IBM TS7610 and TS7620 ProtecTIER® Deduplication Appliance Express

V3.3.6

Service Guide

Part 1

GA32-0915-09

PN 38L6403, EC M13180, EC Date 08 August, 2014

This edition applies to ProtecTIER V3.3.6 of the TS7610 Appliance Express and TS7620 Appliance Express and to all subsequent releases and modifications until otherwise indicated in new editions.

Read This First

This Maintenance Information (MI) is intended for use only by trained, IBM service personnel.

Send Us Your Feedback

Send us your comments about this book by email to *starpubs@us.ibm.com*. When sending your comments, be sure to include:

- Exact publication title
- Form number, or part number and EC level (on the back cover)
- Page numbers to which you are referring

Contents

Figures

Tables

Homologation statement

Attention: This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact an IBM representative or reseller if you have any questions.

Preface

This manual is for use by service personnel who install, remove, diagnose, repair, or test the ProtecTIER® V3.3.6 TS7610 Appliance Express® or TS7620 Appliance Express.

The manuals are available on the *IBM TS7610 ProtecTIER Deduplication Appliance Express and IBM TS7620 ProtecTIER Deduplication Appliance Express Publications* CD are:

- *IBM TS7610 ProtecTIER Deduplication Appliance Express Introduction and Planning Guide*, v3.3, GA32-0914
- *IBM TS7620 ProtecTIER Deduplication Appliance Express Installation and Setup Guide for VTL, and OpenStorage Systems*, v3.3, GA32-0914
- *IBM TS7610 and TS7620 ProtecTIER Deduplication Appliance Express Service Guide*, v3.3, GA32-0915

To access instructional videos and the latest updated service information in the TS7610 Appliance Express and TS7620 Appliance Express Information Center, go to http://pic.dhe.ibm.com/infocenter/ts7610/cust/index.jsp.

The content of this information center is also available on CD-ROM. However, information contained on the CD-ROM might not be as current as the information available online.

- *IBM TS7610 ProtecTIER Deduplication Appliance Express and IBM TS7620 ProtecTIER Deduplication Appliance Express Customer Information Center* DVD
- *IBM TS7610 ProtecTIER Deduplication Appliance Express and IBM TS7620 ProtecTIER Deduplication Appliance Express Service Information Center* DVD

Chapter 1. Troubleshoot by using ProtecTIER V3.3.6 diagnostic tools

Use theProtecTIER Service Menu and ProtecTIER Manager to troubleshoot the TS7610 Appliance Express or TS7620 Appliance Express server.

Interpreting hardware alerts

When a hardware component fails, the system issues alerts.

About this task

If hardware degradation or failure occurs, the components that are listed in Table 1 on page 2 generate one or more of the following types of alerts:

- Beeps or other audible indicators
- Changes in LED state
- Hardware faults reported through the ProtecTIER Manager
- Email alerts or SNMP trap reports (if you enabled either, or both, of these options during system configuration)

Important: Fault occurrences in the MegaRAID controller, SAS expander, Fibre Channel adapter, Ethernet adapter, or DIMM might prevent communication between ProtecTIER Manager and the server. As a result, ProtecTIER Manager might not be able to report the hardware fault.

Because of this limitation, enabling email alerts and SNMP reports is the best course of action. By doing so, you receive fault notifications regardless of ProtecTIER Manager availability. Email alert and SNMP report messages might take up to 45 minutes to arrive after a fault occurrence. The alert (or report) provides information about the faulty component, the nature of the fault, and suggestions for resolution.

To enable email alerts or SNMP traps, refer to the chapter on ProtecTIER configuration, in the *IBM TS7620 ProtecTIER Deduplication Appliance Express Installation and Setup Guide for VTL, and OpenStorage Systems*, v3.3, GA32-0914.

The following table provides an overview of the types of alerts that each component might generate.

- Components that are identified by a square (▪) has those alert options.
- Components that are identified by a triangle (△) might generate an alert in ProtecTIER Manager. This type of failure can be seen as an LED change or in an email alert/SNMP trap report.
- If the component cell in the table does not contain a square or triangle, then that type of alert does not occur. For example, there is no audible alarm for dual-port Ethernet adapter.

Refer to step 1 on page 5 for information about using ProtecTIER Manager alert windows, email alert messages, and SNMP trap reports.

Table 1. Alerts by component type

Component	Type	Audible alarm	LED change	ProtecTIER Manager	Email alert / SNMP trap report
1 TB SATA hard disk drives (HDDs)	CRU	▪	▪	▪	▪
Power supply units (PSUs)	CRU	▪	▪	▪	▪
Cooling fans	CRU	▪	▪	▪	▪
Dual-port Ethernet adapter	CRU		▪	⌂	▪
RAID battery backup unit (BBU)	CRU		▪	▪	▪
Dual in-line memory modules (DIMMs)	CRU		▪	⌂	▪
USB portable DVD drive	CRU		▪		
Fibre Channel host bus adapter (HBA)	FRU	▪	▪		▪
MegaRAID controller	FRU				▪
SAS expander	FRU				▪
Internal boot drive	FRU			▪	▪

Finding information

About this task

In addition to using the step-by-step procedures provided in this document, you can access instructional videos online. The videos demonstrate removing and replacing the HDDs (hard disk drive) and PSUs (power supply unit). The videos, which are in the **Resolution guides,** are easily accessible from ProtecTIER Manager. Instructions for accessing the Resolution guides are provided in "Accessing the Resolution guides from the ProtecTIER Manager Node menu" and "Accessing the Resolution guides from the Hardware faults window" on page 4.

Instructional videos that demonstrate CRU replacement, are available online in the TS7610 Information Center at:http://pic.dhe.ibm.com/infocenter/ts7610/cust/index.jsp.

Accessing the Resolution guides from the ProtecTIER Manager Node menu

About this task

Note: The Resolution guides provide information and instructions for resolving HDD and PSU faults, only. The guides are accessible only when ProtecTIER Manager communicates with the affected server. If ProtecTIER Manager is not available, use email alerts or SNMP reports.

Procedure

1. If it is not already running, start ProtecTIER Manager as described in 1 on page 5.
2. Log in to the system that includes the TS7620 Appliance Express server (node) with the faulty component, as described in 3 on page 6.
3. Return to this procedure and continue with step 4 on page 3.

4. On the menu bar at the top of the ProtecTIER Manager window, click: **Node** > **Hardware**.

   The list of Resolution guides appears:

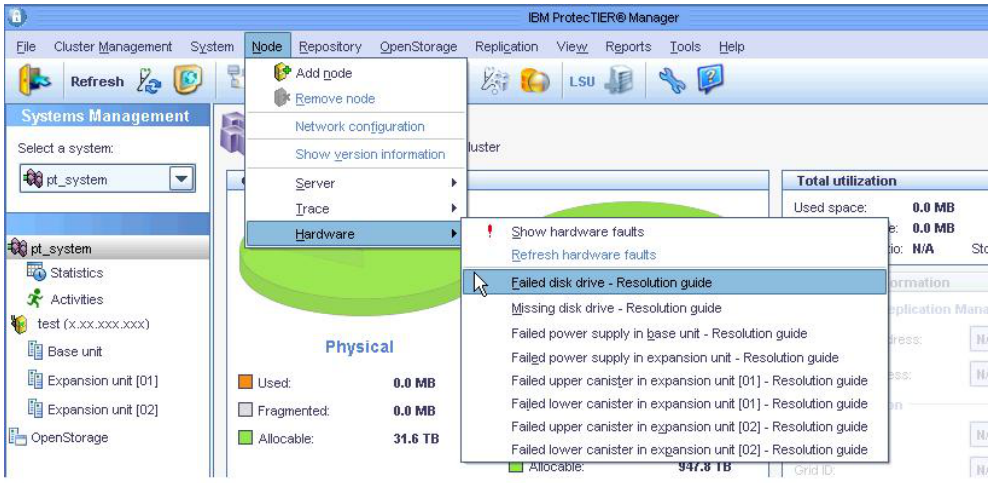


Figure 1. Resolution guides

5. Select the guide that is applicable for your task.

   The guide opens with information and instructions for the task that is displayed, as shown:

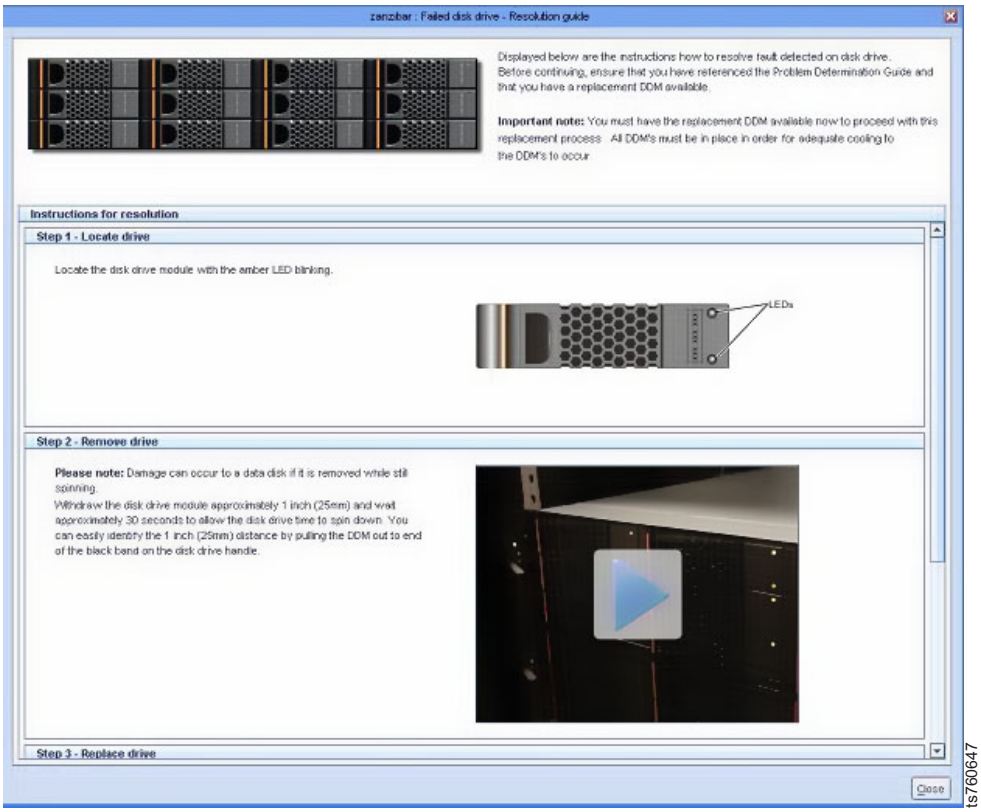


Figure 2. Failed disk drive Resolution guide

6. Scroll down to display any content not currently visible in the window.

7. Click the  (play button) to start the video.
8. When you are finished with the Resolution guide, click **Close.**

Accessing the Resolution guides from the Hardware faults window

About this task

Note: The Resolution guides provide information and instructions for resolving HDD and PSU faults, only. The guides are accessible only when the ProtecTIER Manager can communicate with the affected server. If the ProtecTIER Manager is not available, refer to email alerts or SNMP reports.

Procedure

1. If it is not already running, start ProtecTIER Manager as described in 1 on page 5.
2. Log in to the system that includes the TS7620 Appliance Express server (node) with the faulty component, as described in 3 on page 6.
3. Return to this procedure and continue with step 4.
4. Click **Hardware faults** at the bottom of the ProtecTIER Manager window.

   The Hardware faults window appears, with a list of all hardware faults for the selected server.
5. In the **Actions** column for an HDD or PSU, click the **Resolve fault** link.

   Note: If the **Actions** column is not currently visible, scroll the display to the right.

   The **Resolution guide** for the selected component type displays.
6. Read the information in the guide.
7. Click the  (play button) to start a video.
8. Follow the instructions that are provided to resolve the fault condition.
9. When you finished performing the required actions, return to the **Resolution guide**.
10. Click **Recheck Faults**.

    A confirmation dialog box displays.
11. Click **Yes** to continue.

    The **Refresh Action** dialog box displays, indicating that the refresh is in progress. When the refresh completes, the dialog box closes.

    The Hardware faults window displays. If you successfully resolved the fault, the associated hardware alert no longer appears in the list.
12. When you are finished with the **Resolution guide**, click **Close**.

Accessing instructional videos and other information in the Information Center

Procedure

1. Go to the TS7620 Appliance Express Information Center web page at: http://pic.dhe.ibm.com/infocenter/ts7610/cust/index.jsp.
2. Follow the navigation instructions that are provided on the Information Center page to locate and open the videos.

3. Click the  (play button) to start the video.
4. When you are finished with the **Resolution guide,** click **Close.**

Receiving and responding to hardware alerts

Upon receiving an alert, you must identify which component generated the alert (if it is not readily apparent). Analyze the cause and severity of the fault, and decide on a course of corrective action. Methods for doing so are described in the sections that follow.

ProtecTIER Manager Hardware Resources window

About this task

The Hardware resources window provides information such as component status, FRU ID (part number), and resource fault details; for all of the CRU components, and many of the FRU components.

When ProtecTIER Manager communicates with the server on which hardware faults occurred, the information that is displayed in the Hardware resources window helps identify, diagnose, and resolve the problem.

If ProtecTIER Manager is unavailable, and your system is configured for email alerts or SNMP traps, refer to the hardware fault alert and resolution information that is provided in those resources. FOr more information, see “Email alerts” on page 9 and “Using SNMP traps” on page 10.

Use this procedure to access the Hardware resources window.

Procedure

1. If ProtecTIER Manager is not running, use one of the following options to start it:
   - On a PC with a Windows operating system, click: **Start** > **All Programs** > **IBM** > **ProtecTIER Manager** > **IBM ProtecTIER Manager**.
   - On a PC with a Linux operating system, double-click the **ProtecTIER Manager** icon on the Linux Desktop.

   The **ProtecTIER Manager** window opens.
2. Log in to the system that includes the TS7610 Appliance Express or TS7620 Appliance Express ProtecTIER V3.3.6 server (node) with the faulty component.

   Note: If you are unsure which system contains the faulty node, log in to each system in turn. When a system name appears in red text in the **Systems** list, that is the faulty system.

   a. In the left-side navigation pane of the ProtecTIER Manager, click the applicable system.

      The **Login to system** dialog box opens.
   b. Click **Login**.
   c. In the **Username** field, type: **ptadmin**
   d. In the **Password** field, type: **ptadmin**
   e. Select the **Save password** checkbox, click **Ok**, and then wait while ProtecTIER Manager saves your information and logs you in to the system.

The following message appears:

Figure 3. Configuration wizard reminder

f. Click **Ignore** to close the message.

3. In the **Nodes** section of the **Systems Management** pane, click the TS7610 Appliance Express or TS7620 Appliance Express server on which a fault occurred. Nodes with faults appear in red in the list, as shown:

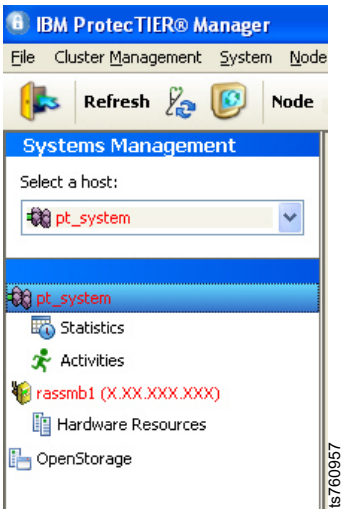


Figure 4. Example of faulty nodes displayed in red on a ProtecTIER OST server

The **ProtecTIER Manager** window refreshes and changes to **Nodes** view, with information for the selected server displayed.

4. In the **Hardware resources** window, click the tab in the middle pane of the ProtecTIER Manager for the component for which you need information.

   You might see these icons if the selected component is degraded ( ) or is in a failed state ( ), or has another type of fault.

   In the next example, the disk drive component was selected and disk drive 12 has a small blue information icon. To see details of the information warning, scroll to the pane on the right.

   ProtecTIER Manager shows disk drive 12 is rebuilding.

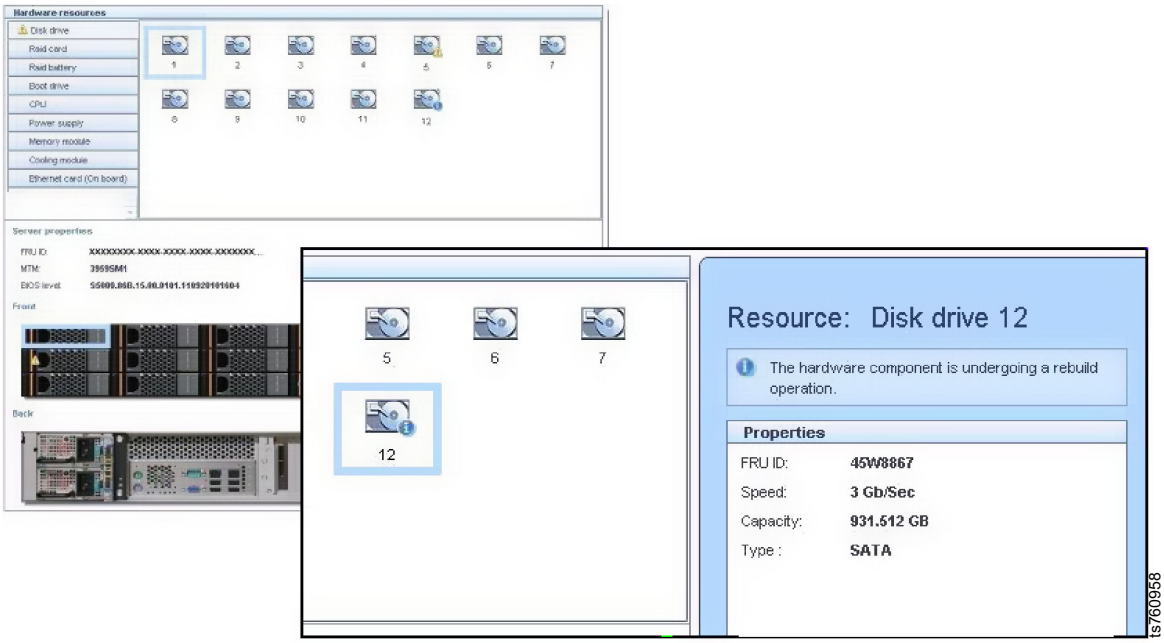


Figure 5. Hardware resources window, disk drive 12 rebuilding

The following example shows the disk drive component where all the disk drives are working.

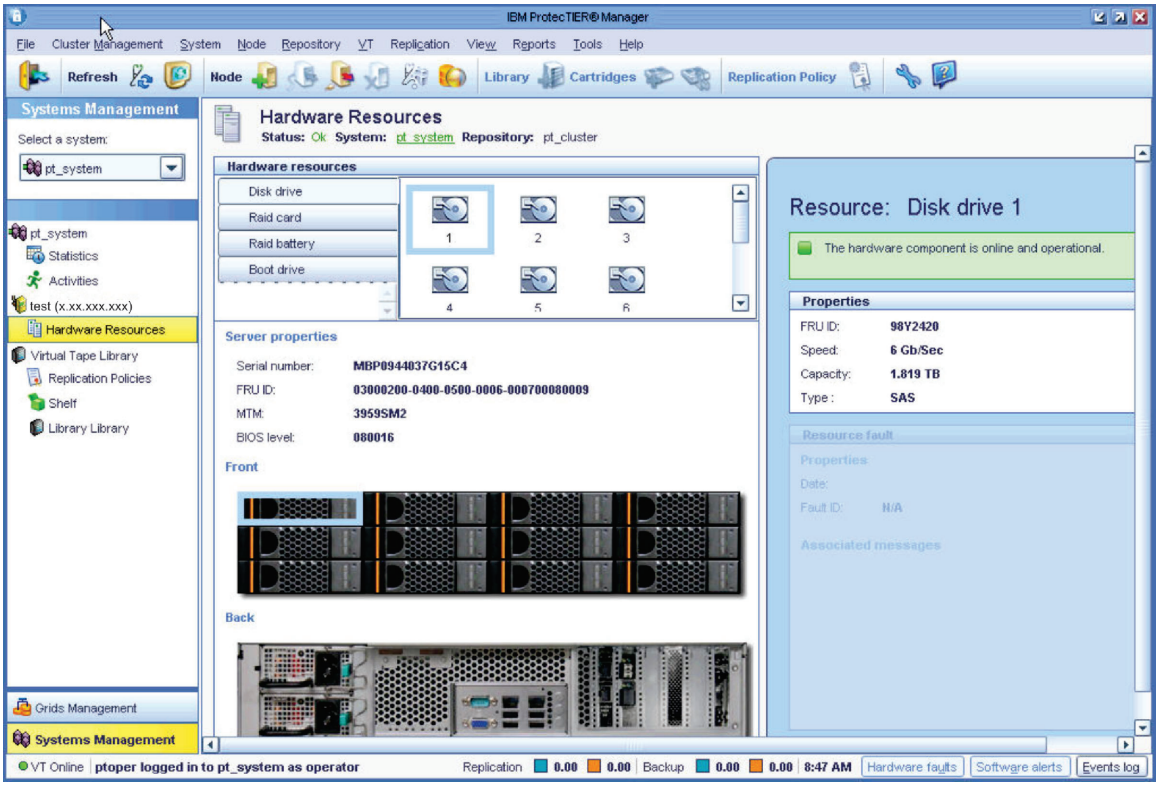


Figure 6. Hardware resources window

5. In the **Resource** pane, on the right side of the window:
   a. Note the name of the component that generated the alert.
   b. Read the problem description to determine what caused the alert.

c. Under **Properties**, note the **FRU ID**.

   Note: The FRU ID (part number) for both CRU and FRU components, is expressed as a FRU ID.

d. Under **Resource fault**, read the information in the **Associated Messages** area, and follow any instructions.

6. When you are finished reviewing fault and component information, use one of the following methods to exit the ProtecTIER Manager:
   - Click **File** > **Exit**.

     OR
   - Click the **X** in the upper-right corner of the window.
7. Verify that the alert received was not caused by an easily resolved condition, such as a loose power cord or a defective cable.

ProtecTIER Manager Hardware Faults window

About this task

The Hardware faults window provides information on all of the hardware faults currently in effect for the specified server. When the ProtecTIER Manager is able to communicate with the server on which a hardware faults occurred, the information in the Hardware faults window might help you to identify, diagnose, and resolve the problem. If the ProtecTIER Manager is unavailable, and your system is configured for email alerts or SNMP traps, refer to the hardware fault alert and resolution information that is provided in those resources.

Use the following procedure to access the Hardware faults window.

Procedure

1. If it is not already running, start PT Manager as described in ProtecTIER Manager Hardware Resources window.
2. Log in to the system that includes the TS7610 Appliance Express or TS7620 Appliance Express server (node) with the faulty component, as described in 2 on page 5.
3. Select the server (node) on which the fault occurred, as described in 3 on page 6.
4. There are two ways to access **Show Hardware Faults**:
   - **Node** > **Hardware** > **Show Hardware Faults**
   - If there is a current hardware fault, click **Recheck faults** at the lower right of the **ProtecTIER Manager** window.

   The **Recheck Faults** window opens, with one or more fault messages on display in the **Associated messages** column:

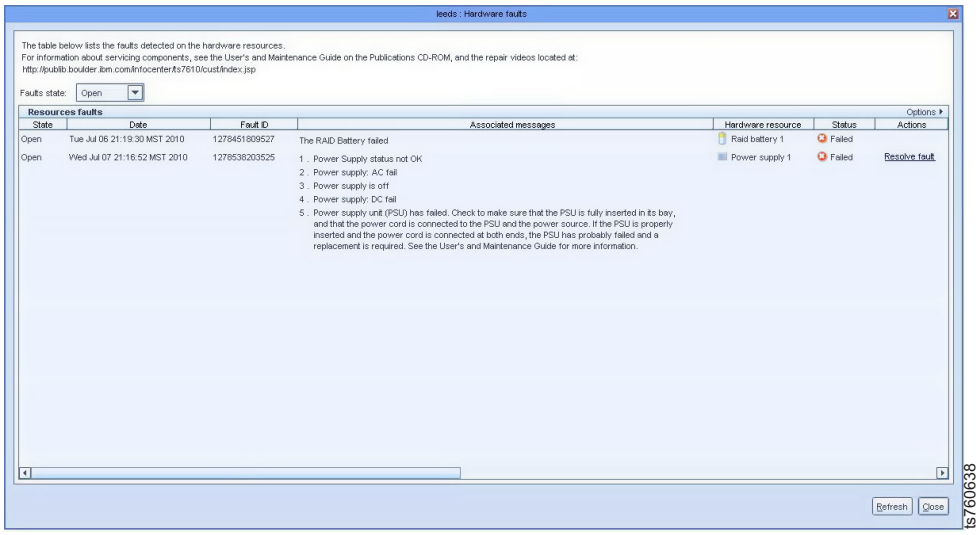


Figure 7. Recheck faults window

5. Review the displayed information, and make note of the defective components name (or type) and FRU ID.

   Note: The FRU ID (part number) for both CRU and FRU components, is expressed as a FRU ID.
6. Verify that the alert received was not caused by an easy to resolve condition, such as a loose power cord or a defective cable.
7. Refer to 4 on page 3

Email alerts

About this task

If a hardware degradation or failure occurs, systems that are configured to use email alerts send a problem report message to one or more designated recipients. Email alerts notify you of hardware fault, even if you do not have access to the ProtecTIER Manager. When a hardware fault occurs, the system generates and sends a problem report, similar to the one shown in Figure 8:

```
The following hardware alert has been issued for the indicated IBM TS7610 Deduplication Appliance Express.
Alert issued for part: Node 0/Enclosure 63,Eth Card 1

# Report time and date.................= 07/09/10 09:15:02 MST
# Source Host Name.....................= rassmb1
# Source IP............................= 9.11.219.152
# Business/Company Name................= A
# Customer Number......................= 2,USA
# Product serial number................=
# Product Software ID..................= 5639-TAA
# Product Machine Type and Model ......= 39595M1
# Date and Time of fault occurrence.....= 07/09/10 08:50:09 MST
# Problem ID...........................= 1278690619611
# Problem Type.........................= Hardware
# Alert issued for part................= Node 0/Enclosure 63,Eth Card 1
# Failing part FRU id..................= 39Y6127
# Problem Severity.....................= FAILED
# SRN..................................= 0xAA030001
# Problem Description..................= Adapter link is down. Verify cabling
```

ts760637

Figure 8. Email alert

Procedure

1. Upon receiving an email alert:
   a. Open the message and review the information in the report.

b. Make note of the defective components name (or type) and FRU ID.

   Note: The FRU ID (part number) for both CRU and FRU components, is expressed as a FRU ID.

2. Verify that the alert you received was not caused by an easy to resolved condition, such as a loose power cord or a defective cable.

Using SNMP traps

About this task

In the event of hardware or software degradation or failure, ProtecTIER systems which are configured to use Simple Network Management Protocol (SNMP) can send a problem notification to designated recipients. SNMP notifications, or traps, can be sent even if the ProtecTIER Manager interface is unavailable.

To use SNMP traps you need the following items:

- SNMP trap receiver software installed on an SNMP trap server. Follow the instructions from the manufacturer to install and configure the SNMP trap receiver software.
- The file name and location of the management information base (MIB) file for the SNMP trap receiver. On the ProtecTIER server, the file name is: `IBM-TS7600-SNMP-MIBV2.mib` located in: `/usr/share/snmp/mibs`. The full path is: `/usr/share/snmp/mibs/IBM-TS7600-SNMP-MIBV2.mib`.
- The `IBM-TS7600-SNMP-MIBV2.mib` file needs to be copied onto the SNMP trap receiver and the trap receiver software must point to the directory location of the MIB file for translation of the trap messaging.
- SNMP trapping enabled on one or more of your ProtecTIER servers. Use the ProtecTIER Manager Configuration wizard to enable the SNMP trap option on 3959 SM1 servers. See the *IBM TS7620 ProtecTIER Deduplication Appliance Express Installation and Setup Guide for VTL, and OpenStorage Systems*, v3.3, GA32-0914 for instructions on SNMP configuration. For 3958 AP1 or 3958 DD4 servers, see the *IBM ProtecTIER User's Guide for Enterprise Edition and Appliance Edition*, V3.3.6, GA32-0922.

The ProtecTIER servers have the following improvements in SNMP support.

- ProtecTIER software events that send specific notifications based on the error that occurred.
- ProtecTIER hardware events that trigger specific notifications are based on the error that occurred, such as a CPU event or power event.
- Send enough detailed information with the SNMP notification so that you can understand the problem. The ProtecTIER Manager Configuration menu gives you the option to filter SNMP traps based on severity.
  - Error-level severities can be filtered by:
    - Error
    - Warning
    - Information
    - Software error categories include:
      - VTL
      - Replication
      - OpenStorage
      - FSI

        - Repository storage
        - Cluster
        - System
      - Hardware error categories include:
        - CPU memory module
        - Cooling module (fan)
        - Internal boot drives
        - Ethernet cards
        - Power supplies
        - RAID card
        - RAID battery
        - Front end adapter, if VTL enabled
        - General server errors
        - General network errors
        - Ethernet switch, if cluster enabled with SMC switch (TS7650 or TS7650G only)
        - Network power switch, if cluster enabled with new network power switch (TS7650 or TS7650G only)
        - 3958 AP1 specific
        - Back end adapter (TS7650 or TS7650G only)
        - Disk controller (TS7650 or TS7650G only)
        - Disk expansion (TS7650 or TS7650G only)
        - 3959 SM1 specific
        - SAS expander
        - SATA hard disk drives
    - Warning-level severity includes:
      - Replication warnings
      - VTL warnings
      - OpenStorage warnings
      - FSI warnings
      - Capacity warnings
      - RAS warnings
    - Information-level severity includes:
      - VTL configuration change events
      - OpenStorage configuration change events
      - FSI configuration change events
      - Replication events
- SNMP in ProtecTIER version 3.1 or later supports threshold monitoring and allows the user to specify thresholds for the following system runtime behavior:
  - Repository space issues
    - Nominal capacity
    - Physical capacity
  - There are two threshold levels a user can set:
    - Information level: a trap is sent when the repository regains free space and rises about the information level.

- Warning level: a trap is sent when the free space in the repository falls below the warning level

  – Going below the informational threshold issues an SNMP trap only if the warning threshold has been crossed. This method is to ensure that the user is not flooded with alerts when the normal operation crosses the low water mark threshold frequently.
  – Capacity thresholds can be set specifying % from the repository or specifying space (GBs).
- Using an IBM-registered management information base (MIB) file.
  – The MIB file is implemented in a tree structure and has a unique OID for each message supported.
  – The MIB file ships on the ProtecTIER server.
- Provide reporting to the network management application software.
- Improved communication options:
  – SNMP traps are sent through the customer network (eth0) by using the UDP protocol.
  – By default, port 162 is used and up to five destinations are supported.
  – Customers can optionally select a different port for SNMP traffic by using the ProtecTIER Manager Configuration menu.

On systems configured to use SNMP traps, an agent monitors the ProtecTIER server and reports fault information to a network management application. Periodically the data is sent to the designated SNMP server in the form of an SNMP trap report, a portion of which is shown in Figure 9 on page 13. SNMP trap reports allow you to receive hardware or software fault notifications whether or not you have access to the ProtecTIER Manager interface. The display format of the trap report varies between different trap receiver software applications. Your trap report might not look exactly like the following example.

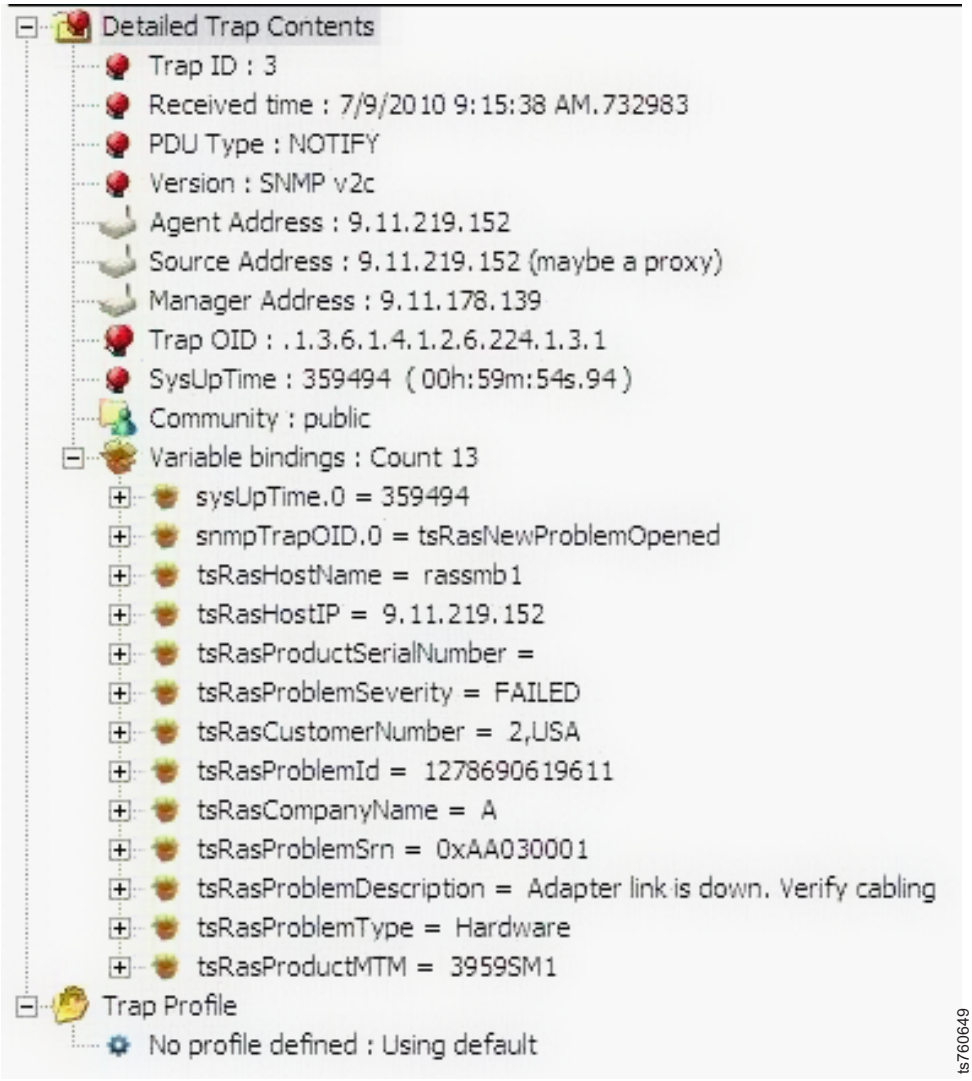


Figure 9. SNMP trap report

Procedure

1. Run the SNMP trap catcher program on the SNMP server.
2. Open the SNMP report and review the information.
3. Make note of the defective component's name (or type) and FRU ID.

