IBM TS7650G Deduplication Gateway for ProtecTIER®
Version 3 Release 4

User's Guide for VTL Systems

IBM

Edition notices

This edition applies to IBM TS7650G Deduplication Gateway for ProtecTIER® 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 information for using the IBM® TS7600 ProtecTIER® Deduplication Solutions, V3.4.

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.

TS7650 Appliance or appliance

> These are terms for IBM's self-contained virtualization solution from the TS7650 family that includes a disk storage repository. The TS7650 Appliance consists of the following:

> **Server** The 3958 AP1 server is based on the IBM System x3850 X5 Type 7145-PBR at the ProtecTIER version 3.4.1 release. When used as a server in the TS7650 Appliance, its machine type and model are 3958 AP1. 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.

> **Disk controller**
> > The disk controller for the TS7650 Appliance is an IBM Feature Code 3708: 4.8 TB Fibre Channel Disk Controller. Use this feature code for service purposes.

> **Disk expansion unit**
> > The disk expansion unit for the TS7650 Appliance is an IBM Feature Code 3707: 4.8 TB Fibre Channel Disk Expansion Unit. Use this feature code for service purposes.

> **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.

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. IBM does support two TS7650 Gateway servers in a single frame (a two-node cluster). The TS7650G consists of the following:

> **Server** There are four types of server that have been used in the Gateway:

> > **3958 DD5**
> > > This is a newer, higher performance server available in May 2012. This server is based on the IBM System x 7143 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 is a higher performance server available in December 2010. This server 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.

3958 DD3

This is a higher performance server available in March 2009. This server is based on the IBM System x3850 M2 Type 7233. When used as a server in the TS7650G, its machine type and model are 3958 DD3. Use this machine type and model for service purposes.

3958 DD1

This is the original server available in August 2008. This server is based on the IBM System x3850 M2 Type 7141. When used as a server in the TS7650G, its machine type and model are 3958 DD1. 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.

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.

OpenStorage

OpenStorage allows ProtecTIER to be integrated with NetBackup to provide the means for backup-to-disk without using a virtual tape library (VTL) emulation. Using a plug-in that is installed on an OpenStorage-enabled media server, ProtecTIER can implement a communication protocol that supports data transfer and control between the backup server and the ProtecTIER server. Therefore, to support the plug-in, ProtecTIER implements a storage server emulation.

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 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 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.

ACL – Access Control List
A list of permissions attached to an object (file, directory, etc). An ACL specifies which users are allowed to access an object and which operations are allowed on the object.

AD – Windows Active Directory
Windows-based software that manages user and group authentication and authorization between multiple servers.

Authentication
The process of presenting credentials (username/password) to a service and having that service validate you.

Authorization
The process of granting access to resources on a server that is in the network.

CIFS – Common Internet File System
The Microsoft file sharing protocol that supports remote mounts over TCP/IP using the SAMBA server message block (SMB) protocol.

DNS – Domain name server
Used to lookup and translate host names and IP addresses.

FSI – File System Interface
This refers to the overall ProtecTIER File System Interface implementation. When used in this document without any qualifiers it will refer to the initial release supporting the CIFS interface.

Kerberos
A computer network authentication protocol that allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner. When used in this document this term will generally refer to the authentication protocol.

NAS - Network attached storage
Storage that may be accessed over IP networks using a variety of different protocols such as CIFS, NFS, and HTTP.

NFS - Networked File system
A file sharing protocol that supports remote mounts over TCP/IP.

Samba
An open source package that provides a CIFS interface on a Linux server. When used in this document this term will generally refer to the CIFS interface.

Stream
Once a connection has been established, the data flowing between a file within the CIFS exported filesystem and a Windows (host) application is referred to as a stream. Both a connection and a file can support multiple streams according to the ProtecTIER FSI implementation.

User file system
Pertaining to the ProtecTIER file system created by the user and presented as a CIFS share.

Who should read this document

This publication is intended for storage administrators, system programmers, and performance capacity analysts.

Getting information, help, and service

IBM provides several options for obtaining help, service, and information about the TS7600 ProtecTIER Deduplication Solutions, V3.4.

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

Information

IBM maintains pages on the World Wide Web that contain information about its products and services.

IBM maintains pages on the World Wide Web where you can get information about IBM products and services and find the latest technical information. For more information refer to Table 1.

Table 1. IBM Web sites for help, services, and information

Description	Web address (URL)
IBM home page	http://www.ibm.com
Directory of worldwide contacts	http://www.ibm.com/planetwide

Table 1. IBM Web sites for help, services, and information (continued)

Description	Web address (URL)
Support for IBM System Storage® and TotalStorage products	http://www.ibm.com/support The **IBM Support Portal** page displays. Do the following: 1. In the **Product Lookup** field, begin typing TS76. As you type, a list of matching products drops down below the input field. 2. Select your product from the drop down list. The product you select appears below the Search field in the **Search supports and downloads** section. Items specific to the product you selected appear in the five areas below the Search field. You can search for specific information, or select one of the links in the **Downloads, Product support content, Tools and resources, Featured links,** or **Common support links**. 3. To view a list of available fixes for your product, for example, click on → Downloads (drivers, firmware, PTFs). Alternatively, you can use the **Browse for a product** link. 1. Click **Browse for a product**. 2. Expand ► System Storage. 3. Expand ► Tape systems. 4. Expand ► Tape virtualization. The page shows a list of products. 5. Select your product from the list. The product you select appears below the Search field in the **Search supports and downloads** section.

Help and service

When you call for service, you must provide certain identifying information.

You can call 1 (800) IBM SERV (1-800-426-7378) 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.

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 customer number is a seven-digit numeric (0000000

- 9999999) assigned by IBM when the PID is purchased. It is located on the customer information worksheet or on the invoice from the software purchase.

Note: If asked for an operating system, say "Storage".

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

Note: Cache modules and cache controllers are supported separately within the TS7650G. If the problem is in the IBM attached storage component, select the hardware option. Enter the appropriate Machine Type and S/N (serial number) for the component. If the attached storage is not IBM branded, contact the appropriate service provider for the component.

Web sites

The most up-to-date information about your product, including documentation and the most recent downloads, can be found at the following Web sites:

- The translated publications for this product are included with the product. These documents and product specification sheets are also available from the following Web site:

  www.ibm.com/storage/support/

- You can order publications through the IBM Publications Ordering System at the following Web site:

  www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss/

- Access the IBM System Storage ProtecTIER TS7650 Customer Information Center at:

  http://publib.boulder.ibm.com/infocenter/ts7650/cust/index.jsp

- Access installation and technical support information via the Web at:

  www.ibm.com/support

- The IBM Web site for Independent Software Vendor (ISV) support is:

  www.ibm.com/servers/storage/tape/resource-library.html

- The IBM System Storage TS7600 Interoperability Matrix Web site can be found at:

  http://www-03.ibm.com/systems/support/storage/ssic/interoperability.wss

- For the latest information about SAN switches and directors, go to the following Web site:

  www.ibm.com/servers/storage/san

- For the latest information about IBM xSeries products, services, and support, go to the following Web site:

  www.ibm.com/eserver/xseries

- For the latest information about operating system and HBA support, clustering support, SAN fabric support, and Storage Manager feature support, see the DS4000® Interoperability Matrix at the following Web site:

  www.ibm.com/servers/storage/disk/ds4000/interop-matrix.html

- For product firmware and software downloads, as well as associated driver code, go to the following Web site:

www.ibm.com/storage/support/

- For accessibility information, go to the following Web site:

  www.ibm.com/able/product_accessibility/index.html

- For the latest information about product recycling programs, go to the following Web site:

  www.ibm.com/ibm/environment/products/prp.shtml

Related IBM publications

The following documents provide information about the IBM System Storage TS7600 with ProtecTIER gateway and appliance server(s) and recommended additional hardware components.

TS7650G Server (x3958 DD4/DD5/DD6) publications

The following publications provide additional documentation about the TS7650G Server:

- *IBM System x3850 M2 (Type 7141, 7144), System x3950 M2 (Type 7141) User's Guide*
- *IBM Safety Information*

The server might have features that are not described in the documentation that you received with the server. The documentation might be updated occasionally to include information about those features, or technical updates might be available to provide additional information that is not included in the server documentation. These updates are available from the IBM Web site. Complete the following steps to check for updated documentation and technical updates:

1. In a Web browser, navigate to http://www.ibm.com/support/publications/us/library/.
2. Click **Information Centers > Systems > xSeries>**.
3. Click **Product information > Servers > xSeries**.
4. From the **Product family** list, select **System x3850**.
5. From the **Type** list, select **System 7141**.
6. Click **Go**.
7. On the Software and device drivers page, click the Documentation link.
8. On the Support for System x3850 page, click the link for the document you want to view.

Integrated Management Module (IMM) publications

The following publications provide additional documentation about the IMM:

- *Integrated Management Module 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 e-mail 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

Part 1. Preparing to work with ProtecTIER

This section of the guide describes the steps for completing the ProtecTIER system setup for new installations and upgrading ProtecTIER servers.

In addition, this part describes how to install and configure the ProtecTIER Manager software and how to manage repositories.

Chapter 1. Introduction

The TS7600 ProtecTIER Deduplication Solutions, V3.4 are advanced disk-based storage systems.

ProtecTIER is a disk-based data storage system. It uses data deduplication technology to store data to disk arrays. The ProtecTIER VTL service emulates traditional automated tape libraries.

Before you use ProtecTIER and this document, ensure that you complete the planning, preparation, and installation tasks. These tasks are described in the *IBM TS7650G ProtecTIER Deduplication Gateway Installation Roadmap Guide*, V3.3.6.1, GA32-0921 publication.

HyperFactor

This topic describes IBM data factoring technology, known as HyperFactor®.

ProtecTIER is the first virtual tape product to contain patented data deduplication technology that IBM calls HyperFactor. This technology detects recurring data in multiple backups. The common data is merged into a single instance store, saving disk space needed to store multiple backups without sacrificing performance or the availability of backups.

HyperFactor is a breakthrough on several fronts:
- It is scalable up to 1024 TB.
- The algorithm used to find the common data between backups does not affect the backup performance of the virtual tape engine.
- Data integrity is not compromised, not even statistically.
- Merged data is stored in a format that preserves restore performance.

HyperFactor saves space by taking advantage of the fact that only a small percentage of data actually changes from backup to backup. Incremental backups include all files with modification dates that have changed since the last full or incremental backup. Full backups store all the data, changed or not.

The amount of space saved depends on many factors, mostly of the backup policies and retention periods and the variance of the data between them. The more full backups retained on ProtecTIER, and the more intervening incremental backups, the more overall space saved.

ProtecTIER Virtual Tape

The ProtecTIER Virtual Tape service acts like a traditional tape drive.

The ProtecTIER Virtual Tape (VT) service emulates traditional tape libraries. Because ProtecTIER VT emulates tape libraries, you can 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 stores data on a deduplicated disk repository on the storage fabric.
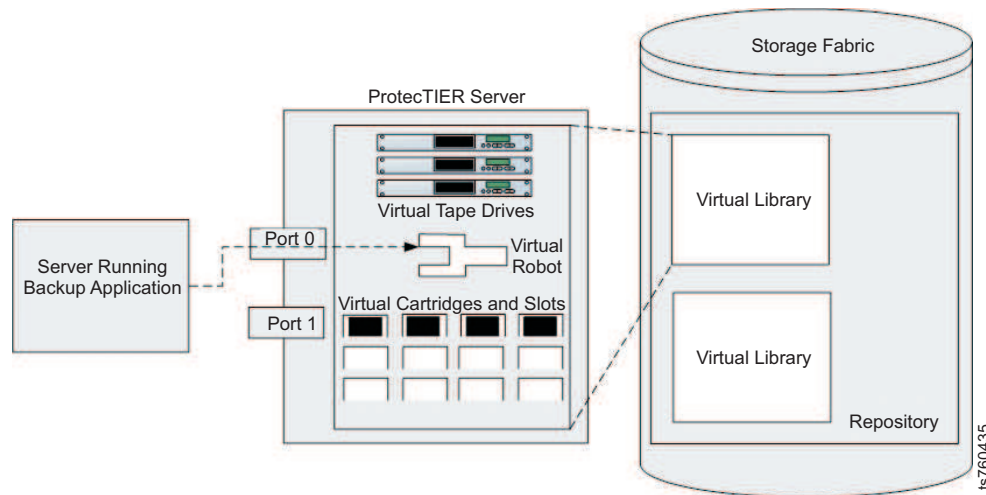
Figure 1. Tape library emulation

ProtecTIER File System Interface (FSI)

This topic provides an overview of the ProtecTIER File System Interface (FSI).

With FSI, ProtecTIER emulates a network attached storage (NAS) backup target capable of using HyperFactor, as well as ProtecTIER Native Replication bandwidth reduction techniques for storing and replicating deduplicated data. ProtecTIER FSI enables backup servers running backup applications to connect over IP networks to ProtecTIER, without the use of FC connectivity and allows customers to use their existing tools and capabilities to integrate a ProtecTIER NAS-based backup target into your environment.

ProtecTIER Manager

This topic provides an overview of the ProtecTIER Manager software.

The ProtecTIER Manager application can be installed on one or more workstations, enabling you to monitor the status of nodes and clusters in your ProtecTIER system along with the accompanying repositories and services. ProtecTIER Manager is used to initially configure your ProtecTIER system and to change the configuration.

Configuration

This topic provides an overview of ProtecTIER system configuration.

ProtecTIER systems can be set up with either one node or two nodes arranged in a cluster. Each cluster operates independently, but you can manage them all from ProtecTIER Manager.

Note: FSI only supports one node configurations, therefore cluster configurations are only available in a VTL system set up.
Attention: To meet electromagnetic immunity requirements, shielded Ethernet cables are required when attaching to a 1 GbE PCIe Ethernet adapter card.

A one node system uses one server to transfer data from the backup server to the storage fabric, as illustrated in the following figure:

Backup Servers
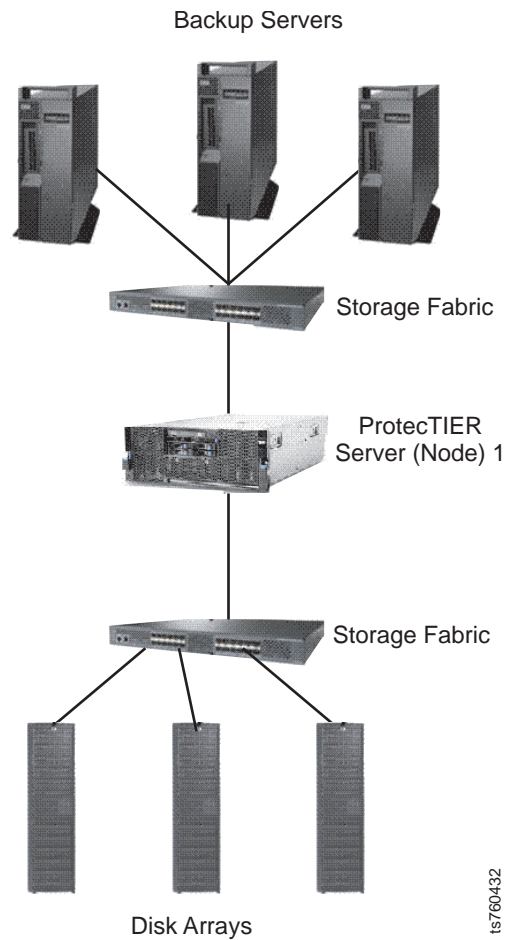
Figure 2. One node system

A two node system uses two servers in an active-active cluster and enables you to build a more sophisticated system, as illustrated in the following figure:
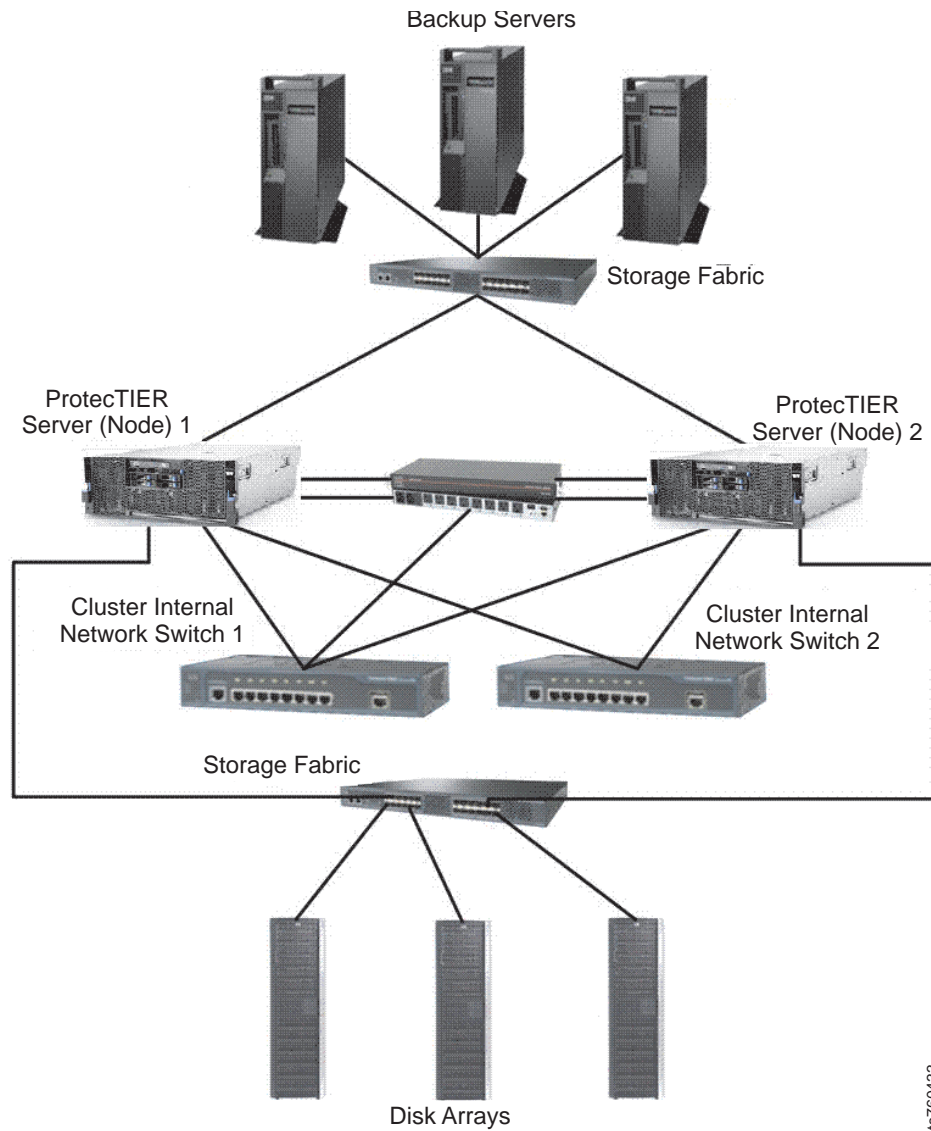
Figure 3. Two node system

Using a two node system provides the following benefits:

- **Higher-Availability** clustered configuration available to provide hardware redundancy in the event of a node failure.
- **Increased Performance** if there are sufficient disk resources, the two servers can share the backup load, and increase the performance of ProtecTIER.

The following diagram illustrates the details of the ProtecTIER cluster setup:
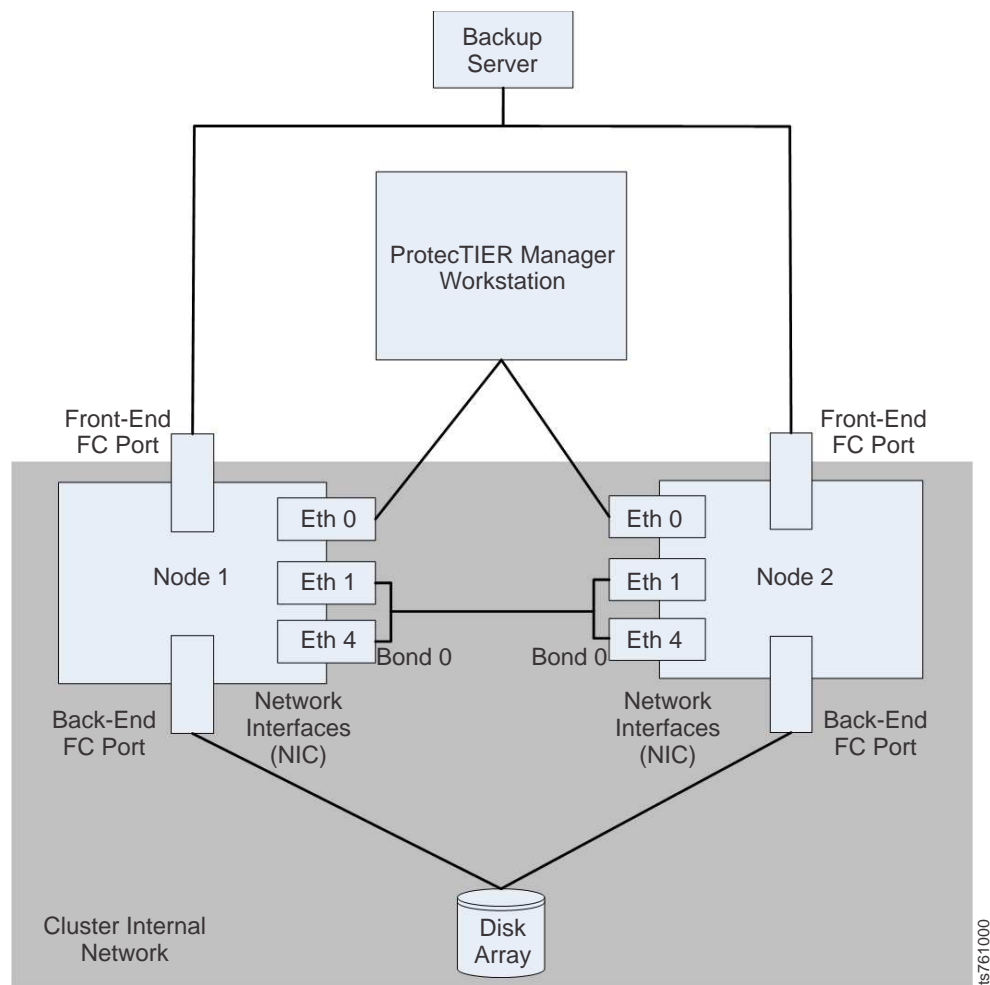
Figure 4. Cluster setup

Each node connects through front-end Fibre Channel ports to the backup server, and through back-end Fibre Channel ports to disk arrays. The network interface cards enable the nodes to connect to each other and to the ProtecTIER Manager workstation.

Native replication

Native replication lets you replicate between repositories connected to a wide area network (WAN) with TCP/IP protocol.

Replication enables you to set rules (depending on your required replication needs) for replicating data objects across ProtecTIER repositories. The ProtecTIER repositories can be different in size as well as physical layout. Since ProtecTIER deduplicates data before storing it, only the changes are transferred to the remote site. You define the rules for replicating data objects in replication policies on a repository.

A replication grid is a logical set of repositories that can replicate from one to the other. The ProtecTIER Replication Manager is a server that remotely manages the configuration of the grid (for example, grid creation or deletion, repository membership in the grid, and so on). In most cases, the ProtecTIER Replication Manager resides on one of the ProtecTIER nodes.

Before defining replication policies, however, you must first create connections between the repositories. To create connections, you define replication groups. Depending on your environment, you create replication groups in either "many-to-one" or "many-to-many" topologies.

In a "many-to-one" topology, you create replication groups in which source repositories can receive local backups and replicate to a single destination. The destination repository can then act as a Disaster Recovery site for any number of the source repositories, and still allow local backups, as well as replication, from the active source repositories.

In a "many-to-many" topology, you create replication groups where multiple repositories can replicate to each other. You can define a many-to-many replication group where each repository assumes the responsibility of a destination repository and can receive local backups, replicate data to remote repositories, and receive replicated data from remote repositories.

Chapter 2. Completing the ProtecTIER system setup for new installations

This chapter details the prerequisites for completing the ProtecTIER system setup for new installations. Configuring the node is described in the *IBM TS7650G ProtecTIER Deduplication Gateway Installation Roadmap Guide*, V3.3.6.1, GA32-0921.

If you are upgrading the ProtecTIER system, refer to the *IBM TS7650 ProtecTIER Software Upgrade Guide*, V3.3.6.1, SC27-3643.

Use the ProtecTIER Service menu to complete the ProtecTIER configuration process that was started in manufacturing. If you are working on a TS7650G, some or all of these configurations may have already been done during the node configuration.

Note: Throughout this chapter the terms server and node are used interchangeably, depending upon the task being performed.

Accessing the ProtecTIER Service menu

Complete this task to access the ProtecTIER Service menu.

Procedure

1. If you are in a single node configuration, connect the USB keyboard and graphics-capable monitor to the server.
2. Verify that the server is running:
3. At the localhost **Login** prompt, type `ptconfig` and press Enter.
4. At the **Password** prompt, type `ptconfig` and press Enter.

    The **ProtecTIER Service Menu** opens:

    ```
    --------------------------------------------------------------------------
      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?
    ```

5. Go on to "Customizing the ProtecTIER server"

Customizing the ProtecTIER server

Complete this task to customize the ProtecTIER server.

About this task

Perform the following steps to configure the server by using the ProtecTIER Service menu:

Procedure

1. On the server, if it is not already displayed, access the ProtecTIER Service menu. See "Accessing the ProtecTIER Service menu" on page 9.

2. Select the **ProtecTIER Configuration (...)** option. Type the corresponding number and press Enter. The **ProtecTIER Configuration (...)** menu appears.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
           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
 14) OS images Management (...)
 15) Replace SAS drive
  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

3. Select the **IP Network configuration (...)** option. Type the corresponding number and press Enter. The **IP Network configuration (...)** menu appears.

```
------------------------------------------------------------------------
  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 cluster Ethernet switches

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

4. Select the option **Configure ProtecTIER's IP interfaces** to configure external. Type the corresponding number and press Enter.

   The following status messages appear:

   ```
   Starting Cluster, please wait
   Starting cluster [ Done ]
   Cluster Started
   ```

   If asked if you would like to stop the vtfd service, type yes and press Enter.

   The following status message displays as the system initiates shutdown:

   ```
   Stopping VTFD [/]
   The shutdown process may take a few minutes to complete.
   ```

   When shutdown completes, the following status message appears:

```
Stopping RAS [ Done ]
Stopping VTFD [ Done ]
```

5. Change the server IP address, netmask, default gateway, and host name factory-set values, to the values specific to the customer environment.

   a. You are prompted, one at a time to enter the following values. At each prompt, type the new value and then press <Enter>:

      • Customer Network IP address

      • Customer Network netmask

      • Customer Network default gateway

      • Customer Network hostname (The fully qualified hostname of the server. For example: `hostname.domain.com`)

   After you enter the hostname, the system automatically starts the network configuration process. The following status messages display:

   ```
   Configuring network [ Done ]
   Updated network configuration successfully
   update updateNetwork ended successfully
   ```

   The system automatically restarts the vtfd service, and you are returned to the command prompt.

6. Change the system name from the one assigned during manufacturing to one specific to the customer environment. In a clustered configuration, run the command from only one of the nodes as it affects the shared name of the system. To do so:

   a. From the **ProtecTIER Configuration (...)** menu, select the **Update System Name** option. Type the number of your choice and press Enter.

   The following status messages appear:

   ```
   Starting Cluster, please wait
   Starting Cluster [ Done ]
   Cluster Started
   Please enter a new system name:
   ```

   b. When prompted, type the new system name of the server and press Enter.

   Note: The system name that was assigned to the server in manufacturing appears in brackets after the prompt. For example: [PORTLAND]. After you enter the system name, the system automatically starts the **Update the System Name** process. The following status message appears:

   ```
   Changing system name [ Done ]
   Updated system name successfully
   UpdateSystemName ended successfully

   End Processing Procedure Successfully
   ```

   Press Enter to continue and return to the command prompt.

7. If you are in a clustered configuration, repeat the steps in these steps on Server B. When you are finished, go on to Chapter 4, "Installing ProtecTIER Manager," on page 29.

Configuring static routes

Complete this task to configure the static routes for replication.

About this task

In this task you will provide information about your source server(s) and the target server(s), in order to define the static routes.

For assistance with this task, refer to the information on your completed **Configure Static Route for Replication** worksheet(s).

Run this procedure on the source server(s) to configure the addresses of all the destination systems and the node on which the ProtecTIER Replication Manager is activated. On the destination server(s), run this procedure to configure the addresses of the source system(s).

On the ProtecTIER Replication Manager node, all the systems (source and destination) must be configured.

Procedure

1. Access the ProtecTIER Configuration Menu. See "Accessing the ProtecTIER Service menu" on page 9.
2. From the ProtecTIER Service Menu, select **ProtecTIER Configuration (...)**. Type the corresponding number and press Enter. The **ProtecTIER Configuration (...)** menu is displayed.

```
     -------------------------------------------------------------------------------
       ProtecTIER Service Menu running on rassmx
                 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
        15) OS images Management (...)

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

3. Select **Configure replication (...)**. Type the corresponding number and press Enter. The **Configure replication (...)** menu is displayed.

```
     -----------------------------------------------------------------------
       ProtecTIER Service Menu running on rasddx
                 ProtecTIER Configuration (...)
                 Configure Replication (...)
     -----------------------------------------------------------------------
         1) Config/Unconfig ProtecTIER Replication Manager on this node
         2) Configure Static Routes

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

4. Select **Configure Static routes**. Type the corresponding number and press Enter.

   The message: `Gathering System information [Done]` displays, followed by a summary of the information that was retrieved for the server on which you are currently working. For example:

ID	Target Network Address	Target Netmask	Local Gateway Address
1	10.11.195.0	255.255.255.0	10.11.195.1
2	10.11.197.0	255.255.255.0	10.11.197.1

Following the summary, the **Available Options** prompt displays:

```
Available Options:
==================
(a)dd a new record
(e)dit a record
(d)elete a record
(c)ommit changes
(q)uit
Please Choose (a,e,d,c,q):
```

5. Select **(a)dd a new record**. Type **a** and press Enter.

   You are prompted to enter information for the first destination (target) server and the local network.

6. At each prompt, type the requested information and then press Enter:

   ```
   Please provide the following information:
   ```

   ```
   Target Network Address:
   ```
   This is the starting network address of the Target (Hub) server. For example: *10.11.194.0*.

   ```
   Target Netmask:
   ```
   This is the network netmask address of the Target (Hub) server. For example: *255.255.255.0*.

   ```
   Local Gateway Address:
   ```
   This is the gateway IP address of the local server you are currently working on. For example: *10.11.195.1*.

   A summary of the information you provided, displays. For example:

ID	Target Network Address	Target Netmask	Local Gateway Address
1	10.11.194.0	255.255.255.0	10.11.195.1

   Note: The addresses in the above summary are examples. Your actual values will vary.

   The Available Options prompt displays a second time:

   ```
   Available Options:
   ==================
   (a)dd a new record
   (e)dit a record
   (d)elete a record
   (c)ommit changes
   (q)uit
   Please Choose (a,e,d,c,q):
   ```

7. Type **a** and press Enter.

You are prompted for the information for the second destination (target - ETH2) server and the local network.

8. At each prompt, type the requested information and then press Enter:

    `Please provide the following information:`

    `Target Network Address:`
    This is the starting network address of the Target (Hub) server. For example: *10.11.196.0*.

    `Target Netmask:`
    This is the network netmask address of the Target (Hub) server. For example: *255.255.255.0*.

    `Local Gateway Address:`
    This is the gateway IP address of the local server you are currently working on. For example: *10.11.197.1*

    An updated summary displays:

ID	Target Network Address	Target Netmask	Local Gateway Address
1	10.11.194.0	255.255.255.0	10.11.195.1
2	10.11.196.0	255.255.255.0	10.11.197.1

   Note: The addresses in the above summary are examples. Your actual values will vary.

   The Available Options prompt displays a third time:

    `Available Options:`

    `==================`

    `(a)dd a new record`

    `(e)dit a record`

    `(d)elete a record`

    `(c)ommit changes`

    `(q)uit`

    `Please Choose (a,e,d,c,q):`

9. Type: **q <enter>**

   The `Would you like to commit the changes performed to the routing table now? (yes|no)` message, displays.

10. Type **yes** and press Enter.

    The `Successfully committed changes!` message displays.

11. Press Enter to return to the **ProtecTIER Configuration Menu**.

12. Quit the menu to exit. Type **q** and press Enter. You are returned to the **login** prompt.

13. Configuration for one source server and the destination server, is now complete. Confirm that your replication configuration was successful. To do so, refer to the instructions in Chapter 10, "Native Replication Management," on page 115.

Setting the timezone

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

Procedure

1. On the **ProtecTIER Configuration (...)** menu (see "Setting the timezone" on page 14), select the **Update Time, Date, Timezone & Timeserver(s)** option. Type the corresponding number for this selection and press Enter.

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

```
 -------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
          Date, Time, Timezone & Timeserver(s) configuration
 -------------------------------------------------------------------------------
   1. Set date & time
   2. Set Timezone
   3. Set Timeserver(s)

   c. Commit changes and exit
   q. Exit without committing changes
 -------------------------------------------------------------------------------
 >>> Please Choose:
```

Figure 5. Date, Time, Timezone & Timeserver(s) configuration menu

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

2. Select the **Set Timezone** option. Type the corresponding number and press Enter.

3. If you are in the United States, when prompted for a country code, type: US and press Enter.

   For locations outside the United States, you must enter an international country code. Refer to Appendix C, "Worldwide time zone codes," on page 261 to locate your information, then return to this task and enter the appropriate country code in step "Setting the timezone" on page 14.

   The time zones for the specified country display. A sample of the US time zones list is shown in "Setting the timezone" on page 14:

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

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

Press <Enter>

27. Pacific/Honolulu

Please choose a timezone:
```

Figure 6. Sample of US time zones

4. If the `Press enter to continue` prompt displays, the time zone list is too long to display on the screen at once. Press Enter to advance the list.

5. At the `Please choose a timezone:` prompt, type the number that corresponds to your timezone and press Enter to return to the **Date, Time, Timezone & Timeserver(s) configuration** menu. Type: c for commit and press Enter.

   The current time, date, and timezone settings display for review.

6. At the `Do you wish to apply those settings? (yes|no)` prompt, type: yes and press Enter.

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

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

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

Setting the date and time

Each server contains a battery that must be calibrated.

About this task

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

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

Procedure

1. On the **ProtecTIER Configuration (...)** menu (see "Setting the date and time" on page 16), select the **Update Time, Date, Timezone & Timeserver(s)** option. Type the corresponding number for this selection and press Enter.

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

2. On the **Date, Time, Timezone & Timeserver(s) configuration** menu (see "Setting the date and time" on page 16), select the **Set date & time** option. Type the corresponding number and press Enter.

3. When prompted for the date:
   - If the default date [displayed in brackets] is correct, press Enter.
   - If the default date is incorrect, type the current date in DD/MM/YYYY format and press Enter. For example, 09/01/2012.

4. When prompted for the time:
   - If the default time [displayed in brackets] is correct, press Enter.
   - If the default time is incorrect, type the current time in HH:MM:SS format and press Enter. For example:08:32:58.

5. At the Please choose: prompt, commit your date and time settings To commit, type: c and press Enter.

   The current time, date, and timezone settings display for review.

6. At the Do you wish to apply those settings? (yes|no) prompt, type: yes and press Enter.

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

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

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

ProtecTIER Replication Network Performance Validation Utility for VTL Systems

The VTL **pt_net_perf_util** utility's objective is to test maximal replication performance between two future ProtecTIER VTL repositories by emulating the network usage patterns of ProtecTIER's Native Replication component. This utility will not predict replication performance, but it may discover performance bottlenecks.

Before you begin

The requirements of this utility are as follows:
- Red Hat Enterprise Linux 5.4
- Standard external utilities expected to be in the current path: ping, netstat, getopt, echo.

The **pt_net_perf_util** utility and the iperf tool it uses are installed as part of the ProtecTIER software installation. To test the replication performance, use the following tool:

- iperf 2.0.4

  ```
  /usr/local/bin/iperf
  ```

This utility has two modes of operation, client and server. The server has to be started before the client. Before running the utility, shut down all other programs on both the client and server ProtecTIER systems. The **client** is the ProtecTIER system that transmits the test data and the **server** is the ProtecTIER system that receives the data (also known as the **target** server). Based on the data sent by the client and received by the server, the script outputs key network parameter values which indicate certain attributes of the network. The goal of these tests is to benchmark the throughput of the network. The most important benchmark is the direction that replication will actually take place, i.e. the target should be tested as the server since the flow of data will be **to** that server from the client. However, it is also important to also test the reverse direction to measure the bandwidth performance during disaster recovery failback. Network bandwidth is not always the same in both directions.

About this task

In the following procedure, the goal is to test network performance between two machines on a WAN, **server1** and **server2**. Each test will run for five minutes. Since there are five tests, the process will take a total of 25 minutes.

Procedure

1. Start the server mode of the utility on **server1** by entering the following commands on the command line:

   ```
   cd /opt/dtc/app/sbin
   ./pt_net_perf_util -s
   ```

2. Start the client mode of the utility on **server2** by entering the following command on the command line:

   ```
   ./pt_net_perf_util -c server1 -t 300
   ```

3. The utility will automatically perform the tests in sequence. The **client** output (**server2** in the example below) will look similar to the following:

   Note: In the sample output below the test ran for only 5 seconds instead of 300.

   ```
   *** Latency
   PING 9.5.53.33 (9.5.53.33) 56(84) bytes of data.

   --- 9.5.53.33 ping statistics ---
   5 packets transmitted, 5 received, 0% packet loss, time 4001ms
   rtt min/avg/max/mdev = 0.257/0.406/0.484/0.079 ms

   *** Throughput - Default TCP
   [  3]  0.0- 5.0 sec  56.6 MBytes  94.8 Mbits/sec

   *** Throughput - 1 TCP stream(s), 1MB send buffer
   [  3]  0.0- 5.0 sec  57.0 MBytes  95.0 Mbits/sec

   *** Throughput - 16 TCP stream(s), 1MB send buffer
   [SUM]  0.0- 5.8 sec  65.0 MBytes  94.3 Mbits/sec

   *** Throughput - 127 TCP stream(s), 1MB send buffer
   [SUM]  0.0-11.3 sec    127 MBytes  94.1 Mbits/sec
   ```

```
Number of TCP segments sent: 230536
Number of TCP retransmissions detected: 21 (0%)

Done.
```

See the next section for information about interpreting the results of the tests.

Interpreting the results

The utility performs five foreground tests (Tests 1-5 below), and one background
test (Test 6 below). The example outputs below are from the client side. Each of the
first five tests below ran for 300 seconds (-t 300), while the last test monitored TCP
performance during that time.

Test 1: Latency

This test checks the nominal network link latency and packet loss. Example result:
```
*** Latency
PING 10.0.13.194 (10.0.13.194) 56(84) bytes of data.

--- 10.0.13.194 ping statistics ---
120 packets transmitted, 120 received, 0% packet loss, time 119060ms
rtt min/avg/max/mdev = 57.403/78.491/104.451/9.872 ms
```

Interpreting the results:
- The average round-trip-time (rtt) was 78.4ms and there was 0% packet loss.
- The latency in WAN topologies may vary, but should never exceed 200ms.
  Contact your network administrator if latency reports more than 200ms, as it
  may significantly decrease replication throughput.
- Higher latency values will cause a major deterioration in replication throughput.
- Packet loss should be 0%. Any other value indicates a major network problem.

Test 2: Throughput - default settings

This test checks maximal TCP throughput using a single data stream with default
TCP settings. Example result:
```
*** Throughput - Default TCP
[ 3]  0.0-120.1 sec  2.41 GBytes    173 Mbits/sec
```

Interpreting the results:
- The test ran for 120.1 seconds, transferred 2.41 GB (2.24 GiB), with an average
  throughput of 173 Mbits/sec.

  Note: 1 MByte = 1,048,576 bytes. **1 Mbit/sec** = 1,000,000 bits/sec.

Test 3: Throughput - single stream, 1MB send buffer

This test checks maximal TCP throughput using a single data stream with a 1MB
(0.95 MiB) send buffer. Example result:
```
  *** Throughput - 1 TCP stream(s), 1MB send buffer
[ 3]  0.0-120.0 sec  2.51 GBytes    180 Mbits/sec
```

Interpreting the results:
- The test ran for 120.0 seconds, transferred 2.51 GB (2.34 GiB), with an average
  throughput of 180 Mbits/sec.

- There may be an improvement here on high-latency links.

Test 4: Throughput - 16 streams, 1MB send buffer

Example result:

```
*** Throughput - 16 TCP stream(s), 1MB send buffer
[SUM]  0.0-121.4 sec  5.91 GBytes    418 Mbits/sec
```

Interpreting the results:
- The test ran for 121.4 seconds, transferred 5.91 GB (5.5 GiB), with an average throughput of 418 Mbits/sec.
- The extra streams yielded higher utilization of the connection.
- The Mbits/sec reported in this test is the maximum replication performance your system will achieve if your backup environment is using up to 2-3 cartridges in parallel.

Test 5: Throughput - 127 streams, 1MB send buffer

Example result:

```
*** Throughput - 127 TCP stream(s), 1MB send buffer
[SUM]  0.0-126.1 sec  8.08 GBytes    550 Mbits/sec
```

Interpreting the results:
- The test ran for 126.1 seconds, transferred 8.08 GB (7.53 Gb), with an average throughput of 550 Mbits/sec.
- TCP takes a while to reach its maximal throughput. Longer testing times, 300 seconds or more, will produce more accurate results.
- The throughput value given by this test is the potential physical replication throughput for this system. It is directly affected by the available bandwidth, latency, packet loss and retransmission rate.
- The Mbits/sec reported in this test is the maximum replication performance your system may achieve. If this number is lower than anticipated, contact your network administrator.

Test 6: TCP Retransmissions vs. Total TCP segments sent

Example result:

```
Number of TCP segments sent: 1619061
Number of TCP retransmissions detected: 201038 (12%)
```

Interpreting the results:
- A total of 1619061 TCP segments were sent during the five tests, out of which, 201038 were lost and retransmitted.
- The retransmission rate imposes a direct penalty on the throughput, as the retransmission of these packets take up bandwidth. The retransmission can be caused by the underlying network (e.g. packet dropping by an overflowed router) or by the TCP layer itself (e.g. retransmission due to packet reordering).
- Segment loss can be caused by each of the network layers.
- TCP retransmission larger than 2% may cause performance degradation and unstable network connectivity. Contact your network administrator to resolve this issue and reduce it to approximately 0%.

What to do next

You may want to run these tests again to test the reverse throughput in the network. To run the tests in reverse, change **server1** to the client and **server2** to the server and repeat the procedures.

ProtecTIER Network Performance Validation Utility for OpenStorage Systems

The OpenStorage **pt_net_perf_util** utility's objective is to test network performance between an OpenStorage host and a ProtecTIER server. This utility will not predict backup and restore performance, but it may discover performance bottlenecks.

Before you begin

The requirements of this utility are as follows:
- Red Hat Enterprise Linux 5.4 or any other platform officially supported by the OpenStorage plug-in
- Standard external utilities expected to be in the current path such as ping and netstat

About this task

The **pt_net_perf_util** utility and the **iperf** tool it uses are installed as part of the ProtecTIER software installation. The location of the utility varies according to the platform:
- Windows plug-in: `%PROGRAMFILES%\IBM\ost_plugin_tools`
- AIX plug-in: `/opt/IBM/ost_plugin_tools`
- ProtecTIER server: `/opp/dtc/app/sbin`

This utility has two modes of operation, client and server. The server has to be started before the client. Before running the utility, shut down all other programs on both the client and server systems. The client is the system that transmits the test data and the server is the system that receives the data (also known as the target server). Based on the data sent by the client and received by the server, the script outputs key network parameter values which indicate certain attributes of the network. The goal of these tests is to benchmark the throughput of the network. It is important to test both OpenStorage host-to-ProtecTIER server and ProtecTIER server-to-OpenStorage host directions to measure the bandwidth performance during both backup and restore activities. Network bandwidth is not always the same in both directions. In addition, if an OpenStorage host or a ProtecTIER server uses more than one IP address for OpenStorage operation, it is essential to test each IP address separately.

In the following procedure, the goal is to test network performance between two machines **server1** and **server2**. Each test will run for five minutes. Since there are five tests, the process will take a total of 25 minutes.

Procedure

1. Start the server mode of the utility on **server1** by entering the following commands on the command line:

   `./pt_net_perf_util -s`

2. Start the client mode of the utility on **server2** by entering the following command on the command line:

```
./pt_net_perf_util -c server1_ip_address -t 300
```

where **server1_ip_address** is one of the IP addresses to be tested for server1.
The default size of a buffer used for sending data is 1024KB. To override this
size to another value, for example 256KB, use the -l parameter as follows:

```
./pt_net_perf_util -c server1_ip_address -t 300 -l 256
```

Note: If server1 is a Windows system, use following command:

```
pt_net_perf_util.bat -c server1_ip_address -t 300 --win-server
```

where **server1_ip_address** is one of the IP addresses to be tested for server1.
The same buffer override command can also be used to change the size of the
buffer.

3. The utility will automatically perform the tests in sequence. The client output
(server2 in the example below) will look similar to the following:

Note: In the sample output below the test ran for only 5 seconds instead of
300.

```
*** Latency
PING 9.5.53.33 (9.5.53.33) 56(84) bytes of data.
--- 9.5.53.33 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.257/0.406/0.484/0.079 ms
*** Throughput - Default TCP
[ 3] 0.0- 5.0 sec 56.6 MBytes 94.8 Mbits/sec
*** Throughput - 1 TCP stream(s), 1MB send buffer
[ 3] 0.0- 5.0 sec 57.0 MBytes 95.0 Mbits/sec
*** Throughput - 16 TCP stream(s), 1MB send buffer
[SUM] 0.0- 5.8 sec 65.0 MBytes 94.3 Mbits/sec
*** Throughput - 127 TCP stream(s), 1MB send buffer
[SUM] 0.0-11.3 sec 127 MBytes 94.1 Mbits/sec
Number of TCP segments sent: 230536
Number of TCP retransmissions detected: 21 (0%)
Done.
```

4. See the next section for information about interpreting the results of the tests.

Interpreting the results

The utility performs five foreground tests (Tests 1-5 below), and one background
test (Test 6 below). The example outputs below are from the client side. Each of the
first five tests below ran for 300 seconds (-t 300), while the last test monitored TCP
performance during that time.

Test 1: Latency

This test checks the nominal network link latency and packet loss. Example result:

```
*** Latency
PING 10.0.13.194 (10.0.13.194) 56(84) bytes of data.

--- 10.0.13.194 ping statistics ---
120 packets transmitted, 120 received, 0% packet loss, time 119060ms
rtt min/avg/max/mdev = 57.403/78.491/104.451/9.872 ms
```

Interpreting the results:
• The average round-trip-time (rtt) was 78.4ms and there was 0% packet loss.

- The round-trip-time in network topologies may vary, but should never exceed 200ms on WAN. Contact your network administrator if round-trip-time reports more than 200ms on WAN or 6ms on LAN, as it may significantly decrease throughput.
- Higher latency values will cause a major deterioration in throughput.
- Packet loss should be 0%. Any other value indicates a major network problem.

Test 2: Throughput - default settings

This test checks maximal TCP throughput using a single data stream with default TCP settings. Example result:

```
*** Throughput - Default TCP
[  3]  0.0-120.1 sec  2.41 GBytes    173 Mbits/sec
```

Interpreting the results:
- The test ran for 120.1 seconds, transferred 2.41 GB (2.24 Gb), with an average throughput of 173 Mbits/sec.

   Note: 1 MByte = 1,048,576 bytes. **1 Mbit/sec** = 1,000,000 bits/sec.

Test 3: Throughput - single stream, 1MB send buffer

This test checks maximal TCP throughput using a single data stream with a 1MB (0.95 MiB) send buffer. Example result:

```
*** Throughput - 1 TCP stream(s), 1MB send buffer
[  3]  0.0-120.0 sec  2.51 GBytes    180 Mbits/sec
```

Interpreting the results:
- The test ran for 120.0 seconds, transferred 2.51 GB (2.34 GiB), with an average throughput of 180 Mbits/sec.
- There may be an improvement here on high-latency links.

Test 4: Throughput - 16 streams, 1MB send buffer

Example result:

```
*** Throughput - 16 TCP stream(s), 1MB send buffer
[SUM]  0.0-121.4 sec  5.91 GBytes    418 Mbits/sec
```

Interpreting the results:
- The test ran for 121.4 seconds, transferred 5.91 GB (5.5 Gb), with an average throughput of 418 Mbits/sec.
- The extra streams yielded higher utilization of the connection.

Test 5: Throughput - 127 streams, 1MB send buffer

Example result:

```
*** Throughput - 127 TCP stream(s), 1MB send buffer
[SUM]  0.0-126.1 sec  8.08 GBytes    550 Mbits/sec
```

Interpreting the results:
- The test ran for 126.1 seconds, transferred 8.08 GB (7.53 Gb), with an average throughput of 550 Mbits/sec.
- TCP takes a while to reach its maximal throughput. Longer testing times, 300 seconds or more, will produce more accurate results.

- The throughput value given by this test is the potential physical throughput for this system. It is directly affected by the available bandwidth, latency, packet loss and retransmission rate.
- The Mbits/sec reported in this test is the maximum throughput your system may achieve. If this number is lower than anticipated, contact your network administrator.

Test 6: TCP Retransmissions vs. Total TCP segments sent

Example result:

```
Number of TCP segments sent: 1619061
Number of TCP retransmissions detected: 201038 (12%)
```

Interpreting the results:
- A total of 1619061 TCP segments were sent during the five tests, out of which, 201038 were lost and retransmitted.
- The retransmission rate imposes a direct penalty on the throughput, as the retransmission of these packets take up bandwidth. The retransmission can be caused by the underlying network (e.g. packet dropping by an overflowed router) or by the TCP layer itself (e.g. retransmission due to packet reordering).
- Segment loss can be caused by each of the network layers.
- TCP retransmission larger than 2% may cause performance degradation and unstable network connectivity. Contact your network administrator to resolve this issue and reduce it to approximately 0%.

What to do next

You may want to run these tests again to test the reverse throughput in the network. To run the tests in reverse, change server1 to the client and server2 to the server and repeat the procedures.

Chapter 3. Configuring replication

Use the applicable options on the ProtecTIER Service Menu to configure your system for replication.

About this task

Once basic system configuration is complete, you can perform the tasks required to configure your system for replication. To do so, you will need to complete the pre-configuration tasks outlined in "Before you begin," as well as "Accessing the ProtecTIER Service Menu" through "Configuring static routes" on page 11, if necessary.

Before you begin

This topic describes the prerequisites for configuring replication.

About this task

Replication configuration requires careful planning, decision-making, and coordination of effort. Before you get started, it is strongly recommended that you complete these tasks:

- Make sure that TCP ports 6520, 6530, 6540, 6550 are open in your firewall. Each ProtecTIER server being used for replication must allow TCP access through these ports.
- Ensure that the replication ports are on a different subnet than the external local area network (LAN) port. Having the replication ports and the external LAN port on the same subnet may cause replication errors.

  In addition, IBM recommends that on all ProtecTIER nodes or servers involved in Native Replication, you configure all rep1 ports on one subnet, and you configure all rep2 ports on a different subnet.
- Identify the person (or persons) responsible for completing the planning worksheets.

  It is strongly recommended that the worksheets be filled out in advance by someone with extensive knowledge of your organization's network and TCP/IP configuration. This will ensure that the information is technically accurate and readily available during replication setup.
- Identify the person (or persons) responsible for configuring the TARGET(S) and SOURCE(S) servers for replication, depending on the replication topology you are using.

  This may or may not be the same person (or persons) who completed the worksheets.
- If replication throughput in excess of 1GbE is required for DD6 replication, ensure the network infrastructure accepts 10Gbase-T connections.

After completing the above tasks, return to this page and go to "Accessing the ProtecTIER Service Menu."

Accessing the ProtecTIER Service Menu

Complete this task to access the ProtecTIER Service menu.

Procedure

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

2. At the **login** prompt, type: **ptconfig** and press Enter.

3. At the **Password** prompt, type: **ptconfig** and press Enter.

   The **ProtecTIER Service Menu** displays:

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

4. Go on to "Configuring ProtecTIER Replication Manager."

Configuring ProtecTIER Replication Manager

Use this procedure to configure the ProtecTIER Replication Manager application on the designated server in your replication grid.

About this task

You must configure the Replication Manager application on the server that remotely manages the replication grid or grids within your organization. IBM recommends configuring the ProtecTIER Replication Manager application on the TARGET server at the remote (destination) site. By doing so, the Replication Manager will remain available in a disaster recovery situation.

Note: This task may be completed at any time during the replication configuration process. However, creation of the replication grid and verification of the replication configuration, cannot take place until ProtecTIER Replication Manager is up and running on the designated server.

Procedure

1. On the designated ProtecTIER Replication Manager server, if it is not already displayed, access the ProtecTIER Service Menu. See "Accessing the ProtecTIER Service Menu" on page 25.

2. From the ProtecTIER Service Menu, select **ProtecTIER Configuration (...)**. Type the corresponding number and press Enter. The **ProtecTIER Configuration (...)** menu is displayed.

```
-------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
            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
 15) OS images Management (...)

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

3. Select **Configure replication (...)**. Type the corresponding number and press
   Enter. The **Configure replication (...)** menu is displayed.

```
-----------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
            ProtecTIER Configuration (...)
            Configure Replication (...)
-----------------------------------------------------------------------
   1) Config/Unconfig ProtecTIER Replication Manager on this node
   2) Configure Static Routes

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

4. Select **Config/Unconfig ProtecTIER Replication Manager on this node**. Type
   the corresponding number and press Enter.

5. When the **Replication Manager is currently unconfigured, do you wish to
   configue it? (yes|no)** prompt displays, type: **yes** and press Enter.

   The warning below displays:

   Warning: You should not configure Replication Manager on more than one
   server in a grid, as doing so may cause conflicts within the grid. It is
   recommended that you designate the Target server (Hub) as the
   Replication Manager.

6. When the Are you sure you want to configure the ProtecTIER Replication
   Manager on this node? (yes|no) prompt displays, type: **yes** and press Enter.

   The status messages below, display:

   Gathering information [Done]

   The configurePTReplicationManager ended successfully message displays.

7. When the Press the ENTER key to continue... prompt displays, press Enter.
   You are returned to the **Configure replication (...)** menu.

8. If the static routes have not been previously configured, continue to
   "Configuring static routes" on page 11.

9. Type **E** and press Enter to exit.

Chapter 4. Installing ProtecTIER Manager

The topics in this chapter describe how to install, configure, and uninstall the ProtecTIER Manager software.

The ProtecTIER system is managed with the ProtecTIER Manager software. It is recommended that you install the ProtecTIER Manager software on one or more workstations and not directly on the ProtecTIER servers.

ProtecTIER Manager enables you to:
- Configure ProtecTIER
- Monitor the status of nodes and clusters
- Manage file systems, repositories, and services
- Change the system configuration
- Manage Native Replication activities with the ProtecTIER Replication Manager software

Prerequisites for the ProtecTIER Manager workstation

This topic describes the workstation prerequisites for installing and running the ProtecTIER Manager.

The ProtecTIER Manager workstation must meet the following prerequisites in order to install and run ProtecTIER Manager effectively:
- One of the following operating systems:
  - Windows 7
  - Windows 8, 2012
  - Linux Red Hat 64 ES/AS (4, 5 and 6)
- At least 1.2 GB of available disk space
- At least 256 MB of RAM
- Workstation access to the ProtecTIER service nodes IP addresses (ports 3501 and 3503 are open on the firewall).

IBM recommends that you use the following settings to configure the monitor for ProtecTIER Manager:
- Resolution of 1024 x 768 pixels or higher (this resolution is the minimum supported, however, 1280 x 1024 is recommended).
- 24 bit color or higher

Note: If you are planning to run ProtecTIER Manager on a UNIX system, configure your graphics card and X Window System. You can perform this task either manually or by use of the Xconfigurator utility. For instructions, refer to the appropriate Linux documentation.

Installing the ProtecTIER Manager software

Use the procedures in this chapter to install the latest version of ProtecTIER Manager software on the ProtecTIER Manager Workstation.

Important: Before starting the installation, make sure that the currently installed ProtecTIER Manager application is closed.

The ProtecTIER Manager installer is provided on your *IBM ProtecTIER Manager V3.3.6.1* DVD.

Different ProtecTIER Manager installers are used for Windows and Linux. Ensure that the installer that you are using is correct for the operating system running on your workstation.

- If you are installing ProtecTIER Manager on a workstation running Windows, see "Installing on Windows."
- If you are installing ProtecTIER Manager on a workstation running Linux, see "Installing on Linux" on page 31.

If you are installing ProtecTIER Manager on a workstation on which an older version of ProtecTIER Manager is already installed, uninstall the older version first. For more information, see "Uninstalling the ProtecTIER Manager software" on page 32.

Installing on Windows

Complete this task to install ProtecTIER Manager on a Windows system.

About this task

Perform the following steps to install ProtecTIER Manager on a Windows system:

Procedure

1. Insert the *IBM ProtecTIER Manager V3.3.6.1* DVD into the CD-ROM drive of the designated ProtecTIER Manager workstation.
   - If the ProtecTIER Manager installer launches and starts the installation, go on to step 2.
   - If the ProtecTIER Manager installer process does not launch automatically, do the following:
     a. On the Windows task bar, click: **Start > Run**. The **Run** dialog box opens.
     b. In the Open box, type: **D:** (where D: is the CD-ROM drive of the server).
     c. Click **OK**.

        The contents of the *IBM ProtecTIER Manager V3.3.6.1* DVD displays.
     d. From the list of files, locate the ProtecTIER Manager for Windows installation file and double-click the file to start the installation.
2. Read the **Introduction** screen, and then click **Next**.
3. Read and accept the license agreement provided, and click **Next**.

   The **Red HAT Enterprise Linux License** screen is displayed.
4. Read and accept the license agreement provided, and click **Next**.

   The **Choose Install Folder** screen is displayed.
5. Specify the folder where the ProtecTIER Manager program files are to be installed, and click **Next**.

   The **Choose Shortcut Folder** screen is displayed.
6. Select the location where the program icons are to be created:
   - **In a new Program Group** - Creates a program group in the Program list of the Start menu.

- **In an existing Program Group** - Adds the shortcut to an existing program group in the Program list of the Start menu.
- **In the Start Menu**
- **On the Desktop**
- **In the Quick Launch Bar**
- **Other** - Enables you to enter a path location for the shortcut, or to browse for a location by clicking Choose.
- **Don't create icons** - No shortcuts are created.

  Note: When relevant, you can select **Create Icons for All Users** to create a shortcut in the defined location for all user accounts on the workstation.

7. Click **Next**.

   The **Pre-Installation Summary** screen displays the Install and Shortcut folder locations and the disk space information of the target for installation.
8. Review the **Summary** screen, and click **Install** to start the installation.

   The **Installing ProtecTIER Manager** screen is displayed.
9. When the installation is complete and ProtecTIER Manager has been successfully installed, click **Done**.

   The ProtecTIER Installation wizard closes and the installation process is complete.

What to do next

Go on to the next chapter.

Installing on Linux

Complete this task to install ProtecTIER Manager on a Linux system.

About this task

Perform the following steps to install ProtecTIER Manager on Linux:

Procedure

1. Insert the *IBM ProtecTIER Manager V3.3.6.1* DVD into the CD-ROM drive of the designated ProtecTIER Manager workstation.
2. Run the ProtecTIER Manager installer.

   Note: This procedure presumes that the workstation has a Linux graphical interface which is required for ProtecTIER Manager.
   a. From the Linux Desktop, select and open the CD drive icon.
   b. Select and open the folder for your Linux version: **Linux** for version **64** or **Linux32** for version **32**.
   c. When the folder opens, drag the **InstallLinuxXX.bin** file from the folder to the Desktop. (XX=either 32 or 64, depending on the Linux folder that you selected.)
   d. Close the open windows.
   e. Right-click on an open area of the Desktop, and from the menu options displayed, select **Open Terminal**.
   f. At the Terminal command prompt, use the following command to change to the Desktop directory (**Note:** Desktop is case-sensitive. Type it using a capital "D".):

```
cd Desktop
```

and press Enter.

  g. From the Desktop directory in the Terminal window, run the ProtecTIER Manager installer:

```
./InstallLinuxXX.bin
```

and press Enter.

(XX= either 32 or 64)

If the message: `Permission Denied` displays, enter the following commands:

```
chmod +x InstallLinuxXX.bin
./InstallLinuxXX.bin
```

after typing each command press Enter.

The **IBM ProtecTIER Manager** wizard **Introduction** screen is displayed.

3. Click **Next**. Two separate **Software License Agreement** screens display.

4. Read the terms for each license agreement, select **I accept both the IBM and non-IBM terms of the License Agreement** and click **Next**. The **Choose Install Folder** screen is displayed.

