IBM Virtualization Engine for Tape TS7520

IBM

User's Guide

IBM Virtualization Engine for Tape TS7520

User's Guide

> **Note:**
> http://www.ibm.com/servers/storage/tape/resource-library.html
>
> Before using this information and the product it supports, read the information in "Notices" on page 273.

Third edition (November 2007)

This edition applies to the IBM Virtualization Engine TS7500 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

Safety and environmental notices

This section contains information about:

Safety notices and labels

When using this product, observe the danger, caution, and attention notices contained in this guide. The notices are accompanied by symbols that represent the severity of the safety condition. The danger and caution notices are listed in numerical order based on their IDs, which are displayed in parentheses, for example (D004), at the end of each notice. Use this ID to locate the translation of these danger and caution notices in the IBM® safety publication that accompanies this product. See the following examples of danger and caution notices for the location of the ID number.

The following sections define each type of safety notice and provide examples.

The following notices and statements are used in IBM documents. They are listed below in order of increasing severity of potential hazards. Follow the links for more detailed descriptions and examples of the danger, caution, and attention notices in the sections that follow.

- **Note:** These notices provide important tips, guidance, or advice.
- **"Attention notices" on page xxiii:** These notices indicate potential damage to programs, devices, or data.
- **"Caution notices" on page xxi:** These statements indicate situations that can be potentially hazardous to you.
- **"Danger notices":** These statements indicate situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these situations.
- In addition to these notices, "Safety labels" on page xix may be attached to the product to warn of potential hazards.

Danger notices

A danger notice calls attention to a situation that is potentially lethal or extremely hazardous to people. A lightning bolt symbol accompanies a danger notice to represent a dangerous electrical condition. Read and comply with the following danger notices before installing or servicing this device.

DANGER

> To prevent a possible shock from touching two surfaces with different protective ground (earth), use one hand, when possible, to connect or disconnect signal cables. (D001)

DANGER

> Overloading a branch circuit is potentially a fire hazard and a shock hazard under certain conditions. To avoid these hazards, ensure that your system electrical requirements do not exceed branch circuit protection requirements. Refer to the information that is provided with your device or the power rating label for electrical specifications. (D002)

DANGER

> If the receptacle has a metal shell, do not touch the shell until you have completed the voltage and grounding checks. Improper wiring or grounding could place dangerous voltage on the metal shell. If any of the conditions are not as described, STOP. Ensure the improper voltage or impedance conditions are corrected before proceeding. (D003)

DANGER

> An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. (D004)

A comprehensive danger notice provides instructions on how to avoid shock hazards when servicing equipment. Unless instructed otherwise, follow the procedures in the following danger notice.

DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous.

To avoid a shock hazard:
- **Connect power to this unit only with the IBM-provided power cord. Do not use the IBM-provided power cord for any other product.**
- **Do not open or service any power supply assembly.**
- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.**
- **Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.**
- **Connect any equipment that will be attached to this product to properly wired outlets.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described below when installing, moving, or opening covers on this product or attached devices.**

To Disconnect:
1. **Turn everything OFF (unless instructed otherwise).**
2. **Remove power cords from the outlet.**
3. **Remove signal cables from connectors.**
4. **Remove all cables from devices.**

To Connect:
1. **Turn everything OFF (unless instructed otherwise).**
2. **Attach all cables to devices.**
3. **Attach signal cables to connectors.**
4. **Attach power cords to outlet.**
5. **Turn device ON.**

(D005)

Safety labels

As an added precaution, safety labels are often installed directly on products or product components to warn of potential hazards. These can be either danger or caution notices, depending upon the level of the hazard.

The actual product safety labels may differ from these sample safety labels:

DANGER

Hazardous voltage, current, or energy levels are present inside any component that has this label attached. (L001)

Do not service, there are no serviceable parts.

DANGER

Frame-mounted devices are not to be used as a shelf or work space. (L002)
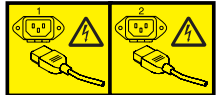
DANGER

Multiple power cords (L003)

To remove all power to the device, disconnect all power cords.

DANGER

High voltage present (L004)

CAUTION:
High energy present (L005)

>240VA

CAUTION:
Hazardous moving parts nearby (L008)

CAUTION:
Pinch point nearby

P/N 18P5850-B

SJ000752

Caution notices

A caution notice calls attention to a situation that is potentially hazardous to people because of some existing condition. A caution notice can be accompanied by different symbols, as in the examples below:

If the symbol is...	It means....
	A hazardous electrical condition with less severity than electrical danger.
	A generally hazardous condition not represented by other safety symbols.
 >55kg (121.2 lb)	A specification of product weight that requires safe lifting practices. The weight range of the product is listed below the graphic, and the wording of the caution varies, depending on the weight of the device.
	A potential hazard of pinching the hand or other body parts between parts.
	A hazardous condition due to moving parts nearby.
 Class I	A hazardous condition due to the use of a laser in the product. Laser symbols are always accompanied by the classification of the laser as defined by the U. S. Department of Health and Human Services (for example, Class I, Class II, and so forth).

Read and comply with the following caution notices before installing or servicing this device.

CAUTION:
Energy hazard present. Shorting may result in system outage and possible physical injury. Remove all metallic jewelry before servicing. (C001)

CAUTION:
Only trained service personnel may replace this battery. The battery contains lithium. To avoid possible explosion, do not burn or charge the battery.
Do Not:

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Exchange only with the IBM-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM part number for the battery unit available when you call. (C002)

CAUTION:
Use safe practices when lifting. The weight of this part or unit is approximately 96 kg (216 lb). It takes specially-trained persons and/or a lifting device to safely lift this part or unit. (C011)

18-32 kg (39.7-70.5 lbs)	32-55 kg (70.5-121.2 lbs)	≥55 kg (≥121.2 lbs)

svc00146

CAUTION:
The system contains circuit cards and/or assemblies that contain lead solder. To avoid the release of lead (Pb) into the environment, do not burn. Discard the circuit card as instructed by local regulations. (C014)

CAUTION:
This product is equipped with a 3-wire (two conductors and ground) power cable and plug. Use this power cable with a properly grounded electrical outlet to avoid electrical shock. (C018)

CAUTION:
This assembly contains mechanical moving parts. Use care when servicing this assembly. (C025)

CAUTION:
This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)

Class I

CAUTION:
Servicing of this product or unit is to be performed by trained service personnel only. (C032)

Attention notices

An attention notice indicates the possibility of damage to a program, device, or system, or to data. An exclamation point symbol may accompany an attention notice, but is not required. A sample attention notice follows:

> **Attention:** Do not bend a fibre cable to a radius less than 5 cm (2 in.); you can damage the cable. Tie wraps are not recommended for optical cables because they can be easily overtightened, causing damage to the cable.

Read and comply with the following attention notices before installing or servicing this device.

Attention: Do not connect an IBM control unit directly to a public optical network. The customer must use an additional connectivity device between an IBM control unit optical adapter (that is, fibre channel, ESCON®, or FICON®) and an external public network. Use a device such as a patch panel, a router, or a switch. You do not need an additional connectivity device for optical connectivity that does not pass through a public network.

Laser safety

When using an NVRAM5 or NVRAM6 cluster (active-active) copper-fiber converter, the storage system must be installed in a restricted access location.

> **CAUTION:**
> **This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)**

This equipment contains Class 1 laser products, and complies with FDA radiation Performance Standards, 21 CFR Subchapter J and the international laser safety standard IEC 60825.

> **CAUTION:**
> **Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of a fiber optic cable or open receptacle.**

Attention: In the United States, use only SFP or GBIC optical transceivers that comply with the FDA radiation performance standards, 21 CFR Subchapter J. Internationally, use only SFP or GBIC optical transceivers that comply with IEC standard 60825. Optical products that do not comply with these standards may produce light that is hazardous to the eyes.

Usage restrictions

The optical ports of the modules must be terminated with an optical connector or with a dust plug.

Rack safety

Rack installation

DANGER

Observe the following precautions when working on or around your IT rack system:

- **Heavy equipment - personal injury or equipment damage might result if mishandled.**
- **Always lower the leveling pads on the rack cabinet.**
- **Always install stabilizer brackets on the rack cabinet.**
- **To avoid hazardous conditions due to uneven mechanical loading, always install the heaviest devices in the bottom of the rack cabinet. Always install servers and optional devices starting from the bottom of the rack cabinet.**
- **Rack-mounted devices are not to be used as a shelf or work space. Do not place any object on top of rack-mounted devices.**
- **Each rack cabinet might have more than one power cord. Be sure to disconnect all power cords in the rack cabinet when directed to disconnect power during servicing.**
- **Connect all devices installed in a rack cabinet to power devices installed in the same rack cabinet. Do not plug a power cord from a device installed in one rack cabinet into a power device installed in a different rack cabinet.**
- **An electrical outlet that is not correctly wired could place hazardous voltage on the metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.**

CAUTION:

- **Do not install a unit in a rack where the internal ambient temperatures will exceed the manufacturer's recommended ambient temperature for all your rack-mounted devices.**

- **Do not install a unit in a rack where the air flow is compromised. Ensure that air flow is not blocked or reduced on any side, front, or back of a unit used for air flow through the unit.**

- **Consideration should be given to the connection of the equipment to the supply circuit so that overloading of the circuits does not compromise the supply wiring or overcurrent protection.**

- **To provide the correct power connection to a rack, refer to the rating labels located on the equipment in the rack to determine the total power requirement of the supply circuit.**

- *(For sliding drawers.)* **Do not pull out or install any drawer or feature if the rack stabilizer brackets are not attached to the rack. Do not pull out more than one drawer at a time. The rack may become unstable if you pull out more than one drawer at a time.**

- *(For fixed drawers.)* **This drawer is a fixed drawer and should not be moved for servicing unless specified by manufacturer. Attempting to move the drawer partially or completely out of the rack may cause the rack to become unstable or cause the drawer to fall out of the rack.**

(R001)

Frame relocation

CAUTION:
Removing components from the upper positions in the rack cabinet improves stability during relocation. Follow these general guidelines whenever you relocate a populated rack cabinet within a room or building:

- **Reduce the weight of the rack cabinet by removing equipment starting at the top of the rack cabinet. When possible, restore the rack cabinet to the configuration of the rack cabinet as you received it. If this configuration is not known, you must do the following:**
  - **Ensure that the heaviest devices are installed in the bottom of the rack cabinet.**
  - **If the rack cabinet you are relocating is part of a suite of rack cabinets, detach the rack cabinet from the suite.**
  - **Inspect the route that you plan to take when moving the rack to eliminate potential hazards.**
  - **Verify that the route that you choose can support the weight of the loaded rack cabinet. Refer to the documentation that came with your rack cabinet for the weight of a loaded rack cabinet.**
  - **Verify that all door openings are at least 760 x 2030 mm (30 x 80 in.).**
  - **Ensure that all devices, shelves, drawers, doors, and cables are secure.**
  - **Ensure that the four leveling pads are raised to their highest position.**
  - **Ensure that there is no stabilizer bracket installed on the rack cabinet during movement.**
  - **Do not use a ramp inclined at more than ten degrees.**
  - **Once the rack cabinet is in the new location, do the following:**
    - **Lower the four leveling pads.**
    - **Install stabilizer brackets on the rack cabinet.**
    - **If you removed any devices from the rack cabinet, repopulate the rack cabinet from the lowest position to the highest position.**
  - **If a long distance relocation is required, restore the rack cabinet to the configuration of the rack cabinet as you received it. Pack the rack cabinet in the original packaging material, or equivalent. Also, lower the leveling pads to raise the casters off of the pallet and bolt the rack cabinet to the pallet.**

(R002)

Safety inspections

Perform the following safety checks to identify unsafe conditions. Be cautious of potential safety hazards that are not covered in the safety checks. If unsafe conditions are present, determine how serious the hazards are and whether you should continue before you correct the problem.

Removing ac power

Perform the following steps to remove the alternating current (ac) power:

1. Perform a controlled system shutdown.
2. Set the power switch on the product to the off position.
3. Disconnect the power cables from the power source.
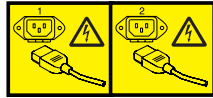
DANGER

Multiple power cords. (L003)

External machine checks

Perform the following external machine checks:

1. Verify that all external covers are present and are not damaged.
2. Ensure that all latches and hinges are in correct operating condition.
3. Check the power cable for damage.
4. Check the external signal cable for damage.
5. Check the cover for sharp edges, damage, or alterations that expose the internal parts of the device.
6. Check that any unused serial ports are covered for dust and ESD protection. The cover should be kept on the serial port whenever it is not being used.
7. Correct any problems that you find.

Internal machine checks

Perform the following internal machine checks:

1. Check for any non-IBM changes that might have been made to the machine. If any are present, obtain the "Non-IBM Alteration Attachment Survey" form, number R009, from the IBM branch office. Complete the form and return it to the branch office.
2. Check the condition of the inside of the machine for:
   - Metal or other contaminants
   - Indications of water or other fluid
   - Fire
   - Smoke damage
3. Check for any obvious mechanical problems, such as loose components.
4. Check any exposed cables and connectors for wear, cracks, or pinching.

Environmental notices

Use the environmental statements and warning in this section to guide you when using this product and in properly disposing of the product and its components.

European directive for product recycling and disposal

This unit must be recycled or discarded according to applicable local and national regulations. IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist equipment owners in recycling their IT products. Information on IBM product recycling offerings can be found on IBM's Internet site at:

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

Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. IBM recomienda a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos
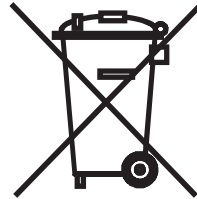
Notice: This mark applies only to countries within the European Union (EU) and
Norway.

This appliance is labelled in accordance with European Directive 2002/96/EC
concerning waste electrical and electronic equipment (WEEE). The Directive
determines the framework for the return and recycling of used appliances as
applicable throughout the European Union. This label is applied to various products
to indicate that the product is not to be thrown away, but rather reclaimed upon end
of life per this Directive.

In accordance with the European WEEE Directive, electrical and electronic
equipment (EEE) is to be collected separately and to be reused, recycled, or
recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the
WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted
municipal waste, but use the collection framework available to customers for the
return, recycling and recovery of WEEE. Customer participation is important to
minimize any potential effects of EEE on the environment and human health due to
the potential presence of hazardous substances in EEE. For proper collection and
treatment, contact your local IBM representative.

注意: このマークは EU 諸国およびノルウェーにおいてのみ適用されます。

この機器には、EU 諸国に対する廃電気電子機器指令 2002/96/EC(WEEE) のラベルが貼られて
います。この指令は、EU 諸国に適用する使用済み機器の回収とリサイクルの骨子を定めてい
ます。このラベルは、使用済みになった時に指令に従って適正な処理をする必要があることを
知らせるために種々の製品に貼られています。

Remarque : Cette marque s'applique uniquement aux pays de l'Union Européenne et à la Norvège.

L'étiquette du système respecte la Directive européenne 2002/96/EC en matière de
Déchets des Equipements Electriques et Electroniques (DEEE), qui détermine les
dispositions de retour et de recyclage applicables aux systèmes utilisés à travers l'Union
européenne. Conformément à la directive, ladite étiquette précise que le produit sur lequel
elle est apposée ne doit pas être jeté mais être récupéré en fin de vie.

Battery return program

This product may contain sealed lead acid, nickel cadmium, nickel metal hydride, lithium, or lithium ion battery. Consult your user manual or service manual for specific battery information. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to the following Web site or contact your local waste disposal facility:

http://www.ibm.com/ibm/environment/products/battery.shtml

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM Equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426-4333. Please have the IBM part number listed on the battery available prior to your call.

In Taiwan, the following applies:

Please recycle batteries.

廢 電 池 請 回 收

About this document

This document provides you with the necessary information to configure and manage the IBM Virtualization Engine™ TS7500 (TS7500 Virtualization Engine).

Use this document to:
- Set up and configure your TS7500 Virtualization Engine.
- Connect your TS7500 Virtualization Engine to your storage network.
- Gain an understanding of the basic features and capabilities of the TS7500 Virtualization Engine.

Terminology

This document uses the following two terms:

TS7500
> This term forms part of the name of the solution when described as a whole, as in TS7500 Virtualization Engine.

TS7520
> This term forms part of the name of the three major internal components of the TS7500 Virtualization Engine solution that provide enhanced capacity and performance:
> - IBM Virtualization Engine TS7520 (TS7520 Server)
> - IBM Virtualization Engine TS7520 Model SV6 (TS7520 Cache Controller)
> - IBM Virtualization Engine TS7520 Model SX6 (TS7520 Cache Drawer)

Who should read this document

This document is intended for system administrators and storage administrators who are responsible for installing storage management software.

Readers should have knowledge of the following concepts:
- Redundant array of independent disks (RAID)
- Fibre channel and serial ATA (SATA) technology

Structure of this document

Chapter 1, "Introduction," describes the TS7500 Virtualization Engine and its components.

Chapter 2, "Getting started," contains instructions for connecting, installing and configuring the TS7500 Virtualization Engine using the configuration wizard.

Chapter 3, "Basic features," contains information about the basic features of the TS7500 Virtualization Engine including searching for tapes, the physical resources, reports and importing and exporting tapes.

Chapter 4, "Failover," contains Failover information including terminology, requirements, and set up. It also presents Failover driver issues.

Chapter 5, "Replication," contains information necessary for replication such as setup requirements, checking the status and promoting a replica resource.

xxxi

Chapter 6, "Secure tape," contains information about the secure tape function, which allows you to create encryption keys for encrypting data exported to physical tape and decrypting data imported from physical tape.

Chapter 7, "Enhanced tape caching," contains information about the enhanced tape caching function, which increases the functionality of the TS7500 Virtualization Engine by acting as a cache to a physical tape library,

Chapter 8, "fibre channel considerations," contains information and instructions for the fibre channel target mode. It includes installation and configuration instructions.

Chapter 9, "iSCSI target mode," contains information about iSCSI Target Mode including supported platforms, configuration and adding your iSCSI client.

Chapter 10, "3494 Tape Library configuration," contains information about the IBM TotalStorage® 3494 Tape Library (3494 Tape Library) configuration, including instructions on adding and removing tapes.

Chapter 11, "IBM System i™ configuration," describes information about the IBM System i configuration, including preparation and setup of the tape library.

Chapter 12, "IBM TS 3500 Tape Library configuration," on page 155 contains information about the IBM System Storage™ TS3500 Tape Library configuration, including instructions on adding and removing tapes.

Chapter 13, "Hosted backup," describes information on the hosted backup function, such as configuration.

Chapter 14, "NDMP backup support," contains information describing Network Data Management Protocol (NDMP) support for backup applications, including configuration.

Chapter 15, "CallHome," contains information about how to use the CallHome customer support utility which identifies, diagnoses potential system or component failures, and automatically notifies system administrators via email.

Chapter 16, "Multi-node groups," contains information about grouping multiple servers into nodes for global access to storage.

Chapter 17, "Troubleshooting," contains troubleshooting information for the TS7500 Virtualization Engine.

Notices used in this document

This document contains the following notices that are designed to highlight key information:

Note: These notices provide tips, guidance, or advice.

Important: These notices provide information or advice that might help you avoid inconvenient or problem situations.

Attention: These notices indicate possible damage to programs, devices or data. An attention notice is placed just before the instruction or situation in which damage could occur.

Getting information, help and service

If you need help, service, technical assistance, or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you.

Note: If you call 1 (800) IBM SERV (1 800 426-7378) within the US to request support for your TS7500 Virtualization Engine, you will be prompted to select either **Hardware (Option 1)** or **Software (Option 2)** for support. Please read the following considerations for TS7500 Virtualization Engine support before reporting a problem:

  - If you are certain the problem involves software, or if you are uncertain of the source of the problem, choose Option 2 for Software support. Identify your software product as IBM Virtualization Engine TS7500 and provide the customer number under which the purchase was made as proof as purchase.

  - Choose Option 1 for Hardware support *only* if you are certain the problem involves *solely* the hardware. After you select Hardware, enter the appropriate four-digit machine type for the hardware component that displays a problem and the unique serial number (S/N) of that component. The machine types are:

    3954 For the TS7520 Server)

    3955 For either of the following:
      - TS7520 Cache Controller
      - TS7520 Cache Drawer

IBM maintains pages on the World Wide Web where you can get information about IBM products and services and find the latest technical information.

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

www.ibm.com/	Main IBM home page
www.ibm.com/storage/support/ For Support information about the TS7500 Virtualization Engine, go to this site and select **Tape & optical** from the Product family menu and select **IBM Virtualization Engine TS7500** from the Product menu.	IBM Support home page
www.ibm.com/planetwide/	IBM support page - points all countries to relevant contact information.

Services available and telephone numbers listed are subject to change without notice.

Software Maintenance

All distributed software licenses include Software Maintenance (software subscription and technical support) for a period of 12 months from the date of acquisition providing a streamlined way to acquire IBM software and assure technical support coverage for all licenses. Extending coverage for a total of three years from date of acquisition may be elected. While your Software Maintenance is in effect, IBM will provide you assistance for your 1) routine, short duration installation and usage (how-to) questions; and 2) code-related questions. IBM

provides assistance via telephone and, if available, electronic access, only to your information systems (IS) technical support personnel during the normal business hours (published prime shift hours) of your IBM support center. (This assistance is not available to your end users.) IBM provides Severity 1 assistance 24 hours a day, every day of the year.

Hardware Warranty

For a period of one year, if required, IBM provides repair or exchange service depending on the type of warranty service specified for your machine. An IBM technician will attempt to resolve your problem over the telephone; you must follow IBM's problem determination and resolution procedures. Scheduling of service will depend upon the time of your call and is subject to parts availability. Service levels are response time objectives and are not guaranteed. The specified level of warranty service may not be available in all worldwide locations; additional charges may apply outside IBM's normal service area. Contact your local IBM representative or your reseller for country and location specific information.

IBM On-Site Repair (IOR) IOR, 24 hours a day, 7 days a week, same-day response.

IBM will provide repair services for the failing machine at your location and verify its operation. You must provide suitable working area to allow disassembly and reassembly of the IBM machine. The area must be clean, well lit, and suitable for the purpose.

Getting help online

Be sure to visit the support page for the TS7500 Virtualization Engine, complete with FAQs, parts information, technical hints and tips, technical publications, and downloadable files, if applicable. This page is at:

http://www-03.ibm.com/systems/storage/tape/ts7520/index.html

For additional Web sites, see "Web sites" on page xxxv.

Before you call for service

Some problems can be solved without outside assistance, by using the online help, by looking in the online or printed documentation that comes with the TS7500 Virtualization Engine, or by consulting the support Web page. Also, be sure to read the information in any README files and release notes that come with the TS7500 Virtualization Engine.

Getting help by telephone

With the original purchase of the TS7500 Virtualization Engine, you have access to extensive support coverage. During the product warranty period, you may call the IBM Support Center (1 800 426-7378 in the U.S.) for product assistance covered under the terms of the hardware IBM warranty or the software maintenance contract that comes with product purchase.

Please have the following information ready when you call:
- Machine type and model or the software identifier. The software identifier can be either the product name (TS7500) or the Product Identification (PID) number.
- Serial numbers of the TS7500 Virtualization Engine components, or your proof of purchase.

- Description of the problem.
- Exact wording of any error messages.
- Hardware and software configuration information

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

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

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:

  http://www.ibm.com/storage/support/

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

  http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi/

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

  http://www.ibm.com/support

- The IBM HBA search Web site is:

  http://www-01.ibm.com/systems/support/storage/config/ssic/index.jsp

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

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

- To access the IBM TS7500 Interoperability Matrix Web site, go to:

  http://www-01.ibm.com/systems/support/storage/config/ssic/index.jsp

- For the latest information about storage area network (SAN) switches and directors, go to the following Web site:

  http://www-01.ibm.com/systems/support/storage/config/ssic/index.jsp

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

  http://www.ibm.com/storage/support/

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

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

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

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

Related publications

The following documents provide information about the TS7500 Virtualization Engine.

TS7500 Virtualization Engine publications

- *IBM Virtualization Engine for Tape TS7520 Introduction and Planning Guide*, GC27-2067

- *IBM Virtualization Engine for Tape TS7520 User's Guide*, GC27-2068
- *Statement of Limited Warranty*, GC26-7770

Remote Supervisor Adapter publications

- *Remote Supervisor Adapter II Slimline and Remote Supervisor Adapter II Installation Guide*, 25K8173
- *Remote Supervisor Adapter II Slimline and Remote Supervisor Adapter II User's Guide*, 25K8174

Additional related publications

- *IBM TotalStorage 3584 Tape Library Introduction and Planning Guide*, GA32-0469
- *IBM TotalStorage Enterprise Automated Tape Library (3494) Introduction and Planning Guide*, GA32-0448

Taiwan contact information

The following applies in Taiwan:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
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

How to send your comments

Your feedback is important to help us provide the highest quality information. If you have any comments about this document, you can submit them in one of the following ways:

- E-mail

  Your feedback is important in helping us to provide the most accurate and high-quality information. If you have comments or suggestions for improving this publication, you can send us comments electronically by using these addresses:

  - Internet: starpubs@us.ibm.com
  - IBMLink™ from U.S.A.: STARPUBS at SJEVM5
  - IBMLink from Canada: STARPUBS at TORIBM
  - IBM Mail Exchange: USIB3WD at IBMMAIL

  Be sure to include the name and order number of the document and, if applicable, the specific location of the text you are commenting on, such as a page number or table number.

- Mail

  Fill out the Readers' Comments form (RCF) at the back of this document and return it by mail or give it to an IBM representative. If the RCF has been removed, you can address your comments to:

International Business Machines Corporation
Information Development
Department GZW
9000 South Rita Road
Tucson Arizona 85744-0001
U.S.A.

Chapter 1. Introduction

The TS7500 Virtualization Engine is a virtual-tape solution designed to help optimize tape processing. Through the implementation of an integrated, tiered storage hierarchy of disk and tape, the benefits of both technologies can be leveraged to help enhance performance and provide the capacity needed for today's tape processing requirements. Deploying this innovative subsystem can help reduce batch processing time and management overhead.

The TS7500 Virtualization Engine uses IBM technology and software to emulate IBM tape libraries, tape drives, and media. This emulation capability is designed to help customers achieve the following operational and throughput efficiencies:

- Backup window reduction
- Restoration time reduction
- Data sharing and resource virtualization optimization
- Operational efficiency
- Improved sharing of tape libraries across applications and servers

The TS7500 Virtualization Engine is a high-performance, high-capacity open systems virtual tape product designed to augment the tape backup and restoration process in large tape environments. The TS7500 Virtualization Engine leverages your existing fibre channel SAN to transfer data to and restore data from disk-based virtual tape at ultra-high speeds.

The TS7500 Virtualization Engine can emulate the following tape libraries:

- IBM System Storage TS3500 Tape Library (TS3500 Tape Library) with any of the following:
    - Linear Tape-Open (LTO) 2 , LTO 3, and LTO 4 tape drives (L32 frames only)
    - IBM System Storage TS1120 Tape Drive Model E05 (TS1120 Tape Drive) (L22 frames only)
    - 3592 Tape Drive Model J1A (3592 J1A TApe Drive) (L22 frames only)
- IBM System Storage TS3100 Tape Library (TS3100 Tape Library):
    - 3576 Model E9U with LTO 3 and LTO 4 tape drives
- IBM System Storage TS3200 Tape Library (TS3200 Tape Library)
    - 3573 Model L4U with LTO 3 and LTO 4 tape drives
- IBM System Storage TS3310 Tape Library (TS3310 Tape Library):
    - 3573 Model L2U with LTO 3 and LTO 4 tape drives
    - 3576 Model E9U with LTO 3 and LTO 4 tape drives
- IBM System Storage TS3400 (TS3400 Tape Library) with TS1120 Tape Drives
- IBM TotalStorage 3583 Tape Library (3583 Tape Library):
    - Model L18 with LTO 3 tape drives
    - Model L36 with LTO 3 tape drives
    - Model L72 with LTO 3 tape drives

Like a conventional tape library, the TS7500 Virtualization Engine virtual tape libraries support bar codes as a mechanism to identify tape cartridges. However, because the tape is virtual, the TS7500 Virtualization Engine eliminates the common problem of backup applications being assigned large quantities of tape

and then actually using only a small portion. With the TS7500 Virtualization Engine, you can create virtual tape libraries and the system automatically allocates additional tape as needed.

You can import data from physical tape into your virtual tape system for redundancy. If you ever need to recover files from physical tape, you can use the TS7500 Virtualization Engine to access the tape for immediate recovery. For additional data protection, or to free disk space in the TS7500 Virtualization Engine, you can export the data on virtual tape to physical tape. You can also copy data to physical tape using your backup application's copy function.

Note: The Enhanced Tape Caching feature only supports data export. Data import is not supported.

The TS7500 Virtualization Engine is a tape virtualization solution for open systems attachment over fibre channel interfaces. Version 2, Release 1, now also supports iSCSI attachment. You can achieve significant operational efficiencies by storing the daily backup in the TS7500 Virtualization Engine disk cache. As backup data ages, you can migrate the older data to physical tape for long-term storage. Since the system now writes daily backup data to virtual tape via the disk cache, daily tape drive usage is greatly reduced. Another advantage of the virtual tape solution is a reduction in the number of personnel required to administer the backup process.

A TS7500 Virtualization Engine has the following numbers of fibre channel ports available for host server or tape attachment:
- One TS7520 Server: up to eight ports
- Two TS7520 Servers: up to 16 ports
- Four TS7520 Servers: up to 32 ports

A TS7500 Virtualization Engine has the following numbers of iSCSI ports available for host server or tape attachment:
- One TS7520 Server: up to 16 ports
- Two TS7520 Servers: up to 32 ports
- Four TS7520 Servers: up to 64 ports

The TS7500 Virtualization Engine supports both fibre channel and iSCSI attachments in one installation.

The TS7500 Virtualization Engine differs from many other open systems virtual tape products by enabling either parallel tape attachment or direct tape attachment. In parallel tape attachment, physical tape drives or libraries attach to the host server and data moves from the TS7500 Virtualization Engine through the host server to physical tape drives or libraries physically attached to the host server. In direct tape attachment, physical tape drives or libraries are physically attached to the TS7500 Virtualization Engine.

Backup window reduction is possible in many installations. Since robotic movement, tape cartridge mounting, and physical tape search and rewind is eliminated with virtual tape, use of the fibre channel interfaces is more effective. More tape jobs can run to virtual tape over a single interface than to physical tape. If the backup window is reduced, the time allowed for migration to physical tape is increased, thus potentially reducing the number of physical tape drives and media needed for longer term backup data storage.

Business continuity improves and provides better restoration time objectives. Restoration times decrease if the data is available in the disk cache of the TS7500 Virtualization Engine. With 1024 virtual tape drives and 128 virtual tape libraries, you can allocate to each backup server its own virtual resources, allowing multiple and disparate backup applications to use the same physical resources. This allows infrastructure simplification. You can allocate multiple tape libraries and tape drives to one or more TS7500 Virtualization Engines, centralizing backup resources and further reducing operational cost.

Key features

Key functional features of the TS7500 Virtualization Engine include:
- Virtual support of the following tape drives:
  - LTO 2 tape drive
  - LTO 3 tape drive
  - LTO 4 tape drive
  - 3592 J1A Tape Drive
  - TS1120 Tape Drive
- Virtual support of the following tape libraries:
  - TS3500 Tape Library
  - TS3100 Tape Library
  - TS3200 Tape Library
  - TS3310 Tape Library
  - TS3400 Tape Library
  - 3583 Tape Library
- Physical attachment to the following tape libraries:
  - TS3500 Tape Library:
  - TS3100 Tape Library
  - TS3200 Tape Library
  - TS3310 Tape Library
  - TS3400 Tape Library
  - 3583 Tape Library
  - IBM TotalStorage 3494 Tape Library (3494 Tape Library)
- A maximum of eight fibre channel ports per node for tape or host server attachment
- A maximum of 16 iSCSI ports for host server attachment
- Physical tape export offered in two modes:
  - Backup software-controlled
  - Operator-initiated
- Policy- or time-based migration
- Configuration of two TS7520 Servers as a dual-node high availability (HA) installation
- Configuration of four TS7520 Servers as a four-node (two dual-node pairs) HA installation
- Support for real-time compression of data
- On-demand allocation of disk storage to maximize storage use using virtual cartridges
- Static allocation support for customized environments

- Support of import/export to an 3494 Tape Library using an Ethernet interface for library management
- Interaction with the IBM Virtualization Engine TS7520 Model SV6 (TS7520 Cache Controller) to perform transparent Failover from either path failure (host bus adapter (HBA), port, switch, channel) or storage controller failure

You manage the TS7500 Virtualization Engine with the TS7500 Virtualization Engine V2R1 Software (5697-N65 or 5697-N66), which executes on a TS7520 Server, machine type and model 3954 CV5 or CV6.

Single-node, dual-node, and four-node configurations

The TS7500 Virtualization Engine is available in a single-node configuration, with one TS7520 Server, a dual-node HA configuration with two TS7520 Servers, or in a four-node HA configuration with four TS7520 Servers (two two-node pairs).

A single-node configuration supports:
- Up to 128 virtual tape libraries (3582, 3583, TS3100, TS3200, TS3310, TS3400, or TS3500)
- Up to 1024 virtual tape drives (LTO 2, LTO 3, LTO 4, 3592 J1A or TS1120)
- Up to 64,000 virtual tape cartridges

A dual-node configuration supports:
- Up to 256 virtual tape libraries (3582, 3583, TS3100, TS3200, TS3310, TS3400, or TS3500)
- Up to 2048 virtual tape drives (LTO 2, LTO 3, LTO 4, 3592 J1A or TS1120)
- Up to 128,000 virtual tape cartridges

A four-node configuration supports:
- Up to 512 virtual tape libraries (3582, 3583, TS3100, TS3200, TS3310, TS3400, or TS3500)
- Up to 4096 virtual tape drives (LTO 2, LTO 3, LTO 4, 3592 J1A or TS1120)
- Up to 256,000 virtual tape cartridges

A HA configuration, with two TS7520 Servers and dual-ac power to the 3952 F05 Frame, provides complete redundancy for servers, cache components, power, and connectivity to tape libraries or host servers.

TS7500 Virtualization Engine components

There are two main components to the TS7500 Virtualization Engine:
- **TS7500 Virtualization Engine hardware** : The hardware provides the drive or drives that hold the virtual tape data. Your hardware includes fibre channel HBAs.
- **VE console** - The Virtualization Engine (VE) console is the graphical administration tool that allows you to configure the TS7500 Virtualization Engine, add and configure clients, set properties, and manage the import and export of virtual tape cartridges.

Backup Servers

3rd party backup software

3rd party backup software

3rd party backup software

Virtual Tape Drive

Virtual Tape Drive

Virtual Tape Drive

COPY

IBM Virtualization Engine TS7500

Fibre Channel

A **Physical Tape Drives/Library**

All three backup servers are using the TS7500 Virtualization Engine for backup to *virtual* tapes. For archiving to *physical* tapes, either the backup application can write directly to the physical tape library (Scenario **A**), or the TS7500 Virtualization Engine's export function can handle the process (Scenario **B**).

B **Physical Tape Drives/Library**

Figure 1. TS7500 Virtualization Engine components

Chapter 2. Getting started

The following sections contain information about setting up and configuring the TS7500 Virtualization Engine.

Network topology considerations

The most appropriate network topology for your TS7500 Virtualization Engine depends upon the type of installation:

Two-node TS7500 EE
> See "Two-node and four-node TS7500 EE installations."

Four-node TS7500 EE
> See "Two-node and four-node TS7500 EE installations."

TS7500 LE
> See "TS7500 LE and single-node TS7500 EE installations" on page 11.

Single-node TS7500 EE
> See "TS7500 LE and single-node TS7500 EE installations" on page 11.

Two-node and four-node TS7500 EE installations

There are three Ethernet network topology options available to you when installing a two-node or four-node TS7500 EE.

Option 1: Server ports split between public and private networks
> In this option, either the eth0 or the eth1 port of each server in a base frame is on a public network, and the other port of each server (and all other components) is on a private network. This is the preferred topology for two-node or four-node TS7500 EE installations. See Figure 2 on page 8.

> **Advantages**
>> *Increased reliability*. Faults affecting the entire public network do not affect the private network.

>> *Reduced public network impact*. This configuration places a smaller administrative burden on the public network than if all components were on the public network. For example, the configuration in Figure 2 on page 8 requires only four public IP addresses. A four-node installation would require eight public IP addresses.

>> *Increased convenience*. You can monitor and operate the TS7500 Virtualization Engine remotely if you have VE console software installed on network workstations on the public network remote to the installation.

> **Disadvantages**
>> *Reduced security*. Unauthorized personnel might be able to gain access to the TS7500 Virtualization Engine.

> Figure 2 on page 8 shows an example of a TS7500 EE installation with two TS7520 Servers installed according to option 1. In this example, the eth0 ports on both servers are on public network *9.47.64.0* and all other components are on private network *192.168.0.0*. This meets the requirement that the eth0 and the eth1 ports be on different subnets when Failover is enabled. The private network uses the Ethernet switch internal to the base frame. The dedicated VE console can be connected to both networks if its workstation has two Ethernet ports. If it has only one port, it

should connect to the private network. If this were a four-node TS7500 EE installation, the eth0, eth1, and RSA connections in the other base frame would be identical except for IP addresses.
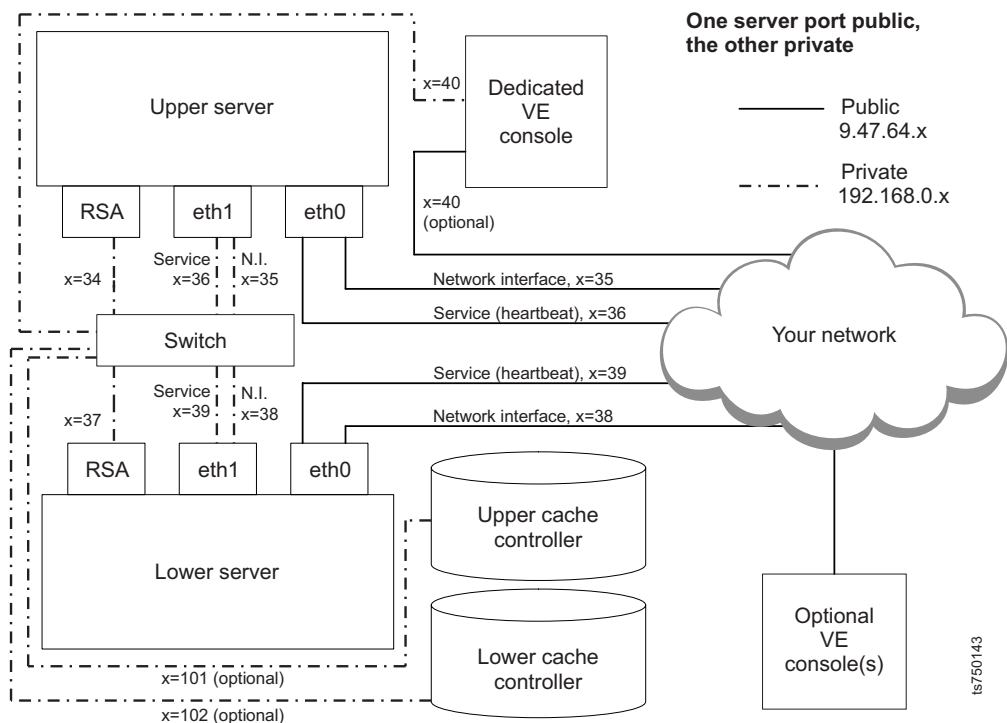
Figure 2. Network topology option 1

Option 2: Both the eth0 and eth1 ports are on a public network
In this option, all components in all base frames are on a public network. See Figure 3 on page 9.

Advantages

Increased convenience. You can monitor and operate the TS7500 Virtualization Engine remotely if you have VE console software installed on network workstations remote to the installation.

Disadvantages

Reduced security. Unauthorized personnel might be able to gain access to the TS7500 Virtualization Engine.

Reduced reliability. Faults affecting the entire network might also affect the TS7500 Virtualization Engine.

Increased public network impact. This configuration places the greatest administrative burden on the public network. For example, the configuration in Figure 3 on page 9 requires eleven public IP addresses. A four-node installation would require 21 public IP addresses.

Figure 3 on page 9 shows an example of a TS7500 EE installation with two TS7520 Servers installed according to option 2. In this example, all components are on public network *9.47.0.0*. Because the eth0 and the eth1 ports must be on different subnets when Failover is enabled, the eth1 ports for both servers are on subnet *9.47.65.0* and the eth0 ports for both servers (and all other components) are on subnet *9.47.64.0*. If this were a four-node TS7500 EE installation, the eth0, eth1, and RSA connections in the other

base frame would be identical except for IP addresses.

Both server ports public

Upper server

Dedicated VE console

x=40

(N.I. = network interface)

RSA | eth1 | eth0

x=34

Service w=65 x=39 | N.I. w=65 x=38 | Service x=36 | N.I. x=35

Your network

Optional VE console

x=37

Service w=65 x=49 | N.I. w=65 x=48 | Service x=39 | N.I. x=38

RSA | eth1 | eth0

Upper cache controller

Lower server

Public
9.47.w.x
w=64 except
as noted

Lower cache controller

x=101 (optional)

x=102 (optional)

ts750142
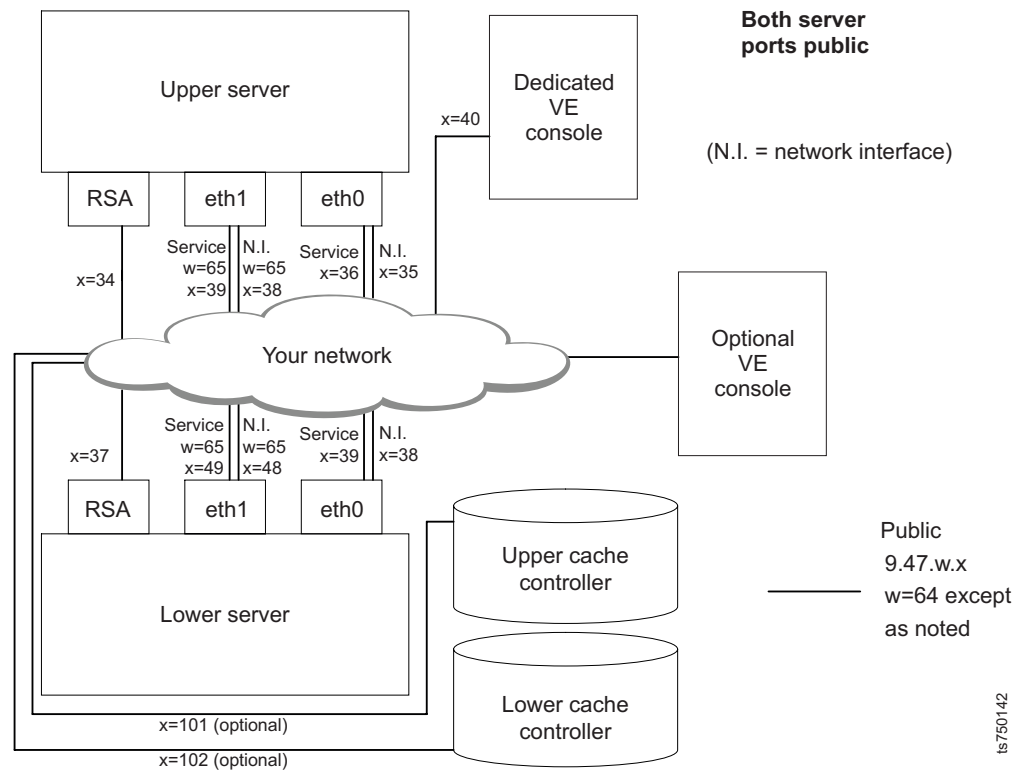
Figure 3. Network topology option 2

Option 3: Both the eth0 and eth1 ports are on a private network

In this option, all components in all base frames are on a dedicated private network. See Figure 4 on page 10.

Advantages

Maximum security. If the private network is in a secure data center, it is very difficult for unauthorized personnel to gain access to the TS7500 Virtualization Engine.

Minimum public network impact. This configuration places no administrative burden on the public network.

Disadvantages

Reduced convenience. You cannot monitor and operate the TS7500 Virtualization Engine remotely.

Reduced functionality. To use features such as Replication and iSCSI, you must purchase additional Ethernet cards for the server.

Figure 4 on page 10 shows an example of a TS7500 EE installation with two TS7520 Servers installed according to option 3. In this example, all components are on private network *192.168.0.0*, which uses the Ethernet switch internal to the base frame. Because the eth0 and the eth1 ports must be on different subnets when Failover is enabled, the eth1 ports for both servers are on subnet *192.168.1.0* and the eth0 ports for both servers (and all other components) are on subnet *192.168.0.0*. There are no optional remote VE consoles. If this were a four-node TS7500 EE installation, the eth0, eth1, and RSA connections in the other base frame

would be identical except for different IP addresses.

Both server ports private

Upper server

x=40

Dedicated VE console

RSA | eth1 | eth0

x=34

Service w=1 x=46

N.I. w=1 x=45

Service x=36

N.I. x=35

Switch

Your network

Service w=1 x=49

N.I. w=1 x=48

Service x=39

N.I. x=38

x=37

RSA | eth1 | eth0

Upper cache controller

Lower server

Private
192.168.w.x
w=0 except
as noted

Lower cache controller

x=101 (optional)

x=102 (optional)

ts750144
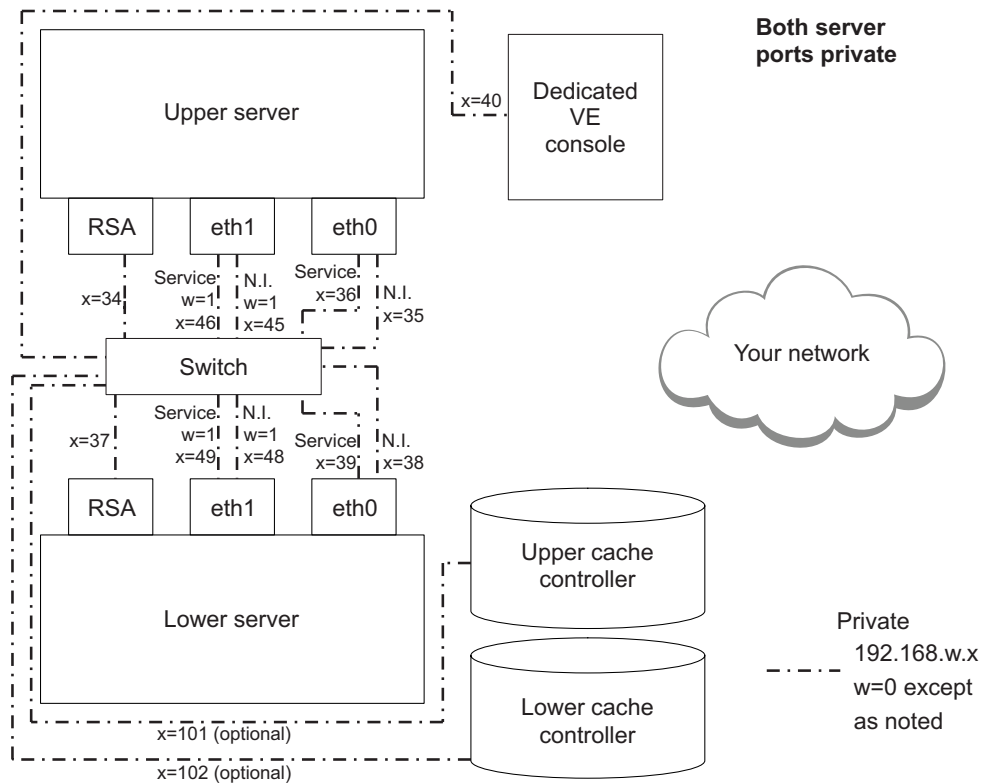
Figure 4. Network topology option 3

In all cases, connection of the cache controllers to an Ethernet network is optional. The controllers usually manage cache storage ″in-band″; that is, through the fibre channel data connections. However, attaching the controllers to an Ethernet network allows for ″out-of-band″ cache storage management, and the server does not need to be operating for you to access the Storage Manager software interface. However, you must install the Storage Manager software on a Windows® PC attached to the Ethernet network to use this option.

TS7500 LE and single-node TS7500 EE installations

Unlike the two-node and four-node installations, there is no requirement to place the IP addresses of the eth0 port on a different subnet or network from the IP addresses of the eth1 port in the TS7500 LE and single-node TS7500 EE installations. To minimize complexity, you can connect all components to either a dedicated private network or to your public network.

Dedicated private network

> **Advantages**
>
> > *Maximum security*. If the private network is in a secure data center, it is very difficult for unauthorized personnel to gain access to the TS7500 Virtualization Engine.
> >
> > *Minimum public network impact*. This configuration places no administrative burden on the public network.
>
> **Disadvantage**
>
> > *Reduced convenience*. You cannot monitor and operate the TS7500 Virtualization Engine remotely.

Public network

> **Advantages**
>
> > *Increased convenience*. You can monitor and operate the TS7500 Virtualization Engine remotely if you have VE console software installed on network workstations remote to the installation.
>
> **Disadvantages**
>
> > *Reduced security*. Unauthorized personnel might be able to gain access to the TS7500 Virtualization Engine.
> >
> > *Reduced reliability*. Faults affecting the entire network might also affect the TS7500 Virtualization Engine.
> >
> > *Increased public network impact*. This configuration places the greatest administrative burden on the public network (for instance, it requires the largest number of public network IP addresses).

Installing the VE console on a workstation running Windows

The VE console provides the capability to manage the TS7500 Virtualization Engine. In addition to installing the VE console local to your TS7500 Virtualization Engine, you can also install it on other workstations running Microsoft® Windows operating systems to allow remote administration. The *Virtualization Engine TS7520 Console Disk* includes a setup program for installation on workstations running Windows operating systems.

Note: The TS7500 Virtualization Engine does not include workstations running Windows; you must provide these.

To install the VE console software on another workstation running Windows, complete the following steps:

1. __ Load the *Virtualization Engine TS7520 Console Disk* into the workstation's CD-ROM drive.
2. __ In the installation browser window, click **Install Products → Install VE for Tape Console**
3. __ Follow the on-screen directions.

Starting the VE console

To start the VE console, use one of the following procedures:

- __ On the workstation's desktop, double-click the VE console icon.
- __ Click **Start** → **Programs** → **IBM** → **VE for Tape** → **VE for Tape Console**.

Connecting to the TS7500 Virtualization Engine

To connect to the TS7500 Virtualization Engine, complete the following steps:

1. __ Right-click the TS7500 Virtualization Engine server icon and then click **Add**.
2. __ In the **VE for Tape Server** field, type the server's full hostname or IP address.
3. __ In the **User Name** field, type `vetapeuser`.
4. __ In the **Password** field, type `veuserpassword`.
5. __ Click **OK**.

See Figure 5.
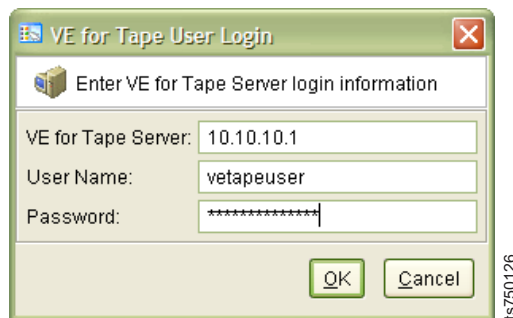
Figure 5. Connecting to the TS7500 Virtualization Engine

Note: If necessary, work with your network administrator to allow access to the TS7500 Virtualization Engine from outside of the data center's firewall.

Setting network information

Attention: Review "Network topology considerations" on page 7 before changing your network information.

To change your network settings from the values set during initial system installation, complete the following steps:

1. __ Connect to the server using the procedure in "Connecting to the TS7500 Virtualization Engine."
2. __ In the VE console, right-click the TS7520 Server icon and then click **System Maintenance** → **Network Configuration**. See Figure 6 on page 13.
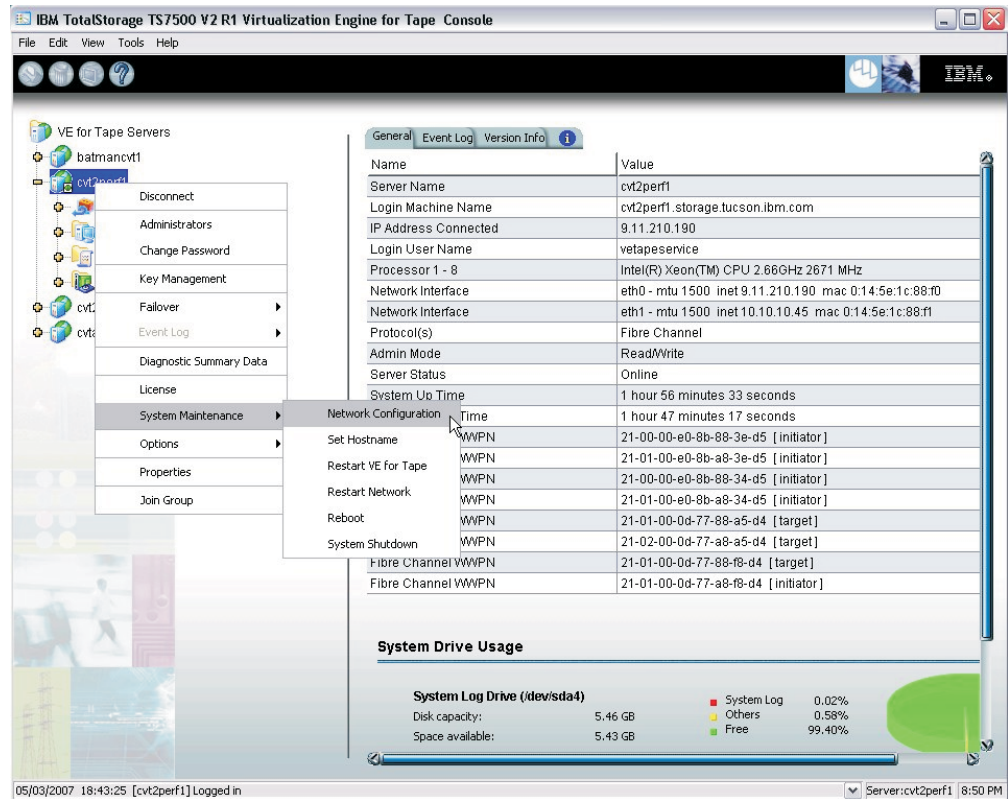
Figure 6. Selecting Network Configuration

3. __ In the Network Configuration window (Figure 7 on page 14), enter the following information:

   a. __ In the **Domain name** field, type the internal domain name.

   b. __ (Optional) Select the **Append suffix to DNS lookup** check box. This appends an entered domain name to the machine name for name resolution purposes.

   c. __ Enter DNS IP addresses:

      1) __ In the **DNS (up to two)** area, click **Add**.

      2) __ Type the IP address of the DNS server.

      3) __ Click **OK**.

      4) __ (Optional) To add a second DNS server, repeat steps 3c1 through 3c3.

   d. __ In the **Default gateway** field, type the IP address of the default gateway.
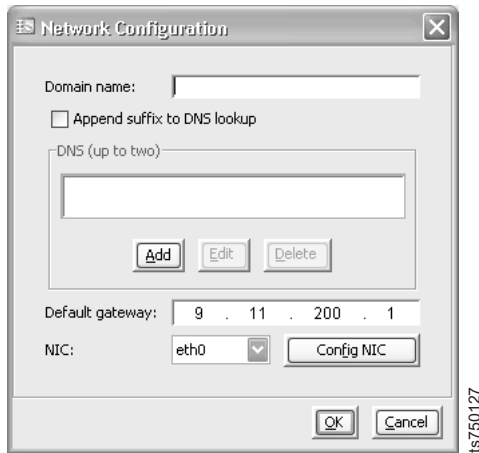
Figure 7. Network Configuration window

    e.   __ From the **NIC** list, select **eth0**.

    f.   __ Click **Config NIC**.
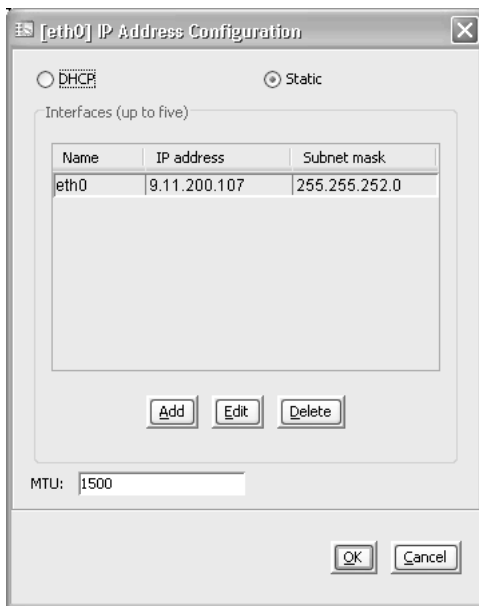
Figure 8. Configuring the eth0 port

    g.   __ Click **Static**.

    h.   __ Click **Edit**.
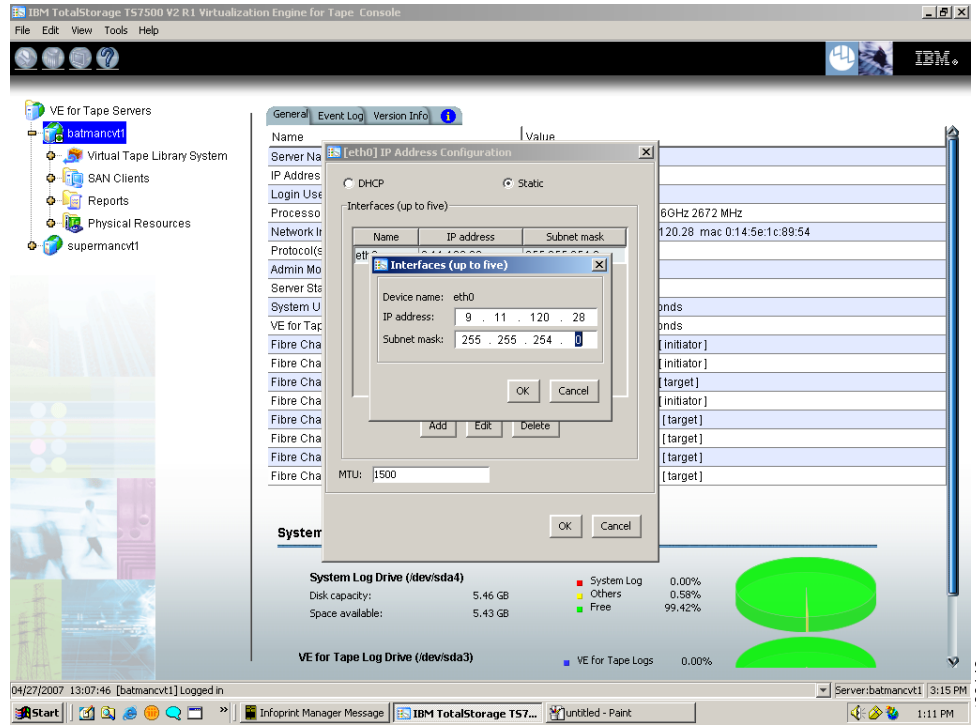
Figure 9. Setting the IP address and subnet mask for the eth0 port

    i.   __ In the **IP address** field, type the IP address.

    j.   __ In the **Subnet mask** field, type the subnet mask.

    k.   __ Click **OK**.
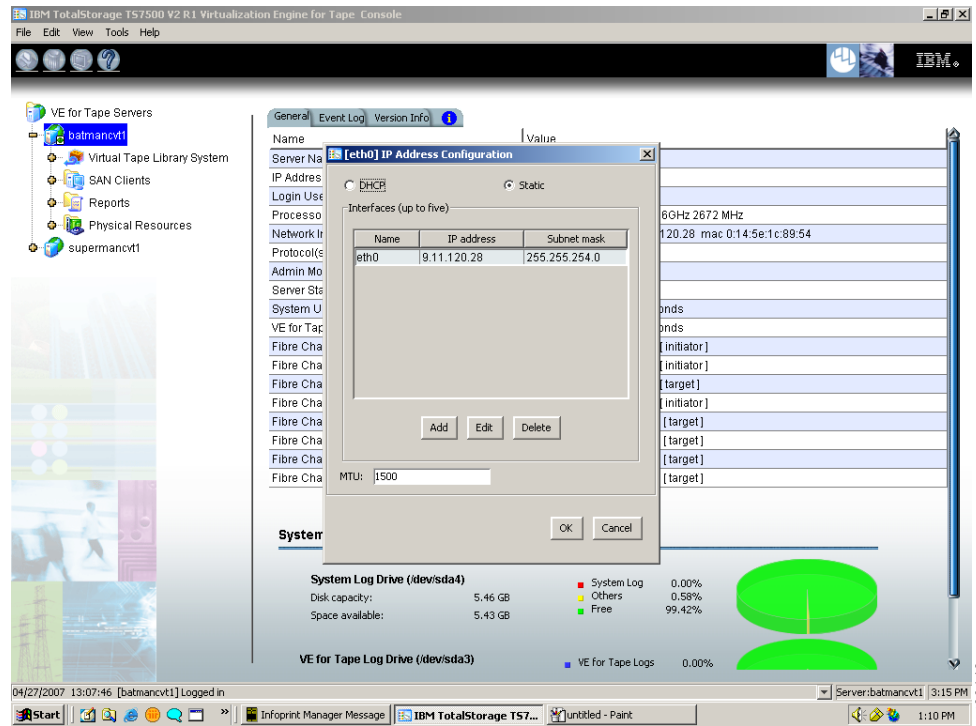
Figure 10. Verifying the IP address for the eth0 port

l.   __ In the **MTU** field, type one of the following:

  • **9000** if the adapter supports this maximum transfer rate

  • **1500** otherwise

m.   __ Click **OK**.

n.   __ From the **NIC** list, select **eth1**.

o.   __ Click **Config NIC**.

p.   __ Determine whether the eth1 port requires a static IP address or a DHCP IP address:

  • **Static** use of a static IP address is required if one or both of the following is true:

    – You want to use the default gateway.

    – The TS7520 Server is in a Failover configuration.

  • **DHCP:** use a DHCP IP address if neither of the preceding requirements for a static IP address is met.

q.   __ Perform one of the following procedures:

  • **To use a static IP address:**

    1) __ Click **Static**.

    2) __ Click one of the following:

        – __ **Add** to enter a new IP address and subnet mask.

        – __ **Edit** to change the current IP address and subnet mask.

    3) __ In the **IP address** field, type the IP address.

    4) __ In the **Subnet mask** field, type the subnet mask.

    5) __ Click **OK**.

    6) __ In the **MTU** field, type one of the following:

        – __ **9000** if the adapter supports this maximum transfer rate

        – __ **1500** otherwise

    7) __ Click **OK**.

  • **To use a DHCP IP address:**

    1) __ Click **DHCP**.

    2) __ In the **MTU** field, type one of the following:

        – __ **9000** if the adapter supports this maximum transfer rate

        – __ **1500** otherwise

    3) Click **OK**.
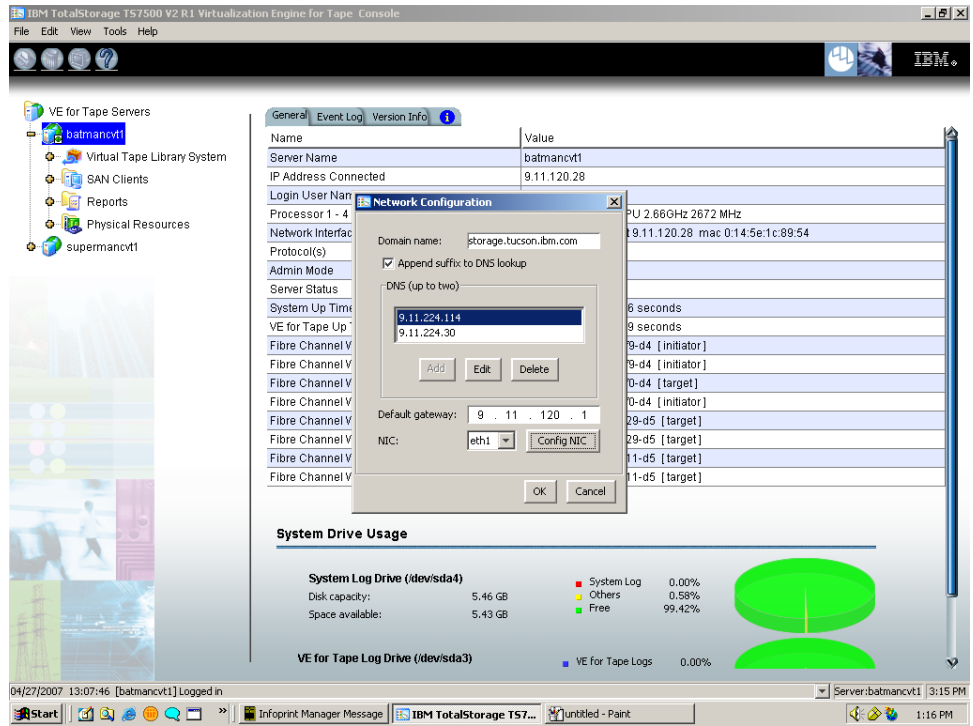
Figure 11. Network configuration

r. __ (Only required if at least one Ethernet card uses a DHCP IP address) In the Network Configuration confirmation window, click **OK**.
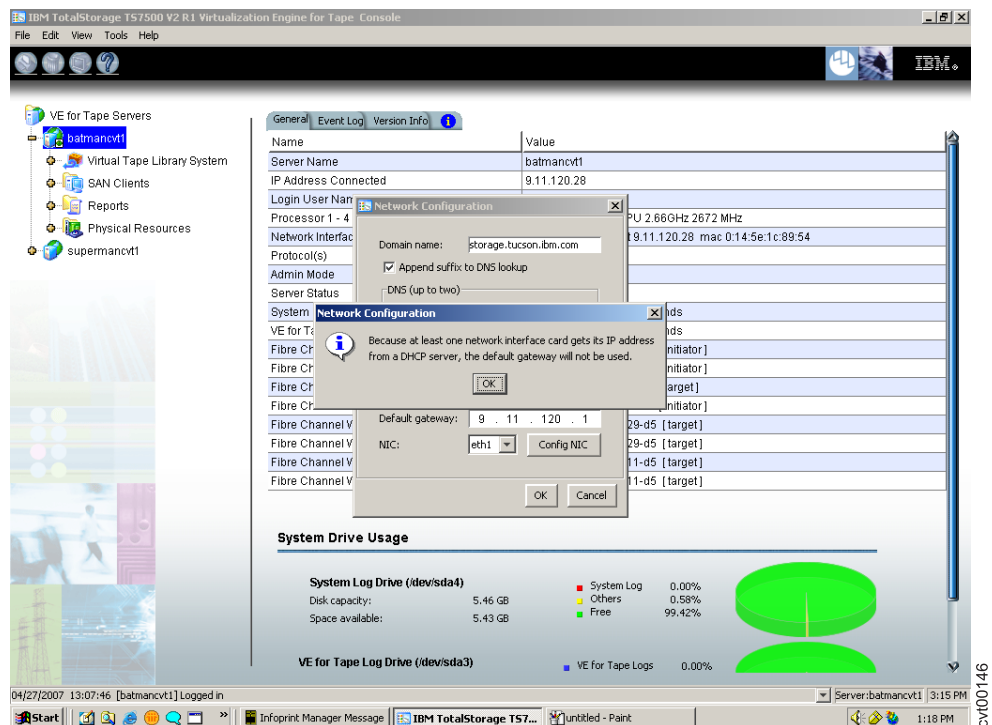
Figure 12. Network change confirmation
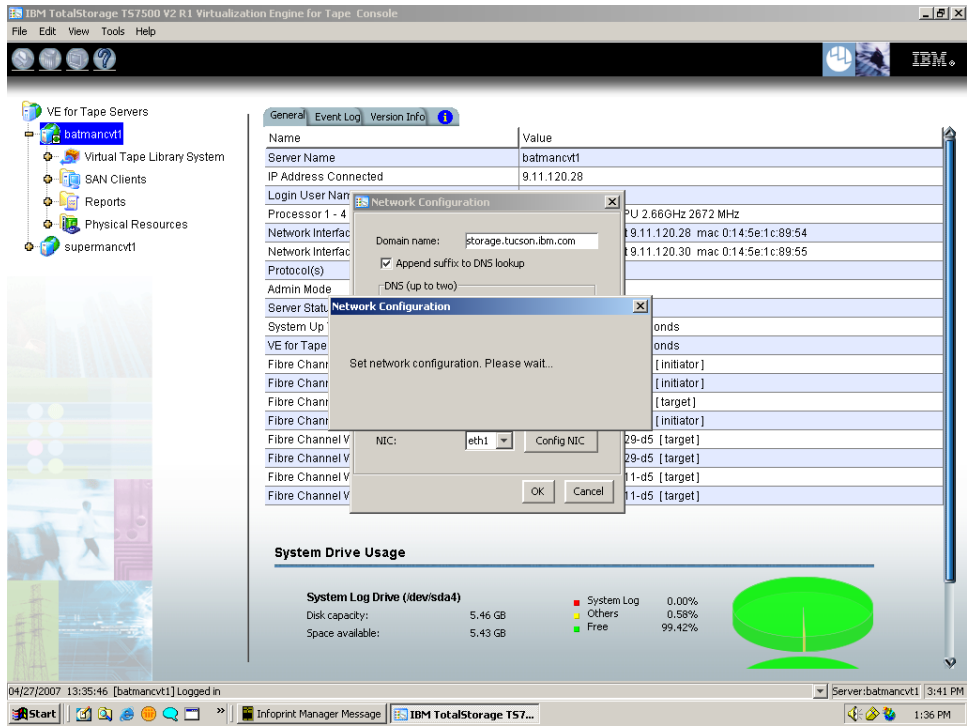
Figure 13. Setting network configuration confirmation

4. __ In the Network Configuration restart confirmation window, click **Yes**.
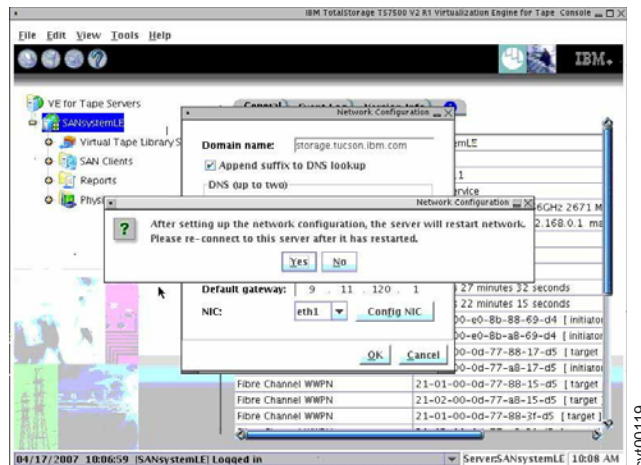
Figure 14. Network Configuration restart confirmation window

The network restarts in 30 - 90 seconds.

5. __ To reconnect to the server, right-click the server and click **Connect**.
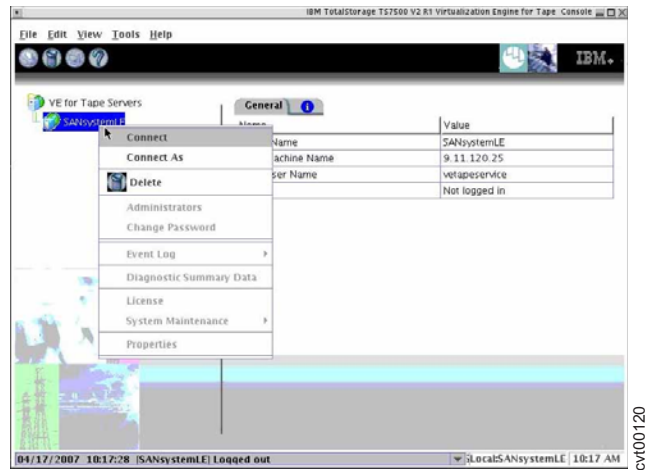
Figure 15. Reconnecting to the server after network restart

6. __ In the VE for Tape Server login window:

   a. __ In the **VE for Tape Server** field, type the new IP address of the eth0 port.

   b. __ In the **User Name** field, type `vetapeuser`.

   c. __ In the **Password** field, type `veuserpassword`.

   d. __ Click **OK**.

Setting the hostname

Note: You will need to restart the server if you change its hostname.

To set the hostname, complete the following steps:

1. __ In the VE console, right-click the TS7520 Server icon and then click **System Maintenance** → **Set Hostname**.
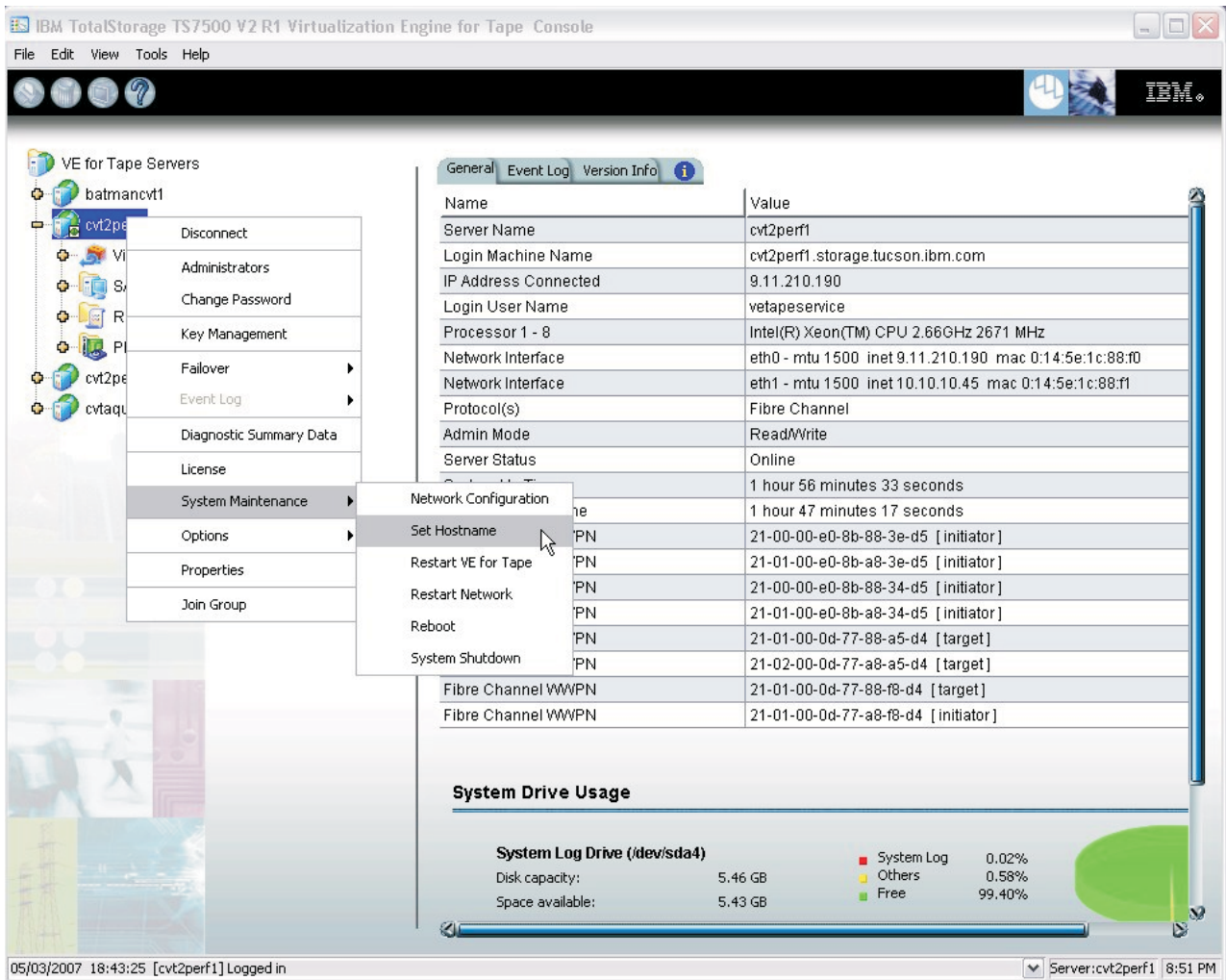
Figure 16. Selecting Set Hostname

2. __ In the **New hostname** field, type a valid hostname.
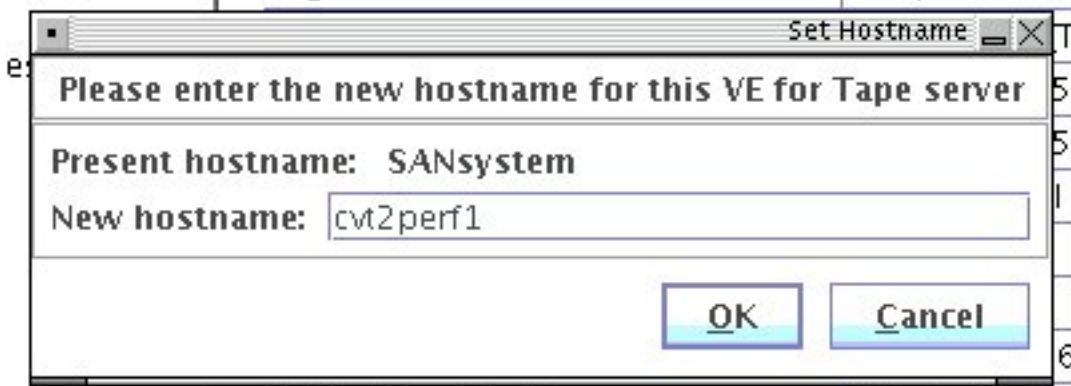
Figure 17. Entering a valid hostname

Valid characters are letters, numerals, and the following special characters: _ -
See Figure 18 on page 21.
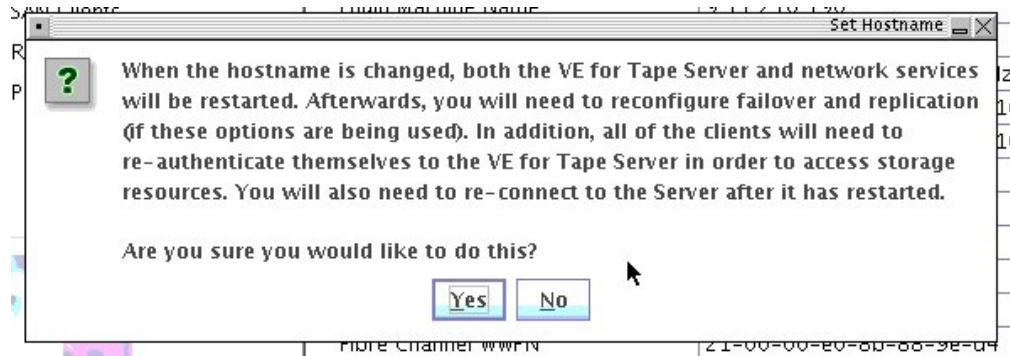
Figure 18. Setting the hostname

3. __ Click **OK**.

