IBM TS7650G 3958 DD6 ProtecTIER Deduplication
Version 3 Release 4

Problem Determination and Service Guide

SC27-8902-03

Note:
Before you use this information and the product it supports, read the information in the *Safety and Environmental Notices* publication, SC27-4622 and "Notices" sections of this publication.

Edition Notice

This edition applies to ProtecTIER version 3.4.3.1 for the TS7650G and to all subsequent releases and modifications until otherwise indicated in new editions.

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.

About this document

This document provides problem determination information for the IBM® TS7650G ProtecTIER® Deduplication Gateway on the 3958 DD6.

Note: Cache modules and cache controllers are supported separately within the TS7650G. If the problem is known to be in the IBM attached storage component, select the hardware option and enter the appropriate Machine Type and serial number for the component. If the attached storage is not IBM branded, contact the appropriate service provider for the component.

Terminology

IBM offers two virtualization solutions:

TS7650
When used alone, this term signifies IBM's family of virtualization solutions that operate on the ProtecTIER platform.

TS7650G or Gateway
These are terms for IBM's virtualization solution from the TS7650 family that does not include a disk storage repository, allowing the customer to choose from a variety of storage options. The TS7650G consists of the following:

Server There are five types of server that have been used in the Gateway. The following are the currently supported servers:

3958 DD6
This is a higher performance server available in March 2016. The enclosure, or chassis, has space for two controller nodes in the rear, which accommodates a cluster configuration in a 2u platform and eliminates the external cluster connection kit. In the front, the 3958 DD6 contains 24 SAS drive slots (only 2 of which actually contain SAS drives). The 3958 DD6 also includes redundant power supplies in the rear of the unit.

3958 DD5
This server, which first shipped in May 2012, is based on the IBM System xy7143 model. When used as a server in the TS7650G, its machine type and model are 3958 DD5. Use this machine type and model for service purposes.

3958 DD4
This server became available in December 2010 and is based on the IBM System x3850 X5 Type 7145-PBR. When used as a server in the TS7650G, its machine type and model are 3958 DD4. Use this machine type and model for service purposes.

System console
The system console is a TS3000 System Console (TSSC). This document uses the terms *system console* and *TSSC* interchangeably. The TSSC is not available (and does not work with) the 3958 DD6.

Under IBM best practices, the TS7650G also contains the following:

Disk controller
The customer must choose the disk controller for use with the TS7650G. A list of compatible controllers is located at the IBM Tape Systems Resource Library website in the *TS7650/TS7650G ISV and interoperability matrix* document.

Disk expansion unit
The customer must choose the disk expansion unit for use with the TS7650G. A list of compatible expansion units is located at the IBM Tape Systems Resource Library website in the *TS7650/TS7650G ISV and interoperability matrix* document.

IBM Tivoli Assist On-site (AOS)
IBM Tivoli Assist On-site (AOS) is a web-based tool that enables a remote support representative in IBM to view or control the management node desktop. More information is located at the Tivoli AOS website.

replication
A process that transfers logical objects like cartridges from one ProtecTIER repository to another. The replication function allows ProtecTIER deployment to be distributed across sites. Each site has a single or clustered ProtecTIER environment. Each ProtecTIER environment has at least one ProtecTIER server. The ProtecTIER server that is a part of the replication grid has one or two dedicated replication ports that are used for replication. Replication ports are connected to the customer's WAN and are configured on two subnets as default.

replication grid
A set of repositories that share a common ID and can potentially transmit and receive logical objects through replication. A replication grid defines a set of ProtecTIER repositories and actions between them. It is configured by using the ProtecTIER Replication Manager. The ProtecTIER Replication Manager is a software component installed on a ProtecTIER server or a dedicated host. The ProtecTIER Replication Manager should be able to recognize all of the members of the entire network that it handles on both replication subnets. The ProtecTIER Replication Manager manages the configuration of multiple replication grids in an organization. An agent on every node in each ProtecTIER server interacts with the server and maintains a table of its grid members.

Note: Customers must license the Replication features on all ProtecTIER systems participating in the replication grid whether the system is sending or receiving data (or both).

replication grid ID
A number from 0 to 63 that identifies a replication grid within an organization.

replication grid member
A repository that is a member in a replication grid.

replication pairs
Two repositories within a replication grid that replicate from one to another.

replication policy
A policy made up of rules that define a set of objects (for example, VTL cartridges) from a source repository to be replicated to a target repository.

repository unique ID (RID)
A number that uniquely identifies the repository. The RID is created from the replication grid ID and the repository internal ID in the grid.

replication timeframe
A scheduled period of time for replication to take place for all policies.

shelf A container of VTL cartridges within a ProtecTIER repository.

virtual tape library (VTL)
The ProtecTIER virtual tape library (VTL) service emulates traditional tape libraries. By emulating tape libraries, ProtecTIER VTL allows you to switch to disk backup without replacing your entire backup environment. Your existing backup application can access virtual robots to move virtual cartridges between virtual slots and drives. The backup application perceives that the data is being stored on cartridges while ProtecTIER actually stores data on a deduplicated disk repository.

visibility switching
The automated process that transfers the visibility of a VTL cartridge from its master to its replica and vice versa. The visibility switching process is triggered by moving a cartridge to the source library Import/Export (I/E) slot. The cartridge will then disappear from the I/E slot and appear at the destination library's I/E slot. To move the cartridge back to the source library, the cartridge must be ejected to the shelf from the destination library. The cartridge will then disappear from the destination library and reappear at the source I/E slot.

Who should read this document

This publication is for IBM service personnel who are installing, diagnosing, or repairing the TS7650G. This publication is intended for use by IBM service personnel only.

Getting information, help, and service

If you need help, service, technical assistance, or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. Available services, telephone numbers, and web links are subject to change without notice.

Websites

IBM maintains pages on the World Wide Web where you can get the most up-to-date information about your product, including documentation and the most recent downloads.

Be sure to visit the support page for the TS7650G, complete with FAQs, parts information, technical hints and tips, technical publications, and downloadable files, if applicable. The support pages are available at IBM Tape Storage Systems (http://www.ibm.com/systems/storage/tape/).

The translated publications for this product are included with the product. These documents and product specification sheets are also available from the IBM Support Portal (http://www.ibm.com/storage/support).

For information about the TS7650, refer to the following sites:

- IBM System Storage ProtecTIER TS7610, TS7620, TS7650, TS7650G Combined Service Information Center (http://pic.dhe.ibm.com/infocenter/ts7600/serv/index.jsp)
- IBM System Storage ProtecTIER TS7650 Customer Information Center (http://pic.dhe.ibm.com/infocenter/ts7650/cust/index.jsp)

For additional websites, see Table 1.

Table 1. IBM websites for help, services, and information

Description	Web address (URL)
IBM Support Portal	http://www.ibm.com/storage/support
IBM home page	http://www.ibm.com
Directory of worldwide contacts	http://www.ibm.com/planetwide
IBM Publications Center	http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss
DS4000 information	http://www.ibm.com/systems/storage/product/disk.html
Independent Software Vendor (ISV) support	http://www.ibm.com/systems/storage/solutions/isv/index.html
TS7650/TS7650G ISV and interoperability matrix	http://www.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=IVL12348USEN
Information about SAN switches and directors	http://www.ibm.com/servers/storage/san
Information about IBM xSeries products, services, and support	http://www.ibm.com/systems/x
DS4000® Interoperability Matrix	http://www.ibm.com/servers/storage/disk/ds4000/interop-matrix.html
Firmware and software downloads, as well as associated driver code	http://www.ibm.com/support/entry/portal/Downloads
Accessibility information	http://www.ibm.com/able/product_accessibility/index.html
Product recycling programs	http://www.ibm.com/ibm/environment/products/recycling.shtml

Help and service

You can call 1 (800) IBM SERV for help and service if you are in the U.S. or Canada. You must choose the software or hardware option when calling for assistance.

Note: This product is equipped with a Software Call Home feature. When enabled, it notifies IBM Service of software error events. Not all countries currently support this feature. Contact your next level of support for more information. The Software Call Home feature is supported in all EMEA/CEEMEA countries.

Choose the software option if you are uncertain if the problem involves TS7650 software or TS7650 hardware. Choose the hardware option *only* if you are certain the problem solely involves the TS7650 hardware.

When calling IBM for service regarding the TS7650, follow these guidelines for the software and hardware options:

Software option
Identify the TS7650 as your product and supply your customer number as proof of purchase. The 7-digit customer number (0000000 to 9999999) is assigned by IBM when the PID is purchased. It should be located on the customer information worksheet or on the invoice from the software purchase.

Hardware option
Provide the serial number and appropriate 4-digit Machine Type for the hardware component that displays a problem (for example: 3958 DD4, 3958 DD5, 3958 DD6).

Note: Cache modules and cache controllers are supported separately within the TS7650G. If the problem is known to be in the IBM attached storage component, select the hardware option and enter the appropriate Machine Type and serial number for the component. If the attached storage is not IBM branded, contact the appropriate service provider for the component.

Before you call for service

Some problems can be solved without outside assistance, by using the online help, by looking in the online or printed documentation that comes with the unit, or by consulting the support Web page. Also, be sure to read the information in any README files and release notes.

Getting help by telephone

With the original purchase of the TS7650G, you have access to extensive support coverage. During the product warranty period, you can call the IBM Support Center (1 800 426-7378 in the U.S.) for product assistance covered under the terms of the hardware IBM warranty or the software maintenance contract that comes with product purchase.

Have the following information ready when you call:

- IBM TS7650G software identifier, or the machine type and model. The software identifier can be either the product name or the Product Identification (PID) number.
- Serial numbers of the TS7650G components, or your proof of purchase.
- Description of the problem.
- Exact wording of any error messages.
- Hardware and software configuration information

If possible, have access to your computer when you call.

In the U.S. and Canada, these services are available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9:00 a.m. to 6:00 p.m. In all other countries, contact your IBM reseller or IBM marketing representative.

When calling IBM for support for the TS7650G, follow these guidelines:

- If you are certain the problem involves the TS7650G software, or if you are uncertain whether the problem involves the software or hardware, choose the software option. Then identify the TS7650G as your product and supply your customer number as proof of purchase
- Choose the hardware option *only* if you are certain the problem involves solely the hardware. After you select hardware, provide the serial number and appropriate 4-digit Machine Type for the hardware component that displays a problem (for example: 3958 DD4, 3958 DD5, 3958 DD6). Cache modules and cache controllers are supported separately within the TS7650G. If the problem is known to be in the IBM attached storage component, select the hardware option and enter the appropriate Machine Type and serial number for the component. If the attached storage is not IBM branded, contact the appropriate service provider for the component.

  Note: US or Canadian Customers calling 1 (800) IBM SERV are asked to select a hardware or software option. Unless you are certain the problem involves the hardware, choose the software option.

Related publications

The following documents provide information about the TS7650G components and related hardware.

TS7650G publications

This topic lists TS7650G publications.

IBM TS7650G ProtecTIER Deduplication Gateway Introduction and Planning Guide, GA32-0918

IBM TS7650G ProtecTIER Deduplication Gateway Installation Roadmap Guide, GA32-0921

IBM TS7650GProtecTIER User's Guide for VTL Systems, GA32-0922

IBM TS7650GProtecTIER User's Guide for FSI Systems, GA32-2235

IBM TS7650G ProtecTIER Deduplication Gateway Problem Determination and Service Guide, GA32-0923

IBM TS7650 ProtecTIER Software Upgrade Guide, SC27-3643

Server publications

- *IBM System x3850 M2 and x3950 M2 Types 7141, 7233, 7144, and 7234 Problem Determination and Service Guide*
- *IBM System x3850 M2 and System x3950 M2 Type 7141 and 7233 User's Guide*
- *IBM System x3850 X5 and x3950 X5 Types 7145, 7146, 7143, and 7191 Installation and User's Guide*
- *IBM System x3850 X5 and x3950 X5 Types 7145, 7146, 7143, and 7191 Problem Determination and Service Guide*

Remote Supervisor Adapter publications

- *Remote Supervisor Adapter II Slimline and Remote Supervisor Adapter II Installation Guide*

- *Remote Supervisor Adapter II Slimline and Remote Supervisor Adapter II User's Guide*

How to send your comments

Your feedback is important in helping to provide the most accurate and highest quality information.

To submit any comments about this book or any other IBM System Storage TS7600 with ProtecTIER documentation:

- Send your comments by email to starpubs@us.ibm.com. Be sure to include the following information:
  - Exact publication title and version
  - Publication form number (for example, GC53-1196-03)
  - Page, table, or illustration numbers that you are commenting on with a detailed description of any information that should be changed

Chapter 1. Maintenance and troubleshooting

This section is the starting point for maintenance, troubleshooting, or repair of a TS7650G on the 3958 DD6.

Hardware ship group CDs

The hardware ship group for the TS7650G includes the following CDs.

The TS7650G 3958 DD6 hardware shipment includes following:

Publications CD

The publications CD contains the following customer and service documents for the TS7650G and ProtecTIER V3.4.1:

- *IBM TS7650G ProtecTIER Deduplication Gateway Introduction and Planning Guide*, GA32-0918
- *IBM TS7650G ProtecTIER Deduplication Gateway Installation Roadmap Guide*, GA32-0921
- *IBM ProtecTIER User's Guide for VTL Systems*, GA32-0922
- *IBM Problem Determination and Service Guide for the TS7650G ProtecTIER Deduplication Gateway*, GA32-0923
- *IBM TS7650 ProtecTIER Software Upgrade Guide*, SC27-3643
- Statements of limited warranty

Cache labels: Ethernet, Fibre, and power

Label instructions

Ethernet cables

Cache configuration CD-ROM

This disk contains the Red Hat Linux operating system and a kick-start file containing scripts to automate the operating system installation process. The customer can use this disk to reinstall the operating system on the server during a recovery scenario.

Software ship group DVDs

As of version 3.4.1, the TS7650 software ship group includes the following DVDs.

IBM ProtecTIER Enterprise Edition **DVD**
The *IBM ProtecTIER Enterprise Edition* DVD contains the software for the TS7650G server that runs on the Red Hat Linux operating system installed on the server. The server uses the software to present the attached disk storage to host systems as "virtual tape" and to perform other functions such as data deduplication.

IBM ProtecTIER Manager **DVD**
The *IBM ProtecTIER Manager* DVD contains the files required to install the ProtecTIER Manager graphical user interface on workstations connected to the TS7650G through a customer's Ethernet network. ProtecTIER Manager allows the user to manage the virtual tape presented to host systems by the server.

Overview of ProtecTIER Manager

ProtecTIER Manager is the primary interface to the TS7650G.

ProtecTIER Manager provides the Ethernet connection to the server Ethernet and RSA ports. It also has the client/server application software for managing the TS7650G. Refer to the *IBM ProtecTIER User's Guide for VTL Systems*, GA32-0922, for installation and setup information.

Note: The optimal screen resolution for the ProtecTIER Manager is 1280 x 1024.

Available configurations

The TS7650G is available in a single node configuration (with one server) and a clustered configuration (with two servers in one enclosure).

For more information regarding the setup of these configurations, see the section titled "Configurations" in the *IBM TS7650G ProtecTIER Deduplication Gateway Installation Roadmap Guide*, GA32-0921.

Disk configurations

The 3958 DD6 support both SATA and SAS disk configurations.

The 3958 DD6 supports the following disk configuration.

Configuration	Application
SATA SSD	Server internal hard disk drives
SATA SSD	Accessible from the rear panel. User data on attached disk storage
SAS	User data on attached disk storage

Problem resolution

This section provides problem resolution procedures.

Important: For any disaster recovery situations, contact your next level of support.

Review the information provided in "Problem resolution considerations," and then continue with "Problem resolution map" on page 5 to determine the appropriate problem resolution procedure.

If there is a problem with the RSA, see Logging in to the 3958 DD1, DD3, and AP1 (DD3-based) server through the RSA connection and Chapter 2, "System troubleshooting tools," on page 11.

Problem resolution considerations

Because of the variety of hardware and software combinations that can be encountered, use the following information to assist you in problem determination. If possible, have this information available when requesting assistance from Service Support and Engineering functions.

- ☐ Machine type and model (see "Terminology" on page xi) _____
- ☐ Microprocessor or hard disk upgrades _____

  Failure symptom _____

  - ☐ Do diagnostics fail? _____
  - ☐ What message appears in the diagnostics log? _____
  - ☐ What, when, where, single, or multiple systems? _____
  - ☐ Is the failure repeatable? _____
  - ☐ Has this configuration ever worked? _____
  - ☐ If it has been working, what changes were made prior to it failing? _____
  - ☐ Is this the original reported failure? _____

  Diagnostics version

  - ☐ Type and version level _____

  Hardware configuration

  - ☐ Print (print screen) configuration currently in use _____
  - ☐ BIOS level _____

  Operating system software

  - ☐ Type and version level _____

Comparing the configuration and software setup between working and non-working systems often leads to problem resolution.

Note: To eliminate confusion, systems are considered identical only if they are exactly alike in all the following criteria:

- Machine type and models
- BIOS level
- Adapters/attachments in the same locations
- Address jumpers/terminators/cabling
- Software versions and levels
- Diagnostics code (version)
- Configuration options set in the system
- Setup for the operation system control files

LC wrap plugs are required to run the loopback test at the host bus adapter or at the end of cables. The part numbers for the wrap plugs are as follows:

- 24P0950 (wrap connector and coupler kit)
  - 11P3847 (wrap connector)
  - 05N6766 (coupler)

The following is a list of general symptoms that can be encountered in your external disk storage devices:

- RAID controller passive
- Failed or moved cluster resource
- Startup long delay
- Systems Management or Storage Manager performance problems

In all cases, refer to the manufacturer's documentation provided with the disk storage devices.

Problem resolution map

Answer the following questions to determine the correct problem resolution procedure to perform.

1. Has the customer-set power-on password been forgotten?
   - Yes, go to Server power-on password override.
   - No, go to step 2.
2. Has a problem been reported against the server?
   - Yes, go to "Troubleshooting server problems" on page 6.
   - No, go to step 3.
3. Has a problem been reported against the preferred path?
   - Yes, go to Resolving preferred path critical events.
   - No, go to step 4.
4. Has a problem been reported against a disk controller?
   - Yes, go to Troubleshooting disk controller problems.
   - No, go to step 5.
5. Has a problem been reported against a disk expansion unit?
   - Yes, go to Troubleshooting disk expansion unit problems.
   - No, go to step 6.
6. Has a problem been reported against an Ethernet switch?
   - Yes, go to Removing and replacing Ethernet switch FRUs .
   - No, go to step 7.
7. Has a problem been reported against an Ethernet or Fibre Channel adapter?
   - Yes, refer to Chapter 6, "FRU replacement for TS7650G systems," on page 49.
   - No, go to step 8.
8. Has a problem been reported with a code update or load?
   - Yes, restart the system. If the problem persists, see Chapter 2, "System troubleshooting tools," on page 11 and contact your next level of support.
   - No, go to step 9.
9. Is there a problem with an MES or a feature?
   - Yes, go to the MES or feature documentation provided. Review the installation procedure.
   - No, return to Chapter 1, "Maintenance and troubleshooting," on page 1; a wrong path has been followed.

Troubleshooting server problems

You can troubleshoot problems with the server by answering a series of questions.

Before you begin

Attention: Before you proceed, become familiar with the server by reviewing the following topics.

- "Power, controls, and indicators" on page 25
- "Front view" on page 25
- Rear view
- For 3958 DD6:

Procedure

To troubleshoot problems with the server, answer the following questions.

1. Is the server power-on light-emitting diode (LED) (see Server rear view) solid and green?
   - Yes, go to step 2.
   - No, go to Power supply error LEDs to determine the status of the power supply. Also, follow the directions in the note at the bottom of the table, if necessary. If you suspect a power supply problem, see Server power checkout or Server power checkout.
2. Is the server system-error LED (see Server operator information panel) lit?
   - No, go to step 5 on page 7.
   - Yes, do the following:

   a. To determine which area of the server has the error, refer to the following sections.
      - Light path diagnostics
      - For 3958 DD1, DD3, and AP1 (DD3-based) servers:
        - Light path diagnostic light-emitting diodes
        - Component labeling
      - For 3958 DD4 and DD5 servers:
        - Light path diagnostic light-emitting diodes
        - Component labeling

   b. For remote supervisor adapter (RSA) failure, see the *IBM System x3850 M2 and x3950 M2 Types 7141, 7233, 7144, and 7234 Problem Determination and Service Guide*. To log in to the RSA, see Logging in to the 3958 DD1, DD3, and AP1 (DD3-based) server through the RSA connection.

   c. For system-management information control of the 3958 DD4 and DD5 over the network, use the SYS MGMT Ethernet port on the rear of the server for web access. This Ethernet connector is used only by the Integrated Management Module (IMM). To log into the IMM , see Logging in to the 3958 DD4 and DD5 servers through the IMM web interface.

   d. After you identify the LEDs on the server, see Identifying problems using status LEDs for removal and replacement procedures.

   e. Continue with step 6 on page 7.
3. Refer to Starting the diagnostic programs to run diagnostics.

   a. Ask the customer to stop all activity to the specific server.

   b. Refer to Server power features to cycle the power.

c. At the boot screen, press **F2** to run the diagnostics.
d. Follow the on-screen options.

4. Did the diagnostics run error-free and is the server system-error LED lit?
   - No, complete Chapter 8, "End-of-call procedure," on page 89 and then return control of the server to the customer.
   - Yes, go to "Problem resolution" on page 2 to review probable causes and return to step 6 when the problem is resolved. If the errors persist, see User-initiated Call Home and contact your next level of support.
5. If you came here from step 2 on page 6, or if the diagnostics do not detect any hardware errors but the problem remains during server operations, use the Problem Manager to check for any problems listed as **open**. See "Problem Manager" on page 12 for information about how to display an open problem, which can aid in resolution of the problem.
6. If ProtecTIER Manager is available, check for alerts and clear any open alerts.
   a. Select the node on which you want to check alerts.
   b. Click the **Alerts** button. The Alerts window is displayed.
   c. Take appropriate action to clear any open alerts (see ProtecTIER software Call Home events) or contact IBM Software Support for assistance.
   d. Repeat for the second node, if applicable.

What to do next

To complete the service call, go to Chapter 8, "End-of-call procedure," on page 89.

Remote support through Call Home on the 3958 DD6

Remote support is available for the TS7650G through the Electronic customer care (ECC) software enabling IBM support to offload call home packages from IBM storage products to an IBM support center. The ECC requires a secure broadband Internet connect to enable client to IBM connectivity. The Call Home feature reports failures detected by the ProtecTIER servers. Whenever a failure is detected, Call Home sends detailed error information to IBM (*home*). The IBM Service Representative can then prepare an action plan to handle the problem before traveling to the affected installation. The appliance or gateway might also periodically send support information (such as configuration, code versions, and error logs) to IBM. Doing so speeds-up problem determination and fault resolution. When enabled on the appliance and gateway, Call Home uses a connection on your Ethernet network to transmit hardware and software problem reports to IBM. Call Home is enabled and tested by IBM Service Representatives during initial system installation.

Note: The 3958 DD6 does not need a TSSC to enable the Call Home feature.

The TS7650G provides four Call Home capabilities: Problem Call Home, Heartbeat Call Home, Test Call Home, and User-Initiated Call Home; descriptions follow. RAS sends data files that may be helpful to IBM Support Center personnel for all four types of Call Home. These data files include error logs and configuration information, such as the Machine Reported Product Data (MRPD) log.

Test Call Home

The IBM Service Representative sends a Test Call Home signal after enabling the Call Home feature during initial installation. You can also send a Test Call Home to ensure that the setup is correct and that the

appliance or gateway can successfully open a Problem Management Record (PMR) in the IBM Remote Technical Assistance Information Network (RETAIN).

Problem Call Home
When RAS detects a problem, RAS initiates a Call Home operation to create a PMR in RETAIN. The PMR is a single page of text data that enables the Support Center or the Service Representative to access an action plan and a list of applicable FRU components.

Heartbeat Call Home
To ensure proper ongoing Call Home functionality, the system sends a Heartbeat Call Home on a regularly-scheduled basis. The heartbeat interval is user-defined.

User-Initiated Call Home
You can manually initiate a call home through the ProtecTIER Manager GUI.

Call Home through ECC

Electronic Customer Care (ECC) is an integrated service tool that uses the Call Home feature to provide automation of error reporting.

Electronic Customer Care is provided as a native tool of ProtecTIER software. For ECC communication to function properly, verify the following:

- Ports 80 and 443 and FTP port 21 are open for outbound traffic.
- Outgoing connections are allowed through the firewall; otherwise, unpredictable results will occur.
- The firewall is set to block and allow connections by both hostname and IP address to avoid unpredictable results.
- The ProtecTIER node can pass through any firewall to which the above IPs have access.

Refer to the IP address worksheet in Appendix B of the Installation Roadmap Guide for information regarding the default IP addresses for the Electronic Customer Care.

Table 2 on page 9 presents the capabilities of remote support with an ECC.

Table 2. Remote support capabilities through ECC

Customer site	Call Home events	• Error initiated • Heartbeat (regular interval) • Test
	Support capability	• Error-initiated problem reporting for up to 43 subsystems • Staged, error-specific data gathering • Subsystem and system console heartbeat reporting • Wellness checking • Log file storage (daily) • Code image and documentation repository (from media and RETAIN Fix Distribution Library)
	Remote support service tools	• Code image broadcast • Call home event log review • End-of-call completion report
IBM support	Remote access	• Authenticated, secure remote access • Simultaneous call in and call home • Data transmission (TCP/IP) supported
	IBM call home database	• 24/7 access by IBM support staff • Error analysis and search capability

Chapter 2. System troubleshooting tools

The ProtecTIER server includes a suite of system troubleshooting tools.

The troubleshooting tools included with the TS7650G can perform the following tasks:

- Collect system information to aid in problem determination (see "Using Dynamic System Analysis" on page 12)
- Manage problems (see "Problem Manager" on page 12)
- Monitor system health (see "System health monitoring" on page 15)
- Capture data and report errors automatically using Call Home (see Call Home)
- Collect system logs and deliver them to the Call Home database (see User-initiated Call Home)

These are discussed individually in the following sections after instructions on how to run any of the system troubleshooting command line tools.

Running command line tools

You can use the Baseboard Management Controller (BMC) to perform system troubleshooting tasks from the command line on the 3958 DD6 .

Procedure

To run the command line interface tools, complete the following steps:

1. Open a browser window and type the IP address of the BMC.
2. Log in with the userID `admin` and the password `admin`.
3. Click on remote control tab.
4. ⌂Click on **console redirection**.

   Note: Make sure popups are enabled on your browser.
5. Click on the **Java console** button.
6. When the prompt asks if you want to run the application, click **Run**.

ProtecTIER Service menu

The ProtecTIER Service menu is a text-based menu that provides access to the ProtecTIER command line interface.

The ProtecTIER Service menu eliminates the need for you to remember commands or look them up in the documentation. By navigating the menus and sub-menus, you can easily understand and choose the possible actions or queries to perform.

To access the ProtecTIER Service menu, log in with username `ptadmin` and password `ptadmin`. Then type `menu` and press **Enter**.