5. Enter the path to the location where you want the ProtecTIER Manager program files installed. Click **Choose** to browse for a location.

   Note: Click **Restore Default Folder** to revert to the default installation path.

6. Click **Next**. The **Choose Link Folder** screen is displayed.

7. Select the location where you want the program links created::
   - **In your Home folder** – Creates the links in the directory where the user files are typically stored. For example: */home/bill*.
   - **Other** – Creates the links in the default location (/opt/IBM/PTManager). To specify a different location, click **Choose** and select a directory on the workstation hard disk drive.
   - **Don't create links** – No links are created.

8. Click **Next**. The **Pre-Installation Summary** screen is displayed.

9. Click **Install**. The **Installing ProtecTIER Manager** screen is displayed and ProtecTIER Manager is installed on your computer. When the installation is complete, the **Install Complete** screen is displayed.

10. Click **Done**. The **ProtecTIER Manager** wizard closes. When the command prompt returns in the Terminal window, type **exit** to close the window.

Uninstalling the ProtecTIER Manager software

This topic describes how to uninstall the ProtecTIER Manager software.

Procedure

To uninstall the ProtecTIER Manager software:

1. From the ProtecTIER Manager directory, run the ProtecTIER Manager uninstaller. The **Uninstall ProtecTIER Manager** wizard **Introduction** screen is displayed.

2. Click **Uninstall**. The **Uninstalling** screen is displayed and the ProtecTIER Manager software is removed from your computer. The **Uninstall Complete** screen is displayed.

3. Click **Done**. The **Uninstall ProtecTIER Manager** wizard closes.

Checking the ProtecTIER 3958 DD6 Firmware version

Complete this task to check the 3958 DD6 Firmware version

About this task

Important: The firmware upgrade process connects to the Baseboard Management Controller (BMC) to get firmware information. Therefore, it is mandatory to have the BMC configured with an IP address on the same customer network segment before continuing with the procedure.

Procedure

1. If you are updating a single node configuration, connect a USB keyboard and graphics-capable monitor to the server.
2. If you are updating a clustered configuration, verify that both Server A and Server B are running:
   - **Yes**, continue to step 3
   - **No**, power on any servers that are not running, wait for the boot cycle to complete, and then continue to step 3
3. At the localhost **Login** prompt, type the user ID **ptconfig** and the password **ptconfig** press **<enter>**.

   The **ProtecTIER System Menu** displays:

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

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

4. Select **Protectier Configuration**. Type the corresponding number and press **<enter>**.

   The **ProtecTIER Configuration (...)** screen displays:

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

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

5. Select **Update Firmware**. Type the corresponding number and press **<enter>**.

   The **Update Firmware (...)** screen is displayed:

```
 --------------------------------------------------------------------------------
  ProtecTIER Service Menu running on rassmx
           ProtecTIER Configuration (...)
           Update Firmware (...)
 --------------------------------------------------------------------------------
  1) Update Server Firmware
  2) Display Firmware Version for BMC and GEM Components
  3) Upgrade Firmware Version for BMC and GEM Components

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

6. Select **Display Firmware Version for BMC and GEM Components**. Type the
   corresponding number and press **<enter>**. Wait for the process to complete:

```
Your choice? 2
Begin Processing Procedure [Jan 31 11:36:18]

Firmware Component : Version
----------------------------------
BMC              : 2.0.003C
CPLD             : 0.6.0004
BIOS             : 0.3.0016
FLASH CONFIG     : 0xAD9E52D7
DISRUPTIVE       : 0x30E4C1D4

End Processing Procedure Successfully [Jan 31 11:36:18]
```

Updating the ProtecTIER 3958 DD6 Firmware

Complete this task to update the 3958 DD6 Firmware

About this task

Important: The firmware upgrade process connects to the Baseboard Management
Controller (BMC) to get firmware information. Therefore, it is mandatory to have
the BMC configured with an IP address on the same customer network segment
before continuing with the procedure.

Procedure

1. If you are updating a single node configuration, connect a USB keyboard and graphics-capable monitor to the server.

2. If you are updating a clustered configuration, verify that both Server A and Server B are running:

   • **Yes**, continue to step 3

   • **No**, power on any servers that are not running, wait for the boot cycle to complete, and then continue to step 3

3. At the **Login** prompt, type the user ID **ptconfig** and the password **ptconfig** press **<enter>**.

   The **ProtecTIER System Menu** displays:

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

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

4. Select **Protectier Configuration**. Type the corresponding number and press **<enter>**.

   The **ProtecTIER Configuration (...)** screen displays:

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

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

5. Select **Update Firmware**. Type the corresponding number and press **<enter>**.

   The **Update Firmware (...)** screen is displayed:

```
-------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
           ProtecTIER Configuration (...)
           Update Firmware (...)
-------------------------------------------------------------------------------
  1) Update Server Firmware
  2) Display Firmware Version for BMC and GEM Components
  3) Upgrade Firmware Version for BMC and GEM Components

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

6. Select Upgrade Firmware Version for BMC and GEM Components. Type the corresponding number and press **<enter>**. The current firmware is checked and if an upgrade is needed, a confirmation message is displayed informing that services will be stopped and 1 or 2 reboots are needed during the upgrade process. Select **Yes** and press **<enter>**. Wait for the process to complete:

```
Your Choice? 3
BeginProcessingProcedure [Jan 30 07:47:33]
Checkcurrent Firmware Versions   [ Done ]
In ordertoupdatetheNode's firmware level, alltheserviceswill be stopped.
The firmware upgradeprocesswill requiere 1 reboot
Do youwanttocontinue? (yes|no) yes
Stoppingptrasd  [ Done ]
Stoppingvtfd  [ Done ]
Stoppingptcluster  [ Done ]
Updating BMC firmware                            [ Done ]
Updating CPLD firmware                           [ Done ]
Updating BIOS firmware                           [ Done ]
Machine will be rebooted
```

7. Once the system is online, run the Update Firmware option again to make sure the process completed. If firmware was upgraded successfully the following message is displayed:

```
Your choice? 3
Begin Processing Procedure [Jan 31 11:25:43]

Check current Firmware Versions                  [ Done ]
All firmware versions are up to date.

End Processing Procedure Successfully [Jan 31 11:25:43]
```

Chapter 5. Getting started with ProtecTIER Manager

Topics in this chapter provide an overview of common ProtecTIER Manager tasks.

After the ProtecTIER Manager software has been installed, familiarize yourself with various common tasks that apply throughout the ProtecTIER Manager application.

Running the ProtecTIER Manager

This task describes how to run the ProtecTIER Manager software on the ProtecTIER Manager workstation.

About this task

The ProtecTIER Manager GUI can be run from either a Windows based, or a Linux based ProtecTIER Manager workstation.

Procedure

1. Run the ProtecTIER Manager application:
   - On a Windows-based ProtecTIER Manager workstation, run the ProtecTIER Manager application:

     Click **Start > All Programs > IBM > ProtecTIER Manager > IBM ProtecTIER Manager**.
   - On a Linux-based ProtecTIER Manager workstation:
     a. Navigate to the directory where you installed ProtecTIER Manager. The default installation directory is: **/opt/IBM/PTManager**.
     b. Double-click the ProtecTIER Manager icon.

   The **ProtecTIER Manager** window is displayed.
2. Go on to Chapter 6, "Managing nodes," on page 43.

Managing users

The topics in this section describe how to manage users of the ProtecTIER Manager system.

ProtecTIER Manager enables you to create user accounts with different permission levels for accessing and configuring your ProtecTIER system.

Notes:
- User accounts (including the default user account) defined in the GUI are different than user accounts used on the ProtecTIER server.
- Do not use the GUI to manage user accounts on the ProtecTIER server.
- The end-user can change passwords according to the required security policy without affecting ProtecTIER functions.
- The GUI does not handle password policies or rotation rules.

Permission levels

This topic describes the various user permission levels in the ProtecTIER Manager system.

The ProtecTIER system supports the following permission levels:

- **Administrator** has full access to the ProtecTIER system.

  Note: Only one Administrator can be logged in to the ProtecTIER system at a time. If you log in as an administrator while another administrator is already logged in, the system displays a notification pane. The notification pane lists the other administrator who is logged in, and offers to force that administrator to log out.

- **Operator** can access ProtecTIER Manager monitoring screens and perform limited tasks.
- **User** can access only ProtecTIER Manager monitoring screens.

Adding user accounts

This topic describes how to add a user account to ProtecTIER Manager.

About this task

Complete this task to add a new user account to the ProtecTIER Manager system.

Procedure

1. Log in to the ProtecTIER Manager system and choose **System > Manage Users**. The **Manage Users** dialog is displayed:
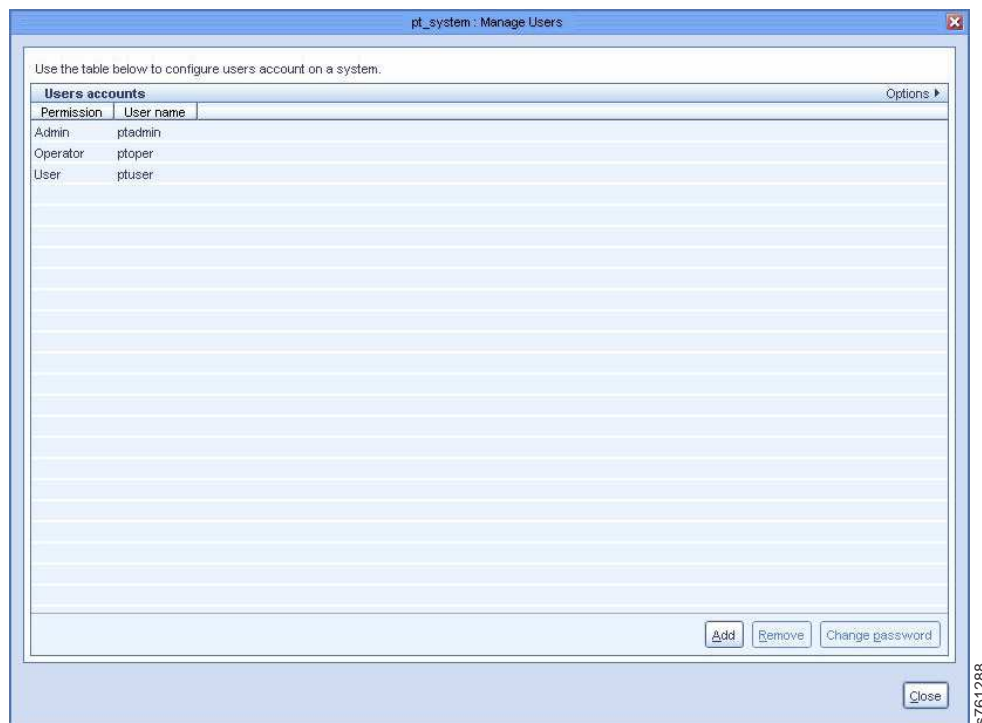
Figure 7. Manage Users dialog

2. Click **Add**. The **Add account** dialog is displayed.

3. In the **User name** field, enter a username for the account.
4. In the **New password** field, enter a password for the account.
5. In the **Verify password** field, reenter the password that you entered in the **New password** field.
6. In the **Permission** field, select a permission level (Administrator, Operator, or User) you want to assign to the user account.

   Note: Before processing, record this information in a manner that allows you to notify the new user. Remind the new user to record the password because you nor the system stores the passwords for later use.
7. Click **Ok**. The **Add account** dialog closes and the account is added to the ProtecTIER Manager system.
8. Click **Close** to exit the **Manage Users** window.

Changing the user account password

This topic describes how to change the password of a user account on the ProtecTIER Manager system.

About this task

Complete this task to change the user password in the ProtecTIER Manager system.

Procedure
1. Choose **System > Manage Users**. The **Manage Users** dialog is displayed.
2. Select a user account from the list and click **Change password**. The **Change password** dialog is displayed.
3. Type the current password in the **Password** field.
4. Type the new password in the **New password** field.
5. Type the new password again in the **Verify password** field.
6. Click **Ok**. The password for the selected user account is changed.
7. Click **Close** to exit the **Manage Users** window.

Changing the Support System settings

This topic explains how to change the support system settings.

About this task

The ProtecTIER Manager installation wizard and the ProtecTIER Manager application are fully compatible with the JAWS screen-reader software. ProtecTIER Manager also allows you to change other accessibility settings, such as the contrast resolution mode and color palette. Instructions for installing JAWS and the Java-based accessibility tools, and for setting the contrast resolution mode and color palette are available in "Accessibility features for TS7600 family of products" on page 273.

Saving and printing data

This task describes how to save or print the data displayed in informational ProtecTIER Manager windows.

About this task

Follow these steps to save or print data in ProtecTIER Manager informational windows and panes:

Procedure

1. Select **Options** in the upper right-hand corner of the window.

   Note: The **Options** menu may not be available on all windows.

2. Select **Save** to save the information or **Print** to print the information. Use the standard saving or printing procedures for your operating system.

Refreshing ProtecTIER Manager

This task describes how to refresh windows, screens, and panes in the ProtecTIER Manager application.

Many windows, screens, and panes of ProtecTIER Manager automatically refresh to display the most current information. However, you need to refresh some windows manually. Because you can have multiple ProtecTIER Manager workstations on the same system, changes made on another workstation are not automatically reflected on your workstation. To ensure that you have the most up to date information, you should periodically refresh the ProtecTIER Manager Navigation pane and View pane.
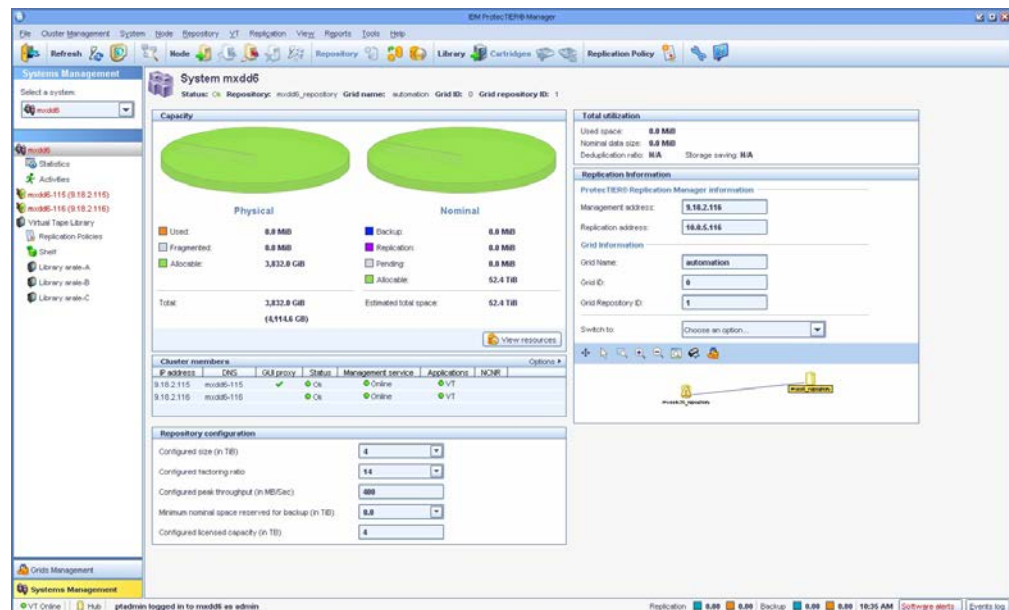
Figure 8. ProtecTIER Manager

Select the **Refresh navigation pane** button to refresh the Navigation pane.

Select the **Refresh current view** button to refresh the View pane.

Running operations in the background

This topic describes enabling operations to run in the background while you are running another operation.

You can use the same instance of ProtecTIER Manager to work with multiple ProtecTIER systems while a specific ProtecTIER Manager operation runs in the background. You cannot, however, run multiple operations in the same ProtecTIER system.

For instance, if you are running a **Delete library** operation, the wizard prompts you to wait while the system goes offline to run the required operation. That system will be busy until it completes, thereby not allowing further administration of other operations.

By selecting **Run in background**, you return control to the user. If additional systems are configured in ProtecTIER Manager, those systems are accessible and can be worked on, even while the required operation is running.

Chapter 6. Managing nodes

Topics in this chapter describe how to manage nodes on the ProtecTIER system.

The ProtecTIER system supports both one-node systems and two-node active-active clusters. Using two nodes in a cluster enables higher throughput and provides higher-availability in the event of node failure.

Adding and removing nodes from ProtecTIER Manager

The topics in this section describe how to add a node, a subnetwork node, and remove a node from the ProtecTIER system using the ProtecTIER Manager.

Note: This section provides instructions for adding and removing nodes when using the TS7650G.

Adding a node registers the node IP address and port number with the instance of ProtecTIER Manager at your workstation. Similarly, removing a node removes the node registration from ProtecTIER Manager at that workstation.

Adding nodes

Complete this task to add a node to your ProtecTIER system with ProtecTIER Manager.

About this task

Adding a node registers the node IP address and port number with the instance of ProtecTIER Manager at your workstation.

To add a node to your ProtecTIER system:

Procedure

1. Run the ProtecTIER Manager application:
   - For a Windows-based ProtecTIER Manager workstation, run the ProtecTIER Manager application:

     Click **Start > All Programs > IBM > ProtecTIER Manager > IBM ProtecTIER Manager**.
   - For a Linux-based ProtecTIER Manager workstation, click the icon for ProtecTIER Manager on the Desktop or the location of the shortcut specified during the installation.

   The **ProtecTIER Manager** window is displayed.
2. From the Systems Management view, click the **Add new node** button on the toolbar located at the top of the **ProtecTIER Manager** window. The **Add new node** dialog box is displayed, prompting you for the IP address and Port number of the node that you want to add.
3. Enter the IP address of the node and click **Ok**. The node is displayed in the **Navigation** pane and the **Login** button is displayed in the **View** pane.

   Note: Do not change the port number of the node unless directed to do so by trained ProtecTIER specialist.

What to do next

Go on to "Logging in and out of the ProtecTIER Manager application" on page 46.

Adding node subnetworks

This topic describes how to add a node subnetwork to your ProtecTIER system with the ProtecTIER Manager.

About this task

In addition to adding individual nodes to ProtecTIER Manager, you can add addresses for subnetworks to which nodes are connected. When ProtecTIER Manager restarts, it automatically detects all nodes on the added subnetworks of the TCP/IP network.

Procedure

1. Click on the **Auto discovery** tab.
2. For each subnetwork you want to add, click a **Sub network** check box and enter the subnetwork address in the corresponding field.
3. Click **Ok**. The **Preferences** dialog box closes and the subnetwork address is added to the ProtecTIER Manager. When you restart the ProtecTIER Manager, all nodes on the defined subnetwork addresses are automatically added to the ProtecTIER Manager.

Removing nodes

This topic describes how to remove a node from your ProtecTIER system using the ProtecTIER Manager.

About this task

Removing a node stops the instance of ProtecTIER Manager at your workstation from registering the node and being able to manage it. The node itself, and the cluster with which the node is associated, is unaffected by removing a node in this way.

Note: If you remove a node that is associated with a two-node cluster, the second node will also be removed.

Perform the following steps to remove a node from ProtecTIER Manager:

Note: Do not log in to the node you want to remove or you will be unable to perform this operation.

Procedure

1. From the **Select a system** dropdown list in the Systems Management view, choose the system from which you want to disconnect.
2. Select **Node** > **Remove node**. A confirmation message box is displayed to remove the connection.
3. Click **Yes**. The node is removed.

Customizing the network configuration of a node

This topic describes how to use the Network Configuration window in ProtecTIER Manager to customize the IP communication interfaces on a node.

About this task

The Network Configuration window lets you reassign the IP communication interfaces to group several physical interfaces into a single virtual interface, and create a bond configuration of several physical interfaces.

Procedure

1. From the Systems Management view, select **Node** > **Network configuration**. The **Network configuration** window is displayed:
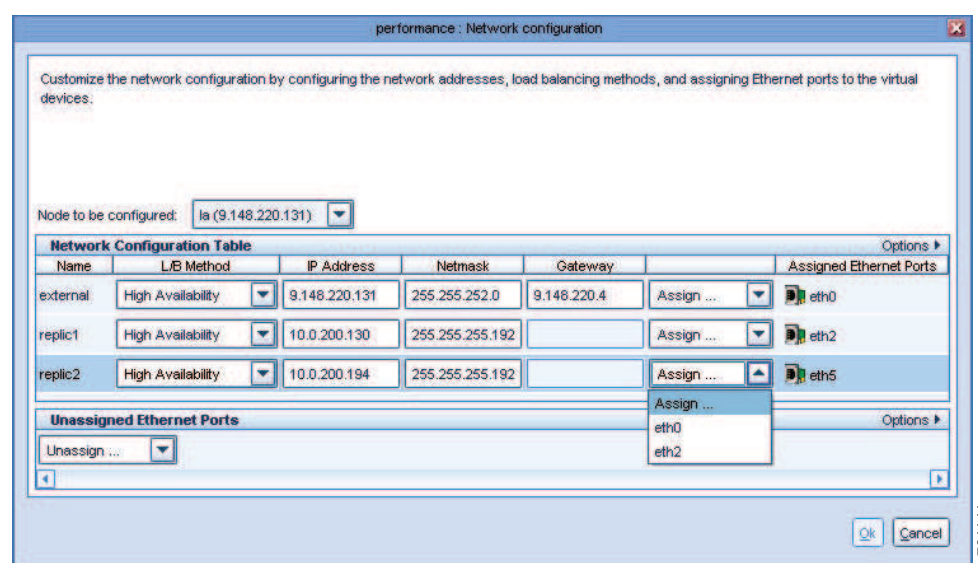
Figure 9. Configure IP interfaces window

2. Select a node from the **Node to be configured** field.

   Note: On clustered systems, there is a separate configuration table for each node.

3. Highlight the virtual interface you wish to edit.

4. Click on the dropdown in the **L/B Method** column to select the load balancing method. The available load balancing methods are displayed:

   RR (Round-robin)
   Outgoing traffic is spread evenly across all of the adapter ports in the bond

   L2 Outgoing traffic is spread using a default transmit hash policy of layer 2

   L2L3
   Outgoing traffic is spread using a transmit hash policy of MAC addresses and IP addresses of the source and the destination

   L3L4
   Outgoing traffic is spread using a transmit hash policy of IP addresses and ports of the source and the destination

HA Active-backup policy: only one slave in the bond is active. A different slave becomes active if, and only if, the active slave fails.

5. Edit the **IP Address**, **Netmask** and **Gateway** addresses, as desired.
6. If you want to reassign a physical interface, select an Ethernet port from the ports available in the **Assign** field.
7. If you want to unassign a port, select the port to unassign from the **Unassigned Ethernet Ports** dropdown.
8. Click **Ok** to save the changes and exit the Network Configuration window.

Logging in and out of the ProtecTIER Manager application

Complete this task to log in to and log out of the ProtecTIER Manager application.

About this task

ProtecTIER Manager has default user accounts corresponding to three user permission levels: Administrator, Operator, and User. For more information, see "Permission levels" on page 38. The default username and password for each of these accounts are as follows:

Table 2. Default usernames and passwords

Permission Level	Default Username	Default Password
Administrator	ptadmin	ptadmin
Operator	ptoper	ptoper
User	ptuser	ptuser

Log in to each ProtecTIER node that you want to manage with the ProtecTIER Manager.

Procedure

1. Click the **Login** button. The **Login** dialog box is displayed.
2. Enter your username and password.
3. Click **Ok**. The **Login** dialog box closes and ProtecTIER Manager displays the information for that node.

Results

IBM recommends that you change or replace these default user accounts. For more information, see "Managing users" on page 37.

Note: Only one Administrator can be logged in to a ProtecTIER node at a time. To avoid conflicts, you should log out at the end of each session by clicking the **Logout** button.

If you log in with Administrator level permission while another Administrator is already logged in, a message box is displayed with the following message:

```
Administrator is already logged in:
Username:
Host:
IP address:
Would you like to login anyway?
```

Clicking **Yes** forces the other Administrator to logout.

What to do next

Go on to Chapter 7, "Managing repositories," on page 49.

Chapter 7. Managing repositories

The topics in this chapter describe how to use the ProtecTIER Manager software to create and manage repositories in TS7600 ProtecTIER Deduplication Solutions, V3.4.

Each ProtecTIER cluster has one repository on which data is stored. In systems enabled for two-node clusters, a repository for common use is a prerequisite for adding a second cluster member.

Use the ProtecTIER Manager software for repository management tasks, including:

- Enabling replication
- Increasing the capacity of repositories
- Configuring the virtual libraries in VTL systems on the ProtecTIER server
- Connecting the user host servers to the ProtecTIER server with the provided FC cards on the Enterprise controllers
- Defragmenting a repository
- Reserving space on a repository

Enabling replication

Perform the following procedure on ProtecTIER Manager to enable replication on systems that have not already been configured for replication.

Before you begin

Note: It is possible that replication has already been enabled on your system. For example, if you performed the **Increase Capacity** operation with ProtecTIER v2.3 or above, replication was automatically enabled.

By default, replication is enabled on new repositories created with ProtecTIER v2.3 and above. Replication is disabled on repositories upgraded from v2.2 (and below) versions. When you enable replication, you must assign files systems, set the estimated factoring ratio, MD raid configuration, and disk size. The procedure allocates metadata for replication and then you can add file systems to the repository as needed. If more storage is required, you can select additional file systems (if they exist) to add to the metadata.

About this task

Enabling replication on the TS7650G might require additional metadata, pending the actual metadata deployment on the specific repository.

To enable replication:

Procedure

1. From the Systems management view, select **Replication > Enable replication**. The **Enable replication** wizard welcome screen is displayed.
2. Click Next. The **Properties** dialog is displayed.
3. Select the Estimated factoring ratio, the MD raid configuration, and the Disk size (in GB) of the metadata disks.

Note: The size of the repository cannot be changed when enabling replication.

4. Click Next. The **Repository resources** dialog displays the total amount of metadata and user data (in GB) allocated for the repository.

5. If more storage is required, click **Advanced**. The **Repository resources** window is displayed with a list of available file systems (if they exist).

6. Select what file systems to use for metadata or user data. Click **Ok**. The resources window closes.

7. Click **Finish**. The summary report is displayed and replication is enabled on ProtecTIER Manager.

Expanding repositories

Complete the tasks in this topic to increase the capacity of a repository.

About this task

Attention: This section provides instructions for increasing the capacity of a repository.

After the repository is created, the ProtecTIER system enables you to increase the capacity of the repository. Much like creating the repository, expanding the repository requires the guidance of a trained ProtecTIER specialist and use of a wizard for planning repository expansions. You might need to expand the repository if:

- Your factoring ratio is higher than originally expected and you are running out of meta data space.
- Your repository needs have expanded beyond the original growth projections and you are running out of user data space.

The increase capacity steps described in this task appear in the order in which they should be performed:

1. Plan the expansion using ProtecTIER Manager.
2. Create new file systems or extend existing ones on the backend storage using the ProtecTIER Service menu and verify that the devices are displayed.
3. Run the Increase Capacity wizard.
4. Complete the operation (for a second cluster node).

Guidelines for increasing the repository and the virtual capacity of a cartridge

Increasing the capacity of a repository impacts the virtual capacity of cartridges.

Increasing the capacity of a repository has a direct impact on the way the ProtecTIER system calculates the logical maximum size of the defined virtual cartridges. When you increase the repository, the maximum size of the cartridges is updated and recalculated based on the new repository size (that is, the size of the cartridges is increased).

When you create a repository, the **nominal size** of the repository is equal to the **factoring and compression ratios** multiplied by its **physical size**. The following calculation is used:

`[nominal size]=[factoring and compression ratio]*[physical size]`

ProtecTIER emulates real cartridges with a given virtual capacity. When adding cartridges to the repository, the **virtual capacity of the cartridge** is equal to the **nominal size of the repository** divided by the **number of cartridges** in the system, as shown in the following calculation:

`[cartridge virtual capacity]=[nominal size]/[number of cartridges in the system]`

The resulting value of the **virtual capacity of the cartridge** is dynamic, such that:

- If you add more cartridges to the system, the virtual capacity of the cartridge decreases.
- If you delete cartridges from the system, the virtual capacity of the cartridge increases.
- If the factoring ratio decreases, the nominal size of the repository decreases, therefore causing the virtual capacity of the cartridge to decrease.
- If more capacity is added to the repository, the nominal size of the repository increases, therefore causing the virtual capacity of the cartridge to increase.

When the virtual capacity size of the cartridge is full, the backup application receives an Early Warning (EW) message, and the cartridge is marked **full** in ProtecTIER Manager. If the capacity of the cartridge increases, the cartridges stay marked as **full**. You must expire cartridges that have reached EW to use the remaining capacity.

If the full cartridges cannot be expired, you must add cartridges after increasing the capacity so that the virtual capacity of each cartridge is less than, or equal to the previous capacity.

Planning an expansion

Complete this task to plan for a repository expansion.

About this task

With the guidance of a trained ProtecTIER specialist, run the **Plan repository increase** wizard to determine the optimum repository size and meta data file system arrangement for your expanded repository.

To plan a repository expansion:

Procedure

1. Choose **Repository > Increase capacity planning**. The **Increase capacity planning** window opens.
2. In the **Repository size** field, select the total physical size, in TB, for the repository.

   Note: If you are expanding the repository only to increase the amount of meta data space, increase the estimated factoring ratio value, but leave the repository physical size value unchanged.
3. In the **Estimated factoring ratio** field, enter the updated factoring ratio estimate for the repository.
4. In the **MD Raid configuration** field, select a configuration option from the drop-down list.
5. In the **Disk size** field, select the physical disk size, in GB, from the drop-down list.

6. Click **Ok**. The **Increase capacity planning** dialog closes and the **Repository meta data storage requirements** window is displayed listing the minimum meta data file system expansion options that are suitable for your expansion needs.

7. Click **Options** to print or save as a *.csv* file the information in the Repository meta data storage requirements dialog using the standard procedures for your operating system.

8. Click **Plan again** to go back to the **Increase capacity planning** window and change the configuration options, or click **Close**. The **Repository meta data storage requirements** dialog closes.

Results

The information from the Repository meta data storage dialog indicates whether you need to create more file systems and/or expand the existing file systems for the increased repository.

Note: If you need to expand an existing file system, refer to "Using the ProtecTIER Service Menu to expand existing file systems." If not, go on to "Using the ProtecTIER Service Menu to create file systems" on page 55.

Using the ProtecTIER Service Menu to create and extend file systems

Use the ProtecTIER Service Menu to create or extend the required file systems. When you select a given option, an interactive dialog starts, allowing you to select desired components and values and to confirm your final choices.

Complete these tasks to increase the physical capacity of a repository.

To extend existing file systems, go to "Expanding the repository" on page 57. To create new file systems, go to "Using the ProtecTIER Service Menu to create file systems" on page 55.

Using the ProtecTIER Service Menu to expand existing file systems

Use the *File Systems Management* menu to extend existing file systems, based on the output of the **Plan repository increase** wizard.

About this task

Note: Before continuing with this task, file systems needed for extending existing file systems should be performed on the backend storage.

Procedure

Follow these steps to **extend** an existing file system for repository metadata storage with a new unused device on a repository.

1. Log in to Server A. Open a Secured Shell (SSH) session to the node and log in using the user ID: **ptconfig** and password: **ptconfig**.

2. At the command line type **menu** and then press Enter. The ProtecTIER Service menu displays:

```
 ------------------------------------------------------------------------
   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. Type the numeral corresponding to ProtecTIER Configuration and press Enter.
   The ProtecTIER Configuration menu displays:

```
 --------------------------------------------------------------------------------
  ProtecTIER Service Menu running on rassmx
            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
  15) OS images Management (...)

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

4. Type the numeral corresponding to File Systems Management and press Enter.
   The File Systems Management menu displays.

```
 ------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
            ProtecTIER Configuration (...)
            File Systems Management (...)
 ------------------------------------------------------------------------
   1) Configure file systems on all available devices
   2) Create file system(s) on a single unused device
   3) Extend a file system with a new unused device
   4) Update /etc/fstab
   5) Display configured devices
   6) Display unused devices
   7) Display GFS repository file systems
   8) Display unused GFS file systems
   9) Increase capacity completion (applicable for a second cluster node)

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

Note: Complete the steps in the order they appear. Display the new volumes created on the backend storage before expanding the file systems.

- To display the list of file systems that are already part of the repository, type the numeral corresponding to `Display GFS repository file systems` and press Enter. An example follows:

```
Device          Size            MountPoint
vg01-lv_vg01    2044.00M        /mnt/vg01-lv_vg01
vg11-lv_vg11    2285196.00M     /mnt/vg11-lv_vg11
vg21-lv_vg21    3430864.00M     /mnt/vg21-lv_vg21
```

- To display the list of available new multipath devices, type the numeral corresponding to `Display unused devices` and press Enter. An example follows:

```
Device:         Size:           MountPoint
mpath0          2048.00M        Unused
mpath1          2285200.00M     Unused
mpath2          2287248.00M     Unused
mpath3          2287248.00M     Unused
```

- To expand an existing file system, type the numeral corresponding to `Extend a file system with a new unused device` and press Enter. You must select a file system and an unused device to which to extend it.

  Note: At the prompt to stop the VTFD service, type y to continue. At the end of the procedure, all services will be automatically restarted.

  For example:

```
GFS File Systems
1. vg1p1-lv_vg1p1
2. vg2p1-lv_vg2p1

Please select file system to extend:1
Display of all available devices
Device:         Size:           Status
1. mpath0       512000.00M      Unused
2. mpath3       512000.00M      Unused

Please select device:1
You have selected to extend file system 'vg1p1-lv_vg1p1' with device 'mpath0' having
size '512000.00M'
Please confirm:? (yes|no) y
This will stop the VTFD service, Do you wish to continue? (yes|no) y
Stopping RAS                                              [ Done ]
Stopping VTFD                                             [ Done ]
Stopping RAS                                              [ Done ]
Stopping VTFD locally                                     [ Done ]
Stopping RAS Remotely                                     [ Done ]
Stopping VTFD remotely                                    [ Done ]
Stopping Remote Cluster Services                          [ Done ]
Creating partition                                       [ Done ]
Creating physical volume                                 [ Done ]
Add PV to VG                                             [ Done ]
Extend LV                                               [ Done ]
Extend FS                                               [ Done ]
Starting VTFD                                            [ Done ]
Starting RAS                                             [ Done ]
Successful file system extension



End Processing Procedure Successfully

Press <ENTER> to continue
```

What to do next

If you are required to create new file systems for repository user data and metadata storage, proceed to "Using the ProtecTIER Service Menu to create file systems." Otherwise, go to "Expanding the repository" on page 57.

If you do not want to continue with expanding the repository at this stage, continue to "Completing the increase capacity operation" on page 59 to complete the increase capacity procedure for a two-node cluster configuration.

Using the ProtecTIER Service Menu to create file systems
About this task

Use the *File Systems Management* menu to create file systems for repository user data and metadata storage, based on the output of the **Plan repository increase** wizard. You need to create the set of file systems only once. Even if you later delete the repository, you can recreate the repository using the existing file systems.

Note: Complete the steps in the order they appear. Before creating the new file systems, display the new volumes created on the backend storage.

Procedure

Follow these steps to **create** file systems on a repository:

1. Log in to a ProtecTIER node server. Open a Secured Shell (SSH) session to the node and log in using the user ID: **ptconfig** and password: **ptconfig**.
2. At the command line type **menu** and then press Enter. The **ProtecTIER Service Menu** displays:

```
 ----------------------------------------------------------------------
   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. Type the numeral corresponding to ProtecTIER Configuration and press Enter. The ProtecTIER Configuration menu displays:

```
-------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
           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
15) OS images Management (...)

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

4. Type the numeral corresponding to File Systems Management and press Enter.
   The File Systems Management menu displays.

```
-----------------------------------------------------------------------
 ProtecTIER Service Menu running on rasddx
           ProtecTIER Configuration (...)
           File Systems Management (...)
-----------------------------------------------------------------------
 1) Configure file systems on all available devices
 2) Create file system(s) on a single unused device
 3) Extend a file system with a new unused device
 4) Update /etc/fstab
 5) Display configured devices
 6) Display unused devices
 7) Display GFS repository file systems
 8) Display unused GFS file systems
 9) Increase capacity completion (applicable for a second cluster node)

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

5. To create file systems on new available multipath devices, type the numeral
   corresponding to Configure file systems on all available devices and press
   Enter. A list of all unused devices is displayed. You must confirm your choice
   to continue. An example follows:

```
Begin Processing Procedure
Devices to be configured
Device:         Size:           Status
1. mpath3       2287248.00M     Unused

Please confirm:? (yes|no)
```

6. Type y to confirm. An example follows:

```
┌─────────────────────────────────────────────────────────────────────────────┐
│  Stopping Remote Cluster Services                                 [ Done ]    │
│                                                                               │
│  Creating physical volume                                         [ Done ]    │
│  Creating volume group                                            [ Done ]    │
│  Creating logical volume                                          [ Done ]    │
│  Creating file system                                             [ Done ]    │
│  Successful capacity upgrade                                                  │
│                                                                               │
│  Display all devices and configuration status                                │
│     Device:      Size:             Status                                     │
│  1. mpath0       2048.00M          Configured                                 │
│  2. mpath1       2285200.00M       Configured                                 │
│  3. mpath2       2287248.00M       Configured                                 │
│  4. mpath3       2287248.00M       Configured                                 │
│                                                                               │
│                                                                               │
│                                                                               │
│  End Processing Procedure Successfully                                        │
│                                                                               │
│  Press <ENTER> to continue                                                    │
└─────────────────────────────────────────────────────────────────────────────┘
```

What to do next

If you have to add file systems to existing metadata file systems, proceed to "Using the ProtecTIER Service Menu to expand existing file systems" on page 52. Otherwise, go to "Expanding the repository."

If you do not want to continue with expanding the repository at this stage, continue to "Completing the increase capacity operation" on page 59 to complete the increase capacity procedure for a two-node cluster configuration.

Expanding the repository

Use ProtecTIER Manager to expand the repository by incorporating the information that is generated during the repository expansion planning process.

About this task

Note: For clustered configurations, ensure that both Server A and Server B are powered on and running before you increase capacity on Server A. If Server B is powered off while you increase capacity on Server A, pay attention to the state of vtfd when you run the **Increase capacity completion** operation on Server B. In this case, vtfd must be offline.

Access ProtecTIER Manager to expand the repository:

Procedure

1. In the Systems Management view, expand the drop-down list and select the system for which you want to expand the repository.
2. Select **Repository** > **Increase capacity**. The **Increase capacity** wizard **Welcome** screen is displayed.
3. Click **Next**. The **Repository size properties** screen is displayed.
4. In the **Repository size** field, enter the physical size, in terabytes, to which you want to expand the repository.
5. In the **Estimated factoring ratio** field, enter the factoring ratio value that you estimate for the expanded repository.
6. Select the **MD Raid configuration** from the options in the drop-down list.

7. Select the **Disk size**, in GB, from the options in the drop-down list.

8. Click **Next**. The **Repository resources** screen is displayed. The **Allocated metadata size** and **Allocated user data size** field values are automatically generated based on the values that are entered in the **Repository size properties** screen.

9. From the **Repository resources** dialog, click **Advanced**. The **Repository resources** window is displayed with a list of available file systems for metadata and user data.

Figure 10. Repository resources dialog

10. Select file systems from the **Available file systems** list and click the arrows to the left and right of the column to add available file systems to either the metadata column or the user data column.

11. Click **Ok**. The **Repository resources** dialog closes.

12. Click **Next**. A summary report is displayed with the new configuration.

13. Click **Finish**. The **Increase capacity** wizard closes and the ProtecTIER system temporarily goes offline to increase the repository capacity.

   When the system comes back online, you can resume use of your ProtecTIER system.

What to do next

If you are working in a single node configuration, the increase capacity operation is now complete and you can resume use of your ProtecTIER system. If you are working in a clustered configuration, access the ProtecTIER Service menu on Server B and run the **Increase capacity completion** operation. Go to "Completing the increase capacity operation" on page 59.

Completing the increase capacity operation

This task explains how to complete the increase capacity procedure for a two-node cluster configuration only. If you are working in a single node configuration, the increase capacity operation is already complete and you can resume use of your ProtecTIER system.

About this task

Note: If you are working on a clustered system, perform the following procedures on Server B.

Procedure

1. Log in to Server B of the cluster. Open a Secured Shell (SSH) session to the node and log in using the user ID: **root** and password: **admin**.

2. At the command line type **menu** and then press Enter. The **ProtecTIER Service Menu** displays:

```
-------------------------------------------------------------------------
  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. Type the numeral corresponding to ProtecTIER Configuration and press Enter. The ProtecTIER Configuration menu displays:

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
            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
 15) OS images Management (...)

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

4. Type the numeral corresponding to File Systems Management and press Enter. The **File Systems Management** menu displays.

```
  -----------------------------------------------------------------------
   ProtecTIER Service Menu running on rasddx
              ProtecTIER Configuration (...)
              File Systems Management (...)
  -----------------------------------------------------------------------
    1) Configure file systems on all available devices
    2) Create file system(s) on a single unused device
    3) Extend a file system with a new unused device
    4) Update /etc/fstab
    5) Display configured devices
    6) Display unused devices
    7) Display GFS repository file systems
    8) Display unused GFS file systems
    9) Increase capacity completion (applicable for a second cluster node)

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

5. Type the numeral corresponding to `Increase capacity completion`
   (`applicable for a second cluster node`) and press Enter. All the necessary
   actions are performed automatically. An example follows:

```
Begin Processing Procedure

Stopping Cluster Services                                    [ Done ]
Refreshing storage                                           [ Done ]
Starting cluster                                             [ Done ]
Starting RAS                                                 [ Done ]
Comparing storage                                            [ Done ]
Updating fstab                                               [ Done ]
Starting VTFD                                                [ Done ]
procedure ended successfully

End Processing Procedure Successfully
```

6. Press Enter to continue.

Defragmentation on a repository

Defragmentation is the process to allocate fragmented space on a repository as
defragmented so that this space can be used to write new data.

Important: Contact a trained ProtecTIER specialist before performing this
operation.

A ProtecTIER repository becomes fragmented over time. The **Defragmentation
control** operation gathers the fragmented (i.e. free, but unusable) space together in
order to improve the speed of reading and writing new data to the repository.

Reserve space for backup for VTL

This topic describes the **Reserve space for backup** feature for a VTL which
provides the ability to exclusively assign a portion of a hub repository's capacity
for local backups.

In cases of large deployments, with many remote systems (i.e., "sources")
replicating back to the replication and backup target in the main DR center (i.e.,
the "destination"), the replication process may fill, or nearly fill, all the space in the
hub repository, leaving insufficient space for backup data. Since the assumption is
that backup has precedence over replication, this feature ensures that the

designated capacity is reserved only for local backup during replication, so that replication cannot be written to the reserved portion of the storage capacity. Error notifications will appear in the event that the capacity reserved on the repository hub is running out of space for the local backup, or for replication.

- If there is no replication, backup data can stream into the repository and fill the entire storage capacity.
- If there is replication going on, backup data can stream into the repository and fill the entire reserved space for backup, while replication data streams into the repository and fills the remainder of the storage capacity. Keep in mind that replication and backup data compete for this space.

To reserve space for backup on a destination repository:
1. From the System's Management view, choose a system from the navigation pane.
2. Select **Reserve space for backup** from the **VT** menu. The **Reserve space for backup** window displays the minimum amount of nominal space that is currently reserved for backup.
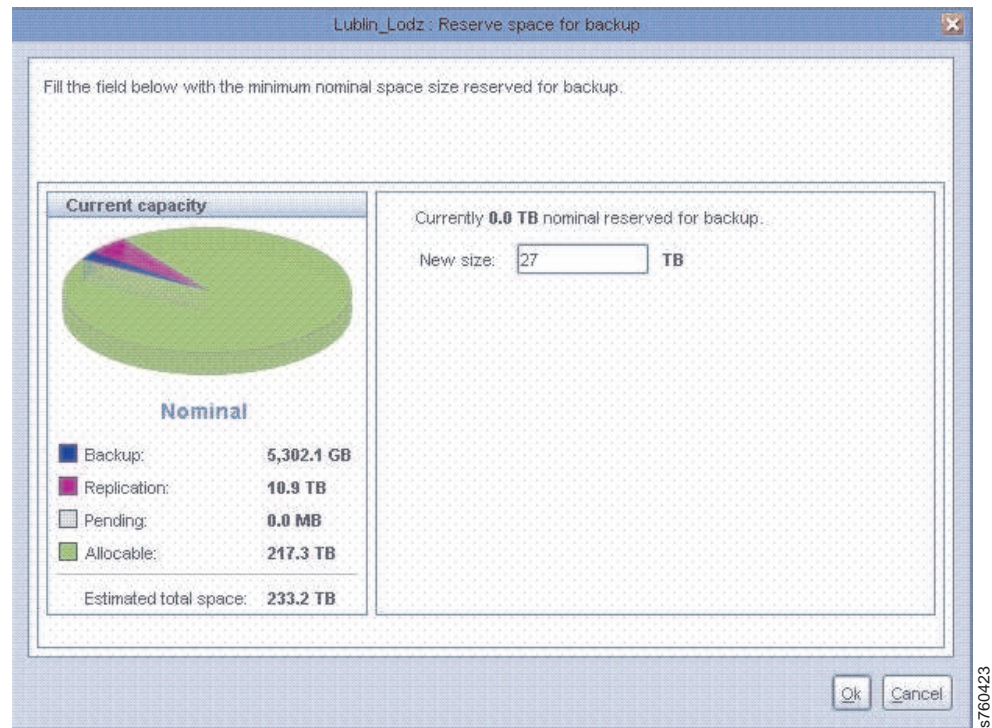
Figure 11. Reserve space for backup window

3. Enter the new minimum nominal space size and click **Ok**. The operation is complete and space for backup is reserved on the repository.

Go on to Chapter 9, "Managing the ProtecTIER Virtual Tape service," on page 83.

Deleting repositories

Complete this task to delete a repository.

Before you begin

In a two-node cluster where the repository was created on one of the nodes, you must remove the second node before you delete the repository.

For more information, see "Removing and adding cluster members" on page 230.

About this task

In general, it is not necessary to delete a repository. Using ProtecTIER Manager, follow the task to delete a repository. To recreate the repository on the existing storage, you must reinstall the operating system and the ProtecTIER code. For further instructions, refer to Chapter 16, "ProtecTIER system recovery procedures," on page 235.

For more information, contact a trained ProtecTIER specialist.

Attention: Deleting the repository results in the loss of all the data contained in the repository.

Perform the following steps to delete a repository:

Procedure
1. Select the repository.
2. Choose **Repository > Delete repository**. A confirmation message box is displayed.
3. Click **Yes**. The **Data Loss Confirmation** dialog box is displayed.
4. In the field, type `data loss` and click **Ok**. A confirmation message box is displayed.
5. Click **Yes**. The ProtecTIER system temporarily goes offline to delete the repository.
6. When the system comes back online, you can resume use of your ProtecTIER system.

   Note: Before you can recreate a repository on the existing storage, contact a trained ProtecTIER specialist for assistance.

Chapter 8. Managing and monitoring ProtecTIER through the CLI

This chapter describes how to query and configure the system via the command line interface (CLI), and to receive various statistics about the ProtecTIER system. This information can provide valuable insight to the administrator on the performance, capacity, configuration and operation of the system, and can be accessed by other management applications.

A CLI is provided for adminstrators who either prefer a text interface or want to automate capture of statistical information.

Understanding the syntax diagrams

A syntax diagram uses symbols to represent the elements of a command and to specify the rules for using these elements.

Syntax diagrams

Main path line
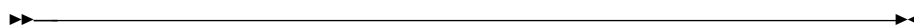
Begins on the left with double arrowheads (>>) and ends on the right with two arrowheads facing each other (><). If a diagram is longer than one line, each line to be continued ends with a single arrowhead (>) and the next line begins with a single arrowhead. Read the diagrams from left-to-right, top-to-bottom, following the main path line.

Keyword
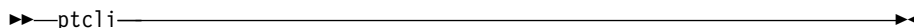
Represents the name of a command, flag, parameter, or argument. A keyword is not in italics. Spell a keyword exactly as it is shown in the syntax diagram.

Required keywords
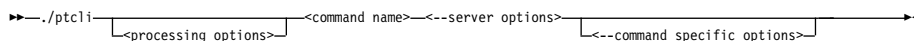
Indicate the parameters or arguments you must specify for the command. Required keywords appear on the main path line. Mutually exclusive required keywords are stacked vertically.

Optional keywords
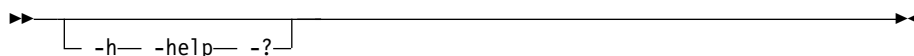
Indicate the parameters or arguments you can choose to specify for the command. Optional keywords appear below the main path line. Mutually exclusive optional keywords are stacked vertically.

Variable

➤➤──*variable*──➤◄

Represents the value you need to supply for a parameter or argument, such as a file name, user name, or password. Variables are in italics.

Special characters

- (minus) or -- (double minus)
Flags are prefixed with a - (minus) sign. Flags define the action of a command or modify the operation of a command. You can use multiple flags, followed by parameters, when you issue a command.

[ ] square brackets
Optional values are enclosed in square brackets.

| vertical bar
A vertical bar indicates that you have a choice between two or more options or arguments.

For example, [a | b] indicates that you can choose a, b, or nothing. Similarly, { a | b } indicates that you must choose either a or b.

ptcli

This topic describes how to use ptcli through the command-line interface (CLI) . The ptcli is loaded during the installation of ProtecTIER software and ProtecTIER Manager software.

Usage

When ptcli is running, the available ptcli commands are listed according to the version of ProtecTIER that is installed. If the ptcli for version 3.4.1 is running on older versions of ProtecTIER, several operations might not be supported.

Use ptcli to do any of the following tasks:
- Configure ProtecTIER (including configuration of a ProtecTIER repository and configuration of ProtecTIER virtual tape [VT] libraries).
- Monitor ProtecTIER (including statistics of ProtecTIER VT and statistics about the ProtecTIER repository).
- Snapshot and filter ProtecTIER VT cartridges (mostly used for DR (disaster recovery)_, scenerios) For more information, see "ptcli Inventory commands" on page 72.

To run ptcli on a ProtecTIER node, move into the following directory: /opt/dtc/ptcli.

To run ptcli on a host running ProtecTIER Manager, move into the ProtecTIER Manager directory (in Windows, C:\Program Files\IBM\ProtecTIER Manager).

The ptcli command is issued from the command line as follows:

```
▶▶──./ptcli──┬──────────────────────┬──<command name>──<--server options>──┬──────────────────────────────┬──▶◀
             └──<processing options>─┘                                      └──<--command specific options>─┘
```
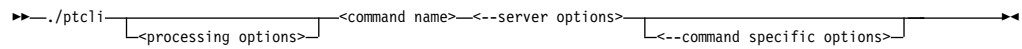
For more information, see:
- "Processing options"
- "Server options" on page 66
- "Commands" on page 67

Creating a profile

This topic describes how to create a profile in order to query the ProtecTIER server through the command line interface (CLI) using ptcli.

About this task

Creating a profile is an optional task that can be completed prior to accessing the ptcli. Creating a profile provides for the user name and password to be saved in a file. You can always enter the user name and password manually if you choose not to create a profile. For more information on using ptcli, see "ptcli" on page 64.

Procedure

1. Activate ptcli with -p followed by a file name with full path.
2. Once prompted, enter the desired user name and password. This step creates the user-specified file with the user name and password that is needed for login.

Example

Note: In the following example, \ptcli is the root directory. Keep in mind that running the command does not create the directory path. Therefore, for the command to work, the root directory (in this case \ptcli) must be created before activating the command.

```
ptcli -p h:\ptcli\ptuser
User name: ptuser
Password:
<?xml version="1.0" encoding="UTF-8"?
<response command="createprofile" status="success"/>
```

Processing options

This topic describes how to use the processing options to query the ProtecTIER server through the command line interface (CLI).

Usage

You can specify the following processing options at the beginning of the command string:

Table 3. Processing options

Processing options	Explanation
`--debug <debug level>`	Specify the debug level to print log messages to the console. Choices for the debug level are as follows: • SEVERE • WARNING • ALL
`[-h (--help)]`	Prints the Help message to the console and exits.
`[-v (--version]`	Prints the version information and exits.
`[-p (--createprofile) FILE]`	Creates or modifies the user profile file. This file is used for logging into the management server.

Server options

This topic describes the server options to use when querying the ProtecTIER server through the command line interface (CLI). Server options are used for connection to the management server. They should appear with each query/action - except for the arguments `-h` or `-v`.

Usage

Note: Administrator privileges are required for configuration operations.

You can specify the following server options at the beginning of the command string:

Table 4. Server options

Server options	Explanation
`--ip <IP>`	Specify the IP address of the management server. This field is required if you are running `ptcli` from a server or PC that is not the ProtecTIER server to which you want to connect.
`[--port <PORT>]`	Specify the port of the management server. The default is: 3501. **Note:** This is optional.
`[--loginFile <FILE>]`	Specify a user profile file for login. **Notes:** • This is optional. • When specifying --loginFile, using --loginInline is mutually exclusive.
`[--loginInline <USERNAME,PASSWORD>]`	Specify a login using the user name and password. **Notes:** • This is optional. • When specifying --loginInline, using --loginFile is mutually exclusive.
`[--force]`	Force the login if another administrator is already logged in. **Note:** This is optional.

Commands

The following tables contain lists of commands to invoke on the management server.

For information about ProtecTIER VT commands, see "ProtecTIER VT commands" on page 68.

For information about ProtecTIER Repository commands, see "ProtecTIER repository commands."

ProtecTIER repository commands

The following tables contain lists of commands to invoke on the ProtecTIER repository.

Table 5. CreateRepository Command

Command	Explanation	Command Specific Options	
		Name	**Explanation**
CreateRepository	Create a repository	--name <NAME>	Repository name
		--system <NAME>	System name
		--size <SIZE>	Repository physical maximum size in TB
		--peak <NUM>	Peak throughput in MB
		--ratio <NUM>	Deduplication ratio
		--raid <X,Y,Z>	Metadata raid configuration in the form of [X,Y,Z] where (X = Type), (Y = Members) and (Z = Disk size in GB) taken from "RaidConfiguations" output
		[--metadata <MOUNT_POINTS>]	List of GFS (global file system) mounted file systems used to store ProtecTIER repository metadata
		[--userdata <MOUNT_POINTS>]	List of GFS mounted file systems used to store ProtecTIER repository user data

Example:

CreateRepository

►►─./ptcli─CreateRepository─── *ip 9.148.220.101* ──-loginFile─ *h:\ptcli\ptadmin* ─┤ Command Specific Options ├──────────────►◄

Command Specific Options:

├── *--name─PTCLI_REP* ───system─ *PTCLI_SYS* ──-size─ *2* ───peak─ *300* ───ratio─ *13* ───raid─ *FC-10K,4+4,120* ─┤ Command specific options ├──────────────┤

Command specific options:

├──┬─────────────────────────────┬──┬─────────────────────────────┬──────────────────────┤
   └── *--metadata─<MOUNT_POINTS>* ─┘ └── *--userdata─<MOUNT_POINTS>* ─┘

Table 6. AddClusterMember Command

Command	Explanation	Command Specific Options	
		Name	**Explanation**
AddClusterMember	Add cluster member	--addip <IP>	External IP of the node to add to the cluster
Example:			
AddClusterMember			
▶▶──./ptcli──AddClusterMember───*ip 9.148.220.102*───loginFile──*h:\ptcli\ptadmin*───addip──*9.148.220.101*───────────▶◀			

Table 7. RaidConfigurations Command

Command	Explanation
RaidConfigurations	Prints information about the supported raid configurations
Example:	
RaidConfigurations	
▶▶──./ptcli──RaidConfigurations───*ip 9.148.220.101*───loginFile──*h:\ptcli\ptadmin*──────────────────▶◀	

Table 8. RepositoryStatistics Command

Command	Explanation
RepositoryStatistics	Prints the repository statistics
Example:	
RepositoryStatistics	
▶▶──./ptcli──RepositoryStatistics───*ip 9.148.220.101*───loginFile──*h:\ptcli\ptadmin*──────────────────▶◀	

Table 9. ServerVersion Command

Command	Explanation
ServerVersion	Prints the server version
Example:	
ServerVersion	
▶▶──./ptcli──ServerVersion───*ip 9.148.220.101*───loginFile──*h:\ptcli\ptadmin*──────────────────▶◀	

ProtecTIER VT commands

The following tables contain lists of commands to invoke on the virtual tape library.

ptcli Configuration commands

This topic describes how to configure the ProtecTIER server through the command line interface (CLI) using Configuration commands.

Table 10. AddCartridges command

Command	Explanation	Command Specific Options	
		Name	Explanation
AddCartridges	Add Cartridges	`--name <NAME>`	Library name (taken from "Libraries" output)
		`--cartridges <NUM>`	Number of cartridges
		`[--maxcartsize <NUM>]`	Maximum cartridge growth in MB. If not specified, the size is not limited.
		`--seed <SEED>`	Bar code seed

Example:

AddCartridges

▶▶──`./ptcli`──`AddCartridges`──`--ip 9.148.220.45`──`--loginFile`──`h:\ptcli\ptadmin`──┤ Command Specific Options ├──────────────◀

Command Specific Options:

├────`--name`──`Lib`──`--cartridges`──`200`──`--seed`──`TS0000`──────────────────────────────────┤
                             └─`[--maxcartsize]`──`NUM`─┘

Table 11. AddLibrary Command

Command	Explanation	Command Specific Options	
		Name	Explanation
AddLibrary	Create library	`--name <NAME>`	New library name defined when creating a library
		`[--slots <NUM>]`	Number of slots (defaults to 0)
		`--impexp <NUM>`	Number of import/export (defaults to 8)
		`--libtype <NAME>`	Library type (taken from "LibraryTypes" output
		`--robot X,Y`	List of robot assignments in the form of [X,Y] where (X = Node external IP), (Y = Port)
		`--drivemodel <NAME>`	Tape drive model (taken from "DriveModels" output)
		`[--drives X,Y,Z]`	List of drive assignments in the form of [X,Y,Z] where (X = Number of drives), (Y = Node external IP), and (Z = Port)

Table 11. AddLibrary Command (continued)

Command	Explanation	Command Specific Options

Example:
 	
AddLibrary
 	
►►──./ptcli─AddLibrary──*--ip 9.148.220.45*──-loginFile─*h:\ptcli\ptadmin*─┤ Command Specific Options ├────────────►◄
 	
Command Specific Options:
 	
├────--name─*Lib1*────────────────--impexp─*5*──-libtype─*TS3500*──-drivemodel─*ULT3580-TD3*────────────┤
          └─[--slots]─*30*─┘
 	
├──-robot─*9.148.220.45,0*──-robot─*7,168.159.150.33,0*──────────────────────────────┤
                └[--drives]─*5,9.148.220.45,0*┘ └[--drives]─*7,168.159.150.33,0*┘		

ptcli Throughput statistics

This topic describes how to view the ProtecTIER server statistics history through
the command-line interface (CLI).

Table 12. NodeVtlStatistics Command

Command	Explanation	Command Specific Options	
		Name	**Explanation**
NodeVtlStatistics	Prints the statistics history on the local host	--hours <NUM>	The number of statistics hours included in the output. By default, the output includes four chronicles (statistic records) per hour (if uptime >= hours).
Example: **NodeVtlStatistics** ►►───./ptcli─NodeVtlStatistics───*--ip 9.148.220.101*──-loginFile─*h:\ptcli\ptadmin*───-hours─*1*───────────►◄			

ptcli Library information

The tables in this topic contain lists of commands to invoke on libraries of the
ProtecTIER repository.