   Note: The FRU ID (part number) for both CRU and FRU components, is expressed as a FRU ID.
4. Verify the alert received was not caused by an easily-resolved condition, such as a loose power cord or a defective cable.

Verifying hardware faults

About this task

Procedure

1. If necessary, start **ProtecTIER Manager** and log into the system that includes the TS7620 Appliance Express server (node) with the faulty component.

For detailed ProtecTIER Manager login instructions, refer to *IBM TS7610 and TS7620 ProtecTIER Deduplication Appliance Express User's and Maintenance Guide*, v3.3, GA32-0916.

Note: If you are unsure which system contains the faulty node, log in to each system in turn, until you find the system that has it's name displayed in red text in the Systems list.

2. In the **Systems Management** pane, click the TS7620 Appliance Express server on which a fault has occurred. Nodes with faults appear in red in the list, as shown below:

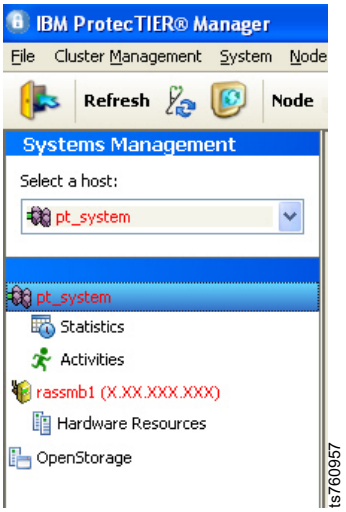


Figure 10. Faulty nodes displayed in red

The **ProtecTIER Manager** window refreshes and changes to **Nodes** view, with information for the selected server displayed.

3. Make sure the alert you received was not caused by an easily-resolved condition, such as a loose power cord or a defective cable.
4. The FRU ID for both CRU components and FRU components is expressed as a FRU ID. To find the FRU ID of the defective component:
   a. Select **Hardware Resources** in the ProtecTIER Manager navigation menu on the left.
   b. Select the specific hardware resource in the middle pane of the ProtecTIER Manager window.
   c. The FRU ID appears in the ProtecTIER Manager **Resource** pane on the right.

Tip: You can watch instructional videos of the procedures by going to the IBM® System Storage® TS7610 ProtecTIER Deduplication Appliance Express Customer Information Center.

ProtecTIER Service menu health monitoring and problem notification

This section explains ProtecTIER Service menu system health monitoring and problem notification tools.

About this task

Complete the following steps to access the Health Monitoring menu. Use Health Monitoring to either diagnosis a hardware problem or verify if hardware replacement fixed the problem

Health Monitoring

Procedure

1. If necessary, power-on the server and the monitor, and wait for the login prompt to display.

   For power-on instructions, see "TS7610 or TS7620 power off sequence" on page 23.
2. Access the **ProtecTIER Service Menu** with a monitor and keyboard plugged into the TS7610 Appliance Express or TS7620 Appliance Express server. Log on with ID **ptconfig**, password **ptconfig**
3. When the **ProtecTIER Service Menu** appears, select the **ProtecTIER Configuration** option.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
--------------------------------------------------------------------------------
  1) ProtecTIER Configuration (...)
  2) Manage ProtecTIER services (...)
  3) Health Monitoring (...)
  4) Problem Alerting (...)
  5) Version Information (...)
  6) Generate a service report
  7) Generate a system view
  8) Update ProtecTIER code

  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

4. Select **Health Monitoring.**

   Health Monitoring contains the following options:
   - Display system health summary - this option reports the current state of the system, without underlying components details
   - Display detailed system health state - this option reports the current state of the system, with details of all the underlying components
   - Run a full system check - this option reports the state of the all the hardware components
   - List open problems - this option lists hardware or system problems
   - Service mode - Select this option before servicing the system to prevent adding false system errors during system maintenance. Exit this mode once system maintenance is done.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
 Health Monitoring (...)
--------------------------------------------------------------------------------
  1) Display system health summary
  2) Display detailed system health
  3) Run a full system check
  4) List open problems
  5) Service Mode

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

Select **Run a full system check**.

5. If a disk drive is missing or defective, you might see this when you run your health check. This example shows that disk drive 5 is missing.

```
+----------------------------------------+
>>> Your choice? 1
Begin Processing Procedure
TS7610 Checkout Version 7123.122-0 executed on: 2011-05-05T20:36:10
================================================
Summary of NON-OK Statuses:
Offline 0
Failed 0
Unknown 0
Degraded 0
Rebuilding 0
Missing 1
================================================
Verify state of DDM 5 (Node 0/Enclosure 8).............MISSING
============================================================
*MISSING: Component Location: Node 0/Enclosure 8/DDM5
*MISSING: FRU ID: 45W8867
*MISSING: Enclosure 8
*MISSING: capacity: 931.512
*MISSING: speed: 3.0
*MISSING: capacityUnit: GB
*MISSING: SpeedUnit: Gb/s
*MISSING: diskType: SATA
*MISSING: SRN: 0xAA100001
*MISSING: The hard disk drive is missing. Check that the disk drive is
*MISSING: present in the dive bay and is properly seated. If not
properly
*MISSING: seated, try reseating the drive. See User's and Maintenance
*MISSING: Guide for more information.
================================================
```

6. If disk drive 12 has been replaced and you rerun the health check, the health check report shows that disk drive 12 is rebuilding.

```
+----------------------------------------+
>>> Your choice? 1
Begin Processing Procedure
TS7610 Checkout Version 7123.122-0 executed on: 2011-05-05T22:46:17
================================================
Summary of NON-OK Statuses:
Offline 0
Failed 0
Unknown 0
Degraded 0
Rebuilding 1
Missing 0
================================================
Verify state of DDM 12 (Node 0/Enclosure 8).............REBUILDING
============================================================
*REBUILDING: Component Location: Node 0/Enclosure 8/DDM12
*REBUILDING: FRU ID: 45W8867
*REBUILDING: Enclosure 8
*REBUILDING: capacity: 931.512
*REBUILDING: speed: 3.0
*REBUILDING: capacityUnit: GB
*REBUILDING: SpeedUnit: Gb/s
*REBUILDING: diskType: SATA
================================================
End Processing Procedure
```

7. Once a component has been successfully replaced or rebuilt than you will see this output when you rerun your health check:

```
TS7610 Checkout Version 7123.122-0 executed on: 2011-05-05T24:46:17
================================================
Summary of NON-OK Statuses:
Offline 0
Failed 0
Unknown 0
Degraded 0
Rebuilding 0
Missing 0
================================================
```

8. To exit the system **ProtecTIER Configuration** menu, type: **E <enter>**.

   You are then returned to the server command prompt.

Problem Alerting

Procedure

1. If necessary, power-on the server and the monitor, and wait for the login prompt to display.

   For power-on instructions, see "TS7610 or TS7620 startup" on page 25.

2. Access the **ProtecTIER Service Menu** with a monitor and keyboard plugged into the TS7610 Appliance Express or TS7620 Appliance Express server. Log on with ID **ptconfig** password **ptconfig**
3. When the **ProtecTIER Service Menu** appears, select the **ProtecTIER Configuration** option.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
--------------------------------------------------------------------------------
  1) ProtecTIER Configuration (...)
  2) Manage ProtecTIER services (...)
  3) Health Monitoring (...)
  4) Problem Alerting (...)
  5) Version Information (...)
  6) Generate a service report
  7) Generate a system view
  8) Update ProtecTIER code

  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

4. Select **Problem Alerting.**

   The system **Problem Alerting** contains the following options:

   - Enable/Disable Call Home - depending on your current Call Home state, select this option to either enable or disable Call Home
   - Send a Test Call Home
   - Configure Call Home Heartbeat frequency - sets how often the Call Home communication path is checked
   - Send a Heartbeat Call Home - this option checks the Call Home communication path
   - Enable/Disable Notification by email - depending on your current Notification by email state, select this option to either enable or disable Notification by email
   - Test Email Notification - sends a test email to verify email address
   - Activate Call Home Polling Function

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
 Problem Alerting (...)
--------------------------------------------------------------------------------
  1) Enable/Disable Call Home
  2) Send a Test Call Home
  3) Configure Call Home Heartbeat frequency
  4) Send a Heartbeat Call Home
  5) Enable/Disable Notification by email
  6) Test Email Notification
  7) Activate Call Home Polling Function

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

5. To exit the **Problem Alerting** menu, type: **E <enter>**.

   You are then returned to the server command prompt.

ProtecTIER V3.3.6 Call Home

IBM recommends that you enable the Call Home feature on each of your ProtecTIER servers. Doing so speeds-up problem determination and fault resolution. When enabled on the TS7610 Appliance Express and TS7620 Appliance Express, Call Home uses a connection on your Ethernet network to transmit hardware and software problem reports to IBM. For detailed instructions on enabling Call Home on your TS7610 Appliance Express and TS7620 Appliance Express servers, see the *IBM TS7620 ProtecTIER Deduplication Appliance Express Installation and Setup Guide for VTL, and OpenStorage Systems*, v3.3, GA32-0914.

When the Reliability, Availability, and Serviceability (RAS) software on the TS7610 Appliance Express and TS7620 Appliance Express server detects an error condition, Call Home sends detailed error information to IBM (home). If the error indicates a problem with a field replaceable unit (FRU), an IBM Service Representative can then prepare an action plan to handle the problem before traveling to your site.

The TS7610 Appliance Express and TS7620 Appliance Express provides three Call Home capabilities: Problem Call Home, Heartbeat Call Home, and Test Call Home; described below. RAS sends data files that may be helpful to IBM Support Center personnel for all three types of Call Home. These data files include error logs and configuration information, such as the Machine Reported Product Data (MRPD) log.

The customer can also chose to have IBM service enable their Call Home. IBM service can activate the customer's Call Home through the TS7620 Appliance Express ProtecTIER Service Menu.

Call Home through the ProtecTIER Service Menu

To access Call Home options through the ProtecTIER Service Menu, you will need the following:

- administrator logon access into the customer's ProtecTIER V3.3.6 TS7610 Appliance Express or TS7620 Appliance Express server
- the ProtecTIER V3.3.6 TS7610 Appliance Express or TS7620 Appliance Express server must have already been installed and configured

Enabling or disabling Call Home

Use the ProtecTIER Service Menu to enable or disable the server's ability to place a Call Home call and alert IBM if a system problem occurs.

About this task

If this is the first time Call Home is being enabled on the server, **you must** do so using the ProtecTIER Configuration window. Refer to *IBM TS7620 ProtecTIER Deduplication Appliance Express Installation and Setup Guide for VTL, and OpenStorage Systems*, v3.3, GA32-0914, for detailed configuration instructions. Should you need to disable or re-enable Call Home in the future, you will have the choice of doing so using the ProtecTIER Configuration menu or the Configuration window in the ProtecTIER Manager.

Accessing the ProtecTIER Service Menu

Procedure

1. If necessary, power-on the server and the monitor, and wait for the login prompt to display.

   For power-on instructions, see "TS7610 or TS7620 startup" on page 25.
2. At the **login** prompt, type: **ptconfig** and press **<enter>**.
3. At the **Password** prompt, type: **ptconfig** and press **<enter>**

   The **ProtecTIER Service Menu** displays:

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
--------------------------------------------------------------------------------
  1) ProtecTIER Configuration (...)
  2) Manage ProtecTIER services (...)
  3) Health Monitoring (...)
  4) Problem Alerting (...)
  5) Version Information (...)
  6) Generate a service report
  7) Generate a system view
  8) Update ProtecTIER code

  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

   Choose **Problem Alerting**

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
 Problem Alerting (...)
--------------------------------------------------------------------------------
  1) Enable/Disable Call Home
  2) Send a Test Call Home
  3) Configure Call Home Heartbeat frequency
  4) Send a Heartbeat Call Home
  5) Enable/Disable Notification by email
  6) Test Email Notification
  7) Activate Call Home Polling Function

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

4. Go to "Enabling Call Home" or "Disabling Call Home" on page 21.

Enabling Call Home

About this task

Procedure

1. On the **Enable/Disable Call HomeMenu** in step 1, select **Enable/Disable Call Home**. Type: **1** and press **<enter>**.

   The following messages, display:

   `Getting Call Home state [ Done ]`

   `Call Home successfully set.`
2. When the `Call Home is currently Disabled, do you wish to enable it? (yes|no)` prompt displays, type: **y <enter>**.

   `The Configuring Call Home [ Done ]` message displays.
3. When the `Press the ENTER key to continue...` message displays, press **<enter>**. You are returned to the **ProtecTIER Service Menu**.

4. You can select **q** to quit the menu and log out (it will close the connection), or proceed to another menu item task.

Disabling Call Home:
About this task

Use the procedure below to disable Call Home functionality.

Procedure

1. Access the ProtecTIER Configuration Menu. See 1 on page 20.
2. Select the **Enable/Disable Call Home** option, as described in step 1 on page 20, above.
3. When the `Call Home is currently Enabled, do you wish to disable it? (yes|no)` prompt displays, type: **y <enter>**.

   message displays:

   ```
   Call Home is disabled          [ Done ]
   Call home succesfully set to false
   ```

4. When the `Press the ENTER key to continue...` message displays, press **<enter>**. You are returned to the **ProtecTIER Service Menu**.
5. You can select **q** to quit the menu and log out (it will close the connection), or proceed to another menu item task.

Possible hardware fault solutions

About this task

Table 2. Easily resolved fault conditions

If you experience a problem related to...	Possible condition	Resolution
Loss of connectivity to the ProtecTIER Manager	An Ethernet cable might be disconnected from the adapter installed in Slot 3 or from the on-board Ethernet port (NIC 2).	Reconnect the cables to the applicable ports. The port LEDs illuminate.
	An Ethernet cable might be damaged or faulty.	Completely disconnect and remove the existing Ethernet cable and replace it with a new cable. The port LED illuminates.
HDD	The HDD might be improperly seated in the drive bay.	Push the HDD fully into the bay until the front of the drive is flush with the front of the server chassis. The HDD LED illuminates.
	After replacing an HDD, the new HDD did not set as the hot spare	1. Remove the drive. 2. Wait for GUI to show drive is missing. 3. Use GUI repair wizard for missing drive. This wizard will guide the user to insert the drive and it will set it to hot spare.

Table 2. Easily resolved fault conditions (continued)

If you experience a problem related to...	Possible condition	Resolution
PSU	The power cord might be loose or unplugged from the PSU or power source.	Fully insert the power cord into the outlets on the PSU and the power source. The PSU LED illuminates.
	The PSU might be improperly seated in the bay.	Push the PSU into the bay until it is fully inserted. The PSU LED illuminates.
Cooling fan	The fan might be improperly seated in the fan tray.	Perform substeps a and b of step 1 on page 89. Check to see that the fan is properly seated then perform substep b of step 2 on page 91.
RAID BBU	The internal cable from the BBU to the MegaRAID controller might may be disconnected.	Perform step 1 on page 100 and substeps a and b of step 2 on page 100. Check to make sure that the cable from the RAID controller to the BBU is securely connected then perform substep f of step 3 on page 100 and step 4 on page 101.
DIMM	One or more DIMMs might be improperly seated in the slot.	Perform step 1 on page 86 and substeps a and b of step 2 on page 86. Check to make sure each of the DIMMs is fully seated then perform substeps d and e of step 3 on page 87 and step 4 on page 88.
Dual-port Ethernet adapter	An Ethernet cable might be disconnected from the adapter installed in Slot 3 or from the on-board Ethernet port (NIC 2).	Reconnect the cables to the applicable ports. The port LEDs illuminate.
	An Ethernet cable might be damaged or faulty.	Completely disconnect and remove the existing Ethernet cable, and replace it with a new cable. The port LEDs illuminate.
Fibre Channel HBA	One, or both, of the Fibre Channel cables might be disconnected from the adapter installed in Slot 5.	Reconnect the cables to the adapter.
	One, or both, of the Fibre Channel cables might be damaged or faulty.	Completely disconnect and remove the existing Fibre Channel cables and replace them with new cables. The port LEDs illuminate.

Chapter 2. General service procedures

This section contains general instructions that are referenced by the component replacement procedures.

Electrostatic discharge procedures

When removing and replacing CRU components, take the precautions listed below to avoid static electricity damage:

- Whenever possible, wear an Electrostatic discharge (ESD) wrist strap. When doing so, ensure that the flexible grounding cord remains connected to you and to the frame of the machine. Because the wrist strap has a high resistance (>1 megohm) resistor in series with the grounding clip, there is no danger to you. The resistor discharges the static electricity from your body. To use the ESD wrist strap:
  1. Place the elastic band around your wrist.
  2. Connect the clip on the flexible grounding cord to an unpainted frame ground point on the rack.
  3. Keep the strap on and connected while you touch, insert, or remove any ESD-sensitive part.
- Do not open the static-protective package that contains the component until you are instructed to do so.
- Limit your movement. Movement can cause static electricity to build up around you.
- Always handle components carefully. Handle adapters and memory modules by the edges. Never touch any exposed circuitry, including the gold connectors along the bottom edge of the PCI adapters.
- Prevent others from touching the components.
- When possible, remove the component and install it directly in the computer without setting the component down. When this is not possible, place the static-protective package on a smooth level surface and then place the component on top of the package.

TS7610 or TS7620 power off sequence

About this task

This is the recommended manual power off sequence for a TS7610 or TS7620 server.

Procedure

1. Attach a keyboard and monitor to the server and access the **ProtecTIER Service Menu**. Log on with the ID **ptconfig** and the password **ptconfig**.
2. In the **ProtecTIER Service Menu**, select the **Manage ProtecTIER Services (...)** option.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
--------------------------------------------------------------------------------
  1) ProtecTIER Configuration (...)
  2) Manage ProtecTIER services (...)
  3) Health Monitoring (...)
  4) Problem Alerting (...)
  5) Version Information (...)
  6) Generate a service report
  7) Generate a system view
  8) Update ProtecTIER code

  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

3. In the **Manage ProtecTIER Services (...)** menu, select **Stop all services**.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassm1
 Manage ProtecTIER Services (...)
--------------------------------------------------------------------------------
  1) Display services status
  2) Start all services
  3) Stop all services
  4) Stop ProtecTIER services only (including GFS)
  5) Stop VTFD service only
  6) Poweroff This Node
  7) Reboot This Node

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

4. When the services are stopped, the system shows the following messages:

```
   Stopping ptrasd                                                [ Done ]
   Stopping vtfd                                                  [ Done ]
   Stopping ptcluster                                             [ Done ]
```

5. Press <enter> to return to the **ProtecTIER Service Menu**.
6. In the **Service Menu**, select **Manage ProtecTIER Services (...)**.
7. In the **Manage ProtecTIER Services (...)** menu, select **Poweroff This Node** to poweroff the server.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassm1
 Manage ProtecTIER Services (...)
--------------------------------------------------------------------------------
  1) Display services status
  2) Start all services
  3) Stop all services
  4) Stop ProtecTIER services only (including GFS)
  5) Stop VTFD service only
  6) Poweroff This Node
  7) Reboot This Node

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

When the power off processes complete, the power LED on the chassis operator panel is off and the monitor screen goes blank.

TS7610 or TS7620 startup

About this task

This is the recommended manual startup sequence for a TS7610 or TS7620 server.

Procedure

1. Verify the power cords are connected to each PSU and secure the cords with the wire bales.

   If the TS7610 or TS7620 chassis is installed within a frame, restore power to the frame by frame's UPO switch or the customer's circuit panel.

2. Press the power button on the TS7610 or TS7620 chassis operator panel to power on the chassis.

   The chassis operator panel has the following buttons and LEDs:

Table 3. Chassis operator panel

1	USB socket
2	Power active
3	Unit fault
4	ID LED
5	On/Off button
6	System reset
7	ID LED switch

   Press the **On/Off** button (5) on the server operator panel.

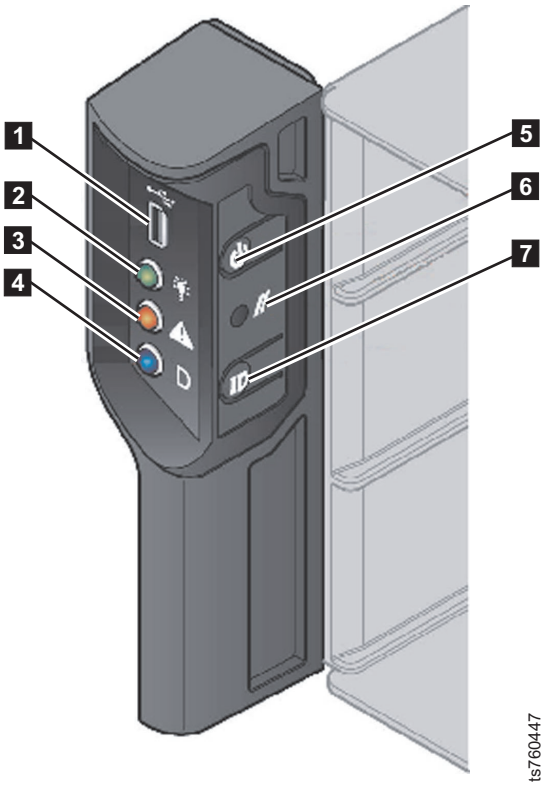


Figure 11. Chassis operator panel

Approximately 15 minutes after the server is powered-on, you will be able to log in to the **ProtecTIER Service Menu**.

3. Attach a monitor and keyboard to the server and access the **ProtecTIER Service Menu**. Log on with the ID **ptconfig** and the password **ptconfig**.
4. In the **ProtecTIER Service Menu**, select the **Manage ProtecTIER Services (...)** option.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
--------------------------------------------------------------------------------
  1) ProtecTIER Configuration (...)
  2) Manage ProtecTIER services (...)
  3) Health Monitoring (...)
  4) Problem Alerting (...)
  5) Version Information (...)
  6) Generate a service report
  7) Generate a system view
  8) Update ProtecTIER code

  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

5. In the **Manage ProtecTIER Services (...)**, select **Display services status**.

CAUTION:
When a hardware component is replaced, a firmware update will automatically start after a reboot or server startup. Please do NOT power off the system during this operation, as interrupting the update may corrupt your system or risk data integrity.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassm1
 Manage ProtecTIER Services (...)
--------------------------------------------------------------------------------
  1) Display services status
  2) Start all services
  3) Stop all services
  4) Stop ProtecTIER services only (including GFS)
  5) Stop VTFD service only
  6) Poweroff This Node
  7) Reboot This Node

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

When the display shows all the services have started, the startup process is complete.

Placing the TS7610 or TS7620 to service position

About this task

To service the internal CRU components, you must place the server in service position. In this position, the server is extended outside of the frame, and is suspended on the slide rails and support tray.

To place the server in service position, follow the procedure below.

Tip: An instructional video of this procedure is available in TS7610 and TS7620 Appliance Express ProtecTIER V3.3.6 Information Center. To access the video, go to: http://pic.dhe.ibm.com/infocenter/ts7600/serv/index.jsp.

Procedure

1. Working from the front of the frame, press the thumb latches on the front of the server downward, to release the catches.
2. Carefully slide the server, tray, and rails, forward, ensuring that no cables are binding or cable tension is exceeded at the back of the server. Continue to slide forward fully until the rails are locked in place. **1** .

   See Figure 12 on page 28.

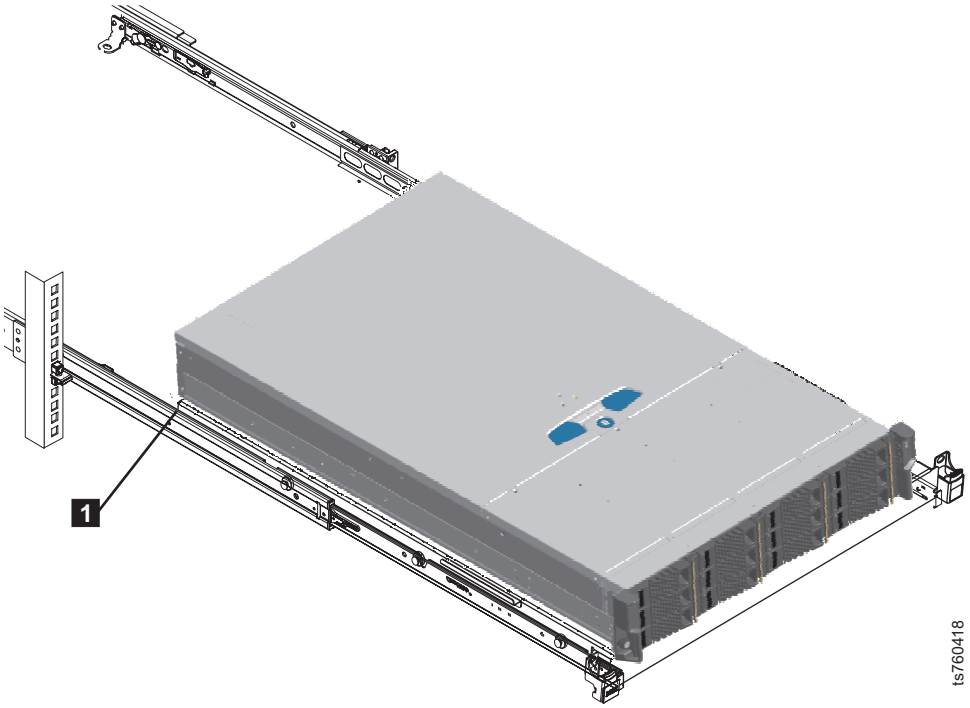


Figure 12. Server extended onto rails

Removing the server's top cover

About this task

With the exception of the cooling fans, you must completely remove the server's top cover to gain access the internal CRUs. There is one locking screw that secure the TS7610 or TS7620 server cover. To do so:

Procedure

Loosen the cover's locking screw **1** 1/4 turn, press the silver button **2** , and slide the cover back and up to remove it **3** . See Figure 13 on page 29.

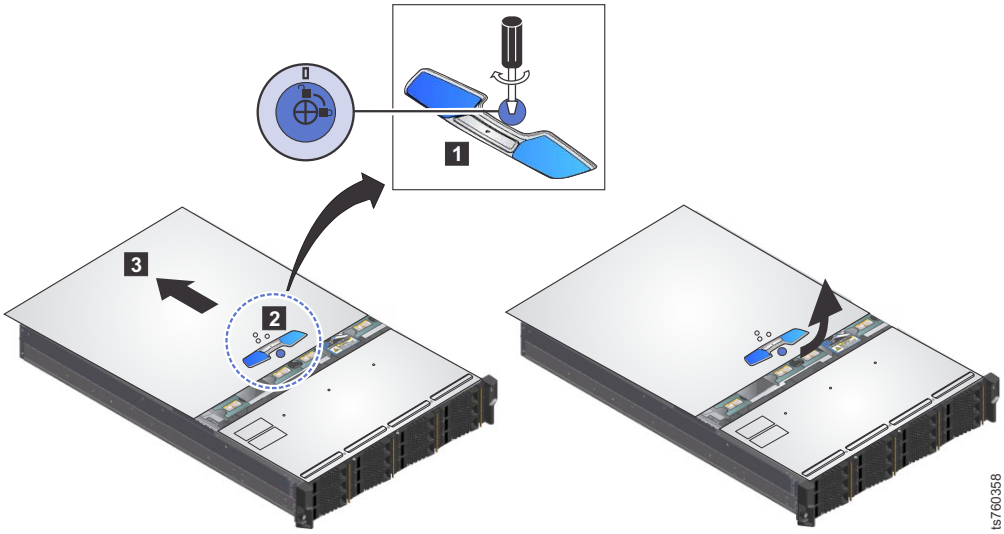


Figure 13. Removing the top cover

Placing the TS7610 or TS7620 to operational position

About this task

Following service, use the procedure below to replace the server's top cover, and return the server to the operational position inside the frame.

Procedure

1. Working from the front of the frame, slide the top cover into place over the chassis **1**.
2. Tighten the cover's locking screw **2**.

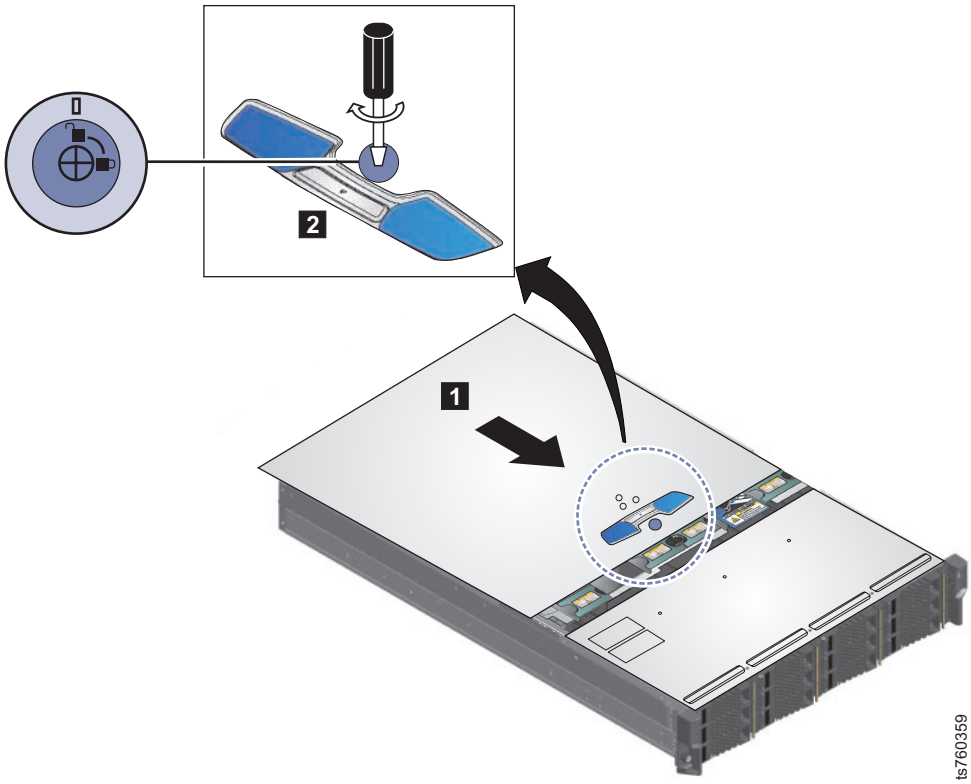


Figure 14. Replacing the top cover

3. Lift up on the blue clips located on the sides of the slide rails, to release the safety catches.
4. Carefully slide the server back into the frame until it is fully retracted and locked into place.

Updating and verifying the TS7610 or TS7620 firmware with the ProtecTIER Service Menu

This procedure explains how to update the firmware for all TS7610 Appliance Express and TS7620 Appliance Express hardware components.

About this task

Firmware automatically updates when the server is rebooted.

Do this procedure if you choose to manually insure that the firmware level of the hardware component is at a level that is supported by your currentProtecTIER server software level.

To perform an update firmware level the TS7610 Appliance Express or TS7620 Appliance Express server must be previously installed and configured.

Procedure

1. If necessary, power-on the server and the monitor, and wait for the login prompt to display.
2. Access the **ProtecTIER Service Menu** with a monitor and keyboard plugged into the TS7610 or TS7620 server. Log on with ID **ptconfig** password **ptconfig**

3. When the **ProtecTIER Service Menu** appears, select the **ProtecTIER Configuration** option.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
--------------------------------------------------------------------------------
  1) ProtecTIER Configuration (...)
  2) Manage ProtecTIER services (...)
  3) Health Monitoring (...)
  4) Problem Alerting (...)
  5) Version Information (...)
  6) Generate a service report
  7) Generate a system view
  8) Update ProtecTIER code

  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

4. Once in the **ProtecTIER Configuration** Menu, select **Update Firmware** to update all the firmware in your TS7610 or TS7620 server.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
 ProtecTIER Configuration (...)
--------------------------------------------------------------------------------
  1) Configure ProtecTIER node
  2) Recover Configuration for a replaced server
  3) Configure enclosure serial number for a replaced enclosure
  4) Update Time, Date, Timezone & Timeserver(s)
  5) Configure replication (...)
  6) IP Network configuration (...)
  7) Update Firmware
  8) Update the System's name
  9) Validate configuration
 10) Single node - code upgrade (For Support Use ONLY)

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

   When the Update Firmware option is selected, the system shows the following prompt:

   ```
   In order to update the Node's firmware level, all the services will be
   stopped. Would you like to update the Node's firmware level? (yes|no)
   ```

5. Type yes and press <enter> to stop all services before updating the firmware.

   Important: Do not power off the server. Powering the server off during a firmware update can damage a hardware component.