Using the default library configuration

The TS7500 Virtualization Engine comes pre-configured with two virtual TS3500 Tape Libraries per TS7520 Server. Each tape library contains 12 virtual LTO 2 tape drives and 253 tape cartridge slots. Each library is pre-configured with virtual tape cartridges. The number of tape cartridges pre-configured is proportional to the total system capacity.

In IBM Virtualization Engine TS7500 Enterprise Edition (TS7500 EE) installations with four fibre channel cards installed, the card's ports are configured as shown in Table 2.

Table 2. Default fibre channel card port assignments, TS7500 EE installations with four fibre channel cards

Fibre channel card	Port	Mode	Use
1	0	Initiator	To cache components
1	1	Initiator	To cache components
2	2	Initiator	To cache components
2	3	Initiator	To cache components
3	4	Target	One virtual tape library assigned
3	5	Initiator	To physical tape
4	6	Target	Other virtual tape library assigned
4	7	Initiator	To physical tape

Both virtual tape libraries and their virtual tape drives are assigned to the *Everyone_FC* client.

In IBM Virtualization Engine TS7500 Limited Edition (TS7500 LE) installations, the default libraries have similar configurations. For example, in a TS7500 LE with two fibre channel cards installed, the first card is dedicated to disk storage and the second card has one fibre channel port configured as a target and the other configured as an initiator. Because only one target port exists in this example, both default libraries would be assigned to the target port.

The default libraries are accessible when the TS7500 Virtualization Engine is turned on. You can immediately start using these libraries without any additional configuration necessary through the VE console. However, the VE console provides information helpful in creating the necessary zones when connecting to a SAN.

If you are not connecting the TS7500 Virtualization Engine to a SAN, you can directly cable your backup server or host to one of the target ports and perform a device discovery. From the rear of the TS7500 Virtualization Engine, the default target ports are PCI Slot 3, Port 1, or PCI Slot 4, Port 1. Each port is assigned to one of the default libraries.

The port assignments are different in a TS7500 LE because only one fibre channel card is required for disk cache attachment. In this case the first target port is port 2 (or the first port of the second PCI slot).

If you are connecting to a SAN, you must zone the target WWPN of the TS7500 Virtualization Engine with the WWPN of your backup server or host.

Example configuration

This section provides an example of configuring an AIX® host to use the default library configuration of the TS7500 Virtualization Engine.

The storage environment contains the following hardware components:
- A TS7500 Virtualization Engine with one TS7520 Server and two TS7520 Cache Controllers
- A System p™ 570 AIX host system with fibre channel cards
- A System x™ server with the VE console installed
- An Ethernet switch
- An IBM SAN32M fibre channel switch

Viewing the default library configuration

To view the default library configuration, complete the following steps:
1. __ Expand the server icon.
2. __ Expand **Virtual Tape Library System** → **Virtual Tape Libraries**.
3. __ Expand nested items.

Figure 19 on page 23 shows the two default libraries. Each library has 253 slots and 12 drives. One library has 11 virtual tape cartridges and the other has 12.
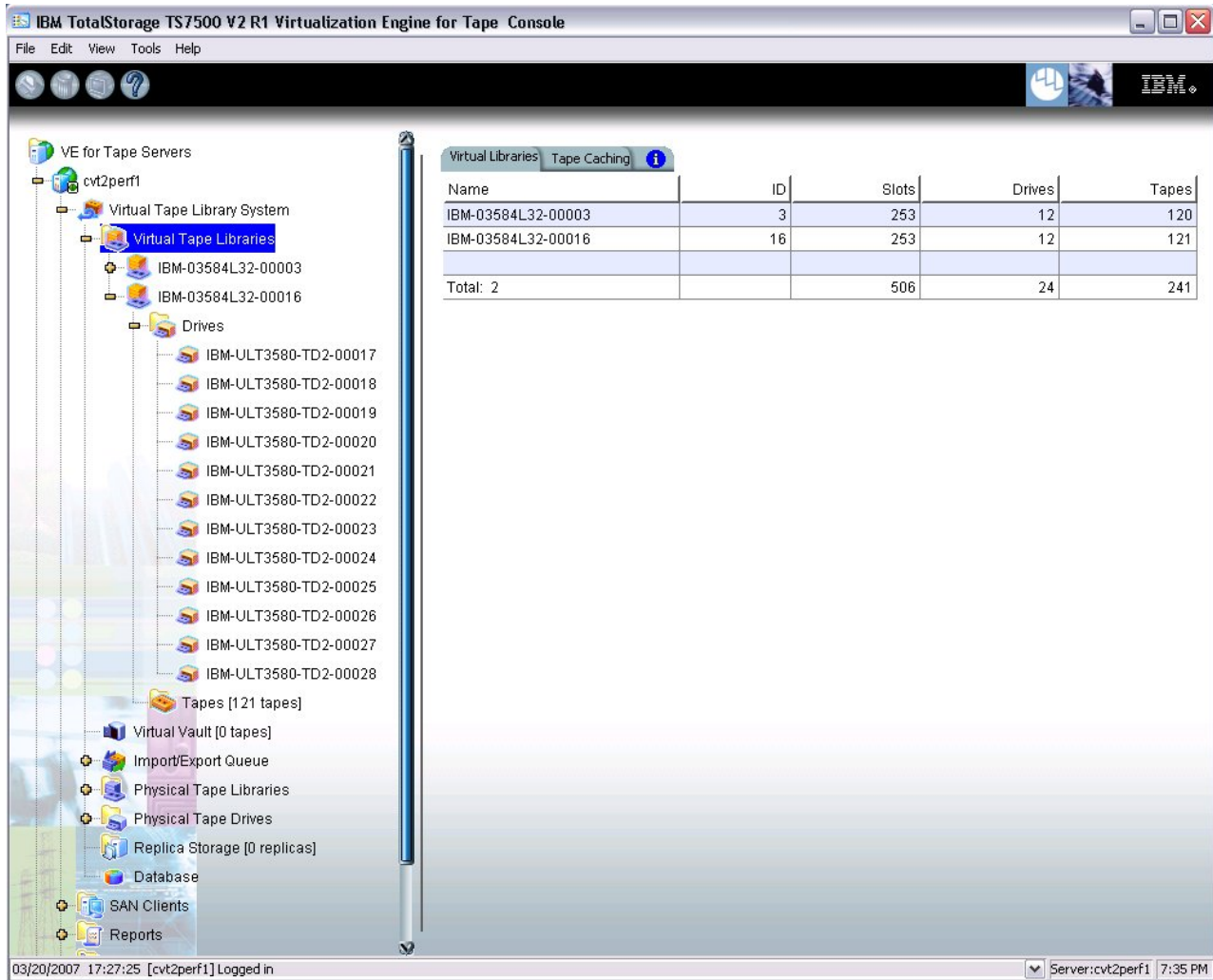
Figure 19. Two default libraries

Selecting one of the default libraries provides additional information.

See Figure 20 on page 24 for the barcode scheme used when creating additional virtual tape cartridges. The media type for the library is ULTRIUM2. The Tape Capacity on Demand function is enabled, and when a virtual tape drive mounts a virtual tape cartridge, the cartridge is initially allocated 5 GB of space. If the tape drive writes more than 5 GB of data to the cartridge, the system allocates another 5 GB. This process repeats up to the maximum capacity of 200 GB.
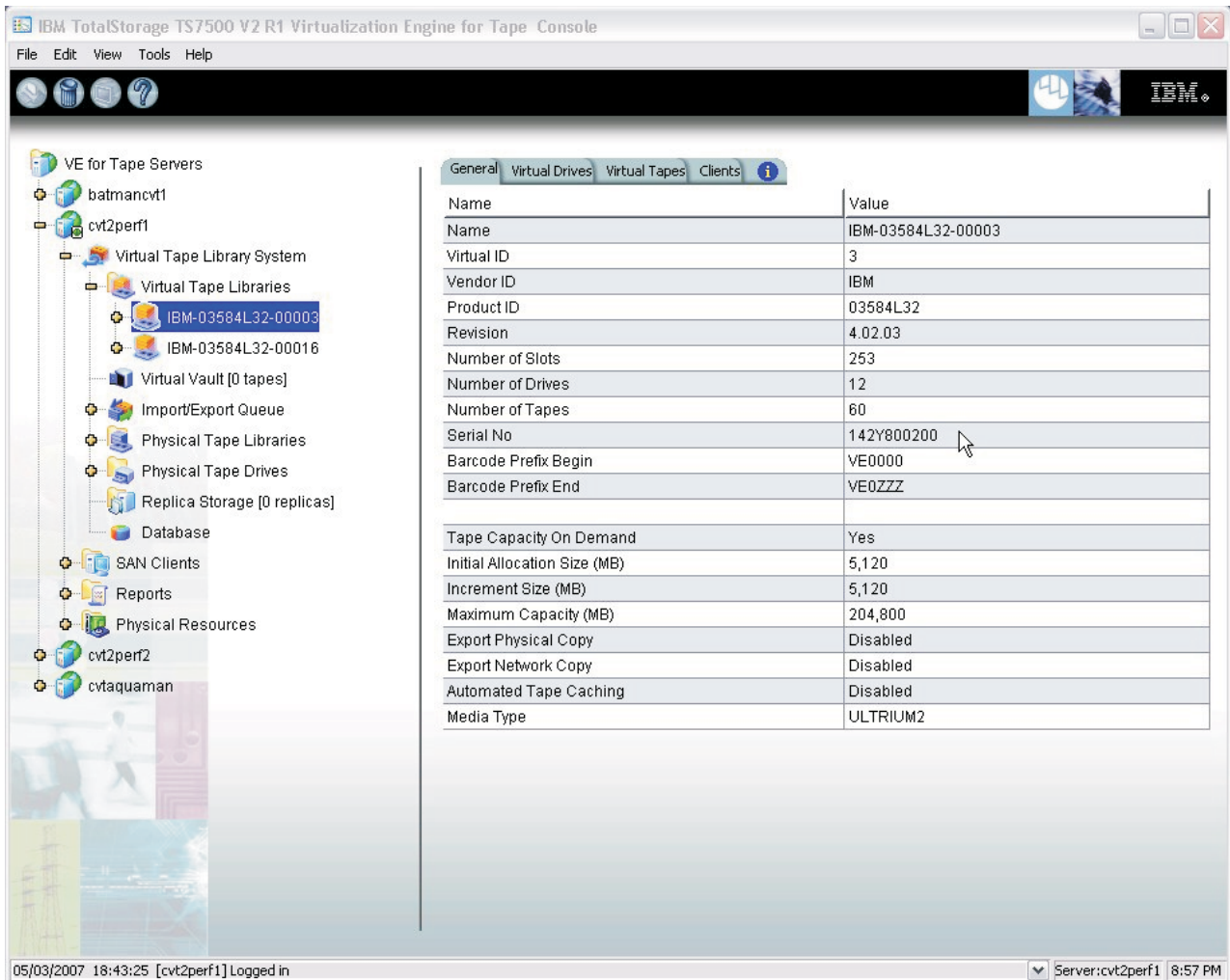
Figure 20. Virtual tape cartridge creation barcode scheme

Establishing physical connectivity

You must establish physical connectivity between the TS7500 Virtualization Engine and host to the SAN.

The AIX host's fibre channel card is cabled to port 1 of the SAN32M. Adapter 4 of the TS7500 Virtualization Engine (PCI Slot 3, Port 1) is cabled to port 12 of the SAN32M.

For more information, see "Physical connectivity" on page 132.
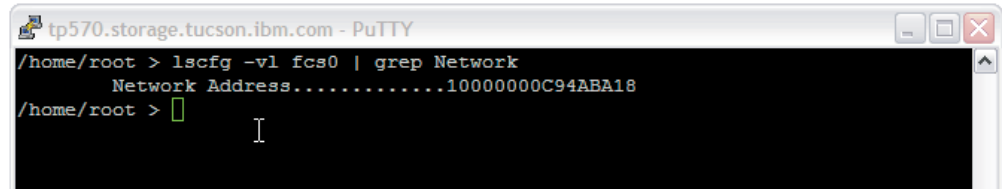
Identifying the host WWPNs

Tip: Obtaining and documenting TS7500 Virtualization Engine and host WWPNs facilitates zoning and SAN client assignment.

Each fibre channel card, operating system, and SAN has its own method of identifying WWPNs. Check the documentation specific to your hardware and environment to identify the correct method.

You can identify the WWPN of an AIX host by using the command `lscfg -vl fcs`*X* `| grep Network`, where *X* is the number of the adapter. The WWPN is also available through the SAN32M.

See Figure 21.

Figure 21. Identifying the WWPNs of the host

The WWPN of the AIX host fibre channel card is 10000000C94ABA18.

Identifying the target WWPNs of the default libraries

One method of identifying the WWPNs of the default libraries is to select the library from the SAN Clients portion of the VE console. Expand the **SAN Clients** object -> **Everyone_FC** object, and then select a library.

To identify the default library WWPNs, complete the following steps:

1. __ In the VE console, expand the server icon.
2. __ Expand **SAN Clients** → **Everyone_FC**.
3. __ Click a default virtual tape library.
4. __ In the **General** tab, note the value in the **Target WWPN** row.

In Figure 22 on page 26 the library has a target WWPN of 21-01-00-0d-77-88-a5-d4.
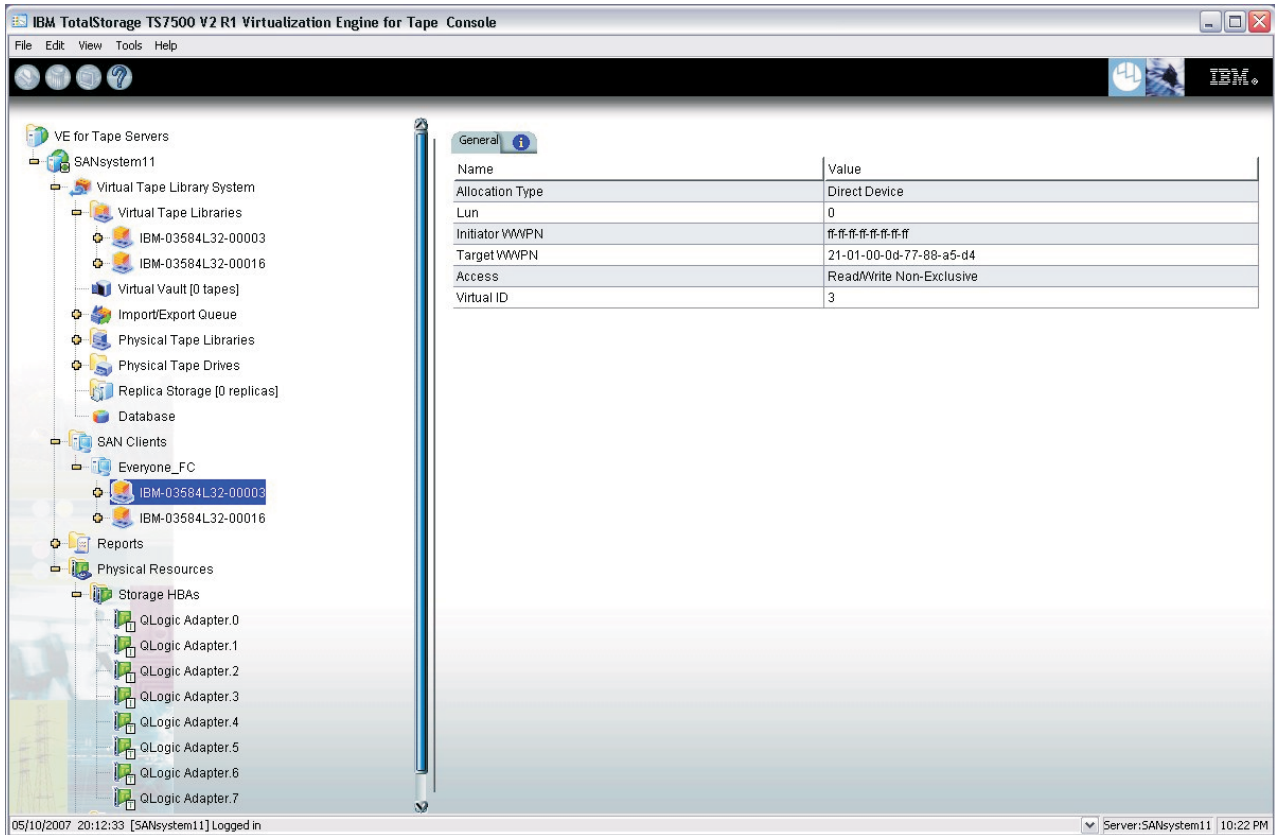
Figure 22. Identifying the target WWPNs of the default libraries

The initiator WWPN is set to *ff-ff-ff-ff-ff-ff-ff-ff*. This indicates that any WWPN can use this virtual library, except WWPNs associated with SAN clients added to the TS7500 Virtualization Engine. Because no SAN clients have been added to this system, all WWPNs can use this virtual library.

To determine the target WWPN of the library with the fibre channel card of the TS7500 Virtualization Engine, complete the following steps:

1. __ Expand **Physical Resources** → **Storage HBAs**.
2. __ Click either **QLogic Adapter 4** or **QLogic Adapter 6**.

See Figure 23 on page 27.
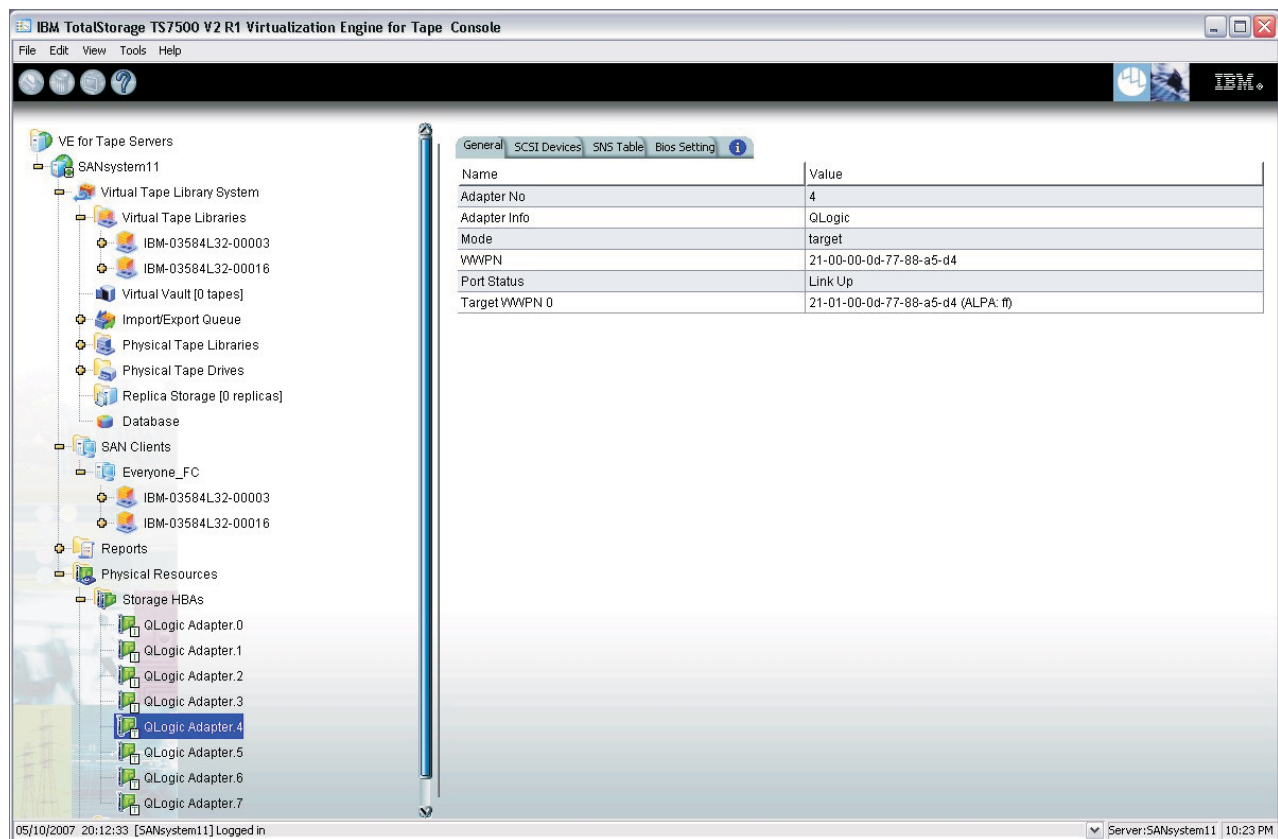
Figure 23. Associating the target library WWPN with the TS7500 Virtualization Engine fibre channel card

The target WWPN of adapter 0 matches the target WWPN of Virtual Library IBM 03584L32-00003.

Creating required zones

The WWPN of the AIX host is 10-00-00-00-C9-4A-BA-18 and the target WWPN of the desired virtual library is 21-01-00-0d-77-88-a5-d4. These two WWPNs must be in the same zone to permit logical connectivity between the host and the TS7500 Virtualization Engine.

Using the identified WWPNs, zone name tp570fcs0 was created and enabled.

Note: There are two WWPNs when you select an adapter in target mode. You must use the target WWPN for zoning purposes.

In Figure 24 on page 28 the effective configuration is viewed to ensure that the proper zoning was established.
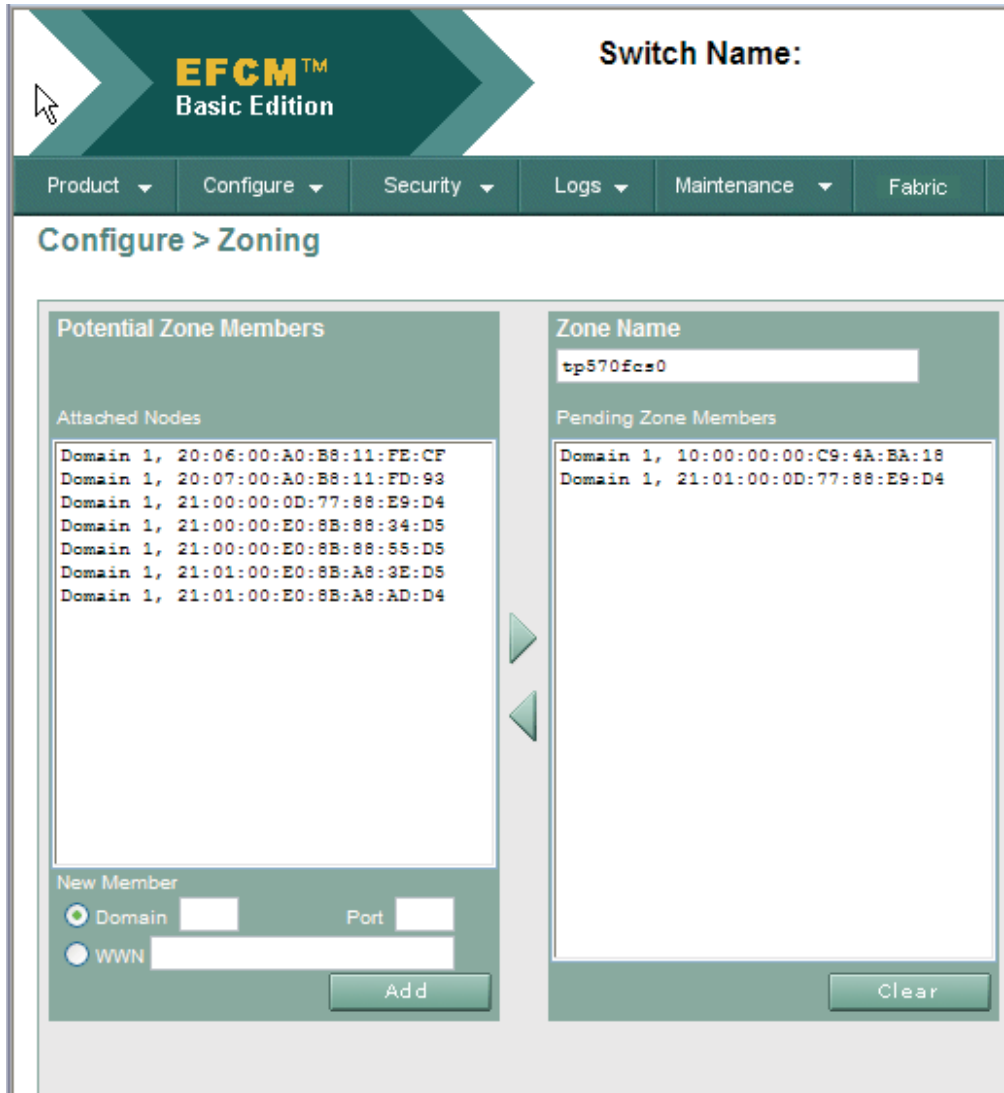
Figure 24. Creating the necessary zone

Figure 25 displays the effective configuration in a terminal window.

Figure 25. Viewing the effective configuration

The WWPN of the AIX host and the WWPN of the desired TS7500 Virtualization Engine virtual library have been zoned together.
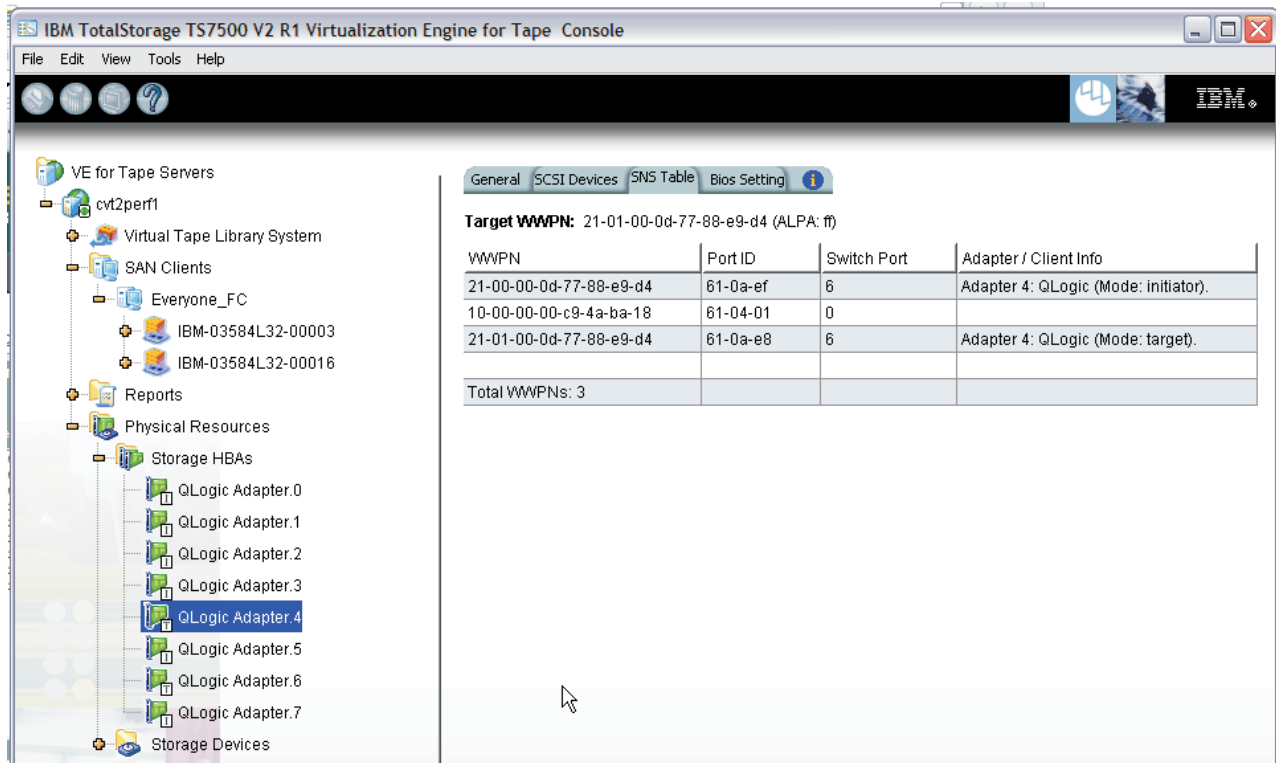
Figure 26. VE console

The TS7500 Virtualization Engine provides fibre channel fabric information via the Simple Name Server (SNS) protocol. If your SAN supports this protocol, additional information is available for each fibre channel card. In this case, the SNS table for Adapter 4 correctly shows the WWPN of the AIX host. This provides verification from the TS7500 Virtualization Engine that the two WWPNs are correctly zoned.
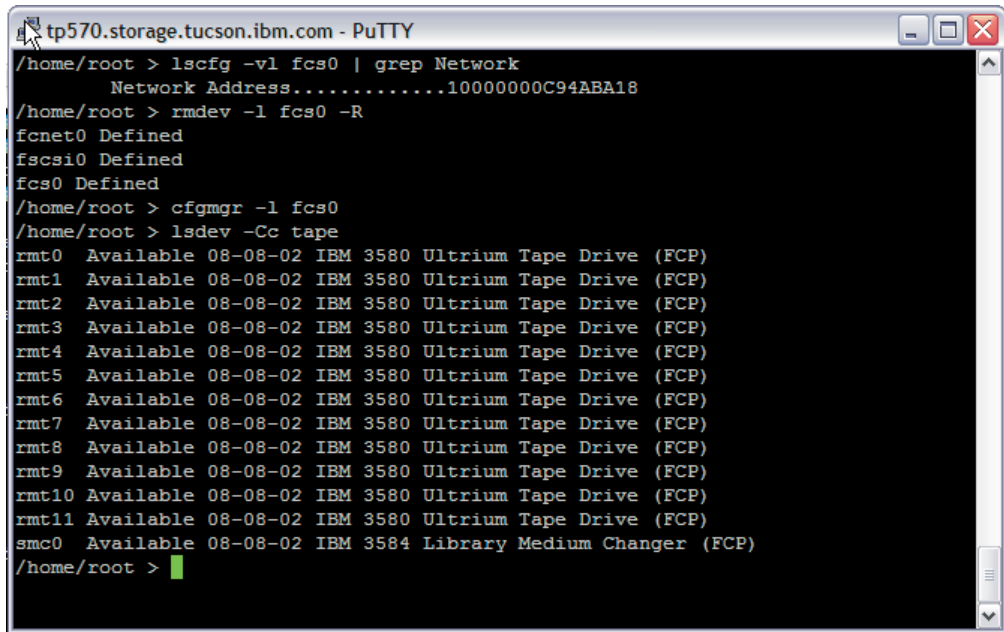
Note: After making changes to your fabric, right-click the adapter and select **Refresh SNS**.

Note: Direct cabling (Point-to-Point topology) will not have entries in the SNS table.

Discovering host devices

Note: Use of QLogic fibre channel cards with AIX hosts might require reloading the fibre channel card's device driver in order to allow virtual device configuration, especially when switching between a Point-to-Point topology and a fabric switch topology.

Figure 27 on page 30 shows the results of host device discovery.

Figure 27. Host device discovery

The **rmdev** and **mkdev** commands reload the fibre channel card's device driver.

The **cfgmgr** command performs the device discovery on the specified fibre channel card.

The **lsdev** command lists the discovered devices.

Using virtual devices

The AIX system has the Atape device driver loaded. The *tapeutil* program is a component of the Atape device driver and can be used to issue commands to the library. See Figure 28.

Figure 28. Using virtual devices

A virtual tape drive at element address 257 mounts a virtual tape cartridge from slot 1025.100 blocks of size 256 KB writes to virtual tape device rmt0.

In Figure 29 on page 31, the VE console shows a tape drive with a mounted tape cartridge. It also identifies the element address of 257.
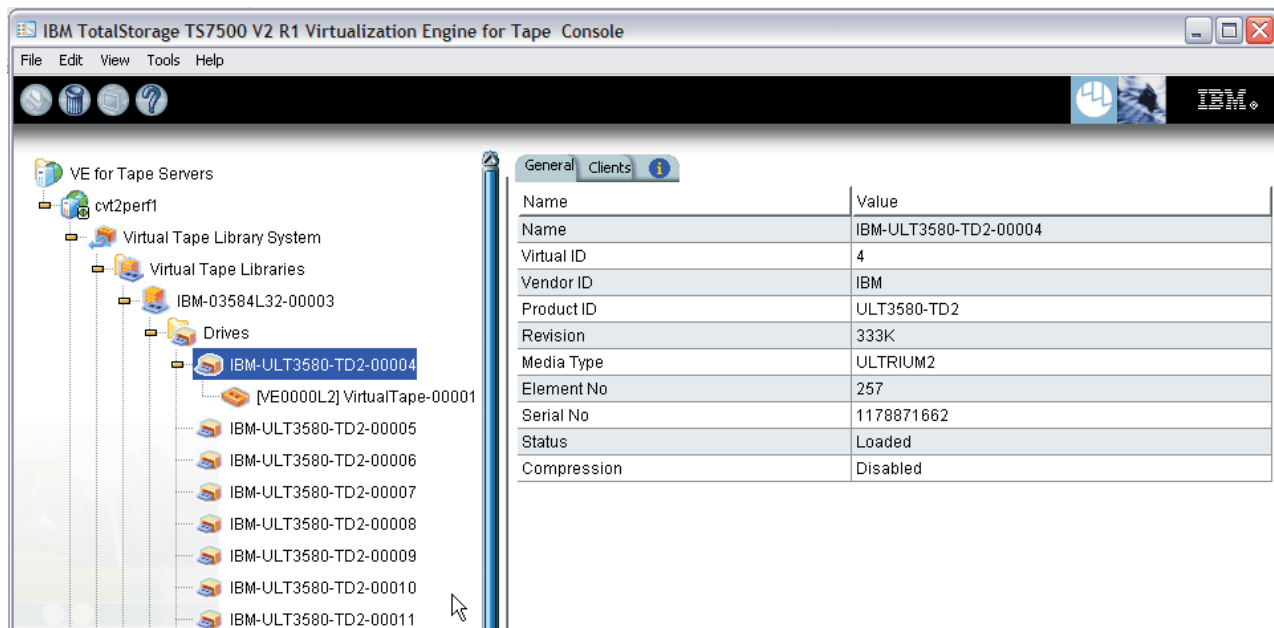
Figure 29. Virtual tape drive with virtual tape cartridge mounted

Changing the default password

> **Tip:** Changing the default password after system configuration enhances system security.

Change the default configuration password by completing the following steps:

1. __ In the VE console, right-click the TS7520 Server icon and then click **Change Password**.
2. __ In the **Old Password** field, type `veuserpassword`.
3. __ In the **New Password** field, type the new password.
4. __ In the **Confirm Password** field, type the new password again.
5. __ Click **OK**.

Performing a device scan on the backup server

After configuring the TS7500 Virtualization Engine, perform a device scan on the backup server by completing the following steps.

> **Note:** The steps to do this vary according to the server's operating system. The procedure below is for all varieties of Windows.

1. __ Click **Start** → **Settings** → **Control Panel**.
2. __ Double-click **Computer Management**.
3. __ Click the **Hardware** tab.
4. __ Click **Device Manager**.
5. __ In the right pane, right-click the device and then click **Scan for hardware changes**.

Saving the TS7500 Virtualization Engine configuration

After completing the TS7500 Virtualization Engine configuration, save the configuration to a secure location on another machine by completing the following steps:

Note: The **Save Configuration** option is available only on single-node (non-Failover) configurations. The **Save Configuration** option is not available in Failover installations. In Failover installations, configuration information is saved on four separate logical units (LUNs), providing multiple copies of configuration information.

1. __ In the VE console, click the server icon.
2. __ In the main menu bar, click **Tools** → **Save Configuration**.

Tip: Save the configuration whenever it changes, including additions, modifications, or deletions of clients or resources. See also "Safeguarding the TS7500 Virtualization Engine configuration" on page 56.

Chapter 3. Basic features

The VE console displays theTS7500 Virtualization Engine configuration organized in a format similar to Windows Explorer.

See Figure 30.
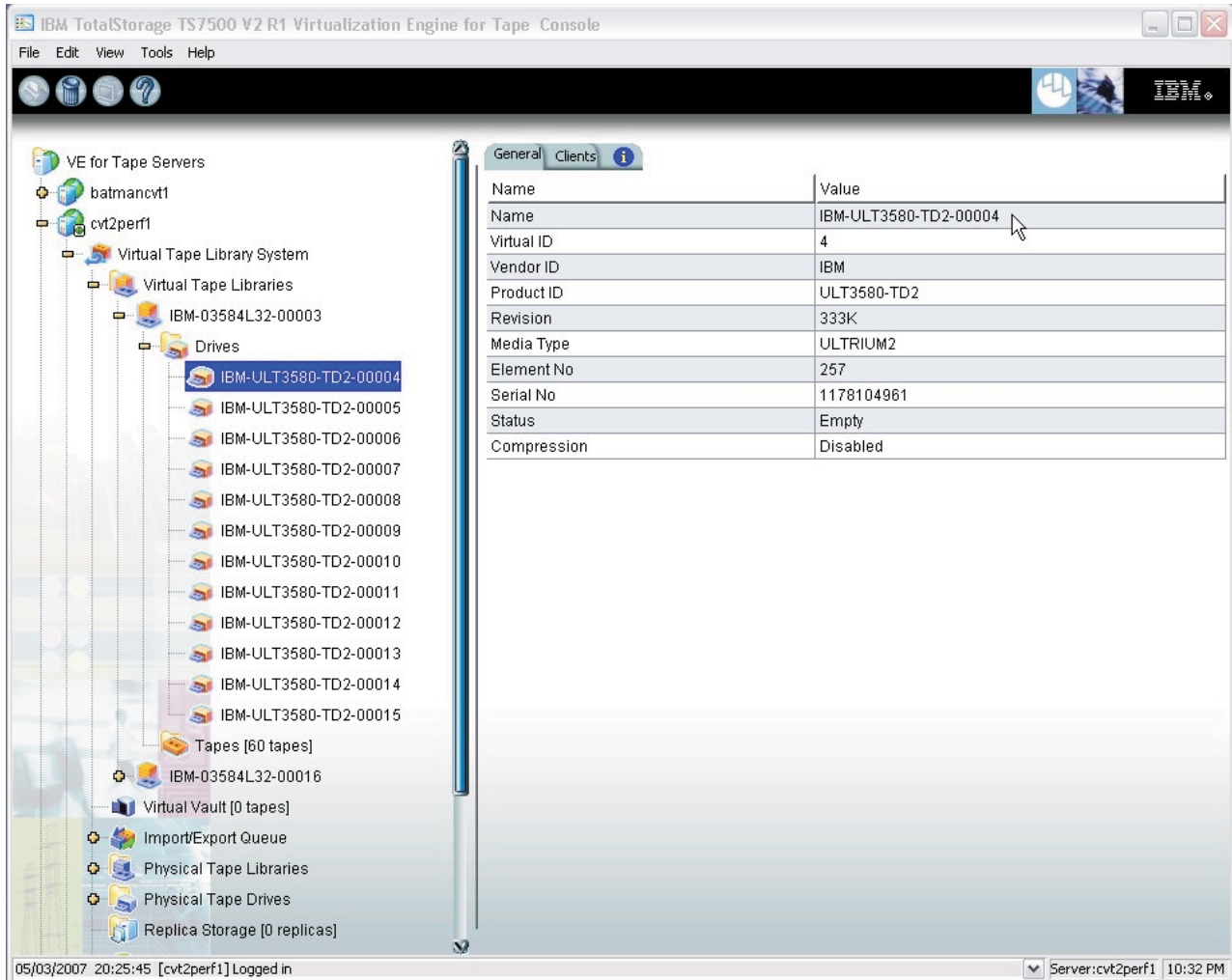
Figure 30. VE console

Figure 30 shows that clicking **Virtual Tape Libraries** → **Drives ->** displays an entry for **IBM-ULT3580-TD2–00004.**. The numeral *00004* is an example of a sequential number that the TS7500 Virtualization Engine assigns as resources are defined. The TS7500 Virtualization Engine uses these numbers internally; they have no effect on any other applications.

The tree allows navigation of the various TS7500 Virtualization Engine components and attached devices. The display expands or collapses to show only desired information. To expand a collapsed item, click the adjacent plus character (+). To collapse an expanded item, click the adjacent minus character (–). Double-clicking an item will also toggle the item's expansion and collapse.

Note: You must connect to a server before you can expand it.

Selecting an item in the navigation pane displays detailed information about the item in the right-hand pane. Select individual tabs for more information.

The log at the bottom of the window displays VE console version information. The log features a list that allows monitoring of activity during the current VE console session.

Physical resources

Physical resources include storage devices and fibre channel cards. Storage devices include hard disks, tape drives, and tape libraries. The TS7500 Virtualization Engine creates virtual tape libraries, virtual tape drives, and virtual tape cartridges on the hard drives.

Physical resource icons

Table 3 shows the icons and icon details describing physical resources in the VE console.

Table 3. Physical resource icons

Icon or detail	Description
	T indicates a target port.
	I indicates an initiator port.
	V indicates a virtualized disk.
	D indicates a physical tape library or tape drive.
	The red arrow indicates that a fibre channel card cannot access its storage.

Logical resources

Logical resources are the virtual resources defined on the TS7500 Virtualization Engine. When you complete the configuration wizard, you see a **Virtual Tape Library System** icon under **Logical Resources**. See Figure 31 on page 35.
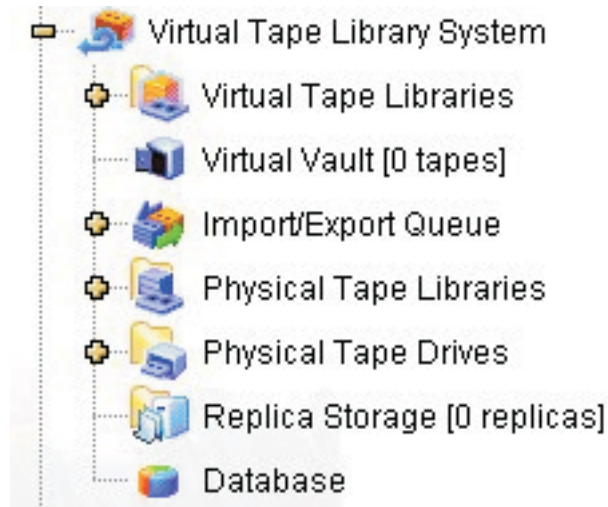
Figure 31. Logical resources

Virtual tape library system

The **Virtual Tape Library System** icon expands to show all information about the TS7500 Virtualization Engine,

Disk compression

Disk compression can save disk space because it compresses the data written to virtual tape. It does not affect data exported to physical tape; the physical tape drive controls that process. Disk compression might affect performance.

To enable disk compression, complete the following steps:

1. __ In the VE console, right-click **Virtual Tape Library System** and then click **Properties**.
2. __ Select the **Enable Virtual Tape Library compression mode** check box.
3. Click **OK**.

Virtual tape libraries

The **Virtual Tape Libraries** icon expands to list available virtual tape libraries. Each virtual tape library consists of one or more virtual tape drives and one or more virtual tape cartridges. You can assign each virtual tape library and tape drive to one or more backup servers (SAN clients). The list displays virtual tape cartridges by barcode order.

For each library, you can:
- Create or delete virtual tape cartridges
- Create or delete virtual tape drives
- Enable replication for tape cartridges in the library

For each virtual tape cartridge, you can:
- Move the virtual tape cartridge to:
  - A slot
  - A tape drive

- – The virtual vault
- Enable replication
- Change tape cartridge properties:
  - – Barcode
  - – Tape capacity on demand
  - – Write protection
  - – The Export Physical Copy/Network Copy function
- Create a remote copy

Virtual vault

The **Virtual Vault** icon expands to list the virtual tape cartridges in the virtual vault. The virtual vault is a storage area for virtual tape cartridges not assigned to a virtual tape library. This permits export of virtual tape cartridges from a virtual tape library defined in the TS7500 Virtualization Engine without immediate deletion. A virtual tape cartridge in the virtual vault can be:

- Imported into any defined virtual tape library within the TS7500 Virtualization Engine
- Copied to a remote TS7500 Virtualization Engine, physical tape library, or tape drive
- Retained in the virtual vault indefinitely
- Deleted from the vault according to a user-defined age policy
- Deleted immediately

The number of tape cartridges that the virtual vault can store is limited only by the TS7500 Virtualization Engine's available disk storage. Virtual tape cartridges will only appear in the virtual vault after export from a virtual tape library. The virtual vault lists tape cartridges by barcode order.

Import/export queue

The **Import/Export Queue** icon expands to list the submitted import and export jobs. The icon allows you to cancel a pending or in-progress job. Up to 32 concurrent import/export jobs can run concurrently, depending upon the number of physical tape drives attached to the TS7500 Virtualization Engine. The maximum number of concurrent import/export jobs is equal to the number of physical tape drives available. If you have more than 32 physical tape drives, the maximum number of concurrent import/export jobs is 32.

Physical tape libraries

The **Physical Tape Libraries** icon expands to list the physical tape libraries available to the TS7500 Virtualization Engine. You can inventory the slots and import or move tape cartridges for each tape library. You can export each physical tape cartridge, copy the physical tape cartridge to a virtual tape cartridge, or link the physical tape cartridge to a virtual tape cartridge for direct access.

Physical tape drives

The **Physical Tape Drives** icon expands to list the stand-alone physical tape drives available to the TS7500 Virtualization Engine. This icon permits the following:

- Checking for physical tape cartridges in physical tape drives
- Ejecting physical tape cartridges from physical tape drives
- Copying physical tape cartridges to virtual tape cartridges

- Linking physical tape cartridges to virtual tape cartridges for direct access

Replica resources

The **Replica Resource**s icon expands to list the replica resources on the TS7520 Server. Replica resources store data from virtual tape cartridges replicated from a remote server. Clients do not have access to replica resources.

Database

The **Database** icon displays configuration information for the TS7500 Virtualization Engine when selected. The database is mirrored for high availability.

SAN clients

SAN clients are the backup servers that use the TS7500 Virtualization Engine. The TS7500 Virtualization Engine supports fibre channel connections to servers. For fibre channel configuration information, see Chapter 8, "Fibre channel considerations," on page 131.

Reports

The TS7500 Virtualization Engine provides reports containing information about the following:

- Performance and throughput
- Physical resources: allocation and configuration
- Disk space usage
- Replication status
- Virtual tape and virtual library information
- Job status

Creating reports

To create a report, do the following:

1. __ Right-click **Reports** and then click **New**.
2. __ Select a report type from the **Report Type** list.
3. __ Click **Next**.
4. __ In the following wizard windows, specify the information for the chosen report type.
5. __ In the final wizard window, verify the information you have specified and click **Finish**.

Viewing reports

An icon for a created report appears in the **Reports** list in the navigation pane. Expand the **Reports** list to view created reports. Click the icon for a created report in the **Reports** list to display it in the right-hand pane.

Exporting data from reports

You can export the data from the following report types:

- All throughput reports
- Virtual tape information report

The export function saves the data in a comma-delimited (.csv) or tab-delimited (.txt) text file.

To export the information in a report, complete the following steps:

1. __ In the **Reports** list, right-click a report and then click **Export**.
2. __ In the Save window:
   a. __ Navigate to the folder location where you want to save the report.
   b. __ If desired, type a file name different from the default in the **File name** field.
   c. __ From the **Files of type** list, select the file format.
   d. __ Click **Save**.

Ordering license keys

The following features require activation by installation of hardware feature license keys. Your IBM service representative installs these license keys. Contact your IBM sales representative for information about these features.

- 3494 Support (TS7500 LE only; standard with TS7500 EE)
- Enhanced Tape Caching (TS7500 LE only; standard with TS7500 EE)
- Failover/Failback Enable
- iSCSI Enable
- Local Replication (TS7500 EE only; not available for TS7500 LE)
- Network Replication
- Hosted Backup
- NDMP
- Network Encryption
- Network Compression
- Network Replication
- Path Failover
- Replication Compression
- Secure Tape

Switching a port between target mode and initiator mode

Table 4 shows the default fibre channel port modes for a TS7520 Server in a TS7500 EE configuration with four fibre channel cards. For fibre channel ports 4 and higher, use target ports to attach to backup application servers and use initiator ports to attach to physical tape.

Table 4. Default fibre channel card port assignments, TS7500 EE installations with four fibre channel cards

Fibre channel card	Port	Mode	Use
1	0	Initiator	To cache components
	1	Initiator	
2	2	Initiator	
	3	Initiator	

Table 4. Default fibre channel card port assignments, TS7500 EE installations with four fibre channel cards (continued)

Fibre channel card	Port	Mode	Use
3	4	Target	One virtual tape library assigned
	5	Initiator	To physical tape
4	6	Target	Other virtual tape library assigned
	7	Initiator	To physical tape

You can change ports 5 and 7 to target mode if you do not use them to connect to physical tape. To change them to target mode, complete the following steps:

1. __ In the VE console, expand the server icon.
2. __ Expand **Physical Resources** → **Storage HBAs**.
3. __ Right-click **QLogic Adapter 5** or **QLogic Adapter 7** and then click **Enable Target Mode**.
4. In the Enable Target Mode window, click **Soft alpa creation method**.

   Attention: Do not choose the hard alpa creation method unless directed to do so by your IBM service representative.
5. Click **OK**. On the **General** tab for the adapter in the VE console, verify that the value for **Mode** now displays **target**.

Attention: Do **not** change ports 0 - 3 from initiator mode to target mode.

To change a port from target mode to initiator mode, complete the following steps:

1. __ In the VE console, expand the server icon.
2. __ Expand **Physical Resources** → **Storage HBAs**.
3. __ Right-click a target mode QLogic adapter and then click **Disable Target Mode**.

Note: A port in initiator mode with devices attached cannot change to target mode. A port in target mode with virtual tape libraries assigned cannot change to initiator mode.

Searching for virtual tape cartridges

You can use the VE console's search function to find virtual tape cartridges. To search for virtual tape cartridges, complete the following steps:

1. __ In the main menu bar, click **Edit** → **Search**.
2. __ In the **Find a tape by Barcode** field, type the tape cartridge's full barcode.
3. __ Click **Search**.

Creating virtual tape libraries

If a physical tape library is attached to the TS7500 Virtualization Engine, you must create a virtual tape library with virtual tape cartridges of the same type. For example, if a physical TS3500 Tape Library with LTO 3 tape drives attaches to the TS7500 Virtualization Engine, you must create a virtual TS3500 Tape Library with virtual LTO 3 tape drives. Virtual and physical libraries and drives with the same

characteristics ensure that virtual and physical tape cartridges also have the same characteristics. This is necessary for import and export functions and permits the backup application to accept either the virtual or physical tape cartridge.

To create a virtual tape library, complete the following steps:

1. __ If you have added a new physical device to the TS7500 Virtualization Engine, prepare a corresponding virtual tape library by completing the following steps:

    a. __ In the VE console, right-click **Physical Resources** and then click **Prepare Devices**.

    b. __ In the Physical Devices Preparation Wizard:

        1) __ Click **Prepare Devices**.

        2) __ From the **Device Category** list, select **Reserved for Virtual Device**.

        3) __ Click **Next**.

        4) __ Select the physical devices to be virtualized.

        5) __ Click **Next**.

        6) __ Verify the selected physical devices.

        7) __ Click **Finish**.

        8) __ In the **Type YES to confirm** field, type **YES**.

        9) __ Click **OK**.

        10) __ Verify that the status for each virtualized device is **Successful**.

        11) __ Click **OK**.

2. __ Start the Create Virtual Library wizard:

    • In the VE console:

        a. __ Right-click **Virtual Tape Library System** and then click **Configuration Wizard**.

        b. __ In the Configure Virtual Tape Library window, click **Next**.

    • In the VE console, right-click **Virtual Tape Libraries** and then click **New**.

3. __ In the Specify Virtual Library Name and Type page:

    a. __ From the list, select the library product that matches the installed physical library product. Its default name appears in the **Virtual Library Name** field.

    b. __ (Optional) In the **Virtual Library Name** field, type a different name for the library product.

    c. __ Click **Next**.
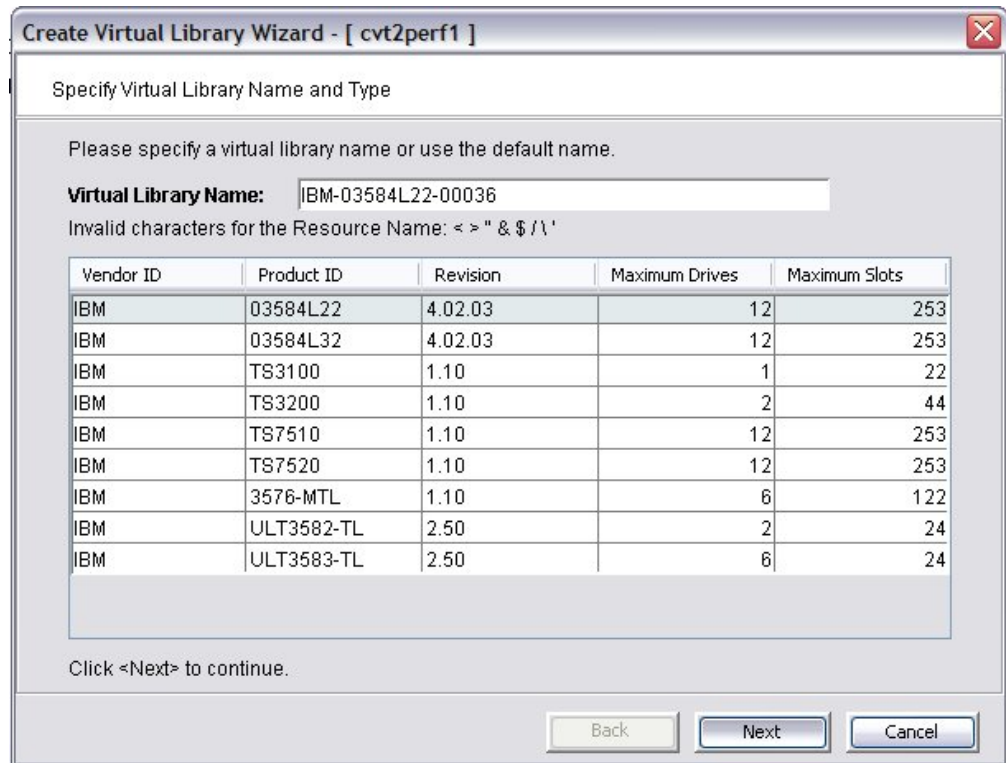
Figure 32. Specify Virtual Library Name and Type window

4. __ In the Enter Virtual Drive Information page:

   a. __ From the list, select the tape drive that matches the installed physical tape drives. Its default name appears in the **Virtual Drive Name Prefix** field.

   b. __ (Optional) In the **Virtual Drive Name Prefix** field, type a different name for the tape drive.

   c. __ In the **Total Virtual Drives** field, type a value or click the arrows to select a value. This value controls the number of jobs that can run concurrently.

   d. __ Click **Next**.
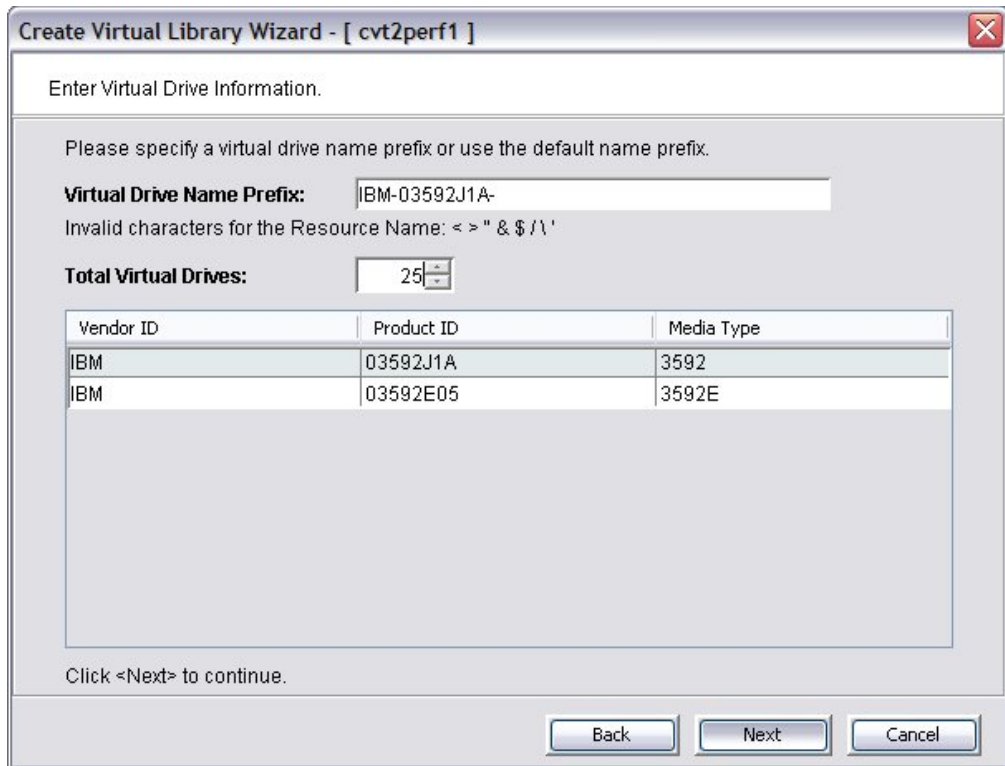
Figure 33. Enter Virtual Drive Information page

5. __ In the "Enable and configure tape caching policy" page (Figure 34), perform one of the following:

Figure 34. "Enable and configure tape caching policy" page

- To create a virtual tape library without Enhanced Tape Caching enabled, click **Next** (The **Enable Automated Tape Caching** check box is not selected) and proceed to step 6 on page 44.

- To create a virtual tape library with Enhanced Tape Caching enabled, complete the following substeps:

  a. __ Select the **Enable Automated Tape Caching** check box.

  b. __ Click **Next**.

  c. __ To select a trigger type, perform one of the following:

    – __ Click **Time Based**.

      1) __ To configure when data migration happens, choose one of the following:

        - __ Daily migration:

          a) __ Click **Daily Data Migration Schedule**.

          b) __ In the **HR:MM** field, type the hour and minute of the day (in 24-hour format) when you want data migration to start.

          c) __ Click **Next**.

        - __ Weekly migration:

          a) __ Click **Weekly Data Migration Check Schedule**.

          b) __ From the list, select the day of the week when you want data migration to occur.

          c) __ In the **HR:MM** field, type the hour and minute of the day (in 24-hour format) when you want data migration to start.

          d) __ Click **Next**.

    – __ Click **Policy Based**.

      1) __ Perform one of the following:

        - __ Click **And**. Data migration occurs when all of the policies you select are met.

        - __ Click **Or**. Data migration occurs when one or more of the policies you select are met.

        Note: You must select at least one of the options listed in steps 5d2 through 5d5.

      2) (Optional) To migrate data based on age, complete the following substeps:

        a) __ Select the **Age Based** check box.

        b) __ In the **Day(s)** field, click the arrows to select a value or type a value.

      3) __ (Optional) To migrate data based on the percentage of disk capacity used, select the **Disk Capacity Based (Triggered if disk usage is above 90%)** check box. You can adjust this value by right-clicking **Virtual Tape Library System** and then clicking **Properties**.

      4) __ (Optional) To migrate when a backup operation completes and a virtual volume dismounts, complete the following substeps:

        a) __ Select the **End of Backup** check box.

        b) __ (Optional) Select the **Only When Tape is Full** check box.

      5) (Optional) To delay migration to a specific time when another trigger has been met, complete the following substeps:

        a) __ Select the **Delay Migration Until** check box

        b) __ In the **HR:MM** field, type the hour and minute of the day (in 24-hour format) when you want data migration to start.

      6) __ Click **Next**.

d. __ In the ″Please select a reclamation trigger″ page, choose one of the following:

– __ To delete migrated data in the cache immediately after migration, click **Immediate**.

– __ To delete migrated data in the cache when cache is full, click **No More Space**.

– __ To delete migrated data after a specified amount of time:

1) __ Click **Retention Period**.

2) __ In the **Day(s)** field, click the arrows to select a value or type a value.

e. __ Click **Next** and proceed to step 7 on page 45.

6. __ Perform one of the following:

• To create a virtual tape library with neither Export Physical Copy nor Network Copy enabled, click **Next** (The **Export Physical Copy / Network Copy** check box is not selected, which is the case if Enhanced Caching is not enabled) and proceed to step 7 on page 45.

• To create a virtual tape library with either Export Physical Copy or Network Copy enabled (you can enable only one), complete the following substeps:

a. __ Select the **Export Physical Copy / Network Copy** check box.

b. __ Perform one of the following:

– __ Click **Export Physical Copy** and perform the following:

1) __ Choose one of the following:

- __ To move data to a physical tape cartridge:

a) __ Click **Move**.

b) __ In the **The grace period before deleting the tape** field, click the arrows to select a value or type a value.

c) __ Select a measure of time (for example, day(s)) from the list.

- __ To copy data to a physical tape cartridge, click **Copy**.

2) __ (Optional) Select the **Eject physical tapes to I/E slots after export** check box.

3) __ (Optional) To encrypt exported data (this option might not be available under your current license):

a) __ Select the **Encrypt data when exporting to physical tape with the selected key** check box.

b) __ From the **Select a key list**, select an encryption key.

4) __ Click **Next** and proceed to step 7 on page 45.

– __ Click **Export Network Copy** and perform the following:

1) __ Perform one of the following:

- __ Click **Copy**.

- __ Click **Move** and perform the following:

a) __ In the **The grace period before deleting the tape** field, click the arrows to select a value or type a value.

b) __ Select a measure of time from the list.

2) __ (Optional) To add a server to the **Remote server name** list:

a) __ Click **Add**.

b) __ In the **VE for Tape Server** field, type the IP address of the server.

       c) __ In the **User Name** field, type the server's default user name.

       d) __ In the **Password** field, type the server's default password.

       e) __ Click **OK**.

    3) __ From the **Remote server name** list, select a server.

    4) __ Click **Next**.
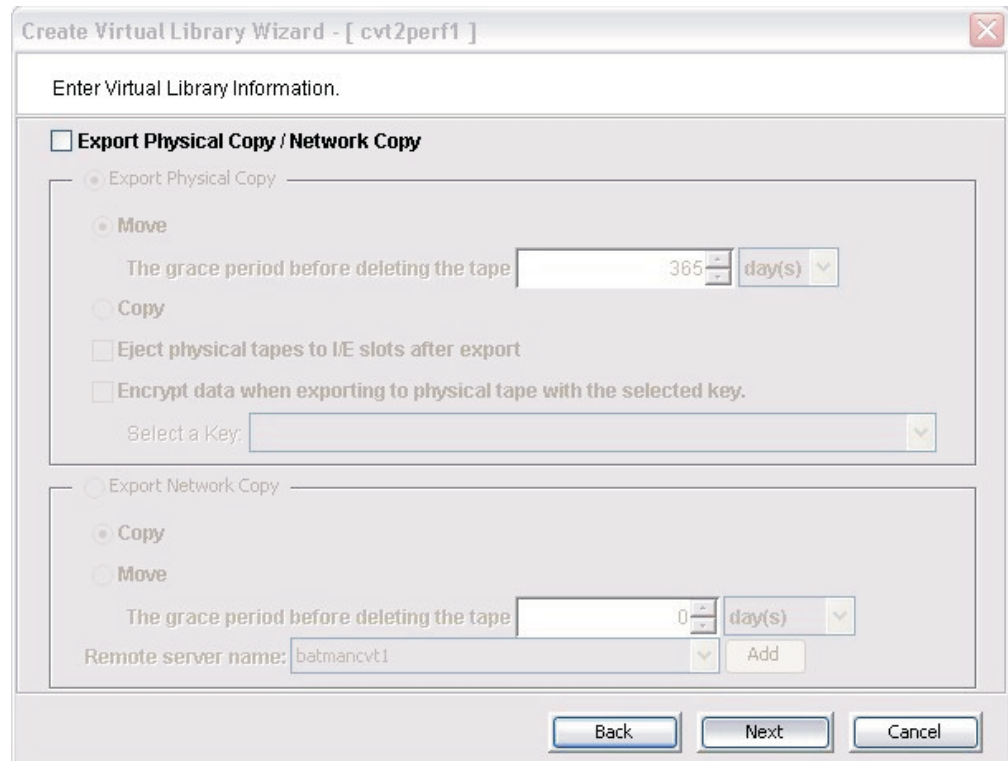
Figure 35. Export Physical Copy/Network Copy setup

7. __ In the Please enter information for the virtual library page:

   a. __ In the **Barcode Starts** field, type the starting barcode value.

   b. __ In the **Barcode Ends** field, type the ending barcode value.

      Note: Barcodes increment in a hexidecimal alphanumeric sequence by default; for example, XXXX09 increments to XXXX0A. To increment barcodes in a decimal numeric sequence (for example, XXXX09 to XXXX10), set the last three digits of the value in the **Barcode Ends** field to 999; for example, XXX999.

   c. __ In the **Slot** field, click the arrows to select a value or type a value. This value is the maximum number of slots in the physical tape library.

   d. __ In the **Import/Export Slots** field, click the arrows to select a value or type a value. This value is the number of slots in the import/export station in the physical tape library.

   e. __ Click **Next**.
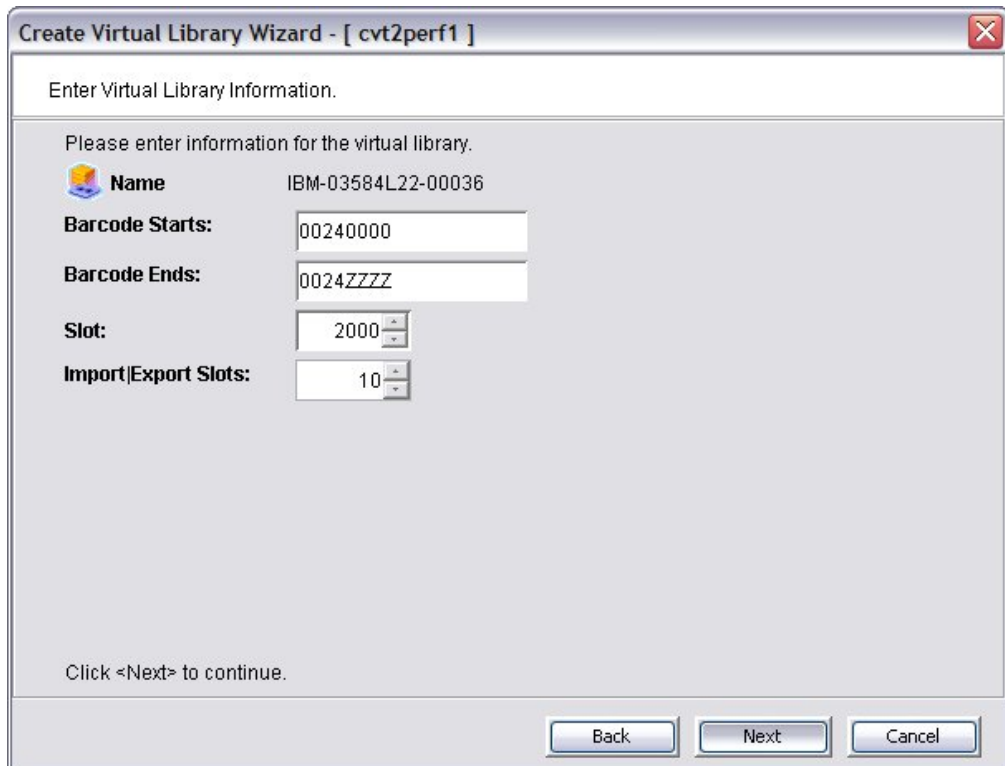
Figure 36. Barcode information setup

> **Note:** In installations without physical tape libraries, you select a range of barcodes as described above. In installations with physical tape libraries, in addition to selecting a range as described above, you can also select barcodes from an inventory list. The TS7500 Virtualization Engine generates this list by performing an inventory operation on the physical tape library. Selecting barcodes from this physical inventory list creates matching lists of virtual barcodes. In these situations, do not use the **Barcode Starts** and **Barcode Ends** fields to create a range of barcodes that overlap with the barcode range selected from the inventory list.
>
> When a physical tape library is attached to the TS7500 Virtualization Engine, within any virtual library you may define a range of virtual volume barcodes with Barcodes Start/End which have no associated physical barcoded volume. When you create a virtual tape volume cache or define volumes for Export Physical Copy, you select the specific barcodes from the physical tape library inventory.

8. __ In the Verify and create virtual library page, ensure the entered information is correct and click **Finish**.

9. __ When prompted to create tapes for the new virtual library (see Figure 37 on page 47, perform one of the following:

   - Click **Yes** to use the default values for Capacity on Demand.
   - Click **No** to change the default values for Capacity on Demand.

Figure 37. Creating virtual tape cartridges

10. __ In the VE console, right-click the new virtual library icon and then click **Properties**.

11. __ On the **Tape Properties** tab:

   a. __ (Optional) Select the **Tape Capacity on Demand** check box.

   - __ (Optional) In the **Initial Tape Size** field, type a value or click the arrows to select a value.

   - __ (Optional) In the **Incremental Size** field, type a value or click the arrows to select a value.

   Note: The tape capacity on demand function creates small tape cartridge resources allocates additional space as needed. Default values are:

   - __ 5 GB for all tape cartridges initially
   - __ Incremental sizes:
     - __ 5 GB for LTO 2 Tape Drives and 3592 J1A Tape Drives
     - __ 7 GB for LTO 3 Tape Drives
     - 12 GB for LTO 4 Tape Drives
     - __ 8 GB for TS1120 Tape Drives

   If you do not select the **Tape Capacity on Demand** check box, the TS7500 Virtualization Engine increments virtual tape cartridges at the full size of the emulated physical tape cartridges.
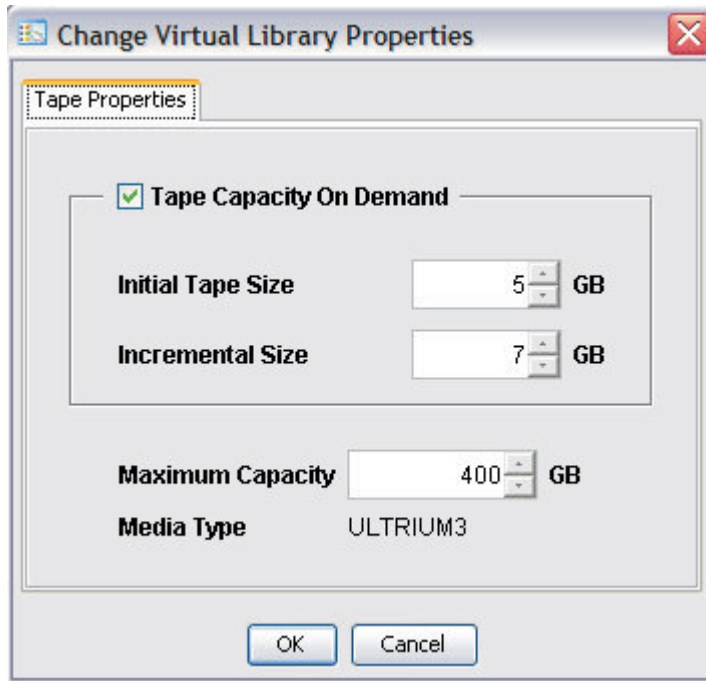
Figure 38. Specifying virtual tape capacities

12. __ In the **Maximum Capacity** field, click the arrows to select a value or type a value.

   Note:

   If you did not select **Export Physical Copy** during the setup wizard, you can enter any maximum capacity. However, if you enter a capacity larger than the tape cartridge's native uncompressed capacity, you cannot export to physical tape.

   If you selected **Export Physical Copy**, the TS7500 Virtualization Engine sets the maximum capacity to a value less than the tape cartridge's native uncompressed capacity in anticipation of using disk compression.

   The default maximum capacity varies by tape drive. If using disk compression, do not change the default value. If not using disk compression, adjusting the maximum capacity to the uncompressed tape cartridge capacity is permitted.

13. __ Click **OK**.

Adding SAN clients

To add fibre channel clients, complete the following steps:

1. __ In the VE console, right-click **SAN Clients** and then click **Add**. The Add Client wizard opens.
2. __ In the Enter the Fibre Channel Client Name window:
   a. __ In the Client Name: field, type a name for the SAN client.
   b. __ Click **Find**.

>   c. __ Click **Next**.

3. __ In the Set Client Fibre Channel Properties window:

>   a. __ From the **Initiator WWPN** list, select the check box for the client's initiator WWPN. If that WWPN is in a zone, you can only select initiators from that zone. If there is only one WWPN in the list, the wizard selects it automatically and does not display this window.
>
>   b. __ Click **Next**.

4. __ (Optional) In the Fibre Channel Option window, select the Enable Volume Setting Address check box and then click **Next**. Volume Set Addressing (VSA) may be required for particular fibre channel storage depending upon the storage system's requirements. For example, storage that is connected to an HP-UX host with an HP fibre channel card requires VSA addressing. Similarly, storage that was formerly connected to HP-UX hosts usually has the VSA option turned on. Refer to the SAN client's documentation to determine whether VSA is required.

5. __ In the Add the Fibre Channel Client window, verify the selected information and then click **Finish**.

Assigning virtual tape libraries to SAN clients

Assign virtual tape libraries to SAN clients by performing one of the following:

- __ In the VE console, right-click **Virtual Tape Library System** and then click **Configuration Wizard**.

  Note: You must first create virtual tape libraries when you use this method. See "Creating virtual tape libraries" on page 39.

- __ In the VE console:

  1. __ Expand **SAN Clients**.
  2. Right-click a SAN client and then click **Assign**.

- __ In the VE console:

  1. __ Expand **Virtual Tape Library System** → **Virtual Tape Libraries**.
  2. __ Right-click a virtual tape library and then click **Assign**.
  3. __ Assign virtual tape libraries or virtual tape drives to backup clients.
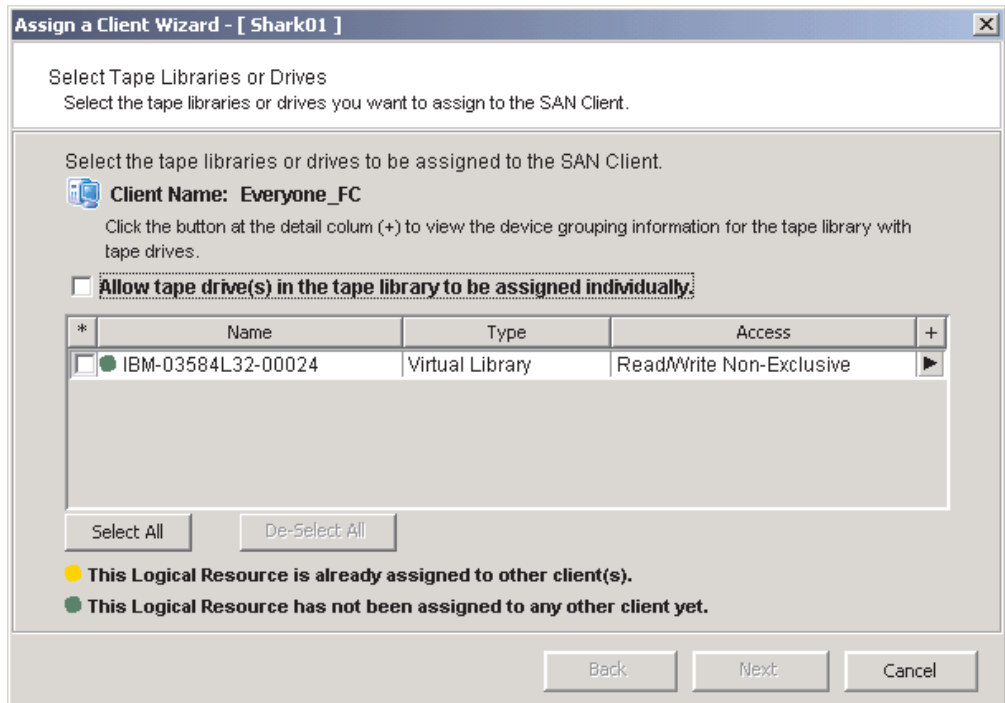
Figure 39. Assign virtual tape libraries or drives to your backup clients

    4. __ Click **Finish**.

Note: You must define backup servers as SAN clients before connecting them to virtual tape libraries. You must also first identify the server's fibre channel properties. For convenience, specify the server's network-resolvable hostname.

Assigning physical tape libraries to the TS7500 Virtualization Engine

If you plan to import data from physical tape cartridges into your virtual tape library, or to export virtual tape cartridges to physical tape cartridges, you must assign your physical tape libraries or tape drives to the TS7500 Virtualization Engine.

1. __ If you added new physical devices, prepare them by performing the procedure in step 1 on page 40.

2. __ Open the Assign Physical Devices Wizard by performing one of the following:

   - __ In the VE console:

     a. __ Right-click **Virtual Tape Library System** and then click **Configuration Wizard**.

     b. __ Click **Skip**.

     c. __ Click **Next**.

     d. __ Click **Next**.

   - __ In the VE console:

     a. __ Expand **Virtual Tape Library System**.

     b. __ Select the physical device:

        - __ Right-click **Physical Tape Libraries** and then click **Assign**.

        - __ Right-click **Physical Tape Drives** and then click **Assign**.

3. __ Select the physical libraries/drives to be assigned to the TS7500 Virtualization Engine.

4. __ Click **Finish/Assign**.

Note: Assigning physical devices also inventories the physical tape cartridges in the tape library or tape drive. This allows you to create virtual tape cartridges matching your physical tape cartridges.

Assigning a 3494 Tape Library to a TS7500 Virtualization Engine

The 3494 Tape Library is an automated tape library that multiple backup servers can share.

The TS7500 Virtualization Engine cannot emulate a 3494 Tape Library. However, it can emulate the tape drives of a 3494 Tape Library. This permits importing data from physical tape cartridges and exporting data on virtual tape cartridges to physical tape cartridges.

To assign a 3494 Tape Library, complete the following steps:

1. __ Right-click **Physical Tape Libraries** and then click **Assign IBM 3494**. See Figure 40 on page 52.
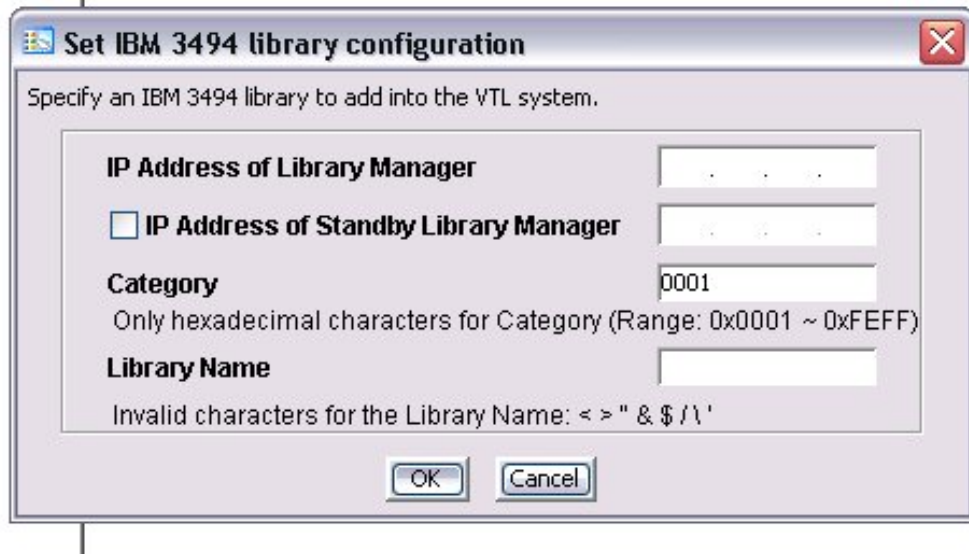
Figure 40. 3494 Tape Library configuration

2. __ In the ″Set IBM 3494 library configuration″ window:

   a. __ In the **IP Address of Library Manager** field, type the IP address of the primary Library Manager.

   b. __ (Optional)

      1) __ Select the **IP Address of Standby Library Manager** check box.