Table 13. CartridgeInfo Command

Command	Explanation	Command Specific Options	
		Name	**Explanation**
CartridgeInfo	Print information about specific cartridges in the library **Note:** The list is sorted by barcode.	`--name <NAME>`	Library name (taken from "Libraries" output)
		`--from <NUM>`	The number of cartridges before the first printed cartridge in the list of cartridges (the number of cartridges can be taken from "NumberOfCartridges" output)
		`--count <NUM>`	The maximum number of cartridges in the output

Example:

CartridgeInfo

```
►►──./ptcli──CartridgeInfo──--ip 9.148.220.45──--loginFile──h:\ptcli\ptadmin──┤ Command Specific Options ├──────────►◄
```
Command Specific Options:

```
├──--name──Lib──--from──0──--count──400─────────────────────────────────┤
```

Table 14. DriveModels Command

Command	Explanation	Command Specific Options	
		Name	**Explanation**
DriveModels	Prints information about the supported tape drive models	`--libtype <NAME>`	Library type (taken from "LibraryTypes" output

Example:

DriveModels

```
►►──./ptcli──DriveModels──--ip 9.148.220.101──--loginFile──h:\ptcli\ptadmin──--libtype──TS3500──────►◄
```

Table 15. Libraries Command

Command	Explanation
Libraries	Prints the list of libraries on the repository

Example:

Libraries

```
►►──./ptcli──Libraries──--ip 9.148.220.101──--loginInline──h:\ptcli\ptadmin────────────────►◄
```

Table 16. LibraryInformation Command

Command	Explanation	Command Specific Options	
		Name	**Explanation**
LibraryInfo	Prints information about a specific library in the repository	--name \<NAME>	Library name (taken from "Libraries" output
Example: **LibraryInformation** ▶▶──./ptcli──LibraryInfo──*--ip 9.148.220.101*───--loginInline──*h:\ptcli\ptadmin*───--name──*Lib*────────▶◀			

Table 17. LibraryTypes Command

Command	Explanation
LibraryTypes	Prints information about a specific library in the repository
Example: **LibraryTypes** ▶▶──./ptcli──LibraryTypes───*--ip 9.148.220.101*───--loginFile──*h:\ptcli\ptadmin*────────────────────▶◀	

Table 18. NumberofCartridges Command

Command	Explanation	Command Specific Options	
		Name	**Explanation**
NumberOfCartridges	Prints the number of cartridges in the library	--name \<NAME>	Library name (taken from "Libraries" output
Example: **NumberOfCartridges** ▶▶──./ptcli──NumberOfCartridges───*--ip 9.148.220.101*───--loginFile──*h:\ptcli\ptadmin*───--name──*Lib*────────▶◀			

ptcli Inventory commands

This topic describes how to query the ProtecTIER server through the command line interface (CLI) using **Inventory** commands.

Usage

The Inventory command options are used to filter cartridges in a ProtecTIER repository using a variety of criteria. Also, these options can be used to move cartridges that match a certain criteria. Before beginning to filter the cartridges, and/or moving cartridges using the CLI, you must first create a snapshot of the cartridges using the InventoryRefresh command. (See Table 19 on page 73.) The snapshot will include the most updated properties of the cartridges at the time it is created.

Note: Any filter/move operation is executed using the snapshot's contents. Running such a command without a previous refresh is considered an error. Also,

for larger repositories, a refresh operation may take considerable time and reduce ProtecTIER's performance during that time.

Moving a cartridge using the CLI may fail if the snapshot is not up to date for the cartridge (for instance, if the cartridge is moved or deleted after a snapshot is taken). Operations on libraries for which the snapshot is not up to date may have undesirable consequences.

Table 19. InventoryRefresh command

Command	Explanation
`InventoryRefresh`	Refresh the cartridges inventory snapshot on the server.
Example: **InventoryRefresh** `►►──./ptcli──InventoryRefresh──--ip 9.148.220.101──--loginFile──h:\ptcli\ptadmin────────────►◄`	

Table 20. InventoryFilter command

Command	Explanation	Command Specific Options	
		Name	**Explanation**
`InventoryFilter`	Queries the cartridges inventory snapshot created by the `InventoryRefresh` command.	`--querytype <QUERYTYPE>`	Type of query to be used by the command: • **All** - All cartridges in the ProtecTIER repository. • **Replica** - All cartridges that were replicated *into* this repository. • **Origin** - All cartridges that were replicated *from* this repository.
		`--query <QUERY>`	Query to be used by the filter command. See "Query" on page 77 for more information.
		`[--output <PATH>]`	The output file path for the query results.
		`[--limit <NUM>]`	The limit for the maximal number of cartridges the query may return.

Example:
 	
InventoryFilter
 	
`►►──./ptcli──InventoryFilter──--ip 9.148.220.101──--loginFile──h:\ptcli\ptadmin──┤ Command Specific Options ├──────►◄`
 	
Command Specific Options:
 	
`├──--querytype──replica──--query──"in_sync = true"──────────────────────────────────────┤`
`                                            └[--output]──<PATH>┘  └[--limit]──<NUM>┘`			

Table 21. InventoryGetQueryFields command

Command	Explanation	Command Specific Options	
		Name	**Explanation**
InventoryGetQueryFields	Returns the fields available for the specified query type	`--querytype <QUERYTYPE>`	Type of query to be used by the command: • **All** - All cartridges in the ProtecTIER repository. • **Replica** - All cartridges that were replicated *into* this repository. • **Origin** - All cartridges that were replicated *from* this repository. See "Query" on page 77 for more information.

Example:

InventoryGetQueryFields

▶▶──./ptcli──InventoryGetQueryFields───*--ip 9.148.220.101*───--loginFile──*h:\ptcli\ptadmin*───--querytype──*all*──────────▶◀

Table 22. InventoryMoveFile command

Command	Explanation	Command Specific Options	
		Name	**Explanation**
InventoryMoveFile	Move a group of cartridges expressed as a file (created manually or using the `InventoryFilter` command).	`--filetype <TYPE>`	The type of the file to be used by the command: • **All** - All cartridges in the ProtecTIER repository. • **Replica** - All cartridges that were replicated *into* this repository. • **Origin** - All cartridges that were replicated *from* this repository. • **barcode** - Lists the barcodes of cartridges in the repository to be moved.
		`--file <PATH>`	The path to a file containing a list of cartridges to be moved
		`--destination <NAME>`	The destination library (or shelf) of the move command

Table 22. InventoryMoveFile command (continued)

Command	Explanation	Command Specific Options
Example:		

InventoryMoveFile

►►──./ptcli─InventoryMoveFile──--ip 9.148.220.45──--loginFile─h:\ptcli\ptadmin─┤ Command Specific Options ├──────────►◄

Command Specific Options:

├──--filetype─replica──--file─/temp/inventory/if2.csv──--destination─shelf──────────────┤

Table 23. InventoryMoveFilter command

Command	Explanation	Command Specific Options	
		Name	**Explanation**
InventoryMoveFilter	Move a group of cartridges (that match a given query)	--querytype <QUERYTYPE>	The type of the query to be used by the command: • **All** - All cartridges in the ProtecTIER repository. • **Replica** - All cartridges that were replicated *into* this repository. • **Origin** - All cartridges that were replicated *from* this repository.
		--query <QUERY>	The query to be used by the filter command See "Query" on page 77 for more information.
		--destination <NAME>	The destination library of the move command.
Example:			

InventoryMoveFilter

►►──./ptcli─InventoryMoveFilter──--ip 9.148.220.45──--loginFile─h:\ptcli\ptadmin─┤ Command Specific Options ├──────────►◄

Command Specific Options:

├──--querytype─replica──--query─"in_synch = true"──--destination─shelf────────────────────┤

Table 24. InventoryStatistics command

Command	Explanation
InventoryStatistics	Display the latest information about the cartridges inventory snapshot
Example:	

InventoryStatistics

►►──./ptcli─InventoryStatistics──--ip 9.148.220.101──--loginFile─h:\ptcli\ptadmin─────────────────►◄

Table 25. InventoryDeleteFile command

Command	Explanation	Command Specific Options	
		Name	**Explanation**
InventoryDeleteFile	Delete a group of cartridges (expressed as a file).	`--filetype <TYPE>`	The type of the file to be used by the command: • **All** - All cartridges in the ProtecTIER repository. • **Replica** - All cartridges that were replicated *into* this repository. • **Origin** - All cartridges that were replicated *from* this repository. • **barcode** - Lists the barcodes of cartridges in the repository to be deleted.
		`--file <PATH>`	The path to a file containing a list of cartridges to be deleted
		`--shelf`	Flag indicating that the cartridges are located in Shelf. Choose this option or Library option.
		`--library <NAME>`	Flag indicating that the cartridges located in the library <NAME>. Choose this option or Shelf option.

Example:

InventoryDeleteFile

►►─┈./ptcli─InventoryDeleteFile──*-ip 9.148.220.88*──-loginFile─*h:\ptcli\ptadmin*─┤ Command Specific Options ├────────────►◄

Command Specific Options:

├──┈--filetype─*all*──┈--file─*/temp/inventory/if2.csv*──┈--shelf─────────────────────────────────┤

Table 26. InventoryDeleteFilter command

Command	Explanation	Command Specific Options	
		Name	**Explanation**
`InventoryDeleteFilter`	Delete a group of cartridges (expressed as a filter).	`--querytype <QUERYTYPE>`	The type of the file to be used by the command: • **All** - All cartridges in the ProtecTIER repository. • **Replica** - All cartridges that were replicated *into* this repository. • **Origin** - All cartridges that were replicated *from* this repository.
		`--query <QUERY>`	The query to be used by the filter command. See "Query"
		`--shelf`	Flag indicating that the cartridges are located in Shelf. Choose this option or Library option.
		`--library <NAME>`	Flag indicating that the cartridges located in the library <NAME>. Choose this option or Shelf option.

Example:

InventoryDeleteFilter

►►——./ptcli——InventoryDeleteFilter——--ip 9.148.220.88——-loginFile——h:\ptcli\ptadmin——| Command Specific Options |————————►◄

Command Specific Options:

├———--querytype——all——-query——"barcode>='000811' AND barcode<="000830'"——-shelf————————————————————┤

Query

This topic describes what a query is and how to use it in Inventory commands.

A query is a statement in which the user can put one of the following:
• White spaces
• Numbers
• Tokens: and/or/not/is/in/between
• String literals (within single quotes): 'AB0000'
• Boolean: TRUE/FALSE/true/false
• Column names as defined by the column names of the query type
• Date: the date format in a query is as follows: datetime('2009-12-27' 08:23:00)

Results can be saved in a .csv file using the --output command switch.

The .csv file can be used as an input to a CLI move command. This .csv file can be partially edited by the user by removing lines (each line represents a cartridge).

User can also create his own barcodes file, and to use this as an input to a move command.

Cartridges set and query type

A filter is always working on the specified set of cartridges:

- *All: All cartridges in the ProtecTIER repository.*

  cart_unique_id
  An internal unique id for a cartridge.

  barcode
  Barcode number.

  nominal_size_in_bytes
  Nominal size measured in bytes.

  last_access_time
  Last access time.

  media_type
  The media type could be L3 for LTO3, L2 for LTO2 or none for DLT.

  read-only
  An indication of the write protection status of the cartridge. True means it is read only and can't be written on. False means it can be written on.

  principality_grid_id
  The Grid ID of the repository that owns the cartridge.

  principality_repository_id
  The ID of the repository within the Grid that owns the cartridge.

  container_name
  Could be only in a single container in a point in time.

  Note: Grid ID will be common to all repositories within a Grid. Repository ID is unique within a Grid.

- *Replica: All cartridges that were replicated into this repository.*

  Note: This is relevant from the stand point of a *Hub*, or in 3.1 a *Target* cartridge

  cart_unique_id
  An internal unique id for a cartridge.

  barcode
  Barcode number.

  nominal_size_in_bytes
  Nominal size measured in bytes.

  last_access_time
  Last access time.

  media type
  The media type could be L3 for LTO3, L2 for LTO2 or none for DLT.

  read-only
  An indication of the write protection status of the cartridge. True means it is read only and can't be written on. False means it can be written on.

  principality_grid_id
  The Grid ID of the repository that owns the cartridge

principality_repository_id
> The ID of the repository within the Grid that owns the cartridge

container_name
> Shelf or library name. Could be only in a single container in a point in time.

last_update_time
> The last time the nominal size was updated - either by backup (in the source) or by replication (at the destination).

source_repository_id_for_last_sync_point
> The ID of the repository this cartridge was replicated from.

source_grid_id_for_last_sync_point
> The ID of the grid this cartridge was replicated from.

source_time_for_last_sync_point
> The time this cartridge was last synchronized with the source, in source clock. For example if the last replication ended at 09:23 according to source clock, and 11:23 according to destination clock, then this will show 09:23.

destination_time_for_last_sync_point
> The time this cartridge was last synchronized with the source, in destination clock. For example if the last replication ended at 09:23 according to source clock, and 11:23 according to destination clock, then this will show 11:23.

in_sync
> Shows if this cartridge is the same as in the source or not. When starting backup at the source this will turn to false. When the replication for this cartridge ends, it will turn to true. Note: this is synchronized only if there is a connection between the source and the destionation. To know what is the time this flag is true, look at the "last sync point" fields above.

- *Origin: All cartridges that were replicated from this repository.*

Note: This is relevant from the stand point of a Spoke, or in 3.1, an Origin cartridge.

cart_unique_id
> This is an internal unique id for a cartridge

barcode
> Barcode number.

nominal_size_in_bytes
> Nominal size measure in bytes.

last_access_time
> Last access time.

media_type
> The media type could be L3 for LTO3, L2 for LTO2 or none for DLT.

read-only
> An indication of the write protection status of the cartridge. True means it is read only and can't be written on. False means it can be written on.

principality_grid_id
> The Grid ID of the repository that owns the cartridge

principality_repository_id
> The ID of the repository within the Grid that owns the cartridge

container_name
> Shelf or library name where the cartridge exists.

destination_repository_id
> The ID of the repository within the Grid that this cartridge was replicated into.

destination_grid_id
> The Grid ID of the repository that this cartridge was replicated into.

last_replication_time
> This is the time when the last DFS file (last data unit) was replicated to the destination.

last_sync_time
> The recent time that the cartridge was being synced with the destination.

replicated_size
> The nominal size (in bytes) replicated to that destination for this cartridge.

backlog_size
> The nominal size of the backlog for this cartridge relative to the destination. This is how much left to replicate for this cartridge to the destination - only for cartridges that have triggers (need to replicate or being replicated).

The set of cartridges is stated in the CLI command as 'querytype'. So the query type can be: 'all', 'replica', 'origin'.

Part 2. Working with ProtecTIER for VTL

This section of the guide describes how to work with ProtecTIER for VTL.

Chapter 9. Managing the ProtecTIER Virtual Tape service

The ProtecTIER system provides many functions to managing the ProtecTIER Virtual Tape (VT) service.

About this task

The ProtecTIER system has a rich set of library management functions. A virtual tape library emulates a physical tape library. The ProtecTIER system emulates the library installation, library expansion, cartridge management, drive addition, and drive allocation.

Setting the ProtecTIER VT host connections

This topic describes how the ProtecTIER front-end ports are connected.

Connect the ProtecTIER front-end ports to your backup environment. ProtecTIER front-end ports can be connected either in FC loop topology or through fibre channel switches.

Important: When modifying the front-end connectivity, it is recommended that Loop topology be used for direct connection and P2P when fibre channel switches are being used. If the topology is set to Loop in a fibre channel switch connection, the link will go down.

For more information on modifying port attributes, see "Modifying port attributes" on page 229.

If fibre channel switches are used, you must create zones to set up the appropriate fibre channel connectivity between the ProtecTIER front-end ports and the fibre channel ports in your backup environment.

Attention: The switch should be installed and correctly cabled before beginning the configuration. For details, see the documentation provided with the switch.

Note: The *Scan port* function can be used to determine if host adapters are visible to ProtecTIER. For more information, see "Fibre Channel port attributes of a node" on page 152.

Creating the zones

A ProtecTIER server front-end port shares zones with only backup server FC ports. Each zone contains only one ProtecTIER front-end port.

Zoning can be defined by switch ports or by worldwide Names (WWNs).

Creating libraries

Complete this task to create a library for your ProtecTIER system.

Before you begin

Ensure that the following items are performed before proceeding with this task:

- Check with your administrator about the number of drives and cartridges supported by your application.
- The virtual devices of the library are assigned to ProtecTIER server ports. Use the Scan button of the Port attributes pane to verify that the ProtecTIER server ports are connected to the correct host.

About this task

A library can be created on a ProtecTIER system of either one node or two nodes.

Note: Check with your backup application administrator to ensure the number of drives and cartridges supported by your application.

	TS7650G
Maximum number of libraries	64
Maximum number of virtual drives	256 (dual-node 512)

Note: The ProtecTIER server ports to which the virtual devices of the library are assigned must be connected to the correct host. Use the Scan button of the Port attributes pane to verify the port connections to the correct host. For more information, see "Fibre Channel port attributes of a node" on page 152.

If your ProtecTIER node has ports connected to a host that is running HP-UX, you must verify that the ports are configured as HP-UX ports. Use the **Flat addressing mode** function from the **Host Initiators Management** screen to verify port configuration. For more information, see "Managing host initiators" on page 107 and "Manually adding host initiators" on page 108. If these conditions are not met, the host might not be able to detect all of the virtual tape drives.

Perform the following steps to create the library:

Procedure

1. Select a cluster on which to add a library.
2. From the toolbar, click the **Create new library** button. The **Create new library** wizard **Welcome** screen is displayed.
3. Click **Next**. The **Library details** screen is displayed.
4. In the **VT name** field, enter a name for the library.
5. Click **Next**. The **Library type** screen is displayed.
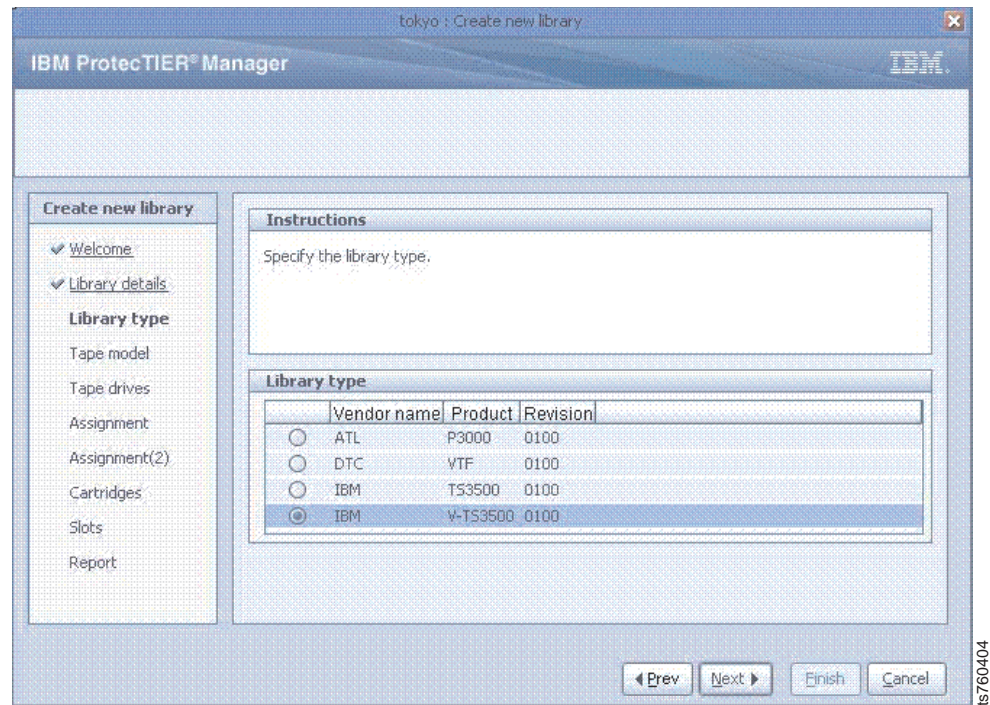
Figure 12. Library type screen

6. Select **IBM TS3500 0100** as the type of physical library model that you want the virtual library to emulate:

   Note: For more information, see "Setting the library type" on page 91.
   - ATL P3000 0100
   - IBM TS3500 0100

   You can also configure the virtual library models:
   - DTC VTF 0100
   - IBM V-TS3500 0100

   Note: Verify that the backup application that you are using supports the type of library model that you select for a virtual tape system. Refer to the *TS7650 Support Matrix* at: http://www-01.ibm.com/common/ssi/cgi-bin/ ssialias?infotype=SA&subtype=WH&htmlfid=IVL12348USEN .

7. Click **Next**. The **Tape model** screen is displayed.
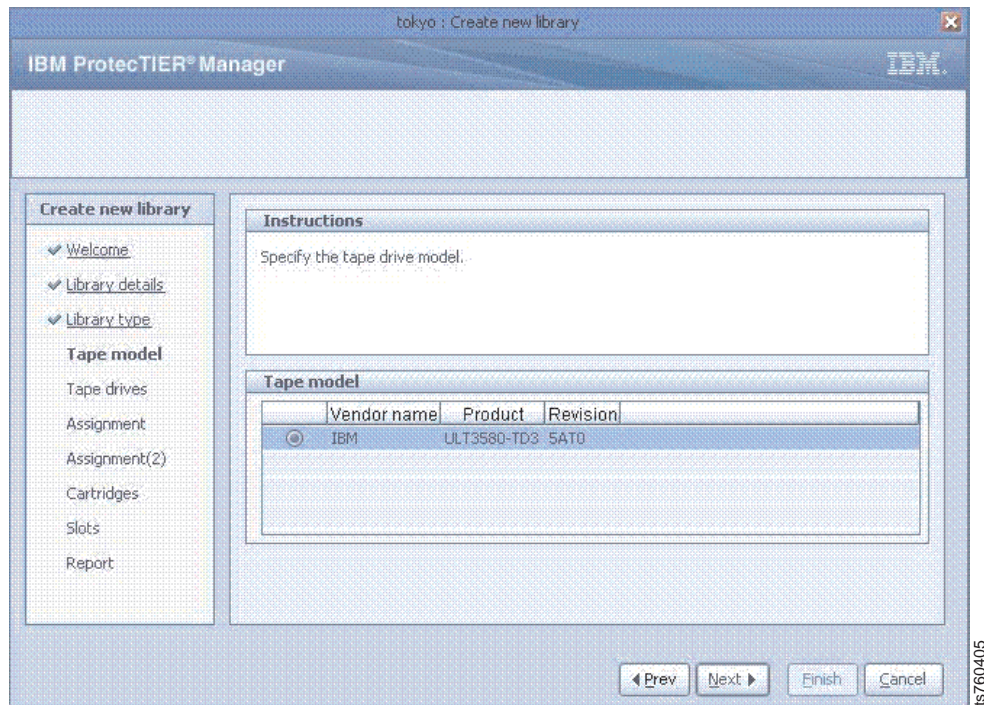
Figure 13. Tape model screen

8. Select the type of tape drive model that you want the virtual library to emulate. The type of tape drive depends on the library type chosen:
   - IBM ULT3580-TD3 (IBM LTO3)

   Note: All tape drives in the library are of this type after your selection, including tape drives added at a later time.
9. Click **Next**. The **Tape drives** screen is displayed.
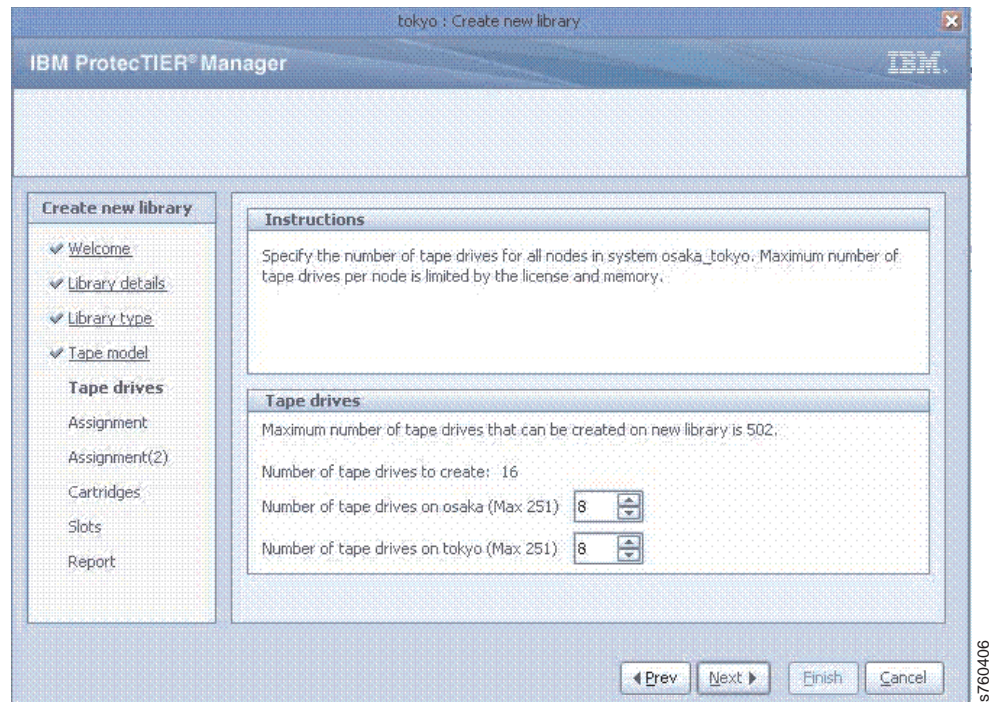
Figure 14. Tape drives screen

10. In the **Number of tape drives** field for each node, enter the number of tape drives to assign to the node. To maximize load balancing, IBM recommends that you distribute tape drives across the nodes based on the relative power of the node servers.

11. Click **Next**. The **Assignment** screen is displayed.
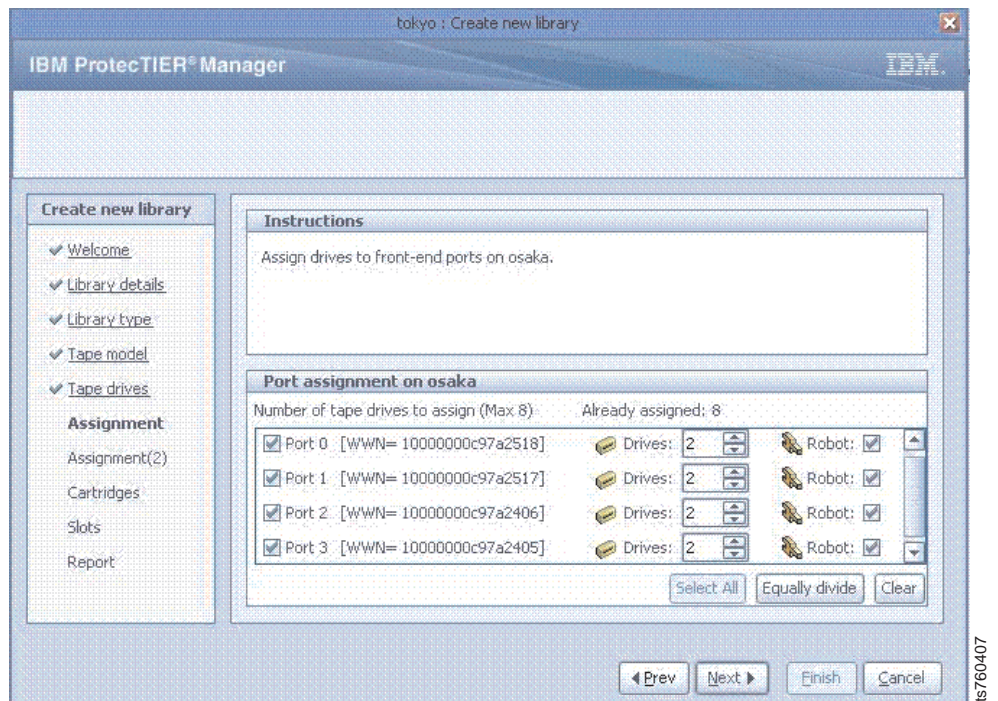
Figure 15. Port assignment screen

12. Select or clear the check boxes next to each port to define which of the node ports are assigned virtual devices.

    Note: If you have chosen an IBM library model, all the ports are selected and enabled. If you have chosen a library model other than IBM, the ports are not checked. In either case, you **must** select at least **one** port assignment that will have a robot on this node or on the second node, in the case of a cluster.

13. In the **Drives** fields corresponding to each selected port, select the number of virtual tape drives that are assigned to each port.

    Note: Optionally, click **Select All** to automatically select both ports. Click **Equally divide** to evenly divide the number of drives between the ports.

14. Check the **Robot** check box if you want the library virtual robot to be accessible through this port.

    Note: For high-availability purposes, ProtecTIER supports the assignment of the virtual robot to multiple ports.

15. Click **Next**. If a second node exists in the cluster, the **Assignment (2)** screen is displayed.
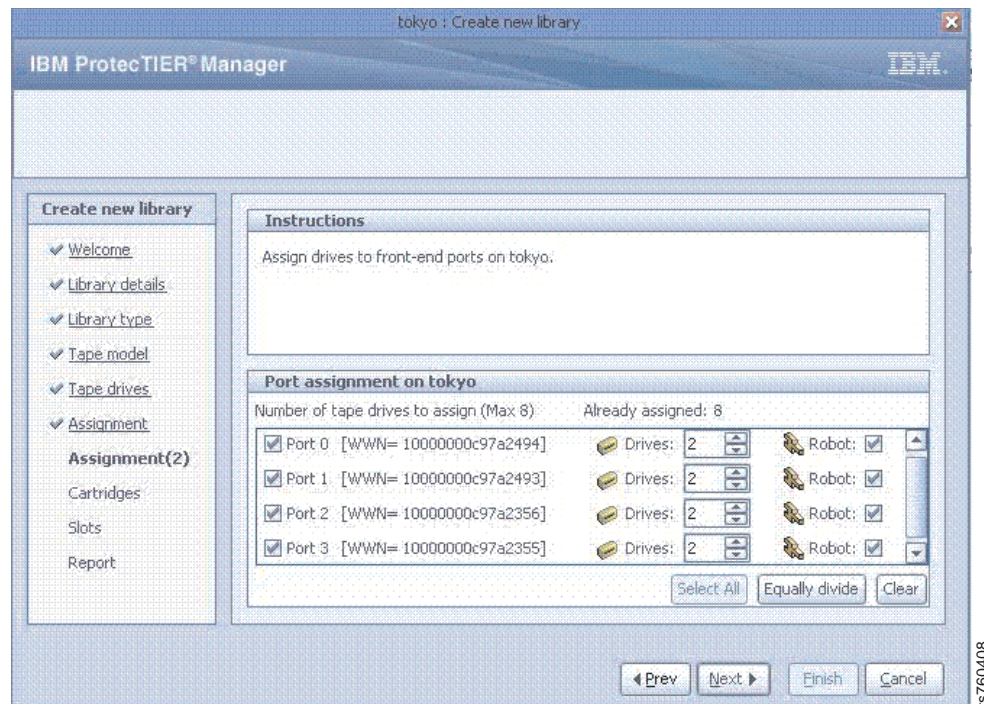
Figure 16. Assignment (2) screen

16. Repeat steps 12 and 13 for the **Assignment (2)** screen.
17. Click **Next**. The **Cartridges** screen is displayed.
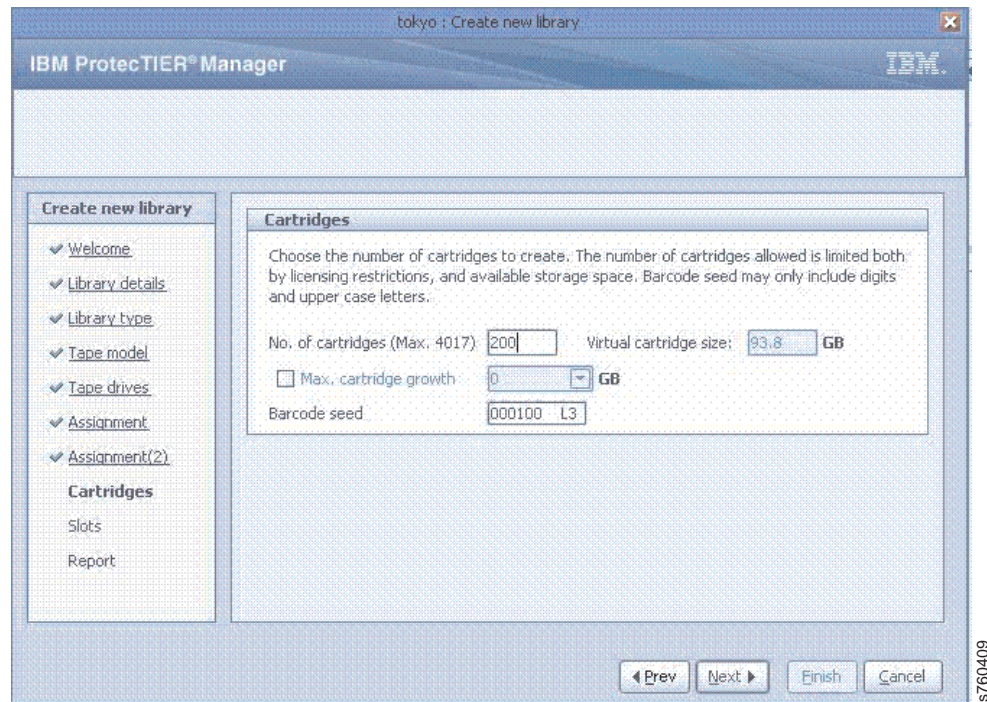
Figure 17. Cartridges screen

18. In the **No. of cartridges** field, enter the number of cartridges that you want to have in the library. The **Virtual cartridge size** field automatically displays the system for virtual cartridges. Capacity is based on the number of cartridges entered, the total amount of available storage space in your repository, and the current HyperFactor ratio.

    Note: Optionally, select the **Max. cartridge growth** check box. When selected, you can limit the maximum amount of nominal data that a cartridge can contain.

    The value of the maximum number of cartridges possible on a system depends on the amount of storage space available on your system. The maximum possible cartridge limit is 62,000, but many systems will have a lower maximum limit because of the storage space available.

19. In the **Barcode seed** field, enter a value for the barcode seed. The barcode seed is the barcode that is assigned to the first cartridge created. Every cartridge added after the first cartridge is assigned a barcode following the initial barcode seed.

    Note: The barcode seed must contain only numbers and capital letters.

20. Click **Next**. The **Slots** screen is displayed.
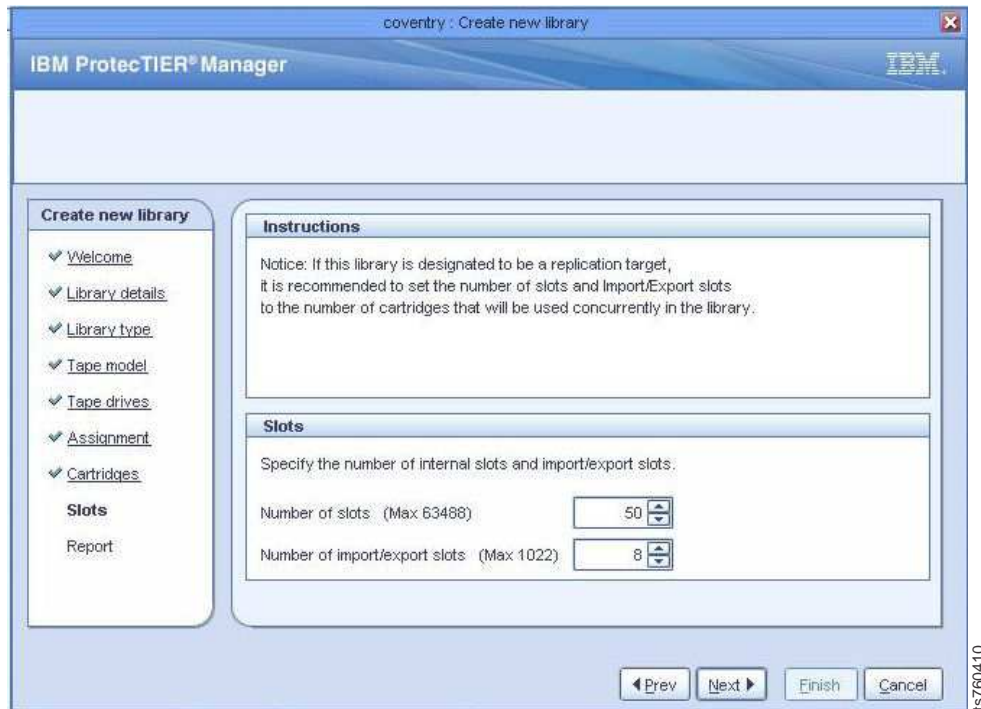
Figure 18. Slots screen

21. In the **Number of slots** field, enter the number of cartridge slots that you want to have in the library.

    Note: The number of cartridge slots must not be less than the number of cartridges that you are creating. If you expect to increase the number of cartridges at a later time, it is recommended that you create additional slots.

22. In the **Number of import/export slots** field, enter the number of import/export slots that you want to have in the library. You can define up to a maximum of 1022 import/export slots for each library.

23. Click **Next** and **Finish**. The **Create new library** wizard closes.

24. Click **Yes** to continue. The ProtecTIER system temporarily goes offline to create the library. The library is displayed in the **Systems Management** pane.

Renaming libraries

Complete this task to rename an existing ProtecTIER library.

About this task

The ProtecTIER system enables you to rename libraries after they have been created.

Perform the following steps to rename an existing library.

Procedure

To rename an existing library:

1. Select a library from the navigation pane.

2. Choose **VT > VT Library > Rename library**. The **Rename library** dialog is displayed.

3. Enter a new name for the selected library and click **0k**. The **Rename library** dialog closes and the library's name is changed.

Setting the library type

Note: Verify that the backup application that you are using supports the type of library model that you select for a virtual tape system. Refer to the *TS7650 Support Matrix* at: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA &subtype=WH&htmlfid=IVL12348USEN .

When you set the library type, you can select the type of physical library model that you want the virtual library to emulate:

- ATL P3000 0100
- IBM TS3500 0100

You can also configure the virtual library models:

- DTC VTF 0100
- IBM V-TS3500 0100

If you chose the TS3500 (or P3000) during the creation of the library and your backup application does not support that library model type as a virtual tape system, the **Set library type** window allows you to change the library type to V-TS3500 (or VTF). Conversely, if you chose the V-TS3500 (or VTF) during library creation, and your backup application supports the TS3500 library, use **Set library type** to change the library type. (You can interchange between the TS3500 and V-TS3500 library models and between the P3000 and VTF library models.)

Example

To set the library type:

1. Select the library in the **Systems Management** pane.

2. Choose **VT > VT Library > Set library type**. The **Set library type** window is displayed.

3. Specify the library type accordingly:
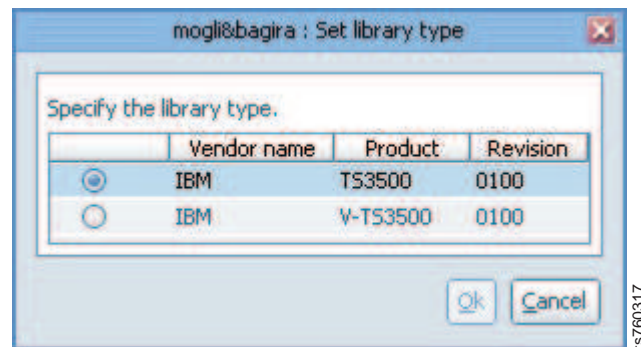
Figure 19. Set library type dialog

4. Click **Ok**.

Editing library parameters

Complete this task to change the parameters of an existing library.

About this task

The ProtecTIER system enables you to change the parameters of libraries, including the assignment of virtual devices, adding virtual tape drives, and increasing library capacity.

Note: The **Change dimensions wizard** does not enable you to assign existing unassigned tape drives. Use the Re-assign devices wizard to assign unassigned tape drives. For more information, see "Reassigning devices" on page 95.

Perform the following steps to change the parameters of an existing library:

Procedure

1. Select a library from the **Systems Management** navigation pane.
2. Choose **VT > VT Library > Change dimensions**. The **Change dimensions** wizard **Welcome** screen is displayed.
3. Click **Next**. The **Tape drives** screen is displayed.
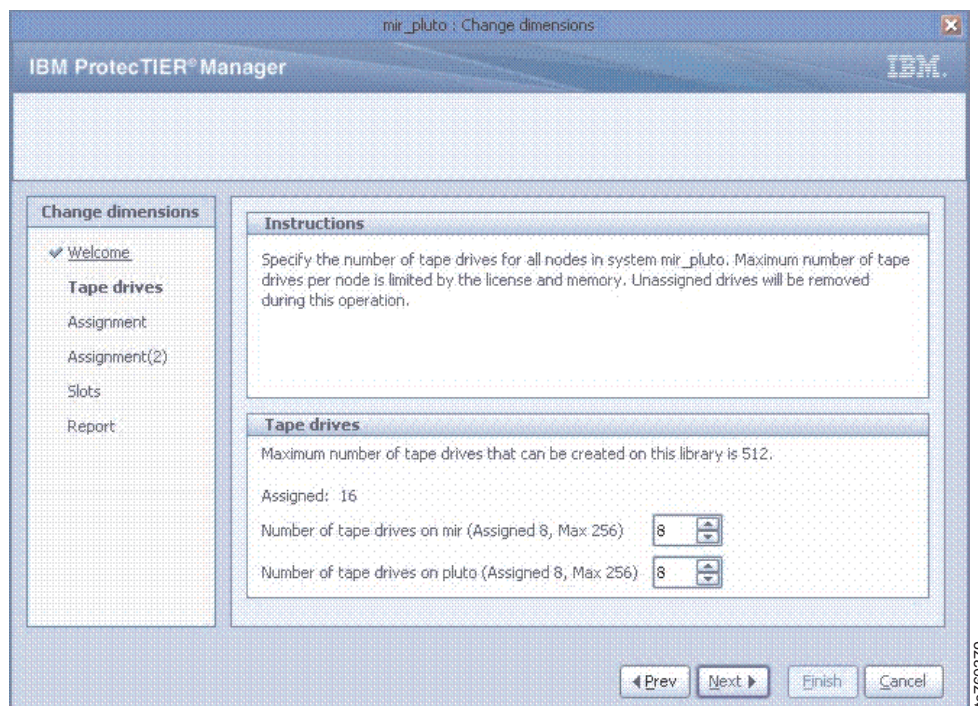
Figure 20. Tape drives screen

4. In the **Number of tape drives** field for each node, enter the number of tape drives that you want to have in the node.In the **Number of tape drives** field enter the number of tape drives that you want to have in the node.
5. Click **Next**. The **Assignment** screen is displayed for the first node in the cluster.Click **Next**. The **Assignment** screen is displayed.
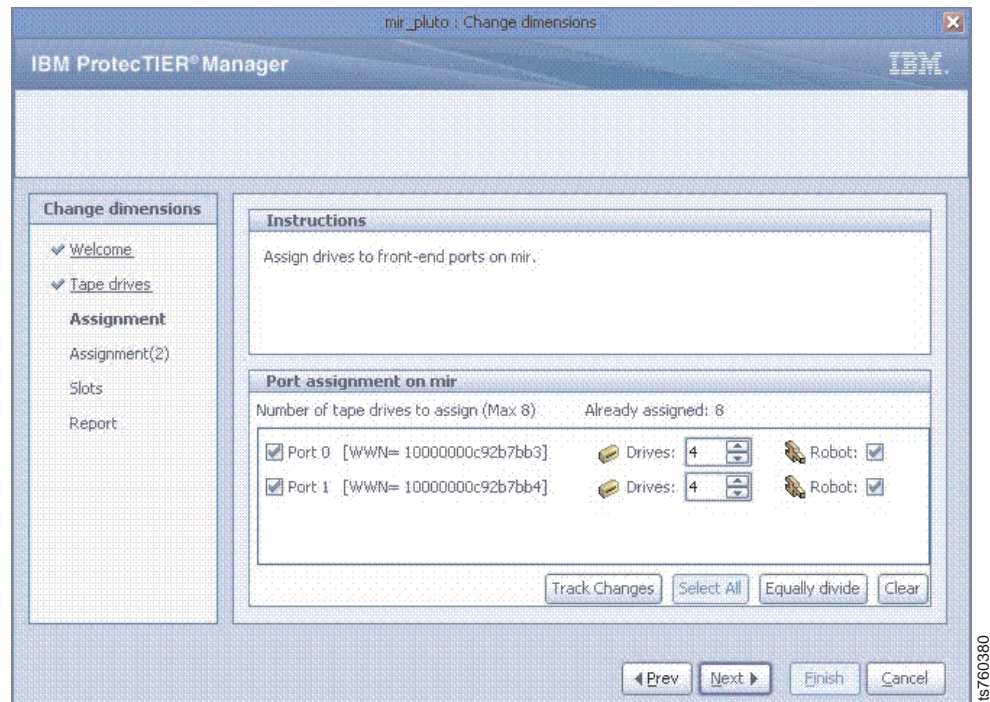
Figure 21. Assignment screen

6. Select or clear the check boxes next to each port to define which of the node ports are assigned virtual tape drives.

7. In the **Drives** fields corresponding to each selected port, select the number of virtual tape drives that are assigned to each port.

   Note: Optionally, click **Select All** to automatically select both ports. Click **Equally divide** to evenly divide the number of drives between the ports.

8. Optionally, click **Track Changes** to display the modifications that the ProtecTIER system might need to make in response to the changes you defined. Then, click **Re-assign ports** to return to the Assignment screen and continue assigning virtual tape drives.

9. Check the **Robot** check box if you want the library virtual robot to be accessible through this port.

   Note: For high-availability purposes, ProtecTIER supports the assignment of the virtual robot to multiple ports.

10. Click **Next**. If a second node exists in the cluster, the **Assignment (2)** screen is displayed.
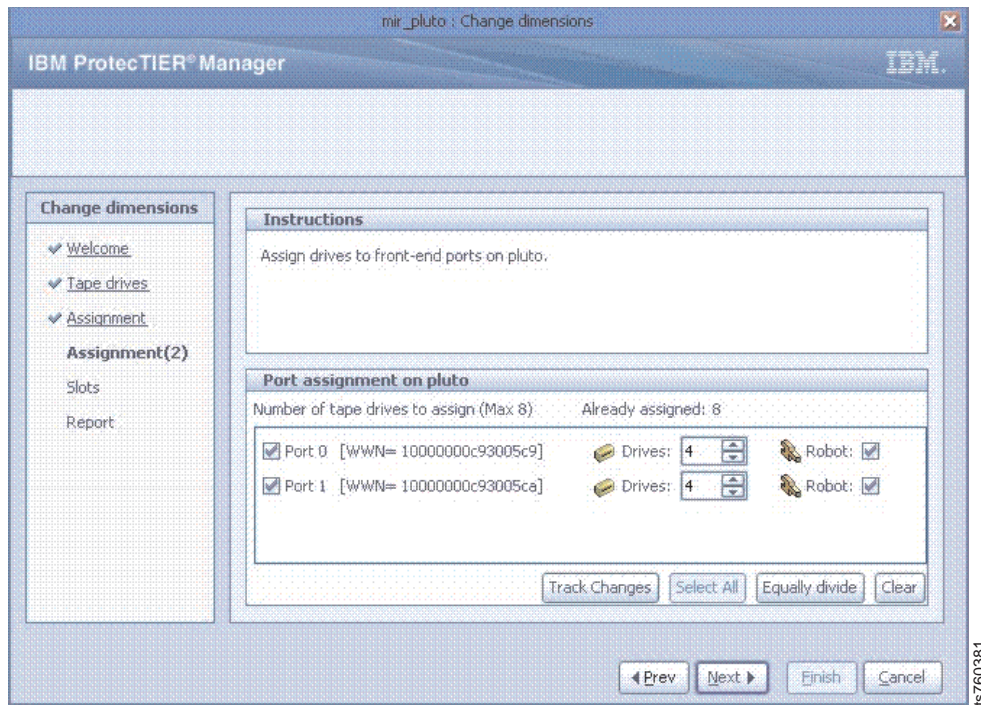
Figure 22. Assignment (2) screen

11. Repeat steps 6 on page 93 through 9 on page 93 for the **Assignment (2)** screen.

12. Click **Next**. The **Slots** screen is displayed.
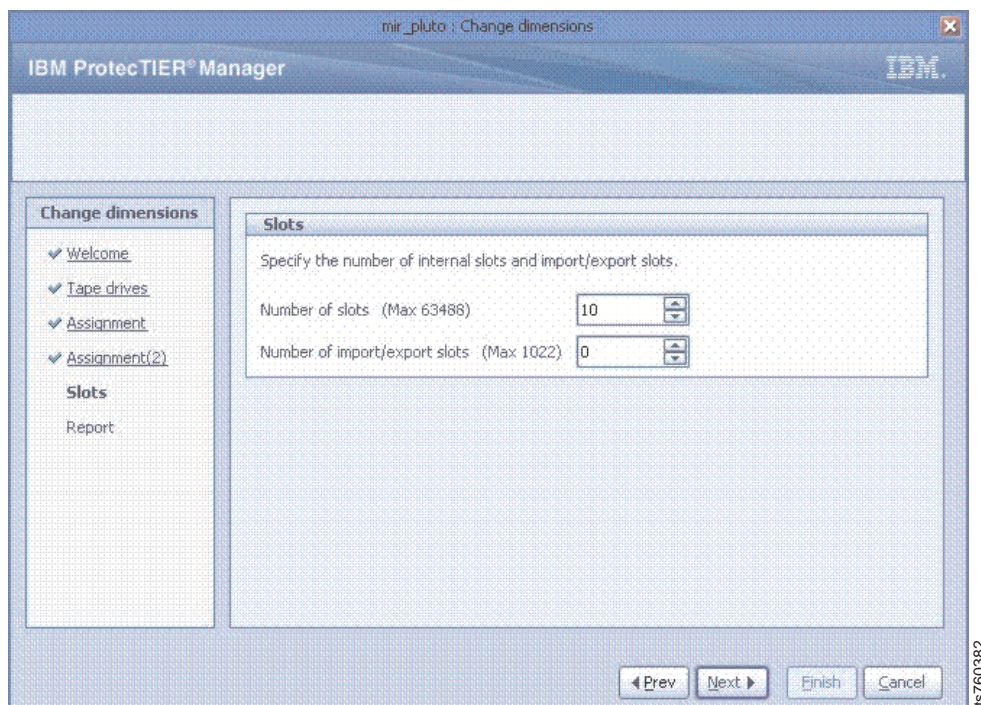
Figure 23. Slots screen

13. In the **Number of slots** field, enter the number of slots that you want in the library.

> **Note:** The number of slots must be at least equal to the number of cartridges in the library.

14. In the **Number of import/export slots** field, enter the number of import/export slots that you want in the library.

15. Click **Next** and **Finish**. The **Change dimensions** wizard closes.

16. Click **Yes** to continue. The ProtecTIER system temporarily goes offline to update the library.

Reassigning devices

Complete this task to reassign the virtual robot and cartridge drives within the ProtecTIER system.

About this task

The ProtecTIER system enables you to relocate the virtual robot and cartridge drives between nodes or node ports.

Perform the following steps to reassign the virtual robot or cartridge drives:

Procedure

1. Select a library from the **Systems Management** navigation pane.

2. Choose **VT > VT Library > Re-assign devices**. The **Re-assign devices** wizard **Welcome** screen is displayed.

3. Click **Next**. The **Tape drives** screen is displayed.
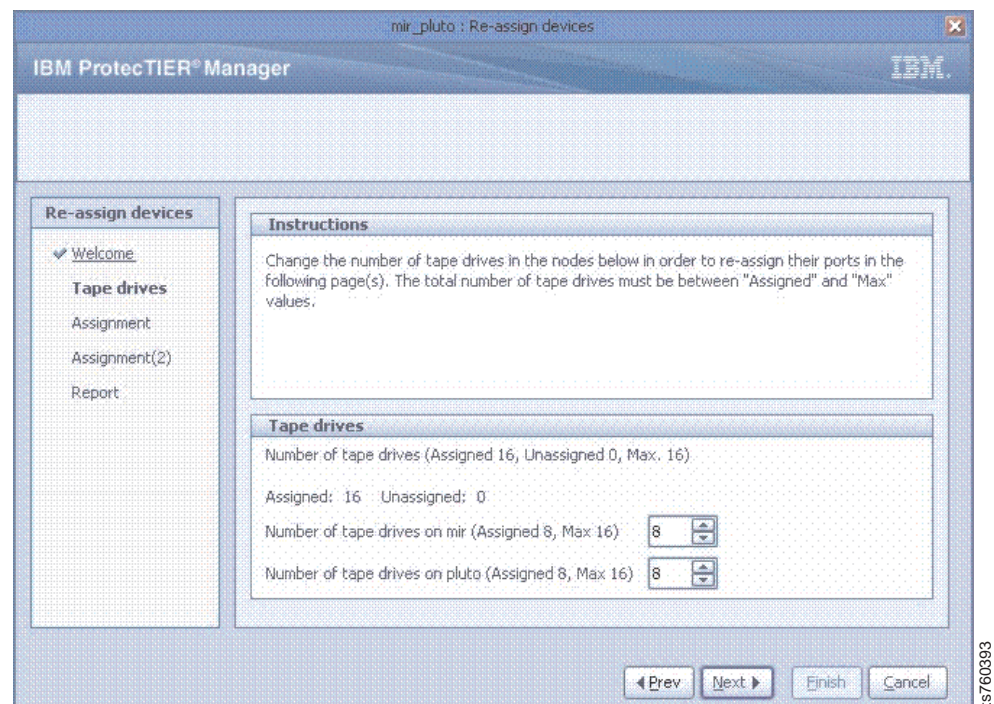
Figure 24. Tape drives screen

4. In the **Number of tape drives** field, select the number of tape drives to assign to the node.

Note: If a node is currently down, you can only remove drives from that node.

5. Click **Next**. The **Assignment** screen is displayed.
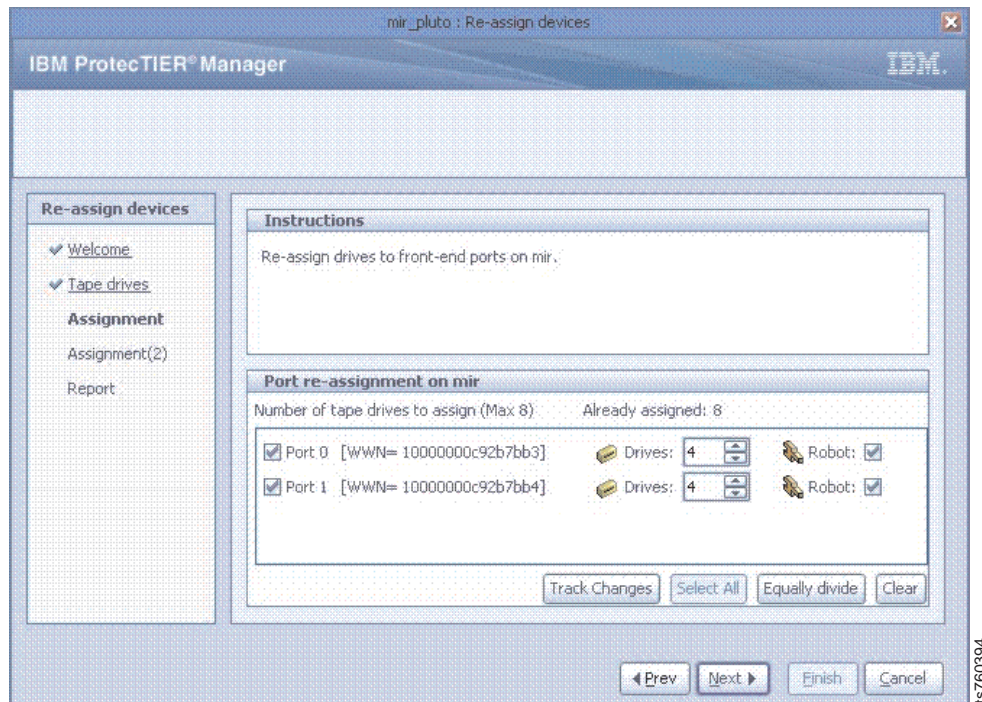
Figure 25. Assignment screen

6. Select or deselect the check boxes next to each port to define which of the node's ports are assigned virtual tape drives.

7. In the **Drives** fields corresponding to each selected port, select the number of virtual tape drives that are assigned to each port.

   Note: Optionally, click **Select All** to automatically select both ports. Click **Equally divide** to evenly divide the number of drives between the ports.

8. Optionally, click **Track Changes** to display the modifications that the ProtecTIER system might need to make in response to the changes that you defined. Then, click **Re-assign ports** to return to the Assignment screen and continue assigning virtual tape drives.

9. Check the **Robot** checkbox if you want the library virtual robot to be accessible through this port.

   Note: For high-availability purposes, ProtecTIER supports the assignment of the virtual robot to multiple ports.

10. Click **Next**. If a second node exists in the cluster, the **Assignment (2)** screen is displayed.
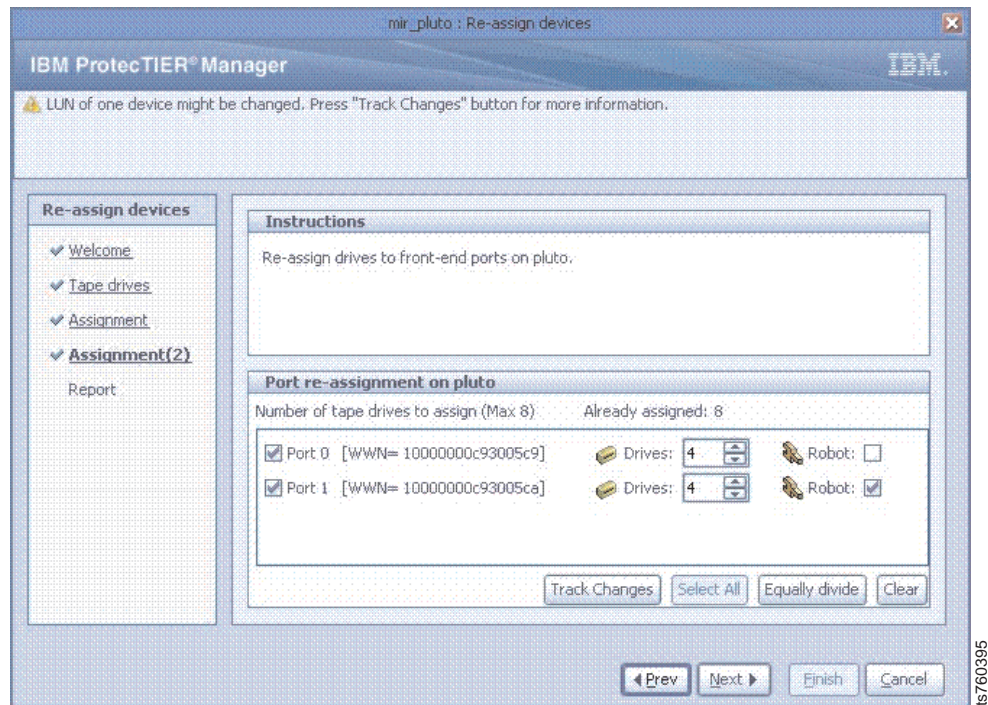
Figure 26. Assignment (2) screen

11. Repeat steps 6 on page 96 through 9 on page 96 for the **Assignment (2)** screen.

12. Click **Next**. The **Summary report** is displayed.
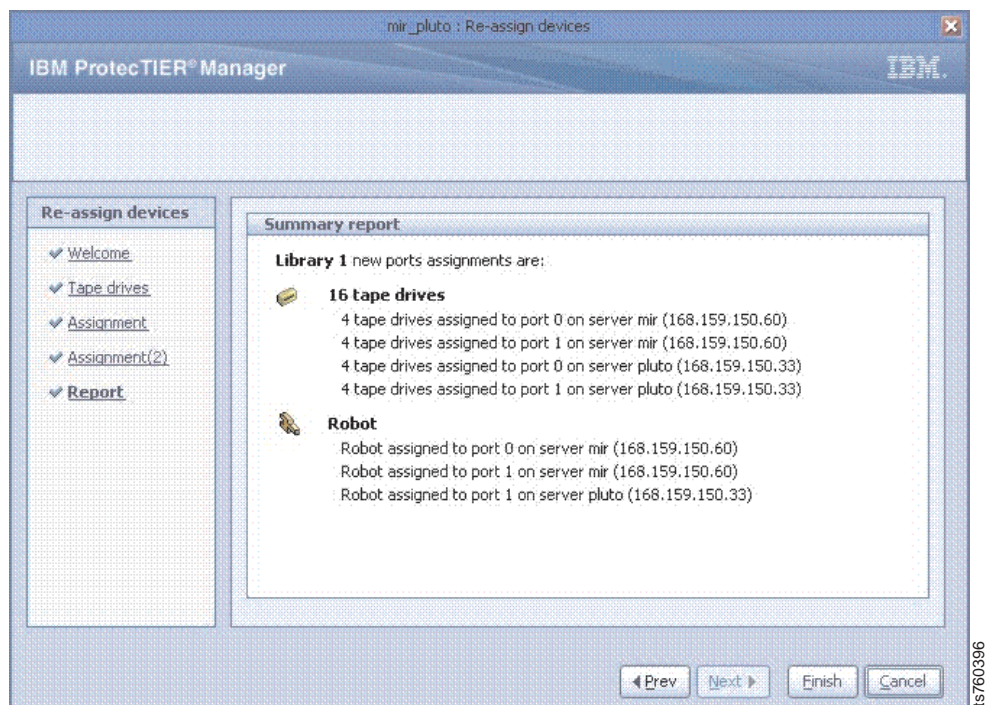
Figure 27. Summary report screen

13. Click **Finish**. The **Re-assign devices** wizard closes.

14. Click **Yes** to continue. The ProtecTIER system temporarily goes offline to reassign the devices.

Control Path Failover (CPF) and Data Path Failover (DPF) support

This topic details the Control Path Failover (CPF) and Data Patch Failover (DPF) that are supported by the emulated IBM library models.