6. The firmware version can be viewed through yourProtecTIER Service Menu **Version Information** option. From the Version Information Menu select **Display Firmware Version**

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
 Version Information (...)
--------------------------------------------------------------------------------
  1) Display version information
  2) Display Machine Reported Product Data (MRPD)
  3) Display Firmware Versions

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system

About this task

This is normally a customer installation task. Once the TS7610 or TS7620 hardware is installed, you are ready to perform the software configuration to set up and customize the system for your working environment. In "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" through "Updating customer network settings" on page 38, use **IP Network Configurations** on the **ProtecTIER Configuration Menu**, to update the system and network server settings.

Note: During the configuration procedure, you will be prompted to stop all services. Stopping services will take the system OFFLINE meaning that all current activities will be stopped including critical ones such as Backups and Restores.

If you experience problems during the TS7610 Appliance Express hardware setup or server configuration process, refer to the *IBM TS7610 and TS7620 ProtecTIER Deduplication Appliance Express User's and Maintenance Guide*, v3.3, GA32-0916, on the *IBM TS7610 ProtecTIER Deduplication Appliance Express and IBM TS7620 ProtecTIER Deduplication Appliance Express Publications* CD.

Accessing the ProtecTIER Service Menu

About this task

Procedure

1. If necessary, power on the server and the monitor, and wait for the login prompt to display.
2. With a monitor and keyboard plugged into the TS7610 or TS7620 server. Log on with ID **ptconfig** password **ptconfig**
3. Log in to access the **ProtecTIER Service Menu**. Select the **ProtecTIER Configuration** option.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
--------------------------------------------------------------------------------
  1) ProtecTIER Configuration (...)
  2) Manage ProtecTIER services (...)
  3) Health Monitoring (...)
  4) Problem Alerting (...)
  5) Version Information (...)
  6) Generate a service report
  7) Generate a system view
  8) Update ProtecTIER code

  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

4. Once in the **ProtecTIER Configuration** Menu, select **Update Time, Date, Timezone & Timeserver(s)** to set your server Time, Date, Timezone & Timeserver(s).

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
 ProtecTIER Configuration (...)
--------------------------------------------------------------------------------
  1) Configure ProtecTIER node
  2) Recover Configuration for a replaced server
  3) Configure enclosure serial number for a replaced enclosure
  4) Update Time, Date, Timezone & Timeserver(s)
  5) Configure replication (...)
  6) IP Network configuration (...)
  7) Update Firmware
  8) Update the System's name
  9) Validate configuration
 10) Single node - code upgrade (For Support Use ONLY)

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

5. Go to "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32.

Setting the timezone

Use the procedures in this task to change the time zone setting to match that of your location. *You must set the timezone to ensure accurate system timekeeping*.

Before you begin

If either of the following conditions is true, skip this task and "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32, and go directly to "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32:

- You have an FSI system on which you plan to implement Active Directory user authentication. A time server is *required* for this configuration.
- You want to use a network time server to simultaneously synchronize the time, date, and timezone settings on all of your TS7620 Appliance Express servers, regardless of their configuration type.

Otherwise, proceed as directed in the steps that follow.

Important: With Version 3.3.6 and later, you must apply each change you make to the timezone, date and time, and time server individually before proceeding to the next task.

Procedure

1. On the **ProtecTIER Configuration (...)** menu (see "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32), select the **Update Time, Date, Timezone & Timeserver(s)** option. Type the corresponding number for this selection and press Enter.

   The **Date, Time, Timezone & Timeserver(s) configuration** menu, displays:

Figure 15. Date, Time, Timezone & Timeserver(s) configuration menu

Note: To prevent selections from scrolling off the screen, consider setting the paging to show fewer lines of information.

2. Select the **Set Timezone** option. Type the corresponding number and press Enter.
3. If you are in the United States, when prompted for a country code, type: `US` and press Enter.

   For locations outside the United States, you must enter an international country code. Refer to Worldwide time zone codes to locate your information, then return to this task and enter the appropriate country code in step "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32.

   The time zones for the specified country display. A sample of the US time zones list is shown in "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32:

```
Time zones under US:
====================

1. America/New_York
2. America/Detroit
3. America/Kentucky/Louisville
4. America/Kentucky/Monticello
5. America/Indiana/Indianapolis
6. America/Indiana/Vincennes
7. America/Indiana/Winamac
8. America/Indiana/Marengo
9. America/Indiana/Petersburg
10. America/Indiana/Vevay
11. America/Chicago
12. America/Indiana/Tell_City
13. America/Indiana/Knox
14. America/Menominee
15. America/North_Dakota/Center
16. America/North_Dakota/New_Salem
17. America/Denver
18. America/Boise
19. America/Shiprock
20. America/Phoenix
21. America/Los_Angeles
22. America/Anchorage
23. America/Juneau
24. America/Yakutat
25. America/Nome
26. America/Adak

Press <Enter>

27. Pacific/Honolulu

Please choose a timezone:
```

Figure 16. Sample of US time zones

4. If the `Press enter to continue` prompt displays, the time zone list is too long to display on the screen at once. Press Enter to advance the list.
5. At the `Please choose a timezone:` prompt, type the number that corresponds to your timezone and press Enter to return to the **Date, Time, Timezone & Timeserver(s) configuration** menu. Type: `c` for commit and press Enter.

   The current time, date, and timezone settings display for review.
6. At the `Do you wish to apply those settings? (yes|no)` prompt, type: `yes` and press Enter.

   The following message appears: `The cluster & VTFD services on all nodes must be stopped in order to continue. Do you wish to continue? (yes|no).` Type: `yes` and press Enter.

A series of status messages appears as the services are stopped and restarted. This process might take up to 10 minutes. When the service restart is complete, the `Press the ENTER key to continue...` message appears.

7. Press Enter to continue and return to the **ProtecTIER Configuration (...)** menu.

What to do next

If you are not planning to connect to a time server:

Leave the menu open and go on to "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32.

If you are connecting to a time server or this is an FSI system on which you plan to implement active directory user authentication:

Leave the menu open and go on to "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32.

Setting the date and time

Each server contains a battery that must be calibrated.

About this task

Use the procedures in this task to check the time and date on the server. If necessary, change the settings to match the time and date at your location.

Important: With Version 3.3.6 and later, you must apply each change you make to the timezone, date and time, and time server individually before proceeding to the next task.

Procedure

1. On the **ProtecTIER Configuration (...)** menu (see "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32), select the **Update Time, Date, Timezone & Timeserver(s)** option. Type the corresponding number for this selection and press Enter.

   The **Date, Time, Timezone & Timeserver(s) configuration** menu, displays:

2. On the **Date, Time, Timezone & Timeserver(s) configuration** menu (see "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32), select the **Set date & time** option. Type the corresponding number and press Enter.
3. When prompted for the date:
   - If the default date [displayed in brackets] is correct, press Enter.
   - If the default date is incorrect, type the current date in DD/MM/YYYY format and press Enter. For example, `09/01/2012`.
4. When prompted for the time:
   - If the default time [displayed in brackets] is correct, press Enter.
   - If the default time is incorrect, type the current time in HH:MM:SS format and press Enter. For example:`08:32:58`.
5. At the `Please choose:` prompt, commit your date and time settings To commit, type: `c` and press Enter.

   The current time, date, and timezone settings display for review.
6. At the `Do you wish to apply those settings? (yes|no)` prompt, type: `yes` and press Enter.

You are notified as follows: `The cluster & VTFD services on all nodes must be stopped in order to continue. Do you wish to continue? (yes|no).` Type: `yes` and press Enter.

A series of status messages appears as the services are stopped and restarted. This process might take up to 10 minutes. When the service restart is complete, the `Press the ENTER key to continue...` message displays.

7. Press Enter to continue and return to the **ProtecTIER Configuration (...)** menu.
8. Skip "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32. Leave the menu open and go on to "Updating the System Name" on page 37.

Specifying a time server

Each server contains a battery that must be calibrated.

About this task

If you have an FSI system on which you plan to implement Active Directory user authentication, you must complete this task. Failure to do so will cause your FSI configuration to fail.

If you already completed "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32 and "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32, skip this task and go directly to "Updating the System Name" on page 37.

Important: With Version 3.3.6 and later, you must apply each change you make to the timezone, date and time, and time server individually before proceeding to the next task.

Procedure

1. Before you start this task, proceed as appropriate:
   - If you already know the IP address of the primary (and optionally, secondary) time server you plan to use, go on to step "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32.
   - Otherwise, do the following:
     a. Locate a primary (and optionally, secondary) time server. There are many websites (for example, `http://www.ntp.org/`) which provide lists of time servers available for public use.
     b. After selecting one or more time servers, make note of the IP addresses on your Pre-Installation Checklist.
     c. Go on to step "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32.
2. On the **ProtecTIER Configuration (...)** menu (see "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32), select the **Update Time, Date, Timezone & Timeserver(s)** option. Type the corresponding number and press Enter.

   The **Date, Time, Timezone & Timeserver(s) configuration** menu, see "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32, displays.

   Note: Selecting this menu option will allow entry of a timeserver's IP address, and also include an option for a backup timeserver IP.

3. Select the **Set Timeserver(s)** option. Type the corresponding number and press Enter.
4. When prompted, type the IP address of the primary network timeserver and press Enter.

   Refer to your completed Pre-installation Checklist for the IP address of the primary network timeserver.
5. At the `Would you like to set a secondary timeserver? (yes|no)` prompt, type: `yes` or `no`, as appropriate.
   - If you typed `yes`, type the IP address of the secondary network timeserver at the prompt, press Enter, and go to step "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32.

     Refer to your completed Pre-installation Checklist for the IP address of the secondary network timeserver.
   - If you typed `no`, go to step "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32.
6. At the `Do you wish to apply those settings? (yes|no)` prompt, type: `yes` and press Enter.

   You are notified as follows: `The cluster & VTFD services on all nodes must be stopped in order to continue. Do you wish to continue? (yes|no).` Type: `yes` and press Enter.

   A series of status messages displays as the services are stopped and restarted. This process can take up to 10 minutes. When the service restart is complete, the `Press the ENTER key to continue...` message displays.
7. Press Enter to continue and return to the **ProtecTIER Configuration (...)** menu.
8. Leave the menu open and go on to "Updating the System Name."

Updating the System Name

About this task

In this task, you will specify the unique system name that will be used to identify the TS7610 Appliance Express server in the ProtecTIER Manager graphical user interface (GUI).

Procedure

1. On the **ProtecTIER Configuration Menu** ("Accessing the ProtecTIER Service Menu" on page 32), select option 2, **Update System's Name**. Type: **8** and press **<enter>**.

   A series of status messages display:
2. At the **Please enter a new system name [pt_system]: prompt**, type the name you want to use to identify the TS7610 Appliance Express server and press **<enter>**.

   Additional status messages display as the system name is updated.
3. When the update is complete, and the **Press the ENTER key to continue...** message displays, press **<enter>**. You are returned to the **ProtecTIER Configuration Menu**.
4. Go to "Updating customer network settings" on page 38.

Updating customer network settings

About this task

In this task, you will provide your network IP address, netmask address, default gateway, and hostname; information.

Procedure

1. On the **ProtecTIER Configuration Menu** ("Accessing the ProtecTIER Service Menu" on page 32), select option **6**, **IP Network configuration**. Type: **3** and press **<enter>**.

   A series of status messages similar to the following, display:

   ```
   Starting cluster, please wait...
   Starting cluster
   Cluster started
   ```

2. When the `Would you like to stop the vtfd service (yes/no)` prompt displays, type: **y <enter>**.

   The `Stopping vtfd` message displays.

3. At each of the prompts listed below, provide the information requested (or leave the field blank to use the defaults within the brackets) and press **<enter>**.

   ```
   Customer Network, IP Address [192.168.167.161]:
   Customer Network, Netmask [255.255.255.0]:
   Customer Network, Default Gateway:
   Customer Network, Hostname [node1]:
   ```

   (For the Hostname, enter the same name that you specified in "Updating the System Name" on page 37, step 2 on page 37, above.)

   A series of status messages display as the services are stopped and restarted and the network settings are configured. This process may take up to 10 minutes. When the service restart is complete, the `Press the ENTER key to continue...` message displays.

4. When the update is complete, and the `Press the ENTER key to continue...` message displays again, press **<enter>**. You are returned to the **ProtecTIER Configuration Menu**.

5.

6. In the **Service Menu**, select **Manage ProtecTIER Services (...)**.

7. In the **Manage ProtecTIER Services (...)** menu, select **Poweroff This Node** to poweroff the server.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassm1
 Manage ProtecTIER Services (...)
--------------------------------------------------------------------------------
  1) Display services status
  2) Start all services
  3) Stop all services
  4) Stop ProtecTIER services only (including GFS)
  5) Stop VTFD service only
  6) Poweroff This Node
  7) Reboot This Node

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

When the power off processes complete, the power LED on the chassis operator panel is off and the monitor screen goes blank.

When the reboot completes you are returned to the login prompt. You are now done replacing you chassis FRU.

Chapter 3. Servicing TS7610 or TS7620 components

This section contains tables of the CRU or FRU hardware components information of the TS7610 or TS7620 Appliance Express, graphics that show the location of components and replacement procedures for each of the hardware components.

TS7610 and TS7620 Appliance Express ProtecTIER V3.3.6 Parts list and hardware component replacement

This section displays the TS7610 Appliance Express and TS7620 Appliance Express chassis and hardware component layout.

Before you begin, take time to review the following information:

- About the TS7610 or TS7620 hardware
- Powering-on the server
- Electrostatic discharge procedure
- How to verify a hardware fault before servicing the component by running a **Health check** through the ProtecTIER Manager Service menu, refer to "Health Monitoring" on page 15 or through ProtecTIER Manager **Hardware resources**, refer to the Figure 7 on page 9.

The TS7610 Appliance Express, ProtecTIER V3.3.6 (SM1) supports either VTL or OpenStorage depending on the servers hardware configuration.

The TS7620 Appliance Express, ProtecTIER V3.3.6 (SM2) supports either VTL, OpenStorage or FSI depending on the servers hardware configuration.

There are two hardware component tables below, one for TS7610 (SM1) and the other for TS7620 (SM2). Each hardware component listed in the tables below is installed in, or connected to their TS7610 or TS7620 server. The components are categorized according to the following criteria:

- **Customer replaceable unit (CRU) vs. Field replaceable unit (FRU) –** Components that can safely and easily be self-serviced by the customer are CRU components. Components for which removal and replacement requires a higher degree of technical expertise and system knowledge are FRU components, and are to be serviced by IBM personnel, only.
- **Internal vs. External –** Internal components are located inside the server chassis, and are accessible only if the servers top cover is removed. External components are accessible with the servers cover in place.
- **Hot-swappable vs. Cold-swappable –** Hot-swappable components do not require stopping input/output (I/O) activity or disconnecting the server from A/C power before removing or replacing the component. Cold-swappable components cannot be removed or replaced while the system is running. I/O must be stopped and the server must be disconnected from the A/C power source before removal or replacement is started.

  Attention: Failure to adhere to the above guidelines could result in component or system damage, data loss, or personal injury.
- **FRU ID –** Each component has a unique FRU ID (part number). The customer schedules a service call for a FRU and provides the FRU ID to you, the IBM customer support representative.

Note: The FRU IDs in this table may become outdated after this document is produced. It is recommended that you first try to locate FRU IDs through one of the resources discussed in "Interpreting hardware alerts" on page 1.

Failure to follow the guidelines and procedures in the mentioned sections may result in component or system damage or personal injury.

The hardware differences between VTL, FSI and OpenStorage SM2 servers are:

- The VTL version is the only ProtecTIER 3959 server that has a Fibre channel, Emulex HBA.
- The VTL version is the only ProtecTIER 3959 server that has one Intel Dual-port Ethernet adapter.
- The OpenStorage and FSI versions of the ProtecTIER server has two Intel Dual-port Ethernet adapters.
- The OpenStorage and FSI versions of the ProtecTIER server has a Quad-port Ethernet adapter.

Table 4. VTL, FSI and OpenStorage ***3959 SM2*** *component categories and FRU IDs*

Component name / hardware name if listed in the ProtecTIER Manager GUI Hardware Resources view	**Quantity**	**CRU**	**FRU**	**Internal**	**External**	**Hot-swappable**	**Cold-swappable**	**FRU ID (Part number)**
Quad Port Ethernet Adapter installed in the SM2 FSI or OST base unit for replication	1		■	■			■	49Y4242
CMOS coin battery	1		■				■	33F8354
2TB NL LFF 3.5″ SAS hard disk drives (HDDs) **/ Disk drive**	12	■			■	■		98Y2420
Power supply units (PSUs) **/ Power supply**	2	■			■	■		98Y3253
Cooling fans **/ Cooling module**	10	■		■		■		45W8018
RAID Battery Backup Unit (BBU battery and adapter card) **/ RAID battery**	1	■		■			■	35P1271
BBU (RAID) replacement battery only (iBBU08)	1	■		■			■	35P2359
DIMM (8GB Dual in-line memory modules) **/ Memory module**	6	■		■			■	35P1121
USB Drive (portable DVD drive)	1	■			■	■		95P9229
Intel Dual-port Ethernet adapter - • one ethernet card for VTL SM2 • two ethernet cards for OST or FSI SM2 **/Ethernet port 0-7**	1 or 2	■		■			■	49Y4232
Fibre channel, Emulex HBA- only VTL SM2	1		■	■			■	42D0500
LSI MegaRAID SAS9280-4i4e (Repository RAID) **/ SAS Expander**	1		■	■			■	35P1368
LSI MegaRAID SAS9240-4i (Boot RAID) **/ RAID card**	1		■				■	35P1369
Seagate 500GB SFF 2.5″ SATA (internal boot drives) **/ Boot drive**	2		■	■			■	35P1193

Table 4. VTL, FSI and OpenStorage **3959 SM2** *component categories and FRU IDs (continued)*

Component name / hardware name if listed in the ProtecTIER Manager GUI Hardware Resources view	**Quantity**	**CRU**	**FRU**	**Internal**	**External**	**Hot-swappable**	**Cold-swappable**	**FRU ID (Part number)**
3959 SM2 MECH ASM (chassis, SAS EXPANDER CARD, ONBOARD ETH CARD, and CPU) **/ CPU , SAS Expander, Ethernet port (On board)**	1		■	■	■		■	00V6991
Power cable - do not use the wire bail if it does not fit over the cable.	2	■			■		■	46X6880
Boot CAGE (Dual Boot Drive Cage Assembly)	1		■	■			■	35P1190
Mounting Tray (support tray)	1	■		■			■	46X1946
AIRDUCT, Air Flow (plastics, 2 parts)	1	■		■		■		35P1191
RAID-SAS Expander mini-SAS cable	1		■	■			■	00V7085
Boot Drive SAS Cable	1		■	■			■	35P1192
Slide Rails for Tray (No Screws)	1	■			■		■	69Y5085
Cable Management Arm	1	■			■	■		49Y4817

Table 5. TS7620 Appliance Express 3959-EXP 11.5 expansion drawer component categories and FRU IDs

Component name / hardware name if listed in the ProtecTIER Manager GUI Hardware Resources view	**Quantity**	**CRU**	**FRU**	**Internal**	**External**	**Hot-swappable**	**Cold-swappable**	**FRU ID (Part number)**
PWR SUPPLY and Power Cooling Module **/ Power supply (99Y1243) or Cooling module(45W8018)**	2	■			■	■		00L4605
CABLE - SAS 1x to 2x	1	■			■		■	35P2255
HARD DRIVE - carrier w/HDD **/ Disk drive**	12	■			■	■		98Y2420
CHASSIS (the chassis base assembly includes the **SAS Expander (35P2384)**)	1	■			■		■	35P3465
ESM (Enclosure SAS module) Canister **/Canister**	2	■			■	■		35P2384
CABLE POWER (2.8M IEC 320-C13)	2	■			■		■	46X2536
CABLE POWER (2.8M NEMA C-13)	2	■			■		■	46X6880
RAIL KIT (Rail kit for EXP)	1	■			■		■	85Y5852
SAS CABLE 1 to 1	2	■			■		■	44V4041

Table 6. VTL, FSI and OpenStorage **3959 SM1** *component categories and FRU IDs*

Component	**Quantity**	**CRU**	**FRU**	**Internal**	**External**	**Hot-swappable**	**Cold-swappable**	**FRU ID (Part number)**
CMOS coin battery	1		■				■	33F8354
1TB SATA hard disk drives (HDDs)	12	■			■	■		45W8867
Power supply units (PSUs)	2	■			■	■		98Y3253
Cooling fans	10	■		■		■		45W8018
RAID battery backup unit (BBU)	1	■		■			■	46X2051

Table 6. VTL, FSI and OpenStorage **3959 SM1** *component categories and FRU IDs (continued)*

Component	Quantity	CRU	FRU	Internal	External	Hot-swappable	Cold-swappable	FRU ID (Part number)
4GB Dual in-line memory modules (DIMMs)	6	■		■			■	45W7764
USB portable DVD drive	1	■			■	■		46X4472
Dual-port Ethernet adapter - • one ethernet card for VTL SM1 • two ethernet cards for OST SM1	1 or 2	■		■			■	39Y6128
Fibre channel host bus 4GB adapter (HBA) or Fibre channel host bus 8GB adapter (HBA)	1		■	■			■	43W7512 or 42D0500
LSI MegaRaid SAS8888ELP	1		■	■			■	46X6759
300GB HDDs (internal boot drives)	2		■	■			■	49Y1840
3959 SM1 chassis (SAS EXPANDER CARD, ONBOARD ETH CARD, and CPU)	1		■	■	■		■	46X1944
Power cable- this cable accommodates the wire bail on the power supply, the previous version 39M5081 did not.	2	■			■		■	46X6880
Dual Boot Drive Cage Assembly	1		■	■			■	46X2434
Mounting Tray (support tray)	1	■		■			■	46X1946
Air Flow plastics (all 3)	1	■		■			■	46X2032
RAID-SAS Expander mini-SAS cable	1		■	■			■	46X2700
Fan tray	1		■	■			■	46X2033
Rails for Tray (No Screws)	1	■			■		■	49Y4817

When a hardware fault occurs on a component that is one of a set, as in the case of the HDDs (hard disk drives), PSUs (power supply units), cooling fans, and DIMMs; you must isolate the specific component (*for example, HDD 5*) that generated the fault, and diagnose the cause and severity of the problem. Refer to the figures below to see how the HDDs, cooling fans, adapters, DIMMs, and PSUs; are arranged and numbered. In the case of the DIMMs, only six of the eight slots (A1, A2, B1, B2, C1, and D1) are used. Slots C2 and D2 are left empty.

- **1** : cooling fans
- **2** : boot drive assembly
- **3** : sysplanar
- **4** : pci card adapters
- **5** : power supplies
- **6** : SAS expander

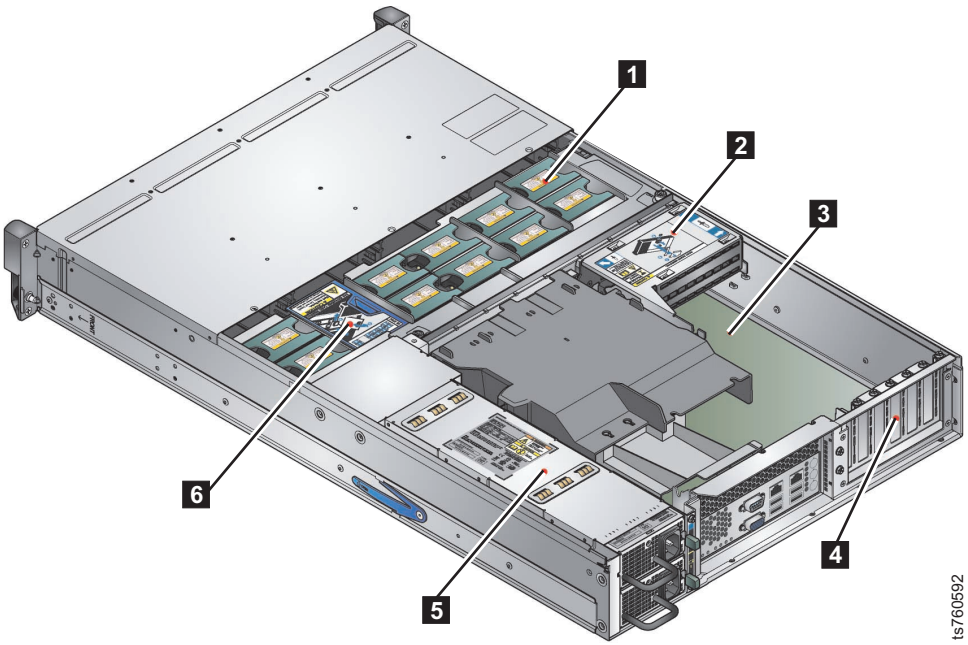


Figure 17. Chassis top view

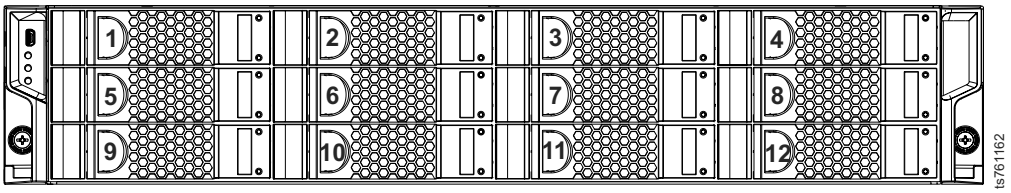


Figure 18. HDD layout

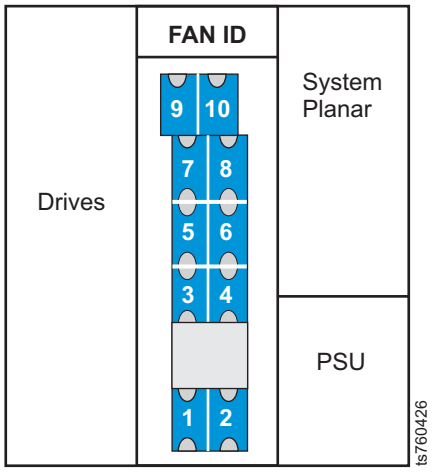


Figure 19. Cooling fan layout

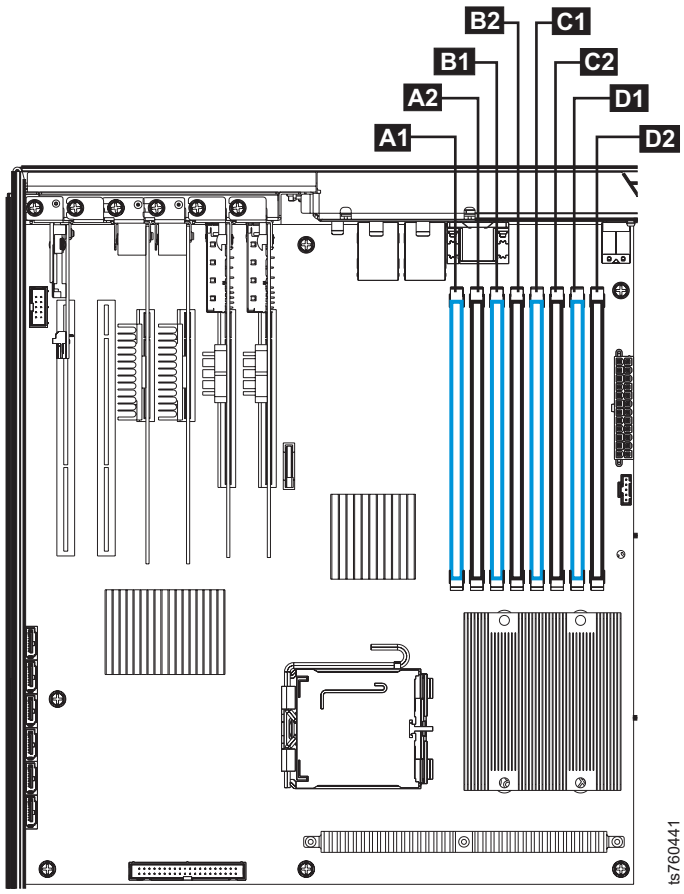


Figure 20. DIMM layout

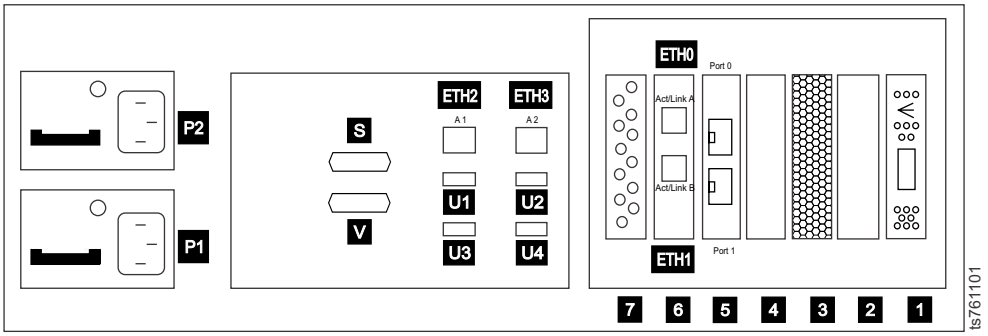


Figure 21. **3959 SM2** *server for VTL Systems rear view*

Table 7. **3959 SM2** *server for VTL Systems slot assignments, ports, and connectors*

P2 Power supply 2	**7** RAID Battery Backup Unit (BBU)
P1 Power supply 1	**6** **ETH0** (Act/Link A) port: LAN **ETH1** (Act/Link B) port: Replication
S RS-232 serial port	**5** Fibre Channel Adapter
V Video port	**4** Unused (Empty)

Table 7. **3959 SM2** *server for VTL Systems slot assignments, ports, and connectors (continued)*

ETH2 (A1) on-board (Port 0) Ethernet port: Replication	**3** Boot Drive MegaRAID Controller
ETH3 (A2) on-board (Port 1) Ethernet port: LAN	**2** Unused (Empty)
U USB ports: Upper left = 1, upper right = 2, lower left = 3, lower right = 4	**1** SAS Expander (for expansion units)

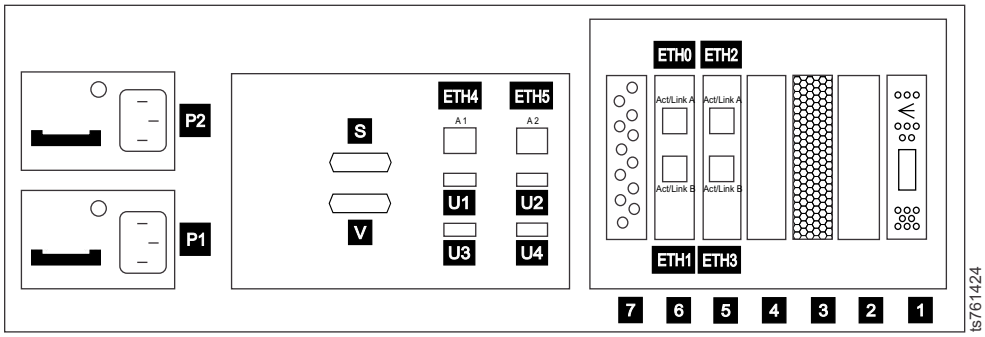


Figure 22. **3959 SM2** *server for OpenStorage or FSI Systems rear view*

Table 8. **3959 SM2** *server for OpenStorage or FSI systems slot assignments, ports, and connectors*

P2 Power supply 2	**7** RAID Battery Backup Unit (BBU)
P1 Power supply 1	**6** **ETH0** (Act/Link A) port: LAN **ETH1** (Act/Link B) port: Replication
S RS-232 serial port	**5** **ETH2** (Act/Link A) port: OpenStorage or FSI **ETH3** (Act/Link B) port: OpenStorage or FSI
V Video port	**4** **ETH4** (Act/Link A) port: replication **ETH5** (Act/Link B) port: replication **ETH6** (Act/Link C) port: replication **ETH7** (Act/Link D) port: replication
ETH4 (A1) On-board (Port 0) Ethernet port: Replication	**4** Unused (Empty)
ETH5 (A2) On-board (Port 1) Ethernet port: LAN	**3** Boot Drive MegaRAID Controller
U USB ports: Upper left = 1, upper right = 2, lower left = 3, lower right = 4	**2** Unused (Empty)
	1 SAS Expander (for expansion units)

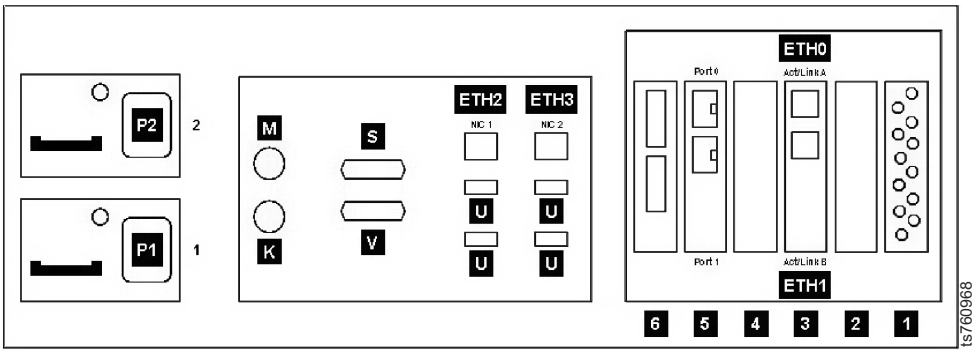


Figure 23. **3959 SM1** *server for VTL Systems rear view*

Table 9. **3959 SM1** *server for VTL Systems slot assignments, ports, and connectors*

2 Power supply 2	**U** USB ports: Upper left = 1, upper right = 2, lower left = 3, lower right = 4
1 Power supply 1	**6** MegaRAID Controller
M PS/2 mouse port	**5** Fibre Channel Adapter
K PS/2 keyboard port	**4** Unused (Empty)
S RS-232 serial port	**3** Ethernet Adapter **ETH0** (Act/Link A) port: LAN **ETH1** (Act/Link B) port: Replication
V Video port	**2** Unused (Empty)
ETH2 (NIC 1) on-board Ethernet port: Replication	**1** RAID Battery Backup Unit (BBU)
ETH3 (NIC 2) on-board Ethernet port: LAN	

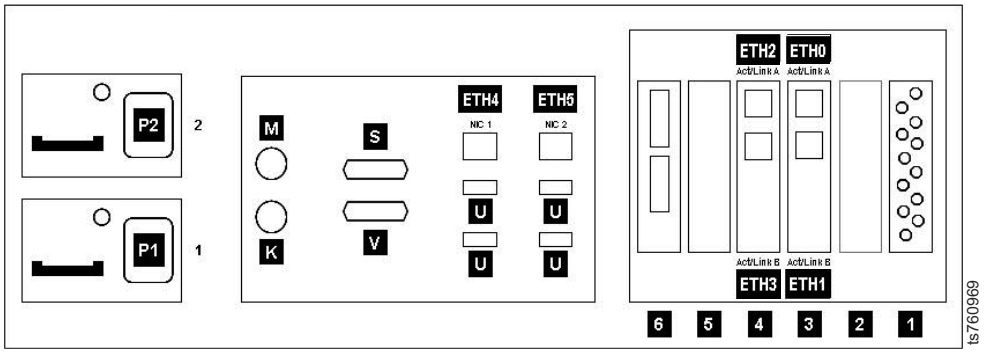


Figure 24. **3959 SM1** *server for OpenStorage Systems rear view*

Table 10. **3959 SM1** *server for OpenStorage Systems slot assignments, ports, and connectors*

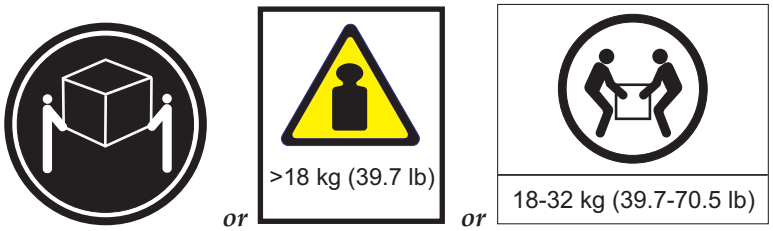
2 Power supply 2	**U** USB ports: Upper left = 1, upper right = 2, lower left = 3, lower right = 4
1 Power supply 1	**6** MegaRAID Controller
M PS/2 mouse port	**5** Unused (Empty)

Table 10. **3959 SM1** *server for OpenStorage Systems slot assignments, ports, and connectors (continued)*

K PS/2 keyboard port	**4** Ethernet Adapter **ETH0** (Act/Link A port): LAN **ETH1** (Act/Link B port): Replication
S RS-232 serial port	**3** Ethernet Adapter **ETH2** (Act/Link A port): OpenStorage **ETH3** (Act/Link B port): OpenStorage
V Video port	**2** Unused (Empty)
ETH4 (NIC 1) On-board Ethernet port: Replication	**1** RAID Battery Backup Unit (BBU)
ETH5 (NIC 2) On-board Ethernet port: LAN	

The TS7610 or TS7620 ProtecTIER V3.3.6 chassis

CAUTION:



or *or*

The weight of this part or unit is between 18 and 32 kg (39.7 and 70.5 lb). It takes two persons to safely lift this part or unit. (C009)

A fully loaded TS7610 or TS7620 ProtecTIER V3.3.6 chassis weighs over 40 lbs which will require two people to move. The following procedure explains how to safely replace a defective chassis alone.