      2) __ In the **IP Address of Standby Library Manager**, type the IP address of the standby Library Manager.

   c. __ In the **Category** field, type the four-character hexadecimal volume category identifier. See the *IBM TotalStorage 3494 Tape Library Operator Guide* for more information about volume categories.

   d. __ In the **Library Name** field, type a name for the 3494 Tape Library.

   e. __ Click **OK**.

Importing and exporting tape cartridges

Importing data from physical tape to virtual tape offer the following advantages:

- Protection of data on existing physical tape cartridges
- Immediate recovery of data from physical tape

Exporting data to physical tape from virtual tape permits long-term archiving.

Depending upon the number of physical tape drives attached to the TS7500 Virtualization Engine, up to 32 import or export operations can run concurrently.

Importing data from a physical tape cartridge

The import function permits the following:

- Copying the contents of physical tape to virtual tape
- Directly accessing physical tape without copying the entire tape cartridge
- Recycling a physical tape cartridge

To import a physical tape cartridge, complete the following steps:

1. __ In the VE console, right-click a physical tape library or tape drive and click **Import Tape**.
2. __ Select the target virtual library and slot for import.

   Note: Select a drive or library with the same tape size capacity.

3. __ Choose one of the following:

   Copy Mode
   This mode copies the entire contents of a physical tape cartridge to a virtual tape cartridge and leaves the physical tape cartridge unchanged.

   Direct Access Mode
   This mode links a physical tape cartridge to its virtual counterpart. This gives the backup application immediate access to the data on the tape before the complete copy operation finishes. This is useful when restoring only a small amount of data from a physical tape cartridge. Direct access tape cartridges are write-protected: a tape drive can only read data from the tape cartridge; it cannot write data to it.

   Recycle Mode
   This mode copies only the first 10 MB of data from the physical tape cartridge. This attempts to preserve the tape header, plus or minus a few MB, without copying backup data. This is useful in making the ISV backup software aware of the cartridge when the data on the cartridge can be deleted.

4. __ Select the physical tape for import, based on either its barcode or its slot location. You can then use the same barcode for the virtual tape or you can enter a new barcode. You can also select a slot for the virtual tape.
5. __ Type a barcode for the virtual tape cartridge. You can use the physical tape cartridge's barcode.
6. __ Select a slot for the virtual tape cartridge.
7. __ Verify the information and then click **Finish** to import the physical tape cartridge.

Exporting data to a physical tape cartridge

The export function copies or moves the contents of a virtual tape cartridge to a physical tape cartridge. Because some third-party backup applications alter what they write to the tape depending on the type of cartridge used, the TS7500 Virtualization Engine only exports virtual tape cartridges to physical tape cartridges of the same media type. This guarantees that the backup application will accept the tape cartridge.

To export a physical tape cartridge, complete the following steps:
1. __ In the VE console, right-click a virtual tape cartridge and then click **Move to Vault**.
2. __ Select the tape cartridges for export.
3. __ If not already done, inventory the physical tape cartridges in the tape library by right-clicking the icon for the library and then clicking **Inventory**.
4. __ Expand **Virtual Vault**.
5. __ In the **Virtual Vault** list, right-click the virtual tape cartridge for export and select **Export Tape**.
6. __ Select the target export physical tape library.
7. __ Choose one of the following:

Copy Mode
> This mode copies the contents of the virtual tape cartridge to its physical counterpart and retains the virtual tape cartridge after the data transfer

Move Mode
> This mode moves the contents of the virtual tape to its physical counterpart and then removes the virtual tape from the system.
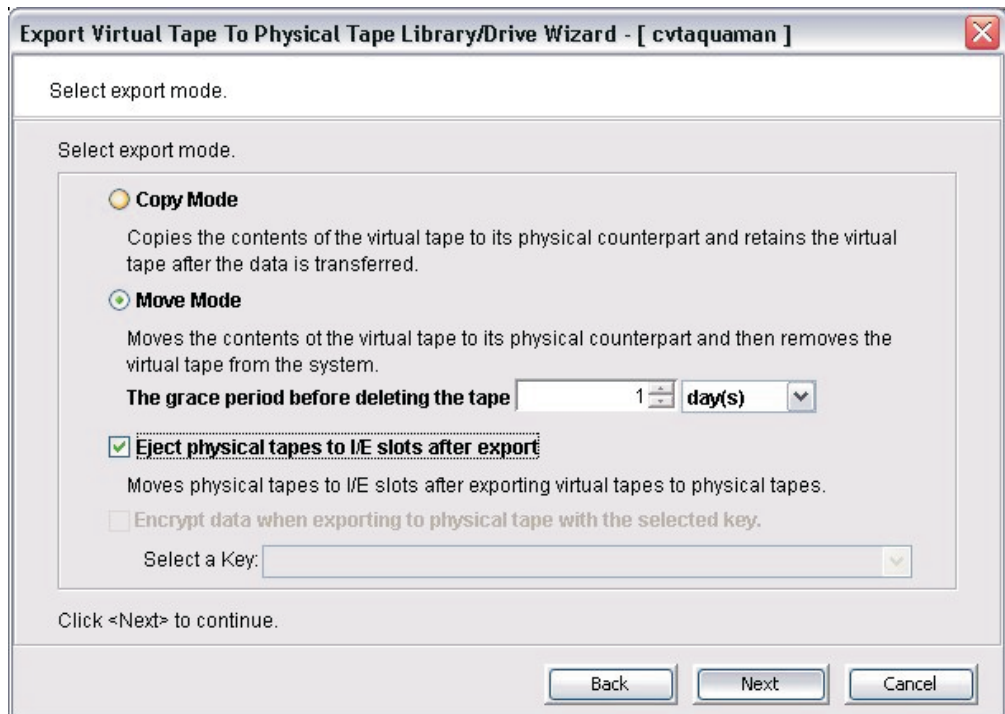
Figure 41. Selecting the export mode

8. __ Select the virtual tape cartridges for export.
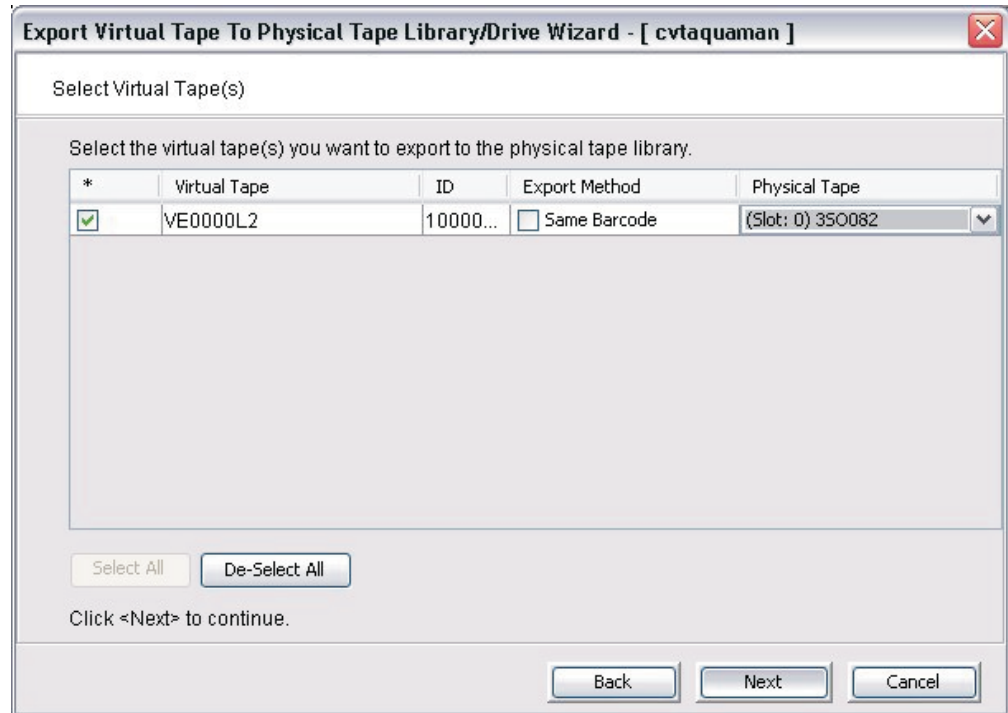
Figure 42. Selecting the virtual tape cartridges for export

9. __ Perform one of the following:

  • **The physical tape library uses barcodes.** Choose one of the following:

    – __ Use the virtual tape cartridge's barcode.

    – __ Type a new barcode.

  • **The physical tape library does not use barcodes.** __ Select a slot for the physical tape cartridge.

10. __ Verify the information and click **Finish** to export the virtual tape cartridge.
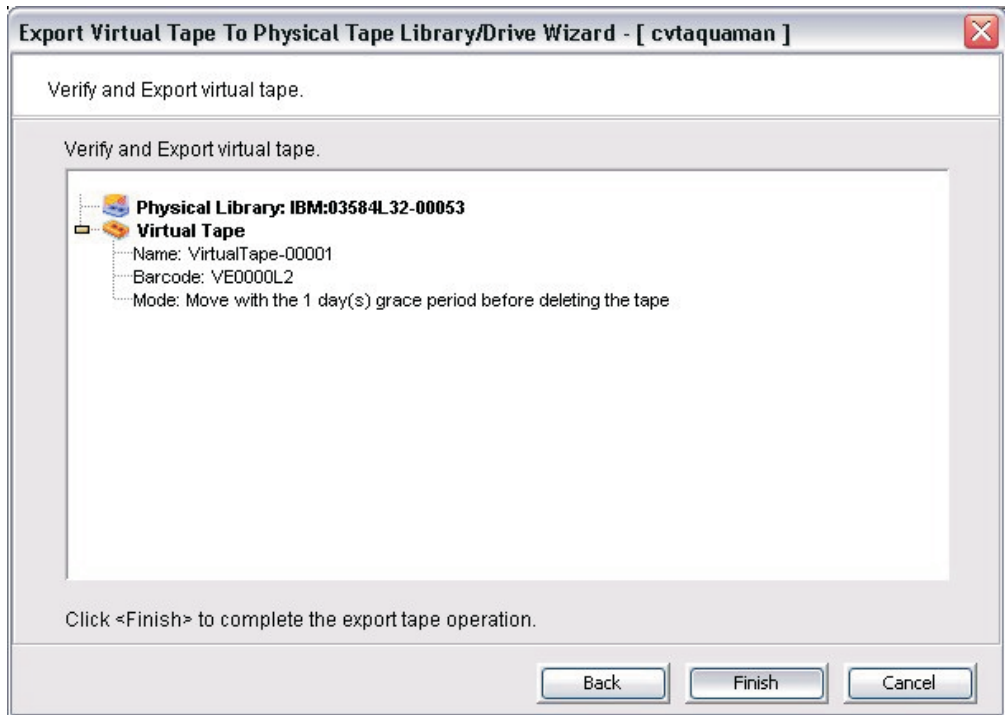
Figure 43. Verifying and exporting the virtual tape cartridge

Safeguarding the TS7500 Virtualization Engine configuration

The TS7520 Server stores its configuration information and virtual tape data in separate components:

- TS7520 Cache Controller
- TS7520 Cache Drawer

If the server becomes inoperable, the cache components maintain the virtual tape data intact. Saving the server configuration to a device other than the cache components helps expedite data recovery.

For stand-alone TS7500 Virtualization Engine installations, there are two options for saving the server configuration externally:

Auto Save
> The Auto Save function replicates the server configuration to another server. See "Auto Save" on page 57 for the procedure.

Save Configuration
> To save the server configuration manually to the workstation running the VE console, complete the following steps:
> 1. __ In the VE console main menu bar, click **Tools** → **Save Configuration**.
> 2. __ In the Save window:
>   a. __ Navigate to the folder where you want to store the server configuration file.
>   b. __ In the **File name** field, type a name for the server configuration file.

c.   __ Click **Save**.

> **Note:** For added protection, saving the configuration to removable media such as a floppy disk, a CD-ROM, or a USB flash memory device allows storage of the media in a secure location.

The TS7500 Virtualization Engine database residing on the disk storage in one TS7520 Cache Controller provides additional protection by mirroring itself to disk storage on another TS7520 Cache Controller. This protects the configuration if the disk storing the database is lost.

Auto Save

The Auto Save function provides consistent protection by periodically replicating server configuration to another location. Auto Save takes a point-in-time snapshot of the TS7500 Virtualization Engine configuration, including the following:

* virtual tape libraries
* virtual tape drives
* virtual tape cartridges
* clients
* client assignments
* replication settings
* Failover configuration

Attention: The server on which Auto Save stores the configuration information file must have an FTP server installed and enabled.

To enable and configure the Auto Save function, complete the following steps:

1.   __ In the VE console, right-click the server icon and then click **Properties**.
2.   __ In the Server Properties window, click the **Auto Save Config** tab.
3.   __ Select the **Enable Auto Save Configuration File** check box.
4.   __ Type configuration information in the following fields:

Ftp Server Name
> This should be the full name to ensure proper name resolution.

Ftp Port

Target Directory
> The directory on the FTP server where Auto Save stores the configuration file. Do not enter an absolute path; for example, for a target directory named `vtlconfig`, type `ftp\vtlconfig`, not `c:\vtlconfig`.

Username
> Auto Save uses this username to log in to the FTP server. You must create this account on the FTP server and give it read and write privileges to the target directory.

Password

Confirm Password

5.   __ From the **Interval** lists, select a value and a measure of time. Choose these values based on how frequently the configuration changes.

6. __ In the **Number of Copies** field, type a value or click the arrows to select a value. Auto Save deletes the earliest copy when it creates the latest copy.

7. __ Click **OK**.

Recovering server configuration after system replacement

If any hardware component of the TS7500 Virtualization Engine becomes inoperable, contact IBM for replacement options.

After installing the replacement, restore the original TS7500 Virtualization Engine configuration by completing the following steps:

1. __ Start the VE console by performing one of the following:
   - On the workstation's desktop, double-click the VE console icon.
   - Click **Start** → **Programs** → **IBM** → **VE for Tape** → **VE for Tape Console**.

2. __ Right-click the TS7500 Virtualization Engine server icon and then click **Add**.

3. __ In the **VE for Tape Server** field, type the server's full hostname or IP address.

4. __ In the **User Name** field, type `vetapeuser`.

5. __ In the **Password** field, type `veuserpassword`.

6. __ Click **OK**.

7. __ On the VE console main menu bar, click **Tools** → **Restore Configuration**.

8. __ In the VE for Tape Console window, click **OK**.

Mirroring the TS7500 Virtualization Engine database

The TS7500 Virtualization Engine saves its configuration database to an image in disk storage in one TS7520 Cache Controller. This image mirrors itself to disk storage in the other TS7520 Cache Controller. This protects the configuration information if the disk storing the database becomes inoperable.

Data written to the database is simultaneously written to the mirrored copy. If the database becomes unusable, the TS7500 Virtualization Engine automatically switches to the mirrored copy.

Viewing mirroring status

View mirroring status by completing the following steps:

1. __ In the VE console, expand **Virtual Tape Library System**.

2. __ Click the **Database** icon.

3. __ Click the **General** tab. The Mirror Synchronization Status list item has the following possible values:

   Synchronized
   > The primary and the backup database disks are synchronized. This is the normal state.

   Not synchronized
   > One of the database disks has failed or synchronization has not started.
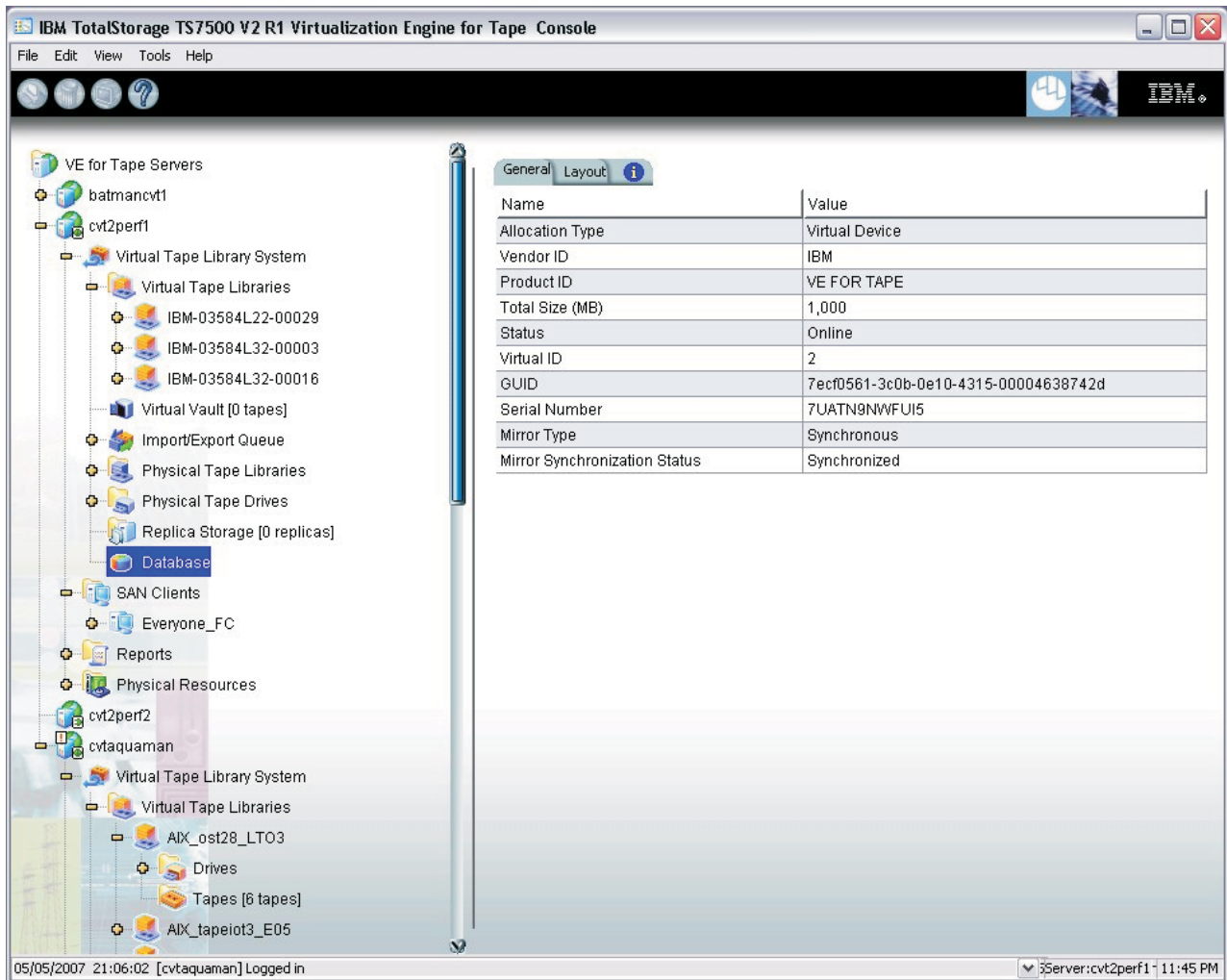
Figure 44. Mirroring configuration status

A progress bar showing percentage complete appears if the synchronization process is in progress.

Mirroring, recovery, and Failover

If mirroring is in progress when a Failover or recovery action occurs, the mirroring process will restart from its interruption point when the Failover or recovery action is complete. If fibre channel connectivity between the server and the cache components is lost, the mirror might become unsynchronized. The mirror will resynchronize automatically after completion of the Failover or recovery action. The mirror remains synchronized during a recovery action.

Managing users

Only an administrator can add or delete a TS7500 Virtualization Engine user or change a user's password.

To manage users, complete the following steps:

1. __ In the VE console, right click the server icon and then click **Administrators**.

Figure 45. VE for Tape User/Administrator Management window

There are two types of user:

Administrators
> Administrators can authorize clients and make changes in the VE console.

Read-only users
> Read-only users can only view information in the VE console. They cannot make changes in the VE console and they cannot authorize clients.

2. __ Choose an action:
- To add a user:
    a. __ In the VE for Tape User/Administrator Management window, click **Add**.
    b. __ In the **Administrator Name** field, type a name for the user. The name must conform to the conventions of the server's operating system. Refer to the operating system's documentation for naming restrictions.
    c. __ In the **Password** field, type the user's password.
    d. __ In the **Confirm Password** field, retype the user's password.
    e. __ From the **Group** list, select the type of user.
    f. __ Click **OK**.

Figure 46. Adding a user

- To delete a user:
  a. __ In the VE for Tape User/Administrator Management window, click a user.
  b. __ Click **Delete**.
  c. __ Click **Yes**.
- To reset a password:

  Note: You must log in as *vetapeuser* to reset a password.
  a. __ In the VE for Tape User/Administrator Management window, click a user.
  b. __ Click **Reset Password**.
  c. __ In the Reset for VE Tape User Password window:
     1) __ In the **Password** field, type the new password. The password must be at least 12 but no greater than 16 characters in length.
     2) __ In the **Confirm Password** field, type the new password again.
     3) __ Click **OK**.

Using compression

Enabling compression on virtual tape drives increases capacity. This increase directly relates to the compressibility of the data being backed up. The TS7500 Virtualization Engine incorporates software compression using an LZO algorithm that runs on the TS7520 Server. You can enable or disable compression for an entire virtual tape library, including all virtual tape drives.

Note: Using the compression option might impact performance.

Using compression allows backup software products to use their compression options. Backup software products commonly support the following two compression methods:

Device-side compression
       Tape drives compress data.

Client-side compression
Backup client software compresses data. Disabled if the server's compression option is also disabled.

Enabling and disabling compression

To enable or disable compression, complete the following steps:

1. __ In the VE console, right-click **Virtual Tape Library System** and select **Properties**.

2. __ In the Change Virtual Tape Library properties window:

   a. __ Select the **Enable Virtual Tape Library compression mode** check box.

   b. __ Click **OK**.

With server compression enabled, you can enable or disable compression on individual virtual tape drives by issuing SCSI commands from the operating of the server running backup software. To enable or disable virtual tape drive compression, perform one of the following:

Windows
Select or clear the option in the backup software that enables or disables hardware tape drive compression.

> **Note:** If TS7520 Server compression is disabled, enabling tape drive compression in this manner has no effect.

Linux®
Specify a compressed tape device file such as the following:

/dev/rmt/0cbn
To enable compression

/dev/rmt/0ubn
To disable compression

In the VE console, compression icons appear next to each virtual tape drive with compression enabled.

Viewing the event log

The event log contains a record of significant events occurring during TS7520 Serveroperation. To view the event log, complete the following steps:

1. __ In the VE console, click the server icon.

2. __ Click the **Event Log** tab.

Table 5 describes the columns visible in the event log.

Table 5. Event log

Column	Description	
Type	I	Informational message. No action is required.
	W	Warning message indicating a condition that might require maintenance or corrective action. The TS7500 Virtualization Engine remains operational.
	E	Error message indicating a failed device or operation or a licensing violation. Corrective action is required to resolve the cause of the error.
	C	Message of a critical error that can prevent proper system operation.
Date	The date an event occurred	
Time	The time an event occurred	
ID	The unique message identifier	
Event Message	Description of the event	

For more info about TS7500 Virtualization Engine error codes, see the *IBM Virtualization Engine TS7500 Error Codes* document.

Sorting the event log

The event log initially sorts information in chronological order with the most recent events at the top. To change how the log displays information, click a column heading. This sorts the event log alphabetically by the items in that column. For example, if you click the ID heading, the events sort numerically by ID number. To reverse the display order, click the column header again.

Filtering the event log

By default, the event log displays all informational system messages, warnings, and errors. To filter the displayed information, complete the following steps:

1. __ Click the **Event Log** tab.
2. __ Right-click the server icon and then click **Event Log** → **Filter**.
3. __ In the Event Log Options window, choose selection criteria:
   - Error types
   - Specific text
   - Maximum number of lines to display
   - Date and time range
4. __ Click **OK**.

Printing or saving the event log

You can print the event log or save it as a text file.

To print the event log, complete the following steps:

1. __ In the VE console, right-click the server icon and then click **Event Log** →
   Print.
2. __ In the Print window:
   a. __ Choose print options.
   b. __ Click **OK**.

To save the event log to a text file, complete the following steps:

1. __ In the VE console, right-click the server icon and then click **Event Log** →
   Export.
2. __ In the Save window:
   a. __ Navigate to the desired folder.
   b. __ In the **File name** field, type a name for the event log file.
   c. __ From the **Files of type** list, select a format:
      • __ Comma-delimited text
      • __ Tab-delimited text
   d. __ Click **OK**.

Purging the event log

To clear the contents of the event log, complete the following steps:

1. __ In the VE console, right-click the server icon and then click **Event Log** →
   Purge.
2. __ In the confirmation window:
   • __ Click **Yes** to save a copy of the event log before purging.
   • __ Click **No** to purge the event log without saving a copy.

Setting server properties

To set a server's properties, complete the following steps:

1. __ In the VE console, right-click the server icon and then click **Properties**.
2. __ In the Server Properties window, click the **Active Database Maintenance**
   tab and complete the following steps:
   a. __ In the **Maximum activity data file size (MB)** field, type a value or click
      the arrows to select a value.
   b. __ In the **Number of days of activities to keep** field, type a value or click
      the arrows to select a value.

   These actions specify settings for the activity log. The server uses information
   from the activity log to generate reports.
3. __ (Optional) Click the **SNMP Maintenance** tab and configure Simple Network
   Management Protocol (SNMP) management as described in "Sending SNMP
   traps" on page 65.
4. __ (Optional) Click the **Auto Save** tab and configure Auto Save as described in
   "Auto Save" on page 57.

5. __ Click the **Storage Monitoring** tab and type a value, or click the arrows to select a value, in the **Storage percentage full threshold** field. When storage use reaches this level, the event log records a warning message.

6. __ Click **OK**.

Sending SNMP traps

The TS7500 Virtualization Engine provides SNMP support to enable integration of the system's management into an existing enterprise management solution.

By default, event log messages will not be sent, but you may want to configure TS7500 Virtualization Engine to send certain types of messages. To do this, complete the following steps:

1. __ In the VE console, right-click the server icon and then click **Properties**.

2. __ Click the **SNMP Maintenance** tab and complete the following steps:

    a. __ In the **SysLocation** field, type the location to be reported to the Simple Network Management Protocol (SNMP) management station.

    b. __ In the **SysContact** field, type the contact information (for example, an person's name or an email address) to be reported to the SNMP management station.

    c. __ From the **Trap Level** list, select the threshold level of the events to be reported to the SNMP management station (see Table 5 on page 63 for more information):

    Informational
    > This level reports informational messages, warnings, error messages, and critical messages.

    Warning
    > This level reports warnings, error messages and critical messages.

    Error   This level reports error messages and critical messages.

    Critical
    > This level reports critical messages only.

    None   This level doesn't report any messages.

    d. __ If you selected a trap level other than **None**, complete the following steps:

    > 1) __ Click **Add**.
    >
    > 2) __ In the **Server Name** field, type the full hostname of the SNMP management server.
    >
    > 3) __ In the **Community** field, type the name of a valid SNMP community.
    >
    > 4) __ Click **OK**.

    e. __ Click **OK**.

3. __ (Optional) Verify proper setup by completing the following substeps:

    a. __ Perform steps 1 and 2 to configure SNMP management at a threshold of **Informational**.

    b. __ Disconnect from the server by right-clicking the server icon and then clicking **Disconnect**.

    c. __ Reconnect to the server by right-clicking the server icond and then clicking **Connect**. These two actions generate informational messages in the event log.

d. __ Verify that SNMP traps for the two events appear at the SNMP management station.

e. __ Perform steps 1 on page 65 and 2 on page 65 to configure SNMP management at the desired threshold.

Searching for virtual tape cartridges

You can use the VE console's search function to find virtual tape cartridges. To search for virtual tape cartridges, complete the following steps:

1. __ In the main menu bar, click **Edit → Search**.
2. __ In the **Find a tape by Barcode** field, type the tape cartridge's full barcode.
3. __ Click **Search**.

Adding and rolling back patches

The following sections contain procedures for adding and rolling back software patches.

Downloading and applying patches

Upon notification of a VE console patch, download and install the patch by completing the following steps:

1. __ In the VE console main menu bar, click **Tools → Add Patch**.
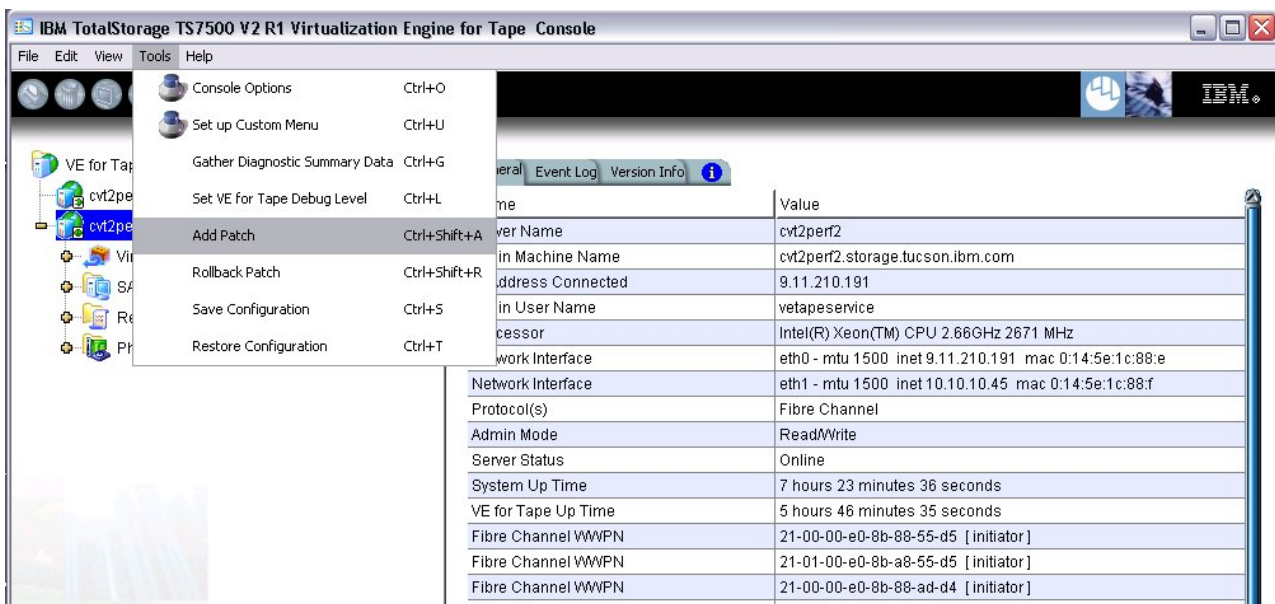
Figure 47. Adding a patch

2. __ In the Add Patch to VE for Tape Server window, click **OK**.

Figure 48. Add Patch to VE for Tape Server window

3. __ In the Select Patch File window, navigate to and select the patch file.
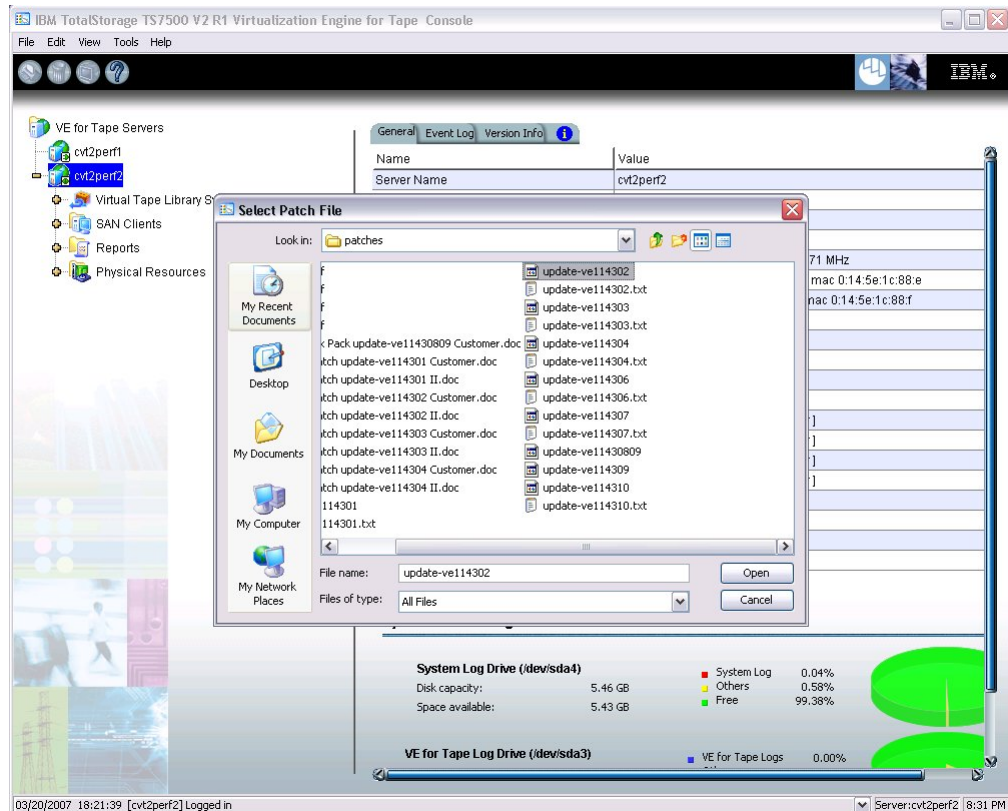
Figure 49. Selecting the patch file

4. __ Click **Open**.
5. __ In the confirmation window, type **yes** in the **Type YES to confirm** field and click **OK**.
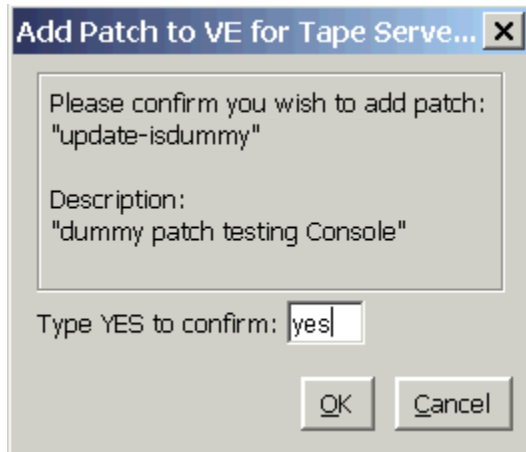
Figure 50. Confirmation window

> **Note:** The patch installation might restart the server.

Rolling back a patch

Roll back an installed patch by completing the following steps:

1. __ In the VE console main menu bar, click **Tools** → **Rollback Patch**.
2. __ In the Rollback Patch on VE for Tape Server window, click **OK**.

Figure 51. Rollback Patch to VE for Tape Server window

3. __ In the Rollback Patch window, select the patch for rollback and then click **OK**. To view the details of any patch listed, click the arrow button in the detail column for that patch. .
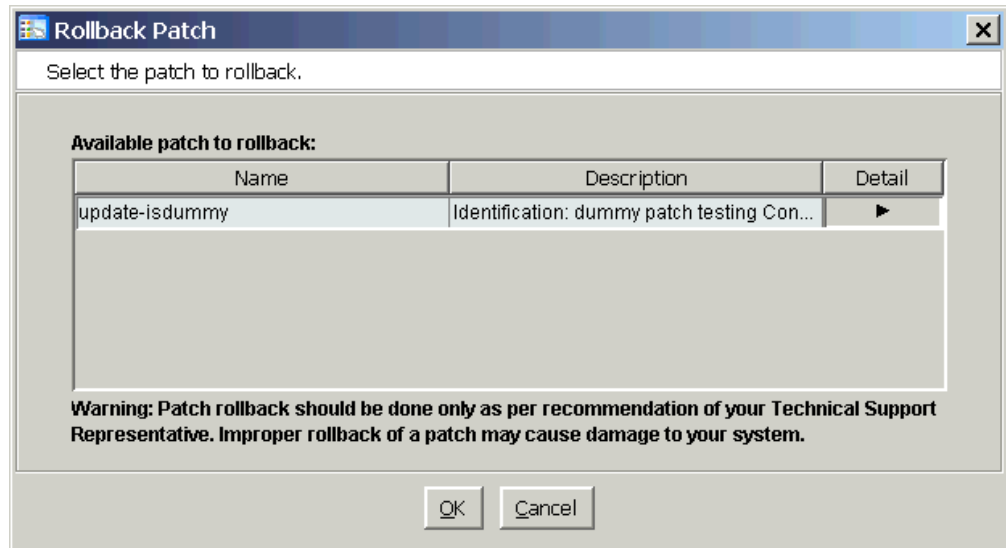
Figure 52. Selecing the patch to roll back

4. __ In the confirmation window, type **yes** in the **Type YES to confirm** field and click **OK**.
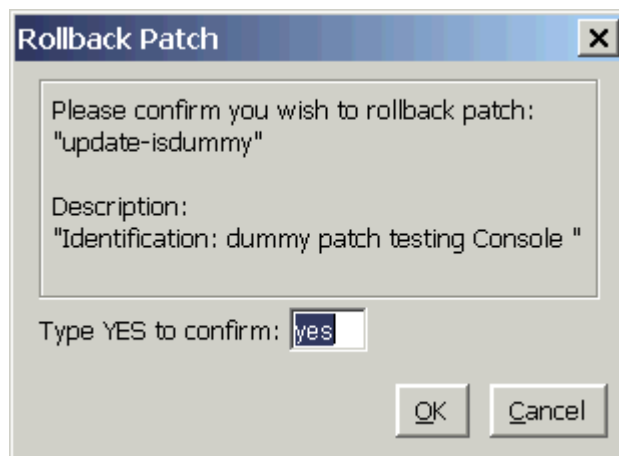
Figure 53. Confirmation window

> **Note:** The patch rollback might restart the server.

Power-off and power-on procedures

Power-off procedure

To turn off all components in the TS7500 Virtualization Engine, complete the following steps:

1. __ Open the front doors to all frames to view the drive fault LEDs on the front of all cache components.

2. __ Ensure that no drive fault LEDs (**1** in Figure 54 on page 70) are lit on any cache component. If any fault lights are lit, refer to the *Checking the LEDs* section of the *IBM Virtualization Engine TS7500 Problem Determination Guide*

to determine the cause and recommended course of action before proceeding.
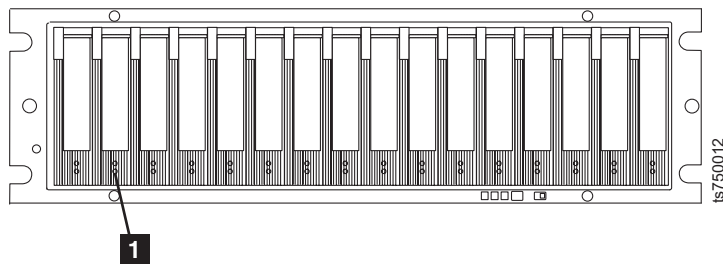
Figure 54. Drive fault LEDs

3. __ Suspend I/O from all host servers attached to the TS7500 Virtualization Engine

4. __ In Table 6, record the following information:
   - Server IP addresses
   - Base frame locations

Table 6. Server IP addresses and base frame locations

Server	Server IP address (from the Ethernet1 label on the rear of each server)	Base frame locations
Lower server, first base frame		
Upper server, first base frame (if installed)		
Lower server, second base frame (if installed)		
Upper server, second base frame (if installed)		

5. __ If you have a high availability installation and Failover is enabled, suspend Failover for servers in the first base frame:

   a. __ In the VE console, right-click the icon for a server in the first base frame.

   b. __ Click **Failover** → **Suspend Failover**.
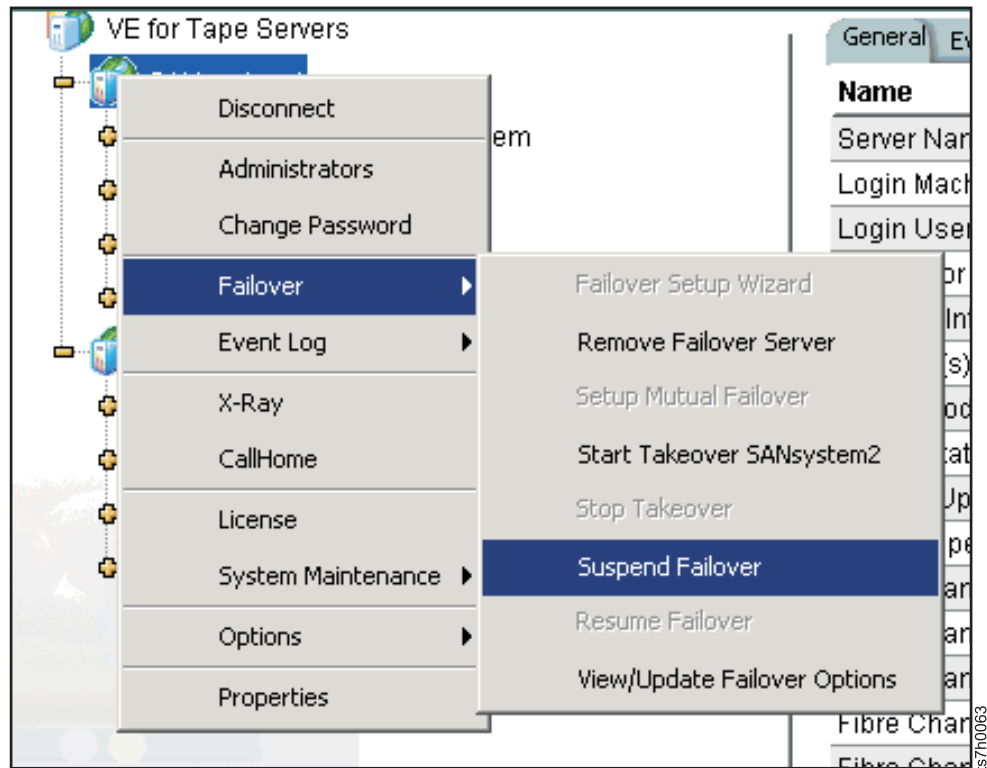
Figure 55. Suspending Failover

6. __ If you have a four-node high availability installation, repeat step 5 on page 70 for the servers in the second base frame.

7. __ In the VE console, click the icon of a server to be turned off.

8. __ In the **General** tab, verify that the **IP Address Connected** value matches the IP address you recorded for the server in Table 6 on page 70.

9. __ In the VE console, right-click the server icon and then click **System Maintenance** → **System Shutdown**. This action shuts down the server's operating system.
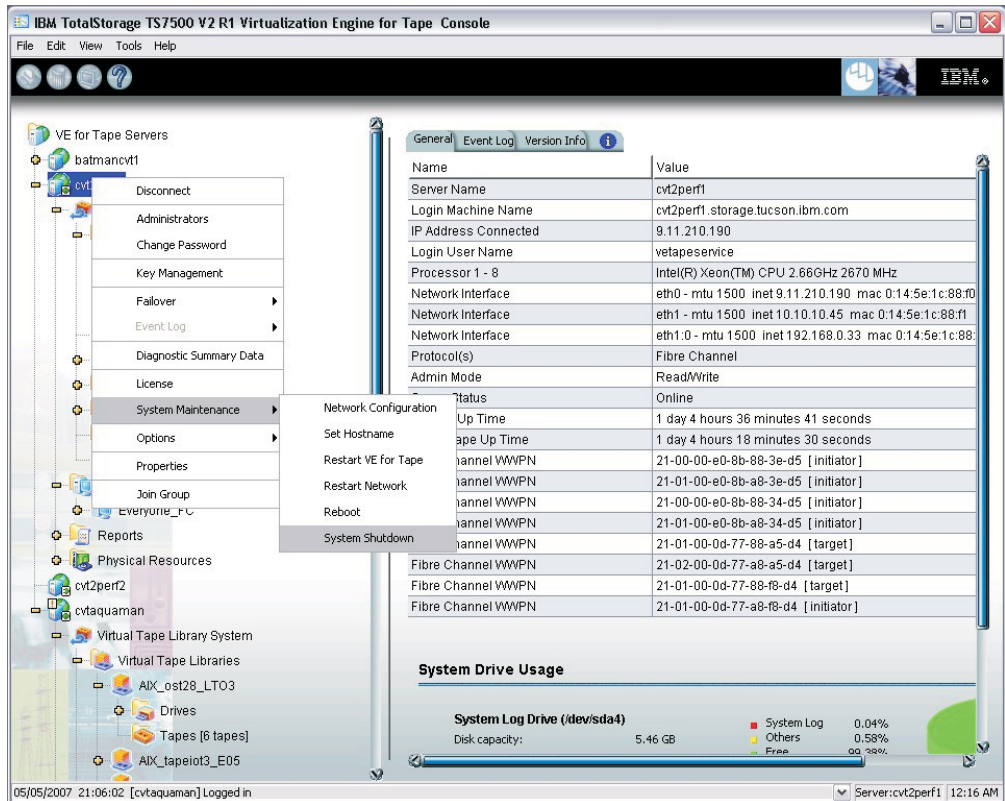
Figure 56. Turning off the server

10. __ In the System Maintenance window, click **Yes**.
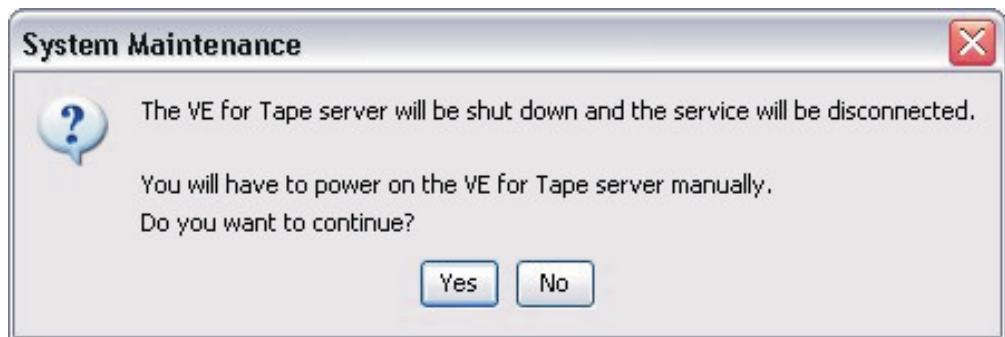
Figure 57. Shutdown confirmation

11. __ Open the base frame front door, observe the power-on LED on the server operator panel (**6** in Figure 58 on page 73), and perform one of the following:
   - **Lit and flashing:** the server is in the standby condition. Proceed to step 12 on page 73.
   - **Lit and steady:** the server is not in the standby condition. Press the white recessed power-control button on the server operator panel (**8** in Figure 58 on page 73) and proceed to step 12 on page 73.
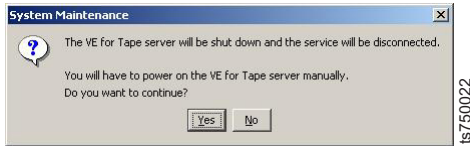
Figure 58. Server operator panel

12. __ If you have a high availability installation, repeat steps 7 on page 71 through 11 on page 72 for all remaining servers.

Important: The TS7520 Cache Drawers and TS7520 Cache Controllers are designed to run continuously. Turn off power to the TS7520 Cache Drawers and TS7520 Cache Controllers only if:

- Instructions in a hardware or software procedure require that you turn off the power.
- An IBM technical service support representative instructs you to turn off the power.
- A power outage or emergency situation occurs.
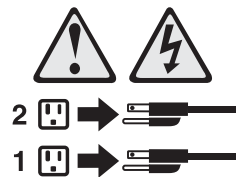
Figure 59. Power control caution statement

CAUTION:
The power control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

13. __ Turn off both power switches on the back of all TS7520 Cache Controllers.

14. __ Turn off both power switches on the back of all TS7520 Cache Drawers.

15. __ (Optional) Close all doors on all frames.

Performing an emergency shutdown

This topic contains the procedure to turn off the TS7500 Virtualization Engine in case of an emergency.

Attention: Emergency situations might include fire, flood, extreme weather conditions, or other hazardous circumstances. If a power outage or emergency situation occurs, always turn off all power switches on all computing equipment. This helps safeguard equipment from potential damage caused by electrical surges when power resumes. If the TS7520 Cache Controller or TS7520 Cache Drawer loses power unexpectedly, it might be due to a hardware failure in the power system or in the mid-plane of the TS7520 Cache Controller or TS7520 Cache Drawer.

1. __ Stop all activity and check all LEDs. Make a note of any Fault LEDs that are lit so that you can correct the problem when you turn on the power.

2. __ Check all LEDs on all components.
3. __ Note any lit fault LEDs. This facilitates correcting the problem when power resumes.
4. __ Turn off all power supply switches.
5. __ Unplug all power cables from all cache components.

Additional power information

The TS7500 Virtualization Engine supports dual-power supplies to its internal components. Always follow the power-on sequence in "Power-on procedure" during any attended power-on procedure.

Ideally, the TS7520 Cache Controllers and the TS7520 Cache Drawers recover automatically from unexpected shutdowns and unattended simultaneous restoration of power to system components. After power resumption, call IBM support if any of the following conditions occur:

- The storage subsystem logical drives and arrays do not come online.
- The storage subsystem logical drives and arrays seem to be degraded.

Note: Always wait at least 30 seconds between the time you turn off a power switch and the time you turn on the power again.

Power-on procedure

To turn on all components in the TS7500 Virtualization Engine, complete the following steps:

1. __ Ensure all power cords are connected to the control assemblies and to al components in all frames.
2. __ Inspect all cable connections (power and data) for positive seating.
3. __ Ensure that all SATA disk drive modules are seated securely in their slots in all cache components
4. __ Ensure that all power switches on all components in all frames are in the **OFF** (○) position.

> **Important:** If the installation contains TS7520 Cache Drawers, you must turn them on before turning on the installation's TS7520 Cache Controllers to ensure successful communication between the controllers and the drawers.

5. __ Press the power toggle buttons on the rear of all TS7520 Cache Drawers.
6. __ Wait at least 30 seconds.
7. __ Press the power toggle buttons on the rear of all TS7520 Cache Controllers.
8. __ On the first server in the first base frame, press the white recessed power-control pushbutton on the server operator panel.
9. __ If you have a high availability installation, repeat step 8 for all other servers.
10. __ Wait ten minutes to allow the servers to finish the start process. This ensures that the servers register in the VE console.
11. __ If you have a high availability installation and wish to resume Failover, complete the following substeps:
   a. __ In the VE console, click the icon for the first server in the first base frame and then click **Failover** → **Resume Failover**.
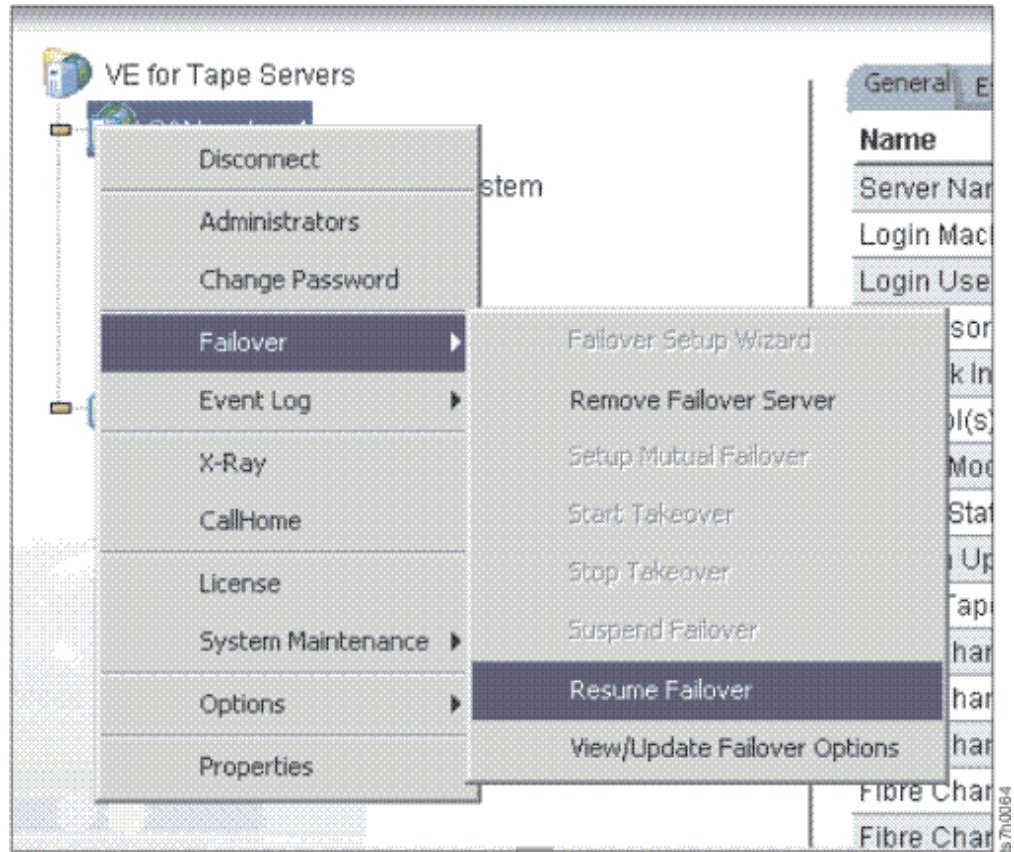
Figure 60. Resuming Failover

    b. __ If you have a four-node high availability installation, repeat step 11a on page 74 for the first server in the second base frame.

12. __ Ensure that no drive fault LEDs (**1** in Figure 61) are lit on any cache component. If any fault lights are lit, refer to the *Checking the LEDs* section of the *IBM Virtualization Engine TS7500 Problem Determination Guide* to determine the cause and recommended course of action before proceeding.
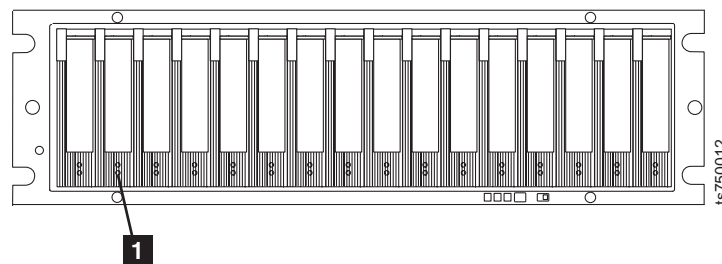
Figure 61. Drive fault LEDs

13. __ Resume I/O from all host servers attached to the TS7500 Virtualization Engine

    Note: It is not necessary to re-inventory physical tape cartridges after turning on the TS7500 Virtualization Engine if there are no changes to physical tape cartridges.

Chapter 4. Failover

The TS7500 Virtualization Engine Failover option provides high availability for the entire storage network, protecting the system from problems including:

- Internal storage device path failure
- TS7520 Server failure
- Cache component failure

Figure 62 compares a stand-alone configuration with potential points of failure to a high availability configuration. The TS7500 Virtualization Engine's high availability options work with redundant hardware to eliminate single points of failure.

**Basic
Virtualization Engine
Configuration
With Points of Failure**

Virtualization
Engine
hardware/
software failure

Storage device
connectivity failure

Storage device
failure

Storage
device

**High-Availability
Virtualization Engine
Configuration
(No Points of Failure)**

Heartbeat

Virtualization
Engine
Servers

Fibre Channel
Switches

Storage
Device

Tape data
replicated to
remote site

Figure 62. Failover

Storage device path failure

Cable or switch/router failure can cause storage device path failure. Providing a multiple path configuration eliminates this potential point of failure. Components of multiple path configuration include multiple fibre channel switches, multiple fibre channel cards, and storage devices with multiple controllers. In a multiple path configuration, the TS7500 Virtualization Engine automatically detects all paths to the storage devices. If one path fails, the TS7500 Virtualization Engine automatically switches to another.

Note: Fibre channel switches can demonstrate different behavior in a multiple path configuration. Before using this configuration with the TS7500 Virtualization Engine, verify that the configuration can work on your server without the TS7500 Virtualization Engine software by completing the following steps:

1. __ Use the hardware vendor's utility or the Linux **cat /proc/scsi/scsi** command to list the devices after loading the driver.

2. __ Use the hardware vendor's utility or the Linux **hdparm** command to access the devices.

3. __ Unplug the cable from one device and use the utilities listed above to verify continued operation.

4. __ Plug the first device back in, unplug the other device, and repeat the test to verify continued operation.

TS7520 Server and cache component failure

The TS7500 Virtualization Engine's Failover option provides high availability for operation by reducing service interruption caused by server hardware or software failure.

In the TS7500 Virtualization Engine Failover design, one TS7520 Server is configured to monitor another TS7520 Server. If the monitored server fails to communicate with its SAN clients, it is serving, the monitoring server will automatically assume its functions.

The TS7500 Virtualization Engine uses a unique system to ensure server health. This system includes a self-monitor and an intelligent heartbeat monitor.

The self-monitor is integral to both stand-alone and high availability TS7520 Servers. It provides continuous health and operational status to such system components as the VE console and supported network management applications through SNMP. The self-monitor checks the TS7520 Server's processes and connectivity to the server's cache components.

In a Failover configuration, one server's intelligent heartbeat function continuously monitors the primary server using the RSA port or the service port. The monitoring server evaluates the heartbeat data; the main possible states are:

- Normal operation (no Failover required)
- Detection of a fatal error in the TS7520 Server's processes that does not affect the network interface. In this case, the secondary server assumes the faulty server's duties to its clients.
- Detection of a connectivity failure between a server and a cache component device. The location of the failure is unknown. The heartbeat reports this error condition The secondary server determines whether it can access the device. If it can, it attempts to access all devices. If it can successfully access all devices, the secondary server assumes the first server's duties to its clients. If the secondary server cannot successfully access all devices, no action occurs.

Because the heartbeat shares the same network path as the server's clients, clients cannot access their resources whenever the heartbeat is unavailable. This situation is a *catastrophic failure*, because the server or the network connectivity is inoperable. In this case, the secondary server will immediately initiate a Failover as described above.

Failover terminology

This section describes Failover terminology.

Primary and secondary TS7520 Servers

> The primary and secondary servers are separate, independent TS7520 Servers. Each server has its own assigned clients. Each server monitors the other. If one server fails, the other takes over.

> The terms *primary* and *secondary* are from the client's perspective, since each server monitors the other. This is referred to as *mutual failover* or *active-active failover*. Each server is primary to its own clients and secondary to the other's clients. Each server normally serves its own clients. In the event one server fails, the other will take over and serve the failed server's clients.

Failover takeover

> Failover takeover occurs when the secondary server takes over the identity of the primary. Failover occurs under the following conditions:
> - One or more TS7500 Virtualization Engine processes fails.
> - Network connectivity fails because of, for example, defective HBAs or loose network cables.
> - Cache component path failure from one server
> - Power failure

> A failover takeover interrupts I/O for three minutes after initiation.

Recovery

> The secondary server transfers identity and virtual resources back to the primary server to allow it to resume operation. Caused by a result of an operator action.

> The recovery process interrupts I/O for three minutes after initiation.

Auto recovery

> Auto recovery occurs when the secondary server determines that the primary server is operational and returns control to it after a failover takeover. It determines this by monitoring the primary server after the Failover. If loss of network connectivity caused the Failover, auto recovery occurs with restoration of heartbeat-monitoring connections. If you use multiple IP addresses for health monitoring ,auto recovery initiates with the restoration of all network connections.

> Once the primary server again has control, the secondary server returns to its normal monitoring mode.

> **Note:** Auto recovery is disabled by default. See "Changing Failover interval settings" on page 99 for more information on using this feature.

In Figure 63 on page 80, both servers are monitoring each other in an active-active configuration. If server A fails, server B takes over and serves the clients of server A in addition to its own clients.
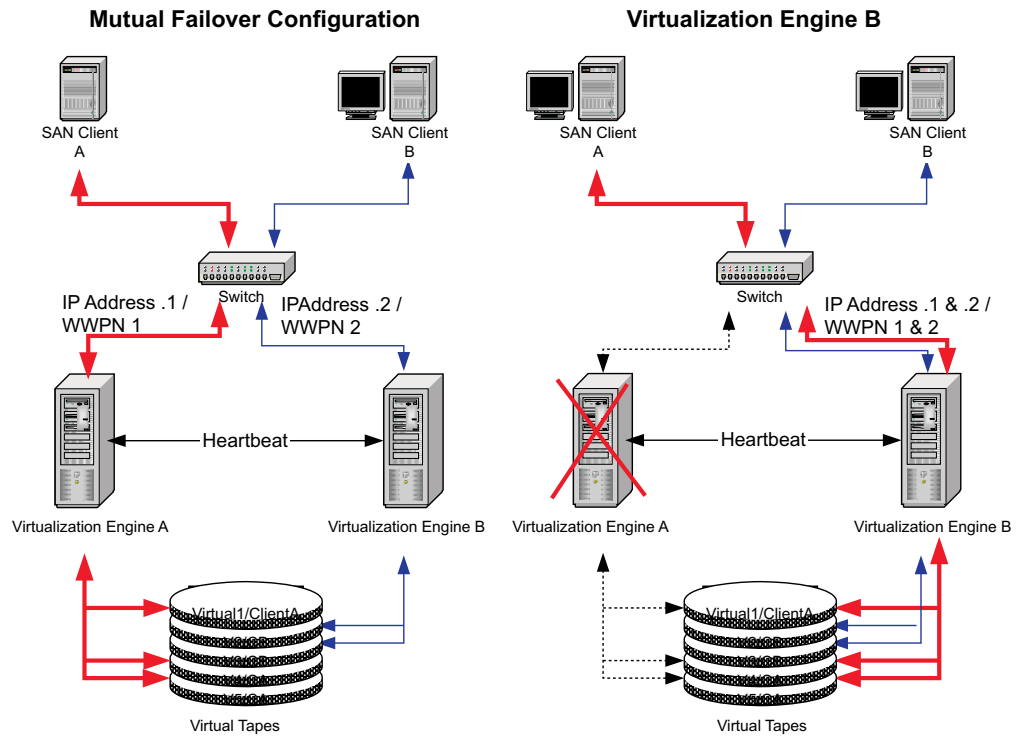
Figure 63. Failover configurations

Failover requirements

Failover requires the following configuration:

- Two or four TS7520 Servers must be present.
- Both servers must have the same TS7500 Virtualization Engine options licensed.
- The servers must have access to all common virtual devices. This means that storage devices must be attached in a multi-host SCSI configuration or attached on a fibre channel loop or switched fabric. In this configuration, both servers can access the same devices at the same time (both read and write).
- The eth0 and the eth1 ports for each server in a frame must have two IP addresses assigned:

  Network interface IP address
  > The network interface IP address is the address the servers use to connect to the VE console and the Ethernet network. The network interface IP addresses were assigned during initial network configuration.

  Service IP address
  > The service IP address is the address that the servers use to monitor each other's status for Failover. You assign the service IP addresses during the Failover Setup Wizard.

  All of these IP addresses must be static.

  Note: TS7500 Virtualization Engine clients and the VE console cannot use the service IP address to connect to a server.
- The following network conditions are required:

– The four IP addresses (network interface and service) for the eth0 ports of both servers must be on the same network or subnet.

– The four IP addresses (network interface and service) for the eth1 ports of both servers must be on the same network or subnet.

– The two IP addresses for the eth0 port (network interface and service) for each server must be on a different network or subnet from the two IP addresses for the eth1 port (network interface and service) for the same server. For instance, the eth0 port's IP addresses for the upper server must be on a different network or subnet from the eth1 port's IP addresses for the upper server. The same requirement applies for the lower server.

See "Two-node and four-node TS7500 EE installations" on page 7 for examples of these requirements.

Failover setup

Attention:

- Your IBM service representative set up Failover during initial system installation. Perform this procedure only if you want to change the Failover configuration.
- During this procedure, you assign two types of IP address to the two Ethernet ports for each server. The setup wizard uses the following terms for these addresses:

  Network interface IP address
  The network interface IP address is the address the servers use to connect to the VE console and the Ethernet network. The network interface IP addresses were assigned during initial network configuration; during this procedure, you look up these existing IP addresses and enter them in the Failover Setup Wizard.

  Service IP address
  The service IP address is the address that the servers use to monitor each other's status for Failover. During this procedure, you assign two service IP addresses to each server in the Failover Setup Wizard. Before starting this procedure, obtain four available IP addresses from your network administrator and record them in rows 3 and 5 of Table 7 on page 85.

- The following network conditions are required:
  - The four IP addresses (network interface and service) for the eth0 ports of both servers must be on the same network or subnet.
  - The four IP addresses (network interface and service) for the eth1 ports of both servers must be on the same network or subnet.
  - The two IP addresses for the eth0 port (network interface and service) for each server must be on a different network or subnet from the two IP addresses for the eth1 port (network interface and service) for the same server. For instance, the eth0 port's IP addresses for the upper server must be on a different network or subnet from the eth1 port's IP addresses for the upper server. The same requirement applies for the lower server.

  See "Two-node and four-node TS7500 EE installations" on page 7 for examples of these requirements. Before starting this procedure, consult your network administrator and obtain four available IP addresses (for use as service IP addresses) that meet these requirements and record them in rows 3 and 5 of Table 7 on page 85.

- If you want to change the server's fibre channel port modes from target to initiator or initiator to target, you must do so before enabling Failover. See "Switching a port between target mode and initiator mode" on page 38.

- You can run the Failover Setup Wizard on either the upper server or the lower server in the frame. If you choose the upper server, the wizard uses the term *secondary server* for the lower server. If you choose the lower server, the wizard uses the term *secondary server* for the upper server. This procedure assumes that you run the wizard on the lower server; for the sake of consistency, the example screen captures in this procedure show the wizard running on the lower server.

1. __ If not already connected, connect to both servers using the procedure in "Connecting to the TS7500 Virtualization Engine" on page 12.

2. __ Ensure that neither server is a member of a multi-node server group. See Chapter 16, "Multi-node server groups," on page 183 for more information about multi-node server groups and for the procedure to remove a server from a multi-node server group.

3. __ Ensure that both the eth0 and eth1 ports on both servers have static IP addresses defined. See "Setting network information" on page 12 for the procedure to define static IP addresses.

4. __ Ensure the following services and features are set the same for both servers (for example, if iSCSI is enabled for the lower server, it must also be enabled for the upper server; if CallHome is disabled for the lower server, it must also be disabled for the upper server):

   • __ iSCSI (see Chapter 9, "iSCSI," on page 147)

   • __ Hosted Backup (see Chapter 13, "Hosted Backup," on page 169)

   • __ NDMP (see Chapter 14, "NDMP," on page 171)

   • __ CallHome (see Chapter 15, "CallHome," on page 175)

5. __ In the VE console, perform the following substeps (see Figure 64):

   a. __ Click the icon for the lower server.

   b. __ Click the **General** tab.

   c. __ Record the lower server's *hostname* (**1** in Figure 64) in row **1** of Table 7 on page 85.

   d. __ Record the lower server's *Adapter 1 (eth0) network interface IP address* (**2** in Figure 64) in row **2** of Table 7 on page 85.

   e. __ Record the lower server's *Adapter 2 (eth1) network interface IP address* (**3** in Figure 64) in row **3** of Table 7 on page 85.
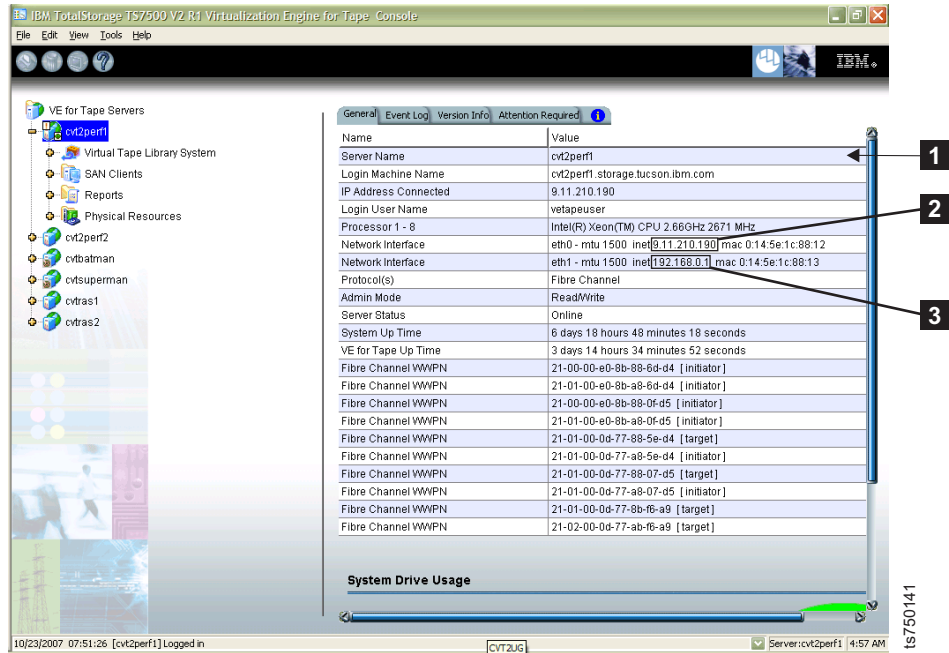
Figure 64. Determining hostname and network interface IP addresses

6. __ Repeat step 5 for the upper server.

7. __ If you have not already done so, record in rows **4** and **5** of Table 7 the service IP addresses you obtained from your network administrator that you wish to assign to Adapters 1 (eth0 port) and 2 (eth1 port) in each server.

Table 7. Failover setup information

Row	Item	Lower server	Upper server
1	hostname		
2	Adapter 1 (eth0 port) network interface IP address		
3	Adapter 2 (eth1 port) network interface IP address		
4	Adapter 1 (eth0 port) service IP address		
5	Adapter 2 (eth1 port) service IP address		

8. __ Ensure that the IP addresses recorded in Table 7 meet the requirements:
   - __ The four IP addresses (network interface and service) for the eth0 ports of both servers must be on the same network or subnet.
   - __ The four IP addresses (network interface and service) for the eth1 ports of both servers must be on the same network or subnet.
   - __ The two IP addresses for the eth0 port (network interface and service) for each server must be on a different network or subnet from the two IP addresses for the eth1 port (network interface and service) for the same server. For instance, the eth0 port's IP addresses for the upper server must be on a different network or subnet from the eth1 port's IP addresses for the upper server. The same requirement applies for the lower server.

   See "Two-node and four-node TS7500 EE installations" on page 7 for examples of these requirements.

9. __ Right-click the icon for one of the servers and then click **Failover** →
Failover Setup Wizard. Figure 65 shows this step for the lower server. The
Failover Setup Wizard starts.
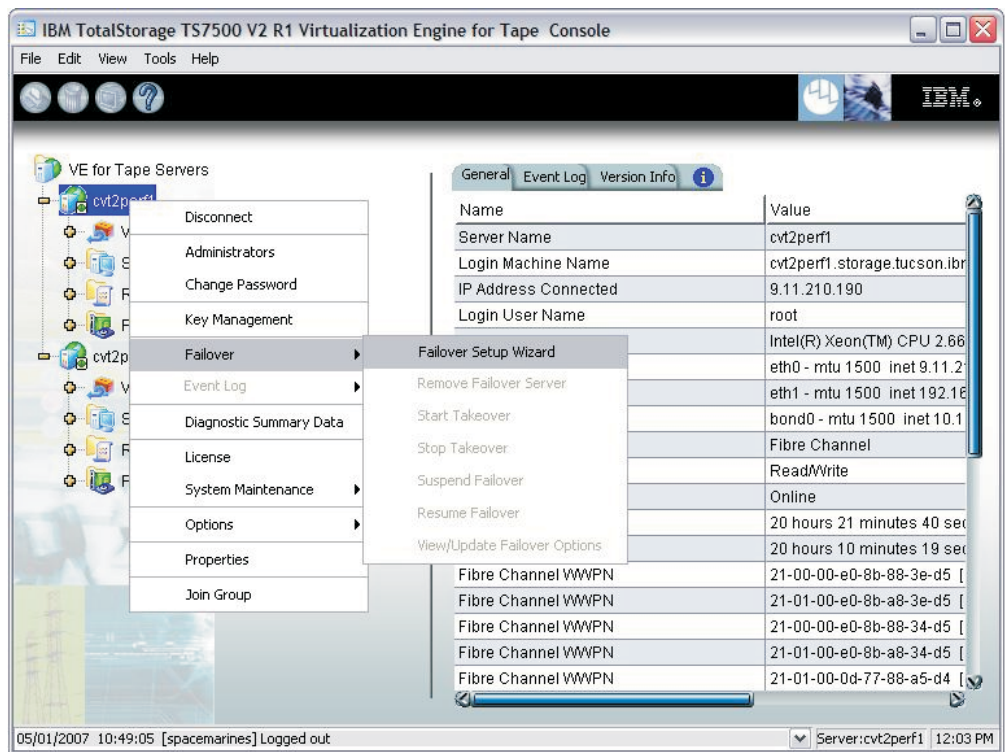
Figure 65. Starting the Failover Setup Wizard

10. __ In the Select the Secondary Server window (see Figure 66):

    a. __ From the **VE for Tape Server** list, select the hostname of the secondary server. The secondary server is the other server in the frame. For instance, if you started the Failover Setup Wizard on the lower server in the frame, the secondary server is the upper server. You recorded the hostname for both servers in row **1** of Table 7 on page 85.
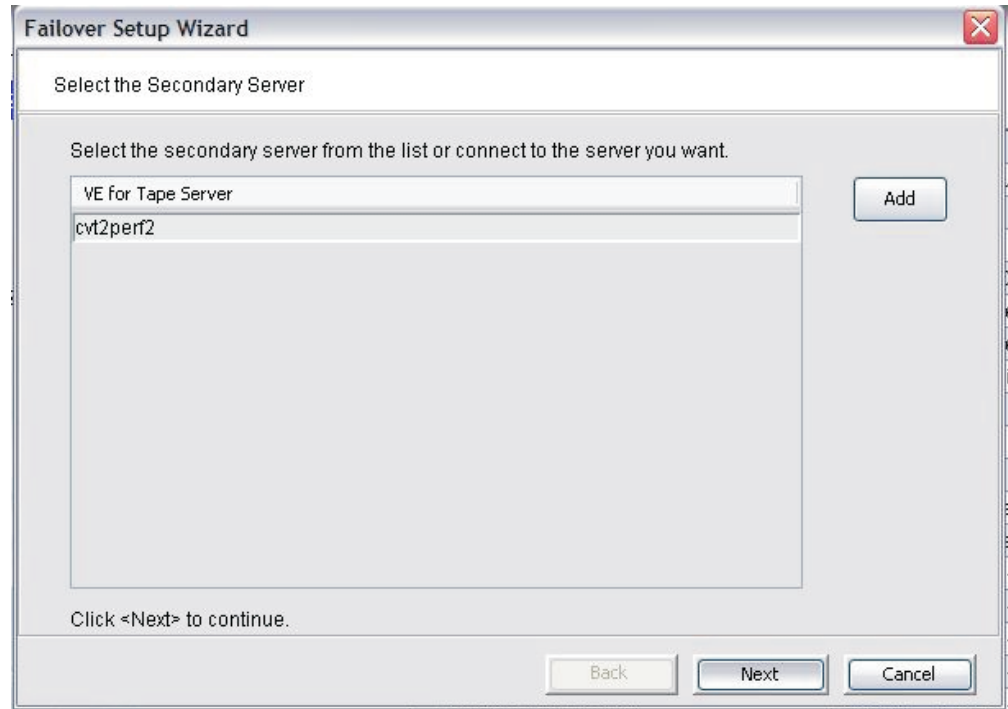
Figure 66. Select the Secondary Server window

    b. __ Click **Next**.

11. __ Perform one of the following:

- __ If the ″Rescanning Physical Devices is required″ window (Figure 67) opens, proceed to step 12.
- __ If the Enter the IP addresses of the Servers (Adapter 1) window (Figure 71 on page 92) opens, proceed to step 16 on page 92.

12. __ In the ″Rescanning Physical Devices is required″ window (Figure 67), click **OK**.