Before you begin

Setting CPF/DPF within the IBM tape device driver is described in the *IBM Tape Device Drivers Installation and User's Guide* located on the following Web site: https://www-304.ibm.com/support/docview.wss?rs=577&uid=ssg1S7002972.

By default, Data Path Failover is always enabled on the emulated IBM library models and requires no feature code.

By default, CPF is also enabled on the emulated IBM library models. However, when troubleshooting host connectivity issues, you might be asked to disable CPF.

About this task

This task describes how to disable CPF:

Procedure

1. Select a library from the **Systems Management** navigation pane.
2. Select **VT > VT Library > Set control path failover mode**. The **Set control path failover mode** dialog is displayed.
3. Set the CPF mode to **Control path failover disabled**. CPF is now disabled.

Deleting libraries

Complete this task to delete a ProtecTIER library.

About this task

Attention: Deleting a library results in the loss of all data contained in that library. Only a person with administrator authority can perform this task.

Perform the following steps to delete a ProtecTIER library.

Procedure

To delete a library:
1. Select a library from the **Systems Management** navigation pane.
2. Choose **VT > VT Library > Delete library**. A confirmation message box is displayed.
3. Click **Yes**. The Data Loss Confirmation dialog is displayed.
4. In the field, type **data loss** and click **Ok**. A confirmation message box is displayed.
5. Click **Yes** to continue. The ProtecTIER system temporarily goes offline to delete the library.

Managing cartridges

The topics in this section describe how to manage cartridges from your libraries within the ProtecTIER system.

Resyncing cartridges

Complete this task to add cartridges to your ProtecTIER system.

About this task

If your virtual library has enough empty slots to accommodate the additional cartridges, the Resyncing cartridges process occurs online without disrupting backup. If the virtual library does not have enough empty slots, Resyncing cartridges causes the ProtecTIER system to temporarily go offline to create more slots for the cartridges.

Note: Resyncing cartridges to an existing library decreases the capacity size of cartridges in all libraries in the repository by a percentage proportional to the percent increase in the number of cartridges. The change affects future backups. The Data Size of full cartridges does not change.

You can also use the AddCartridges ptcli command to add cartridges. See "ptcli Configuration commands" on page 68.

Perform the following steps to add cartridges:

Procedure
1. Select a library from the **Systems Management** navigation pane.
2. Click the **Add cartridges** button. The **Add cartridges** wizard **Welcome** screen is displayed.
3. Click **Next**. The **Cartridges** screen is displayed:
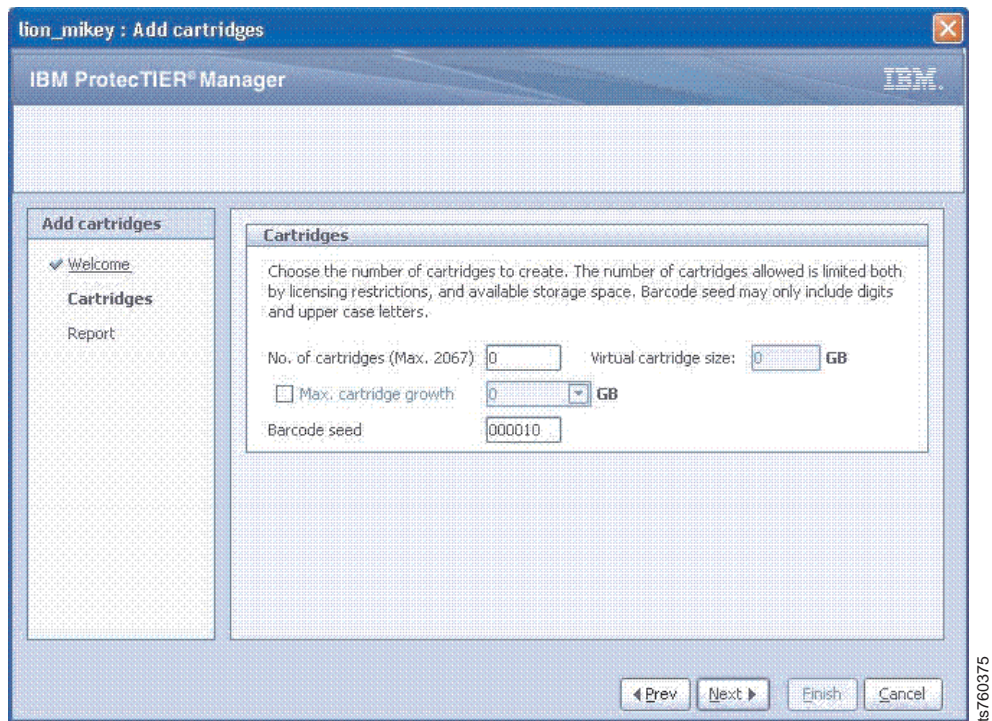
Figure 28. Cartridges screen

4. In the **No. of cartridges** field, enter the number of cartridges that you want to have in the library. The **Virtual cartridge size** field automatically displays the maximum possible size for virtual cartridges for your system. This number is based on the number of cartridges entered, the total amount of available storage space in your repository, and the current HyperFactor ratio.

   Note: Optionally select the **Max. cartridge growth** checkbox. When selected, you can limit the maximum amount of nominal data that a cartridge can contain.

   The value of the maximum number of cartridges possible on a system depends on the amount of storage space available on your system.

5. In the **Barcode seed** field, enter a value for the barcode seed. The default barcode seed is the continuation of the initial barcode seed assigned when the library was created.

   Note: The barcode seed must contain only numbers and capital letters.

6. Click **Next** and **Finish**. The **Add cartridges** wizard closes.

7. Click **Yes** to continue and add the cartridges to the library. If the necessary number of cartridge slots are not already available, the ProtecTIER system temporarily goes offline to create them. When the system returns online, the cartridges are added to the library.

8. Continue working with the ProtecTIER system.

Deleting cartridges

Complete this task to delete a cartridge within the ProtecTIER VT system.

About this task

Deleting a cartridge results in the loss of all data contained in the cartridge.

Note: Deleting cartridges from an existing library increases the capacity size of cartridges in all libraries in the repository by a percentage proportional to the percent decrease in the number of cartridges. The change affects future backups. The Data Size of full cartridges does not change.

Perform the following steps to delete a cartridge:

Note: Alternatively, you can delete a cartridge from the shelf. Deleting a cartridge from the shelf is a nondisruptive operation (i.e. the VTL stays online). Thus, it is recommended that you eject the cartridges you want to delete to the local shelf on the repository, and then delete the cartridge.

Procedure

1. Select the library that contains the cartridge you want to delete. The **VT** window is displayed.
2. Click the **Cartridges** tab. The **Cartridges** window is displayed.
3. Select a cartridge from the list of the cartridges displayed.
4. Choose **VT > VT Cartridge > Delete Cartridges**. A confirmation message box is displayed.
5. Click **Yes**. The **Data Loss Confirmation** dialog is displayed.
6. In the field, type `data loss` and click **Ok**. A confirmation message box is displayed.
7. Click **Yes**. The cartridge is deleted from the list.

   Note: If the cartridges are deleted directly from the library (and not the shelf), a confirmation message will display for the system to go offline.

Switching cartridges to read-only mode

Complete this task to change the cartridge mode to read-only.

About this task

Perform the following steps to change the cartridge mode to read-only:

Procedure

1. From the **Systems Management** view, select a library from the navigation pane.
2. Click on the **Slots** tab.
3. Select a cartridge.
4. Choose **VT > VT Cartridge > Read/Write cartridge**. A confirmation message box is displayed.
5. Click **Yes**. The cartridge switches to read-only mode.

   Note: Clicking Read/Write cartridge for a read-only cartridge switches the cartridge to the read/write mode.

Verifying cartridge metadata

This task describes how to verify a cartridge's metadata.

About this task

Cartridge metadata is verified by reading the cartridge metadata to ensure that it is intact and the cartridge is usable.

Follow the procedure to verify cartridge metadata:

Procedure
1. From the Systems Management view, select a library from the navigation pane.
2. Click on the **Slots** tab.
3. Highlight the cartridges to check.
4. Choose **VT > VT Cartridge > Meta-data verification**.
5. Click **Yes** to proceed with the operation. The **Verification results** display the status of the selected cartridges, the barcode numbers and file marks.
6. Click **Ok** to close the window.

Verifying cartridge integrity

This task describes how to verify a cartridge's integrity.

About this task

Cartridge integrity is verified by reading the cartridge actual data while performing CRC comparisons to ensure that the data is intact and the cartridge is usable.

Follow the procedure to verify cartridge integrity:

Procedure
1. From the Systems Management view, select a library from the navigation pane.
2. Click on the **Slots** tab.
3. Highlight the cartridges to check.
4. Choose **VT > VT Cartridge > Cartridges integrity verification**.
5. Click **Yes** to proceed with the operation. The **Verification results** display the status of the selected cartridges and the barcode numbers.
6. Click **Ok** to close the window.

Changing cartridge ownership (Principality)

Complete this task to change the ownership of a cartridge.

Before you begin

Using ProtecTIER Manager, you can change the principality of synchronized cartridges to a different repository in the same replication group (without entering DR mode). The following conditions must be true:

Both repositories must be available

Both cartridges (source cartridge and it's replica cartridge) must exist (have not been deleted) on relevant repositories.

Note: When you run a VTL repository takeover, the principality of the cartridges from the destroyed repository is automatically changed to the replacing repository. Refer to "Replacing a destroyed VTL repository " on page 172 for more information.

About this task

Cartridge ownership, or "principality", is the privilege to write to a cartridge (set it to read/write mode). The principality of each cartridge belongs only to one repository in the grid, and, by default, principality belongs to the source repository.

Follow the procedure below to change the cartridge principality:

Procedure

1. In the Systems Management view, select a VT library from the navigation pane.
2. Click the **Cartridges** tab to display detailed information about the virtual tape cartridges in the library.
3. Highlight the synched cartridges from the VT library on which you want to change principality and right-click.

   Note: Additionally, you can use the **Principality Cartridge Query Tool** to select cartridges for principality change by filtering the cartridges that are "in-sync".

   To access the **Principality Cartridge Query Tool**, choose one of the following options:
   - Right-click and select **Cartridge principality change** > **Principality Cartridge Query Tool** , or
   - Select **VT** > **VT Cartridges** > **Principality Cartridge Query Tool** from the menu.

   Refer to "Using the cartridge query tool (for VTL)" on page 189 for more information.
4. Select **Cartridge principality change > Mark selected cartridges to be processed** from the popup menu.

   The following message is displayed:
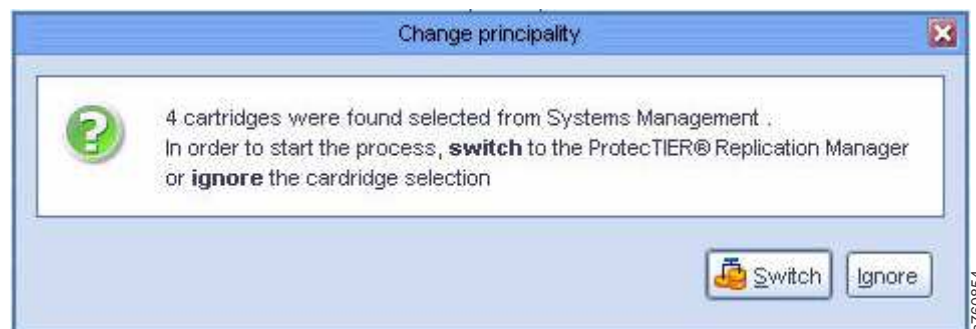
Figure 29. Cartridge selection details message

5. Click **Switch**. You are automatically switched to the ProtecTIER Replication Manager and the **Change principality** window is displayed:
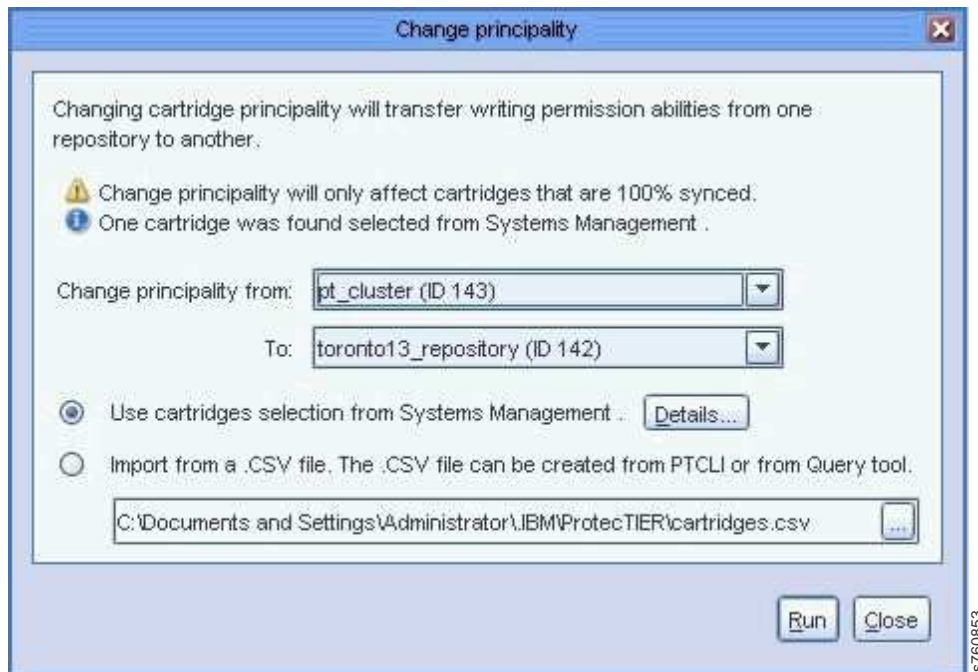
Figure 30. Change principality window

> **Note:** Additionally, you can display the Change principality window by selecting **Group > Change principality**.

6. From the drop-down lists, select the repository from the **Change principality from:** field from which to change the cartridge principality.

   > **Tip:** If this window was displayed immediately after selecting cartridges in the System Management view, the repository displayed in the **Change principality from:** field should be correctly displayed by the system. Choosing a different repository from the drop-down list forces you to use the **Import from a .CSV file** option.

7. Select the repository from the **To** field to which to change the cartridge principality.

8. Click **Run**.

9. Click **Yes** to confirm running the operation.

   If the change principality operation is successful, a message will display that the operation succeeded, how many cartridges were sent for processing, and how many of the cartridges were valid for principality change.

10. Click **Yes** to download a summary report.

11. If cartridges were marked for change principality in the Systems Management view, then the **Use cartridges selection** button is enabled. Click **Details...** to view the cartridges selected.

    > **Note:** If no cartridges were marked for change principality in the Systems Management view, then the only option offered is to import the cartridge selection from a *.csv* file created from either the PTCLI, or Cartridge query tool.

Results

Once the change principality operation has succeeded, the **Principal** column in the cartridge view will show to which repository the principality has been changed.

What to do next

Go to "Backup properties" on page 161.

Resyncing cartridges

Complete this task to resynchronize cartridges that have become out of sync.

Before you begin
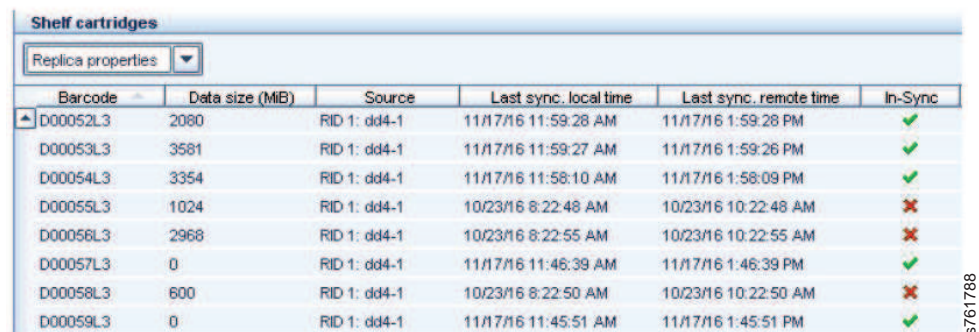
Ensure that:
- VTL is running on both the source and the destination sites
- There is connectivity between the source and the destination site
- The out-of-sync cartridges replication policy is enabled.

About this task

For various reasons, cartridges in your virtual library may become out of sync. To resynchronize cartridges, use the re sync_carts.sh script that is located in `/opt/dtc/app/sbin/` folder.

You can also use the resync_cart.sh script to replicate cartridges that have replication backlog.

The following example shows three cartridges (D00055L3, D00056L3, and D00058) that are out of sync with the others.

Barcode	Data size (MiB)	Source	Last sync. local time	Last sync. remote time	In-Sync
D00052L3	2080	RID 1: dd4-1	11/17/16 11:59:28 AM	11/17/16 1:59:28 PM	✔
D00053L3	3581	RID 1: dd4-1	11/17/16 11:59:27 AM	11/17/16 1:59:26 PM	✔
D00054L3	3354	RID 1: dd4-1	11/17/16 11:58:10 AM	11/17/16 1:58:09 PM	✔
D00055L3	1024	RID 1: dd4-1	10/23/16 8:22:48 AM	10/23/16 10:22:48 AM	✖
D00056L3	2968	RID 1: dd4-1	10/23/16 8:22:55 AM	10/23/16 10:22:55 AM	✖
D00057L3	0	RID 1: dd4-1	11/17/16 11:46:39 AM	11/17/16 1:46:39 PM	✔
D00058L3	600	RID 1: dd4-1	10/23/16 8:22:50 AM	10/23/16 10:22:50 AM	✖
D00059L3	0	RID 1: dd4-1	11/17/16 11:45:51 AM	11/17/16 1:45:51 PM	✔

Figure 31. Cartridges screen

Procedure

1. Navigate to the root directory and enter this command: `/opt/dtc/app/sbin/resync_carts.sh` as shown in the example.

Figure 32. Command example

When the script completes, an additional messages appears.

Figure 33. Message indicating that the script has completed

A summary of the process is recorded in `/root/replicationReport.sh`.

Note: The time it takes for the resync_cart.sh script to complete varies depending on your ProtecTIER configuration.

2. Review the Replica properties report to observe that the cartridges are now in-sync. The Replica properties report shows that the cartridges are in-sync.

Figure 34. Cartridges screen

About LUN Masking

Use LUN Masking to monitor device visibility. LUN Masking "masks" specific devices (tape drives or robots) from the view of host initiators while allowing a selected host initiator group to view them.

LUN Masking allows you to assign specific devices to a specific host running backup application modules. It enables multiple initiators to share the same target FC port without having conflicts on the devices being emulated.

The LUN Masking setup can be monitored and modified at all times during system operation. LUN Masking in ProtecTIER influences the visibility of the devices by the hosts systems. Keep in mind that every modification in the LUN Masking in ProtecTIER might affect the host configuration and might require rescanning by the hosts.

Enabling or disabling LUN Masking

The LUN Masking settings are disabled, by default, but can be either enabled or disabled. Configuration operations can be done in either mode, but the relevant changes are applied only when LUN Masking is enabled.

About this task

If LUN Masking is enabled, devices are seen only by the hosts that are defined with them in the same LUN Masking group. If LUN Masking is disabled, all devices are seen by all hosts. Follow the steps below to enable or disable LUN Masking:

Procedure

1. Select **VT > LUN Masking > Set LUN Masking enablement**.
2. Select **Enable LUN masking** to turn *on* LUN Masking, or **Disable LUN masking** to turn *off* LUN Masking.
3. Click **Ok**.

What to do next

Once you have enabled or disabled the LUN Masking option, IBM recommends that you re-scan the devices from the host systems. Re-scanning sends the updated information for the list of visible devices and their associated LUN numbers.

Go on to "Managing host initiators."

Managing host initiators

The **Host Initiators Management** option is used to add, modify, or delete host initiators from the list of host initiators known to ProtecTIER.

Note: A host initiator must be defined before it can be a part of a LUN Masking group. Up 1024 host initiators can be defined on a system. See "Working with LUN Masking groups" on page 110.

To add, modify or delete host initiators, select **VT > Host Initiators Management** to access the Host Initiators Management functions. The **Host Initiators Management** screen displays the following details of the host initiator:

- WWN
- Alias – a name that is defined other than the WWN
- Group associated – the LUN Masking group to which the host initiator belongs
- Flat addressing mode - a technique used by HP-UX to work around certain SCSI addressing limitations when accessing many devices over a Fibre Channel
- Link up – displays whether there is an active link between ProtecTIER and the host initiator

From this screen, go on to adding or scanning host initiators, modifying host initiator configurations, or deleting host initiators.

Adding Host Initiators

This section describes how to add host initiators with the Host Initiators Management window.

Host initiators can be added to the host initiators list either manually, or by scanning the system for new host initiators. Follow either one of the following procedures below for adding host initiators:

- "Manually adding host initiators"
- "Scanning host initiators" on page 109

Manually adding host initiators:

Host initiators can be added manually by entering the host WWN, alias, and addressing mode. A host initiator can be added either by accessing the Host Initiator Management window from the VT menu, or from the LUN Masking group configuration window.

About this task

Manually adding host initiators is primarily done when hosts are not yet connected to ProtecTIER.

Note: A host initiator must first be defined before it can be a part of a LUN Masking group.

Procedure

To add a new host initiator:

1. Select **VT** > **Host initiators management**. The **Host initiator management** window displays.
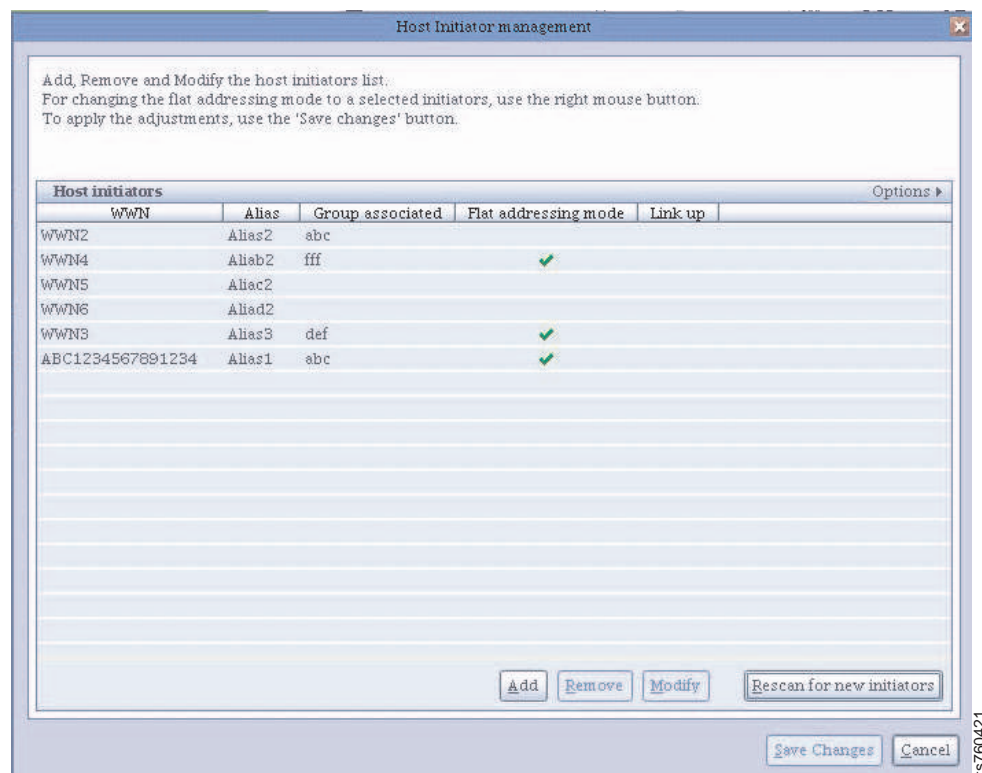
Figure 35. Host Initiator management window

2. Click **Add**. The **Add host initiator** screen is displayed.

3. Select a WWN from the WWN drop-down box or type in a new WWN.

4. Enter an alternative name for the WWN in the **Alias** field.

5. Select the **Flat addressing mode** check box if the flat addressing technique is to be used.

6. Click **Ok**. The new host initiator is listed on the Host initiators management screen.

What to do next

Go on to add more new host initiators or to modify or delete existing host initiators. Once you have defined a host initiator, you can create LUN Masking groups. See "Working with LUN Masking groups" on page 110.

Scanning host initiators:

Host initiators can be added to the configured host initiators list after scanning the system. Scanning for new host initiators is recommended when the host initiators are already physically connected, but you have not yet added them to the **Host Initiators** list.

About this task

Use the following procedure to scan for new host initiators.

Procedure

To scan for new host initiators:

1. Select **VT** > **Host initiators management**. The **Host initiator management** window displays.

2. Click **Re-scan for new initiators** to scan for new host initiators. If new host initiators are found that are not already configured in the Host Initiators list, a dialog with the available host initiators appears.

3. Select the Host Initiators you want to add.

4. Click **Yes** to add the new host initiators to the list, or click **Cancel** to exit without adding.

What to do next

Go on to "Working with LUN Masking groups" on page 110.

Modifying Host Initiators
You can change the host initiator alias or addressing mode or both.

About this task

Use the following procedure to change the host initiator alias or addressing mode or both:

Procedure

1. Select **Host initiators management** from the **VT** menu. The **Host initiators management** screen is displayed.

2. Select a host initiator from the list and click **Modify**. The **Modify host initiator** dialog is displayed.

3. Change the host initiator alias by typing a new name in the **Alias** field.

4. Change the addressing mode by selecting or clearing the **Flat addressing mode** check box.
5. Click **Ok** to save and close the **Modify host initiator** dialog, or select a different host initiator to modify from the drop-down list in the **WWN** field.

What to do next

Continue working with the options available from the **Host Initiators Management** screen to add, remove, modify, or rescan for new initiators.

If you have finished working with the **Host Initiators Management** screen, click **Save Changes** to save your changes and exit, or click **Cancel** to exit without saving your changes.

Removing Host Initiators

Configured host initiators cannot be deleted if they act as members of a LUN Masking group. See *Removing a LUN Masking group* for more information.

About this task

Use the following procedure to remove a host initiator that is not a member of a LUN Masking group:

Procedure

1. Select **Host initiators management** from the **VT** menu. The **Host initiators management** screen is displayed.
2. Select a host initiator from the list and click **Remove**. The **Remove host initiator** dialog is displayed.
3. Click **Yes** to remove.

What to do next

Continue working with the options available from the **Host Initiators Management** screen to add, remove, modify, or rescan for new initiators. If you have finished working with the Host Initiators Management screen, click **Save Changes** to save your changes and exit, or click **Cancel** to exit without saving your changes.

Working with LUN Masking groups

LUN Masking groups define the connection between the host initiators and the VT library devices (robots or tape drives). Devices which belong to a certain group can be seen by the host initiators of the group. A device can belong to multiple LUN Masking groups, but a host initiator can belong to only one LUN Masking group.

Select the **Configure LUN Masking groups** option from the **VT > LUN Masking** menu to begin configuring LUN Masking groups.

You can add LUN Masking groups. If a group exists, configure the group by adding Host Initiators, adding or modifying libraries, or adding or modifying the devices within the libraries.

Note: Keep in mind that changes you make in the LUN Masking configuration requires scanning by the host and by the backup application.

Creating LUN Masking groups

Begin working with LUN Masking groups by adding a group via the **LUN Masking** window. A maximum of 512 groups can be configured per system and a maximum of 512 drives can be configured per group. (A maximum of 1024 host initiators can be defined on a system.) Each group needs to contain at least one host initiator and one device (tape drive or robot). Robots can be added as required.

To add a LUN Masking group:

1. On the left side of the LUN Masking window, click **Add** at the bottom of the **LUN Masking Groups** pane. The group details appear to the right of the window.
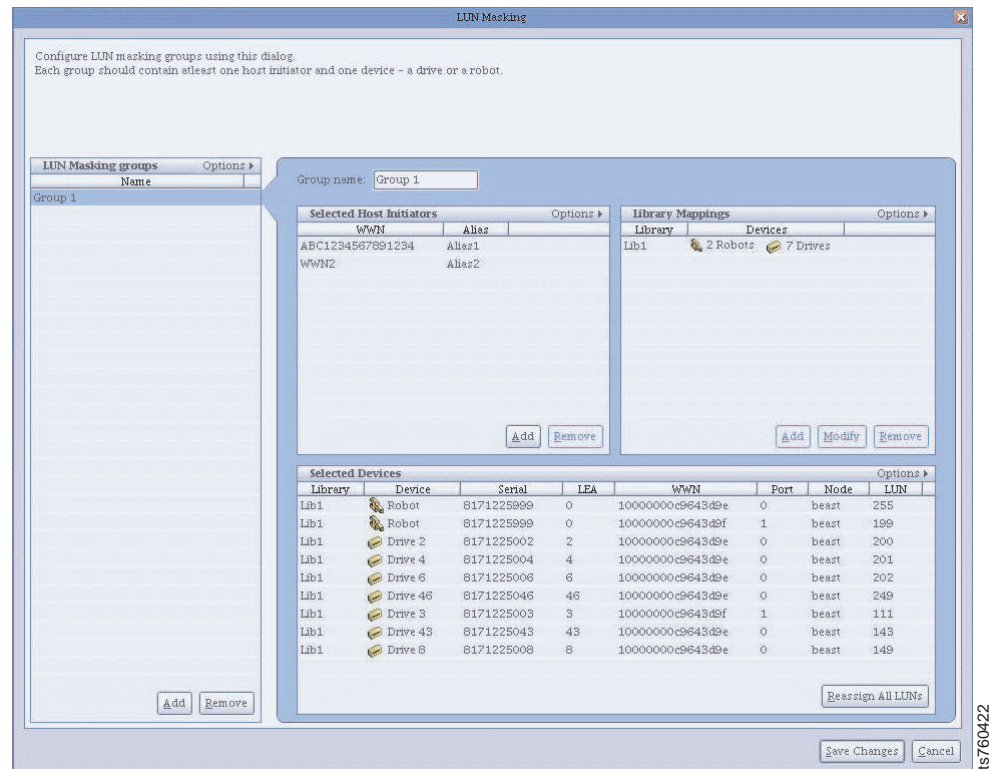
Figure 36. LUN Masking window

2. Type a new name for the group in the **Group name** field.
3. Add host initiators by clicking **Add** in the **Selected Host Initiators** pane. The **Add Host Initiators** dialog is displayed.
4. Select the Host Initiators to add to the LUN Masking group from the list displayed and click Ok.
5. Continue adding more host initiators, or go on to add the library devices.

From the **Library Mappings** pane, you can add the library devices you want to be visible to the host initiators in the group.

1. To define the devices, click Add at the bottom of the Library Mappings pane in the LUN Masking group details view. A list of libraries in the system is displayed.
2. Select the relevant libraries from the list and click Ok

Continue selecting the library devices to be viewed by the host initiators in the group.

Modifying a LUN Masking group

From the **Selected Devices** pane, modify the libraries and devices defined in the LUN Masking group. Once you have finished, click **Save changes** to save your modifications and exit the LUN Masking configuration.

After modifying a LUN Masking group, undesired holes might occur within the LUN numbering sequence. For example, removing a device from an existing group causes holes in the LUN numbering if this device does not have the highest LUN number. As a result, the backup application might have trouble scanning the devices. If your backup application has trouble scanning the devices, it is recommended that you reassign or renumber the LUN.

1. Reassign the LUNs by clicking **Reassign All LUNs** at the bottom of the Selected Devices pane.

   The system displays the Reassign LUNs dialog, which states "You are about to renumerate the LUN values of the available devices in the group. All the connected hosts must be rescanned."

2. Click **Yes** to renumerate.

   The LUN values are renumbered and all the devices in the Selected Devices pane are assigned new LUN numbers, sequentially, starting with "0" (zero).

3. Click **Save changes** to keep the modifications or Cancel to close the wizard.

Remember: As noted in the dialog opened in step 1, you must rescan drives from all affected Host Initiators in the specific group.

Continue to the next section.

Removing a LUN Masking group

If a LUN Masking group is removed while LUN Masking is enabled, the host initiators of that group become ineffective. They are unable to "see" any devices on this system. The host initiators must be reassigned to a different group to be reconnected.

To remove a LUN Masking group, click **Remove** at the bottom of the LUN Masking groups pane. The LUN Masking group is removed from the list.

Continue configuring the LUN Masking groups as appropriate. Click **Save changes** to save your modifications and exit the LUN Masking configuration.

Library-related operations

Some library configuration operations might affect the LUN masking groups. Most of these operations are blocked by the system, with the exception of operations where the removal of the devices might directly affect the relevant LUN Masking group. The **Delete library** operation and the **Change library dimensions** operation to reduce the number of drives are not blocked by the system.

Deleting a library

If devices from a deleted library are members of LUN Masking groups, a warning is issued to the log file and to the user. If the user proceeds with the operation, the

devices are removed from the relevant LUN Masking groups, and the configuration file data is updated accordingly.

Removing a library can cause "holes" in the LUN Masking numbering and, therefore, the backup application might have trouble scanning the devices. In this case, you must reassign the LUN.

Modifying the dimensions or reassigning devices of a library

The following rules apply when you modify the dimensions of a library or reassign library devices that belong to a LUN masking group:

- The device cannot be deleted or reassigned to another FE port. To reassign the device to a different port, you must remove the device from all of its related groupings.
- The number of drives in the library cannot be reduced.

Continue to the next chapter.

Chapter 10. Native Replication Management

This chapter provides the information needed to manage Native Replication configuration and monitoring of ProtecTIER VTL systems.

The ProtecTIER Replication Manager tasks include:
- Managing the repositories in the replication grid that can be replicated to
- Maintaining the IP addresses of all repositories
- Updating of repositories leaving and joining the grid
- High-level monitoring and statistics of traffic in the replication grids

Native Replication lets you replicate data objects between ProtecTIER repositories. In order for a logical set of repositories to replicate from one to another, you must create a replication grid. The replication grid is remotely created and managed by the Replication Manager.

The ProtecTIER Replication Manager is a server that remotely manages the replication grids within an organization. ProtecTIER Manager connects to the ProtecTIER Replication Manager using the IP address of the ProtecTIER Replication Manager server. The ProtecTIER Replication Manager is installed on a ProtecTIER node and can manage up to one grid with up to 24 repositories.

Each ProtecTIER Replication Manager has a unique identity. A repository, once it has joined a replication manager cannot join a replication grid managed by a different replication manager, even if it has left the grid. This restriction prevents data collision.

In a VTL environment, replication groups are created where multiple source repositories can replicate to a single target. This target can then act as a Disaster Recovery site for any number of the sources, while still allowing local backups, as well as replication, from the active source repositories.

Go on to "Working with ProtecTIER Replication Manager."

Working with ProtecTIER Replication Manager

This section describes how to manage ProtecTIER Replication Manager by working with ProtecTIER Manager.

Connecting to a ProtecTIER Replication Manager

To begin adding and working with a replication grid, click the **Grids Management** button at the bottom of the navigation pane of ProtecTIER Manager.

Use the following procedure to connect to a new ProtecTIER Replication Manager:
1. Select **Replication Manager > Add Replication Manager**. The **Add ProtecTIER Replication Manager** dialog is displayed.
2. Enter the **IP address** of the ProtecTIER Replication Manager you want to add and click **Ok**. The **ProtecTIER Replication Manager Login** is displayed.

Logging in to a ProtecTIER Replication Manager

Log in to a ProtecTIER Replication Manager:

1. Select **Replication Manager > Login**. The login screen is displayed.
2. Enter the Username: `gmadmin` and Password: `gmadmin`.
3. Click **Ok**. The **Replication Manager** view is displayed.

Removing a ProtecTIER Replication Manager

Before you remove a ProtecTIER Replication Manager, you must first log out of the Replication Manager you want to remove.

1. Select the **Replication Manager** for removal from the **Grids Management** navigation pane.
2. Select **Replication Manager > Logout**. You are now logged out.
3. Select **Replication Manager > Remove Replication Manager**. The **Remove Replication Manager** dialog is displayed asking if you want to remove the connection to the Replication Manager you selected.
4. Click **Yes**. The Replication Manager is removed from the list in the Grids Management navigation pane.

Go on to "Managing the replication grid."

Managing the replication grid

The topics in this section define tasks used when working with the replication grid in a VTL environment.

Management and configuration of a replication grid is done through the ProtecTIER Replication Manager **Grids Management** view of ProtecTIER Manager. A replication grid is composed of a set of repositories that share a common ID and can potentially transmit and receive logical objects through replication. Repositories do not need physical connections between them. However, all repositories do need a network connection to the ProtecTIER Replication Manager server. ProtecTIER Replication Manager is installed on a ProtecTIER node and can manage up to one grid with up to 24 repositories.

In a many-to-one environment, a single replication grid can include up to eight target repositories and, therefore, up to 8 "topology groups". A "topology group" is a replication group of one target repository with up to 12 source repositories connected to it.

In a many-to-many environment, a replication grid can have up to 2 groups of 4 target/source repositories replicating to each other per group. So, it can have up to two "topology groups" for a total of 8 members.

Creating a replication grid

Use the following procedure to create a replication grid:

Note: Grid IDs and repository IDs are numbers that are never recycled. Even if a repository "leaves" the grid and "re-enters" the grid, it does not receive the same ID. Thus, actions like leaving a grid are expected to be rare and are not a part of the normal flow of work.

1. Click **Create new grid**. The **Create new grid** dialog is displayed.

2. Complete the fields to define a grid. Type a unique **Grid ID** or select a unique **Grid ID** number (0 - 63) from the drop-down list and enter a name in the **Name** field.

   Note: ProtecTIER does not allow you to choose an ID that has already been used.

3. Click **Ok**. The new grid is added to the **Grids** list in the navigation pane of the Grids Management view.

Deleting a replication grid

Deleting a grid is only allowed if the grid is empty. In addition, once you have deleted a grid, the Grid ID cannot be reused. Being that there are only 64 grid numbers (0 - 63), deleting a grid means that you 'lose' one grid ID.

Taking over a VTL repository

If the repository at the production site (source) has been destroyed and cannot be repaired, you can replace it with a new repository. See "Replacing a destroyed VTL repository " on page 172.

Displaying removed repositories

To display a list of removed (unrecoverable) repositories and their replacements, click **Grid > Show removed repositories**. A table is displayed showing the list of removed repositories and their replacements according to their ID numbers and names.

Figure 37. Show removed repositories window

Go on to "Working with repositories in a replication grid" on page 118.

Working with repositories in a replication grid

The topics in this section explain how to manage and work with repositories in a replication grid.

Note: Repositories can replicate to each other only if they are part of the same grid and the same group. In addition, a repository cannot be a member of more than one grid.

Adding a repository to a replication grid

This task explains how to add a repository to a grid.

About this task

When you add a repository to a replication grid, the repository can be defined as a source or a destination.

To add a repository to a replication grid:

Procedure

1. From the Grids Management view, select **Repository > Add repository to grid**. The **Add repository to grid** window is displayed.

   Note: A repository cannot be a grid member of more than one grid.
2. Type the network replication IP address of the repository in the **Replication IP address** field.
3. Enter the username and password of the repository (User name: **ptadmin** and Password: **ptadmin**).
4. Click **Ok**. The repository is added to the replication grid.
5. If you have additional repositories to add to the replication grid, repeat this procedure for each one.

What to do next

Go on to "Working with Replication Groups in VTL" on page 119.

Removing a repository from a grid

You can use the **ProtecTIER Replication Manager** to remove a repository from a grid.

About this task

Note: Before removing a repository from a grid, carefully consider the potential effects on the system configuration. Once the source repository is removed from the grid, all the bandwidth reduction and replication deduplication information is deleted. The relationship between the original and replicated cartridge pair is lost and they cannot be updated in the same pair. If the repository rejoins the same grid, it looks like a new repository in the grid with a new ID, and all data should be replicated from beginning by new policies. Therefore, removing a repository from a grid is an operation you should plan with a PT specialist.

A repository can be removed from a grid only if it is a single node repository. See "Modifying a Replication Group for VTL" on page 124.

To remove a repository from a grid:

Procedure
1. From the Grids Management view, click the repository you want to remove.
2. Select **Repository > Remove repository from grid**. The **Remove repository from grid** window is displayed.
3. Complete the login information by typing the **User name** and **Password** of the repository.
4. Click **Ok**. The repository is removed from the grid.

What to do next

Note: Remove a repository from a grid, without coordination with the Replication Manager, only if the ProtecTIER Replication Manager thinks that the repository is not a part of the grid already, or the Replication Manager was destroyed and is not meant to be restored. To remove a repository from a grid without coordination, see "Forcing a repository to leave a grid" on page 251.

Updating the replication IP address of a grid member

Complete this task to update the Replication Manager about a change in the replication IP address of a grid member.

If the replication IP address of a grid member is changed, you need to update the ProtecTIER Replication manager with the new IP address.

To update the replication manager about a change in the IP address of a repository, select **Repository > Update repository address**. The **Update repository address** screen is displayed. Enter the updated IP address and click **Ok.**

Working with Replication Groups in VTL

This section describes how to work with replication groups in "many-to-one" and "many-to-many" VTL environments.

In a "many-to-one" VTL environment, replication groups are created where up to 12 source repositories ("spokes") can receive local backups and replicate to a single destination ("hub"). The destination repository can, then act as a Disaster Recovery site for any number of the source repositories, and still allowing local backups, as well as replication, from the active source repositories.

In a "many-to-many" VTL environment, replication groups are created where multiple repositories can replicate to each other. A many-to-many replication group can be defined with up to four repositories, where each repository assumes the responsibility of a hub repository and can receive local backups, replicate data to remote hub repositories, as well as receive replicated data from remote hub repositories.

The same cartridge can be replicated from its principal repository to up to three destination repositories. Different cartridges can be replicated between multiple hub repositories in a bidirectional manner.

Note: Source repositories are not supported in a four-way many-to-many replication grid.

Creating a Replication Group for VTL

This task explains how to create a replication group in a replication grid for VTL.

About this task

Before defining any replication policy, you must create a replication group with a physical connection between the repositories. Different steps are followed for creating a replication group in "many-to-one" and "many-to-many" topologies.

- If you are creating a replication group in a many-to-one topology, see "Many-to-one topology."
- If you are creating a replication group in a many-to-many topology, see "Many-to-many topology" on page 121.

Many-to-one topology

Follow this procedure to connect a source and destination repository in a many-to-one replication group.

Procedure

1. From the Grids Management view, click a single node repository.
2. Select **Group > Replication group management**. The **Replication group management** wizard is displayed. Click **Next**.

   Tip: The **Replication group management** wizard can be accessed in a number of ways, either: right-click on a repository and select **Replication group management**, click the **Replication group management** icon on the toolbar, or select **Group > Replication group management**.
   The following window is displayed:

Figure 38. Many-to-one replication method topology window

3. Select the **Many-To-One (VT systems)** topology and click **Next**. The **Hub selection** window is displayed.

4. Select a repository to set as the destination from the **Hub repository** drop-down list and click **Next**. The **Repositories selection** window is displayed.

5. Select the repositories to connect as spokes for the selected hub and click **Next**. The **Preview** window of the replication group is displayed.

6. Type a **Group name** in the **Replication group settings** window and click **Finish**. The **Replication group management** wizard closes and the replication group is displayed in the Replication Manager.

What to do next

Repeat this procedure or run the "Many-to-many topology" procedure to create additional replication groups, or go on to define and create replication policies (see "Replication policies" on page 124). To continue modifying the replication group (see "Modifying a Replication Group for VTL" on page 124.

Many-to-many topology

Follow this procedure to connect up to 4 destination repositories in a many-to-many replication group.

Procedure

1. From the Grids Management view, click a single node repository.

2. Select **Group > Replication group management**. The **Replication group management** wizard is displayed. Click **Next**.

   Tip: The **Replication group management** wizard can be accessed in a number of ways, either: right-click on a repository and select **Replication group management**, click the **Replication group management** icon on the toolbar, or select **Group > Replication group management**.

3. Select the **Many-To-Many (VT systems)** topology as shown:
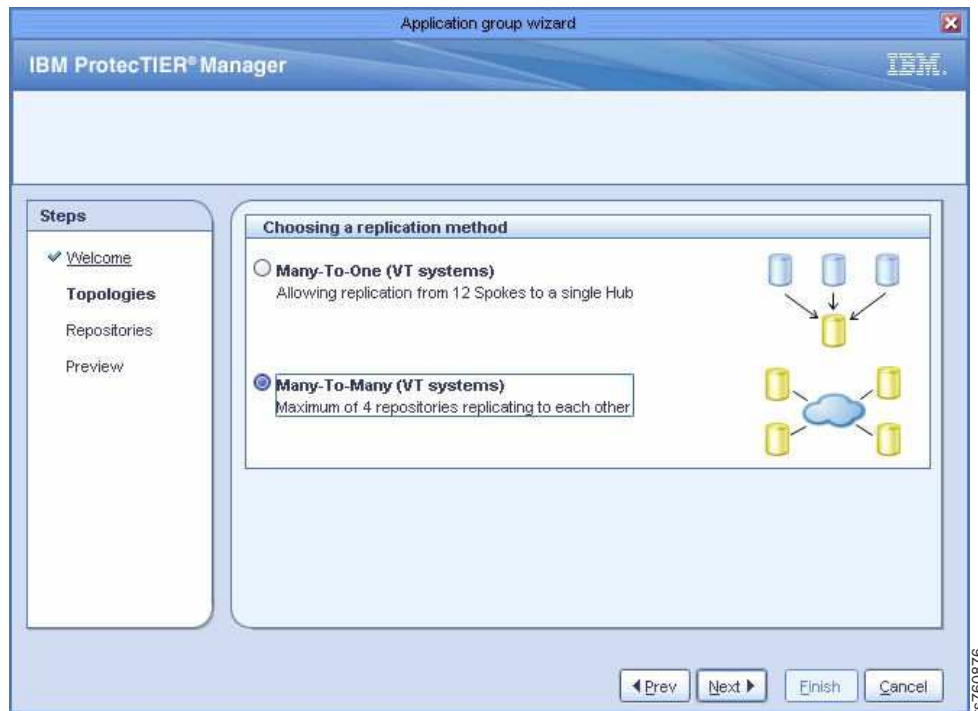
Figure 39. Many-to-many replication method topology window

4. Click **Next**. The **Repositories selection** window is displayed.
5. Select the destination repositories from the list that appears to be part of the replication group.
6. Click **Next**. The **Preview** window of the Replication Group is displayed.
7. Type a **Group name** in the **Replication group settings** window and click **Finish**. The **Replication group management** wizard closes and the replication group is displayed in the Replication Manager.

What to do next

Repeat this procedure or run the "Many-to-one topology" on page 120 to create additional replication groups, or go on to define and create replication policies (see "Replication policies" on page 124). To continue modifying the replication group (see "Modifying a Replication Group for VTL" on page 124.

Adding a single node repository to a replication group

This task explains how to add a single node repository to a replication group.

About this task

Use the **Replication group management** wizard to add and remove single node repositories from a replication group.

Procedure

1. From the Grids Management view, click a single node repository.
2. Select **Group > Replication group management**. The **Replication group management** wizard is displayed.

Tip: The **Replication group management** wizard can be accessed in one of the following ways:
- Right-click on a repository
- Click the **Replication group management** icon on the toolbar
- Select **Group > Replication group management**

3. Click Next. The following options appear:
   - Creating a new replication group
   - Join an existing replication group

   Note: In order to create a replication group, there must be at least two single node repositories in the grid.

   To join an existing replication group, go on to "Adding a single node repository to an Existing Replication Group." If you are adding a repository to a new replication group, continue with step 4

4. Select **Creating a new replication group**.
5. Click Next. The **Repositories selection** window is displayed.
6. Select the repositories to be added to the replication group.
7. Click Next. A preview of the replication group is displayed.
8. Type the appropriate name of the replication group and click Finish. The **Replication group management** wizard closes and a new replication group is created.

What to do next

Once the operation is complete, go on to define and create replication policies (see "Replication policies" on page 124), or continue working with replication groups.

Adding a single node repository to an Existing Replication Group
Procedure

1. From the Grids Management view, click a single node repository.
2. Select **Repository > Replication group management**. The **Replication group management** wizard is displayed.
3. Click Next. The following options appear:
   - Creating a new replication group
   - Join an existing replication group
4. Select **Join an existing replication group**.
5. Click Next. The **Group selection** window is displayed.
6. Choose an existing replication group to join from the **Existing replication group** drop-down list. A preview of the existing replication group selected is displayed.
7. Click Finish. The wizard closed and the repository is added to the existing replication group.

What to do next

Once the operation is complete, go on to define and create replication policies (see "Replication policies" on page 124), or continue working with replication groups.

Modifying a Replication Group for VTL

This task explains how to modify an existing replication group by adding or removing members.

About this task

Use the **Replication group management** wizard to add and remove repositories from an existing replication group.

Procedure

1. From the Grids Management view, click a repository in an existing replication group.

2. Select **Group > Replication group management**. The **Replication group management** wizard is displayed.

   Tip: The **Replication group management** wizard can be accessed in one of the following ways:
   - Right-click on a repository
   - Click the **Replication group management** icon on the toolbar
   - Select **Group > Replication group management**

3. Click **Next**. The **Repositories selection** window is displayed. Repositories that are already members of the replication group are checked and standalone grid members appear cleared.

   Note: In a many-to-one topology, this window will appear as **Spokes selection**.

4. Select or clear the repositories to add or remove from the replication group. Alternatively, **Select all** adds all the repositories in the selection list to the replication group. **Select none** removes all the repositories from the replication group.

   Note: When you clear a check box for a repository, the **Group status** appears as **Deleted**. If you select a repository to add, the **Group status** appears as **New**.

5. Click **Next**. The **Preview** window of the replication group is displayed.

6. Click **Finish**. The **Replication group management** wizard closes. A **Confirm operation** window is displayed with a notification that all running and pending replications will be aborted from the deleted members and that unreachable repositories will not be updated with the changes.

7. Click **Yes** to continue with the operation, or **No** to cancel the operation.

What to do next

Once the operation is complete, go on to define and create replication policies (see "Replication policies"), or continue working with replication groups.

Replication policies

The topics in this section describe how to manage replication policies in a VTL environment.

Defined and managed through the Systems Management view of ProtecTIER Manager, a replication policy can only be created on a repository that is a member of a replication group and applies only to the repository on which it's defined. A replication policy defines a set of objects (for example, cartridges) from a repository

that need to be replicated to a remote repository. A replication policy serves as the only means to transfer de-duplicated data from a source repository to a destination repository.

Using a set of rules, an event occurs, for example, which indicates that the data segment on a cartridge has changed and that replication may be needed for the specific cartridge. Once the event matches with a policy, a "trigger" is created for replication activity and a job occurs.

In a many-to-many environment, up to 256 policies may be defined per repository and up to 1023 ranges of cartridges may be defined per replication policy. A source repository can replicate a range of cartridges to up to three different destination repositories with different priorities. "Visibility switching" can be enabled on one of the destination repositories. See "Creating a replication policy" on page 126 for more information.

Select **Replication Policies** in the navigation pane to view the policies defined. Select a policy from the list to view the policy details and replication statistics per destination.
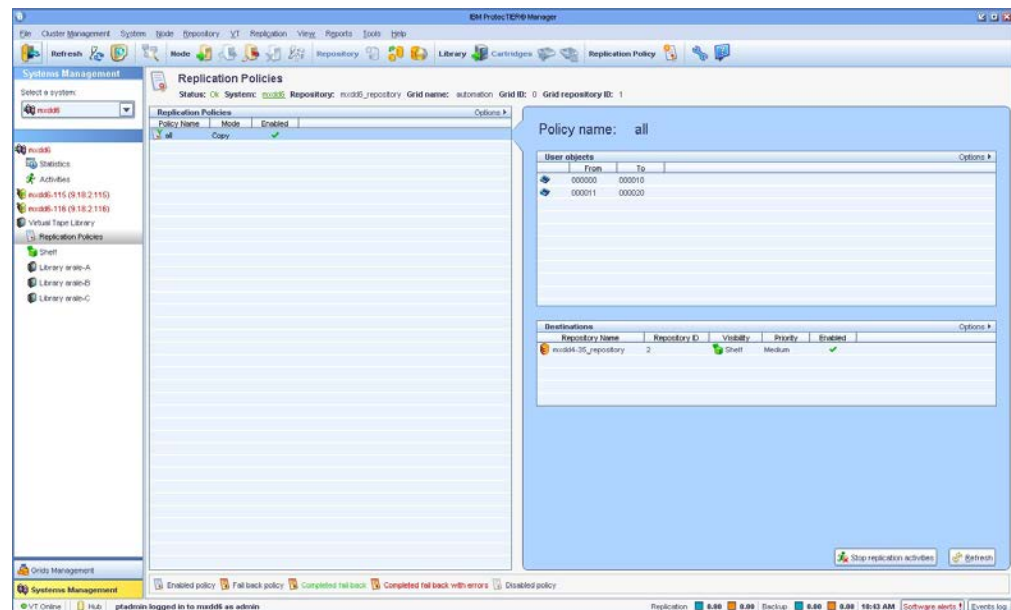
Figure 40. View of replication policy

The following sections describe how to create and work with replication policies:
- "Setting the weekly replication timeframe" on page 130
- "Setting the centralized time frame" on page 131
- "Setting the replication rate limit" on page 132
- "Limiting the network interface bandwidth" on page 133
- "Creating a replication policy" on page 126
- "Enabling and disabling a policy" on page 127
- "Running a policy" on page 128
- "Modifying a policy" on page 129
- "Deleting a policy" on page 130

Creating a replication policy

This section describes how to create a replication policy using the **Create policy** wizard in the ProtecTIER Manager software.

When creating a replication policy, the following parameters are defined:
- Replication policy name
- Barcode ranges
- Replication destination
- Visibility change

  "Visibility change" is the means by which you can determine "where" cartridges actually exist. From a backup application standpoint, a specific cartridge or barcode can "exist" in only one location at a given time. Once exported by the backup application, cartridges can be placed on a virtual *shelf* that is visible via ProtecTIER, providing more flexibility in managing tapes/cartridges and where they are kept – similar to keeping physical tapes on an actual shelf outside of the tape library.

About this task

To create a replication policy, complete the following steps:

Procedure

1. Choose **Replication > Replication Policy > Create policy**. The Welcome window of the **Create policy** wizard is displayed.
2. Click **Next**. The **Properties** window is displayed. Type a unique policy name in the Policy name field. You cannot have the same policy name twice. If you do define the same policy name, an error message is displayed.
3. Select the **Policy enabled** checkbox to run the policy within the timeframe defined. All incoming replication events will look to apply their rules to the policy's definition. If the **Policy enabled** checkbox is not selected, no replication activities will take place.
4. Click **Next**, the **Destinations** window is displayed.
5. From the **Destinations** option, select the repositories on which to run the defined policy.

   Note: If a member has left the replication group, the policy destination will be removed from the list and a warning will display that the member will be removed from the policy.
6. Select a **Priority** per destination.

   Policies have 3 options of priority: High, Medium, Low. Define the policy's **Priority** according to the importance and/or urgency of the data that needs to be transferred. For example, a policy with a high priority is transferred first, then a policy with medium priority, followed by low priority. The default is Low for every policy.
7. Click **Next**. The **Visibility** window is displayed.

   Visibility controls the location of replicated cartridges at the destination repository. Destination replica cartridges can be "invisible" (if you choose shelf) or "visible" (if you choose a library).
   - If **Visibility enabled** is not activated, the destination will be shelf for all of the repository destinations.

- If **Visibility enabled** is activated, you can choose a library for one of the destination repositories. The other destination repository targets will be shelf.

  Upon ejecting a cartridge, it is first moved to the shelf on the local repository. On the remote repository, the cartridge is moved to the import/export slot of a library so that the backup application on the remote site can see it.

8. Select a repository from the **Repository** dropdown list and the target on the destination repository, either the shelf or a library, from the **Library** dropdown list.

9. Click **Next**. The **Ranges** window is displayed. The policy objects, i.e. cartridges, are defined as barcode ranges. There can be up to 256 ranges in a single policy.

10. Type the **From** and **To** barcodes for a range of cartridges to be replicated.

11. Click **Add** to view the range in the **Ranges** table. If a barcode number or barcode range appears more than once, an error message is displayed with the conflict.

12. To delete the barcode ranges from the table, click **Select all and Remove**, or click **Select none** to deselect.

13. Click **Next** and **Finish** to commit and save the policy on the server. The **Summary report** is displayed with the policy name and the number of barcode ranges that were defined.

What to do next

Go on to "Enabling and disabling a policy."

Enabling and disabling a policy

You can enable or disable a policy from ProtecTIER Manager.

A policy can be enabled or disabled per destination. In the detailed view of a policy, an indication displays whether the policy is enabled, disabled, or enabled with some of its destinations disabled.

Enabling a policy

Upon successfully creating a policy, by default, the policy is enabled. This means that all incoming replication events will look to apply their rules to the policy's definition. If a policy is disabled, you can enable it from ProtecTIER Manager. This does not affect current running activities. Selecting **Policy enabled** automatically runs the policy within the timeframe defined. If **Policy enabled** is not selected, no activities will take place.

To enable a policy:

1. From the Systems Management view, select a policy from the **Replication Policies** pane.

2. Select **Replication > Replication policy > Enable policy**. The policy is enabled.

3. Go on to "Running a policy" on page 128.

   Important: After you enable a policy, it is best to run the new policy quickly to ensure that all the pending replication activities are included in the replication. Otherwise, only further backups will be triggered for a replication.

Disabling a policy

A policy can be disabled at any time from ProtecTIER Manager. If a policy is disabled, all new replication triggers will be ignored for the cartridge from the moment it is disabled. This does not affect currently replicated cartridges and the replication activities are gradually finished.

To disable a policy:
1. From the Systems Management view, select a policy from the **Replication Policies** pane.
2. Select **Replication > Replication policy > Disable policy**. The policy is disabled.
3. Go on to "Running a policy."

Important Notes:
- Disabling a policy clears the replication backlog of the specific replication policy only.
- After enabling a previously disabled policy, it is best to run the new policy quickly to ensure that all the pending replication activities are included in the replication. Otherwise, only further backups will be triggered for a replication.

Running a policy

Complete this task to run a policy.

Policies can be run either manually or automatically. Whenever replication events are received, policies are continuously run. The most common types of triggers for automatic replication are:
- backup
- eject
- unload cartridge

Manually run policies create replication jobs for all the valid cartridges in their list, whether or not they need to be replicated.

Running a policy leads to lining up replication jobs in their respective priority queues where they wait for resources and the replication timeframe to start replicating.

To run a policy:
1. Select **Replication > Replication Policy > Run replication policy**.
2. Select the destination repositories on which to run the repository.
3. Click **Run**. The replication policy will begin to run.

Note: If you run a policy with a single destination, no destinations need to be selected. Or, if you select multiple policies to run, no destinations are chosen.

Running a policy on a cartridge

You can also replicate a specific cartridge that is within the range of cartridges in a specific policy. To manually run the policy on the specific cartridge, do the following:
1. Select the **Cartridges** tab view of the library.

2. Right-click on the cartridge or group of cartridges.
3. Select **VT** > **VT Cartridge** > **Cartridge replication** and click **Yes**. The policy will run on the selected cartridge.

Modifying a policy

You can modify a policy to change the parameters originally defined during policy creation.

About this task

Complete the following steps to modify a policy:

Procedure

1. Select **Replication > Replication Policy > Modify policy**. The **Modify policy** welcome screen is displayed.
2. Click **Next**. The **Properties** window is displayed. Type a unique policy name in the Policy name field. You cannot have the same policy name twice. If you do define the same policy name, an error message is displayed.
3. Select the **Policy enabled** checkbox to run the policy within the timeframe defined. All incoming replication events will look to apply their rules to the policy's definition. If the **Policy enabled** checkbox is not selected, no replication activities will take place.
4. Click **Next**, the **Destinations** window is displayed.
5. From the **Destinations** option, select the repositories on which to run the defined policy.

   Note: If a member has left the replication group, the policy destination will be removed from the list and a warning will display that the member will be removed from the policy.

6. Select a **Priority** per destination.

   Policies have 3 options of priority: High, Medium, Low. Define the policy's **Priority** according to the importance and/or urgency of the data that needs to be transferred. For example, a policy with a high priority is transferred first, then a policy with medium priority, followed by low priority. The default is *Low* for every policy.

7. Click **Next**. The **Visibility** window is displayed.

   Visibility controls the location of replicated cartridges at the destination repository. Destination replica cartridges can be "invisible" (if you choose shelf) or "visible" (if you choose a library).

   • If **Visibility enabled** is not activated, the destination will be shelf for all of the repository destinations.
   • If **Visibility enabled** is activated, you can choose a library for one of the destination repositories. The other destination repository targets will be shelf.

     Upon ejecting a cartridge, it is first moved to the shelf on the local repository. On the remote repository, the cartridge is moved to the import/export slot of a library so that the backup application on the remote site can see it.

8. Select a repository from the **Repository** dropdown list and the target on the destination repository, either the shelf or a library, from the **Library** dropdown list.

9. Click **Next**. The **Ranges** window is displayed. The policy objects, i.e. cartridges, are defined as barcode ranges. There can be up to 256 ranges in a single policy.