TS7610 and TS7620 Appliance Express ProtecTIER V3.3.6 Chassis FRU Removal and Replacement

The following procedure explains how a service person, working alone, can safely remove and replace the chassis without lifting anything over 18 kg (39.7 lbs.).

Before you begin

Before starting, you will need the following:

- a chassis FRU (Field Replacement Unit)
- a monitor connected to the TS7610
- a keyboard connected to the TS7610
- labels on all the cables connected to the TS7610
- a work surface or work surfaces where you can set aside two power supplies, 12 1TB HDD drives and a defective chassis.
- ESD strap
- a phillips head screwdriver
- pliers

Important: When a Chassis FRU is removed, the chassis also includes the following hardware subcomponents: sysplanar (motherboard) and 2.33Ghz central processing unit (CPU); DASD backplane; air flow control, air flow cover, and brace assembly; DIMMS; RAID SAS expander card and RAID SAS expander mini-cable.

This procedure ensures any hardware you lift will be under 18 kg (39.7 lbs.).

Procedure

1. Verify all external cables are labeled. If they are not, label them at this time for correct placement later.
2. Power off the TS7610 or TS7620 server. Refer to "TS7610 or TS7620 power off sequence" on page 23. Once power has turned off unplug the two power cables from the power supplies.
3. Remove all external cables.
4. Refer to Figure 25.

   Important: Label the 1TB HDDs from 0 to 11. This is to ensure that each HDD will be inserted into the same corresponding location in the replacement chassis. Once the HDDs are labeled, move the HDDs to the work surface.

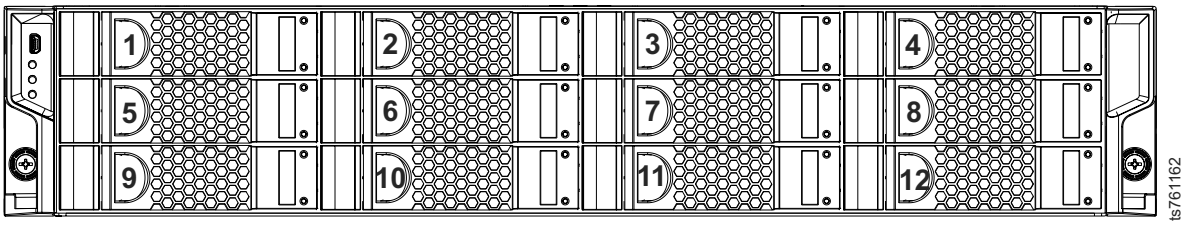


Figure 25. HDD position order

5. Remove the power supplies from the defective chassis and set them aside on the work surface. Once the power supplies are removed, the defective chassis will be below the 40 lb. weight limit.
6. To place the TS7610 or TS7620 server into the service position, push the front tab and pull the slide rails and support tray forward, until the rails are fully extended and click into the locked position **1** . Refer to Figure 26 on page 51

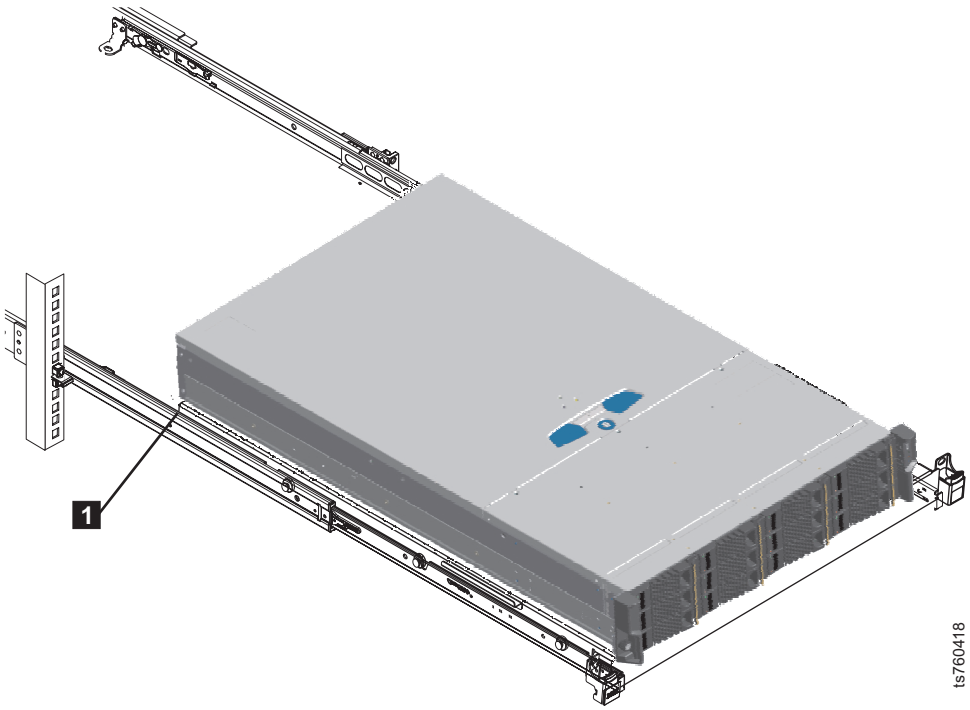


Figure 26. Extending the slide rails and support tray

7. Refer toFigure 27. Loosen the center thumbscrew on the rear of the tray.

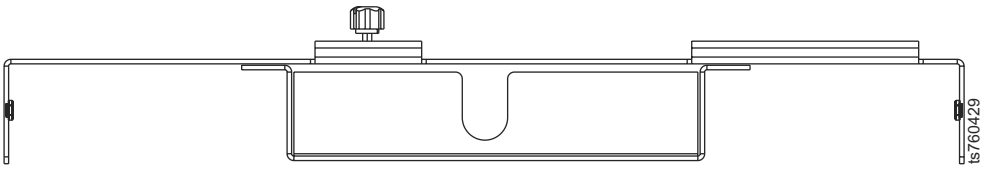


Figure 27. Center thumbscrew

8. Move the defective chassis to the work surface.
9. Remove the covers from both the defective chassis and the replacement chassis. Refer to Figure 28 on page 52. **1** Loosen the cover's holding screw 1/4 turn clockwise. **2** Press the silver button and **3** slide the cover back and up to remove it.

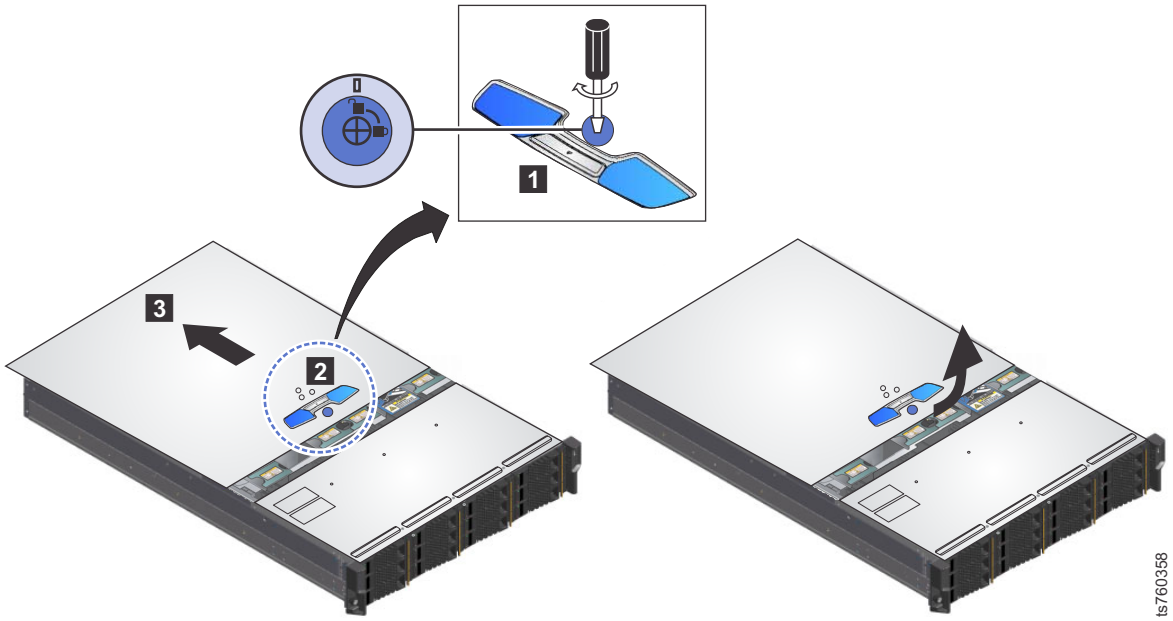


Figure 28. Removing server cover

10. Refer to Figure 29. Remove the **1** baffle and than the **2** L-shaped plastic covers.

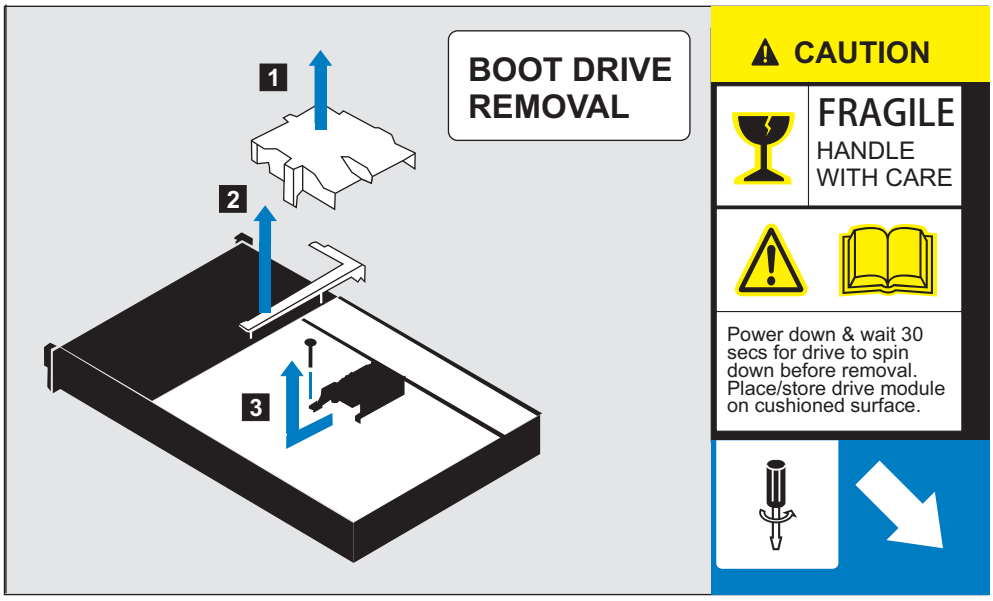


Figure 29. Boot cage label

11. Remove Boot Drive Assembly (with boot drives in the cage).

    You will be handling two boot drive cages, an empty boot drive cage from the replacement chassis and a populated boot drive cage from the defective chassis. The following instructions explains how to remove the boot cages and replace them.

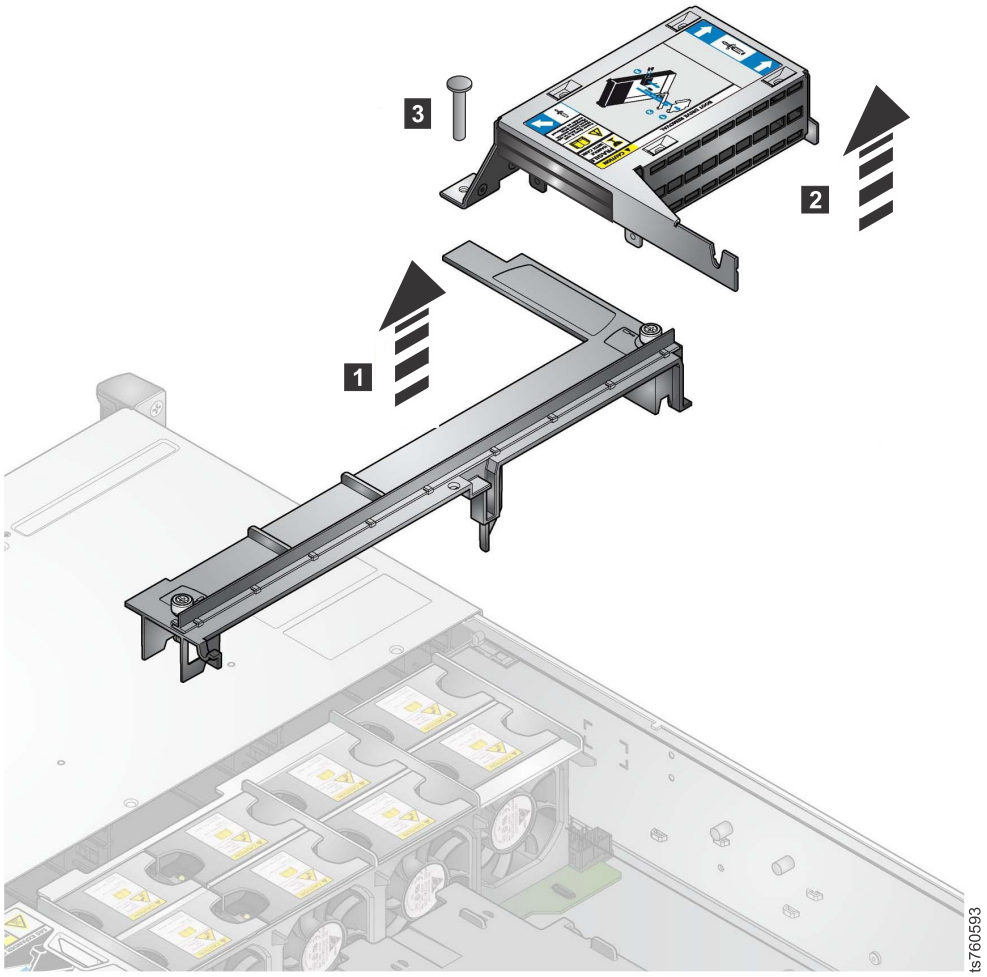


Figure 30. Air baffle and boot drive assembly

a. There are two boot drive cages, one in the defective chassis and one in the replacement chassis. Do this for both boot cage drives. Refer to Figure 29 on page 52. The caution label also show the three mounting points holding the boot drive cage in place. These have rubber shock absorbers around them. With a phillips head screwdriver, **2** remove the single upright screw holding the boot drive cage down. To remove the retention screw, you may need pliers to hold the post stationary while removing the screw.

b. Do this for both boot drive cages. Carefully pull the boot drive assembly toward the center of the chassis and parallel to the chassis sysplanar until the boot drive assembly is pulled off of the two mounting pins on the inside wall of the chassis.

c. From here on the procedure is for the populated boot drive cage unless other wise noted. The top of the boot drive cage has the caution label. The drive closest to the boot cage caution label is the top drive. The other drive is the bottom drive. Lift the boot drive cage away from the chassis and turn it over to look at the bottom side of the cage.

d. There are two flat SATA cables and one power cable connecting to the small backplane (of the boot drive assembly) to the sysplanar (of the chassis). The two flat SATA cables are connected side by side on the sysplanar board of the chassis. If the SATA cables are not labeled, mark the cables left or right to indicate their placement on the sysplanar board.

e. Also mark on the SATA cables to indicate if they are connected to the bottom connector or top connector of the backplane board (of the boot drive assembly). This will help ensure the same boot drive cable reconnection in the replacement chassis.

f. Unplug the two flat SATA cables extending down from the boot drive cage to the sysplanar and than unplug the power cable from the backplane.

g. Remove the whole boot drive assembly.

12. Install the Boot Drive Assembly just removed from the failing chassis into the replacement chassis. Also install the empty boot drive cage into the defective chassis to return back to IBM.

    a. Connect the two SATA cables and one power cable connecting to the backplane (of the boot drive assembly) to the sysplanar in the replacement chassis.

    b. Slide the boot drive assembly on the two mounting pins on the inside wall of the replacement chassis.

    c. With a screwdriver, screw in the single upright screw to secure the boot drive cage to the sysplaner.

13. Unplug the connection cord between the battery card and the MegaRaid card. You will than be able to move BBU(LSI Battery) to the replacement chassis.

14. Move the fibre channel adapter (Emulex HBA card) to the replacement chassis. Refer to "Removing and replacing the TS7610 or TS7620 ProtecTIER V3.3.6 fibre channel adapter" on page 73.

15. Move the Ethernet adapter (Intel Nic card) to the replacement chassis. Refer to "Removing and replacing the Ethernet adapter" on page 92.

16. Move the MegaRAID(LSI 8888ELP) card. Refer to "Removing and replacing the LSI MegaRAID SAS9280-4i4e, 12 HDD RAID card respository control (for TS7620) or LSI MegaRaid SAS8888ELP repository controller(for TS7610)" on page 78.

17. Refer to Figure 29 on page 52. Put the **2** L-shaped and the **1** baffle plastic covers back on.

    Important: The WWN sticker is attached to the plastic air baffle, so the original air baffle must be taken from the defective chassis, and put into the replacement chassis.

18. Put the server tray covers back on.

19. Install the chassis replacement unit onto the server tray. Slide the chassis under the side hinges on both sides of the tray to secure the replacement chassis on to the tray.

20. Refer to Figure 27 on page 51. Tighten the center screw of the chassis.

21. Refer to Figure 31 on page 55. Install each of the 12 1 TB HDD drives into their same corresponding locations in the new chassis. "Removing and replacing the TS7610 or TS7620 ProtecTIER V3.3.6 fibre channel adapter" on page 73.

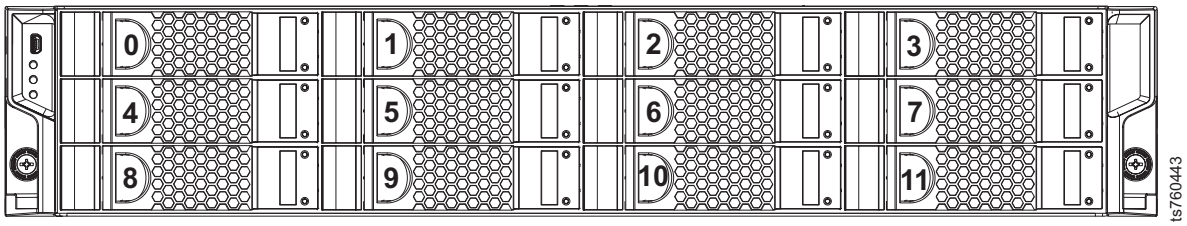


Figure 31. HDD position order

22. Push the server tray back into the rack. Using your fingers or a screwdriver, tighten the left- and right-side thumbscrews on the front of the server.
23. Now that server is back in the rack, we can put in the PSU's with ease and plug in power.
24. Connect all external cables to the chassis, connect the chassis power cables last.
25. Power up the system. Refer to "TS7610 or TS7620 startup" on page 25.
26. Verify the IP address set the IP address. Refer to "Server IP verification"
27. Verify that the system time is correct. If the time is not correct, update your time through the ptconfig menu. Refer to "Configuring the ProtecTIER V3.3.6 TS7610 or TS7620 system" on page 32.
28. Use this procedure to verify and if necessary update firmware. Refer to "Verify chassis firmware and update as needed" on page 57.
29. Verify the chassis serial number of the replacement chassis is changed to the original chassis serial number. The hardware warranty is linked to the original serial number. Refer to "The TS7610 or TS7620 ProtecTIER V3.3.6 chassis serial number update through the ProtecTIER Service Menu" on page 58.
30. Check the health of the system before returning the system to the customer. Refer to"ProtecTIER Service menu health monitoring and problem notification" on page 14.

Server IP verification

Do this procedure to verify and set up the IP addresses of the TS7610 Appliance Express before handing the server over to the customer.

Before you begin

You need a keyboard and a monitor attached to the TS7610 Appliance Express to do this task.

About this task

Following these instructions insures that the server has the IP addresses properly set.

Procedure

1. Access the **ProtecTIER Service Menu** with a monitor and keyboard plugged into the TS7610 Appliance Express. Log on with ID **ptconfig** , password **ptconfig**
2. When the **ProtecTIER Service Menu** appears, select the **ProtecTIER Configuration** option.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
--------------------------------------------------------------------------------
  1) ProtecTIER Configuration (...)
  2) Manage ProtecTIER services (...)
  3) Health Monitoring (...)
  4) Problem Alerting (...)
  5) Version Information (...)
  6) Generate a service report
  7) Generate a system view
  8) Update ProtecTIER code

  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

3. In the **ProtecTIER Configuration** menu, select **IP Network configuration** to set your server IP addresses.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
 ProtecTIER Configuration (...)
--------------------------------------------------------------------------------
  1) Configure ProtecTIER node
  2) Recover Configuration for a replaced server
  3) Configure enclosure serial number for a replaced enclosure
  4) Update Time, Date, Timezone & Timeserver(s)
  5) Configure replication (...)
  6) IP Network configuration (...)
  7) Update Firmware
  8) Update the System's name
  9) Validate configuration
 10) Single node - code upgrade (For Support Use ONLY)

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

4. When you are asked to stop the vtfd service, you must type yes and then click enter.

```
Starting Cluster, please wait
Starting cluster [Done]
Cluster Started
Would you like to stop the VTFD service? (yes|no) yes
```

5. You will see the option to update the IP addresses. Even if you will be using the same IP address as before you must reenter the IP address.

   Important: Do not just hit enter, you must type the IP address in and then press **Enter**.

```
Stoppping VTFD [Done]
Please provide the following information:
=========================================
Customer Network, IP Address [9.11.123.123]: 9.11.123.123
Customer Network, Customer Network, Netmask [255.255.255.0]:
255.255.255.0
Customer Network, Default Gateway [9.11.123.123]: 9.11.123.123
Customer Network, Hostname [nodel]: nodel
Configuring Network
```

6. Once complete you will see the following screen.

```
Setting Hostname [Done]
Saving configuration [Done]
Scalars leaked: 1
Collecting RAS Persistent configuration [Done]
Running RAS Eth Agent [Done]
Updated network configuration successfully
Starting VTFD [Done]
Starting RAS [Done]
UpdateNetwork ended successfully [Done]
Press the ENTER key to continue...
```

Go back to "TS7610 and TS7620 Appliance Express ProtecTIER V3.3.6 Chassis FRU Removal and Replacement" on page 49, step 28 to change the chassis serial number back to the original chassis serial number.

Verify chassis firmware and update as needed

On the rare occasions where the chassis firmware requires an update, this is the procedure you will need to do.

About this task

Do this step to insure that the firmware level of the hardware component is at a level that is supported by your currentProtecTIER server software level.

To update firmware level the TS7610 or TS7620 must have already been installed and configured.

Procedure

1. If necessary, power-on the server and the monitor, and wait for the login prompt to display.
2. This will be done with a monitor and keyboard plugged into the TS7610 or TS7620. Log on with ID **ptconfig** password **ptconfig**
3. Once you login, you will see the **ProtecTIER Service Menu**. Select the **ProtecTIER Configuration** option.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
--------------------------------------------------------------------------------
  1) ProtecTIER Configuration (...)
  2) Manage ProtecTIER services (...)
  3) Health Monitoring (...)
  4) Problem Alerting (...)
  5) Version Information (...)
  6) Generate a service report
  7) Generate a system view
  8) Update ProtecTIER code

  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

4. Once in the **ProtecTIER Configuration** Menu, select **Update Firmware** to verify or update if needed the firmware in your TS7610 Appliance Express.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
 ProtecTIER Configuration (...)
--------------------------------------------------------------------------------
  1) Configure ProtecTIER node
  2) Recover Configuration for a replaced server
  3) Configure enclosure serial number for a replaced enclosure
  4) Update Time, Date, Timezone & Timeserver(s)
  5) Configure replication (...)
  6) IP Network configuration (...)
  7) Update Firmware
  8) Update the System's name
  9) Validate configuration
 10) Single node - code upgrade (For Support Use ONLY)

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

Note: The firmware version can be viewed through yourProtecTIER Service Menu **Version Information** option.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
--------------------------------------------------------------------------------
  1) ProtecTIER Configuration (...)
  2) Manage ProtecTIER services (...)
  3) Health Monitoring (...)
  4) Problem Alerting (...)
  5) Version Information (...)
  6) Generate a service report
  7) Generate a system view
  8) Update ProtecTIER code

  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

From the Version Information Menu select **Display Firmware Version**.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
 Version Information (...)
--------------------------------------------------------------------------------
  1) Display version information
  2) Display Machine Reported Product Data (MRPD)
  3) Display Firmware Versions

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

The TS7610 or TS7620 ProtecTIER V3.3.6 chassis serial number update through the ProtecTIER Service Menu

The customer's warranty is linked to the serial number of the original chassis. This procedure explain how to put the customer's original chassis serial number on the chassis FRU.

Procedure

1. If necessary, power-on the server and the monitor, and wait for the login prompt to display.

2. This will be done with a monitor and keyboard plugged into the TS7610 or TS7620. Log on with ID **ptconfig** password **ptconfig**
3. Once you login, you will see the **ProtecTIER Service Menu**. Select the **ProtecTIER Configuration** option.

```
------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
------------------------------------------------------------------------------
  1) ProtecTIER Configuration (...)
  2) Manage ProtecTIER services (...)
  3) Health Monitoring (...)
  4) Problem Alerting (...)
  5) Version Information (...)
  6) Generate a service report
  7) Generate a system view
  8) Update ProtecTIER code

  E) Exit
------------------------------------------------------------------------------
>>> Your choice?
```

4. Once in the **ProtecTIER Configuration** Menu, select **Configure enclosure serial number for a replaced enclosure** to set your chassis serial number back to your original chassis serial number. The warranty of your TS7610 or TS7620 server is linked to the serial number of your original chassis.
5. The following prompt appears:

   `Please enter enclosure number to set serial number. (0 for base enclosure):`

   The chassis for either the TS7610 (SM1) or TS7620 (SM2) server is a base enclosure. Enter "0" for a base enclosure.
6. Write the serial number of the customer's original chassis on the Repair ID Tag. The IBM warranty is linked to the original serial number record of the chassis.

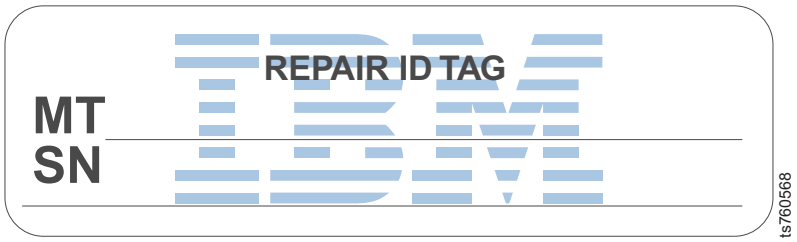


Figure 32. Service RID Tag

A RID (Replacement Identification) Tag maintains the original serial number record of the machine and allows IBM to entitle the machine for future maintenance or warranty service. Mail in exchange requires the completion and securing a Replacement ID tag (part number 19P5941) to the replacement unit.

- Verify that the machine serial number on the failing unit matches the serial number reported to IBM technical support.
- Transcribe the machine type, model, and serial number of the failing unit to the Replacement ID tag for the replacement unit.

  Note: USE BALLPOINT PEN TO COMPLETE THE RID TAG.
- Place the Replacement Identifier tag on the location indicated in the picture below.

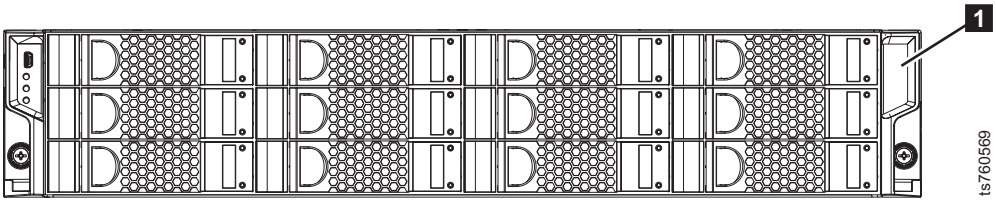


Figure 33. RID Tag Placement

- The use of the Repair ID tag is important for customer inventory accuracy.

Removing and replacing a TS7620 boot drive

The TS7620 Appliance Express, ProtecTIER V3.3.6 has two boot drives that are contained within a boot drive cage assembly. Take time to review the "Electrostatic discharge procedures", "Suspending I/O and powering-off the server" and "Powering-on the server and resuming I/O".

Before you begin

Put on your ESD strap. If your server is not already off, follow the instructions in "Suspending I/O and powering-off the server. If your server does not shut down in the standard manner, then press the white button to force a power shutdown of the chassis.

About this task

Procedure

1. Power off the TS7620 server. When power is off, unplug the two power cables from the power supplies.
2. Refer toFigure 34 on page 61. Working from the front of the rack, push the front tab and pull the slide rails and support tray forward. Continue pulling until the rails are fully extended and click into the locked position **1** .

