Sun StorageTek Virtual Tape Library

VTL Plus 2.0 Update 1

User Guide

Virtual Tape Library

VTL User Guide (Plus 2.0 Update 1)

Adobe PostScript

Revision History

Short Name	Part #	Revision	Date	Comments
VTL User Guide Update 1	96267		Nov 2006	Base document supplied by the vendor.
		A	Jan 2007	Major revision.
		B	Mar 2007	Published. EC 131376.
		C	Aug 2007	Major revision.
		D	Nov 2007	Minor revision.
		E	Feb 2008	Major revision to cover VTL Plus 2.0
		F	Mar 2008	Major revision to the commandline appendix
		G	May 2008	Revised for VTL Plus 2.0 Update 1.
		GG	July 2009	Minor updates for Update 1.
		GH	September 2009	Minor updates for Update 1.
		GI	December 2009	Added Error Codes section.

About this book

This book introduces tape virtualization and guides you through the administration of Sun StorageTek Virtual Tape Library (VTL) solutions, including VTL Plus 2.0 and VTL Value systems. It starts with a high-level explanation of VTL technology, common deployment architectures, and special features. It then provides detailed instructions for carrying out the tasks common to VTL administration according to Sun VTL best practices, including:

- SAN zoning
- using the VTL Console graphical user interface (GUI) and installing copies on management stations
- administering local area network (LAN) connections
- designing, creating, and managing virtual libraries and virtual tapes
- using special features like automatic tape caching, automatic tape archiving, and tape replication
- using encryption and data compression features to best advantage
- handling failback after a high-availability system has failed over
- reporting
- configuring and using email notifications

Finally, appendices provide additional information that, while not essential to a normal installation, may prove useful in special circumstances.

The document is *task-oriented*, organized around the work you have to do rather than around the features or components of the product. Each chapter and section begins with a list of the tasks it contains. Tasks are presented in order, and the steps in each process are numbered, in the sequence in which they are to be performed. Conditional steps (steps that you perform only in specified circumstances) begin with the condition ("If *A* ...") and end with the corresponding action ("... do *B*"); if the condition does not apply, you simply skip the step. Each task ends with a reference to the next task in the sequence:

Next task: "Installing ..." on page 3.

When the setup process branches, the task ends with conditional alternatives:

Next task:

- If the customer does not plan to run the management console from a host on the local area network (LAN), press Skip, and go to the next task.

- Otherwise, carry out the procedure "Configuring the Ethernet LAN" on page 57.

When you have finished a sequence of tasks, this is clearly noted:

Stop here.

To minimize the time you spend switching between publications or between major sections of the document, we have made an effort to avoid cross references to external information wherever possible. If you need to have a figure, a table, or a procedure, it should always be, at worst, on a neighboring page.

Taking advantage of this book's hypertext features

If you choose to view this book online, rather than in printed form, you can jump quickly to any part of the book by clicking on the corresponding entry under the Bookmarks tab on the left side of the Adobe Acrobat interface. In addition, clicking on entries in the table of contents, cross references, or references to subsequent tasks will take you directly to the indicated part of the document. You can then use the back arrow on the Adobe Acrobat Reader to return, if desired, to the point you left. In addition, clicking on most Uniform Resource Locators (URLs) and on most references to online resources will open your default web browser to the corresponding web page, so that you can, if necessary, obtain a required download immediately (be aware, however, URLs to specific pages change frequently and may not always be accurate).

Understanding the conventions used in this book

The table below illustrates the conventions that represent literal and variable values, commands, and property names in this book.

Convention	Meaning	Examples
`AaBbCc123`	Fixed-width text is used for literal values, including names of commands, files, directories, literal computer inputs/outputs, and Uniform Resource Locators (URLs)	Edit your `.login` file. Use `ls -a` to list files. `% You have mail.`
AaBbCc123 *AaBbCc123*	Oblique text is used for variables that stand for real names or values and for book titles.	To delete a file, type: `rm` *filename*.
ABCD	Bold, san-serif text indicates callouts in illustrations.	Click `Submit` (**A** below).
1.	Numbered paragraphs indicate steps in a process that should be executed in sequential order.	
■	Bulleted paragraphs indicate lists of alternatives or components.	
`[`*VTL_Plus*`]#`	a commandline prompt	

Obtaining the latest information and supporting resources

The Sun StorageTek Support portal <`www.support.storagetek.com`> provides links to the latest documentation, software updates, and licensing resources for VTL Plus solutions. Always check the portal for updates to this document before proceeding. Documents distributed on CDROM may not reflect the latest changes to VTL hardware, software, and services.

Commenting on this book

Sun welcomes your comments and suggestions for improving this book. Contact us at `glsfs@sun.com`. Please include the title, part number, issue date, and revision: *VTL User Guide (Plus 2.0 Update 1)*, part number 96267 (December 2009 Revision GI).

Contents

Introduction: VTL appliances and enterprise data-protection

Sun StorageTek VirtualTape Library (VTL) technology makes the benefits of disk-to-disk-to-tape architecture available to complex backup environments that cannot readily accommodate the disruptions and administrative burdens that often accompany major changes to information-management environments and processes. VTL solutions make disk media available to applications that are configured to work with tape. VTL software presents your existing tape-centric backup architecture with what appear to be familiar tape libraries, drives, and data cartridges while managing the complexities of the implementation—disk arrays, RAID groups, and logical volumes—internally.

Such transparency is absolutely critical when backup is just one aspect of an enterprise-wide business-continuity plan. When legacy systems and multiple, interdependent applications, procedures, policies, and/or service providers are involved, even modest changes to a backup architecture can have unforeseen, far-reaching consequences.

The advantages that disk-to-disk backup has to offer are no less critical in complex environments. Heavy workloads, tight schedules, and multiple dependencies often make backup windows very tight or non-existent. Jobs that fail to complete cannot, in most cases, be retried. Tape-based backup systems perform well when handling big jobs, like full backups of large files and file systems that can stream large amounts of sequential data. But much of the current backup workload consists of intermittent, essentially random I/O—incrementals, full backups of heterogeneous small servers and workstations, and small files (such as those associated with email systems). Tape drives perform poorly under these conditions. But disk-based storage is ideally placed to handle this type of I/O.

The remainder of this chapter provides:

- a brief summary of VTL "Features" on page 2
- a detailed discussion of the "Advantages of VTL tape virtualization" on page 4
- a more in-depth look at selected, "Key VTL features and options" on page 8.

Features

The Sun StorageTek VTL solution has the following features:

- Emulation of most widely used tape libraries, drives, and media types, including the latest Sun StorageTek T10000-series drives and media

- Dynamic allocation of disk capacity

  VTL software can allocate disk space to virtual tapes in 5-GB increments, up to the full, rated capacity of the emulated media. This minimizes wasted space, provides natural load balancing, and optimizes the performance of the disk array.

- Auto Archive feature

  The Auto Archive option writes data to physical tape whenever a backup application or utility moves a virtual tape from a virtual library to an import/export slot. The physical tape library must support barcodes: the VTL software has to find a matching barcode in the physical library in order to export a virtual tape to a physical cartridge.

- Replication of tapes to local and remote VTL systems

  VTL software supports manual copying and both event- and policy-driven automatic replication methods.

- Automated Tape Caching option

  With the optional tape-caching feature, VTL software can automatically save a single virtual volume with a single barcode in two physical forms, one on disk and one on physical tape. The tape-caching feature manages retention and migration of the physical images, under the control of user-specified policies and schedules. This lets users keep space in the disk cache free for new backup sets while retaining the tape images of older virtual volumes. When a virtual volume no longer resides in the disk cache, a pointer in the cache seamlessly redirects requests to the tape image.

- High availability option

  An optional, high-availability configuration provides intelligent failover, with duplicate, self-monitoring VTL server nodes and redundant, primary and standby paths between backup applications and VTL data.

- Encryption and secure data destruction

  To ensure that the data that you export to physical tape is confidential and secure, VTL offers a Secure Tape Option that uses the Advanced Encryption Standard (AES) algorithm published by the National Institute of Standards and Technology, an agency of the U.S. government.

The Shred feature insures military standard, secure data destruction by overwriting virtual tape with random bit patterns. Data destruction jobs are queued so that the shred process does not have an excessive impact upon performance.

■ Data compression

Sun VTL Plus 2.0 supports both software-based and hardware-based data compression.

Both data-compression technologies offer similar functionality. Both are based on the LZO algorithm. When necessary, either can increase the amount of data that will fit on a virtual tape of a given capacity. Compression ratios can approach 2:1 for data sets made up of highly compressible file types, such as plain text and uncompressed bitmapped images (incompressible file types, such as ZIP archives, GIF images, and JPG images reduce the attainable compression proportionately).

However, the optional VTL Plus 2.0 compression hardware offers significantly higher throughput performance compared with the software-only approach. Specialized ASICs (application-specific integrated circuits) on the optional compression cards perform the calculations that software-only solutions must perform on the system CPU.

■ Support for Sun StorageTek ACSLS and Library Station library-management software

ACSLS and Library Station support makes a high degree of integration possible between VTL solutions and complex enterprise storage environments that include large libraries with multiple partitions and mixed open systems and mainframe systems. Sun VTL virtual libraries can cache or copy tape volumes to storage pools on shared, ACSLS-managed libraries. Alternatively, ACSLS can be configured to manage virtual libraries.

■ Email notifications

The VTL email alerts feature monitors an extensible set of pre-defined critical system functions and automatically notifies a local system administrator by email. You can extend or modify the CallHome monitoring scripts to customize monitoring for your needs.

■ X-ray diagnostics

The X-ray feature combines snapshots of the current state of the appliance, its configuration, and its environment with system event logs and saves the result in a standard, tape-archive (tar) format.

Key VTL features are discussed in more detail later in this chapter.

Advantages of VTL tape virtualization

Adding Sun StorageTek VirtualTape Library appliances to an existing tape-based backup architecture can thus realize the following advantages:

- "Shorter runtimes and reduced dependency on backup windows" on page 4
- "Shorter run times for non-sequential backup jobs" on page 5
- "Improved reliability" on page 5
- "Better utilization of tape subsystems" on page 5
- "Larger, more flexible libraries" on page 6
- "Compatibility with ACSLS management software" on page 6
- "True tape virtualization with dynamically allocated disk space" on page 7.

Shorter runtimes and reduced dependency on backup windows

VTL appliances can handle a narrow backup window by using numbers of virtual drives operating in parallel, something that would be highly impractical with physical tape drives. In this way, the critical, first copy of the primary data is reliably transferred to disk-based virtual tape in minimum time. Thereafter, vaulting software and/or VTL tape-caching features can copy the backup from virtual to physical media using a smaller, more economical number of physical drives. See the figure below:

Multiple virtual drives speed backup during the critical backup window

primary storage   virtual library   physical library

virtual tape drives

physical tape drives

backup window

Back up to multiple virtual tape drives during the critical backup window

At other times, copy virtual tapes to physical media using one or two dedicated tape drives
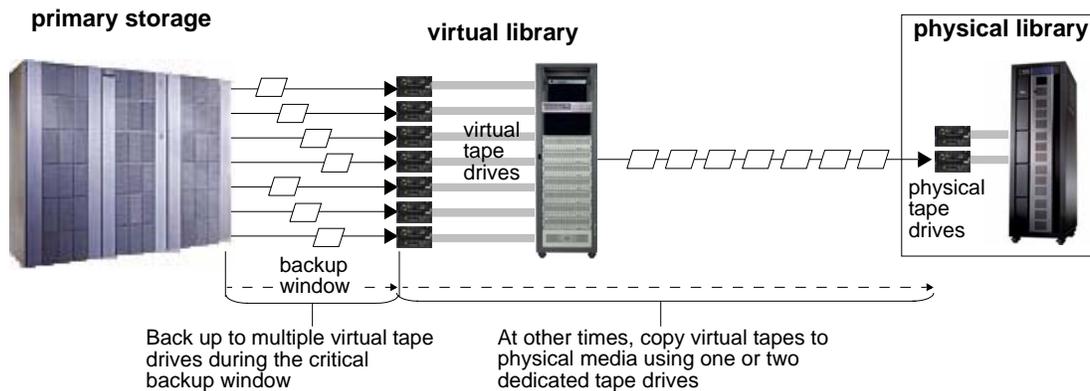
Shorter run times for non-sequential backup jobs

Disk-based VTL systems reduce run time when storage operations are poorly matched to the operational characteristics of tape backup systems. Properly configured, streaming tape backups achieve transfer rates that are as high as or higher than those attainable by disk technology. But many common jobs—such as incrementals and full backups of workstations—produce semi-random I/O. Non-sequential I/O keeps tape drives busy mounting, unmounting, and positioning media, greatly reducing throughput. Disk-based secondary storage is much better suited to these semi-random backup jobs.

Improved reliability

Disk-based VTL systems can significantly increase the reliability of the backup process. Backup jobs are more likely to succeed the first time, because the critical step—the creation of a copy of the data—is a simple, fast write to a RAID subsystem. Jammed tapes, lack of ready media, and off-line drives no longer ruin jobs. See the figure below:

Backup is more reliable with virtual tape libraries

backup window

primary storage

physical library

FAILURE!

A backup to physical tape can fail when a tape drive jams or media breaks, because a retry may not be possible before the backup window closes.

A backup to disk-based virtual media always succeeds, so all data is copied to secondary media before the backup window closes.

SUCCESS!

virtual library

physical library

Virtual volumes are subsequently copied to physical media outside the backup window. If problems arise, copy jobs can be retried later.

Better utilization of tape subsystems

Disk-based VTL systems can improve utilization, performance, and reliability of tape-storage subsystems. When non-sequential I/O is backed up to disk, tape can be reserved for sequential jobs that can stream a physical tape drive. Large-scale full backups can, for instance, go directly to tape, insuring maximum performance. Jobs

that produce intermittent or non-sequential I/O, such as incrementals and backups of work stations, are copied to tape only after they have been backed up to disk and incorporated into large, sequential backup sets. This approach uses tape drives continuously, at close to their maximum throughput. The drives spend less time idle, since they mount and reposition less often. Fewer drives and tapes are needed for a given workload. Devices and media suffer less wear and tear.

Improved utilization of backup media

Tape virtualization lets you create emulated tape volumes that are more closely sized to the average size of your backup media. If you do not decide to use tape caching (see "Automated Tape Caching" on page 12), you set the maximum capacity of your virtual tapes to 50-60 GB or to the average size of your backup jobs (whichever is larger). This approach minimizes wasted space in the critical disk cache, where the first copy of each backup job is stored, and makes a maximum number of cartridges available for backup jobs at any given time. Your copy/vault software can then consolidate these smaller volumes onto full-sized physical tape cartridges outside the backup window. If you also enlarge the size of the library, as described below, you can accomodate a larger total number of these smaller virtual tapes.

If you adopt tape caching, you cannot size virtual tapes this way, since, as we shall see, the disk and physical-tape images of the virtual tape must be logically identical.

Larger, more flexible libraries

The Sun VTL virtual library faithfully emulates a Sun L700 physical tape library. But, while the L700 has 678 slots, the Sun VTL can have up to 64000 in a non-tape caching solution, depending on the backup application (see "Automated Tape Caching" on page 12). This is a particularly important consideration if you improve media utilization by reducing the size of your virtual tape volumes, as described above. One large virtual library can, on its own, serve all the needs of a backup application master server.

Compatibility with ACSLS management software

Tape virtualization lets you control disk-based virtual libraries with the same industry-standard, Sun ACSLS software that controls physical tape libraries. ACSLS adds an additional virtualization layer to your backup environment, further reducing disruptions to established infrastructure and policies while, at the same time, bringing new capabilities.

Operating systems and backup applications that currently interact with a physical library via ACSLS continue to use ACSLS when accessing VTL virtual libraries. ACSLS further hides the particulars of disk-based tape virtualization behind a standard, well-known interface.

This ability to mask the library implementation from client applications and operating systems lets ACSLS make disk-based tape-virtualization available to platforms that could not otherwise support it. Platforms that do not support SCSI passthrough library control, such as Unisys, Tangent, and mainframe operating systems, can back up to Sun VTL virtual libraries using ACSLS.

The more powerful, more specialized library-control functionality of ACSLS improves the availability of suitably configured VTL solutions. The brief SCSI path interruptions that may accompany failover and failback are less likely to interfere with the backup application, because ACSLS retries the connection aggressively enough to restore the path.

True tape virtualization with dynamically allocated disk space

Correctly configured, dynamically sized virtual tape volumes provide the highest capacity and performance. When tapes are created with the VTL Capacity On Demand feature enabled, the VTL software allocates space as data is written to disk rather than all at once. For instance, a physical tape with a capacity of 400-GB can be emulated without allocating any space initially, and thereafter enlarged as needed in 5-GB increments (see the figure below).
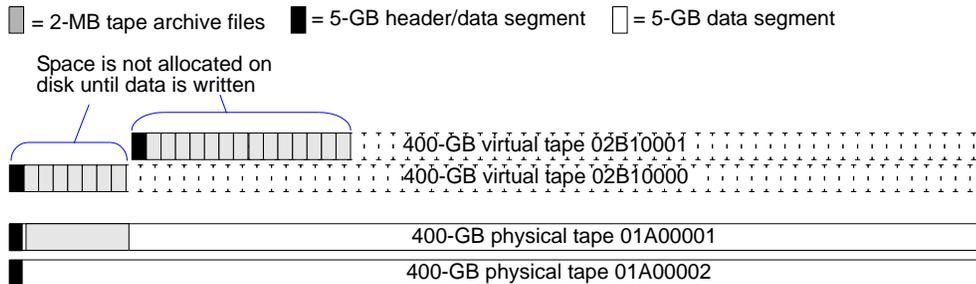
This approach to space allocation has two major advantages. First, it minimizes wasted disk capacity. Second, and perhaps more importantly, it maximizes array performance and reliability. Dividing data into multiple segments distributes it more evenly across the array, involves more volume groups in each I/O, and reduces the average length of each seek during I/O.

Key VTL features and options

NDMP migration

Backup applications that support Network Data Management Protocol (NDMP) 4.0 with `Sun VTL` virtual libraries can mount virtual tapes on a suitably configured VTL Plus 2.0 server, copy them to physical media, and track copies using backup application management databases. The backup application backs up data across the SAN, creating the critical first copy on VTL virtual tape (**A** below). The backup application then mounts the virtual tapes to an NDMP agent hosted on the VTL server (**B**) and copies them over the SAN to physical media (**C**) by sending NDMP command and control information across the Ethernet LAN (**D**).

To take advantage of this functionality, you must enable the VTL Plus 2.0 Hosted Backup and NDMP options.
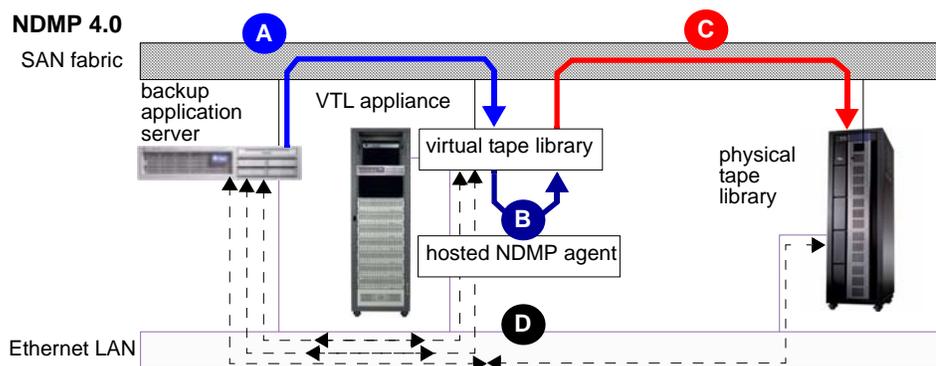
Note that the Sun VTL Plus Hosted Backup and NDMP options are not required when backing up a Network Attached Storage (NAS) filer to a VTL applaince. In this instance, the NAS filer is simply a backup client. The backup application server

controls NDMP agent software on the filer (**D** below). This agent software copies data from the filer over the SAN to virtual tape volumes (**E**) mounted by the backup media server (**F**), so no softwre has to be hosted on the VTL appliance.
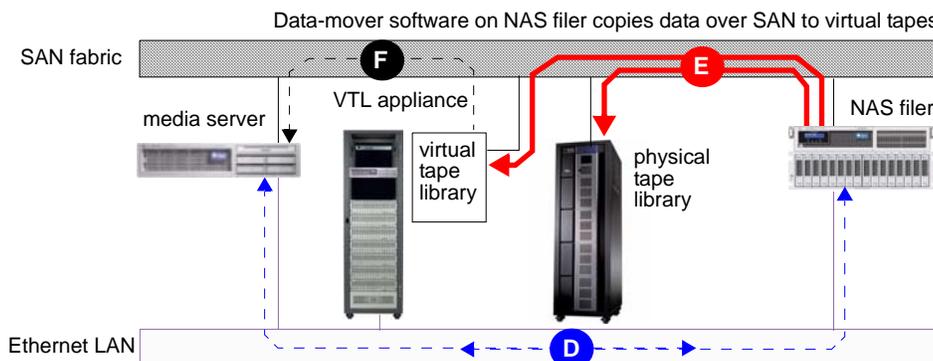
VTL high-availability option

In a VTL high-availability system, intelligent self-monitoring software, redundant hardware, and high-availability LAN and SAN configurations protect both the data path and your ability to manage storage. To help you to better understand the steps in the failover configuration process, this section provides a high-level description of the three key components of the high-availability VTL solution:

- "Server node failover" on page 9
- "Management path failover" on page 10
- "Storage path failover" on page 11.

Server node failover

The Sun StorageTek VTL high availability option uses two server nodes, each configured to monitor its companion. Each member of the pair serves as the primary server for its own storage clients and as the secondary, standby server for those of its companion. To protect against server failures, each server sends heartbeat information to its secondary using a service IP address. If heartbeat information indicates a fatal error in a companion server's processes, the healthy server notifies its companion that it is assuming primary server responsibility for both sets of clients and initiates failover. If the heartbeat information stops altogether, the healthy server immediately initiates failover. Finally, if a primary server's own, self-monitoring routines detect a storage device connectivity failure and cannot determine if the failure is local, the primary reports the failure to its companion via the heartbeat signal. If the companion, secondary server can access all devices,

including the device in question, the failure is local to the primary, and the secondary initiates failover. If the secondary cannot access devices, the outage is global, and no failover occurs.

Service IP addresses carry heartbeat information between VTL nodes and management IP addresses carry commands between nodes and VTL management consoles
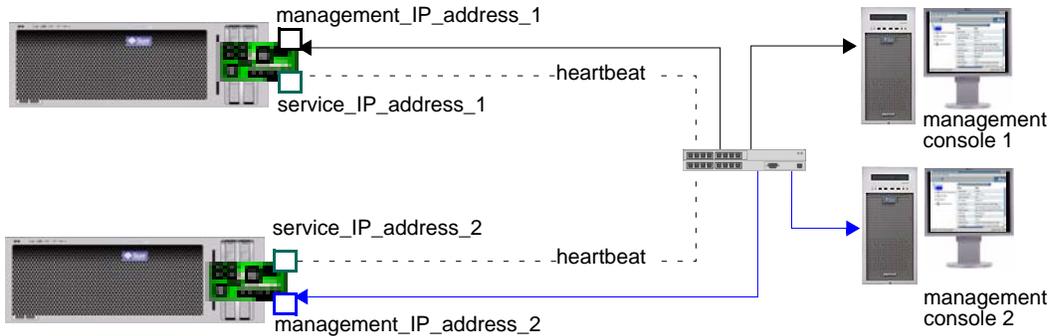
Management path failover

When a high-availability VTL system fails over, the failover server automatically inherits the failed server's management IP address, so that remote management consoles can still reach the VTL system.

If the heartbeat signal is lost, the management IP address for the failed node transfers to the healthy node
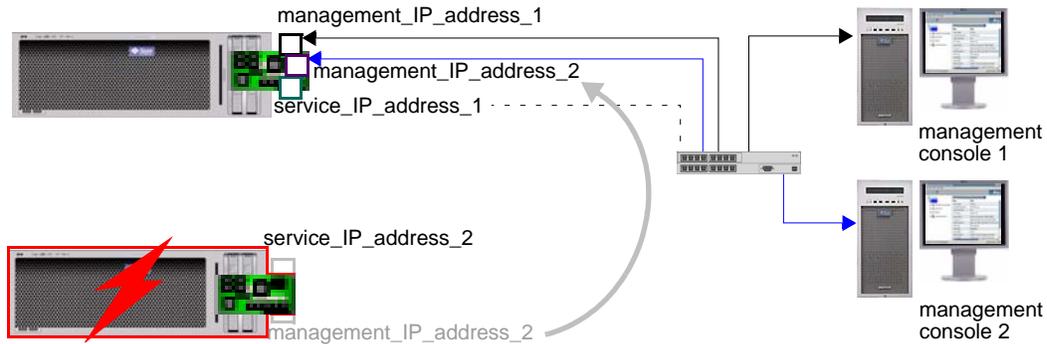
Storage path failover

In a standard-availability VTL system, there is one logical path from a VTL client to VTL storage, and every Fibre Channel port is either a target port for a VTL client or a storage-facing initiator. But in a high-availability system, there are two paths, a *primary* and a *secondary* or standby path, as shown below.

Fibre Channel path failover in high-availability VTL systems
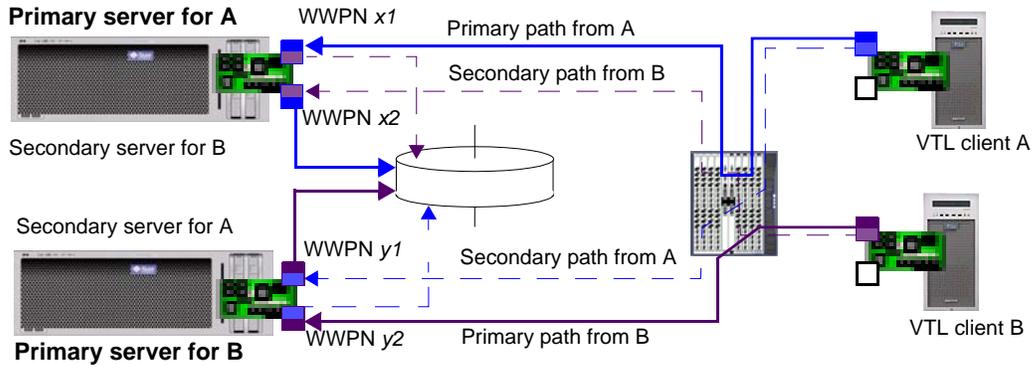
Failover during replication

If a replication operation is in progress when failover or failback occurs, replication stops. Once failover/failback has completed, replication resumes with the next normally scheduled operation.

Mirroring and failover

If mirroring is in progress during failover/recovery, after the failover/recovery the mirroring will restart from where it left off.

If the mirror is synchronized but Fibre Channel connectivity is lost between the server and storage, the mirror may become unsynchronized. It will resynchronize automatically after failover/recovery.

A synchronized mirror will always remain synchronized during a recovery process.

Automated Tape Caching

The Automated Tape Caching option presents backup applications with virtual tape volumes that are physically implemented on disk, tape, or both. This keeps the implementation simple—the backup application manages only the virtual tape volumes and virtual libraries—while giving the backup administrator the ability to fine tune the physical implementation for best performance and reliability.

VTL software can implement virtual tape volumes and virtual libraries using an optimal combination of resources: disk arrays, physical tapes, physical libraries, and physical tape drives. VTL policies specify where data should reside—on disk for fast random access, on tape for longer term storage, or on both for maximum redundancy—and for how long. Under policy control, VTL software can automatically copy backup sets from disk to tape, outside of the backup window. It can retain the backup sets in the disk cache for a specified period, so that users can rapidly restore data during the period when the need is highest. It can then free up the disk cache for new backup sets while retaining an image on tape. If a restore is necessary, a pointer in the disk cache points the request to the physical tape image, transparently and automatically. The Automated Tape Caching option thus simplifies and automates management of the disk cache, insuring adequate capacity with minimum disk resources.

Policies can be built around the number of days that data sets reside on disk, around a disk-capacity high water mark, or around a specified event or time of day. Physical tape I/O can thus be run as a background process that does not interfere with production datacenter operations.

Note – Automated Tape Caching and Auto Archive/Replication cannot be used at the same time on the same virtual library.

Virtual tape replication

Replicating data provides additional protection for the information on a virtual tape by maintaining a copy locally or on another VTL server. VTL software supports three replication methods, two of them automatic and one a manual process that can be used if you are not using the automatic methods.

See the following subsections for additional information:

- "Auto Replication" on page 13
- "Replication" on page 13
- "Remote Copy" on page 14.

Auto Replication

The `Auto Replication` option copies virtual tapes from a virtual library to another VTL server whenever a backup application or utility moves a virtual tape to an import/export slot.

You enable Auto Replication at the library level when you create a virtual tape library (see "Setting up the Auto Replication option" on page 54). You can then selectively enable the feature on a tape-by-tape basis as tapes are created. You cannot alter the Auto Replication status of an existing virtual tape.

Replication

The VTL `Replication` feature maintains synchronized *replica resource* copies of virtual tapes on a designated VTL server. At the end of a policy-defined replication interval, VTL software copies data that has changed and is not currently in use from the primary virtual tapes to the replica resources.

During normal operation, backup clients have no access to replica resources—the latter are purely internal protections within the VTL system. If the primary virtual tape is corrupt or otherwise unusable, however, administrators can *promote* replica resources as part of their disaster recovery process. Once promoted, the replica resource becomes the primary virtual tape, with the same barcode and attributes. Backup clients can thus use it for recovery as if it were, in fact, the original copy.

You can configure the VTL Replication feature for either:

- Remote Replication or
- Local Replication.

Remote Replication

Remote Replication maintains synchronized copies of virtual tape volumes on the storage arrays of a pair of VTL appliances that are connected across Ethernet local area networks (LANs) or Wide Area Networks (WANs). Data is thus transferred at LAN/WAN speed, but is not subject to the distance limitation imposed by Fibre Channel storage area network (SAN) technology.

Local Replication

Local Replication maintains local, synchronized copies of virtual tape volumes on the storage arrays of a single VTL appliance. Data is transferred at SAN speed over distances limited to the maximum possible with a Fibre Channel SAN.

Remote Copy

Remote Copy copies a single virtual tape to another server on demand.

Replication requirements

The following are the requirements for setting up a replication configuration:

- (Remote Replication) You must have two VTL servers.
- (Remote Replication) You must have write access to both servers.
- You must have enough space on the target server for the replica resource.
- The target server must be a 64-bit server.

Port requirements for replication

The Sun VTL appliance comes with four gigabit Ethernet ports configured in the software. The primary port is net0, and it is called nge0 or e1000g0, depending upon which server node you have. That port should be connected to the customer's network for management purposes (running the console, issuing CLI commands, etc).

The second port, net1, is configured on the appliance's private 10.0.0.x network. That should be left as-is, configured for use by Sun service representatives or customer personnel under the direction of Sun support. There is a cable connected from that port to the 3COM switch included with the appliance, and that network is used to manage the appliance components (servers, switches, and disk controllers).

Two ports are left available for use with IP replication. Those ports are net2 and net3, and they come pre-configured with the IP addresses 192.168.0.1xx (the addresses are different for each port and for each server within the appliance).

To use these last two ports for IP Replication, the ports must be connected to a customer switch (not the appliance's internal 3COM switch). To make sure these ports and only these ports are used for replication, configure them with IP addresses on the same subnet as the replication ports on the target server. If you use the same network segment as your main management port, replication traffic will use that port, regardless of whatever IP addresses you have set for the replication ports. The same holds true for the target server. Replication traffic will go to the principle port on the target server, the one that is used for management traffic.

To set the addresses, do not use Solaris commands like ifconfig. Set the IP addresses from within the VTL console. Log in with root permissions and right-click on the server name so that a menu pops up and allows you to select "System Maintenance." From within "System Maintenance," select "Network." Select the interface you want

to configure (net2 or net3), assign the port the proper address, netmask and gateway. Configure the second port with its own address, but use the same netmask and gateway.

When you set up replication, select the target server's IP addresses that are to be used for replication. Do not use the target server's main management port. If you follow these instructions, replication traffic will have two ports to use on both ends and replication traffic will not be competing with traffic for VTL management or internal VTL management. The best performance will come if you are able to dedicate the network segment for replication and not have the replication traffic.

VTL Secure Tape encryption option

The VTL Secure Tape option uses the Advanced Encryption Standard (AES) algorithm to protect physical media that might otherwise be vulnerable to theft or diversion during transit. VTL software encrypts data when it is exported to physical tape and decrypts it when it is reimported to virtual tape.

Key management

The Secure Tape feature provides for flexible cryptographic key management that can be adapted to local security requirements and policies. Administrators can generate a single key for all exported tapes or multiple, unique keys for different tapes or sets of tapes. Multiple keys are more secure in the sense that the compromise of a single key exposes fewer tapes. But keys are harder to manage. Administrators must keep track of which key applies to which tape, because using the wrong key will cause indecipherable data to be imported into the virtual library. To facilitate centralized key management, keys can be exported to an external *key package* file. Key packages can be centrally generated and distributed, by secure means, to remote sites where data is imported to or exported from VTL systems.

Password protection

For additional security, each key is password-protected. Administrators must provide the correct password before changing a key name, password, or password hint, and before deleting or exporting a key.

Sun VTL Operational Restrictions

VTL Plus and VTL Prime are appliances running a specialized version of Solaris 10 on Sun Servers with Sun disk arrays. They use specific versions of software, firmware and configuration scripts that have been tuned for VTL. These cannot be viewed as individual components such as Solaris 10 on a server or a Sun 6140 disk array connected to a host. It cannot be modified based on readily available component upgrades such as FRUs, hardware upgrades, firmware, software maintenance, or software applications that are not specifically noted as part of the VTL offering or VTL maintenance. Special purpose scripts or software cannot be loaded onto the Solaris 10 host running the VTL software even if they've been shown to be effective or helpful with non-VTL systems. If there are specific questions or concerns with your implementation, open a support case to Sun VTL Backline Support -- don't rely on general email aliases.

VTL password-protected login accounts

There are three password-protected login accounts set up in the VTL appliance. These are named **root**, **vtl**, and **vtladmin**.

root

The **root** account is restricted to authorized support personnel and to those customers who have signed an amendment to the software license agreement regarding usage terms.

vtl

The **vtl** account is a VTL Administrator account that can be used for both Solaris logins and VTL Console logins.

You should use this account for managing the VTL.

The **vtl** account can log in from a remote session over ssh, and provides the ability to perform nearly every VTL administrative action via either the VTL Console or the Command Line Interface (see "VTL command line reference" on page 173 for information about the CLI).

Restrictions: "Create new accounts" and "Change administrative password" functions are disabled for the **vtl** account; these functions are restricted to the **root** account. Also, while both **root** and **vtl** can perform the iscon commands, only **root** can perform commands beginning with "vtl" (those commands are used to stop,

start and restart the VTL services and are restricted to **root**-level access). Any additional administrator accounts created in VTL will also be denied permissions that are restricted to **root**.

vtladmin

The **vtladmin** account is created for Solaris logins. It will not work for VTL console logins. This account allows some Solaris actions without having **root**-level access.

Understanding VTL Zoning

Zoning is the crucial first step when integrating a storage system, such as the VTL appliance, into a Fibre Channel storage area network (SAN). While specific zoning recommendations must vary from SAN environment to SAN environment, this chapter describes the basic requirements that all successful VTL deployments must address.

■ "Zoning for standard-availability systems" on page 19

■ "Zoning for high-availability systems" on page 20.

Zoning for standard-availability systems

The basic zoning requirement for VTL solutions that do not implement the high-availability feature is that each SAN zone contain only one initiator and one target, as shown in the figure below.
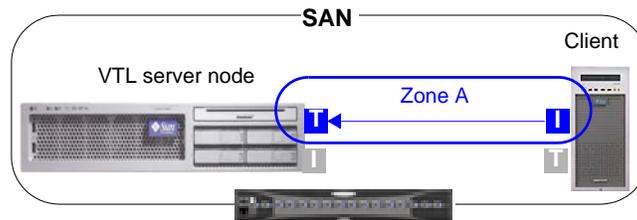
You zone standard-availability VTL systems the same way, regardless of the type of zoning you use. In a soft-zoned SAN, each target and initiator is defined by a logical World Wide Port Name (WWPN), while in a hard-zoned SAN, target and initiator are defined by physical port numbers. But, in either case, you have one client initiator and one VTL target per zone.

Zoning for high-availability systems

Zoning a high-availability system is slightly more complex than zoning a standard system, due to the need for redundant paths between initiators and targets. Once again, each SAN zone can have only one initiator and one target. But the total number of zones you need depends on whether the SAN is soft-zoned (by World Wide Port Name) or hard-zoned (by port number). See:

- "WWPN zoning (soft zoning)" on page 20
- "Port zoning (hard zoning)" on page 21.

WWPN zoning (soft zoning)

A soft-zoned SAN maps initiator to target using a logical World Wide Port Name (WWPN), rather than a physical hardware address. This name-to-name zoning establishes a logical route that may traverse varying physical ports and varying physical paths through the SAN. To accomplish failover, we thus need only a single zone for the client initiator, the active VTL target, and the standby VTL target.

See the figure below shows a soft-zoned SAN before VTL failover:
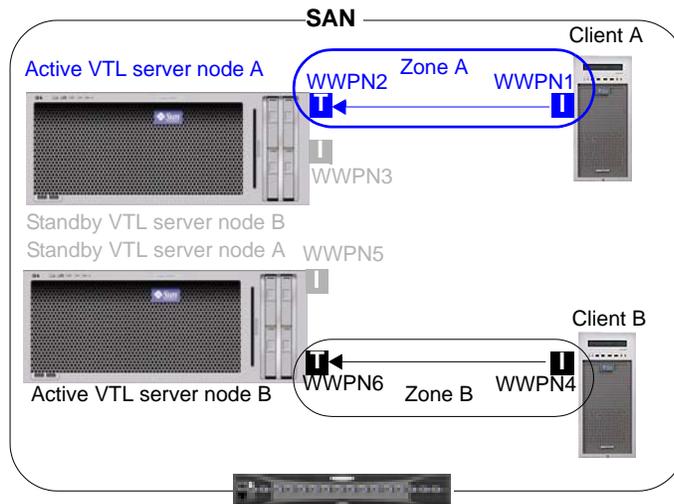
During failover, the zone still contains only one initiator and one target at a time. But the target WWPN is remapped from a port on the failed server node to a physical port on the standby server. The standby physical port spoofs the WWPN of the failed port, so zoning does not change. The figure below shows a soft-zoned SAN after VTL failover, with a standby port spoofing the WWPN of the failed port:
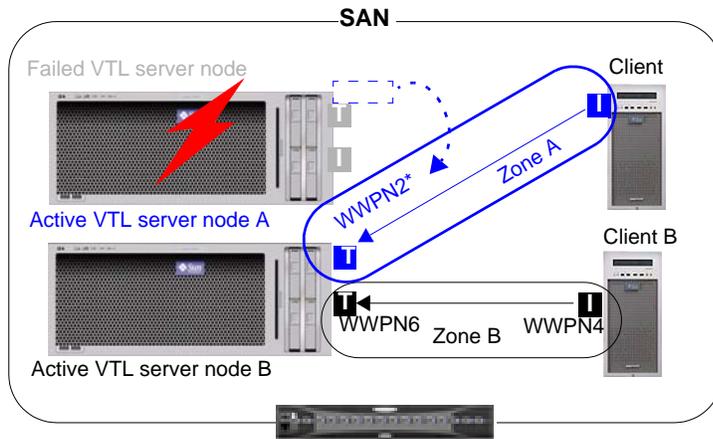
Port zoning (hard zoning)

A hard-zoned SAN maps initiator to target using a physical port address. This port-to-port zoning establishes a fixed, physical route through the SAN. So, since each SAN zone can contain only one initiator and one target, you must provide two zones for each initiating client. The figure below shows a hard-zoned SAN before VTL failover:
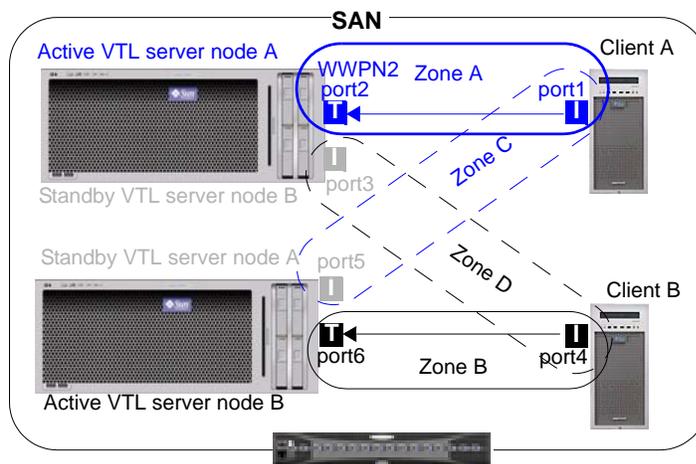
As the above figure shows:

- one zone defines the path to the primary VTL server node
- the other zone defines the path to the standby server.

During failover, the standby port becomes active by spoofing the WWPN of the failed port. The figure below represents a hard-zoned SAN after VTL failover:

SAN

Client A
port2
port1
port3
WWPN2 Zone A
Active VTL server node A port5
Client B
port6 Zone B port4
Active VTL server node B

sample.wwpnchart.ods - OpenOffice.org Calc

File   Edit   View   Insert   Format   Tools   Data   Window   Help
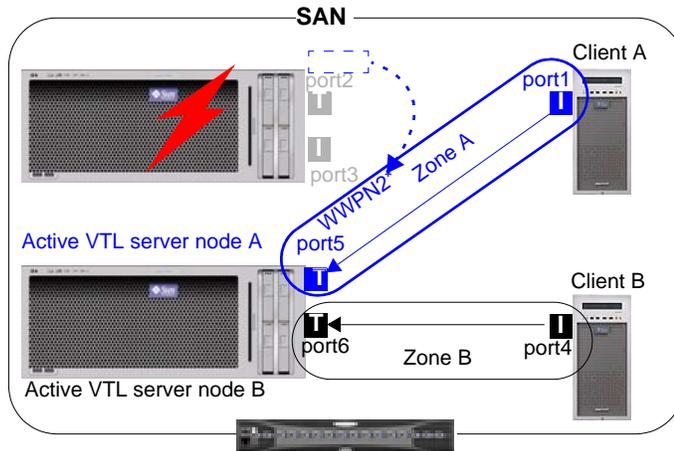
	A	B	C	D	E
	VTL Port #	**WWPN**	**Port function**	**Stands by for port #**	**Fails over to port #**
2	0	[21][00][00][e0][8b][0e][b8][94]	Disk		
3	1	[21][01][00][e0][8b][2e][b8][94]	Disk		
4	2	[21][00][00][e0][8b][0e][bc][9c]	Host	8	12
5	3	[21][01][00][e0][8b][2e][bc][9c]	Host	9	13
6	4	[21][00][00][e0][8b][1e][e8][e9]	Disk		
7	5	[21][01][00][e0][8b][3e][e8][e9]	Disk		
8	6	[21][02][00][e0][8b][5e][e8][e9]	Host	10	14
9	7	[21][03][00][e0][8b][7e][e8][e9]	Host	11	15
10	8	[21][00][00][e0][8b][1e][72][e4]	Host	12	2
11	9	[21][01][00][e0][8b][3e][72][e4]	ACSLS server	13	3
12	10	[21][02][00][e0][8b][5e][72][e4]	Host	14	6
13	11	[21][03][00][e0][8b][7e][72][e4]	Host	15	7
14	12	[21][00][00][e0][8b][0a][49][d5]	Host	2	8
15	13	[21][01][00][e0][8b][2a][49][d5]	Host	3	9
16	14	[21][00][00][e0][8b][1a][5e][93]	Host	6	10
17	15	[21][01][00][e0][8b][3a][5e][93]	Host	7	11

Sheet1 / Sheet2 / Sheet3

Sheet 1 / 3   Default   100%   STD   *   Sum=0

SAN clients include backup application hosts, such as Symantec NetBackup master servers, and ACSLS servers (if ACSLS is to control VTL virtual libraries). VTL must not share initiator ports with other SAN clients, such as physical tape devices.

Next task: When you have completed zoning, log in to the VTL server, scan for Fibre Channel devices, and make sure that all devices are visible.

Using the VTL console

The Virtual Tape Library console application is the graphical user interface that you use when administering and managing the VTL system. The console provides you with full control over virtual library operations, from creating libraries and tapes to managing disk storage and data migration from disk to physical tape.

The VTL console software is installed on a management workstation that you provide and communicates with the appliance via your local area network (LAN). In most deployments, your Sun service representative will install one instance of the console for you (you can install as many additional instances as you require on other machines, though no more than two instances can access the same VTL server at the same time). For information on installing additional instances of the console, see "Installing the VTL console" on page 147.

The following sections explain how you use the console application:

- "Running the VTL console application" on page 24
- "Populating the console" on page 24
- "Understanding the VTL console interface" on page 26.

Note – For information on the text-based, VTL command line user interface, see Appendix A, "VTL command line reference" on page 173.

Running the VTL console application

▼ Launching the VTL console

1. **To launch the console on a Sun Solaris workstation, open a terminal window and enter the command shown below:**

```
% /usr/local/vtlconsole/vtlconsole &
```

2. **On a Microsoft Windows system, press the** `Start` **bar to access the main menu system, and select** `All Programs > Sun Microsystems > VTL 5.0 > VTL Console`**.**

3. **To launch the console on a Linux workstation, open a terminal window and enter the command shown below:**

```
% /usr/local/vtlconsole/vtlconsole &
```

Stop here.

Populating the console

Once the console is running, you can specify the VTL servers that you want to see in the object tree at the left side of the VTL console. You can discover, add, or remove servers:

- "Discovering VTL server nodes" on page 24.
- "Adding a server node to the console tree" on page 25
- "Deleting a server node from the console tree" on page 26

▼ Discovering VTL server nodes

Whenever a VTL server is added to the subnet managed by a VTL console, you can discover the new addition and its properties using the procedure below.

1. **From the console main menu, select** `Tools` **(A below), then select** `Discover VTL Servers` **from the submenu (B).**
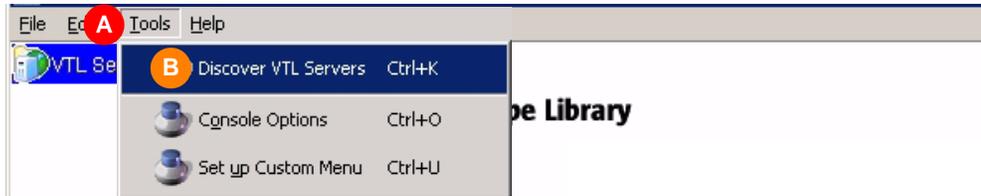
2. **When the** `Discover Virtual Tape Library Server` **dialog appears, enter the subnet filter (F below) and subnet mask (G) for the VTL appliance. Then press** `OK` **(H).**
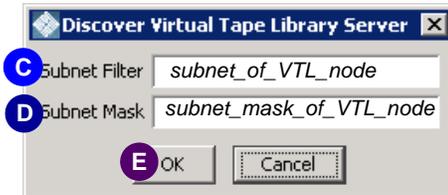
After a short wait, the VTL console application discovers the appliance and adds it to the list on the left side of the graphical user interface (GUI).

Stop here.

▼ Adding a server node to the console tree

1. **In the tree view of the VTL console, right-click on** `VTL Servers` **(A below).**
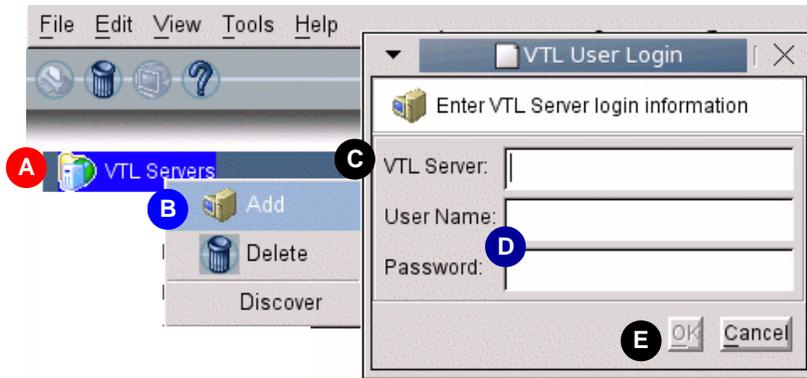
2. **From the context menu, select** `Add` **(B above).**

3. When the `VTL User Login` **dialog appears, enter the** `VTL Server` **host name or IP address (C above) and the** `User Name`**, and** `Password` **(D), and press** `OK` **(E).**

Stop here.

▼ Deleting a server node from the console tree

1. **In the tree view of the VTL console, right-click on the name of the server you wish to delete from the console view.**

2. **From the context menu, select** `Delete`**.**

3. **When the confirmation dialog appears, select** `Yes`**.**

Stop here.

──────────

Understanding the VTL console interface

The VTL console interface consists of four main parts: a main menu, a left-hand main window pane, a right-hand main window pane, and a status bar at the bottom of the interface. The VTL main menu system (**A** below) lets you control the console and carry out the administrative functions it supports. The left hand pane of the VTL console interface represents the component objects of the VTL system as the branches of a tree (**B** and **C** below). It contains the following major branches:

■ "Virtual Tape Library System" on page 28

■ "SAN Clients" on page 29

■ "Reports" on page 29

■ "Physical Resources" on page 30.

Clicking on the icon for a VTL server (**B** below) opens the log-in dialog.
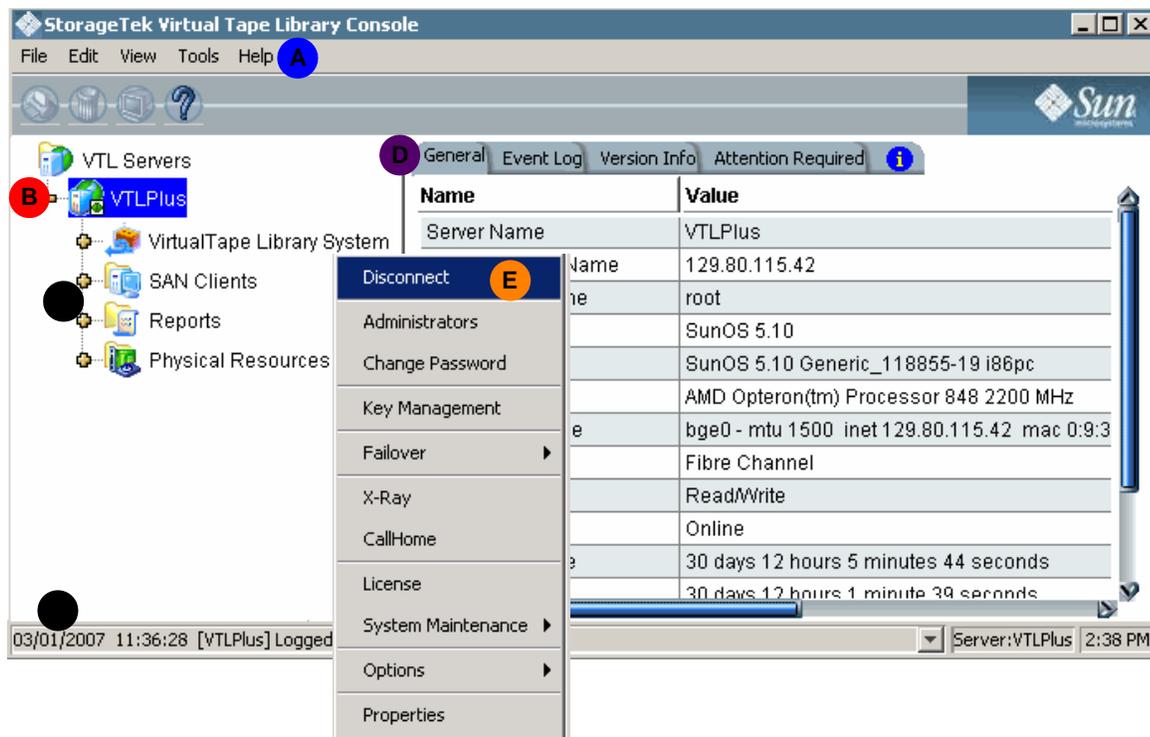
Once you have logged in to the server, clicking on the plus (+) symbol next to the icon expands the server branch of the interface, revealing the sub-components of the VTL system: the `Virtual Tape Library System`, `SAN Clients`, `Reports`, and `Physical Resources` (**C** above).

Clicking on the plus (+) symbol next to any icon expands the corresponding branch of the object tree, revealing the sub-components and sub-branches that lie beneath it. Clicking on the minus (-) symbol collapses the branch.

Selecting an object in the tree displays a tabbed property sheet for the object in the right-hand pane of the console (**D** above). Right-clicking an object opens a context menu system that lets you change the properties of the object or perform tasks with the object (**E**).

The status bar at the bottom of the window (**F** above) displays versioning information for the locally installed console software. A drop-down box displays console session information.

Virtual Tape Library System

The `Virtual Tape Library System` branch of the object tree is the primary management tool for routine VTL operations. Right-clicking on the subbranches of the `Virtual Tape Library System` gives you access to context sensitive menus that control most of the common VTL management operations.

Virtual Tape Library System icons

The following table explains the icons that represent virtual tape drives and virtual tapes in the console object tree.

Icon	Description
	The **C** icon indicates that a virtual tape drive has compression enabled.
	The **A** icon indicates that a virtual tape is a cache for a physical tape. Requires the Automated Tape Caching option.
	The **S** icon indicates a direct link tape (a link to the physical tape). Requires the Automated Tape Caching option.
	The yellow **O** icon indicates that data has been written to the virtual tape and not yet cached to physical tape.

The structure of the Virtual Tape Library System

The `Virtual Tape Libraries` branch lists the virtual tape libraries that are currently defined. Each virtual tape library contains a virtual tape drive branch containing one or more drives and a virtual tape branch containing one or more tapes, sorted in barcode order. Right clicking on the members of the `Virtual Tape Libraries` subbranch brings up a context menu listing operations that can be performed on the branch. These include:

- assigning virtual tape libraries and/or drive to SAN clients (backup servers).
- creating and deleting virtual tapes
- creating and deleting virtual tape drives
- enabling replication or auto-archiving features for tapes in the library
- setting Automated Tape Caching policies (if you are using this option)
- enabling, disabling, or configuring the tape capacity on demand feature
- moving virtual tapes between slots, drives, and the virtual vault
- modifying tape properties, such as barcodes and write protection

The `Virtual Tape Drives` branch lists the standalone virtual tape drives that are currently defined. Right clicking on the members of the `Virtual Tape Drives` subbranch brings up a context menu listing operations that can be performed on the branch.

The `Virtual Vault` branch lists the virtual tapes that are currently being stored outside the virtual tape libraries, in barcode order. Virtual tapes in the vault can be replicated, exported to a physical tape, or moved to a virtual library or standalone drive. The number of tapes that can be stored in the vault is limited only by the available disk storage space.

The `Import/Export Queue` branch lists the import and export jobs and Automated Tape Caching jobs that have been submitted. If needed, you can cancel a pending job from here. You can have up to 32 concurrent import/export jobs running, depending upon the number of physical tape drives attached to your VTL.

The `Physical Tape Libraries` branch lists the physical tape libraries that are available to VTL. Right clicking on the members brings up a context menu that lets you inventory slots, import/export or move physical tapes, copy the physical tape to virtual tape, or link physical tape to virtual tape for direct access.

The `Physical Tape Drives` branch lists the standalone physical tape drives that are available to VTL. Right clicking on the members brings up a context menu that lets you eject physical tapes, copy physical tapes to virtual media, or link physical tapes to virtual media for direct access.

The `Replica Resources` branch lists the virtual tapes that have been replicated from a remote server. Clients do not have access to replica resources.

The `Database` branch contains configuration information for the VTL. The database can be mirrored for high availability.

SAN Clients

The `SAN Clients` branch of the VTL object tree lists the backup servers that back up data to VTL libraries. By right-clicking on this branch and its subbranches, you can add SAN clients, assign them to libraries, unassign them, view client properties, etc.

Reports

The `Reports` branch of the VTL object tree holds reports that you generate. Reports can cover:

■ throughput

- physical resource allocation and configuration
- disk space usage
- Fibre Channel adapter status and configuration
- replication status
- virtual tape and library information
- job status

By right-clicking on this branch, you can select and generate reports.

Physical Resources

The `Physical Resources` branch of the VTL object tree lists Fibre Channel HBAs and storage devices attached to the VTL server. Storage devices include the disk volumes that hold virtual tapes, physical tape libraries and physical tape drives. Right-clicking on this branch or its subbranches brings up context menus that let you scan devices or prepare devices for use as virtual tape.

The following table describes the icons that describe physical resources in the console object tree:

Icon	Description
	The **T** interface icon indicates that this is a target port.
	The **I** interface icon indicates that this is an initiator port.
	The **D** interface icon indicates that this is a dual-port interface card.
	The red arrow indicates that this interface has no access to storage. Either a device is not connected to the interface, or the device is down.
	The **V** icon indicates that this disk has been virtualized.
	The **D** icon indicates that this is a physical ("**D**irect") device.
	The **F** icon indicates that this is shared storage and is being used by another server. The `Owner` field lists the other server.

CHAPTER **4**

VTL operations

This chapter covers routine configuration, administration, and management of server nodes, virtual tape libraries, drives, and tapes, including:

- "Managing network connectivity" on page 31
- "Managing virtual libraries" on page 37
- "Managing tapes" on page 90
- "Managing tape caching" on page 124
- "Creating and viewing reports" on page 127
- "Encrypting and shredding data" on page 131
- "Working with the Event Log" on page 139
- "Managing VTL servers" on page 144.

Managing network connectivity

VTL appliances use your Ethernet local area network (LAN) for system management and administration and your storage area network (SAN) for connecting to the system's storage clients (your backup hosts). Sun services personnel establish required connectivity during the system installation process. However, if you subsequently make changes to your network configurations, you can update the VTL configuration using the procedures in this section.

- "Configuring local area network connections" on page 32
- "Setting the VTL server node host name" on page 34
- "Obtaining SAN interface configuration information" on page 35
- "Administering SAN client connections" on page 36.

▼ Configuring local area network connections

1. **In the** `Network Configuration` **property sheet, enter the** `Domain name` **(A below). Check the** `Append suffix to DNS lookup` **check box (B) if the customer needs to append the domain name to the machine name during DNS lookup.**
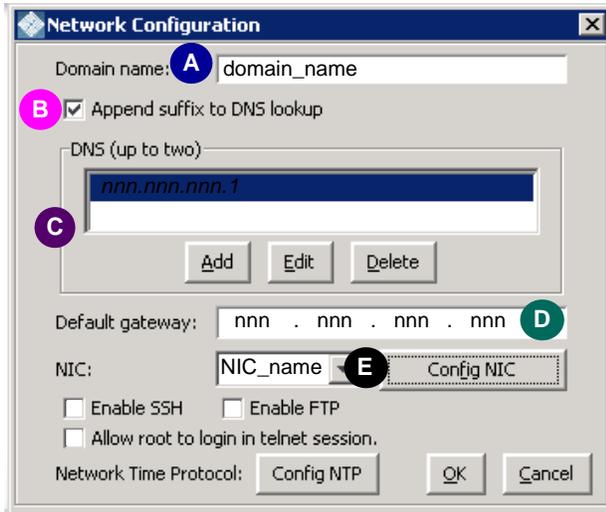
2. **Enter IP address information for the Domain Name Server (if used) in the** `DNS` **section (C above), using the** `Add` **and** `Edit` **buttons.**

3. **Enter the IP address of the** `Default gateway` **(D above).**

4. **Select the** *NIC_name* **Ethernet interface, and push the** `Config NIC` **button (E above).**

   NIC_name is `nge0` on VTL Plus systems and `e1000g0` on VTL Value systems.

   On VTL Plus systems, do not change the configuration of the other Ethernet interfaces. They are reserved for system use. For details, see the appendix on VTL private network addresses.

5. **When the** `IP Address Configuration` **property sheet appears, click the** `Static` **radio button (F below).**
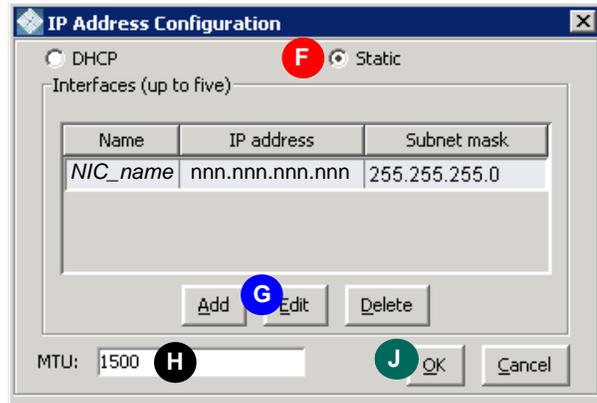
6. **Click the** `Edit` **button (G above), and enter the IP address that the customer provided.**

7. **Leave the** `MTU` **text field (H above) as set by the factory.**

8. **Press** `OK` **(J above).**

   You return to the `Network Configuration` property sheet.

9. **If Network Time Protocol (NTP) is in use, press** `Config NTP` **(K above). When the Network time Protocol Servers dialog appears, use the controls provided (L) to enter the NTP server IP addresses. Click** `OK` **(M).**
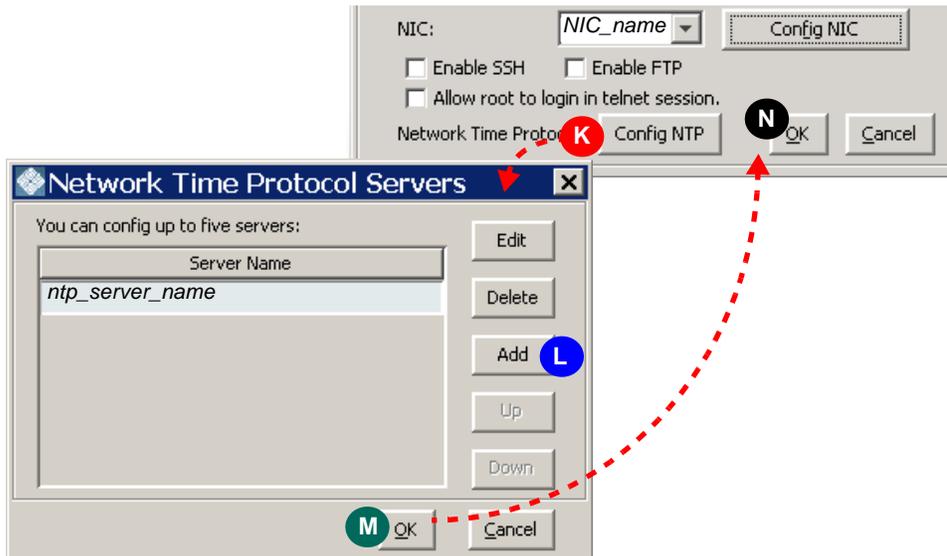
Note the `Enable SSH`, `Enable FTP`, and `Allow root to login in telnet session` check boxes. While `ssh` is enabled by default, `ftp` and remote login by root are disabled for security reasons. Sun recommends that you leave these options set to the defaults. For secure remote access, use the `vtladmin` account with `ssh` or `sftp`. Then, if root privileges are required, use the `su` command after logging in.