The script resides in the `/opt/ras/bin` directory. It displays a menu. Type the number of the operation you want to use and press **Enter**. The top-level menu is similar to the example shown in Figure 1 on page 12.

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

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

Figure 1. ProtecTIER Service menu

Note: Some of the items lead to sub-menus, which are denoted by **(...)**. See "Problem Manager" for the Health Monitoring menu structure.

Using Dynamic System Analysis

Dynamic System Analysis (DSA) collects and analyzes system information to aid in diagnosing server problems.

Procedure

1. To access DSA from the ProtecTIER Service menu, select **Generate a service report**. The following options display:

```
Please choose a profile:
1)  Default - Collects all system information reports and all log
    files from the either the last 4 days, or a maxiumum of 10 file
    entries, whichever comes first
2)  Performance - Used to troubleshoot performance-related issues
3)  Deduplication - Used to troubleshoot deduplication-related issues
4)  Basic - Used when customer has an issue that requires a quick
    problem determination
5)  Monitoring - Used in cases where Support provides frequent summaries
    on the system's health and behavior
6)  Full - Collects all system information reports and all log files
    in their entirety
7)  Systemview - Collect system information required to generate the
    system view html output
8)  Coredump - Collects the vmcore dumps from the system
q)  Quit
Choose:
```

2. Choose a profile from the options displayed. Type the corresponding number and press Enter.

Problem Manager

Problem Manager is the Reliability, Availability, and Serviceability (RAS) component that processes problems detected by system health monitoring.

Problem Manager consolidates the detected problems, filters out duplicate and sympathetic problems (secondary problems that are generated by primary problems), and maintains a problem log of the results (all open primary problems) for use in service actions and information.

Accessing Problem Manager from the ProtecTIER Service menu

You can access Problem Manager from the ProtecTIER Service menu.

Problem Manager tools are available from the ProtecTIER Service menu (see "ProtecTIER Service menu" on page 11) and from the command line. The preferred way to access the tools is through the ProtecTIER Service menu.

To access Problem Manager tools from the ProtecTIER Service menu, type the number of the operation you want to use and press Enter.

- To get a list of open problems, select **Health Monitoring** > **List open problems**.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
  Health Monitoring (...)
--------------------------------------------------------------------------
   1) Display health summary for this node
   2) Display detailed health for this node
   3) Run a full check on this node
   4) Reset RSA/IMM
   5) List open problems
   6) Service Mode
   7) Enable cluster switch trunk check

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

Figure 2. ProtecTIER system Health Monitoring menu

- To close or cancel an open problem once it has been fixed, select **Health Monitoring** > **List open problems**. Follow the on-screen instructions to either run the full refresh process or skip it, and respond `yes` or `no` to close out the problem records. Read the screen carefully to determine the correct choice of action in your responses.

```
Problem Record 1: problemID=<1304366542460>
        problem type=SW
        component type=protecTier
        component location=Node 0/PT
        problem severity=DEGRADED
        number of occurrences=14
        time of first occurrence=2011-05-02,19:39:59
        time of last occurrence=2011-05-02,22:40:41
        notify state=Sent by node 0
        notify time=2011-05-02,20:02:56
        message iDs={0xAA043040}
["MESSAGE:<1304366542460>"][1] => {messageID(0xAA043040) message("Internal error
 (3377699721773068) in file source_dir/cmnt/process/service_quorum.cc line 1071.
") debugInfo(".")}

Number of Problem Records is 1
>>> You can choose to cancel a problem.
Please note that if problem still exists a new similar problem may reoccur.

Do you want to cancel a problem?
Enter y or yes to cancel a problem or any other key to exit. (yes|no) yes
>>> Please enter Problem Record Number to cancel : 1
>>> Are you sure you want to cancel Problem Record 1? (yes|no) yes
End Processing Procedure Successfully

Press <ENTER> to continue
```

Figure 3. Canceling a problem

Note: Allow up to 20 minutes for Service Mode to be disabled.

Service Mode is used to inhibit Call Home, SNMP, and email alerts. Service Mode is available with ProtecTIER V3.1 or later. It should be enabled at the start of a service call and disabled at the End-of-call. A health check shows degraded when Service Mode is enabled. Service Mode is automatically disabled after 48 hours.

To enable Service Mode, select **Health Monitoring** > **Service Mode**. Then type `yes` and press Enter.

If the ProtecTIER Service menu is not available, run the Problem Manager commands from a server command line (see "Accessing Problem Manager from the command line").

Accessing Problem Manager from the command line

You can access Problem Manager directly from the command line.

If the ProtecTIER Service menu is not available, run the Problem Manager commands from a server command line.

Get open problems: The following command retrieves and displays all open problems from Problem Manager. Each problem is identified by a unique 12-digit problem ID.

`rsCerPMGetOpenProblems`

Arguments

This command takes no arguments.

Cancel problem: This command closes an open problem in the problem log after it is fixed.

`rsCerPMCancelProblem` *`problemID`*

Arguments

Other than the problem ID, this command takes no arguments.

problemID: The unique 12-digit number (displayed by `rsCerPMGetOpenProblems`) that identifies the problem.

Refer to Chapter 2, "System troubleshooting tools," on page 11 for instructions about how to run the command line tools.

System health monitoring

Various tools are provided for monitoring system health.

The preferred method for monitoring system health is using the ProtecTIER Service menu. See "Accessing Problem Manager from the ProtecTIER Service menu" on page 13. If the ProtecTIER Service menu is not available you can monitor system health using the command line tools.

System health monitoring command line tools

This topic describes system health monitoring command line tools.

The system health monitoring tool consists of the following:

System health monitoring daemon

The system health monitoring daemon controls system component status changes, schedules and runs required health monitoring programs and scripts, and provides an interface for checking execution based on user requests. The daemon runs upon system startup.

Health monitoring scripts and programs

These perform checks against specific system components or elements known as *health point elements*. Health point element summary data include:

- Name of the health point element (for example, "internal network").
- Type of health point element. These include Network, Filesystem, Server, Devices, ProtecTIER Software, and Reliability, Availability, and Serviceability (RAS).

  Note: The ProtecTIER server only calls home for the Disk Controller and expansion units when attached to the TS7650 Appliance.
- Point identifier, which together with the path uniquely identifies the health point.
- Path format. This includes the node identifier (Node 0 or Node 1). If a disk repository related element, the path includes the disk array identifier and the disk tray identifier.

  Note: Node 0 refers to the lower server normally described as Node A and Node 1 refers to the upper server which is normally described as Node B.
- Location description (for example, "left power supply").
- Timestamp indicating the latest health point update.
- Health point element status. Values are:
  - OK
  - WARNING

  - DEGRADED
  - FAILED
  - OFFLINE
  - SERVICE (currently not used)
  - UNCONFIGURED
- Expiration time/status interval. The maximum amount of time for each of the components listed below before the system rechecks itself by running its own internal health checks:
  - Network: 10 minutes
  - Filesystem: 20 minutes
  - Server: 25 minutes
  - Devices: 15 minutes
  - ProtecTIER software: 30 minutes
  - RAS: 30 minutes
- Health status message

XML status file
The current status of system components resides in this file.

Interface tools
The interface tools allow collection of information from the XML status file and display the information collected. They also allow the user to monitor the status of currently running checks or to run any check immediately. See "Using system health monitoring command line tools."

Log files
The log files record the results of checks, status changes, and detailed error correction action information.

Using system health monitoring command line tools

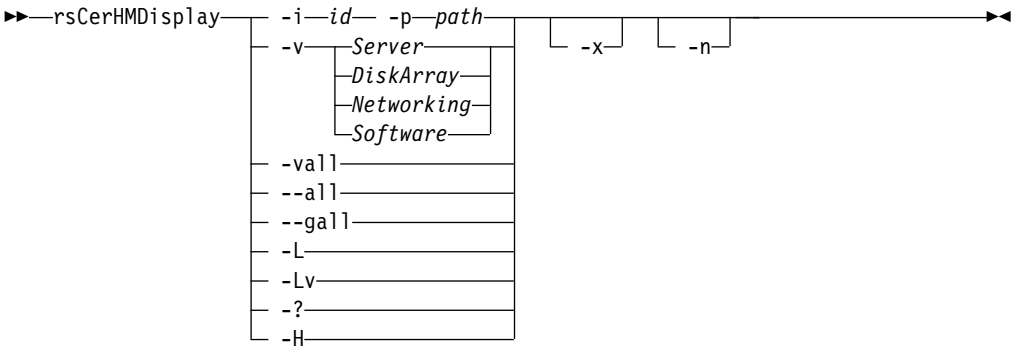
You can use system health monitoring tools directly from the command line.

In a command line session to the server, you can use two commands related to system health monitoring:

Command	Description
rsCerHMDisplay	**System health monitoring display.** This tool is used to view the results of the latest check that was performed on the system. This utility is also available through the ProtecTIER Service menu (see "ProtecTIER Service menu" on page 11). Select **System Health Monitoring** > **Display All System Health Points**.
rsCerHMStatusCtl	**System health monitoring status control.** This tool is used to immediately invoke one or more checks on the system. To view the results, type the display command.

System health monitoring display

The **rsCerHMDisplay** command provides access to the system health monitoring display.



-i *id* **-p** *path*
Display the status of the specified healthpoint (ID and path).

-v Display the status of the specified virtual object.

-vall Display the status of all virtual objects.

--all Display the status of all health points.

--gall Display the status of all health points in groups.

-L Return the status of the system:

- **0** All OK or unconfigured
- **1** Any number of OFFLINEs
- **2** Any number of WARNINGs
- **3** Any number of DEGRADEDs
- **4** Any number of FAILEDs

-Lv Display the status of the system in words.

-x Convert any output to XML.

-n Do not check for the system state before trying to run.

-? Display the syntax for the command.

-h Display the syntax for the command.

Some examples are shown in Figure 4 and Figure 5.

```
rsCerHMDisplay -i "harddrive1" -p "Node 0"
TS7650 Checkout Version 4-3.2.21_020410 executed on: 2010-02-07T04:13:07
Verify state of harddrive1 (Node 0) ........................... DEGRADED
------------------------------------------------------------
*DEGRADED: Component Location: messi.haifa.ibm.com
*DEGRADED: SRN: 0xAA020095
*DEGRADED: Hard Drive 1 Fault
------------------------------------------------------------
```

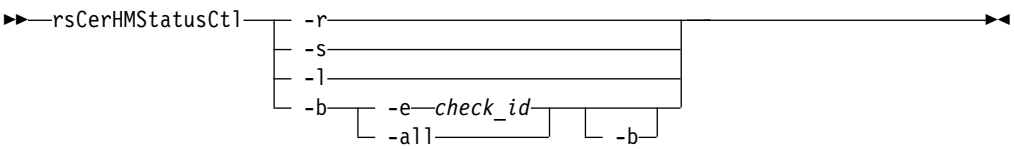
Figure 4. Displaying status of a hard drive

```
rsCerHMDisplay -i "PowerFan 2" -p "DiskArray-180-1/Enclosure85"
TS7650 Checkout Version 4-3.2.21_020410 executed on: 2010-02-07T04:13:07
Verify state of PowerFan 2 (DiskArray-180-1/Enclosure85) ........ OK
```

Figure 5. Displaying status of a power supply and fan

System health monitoring status control

The **rsCerHMStatusCtl** command provides access to system health monitoring status control.



-r List the checks currently running on the component queried.

-s List the current status of all health point checks, including name, when last run, and whether the check is currently running on the component queried.

-l List the check IDs of all possible checks, one per line.

-b Perform one or more checks, as indicated by the additional arguments:

-e *check_id*
Perform the specified check immediately.

-all Perform all checks immediately.

-b Force the health monitoring daemon to run the specified checks the next time it starts.

Some examples of arguments are shown in Figure 6, Figure 7 on page 19, and Figure 8 on page 19.

```
>rsCerHMStatusCtl -l
hwCheck
fsCheck
ds4kCheck
rasCheck
ptCheck
networkCheck
serverCheck
```

Figure 6. Listing all possible checks

```
> rsCerHMStatusCtl -s
There are currently 7 checks registered

Check ID: hwCheck
   Name: Hardware check
   Duration: 900
   Description: Checks the frontend and backend adapters
   Instances Running: 0
   Last Started at: Dec 22  13:37:44
   Last Completed at: Dec 22  13:37:53
   Last Return Code: 0
   Next Scheduled at: Dec 22  13:52:44

Check ID: fsCheck
   Name: Filesystem check
   Duration: 1200
   Description: Checks the local filesystem
   Instances Running: 0
   Last Started at: Dec 22  13:42:44
   Last Completed at: Dec 22  13:42:45
   Last Return Code: 0
   Next Scheduled at: Dec 22  14:02:44
```

Figure 7. Listing status of all health point checks

```
> rsCerHMStatusCtl -e ds4kCheck
ds4kCheck:0
> rsCerHMStatusCtl -r
Check ID: ds4kCheck
   Name: DS4000 hardware check
   Started at: Dec 22  13:50:01
   Timeout at: Dec 22  13:55:01
There are 1 checks currently active
```

Figure 8. Performing a specific check immediately

Remote support through Call Home

Remote support is available for the TS7650G through the Call Home capability provided either in the ProtecTIER software or with TSSC. Please note that TSSC with the Call Home feature is not available on the 3958 DD6 server; however, Call Home is supported for 3958 DD6 using native call home tools provided in the ProtecTIER software. The Call Home feature reports failures detected by the ProtecTIER servers. Whenever a failure is detected, Call Home sends detailed error information to IBM (*home*). The IBM Service Representative can then prepare an action plan to handle the problem before traveling to the affected installation. The appliance or gateway might also periodically send support information (such as configuration, code versions, and error logs) to IBM. Doing so speeds-up problem determination and fault resolution. When enabled on the appliance and gateway, Call Home uses a connection on your Ethernet network to transmit hardware and software problem reports to IBM. Call Home is enabled and tested by IBM Service Representatives during initial system installation.

Tip: To enable Call Home, go to the TSSC General Settings page. The Call Home option allows you to select either a Modem or Ethernet interface. Set the Call Home option to use the Ethernet interface for the most reliable error notification.

When the Reliability, Availability, and Serviceability (RAS) software on the ProtecTIER 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 TS7650Gprovides four Call Home capabilities: Problem Call Home, Heartbeat Call Home, Test Call Home, and User-Initiated Call Home; descriptions follow. RAS sends data files that may be helpful to IBM Support Center personnel for all four types of Call Home. These data files include error logs and configuration information, such as the Machine Reported Product Data (MRPD) log.

Test Call Home
The IBM Service Representative sends a Test Call Home signal after enabling the Call Home feature during initial installation. You can also send a Test Call Home to ensure that the setup is correct and that the appliance or gateway can successfully open a Problem Management Record (PMR) in the IBM Remote Technical Assistance Information Network (RETAIN).

Problem Call Home
When RAS detects a problem, RAS initiates a Call Home operation to create a PMR in RETAIN. The PMR is a single page of text data that enables the Support Center or the Service Representative to access an action plan and a list of applicable FRU components.

Heartbeat Call Home
To ensure proper ongoing Call Home functionality, the system sends a Heartbeat Call Home on a regularly-scheduled basis. The heartbeat interval is user-defined.

User-Initiated Call Home
You can manually initiate Call Home from the TSSC GUI to collect a product engineering (PE) package.

For more information about Electronic Customer Care (ECC) and TSSC, refer to the following topics:

- "Call Home through ECC" on page 8
- Call Home through the TSSC

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

servers. See the *IBM TS7620 ProtecTIER Deduplication Appliance Express® Installation and Setup Guide for VTL Systems*, GA32-0914 for instructions on SNMP configuration. For 3958 DD4 servers, see the *IBM ProtecTIER User's Guide for VTL Systems*, 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)
      - 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 23. 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.

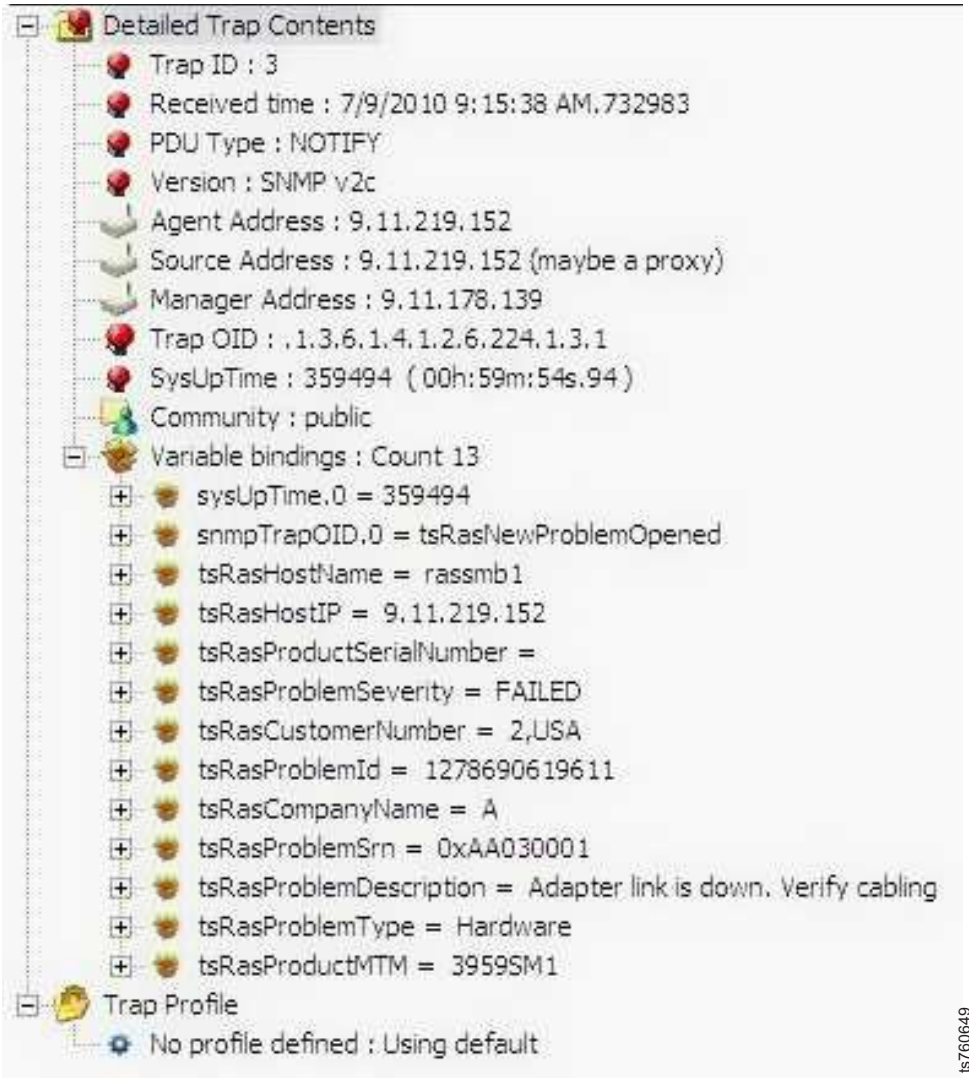


Figure 9. SNMP trap report

Chapter 3. 3958 DD6 ProtecTIER server

This section provides detailed information about the 3958 DD6 ProtecTIER server, such as explanations of the controls and indicators.

Component labeling

The colors of component labels indicate different types of components.

A blue label on a component or near a component indicates touch points, where you can grip the component to remove it from or install it in the server, open or close a latch, and so on.

An orange label on a component or near a component indicates that the component can be hot-swapped. This indicates that if the server and operating system support hot-swap capability, you can remove or install the component while the server is running.

Note: Orange can also indicate the touch points on hot-swap components.

Use the procedures in "Removing and replacing FRUs in 3958 DD6 servers" on page 49 for removing or installing a specific component.

Note: Adapters in the TS7650 (including the hot-swap adapter ports) are not hot-swap capable due to the limitations of the Linux operating system. The system must be shut down when an adapter needs to be replaced.

Power, controls, and indicators

The topics in this section describe the controls and indicators for the 3958 DD6 server.

Front view

This topic describes the front view of the two 3958 DD6 server models.

Figure 10 on page 26 shows the controls, LEDs, and connectors on the front of the server.

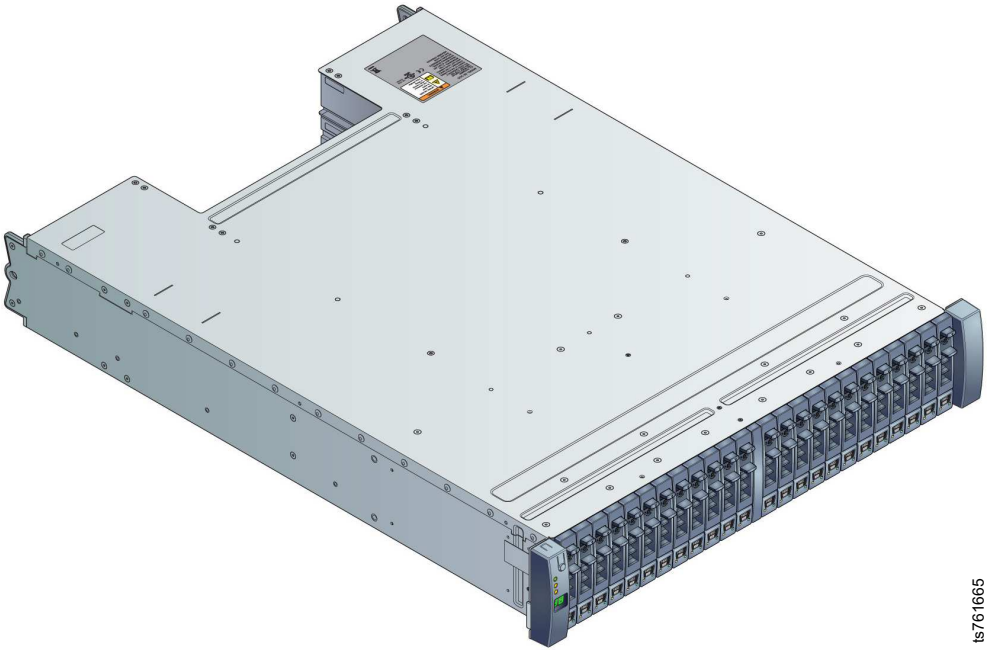


Figure 10. Front view of the 24 component server model

The front of the enclosure contains the 24 drive slots, each of which accommodates a plug-in drive carrier module that support 2.5 inch form factor SAS or SATA disk drives. SATA drives require a SAS-SATA bridge card. There are two operators panels, one on each side of the front of the server, that provide status LEDs, enclosure ID and an alarm silence button.

Operator information panels

This topic describes the operator information panels on the front of the 3958 DD6 servers.

Figure 11 shows the controls and LEDs on the operator information panel.

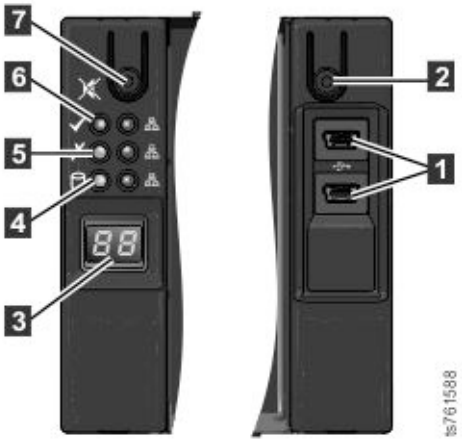


Figure 11. Operator information panels (left and right)

The following controls and LEDs are on the operator information and control panel on the right and left sides of the server.

1 Two Mini-B type USB 2.0 sockets, one connected to each controller.

2 Power button. You can use the power button in one of two ways:

A quick press of the button causes a soft shutdown of the controllers.

Holding the button for 4 seconds immediately performs a hard power off of the controllers –Note: this could cause data loss.

3 The Unit ID Display usually displays the enclosure identification number (for use with multiple enclosure systems), but can be configured via VPD.

4 Logical Fault LED - when this LED is amber, it indicates a system hardware fault. There may also be an associated fault LED on a PCM or controller identifying the faulty component.

6 The System Power LED displays the system Off, Standby, and On status.

Off The system is off.

Amber
The system is in standby and not operational.

Green The system is on and operational.

7 Input mute button is used in the setting of the LED display. Also used to transition alarm states (although this is dependent on the VPD setup).

Rear view

This topic describes the connectors located on the rear of the 3958 DD6 servers.

Figure 12 shows the connectors on the rear of the server.

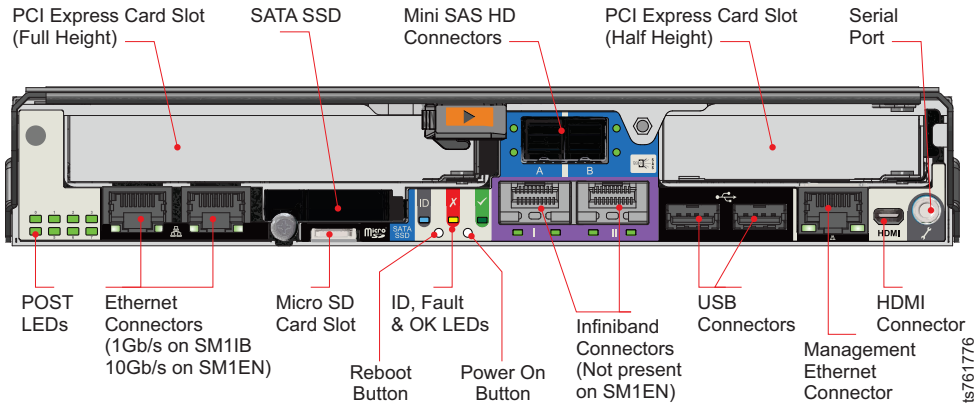


Figure 12. Server rear view

Figure 12 shows the connectors on the rear of the server.

PCI Express Card (Full Height)
Full height PCIe cards can be used to provide host attachment via Fibre Channel, Fibre Channel over Ethernet (FCOE), iSCSI or other technologies depending on requirements. This card can be a Host Bus Adapter (HBA), a Network Interface Card (NIC) or a Converged Network Adapter (CNA). PCIe cards are connected to the controller motherboard by means of a riser card.

SATA SSD
Serial attached solid state drive

Mini SAS HD Connectors
Serial Attached SCSI (SAS) is a point-to-point serial protocol that moves data to and from computer storage devices such as hard drives and tape drives.

PCI Express Card (Half Height)
Half height PCIe cards can be used to provide host attachment via Fibre Channel, Fibre Channel over Ethernet (FCOE), iSCSI or other technologies depending on requirements. This card can be a Host Bus Adapter (HBA), a Network Interface Card (NIC) or a Converged Network Adapter (CNA). PCIe cards are connected to the controller motherboard by means of a riser card.

Serial port
An RS-232 standard port for interface with a modem or with a similar communication device.

HDMI Connectors
A High-Definition Multimedia Interface connector, an audio/video interface for transferring uncompressed video data and compressed or uncompressed digital audio data.

Management Ethernet Connector
A 1Gb/s port that is used to connect to the x86 subsystem or directly to the baseboard management controller (BMC). Supports the Intelligent Platform Management Interface (IPMI) .

USB Connectors
Universal serial bus connectors

Infiniband Connectors

Power On Button

Controller LEDs (OK, Fault, and ID LEDs)

ID LED
Blue when the module is being identified.