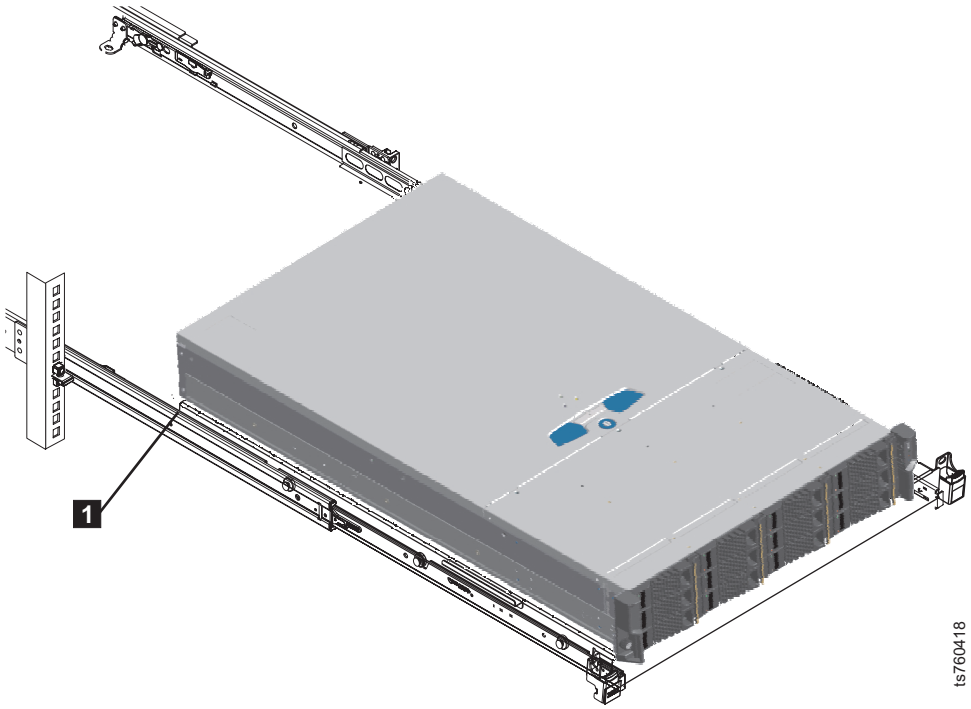


Figure 34. Extending the slide rails and support tray

3. Refer to Figure 35. Loosen the cover's holding screw **1** by 1/4 turn clockwise. Press the silver button **2** and **3** slide the cover back and up to remove it.

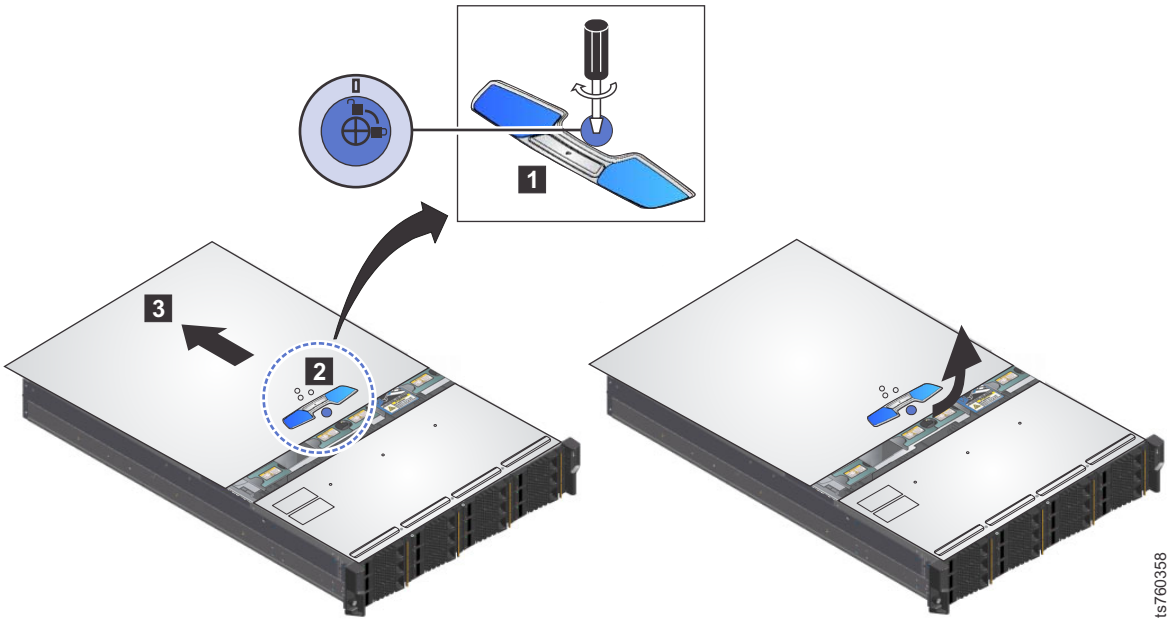


Figure 35. Remove chassis cover

4. See Figure 36 on page 62 where **2** shows the location of the boot drive assembly within the chassis.

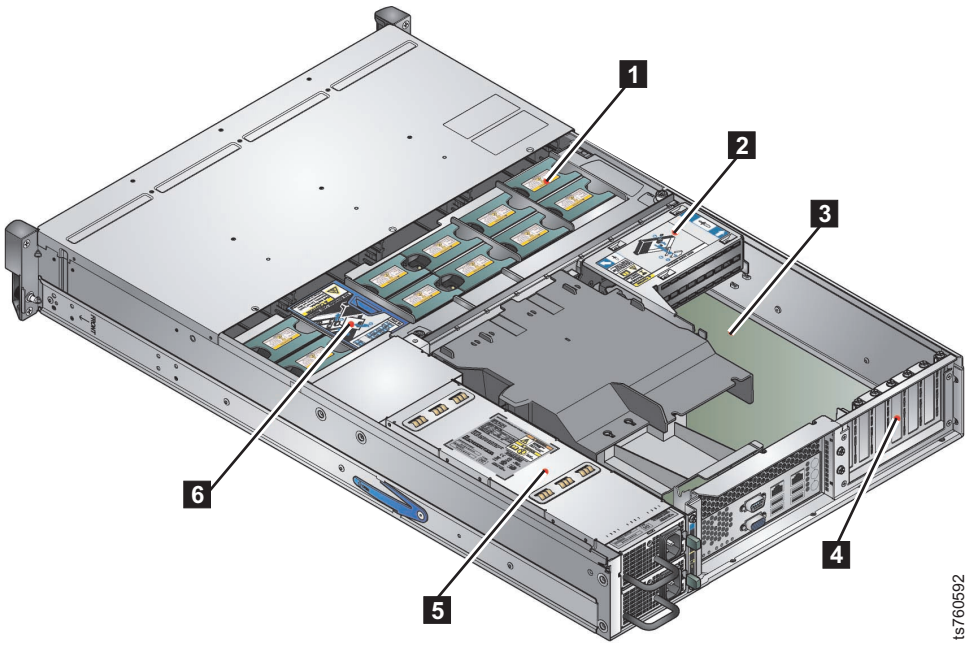


Figure 36. Location of boot drive assembly

5. Refer to Figure 37. You can identify the boot drive cage by the Boot Drive Removal caution label. The label shows the plastic covers **1**, the air baffle, and the L-shaped cover **2**. Remove both plastic covers.

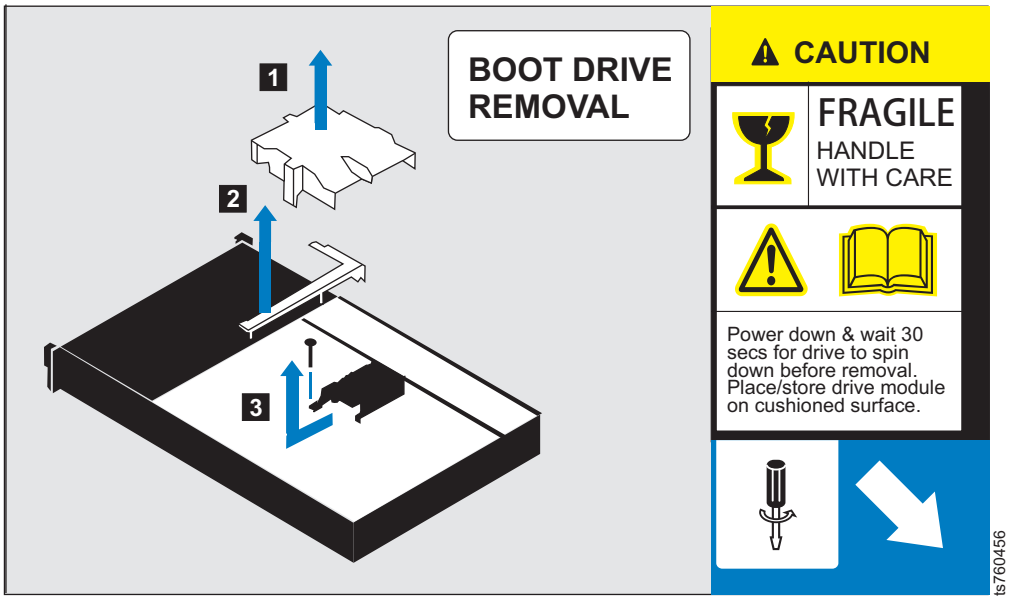


Figure 37. Boot cage caution label

a. Refer to Figure 38 on page 63. Three mounting points hold the boot drive cage in place; a retention screw and two mounting points on the inside of the chassis. With a screwdriver, remove the single upright retention screw **3** from the boot drive cage. You might need to use pliers to hold the post stationary to unscrew the retention screw.

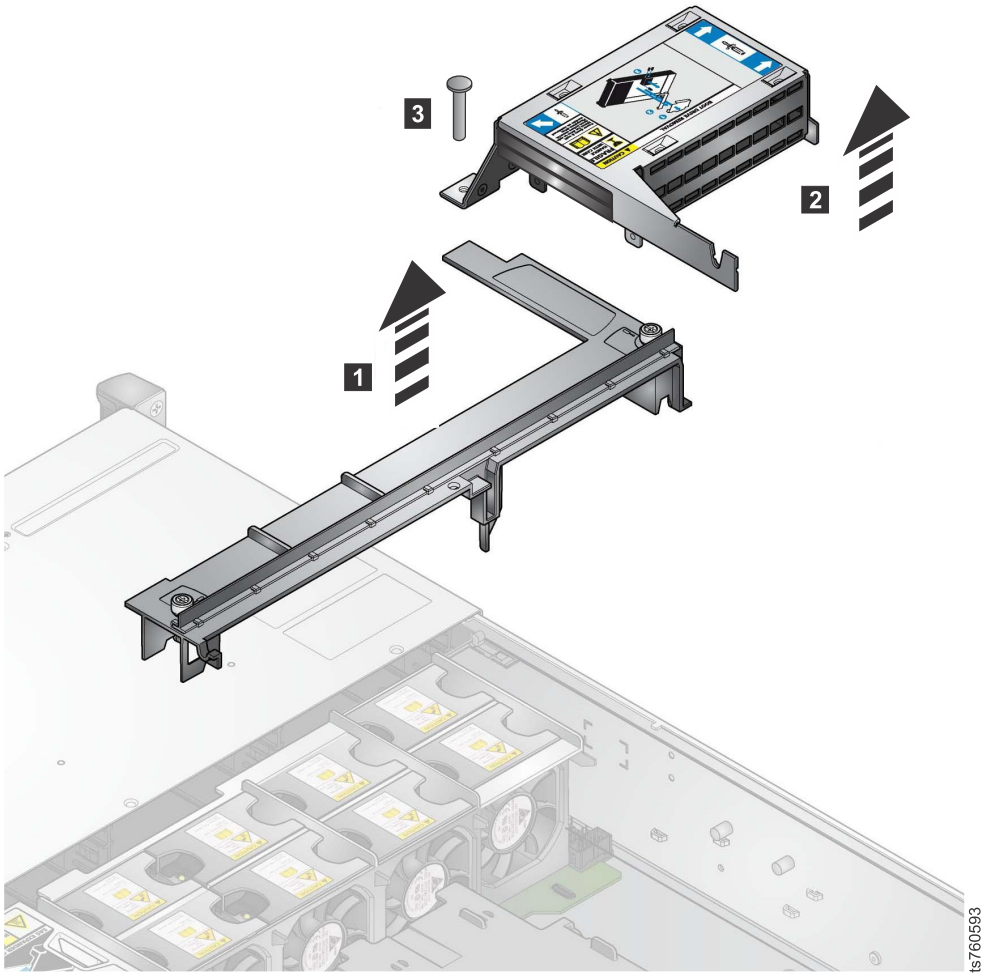


Figure 38. Boot Cage Assembly Retention Screw

b. Hold the boot cage and gently pull toward to the center of the chassis. Continue pulling until the boot drive assembly is free from the two mounting pins on the inside of the chassis. See Figure 38, which shows the boot drive assembly and the mounting pins. The boot drive assembly consists of a boot drive cage, two boot drives and a small backplane board.

c. There are two SAS cables and one power cable that connects to backplane board of the boot drive assembly. The SAS cables are labeled P1 and P2. The other end of this mini SAS cable is connected to MegaRaid SAS9240-4i boot raid adapter in slot 3.

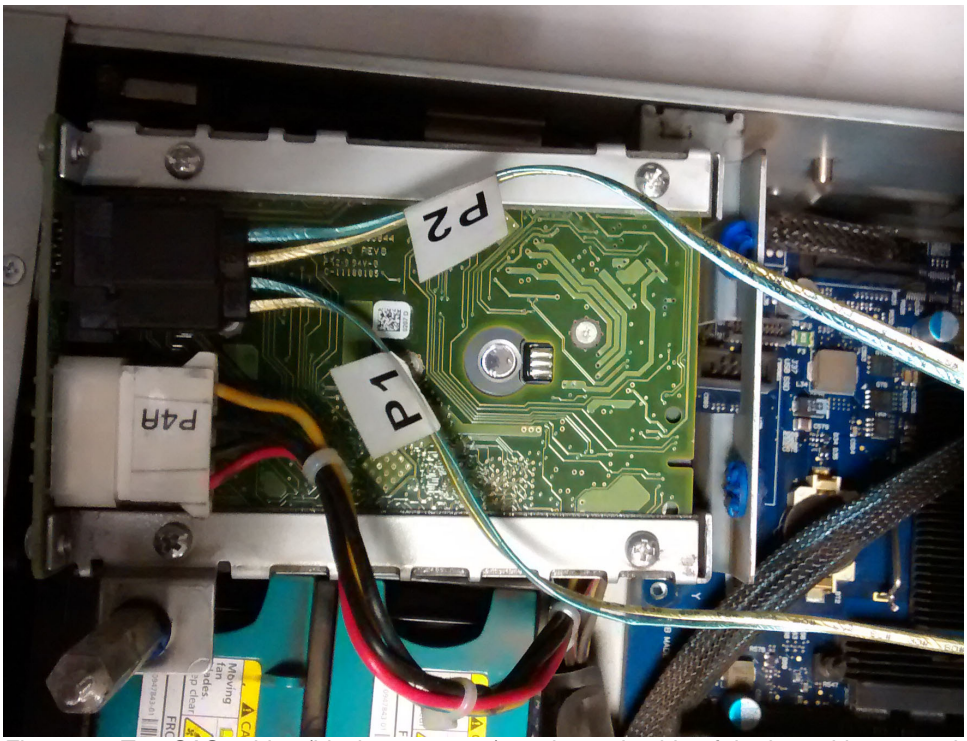


Figure 39. Two SAS cables (black connectors) on the underside of the boot drive assembly

d. Detach the SAS cables from backplane board of boot drive ASM but leave the mini SAS cable connected to the MegaRAID SAS9240-4i boot RAID adapter.

e. Remove the whole boot drive assembly.

6. When you have the boot disk cage assembly free from the sysplaner, you can remove the backplane board from the boot drive cage.

7. The boot drives are each attached to the backplane board by a connector. Remove the four screws that are securing the defective drive to the cage and gently pull the backplane board off the boot drives.

8. Remove only the failing drive. To use the GUI to see which boot drive is failingProtecTIER Manager, see “Receiving and responding to hardware alerts” on page 5.

Figure 40. Orientation and location of boot drives 1 and 2 in the boot cage assembly

When the boot drive assembly cage is facing up, boot drive 1 (cable P1) is on the top. Boot drive 2 (cable P2) is at the bottom.

9. Take the new boot drive and slide it into the cage assembly and secure with four screws. Leave the drive screws a little loose so that the boot drive can shift a little. Having the screws a little loose is helpful when you reconnect the backplane to the boot drives and the boot drive cage.
10. Insert the small backplane card so the pins seat into each boot drive connector. Tighten the four screws that hold the boot drive in place. Then, tighten the four screws that hold the backplane card in place.
11. Reconnect the two cables from the sysplaner to the connectors on the small backplane. Make sure to plug the MegaRAID SAS adapter cables into the same connectors they were removed from.
12. Slide the boot cage assembly, caution label up on to the two mounting pins on the chassis wall.
13. Tighten the retention screw and washer back to the mounting point on the chasis.
14. Put the plastic L-shaped and air baffle covers back on.
15. Put the cover back on the chassis.
16. Slide the server chassis drawer back into the rack.
17. Connect all the cables back to the chassis except for the chassis power cord.
18. Connect the power cable and refer to the “TS7610 or TS7620 startup” on page 25.
19. If you replaced only one of the boot drives, observe the server as it powers up. Verify that both drives are displayed. The status is degraded because the mirroring is not completed. The mirroring starts automatically. It can take roughly 5 hours for the mirroring to complete. The rebuild runs in the background. When the mirroring is complete, go to step 21.

    If you replaced both boot drives, all configuration information, including the mirrored configuration information is lost. The customer must reconfigure their TS7610 system after boot drive replacement is complete. Refer your customer to the applicable chapters in their *IBM TS7620 ProtecTIER Deduplication Appliance Express Installation and Setup Guide for VTL, and OpenStorage Systems*, v3.3, GA32-0914 for information and instructions.

20. Log in and verify that vtfd is running. Type `service vtfd status` and press Enter. Wait for vtfd to start completely.
21. To verify and, if necessary, update firmware, use the procedure that is described in “Updating and verifying the TS7610 or TS7620 firmware with the ProtecTIER Service Menu” on page 30.
22. Type: `menu` and press Enter to open the ProtecTIER Service Menu.
23. Type the number corresponding to `Health Monitoring (...)` and press Enter.
24. In the ProtecTIER Health Monitoring Service window, type the number corresponding to `Run a full system check (...)` and press Enter.
25. Ensure that all system status is normal.
26. Turn the system over to the customer.

Removing and replacing a TS7610 boot drive

The TS7610 Appliance Express has two boot drives that are contained within a boot drive cage assembly. Take time to review the "Electrostatic discharge procedures", "Suspending I/O and powering-off the server" and "Powering-on the server and resuming I/O".

Before you begin

Put on your ESD strap. If your server is not already off, follow the instructions in "Suspending I/O and powering-off the server. If your server does not shut down in the standard manner, then press the white button to force a power shutdown of the chassis.

About this task

Procedure

1. Power off the TS7610 server. When the power is off, unplug the two power cables from the power supplies.
2. Refer to Figure 41 on page 67. Working from the front of the rack, push the front tab and pull the slide rails and support tray forward. Keep pulling forward until the rails are fully extended and click into the locked position **1**.

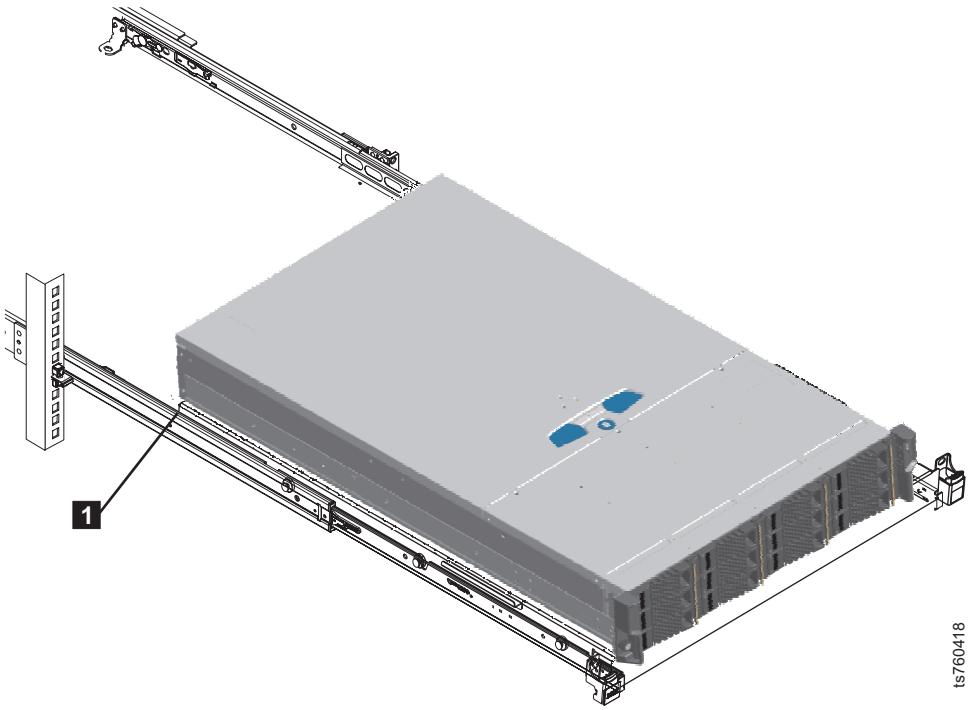


Figure 41. Extending the slide rails and support tray

3. Refer to Figure 42. Loosen the cover's **1** holding screw 1/4 turn clockwise. Press the silver button **2** and **3** slide the cover back and up to remove it.

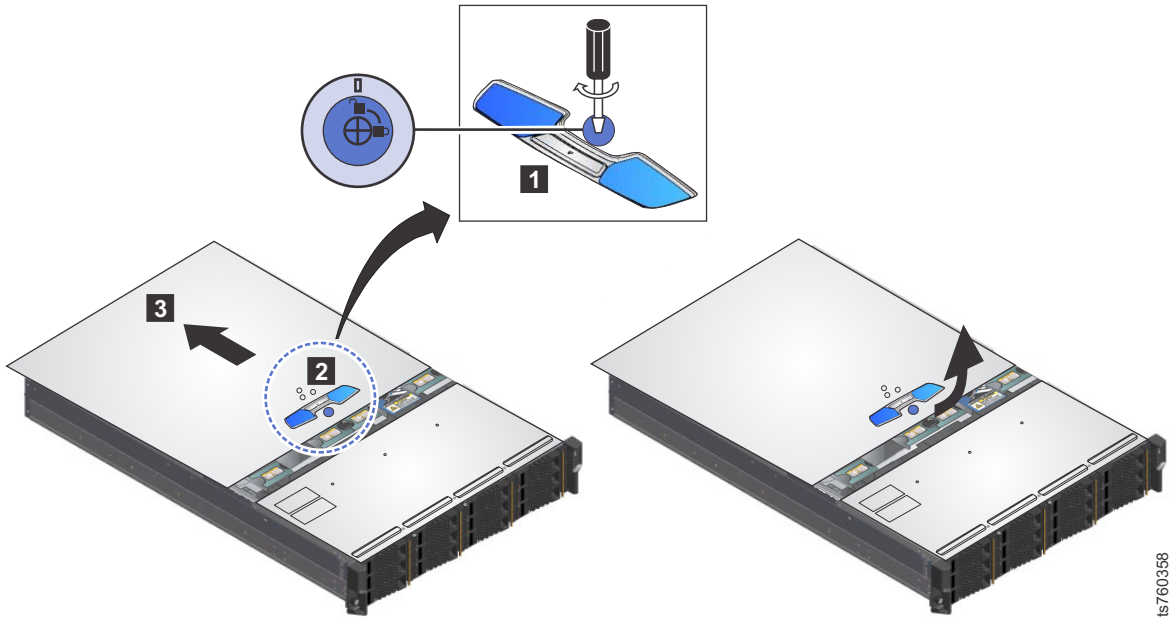


Figure 42. Remove chassis cover

4. Refer to Figure 43 on page 68 where **2** shows the location of the boot drive assembly within the chassis.

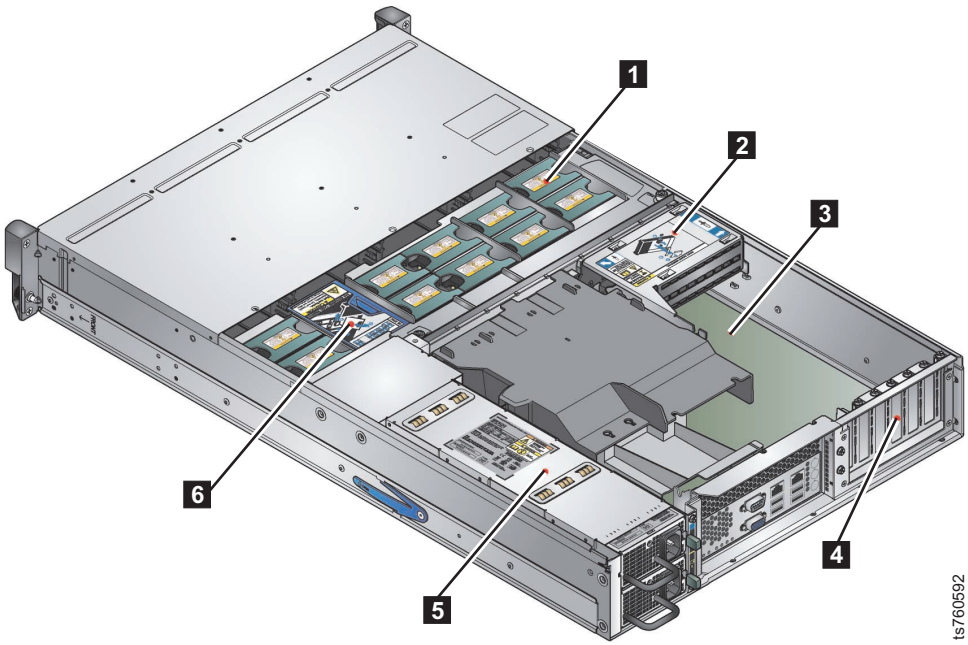


Figure 43. Location of boot drive assembly

5. Refer to Figure 44. You can identify the boot drive cage by the Boot Drive Removal caution label. The label shows the plastic covers **1** the air baffle and the L-shaped cover **2** . Remove both plastic covers.

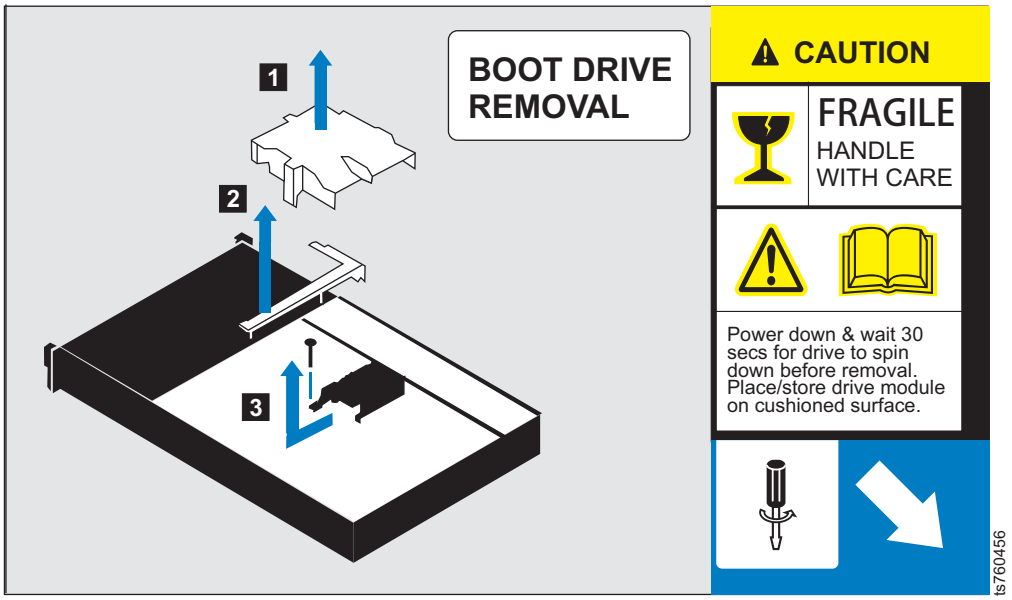


Figure 44. Boot cage caution label

a. Refer to Figure 45. Three mounting points hold the boot drive cage in place; a retention screw, and two mounting points on the inside of the chassis. With a screwdriver, remove the single upright retention screw 3 from the boot drive cage. You might need to use pliers to hold the post stationary to unscrew the retention screw.

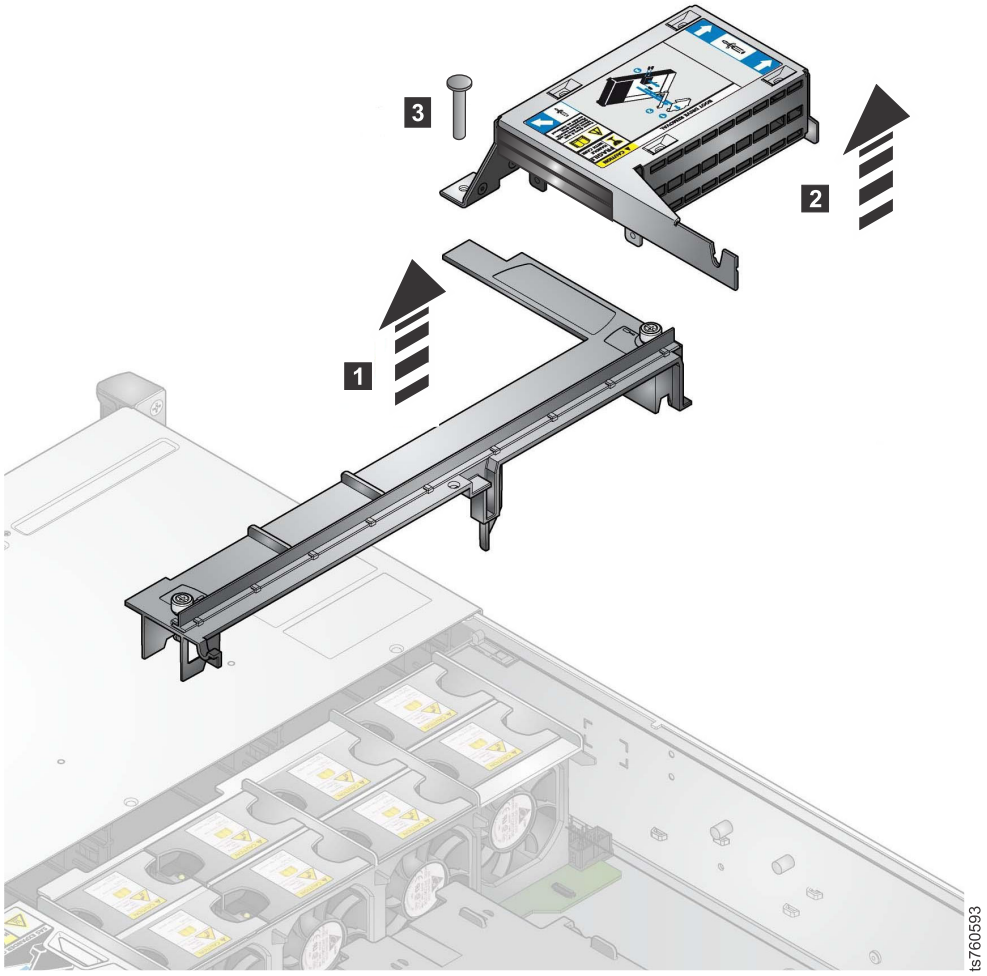


Figure 45. Boot Cage Assembly Retention Screw

b. Hold the boot cage and gently pull toward to the center of the chassis. Continue pulling until the boot drive assembly is pulled free from the two mounting pins on the inside of the chassis. Refer to Figure 45 which shows the boot drive assembly and the mounting pins. The boot drive assembly consists of a boot drive cage, two boot drives and a small backplane board.

c. There are two SATA cables and one power cable that connect the small backplane board of the boot drive assembly to the sysplanar (the chassis motherboard). If the SATA cables are not labeled, mark each cable to note if the cable is connected to the bottom or the top connector of the backplane board.

Figure 46. The SATA cables are connected to both the backplane board and the sysplanar.

d. After ensuring that the cables are labeled, detach the SATA cables from the backplane board but leave the SATA cables connected to the sysplanar.