Figure 67. ″Rescanning Physical Devices is required″ window

13. __ In the ″Virtual Device or Service Enabled Device...″ window (Figure 68), click **OK**.
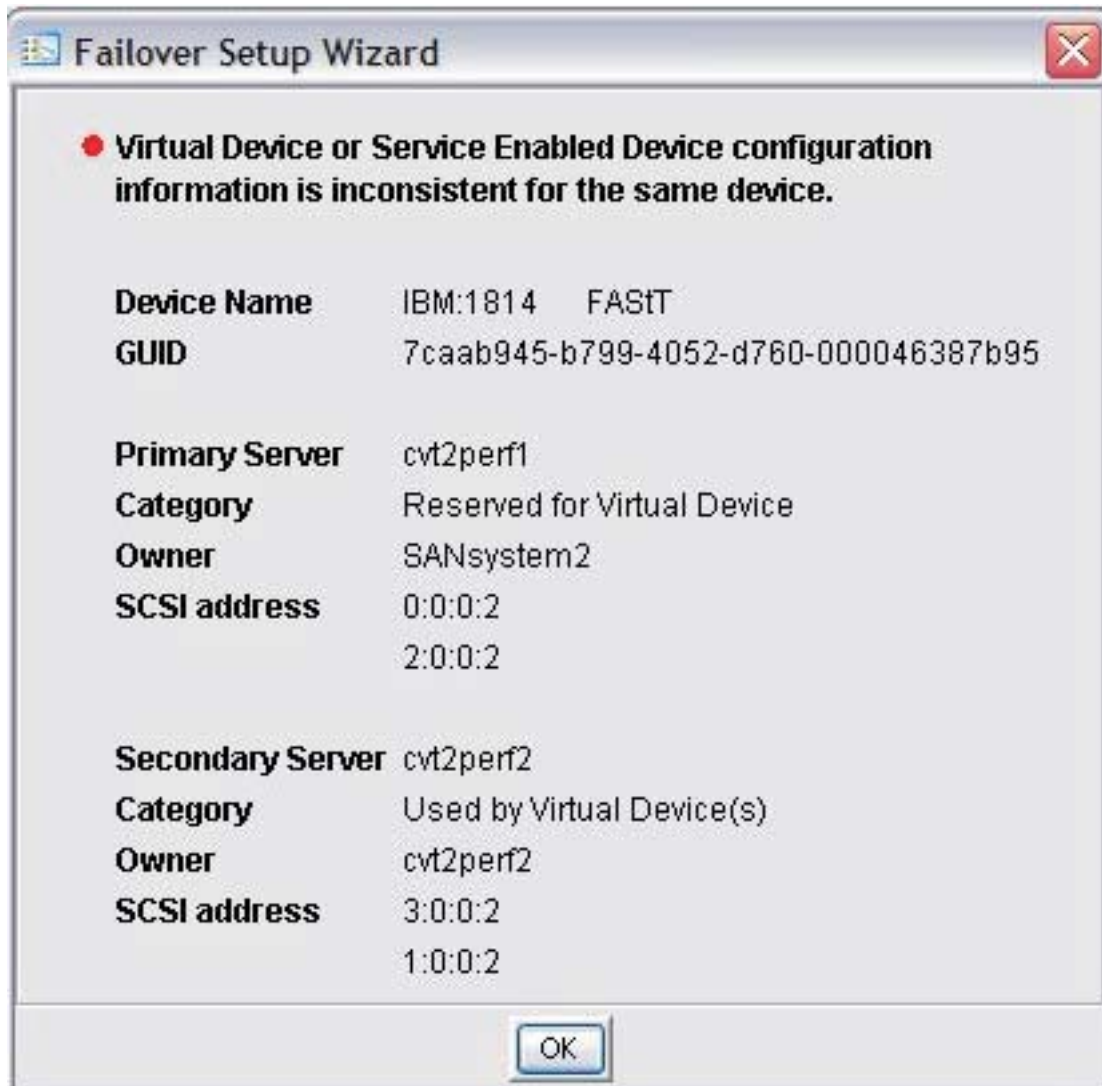
Figure 68. Summary of inconsistent device information

14. __ In the VE console (Figure 69):
   a. __ Expand the icon for the lower server.
   b. __ Right-click **Physical Devices** and then click **Rescan**.
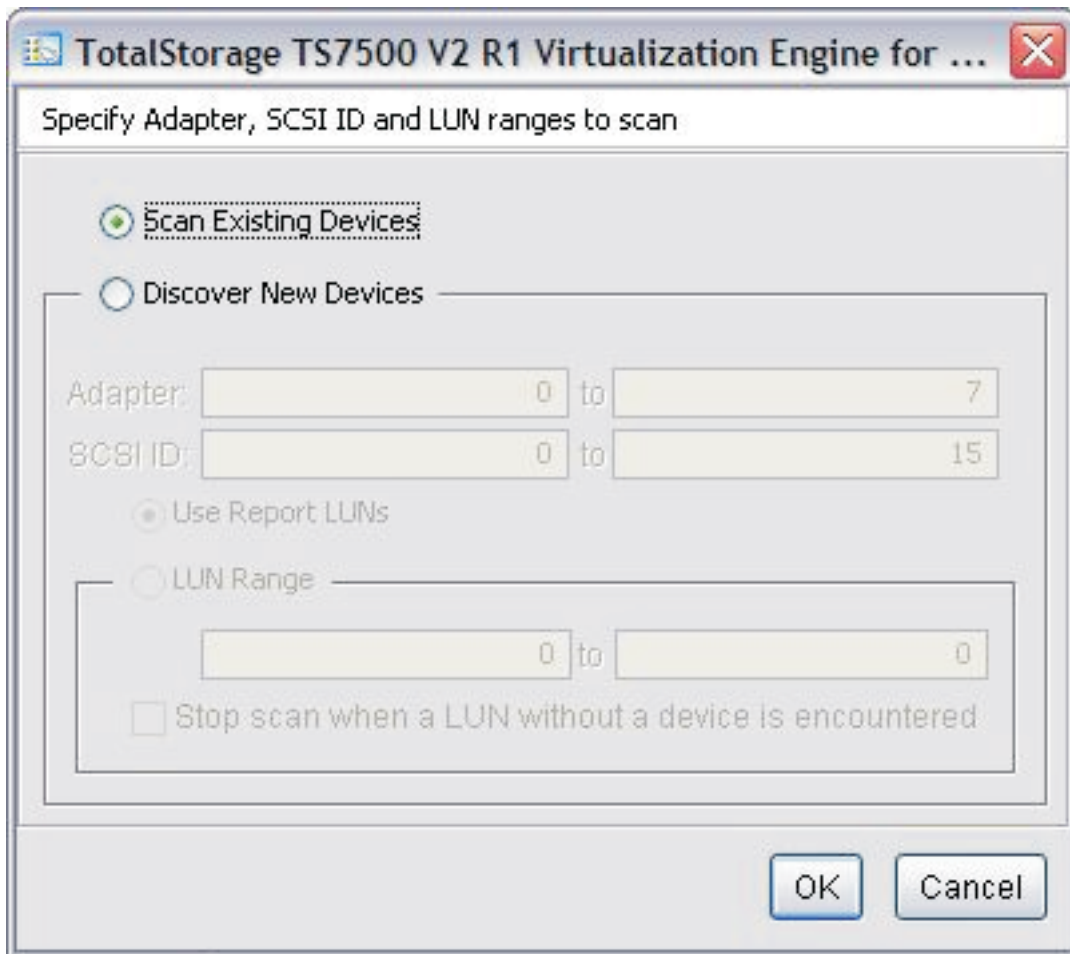
Figure 69. Rescanning physical devices

c. __ In the ″Specify Adapter, SCSI ID and LUN ranges to scan″ window (Figure 70):

1) __ Click **Scan Existing Devices**.

2) __ Click **OK**.

Figure 70. Scanning existing devices

15. __ Return to the Failover Setup Wizard.

16. __ In the Enter the IP addresses of the Servers (Adapter 1) window (Figure 71):

   a. __ In the IP address fields, confirm that the wizard retrieved and filled in the network interface IP addresses for adapter 1 (eth0) for the servers. You recorded this information in row **2** of Table 7 on page 85. If the wizard did not automatically fill in these values, type them in the IP address fields.

Figure 71. Entering or confirming network interface IP addresses for adapter 1

   b. __ Click **Next**.

17. __ In the Enter Service IP addresses for the Servers (Adapter 1) window (Figure 72):

    a. __ In the IP address fields, type the service IP addresses for adapter 1 (eth0) for the lower and upper servers. You recorded this information in row **4** of Table 7 on page 85.

Figure 72. Entering or confirming service IP addresses for adapter 1

    b. __ Click **Next**.

18. __ In the Enter the IP addresses of the Servers (Adapter 2) window (Figure 73):

  a. __ In the IP address fields, confirm that the wizard retrieved and filled in the network interface IP addresses for adapter 2 (eth1) for the lower and upper servers. You recorded this information in row **3** of Table 7 on page 85. If the wizard did not automatically fill in these values, type them in the IP address fields.
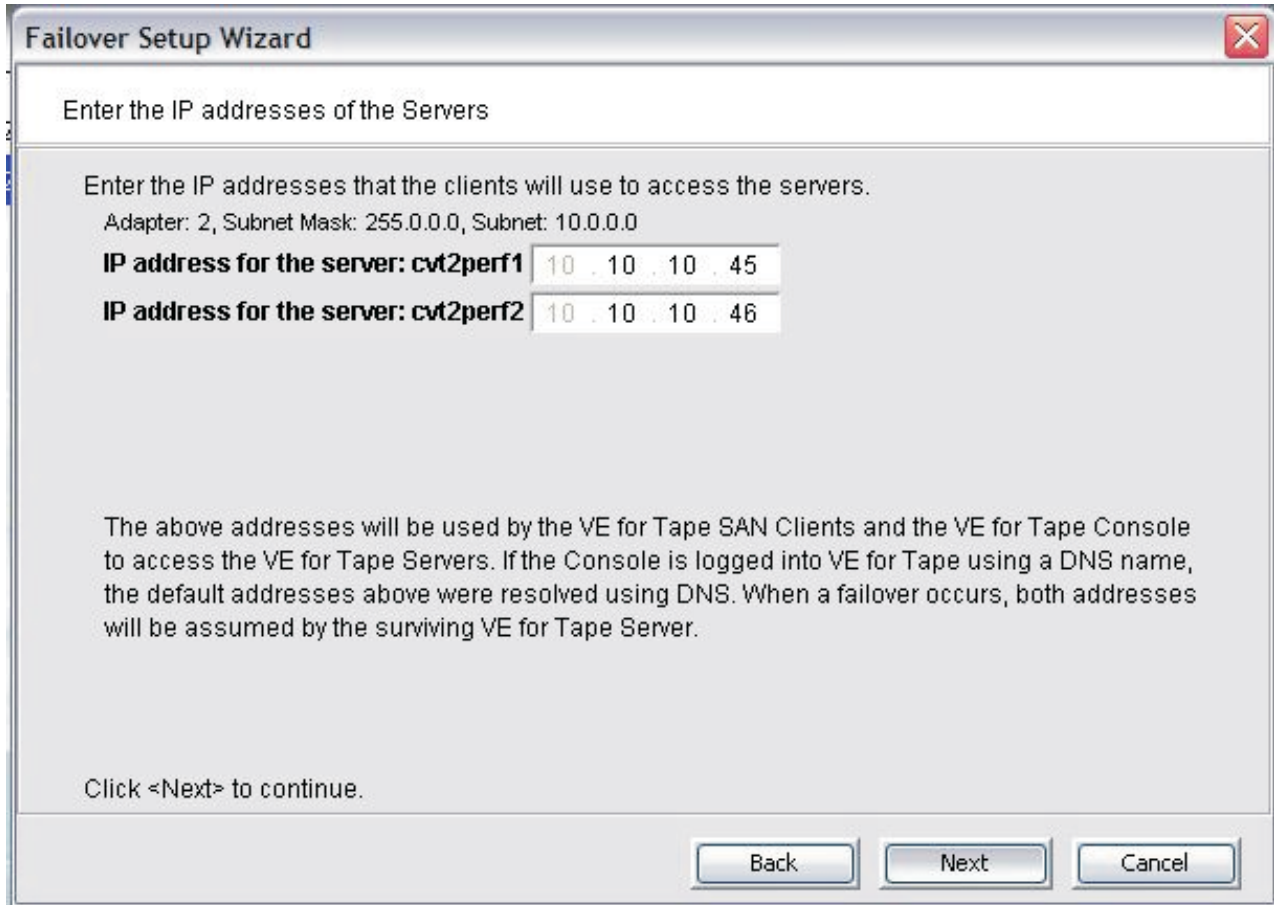
Figure 73. Entering or confirming network interface IP addresses for adapter 2

  b. __ Click **Next**.

19. __ In the Enter Service IP addresses for the Servers (Adapter 2) window (Figure 74):

a. __ In the IP address fields, type the service IP addresses for adapter 2 (eth1) for the lower and upper servers. You recorded this information in row **5** of Table 7 on page 85.
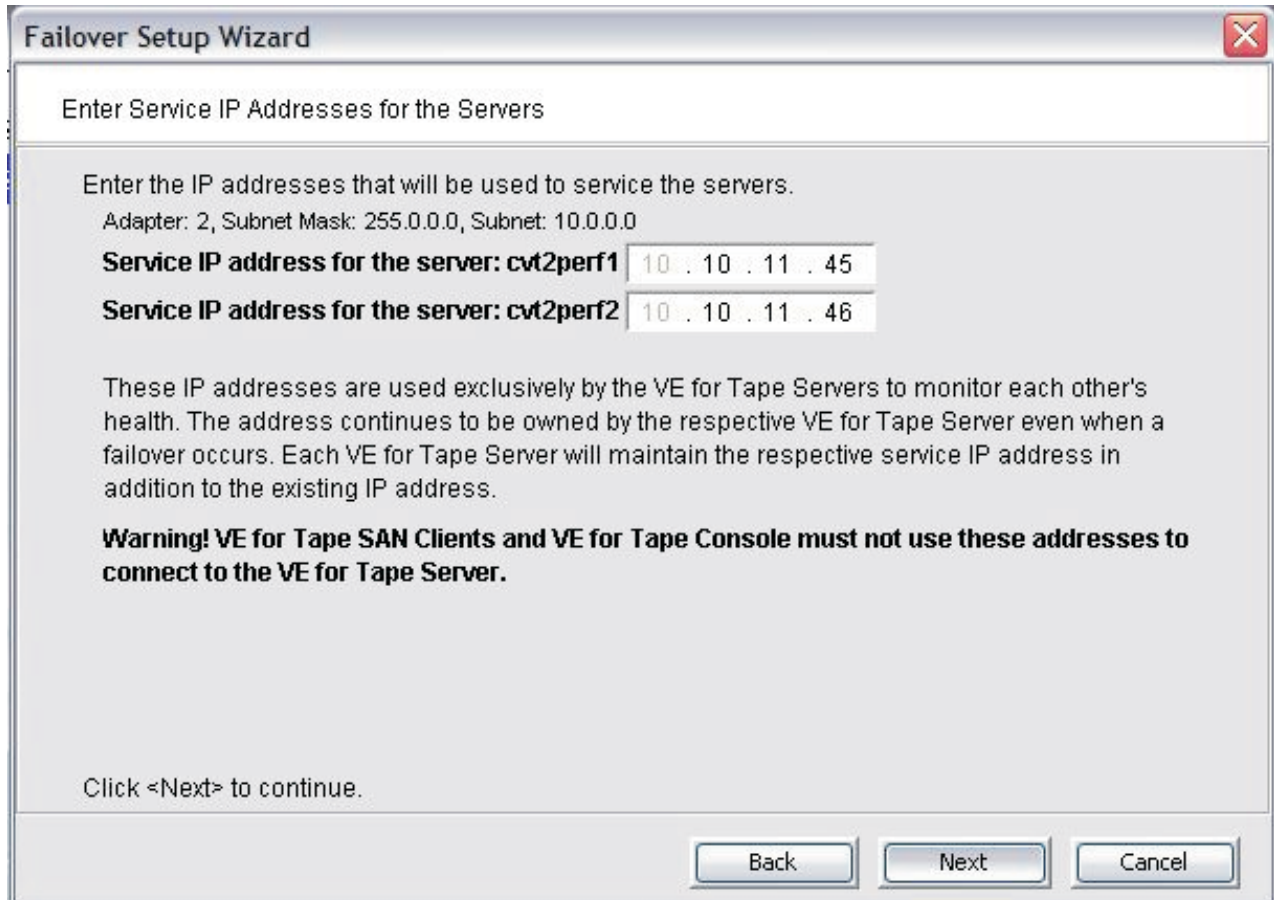
Figure 74. Entering or confirming service IP addresses for adapter 2

b. __ Click **Next**.

20. __ In the Confirm the Failover Configuration window (Figure 75), verify that the entered information is correct and click **Finish**.
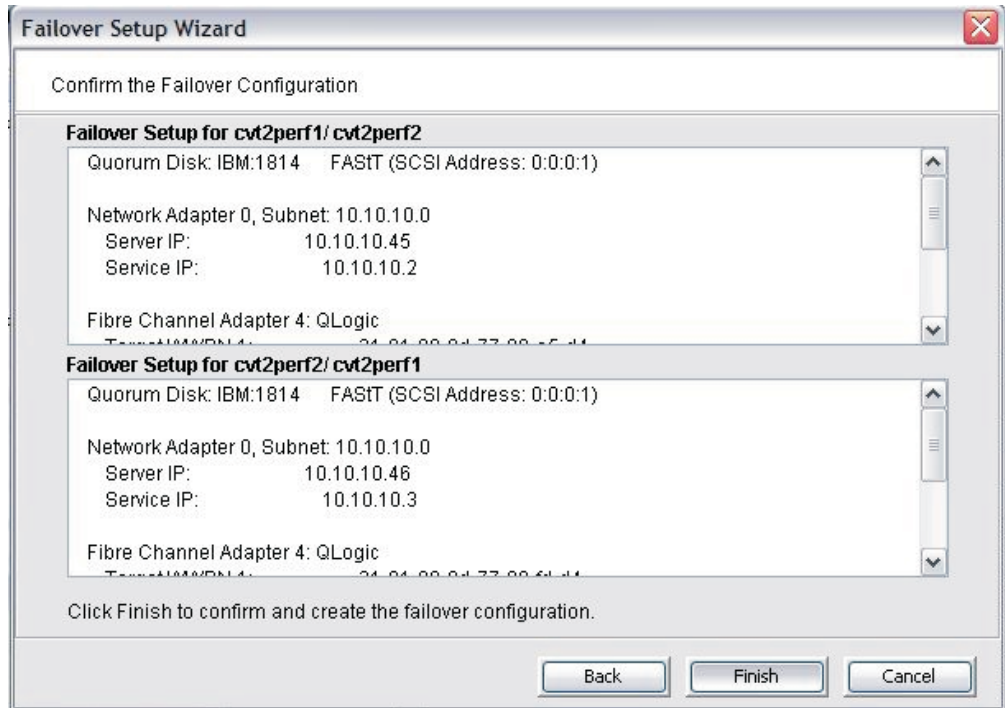
Figure 75. Confirm the Failover Configuration window

21. __ In the Successful Configuration Notification window, click **OK**.
22. __ Verify successful configuration by performing the following substeps:
    a. __ In the VE console, click a server icon.
    b. __ Click the **General** tab.
    c. __ Verify that the server status is **Online**.
    d. __ Click the **Failover Information** tab.
    e. __ Verify that the Failover State is **Normal**.
    f. __ Verify that the Failover Suspended value is **No**.
    g. __ Repeat the substeps above for the other server.

With Failover enabled, connecting to one server in the VE console automatically connects to the other also.

For Failover issues relating to specific drivers, refer to "Failover driver issues" on page 103.

Note: If Failover setup fails during the setup configuration stage (for example, one server saves the configuration but the other server loses connectivity while saving), you can remove the Failover server to delete the partially saved configuration. You can then create a new Failover configuration. See "Removing a Failover server" on page 101.

You can change some Failover properties by right-clicking a server icon and then clicking **Failover** → **View/Update Failover Options**. See Figure 76.
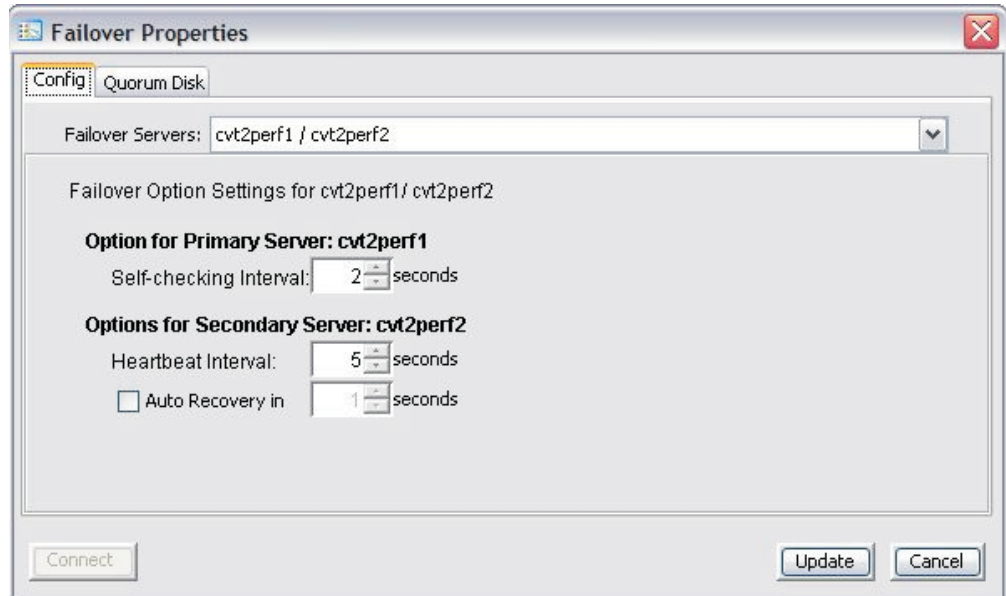
Figure 76. Failover Properties window

Checking Failover status

You can view current Failover configuration status on the server's **Failover Information** tab in the VE console.
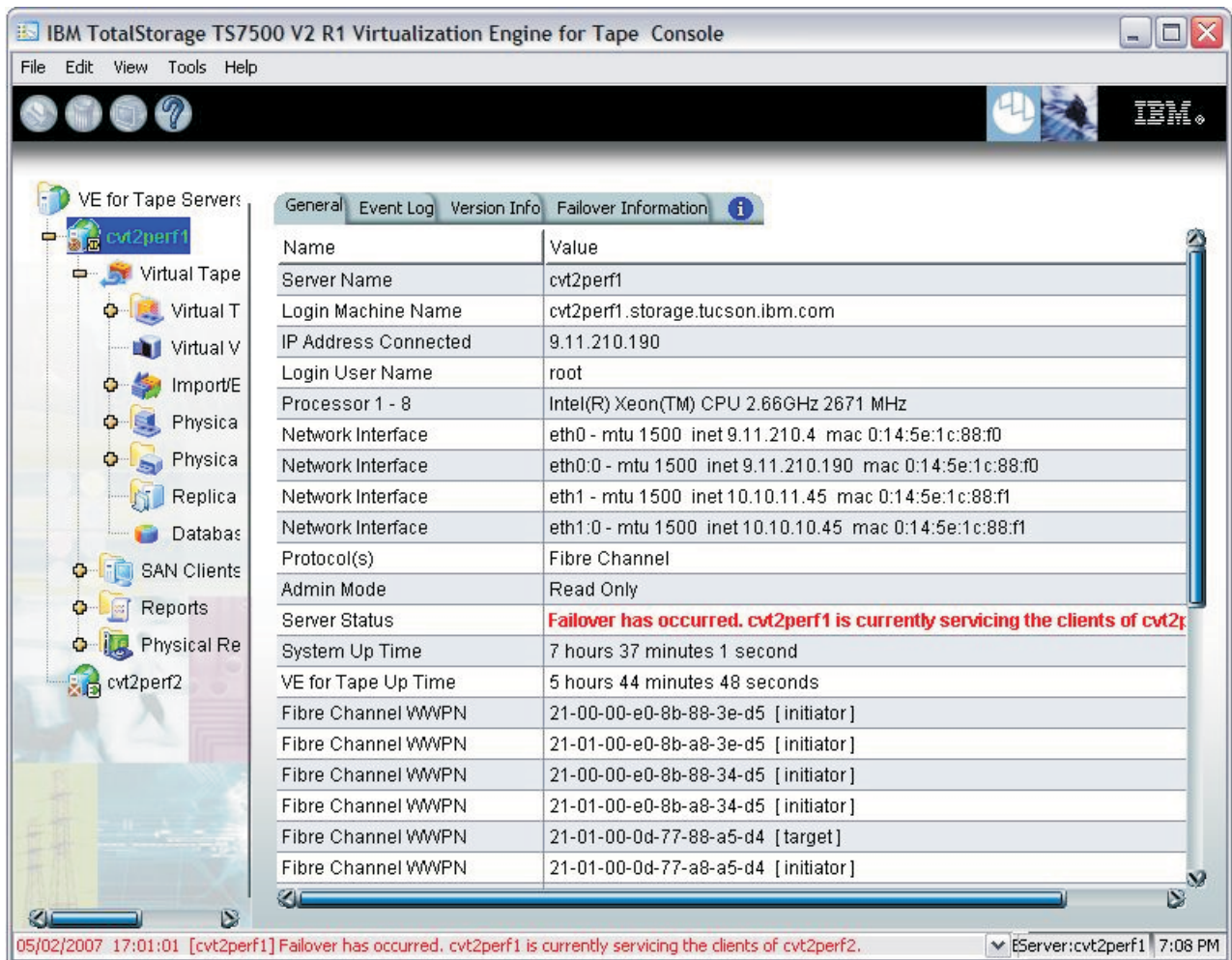
Figure 77. Failover Information

The VE console uses different colors to indicate Failover status:

Black server name
> Normal operation

Red server name
> The server is in Failover the secondary server has taken over its operations

Green server name
> The server is in Failover and has taken over the primary server's operations

Yellow dot beside server name
> Failover is suspended for this server and it will not take over the primary server's operations in the event of failure

The primary server's event log records Failover events. Review the event log for status, operational information, and errors. Upon Failover, the VE console shows the event log for the failed server.

Changes to servers with Failover enabled

The secondary server cannot have logical resources (such as logical tape or replica resources) assigned during initial Failover configuration. After failover configuration, you can assign these resources to the secondary server. The VE console must have write access to both servers to allow these assignments.

The VE console will automatically log on to the Failover pair when you attempt any changes to either server. If the servers have different usernames or passwords, The VE console prompts for them.

If you make a change to a physical device (For instance, if you add a network card for Failover use), you must run the Failover Setup Wizard again.

Changing Failover interval settings

To change Failover interval settings, complete the following steps:

1. __ Right-click one of the server icons and then click **Failover** → **View/Update Failover Options**.
2. Click the **Config** tab.
   - __ To change the self-checking interval, type a value or click the arrows to select a value in the **Self-checking interval** field. This interval determines how often the server checks itself.
   - __ To change the heartbeat interval, type a value or click the arrows to select a value in the **Self-checking interval** field. This interval determines how often each server checks the heartbeat of its Failover partner.

     Note: If practical, do not change the self-checking and heartbeat values from their defaults. Changing the values can result in a significantly longer Failover and recovery process.

   - __ To enable or disable auto recovery, select or clear the **Auto Recovery** check box. If auto recovery is disabled, you must manually initiate all recovery operations except for Failover caused by physical network cable failure, which always initiate automatic recovery when connectivity returns.
   - __ To change the auto recovery interval with auto recovery enabled, type a value or click the arrows to select a value in the **Auto Recovery in** field. This interval determines how long the secondary server delays before returning control to the primary server after that server recovers.
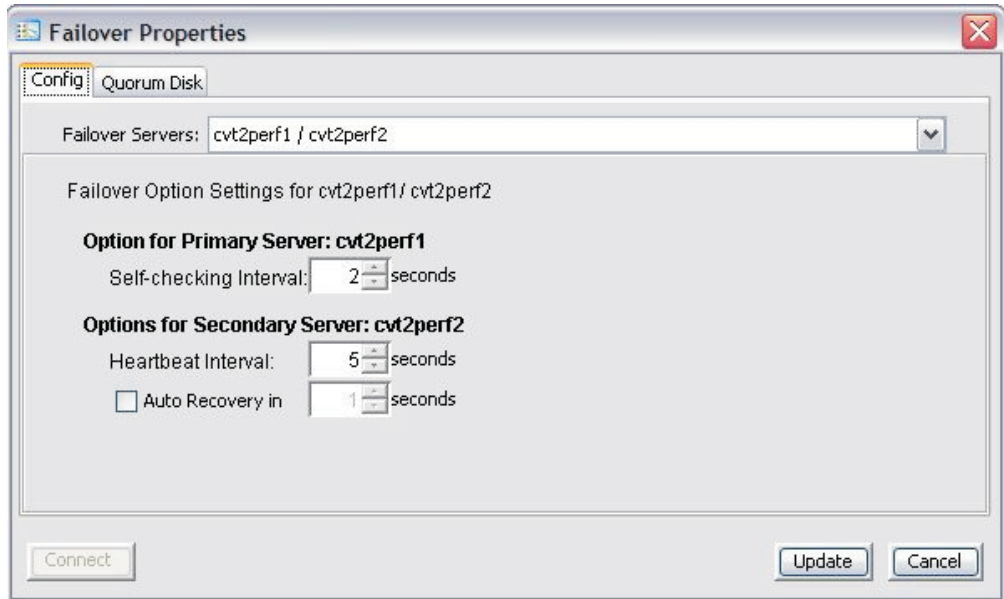
Figure 78. Failover Properties window: Config tab

3. __ From the **Failover Servers** list, select the other Failover direction (for example, in Figure 78, select cvt2perf2/cvt2perf1).

4. __ Change all intervals to the same values you selected in step 2 on page 99.

5. __ (Optional) To view the quorum disks for the Failover configuration, click the **Quorum Disk** tab. The quorum disks store information critical to determining whether a server has failed or recovered.
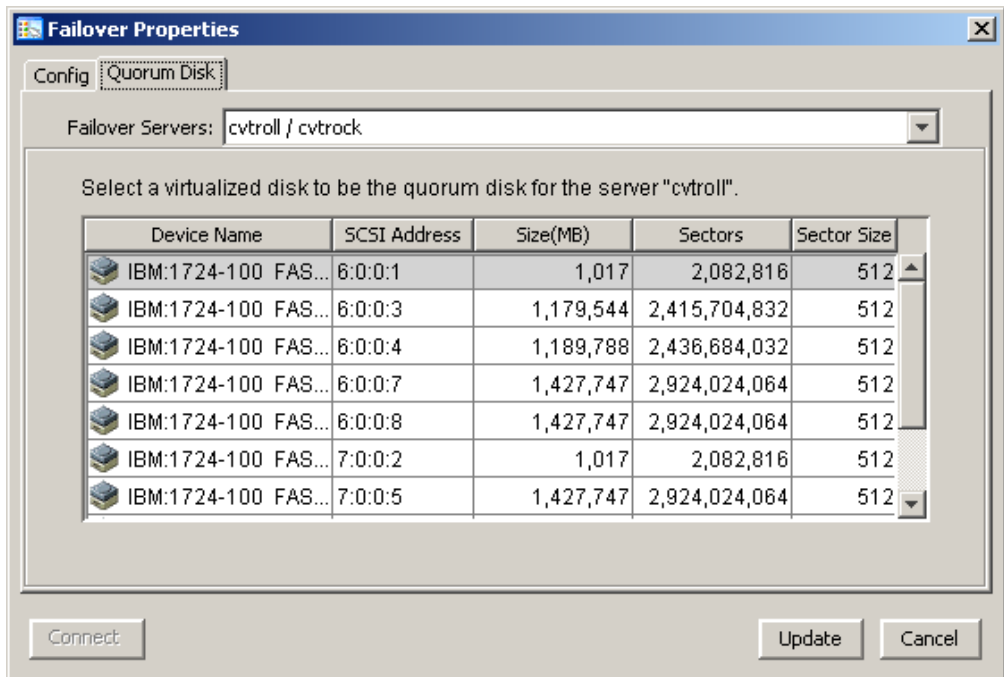
Figure 79. Failover Properties window: Quorum Disk tab

6. __ Click **Update**.

Attention: If an auto recovery occurs during an active job, it can cause that job to fail.

Manually initiating a takeover

Manual initiation of a takeover is useful in situations where one server must come offline, such as for a maintenance operation.

To manually initiate a takeover in the VE console, right-click the icon for the secondary server and then click **Failover** → **Start Takeover**.

Manually initiating a recovery

Manual initiation of a recovery is necessary when the auto recovery option is disabled or after an earlier manual takeover initiation.

To manually initiate a recovery in the VE console, right-click the icon for the secondary server and then click **Failover** → **Stop Takeover**.

Suspending and resuming Failover

Suspend Failover during periods of online maintenance to the TS7500 Virtualization Engine installation. During Failover suspension, the servers ignore events that would normally result in a Failover condition. When online maintenance is complete, resume Failover.

*   __ To suspend Failover, right-click either server icon in the VE console and then click **Failover** → **Suspend Failover**.
*   __ To resume Failover, right-click either server icon in the VE console and then click **Failover** → **Resume Failover**.

Removing a Failover server

To change server IP addresses, you must remove the server from its Failover configuration.

To remove a server from its Failover configuration:

1. __ Right-click a server icon in the VE console and then click **Failover** → **Remove Failover Server**.
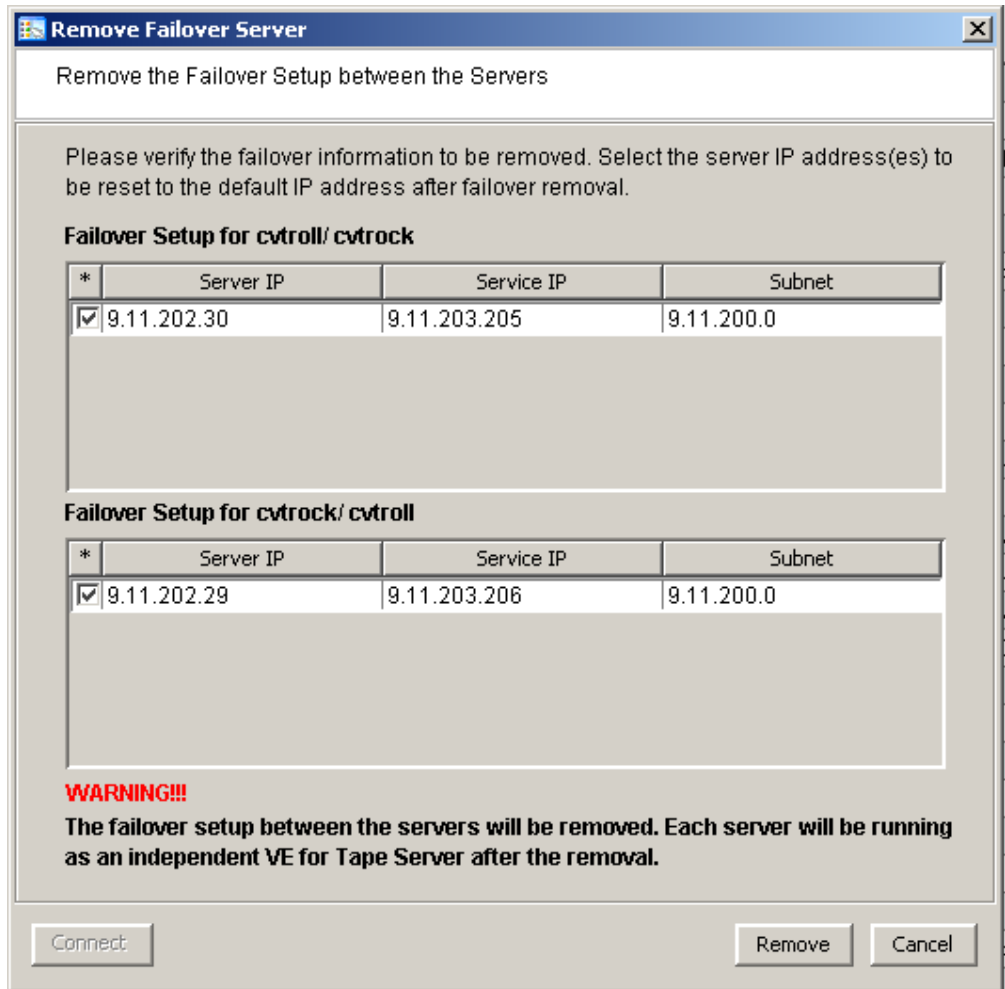
Figure 80. Remove Failover Server window

2. __ Select or clear one or both server IP addresses:
   - __ Selecting a **Server IP address** check box removes the service IP address from the server and restores the default server IP address.
   - __ Clearing a **Server IP address** check box causes the service IP address to become the server IP address.
3. __ Click **Remove**.

Failover server disaster recovery

During a Failover event, the primary server becomes inoperable and the secondary server assumes its operations. This section contains information about recovering the primary server.

1. __ If possible, save the primary server's configuration as described in "Saving the TS7500 Virtualization Engine configuration" on page 32.
2. __ Disable auto recovery from the secondary server as described in "Changing Failover interval settings" on page 99.
3. __ Perform corrective maintenance on the primary server.

4. __ Restart the primary server using the *Virtualization Engine TS7520 Recovery/Update Disk*. This step retrieves the primary server's configuration. Contact your site service representative if you encounter errors during this process.

5. __ Recover the primary server:

   • Enable auto recovery from the secondary server as described in "Changing Failover interval settings" on page 99.

   • Initiate a manual recovery as described in "Manually initiating a recovery" on page 101

6. __ (Optional) Recreate the following for the primary server:

   • Reports, as described in "Creating reports" on page 37

   • User accounts, as described in "Managing users" on page 59

   • DNS entries, as described in "Setting network information" on page 12

Failover driver issues

The following sections contain information about specific drivers associated with Failover.

Resuming backups after Failover and recovery

During Failover and recovery, the servers suspend I/O for three minutes. All backup jobs, including import/export and replication jobs, fail during this interval. Failover and recovery are transparent for the TS7520 Server, but you might need to take steps in your backup application to restore proper operation with the TS7500 Virtualization Engine. The steps you take vary with backup application and operating system. The following sections describe commonly required actions. Your environment might differ from these. See your backup application's documentation for more details.

IBM Tivoli Storage Manager

You must restart the IBM Tivoli® Storage Manager (TSM) Server backup or archive operation that was active at the time of the Failover action. Data written to the virtual tape up to the last synchronization point is valid. TSM will mark the virtual tape as logically full and will continue, on task restart, with a new tape. After primary server repair, recover the primary server only when no jobs are active to that server's virtual tape drives.

Note: After the primary server recovers, restart the TSM server to restore the devices before submitting any jobs.

BakBone NetVault

Restart the NetVault server in the following situations:

• If, after Failover, the Windows Device Manager stops responding

• If a NetVault job stalls while waiting to connect to tape media after devices are visible to both the operating system and to the NetVault application

CommVault Galaxy

If Galaxy has pending jobs, right-click pending jobs to resume them.

Before resuming jobs in Windows, scan for hardware changes using the Windows Device Manager and confirm that the tape drives are again visible.

Computer Associates ARCserve

If the operating system or the ARCServe application lose devices after Failover:

1. __ Stop the ARCServe tape engine.
2. __ Rescan the operating system.
3. __ Restart the ARCServe tape engine.
4. __ If devices are still not visible, restart the ARCServe server.

When devices are visible in both the operating system and in the ARCServe application:

1. __ Start the ARCServe application.
2. __ Eject all tape cartridges from tape drives.
3. __ Re-inventory the tape library.

HP OpenView Storage Data Protector

If backup jobs fail during Failover, the tape cartridge is marked ″poor quality″ and it remains in the tape drive. Manually move the tapecartridge back to the slot.

LEGATO NetWorker

After Failover, Networker marks the tape cartridge for the current backup job as full and uses a new blank tape cartridge to continue the job.

Symantec BackupExec

If there are no stalled jobs, but drives are offline. During Failover, the system should recover automatically. If BackupExec has stalled jobs, restart the BackupExec server.

Symantec NetBackup

When Failover occurs during an active backup or archive operation to the TS7500 Virtualization Engine, the Symantec NetBackup Server task that was active pauses and retries I/O. The task attempts to maintain data block orientation. In most cases, the backup task resumes when Failover is complete. Similarly, on failback, the NetBackup task pause. It resumes when failback is complete.

Path Failover

The Control Path Failover and Data Path Failover (Path Failover) feature adds the ability to use multiple physical paths from a backup application server (or *host system*) to a TS7500 Virtualization Engine with Path Failover enabled, and allows the device drivers at the host system to use the configured alternate path if a primary path fails.
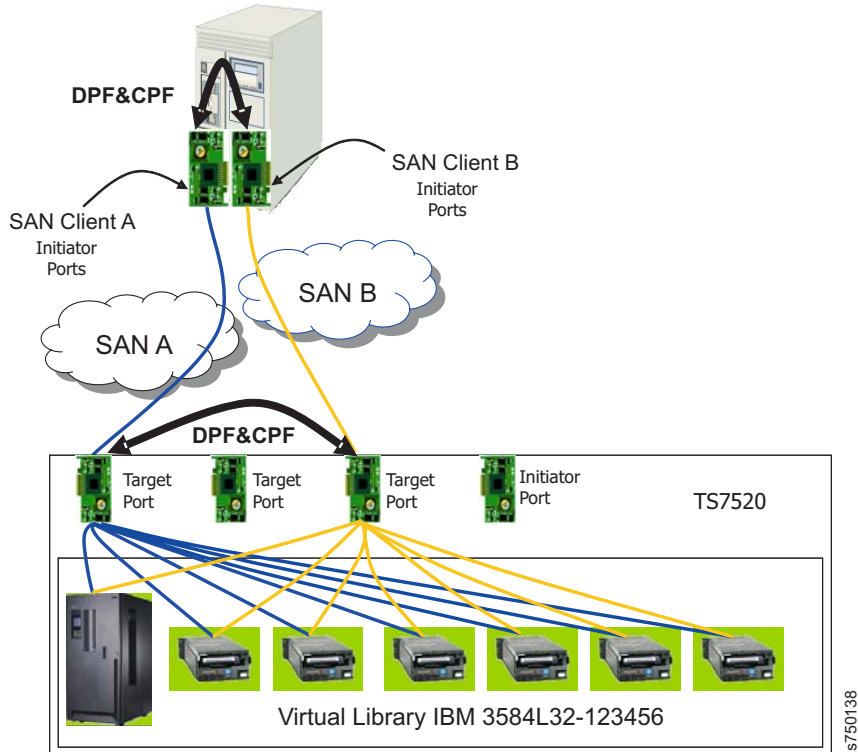
Figure 81. Path Failover, host system and TS7500 Virtualization Engine configuration

Figure 81 shows an example of Path Failover configuration between a host system and a TS7500 Virtualization Engine. The host system has two initiator ports, labeled *SAN Client A* and *SAN Client B*, available for connection to the TS7500 Virtualization Engine. The TS7500 Virtualization Engine has two target ports, labeled *Target Port 1* and *Target Port 2*, available for attachment to the host system. SAN Client A and Target Port 1 are in one zone, SAN A, while SAN Client B and Target Port 2 are in a second zone, SAN B. A virtual tape library, named *Virtual Library IBM 3584L32-123456*, is assigned to both SAN clients. All virtual tape drives in the virtual tape library have Control Path Failover and Data Path Failover support.

For more detailed information regarding Control Path Failover and Data Path Failover, download the latest version of the *IBM TotalStorage and System Storage Tape Device Drivers Installation and User's Guide*, available at ftp.software.ibm.com/storage/devdrvr/Doc.

When installing the operating system-appropriate IBM device driver with Control Path Failover and Data Path Failover support, follow the directions in the corresponding operating system chapter in the *IBM TotalStorage and System Storage Tape Device Drivers Installation and User's Guide* to configure the SAN client's device driver for Path Failover support.

Note: Your site service representative installed the Path Failover license key during initial installation of your TS7500 Virtualization Engine. When following the instructions in the *IBM TotalStorage and System Storage Tape Device Drivers Installation and User's Guide*, some operating systems might instruct you to install a 16-bit Data Path Failover key on the host system. This step is not required for a TS7500 Virtualization Engine.

To set up Path Failover for a particular host system, complete the following steps:

1. At the host system, record the WWPNs of two available initiator ports.

2. At the VE console, record the WWPNs of two available target ports.

3. __ Ensure that two SAN zones are available and zone one target port to one initiator port and the other target port to the other initiator port similar to the example in Figure 81 on page 105.

4. __ In the VE console, add two SAN clients using the procedure in "Adding SAN clients" on page 48. Use the WWPNs recorded in step 1 as the initiator WWPNs.

5. __ In the VE console, assign the desired virtual tape library to both new SAN clients using the procedure in "Assigning virtual tape devices to fibre channel clients" on page 140. Use the target WWPNs recorded in step 2. For example, Figure 82 shows virtual tape library *POCaixlib2* assigned to SAN clients *atssan3465a* and *atssan3465b*.
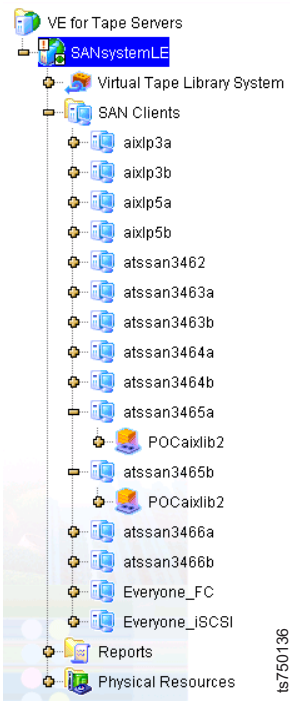
Figure 82. Virtual tape library assignment to SAN clients for Path Failover

6. __ At the host system, install and configure the IBM tape device driver appropriate for the host's operating system in accordance with the applicable procedure in the *IBM TotalStorage and System Storage Tape Device Drivers Installation and User's Guide*.

7. __ At the host system, verify that multiple devices are defined and configured as *primary* and *alternate* in accordance with the instructions in the *IBM TotalStorage and System Storage Tape Device Drivers Installation and User's Guide*.

8. __ At the host system, when assigning devices to your backup application, select the primary device in accordance with the instructions in the *IBM TotalStorage and System Storage Tape Device Drivers Installation and User's Guide*. Upon failure of the primary device path, the device driver will shift to the alternate path.

Chapter 5. Replication

Replication protects the data on a virtual tape cartridge by maintaining a remote copy of the cartridge on another TS7500 Virtualization Engine (called the *target server*) over the IP network.

At specified intervals, when the virtual tape cartridge is not in use, changed data from the *primary* virtual tape cartridge is transmitted to the *replica resource* on the target server to keep them synchronized. The target server is usually housed at a remote location. Under normal operation, backup clients do not have access to the replica resource on the target server.

If a disaster occurs and the replica is needed, the administrator can *promote* the replica to become the primary virtual tape cartridge for client access.

The TS7500 Virtualization Engine has three methods to replicate tape data. Two provide automatic replication and one is a manual process used as an alternative to the automatic methods.

Feature	Automatic/Manual	Description
Export Network Copy	Automatic	This method replicates the contents of a single tape cartridge to another TS7500 Virtualization Engine whenever a virtual tape library exports a virtual tape cartridge (such as from a backup application or other utility).
Replication	Automatic	This method replicates *changed* data from a virtual tape cartridge to another TS7500 Virtualization Engine at specified intervals, based on user-defined policies.
Remote Copy	Manual	This method replicates the contents of a single tape cartridge to another TS7500 Virtualization Engine on demand.

Requirements

The requirements to set up a replication configuration are:

- Installation of the corresponding hardware enablement feature license keys. See your IBM service representative to ensure that the license keys for the hardware feature are active.
- Write access to both systems.
- Sufficient storage capacity on the target server for the replica resource.

Export Network Copy

The Export Network Copy feature replicates the contents of a single tape cartridge to another TS7500 Virtualization Engine whenever a virtual tape library exports the virtual tape cartridge (such as from a backup application or other utility).

Export Network Copy is enabled when you create a virtual tape library. Upon creation of tape cartridges for the library, you can enable or disable Export Network Copy for individual tape cartridges. Upon tape creation, you cannot change the Export Network Copy configuration.

To enable Export Network Copy for an existing library, complete the following steps:

1. __ In the VE console, right-click the icon for a virtual tape library and then click **Properties**.
2. Click **Export Network Copy** and perform the following:
   a. __ Perform one of the following:
      - __ Click **Copy**.
      - __ Click **Move** and perform the following:
         1) __ In the **The grace period before deleting the tape** field, click the arrows to select a value or type a value.
         2) __ Select a measure of time from the list.
   b. __ (Optional) To add a server to the **Remote server name** list:
      1) __ Click **Add**.
      2) __ In the **VE for Tape Server** field, type the full hostname or the IP address of the server.
      3) __ In the **User Name** field, type the server's default user name.
      4) __ In the **Password** field, type the server's default password.
      5) __ Click **OK**.
   c. __ From the **Remote server name** list, select a server.
3. __ Select whether you want the virtual tape copied (retained) or moved (removed) after the data is replicated.

   If you select to move it, indicate how long to wait before deleting it.
4. __ Enter the name of the remote server.
5. __ Click **OK**.

Remote Copy

You can copy the contents of a single tape cartridge to a remote target server. Because the Remote Copy feature replicates the full tape instead of appending it to an existing tape, you can only copy a tape if there is no virtual tape on the remote target server with the same barcode. If the tape was previously copied, you must delete the copy from the remote target server before continuing.

Note: You cannot copy a tape that is configured for replication or for Export Network Copy/Physical Copy.

To use the Remote Copy function, complete the following steps:

1. In the VE console, expand **Virtual Tape Library System** until the virtual tape cartridge is visible.
2. __ Right-click the tape cartridge and then click **Remote Copy**.

3. __ Select the target server. If the target server is not in the list, click **Add**.

4. __ In the target server IP address field, type or confirm the target server's IP address.

5. __ In the Specify a Location window, navigate to and select a location for the tape to be copied. See Figure 83.
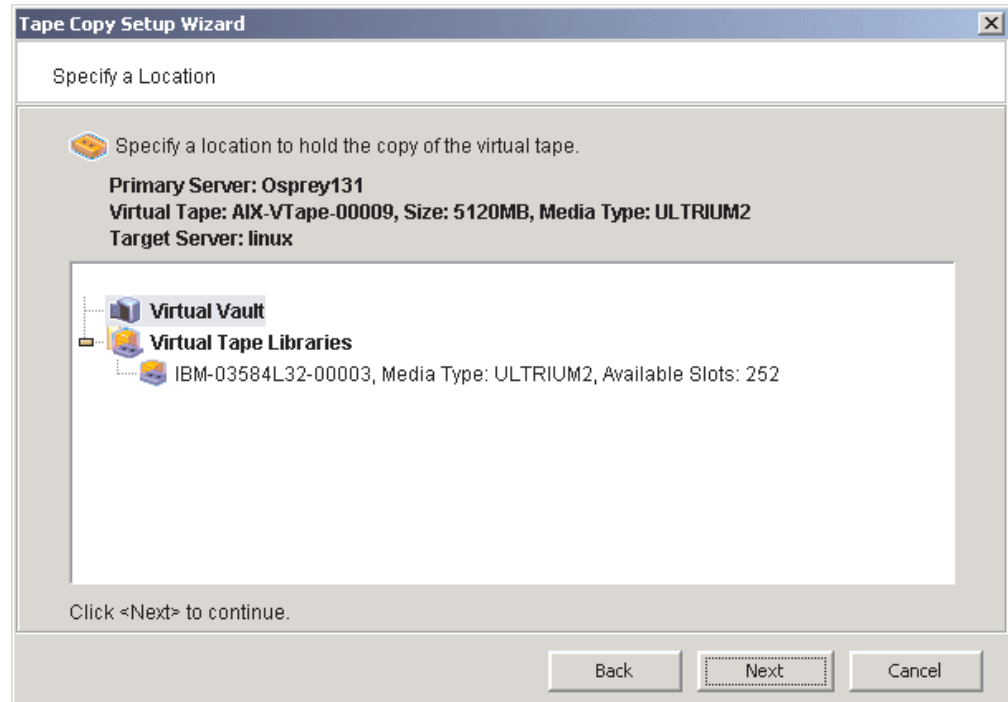
Figure 83. Tape Copy Setup Wizard

If you select a tape library, the media must be compatible.

6. __ Confirm that all information is correct and then click **Finish**.

Replication setup

You must enable replication for each virtual tape cartridge to be replicated.

To set up replication, complete the following steps:

1. __ If necessary, disable the Export Physical Copy/Network Copy function for the tape cartridge or tape library by performing one of the following:

   • For a single tape cartridge:

      a. __ Right-click the tape cartridge and then click **Properties**.

      b. __ Click the **Export Physical Copy/Network Copy** tab.

      c. __ Clear the **Export Physical Copy/Network Copy** check box.

      d. __ Click **OK**.

   • For a tape library with multiple tape cartridges:

      a. __ Right-click the tape library and then click **Properties**.

      b. __ Click the **Export Physical Copy/Network Copy** tab.

      c. __ Clear the **Export Physical Copy/Network Copy** check box.

      d. __ Click **OK**.

2. __ In the VE console, perform one of the following:
- To enable replication for a single tape cartridge, right-click the tape cartridge and then click **Replication** → **Add**.
- To enable replication for multiple tape cartridges in a tape library, right-click the tape library and then click **Replication** → **Add**.
3. __ In the Select the Target Server window:
   a. __ If the target server is not in the **Server** list, click **Add**.
   b. __ From the **Server** list, select the target server.
   c. __ Click **Next**.
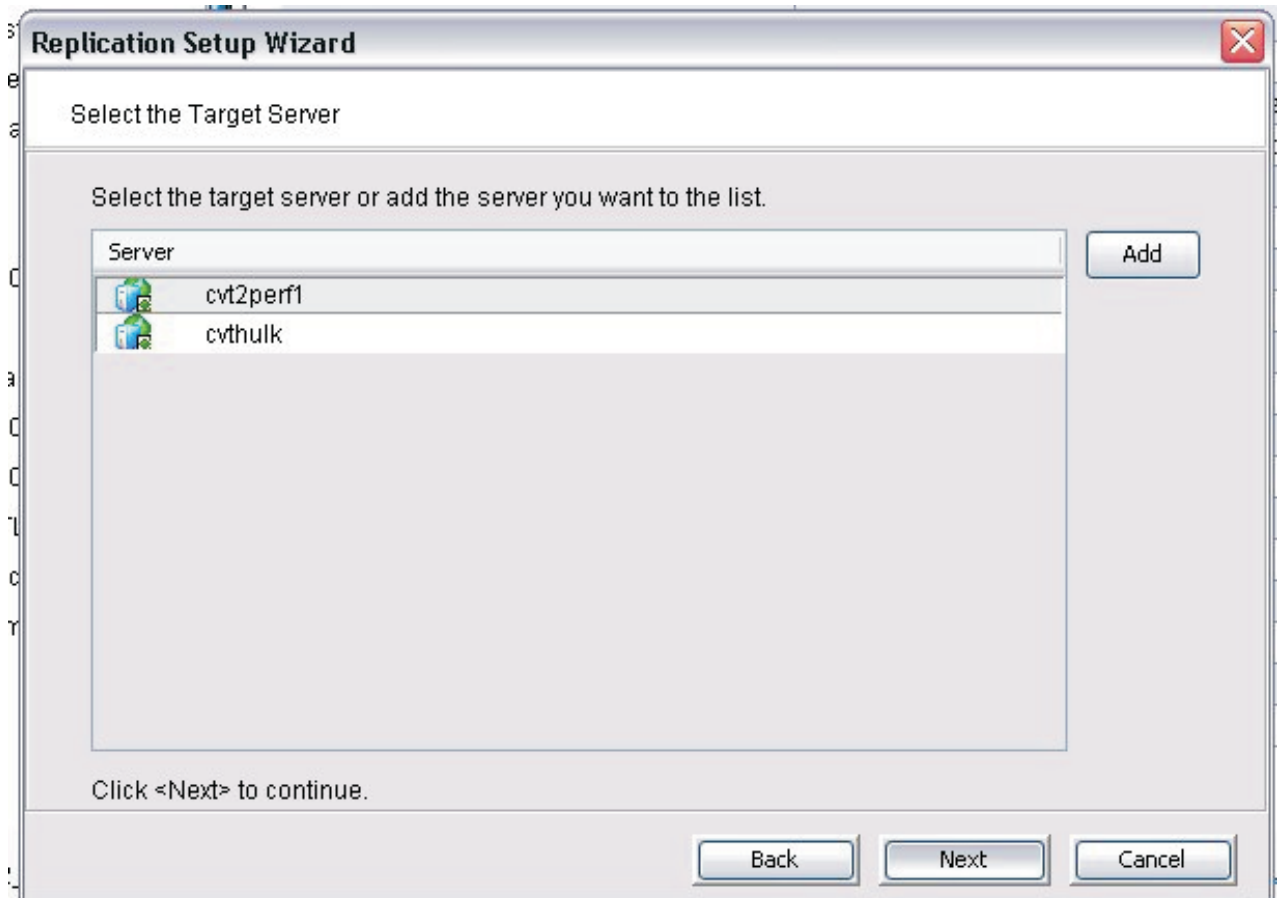
Figure 84. Select the Target Server window

4. __ In the Select the Replication Policy for the Virtual Tape window:
- (Optional)
   a. __ Select the **Start replication when the amount of new data reaches** check box.
   b. __ In the **MB** field, type a value or click the arrows to select a value.
- (Optional)
   a. __ Select the **Start replication every day at** check box.
   b. __ Type a value for the start time in hours and minutes (24-hour format).
- (Optional)
   a. __ Select the **Schedule the replication every** check box.

b. __ Type a value or click the arrows to select a value.

c. __ From the **Unit of Time** list, select a unit of time.

Note: You must select at least one option.
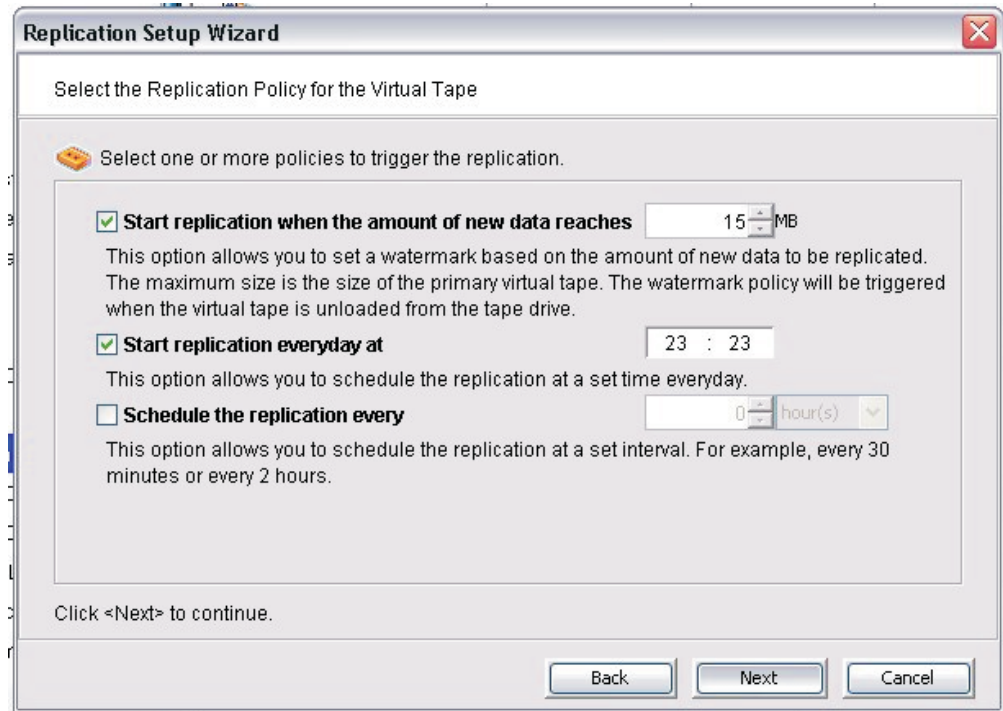
Figure 85. Select the Replication Policy for the Virtual Tape window

5. __ Click **Next**.

6. __ In the Specify Replication Timeout and Retry Policy window:

a. __ In the **Timeout replication in** field, type a value or click the arrows to select a value.

b. __ In the **Retry replication in** field, type a value or click the arrows to select a value.

c. __ In the **Retry replication for** field, type a value or click the arrows to specify a value.
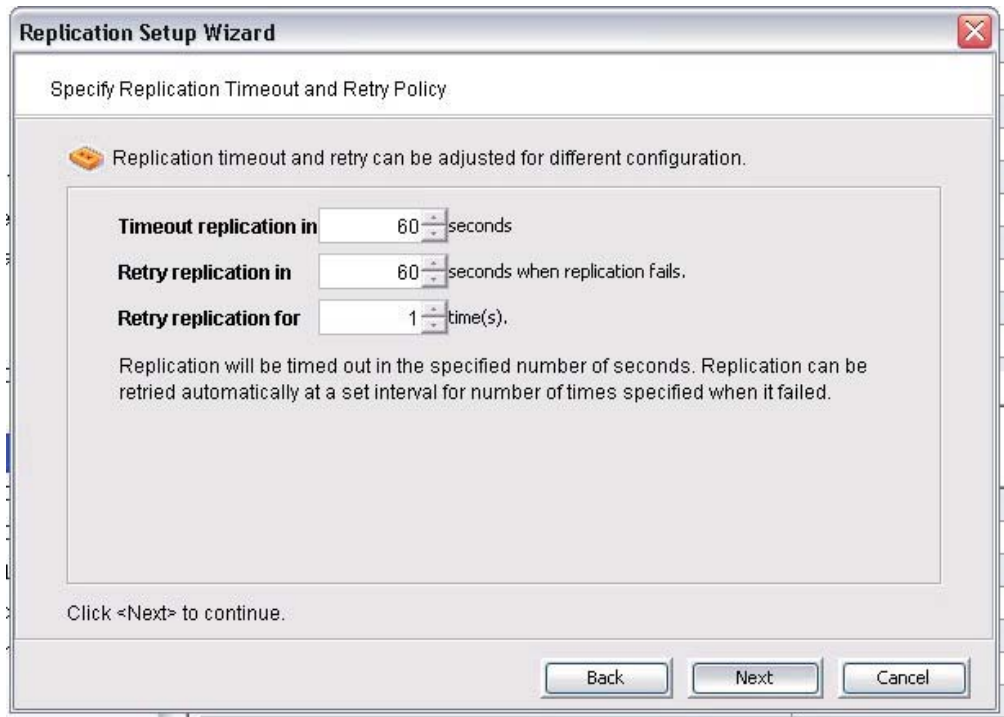
Figure 86. Specify Replication Timeout and Retry Policy window

7. __ Click **Next**.
8. __ In the Specify the Options for Data Transmission window:
    *   (Optional) Select the **Compress Data** check box. This option provides enhanced throughput during replication by compressing the data stream. TS7500 Virtualization Engine compression is software compression and may impact performance. Non-compressible data may impact performance more severely. If the data is compressed on the disk cache, data will be sent compressed. In this case the compression option is not required.
    *   (Optional) Select the **Encrypt Data** check box. The Encryption option secures data transmission over the network during replication. Initial key distribution uses the authenticated Diffie-Hellman exchange protocol. Subsequent session keys derive from the initial shared secret key.

Figure 87. Specify the Options for Data Transmission window

9. __ Click **Next**.

10. __ In the Enter the Virtual Tape Replica Name window, type a value in the **Virtual Tape Replica Name** field. Entered names are not case-sensitive.
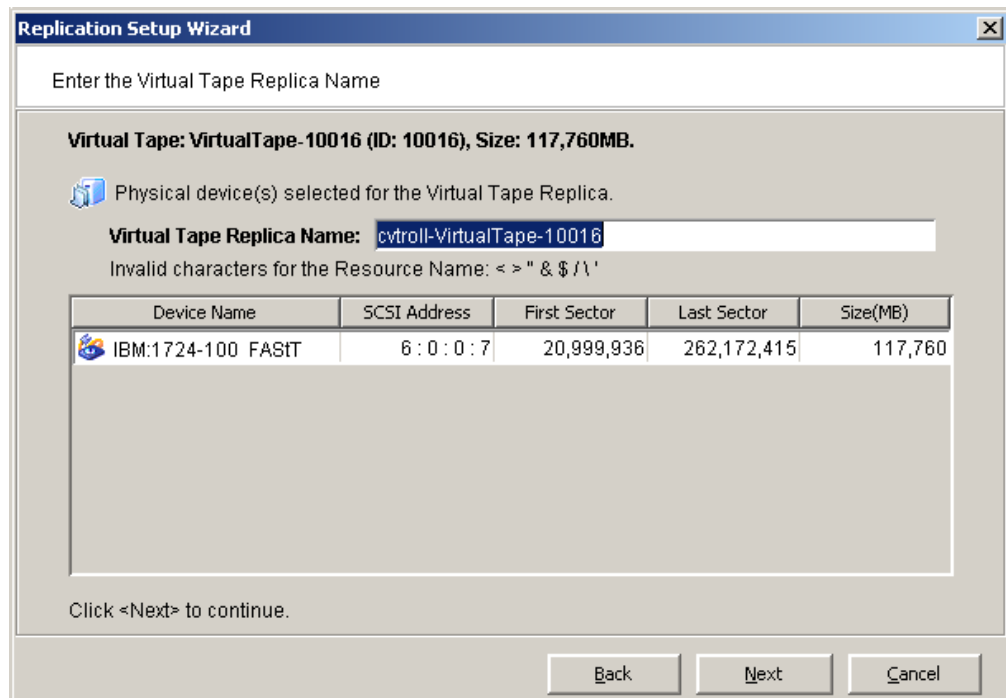
Figure 88. Enter the Virtual Tape Replica Name window

11. __ Click **Next**.

12. __ In the Create the Virtual Tape Replica window, confirm the configuration information and then click **Finish**.
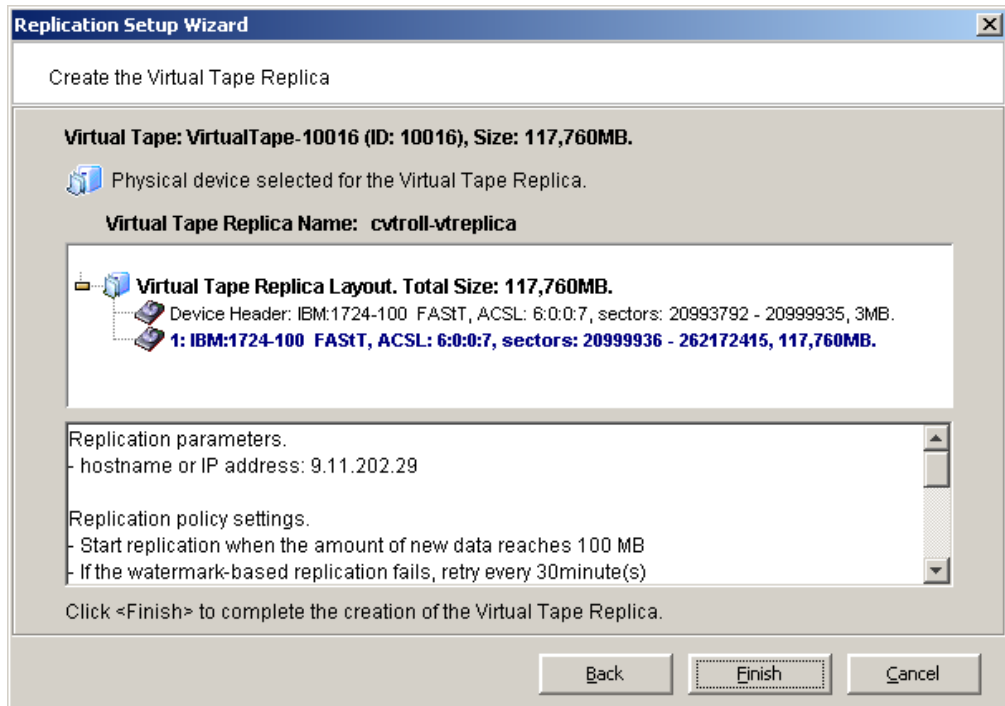
Figure 89. Replication Setup Wizard window for confirming correct information

Note: If you change the host name of the source (primary) server, you must recreate the replication configuration.

Checking replication status

The following VE console items display replica status information:

- The **Replication** tab of the primary virtual tape displays the policies set for replication and the replication status.

  Note: The **Replication** tab is only visible if replication is configured.

- The **General** tab of the Replica Resource on the target server displays the status of replication in progress.
- The event log displays status and operational information and any related errors.
- The Replication Status Report is an option under the Reports icon. It provides a centralized view for displaying real-time replication status for all tape cartridges enabled for replication. The Reports function can generate a replication status report for individual tape cartridges, multiple tape cartridges, the source server or the target server, for any range of dates. This report is useful for administrators managing multiple servers that either replicate data or are the recipients of replicated data. The report can display information about existing replication configurations only, or it can include information about promoted or deleted replication configurations. Figure 90 on page 115 shows a sample replication status report.

Figure 90. Replication status report sample

Promoting a replica resource

The replication promotion function can transform a needed replica to a usable virtual tape. After promotion, the virtual tape moves to the virtual vault. You can then move it to any virtual library on the target server. If you need to move the virtual tape back to the source server, you must replicate it back to that server. Promoting a replica resource disables the replication configuration. A replica resource, once promoted, cannot revert back to a replica resource. A valid replica resource must exist in order to promote it. For example, if a problem occurred (for example, transmission problem or replica resource corruption) during the first and only replication, the replicated data would be compromised and could not be promoted to a primary virtual tape cartridge. You cannot promote a replica resource while a replication is in progress.

To promote a replica resource, complete the following steps:

1. __ In the VE console, expand the icon for the target server.
2. __ Expand **Virtual Tape Library System** → **Replica Storage**.
3. __ Right-click the desired replica resource and then click **Replication** → **Promote**.
4. __ Confirm the promotion and then click **OK**.
5. __ From the SAN Client Monitor on the host system, rescan devices or restart the client to make the promoted virtual tape visible.

For the procedure to create a remote copy, see "Remote Copy" on page 108.

Changing the replication configuration

You can change the following replica configuration items:

- Static IP address of the target server
- Policies that trigger replication (watermark, interval, time)
- Timeout and retry policies
- Data transmission options (encryption, compression)

To change any of these items, complete the following steps:

1. __ Right-click the primary virtual tape and then click **Replication** → **Properties**.
2. __ Make the appropriate changes and click **OK**.

Suspending or resuming replication

You can suspend your replication policies (watermark, interval, time) from triggering future replications. This will not stop a replication that is currently in progress. You can still start the replication process manually during the suspension.

To suspend or resume replication, right-click the primary virtual tape and then click **Replication** → **Suspend** or **Replication** → **Resume**.

To view current replication settings, check the **Replication Schedule** field on the **Replication** tab of the primary virtual tape.

Stopping a replication in progress

To stop a replication that is currently in progress, right-click the primary virtual tape and then click **Replication** → **Stop**.

Manually starting a replication

To start a replication, right-click the primary virtual tape and then click **Replication** → **Synchronize**.

Removing a replication process

Right-click the primary virtual tape and then click **Replication** → **Remove**. This allows you to remove the replication configuration on the source server and to either delete or promote the replica resource on the target server at the same time.

Replication and Failover

If a Failover or a Failover recovery occurs during a replication, the replication stops. After the Failover or Failover recovery, the replication starts at the next normally scheduled interval.

Consolidating tape cartridges from multiple locations to a single data center

This information in this section applies to environments with multiple TS7500 Virtualization Engines without physical tape libraries that replicate data to a remote TS7500 Virtualization Engine with a physical tape library that supports barcodes.

See Figure 91 on page 117.

Site 1

Virtual Tape

Virtualization Engine Primary Disk

Site 2

Virtual Tape

Virtualization Engine Primary Disk

Site 3

Virtual Tape

Virtualization Engine Primary Disk

IP Replication

Data Center

Virtual Tape

Virtualization Engine Replica Disk

Physical Tape Library
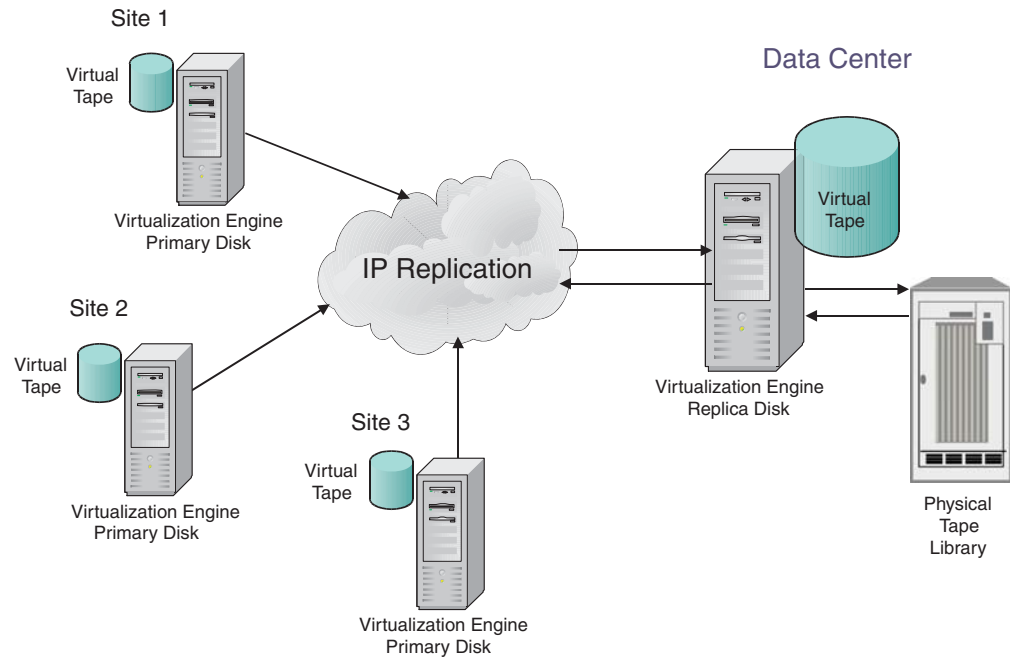
Figure 91. Consolidating tape cartridges from multiple locations to a single data center

Network compression and encryption

Network compression uses software compression on data transferred across an Ethernet network during a network replication. This reduces overall bandwidth used between two TS7520 Servers replicating virtual volumes because the data is compressed before transmission over the Ethernet network.

Network encryption secures data transmitted over the network during replication. Initial key distribution uses the authenticated Diffie-Hellman exchange protocol. Subsequent session keys derive from the initial shared secret key.

Chapter 6. Secure tape

Secure tape uses the Advanced Encryption Standard (AES) algorithm published by the National Institute of Standards and Technology, an agency of the US government. With this option, you can create one or more keys for encrypting the data when it exports to physical tape and decrypting it when it imports back to virtual tape cartridges. The data on the tape cannot be read or be decrypted without using the appropriate key.

Managing tape encryption keys

Each secure tape key consists of a secret phrase. For additional security, each key is password-protected. You must provide this password in order to change the key name, password, or password hint, or to delete or export the key.

You can apply a single key to all virtual tape cartridges when you export them to physical tape, or you can create a unique key for each. Creating multiple keys provides more security; in the unlikely event that a key is compromised, only the tape cartridges that use that key are affected. However, if you use multiple keys, you must keep track of which key applies to which tape.

Note: If you apply an incorrect key when importing a tape, the data imported from that tape will be indecipherable.

Once you have created one or more keys, you can export them to a separate file called a key package. If you send encrypted tape cartridges to other TS7500 Virtualization Engine installations, you can also send the key package. By importing the key package, administrators at the other sites can then decrypt the tape cartridges when they are imported back into virtual tape libraries on a TS7500 Virtualization Engine.

You can enable encryption and specify which key to use when you either manually import or export a tape or when you use the auto-archive/replication feature.

Creating a data encryption key

To create a data encryption key, complete the following steps:

1. __ In the VE console, right-click the server icon and then click **Key Management**.
2. __ Click **New**.
3. __ In the **Key Name** field, type a name for the key. The name can be from 1 to 32 characters in length.
4. __ In the **Secret Phrase** field, type a phrase for data encryption use. The phrase can be from 25 to 32 characters in length.

   Note: Save your secret phrase in a secure location. Once you have created the key, you cannot change the key's secret phrase.
5. __ In the **New Password** field, type a password for key access. The password can be from 10 to 16 characters in length. The password permits you to change the key name, the password, or the password hint. It also permits you to delete or export the key. You can use one password for multiple keys; in this situation, you only provide the password once when exporting multiple keys.

6. __ In the **Confirm Password** field, type the password again.

7. __ (Optional) In the **Password Hint** field, type a hint to aid remembering the password. The hint can be from 0 to 32 characters in length.

8. __ Click **OK**.

Changing the name or password of a data encryption key

You cannot change the secret phrase associated with a data encryption key, but you can change the following:

- Key name
- Key password
- Key password hint

If you change the name of a key, you can still use that key to decrypt data encrypted using the old key name.

To change the name or password of a key, complete the following steps:

1. __ In the VE console, right-click the server icon and then click **Key Management**.

2. __ From the **Key Name** list, select the name of the key that you want to change.

3. __ Click **Edit**.

4. __ If prompted, type the key's password in the **Password** field and click **OK**.

5. __ Change the key name, password, or password hint.

6. __ Click **OK**.

Deleting a data encryption key

CAUTION:
After deleting a key, you can no longer decrypt tape cartridges that were encrypted using that key unless you do one of the following:

- **Create a new key with the same secret phrase**
- **Import the deleted key from a key package**

To delete a key, complete the following steps:

1. __ In the VE console, right-click the server icon and then click **Key Management**.

2. __ From the **Key Name** list, select the key for deletion.

3. __ Click **Delete**.

4. __ Type the key's password in the **Password** field and click **OK**.

5. __ In the confirmation field, type **yes**.

6. __ Click **OK**.

Exporting a data encryption key

Exporting a key creates a separate file called a key package that contains one or more keys. You can send this file to another site with a TS7500 Virtualization Engine. Administrators at that site can import the key package and use the included keys to encrypt or decrypt data.

Creating a key package also provides a backup set of keys. If a key is accidentally deleted, you can import it from the key package to enable continued access to data encrypted with that key.

To export a key, complete the following steps:

1. __ In the VE console, right-click the server icon and then click **Key Management**.

2. __ Click **Export**.

3. __ In the **Package Name** field, type the file name for the key package. The name can be from 1 to 32 characters in length.

4. __ In the **Decryption Hint** field, type a three-character hint. The decryption hint appears correctly in the Import Keys window if you use a valid password during the import operation. If you use an invalid password, a different decryption hint appears. You can import keys using an invalid password, but you cannot decrypt data using those keys.

5. __ From the **Select Keys to Export** list, select the key or keys for inclusion in the key package. When you select a key or click **Select All**, you must provide the password for each key. If multiple keys use the same password, you only need to provide the password once upon selection of the first key using that password.

   After typing the password, the password appears in the **Password for all Keys in Package** area of the Export Keys window. By default, the password displays as a sequence of asterisks (*). To display the password, select the **Show clear text** check box.

   If you decide not to include a selected key, clear the key's check box. If you decide not to include any of the selected keys, click **De-Select All**.

6. __ (Optional) Perform one of the following:

   - To specify a separate password for the key package, select the **Prompt for new password for all keys in package** check box.

   - To use the same password for the package as the first selected key (which appears in the **Password for All Keys in Package** area), clear the **Prompt for new password for all keys in package** check box.

7. __ In the **Save in this directory** field, type the complete path for the file.

8. __ Click **OK**.

9. __ If you selected the **Prompt for new password for all keys in package** check box:

   a. __ Type the new password in the **New Password** and **Confirm Password** fields. The password can be from 10 to 16 characters in length.

   b. __ (Optional) In the **Password Hint** field, type a hint for the password. The hint can be from 0 to 32 characters in length.

10. __ Click **OK**.

Importing a data encryption key

Upon creation of a key package, you can open the package and specify which keys to import into the TS7500 Virtualization Engine. Once you import a key, you can use that key to encrypt or decrypt data.

To import a key, complete the following step:

1. __ In the VE console, right-click the server icon and then click **Key Management**.

2. __ Click **Import**.

3. __ In the **Find Package** field, type the full path to the key package.

4. __ Click **View**.

5. __ In the **Password** field, type the password for the key package.

6. __ Ensure that the displayed decryption hint matches the decryption hint specified at key package creation. If it does not, click **Password** and provide the correct password for key package access. If you provide an invalid password, you can still import the key package, but you will not be able to use any keys from the package to decrypt data encrypted with those keys.

7. __ From the **Select Keys to Import** list, select the keys for import. You can only import keys displaying a green dot and the phrase ″Ready for Import″ in the Status column. A red dot and the phrase ″Duplicate Key Name″ indicate that a key with the same name already exists in the TS7500 Virtualization Engine. This prevents import of the selected key.

   Note: A key of the same name might not necessarily have the same secret phrase. For example, you might have a key named Key1 with a secret phrase of *ThisIsTheSecretPhraseForKey1*. If the key package was created by another TS7500 Virtualization Engine, it might also have a key named Key1, but its secret phrase might be *ThisIsADifferentSecretPhrase*. Since the key names are the same, you will not be able to import the key in the key package unless you rename the existing Key1. After you rename the key, you can continue to use it to decrypt tape cartridges that were encrypted using that key, and you can also import the key named Key1 from the key package and use it to decrypt tape cartridges that were encrypted using that key.

   If you decide not to import a selected key, clear the key's check box. If you decide not to import any selected keys, click **De-Select All**. This control is available only if the **Show All Keys** check box is not selected.

8. __ Click **OK**. The imported keys appear in the **Key Name** list in the Key Management window.

TS1120 Tape Drive encryption

The TS7500 Virtualization Engine also supports the native encryption capabilities of the TS1120 Tape Drive. For information about using the encryption capabilities of the TS1120 Tape Drive, go to http://www-03.ibm.com/systems/storage/tape/ts1120/index.html.