Fault LED
Amber when there is a fault in the controller.

OK LED

Green when the controller is operating correctly.

Flashing green when there is a controller VPD error.

SAS Activity LED

Steady green when there is a connection but no activity.

Flashing green when there is a connection and activity.

OK, Fault, and ID LEDs

Reboot Button

Micro-SD Card Slot

Ethernet Connectors

POST LEDs

Rear view LEDs

This topic describes the LEDs located on the rear of the 3958 DD6 servers.

Figure 13 shows the LEDs on the rear of the server.

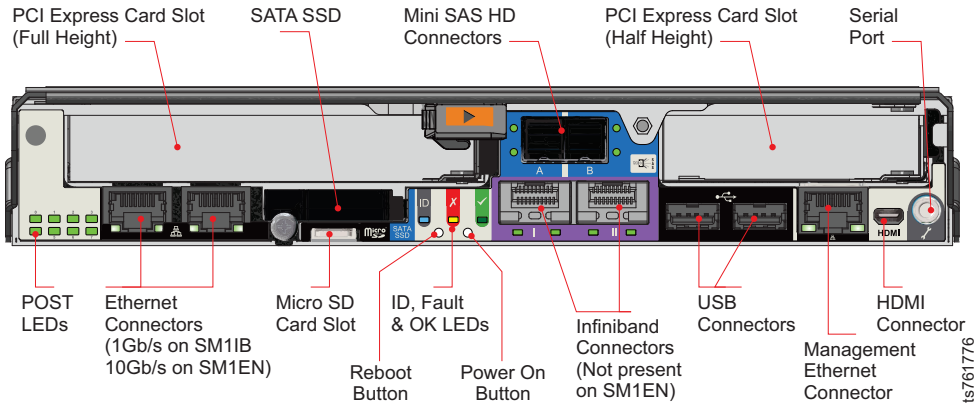


Figure 13. 1U Controller LEDs rear view

Table 3. Controller LEDs

LED	Description
ID LED	Blue when the module is being identified.
Fault LED	Amber when there is a fault in the controller.
OK LED	Green when the controller is operating correctly. Flashing green when there is a controller VPD error.
SAS Actvity LEDs	Steady green when there is a connection but no activity. Flashing green when there is a connection and activity.
Ethernet status LEDs (on either side of the Ethernet connectors	Left side: • Off when there is no connection. • Steady green when the network link is active. • Flashing green when there is network activity. Right side – network speed: • SM controller management port and E12EBD: – Off: 10/100Mb/s.\ – Green: 1Gb/s. • SM controller twin Ethernet ports: – - Off: No link. - Amber: 100Mb/s. - Green: 1Gb/s or 10Gb/s

Table 3. Controller LEDs (continued)

LED	Description
POST LEDs	Power On Self Test LEDs are used to show the boot progress of the x86 subsystem. If it fails to boot, the LEDs will show what stage of the process was being performed when the problem occurred. For more information on the POST LEDs, go to "Power-on self-test error log" on page 42.

Remote system management access

The system management Ethernet port of the 3958 DD6 server is used for system management information and control.

See Figure 12 on page 27 for the location of the system management Ethernet port.

Power cooling module LEDs

Six LEDs on the rear of the power cooling module (PCM) provide status information about the power supply, cooling fans, and the battery backup module.

When the amber LED on the rear panel of a server power supply is lit, it indicates an error condition within the power supply.

Note: If a power supply fails, it shows up in System Health Monitoring as a Power Supply 1 or 2 good fault. Replacing the power supply restores the power, but does not clear the problem for System Health Monitoring. To clear the error, refer to "Clearing system errors after power supply replacement" on page 31.

The top four LEDs give you status on the AC power, the PCM, and the PCM fan as described in Table 4 on page 31

The following figure shows the locations of the LEDs on the rear of the PCM.

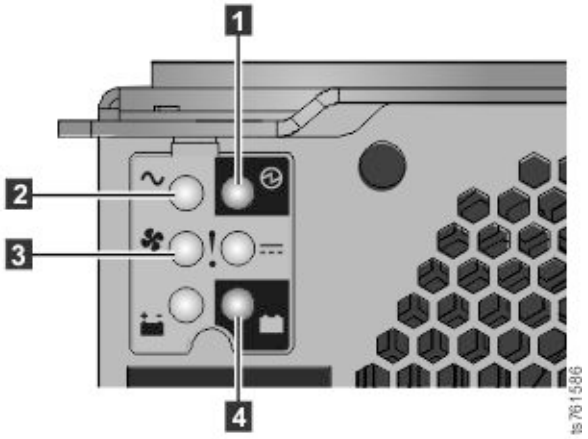


Figure 14. LEDs on the rear of the PCM

Table 4.

1 PCM OK (Green)	2 AC Fail (Amber)	3 Fan Fail (Amber)	DC Fail (Amber)	Status
OFF	OFF	OFF	OFF	No AC power source is being applied to any PCM
OFF	ON	OFF	ON	No AC power source is being applied to this PCM
ON	OFF	OFF	OFF	AC power source is present, the power supply is on and operating normally.
OFF	OFF	ON	OFF	PCM fan failed.
OFF	ON	ON	ON	PCM fault (over amperage, over voltage, or over current
FLASHING	OFF	OFF	OFF	Standby mode
OFF	FLASHING	FLASHING	FLASHING	PCM firmware in update state

The bottom two LEDs give status of the backup battery, as described in Table 5.

Table 5. Backup battery status

Battery Good on right (Green)	Battery Fault on left (Amber)	Status
OFF	OFF	Battery not present.
ON	OFF	Battery present and charged.
FLASHING	OFF	Battery charging or Maintenance Discharge.
OFF	FLASHING	Battery "soft" fault (recoverable)
OFF	ON	Battery "hard" fault (non-recoverable)
FLASHING	OFF	Battery disarmed.

Clearing system errors after power supply replacement

If a power supply fails, it shows up in system Health Monitoring as a Power Supply 1 or 2 good fault. Replacing the power supply restores the power, but does not clear the problem for system Health Monitoring. You must clear the error manually.

Procedure

To clear the system error, perform the following steps:

For ProtecTIER V3.1 or later:

1. To display a list of open problems, select **Health Monitoring** > **List open problems**.
2. Follow the on-screen instructions to enter the Problem Record number and cancel the power supply problem. Read the screen carefully to determine the correct choice of action in your responses.

Call Home through ECC

Electronic Customer Care (ECC) is an integrated service tool that uses the Call Home feature to provide automation of error reporting.

Electronic Customer Care is provided as a native tool of ProtecTIER software. For ECC communication to function properly, verify the following:

- Ports 80 and 443 and FTP port 21 are open for outbound traffic.
- Outgoing connections are allowed through the firewall; otherwise, unpredictable results will occur.
- The firewall is set to block and allow connections by both hostname and IP address to avoid unpredictable results.
- The ProtecTIER node can pass through any firewall to which the above IPs have access.

Refer to the IP address worksheet in Appendix B of the Installation Roadmap Guide for information regarding the default IP addresses for the Electronic Customer Care.

Table 2 on page 9 presents the capabilities of remote support with an ECC.

Table 6. Remote support capabilities through ECC

Customer site	Call Home events	• Error initiated • Heartbeat (regular interval) • Test
	Support capability	• Error-initiated problem reporting for up to 43 subsystems • Staged, error-specific data gathering • Subsystem and system console heartbeat reporting • Wellness checking • Log file storage (daily) • Code image and documentation repository (from media and RETAIN Fix Distribution Library)
	Remote support service tools	• Code image broadcast • Call home event log review • End-of-call completion report

Table 6. Remote support capabilities through ECC (continued)

IBM support	Remote access	• Authenticated, secure remote access • Simultaneous call in and call home • Data transmission (TCP/IP) supported
	IBM call home database	• 24/7 access by IBM support staff • Error analysis and search capability

Connect to BMC using a web-browser

This topic provides instructions for connecting to Baseboard Management Controller with a web-browser.

Procedure

1. Connect your computer to the ProtecTIER canister using the Ethernet cable from the ProtecTIER canister to the computer with the fixed IP setup (192.168.10.160).

   Note: The BMC port is the port on the far right of the ProtecTIER canister.
2. Start BMC in a Web Browser (Mozilla Firefox or Microsoft Internet Explorer) using the IP address configured in the BMC interface, in this case the default BMC IP address is 192.168.10.163 for the lower node and 192.168.10.164 for the upper node in case you have a clustered environment.

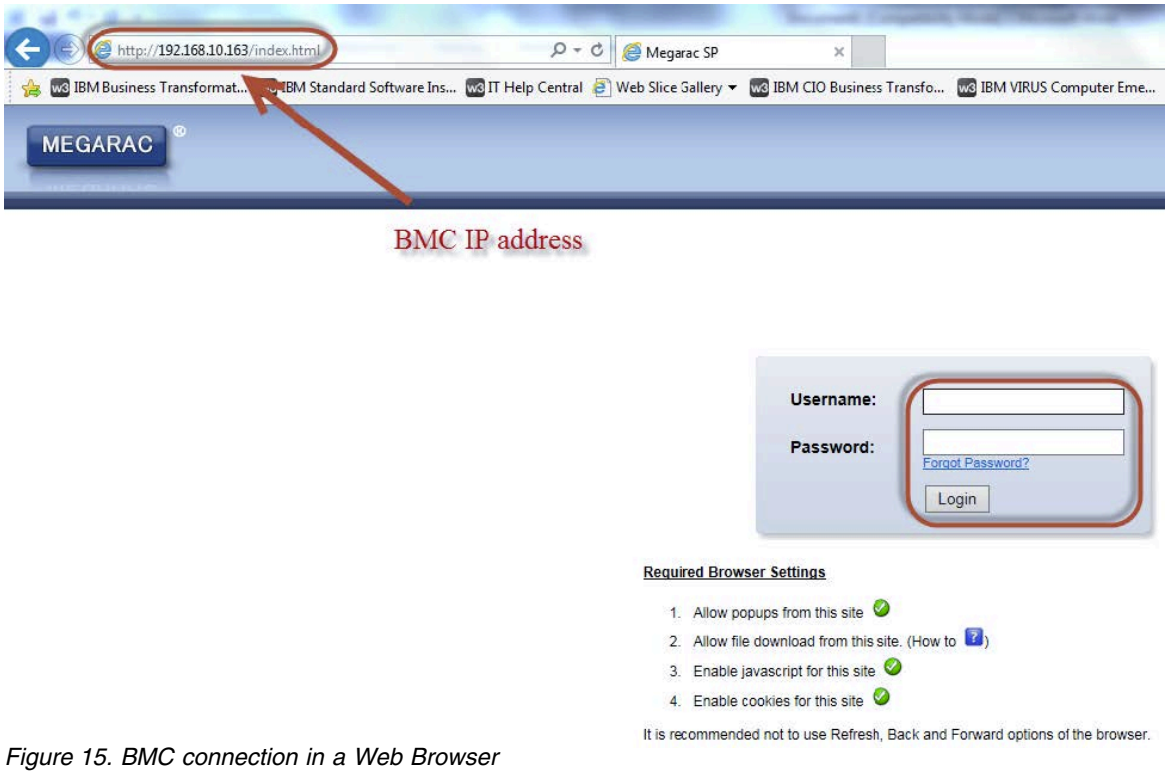


Figure 15. BMC connection in a Web Browser

3. Log in to the BMC interface. At the login prompt, log in with the ID `admin` and the password `admin`.
4. Select **Remote Control** > **Console Redirection**.

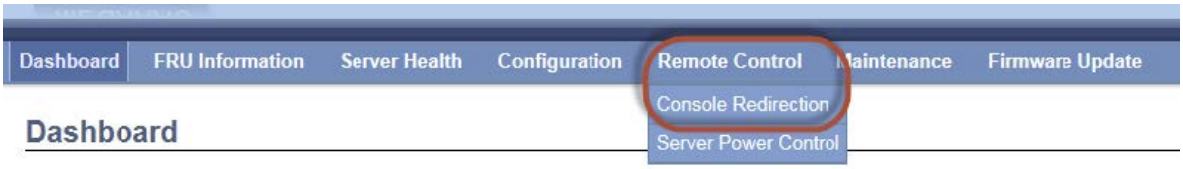


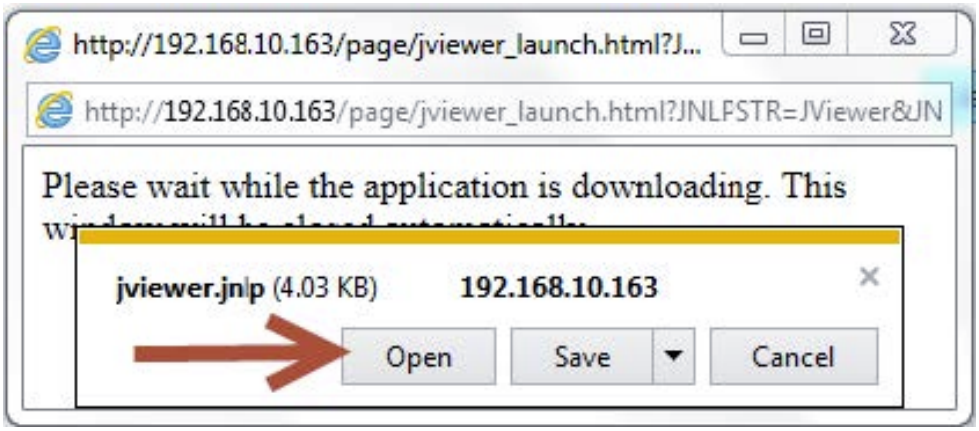
Figure 16. Console redirect menu

The Console Redirection Page is displayed.

5. Click **Java Console** to launch the redirection console.

Figure 17. Console Redirection page

6. Click **Open** in the dialog-box displayed.



7. If a security warning is displayed, click **Allow** to continue.

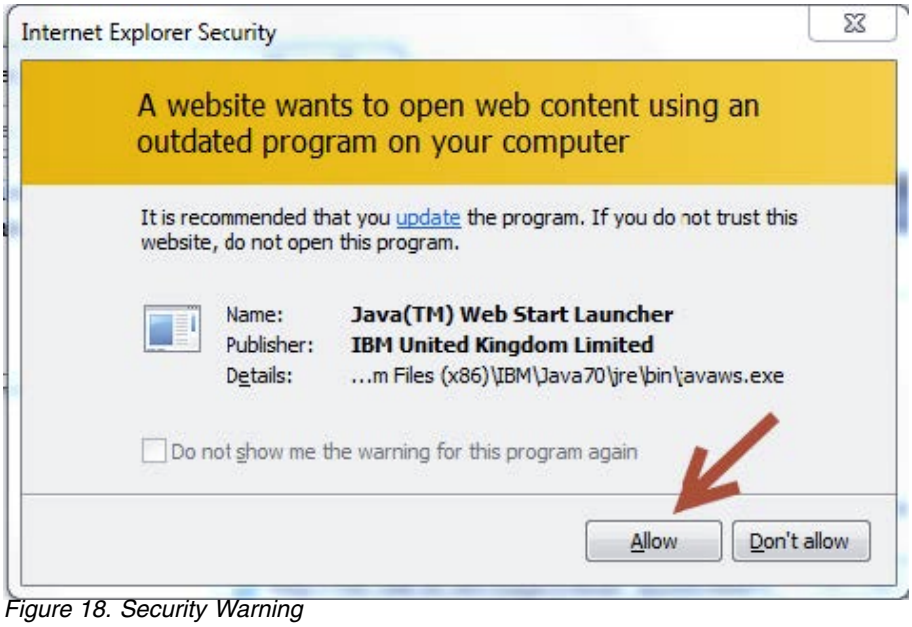


Figure 18. Security Warning

8. Another security warning will appear, click the checkbox to accept the security risk and then click **Execute** to continue.
9. You are connected to the system. If a blank screen is displayed, press **Enter** to refresh the view and obtain a video signal from the system.

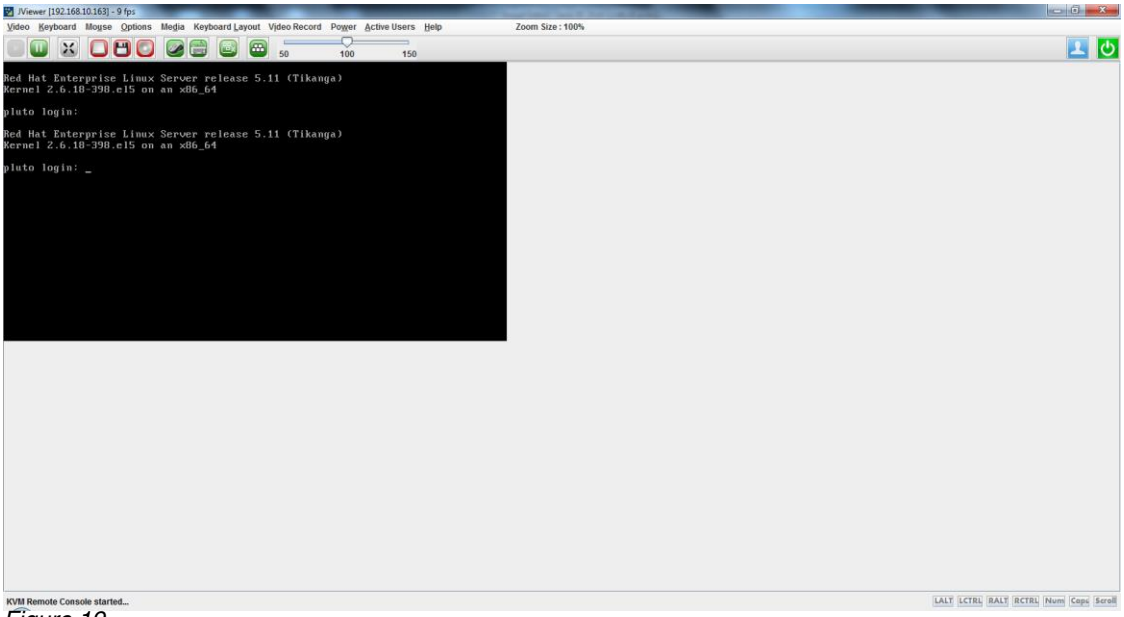


Figure 19.

10. Select Option in the pop-up message bar to allow pop-up windows in the browser.
11. Select **Allow pop-ups for 9.11.243.44**.

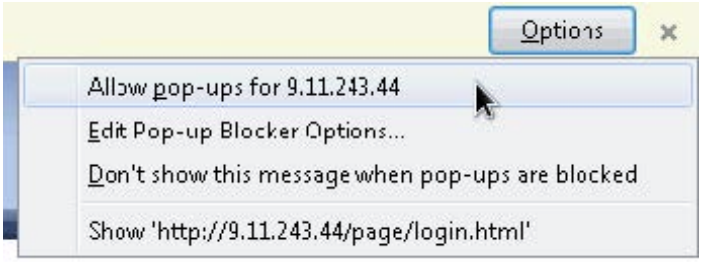


Figure 20. Firefox Options menu

Results

You are now connected to the BMC interface through your Web Browser.

Installing Red Hat Linux and ProtecTIER using BMC and CD/DVD media

To install Red Hat Linux and ProtecTIER using the baseboard management controller and CD/DVD media, you need to open a web-browser and connect to BMC using the default IP address previously defined.

Procedure

1. Connect to the BMC default IP address using a web-browser. This is the IP address configured in the BMC interface, in this case the default BMC IP address is 192.168.10.163 for the lower node and 192.168.10.164 for the upper node in case you have a clustered environment.
2. Launch the **Remote Control Console** and select **Virtual Media Wizard...**.

Figure 21. Remote control console window

3. Insert the **IBM System Storage ProtecTIER Maintenance and Recovery Disk** into the local DVD/CD-ROM drive.
4. On the Virtual Media window, check the Status pane and verify that all Target Drives are in a **Not Connected** state.
5. Select the drive associated with your DVD/CD-ROM. In this case select **D** to redirect the device.

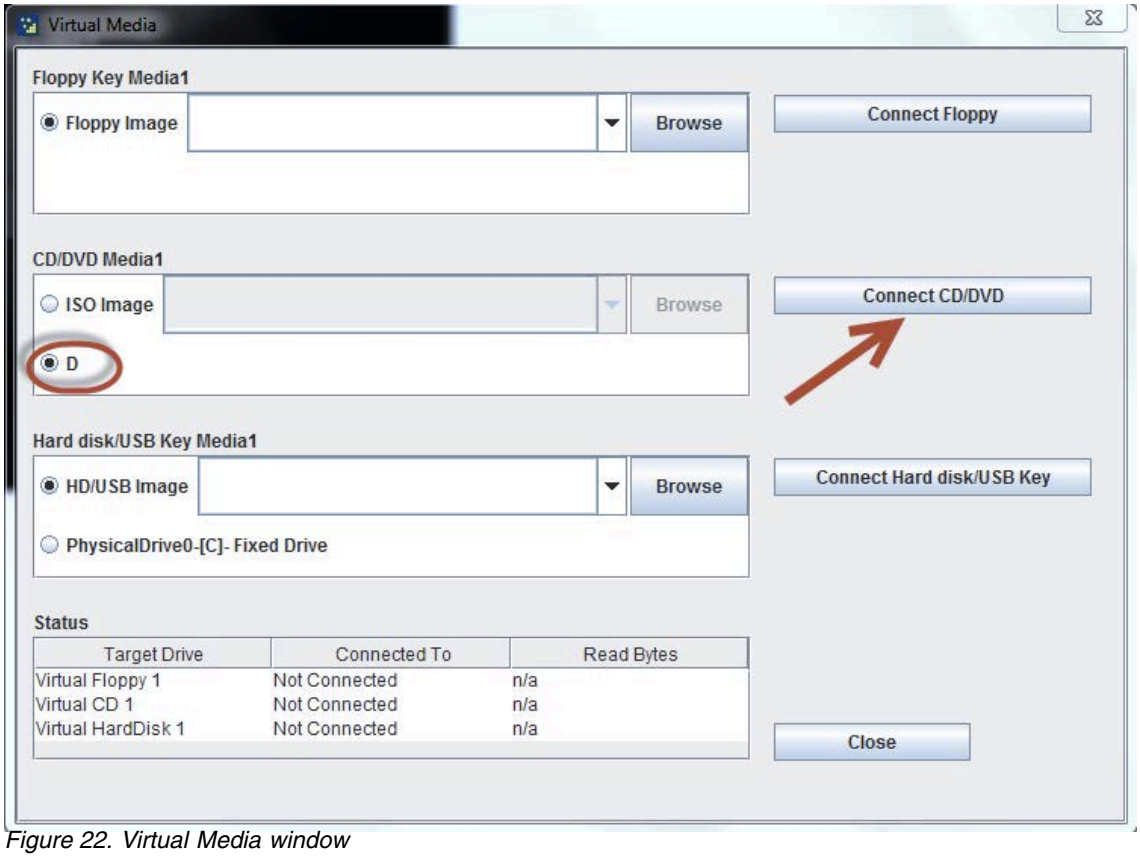
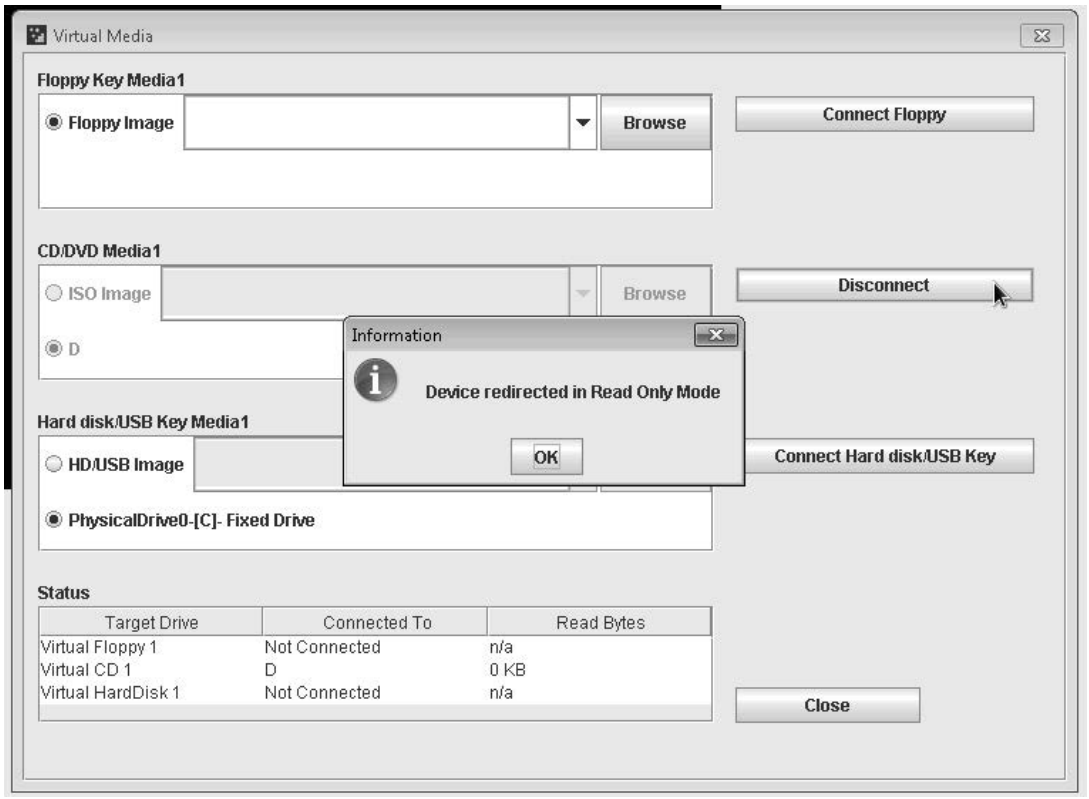
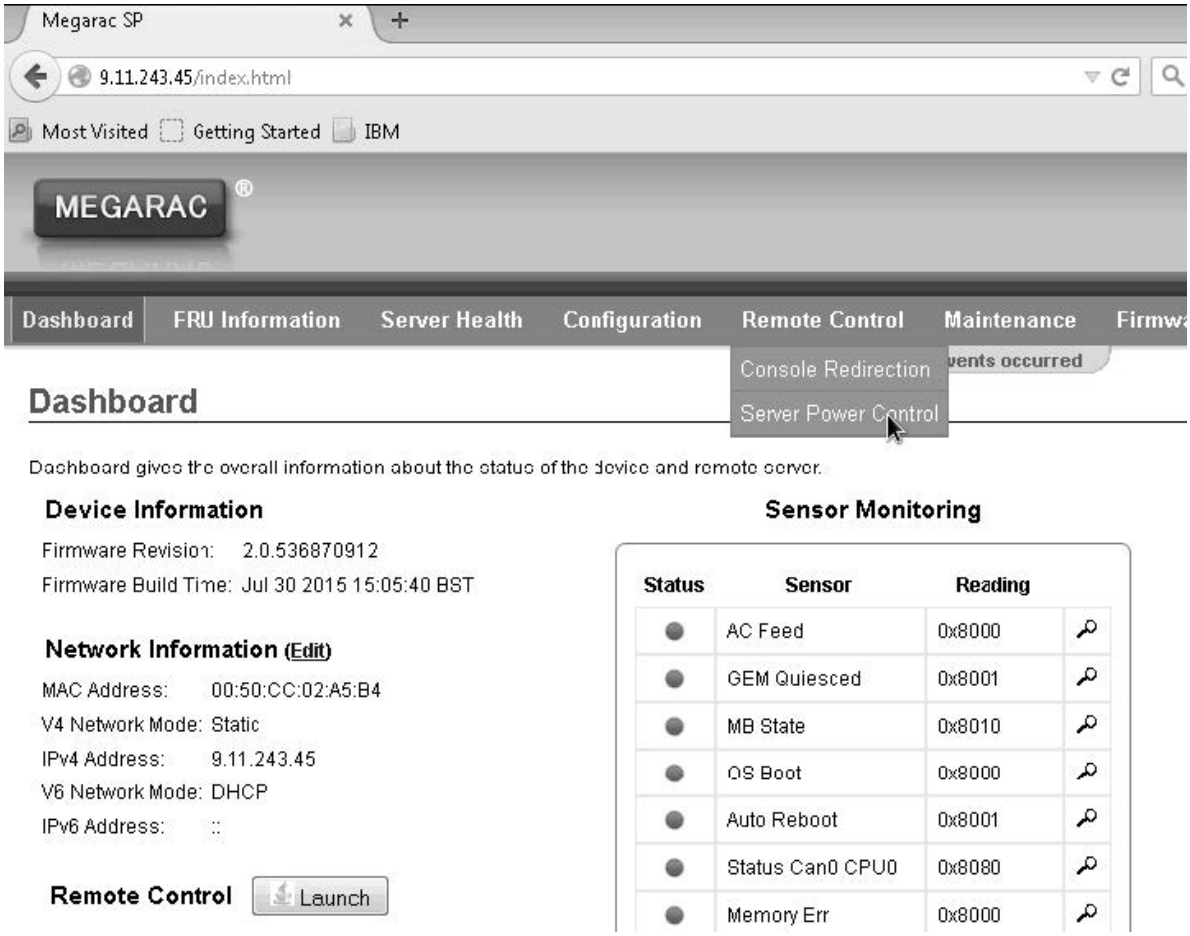


Figure 22. Virtual Media window

6. Select **Connect CD/DVD**. The device is redirected in Read Only Mode.



7. The device redirect dialog box is displayed. Select **OK**.
8. Select **Close** to exit the Virtual Media window.
9. Power cycle the canister by doing the following:
   a. Select the BMC web-browser window.



   b. Select **Remote Control** > **Server Power Control**.
   c. Select **Power Cycle the Server** and then select **Perform Action**. The canister is power cycled.
10. After a few minutes, the Red Hat Linux version 5.6 splash screens opens. Select the appropriate action to install, upgrade or restore.