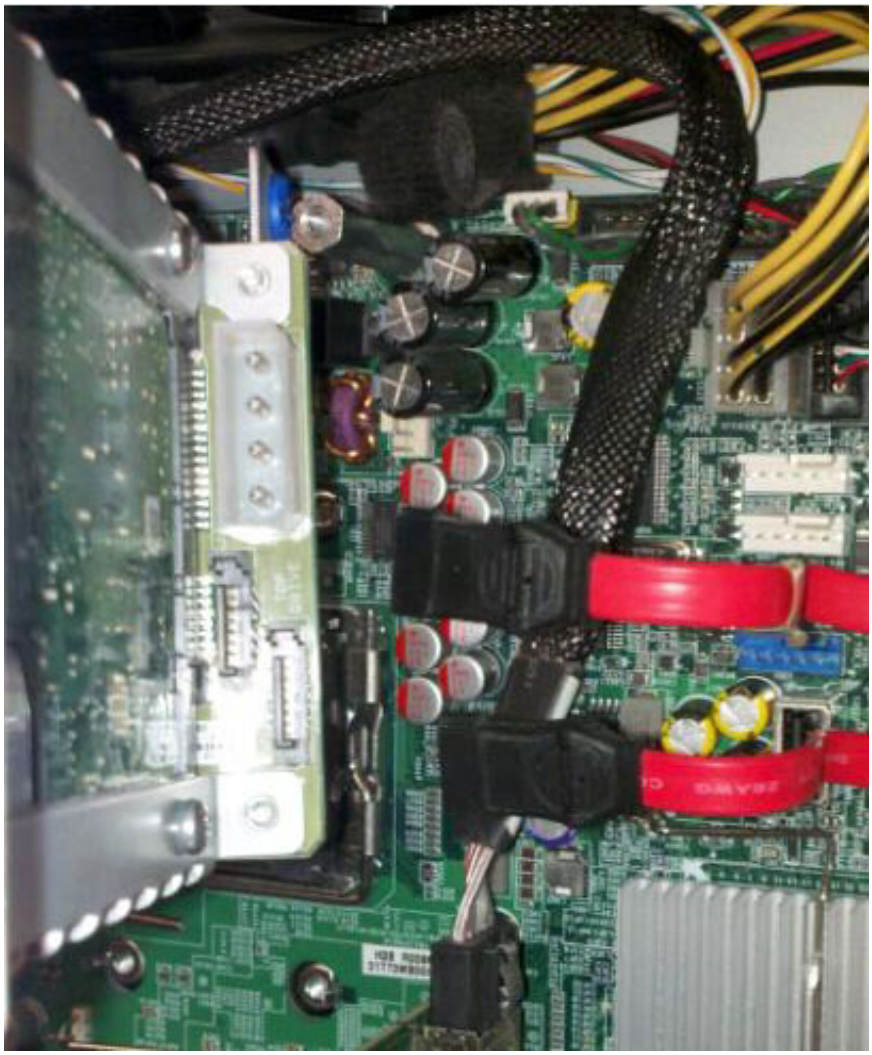


Figure 47. The SATA cables are disconnected from the backplane board.

e. Remove the whole boot drive assembly.

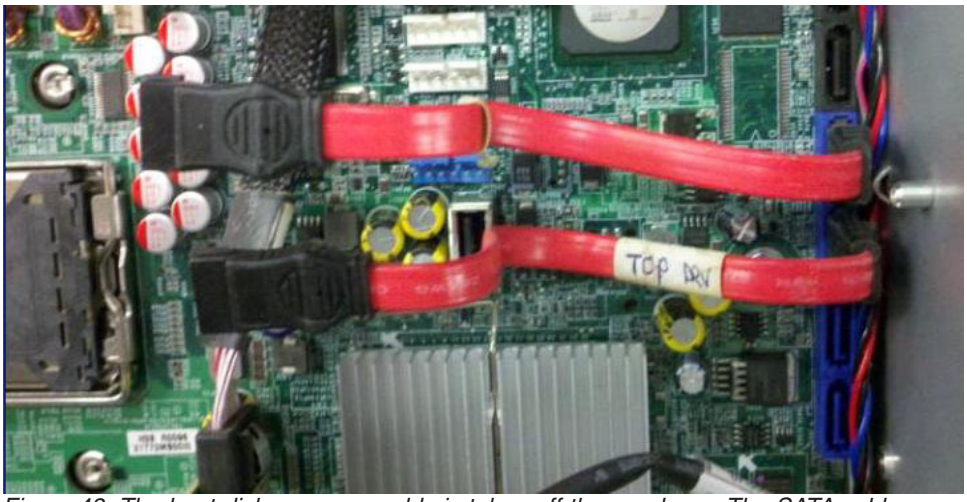


Figure 48. The boot disk cage assembly is taken off the sysplanar. The SATA cables remain connected to the sysplanar.

6. When you have the boot disk cage assembly free from the sysplaner, you can remove the backplane board from the boot drive cage.
7. The boot drives are each attached to the backplane board by a connector. Remove the four screws that are securing the defective drive to the cage and gently pull the backplane board off the boot drives.
8. Remove only the failing drive. Refer to “Receiving and responding to hardware alerts” on page 5 to see which boot drive is failing using the ProtecTIER Manager GUI.

Figure 49. Orientation and location of boot drives 1 and 2 in the boot cage assembly

When the boot drive assembly cage is facing up, boot drive 1 is on the bottom and boot drive 2 is on the top.

9. Take the new boot drive and slide it into the cage assembly and secure it with the four screws. Leave the drive screws a little loose so that the boot drive can shift a little. This is helpful when you reconnect the backplane to the boot drives and the boot drive cage.
10. Insert the small backplane card so the pins seat into each boot drive connector. Tighten the four screws that hold the boot drive in place. Then, tighten the four screws that hold the backplane card in place.
11. Reconnect the two cables from the sysplaner to the connectors on the small backplane. Make sure to plug the cables into the same connectors they were removed from.
12. Slide the boot cage assembly, caution label up on to the two mounting pins on the chassis wall.
13. Tighten the retention screw and washer back to the mounting point on the chassis.
14. Put the plastic L-shaped and air baffle covers back on.
15. Put the cover back on the chassis.
16. Slide the server chassis drawer back into the rack.
17. Connect all the cables back to the chassis except for the chassis power cord.
18. Connect the power cable and refer to the “TS7610 or TS7620 startup” on page 25.
19. If you replaced only one of the boot drives, observe the server as it powers up. Verify that both drives are displayed. The status is degraded because the mirroring is not complete yet. The mirroring starts automatically. It can take

roughly 5 hours for the mirroring to complete. The rebuild runs in the background. When mirroring is complete, go to step 21.

If you replaced both boot drives, all configuration information, including the mirrored configuration information is lost. The customer must reconfigure their TS7610 system after boot drive replacement is complete. Refer your customer to the applicable chapters in their *IBM TS7620 ProtecTIER Deduplication Appliance Express Installation and Setup Guide for VTL, and OpenStorage Systems*, v3.3, GA32-0914 for information and instructions.

20. Log in and verify that vtfd is running. Type `service vtfd status` and press Enter. Wait for vtfd to start completely.
21. To verify and, if necessary, update firmware, use the procedure that is described in "Updating and verifying the TS7610 or TS7620 firmware with the ProtecTIER Service Menu" on page 30.
22. Type: `menu` and press Enter to open the ProtecTIER Service Menu.
23. Type the number corresponding to `Health Monitoring (...)` and press Enter.
24. In the ProtecTIER Health Monitoring Service window, type the number corresponding to `Run a full system check (...)` and press Enter.
25. Ensure that all system status is normal.
26. Turn the system over to the customer.

Removing and replacing the TS7610 or TS7620 ProtecTIER V3.3.6 fibre channel adapter

About this task

The fibre channel adapter provides connectivity to your host network.

Important:

- The fibre channel adapter is internal and cold-swappable. The server must be powered off for adapter replacement.
- Before you begin, review the information in "Electrostatic discharge procedures" on page 23.
- Take care to avoid touching the gold contacts along the lower edge of the adapter.
- The ProtecTIER V3.3.6 TS7610 or TS7620 , VTL server requires a fibre channel card.
- ProtecTIER TS7610 Appliance Express v2.1 supports 4GB fibre channel.
- TS7610 Appliance Express ProtecTIER v3.2 and TS7620 Appliance Express supports 4GB and 8GB fibre channel.
- When replacing the fibre channel card, it is important to replace your defective fibre channel with a card of the same link speed value. For example, replace a 4GB fibre channel card with a 4GB card.

  Note: Replacing a 4GB fibre channel adapter with an 8GB fibre channel adapter is not supported.
- Figure 50 on page 74 displays the locations of the PCI cards. The fibre channel card is placed in PCI slot marked **3** .

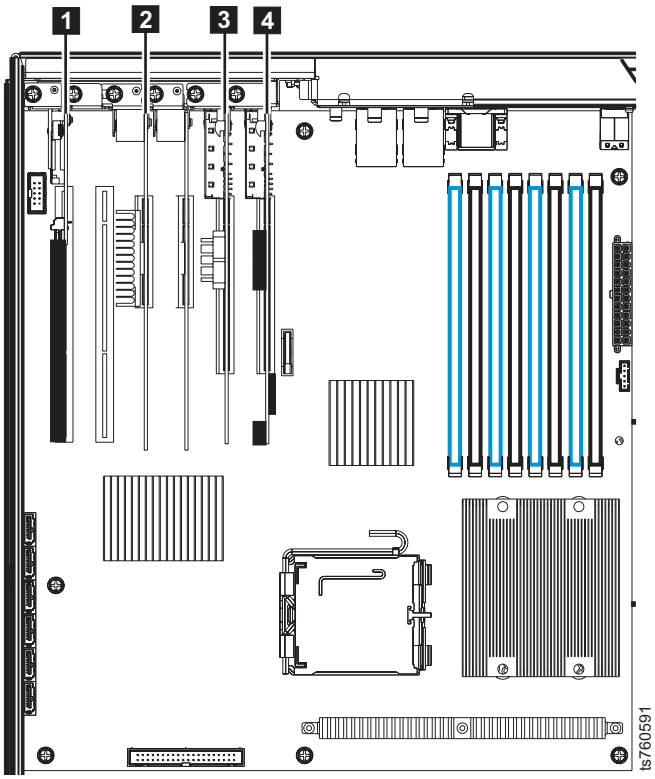


Figure 50. PCI Cards

Power off the server using one of the following methods:

- Controlled software shutdown:
  1. With a graphics capable monitor and USB keyboard attached to the back of the server, from command line prompt, login as **ptadmin** with a password of **ptadmin**.
  2. Enter the command: **poweroff** <enter>
  3. When the server is fully powered-off, the LEDs on the operator panel go dark.
- Manual power off:

Procedure

1. Use this manual power off method only if the controlled software shutdown is not possible.
   a. Locate the server's **On/Off** button (**5**) on the side of the server operator panel. See Figure 51 on page 75.

      The server operator panel has these buttons: **1** : USB socket , **2** : Power active, **3** : Unit fault, **4** : ID LED, **5** : On/Off button, **6** : System reset, **7** : ID LED switch.

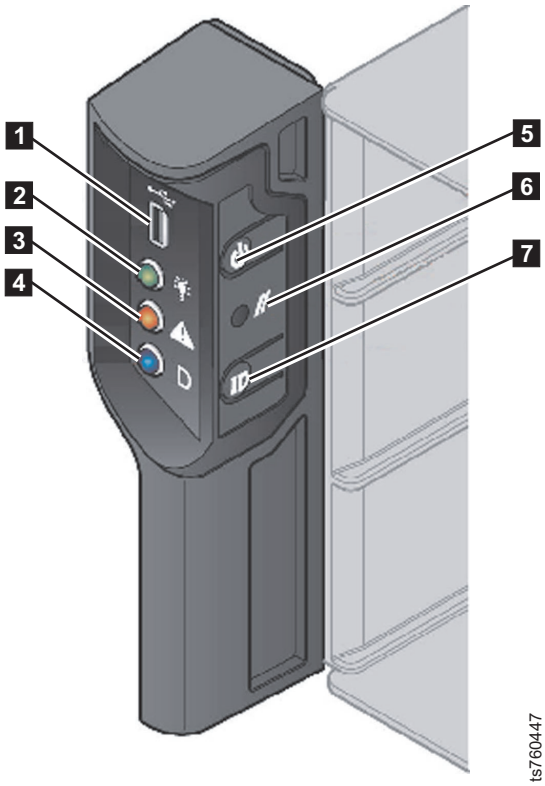


Figure 51. On/Off button

b. Press and hold the **On/Off** button for five seconds.

   When the server is fully powered-off, the LEDs on the operator panel go dark.

2. To remove the fibre channel adapter:
   a. If not already tagged, tag and disconnect the fibre channel cables from the adapter. Before moving the server into the service position, label other cables such as power cables, display connection, USB, and network connections.
   b. Place the TS7610 Appliance Express in the service position and remove the top cover, as described in "Placing the TS7610 or TS7620 to service position" on page 27 and remove cover.
   c. Remove the retention screw from the adapter's mounting bracket, and set the screw aside.
   d. Carefully grasp the adapter by the upper corners and lift it up and out of the slot.

      Note: You may need to gently wiggle the adapter from front to back to free it from the slot.

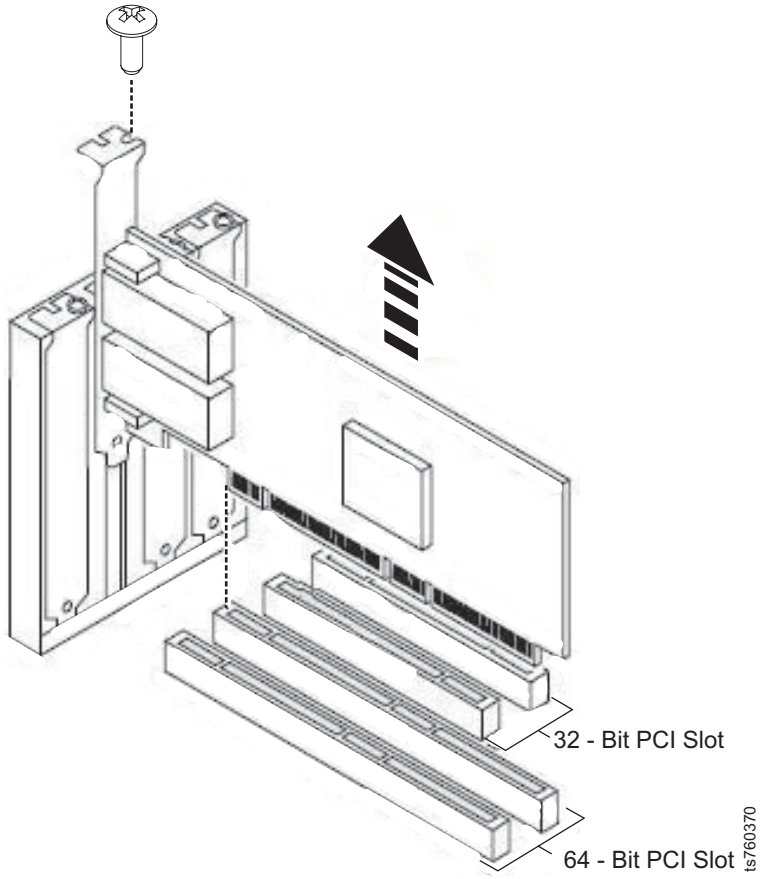


Figure 52. Remove fibre channel adapter

3. **IMPORTANT:** Take a moment to make note of the World Wide Name (WWN) values printed on the label attached to the plastic air baffle. To do so:
   a. Locate the label (similar to Figure 53) on the plastic air baffle.

(port)	original nodename	original portname
(0)	20000000c97bd994	10000000c97bd994
(1)	20000000c97bd995	10000000c97bd995

ts760634

Figure 53. World Wide Name (WWN) label

4. Write down all of the information exactly as it is printed on the label.
   The label contains the node name and port name values for the fibre channel adapter that was originally installed in the server. In order to avoid problems after an adapter is replaced, the values from the original adapter must be applied to the new adapter.
5. To replace the fibre channel adapter:
   a. Remove the new adapter from its anti-static packaging.
   b. Carefully grasp the adapter by the upper corners and align it with the appropriate slot.

Note: When the component is installed correctly, the tapered tab on the lower edge of the mounting bracket will be visible when viewed from inside the chassis.

c. Press down gently until the adapter is firmly seated.

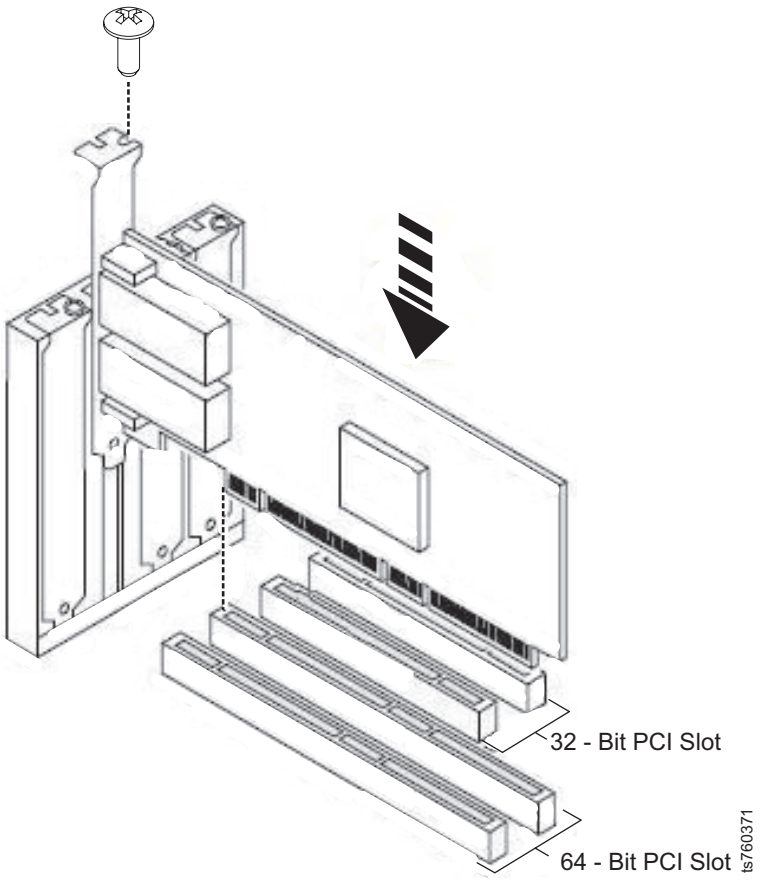


Figure 54. Replace fibre channel adapter

d. Replace the retention screw, tightening it to secure the mounting bracket to the server chassis.

e. Replace the top cover.

f. Return the TS7610 Appliance Express to the operational position, as described in "Placing the TS7610 or TS7620 to operational position" on page 29.

g. Reconnect the fibre channel cables to the new adapter and all other disconnected cables.

6. Power-on the server. To do so, refer to "TS7610 or TS7620 startup" on page 25.
7. While the system is powering on, a number of status messages, (which may include failure notices) display on the screen. As long as the failures do not stop the process, ignore the messages and allow the power on cycle to continue. It may take up to 10 minutes. Once complete, you are returned to the login prompt.
8. Use the ProtecTIER Service Menu to update firmware and automatically pick up the original WWN of the ports. See "Updating and verifying the TS7610 or TS7620 firmware with the ProtecTIER Service Menu" on page 30.
9. Reboot the server by exiting the ProtecTIER Service Menu by selecting the **Manage ProtecTIER Services** option.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
--------------------------------------------------------------------------------
  1) ProtecTIER Configuration (...)
  2) Manage ProtecTIER services (...)
  3) Health Monitoring (...)
  4) Problem Alerting (...)
  5) Version Information (...)
  6) Generate a service report
  7) Generate a system view
  8) Update ProtecTIER code

  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

10. From the **Manage ProtecTIER Services** menu, select the **Reboot This Node** . You will be prompted:

    ```
    Would you like to continue ? (yes|no)
    ```

    Type `yes` <enter>.

11. Verify that the WWN retrieve has occurred by entering **`dmesg | grep WNN`** and than press <enter>. The current WWN that is assigned to the server appears in the screen. Verify that the number on the screen matches the original nodename in the WWN label on the plastic air baffle.

```
[root@rassmb2 ~]# dmesg | grep WNN
ptlpfc(0,0): TGTPORT: tgtport_dump: WWPN=10:00:00:00:c9:7a:1c:98 WWNN=20:00:00:0
0:c9:7a:1c:98
ptlpfc(1,0): TGTPORT: tgtport_dump: WWPN=10:00:00:00:c9:7a:1c:97 WWNN=20:00:00:0
0:c9:7a:1c:97
[root@rassmb2 ~]#
```

ts761098

Figure 55. Output example of an dmesg | grep WNN

12. With a graphics capable monitor and USB keyboard attached to the back of the server, from command line prompt, login as **`ptadmin`** with a password of **`ptadmin`**.
13. Verify that replacing the component resolved the hardware fault. See "Rechecking faults in the Hardware Faults window" on page 125.

    After you have verified that the steps taken to resolve a fault were successful, and that any residual fault alert information is cleared from the ProtecTIER Manager, the component replacement is complete.

Removing and replacing the LSI MegaRAID SAS9280-4i4e, 12 HDD RAID card respository control (for TS7620) or LSI MegaRaid SAS8888ELP repository controller(for TS7610)

About this task

The LSI MegaRAID SAS9280-4i4e (for TS7620) or LSI MegaRaid SAS8888ELP (for TS7610) controller manages the allocation of meta- and customer data across the 12 SATA HDDs. As transactions occur, the data is temporarily held in the MegaRAID controller's memory before being written to the drives.

Important:

- For the TS7620:
  - SM2 uses a LSI MegaRAID SAS9280-4i4e repository controller card.

  - It is stored in slot 1. Facing the back of the server, it is the slot farthest to the left. Refer to Figure 21 on page 46 for a graphical view.
  - The repository cable is connected to the back side of the card. The BBU cable is connected to the side of the card.
- For the TS7610:
  - SM1 uses a LSI MegaRaid SAS8888ELP repository controller card.
  - It is stored in slot 6. Facing the back of the server, it is the slot farthest to the right. Refer to Figure 23 on page 48 for a graphical view.
  - The repository cable is connected to the top side of the card. The BBU cable is connected to the side of the card.

    Tip: Since this cable connection is on the top of the card, it sometimes gets caught on the lid. After replacing the card, gently bend the cable down away from the lid.

  and
- The MegaRAID controller is internal and cold-swappable.
- Before you begin, review the information in "Electrostatic discharge procedures" on page 23.
- Before removing the MegaRAID controller, verify that no data is resident in the controller's memory.
- Take care to avoid touching the gold contacts along the lower edge of the controller.

Tip: In addition to following the instructions provided below, you can watch instructional videos of the procedures by going to the TS7610 Information Center, located at http://pic.dhe.ibm.com/infocenter/ts7600/serv/index.jsp.

Procedure

1. Power-off the server. To do so, refer to "TS7610 or TS7620 power off sequence" on page 23.

   After the server is fully powered-off, return to this page and continue with step 2.
2. To remove the MegaRAID controller:
   a. Place the TS7610 or TS7620 server in the service position, as described in "Placing the TS7610 or TS7620 to service position" on page 27, and remove the server's top cover.
   b. Remove the retention screw from the adapter's mounting bracket, and set the screw aside.
   c. Disconnect the BBU cable from the MegeRAID controller card.
   d. Carefully grasp the adapter by the upper corners and lift it up and out of the slot.

      Note: You may need to gently wiggle the adapter from side-to-side to free it from the slot. Do not use this picture as a reference for slot placement.

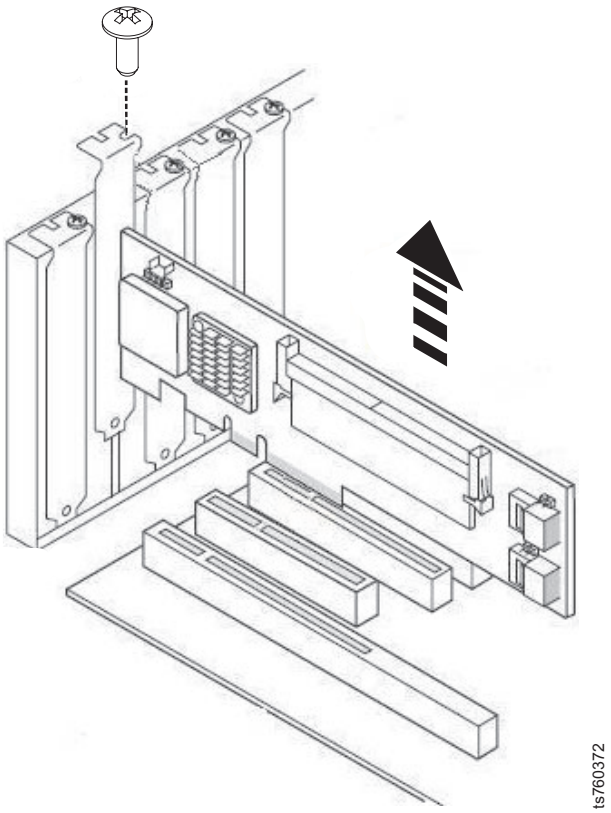


Figure 56. Removing the MegaRAID controller

e. Carefully disconnect the repository cable from the MegaRAID controller card.

3. To replace the MegaRAID controller:
   a. Remove the new adapter from its anti-static packaging.
   b. Carefully connect the SAS cable to the lower connector on the new controller.

      Note: When connecting the SAS cable, make sure that the side of the connector with the double row of silver contacts faces **away** from the controller.
   c. Carefully grasp the adapter by the upper corners and position it in the appropriate slot.

      Note: When the component is installed correctly, the tapered tab on the lower edge of the mounting bracket will be visible when viewed from inside the chassis. Do not use this picture as a reference for slot placement.

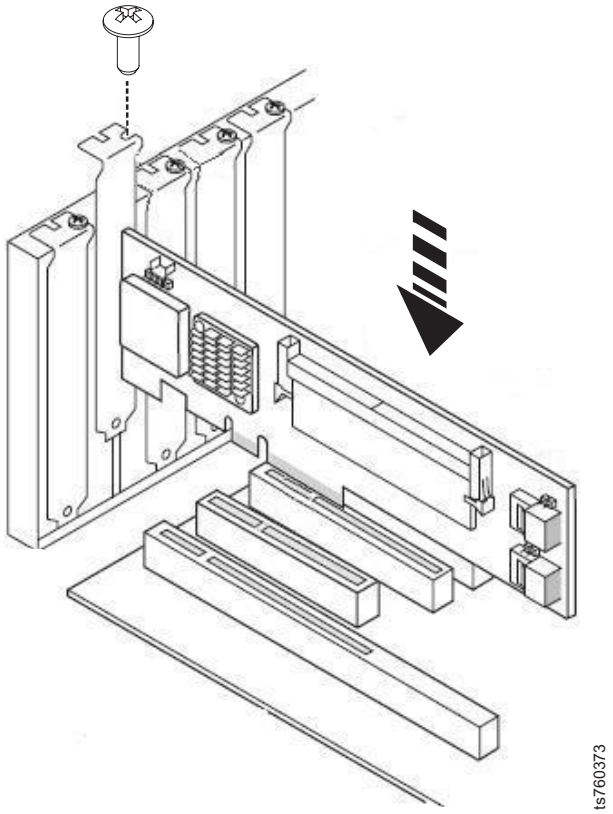


Figure 57. Replacing the MegaRAID adapter

d. Press down gently until the controller is firmly seated.

e. Replace the retention screw, tightening it to secure the mounting bracket to the server chassis.

f. Carefully connect the BBU cable to the new controller.

Note: When connecting the BBU cable, make sure that the side of the connector with the double row of silver contacts faces **away** from the controller.

g. Replace the plastic air baffle.

h. Return the server to the operational position, as described in "Placing the TS7610 or TS7620 to operational position" on page 29.

4. Power-on the server. To do so, refer to "TS7610 or TS7620 startup" on page 25, and then return to this page.

   You should now be logged into the server, with the server command prompt displayed.

5. Use this procedure to verify and if necessary update firmware. See "Updating and verifying the TS7610 or TS7620 firmware with the ProtecTIER Service Menu" on page 30.

6. Verify that replacing the component resolved the hardware fault. See "Verifying fault resolutions in the TS7610 or TS7620 ProtecTIER V3.3.6ProtecTIER Service menu" on page 126.

   After you have verified that the steps taken to resolve a fault were successful, and that any residual fault alert information is cleared from the ProtecTIER Manager, the component replacement is complete.

Removing and replacing the TS7620 Appliance Express, ProtecTIER V3.3.6 LSI MegaRAID SAS9240-4i boot RAID

About this task

The boot MegaRAID (LSI MegaRAID SAS9240-4i0) manages the data across the 2 internal boot drives.

Important:

- Only the TS7620 server uses the boot MegaRAID.
- The boot drive RAID card is internal and cold-swappable.
- Before you begin, review the information in "Electrostatic discharge procedures" on page 23.
- Before removing the boot drive RAID, verify that no data is resident in the controller's memory.
- Take care to avoid touching the gold contacts along the lower edge of the controller.
- The boot drive RAID card has one cord that is connects to the boot drives.

Tip: In addition to following the instructions provided below, you can watch instructional videos of the procedures by going to the TS7610 Information Center, located at: http://pic.dhe.ibm.com/infocenter/ts7600/serv/index.jsp.

Procedure

1. Power-off the server. To do so, refer to "TS7610 or TS7620 power off sequence" on page 23.

   After the server is fully powered-off, return to this page and continue with step 2.
2. To remove the boot drive RAID card:
   a. Place the TS7620 Appliance Express server in the service position, as described in "Placing the TS7610 or TS7620 to service position" on page 27, and remove the server's top cover.
   b. Remove the retention screw from the adapter's mounting bracket, and set the screw aside.
   c. Carefully grasp the adapter by the upper corners and lift it up and out of the slot.

      Note: You may need to gently wiggle the adapter from side-to-side to free it from the slot.

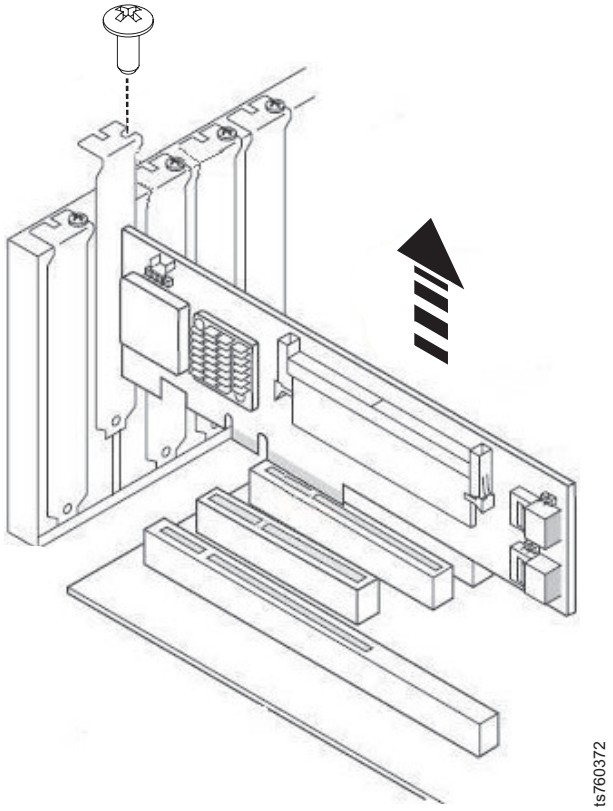


Figure 58. Removing the MegaRAID controller

d. Carefully disconnect the boot drive cable from the boot drive RAID card.

3. To replace the boot drive RAID card:
   a. Remove the new adapter from its anti-static packaging.
   b. Carefully connect the boot drive cable to the connector on the new RAID card.
   c. Carefully grasp the adapter by the upper corners and position it in the appropriate slot.

      Note: When the component is installed correctly, the tapered tab on the lower edge of the mounting bracket will be visible when viewed from inside the chassis.

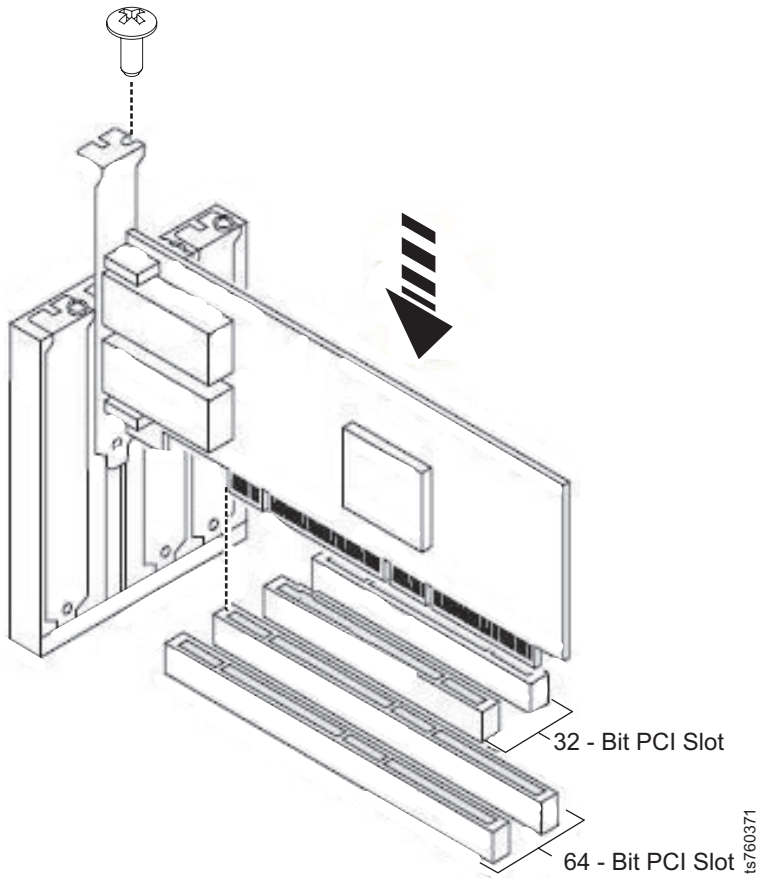


Figure 59. Replacing the boot drive RAID adapter

d. Carefully reconnect the boot drive cable to the new boot drive RAID card.
e. Press down gently until the controller is firmly seated.
f. Replace the retention screw, tightening it to secure the mounting bracket to the server chassis.
g. Replace the plastic air baffle.
h. Return the TS7620 Appliance Express server to the operational position, as described in "Placing the TS7610 or TS7620 to operational position" on page 29.

