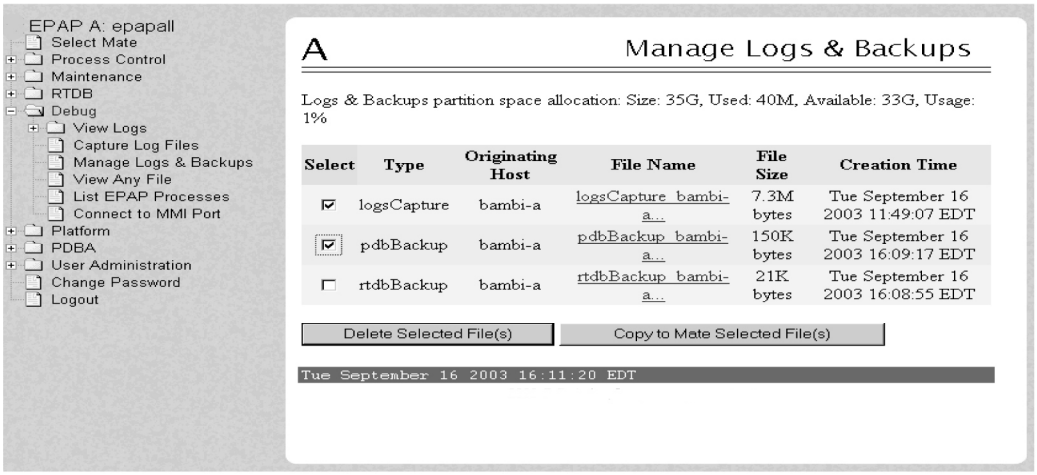


6. Contact My Oracle Support to analyze and check the log files.

7. When My Oracle Support 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 check boxes for the files you want to delete and then click the **Delete Selected File(s)** button.

   An example is shown in Figure A-13.

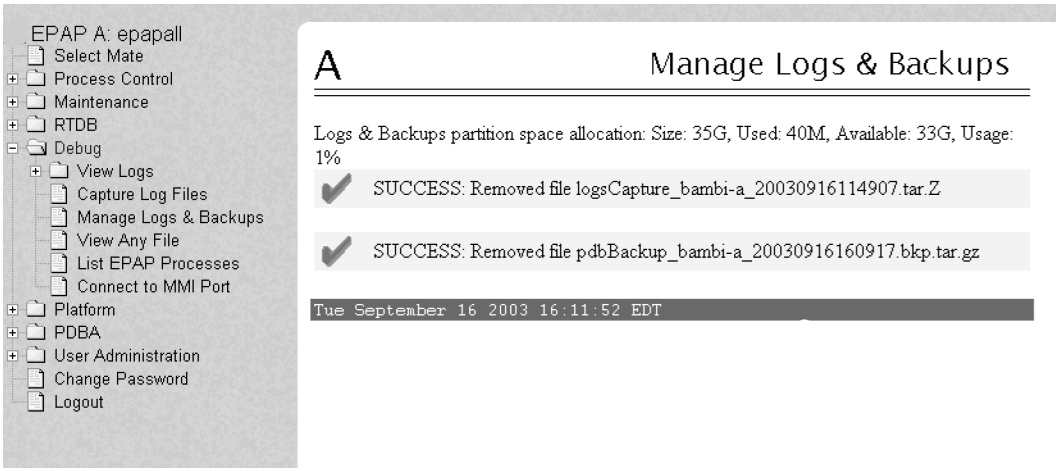
Figure A-13 Deleting Captured Log Files



.

When the log files have been deleted, the GUI displays confirmation, as shown in Figure A-14.

Figure A-14 Delete Log Files Success



A.6 Resolution Of Known Issues

1. **Platform Data Collection Error**
   Issue: TKSPLATMI39 – Platform Data Collection Error (5000004000000000) is observed on Eagle

Description: The Platform Data Collector is a TPD tool that periodically collects various software and hardware information about the server. It helps the customer to collect hardware and software information of all the servers in a 'Discovery Domain'.

For E5-APP-B, one of the collection modules attempts to get the PSoC version and fails.

```
rept-stat-mps
              VERSION       PST           SST        AST
   EPAP B             016-003-000   IS-ANR         Fault      Active
         MINOR    PLATFORM    ALARM DATA = H'5000004000000000
          ALARM STATUS        =  *0374 Minor Platform Failure(s)
```

Solution:

Run the following command to clear the alarm. Use sudo if running as admusr.

```
$ /usr/TKLC/plat/bin/pdcAdm
```

2. **Issue**: MySQL Lock Wait Timeout Exceeded alarm in EPAP (Bug# 28486392)
   Description: When large-scale data provisioning happens in a short span of time, sometimes MySQL lock wait times out and an alarm (MySQL Lock Wait Timeout Exceeded) is raised in EPAP. The provisioning is not disturbed.

   Solution:

   Restart the PDBA software.

   On the menu, click **PDBA**, select **Process Control** and click **Start PDBA software**.

3. **Issue**: GUI does not open in Backup PROV network in https mode after disaster recovery procedure (Bug# 26173039)
   Description: After disaster recovery, GUI does not open in backup PROV network in https mode.

   Solution:

   Reconfigure the backup prov IPs from epapconfig menu.

   On the epapconfig menu, configure **Network Interfaces** Menu, **Provisioning Network**, and then **Backup Provisioning Network**.

4. **Issue**: There is discrepancy in the mysqld@pdb service status on Non-Prov Servers (A and B) (Bug# 35026943)
   Description: mysqld@pdb service status is displayed as failed on Non-Prov server A and mysqld@pdb service status is displayed as Active on Non-Prov server B.

   Solution: This is legacy behaviour. It has no effects on EPAP operations and should be neglected.

5. **Issue**: RN entry present in PDB but not present in RTDB (Bug# 36552163)
   Description: When RN is provisioned with DN/DNBlock, RN gets into the PDB, but the entry is not present in RTDB.

   Solution: RTDB reload from PDB will resolve the issue. In case of Dual PDBA setup, perform RTDB reload from PDBA on the StandBy side, and Active side PDBA will continue provisioning data.

6. **Issue**: Standby PDBA Falling Behind (Bug# 36186109)
   Description: When there is no difference in the DB level of Active and StandBy PDB, "Standby PDBA Falling Behind" alarm is showing.

Solution: When Standby PDB falls behind Active PDB by a predefined margin, the alarm "Standby PDBA Falling Behind" is raised. It gets cleared automatically when the Standby PDB catches up with the Active PDB. In this scenario, StandBy side and Active side PDBA will continue provisioning data. If the alarm is not cleared even after Standby PDBA catches up the db level of Active PDBA, use the command `$ eagle_alarm_util 6000000000000020 OFF` to clear the alarm manually.