    Important: Do not change the IP Address of the BMC interface when performing the initial setup of ProtecTIER during this procedure; otherwise, the connection is immediately lost and opens another connection to the new IP address assigned.

Results

You have completed the initial setup of BMC.

What to do next

The IP Address of BMC can be modified through the ProtecTIER CLI menu. Refer to the "Update or change the BMC IP address" topic for more information.

Update or change the BMC IP address

You can change or update the IP address for the Baseboard Management Controller (BMC) using the ProtecTIER Service Menu.

Before you begin

For the purposes of these procedures, it is assumed that the IP address configured for the BMC is 192.168.10.163 for the lower node and 192.168.10.164 for the upper node in case you have a clustered environment.

Note: To ensure communications between ProtecTIER and the BMC, configure the BMC over the same subnet as the ProtecTIER server, or make sure that network routing exists. If you do not establish communications between the BMC and ProtecTIER, functions such as BMC reports and health monitoring on the BMC do not work.

Procedure

1. Login to the local console. At the login prompt, log in with the ID `root` and the password `admin`.
2. Type: `menu` on the CLI, The main **ProtecTIER Service Menu** is displayed.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
--------------------------------------------------------------------------
   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
   9) ProtecTIER analysis (...)

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

3. From the main **ProtecTIER Service Menu**, select the **ProtecTIER Configuration (...)** option.
4. The **ProtecTIER Configuration Menu** is displayed, select the **IP Network Configuration (...)** option.

```
------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
  ProtecTIER Configuration (...)
------------------------------------------------------------------------
   1) Configure ProtecTIER node
   2) Recover Configuration for a replaced server
   3) Configure machine serial number for a replaced server
   4) Configure RAS
   5) Update Time, Date, Timezone & Timeserver(s)
   6) Scan storage interconnections
   7) File Systems Management (...)
   8) Configure replication (...)
   9) IP Network configuration (...)
   10) Update Firmware
   11) Update the System's name
   12) Validate configuration
   13) Single node - code upgrade (for Support Use Only)

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

5. The **IP Network Configuration Menu** is displayed, select the **Configure Baseboard Management Controller (BMC) IP**.

```
------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
  ProtecTIER Configuration (...)
  IP Network Configuration (...)
------------------------------------------------------------------------
   1) Configure hostname
   2) Configure ProtecTIER's IP interfaces
   3) Configure Static Routes
   4) Configure Baseboard Management Controller (BMC) IP


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

```
Begin Processing Procedure [Jan 14 17:20:30]
Gathering System information [ Done ]
Please provide the following information:

BMC IP Address [192.168.10.163]: x.x.x.x
BMC Netmask [255.255.255.0]: x.x.x.x
BMC Gateway [192.168.10.1]: x.x.x.x
Configuring BMC [ Done ]

End Processing Procedure Successfully [Jan 14 17:20:30]

Press <Enter> to continue
```

Identifying problems using status LEDs

You can identify server problems using the status light-emitting diodes (LEDs) on the front of the server.

The server is designed so that any LEDs that are lit remain lit when the server shuts down, as long as the server is connected to ac power, and is able to remain in standby mode (that is, dc power is provided to the system board).

If the module fault LED on the front control panel of the server is on, one or more LEDs inside the server or on the power supply are on. The server has LEDs to

help you identify problems with some server components. These LEDs are part of the light path diagnostic feature built into the server. By following the light path, you can quickly identify the type of system error that occurred. See Light path diagnostics.See Power supply LEDs for troubleshooting with the power supply LEDs and power-on LED.

Diagnostics

The topics in this section provide basic troubleshooting information to help you resolve some common problems that might occur with the server.

General checkout procedure

Complete this task in order to checkout the subcomponents of the ProtecTIER server hardware.

About this task

The following diagnostic tools are available to you for diagnosis and solving of hardware-related problems:

Power-On Self-Test (POST)
When connected to a console via the RS232 serial interface, the system will output information when the system boots. See “Power-on self-test error log” on page 42 for more information.

Enclosure component inventory
You might want to write code to discover enclosure components and, where appropriate, their firmware revision levels. Once logged into the x86 subsystem (see section 6.3 on page 76), the commands in Table 8–1 can be used to create this component inventory. See “Using Dynamic System Analysis” on page 12 for more information.

BMC logs
The SEL is a circular non-volatile log maintained by the BMC. The SEL, which only logs sensors owned by the x86 subsystem, is a very useful first pass diagnostic aid.

Complete the following steps to perform the checkout procedure to identify system problems:

1. Check the power supply LEDs (see “Power cooling module LEDs” on page 30).
2. Turn off the server and all external devices.
   a. Undo any recent system changes, such as new settings or newly installed devices.
   b. Remove all hardware that is not listed on the ServerProven website.
3. Check all cables and power cords.
4. Turn on all external devices.
5. Restart the server. If the server does not start, see “Troubleshooting tables” in the *IBM System x3850 X5 and x3950 X5 Types 7145, 7146, 7143, and 7191 Problem Determination and Service Guide*.
6. Record any POST error code and message that is displayed on the screen. If an error is displayed, look it up in the“Power-on self-test error log” on page 42.

Diagnostic tools overview

This topic describes the tools that are used to diagnose the ProtecTIER server.

The following tools are available to help you diagnose and solve hardware-related problems:

Power-on self test (POST) error codes, error messages, and error logs
The POST generates error codes and messages to indicate detection of a problem.

Diagnostic programs and error messages
The diagnostic programs are stored in memory on the system board. These programs are the primary method of testing the major components of the server.

Log and configuration capture
Each controller has a logging sub-system and records various pieces of information to a set of RAM-based and flash-based logs. You can view the contents of the main log using the ipmitool sel list or ipmitool sel elist commands (with the -v argument giving extra information).

- Generic enclosure management (GEM) logs. GEM is the firmware that actively manages the SM controller and enclosure electronics.
- Baseboard Management Controller (BMC). The BMC chip is a system management controller that runs the GEM code and provides access to the system using IPMI, and maintains the following non-volatile logs:

  SEL (System Event Log)

  Battery log

  GEM log

Power-on self-test error log

Power On Self Test LEDs are used to show the boot progress of the x86 subsystem. If it fails to boot, the LEDs will show what stage of the process was being performed when the problem occurred.

The POST LEDs are on the back of the controller. Each LED has a bit value as shown in the following table. Use the LED values to determine the HEX code.

Table 7. POST LED Bit Values

LED Number	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Value	1	2	4	8	16	32	64	128

Add the values of the LEDs that are on to obtain the number and then convert that number to hex. For example, if LEDs 0, 2, 3, 4, 5 and 6 are lit, this equates to: 1 + 4 + 8 + 16 + 32 + 64 = 125 or 0x7D in hex. Refer to the following tables to determine the meaning of the hex code.

For a list of POST codes, go to Appendix A, “Power-On Self-Test (POST) codes,” on page 91.

Viewing the captured operating system error logs on the 3958 DD6

Each controller records various pieces of information to a set of RAM-based and flash-based logs. You can use the ipmitool view the contents of the main log.

About this task

The host application collects log entries and configuration data that can be used to determine the cause when a problem occurs. If you need to contact IBM support services, providing this data can be crucial for fault tracking.

Regardless of the initial symptoms, you should collect all these logs for all node failures. Sometimes you have to perform a deep analysis to discover the source of an issue.

Important: For the most accurate snapshot of the system state at the time of the failure, collect these logs, if possible, before you recover the node or before performing any automatic fail-over operations.

Linux operating system

Procedure

1. Log in to the x86 operating system.
2. Use the following command to change to the log directory:
   ```
   cd /var/log
   ```
3. Type this command to list all the log messages:
   ```
   ls -la messages*
   ```
4. Scan the timestamps to select the logging period of interest.

Windows operating system

Procedure

1. Log in to the x86 operating system.
2. Launch the Event Viewer application by clicking **Control Panel** > **Administrative Tools** > **Event Viewer**.
3. Choose a desired log type (for example, “System”).
4. Depending on your version of Windows, use either the **Export List** or **Save Events as** option to save the logs.

Chapter 4. CD and DVD overview

The topics in this section provide information about the documentation and software CDs and DVDs of the TS7650G Gateway ProtecTIER software. The Red Hat Linux and ProtecTIER code are loaded by manufacturing.

Documentation CD

The *IBM TS7650 with ProtecTIER Publications* CD contains documentation for the TS7650G Gateway.

See “Hardware ship group CDs” on page 1 for more information.

Recovery disk

There are multiple levels of Recovery Disks.

Make sure the Recovery Disk matches the level of ProtecTIER software you are recovering.

Software CDs

This topic addresses the CDs included in the software ship group.

For an overview of the CDs included in the software ship group, refer to “Software ship group DVDs” on page 2.

Chapter 5. Parts catalog

The topics in this section provide information about the field-replaceable units unique to each ProtecTIER server.

Field-replaceable units unique to the 3958 DD6 servers

This topic lists the field-replaceable units (FRUs) that are unique to the 3958 DD6 servers.

Table 8. 3958 DD6 server FRUs

IBM part number	FC	FRU Description
00VJ249		128GB boot drive
00VJ250	DD6 Base, AGK6	600GB 15k 12Gb SAS HDD
00VJ251	DD6 base	1220W power supply unit
00WT000	00WT000	Full Height Quad Port 8Gbps FC
00VJ256		XP controller blanking plate
00VJ257	DD6	ES-DUM drive carrier dummy
00VJ258	AGK4	Quad Ethernet Adapter
00VJ259		Half Height Quad Port 8Gb/s FC adapter
00VJ260	AGK7	Dual Ethernet Converged Network Adapter
00VJ261	AGK7	Ethernet SFP+ SR Optics
00VJ266		XP-3224 OneStor - XP 2U 24-bay 12Gb/s chassis module with midplane and Ops Panel
00VJ267		Universal Rail Kit
17R7231		3958 DD6 controller server V2
00VJ598	DD6 base, AGK6	1U controller with 10 Gb/s ethernet
2726256	DD6	Enet Cat6 cable
00VJ353	DD6	Power Control Module
00VJ365	DD6	Fan Control Module

Chapter 6. FRU replacement for TS7650G systems

The TS7650G Gateway uses standard field-replaceable units (FRUs) and some unique FRUs. To replace a FRU, refer to the removal and replacement instructions in the service guide section of this manual. Some FRUs are hot-swap capable and can be hot-swapped if the service guide instructs you to do so (for example, power supplies). For FRUs that are not hot-swap capable (for example, Fibre Channel adapters), you might have to turn off the component.

To remove or replace FRUs in the ProtecTIER server, refer to "Removing and replacing FRUs in 3958 DD6 servers."

The *IBM RAS/BIOS and Firmware Update* DVD contains the following:

- Files for updating firmware after a FRU has been replaced
- Files for enabling Call Home
- A script to configure the server E2 port for connection to the system console network
- FRU BIOS and firmware levels

Note: Adapters in the TS7650 (including the hot-swap adapter ports) are not hot-swap capable due to the limitations of the Linux operating system. The system must be shut down when replacing an adapter.
After replacing a Fibre Channel HBA or Ethernet adapter, additional steps might be required in order to complete the replacement. The Fibre Channel HBA might require ports set to target or initiator mode. To set the IP address on the Ethernet adapter, see the *IBM ProtecTIER User's Guide for VTL Systems*, GA32-0922.

Removing and replacing FRUs in 3958 DD6 servers

The following topics provide instructions for removing and replacing field-replaceable units (FRUs) in 3958 DD6 servers.

Preparing the system for FRU replacement

Complete the task in this topic to prepare the ProtecTIER Model 3958 DD6 server for replacement of a field-replaceable unit (FRU).

Before you begin

Procedure

1. Have the customer stop all activities from attached hosts and quiesce all jobs.
2. Access the server:
   a. Attach a keyboard and monitor to the server and access the **ProtecTIER Service Menu**. Log on with the user ID `ptconfig` and the password `ptconfig` to access the **ProtecTIER Service Menu**.

```
------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
------------------------------------------------------------------------
   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
   9) ProtecTIER analysis (...)

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

b. In the **Service Menu**, select **Manage ProtecTIER Services (...)** [Option 2].

Note: Alternatively, you can type the following command:

```
ssh ptadmin@xxx.xxx.xxx.xxx
```

where *xxx.xxx.xxx.xxx* is the server IP address.

3. In the **Manage ProtecTIER Services** menu, select **Power off This Node** to power off the server.

```
------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
            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? 6
```

Removing the controller from the chassis

Complete this task to remove the controller from 3958 DD6 server.

Procedure

Perform the following steps to remove the controller from the chassis of the 3958 DD6:

1. Prepare the system for FRU replacement (see "Preparing the system for FRU replacement" on page 49).
2. Verify that the server is powered off by checking that the power LED is flashing on the operator information panel.
3. Disconnect all cables attached to the controller, including the front end and back end cables.
4. To release the controller handle, push the latch on the center of the controller to the right. (see Figure 23 on page 51).

Figure 23. Releasing the controller handle

5. Use the handle to pull the controller out slowly. (see Figure 24 and Figure 25).

Figure 24. Grasp the controller handle

Figure 25. Slide the controller from the chassis

Replacing the controller in the chassis

Complete this task to replace the controller with a new one on the 3958 DD6 server.

Before you begin

Before you can replace the old controller with a new one, you need to remove the following FRUs from the old controller and install them in the new controller:

- The two PCI host bus adapter (HBA) cards. See "Removing and replacing the front host bus adapter (HBA) from the canister" on page 65 and "Removing and replacing the back host bus adapter (HBA) from the canister" on page 64.
- The SSD. See "Removing and replacing the SSD" on page 70.

Procedure

Perform the following steps to replace the controller with a new one on the 3958 DD6:

1. Remove the cover from the new controller as explained in “Removing the top cover from the controller” on page 56.
2. Install the SSD that you removed from the old controller as decribed in “Removing and replacing the SSD” on page 70.
3. Install the HBA that supports the rear connectors as described in “Removing and replacing the back host bus adapter (HBA) from the canister” on page 64
4. Install the HBA that supports the front connectors as described in “Removing and replacing the front host bus adapter (HBA) from the canister” on page 65
5. Replace the cover on the controller as described in “Replacing the controller cover” on page 57.
6. Align the front of the controller with the opening in the chassis and push the controller into the chassis.
7. Lift the handle and push the controller in until the handle latches into place. (see Figure 26).
   The controller should power on automatically in a few minutes.

Figure 26. Use the handle to push the controller into place

8. If the controller does not power on after a few minutes, insert a small screw driver or Allen wrench into the power on button on the right beneath the OK, Fault, and ID LEDs on the back of the controller.

Figure 27. Pressing the Power On button if the controller does not power on automatically

9. In the ProtecTIER Service Menu, select ProtecTIER Configuration (...) [Option 1].

```
--------------------------------------------------------------------------------
ProtecTIER Service Menu
--------------------------------------------------------------------------------
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? 1
```

10. In the ProtecTIER Configuration (...)option, select Configure machine serial number for a replaced server [Option 3].