10. Type the **From** and **To** barcodes for a range of cartridges to be replicated.

11. Click **Add** to view the range in the **Ranges** table. If a barcode number or barcode range appears more than once, an error message is displayed with the conflict.

12. To delete the barcode ranges from the table, click **Select all and Remove**, or click **Select none** to deselect.

13. Click **Next** and **Finish** to commit and save the policy on the server. The **Summary report** is displayed with the policy name and the number of barcode ranges that were defined.

Deleting a policy

Deleting a policy removes the policy in its entirety from the repository. All running and pending activities are aborted.

Complete the following steps to delete a policy:

Select **Replication > Replication Policy > Delete policy**. A dialog will appear to confirm the action and a message that all running and pending activities will be aborted. Although the effect is not immediate, the backlog is reduced because the pending activities are canceled one by one in the background.

Setting the weekly replication timeframe

Scheduling a timeframe for replication to take place for all policies allows you to maximize your system's resources and prioritize between backups and replication.

About this task

Defining a replication timeframe gives replication the highest priority with the maximum system resources used to complete the replication during the "replication window". You can define a replication timeframe using the **Set Replication Timeframe** dialog. Outside of the set timeframe replication is **off** and does not run.

If you choose backup as the priority, or no replication timeframe is defined, replication runs continuously all day, but on low priority, thereby consuming minimal resources from the system.

You can also limit the replication throughput through the **Replication Rate Limits** window (see "Setting the replication rate limit" on page 132).

Note: If you define a timeframe both on the source and on the destination repositories, you need to adjust both to the same time settings.

To set the replication timeframe:

Procedure

1. From the Systems Management view, select **Replication > Set Replication timeframe**. The **Set Replication timeframe** dialog box is displayed.
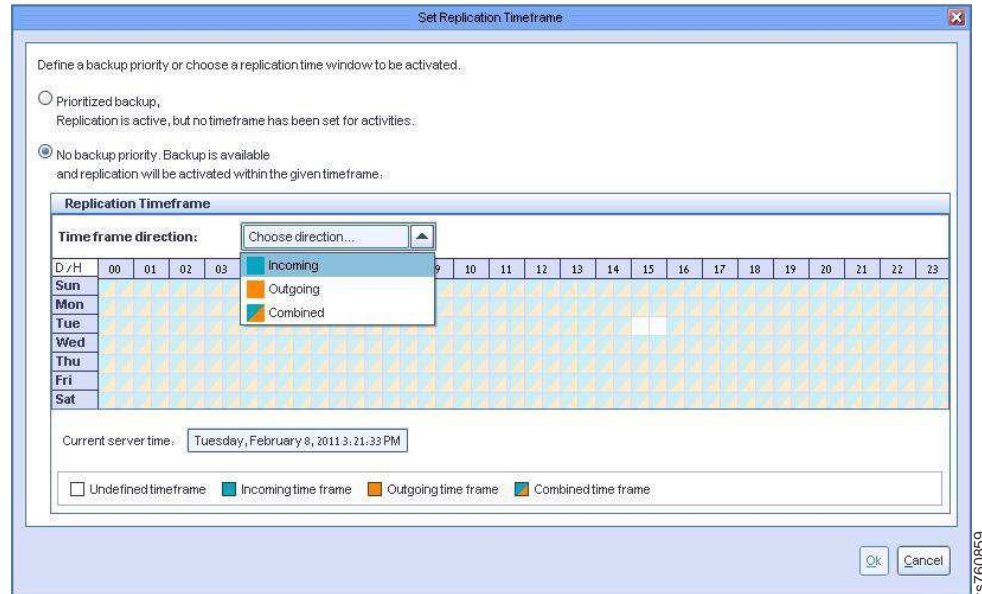
Figure 41. Set replication time frame window

2. Select an option:
   - **Prioritized backup** – Replication is active, but is of low priority.
   - **No backup priority** – Replication is off and only activated during defined timeframe.
3. Select the **Time frame direction** from the dropdown list to display the time frames scheduled for each replication task, or you can schedule a time frame for incoming, outgoing, or bi-directional (combined) replication tasks.
4. Select the replication window in daily half-hour intervals.
5. Click **OK**. The replication timeframe is set.

What to do next

Go on to "Setting the centralized time frame."

Setting the centralized time frame

The centralized timeframe shifts the scheduling management of replication policies from the repository scope to the grid level scope to provide improved management of different replication windows.

About this task

The centralized time frame allows for alignment of repositories in different time zones and provides a centralized view for managing the replication time frames for all repositories in a replication grid. The time frames associated with specific replication topology groups can be configured individually.

Procedure

1. To set the centralized time frame, select a repository in the **Grids Management** view.

2. Right-click on the repository and select **Centralized time frame**, or select **Centralized time frame** from the **Group** menu. The **Centralized Time Frame** window displays with the repositories in the replication grid.

3. Select the **Time frame direction** from the dropdown list to display the time frames scheduled for each replication task, or you can schedule a time frame for incoming, outgoing, or bi-directional replication tasks.

4. Define the task precedence by selecting **Replication timeframe** to activate replication within a given time frame, or select **Backup precedence** to keep replication active, but with low priority. If no time frame is selected, replication activities are blocked.

5. Select the replication window in daily half-hour intervals.

   If the repository selected is in the same time zone with other repositories, the time zone will be displayed as *Local* in the **Time zone** column. Otherwise, the time adjustment is displayed.

6. Click **Save changes** and **Close** when finished.

Setting the replication rate limit

Setting the replication rate control allows you to limit the nominal and physical throughput (data flow rate) of replication.

About this task

The values set for the physical and nominal limits have no explicit influence on one another. That is, the values set in the physical throughput may, but do not necessarily impact those values set in the nominal throughput, and vice versa.

The physical throughput limit restrains the amount of I/O and resources replication consumes on the local repository. Implicitly, this reduces the total load on the replication networks used by the repository (you can have 2 networks) and the amount of resources needed on the peer repository, as well.

The nominal throughput directly affects the load on the destination repository. On the source repositories, the replication nominal rate does not necessarily compete with the backup. Setting the limit on a source repository guarantees that the backup gets the total possible throughput minus the nominal limit, but in many cases this is not needed.

The **Replication Rate Limits** window displays physical and nominal throughput. You can define one limit that applies to both incoming and outgoing replication activity or accept the **Default settings** mode, **Combined settings** mode, or you can define separate limits for incoming and outgoing replication activity by choosing the **Individual settings** mode.

Procedure

1. From the Systems Management view, select **Set replication rate limits** from the **Replication** menu.

2. Choose the preferred mode to define the incoming and outgoing replication rate limits:
   - **Default settings**
   - **Combined settings**
   - **Individual settings**

3. Select the checkbox next to the desired option and enter a value (in MB/Sec). If a checkbox is not selected, the value will revert to an unlimited replication rate.

Note: When replication time frames are defined and replication is taking place with the time frame, replication will not be limited. If the system is not within the replication time frame, no replication will take place.

4. To return to the original replication rate limits that were defined during installation for the physical and/or nominal throughputs, select **Default system settings** as the mode. The values will default to their original settings at setup.

Following are the default values for the **combined** replication rate limits:

Table 27. Combined replication rate limits

Combined settings	Default values (Incoming & Outgoing)
Physical throughput limits (MB/Sec)	Unlimited
Limit when no backup or restore load (MB/Sec)	Max nominal throughput (the value selected during new repository creation)
Limit during backup or restore load (MB/Sec)	15% of max nominal throughput
Limit within a replication timeframe (MB/Sec)	Unlimited

Following are the default values for the **individual** replication rate limits:

Table 28. Individual replication rate limits

Individual settings	Default values (Incoming)	Default values (Outgoing)
Physical throughput limits (MB/Sec)	Unlimited	Unlimited
Nominal throughput limit when no backup or restore load (MB/Sec)	Max throughput	Max throughput
Nominal throughput limit during backup or restore load (MB/Sec)	15% of max throughput	15% of max throughput
Nominal throughput limit within a replication timeframe (MB/Sec)	Unlimited	Unlimited

5. Click **Ok** to save the changes and close the window.

What to do next

Go on to "Limiting the network interface bandwidth."

Limiting the network interface bandwidth

Complete the task in this topic to limit the bandwidth or throughput of a network interface, such as a port, on a node that is running replication.

About this task

Note: This task should be performed only if it is important to limit each one of the interfaces separately. If you want to limit the total throughput over the networks, refer to "Setting the replication rate limit" on page 132 and set the physical replication rate limit of the repository.

Procedure

1. From the Systems Management view, select a system that is being used for replication from the navigation pane. The **IP network configuration** is displayed.
2. Highlight one of the devices (e.g. eth3 or eth4) under **Replication network** appearing in the **IP Network configuration** pane. The device properties are displayed to the right.
3. Click **Limit bandwidth** on the bottom-right of the **Device properties** window. The **Limit network interface bandwidth** window is displayed:
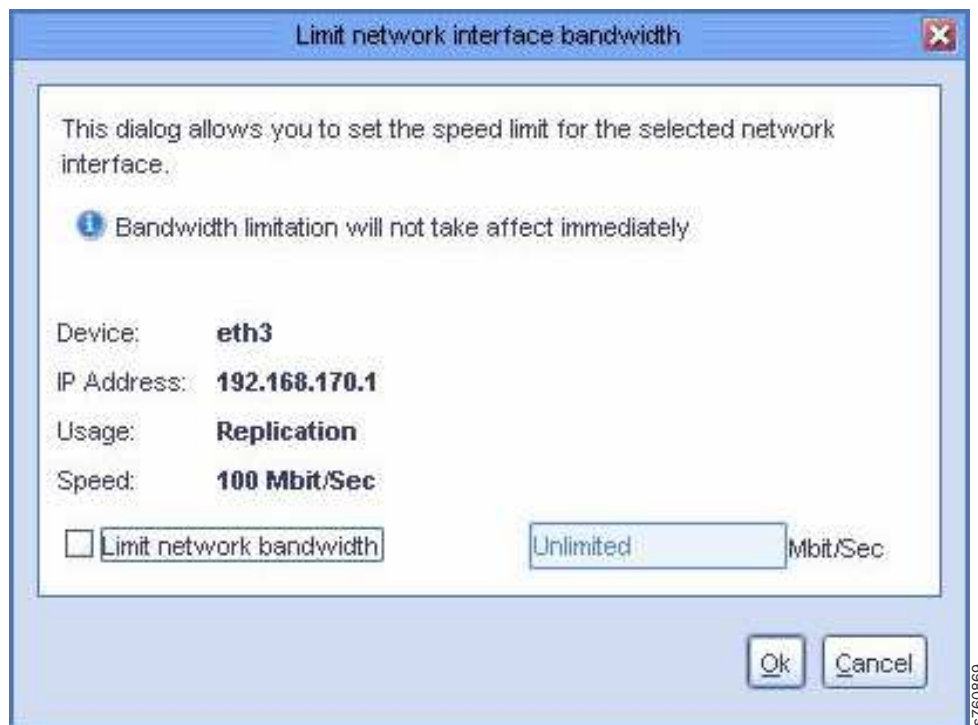
Figure 42. Limit network interface bandwidth window

4. Select the **Limit network bandwidth** checkbox to redefine the bandwidth speed (in Mbit/Sec). The bandwidth limit value can range from 1 to 1000. Other values will not be accepted. If the checkbox is not selected, the value will default to an unlimited bandwidth speed.
5. Click **Ok**. The defined limit is displayed in the **Limit (Mbit)** field of the **Replication network** display of the device.

Results

Note: If the bandwidth limitation is changed during replication, the change does not take effect immediately. If replication begins after the bandwidth limitation change, the effect is immediate.

What to do next

Go on to "Creating a replication policy" on page 126.

Monitoring the replication grid

ProtecTIER Manager is used to monitor a replication grid. It is possible to see current grid members and their status, the relationship between the grid members and the actual throughput of replication data between the grid members.

The ProtecTIER Replication Manager periodically updates the status of the grid members and ProtecTIER Manager receives the status updates from the ProtecTIER Replication Manager. The status includes whether the grid member is online, if the grid member reports any errors related to replication, and statistics regarding replication activity currently being run on the grid member.

The grid map feature provides a consolidated view of the entire replication grid with the actual topology groups deployment. The map provides indications for local backups, replication rates and allows panning and zooming capabilities.

Select a grid from the navigation pane and click on one of the repositories. The grid member details are displayed to the right.

The Information tab displays the following:
- Capacity - physical and nominal
- Replication activities - running, pending, and backlog
- Backup activities
- Grid member replication configuration

The details displayed are a partial view of the full repository view. For more information, see "Monitoring the ProtecTIER VTL system performance statistics" on page 143.
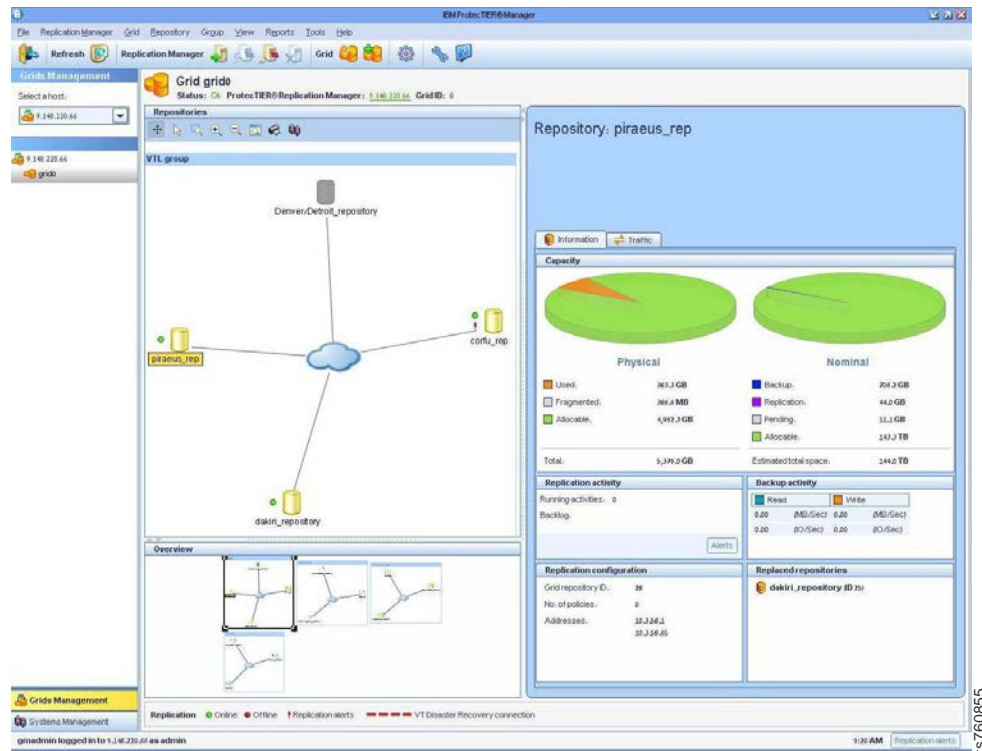
Figure 43. Detailed view of a repository in a replication group

Click the **Traffic** tab to display the replication direction.

Chapter 11. Monitoring ProtecTIER Virtual Tape Libraries

The topics in this chapter describe how to use ProtecTIER Manager to monitor the status and performance of the ProtecTIER VTL system elements. In addition, information is provided for monitoring system functions and host activity from within the Linux shell.

Monitoring ProtecTIER systems

This section describes how to use ProtecTIER Manager to monitor all the systems in the ProtecTIER environment from one common view.

The **All systems view** displays a list of all the systems in ProtecTIER that are configured in ProtecTIER Manager, as shown:
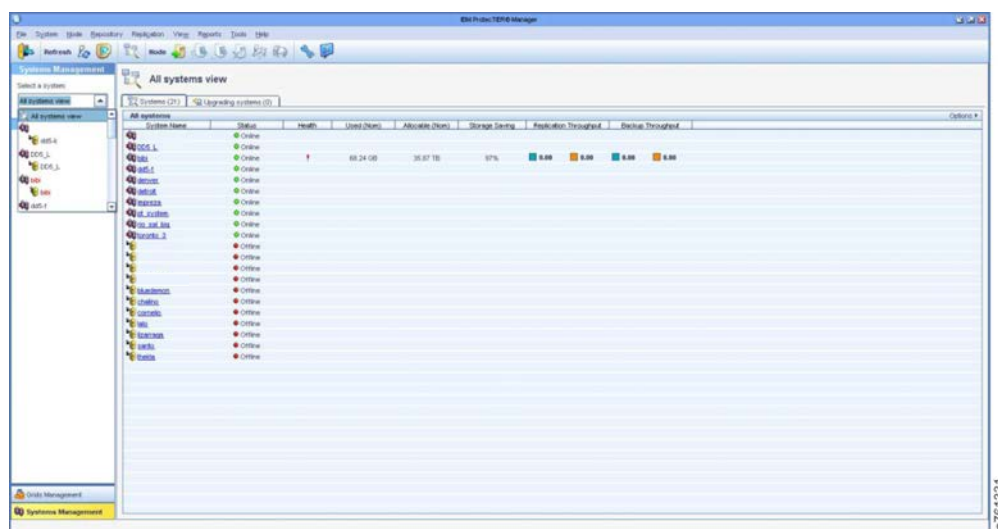

Figure 44. All systems view

Any node that has been added to ProtecTIER Manager using the **Add node** option appears in this view.

From the **All systems view**, you can log in to *online* systems by clicking on the hyperlink of the **System Name**. When you click on the hyperlink, the system's login window displays. Type in your username and password as you do when selecting a specific system from the **Select a system** dropdown list.

If the system is offline, ProtecTIER Manager refreshes the system view, and you can try to log in again. If the system still remains offline, a message displays that the system cannot be detected.

Table 29. All systems view description. The **All systems view** is the first option appearing in the **Select a system** dropdown list. From the **All systems view**, select the **Systems** tab to monitor the following system details:

Column name	Description
System Name	Displays the name of the ProtecTIER system as it appears in ProtecTIER Manager.

Table 29. All systems view description (continued). The **All systems view** is the first option appearing in the **Select a system** dropdown list. From the **All systems view**, select the **Systems** tab to monitor the following system details:

Column name	Description
Status	Displays if the system is online, offline, or upgrading. If the system is a two-node cluster and one node is down, the status appears as *partially* online with a warning that a node is down.
Health	Displays an exclamation point (!) if there is a software error, hardware error, or both.
Used (Nom)	Displays the total nominal capacity used for backup and replication.
Allocable (Nom)	Displays the amount of nominal space available for backup and replication.
Storage Saving	Displays the percentage of data saved that is derived from the deduplication ratio. The storage savings is equal to (1-1/*deduplication ratio*) x 100.
Replication Throughput	Displays the physical and nominal throughput of incoming and outgoing replication activity.
Backup Throughput	Displays the read and write throughput during backup activity.

From the **All systems view**, select the **Upgrading systems** tab to monitor the progress of the ProtecTIER systems undergoing a code upgrade. For more information on upgrading ProtecTIER software, refer to the *IBM TS7650 ProtecTIER Software Upgrade Guide*, V3.3.6.1, SC27-3643.

Monitoring the ProtecTIER VTL system

The topics in this section describe monitoring of the ProtecTIER VTL system.

In the **Systems Management** view, select a system name from the **Select a system** dropdown list in the navigation pane. The **System** monitoring window is displayed:
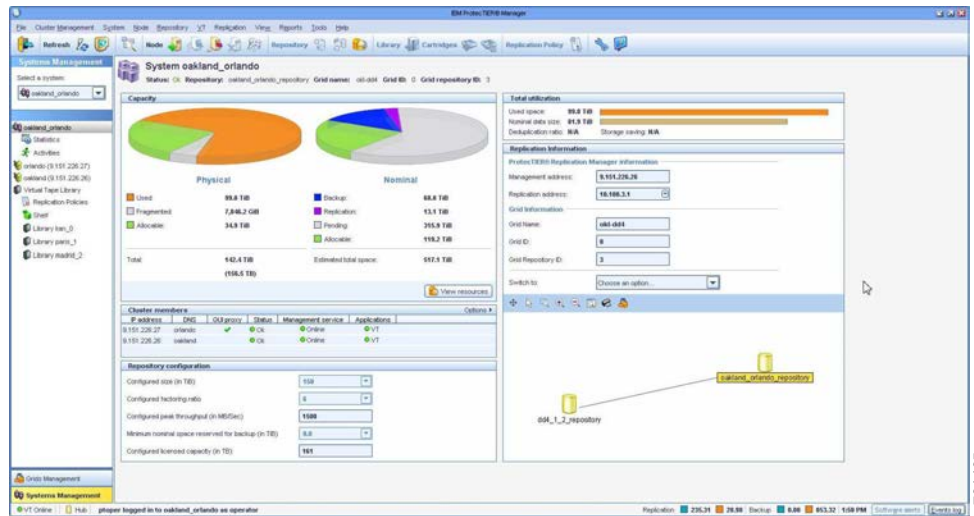
Figure 45. VTL System monitoring screen

The **System** window displays the general system configuration.

In addition, the ProtecTIER Manager status bar displays icons. These icons are for the total read and write replication and backup throughput rates for the selected system and the system time. (The status bar is at the bottom of the window.)

The status bar at the bottom of the view pane also displays the Software alerts and Events log buttons which enable you to view alert and event information for the nodes of the selected system. (For more information, see "Viewing the alerts and events log windows" on page 215.)

The **System** window consists of the following panes:

"Capacity" displays the breakdown of the physical and nominal data capacity of the system.

"Cluster members" on page 141 displays the makeup of the cluster members.

"Repository configuration" on page 141 displays the configuration settings used to build the repository of the system.

"Total utilization" on page 142 describes the total utilization of the system.

"Replication information" on page 142 displays the replication information about the system.

Capacity

This topic describes the breakdown of the ProtecTIER physical and nominal data capacity.

The **Capacity** pane displays the physical and nominal data breakdown of the repository of the selected system:

Physical

- **Used** refers to the amount of disk space currently containing physical data
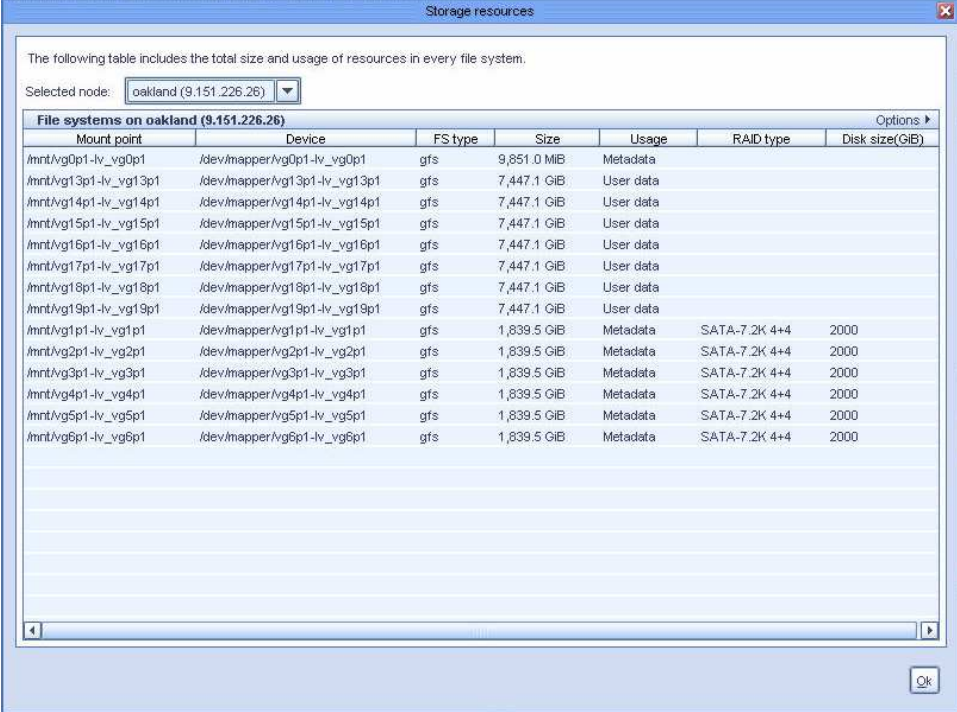
- **Fragmented** refers to the amount of disk space pending the ProtecTIER defragmentation operation
- **Allocable** refers to the amount of free disk space available to contain physical data
- **Total** refers to the overall physical space available to the system

Nominal

- **Backup** refers to the amount of nominal data containing backup data
- **Replication** refers to the amount of nominal data used for replication
- **Pending** refers to the amount of nominal data pending deletion and defragmentation activities
- **Allocable** refers to the amount of free disk space available to hold nominal data
- **Estimated space** refers to the overall estimated nominal space supported by the system

  Note: The **Estimated space** value is based on the current deduplication ratio.

Click **View resources** to open the **Storage resources** window.

The following table includes the total size and usage of resources in every file system.

Selected node: oakland (9.151.226.26)

File systems on oakland (9.151.226.26)   Options ▶

Mount point	Device	FS type	Size	Usage	RAID type	Disk size(GiB)
/mnt/vg0p1-lv_vg0p1	/dev/mapper/vg0p1-lv_vg0p1	gfs	9,851.0 MiB	Metadata		
/mnt/vg13p1-lv_vg13p1	/dev/mapper/vg13p1-lv_vg13p1	gfs	7,447.1 GiB	User data		
/mnt/vg14p1-lv_vg14p1	/dev/mapper/vg14p1-lv_vg14p1	gfs	7,447.1 GiB	User data		
/mnt/vg15p1-lv_vg15p1	/dev/mapper/vg15p1-lv_vg15p1	gfs	7,447.1 GiB	User data		
/mnt/vg16p1-lv_vg16p1	/dev/mapper/vg16p1-lv_vg16p1	gfs	7,447.1 GiB	User data		
/mnt/vg17p1-lv_vg17p1	/dev/mapper/vg17p1-lv_vg17p1	gfs	7,447.1 GiB	User data		
/mnt/vg18p1-lv_vg18p1	/dev/mapper/vg18p1-lv_vg18p1	gfs	7,447.1 GiB	User data		
/mnt/vg19p1-lv_vg19p1	/dev/mapper/vg19p1-lv_vg19p1	gfs	7,447.1 GiB	User data		
/mnt/vg1p1-lv_vg1p1	/dev/mapper/vg1p1-lv_vg1p1	gfs	1,839.5 GiB	Metadata	SATA-7.2K 4+4	2000
/mnt/vg2p1-lv_vg2p1	/dev/mapper/vg2p1-lv_vg2p1	gfs	1,839.5 GiB	Metadata	SATA-7.2K 4+4	2000
/mnt/vg3p1-lv_vg3p1	/dev/mapper/vg3p1-lv_vg3p1	gfs	1,839.5 GiB	Metadata	SATA-7.2K 4+4	2000
/mnt/vg4p1-lv_vg4p1	/dev/mapper/vg4p1-lv_vg4p1	gfs	1,839.5 GiB	Metadata	SATA-7.2K 4+4	2000
/mnt/vg5p1-lv_vg5p1	/dev/mapper/vg5p1-lv_vg5p1	gfs	1,839.5 GiB	Metadata	SATA-7.2K 4+4	2000
/mnt/vg6p1-lv_vg6p1	/dev/mapper/vg6p1-lv_vg6p1	gfs	1,839.5 GiB	Metadata	SATA-7.2K 4+4	2000

Ok

Figure 46. Storage resources window

The **Storage resources** window displays the list of metadata and user data file systems for the repository of the selected system.

When the physical capacity on a file system, specifically ProtecTIER user data, is defined, a portion of the physical space is reserved for internal metadata structures. This metadata contains information such as data block allocation mapping and reference count (a number depicting how many objects are using, or

referencing, a specific block). For ProtecTIER, it means that the usable capacity is lower than the physical capacity by approximately 3 percent.

Note: You can open the **Storage resources** dialog at any time by selecting **View resources** from the **Repository** menu.

When the physical capacity on a file system, specifically ProtecTIER user data, is defined, a portion of the physical space is reserved for internal metadata structures. This metadata contains information such as data block allocation mapping and reference count (a number depicting how many objects are using, or referencing, a specific block). For ProtecTIER, it means that the usable capacity is lower than the physical capacity by approximately 3 percent.

Cluster members

This topic describes how to monitor the cluster members of a ProtecTIER system.

The **Cluster members** pane displays the following information about each node in the cluster:

Table 30. Cluster member information

Column	Definition
IP Address	IP address of the node.
DNS	Name of the node.
GUI proxy	Indicates which node is currently being used by ProtecTIER Manager to monitor the cluster.
Status	Indicates whether ProtecTIER is online or offline on the node.
Management service	Indicates whether the Management service is online or offline.
Applications	Indicates whether the VT service for that node is online or offline.

Repository configuration

This topic describes how to monitor the configuration settings used to build the repository on the ProtecTIER system.

The **Repository configuration** pane displays the following information:

Table 31. Repository information

Field	Description
Configured size (in TiB)	The physical repository size, in tebibytes, that was specified when the repository was created.
Configured factoring ratio	The estimated HyperFactor factoring ratio that was specified when the repository was created.
Configured peak throughput (in MB/Sec)	The expected maximum peak throughput that was specified when the repository was created.

Table 31. Repository information (continued)

Field	Description
Minimum nominal space reserved for backup (in TiB)	The minimum amount of nominal space that is currently reserved for backup on the repository.
Configured license capacity (in TiB)	The physical capacity of the repository, in tebibytes, that is specified by the user license. (The unit is shown in TiB as a decimal format, which means it is a multiple of 1024.)

Total utilization

This topic describes how to monitor the total utilization on a ProtecTIER system.

The **Total utilization** pane displays the following information in both graphical and numerical format:

Table 32. Total utilization information

Field	Definition
Used space	The amount of disk space currently containing physical data.
Nominal data size	The amount of nominal data used for backup and replication.
Deduplication ratio	The ratio of the nominal data size divided by the used space.
Storage saving	The percentage of the data saved derived from the deduplication ratio. Storage savings = (1-1/deduplication ratio) x 100.

Replication information

This topic describes how to monitor the replication information about a ProtecTIER system.

The **Replication information** pane displays the replication properties of the ProtecTIERsystem:

- ProtecTIER Replication Manager information:

Field	Definition
Management address	The external IP address of the ProtecTIER Replication Manager server used by ProtecTIER Manager to connect to the Replication Manager.
Replication address	The replication IP address of the ProtecTIER Replication Manager.

- Grid information:

Field	Definition
Grid name	The name of the grid to which this repository is assigned.
Grid ID	The identification number of the grid to which this repository is assigned.

- The **Switch to:** field enables you to toggle between the ProtecTIER Replication Manager and the system view, or other ProtecTIER systems in the grid. A preview pane displays the replication group to which this system belongs.

Monitoring the ProtecTIER VTL system performance statistics

This topic defines how to use ProtecTIER Manager to monitor the VTL system performance statistics.

From the Systems Management view, select a system from the drop-down list in the navigation pane and click **Statistics**. The Statistics monitoring window displays performance graphs of the repository throughput for both backup and replication.

The **Statistics** monitoring window consists of the following tabs:
- "Repository statistics"
- "Backup statistics" on page 144
- "Replication statistics" on page 146

Repository statistics

This topic describes the utilization statistics of the repository.

The **Repository** tab of the **Statistics** monitoring window displays the following performance graphs:
- "Nominal data size graph"
- "HyperFactor ratio over time graph"
- "Utilization graph" on page 144

Nominal data size graph
The **Nominal data size graph** displays the amounts of nominal data contained in the repository over time.
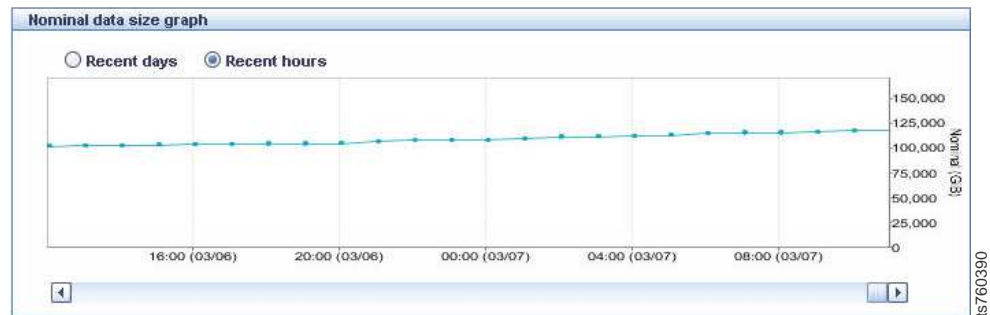
Figure 47. Nominal data size graph

HyperFactor ratio over time graph
The **HyperFactor ratio over time** graph displays the cumulative HyperFactor ratio as it changes over time.
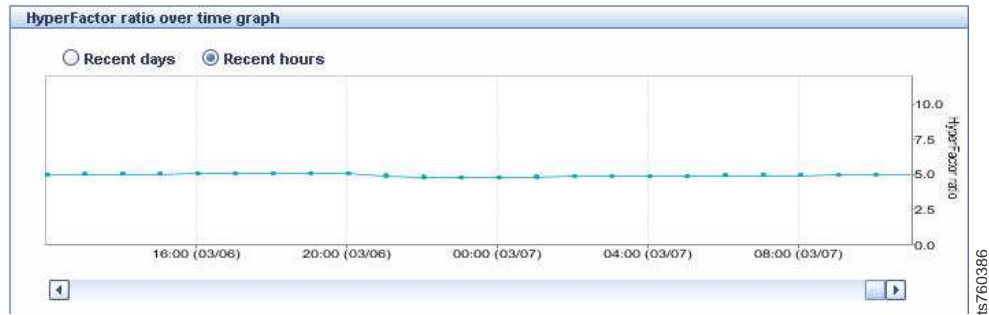
Figure 48. HyperFactor ratio over time graph

Utilization graph

The **Utilization graph** displays the amounts of physical repository space used over time.
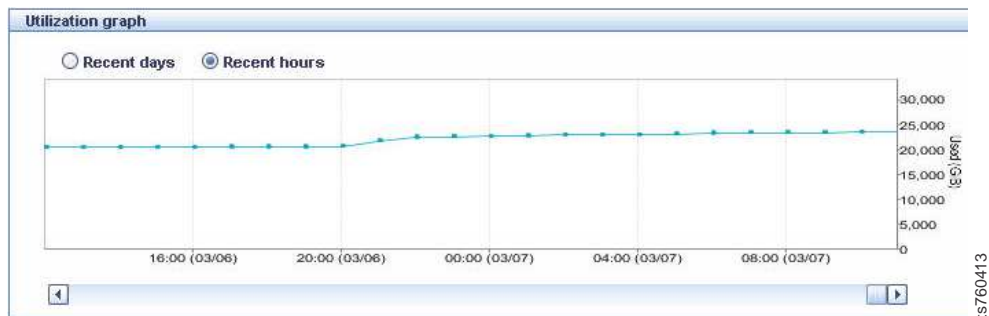
Figure 49. Utilization graph

Backup statistics

This topic describes the system's I/O throughput statistics.

The **Backup** tab of the **Statistics** monitoring window displays the following graphs:

- "Backup read graph"
- "Backup Marginal HyperFactor ratio graph" on page 145
- "Backup write graph" on page 145

Backup read graph

The **Backup read** graph displays the throughput (in MB/Sec) and streams of data read from the repository over time.
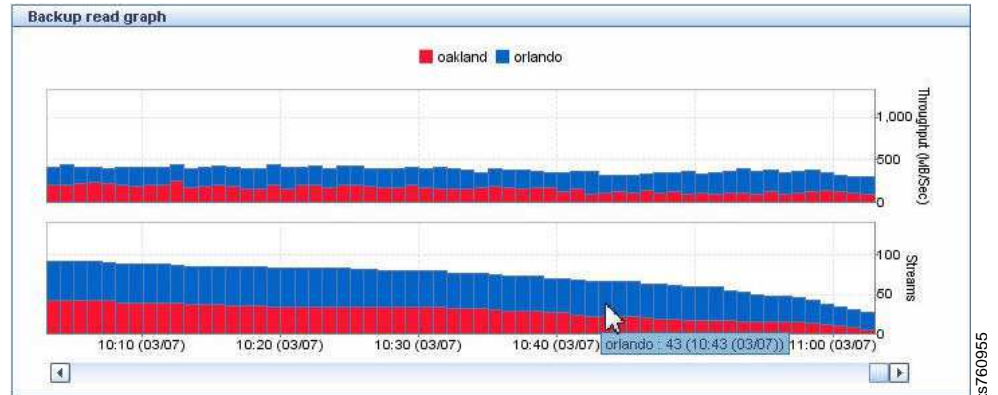
Figure 50. Backup read graph

The view displays the data over a 24-hour period in 1-minute intervals.

Backup Marginal HyperFactor ratio graph

The **Marginal HyperFactor ratio** graph displays the amount of data written to the repository, and the physical space it occupies, at each point in time. Comparing these two values enables you to evaluate the effect of HyperFactor on the data written.
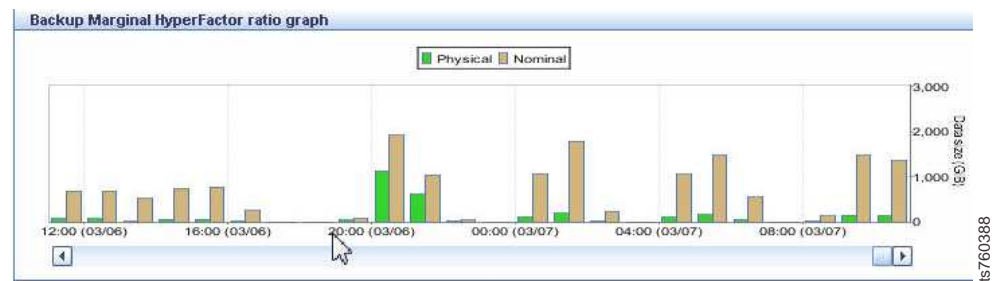
Figure 51. Marginal HyperFactor ratio graph

Backup write graph

The **Backup write** graph displays the throughput (in MB/Sec) and streams of data written to the repository over time.
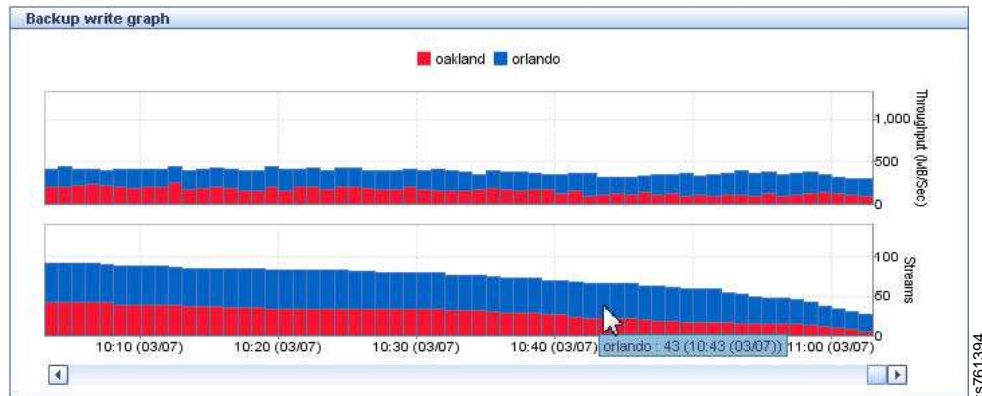
Figure 52. Backup write graph

The view displays the data over a 24-hour period in 1-minute intervals.

Replication statistics

This topic describes the replication throughput statistics of the system.

The **Replication** tab of the **Statistics** monitoring window displays the following performance graphs:

- "Incoming replication graph"
- "Outgoing replication graph"
- "Backlog replication graph" on page 147

Incoming replication graph

The **Incoming replication** graph displays the throughput (in MB/Sec) and streams of data replicated to the local repository from the remote repository, or repositories, over time.
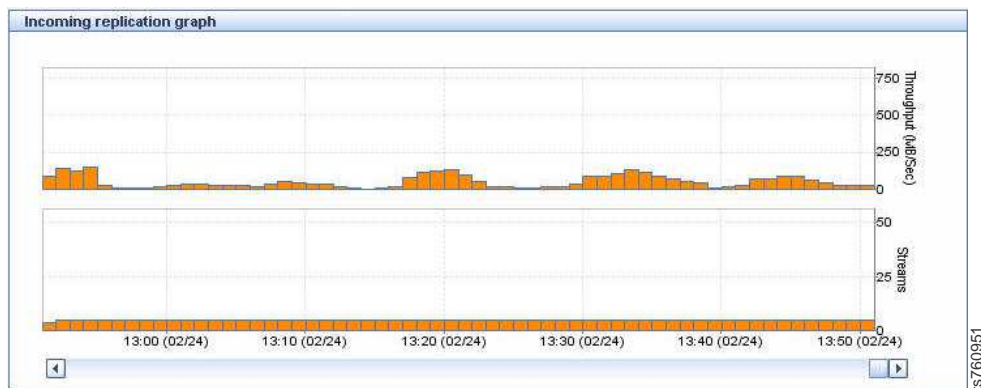
Figure 53. Incoming replication graph

The view displays the data over a 24-hour period in 1-minute intervals.

Outgoing replication graph

The **Outgoing replication** graph displays the throughput (in MB/Sec) and streams of data replicated to the destination repository, or repositories, over time.
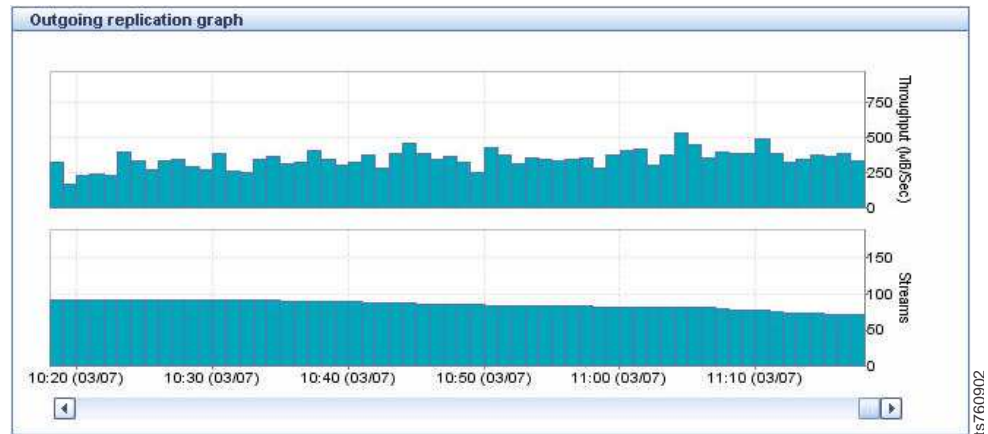
Figure 54. Outgoing replication graph

The view displays the data over a 24-hour period in 1-minute intervals.

Backlog replication graph

The **Backlog replication** graph displays the overall data pending replication over time.

Figure 55. Backlog replication graph

Monitoring activities

This topic describes how to use ProtecTIER Manager to monitor ongoing activities (I/O and replication) of a system.

From the **Systems Management** view, select a system from the dropdown list. Click **Activities** in the navigation pane. During replication, the list of objects undergoing replication activity is displayed. During backup, the drivers will be displayed. Select an object from the list to view additional activity details.
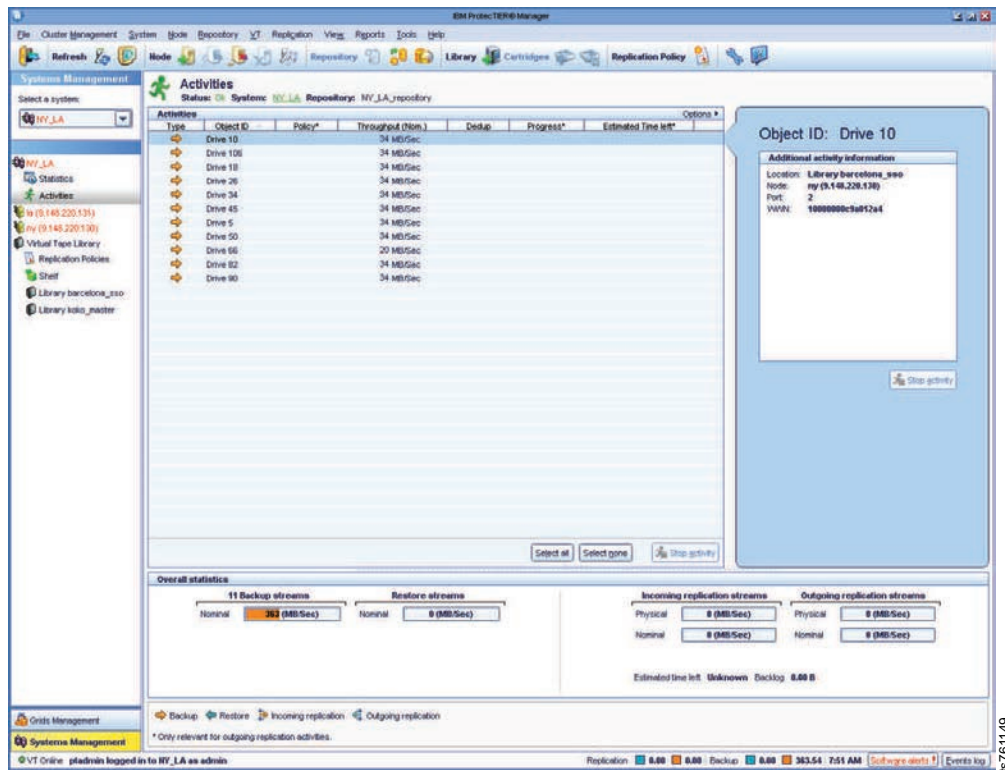
Figure 56. Activities view window

Note: The replication activities view is ad hoc. So, if new data is written to a cartridge while it is being replicated, the progress of the displayed data details appears in the replication view restarted.

Note: During backup activities, read streams may appear in the backup read stream graphs, as well as restore activity in the *Activities* view.
Columns that appear with an asterisk (*) next to the column name display data that is only relevant to outgoing replication activities.

Type   the type of replication activity

Object ID
> the barcode of the cartridge or the driver ID

Policy   the name of the policy that contains the respective cartridge in its
> definition

Throughput
> the nominal throughput of replicating or backup data in MB/sec

Dedup*
> displays the savings in the bandwidth for replicating this cartridge

Progress*
> the progress of replicating the latest changes to their destination

Estimated time left*
> the estimated amount of time remaining for the replication process to
> complete

Overall statistics

The **Overall statistics** pane displays the nominal throughput of backup and restore streams.

The **Replication** tab displays the nominal and physical throughput of incoming and outgoing replication streams. The **Backlog** tab displays the nominal replication backlog data per destination.

Viewing the replication data backlog by source

This topic describes how to monitor the amount of replication data backlog on a source repository for each system in a replication group.

About this task

The **Backlog by source** window displays the backlog of nominal replication data per source repository.

The backlog displayed is updated only when replication is active and at the end of each cartridge replication. When there is no replication activity, the backlog is not updated, even if there are changes on the source repository.

Follow the procedure below to view the backlog per source:

Procedure

1. From the Systems Management view, select **Replication > Replication Disaster Recovery > Show backlog by source**. The **Backlog by source** window displays the backlog of nominal replication data by source repository.
2. Click **Close** to exit the window.

What to do next

Go on to "Monitoring nodes."

Monitoring nodes

These topics describe how to monitor a node with ProtecTIER Manager.

From the navigation pane, select a node. The **Node** monitoring screen displays.
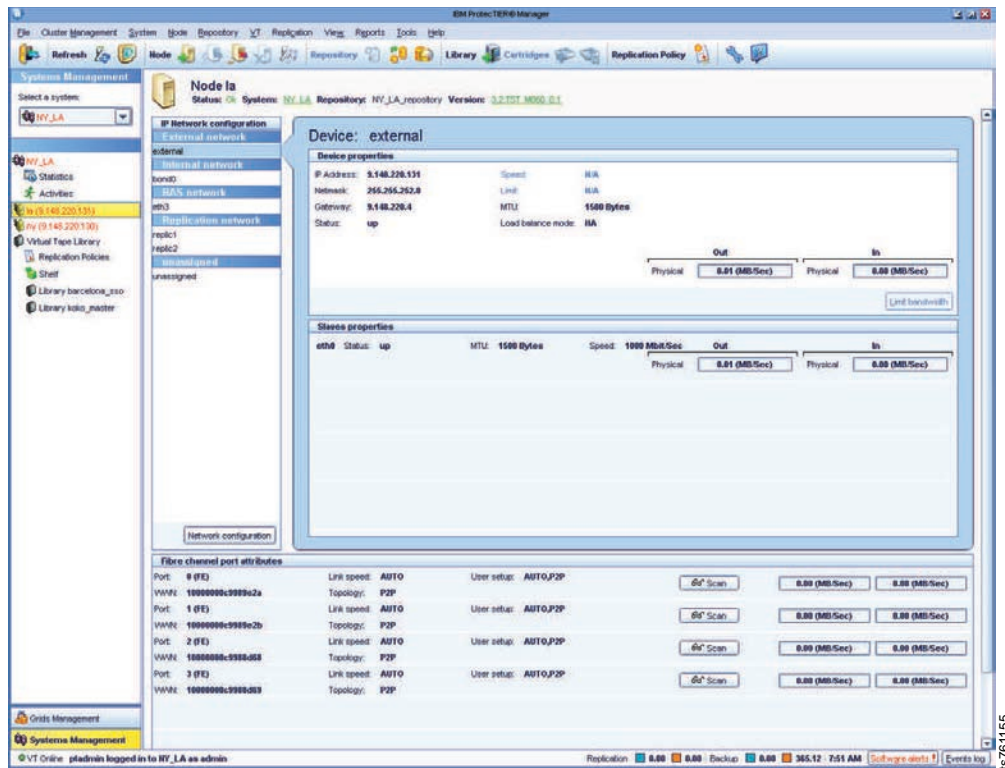
Figure 57. Node selection window

The **Node** monitoring screen consists of the following panes:
- "IP Network configuration of a node" on page 151
- "Fibre Channel port attributes of a node" on page 152

Viewing version information

ProtecTIER Manager displays machine information and code levels for the versions of ProtecTIER and the drivers installed on the node.

To view the version and machine information of a node from ProtecTIER Manager, select a node in the navigation pane of the Systems Management view. A hyperlink of the **Version:** is displayed at the top of the view pane.

Click on the hyperlink and the **Show version information** window displays the version numbers for the following information:

Table 33. Version information

Version information	Description
Release version	Displays the version number of the ProtecTIER release
ProtecTIER model	Displays the ProtecTIER server model type
Linux RPM version	Displays the version number of the Linux package installed on the server
DTC Emulex RPM version	Displays the version number of the ProtecTIER device driver
ProtecTIER Replication Manager version	Displays the version of the ProtecTIER Replication Manager

Table 33. Version information (continued)

Version information	Description
Machine type model	Displays the machine type and the model of the server
Machine serial number	Displays the machine's serial number

IP Network configuration of a node

This topic describes how to monitor the IP Network configuration.

The **IP Network configuration** pane displays information about the network interface card (NIC) setup of the node. Click on the devices to display the device properties. To customize the network configuration of a node, click on the **Network configuration** button at the bottom of the pane. For more information, see "Customizing the network configuration of a node" on page 45.

Table 34. Network interface card information

Column	Definition
Device	The devices in the NIC: **External network** - External is the virtual bond master device to which the external network ports are enslaved. **Note:** Bond devices are defined as part of the installation process. - Eth0 is the customer network port that communicates with the ProtecTIER Manager workstation **Internal network** - bond0 is the virtual bond master device to which the internal network ports are enslaved **Note:** Bond devices are defined as part of the installation process. - Eth1 and Eth4 are the cluster-internal network ports used for VTL **RAS** RAS is the virtual bond master device to which the RAS network ports are enslaved. **Note:** Bond devices are defined as part of the installation process. **Replication network** - replic1/replic2 is the virtual bond master device to which the replication network ports are enslaved. **Note:** Bond devices are defined as part of the installation process. - Eth2 and Eth5 are the replication ports used for VTL

The following table describes the Device properties for the configured node.

Note: Items not relevant to your configuration are grayed out.

Table 35. Device properties

Column	Definition
IP Address	IP address of the device.
Netmask	32-bit mask used to divide an IP address into subnets and specify the network's available hosts.
Gateway	The network point that acts as an entrance to another network.
Status	Indicates whether the device is functioning properly.
Speed	The supported speed of data transfer across the device in Megabits per second.
Limit	The configured value of bandwidth limit in Megabits per second.
MTU	Configured maximum transmission unit for the device.
Load balance mode	The load balancing method used within a bond.
Physical OUT / IN , MB/Sec	The actual usage of network bandwidth of a bond.
Limit bandwidth	Allows you to configure the bandwidth limitation of a bond.

The following table describes the Slave properties for the configured node.

Note: Items not relevant to your configuration are grayed out.

Table 36. Slave properties

Column	Description
Name (for example, ethX)	The interface name enslaved in the selected bond.
Status	Indicates whether the device is functioning properly.
MTU	Configured maximum transmission unit for the device.
Speed	The supported speed of data transfer across the device in Megabits per second.
Physical OUT/IN, MB/Sec	The actual usage of network bandwidth for a device.

Fibre Channel port attributes of a node

The **Fibre channel port attributes** pane displays the following information for each port in the node:

Table 37. Port attribute information

Column	Definition
Port	Port number and port mode. All ports in the ProtecTIER system are front-end ports that connect the node with the backup server(s). This mode is labeled FE.
WWN	Worldwide Name of the port.
Link Speed	Transmission speed of the port.
Topology	Fiber Channel topology of the port. The possible values are as follows: • Point-to-point (P2P) • Fiber channel-arbitrated loop • Down - meaning there is no fiber channel connection
User setup	User-assigned link speed and topology.

In addition, for each port you can click the **Scan** button to open the **Scan Port** dialog box.

The **Scan Port** dialog box displays a numbered list of the Worldwide Names of the remote ports detected by the port. This feature can be used to determine if host adapters are visible to ProtecTIER either for first time setup or for ongoing monitoring

Monitoring Virtual Tape Libraries

This topic defines how to monitor VT (Virtual Tape) libraries using ProtecTIER Manager.

From the Systems Management view, choose a system from the dropdown list. Select **Virtual Tape Library** from the navigation pane to display the statistics, performance, and configuration of the defined virtual tape libraries.
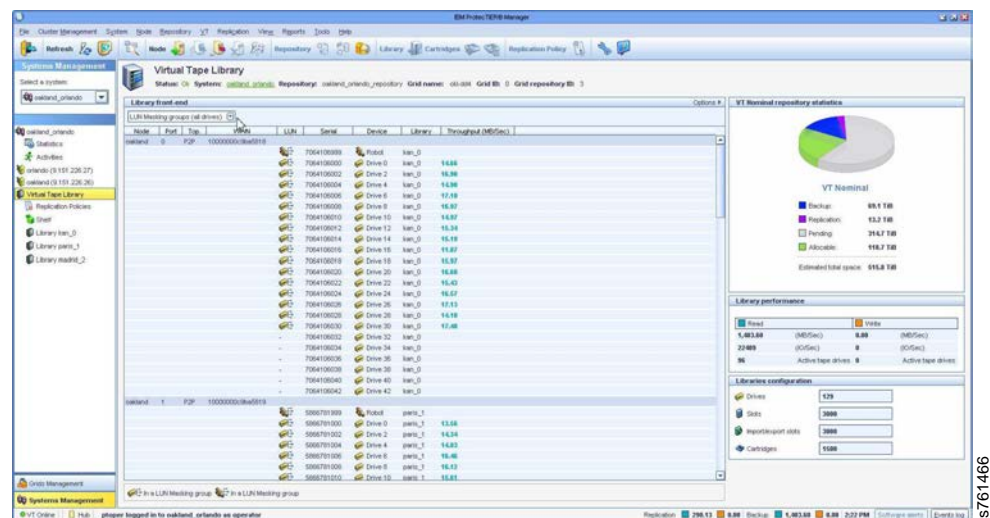
Figure 58. Virtual Tape Library view

If the system is configured for LUN Masking a dropdown is displayed in the Library front-end pane. Selecting **LUN Masking group** changes the view to display a list of configured drives per configured LUN Masking group from all defined libraries on this repository.

The **Virtual Tape Library** window consists of the following panes:

- **Library front-end** - Displays the libraries and devices per port for each node. For more information, see "Library front-end" on page 157.

- **VT Nominal repository statistics**- Displays the current repository breakdown of nominal data.

  - **Backup** refers to the amount of nominal data containing backup data

  - **Replication** refers to the amount of nominal data used for replication

  - **Pending** refers to the amount of nominal data pending deletion and defragmentation activities

  - **Allocable** refers to the amount of free disk space available to hold nominal data

  - **Estimated space** refers to the overall estimated nominal space supported by the system

    Note: The **Estimated space** value is based on the current deduplication ratio.

- **Libraries performance** - Displays the current total performance of the libraries in the system. For more information, see "VT overview" on page 157.

- **Libraries configuration** - Displays the total number of drives, slots, import/export slots, and cartridges for all the libraries in the system. For more information, see "Configuration" on page 158.

Monitoring replication policies

This topic describes how to monitor replication policies of a system using ProtecTIER Manager.

From the Systems Management view, click on **Replication Policies** on the navigation pane to see the replication policies defined on the repository. The following information is displayed for each defined policy:
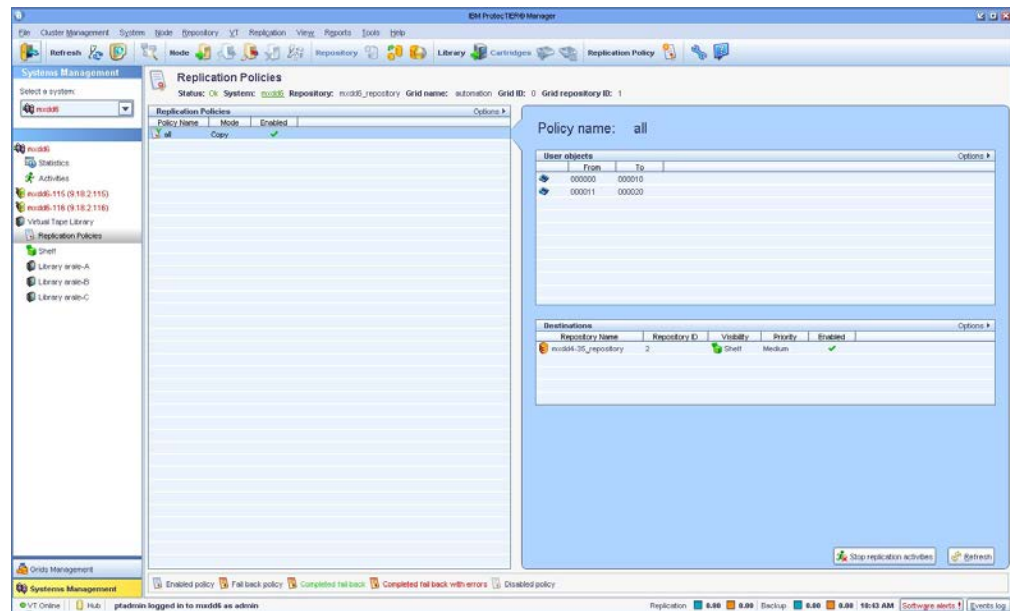
Figure 59. Replication Policies

Policy name
> The name that you defined for the policy.

Mode   Cartridges are either copied or moved. (Note: In this release, "copy" is the only mode of operation.)

Enabled
> Policy can be enabled or disabled for execution, or partially enabled with some of the destinations disabled. A policy can also be enabled or disabled per destination.

Select a policy to see the policy's details, such as: destination repository, range of barcodes, and current activities.

Additionally, in the policy's details view, the priority of the policy is displayed. A policy can be prioritized per destination, meaning that each policy destination can have a different priority.

Policies have 3 options of priority: High, Medium, Low. The policy's Priority is defined according to the importance and/or urgency of the data that needs to be transferred. For example, a policy with a high priority is transferred first, then a policy with medium priority, followed by low priority. The default is Low for every policy.

Go on to "Monitoring the ProtecTIER VT service."

Monitoring the ProtecTIER VT service

The topics in this section describe how to monitor the VT services with ProtecTIER Manager.

From the Systems Management view, click a library. The **Library** monitoring screen displays with the **General** tab selected by default.

The type of monitoring information that is provided for VT services, or library, consists of the following types of information:
- General
- Drives
- Cartridges
- Slots
- Import/Export Slots

Go on to the "Monitoring Virtual Tape service - General tab".

Monitoring Virtual Tape service - General tab

This topic defines the general information provided by ProtecTIER Manager when it is used for monitoring Virtual Tape (VT) services.

The **Library** monitoring screen displays the **General** tab by default. The **General** tab displays information about the selected virtual library.

Figure 60. General tab

If the system is configured for LUN Masking a dropdown is displayed in the Library front-end pane. Selecting **LUN Masking group** changes the view to display a list of configured drives per configured LUN Masking group from all defined libraries on this repository.