Chapter 7. Enhanced Tape Caching (automated tape caching)

Note: The VE console interface uses the term ″automated tape caching″ to refer to the TS7500 Virtualization Engine feature ″Enhanced Tape Caching″. This chapter also uses the term ″automated tape caching″.

Automated tape caching enhances the functionality of the TS7500 Virtualization Engine by acting as a cache to the physical tape library, providing transparent access to data regardless of its location.

With automated tape caching enabled, tape cartridges always appear inside virtual libraries and are visible to the backup application regardless of whether the data is actually on disk or tape. This means that the backup application always has direct access to data regardless of its location.

The automated tape caching option also provides advanced flexibility that allows setting policies to automatically trigger data migration to physical tape cartridges based on specified criteria. These criteria can include the number of days data has been on disk or the amount of used disk space.

Automated tape caching allows determining which events trigger caching and when the caching occurs. For example, you can set the policy to migrate data immediately upon its arrival in cache, or at a specific time or day. The latter option enables writing of data to physical tape cartridges as a background process, without impacting production servers.

Reclamation policies permit specification of how and when data is deleted from cache after it has moved to physical tape. This frees capacity in the cache for new data.

In order to use automated tape caching, you must:
- Disable the Export Physical Copy, Network Copy, and Replication functions
- Enable automated tape caching
- Set migration and reclamation policies
- Create cache for each physical tape cartridge

The following sections contain information about setting up the automated tape caching function. If the function was enabled during initial TS7500 Virtualization Engine installation, use this information to change automated tape caching settings if desired.

Creating or changing a tape caching policy

To create or change a tape caching policy, complete the following steps:

1. __ In the VE console, expand **Virtual Tape Library System** → **Virtual Tape Libraries**.
2. __ Right-click a virtual tape library and then click **Automated Tape Caching**.
3. __ Select the **Enable Automated Tape Caching** check box.

123
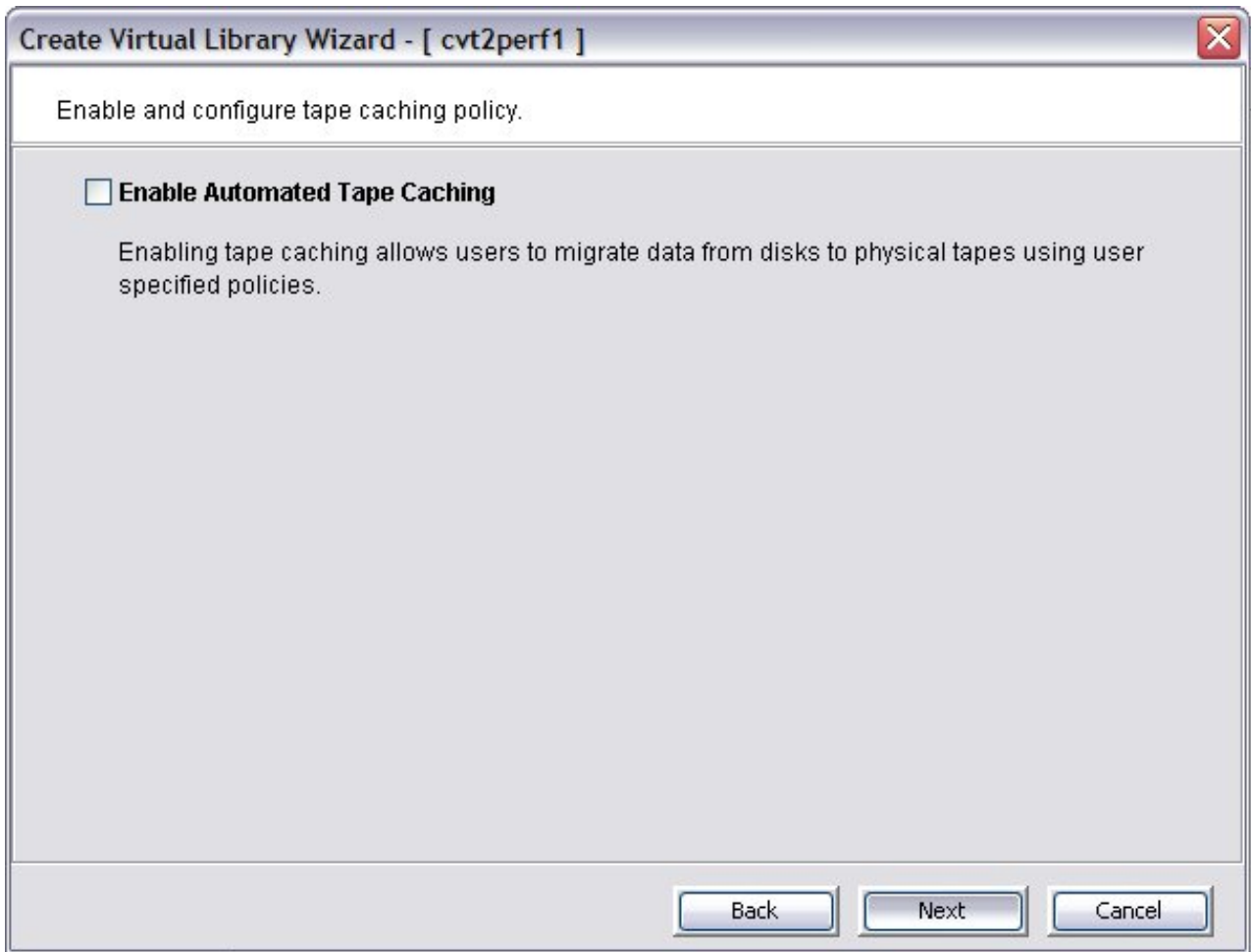
Figure 92. Enabling automated tape caching

4. __ Click **Next**.

5. __ On the **Data Migration Triggers** tab, perform one of the following:

   - __ Click **Time Based**.

     a. __ To configure when data migration happens, choose one of the following:

        – __ Daily migration:

           1) __ Click **Daily Data Migration Schedule**.

           2) __ In the **HR:MM** field, type the hour and minute of the day when you want data migration to start.

        – __ Weekly migration:

           1) __ Click **Weekly Data Migration Check Schedule**.

           2) __ From the list, select the day of the week when you want data migration to occur.

           3) __ In the **HR:MM** field, type the hour and minute of the day when you want data migration to start.
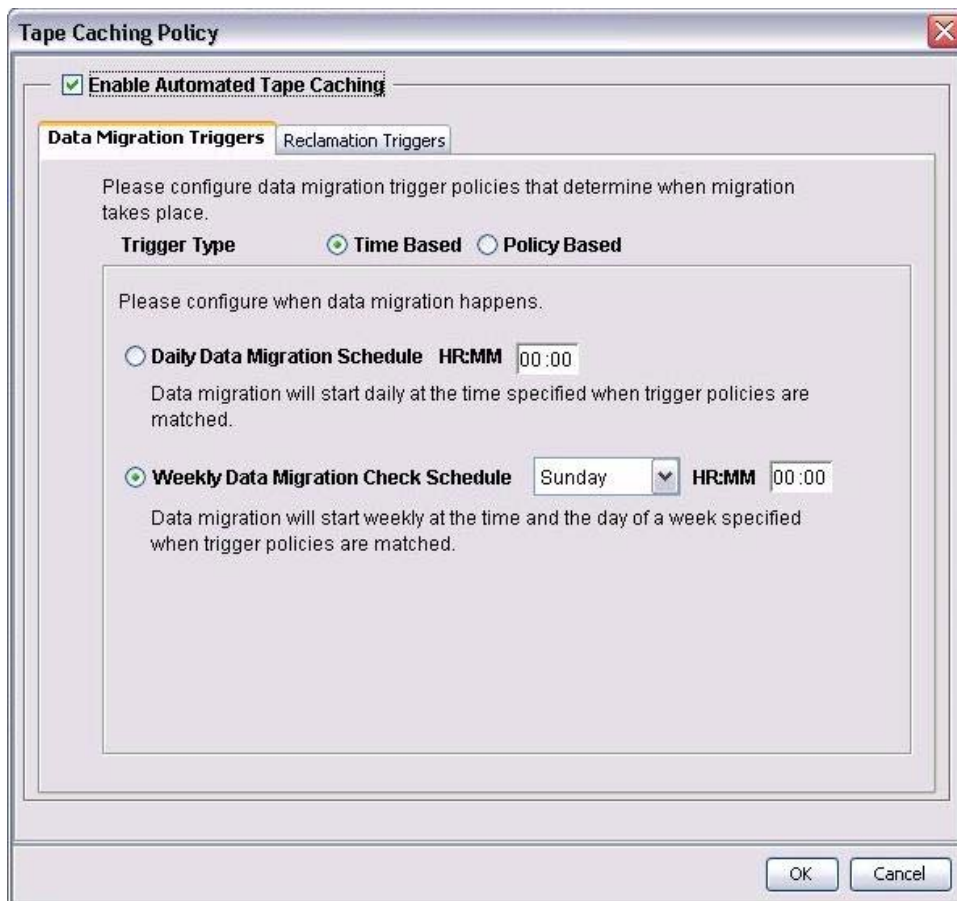
Figure 93. Selecting weekly data migration check schedule

- __ Click **Policy Based**.
  a. __ Perform one of the following:
     - __ Click **And**. Data migration occurs when all of the policies you select are met.
     - __ Click **Or**. Data migration occurs when any one of the policies you select are met.
  b. __ (Optional)
     1) __ Select the **Age Based** check box.
     2) __ In the **Day(s)** field, click the arrows to select a value or type a value.
  c. __ (Optional) Select the **Disk Capacity Based (Triggered if disk usage is above 90%)** check box.
  d. __ (Optional)
     1) __ Select the **End of Backup** check box.
     2) __ (Optional) Select the **Only When Tape is Full** check box.
  e. __ (Optional)
     1) __ Select the **Delay Migration Until** check box.
     2) __ In the **HR:MM** field, type the hour and minute of the day when you want data migration to start.
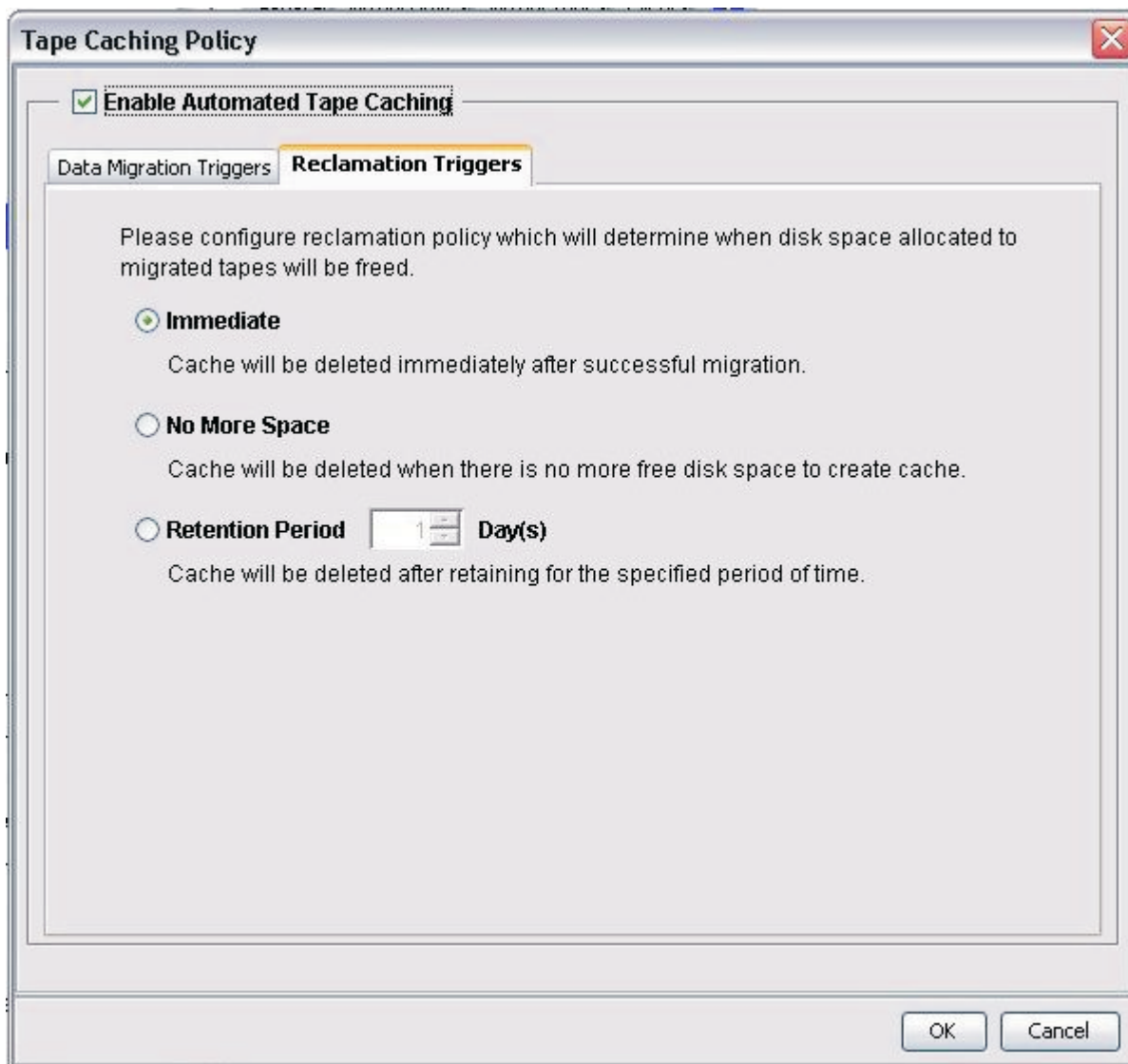
Figure 94. Selecting migration delay

6. __ Click the **Reclamation Triggers** tab and perform one of the following:
   - __ To delete migrated data in the cache immediately after migration, click **Immediate**.
   - __ To delete migrated data in the cache when cache is full, click **No More Space**.
   - __ To delete migrated data after a specified amount of time:
     a. __ Click **Retention Period**.
     b. __ In the **Day(s)** field, click the arrows to select a value or type a value.
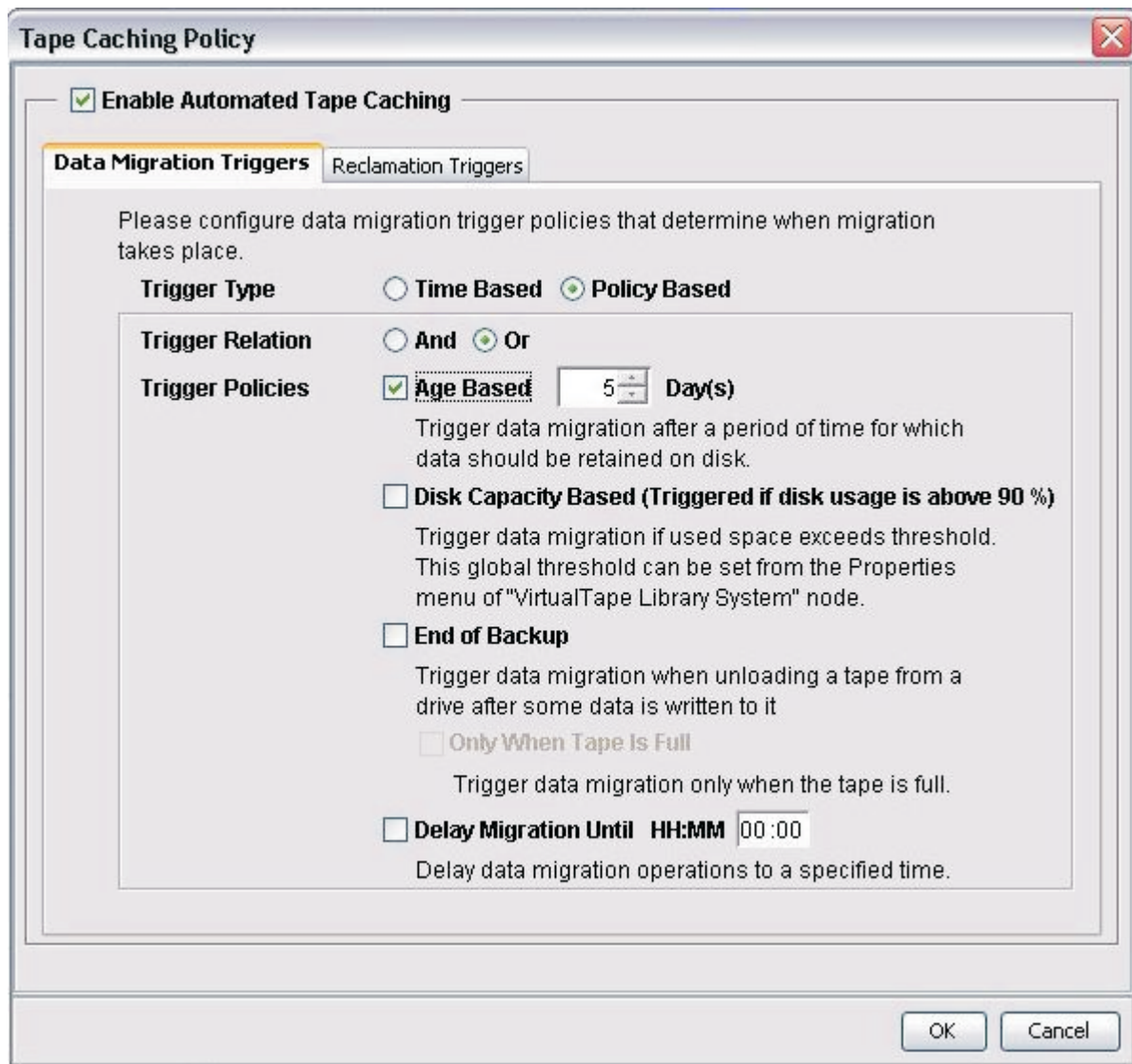
Figure 95. Defining a retention period

7. __ Click **OK**. The specified policies take effect immediately.

> **Note:** A tape moved from a virtual tape library to a virtual vault retains the tape caching policies associated with the original virtual tape library.

Disabling a tape caching policy

To disable a tape caching policy, complete the following steps:

1. __ In the VE console, expand **Virtual Tape Library System** → **Virtual Tape Libraries**.
2. __ Right-click a virtual tape library and then click **Automated Tape Caching**.
3. __ Clear the **Enable Tape Caching Policy** check box.
4. __ Click **OK**. Selected policy options remain intact but data migration no longer occurs.

Creating a cache for physical tape cartridges

With automated tape caching enabled, data resides on disk before migrating to physical tape. This requires creation of a cache for each physical tape cartridge. Cache creation effectively creates a virtual copy of a physical tape cartridge. The virtual copy has the same barcode as the linked physical tape cartridge.

To create a cache for a physical tape cartridge, complete the following steps:

1. __ In the VE console, right-click the virtual tape library and then click **Sync Library**.
2. __ Select the physical tape library from the list and click **Next**.
3. __ Select the physical tape cartridge or cartridges for cache creation and click **Next**.
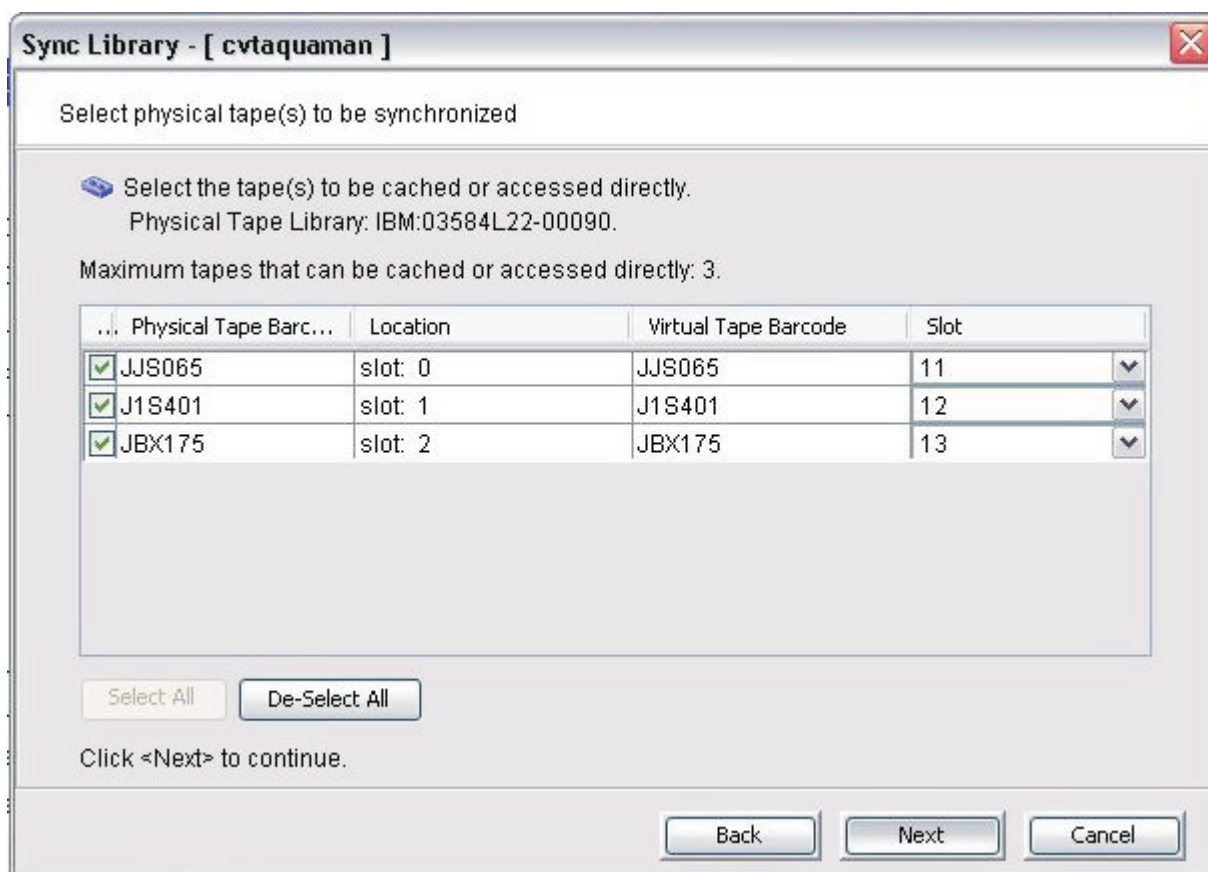
Figure 96. Selecting physical tape cartridges for cache creation

4. __ Click **Create Cache**.
5. __ (Optional) select the **Copy meta data** check box. Select this if your backup application requires a tape header to identify a tape cartridge.
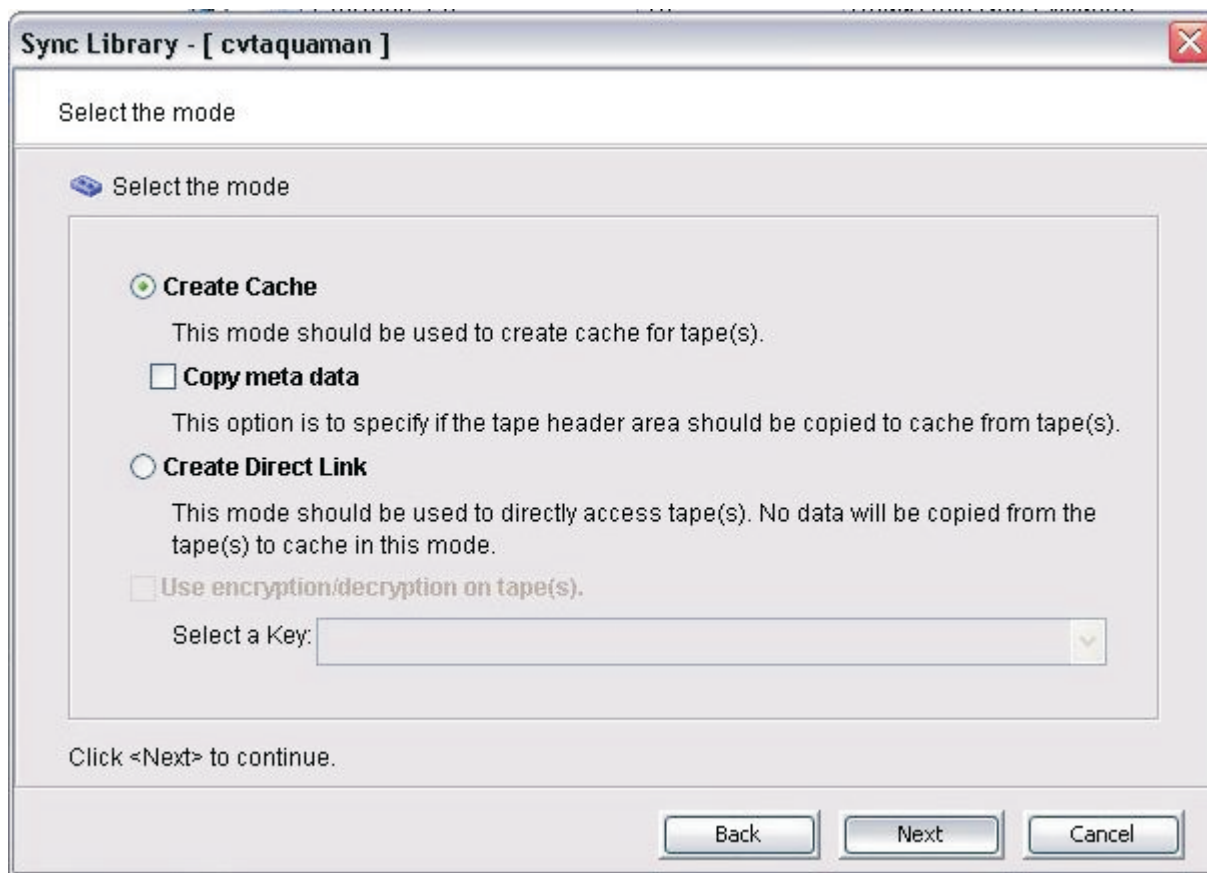
Figure 97. Selecting the cache mode

6. __ Click **Next**.
7. __ Verify all information and click **Finish**.

Creating virtual tape cartridges

With automated tape caching enabled, you can also create non-cached virtual tape cartridges that will not migrate to physical tape cartridges. This is useful for occasional single backups that is not part of the routine backup schedule.

To create one or more virtual tape cartridges, right-click a virtual tape cartridge icon and then click **New Tape(s)**.

Note: Virtual tape cartridge barcodes cannot match the barcodes of existing physical tape cartridges.

Forcing migration to physical tape

To manually initiate migration of data in cache to physical tap, right-click a virtual tape cache icon and then click **Migrate to Physical Tape**.

Note: This action overwrites all data on the physical tape cartridge.

Reclaiming disk space manually

You can reclaim disk space from data that has migrated to physical tape. This allows overwriting of data in the cache.

To reclaim disk space, perform one of the following:

- __ For a single cache, right-click a virtual tape cache in the VE console and then click **Reclaim Disk Space**.
- __ For multiple tape caches, right-click **Virtual Tape Library System** in the VE console and then click **Reclaim Disk Space**.

Renewing cache for a direct-link tape

If the backup application overwrites the direct-link tape, the TS7500 Virtualization Engine caches the physical tape. This eliminates the direct link and creates a cache for the physical tape cartridge. Ensure that this cartridge is either empty or is a scratch cartridge.

To renew the cache for a direct-link tape, right-click a direct-link tape in the VE console and then click **Renew Cache**.

Recovering data

In a cached environment, tape cartridges are always visible to the backup application whether the data is on disk or on a physical tape cartridge. The backup application reads the data from the disk, if it is still there, or from the physical tape cartridge. If the data no longer resides on disk and if the physical tape library has not ejected the tape cartridge,

However, if the data is no longer on disk and the physical tape has not been ejected from the physical tape library, you must create a link to the physical tape cartridge. To create a direct link, complete the following steps:

1. __ In the VE console, right-click a virtual tape library and then click **Sync Library**.
2. __ If required, select the appropriate library from the list.
3. __ Select the appropriate tape cartridge.
4. __ Click **Create Direct Link**.

Chapter 8. Fibre channel considerations

The TS7500 Virtualization Engine support for the Fibre Channel protocol allows any fibre channel-enabled system to take advantage of the TS7500 Virtualization Engine's extensive storage capabilities such as virtualization, mirroring, replication, and security. The TS7500 Virtualization Engine supports the Arbitrated Loop fibre channel topology.

This chapter provides configuration information for fibre channel target mode and the associated fibre channel SAN equipment, including switch, T3 and so on).
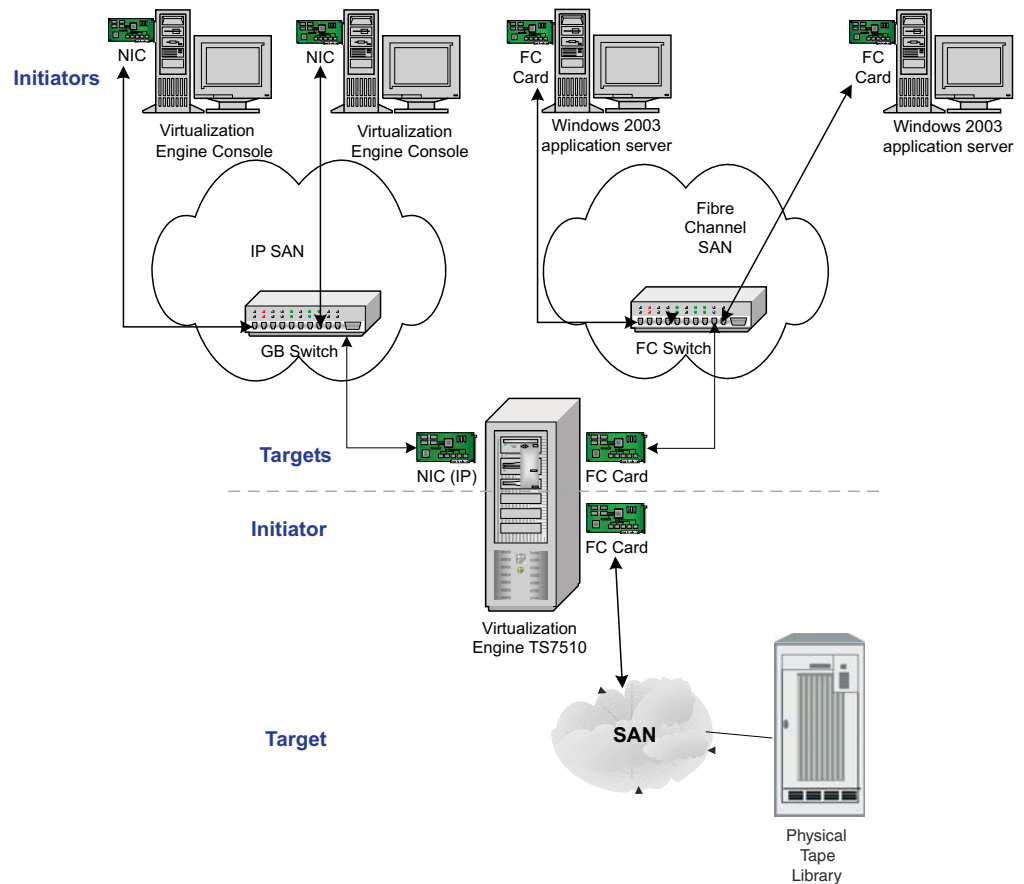
Figure 98. Fibre channel target mode

Installation and configuration overview

The TS7500 Virtualization Engine comes with a default library configuration installed. For more information on the default library configuration, see "Using the default library configuration" on page 21. You can customize this configuration if you need more bandwidth for your backup server or if you need to isolate virtual tape libraries from other SAN clients. Follow these steps to customize your configuration:

1. Prepare fibre channel physical connectivity. For more information, see "Physical connectivity" on page 132.
2. (If applicable) Set fibre channel ports to target mode.
3. Set target port binding for initiators.

4. (Optional) Set up Failover configuration.

5. Add fibre channel clients.

6. (Optional) Associate WWPNs with clients.

7. Assign virtual libraries or virtual tape drives to fibre channel clients.

8. Rescan devices or restart client machines to access new devices.

Physical connectivity

Physical connectivity, the connection of cables from the TS7500 Virtualization Engine to SAN clients, is identical whether a fibre channel port is in initiator mode for attachment to physical tape resources, or in target mode for SAN client access to virtual tape resources.

The TS7500 Virtualization Engine uses QLogic dual-port 2462 four-Gbps short-wave fibre channel cards for physical connectivity. You cannot change this card. See the certification matrix on the TS7500 Virtualization Engine Web site for an up-to-date list of supported fibre channel switches. The certification matrix is at: http://www.ibm.com/storage. For more information, see the *IBM Virtualization Engine TS7500 Introduction and Planning Guide* .

To establish physical connectivity, cable the customer-attachable ports of the TS7500 Virtualization Engine to SAN clients or physical tape resources either through point-to-point topology or through a SAN. The customer-attachable ports are:

For TS7500 EE installations
Ports other than 0, 1, 2, or 3

For TS7500 LE installations
Ports other than 0 or 1

Fibre channel ports 0, 1, 2, and 3 are reserved for connection to the disk cache.

The TS7500 Virtualization Engine provides indicators to assist in determining whether physical connectivity exists. In the VE console, expand **Physical Resources** → **Storage HBAs**. If physical connectivity exists, the adapter icon is green and the **General** tab displays a **Port Status** value of **Link Up**. If physical connectivity does not exist or the connection is faulty, the adapter icon displays a red arrow and

If you do not have physical connectivity or there is a problem with the connection, the adapter icon will have a red arrow and the **General** tab displays a **Port Status** value of **Link Down**.

Sun T3 and non-fabric aware devices

If you have Brocade fibre channel switches installed and connected to the TS7500 Virtualization Engine, the following instructions contain information about managing Sun T3 or other devices that are not fabric-aware (that is, they do not operate correctly when the switch is in fabric mode).

You must enable Quick Loop support for the Brocade switch to permit the TS7520 Server's initiator to detect devices that are not fabric-aware. To do this, complete the following steps:

1. __ Obtain and activate a Quick Loop license from Brocade.
2. __ Open a telnet connection to the Brocade switch.
3. __ Type the following command:

```
qlEnable
```

   and press the **Enter** key. This enables Quick Loop on the switch.
4. __ Type the following command:

```
qlPortEnable x
```

   (where *x* is the port number of the device) and press the **Enter** key. This allows the device, in loop mode, to communicate with N-port devices or fabric-aware loop-port devices.
5. __ Perform a rescan on the adapter from the VE console for all devices by completing the following substeps:.
   a. __ If necessary, connect to the server using the procedure in "Connecting to the TS7500 Virtualization Engine" on page 12.
   b. __ In the VE console, expand the server icon.
   c. __ Expand **Physical Resources** → **Storage HBAs**.
   d. __ Right-click the adapter and then click **Rescan**.
   e. __ Click **Scan Existing Devices**.
   f. __ Click **OK**.
6. __ Verify that the devices are now listed in the VE console by performing the following steps:
   a. __ In the VE console, expand the server icon.
   b. __ Expand **Physical Resources** → **Storage Devices** → **Fibre Channel Devices**.

Setting QLogic ports to target mode

The default settings for the additional four QLogic ports provided by adding two more fibre channel cards are two ports (4 and 6) in target mode and two ports (5 and 7) in initiator mode. In initiator mode, a port initiates requests to physical tape drives. In target mode, a port receives requests from fibre channel clients.

If no tape drives attach to the TS7500 Virtualization Engine, or if you need more bandwidth to fibre channel clients, you can reset one or both of the two initiator ports, 5 and 7, to target mode. If all initiator mode ports are reset to target mode, no tape drives can connect to the TS7500 Virtualization Engine.

Note: You can add a total of four additional fibre channel cards to each TS7520 Server.

Figure 99 on page 134 shows the server's PCI slots 1 - 6. Slots 1 and 2 are for attachment to the cache components. They always contain either two fibre channel cards (for TS7500 EE installations) or one fibre channel card in slot 1 (for TS7500 LE installations). Slots 3 - 6 are for attachment to the host servers and to physical tape resources.

SP Ethernet
10/100 activity LED
SP Ethernet 10/100
SP Ethernet
10/100 link LED
USB 1
USB 2
Power-supply
Video
System serial
SP serial

Gigabit Ethernet 1
link LED
Mouse
Keyboard
Gigabit Ethernet 1
Remote Supervisor Adapter II
Gigabit Ethernet 1
activity LED
SlimLine status LED
IXA RS485
Gigabit Ethernet 2
link LED
I/O board error LED
Gigabit Ethernet 2
Gigabit Ethernet 2
activity LED

Figure 99. Server fibre channel card slots (PCI slots 1 - 6)

Note: The TS7500 Virtualization Engine configuration steps refer to *Ethernet 1* and *Ethernet 2* as *eth0* and *eth1*.

Table 8 shows the default settings for configurations with four fibre channel cards in each server. You can change the settings for the physical tape connections from initiator mode to target mode if your installation does not attach to physical tape.

Note: Do not change the cards or move the cables in slots 1 and 2. Only modify QLogic adapters 4 and higher (for TS7500 EE installations) or adapters 2 and higher (for TS7500 LE installations).

Table 8. Default configuration for server with four QLogic fibre channel cards (HBAs)

VE console adapter number	Server HBAs	Lower server attachments, first base frame	Upper server attachments, first base frame	Lower server attachments, second base frame	Upper server attachments, second base frame
Adapter 0	PCI Slot 1: QLA2462 Port 1	Lower TS7520 Cache Controller - Controller A - Host 1 Switch 1 – port 0	Upper TS7520 Cache Controller - Controller A - Host 1 Switch 2 – port 0	Switch 1 – port 4	Switch 2 – port 4
Adapter 1	PCI Slot 1: QLA2462 Port 2	Upper TS7520 Cache Controller - Controller A - Host 2 Switch 2 – port 1	Lower TS7520 Cache Controller - Controller A - Host 2 Switch 1 – port 1	Switch 2 – port 5	Switch 1 – port 5

Table 8. Default configuration for server with four QLogic fibre channel cards (HBAs) (continued)

VE console adapter number	Server HBAs	Lower server attachments, first base frame	Upper server attachments, first base frame	Lower server attachments, second base frame	Upper server attachments, second base frame
Adapter 2	PCI Slot 2: QLA2462 Port 1	Lower TS7520 Cache Controller - Controller B - Host 1 Switch 2 – port 2	Upper TS7520 Cache Controller - Controller B - Host 1 Switch 1 – port 2	Switch 2 – port 6	Switch 1 – port 6
Adapter 3	PCI Slot 2: QLA2462 Port 2	Upper TS7520 Cache Controller - Controller B - Host 2 Switch 1 – port 3	Lower TS7520 Cache Controller - Controller B - Host 2 Switch 2 – port 3	Switch 1 – port 7	Switch 2 – port 7
Adapter 4	PCI Slot 3: QLA2462 Port 1	Target port for host attachment	Target port for host attachment	Target port for host attachment	Target port for host attachment
Adapter 5	PCI Slot 3: QLA2462 Port 2	Initiator port for real tape	Initiator port for physical tape	Initiator port for real tape	Initiator port for physical tape
Adapter 6	PCI Slot 4: QLA2462 Port 1	Target port for host attachment	Target port for host attachment	Target port for host attachment	Target port for host attachment
Adapter 7	PCI Slot 4: QLA2462 Port 2	Initiator port for physical tape	Initiator port for physical tape	Initiator port for physical tape	Initiator port for physical tape

To change a QLogic port from initiator mode to target mode, complete the following steps:

Note: You cannot change a port in initiator mode to target mode if the port connects physically to physical tape.

1. __ In the VE console, expand **Physical Resources** → **Storage HBAs**.
2. __ Right-click a QLogic adapter and then click **Enable Target Mode**.
3. __ In the Enable Target Mode window, click **Soft alpa creation method**.

   Attention: Do not choose the hard alpa creation method unless directed to do so by your IBM service representative.
4. __ Click **OK**. On the **General** tab for the adapter in the VE console, verify that the value for **Mode** now displays **target**.
5. __ (Optional) View the modes and WWPNs of all of the server's fibre channel cards by completing the following steps: .

   a. __ In the VE console, click the server icon.

   b. __ Click the **General** tab. See Figure 100 on page 136.
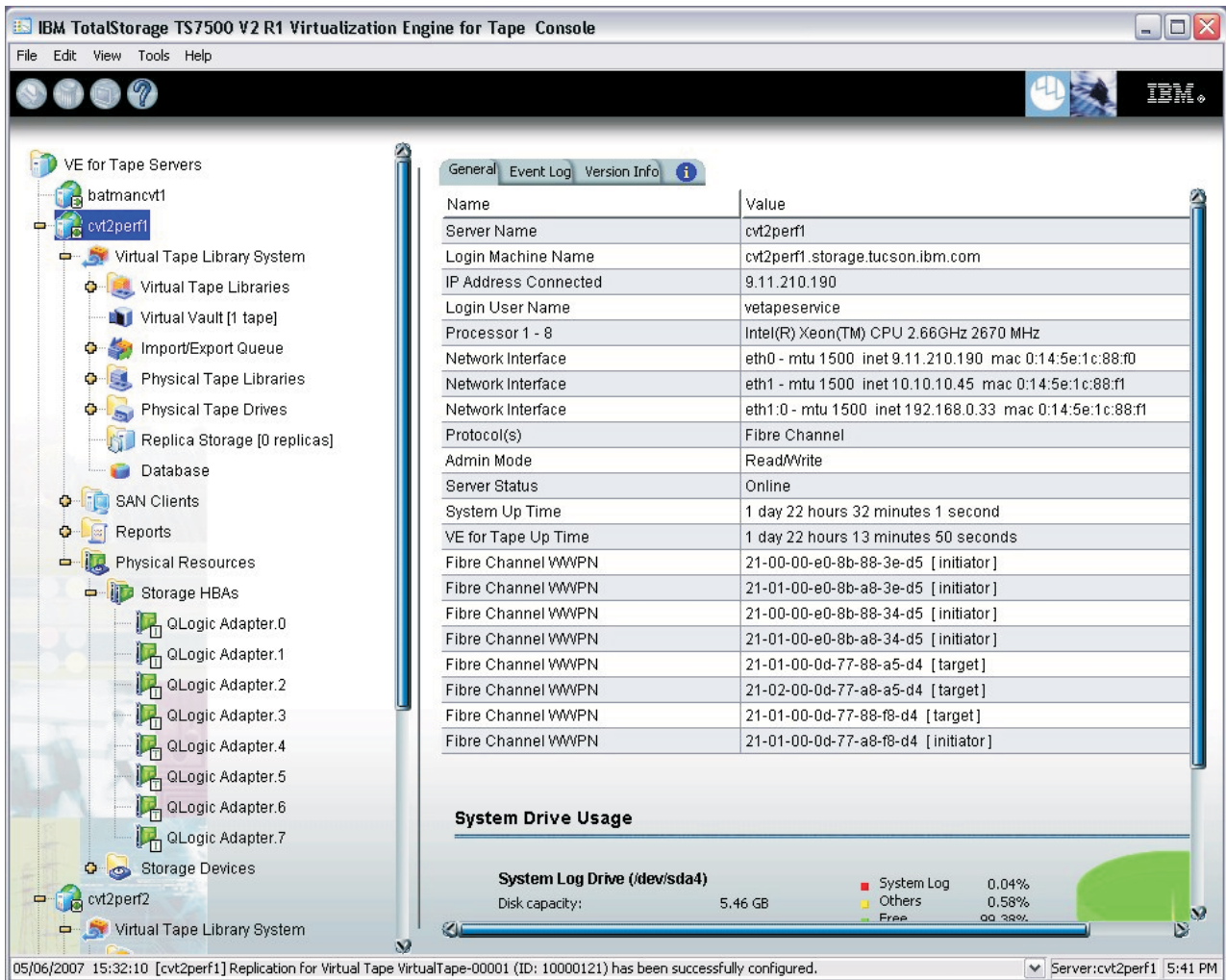
Figure 100. Server fibre channel port modes and WWPNs

Scanning, preparing, and assigning physical tape devices

To prepare the TS7500 Virtualization Engine to use physical tape resources, complete the following steps:

1. __ Verify the following conditions:

   - Physical connectivity exists between the physical tape resources and the appropriate fibre channel ports:

     TS7500 EE installations
     > QLogic adapters 5, 7, 9, or 11

     TS7500 LE installations
     > QLogic adapter 3. If more than two fibre channel cards are installed, any ports numbered higher than 3 are also available for connectivity.

   - All ports connected to physical tape resources are set to initiator mode. To set a port to initiator mode, perform the following steps:

     a. __ In the VE console, expand **Physical Resources** → **Storage HBAs**.

     b. __ Right-click the adapter and then click **Disable Target Mode**.

     c. __ In the Disable Target Mode window, click **OK**.

2. __ In the VE console:
   a. __ Expand the icon for the server.
   b. __ Right-click **Physical Devices** and then click **Rescan**.
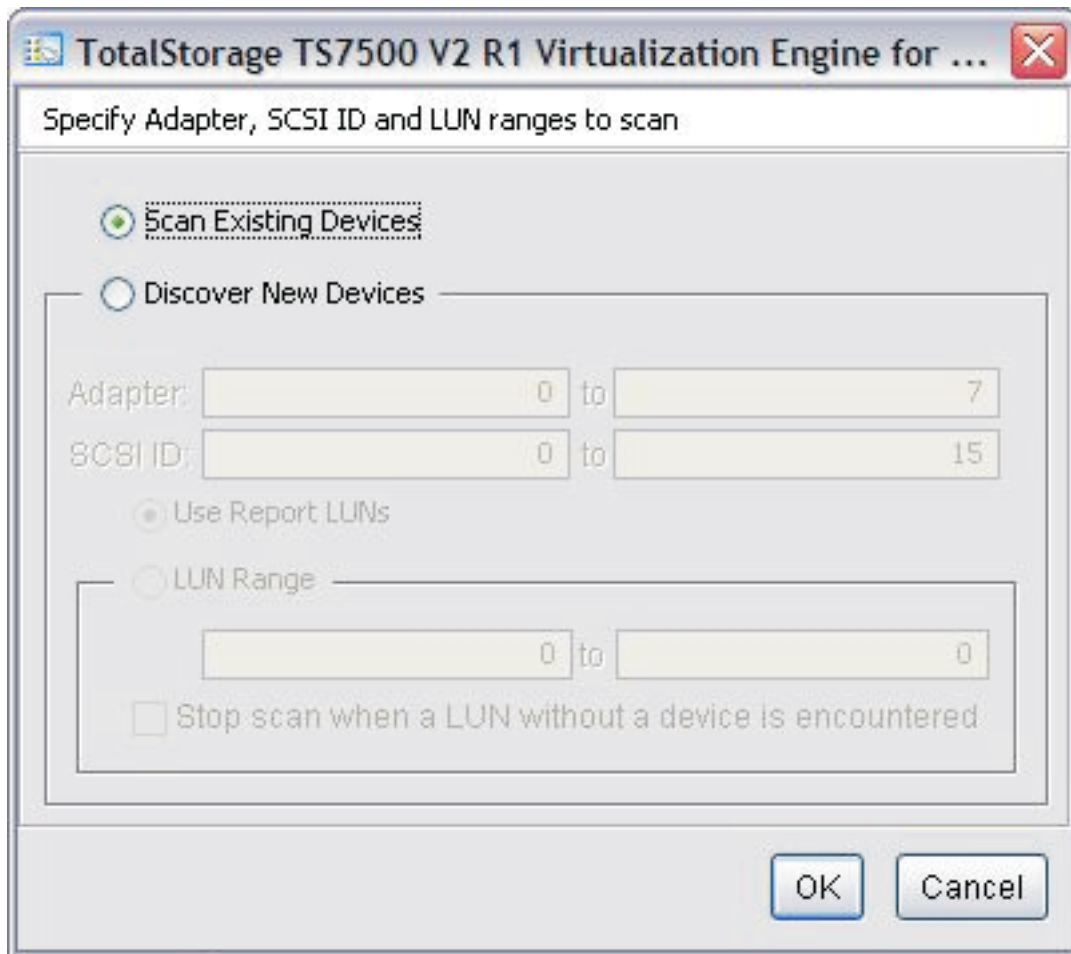
Figure 101. Rescanning physical devices

   c. __ In the ″Specify Adapter, SCSI ID and LUN ranges to scan″ window:
      1) __ Click **Scan Existing Devices**.
      2) __ Click **OK**.
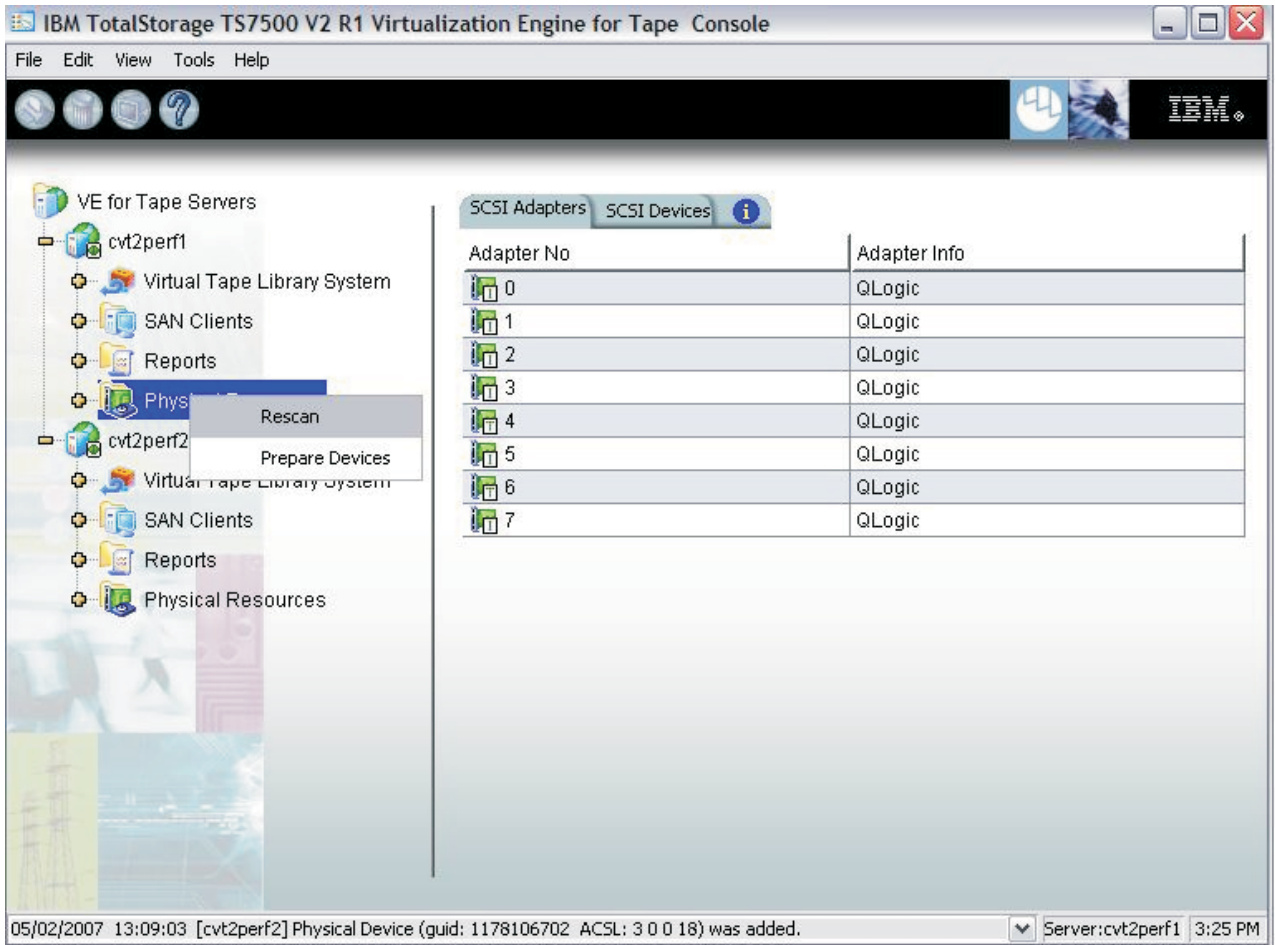
Figure 102. Scanning existing devices

3. __ In the VE console, expand **Physical Resources** → **Storage Devices** → **Fibre Channel Devices**.

4. __ Right-click **Fibre Channel Devices** and then click **Prepare Devices**.

5. __ In the Select a Preparation Operation window, select **Reserved for Direct Device** from the **Device Category** list.

6. __ Click **Next**.

7. __ In the Select Physical Devices page:

   a. __ Select the physical devices.

   b. __ Click **Next**.

8. __ In the Prepare Devices page:

   a. __ Verify the correct physical devices were selected.

   b. __ Click **Finish**.

9. __ In the VE console, right-click **Physical Tape Libraries** and then click **Assign**.

10. __ In the Assign Physical Tape Libraries window:

    a. __ From the **Device Name** list, select the library or libraries.

    b. __ Click **Assign**.

    c. __ In the notification window, click **OK**.

11. __ Right-click the newly-assigned library and then click **Assign**.

12. __ In the Assign Physical Tape Drives window:

   a. __ From the **Device Name** list, select the tape drive or drives.

   b. __ Click **Assign**.

   c. __ In the notification window, click **OK**.

Adding fibre channel clients

To add fibre channel clients, complete the procedure in "Adding SAN clients" on page 48.

Associating WWPNs with clients

A switched fibre channel environment can make it difficult to determine the WWPN for each port.

- In a switched fibre channel environment, the TS7500 Virtualization Engine queries the fibre channel switch for its simple name server (SNS) database and then displays a list of all available WWPNs. You must still identify which WWPN is associated with each machine.

- In a non-switched fibre channel environment, you can manually determine the WWPN for each port. The method to do so varies by hardware vendor.

In either case, see the documentation for your hardware for the procedure to determine WWPNs.

The *Everyone_FC* client is a generic client that you can assign to your virtual resources. It allows any WWPN not already associated with a fibre channel client to have read/write non-exclusive access to any virtual resources assigned to *Everyone_FC*.

For security purposes, assign specific WWPNs to specific clients. Use the *Everyone_FC* client for remaining WWPNs.

To associate particular WWPNs to clients, complete the following steps:

1. __ In the VE console, expand **SAN Clients**.

2. __ Right-click the client and then click **Properties**.

3. __ Click the **Initiator WWPNs** tab.

4. __ From the **Initiator WWPN** list, select the WWPNs you wish to associate with the client.

5. __ (Optional) To add WWPNs to the **Initiator WWPN** list:

   a. __ Click **Add**.

   b. __ In the Add Initiator WWPN window, type the WWPN in the **Initiator WWPN** field.

   c. __ Click **OK**.

6. __ Click **OK**.

Refer to the documentation for your client machines for the method to determine their WWPNs.

Assigning virtual tape devices to fibre channel clients

To assign virtual tape devices to fibre channel clients, complete the following steps:

1. __ In the VE console, expand **SAN Clients**.
2. __ Right-click a SAN client and then click **Assign**.
3. __ (Optional) Select the **Allow tape drive(s) in the tape library to be assigned manually** check box. This allows selection of individual tape drives. Not selecting this check box only allows selection of virtual tape libraries only.
4. __ From the list, select the virtual tape drives or tape libraries to be assigned. If a client has multiple ports, balance the association of client ports to virtual devices for best performance.
5. __ Click **Next**.
6. __ From the Target WWPN list, select a fibre channel target.
7. __ Click **Next**.
8. __ Verify your selections and click **Finish**.

Accessing new virtual devices

In order to access new virtual devices after fibre channel client configuration, rescan for the new devices at the client machine or restart the client machine, depending upon the requirements of the operating system.

Splitting virtual tape drives among separate fibre channel ports

The TS7500 Virtualization Engine can split the tape drives in a virtual tape library across separate ports. This increases fibre channel bandwidth between the TS7500 Virtualization Engine and the host system.

If connecting through a SAN, you must zone the target WWPNs of the TS7500 Virtualization Engine with the WWPNs of your backup server or host.

This section provides an example of configuring an AIX host to use a virtual tape library with the virtual tape drives split across separate ports. In the example, the default libraries were unassigned from the Everyone_FC SAN client and deleted. Adapters 5 and 7 were changed to target mode.

The following hardware components comprise the storage environment in this example.

- A TS7500 Virtualization Engine with one TS7520 Server and two TS7520 Cache Controllers
- A System p AIX host system with fibre channel HBAs
- A System x server with the VE console installed
- An Ethernet switch
- A 2109 F32 fibre channel switch

Establishing physical connectivity

In this example, four fibre channel HBAs on the AIX host connect to the TS7500 Virtualization Engine. The fibre channel HBAs of the AIX host connect to ports 28,
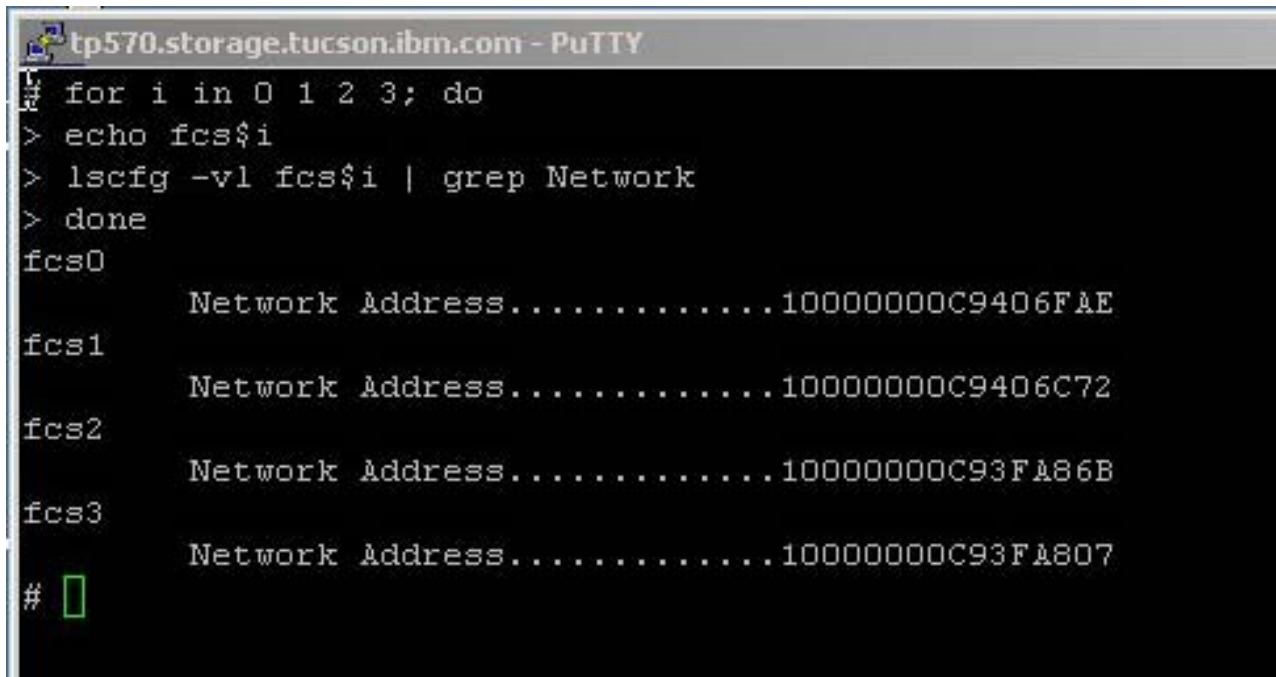
29, 30, and 31 of the 2109 F32 fibre channel switch. Adapters 0, 1 ,2, 3 of the
TS7500 Virtualization Engine connect to ports 16, 17, 18, and 19 of the 2109 F32
fibre channel switch.

Identifying the WWPNs of the host

Tip: Obtaining and documenting the WWPNs of your hosts and TS7500
Virtualization Engines facilitates zoning and SAN client assignment.

Each fibre channel HBA, operating system, and storage area network have their
own methods of identifying WWPNs. See the documentation specific to your
hardware and environment to determine the correct method.

In the example, the WWPNs of the AIX host were obtained by using the command
`lscfg -vl fcsX | grep Network`, where *X* is the adapter number.


```
tp570.storage.tucson.ibm.com - PuTTY
# for i in 0 1 2 3; do
> echo fcs$i
> lscfg -vl fcs$i | grep Network
> done
fcs0
        Network Address..............10000000C9406FAE
fcs1
        Network Address..............10000000C9406C72
fcs2
        Network Address..............10000000C93FA86B
fcs3
        Network Address..............10000000C93FA807
#
```

Figure 103. Identifying the WWPNs of the AIX host

In the example, the WWPNs of the AIX host HBAs are:
- 10-00-00-00-C9-40-6F-AE
- 10-00-00-00-C9-40-6C-72
- 10-00-00-00-C9-3F-A8-6B
- 10-00-00-00-C9-3F-A8-07

Identifying the target WWPNs of the TS7500 Virtualization Engine

To identify the target WWPN of a fibre channel port in the TS7500 Virtualization
Engine, complete the following steps:
1. __ In the VE console, expand the server icon.
2. __ Expand **Physical Resources** → **Storage HBAs**.

3. __ Click an adapter.
4. __ Click the **General** tab.
5. __ Note the value for **Target WWPN**.

Note: The value for **WWPN** is the adapters actual WWPN. For zoning, use the target WWPN. This is an alias created to facilitate Failover and physical card replacement.

Creating zones

After identifying WWPNs, you must configure SAN zones. To optimize performance, balance the number of virtual devices across the available TS7500 Virtualization Engine target WWPNs. In this example, it does not matter which AIX adapter is zoned with which TS7500 Virtualization Engine adapter. Your specific SAN topology and configuration dictate zoning configuration.

Table 9 shows an one-to-one mapping between the TS7500 Virtualization Engine and the AIX host. This mapping forms the basis to create the respective zones.

Table 9. Mapping for zone creation

Zone Name	TS7500 Virtualization Engine WWPNs	AIX Host WWPNs
Tp570fcs0	21-01-00-0d-77-17-32-46	10-00-00-00-C9-40-6F-AE
Tp570fcs1	21-02-00-0d-77-37-32-46	10-00-00-00-C9-40-6C-72
Tp570fcs2	21-01-00-0d-77-07-f1-7d	10-00-00-00-C9-3F-A8-6B
Tp570fcs3	21-02-00-0d-77-37-f1-7d	10-00-00-00-C9-3F-A8-07

The WWPN of the AIX host is 10-00-00-00-C9-40-6F-AE and the target WWPN of the desired virtual library is 21-01-00-0d-77-17-32-46. These two WWPNs must be in a zone so that there is logical connectivity between the host and the TS7500 Virtualization Engine. In the example, the operator established a zone named *Tp570fcs0*. The operator then created three additional zones for the WWPN pairs shown in Table 9. See Figure 104 on page 143.
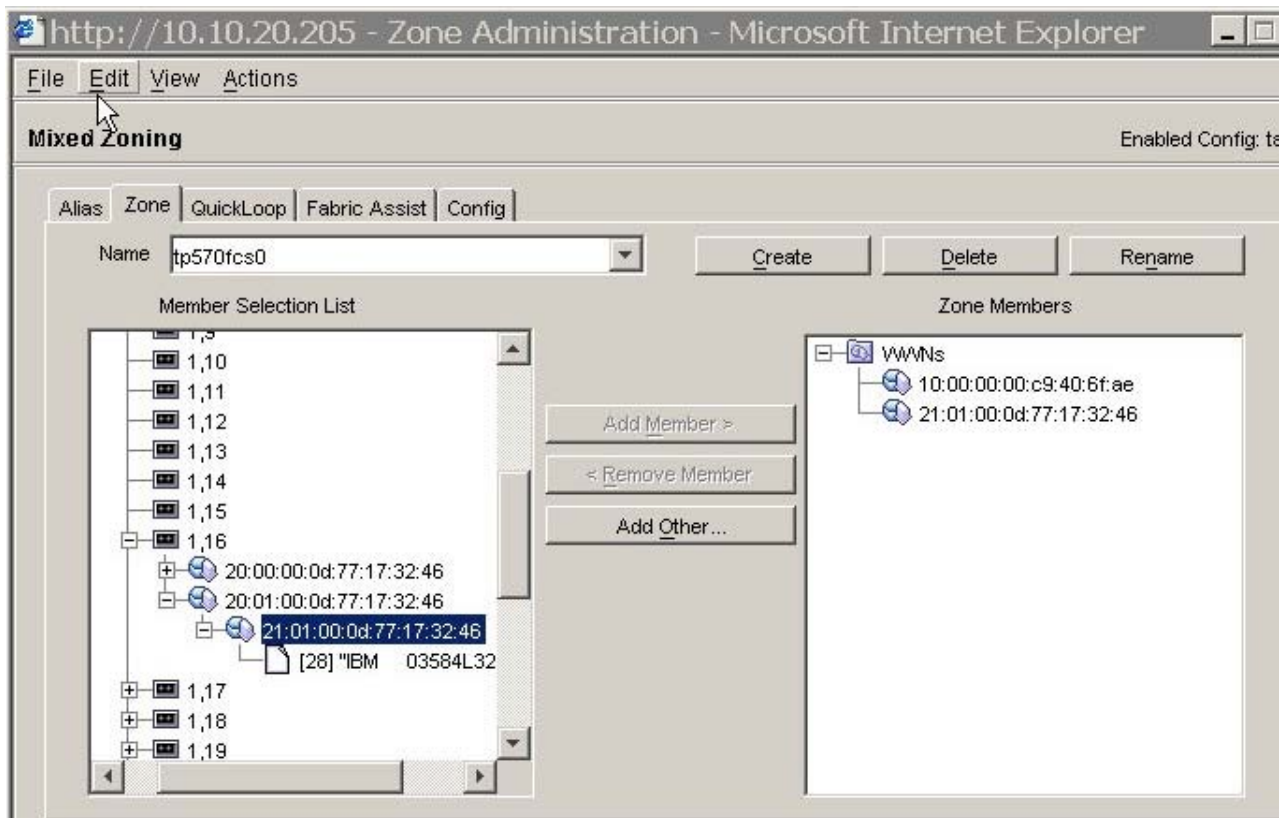
Figure 104. Creating the zones

Verify correct zone configuration. See Figure 105.
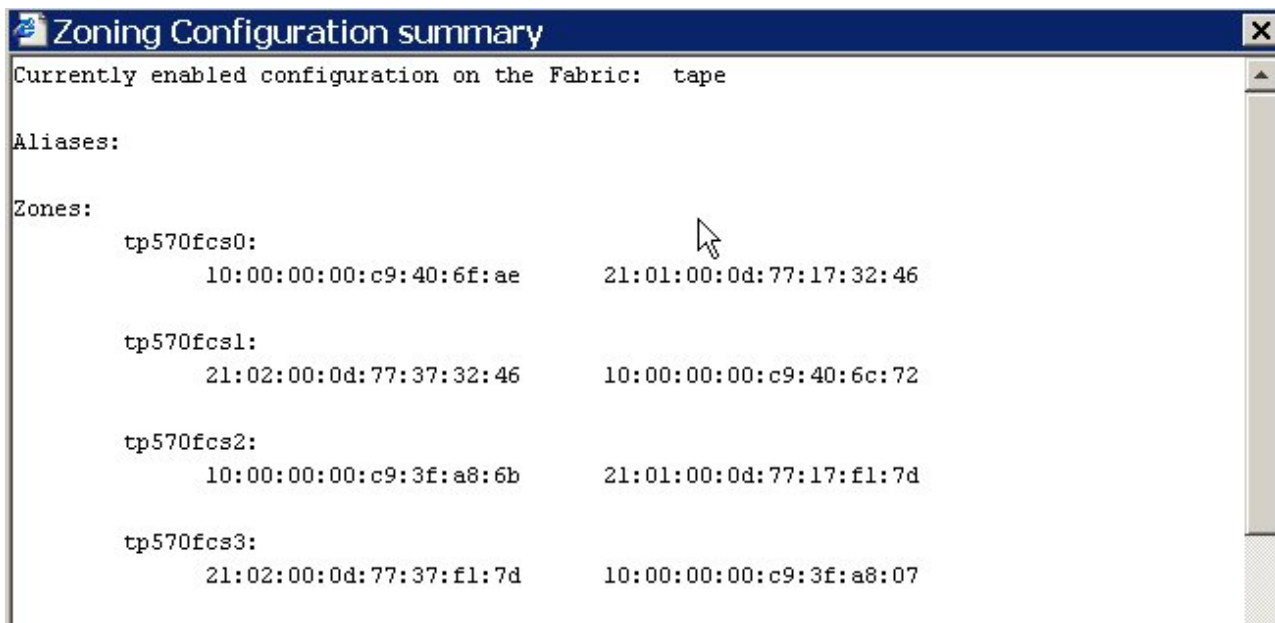
Figure 105. Zone configuration summary

The new zones group together the WWPNs of the AIX host and the WWPNs of the TS7500 Virtualization Engine. This step facilitates setting up the SAN clients and making virtual device assignments in the VE console. The TS7500 Virtualization Engine queries the SAN fabric and uses the resulting information to assist with those operations.

The TS7500 Virtualization Engine provides fibre channel fabric information using the SNS protocol. If your SAN supports this protocol, additional information is available for each Qlogic adapter. In this example, the SNS table for adapter 4 correctly shows the WWPN of the AIX host. This provides verification from the TS7500 Virtualization Engine that the two WWPNs are correctly zoned.

Note: To refresh the display after making changes to the SAN fabric, right-click the adapter and then click **Refresh SNS**.

Note: Direct cabling (that is, point-to-point topology) does not appear in the SNS table.

Adding a SAN client

Adding a SAN client allows you to restrict access to a virtual library or drive to a specific WWPN / SAN Client. See "Adding SAN clients" on page 48 for the procedure to add SAN clients.

Creating a virtual tape library

See "Creating virtual tape libraries" on page 39 for the procedure to create virtual tape libraries. In this example, a virtual TS3500 Tape Library with 16 virtual Ultrium 3 drives was created.

Making SAN client to virtual device assignment

To access a virtual device, the device must be assigned to a SAN client. The assignment can be to either the *Everyone_FC* client or to a user-added SAN client. A virtual device can be assigned to multiple SAN clients. This is required when configuring a LAN-free setup with TSM. The TSM server and the TSM storage agent must be able to access the same virtual tape devices. Two assignments enable this to happen.

In this example, the 16 virtual drives are split evenly among the four TS7500 Virtualization Engine WWPNs and the four AIX WWPNs.

To assign virtual devices to SAN clients, see "Assigning virtual tape libraries to SAN clients" on page 49.

Performing a device discovery on the host

After establishing physical and virtual connectivity, you must perform a device discovery on the host system.

Note: With AIX hosts after a switch from point-to-point topology to fabric switch topology, remove and then re-install the fibre channel HBA device driver to ensure that the virtual devices configure correctly. topology.

```
tp570.storage.tucson.ibm.com - PuTTY
# cfgmgr -l fcs0
# cfgmgr -l fcs1
# cfgmgr -l fcs2
# cfgmgr -l fcs3
# lsdev -Cc tape
rmt0   Available 0A-08-01 IBM 3580 Ultrium Tape Drive (FCP)
rmt1   Available 0A-08-01 IBM 3580 Ultrium Tape Drive (FCP)
rmt2   Available 0A-08-01 IBM 3580 Ultrium Tape Drive (FCP)
rmt3   Available 0A-08-01 IBM 3580 Ultrium Tape Drive (FCP)
rmt4   Available 0B-08-01 IBM 3580 Ultrium Tape Drive (FCP)
rmt5   Available 0B-08-01 IBM 3580 Ultrium Tape Drive (FCP)
rmt6   Available 0B-08-01 IBM 3580 Ultrium Tape Drive (FCP)
rmt7   Available 0B-08-01 IBM 3580 Ultrium Tape Drive (FCP)
rmt8   Available 0C-08-01 IBM 3580 Ultrium Tape Drive (FCP)
rmt9   Available 0C-08-01 IBM 3580 Ultrium Tape Drive (FCP)
rmt10  Available 0C-08-01 IBM 3580 Ultrium Tape Drive (FCP)
rmt11  Available 0C-08-01 IBM 3580 Ultrium Tape Drive (FCP)
rmt12  Available 0D-08-01 IBM 3580 Ultrium Tape Drive (FCP)
rmt13  Available 0D-08-01 IBM 3580 Ultrium Tape Drive (FCP)
rmt14  Available 0D-08-01 IBM 3580 Ultrium Tape Drive (FCP)
rmt15  Available 0D-08-01 IBM 3580 Ultrium Tape Drive (FCP)
smc0   Available 0A-08-01 IBM 3584 Library Medium Changer (FCP)
#
```

Figure 106. Device discovery on the host

The sixteen virtual tape drives and the virtual tape library are available to the host.

Summary

This section showed one example of configuring the TS7500 Virtualization Engine to a host. Additional hosts increase the complexity of the configuration; carefully plan any such configuration operations.

Chapter 9. iSCSI

The TS7500 Virtualization Engine supports the iSCSI target protocol.

iSCSI builds on the SCSI standard by using the IP network as the connection link between various entities involved in a configuration. iSCSI inherits many of the basic concepts of SCSI. For example, the entity making requests is called an initiator, while the entity responding to requests is called a target, as with SCSI. Initiators can make requests to targets, but the reverse is not true. Each target and initiator entity has a unique identifier.

By default, when a machine connects to the TS7500 Virtualization Engine as an iSCSI client, it becomes an iSCSI initiator.

Supported platforms

The following platforms support iSCSI:
- Windows
- Linux

Windows configuration for iSCSI

Requirements

The following are requirements for iSCSI configuration on a Windows client:
- A TS7500 Virtualization Engine with installed Ethernet card.
- A Windows client machine.
- iSCSI initiator software installed on each client machine. Microsoft makes available for download iSCSI initiator software for Windows at http://www.microsoft.com/windowsserversystem/storage/iscsi.mspx.

Important: Do not install TS7500 Virtualization Engine client software on any Windows client.

Enabling iSCSI

To enable iSCSI in the TS7500 Virtualization Engine, right-click the server icon in the VE console and then click **Options** → **Enable iSCSI**.
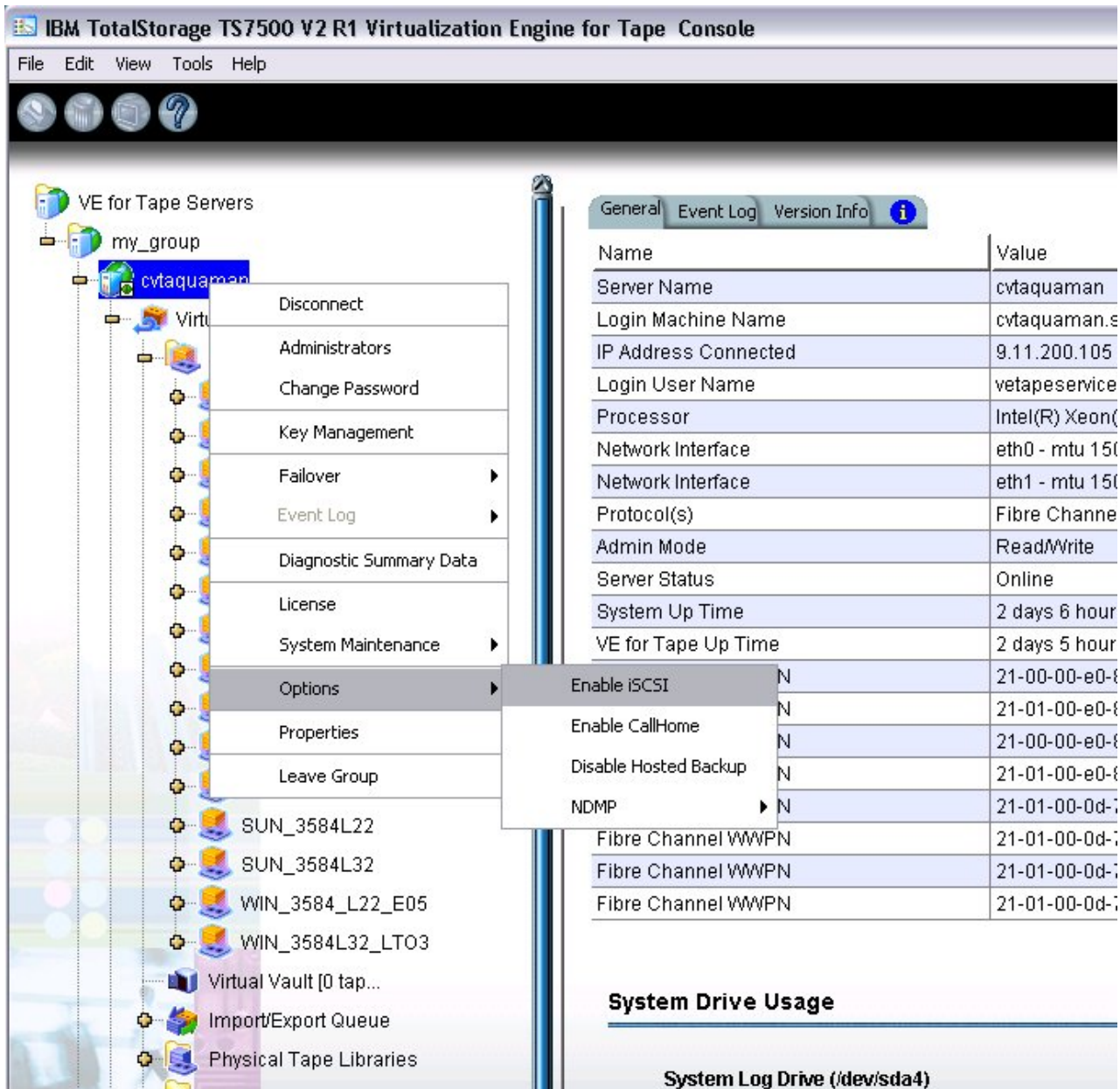
Figure 107. Enabling iSCSI

This enables iSCSI and also creates a SAN client called *Everyone_iSCSI*. This client does not correspond to any specific client machine. You can use this client to create iSCSI targets accessible by any iSCSI client connecting to the TS7500 Virtualization Engine.

The following sections contain information about configuring the TS7500 Virtualization Engine to access iSCSI clients.

Registering client initiators with the TS7500 Virtualization Engine

Registering the client initiators with the TS7520 Server allows the server to access the available initiators To register the client initiators using Microsoft iSCSI Initiator, complete the following steps:

Note: If you are using a different iSCSI initiator, see the documentation provided by the vendor for the procedure.

1. __ Start Microsoft iSCSI Initiator by performing one of the following:
   - On the Windows desktop, double-click the **Microsoft iSCSI Initiator** icon.
   - Perform the following:
     a. __ Click **Start** → **Settings** → **Control Panel**.
     b. __ Double-click the **SCSI Initiator** icon.
2. __ In the iSCSI Initiator, click the **Discovery** tab.
3. __ In the **Target Portals** area, click **Add**.
4. __ In the **IP address or DNS name** field, type the TS7520 Server's IP address or resolvable DNS name.
5. __ (Optional) If the client is a mobile client:
   a. __ Click **Advanced**.
   b. __ Select the **CHAP logon information** check box.
   c. __ In the **User name** field, type a user name that belongs to one of the TS7500 Virtualization Engine server's mobile clients.
   d. __ In the **Target secret** field, type the password for the mobile client's user name.
   e. __ Click **OK**.
6. __ Click **OK**. Any iSCSI targets assigned to the client appear in the **Targets** list on the **Targets** tab. The list is blank at this point because no iSCSI targets are assigned to the server's iSCSI clients.