10. **When you return to the** `Network Configuration` **property sheet, click OK (N above).**

11. **When you are prompted to restart the network, press** `Yes` **(O below).**
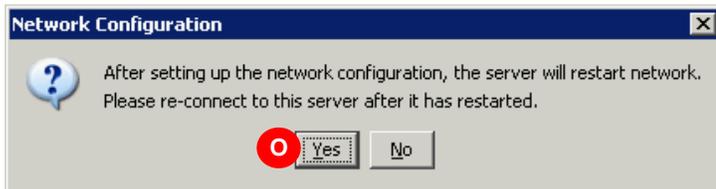
The network should restart automatically.

12. **Reconnect to the VTL server node.**

Stop here.

▼ Setting the VTL server node host name

1. **When the** `Set Hostname` **dialog appears, enter a valid name for your VTL appliance (A below).**
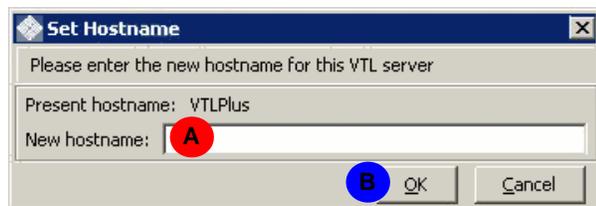
Valid characters include letters, numbers, underscores, and dashes.

2. **Press** `OK` **(B above).**

3. **When prompted to restart the network and server, press** `Yes` **(C below).**
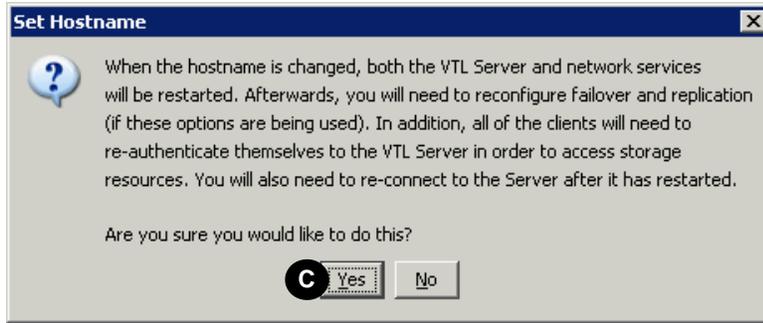
4. **Log back in to the server to continue working.**

Stop here.

▼ Obtaining SAN interface configuration information

You can obtain the configuration information for any of the Fibre Channel host bus adapters on the VTL server by examining the object in the VTL console.

1. **In the tree-view pane of the VTL console, select** `Physical Resources` **(A below) and** `Storage HBAs` **(B).**
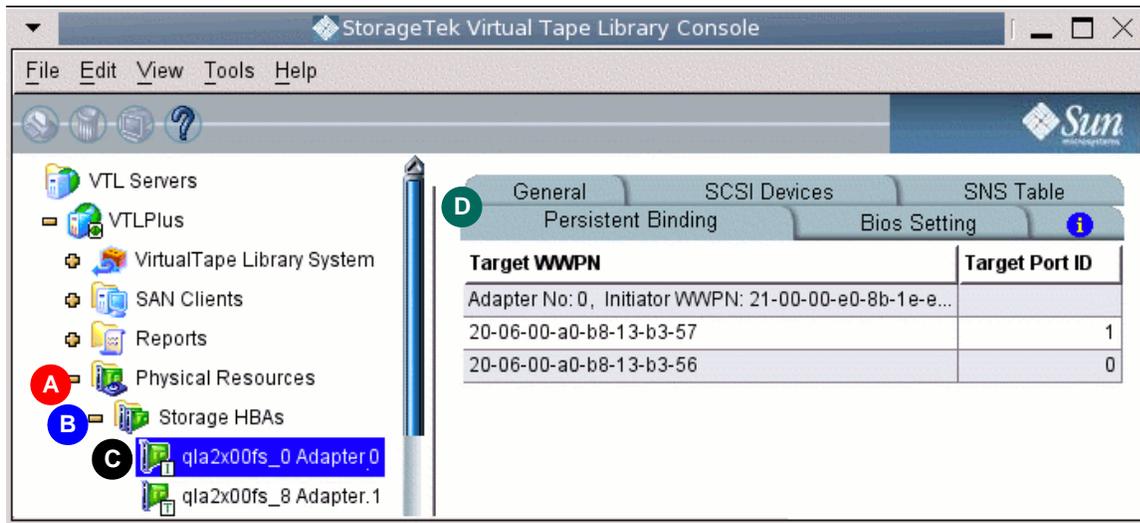
2. **Select the HBA that you wish to check (C above), and, in the pane at right, use the tabs to locate the required information (D).**

Stop here.

▼ Administering SAN client connections

You can obtain the configuration information for any of a VTL server's SAN clients by examining the object in the VTL console, as described below.

To add a SAN client, see "Connecting virtual libraries with storage clients" on page 68.

1. **In the tree-view pane of the VTL console, select SAN Clients (A below) and click on the name of the client (B).**

2. **In the pane at right, use the tabs to see adapter information (C above).**

3. **To see virtual device assignments, expand the client node (D below) and** `Fibre Channel` **protocol node (C) of the tree view.**
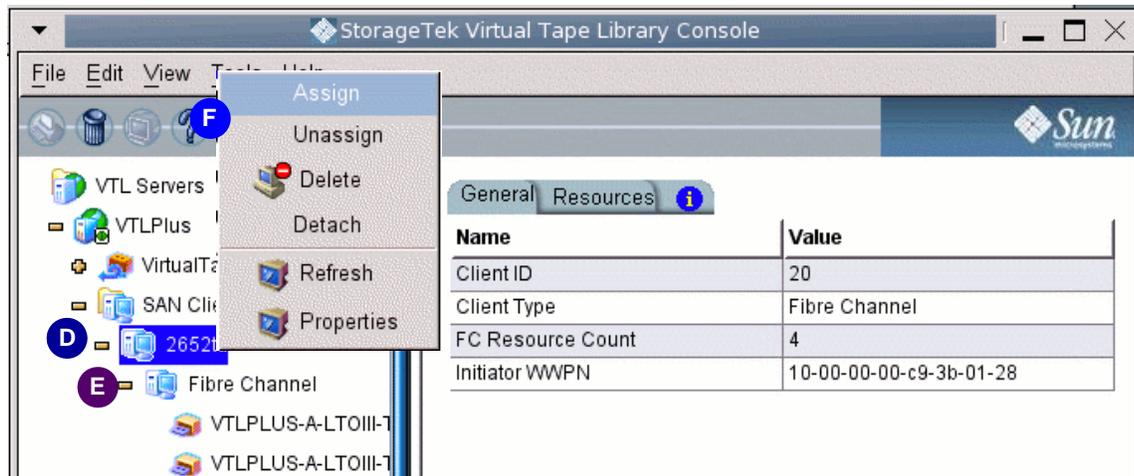
4. **Right-clicking on the client node (D above) or** `Fibre Channel` **protocol (C) node opens a menu of administrative actions (F).**

Using the context menu, you can `Assign` virtual devices to clients, `Unassign` virtual devices from clients, `Delete` the client or protocol, `Detach` devices, and view or refresh client properties.

Stop here.

Managing virtual libraries

This section covers the essential configuration tasks that are performed whenever virtual libraries, devices, and media are added to the VTL system. During initial configuration, the tasks in this section are run sequentially by the VTL configuration wizard. During routine system maintenance, you may also run them independently, as described below:

■ "Configuring and provisioning virtual libraries" on page 43 (includes "Creating virtual tape libraries" on page 45 and "Creating virtual tapes" on page 60)

■ "Connecting virtual libraries with storage clients" on page 68.

Configuring physical libraries and devices

VTL software supports either direct-attached libraries or, optionally, shared libraries managed by ACSLS/Library Station software.

- If you are using a direct-attached library, see "Managing direct-attached physical tape storage" on page 38.
- If you are using a shared library, see "Managing ACSLS and Library Station tape pools" on page 42.

Managing direct-attached physical tape storage

If you have a direct-attached library or device, you must assign the library or device to VTL using the VTL console software. Carry out the following tasks:

- "Preparing physical libraries and devices for assignment" on page 38
- "Assigning direct-attached physical tape libraries/devices" on page 41.

▼ Preparing physical libraries and devices for assignment

1. **If you have not added a new physical library or tape device, stop here and go to the next task.**

2. **Otherwise, in the object tree of the VTL console, right-click the** `Physical Resources` **node (A below), and select** `Prepare Devices` **from the context menu (B).**
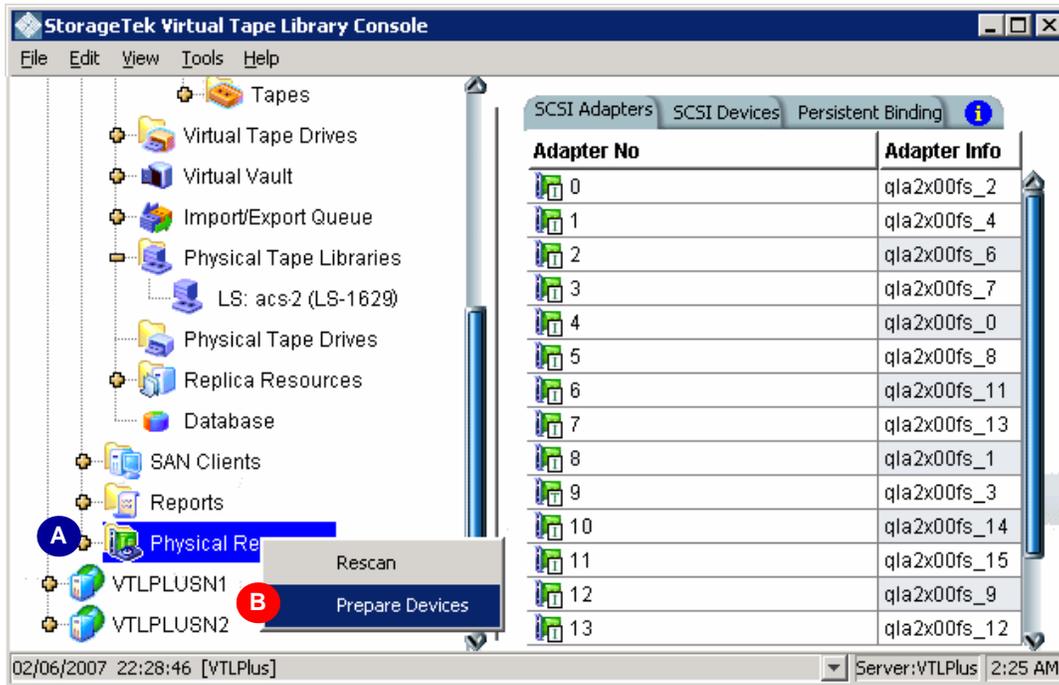
3. **When the** `Select a Preparation Operation` **dialog appears, click the** `Prepare Device(s)` **radio button (C below).**

4. **Select** `Reserved for Direct Device` **from the** `Device Category` **list control (D above), and press** `Next` **(E).**

5. **When the** `Select Physical Devices` **panel appears, use the check boxes and/or the selection buttons (F below) to select the libraries or devices that you want to assign to the VTL system. Press** `Next` **(G).**

   If you are configuring an IBM iSeries/AS400 solution, assign IBM Magstar 3590E11, 3592, or Ultrium LTO1, LTO2, or LTO3 physical drives to the virtual tape library for use in import and export operations.

Physical Devices Preparation Wizard ☒

Select Physical Devices

Select physical devices to be Direct

*	Device Name	SCSI Address	Size(MB)	Category
☑	HP:Ultrium 3-SCSI	0:0:0:0	0	Unassigned
☑	HP:Ultrium 3-SCSI	1:0:0:0	0	Unassigned
☑	HP:Ultrium 3-SCSI	2:0:0:0	0	Unassigned

☑ Continue to process the rest of the devices when an error occurs.

(A) Select All   De-Select All

Back   **(B)** Next   Cancel
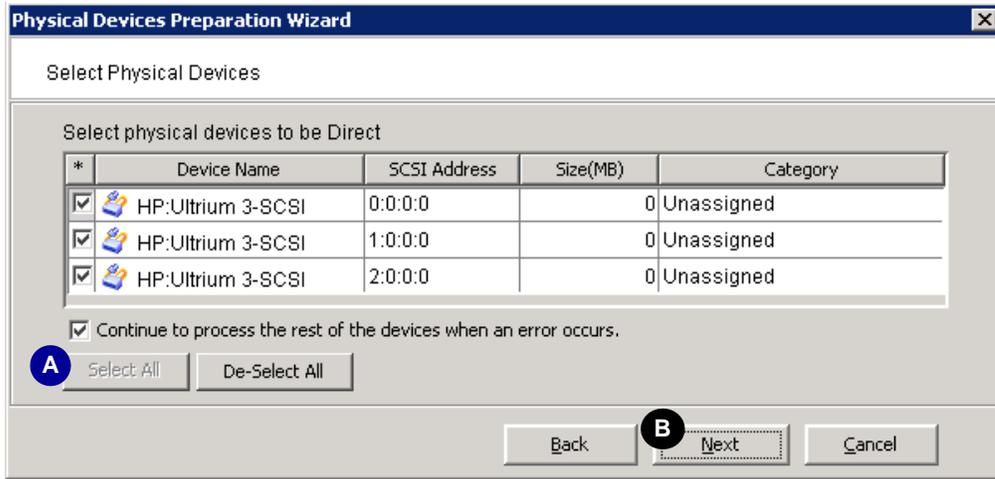
6. **When the** `Prepare Device` **panel appears, press** `Finish`**.**

Next task: "Assigning direct-attached physical tape libraries/devices" on page 41.

▼ Assigning direct-attached physical tape libraries/devices

1. In the object tree of the VTL console application, open the branch for the VTL server (A below).
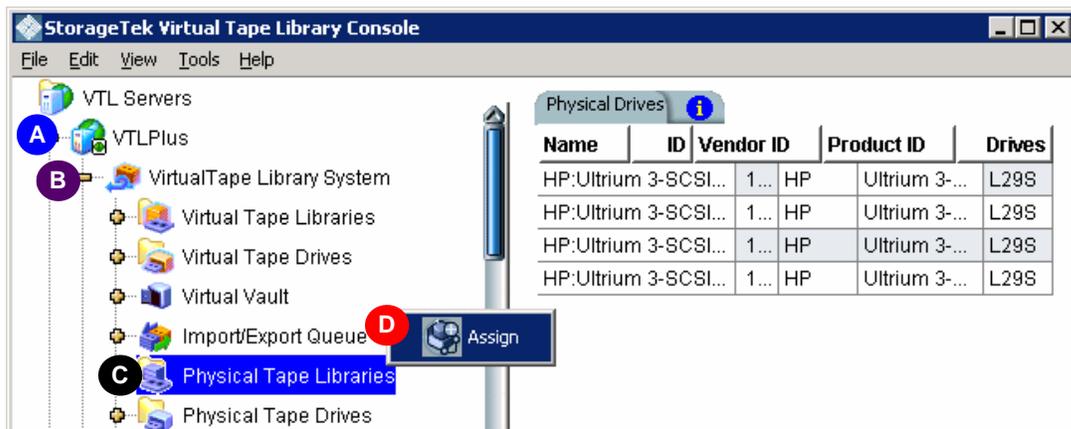
2. Open the branch for the `Virtual Tape Library System` **(B above).**

3. Right-click on the `Physical Tape Libraries` **branch (C above), and select** `Assign` **from the context menu (D).**

4. When the `Select Libraries or Drives` **dialog appears, use the check boxes and or selection buttons (E below) to assign physical tape drives to the VTL system.**
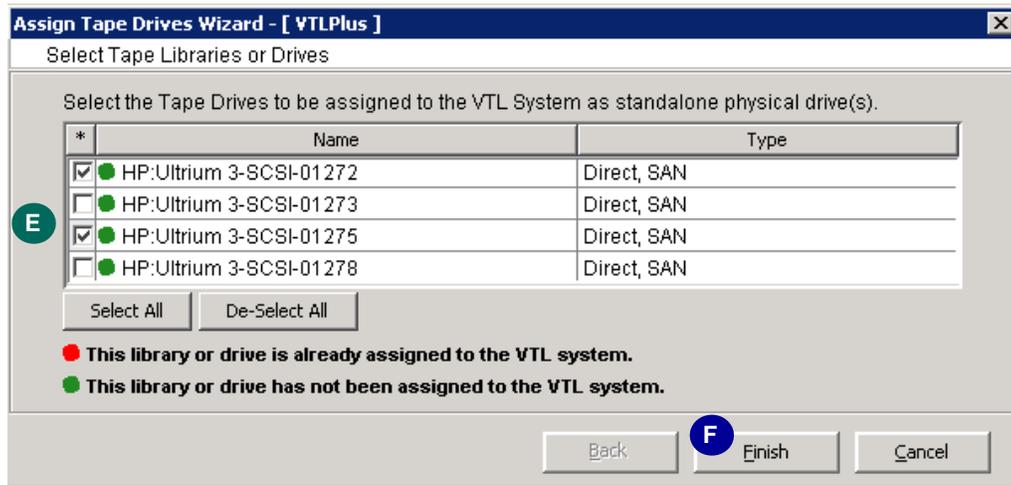
5. Press `Finish` **(F above).**

Stop here.

Managing ACSLS and Library Station tape pools

When the VTL software's ACSLS/Library Station option is enabled, Sun StorageTek ACSLS Manager™ or Library Station software manages the physical library and the tape volumes in the VTL system's assigned tape pools. You merely need to update the VTL console view whenever tapes are added or removed from the pool. Proceed as follows.

▼ Inventorying ACSLS/Library Station libraries from VTL whenever tapes are added to or removed from pools

When you add or remove tapes from an ACSLS/Library Station pool, inventory the tapes through the VTL Console:

1. **In the object tree of the VTL console, open the branch for the VTL server (A below).**

2. **Open the branch for the** `Virtual Tape Library System` **(B below).**

3. **Open the branch for the** `Physical Tape Libraries` **(D below).**

4. **Right-click on the name of the physical library (D below), and select** `Inventory` **from the context menu (E).**

Stop here.

Configuring and provisioning virtual libraries

This section describes the procedures for creating and maintaining virtual libraries, with their virtual drives and media. It documents the following procedures:

- "Setting virtual library system properties" on page 43
- "Creating virtual tape libraries" on page 45
- Setting up optional functionality (see "Configuring Automated Tape Caching" on page 49, "Setting up the Auto Archive feature" on page 53, or "Setting up the Auto Replication option" on page 54)
- "Generating the virtual library" on page 55
- "Creating virtual tapes" on page 60.

▼ Setting virtual library system properties

1. **In the tree view at the left of the VTL console, right-click the** `VirtualTape Library System` **(A below), and select** `Properties` **from the context menu (B).**
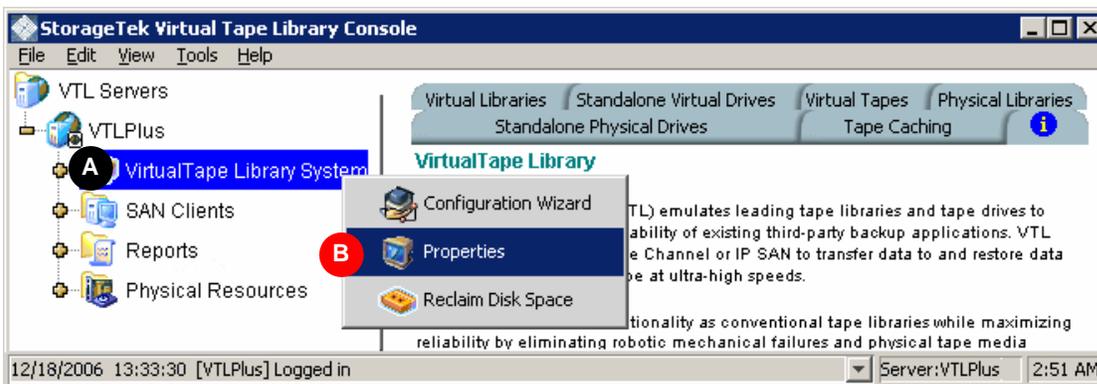
2. **When the** `Change VirtualTape Library` **properties sheet appears, if you wish to use VTL compression software, check the** `Enable Virtual Tape Library compression mode` **check box (C below).**

Consider your requirements carefully before enabling software compression. Software compression is a computationally demanding operation that consumes processor cycles that would otherwise be used to move data. When you enable the feature, you thus trade throughput performance for capacity. Most VTL solutions are aimed at increasing backup performance. VTL storage is used as a fast, temporary repository for data that will be moved to physical tape for long-term storage. In such cases, the hardware-based compression capabilities of physical tape drives provide

both the needed long-term storage capacity and the fastest possible transfer to tape media. Compression hardware cannot further compress data that has been compressed by software, so the end-to-end backup process is significantly slower.

On the other hand, the VTL software compression feature is valuable when it is truly needed:

- when data is stored on the appliance long-term, rather than cached pending migration to long-term storage on physical tape
- when data has to be replicated across a slow WAN link.
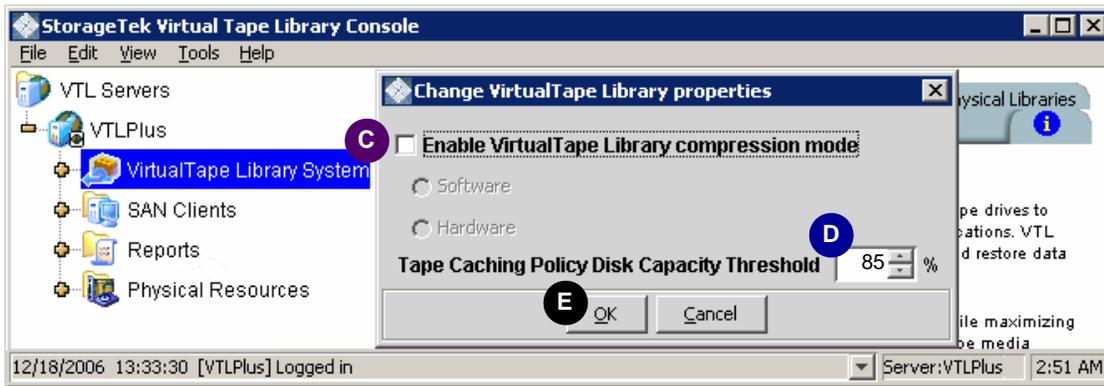
3. **If you plan to use tape caching, use the spinner control to adjust the** `Tape Caching Policy Disk Capacity Threshold` **to 85% (D above).**

When using automatic tape caching, you have to make sure that the disk never fills up, preventing you from creating new virtual volumes. The 75% threshold has been found to offer a good margin of safety.

4. **Press** `OK` **(E above).**

Stop here.

▼ Creating virtual tape libraries

1. **When the** `Create Virtual Library Wizard` **appears, select the type of library that you want to emulate (A below), enter a** `Virtual Library Name` **(B) or use the default, and press** `Next` **(C).**

Select a unique, informative virtual library name. A name that indicates the backup application media server and the function or usage of the library (such as NDMP data migration) is one useful possibility.

Select the `Sun VTL` library type for compatibility with major backup applications, such as Symantec NetBackup. For compatibility with IBM i-Series/AS400 clients, choose the IBM3590, IBM3584, or IBM3583 library type.

Vendor ID	Product ID	Revision	Maximum Drives	Maximum Slots
SPECTRA	GATOR 64000	2.00	32	644
OVERLAND	NEO Series 2000	2.21	2	30
OVERLAND	NEO Series 4100	2.21	4	60
SUN	VTL	3.15	20	678

Virtual Library Name: *mediaServerName_libraryUsage*

Invalid characters for the Resource Name: < > " & $ / \ '
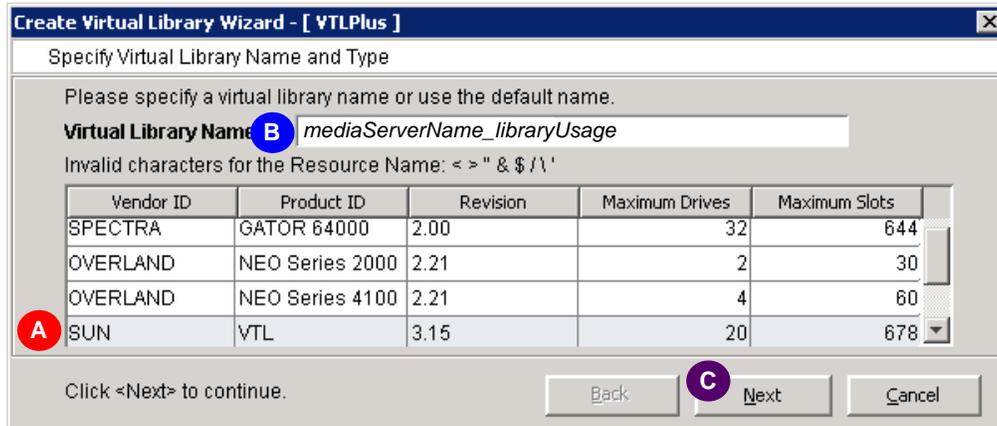
2. **When the** `Enter Virtual Drive Information` **dialog appears, select the type of tape drive you want to emulate (D below), and enter a** `Virtual Drive Name Prefix` **(E).**

Virtual Drive Name Prefix: *virtualLibraryName_make_model-*

Invalid characters for the Resource Name: < > " & $ / \ '

Total Virtual Drives: 10

Vendor ID	Product ID	Media Type
STK	T9840B	T9840B
STK	T9840C	T9840C
STK	T9940B	T9940A
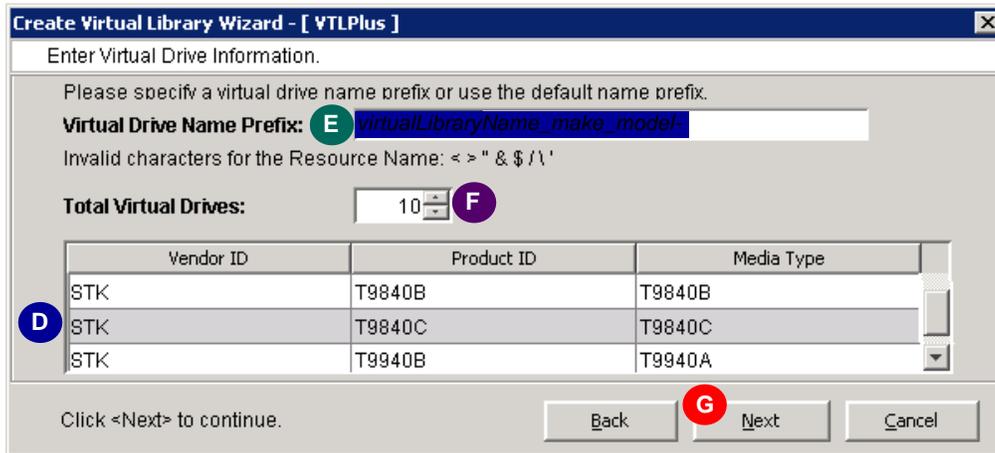
If you plan to attach a physical tape library to the VTL appliance for tape import or export, emulate the physical library so that virtual tapes will be compatible with their physical counterparts.

Select an informative virtual drive-name prefix that shows the relationships between virtual libraries and drives. Using the virtual library name plus the make and model of the emulated drive is one possibility.

3. **Select the** `Total Virtual Drives` **using the spinner control (F above), and press** `Next` **(G).**

To insure that the four target ports on a VTL appliance are fully and evenly utilized, create one virtual library and at least four virtual tape drives for each client (backup server) that connects to the VTL system.

4. **If you are going to use tape caching, check the** `Enable Automated Tape Caching` **check box when the dialog appears (H below). Press** `Next` **to enter the change (J). Then stop here, and go to the Next task list at the end of this procedure.**

5. **If you are not going to use tape caching, press** `Next` **(K below) to skip over the** `Enable and configure tape caching policy` **dialog.**
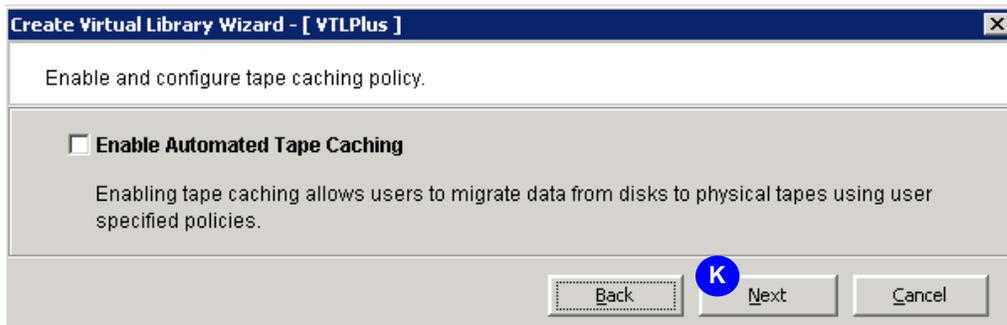
The `Auto Archive/Replication` dialog appears.

6. **If you do not intend to implement autoarchiving or replication, press** `Next` **(L below) to skip over the** `Auto Archive/Replication` **dialog.**
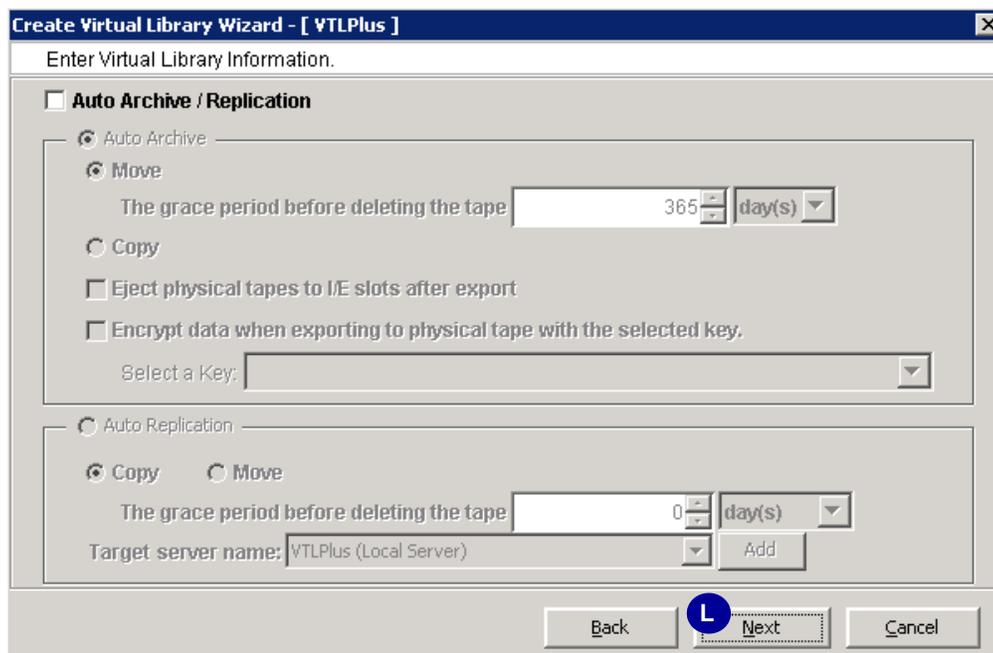
The `Auto Archive` option writes data to physical tape whenever a backup application or utility moves a virtual tape from a virtual library to an import/export slot. The physical tape library must support barcodes: the VTL software has to find a matching barcode in the physical library in order to export a virtual tape to a physical cartridge (you do not need to specify which physical library).

The `Auto Replication` option copies virtual tapes from a virtual library to another VTL server whenever a backup application or utility moves a virtual tape to an import/export slot.

7. Indicate if you want to use tape duplication.

Tape duplication allows you to make up to five duplicate copies of a physical tape whenever virtual tape data is exported to physical tape. You must have at least two identical physical libraries (same model, same number of drives, same tapes with the same barcodes). When data is exported, separate export jobs will be created for each physical library and each job will have a unique job ID.

The duplication job will look for a tape with a matching barcode in another library. If one is found, the data is duplicated to that physical library. If a matching tape is not found, but there are additional identical physical libraries, the system will look for a match there.

Note – You should not have duplicate physical tape barcodes in your system unless you are using tape duplication.

If this library is using Automated Tape Caching or if you selected the Move option for Auto Archive on the previous dialog, the virtual tape data will not be deleted until the duplication job finishes successfully.

Next task:

- If you are going to configure tape caching on this virtual library, go to "Configuring Automated Tape Caching" on page 49.
- If you are going to use the automatic archiving features, go to "Setting up the Auto Archive feature" on page 53.
- If you are going to use the automatic replication feature, go to "Setting up the Auto Replication option" on page 54
- Otherwise, go to "Generating the virtual library" on page 55.

Configuring Automated Tape Caching

You configure Automated Tape Caching for the virtual library by defining a *migration policy* and a *reclamation policy*. A VTL policy is simply a set of criteria (*triggers*) that control how and when VTL software automatically moves data from its physical disk cache. Using the configuration dialogs, you can specify simple schedules or more complex state- and event-driven policies.

Migration policies control when VTL copies data from the disk cache to physical tape. Good migration policies maximize the performance and reliability of the disk cache by minimizing simultaneous reads and writes. Simultaneous reads and writes—cross I/O—force disk arrays to switch back and forth between multiple, competing I/O steams, reducing throughput and subjecting hardware to excessive wear. So best practice is to schedule migration as soon as possible after a backup AND at a time when other backup jobs are not running.

Reclamation polices control when VTL releases the disk space that is used by a data set that has already migrated to tape. Prompt and efficient reclamation prevents over-subscription of the disk and consequent backup failures and system down time, while minimizing investment in cache capacity. Best practice is to reclaim space as soon as the highest demand for restores has passed—typically after three to five days. This approach strikes the best balance between taking advantage of the speed and convenience of a disk-based restore and minimizing consumption of cache space.

To create a migration policy, select one of the following approaches:

- "Creating simple schedule-driven migration policies" on page 50
- "Creating state- and event-based migration policies" on page 50.

Then go to "Creating a reclamation policy" on page 52.

▼ Creating simple schedule-driven migration policies

When the `Please select migration trigger(s)` dialog appears, proceed as follows.

1. Click the `Time Based` **radio button (A below).**

2. **To migrate data every day, click the** `Daily Migration Schedule` **radio button (B below). Using the controls provided (C), enter the time when migration should begin.**

3. **To migrate data every week, click the** `Weekly Migration Check Schedule` **radio button (D below), and specify the day of the week and time of day when migration should begin (E).**
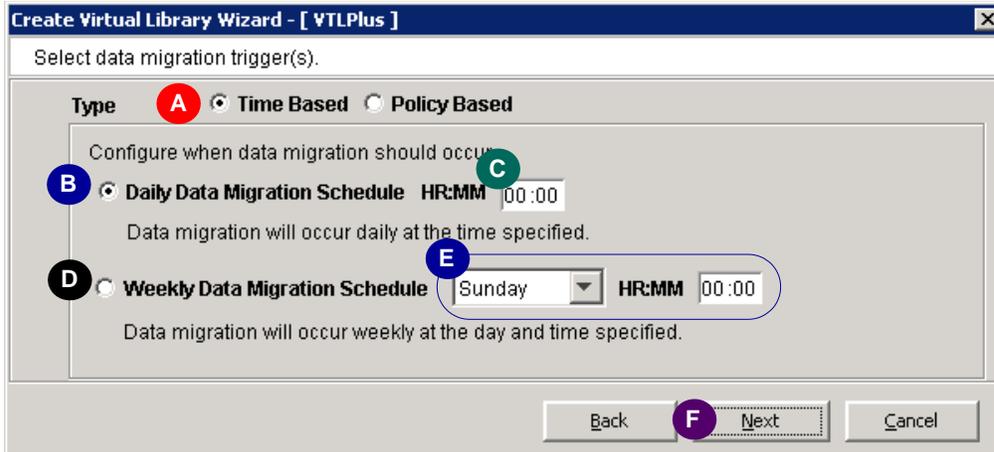
4. **Press** `Next` **(F above).**

Next task: "Creating a reclamation policy" on page 52.

▼ Creating state- and event-based migration policies

When the `Please select migration trigger(s)` dialog appears, proceed as follows.

1. **To migrate data based on the state of data and/or virtual storage, click the** `Policy Based` **radio button (A below).**

2. **To migrate data when ALL of of the conditions specified are satisfied, click the** `And` **radio button (B below).**
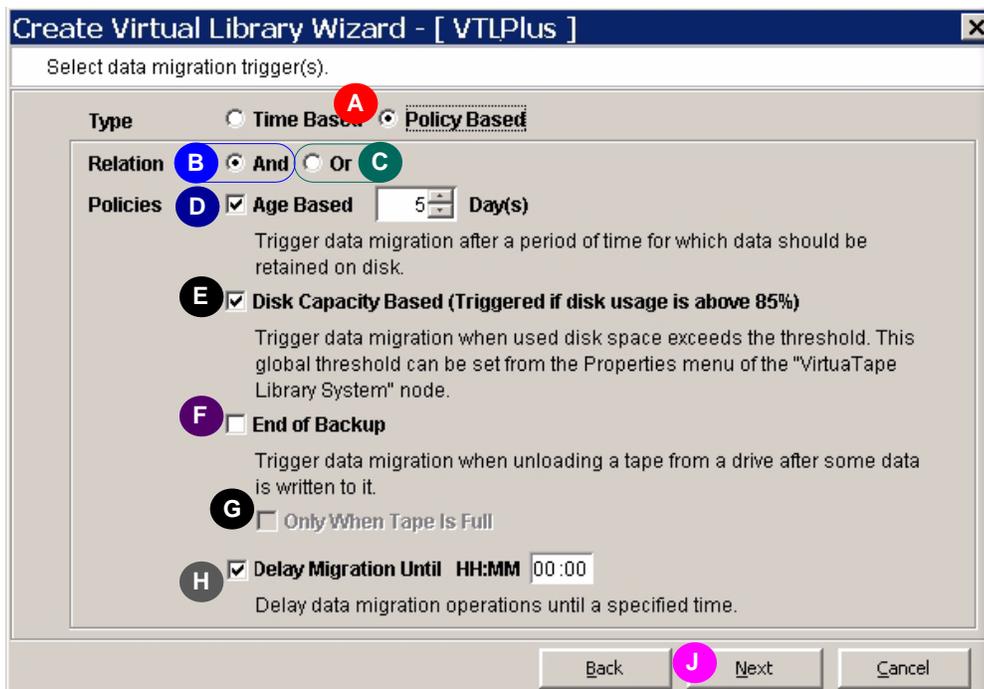
3. **To migrate data when ONE OR MORE of the conditions specified is satisfied, click the the** `Or` **radio button (C above).**

4. **To trigger migration based on the age of the data, check the** `Age Based` **check box, and use the spinner control to select the desired number of days (D above).**

5. **To trigger migration based on disk usage, check the** `Disk Capacity Based` **check box (E above).**

6. **To trigger migration based on the end of a backup job, check the** `End of Backup` **check box (F above). If you want the end of a backp job to trigger migration only when a tape is full, also check the** `Only When Tape Is Full` **check box (G above).**

7. **To delay migration for a specified period following another triggering event, check the check** `Delay Migration Unitl` **check box, and enter the number of hours and minutes for the dealy in the box provided (H above).**

8. **Press** `Next` **(J above).**

Next task:

▼ Creating a reclamation policy

The reclamation policy determines when expired virtual volumes are released. Proceed as follows.

1. **When the** `Please select a reclamation trigger` **dialog appears, click the radio button that corresponds to the desired triggering condition (A below).**

Create Virtual Library Wizard - [VTLPlus]   [×]

Select a reclamation trigger.

(A) ○ **Immediate**

    The cache will be deleted immediately after successful migration.

(B) ○ **Used Space Reaches 85%**

    The cache will be deleted when the used space reaches the threshold.

(C) ◉ **Retention Period**   4 ⬍ **Day(s)**

    The cache will be deleted after data is retained for the specified period of time.

(D) ○ **Never**

    Cache will never be deleted.

                     [Back]   (E)[Next]   [Cancel]

2. **If you choose to specify a** `Retention Period`**, use the spinner control (B above) to specify the number of** `Day(s)`**.**

3. **Then press** `Next` **(C above).**

Next task: "Generating the virtual library" on page 55.

▼ Setting up the Auto Archive feature

1. **When the** `Auto Archive/Replication` **dialog appears, check the** `Auto Archive/Replication` **check box (A below).**
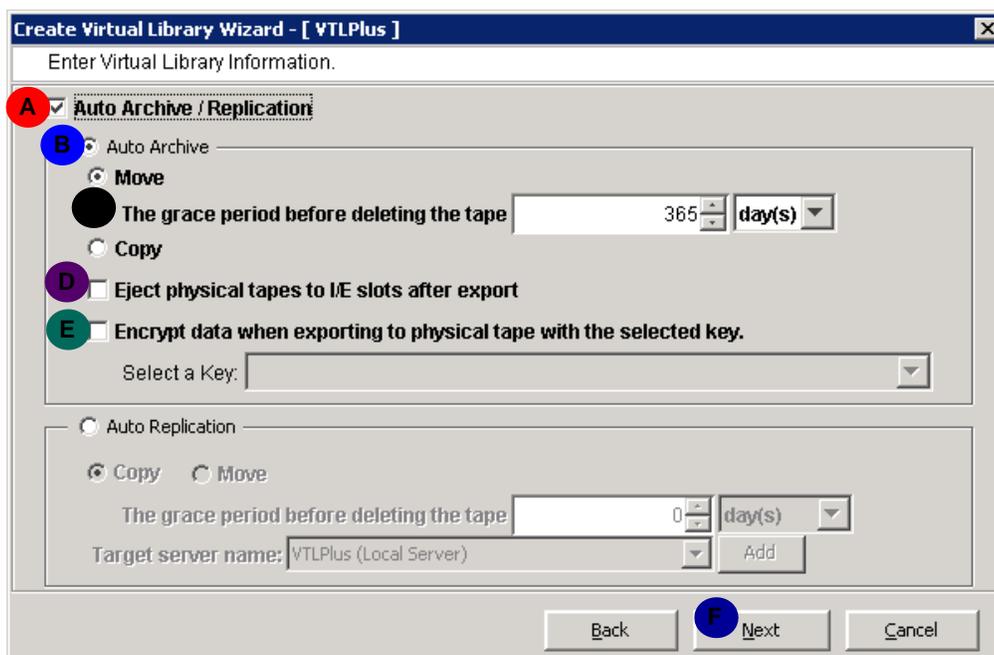
2. **Specify Auto Archive by clicking the** `Auto Archive` **radio button (B above).**

3. **Select the desired archiving behavior by clicking either the** `Move` **radio button (and setting the grace period using the spinner and list controls provided) or the** `Copy` **radio button (C above).**

   The `Copy` option copies the virtual volume to physical media, leaving the virtual volume on disk. The `Move` option deletes the virtual volume from disk once the specified grace period has expired.

4. **If you wish to eject tapes to import/export slots, check the** `Eject physical tapes to I/E slots after export` **check box (D above).**

5. **If you wish to encrypt the archived data, check the** `Encrypt data . . .` **check box, and select a key from the list control provided (E above).**

6. **Press** `Next` **(F above).**

Next task: "Generating the virtual library" on page 55.

▼ Setting up the Auto Replication option

1. **When the** `Auto Archive/Replication` **dialog appears, check the** `Auto Archive/Replication` **check box (A below).**
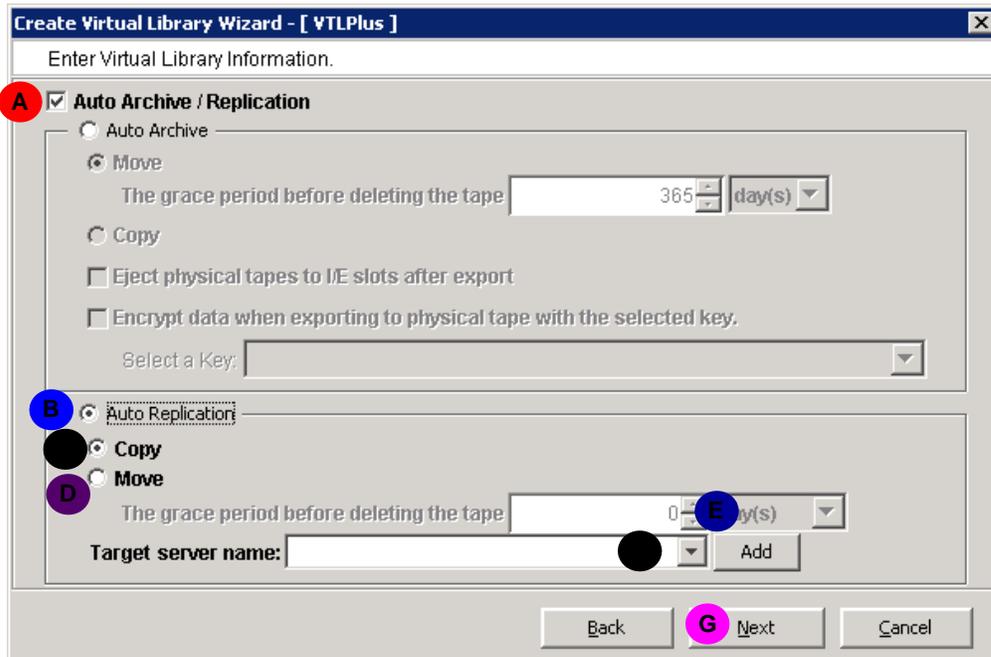
2. **Click the** `Auto Replication` **radio button (B above).**

3. **To copy virtual media to the target library while leaving the source virtual media in the source library, click the** `Copy` **radio button (C above).**

4. **To move virtual media to the target library, deleting the source virtual media, click the** `Move` **radio button (D above). If you want to retain the source volumes in the source library for a specified period before deleting them, define a grace period using the spinner and list controls at right (E).**

5. **Select the** `Remote server name` **for the server that will host the replicated data. Select a name from the list control provided, or press** `Add` **to add a server to the list (F above).**

6. **Press** `Next` **(G above).**

Next task: "Generating the virtual library" on page 55.

▼ Generating the virtual library

Using this procedure, you define the remaining characteristics of your virtual library and media. You supply a barcode range, slot count, and import/export slot count for the library and define the capacity of the media.

Setting the barcode range defines the set of barcodes that the virtual library will support. Each batch of cartridges that you subsequently create must be a subset of the range you define now—you cannot change it later. So Sun recommends setting this value to the widest range possible, `000000-ZZZZZZ`. The virtual library can then support any barcoding scheme that you will ever need.

By default, the slot count for a virtual library is the maximum defined for the Sun L700 physical library that the `Sun VTL` virtual library emulates, `678`. Sun recommends adjusting this value to the maximum possible—`4096`—so that you are not needlessly constrained by it later. Once a library is defined, you cannot change the number of slots that it contains.

Proceed as follows.

1. **When the** `Enter Virtual Library Information` **dialog appears, enter a** `Barcode Starts` **value in the text field provided (A below).**

   The starting value shown, `000000`, allows you the greatest range possible. But whatever you choose, enter exactly six (6) barcode characters when emulating Sun StorageTek libraries—neither more nor less.

2. **Enter a** `Barcode Ends` **value in the text field provided (B above).**

   The ending value shown, `ZZZZZZ`, allows you the greatest range possible. But whatever you choose, enter exactly six (6) barcode characters when emulating Sun StorageTek libraries—neither more nor less.

3. **Using the spinner control provided, adjust the** `Number of Slots` **to** `4096`**, the maximum supported by major backup application software for a single virtual library (C above).**

   In most cases, set the slot number to the maximum value. Once a library is defined, you cannot change the number of slots that it contains, so it makes sense to set this number as high as possible.

   However, if you have to emulate a particular physical library (such as an IBM3590) rather than the `Sun VTL` library type, exercise care when changing the number of slots (or any other library properties). From an application or client point of view, virtual and physical instances of a given library type should generally be functionally identical. If they are not, clients and applications may behave in unanticipated ways.

   Finally, if you set up multiple libraries, you will not be able to create more than 65536 tapes per VTL server node, regardless of the number of slots and libraries configured.

4. **Press** `Next` **(D above).**

5. If you changed the default `Number of Slots`, the VTL software displays the following warning. Press `OK`.

   StorageTek Virtual Tape Library Console

   The slot number "4096" you specified exceeds the number "678" supported by this physical library. Click "OK" to continue if you are sure about it.

   [OK] [Cancel]

6. **When the** `Enter virtual tape properties` **dialog appears, check the** `Tape Capacity On Demand` **check box (E below).**

   Sun recommends capacity on demand for most users.
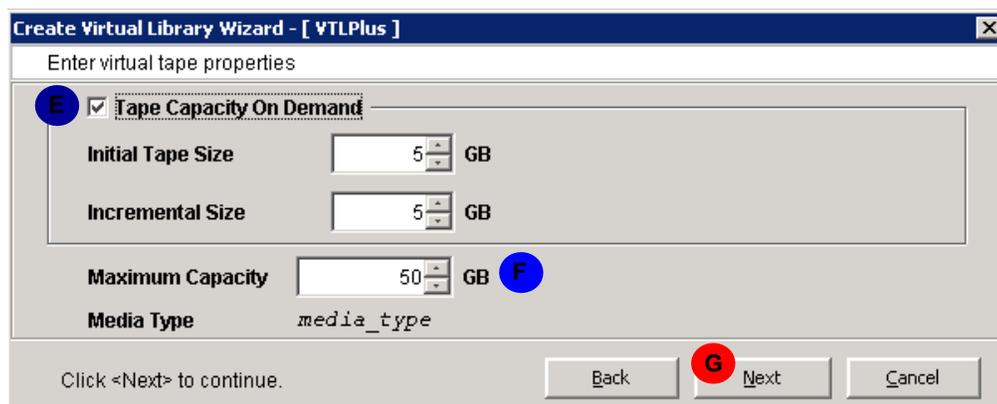
7. **If you are not using tape caching, use the** `Maximum Capacity` **spinner control (F above) to set the maximum size of your virtual tapes to 50-60 GB or to the average size of your backup jobs (whichever is larger).**

   This approach minimizes wasted space in the critical disk cache, where the first copy of each backup job is stored. It maximizes the number of cartridges available for backup jobs at any given time. Your copy/vault software can then consolidate these smaller volumes onto full-sized physical tape cartridges outside the backup window.

8. **If you are using VTL data compression with tape caching, use the** `Maximum Capacity` **spinner control (F above) to reduce the** `Maximum Capacity` **to 85-90% of the encompassed capacity of the selected media.**

   In the example above, you would reduce maximum capacity to 42-43 GB when using compression.

   When you enable tape caching, a single virtual tape has two images, one in the disk cache and one in the tape cache. Both images must be logically identical. But when you use compression with tape caching, you cannot be sure that the disk and tape images will be identical. Different compression algorithms can produce slightly different compression ratios. So, unless you allow a 10-15% margin of safety, you might find that a compressed data set that fills a tape image on disk will not fit on a physical cartridge.

9. **If you are using tape caching, leave the** `Maximum Capacity` **control set to the maximum capacity of the physical media, unless you are also using VTL data compression.**

   The disk and physical-tape images of a virtual tape must be logically identical when you enable tape caching. They cannot be different sizes.

10. **Press** `Next` **(E above).**

11. **When the confirmation screen appears, press** `Finish` **(F below).**
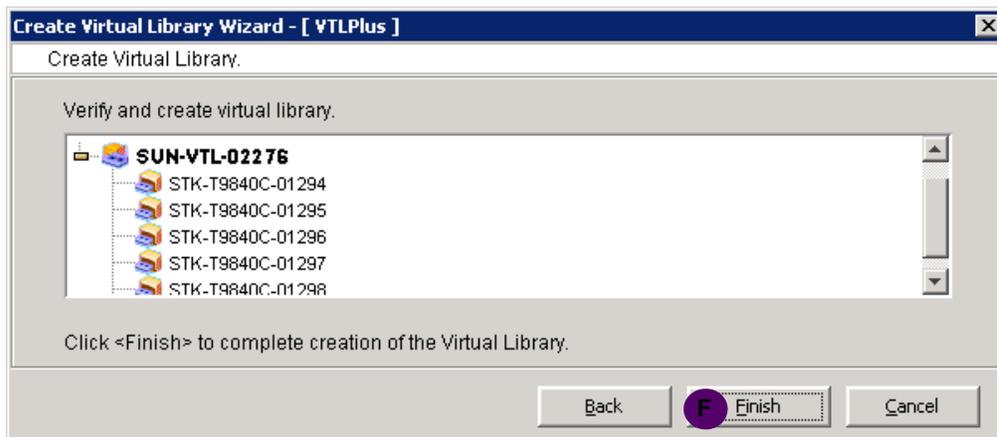
12. **When the** `Batch Creation Status` **panel appears, press** `OK` **(G below).**
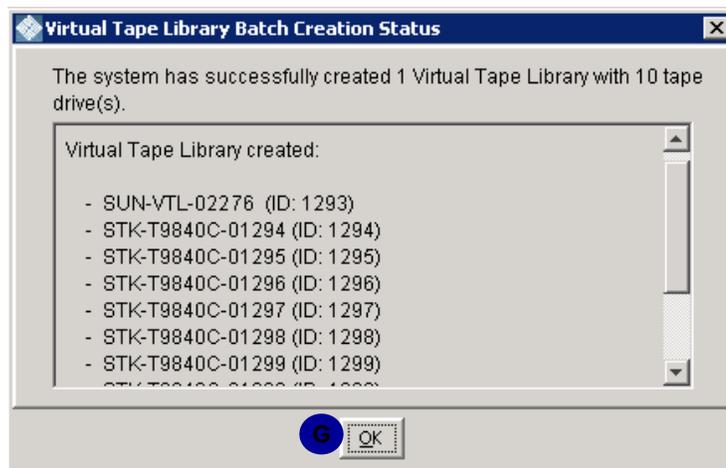
Next task: If you decided to create tapes, go to "Creating virtual tapes" on page 60.

▼ Enabling Auto Replication on an existing library

1. **In the object tree of the VTL console, expand the node for the VTL server.**

2. **Under the VTL server, expand the** `Virtual Tape Library System` **and** `Virtual Tape Libraries` **nodes.**

3. **Under the** `Virtual Tape Libraries` **node, right-click on the virtual tape library that you want to enable, and select** `Properties`**.**

4. **When the** `Change Virtual Library Properties` **property sheet appears, check the** `Auto Archive/Replication` **check box (A below), and click the** `Auto Replication` **radio button (B).**
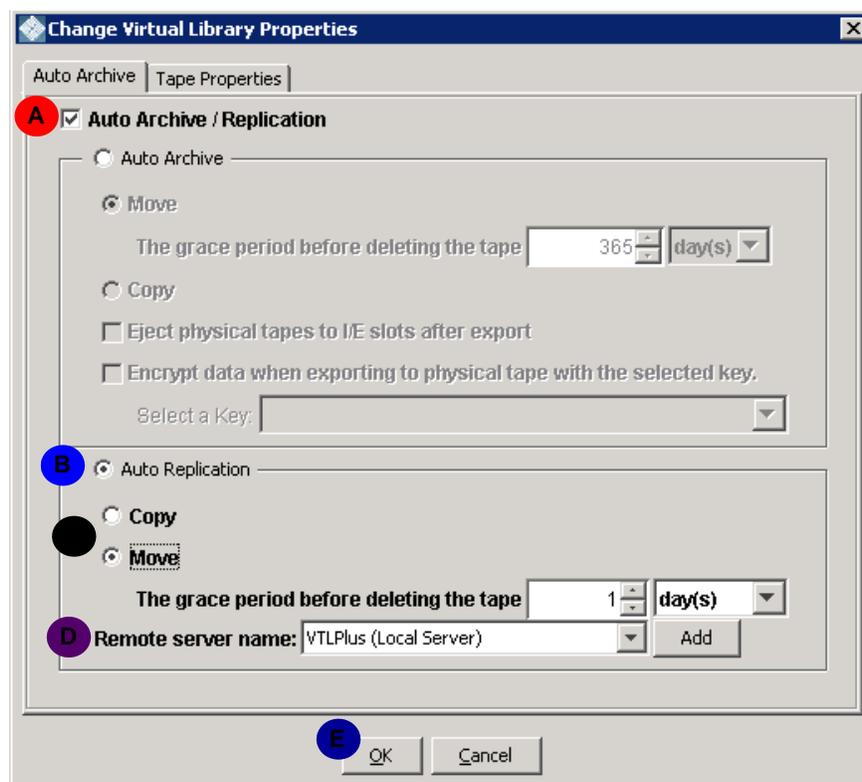
5. **Select the desired replication method by clicking the** `Copy` **radio button or by clicking the** `Move` **radio button and entering a grace period using the list and spinner controls provided (C above).**

6. **Select the** `Remote server name` **for the server that will host the replicated data. Selecting a name from the list control provided, or press** `Add` **to add a server to the list (D above).**

7. **Press** `OK` **(E above).**

Stop here.

Creating virtual tapes

Follow the procedures outlined below:

- "Enabling the advanced tape creation method" on page 60
- "Setting replication parameters for virtual tape volumes" on page 65
- "Launching the virtual tape batch creation process" on page 68.

▼ Enabling the advanced tape creation method

1. **If you have not already done so, from the console main menu, select** `Tools` **(A below), then select** `Console Options` **(B) from the submenu.**

2. **When the** `Console Options` **property sheet appears, make sure that the** `Enable advanced tape creation method` **check box (E above) is checked, and press** `OK` **(F).**
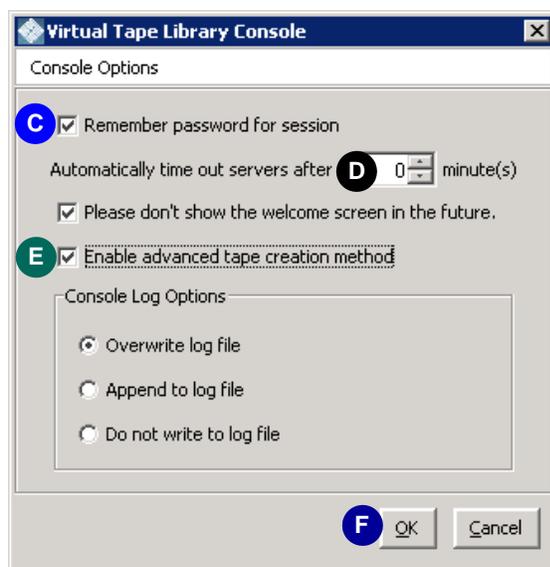
The advanced tape creation method is enabled by default starting with VTL Plus 2.0. Sun recommends the advanced tape-creation method because it makes it easier to avoid creating more virtual tapes than the available disk space can hold and makes it easier to manage multiple virtual tapes in multiple libraries.

When the advanced method is enabled, tape creation dialogs display the available disk space alongside the controls that specify initial tape size and the desired number of tapes. Using this value, you can calculate the maximum number of full cartridges that you can create without oversubscribing the disk. While VTL software

tries to calculate this value for you, it does so using the *currently allocated size* of the virtual tapes. If you are using the capacity on demand feature of the Sun VTL, the currently allocated size is the increment size (typically 5 GB), *not* the full capacity of the emulated media (for example, 40 GB for Sun StorageTek 9840C cartridges). As a result, the software will let you create as many *increment-sized* tapes as will fit in the available disk space, up to the maximum number of slots defined for the library (658 for the `Sun VTL` library type). If you accept this number and create the tapes, the system will run out of disk space long before the tapes appear to be full.

The advanced method also adds a control to the tape-creation interface that lets you assign prefixes to tape names. By assigning the same prefix to both the virtual library and each of its virtual tapes, you can greatly simplify subsequent library management.

Next task: "Selecting physical disk resources for use as virtual tape" on page 61.

▼ Selecting physical disk resources for use as virtual tape

1. **When the** `Select Physical Devices` **dialog appears, press** `Select All` **(A below).**
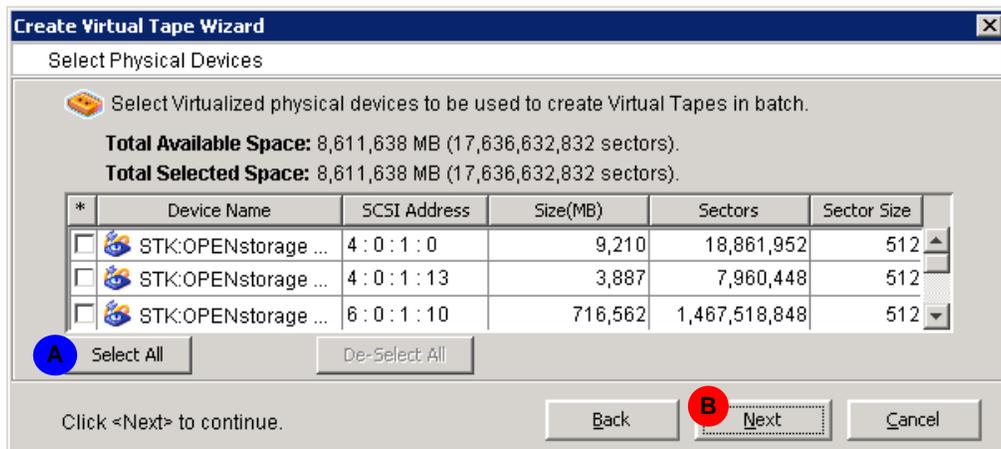
2. **Press** `Next` **(B).**

Next task: at this point, the behavior of the configuration wizard depends on the configuration of the virtual library:

■ If the new virtual tapes will reside in a library that has the Auto Archive option enabled, the wizard displays two additional dialogs at this point, `Select a Physical Tape Library` and `Select Physical Tapes`. So go to "Setting Auto Archive parameters for virtual tape volumes" on page 62.

- Otherwise, the wizard skips directly to the `Specify Batch Mode Information` dialog. So go to "Allocating disk space to virtual tapes" on page 64.