Note: The LUN Masking dropdown is only displayed if your system is configured for LUN Masking. In this case, the system was not configured for LUN Masking so the selection is not available.

The **General** tab consists of the following panes:

- "Library front-end"
- "VT overview"
- "Configuration" on page 158

Library front-end

The **Library front-end** pane displays the virtual robots and tape drives assigned to each port of each node in your ProtecTIER system. You can filter the display to show all the devices in the library, or to display the devices per robot or tape drive.

Table 38. Virtual robots and tape drive

Column	Definition
Node	The node on which the virtual device is assigned.
Port	The port within the node on which the virtual device is assigned.
Top.	The Fiber Channel topology of the port. Possible values: • Point-to-point (P2P) • Fiber channel-arbitrated loop (Loop) • Down - meaning there is no fiber channel connection
WWN	The Worldwide Name of the port.
LUN	The logical unit number of the robot or tape drive relative to the port. An icon displays if the device is, or is not, part of a LUN Masking group.
Serial	The drive's serial number of the robot or tape drive.
Device	The type of device (robot or tape drive).
Library	The name of the virtual tape library.
Throughput	The current rate of data transfer across the device.

Note: Change the device assignments for your libraries by clicking **Reassign devices**. (For more information, see "Reassigning devices" on page 95.)

VT overview

The **VT overview** pane displays general information about the performance of the selected library for Read and Write operations.

The following information is displayed:
- Status of each tape drive
- Rate of data transfer in Mbps
- Number of I/O operations per second
- Number of active tape drives

Each tape drive in the library is graphically represented. If the drive is currently writing, an orange icon is displayed on the graphic. If the drive is currently

reading, a blue icon is displayed. To see the drive number, the current read/write rate of the drive in Mbps, hover your cursor over the graphic. Hovering your cursor over the graphic will also display the percentage of time that the tape drive is idle during backup operations. Idleness in the tape drive is due to low backup application data transfer rates.

Configuration

The **Configuration** pane displays the configuration parameters of the selected library.

The following information is displayed:

Table 39. Library configuration information

Field	Definition
VT version	Displays the version number of the ProtecTIER virtual tape library
Compression mode	Displays whether data compression is enabled or disabled. This field can be modified using the dropdown list.
HyperFactor mode	Displays whether data factoring is enabled or disabled. This field can be modified using the dropdown list.
Control path failover mode	Displays whether the control path failover mode is enabled or disabled. This field can be modified using the dropdown list.
Drives	Displays the current number of drives in the selected library. Select **Modify** to open the Change Dimensions wizard.
Slots	Displays the current number of slots in the selected library. Select **Modify** to open the Change Dimensions wizard.
Import/Export slots	Displays the current number of import/export slots in the selected library. Select **Modify** to open the Change Dimensions wizard.
Cartridges	Displays the current number of cartridges in the selected library. Select **Modify** to open the Change Dimensions wizard.
Vendor name	Displays the vendor name of the emulated virtual library type. Select **Modify** to open the Set Library Type wizard.
Product	Displays the product name of the emulated virtual library type. Select **Modify** to open the Set Library Type wizard.

Table 39. Library configuration information (continued)

Field	Definition
Revision	Displays the revision number of the emulated virtual library type.
	Select **Modify** to open the Set Library Type wizard.

The current number of drives, slots, import/export slots, and cartridges in the selected library are displayed.

Note: Change the number of devices per port or node in the library by clicking **Re-assign devices**. The **Change dimensions** wizard is displayed. (For more information, see "Editing library parameters" on page 92)

Go on to the "Monitoring Virtual Tape service - Drives tab".

Monitoring Virtual Tape service - Drives tab

This topic defines the drives information provided by the ProtecTIER Manager when it is used for monitoring Virtual Tape (VT) services.

The **Drives** tab displays detailed information about the virtual tape drives in the selected library.
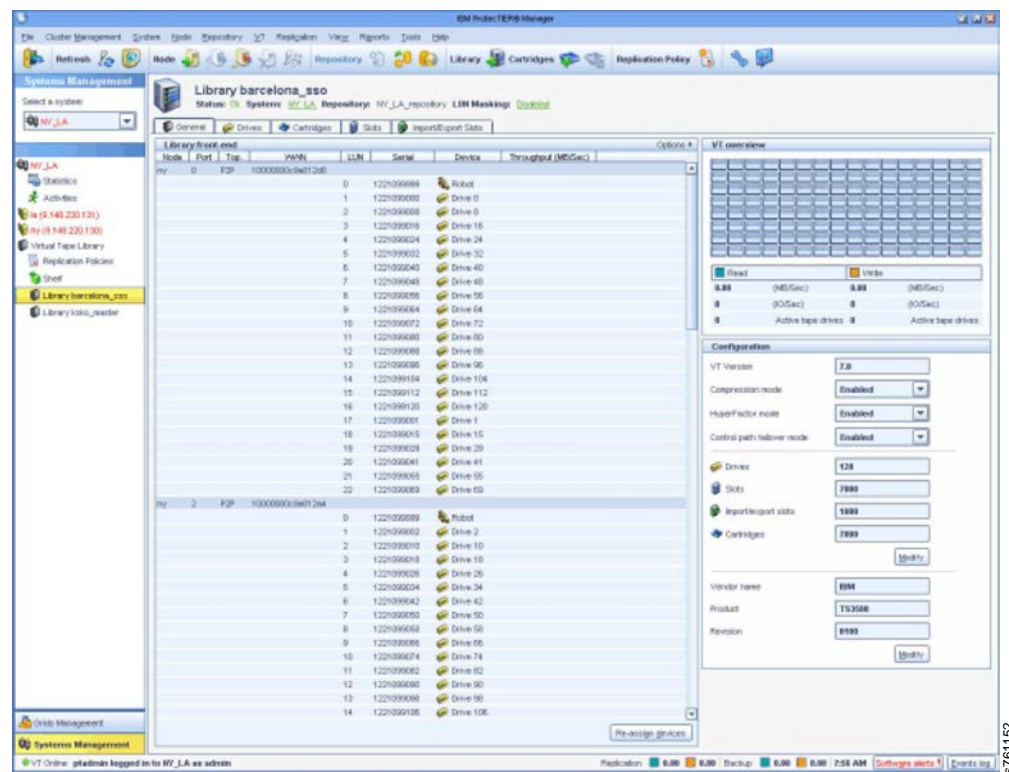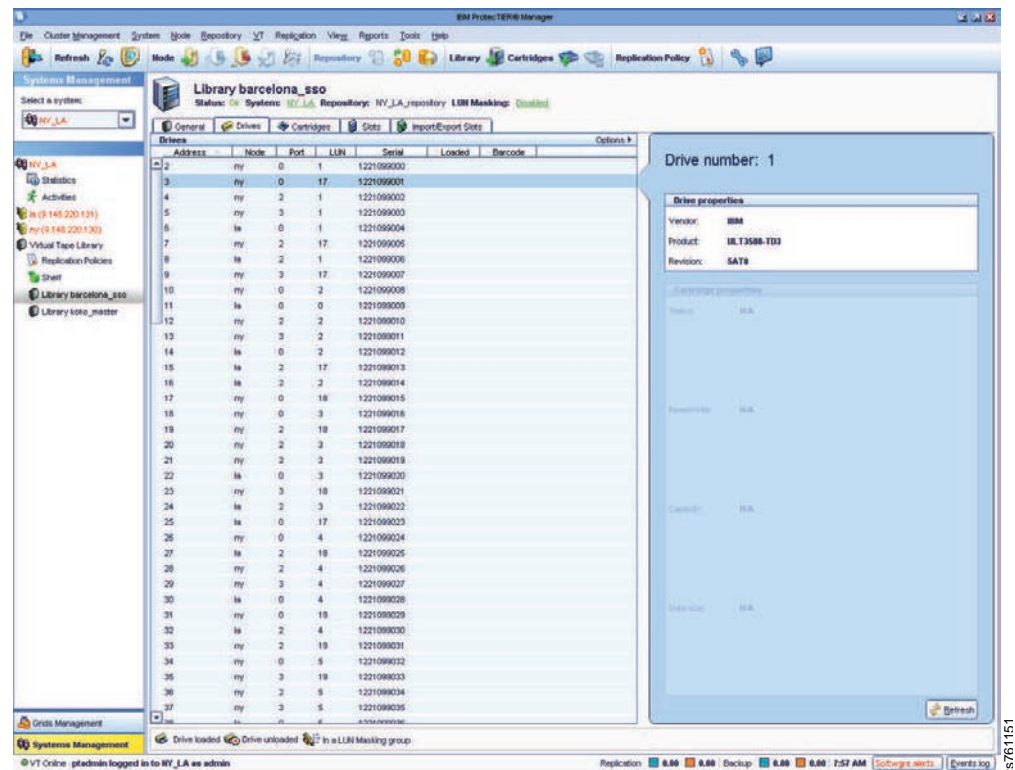

Figure 61. Drives tab

If the system is configured for LUN Masking a dropdown is displayed in the Library front-end pane. Selecting **LUN Masking group** changes the view to display a list of configured drives per configured LUN Masking group from all defined libraries on this repository.

Note: The LUN Masking dropdown is only displayed if your system is configured for LUN Masking. In this case, the system was not configured for LUN Masking so the selection is not available.

The following information is displayed:

Table 40. Drives tab information

Column	Definition
Drive No.	The drive number. This number is displayed to the right of the view pane when a specific virtual tape drive is selected from the **Drives** list.
Vendor	The name of the vendor whose product the virtual drive emulates. This information is displayed to the right of the view pane when a specific virtual tape drive is selected from the **Drives** list.
Product	The product name for the product that the virtual drive emulates. This information is displayed to the right of the view pane when a specific virtual tape drive is selected from the **Drives** list.
Revision	The revision number for the product that the virtual drive emulates. This information is displayed to the right of the view pane when a specific virtual tape drive is selected from the **Drives** list.
Address	The drive's address within the library
Node	The node to which the drive is assigned
Port	The port on the node to which the drive is assigned
LUN	The drive's logical unit number relative to the port
Serial	The drive's serial number
Loaded	Indicates whether the drive is loaded with a virtual cartridge. If the drive is loaded with a virtual cartridge, is displayed.
Barcode	If the drive is loaded with a cartridge, this column displays the cartridge's barcode.

Go on to the "Cartridges tab."

Cartridges tab

This topic defines the cartridges information provided by ProtecTIER Manager when it is used for monitoring Virtual Tape (VT) services.

Go to the Systems Management view of ProtecTIER Manager to see detailed information about the virtual tape cartridges in a selected library:

1. Select a library in the navigation pane.
2. Click the **Cartridges** tab to view detailed information about the virtual tape cartridges in the chosen VT library. The cartridge configuration is displayed:
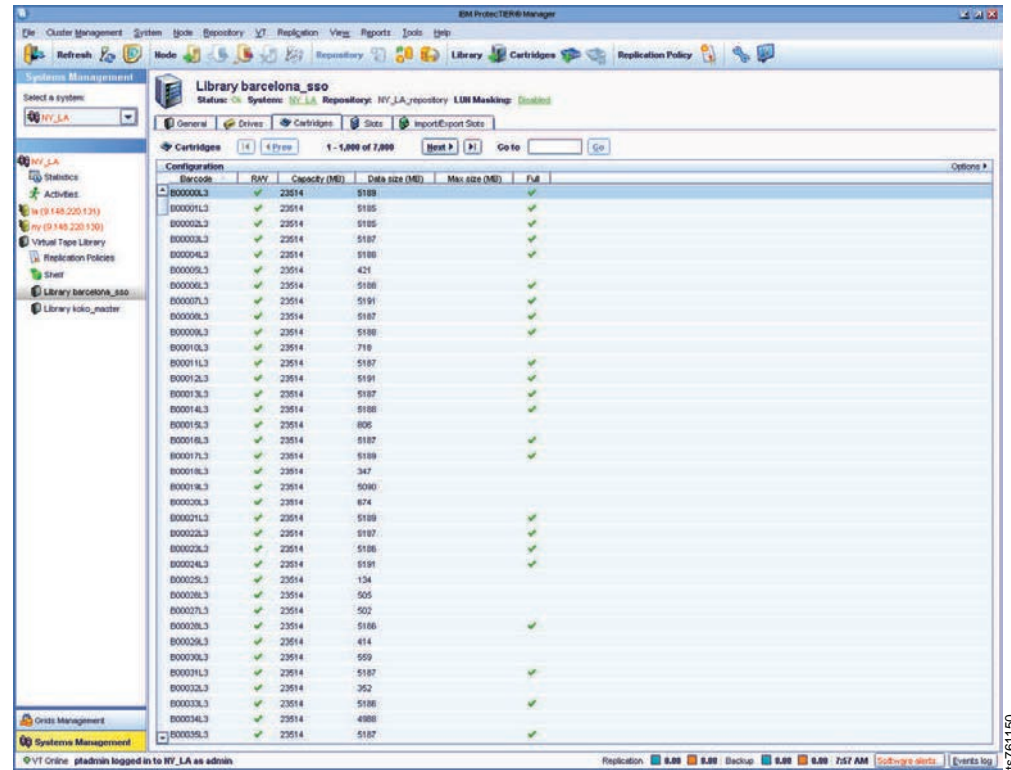
Figure 62. Cartridges tab

If the system is configured for replication, a dropdown list will appear in the **Configuration** pane. You can filter the configuration properties view of the cartridges displayed by selecting one of the following options from the **Configuration** dropdown field:

- "Backup properties"
- "Origin properties" on page 163
- "Replica properties" on page 164

Backup properties

This topic illustrates the backup properties of a cartridge.

The **Backup properties** filter displays the general properties of the cartridge's configuration (not related to replication).
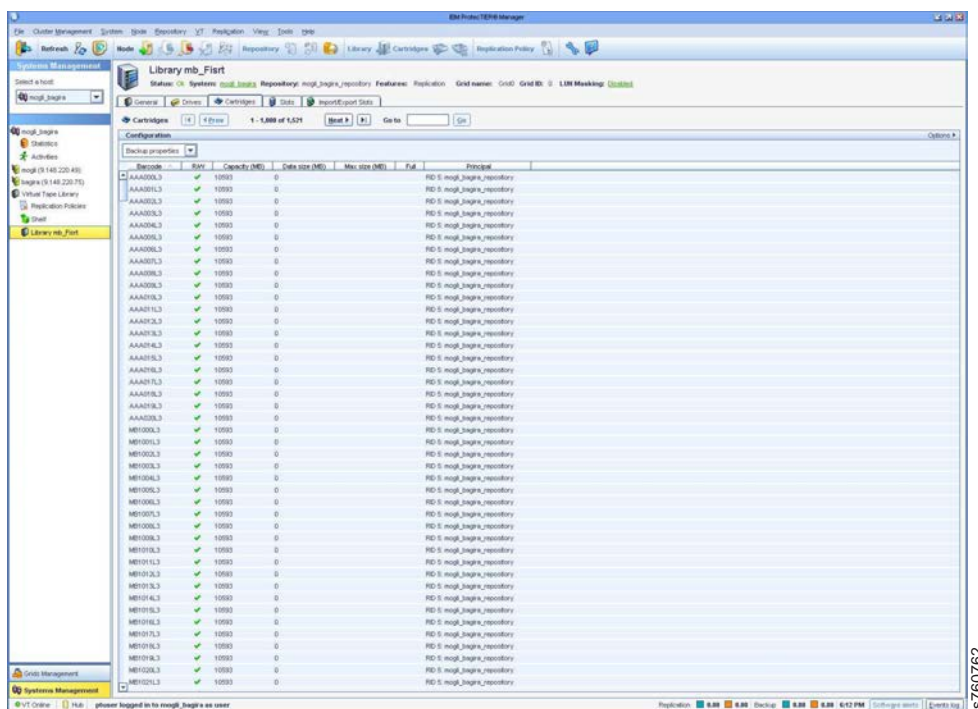
Figure 63. Cartridges tab - backup properties

The following general information is provided for the cartridges of the library you have chosen:

Table 41. Cartridges backup properties

Column	Definition
Barcode	The cartridge's barcode.
R/W	Whether the cartridge is write enabled. If the cartridge is write enabled, a green checkmark is displayed.
Capacity (MB)	The cartridge's estimated data capacity in megabytes. This value varies over time depending on the HyperFactor ratio and the number of cartridges configured in the system.
Data Size (MB)	The amount of nominal data, in megabytes, currently stored on the cartridge.
Max Size (MB)	The maximum amount of nominal data, in megabytes, the cartridge can contain.
Full	Indicates whether the cartridge has reached Early Warning. If so, the cartridge is regarded as full and a green checkmark is displayed.
Principal	The repository on which the cartridge was created and backed up. (For more information on "principality", see "Changing cartridge ownership (Principality)" on page 102)

Go on to "Origin properties" on page 163.

Origin properties

This topic illustrates the origin properties of a cartridge.

The **Origin properties** of a cartridge are typically useful when viewed from a source repository. The origin properties are used to understand the status of replicating the cartridges to the destination repository. Using this view, you can understand if cartridges are still pending replication (e.g. backlog > 0) and to what repository the cartridge was replicated.

Note: The **Origin properties** view from the destination repository is useful for situations when the destination has failed back cartridges. See "The failback policy in DR mode" on page 173.

Figure 64. Cartridges tab - origin properties

The following information about the cartridges' origin is provided for the cartridges of the library you have chosen:

Table 42. Cartridges origin properties

Column	Definition
Barcode	The cartridge's barcode.
Data Size (MB)	The amount of nominal data, in megabytes, currently stored on the cartridge.
Destination	The name of the destination repository to which the cartridges will be replicated.
Replicated data size	The amount of nominal data that has already been replicated.
Backlog	The data on the cartridge that still needs to be replicated.

Table 42. Cartridges origin properties (continued)

Column	Definition
Last sync time	The most updated date and time when the backup data on the cartridge was last synchronized with the destination repository.
% Replicated	The percentage of the cartridge that has been replicated.

Go on to "Replica properties."

Replica properties

This topic illustrates the replica properties of a cartridge.

The **Replica properties** are used to analyze cartridges that were replicated into this repository. The replica properties are typically useful from the destination repository. The most useful property of this view is the **In-Sync** column that displays whether or not the cartridge is synchronized with the most up-to-date data from the source.

Figure 65. Cartridges tab - replica properties

The following information about cartridge replication is displayed for the cartridges of the library you have chosen:

Table 43. Cartridges replica properties

Column	Definition
Barcode	The cartridge's barcode.
Data Size (MB)	The amount of nominal data, in megabytes, currently stored on the cartridge.

Table 43. Cartridges replica properties (continued)

Column	Definition
Source	The name of the source repository from which the cartridges are being replicated.
Last sync local time	The most updated date and time on the destination repository when the backup data on the cartridge was last synchronized with the destination repository.
Last sync remote time	The most updated date and time on the source when the backup data on the cartridge was last synchronized with the destination repository.
In-Sync	Shows whether or not the cartridge has been replicated and is synchronized with the source repository.

Go on to the "Monitoring Virtual Tape service - Slots tab."

Monitoring Virtual Tape service - Slots tab

This topic defines the slots information provided by the ProtecTIER Manager when it is used for monitoring Virtual Tape (VT) services.

The **Slots** tab displays detailed information about the slots in the selected library.

*Figure 66. Slots tab*

The **Slots** tab displays the following information:

Table 44. Slots tab information

Column	Definition
Slot No.	Indicates the slot's number in the library.
Address	Indicates the slot's address number.
Barcode	If the slot contains a cartridge, this column displays the cartridge's barcode.
Capacity	If the slot contains a cartridge, this column displays the estimated cartridge capacity in megabytes.
Data Size	If the slot contains a cartridge, this column displays, in megabytes, the amount of nominal data currently stored on the cartridge.
Principle	If replication is configured, this column displays. Principle is the repository on which the cartridge was created and backed up. (For more information on "principality", see "Changing cartridge ownership (Principality)" on page 102)

Go on to the "Monitoring Virtual Tape service - Import/Export slots tab"

Monitoring Virtual Tape service - Import/Export slots tab

This topic defines the import/export slot information provided by the ProtecTIER Manager when it is used for monitoring Virtual Tape (VT) services.

The**Imports/Exports** tab displays detailed information about the import/export slots in the selected library.
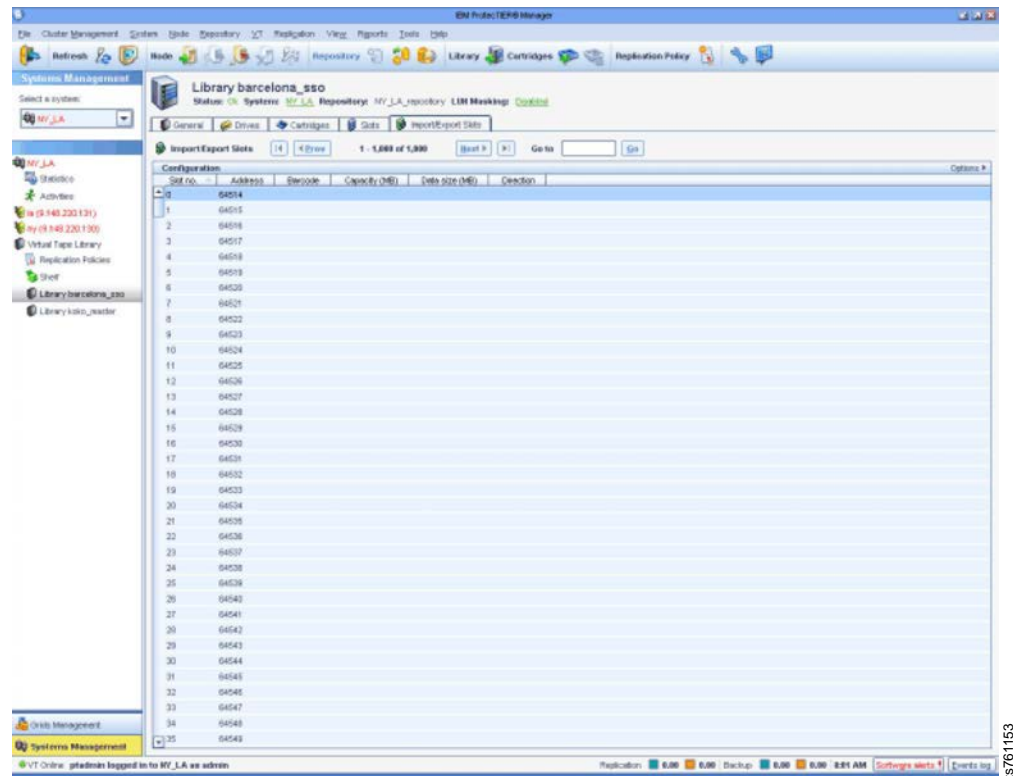
Figure 67. Imports/Exports tab

The **Imports/Exports** tab displays the following information:

Table 45. Imports/Exports tab information

Column	Definition
Imp/Exp No.	The number of the import/export slot.
Address	The import/export slot's address number.
Barcode	If the import/export slot contains a cartridge, this column displays the cartridge's barcode.
Capacity	If the import/export slot contains a cartridge, this column displays the estimated cartridge's data capacity in megabytes.
Data Size	If the import/export slot contains a cartridge, this column displays, in megabytes, the amount of nominal data currently stored on the cartridge.
Principle	If replication is configured, this column displays. Principle is the repository on which the cartridge was created and backed up. (For more information on "principality", see "Changing cartridge ownership (Principality)" on page 102)

Go on to "Monitoring the shelf" on page 168.

Monitoring the shelf

This topic details monitoring the shelf.

The shelf is a container for cartridges that do not belong to any library. Each repository contains only one shelf and whenever a cartridge in a library is moved to the library's export slot, it is automatically displaced to the shelf.

The cartridges in the shelf cannot be seen by backup applications and this facilitates the concept of being out of the library. ProtecTIER Manager displays a view of the shelf and allows access to the cartridges in the shelf.

From the shelf, cartridges can be moved to a library's import slot, replicated to another repository, or be deleted. Cartridges can also be automatically moved to a library's import slot through the visibility switching process. A cartridge that is moved to an export slot is automatically displaced to the shelf.

The monitoring view of the shelf is similar to the monitoring views of cartridges in a library. For more information, see "Cartridges tab" on page 160.

Chapter 12. Disaster recovery (DR) mode operations

The topics in this section includes tips, guidelines, and tasks for disaster recovery (DR).

In Disaster Recovery (DR) mode, the disaster recovery site (destination) temporarily replaces the production site when a "disaster" occurs or the production site goes offline. The disaster recovery site acts as the production site until the primary site comes back online or a new one is created.

If you cannot use the primary repository (if it is down or has been destroyed) and you want to use the remote repository as your backup target, enter DR mode on the remote repository before you start working with it as the primary site. See "Entering Disaster Recovery (DR) mode." Once you enter DR mode, all incoming replication activities from the production site to the DR site are blocked. When the primary site is rebuilt or replaced, you can return the data to the primary site and continue backups and replication. Replicated or newly created tapes can then be moved back to the main production site.

Working at the DR site

Complete these tasks when working with the disaster recovery site after a disaster has occurred or when testing disaster recovery.

Begin working at the DR site by entering the DR mode. Cartridges that were created at the production site are in "read only" mode at the DR site. To work with the DR site as the new backup target, the backup application must have read/write (R/W) permission on cartridges originating from the production site so that the cartridges can be used for backup.

Cartridges at the DR site can be restored for recovery at any time. If you want to work with the DR site as the new backup target, instead of the primary site, you can either:

- Create new cartridges at the DR site and work with them
- Run the cartridge ownership takeover procedure to take control of the cartridges belonging to a down repository in order to have R/W permission at the DR site (see "Changing cartridge ownership (Principality)" on page 102.)

Entering Disaster Recovery (DR) mode

Complete this task to enter disaster recovery (DR) mode and failover to the DR site.

Before you begin

Note: You can enter DR mode only on a repository that is defined as the destination repository in the grid. See Chapter 10, "Native Replication Management," on page 115.

About this task

Entering DR mode on the DR site destination repository "declares" that the primary, or source site is now down. Furthermore, all incoming replication

activities to the DR site are blocked from the selected source. To enter DR mode on the destination repository:

Procedure

1. From the Systems Management view, click on the destination repository.
2. Select **Replication > Replication Disaster Recovery > Enter DR mode**.
3. Choose the repository from which you want to block incoming replication activities, if required.
4. Type yes to confirm that you want to enter DR mode. An automatic procedure is executed that blocks incoming replication to the DR site from the source selected.

   Note: If replication is not blocked, the safety of the data at the DR site cannot be guaranteed.
5. Repeat steps 2 through 4 to block incoming replication on additional repositories.

What to do next

Once you have entered DR mode, go to "Assessing cartridge status and syncing with the catalog."

Assessing cartridge status and syncing with the catalog

The following section explains the process for assessing cartridge status on the DR site and synchronizing the backup application catalog with the cartridges.

Before running a restore for disaster recovery, you must verify that the list of associated cartridges are marked as "In-Sync" with the primary site, otherwise an earlier full backup image must be used for recovery. The easiest way to determine the time of the last full backup is if you have a specific time each day where your replication backlog is zero (i.e. there is no pending data to replicate and backups are not running). If this is not the case, you can assess the cartridges by recovering the backup application catalog and scanning it to find the last full backup where its associated cartridges completed replication.

Recovering the backup application catalog

There are several ways to obtain a copy of the catalog at the remote site:
- From a catalog backup on a virtual cartridge that will be replicated to the remote site
- From disk-based replication, or by other means

If the catalog is backed up to a virtual cartridge, check on the DR site that this cartridge appears as In-Sync with the primary site. If the cartridge is not In-Sync, you will need to compare the cartridge's last sync time with the time of the last full backup.

To recover the backup application catalog from a backup on a virtual cartridge, you must work with the replicated cartridges on the hub to get an updated copy of the catalog back to the remote site. From the Systems Management window, select the **Replica properties** view on the **Cartridges** tab and use the following guidelines for each cartridge before running the procedure for recovering the catalog:

Note: The procedure for recovering the selected catalog backup depends on the backup application and is documented in the backup application official documentation.

- If the cartridge has been replicated, either a red `X` or a green checkmark will appear in the **In-Sync** column. If the In-Sync property has a green checkmark, then nothing further needs to be verified and this cartridge is valid for recovery.
- If the cartridge is not marked In-Sync, refer to the **Last sync time** column. This column displays the last time each cartridge's data was fully replicated to the DR site. The cartridge marked with the most recent **Last sync time** date should be used to recover the backup application catalog.

Note: The sync time is updated during replication, and not only when replication for this cartridge is finished.

Recovering the data

Once recovered, scan the backup application catalog and search for the full backup image you want to recover:

- Get the start and end backup time of the full backup image.
- View the list of cartridges associated with this full backup.

Use the Cartridge Query Tool (see "Using the cartridge query tool (for VTL)" on page 189), or the PTCLI inventory filter command to filter the cartridges according to the following properties (see Table 20 on page 73 for more information on running the command):

- In-Sync
- Last update time
- Last sync time

All the cartridges marked as *In-Sync* are valid for recovery. For those cartridges not marked as In-Sync, compare between the **last update time**, which represents the last time the replica was updated, and the **last sync point destination time**.

If the **last update time** is less than or equal to the **last sync point destination time**, the replica cartridge has consistent point in time. Otherwise, the cartridge is incomplete, or in-transit. If the cartridge has consistent point in time, ensure this time stamp is larger than the full backup image end time. This will indicate that the cartridge contains all the required data for this recovery operation. Otherwise, you will have to use a previous full backup image for recovery.

barcode	nominal_size_in_bytes	last_access_time	principality	principality	container	last_update_time	source_rep	source_gri	source_time_for_last_sync_point	destination_time_for_last_sync_point	in_sync
T00000	10212314112	4/22/2010 11:10	0	3	shelf	4/22/2010 11:10	3	0	4/22/2010 9:11	4/22/2010 11:10	1
T00001	9901607936	4/22/2010 11:10	0	3	shelf	4/22/2010 11:10	3	0	4/22/2010 9:11	4/22/2010 11:10	1
T00002	9795963904	4/22/2010 11:10	0	3	shelf	4/22/2010 11:10	3	0	4/22/2010 9:11	4/22/2010 11:10	1
T00003	9259322368	4/22/2010 11:07	0	3	shelf	4/22/2010 11:07	3	0	4/22/2010 9:09	4/22/2010 11:07	1
T00004	12468096000	4/22/2010 11:10	0	3	shelf	4/22/2010 11:10	3	0	4/22/2010 9:12	4/22/2010 11:10	1
T00005	9858485248	4/22/2010 11:10	0	3	shelf	4/22/2010 11:10	3	0	4/22/2010 9:11	4/22/2010 11:10	1
T00006	10139569152	4/22/2010 11:10	0	3	shelf	4/22/2010 11:10	3	0	4/22/2010 9:12	4/22/2010 11:10	1
T00007	10215296000	4/22/2010 11:10	0	3	shelf	4/22/2010 11:10	3	0	4/22/2010 9:12	4/22/2010 11:10	1
T00008	10078620672	4/22/2010 11:10	0	3	shelf	4/22/2010 11:10	3	0	4/22/2010 9:11	4/22/2010 11:10	1
T00009	9994472448	4/22/2010 11:10	0	3	shelf	4/22/2010 11:10	3	0	4/22/2010 9:11	4/22/2010 11:10	1
T00010	2048	4/22/2010 12:03	0	3	shelf	4/22/2010 12:03	3	0	4/22/2010 10:06	4/22/2010 12:05	1
T00011	2048	4/22/2010 12:03	0	3	shelf	4/22/2010 12:03	3	0	4/22/2010 10:05	4/22/2010 12:04	1
T00012	2048	4/22/2010 12:03	0	3	shelf	4/22/2010 12:03	3	0	4/22/2010 10:06	4/22/2010 12:04	1
T00013	2048	4/22/2010 12:03	0	3	shelf	4/22/2010 12:03	3	0	4/22/2010 10:07	4/22/2010 12:06	1
T00014	2048	4/22/2010 12:03	0	3	shelf	4/22/2010 12:03	3	0	4/22/2010 10:06	4/22/2010 12:05	1

Figure 68. Cartridge status report (in Excel)

You may have a case where the cartridge sync point is after the backup start time, but before the end of the backup. This may happen in cases where replication is

working in parallel to the backup. If the backup has many cartridges, the first cartridges may finish replicating before the backup ends and they get a sync point earlier than the backup end time.

As such, if the **last sync time** flag on one (or more) of the cartridges indicates a time later than the **backup start time**, but earlier than the **backup complete time**, those cartridges need further inspection. Scan the backup application catalog for each of those cartridges and get the **backup start time** and the **backup complete time**. If the **last sync time** flag on all the cartridges indicates a time later than the **backup complete time**, your backup image was fully replicated.

Remember: When processing the cartridge list to find a complete set of DR tapes, you must keep track of the date/time discrepancies. Compare the date/time values of the source master backup server and the source ProtecTIER system. The destination environment may be in a different time zone or may be set to the incorrect date/time and as such, is unreliable. Thus, use the source date/time, rather than the destination sync time when comparing cartridge states to the backup catalog/database. The destination sync time should only be used to determine which cartridges are whole.

In addition, there could be a time difference between the source backup server and the source ProtecTIER server. Your Administrator should be aware of the discrepancy, measure it regularly and communicate the delta to the DR Administrator or operator(s). For instance, if the backup server is 2 hours behind, a cartridge may have a sync time that precedes its backup complete time, i.e. it will appear as a previous, old backup.

If there is uncertainty regarding the time differences, compare the nominal size of the cartridge to the Catalog/DB value as an additional (not a substitute) layer of verification.

Go on to "Re-establishing the production site in DR mode."

Re-establishing the production site in DR mode

Complete these tasks to re-establish and update the production site.

In order for the production site to come back online, or for a new site to be established to replace the original production site, these actions are required to reestablish and update the site with the most recent and up-to-date data.

Follow these procedures for re-establishing and updating the production site:
- Replacing the destroyed repository with a new one
- Creating a failback policy when DR mode is set

Replacing a destroyed VTL repository

Complete this task to initiate a VTL repository takeover that will replace the destroyed repository at the production site with a new repository.

Before you begin

Note: Be careful when replacing a repository that you do not accidentally replace a good repository.

If the repository at the production site (source) has been destroyed and cannot be repaired, you can replace it with a new, or existing, repository that isn't part of another replication group. The replacing repository must be part of the replication grid.

About this task

Follow the steps below in the order in which they appear:

Procedure

1. Enter DR mode as described in "Entering Disaster Recovery (DR) mode" on page 169
2. From the Grids Management view, select **Grid > VTL Repository takeover** to run the **VTL Repository takeover** wizard.
3. Select the **Unrecoverable repository** from the dropdown list.
4. From the **Replacing repository** dropdown list, select the repository with which you want to replace the unrecoverable repository (the repository should appear in the dropdown list).

   Note: This operation is not reversible.
5. Click **Ok** to begin.

Results

When you run the **Repository takeover** wizard, the ProtecTIER Replication Manager will internally do the following actions:

- Remove the unrecoverable repository from its group and its grid.
- Rebuild the group with the replacing repository at the new primary site.

If the replacing repository is a new repository, then no cartridge ownership is changed. Otherwise, the "principality" is changed to the replacing repository.

Note: If cartridges remain on other repositories within the group with the principality of the destroyed repository, the **Repository takeover** wizard must be run on the additional repositories.

What to do next

Go on to "The failback policy in DR mode" section for more information on failback policies and how to create them.

The failback policy in DR mode

This topic explains the failback policy and how to create one.

Failback is the procedure for replicating back new or old updated cartridges from a DR site to their original restored production site (in order to bring it up-to-date in case it was down), or to a new production site.

If the primary repository was down and has been restored, you can return to working with the primary site as the production site and use the DR site as the secondary site. In order to replicate back new or old updated cartridges from the DR site, create a failback policy.

Note: The cartridges that originally came from the primary site do not need to be replicated because they were not changed at the DR site, unless they were deleted or destroyed at the primary site.

Note: The failback policy, in addition to copying the cartridges, also takes care of transferring the principality, or ownership, of all the cartridges from the temporary primary repository at the DR site to the restored primary repository at the production site.

Go on to "Creating a failback policy."

Creating a failback policy

Complete this task to create a failback policy.

Before you begin

Important: Only cartridges on the shelf are valid for failback.

Procedure

1. Select **Replication > Replication Disaster recovery > Fail back**. The Fail back wizard welcome screen is displayed.
2. Click **Next**. The **Properties** screen is displayed. Type a unique name for the failback policy in the **Policy name** field.
3. Select a spoke repository on which to create the failback policy.
4. Click **Next**. The **Barcode ranges** screen is displayed.
5. Enter the barcode range of the cartridges that you want to fail back to the old or replaced primary repository.
6. Click **Add** to validate and submit the defined barcode range. If the barcode range is invalid, an error message is displayed.
7. Click **Next**. The **Validation Results** window displays the validation results of the cartridges in range, the cartridges valid for failback, and those that are invalid for failback.

What to do next

Click the **Save report as...** button if you want to save the validation summary report. Click **Next** to view the validation summary report and exit the Failback wizard.

Go on to "Completing failback and leaving DR mode."

Completing failback and leaving DR mode

Complete this task to create the failback policy and leave disaster recovery (DR) mode.

Before you begin

Once the primary site is rebuilt or replaced, create the failback policy and wait for it to complete. When the data is returned to the primary site, you can exit DR mode and continue with backups and replication as usual.

The failback policy is a one-time policy. When failback is complete, the policy still remains in the **Replication policies** list. Running and/or modifying this policy is not allowed, and on trying to do so, an error message is displayed. For example, if

you select the **Modify failback policy** option, the following messages appears. You need to delete the old failback policy from the list and create a new one. You
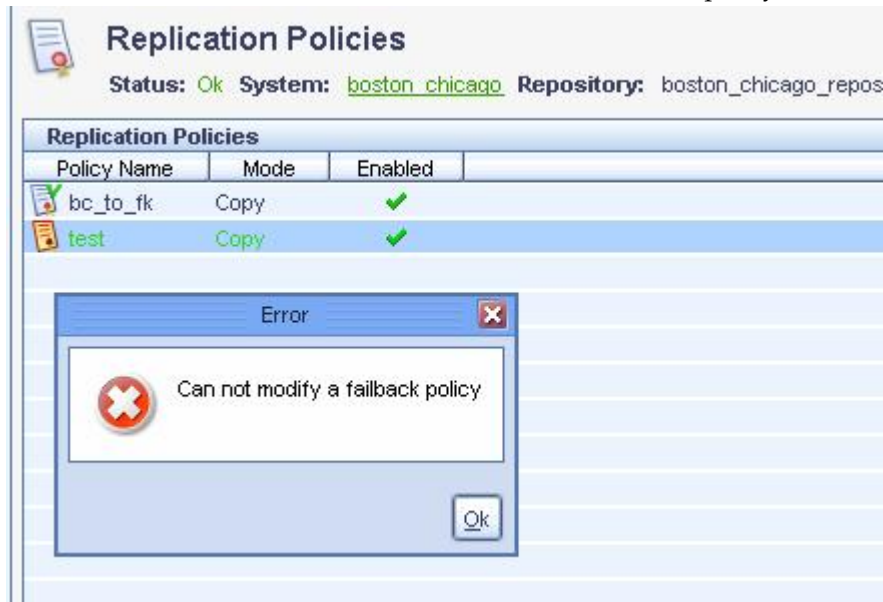
cannot run a failback policy more than once so selecting **Run the replication policy** option results in a the following message
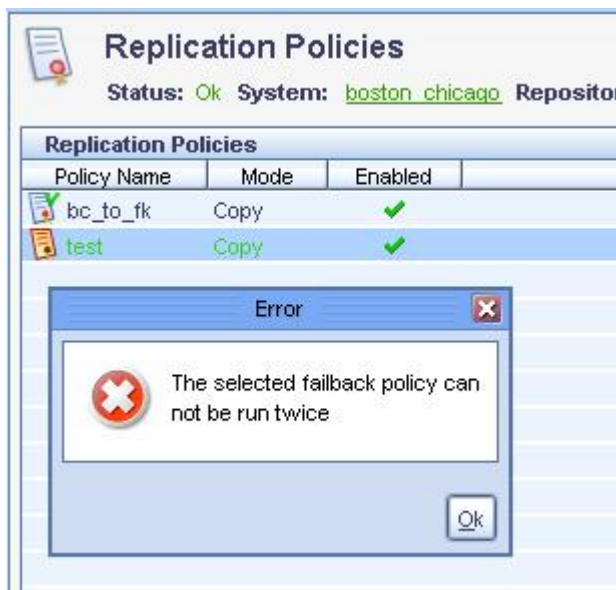
The **Stop replication policy** is enabled but is not functional because you can't stop and resume the failback policy. Once the failback policy is started it can only end or be deleted.

Note: Do not run any backup activities on the restored repository until the failback operation is complete.

About this task

When the failback operation is complete, follow the steps below to exit DR mode:

Procedure

1. Select **Replication > Replication Disaster Recovery > Leave DR mode**. The **Leave DR mode** window is displayed.

2. From the dropdown menu, select the repository from which you want to exit DR mode.

3. Type Yes to confirm that you want to exit DR mode. An automatic procedure is executed that removes blocks on incoming replication to the DR site only from the selected source repository.

4. Click **Ok**. Once the repository is out of DR mode, any replication policy defined on the spoke repository can modify the cartridge data.

What to do next

You can now begin working again with the restored repository.

Part 3. Performance optimization, reporting and troubleshooting

This part contains information about performance optimization, creating and generating reports, and troubleshooting procedures using ProtecTIER Manager.

Chapter 13. Optimization

The topics in this section describe how to optimize the performance of the ProtecTIER system using ProtecTIER Manager.

Changing the CRC setting

This topic explains how to change the CRC calculation algorithm for optimized backup and replication activities on a DD4 server, or higher.

The Change CRC calculation window allows you to change the CRC calculation algorithm to a different algorithm that consumes less CPU resources and can help improve the performance of backup, restore, and replication activities.

CRC is also used in replication communication, regardless of the kind of CRC used for backups, or replication.

Note: It is recommended that all repositories within a replication group have ProtecTIER version 3.1.8, or higher. If the version level of a member in the replication group does not support the fast 32-bit CRC calculation, replication will fail.

Typically, changing the CRC calculation is a onetime event. Once the calculation is changed from the default value, you are not expected to change the calculation back to the default setting. When new data is written to the repository, the latest CRC algorithm selected is used.

"Old" data remains with the CRC calculation that was selected at the time of backup. Even if the "old" data is replicated, the CRC calculation that was selected at the time of backup remains the same and is transferred togetherwith the replicated data.

Note: Changing the CRC calculation does not affect deduplication in any way.

You can change the CRC calculation algorithm from the **Systems Management** view in ProtecTIER Manager. To access the **CRC calculation** window, select **System** > **Optimization** > **CRC calculation**.

Select a CRC calculation option from the dropdown list:
- Software 64-bit CRC
- Hardware/Software fast 32-bit CRC

Click **Ok** to save and exit the window.

Chapter 14. Reporting

The topics in this section describe how to create and generate various reports from the ProtecTIER system using ProtecTIER Manager.

Simple Network Management Protocol (SNMP), when it is configured on a ProtecTIER system, can be used to send a problem notification in the event of hardware or software degradation or failure to designated recipients.

Use the Cartridge Query tool to filter cartridges in a repository for use in generating service and statistics reports, or to select a range of cartridges for various ProtecTIER tasks.

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, and OpenStorage Systems*, v3.3, GA32-0914 for instructions on SNMP configuration. For 3958 DD4 servers, see the *IBM ProtecTIER User's Guide for Enterprise Edition and Appliance Edition*, V3.3.6.1, 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 69 on page 184. 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.

```
Detailed Trap Contents
    Trap ID : 3
    Received time : 7/9/2010 9:15:38 AM.732983
    PDU Type : NOTIFY
    Version : SNMP v2c
    Agent Address : 9.11.219.152
    Source Address : 9.11.219.152 (maybe a proxy)
    Manager Address : 9.11.178.139
    Trap OID : .1.3.6.1.4.1.2.6.224.1.3.1
    SysUpTime : 359494 ( 00h:59m:54s.94 )
    Community : public
    Variable bindings : Count 13
        sysUpTime.0 = 359494
        snmpTrapOID.0 = tsRasNewProblemOpened
        tsRasHostName = rassmb1
        tsRasHostIP = 9.11.219.152
        tsRasProductSerialNumber =
        tsRasProblemSeverity = FAILED
        tsRasCustomerNumber = 2,USA
        tsRasProblemId = 1278690619611
        tsRasCompanyName = A
        tsRasProblemSrn = 0xAA030001
        tsRasProblemDescription = Adapter link is down. Verify cabling
        tsRasProblemType = Hardware
        tsRasProductMTM = 3959SM1
Trap Profile
    No profile defined : Using default
```

Figure 69. SNMP trap report

Using the ProtecTIER Manager Configuration menu

About this task

This task describes how to use the **ProtecTIER Manager Configuration** menu to enable and define the parameters for SNMP reporting.

Typically, hardware faults are reported in ProtecTIER Manager. However, certain conditions will prevent the GUI from communicating with the server, and prevent the reporting of fault information for the failed component. By enabling SNMP reporting, you will have greater assurance that hardware faults do not go undetected.

Accessing the Configuration menu
Procedure
1. If it is not already running, launch ProtecTIER Manager and log in to your system.
2. In the **ProtecTIER Manager** window, select the **Systems Management** view.
3. Open the **ProtecTIER Manager Configuration** menu. From the menu bar at the top of the **ProtecTIER Manager** window, click: **System** > **Configuration**.

   The **Configuration** menu is displayed with the **SNMP Traps** option selected and the **Communities** window open.

   Note: You can complete the menu options in any order. However, for best results and proper operation of all functions, it is recommended that you start by configuring SNMP traps in "Configure SNMP Traps" on page 186, and then complete the remaining tasks in the order in which they are documented.
4. Go on to "Configure SNMP Traps" on page 186.

Entering registration details
Procedure
1. In the **Registration** window (shown in Figure 70), enter the requested **Company** and **System Administration** information:

Figure 70. Registration

ⓘ Until you have completed all of the fields in the **Registration** window, the pop-up reminder displays each time you log in to ProtecTIER Manager. To dismiss the reminder, click **Ignore**.

2. When you have finished entering registration information, go on to "Configure SNMP Traps" on page 186.

Configure SNMP Traps

Procedure

1. From the **Configuration** menu, select the **SNMP Traps** option.

   The **SNMP Traps** window opens.

   Note: In order to receive and display SNMP trap reports, you must have SNMP trap receiver software installed on the SNMP trap server. For instructions about the installation, configuration, and use of your SNMP trap receiver software, refer to the documentation that came with the product.

   In addition, to enable the trap receiver to translate and display the SNMP trap data, you must specify the filename and location of the management information base (MIB) files for the SNMP trap receiver. On the TS7600 servers, the MIB filename 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`.

2. In the **Communities** pane, click **Add**.

   The **Add SNMP Trap Destination** dialog box is displayed.

3. In the **Host address** field, enter the SNMP IP address of the host server.

   This is the IP address of the destination server that collects the SNMP traps.

4. In the **Community** field, select one of the default community names (**public** or **private**), from the dropdown list, or type in a custom community name.

   The community name defines a device (or group of devices) that sends traps to the SNMP trap receiver. The receiver accepts traps from the default public and private communities, and any custom communities that were manually added to the communities list in the trap receiver program. Traps from unrecognized community names are ignored.

5. If the default **Port** value does not match the port value used by the SNMP trap receiver for the corresponding community, enter the correct value.

6. Click **Add**.

   You are returned to the **SNMP Trap** window. The new SNMP trap destination displays in the **Communities** list, and a test SNMP trap is automatically sent to the destination.

7. Repeat steps 2 through 6 to add additional SNMP trap destinations, if needed, and click **Submit**.

8. Proceed as appropriate:

   - If you selected public or private in step 4, go on to step 9.
   - If you entered a custom community name in step 4:
     a. Add the custom community name(s) to the communities list on the trap receiver. Refer to the documentation that came with the product for instructions.
     b. Enter the port value(s) that correspond to the ones specified in step 5.
     c. Go on to step 9.

9. *(Optional, but recommended for any communities that were added with a custom name.)* To manually send an SNMP trap, select an SNMP host server from the **Communities** list, and then click **Test**. The system sends a test SNMP trap to the selected SNMP server. Repeat this step to manually send test SNMP traps to other host servers.

   Note: To remove an SNMP trap destination from the **Communities** list, select the destination and click **Remove**.

10. When you are finished adding and testing SNMP trap destinations, from the navigation pane, select the **Alert Filtering by Severity** option.

    The **Alert Filtering by Severity** window opens.

    Use the options in this window to specify the severity level(s) which trigger the generation of an SNMP trap. The filter levels are listed from most severe (Error) to least severe (Information).

11. Select the checkbox for each severity level for which an SNMP trap report should be generated and sent.

    Note: To send SNMP traps, you must select at least one check box in the **Alert filtering by severity configuration** pane. Also, note that the level(s) of severity selected apply to all SNMP destinations in the **Communities** list.

12. When you have finished setting the severity levels, click **Submit** and from the navigation pane, select the **Physical Space Threshold Alerts** option.

    The **Physical Space Threshold Alerts** window opens with the **Physical space threshold alerts configuration** options disabled.

13. Read the information provided in the **Physical Space Threshold Alerts** pane to determine whether you want to set physical space threshold limits.

    - If you **do not** want to set physical threshold limits, leave the checkbox clear and go on to step 15.

    - If you **do** want to set physical threshold limits, in the **Physical space threshold alerts configuration** pane, select the checkbox (as shown in Figure 71) then go on to step 14

      Note: The physical threshold limits specified will apply to all SNMP destinations in the **Communities** list.

14. Select the threshold unit type (GB or Percent) and enter the corresponding values for the lower and upper free space threshold limits in the input fields, as shown in Figure 71:

Figure 71. Physical space threshold alerts configuration options

15. When you have finished setting the physical threshold limits, click **Submit** and from the navigation pane, select the **Nominal Space Threshold Alerts** option.

    The **Nominal space threshold alerts configuration** window opens.

16. Read the information provided in the **Nominal Space Threshold Alerts** pane to determine whether you want to set nominal threshold limits.

- If you **do not** want to set nominal threshold limits, leave the check box clear and go on to 18.
- If you **do** want to set nominal threshold limits, in the **Nominal space threshold alerts configuration** pane, select the checkbox (as shown in Figure 72) then go on to step 17.

  The nominal threshold limits specified will apply to all SNMP destinations in the **Communities** list.

17. Select the threshold unit type (GB or Percent) and enter the corresponding values for the lower and upper free space threshold limits in the input fields, as shown in Figure 72:

Figure 72. Nominal space threshold alerts configuration

18. When you have finished setting the nominal threshold limits, click **Submit**.

    Note: The **Backlog Threshold SNMP Alerts** option appears on the menu only if a replication grid has been created on the server. If the **Backlog Threshold SNMP Alerts** does not appear in the navigation pane, go on to 24 on page 189.

19. From the navigation pane, select the **Backlog Threshold SNMP Alerts** option. The **Backlog Threshold SNMP Alerts** window opens and displays the replication backlog threshold settings status of the remote repositories, if any exist.

20. Read the information provided in the **Backlog Threshold SNMP Alerts** pane to determine whether you want to set the replication backlog threshold limits.
    - If you **do not** want to set replication backlog threshold limits, go on to 23 on page 189.
    - If you **do** want to set replication backlog threshold limits, go on to 21.

21. From the **Replication Backlog Thresholds** pane, select the remote repository on which to set the backlog threshold and click **Set Threshold**. The **Set backlog threshold for repository** window is displayed, as shown in Figure 73 on page 189:
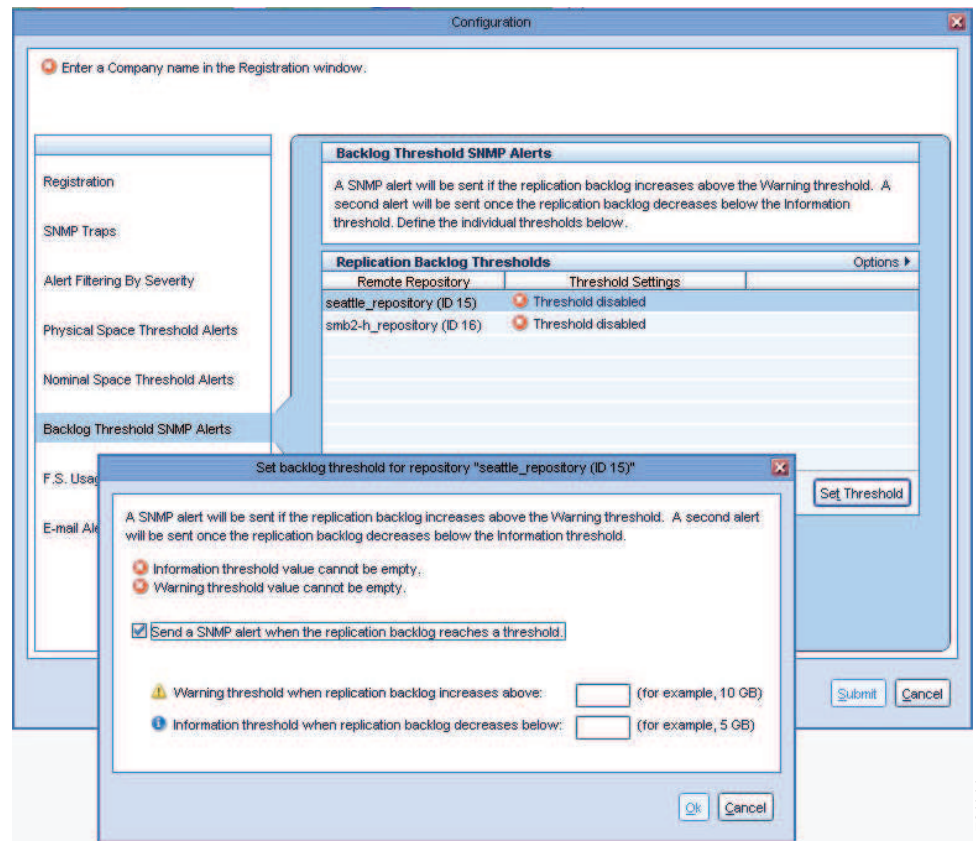
Figure 73. Set backlog threshold for repository

22. Select the checkbox to enable the threshold value input fields and enter the corresponding values (in GB) for the upper and lower replication backlog threshold limits.

23. When you have finished setting the replication backlog threshold limits, click **Ok** to close the window and click **Submit**. The threshold settings values for the selected repository display in the **Replication Backlog Thresholds** pane.

24. From the navigation pane, select the **E-mail Alerts** option. The **E-mail Alerts** window opens displaying the e-mail to which the alerts will be sent.

    Note: The e-mail displayed is the e-mail address that was configured during RAS configuration.

25. The system configuration to enable and define the parameters for SNMP reporting is now complete.

Using the cartridge query tool (for VTL)

This topic describes how to use the cartridge query tool to filter a specified set of cartridges in a repository.

About this task

Note: To use the cartridge query tool, an up-to-date repository must be created.

Use this procedure to run a query:

Procedure

1. From the Systems Management view, select **Reports** > **Cartridge Query tool**.

   A message displays when the repository inventory was last refreshed.

   Note: If you are using the Cartridge Query Tool to change the principality of a cartridge, or a set of cartridges, select **VT** > **VT Cartridges** > **Principality Cartridge Query Tool**. See "Changing cartridge ownership (Principality)" on page 102 for more information.

2. Click **Yes** to refresh the cartridge inventory. When the operation completes, the following window is displayed:
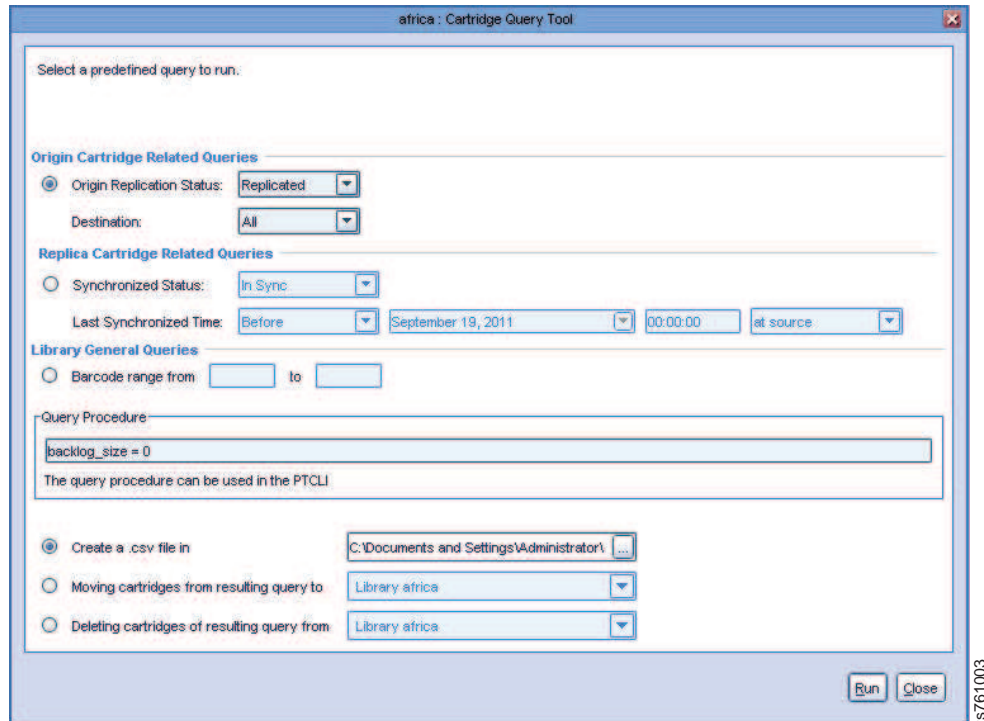
Figure 74. Cartridge Query Tool window

3. Select one of the desired predefined query types:

   - Origin Cartridge Related Queries

     Select the replication status from the dropdown list of the cartridges on the repository from which they were replicated and their destination.

   - Replica Cartridge Related Queries

     Select the synchronized status from the dropdown list of the cartridges on the repository to which they were replicated and the last synchronized time.

   - Library General Queries

     Select a range of cartridges to query by entering the barcode range (from/to).

4. Depending upon your selections, a predefined query is formulated in the **Query Procedure** frame. This procedure can be copied and used to run the query from a command-line interface using PTCLI (or you can click **Run** to run the procedure). Refer to "Query" on page 77 for more information.

5. Choose one of the following options to be performed with the query results:

   - Choose a file directory in which you want to create and save a .csv file with the query results.

- Select a library from the dropdown list **to** where you want to **move** the filtered cartridges resulting from the query.
- Select a library from the dropdown list **from** where you want to **delete** the filtered cartridges resulting from the query.

6. Click **Run**. The query is generated and the resulting task is performed.

   Note: If you chose to **delete** the cartridges of the resulting query, you will be prompted to type `data loss` to confirm running the procedure.

Generating a ProtecTIER service report

Complete this task to generate a service report on your ProtecTIER system for use by IBM Service.

About this task

A trained ProtecTIER specialist might request that you generate a service report detailing the status of your ProtecTIER system. Service report files can be attached to a support ticket and sent to a trained ProtecTIER specialist. Service reports can be generated for only one node at a time. You must be logged in as an administrator (ptadmin) to perform this function.

Procedure

1. From the Systems Management view, choose **Reports > Create service report**. The **Create service report** window is displayed.

Figure 75. Create service report window

2. From the **Selected node:** dropdown list, select a node for which to generate a service report.

3. Complete each of the input fields in the **Backup application** pane:
   - Host operating system
   - Backup application name
   - Backup application version

4. In the **Problem description** pane, type a brief description describing the problem.

5. From the **Filters** pane, select a report profile from the **Selected profile:** dropdown list. The following profile options are available:

Profile name	Description
Default	Collects all system information reports and all log files from either 4 days prior, or a maximum of 10 file entries, whichever comes first
Performance	Troubleshoots performance-related issues
Deduplication	Troubleshoots deduplication-related issues
Basic	Collects the minimum information (small size) and can be used for quick monitoring of performed procedures and fast results. Use only if asked by IBM Support.
Monitoring	Used when IBM Support requires frequent summaries on the system's health and behavior
Full	Collects all system information reports and all log files in their entirety
System view	Collects system information required to generate the system view html output
Coredump	Collects the *vmcore* dumps from the system to determine the cause of a system crash

6. Select the start and end dates to filter the report data by date range. Unless otherwise specified by IBM Support, the end date is the day the report is collected.

7. Click **Ok**. The Service Report file is created on the ProtecTIER server and a standard save dialog box is displayed.

8. Click **Save**. The report file is saved to the selected location.

9. If the cluster contains a second node, repeat steps 1 on page 191 though 8 for the second node in the cluster.

   Note: Perform a system check on the server by typing **sosreport**. The sosreport operation is time-consuming and is to be used only when you are directed to do so by a trained ProtecTIER specialist.