Adding iSCSI clients

To add an iSCSI client, complete the following steps:

1. __ In the VE console, expand the server icon.
2. __ Right-click **SAN Clients** and then click **Add**.
3. __ Click **iSCSI**.
   a. __ Click **iSCSI**.
   b. __ Perform one of the following: If the new client is a mobile client, select the **Create this iSCSI client as a mobile user** check box.
   c. __ Click **Next**.
4. __ Perform one of the following:
   - **The new client is a mobile client.** A mobile client is an account with a user name and password with which you can authenticate to the TS7520 Server from any iSCSI client. In contrast, a stationary iSCSI client corresponds to a specific iSCSI client initiator and to the client machine that owns it.
     a. __ Select the **Create this iSCSI client as a mobile user** check box.
     b. __ Click **Next**.
     c. __ Perform one of the following:
        - __ If a mobile client user account that you want to use already exists, select it from the **Username** list.
        - __ If no mobile client user accounts exist that you want to use:
          1) __ Click **Add**.
          2) __ In the **User Name** field, type a user name.
          3) __ In the **Password** field, type a password. The password must be between 12 and 16 characters in length.

4) __ In the **Confirm Password** field, type the password again.

5) __ Click **OK**.

6) __ Select the new mobile client user account from the **Username** list.

d. __ Click **Next**.

- **The new client is not a mobile client.**

  a. __ Click **Next**.

  b. __ In the Client Display Name window, perform one of the following:

    – __ Click **Create from Initiator Name** to automatically extract the host name from the iSCSI initiator name for use as the client's display name in the VE console.

    – __ Click **Create Custom Name** and type a desired display name in the **Display Name** field.

  c. __ Click **Next**.

  d. __ Perform one of the following:

    – __ If an initiator name that you want to use already exists, select it from the **Initiator Name** list.

    – __ If no initiator names exist that you want to use:

      1) __ Click **Add**.

      2) __ In the **Initiator Name** field, type the name of the initiator you want to use. For example, if you want to use a client initiator that you registered with Microsoft iSCSI Initiator in "Registering client initiators with the TS7500 Virtualization Engine" on page 148, type the name that appears under **Initiator Node Name** on the **General** tab of the iSCSI Initiator Properties window that opens when you start the Microsoft iSCSI Initiator application.

      3) __ Click **OK**.

      4) __ Select the new initiator name from the **Initiator Name** list.

  e. __ Click **Next**.

  f. __ Perform one of the following:

    – __ If an iSCSI user access account that you want to use already exists, select it from the **Username** list.

    – __ If no iSCSI user access accounts exist that you want to use:

      1) __ Click **Add**.

      2) __ In the **User Name** field, type a user name.

      3) __ In the **Password** field, type a password. The password must be between 12 and 16 characters in length.

      4) __ In the **Confirm Password** field, type the password again.

      5) __ Click **OK**.

      6) __ Select the new iSCSI user access account from the **Username** list.

  g. __ Click **Next**.

5. __ In the Add the iSCSI Client window, verify the information entered is correct and then click **Finish**.

Creating targets for iSCSI clients

To create targets for iSCSI clients, complete the following steps:

1. __ In the VE console, add at least one iSCSI device for use as a target for iSCSI clients. See "Adding iSCSI clients" on page 149.
2. __ In the VE console, right-click an iSCSI client and then click **Create Target**.
3. __ In the Create iSCSI Target window:
    a. __ (Optional) In the **Target Name** field, type a new name for the target.
    b. __ From the **IP Address** list, select the IP address of the TS7520 Server.
    c. __ Select one of the following:

        Read/Write Non-Exclusive access mode
            Select this option if your servers are clustered. Clustered servers prevent multiple clients from writing data at the same time, which can corrupt data.

        Read/Write Exclusive access mode
            Select this option if your servers are not clustered, allowing servers to write data at the same time. This option prevents multiple servers from writing data at the same time, thus preventing data corruption.

    d. __ In the **Starting LUN** field, type or click the arrows to select **0**.
    e. __ Click **Next**.
4. __ In the Verify iSCSI Target Properties window, verify the information selected for the target is correct and then click **Finish**.
5. __ In the successful creation notification window, click **OK**.
6. __ In the Create iSCSI Target window, click **Yes**.
7. __ (Optional) Select the **Allow tape drive(s) in the tape library to be assigned manually** check box. This allows selection of individual tape drives. Not selecting this check box only allows selection of virtual tape libraries only.
8. __ From the list, select the virtual tape drives or tape libraries to be assigned. If a client has multiple ports, balance the association of client ports to virtual devices for best performance.
9. __ Click **Next**.
10. __ From the list, select a virtual resource.
11. __ Click **Next**.
12. __ Verify your selections and click **Finish**.

Logging the iSCSI client on to the target

To log an iSCSI client on to a target using Microsoft iSCSI Initiator, complete the following steps:

Note: If you are using a different iSCSI initiator, see the documentation provided by the vendor for the procedure.

1. __ Start Microsoft iSCSI Initiator by performing one of the following:
    • On the Windows desktop, double-click the **Microsoft iSCSI Initiator** icon.
    • Perform the following:
        a. __ Click **Start** → **Settings** → **Control Panel**.
        b. __ Double-click the **SCSI Initiator** icon.
2. __ In the iSCSI Initiator, click the **Targets** tab.
3. __ Click **Refresh**.
4. __ From the **Targets** list, select the desired target.

5. __ Click **Log On**.
6. __ (Optional) Select the **Automatically restore this connection when the system reboots** check box.
7. __ Click **Advanced**.
   a. __ Click **Advanced**.
   b. __
   c. __
   d. __
   e. __ Click **OK**.
8. __ Select the **CHAP logon information** check box.
9. __ Perform one of the following:
   • **The iSCSI client is a mobile client**.
      a. __ In the **User name** field, type a user name that belongs to one of the TS7500 Virtualization Engine server's mobile clients.
      b. __ In the **Target secret** field, type the password for the mobile client's user name.
      c. __ Click **OK**.
   • **The iSCSI client is not a mobile client.**
      a. __ In the **User name** field, type the user name entered when the iSCSI client was created in the VE console.
      b. __ In the **Target secret** field, type the password entered when the iSCSI client was created in the VE console.
      c. __ Click **OK**.
10. __ Click **OK**.
11. __ On the **Targets** tab of the iSCSI Initiator Properties window, verify that the target status now shows **Connected**.

To log an iSCSI client off from a target using Microsoft iSCSI Initiator, complete the following steps:

Note: If you are using a different iSCSI initiator, see the documentation provided by the vendor for the procedure.

1. __ In Microsoft iSCSI Initiator, click the **Targets** tab.
2. __ From the **Targets** list, select the target's check box.
3. __ Click **Details**.
4. __ From the **Identifier** list, select the target's identifier.
5. __ Click **Log Off**.
6. __ Click **OK**.
7. __ On the Targets tab, verify that the target status now shows **Inactive**.

Disabling iSCSI

Note: Before disabling iSCSI, you must first remove all iSCSI initiators and targets for the TS7520 Server.

To disable iSCSI in the TS7500 Virtualization Engine, right-click the server icon in the VE console and then click **Options** → **Disable iSCSI**.

Linux configuration for iSCSI

Installing and configuring Linux iSCSI initiators

Install and configure an iSCSI software initiator on each of your Linux client machines by performing the following steps on each machine:

1. __ Download the latest production iSCSI initiator from the following website: http://sourceforge.net/projects/linux-iscsi/

2. __ Extract the files from the downloaded .gz file by completing the following substeps:

   a. __ In the Linux client machine's command line interface, type the following:

   ```
   tar xfvz filename
   ```

   where *filename* is the name of the .gz file; for example, `linux-iscsi-3.4.3.gz`.

   b. __ Press the **Enter** key.

3. __ Compile the iSCSI initiator by completing the following substeps:

   a. __ In the Linux client machine's command line interface, navigate to the directory created by the file extraction (for example, the extraction of file `linux-iscsi-3.4.3.gz` creates a directory named `linux-iscsi-3.4.3`).

   b. __ Type `make clean` and then press the **Enter** key.

   c. __ Type `make` and then press the **Enter** key.

   d. __ Type `make install` and then press the **Enter** key.

4. __ Edit the `/etc/iscsi.conf` file by completing the following substeps:

   a. __ Perform one of the following:

   - __ **Not using CHAP** Add the following line to the end of the file:

     ```
     DiscoveryAddress=w.x.y.z
     ```

     where *w.x.y.z* is the IP address of the TS7520 Server.

   - __ **Using CHAP** Add the following lines to the end of the file:

     ```
     DiscoveryAddress=w.x.y.z
     OutgoingUsername=CHAP username
     OutgoingPassword=CHAP password
     ```

     where *w.x.y.z* is the IP address of the TS7520 Server.

     Tip: Record the CHAP username and password; you must enter them in the VE console.

5. __ In the Linux client machine's command line interface, start the iSCSI initiator by typing `/etc/init.d/iscsi start` and then pressing the **Enter** key.

Adding iSCSI clients

To add an iSCSI client, complete the following steps:

1. __ In the VE console, expand the server icon.

2. __ Right-click **SAN Clients** and then click **Add**.

3. __ Click **iSCSI**.

a. __ Click **iSCSI**.

b. __ Perform one of the following: If the new client is a mobile client, select the **Create this iSCSI client as a mobile user** check box.

c. __ Click **Next**.

4. __ Perform one of the following:

- **The new client is a mobile client.** A mobile client is an account with a user name and password with which you can authenticate to the TS7520 Server from any iSCSI client. In contrast, a stationary iSCSI client corresponds to a specific iSCSI client initiator and to the client machine that owns it.

  a. __ Select the **Create this iSCSI client as a mobile user** check box.

  b. __ Click **Next**.

  c. __ Perform one of the following:

  - __ If a mobile client user account that you want to use already exists, select it from the **Username** list.
  - __ If no mobile client user accounts exist that you want to use:
    1) __ Click **Add**.
    2) __ In the **User Name** field, type a user name.
    3) __ In the **Password** field, type a password. The password must be between 12 and 16 characters in length.
    4) __ In the **Confirm Password** field, type the password again.
    5) __ Click **OK**.
    6) __ Select the new mobile client user account from the **Username** list.

  d. __ Click **Next**.

- **The new client is not a mobile client.**

  a. __ Click **Next**.

  b. __ In the Client Display Name window, perform one of the following:

  - __ Click **Create from Initiator Name** to automatically extract the host name from the iSCSI initiator name for use as the client's display name in the VE console.
  - __ Click **Create Custom Name** and type a desired display name in the **Display Name** field.

  c. __ Click **Next**.

  d. __ Perform one of the following:

  - __ If an initiator name that you want to use already exists, select it from the **Initiator Name** list.
  - __ If no initiator names exist that you want to use:
    1) __ Click **Add**.
    2) __ In the **Initiator Name** field, type the name of the initiator you want to use. For example, if you want to use a client initiator that you registered with Microsoft iSCSI Initiator in "Registering client initiators with the TS7500 Virtualization Engine" on page 148, type the name that appears under **Initiator Node Name** on the **General** tab of the iSCSI Initiator Properties window that opens when you start the Microsoft iSCSI Initiator application.
    3) __ Click **OK**.
    4) __ Select the new initiator name from the **Initiator Name** list.

  e. __ Click **Next**.

f. __ Perform one of the following:

  – __ If an iSCSI user access account that you want to use already exists, select it from the **Username** list.

  – __ If no iSCSI user access accounts exist that you want to use:

    1) __ Click **Add**.

    2) __ In the **User Name** field, type a user name.

    3) __ In the **Password** field, type a password. The password must be between 12 and 16 characters in length.

    4) __ In the **Confirm Password** field, type the password again.

    5) __ Click **OK**.

    6) __ Select the new iSCSI user access account from the **Username** list.

g. __ Click **Next**.

5. __ In the Add the iSCSI Client window, verify the information entered is correct and then click **Finish**.

Creating targets for iSCSI clients

To create targets for iSCSI clients, complete the following steps:

1. __ In the VE console, add at least one iSCSI device for use as a target for iSCSI clients. See "Adding iSCSI clients" on page 149.

2. __ In the VE console, right-click an iSCSI client and then click **Create Target**.

3. __ In the Create iSCSI Target window:

   a. __ (Optional) In the **Target Name** field, type a new name for the target.

   b. __ From the **IP Address** list, select the IP address of the TS7520 Server.

   c. __ Select one of the following:

   Read/Write Non-Exclusive access mode
   Select this option if your servers are clustered. Clustered servers prevent multiple clients from writing data at the same time, which can corrupt data.

   Read/Write Exclusive access mode
   Select this option if your servers are not clustered, allowing servers to write data at the same time. This option prevents multiple servers from writing data at the same time, thus preventing data corruption.

   d. __ In the **Starting LUN** field, type or click the arrows to select **0**.

   e. __ Click **Next**.

4. __ In the Verify iSCSI Target Properties window, verify the information selected for the target is correct and then click **Finish**.

5. __ In the successful creation notification window, click **OK**.

6. __ In the Create iSCSI Target window, click **Yes**.

7. __ (Optional) Select the **Allow tape drive(s) in the tape library to be assigned manually** check box. This allows selection of individual tape drives. Not selecting this check box only allows selection of virtual tape libraries only.

8. __ From the list, select the virtual tape drives or tape libraries to be assigned. If a client has multiple ports, balance the association of client ports to virtual devices for best performance.

9. __ Click **Next**.

10. __ From the list, select a virtual resource.

11. __ Click **Next**.
12. __ Verify your selections and click **Finish**.

Logging the iSCSI client on to the target

To log an iSCSI client on to a target, type the following in the Linux client machine's command line interface:

```
/etc/init.d/iscsi reload
```

and then press the **Enter** key.

To display a list of all disk drives (including the target) that the client can access, type the following in the Linux client machine's command line interface:

```
cat /proc/scsi/scsi
```

and then press the **Enter** key.

Chapter 10. 3494 Tape Library configuration

The 3494 Tape Library is an automated tape library that multiple backup servers can share.

The 3494 Tape Library option for the TS7500 Virtualization Engine does not emulate the tape library, but it does emulate the tape drives inside, such as 3592 J1A Tape Drives. This makes it possible to import data from physical tape cartridges and export data on virtual tape cartridges to physical tape cartridges.
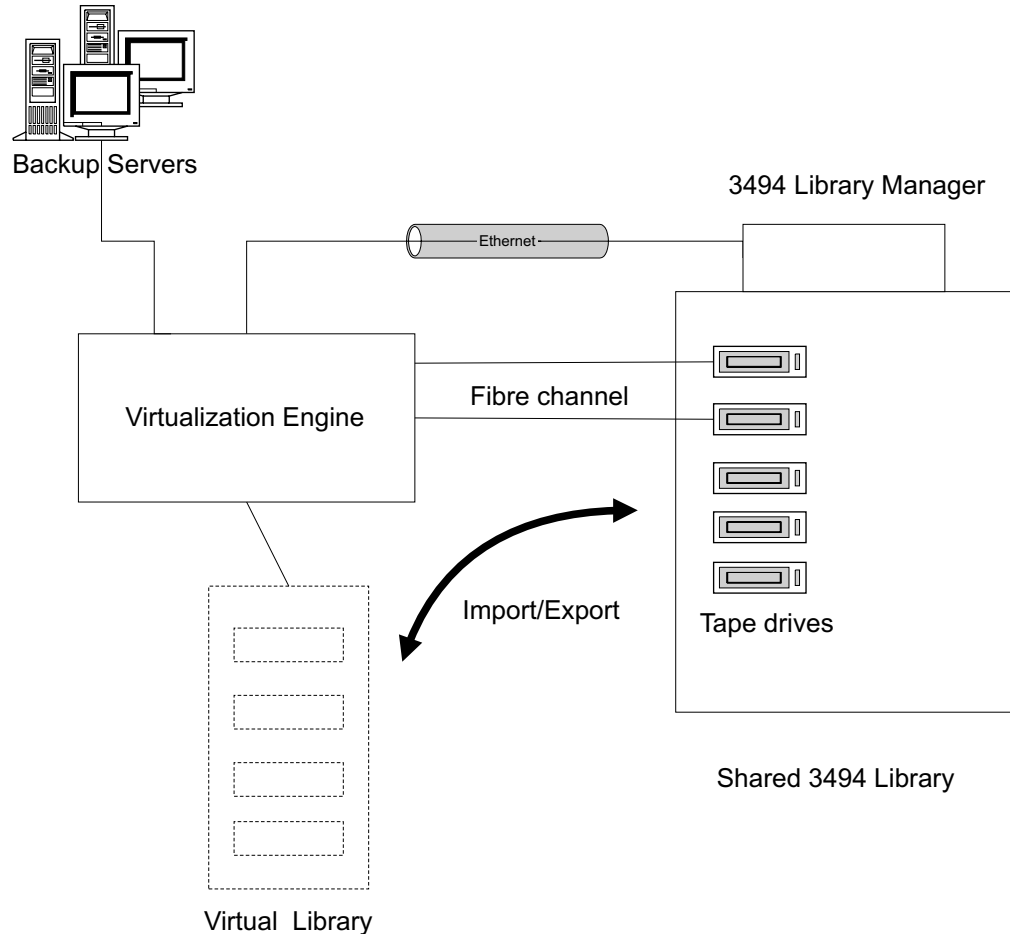
Figure 108. 3494 Tape Library configuration

To configure a TS7500 Virtualization Engine for a 3494 Tape Library, complete the following steps:

1. __ In the VE console, expand the server icon and then expand **Virtual Tape Library System**.
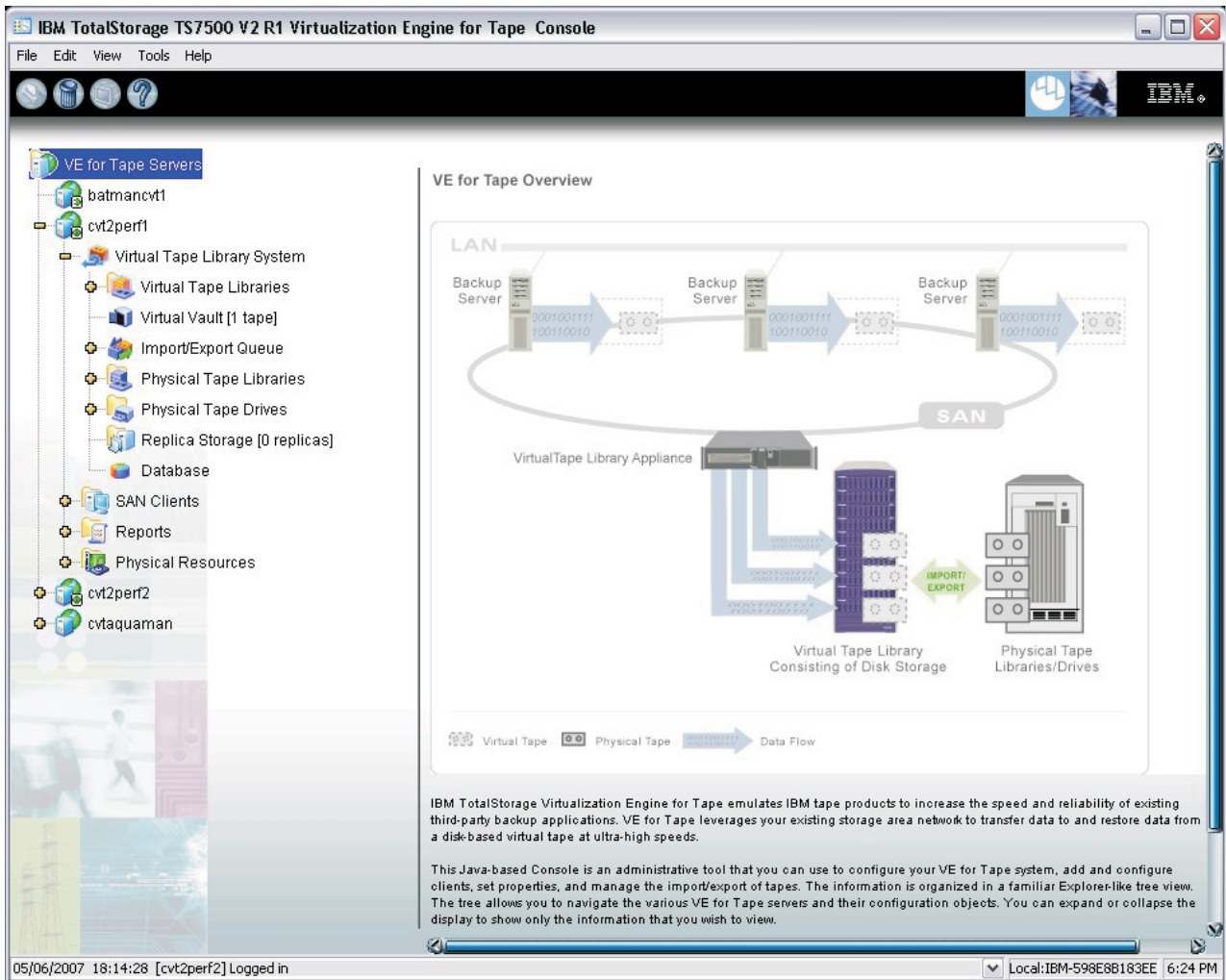
Figure 109. Expanding Virtual Tape Library System

2. __ Right-click **Physical Tape Libraries** and then click **Assign IBM 3494**.
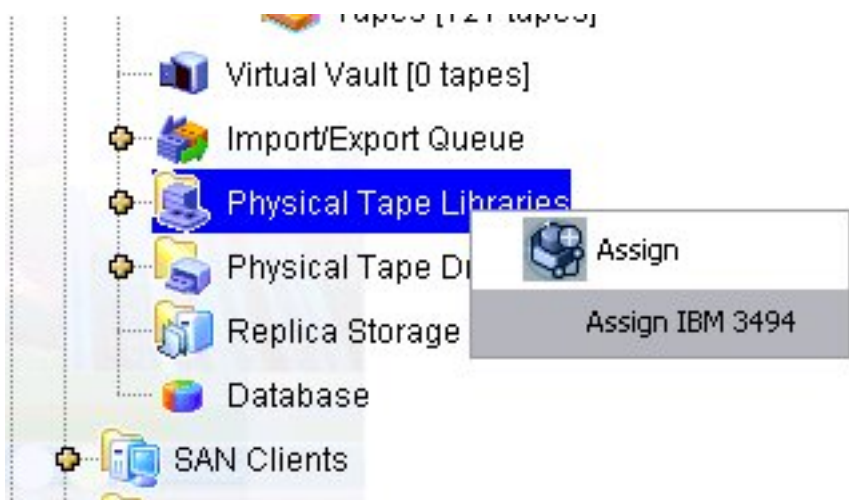
Figure 110. Assigning IBM 3494

3. __ Complete the following steps in the Set IBM 3494 library configuration window (see Figure 111):

Figure 111. Set IBM 3494 library configuration window

    a. __ In the **IP Address of Library Manager** field, type the primary Library Manager's IP address.

    b. __ (Optional) If there is a standby Library Manager:

        1) __ Select the **IP Address of Standby Library Manager** check box.

        2) __ In the **IP Address of Standby Library Manager** field, type the IP address of the standby Library Manager.

    c. __ In the **Category** field, type the category of media assigned to the TS7520 Server and to the 3494 Tape Library.

    d. __ In the Library Name field, type the name of the 3494 Tape Library.

    e. __ Click **OK**.

4. __ In the VE console, verify that the 3494 Tape Library appears in the **Physical Tape Libraries** list.
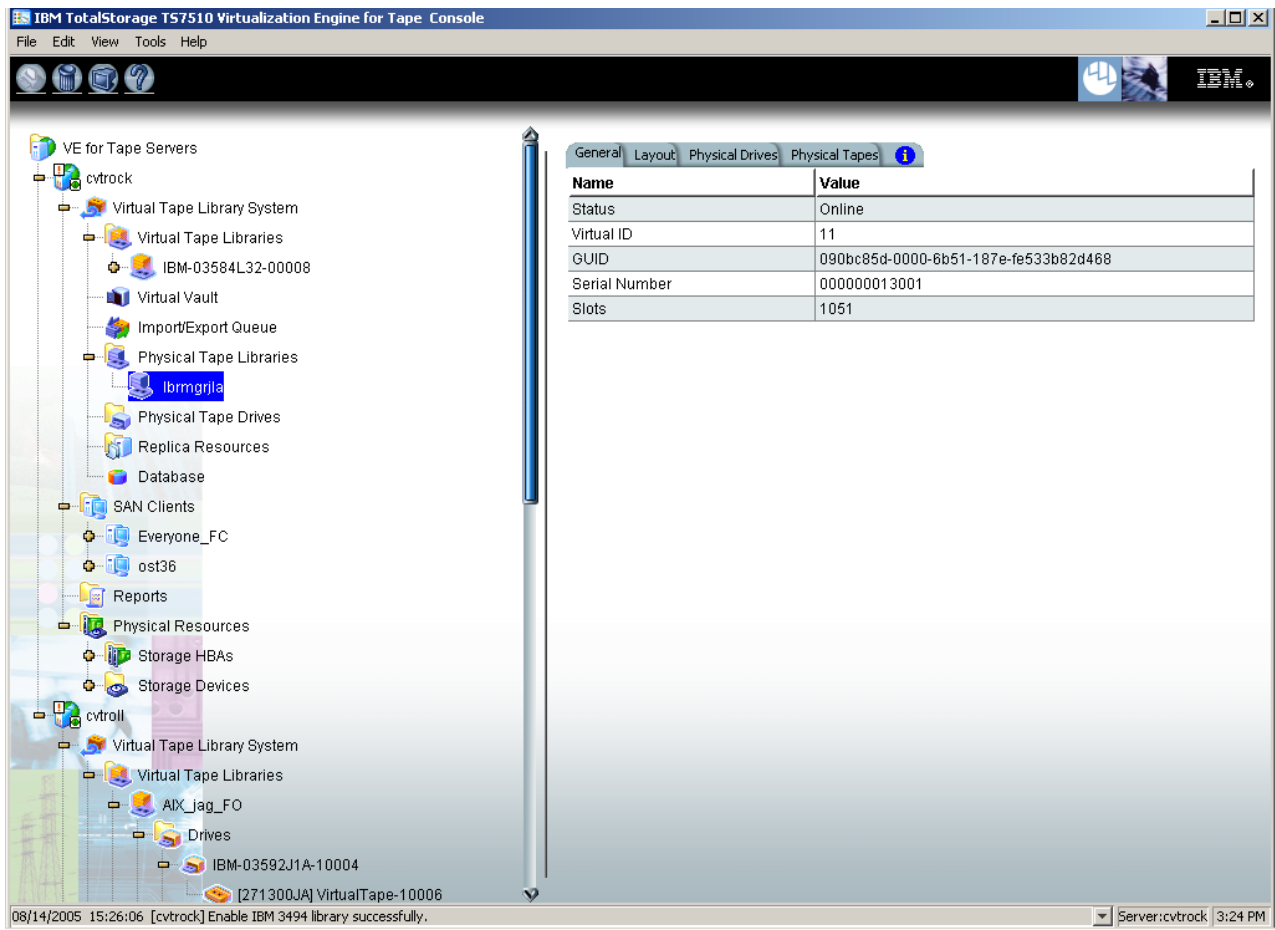
Figure 112. Physical Tape Libraries list

5. __ In the VE console, right-click the newly-assigned 3494 Tape Library and then click **Assign**.
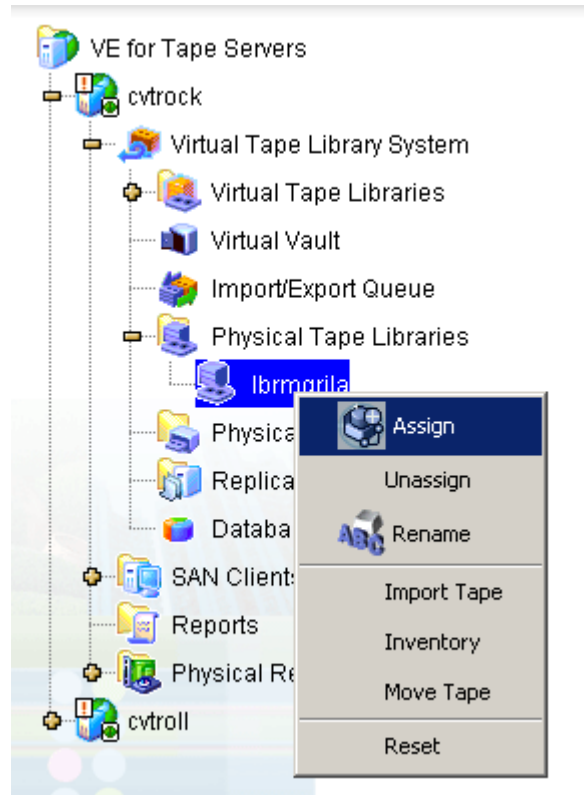
Figure 113. Assigning tape drives in the tape library

6. __ In the Assign Physical Tape Drives window, select the tape drives to be assigned and then click **Assign**.

7. __ In the Assign Physical Tape Drives notification window, click **OK**.

8. __ In the VE console, right-click the 3494 Tape Library and then click **Inventory**.

9. __ To view the available tape drives, click the 3494 Tape Library and then click the **Physical Drives** tab.

10. __ To view the available tape cartridges, click the 3494 Tape Library and then click the **Physical Tapes** tab.

Chapter 11. IBM System i configuration

IBM System i servers support several types of tape libraries, ranging from relatively simple solutions that can automatically load tape cartridges during operation and maintain a limited cartridge inventory to tape automation systems capable of supporting many systems and managing vast cartridge inventories.

The VirtualTape Library for IBM System i allows System i servers to connect to a TS7500 Virtualization Engine, which emulates the following:

Emulated tape libraries

- Machine type 3584 (TS3500 Tape Library)
- Machine type 3582
- Machine type 3583
- TS3100 Tape Library
- TS3200 Tape Library
- TS3310 Tape Library

Emulated tape drives

- Ultrium LTO 2 Tape Drive
- Ultrium LTO 3 Tape Drive
- Ultrium LTO 4 Tape Drive
- 3592 J1A Tape Drive
- TS1120 Tape Drive

Before you begin

Before you can use VirtualTape Library for IBM System i, your environment must meet the following criteria:

- The System i operating system must be V5R2 or V5R3.
- There must be a fibre channel connection between the System i server and the TS7500 Virtualization Engine.
- The AS/400® must use either the IBM 2765 PCI or IBM 5704 PCI-x fibre channel tape controller or equivalent.
- In the VE console, VirtualTape Library for IBM System i must be licensed.

Setting up the tape library

With VirtualTape Library for IBM System i, you use the procedures described earlier in this guide to create a virtual tape library and assign it to a System i host.

Note: When you create a virtual tape library for use with a System i host, you must select one of the supported virtual tape libraries.

For import/export, you must use one of the supported tape drives (IBM 3592 or TS1120, or Ultrium LTO 2, LTO 3, or LTO 4) in the physical tape library. This ensures that you have 1:1 data transfer between the virtual volume and the physical tape media.

163

After you have created a virtual tape library and assigned it to the host, perform the following tasks to ensure that the System i server can detect and function properly with the tape library.

1. __ At the System i server, display the library status functions by completing the following substeps:

   a. __ Open the server's command line interface.

   b. __ Type the following:

   ```
   WRKMLBSTS
   ```

   and press the **Enter** key.

2. __ Make resources available to the tape drive by typing 4 (ALLOCATE) in the option field next to each resource to be made available and then pressing the **Enter** key.

3. __ Inventory the tape library by typing 9 (INVENTORY) in the option field next to the tape library and then pressing the **Enter** key.

4. __ In the System i server's command line interface, add a tape to the inventory by typing the following command at the command line and then pressing the **Enter** key:

   ```
   ADDTAPCTG DEV xxx CTG yyy CGY(*NOSHARE) CHKVOL(*NO)
   ```

   where xxx is the library device name and yyy is the cartridge identifier. Alternatively, you can use *SHARE400 for the CGY parameter. After you issue this command, the tape status changes from INSERT to AVAILABLE.

5. __ In the System i server's command line interface, mount a tape on to a drive by typing the following command and then pressing the **Enter** key:

   ```
   CHKTAP DEV xxx VOL yyy
   ```

   where xxx is the device name and yyy is the volume identifier. After you issue this command, the tape status changes from AVAILABLE to MOUNTED.

6. __ In the System i server's command line interface, create a library object by typing the following command and then pressing the **Enter** key:

   ```
   CRTLIB LIB xxx
   ```

   where xxx is the library name.

7. __ In the System i server's command line interface, back up a library object by typing the following command and then pressing the **Enter** key:

   ```
   SAVLIB LIB xxx DEV yyy VOL zzz
   ```

   where xxx is the library name, yyy is the tape media library device name, and zzz is the volume identifier.

8. __ In the System i server's command line interface, restore a library object by typing the following command and then pressing the **Enter** key:

   ```
   RSTLIB SAVLIB xxx DEV yyy VOL zzz
   ```

where xxx is the original library name, yyy is the tape media library device name, and zzz is the volume identifier.

9. __ In the System i server's command line interface, display the library object content to confirm that the restoration was successful by typing the following command and then pressing the **Enter** key:

```
DSPLIB LIB xxx
```

where xxx is the library name.

10. __ In the System i server's command line interface, delete a library object by typing the following command and then pressing the **Enter** key:

```
DLTLIB LIB xxx
```

where xxx is the library name.

11. __ In the System i server's command line interface, demount a tape cartridge by typing the following command and then pressing the **Enter** key:

```
CHKTAP DEV xxx VOL yyy ENDOPT(*UNLOAD)
```

where xxx is the device name and yyy is the volume identifier. After you issue this command, the tape status changes from MOUNTED to AVAILABLE.

Importing tape cartridges

The process of adding tape cartridges to the tape library inventory is called *importing*. Most tape libraries provide an I/O station for importing cartridges without interrupting automated operations. To import tape cartridges into the tape library, complete the following steps:

1. __ In the VE console, move the tape cartridge from the virtual vault to the virtual tape library by performing the following substeps:.
   a. __ Expand **Virtual Tape Library System**.
   b. __ Click the **Virtual Vault** icon.
   c. __ In the list of virtual tape cartridges, right-click the tape cartridge to be moved and then click **Move to Virtual Library**.
   d. __ From the destination library list, select the destination virtual tape library.
   e. __ Select the check box for the virtual tape cartridge to be moved.
   f. __ Click **OK**.
2. __ At the AS/400, re-inventory the library as described in 3 on page 164.
3. __ Add the tape into inventory as described in 4 on page 164.

Exporting tape cartridges (moving cartridges to the virtual vault)

Exported tape cartridges are cartridges that have been removed from the tape library inventory.

To export a cartridge, type the following command at the command line:

RMVTAPCTG DEV (library device name) CTG (cartridge identifier)

After you issue this command, if you re-inventory the library from the AS/400, the tape is no longer there. From the VE console, you can see the tape in the virtual vault.

Chapter 12. TS3500 Tape Library (IBM machine type 3584) configuration

This section contains information about TS3500 Tape Library (IBM machine type 3584) configuration.

Adding tape cartridges to a TS3500 Tape Library

After adding physical tape cartridges to a TS3500 Tape Library, define the new cartridges logically by completing the following steps:

1. __ In the VE console, inventory the physical tape library by completing the following substeps:

   a. __ Expand the server icon.

   b. __ Expand **Virtual Tape Library System** → **Physical Tape Libraries**.

   c. __ Right-click the physical tape library icon and then click **Inventory**.
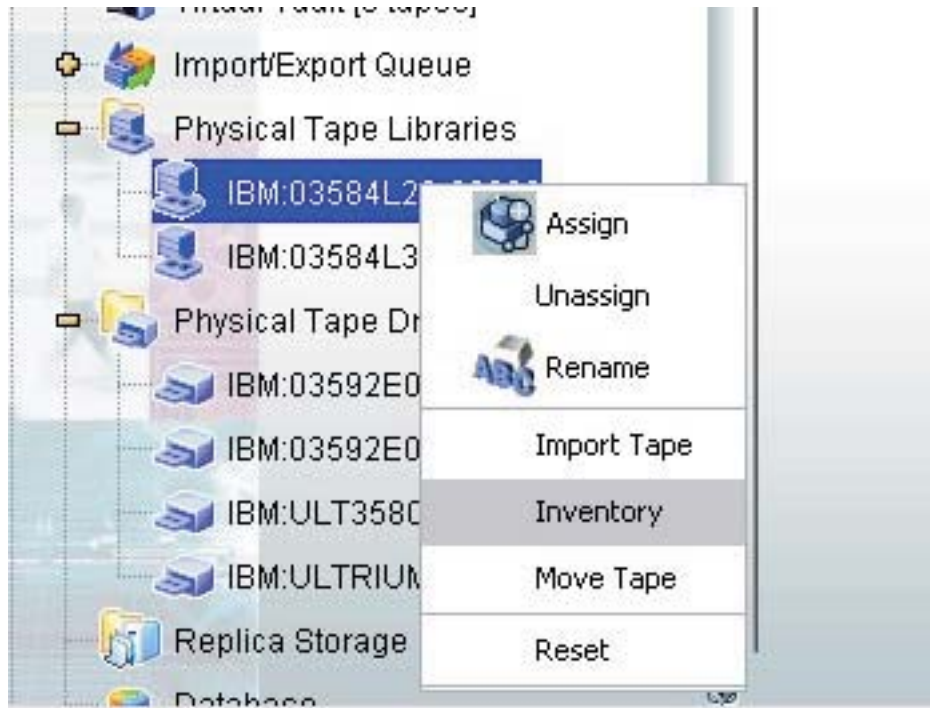
Figure 114. Inventorying a physical tape library

2. __ To display the added tape cartridge, click the physical tape library icon and then click the **Physical Tapes** tab.
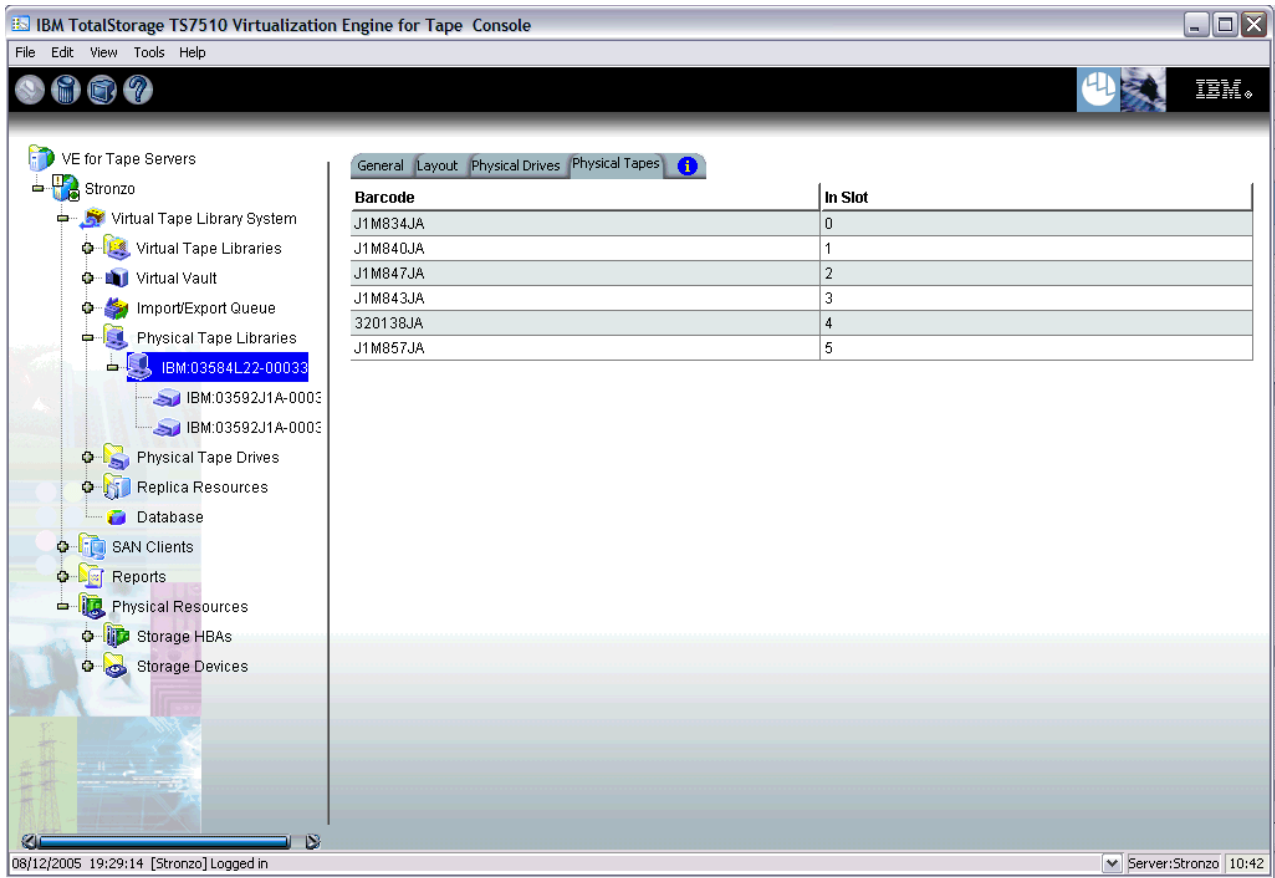
Figure 115. Displaying the added tape cartridge

Chapter 13. Hosted Backup

The Hosted Backup feature makes virtual tape libraries and tape drives available to the local system, allowing certified backup applications to be installed directly onto the TS7500 Virtualization Engine and eliminating the need for a dedicated backup server and separate media servers. Because the backup application is hosted by the TS7500 Virtualization Engine, it can enhance performance by directly accessing the virtual tape libraries without relying on external fibre channel or IP connections.

Note: Hosted Backup is a prerequisite for NDMP support.

Configuring Hosted Backup

To configure Hosted Backup, complete the following steps:

1. __ Install Tivoli Storage Manager on the TS7520 Server using the procedure in the appendix if it is not already installed.

2. __ In the VE console, right-click the server icon and then click **Options** → **Enable Hosted Backup**. A new client named **HostedBackupClient** appears in the **SAN Clients** list.
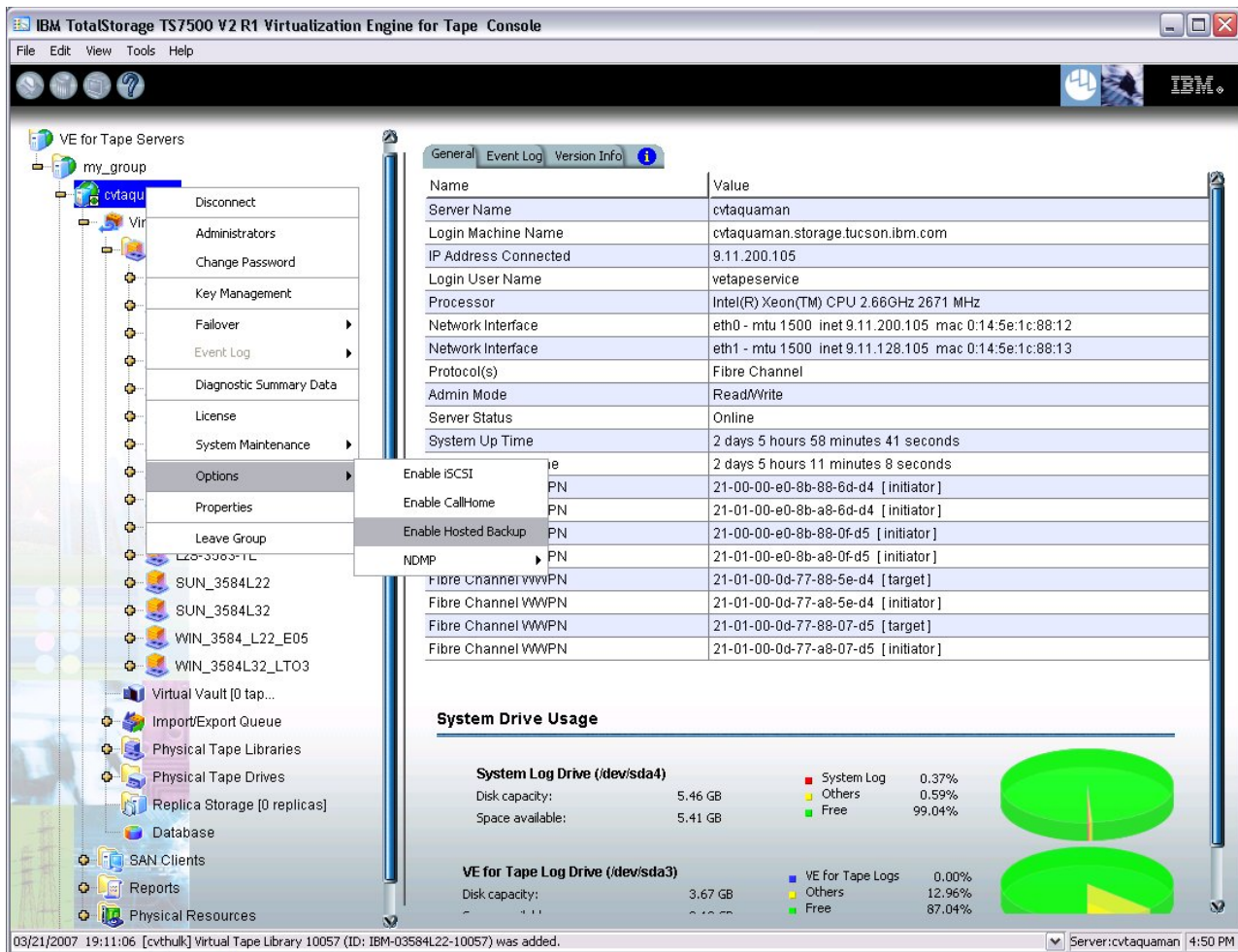
Figure 116. Enabling Hosted Backup

3. __ Right-click **HostedBackupClient** and then click **Assign**.
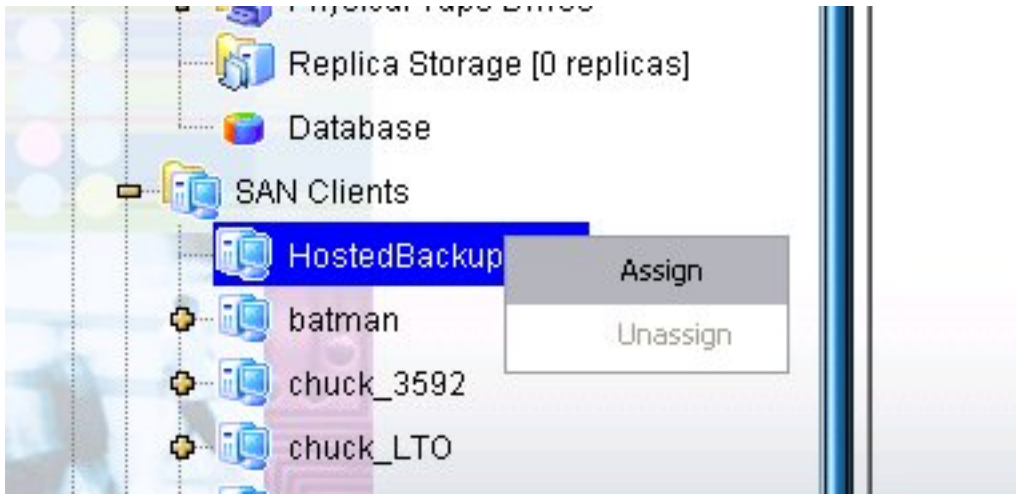
Figure 117. Assigning virtual tape libraries to the HostedBackupClient

4. __ Assign virtual tape libraries or virtual tape drives to **HostedBackupClient**.
5. __ Click **Next**.
6. __ Verify all information and then click **Finish**. The backup application will now see the devices as local devices. If you type: `/sys/devices/platform/host32` on your TS7500 Virtualization Engine, you will see the library and all of the drives in the library listed as local devices (they will have SCSI addresses beginning with 32).
7. __ Verify that the applicable rpm packages are installed on the TS7500 Virtualization Engine and install them if they are not installed. Refer to the backup application's documentation to determine whether any additional packages are required.

   Note: Contact your IBM marketing representative for a certified application list.
8. __ Install and configure the backup application on the TS7500 Virtualization Engine.
9. __ If the TS7500 Virtualization Engine's operating system detects the hosted backup devices but the backup application does not, rescan for them in the backup application or restart the backup application.

Chapter 14. NDMP

The Network Data Management Protocol (NDMP) option allows certified backup applications and industry-standard network-attached storage (NAS) devices, such as NetApp filers, to perform backup and restoration operations using NDMP over an IP network. The NDMP option is only available for TS7500 EE installations.

With NDMP enabled, the TS7500 Virtualization Engine acts as an NDMP server, centralizing management by eliminating locally-attached tape devices from each NAS device. When a backup operation occurs, data moves from the NAS device directly to the virtual library.

The NDMP option can be disabled when presenting a virtual tape library over fibre channel to a NAS filer as a replacement for a physical library.

Configuring NDMP

To configure NDMP, complete the following steps:

1. __ If it is not already enabled, enable Hosted Backup by right-clicking the server icon in the VE console and then clicking **Options** → **Enable Hosted Backup**. A new client called *HostedBackupClient* appears in the **SAN Clients** list.

2. __ In the VE console, right-click the server icon and then click **Options** → **NDMP** → **Enable**.
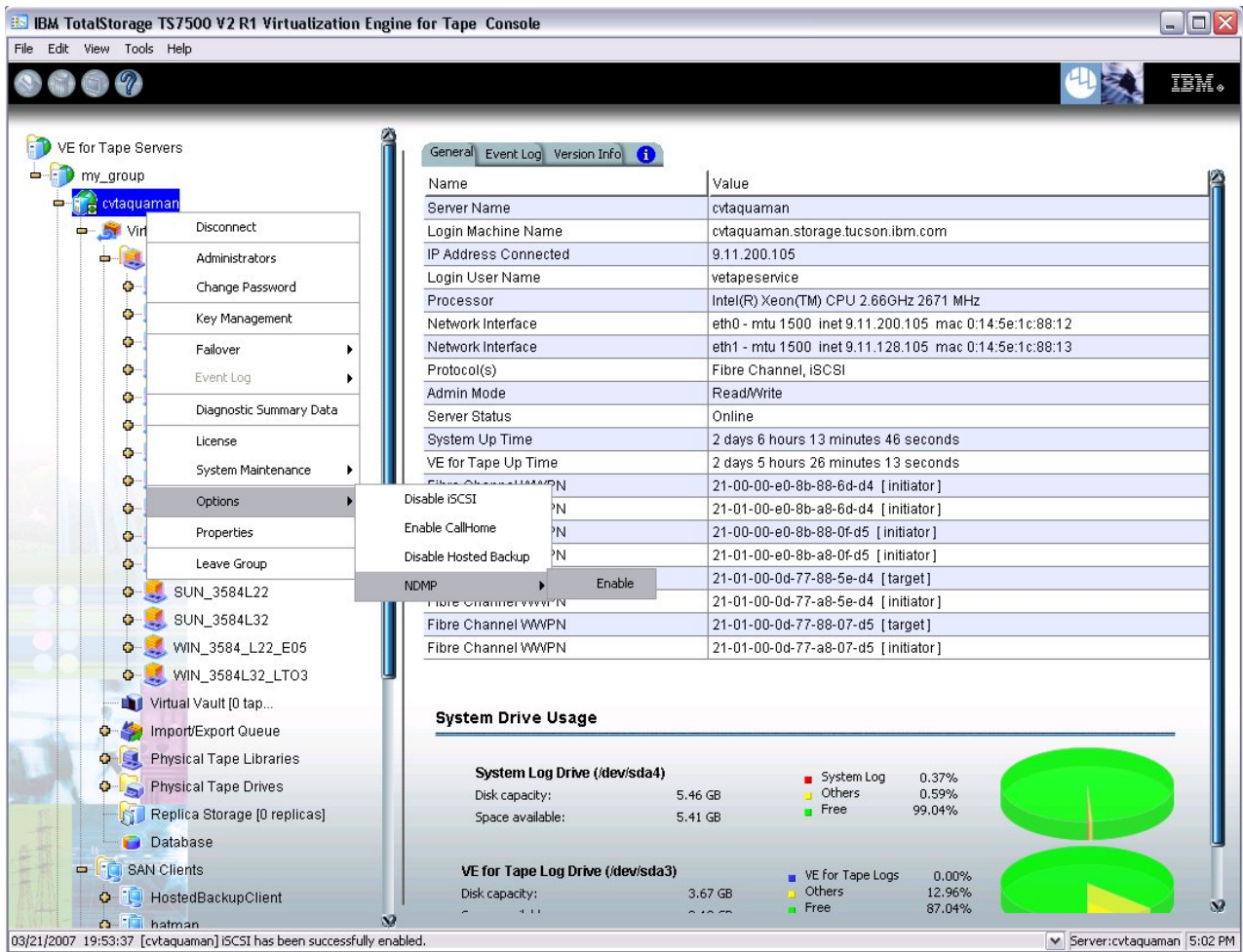
Figure 118. Enabling NDMP

3. __ In the ″Enter NDMP user info″ window:

   a. __ In the **UserName** field, type the name for the NDMP account.

   b. __ In the **Password** field, type the account's password.

   c. __ In the **Confirm Password** field, type the account's password again.

   d. __ Click **OK**.
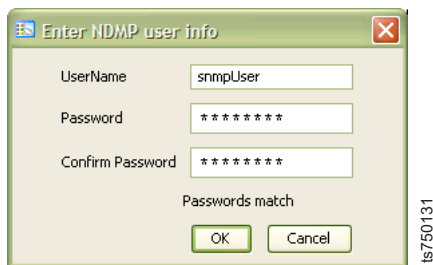
Figure 119. Entering username and password for NDMP

4. __ In the VE console, expand the **SAN Clients** list.

5. __ Right-click the *HostedBackupClient* icon and then click **Assign**.

6. __ In the Select Tape Libraries or Drives window:

a. __ (Optional) Select the **Allow tape drive(s) in the tape library to be assigned individually** check box. This will list tape drives separately from their tape libraries in the selection list.

b. __ In the selection list, select the tape libraries or tape drives to be assigned to *HostedBackupClient*.

c. __ Click **Next**.

7. __ In the Assign Tape Libraries or Drives to the SAN Client window, verify the information for the assignment and then click **Finish**.

The backup application will now see the devices as local devices.

In the TS7500 Virtualization Engine command line interface, type `/sys/devices/platform/host32` and then press the **Enter** key. The interface lists the assigned tape library and drives listed as local devices with SCSI addresses beginning with *32*.

Chapter 15. CallHome

In the TS7500 Virtualization Engine, CallHome is a unique customer support utility that proactively identifies and diagnoses potential system or component failures and automatically notifies system administrators via email. It is **not** the IBM function that allows the transmission of operational and error-related data to IBM.

Using pre-configured scripts called *triggers*, CallHome monitors a set of pre-defined critical system components. These include SCSI drive errors, offline device, etc. With its open architecture, administrators can easily register new elements for triggers to monitor.

When an error occurs, CallHome captures the appropriate information and creates a snapshot of the TS7500 Virtualization Engine 's current configuration and environment. CallHome then creates an entry in the TS7500 Virtualization Engine event log.

With CallHome enabled, system administrators have the ability to take corrective measures more quickly, minimizing system downtime and increasing efficiency.

To enable and configure CallHome, complete the following steps:

1. __ In the VE console, right-click the server icon and then click **Options** → **Enable CallHome**.

2. __ In the Set CallHome General Properties window (Figure 120):
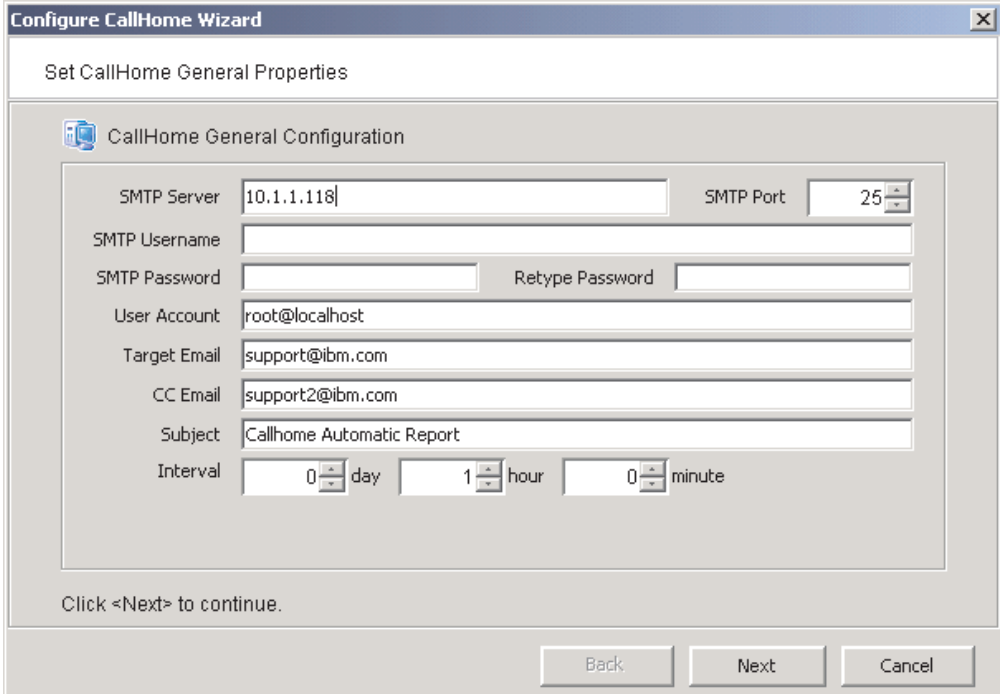
Figure 120. Set CallHome General Properties window

   a. __ In the **SMTP Server** field, type either the IP address or the full name of the mail server for CallHome to use to send email notifications.

   b. __ In the **SMTP Port** field, type or click the arrows to select the number of the port for CallHome to use.

175

c. __ In the **SMTP Username** field, type the name of the account for CallHome to use to log in to the mail server.

d. __ In the **SMTP Password** field, type the password for the CallHome account.

e. __ In the **Retype Password** field, type the password for the CallHome account again.

f. __ In the **User Account** field, type the email address or addresses to be displayed in the **From** field of emails that CallHome sends. Separate multiple email addresses by semicolons (;).

g. __ In the **Target Email** field, type the email address or addresses that will receive emails from CallHome; these email addresses display in the **To** field. Separate multiple email addresses by semicolons (;).

h. __ (Optional) In the **CC Email** field, type the email address or addresses that should receive copies of the emails sent by CallHome. Separate multiple email addresses by semicolons (;).

i. __ In the **Subject** field, type the text to appear in the subject line of emails that CallHome sends.

j. __ In the **Interval** fields, type or click the arrows to select the number of days, hours, and minutes of the time period between activations of CallHome.

k. __ Click **Next**.

3. __ In the Set CallHome Signature Properties window (Figure 121):
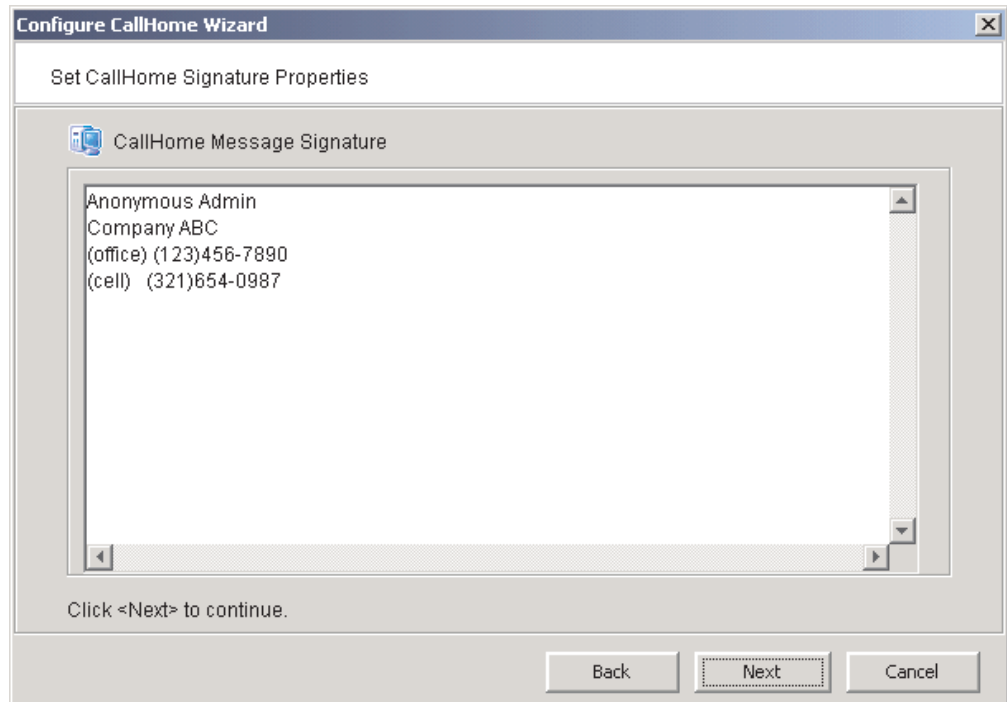
Figure 121. Set CallHome Signature Properties window

a. __ Modify the contact information to be appended to the bottom of each email CallHome sends.

b. __ Click **Next**.

4. __ In the Set CallHome Trigger Properties window (Figure 120 on page 175):
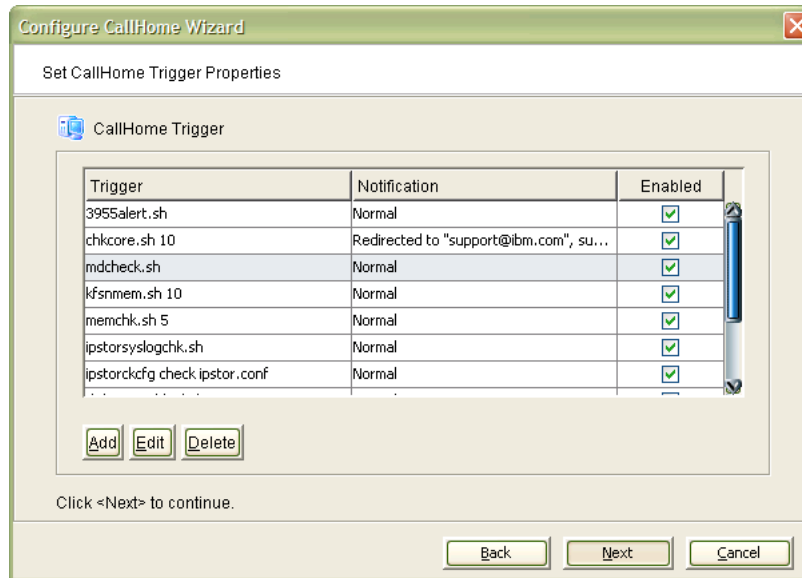
Figure 122. Set CallHome Trigger Properties window

a. __ In the **Enabled** column, select the check boxes for each trigger that you want to activate CallHome. Standard triggers include:

3955alert.sh
This trigger detects critical hardware and configuration failures in the cache components, causing CallHome to send an email alert.

chkcore.sh 10
This trigger detects new core files created by the operating system in the **bin** directory of the TS7500 Virtualization Engine. If the trigger detects a new core file, CallHome compresses it, deletes the original, and sends an email alert. However, it does not send the compressed core file. If there are more than ten compressed core files, CallHome deletes them all.

mdcheck.sh
This trigger detects failure of the Linux RAID 1 array. If it fails, CallHome sends an email alert.

kfsnmem.sh 10
This trigger detects whether the value for the maximum number of memory pages has been set. If it hasn't, CallHome sends an email alert. If it has, the trigger determines the percentage of available memory pages. If the percentage is lower than the specified percentage, which has a default value of 10%, CallHome sends an email alert.

memchk.sh 5
This trigger takes a percentage as its parameter and determines whether the available system memory is below the percentage. If it is, CallHome sends an email alert.

ipstorsyslogchk.sh
This trigger monitors the system log for specific entries that need reporting. You select the entries that need reporting in the CallHome System Log Check and CallHome System Log Ignore windows later in the Configure CallHome wizard. If the trigger detects entries that need reporting, CallHome sends an email alert.

ipstorckcfg check ipstor.conf

This trigger compares the current version of `ipstor.conf`, the XML configuration file for the TS7500 Virtualization Engine, to the version extant when the script last ran. If there is no previous version of the file, the trigger creates a copy of the current version. When the trigger runs, it compares the two versions. If the trigger detects any changes, it records them in a file named `ipstorconf.diff` and sends an email alert. If the trigger detects further changes when it next runs, it saves the current contents of `ipstorconf.diff` to new file `ipstorconf.diff.001` and records the new changes in `ipstorconf.diff`. This process repeats each time `ipstorconf.diff` changes, with the number appended to the name of each file incrementing each time.

diskusagechk.sh / 95

This trigger monitors the disk space usage of the root file system. If the percentage is higher than the specified percentage, which has a default value of 95%, CallHome sends an email alert. You can add more diskusagechk.sh triggers for different mount points; for example, `/home`.

defaultipchk.sh eth0 10.1.1.1

This trigger determines whether the IP address for the specified Ethernet card matches the value specified in the trigger. If it does not, CallHome sends an email alert. You can add more defaultipchk.sh triggers and specify different IP addresses for different Ethernet cards; for example, defaultipchk.sh eth1.

xfilechk.sh

This trigger detects changes to the executable files. If it detects changes, CallHome sends an email alert.

ipstorstatus.sh

This trigger calls the **ve status** function. If any module listed in the **ve status** function has stopped, CallHome sends an email alert.

b. __ Click **Next**.

5. __ In the Set CallHome Diagnostic Summary Data Properties window (Figure 123 on page 179):
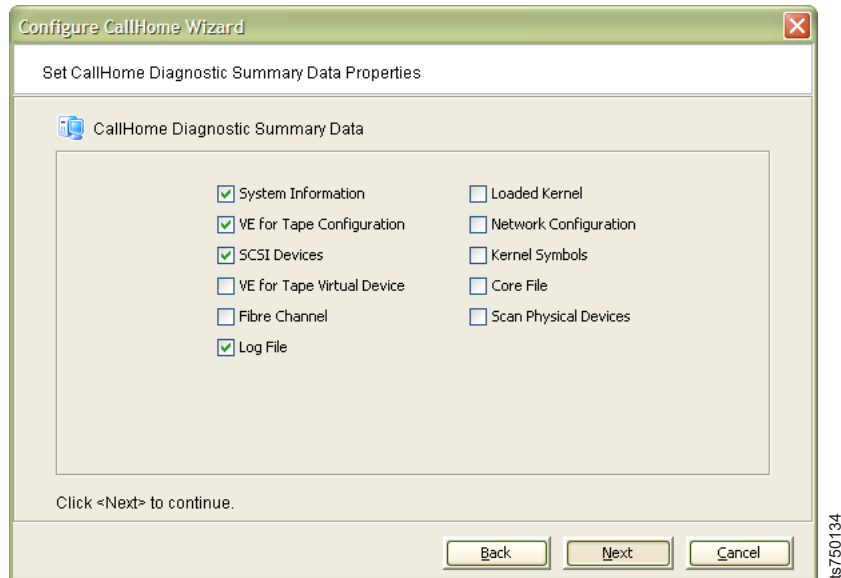
Figure 123. Set CallHome Diagnostic Summary Data Properties window

a. __ Select the items to be included in the diagnostic summary file.

> **Note:** See the VE console Online Help for more information about each option and about the diagnostic summary file.

b. __ Click **Next**.

6. __ In the Set CallHome System Log Check Properties window (Figure 124):
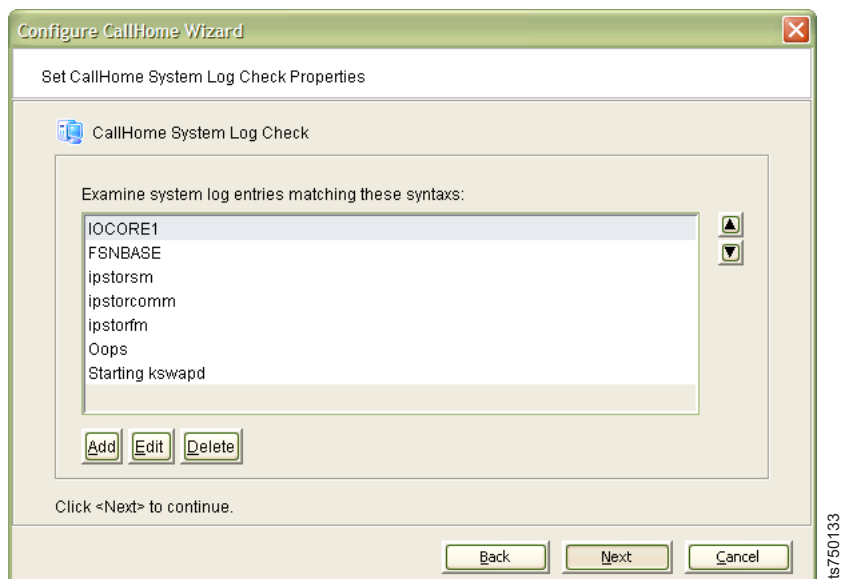
Figure 124. Set CallHome System Log Check Properties window

a. __ Specify the terms in the system log for the ipstorsyslogchk.sh trigger to track. The system log records important events and errors occurring in the system, including the TS7500 Virtualization Engine. This window allows you to select general criteria relevant to the TS7500 Virtualization Engine for CallHome reporting. CallHome monitors system log entries that match the

criteria here you select here. Each line is a regular expression. The regular expression rules follow the pattern for AWK, a standard Unix utility.

The criteria selected here, along with those selected in the next window (the Set CallHome System Log Ignore Properties window), act as a filter for the trigger. The trigger ignores terms selected in the Set CallHome System Log Ignore Properties window. This eliminates entries that match the criteria you select in the Set CallHome System Log Check Properties window above but that the trigger can still disregard. The remaining entries form a subset for which CallHome sends email alerts.

    b. __ Click **Next**.

7. __ In the Set CallHome System Log Ignore Properties window (Figure 125):
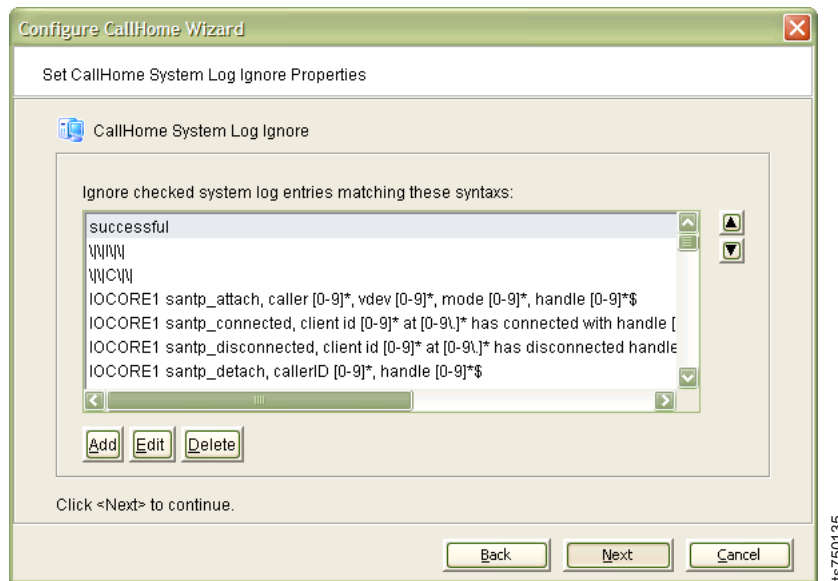
Figure 125. Set CallHome System Log Ignore Properties window

    a. __ Specify the terms in the system log for the ipstorsyslogchk.sh trigger not to track. As for the previous window, each line is a regular expression following the pattern for the standard Unix utility AWK.

    b. __ Click **Next**.

8. __ In the Enabling CallHome for VE for Tape Server <server name> window, verify the information you selected in the previous wizard pages is correct and then click **Finish**.

Modifying CallHome properties

Once you enable CallHome, you can modify the information by right-clicking the server icon in the VE console and then clicking **CallHome**. See Figure 126 on page 181.
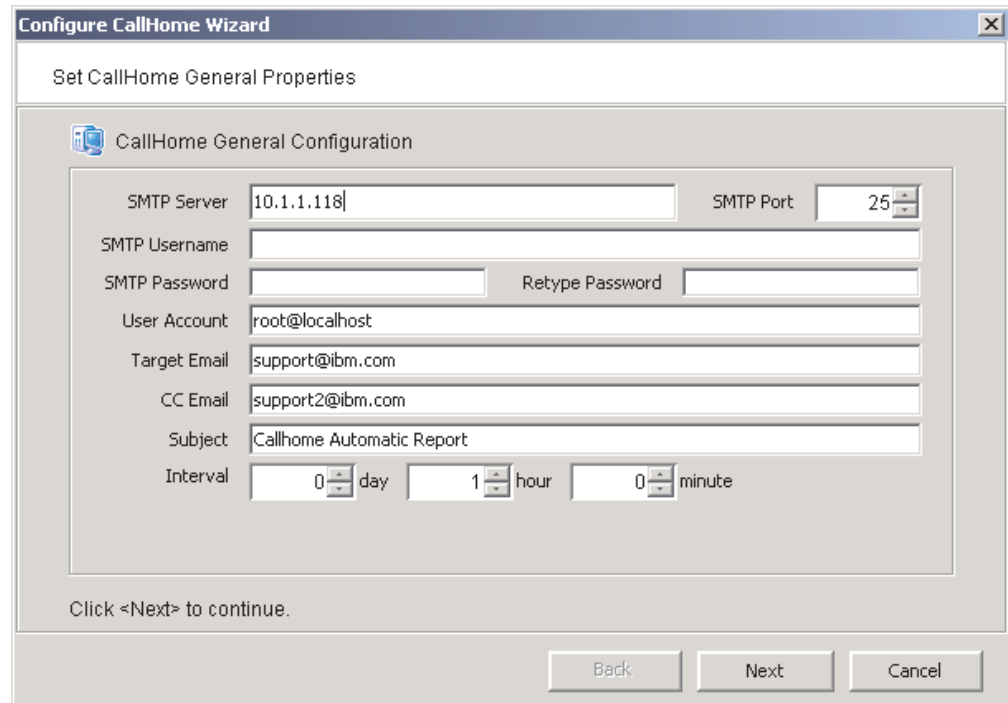
Figure 126. Modifying Callhome properties

Click the appropriate tab to update the desired information.

Custom email destination

To specify an email address to replace the default target email address or a subject line to replace the default subject line, complete the following steps:

1. __ In the VE console, right-click the server icon and then click **CallHome**.
2. __ Click the **Trigger** tab.
3. __ Perform one of the following:
   - To add a new trigger, click **Add**.
   - To edit an existing trigger, select the trigger and then click **Edit**.

Note: An email address specified in this procedure overrides the return code; CallHome does not send an attachment with the email alert, regardless of the return code.

Adding a trigger

Attention: IBM recommends that you use only the provided standard triggers.

The trigger can be a shell script or a program (Java™, C, and so on). If you create a new trigger, you must add it in the VE console so that CallHome can detect it. To add a new trigger, complete the following steps:

1. __ In the VE console, right-click the server icon and then click **CallHome**.
2. __ Click the **Trigger** tab.
3. __ Click **Add**.

Return codes

Attention: IBM recommends that you use only the provided standard triggers.

Return codes determine the result of a trigger's execution. The following are valid return codes:

0   No action is required; CallHome does not send an email alert.

1   CallHome attaches all files in the $ISHOME/etc and the $ISHOME/log directories and sends the email alert.

2   CallHome sends the email alert without attachments.

The $ISHOME/etc directory contains a TS7500 Virtualization Engine configuration file that contains information about virtual devices, physical devices, HBAs, NAS, database agents, and so on). The $ISHOME/log directory contains CallHome logs, which contain events and trigger outputs.

Sample script

Attention: IBM recommends that you use only the provided standard triggers.

Below is the content of the TS7500 Virtualization Engine status check trigger, vestatus.sh:

```
#!/bin/sh
RET=0
if [ -f /etc/.is.sh ]
then
. /etc/.is.sh
else
echo Installation is not complete. Environment profile is missing in /etc.
echo
exit 0 # don't want to report error here so have to exit with error code 0

fi
$ISHOME/bin/ve status | grep STOPPED >> $IPSTORCLHMLOG
if [ $? -eq 0 ] ; then
RET=1
fi
exit $RET
```

In order for a trigger to send useful information in the email body, it must redirect its output to the environment variable $IPSTORCLHMLOG, as shown in the example above.

If any TS7500 Virtualization Engine module has stopped, this trigger generates a return code of 1 and attaches all files in the $ISHOME/etc and $ISHOME/log directories to the email alert it sends.

Chapter 16. Multi-node server groups

TS7500 EE installations with two or four TS7520 Servers have a shared storage architecture; all servers have access to the same cache components. This allows you to group multiple servers together for global tape cartridge access. Any member of a group can access any tape cartridge from any other server in the group.

Each group can contain from one to four nodes. A group can also contain Failover pairs, but Failover must be enabled and configured before adding the pair to a group.

You can manage all servers in a group together. Group management allows, for example, managing administrator accounts for all group servers or logging in to all servers in the group at the same time.