```
--------------------------------------------------------------------------------
ProtecTIER Service Menu
ProtecTIER Configuration (...)
--------------------------------------------------------------------------------
1) Configure ProtecTIER node
2) Recover Configuration for a replaced server
3) Configure machine serial number for a replaced server
4) Configure RAS
5) Update Time, Date, Timezone and Timeserver(s)
6) Scan storage interconnections
7) File Systems Management (...)
8) Configure replication (...)
9) IP Network configuration (...)
10) Update Firmware
11) Update the System's name
12) Validate configuration
13) Single Node
-
code upgrade (For Support Use ONLY)
B) Back
E) Exit
--------------------------------------------------------------------------------
>>>Your choice? 3
```

11. Wait until the process indicates that the "Configure machine serial number for a replaced server" was replaced successfully.
12. Verify the operation and availability of the replaced node.
13. Return to the old controller that you removed and follow the instructs in Figure 26 on page 52

Removing and disposing of the battery from the controller

After you remove the HBAs and the SSD HD from the controller, complete the following steps to remove the battery for disposal.

Procedure

1. Remove the screws holding the top cover in place near the rear of the canister. Figure 28 on page 54).

Figure 28. Remove the screws holding cover in place

2. Locate the battery near the rear end of the canister. See Figure 29 and Figure 30 on page 55

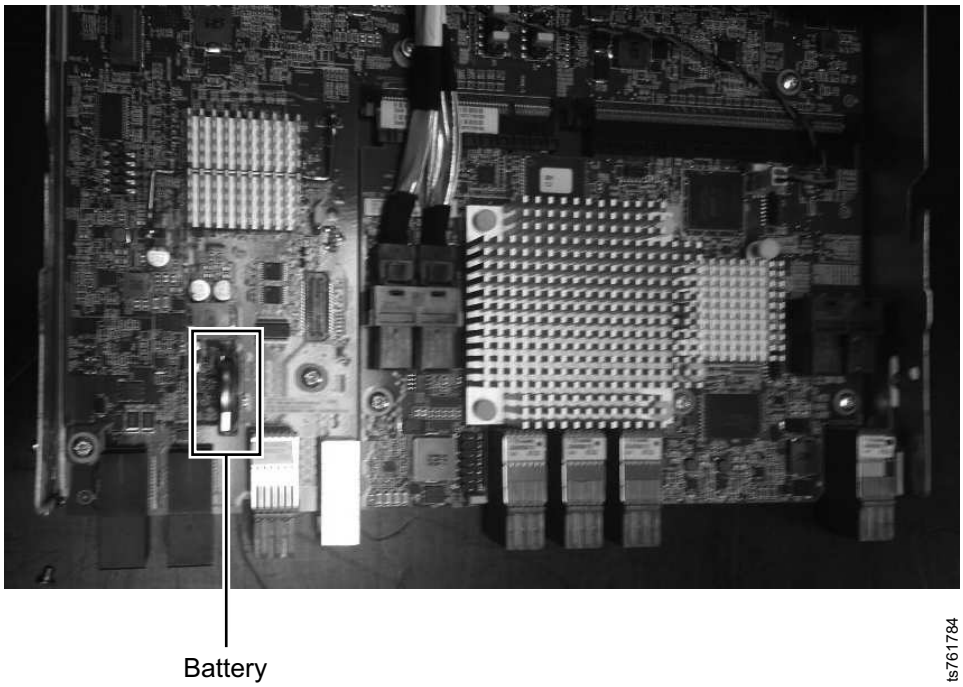


Figure 29. Locate the battery

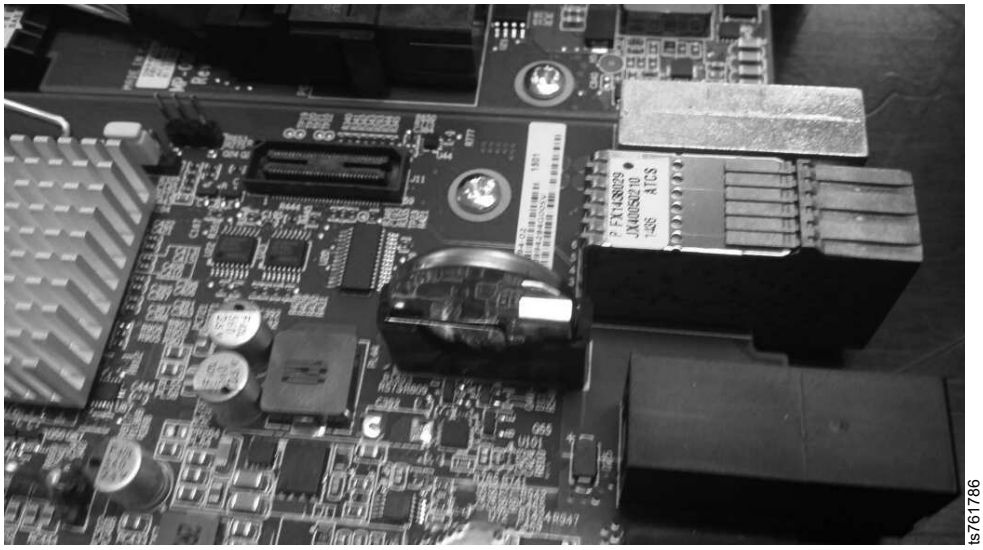


Figure 30. Closeup view of the side of the battery.

3. Remove the system battery.
   a. If there is a rubber cover on the battery holder, use your fingers to remove the cover.
   b. Use one finger to gently tilt the battery horizontally, pushing it away from the socket.
   c. Use your thumb and forefinger to lift the battery from the socket.

      Note: To avoid damaging the battery socket, do not use excessive force to remove the battery.
      Figure 31

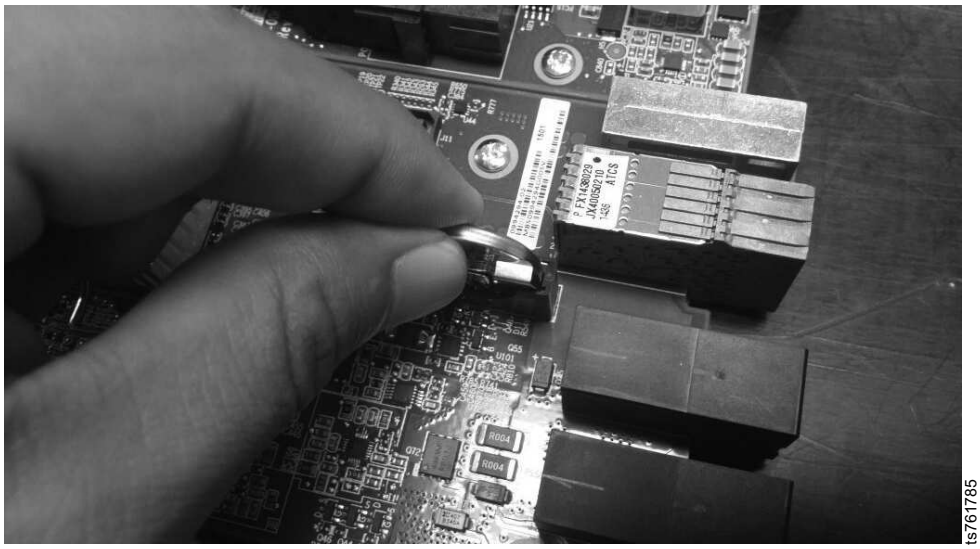


Figure 31. Lift to remove battery.

4. Dispose of the battery as required by local ordinances or regulations. See the *IBM Environmental notices and User's Guide* on the IBM Documentation CD for more information.

Removing the top cover from the controller

Complete this task to remove the top cover from the controller on the 3958 DD6 server.

Procedure

Perform the following steps to remove the top cover from the controller of the3958 DD6:

1. Prepare the system for FRU replacement (see "Preparing the system for FRU replacement" on page 49).
2. Verify that the server is powered off by checking that the power LED is flashing on the operator information panel. Then, disconnect the power cords and all external cables as necessary to replace the device.
3. Remove the controller from the chassis as described in "Removing the controller from the chassis" on page 50).
4. To gain access to internal FRUs, you must completely remove the controller's top cover.
5. Locate the two blue clips towards the back of the top cover. See Figure 32

Figure 32. Locate the two blue clips

6. To loosen the cover, push the two blue clips towards the front of the controller as shown in Figure 33 on page 57

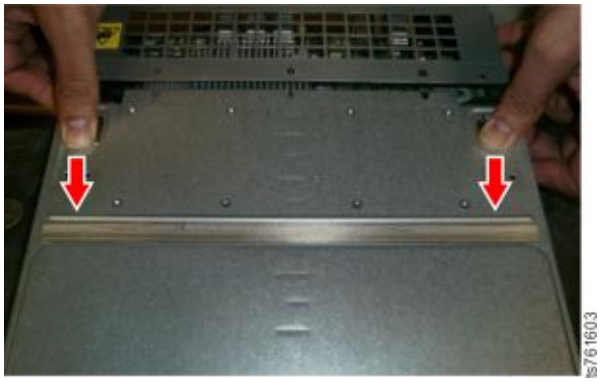


Figure 33. Move the blue clips towards the front

7. Remove the cover by moving it slightly forward and lifting it up to reveal the internal components. See Figure 34

Figure 34. Lifting the cover from the controller

Replacing the controller cover

Complete this task to replace the cover on the controller in the 3958 DD6 server.

Procedure

Perform the following steps to replace the cover on the controller of the 3958 DD6:

1. Align the rear of the cover with the lip near the back of the controller.
2. Lay the cover flat on top of the controller and slide it towards the rear and under the lip.
3. Once the cover is in place, slide the blue clips towards the rear to lock the cover.

Removing and replace the power supply

Complete this task to remove and replace the 3958 DD6 server power supply.

About this task

The 3958 DD6 is equipped with two power supply modules located on either side of the canister. Because there are two power supplies, you do not need to power off the system to replace a power supply.

Procedure

Perform the following steps to remove and replace a power supply 3958 DD6:

1. Locate the faulty power supply.
2. Turn off the Power supply interrupter/switch.
3. Disconnect the power cable of the PCM that you are removing.

   Attention: The fans in the PCM continue to run and supply cool air.
4. Push the latch on the side of the power supply down to release the handle. See Figure 35

Figure 35. Pushing the latch to release the handle

5. Use the handle to pull the power supply out slowly. See Figure 36

   Note: To maintain proper cooling and airflow, do not leave the slot empty; re-install the replacement soon.

Figure 36. Power supply removal handle

6. To replace the power supply, locate the power supply slot and push the power supply module back into the slot. See Figure 37 on page 59. Close the handle until it latches into place.

Figure 37. Replacing the power supply

Removing and replacing the power cooling module from the power supply

Complete this task to remove and replace the power cooling module from the 3958 DD6 server power supply.

About this task

Each of the two power supplies in the 3958 DD6 is protected by a power cooling module (PCM). Use this procedure to remove a faulty PCM.

Procedure

1. Remove the power supply as described in "Removing and replace the power supply" on page 58.
2. Near the rear of the power supply, locate the two Phillips head screws that secure the cover to the power supply, and remove them.

Figure 38. One of the two screws that hold the PCM cover in place

3. Locate the small blue clip on the top of the cover near the rear of the power supply. Press down on the blue clip and push towards the front of the power supply to release the cover. See Figure 39 on page 60

Figure 39. Blue latch on top of the power supply

4. Then pull the cover slightly forward and upwards to remove it.
5. Carefully disconnect both wiring harnesses. See Figure 40.

Figure 40. Disconnect the two wiring harnesses

6. Use a Phillips head screwdriver to remove the eight screws that secure the PCM in the power supply. See Figure 41.

Figure 41. Remove the eight screws that secure the PCM into the power supply (six screws are shown here; the other two are near the rear where the cables attach)

7. Remove the PCM and replace it with the new one. See Figure 42

Figure 42. Power cooling module (PCM)

8. Replace the eight screws that secure the PCM in the power supply.
9. Plug in the two wiring harnesses on the rear of the PCM.
10. Line up the rear of the power supply cover with the slot on the rear of the power supply. Lay the cover on top of the power supply and push the cover towards the rear until the blue latch clicks into place.
11. Replace the two screws that secure the cover on the power supply.
12. Replace the power supply in the slot on the server.

Removing and replacing the power supply fan

Complete this task to remove and replace the power supply fan on the 3958 DD6.

About this task

Each of the two power supplies in the 3958 DD6 is protected by a fan in addition to the power cooling module (PCM). Use this procedure to remove and replace a faulty fan.

Procedure

1. To prepare the power supply for fan replacement, follow 1 on page 59 to 5 on page 60. Then return here to complete the remaining steps.
2. Use a Phillips head screwdriver to remove the five screws on the top cover and two on the sides of the top cover that secure the cover. See Figure 43 and Figure 44.

Figure 43. Remove the five screws on the top cover

Figure 44. Remove the two screws on either side of the top cover

3. Move the cover slightly forward and then up to remove it. See Figure 45

Figure 45. Remove the cover

4. Remove the screws at the bottom and on the side that secure the fan in the power supply. See Figure 46

Figure 46. Remove the screws that secure the fan in the power supply

5. Carefully remove the fan from the power supply. See Figure 47 on page 64

Figure 47. Remove the fan from the power supply

6. Insert the replacement fan in the proper slot, taking care to align the notch in the side edge of the fan. Press down gently. See Figure 48

Figure 48. Insert the replacement fan

7. Replace the screws on the side and the bottom of the power supply to secure the fan.
8. Plug in the two wiring harnesses on the rear of the PCM.
9. Line up the rear of the power supply cover with the slot on the rear of the power supply. Push the cover into place taking care to align the screw holes on the sides of the cover.
10. Replace the seven screws that secure the cover on the power supply.
11. Replace the power supply in the slot on the server.

Removing and replacing the back host bus adapter (HBA) from the canister

Complete this task to remove and replace the host bus adapter (HBA) PCI card that controls the attachments on the rear of the 3958 DD6.

About this task

There are two PCI host bus adapters (HBAs) in the canister. The smaller one controls the attachments on the rear end of the 3958 DD6. The larger of the two controls the attachments on the front of the 3958 DD6. Follow these instructions to remove and replace the rear HBA.

Procedure

1. Prepare the system for FRU replacement (see “Preparing the system for FRU replacement” on page 49).
2. Verify that the server is powered off by checking that the power LED is flashing on the operator information panel. Then, disconnect the power cords and all external cables as necessary to replace the device.
3. Remove the canister from the chassis as described in “Removing the controller from the chassis” on page 50).
4. Remove the cover of the canister as described in “Removing the top cover from the controller” on page 56
5. Locate the HBA for the back attachments. It is the one on the left in the following photo.

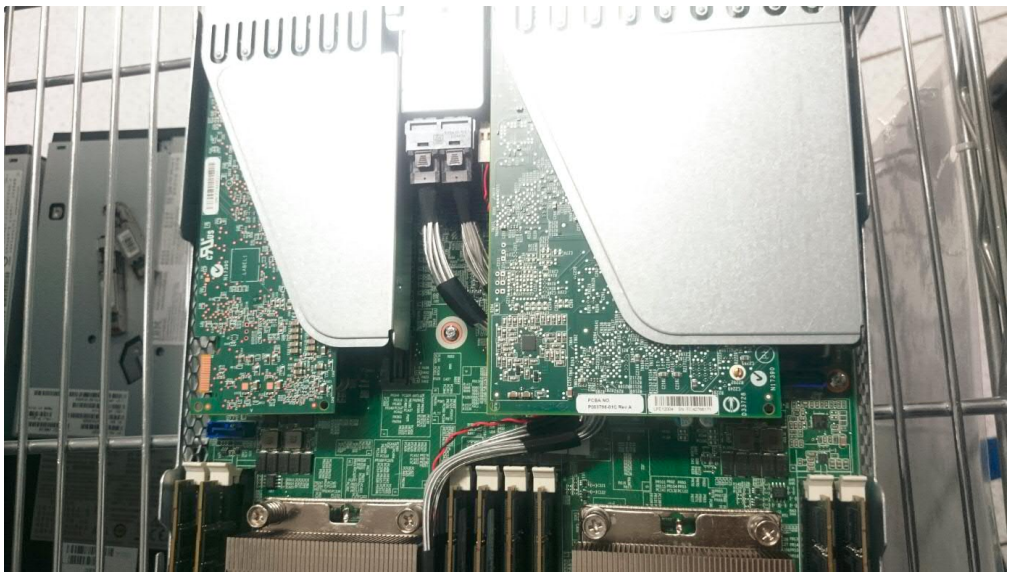


Figure 49. The back PCI assemblies is shown on the left

6. Carefully grasp the front end of the PCI adapter card and lift it up and out of the slot on the riser card.
7. Remove the new PCI adapter card from its anti-static packaging.
8. Carefully grasp the upper corners of new PCI adapter card and position the bottom corners of the card in the PCI riser card attached to the mother board. The adapter card is keyed to fit in only one direction, so take care to align the notch in the lower edge of the adapter card with the cross-piece in the bottom slot of the riser card.
9. Carefully, press down firmly until the new adapter is seated in the slot of the riser card.
10. Replace the cover of the canister as described in “Replacing the controller cover” on page 57
11. Replace the canister from the chassis as described in “Replacing the controller in the chassis” on page 51).

Removing and replacing the front host bus adapter (HBA) from the canister

Complete this task to remove and replace the host bus adapter (HBA) PCI card that controls the attachments on the front of the 3958 DD6.

About this task

There are two PCI host bus adapters (HBAs) in the canister. The one on the right controls the attachments on the front end of the 3958 DD6. Follow these instructions to remove and replace the front HBA.

Procedure

1. Prepare the system for FRU replacement (see “Preparing the system for FRU replacement” on page 49).
2. Verify that the server is powered off by checking that the power LED is flashing on the operator information panel. Then, disconnect the power cords and all external cables as necessary to replace the device.
3. Remove the canister from the chassis as described in “Removing the controller from the chassis” on page 50).
4. Remove the cover of the canister as described in “Removing the top cover from the controller” on page 56
5. Locate the HBA for the front attachments. It is the one on the right in the following figure.

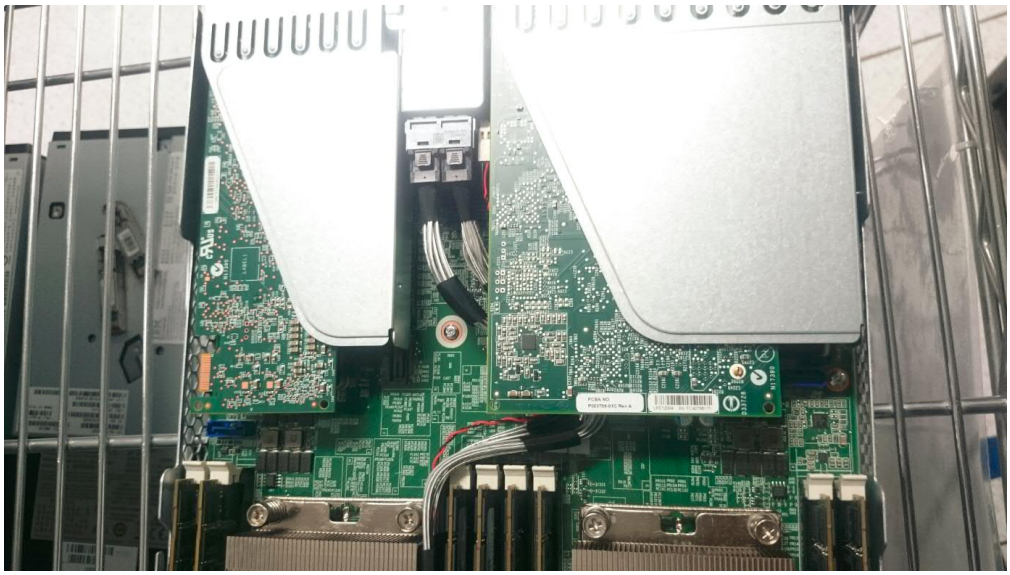


Figure 50. The front PCI assemblies is shown on the right

6. Carefully grasp the front end of the PCI adapter card and lift it up and out of the slot on the riser card.
7. Remove the new PCI adapter card from its anti-static packaging.
8. Carefully grasp the upper corners of new PCI adapter card and position the bottom corners of the card in the PCI riser card attached to the mother board. The adapter card is keyed to fit in only one direction, so take care to align the notch in the lower edge of the adapter card with the cross-piece in the bottom slot of the riser card.
9. Carefully, press down firmly until the new adapter is seated in the slot of the riser card.
10. Replace the cover of the canister as described in “Replacing the controller cover” on page 57
11. Replace the canister from the chassis as described in “Replacing the controller in the chassis” on page 51).

Removing and replacing a SAS drive from the chassis

Complete this task to remove and replace a SAS drive from the front of the 3958 DD6.

About this task

The 3958 DD6 can have 24 serial-attached SCSI (SAS) drives. Only slot 1 and slot 24 actually contain SAS drives. Follow these instructions to remove and replace a SAS drive.

Procedure

1. Keep the power turned on.
2. Locate the SAS drive you need to replace.

   CAUTION:
   Wear an electrostatic discharge (ESD) wrist strap when removing and replacing the SAS drives from the chassis.
3. Unlock the SAS drive by using a Torx T10 screwdriver to turn the locking screw clockwise. See Figure 51

Figure 51. Unlocking the SAS drive

4. Using the handle to pull the SAS drive out slowly as shown in Figure 52 on page 68 and Figure 53 on page 68

Figure 52. Removing the SAS drive

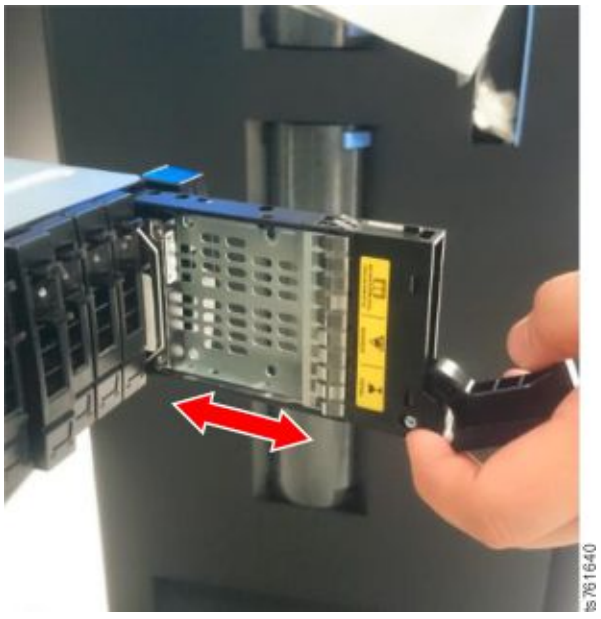


Figure 53. SAS drive case extended from chassis

5. Use a Torx T10 screwdriver to unscrew the four screws on the top and bottom of the drive case and slide the drive out from the rear of the case.

Figure 54. Unscrew drive from case

6. Remove the new SAS drive from its packaging.
7. Carefully grasp the new SAS drive module by the edges and position it in the case.
8. Use a Torx T10 screwdriver to tighten the four screws that secure the SAS drive in the case.
9. Slide the drive and case into the slot on the front of the 3958 DD6 until it seats itself. Then push the handle in place.
10. Use a Torx T10 screwdriver to turn the locking screw counter-clockwise to lock the drive in place.
11.

    Note:
    If the replacement is taking place in a ProtecTIER running V3.4.0 or V3.4.1, perform the procedure described in Appendix D, “SAS replacement on a ProtecTIER server running version V3.4.0 or V3.4.1,” on page 111

12. On the ProtecTIER Service Menu, select **ProtecTIER Configuration (...)** (Option 1).

```
------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
------------------------------------------------------------------------
   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
   9) ProtecTIER Analysis (...)
  10) USB Installation (...)

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

13. On the ProtecTIER Configuration (...) menu, select **Replace SAS Drive** (Option 15)

```
------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
  ProtecTIER Configuration (...)
------------------------------------------------------------------------
   1) Configure ProtecTIER node
   2) Recover Configuration for a replaced server
   3) Configure machine serial number for a replaced server
   4) Configure RAS
   5) Update Time, Date, Timezone & Timeserver(s)
   6) Scan storage interconnections
   7) File Systems Management (...)
   8) Configure replication (...)
   9) IP Network configuration (...)
  10) Update Firmware
  11) Update Firmware (...)
  12) Update the System's name
  13) Validate configuration
  14) Single node - code upgrade (for Support Use Only)
  15) OS images Management (...)

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

14. Wait until the process indicates that the SAS drive was replaced successfully.

Removing and replacing the SSD

Complete this task to remove and replace the solid state drive (SSD) located in the rear of the control unit of the 3958 DD6.

About this task

The 3958 DD6 has two solid state drives (SSDs), one located internally and the other accessible from the rear of the control unit.

Procedure

1. Before you begin, power off the system as described in "Preparing the system for FRU replacement" on page 49.
2. Locate the SSD in the rear of the control unit.

3. Use a Phillips head screwdriver to loosen the screw that holds the SSD in place.

4. Press the handle to release the SSD module and pull the SSD out slowly.
5. If the replacement SSD comes mounted in a plastic base, skip to step 7. If the replacement SSD is not mounted in a plastic base, continue with the next step.
6. If the replacement SSD does not come with a plastic base, follow these substeps to remove the old SSD from the plastic base, and to mount the new SSD on the plastic base.
   a. Use a Phillips head screwdriver to remove the screw that secures the SSD on the plastic base.

Figure 55. SSD on plastic base

   b. Remove the new SSD drive from its packaging.
   c. Carefully grasp the new SSD by the edges and position it on the plastic base.
   d. Tighten the screw that holds the SSD on the plastic base.
7. Position the new SSD in the slot from which you removed the old one, making sure to align the notch.
8. Tighten the screw that holds the SSD in the control unit. Then push the handle in place.
9. If the menu option “to restore (only DD6)” is present, use the Red Hat installation disc to recover the system.
10. Reinstall Red Hat and select the option **To restore (only DD6)** from the user screen to restore the system to the new SSD.

Removing and replacing a drive carrier blank

Complete this task to remove and replace a drive carrier blank from the front of the 3958 DD6.

Procedure

1. Keep the power turned on.
2. Locate the drive carrier blank you need to replace.
3. Using the handle to pull the drive carrier blank out as shown in Figure 56 on page 72.

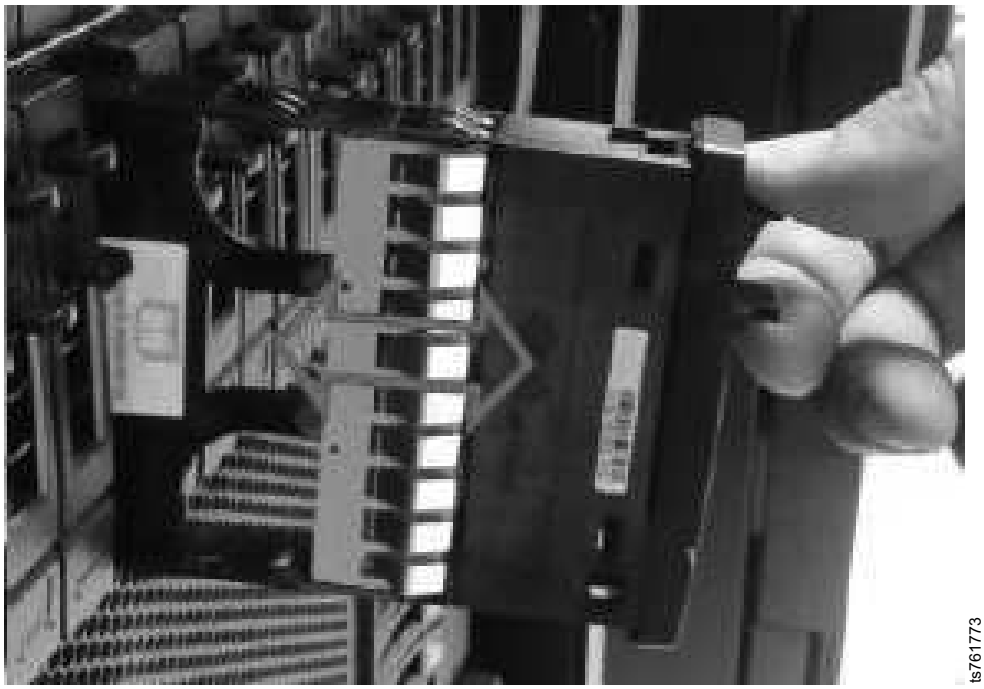


Figure 56. Removing the drive carrier blank

4. Remove the new drive carrier blank from its packaging.
5. Push the new drive carrier blank into the slot from which you removed the old one.

Removing and replacing SFP modules

Complete this task to remove and replace an SPF module from the rear of the controller in the 3958 DD6.

About this task

The controller can have up to four Fibre Channel Small form-factor pluggable (SFP+) host interface connections. These optical transceivers are removable and are located in the four SFP cages on the rear of the controller.

Procedure

1. Keep the power turned on.
2. Locate the SFP module you need to replace and remove the cable attached to it.
3. Use the handle to pull the SFP module out as shown in Figure 57 on page 73

Figure 57. Removing an SFP module

4. Remove the new SFP module from its packaging.
5. Carefully push the new SFP module into the slot from which you removed the old one.
6. Close the handle and reattach the cables.

Removing the components from the chassis enclosure

When the midplane interconnect is failing, you need to replace the enclosure chassis with a new one.

About this task

To replace the chassis you must first remove all the components in the chassis enclosure. Follow the procedures described below.

Procedure

1. Before you begin, power off the system as described in "Preparing the system for FRU replacement" on page 49.
2. Disconnect each cable that you have connected to the canister or canisters.
3. Remove any controller canisters as described in "Removing the controller from the chassis" on page 50.
4. Remove the two power supply units on both sides of the enclosure as described in "Removing and replace the power supply" on page 58.
5. Remove SAS drives 1 (far left) and 24 (far right) from the front of the enclosure as described in Removing and replacing the SAS HD connector from the canister
6. Remove the new enclosure from its packaging.
7. Replace the two power supply units in the new enclosure as described in 6 on page 58.
8. Replace the controller canister or canisters removed in 3.

9. Replace the SAS drives removed in 5 on page 73.
10. Reinstall the cables and power cords.
11. Turn the power back on.

Removing and replacing the Cat6a Ethernet cable

On a DD6 clustered enclosure the E1 ports on both nodes are connected together with a Cat6a Ethernet cable.

About this task

When in a cluster the Cat6a Ethernet cable is failing and leaving either Node A or Node B in fence mode, it is necessary to remove the Cat6a Ethernet cable and replace it with a new one.

Procedure

1. Before you being, bring down services in the Node B, to do so, follow the procedure mentioned in “Chapter 2. TS7650 [DD6] – Power off Sequence”.
2. Wait a few minutes while the Node B is powered off. When the Node B is powered off, go to the Node A and repeat the same procedure described in the step 1 to bring down services in Node A.
3. After stopping the services on Node A, remove the old Cat6a Ethernet cable and replace it with the new Cat6a Ethernet cable.Figure 58

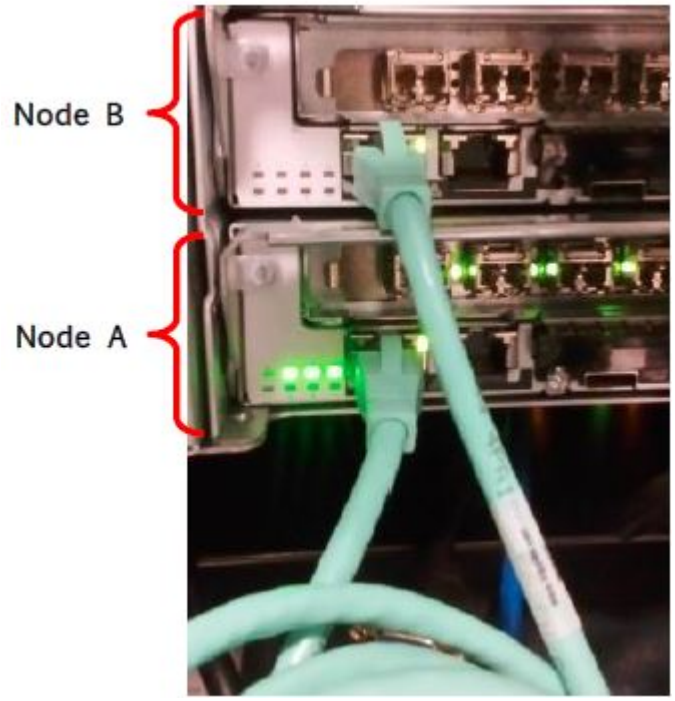


Figure 58. Removing and replacing a Cat6a Ethernet cable

4. Use the following commands to bring up services on Node A:

```
service cman start
service clvmd
service gfs start
chkconfig ptcluster
chkconfig vtfd on
service vtfd init
```

5. From the ProtecTIER Service menu (...) option, select Manage ProtecTIER services (...) [Option 2]

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
--------------------------------------------------------------------------
   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
   9) ProtecTIER Analysis (...)
  10) USB Installation (...)

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

Figure 59. ProtecTIER Service menu

6. From the Manager ProtecTIER services (...) menu, select Display services status [Option 1]

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
--------------------------------------------------------------------------
   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
   9) ProtecTIER Analysis (...)
  10) USB Installation (...)

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

Figure 60. ProtecTIER Service menu

7. When the Display services status window appears, make sure that all service status is UP.