▼ Setting Auto Archive parameters for virtual tape volumes

If the new virtual tapes will reside in a library that has the Auto Archive option enabled, proceed as follows.

1. **In the** `Select a Physical Tape Library` **dialog, check the** `Create virtual tape(s) to match physical tape(s) ...` **check box (A below). Press** `Next` **(B).**
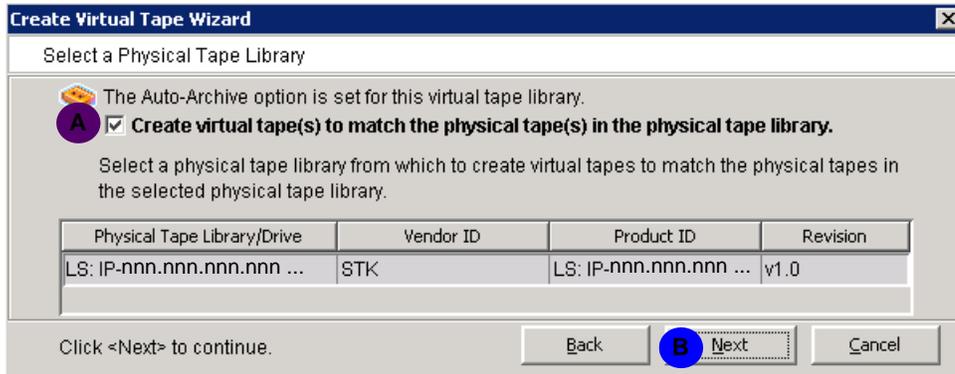
Checking the `Create virtual tape(s) to match physical tape(s) ...` check box insures that the barcodes of the new virtual tapes will match those of the physical tapes, thus fulfilling an essential prerequisite for auto archiving.

2. **In the** `Select Physical Tapes` **dialog , select physical tapes using the check
boxes (C below) and/or button controls provided (D). Then press** `Next` **(E).**
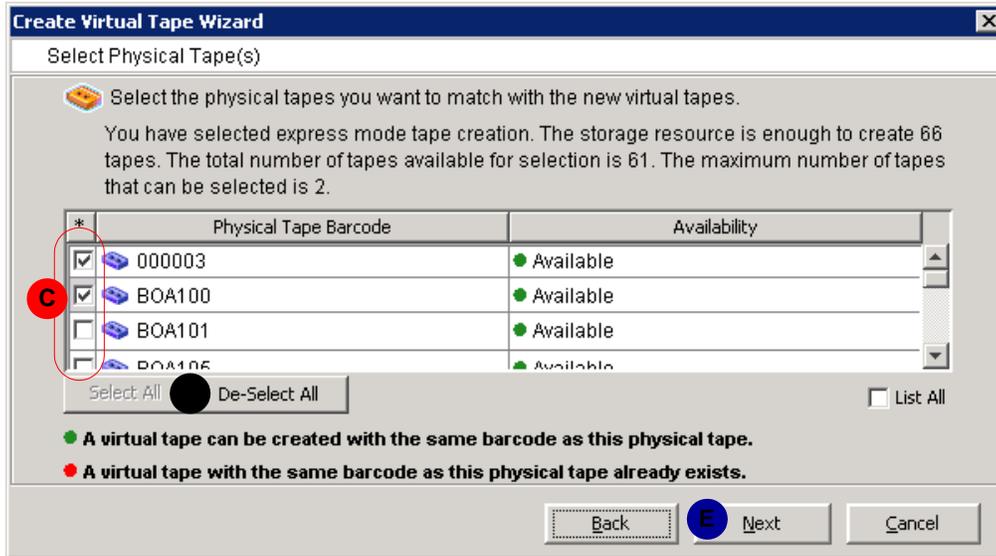
Next task: "Allocating disk space to virtual tapes" on page 64.

▼ Allocating disk space to virtual tapes

1. **When the** `Specify Batch Mode Information` **panel appears, enter a descriptive prefix for the virtual tape labels (A below).**

   Choose a meaning name prefix that shows the relationships between virtual tape volumes and virtual libraries.

Create Virtual Tape Wizard					✕
Specify Batch Mode Information					

Enter the information required to create the Virtual Tapes.

Virtual Tape Name Prefix: *virtualLibraryName*_VTV **A**

Invalid characters for the Resource Name: < > " & $ / \ '

Virtual Tape Size: 36   GB

Starting Number: 1   **Number of Virtual Tapes:**   1   (Maximum: 232)

Total Selected Space: 2,869,932 MB (5,877,620,096 sectors).

Device Name	SCSI Address	Size(MB)	Sectors	Sector Size
STK:OPENstorage D...	4 : 0 : 1 : 5	716,562	1,467,518,848	512
STK:OPENstorage D...	4 : 0 : 1 : 13	3,887	7,960,448	512
STK:OPENstorage D...	8 : 0 : 1 : 3	716,359	1,467,103,104	512

☑ Use default ID for Starting Number.

[Back] [Next] [Cancel]

2. **If you only plan to create one virtual library for your VTL system, you can use all of the available disk capacity for tapes. Enter the** `Maximum` **(B below) as the new value for the** `Number of Virtual Tapes` **(C below).**

Create Virtual Tape Wizard					✕
Specify Batch Mode Information					

Enter the information required to create the Virtual Tapes.

Virtual Tape Name Prefix: *virtualLibraryName*_VTV

Invalid characters for the Resource Name: < > " & $ / \ '

Virtual Tape Size: 36   GB **B**

Starting Number: 1   **Number of Virtual Tapes:**   1   (Maximum: 232)

Total Selected Space: 2,869,932 MB (5,877,620,096 sectors).

Device Name	SCSI Address	Size(MB)	Sectors	Sector Size
STK:OPENstorage D...	4 : 0 : 1 : 5	716,562	1,467,518,848	512
STK:OPENstorage D...	4 : 0 : 1 : 13	3,887	7,960,448	512
STK:OPENstorage D...	8 : 0 : 1 : 3	716,359	1,467,103,104	512

D ☑ Use default ID for Starting Number.

[Back] **E** [Next] [Cancel]

3. **Otherwise, if you plan to create additional libraries later, divide the** `Maximum` **(B above) between the libraries, and enter the number allocated to this library as the** `Number of Virtual Tapes` **(C).**

   The new value has to be less than the `Maximum`, so that capacity is reserved for creating tapes for the additional libraries.

4. **Check the** `Use Default ID for Starting Number` **check box (D above). Press** `Next` **(E).**

5. **When the** `Set Barcode Range Option` **panel appears, check the** `Use the following barcode range for this batch` **check box (F below), and press** `Next` **(G).**

   The `Set Barcode Range Option` panel defines the set of barcodes that the virtual library will support. Each batch of cartridges that you subsequently create must be a subset of the range you define now—you cannot change it later. So Sun recommends setting this value to the widest range possible, `000000-ZZZZZZ`. The virtual library can then support any barcoding scheme that you will ever need.
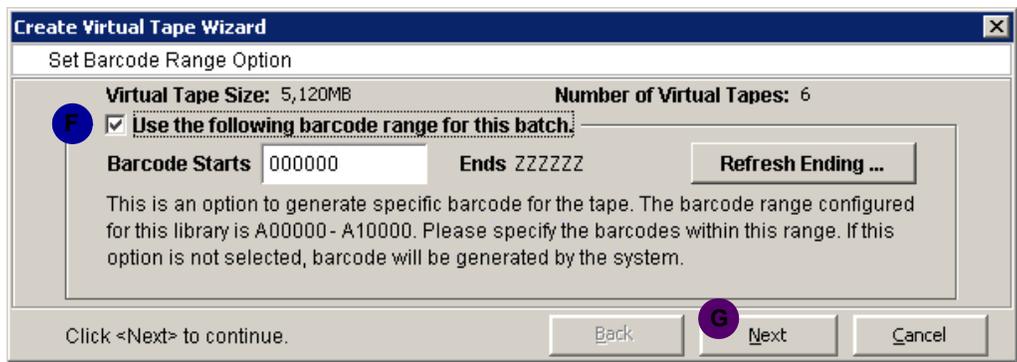
Next task:

- If you are using the Auto-Replication feature, go to "Setting up the Auto Replication option" on page 54.
- Otherwise, go to "Launching the virtual tape batch creation process" on page 68.

▼ Setting replication parameters for virtual tape volumes

If the new virtual tapes will reside in a library that has the Auto-Replication option enabled, proceed as follows.

1. **When the** `Select Target Server for Auto-Replication Option` **dialog appears, check the** `Automatically replicate the virtual tape(s) to the selected target server` **check box (A below).**
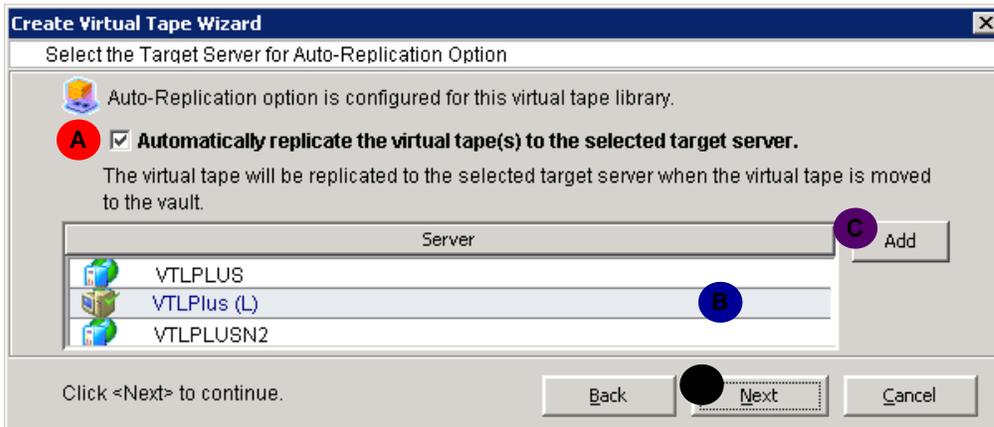
2. **Select the remote server from the list (B above), or press** `Add` **to add a server to the list (C). Press** `Next` **(D).**

3. **When the** `Target Server Information` **panel appears, press** `Next` **(E below).**
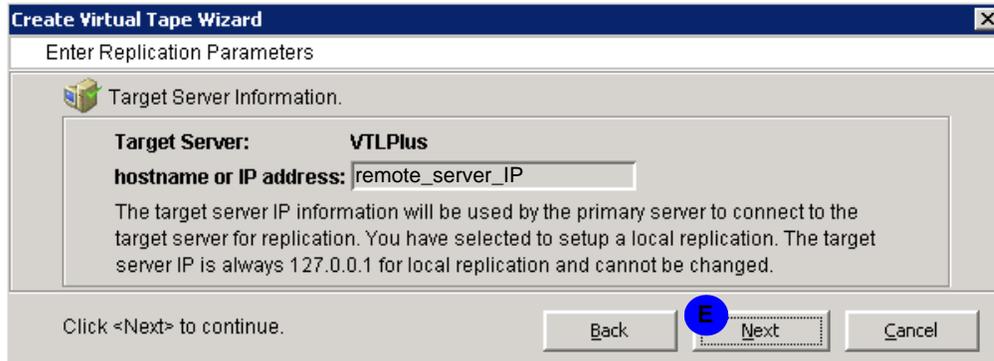
4. **When the** `Specify Replication Timeout and Retry Policy` **property sheet appears, configure timeout and retry intervals using the spinner controls provided (F below). Then press** `Next` **(G).**
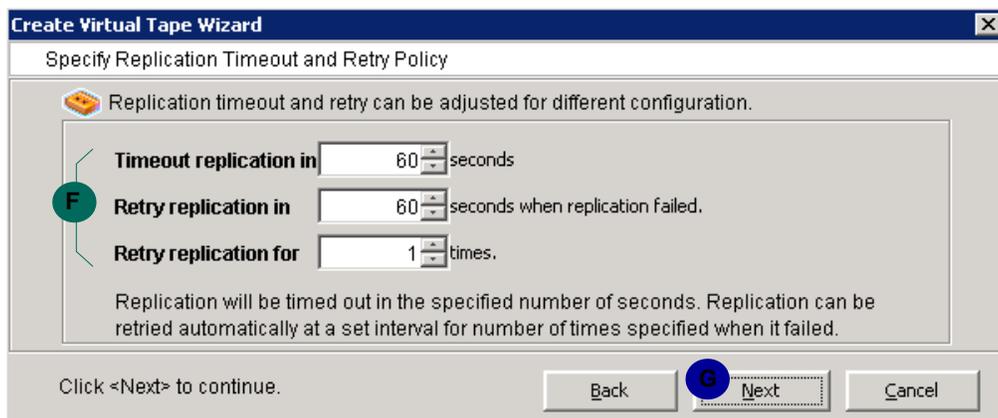
5. **When the** `Specify the Options for Data Transmission` **property sheet appears, check the** `Compress Data` **(H below) check box to enable compression.**

   Compression software can be valuable when transmitting replica data over slow links. However, assess requirements carefully. Consider the operational impact of the additional processor workload and consequent reductions in throughput before enabling this option.
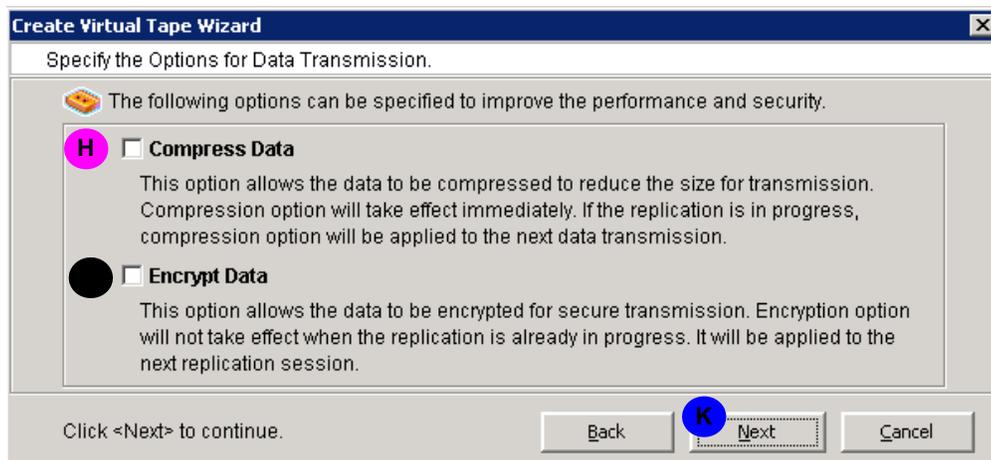
6. **Check the** `Encrypt Data` **check box (J above) to enable encrypted transmissions.**

   Encryption software is often necessary when replicating data over insecure links. However, assess requirements carefully. Consider the operational impact of the additional processor workload and consequent reductions in throughput before enabling this option.

7. **Press** `Next` **(K above).**

Next task: "Launching the virtual tape batch creation process" on page 68.

▼ Launching the virtual tape batch creation process

1. **When the** `Create Virtual Tapes` **summary screen appears, press** `Finish` **(A below).**
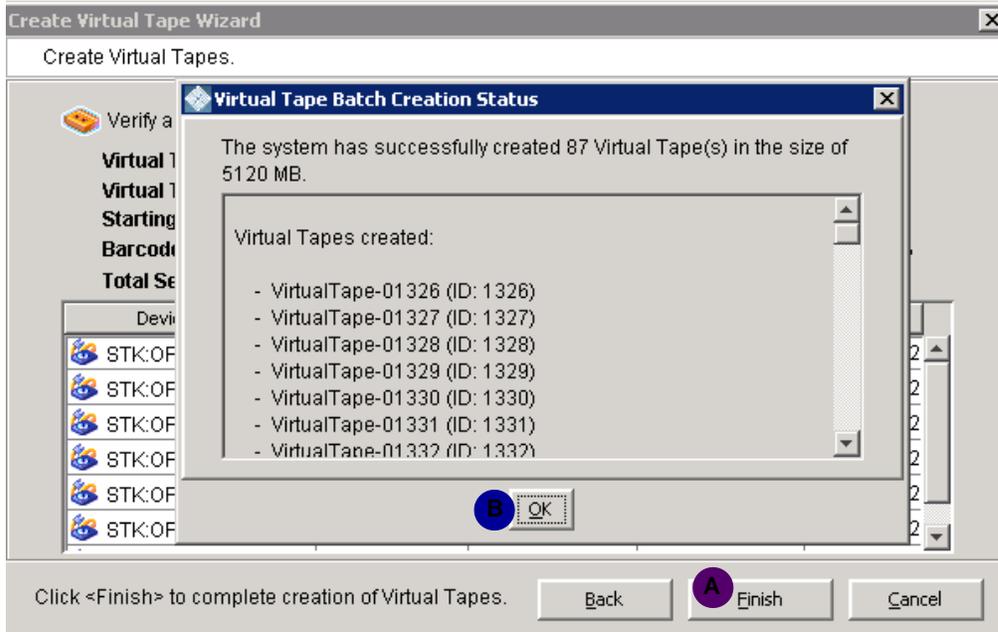
2. **When the batch job finishes and the** `Virtual Tape Batch Creation Status` **panel appears, press** `OK` **(B above).**

   Note that tape creation can take some time, so the status panel will not appear immediately.

Stop here.

Connecting virtual libraries with storage clients

To connect virtual libraries with client machines (typically backup application or NDMP agent hosts), carry out the following tasks:

■ "Starting the Add Client Wizard" on page 69

■ "Adding Fibre Channel SAN clients" on page 70

■ "Assigning virtual libraries to storage clients" on page 73.

▼ Starting the Add Client Wizard

1. In the tree menu of the VTL console, select the VTL server branch.

2. Right-click the SAN Clients branch (**A** below).

3. Select Add from the context menu (**B** below).
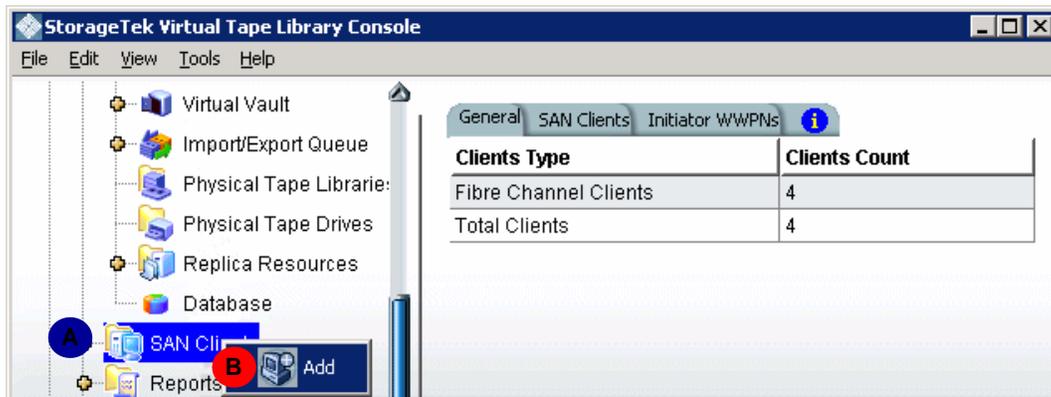
Next task: "Adding Fibre Channel SAN clients" on page 70.

▼ Adding Fibre Channel SAN clients

1. **When the** `Enter the Generic Client Name` **dialog appears, enter the client name in the text field provided (A below). Press** `Next` **(B).**

   The client is typically an ACSLS server or a backup application host, such as a Symantec NetBackup master server.
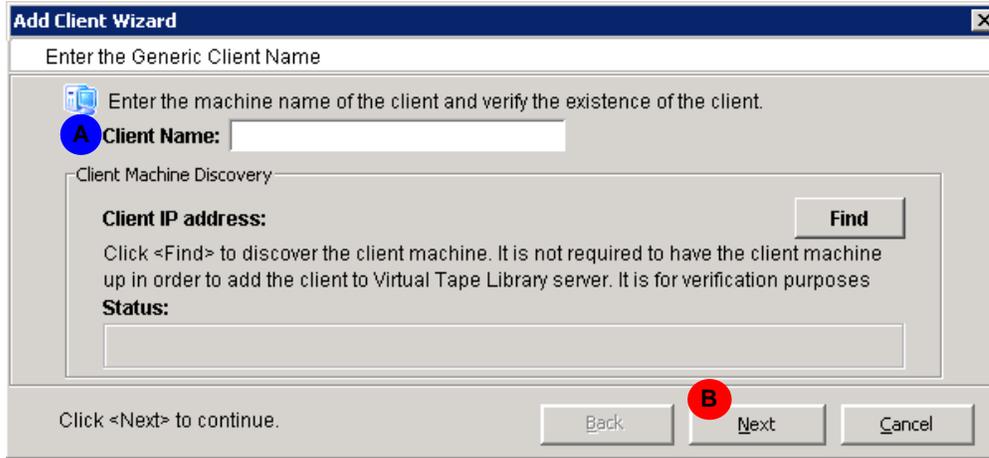
2. **When the** `Select Client Protocols` **dialog appears, check the** `Fibre Channel` **check box (C below), and press** `Next` **(D).**
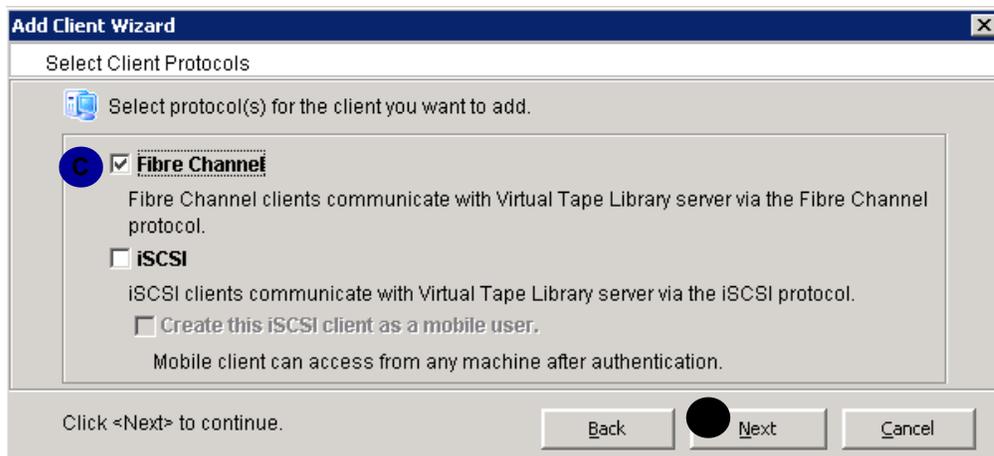
3. **When the** `Set Client Fibre Channel Properties` **property sheet appears, select the World Wide Port Name (**`WWPN`**) of the initiator by checking the corresponding check box (E below), or press the** `Add` **button (F), enter a new** `Initiator WWPN`**, and press** `OK` **(G). Then press** `Next` **(H).**
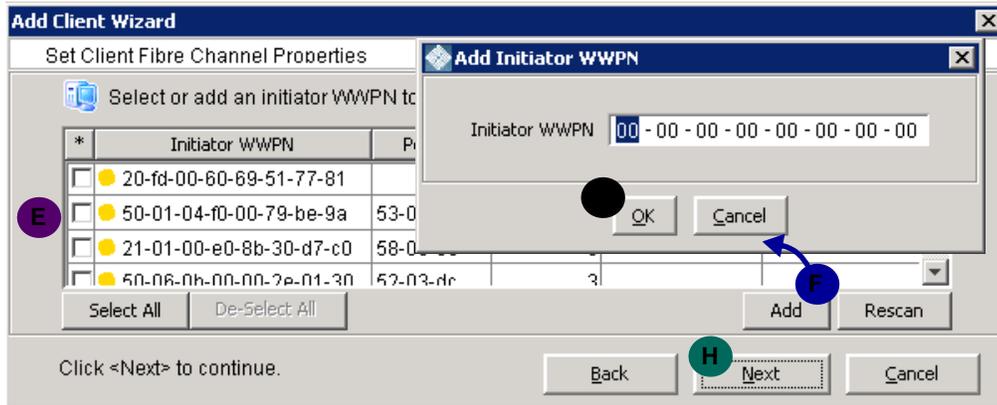
4. **When the** `Fibre Channel Option` **panel appears, check the check boxes for any optional support that the client requires (J below). Then press** `Next` **(K).**
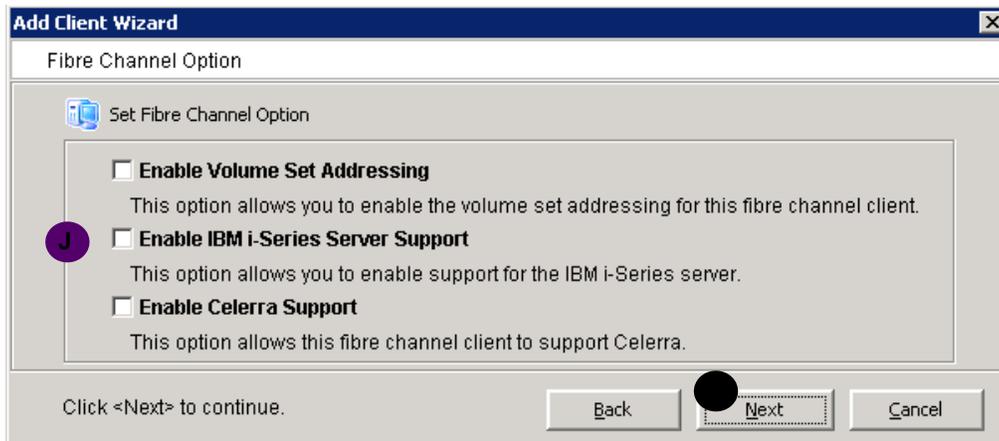
5. **When the** `Add the Generic Client` **summary screen appears, press** `Finish`
   (L below) to add the client.
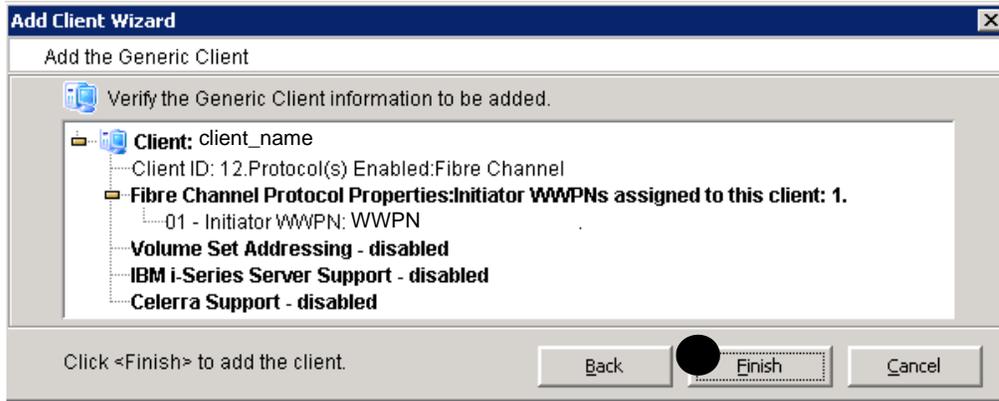
Next task: "Starting the Assign a Virtual Tape Library Wizard" on page 72.

▼ Starting the Assign a Virtual Tape Library Wizard

VTL storage clients are the backup application hosts that manage your backup jobs.
To assign libraries to clients, proceed as follows.

1. **Open the** `Assign a Virtual Tape Library Wizard` **by right-clicking on the
   object-tree node for virtual library, and selecting** `Assign` **from the context menu
   (A below).**
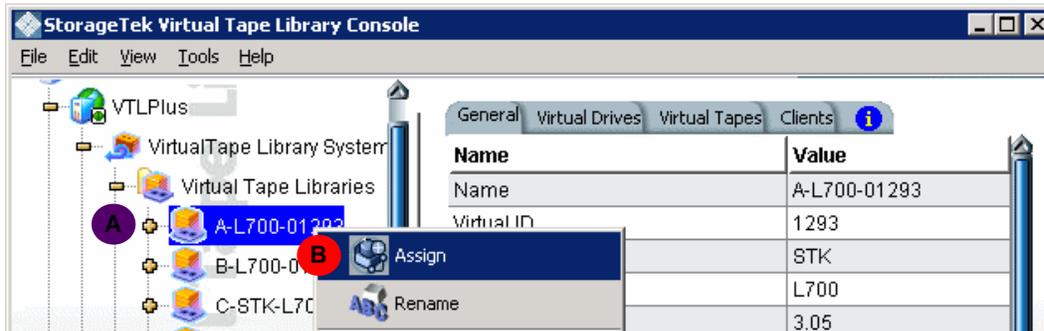
2. **Press** `Next` **(B above).**

Next task: "Assigning virtual libraries to storage clients" on page 73

▼ Assigning virtual libraries to storage clients

1. **When the** `Assign a Virtual Tape Library Wizard` **appears, check the** `Assign the tape library and all drives...` **check box (A below), select a client (B), and press** `Next` **(C).**

   As a general rule, assign one library per client.
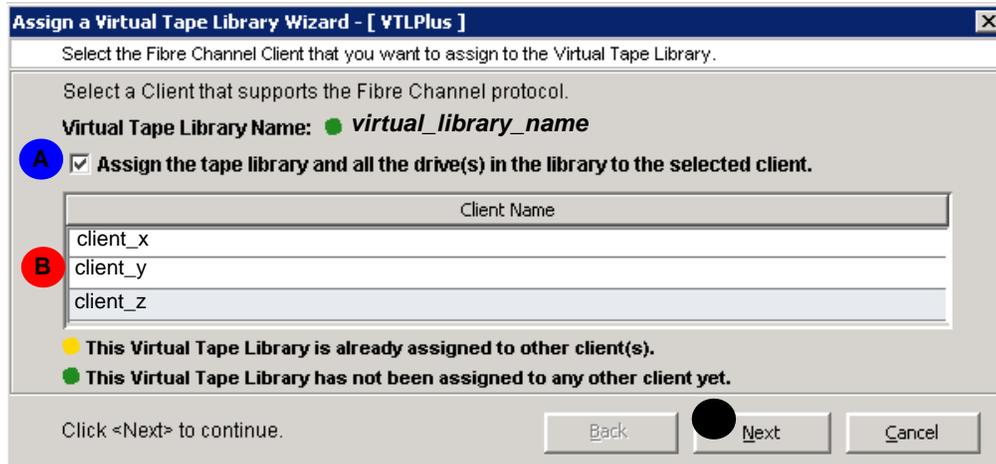
2. **When the** `Select a Fibre Channel Target` **panel appears, select the** `Target WWPN` **that you will zone to the client from the list (D below), and press** `Next` **(E).**

   To insure that the four target ports on the VTL appliance are fully and equally utilized, assign a minimum of four virtual tape drives per client.
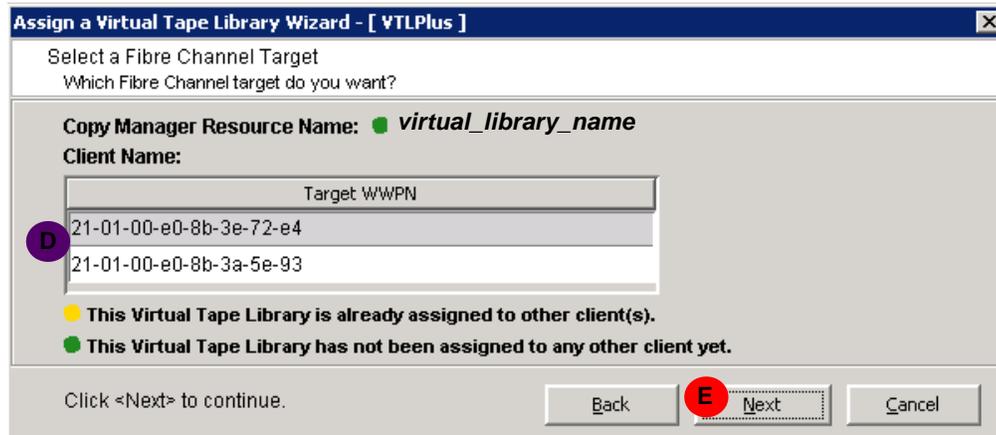
3. **When the** `Assign a Fibre Channel Client to the Virtual Tape Library` **confirmation screen appears, press** `Finish` **(F).**
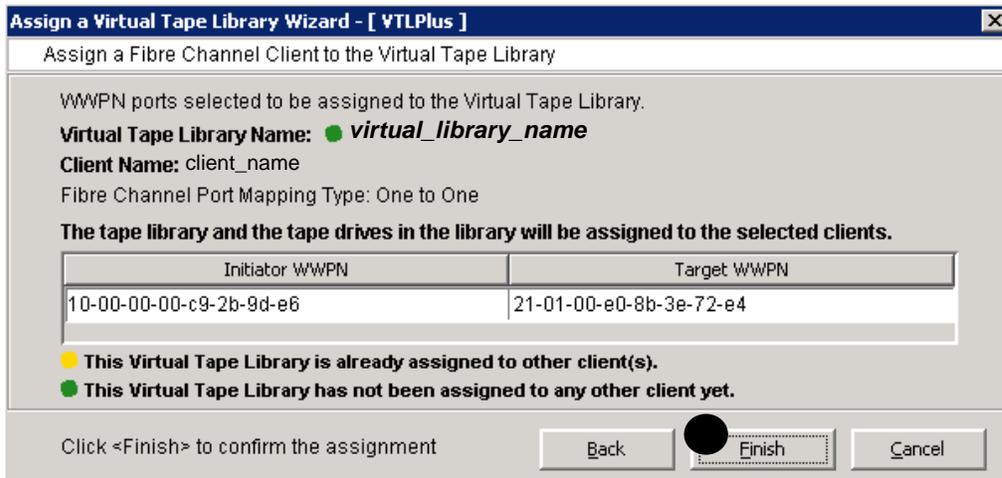
4. **Log in to each VTL client (each backup server), and scan for new Fibre Channel devices.**

Stop here.

Controlling VTL virtual libraries with ACSLS

If you plan to administer VTL virtual libraries using the Sun ACSLS application, you need to carry out the following tasks:

- "Discovering SAN virtual libraries from the ACSLS host" on page 74
- "Creating ACSLS host driver instances for virtual libraries" on page 75
- "Adding virtual libraries to the ACSLS configuration" on page 77.

▼ Discovering SAN virtual libraries from the ACSLS host

1. **Log in to the ACSLS server as** `root`.

2. **Configure all Fibre Channel-connected virtual libraries into the system with the** `devfsadm` **command:**

```
[ACSLS_server]root:# ./devfsadm
```

3. Perform a configuration reboot:

```
[ACSLS_server]root:# ./reboot -- -r
```

Next task: "Creating ACSLS host driver instances for virtual libraries" on page 75.

▼ Creating ACSLS host driver instances for virtual libraries

Once you have discovered the newly attached VTL virtual libraries, proceed as follows.

1. Log in to the ACSLS server as `root`**.**

2. Change to the the home directory of the `ACSSS` user**,** `$ACSSS_HOME`**:**

```
[ACSLS_server]root:# cd $ACSSS_HOME
```

The default location of `$ACSSS_HOME` is /export/home/ACSSS.

3. Quiesce ACSLS with the `kill` **command:**

```
[ACSLS_server]root:# ./kill.acsss
kill.acsss: Bringing down ACSLS
kill.acsss: ACSLS is down
```

A message that states that the PID file does not exist means that ACSLS was not running.

4. Obtain the World Wide Names (WWNs) for the remote Fibre Channel ports that connect the new virtual libraries. Run the `cfgadm` **command with the** `show_SCSI_LUN` **option, and check the output for the WWNs of** `med-changer` **devices:**

The WWNs are part of the `Ap_Id` string, located between the controller number and the LUN number:

```
[ACSLS_server]root:# ./cfgadm -o show_SCSI_LUN -al
Ap_Id                       Type          Receptacle   Occupant      Condition
c2                          fc-fabric     connected    configured    unknown
c2:: 202700a0b811158a ,0    unavailable   connected    configured    unknown
c2:: 210000e08b8a0bc2 ,0    med-changer   connected    unconfigured  unknown
c2:: 210000e08b8affc2 ,1    med-changer   connected    unconfigured  unknown
c2:: 202700a0b811158a ,31   disk          connected    configured    unknown
c2:: 210000e08b8a0bc2 ,1    disk          connected    configured    unknown
c2:: 210100e08ba57d7c ,2    med-changer   connected    unconfigured  unknown
```

5. **Edit the file** /usr/kernel/drv/mchanger.conf, **adding an entry for each virtual library that the oeprating system discovered.**

   Each library entry includes a driver name (mchanger), a parent driver (fp, the Solaris Fibre Channel port driver), a driver class (scsi), a logical unit number (lun), and a World Wide Name for the remote Fibre Channel port (fc-port-wwn):

```
[ACSLS_server]root:# vi /usr/kernel/drv/mchanger.conf
name="mchanger" class="scsi" target="is" lun="by"
name="mchanger" class="scsi" target=0 lun=0;
name="mchanger" class="scsi" target=0 lun=1;
name="mchanger" class="scsi" target=0 lun=2;
name="mchanger" parent="fp" class="scsi" lun=0 fc-port-wwn="210000e08b8a0bc2";
name="mchanger" parent="fp" class="scsi" lun=1 fc-port-wwn="210000e08b8affc2";
name="mchanger" parent="fp" class="scsi" lun=2 fc-port-wwn="210100e08ba57d7c";
:wq
[ACSLS_server]root:#
```

6. **Unload the unattached driver** mchanger:

```
[ACSLS_server]root:# ./rem_drv mchanger
```

7. **Change to the install subdirectory of the ACSSS home directory,** $ACSSS_HOME, **and execute the driver installation script,** install_scsi_sol.sh.

   The default location of $ACSSS_HOME is /export/home/ACSSS.

```
[ACSLS_server]root:# cd /export/home/ACSSS/install
[ACSLS_server]root:# ./install_scsi_sol.sh
Installing 64-bit mchanger
Probing for libraries...
/export/home/ACSSS/utils/probeFibre.sh[46]: test: argument expected
 Unable to auto-sense any fibre-attached libraries.
```

8. **When the script fails to find libraries and asks if any are attached, enter** y **(yes).**

```
Are there additional libraries attached? (y or n): y
```

9. **Enter a space-delimited list of target:LUN pairs, one pair for each library.**

```
Enter the target:LUN pair corresponding to each library.
Separate target:LUN pairs with a space.
example: 4:0 5:0 5:1 5:2
==> 0:0 0:1 0:2# General form = Target:LUN e.g. 0:1
Use target 0 LUN 0
Use target 0 LUN 1
Use target 0 LUN 2
```

10. When prompted, confirm your entries by entering `y` **(yes).**

The script builds the driver instances for the specified libraries:

```
Is this correct? (y or n): y

Building an mchanger instance for each library...
Successfully built the following...
        /dev/mchanger0: STK L700 678-cells 10-drives
        /dev/mchanger1: STK L700 678-cells 10-drives
        /dev/mchanger2: STK L700 678-cells 10-drives
```

11. Load the driver:

```
[ACSLS_server]root:# ./add_drv mchanger
```

12. Change to the ACSSS home directory, and start ACSLS:

```
[ACSLS_server]root:# cd ../
[ACSLS_server]root:# ./rc.acsss
Copyright 2007 Sun Microsystems, Inc. All rights reserved.
    Use is subject to license terms.
NOW IN SU - ACSSS.
Copyright 2007 Sun Microsystems, Inc. All rights reserved.
    Use is subject to license terms.
[ACSLS_server]root:#
```

13. Change to the `acsss` **user account:**

```
[ACSLS_server]root:# su - acsss
[ACSLS_server]acsss:$
```

Next task:

▼ Adding virtual libraries to the ACSLS configuration

Once you have created driver instances for the VTL virtual libraries, add the libraries to the ACSLS host configuration using the following procedure.

1. Start the `config acs new` **utility:**

```
[ACSLS_server]acsss:$ config acs new
  2008-03-20 10:28:07
  Enter the new ACS Configuration details
```

2. When you are asked if the `ACS` **(Automated Cartridge Subsystem) is in a partitioned library, enter** `n` **(no):**

```
Is ACS in a partitioned library? (y or n): n
Number of connections to ACS: 1
Device or host - ACS, connection #0:
2008-03-20 10:28:13
Obtaining Configuration details, please wait
2008-03-20 10:28:13
Configuration Details for ACS # 2
 Partition ID                 Not partitioned
 Number of LSMs                     1
 Number of Ports                    1
   Port Name                    /dev/mchanger2
   Port Status                  Communicating
 LSM Details
 Lsm # 2,0 :
 ---------
 Lsm Type                     700
 Number of CAPS                     1
 Number of PTPS                     0
 Number of Panels                   4
 Number of Drives                  10
 Number of Available cells       678
 For details about this configuration change, please look in acsss_config.log.
```

3. When you are prompted, confirm the changes by entering `y` **(yes):**

```
Enter 'y' to confirm changes to the acs configuration for this ACS : y
2008-03-20 10:28:16
Please wait, Configuration update is in progress...
2008-03-20 10:28:18
ACS configuration updated.
```

4. **Wait for 60 seconds (one minute), then start the ACSLS command preocessor,** `cmd_proc`**:**

```
$ cmd_proc
                        (c) Copyright (2004)
                   Storage Technology Corporation
                        All Rights Reserved

This material is confidential and proprietary to StorageTek and
may be licensed only under a valid StorageTek licence. Do not
copy or distribute unless authorized in writing by StorageTek.

If this software is used by the Government, use, duplication, or
disclosure by the Government is subject to restrictions as set
forth in subparagraph (c)(1)(ii) of the Rights in Technical
Data and Computer Software clause at DFARS 2.52.7-7013.


------------------------------ACSLS 7.2.0----------------------------
ACSSA>
```

5. **Audit the newly added libraries. At the** `ACSSA>` **prompt, enter** `audit`**:**

```
ACSSA> audit
        CAP identifier(acs,lsm,cap): 0,0,0
        Type(acs/lsm/panel/server/subpanel): acs
        ACS identifier(acs): 0
        ACS identifier(acs): 1
        ACS identifier(acs): 2
        ACS identifier(acs): 3
        ACS identifier(acs):
Audit: Audit completed, Multiple ACS audit.
Audit: Audit of ACS   0, Valid.
Audit: Audit of ACS   1, Valid.
Audit: Audit of ACS   2, Valid.
Audit: Audit of ACS   3, Valid.
```

6. **Log the configuration events:**

```
ACSSA> log
```

Stop here. The VTL virtual libraries have been configured for ACSLS administration.

Backing up the VTL system configuration

Whenever you change the VTL configuration, you should backup the configuration to a secure location on another machine. This process preserves the virtual tape libraries, virtual tape drives, clients, client assignments, replication configurations, and failover configurations for the server. You can do this in either of two ways:

- "Manually saving the VTL configuration" on page 80
- "Automatically backing up the VTL configuration" on page 80.

▼ Manually saving the VTL configuration

1. **In the object tree of the VTL console, highlight the VTL server node (A below).**
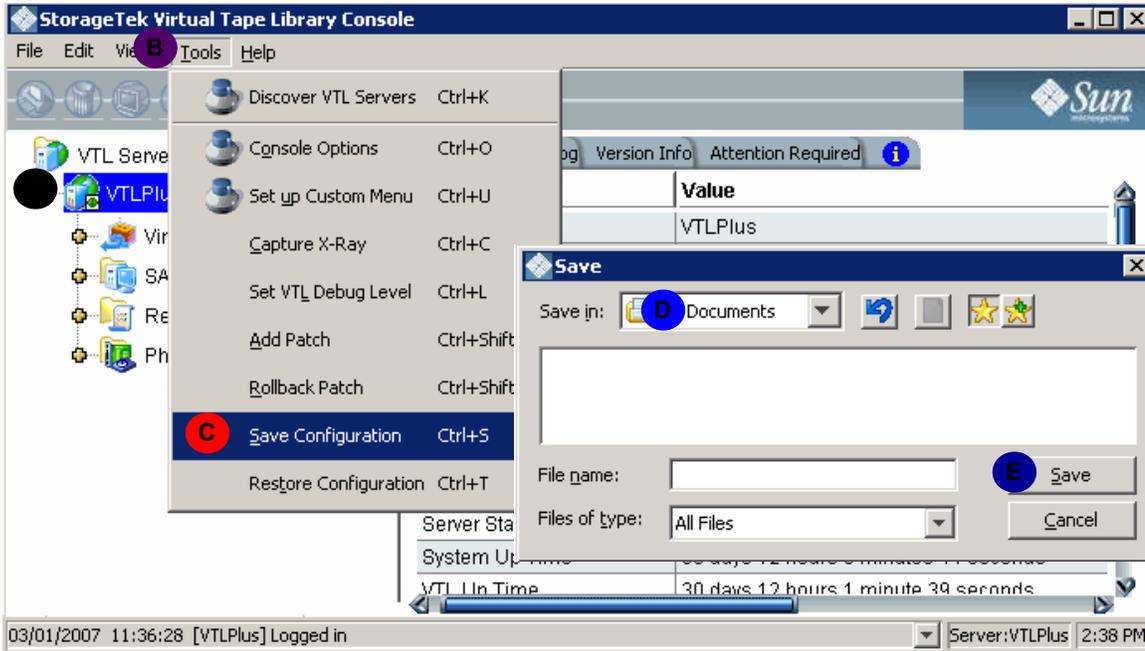
2. **From the VTL main menu, select `Tools` (B above).**

3. **From the submenu, select `Save Configuration` (C above).**

4. **When the `Save` dialog appears, supply a filename (D above), and press `Save` (E).**

Stop here.

▼ Automatically backing up the VTL configuration

To insure that the VTL configuration is alway protected, use the Auto Save feature to periodically create a point-in-time snapshot of the VTL configuration on another server.

1. **In the object tree of the VTL console, right-click on the the VTL server branch (A below).**
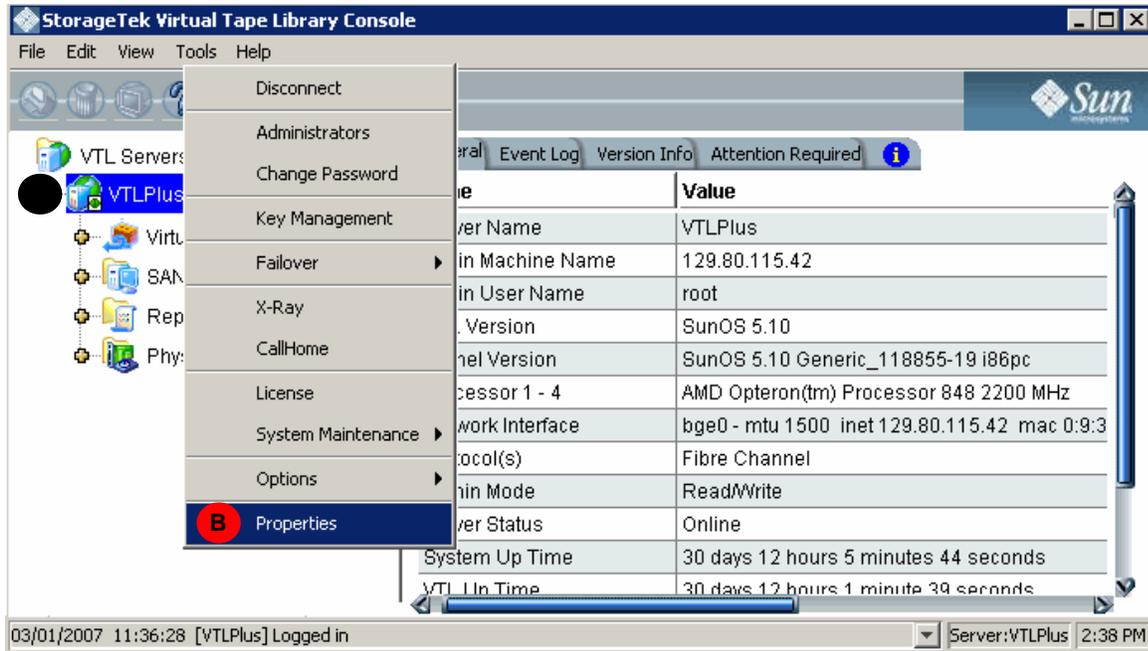
2. **From the context menu, select `Properties` (B above).**

3. Select the `Auto Save Config` **tab (C below).**
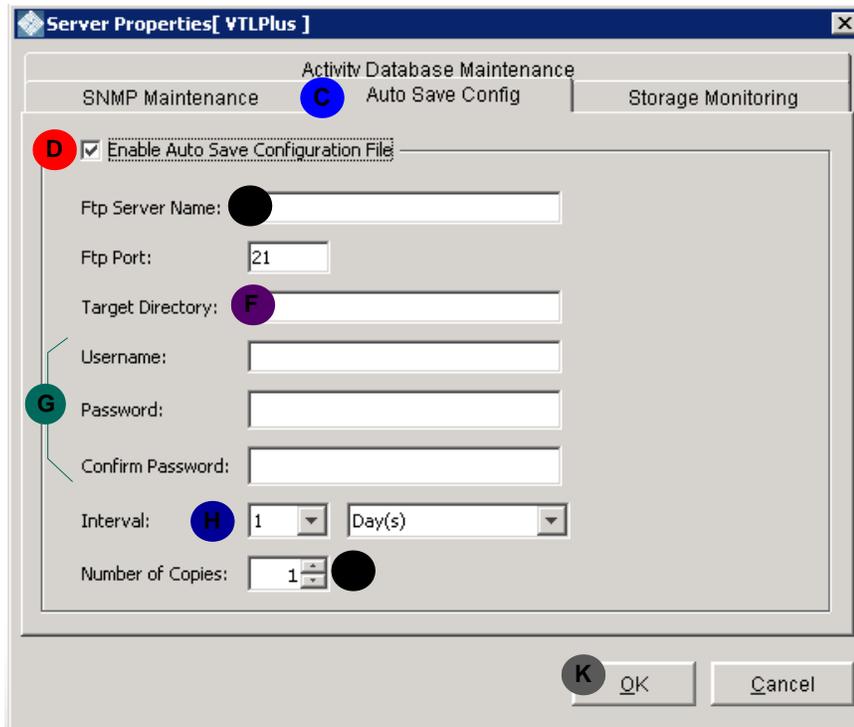
4. Check `Enable Auto Save Configuration File` **check box (D above).**

5. In the field provided, enter the `Ftp Server Name` **for the machine that will host the backup configuration files (E above).**

The target server must have FTP server installed and enabled.

6. Enter the relative path to the `Target Directory` **in the field provided (F above).**

The specified path should be relative to the root directory of the ftp server. Do not use an absolute path.

7. Enter host log on information for the remote server in the fields provided (G above).

The specified user must be an ftp user on the remote host and must have read/write access to the specified target directory.

8. Specify a replication `Interval` **using the list controls provided (H above).**

9. Specify the `Number of Copies` **that should be retained using the spinner provided (J above).**

10. Click `OK` **(K above).**

Stop here.

Recovering the server configuration

If the VTL server configuration is lost or corrupt, you can recover it from a backup file using the procedure below.

Caution – This is a disaster recovery procedure only. Never execute it during day-to-day operation of the server. Restoring a configuration overwrites existing virtual device and client configurations and does not restore VTL partition information.

▼ Restoring the configuration

1. **In the object tree of the VTL console, select the branch for the VTL server that has lost its configuration information.**

2. **From the VTL main menu, select** `Tools`**.**

3. **From the submenu, select** `Restore Configuration`**.**

4. **Click** `OK` **to confirm.**

5. **When prompted, locate the backup configuration file.**

   The VTL server restarts. Resources added after the configuration was saved will show up in the `Virtual Vault` after the configuration is restored. Deleted resources will be displayed in the virtual tape library with a red dot, indicating incomplete status.

Stop here.

Protecting VTL metadata

The VTL database holds the metadata that maps data stored on virtual tape to locations on the physical, random-access disk media. Without this critical information, virtual tape data cannot be recovered, so protecting it is essential.

Sun StorageTek VTL appliances protect this metadata by storing it on a RAID system, a set of storage disks configured to survive the loss of any single member of the set without loss of data.

Mirroring supplies an additional layer of protection. Mirrored databases maintain two separate, synchronized copies of the metadata, either of which can provide access to virtual tape data on its own.

▼ Mirroring the VTL database

1. **In the object tree of the VTL console, expand the branch for the VTL server (A below).**

2. **Expand the** `Virtual Tape Library System` **branch (B below).**

3. **Right-click on the** `Database` **object (C below).**
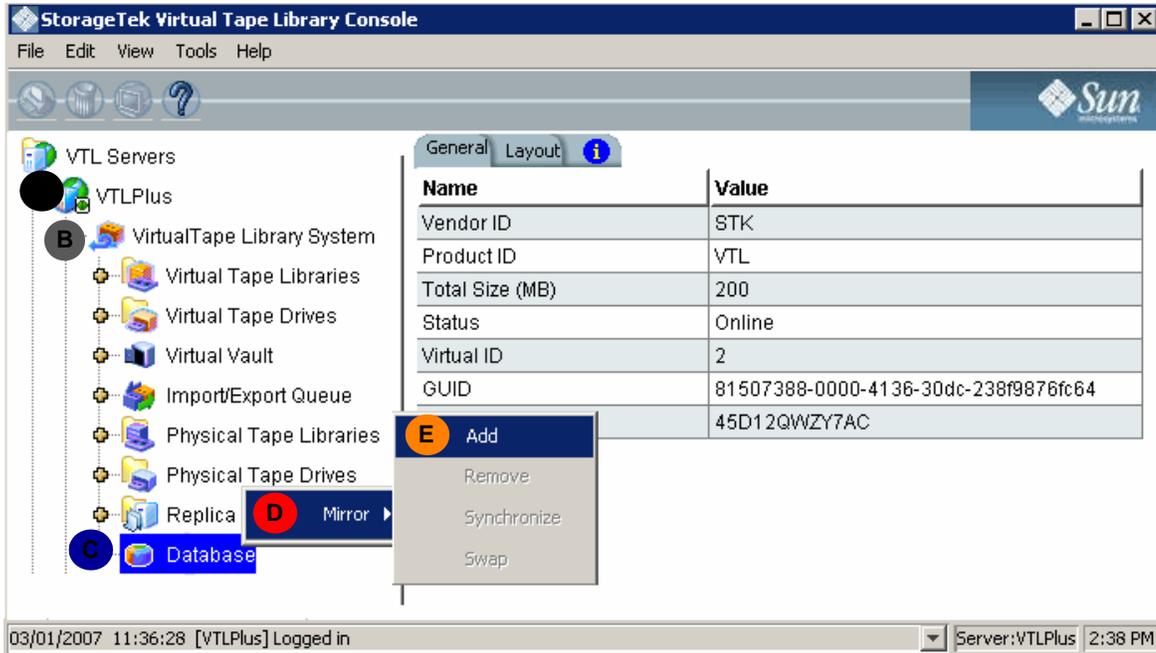
4. **From the context menus, select** `Mirror` **(D above) and** `Add` **(E).**

5. **When the** `Select a Creation Method` **dialog appears, select** `Express`
 (F below), and press `Next` **(G).**
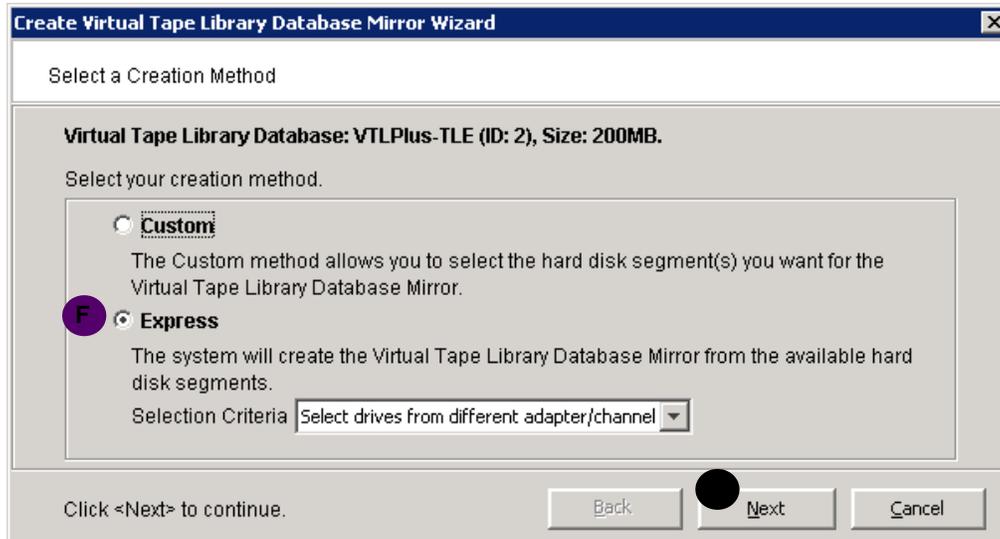
The `Express` method takes advantage of the intelligence built in to the RAID
subsystem to make best use of disk resources.

6. **When the confirmation dialog appears, confirm that all information is correct, and then click** `Finish` **to create the mirrors.**

The VTL software creates and synchronizes the mirror database. When the process completes, the value of the `Mirror Synchronization Status` field of the database property sheet becomes `Synchronized` (**H** below).
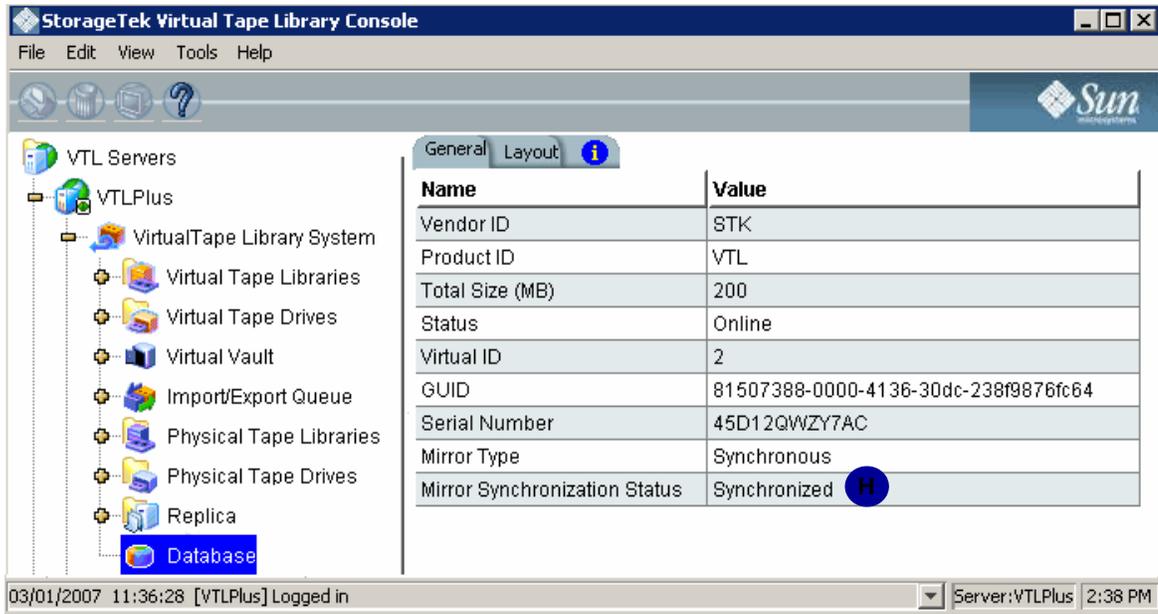
Stop here.

▼ Removing a mirror configuration

1. **Right-click on the database.**

2. **Select** `Mirror --> Remove` **to delete the mirrored copy and cancel mirroring. You will not be able to access the mirrored copy afterwards.**

Stop here.

Administering user acounts and passwords

You can perform the following tasks from the VTL console:

■ "Managing administrators" on page 87
■ "Changing administrator passwords" on page 88.

▼ Managing administrators

Only the root user can add or delete a VTL administrator or change an administrator's password.

1. **In the object tree of the VTL console, right click on the server name (A below), and select** `Administrators` **from the context menu (B).**
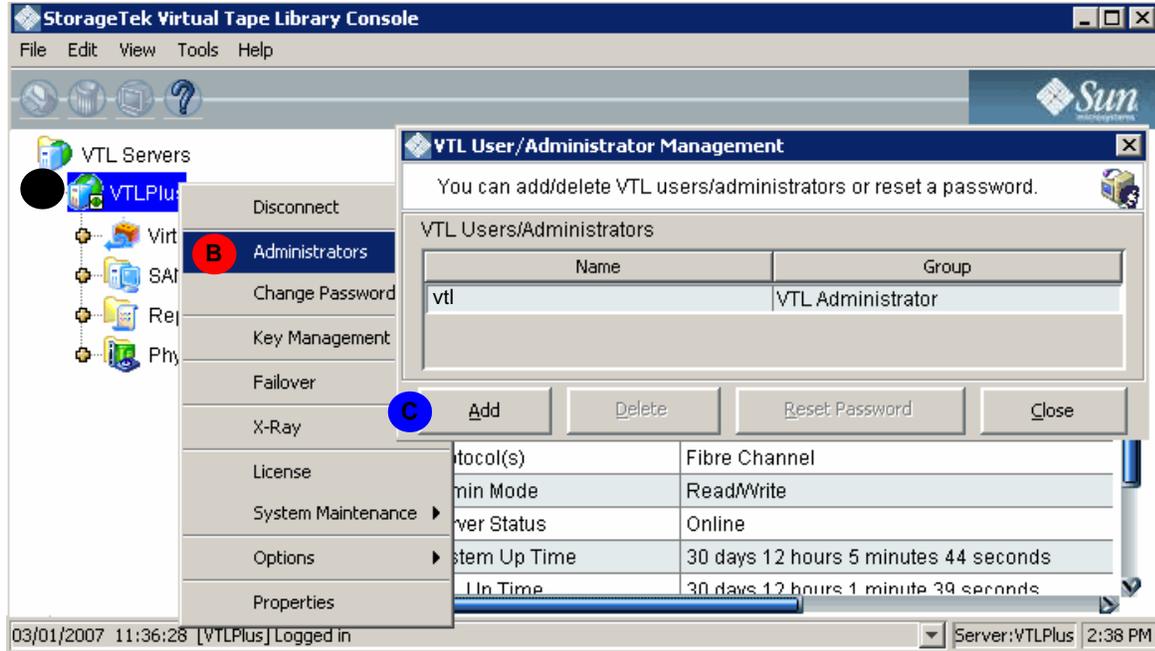
There are two types of administrators:

- `VTL Administrators` are authorized for full VTL console access.
- `VTL Read-Only Users` are only permitted to view information in the Console. They are not authorized to make changes and they are not authorized for client authentication.