Creating a server group

To create a server group, complete the following steps:

1. __ In the VE console, right-click **VE for Tape Servers** and then click **Create Group**.
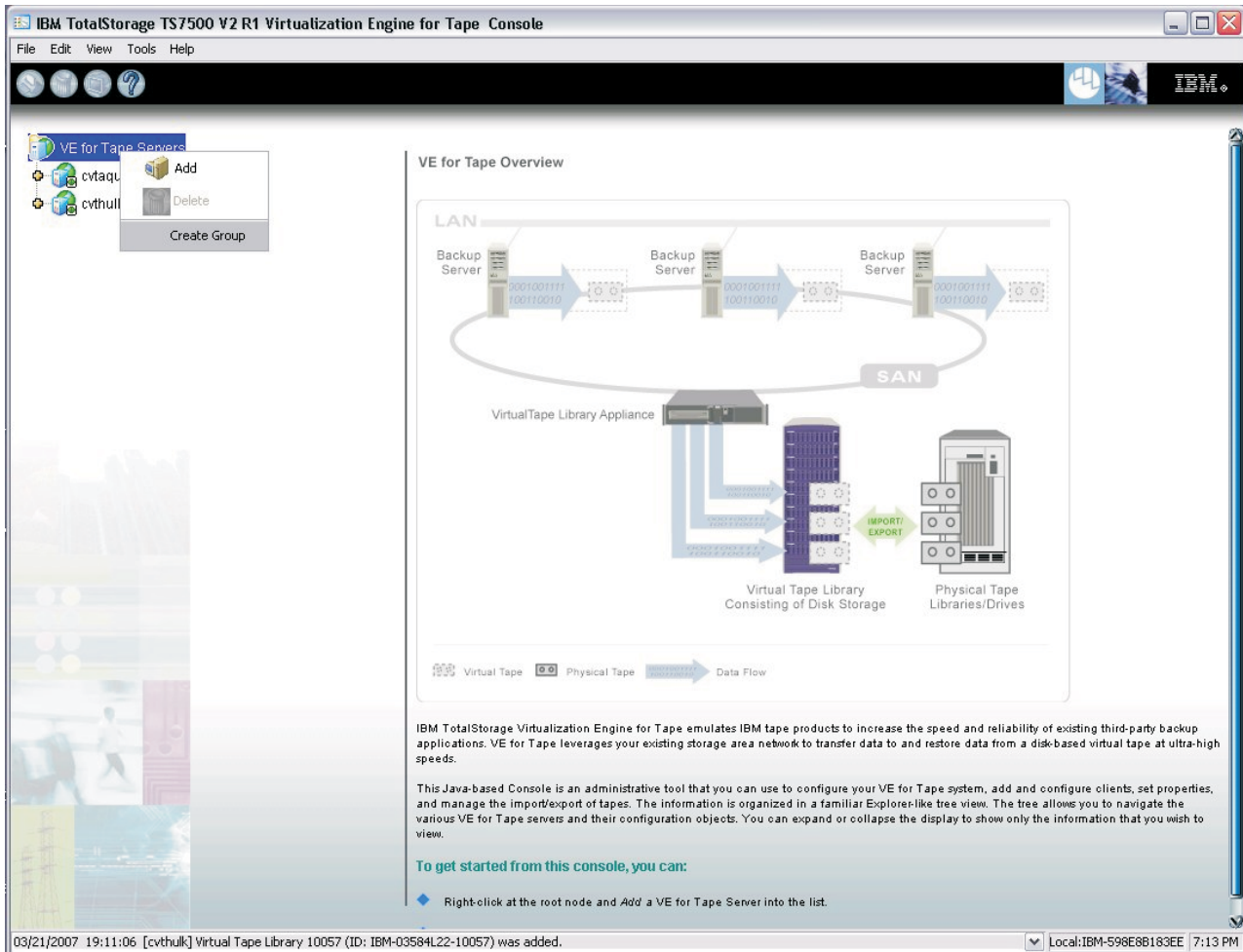
Figure 127. Creating a server group

2. __ In the Input Group Name window, type a name for the group. Valid characters include letters, numerals, the dash character (-), and the underscore character (_).

Figure 128. Input Group Name window

3. __ In the Input Group Name window, click **OK**. An icon for the group appears in the VE console navigation pane.

Adding servers to a server group

Note:

- If you want to add Failover servers to a server group, you must first enable and configure Failover for the servers.
- You need not connect to a server before adding it to a server group.

To add a server to the server group, perform one of the following:

If you are connected to a server:

1. __ In the VE console, right-click a server icon and then click **Join Group**.
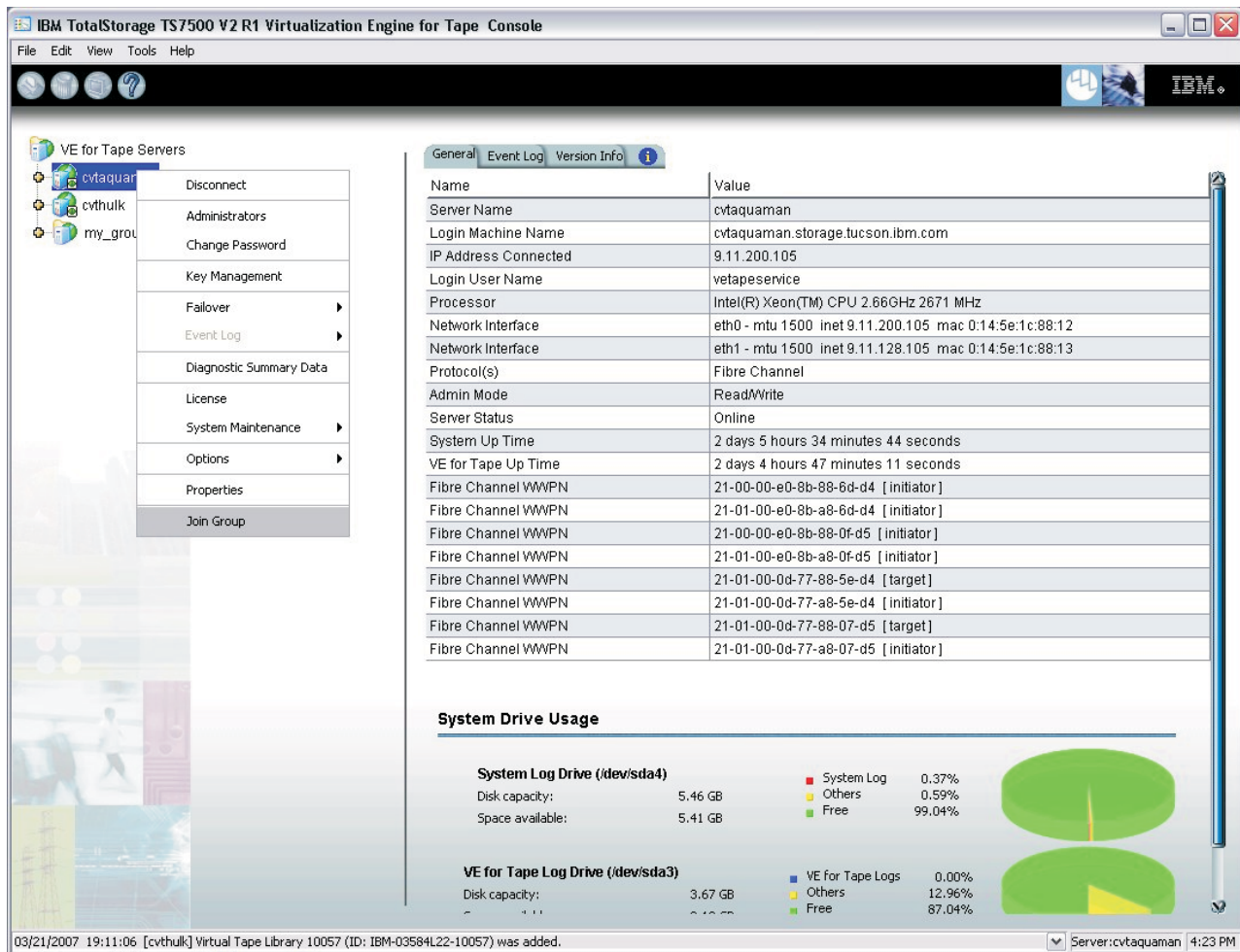
Figure 129. Joining a server group

2. __ In the Input Group Name window, type the name of the server group in the **Group Name** field and then click **OK**.

If you are not connected to a server:

1. __ In the VE console, right-click on a server group icon and then click **Add Member**.
2. __ In the Add Group Member window:
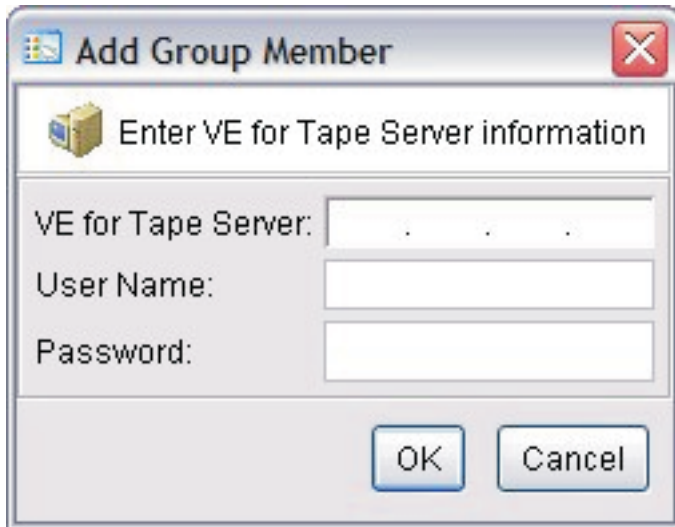
Figure 130. Add Group Member window

     a. __ In the **VE for Tape Server** field, type the IP address of the server to be added.

     b. __ In the **User Name** field, type a valid user name for the server.

     c. __ In the **Password** field, type the password for the user account.

     d. __ Click **OK**.

All added servers will appear in a list under the server group icon in the VE console navigation pane.

Removing a server from a server group

To remove a server from a server group, complete the following steps:

1. __ In the VE console, right-click the server icon and then click **Leave Group**.

2. __ Click **Yes**.

Accessing a tape cartridge from another server in a server group

You can access any tape cartridge from any other server in the same server group. To do so, complete the following steps:

1. __ In the VE console, right-click a virtual tape cartridge and then click **Move to Vault**. See Figure 131 on page 187.
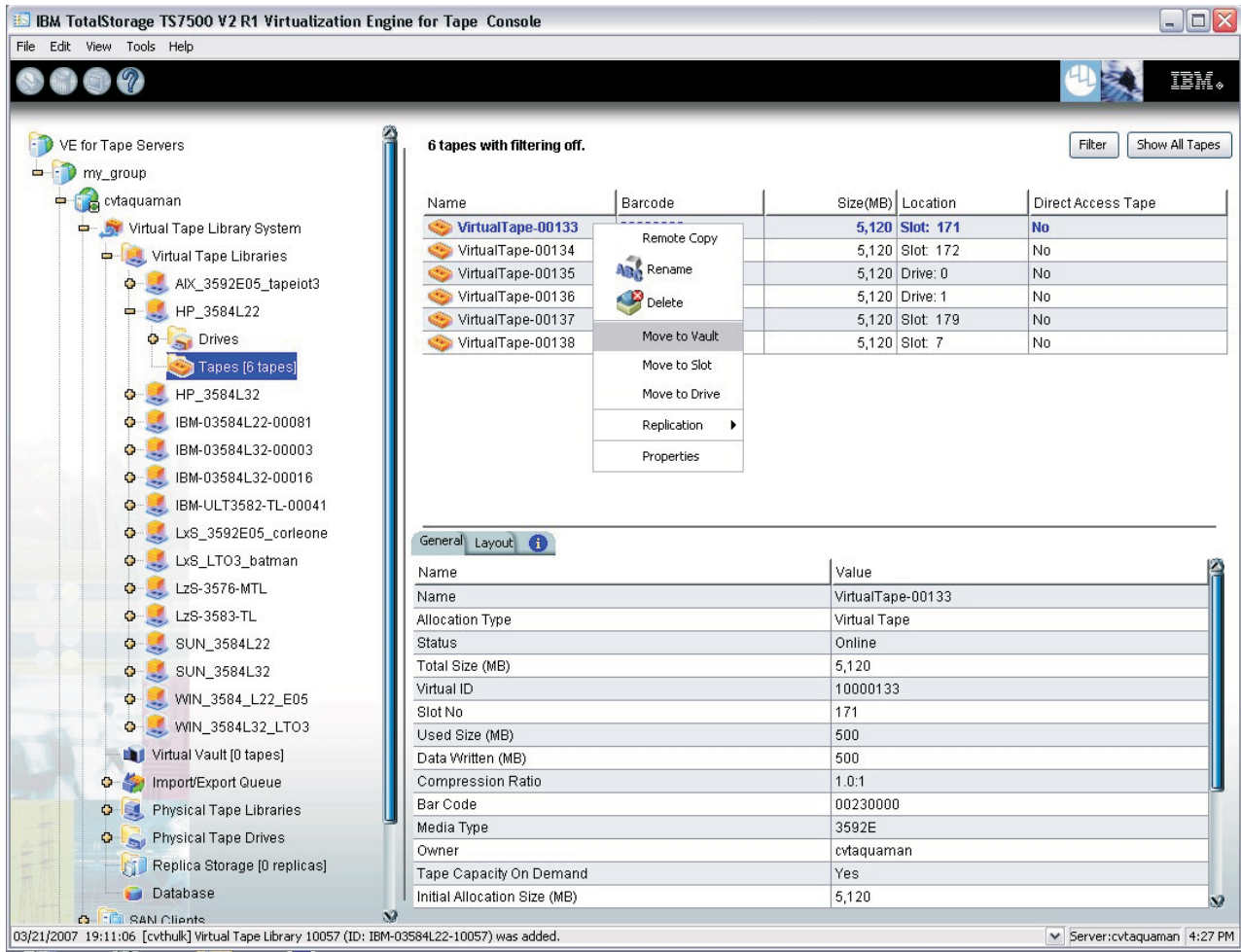
Figure 131. Moving the tape cartridge to the virtual vault

2. __ In the Move tape to Virtual Vault window, select the virtual volume to be moved and then click **OK**.
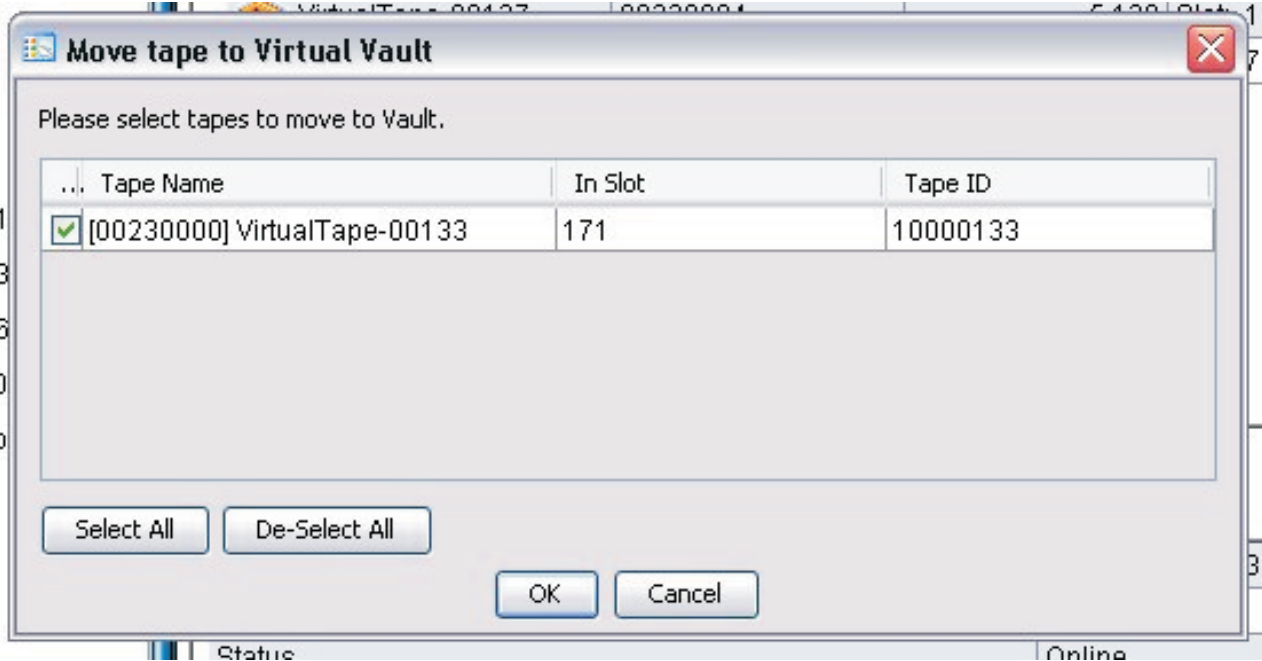
Figure 132. Selecting virtual volume to be moved

3. __ In the virtual vault, right-click the tape cartridge and then click **Move to Remote Server**.
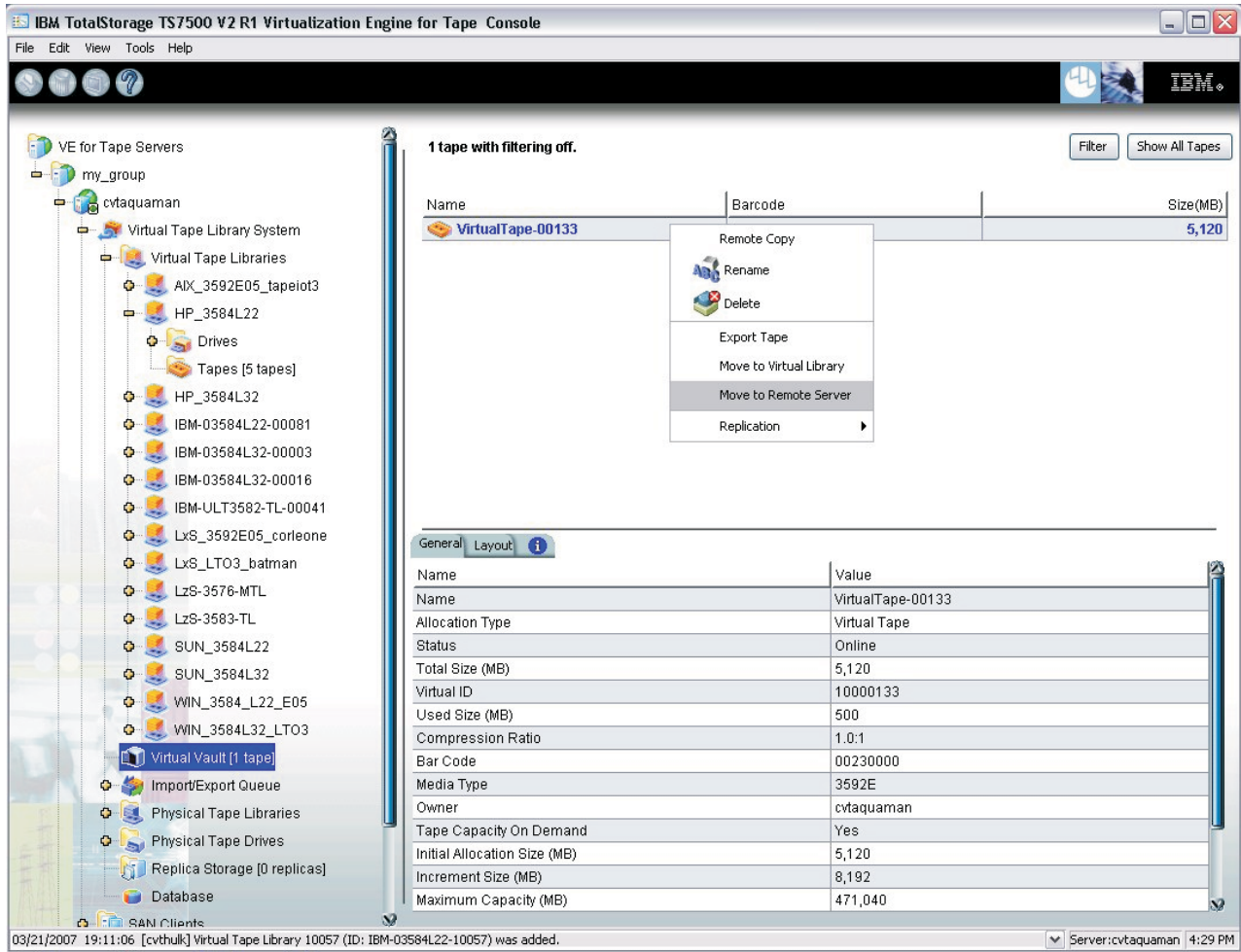
Figure 133. Moving the tape cartridge to a remote server in the same server group

4. __ In the Select the Virtual Tapes to Move window, select the virtual volume in the virtual vault to be moved to the other server and then click **Next**.
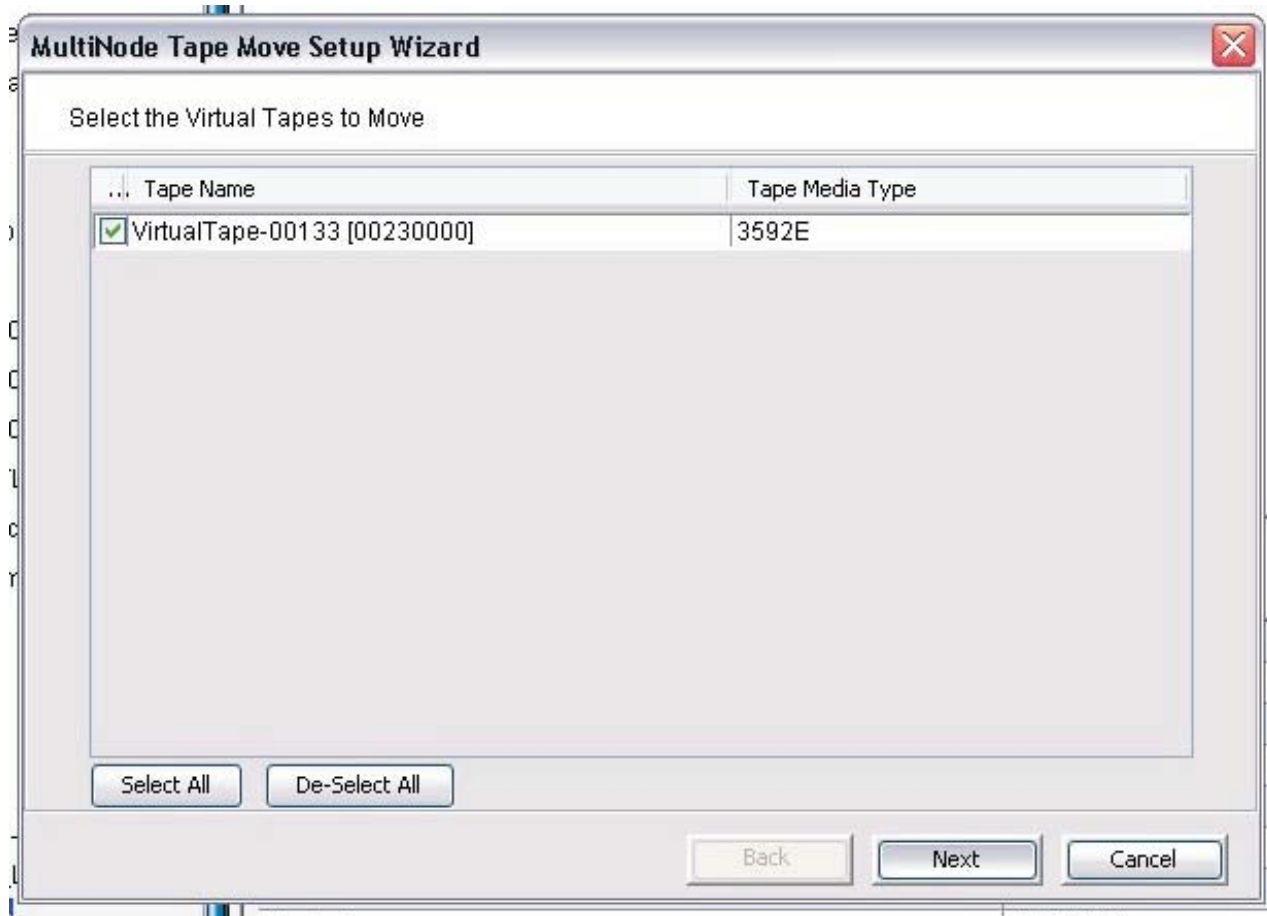
Figure 134. Selecting the virtual tape cartridges to be moved

5. __ In the Select the Target Server window, select the server in the server group to which you want to move the virtual tape cartridge and then click **Next**.
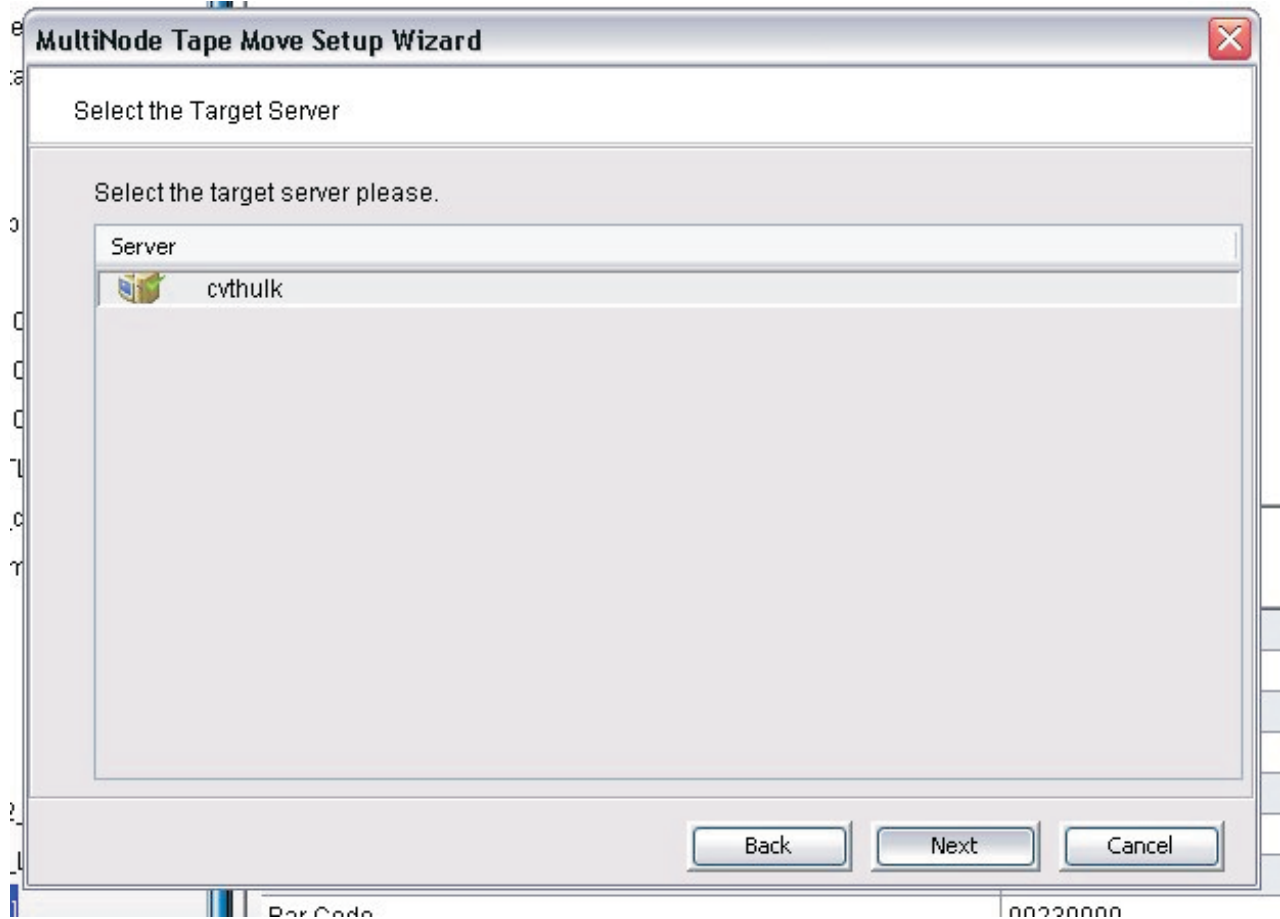
Figure 135. Selecting the target server

6. __ In the "MultiNode tape move" window, confirm the hostname or IP address of the server receives new virtual volume and then click **Next**.
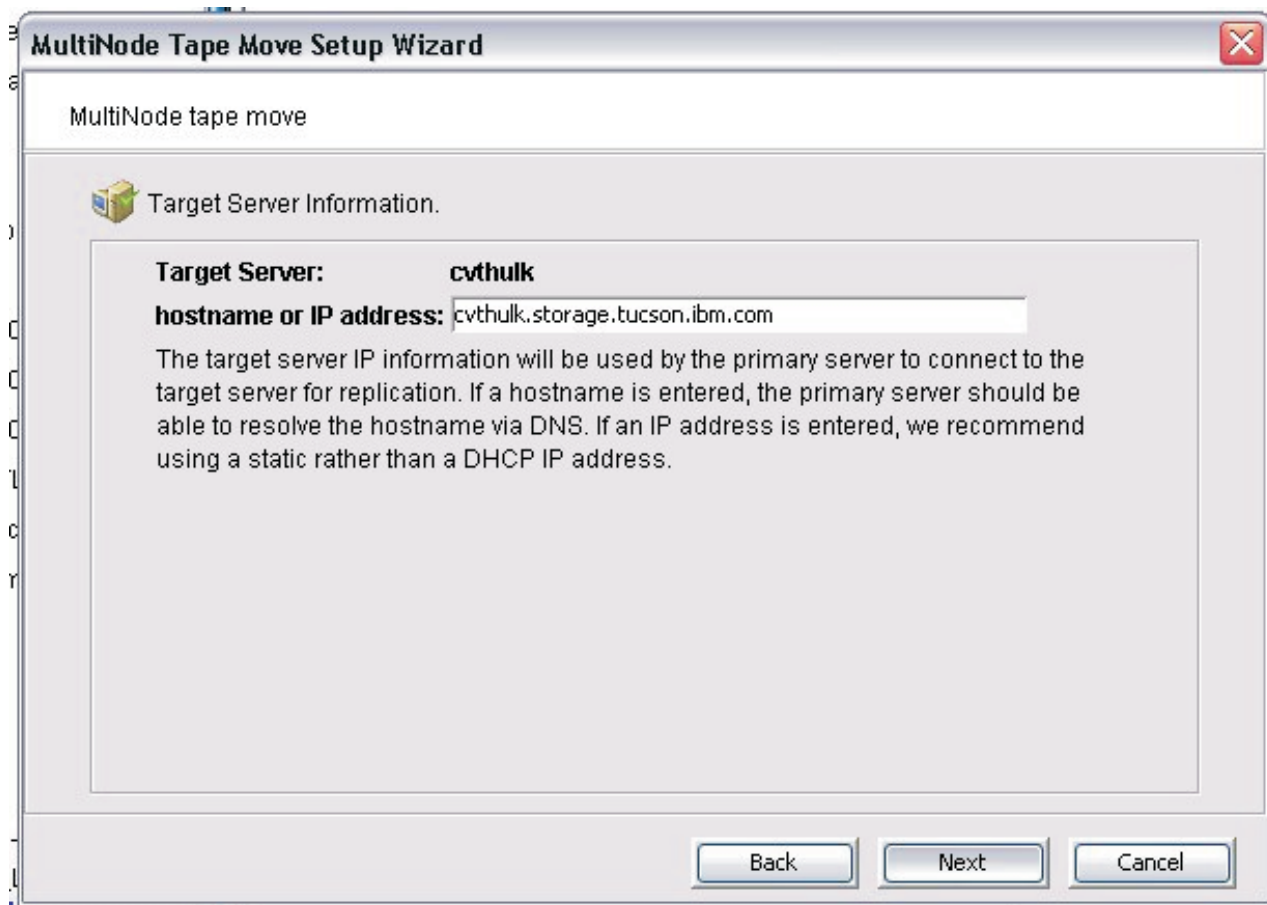
Figure 136. Confirming the hostname or IP address of the target server

7. __ In the Specify a Location window, select the target virtual tape library within the target server and then click **Next**.
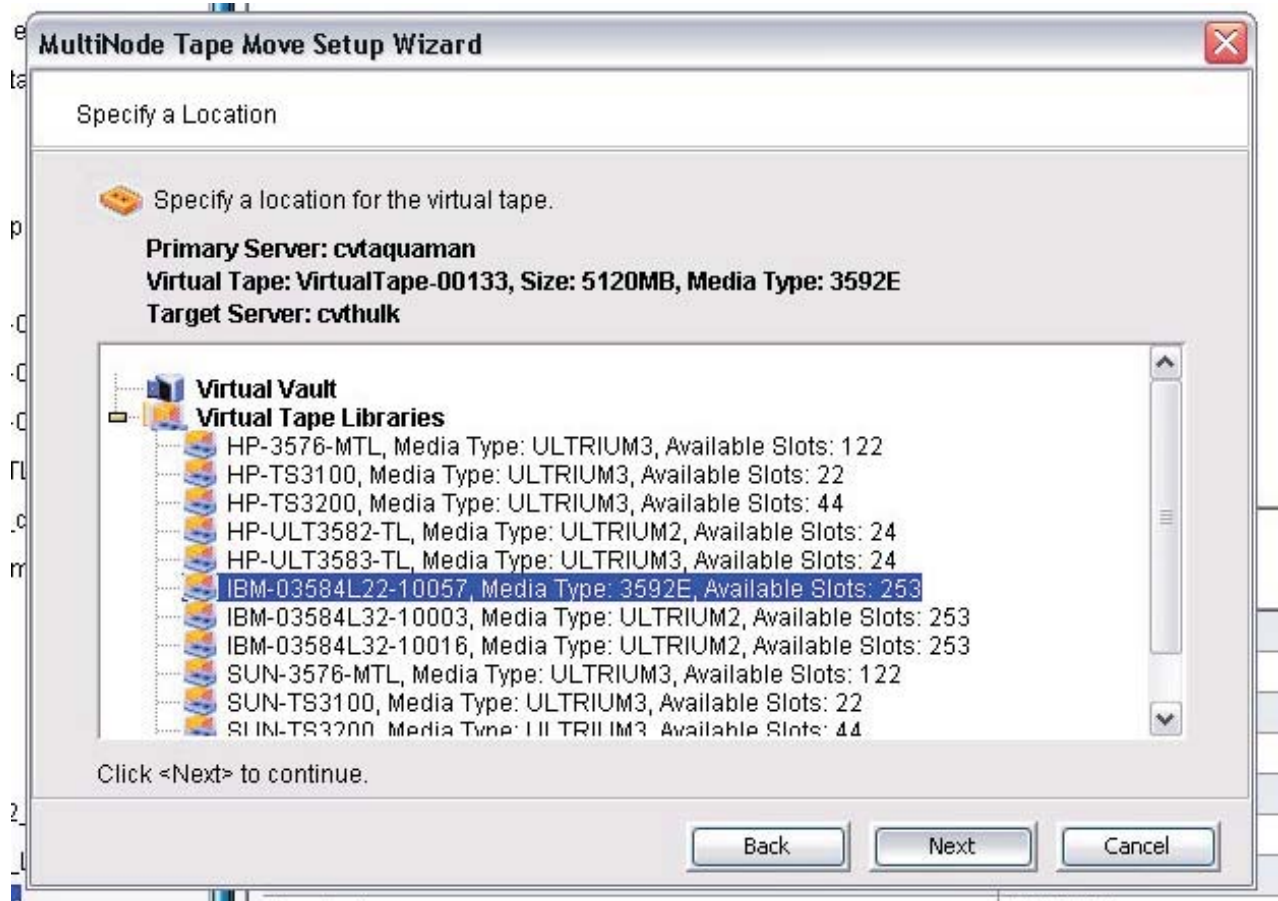
Figure 137. Specifying a target virtual tape library

8. __ In the Setup Tape Move window, verify the move information is correct and then click **Finish**.
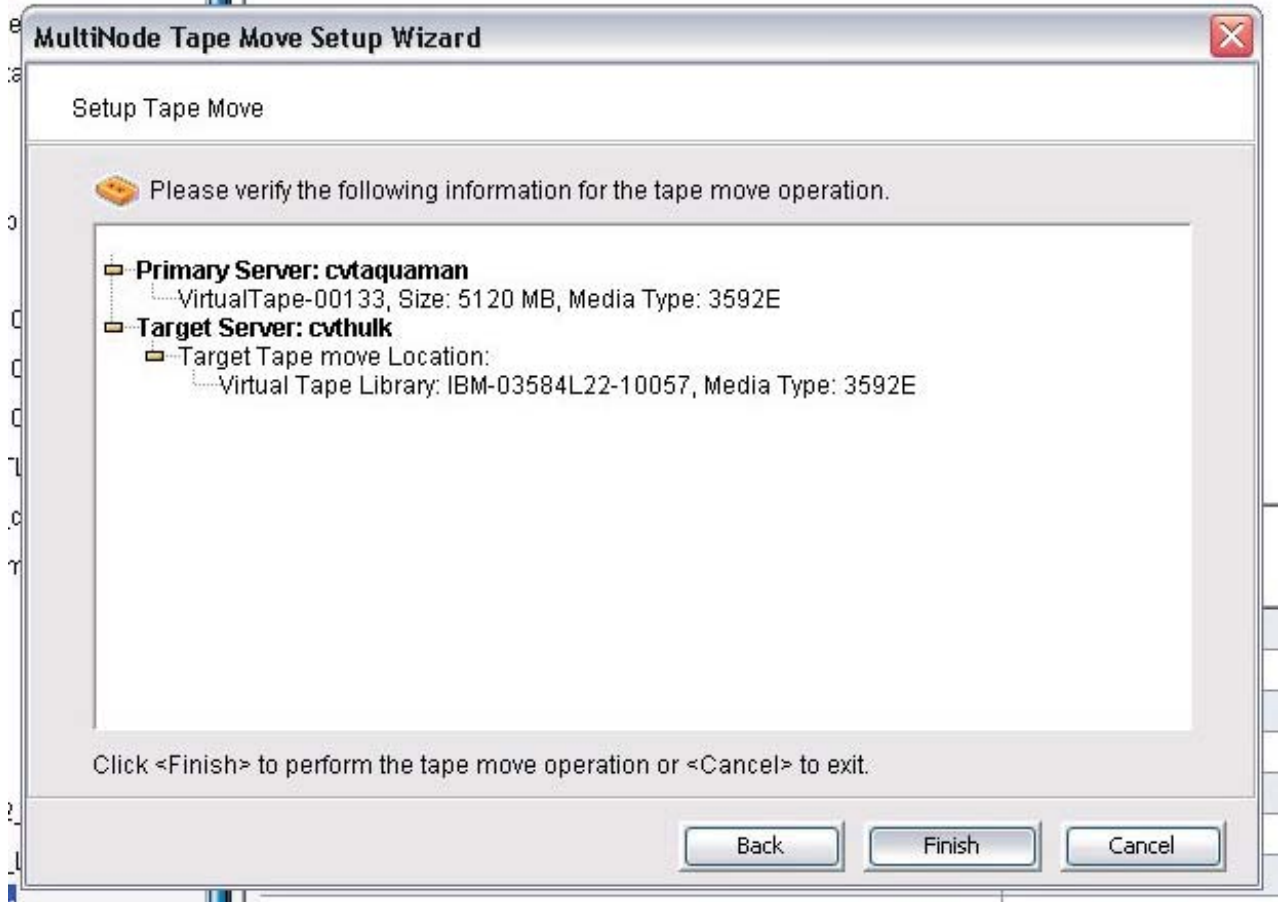
Figure 138. Completing the tape move operation

Note: Tape cartridges are always expanded locally irrespective of which server is accessing the cartridge. For example, a tape created on server1 is being accessed by server2. If the tape cartridge needs to be expanded, expansion will happen on server1, using server1's cache components.

To return the virtual volume back to its owning server, complete the following steps:

1. __ Move the virtual volume to the virtual vault of the server that is currently controlling it.
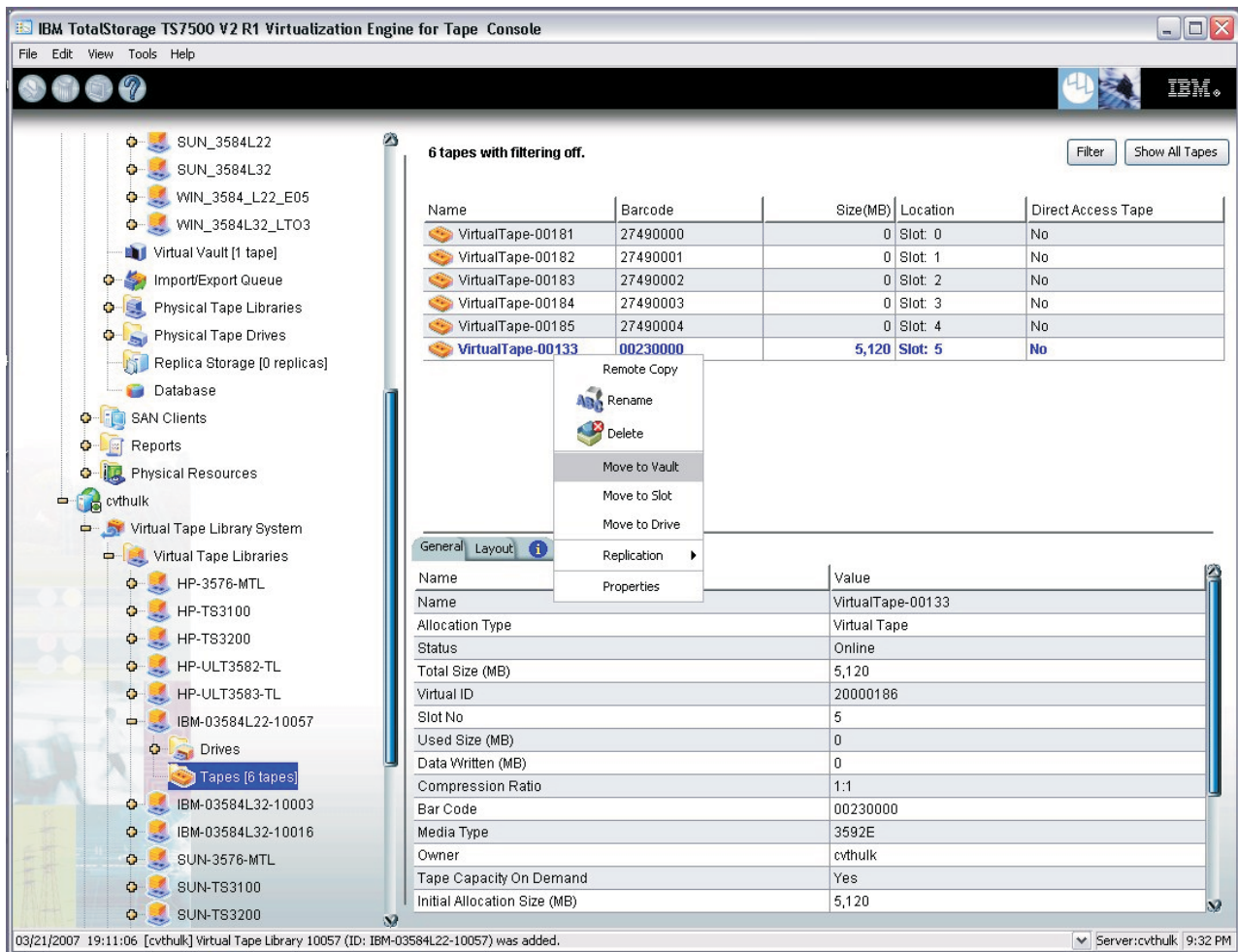
Figure 139. Moving the virtual volume to the virtual vault of controlling server

2. __ In the virtual vault, right-click the virtual volume and then click **Force ownership return**.
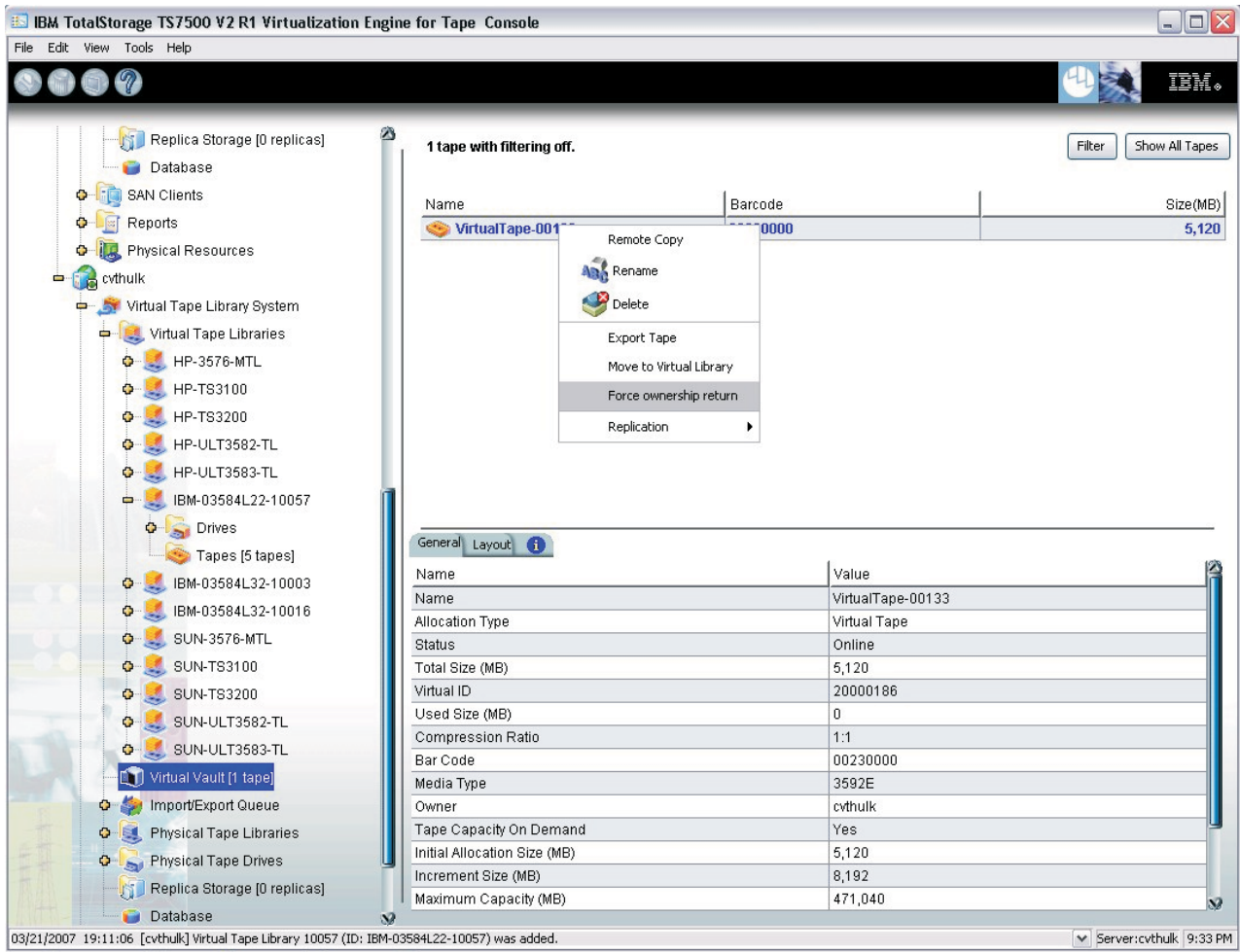
Figure 140. Returning a virtual volume to its owning server

Chapter 17. Troubleshooting

This chapter contains troubleshooting information in the following areas:
- "General VE console operations"
- "Physical resources" on page 198
- "Logical resources" on page 199
- "Import/Export" on page 203
- "Gathering diagnostic data for technical support" on page 204

General VE console operations

The following sections provide troubleshooting tips for general console operations.
- "VE console is unable to connect to a TS7520 Server"
- "Requested operations cannot be performed from the VE console" on page 198
- "Slow VE console operations" on page 198

VE console is unable to connect to a TS7520 Server

The server might be busy while trying to connect. Wait for a few moments and then try to connect again.

There are several operations that occur when the VE console connects to the server. A message window indicates the current step. If there is a failure, the word *Failed* appears at the end of the step. Determining the current phase of connection can help you pinpoint the problem.

Connecting to the TS7520 Server

If the IP address of the server has recently changed, delete the server from the VE console and re-add it. If you entered a server name, try entering its IP address instead. If this does not help or if the IP address has not changed, ping the target machine.

If ping does not reply, ping other machines in the same subnet. If there is still no response, there is a network problem. Run a network command or utility to show the status of the network.

Verifying user name and password

Check the user name and the password. You may use the VE Tape Administrator password or any other administrator or read-only user that you have created with the TS7500 Virtualization Engine previously. Make sure the user name and password exist on the server by opening a local session. The password is case-sensitive. Make sure the **Caps Lock** key is not pressed on the keyboard.

From the workstation where VE console is installed, open a Secure Shell (SSH) session (such as PuTTY) to the TS7520 Server. Log in to the server with the same user name and password. If the connection between the two machines is operational, the SSH session should terminate immediately upon login, as user accounts are not authorized for SSH connection.

Expanding the TS7520 Server node

If the connection operation fails repeatedly during this phase, contact technical support.

Requested operations cannot be performed from the VE console

The TS7520 Server occasionally performs operations, such as data compression or tape cartridge expansion, that cause high processor use. You can check the event log or the system log (in directory `/var/log/messages`) for messages indicating the system's current processor activity. If messages such as **Server Busy** appear in the logs, wait until the current operation finishes, the try requested operation again. If the problem persists or the logs do not indicate high processor use, contact technical support.

Slow VE console operations

Checking VE console workstation memory usage

On the workstation where the VE console is installed, use the appropriate system utility, such as Task Manager, to show the memory usage of all running processes. If the memory usage is unusual, stop all unnecessary processes from running or provide more memory.

Checking server activity

The TS7520 Server occasionally performs operations, such as data compression or tape cartridge expansion, that cause high processor use. You can check the event log or the system log (in directory `/var/log/messages`) for messages indicating a possible increase in workload that might delay update requests from the VE console. Start a second instance of the VE console; if the second VE console cannot establish a connection, the server is busy with other operations. Wait until the current operation finishes, then try requested operation again. If the problem persists or the logs do not indicate high processor use, contact technical support.

Physical resources

This section provides troubleshooting information for problems involving physical resources.

VE console does not show physical storage devices as expected

If physical storage devices have been connected or assigned to the TS7520 Server but do not appear in the VE console, perform the following.

Rescan devices and check logs

1. __ In the VE console, expand the server icon.
2. __ Right-click **Physical Devices** and then click **Rescan**.
3. __ In the "Specify Adapter, SCSI ID and LUN ranges to scan" window:
   a. __ Click **Discover New Devices**.
   b. __ Click **LUN Range**.
   c. __ In the **LUN Range** fields, type a range that you would reasonably expect to include the LUN.
   d. __ Click **OK**.

4. __ Check the event log or the system log (in the `/var/log/messages` directory) for error messages that might correspond to the rescan operation and for reported failures of SCSI devices. The rescan operation might have discovered devices but could not access them because of errors.

Logical resources

This section provides troubleshooting advice for problems involving logical resources, including the following:

- "Virtual tape cartridges are displayed as offline in the VE console"
- "Tape expansion is inoperable"
- "Client cannot detect tape libraries or tape drives"
- "Client can detect but cannot access tape library or tape drive" on page 202

Virtual tape cartridges are displayed as offline in the VE console

If a physical resource that created a virtual tape cartridge is missing, the cartridge's status displays as *offline (missing segment)*. Determine which physical resources comprise the virtual tape cartridge in the VE console by completing the following steps:

1. __ In the VE console, expand **Virtual Tape Library System** and the virtual tape library containing the cartridge until the virtual tape cartridge is visible.
2. __ Click the **Layout** tab.
3. __ Record the SCSI addresses used for the given tape cartridge.
4. __ Expand **Physical Resources** → **Storage Devices** → **Fibre Channel Devices**.
5. __ For all SCSI addresses recorded in step 3, ensure the following conditions exist:
   - __ All physical devices (that is, cache components) are turned on.
   - __ No physical devices have been removed.
   - __ All physical devices are in a normal state and none show failure.
   - __ There is no failures at the connection level.
   - __ Fibre channel connectivity from all physical devices to the TS7500 Virtualization Engine exist.

Tape expansion is inoperable

If you cannot perform tape expansion, check the event log for any error messages related to tape expansion. Errors can occur if any of the following conditions exist:

- There is not enough physical disk space for the expansion. Add more physical storage (that is, cache) or reduce the number of virtual volumes available.
- The physical partition is invalid. Check the cache components.
- An I/O error occurred.

Try to correct the problem and then try to expand the virtual tape cartridge again. If you still cannot do so or if the event log does not show any errors relating to the expansion, contact technical support.

Client cannot detect tape libraries or tape drives

If the client cannot detect tape libraries or tape drives, perform the following troubleshooting items.

Check device discovery by client operating system

Determine whether the client's operating system can detect the device. The method of device detection varies by operating system:

Windows
> Tape libraries appear under **Medium Changers** and tape drives under **Tape drives**. Usually the tape drive is indicated as **\tape<index>**.

Linux The tape library is usually indicated by /dev/sg<index> (the **sg** module should be loaded) and the tape drive is indicated by /dev/st/<index>, /dev/nst/<index>, and /dev/sg/<index> (The **st** module should be loaded).

Solaris
> The tape library is usually indicated by /dev/sg<index> (the **sg** module should be loaded) and the tape drive by /dev/rmt/<index> (the **st** module should be loaded).

HP-UX
> The tape library is usually indicated by /dev/rac/cXtXdX (the **schgr** driver must be loaded) and the tape drive by /dev/rmt/<index> (the **stape** driver should be loaded).

AIX The tape device is usually indicated by /dev/rmt<index> (for all LTO and 3592 tape drives).

See one of the following sections, depending upon whether the operating system can detect the device:
- "Operating system cannot detect device"
- "Operating system can detect device" on page 201

Operating system cannot detect device:

If the operating system cannot detect the device, troubleshoot virtual device discovery by completing the following steps:

1. __ In the VE console, expand **Virtual Tape Library System** and the tape library with the device until the device is visible.
2. __ Click the virtual device.
3. __ In the **General** tab, check the value for **Status**.
4. __ Perform one of the following:
   - __ If the status is *offline*, the repository disk is offline. Check the repository disk.
   - __ If the status is any state other than *offline*, check the following items:

     Zoning
     > The TS7500 Virtualization Engine requires zoning one initiator to one target.

     WWPN
     > a. __ In the VE console, expand the SAN client for the HBA for which the virtual tape library is assigned.
     >
     > b. __ Click the virtual tape library.
     >
     > c. __ From the **General** tab, record the target and initiator WWPNs.
     >
     > d. __ Expand **Physical Resources** → **Storage HBAs**.
     >
     > e. __ Locate the HBA with the WWPN that matches the recorded target WWPN.

f. __ Click the **SNS Table** tab.

g. __ In the SNS table, locate the WWPN that matches the recorded initiator WWPN.

h. __ If the initiator WWPN is not listed, add it by performing the following substeps:

1) __ Right-click the SAN client and then click **Properties**.

2) __ In the Fibre Channel Client Properties window, click the **Initiator WWPNs** tab.

3) __ If the initiator WWPN is listed on the **Initiator WWPNs** tab, select its check box.

4) __ If the initiator WWPN is not listed on the **Initiator WWPNs** tab:

a) __ Click **Add**.

b) __ In the Add Initiator WWPN window, type the missing initiator WWPN.

c) __ Click **OK**.

d) __ Ensure that the new initiator WWPN is listed and selected on the **Initiator WWPNs** tab.

5) __ Click **OK**.

i. __ Repeat steps 4a on page 200 through 4h for any other HBAs from either the client or the TS7500 Virtualization Engine target.

VSA addressing

If the SAN client uses the VSA addressing method (used primarily for addressing virtual buses, targets, and LUNs), ensure that VSA is enabled for the SAN client. If VSA is not enabled, some clients cannot detect more than eight LUNs.

To enable VSA addressing, perform the following:

a. __ In the VE console, right-click the SAN client and then click **Properties**.

b. __ In the Fibre Channel Client Properties window, click the **Option** tab.

c. __ Select the **Enable Volume Set Addressing** check box.

d. __ Click **OK**.

Operating system can detect device:

If the operating system can detect the device but the backup application cannot detect the device at all:

- Ensure that the backup application's driver corresponds to the nature of the tape library and the tape drive
- See the documentation for the backup application to determine whether a specific driver version or specific settings are required
- Ensure that there is not more than one backup application installed on a single backup server; this situation can cause interference between the applications

If both the operating system and the backup application can detect the device, but the backup application does not detect it in the expected location, check serialization. TS7500 Virtualization Engine libraries support serialization. Serialization is the conversion of the content of an object into a sequential stream. It identifies the owner of each component, such as robot, slots, and tape drives. If the

backup application detects the device but not connected to the expected component, serialization might be the cause. Refer to the documentation for the backup application to determine whether a patch or upgrade related to serialization might be required.

Client can detect but cannot access tape library or tape drive

If the client detects the tape library or tape drive but cannot access it, perform the following troubleshooting items.

Check device access by client operating system

Determine whether the client's operating system can access the device. The method of device detection varies by operating system.

Operating systems other than Windows and Unix should use IBM's System Storage Interoperation Center at http://www-01.ibm.com/systems/support/storage/config/ssic/index.jsp

Windows and Unix clients support the use of raw device utilities. These work with tape drives, but are not capable of mounting tape cartridges into tape drives. Before using these tools, complete the following:

- __ Use the VE console to mount a tape cartridge in a tape drive
- __ Stop the backup application

Windows
> `ntutil` is a command line tool that can check tape drives (IBM Ultrium tape drives only).

Unix The `mt` or `tar` commands can access the tape drive. For example, at the Unix command line, you might type the following command: `mt -f /dev/rmt/0 status`.

See one of the following sections, depending upon whether the operating system can access the device:
- "Operating system cannot access device"
- "Operating system can access device" on page 203

Operating system cannot access device:

If the operating system cannot access the device, troubleshoot virtual device access by completing the following steps:
- __ Check the cache components to verify that they are not in error or in an abnormal state. The assigned devices must not be in read-only mode. To verify that the assigned devices are not in read-only mode, perform the following:
  1. __ In the VE console, click the server icon.
  2. __ Expand **Physical Resources** → **Storage Devices** → **Fibre Channel Devices.**
  3. __ Verify that no device icon displays a red dot. The red dot indicates read-only mode.
- __ Check the event log or the system log (in the `/var/log/messages` directory) for messages indicating I/O errors. Such messages often begin with the term `log_scsi_error`.

- __ Check that the adapter driver at the client machine is certified for use with the TS7500 Virtualization Engine.

Operating system can access device:

If the operating system can access the device, verify that the backup application has the correct drivers.

Import/Export

This section provides troubleshooting advice for problems involving the import/export function.

Check for errors

1. __ In the VE console, click the server icon.
2. __ Click the **Attention Required** tab and note any information given there.
3. __ Check the event log or the system log (in the `/var/log/messages` directory) for error messages relating to the physical tape library or tape drive.

Check type of tape cartridge

When you export data from a virtual device to a physical tape device, ensure that the tape devices are of the same type. Because some third-party backup applications alter what they write to the tape depending on the type of tape cartridge used, the TS7500 Virtualization Engine only exports tape cartridges to like media. You cannot export to a dissimilar physical tape cartridge.

Check tape cartridge capacity

Before you import or export data between a virtual device and a physical tape device, ensure that sufficient capacity exists on the tape cartridge. If there is insufficient capacity, an end-of-media-hit condition occurs and the job fails.

If data compression is enabled, ensure that the maximum tape capacity of the virtual tape cartridge is *less than* the actual uncompressed capacity of the physical tape cartridge. This is necessary because the TS7500 Virtualization Engine's disk compression ratio can vary depending upon the dataset. Certain file types (for example, ZIP, PDF, GIF, RAR, and so on) are already compressed and cannot be compressed further.

Check job status

1. __ In the VE console, expand **Virtual Tape Library System**.
2. __ Click **Import/Export Queue**.
3. __ Determine whether the job is still in the queue. Jobs do not start if a barcode problem exists. Ensure that virtual tape cartridges have unique barcodes before importing data from physical tape; otherwise, the import operation fails. Use the Inventory function in the VE console to update barcodes and status from the physical tape library.

Check physical tape library and device status

Ensure that no abnormal conditions exist within the physical tape library; for example, tape drives requiring cleaning or tape cartridges in improper locations.

Check element address on the physical library

Before importing data, review the physical tape library configuration to confirm that all element addresse are sequential and that the SCSI IDs assigned are in the same numeric order as the element addresses.

Gathering diagnostic data for technical support

Gathering diagnostic data is useful for your technical support team to help solve system problems. Each file contains technical information about your server, including server messages and a snapshot of your server's current configuration and environment. You should not create diagnostic data unless you are requested to do so by your technical support representative.

To create a diagnostic data file:

1. __ In the VE console, right-click the server icon and then click **Diagnostic Summary Data**.
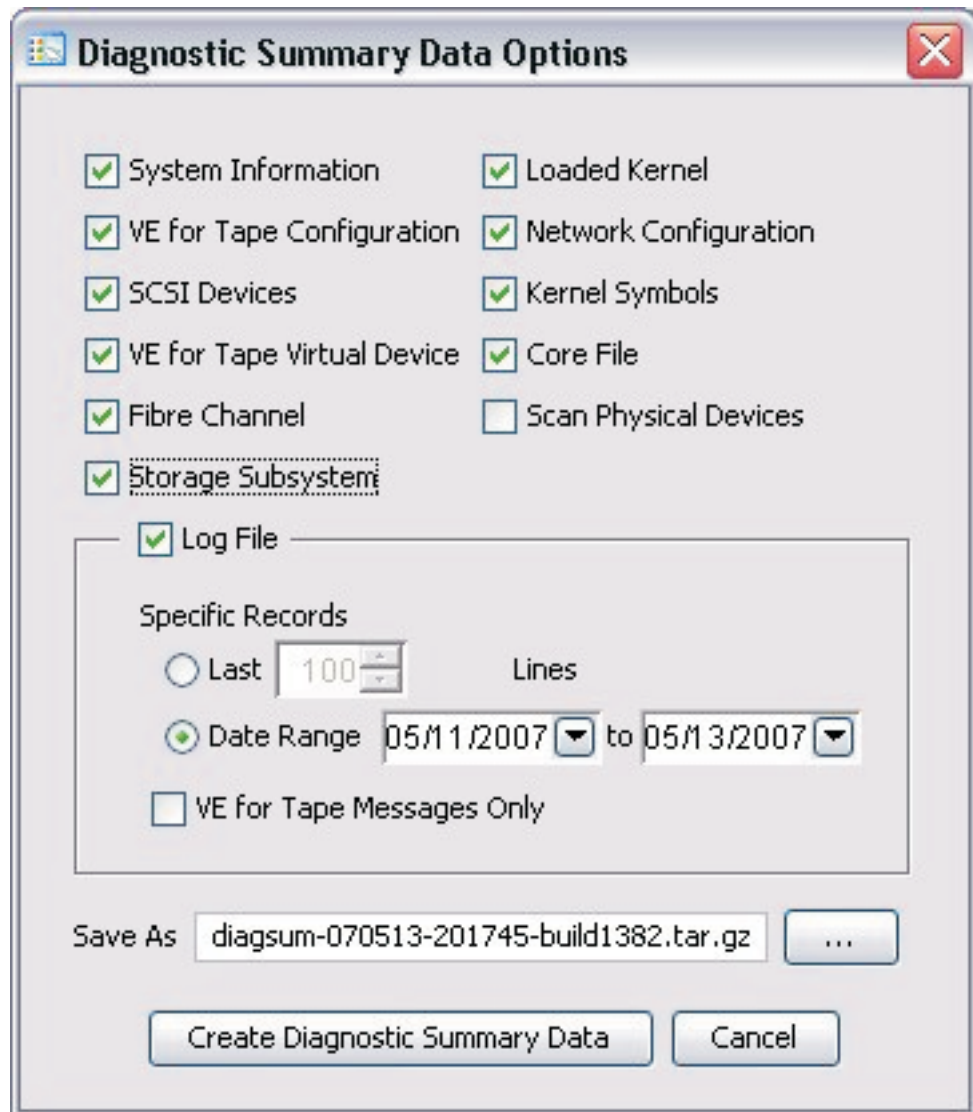
Figure 141. Diagnostic Summary Data Options window

2. Based on the discussion with your technical support representative, select the options to include and set the diagnostic summary file name.

3. If you select the **Storage Subsystem** check box, a warning message appears stating that it might take up to 30 minutes to collect the diagnostic data. This is normal, but select this option only if your support representative advises you to do so.

Appendix A. Command line interface

The TS7500 Virtualization Engine provides a simple utility that allows you to perform some of the more common TS7500 Virtualization Engine functions at a command line instead of through the VE console. You can use this command line utility to automate many tasks, as well as integrate the TS7500 Virtualization Engine with your existing management tools.

Accessing the command line utility

You can access the command line in one of two ways:

- Through the Windows command prompt on a workstation running the VE console software. See "Through the Windows command prompt."
- Through an SSH client program. See "Through an SSH client program."

Through the Windows command prompt

To access the TS7500 Virtualization Engine command line through the Windows command prompt on a workstation that has the VE console installed, perform the following:

1. __ Open the Windows command prompt by clicking **Start→Programs→Accessories→Command Prompt**.
2. __ In the Command Prompt window, navigate to the `C:\Program Files\IBM\VE for Tape\Console\Bin` directory.

Through an SSH client program

To access the TS7500 Virtualization Engine command line through an SSH client program, perform the following:

1. __ If you do not have an SSH client installed at the workstation where the VE console is installed, install the PuTTY SSH client using the procedure in Appendix C, "Installing and starting PuTTY," on page 269.
2. __ Start the SSH client and connect to the TS7520 Server. For an example, see Appendix C, "Installing and starting PuTTY," on page 269 for the procedure to do this using the PuTTY SSH client.
3. __ At the **login as** prompt, type `vetapeservice` and then press the **Enter** key.
4. __ At the **Password** prompt, type `service4u` and then press the **Enter** key.

Using the command line utility

Attention: The `sudo` prefix in the following commands is *only* required if you access the command line through an SSH client program. If you access the command line through the Windows command prompt, do not use the `sudo` prefix; for instance, type `iscon` instead of `sudo iscon`.

Type `sudo iscon` at the command line to display a list of commands. Each command must be combined with the appropriate long or short arguments (ex. Long: --server-name Short: -s servername) that are described in this chapter.

If you type the command name (for example, `c:\sudo  iscon importtape`), a list of arguments will be displayed for that command.

207

Commands

On the following pages is a list of commands you can use to perform system functions from the command line. You should be aware of the following as you enter commands:

- Type each command on a single line, separating arguments with a space.
- You can use either the short or long arguments.
- Variables are listed in <> after each argument.
- Arguments listed in brackets [ ] are optional.
- The order of the arguments is irrelevant.
- Arguments separated by | are choices. Only one can be selected.
- For a value entered as a literal, it is necessary to enclose the value in quotes (double or single) if it contains special characters such as *, <, >, ?, |, %, $, or space. Otherwise, the system will interpret the characters with a special meaning before it is passed to the command.
- Literals cannot contain leading or trailing spaces. Leading or trailing spaces enclosed in quotes will be removed before the command is processed.

Common arguments

The following arguments are used by many commands. For each, a long and short variation is included. You can use either one. The short arguments ARE case sensitive. For arguments that are specific to each command, refer to the section for that command.

Table 10. Common arguments

Short Argument	Long Argument	Value/Description
-s	--server-name	Server Name (hostname or IP address)
-u	--server-username	Server Username
-p	--server-password	Server User Password
-c	--client-name	Client Name
-v	--vdevid	Virtual Device ID

Note: You only need to use the --server-username (-u) and --server-password (-p) arguments when you log into a server. You do not need them for subsequent commands on the same server during your current session. Throughout this appendix, whenever *username* and *password* is specified, use *vetapeservice* and *service4u*.

In addition, the server name should always be the IP address of the server that the command is running on.

Login/logout to the TS7520 Server

This section provides information about logging in and logging out of the TS7520 Server.

Log in to the TS7520 Server

```
sudo  iscon login [-s <server-name> -u <username> -p <password>|-e] [-X <rpc - timeout>]
sudo  iscon login [--server-name=<server-name> --server-username=<username>
--server-password=<password>|--environment] [--rpc-timeout=<rpc - timeout>]
```

Description:

This command allows you to log into the specified TS7520 Server with a given username and password. Once successfully logged into the server, -u (--server-username) and –p (--server-password) are not necessary for the other CLI commands with optional –u and –p arguments.

In order to use the -e (--environment) parameter, you must set the following three environment variables:
- ISSERVERNAME
- ISUSERNAME
- ISPASSWORD

After setting these variables, the environment parameter can be used in the login command in place of -s <server-name> -u <user-name> -p <password>. Therefore, you could type the following to log in: sudo iscon login -e

To set these environment variables in the bash shell, you must set three variables as follows:
- export ISSERVERNAME=10.1.1.1
- export ISUSERNAME=root
- export ISPASSWORD=password

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Log out from the TS7520 Server

```
sudo  iscon logout -s <server-name> [-X <rpc - timeout>]
sudo  iscon logout --server-name = <server-name> [--rpc-timeout = <rpc - timeout>]
```

Description:

This command allows you to log out from the specified TS7520 Server. If the server was not logged in or you have already logged out from the server when this command is issued, error *0x0902000f* will be returned. After logging out from the server, the -u and –p arguments will not be optional for the server commands.

Virtual Devices - client commands

This section describes Virtual Devices - client commands.

Get virtual device list

```
sudo  iscon getvdevlist -s <server-name> [-u <username> -p <password>]
[-l [-v <vdevid> | -n <vdename> ] [-a | -A] [-c | -C] [-M <output - delimiter>] ]
[-X <rpc - timeout>]

sudo  iscon getvdevlist --server-name = <server-name>
[--server-username=<username> --server-password=<password>]
[--longlist [--vdevid=<vdevid> | --vdevname=<vdename>]
[--client-list | --long-client-list] [--physical-layout | --long-physical-layout]
[--output-delimiter=<output-delimiter>] ] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command retrieves and displays information about all virtual devices or a specific virtual device from the specified server. The default output format is a list with a heading.

The –l (--longlist) optional argument displays detailed information for each virtual device. Additional options can be specified along with the –l (--longlist) option to display the physical device layout and/or the assigned client information.

-v (--vdevid) or -n (--vdevname) are options to display only the specified virtual device information when -l (--longlist) is specified.

-a (--physical-layout) or -A(--long-physical-layout) are options to display the physical layout when -l (--longlist) is specified.

-c (--client-list) or -C (--long-client-list) are options to display the assigned client list when -l (--longlist) option is specified.

-M (--output-delimiter) can be specified when -l is specified to replace the linefeed with the specified delimiter. The maximum length of the delimiter is 8.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Get client virtual device list

```
sudo  iscon getclientvdevlist -s <server-name> [-u <username> -p <password>]
-c <client-name> [-t <client-type>] [-l [-a | -A] [-M <output-delimiter>] ]
[-X <rpc-timeout>]

sudo  iscon getclientvdevlist --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--client-name=<client-name> [--client-type=<client-type>]
[--longlist [--physical-layout | --long-physical-layout]
[--output-delimiter=<output-delimiter>] ] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command retrieves and displays information about all virtual devices assigned to the client from the specified server. The default output format is a list with heading. Use -c (--client-name) to specify a client name or * for all clients. -t (client-type) is the type of the client protocol to be retrieved in one of the following values: SCSI, FC, or ISCSI. The client type will only take effect when the client name is *. Be aware that in some platforms you are required to enclose the ″*″ in double quote to take it as a literal.

-l(--longlist) is an option to display the long format.

-a(--physical-layout) or -A(--long-physical-layout) is an option to display the physical layout when -l(--longlist) is specified.

-M (--output-delimiter) can be specified when -l is specified to replace the linefeed with the specified delimiter. The maximum length of the delimiter is 8.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Add client

```
sudo  iscon addclient -s <server-name> [-u <username> -p <password>]
-c <client-name> [-t <client-type>]
[-I <initiator-wwpns>] [-a <on>] [-A <on>] [-X <rpc-timeout>]
```

```
sudo  iscon addclient --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--client-name=<client-name> [--client-type=<client-type>]
[--initiator-wwpns=<initiator-wwpns>] [--enable-VSA=<on>] [--enable-AS400=<on>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to add a client to the specified server. -c (--client-name) is a unique client name for the client to be created. The maximum length of the client name is 64. The following characters are invalid for a client name: <>"&$/\'

-t (--client-type) is an option to specify the type of the client protocol, SCSI, iSCSI, or FC. '

-I (--initiator-wwpns), -a (--enable-VSA) and -A (--enable-AS400) are options for Fibre Channel clients, which can be set when the client type is FC.

-I (--initiator-wwpns) is the option to set the initiator WWPNs. An initiator WWPN is a 16-byte Hex value. Separate the initiator WWPN by comma if more than one initiator WWPN is specified. For example: *13af35d2f4ea6fbc,13af35d2f4ea6fad*

-a (--enable-VSA) is an option for Volume Set Addressing with the following values: on or off (default).

-A (--enable-AS400) is an option to support IBM iSeries® Server with the following values: on or off (default).

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Delete client

```
sudo  iscon deleteclient -s <server-name> [-u <username> -p <password>]
-c <client-name> [-X <rpc-timeout>]

sudo  iscon deleteclient --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--client-name=<client-name> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to delete a client from the specified server. -c (--client-name) is the name of the client to be deleted.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Get client properties

```
sudo  iscon getclientprop -s <server-name> [-u <username> -p <password>]
-c <client-name> [-X <rpc-timeout>]

sudo  iscon getclientprop --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--client-name=<client-name> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command gets client properties. -c (--client-name) is required to specify the client name.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Set fibre channel client properties

```
sudo  iscon setfcclientprop -s <server-name> [-u <username> -p <password>] -c <client-name>
[-I <initiator-wwpns>] [-a <on>] [-A <on>] [-X <rpc-timeout>]

sudo  iscon setfcclientprop --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--client-name=<client-name> [--initiator-wwpns=<initiator-wwpns>]
[--enable-VSA=<on>] [--enable-AS400=<on>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to set fibre channel client properties. -c (--client-name) is required.

-I (--initiator-wwpns) is the option to set the initiator WWPNs for the client. An initiator WWPN is a 16-byte hex value. Separate the initiator WWPNs with a comma if more than one initiator WWPN is specified. For example, *13af35d2f4ea6fbc,13af35d2f4ea6fad*

To clear the initiator WWPNs from the Fibre Channel client properties, specify * as the initiator WWPN list.

-a (--enable-VSA) is an option for Volume Set Addressing with the following values: *on* and *off*.

-A (--enable-AS400) is an option to support IBM iSeries Server with the following values: *on* and *off*.

This option cannot be set if the client is already assigned to virtual devices.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Assign virtual device

```
sudo  iscon assignvdev -s <server-name> [-u <username> -p <password>]
-v <vdevid> -c <client-name> -a <access-mode> [-y]
[-I <initiatorWWPN>] [-T <targetWWPN>] [-l <lun>] [-X <rpc-timeout>]

sudo  iscon assignvdev --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --vdevid=<vdevid>
--client-name=<client-name> --access-mode=<access-mode> [--vlib-only]
[--initiatorWWPN=<initiatorWWPN>] [--targetWWPN=<targetWWPN>] [--lun=<lun>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to assign a virtual device on a specified server to a client.

-v (--vdevid) is required to specify the virtual device ID of the virtual tape library or virtual tape drive to be assigned.

-c (--client-name) is required to specify the client to which the virtual tape library or drive will be assigned.

The values for `<access-mode>` are: *Readonly, ReadWrite, ReadWriteNonExclusive*. The values for the short format are: *R* / *W* / *N*.

-y (--vlib-only) is an option that allows you to assign the virtual tape library to the client without assigning all of the virtual tape drives in the library. The default is to assign all of the virtual tape drives in the library.

-I (--initiatorWWPN) and -T (--targetWWPN) are options for Fibre Channel clients. The initiator WWPN or target WWPN is a 16-byte hex value or "*" for all. For example, *13af35d2f4ea6fbc*. The default is "*" if it is -I or the -T option is not specified.

-l (--lun) is another option for Fibre Channel clients. The range is between 0 and 15. The next available LUN will be assigned if is it is not specified.

-M (--output-delimiter) can be specified when -l is specified to replace the linefeed with the specified delimiter. The maximum length of the delimiter is 8.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Unassign virtual device

```
sudo  iscon unassignvdev -s <server-name> [-u <username> -p <password>]
-v <vdevid> -c <client-name> [-y] [-f] [-X <rpc-timeout>]

sudo  iscon unassignvdev --server-name=<server-name> [--server-username=<username>]
[--server-password=<password>] --vdevid=<vdevid> --client-name=<client-name>
[--vlib-only] [--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to unassign a virtual device on the specified server from a client.

-v (--vdevid) is required to specify the virtual device ID of the virtual tape library or drive to be unassigned.

-c (--client-name) is required to specify the client name from which to unassign the library or drive.

-y (--vlib-only) is an option that allows you to unassign the virtual tape library to the client without unassigning all of the virtual tape drives in the library. The default is to unassign all of the virtual tape drives in the library.

The -f (--force) option is required to unassign the virtual device when the client is connected and the virtual device is attached. An error will be returned if the force option is not specified.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Create virtual device

```
sudo  iscon createvdev -s <server-name> [-u <username> -p <password>]
-I <ACSL> [-n <vdevname>] [-X <rpc-timeout>]

sudo  iscon createvdev --server-name=<server-name>
```

```
[--server-username=<username> --server-password=<password>]
--scsiaddress=<ACSL> [--vdevname=<vdevname>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to create a direct virtual device, such as virtual tape library or virtual tape drive.

-I (--scsiaddress) is required to specify the SCSI address of the virtual tape library or virtual tape drive in the following format: *ACSL=#:#:#:# (adapter:channel:id:lun)*

-n (--vdevname) is an option to specify the direct virtual device name. A default name will be generated if the name is not specified. The maximum length is 64. Leading and trailing spaces will be removed. Enclose the name in double quotes. The following characters are invalid for the direct virtual device name: <>"&$/\'

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Delete virtual device

```
sudo  iscon deletevdev -s <server-name> [-u <username> -p <password>]
-v <vdevid> [-d] [-f] [-X <rpc-timeout>]]

sudo  iscon deletevdev --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --vdevid=<vdevid>
[--delete-virtual-tapes] [--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to delete a direct virtual device, such as virtual tape library or virtual tape drive. The virtual device cannot be deleted if there are clients currently connected to the library or drive.

-v (--vdevid) is required to specify the virtual tape, library, or virtual tape drive to be deleted.

-d (--delete-virtual-tapes) is an option to delete the associated tapes. -f (--force) option is required to delete the tapes. If this option is not specified, the tapes will be moved to the vault.

The *force* option is required to delete the resource if any of the following conditions applies:
- The virtual device is a virtual tape and is configured as a primary replica. The replica will be promoted as long as the replication is not in progress. Otherwise, the replica will be deleted.
- The virtual device is a virtual tape library or a virtual tape drive, and -d (--delete-virtual-tapes) option is specified to delete the tapes.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Virtual devices - TS7520 Server commands

This section describes Virtual devices - TS7520 Server commands.