4. Power-on the server. To do so, refer to "TS7610 or TS7620 startup" on page 25, and then return to this page.

   You should now be logged into the server, with the server command prompt displayed.
5. Use this procedure to verify and if necessary update firmware. See "Updating and verifying the TS7610 or TS7620 firmware with the ProtecTIER Service Menu" on page 30.
6. Verify that replacing the component resolved the hardware fault. See "Verifying fault resolutions in the TS7610 or TS7620 ProtecTIER V3.3.6ProtecTIER Service menu" on page 126.

   After you have verified that the steps taken to resolve a fault were successful, and that any residual fault alert information is cleared from the ProtecTIER Manager, the component replacement is complete.

Removing and replacing a DIMM

About this task

The TS7610 or TS7620 server is equipped with six, 4GB dual in-line memory modules (DIMMs), for a total of 24GB.

Figure 60 shows the numbering order of the eight DIMM slots. The six installed DIMMs occupy slots A1 and A2, B1 and B2, C1, and D1. Slots C2 and D2 are left empty.

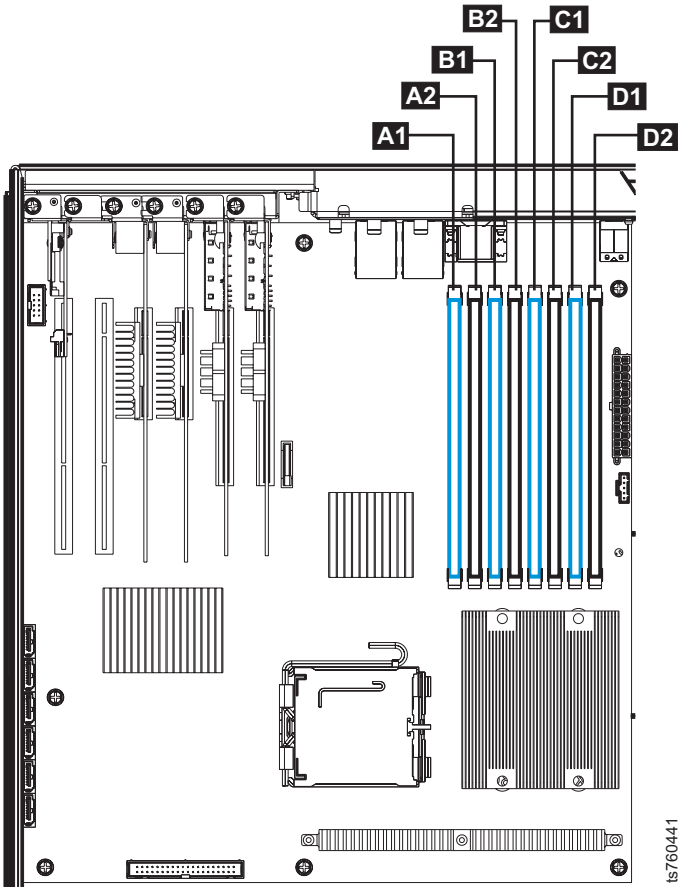


Figure 60. DIMM layout

Important:

- DIMMs are internal and cold-swappable.
- Before you begin, review the information in "Electrostatic discharge procedures" on page 23.
- Take care to avoid touching the gold contacts along the lower edge of the memory modules.

Note: To see a complete list of the TS7610 repair videos, go to the TS7610 Customer Information Center, located at: http://pic.dhe.ibm.com/infocenter/ts7600/serv/index.jsp. Once in the TS7610 Customer Information Center, search for **`repair video`** and click **`Go`**. The video list will appear in the left column.

Procedure

1. Power-off the server. To do so, refer to “TS7610 or TS7620 power off sequence” on page 23.

   After the server is fully powered-off, return to this page and continue with step 2.

2. To remove a DIMM:
   a. Place the TS7610 or TS7620 server in the service position, as described in “Placing the TS7610 or TS7620 to service position” on page 27, and remove the server's top cover.
   b. Lift and remove the plastic airflow baffle and set it aside. See Figure 61.

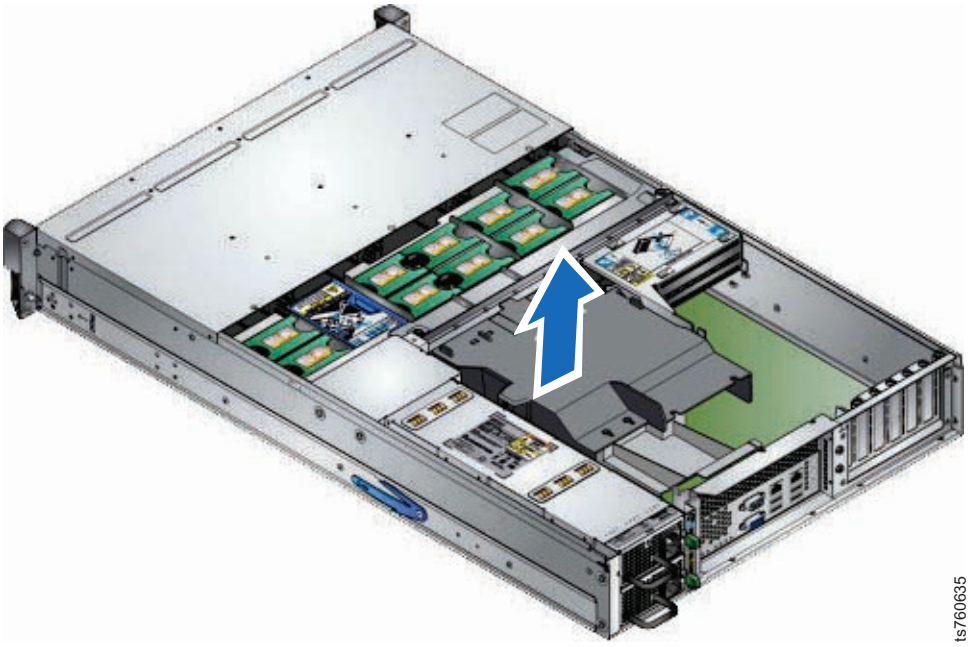


Figure 61. Remove airflow baffle

   c. Locate the defective DIMM, and simultaneously press the white release latches, located on either side of the DIMM, downward and outward until the latches lock in the open position. See Figure 62 on page 87.

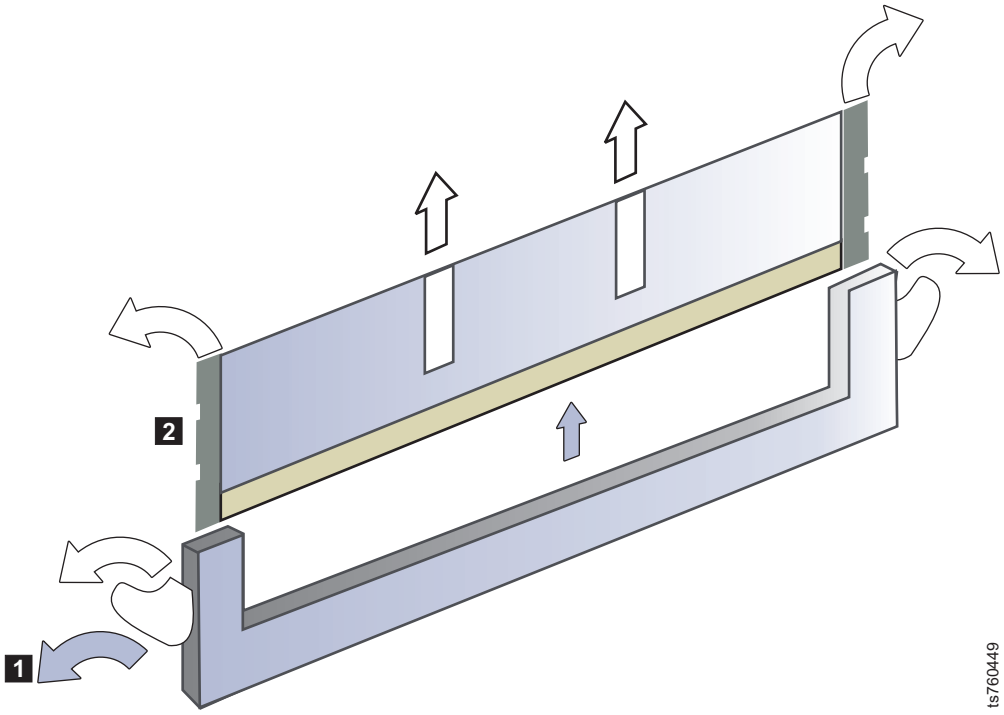


Figure 62. Remove DIMM

d. Carefully grasp the DIMM by the upper corners and lift it up and out of the slot.

3. To replace a DIMM:
   a. Remove the new DIMM from its anti-static packaging.
   b. Carefully grasp the new memory module by the upper corners and position the bottom corners of the DIMM in the upright columns.
   c. Press down gently, taking care to align the notch in the lower edge of the DIMM with the cross-piece in the bottom of the slot, as the DIMM modules are keyed to fit in only one direction.. Continue to press downward until the new DIMM is firmly seated in the slot, and the white release latches return to the closed position.

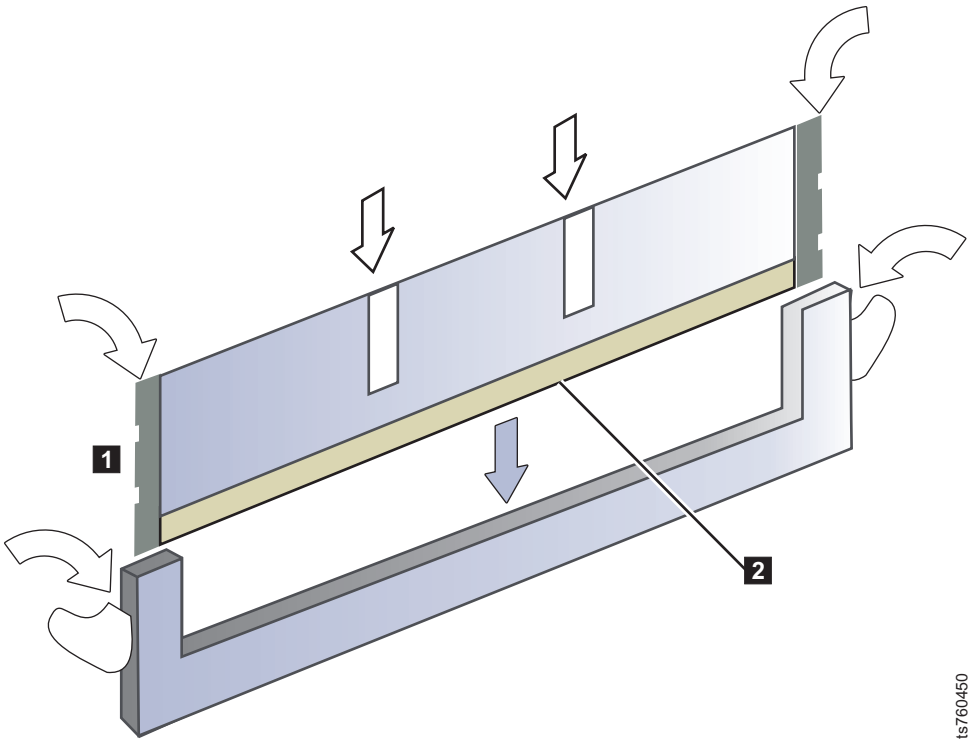


Figure 63. Replace DIMM

d. Replace the plastic airflow baffle. See Figure 64.

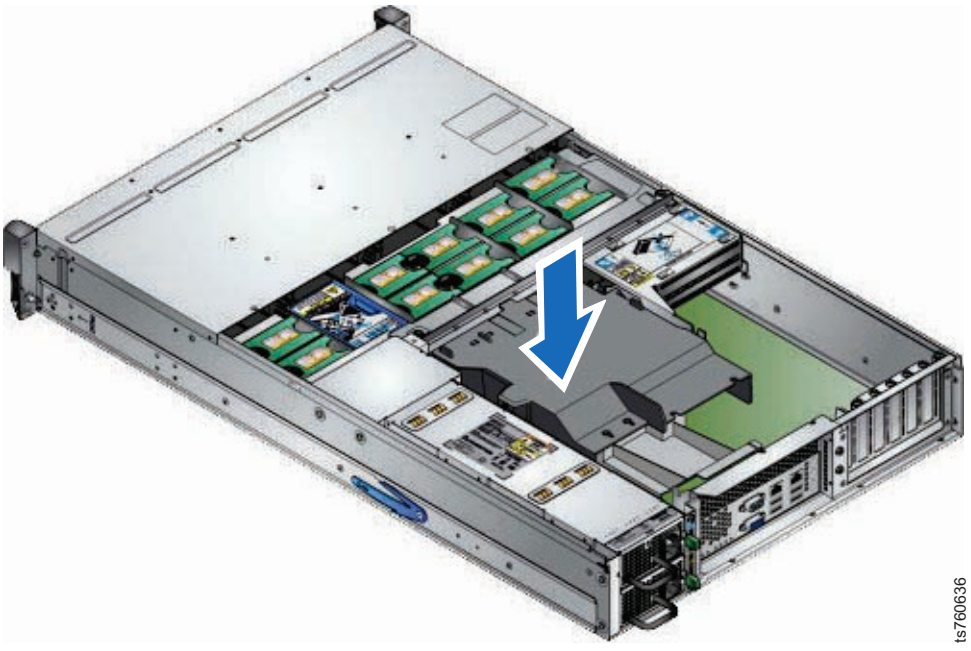


Figure 64. Replace airflow baffle

e. Return the TS7610 or TS7620 server to the operational position, as described in "Placing the TS7610 or TS7620 to operational position" on page 29.

4. Power-on the server. To do so, refer to "TS7610 or TS7620 startup" on page 25, and then return to this page and continue with step 5 on page 89.

5. To clear hardware faults following the maintenance, the ProtecTIER Manager GUI must be refreshed. If the ProtecTIER Manager GUI is not available, verify that replacing the component resolved the hardware fault, as described in "Verifying fault resolutions in the TS7610 or TS7620 ProtecTIER V3.3.6ProtecTIER Service menu" on page 126.

   After you have verified that the steps taken to resolve a fault were successful and that residual fault alert information is cleared from the ProtecTIER Manager GUI, the component replacement is complete.

Removing and replacing a TS7610 or TS7620 ProtecTIER V3.3.6 cooling fan

About this task

The TS7610 or TS7620 server is equipped with ten cooling fans. In the event of a hardware failure, the remaining fans automatically increase their speed to compensate for the loss. This allows the server to maintain an acceptable operating temperature and continue functioning.

Important:

- Cooling fans are internal and hot-swappable.
- Before you begin, review the information in "Electrostatic discharge procedures" on page 23.
- Immediately after a hardware failure, it may take a few moments for the fan blades to come to a complete stop. Use caution to avoid injury.
- To prevent system damage, replace a cooling fan within 72 hours. Leave the defective cooling fan in place until you have the new component and are ready to perform the replacement.

Note: To see a complete list of the TS7610 repair videos, go to the TS7610 Customer Information Center, located at: http://pic.dhe.ibm.com/infocenter/ts7600/serv/index.jsp. Once in the TS7610 Customer Information Center, search for **repair video** and click **Go**. The video list will appear in the left column.

Procedure

1. To remove a cooling fan:
   a. Place the TS7610 or TS7620 server in service position, as described in "Placing the TS7610 or TS7620 to service position" on page 27.
   b. Loosen the cover's holding screw **1**, press the silver button **2**, and slide the cover back to expose the fans **3**.

      See Figure 65 on page 90.

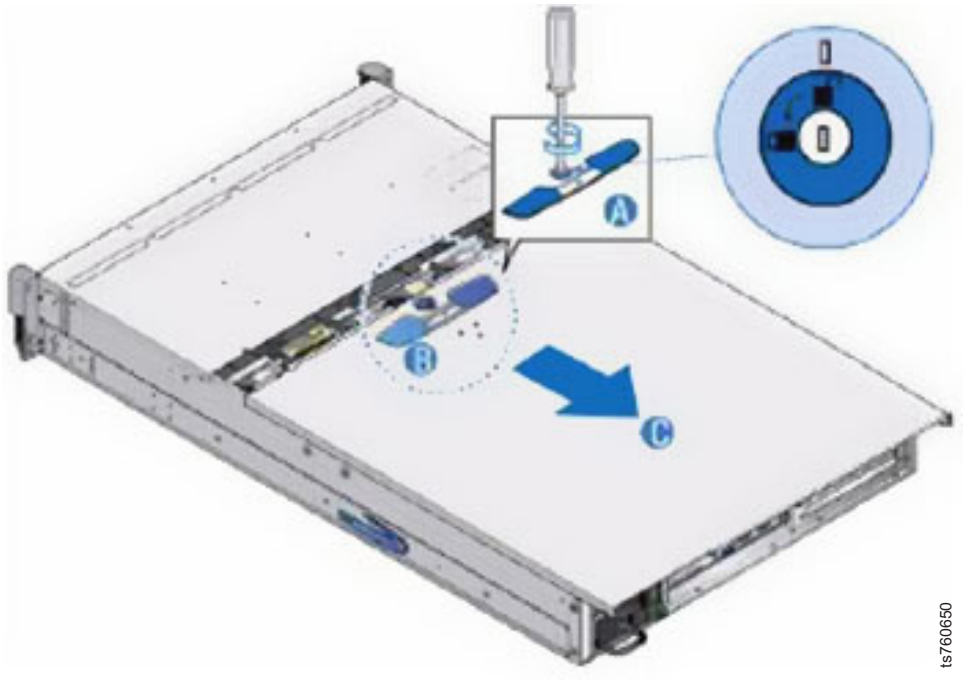


Figure 65. Expose cooling fans

c. Using Figure 66 for reference, locate the defective cooling fan.

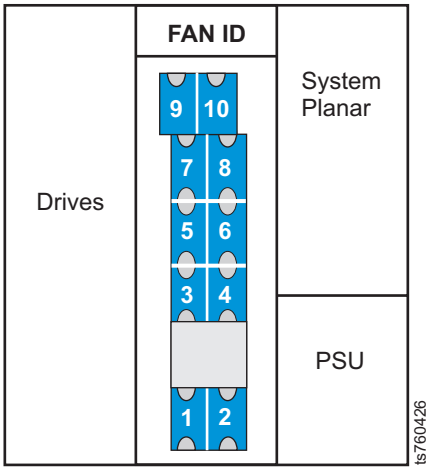


Figure 66. Cooling fan layout

d. Grasp the defective fan by the finger-holds on the top, and lift the fan up to remove it.

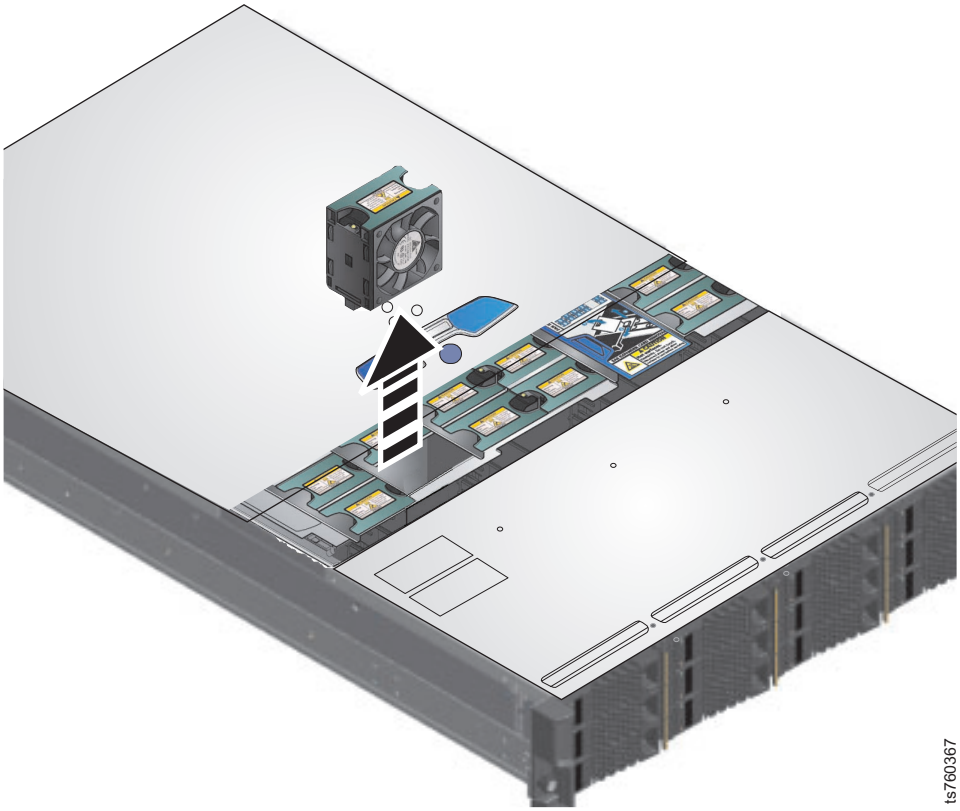


Figure 67. Removing a cooling fan

2. To replace a cooling fan:
   a. With the TS7610 or TS7620 server in service position, as described in "Placing the TS7610 or TS7620 to service position" on page 27, grasp the new fan by the finger-holds on the top and drop it into place inside the chassis:

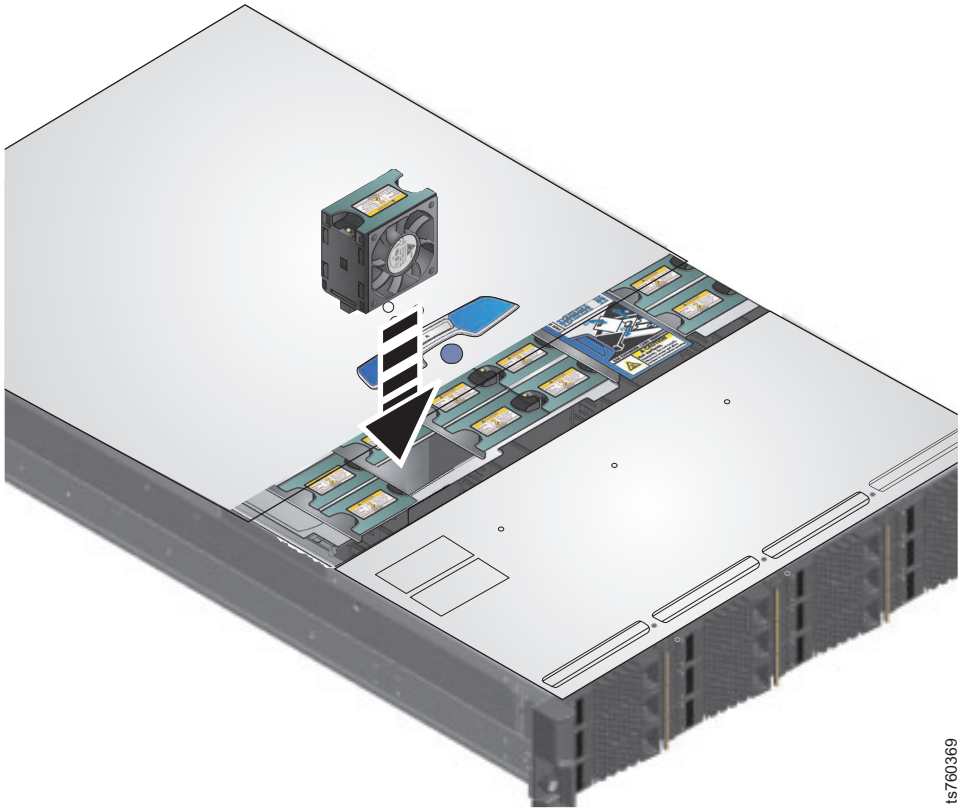


Figure 68. Replacing a cooling fan

The new fan's LED comes on and stays illuminated until the system recognizes the component. The LED then goes off and the other fans return to regular operating speed.

b. Replace the top cover, and return the TS7610 or TS7620 server to the operational position, as described in "Placing the TS7610 or TS7620 to operational position" on page 29.

3. Verify that replacing the component resolved the hardware fault, as described in "Verifying fault resolutions in the TS7610 or TS7620 ProtecTIER V3.3.6ProtecTIER Service menu" on page 126.

   After you have verified that the steps taken to resolve a fault were successful, and that any residual fault alert information is cleared from the ProtecTIER Manager, the component replacement is complete.

Removing and replacing the Ethernet adapter

About this task

The Ethernet adapter provides connectivity from the server to your local area network (LAN).

Important:

- The Ethernet adapter is internal and cold-swappable.
- Before you begin, review the information in "Electrostatic discharge procedures" on page 23.
- Take care to avoid touching the gold contacts along the lower edge of the adapter.

Note: To see a complete list of the TS7610 repair videos, go to the TS7610 Customer Information Center, located at: http://pic.dhe.ibm.com/infocenter/ts7600/serv/index.jsp. Once in the TS7610 Customer Information Center, search for **repair video** and click **Go**. The video list will appear in the left column.

Procedure

1. Power-off the server. To do so, refer to "TS7610 or TS7620 power off sequence" on page 23.

   After the server is fully powered-off, return to this page and continue with step 2

2. To remove the Ethernet adapter:
   a. Disconnect the Ethernet cable from the adapter.

      If you are unsure of the Ethernet adapter's location, refer to "TS7610 and TS7620 Appliance Express ProtecTIER V3.3.6 Parts list and hardware component replacement" on page 41.

   b. Place the TS7610 Appliance Express in the service position, as described in "Placing the TS7610 or TS7620 to service position" on page 27, and remove the server's top cover.

   c. Remove the retention screw from the adapter's mounting bracket, and set the screw aside.

   d. Carefully grasp the adapter by the upper corners and lift it up and out of the slot.

      Note: You may need to gently wiggle the adapter from side-to-side to free it from the slot.

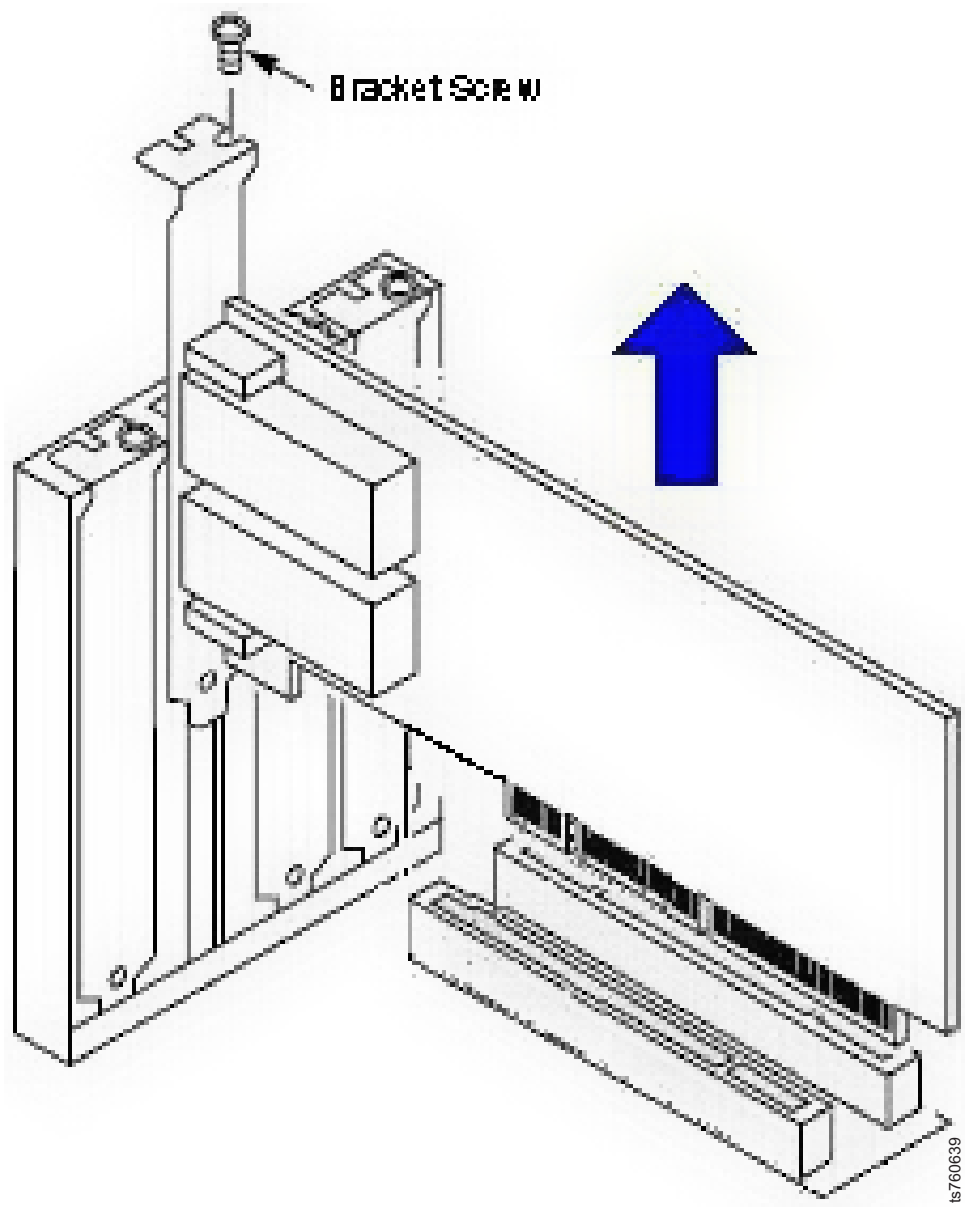


Figure 69. Remove Ethernet adapter

3. To replace the Ethernet adapter:
   a. Remove the new adapter from its anti-static packaging.
   b. Carefully grasp the adapter by the upper corners and align it with the appropriate slot.

      Note: When the component is installed correctly, the tapered tab on the lower edge of the mounting bracket will be visible when viewed from inside the chassis.
   c. Press down gently until the adapter is firmly seated.

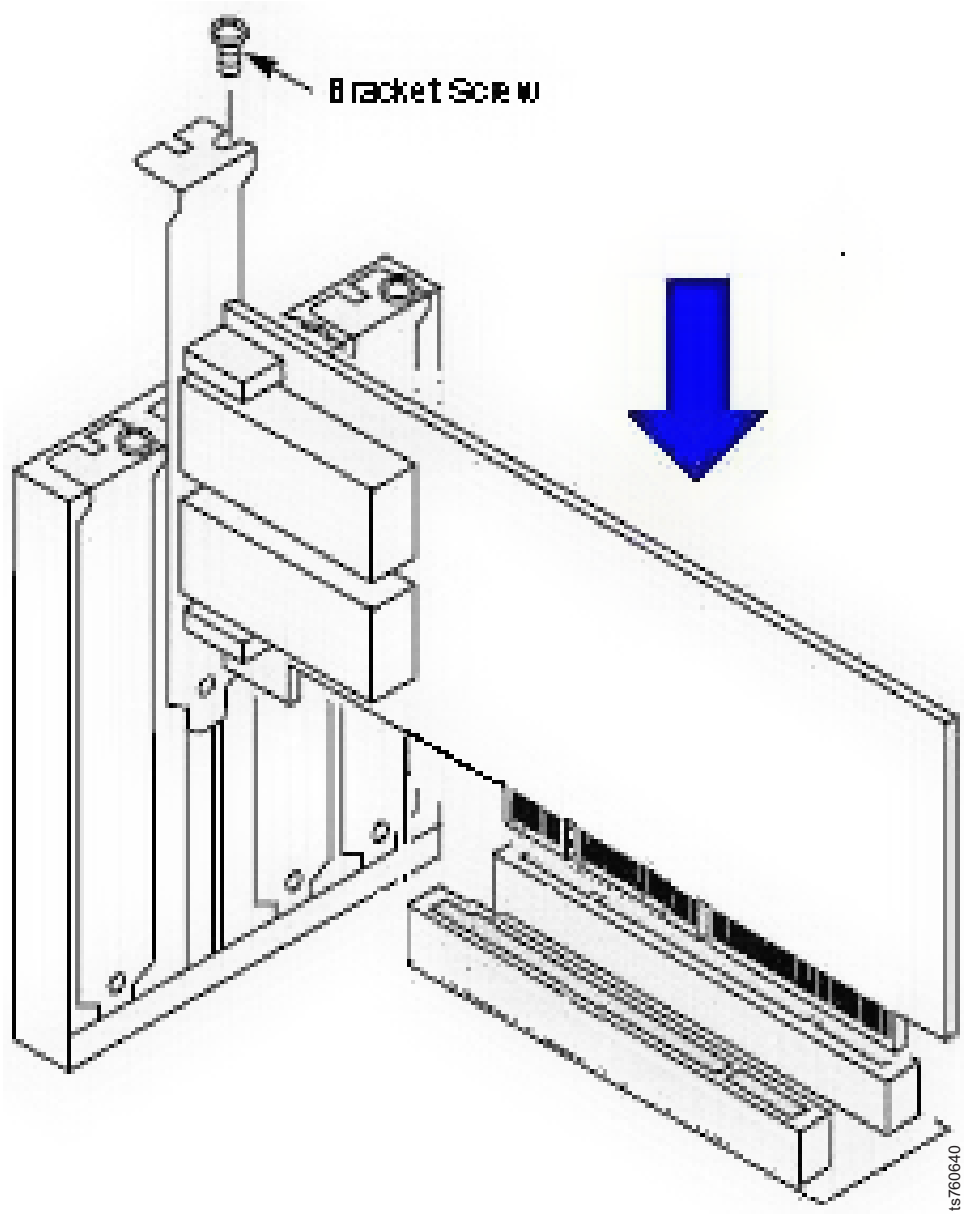


Figure 70. Replace Ethernet adapter

d. Replace the retention screw, tightening it to secure the mounting bracket to the server chassis.

e. Return the TS7610 or TS7620 server to the operational position, as described in "Placing the TS7610 or TS7620 to operational position" on page 29.

f. Reconnect the Ethernet cable to the new adapter.