2. **When the** `VTL User/Administrator Management` **dialog appears, use the controls provided to manage administrator accounts (C above).**

When you add an administrator, the name must adhere to the naming convention of the operating system running on your VTL Server. Refer to your operating system's documentation for naming restrictions.

You cannot delete the `vtl` user or change the `vtl` password from this screen. Use the `Change Password` option instead.

Stop here.

▼ Changing administrator passwords

1. **Right-click on the VTL server node name (A below), and select** `Change Password` **from the context menu (B).**
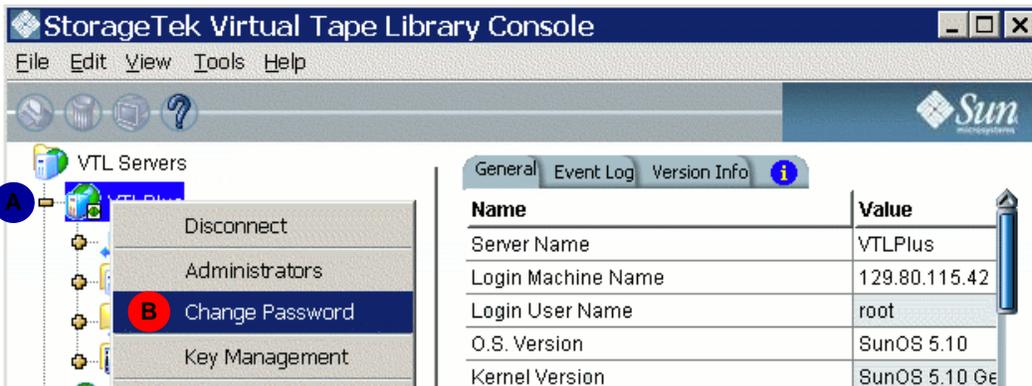
2. **When the dialog appears, enter the password that you need to change in the** `Old Password` **text box (C below).**

3. **Enter the changed password in the** `New Password` **and** `Confirm Password` **text boxes (D above).**

4. **Press OK (E).**

Stop here.

Virtual tape drive compression

VTL's compression saves disk space by compressing files so that more data can be stored by a virtual tape drive. The increase in capacity is directly related to the compressibility of the data being backed up. If you can compress the data being backed up by a factor of up to 2:1, you can store up to twice as much information on the virtual tape. Disk compression can vary depending upon the dataset; certain file types (ZIP, PDF, GIF, RAR, etc.) are already compressed and cannot be compressed further.

VTL supports two types of compression:

- Hardware compression - uses a Hifn Express DR1000 (1 GB/sec compression) or DR600 (600 MB/sec) compression card. A license keycode is required for hardware compression.
- Software compression - uses an LZO algorithm that runs on the VTL server.

In order to use compression, you must also enable tape drive compression in your backup application.

Note – Note: If you are already using software compression that is supplied by your backup application, you should not use VTL's compression. Using both types of compression will cause VTL to try to compress already-compressed data and this can slow down your backups.

▼ To enable or disable compression:

1. **Enable tape drive compression in your backup application.**

2. **If you are using hardware compression, install a certified compression card in your VTL server.**

   You can have up to two compression cards per VTL server.

   The compression card(s) must be installed before compression begins. If you try to use hardware compression and a compression card is not available, VTL will send an error message to the console event log and uncompressed data will be written to the virtual tape drive.

3. **In the VTL Console, right-click on VirtualTape Library System and select Properties.**

4. **Select the Enable VirtualTape Library compression mode checkbox and specifywhether you are using Software or Hardware compression.**

   If you are upgrading a VTL system that previously used software compression to now use hardware compression, the compression mode will be switched to hardware when the tape is overwritten.

   Both types of compression are global settings, which means that they will apply to all tapes in your system.

   If compression is enabled on the VTL server, you can still disable or enable compression on each individual virtual tape drive in the same manner as real tape drives -- via your backup application or via SCSI commands which are sent by the operating system.

UNIX — On backup servers that run Solaris or other UNIX operating systems, specify a compressed tape device file such as /dev/rmt/0cbn to enable compression or /dev/rmt/0ubn to disable compression.

Windows — On Windows servers select the option in your backup software to enable or disable hardware tape drive compression. If global VTL compression is disabled, it is possible to enable individual drive compression, but it will have no effect.

You will see a compression icon next to each virtual tape drive with compression enabled.

Managing tapes

This section addresses the following topics:

- Locating virtual tapes
- Copying a tape to a remote server.

Locating virtual tapes

To locate a virtual tape, proceed as follows.

▼ Searching for virtual tapes by barcode

1. **To locate a virtual tape, select** `Edit` **from the main menu.**

2. **Then select** `Find` **from the context menu.**

3. **When prompted, enter the full barcode for the virtual tape, and press** `Search`**.**

   The console opens the object tree at the virtual tape.

Stop here.

Replicating tapes

This section covers creating and working with synchronized replicas of virtual tapes on local and/or remote VTL servers. Topics include:

- "Setting up tape replication for multiple tapes" on page 91

- "Setting up replication for individual tapes" on page 96
- "Manually synchronizing replicas (manual replication)" on page 102
- "Stopping a replication that is already under way" on page 103
- "Manually synchronizing replicas (manual replication)" on page 102
- "Checking replication status from the target VTL server" on page 105
- "Checking replication status with a report" on page 105
- "Changing replication properties" on page 106
- "Deleting a replication configuration" on page 107
- "Promoting a replica resource" on page 107.

▼ Setting up tape replication for multiple tapes

1. **Before continuing, make sure that you have write access to both the primary (local) and target (remote) VTL servers and that there is enough space available on the target for the replica resources you intend to create.**

2. **In the object tree of the VTL console, expand the VTL server node.**

3. **Under the VTL server, expand the** `Virtual Tape Library System` **and** `Virtual Tape Libraries` **nodes.**

4. **Under the** `Virtual Tape Libraries` **node, right-click on the virtual tape library for which you want to enable replication (A below).**

5. **From the context menus, select** `Replication` **(B below),** `Add` **(C).**
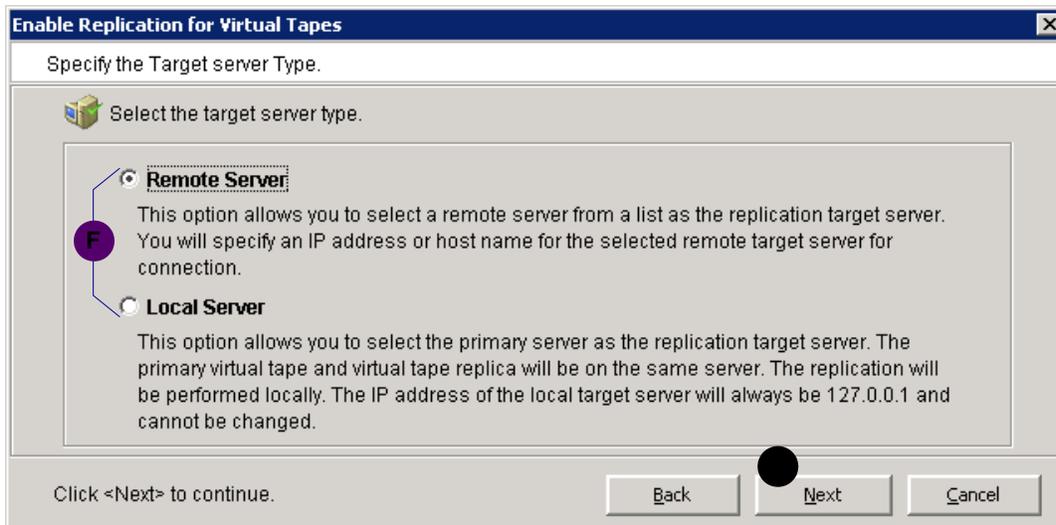
8. **When the** `Select Target Server` **panel appears, use the list (J below) to select or server or press** `Add` **(K) to add one to the list. Press** `Next` **(L).**

Enable Replication for Virtual Tapes

Select the Target Server

Select the target server or add the server you want to the list.

Server	
VTLPLUSN1	
VTLPLUSN2	

(J) Add

(H)

Click <Next> to continue.   Back   **●** Next   Cancel
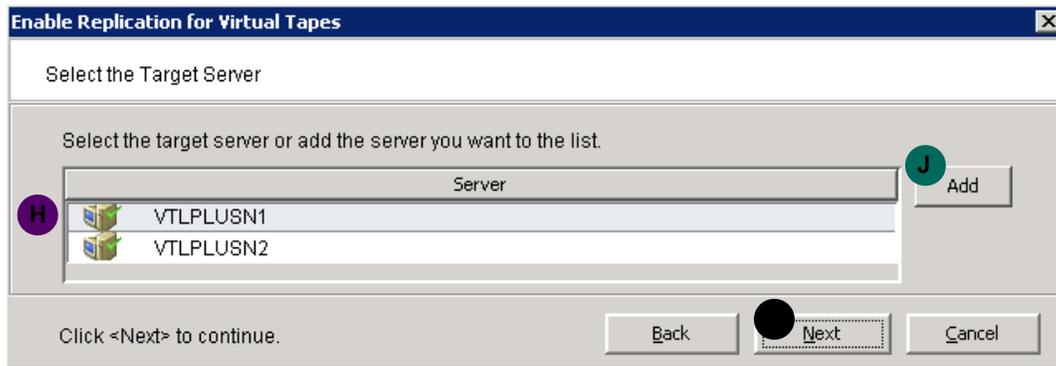
9. **If you chose the** `Remote Server` **option above, in Step 7, edit the IP address of the remote VTL server in the space provided (M below), if necessary, then press** `Next` **(N).**

Enable Replication for Virtual Tapes

Enter Replication Parameters

Target Server Information.

Target Server: **VTLPLUSN1**

hostname or IP address: [   ] **(M)**

The target server IP information will be used by the primary server to connect to the target server for replication. If a hostname is entered, the primary server should be able to resolve the hostname via DNS. If an IP address is entered, we recommend using a static rather than a DHCP IP address.

Click <Next> to continue.   Back   **(N)** Next   Cancel

10. **If you chose the** `Local Server` **option above, in Step 7, press** `Next` **(O below).**
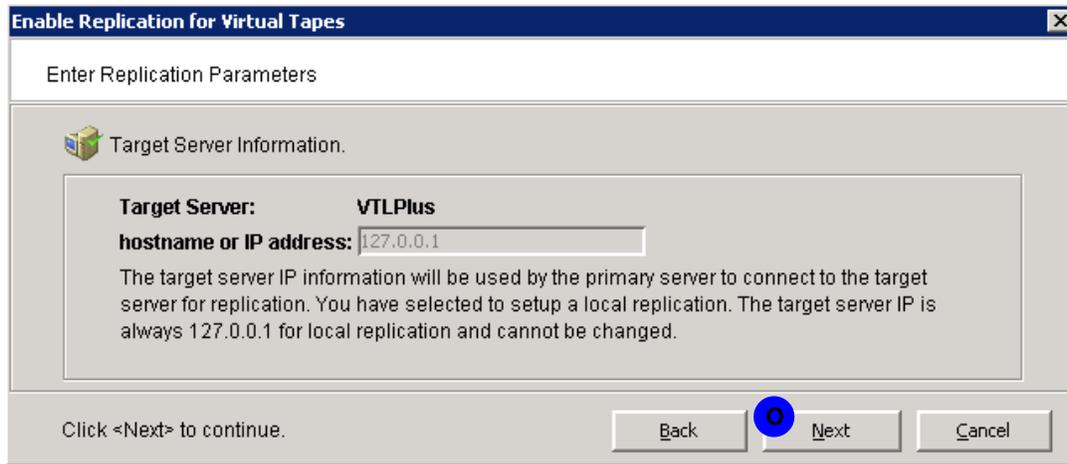
11. **When the** `Select the Replication Policy` ... **panel appears, use the check boxes, list boxes, and spinner controls provided to define the policy you want to apply (P below). Press** `Next` **(R).**
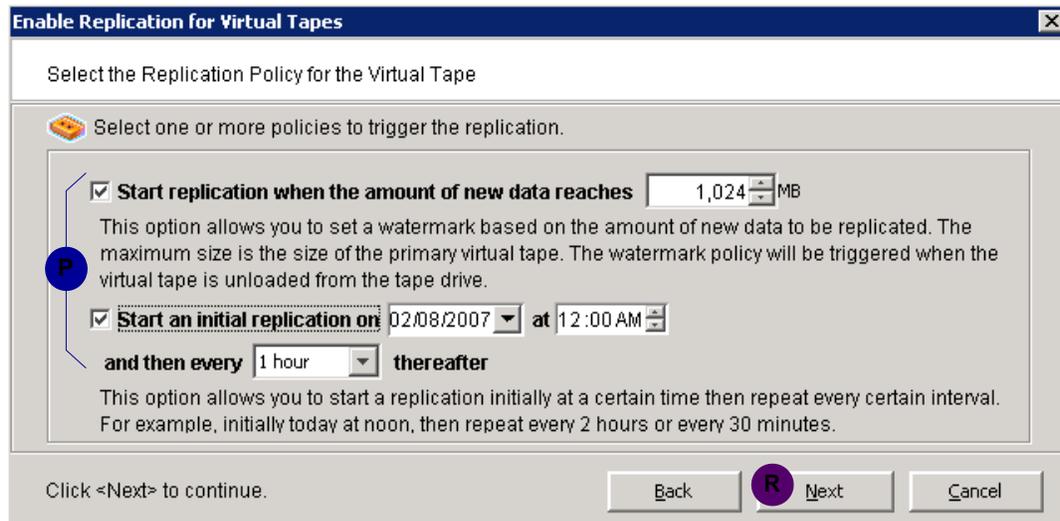
12. **When the** `Select the Replication Timeout and Retry Policy` **panel appears, use the spinner controls provided to define the policy you want to apply (S below). Press** `Next` **(T).**
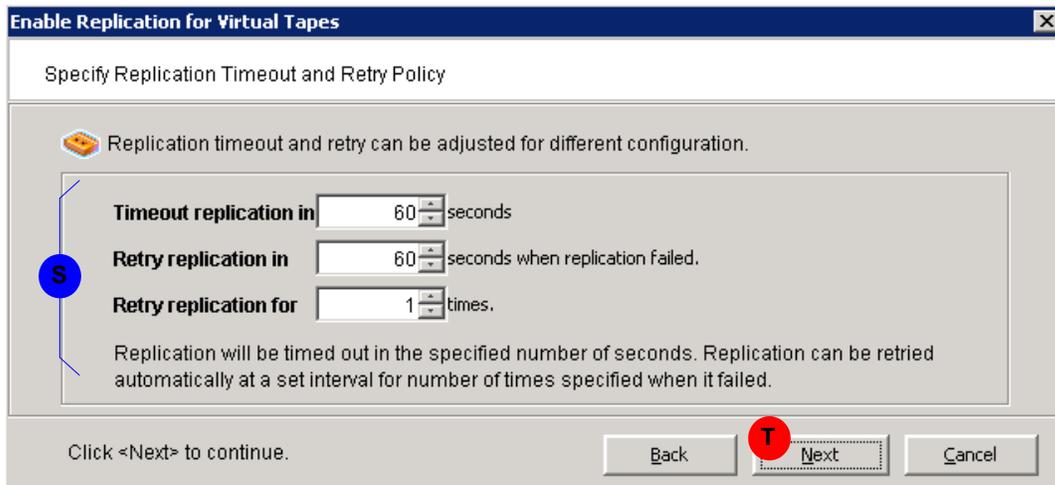
13. **When the** `Specify the Options for Data Transmission` **panel appears, use the check boxes provided to select the options you want to use (U below). Press** `Next` **(V).**

Remember that compression and encryption are CPU-intensive software processes that reduce system throughput. Use them judiciously, when necessary.
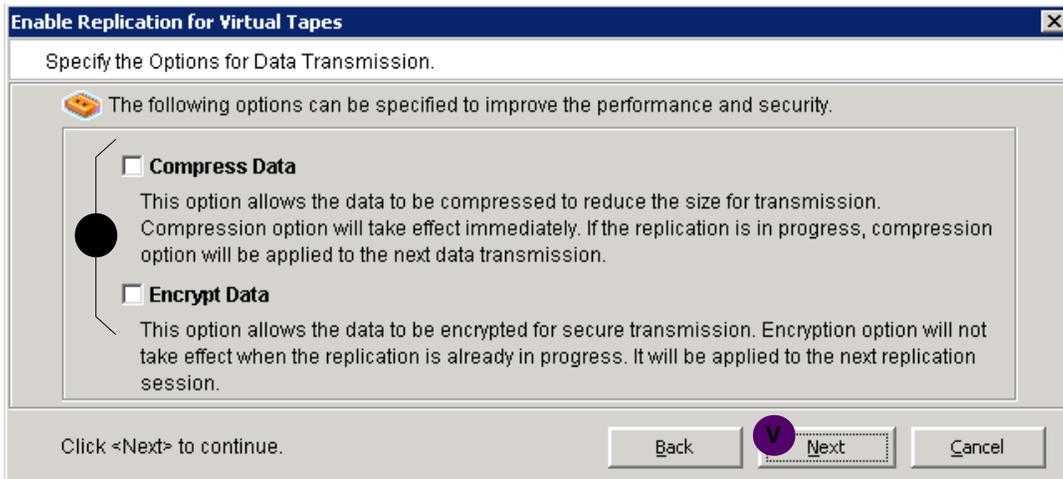
14. **When the confirmation panel appears, press** `Finish` **(W below).**
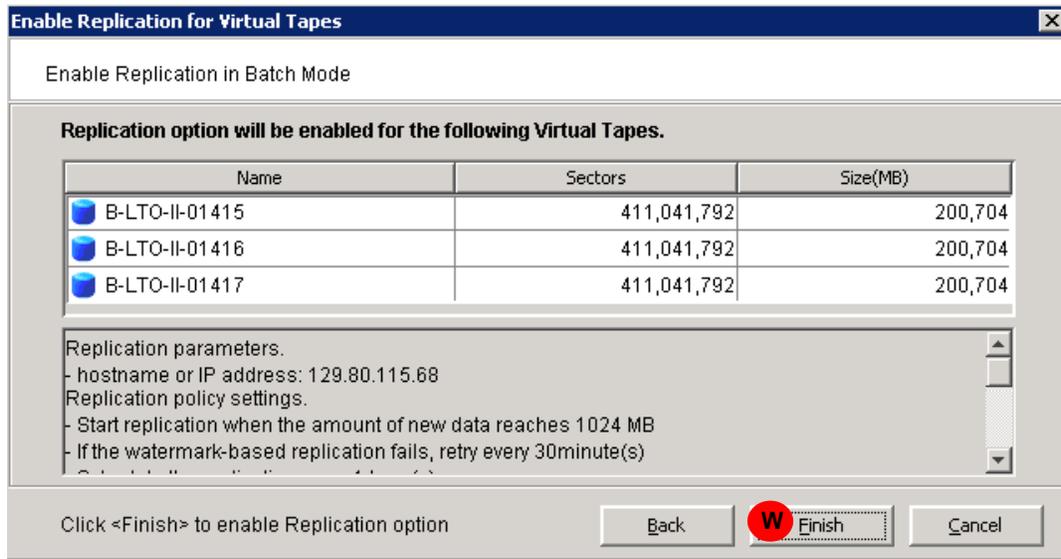
Stop here.

▼ Setting up replication for individual tapes

1. **In the object tree of the VTL console, expand the VTL server node, the** `Virtual Tape Library System` **node, and the** `Virtual Tape Libraries` **node.**

2. **Then open the node for the library that holds the tape you want to replicate (A below), and open the** `Tapes` **node (B).**
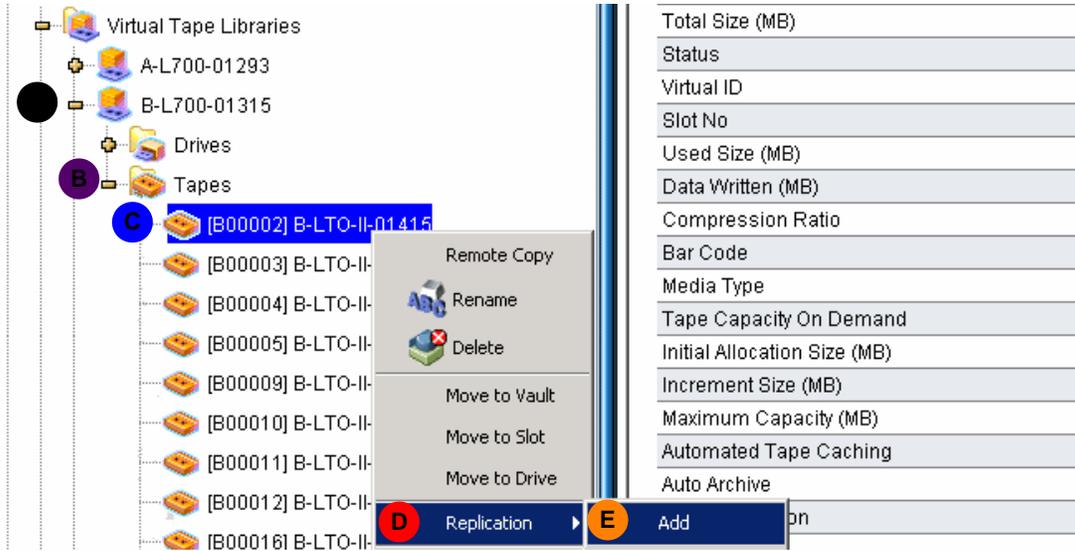
3. **Right-click on the virtual tape for which you want to enable replication (C above).**

4. **From the context menus, select** `Replication` **(D above), then select** `Add` **(E).**

5. **When the** `Specify the Target server Type` **panel appears, click the radio button for a** `Remote or Local Server` **(F below). Then press** `Next` **(G).**
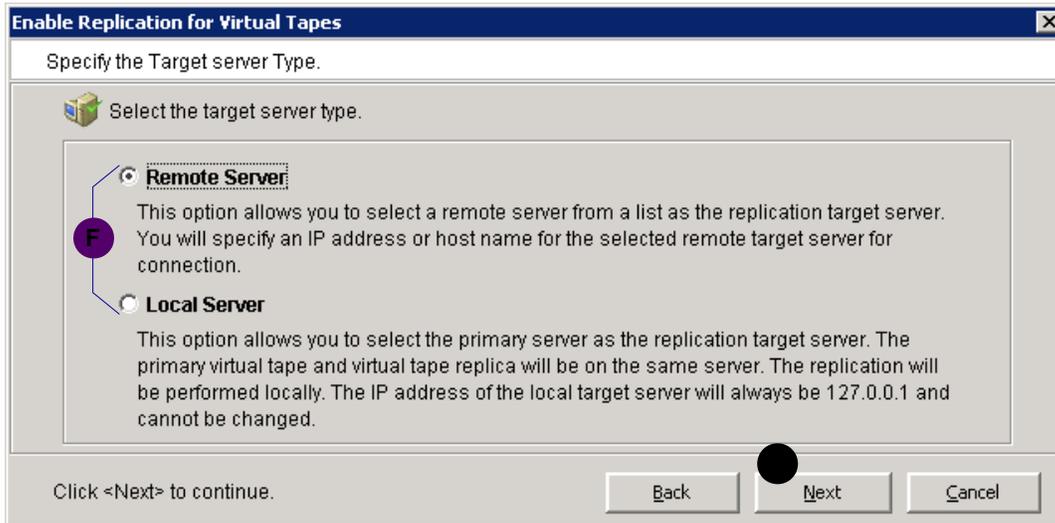
6. **When the** `Select Target Server` **panel appears, use the list (H below) to select or server or press** `Add` **(J) to add one to the list. Press** `Next` **(K).**

Enable Replication for Virtual Tapes ☒

Select the Target Server

Select the target server or add the server you want to the list.

Server	J Add

H VTLPLUSN1
   VTLPLUSN2

Click <Next> to continue.   Back   ● Next   Cancel
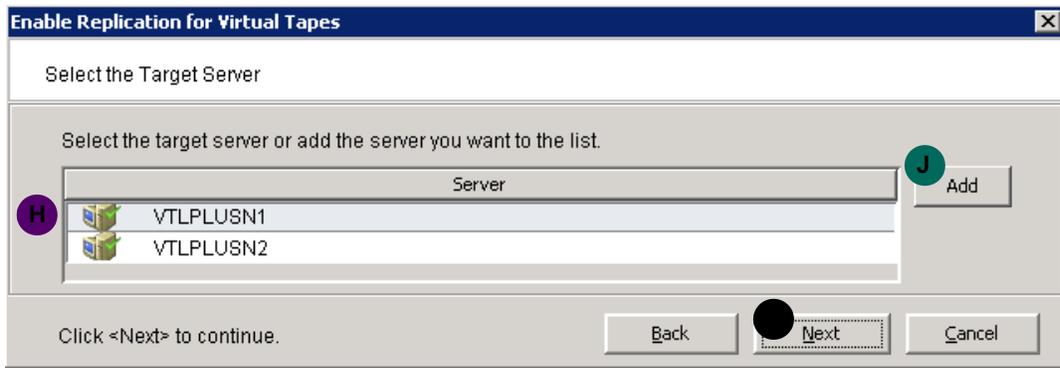
7. **If you chose the** `Remote Server` **option above, in Step 7, edit the IP address of the remote VTL server in the space provided (L below), if necessary, then press** `Next` **(M).**

Enable Replication for Virtual Tapes ☒

Enter Replication Parameters

Target Server Information.

Target Server: **VTLPLUSN1**
hostname or IP address: [L   ]
The target server IP information will be used by the primary server to connect to the target server for replication. If a hostname is entered, the primary server should be able to resolve the hostname via DNS. If an IP address is entered, we recommend using a static rather than a DHCP IP address.

Click <Next> to continue.   Back   M Next   Cancel

8. **If you chose the** `Local Server` **option above, in Step 7, press** `Next` **(N below).**

9. **When the** `Select the Replication Policy ...` **panel appears, use the check boxes, list boxes, and spinner controls provided to define the policy you want to apply (N below). Press** `Next` **(P).**

10. **When the** `Select the Replication Timeout and Retry Policy` **panel appears, use the spinner controls provided to define the policy you want to apply (Q below). Press** `Next` **(R).**
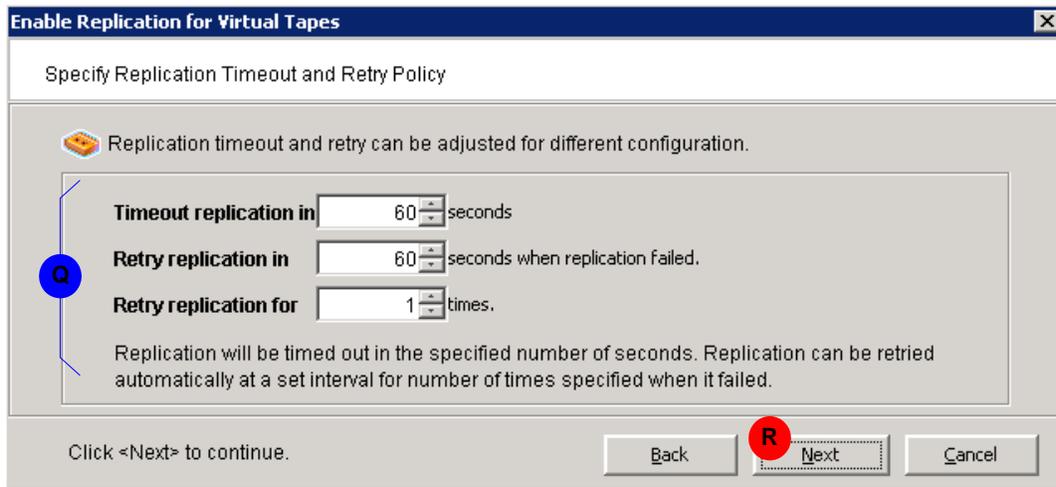
11. **When the** `Specify the Options for Data Transmission` **panel appears, use the check boxes provided to select the options you want to use (S below). Press** `Next` **(T).**
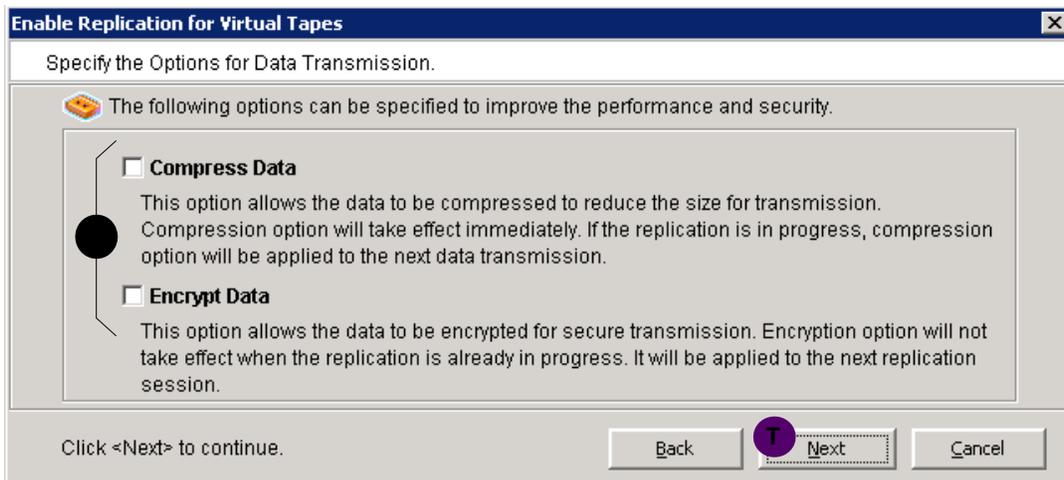
Remember that compression and encryption are CPU-intensive software processes that reduce system throughput. Use them judiciously, when necessary.

12. When the `Select a Creation Method` **panel appears, click the** `Express` **radio button (U below), and press** `Next` **(V).**
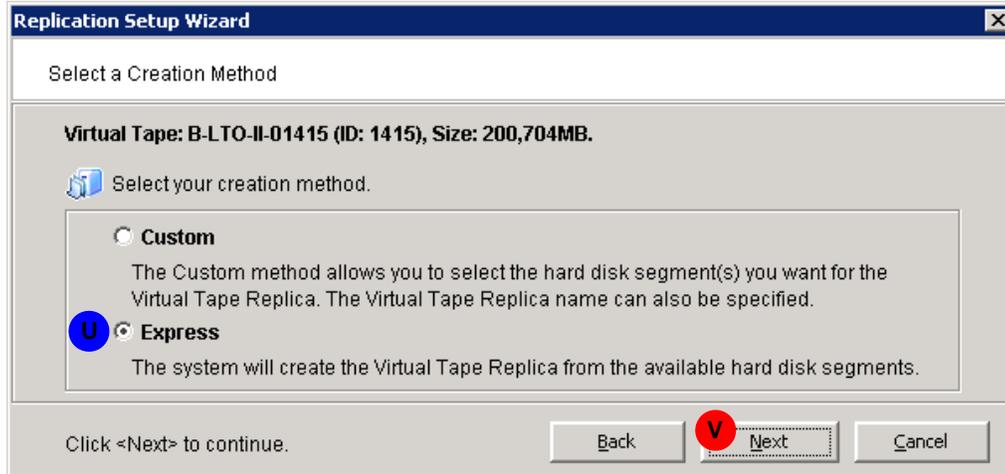
The Sun StorageTek VTL appliance includes an integrated RAID device, so there is no advantage to manually selecting target volumes using the `Custom` method. The `Custom` method may also result in load balancing problems and significantly greater management overhead.

13. When the `Enter the Virtual Tape Replica Name` **panel appears, enter a name or accept the default (W below), and press** `Next` **(X).**
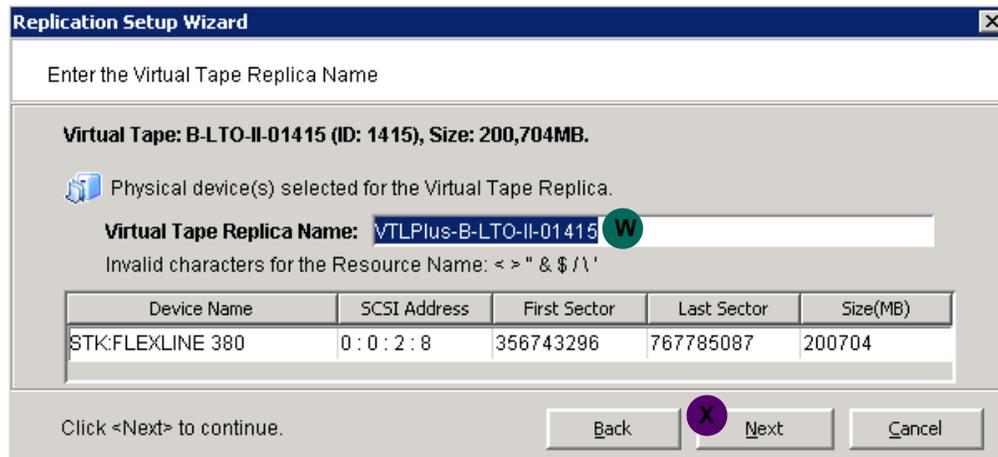
14. When the confirmation panel appears, press `Finish` **(Y below).**

Replication Setup Wizard

Create the Virtual Tape Replica

Virtual Tape: B-LTO-II-01415 (ID: 1415), Size: 200,704MB.

Physical device selected for the Virtual Tape Replica.

Virtual Tape Replica Name: VTLPlus-B-LTO-II-01415

Virtual Tape Replica Layout. Total Size: 200,704MB.
  Device Header: STK:FLEXLINE 380, ACSL: 0:0:2:8, sectors: 356737152 - 356743295, 3MB.
  1: STK:FLEXLINE 380, ACSL: 0:0:2:8, sectors: 356743296 - 767785087, 200,704MB.

Replication parameters.
- hostname or IP address: 129.80.115.68
Replication policy settings.
- Start replication when the amount of new data reaches 1024 MB
- If the watermark-based replication fails, retry every 30minute(s)

Click <Finish> to complete the Virtual Tape Replica.   Back   Finish   Cancel

---

Note – Once you create your replication configuration, you should not change the hostname of the source (primary) server. If you do, you will need to recreate your replication configuration.

Stop here.

▼ Manually synchronizing replicas (manual replication)

You can synchronize replicas manually, when necessary. To do so, proceed as follows.

1. Right-click on the primary virtual tape, and select `Replication` **from the context menu.**

2. Select `Synchronize` **from the following context menu.**

Stop here.

▼ Suspending and resuming replication

You can manually suspend forthcoming replications that would otherwise be launched automatically from your replication policies (currently active replications are unaffected). To do so, proceed as follows.

1. **Right-click on the primary virtual tape, and select** `Replication` **and** `Suspend` **from the context menus.**

2. **If desired, you can synchronize replicas manually during the suspension period by right-clicking on the primary virtual tape, and selecting** `Replication` **and** `Synchronize` **from the context menus.**

3. **To continue with normal replication, right-click on the primary virtual tape, and select** `Replication` **and** `Resume` **from the context menus.**

Stop here.

▼ Stopping a replication that is already under way

1. **To stop a replication that is currently in progress, right-click on the primary virtual tape.**

2. **Select** `Replication` **from the context menu.**

3. **Select** `Stop` **from the following context menu.**

Stop here.

▼ Checking replication status from the primary VTL server

1. **In the object tree of the VTL console, drill down to the `Tapes` node, and select the primary virtual tape (A below).**
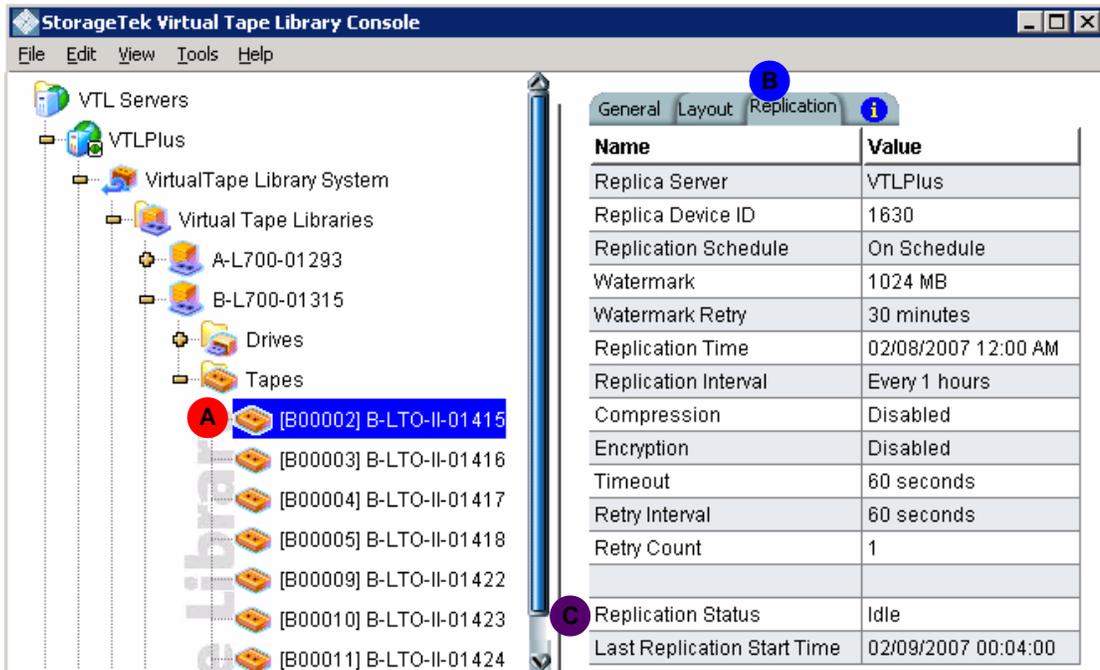
2. **In the properties sheet at the right, select the `Replication` tab (B above).**

3. **Scan down the sheet until you see the `Replication Status` row (C above).**

Stop here.

▼ Checking replication status from the target VTL server

1. **In the object tree of the VTL console, drill down to the** `Replica Resources` **node (A below).**
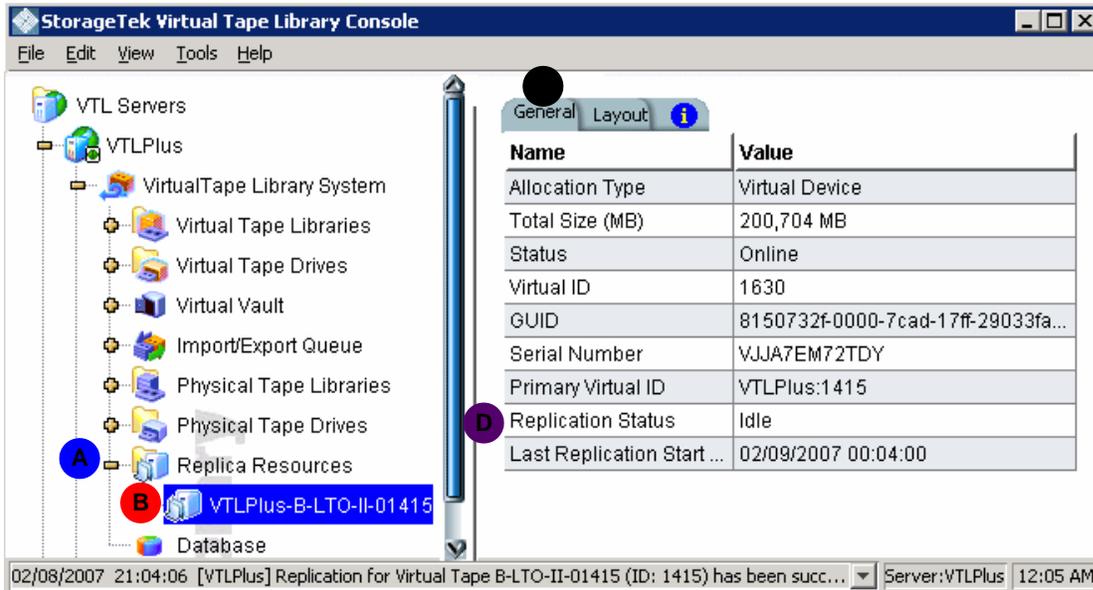
2. **Select the replica resource corresponding to the primary virtual tape (B above))**

3. **In the properties sheet at the right, select the** `General` **tab (C above).**

4. **Scan down the sheet until you see the** `Replication Status` **row (D above).**

Stop here.

▼ Checking replication status with a report

1. **Use the procedure in "Creating a report" on page 127 to create a Replication Status Report**

   While a report can be generated for a single tape, it is most useful for assessing the replication status of multiple tapes. Reports can be created to fit a range of criteria, including:

   - all tapes that have replication enabled
   - all tapes replicated from a source server
   - all tapes replicated to a target server
   - all tapes in a given range of dates.

■ all tapes on a group of servers

Reports can be filtered to exclude all but current replication configurations, all but deleted or prompted configurations, or any desired combination.

2. Examine the report for the status (A below) of the job or jobs you are interested in.

Stop here.

▼ Changing replication properties

You can change the following for your replication configuration:

■ Static IP address of your target server

■ Policies that trigger replication (watermark, interval, time)

■ Timeout and retry policies

■ Data transmission options (encryption, compression)

To change properties, proceed as follows:

1. Right-click on the primary virtual tape, and select `Replication` **and** `Properties` **from the context menus.**

2. Make the appropriate changes, and press `OK`**.**

Stop here.

▼ Deleting a replication configuration

1. **Right-click on the primary virtual tape, and select** `Replication` **from the context menu.**

2. **Select** `Remove` **from the following context menu.**

   This allows you to remove the replication configuration on the primary and either delete or promote the replica resource on the target server at the same time.

Stop here.

▼ Promoting a replica resource

If a primary virtual tape is damaged or corrupted, administrators can restore the data by `promoting` the equivalent replica. After promotion, the virtual tape is placed in the virtual vault on the former target server (now the primary). An administrator can then:

- move the virtual tape to a virtual library on the local server
- replicate the virtual tape back to the original source server.

Once promoted, a replica resource cannot revert to being a replica resource. You must create a new replication configuration for the new primary tape.

TIn order to maintain the integrity of restored data, the VTL software will not promote an invalid replica resource, such as a replica that has been damaged or left incomplete by a transmission fault. It will likewise refuse to promote a replica resource while a replication is still in progress.

1. **In the object tree of the VTL console, expand the VTL target server node, expand the** `Virtual Tape Library System` **and** `Replica Resources` **nodes.**

2. **Under the** `Replica Resources` **node, right-click on the replica that you want to promote (A below).**

3. From the context menus, select `Replication` **(B below),** `Promote` **(C).**
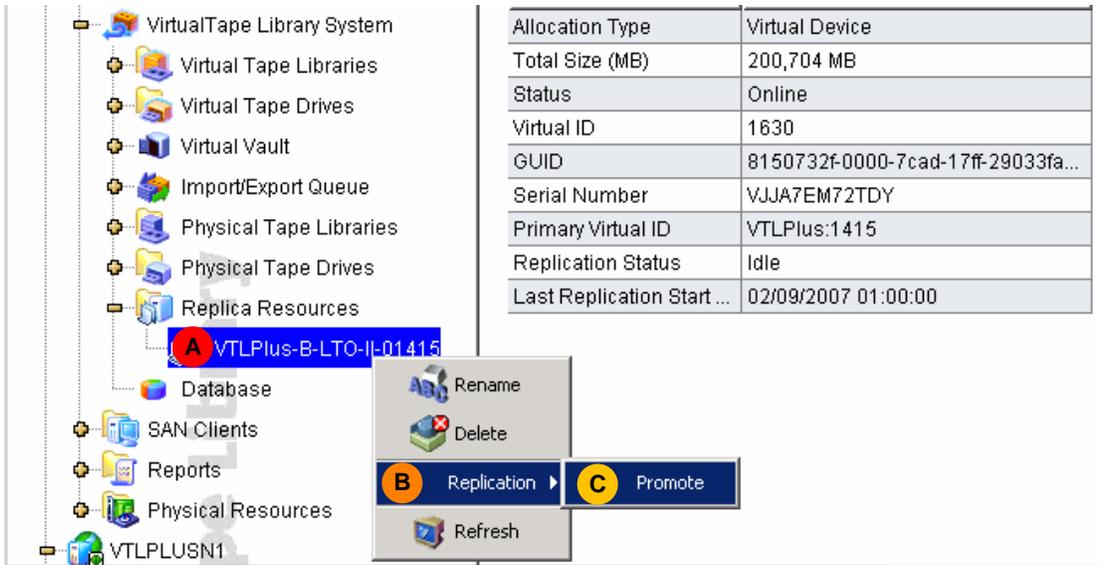
4. When the confirmation panel appears, press `OK` **(D below).**
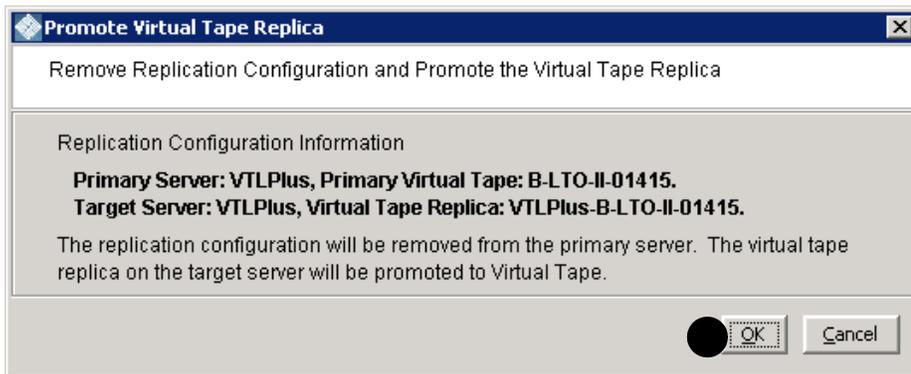
5. Rescan devices from the SAN client or restart the client so that it can see the promoted virtual tape.

Stop here.

Copying tapes

You can copy the contents of a single tape to a remote server, on demand, using the VTL `Remote Copy` feature. The `Remote Copy` feature replicates full tapes. It does not append data to existing virtual tapes or overwrite the contents of tapes.

You can only copy tapes with barcodes that are not found on the remote server. If a copy exists and you wish to proceed, you must first delete the existing remote copy copy.

You cannot copy a tape that is configured to take advantage of the `Replication`, `Auto Replication`, or `Auto Archive` features.

To copy tapes to a remote server, proceed as follows.

▼ Copying a tape to a remote server

1. **In the object tree of the VTL console, expand the VTL server node.**

2. **Under the VTL server, expand the** `Virtual Tape Library System` **and** `Virtual Tape Libraries` **nodes.**

3. **Under the** `Virtual Tape Libraries` **node, right-click on the virtual tape library that you want to enable (A below), and expand the** `Tapes` **node.**

4. **Right-click on the virtual tape that you want to copy (B below), and select** `Remote Copy` **from the context menu (D).**
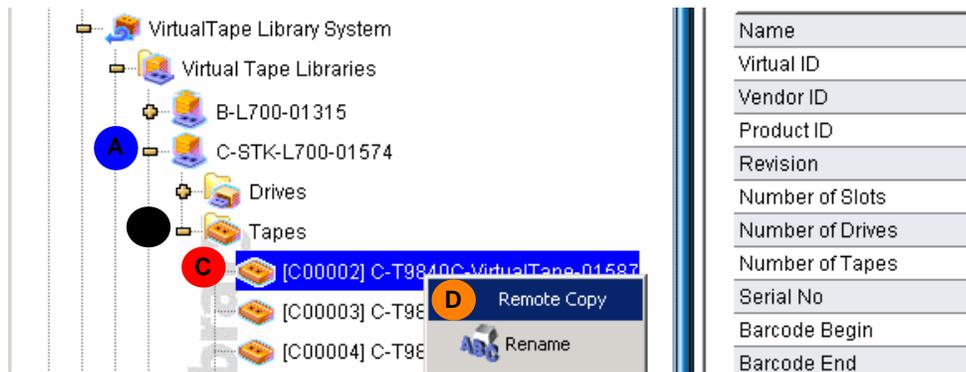
5. **When the** `Select the Target Server` **panel appears, use the list to select the server where you want to copy the tape (E below) or press** `Add` **(F) to add a server to the list. Then press** `Next` **(G).**

Remote Copy Setup Wizard

Select the Target Server

Select the target server or add the server you want to the list.

Server
E VTLPLUSN1
VTLPLUSN2

Add (F)

Back   G Next   Cancel
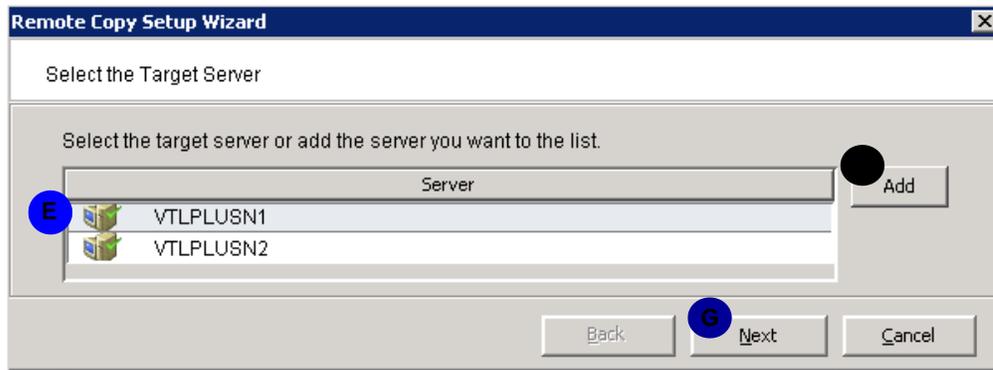
6. **When the** `Enter Replication Parameters` **panel appears, edit the IP address if necessary (H below), then press** `Next` **(J).**

Remote Copy Setup Wizard

Enter Replication Parameters

Target Server Information.

Target Server: VTLPLUSN1
hostname or IP address: nnn.nnn.nnn.nnn   H

The target server IP information will be used by the primary server to connect to the target server for replication. If a hostname is entered, the primary server should be able to resolve the hostname via DNS. If an IP address is entered, we recommend using a static rather than a DHCP IP address.

Back   Next   Cancel

7. **When the** `Specify a Location` **panel appears, select a location on the remote server (K below), and press** `Next` **(L).**
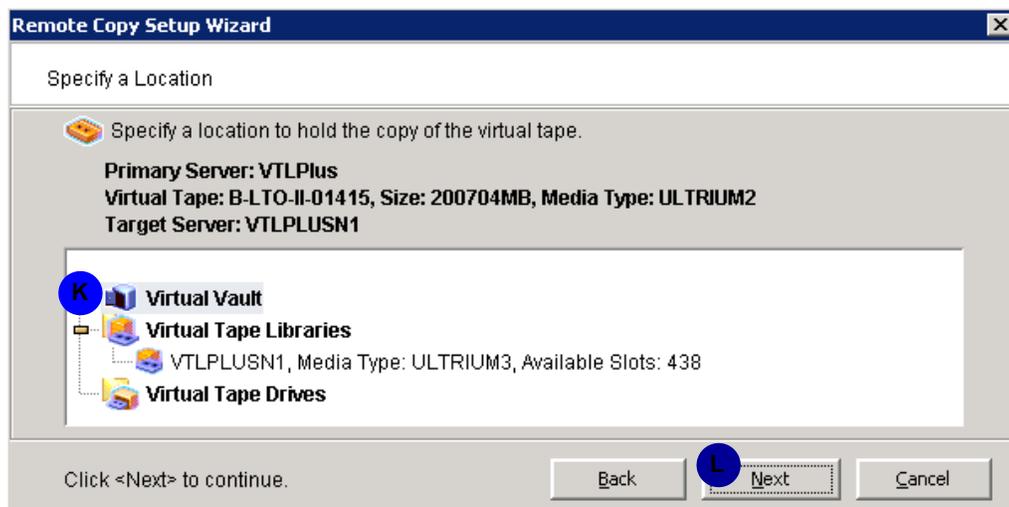
8. **When the confirmation panel appears, press** `Finish` **(M below).**
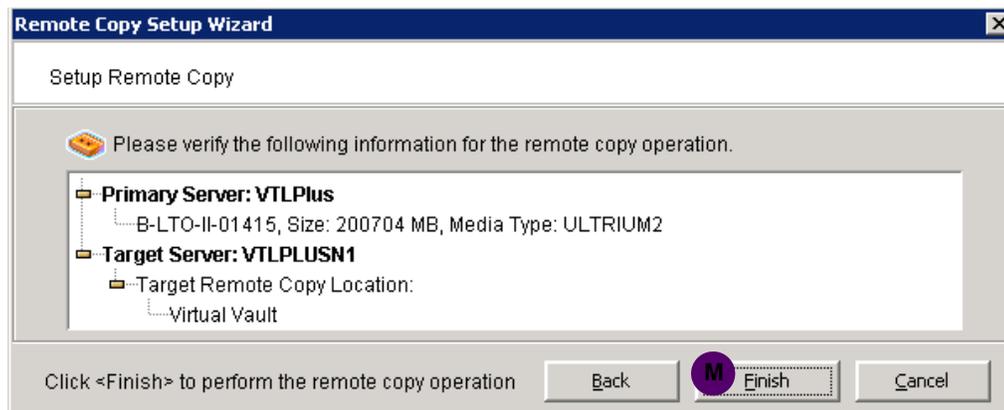
Stop here.

Moving tapes between virtual and physical libraries

VTL software can import a physical tape as a virtual tape or export virtual tape to physical tape, using an attached physical tape library or tape drive. You can thus use the import and export functions to:

- copy a physical tape to a virtual tape that emulates the same type of media
- directly access a physical tape without copying the entire tape
- recycle a physical tape after importing its contents to virtual media
- move data from a virtual tape to a physical tape of the same media type

VTL import/export capabilities are particularly useful when you are not using the Automated Tape Caching feature and want to move tapes from a virtual library to physical media for long term storage. Should you subsequently need to recover files, you can access the physical tape volume directly, in the physical library, by using the VTL import function. This gives the backup application immediate access to the tape data without waiting for a complete copy—a big advantage when you need to restore only a small amount of data.

You should note, however, that VTL software supports several of ways of moving data from virtual to physical storage, each of which has advantages in particular situations. In addition to VTL's export function, each of the following methods supports migration of data from virtual to physical media:

- copying virtual tape to physical tape using the functionality provided by your backup or copy-/vault-management application
- automatically cloning virtual volumes to physical media after each backup using the VTL Auto Archive function
- automatically cloning virtual volumes to physical media using the policy-driven VTL Automated Tape Caching option.

You should thus consider your options before deciding on a method. Automated Tape Caching and Auto Archive cannot be used together.

Up to 32 import/export jobs can run concurrently, although, in practice, this is generally limited to something less by the number of physical tape drives available on the attached library.

This section holds instructions for the following tasks:

- "Importing a physical tape into a virtual library" on page 113
- "Importing cartridges in an IBM iSeries environment" on page 119
- "Exporting virtual tape to physical tape" on page 119
- "Exporting cartridges to the virtual vault in an IBM iSeries environment" on page 123.

▼ Importing a physical tape into a virtual library

1. **In the object tree of the VTL console, right-click the node for the physical tape library or drive that holds the tape you wish to import (A below). Select** `Import Tape` **from the context men (B).**
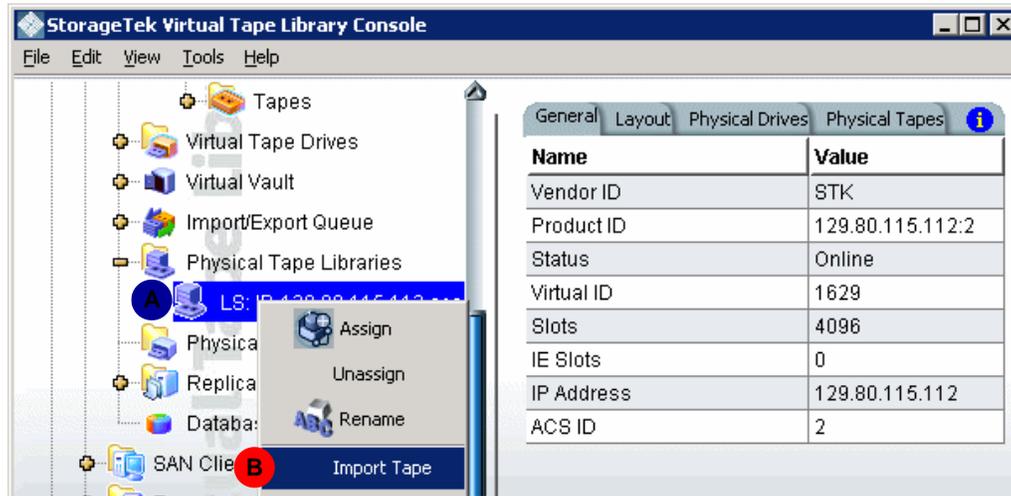
2. **When the** `Select virtual library ...` **panel appears, use the list to select a virtual library that holds volumes of the same capacity as the volume you want to import (C below). Press** `Next` **(D).**
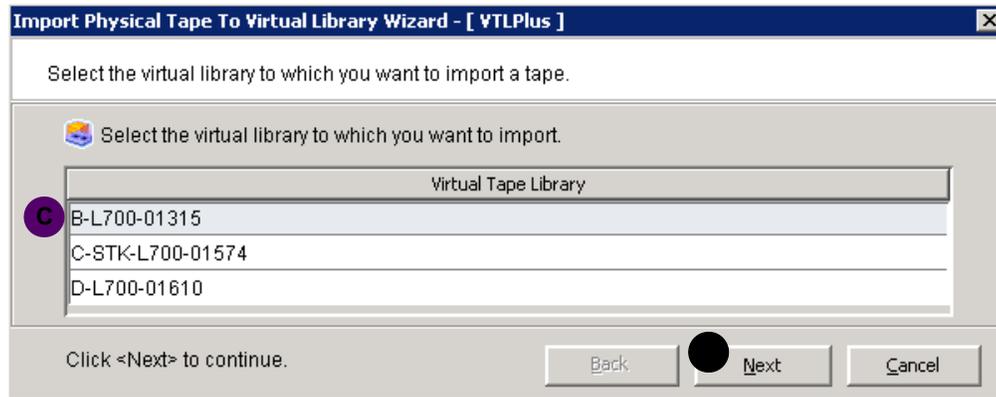
VTL exports tapes to like media only. You cannot export to a dissimilar physical tape.

3. **When the** `Select the import mode ...` **panel appears, click the radio button that corresponds to the behavior you want (E below).**
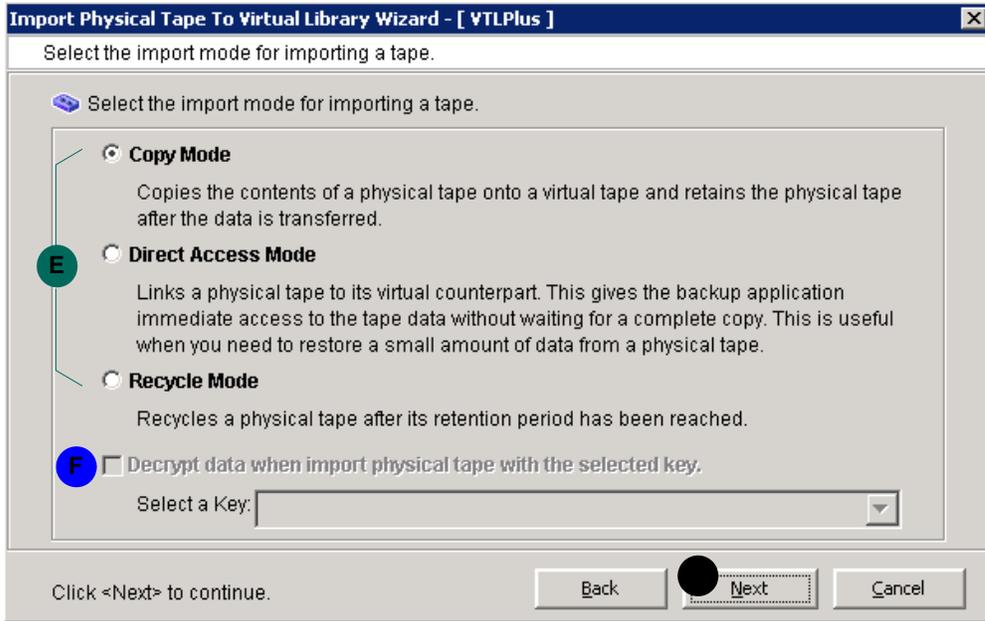
4. **If the tape is encrypted and you wish to decrypt it, check the** `Decrypt data ...` **check box (F above), and enter the correct key.**

   If the data was not previously encrypted, imported data is unusable. If you supply an incorrect key or if you enter an invalid password when challenged, the imported data is not decrypted.

5. **Press** `Next` **(G above).**

6. **When the** `Select the physical tape to import ...` **panel appears, use the check boxes and/or selection buttons provided to select the tape(s) that you want to import (H below). Then press** `Next` **(J).**
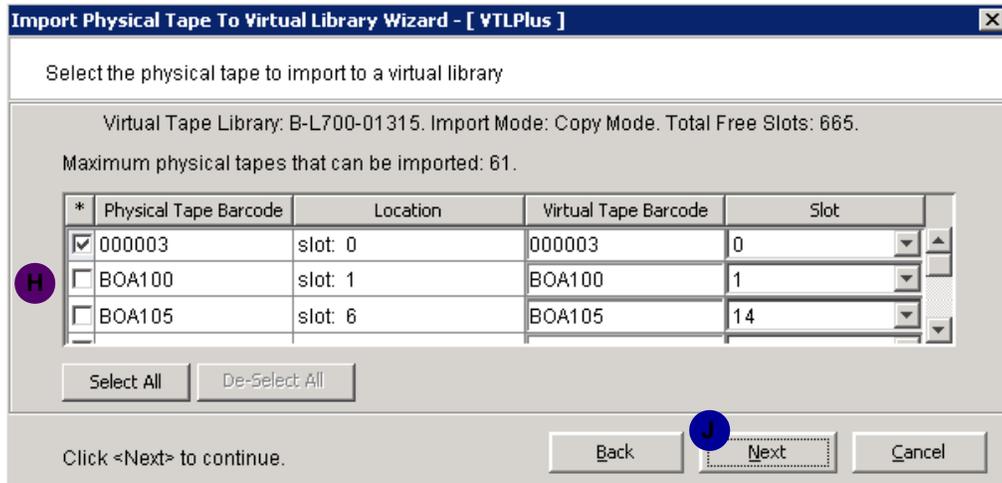
You can select a tape based on its barcode or slot location. You can then use the same barcode for the virtual tape or you can enter a new barcode. You can also select a slot for the virtual tape.