```
Begin Processing Procedure [Nov 6 19:24:10]
Service Status
==============================
cman UP
clvmd UP
gfs UP
vtfd UP
ptrasd UP
tl UP
End Processing Procedure Successfully [Nov 6 19:24:10]
Press <Enter> to continue
```

8. To bring up Node B follow steps 3 - 6 on Node B.

Updating the firmware of an Emulex adapter

This procedure is performed after the replacement of an Emulex adapter to ensure that the firmware levels remain consistent across all the adapters.

Procedure

1. Connect a USB keyboard and monitor to the 3958 server to switch to the node you are working on.
2. Power on the node.
3. Wait until the node has completed power-on. To update the firmware, go to the ProtecTIER Service menu (see "ProtecTIER Service menu" on page 11) and, select **ProtecTIER Configuration** > **Update Firmware**.

Results

The firmware update procedure for the Emulex adapter is complete.

What to do next

- If a customer uses a fibre switch to connect the TS7650 to the storage, warn the customer that replacing an Emulex adapter creates a different WWNN from the one that is currently used. If the customer is zoning the switch, they must rezone it with the new Emulex WWNN. If the customer is zoning the switch, they must rezone it with the new Emulex WWNN..
- If the customer has configured LUN Mapping on the backend disk system the LUN Mapping must be reconfigured to the new WWNN.
- If your system uses ProtecTIER V2.5 or later, the frontend WWNN for the new Emulex adapter is automatically reset to its original value by the firmware update and reboot in step 2.

Updating the server microprocessor board (system planar) firmware and BIOS settings

After the replacement of the microprocessor board (system planar), the BIOS level must be checked and updated to the tested level.

Procedure

1. Connect a USB keyboard and monitor to the server or use the TSSC keyboard and monitor to access the command line of the node.

   Note: On 3958 DD4 and 3958 DD5 servers, in a small number of cases, it is necessary to update the firmware through the IMM web interface. See Logging in to the 3958 DD4 and DD5 servers through the IMM web interface.
2. Insert the appropriate software DVD.

ProtecTIER software version	DVD
2.3	*IBM System Storage RAS/BIOS and Firmware Update DVD* (if not already inserted)
2.4	ProtecTIER 2.4 DVD (if not already inserted)
2.5 or later	No DVD needed

3. At the login prompt, log in as ID `ptadmin` and password `ptadmin`.
4. Display the current firmware versions.

- For ProtecTIER software V3.1 or later, from the ProtecTIER Service menu, select **Version Information** > **Display Firmware Levels** (see "ProtecTIER Service menu" on page 11).
- For ProtecTIER software V2.4 or V2.5, from the ProtecTIER Service menu, select **Display Firmware Versions**.
- For ProtecTIER software V2.3 or earlier, from a command line type **versions**. If the command is not found, type the following commands to mount the *IBM RAS/BIOS and Firmware Update* DVD and display the firmware versions:

```
mount /dev/hda /mnt/cdrom
cd /mnt/cdrom
./versions
```

The output is similar to that shown in Example output of versions check. Make a note of the displayed levels.

5. Compare the displayed levels to the levels listed in this document.
   - If the firmware levels are up to date, **STOP**. Skip the rest of this procedure.
   - If the firmware is not at the current level, perform the following steps to update the firmware to current supported field levels.
6. From the command line, type the appropriate commands to mount the software DVD (if any) and update the sysplanar.

ProtecTIER software version	Commands

V2.3 and earlier	`mount /dev/hda /mnt/cdrom`
	`cd /mnt/cdrom`
	`./update_sysplanar`

V2.4 and later	`/opt/dtc/install/ptconfig -updateFirmwares`

7. Type the appropriate commands to update the Sysplanar Broadcom Ethernet firmware.

ProtecTIER software version	Commands

V2.3 and earlier	`mount /dev/hda /mnt/cdrom`
	`cd /mnt/cdrom`
	`./installBRCM`

V2.4 and later	`/opt/dtc/install/ptconfig -updateFirmwares`

Results

The process of updating the server system planar firmware and BIOS settings is complete.

What to do next

- The Broadcom firmware update script updates only active ports with unique IP addresses. Sysplanar Port 1 (eth4) is used for the replication feature. Replication configuration is required before the firmware for Port 1 is updated. Sysplanar Port 2 (eth5) is used for connection to the TSSC. Installation of the RAS package is also required before firmware for Port 2 is updated. 3958 DD4 and 3958 DD5 servers in VTL configuration have eth4 and eth5 onboard. Port eth5 is already active as a replication port, but eth4 must be temporarily reconfigured as an another active replication port for correct firmware update. After the firmware update, port eth4 can be restored to its previous configuration.
- After firmware updates have been completed on 3958 DD4 and 3958 DD5 servers, you must rebuild the RAS package.

- For ProtecTIER V2.5 or earlier, type the following command: **/opt/dtc/install/ptconfig -configRAS**
- For ProtecTIER V3.1 or later, select **ProtecTIER Configuration** > **Configure RAS** from the ProtecTIER Service menu (see "ProtecTIER Service menu" on page 11).

After the rebuild is complete, continue with Chapter 8, "End-of-call procedure," on page 89.

- If you are performing any other FRU or firmware updates, proceed to the appropriate section.

Initializing a used hard disk drive for reuse

Re-initialized hard disk drives (HDDs) *cannot* be used for hot-swapping. They can be used as a replacement field-replaceable unit (FRU) as shown in the following procedure.

About this task

Attention: This procedure initializes both of the HDDs in the server and requires a reload of the Red Hat Linux operating system and ProtecTIER code.

Note: Only a fresh field-replaceable unit HDD can be used for hot-swapping. However, if a used HDD, with the same FRU part number, from another 3958 DD4 or 3958 DD5 with a ServeRAID M5015 controller, and to be reinstalled in a 3958 DD4/3958 DD5 server. Plug the used HDD as a replacement FRU into the appropriate HDD slot when the server is powered down.

Procedure

To initialize the HDD, perform the following steps.

1. On the powered-down server, plug the used HDD into the SCSI ID 0 slot or SCSI ID1 slot.
2. When the system starts up, after the System x logo is displayed, press **Ctrl-H**.
3. Click the **Start** button.
4. Click **Configuration Wizard** on the WebBIOS main screen. The Configuration Wizard screen is displayed.
5. Select the **New Configuration** option, which clears the existing configuration on the drives and lets you create a new configuration.
6. Click **Next**. The WebBIOS Configuration Method screen is displayed.
7. Select **Automatic Configuration** to create RAID 1 for the disk pair. Leave **Redundancy when possible** selected in the menu.
8. Click **Next** to continue. WebBIOS carries out the automatic configuration to create a virtual drive, based on two available drives. The Virtual Drive group and RAID 1 configuration are displayed.
9. Click **Fast Initialize** > **Go**. The HDD is initialized.
10. When the process completes, exit WebBIOS for a fresh load of Red Hat Linux and ProtecTIER code.

Replacing a Dual-Port or Quad-Port Ethernet card and recovering Ethernet settings

None of the 3958 adapter cards are hot-swap capable because the server operating system does not permit the adapters to be varied offline prior to removal. The Ethernet replacement tool is an interactive tool that is designed to recover the Ethernet settings after replacing an Ethernet card.

Before you begin

Attention: (ProtecTIER V2.3 and earlier only) When using the Ethernet Replacement Tool procedure, you must load the latest RAS package (verson 3.1.x or higher) prior to running the tool from the menu selection. Refer to the RAS package update information in the *IBM System Storage TS7600 with ProtecTIER Installation Instructions for the RAS Package, BIOS, and Firmware updates following a FRU replacement for models 3958 DD1, 3958 DD3, and 3958 AP1*, PN 46X2459 and then return to this procedure.

Procedure

Perform the following steps to replace a Dual-Port or Quad-Port Ethernet card and recover Ethernet settings.

1. Prepare the system for FRU replacement (see Preparing the system for FRU replacement).
2. Replace the Ethernet adapter (see Replacing the field-replaceable unit). After replacing the FRU, continue with step 3.
3. Replug the disconnected Ethernet cables and power on the server.
4. Log in with user ID **ptadmin** and password **ptadmin**.
5. Run the Ethernet card replacement tool on the server by using one of the following methods.
   - ProtecTIER V2.5 or later: The Ethernet card replacement tool is activated automatically on bootup of the server. (This activation includes the automatic update of the quad-port Ethernet replacement card on the 3958 DD4 or 3958 DD5 server.) To check that all is repaired as expected, from the ProtecTIER Service menu (see "ProtecTIER Service menu" on page 11), select the options to run a full check on the node.
     – For ProtecTIER V2.5 or earlier, select **System Health Monitoring** > **Run a full check on this node**.
     – For ProtecTIER V3.1 or later, select **Health Monitoring** > **Run a full check on this node**.

     If no degraded check points are indicated, then the Ethernet settings of the replaced adapter have been successfully recovered.

     After the health check has been successfully completed, **STOP**. Skip the remaining steps of this procedure and continue with Chapter 8, "End-of-call procedure," on page 89.
   - ProtecTIER V2.4 or earlier, at the command line, type: **rsCerCfgUpdateEthConnections**.

     - OR -
   - ProtecTIER 2.4 or earlier, select **Manage Configuration** > **Update Eth Connections**.
6. To verify, ping other parties on the network.

Example

The following example shows activation of this tool for the dual-port Ethernet card on a system running ProtecTIER V2.4 or earlier.

1. Type the command **rsCerCfgUpdateEthConnections**.

   ```
   # /opt/ras/bin/rsCerCfgUpdateEthConnections
   ```

2. The Ethernet replace tool identifies the replaced card:

   ```
   The following replacement(s) were discovered for 2 port Ethernet card on slot 3
   eth1
   Old MAC address = 00:15:17:1e:2d:71
   New MAC address= 00:15:17:7f:28:8d
   eth0
   Old MAC address = 00:15:17:1e:2d:70
   New MAC address= 00:15:17:7f:28:8c
   IP: 9.148.41.82
   Do you wish to correct the ethernet configuration? YES/NO
   ```

   If you wish to correct the Ethernet configuration, type yes.

   ```
   Do you wish to correct the ethernet configuration? YES/NO
   yes
   port to configure:0
   Please disconnect ethernet cables from the replaced card,
   press Enter to continue or type exit
   ```

3. Disconnect all Ethernet cables from the replaced card, and press Enter.

   ```
   Verifying cables are disconnected... may take a few minutes

   Configuring eth0
   Please connect ethernet cable to eth0
   press Enter to continue or type exit
   ```

4. Connect a single cable to the requested port (Eth0 in our case) and press Enter.

   ```
   Checking for connected cable... may take a few minutes

   About to configure eth0
   IP=9.148.41.82
   Please confirm YES/NO
   ```

   Note: In some instances, you are requested to connect the other cable as well. In such a case you do not have to follow steps 6 through 8 on page 81.

   ```
   This action would also update eth1
   If you wish to connect a cable to eth1
   Please connect it before typing YES
   Please confirm YES/NO
   ```

5. If you agree with the settings, type yes.

   ```
   Please confirm YES/NO
   Yes

   Successfully configured eth0
   ```

6. In the following steps, the configuration for the port on the replaced card is continued.

```
port to configure:1

Configuring eth1
Please connect ethernet cable to eth1
press Enter to continue or type exit
```

7. If you wish to configure the port, connect the Ethernet cable to the port and press Enter.

```
Checking for connected cable... may take a few minutes

About to configure eth1

Please confirm YES/NO
```

8. If you accept the settings, type yes.

```
Successfully configured eth1
Please remember to connect all disconnected cables!
```

   The Ethernet settings are recovered.

9. To verify, ping other parties on the network.
10. The Intel Network DHCP-boot can be disabled by booting from one of the DVDs listed below (depending on the installed version of ProtecTIER) and disabling the Intel Network DHCP-boot.
    a. Insert one of the following in the CD/DVD drive:
       - *IBM RAS/BIOS and Firmware Update* DVD
       - TS7650 ProtecTIER 2.4.x server DVD
       - TS7650G ProtecTIER 2.4.x server DVD
    b. Restart the server. The TS7600 BIOS and Firmware tool menu is displayed.

```
        IBM TS7600 BIOS and Firmware tool

        Select from the following options:

          [1] Update the Qlogic Firmware

          [2] Update the Emulex Firmware

          [3] Run Intel Boot Agent Utility

          [4] Run all updates

          [X] Exit to command prompt

          [0] Reboot
```

    c. Select **Run Intel Boot Agent Utility**.
    d. When the Intel Boot Agent Utility menu is displayed, select **Disable DHCP-Boot on all Intel NIC adapters**.
    e. Select the option to **Reboot**.

What to do next

If the Ethernet adapter replacement procedure is complete, and no further firmware is being updated, go to Chapter 8, “End-of-call procedure,” on page 89.

If additional updates are being performed, continue to the relevant section of this document.

Recovering a node

Reinstalling the Red Hat Linux operating system overlays all the Reliability, Availability, and Serviceability (RAS), basic input/output system (BIOS), and firmware scripts and utility rpms. As a result, an IBM Service Representative must reload the RAS package after the customer reloads Red Hat Linux.

Attention: TS7600 products require a TSSC. The TSSC is a vital part of the service strategy. For the RAS package to gather logs at the time of the failure and send a call home packet, a TSSC is required. If the RAS package is not installed, the customer must call 1(800) IBM SERV (7378) (in North America, only) or visit the IBM Directory of worldwide contacts web page to obtain hardware support. ProtecTIER must also be reinstalled following reinstallation of Red Hat Linux. This is typically a customer responsibility. Refer to the system recovery information in the *IBM ProtecTIER User's Guide for VTL Systems*, GA32-0922, provided on the *IBM TS7650 with ProtecTIER Publications* CD.

The following items are required when recovering a node in a clustered installation:

1. Installation of the appropriate version of Red Hat Linux on the new server. See the system recovery information in the *IBM ProtecTIER User's Guide for VTL Systems*, GA32-0922 for more information.
2. Extraction and reload of the ProtecTIER package. See the "Unpacking the ProtecTIER package" section of the *IBM ProtecTIER User's Guide for VTL Systems*, GA32-0922 for more information.
3. Reinstallation of the RAS package on the new server. Reinstallation of the RAS package is required. A reload of the Red Hat Linux operating system erases all components of the RAS package. To reinstall the RAS package, see "Reinstalling the RAS package (ProtecTIER software V2.3 or earlier only)" on page 83.

Automatic node recovery

All of the procedures for automatic node recovery are documented in the "Recovery Procedures" appendix of the *IBM ProtecTIER User's Guide for VTL Systems*, GA32-0922.

The recovery initiates the automatic node replacement procedure. This includes missing node identification and performing the following tasks:

- Configures network settings
- Configures hostname
- Configures bond
- Configures V5.11 cluster
- Restarts all cluster activities on the other node in the cluster if in a clustered installation
- Discovers and registers the repository file systems in the `/etc/fstab` directory
- Configures multipath

Reinstalling the RAS package (ProtecTIER software V2.3 or earlier only)

This topic provides the steps for reinstalling the RAS package on a system running ProtecTIER software V2.3 or earlier.

About this task

For more detailed information about installing the RAS package on a system running ProtecTIER software V2.3 or earlier, see the *IBM System Storage TS7600 with ProtecTIER Installation Instructions for the RAS Package, BIOS, and Firmware updates following a FRU replacement for models 3958 DD1, 3958 DD3, and 3958 AP1*, PN 46X2459.

- To perform the RAS package installation, you must first establish a server connection.
- If you are installing the RAS package in a clustered configuration, perform the installation on Server A (the bottom server) first.
- If this is the second node installation in a clustered configuration, make sure the first node is up and running before proceeding.

Procedure

1. Insert the *IBM RAS/BIOS and Firmware Update* DVD into the DVD drive on the 3958 server on which you are installing this package.
2. If not already logged in, log into the 3958 server with the user ID `ptadmin` and password `ptadmin`.
3. From the command line, enter in the following commands to mount the *IBM RAS/BIOS and Firmware Update* DVD and launch the installation application:

   ```
   mkdir /mnt/cdrom
   ```

   Note: If the `/mnt/cdrom` directory already exists, the following message is displayed:

   ```
   mkdir: cannot create directory '/mnt/cdrom': File exists
   ```

   If this message is displayed, ignore it and proceed to the next step.

   ```
   mount /dev/hda /mnt/cdrom
   cd /mnt/cdrom
   ./rsCerCfgInstall
   ```

   Follow the instructions on the screen to complete the installation.

   Important: Use the same frame number for both nodes when clustered together in the same frame.
4. The 3958 DD1 first release (August 2008) supported RSA Ethernet connections on the local customer LAN. This procedure alters that configuration to now connect the 3958 RSA ethernet connection to connect to the TSSC private network (172.31.1.*xxx*). Disconnect the local LAN Ethernet connection to the RSA adapter port, and connect a new Ethernet cable between the RSA Ethernet port and the TSSC SMC hub. You are prompted for this action during the installation. If the connection between the RSA Ethernet port and the TSSC SMC hub is already established, proceed to the next step.

   Note: Depending upon the model of the TSSC and TSSC network switch being used, the port layout might be different than shown. If so, attach and label the cables according to the port number assignments specified, regardless of the position of the ports on the TSSC or the TSSC network switch.

5. After the installation is complete, unmount the *IBM RAS/BIOS and Firmware Update* DVD and eject it using the following commands:

   ```
   cd /
   eject /dev/hda
   ```

6. Repeat steps 1 on page 83 through 5 for the second 3958 server if applicable. You are prompted for "frame number".
7. Enter the same number that you entered for the first node. For example, if you configured the frame on the first node to be 110, configure the frame on the second node to 110 also, provided the two servers are being clustered together.
8. When all procedures have been completed and you are returned to a command line, type **exit** to log out of the server.

Results

The process of reinstalling the RAS package (for ProtecTIER software V2.3 or earlier only) is complete.

Chapter 7. Power off and power on procedures

This section provides procedures for turning on or off all components of the ProtecTIER server.

Power procedures for ProtecTIER version 3.4 or later

This section provides procedures for turning on or off all the components of the ProtecTIER server V3.4 or later on the 3958 DD6.

Powering off a TS7650G server version 3.4 or later on the 3958 DD6

About this task

The following is the recommended manual power off sequence for either a single node or clustered TS7650G on the 3958 DD6 model server.

Procedure

1. Have the customer stop all activities from attached hosts and quiesce all jobs.
2. Access the server:
   a. Attach a keyboard and monitor to the server and access the ProtecTIER Service Menu. Log on with the user ID `ptconfig` and the password `ptconfig` to access the ProtecTIER Service Menu.

```
------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
------------------------------------------------------------------------
   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
   9) ProtecTIER analysis (...)

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

   b. In the Service Menu, select Manage ProtecTIER Services (...) [Option 2].

      Note: Alternatively, you can type the following command:

      `ssh ptadmin@`*`xxx.xxx.xxx.xxx`*

      where *xxx.xxx.xxx.xxx* is the server IP address.
3. In the Manage ProtecTIER Services menu, select **Power off This Node** to power off the server.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
             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? 6
```

Powering on a TS7650G server version 3.4 or later on a 3958 DD6

About this task

This is the recommended manual power on sequence for a TS7650G server.

Procedure

1. Using the frame's UPO switch or the customer's circuit breaker, restore power to the frame (or frames).
2. Power on all expansion units.
3. Power on all storage controllers.
4. Attach the AC power cords to the PCMs or PSUs.

   Depending on the chassis power policy, one of the following occurs:
   - If the controllers are configured as “always-on”, the BMC causes a staged boot of the x86 subsystem.
   - the controllers are onfigured as “always-off”, the BMC starts, but the x86 subsystem does not start until you do one of the following actions:
     - Press the power on button on the rear of each SM controller.
     - Press the power button on the front right of the XP enclosure. This starts the x86 subsystem on all installed controllers.
     - Power up the unit remotely using the web management interface. A remote browser session communicates with the BMC over one of the Ethernet ports and provides power control of the system.
     - Issue the ipmitool power on command to the BMC of each controller.

   On starting up, GEM performs an enclosure validation procedure. This is the process of determining whether the PSUs can supply sufficient power for the system’s high power elements (such as the CPU, chipset and drives). This protects against mis-configuration of the hardware. Until this validation has succeeded, power consumption is kept under 60W.
5. Turn on the power switch on each of the PCM/PSU rear panels. The BMC will start to boot.
6. Press the power button on the server's front panel.

   Approximately 15 minutes after the server is powered-on, following the reboot, you can log in to the **ProtecTIER Service Menu**.

7. Access the **ProtecTIER Service Menu** with a monitor and keyboard plugged into the TS7650 server. Log in with the ID **ptconfig** and the password **ptconfig**.
8. From the **ProtecTIER Service Menu**, select the **Manage ProtecTIER services** option.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
--------------------------------------------------------------------------
   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
   9) ProtecTIER analysis (...)

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

9. From the **Manage ProtecTIER services** menu, select **Display services status**.

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

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

10. Wait until the display shows all the services have started.
11. The stand-alone TS7650 server power on process is complete.

Performing an emergency shutdown

Complete the task in this topic to perform an emergency shut down of the ProtecTIER server.

About this task

This topic describes how to shut down the TS7650G in case of an emergency.

Attention: Emergency situations might include fire, flood, extreme weather conditions, or other hazardous circumstances. If a power outage or emergency situation occurs, always turn off all power switches on all computing equipment. This helps to safeguard your equipment from potential damage due to electrical surges when power is restored. If the disk controller or disk expansion module loses power unexpectedly, it might be due to a hardware failure in the power system or in the midplane of the disk controller or disk expansion module.

Procedure

1. Stop all activity.
2. Check all of the light-emitting diodes (LEDs). Make a note of any Fault LEDs that are lit so that you can correct the problem when you turn on the power.

3. Turn off the emergency power off (EPO) switch and back-end disk repository.

   Important: 19-inch racks (Gateway) do not have an EPO switch. You can only power off by toggling the circuit breakers on the power distribution units.
4. Unplug the power cables from the disk controller and disk expansion module.

Chapter 8. End-of-call procedure

Before you hand the system back to the customer, finish the call by checking for and clearing any alerts.

Checking the BMC log on the 3958 DD6

Use the following procedure to check the BMC logs alerts and clear any open alerts on a 3958 DD6.

Procedure

1. Open a browser window and type the IP address of the BMC.
2. Log in with the userID `admin` and the password `admin`.
3. Click on the remote control tab.
4. Click on **console redirection**.

   Note: Make sure popups are enabled on your browser.
5. Click on the **Java console** button.
6. When the prompt asks if you want to run the application, click **Run**.
7. Review the log for error entries (a red E), or warnings (a yellow W) and verify that the notifications are valid.
8. After the problems are identified, if the fix was implemented, scroll to the bottom of the log and choose either the option to save the log as a text file (recommended in case it is needed later), or to clear the log. If you save the log as a text file, clear the log after saving.
9. After the log is cleared, from the left navigation pane, select **Log Off**. Close the browser window.
10. If this is a clustered system, repeat 2 through 9 for Node B.
11. Use the ProtecTIER Service menu (see "ProtecTIER Service menu" on page 11) to check for open problems in each node. Then, close all open problems.
    a. To display a list of open problems, select **Health Monitoring** > **List open problems**.
    b. Review any listed open problem records and verify that they were resolved.
    c. To cancel a problem, follow the on-screen instructions to enter the Problem Record number and cancel the problem. Read the screen carefully to determine the correct choice of action in your responses.
    d. After you close out the records, check for open problems again to verify that no further error records are listed.
    e. After all problems are closed, select the option to **Exit**.
12. Verify that there are no visible failure indicators on the front or rear of the server and any attached disk storage is free of any failure conditions:
    a. At the TSSC, right-click on the blue desktop and select **System Console Actions** > **Console Configuration Utility**.
    b. If prompted, log in with user ID **`service`** and password **`service`**.
    c. Select **Attached Systems**. From the list of attached systems, click to add a check mark in the box next to the server, then click the **Update Health** button. Click **OK**.

d. When the health status is returned, verify that the state reports no problems found.
e. If a **Warning**, **Failure**, or **Communications** error exists, you must resolve it. To help identify the fault, place a check mark next to the server again and click **View Health**. Review the returned information assistance in the cause. If it cannot be isolated, contact your next level of support.

   Note: If the message "RAS Service Mode Started" displays, ignore it at this time. Service Mode is disabled in the final steps of this procedure.
f. Continue to the next step.

13. To verify that both nodes are online and operational and that the filesystems are mounted, select **Manage ProtecTIER Services** > **Display Services Status** from the ProtecTIER Service menu (see “ProtecTIER Service menu” on page 11). Check the status of the vtfd, cman, clvmd, and gfs services.
14. After verifying all the services are operational and running, check the ProtecTIER Manager and verify that the node or nodes (if clustered) are accessible and online..
    a. At the TSSC, if not already logged in, log in with user ID `service` and password `service`.
    b. Right-click on the blue desktop and from the menu, select **Browser Functions** > **ProtecTIER Manager Functions** > **Launch GUI**.
    c. In the left navigation pane, select the tab for **Nodes**. Select the server. At the login for the node, click the **login** button. Type the user ID `ptoper` and the password `ptoper`. Click **OK**.
    d. Once logged in to the node, from the left navigation pane, select the tab for **Systems**. Verify that the node (or nodes if clustered) shows a **Status** of **OK**, the **Management Service** shows as **Online** and the **VT** shows as **Online**.
    e. If the status is online and **OK**, close the ProtecTIER Manager. Right-click on the TSSC blue desktop and select **Logout**.
15. Disable Service Mode on the servers:
    a. From a command line on Node A, access the ProtecTIER Service menu by entering `menu`.
    b. From the ProtecTIER Service menu, select **Health Monitoring** > **Service Mode**.
    c. Type `no` to disable Service Mode.

       Note: Allow up to 20 minutes for Service Mode to be disabled.
    d. Repeat steps a. through c. on Node B.
    e. Notify the customer that the system is available.
16. If the server or servers continue to report problems or show as offline, contact your next level of support.

Appendix A. Power-On Self-Test (POST) codes

This appendix gives the codes for the Power-On Self-Test (POST).

The POST LEDs are on the back of the controller. Each LED has a bit value as shown in the following table. Use the LED values to determine the HEX code.

Table 9. POST LED Bit Values

LED Number	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Value	1	2	4	8	16	32	64	128

Add the values of the LEDs that are on to obtain the number and then convert that number to hex. For example, if LEDs 0, 2, 3, 4, 5 and 6 are lit, this equates to: 1 + 4 + 8 + 16 + 32 + 64 = 125 or 0x7D in hex. Refer to the following tables to determine the meaning of the hex code.

List of POST codes

Power -On Self-Test (POST) LEDs show the boot progress of the x86 subsystem. If it fails to boot, the LEDs will show what stage of the process was being performed when the problem occurred.

Table 10. POST Codes - SEC Phase

Code	**SEC Phase**
0x01	SEC_SYSTEM_POWER_ON
0x02	SEC_BEFORE_MICROCODE_PATCH
0x03	SEC_AFTER_MICROCODE_PATCH
ox04	SEC_ACCESS_CSR
0x05	SEC_GENERIC_MSRINIT
0x06	SEC_CPU_SPEEDCFG
0x07	SEC_SETUP_CAR_OK
0x08	SEC_FORCE_MAX_RATIO
0x09	SEC_GO_TO_SECSTARTUP
0x0A	SEC_GO_TO_PEICORE

Table 11. POST Codes - PEI Phase

Code	**PEI Phase**
0x70	PEI_SIO_INIT
0x71	PEI_CPU_REG_INIT
0x72	PEI_CPU_AP_INIT
0x73	PEI_CPU_HT_RESET
0x74	PEI_PCIE_MMIO_INIT 0x74
0x75	PEI_NB_REG_INIT
0x76	PEI_SB_REG_INIT

Table 11. POST Codes - PEI Phase (continued)

Code	PEI Phase
0x77	PEI_PCIE_TRAINING
0x78	PEI_TPM_INIT
0x79	PEI_SMBUS_INIT
0x7A	PEI_PROGRAM_CLOCK_GEN
0x7B	PEI_IGD_EARLY_INITIAL
0x7C	PEI_HECI_INIT
0x7D	PEI_HECI_INIT
0x7E	PEI_MEMORY_INIT
0x7F	PEI_MEMORY_INIT_FOR_CRISIS
0x80	PEI_MEMORY_INSTALL
0x81	PEI_TXTPEI
0x82	PEI_SWITCH_STACK
0x83	PEI_MEMORY_CALLBACK
0x84	PEI_ENTER_RECOVERY_MODE
0x85	PEI_RECOVERY_MEDIA_FOUND
0x86	PEI_RECOVERY_MEDIA_NOT_FOUND
0x87	PEI_RECOVERY_LOAD_FILE_DONE
0x88	PEI_RECOVERY_START_FLASH
0x89	PEI_ENTER_DXEIPL
0x8A	PEI_FINDING_DXE_CORE
0x8B	PEI_GO_TO_DXE_CORE
0x8C	PEI_IFFS_TRANSITION_START
0x8B	PEI_IFFS_TRANSITION_END

Table 12. POST Codes DXE Phase

Code	DXE Phase
0x40	DXE_TCGDXE
0x41	DXE_SB_SPI_INIT
0x42	DXE_CF9_RESET
0x43	DXE_SB_SERIAL_GPIO_INIT
0x44	DXE_SMMACCESS
0x45	DXE_NB_INIT
0x46	DXE_SIO_INIT
0x47	DXE_LEGACY_REGION
0x48	DXE_SB_INIT
0x49	DXE_IDENTIFY_FLASH_DEVICE
0x4A	DXE_FTW_INIT
0x4B	DXE_VARIABLE_INIT
0x4C	DXE_VARIABLE_INIT_FAIL
0x4D	DXE_MTC_INIT

Table 12. POST Codes DXE Phase (continued)

Code	DXE Phase
0x4E	DXE_CPU_INIT
0x4F	DXE_MP_CPU_INIT
0x50	DXE_SMBUS_INIT
0x51	DXE_SMART_TIMER_INIT
0x52	DXE_PCRTC_INIT
0x53	DXE_SATA_INIT
0x54	DXE_SMM_CONTROLER_INIT
0x55	DXE_LEGACY_INTERRUPT
0x56	DXE_RELOCATE_SMBASE
0x57	DXE_FIRST_SMI
0x58	DXE_VTD_INIT
0x59	DXE_BEFORE_CSM16_INIT
0x5A	DXE_AFTER_CSM16_INIT
0x5B	DXE_LOAD_ACPI_TABLE
0x5C	DXE_SB_DISPATCH
0x5D	DXE_SB_IOTRAP_INIT
0x5E	DXE_SUBCLASS_DRIVER
0x5F	DXE_PPM_INIT
0x60	DXE_HECIDRV_INIT
0x61	DXE_VARIABLE_RECLAIM
0x62	DXE_FLASH_PART_NONSUPPORT

Table 13. POST Codes - BDS Phase

Code	BDS Phase
0x10	BDS_ENTER_BDS
0x11	BDS_INSTALL_HOTKEY
0x12	BDS_ASF_INIT
0x13	BDS_PCI_ENUMERATION_START
0x14	BDS_BEFORE_PCIIO_INSTALL
0x15	BDS_PCI_ENUMERATION_END
0x16	BDS_CONNECT_CONSOLE_IN
0x17	BDS_CONNECT_CONSOLE_OUT
0x18	BDS_CONNECT_STD_ERR
0x19	BDS_CONNECT_USB_HC
0x1A	BDS_CONNECT_USB_BUS
0x1B	BDS_CONNECT_USB_DEVICE
0x1C	BDS_NO_CONSOLE_ACTION
0x1D	BDS_DISPLAY_LOGO_SYSTEM_INFO
0x1E	BDS_START_IDE_CONTROLLER
0x1F	BDS_START_SATA_CONTROLLER

Table 13. POST Codes - BDS Phase (continued)

Code	BDS Phase
0x20	BDS_START_ISA_ACPI_CONTROLLER
0x21	BDS_START_ISA_BUS
0x22	BDS_START_ISA_FDD
0x23	BDS_START_ISA_SERIAL
0x24	BDS_START_IDE_BUS
0x25	BDS_START_AHCI_BUS
0x26	BDS_CONNECT_LEGACY_ROM
0x27	BDS_ENUMERATE_ALL_BOOT_OPTION
0x28	BDS_END_OF_BOOT_SELECTION
0x29	BDS_ENTER_SETUP
0x2A	BDS_ENTER_BOOT_MANAGER
0x2B	BDS_BOOT_DEVICE_SELECT
0x2C	BDS_EFI64_SHADOW_ALL_LEGACY_ROM
0x2D	BDS_ACPI_S3SAVE
0x2E	BDS_READY_TO_BOOT_EVENT
0x2F	BDS_GO_LEGACY_BOOT
0x30	BDS_GO_UEFI_BOOT
0x31	BDS_LEGACY16_PREPARE_TO_BOOT
0x32	BDS_EXIT_BOOT_SERVICES
0x33	BDS_LEGACY_BOOT_EVENT
0x34	BDS_ENTER_LEGACY_16_BOOT
0x35	BDS_RECOVERY_START_FLASH
0x36	BDS_START_SDHC_BUS
0x37	BDS_CONNECT_ATA_LEGACY
0x38	BDS_CONNECT_SD_LEGACY
0xF9	POST_BDS_NO_BOOT_DEVICE
0xFB	POST_BDS_START_IMAGE
0xFD	POST_BDS_ENTER_INT19
0xFE	POST_BDS_JUMP_BOOT_SECTOR

Table 14. POST Codes - SMM Phase

Code	SMM Phase
0xA0	SMM_IDENTIFY_FLASH_DEVICE
0xA2	SMM_SMM_PLATFORM_INIT
oxA6	SMM_ACPI_ENABLE_START
0xA7	SMM_ACPI_ENABLE_END
0xA1	SMM_S1_SLEEP_CALLBACK
0xA3	SMM_S3_SLEEP_CALLBACK
0xA4	SMM_S4_SLEEP_CALLBACK
0xA5	SMM_S5_SLEEP_CALLBACK

Table 14. POST Codes - SMM Phase (continued)

Code	SMM Phase
0xAB	SMM_ACPI_DISABLE_START
0xA9	SMM_ACPI_DISABLE_END

Appendix B. ProtecTIER Network Performance Validation Utility

The objective of the **pt_net_perf_util** is to test maximal network performance in order to discover potential performance bottlenecks. On VTL systems, the utility tests maximal replication performance between two future ProtecTIER VTL repositories by emulating the network usage patterns of the ProtecTIER Native Replication component. On OpenStorage systems, the utility tests network performance between an OpenStorage host and a ProtecTIER server to identify possible bottlenecks in a backup and restore scenario.

Appendix C. Worldwide time zone codes

Use the information in the following table to help you set the system's time zone.

Time zone codes

The following table lists all of the worldwide time zone codes and the associated time zone descriptions. Additional information about the time zone is located in the Comments column.

Code	Time zone	Comments
AD	Europe/Andorra	
AE	Asia/Dubai	
AF	Asia/Kabul	
AG	America/Antigua	
AI	America/Anguilla	
AL	Europe/Tirane	
AM	Asia/Yerevan	
AN	America/Curacao	
AO	Africa/Luanda	
AQ	Antarctica/McMurdo	McMurdo Station, Ross Island
AQ	Antarctica/South_Pole	Amundsen-Scott Station, South Pole
AQ	Antarctica/Rothera	Rothera Station, Adelaide Island
AQ	Antarctica/Palmer	Palmer Station, Anvers Island
AQ	Antarctica/Mawson	Mawson Station, Holme Bay
AQ	Antarctica/Davis	Davis Station, Vestfold Hills
AQ	Antarctica/Casey	Casey Station, Bailey Peninsula
AQ	Antarctica/Vostok	Vostok Station, S Magnetic Pole
AQ	Antarctica/DumontDUrville	Dumont-d'Urville Station, Terre Adelie
AQ	Antarctica/Syowa	Syowa Station, E Ongul I
AR	America/Argentina/Buenos_Aires	Buenos Aires (BA, CF)
AR	America/Argentina/Cordoba	most locations (CB, CC, CN, ER, FM, LP, MN, NQ, RN, SA, SE, SF, SL)
AR	America/Argentina/Jujuy	Jujuy (JY)
AR	America/Argentina/Tucuman	Tucuman (TM)
AR	America/Argentina/Catamarca	Catamarca (CT), Chubut (CH)
AR	America/Argentina/La_Rioja	La Rioja (LR)
AR	America/Argentina/San_Juan	San Juan (SJ)
AR	America/Argentina/Mendoza	Mendoza (MZ)
AR	America/Argentina/Rio_Gallegos	Santa Cruz (SC)
AR	America/Argentina/Ushuaia	Tierra del Fuego (TF)
AS	Pacific/Pago_Pago	

Code	Time zone	Comments
AT	Europe/Vienna	
AU	Australia/Lord_Howe	Lord Howe Island
AU	Australia/Hobart	Tasmania - most locations
AU	Australia/Currie	Tasmania - King Island
AU	Australia/Melbourne	Victoria
AU	Australia/Sydney	New South Wales - most locations
AU	Australia/Broken_Hill	New South Wales - Yancowinna
AU	Australia/Brisbane	Queensland - most locations
AU	Australia/Lindeman	Queensland - Holiday Islands
AU	Australia/Adelaide	South Australia
AU	Australia/Darwin	Northern Territory
AU	Australia/Perth	Western Australia - most locations
AU	Australia/Eucla	Western Australia - Eucla area
AW	America/Aruba	
AX	Europe/Mariehamn	
AZ	Asia/Baku	
BA	Europe/Sarajevo	
BB	America/Barbados	
BD	Asia/Dhaka	
BE	Europe/Brussels	
BF	Africa/Ouagadougou	
BG	Europe/Sofia	
BH	Asia/Bahrain	
BI	Africa/Bujumbura	
BJ	Africa/Porto-Novo	
BL	America/St_Barthelemy	
BM	Atlantic/Bermuda	
BN	Asia/Brunei	
BO	America/La_Paz	
BR	America/Noronha	Atlantic islands
BR	America/Belem	Amapa, E Para
BR	America/Fortaleza	NE Brazil (MA, PI, CE, RN, PB)
BR	America/Recife	Pernambuco
BR	America/Araguaina	Tocantins
BR	America/Maceio	Alagoas, Sergipe
BR	America/Bahia	Bahia
BR	America/Sao_Paulo	S & SE Brazil (GO, DF, MG, ES, RJ, SP, PR, SC, RS)
BR	America/Campo_Grande	Mato Grosso do Sul
BR	America/Cuiaba	Mato Grosso
BR	America/Porto_Velho	W Para, Rondonia
BR	America/Boa_Vista	Roraima

Code	Time zone	Comments
BR	America/Manaus	E Amazonas
BR	America/Eirunepe	W Amazonas
BR	America/Rio_Branco	Acre
BS	America/Nassau	
BT	Asia/Thimphu	
BW	Africa/Gaborone	
BY	Europe/Minsk	
BZ	America/Belize	
CA	America/St_Johns	Newfoundland Time, including SE Labrador
CA	America/Halifax	Atlantic Time - Nova Scotia (most places), PEI
CA	America/Glace_Bay	Atlantic Time - Nova Scotia - places that did not observe DST 1966-1971
CA	America/Moncton	Atlantic Time - New Brunswick
CA	America/Goose_Bay	Atlantic Time - Labrador - most locations
CA	America/Blanc-Sablon	Atlantic Standard Time - Quebec - Lower North Shore
CA	America/Montreal	Eastern Time - Quebec - most locations
CA	America/Toronto	Eastern Time - Ontario - most locations
CA	America/Nipigon	Eastern Time - Ontario & Quebec - places that did not observe DST 1967-1973
CA	America/Thunder_Bay	Eastern Time - Thunder Bay, Ontario
CA	America/Iqaluit	Eastern Time - east Nunavut - most locations
CA	America/Pangnirtung	Eastern Time - Pangnirtung, Nunavut
CA	America/Resolute	Eastern Time - Resolute, Nunavut
CA	America/Atikokan	Eastern Standard Time - Atikokan, Ontario and Southampton I, Nunavut
CA	America/Rankin_Inlet	Central Time - central Nunavut
CA	America/Winnipeg	Central Time - Manitoba & west Ontario
CA	America/Rainy_River	Central Time - Rainy River & Fort Frances, Ontario
CA	America/Regina	Central Standard Time - Saskatchewan - most locations
CA	America/Swift_Current	Central Standard Time - Saskatchewan - midwest
CA	America/Edmonton	Mountain Time - Alberta, east British Columbia & west Saskatchewan
CA	America/Cambridge_Bay	Mountain Time - west Nunavut
CA	America/Yellowknife	Mountain Time - central Northwest Territories
CA	America/Inuvik	Mountain Time - west Northwest Territories
CA	America/Dawson_Creek	Mountain Standard Time - Dawson Creek & Fort Saint John, British Columbia
CA	America/Vancouver	Pacific Time - west British Columbia
CA	America/Whitehorse	Pacific Time - south Yukon
CA	America/Dawson	Pacific Time - north Yukon
CC	Indian/Cocos	

Code	Time zone	Comments
CD	Africa/Kinshasa	west Dem. Rep. of Congo
CD	Africa/Lubumbashi	east Dem. Rep. of Congo
CF	Africa/Bangui	
CG	Africa/Brazzaville	
CH	Europe/Zurich	
CI	Africa/Abidjan	
CK	Pacific/Rarotonga	
CL	America/Santiago	most locations
CL	Pacific/Easter	Easter Island & Sala y Gomez
CM	Africa/Douala	
CN	Asia/Shanghai	east China - Beijing, Guangdong, Shanghai, etc.
CN	Asia/Harbin	Heilongjiang (except Mohe), Jilin
CN	Asia/Chongqing	central China - Sichuan, Yunnan, Guangxi, Shaanxi, Guizhou, etc.
CN	Asia/Urumqi	most of Tibet & Xinjiang
CN	Asia/Kashgar	west Tibet & Xinjiang
CO	America/Bogota	
CR	America/Costa_Rica	
CU	America/Havana	
CV	Atlantic/Cape_Verde	
CX	Indian/Christmas	
CY	Asia/Nicosia	
CZ	Europe/Prague	
DE	Europe/Berlin	
DJ	Africa/Djibouti	
DK	Europe/Copenhagen	
DM	America/Dominica	
DO	America/Santo_Domingo	
DZ	Africa/Algiers	
EC	America/Guayaquil	mainland
EC	Pacific/Galapagos	Galapagos Islands
EE	Europe/Tallinn	
EG	Africa/Cairo	
EH	Africa/El_Aaiun	
ER	Africa/Asmara	
ES	Europe/Madrid	mainland
ES	Africa/Ceuta	Ceuta & Melilla
ES	Atlantic/Canary	Canary Islands
ET	Africa/Addis_Ababa	
FI	Europe/Helsinki	
FJ	Pacific/Fiji	

Code	Time zone	Comments
FK	Atlantic/Stanley	
FM	Pacific/Truk	Truk (Chuuk) and Yap
FM	Pacific/Ponape	Ponape (Pohnpei)
FM	Pacific/Kosrae	Kosrae
FO	Atlantic/Faroe	
FR	Europe/Paris	
GA	Africa/Libreville	
GB	Europe/London	
GD	America/Grenada	
GE	Asia/Tbilisi	
GF	America/Cayenne	
GG	Europe/Guernsey	
GH	Africa/Accra	
GI	Europe/Gibraltar	
GL	America/Godthab	most locations
GL	America/Danmarkshavn	east coast, north of Scoresbysund
GL	America/Scoresbysund	Scoresbysund / Ittoqqortoormiit
GL	America/Thule	Thule / Pituffik
GM	Africa/Banjul	
GN	Africa/Conakry	
GP	America/Guadeloupe	
GQ	Africa/Malabo	
GR	Europe/Athens	
GS	Atlantic/South_Georgia	
GT	America/Guatemala	
GU	Pacific/Guam	
GW	Africa/Bissau	
GY	America/Guyana	
HK	Asia/Hong_Kong	
HN	America/Tegucigalpa	
HR	Europe/Zagreb	
HT	America/Port-au-Prince	
HU	Europe/Budapest	
ID	Asia/Jakarta	Java & Sumatra
ID	Asia/Pontianak	west & central Borneo
ID	Asia/Makassar	east & south Borneo, Celebes, Bali, Nusa Tengarra, west Timor
ID	Asia/Jayapura	Irian Jaya & the Moluccas
IE	Europe/Dublin	
IL	Asia/Jerusalem	
IM	Europe/Isle_of_Man	

Code	Time zone	Comments
IN	Asia/Calcutta	
IO	Indian/Chagos	
IQ	Asia/Baghdad	
IR	Asia/Tehran	
IS	Atlantic/Reykjavik	
IT	Europe/Rome	
JE	Europe/Jersey	
JM	America/Jamaica	
JO	Asia/Amman	
JP	Asia/Tokyo	
KE	Africa/Nairobi	
KG	Asia/Bishkek	
KH	Asia/Phnom_Penh	
KI	Pacific/Tarawa	Gilbert Islands
KI	Pacific/Enderbury	Phoenix Islands
KI	Pacific/Kiritimati	Line Islands
KM	Indian/Comoro	
KN	America/St_Kitts	
KP	Asia/Pyongyang	
KR	Asia/Seoul	
KW	Asia/Kuwait	
KY	America/Cayman	
KZ	Asia/Almaty	most locations
KZ	Asia/Qyzylorda	Qyzylorda (Kyzylorda, Kzyl-Orda)
KZ	Asia/Aqtobe	Aqtobe (Aktobe)
KZ	Asia/Aqtau	Atyrau (Atirau, Gur'yev), Mangghystau (Mankistau)
KZ	Asia/Oral	West Kazakhstan
LA	Asia/Vientiane	
LB	Asia/Beirut	
LC	America/St_Lucia	
LI	Europe/Vaduz	
LK	Asia/Colombo	
LR	Africa/Monrovia	
LS	Africa/Maseru	
LT	Europe/Vilnius	
LU	Europe/Luxembourg	
LV	Europe/Riga	
LY	Africa/Tripoli	
MA	Africa/Casablanca	
MC	Europe/Monaco	
MD	Europe/Chisinau	

Code	Time zone	Comments
ME	Europe/Podgorica	
MF	America/Marigot	
MG	Indian/Antananarivo	
MH	Pacific/Majuro	most locations
MH	Pacific/Kwajalein	Kwajalein
MK	Europe/Skopje	
ML	Africa/Bamako	
MM	Asia/Rangoon	
MN	Asia/Ulaanbaatar	most locations
MN	Asia/Hovd	Bayan-Olgiy, Govi-Altai, Hovd, Uvs, Zavkhan
MN	Asia/Choibalsan	Dornod, Sukhbaatar
MO	Asia/Macau	
MP	Pacific/Saipan	
MQ	America/Martinique	
MR	Africa/Nouakchott	
MS	America/Montserrat	
MT	Europe/Malta	
MU	Indian/Mauritius	
MV	Indian/Maldives	
MW	Africa/Blantyre	
MX	America/Mexico_City	Central Time - most locations
MX	America/Cancun	Central Time - Quintana Roo
MX	America/Merida	Central Time - Campeche, Yucatan
MX	America/Monterrey	Central Time - Coahuila, Durango, Nuevo Leon, Tamaulipas
MX	America/Mazatlan	Mountain Time - S Baja, Nayarit, Sinaloa
MX	America/Chihuahua	Mountain Time - Chihuahua
MX	America/Hermosillo	Mountain Standard Time - Sonora
MX	America/Tijuana	Pacific Time
MY	Asia/Kuala_Lumpur	peninsular Malaysia
MY	Asia/Kuching	Sabah & Sarawak
MZ	Africa/Maputo	
NA	Africa/Windhoek	
NC	Pacific/Noumea	
NE	Africa/Niamey	
NF	Pacific/Norfolk	
NG	Africa/Lagos	
NI	America/Managua	
NL	Europe/Amsterdam	
NO	Europe/Oslo	
NP	Asia/Katmandu	

Code	Time zone	Comments
NR	Pacific/Nauru	
NU	Pacific/Niue	
NZ	Pacific/Auckland	most locations
NZ	Pacific/Chatham	Chatham Islands
OM	Asia/Muscat	
PA	America/Panama	
PE	America/Lima	
PF	Pacific/Tahiti	Society Islands
PF	Pacific/Marquesas	Marquesas Islands
PF	Pacific/Gambier	Gambier Islands
PG	Pacific/Port_Moresby	
PH	Asia/Manila	
PK	Asia/Karachi	
PL	Europe/Warsaw	
PM	America/Miquelon	
PN	Pacific/Pitcairn	
PR	America/Puerto_Rico	
PS	Asia/Gaza	
PT	Europe/Lisbon	mainland
PT	Atlantic/Madeira	Madeira Islands
PT	Atlantic/Azores	Azores
PW	Pacific/Palau	
PY	America/Asuncion	
QA	Asia/Qatar	
RE	Indian/Reunion	
RO	Europe/Bucharest	
RS	Europe/Belgrade	
RU	Europe/Kaliningrad	Moscow-01 - Kaliningrad
RU	Europe/Moscow	Moscow+00 - west Russia
RU	Europe/Volgograd	Moscow+00 - Caspian Sea
RU	Europe/Samara	Moscow+01 - Samara, Udmurtia
RU	Asia/Yekaterinburg	Moscow+02 - Urals
RU	Asia/Omsk	Moscow+03 - west Siberia
RU	Asia/Novosibirsk	Moscow+03 - Novosibirsk
RU	Asia/Krasnoyarsk	Moscow+04 - Yenisei River
RU	Asia/Irkutsk	Moscow+05 - Lake Baikal
RU	Asia/Yakutsk	Moscow+06 - Lena River
RU	Asia/Vladivostok	Moscow+07 - Amur River
RU	Asia/Sakhalin	Moscow+07 - Sakhalin Island
RU	Asia/Magadan	Moscow+08 - Magadan
RU	Asia/Kamchatka	Moscow+09 - Kamchatka

Code	Time zone	Comments
RU	Asia/Anadyr	Moscow+10 - Bering Sea
RW	Africa/Kigali	
SA	Asia/Riyadh	
SB	Pacific/Guadalcanal	
SC	Indian/Mahe	
SD	Africa/Khartoum	
SE	Europe/Stockholm	
SG	Asia/Singapore	
SH	Atlantic/St_Helena	
SI	Europe/Ljubljana	
SJ	Arctic/Longyearbyen	
SK	Europe/Bratislava	
SL	Africa/Freetown	
SM	Europe/San_Marino	
SN	Africa/Dakar	
SO	Africa/Mogadishu	
SR	America/Paramaribo	
ST	Africa/Sao_Tome	
SV	America/El_Salvador	
SY	Asia/Damascus	
SZ	Africa/Mbabane	
TC	America/Grand_Turk	
TD	Africa/Ndjamena	
TF	Indian/Kerguelen	
TG	Africa/Lome	
TH	Asia/Bangkok	
TJ	Asia/Dushanbe	
TK	Pacific/Fakaofo	
TL	Asia/Dili	
TM	Asia/Ashgabat	
TN	Africa/Tunis	
TO	Pacific/Tongatapu	
TR	Europe/Istanbul	
TT	America/Port_of_Spain	
TV	Pacific/Funafuti	
TW	Asia/Taipei	
TZ	Africa/Dar_es_Salaam	
UA	Europe/Kiev	most locations
UA	Europe/Uzhgorod	Ruthenia
UA	Europe/Zaporozhye	Zaporozh'ye, E Lugansk / Zaporizhia, E Luhansk
UA	Europe/Simferopol	central Crimea

Code	Time zone	Comments
UG	Africa/Kampala	
UM	Pacific/Johnston	Johnston Atoll
UM	Pacific/Midway	Midway Islands
UM	Pacific/Wake	Wake Island
US	America/New_York	Eastern Time
US	America/Detroit	Eastern Time - Michigan - most locations
US	America/Kentucky/Louisville	Eastern Time - Kentucky - Louisville area
US	America/Kentucky/Monticello	Eastern Time - Kentucky - Wayne County
US	America/Indiana/Indianapolis	Eastern Time - Indiana - most locations
US	America/Indiana/Vincennes	Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
US	America/Indiana/Knox	Eastern Time - Indiana - Starke County
US	America/Indiana/Winamac	Eastern Time - Indiana - Pulaski County
US	America/Indiana/Marengo	Eastern Time - Indiana - Crawford County
US	America/Indiana/Vevay	Eastern Time - Indiana - Switzerland County
US	America/Chicago	Central Time
US	America/Indiana/Tell_City	Central Time - Indiana - Perry County
US	America/Indiana/Petersburg	Central Time - Indiana - Pike County
US	America/Menominee	Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
US	America/North_Dakota/Center	Central Time - North Dakota - Oliver County
US	America/North_Dakota/New_Salem	Central Time - North Dakota - Morton County (except Mandan area)
US	America/Denver	Mountain Time
US	America/Boise	Mountain Time - south Idaho & east Oregon
US	America/Shiprock	Mountain Time - Navajo
US	America/Phoenix	Mountain Standard Time - Arizona
US	America/Los_Angeles	Pacific Time
US	America/Anchorage	Alaska Time
US	America/Juneau	Alaska Time - Alaska panhandle
US	America/Yakutat	Alaska Time - Alaska panhandle neck
US	America/Nome	Alaska Time - west Alaska
US	America/Adak	Aleutian Islands
US	Pacific/Honolulu	Hawaii
UY	America/Montevideo	
UZ	Asia/Samarkand	west Uzbekistan
UZ	Asia/Tashkent	east Uzbekistan
VA	Europe/Vatican	
VC	America/St_Vincent	
VE	America/Caracas	
VG	America/Tortola	
VI	America/St_Thomas	

Code	Time zone	Comments
VN	Asia/Saigon	
VU	Pacific/Efate	
WF	Pacific/Wallis	
WS	Pacific/Apia	
YE	Asia/Aden	
YT	Indian/Mayotte	
ZA	Africa/Johannesburg	
ZM	Africa/Lusaka	
ZW	Africa/Harare	

Appendix D. SAS replacement on a ProtecTIER server running version V3.4.0 or V3.4.1

Complete the task in this topic on existing Seagate SAS drives before performing a SAS replacement.

About this task

If there are any Seagate SAS drives in the TS7650G, the regular SAS replacement procedure described in "Removing and replacing a SAS drive from the chassis" on page 67 it can cause the SAS replacement script to fail. This appendix describes a preliminary procedure you must run before performing a SAS replacement on a TS7650G running ProtecTIER V3.4.0 or V3.4.1.

Procedure

1. Check if multipath is using any Seagate SAS drive by typing the typing the following command on the CLI, `# multipath -ll | grep SEAGATE` This is an example of the output from the above command.

   ```
   mpath19 (35000c5008e674907) dm-0 SEAGATE,ST600MP0005
   ```

   The result indicates that the drive is a Seagate, Model Number ST600MP0005. Also notice that the WWID is only a 16 digit number (35000c5008e674907) rather than a 32 digit number (for example, 360050768028c059bb000000000000064).
2. Annotate the mpath device associated with the SEAGATE SAS drive.
3. Confirm the correspondence between the multipath driver devices and the devnode assigned to the physical SAS disk you are replacing.

   Node A uses the drive in the slot 1 (of the 24 SAS drive slots). In the persistent naming convention, the LUN for this device is expected to always be 47.
4. Check the devnode assigned to the LUN 47 by entering the following command `# ls -l /dev/disk/by-path/*sas*:47` Following is an example of the output from this command.

   ```
   lrwxrwxrwx 1 root root 9 Apr 15 03:57
   /dev/disk/by-path/pci-0000:0d:00.0-sas-0x50050cc10f26f73f:1:47-0x5000c5007f373826:47 -> ../../sdf
   ```
5. Node B uses the drive in the slot 24 (of the 24 SAS drive slots). In the persistent naming convention, the LUN for this device is expected to always s be 5. Check the devnode assigned to the LUN 5 by entering the following command: `# ls -l /dev/disk/by-path/*sas*:5` Following is an example of the output from this command.

   ```
   lrwxrwxrwx 1 root root 9 Apr 15 03:57
   /dev/disk/by-path/pci-0000:0d:00.0-sas-0x50050cc10f26f73f:1:5-0x5000c5007f180142:5 -> ../../sde
   ```
6. Check that the devnode showed in the multipath output is the same as the devnode from the persistent naming assigned to the SAS drive that you are replacing.

   This is an example of replacing the SAS drive in slot 24:

   The devnode showed in the multipath output.

   ```
   mpath19 (35000c5008e674907) dm-0 SEAGATE,ST600MP0005
   [size=559G][features=0][hwhandler=0][rw]
   \_ round-robin 0 [prio=1][active]
   \_ 9:0:0:0 sde 8:64 [active][ready]
   ```

The devnode from the persistent naming command.

```
# ls -l /dev/disk/by-path/*sas*:5
lrwxrwxrwx 1 root root 9 Apr 15 03:57
/dev/disk/by-path/pci-0000:0d:00.0-sas-0x50050cc10f26f73f:1:5-0x5000c500f180 142:5-> ../../sde
```

7. Using the devnode identified, check if the disk has partitions by running the following command:

   ```
   # fdisk -l /dev/sde
   ```

   Example of a disk with a partition:

   ```
   # fdisk -l /dev/sde

   WARNING: GPT (GUID Partition Table) detected on '/dev/sde'!
   The util fdisk doesn't support GPT. Use GNU Parted.