Generating a service report using the ProtecTIER Service menu

Complete this task to generate a service report on your ProtecTIER system using the ProtecTIER Service menu.

About this task

A trained ProtecTIER specialist might request that you generate a service report detailing the status of your ProtecTIER system. Service report files can be attached to a support ticket and sent to a trained ProtecTIER specialist.

Note: Only one service report can be generated per node at a time.

Procedure

1. If you are in a single node configuration, connect a USB keyboard and graphics-capable monitor to the server.
2. If you are in a clustered configuration, verify that Servers A and B are running:
   - If they are, go on to step 3.
   - If they are not running, power on any servers that are not running, wait for the boot cycle to complete, and then go on to step 3.
3. At the localhost **Login** prompt, type: **ptconfig** and press **<enter>**.
4. At the **Password** prompt, type: **ptconfig** and press **<enter>**

   The **ProtecTIER System Menu** displays:

   ```
   ----------------------------------------------------------------------
    ProtecTIER Service Menu running on rasap1
   ----------------------------------------------------------------------
       1) ProtecTIER Configuration (...)
       2) Manage ProtecTIER services (...)
       3) Health Monitoring (...)
       4) Problem Alerting (...)
       5) Version Information (...)
       6) Generate a service report
       7) Generate a system view
       8) Update ProtecTIER code

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

5. Select **Generate a service report**. Type the corresponding number and press **<enter>**. The following output is displayed:

   ```
   Your choice? 6
   Begin Processing Procedure

   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:
   ```

6. Choose a profile from the options displayed. Type the corresponding number and press <enter>. The following output is displayed:

```
Choose: 1
Please choose from what date to collect log files: ('q' to quit)
Choose: [YYYYMMDD]
```

7. Enter the date range to filter the report data. Type the start date in the format specified **[YYYYMMDD]** and press **<enter>**.

8. Type the end date in the format specified **[YYYYMMDD]**. The following example output is displayed:

```
Choose: [YYYYMMDD] 20110401
Please choose until what date to collect log files: ('q' to quit)
Choose: [YYYYMMDD] 20110410
```

9. Press **<enter>**. The service report is generated according to the chosen profile and a series of prompts are then displayed.

10. Complete the prompts as they appear:

   a. **Please specify the customer name (less than 10 characters or digits)** Type your customer name and press **<enter>**.

   b. **What is the operating system running on the host ?** Type the operating system running on the host and press **<enter>**.

   c. **What backup application (including version) is running on the host ?** Type the backup application and version running on the host and press **<enter>**.

   d. **Please describe the problem briefly.** Type a brief description of the problem and press **<enter>**.

11. The following example output is displayed:

```
Please wait...
Creating report...
done

Created /pt_work/ProtecTier_customer_popeye_default_Apr_12_2011_18_37_58_Report.tar.gz

End Processing Procedure with return code=1
+-----------------------------------------------------------------------------+
| ProtecTIER Service Menu running on popeye                                   |
+-----------------------------------------------------------------------------+
|   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?
```

The service report is now complete. You can repeat this procedure for additional nodes, or type **e** to exit the menu.The service report is now complete. Type **e** to exit the menu.

What to do next

When you have finished, contact a trained ProtecTIER specialist.

Creating a long-term statistics report

This task describes how to generate a long-term statistics report using ProtecTIER Manager.

About this task

Create a long-term statistics report for the nodes in your system when you want to analyze your system statistics.

Procedure

1. From the Systems Management view, choose **Reports > Create long term statistics report**. The **Create long term statistics report** window is displayed.
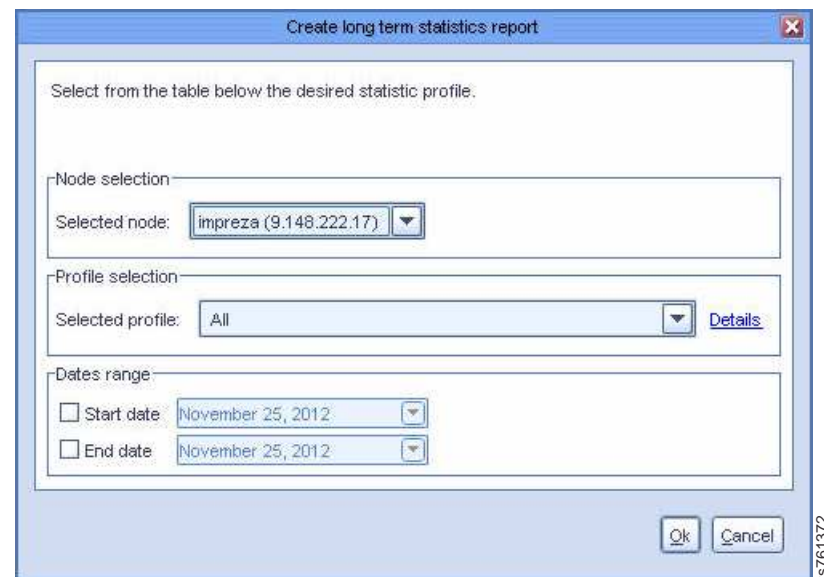
Figure 76. Create long term statistics report window

2. From the Node selection pane, select a node from the **Selected node:** dropdown list, or select **All** for all of the nodes in the system.
3. From the Profile selection pane, select a statistics profile from the **Selected profile:** dropdown list. The following options are available:

Profile name	Description
All (for support)	Collects all of the statistical data from the system. The report can be sent as a file to IBM Service for analysis.
ProtecTIER VTL Statistics Report	Displays statistics data for monitoring purposes.

The following table displays the information included in the ProtecTIER Statistics report. Each record measures the data from the timestamp of the previous record to the timestamp of the current record.

Contents of the **ProtecTIER VTL Statistics Report**:

Column	Description
processId	The ID number of the process.

Contents of the **ProtecTIER VTL Statistics Report**:

Column	Description
pollId	The time according to the Unix timestamp conversion.
Timestamp	The readable date and time of the sampling.
SamplingTimeSeconds	The duration, in seconds, between samples.
nSamplesPerPoll	The number of samples used for each poll.
Physical Size of Repository (bytes)	The physical size of the repository.
Nominal Data Size (bytes)	The amount of nominal data on the repository.
Used Physical Space (bytes)	The amount of space on the repository currently containing physical data.
Allocable Space (bytes)	The amount of free physical space on the repository that is available for new allocations.
Non-Allocable Space (bytes)	The amount of fragmented space on the repository that has to be defragmented to be available for new allocations.
Average Write Throughput (bytes/sec)	The average throughput of nominal data written to this node, in bytes/second.
Average Number of Writing Streams	The average amount of write streams on this node.
Average Read Throughput (bytes/sec)	The average throughput of nominal data read from this node, in bytes/second.
Average Number of Reading Streams	The average amount of read streams on this node.
Nominal Deleted Size (bytes)	The amount of nominal data deleted from the repository during the last poll.
Average Delete Throughput (bytes/sec)	The average throughput of nominal data that has been deleted.
Average Delete Backlog Per Node (bytes)	The average amount of nominal data backlog per node, in bytes, that still needs to be deleted from the repository.
Factoring Ratio	The ratio of the total amount of nominal data size over the used physical space.
Number of Defraggers tasks Finished	The number of defraggers tasks that have completed during this poll.
Defraggers Defragmented Size Bytes (cluster wide)	The amount of space freed up after defragmentation operations.
Nominal Incoming Throughput Average (KB/sec)	The average amount of incoming nominal throughput from the different sources replicating to this node.
Physical Incoming Throughput Average (KB/sec)	The average amount of incoming physical throughput from the different sources replicating to this node.
Nominal Outgoing Throughput Average (KB/sec)	The average amount of outgoing nominal throughput sent from this node to the destination(s).

Contents of the **ProtecTIER VTL Statistics Report**:

Column	Description
Physical Outgoing Throughput Average (KB/sec)	The average amount of outgoing physical throughput sent from this node to the destination(s).
Total Replication Backlog Average (bytes)	The average of the total amount of nominal data in the queue pending replication.
Replication Backlog Average Dest RID 0-3 (bytes)	The average of the total amount of nominal data in the queue pending replication per destination repository ID.

4. From the **Dates range** pane, select the start and end dates to filter the report data by date range.
5. Click **OK**. The long term statistics report file is created on the ProtecTIER server and a standard save dialog box is displayed.
6. Click **Yes** to download the report and save the file on the ProtecTIER Manager workstation.

Creating a performance analysis report

Complete this task to create a performance analysis report on your ProtecTIER system for use by IBM Service.

About this task

Create a performance analysis report for the nodes in your system when you want to analyze your system statistics.

Procedure

1. If you are using a single node configuration, connect a USB keyboard and graphics-capable monitor to the server.
2. If you using in a clustered configuration, verify that both Server A and Server B are running:
   - **Yes**, continue to step 3
   - **No**, power on any servers that are not running, wait for the boot cycle to complete, and then continue to step 3
3. At the localhost **Login** prompt, type: **ptconfig** and press **<enter>**.
4. At the **Password** prompt, type: **ptconfig** and press **<enter>**

   The **ProtecTIER System Menu** displays:

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

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

5. Select **ProtecTIER Analysis**. Type the corresponding number and press **<enter>**. The **Performance Analysis (...)** menu displays:

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
            Performance Analysis (...)
--------------------------------------------------------------------------------
  1) Performance Analysis

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

6. Select **Performance Analysis**. Type the corresponding number and press **<enter>**. The following output is displayed:

```
Begin Processing Procedure [Jan 29 06:50:41]
Please provide the following information: ('q' to quit)
1) Date interval.
2) Specific number of days from current date backwards.
Choose:
```

7. Enter the date to filter the report data in one of the following ways:

   - Provide date interval on the next format [YYYYMMDDHHMMSS].

   - Provide specific number of days to analyze, for example: 20D (20 days), 1W (one week), 1M (one month).

8. In case of running on a cluster system the script will prompt to ask if a performance analysis of the other node is needed. Select **Yes** or **No** and press **<enter>**. If running on a single node the script will start.

9. The performance analysis is generated according to the dates provided. The following example output is displayed:

```
Choose: 2
Period of time to analyze (Example: 20D, 2W, 1M, 1Y) : 20D
Do you want to performa a cluster analysis? (yes|no) yes
Getting Statistics                              [ Done ]
Running performance analysis                    [ Done ]
Performance analysis located at /pt_work/performance_2016_01_29_22_41_06.tar.gz

End Processing Procedure Successfully [Jan 29 22:37:09]

Press <enter> to continue.
```

Results

HTML files are created presenting the analysis report. The tar file generated needs to be extracted from ProtecTIER and opened on a host machine. After the file is uncompressed the directory will have the next files:

```
[root@Ronaldo Charts]# ll -h
total 64K
-rw-r--r-- 1 root root  16K Jan 29 22:41 clusterwide.htm
drwxr-xr-x 7 root root 4.0K Jan 26 09:26 HTML
-rw-r--r-- 1 root root 6.8K Jan 29 22:41 index.html
-rw-r--r-- 1 root root  15K Jan 29 22:41 node1.htm
-rw-r--r-- 1 root root  15K Jan 29 22:41 node2.htm
drwxr-xr-x 5 root root 4.0K Jan 29 22:28 Results
```

Open the index.html file in a browser to view the report.

Understanding the ProtecTIER Performance Analysis

This topic explains how to interpret the output of the Performance Analysis Report.

The Performance Analysis Report parses the long-term statistics from the node and creates easy to read HTML files with the performance information.

Report sections

The report will contain 3 main sections; each section contains a summary of the analysis and several charts with different information from the node.

Table 46. Performance analysis report sections

Section	Explanation
Repository	This section contains repository information such as allocated, used and fragmented space.
Node 1/ Node 2	This section contains the node specific performance information, such as backup and restore activity, delete, defrag and replication information.
Cluster	This section will be created only when the report is executed for both nodes. This section contains cluster wide performance information.

Charts

Performance analysis charts explain how the system was working at some specific period of time. Each chart represents 10 days of information so if the report was executed with a period of time of one month. There are four possible charts. You can move between the charts to view and understand system activities. Each activity on the chart gets a specific color and an axis. For example, the following chart shows how the allocated space is affected by the delete operation. Each time a delete operation is executed the allocated space increases.
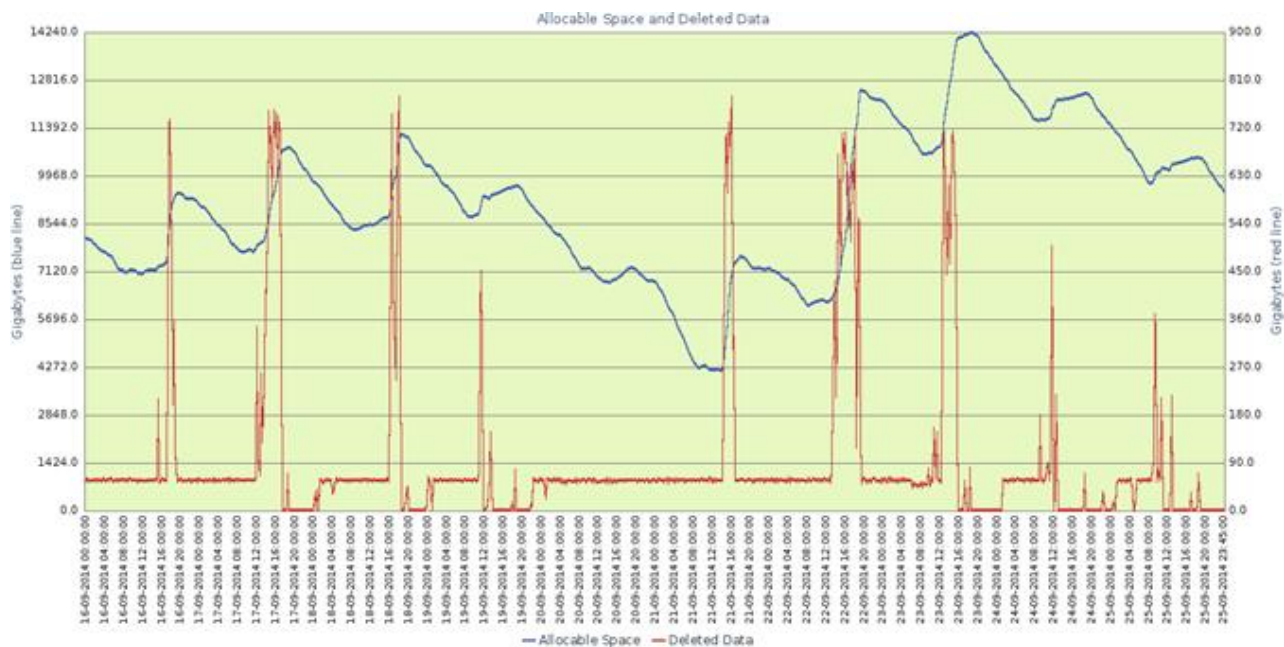
Figure 77. Performance analysis chart

Creating a system activities statistics report

This task describes how to generate a statistics report of the system activities in frequent and short-term intervals..

About this task

Create a system activities statistics report for each node in your system when you want to analyze your short-term system activities.

Note: By default the output file covers the past 4 days and has a resolution of 1 minute. This default can not be changed.

Procedure

1. From the Systems Management view, choose **Reports > Create system activites statistics report**. The **Create system activities statistics report** window is displayed.
2. From the Node selection pane, select a node from the **Selected node:** list.
3. Click **OK**. The system activities statistics report file is created on the ProtecTIER server and a standard save window is displayed.
4. Click **Yes** to download the report and save the *.csv* file on the ProtecTIER Manager workstation.
5. Click **Ok** to complete the procedure.

   The following table displays the information included in the System Activities Statistics report. Each record measures the data from the timestamp of the previous record to the timestamp of the current record.

Contents of the **System Activities Statistics Report**:

Column	Description
poll-id	The time according to the UNIX timestamp conversion.
friendly-poll-id	The readable date and time of the sampling.
timestamp	The time according to the UNIX timestamp conversion.
Deletion throughput (bytes/sec)	The rate at which data is deleted.
Defragmented throughput (bytes/sec)	The rate at which data is defragmented.
write throughput (bytes/sec)	The average throughput of nominal data that is written to the repository, in bytes.
Writing tapes	The average number of writing tapes on the system.
read throughput (bytes/sec)	The average throughput of nominal data that is read from the repository, in bytes.
Reading tapes	The average number of reading tapes on the system.
Physical in-replication throughput (bytes/sec)	The average throughput of incoming physical data from the different sources that replicate to this node.
Nominal in-replication throughput (bytes/sec)	The average throughput of incoming nominal data from the different sources that replicate to this node.
In-replication activities	The average number of replication streams in to the system.
Physical out-replication throughput (bytes/sec)	The average throughput of outgoing physical data that is sent from this node to the destination(s).
Nominal out-replication throughput (bytes/sec)	The average throughput of outgoing nominal data that is sent from this node to the destination(s).
Out-replication activities	The average number of replication streams out of the system.

Viewing machine reported product data (MRPD)

This topic explains how to view machine reported product data, or MRPD.

MRPD is the sub process that provides the capability of a system to report its own current hardware and software configuration information and vital product data, and make it available to those IBM processes and applications that need timely and accurate machine configuration information. Product data is gathered by a machine and sent to a destination, such as an IBM support server.

You can display machine product data using ProtecTIER Manager:
1. From the Systems Management view, choose **Reports** > **View product data (MRPD)**. The **View product data (MRPD)** window is displayed:

Figure 78. View product data (MRPD) window

2. Analyze the data to determine the required action. When you are finished, click **Ok** to close the window.

Monitoring backup and deduplication activities

This topics in this section describe how to use collect and analyze ProtecTIER backup and deduplication data.

Analyze Sessions is a utility used to monitor the data statistics for the backup and deduplication sessions of ProtecTIER. This utility can measure the change rate resolution by session (or daily, hourly, monthly).

The Dedup Estimator is an online tool that provides the current deduplication for the requested data (set of cartridges or per tape library) and therefore provides accurate results for an existing point in time.

Using the analyze_sessions utility

This topic describes how to collect and analyze ProtecTIER backup and deduplication data using the analyze_sessions utility

About this task

Use the analyze_sessions utility, under the **/opt/dtc/app/utils/** directory, to monitor the data statistics for the backup and deduplication sessions of your ProtecTIER system.

Note: In a 2-node cluster configuration, the analyze_sessions utility collects data from both nodes, so there is no need to run the command on each node separately.

Procedure

1. Change to the `/opt/dtc/app/utils/` directory.
2. Type `./analyze_sessions` at the command prompt.

Usage options	Explanation
-n	Number of previous months back to scan.
-sd	The <source directory> option is for working on compressor (.csv) files in locations other than the default miscellaneous directory of compressor
-io	(I/O throttle in MB/s) This tool runs on the machine, so that the available resources from the machine are not depleted. The default value is 5MB/s.
-daily	Adds a section with a line for each day.
-hourly	Add a section with a line for each hour.
-d	After the session is idle for more than <x> (1-20 minutes) amount of time, a new session is started.
-s	(Start date) Date format is YYYY-MM-DD-HH-MM, e.g. 2006-09-30-05-23. The processed times are startTime <= time <= endTime.
-e	(End date) Date format is YYYY-MM-DD-HH-MM, e.g. 2006-09-30-05-23. The processed times are startTime <= time <= endTime
-i	<cart_list_file> is the file name (full path) of the file that contains a list of cartridges names. The file report format contains each cartridge name on a separate line. The file format must be a Unix text file (and not Windows). **Note:** Make sure there are no empty lines at the end of the cartridge list. If an empty line exists at the end of the cartridge list, the data will not filter.
-c	This option is only relevant with the -i option. Creates a file with the name of the cartridge file + __.csv that contains the rows from the original compressor .csv files, related to the cartridges in the list. The .csv file is saved in the `/pt_work` directory.
-o	<output file name> The output data is dumped into this file, instead of output on the screen.
-min	Minimal output displays "all" with the grand totals and headers. The daily and hourly flags are overridden.

Usage options	Explanation
-l	This option is only relevant with the -i option. Adds a section to the regular report file with a line of the totals for each cartridge in the list (limited to 4K cartridges). If there are more than 4K cartridges with the -l option, an error message will be displayed and the utility will exit.
Nosessionfilter	Includes all sessions, even the small ones, in the sessions list. For example, if you have a session that is smaller than 1MB, it is included in the output. (The minimum file size with the session filter is 1MB.)

3. An output file containing statistics for the recent sessions is generated at the following location: /ptwork/<server name>-<date>-<time>.csv during the respective time period.

Results

The following is an example of running the analyze_sessions utility with the -l and -i server options to display a list of the cartridge names and their totals in the report:

```
[root@ny utils]# ./analyze_sessions -d 5 -s 2012-12-01-00-00 -e  2012-12-31-01-00
  -l -i /pt_work/cart_list

analyze_sessions: this program analyzes the logs on the current
ProtecTIER server.  Its output is the change rate between each
session and data that was available in the repository at the time.

This program and its output contain proprietary information of
International Business Machines Corporation.

(c) Copyright International Business Machines Corporation 113. All rights reserved.

startDate date: 2012-12-1 00:00:00
endDate date: 2012-12-31 01:00:59

Read 167MB, throughput: 5.21MB/s
Output file is /pt_work/ny-2013-01-03-16-27-09.csv
[root@ny utils]#
```

The .csv file looks similar to the following:

Analysis of factoring results from ny							
03/01/2013 16:27							
This output was generated by analyze_sessions and contains proprietary information of International Business Machines Corporation.							
(c) Copyright International Business Machines Corporation 2013. All rights reserved.							
Name	Total data (TB)	Total data (GB)	System change rate	Factoring ratio	compressed Bytes Count (GB)	start time	end time

Analysis of factoring results from ny							
03/01/2013 16:27							
Grand totals							
all	0.146472	149.988	35.13%	2.84659	31.2975	23/12/2012 12:31	30/12/2012 04:05
carts total							
B00000	0.0360501	36.9153	35.84%	2.79007	7.85946	23/12/2012 12:32	30/12/2012 04:01
B00001	0.0367187	37.6	34.50%	2.8982	7.70792	23/12/2012 12:31	30/12/2012 03:49
B00002	0.0366516	37.5312	36.33%	2.75257	8.09903	23/12/2012 12:33	30/12/2012 04:05
B00003	0.0370518	37.9411	33.87%	2.95244	7.63114	23/12/2012 12:33	30/12/2012 04:05
By session (summary)							
2012-12-23 12:31:32 to 2012-12-23 13:04:19	0.0490185	50.195	100%	1	29.8033	23/12/2012 12:31	23/12/2012 13:04
2012-12-27 12:16:30 to 2012-12-27 12:24:06	0.0247249	25.3183	0.05%	2145.05	0.00807142	27/12/2012 12:16	27/12/2012 12:24
2012-12-27 12:39:27 to 2012-12-27 12:47:20	0.0237776	24.3483	5.52%	18.1139	0.803133	27/12/2012 12:39	27/12/2012 12:47
2012-12-30 03:45:10 to 2012-12-30 04:05:31	0.0489512	50.126	2.27%	43.9995	0.683006	30/12/2012 03:45	30/12/2012 04:05

A summary of statistical information is included by session:

Table 47. Recent backup session and deduplication statistics

Statistic	Description
Total data (TB)	Total amount of data backed up during the session, in terabytes.
Total data (KB)	Total amount of data backed up during the session, in kilobytes.
System change rate	Percentage of nominal data in the backup session that was factored and recognized as changed relative to the previous backup session.

Table 47. Recent backup session and deduplication statistics (continued)

Statistic	Description
Factoring ratio	The factoring ratio is the deduplication of the nominal data size before compressing.
compressedBytesCount (GB)	The amount of data that was written to the disk after factoring and compression.
Start time	Start time of the backup session.
End time	End time of the backup session.

Using the dedup estimator tool

This topic describes how to collect and analyze ProtecTIER backup and deduplication data using the dedup estimator tool

Before you begin

Before you can use the dedup estimator tool, you must create a profile using ptcli utility. See "Creating a profile" on page 65 for instructions.

About this task

Use the online dedup estimator tool to monitor the data statistics for the backup and deduplication sessions of your ProtecTIER system. You can use the dedup estimator tool to calculate deduplication ratios in four ways; by file, library, range, or parameter.

Procedure

1. To calculate deduplication ratios by file, change to the `/opt/dtc/ptcli/ptcli/` directory and type `./CalculateVtlDedupRatioByFile` at the command prompt.

Usage options	Explanation

--file PATH	The path to a file containing a list of cartridges to be calculated. The file structure must be in a format in which each cartridge is in a separate line, without any other characters. For example:
	
	`L00000`
	`L00001`

[--maxErrorsPercentage NUM]	The Maximum errors percentage between 0 to 100. (Default value is taken from GetDedupRatioParameters output)
[--tolerancePercentage NUM]	The tolerance percentage between 0 to 100. (Default value is taken from GetDedupRatioParameters output)
[--numOfSamples NUM]	The number of samples within server limits. (Default is taken from GetDedupRatioParameters output)

2. To calculate deduplication ratios by library, change to the `/opt/dtc/ptcli/ptcli/` directory and type `./CalculateVtlDedupRatioByLibrary` at the command prompt.

Usage options	Explanation
libraryName LIBRARY	Library name to calculate. Only one library can be processed at a time.
[--maxErrorsPercentage NUM]	The Maximum errors percentage between 0 to 100. (Default value is taken from GetDedupRatioParameters output)
[--tolerancePercentage NUM]	The tolerance percentage between 0 to 100. (Default value is taken from GetDedupRatioParameters output)
[--numOfSamples NUM]	The number of samples within server limits. (Default is taken from GetDedupRatioParameters output)

3. To calculate deduplication ratios by range, change to the `/opt/dtc/ptcli/ptcli/` directory and type `./CalculateVtlDedupRatioByRange` at the command prompt.

Usage options	Explanation
--fromBarcode	BARCODE From cartridge barcode.
--toBarcode	BARCODE To cartridge barcode.
[--maxErrorsPercentage NUM]	The Maximum errors percentage between 0 to 100. (Default value is taken from GetDedupRatioParameters output)
[--tolerancePercentage NUM]	The tolerance percentage between 0 to 100. (Default value is taken from GetDedupRatioParameters output)
[--numOfSamples NUM]	The number of samples within server limits. (Default is taken from GetDedupRatioParameters output)

4. To calculate deduplication ratios by parameters, change to the `/opt/dtc/ptcli/ptcli/` directory and type `./CalculateVtlDedupRatioByParameters` at the command prompt.

Results

The following is an example of running the dedup estimator tool by file, library or range:

```
#### WARNING!! ####
All open sessions of PT Manager must be terminated before running Dedup Estimator utility.
To continue working with PT Manager while running the Dedup Estimator utility,
connect to PT Manager as ptoper.

Please wait while Dedup Estimator is working. This may take a few minutes to complete.
Preparing: 100% completed
Analyzing: 100% completed
Calculating: 100% completed

Node-id = 1
Estimated compression-ratio = 1:2.09
Estimated dedup-ratio = 1:3.61
Estimated overall factoring-ratio = 1:7.54
16384 successful samples out of 16384
```

The following is an example of running the dedup estimator tool by parameter:

```
#### WARNING!! ####
All open sessions of PT Manager must be terminated before running Dedup Estimator utility.
To continue working with PT Manager while running the Dedup Estimator utility,
connect to PT Manager as ptoper.
####
Node-id = 1
defaults :
    confidence-percentage = 90
    max-errors-percentage = 10
Limits :
     num-of-samples :
         from = 1
         to = 16384
Function completed successfully.
```

Chapter 15. Troubleshooting

The topics in this section provide tips, guidelines, and procedures for handling error situations that might arise within the ProtecTIER system.

Errors that occur in your ProtecTIER system can be monitored using the Alerts dialog and the Event Log dialog. All errors within the ProtecTIER system should be reported to a trained ProtecTIER specialist. A trained ProtecTIER specialist can guide you in determining the cause of the error and finding a solution. In addition, the **Check and recover** wizard, included in ProtecTIER Manager, can find and repair some errors.

Common troubleshooting tasks

The topics in this section describe common troubleshooting tasks you might perform while working with a trained ProtecTIER specialist.

Miscellaneous tasks that a trained ProtecTIER specialist might ask you to perform during the troubleshooting process are listed here.

Attention: Do not perform these tasks unless you are directed to do so by IBM Support.

- **Disabling defragmentation** - Enables you to stop the defragmentation process. For more information, see "Disabling defragmentation."
- **Disabling compression** - Enables you to stop the data compression process. For more information, see "Disabling data compression" on page 210.
- **Changing the HyperFactor mode** - Enables you to stop the HyperFactoring process. For more information, see "Changing the HyperFactor mode" on page 210.
- **Modifying the trace buffer** - Enables you to dump or reset the trace buffer, or to change the trace settings. For more information, see "Modifying the trace buffer" on page 211.
- **Resetting devices** - Enables you to reset a robot or tape drive in a virtual library. For more information, see "Resetting devices" on page 213.
- **Unloading and moving cartridges** - Enables you to manually move virtual cartridges between slots and tape drives. For more information, see "Unloading and moving cartridges" on page 214.

Disabling defragmentation

Complete this task to disable defragmentation.

About this task

The ProtecTIER system automatically defragments fragmented repository disk space as a background task at a rate that does not cause the system to slow down. Stop defragmentation to free the resources used by the defragmentation process.

Procedure

1. Choose **Repository > Defragmentation control**. The **Defragmentation control** dialog is displayed.

2.	Select **Disable defragmentation** and click **Ok**. The **Defragmentation control pane** closes and defragmentation is disabled.

Results

Note: Selecting Enable defragmentation in the Defragmentation control pane resumes system defragmentation.

Disabling data compression

Complete this task to disable data compression.

About this task

Under normal circumstances, the ProtecTIER system compresses data. Stop compression on a specific virtual library to free the resources usually demanded by the compression process.

Perform the following steps to disable data compression for a specified Virtual Tape (VT) library.

Procedure

1.	Choose **VT** > **VT Library** > **Set compression type**. The **ProtecTIER compression mode** dialog is displayed.
2.	Select **VT**, **VT Library**, and finally **Set compression type**. The compression mode dialog box is displayed.
3.	Select **Disable compression** and click **Ok**. The **ProtecTIER compression mode** dialog closes and compression is stopped.

	Note: Selecting **Enable compression** in the **ProtecTIER compression mode** dialog box resumes data compression.

Changing the HyperFactor mode

Complete this task to change the HyperFactor mode for a specified library.

About this task

By default, ProtecTIER factors all new incoming data, detecting recurring data and storing only the data segments that have not previously been written to the repository. You can change the default HyperFactor mode for each library.

Perform the following steps to change the HyperFactor mode on a specified VT library.

Procedure

1.	Choose **VT** > **VT Library** > **Set HyperFactor mode**. The **ProtecTIER VT HyperFactor mode** dialog is displayed.
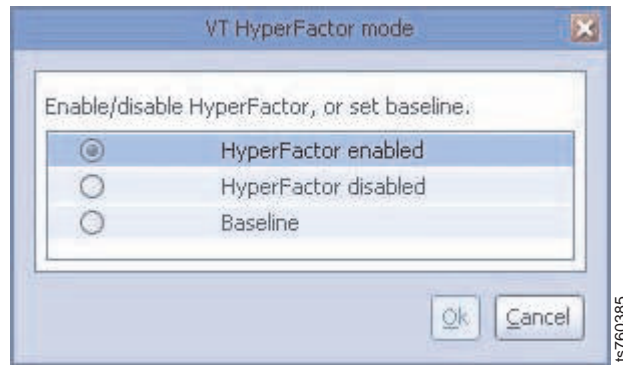
Figure 79. ProtecTIER VT HyperFactor mode dialog

2. Select one of the following options, as directed by a trained ProtecTIER specialist:
   - **Hyperfactor enabled**. HyperFactor operates as normal.
   - **HyperFactor disabled**. HyperFactor stops. When you restart HyperFactor, the HyperFactor process proceeds as normal based on the data stored from before HyperFactor stopped.
   - **Baseline**. HyperFactor stops factoring incoming data and uses the newly stored non-factored data as the reference for factoring new data after Hyperfactor is resumed.
3. Click **Ok**. The **ProtecTIER VT HyperFactor mode** dialog closes and HyperFactor stops.

Modifying the trace buffer

The ProtecTIER system stores runtime information in a cyclic memory buffer. A trained ProtecTIER specialist might direct you to dump the trace buffer for analysis, set the trace recording levels, or reset the trace buffer.

Note: You can manage the trace buffer for only one node at a time.

Dumping the trace buffer

Complete this task to create a file of the trace buffer contents for a specified node and save it to the ProtecTIER server.

About this task

Dumping the trace buffer saves a file of the trace buffer contents to the ProtecTIER server. Attach this file to a support ticket to send to a trained ProtecTIER specialist.

Procedure

1. In the **Systems Management** view, select a node from the navigation pane.
2. Choose **Node** > **Trace** > **Dump trace**. A confirmation message box is displayed.
3. Click **Yes**. The trace buffer information is saved to the ProtecTIER server.

   The trace buffer report is generated for the node and saved to the ProtecTIER server.

   Note: Record the file name so that you can find it when IBM Service asks you to send it in with an attached support ticket.

Setting the trace levels

Complete this task to change the trace levels for a specified node.

About this task

The ProtecTIER system traces and records many types of operation information at various levels of detail. These trace levels are initially set in manufacturing.

IBM Support might direct you to reduce the level of detail traced for certain components. This request is made so that system resources are freed up or to increase the level of detail for system components that are suspected to be problematic.

Perform the following steps to set the trace levels for a specified node.

Procedure

1. From the **Systems Management** view, select a node in the navigation pane.
2. Choose **Node** > **Trace** > **Set trace levels**. The **Set trace levels** window is displayed.
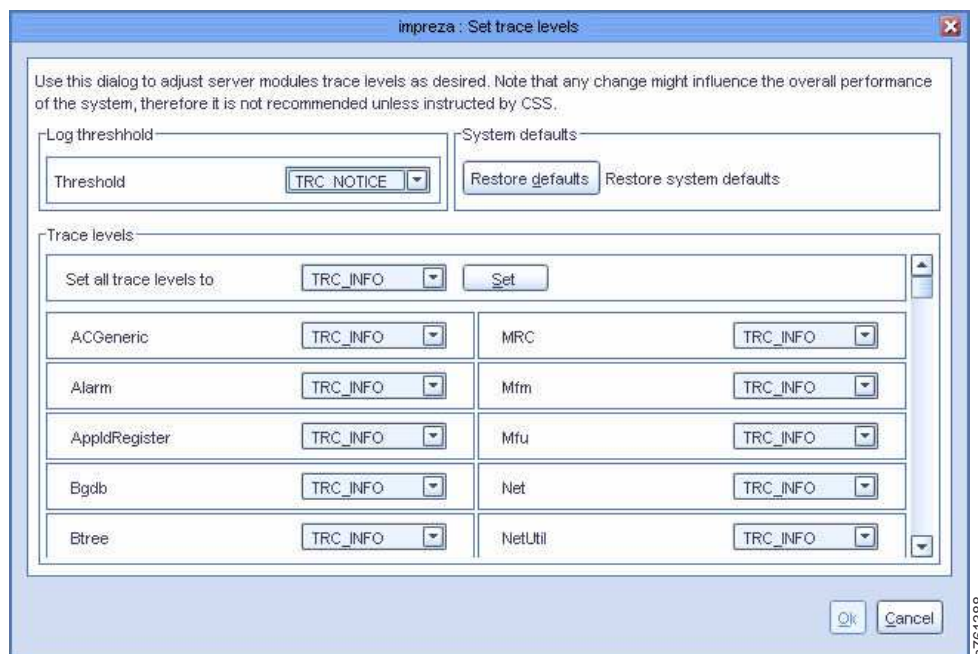
Figure 80. Set trace levels window

3. Change the trace level settings, as directed by IBM Support.
4. Click **Ok**. The **Set trace levels** window closes and the new trace levels are set.

Resetting the trace buffer
About this task

Resetting the trace buffer empties the buffer.

Procedure

1. From the **Systems Management** view, select a node from the navigation pane.
2. Choose **Node** > **Trace** > **Reset trace**. A confirmation message box is displayed.

3. Click **Yes**. The trace buffer is reset for the designated node and new information begins to be gathered for that node.

Resetting devices

If a virtual robot or tape drive is locked, reset the device to break any existing SCSI2 reservations on the device.

Attention: Resetting a robot or tape drive while the backup application is accessing the library can harm the backup operations. Do not reset a device unless directed to do so by a trained ProtecTIER specialist.

Resetting robots

Complete this task to reset a robot.

About this task

There might be times when a virtual robot is locked and you need to reset the robot to break any existing SCSI2 reservations on the robot.

Note:
1. Do not initiate this action unless directed to do so by a trained ProtecTIER specialist.
2. Resetting a robot while the backup application is accessing the library can harm the backuphost operations.

Perform the following steps to reset a robot:

Procedure

1. From the **Systems Management** view, select a library from the navigation pane.
2. Choose **VT > VT Library > Reset robot**. A confirmation message box is displayed.
3. Choose the port and click **Yes**. The robot is reset.

Resetting the virtual tape drives

Complete this task to reset a virtual tape drive.

About this task

There might be times when a virtual tape drive is locked and you need to reset the drive to break any existing SCSI2 reservations on the tape.

Note:
1. Do not initiate this action unless directed to do so by a trained ProtecTIER specialist.
2. Resetting a virtual tape drive while the backup application is accessing the library can harm the backup operations.

Perform the following steps to reset a virtual tape drive.

Procedure

1. From the **Systems Management** view, select a library in the navigation pane.
2. Click the **Drives** tab.
3. Select a drive.

4. Choose **VT > VT Drive > Reset drive**. A confirmation message box is displayed.
5. Click **Yes**. The tape drive is reset.

Unloading and moving cartridges

Attention: Manual unloading and moving of cartridges is not detected by your backup application and can result in the loss of synchronization between your backup application and ProtecTIER. Furthermore, unloading or moving cartridges while the backup application is using the library can harm the backup operations. Do not unload or move a cartridge manually unless directed by a trained ProtecTIER specialist.

Unloading cartridges
Complete this task to unload a cartridge by using ProtecTIER Manager.

About this task

You must unload a cartridge from its drive before you can move it to a slot.

Perform the following steps to disconnect (unload) a cartridge from a drive:

Procedure
1. From the **Systems Management** view, select a library from the navigation pane.
2. Click the **Drives** tab.
3. Select a drive that contains a loaded cartridge.

   Note: Loaded drives are indicated with .
4. Choose **VT > VT Drive > Unload drive**. A confirmation message box is displayed.
5. Click **Ok**. The drive is unloaded.

   Note: Unloaded drives are indicated with .

Moving cartridges
Complete this task to move a cartridge after it has been disconnected (unloaded) from a virtual tape drive.

Procedure
1. From the **Systems Management** view, select a library from the navigation pane.
2. Navigate to the Services pane and select a library.
3. Click the **Drives** tab.
4. Select a drive that contains an unloaded cartridge.

   Note: When moving cartridges from a slot, select the Slot tab and select a slot that contains a cartridge.
5. Choose **VT > VT Cartridge > Move cartridge**. The **Move cartridge** window is displayed.
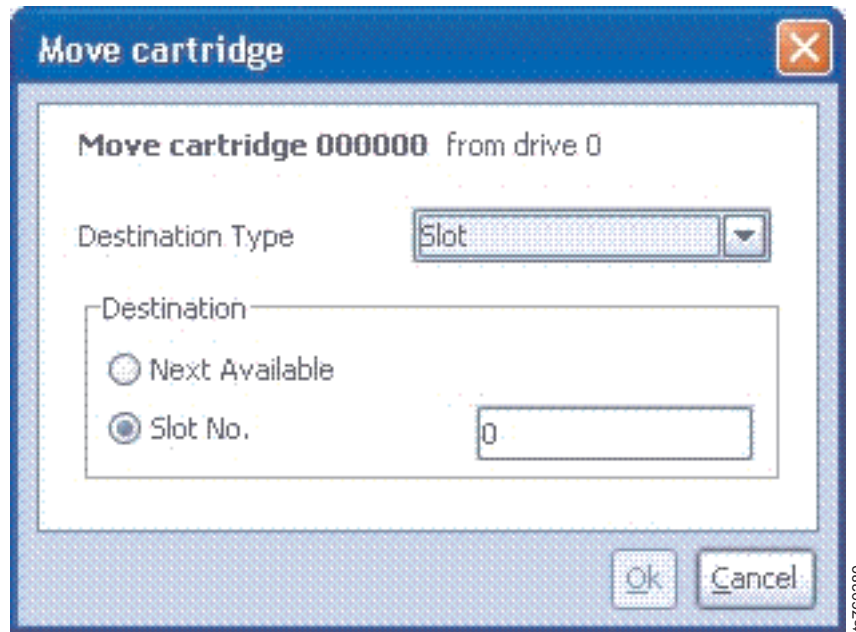
Figure 81. Move cartridge window

6. In the **Destination Type** field, select one of the following destinations:
   - Drive
   - Slot
   - Import / Export
7. In the **Destination** area, select one of the following options:
   - **Next Available** - The cartridge is placed in the next available location of the selected type.
   - **Slot/Drive No.** - The cartridge is placed in the slot or drive with the number specified in the field. The name of this field depends on your selection in the **Destination Type** field.
8. Click **Ok**. The cartridge is moved to the specified location.

Viewing the alerts and events log windows

This topic describes how to view alerts and events in the ProtecTIER system logs using the ProtecTIER Manager application.

About this task

If an error occurs, the Alerts button on the bottom-right of the View pane turns red and features a blinking exclamation mark.

Click **Software Alerts** to view the list of error events in the **Alerts Log** dialog.
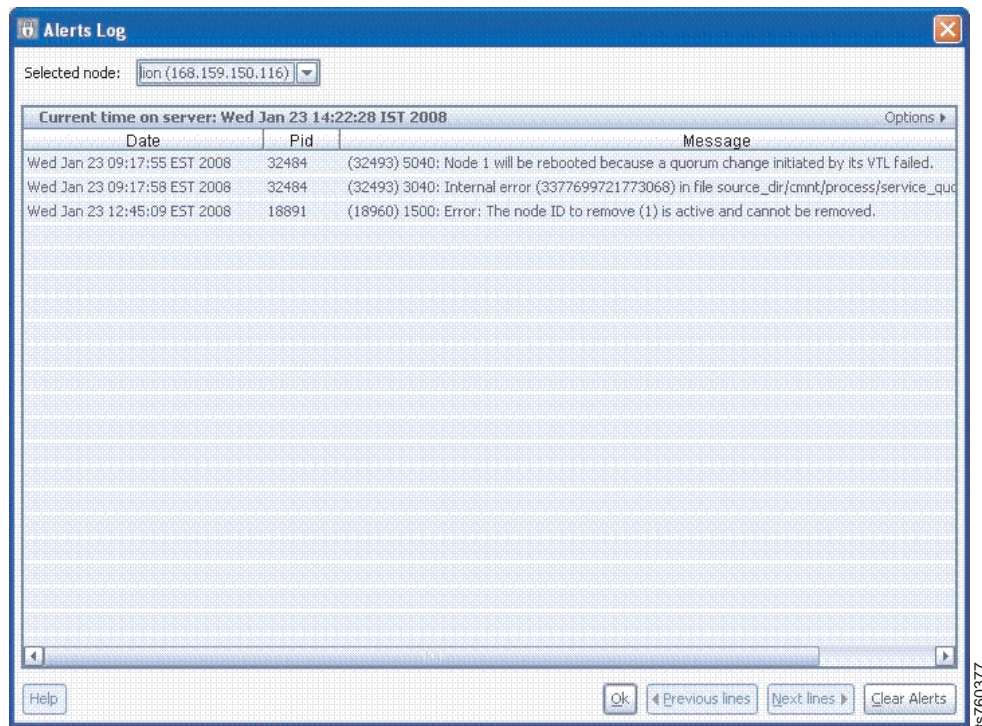
Figure 82. Alerts log

The **Alerts Log** and **Events Log** dialogs only display information for one node at a time. In addition, the **Alerts Log** and **Events Log** dialogs only display up to 200 alert events at one time. Navigate to a previous set of 200 alert events by clicking **Previous lines**. Navigate to a later set of 200 alert events by clicking **Next lines**.

Note: View the error log directly on a ProtecTIER server by opening the /pt_work/log/vtf_error.log file. View the alerts log by opening the /pt_work/log/vtf_event.log file.

Wizard error messages

ProtecTIER Manager wizards feature a **Message** area to inform you of issues that relate to each wizard screen.
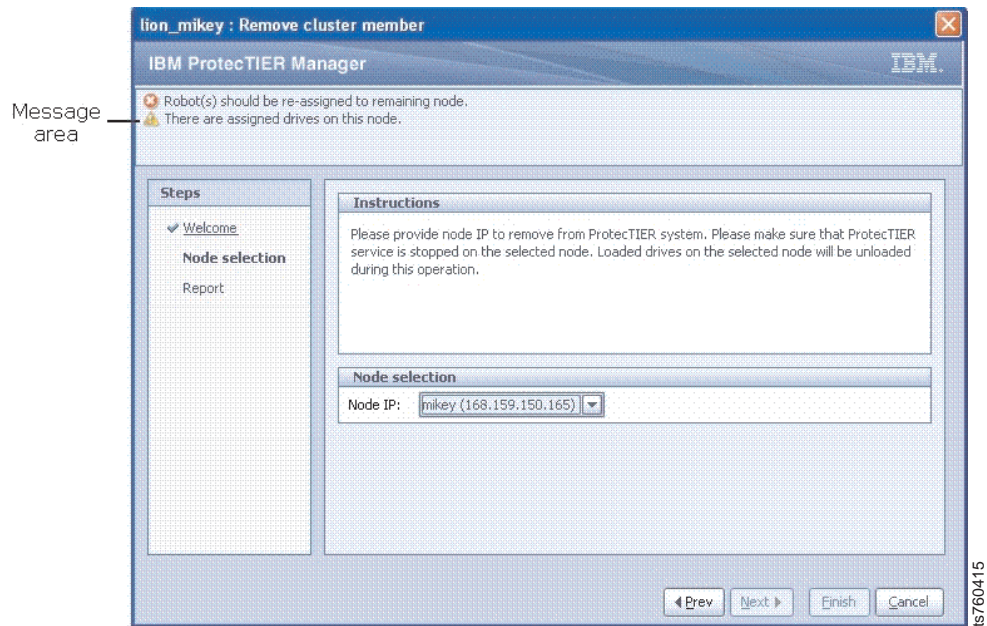
Figure 83. Message area

Messages can be of the following types:

You cannot continue the wizard until this problem is resolved.

You can continue the wizard without resolving this issue, but it is not recommended.

Checking and repairing errors

Before checking and recovering errors with ProtecTIER Manager, ensure that the file systems are stable and free of errors that require fsck. Running the ProtecTIER Manager check and recovery wizard on inconsistent file systems can impair the consistency of the repository.

Checking for errors requiring fsck

Complete this task to check for file system consistency.

About this task

The purpose of this task is to discover all error messages that indicate the need to run fsck. Perform the following steps to check for file system consistency errors:

Procedure

1. Open the `/var/log/messages` file.
2. Search for error messages of the following types:
   - GFS: fsid=<cluster name>:<file system name>: fatal filesystem consistency error
   - GFS: fsid=<cluster name>:<file system name>: about to withdraw from the cluster
   - GFS: fsid=<cluster name>:<file system name>: telling LM to withdraw
   - GFS: fsid=<cluster name>:<file system name>: withdrawn
   - kernel: [<ffffffff887e8094>] :gfs:gfs_lm_withdraw+0xc4/0xd3
   - gfs_controlId[2905]: <file system name> finish: needs recovery jjd 0 nodeid 2 status 1

Results

If you find these types of error messages, run **fsck** on the file systems referenced by the error messages.

Determining the volume names of file systems

Complete this task to find the volume names for file systems.

Procedure

1. Run `gfs_tool df`. Summary information for all Global File Systems (GFS) in your repository is displayed.
2. Locate the appropriate file system names and determine their mount points.

   The following output file is an example of the system output when you run `gfs_tool df`. The file system name is in bold and the mount point name is italicized:

   ```
   /mnt/vgfs0113-lvfs0113
   SB lock proto = "lock_dlm"
   SB lock table = "lurebimepegoco:gfs_0113"
   SB ondisk format = 1309
   SB multihost format = 1401
   Block size = 4096
   Journals = 3
   Resource Groups = 16384
   Mounted lock proto = "lock_dlm"
   Mounted lock table == "lurebimepegoco:gfs_0113"
   Mounted host data = "jid=0:id=14876673:first=0"
   Journal number = 0
   Lock module flags = 0
   Local flocks = FALSE
   Local caching = FALSE
   Oopses OK = FALSE
   Type      Total Blocks   Used Blocks   Free Blocks    use%
   ----------------------------------------------------------------
   inodes    512        512        0        100%
   metadata     5176264    4223508    952756      82%
   data    2142060068   2111434535   30625533     99%
   ```

3. Open `/etc/fstab` and determine the corresponding logical volumes names. The following output is an example of the fstab entry format:

   ```
   /dev/mapper/<logical volume name> /<mount point> gfs defaults,noatime,nodiratime,noquota,acl 0 0"
   ```

Running fsck online

ProtecTIER Version 3.3.7 includes the capability of running `fsck` online. You do not need to take the system offline while you run fsck. The system stays operational so that backups and restores continue while you check the consistency of the file systems.

Before you begin

Before you run `fsck`, run the procedure in "Checking and repairing errors" on page 217 to check for errors that require the use of `fsck`. Also, ensure that the file system on which you intend to run `fsck` is unmounted.

To run the Online `fsck` Recovery, your system must meet the following requirements:
- ProtecTIER must be configured as a 2-node cluster.
- Each node in the ProctecTIER cluster must be configured with at least 64 GB of RAM.
- One of the following criteria must be true:
  - Medium changer is active on the node that is up during the FSCK Recovery process, OR
  - Control Path Failover (CPF) is enabled if you use Tivoli Storage Manager as its backup application.

If your system does not meet this criteria, use the procedure that is described in "Running fsck" on page 220.

Procedure

1. Select one of the ProtecTIER nodes.
2. At the **login:** prompt, log in with the ID `root` and the password `admin`.
3. Shut down the **vtfd** and **ptcluster** services in the following order:
   ```
   # service vtfd shutdown
   # service ptcluster shutdown
   ```

   Attention: Make sure to use the *shutdown* option and not the *stop* option. If you use *stop*, the services restart automatically if a reboot occurs.
4. Start the **cman** and **clvmd** services in the following order:
   ```
   # service cman start
   # service clvmd start
   ```
5. For each of the problematic file systems, run the **gfs_fsck –yv** command in the background with high verbosity and direct the output to a file:
   ```
   # gfs_fsck -yv logical volume name > /pt_work/vgxx_fsck.out 2>&1 &
   ```

   For example, the following command runs gfs_fsck on the logical volume */dev/mapper/vg0-lv_vg0*:
   ```
   # gfs_fsck -yv /dev/mapper/vg0-lv_vg0 > /pt_work/vg0_fsck.out 2>&1 &
   ```
   The output is saved in the file "/pt_work/vg0_fsck.out."

   Note: ProtecTIER supports up to 10 parallel gfs_fsck instances.
6. When all the gfs_fsck processes are complete, remove the /etc/pt/dont_start_vtfd and /etc/pt/dont_start_ptcluster.
   ```
   # rm –f /etc/pt/dont_start_vtfd
   # rm –f /etc/pt/dont_start_ptcluster
   ```

7. Restart the node.

   `# reboot –nf`

   ProtecTIER is now up and running.

8. Send the `fsck` output to trained ProtecTIER specialist to determine the next step.

Running fsck

Complete this task to run `fsck` to check the consistency of the file systems before you run ProtecTIER Manager to check and repair any ProtecTIER system errors.

Before you begin

Before you run `fsck`, run the procedure in "Checking and repairing errors" on page 217 to check for errors that require the use of `fsck`. Also, ensure that the file system on which you intend to run `fsck` is unmounted.

Procedure

1. On a two-node cluster, select one of the ProtecTIER nodes. If you have a single node system begin with step 7 on page 221.
2. At the **login:** prompt, log in with the ID root and the password `admin`.
3. Type `menu` on the command line and press Enter. The ProtecTIER Service main menu appears.

```
----------------------------------------------------------------------
  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?
```

4. Select **Manage ProtecTIER services (...)**. The **Manage ProtecTIER services (...)** menu is displayed.

```
----------------------------------------------------------------------
  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?
```

5. Select **Stop all services** to stop the ProtecTIER services on the node.
6. Shut down the stopped node.

7. On the active node, shut down the **vtfd** and **ptcluster** services in the following order:

```
# service vtfd shutdown
# service ptcluster shutdown
```

Attention: Make sure to use the *shutdown* option and not the *stop* option. If you use *stop*, the services restart automatically if a reboot occurs.

8. Start the **cman** and **clvmd** services in the following order:

```
# service cman start
# service clvmd start
```

9. For each of the problematic file systems, run the **gfs_fsck –yv** command in the background with high verbosity and direct the output to a file:

```
# gfs_fsck -yv logical volume name > /pt_work/vgxx_fsck.out 2>&1 &
```

For example, the following command runs gfs_fsck on the logical volume */dev/mapper/vg0-lv_vg0*:

```
# gfs_fsck -yv /dev/mapper/vg0-lv_vg0 > /pt_work/vg0_fsck.out 2>&1 &
```

The output is saved in the file "/pt_work/vg0_fsck.out."

Note: ProtecTIER supports up to 10 parallel gfs_fsck instances.

10. When all the gfs_fsck processes are complete, remove the /etc/pt/dont_start_vtfd and /etc/pt/dont_start_ptcluster so that these services begin again when you restart the node.

```
# rm –f /etc/pt/dont_start_vtfd
# rm –f /etc/pt/dont_start_ptcluster
```

11. Restart the node.