4. Power-on the server. To do so, perform the steps in "TS7610 or TS7620 startup" on page 25.

   While the server is powering on the display may blink on and off. A number of status messages, which may include one or more failure notices, display on the screen. As long as the failures do not disrupt the boot cycle, ignore the messages and allow the process to continue.

   Note: During the power-on, the system auto-starts the ProtecTIER vtfd and ptcluster services. The server login prompt displays on the monitor before vtfd

and ptcluster services have finished loading. However, you cannot use the ProtecTIER Manager to access the server until the services have started completely, which may take up to 10 minutes. When service startup is complete, communication between the server and the ProtecTIER Manager is restored, and the server is ready to resume normal operation.

As the boot cycle nears completion, messages similar to those shown below, display:

```
registered calypso with major device 248
GFS: fsid=xuxoqugedahide:gfs_lv_vg0.0:fast statfs start time =
1276105582
GFS: fsid=xuxoqugedahide:gfs_lv_vg1.0:fast statfs start time =
1276105582
GFS: fsid=xuxoqugedahide:gfs_lv_vg2.0:fast statfs start time =
1276105582
GFS: fsid=xuxoqugedahide:gfs_lv_vg3.0:fast statfs start time =
1276105583
GFS: fsid=xuxoqugedahide:gfs_lv_vg4.0:fast statfs start time =
1276105583
```

5. When message activity has ceased, press **<enter>**.

   The server login: prompt displays.
6. Use this procedure to verify and if necessary update firmware. See "Updating and verifying the TS7610 or TS7620 firmware with the ProtecTIER Service Menu" on page 30.
7. Verify that replacing the component resolved the hardware fault. See "Verifying fault resolutions in the TS7610 or TS7620 ProtecTIER V3.3.6ProtecTIER Service menu" on page 126.

   After you have verified that the steps taken to resolve a fault were successful, and that any residual fault alert information is cleared from the PT Manager GUI, the component replacement is complete.

Removing and replacing a TS7610 Appliance Express and TS7620 Appliance Express power supply unit

About this task

The TS7610 or TS7620 server is equipped with dual power supply units (PSUs). This allows the system to temporarily continue functioning if one of the power supplies becomes disconnected from the AC source, or in the event of a hardware failure.

Important:

- PSUs are external and hot-swappable.
- Before you begin, review the information in "Electrostatic discharge procedures" on page 23.
- Before removing a PSU, confirm that the hardware fault was not the result of a loose or unplugged power cord.
- Only one PSU can be replaced at a time. The second PSU must remain connected to AC power.
- To prevent system damage, replace a faulty PSU within 24 hours. Do not remove a PSU until you have a replacement available.

Tip: You can access instructional videos for removing and replacing a PSU in the *Failed power supply Resolution guide*, located in the ProtecTIER Manager GUI. For instructions on accessing the Resolution guide, see "Finding information" on page 2.

Procedure

1. To remove a power supply:
   a. Working from the rear of the frame with the TS7610 or TS7620 server in operational position, disconnect the power cord from the faulty PSU.
   b. Squeeze and hold the PSU's green locking tab to the left:

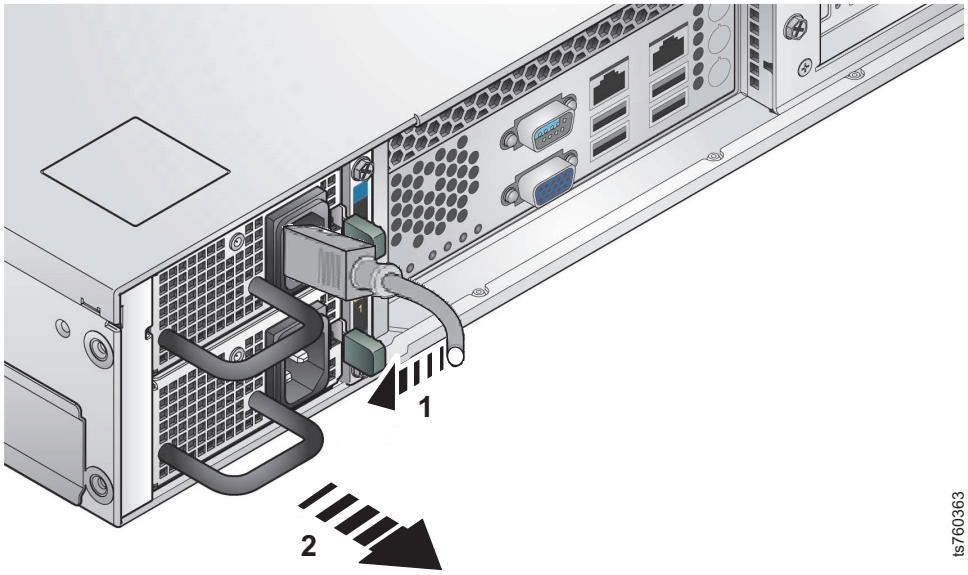


Figure 71. Squeeze the locking tab

   c. Grasp the handle and carefully pull the PSU forward to remove it from the chassis:

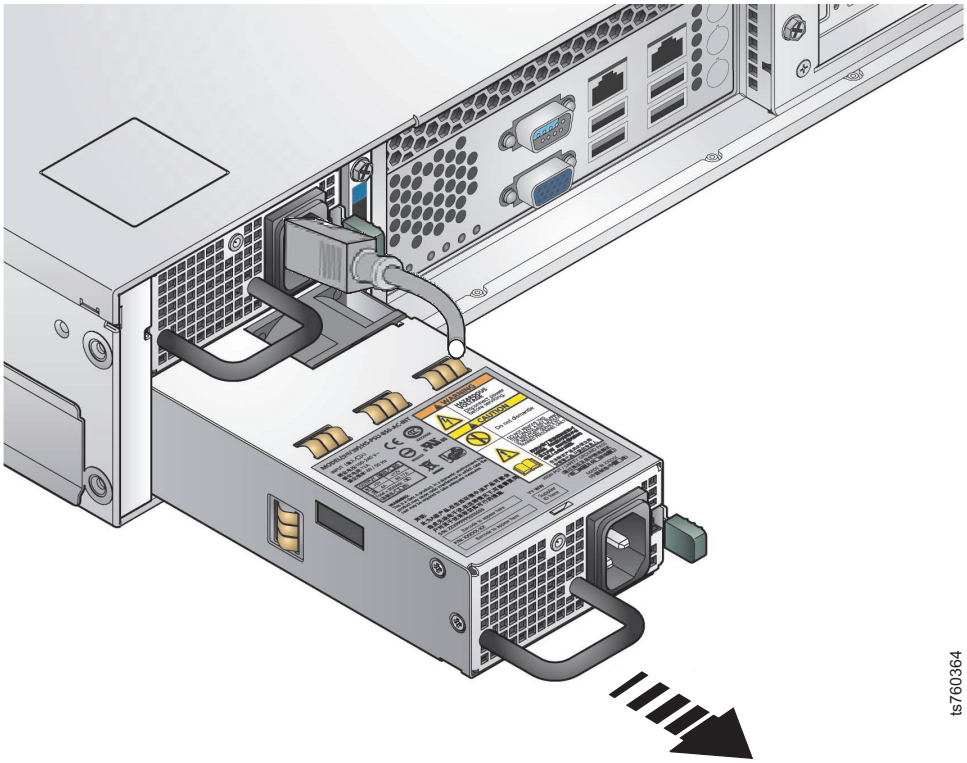


Figure 72. Remove the PSU

2. To replace a power supply:
   a. Working from the rear of the frame with the TS7610 or TS7620 server in operational position, align the new PSU with the bay in the chassis.
   b. Press the PSU forward until is firmly seated and clicks into place:

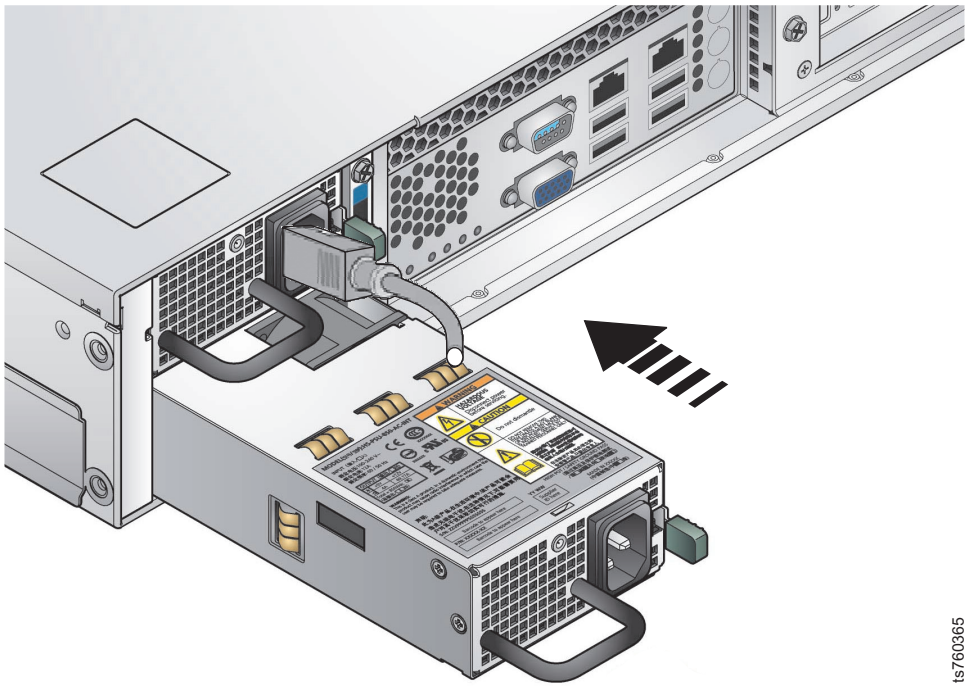


Figure 73. Replace the PSU

c. Connect the power cord from the power source to the new PSU:

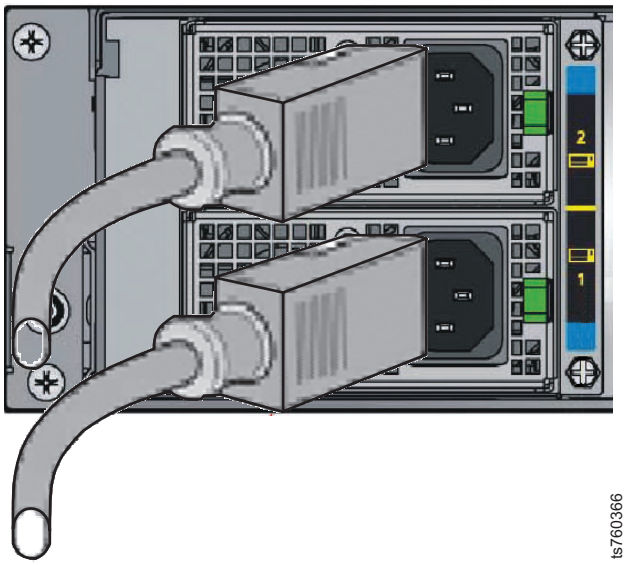


Figure 74. Connect the power cord to the new PSU

d. Fasten the wire bale across the plug to secure the cord to the server's chassis.

3. Verify that replacing the component resolved the hardware fault, as described in "Verifying fault resolutions in the TS7610 or TS7620 ProtecTIER V3.3.6ProtecTIER Service menu" on page 126.

   After you have verified that the steps taken to resolve a fault were successful, and that any residual fault alert information is cleared from the PT Manager GUI, the component replacement is complete.

Removing and replacing the RAID battery backup unit

About this task

For up to 72 hours following a power outage or power failure, the RAID battery backup unit (BBU) protects the integrity of any data residing on the MegaRAID controller.

Important:

- The RAID BBU is internal and cold-swappable.
- Before you begin, review the information in "Electrostatic discharge procedures" on page 23.
- Take care to avoid touching the gold contacts along the lower edge of the battery.

Note: Tip: You can watch the instructional video of putting the TS7610 or TS7620 server into service position by going to the TS7610 Customer Information Center, located at: http://pic.dhe.ibm.com/infocenter/ts7610/cust/index.jsp.

Once you are in the TS7610 Customer Information Center, search for **videos** and click **Go**. From the list that appears, select **Removing and replacing the RAID Battery backup unit**.

Procedure

1. Power-off the server. To do so, refer to "TS7610 or TS7620 power off sequence" on page 23.

   After the server is fully powered-off, return to this page and continue with step 2.
2. To remove the RAID BBU:
   a. Place the TS7610 or TS7620 server in the service position, as described in "Placing the TS7610 or TS7620 to service position" on page 27, and remove the server's top cover.
   b. Carefully disconnect the cable from the top of the BBU.

      If you are unsure of the BBU's location, refer to "TS7610 and TS7620 Appliance Express ProtecTIER V3.3.6 Parts list and hardware component replacement" on page 41.
   c. Remove the retention screw from the BBU's mounting bracket, and set the screw aside.
   d. Carefully grasp the BBU by the plastic shield and lift the BBU up and out of the slot.

      Note: You may need to gently wiggle the BBU from side-to-side to free it from the slot.
3. To replace the RAID BBU:
   a. Remove the new BBU from its anti-static packaging.
   b. Carefully grasp the BBU by the plastic shield and position it in the appropriate slot.

      Note: When the component is installed correctly, the tapered tab on the lower edge of the mounting bracket will be visible when viewed from inside the chassis.
   c. Press down gently until the BBU is firmly seated.

d. Replace the retention screw, tightening it to secure the mounting bracket to the server chassis.

e. Reconnect the cable from the MegaRAID controller to the top of the BBU.

Note: When connecting the cable, make sure that the side of the connector with the double row of silver contacts faces **away** from the BBU.

f. Return the TS7610 or TS7620 server to the operational position, as described in "Placing the TS7610 or TS7620 to operational position" on page 29.

4. Power-on the server. To do so, refer to "TS7610 or TS7620 startup" on page 25, and then return to this page and continue with step 5.
5. Verify that replacing the component resolved the hardware fault, as described in "Verifying fault resolutions in the TS7610 or TS7620 ProtecTIER V3.3.6ProtecTIER Service menu" on page 126.

   After you have verified that the steps taken to resolve a fault were successful, and that any residual fault alert information is cleared from the PT Manager GUI, the component replacement is complete.

Removing and Replacing a SATA hard disk drive

About this task

The TS7610 or TS7620 server is equipped with 12 serial advanced technology attachment (SATA) hard disk drives (HDDs), located on the front of the server. Drives 0 - 11 store your repository meta-and customer data. In the event of an HDD failure, the MegaRAID controller automatically redistributes the stored data from the failed HDD to drive 11, which is used as a hot spare.

Important: The figure below shows the HDDs' numbering sequence. You must maintain the original numbering order. Rearranging the order in which the drives were originally installed will result in data loss.

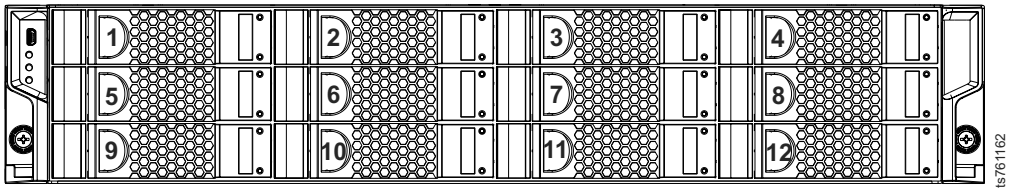


Figure 75. HDD numbering sequence

Important:

- HDDs are external and hot-swappable.
- Before you begin, review the information in "Electrostatic discharge procedures" on page 23.
- Always replace a failed hard drive with the exact manufacturer, model, and capacity; as the one that you removed.
- Be sure to install the new hard drive into the same bay that was previously occupied by the failed hard drive. Do not rearrange the original order of the drives.
- Each HDD is enclosed in a drive carrier. There is no need to remove the drive from the carrier to replace the drive.

- Slot 12 contains the Hot Spare for the array. If there is a failure of the Hot Spare drive, and replacement is required, and if a replacement drive is inserted that contains any previous information or data, you will be prompted to format that drive. If prompted, answer: Yes.

Tip: You can access instructional videos for removing and replacing an HDD in the *Failed disk drive Resolution guide* and the *Missing disk drive Resolution guide*, located in the ProtecTIER Manager. For instructions on accessing the guides, see "Finding information" on page 2.

Procedure

1. Verify the hardware fault once more before servicing the component by running a **Health check** either through the ProtecTIER Manager Service menu, refer to "Health Monitoring" on page 15 or through ProtecTIER Manager **Hardware resources**, refer to the Figure 7 on page 9.
2. To remove an HDD:
   a. Working from the front of the frame with the TS7610 or TS7620 server in operational position, confirm that the LEDs on the front of each hard drive have stopped blinking.
   b. Squeeze and hold the release latch on the defective drive's carrier to the right, toward the hinge:

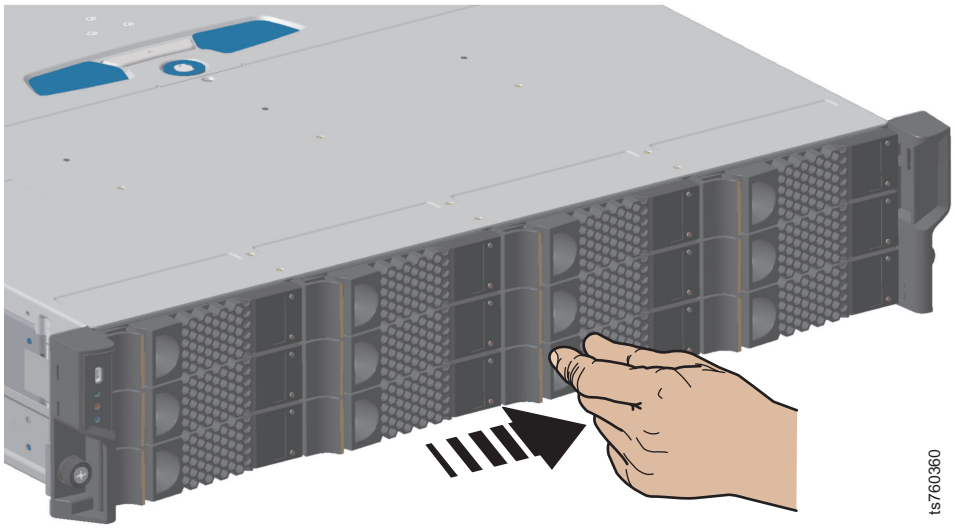


Figure 76. Squeeze drive carrier release latch

   c. Carefully slide the carrier toward you, until it is free of the drive bay.

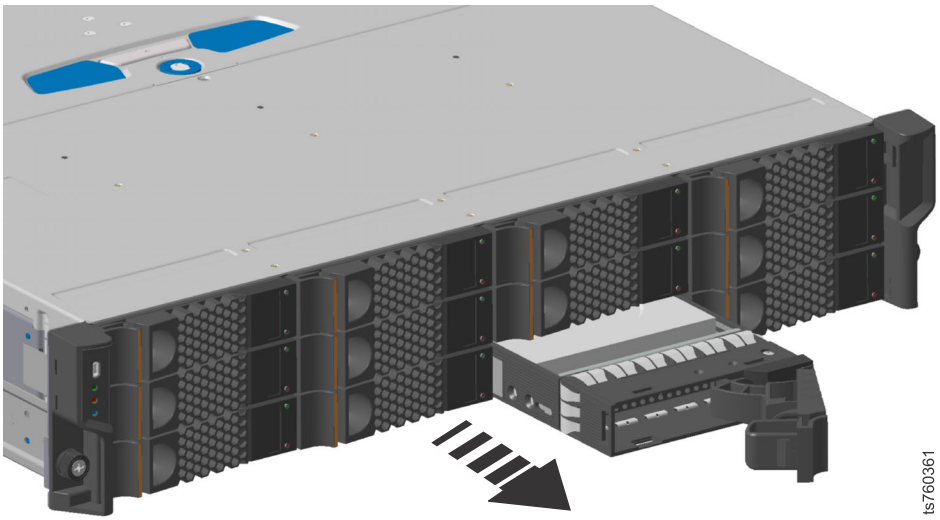


Figure 77. Remove the drive carrier

3. To replace a SATA hard drive:
   a. Working from the front of the frame with the TS7610 or TS7620 server in operational position, carefully slide the new drive carrier into the empty drive bay:

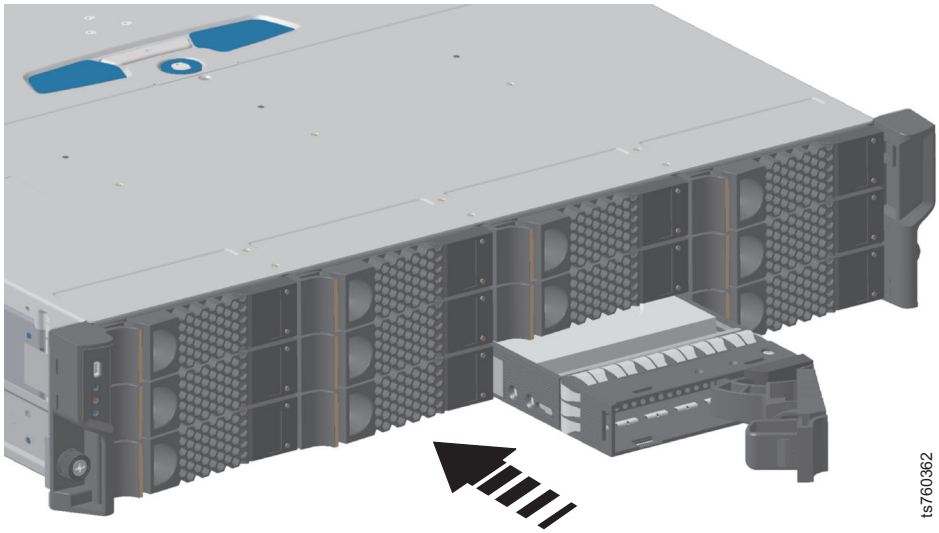


Figure 78. Replace the drive carrier

   b. Press the new drive carrier forward until it is firmly seated and the handle engages and snaps into place.

      When inserted correctly, the new drive carrier will be flush with the other drives in the bay.

4. Once replaced, the rebuilding starts automatically. The component status appears as **rebuilding** in the Health check output during the rebuild process. It might take 5 to 12 hours to complete rebuilding depending on the amount of data.
5. Verify that replacing the component resolved the hardware fault or check if the hard disk is still rebuilding, by running a **Health check** through the ProtecTIER Manager Service menu, refer to "Health Monitoring" on page 15 or check the ProtecTIER Manager **Hardware resources**, refer to the Figure 7 on page 9

   After you have verified that the steps taken to resolve a fault were successful, and that any residual fault alert information is cleared from the ProtecTIER Manager, the component replacement is complete.

Coin battery replacement procedure

This procedure describes how to replace the TS7610 or TS7620 motherboard CMOS coin battery.

About this task

Power provided by the complementary metal-oxide semiconductor (CMOS) battery helps maintain the TS7610 or TS7620 server date and time, basic input/output settings (BIOS), and other system functions, when the computer is turned off.

If you notice that the date and time frequently need to be reset when the server is powered off and on, the battery is probably starting to fail and should be replaced.

Important:

- CMOS battery repair is cold-swappable (non-concurrent) FRU.
- You may need to reset the date and time, BIOS, and other settings following CMOS battery replacement.

CAUTION:
Data will be lost if the motherboard is disconnected. Back up all data before removing/replacing the coin battery

Procedure

1. Remove the CPU/memory air duct.
2. Remove the MegaRAID controller, as described in *IBM TS7610 and TS7620 ProtecTIER Deduplication Appliance Express User's and Maintenance Guide*, v3.3, GA32-0916, and set the controller aside.
3. Pull back the spring clip that secures the battery to the motherboard.
4. Remove the CMOS battery from its holder.

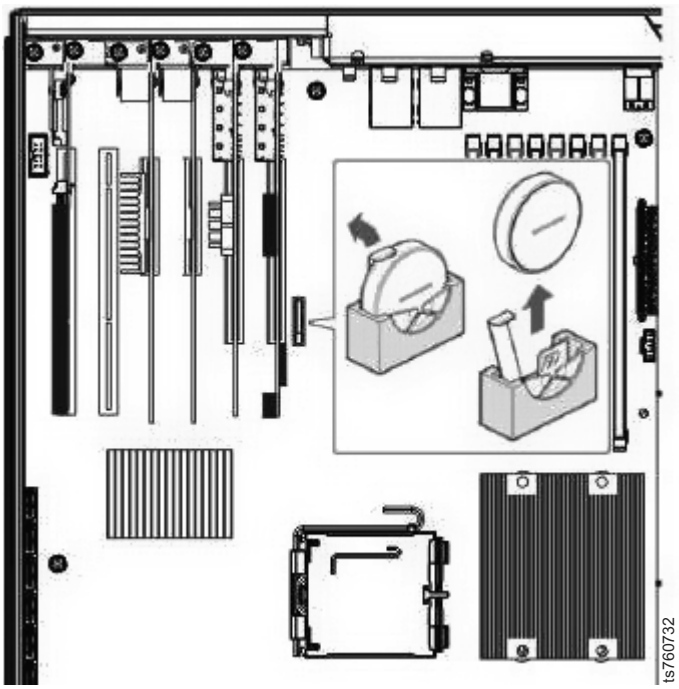


Figure 79. Removing coin battery

CAUTION:
Make sure that you replace the battery with the same type that was removed. There is a danger of explosion if the battery is replaced by an incorrect type.

5. Place the new battery into the holder, with the smooth, flat side of the battery facing away from the DIMMs.

   Note: You may need to pull the silver spring clip out to get the new battery into the holder.
6. Press down on the top of the battery to make sure it is properly seated.
7. Replace the MegaRAID controller card.
8. Replace the CPU/memory air duct.
9. Return the TS7610 or TS7620 server to the operational position, as described in "Placing the TS7610 or TS7620 to operational position" on page 29.
10. If they are not already present, connect a keyboard (USB or PS/2) and monitor to the rear of the server, and connect the monitor to a 110v power source.
11. Connect the power cords to each PSU and secure the cords with the wire bales.
12. Turn on monitor.

    Note: You cannot use the ProtecTIER Manager interface to power-on the server. It must be done manually.
13. Turn on server. Press the **On/Off** button (**5**) on the side of the server operator panel.

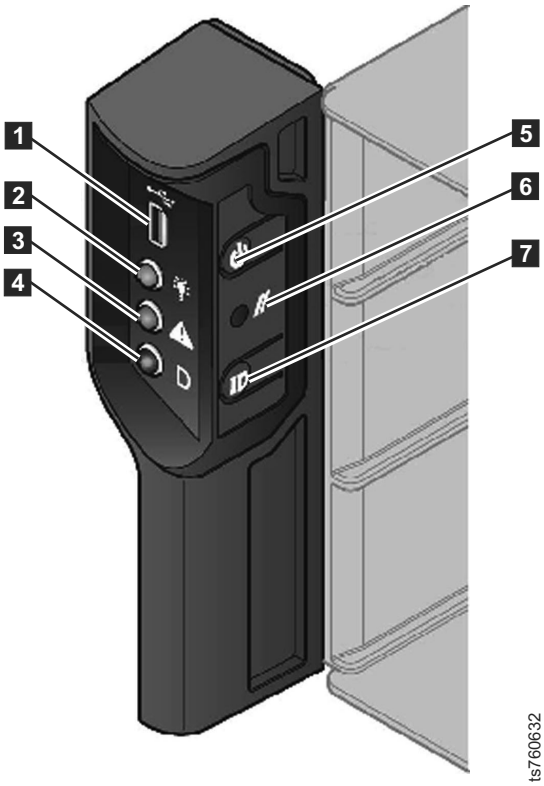


Figure 80. Server operator panel

14. Once the server has rebooted, you are done with the coin replacement procedure.

    Attention: If the server fails to boot up after replacement, follow these steps:

15. Press and hold **F2** during bootup until both the Intel screen appears and `Entering setup..` appears at the bottom of the screen. At that time you can release the F2 key. It will take a few minutes for the BIOS main menu to appear.
16. Go into BIOS by pushing F2 when prompted on the server bootup.
17. On Advanced tab go to 'Mass Storage 3. Controller Configuration'
18. Confirm 'SAS Controller' is enabled
19. Enable 'Configure SAS as SW RAID
20. On the main tab need to disable quiet boot
21. Press F10 to save and exit. The server will then reboot.

Removing and replacing the lithium ion battery

About this task

Important:

- For the TS7620:
  - It is stored in slot 7. Facing the back of the server, it is the first slot from the left. Refer to Figure 21 on page 46 for a graphical view.
- The lithium ion battery is internal and cold-swappable.

- Before you begin, review the information in “Electrostatic discharge procedures” on page 23.
- Take care to avoid touching the gold contacts along the lower edge of the controller.

Procedure

1. Power-off the server. To do so, refer to “TS7610 or TS7620 power off sequence” on page 23.

   After the server is fully powered-off, return to this page and continue with step 2.
2. Remove plastic air baffle.
3. Disconnect the cable that connects the lithium battery to the RAID card in slot 1. This cable is sometimes placed under other cards that exist in slots 2-6. The location of the cable may make it difficult to remove the cable without removing the other cards. The replacement battery includes a new cable.

   Note: The battery cable has small connections and you need care removing and connecting to the battery and the RAID card in slot 1
4. To remove the lithium ion battery:
   a. Place the TS7610 or TS7620 server in the service position, as described in “Placing the TS7610 or TS7620 to service position” on page 27, and remove the server's top cover.
   b. Carefully grasp the adapter by the upper corners and lift it up and out of the slot.

      Note: You may need to gently wiggle the adapter from side-to-side to free it from the slot. Do not use this picture as a reference for slot placement.
   c. Remove the three screw holding the battery to the card.
   d. Lift defective battery from card.
5. To replace the lithium ion battery:
   a. Remove the new lithium ion battery from its anti-static packaging.
   b. Position new battery on card to the 3 screw holes.
   c. Screw in 3 screws to hold the battery in place on the card.
   d. Reseat the lithium battery card back into the pci slot of the SM2 server.
   e. Replace the plastic air baffle.
   f. Return the server to the operational position, as described in “Placing the TS7610 or TS7620 to operational position” on page 29.
6. Power-on the server. To do so, refer to “TS7610 or TS7620 startup” on page 25, and then return to this page.

   You should now be logged into the server, with the server command prompt displayed.
7. Use this procedure to verify and if necessary update firmware. See “Updating and verifying the TS7610 or TS7620 firmware with the ProtecTIER Service Menu” on page 30.
8. Verify that replacing the component resolved the hardware fault. See “Verifying fault resolutions in the TS7610 or TS7620 ProtecTIER V3.3.6ProtecTIER Service menu” on page 126.

   After you have verified that the steps taken to resolve a fault were successful, and that any residual fault alert information is cleared from the ProtecTIER Manager, the component replacement is complete.

9. Return the used battery through the parts system for proper disposal.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATIONS "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been

estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

- AIX®
- DS4000®
- Enterprise Storage Server®
- ESCON®
- FICON®
- i5/OS™
- iSeries®
- IBM
- ProtecTIER
- pSeries
- S/390®
- ServeRAID
- System x®
- System Storage
- TotalStorage
- Wake on LAN
- z/OS®
- zSeries

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol ((R) or (TM)), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or

common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks are trademarks of Oracle, Inc. in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Electronic emission notices

This section contains the electronic emission notices or statements for the United States and other countries.

Federal Communications Commission statement

This explains the Federal Communications Commission's (FCC) statement.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device might not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

European Union Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of European Union (EU) Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Responsible Manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European community contact:

IBM Deutschland GmbH
IBM Technical Regulations, Department M456
IBM-Allee 1, 71139 Ehningen, Germany

Australia and New Zealand Class A Statement

Attention: This is a Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Germany Electromagnetic compatibility directive

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der

IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Mabnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)." Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

```
International Business Machines Corp.
New Orchard Road
Armonk,New York 10504
Tel: 914-499-1900
```

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

People's Republic of China Class A Electronic Emission statement

中华人民共和国“A类”警告声明

声 明
此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Taiwan Class A compliance statement

警告使用者:
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。 taiemi

Taiwan contact information

This topic contains the product service contact information for Taiwan.

IBM Taiwan Product Service Contact Information:
IBM Taiwan Corporation
3F, No 7, Song Ren Rd., Taipei Taiwan
Tel: 0800-016-888

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

f2c00790

Japan Voluntary Control Council for Interference (VCCI) Class A Statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

Japan Electronics and Information Technology Industries Association (JEITA) Statement (less than or equal to 20 A per phase)

高調波ガイドライン適合品 jjieta1

Korean Communications Commission (KCC) Class A Statement

이기기는 업무용으로 전자파 적합등록을 받은 기기
이오니, 판매자 또는 사용자는 이점을 주의하시기
바라며, 만약 잘못 구입하셨을 때에는 구입한 곳에
서 비업무용으로 교환하시기 바랍니다.

Russia Electromagnetic Interference (EMI) Class A Statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

rusemi

Index

Part Number: 38L6403

Printed in USA

(1P) P/N: 38L6403

GA32-0915-09