   Disk /dev/sde: 600.1 GB, 6001272668 16 bytes
   255 heads, 63 sectors/track, 72961 cylinders
   Units = cylinders of 16065 * 512 = 822528 bytes
   Device Boot Start End Blocks ID System
   /dev/sde1 1 72962 586061783+ ee EFI GPT
   ```

   Example of a disk without a partition:

   ```
   # fdisk -l /dev/sde

   WARNING: GPT (GUID Partition Table) detected on '/dev/sde'!
   The util fdisk doesn't support GPT. Use GNU Parted.

   Disk /dev/sde: 600.1 GB, 6001272668 16 bytes
   255 heads, 63 sectors/track, 72961 cylinders
   Units = cylinders of 16055 * 512 = 8225280 bytes
   Disk /dev/sde doesn't contain a valid partition table
   ```

8. If the disk has a partition, proceed to go to step 9. If the disk does not have a partition, go to step 10.
9. If the disk has partitions, run the dd command to eliminate the content of the device, including the partition:

   Note: Change the devnode accordingly with the device identified in step 3 on page 111.

   ```
   # dd if=/dev/zero of=/dev/sde bs=2048 count=6144
   ```

10. Run a multipath flush command for the mpath identified in Appendix D, “SAS replacement on a ProtecTIER server running version V3.4.0 or V3.4.1,” on page 111 by typing the following command in the CLI: `# multipath =f mpath 19`. This makes the multipath driver discard the mpath using the SAS drive.
11. Once the device is flushed, confirm the multipath is no longer assigning an mpath to it by running a multipath -ll command.

    Change the devnode accordingly with the device identified in step 3 on page 111. # multipath -ll | grep **sde**

    Regardless of whether only one SAS drive was replaced, and regardless of which SAS drive was replaced (slot 1 or slot 24), the following steps must be performed on both nodes A and B.
12. Update the multipath.conf with the WWID/WWN saved in step 2 on page 111.
13. Edit the /etc/mulitpath.conf file and look for the blacklist section. Before the change, the black list sections only shows the WWID of the two original SAS drives.

    ```
    blacklist {
    wwid SATA_Micron_M600_MTF_15240FE38574
    wwid 35000c500e664ab3
    wwid 35000c508e6704ef
    }
    ```

14. After the last WWID in the blaacklist section, add the WWN of the new SAS drives inserted in the replacement.

    Once changed, the blacklist section will have one or two new WWIDs (depending on how many SAS drives were replaced. You can add a comment to the WWID entries if you like:

    ```
    blacklist {
    wwid SATA_Micron_M600_MTF_15240FE38574
    wwid 35000c5008e664ab3
    wwid 35000c50086704ef
    wwid 35000c5008e668ab7   # Node A SAS drive replaced on 2016-04-22
    wwid 35000c5008e674907   # Node B SAS drive replaced on 2016-04-22
    }
    ```

15. Save the multipath.conf file.
16. Reload the multipathd service to keep the new configuration by typing the following command in the CLI: `# service multipathd reload` The following is an example of the output displayed:

    ```
    Reloading multipathd: [ OK ]
    ```

Accessibility for publications and ProtecTIER Manager

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. Use these procedures to enable screen-reader compatibility, change the Windows contrast setting, and customize the color palette used in ProtecTIER Manager.

About this task

If you experience difficulties when you use the PDF files and want to request a Web-based format for a publication, send your request to the following address:

International Business Machines Corporation
Information Development
Department GZW
9000 South Rita Road
Tucson, Arizona 85744-001 U.S.A

In the request, be sure to include the publication number and title. When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

About the Windows-based accessibility features

About this task

The accessibility features in ProtecTIER Manager help persons with limited vision use the ProtecTIER Manager installation wizard and software. After preparing the ProtecTIER Manager workstation for accessibility, you can use Windows-based screen-reader software and a digital voice synthesizer to hear what is displayed on the screen.

The installation, configuration, and instructional screens in the Windows versions of the ProtecTIER Manager installation wizard and the ProtecTIER Manager software have been tested with Job Access with Speech (JAWS). However, the associated diagrams and graphs in ProtecTIER Manager and ProtecTIER Replication Manager, do not currently support keyboard navigation or screen-reader use. You can obtain full system statistics (typically provided in the diagrams and graphs) by going to the ProtecTIER Manager toolbar and clicking: **Reports** > **Create long term statistics report**, and downloading the results.

To enable screen-reader compatibility, you must prepare the ProtecTIER Manager workstation by completing these tasks. Instructions are provided in the topics that follow:

Before you install ProtecTIER Manager:

- Download and install the Java Runtime Environment (JRE).
- Download and install the Java Access Bridge (JAB).

After you install ProtecTIER Manager:

- Change the ProtecTIER Manager preferences to enable support of the Windows system settings *(required)*.
- Select a high-contrast color scheme in Windows *(optional)*.
- Customize the color palette used in the ProtecTIER Manager display *(optional)*.

About the Java-based tools

About this task

Complete the following procedures to download and install the Java-based tools that are required to enable full screen-reader compatibility on the ProtecTIER Manager workstation.

Install the Java™ Runtime Environment (JRE) first, and then install the Java Access Bridge (JAB). Both of these tools must be installed before you install the ProtecTIER Manager software.

For simplicity, download the Java-based tools by using the ProtecTIER Manager workstation on which you are installing the JRE and JAB. If this is not possible, try to use another computer that is running Windows.

Installing the Java Runtime Environment

About this task

The JRE includes the Java Virtual Machine (JVM). These tools are necessary for your computer to run Java-based applications.

Procedure

1. Go to http://www.java.com. The Java website opens.

   The java.com website auto-detects the operating system and Internet browser of the computer you use when you access the site.
2. Click **Free Java Download**, and proceed as appropriate:
   - If the **Download Java for Windows** page opens, go on to step 3
   - If the **Download Java for...** page title contains the name of an operating system other than Windows, do the following:
     a. Click the **See all downloads here** link.

        The list of available downloads, categorized by operating system, displays.
     b. In the Windows section, click **Windows 7/XP/Vista/2000/2003/2008 Online**.
3. Review the information provided, and then click **Agree and Start Free Download**.

   The download dialog box opens.
4. Follow the on-screen instructions to save the executable (.exe) installer file to the hard disk drive.
5. After the download is complete, find the installer file on the hard disk drive and write down the full path to the location of the file. For example: *C:\Program Files\Java\jre6\bin\java.exe*. This path is needed during ProtecTIER Manager installation.
6. Proceed as appropriate:

- If you downloaded the installer on the ProtecTIER Manager workstation on which you are installing the JRE, go on to step 7.
- If you downloaded the installer on a PC other than the applicable ProtecTIER Manager workstation, do the following:
  a. Copy the installer file onto a CD, flash memory drive, or other form of removable media.
  b. Copy the installer file from the removable media to the hard disk drive of the ProtecTIER Manager workstation.
  c. Go on to step 7.

7. Double-click the installer file to start the **Java installation wizard**.

   The **Java Setup – Welcome** window opens.
8. Click **Install** and follow the on-screen instructions to complete the installation process.
9. When you have successfully installed the JRE, go on to "Installing the Java Access Bridge."

Installing the Java Access Bridge

About this task

The Java Access Bridge (JAB) makes it possible for you to use Java-based screen readers with the ProtecTIER Manager installation wizard and software.

Procedure

1. Go to: http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136191.html.

   The **Java SE Desktop Accessibility** page of the Oracle website opens.
2. Read the information provided, then click **Access Bridge**.
3. Scroll down to the **Java Access Bridge for Microsoft Windows Operating System x.x.x** (where *x.x.x* is the most recent version listed) section. Click the **Download Java Access Bridge x.x.x** link.

   The **Software License Agreement** page opens.
4. Read the license agreement, and then select the **I agree to the Software License Agreement** check box.

   The **Download Java Access Bridge for Windows Operating System x.x.x** page opens.
5. In the **Required Files** list, click the link to download the **Access Bridge x.x.x, accessbridge-x.x.x.exe** file.

   The download dialog box opens.
6. Follow the on-screen instructions to save the executable (.exe) installer file to the hard disk drive.
7. When the download is complete, locate the installer file on the hard disk drive and proceed as appropriate:
   - If you downloaded the installer by using the ProtecTIER Manager workstation on which you are installing the JAB, go on to step 8 on page 118.
   - If you downloaded the installer by using a PC other than the applicable ProtecTIER Manager workstation, do the following:
     a. Copy the installer file onto a CD, flash memory drive, or other removable media device.

b. Copy the installer file from the removable media device to the hard disk drive of the ProtecTIER Manager workstation.
c. Go on to step 8.

8. On the ProtecTIER Manager workstation, double-click the **accessbridge-x.x.x.exe** installer file.

   A security warning dialog box displays.

9. Click **Run**.

   The **Java Access Bridge – InstallShield Wizard** opens.

10. Read the welcome information, then click **Next** and follow the on-screen instructions to complete the installation.
11. When the installation is complete, restart the workstation as directed.

    You now have the necessary Java tools for compatibility between the ProtecTIER Manager installation wizard and screen reader software.

12. Follow the instructions in "Using a screen reader to install ProtecTIER Manager" to start the ProtecTIER Manager installation wizard by using a screen reader.

Using a screen reader to install ProtecTIER Manager

About this task

Install ProtecTIER Manager according to the following command line-based instructions.

When entering the commands, type them exactly as shown, including any spaces or quotation marks. Any deviation in the procedure can cause the installation to start in the non-accessible mode, or fail completely.

Procedure

1. If your workstation is configured to automatically open DVDs, temporarily disable the Windows **AutoPlay** feature for the CD/DVD device. Use the Windows Help or other Windows documentation for instructions, and then go on to step 2.
2. Insert the *IBM ProtecTIER Manager DVD* into the CD/DVD drive of the ProtecTIER Manager workstation.
3. Access the command prompt on the ProtecTIER Manager workstation:
   a. Click **Start** > **Run...**.

      The **Run** dialog box opens.

4. In the **Open** field, type: **cmd** and click **Ok**.

   The command window opens.

5. Browse to the ProtecTIER Manager installation directory on the DVD. To do so:
   a. At the command prompt, type: **D:** (where D: is the letter assigned to the CD/DVD drive of the workstation) and press **<enter>**.
   b. At the command prompt, list the contents of the DVD. Type: **dir** and press **<enter>**.
   c. Locate the name of the ProtecTIER Manager directory on the DVD. For example: *PT_Manager_V3.3*.
   d. At the command prompt, change to the **ProtecTIER Manager** directory. Type: **cd <directory name>** and press **<enter>**. For example: `cd PT_Manager_V3.3` **<enter>.**

e. At the command prompt, change to the **Windows** directory. Type: **cd windows** and press **<enter>**.

f. At the command prompt, type: **Install.exe LAX_VM "C:\Program Files\Java60\jre\bin\java.exe"** and press **<enter>**, where the path contained within the quotation marks is the same as the path that you noted in step 5 on page 116.

The screen-reader-enabled ProtecTIER Manager installation wizard starts.

g. Follow the spoken prompts to compete the installation.

6. When the installation completes, proceed as appropriate:
   - If you **do not** want to enable the Windows High Contrast option or customize the color palette, resume your regular use of ProtecTIER Manager.
   - To change the contrast mode for ProtecTIER Manager, go to "Enabling the Windows High Contrast option." To customize the color palette, go to "Customizing the color palette" on page 123.

Enabling the Windows High Contrast option

About this task

To make it possible for ProtecTIER Manager to display in high contrast, you must first enable the **Use High Contrast** option in Windows.

Procedure

1. On the ProtecTIER Manager workstation, go to **Windows** > **Control Panel** > **Accessibility Options**.

   The **Accessibility Options** dialog box opens.

2. Select the **Display** tab.
3. In the **High Contrast** area of the **Display** tab, select the **Use High Contrast** check box, as shown in Figure 61 on page 120:

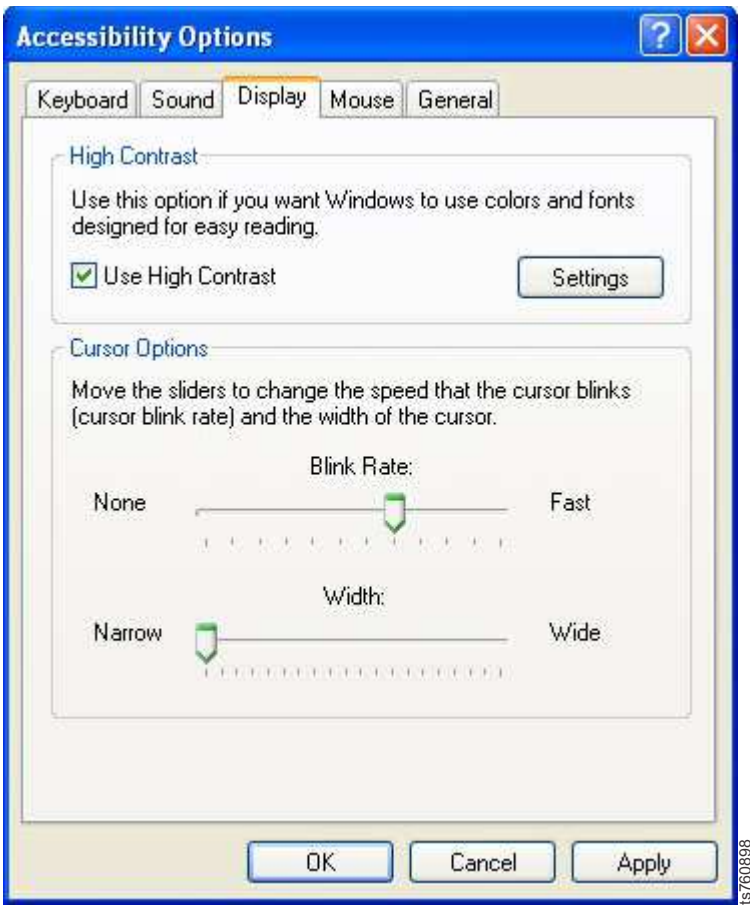


Figure 61. Display tab

4. Click **Settings**.

   The **Settings for High Contrast** dialog box displays, as shown in Figure 62 on page 121:

Figure 62. Settings for High Contrast

By default, the **High Contrast Black (large)** scheme is selected.

5. Do one of the following:
   - To use the default, **High Contrast Black (large)**, scheme:
     a. Click **Ok** to close the **Settings for High Contrast** dialog box.
     b. Click **Ok** to close the **Accessibility Options** dialog box.
        After a few moments, the display changes to the new color scheme.
     c. Go on to "Using the Windows high contrast scheme with ProtecTIER Manager."
   - To use a different high contrast scheme:
     a. Click the arrow to show the list of available color schemes.
     b. Select the high contrast scheme that you want to use.
     c. Click **Ok** to close the **Settings for High Contrast** dialog box.
     d. Click **Ok** to close the **Accessibility Options** dialog box.
        After a few moments, the display changes to the new color scheme.
     e. Go on to "Using the Windows high contrast scheme with ProtecTIER Manager."

Using the Windows high contrast scheme with ProtecTIER Manager

About this task

Now that you have changed the contrast scheme in Windows, you must enable the **Support system settings** option in ProtecTIER Manager.

Procedure

1. Launch **ProtecTIER Manager**:

a. Click: **Start** > **All Programs** > **IBM** > **ProtecTIER Manager** > **IBM ProtecTIER Manager**.

The ProtecTIER Manager window opens, as shown in: Figure 63.

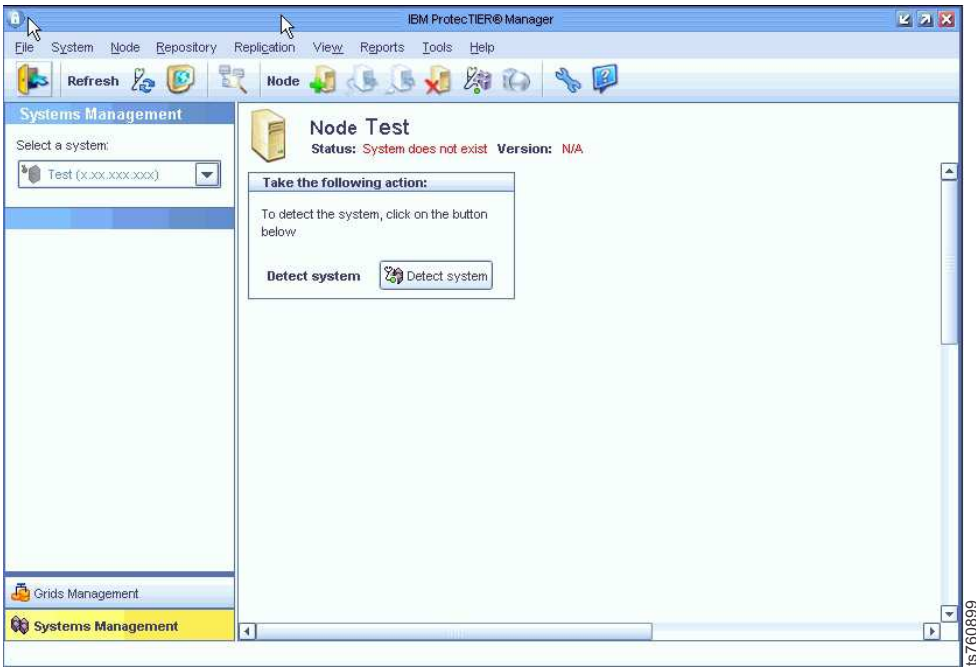


Figure 63. ProtecTIER Manager window

2. On the toolbar, click: **Tools** > **Preferences**.

   The **Preferences** dialog box opens with the **Appearance** tab selected, as shown in Figure 64:

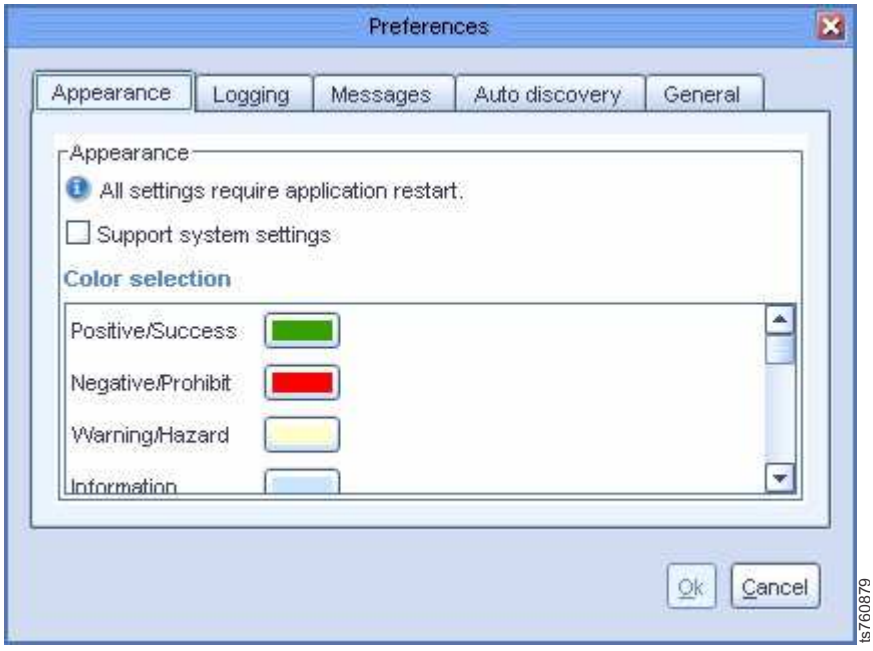


Figure 64. Preferences dialog box

3. On the **Appearance** tab, select the **Support system settings** check box.
   You are returned to the **ProtecTIER Manager** window.
4. Exit and restart ProtecTIER Manager so the contrast settings take effect:
   a. On the **ProtecTIER Manager** toolbar, click: **File** > **Exit**.
      The **ProtecTIER Manager** window closes.
   b. Click: **Start** > **All Programs** > **IBM** > **ProtecTIER Manager** > **IBM ProtecTIER Manager**.
      When the ProtecTIER Manager window opens, the display reflects the contrast change, as shown in: Figure 65.

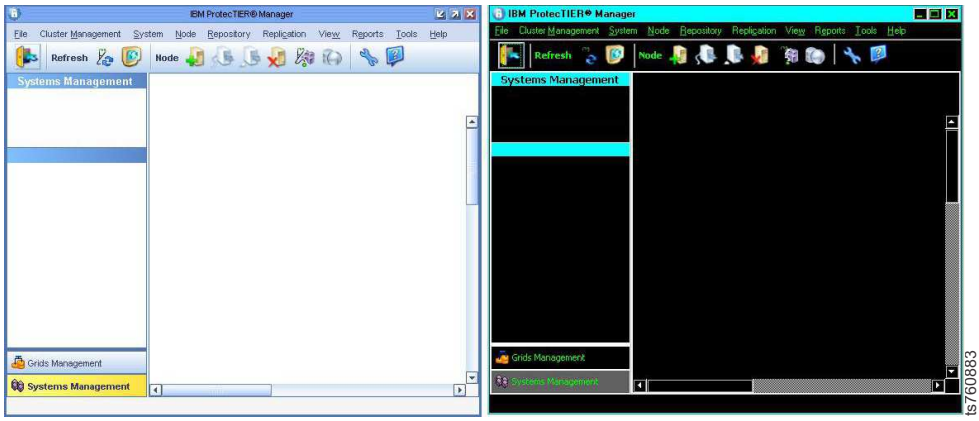


Figure 65. Normal contrast versus high contrast

5. Proceed as appropriate:
   - If you want to change one or more of the colors used in the ProtecTIER Manager display, continue to "Customizing the color palette."
   - If you **do not** want to customize the color palette, resume your regular use of ProtecTIER Manager.

Customizing the color palette

About this task

Use this procedure to customize the color palette for ProtecTIER Manager to improve visibility in the display, or to suit your personal preferences.

Procedure

1. If necessary, start ProtecTIER Manager as described in step 1 on page 121.
2. Open the **Preferences** dialog box, as described in 2 on page 122.
3. Scroll down (if necessary) to see the entire **Color selection** list, and then select the color you want to change.
   The **Color selection** dialog box opens, with the **Swatches** tab selected, as shown in Figure 66 on page 124:

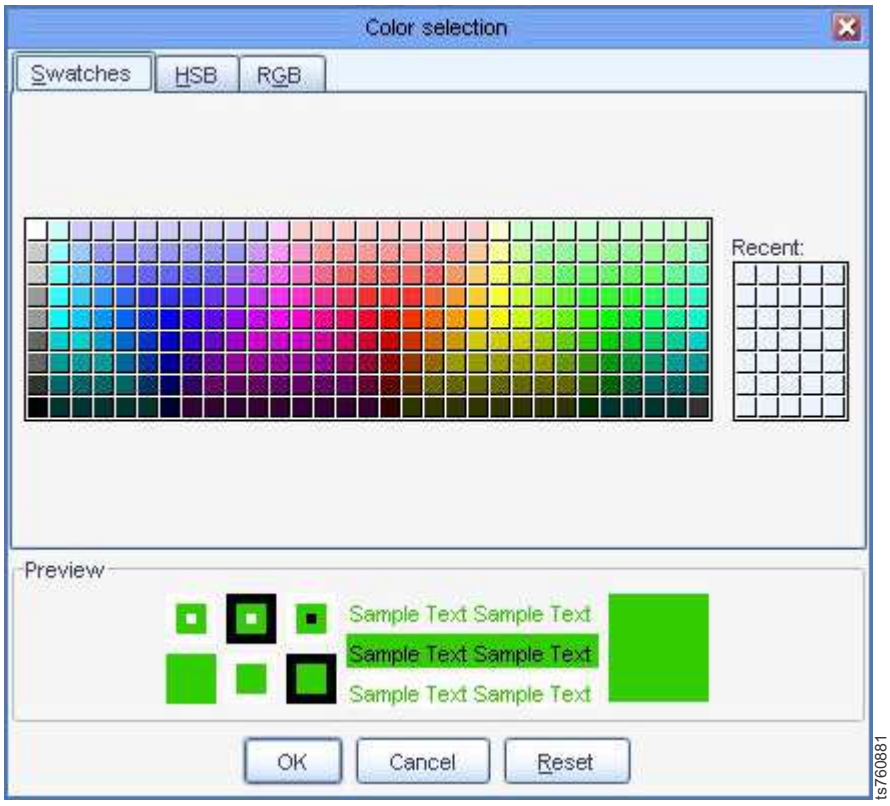


Figure 66. Color selection, Swatches tab

The color that is currently defined for your selection is shown in the **Preview** pane.

4. Select a new color from the color palette.

   You can also specify a new color by using the Hue/Saturation/Brightness (HSB) or Red/Green/Blue (RGB) color models. To do so, click the tab for the model you want to use and enter the required values.

5. When you have finished selecting or specifying the new color, click **Ok**.

   You are returned to the **Appearance** tab.

6. To change another color, repeat steps 3 on page 123 through 5.
7. When you are finished making changes in the **Appearance** tab, click **Ok**.

   You are returned to the ProtecTIER Manager window.

8. Exit and restart ProtecTIER Manager (as described in step 4 on page 123) so the color palette changes take effect.

   After you log in to ProtecTIER Manager and add a node, the display reflects your custom color selections.

   An example of the default color versus a custom color for **Allocable** resources, is shown in: Figure 67 on page 125

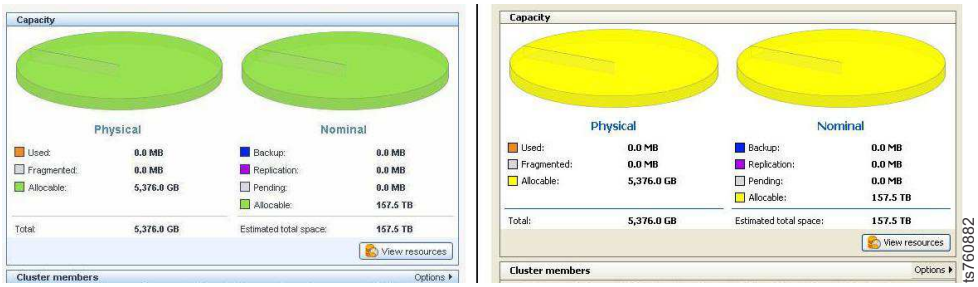


Figure 67. Default color versus custom color

9. Proceed as appropriate. Return to the task from which you were sent to these instructions or resume your regular use of ProtecTIER Manager.

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.

Red Hat Notice

IBM delivers patches (including security fixes) for Red Hat Enterprise Linux (RHEL) based on the Red Hat Enterprise Linux Life Cycle policy. As stated in the Red Hat policy, fixes are not provided for all vulnerabilities on all RHEL versions, which means that IBM cannot deliver security fixes for some RHEL issues.

When security and other related updates are available from Red Hat, IBM delivers those updates in software packages that can be downloaded and applied to ProtecTIER. IBM may also publish Security Bulletins with additional information for security related updates. Customers should subscribe to My Notifications to be notified of important ProtecTIER support alerts.

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.

Red Hat is a registered trademark of Red Hat, Inc. 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 regions.

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
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15 2941
e-mail: lugi@de.ibm.com

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
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372

IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15 2941
e-mail: lugi@de.ibm.com

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 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

jieta1

Korean Electromagnetic Interference (EMI) Statement

This explains the Korean Electromagnetic Interference (EMI) statement.

이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서

가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

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

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

U

V

W

SC27-8902-03