7. **When the** `Select Virtual Tape Creation Method` **panel appears, click the** `Express` **radio button (K below), and press** `Next` **(L).**
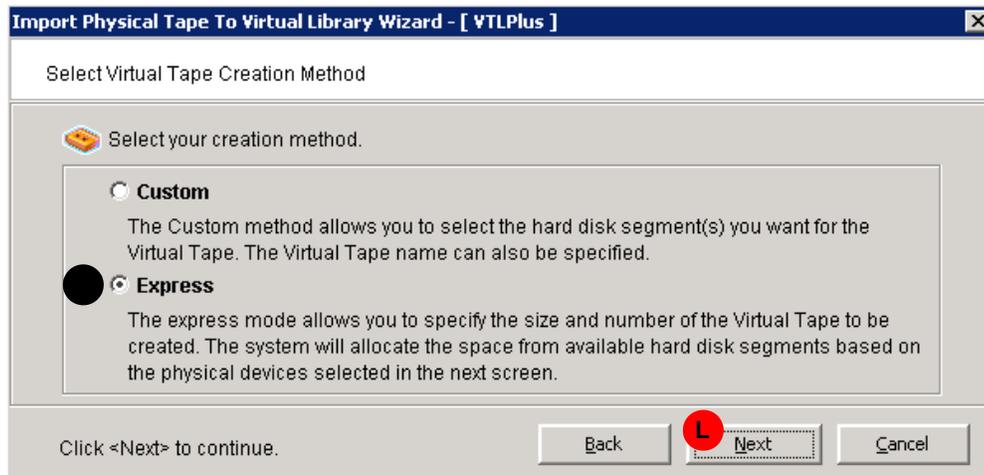
The Sun StorageTek VTL appliance includes an integrated RAID subsystem, so there is no advantage to manually selecting target volumes using the `Custom` method. The `Custom` method may also result in load balancing problems and significantly greater management overhead.

8. **When the** `Select Physical Devices` **panel appears, use the check boxes and/or selection buttons provided to select the LUNs that you wish to use (M below). Press** `Next` **(N).**
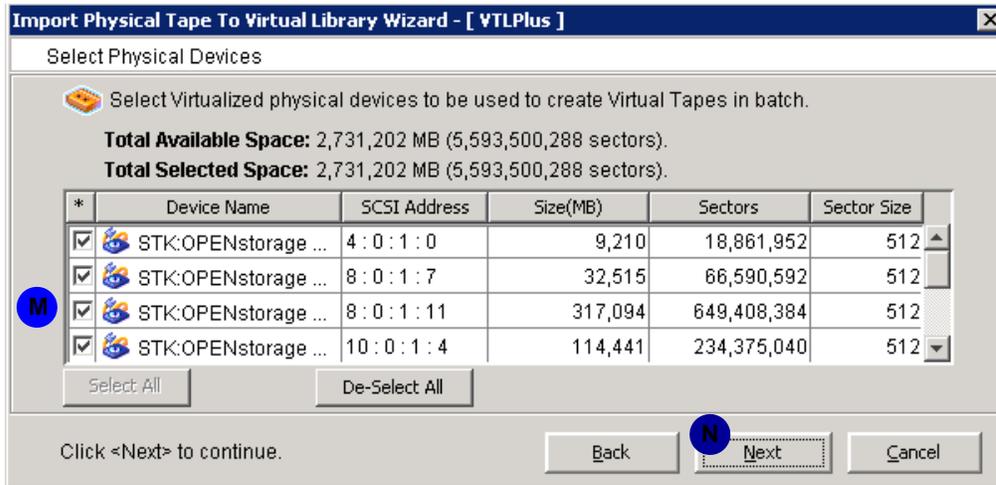
9. **When the** `Specify Batch Mode Information` **panel appears, enter a** `Virtual Tape Name Prefix` **that matches the convention used in the rest of the virtual library (P below).**
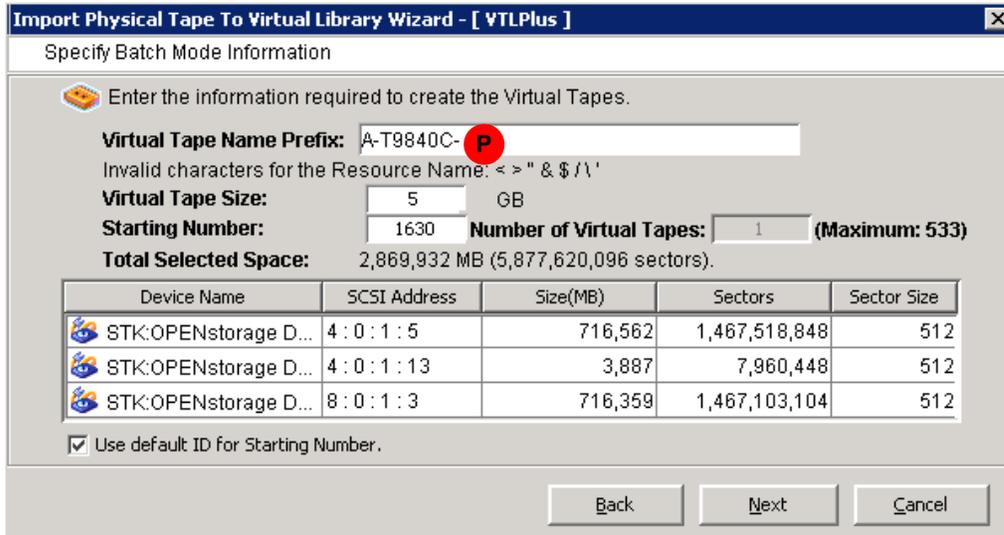
10. **Set the** `Virtual Tape Size` **to the full size of the emulated media (Q below), and** `Tab` **to another field to recalculate the** `Maximum` **number of tapes possible with the available storage (S). Make sure that the** `Number of Virtual Tapes` **that you will create in order to import your specified number of physical tapes (R) does not exceed the recalculated** `Maximum` **(S).**

11. **If the** `Number of Virtual Tapes` **that you will create in order to import your specified number of physical tapes (R above) exceeds the recalculated** `Maximum` **(S), stop here. You cannot import the number of tapes you specified.**

12. **Otherwise, reset the** `Virtual Tape Size` **to the default value for using capacity on demand with this type of media (T below). Check the** `Use default ID for Starting Number` **check box (U), and press** `Next` **(V).**
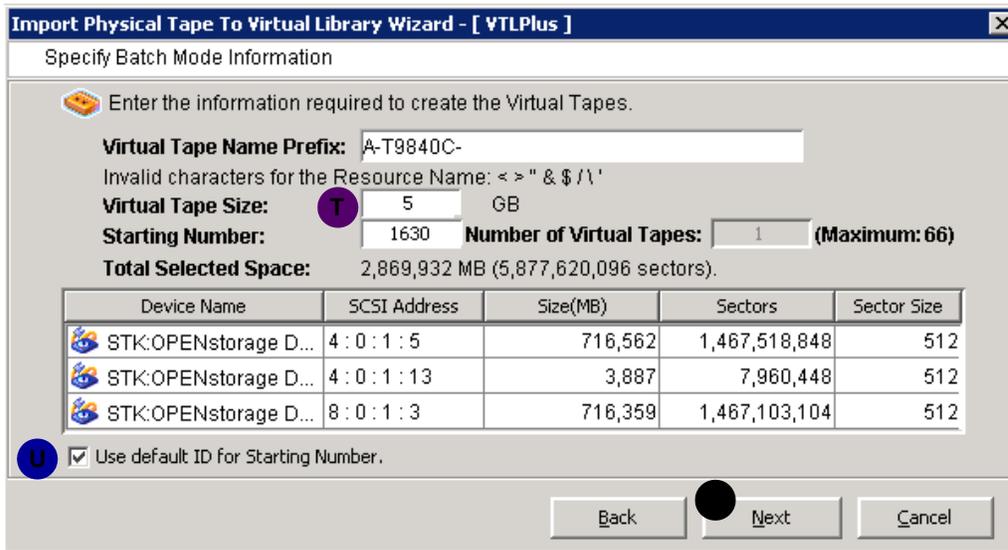
13. **Verify the information, and press** `Finish` **(W below) to import the tape.**
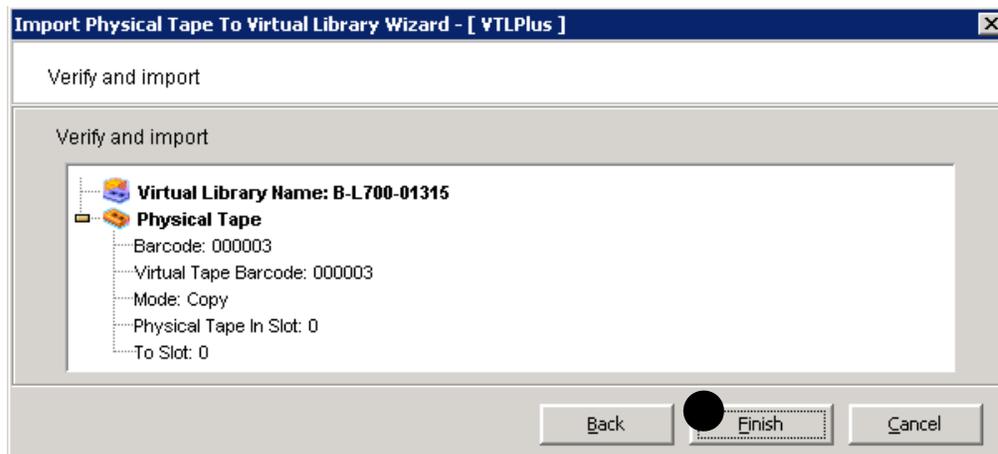
Next task: If you are working in an IBM iSeries/AS400 environment, go to "Importing cartridges in an IBM iSeries environment" on page 119. Otherwise, stop here.

▼ Importing cartridges in an IBM iSeries environment

1. **If you have not already done so, import tapes into the virtual library using the VTL console, as described in "Importing a physical tape into a virtual library" on page 113.**

2. **At the AS/400, re-inventory the tape library. In the option field next to the tape library, enter** `9 (INVENTORY)`**.**

3. **Add tapes to the inventory by entering either of the following at the command line:**

```
ADDTAPCTG DEV(library_device_name ) CTG(cartridge_identifier ) CGY(*NOSHARE)
CHKVOL(*NO)
```

```
ADDTAPCTG DEV(library_device_name ) CTG(cartridge_identifier ) CGY(*SHARE400)
CHKVOL(*NO)
```

The tape status changes from `INSERT` to `AVAILABLE`.

Stop here.

▼ Exporting virtual tape to physical tape

1. **In the object tree of the VTL console, right-click on the virtual tape node that you want to export (A below), and select** `Move to Vault` **from the context menu (B).**
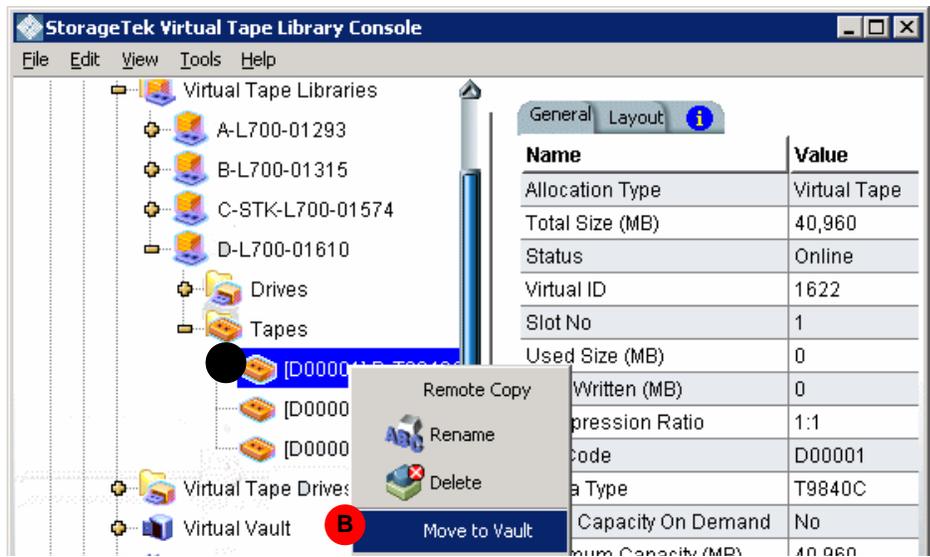
2. **When the** `Move Tape to Virtual Vault` **dialog appears, select the tape(s) that you want to move using the check boxes and/or selection buttons provided (C below). Press** `OK` **(D).**
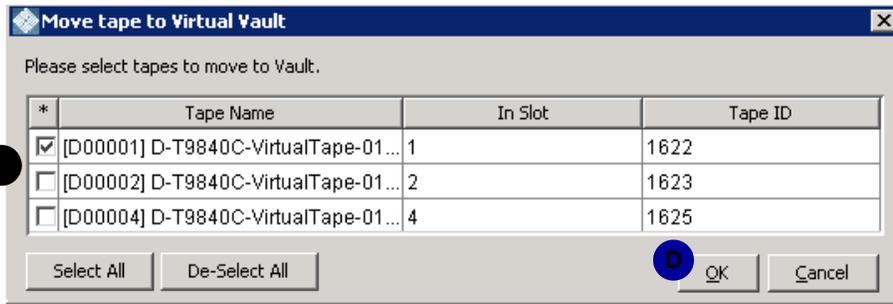
3. **Now, in the object tree of the VTL console, open the** `Virtual Vault` **node, and right-click the virtual tape that you want to export (E below). Select** `Export Tape` **from the context menu (F)**
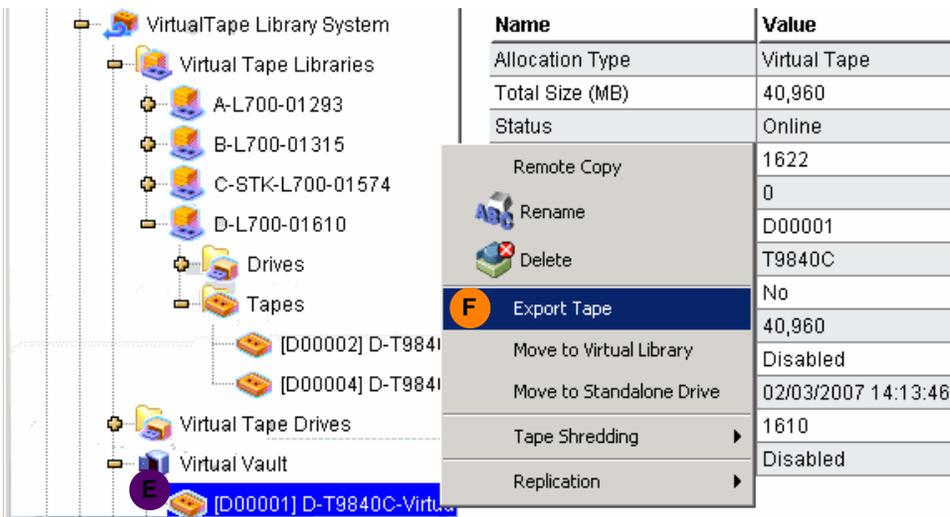
4. **When the** `Select a physical library or drive` **panel appears, use the list to select the library or device to which you want to export virtual tape (G below). Press Next (H).**

Export Virtual Tape To Physical Tape Library/Drive Wizard - [VTLPlus]

Select a physical library or drive

Select the physical tape library or drive to which you want to export this virtual tape.

Physical Tape Library/Drive
Library: LS: IP-129.80.115.112 acs-2 (LS-1629)

G

Click <Next> to continue.   Back   H Next   Cancel
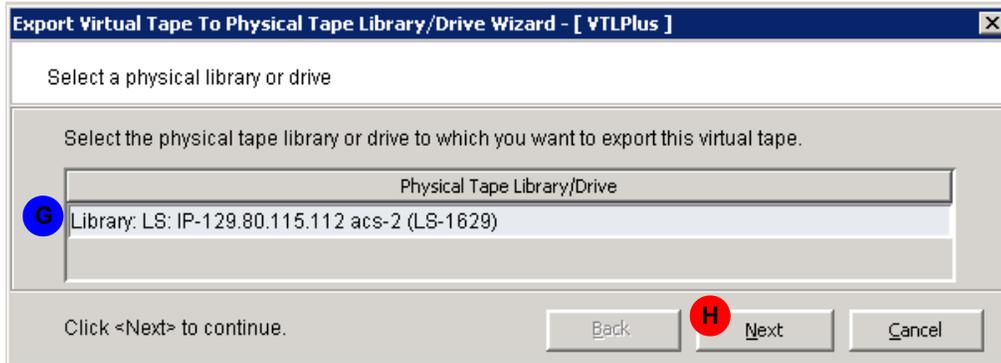
5. **Select how you want the data exported.**

   ■ Move Mode - Copies the contents of the virtual tape to its physical counterpart and then removes the virtual tape from the system. Specify a grace period if you want to keep the virtual tape for a time before deleting it. If you select EnableTape Duplication on the next dialog, the virtual tape data will not be deleted until the duplication job finishes successfully.

   ■ Copy Mode - Copies the contents of the virtual tape to its physical counterpart and retains the virtual tape after the data is transferred.

Export Virtual Tape To Physical Tape Library/Drive Wizard - [VTLPlus]

Select export mode.

Select export mode.

⊙ **Move Mode**

Moves the contents of the virtual tape to its physical counterpart and then removes the virtual tape from the system.

The grace period before deleting the tape   365   day(s)

○ **Copy Mode**

Copies the contents of the virtual tape to its physical counterpart and retains the virtual tape after the data is transferred.

J

□ **Eject physical tapes to I/E slots after export**

Moves physical tapes to I/E slots after exporting virtual tapes to physical tapes.

L □ Encrypt data when exporting to physical tape with the selected key.

Select a Key:

Click <Next> to continue.   Back   Next   Cancel

6. **Select or clear the Eject physical tapes to I/E slots after export check box.**

7. **Select Encrypt data when exporting to physical tape with the selected key if you want to encrypt the data on the tape.**

   You can select this option only if at least one key has been created. If you select this option, you must select the key to use. All the data on the tape will be indecipherable until is imported back to a virtual tape library and decrypted using the same key. Note that when you encrypt data, physical tape drive compression is disabled; it will be enabled if you do not encrypt data.

8. **Indicate if you want to enable tape duplication.**

   Tape duplication makes a duplicate copy of the physical tape when data is exported. You must have at least two identical physical libraries (same mode).

9. **If you wish to move the physical tapes to an import/export slot after the export operation is complete, check the** `Eject physical tapes ...` **check box (K above).**

10. **If you wish to encrypt the physical tape, check the** `Encrypt data ...` **check box, and supply a key using the control provided (L above).**

11. **Press** `Next` **(M above).**

12. **When the** `Select Virtual Tape(s)` **panel appears, select each virtual tape that you want to export using the check boxes at left (N below) or use the selection buttons (P).**

13. **For each tape, check the** `Same Barcode` **check box (Q below) unless you do not want to preserve the barcode.**

    If you check the `Same Barcode` check box, the VTL software will automatically export to a physical cartridge with the same barcode as the virtual cartridge.

    Your backup application may not be able to restore data from the physical backup tape if the barcode differs from that of the virtual tape.

14. **If you did not check the** `Same Barcode` **check box (Q below), use the** `Physical Tape` **spinner control (R) to select the physical tape that will hold the exported data.**

15. **Press** Next **(S below).**
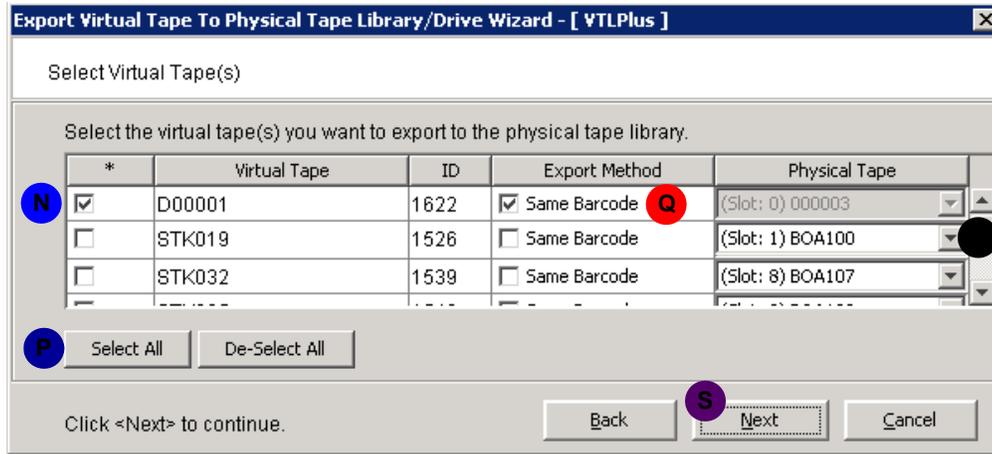
16. **When the** Verify and Export ... **panel appears, press** Finish **(T below).**
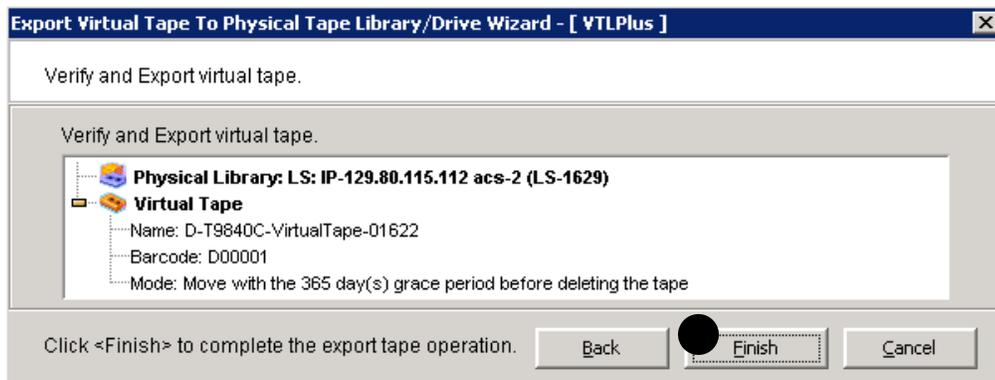
Stop here.

▼ Exporting cartridges to the virtual vault in an IBM iSeries environment

1. **Export a cartridge by entering the following at the command line:**

```
RMVTAPCTG DEV(library_device_name ) CTG(cartridge_identifier)
```

2. **If desired, use the VTL console to verify that the cartridges have been removed from the virtual library and placed in the virtual vault.**

Stop here.

Managing tape caching

In most circumstances, the Automated Tape Caching feature maintains tape caches and linkages automatically, provided that policies are suitably defined. However, when necessary, you can manage caching manually. This section explains:

- "Forcing migration to physical tape" on page 124
- "Manually freeing cache space" on page 124
- "Renewing cache for a directly linked tape" on page 124
- "Relinking physical tapes" on page 125

▼ Forcing migration to physical tape

To manually cause data in a cache to be migrated to physical tape, proceed as follows:

1. **In the object tree of the VTL console, right-click on a virtual tape cache.**

2. **Select** `Migrate to Physical Tape` **from the context menu.**

   Note that all data on the physical tape is overwritten.

Stop here.

▼ Manually freeing cache space

1. **If you need to release space in a single cache, in the object tree of the VTL console, right-click on a virtual tape cache, and select** `Reclaim Disk Space`**.**

   Note that all data in the cache is overwritten.

2. **To release space in multiple tape caches, in the object tree of the VTL console, right-click on the** `Virtual Tape Library System` **node, and select** `Reclaim Disk Space` **from the context menu.**

Stop here.

▼ Renewing cache for a directly linked tape

VTL software automatically recaches a direct link physical tape if the link is overwritten by a backup application. To manually renew the cache for a direct link tape, proceed as follows:

1. **In the object tree of the VTL console, right-click on the direct link tape that you wish to recache.**

2. **Select** `Renew Cache` **from the context menu.**

Stop here.

▼ Disabling a policy

To disable a tape caching policy:

1. **In the object tree of the VTL console, right-click on a virtual tape library, and select** `Automated Tape Caching` **from the context menu.**

2. **Clear the** `Enable Tape Caching Policy` **check box.**

   All the options that you previously set are retained, but data migration will not occur automatically until you select this check box again.

3. **Click** `OK`**.**

Stop here.

▼ Relinking physical tapes

If a directly linked physical tape is ejected from the physical tape library after the virtual tape has been released from cache, you have to relink the physical tape before you can access it from the VTL console.

Note – Once the physical tape is reloaded in a library, the backup application can inventory access the library and access the tape directly, if necessary.

---

1. **In the object tree of the VTL console, right-click on the virtual tape library, and select** `Sync Library` **from the context menu.**

2. **If you have multiple libraries, select the appropriate physical library.**

3. **When the** `Sync Library` **dialog appears, check the checkbox that corresponds to the physical tape that needs to be relinked (A below) or use the** `Select-All` **button.**
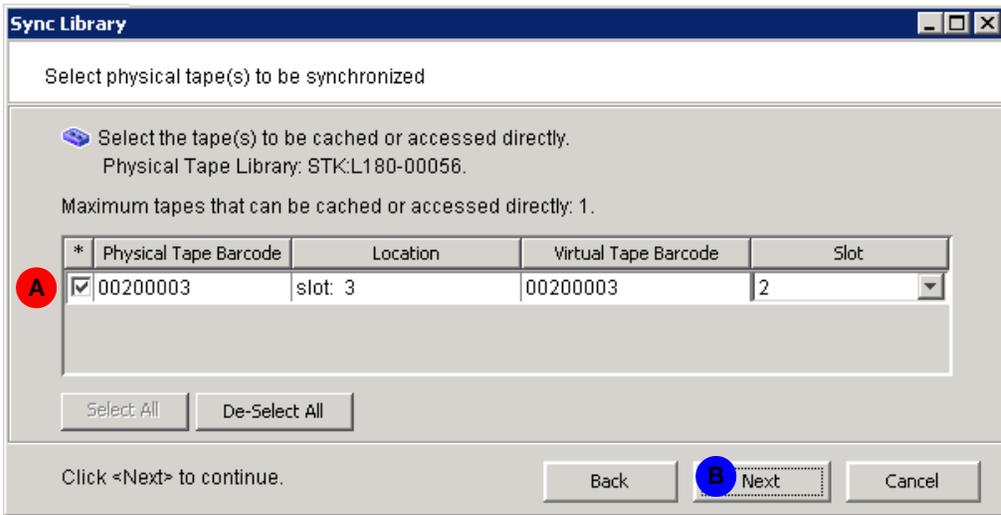
4. **Press** `Next` **(B above).**

5. **When the select the mode panel appears, click the** `Create Direct Link` **radio button (C below).**
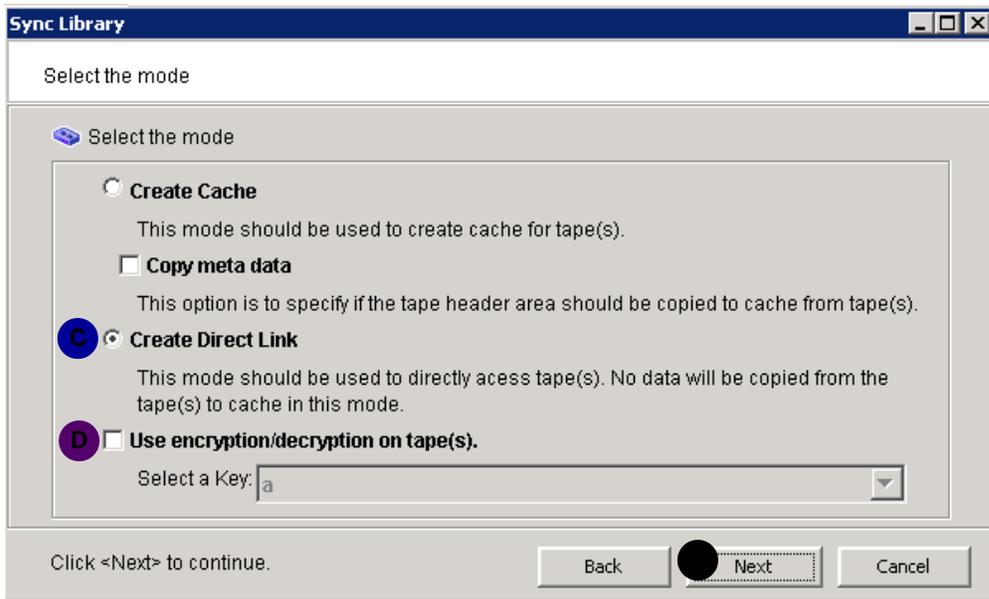
6. **If the data was encrypted before being migrated, check the** `Use encryption/decryption on tape(s)` **check box, and supply the select the appropriate key using the list control provided (D above).**

7. **Press** `Next` **(E above), then** `Finish`**.**

Stop here.

Creating and viewing reports

You can work with reports using the VTL console. See:

■ "Creating a report" on page 127

■ "Viewing a report" on page 130

■ "Exporting data from a report" on page 131.

▼ Creating a report

1. **In the object tree of the VTL console, right-click on the** `Reports` **node (A below), and select** `New` **from the context menu (B).**
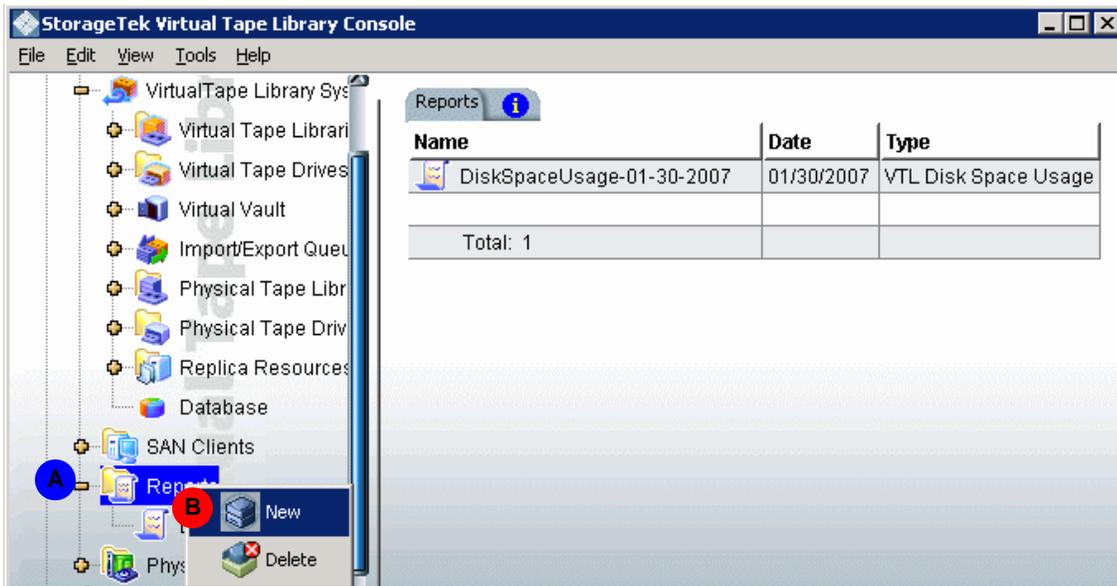
2. **When the** `Select a Report Type` **dialog appears, select a type from the list (C below). Press** `Next` **(D).**
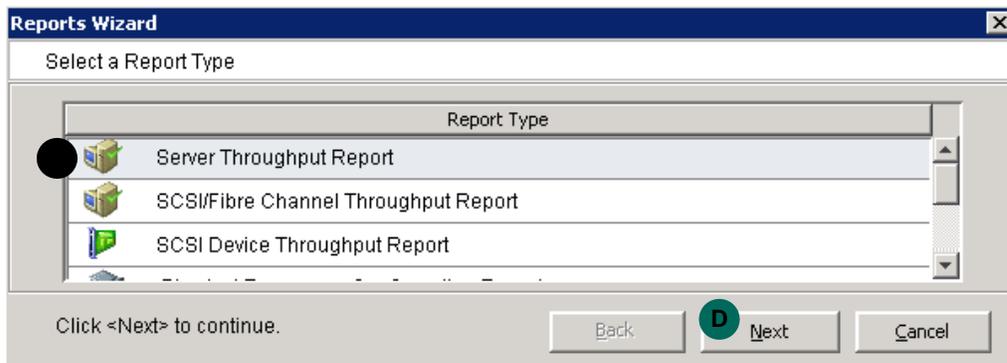
3. **When the** `Select Report Options` **panel appears, select the desired report properties using the controls provided (E and F below). Press** `Next` **(G).**
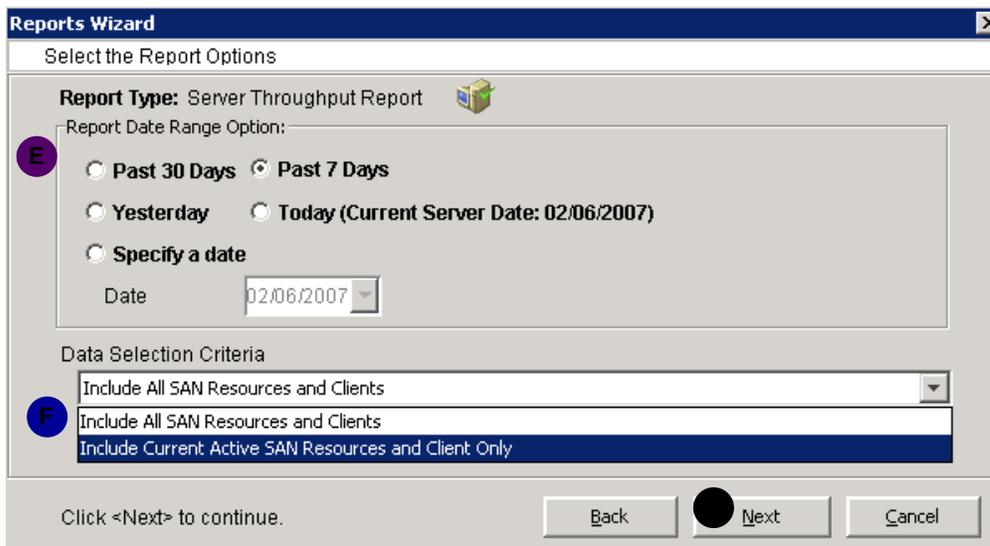
Note that different report types offer different options.

In the example above, the `Include All SAN Resources and Clients` option covers all current and previous configurations for the server (including physical tape libraries/drives and clients that you may have changed or deleted). The `Include Current Active SAN Resources and Clients Only` option covers only the physical tape libraries/drives and clients that are currently configured for this server.

4. **When the** `Enter the Report Name` **dialog appears, for the report, enter the name in the field provided (H below), and press** `Next` **(J).**

Reports Wizard

Enter the Report Name

Report Type: Server Throughput Report

(H) Report Name: ServerThroughput-02-06-2007

Invalid characters for the Report Name: , / \

Selected Report Options and Filters:

Date Time Range:
    Past 7 Days (01/30/2007 - 02/05/2007)
Data Selection Criteria
    Include All SAN Resources and Clients

Click <Next> to continue.   Back   **(J)** Next   Cancel
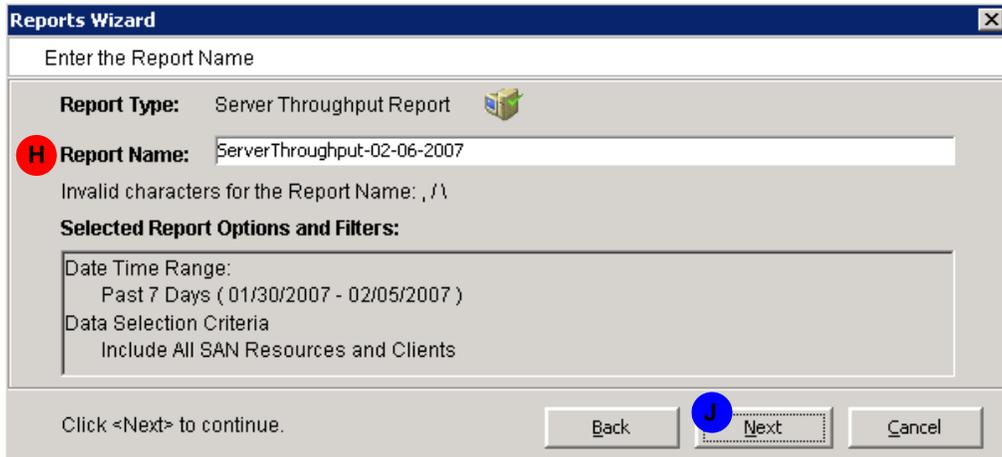
5. **When the** `Create the Report` **panel appears, press** `Finish` **(K below).**

Reports Wizard

Create the Report

Report Type: Server Throughput Report

Report Name: ServerThroughput-02-06-2007

Selected Report Options and Filters:

Date Time Range:
    Past 7 Days (01/30/2007 - 02/05/2007)
Data Selection Criteria
    Include All SAN Resources and Clients

Click <Finish> to confirm the creation of the report.   Back   **(K)** Finish   Cancel

Stop here.

▼ Viewing a report

1. **In the object tree of the VTL console, expand the** `Reports` **node (A below) to view the list of current reports.**

2. **Select the current report that you wish to view (B above).**

The desired report appears in the right-hand pane of the console (**C** above).

Stop here.

▼ Exporting data from a report

1. **In the object tree of the VTL console, expand the** `Reports` **node and right-click the name of the report that you want to export (A below).**

   You can export server and device throughput and usage report data to comma-or tab-delimited text files.
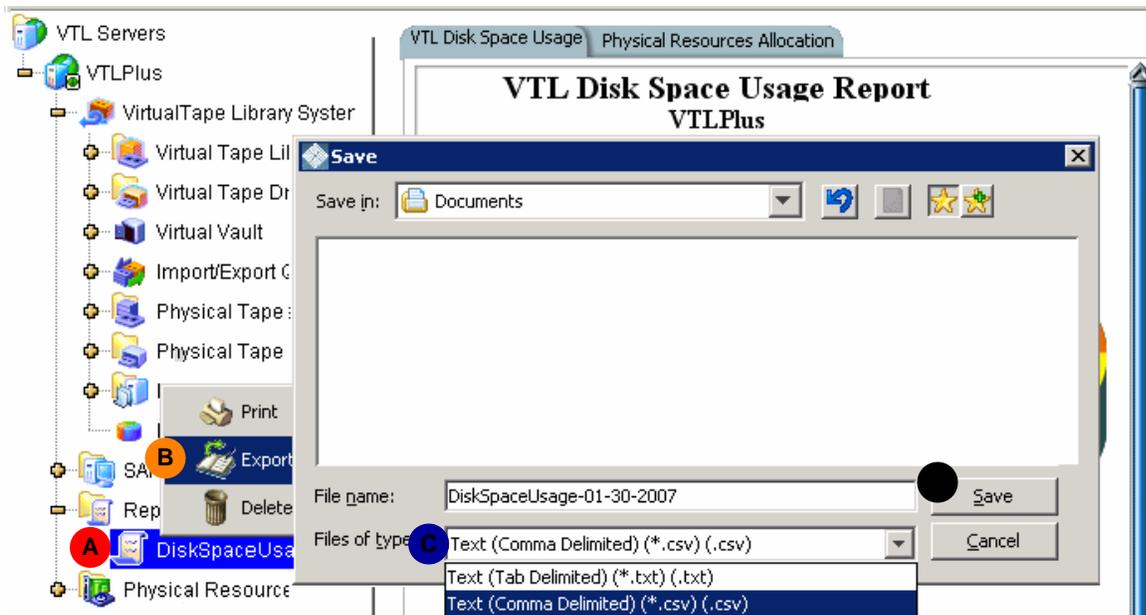
2. **In the context menu., select** `Export` **(B above).**

3. **When the** `Save` **dialog appears, use the** `Files of type` **list control to select the desired format (C above), and press** `Save` **(D).**

   Stop here.

Encrypting and shredding data

To ensure that the data that you export to physical tape is confidential and secure, VTL offers a Secure Tape Option that uses the Advanced Encryption Standard (AES) algorithm published by the National Institute of Standards and Technology, an agency of the U.S. government. With this option, you can create one or more keys that can be used to encrypt the data when it is exported to physical tape and decrypt it when it is imported back to virtual tapes. The data on the tape cannot be read without being decrypted using the appropriate key.

Each 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 tapes when you export them to physical tape, or you can create a unique key for each one. Creating multiple keys provides more security; in the unlikely event that a key is compromised, only the tapes that use that key would be affected. However, if you use multiple keys, you must keep track of which key applies to each tape so that you use the correct key to decrypt the data when you import the physical tape back to virtual 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 tapes to other locations that run VTL, you can also send them the key package. By importing the key package, administrators at the other sites can then decrypt the tapes when they are imported back into virtual tape libraries managed by VTL.

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.

For instructions, see the following:

- "Creating a key" on page 132
- "Changing a key name or password" on page 133
- "Deleting a key" on page 134
- "Exporting a key" on page 135
- "Importing a key" on page 136
- "Shredding a virtual tape" on page 137.

▼ Creating a key

1. **In the navigation tree, right-click the server name and click** `Key Management`**.**

2. **Click** `New`**.**

3. **In the** `Key Name` **text box (A below), type a unique name for the key (1–32 characters).**

4. **In the** `Secret Phrase` **text box (B below), type the phrase (25–32 characters, including numbers and spaces) that will be used to encrypt the data.**

   Save your secret phrase. Once you have created a key, you cannot change the secret phrase associated with that key.

5. **In the** `New Password` **and** `Confirm Password` **text boxes (C below), type a password for accessing the key (10–16 characters).**

You will need to provide this password when changing the key name, password, or password hint and when deleting or exporting the key.

You do not have to provide a unique password for each key. In fact, if you use the same password for multiple keys, you have to provide the password only once when you export multiple keys that all use the same password.

6. **In the** `Password Hint` **text box (D below), type a hint (0–32 characters) that will help you remember the password.**

This hint appears when you type an incorrect password and request a hint.

7. **Click** `OK` **(E above).**

Stop here.

▼ Changing a key name or password

Once you have created a key, you cannot change the secret phrase associated with that key. However, you can change the name of the key, as well as the password used to access the key and the hint associated with that password.

If you rename a key, you can still use that key to decrypt data that was encrypted using the old key name. For example, if you encrypt data using `Key1`, and you change its name to `Key2`, you can decrypt the data using `Key2`, since the secret phrase is the same.

To change a key name or password:

1. **In the navigation tree, right-click the server name, and click** `Key Management`**.**

2. **From the** `Key Name` **list, click the key you want to change.**

3. **Click** `Edit`**.**

4. **If you closed the** `Key Management` **dialog box after creating the key, type the current password for accessing this key in the** `Password` **text box.**

   If you just created the key, did not close the `Key Management` dialog box, and subsequently decided to change the key, you are not prompted for the password.

5. **Make the desired changes:**

6. **Click** `OK`**.**

Stop here.

▼ Deleting a key

Caution: Once you delete a key, you can no longer decrypt tapes that were encrypted using that key unless you subsequently create a new key that uses the exact same secret phrase, or import the key from a key package.

1. **In the navigation tree, right-click the server name and click** `Key Management`**.**

2. **From the** `Key Name` **list, click the key that you want to delete.**

3. **Click** `Delete`**.**

4. **In the** `Password` **text box, type the password for accessing this key.**

5. **Type** `YES` **to confirm.**

6. **Click** `OK`**.**

Stop here.

▼ Exporting a key

When you export a key, you create a separate file called a `key package` that contains one or more keys. You can then send this file to another site that uses VTL, and administrators at that site can import the key package and use the associated keys to encrypt or decrypt data.

Creating a key package also provides you with a backup set of keys. If a particular key is accidentally deleted, you can import it from the key package so that you can continue to access the data encrypted using that key.

1. **In the navigation tree, right-click the server name and click** `Key Management`**.**

2. **Click** `Export`**.**

3. **In the** `Package Name` **text box, type the file name to use for this key package (1–32 characters).**

4. **In the** `Decryption Hint` **text box, type a three-character hint.**

   When you subsequently attempt to import a key from this key package, you are prompted for a password. If you provide the correct password, the decryption hint specified here appears correctly on the `Import Keys` dialog box. If you provide an incorrect password, a different decryption hint appears. You can import keys using an incorrect password, but you will not be able to decrypt any files using those keys.

5. **From the** `Select Keys to Export` **list, select the key(s) that you want to include in the key package.**

   When you select a key or click `Select All`, you are prompted to provide the password for each key. (If multiple selected keys use the same password, you are prompted for the password only once, when you select the first key that uses that password.)

   After you type the password in the `Password` text box, that password appears in the `Password for All Keys in Package` area on the `Export Keys` dialog box. By default, the password is displayed as asterisks. To display the actual password, select the `Show clear text` check box.

   If you selected a key and subsequently decide not to include it in the key package, you can clear the key. You can also clear all selected keys by clicking `De-Select All`.

6. **Select** `Prompt for new password for all keys in package` **if you want to create a new password for the key package.**

   If you select this option, you will be prompted to provide the new password when you click `OK` on the `Export Keys` dialog box. You will subsequently be prompted for this password when you try to import a key from this package. In addition, all keys imported from this package will use this new password rather than the password originally associated with each key.

   If you clear this option, this package will use the same password as the first selected key (which appears in the `Password for All Keys in Package` area), and you must provide this password when you try to import a key from this package. You must also provide this password when you subsequently change, delete, or export any key imported from this package.

7. **In the** `Save in this directory` **text box, type the full path for the file.**

8. **Click** `OK`**.**

   If you selected the `Prompt for new password for all keys in package` check box, type the new password (10–16 characters) in the `New Password` and `Confirm Password` text boxes, type a hint for that password (0–32 characters) in the `Password Hint` text box.

   A file with the specified package name and the extension `.key` is created in the specified location.

Stop here.

▼ Importing a key

Once you have created a key package, you can open that package and specify which keys to import into VTL. Once you import a key, you can use that key to encrypt or decrypt data.

To import a key:

1. **In the navigation tree, right-click the server name and click** `Key Management`**.**

2. **Click** `Import`**.**

3. **In the** `Find Package` **text box, type the full path to the key package.**

4. **Click** `View`**.**

5. **Type the password for accessing the key package in the** `Password` **text box.**

   Note: After you provide the password, make sure that the displayed `Decryption Hint` matches the decryption hint specified when the key package was created. If the hint is not correct, click `Password` and provide the correct password for accessing

the key package. If you provide an incorrect password, you will still be able to import the keys in the package, but you will not be able to use them to decrypt any data that was previously encrypted using those keys.

6. **From the** `Select Keys to Import` **list, select the keys that you want to import.**

   You can select only those keys that have a green dot and the phrase `Ready for Import` in the `Status` column. A red dot and the phrase `Duplicate Key Name` indicates that a key of the same name already exists in this instance of VTL and cannot be imported.

   If you selected a key and subsequently decide not to import it, you can clear the key. You can also clear all selected keys by clicking `De-Select All`. (You can click this button only if the `Show All Keys` check box is cleared.)

   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 instance of VTL, 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 tapes that were encrypted using that key, and you can also import the key named Key1 from the key package and use it to decrypt tapes that were encrypted using that key.

7. **Click** `OK`**.**

   The imported keys appear in the `Key Name` list on the `Key Management` dialog box. When you subsequently export or import a tape, these key names also appear in the `Select a Key` list.

Stop here.

▼ Shredding a virtual tape

Just as deleting a file from your hard drive does not completely destroy the file, deleting a virtual tape does not completely destroy the data on the tape. If you want to ensure that the data is unrecoverable, you must shred the tape.

Shredding a virtual tape destroys all data on the tape, making it impossible to recover the data. Tape shredding uses a military standard to destroy data on virtual tapes by overwriting it with a random patterns of bits, rendering the data unreadable.

To shred tapes:

1. **Move the tape(s) you want to shred to the virtual vault. In the object tree of the VTL console, start by right-clicking on a tape that you want to shred (A below), and select** `Move to Vault` **(B) from the context menu.**
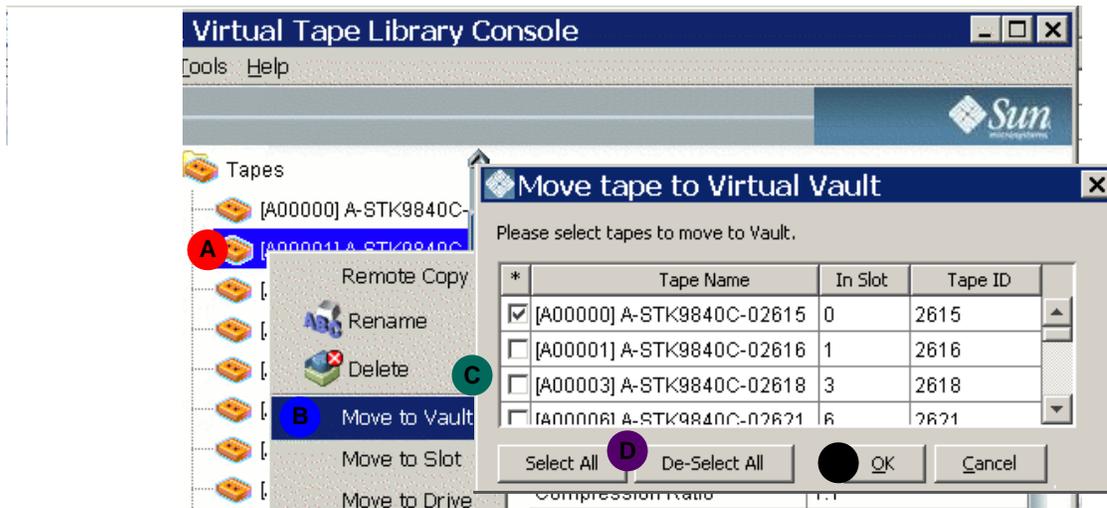
2. **When the** `Move tape to Virtual Vault` **dialog appears, use the check boxes (C above) and selection buttons (D) to select the tapes you want to shred. Press** `OK` **(E).**

3. **Select the tape(s) you want to shred. In the object tree of the VTL console, click on the** `Virtual Vault` **(F below).**
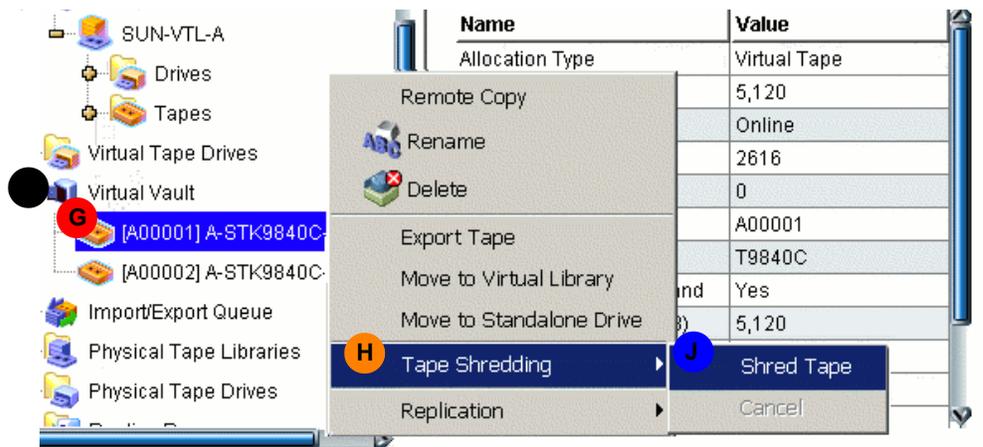
4. **Right-click on one of the tapes that you want to shred (G above), and select** `Tape Shredding` **(H) and** `Shred Tape` **(J) from the context menus.**

5. **When the** `Shred Virtual Tape Resource` **dialog appears, check the** `Delete After Shredding` **check box (K above) if you wish to delete the tape after shredding.**

6. **In the space provided, type** `YES` **(L above) to confirm the shredding operation, and press** `OK` **(M).**

   You can view the status by highlighting the virtual tape in the vault. The status bar displays the progress.

   If you want to cancel the shredding process, right-click on the tape or the `Virtual Vault` object and select `Tape Shredding > Cancel`.

Note – Tape shredding may adversely affect backup performance. We recommend that you perform tape shredding when there are no backups running.

Stop here.

Working with the Event Log

The Event Log details significant occurrences during the operation of the VTL Server. The Event Log can be viewed in the VTL Console when you highlight a server in the tree and select the `Event Log` tab in the right pane.

The columns displayed are:

Type	**I**: This is an informational message. No action is required.
	W: This is a warning message that states that something occurred that may require maintenance or corrective action. However, the VTL system is still operational.
	E: This is an error that indicates a failure has occurred such that a device is not available, an operation has failed, or a licensing violation. Corrective action should be taken to resolve the cause of the error.
	C: These are critical errors that stop the system from operating properly.
Date	The date on which the event occurred.
Time	The time at which the event occurred.
ID	This is the message number.
Event Message	This is a text description of the event describing what has occurred.

The VTL console lets you work with logs in the following ways:

- "Viewing an event log" on page 140
- "Sorting an event log" on page 140
- "Quickly printing an event log" on page 141
- "Filtering, exporting, purging, and printing an event log" on page 141

▼ Viewing an event log

1. **In the object tree of the VTL console, select the server that you want to check.**

2. **In the panel on the right side of the VTL console, click on the** Event Log **tab.**

Stop here.

▼ Sorting an event log

1. **On the** Event Log **tab, click on the column head that you want to use as a sort key.**

2. **If you want to reverse the sort order, click on the column heading again.**

Stop here.

▼ Quickly printing an event log

1. **From the VTL console main menu, select** `File`.

2. **From the submenu, select** `Print`.

Stop here.

▼ Filtering, exporting, purging, and printing an event log

1. **With the** `Event Log` **tab (A below) of the server open, right-click on the server icon in object tree of the VTL console (B).**
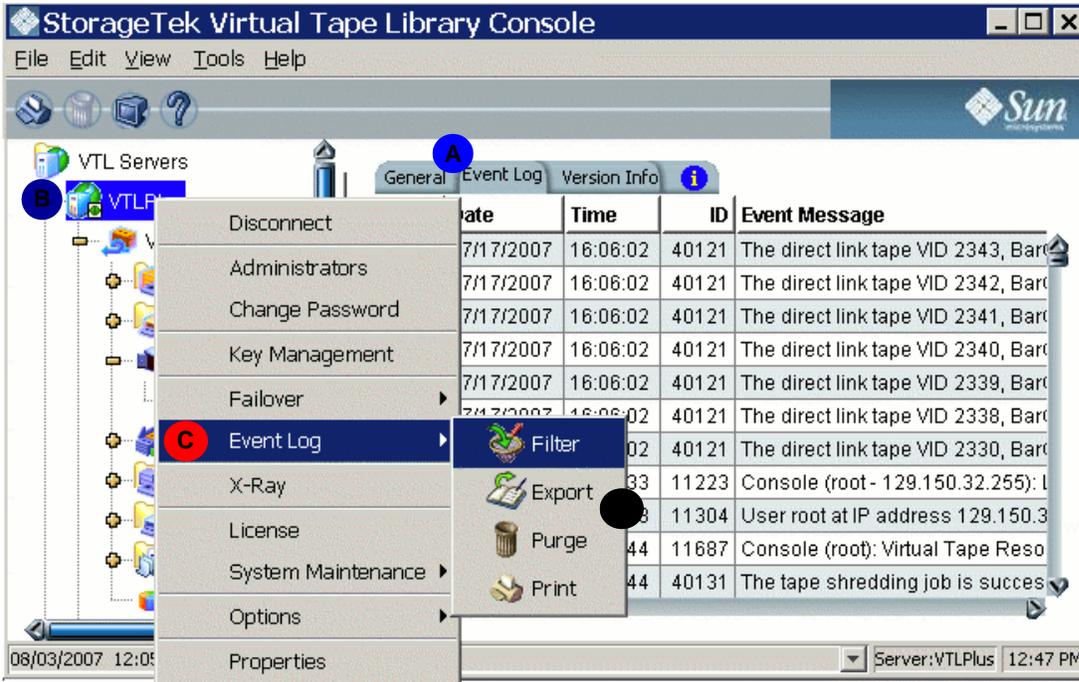
2. **From the context menu, select** `Event Log` **(C above).**

3. **From the submenu, select the operation that you wish to perform (D above).**

   If you wish to search or filter the log, the `Event Log Options` dialog (**E** below) lets you set up and apply your criteria.
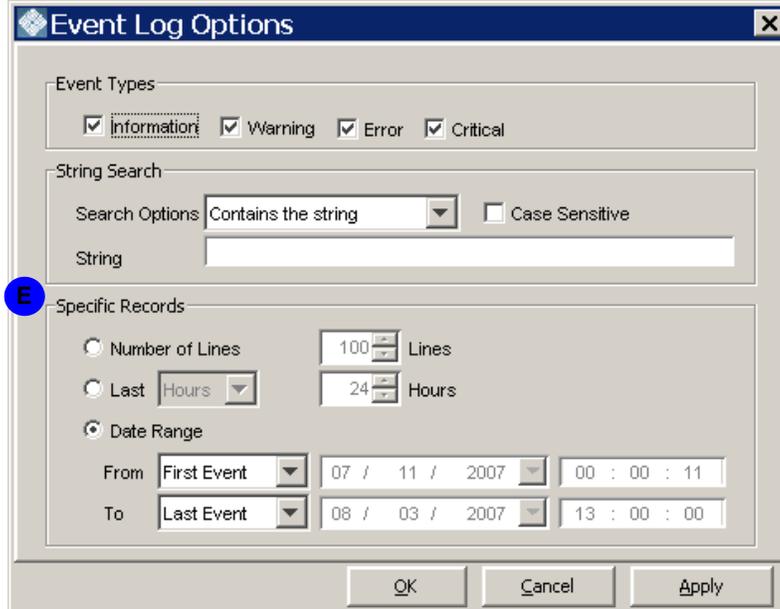
Stop here.

Using the Attention Required tab

When events that may require user intervention occur, the VTL console flags the server icon with an exclamation point (`!`) and displays notifications in the `Attention Required` tab of the server properties sheet. Typical events include physical library failures, appliance hardware errors, replication errors, and completed import/export jobs. The VTL console lets you manage Attention Required notifications notifications in the following ways:

■ "Accessing the Attention Required tab" on page 143

■ "Clearing issues from the Attention Required list" on page 143.

▼ Accessing the Attention Required tab

1. In the VTL object tree, locate the flagged server (A below).
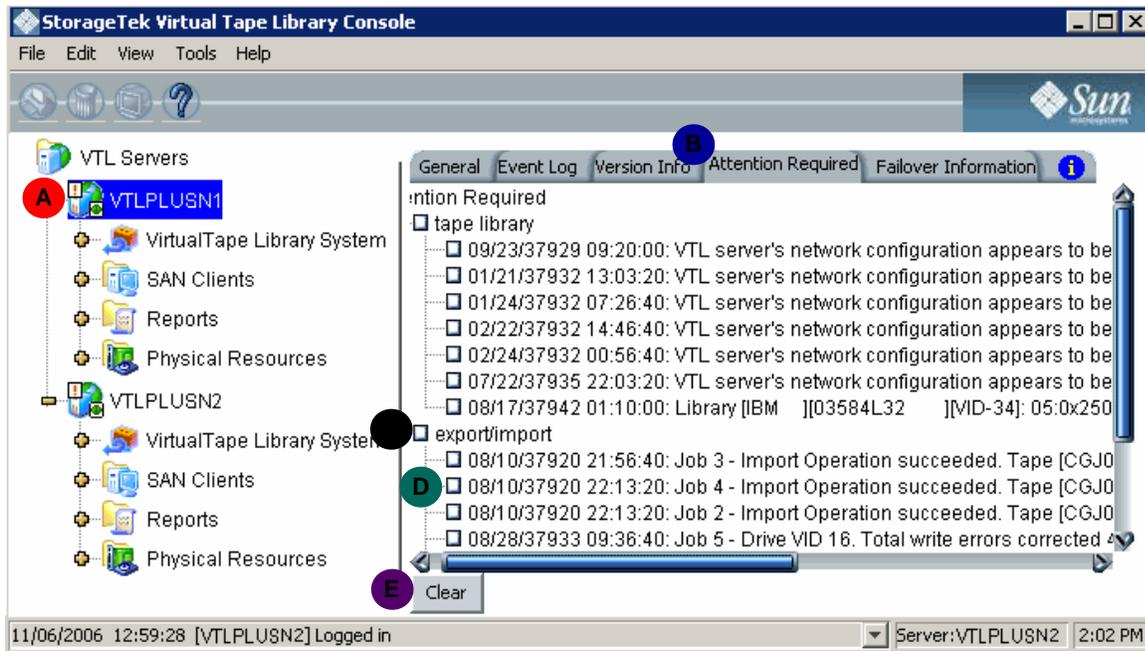
2. In the right-hand pane, select the `Attention Required` tab of the server property sheet (B above).

Stop here.

▼ Clearing issues from the Attention Required list

1. If you want to clear an entire class of events from the list, check the check box for the event type (C above).

2. If you want to clear an individual event, check the corresponding check box (D above)

3. Click the `Clear` button (E above).

Stop here.

Managing VTL servers

The VTL console lets you manage the server node by:

- "Setting server properties" on page 144
- "Configuring SNMP traps" on page 144.

▼ Setting server properties

1. **Right-click on the server and select** `Properties`.

2. **On the** `Activity Database Maintenance` **tab, indicate how often the VTL activity data should be purged.**

   The Activity Log is a database that tracks all system activity, including all data read, data written, number of read commands, write commands, number of errors etc. This information is used to generate information for the VTL reports.

3. **On the** `SNMP Maintenance` **tab, VTL to send traps to your SNMP manager.**

   Refer to "Configuring SNMP traps" on page 144 for more information.

4. **On the** `Auto Save` **tab, enter information to replicate your VTL configuration to another server.**

   This protects your configuration if the VTL server is lost. Refer to "Automatically backing up the VTL configuration" on page 80 for more information.

5. **On the** `Storage Monitoring` **tab, enter the maximum amount of storage that can be used by VTL before you should be alerted.**

   When the utilization percentage is reached, a warning message will be sent to the Event Log.

Stop here.

▼ Configuring SNMP traps

VTL provides Simple Network Management Protocol (SNMP) support to integrate VTL management into an existing enterprise management solution, such as HP OpenView, CA Unicenter, IBM Tivoli NetView, or BMC Patrol.

By default, event log messages will `not` be sent, but you may want to configure VTL to send certain types of messages. To do this:

1. **In the Console, right-click on your VTL server appliance and select** `Properties`.