```
# reboot –nf
```

12. Restart the inactive node.

ProtecTIER is now up and running.

13. Send the `fsck` output to trained ProtecTIER specialist to determine the next step.

Checking and repairing with ProtecTIER Manager

After any problematic file systems have been repaired, scan the ProtecTIER system for errors, and attempt to repair them, using the **Check and recover** wizard.

Notes:

- For v3.3 and earlier, the check and recovery process is time-consuming and the ProtecTIER system goes offline for the duration of the process. IBM therefore recommends that you use the **Check and recover** wizard only for severe problems.
- ProteTier v3.4 introduces a new feature, Near-Online check and recovery. This feature reduces the downtime of ProteTIER during check and recovery by enabling a continuous backup flow for most of the process. See "Near online check and recovery" on page 223.

Checking the system

Complete this task to check the system for errors.

About this task

Attention: The check and recovery process is time-consuming and is to be used only when you suspect a severe problem. Running the ProtecTIER Manager check and recovery wizard on top of inconsistent file systems can impair the consistency of the repository.

Perform the following steps to use ProtecTIER Manager to check for errors:

Procedure

1. Choose **System** > **Check and recover**. A confirmation message box is displayed.
2. Click **Yes**. The ProtecTIER system goes offline and scans itself. The **Check and recover** dialog is displayed with the results of the scan.
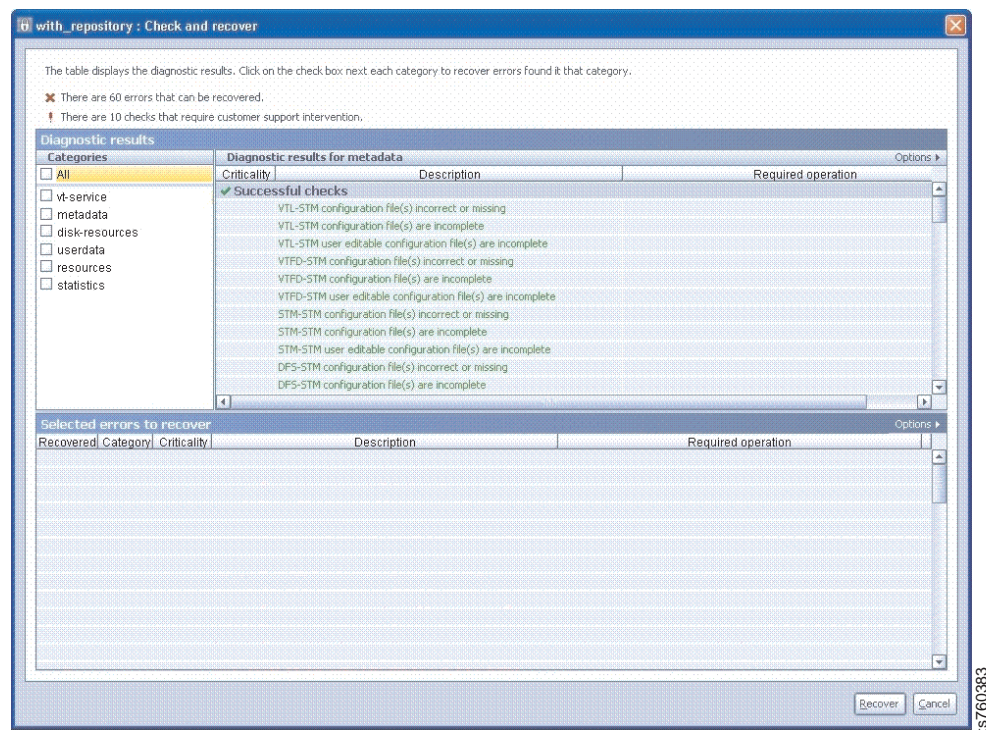
Figure 84. Check and recover dialog

Results

The Diagnostic results pane displays each element of the ProtecTIER system in one of the following lists:

- **Positive checks** - no errors.
- **ProtecTIER recoverable errors** - has errors that the ProtecTIER system might be able to repair.
- **Support required errors** - has errors that cannot be repaired by the ProtecTIER system without the assistance of a trained ProtecTIER specialist.

In the **Category** subpane, filter the list contents by selecting individual categories.

Categories that contain errors of the type **ProtecTIER recoverable errors** feature an empty check box.

Repairing the system
About this task

If the checking process discovers errors of the type ProtecTIER recoverable errors, attempt to repair the errors using ProtecTIER Manager.

Attention: Make sure to allot sufficient down-time for system recovery. The recovery process is time-consuming and the ProtecTIER system goes offline for the duration of that process.

Procedure

1. In the **Categories** sub-pane, select the checkbox for each category for which you want to repair errors. All list items of the type **ProtecTIER recoverable errors** in each selected category appear in the **Selected errors to recover** pane and are labeled with a red X.

2. Click **Recover**. ProtecTIER Manager attempts to repair the errors. Errors that are successfully repaired are labeled with a green checkmark. Errors that cannot be repaired remain labeled with a red X.

   Note: For assistance with errors that cannot be repaired, contact a trained ProtecTIER specialist.

Near online check and recovery

Near online check and recovery allows you to scan your system for errors and repair them. Once the process completes, you will be able to generate a file to help locate the cartridges that might contain corrupted data.

Near online check and recovery process

Near online check and recovery consists of three stages:

Stage 1: Pre-Recover
> This stage is performed offline. All ProtecTIER structures are scanned and checked for inconsistency and data integrity. All STUs are checked to see if they are in error mode or if the DSPF is damaged.

Stage 2: Dfs_map
> This stage is performed online. During this stage RAM is preserved by postponing deletes, and the process checks for data integrity in the STUs found in error mode in the previous stage.

Stage 3: Recovery
> This stage is performed offline. Damaged STUs are rebuilt and recovered.

Checking the system with near online check and recovery

Complete this task to check the system for errors.

About this task

Perform the following steps to use near online check and recovery to check for errors:

Note: This procedure takes the ProtecTIER system offline. Before taking the system offline, you must make sure to stop all running backup jobs.

Procedure

1. Choose **System** > **Check and recover nearline** > **Check and recover on-line** as shown here.
   The **Confirm operation** menu opens.
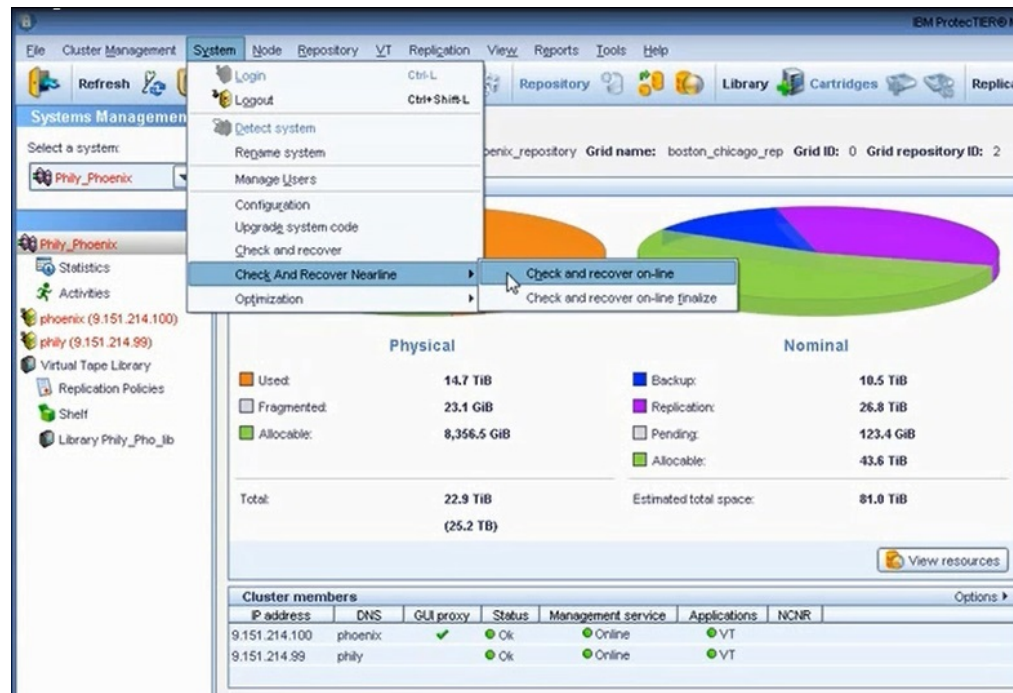
Figure 85. Starting NCNR

Figure 86. Confirm operation

2. Click **Yes**. Before taking the ProtecTIER system offline, you must make sure to stop all running backup jobs.
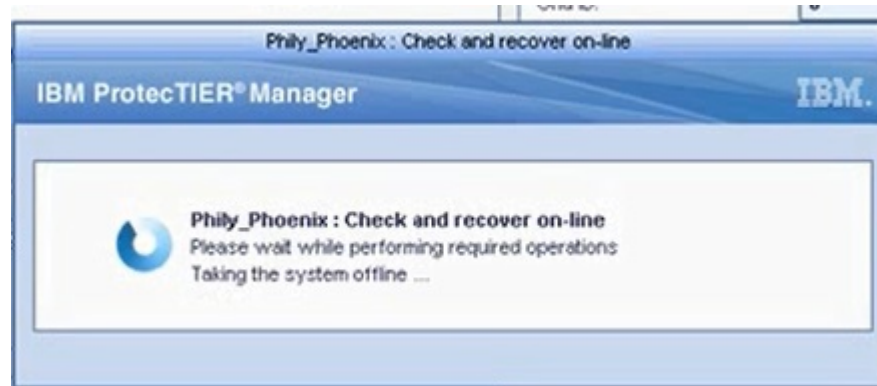
Figure 87. NCNR information status dialog

All ProtecTIER structures are scanned and checked offline.

When the scan is complete, the **Diagnostic results** screen appears.
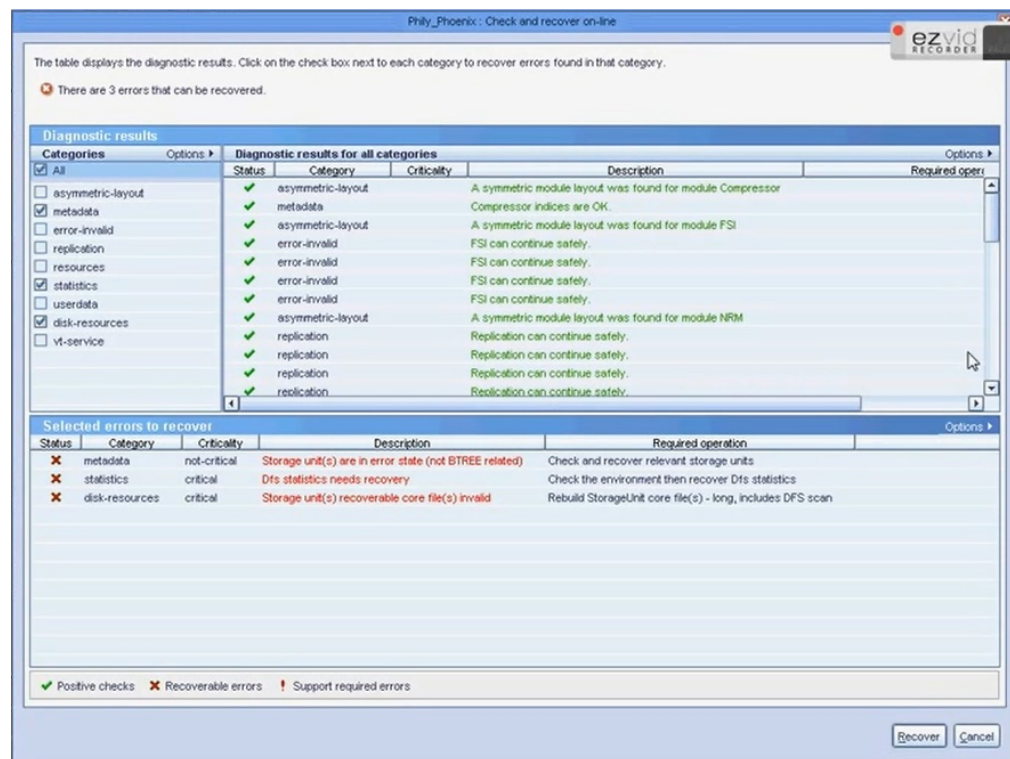
Figure 88. NCNR Diagnostic results

3. If the Diagnostics results show that errors are present, click **Recover** on the bottom right of the screen. The system prepares itself to run the scan and recovery operations. The following status message appears.

Figure 89. The near-ine stage status message

The system starts VTL. Two sections appear at the bottom of the **NCNR Status** window:

- On the **Cluster members** table a checkmark under the NCNR column indicates that a member is being checked.
- The **Check and recover on-line scan progress bar** shows the current scan status.
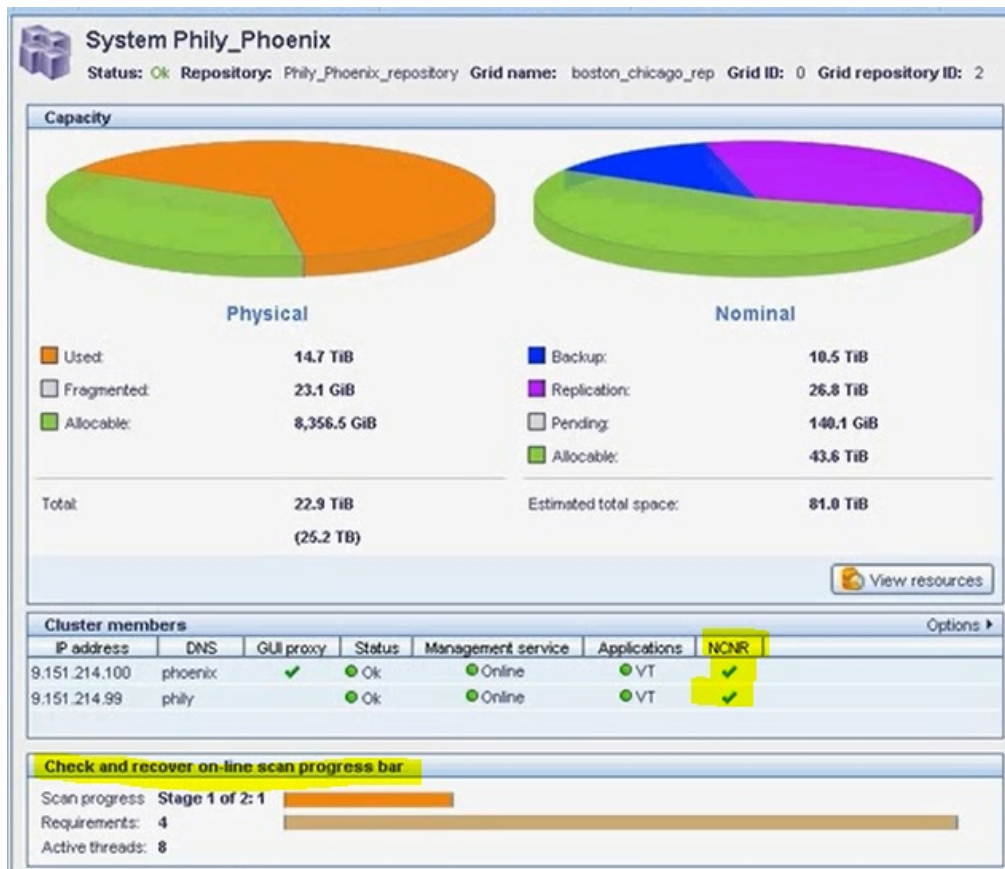
Figure 90. NCNR Status window

At this point, backups can run regularly and VTL is up and running.

Note: While the scan process continues, no deletes are permitted.

The backlog of files to be deleted increases as designed because ProtecTIER cannot delete files while DFS structures are being rebuilt and modified in background.

Any time you open or close a GUI window during this phase, a popup window shows that the system is still in check and recovery scanning mode.
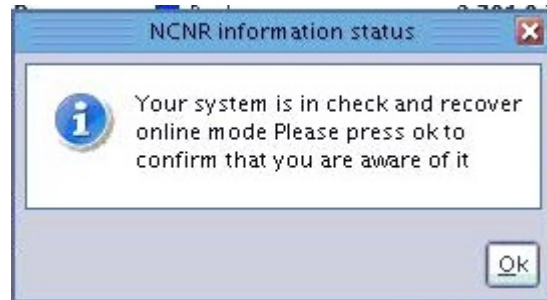
Figure 91. NCNR information status message

4. Press **Ok** to acknowledge status. When the scan is complete, a status message appears to inform you and to direct you to the next step to complete the task.
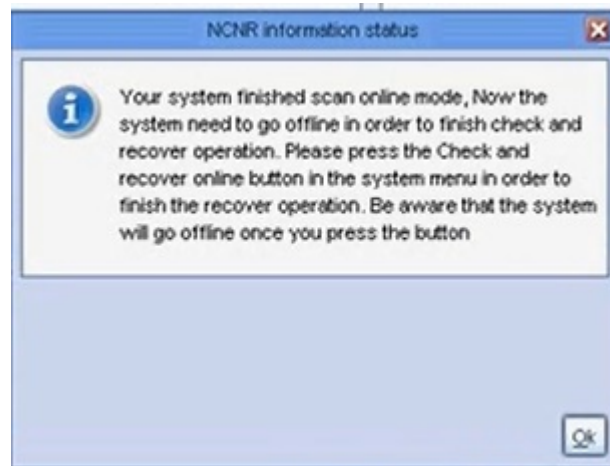
Figure 92. NCNR information status message

5. To finalize this stage, select **System** > **Check and Recover Nearline** > **Check and Recover on-line finalize**.

Note: You can decide to delay the finalize stage as long as necessary, but take under consideration the fact that deletes are not running at this stage and the delete backlog increases.
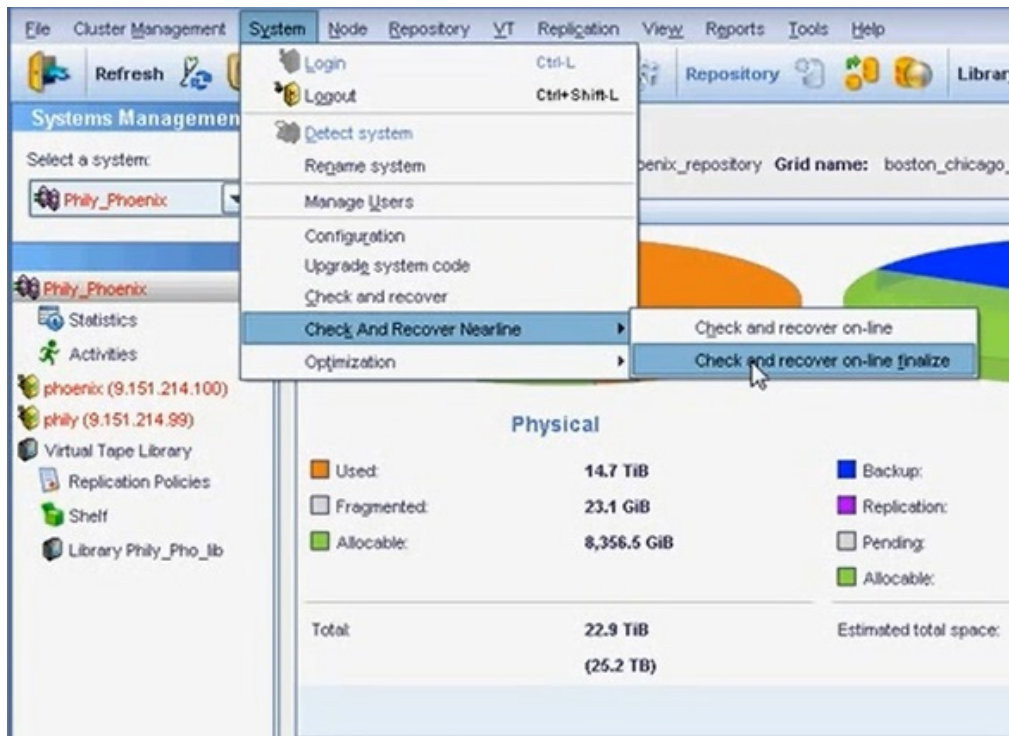
Figure 93. Finalizing the NCNR process

When you start the finalize stage, the application is stopped and the rebuilding process begins to run. The following message appears to ask for confirmation to go offline and complete the process.

Figure 94. Finalizing the NCNR process confirmation message

Results

After the finalize stage is complete, a Diagnostic result panel appears. The expected behavior is to see a "green" and error free table. If there are still errors in results panel, please contact ProtecTIER support for further analysis.

What to do next

If you receive a message about missing blocks when running the near online check and recover process, you can run the /opt/dtc/app/sbin/ scan_for_suspected_carts script to locate potentially harmed cartridges. This script can be run while the system is operational and online. The output file will contain the names of potentially harmed cartridges. To save data, use the native

| backup application to partially restore the cartridges identified. You can monitor
| the scanning progress by using: grep "DfsMapStatistics::LogStatus:"
| /pt_work/log/vtf_internal.log.

Turning on the WTI power switch outlets

This topic describes how to turn on the WTI power switch outlets.

If both cluster nodes have been powered off and their power switch outlets are off, bring the ports back to on by pressing and holding down the Default button for three seconds. All IPS power outlets will be toggled On or Off.

Modifying port attributes

This task describes how to use the ProtecTIER Manager software to modify a port attribute.

Procedure

1. From the **Systems Management** view, select the node where you want to change the port attributes from the navigation pane.
2. Choose **Nodes > Port attributes**. The **Port attributes** wizard **Welcome** screen is displayed.
3. Click **Next**. The **Port Details** screen is displayed.
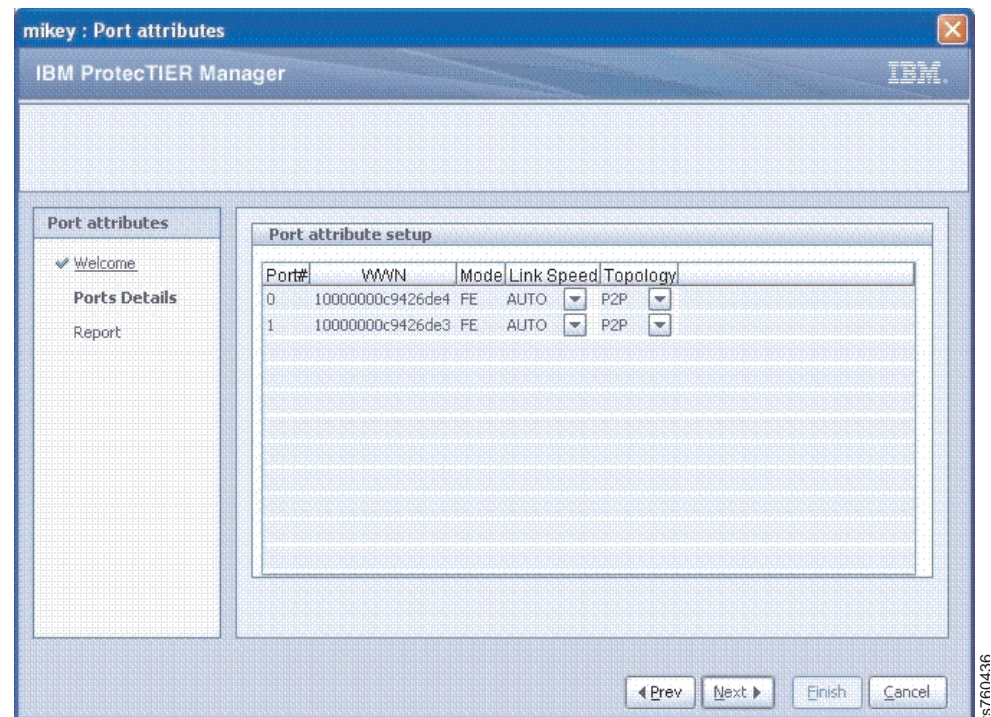
Figure 95. Port Details screen

4. In the **Link speed** column, click the Down Arrow key to select a link speed from the dropdown list. The options are as follows:
   - Auto
   - 1 GB
   - 2 GB

- 4 GB
- 8 GB

5. In the **Topology** column, click the Down Arrow key to select a network topology from the drop-down list. The options are as follows:

Loop   Fibre channel-arbitrated loop

P2P   Point-to-point

Important: When modifying the front-end connectivity, it is recommended that **Loop** topology is used for direct connection and **P2P** when Fibre Channel switches are being used. If the topology is set to **Loop** in a Fibre Channel switch connection, the link goes down.

6. Click **Next** and **Finish**. The new port attributes are set.

Removing and adding cluster members

The topics in this section describe how to remove or add cluster members.

In some troubleshooting scenarios, such as deleting a ProtecTIER repository, you may be asked to remove one of the nodes from a two-node cluster, and later add it back.

If you have a two-node cluster, you first need to remove one of the cluster members before deleting the repository. After you delete the repository and create a new repository in its place, add the cluster member back.

Removing a cluster member

Complete this task to remove a cluster member.

About this task

You can only remove a node from a cluster if the ProtecTIER service on the node is down. If there is only one node in the cluster, that node cannot be removed from the cluster. If you remove a node on which VT service devices are assigned, the devices remain offline and unassigned until they are assigned to an active cluster member node. If there are cartridges loaded into drives on that node, the cartridges are automatically unloaded.

Attention: If you want to remove a cluster member to which tape drives are assigned, it is recommended that you first reassign the tape drives. Nodes that have robots assigned to them cannot be removed from a cluster until the robot is reassigned. For more information, see "Reassigning devices" on page 95.

Procedure

1. From the Systems Management view, select a system from the dropdown list.
2. Select the node that you want to remove from its cluster and choose **Node > Server > Stop server**. You are prompted to enter your username and password.
3. Enter your username and password and click **Ok**. The ProtecTIER service stops for the selected node and you are automatically logged out.
4. In the **Navigation** pane, select a cluster.
5. Click **Login**. You are prompted for your username and password.
6. Enter your username and password and click **Ok**. You are logged in.

7. Verify that the selected node is offline.

8. Choose **Cluster Management > Remove cluster member**. The **Remove cluster member** wizard **Welcome** screen is displayed.

9. Click **Next**. The **Node selection** screen is displayed.
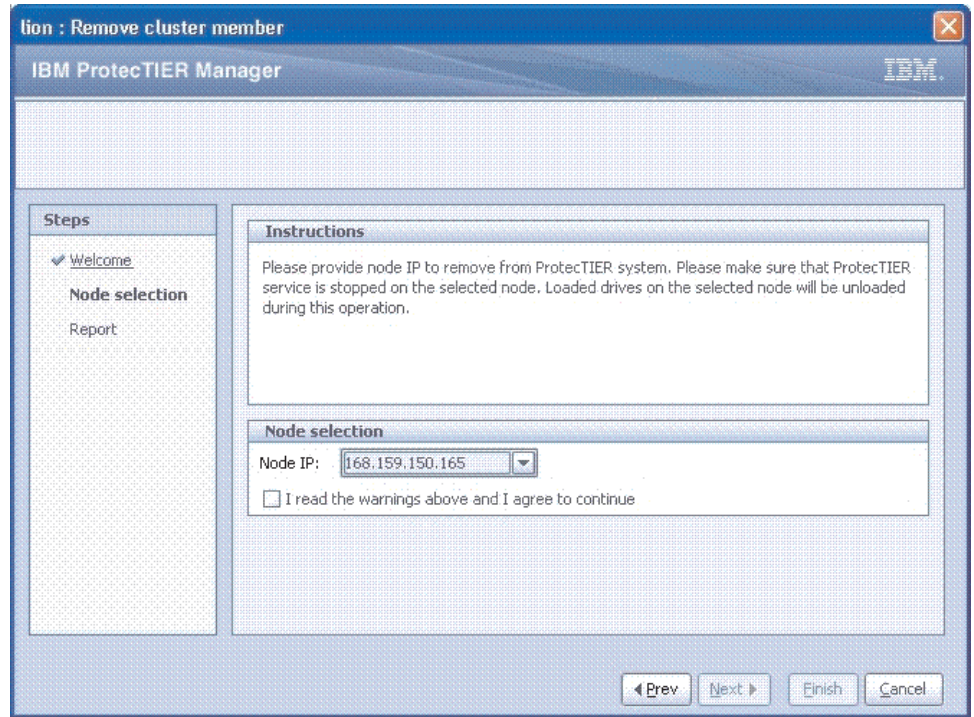
Figure 96. Node Selection screen

10. In the **Node IP** field, select the node that you want to remove from the cluster.

11. Read the instructions and select the **I read the warnings above and I agree to continue** checkbox.

12. Click **Next** and **Finish**. The **Remove cluster member** wizard closes and the selected node is removed from the cluster.

Adding a cluster member

Complete this task to add a cluster member back into a two-node cluster.

About this task

The need for this action becomes necessary when you are asked to remove a ProtecTIER repository. You generally have to remove one of the nodes from a two-node cluster, and add it back to the cluster later.

Perform the following steps to add a cluster member into a two-node cluster.

Procedure

1. From the Systems Management view, select a cluster in the **Navigation** pane.

2. Choose **Cluster Management > Add Cluster member**. The **Add cluster member** wizard **Welcome** screen is displayed.

3. Click **Next**. The **Node Selection** screen is displayed.
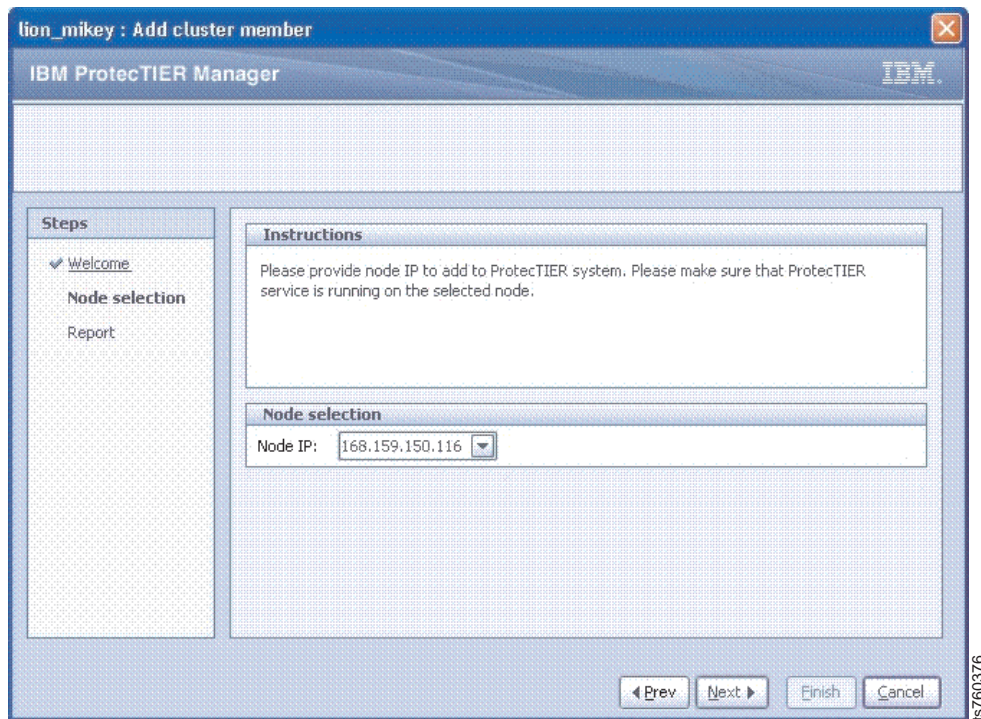
Figure 97. Node Selection screen

4. In the **Node IP** field, enter the IP address of the node associated with the cluster; or select the IP address from the dropdown list.

   Note: If the IP address you need is not in the list, you can enter the IP address you need in the input field.
5. Click **Next** and **Finish**. The **Add cluster member** wizard closes and the node is added to the selected cluster.

Part 4. System recovery procedures

This section of the guide describes the system recovery procedures.

234 IBM TS7650G Deduplication Gateway for ProtecTIER®: User's Guide for VTL Systems

Chapter 16. ProtecTIER system recovery procedures

The topics in this section provide instructions for recovering a ProtecTIER server. This procedure should be used for node replacement with the same server model in a Disaster Recovery scenario.

If you want to perform a node replacement and the server model of the new node is different from the server being replaced, contact IBM. This replacement must be ordered as an RPQ.

Note: In addition to the procedures outlined in the following topics, the TS7650G 3958 DD6 provides the new Operating System (OS) Recovery feature. This feature adds redundancy to the ProtecTIER server by enabling it to create *images* of its current configuration. These can be used to reduce the time needed to recover a server from a catastrophic failure. For information about using OS Recovery, see the *IBM ProtecTIER Implementation and Best Practices Guide*, publication SG24-8025-03 available on the following Web site:

http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/
sg248025.html?Open.

The recovery process described in these topics define the customer responsibilities and includes the following procedures:

1. Preparing to reload a node
2. Installing the Red Hat Enterprise Linux Advanced Platform operating system v5.11
3. Installing the ProtecTIER code v3.4
4. Recovering a server for use with the TS7650G.
5. Activating ProtecTIER Replication Manager (if the Replication Manager was originally installed on the designated server before node replacement)
6. Backing up the configuration files
7. Analyzing and restoring the replication manager

Preparing to reload a node

Complete this task to prepare to reload a node as part of the system recovery process.

About this task

To reload a node, you must first install the Red Hat Enterprise Linux Server release 5.6. If this is a single node server that is being recovered, proceed to "Installing Red Hat Linux version 5.11 and ProtecTIER version 3.4.1" on page 236.

If the node you are recovering is still running, perform the following steps to prepare to reload the node:

Procedure

1. Ensure a connection is established for the Baseboard Management Controller (BMC).

2. Login to the local console. At the login prompt, log in with the ID `root` and the password `admin`. The ProtecTIER System menu is displayed:

3. From the main menu, select the **Manage ProtecTIER services (...)** option. Type the corresponding number and press **<Enter>**. The **Manage ProtecTIER services (...)** is displayed:

```
------------------------------------------------------------------------
 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?
```

4. Select the **Reboot This Node** option. Type the corresponding number and press**<Enter>**.

   Rebooting the node will avoid any possibility of corrupting meta data on the repository's management file system, in case the recognition procedure encounters unexpected issues.

5. Proceed to "Installing Red Hat Linux version 5.11 and ProtecTIER version 3.4.1."

Installing Red Hat Linux version 5.11 and ProtecTIER version 3.4.1

This task is part of the recovery process. Complete this task to install Red Hat Linux version 5.11 and ProtecTIER version 3.4.1 on the server that you are reloading.

Procedure

1. Power on the server if it is not already powered on.

2. Insert the *IBM ProtecTIER Maintenance and Recovery Disk* into the DVD/CD-ROM drive on the server.

TS7610 / TS7620
TS7650 / TS7650G
IBM System Storage®ProtecTIER®
Maintenance & Recovery Disk
for 3958-AP1/DDx & 3959-SM1/SM2

Engineering-RHEL5.6-NoQlgLpfc-SMB-PT-7.05-x86_64-DTC.iso

3. Reboot the server by entering in the following command at the command line: `reboot`.

   a. To boot from the *IBM ProtecTIER Maintenance and Recovery Disk* , during the start-up sequence, press the **F12** key when the IBM logo screen appears.

   b. Select the CD/DVD ROM drive as the Boot Device. After the selection is made, it will boot from the specified device.
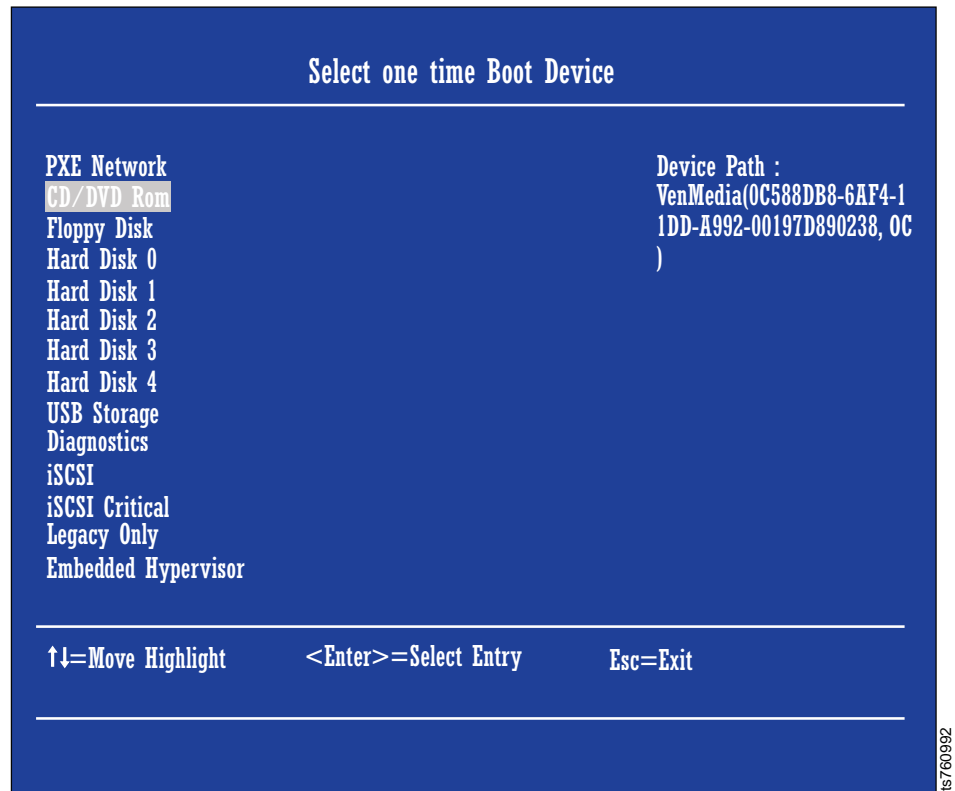
4. After a few minutes, the Red Hat Linux version 5.11 splash screen opens. At the text prompt at the bottom of the screen, there are options for **install** or **upgrade**.

5. Type **1** to select the **Install** option.
6. Type **yes** to confirm the installation and press Enter to view the license agreement.

7. Press **Enter** to read the next page, repeating until you reach the end of the license agreement.

8. When prompted to accept the software license agreement, type **yes** and press **Enter** to continue.

9. The installation begins. The installation takes approximately 30 minutes to complete.

Figure 98. Red Hat Linux Installation Progress Screen

10. The server restarts automatically at the end of the installation process. Manually eject and remove the *IBM ProtecTIER Maintenance and Recovery Disk* from the DVD drive during the restart.

    Note: If you do not remove the disk during the reboot cycle, it will attempt to boot to the Recovery DVD again, and as long as no option (1.install or 2.upgrade) is selected, it will time out and boot to the hard drives in the server that were just reloaded.

11. Proceed with one of the following options:
    - If you are working in a single node configuration, continue to step 12 on page 239.
    - If you are working in a clustered configuration and performing a recovery on Server A, you must stop the ProtecTIER services on Server B. Continue to substep **a** to stop the services on Server B.
    - If you are working in a clustered configuration and performing a recovery on Server B, you must stop the ProtecTIER services on Server A. Continue to substep **a** to stop the services on Server A.
    a. Connect a USB keyboard and monitor to Server B. Or, use the KVM if a TSSC and KVM are installed in the frame. If you are using the KVM, press the PrtSc key and select Server B.

b. Log in to the active server. At the **login:** prompt, log in with the ID root and the password admin.

c. Stop the services on the active server. Type menu <enter> on the command line and continue to substep **d**.

d. The 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?
```

e. Select **Manage ProtecTIER services (...).**

f. The **Manage ProtecTIER services** menu is displayed.

```
--------------------------------------------------------------------------
  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?
```

g. Select **Reboot This Node**.

h. After the server has been rebooted, log out of the active server and continue with the next step on the server to be recovered.

12. At the **login:** prompt, log in with the ID **ptconfig** and the password **ptconfig**.

13. The slim version of the ProtecTIER Service menu is displayed.
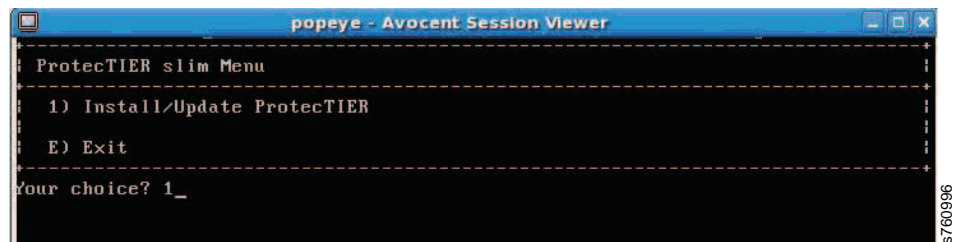
14. Type the number for the option to **Install/Update ProtecTIER** and press **Enter**.

15. The system displays the following message:

```
Locating the CDROM device...done

Place the ProtecTIER code disc in the DVD tray, close the tray
and press <enter>.
```

16. Insert the DVD that contains the file PT_TS7650G_v3.4.1.0.x.x86_64.tar or PT_TS7650_AP1_v3.4.1.0.x.x86_64.tar into the server CD/DVD drive and press **Enter**. The system displays the following message:

```
Mounting... done
Extracting the code package...
```

17. Press Enter. The system shows the following message:

```
Copying files...
Copied.... 100% Done
Please remove the disc from the drive, and press <enter> to continue.
```

   Note: This process will take about 7 minutes to complete. The progress is displayed until it reaches 100%, as shown in the example message.

18. After the operation is done, follow the instructions and remove the disk from the CD/DVD-ROM drive.

19. Press **Enter** to continue. The ProtecTIER code installation begins.

20. When the ProtecTIER installation is complete, the process will restart the cluster services. It may take several minutes, or longer. You are prompted to restart the server. Press Enter to restart.

21. When the reboot completes, the login: prompt is shown. Verify the Microcode version on the server by using the ProtecTIER Service menu.

   a. At the **login:** prompt, log in with the ID **ptconfig** and the password **ptconfig**.

   b. The 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?
```

   c. From the main menu, select **Version information**.

   d. The **Version information** menu is displayed.

```
   -------------------------------------------------------------------------
     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?
```

e. Select **Display version information**. The ProtecTIER version is shown in the first line of output, in the first three digits after the colon. The version information looks similar to the following message:

```
PT version : 3.4.1
```

If the ProtecTIER version is correct, continue to the next step. If the ProtecTIER version is incorrect, the installation has failed. Contact IBM Support for assistance.

Results

The re-installation process for Red Hat Linux version 5.11 and ProtecTIER version 3.4.1 is complete. Proceed to "Recovering the configuration of a replaced server."

Recovering the configuration of a replaced server

Complete this task to recover the configuration of a replaced server as part of the recovery process.

Procedure

1. After the system boots up from installing the ProtecTIER package, type **ptconfig** at the `login as:` prompt and **ptconfig** at the **password:** prompt. The 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?
```

2. From the ProtecTIER Service Menu, select **ProtecTIER Configuration (...)**. Type the corresponding number and press **<Enter>**. The **ProtecTIER Configuration (...)** menu is displayed:

```
 -------------------------------------------------------------------------------
  ProtecTIER Service Menu running on rassmx
            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
  15) OS images Management (...)

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

3. Select the `Recover Configuration for a replaced server` option. Type the corresponding number and press `<Enter>`.

   The server type and application are automatically detected where `Application` is `VTL` if replacing a VTL server.

4. On a TS7650G, the following sample output is displayed:

```
Begin Processing Procedure


About to execute:
Operation:    replace
Model:        TS7650G
Application:  VTL

Continue? (yes|no) yes
```

5. Type **yes** to continue.

   Note: When prompted to select the node to be replaced, enter the proper node option number. This is especially important when replacing a 2-node system when both nodes are down. Only the valid options for replacement are displayed, i.e. if one of the nodes is running and accessible, only the option of replacing the node that is **not** running is displayed. Meaning, the system will identify the components installed, and make a determination of the model you are trying to recover.
   The following sample output is displayed:

```
Stopping services, please wait
Stopping Cluster Services                                    [ Done ]
Services stopped
Checking BOM                                                 [ Done ]
Checking for existing nodes                                  [ Done ]
Comparing mapped devices                                     [ Done ]
Checking Application Interfaces                              [ Done ]
NOTICE: In order to continue the ProtecTIER Services must be stopped on the other node.
Would you like To Stop the ProtecTIER services on the other node?
```

6. Type **yes**. The following sample output is displayed:

```
Checking repository                                          [ Done ]
Checking installed applications                              [ Done ]
Checking installed applications                              [ Done ]
Checking local raid                                          [ Done ]
Checking conditions done

Checking live nodes                                          [ Done ]
```

7. The procedure will prompt you to enter the option of the server you are
   recovering. Enter the option number and press **<Enter>**.

   Note: During the server replacement procedure, you may be prompted to
   perform a fence test on the nodes. Type yes to accept any prompts to perform
   the fence test.
   The following sample output is displayed:

```
Model <TS7650_DS4700_128_450>

Option 1
**************************************************
        node id   : 2
        hostname  : pinsk
        ip        : 9.148.220.155
Select option: 1
Recoverable static routes configuration found, would you like to restore it?
(yes|no) yes
Recovering Static Routes [ Done ]
Configuring network                                      [ Done ]
Configuring Replication Network                          [ Done ]
Restarting Network Service                               [ Done ]
Stopping Remote VTFD                                     [ Done ]
Stopping Remote RAS                                      [ Done ]
Stopping cluster                                         [ Done ]
Configuring cluster                                      [ Done ]
Starting cluster                                         [ Done ]
Installing NTP                                           [ Done ]
Mounting file systems                                    [ Done ]
Restoring node ID                                        [ Done ]
Starting VTFD locally                                    [ Done ]
Starting RAS                                             [ Done ]
Starting VTFD remotely                                   [ Done ]
Starting RAS remotely                                    [ Done ]
Checking RAS Configuration                               [ Done ]
Restoring RAS Configuration                              [ Done ]
Collecting RAS Persistent configuration                  [ Done ]
Running RAS Eth Agent                                    [ Done ]
validation will start in 10 seconds
Testing customer network connectivity                    [ Done ]
Testing connectivity to the Default Gateway              [ Done ]
Getting number of nodes                                  [ Done ]
Testing NTP configuration                                [ Done ]
Testing cluster's network speed                          [ Done ]
replace ended successfully

End Processing Procedure Successfully

Press <ENTER> to continue
```

8. Press **<Enter>** to continue. The replacement procedure will restore the configuration files from the server's repository, and this will take several minutes to complete.
9. Once the information has been provided, proceed to "Activating ProtecTIER Replication Manager" on page 248.

Replacing a two-node system with a single node configuration for disk-base replication

Complete this task, when you are using disk-based replication, to recover a server that was part of a two-node system and configure it as a single node.

Before you begin

Note: This procedure should **not** be run on a system using Native Replication.

Before you begin, ensure that the WTI fence device is disconnected from the network.

About this task

This task is done when you have a cluster at the local site with a single node system at the remote site. This command should only be used when you are replacing a two-node system with a single node system that will **not** be upgraded to a two-node cluster. In such a scenario, the single node will fail to start after the replacement, since there is no connection to a WTI fence device. Adding a second node to this single node system may cause data corruption, as the fence device will not be used.

The command's syntax is:

`./ptconfig -replace -app=<app> -model=<model> -dualBySingle`

where **<app>** is **VTL** if replacing a VTL server, and **<model>** is the ProtecTIER server model.

To replace a two-node system by a single node when using disk-based replication:

Procedure

1. Connect or verify a USB keyboard and display are connected to the ProtecTIER server.
2. Follow the procedure for "Installing Red Hat Linux version 5.11 and ProtecTIER version 3.4.1" on page 236. Wait for the system to boot up and continue to step 3.
3. From the login prompt, login with user ID **root** and password **admin**.
4. Change the directories to the /opt/dtc/install directory. From the command line, type the following command:

   `cd /opt/dtc/install     <Enter>`
5. From the /opt/dtc/install directory, type the following command:

   `./ptconfig -replace -app=VTL -model=TS7650G -dualBySingle     <Enter>`

   The following sample output is displayed:

   Example

```
By selecting the dualBySingle option you are converting this node.
Once this action is complete this installed node must NEVER be a part of a
2 node Cluster.
Step Converting to dual by single                          - started
Step Converting to dual by single                          - done
Stopping services, please wait
Step Stopping Cluster Services                             - started
Step Stopping Cluster Services                             - done
Services stopped
Screen started - Tue Feb 28 22:11:49 2012
Step Checking BOM                                         - started
Step Checking BOM                                         - done
Step Checking for existing nodes                          - started
Step Checking for existing nodes                          - done
Step Checking Application Interfaces                      - started
Step Checking Application Interfaces                      - done
Step Checking repository                                  - started
Step Checking repository                                  - done
Step Checking installed applications                      - started
Step Checking installed applications                      - done
Step Checking local raid                                  - started
Step Checking local raid                                  - done
Checking conditions done

Step Checking live nodes                                  - started
Step Checking live nodes                                  - done
Model <TS7650_DS4700_128_450>

Option 1
*************************************************
 node id   : 1
 hostname  : kokomo
 ip        : 9.11.200.174

Option 2
*************************************************
 node id   : 2
 hostname  : auburn
 ip        : 9.11.200.173
Question: Select option:
```

6. The procedure will prompt you to enter the option of the server you are
   replacing. Enter the option number and press <Enter>. The following sample
   output is displayed:

```
Answer: 1
Step Configuring Application Interfaces              - started
Step Configuring Application Interfaces              - done
Step Configuring network                            - started
Step Configuring network                            - done
Step Restarting Network Service                     - started
Step Restarting Network Service                     - done
Step Stopping cluster                               - started
Step Stopping cluster                               - done
Step Configuring cluster                            - started
Step Configuring cluster                            - done
Step Starting cluster                               - started
Step Starting cluster                               - done
Step Installing NTP                                 - started
Step Installing NTP                                 - done
Step Set interfaces addresses                       - started
Step Set interfaces addresses                       - done
Step Mounting file systems                          - started
Step Mounting file systems                          - done
Step Restoring node ID                              - started
Step Restoring node ID                              - done
Step Starting VTFD                                  - started
Step Starting VTFD                                  - done
Step Checking RAS Configuration                     - started
Step Checking RAS Configuration                     - done
Step Restoring RAS Configuration                    - started
Step Restoring RAS Configuration                    - done
Step Collecting RAS Persistent configuration        - started
Step Collecting RAS Persistent configuration        - done
Step Running RAS Eth Agent                          - started
Step Running RAS Eth Agent                          - done
validation will start in 10 seconds
Step Testing customer network connectivity          - started
Step Testing customer network connectivity          - done
Step Testing connectivity to the Default Gateway    - started
Step Testing connectivity to the Default Gateway    - done
Step Getting number of nodes                        - started
Step Getting number of nodes                        - done
This is a 1 node cluster, will not test fencing
validation ended
replace ended successfully
```

Note: Once the configuration is complete, a validation procedure runs automatically. Even if, for some reason, the validation fails, the procedure is not rolled back since the configuration completed successfully.

What to do next

Go on to "Installing the ProtecTIER Manager software" on page 29.

Activating, analyzing and restoring ProtecTIER Replication Manager

This section describes the procedure for activating, analyzing and restoring an inactive or "lost" ProtecTIER Replication Manager server using ProtecTIER Manager.

The ProtecTIER Replication Manager restore procedure is done grid by grid and can be done in either of the following ways:

- Using an existing backup file:

  PtReplicationManager_**<hostName>_<customerName>_time**_ConfigurationBackup.zip

- Using an accessible repository that was once a member of a grid.

Important: Use the most updated file determined by the newest **time** value.

Go on to "Activating ProtecTIER Replication Manager."

Backing up the configuration files

The ProtecTIER Replication Manager configuration files are automatically backed up and saved by default. However, you can choose to cancel the automatic configuration file backups and perform the operation manually. The following task explains how to manually back up the Replication Manager configuration files.

About this task

Backups of the configuration files from ProtecTIER Replication Manager are saved as a .zip file.

Automatic backups can be cancelled by deselecting the **Backup configuration files** checkbox found on the **Backup** tab under the **Tools > Preferences** window in the **Grids Management** view.

From the Preferences window, you can also specify the number of backup files to save (the default is 20). The backup is done by rotation on the saved files. For instance, the backup files are named consecutively from `gm_backup.0` to `gm_backup.20`. When a new backup is generated, `gm_backup.0` is renamed to `gm_backup.1` and the new backup is saved as `gm_backup.0`. This continues until the backups reach the total number saved and the old backups are deleted.

To manually back up the configuration files:

Procedure

1. From the Grids Management view, select **Replication Manager > Backup configuration files**. The **Backup configuration files** dialog is displayed.
2. Enter the customer name in the **Customer name** field for which to provide backup information and click Ok. A message is displayed that the backup .zip file was saved on the ProtecTIER Replication Manager server in the `/tmp` directory.
3. Click **Yes** if you want to download the backup file to a specific directory or **No** to close the window.
4. If **Yes**, browse to the directory in which you want to save the backup configuration file and click **Save**. The file is saved to the respective directory and the **Save** window closes.

Activating ProtecTIER Replication Manager

Use this procedure to reactivate the ProtecTIER Replication Manager application on a replaced server in your replication grid in a disaster recovery scenario. This procedure should only be used if the Replication Manager was originally installed on the designated server before node replacement and if there is no Replication Manager running on any other node in the replication grid.

About this task

The Replication Manager should be activated on the server that remotely manages the replication grid or grids within an organization. IBM recommends activating the ProtecTIER Replication Manager on the target server at the remote (destination) site. By doing so, the Replication Manager remains available in a disaster recovery situation.

This task might be completed at any time during the replication configuration process. However, creation of the replication grid and verification of the replication configuration, cannot take place until ProtecTIER Replication Manager is up and running on the designated server.

Procedure

1. If it is not already displayed, access the ProtecTIER System menu on the designated ProtecTIER Replication Manager server. See "Accessing the ProtecTIER Service menu" on page 9.

2. From the main menu, select **ProtecTIER Configuration (...)**. Type the corresponding number and press **<Enter>**. The **ProtecTIER Configuration (...)** menu is displayed.

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
             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
 15) OS images Management (...)

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

3. Select **Configure replication (...)** . Type the corresponding number and press **<Enter>**. The **Configure replication (...)** menu is displayed.

```
------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
             ProtecTIER Configuration (...)
             Configure Replication (...)
------------------------------------------------------------------------
   1) Config/Unconfig ProtecTIER Replication Manager on this node
   2) Configure Static Routes

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

4. Select **Configure/Unconfigure ProtecTIER Replication Manager on this node**. Type the corresponding number and press **<Enter>**.

5. When the **Replication Manager is currently unconfigured, do you wish to configure it? (yes|no)** prompt displays, type: **yes <Enter>**.

   The system displays the following warning displays:

   Warning: You should not configure Replication Manager on more than one server in a grid, as doing so may cause conflicts within the grid. It is recommended that you designate the Target server (Hub) as the Replication Manager.

6. When the `Are you sure you want to configure the ProtecTIER Replication Manager on this node? (yes|no)` prompt displays, type: **yes <Enter>**.

   The system displays the following message:

   `Gathering information [ Done ]`

   The `"activatePTReplicationManager ended successfully"` message displays.

7. When the `Press the ENTER key to continue...` prompt displays, press **<Enter>**. You are returned to the **Configure replication (...)** menu.

8. Type **E** and press **<Enter>** to exit.

9. After configuring ProtecTIER Replication Manager, you must restore the replication grid using the **Restore grid** procedure. Go on to "Restoring the ProtecTIER Replication Manager."

Restoring the ProtecTIER Replication Manager

The following tasks describe the different methods for restoring the processed grid using the **Restore grid** procedure.

The ProtecTIER Replication Manager server automatically handles *grid analysis*. Grid analysis validates and checks the integrity of the grid in relation to its grid members. To begin restoring a grid, import a grid for analysis by selecting one of the tabs appearing on the **Restore grid** window:

- File (see "The File tab")
- IP Address (see "The IP Address tab" on page 251)

The File tab

The following task describes how to restore the Replication Manager from the **File** tab.

About this task

If you are restoring a grid from a backup `.zip` file, follow the steps below to import a grid for analysis and restore:

Procedure

1. Select the **Restore grid** option from the **Replication Manager** menu. The **Restore grid** dialog is displayed.

2. Select the **File** tab.

3. Browse to the backup filename from which you want to analyze and restore the grid, or enter a filename in the **Backup .ZIP file name** field.

4. Click **Read file**.

5. Select a grid to analyze from the dropdown list. The grid analysis is displayed.

6. Click **Restore**. The current grid is restored and removed from the grid analysis list.

7. Select the next grid for analysis from the dropdown list. Continue restoring, grid by grid, until the entire Replication Manager is restored.

What to do next

If there are inconsistencies and ProtecTIER Replication Manager does not recognize the repository as part of the grid, proceed with "Forcing a repository to leave a grid" on page 251.

If the **Restore grid** procedure was successfully completed, proceed to "Working with ProtecTIER Replication Manager" on page 115.

The IP Address tab

The following task describes how to restore a grid from the Replication IP address of a repository from the **IP Address** tab.

About this task

If you search for a backup file and cannot find one, then you can restore a grid on which the repository was previously a member. With a given replication IP address, the analysis phase is done with the respective repository's grid data in relation to the other grid members.

Follow the steps below to import a grid for analysis and restore:

Procedure

1. Select the **Restore grid** option from the **Replication Manager** menu. The **Restore grid** dialog is displayed.
2. Select the **IP Address** tab.
3. Enter the **Replication IP address** of the accessible repository that was previously a member of the grid.
4. Click **Analyze grid**. The grid analysis is displayed.
5. Click **Restore**. The current grid is restored.

What to do next

If there are inconsistencies and ProtecTIER Replication Manager does not recognize the repository as part of the grid, proceed with "Forcing a repository to leave a grid."

If the **Restore grid** procedure was successfully completed, proceed to "Working with ProtecTIER Replication Manager" on page 115.

Forcing a repository to leave a grid

Complete this task to force a repository to leave a grid.

About this task

Important: Do not perform this procedure without instruction from a trained ProtecTIER specialist.

Note: A repository can be removed from a replication grid without the "cooperation" of the repository. However, it is preferable to remove a repository from a grid with coordination between the two. A temporary network disconnection between the replication manager and the repository is not enough reason for forcing a repository from a grid.

Force a repository to leave a grid **only** if the repository has been destroyed and should not be part of the grid or is inconsistent with the grid. This situation might arise if the Replication Manager was permanently destroyed, or if the repository was removed from the grid without coordination due to temporary network disconnection.

For example, if the Replication Manager was installed on a Target repository which was destroyed, the replication grid can be restored from a Source repository that was a member of the now destroyed grid. After restore, the repository "thinks" it is part of the grid, but the Replication Manager might not recognize the repository as part of the grid. The repository will, therefore, be marked as *inconsistent* and must be forcibly removed from the replication grid via the Grids Management view.

Procedure

From the Grids Management view, select **Repository > Uncoordinated repository removal** to forcibly remove a repository from a grid.

Note:

If this procedure is being performed in a Disaster Recovery (DR) mode scenario, the repository can be forcibly removed from the grid from the Systems Management view. Select **Replication > Uncoordinated repository removal from grid**.

For more information, see Chapter 12, "Disaster recovery (DR) mode operations," on page 169.

What to do next

Once the repository has been removed from the replication grid, add the new repository to the replication grid. Go to "Adding a repository to a replication grid" on page 118 and "Replacing a destroyed VTL repository " on page 172.

Part 5. Appendixes

Appendix A. Remote access with IBM Endpoint Manager for Remote Control through Assist-on-Site (AOS)

AOS is the preferred remote assistance tool that support engineers can use to connect to, view, and control client systems. AOS enables IBM support representatives to remotely takeover the client's endpoint quickly and resolve problems collaboratively.

AOS terminology

The following terminology is commonly used with IBM Remote Assistance, AOS.

Console Support engineer interface
provides a login point, utilities toolbar, help, configuration and connection options.

Client Customer interface
entry point into client, which manifests itself as the ibmaos process.

Relay geographically based server selected by a customer when he or she initiates the connection or by support on the HTTP link form. It is also the connection point between the client and the console and comprises AOS.war file.

Controller
Entry point for the console to authenticate support credentials, and create or join a session. It consists of the Admin.war and AOS.war files. The two URLs used for the controllers are us.ihost.ibm.com and uk.ihost.ibm.com.

AOS in ProtecTIER (SM2 and DD6)

Although AOS offers several different connection options, only Port Forwarding (the default) is available with the SM2 and DD6. Port Forwarding creates a tunnel connection to a specific port (port 22 ssh) in the server.

To access the AOS menu, select **Problem Alerting (...)** from the ProtecTIER service menu, then select **Manage Assist On Site service (...).**

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on vela
 Problem Alerting (...)
 Manage Assist On Site service (...)
--------------------------------------------------------------------------------
  1) Start the AOS (ibmtrct) service
  2) Stop the AOS (ibmtrct) service
  3) Configure the AOS (ibmtrct) service
  4) Get status of the AOS (ibmtrct) service
  5) Enable the AOS (ibmtrct) service
  6) Disable the AOS (ibmtrct) service
  7) Test Connectivity of AOS service

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

The options available on the AOS Main Menu include:

Start the AOS (ibmtrct) service :
> This option issues the **service ibmtrct start** command. This causes the AOS daemon to be executed by RedHat in order to be able to receive incoming connection requests. If AOS daemon is not running, then there is no possibility of having remote access for support.

Stop the AOS (ibmtrct) service
> This option issues the **service ibmtrct stop** command that terminates the AOS daemon. No further remote connections are supported. This is the default state of the AOS daemon unless it's **Enabled** (see option 5 of this menu)

Configure the AOS (ibmtrct) service
> This option allows you to modify the AOS configuration file and add the necessary values to configure it in **lights out mode** with port 22 exported only. Use this option whenever a change such as a new host name, customer name or customer number is made in the system. The file that gets affected is located under `/var/opt/ibm/trc/target/profiles/lightsoutprofile.properties`.

Get status of the AOS (ibmtrct) service
> This option issues the **service ibmtrct status** command which displays the output on the screen.

Enable the AOS (ibmtrct) service
> This option issues the **chkconfig ibmtrct on** command which configures the AOS daemon to be executed automatically after every reboot. This option will NOT start the daemon in case it's stopped, so the status of the daemon should be checked with option 4 of this menu and started if needed with option 1 of this daemon.

Disable the AOS (ibmtrct) service
> This option issues the **chkconfig ibmtrct off** command, which configures the AOS daemon so that it does not to get started automatically after every reboot. This option does NOT stop the daemon in case it's stopped, so the status of the daemon should be checked with option 4 of this menu and started if needed with option 2 of this daemon.

Test Connectivity of AOS service
> This option tries to connect to a known internet DNS (8.8.8.8) and then to the AOS broker as defined in the `/etc/hosts` file. If both connection attempts succeed, the test passes, otherwise it fails.

Appendix B. 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 TS7650G 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"
* "Call Home through the TSSC" on page 259

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 48 presents the capabilities of remote support with an ECC.

Table 48. 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

Call Home through the TSSC

The TSSC is a service tool that **must** be present in an IBM-supported 3958 DD4 or 3958 DD5 TS7650G server. You can either order a TSSC with your gateway, or use a TSSC already installed at your site.

Note: Please note that TSSC with the Call Home feature is not available on the 3958 DD6 server; Call Home is supported for 3958 DD6 using native call home tools provided in the ProtecTIER software.

Attention: While it is possible to operate a 3958 DD4 or 3958 DD5 without a connected TSSC, note that IBM **does not support** this configuration.

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.

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.

Table 49 presents the capabilities of remote support with a TSSC.

Table 49. Remote support capabilities with a TSSC

Customer site	Call Home events	• Error initiated • Heartbeat (regular interval) • Test
	TSSC 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)
	TSSC and remote support service tools	• Code image broadcast • Call home event log review • End-of-call completion report
IBM support	TSSC 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

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	

Accessibility features for TS7600 family of products

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

These are the major accessibility features in the TS7600 family of products

- You can use screen-reader software and a digital speech synthesizer to hear what is displayed on the screen. HTML documents have been tested using JAWS version 15.0.
- You can operate features using the keyboard instead of the mouse.

Keyboard navigation

You can use keys or key combinations to perform operations and initiate menu actions that can also be done through mouse actions. You can navigate the TS7600 family of products information from the keyboard by using the shortcut keys for your browser or screen-reader software. See your browser or screen-reader software Help for a list of shortcut keys that it supports.

Accessing the publications

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility:

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 Sun Microsystems, Inc. in the United States, other countries, or both.

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

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

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

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

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

Electronic emission notices

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

jjieta1

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

Special characters

[] 174

A

about this document xiii
  sending comments xx
accessibility 273
Accessing the ProtecTIER Service
 menu 9
adding
  cartridges 99
  cluster members 231
  nodes 43
  nodes to a subnetwork 44
  user accounts 38
administrator
  default password 46
  role 38
alerts log 215
all systems view
  monitoring 137

B

backlog
  viewing replication backlog by
   source 149
backlog by source
  monitoring 149
Backup
  Reserve space on a repository 60
backup catalog 170
backup environment 83
backup monitoring 202, 206
Backup write graph
  repository backup statistics 145

C

cartridge
  adding 99
  deleting 100
  moving 214
  read-only mode 101
  read/write mode 101
  resynchronizing 105
  resyncing 105
  switching modes 101
  unloading 214
cartridge drive
  reassigning 95
cartridge integrity
  verifying 102
cartridge metadata
  verifying 102
Cartridge query tool 189
cartridges
  adding and removing 99

cartridges *(continued)*
  managing 99
Cartridges
  unloading and moving 214
Centralized time frame
  setting 131
Change principality
  changing cartridge ownership 102
changing
  HyperFactor mode 210
  user password 39
Changing cartridge ownership
  Principality 102
Changing support system settings 39
checking
  errors 222, 223
cluster
  cluster member monitoring, see
   cluster member 141
  disk space monitoring 139
  overview 43
  physical and nominal capacity 139
cluster member
  adding 231
  monitoring 141
  removing 230
cluster members
  adding 230
  removing 230
commands
  AddCartridges 69
  AddClusterMember 68
  AddLibrary 69
  CartridgeInfo 71
  CreateRepository 67
  DriveModels 71
  InventoryDeleteFile 76
  InventoryDeleteFilter 77
  InventoryFilter 73
  InventoryGetQueryFields 74
  InventoryMoveFile 74
  InventoryMoveFilter 75
  InventoryRefresh 73
  InventoryStatistics 75
  Libraries 71
  LibraryInformation 72
  LibraryTypes 72
  NodeVtlStatistics 70
  NumberofCartridges 72
  ptcli 67
  RaidConfigurations 68
  RepositoryStatistics 68
  ServerVersion 68
comments, sending xx
completing ProtecTIER system setup 9
compression
  disabling 210
configuration
  cluster setup 4
  one node system 4
  two node system 4

Configuration file backups 248
configuring
  ProtecTIER server 10
configuring ProtecTIER
  using ptcli 69
configuring replication
  using the ProtecTIER Service
   Menu 25
configuring static routes 11
Configuring the ProtecTIER server 10
Control path failover (CPF)
  setting CPF 98
CRC
  changing the CRC setting 179
creating
  file systems 52, 59
  increase capacity 59
  libraries 83
  performance analysis reports 197
  zones 83
creating file systems
  File systems Management 52

D

data deduplication 3
date and time
  setting 16
dedup estimator
  backup monitoring 206
deduplication 3
defragmentation
  disabling 209
Defragmentation control
  on a repository 60
deleting
  cartridges 100
  libraries 98
  repositories 62
  user accounts 38
Destination repository
  Connecting a source 120
device
  reassigning 95
  resetting 213
disabling
  compression 210
  defragmentation 209
Disaster recovery
  operations 169
  replace dual node by single 244
Disaster Recovery
  Entering DR mode 169
documentation
  improvement xx
DR mode
  See also Disaster recovery
  completing failback 174
  creating a failback policy 174
  Entering DR mode 169
  Failback policy 173

Z

IBM ®

Printed in USA