Get TS7500 Virtualization Engine information

```
sudo  iscon getvtlinfo -s <server-name> [-u <username> -p <password>]
[-T <vtl-info_type> [-L <tape-library-vid>]] [-F <vtl-info-filter>] [-l [-M]]
```

```
| [-X <rpc-timeout>]
|
| sudo  iscon getvtlinfo --server-name=<server-name>
| [--server-username=<username> --server-password=<password>]
| [--vtl-info-type=<vtl-info_type> [--tape-library-vid=<tape-library-vid>] ]
| [--vtl-info-filter=<vtl-info-filter>]
| [--longlist [--ouput-delimiter=<output-delimiter>] ] [--rpc-timeout=<rpc-timeout>]
```

| **Description:**

| This command retrieves TS7500 Virtualization Engine information.

| -T (--vtl-info-type) is the TS7500 Virtualization Engine information type with one of the following values:
| *VLIBS* or *VDRIVES* or *VAULT* or *PLIBS* or *PDRIVES*.
| • *VLIBS* = display virtual tape libraries only.
| • *VDRIVES* = display standalone virtual tape drives only
| • *VAULT* = display virtual tape vault only.
| • *PLIBS* = display physical tape libraries only.
| • *PDRIVES* = display standalone physical tape drives only.

| The default is to display all the information.

| -L (--tape-library-vid) is an option to specify the virtual tape library when VLIBS is specified, or to specify
| the physical tape library when PLIBS is specified.

| -F (--vtl-info-filter) is an additional filter that can be combined using the following values separated by
| comma: *library* or *drive* or *tape*.
| • *library* = include physical and/or virtual library information.
| • *drive* = include physical and/or virtual drive information.
| • *tape* = include physical and/or virtual tape information.

| For example: *-F "library,drive,tape"* or *--vtl-info-filter="library,drive,tape"*

| The default is to display all of the information that applies. There will be an error if `<vtl-info-type>` is
| specified and the `<vtl-info-filter>` specified does not apply. For example, "library" does not apply to
| "VDRIVES".

| -l (--longlist) is an option to display the information in a detail format.

| -M (--output-delimiter) can be specified when -l is specified to replace the linefeed with the specified
| delimiter. The maximum length of the delimiter is 8.

| -X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout.
| The system will retry the command for the amount of time specified if the server does not respond. The
| default RPC timeout is 30 seconds if it is not specified.

| # Get supported virtual libraries
```
| sudo  iscon getsupportedvlibs -s <server-name> [-u <username> -p <password>]
| [-l [-t <vlib-type>] [-c][-M <output-delimiter>] ] [-X <rpc-timeout>]
|
| sudo  iscon getsupportedvlibs --server-name=<server-name>
| [--server-username=<username> --server-password=<password>]
```

```
| [--longlist [--vlib-type=<vlib-type>] [--compatible-drive-list]
| [--output-delimiter=<output-delimiter>] ] [--rpc-timeout=<rpc-timeout>]
```

| **Description:**

| This command retrieves information about all supported virtual tape libraries.

| -l (--longlist) can be specified to get the supported library information in a long format. The default is to
| display the information in a list format.

| -t (--vlib-type) is an option with the -l (--longlist) option to get the detail library information for a specific
| library. The format for the `<vlib-type>` is: `<vendorID>:<productID>`. For example, *ADIC:Scalar 100*

| -c (--compatible-drive-list) is an option to display the compatible drives in a tabular format instead of the
| default long format.

| -M (--output-delimiter) can also be specified with the -l (--longlist) option to replace the linefeed with the
| specified delimiter. The maximum length of the delimiter is 8.

| -X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout.
| The system will retry the command for the amount of time specified if the server does not respond. The
| default RPC timeout is 30 seconds if it is not specified.

| # Get supported virtual drives
```
| sudo  iscon getsupportedvdrives -s <server-name> [-u <username> -p <password>]
| [-l [-M <output-delimiter>] ] [-X <rpc-timeout>]
|
| sudo  iscon getsupportedvdrives --server-name=<server-name>
| [--server-username=<username> --server-password=<password>]
| [--longlist [--output-delimiter=<output-delimiter>] ] [--rpc-timeout=<rpc-timeout>]
```

| **Description:**

| This command retrieves information about all supported virtual tape drives.

| -l (--longlist) can be specified to get the supported drive information in a long format. The default is to
| display the information in a list format.

| -M (--output-delimiter) can be specified when -l is specified to replace the linefeed with the specified
| delimiter. The maximum length of the delimiter is 8.

| -X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout.
| The system will retry the command for the amount of time specified if the server does not respond. The
| default RPC timeout is 30 seconds if it is not specified.

| # Create virtual tape library
```
| sudo  iscon createvirtuallibrary -s <server-name> [-u <username> -p <password>]
| -t <vlib-type> [-n <vlib-name>] -d <vdrive-type> [-r <vdrive-name-prefix>]
| [-R <num-of-drives>] [-A <auto-archive-mode> [-j] | -N <auto-repl-mode> -S <target-name>
| [-M <#[D|H|M]>] ] [-B <barcode-range>] [-T <num-of-slots>] [-e]
| [-E <import-export-slots>] [-D -I <initial-size> -C <increment-size>]
| [-m <max-capacity>] [-X <rpc-timeout>]
|
| sudo  iscon createvirtuallibrary --server-name=<server-name>
| [--server-username=<username> --server-password=<password>]
```

```
| --vlib-type=<vlib-type> [--vlib-name=<vlib-name>] --vdrive-type=<vdrive-type>
| [--vdrive-name-prefix=<vdrive-name-prefix>] [--num-of-drives=<num-of-drives>]
| [--auto-archive-mode=<auto-archive-mode> [--auto-eject-to-ie] |
| --auto-replication=<auto-repl-mode> --target-name=<target-name>
| [--delay-delete-time=<#[D|H|M]>] ] [--barcode-range=<barcode-range>]
| [--num-of-slots=<num-of-slots>] [--export-to-ptape]
| [--import-export-slots=<import-export-slots>] [--capacity-on-demand
| --initial-size=<initial-size> --increment-size=<increment-size>]
| [--max-capacity=<max-capacity>] [--rpc-timeout=<rpc-timeout>]
```

| **Description:**

| This command creates a virtual tape library.

| -t (--vlib-type) is required in the following format:`<vdendorID>:<productID>`

| -n (--vlib-name) is optional. A default name will be provided in the format of `<vendorID>-<productID>-<vid>`
| if it is not specified.

| -d (--vdrive-type) is required to specify the type of tape drive to be created in the library. The format of
| `<vdrive-type>` is as follows: `<vdendorID>:<productID>`

| -r (--vdrive-name-prefix) is an option to specify the prefix of the virtual drive. The default prefix is in the
| format of `<drive-vdendorID>-<drive-productID>-<vid>`.

| -R (--num-of-drives) can also be specified up to the maximum number of drives supported by the library.
| The default is 1 if it is not specified.

| -A (--auto-archive-mode) is an option with one of the following values: *copy* or *move*.

| -j (--auto-eject-to-ie) is an option to be specified with -A (--auto-archive-mode) to eject the tape to the
| import/export (IE) slot after the export job.

| -N (--auto-replication) is an option with one of the following values: *remotecopy* or *remotemove*.

| -S (--target-name) is the remote server name for auto-replication. It is required for auto-replication.

| -M (--delay-delete-time) is an option for remotemove mode to specify a time to wait before deletion. It can
| be specified in days(D), hours(H) or minutes(M). For example, 2D, 10H, 150M

| -B (--barcode-range) can be specified in the following format: `<barcodeB>-<barcodeE>`

| Barcode is an alpha-numeric value with a length of 6 to 8. `<barcodeB>` and `<barcodeE>` have to be the
| same length.

| `<barcodeE>` has to be greater then `<barcodeB>`. A default `<barcode-range>` will be generated if it is not
| specified.

| -T (--num-of-slots), -e (--export-to-tape) and -E (--import-export-slots) are optional. The range of the
| `<num-of-slots>` and `<import-export-slots>` is between 1 and the maximum number supported by the
| specified library type. The default for the library will be used if it is not specified.

| -D (--capacity-on-demand) is an option to expand the virtual tape when needed. The default is to create
| the virtual tape with the maximum capacity if it is not specified.

| -I (--initial-size) and -C (--increment-size) are options to be specified with `<capacity-on-demand>` option.

-m (--max-capacity) is an option to specify the maximum capacity of the virtual tape. The maximum capacity configured for the specified type of virtual library will be used if it is not specified.

The unit of `<max-capacity>`, `<initial-size>` and `<increment-size>` are all in GB. A virtual device ID will be assigned to the virtual library when it is created successfully.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Add virtual tape drive

```
sudo  iscon addvirtualdrive -s <server-name> [-u <username> -p <password>]
-L <tape-library-vid> [-r <vdrive-name-prefix>] [-R <num-of-drives>] [-X <rpc-timeout>]

sudo  iscon addvirtualdrive --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--tape-library-vid=<tape-library-vid> [--vdrive-name-prefix=<vdrive-name-prefix>]
[--num-of-drives=<num-of-drives>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command adds a virtual tape drive to a specify virtual tape library.

-L (--tape-library-vid) is required to specify the virtual tape library to add the virtual tape drive(s).

-r (--vdrive-name-prefix) is an option to specify the prefix of the virtual tape drive. The default prefix is in the format of `<drive-vdendorID>-<drive-productID>-<vid>`.

-R (--num-of-drives) is optional, the default is 1 if it is not specified.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Creating standalone tape drive

```
sudo  iscon createstandalonedrive -s <server-name> [-u <username> -p <password>]
-d <vdrive-type> [-r <vdrive-name-prefix>] [-R <num-of-drives>]
[-D -I <initial-size> -C <increment-size>] [-m <max-capacity>] [-X <rpc-timeout>]

sudo  iscon createstandalonedrive --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--vdrive-type=<vdrive-type> [--vdrive-name-prefix=<vdrive-name-prefix>]
[--num-of-drives=<num-of-drives>] [--capacity-on-demand --initial-size=<initial-size>
--increment-size=<increment-size>] [--max-capacity=<max-capacity>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a standalone virtual tape drive.

-d (--vdrive-type) is required to specify the type of tape drive to be created in the following format:
`<vdendorID>:<productID>`

-r (--vdrive-name-prefix) is an option to specify the prefix of the virtual drive. The default prefix is in the format of `<drive-vdendorID>-<drive-productID>-<vid>`.

-R (--num-of-drives) can be specified to create multiple drives of the same type. The default is 1 if it is not specified. The maximum number of drives is 10.

-D (--capacity-on-demand) is an option to expand the virtual tape when needed. The default is to create the virtual tape with the maximum capacity if it is not specified.

-I (--initial-size) and -C (--increment-size) are options to be specified with `<capacity-on-demand>` option.

-m (--max-capacity) is an option to specify the maximum capacity of the virtual tape. The maximum capacity configured for the specified type of virtual tape drive will be used if it is not specified.

The unit of `<max-capacity>`, `<initial-size>` and `<increment-size>` are all in GB.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Create virtual tape

```
sudo  iscon createvirtualtape -s <server-name> [-u <username> -p <password>] -v <parent-vid>
[ [-g <#(GB)> [-I <ACSL>] | -M <custom-method> | -L <custom-layout>] ]
[-n <vdevname>] [-B <barcode>] [-A -l <plib-vid> -b <physical-tape-barcode> [-j] |
-N [-S <target-name>] [-U <target-username> -P <target-password>] [-c <on>]
[-e <on>] ] [-t <count>] [-X <rpc-timeout>]

sudo  iscon createvirtualtape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--parent-vid=<parent-vid> [ [--size-gb=<#(GB)>] [--scsiaddress=<ACSL>] |
--custom-method=<custom-method> --custom-layout=<custom-layout>] ]
[--vdevname=<vdevname>] [--barcode=<barcode>]
[--enable-auto-archive --plib-vid=<plib-vid>
--physical-tape-barcode=<physical-tape-barcode>
[--auto-eject-to-ie] | --enable-auto-replication
--target-name=<target-name> [--target-username=<target-username>
--target-password=<target-password>] [--compression=<on>] [--encryption=<on>] ]
[--count=<count>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a virtual tape.

-v (--parent-vid) is the virtual device id of the virtual tape library or standalone tape drive.

-g (--size-gb) is an option to specify the size in GB. The size of the virtual tape will be the size configured in the properties of the virtual tape library or virtual tape drive if it is not specified.

-I (--scsiaddress) is the option to specify a specific physical device to be used to create the virtual device. *ACSL=#:#:#:# (adapter:channel:id:lun)*

The -M (--custom-method) and -L (--custom-layout) are options for specific physical segments. There can be a list or a file enclosed in <> containing physical segment in each line.

The format of the physical segment for <custom-mode> is: *adapter:channel:scsi-id:lun:first-sector:size-in-MB* The format for `<custom-layout>` is: *adapter:channel:scsi-id:lun:first-sector:last-sector.*

The -g, -I options cannot be specified with -M or -L option.

-n (--vdevname) is an option to specify the virtual tape name or prefix when creating more than one tape. The maximum length of the virtual device name is 64. Leading and trailing spaces will be removed. Enclose the name in double quotes to ensure the proper name. The following characters are invalid for the name: <>″&$/\'

-B (--barcode) is the option to specify the barcode range for the tape(s). The format for the barcode range is: *BBBBBBBB-EEEEEEEE*. This option cannot be specified when -A (--enable-auto-archive) option is specified.

-A (--enable-auto-archive) is an option when the parent library is enabled with auto-archive option.

-l (--plib-vid) is required when `<auto-archive-mode>` is specified. It is the physical tape library where the tape will be exported to automatically.

-b (--physical-tape-barcode) is required to specify the list of physical tape barcode(s) when auto-archive option is specified. Separate barcodes by comma for more than one physical tape. For example, *-b 00010001,00010009,0001000A*

-e (--auto-eject-to-ie) is optional when `<auto-archive-mode>` is specified.

-N (--enable-auto-replication) is an option when the parent library is enabled with the auto-replication option.

-S (--target-name) can be specified when auto-replication option is specified. The default remote server from the parent library will be used if it is not specified.

-c (--compression) and -e (--encryption) can be specified when auto-replication option is specified.

-c (--compression) is an option to enable or disable compression with one of the values: *on* or *off*.

-e (--encryption) is an option to enable or disable encryption with one of the values: *on* or *off*.

-t (--count) is an option to create multiple tapes in a virtual tape library. This option cannot be specified when -A (-- enable-auto-archive) option is specified because the number of tapes will be obtained from the list of barcodes specified with -b (--physical-tape-barcode) option.

If a barcode range is specified with -B (--barcode) option and -t (--count) option is also specified, `<count>` will be served as the maximum number of tapes to be created. If the number of the barcodes from the specified range is less than the `<count>`, an error will be returned to indicate that there are not enough barcodes for the specified number of tapes.

If neither barcode nor count is specified, the default `<count>` will be 1.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Move virtual tape

```
sudo  iscon movevirtualtape -s <server-name> [-u <username> -p <password>] -v <vdevid>
[-L <tape-library-vid> | -D <tape-drive-vid> | -l <slot-no>] [-X <rpc-timeout>]

sudo  iscon movevirtualtape --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --vdevid=<vdevid>
[--tape-library-vid=<tape-library-vid> | --tape-drive-vid=<tape-drive-vid> |
--slot-no=<slot-no>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command moves a virtual tape to a different location.

-v (--vdevid) is required to specify the ID of the virtual tape to be moved.

-L (--tape-library-vid) is the virtual library to move to.

-D (--tape-drive-vid) is the virtual drive in a library or the standalone drive to move to.

-l (--slot-no) is the slot in a library to move to.

If none of the above locations are specified, the vault will be assumed to be the new location. If the tape is in a slot in a library, it can be moved to a different slot or a drive in the library, or it can be moved to the vault.
- Vlib Slot -> Tape drive (in the library only)
- Vlib Slot -> Slots in same library
- Vlib Slot -> Vault

If it is in a drive in the library, it can be moved to an available slot in the library or to the vault.
- Vlib Drive -> Slots in same library
- Vlib Drive -> Vault

If the tape is in a standalone drive, it can only be moved to the vault.
- Standalone Tape Drive -> Vault

If the tape is in the vault, it can be moved to an available slot in a library, or an available standalone drive.
- Vault -> Vlib (First available slot)
- Vault -> Standalone Tape Drive

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Inventory physical tape library

```
sudo  iscon plibinventory -s <server-name> [-u <username> -p <password>]
[-L <tape-library-vid>] [-X <rpc-timeout>]

sudo  iscon plibinventory --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--tape-library-vid=<tape-library-vid>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command performs an inventory of the physical tapes in a physical tape library.

-L (--tape-library-vid) is an option to specify the physical tape library to perform the inventory.

Inventory operation will be performed for all the physical tape libraries if -L (--tape-library-vid) is not specified.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Assign physical resource to the TS7500 Virtualization Engine

```
sudo  iscon assignresourcetovtl -s <server-name> [-u <username> -p <password>]
-v <vdevid> [-L <tape-library-vid>] [-X <rpc-timeout>]

sudo  iscon assignresourcetovtl --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--vdevid=<vdevid> [--tape-library-vid=<tape-library-vid>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command assigns a physical tape library or drive to the TS7500 Virtualization Engine.

-v (--vdevid) is required to specify the ID of the physical tape library or the physical tape drive to be assigned to the TS7500 Virtualization Engine.

-L (--tape-library-vid) is an option to specify the physical tape library as a parent when assigning physical tape drive to physical tape library that is already assigned to the TS7500 Virtualization Engine.

The physical tape library information can be retrieved by issuing the getvtlinfo command.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Unassign physical resource from the TS7500 Virtualization Engine

```
sudo  iscon unassignresourcefromvtl -s <server-name> [-u <username> -p <password>]
-v <vdevid> [-X <rpc-timeout>]

sudo  iscon unassignresourcefromvtl --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --vdevid=<vdevid>
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command unassigns a physical tape library or drive from the TS7500 Virtualization Engine.

-v (--vdevid) is required to specify the ID of the physical tape library or the physical tape drive to be unassigned from the TS7500 Virtualization Engine.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Tape copy

```
sudo  iscon tapecopy -s <server-name> [-u <username> -p <password>]
-v <source-vdevid> -S <target-name> [-U <target-username> -P <target-password>]
[-L <tape-library-vid> | -D <tape-drive-vid>] [-n <vdevname>] [-f]
[-X <rpc-timeout>]

sudo  iscon tapecopy --server-name=<server-name>
```

```
| [--server-username=<username> --server-password=<password>]
| --source-vdevid=<source-vdevid> --target-name=<target-name>
| [--target-username=<target-username> --target-password=<target-password>]
| [--tape-library-vid=<tape-library-vid> | --tape-drive-vid=<tape-drive-vid>]
| [--vdevname=<vdevname>] [--force] [--rpc-timeout=<rpc-timeout>]
```

| **Description:**

| This command copies a tape.

| -v (--source-vdevid) is required to specify the ID of the virtual tape to be copied from.

| -S (--target-name) is required to specify the target server name where the remote tape copy will be
| created and copied to.

| -U (--target-username) and -P (--target-password) are optional for connection and login to the target server
| if the target server was not logged in with login command.

| -L `<tape-library-vid>` and -D `<tape-drive-vid>` are options to move the tape copy to the virtual tape
| library or virtual tape drive when the copy is completed.

| -n (--vdevname) is an option to specify the virtual tape name of the tape copy. The maximum length of the
| virtual device name is 64. Leading and trailing spaces will be removed. Enclose the name in double
| quotes. The following characters are invalid for the name: <>"&$/\'

| A default name with the primary server and source virtual tape name will be generated if it is not specified.

| -f (--force) option is required when the tape is scheduled to be deleted. The deletion schedule for the
| virtual tape will be removed and the replication will be configured.

| -X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout.
| The system will retry the command for the amount of time specified if the server does not respond. The
| default RPC timeout is 30 seconds if it is not specified.

| # Set tape properties
```
| sudo  iscon settapeproperty -s <server-name> [-u <username> -p <password>]
| -v <vdevid> [-B <barcode>] [-f] [-F] [-w <on>] [-A <auto-archive-mode>]
| [-X <rpc-timeout>]
|
| sudo  iscon settapeproperty --server-name=<server-name>
| [--server-username=<username> --server-password=<password>] --vdevid=<vdevid>
| [--barcode=<barcode>] [--force] [--full-capacity] [--tape-write-protect=<on>]
| [--auto-archive-mode=<auto-archive-mode>] [--rpc-timeout=<rpc-timeout>]
|
```

| **Description:**

| This command sets tape properties.

| -v (--vdevid) is required to specify the ID of the virtual tape to set the properties.

| -B (--barcode) is the option to specify the new barcode for the tape. -f (--force) option is required if the new
| barcode is not in the barcode range specified for the parent library.

-F (--full-capacity) is an option to expand the tape to the maximum capacity and turn off the `<capacity-on-demand>` option if it is enabled for the virtual tape.

-w (--tape-write-protect) is an option to turn on and off the tape write protection with the following values: *on* or *off*.

-A (--auto-archive-mode) is an option with one of the following values: *copy* or *move* or *inherited* or *none*.
- "none" is the value to turn off the auto-archive mode if the virtual tape is enabled with auto-archive option.
- "inherited" can only be specified when the parent library is enabled with auto-archive option.

-A (--auto-archive-mode) cannot be specified if auto-replication is enabled for the tape.

At least one of the properties has to be specified.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Import/Export

This section describes command lines for importing and exporting tape.

Import tape

```
sudo  iscon importtape -s <server-name> [-u <username> -p <password>]
[-M <import-mode>] -v <plib-or-pdrive-vid> [-B <barcode> | -l <slot-no>]
-L <tape-library-vid> [-b <virtual-tape-barcode>] -t <virtual-tape-slot-no>
[-j <job-description>] [-X <rpc-timeout>]

sudo  iscon importtape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--import-mode=<import-mode>] --plib-or-pdrive-vid=<plib-or-pdrive-vid>
[--barcode=<barcode> | --slot-no=<slot-no>] --tape-library-vid=<tape-library-vid>
--virtual-tape-slot-no=<virtual-tape-slot-no>
[--virtual-tape-barcode=<virtual-tape-barcode>] [--job-description=<job-description>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command imports the data from a tape into the TS7500 Virtualization Engine.

-M (--import-mode) is an option in one of the following values: *copy (default)* or *direct-access* or *recycle*.

-v (--pdrive-or-pdrive-vid) is required to specify the virtual device ID of the physical tape library or physical tape drive from which the physical tape is to be imported.

If the physical tape is from a physical tape library, either `<barcode>` or `<slot-no>` of the physical tape should be specified with -B (--barcode) or -l (--slot-no) to identify the physical tape. The physical tape information is not required if it is from a physical tape drive.

-L (--tape-library-vid) is the virtual device ID of the virtual tape library to which the physical tape is to be imported.

-t (--virtual-tape-slot-no) is required for the virtual tape location.

-b (--virtual-tape-barcode) is optional when the physical tape from a physical tape library contains barcode. It is required if the physical tape does not have a barcode or when it is from a physical tape drive. -j (--job-description) is an option to specify a description for the tape import job.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Export virtual tape

```
sudo  iscon exportvirtualtape -s <server-name> [-u <username> -p <password>] -v <vdevid>
-L <tape-library-vid> [-M <export-mode>] -b | -B <barcode> | -l <slot-no>
[-j <job-description>] [-f] [-X <rpc-timeout>]

sudo  iscon exportvirtualtape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--vdevid=<vdevid> --tape-library-vid=<tape-library-vid>
[--export-mode=<export-mode>] --same-barcode | --barcode=<barcode> | --slot-no=<slot-no>
[--job-description=<job-description>] [--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command exports the information from a virtual tape to a physical tape.

-v (--vdevid) is required to specify the ID of the virtual tape to be exported to the physical tape.

-L (--tape-library-vid) is also required to specify the ID of the target physical tape library.

-M (--export-mode) is an option with one of the following values: *copy (default)* or *move*.

One of the three export methods below is required to select the physical tapes:
- -b (--same-barcode) is the option to select a physical tape with the same barcode of the virtual tape if a physical tape with the same barcode exists.
- -B (--barcode) is the option to specify the barcode of an available physical tape in the physical tape library.
- -l (--slot-no) is the option to specify the slot number of an available physical tape in the physical tape library.

-j (--job-description) is an option to specify a description for the tape export job.

-f (--force) is required when the tape is scheduled to be deleted.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Replication

This section describes information on replication commands.

Create a replica

```
sudo  iscon createreplication -s <server-name> [-u <username> -p <password>]
-v <source-vdevid> -S <target-name> [-U <target-username> -P <target-password>]
[-w <watermark> [-r <watermark-retry>]] [-T <hh>] [-i <#[H|M]>]
[-c <on>] [-e <on>] [-f] [-X <rpc-timeout>]
```

```
| sudo  iscon createreplication --server-name=<server-name>
| [--server-username=<username> --server-password=<password>]
| --source-vdevid=<source-vdevid> --target-name=<target-name>
| [--target-username=<target-username> --target-password=<target-password>]
| [--watermark=<watermark> [--watermark-retry=<watermark-retry>]]
| [--replication-time=<hh>] [--interval=<#[H|M]> [--compression=<on>]
| [--encryption=<on>] [--force] [--rpc-timeout=<rpc-timeout>]
```

| **Description:**

| This command allows you to set up a replication configuration.

| -v (--source-vdevid) is required to specify the ID of the virtual tape to be configured for replication.

| -S (--target-name) is required to specify the target server name.

| -U (--target-username) and -P (--target-password) are optional for connection and login to the target server
| if the target server are not logged in with a login command.

| -w (--watermark), -r (--watermark-retry), -T (replication-time), and -i (--interval) are options for replication
| policy.

| Replication will be triggered based on one or more of the three policies:
| • Watermark in MB with watermark retry in minutes. The default is 30 minutes if watermark is specified.
| For example, *-w 50 -r 30, --watermark=50 --watermark-retry=30*
| • Replication time in hh:mm. For example, *-T 12:00, --replication-time=12:00*
| • Replication interval in Hours(H) or Minutes(M). For example, *-i 2H, -i 120M, --interval=2H,*
| *--interval=120M*

| The default policy is to replicate at 12:00 every day if none of the policies are specified.

| -c (--compression) is an option to enable or disable compression with one of the values: *on* or *off*.

| -e (--encryption) is an option to enable or disable encryption with one of the values: *on* or *off*.

| -f (--force) option is required when the tape is scheduled to be deleted. The deletion schedule for the
| virtual tape will be removed and the replication will be configured.

| -X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout.
| The system will retry the command for the amount of time specified if the server does not respond. The
| default RPC timeout is 30 seconds if it is not specified.

| Promote a replica

```
| sudo  iscon promotereplica -s <server-name> [-u <username> -p <password>]
| -v <vdevid> | -S <target-name> [-U <target-username> -P <target-password>]
| -v <replicaid> [-f] [-X <rpc-timeout>]
|
| sudo  iscon promotereplica --server-name=<server-name>
| [--server-username=<username> --server-password=<password>]
| --vdevid=<vdevid> | --target-name=<target-name> [--target-username=<target-username>
| --target-password=<target-password>] --replicaid=<replicaid> [--force]
| [--rpc-timeout=<rpc-timeout>]
```

| **Description:**

This command allows you to promote a replica to a regular virtual device if the primary disk is available and the replica disk is in a valid state.

-v (--vdevid) is the ID of the source virtual tape and -v (--replicaid) is the ID of the tape replica.

Either the primary server with the source virtual tape or the target server with the tape replica can be specified for promotion, but not both.

If the source virtual tape is still valid and available, and the tape replica is in an invalid state, the tape replica can be promoted with the force option. But, it is recommended to synchronize the tape replica with the source virtual tape first unless the source virtual tape is physically defective or unavailable.

If the source virtual tape is no longer available, the tape replica can be promoted with the force option even when it is in invalid state if you are sure the data on the tape replica is useful.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Remove replication

```
sudo  iscon removereplication -s <server-name> [-u <username> -p <password>]
-v <vdevid> | -S <target-name> [-U <target-username> -P <target-password>]
-v <replicaid> [-f] [-X <rpc-timeout>]

sudo  iscon removereplication --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--vdevid=<vdevid> | --target-name=<target-name> [--target-username=<target-username>
--target-password=<target-password>] --replicaid=<replicaid>
[--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to remove the replication configuration from the primary disk on the primary server and delete the replica disk on the target server. Either primary server with source virtual tape or the target server with the tape replica can be specified, but not both.

-v (--vdevid) is the ID of the source virtual tape and -v (--replicaid) is the ID of the tape replica.

If the target server no longer exists or cannot be connected to, only the replication configuration on the primary server will be removed.

If the primary server no longer exists or cannot be connected to, only the tape replica will be deleted.

-f (--force) option has to be specified when either the primary server or target server no longer exists or cannot be connected.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Suspend replication

```
sudo  iscon suspendreplication -s <server-name> [-u <username> -p <password>]
-v <vdevid> [-X <rpc-timeout>]
```

```
| sudo  iscon suspendreplication --server-name=<server-name>
| [--server-username=<username> --server-password=<password>] --vdevid=<vdevid>
| [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to suspend scheduled replications for a virtual device that will be triggered by your replication policy. It will not stop a replication that is currently in progress.

-v (--source-vdevid) is the ID of the source virtual tape on the primary server to be suspended.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Resume replication

```
| sudo  iscon resumereplication -s <server-name> [-u <username> -p <password>]
| -v <vdevid> [-X <rpc-timeout>]
|
| sudo  iscon resumereplication --server-name=<server-name>
| [--server-username=<username> --server-password=<password>] --vdevid=<vdevid>
| [--rpc-timeout=<rpc-timeout>]
|
```

Description:

This command allows you to resume replication for a virtual device that was suspended by the suspendreplication command. The replication will then be triggered by the replication policy once it is resumed.

-v (--source-vdevid) is the ID of the source virtual tape on the primary server to be resumed.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Set replication properties

```
| sudo  iscon setreplicationproperties -s <server-name> [-u <username> -p <password>]
| -v <source-vdevid> [-w <watermark> [-r <watermark-retry>]]
| [-T <hh>] [-i <#[H|M]>] [-c <on>] [-e <on>] [-X <rpc-timeout>]
|
| sudo  iscon setreplicationproperties --server-name=<server-name>
| [--server-username=<username> --server-password=<password>]
| --source-vdevid=<source-vdevid> [--watermark=<watermark>
| [--watermark-retry=<watermark-retry>]] [--replication-time=<hh>]
| [--interval=<#[H|M]>] [--compression=<on>] [--encryption=<on>]
| [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to set the replication policy for a virtual device configured for replication.

-v (--source-vdevid) is required to specify the ID of the source virtual tape.

-w (--watermark), -r (--watermark-retry), -T (replication-time), and -i (--interval) are options for replication policy.

Replication will be triggered based on one or more of the three policies:

- Watermark in MB with watermark retry in minutes. The default is 30 minutes if watermark is specified. For example, *-w 50 -r 30, --watermark=50 --watermark-retry=30*
- Replication time in hh:mm. For example, *-T 12:00, --replication-time=12:00*
- Replication interval in Hours(H) or Minutes(M). For example, *-i 2H, -i 120M, --interval=2H, --interval=120M*

At least one of the properties has to be specified.

To unset the watermark, specify **0** for the watermark. To unset the replication time, specify **NA** instead of the time. To unset the interval, specify **0** for the interval.

The watermark retry value will be ignored if the watermark is not set.

-c (--compression) is an option to enable or disable compression with one of the values: *on* or *off*.

-e (--encryption) is an option to enable or disable encryption with one of the values: *on* or *off*.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Get replication properties

```
sudo  iscon getreplicationproperties -s <server-name> [-u <username> -p <password>]
-v <source-vdevid> [-X <rpc-timeout>]

sudo  iscon getreplicationproperties --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--source-vdevid=<source-vdevid> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to get the replication properties for a virtual device configured for replication.

-v (--source-vdevid) is required to specify the ID of the source virtual tape.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Get replication status

```
sudo  iscon getreplicationstatus -S <target-name> [-U <username> -P <password>]
-v <replicaid> [-X <rpc-timeout>]

sudo  iscon getreplicationstatus --target-name=<target-name>
[--target-username=<username> --target-password=<password>]
--replicaid=<replicaid> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command shows the replication status.

-S (--target-name) is the target server and -v (--replicaid) is ID of the tape replica, both of which are required.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Start replication

```
sudo  iscon startreplication -s <server-name> [-u <username> -p <password>]
-v <vdevid> [-X <rpc-timeout>]

sudo  iscon startreplication --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--vdevid=<vdevid> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to start replication on demand for a virtual device.

-v (--source-vdevid) is the ID of the source virtual tape on the primary server to start.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Stop replication

```
sudo  iscon stopreplication -s <server-name> [-u <username> -p <password>]
-v <vdevid> [-X <rpc-timeout>]

sudo  iscon stopreplication --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
-vdevid=<vdevid> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to stop the replication that is in progress for a virtual device.

-v (--source-vdevid) is the ID of the source virtual tape on the primary server to stop.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Physical devices

This section describes physical device command lines.

Get physical device information

```
sudo  iscon getpdevinfo -s <server-name> [-u <username> -p <password>]
[-F [-M | -C <category>] | [-a] [-A] [-I <ACSL>] ] [-o <output-format>]
[-X <rpc-timeout>]
```

```
sudo  iscon getpdevinfo --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--config [--include-system-info | --category=<category>] |
[--allocated-list] [--available-list] [--scsiaddress=<ACSL>] ]
[--output-format=<output-format>] [--rpc-timeout=<rpc-timeout>]
```

Description:

-F (--config) is an option to get the physical device configuration information. The default is to exclude the system device information.

-M (--include-system-info) is an option to include the system device information.

-C (--category) is an option to be used as a filter to get the configuration information for the specified category with one of the values: *virtual (default)* or *service-enabled* or *direct*.

The -M (--include-system-info) and -C (--category) options are mutually exclusive.

-o (--output-format) is the option to specify the output format. The `<output-format>` for the -F (--config) option is one of the following values: *list* or *detail* or *guid* or *scsi*.

-a (--allocated-list) is an option to get the allocated physical device information.

-A (--available-list) is an option to get the available physical device information.

-I (--scsiaddress) is an option to specify the SCSI address as a device filter in the following format: *`<ACSL>`=#:#:#:# (adapter:channel:id:lun)*

The `<output-format>` for the -a (--allocated-list) and the -A (--available-list) options is one of the following values: *list* or *detail* or *size-only*.

-F (--config), and -a (--allocated-list) and/or -A (--available-list) are mutually exclusive. You can either get the configuration information or get the allocation information. When getting the allocation information, you can specify either -a (--allocated-list), or -A (--available-list) or both. The default is to display both the device allocation and availability information if none of the options is specified.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Rescan physical devices

```
sudo  iscon rescandevices -s <server-name> [-u <username> -p <password>]
[-a <adapter-range>] [-i <scsi-range>] [-l <lun-range>] [-L] [-X <rpc-timeout>]

sudo  iscon rescandevices --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--adapter-range=<adapter-range>] [--scsi-range=<scsi-range>] [--lun-range=<lun-range>]
[--sequential] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to rescan the physical resource(s) on the specified server to get the proper physical resource configuration.

-a (--adapter-range) is the adapter or adapter range to be rescanned. The default is to rescan all the adapters if it is not specified. For example, e.g. *-a 5 or -a 5-10*

-i (--scsi-range) is the starting SCSI ID and ending SCSI ID to be rescanned. The default is to rescan all the SCSI IDs if the range is not specified. For example, e.g. *-i 0-5*

-l (--lun-range) is the starting LUN and ending LUN to be rescanned. The default is not to rescan any LUN if it is not specified. For example, e.g. *-l 0-10*

If you want the system to rescan the device sequentially, you can specify the –L (--sequential) option. The default is not to rescan sequentially.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Import disk

```
sudo  iscon importdisk -s <server-name> [-u <username> -p <password>]
-i <guid> | -I  <ACSL> [-X <rpc-timeout>]

sudo  iscon importdisk --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--scsiaddress= <ACSL> | --guid=<guid> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to import a foreign disk to the specified server. A foreign disk is a virtualized physical device containing TS7500 Virtualization Engine logical resources previously set up on a different TS7520 Server. If the previous server is no longer available, the disk can be set up on a new TS7520 Server and the resources on the disk can be imported to the new server to make them available to clients.

The `<guid>` is the unique identifier of the physical device. `<ACSL>` is the SCSI address of the physical device in the following format: *#:#:#:# (adapter:channel:scsi id:lun)*

Either -i (--guid) or -I (--scsiaddress) has to be specified.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Prepare physical device for the TS7520 Server

```
sudo  iscon preparedisk -s <server-name> [-u <username> -p <password>]
[-U <target-username> -P <target-password>] -i <guid> | -I <ACSL>
-C <category> [-N <new-guid>] [-X <rpc-timeout>]

sudo  iscon preparedisk --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--target-username=<username> --target-password=<password>]
--scsiaddress=<ACSL> | --guid=<guid> --category=<category> [--new-guid=<new-guid>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to prepare a physical device to be used by a TS7520 Server or reserve a physical device for other usage.

The `<guid>` is the unique identifier of the physical device. `<ACSL>` is the SCSI address of the physical device in the following format: *#:#:#:# (adapter:channel:scsi id:lun)*

Either -i (--guid) or -I (--scsiaddress) has to be specified.

-C (--category) is the required to specify the new category for the physical device in one of the following values: unassigned or virtual or direct or service-enabled.

-N (--new-guid) is an option to specify the new guid for the physical device if the new category is ″virtual″.

If the server is set up for failover, the failover partner has to be rescanned after the disk preparation.

`<target-username>` and `<target-password>` are options to specify the user name and password for the failover partner.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Failover

This section describes Failover commands.

Get Failover status

```
sudo  iscon getfailoverstatus -s <server-name> [-u <username> -p <password>] [-X <rpc-timeout>]

sudo  iscon getfailoverstatus --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command shows you the current status of your failover configuration. It also shows all Failover settings, including which IP addresses are being monitored for failover. Failover status can be obtained from either the failover primary server or the failover secondary server.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Suspend Failover

```
sudo  iscon suspendfailover -s <server-name> [-u <username> -p <password>] [-X <rpc-timeout>]

sudo  iscon suspendfailover --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command suspends your failover configuration. Failover can only be suspended from the secondary failover server. Specify the secondary server name or IP address to suspend failover.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Resume Failover

```
sudo  iscon resumefailover -s <server-name> [-u <username> -p <password>] [-X <rpc-timeout>]

sudo  iscon resumefailover --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command resumes a suspended failover configuration. Failover can only be resumed from the secondary failover server. Specify the secondary server name or IP address to resume failover.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Start takeover

```
sudo  iscon starttakeover -s <server-name> [-u <username> -p <password>] [-f]
[-X <rpc-timeout>]

sudo  iscon starttakeover --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--force]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command initiates failover to the secondary server in a failover configuration. Takeover can only be performed from the secondary failover server. Specify the secondary server name or IP address to start failover.

Auto recovery will not take effect when the failover primary server is taken over manually. If auto recovery is set, the -f (-force) option is required to start takeover.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Stop takeover

```
sudo  iscon stoptakeover -s <server-name> [-u <username> -p <password>] [-X <rpc-timeout>]

sudo  iscon stoptakeover --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command initiates failback in a failover configuration. This operation can only be performed from the secondary failover server. Specify the secondary server name or IP address to stop. -

X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Server configuration

This section describes server configuration commands.

Save configuration

```
sudo  iscon saveconfig -s <servername> [-u <username> -p <password>]
[-o <filename>] [-f] [-X <rpc-timeout>]

sudo  iscon saveconfig --server-name=<servername>
[--server-username=<username> --server-password=<password>] [--output-file=<filename>]
[--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command saves the configuration of your TS7520 Server. You should save the configuration any time you change it, including any time you add/change/delete a client or resource, or assign a client.

-o (--output-file) is the full path of the file name to save the configuration to.

The default output filename is: *config-YYYY-MM-DD-hh-mm-<servername>.tar.gz* if the file name is not specified. Specify -f (--force) option if you want to overwrite the existing file when the output file already exists. Otherwise, an error will be returned.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Restore configuration

```
sudo  iscon restoreconfig -s <server-name> [-u <username> -p <password>]
-i <filename> [-X <rpc-timeout>]

sudo  iscon restoreconfig --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--input-file=<filename> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command restores the configuration of your TS7520 Server. Specify the configuration file name that was saved with saveconfig command.

Restoring a configuration overwrites existing virtual device and client configurations for that server. TS7500 Virtualization Engine partition information will not be restored. This feature should only be used if your configuration is lost or corrupted.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Event Log

This section describes commands for getting the Event Log.

Get Event Log

```
sudo  iscon geteventlog -s <server-name> [-u <username> -p <password>]
[-D <date-range>] [-F <fileFormat>] [-o <filename>] [-H] [-f] [-X <rpc-timeout>]

sudo  iscon geteventlog --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--date-range=<date-range>]
[--file-format=<fileFormat>] [--include-heading] [--output-file=<filename>] [--force]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command gets the event log.

-D (--date-range) is the starting date/time and ending date/time in the following format:
YYYYMMDDhhmmss-YYYYMMDDhhmmss or *YYYYMMDDhhmmss*

-F (--fileFormat) is one of the following formats: csv (default) or txt.

-H (--include-heading) is the option to include the event log data heading.

-o (--output-file) is the full path of the file name to save the event log data. If output filename is not
specified, the default filename is: *eventlogYYYY-MM-DD-hh-mm-<server-name>[.#]*

[.#] is the additional suffix when there is a duplicate.

Specify -f (--force) option if you want to overwrite the existing file when the output file already exists.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout.
The system will retry the command for the amount of time specified if the server does not respond. The
default RPC timeout is 30 seconds if it is not specified.

Report data

This section describes report data commands.

Get report data

```
sudo  iscon getreportdata -s <server-name> [-u <username> -p <password>]
[-T <report-type>] [-d <date>] [-I #[D|W|M] ] [-c <client-name> | -C <clientList>]
[-v <vdevid>| -R <resourceList>] [-N] [-o <outputFilename>] [-F <fileFormat>] [-H] [-f]
[-X <rpc-timeout>]

sudo  iscon getreportdata --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--report-type=<report-type>] [--date=<date>] [--units=[D|W|M.] ] [--no-system-info]
[--client-name=<client-name> | --client-list=<clientList>]
[--vdevid=<vdevid> | --resource-list=<resourceList>] [--include-heading]
[--file-format=<fileFormat>] [--output-file=<outputFilename>] [--force]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to get report data from the specified server and save the data to an output file in csv or text file format.

-T (--report-type) is an option to specify the report type with one of the following values: *ServerThroughputReport* (default) or *ClientThroughputReport* or *ResourceThroughputReport*.

-d (--date) is an option to specify the date in the format of *YYYYMMDD*. The default is today's date.

The time units can be specified in three different units:
- D = Day
- W = Week
- M = Month

-c (--clientName) is required for the *ClientThroughputReport*.

-v (--vdevId) is required for the *ResourceThroughputReport*.

-R (--resource-list) can be either a list of resource IDs separated by commas, or "*" for all the resources, or a filename of a file enclosed in <> containing resource ID in each line. Two examples:
- -R 1,3,5,10
- -R "<res_id_file.txt>"

For the *ClientThroughputReport*, only the resources assigned to the client can be specified.

-C (--clientList) can be either a list of client names separated by commas, or "*" for all the clients, or a filename of a file enclosed in <> containing client name in each line. Two examples:
- -C client1,client2
- -C "<client_file.txt>"

For the *ResourceThroughputReport*, only the clients assigned to the resource can be specified.

System information include Memory and CPU usage information on the server, the default is to include the system information for the *ServerThroughputReport*. The information will not be included for the *ClientThroughputReport*.

-N (--no-system-info) allows you to exclude the information. -N can only be specified for the *ServerThroughputReport*.

-H (--include-heading) is the option to include the data heading.

-F (--fileFormat) is one of the following: csv (default) or txt.

-o (--output-file) is the full path of the file name to save the report data to. If output filename is not specified, the default filename is: *ServerThroughputYYYY-MM-DD[.#]*

[.#] is the additional suffix when there is a duplicate.

Specify -f (--force) option if you want to overwrite the existing file when the output file already exists.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Appendix B. Error codes

This document describes the error codes for the TS7500 Virtualization Engine Software Version 2 Release 1.

Table 11. TS7500 Virtualization Engine Software Version 2 Release 1 error codes

Error Code	Type	Text	Probable Cause	Customer Action
1005	Error	Out of kernel resources. Failed to get major number for CVT SCSI device. **Note:** *CVT* stands for *Centralized Virtual Tape*, an IBM-internal term for the TS7500 Virtualization Engine.	Too many Linux device drivers installed.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
1006	Error	Failed to allocate memory.	Memory leak from various modules in the Linux OS, most likely from network adapter or other third party interface drivers.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
1008	Error	Failed to set up the network connection due to an error in SANRPCListen -- [Error].	Another application is using UDP port 11577.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
1023	Error	Failed to connect to physical device [Device number]. Switching to alias to [ACSL].	Adapter or cable problem.	Check for loose or damaged cable on affected drive.
1030	Error	Failed to start replication -- replication is already in progress for virtual tape.	Replication is still in progress when a new replication is manually triggered by a user or started by the scheduler based on the replication policy.	If the replication is manually triggered by the user, check the replication status at the right panel of the replica before starting another replication. If the replication is triggered by the scheduler, adjust the schedule in the replication policy to avoid replicating too often.

Error Code	Type	Text	Probable Cause	Customer Action
1043	Error	A SCSI command terminated with a non-recoverable error condition that was most likely caused by a flaw in the medium or an error in the recorded data.	Most likely caused by a flaw in the medium or an error in the recorded data.	Check the system log for additional information. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
1044	Error	A SCSI command terminated with a non-recoverable hardware failure (for example, controller failure, device failure, parity error, and so on). Please check the system log for additional information.	General I/O error that is not medium related. This can be caused by a number of potential failures, including controller failure, device failure, parity error, and so on	Check the system log for additional information. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
1061	Warning	I/O path failure detected. Alternate path will be used. Failed path (A.C.S.L): [ACSL]; New path (A.C.S.L): [ACSL].	An alias is in use due to primary path failure.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
1067	Error	Replication cannot proceed -- unable to connect to replica server.	The primary server cannot connect to the target server. Either there's problem with the network or the target server is busy.	Check if the network is working properly as well as the server activity. If the replication is triggered by the user, wait until the network is working properly or when the server is not as busy. If the replication is triggered by the scheduler, next replication will be started at the next scheduled time. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/

Error Code	Type	Text	Probable Cause	Customer Action
1069	Error	Replication cannot proceed -- virtual tape %1 no longer has a replica or the virtual tape replica does not exist.	The replica of the virtual tape no longer exists on the target server. It might have been removed from the target server while the primary server is not available.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
1084	Error	A SCSI command terminated with a recovered error condition. This may indicate that the device is becoming less reliable. Please check the system log for additional information.	The physical devices, that is, the SCSI disks or the RAID, returned an error code reporting that the I/O operation initially encountered an error, but was successful after a retry. This may indicate the reliability of the storage device may be questionable.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
10001	Error	Insufficient privilege (uid: [UID]).	TS7520 software is not running with root privilege.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
10002	Error	TS7520 Server environment is corrupt.	The configuration file in the /etc directory which provides the TS7520 home directory and other environmental information is either corrupted or deleted.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
10003	Error	Failed to initialize configuration [File name].	During the initialization process, one or more critical processes experienced a problem. This may be due to system drive failure, storage hardware failure, or system configuration corruption.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/

Table 11. TS7500 Virtualization Engine Software Version 2 Release 1 error codes (continued)

Error Code	Type	Text	Probable Cause	Customer Action
10004	Error	Failed to get SCSI device information.	Error occurred when adding newly discovered the SCSI devices to the system. Most likely due to unreliable storage connectivity, hardware failure, or low system resources.	Check the storage devices for power status, controller status, and so on. Check for proper connectivity. Fibre Channel Switch connection status lights do not guarantee a solid connection. Disconnect and reconnect the Fibre Channel connector for verification. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
10006	Error	Failed to write configuration [File name].	Error encountered when writing the TS7520 configuration file to the system drive. This can only happen if the system drive ran out of space, is corrupted, or encountered a hardware failure.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
10100	Error	Failed to scan new SCSI devices.	Error occurred when adding newly discovered SCSI devices to the system. Most likely due to unreliable storage connectivity, hardware failure, or low system resources.	See 10004.
10101	Error	Failed to update configuration [File name].	Error encountered when updating the TS7520 configuration file on the system drive. This can only happen if the system drive is corrupted or has failed.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/

Table 11. TS7500 Virtualization Engine Software Version 2 Release 1 error codes (continued)

Error Code	Type	Text	Probable Cause	Customer Action
10102	Error	Failed to add new SCSI devices.	Error occurred when adding newly discovered the SCSI devices to the system. Most likely due to unreliable storage connectivity, hardware failure, or low system resources.	See 10004.
10200	Warning	Configuration [File name] exists.	A TS7520 configuration file already exists when installing the TS7520 software, possibly from previous installation. The configuration file will be reused.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
10210	Warning	Marked virtualized PDev [GUID] OFFLINE, guid does not match SCSI guid [GUID].	A physical device has a different GUID written on the device header than the record in the configuration file. This is most likely caused by old drives being imported without proper initialization, or much unlikely, due to the corruption of the configuration or the device header.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
10212	Warning	Marked PDev [GUID] OFFLINE because scsi status indicate OFFLINE.	The physical storage system response indicates the specific device is off-line. It may have been removed, turned off, or malfunctioning.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
10213	Warning	Marked PDev [GUID] OFFLINE because it was not detected.	The physical device that exists in the configuration is not responding to commands. Its status is now set to OFF-LINE. All virtual drives affected will also be set to OFF-LINE. Most likely the drive or storage system is turned off, or the cable is disconnected, and so on.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/

Error Code	Type	Text	Probable Cause	Customer Action
10214	Warning	Marked PDev [GUID] OFFLINE because its GUID is an invalid FSID.	The GUID in the header of the drive does not match the unique ID, called the FSID, which is based on the external properties of the physical drive. It maybe caused by drives changed while TS7520 is down.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
10215	Warning	Marked PDev [GUID] OFFLINE because its storage capacity has changed.	The physical drive geometry, including the number of sectors, are different from the original record.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
10240	Error	Missing SCSI Alias [A,C,S,L].	One of the existing SCSI path for the device is not accessible. This is most like caused by storage cable being disconnected, or fibre channel switch re-zoning. This can also be caused by failure of one of the storage ports.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
10241	Error	Physical Adapter [Adapter number] could not be located in /proc/scsi/.	The adapter driver could be unloaded.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
10244	Error	Invalid FSID, device [Device ID] LUN in FSID [FSID] does not match actual LUN.	The FSID is generated with the LUN of the device. Once a device is used by TS7520, it is not allowed to have the LUN changed.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
10246	Error	Fail to generate FSID for device acsl:[A C S L], can't validate FSID.	The physical drive does not present valid data for unique ID generation, even the inquiry pages exist.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/

Table 11. TS7500 Virtualization Engine Software Version 2 Release 1 error codes (continued)

Error Code	Type	Text	Probable Cause	Customer Action
10247	Error	Device (acsl:[A C S L]) GUID is blank, can't validate FSID.	Some process may have erased the disk header. This can be due to the accidental erase by fdisk.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11000	Error	Failed to create socket.	This kind of problem should rarely happen. If it does, it may indicate network configuration error, possibly due to system environment corruption. It is also possible that the network adapter failed or is mis-configured. It is also possible that the network adapter driver is the problem.	Restart the network. If problem persists, call 1-800-IBM-SERV for software support services within the US. Outside the US, please see http://www.ibm.com/ planetwide/
11001	Error	Failed to set socket to re-use address.	System network configuration error, possibly due to system environment corruption.	See 11000.
11002	Error	Failed to bind socket to port [Port number].	System network configuration error, possibly due to system environment corruption.	See 11000.
11003	Error	Failed to create TCP service.	System network configuration error, possibly due to system environment corruption.	See 11000.
11004	Error	Failed to register TCP service (program: [Program name], version: [Version number]).	System network configuration error, possibly due to system environment corruption.	See 11000.
11006	Error	TS7520 communication module Failed to start.	Most likely due to the port for TS7520 comm module is being occupied by a previous unexpected failure of the communication module, or by another application.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/

Error Code	Type	Text	Probable Cause	Customer Action
11032	Error	Auto save configuration: cannot connect to ftp server port.	FTP sever is not accessible.	Please make sure that FTP server is running and accessible from TS7520 system. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
11033	Error	Auto save configuration: cannot login user.	Incorrect user name or password	Please double check the user name and password. settings. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
11034	Error	Auto save configuration: directory doesn't exist.	The target directory specified in the auto save configuration setting doesn't exist on the FTP server.	Please create the specified directory or use an existing directory. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
11035	Error	Auto save configuration: failed to copy to ftp server.	The specified FTP user may not have write access to copy files. It can also happen if the FTP server doesn't have enough space.	Please check the user access rights for the FTP user specified in the auto save configuration setting. Also check the free space available on the FTP server. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/

Table 11. TS7500 Virtualization Engine Software Version 2 Release 1 error codes (continued)

Error Code	Type	Text	Probable Cause	Customer Action
11036	Error	Auto save configuration: failed to delete old file from ftp server.	The specified user doesn't have rights to delete files on the FTP server.	Please check the access rights of the specified user. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11101	Error	SAN Client ([host name]): Failed to add SAN Client.	This error is most likely due to system configuration error, or system resources running low.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11104	Error	Too many SAN Client connections	The number of simultaneous connections exceeded the supported limit the current system resource can handle.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11112	Error	SAN Client ([host name]): Failed to parse configuration file [File name].	The configuration file is corrupted, or manually tempered to the degree that is no longer recognizable by TS7520. If corruption is the cause, then it is most likely due to a system drive hardware error.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11114	Error	SAN Client ([host name]): Failed to allocate memory.	System resources are running low. This may be due to too little memory installed for the system, or a runaway process that is consuming too much memory.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11201	Error	Too many Console connections.	Too many TS7520 console processes are connected to the particular TS7520 server. This is a highly unlikely condition.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/

Error Code	Type	Text	Probable Cause	Customer Action
11202	Error	Console ([host name]): Illegal access.	The TS7520 console host attempts to perform operation outside of the granted privilege level. This almost never happens. If it does, it is either due to a retry operation from an unexpectedly terminated connection that was assigned a different privilege level, or it is a deliberate break-in attempt by reverse engineering of TS7520 console software, which as indicated by this error message, is not feasible.	See 11107.
11203	Error	Console ([host name]): SCSI device re-scanning has failed.	Error occurred when adding newly discovered the SCSI devices to the system. Most likely due to unreliable storage connectivity, or hardware failure, or system resource is running low.	See 10100.

Error Code	Type	Text	Probable Cause	Customer Action
11204	Error	Console ([host name]): SCSI device checking has failed.	Error occurred when accessing the SCSI devices when console requests the server to check the known storage devices. Most likely due to storage connectivity failure or hardware failure.	Check the storage devices, for example, power status; controller status, and so on. Check the connectivity, for example, cable connectors. In fibre channel switches, even the connection status light indicates the connection is good, it is still not a guarantee. Disconnect and reconnect the connector to make sure. Within the US, call 1-800-IBM-SERV for hardware support services. Outside the US, please see http://www.ibm.com/planetwide/
11209	Error	Console ([host name]): Insufficient privilege access.	A 'read only' user attempts to do an operation that requires configuration change.	Log in as administrator user if configuration changes need to be made. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
11211	Error	Console ([host name]): Failed to save file [filename].	Error encountered when writing the TS7520 configuration file to the system drive. This can only happen if the system drive ran out of space, or is corrupted, or if there is hardware failure in the system drive.	See 10006.

Error Code	Type	Text	Probable Cause	Customer Action
11212	Error	Console ([host name]): Failed to create index file [file name] for Event Log.	Failed to create an index file for the event log retrieval. Most likely due to insufficient system disk space.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11216	Error	Console ([host name]): Out of system resources. Failed to fork process.	The TS7520 server is low in memory resource for normal operation.	See 11114.
11219	Error	Console ([host name]): Failed to add virtual device [Device number].	Failed to create a virtual drive due to either system configuration error, or storage hardware failure, or system resource access failure.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11233	Error	Console ([host name]): Failed to map the SCSI device name for [A C S L].	The mapping of the SCSI address, namely the adapter, channel, SCSI ID, and lun, (ACSL) is no longer valid. This must be due to sudden failure, or improper removal, or change of storage devices in the TS7520 server.	See 11204. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11234	Error	Console ([host name]): Failed to execute hdparm for [Device number].	Failed to perform the device throughput test for the given device. This can be due to either OS in a bad state such that the program cannot be run, or the storage device failed.	See 11204. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/

Error Code	Type	Text	Probable Cause	Customer Action
11240	Error	Console ([host name]): Failed to start the TS7520 Server module.	When any TS7520 process cannot be started, it is most likely due to insufficient system resources, an invalid state left by TS7520 processes that may not have been stopped properly, or an unexpected OS process failure that left the system in an unstable state. This should happen very rarely. If this frequently occurs, there must be external factors that contributed to the behavior and these must be investigated and removed before running the TS7520 server.	
11242	Error	Console ([host name]): Failed to stop the TS7520 Server module.	When any TS7520 process can not be started, it is most likely due to insufficient system resources, an invalid state left by TS7520 processes that may not have been stopped properly, or an unexpected OS process failure that left the system in an unstable state. This should happen very rarely. If this frequently occurs, there must be external factors that contributed to the behavior and these must be investigated and removed before running the TS7520 server.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11257	Error	Console ([host name]): Failed to add SAN Client ([Host name]).	See 11101.	See 11101.

Table 11. TS7500 Virtualization Engine Software Version 2 Release 1 error codes (continued)

Error Code	Type	Text	Probable Cause	Customer Action
11261	Error	Console ([Host name]): Failed to get SAN Client connection status for virtual device [Device ID].	Failed to inquire a SAN Client connection status due to either system configuration error, or storage hardware failure, or system resource access failure. This should rarely happen.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
11262	Error	Console ([host name]): Failed to parse configuration file [File name].	See 11112.	See 11112.
11263	Error	Console ([host name]): Failed to restore configuration file [File name].	See 10006.	See 10006.
11266	Error	Console ([host name]): Failed to erase partition of virtual device [Device number].	Storage hardware failure.	See 10004.
11278	Error	Console: Failed to swap mirror for repository.	Hardware problem with the repository mirror disk.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
11291	Error	Console ([host name]): Failed to update meta information of physical device [Device number].	Storage hardware failure.	See 10004.
11292	Error	Console ([host name]): Failed to swap IP address from [IP address] to [IP address].	See 11000.	See 11000.
11295	Error	Console ([host name]): Invalid configuration format.	See 11112.	See 11112.
11406	Error	Failed to prepare the failover configuration package.	Suspend failover initiated while packaging failover configuration information.	No action required. (Operation will be retried automatically.)
11407	Error	Failed to extract the failover configuration package.	Suspend failover initiated while packaging failover configuration information.	No action required. (Operation will be retried automatically.)

Error Code	Type	Text	Probable Cause	Customer Action
11500	Error	Out of disk space to expand virtual tape.	There is no more storage space available for expanding a virtual tape.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11512	Error	Console : Failed to add a replica for virtual tape to TS7520 Server (watermark: MB, time: , interval: , watermark retry: , suspended:).	It can be connection error while the primary server is synchronizing the initial status of the virtual tape to the replica on the target server, or the virtual tape is loaded to the drive at the moment by backup software or the console on different machine.	Check if the network is working properly first and correct the problem first if it is. If the virtual tape is moved to the drive, reconfigure the replication later.
11514	Error	Console: Failed to remove the replica for virtual tape from TS7520 Server (watermark: MB, time: , interval: , watermark retry: , suspended:).	Error encountered when writing the updated configuration to the TS7520 configuration file to the system drive. This can only happen if the system drive ran out of space, or is corrupted, or if there is hardware failure in the system drive.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11516	Error	Console: Failed to create the virtual tape replica.	Could not update the virtual tape partition information on disk.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11518	Error	Console: Failed to start replication for virtual tape.	The replication triggered manually by the user failed. It can be due to one of the following reasons. Network problems, Virtual tape is loaded in a drive, replication is in progress or the replica no longer exists.	See actions for corresponding events: 1067, 1030 and 1069.

Error Code	Type	Text	Probable Cause	Customer Action
11522	Error	Console: Failed to promote virtual tape replica to a virtual tape.	Failed to update the virtual tape partition information.	Check if the physical disk is working properly or the server is busy. Retry the operation when the physical disk is working properly or when the server is not busy.
11524	Error	Console ([host name]): Failed to run TS7520 Server X-Ray.	See 11240.	See 11240.
11534	Error	Console ([host name]): Failed to reset the umap for virtual device [Device number].	Storage hardware failure.	See 10004.
11535	Error	Console: Failed to update the replication parameters for virtual tape to TS7520 Server (watermark: MB, time: , interval: , watermark retry: , suspended:).	Error encountered when writing the updated configuration to the TS7520 configuration file to the system drive. This can only happen if the system drive ran out of space, or is corrupted, or if there is hardware failure in the system drive.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11537	Error	Console ([host name]): Failed to claim physical device [Device number].	This may due a specific version of the TS7520 server limiting the support of the storage.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11539	Error	Console ([host name]): Failed to import physical device [Device number].	Storage hardware failure.	See 10004.
11542	Error	Console: Failed to remove virtual tape replica.	Error encountered when writing the updated configuration to the TS7520 configuration file to the system drive. This can only happen if the system drive ran out of space, or is corrupted, or if there is hardware failure in the system drive.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/

Table 11. TS7500 Virtualization Engine Software Version 2 Release 1 error codes (continued)

Error Code	Type	Text	Probable Cause	Customer Action
11554	Error	Console (%1): Failed to set failover option <selfCheckInterval:>	IP Network communication failure.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11569	Error	Console ([host name]): Failed to set [Device number] to Fibre Channel mode [Mode].	This is possibly due to the fibre channel driver being improperly loaded, or the wrong version of the driver is loaded. TS7520 FC target mode requires the IBM TS7520 version of the driver to be used.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11578	Error	Console ([host name]): Failed to get Fibre Channel initiator information.	See 11569.	See 11569.
11632	Error	Console: Failed to set failover option on secondary server <heartbeatInterval: sec, autoRecoveryInterval: sec>.	IP Network communication failure.	Check Network connectivity. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11633	Error	Console : Failed to set failover option on secondary server <heartbeatInterval: sec, autoRecoveryInterval: disabled>.	Same as 11632.	Check Network connectivity. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
11648	Error	Failed to get inquiry string on SCSI device [Device ID].	Hardware problem with SCSI device.	Hardware problem with SCSI device. Check hardware.
11650	Error	Failed to get capacity size for SCSI device [Device ID].	Hardware problem with SCSI device.	Hardware problem with SCSI device. Check hardware.
11651	Error	Medium test failed for SCSI device [Device name].	Hardware problem with SCSI device.	Hardware problem with SCSI device. Check hardware.

Table 11. TS7500 Virtualization Engine Software Version 2 Release 1 error codes (continued)

Error Code	Type	Text	Probable Cause	Customer Action
11652	Error	Could not get type for SCSI device [Device ID] because of inquiry string failure.	Hardware problem with SCSI device.	Hardware problem with SCSI device. Check hardware.
11655	Error	Discarded scsi device [Device ID], bad capacity size.	Hardware problem with SCSI device.	Hardware problem with SCSI device. Check hardware.
11782	Error	Barcode of the source tape already exist on target server. Auto-replication cannot be configured.	A tape with the same barcode exist on the remote sever.	Remove the tape with same barcode from the remote server or change its barcode.
11791	Error	Failed to re-size virtual tape to MB. Error:	Virtual tape partition information couldn't be updated. This could happen in rare cases when the system is extremely busy and updates to disks take too long.	No user action required. Virtual tape partition information couldn't be updated. This could happen in rare cases when the system is extremely busy and updates to disks take too long.
13309	Error	Failed to communicate with the primary server.	Secondary server failed to talk to primary server.	Check network connectivity.
13704	Warning	TS7520 failure detected.	TS7520 secondary server detected software or hardware failure on Primary server. This will trigger a take over operation.	TS7520 secondary server detected software/hardware failure on Primary server. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
13711	Error	The following options are not licensed: [TS7520 option]. Please contact IBM or its representative to purchase a license.	The specific option is not licensed properly.	Contact IBM or representative to obtain proper license.

Error Code	Type	Text	Probable Cause	Customer Action
13800	Warning	lPrimary server failure detected. Failure condition:	TS7520 Primary server detected software or hardware failure on itself. This will trigger a failover operation to secondary server.	TS7520 Primary server detected software or hardware failure on itself. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
13804	Error	Quorum disk failed to release to secondary.	Negotiation through Quorum disk failed.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
13817	Error	Primary server failback operation failed.	Primary server had a software or hardware failure condition during fail back.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
13820	Warning	Primary server heartbeat not detected. Testing network connectivity.	Network communication failure.	Check network connectivity.
13821	Error	Failed to contact other entities in network. Assume failure in secondary side. Failover not initiated.	Network connectivity failure and no connectivity to outside network.	Check network connectivity and the secondary server health. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
13822	Warning	Secondary will not take over because storage connectivity is not 100%.	Storage or Storage connectivity failure on secondary.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/

Error Code	Type	Text	Probable Cause	Customer Action
13828	Warning	Almost running out of file handler (current [Number of handles], max [Number of handles]).	The Linux system is running out of resource for file handles.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
13829	Error	Almost running out of memory (current [Number of KB] K, max [Number of KB]).	The Linux system is running out of memory.	See 13828.
13830	Error	Failed to get configuration file from storage.	Failed to access storage LUN where the repository is located during recovery process.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
15055	Error	Server ioctl call [Device ID] failed on vdev id [Device ID]: Device or resource is busy (EBUSY).	The virtual drive is busy with I/O and is not responsive to the upper layer calls.	Try again when the system is less busy. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
19004	Warning	Allocate space at MB has reached the threshold of the total capacity.	Storage utilization has reached limit specified by user.	Check Storage utilization and delete unused virtual tapes to free up space or add more storage.
19057	Error	[Remote Copy] Copying of the virtual tape to the remote server cannot proceed -- unable to connect to remote server.	Replication configured using remote copy failed due to network problem.	See 1067.
19065	Error	[Remote Copy] Copying of the virtual tape to the remote server cannot proceed -- virtual tape is in the drive.	Virtual Tape is moved to the tape drive while remote copy processing started.	Remove the replication setup configured through remote copy. Reconfigure remote copy when the virtual tape is moved to the vault or slot.
40002	Error	Block list full on tape.	Too many very small sized blocks (< 512 bytes) have been written to tape.	Increase the block size used by backup application.

Error Code	Type	Text	Probable Cause	Customer Action
40010	Error	Attach to tape failed.	A physical device is not available.	Check the storage device connectivity and make sure that the software can access the devices. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
40011	Error	Failed to read from Virtual Tape.	The storage LUN where the virtual tape is stored cannot be accessed.	Check the storage LUN where the virtual tape is located. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
40013	Error	Export Tape failed, not enough memory.	System is running low on memory. May be because too many concurrent operations are in process.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
40014	Error	Read tape info failed.	The storage LUN where the virtual tape is stored cannot be accessed.	Check the storage LUN where the virtual tape is located. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
40015	Error	Export tape failed, unsupported block size.	Backup application has used an unsupported block size on virtual tape. 1MB is currently the max block size supported.	Change backup application configuration to use smaller block size. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/

Error Code	Type	Text	Probable Cause	Customer Action
40017	Error	Failed to write to Physical Tape.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40018	Error	Failed to load Physical Tape.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40019	Error	Failed to write to Virtual Tape.	The storage LUN where the virtual tape is stored cannot be accessed.	Check the storage LUN where the virtual tape is located. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40022	Error	Failed to get Physical Tape block size.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40023	Error	Import failed, not enough memory.	System is running low on memory. May be because too many concurrent operations are in process.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40030	Error	Failed to read from repository	The storage LUN where the repository is located cannot be accessed.	Check the LUN where the repository is located. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/

Table 11. TS7500 Virtualization Engine Software Version 2 Release 1 error codes (continued)

Error Code	Type	Text	Probable Cause	Customer Action
40031	Error	Failed to write to repository.	The storage LUN where the repository is located cannot be accessed.	Check the LUN where the repository is located. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40032	Warning	Physical Tape not available to start export job in lib.	There is an import or export job in the queue waiting for a physical tape.	Insert tapes with appropriate barcodes in the physical library and perform an inventory operation.
40039	Error	Read Element command to Physical Library failed.	There is a hardware problem with the physical tape library.	Check with the tape library vendor. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40043	Error	Move Medium command failed in Physical Library.	There is a hardware problem with the physical tape library.	Check with the tape library vendor. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40044	Error	Unload command failed on Physical Tape Drive.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/

Error Code	Type	Text	Probable Cause	Customer Action
40045	Error	Read from Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40046	Error	Write to Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40047	Error	Write File Mark to Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40048	Error	Mode sense command to Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40049	Error	Mode select command to physical device failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/

Table 11. TS7500 Virtualization Engine Software Version 2 Release 1 error codes (continued)

Error Code	Type	Text	Probable Cause	Customer Action
40050	Error	Rewind command to Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40051	Error	Inquiry command to Physical device failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40065	Error	Read data from Virtual Tape failed.	The storage LUN where the virtual tape is located cannot be accessed.	Check the LUN where the virtual tape is located. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40066	Error	Write data to Virtual Tape failed.	The storage LUN where the virtual tape is located cannot be accessed.	Check the LUN where the virtual tape is located. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/

Error Code	Type	Text	Probable Cause	Customer Action
40069	Error	Cannot expand Tape.	Not enough storage space is available to expand a virtual tape.	Add more storage space to the system or free up space by deleting virtual tapes that are no longer required. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40074	Error	Export to Physical Tape failed.	Check the event log messages prior to this message for the exact reason for the failure.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40076	Error	Import Physical Tape failed.	Check the event log messages prior to this message for the exact reason for the failure.	Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40077	Error	Import Physical Tape failed. Duplicate Virtual Tape Barcode.	A virtual tape with the same barcode already exists in the virtual library.	Duplicate barcodes in a system are not allowed. Delete the existing tape or use a different barcode while importing.
40078	Error	Import Physical Tape failed. Duplicate Virtual Tape Barcode.	A virtual tape with the same barcode already exists in the virtual library.	Duplicate barcodes in a system are not allowed. Delete the existing tape or use a different barcode while importing.
40085	Error	Init Element Status command failed on Physical Library, Error.	Physical Library hardware problem.	Check physical library hardware. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/planetwide/

Error Code	Type	Text	Probable Cause	Customer Action
40086	Error	Write command to Configuration Repository Failed. Please check repository LUNs.	Storage or Storage connectivity problems.	Check Storage and Storage connectivity. Within the US, call 1-800-IBM-SERV for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
40089	Warning	The direct link tape has been deleted.	The physical tape linked with this direct link does not exist.	Check the physical library/drive connectivity.
40090	Error	Failed to load tape because it is a cleaning tape.	A cleaning tape was selected for import/export job.	Select a non-cleaning tape for the import/export job.
40091	Error	Write command to Configuration Repository failed.	There is a storage or storage connectivity problem.	Check storage connection and retry operation. If problem persists, call 1-800-IBM-SERV within the US for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
40093	Error	Failed to reclaim the tape in the library.	Check the event log messages prior to this message for the exact reason for the failure.	Check the suggested action for the error message that occurred prior to this message.
40095	Error	Failed to reclaim the tape in the vault.	Check the event log messages prior to this message for the exact reason for the failure.	Check the suggested action for the error message that occurred prior to this message.
40097	Warning	Unable to renew cache tape. Data will be written to physical tape.	There is not enough available storage to create a cache tape.	Delete unused tapes and free up the space.
40098	Warning	Physical tape %1 not available to start tape caching job. Waiting for tape...	The physical tape is not available.	No action is necessary.
40100	Warning	The export job is not allowed because the physical tape in the library is being used for tape caching.	The physical tape is being used by the tape caching library.	Select a different physical tape to be used for export.

Error Code	Type	Text	Probable Cause	Customer Action
40116	Error	Hardware compression failed.	Hardware compression card failure.	Retry operation. If problem persists, call 1-800-IBM-SERV within the US for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40117	Error	Hardware decompression failed.	Hardware compression card failure.	Retry operation. If problem persists, call 1-800-IBM-SERV within the US for software support services. Outside the US, please see http://www.ibm.com/planetwide/
40118	Error	Software decompression of a block compressed using hardware failed.	Check the event log message for detailed information.	Check the suggested action for the error message.
40120	Error	Space command to the physical tape drive failed.	There is a hardware problem with the physical tape drive.	Check connection for attached physical drive. If problem persists, use hardware problem determination guide for specific drive in question.
40121	Warning	The virtual tape has no new data. No export job will be submitted.	There has not been any data written since the last migration or this virtual tape does not have data to migrate.	No action is necessary.
40122	Warning	The physical tape is not available to start the export job. Resubmit the job when the physical tape is ready in the physical library.	The specified physical tape does not exist in the library.	Insert required physical tape into the library, re-inventory and resubmit the job.
50000	Error	Missing target name in normal login session from initiator.	The target name specified in the iSCSI initiator is incorrect.	Check iSCSI host setup and retry login session. If problem persists, call 1-800-IBM-SERV within the US for software support services. Outside the US, please see http://www.ibm.com/planetwide/

Table 11. TS7500 Virtualization Engine Software Version 2 Release 1 error codes (continued)

Error Code	Type	Text	Probable Cause	Customer Action
50002	Error	Login request to nonexistent target from initiator.	The target name no longer exists.	Check iSCSI host setup and retry login session. If problem persists, call 1-800-IBM-SERV within the US for software support services. Outside the US, please see http://www.ibm.com/ planetwide/
50003	Error	iSCSI CHAP authentication method rejected.	The iSCSI CHAP password is incorrect.	Make sure the password is entered correctly.

For additional error codes in reference to the IBM System Storage DS4000™, please see the *IBM System Storage DS4000 Problem Determination Guide*, GC27-2076.

Appendix C. Installing and starting PuTTY

To install and start the PuTTY SSH client at the workstation where the VE console application is installed, complete the following steps:

1. __ Insert the *Virtualization Engine TS7500 Base Firmware Update Disk* into the CD-ROM drive of the workstation.

2. __ Start Windows Explorer if it does not automatically start.

3. __ In Windows Explorer, navigate to *X:*➔**Tools**➔**putty**➔**installer**, where *X* is the letter of the CD-ROM drive.

4. __ Double-click the file named *putty-0.58-installer.exe*. The PuTTY Setup Wizard starts.

5. __ Click **Next**.

6. __ In the Select Destination Location window, click **Next**.

7. __ In the Select Start Menu Folder window, click **Next**.

8. __ In the Select Additional Tasks window, click **Next**.

9. __ In the Ready to Install window, click **Install**.

10. __ In the Completing the PuTTY Setup Wizard window, click **Finish**.

11. __ Close the Read Me window when desired.

12. __ Remove the *Virtualization Engine TS7500 Base Firmware Update Disk* from the CD-ROM drive.

13. __ Start PuTTY and connect to the TS7520 Server by completing the following substeps:

    a. Click **Start**➔**Programs**➔**PuTTY**➔**PuTTY**.

    b. In the **Host Name (or IP address)** field, type the full host name or the primary IP address of the TS7520 Server.

    c. Click **SSH**.

    d. Click **Open**.

    e. If the PuTTY Security Alert window opens, click **Yes**.

Appendix D. Installing Tivoli Storage Manager on the TS7520 Server

To install Tivoli Storage Manager on the TS7520 Server, complete the following steps:

1. __ If you do not have an SSH client installed at the workstation where the VE console is installed, install the PuTTY SSH client using the procedure in Appendix C, "Installing and starting PuTTY," on page 269.

2. __ Start the SSH client and connect to the TS7520 Server. For an example, see Appendix C, "Installing and starting PuTTY," on page 269 for the procedure to do this using the PuTTY SSH client.

3. __ At the **login as** prompt, type vetapeservice and then press the **Enter** key.

4. __ At the **Password** prompt, type service4u and then press the **Enter** key.

5. __ Perform one of the following:

   Installation from a CD-ROM

   a. __ Insert the TSM installation CD into the CD-ROM drive of the TS7520 Server.

   b. __ Mount the CD by typing

   ```
   sudo mount /dev/cdrom /media/cdrom
   ```

   and then pressing the **Enter** key.

   c. __ Navigate to the /media/cdrom directory.

   Installation from a downloaded .bz2 file

   a. __ Navigate to the directory where the TSM .bz2 installation file is stored.

   b. __ Expand the .bz2 file by typing the following:

   ```
   sudo tar xjf *86.tar.bz2
   ```

   and then pressing the **Enter** key. The * character denotes a variable string that contains the version number of the TSM software.

6. __ Create a directory called /application if one does not already exist.

7. __ Start the installation script by typing

   ```
   sudo ./install_server -p /application
   ```

   and then pressing the **Enter** key. The -p prefix specifies /application as the directory where the script will install TSM.

8. __ If prompted, select the number for the preferred language for the license agreement and then press the **Enter** key.

9. __ Press the **Enter** key as necessary to view the entire license agreement, if desired.

10. __ Accept the license agreement by typing the numeral **1** and then pressing the **Enter** key. The installation option menu appears.

11. __ Select the Basic Install option by typing the letter **B** and then pressing the **Enter** key.

12. __ Confirm the Basic Install option by typing the letter **Y** and then pressing the **Enter** key. When installation is complete, the installation option menu again appears.

13. __ Exit the installation script by typing the letter **Q** and then pressing the **Enter** key.

14. __ If you installed TSM from a CD, remove the CD from the CD-ROM drive by performing the following substeps:

   a. __ Navigate away from the `/media/cdrom` directory.

   b. __ Type the following:

```
sudo umount /dev/cdrom
```

   and then press the **Enter** key.

   c. __ Eject the CD from the CD-ROM drive.

15. __ Log out of the SSH session with the TS7520 Server by typing `exit` or `logout` and then pressing the **Enter** key.

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 grant 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.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

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 publications. IBM may make improvements or changes (or both) in the product(s) or program(s) (or both), 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.

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,

273

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.

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

Some software may differ from its retail version (if available), and may not include user manuals or all program functionality.

Trademarks

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

AIX	IBM	System x
AS/400	IBMLink	System Storage
DS4000	iSeries	Tivoli
ESCON	System i	TotalStorage
FICON	System p	Virtualization Engine

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

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

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

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

Electronic emission notices

The following statements apply to this product. The statements for other products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) Class A Statement

Note: 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, may 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 may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A Emission Compliance Statement

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

Avis de conformité à la réglementation d'Industrie Canada

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

European Union (EU) Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive [select either 89/336/EEC, as amended by Council Directive 93/68/EEC, or select 2004/108/EC, as appropriate] 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.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

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

Properly shielded and grounded cables and connectors must be used in order to reduce the potential for causing interference to radio and TV communications and to other electrical or electronic equipment. Such cables and connectors are available from IBM authorized dealers. IBM cannot accept responsibility for any interference caused by using other than recommended cables and connectors.

European Community contact:

```
IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Tele: 0049 (0)711 785 1176
Fax: 0049 (0)711 785 1283
e-mail: tjahn@de.ibm.com
```

Germany Electromagnetic Compatibility Directive

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit (vom: 2007/05/25)

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 Maßnahmen 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 Konformitätserklärung des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

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 Electronic Emission 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。

Japan VCCI Class A ITE Electronic Emission Statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に
基づくクラス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。

Korea Class A Electronic Emission Statement

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

Index

Numerics

A

B

C

D

Readers' Comments — We'd Like to Hear from You

IBM Virtualization Engine for Tape TS7520
User's Guide

Publication No. GC27-2068-02

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:
• Send your comments to the address on the reverse side of this form.

If you would like a response from IBM, please fill in the following information:

Name _____   Address _____

Company or Organization _____   _____

Phone No. _____   E-mail address _____

IBM®

Fold and Tape   **Please do not staple**   Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL   PERMIT NO. 40   ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Information Development
Department GZW
9000 South Rita Road
Tucson, Arizona
USA 85744-0001

Fold and Tape   **Please do not staple**   Fold and Tape

IBM ®

Printed in USA

Spine information:

IBM Virtualization Engine for Tape
TS7520

User's Guide

IBM