2. **Select the** SNMP Maintenance **tab.**

3. **Indicate the information that should be included in traps sent to your SNMP manager.**

   SysLocation - Enter the location that should be included in traps.

   SysContact - Enter any contact information that should be included in traps. This could be a name or an email address.

4. **Specify the type of message that should be sent.**

   Five levels of messages are available:

   - None: no messages will be sent.
   - Critical: only critical errors that stop the system from operating properly will be sent.
   - Error: errors (failure such as a resource is not available or an operation has failed) and critical errors will be sent.
   - Warning: warnings (something occurred that may require maintenance or corrective action), errors, and critical errors will be sent.
   - Information: informational messages, errors, warnings, and critical error messages will be sent.

5. **Click** Add **to enter the name of your SNMP server and a valid SNMP community name.**

6. **To verify that SNMP traps are set up properly, set the level to** Informational **and then do anything that causes an entry to be added to the event log (such as logging into the VTL console or creating a new virtual tape library or virtual tape drive).**

   You should see an SNMP trap for the event.

Stop here.

Installing the VTL console

The Virtual Tape Library console application can be installed on a full range of operating platforms. In most cases, a Sun service representative installs the console on one customer-provided server as part of the initial deployment. Customers can install as many additional instances as required on other machines. Note, however, that no more than two (2) instances of the console can access the same VTL server at the same time.

To install the console, follow the instructions for the selected host type:

■ "For information on the text-based, VTL command line user interface, see Appendix A, "VTL command line reference" on page 173." on page 147

■ "Installing the console on Linux platforms" on page 148

■ "Installing the console on Microsoft Windows platforms" on page 148.

Note – For information on the text-based, VTL command line user interface, see Appendix A, "VTL command line reference" on page 173.

▼ Installing the console on Solaris platforms

On Solaris systems, you install the console using the procedure below.

1. **Log in to the host as the** `root` **user.**

2. **Using Secure File Transfer Protocol (`sftp`), download the installation files to the client.**

   For x86 platforms, select the `i386` package:

   ```
   % sftp vtladmin@appliance_IP-address
   sftp> get /software/Solaris/vtlconsole-n.nn-n.nnn.i386.pkg
   ```

   For SPARC platforms, select the `sparc` package:

   ```
   % sftp vtladmin@appliance_IP-address
   sftp> get /software/Solaris/vtlconsole-n.nn-n.nnn.sparc.pkg
   ```

3. **If you are installing the console software on an x86 platform, enter the following command, and respond to the on-screen prompts:**

```
% pkgadd -d vtlconsole-n.nn-n.nnn.i386.pkg
```

4. **If you are installing the console software on a SPARC platform, enter the following command, and respond to the on-screen prompts:**

```
% pkgadd -d vtlconsole-n.nn-n.nnn.sparc.pkg
```

5. **To launch the console, enter the following command:**

```
% /usr/local/vtlconsole/vtlconsole &
```

Stop here.

▼ Installing the console on Linux platforms

On Linux systems, you install the console manually, using the procedure below.

1. **To install the console software, log in to the host as the** `root` **user.**

2. **Using Secure File Transfer Protocol (**`sftp`**), download the installation files to the client:**

```
% sftp vtladmin@appliance_IP-address
sftp> get /software/Linux/vtlconsole-n.nn-n.nnn.i386.rpm
```

3. **To install the console software, enter the following command, and respond to the on-screen prompts:**

```
% rpm -i vtlconsole-n.nn-n.nnn.i386.rpm
```

   The console will install in the `/user/local/vtlconsole` directory.

4. **To launch the console, enter the following command:**

```
% /usr/local/vtlconsole/vtlconsole &
```

Stop here.

▼ Installing the console on Microsoft Windows platforms

The VTL installation directory on the server includes a setup program that installs the console software on Windows computers.

1. **If you are not a member of the** `Power User` **or** `Administrator` **groups on the host, obtain the required level of permissions or stop here.**

   You must be a `Power User` or `Administrator` to install software on a Windows host.

2. **Using Secure File Transfer Protocol (**`sftp`**), log on to the VTL server, change to the** `usr/vtl/packages/build/Windows/` **directory, and download all listed installation files to a temporary directory on the client:**

```
% sftp vtladmin@appliance_IP-address
sftp> cd /software/Windows/
sftp> ls
data1.cab     ikernel.ex_    layout.bin     Setup.ini
data1.hdr     ISInstall.exe  setup.bmp      setup.inx
data2.cab     ISInstall.ini  Setup.exe
sftp> get *.*
```

`sftp` software is not standard with most versions of Microsoft Windows, but various, compatible, third-party `sftp` implementations are available, notably the one that comes with the puTTY open-source terminal-emulation application.

3. **Using Explorer, change to the temporary directory, and double-click on** `setup.exe` **to launch the console installation program.**

Stop here.

▼ Launching the VTL console on a remote host

1. **To launch the console on a Sun Solaris workstation, open a terminal window and enter the command shown below:**

```
% /usr/local/vtlconsole/vtlconsole &
```

2. **On a Microsoft Windows system, press the** `Start` **bar to access the main menu system, and select** `All Programs > Sun Microsystems> VTL 5.0> VTL Console`**.**

3. **To launch the console on a Linux workstation, open a terminal window and enter the command shown below:**

```
% /usr/local/vtlconsole/vtlconsole &
```

Stop here.

Recovery following a system failure

To recover a VTL high-availability system following a failure on one node, carry out the following tasks:

■ "Failback" on page 151

■ "Resuming backups following a failover/failback" on page 161.

Failback

For best results, run failback as a manual process, using the procedure outlined below.

▼ Initiating failback

For the purposes of this description, the current, active node is *VTLPLUSN2*, the failover node for *VTLPLUSN1*, the failed/offline node.

1. **Open a terminal window on the management host, and** ssh **to the IP address of the currently active node,** *VTLPLUSN2***:**

```
[VTL_Plus]vtladmin# ssh vtladmin@nnn.nnn.nnn.nny
Connecting to nnn.nnn.nnn.nny ...
Password:
```

where *nnn.nnn.nnn.nny* is the management or "server" IP address of *VTLPLUSN2*, the node that took over for the failed server node, *VTLPLUSN1* and vtladmin is the VTL administrator account user ID.

2. **Make sure that you are logged in to the actual, active node:**

```
[VTL_Plus]vtladmin# uname -a
SunOS VTLPLUSN2 n.nn Generic_nnnnnn-nn i86pc i386 i86pc
```

The system should display the expected node name.

3. **If you are not logged in to the correct system, you may have accidently logged into the service ("monitoring") IP address of the failed node. Close the** `ssh` **session, and** `ssh` **to the other IP address for the current, active node.**

4. **Change to the directory that holds the VTL executables:**

```
[VTL_Plus]vtladmin# cd /usr/local/vtl/bin
```

5. **Run the** `vtl status` **command:**

```
[VTL_Plus]vtladmin# vtl status

Sun Microsystems VTL Server vn.nn  (Build nnnn)
Copyright 2001-2007 by FalconStor. All Rights Reserve

Status of VTL SNMPD Module................ [RUNNING]
Status of VTL QLogic Module.............. [RUNNING]
Status of VTL Authentication Module....... [RUNNING]
Status of VTL Server (Compression) Module. [RUNNING]
Status of VTL Server (FSNBase) Module..... [RUNNING]
Status of VTL Server (Upcall) Module...... [RUNNING]
Status of VTL Server (Event) Module....... [RUNNING]
Status of VTL Server (Path Manager) Module [RUNNING]
Status of VTL Server (Application)........ [RUNNING]
Status of VTL FC Target Module............ [RUNNING]
Status of VTL Server VTL Upcall Module.... [RUNNING]
Status of VTL Server VTL Upcall Daemon.... [RUNNING]
Status of VTL Server VTL Module........... [RUNNING]
Status of VTL Communication Module........ [RUNNING]
Status of VTL Logger Module............... [RUNNING]
Status of VTL Self Monitor Module......... [RUNNING]
Status of VTL Failover Module............. [RUNNING]
```

6. **If one or more VTL processes are not** `RUNNING`**, stop the server software and then restart:**

```
[VTL_Plus]vtladmin# vtl stop all
...
[VTL_Plus]vtladmin# vtl start
```

7. Run the `sms` **command. The results should look like those shown.**

```
[VTL_Plus]vtladmin# sms
Usage: sms {force|nas|nasc|fm|sm|bmr|bmrreset|setroot
(sm/fm)|clearreboot(sm/fm)
} {value}
          bmr - to set the BMR health status
          bmrreset - to reset BMR value
          nas - to reset the NAS failure status
          nasc - to set nas health check
          force - enable force up fm - to set ipstorfm debug level
          sm - to set ipstorsm debug level
Last Update by SM: Sun Jan 28 15:32:39 2007
Last Access by RPC: Sun Jan 28 15:32:35 2007
FailOverStatus: 3(UP)
Status of IPStor Server (Transport) : OK
Status of IPStor Server (Application) : OK
Status of IPStor Authentication Module : OK
Status of IPStor Logger Module : OK
Status of IPStor Communication Module : OK
Status of IPStor Self-Monitor Module : OK
Status of IPStor NAS Modules: OK(0)
Status of IPStor Fsnupd Module: OK
Status of IPStor ISCSI Module: OK
Status of IPStor BMR Module: OK( 0)
Status of FC Link Down : OK
Status of Network Connection: OK
Status of force up: 0
Broadcast Arp : NO
Number of reported failed devices : 0
NAS health check : NO
XML Files Modified : NO
IPStor Failover Debug Level : 0
IPStor Self-Monitor Debug Level : 0
Do We Need To Reboot Machine(SM): NO
Do We Need To Reboot Machine(FM): NO
Nas Started: NO
```

8. Open a terminal window on the management host, and `ssh` **to the service ("monitoring") IP address of the failed node,** *VTLPLUSN1***:**

```
[mgt_host]user# ssh vtladmin@nnn.nnn.nnn.nnw
Connecting to nnn.nnn.nnn.nnw ...
Password:
```

where *nnn.nnn.nnn.nnw* is the service IP address of the failed node, and `vtladmin` is the VTL administrator account user ID. We use the service/monitoring address because it stays with the host following failover (the management IP address of a failed node transfers to the remaining active node during failover).

9. **Make sure that you are logged in to the actual, failed node:**

```
[VTL_Plus]vtladmin# uname -a
SunOS VTLPLUSN1 n.nn Generic_nnnnnn-nn i86pc i386 i86pc
```

The system should display the expected node name.

10. **If you are not logged in to the correct system, you have accidently logged into the management IP address (which always connects to the active node) rather than the service ("monitoring") address. Close the** `ssh` **session, and** `ssh` **to the other IP address for the failed node.**

11. **Change to the directory that holds the VTL executables:**

```
[VTL_Plus]vtladmin# cd /usr/local/vtl/bin
```

12. **Before proceeding further, make sure that no I/O is being sent to the failed node. Make sure that all backup jobs have completed and that failover has completed successfully. Stop I/O, if necessary.**

If host I/O is not stopped, data may be lost.

13. **Run the** `sms` **command, and make sure that the** `FailOverStatus` **is** `DOWN` **(failed over to the standby server):**

```
[VTL_Plus]vtladmin# sms
Usage: sms {force|nas|nasc|fm|sm|bmr|bmrreset|setroot
(sm/fm)|clearreboot(sm/fm)
} {value}
          bmr - to set the BMR health status
          bmrreset - to reset BMR value
          nas - to reset the NAS failure status
          nasc - to set nas health check
          force - enable force up fm - to set ipstorfm debug level
          sm - to set ipstorsm debug level
Last Update by SM: Sun Jan 28 15:32:39 2007
Last Access by RPC: Sun Jan 28 15:32:35 2007
FailOverStatus: 3(DOWN)
Status of IPStor Server (Transport) : OK
Status of IPStor Server (Application) : OK
Status of IPStor Authentication Module : OK
Status of IPStor Logger Module : OK
Status of IPStor Communication Module : OK
Status of IPStor Self-Monitor Module : FAIL
Status of IPStor NAS Modules: OK(0)
Status of IPStor Fsnupd Module: OK
Status of IPStor ISCSI Module: OK
Status of IPStor BMR Module: OK( 0)
Status of FC Link Down : OK
Status of Network Connection: OK
Status of force up: 0
Broadcast Arp : NO
Number of reported failed devices : 0
NAS health check : NO
XML Files Modified : NO
IPStor Failover Debug Level : 0
IPStor Self-Monitor Debug Level : 0
Do We Need To Reboot Machine(SM): NO
Do We Need To Reboot Machine(FM): NO
Nas Started: NO
```

14. **Restart the failed server node gracefully, using the** `init6` **command:**

```
[VTL_Plus]vtladmin# init6
```

15. **Once the restart has completed, open a terminal window on the management host, and** `ssh` **to the IP address of the restarted node,** *VTLPLUSN1*:

```
[mgt_host]user# ssh vtladmin@nnn.nnn.nnn.nnx
Connecting to nnn.nnn.nnn.nnx ...
Password:
```

where *nnn.nnn.nnn.nnx* is the service ("monitoring") IP address of the restarted node, and `vtladmin` is the VTL administrator account user ID.

16. **Make sure that you are logged in to the actual, restarted node:**

```
[VTL_Plus]vtladmin# uname -a
SunOS VTLPLUSN1 n.nn Generic_nnnnnn-nn i86pc i386 i86pc
```

The system should display the expected node name.

17. **If you are not logged in to the correct system, you have accidently logged into the management IP address (which always connects to the active node) rather than the service ("monitoring") address. Close the ssh session, and ssh to the other IP address for the failed node.**

18. **Change to the directory that holds the VTL executables:**

```
[VTL_Plus]vtladmin# cd /usr/local/vtl/bin
```

19. **Run the `vtl status` command:**

```
[VTL_Plus]vtladmin# vtl status

Sun Microsystems VTL Server vn.nn (Build nnnn)
Copyright 2001-2007 by FalconStor. All Rights Reserve

Status of VTL SNMPD Module............... [RUNNING]
Status of VTL QLogic Module.............. [RUNNING]
Status of VTL Authentication Module....... [RUNNING]
Status of VTL Server (Compression) Module. [RUNNING]
Status of VTL Server (FSNBase) Module..... [RUNNING]
Status of VTL Server (Upcall) Module...... [RUNNING]
Status of VTL Server (Event) Module....... [RUNNING]
Status of VTL Server (Path Manager) Module [RUNNING]
Status of VTL Server (Application)........ [RUNNING]
Status of VTL FC Target Module............ [RUNNING]
Status of VTL Server VTL Upcall Module.... [RUNNING]
Status of VTL Server VTL Upcall Daemon.... [RUNNING]
Status of VTL Server VTL Module........... [RUNNING]
Status of VTL Communication Module........ [RUNNING]
Status of VTL Logger Module.............. [RUNNING]
Status of VTL Self Monitor Module......... [RUNNING]
Status of VTL Failover Module............. [RUNNING]
```

20. **If one or more VTL processes are not RUNNING, stop the server software and then restart:**

```
[VTL_Plus]vtladmin# vtl stop all
...
[VTL_Plus]vtladmin# vtl start
```

21. Run the `sms` **command, and make sure that the** `FailOverStatus` **is** `READY` **for failback:**

```
[VTL_Plus]vtladmin# sms
Usage: sms {force|nas|nasc|fm|sm|bmr|bmrreset|setroot (sm/fm)|clearreboot(sm/fm)
} {value}
          bmr - to set the BMR health status
          bmrreset - to reset BMR value
          nas - to reset the NAS failure status
          nasc - to set nas health check
          force - enable force up fm - to set ipstorfm debug level
          sm - to set ipstorsm debug level
Last Update by SM: Sun Jan 28 15:32:39 2007
Last Access by RPC: Sun Jan 28 15:32:35 2007
FailOverStatus: 2(READY)
Status of IPStor Server (Transport) : OK
Status of IPStor Server (Application) : OK
Status of IPStor Authentication Module : OK
Status of IPStor Logger Module : OK
Status of IPStor Communication Module : OK
Status of IPStor Self-Monitor Module : OK
Status of IPStor NAS Modules: OK(0)
Status of IPStor Fsnupd Module: OK
Status of IPStor ISCSI Module: OK
Status of IPStor BMR Module: OK( 0)
Status of FC Link Down : OK
Status of Network Connection: OK
Status of force up: 0
Broadcast Arp : NO
Number of reported failed devices : 0
NAS health check : NO
XML Files Modified : NO
IPStor Failover Debug Level : 0
IPStor Self-Monitor Debug Level : 0
Do We Need To Reboot Machine(SM): NO
Do We Need To Reboot Machine(FM): NO
Nas Started: NO
```

22. Log in using the VTL management console.

23. In the object tree of the VTL console, right-click the restarted server node,
***VTLPLUSN1*, and select** `Failover > Stop Takeover` **from the context menu.**
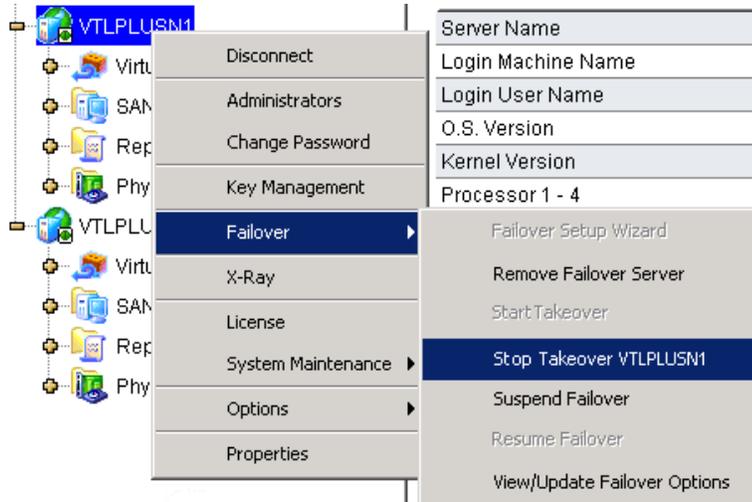
24. Open a terminal window on the management host, and again `ssh` **to the management ("server") IP address of the restarted node,** *VTLPLUSN1***:**

```
[mgt_host]user# ssh vtladmin@nn.nnn.nnn.nnx
Connecting to nnn.nnn.nnn.nnx ...
Password:
```

where *nnn.nnn.nnn.nnx* is the as-configured IP address of the restarted node, and `vtladmin` is the VTL administrator account user ID.

25. Make sure that you are logged in to the actual, restarted node:

```
[VTL_Plus]vtladmin# uname -a
SunOS VTLPLUSN1 n.nn Generic_nnnnnn-nn i86pc i386 i86pc
```

The system should display the expected node name.

26. If you are not logged in to the correct system, you may have accidently logged into the service IP address of the other node rather than the management ("server") address. Close the telnet session, and telnet to the other IP address for the restarted node.

27. Change to the directory that holds the VTL executables:

```
[VTL_Plus]vtladmin# cd /usr/local/vtl/bin
```

28. **Run the** `vtl status` **command:**

```
[VTL_Plus]vtladmin# vtl status

Sun Microsystems VTL Server vn.nn (Build nnnn)
Copyright 2001-2007 by FalconStor. All Rights Reserve

Status of VTL SNMPD Module................ [RUNNING]
Status of VTL QLogic Module............... [RUNNING]
Status of VTL Authentication Module....... [RUNNING]
Status of VTL Server (Compression) Module. [RUNNING]
Status of VTL Server (FSNBase) Module..... [RUNNING]
Status of VTL Server (Upcall) Module...... [RUNNING]
Status of VTL Server (Event) Module....... [RUNNING]
Status of VTL Server (Path Manager) Module [RUNNING]
Status of VTL Server (Application)........ [RUNNING]
Status of VTL FC Target Module............ [RUNNING]
Status of VTL Server VTL Upcall Module.... [RUNNING]
Status of VTL Server VTL Upcall Daemon.... [RUNNING]
Status of VTL Server VTL Module........... [RUNNING]
Status of VTL Communication Module........ [RUNNING]
Status of VTL Logger Module............... [RUNNING]
Status of VTL Self Monitor Module......... [RUNNING]
Status of VTL Failover Module............. [RUNNING]
```

29. **If one or more VTL processes are not** RUNNING, **stop the server software and then restart:**

```
[VTL_Plus]vtladmin# vtl stop all
...
[VTL_Plus]vtladmin# vtl start
```

30. Run the `sms` **command, Make sure that the** `FailOverStatus` **is now** `UP`**:**

```
[VTL_Plus]vtladmin# sms
Usage: sms {force|nas|nasc|fm|sm|bmr|bmrreset|setroot
(sm/fm)|clearreboot(sm/fm)
} {value}
        bmr - to set the BMR health status
        bmrreset - to reset BMR value
        nas - to reset the NAS failure status
        nasc - to set nas health check
        force - enable force up fm - to set ipstorfm debug level
        sm - to set ipstorsm debug level
Last Update by SM: Sun Jan 28 15:32:39 2007
Last Access by RPC: Sun Jan 28 15:32:35 2007


Status of IPStor Server (Transport) : OK
Status of IPStor Server (Application) : OK
Status of IPStor Authentication Module : OK
Status of IPStor Logger Module : OK
Status of IPStor Communication Module : OK
Status of IPStor Self-Monitor Module : OK
Status of IPStor NAS Modules: OK(0)
Status of IPStor Fsnupd Module: OK
Status of IPStor ISCSI Module: OK
Status of IPStor BMR Module: OK( 0)
Status of FC Link Down : OK
Status of Network Connection: OK
Status of force up: 0
Broadcast Arp : NO
Number of reported failed devices : 0
NAS health check : NO
XML Files Modified : NO
IPStor Failover Debug Level : 0
IPStor Self-Monitor Debug Level : 0
Do We Need To Reboot Machine(SM): NO
Do We Need To Reboot Machine(FM): NO
Nas Started: NO
```

31. In the object tree of the VTL console, make sure that neither node name is shown in red, indicating an error.

In normal operations, server node names are displayed in black. Red indicates that the server has failed over to its primary. Green indicates that the server has taken over for a failed primary server node. A yellow marker indicates that the administrator has suspended failover.

32. For each server, select the server node in the object tree of the VTL console, select the `Failover Information` **tab in the window at right, and make sure that the failback was successful.**

Failover events are also available via the primary server's Event Log.

Next task: "Resuming backups following a failover/failback" on page 161.

Resuming backups following a failover/failback

Failover/failback take approximately three minutes to complete. During this period, I/O is not possible, and any backup, import/export, replication jobs that are launched fail.

Thereafter, you may or may not need to restart backup operations, depending on the application used and the backup host operating system.

Configuring email alerts

You can configure VTL appliances to send automatic notifications to local system administrators via email whenever system problems arise.

▼ Configuring email alerts

1. **In the object tree of the VTL console, right-click on the VTL server node, and select** `Options > Enable CallHome`**.**

2. **When the** `Configure Email Alerts Wizard` **appears, enter the name of the outgoing mail server (A below), the email address that the VTL appliance will use when sending notifications (B), the email address(es) that will receive notifications for the desired configuration (C).**

Note that email notifications cannot use an SSL connection. If the email server requires SSL, configure email notification to use the local host SMTP server, and make sure that DNS and SMTP are set up and running on the VTL server node.

The email account password is stored in plain text, so set up an account that the SMTP server will use exclusively for email notification.

3. **Use the** `Interval` **controls provided (D above) to specify the frequency with which notifications are sent. Then press** `OK` **(E).**

4. **When the** `Set Email Alerts Signature Properties` **panel appears, enter the email signature that should appear in each notification, and press** `Next`**.**

5. **When the** `Set Email Alerts Trigger Properties` **panel appears, check the check boxes for the scripts that should trigger an email (F below). Then press** `Next` **(G).**
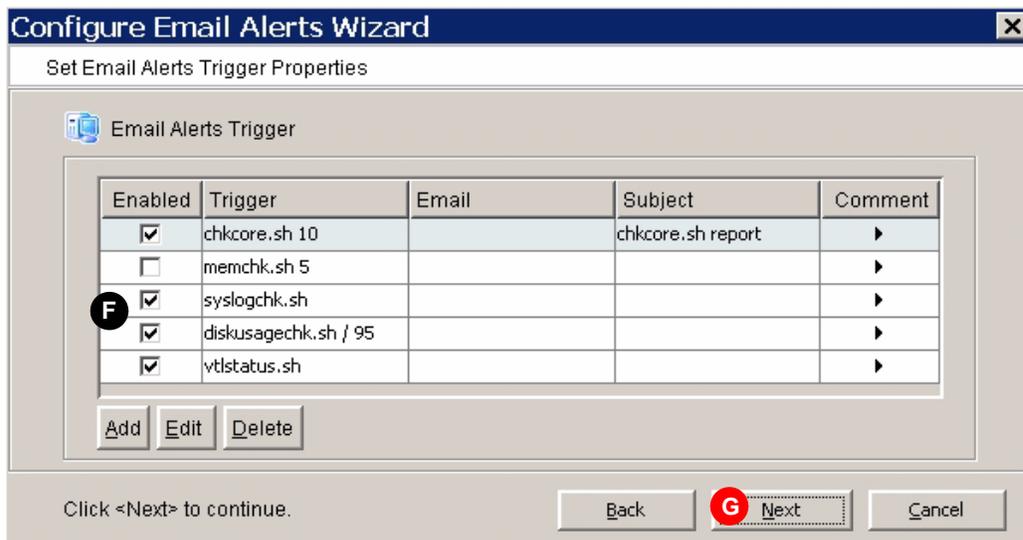
Default scripts include the following:

- `chkcore.sh 10` notifies the administrator if a new core file is found in the VTL `bin` directory. New core files are compressed and the originals are deleted, along with older compressed core files that exceed the maximum (10 is the default).

- `kfsnmem.sh 10` notifies the administrator if the maximum number of memory pages has not been set or if the number of available pages fall below a predefined percentage.

- `memchk.sh 5` notifies the administrator if the available system memory falls below a pre-defined percentage.

- `ipstorsyslogchk.sh` notifies the administrator if any instances of a pre-defined set of messages appear in the system log

- `ipstorckcfg check ipstor.conf` (VTL configuration check) notifies the administrator if the VTL software's XML configuration file, `ipstor.conf`, changes. If changes are found or if no previous version exists, the script creates a copy of the current file under the name `ipstorconf.diff.`*nnn*, where *nnn* is the script-generated version number of the file.

- `diskusagechk.sh / 95` notifies the administrator if root file system utilization exceeds a pre-defined percentage. If the current percentage is over the specified percentage (by default, 95%). Copies of the script can be modified to monitor any chosen mount point.

- `defaultipchk.sh eth0 10.1.1.1` notifies the administrator if the IP address for the specified NIC does not match a specified value. Copies of the script can be modified to monitor additional NICs.

- `ipstorstatus.sh` runs the `vtl status` command and notifies the administrator if one or more VTL software modules have stopped.

6. **When the** `Set Email Alerts System Log Check Properties dialog` **appears, add the regular expressions for any patterns that you want the notification process to parse for when examining logs. To add an expression, press** `Add` **(H below) to bring up a dialog box, then enter the pattern in the space provided. Press** `Next` **(J)** `when ready.`
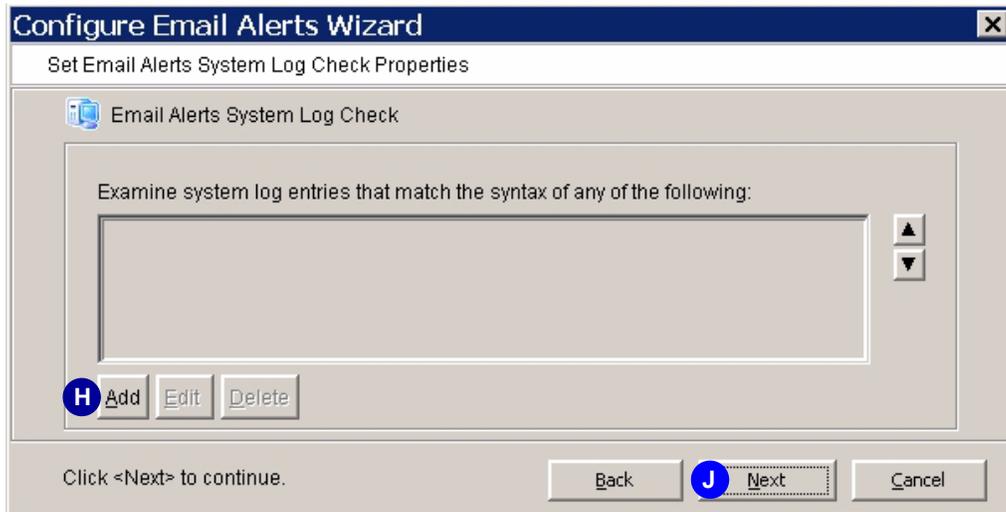
7. **When the** `Set Email Alerts Event Notification Properties` **panel appears, use the radio buttons to select the event-severity level that should trigger notification (K below), use the spinner control to set the** `Maximum event wait time` **(L), and press** `Next` **(M).**

8. **When the** `Verify the Email Alerts Properties` **panel appears, press** `Finish`**.**

Stop here.

▼ Modifying email alerts properties

Once email alerts are enabled, you can modify the information as follows:

1. **In the object tree of the VTL console, right-click on the VTL server node.**

2. **Select** `Email Alerts` **from the context menu.**

3. **When the property sheet appears, click on the appropriate tab to make your changes.**

Stop here.

▼ Customizing email fields

You can override the default `Target Email` or `Subject` by specifying an email address subject line. Proceed as follows:

1. **In the object tree of the VTL console, right-click on the VTL server, and select** `Email Alerts` **from the context menu.**

2. **When the** `Set Email Alerts Properties` **dialog appears, select the** `Trigger` **tab (A below).**
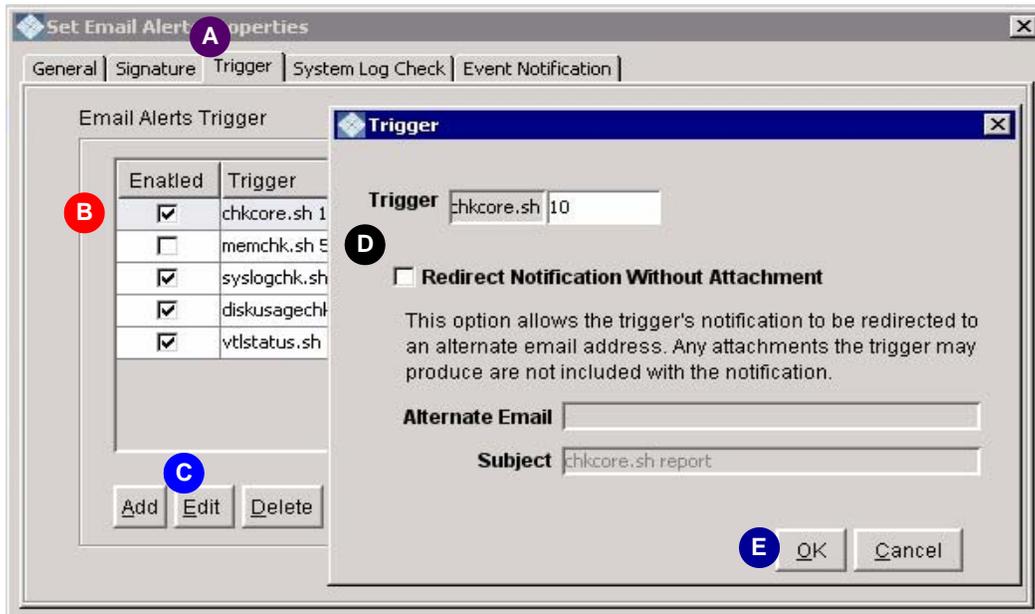
3. **If you want to modify an existing trigger, highlight the trigger (B above), and press** `Edit` **(C). In the** `Trigger` **dialog, make your changes (D), and press** `OK` **(E).**

4. **To create a new trigger, press** Add **(F below). When the** Add a Customized Trigger **dialog appears, supply a** Trigger Name**, a command line** Argument **string, and a** File Location **(path and filename) for the script (G), and redirect notifications, if desired (H). Press** OK **(J).**
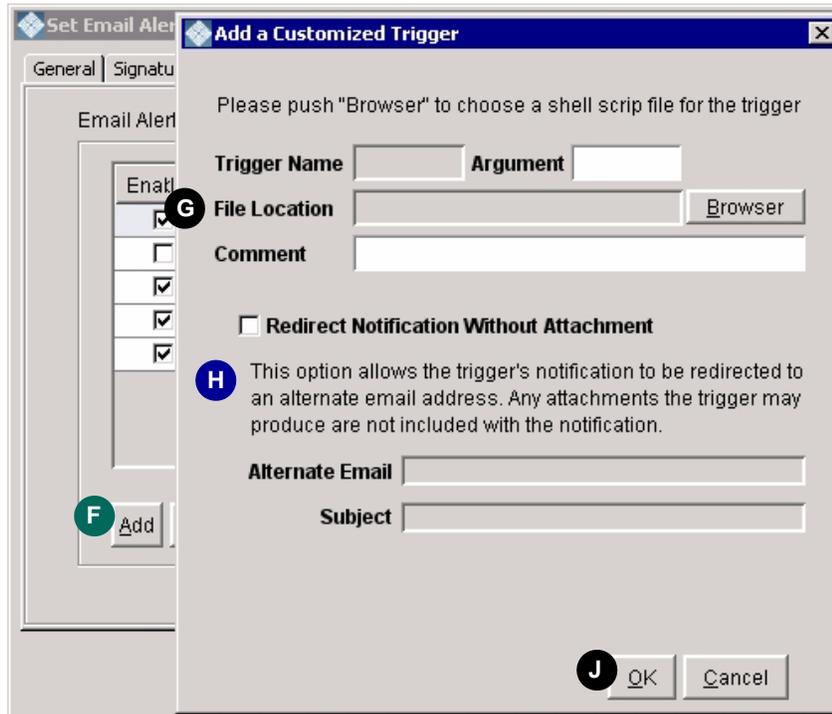
5. **Press** OK **to exit the** Set Email Alerts Properties **dialog.**

Stop here.

Updating VTL software

When software patches become available, they are posted on the online Sun StorageTek Customer Resource Center with accompanying, explanatory text ("readme") files. Download the patch files to a temporary directory on the VTL console host, and install them using the process below.

In general, you should consult your Sun support representative before downloading and applying patches. Never apply patches from sources other than Sun.

▼ Applying patches

Each patch file has a name of the form `update-vt`*xxxxxx*`solaris`*nn*, where *xxxxxx* represents the patch build number and *nn* represents the applicable version of the Solaris operating system. The corresponding text ("readme") files have the the same name, plus the suffix `.txt`.

All patches are applied using the VTL console software, as follows.

1. **Understand the behavior of each patch before proceeding: read the accompanying text file (the "readme").**

   Some VTL patches require a platform reboot, while others merely stop and restart the server software.

2. **Make sure that no critical processes are running before you proceed.**

   Processes will stop when the server software restarts.

3. Then, from the VTL console main menu, select `Tools` (**A below**).
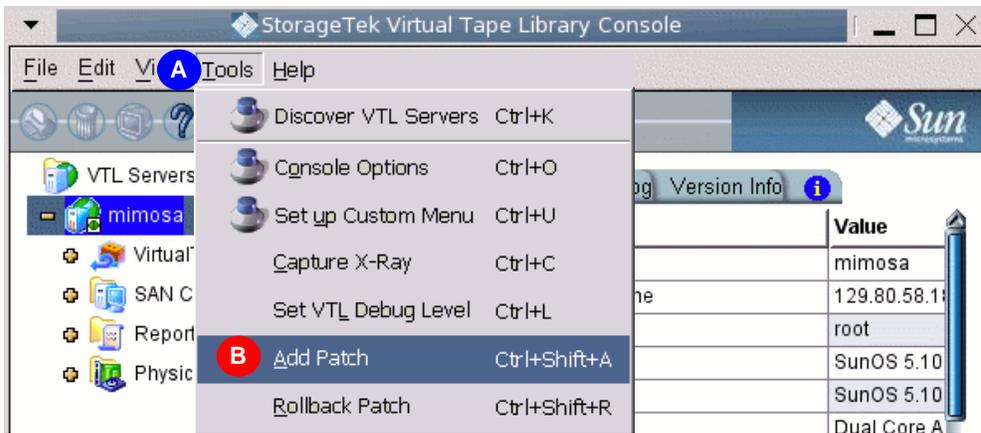
4. From the submenu, select `Add Patch` (**B above**).

5. When the warning notice appears, click `OK` (**C below**) to continue.
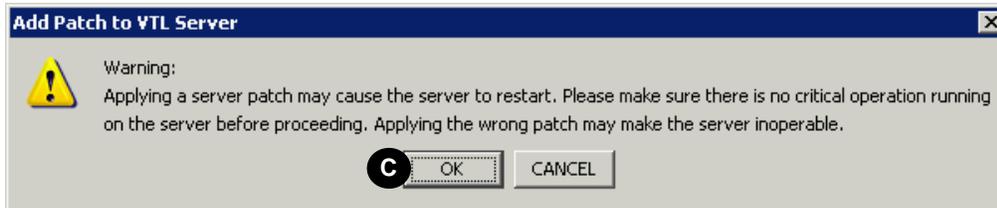
6. **Locate the subdirectory where the patch files reside (D below), select the patch file (E), and press** `Open` **(F).**
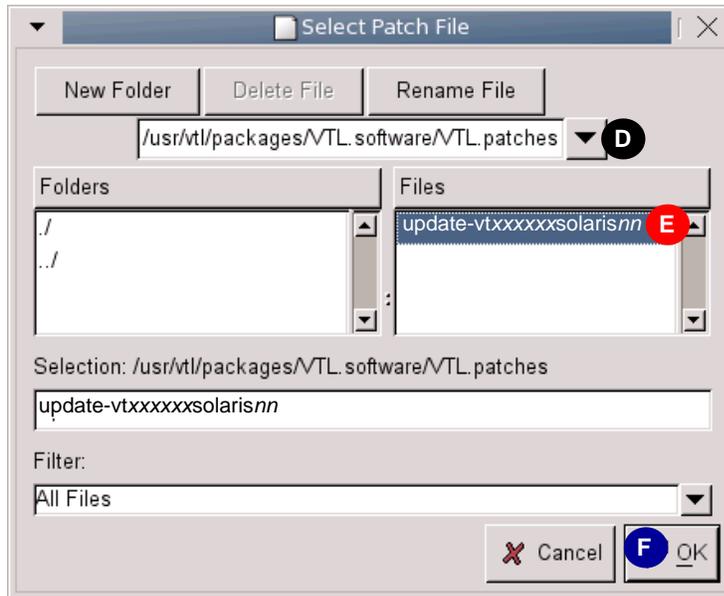
In the example, the patch files are shown in the standard location where patches are kept on the VTL appliance. If you are running the console from a remote host, the patch files will be in the temporary download directory that you selected.

7. **When the confirmation dialog appears, type** `YES` **in the text box (G below), and press** `OK` **(H).**
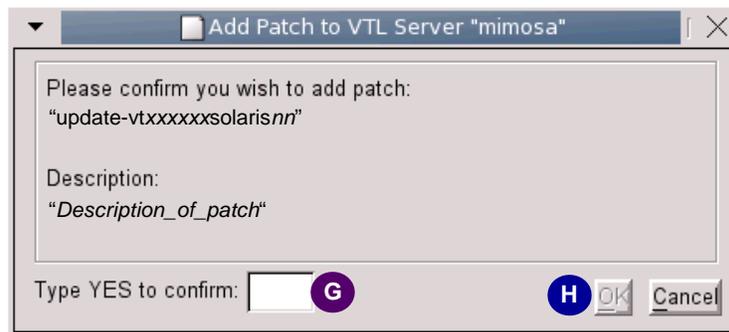
8. **If the patch requires it, reboot the server, log back in to Solaris, and restart the VTL console.**

Otherwise, the patches install and restart the VTL service, logging you out. After a minute or two, you can reconnect.

9. **Reconnect to the VTL server by double-clicking on the server node in the object tree at the left of the VTL console.**

10. **Verify that the patch was successfully applied: after you have connected, select the** `Version Info` **tab for the server (J below), and make sure that the** `Version` **and** `Build` **(K) have been updated.**
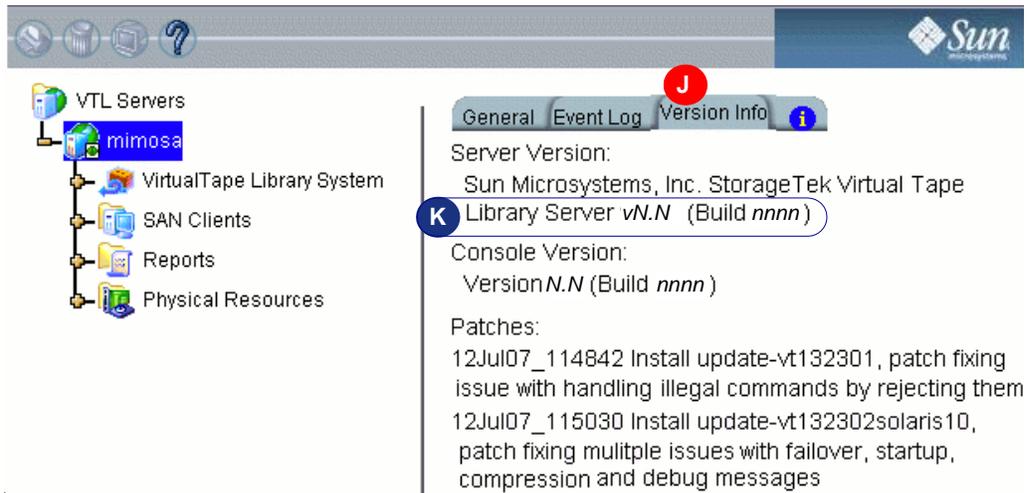
VTL command line reference

VirtualTape Library (VTL) provides a simple utility that allows you to perform some of the more common VTL functions at a command line instead of through the VTL Console. You can use this command line utility to automate many tasks, as well as integrate VTL with your existing management tools.

Using the command line utility

Type 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:\iscon importtape), a list of arguments will be displayed for that command.

Commands

On the following pages is a list of commands you can use to perform VTL 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.

Short Argument	Long Argument	Value/Description
-s	--server-name	VTL Server Name (hostname or IP address)
-u	--server-username	VTL Server Username
-p	--server-password	VTL Server User Password
-c	--client-name	VTL Client Name
-v	--vdevid	VTL 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.

Login/logout to the VTL Server

Log in to the VTL Server

```
iscon login [-s <server-name> -u <username> -p <password>|-e] [-X <rpc-
timeout>]
```

```
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 VTL 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.

See "VTL password-protected login accounts" on page 16 for information about VTL login accounts.

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: 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.

Log out from the VTL Server

```
iscon logout -s <server-name> [-X <rpc-timeout>]

iscon logout --server-name=<server-name> [--rpc-timeout=<rpc-timeout>]
```

Description:

> This command allows you to log out from the specified VTL 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 / Clients

Get virtual device list

```
iscon getvdevlist -s <server-name> [-u <username> -p <password>]
[-l [-v <vdevid> | -n <vdevname>] [-A] [-C] [-M <output-delimiter>] ]
[-X <rpc-timeout>]

iscon getvdevlist --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--longlist [--vdevid=<vdevid> | --vdevname=<vdevname>]
[--long-physical-layout] [--long-client-list]
[--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(--long-physical-layout) displays the physical layout when -l (--longlist) is specified.

-C (--long-client-list) displays 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.

Get Client virtual device list

```
iscon getclientvdevlist -s <server-name> [-u <username> -p <password>]
-c <client-name> [-t <client-type>] [-l [-M <output-delimiter>] ]
[-X <rpc-timeout>]

iscon getclientvdevlist --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--client-name=<client-name> [--client-type=<client-type>]
[--longlist [--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.

-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.

Add client

```
iscon addclient -s <server-name> [-u <username> -p <password>]
-c <client-name>
[-I <initiator-wwpns>] [-a <on|off>] [-A <on|off>]] | [-C <on|off>] [-X <rpc-
timeout>]

iscon addclient --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--client-name=<client-name> [--initiator-wwpns=<initiator-wwpns>]
[--enable-VSA=<on|off>] [--enable-iSeries=<on|off>]] | [--enable-
Celerra=<on|off>]
[--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: <>"&$/\'
>
> -I (--initiator-wwpns) is the option to set the initiator WWPNs. An initiator WWPN is a 16-byte Hex value. Separate initiator WWPNs with commas 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-iSeries) is an option to support IBM iSeries Server with the following values: *on* or *off* (default).
>
> -C (--enable-Celerra) is an option to support Celerra with the following values: *on* or *off* (default).
>
> Enabling Celerra will automatically disable VSA and iSeries, and vice versa.
>
> -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.

Delete client

```
iscon deleteclient -s <server-name> [-u <username> -p <password>]
-c <client-name> [-X <rpc-timeout>]

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.

Get client properties

```
iscon getclientprop -s <server-name> [-u <username> -p <password>]
-c <client-name> [-X <rpc-timeout>]

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.

Assign virtual device

```
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>]

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.

Unassign virtual device

```
iscon unassignvdev -s <server-name> [-u <username> -p <password>]
-v <vdevid> -c <client-name> [-y] [-f] [-X <rpc-timeout>]

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.

Create virtual device

```
iscon createvdev -s <server-name> [-u <username> -p <password>]
-I <ACSL> [-n <vdevname>] [-X <rpc-timeout>]

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 300 seconds.

Delete virtual device

```
iscon deletevdev -s <server-name> [-u <username> -p <password>]
-v <vdevid> [-d] [-f] [-X <rpc-timeout>]]

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 virtual tape library, virtual tape drive, standalone virtual tape drive, or virtual tape.

In order to delete a virtual tape drive from a virtual tape library, the virtual tape drive must have the highest element number in the library.

-v (--vdevid) is required to specify the virtual device ID.

A virtual device cannot be deleted if any of the following conditions apply:

- The specified virtual device is a virtual tape library or a virtual tape drive and there are clients currently connected to the library or drive.
- The specified virtual device is a virtual tape configured for replication, unless the -f (--force) option is used.
- The specified virtual device is the only existing virtual tape drive in the parent virtual tape library.

-d (--delete-virtual-tapes) is an option to delete all of the existing virtual tapes from a virtual tape library, a standalone virtual tape drive, or a loaded virtual tape drive selected for deletion. By default, the virtual tapes are moved to the vault, or, if a loaded virtual tape drive is selected, back to the library.

-f (--force) is an option to force the deletion of a virtual tape configured for replication. The corresponding virtual tape replica will not be deleted or promoted.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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.

Get supported virtual libraries

```
iscon getsupportedvlibs -s <server-name> [-u <username> -p <password>]
[-l [-t <vlib-type>] [-c][-M <output-delimiter>] ] [-X <rpc-timeout>]

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.

Get supported virtual drives

```
iscon getsupportedvdrives -s <server-name> [-u <username> -p <password>]
[-l [-M <output-delimiter>] ] [-X <rpc-timeout>]

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.

Create virtual tape library

```
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> [-Y <days>] [-J] | -N <auto-
repl-mode>
-S <target-name> [-M <#[D|H|M]>] ] [-B <barcode-range>] [-T <num-of-slots>]
[-E <import-export-slots>] [-D -I <initial-size> -C <increment-size>]
[-m <max-capacity>] [-L <on|off>] [-k <key-name> -W <key-password>] [-X <rpc-
timeout>]

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> [--delay-delete-days=<days>]
[--auto-eject-to-ie] | --auto-replication=<auto-repl-mode> --target-
name=<target-name>
[--delay-delete-time=<#[D|H|M]>] ] [--barcode=<barcode-range>]
[--num-of-slots=<num-of-slots>][--import-export-slots=<import-export-slots>]
```

```
[--capacity-on-demand --initial-size=<initial-size> --increment-
size=<increment-size>]
[--max-capacity=<max-capacity>] [--auto-loader=<on|off>]
[--key-name=<key-name> --key-pasword=<key-password>] [--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*.

-Y (--delay-delete-days) is an option for move mode to specify the number of days to wait before deletion. The maximum is 365 days.

-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: *replication* 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. The default value is one day.

-B (--barcode) can be specified in the following format: <barcodeB>-<barcodeE>

Barcode is an alpha-numeric value with a length of 4 to 12. <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) and -E (--import-export-slots) are optional. The <num-of-slots> can exceed the maximum number of slots supported by the specified library type, but it is limited to 65536. The <--import-export-slots> cannot exceed the maximun number of IE slots supported by the specified library type. The default is to use the maximum number of slots supported by the specified library type.

-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. The default value for both options is 5 GB. The <--increment-size> cannot be less than 5 GB.

-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.

-L (--auto-loader) is an option to set the auto-loader for those libraries that support the feature. The default value is *off*.

-k (--key-name) and -W (--key-password) are options for tape encryption support to be set in conjunction with Auto-Archive Mode. Specify the key name and key password of the encryption key if you wish to encrypt the data when exporting the virtual tape to the physical tape.

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.

Add virtual tape drive

```
iscon addvirtualdrive -s <server-name> [-u <username> -p <password>]
-L <tape-library-vid> [-r <vdrive-name-prefix>] [-R <num-of-drives>] [-X
<rpc-timeout>]

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 300 seconds.

Create standalone tape drive

```
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>]

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. The default value for both options is 5 GB. The <--increment-size> cannot be less than 5 GB.

-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.

Create virtual tape

```
iscon createvirtualtape -s <server-name> [-u <username> -p <password>] -v
<parent-vid>
[ [-g <#(GB)> [-I <ACSL>] ] [-n <vdevname>] [-B <barcode | barcode-range>] -t
<count>]
[-A -l <plib-vid> -b <physical-tape-barcode> [-J] | -N [-S <target-name>]
[-U <target-username> -P <target-password>] [-X <rpc-timeout>]

iscon createvirtualtape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--parent-vid=<parent-vid> [ [--size-gb=<#(GB)>] [--scsiaddress=<ACSL>] ]
[--vdevname=<vdevname>] [--barcode=<barcode | barcode-range>] [--
count=<count>]
[--enable-auto-archive --plib-vid=<plib-vid>
--physical-tape-barcode=<physical-tape-barcode>
[--auto-eject-to-ie] | --enable-auto-remotecopy
--target-name=<target-name> [--target-username=<target-username>
--target-password=<target-password>] [--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. This option cannot be specified if the capacity on demand option is not enabled at parent level.

-I (--scsiaddress) is an option to specify specific physical devices to be used to create a virtual device. It can be a list of ACSLs separated by a comma or a file enclosed in <> containing an ACSL on each line.
ACSL=#:#:#:# (adapter:channel:id:lun)

-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 an option to either set the virtual tape with the provided barcode or create virtual tapes in batch mode configured with barcodes form the specified barcode range. The argument must be within the barcode range configured for the library and must not contain used barcodes. When provided as a barcode range, the option creates a virtual tape for each barcode in the range.

-t (--count) is an option to create multiple virtual tapes having the barcode automatically chosen from within the barcode range configured at library level. The library must have the required number of free slots available. If combined, "count" and "barcode" options must agree in number.

If the parent library has the auto-archive/remotecopy property enabled, use the following options to provide additional information for virtual tape creation:

-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 the auto-archive option is specified. Separate multiple barcodes with commas. For example,
-b 00010001,00010009,0001000A

-J (--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.

The *count* and *barcode* options cannot be specified when the -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.

-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.

Move virtual tape

```
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>]
```

```
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. It is not required if the virtual tape is moved within the library.

-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.

Tape copy

```
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>]

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.

Set tape duplication

```
iscon setvirtuallibrarytapeduplication -s <server-name> [-u <username> -p
<password>]
```

```
-v <vdevid> -Z <on|off> -Q <num-of-copies> [-X <rpc-timeout>]

iscon setvirtuallibrarytapeduplication --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--vdevid=<vdevid> --tape-duplication=<on|off> --num-of-copies=<num-of-copies>
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command sets the Tape Duplication property for a virtual tape library.

-v (--vdevid) is required in order to identify the virtual library.

-Z (--tape-duplication) is required in order to enable or disable the Tape Duplication property: *on* (enable) or *off* (disable).

-Q (--num-of-copies) is an option to specify the number of copies to be made using the same barcode if tape duplication option is enabled. The maximum value is 5. The default value is 1.

The virtual library must have the Auto Archive or Tape Caching property enabled in order to enable tape duplication.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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.

Set tape properties

```
iscon settapeproperty -s <server-name> [-u <username> -p <password>]
-v <vdevid> [-B <barcode>] [-f] [-F] [-w <on|off>] [-A <auto-archive-mode> [-
Y <days>]
[-J <on|off>] | -N <auto-repl-mode> -S <target-name>
[-U <target-username> -P <target-password>]
[-M <#[D|H|M]>] ] [-k <key-name> -W <key-password> | -d]
[-Z <on|off> -Q <num-of-copies>] [-X <rpc-timeout>]

iscon settapeproperty --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --vdevid=<vdevid>
[--barcode=<barcode>] [--force] [--full-capacity] [--tape-write-
protect=<on|off>]
[--auto-archive-mode=<auto-archive-mode> [--delay-delete-days=<days>]
[--auto-eject-to-ie] | --auto-replication=<auto-repl-mode> --target-
name=<target-name>
[--server-username=<username> --server-password=<password>]
[--delay-delete-time=<#[D|H|M]>] ] [--key-name=<key-name> --key-pasword=<key-
password> |
--disable-key] [--tape-duplication=<on|off> --num-of-copies=<num-of-copies>]
[--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. Barcode is an alpha-numerical value with a length of 4 to 12.

-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.

-Y (--delay-delete-days) is an option for *move* mode to specify the number of days to wait before the deletion. The maximum is 365 days.

-J (--auto-eject-to-ie) is an option for auto-archive mode in order to enable or disable the ejection of the physical tape to the IE slot after a successful archive job: *on* (enable) or *off* (disable).

-N (--auto-replication) is an option with one of the follwing values: *localcopy*, *localmove*, *replication*, *remotemove*, or *none*.

-S (--target-name) is the remote server name for auto-replication. It is required for auto-replication.

-U (--target-username) and -P (--target-password) are options to specify a different user ID and password to log in to the remote server.

-M (--delay-delete-time) is an option for auto-replication move mode to specify up to 30 days of retention period before deletion. The default value is 1 day. The value can be specified in days(D), hours(H) or minutes(M). For example: 2D, 10H, 150M.

-A (--auto-archive-mode) and -N (--auto-replication) cannot be specified if replication is enabled for the tape.

-k (--key-name), -W (--key-password) and -d (--disable-key) are options for tape encryption support to be set in conjunction with Auto-Archive Mode. Specify the key name and key password of the encryption key if you wish to encrypt the data when exporting the virtual tape to the physical tape. Specify -d (--disable-key) if you wish to disable tape encryption for this tape.

-Z (--tape-duplication) is an option to set the Tape Duplication property with one of the following values: *on* (enable), *off* (disable), or *inherit*.

-Q (--num-of-copies) is an option to specify the number of copies to be made using the same barcode if the tape duplication option is enabled. The maximum value is 5. The default value is 1.

Tape Duplication can be enabled only if the virtual library hosting the virtual tape has the Tape Caching property enabled or the virtual tape has the Auto Archive property enabled.

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.

Automated tape caching

Set tape caching

```
iscon settapecaching -s <server-name> [-u <username> -p <password>]
-L <library-vid> -t <tape-caching-enable> [-S <start-time>][-W <day-of-the-
week>]
[-b <and-or>] [[-e][-f]][-c <disk-capacity>][-d <days-old>]
[-R <retention-days> | -I | -M | -N] [-X <rpc-timeout>]

iscon settapecaching --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--tape-library-vid=<library-vid> [--start-time=<start-time>]
[--day-of-the-week=<day-of-the-week>] --tape-caching-enable=<tape-caching-
enable>
[--trigger-combine=<and-or>] [[--end-of-backup] [--tape-full]]
[--disk-capacity=<disk-capacity>] [--days-old=<days-old>]
[--retention-days=<retention-days> | --immediately | --no-more-space | --
never]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command can be used in order to enable, disable, or change the Automated Tape Caching policy for a virtual tape library.

-L (--tape-library-vid) is the virtual device ID of the virtual tape library to be set.

Set -t (--tape-caching-enable) to 1 for enable or 0 to disable.

If the *disable* option is used all other arguments will be ignored.

The *enable* option must be used in order to set or change the tape caching policy.

Time based data migration triggers:

-S (--start-time) alone can be used to start daily migrations at the time specified. The default value is 00:00(am)(hh:mm). When combined with other data migration triggers, the *-S* option will delay the migration execution to the specified time.

-W (--day-of-the-week) can be used to start weekly migrations on the specified day at 00:00(am): Sunday: 0, Monday: 1, ..., Saturday: 6. The default value is -1. This option is ignored if Policy Based triggers are used.

Policy based data migration triggers:

-b (--trigger-combine) tells how trigger policies are combined (specified by -e, -c, -d). 1 -- and; 0 -- or. The default value is 1 (and).

-e (--end-of-backup) triggers data migration when unloading a tape from a drive after some data is written to it.

-f (--tape-full) applies to -e options. Data is migrated only if the tape becomes full.

-c (--disk-capacity) triggers data migration when disk usage percentage is above the global disk space threshold.

-d (--days-old) triggers date migration after data was retained on disk for (days-old) days (up to 3650 days).

Reclamation triggers:

-R (retention-days) determines the number of days virtual tapes will be kept in the system before they are deleted.

Select -I (--immediately) and virtual tapes will be deleted immediately after data migration completes.

Select -M (--no-more-space) and virtual tapes will be deleted when disk space is needed to create (or expand) a virtual tape. The last used will be deleted.

Select -N (--never) and virtual tapes will never be deleted.

The reclamation triggers are exclusive.

-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.

Sync physical tapes

```
iscon syncphysicaltape -s <server-name> [-u <username> -p <password>]
-l <plib-vid> -b <physical-tape-barcode> -L <virtual-tape-library-id>
-t <virtual-tape-slot-no> [-M <sync-mode>] [-k <key-name> -W <key-password>]
[-I <ACSL list>] [-n <vdevname>] [-g <#(GB)>] [-X <rpc-timeout>]

iscon syncphysicaltape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--plib-vid=<physical-tape-library-vid> --physical-tape-barcode=<physical-
tape-barcode>
--tape-library-vid=<virtual-tape-library-id>
--virtual-tape-slot-no=<virtual-tape-slot-no> [--sync-mode=<sync-mode>]
[--key-name=<key-name> --key-password=<key-password>] [--scsiaddress=<ACSL
list>]
[--vdevname=<vdevname>] [--size-gb=<#(GB)>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a synchronized virtual tape for the specified physical tape. The physical tape must be from the specified physical tape library and the virtual tape will be created in the specified virtual tape library. The virtual tape library must have the tape caching feature enabled.

-l <--plib-vid> is the virtual ID of the physical tape library where the physical tapes are located.

-b <--physical-tape-barcode> is the barcode of the physical tape. The virtual tape will be created with the same barcode. The barcode must not be in use by any other virtual tape in the system. If the barcode contains leading or trailing space characters, it must be enclosed in double quotes.

-L <--tape-library-vid> is the ID of the virtual tape library where the virtual tapes will be created.

-t <--virtual-tape-slot-no> is an option to provide an empty destination slot for the virtual tape. Not for "-M cache" mode.

[-M <--sync-mode>] is an option to select the synchronization mode from one of the following values (default is "cache"):

■ cache (create cache)

■ metadata (create cache and copy meta data)

■ directlink (create direct link)

-k (--key-name) and -W (--key-password) are options for tape encryption support. If the tape to be synchronized was encrypted through the system, you need to specify the key name and the key password of the encryption key to decrypt the data on the imported tape.

[-I <--scsiaddress>] is the option to specify which physical devices to be used to create the virtual device. It can be a list of ACSLs separated with commas. ACSL=#:#:#:# (adapter:channel:id:lun)

-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. Please enclose the name in double quotes to ensure the proper name. The following characters are invalid for the name: <>"&$/\'

-g (--size-gb) is an option to specify the initial size, in GB, of the virtual tapes, if the capacity-on-demand property for the virtual tape library is enabled. The default is 1 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.

Migrate virtual tapes

```
iscon migratevirtualtapes -s <server-name> [-u <username> -p <password>]
-T <tape-vid-list> [-f] [-X <rpc-timeout>]

iscon migratevirtualtapes --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--tape-vid-list=<tape-vid-list> [--tape-full] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command migrates the specified virtual tapes to the physical libraries they are synchronized with.

-T (--tape-vid-list) is a list of virtual tape ID(s) separated with commas.

-F (--tape-full) is an option to force full tape migration. By default, the migration operation is incremental.

-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.

Reclaim disk space

```
iscon reclaimtapes -s <server-name> [-u <username> -p <password>]
-T <tape-vid-list> [-X <rpc-timeout>]

iscon reclaimtapes --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--tape-vid-list=<tape-vid-list> [--rpc-timeout=<rpc-timeout>]
```

Description:

>   This command reclaims the disk space occupied by the specified migrated virtual
>   tapes.
>
>   -T (--tape-vid-list) is required to specify the ID of the virtual tapes to be reclaimed,
>   separated with commas.
>
>   -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 300 seconds.

Renew cache

```
iscon renewcache -s <server-name> [-u <username> -p <password>]
-v <vdevid> [-M <metadata>] [-k <key-name> -W <key-password>] [-I <ACSL>] [-n
<vdevname>] [-g <#(GB)>] [-X <rpc-timeout>]

iscon renewcache --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--import-
mode=<metadata>] [--key-name=<key-name> --key-password=<key-password>] [--
scsiaddress=<ACSL>]
[--vdevname=<vdevname>] [--size-gb=<#(GB)>] [--rpc-timeout=<rpc-timeout>]
```

Description:

>   This command converts a virtual stub tape into a virtual cache tape.
>
>   -v (--vdevid) is required to specify the ID of the virtual stub tape.
>
>   -M (--import-mode) is an option to specify that the header area should be copied
>   from the physical tape to the new virtual tape cache. The value of this option must
>   be: *metadata*.
>
>   -k (--key-name) and -W (--key-password) are options for tape encryption support. If
>   the tape to be renewed was encrypted through the system, you need to specify the
>   key name and the key password of the encryption key to decrypt the data.
>
>   The following properties of the virtual cache tape can be set if the "-M" option is not
>   specified:

-I (--scsiaddress) is the option to specify which physical devices should be used to create the virtual device. It can be a list of ACSLs separated with commas or a file enclosed in <> containing an ACSL on each line.
ACSL=#:#:#:# (adapter:channel:id:lun)

-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 it is properly parsed and interpreted. The following characters are invalid for the name: <>"&$/\'

-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. This option cannot be specified if the capacity-on-demand option is not enabled at library level.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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.

System configuration

Add a license keycode

```
iscon addlicense -s <server-name> [-u <username> -p <password>] -k <license-
keycode>
[-X <rpc-timeout>]

iscon addlicense --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --
license=<license-keycode>
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command adds a license keycode.

-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.

Remove a license keycode

```
iscon removelicense -s <server-name> [-u <username> -p <password>] -k
<license-keycode>
[-X <rpc-timeout>]

iscon removelicense --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --
license=<license-keycode>
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command removes a license keycode.

-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.

Get VTL info

```
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>]

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 VTL information.

-T (--vtl-info-type) is the VTL 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 with commas: *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.

Import/Export

Import tape

```
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>] [-k <key-name> -W <key-password>] [-X <rpc-timeout>]

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>]
[--key-name=<key-name> --key-pasword=<key-password>] [--rpc-timeout=<rpc-
timeout>]
```

Description:

This command imports the data from a tape into the VTL.

-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. If the barcode contains leading or trailing space characters, it must be enclosed in double quotes. No physical tape information is required if the physical tape is imported from a standalone 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.

-k (--key-name) and -W (--key-password) are options for tape encryption support. If the tape to be imported was encrypted through the system, you need to specify the key name and the key password of the encryption key to decrypt the data on the imported 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 300 seconds.

Export virtual tape

```
iscon exportvirtualtape -s <server-name> [-u <username> -p <password>] -v
<vdevid>
-L <tape-library-vid> -b | -B <barcode> | -l <slot-no>
[-M <export-mode> [-Y <days>] ] [-j <job-description>] [-f] [-J]
[-k <key-name> -W <key-password>] [-Z <on> -Q <num-of-copies>] [-X <rpc-
timeout>]

iscon exportvirtualtape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--vdevid=<vdevid> --tape-library-vid=<tape-library-vid>
--same-barcode | --barcode=<barcode> | --slot-no=<slot-no>
[--export-mode=<export-mode>] [--delay-delete-days=<days>] ]
[--job-description=<job-description>] [--force] [--auto-eject-to-ie]
[--key-name=<key-name> --key-pasword=<key-password>]
[--tape-duplication=<on> --num-of-copies=<num-of-copies>] [--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.

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.

-M (--export-mode) is an option with one of the following values: *copy* (default) or *move*.

-Y (--delay-delete-days) is an option for *move mode* to specify the number of days to wait before deletion. The maximum is 365 days. The default value is 365 days.

-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.

-J (--auto-eject-to-ie) is an option to eject the tape to the IE slot after the export job.

-k (--key-name) and -W (--key-password) are options for tape encryption support. Specify the key name and key password of the encryption key if you wish to encrypt the data when exporting the virtual tape to the physical tape.

-Z (--tape-duplication) is an option to enable tape duplication with the following value: *on*.

-Q (--num-of-copies) is an option to specify the number of copies to be made using the same barcode if the tape duplication option is enabled. The maximum value is 5. The default value is 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.

Get import/export job status

```
iscon getimportexportjobstatus -s <server-name> [-u <username> -p <password>]
```

```
[-j <job-id-list>] [-T <job-type> -S <job_status>] [-X <rpc-timeout>]

iscon getimportexportjobstatus --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--job-id-list=<job-id-list>] | [--job-type=<job_type> --
job_status=<job_status>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command displays the status of the import/export jobs present in the queue. If no filters are specified, the command displays all the jobs that are in the queue.

-j <--job-id-list> is an optional list of job IDs separated with commas. The command displays the status of specified jobs only. All other filters are ignored.

-T <--job-type> is an optional job type based filter. The command displays those jobs matching the provided type. The accepted job type values are: IMPORT, EXPORT, or OTHER.

-S <--job_status> is an optional job status based filter. The command displays those jobs matching the provided status. The accepted job status values are: FAILED, HOLD, READY, or OTHER.

-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.

Resume import/export jobs

```
iscon resumeimportexportjobs -s <server-name> [-u <username> -p <password>]
-j <job-id-list> [-X <rpc-timeout>]

iscon resumeimportexportjobs --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --job-id-
list=<job-id-list>
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command resumes specified import/export jobs. The jobs must be held in the import/export queue in a suspended state.

-j <--job-id-list> is a list of job IDs separated with commas.

-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.

Delete import/export jobs

```
iscon deleteimportexportjobs -s <server-name> [-u <username> -p <password>]
-j <job-id-list> [-X <rpc-timeout>]

iscon deleteimportexportjobs --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --job-id-
list=<job-id-list>
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command deletes specified import/export jobs. The jobs must be held in the import/export queue.

-j <--job-id-list> is a list of job IDs separated with commas.

-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.

Suspend import/export jobs

```
iscon suspendimportexportjobs -s <server-name> [-u <username> -p <password>]
-j <job-id-list> [-X <rpc-timeout>]

iscon suspendimportexportjobs --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --job-id-
list=<job-id-list>
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command suspends specified import/export jobs. The jobs must be held in the import/export queue and must be idle.

-j <--job-id-list> is a list of job IDs separated with commas.

-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.

Cancel import/export jobs

```
iscon cancelimportexportjobs -s <server-name> [-u <username> -p <password>]
-j <job-id-list> [-X <rpc-timeout>]

iscon cancelimportexportjobs --server-name=<server-name>
```

```
[--server-username=<username> --server-password=<password>] --job-id-
list=<job-id-list>
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command cancels specified import/export jobs. The jobs must be held in the import/export queue and must be running.

-j <--job-id-list> is a list of job IDs separated with commas.

-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.

Replication

Create a replica

```
iscon createreplication -s <server-name> [-u <username> -p <password>]
-v <source-vdevid> -S <target-name> [-U <target-username> -P <target-
password>]
[-w <watermark(MB)> | [-d <YYYYMMDDHHMM> -i <#[H|M]>]] [-r <on>]
[[-t <timeout>] [-I <retry-in>]] [-C <retry-for>]] [-c <on|off>] [-e
<on|off>]
[-n <replica-vdev-name>] [-X <rpc-timeout>]

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(MB)> | [--date=<YYYYMMDDHHMM> --interval=<#[H|M]>]] |
[--repl-first <on>] [[--replication-timeout=<timeout>]
[--replication-retry-interval=<retry-in>] [--replication-retry-count=<retry-
for]]
[--compression=<on|off>] [--encryption=<on|off>] [--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.

The replication configuration requires a trigger policy to be set. If no trigger policy is specified, the command will automatically apply the appropriate default policy based on the tape caching property of the specified virtual tape.

Any combination of the following two options can be used to set up a replication trigger policy for a virtual tape with the tape caching property disabled. The default policy is 1024 MB watermark.

-w (--watermark) is a data size based trigger in MB. The watermark is checked when the tape is unloaded from the tape drive and the replication is triggered if the amount of new data on the tape has reached the specified watermark.

-d (--date) combined with -i (--interval) is a time based trigger. The replication is triggered at the time specified by date and then repeated every interval. -d (--date) format is YYYYMMDDHHMM and -i (--interval) format is a number followed by H for hours or M for minutes (e.g. -i 2H or --interval=120M). The default value for interval is 1H (one hour).

-r (--repl-first) is an option to replicate the virtual tape before it is migrated. Use "on" in order to enable this policy or "off" to have tape migration executed first. The default policy is to replicate the virtual tape after it is migrated.

- Replication is retried based on the timeout policy:
- -t (--replication-timeout) in seconds (default 60).
- -I (--replication-retry-interval) in seconds (default 60).
- -C (--replication-retry-count) retry count (default 1).

-c (--compression) is an option to enable or disable compression with one of the values: *on* or *off*.

-e (--encryption) is an option for remote replication only to set 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.

Promote a replica

```
iscon promotereplica -s <server-name> -v <vdevid> | -S <target-name> -V
<replicaid>
[-u <username> -p <password>] [-U <target-username> -P <target-password>] [-
f]
[-X <rpc-timeout>]

iscon promotereplica --server-name=<server-name> --vdevid=<vdevid> |
--target-name=<target-name> --replicaid=<replicaid> [--server-
username=<username>
--server-password=<password>] [--target-username=<target-username>
--target-password=<target-password>] [--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.

Specify either the primary server and the source virtual tape ID or the target server
and the tape replica ID. The user name and password must be provided for both
servers, if the servers were not registered using the login command.

-v (--vdevid) is the ID of the source virtual tape and -V (--replicaid) is the ID of the
tape replica.

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.

-f (--force) is an option to enforce the promotion if the source virtual tape is no
longer available or the tape replica 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.

Remove replication

```
iscon removereplication -s <server-name> -v <vdevid> | -S <target-name> -V
<replicaid>
[-u <username> -p <password>] [-U <target-username> -P <target-password>] [-
f]
[-X <rpc-timeout>]

iscon removereplication --server-name=<server-name> --vdevid=<vdevid> |
--target-name=<target-name> --replicaid=<replicaid> [--server-
username=<username>
```

```
--server-password=<password>] [--target-username=<target-username>
--target-password=<target-password>] [--force] [--rpc-timeout=<rpc-timeout>]
```

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.

Specify either the primary server and the source virtual tape ID or the target server and the tape replica ID. The user name and password must be provided for both servers, if the servers were not registered using the login command.

-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.

Suspend replication

```
iscon suspendreplication -s <server-name> [-u <username> -p <password>]
-v <vdevid> [-X <rpc-timeout>]

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.

Resume replication

```
iscon resumereplication -s <server-name> [-u <username> -p <password>]
-v <vdevid> [-X <rpc-timeout>]

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.

Set replication properties

```
iscon setreplicationproperties -s <server-name> [-u <username> -p <password>]
-v <source-vdevid> [-w <watermark(MB)> | [-d <YYYYMMDDHHMM> -i <#[H|M]>]] |
[-r <on|off>] [[-t <timeout>] [-I <retry-in]>] [-C <retry-for>]] [-c
<on|off>]
[-e <on|off>] [-X <rpc-timeout>]

iscon setreplicationproperties --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--source-vdevid=<source-vdevid>
[--watermark=<watermark(MB)> | [--date=<YYYYMMDDHHMM> --interval=<#[H|M]>]] |
[--repl-first <on|off>] [[--replication-timeout=<timeout>] [--replication-
retry-interval=<retry-in>] [--replication-retry-count=<retry-for]][--
compression=<on|off>]
[--encryption=<on|off>] [--rpc-timeout=<rpc-timeout>]
```

Description:

> This command allows you to change the replication policy for the specified virtual
> tape.
>
> -v (--source-vdevid) is required to specify the ID of the source virtual tape.
>
> Any combination of the following two options can be used to set up a replication
> trigger policy for a virtual with the tape caching property disabled.

-w (--watermark) is a data size based trigger in MB. The watermark is checked when the tape is unloaded from the tape drive and the replication is triggered if the amount of new data on the tape has reached the specified watermark.

-d (--date) combined with -i (--interval) is a time based trigger. The replication is triggered at the time specified by date and then repeated every interval. -d (--date) format is YYYYMMDDHHMM and -i (--interval) format is a number followed by H for hours or M for minutes (e.g. -i 2H or --interval=120M).

To delete a watermark trigger specify 0 for the watermark. To delete a time based trigger specify NA for date. At least one trigger must remain active.

The date argument is not required if you are only changing the interval.

For virtual tapes having the tape caching property enabled, replication is triggered based on the tape caching policy:

-r (--repl-first) is required to replicate the virtual tape before it is migrated. Use "on" in order to enable this policy or "off" to have tape migration executed first.

The replication retry policy can be changed using the following options:

- -t (--replication-timeout) in seconds (default 60).
- -I (--replication-retry-interval) in seconds (default 60).
- -C (--replication-retry-count) retry count (default 1).

-c (--compression) is an option to enable or disable compression with one of the values: *on* or *off*.

-e (--encryption) is an option for remote replication only to set the 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.

Get replication properties

```
iscon getreplicationproperties -s <server-name> [-u <username> -p <password>]
-v <source-vdevid> [-X <rpc-timeout>]

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.

Get replication status

```
iscon getreplicationstatus -S <target-name> [-U <username> -P <password>]
-V <replicaid> [-X <rpc-timeout>]

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.

Start replication

```
iscon startreplication -s <server-name> [-u <username> -p <password>]
-v <vdevid> [-X <rpc-timeout>]

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.

Stop replication

```
iscon stopreplication -s <server-name> [-u <username> -p <password>]
-v <vdevid> [-X <rpc-timeout>]

iscon stopreplication --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
-vdevid=<vdevid> [--rpc-timeout=<rpc-timeout>]
```

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.

Physical devices

Inventory physical tape library

```
iscon plibinventory -s <server-name> [-u <username> -p <password>]
[-l <physical-tape-library-vid>] [-X <rpc-timeout>]

iscon plibinventory --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--plib-vid=<tape-library-vid>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command performs an inventory of the physical tapes in a physical tape library.

-l (--plib-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 (--plib-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.

Get physical tape list

```
iscon getphysicaltapelist -s <server-name> [-u <username> -p <password>]
-l <physical-tape-library-vid> [-X <rpc-timeout>]

iscon getphysicaltapelist --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--plib-vid=<physical-tape-library-vid> [--rpc-timeout=<rpc-timeout>]
```

Description:

> This command displays a list of physical tapes located in the specified physical tape library.
>
> -l (--plib-vid) is the ID of the physical tape library.
>
> -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 300 seconds.

Move physical tape

```
iscon movephysicaltape -s <server-name> [-u <username> -p <password>]
-m <move-operation> -L <physical-tape-library-vid>
-B <physical-tape-barcode> | -l <from-location-id> -t <to-location-id>
[-X <rpc-timeout>]

iscon movephysicaltape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--move-operation=<move-operation> --tape-library-vid=<physical-tape-library-
vid>
--physical-tape-barcode=<barcode> | --from-location-id=<from-location-id>
--to-location-id=<to-location-id> [--rpc-timeout=<rpc-timeout>]
```

Description:

> This command moves a physical tape to a new location.
>
> -m(--move-operation) is one of the following operations:
>
> - DriveToSlot
> - SlotToSlot
> - SlotToDrive
> - IESlotToSlot
> - SlotToIESlot
>
> -L(--tape-library-vid) is the physical library virtual ID where the tape is located.

Assign physical resource to VTL

```
iscon assignresourcetovtl -s <server-name> [-u <username> -p <password>]
-I <ACSL> [-L <tape-library-vid>] [-X <rpc-timeout>]

iscon assignresourcetovtl --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--scsiaddress=<ACSL> [--tape-library-vid=<tape-library-vid>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command assigns a physical tape library or drive to VTL.

-I (--scsiaddress) is required in order to identify the physical tape library or the physical tape drive to be assigned to VTL.

-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 VTL.

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.

Unassign physical resource from VTL

```
iscon unassignresourcefromvtl -s <server-name> [-u <username> -p <password>]
-v <vdevid> [-q] [-X <rpc-timeout>]

iscon unassignresourcefromvtl --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --vdevid=<vdevid>
[--preserve-directlink] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command unassigns a physical tape library or drive from VTL.

-v (--vdevid) is required to specify the ID of the physical tape library or the physical tape drive to be unassigned from VTL.

-q (--preserve-directlink) in an option to preserve the direct linked tapes for physical tape libraries.

-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.

Get physical device information

```
iscon getpdevinfo -s <server-name> [-u <username> -p <password>]
[-F [-M | -C <category>] | [-a] [-A] [-I <ACSL>] ] [-o <output-format>]
[-X <rpc-timeout>]

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.

Rescan physical devices

```
iscon rescandevices -s <server-name> [-u <username> -p <password>]
[-a <adapter-range>] [-i <scsi-range>] [-l <lun-range>] [-L] [-X <rpc-
timeout>]

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 adapters, if it is not specified. For example: -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: -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: -l 0-10

-L (--sequential) is an option 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 300 seconds.

Import disk

```
iscon importdisk -s <server-name> [-u <username> -p <password>]
-i <guid> | -I <ACSL> [-X <rpc-timeout>]

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 VTL logical resources previously set up on a different VTL server. If the previous server is no longer available, the disk can be set up on a new VTL 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 300 seconds.

Prepare physical device for VTL server

```
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>]

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 an VTL 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 300 seconds.

Reports

Server throughput report

```
iscon createserverthroughputreport -s <server-name> [-u <username> -p
<password>]
[-z <report period>] | [-D <date-range>] [-o <filename>] [-f] [-X <rpc-
timeout>]

iscon createserverthroughputreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--report-period=<report-period>] | [--date-range=<date-range>]
[--output-file=<filename>] [--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a report that displays throughput data and configuration information for a specific server.

-z (--report-period) is the period of time that the report should cover. The accepted values are:

- t - today
- y - yesterday
- 7 - last seven days
- 30 - last thirty days

-D (--date-range) is the starting date and ending date in the following format (maximum 30 days):
YYYYMMDD-YYYYMMDD or YYYYMMDD

Either -z (--report-period) or -D (--date-range) can be specified, but not both. The date option is applied to the server local time. The default value is: "-z t" (today).

-o (--output-file) is the file name used to save the report data. If an output filename is not specified, the default filename is: ServerThroughput-server-MM-DD-YYYY-hh-mm-ss[.#]

[.#] is the additional suffix when there is a duplicate.

Specify the -f (--force) option if you want to overwrite the existing file if 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 default RPC timeout is 300 seconds.

SCSI channel throughput report

```
iscon createscsichannelthroughputreport -s <server-name> [-u <username> -p
<password>]
[-z <report period>] | [-D <date-range>] -t <adapter-no> [-o <filename>] [-f]
[-X <rpc-timeout>]

iscon createscsichannelthroughputreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--report-period=<report-period>] | [--date-range=<date-range>]
--adapter-no=<adapter-no> [--output-file=<filename>] [--force] [--rpc-
timeout=<rpc-timeout>]
```

Description:

This command creates a report that displays the throughput values for a specific SCSI/Fibre channel.

-t (--adapter-no) is required in order to identify the requested SCSI/Fibre Channel adapter.

-z (--report-period) is the period of time that the report should cover. The accepted values are:

- t - today
- y - yesterday
- 7 - last seven days
- 30 - last thirty days

-D (--date-range) is the starting date and ending date in the following format (maximum 30 days):
YYYYMMDD-YYYYMMDD or YYYYMMDD

Either -z (--report-period) or -D (--date-range) can be specified, but not both. The date option is applied to the server local time. The default value is: "-z t" (today).

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: SCSIChannelThroughput-server-MM-DD-YYYY-hh-mm-ss[.#]

[.#] is the additional suffix when there is a duplicate.

Specify the -f (--force) option if you want to overwrite the existing file if 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 default RPC timeout is 300 seconds.

Device throughput report

```
iscon createdevicethroughputreport -s <server-name> [-u <username> -p
<password>]
-I <ACSL> [-z <report period>] | [-D <date-range>] [-o <filename>] [-f]
[-X <rpc-timeout>]

iscon createdevicethroughputreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --
scsiaddress=<ACSL>
[--report-period=<report-period>] | [--date-range=<date-range>]
[--output-file=<filename>] [--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a report that displays throughput values for a specific device.

-I <ACSL> (--scsiaddress) is the LUN address of the device.

-z (--report-period) is the period of time that the report should cover. The accepted values are:

■ t - today

■ y - yesterday

■ 7 - last seven days

■ 30 - last thirty days

-D (--date-range) is the starting date and ending date in the following format (maximum 30 days):
YYYYMMDD-YYYYMMDD or YYYYMMDD

Either -z (--report-period) or -D (--date-range) can be specified, but not both. The date option is applied to the server local time. The default value is: "-z t" (today).

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: SCSIDeviceThroughput-server-MM-DD-YYYY-hh-mm-ss[.#]

[.#] is the additional suffix when there is a duplicate.

Specify the -f (--force) option if you want to overwrite the existing file if 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 default RPC timeout is 300 seconds.

Physical resources configuration report

```
iscon createphyresourcesconfreport -s <server-name> [-u <username> -p
<password>]
[-o <filename>] [-f] [-X <rpc-timeout>]

iscon createphyresourcesconfreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--output-
file=<filename>]
[--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

> This command creates a report that displays the physical resources configuration for
> a specific server. This report lists all of the physical resources on this server,
> including each physical adapter and physical device.
>
> -o (--output-file) is the file name used to save the report data. If the output filename
> is not specified, the default filename is: PhysicalResourcesConfiguration-server-MM-
> DD-YYYY-hh-mm-ss[.#]
>
> [.#] is the additional suffix when there is a duplicate.
>
> Specify the -f (--force) option if you want to overwrite the existing file if 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 default RPC timeout is 300 seconds.

Disk usage report

```
iscon creatediskusagereport -s <server-name> [-u <username> -p <password>][-o
<filename>] [-f] [-X <rpc-timeout>]

iscon creatediskusagereport --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--output-
file=<filename>]
[--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

> This command creates a report that displays the amount of disk space used by disk
> libraries on a specific server.
>
> -o (--output-file) is the file name used to save the report data. If the output filename
> is not specified, the default filename is: DiskSpaceUsage-server-MM-DD-YYYY-hh-
> mm-ss[.#]
>
> [.#] is the additional suffix when there is a duplicate.

Specify the -f (--force) option if you want to overwrite the existing file if 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 default RPC timeout is 300 seconds.

Physical resources allocation report

```
iscon createphyresourcesallocreport -s <server-name> [-u <username> -p
<password>]
[-o <filename>] [-f] [-X <rpc-timeout>]

iscon createphyresourcesallocreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--output-
file=<filename>]
[--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a report that displays the physical resource allocation for a specific server.

-o (--output-file) is file name used to save the report data. If the output filename is not specified, the default filename is: PhysicalResourcesAllocation-server-MM-DD-YYYY--hh-mm-ss[.#]

[.#] is the additional suffix when there is a duplicate.

Specify the -f (--force) option if you want to overwrite the existing file if 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 default RPC timeout is 300 seconds.

Specific physical resource allocation report

```
iscon createphyresourceallocreport -s <server-name> [-u <username> -p
<password>]
-I <ACSL> [-o <filename>] [-f] [-X <rpc-timeout>]

iscon createphyresourceallocreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--
scsiaddress=<ACSL>]
[--output-file=<filename>] [--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a report that displays the physical resource allocation of a specific device on a specific server.

-I <ACSL> (--scsiaddress) is the LUN address of the device.

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: PhysicalResourceAllocation-server-MM-DD-YYYY--hh-mm-ss[.#]

[.#] is the additional suffix when there is a duplicate.

Specify the -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 default RPC timeout is 300 seconds.

Fibre Channel adapter configuration report

```
iscon createfcaconfreport -s <server-name> [-u <username> -p <password>] [-o
<filename>] [-f] [-X <rpc-timeout>]

iscon createfcaconfreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--output-
file=<filename>]
[--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a report that displays the Fibre Channel adapter configuration for a specific server.

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: FCAdaptersConfig-server-MM-DD-YYYY-hh-mm-ss[.#]

[.#] is the additional suffix when there is a duplicate.

Specify the -f (--force) option if you want to overwrite the existing file if 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 default RPC timeout is 300 seconds.

Replication status report

```
iscon createreplicationstatusreport -s <server-name> [-u <username> -p
<password>]
```

```
[-D <date-range>] [-r <repl-resource-type> | -R <resourceList>] [-o
<outputFilename>]
[-f] [-X <rpc-timeout>]

iscon createreplicationstatusreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--date-
range=<date-range>]
[--repl-resource-type=<repl-resource-type> | --resource-list=<resourceList>]
[[--output-file=<outputFilename>] [--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a report that displays the status of a specified resource on a specific server.

-D (--date-range) is an option to specify the date range to be queried. The date format is YYYYMMDD or YYYYMMDD-YYYYMMDD. If date range is not specified, the default is today's date.

-r (--repl-resource-type) is an option to specify a generic resourse type to be queried. It can be one of the following:

■ TAPE

■ TAPEReplica

The default value is TAPE.

-R <--resource-list> in an option to report the status of the specified resources only. The argument can be a list of virtual identificators separated with commas or the name of a file enclosed in <> containing the resource ID on each line. All the resources must be of the type specified by "-r".

■ Example 1: -R 10000005,10000006

■ Example 2: -R "<res_id_file.txt>"

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: ReplicationStatus-server-MM-DD-YYYY-hh-mm-ss[.#]

[.#] is the additional suffix when there is a duplicate.

Specify the -f (--force) option if you want to overwrite the existing file if 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 default RPC timeout is 300 seconds.

Virtual library information report

```
iscon createvirlibinforeport -s <server-name> [-u <username> -p <password>]
```

```
[-o <filename>] [-f] [-X <rpc-timeout>]

iscon createvirlibinforeport --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--output-
file=<filename>]
[--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a report that displays all of the virtual libraries for a specific server.

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: VirtualLibraryInfo-server-MM-DD-YYYY-hh-mm-ss[.#]

[.#] is the additional suffix when there is a duplicate.

Specify the -f (--force) option if you want to overwrite the existing file if 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 default RPC timeout is 300 seconds.

Virtual tape information report

```
iscon createvirtapeinforeport -s <server-name> [-u <username> -p <password>]
[-o <filename>] [-f] [-X <rpc-timeout>]

iscon createvirtapeinforeport --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--output-
file=<filename>]
[--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a report that displays all of the virtual tapes for a specific server.

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: VirtualTapeInfo-server-MM-DD-YYYY-hh-mm-ss[.#]

[.#] is the additional suffix when there is a duplicate.

Specify the -f (--force) option if you want to overwrite the existing file if 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 default RPC timeout is 300 seconds.

Create job report

```
iscon createjobreport -s <server-name> [-u <username> -p <password>]
[-z <report period>] | [-D <date-range>] [-o <filename>] [-f] [-X <rpc-
timeout>]

iscon createjobreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--report-period=<report-period>] | [--date-range=<date-range>]
[--output-file=<filename>] [--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a report that displays all of the jobs executed during a
selected period of time for a specific server.

-z (--report-period) is the period of time that the report should cover. The accepted
values are:

- t - today

- y - yesterday

- 7 - last seven days

- 30 - last thirty days

-D (--date-range) is the starting date and ending date in the following format
(maximum 30 days):
YYYYMMDD-YYYYMMDD or YYYYMMDD

Either -z (--report-period) or -D (--date-range) can be specified, but not both. The
date option is applied to the server local time. The default value is: "-z t" (today).

-o (--output-file) is the file name used to save the report data. If the output filename
is not specified, the default filename is: JobReport-MM-DD-YYYY-hh-mm-ss[.#]

[.#] is the additional suffix when there is a duplicate.

Specify the -f (--force) option if you want to overwrite the existing file if 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 default RPC timeout is 300 seconds.

Event Log

Get Event Log

```
iscon geteventlog -s <server-name> [-u <username> -p <password>]
[-D <date-range>] [-F <fileFormat>] [-o <filename>] [-H] [-f] [-X <rpc-
timeout>]

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 an output filename is not specified, the default filename is: eventlogYYYY-MM-DD-hh-mm-<servername>[.#]

[.#] is the additional suffix when there is a duplicate.

Specify the -f (--force) option if you want to overwrite the existing file if 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.

Technical support

Get X-Ray

```
iscon getxray -s <server-name> [-u <username> -p <password>]
[-l <#|all|YYMMDDhhmm-YYMMDDhhmm>] [-r] [-o <filename>] [-f] [-X <rpc-
timeout>]

iscon getxray --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--get-log=<#|all|YYMMDDhhmm-YYMMDDhhmm>] [--rescan-for-xray] [--output-
file=<filename>] [--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to get X-ray information from the VTL Server for diagnostic purposes. Each X-ray contains technical information about your server, such as server messages and a snapshot of your server's current configuration and environment. You should not create an X-ray unless you are requested to do so by your Technical Support representative.

-l (--get-log) is a filter to get the specified log messages.

- # = number of lines
- all = all the log messages
- YYMMDDhhmm-YYMMDDhhmm = log messages in date/time range

The default is to get all the log messages.

-r (--rescan-for-xray) is an option to rescan the physical devices before the xray is taken. The default is not to rescan the devices.

-o (--output-file) is the full path of the file name to save the xray to. The default output filename format is:
xray-YYYY-MM-DD-hh-mm-<servername>.tar.gz

Specify the -f (--force) option if you want to overwrite the existing file if 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 300 seconds.

Get attention required information

```
iscon getattentionrequired -s <server-name> [-u <username> -p <password>]
[-X <rpc-timeout>]

iscon getattentionrequired --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This commands displays the attention required messages.

-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 300 seconds.

Required ports

In order to maintain a high level of security, you should disable all unnecessary ports. The only ports required by VTL are:

- TCP port 11576 - Used for VTL Console to VTL Server management communication.
- UDP port 11577 - Used for IP replication.
- UDP port11578 - Used for encryption.
- UDP port11579 - Used for encryption.
- TCP port 11580 - Used for communication between a failover pair.
- UDP port 161 - Used for SNMP traps.
- TCP port 161 - Used for SNMP traps.
- TCP/UDP port 3205 - Used for iSCSI.
- TCP port 3260 - Used for iSCSI.

Although you may temporarily open some ports during initial setup of the VTL server, such as the telnet port (23) and FTP ports (20 and 21), you should shut them down after you have done your work.

Troubleshooting

This appendix addresses the following issues:

- "Problems during console operations" on page 233
- "Problems affecting physical resources" on page 236
- "Problems with virtual resources" on page 237
- "Problems during import/export operations" on page 241
- "Taking an X-ray for technical support" on page 243

Problems during console operations

Issue: **VTL console is unable to connect to a VTL server**

Indications: The VTL console does not connect to the server node. The word `Failed` appears at during the connection process.

Diagnostics: Determine the cause of the failure using the following procedure.

Case: Connection fails before login

1. Wait for a while. Then attempt to connect again.

2. If you can now connect, stop here.

   The server was busy and unable to respond immediately.

3. If the IP address of the server changed recently, delete the server from the VTL console. Then re-add it, and try to connect.

4. If you can now connect, stop here.

   The VTL console was still using the old IP address.

5. If you still cannot connect, try to connect using the server's IP address instead of its server name (or vice versa).

6. If you can now connect, stop here.

   The host name or IP address that failed may be incorrect.

7. If you still cannot connect, check network connectivity. Ping the target server and other machines in the same subnet.

8. If you cannot ping the server or the hosts on the same subnet, there is a network outage. Stop here, and correct the problem. Then reconnect to the VTL server.

Case: Connection fails during log in

1. Verify the user name and password.

   The password is case-sensitive. Make sure the Caps Lock key is not pressed on the keyboard

2. If the user name or password was incorrect, stop here, and log in using the correct credentials.

3. If the user name and password seem to be correct, make sure they exist on the server. From the machine where VTL console is installed, open a secure shell (ssh) session on the VTL server, and log on using the same user name and password as above.

   Note that ssh may be disabled if local security policies so require.

4. If ssh is enabled but you still cannot log in, the user name or password is probably incorrect. Stop here, and obtain proper credentials.

5. If you can log in using ssh, check the status of the VTL server software modules. From the ssh commandline, run the following command:

```
# ipstor status
```

6. If a module has stopped, restart it with the following command, and stop here.

```
# vtl restart <module name>
```

Case: Connection fails while retrieving the server configuration

1. If the connection fails while retrieving the server configuration, note any error messages that appear.

2. Then contact Sun technical support.

Case: Connection fails while checking the VTL license

1. Contact Sun technical support.

Case: Connection fails while expanding the VTL server node

1. Check the memory consumption on the console host.

2. If memory consumption is excessive, stop unnecessary processes, and retry.

3. If you can connect, stop here.

   Avoid running memory-intensive applications on this host when the console is in use.

4. If you cannot connect or if memory consumption appears to be within normal limits, contact Sun technical support.

Issue: Requested operations cannot be performed from the VTL console

Indications: The server exhibits symptoms of high CPU utilization, such as `Server Busy` or `RPC Timeout` messages.

Diagnostics: Determine whether high CPU utilization is normal.

1. Check the Event Log or syslog (`/var/adm/messages`) for CPU-intensive activity on the server.

   Backup jobs that backup to multiple virtual or physical devices in parallel, data compression, and encryption all place heavy demands on the CPU.

2. If CPU-intensive processes are running on the server, stop here, and retry the console later.

   The VTL server is behaving normally.

3. If CPU-intensive processes are not running on the server, if the CPU is not actually busy, or if the problem persists, contact Sun technical support.

Issue: VTL console operations are very slow

Indications: The VTL console is abnormally slow or unresponsive.

Diagnostics: Determine the reason.

Case: Low host system memory

1. Check memory utilization for all running processes on the host.

2. Stop unnecessary processes.

3. If no unnecessary processes are running, provide the host with more memory.

Case: High server activity

1. Check the Event Log or syslog (`/var/adm/messages`) for CPU-intensive activity on the server.

   Backup jobs that backup to multiple virtual or physical devices in parallel, data compression, and encryption all place heavy demands on the CPU.

1. Also, try starting a second instance of the VTL console. If the second VTL console cannot establish connections, that means the server is busy with previous RPC operations.

2. If CPU-intensive processes are running on the server, stop here, and retry the console later.

   The VTL server is behaving normally.

3. If CPU-intensive processes are not running on the server, if the CPU is not actually busy, or if the problem persists, contact Sun technical support.

Problems affecting physical resources

Issue: **The VTL console does not display some physical storage devices**

Indications: The console does not display all expected physical devices.

Diagnostics: Check to see if the devices are present and accessible.

1. Rescan physical devices from the VTL console by right-clicking on `Physical Resources` and selecting `Rescan` from the context menu. Make sure that `Discover New Devices` is specified. Specify a `LUN Range` that you reasonably expect will include the device.

2. If the console now displays the missing devices, stop here.

3. If rescanning does not detect the missing devices, check the system Event Log or syslog (`/var/adm/messages`) for error messages that may correspond to the rescan operation. Look for failed devices or errors that kept an otherwise discoverable device from being accessed.

4. If the logs reveal a device failure or error, stop here. Correct the device problem.

5. If the logs do not reveal the source of the problem, make sure that the VTL server is powered up and that all cable connectors are securely connected.

6. If the VTL server is not powered up or if cables are not connected, stop here. Correct the problem.

7. If you have still not solved the problem, contact Sun technical support.

Problems with virtual resources

Issue: **Virtual tapes are shown `offline` in the console**

Indications: Virtual tapes are `offline`.

Diagnostics: Locate the physical resources that back the virtual tapes and assess their state.

1. Identify the physical resources that back the virtual tapes. In the Virtual Tape Library System branch of the VTL object tree, highlight the branch representing the offline virtual tape, select the `Layout` tab from the property sheet at right, and note the identifying information for the disk that corresponds to the offline tape.

2. In the Physical Resource branch, under the `Storage Devices` > Fibre Channel Devices, locate the physical resources that you identified in the preceding step. Make sure that each physical device is present, operating normally and accessible.

3. If physical devices appear to be missing, inaccessible, or failing, contact Sun technical support.

Issue: **Tape expansion does not work**

Indications: The size of virtual tape cannot be expanded.

Diagnostics: Determine the cause.

1. In the Virtual Tape Library System branch of the VTL object tree, highlight the tape in the console, and make sure that the `Total Size` field is accurate.

2. If the `Total Size` field is accurate, make sure that client machine has been refreshed to see the updated virtual resource. Rescan devices.

   The expansion has succeeded, but the client machine does not yet see the new size of the expanded device.

3. If rescanning resolves the problem, stop here.

4. If the `Total Size` field is accurate or if the problem persists after a rescan, check the Event Log for error messages.

   The expansion probably failed.

5. If you find disk space errors, there may not be enough physical disk space for the expansion. Add more physical storage or change the size of expansion. Then retry.

6. If no disk space problems were found, or if correcting them does not solve the problem, make sure that the physical storage partition is valid. Correct any problems, and retry.

7. If the partition is valid or if correcting it does not solve the problem, look for I/O errors.

8. If I/O errors are found, consult technical support.

9. Otherwise, look for an RPC timeout during execution of the expand command. See if the server is busy by running the `top` or `ps -x` command on the VTL server.

10. If the server seems excessively busy, stop any unnecessary processes, and retry the expansion operation.

11. If the problem persists or if the event logs show no obviously relevant errors, contact technical support.

Issue: **Client cannot see tape library/drives provisioned by VTL**

Indications: A client operating system or application does not correctly detect virtual devices.

Diagnostics: Further characterize the problem, and determine the cause.

Case: Neither the operating system nor applications appear to see the device

1. See if the operating system includes the device in its configuration.

   - On Sun Solaris platforms, tape libraries are usually shown in the form `/dev/sg<index>`, if the `sg` module is loaded. Tape drives are displayed in the form `/dev/rmt/<index>`, if the `st` module loaded.

   - On Linux platforms, tape libraries are usually shown in the form `/dev/sg<index>`, assuming that the `sg` module is loaded. Tape drives are displayed in the form `/dev/st/<index>`, `/dev/nst/<index>`, and `/dev/sg/<index>`, if the `st` module loaded.

   - On Microsoft Windows platforms, tape libraries appear under `Media Changers` and tape drives under `Tape drives`. Usually the tape drive is represented as `\tape<index>`.

   - HP-UX represents tape libraries with a string of the form `/dev/rac/cXtXdX`, if the `schgr` driver is loaded. Tape drives are represented by `/dev/rmt/<index>`, if the `stape` driver is loaded.

   - AIX displays tape devices as `/dev/rmt<index>` (for LTO1/LTO2) or `/dev/mt<index>` (for DLT/SDLT).

2. If the operating system does not show the device, got to "The operating system cannot detect the device" on page 239.

3. If the operating system does show the device, go to "Applications cannot see the device" on page 239.

Case: The operating system cannot detect the device

1. If the operating system does not see the device, use the VTL console to check the status of the virtual device.

2. If the virtual device is `offline`, stop here, and go to "Virtual tapes are shown `offline` in the console" on page 237.

3. If the virtual device is `online`, check the client configuration. In the VTL console, right-click on the client, and examine the `Resources` tab of the properties sheet in the right-hand pane.

4. If you do not see virtual devices on the `Resources` tab, assign devices to the client.Make sure that devices that are shared by clients attach in `Read/Write non-exclusive` mode. On the client, rescan devices.

5. If the client can see the devices after rescanning, stop here.

6. If the client cannot see its assigned devices, check World Wide Port Names (WWPNs). In the VTL console, right-click on the client, and select `Properties` from the context menu. Record the initiator and target WWPNs.

7. Select the Physical Resources object and locate the HBA that corresponds to the recorded target WWPN. In the property sheet at right, select the `SNS table` tab and look up initiator WWPN that you recorded in the previous step. If multiple HBAs exist, either from the client host or from the VTL target, look up all entries from all target SNS tables.

8. If the VTL console does not record the correct initiator WWPN, unassign the client and the reassign it using the correct mapping. On the client, rescan devices.

9. If the client can see the devices after rescanning, stop here.

Case: Applications cannot see the device

1. If an application fails to find the device, see "The backup application cannot see the device at all" on page 240.

2. If an application finds the device in an unexpected location, see "The backup software does not see the device in the expected place" on page 240.

Case: The backup application cannot see the device at all

1. If the operating system sees the device but a backup application does not, check the drivers for the backup software. Make sure the driver is appropriate for the library and tape drive type.

2. If a driver appears to be inappropriate, refer to the backup software manual. Some backup products recommend specific versions of drivers or special settings. Apply the correct driver.

3. If changing the driver solves the problem, stop here.

4. If the recommended driver is installed or if installing it did not help, check the driver version and upgrade as necessary.

5. If upgrading the driver solves the problem, stop here.

6. If the driver is correctly versioned or if upgrading the driver does not help, look for application software conflicts. Multiple backup products on a single server can cause this sort of problem.

Case: The backup software does not see the device in the expected place

1. If the operating system correctly recognizes the device, but the backup software does not see the device in the expected place, suspect a serialization error in the application. Consult the application vendor and documentation, and install applicable software patches or upgrades.

   Serialization converts objects into streams of sequential object properties. If the application misinterprets the sequence, it may confuse properties such as ownership.

Issue: Client sees the tape library/drive but cannot access it

Indications: A client operating system or application cannot access virtual devices.

Diagnostics: Further characterize the problem, and determine the cause.

Case: Neither the operating system nor applications appear to have access

1. Obtain an operating system-specific raw device utility that can access tape drives.

   - Microsoft Windows clients can use `ntutil` to check emulated IBM Ultrium devices.
   - UNIX systems can use the `mt` or `tar` command to access the tape device (using a syntax like `mt -f /dev/rmt/0 status`).

2. Stop the backup application.

3. Using the VTL console, load a tape into a virtual drive.

   While most raw device utilities work with tape drives, they cannot, in most cases, load tapes. Even if some can move tapes, you need to know the exact address of the tape and the drive.

4. Attempt to access the device using the raw utility.

5. If you cannot access the device, go to "The operating system cannot access the device" on page 241.

6. If you can access the device, go to "The operating system can access the device." on page 241.

Case: The operating system cannot access the device

1. If the operating system `cannot access` the device, make sure that physical storage resources are accessible and in read/write mode.

2. Check the Event Log or syslog (`/var/adm/messages`) for I/O errors.

   I/O error messages usually begin with `log_scsi_error`.

3. Make sure that the adapter driver on the client is certified for use with VTL.

Case: The operating system can access the device.

1. If the operating system `can  access` the device, the backup software is causing the problem. Consult the application documentation and/or application vendor customer support.

2. Make sure that you have the correct drivers.

Problems during import/export operations

Issue: Import/Export does not work as expected

Indications: Import/export operations fail or result in unexpected behavior.

Diagnostics: Determine the cause.

   Case: Tape devices and/or media types are mismatched

   1. Make sure that you are importing from or exporting to the same type of media and device.

You can only import and export data between a physical tape device and a virtual tape device of the same type, using physical and virtual media of the same capacity.

2. If dissimilar physical and virtual devices or media are being used, stop here. Correct the condition, and retry the import/export job.

3. If physical and virtual devices are identical or if making them so does not solve the problem, see if compressed data is being imported/exported.

4. If compressed data is being imported/exported, make sure that virtual and physical media have the same uncompressed capacity.

   Import/export operations fail if the target media does not have enough capacity to accommodate decompressed data.

5. If compression is not an issue, see "The export/import job is not complete" on page 242.

Case: The export/import job is not complete

1. If dissimilar media capacity is not the problem, make sure that the job is not still running. In the VTL console, select the `Import/Export Queue`, and search for related export/import jobs.

2. If a related job is found, the job is not yet complete. Stop here, and recheck it later.

   Jobs are only listed in the queue while active, so listed jobs are still running.

3. If related jobs are not listed in the queue or if the problem persists after the job completes, use the VTL console to examine the `Event Log` for failure messages.

4. If failure messages are found, stop here, correct the error condition(s), and retry the import/export job.

5. If the problem persists, see "Virtual tape barcodes duplicate physical tape barcodes" on page 242.

Case: Virtual tape barcodes duplicate physical tape barcodes

1. If export/import problems persist, make sure that virtual and physical tapes each have their own, unique barcodes. Use the VTL console to `Inventory` the physical library, and check the results against the virtual tapes.

2. If duplicates are found, stop here. Correct the situation, and retry the import/export operation.

3. Otherwise, see "A physical tape library or device is not ready" on page 242.

Case: A physical tape library or device is not ready

1. Check the status of physical tape drives.

2. If physical tape drives require cleaning, clean them, and stop here. Retry the import/export operation.

3. If cleaning is unnecessary or does not help, see if physical tapes need to be moved and mounted before the import/export operation can continue.

4. If tapes have to be moved, move them, and stop here. Retry the import/export operation.

5. If tapes do not need to be moved, check for other anomalous conditions.

6. It other anomalous conditions are found, correct them, and stop here. Retry the import/export operation.

7. If problems persist, see "VTL drive assignments do not reflect library element addresses" on page 243.

Case: VTL drive assignments do not reflect library element addresses

1. When you import data, make sure the assignment of drive in VTL follows the element address of the drives in the physical library. Assign the tape drive in the order of their element address.

2. If VTL assigns drives out of element order, unassign and reassign tape drives in the correct order. Stop here, and retry the import/export operation.

3. If drive order is not an issue or if correcting it fails to resolve the problem, see "Some other system error is causing the problem" on page 243.

Case: Some other system error is causing the problem

1. If problems persist after other possibilities have been exhausted, examine the VTL Event Log or the server syslog (`/var/adm/messages`) for error messages that relate to the physical tape library or drive.

2. If you find error messages, correct the issues if possible. Stop here, and retry the import/export operation.

3. If you cannot find relevant errors or cannot determine a cause or resolution for an error condition, contact Sun technical support.

Taking an X-ray for technical support

If, during a technical support call, a Sun technical support representative asks you to take an X-Ray of your system, note the items that you need to include. Then proceed as follows.

▼ Taking an X-Ray

1. **In the object tree of the VTL console, right-click on the branch representing the VTL server (A below), and select** `X-Ray` **from the context menu (B).**
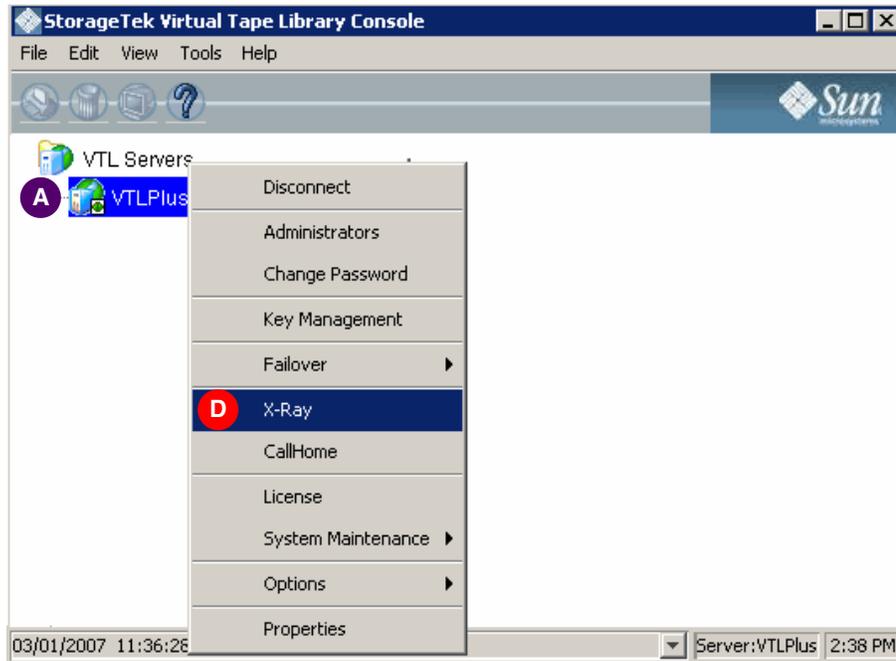
2. **When the** `X-Ray Options` **dialog appears, check the checkboxes corresponding to the items that you need to include (C below).**

The defaults are shown below:
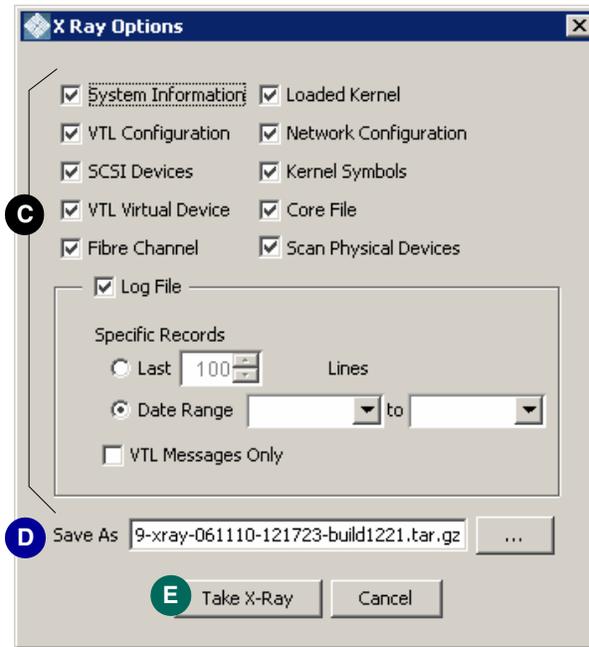
If you select the `Log File` option, you can filter the output by specifying a number of records or a date range. You can limit the results to VTL system-related messages by checking the `VTL Messages Only` check box.

3. **In the** `Save As` **text box (D above), specify an output path and filename for the X-Ray archive.**

4. **X-Rays are saved as gzipped tar archives.**

5. **Press** `Take X-Ray` **(E above) to generate the output.**

Error Messages

No.	Type	Text	Probable Cause	Suggested Action
1005	Error	Out of kernel resources. Failed to get major number for VTL SCSI device.	Too many Linux device drivers are installed.	Type cat /proc/devices for a list to see if any can be removed.
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.	Check Knowledge Base for known memory leak problems in various drivers.
1008	Error	Failed to set up the network connection due to an error in SANRPCListen -- [Error].	Another application is using UDP port 11577.	Confirm using netstat -a, then remove or reconfigure the offending application.
1023	Error	Failed to connect to physical device [Device number]. Switching to alias to [ACSL].	Adapter/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.\n\nIf the replication is triggered by the scheduler, adjust the schedule in the replication policy to avoid replicating too often.

No.	Type	Text	Probable Cause	Suggested 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. Contact hardware manufacturer for diagnostic procedure.
1044	Error	A SCSI command terminated with a non-recoverable hardware failure (for example, controller failure, device failure, parity error, etc.).	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, etc.	Check the system log for additional information. Contact hardware manufacturer for diagnostic procedure.
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.	Check primary path from VTL appliance to physical device.
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.
1069	Error	Replication cannot proceed -- virtual tape [VT#] 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.	Remove replication setup from the virtual tape console since it no longer has a valid replica.

No.	Type	Text	Probable Cause	Suggested Action
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, i.e., 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.	If possible, determine the true cause of the problem by contacting the hardware manufacturer. If the drive is reaching MTBF*, it may be prudent to replace the drive.
7000	Informational	Patch %1 installation completed successfully.	A patch has been applied to the server.	None.
7001	Error	Patch %1 failed -- environment profile is missing in /etc.	Unexpected loss of environment variables defined in /etc/.is.sh on the server.	Check server package installation.
7002	Error	Patch %1 failed -- it applies only to build %2.	The server is running a different build than the one for which the patch is made.	Get the patch, if any, for your build number or apply the patch on another server that has the expected build number.
7003	Error	Patch %1 failed -- you must be the root user to apply the patch.	The user account running the patch is not root user	Run the patch with root account.
7004	Warning	Patch %1 installation failed -- it has already been applied.	You tried to apply the patch again.	None.
7005	Error	Patch %1 installation failed -- prerequisite patch %2 has not been applied.	Required previous patch is not applied.	Apply the required patch before applying this one.
7006	Error	Patch %1 installation failed -- cannot copy new binaries.	Unexpected error on the binary file name or path in the patch.	Contact Tech Support.
7007	Informational	Patch %1 rollback completed successfully.	A patch is rolled back.	None.

No.	Type	Text	Probable Cause	Suggested Action
7008	Warning	Patch %1 rollback failed -- there is no original file to restore.	Patch has not been applied or already rolled back.	None.
7009	Error	Patch %1 rollback failed -- cannot copy back previous binaries.	Unexpected error on the binary file name or path in the patch.	Contact Tech Support.
7010	Error	Patch %1 failed -- the file %2 has the patch level %3, higher than this patch. You must rollback first %4.	A patch with higher level and conflicting with the current patch has been applied.	Roll back first the high level patch, apply this patch, and then apply again the high level patch.
7011	Error	Patch %1 failed -- it applies only to kernel %2.	Patch applied to a server running on an unexpected OS.	Apply the patch on a server that has the expected kernel.
10001	Error	Insufficient privilege (uid: [UID]).	VTL software is not running with root privilege.	Login as root to the Linux server where VTL is to be running before starting VTL.
10002	Error	VTL Server environment is corrupt.	The configuration file in the /etc directory which provides the VTL home directory and other environmental information is either corrupted or deleted.	Determine the cause of such corruption and correct the situation. Perform regular backups of VTL configuration data so it can be restored if corrupted by known elements.
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.	Check storage device connectivity, check the system drive for errors (use OS provided utilities), and check for VTL environment corruption as described in 10002.

No.	Type	Text	Probable Cause	Suggested 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, etc. Check for proper connectivity. Fibre Channel Switch connection status lights do not guarantee a solid connection. Disconnect/Reconnect the Fibre Channel connector for verification. Check the specific storage device using OS provided utilities such as hdparm.
10006	Error	Failed to write configuration[File name].	Error encountered when writing the VTL 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.	Check the system drive using OS provided utilities. Free up space if necessary. If the drive is unreliable or reaching MTBF*, it may be prudent to replace the drive.
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 for checking storage devices. If system resource is low, use top to check the process that is using the most memory. If physical memory is below the recommendation, install more memory to the system. If the OS is suspected in bad state due to unexpected failure in either hardware of software components, restart the server machine to make sure the OS is in a healthy state before trying again.

No.	Type	Text	Probable Cause	Suggested Action
10101	Error	Failed to update configuration [File name].	Error encountered when updating the VTL configuration file on the system drive. This can only happen if the system drive is corrupted or has failed.	Check the system drive using OS provided utilities.
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 VTL configuration file already exists when installing the VTL software, possibly from previous installation. The configuration file will be reused.	If there is reason to believe the existing configuration should not be used, e.g.. the file is suspected to be corrupted, then remove the VTL directory before reinstallation.
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.	Check the physical connection of the storage, and the storage system. If problem persists, call tech support.
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.	Check the storage system, including all cabling. Once the problem is corrected, rescan on the adapter with the connected drive. Limit the scope of the scan to that SCSI address.

No.	Type	Text	Probable Cause	Suggested Action
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, etc.	Check the storage system, including all cabling. Once the problem is corrected, rescan on the adapter with the connected drive. Limit the scope of the scan to that SCSI address.
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 VTL is down.	Make sure drives are not changed without using the VTL console to eliminate them from the virtual resource list first. Also never allow other applications to directly access the physical drives without going through VTL.
10215	Warning	Marked PDev [GUID] OFFLINE because its storage capacity has changed.	The physical drive geometry, including the number of sectors, is different from the original record.	Rescan the drive to re-establish its properties.
10240	Error	Missing SCSI Alias [A,C,S,L].	One of the existing SCSI paths 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.	Check cabling and storage system. After situation is corrected, rescan the adapter connected to the drive, and limit the scope to that path.
10241	Error	Physical Adapter [Adapter number] could not be located in /proc/scsi/.	The adapter driver could be unloaded.	Check the loaded drivers.

No.	Type	Text	Probable Cause	Suggested Action
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 VTL, it is not allowed to have the LUN changed.	Do not change the LUN of a virtualized drive. Revert back to the original LUN.
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 if the inquiry pages exist.	Only use this type of drive for virtual drive, and not SED.
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.	Never access the virtual drives bypassing VTL.
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, restart the OS, or restart the machine (hard/cold reset). If problem still persists, you may need to reinstall the OS. If that is the case make sure you properly save all VTL configuration information before proceeding.
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.

No.	Type	Text	Probable Cause	Suggested Action
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	VTL communication module Failed to start.	Most likely due to the port for VTL comm module is being occupied by a previous unexpected failure of the communication module, or by another application.	Restart the OS and try again. If problem persists, use the OS provided utilities, such as netstat to check the port used.
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 VTL system.
11033	Error	Auto save configuration: cannot login user.	Incorrect user name or password	Please double check the user name and password specified in the auto save configuration settings.
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.
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.
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.
11050	Warning	Cannot start replication for virtual device [VD#] because it's on LUN [L#], which is being migrated.	A replication operation was triggered for a tape that has segments on a LUN that is being migrated.	No specific user action required. Replication will continue at the next scheduled time, after the LUN migration is completed.

No.	Type	Text	Probable Cause	Suggested Action
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.	Check OS resources using provided utilities such as top.
11104	Error	There are too many SAN Client connections.	The number of simultaneous connections exceeded the supported limit the current system resource can handle.	This is an unlikely condition as long as the recommended memory is available for the server.
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 VTL. If corruption is the cause, then it is most likely due to a system drive hardware error.	If there is a valid configuration file saved, it can be restored to the system. Make sure to use reliable storage devices for any critical system functions.
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.	Use top to check the process that is using the most memory. If physical memory is below the recommendation, install more memory to the system.
11170	Error	Failed to virtualize LUN [L#] because of mismatching size between configuration file and disk. Please do rescan and try it again.	Attempting to virtualize a LUN that has a different capacity than what was previously seen.	Rescan for new devices and try again.
11201	Error	There are too many Console connections.	Too many VTL console processes are connected to the particular VTL server. This is a highly unlikely condition.	None.

No.	Type	Text	Probable Cause	Suggested Action
11202	Error	Console ([host name]): Illegal access.	The VTL console host attempts to perform operation outside of the granted privilege level. This rarely 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 VTL 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.
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, e.g., power status; controller status, etc. Check the connectivity, e.g., cable connectors. In Fibre Channel switches, even the connection status light indicates the connection is good, it is still not a guarantee. Disconnect/reconnect the connector to make sure. Check the specific storage device using OS provided utilities such as hdparm.
11209	Error	Console ([host name]): Insufficient privilege access.	A 'read only' user attempts to do an operation that requires configuration change.	Login as administrator user if configuration changes need to be made.

No.	Type	Text	Probable Cause	Suggested Action
11211	Error	Console ([host name]): Failed to save file [filename].	Error encountered when writing the VTL 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.
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.	Free up disk space, or add additional disk space to system drive.
11216	Error	Console ([host name]): Out of system resources. Failed to fork process.	The VTL 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.	Check system resources, such as memory, system disk space, and storage device connectivity (cable connections).
11233	Error	Console ([host name]): Failed to map the SCSI device name for [ACSL].	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 VTL server.	See 11204. Check and restore the physical configuration to proper state if changed improperly.
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.	Test run the hdparm program from the VTL server console directly. Check storage devices as described in 11204.

No.	Type	Text	Probable Cause	Suggested Action
11240	Error	Console ([host name]): Failed to start the VTL Server module.	When any VTL process cannot be started, it is most likely due to insufficient system resources, an invalid state left by VTL 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 VTL server.	If system resource is low, use top to check the process that is using the most memory. If physical memory is below the recommendation, install more memory to the system. If the OS is suspected in bad state due to unexpected failure in either hardware of software components, restart the server machine to make sure the OS is in a healthy state before trying again.
11242	Error	Console ([host name]): Failed to stop the VTL Server module.	When any VTL process cannot be started, it is most likely due to insufficient system resources, an invalid state left by VTL 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 VTL server.	If system resource is low, use top to check the process that is using the most memory. If physical memory is below the recommendation, install more memory to the system. If the OS is suspected in bad state due to unexpected failure in either hardware of software components, restart the server machine to make sure the OS is in a healthy state before trying again.
11257	Error	Console ([host name]): Failed to add SAN Client ([Host name]).	See 11101.	See 11101.

No.	Type	Text	Probable Cause	Suggested 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.	Check system resource, such as memory, system disk space. Check the syslog for specific reason of the failure.
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.	Check the repository mirror disk.
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]): Invalidconfigurationformat.	See 11112.	See 11112.
11406	Error	Failed to prepare the failover configuration package.	Suspend fail over initiated while packaging fail over configuration information.	No action required. (Operation will be retried automatically)

No.	Type	Text	Probable Cause	Suggested Action
11407	Error	Failed to extract the failover configuration package.	Same as 11406	No action required (Operation will be retried automatically)
11500	Error	Out of disk space to expand virtual tape.	There is no more storage space available for expanding a virtual tape.	Add more storage to VTL system.
11512	Error	Console: Failed to add a replica for virtual tape to IPStor 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 IPStor Server (watermark: MB, time: , interval: , watermark retry: , suspended:).	Error encountered when writing the updated configuration to the VTL 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.	Check to make sure there is enough free space on the system disk. (This should never happen since the VTL system has a mechanism to automatically prune the syslog periodically to prevent syslog from using up all system disk free space). If enough space is available on system disk, check the integrity of system disk file system using fsck utility
11516	Error	Console: Failed to create the virtual tape replica.	Could not update the virtual tape partition information on disk.	Check the Storage system and make sure that storage is working properly.

No.	Type	Text	Probable Cause	Suggested Action
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.
11522	Error	Console: Failed to promote virtual tape replica to a virtual tape.	Failed to update the virtual tape partition information. It	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 VTL 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 IPStor Server (watermark: MB, time: , interval: , watermark retry: , suspended:).	Error encountered when writing the updated configuration to the VTL 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.	Check if the system drive is out of space or has any corruption.
11537	Error	Console ([host name]): Failed to claim physical device [Device number].	This may due a specific version of the VTL server limiting the support of the storage.	Check license agreement for the version of VTL server.
11539	Error	Console ([host name]): Failed to import physical device [Device number].	Storage hardware failure.	See 10004.

No.	Type	Text	Probable Cause	Suggested Action
11542	Error	Console: Failed to remove virtual tape replica.	Error encountered when writing the updated configuration to the VTL 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.	Check if the system drive is out of space or has any corruption.
11554	Error	Console ([host name]): Failed to set failover option <selfCheckInterval:>	IP Network communication failure	Check network connectivity.
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. VTL FC target mode requires the VTL version of the driver to be used.	Use lsmod to check that the proper VTL driver is loaded. If it is, check to make sure it is the correct revision. The correct revision should be located in the VTL/lib directory.
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 connectivityNotes Link
11633	Error	Console : Failed to set failover option on secondary server <heartbeatInterval: sec, autoRecoveryInterval: disabled>.	Same as 11632	Check Network connectivity.
11648	Error	Failed to get inquiry string on SCSI device [Device ID].	Hardware problem with SCSI device.	Check hardware.
11650	Error	Failed to get capacity size for SCSI device [Device ID].	Hardware problem with SCSI device.	Check hardware.

No.	Type	Text	Probable Cause	Suggested Action
11651	Error	Medium test failed for SCSI device [Device name].	Hardware problem with SCSI device.	Check hardware.
11652	Error	Could not get type for SCSI device [Device ID] because of inquiry string failure.	Hardware problem with SCSI device.	Check hardware.
11655	Error	Discarded scsi device [Device ID], bad capacity size.	Hardware problem with SCSI device.	Check hardware.
11741	Error	Console: Failed to create virtual library with [#of Slots] slots due to only [#of Slots] slots available.	Specified slot count for the virtual library exceeds the total slot count supported by the system.	Specify appropriate slot count.
11742	Error	Console: Create only [count] out of [count] virtual drives requested due to memory allocation failure.	System is out of memory, which prevents the creation of the specified number of virtual tape drives.	Increase system memory.
11744	Error	Console: The configuration file update for testmode promoting [#of tapes] tapes was rolled back.	Failed to write to the VTL configuration file.	Check /usr partition for free space. If the partition is out of space, delete unwanted files to create space.
11745	Error	Console: The disk partition update for testmode promoting [#of tapes] tapes was rolled back.	Failed to write update partition information to disks.	Check physical connectivity to the storage system/LUN.
11746	Error	Console: The testmode promotion of [# of tapes] tapes was rolled back.	Cannot add device to IOCore module.	Call technical support.
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 it's barcode.
11788	Error	Appliance Hardware Problem:	Detected an error on the VTL appliance.	Check the error message for information on the error to determine the solution.

No.	Type	Text	Probable Cause	Suggested Action
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 since it doesn't cause any problem for backup/restore. If this error happens the tape will not be resized.
11793	Warning	Appliance Hardware Problem: message	Detected a hardware problem with the appliance	Check the error message and take appropriate hardware maintenance.
11796	Error	Failed to set the migration disk threshold.	Connectivity issues with the storage where VTL repository is located.	Check storage connectivity.
11797	Error	Failed to set the reclamation disk threshold, error = EC.	Connectivity issues with the storage where VTL repository is located.	Check storage connectivity.
12509	Error	Failed to inventoryphysical library VID.	Physical library inventory process failed.	Check server log for more information on the cause of the HW failure.
12511	Error	Failed to move tape in library VID from slot %2 to drive VID.	Physical tape move from slot to drive failed.	Check server log for more information on the cause of HW failure.
12521	Error	Failed to move tape in library VID from drive VID to slot VID.	Physical library may have hardware issues.	Check server log for more information on the cause of HW failure.
13309	Error	Failed to communicate with the primary server.	Secondary server failed to talk to primary server	Check network connectivity
13704	Warning	VTL failure detected.	VTL secondary server detected software/hardware failure on Primary server. This will trigger a take over operation.	Once the primary server is brought back up, initiate fails back operation manually.

No.	Type	Text	Probable Cause	Suggested Action
13710	Warning	The Live Trial period has expired for VTL Server[Server name]. Please contact Sun StorageTek or its representative to purchase a license.	Exceeded the 30-day live trial grace period.	Contact Sun StorageTek or its representative to obtain proper license.
13711	Warning	The following options are not licensed: [VTL option]. Please contact Sun StorageTek or its representative to purchase a license.	The specific option is not licensed properly.	Contact Sun StorageTek or its representative to obtain proper license.
13800	Warning	Primary server failure detected. Failure condition:	VTL Primary server detected software/hardware failure on itself. This will trigger a fail over operation to secondary server.	Once the primary server is brought back up, manually fail back operations to primary.
13804	Error	Quorum disk failed to release to secondary.	Negotiation through Quorum disk failed.	Check Storage or connectivity to Storage.
13817	Error	Primary server failback operation failed.	Primary server had a software/hardware failure condition during fail back.	Check Hardware such as FC ports, Storage and connectivity to Storage.
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.
13822	Warning	Secondary will not take over because storage connectivity is not 100%.	Storage or Storage connectivity failure on secondary.	Check Storage or connectivity to storage.

No.	Type	Text	Probable Cause	Suggested 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.	Determine the appropriate amount of memory required for the current configuration and applications. And determine if there are processes that are leaking memory.
13829	Warning	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.	Check storage LUN where the repository is located.
13856	Error	Secondary server ServerName failed to communicate with primary server ServerName through IP IPAddress.	Network connectivity failure happened between primary and secondary servers.	Check network connectivity between primary and secondary servers.
14005	Error	Cannot update ipstor partition information.	Storage is offline.	Check connectivity to storage.
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, or determine the cause of the extensive I/O, and correct the situation if necessary.
16100	Warning	Email Alerts failed to connect to SMTP server ServerIP on port PortID.	Connectivity problems with the SMTP server due to IP address or PortID.	Check network connectivity, SMTP server IP address and PortID.
16101	Warning	Email Alerts failed to send email to SMTP server ServerIP on port PortID.	See 16100.	See 16100.
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.

No.	Type	Text	Probable Cause	Suggested Action
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.
19202	Error	Console (User Name): Failed to create key KEYNAME	Key name already exists. Another user using a different console may have created key with same name.	Retry the operation.
19204	Error	Console (User Name): Failed to delete Key KEYNAME	The key may be deleted or renamed by somebody else in different console.	Retry the operation. Console will be automatically updated, if another user had deleted the key from another console.
19206	Error	Console (User Name): Failed to update information for key KEYNAME	The key name maybe deleted or changed, or the new key name may exist already.	Retry the operation. Console will be automatically updated, if another user had deleted/created the key from another console.
19208	Error	Console (User Name): Failed to create key package PACKAGENAME.	The keys to be exported may be modified or deleted.	Retry the operation.
19210	Error	Console (User Name): Failed to get key package information.	The key package format/content may be invalid.	Recreate the key package.
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.

No.	Type	Text	Probable Cause	Suggested 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.
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.
40013	Error	Export Tape failed, not enough memory.	System is running low on memory. May be because too many concurrent operations are in process.	If too many operations are in progress, wait till some operations are completed. Increasing the physical memory available on the system may also resolve the problem.
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.
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.
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.
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.
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.

No.	Type	Text	Probable Cause	Suggested Action
40023	Error	Import failed, not enough memory.	System is running low on memory. May be because too many concurrent operations are in process.	If too many operations are in progress, wait till some operations are completed. Increasing the physical memory available on the system may also resolve the problem.
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.
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.
40032	Warning	Physical Tape not available to start export job in lib.	There is an import/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.
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.
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.
40045	Error	Read from Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40046	Error	Write to Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
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.
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.
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.
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.

No.	Type	Text	Probable Cause	Suggested Action
40051	Error	Inquiry command to Physical device failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
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.
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.
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.
40074	Error	Export to Physical Tape failed.	Check the event log messages prior to this message for the exact reason for the failure.	Check suggested action for the error message prior to this message.
40076	Error	Import Physical Tape failed.	Check the event log messages prior to this message for the exact reason for the failure.	Check suggested action for the error message prior to this message.
40077	Error	Import Physical Tape failed. Duplicate Virtual Tape Barcode.	A virtual tape with the same barcode already exists in the virtual library.	VTL doesn't allow duplicate barcodes in a system. 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.	VTL doesn't allow duplicate barcodes in a system. 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.
40086	Error	Write command to Configuration Repository Failed. Please check repository LUNs.	Storage or Storage connectivity problems.	Check Storage and Storage connectivity.

No.	Type	Text	Probable Cause	Suggested Action
40090	Error	Failed to load tape because it is a cleaning tape. Lib VID ##, Drive VID ##, BC ###	A cleaning tape is manually moved into a drive from console or a cleaning tape is used for import/export jobs.	Please check and make sure that cleaning tapes are not used for import/export jobs.
40092	Error	Error in retrieving the hostname of this CDL server.	Cannot get the system's hostname.	On CDL appliance verify that 'uname -a' returns the hostname.
40093	Error	Failure in looking up the IP address of the CDL server (ServerName). Please verify that DNS is configured correctly for both ACSLS and CDL server.	Couldn't find the IP address of the CDL server from DNS nor the /etc/hosts file.	If DNS is configured then verify that the DNS server is running and is configured correctly for both CDL appliance and ACSLS. If DNS is not configured then verify that the /etc/hosts file contains the public IP of the CDL appliance.
40096	Error	Failed to open [AAA].	Could not open ACSLS configuration file.	Verify that the ACSLS conf file exists at /usr/local/VTL/etc/acsls_ls_cdk.conf
40097	Error	DNS configuration for CDL server is incorrect. DNS or /etc/hosts is returning x.x.x.x as the IP of CDL server ServerName	Couldn't find the IP of the DL server from DNS nor the /etc/hosts file.	If DNS is configured then verify that the DNS server is running and is configured correctly for both CDL and ACSLS server. If DNS is not configured then verify that the /etc/hosts file contains the public IP of the CDL appliance.
40098	Error	Failed to successfully query ACSLS server with IP x.x.x.x Error from ACSLS: EC	Failed to contact the ACSLS with the entered IP address.	Please verify that the IP is valid and that users can ping the ACSLS server from the DL server.
40099	Error	Waited N seconds to get a response from ACSLS x.x.x.x. Timing out...	Failed to contact the ACSLS with the entered IP address.	Please verify that the IP is valid and that users can ping the ACSLS server from the DL server.

No.	Type	Text	Probable Cause	Suggested Action
40100	Error	Failed to mount BARCODE on drive x.x.x.x. Error from ACSLS x.x.x.x: [Error message from ACSLS]	Mount operation failed.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the mount failed.
40101	Error	Waited ## seconds to get a response from ACSLS x.x.x.x after trying to mount BARCODE on drive x.x.x.x. Timing out...	Mount operation failed, timing out.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the mount failed.
40102	Error	Failed to dismount BARCODE from drive x.x.x.x. Error from ACSLS x.x.x.x: [Error message from ACSLS server].	Dismount operation failed.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the dismount failed.
40103	Error	Waited ## seconds to get a response from ACSLS x.x.x.x after trying to dismount BARCODE from drive x.x.x.x. Timing out…	Dismount operation failed, timing out.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the dismount failed.
40104	Error	Failed to retrieve drive information in ACS ##. Error from ACSLS x.x.x.x: [Error message from ACSLS server]	Failed to get drives list from ACSLS server.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the 'display' command failed.
40105	Error	|Waited ## seconds to get a response from ACSLS x.x.x.x after trying to retrieve drive information in ACS ##. Timing out...	Failed to get drives list from ACSLS server. Timing out.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the 'display' command failed.
40106	Error	Failed to retrieve volume information in ACS ## and Pool ##. Error from ACSLS x.x.x.x: [Error message from ACSLS server]	Failed to get volume list from ACSLS server.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the 'display' command failed.

No.	Type	Text	Probable Cause	Suggested Action
40107	Error	Waited ## seconds to get a response from ACSLS x.x.x.x after trying to retrieve volume information in ACS ## and Pool ##. Timing out.	Failed to get volume list from ACSLS server. Timing out.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the 'display' command failed.
40108	Error	Failed to retrieve LSM information in ACS ##. Error from ACSLS x.x.x.x: [Error message from ACSLS server]	Failed to get LSM list from ACSLS server.	Check the ACSLS manager server's event log to see why the 'display' command failed.
40109	Error	Waited ## seconds to get a response from ACSLS x.x.x.x after trying to retrieve LSM information in ACS ##. Timing out.	Failed to get LSM list from ACSLS server. Timing out.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the 'display' command failed.
40136	Error	Space command to Physical Library DriveVID failed. EC ErrorCode.	A space command to a physical tape drive failed.	Check physical tape drive. Sense key/ASC/ASCQ will give more information about the cause of the error.
40137	Error	Failed to add import/export job to the job queue. Maximum of 26244 jobs reached. Job ID:JOBID Physical tape barcode:[BARCODE].	No space in job queue to hold new import/export jobs. Max limit is 65536.	Remove old jobs from the queue.
40141	Error	Scan Physical Tape failed. Job ID JobID, EC ErrorCode, SrcTape [BARCODE]	Scanning physical tape failed due to hardware error.	Check physical library/drive HW.
40142	Error	Stack Import Physical Tape failed. Job ID JobID, EC ErrorCode, SrcTape [BARCODE]	Importing a stacked physical tape failed due to hardware error.	Check physical library/drive HW.

No.	Type	Text	Probable Cause	Suggested Action
40143	Error	Stack Export to Physical Tape failed. Job ID JobID, EC ErrorCode, SrcTape [BARCODE] DestTape [BARCODE]	Stacked export to physical tapes failed due to hardware error.	Check physical library/drive HW.
40148	Error	Stack Export Tape failed with not enough memory. Job id JobID	System is out of memory.	Check system memory usage. If required add additional memory to system.
40152	Error	Stack Import failed, not enough memory JobID	System is out of memory.	Check system memory usage. If required add additional memory to system.
40155	Error	ACSLS/LS: Failed to eject [BARCODES] from CAP x.x.x. Error from ACSLS (IP): ErrorString.	Ejecting physical tapes from ACSLS CAP failed due to hardware or software error on the ACSLS server.	Check ACSLS library and make sure its CAPs are online and there are no HW/SW issues.
40156	Error	ACSLS/LS: Waited ## seconds for eject operation ([BARCODES] from ACSLS/LS IP, CAP x.x.x) to complete. Timing out.	Timed out ejecting physical tapes from ACSLS library.	Check IP connectivity between VTL and ACSLS servers or the health of the ACSLS server and library.
40158	Error	ACSLS/LS: Failed to enter tapes from CAP [BARCODES]. Error from ACSLS/LS (IP): ErrorString.	Failed to enter physical tapes into ACSLS library via its CAPs.	Check if CAPs of ACSLS library are empty or not.
40159	Error	ACSLS/LS: Waited ## second(s) for ACSLS/LS server to enter tapes from CAP [CAP id]. Timing out.	Timed out entering physical tapes into ACSLS library.	Check IP connectivity between VTL and ACSLS servers or the health of the ACSLS server and library.
40161	Error	ACSLS/LS: Failed to query CAP information for ACS ##. Error from ACSLS/LS (IP): ErrorString.	Failed to retrieve CAP information of ACSLS library.	Check health of ACSLS server.

No.	Type	Text	Probable Cause	Suggested Action
40162	Error	ACSLS/LS: Waited ## second(s) for ACSLS/LS server (IP) to return CAP information for ACS ##. The operation is timed out.	Timed out retrieving CAP information from ACSLS server.	Check IP connectivity between VTL and ACSLS servers or the health of the ACSLS server and library.
40165	Warning	Door opened condition reported on Physical Library VID-VID VendorID ProductID	Physical library door is open.	Check physical library door.
40166	Warning	Tape Alert from device [VendorID][ProductID] ACSL A:C:S:L – ErrorMessage	Physical tape drive reported a Tape Alert message.	Check Error message for further information.
40168	Warning	No license for Virtual Tape Encryption. Decryption/tape writing disabled for tape VID TapeVID.	No license for tape encryption feature.	Acquire and install tape encryption feature license.
40176	Warning	Physical Tape [BARCODE] is not available to start tape duplication job. Set the job JobID to HOLD.	A physical tape needed for tape duplication job is not available.	Check physical library inventory and make sure that the needed tape is present.
40177	Error	Failed to read SIR data disk with GUID GUID; Error code ErrorCode; Check the disk which might not be accessible.	SIR data disk is not accessible.	Check storage connectivity.
40183	Warning	TapeDuplication: Job JobID - An extra tape copy job cannot be created due to no more physical libraries with same barcode [Barcode].	Physical libraries needed for tape duplication jobs do not exist. (Note: tape duplication requires as many physical library as the number of copies to be made.)	Make sure that as many physical libraries as the number of copies needed are configured.
40184	Warning	TapeDuplication: Job JobID.Copy# - The tape [Barcode] cannot not be moved when copy job will be done because an extra copy job cannot be created.	Copy job was submitted with 'move' option (to delete tape after export). Not all copy jobs could be created, and hence virtual tape being copied will not be deleted at the end of the copy jobs.	Check physical library inventory and make sure that all tapes needed for tape duplication jobs are present in the system.

No.	Type	Text	Probable Cause	Suggested Action
40185	Warning	TapeDuplication: Job JobID.Copy#- The tape [Barcode] cannot not be reclaimed when copy job will be done because an extra copy job cannot be created.	Virtual tape being duplicated to physical tape will not be reclaimed, because not all copy jobs could be submitted successfully.	Check physical library inventory and make sure that all tapes needed for tape duplication jobs are present in the system.
40186	Warning	TapeDuplication: Job JobID - The tape [Barcode] cannot be reclaimed because an extra tape copy job was not completed successfully.	Virtual tape duplicated to physical tapes cannot be reclaimed. One ore more of the copy jobs failed.	Make sure all tapes needed for duplication jobs are in appropriate physical tape libraries. If tapes are present, make sure that physical libraries, drives are online and are functioning correctly.
40187	Warning	TapeDuplication: Job JobID - The tape [Barcode] cannot be moved because an extra tape copy job was not completed successfully.	One ore more copy job failed. Virtual tape will not be deleted since not all copies were made.	Check both physical library and drive status to make sure they are online.
40188	Warning	Stack Import job JobID completed: VLib VID VID, SrcTape [Barcode] Throughput Throughput MB/min. [Copies] tapes with non unique barcodes not imported.	Physical tape has multiple virtual tapes with the same barcode.	Avoid stacking multiple tapes with the same barcode to physical tape.

SNMP traps

The VTL product family defines the following Simple Network Management Protocol (SNMP) traps.

Trap	Severity	Message
9	Error	SCSI Port Error -- %1.
1000	Error	Socket connection could not be terminated properly -- %1.
1001	Error	Socket connection could not be terminated properly due to error during shutdown -- %1.
1002	Error	Unexpected interrupt occurred.
1003	Informational	"VTL Server has detected virtual device[%1] at SCSI %2, channel %3, ID %4, LUN %5."
1004	Informational	VTL Server has not detected any virtual device.
1005	Error	Out of kernel resources. Failed to get major number for VTL SCSI device.
1006	Error	Failed to allocate memory.
1007	Error	Failed to set up the network connection due to an error in SANRPC_Init -- %1.
1008	Error	Failed to set up the network connection due to an error in SANRPCListen -- %1.
1009	Informational	There are %1 real device(s) associated with virtual device [%2].
1010	Informational	Real Device[%1 %2 %3 %4].
1011	Error	Error while writing -- write(%1) result = 0x%2 cmd = 0x%3.
1012	Error	Error while reading -- read(%1) result = 0x%2 cmd = 0x%3.
1013	Informational	VTL Server [Build %1] is running on Linux %2.
1014	Informational	VTL Server has been shut down.
1015	Informational	"Maximum SCSI devices reached. On your VTL Server, verify with the command: cat /proc/scsi/scsi"
1016	Informational	Primary virtual device %1 has failed. VTL is switching to the secondary virtual device.
1017	Informational	Secondary virtual device %1 has failed.

Trap	Severity	Message
1020	Informational	Replication for virtual tape %1 started.
1021	Informational	Replication for virtual tape %1 finished.
1022	Warning	Replication has failed for virtual tape %1 -- %2.
1023	Error	Failed to connect to physical device %1. Switching alias to %2.
1024	Informational	Device %1 has attached to the VTL Server.
1025	Informational	Device %1 has detached from the VTL Server.
1026	Informational	Replication has been started for virtual tape %1; it was triggered by the watermark.
1027	Informational	Replication has been started for virtual tape %1; it was triggered by the interval schedule.
1028	Informational	Replication has been started for virtual tape %1; it was triggered by the time of day schedule.
1029	Informational	Replication has been started for virtual tape %1; it was manually triggered by the administrator.
1030	Error	Failed to start replication -- replication is already in progress for virtual tape %1.
1031	Error	Failed to start replication -- replication control area not present on virtual tape %1.
1032	Error	Failed to start replication -- replication control area has failed for virtual tape %1.
1034	Error	Replication failed for virtual device %1 -- the network transport returned error %2.
1035	Error	Replication failed for virtual device %1 -- the local disk failed with error %2.
1038	Error	Replication failed for virtual device %1 -- the local server could not allocate memory.
1039	Error	Replication failed for virtual device %1 -- the replica failed with error %2.
1040	Error	Replication failed for virtual device %1 -- failed to set the replication time.
1041	Informational	Mirror synchronization started for virtual device %1.
1042	Informational	Mirror synchronization finished for virtual device %1.
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. Please check the system log for additional information.
1044	Error	"A SCSI command terminated with a non-recoverable hardware failure (for example, controller failure, device failure, parity error, etc.). Please check the system log for additional information."
1045	Informational	Rescan replica has completed for virtual device %1
1046	Error	Rescan replica has failed for virtual device %1 -- the local device failed with error %2.

Trap	Severity	Message
1047	Error	Rescan replica has failed for virtual device %1 -- the replica device failed with error %2.
1048	Error	Rescan replica has failed for virtual device %1 -- the network transport returned error %2.
1049	Error	Rescan replica cannot proceed -- replication control area not present on virtual device %1
1050	Error	Rescan replica cannot proceed -- replication control area has failed for virtual device %1
1051	Error	Rescan replica cannot proceed -- a merge is in progress for virtual device %1
1052	Error	Rescan replica failed for virtual device %1 -- replica status returned %2
1053	Error	Rescan replica cannot proceed -- replication is already in progress for virtual device %1
1054	Error	Replication cannot proceed -- a merge is in progress for virtual device %1
1055	Error	Replication failed for virtual tape %1 -- replica status returned %2
1056	Error	Replication control area exchange failed for virtual tape %1 -- the error code is %2
1057	Informational	Replication control area exchange has completed for virtual tape %1
1058	Informational	Replication has finished for virtual tape %1. %2 KB in %3 seconds (%4KB/sec)
1059	Error	Replication failed for virtual tape %1 -- start replication returned %2
1060	Error	Rescan replica failed for virtual device %1 -- start scan returned %2
1061	Warning	I/O path failure detected. Alternate path will be used. Failed path (A.C.S.L): %1; New path (A.C.S.L): %2
1062	Informational	Replication has been started for group %1; it was triggered by the watermark.
1063	Informational	Replication has been started for group %1; it was triggered by the interval schedule.
1064	Informational	Replication has been started for group %1; it was triggered by the time of day schedule.
1065	Informational	Replication has been started for group %1; it was manually triggered by the administrator.
1067	Error	Replication cannot proceed -- unable to connect to replica server %1.
1068	Error	Replication cannot proceed -- group %1 is corrupt.
1069	Error	Replication cannot proceed -- virtual tape %1 no longer has a replica or the virtual tape replica does not exist.
1070	Error	Replication cannot proceed -- replication is already in progress for group %1.
1071	Error	Replication cannot proceed -- virtual tape %1 no longer has a replica or the virtual tape replica does not exist.
1072	Error	Replication cannot proceed -- missing a remote replica device in group %1.
1073	Error	Replication cannot proceed -- unable to open configuration file.

Trap	Severity	Message
1074	Error	Replication cannot proceed -- unable to allocate memory.
1075	Error	Replication cannot proceed -- unexpected error %1.
1076	Informational	Starting replication for virtual device %1 of group %2 to replica device %3.
1077	Informational	Replication for group %1 has completed successfully.
1079	Error	Replication for group %1 has failed due to error on virtual device %2
1082	Error	Replication for virtual tape %1 has been manually aborted by user
1083	Error	Replication for group %1 has been manually aborted by user
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.
1085	Error	for virtual device %1 has been auto-disabled due to an error.
1086	Error	Replication cannot proceed -- failed to load the virtual tape %1.
1087	Error	Replication cannot proceed -- virtual tape %1 is in the drive.
1088	Error	Replication cannot proceed -- failed to set initialization status in VirtualLibrary System for virtual tape %1.
1089	Informational	No data has been updated to the virtual tape %1 since last replication. Replication is completed without updating the replica.
1201	Warning	Kernel memory is low. Add more memory to the system if all possible! Restart the host if possible.
1202	Informational	Path trespassed to %1 successfully.
1203	Error	Path failed to trespass to %1.
1204	Error	Failed to add path group. ACSL: %1.
1205	Informational	Activated path successfully: %1.
1206	Error	Failed to activate path: %1.
1207	Error	Critical path failure detected. Path %1 will be removed.
1208	Warning	Path %1 does not belong to active path group.
1209	Informational	Rescan the FC adapters is recommended to correct the configuration.
1210	Warning	No valid path is available for device %1.
1211	Warning	No valid group is available.
1212	Warning	"No active path group found. Storage connectivity failure. Check cables, switches and storage system to determine cause. GUID: %1."
1213	Informational	Storage device added new path: %1.
1214	Error	Failed to add path: %1.
2000	Informational	Path status has changed : %1
7000	Informational	Patch %1 installation completed successfully.
7001	Error	Patch %1 failed -- environment profile is missing in /etc.

Trap	Severity	Message
7002	Error	Patch %1 failed -- it applies only to build %2.
7003	Error	Patch %1 failed -- you must be the root user to apply the patch.
7004	Warning	Patch %1 installation failed -- it has already been applied.
7005	Error	Patch %1 installation failed -- prerequisite patch %2 has not been applied.
7006	Error	Patch %1 installation failed -- cannot copy new binaries.
7007	Informational	Patch %1 rollback completed successfully.
7008	Warning	Patch %1 rollback failed -- there is no original file to restore.
7009	Error	Patch %1 rollback failed -- cannot copy back previous binaries.
10000	Informational	VTL Server setup has begun.
10001	Error	Insufficient privilege (uid: %1).
10002	Error	VTL Server environment is corrupt.
10003	Error	Failed to initialize configuration %1.
10004	Error	Failed to get SCSI device information.
10005	Error	A physical device will not be available because we cannot create a Global Unique Identifier for it.
10006	Error	Failed to write configuration %1.
10007	Informational	VTL Server setup is complete.
10050	Informational	VTL Server FSID update has begun.
10051	Informational	"VTL Server FSID update vdev %1, local sect %2, pdev sect %3, from %4 to %5."
10052	Informational	"VTL Server FSID update pdev a:%1, c:%2, s:%3, l:%4 from %5 to %6."
10053	Informational	VTL Server FSID update dynamic xml pdev from %1 to %2.
10054	Error	VTL Server FSID update error.
10055	Informational	VTL Server FSID update is complete.
10056	Informational	Server Persistent Binding update has begun.
10057	Informational	"Server Persistent Binding update, swap binding %1."
10058	Informational	"Server Persistent Binding update, set default binding for %1."
10059	Error	Server Persistent Binding update error.
10060	Informational	"Server Persistent Binding update is complete, %1 changes."
10100	Error	Failed to scan new SCSI devices.
10101	Error	Failed to update configuration %1.
10102	Error	Failed to add new SCSI devices.
10200	Warning	Configuration %1 exists.
10201	Warning	Overwriting existing configuration %1.
10202	Informational	Cancelled overwriting configuration %1.

Trap	Severity	Message
10206	Informational	Add scsi alias=%1.
10207	Error	"Add Adapter %1 failed, not enough memory."
10208	Informational	"Set Adapter %1 offline, adapter count %2."
10209	Error	"Add Physical Device %1 failed, not enough memory."
10210	Warning	Marked Physical Device [%1] OFFLINE because its GUID: %2 does not match scsi GUID: %3.
10211	Warning	"Marked Physical Device [%1] OFFLINE because its wwid %2 does not match scsi wwid %3, [GUID: %4]."
10212	Warning	"Marked Physical Device [%1] OFFLINE because scsi status indicate OFFLINE, [GUID: %2]."
10213	Warning	"Marked Physical Device [%1] OFFLINE because it did not respond correctly to inquiry, [GUID: %2]."
10214	Warning	"Marked Physical Device [%1] OFFLINE because its GUID is an invalid FSID, [GUID: %2]."
10215	Warning	"Marked Physical Device [%1] OFFLINE because its storage capacity has changed, [GUID: %2]."
10240	Error	Missing SCSI Alias %1.
10241	Error	Physical Adapter %1 could not be located in /proc/scsi/.
10242	Error	Duplicate Physical Adapter number %1 in /proc/scsi/.
10243	Error	Physical Device data structure is null.
10244	Error	"Invalid FSID, device %1 - the LUN byte (4th byte) in FSID %2 does not match actual LUN."
10245	Error	"Invalid FSID, Generate FSID %1 does not match device acsl:%2 GUID %3."
10246	Error	"Fail to generate FSID for device acsl:%1, can't validate FSID."
10247	Error	"Device (acsl:%1) GUID is blank, can't validate FSID."
10248	Warning	Remove all scsi alias from %1.
10249	Warning	Remove missing scsi alias %1 from %2.
10250	Warning	Remove scsi alias %1 from %2 because their categories are different.
10251	Warning	Remove scsi alias %1 from %2 because their GUIDs are different.
10496	Error	Failed to attach tle repository.
11000	Error	Failed to create socket.
11001	Error	Failed to set socket to re-use address.
11002	Error	Failed to bind socket to port %1.
11003	Error	Failed to create TCP service.
11004	Error	"Failed to register TCP service (program: %1, version: %2)."
11005	Informational	VTL communication module started.

Trap	Severity	Message
11006	Error	VTL communication module failed to start.
11007	Warning	There is not enough disk space available to successfully complete this operation and maintain the integrity of the configuration file. There is currently %1 MB of disk space available. VTL requires %2 MB of disk space to continue.
11010	Informational	Changed server time to %1.
11020	Informational	Auto save configuration enabled: ftp_server=%1 directory=%2 interval=%3 copies=%4.
11021	Informational	Auto save configuration enabled: ftp_server=%1 port=%2 directory=%3 interval=%4 copies=%5.
11022	Informational	Auto save configuration disabled.
11030	Error	Auto save configuration: cannot setup crontab.
11031	Error	Auto save configuration: cannot create the running script %1.
11032	Error	Auto save configuration: cannot connect to ftp server %1 port %2.
11033	Error	Auto save configuration: cannot login user %1.
11034	Error	Auto save configuration: directory %1 doesn't exist.
11035	Error	Auto save configuration: failed to copy %1 to ftp server.
11036	Error	Auto save configuration: failed to delete old file %1 from ftp server.
11037	Informational	Automated Tape Caching is %1 for virtual library %2.
11100	Informational	SAN Client (%1): SAN Client added.
11101	Error	SAN Client (%1): Failed to add SAN Client.
11102	Informational	SAN Client (%1): Authentication succeeded.
11103	Error	SAN Client (%1): Authentication failed.
11104	Error	Too many SAN Client connections.
11105	Informational	SAN Client (%1): Logged in.
11106	Error	SAN Client (%1): Failed to log in.
11107	Error	SAN Client (%1): Illegal access.
11108	Informational	SAN Client (%1): Logged out.
11109	Error	SAN Client (%1): Failed to open file %2.
11110	Error	SAN Client (%1): Failed to get hostname.
11111	Error	SAN Client (%1): Failed to resolve hostname %2.
11112	Error	SAN Client (%1): Failed to parse configuration file %2.
11113	Error	SAN Client (%1): Failed to restart authentication module.
11114	Error	SAN Client (%1): Failed to allocate memory.
11115	Error	"SAN Client (%1): License conflict -- Number of CPU's approved: %2, number of CPU's used: %3."

Trap	Severity	Message
11170	Error	Failed to virtualize LUN %1 because of mismatching size between configuration file and disk. Please do rescan and try it again.
11200	Error	Buffer overflow.
11201	Error	Too many Console connections.
11202	Error	Console (%1): Illegal access.
11203	Error	Console (%1): SCSI device re-scanning has failed.
11204	Error	Console (%1): SCSI device checking has failed.
11205	Error	Console (%1): Failed to get information for file %2.
11206	Error	Console (%1): Failed to allocate memory.
11207	Error	Console (%1): Failed to open file %2.
11208	Error	Console (%1): Failed to read file %2.
11209	Error	Console (%1): Insufficient privilege access.
11210	Informational	Console (%1): Physical SCSI devices have changed.
11211	Error	Console (%1): Failed to save file %2.
11212	Error	Console (%1): Failed to create index file %2 for Event Log.
11213	Error	Console (%1): Illegal time range (%2 - %3) for Event Log.
11214	Error	Console (%1): Failed to get Event Log (%2 - %3).
11215	Error	Console (%1): Failed to open directory %2.
11216	Error	Console (%1): Out of system resources. Failed to fork process.
11217	Error	Console (%1): Failed to execute program %2.
11218	Error	Console (%1): Failed to remove file %2.
11219	Error	Console (%1): Failed to add device %2.
11220	Error	Console (%1): Failed to remove device %2.
11221	Error	Console (%1): Failed to add SAN Client (%2) to virtual device %3.
11222	Error	Console (%1): Failed to remove SAN Client (%2) from virtual device %3.
11223	Informational	Console (%1): Logged in with read/write privileges.
11224	Informational	Console (%1): Logged in with read only privileges.
11225	Informational	Console (%1): Logged out.
11226	Informational	Console (%1): Configuration file %2 saved.
11227	Informational	Console (%1): Virtual device %2 added.
11228	Informational	Console (%1): Virtual device %2 removed.
11229	Informational	Console (%1): SAN Client (%2) added to virtual device %3.
11230	Informational	Console (%1): SAN Client (%2) removed from virtual device %3.
11231	Error	Console (%1): Failed to get CPU status.

Trap	Severity	Message
11232	Error	Console (%1): Failed to get memory status.
11233	Error	Console (%1): Failed to map the SCSI device name for [%2 %3 %4 %5].
11234	Error	"Console (%1): Failed to execute ""hdparm"" for %2."
11235	Error	Console (%1): Failed to get the VTL Server module status.
11236	Error	Console (%1): Failed to get the version information for the message file.
11237	Error	Console (%1): Failed to get file %2.
11238	Error	Console (%1): Failed to restart the authentication module.
11239	Informational	Console (%1): Authentication module restarted.
11240	Error	Console (%1): Failed to start the VTL Server module.
11241	Informational	Console (%1): VTL Server module started.
11242	Error	Console (%1): Failed to stop the VTL Server module.
11243	Informational	Console (%1): VTL Server module stopped.
11244	Error	Console (%1): Failed to access the VTL administrator list.
11245	Error	Console (%1): Failed to add user %2.
11246	Informational	Console (%1): User %2 added.
11247	Error	Console (%1): Failed to delete user %2.
11248	Informational	Console (%1): User %2 deleted.
11249	Error	Console (%1): Failed to reset password for user %2.
11250	Informational	Console (%1): Password for user %2 reset.
11251	Error	Console (%1): Failed to update password for user %2.
11252	Informational	Console (%1): Password for user %2 updated.
11253	Error	Console (%1): Failed to modify virtual device %2.
11254	Informational	Console (%1): Virtual device %2 modified.
11255	Error	Console (%1): Failed to modify virtual device %3 for SAN Client (%2).
11256	Informational	Console (%1): Virtual device %3 for SAN Client (%2) modified.
11257	Error	Console (%1): Failed to add SAN Client (%2).
11258	Informational	Console (%1): SAN Client (%2) added.
11259	Error	Console (%1): Failed to delete SAN Client (%2).
11260	Informational	Console (%1): SAN Client (%2) deleted.
11261	Error	Console (%1): Failed to get SAN Client connection status for virtual device %2.
11262	Error	Console (%1): Failed to parse configuration file %2.
11263	Error	Console (%1): Failed to restore configuration file %2.
11264	Informational	Console (%1): Configuration file %2 restored.

Trap	Severity	Message
11265	Error	Console (%1): Failed to restart IOCore module.
11266	Error	Console (%1): Failed to erase partition of virtual device %2.
11267	Informational	Console (%1): Virtual device %2 partition erased.
11268	Error	Console (%1): Failed to update meta information of virtual device %2.
11269	Error	Console (%1): Failed to get ID for SAN Client (%2).
11270	Error	Console (%1): Failed to add mirror for virtual device %2.
11271	Informational	Console (%1): Mirror added for virtual device %2.
11272	Error	Console (%1): Failed to remove mirror for virtual device %2.
11273	Informational	Console (%1): Mirror removed for virtual device %2.
11274	Error	Console (%1): Failed to stop mirroring for virtual device %2.
11275	Informational	Console (%1): Mirroring stopped for virtual device %2.
11276	Error	Console (%1): Failed to start mirror synchronization for virtual device %2.
11277	Informational	Console (%1): Mirror synchronization for virtual device %2 started.
11278	Error	Console (%1): Failed to swap mirror for virtual device %2.
11279	Informational	Console (%1): Mirror swapped for virtual device %2.
11280	Error	Console (%1): Failed to create shared secret for VTL Server %2.
11281	Informational	Console (%1): Shared secret created for VTL Server %2.
11282	Error	Console (%1): Failed to change device category for physical device %2 to %3.
11283	Informational	Console (%1): Device category changed for physical device %2 to %3.
11284	Error	Console (%1): Failed to get raw device name for physical device %2.
11285	Error	Console (%1): Failed to execute failover command (%2).
11286	Informational	Console (%1): Failover command executed (%2).
11287	Error	Console (%1): Failed to set failover mode (%2).
11288	Informational	Console (%1): Failover mode set (%2).
11289	Error	Console (%1): Failed to restart VTL Server module.
11290	Informational	Console (%1): VTL Server module restarted.
11291	Error	Console (%1): Failed to update meta information of physical device %2.
11292	Error	Console (%1): Failed to swap IP address from %2 to %3.
11293	Informational	Console (%1): IP address swapped from %2 to %3.
11294	Error	Console (%1): Failed to get host name.
11295	Error	Console (%1): Invalid configuration format.
11296	Error	Console (%1): Failed to resolve host name -- %2.
11297	Informational	Console (%1): Report file %2 removed.

Trap	Severity	Message
11298	Error	Console (%1): Failed to reset cache on target device %2 (ID: %3) for %4 copy.
11300	Error	Invalid user name (%1) used by client at IP address %2.
11301	Error	Invalid password for user (%1) used by client at IP address %2.
11302	Error	Invalid passcode for machine (%1) used by client at IP address %2.
11303	Error	Authentication failed in stage %1 for client at IP address %2.
11304	Informational	User %1 at IP address %2 authenticated.
11305	Informational	Machine %1 at IP address %2 authenticated.
11306	Error	The VTL Administrator group does not exist.
11307	Error	User %1 at IP address %2 is not a member of the VTL Administrator's group.
11308	Error	The VTL Client group does not exist.
11309	Error	User ID %1 at IP address %2 is invalid.
11310	Error	VTL Client User name %1 does not match with the client name %2.
11311	Error	Client agent %1 failed to request license.
11312	Informational	Client agent %1 requested license successfully.
11313	Error	Client agent %1 failed to release license.
11314	Informational	Client agent %1 released license successfully.
11400	Error	Failed to communicate with the Self-Monitor module.
11401	Error	Failed to release IP address %1.
11402	Error	Failed to read %1.
11403	Error	Failed to retrieve authentication information.
11404	Error	Failed to merge authentication information.
11405	Error	Failed to obtain IP address %1.
11406	Error	Failed to prepare the failover configuration package -- %1.
11407	Error	Failed to extract the failover configuration package -- %1.
11408	Warning	Synchronizing the system time with %1. A system reboot is recommended.
11500	Error	Out of disk space to expand virtual tape %1.
11501	Error	Failed to expand virtual tape %1: maximum segment exceeded (error code %2).
11502	Error	Failed to expand virtual tape %1 (segment allocation error code %2).
11503	Informational	Expand %1 by %2 MBytes.
11504	Error	Failed to expand virtual tape id %1 by %2 MBytes.
11505	Error	Failed to change virtual tape %1 to direct link mode.
11507	Error	Console (%1): Failed to create X-Ray file.
11508	Error	Console (%1): Failed to set the properties for the VTL Server.

Trap	Severity	Message
11509	Informational	Console (%1): Properties set for the VTL Server.
11510	Error	Console (%1): Failed to save report -- %2.
11511	Error	Console (%1): Failed to get the information for the NIC.
11512	Error	"Console (%1): Failed to add a replica for virtual tape %2 to VTL Server %3 (watermark: %4 MB, time: %5, interval: %6, watermark retry: %7, suspended: %8)."
11513	Informational	"Console (%1): Replica for virtual tape %2 was added to VTL Server %3 (watermark: %4 MB, time: %5, interval: %6, watermark retry: %7, suspended: %8)."
11514	Error	"Console (%1): Failed to remove the replica for virtual tape %2 from VTL Server %3 (watermark: %4 MB, time: %5, interval: %6, watermark retry: %7, suspended: %8)."
11515	Informational	"Console (%1): Replica for virtual tape %2 was removed from VTL Server %3 (watermark: %4 MB, time: %5, interval: %6, watermark retry: %7, suspended: %8)."
11516	Error	Console (%1): Failed to create the virtual tape replica %2.
11517	Informational	Console (%1): Virtual tape replica %2 was created.
11518	Error	Console (%1): Failed to start replication for virtual tape %2.
11519	Informational	Console (%1): Replication for virtual tape %2 started.
11520	Error	Console (%1): Failed to stop replication for virtual tape %2.
11521	Informational	Console (%1): Replication for virtual tape %2 stopped.
11522	Error	Console (%1): Failed to promote virtual tape replica %2 to a virtual tape.
11523	Informational	Console (%1): Virtual tape replica %2 promoted to a virtual tape.
11524	Error	Console (%1): Failed to run VTL Server X-Ray.
11525	Informational	Console (%1): VTL Server X-Ray has been run.
11530	Error	Console (%1): Failed to back up configuration files.
11531	Informational	Console (%1): Backed up Configuration files successfully.
11532	Error	Console (%1): Failed to restore configuration files.
11533	Informational	Console (%1): Restored VTL configuration files successfully.
11534	Error	Console (%1): Failed to reset the umap for virtual device %2.
11535	Error	"Console (%1): Failed to update the replication parameters for virtual tape %2 to VTL Server %3 (watermark: %4 MB, time: %5, interval: %6, watermark retry: %7, suspended: %8)."
11536	Informational	"Console (%1): Replication parameters for virtual tape %2 to VTL Server %3 updated (watermark: %4 MB, time: %5, interval: %6, watermark retry: %7, suspended: %8)."
11537	Error	Console (%1): Failed to claim physical device %2.
11538	Informational	Console (%1): Physical device %2 has been claimed.

Trap	Severity	Message
11539	Error	Console (%1): Failed to import physical device %2.
11540	Error	"Console (%1): Host name mismatch (old: %2, new: %3)."
11541	Error	Console (%1): Failed to save event message (ID: %2).
11542	Error	Console (%1): Failed to remove virtual tape replica %2.
11543	Informational	Console (%1): Virtual tape replica %2 removed.
11544	Error	Console (%1): Failed to modify virtual tape replica %2.
11545	Informational	Console (%1): Virtual tape replica %2 modified.
11546	Error	Console (%1): Failed to mark the replication for virtual tape %2.
11547	Informational	Console (%1): Replication for virtual tape %2 is marked in sync.
11548	Error	Console (%1): Failed to determine if data was written to virtual device %2.
11549	Error	"Console (%1): Failed to set option ""%2 %3."""
11550	Informational	"Console (%1): Option ""%2 %3"" set."
11553	Error	Console (%1): Failed to get login user list.
11554	Error	Console (%1): Failed to set failover option <selfCheckInterval: %d sec>.
11555	Informational	Console (%1): Failover option <self check interval: %2 sec> has been set.
11560	Error	Console (%1): Failed to get licenses.
11561	Error	Console (%1): Failed to add license %2.
11562	Informational	Console (%1): License %2 added.
11563	Error	Console (%1): Failed to remove license %2.
11564	Informational	Console (%1): License %2 removed.
11565	Error	Console (%1): Failed to check licenses -- option mask %2.
11566	Error	"Console (%1): License conflict -- Number of CPU's available: %2, number of CPU's used: %3."
11567	Error	Console (%1): Failed to clean up failover server directory %2.
11568	Error	Console (%1): Failed to set (%2) I/O Core for failover -- Failed to create failover configuration.
11569	Error	Console (%1): Failed to set %2 to Fibre Channel mode %3.
11570	Informational	Console (%1): Set %2 to Fibre Channel mode %3.
11571	Error	Console (%1): Failed to assign Fibre Channel device %2 to %3 (rolled back).
11572	Error	Console (%1): Failed to assign Fibre Channel device %2 to %3 (not rolled back).
11573	Informational	Console (%1): Fibre Channel device %2 assigned to %3.
11574	Error	Console (%1): Failed to unassign Fibre Channel device %2 from %3 (rolled back) and returns %4.

Trap	Severity	Message
11575	Error	Console (%1): Failed to unassign Fibre Channel device %2 from %3 (not rolled back) and returns %4.
11576	Informational	Console (%1): Fibre Channel device %2 unassigned from %3.
11577	Error	Console (%1): Failed to get Fibre Channel target information.
11578	Error	Console (%1): Failed to get Fibre Channel initiator information.
11579	Error	Console (%1): Failed to set %2 to Fibre Channel authentication mode %3.
11580	Informational	Console (%1): Set %2 Fibre Channel Properties.
11583	Informational	Console (%1): Failed to update Fibre Channel client (%2) WWPNs.
11584	Informational	Console (%1): Fibre Channel client (%2) WWPNs updated.
11585	Error	Console (%1): Failed to set Fibre Channel option %2.
11586	Informational	Console (%1): Set Fibre Channel option to %2.
11587	Error	Console (%1): Failed to demote virtual device %2 to a replica.
11588	Informational	Console (%1): Virtual device %2 demoted to a replica.
11589	Error	Authentication failed to connect to client %1 and returned %2.
11592	Error	Console (%1): Failed to sync replication status for virtual tape %2 to the new target server.
11594	Error	Console (%1): Failed to set CallHome option %2.
11595	Informational	Console (%1): Set CallHome option to %2.
11596	Error	Console (%1): Failed to set hostedbackup option %2.
11597	Informational	Console (%1): Set hostedbackup option to %2.
11598	Informational	Console (%1): Failed to set hostedbackup option %2 because of conflicting adapter number %3.
11599	Informational	Console (%1): Set ndmp option to %2.
11616	Informational	Console (%1): Replication schedule for virtual tape %2 id %3 suspended.
11617	Informational	Console (%1): Replication schedule for virtual tape %2 id %3 resumed.
11632	Error	"Console (%1): Failed to set failover option on secondary server <heartbeatInterval: %2 sec, autoRecoveryInterval: %3 sec>."
11633	Error	"Console (%1): Failed to set failover option on secondary server <heartbeatInterval: %2 sec, autoRecoveryInterval: disabled>."
11634	Informational	"Console (%1): Failover option on secondary server <heartbeatInterval: %2 sec, autoRecoveryInterval: %3 sec> has been set."
11635	Informational	"Console (%1): Failover option on secondary server <heartbeatInterval: %2 sec, autoRecoveryInterval: disabled> has been set."
11648	Error	Failed to get inquiry string on SCSI device %1.
11649	Error	Failed to convert inquiry string on SCSI device %1.
11650	Error	Failed to get capacity size for SCSI device %1.

Trap	Severity	Message
11651	Error	Medium Test failed for SCSI device %1.
11652	Error	"Could not get type for SCSI device %1, because of inquiry string failure."
11653	Error	"Discarded scsi device %1, unsupported type ""%2""."
11654	Error	"Discarded scsi device %1, missing MTI vendor in inquiry string."
11655	Error	"Discarded scsi device %1, bad capacity size."
11656	Error	"Discarded scsi device %1, unsupported Cabinet ID."
11657	Error	"Discarded scsi device %1, missing ""%2"" vendor in inquiry string."
11664	Informational	Console (%1): Enable backup for virtual device %2.
11666	Informational	Console (%1): Disable backup for virtual device %2.
11669	Informational	Console (%1): Stopped active backup sessions for virtual device %2.
11674	Informational	Console (%1): Virtual tape %2 is in replication session.
11675	Informational	Console (%1): Virtual device %2 is in backup session.
11680	Informational	Console (%1): Cache resource %2 (ID: %3) resumed successfully.
11682	Informational	Console (%1): Cache resource %2 (ID: %3) suspended successfully.
11685	Informational	Console (%1): %2 Resource %3 (ID: %4) added successfully.
11687	Informational	Console (%1): %2 Resource %3 (ID: %4) deleted successfully.
11689	Informational	Console (%1): resource %2 (ID: %3) resumed successfully.
11691	Informational	Console (%1): resource %2 (ID: %3) suspended successfully.
11693	Error	Console (%1): policy for resource %2 (ID: %3) updated successfully.
11694	Error	Console (%1): Failed to update policy for resource %2 (ID: %3).
11695	Error	Console (%1): Failed to get statistic information.
11696	Error	Console (%1): Failed to get status.
11699	Error	Console (%1): Failed to get port mapping for adapter no %2 persistent binding.
11702	Informational	VirtualTape Library Emulation option was enabled successfully.
11703	Informational	VirtualTape Library Emulation option was disabled successfully.
11704	Error	Console (%1): The configuration file update for %2 %3(s) was rolled back.
11705	Error	Console (%1): The disk partition update for %2 %3(s) was rolled back.
11706	Error	Console (%1): The device creation for %2 %3(s) was rolled back.
11707	Error	Console (%1): Failed to create %2 %3(s). Error: %4.
11708	Informational	Console (%1): %2 %3(s) created successfully.
11709	Error	Console (%1): The configuration file update for replication setup for %2 %3(s) was rolled back.
11710	Error	Console (%1): The disk partition update for replication setup for %2 %3(s) was rolled back.

Trap	Severity	Message
11711	Error	Console (%1): The replication setup for %2 %3(s) was rolled back.
11712	Error	Console (%1): Failed to configure replication for %2 %3(s). Error: %4.
11713	Informational	Console (%1): Replication for %2 %3(s) configured successfully.
11714	Error	Console (%1): The configuration file update for replication removal for %2 %3(s) was rolled back.
11715	Error	Console (%1): The disk partition update for replication removal for %2 %3(s) was rolled back.
11716	Error	Console (%1): The replication removal for %2 %3(s) was rolled back.
11717	Error	Console (%1): Failed to remove replication for %2 %3(s). Error: %4.
11718	Informational	Console (%1): Replication for %2 %3(s) removed successfully.
11719	Error	Console (%1): The configuration file update for deleting %2 %3(s) was rolled back.
11720	Error	Console (%1): The disk partition update for deleting %2 %3(s) was rolled back.
11721	Error	Console (%1): The deletion of %2 %3(s) was rolled back.
11722	Error	Console (%1): Failed to delete %2 %3(s). Error: %4.
11723	Informational	Console (%1): %2 %3(s) are deleted successfully.
11724	Error	Console (%1): The configuration file update for promoting %2 %3(s) was rolled back.
11725	Error	Console (%1): The disk partition update for promoting %2 %3(s) was rolled back.
11726	Error	Console (%1): The promotion of %2 %3(s) was rolled back.
11727	Error	Console (%1): Failed to promote %2 %3(s). Error: %4.
11728	Informational	Console (%1): %2 %3(s) are promoted successfully.
11729	Error	Console (%1): Failed to update replication properties for %2 %3(s). Error: %4.
11730	Informational	Console (%1): Replication properties for %2 %3(s) are updated successfully.
11731	Error	Console (%1): Failed to update replica properties for %2 %3(s). Error: %4.
11732	Informational	Console (%1): Replica properties for %2 %3(s) are updated successfully.
11733	Informational	Console (%1): Virtual library %2 created successfully.
11734	Error	Console (%1): The configuration file update for virtual library creation was rolled back.
11735	Error	Console (%1): Adding virtual library to the system was rolled back.
11736	Error	Console (%1): Failed to create virtual library. Error: %2.
11737	Informational	Console (%1): %2 virtual tape drives created successfully.
11738	Error	Console (%1): The configuration file update for virtual drive creation was rolled back.
11739	Error	Console (%1): Adding virtual tape drives to the system was rolled back.

Trap	Severity	Message
11740	Error	Console (%1): Failed to create virtual tape drives. Error: %2.
11750	Informational	Console (%1): Add VirtualTape Library Emulation option successfully.
11751	Informational	Console (%1): Remove VirtualTape Library Emulation option successfully.
11780	Informational	Tape id %1 [%2] is enabled with auto-replication move mode and will be deleted in %3 at about %4.
11781	Informational	The scheduled deletion for virtual tape id %1 is cancelled.
11782	Error	Barcode [%1] of the source tape id %2 already exist on target server %3. Auto-replication cannot be configured.
11783	Error	Failed to setup auto-replication for tape id %1 on target server %2. Error: %3.
11788	Error	Appliance Hardware Problem: %1.
11791	Error	Failed to re-size virtual tape %1 to %2 MB. Error: %3.
11792	Informational	Virtual tape %1 is resized to %2 MB successfully.
11793	Warning	Appliance Hardware Problem: %1.
11794	Informational	FC client %1 VSA mode is changed from %2 to %3.
11795	Informational	FC client %1 celerra mode is changed from %2 to %3.
11900	Error	Failed to import report request.
11901	Error	Failed to parse report request %1 %2.
11902	Error	Undefined report type %1.
11903	Error	Failed to allocate memory.
11904	Error	Failed to create directory %1.
11905	Informational	Directory %1 created.
11906	Error	Failed to open file %1.
11907	Error	Failed to write file %1.
11908	Warning	File %1 does not exist.
11909	Error	Failed to parse log file %1 %2.
11910	Error	Failed to create report file %2 (type %1).
11911	Informational	Report file %2 (type %1) created.
11912	Informational	%1 property set for the VTL server.
12000	Informational	VTL logger started.
12001	Error	VTL logger stopped.
12002	Error	Failed to open directory %1.
12003	Error	Failed to open file %1.
12004	Error	Failed to create directory %1.

Trap	Severity	Message
12005	Error	Failed to allocate memory.
12006	Warning	Log size warning.
12007	Error	Failed to delete file %1.
12008	Error	Wrong file format %1.
12009	Error	Missing parameter %1.
12010	Error	Invalid parameter %1.
12011	Error	Wrong status for file %1.
13000	Informational	"VTL Failover Module started -- [Primary %1, IP %3, Heartbeat %4][Secondary %2](HBInterval %5)(AutoRecovery %6)"
13001	Informational	The VTL Console has requested that this server take over for the primary server.
13002	Informational	Transferring primary static configuration to secondary.
13003	Informational	Transferring primary dynamic configuration to secondary.
13004	Informational	Transferring primary credential information to secondary.
13005	Informational	Taking over tasks for the primary server.
13006	Informational	The primary VTL Server is recovering.
13007	Informational	Restoring this server to its original configuration.
13008	Informational	VTL Failover Module stopped.
13009	Informational	Synchronizing the VTL configuration with the primary server.
13100	Error	fail to retrieve primary's heartbeat information.
13101	Error	Failed to communicate with primary. Error: %1
13102	Error	Failed to run %1.
13103	Informational	The system times of the failover pair differ by more than %1 second(s).
13300	Error	Failed to authenticate to the primary server -- Failover Module stopped.
13301	Error	Failed to authenticate to the local server -- Failover Module stopped.
13302	Error	Failed to transfer primary static configuration to secondary.
13303	Error	Failed to transfer primary dynamic configuration to secondary.
13304	Error	Failed to rename file %1.
13305	Error	Failed to write to file %1.
13306	Error	Failed to open file %1.
13307	Error	Failed to transfer primary credential information to secondary.
13308	Error	Invalid failover configuration detected. Failover will not occur.
13309	Error	Primary server failed to respond command from secondary. Error: %1.
13310	Error	Failed to copy from %1 to %2.

Trap	Severity	Message
13311	Error	Failed to merge static configuration for the primary server.
13312	Error	Failed to merge dynamic configuration for the primary server.
13313	Error	Out of memory -- %1.
13314	Error	Failed to read from file %1.
13315	Error	Failed to merge authentication information for the primary server.
13316	Error	Fail to add virtual IP address. Error: %1.
13317	Error	Fail to release virtual IP address. Error: %1.
13318	Error	Failed to restore authentication information for this server.
13319	Error	Fail to stop VTL failover module. Host may need to reboot.
13320	Error	Failed to update the configuration files to the primary server -- %1.
13500	Informational	VTL Self-Monitor Module started -- (%1)(%2)
13501	Informational	all VTL related processes and resources function normally
13502	Informational	Take back the virtual IP address: %1.
13503	Warning	No heartbeat request detected for %1 seconds.
13504	Informational	Stopping Self-Monitor module.
13600	Informational	Releasing virtual IP address: %1.
13700	Error	Failed to allocate memory -- Self-Monitor Module stopped.
13701	Error	Failed to release virtual IP address. Error: %1. Retrying the operation.
13702	Error	Failed to add virtual IP address: %1. Retrying the operation.
13703	Error	Failed to stop VTL Self-Monitor Module.
13704	Error	VTL module failure detected. Condition: %1.
13710	Warning	"The Live Trial period has expired for VTL Server %1. Please contact Sun Microsystems, Inc. or its representative to purchase a license."
13711	Warning	"The following options are not licensed: %1. Please contact Sun Microsystems, Inc. or its representative to purchase a license."
13800	Critical	Primary server failure detected. Failure condition: %1
13801	Informational	Secondary server will take over primary server operation.
13802	Informational	Manual failover initiated.
13803	Informational	Primary acknowledged takeover request. Resources are released.
13804	Informational	Quorum disk failed to release to secondary.
13805	Informational	Virtual drives released successfully.
13808	Informational	IP address released successfully.
13809	Informational	Failover completed successfully.
13810	Informational	Primary server restored. Waiting for failback.

Trap	Severity	Message
13811	Informational	Primary server failback initiated.
13812	Informational	Server IP address add successfully.
13814	Informational	Quorum disk returned to primary.
13815	Informational	Virtual drives added successfully.
13816	Informational	Primary server restored.
13817	Critical	Primary server failback was unsuccessful. Failed to update the primary configuration.
13818	Error	Quorum disk negotiation failed.
13820	Warning	Failed to detect primary server heartbeat.
13821	Error	Failed to contact other entities in network. Assume failure in secondary side. Failover not initiated.
13822	Warning	Secondary will not take over because storage connectivity is not 100%.
13823	Warning	Primary failed to acknowledge takeover request in time. Secondary will take over forcefully.
13824	Informational	Environment variable ISFCFORPCTO set to %1
13825	Informational	Environment variable ISFOQUORUMREQ set to %1
13826	Informational	Environment variable ISFOQUORUMCON set to %1
13827	Error	Fail to stop quorum updating process. PID: %1. Maybe due to storage device or connection failure.
13828	Informational	"Almost running out of file handlers (current %1, max %2)"
13829	Informational	"Almost running out of memory (current %1 K, max %2 K)"
13830	Error	Get configuration file from storage failed.
13831	Informational	Get configuration file from storage successful.
13832	Error	"Primary server operation is resumed either by user initiated action, or secondary server is suspended.."
13833	Error	Failed to backup file from %1 to %2.
13834	Error	Failed to copy file out from Quorum repository.
13835	Error	Failed to take over primary.
13836	Error	Failed to get configuration files from repository. Check and correct the configuration disk.
13837	Informational	Configuration files retrieved from repository successfully.
13838	Informational	Successfully copy file out from Quorum repository.
13839	Informational	Secondary server initiated failback to primary (%1) .
13840	Informational	Secondary server will take over (%1).
13841	Error	Secondary server does not match primary server status (%1).
13842	Warning	Secondary server will takeover. Primary is still down.

Trap	Severity	Message
13843	Error	Secondary server fail to get original conf file from repository before failback .
13844	Error	Failed to write %1 to repository.
13845	Warning	Quorum disk failure detected. Secondary is still in takeover mode.
13846	Informational	Force takeover is initiated. Secondary will perform SCSI reserve to lock the storage.
13847	Informational	Secondary server is performing SCSI release to storage.
13848	Warning	Primary is already shut down. Secondary will take over immediately.
13849	Warning	One of the heartbeat channels is down: IP address: %1.
13850	Error	"Secondary server can not locate quorum disk. Either the configuration is wrong, or the drive is offline."
13851	Error	Secondary server can't take over due to %1
13852	Informational	Secondary server is being requested to release its own resources during takeover %1
13853	Informational	Secondary notified primary to go up because secondary is unable to take over.
13854	Informational	Secondary suspended failover for %1 min.
13855	Informational	Secondary resumed failover.
13860	Error	failed to merge configuration file %1 %2.
13861	Error	failed to rename file from %1 to %2.
13862	Error	failed to write file %1 to repository
13863	Critical	Primary server is commanded to resume. %1
13864	Critical	Primary server operation will terminate. %1
13865	Informational	Primary server will resume due to user initiated action.
13866	Error	Failed to remove schedule
13867	Informational	Primary server is resuming and forcing device reset to clear SCSI reservation
13868	Informational	Secondary server takeover unilaterally. All resources will be released. Primary server reboot is required for recovery.
13869	Informational	Removing schedule %1 for failover process clean-up.
13870	Informational	Schedule removal completed
13871	Informational	Primary server failure condition still exists: %1
13872	Informational	Waiting for primary to acknowledge takeover request. May take approx. %1 sec.
13873	Informational	Waiting for primary to release resources. May take approx. %1 sec.
13875	Informational	Primary server is starting to activate virtual drives.
13876	Informational	Primary server has completed activating virtual drives.
13877	Informational	Secondary server failed to take over.

Trap	Severity	Message
13878	Error	Primary server has invalid failover configuration.
13879	Critical	Secondary server detect kernel module failure, reboot machine may need.
15050	Error	Server ioctl call %1 failed on vdev id %2: Invalid Argument (EINVAL).
15051	Error	Server ioctl call %1 failed on vdev id %2: I/O error (EIO).
15052	Error	Server ioctl call %1 failed on vdev id %2: Not enough memory space (ENOMEM).
15053	Error	Server ioctl call %1 failed on vdev id %2: No space left on device (ENOSPC).
15054	Error	Server ioctl call %1 failed on vdev id %2: Already existed (EEXIST).
15055	Error	Server ioctl call %1 failed on vdev id %2: Device or resource is busy (EBUSY).
16001	Error	Console(%1): Converting file system failed: %2.
17001	Error	Rescan replica cannot proceed due to replication already in progress.
17002	Error	Rescan replica cannot proceed due to replication control area missing.
17003	Error	Rescan replica cannot proceed due to replication control area failure.
17004	Error	Replication cannot proceed due to replication control area failure.
17005	Error	Replication cannot proceed due to replication control area failure.
17006	Error	Rescan replica cannot proceed due to replication control area failure.
17007	Error	Rescan replica failed.
17008	Error	Replication failed.
17009	Error	Failed to start replica rescan.
17010	Error	Failed to start replication.
17011	Error	Rescan replica failed due to network transport error.
17012	Error	Replicating replica failed due to network transport error.
17013	Error	Rescan replica failed due to local disk error.
17014	Error	Replication failed due to local disk error.
17017	Error	Rescan replica failed due to replica failed with error.
17018	Error	Replication failed due to replica failed with error.
17019	Error	Replication control area exchange failed with error.
17020	Error	Replication failed with error.
19000	Informational	"The replication configuration has been created successfully. Primary Server: %1, Virtual Tape: %2, Target Server: %3, Virtual Tape Replica: %4."
19001	Informational	"The failover configuration has been created successfully. Primary Server: %1, Secondary Server: %2"
19004	Warning	"The allocated space at %1MB has reached the threshold, %2% of the total capacity(%3MB)."
19050	Informational	"[Remote Copy] The configuration for remote copy has been set up successfully. Server: %1, Virtual Tape: %2, Remote Server: %3, Tape Replica: %4."

Trap	Severity	Message
19051	Informational	[Remote Copy] The copying of the virtual tape %1 to the remote server has been started.
19052	Informational	[Remote Copy] The copying of the virtual tape %1 to the remote server has finished.
19053	Informational	"[Remote Copy] The configuration for remote copy is removed. Server: %1, Virtual Tape: %2, Remote Server: %3, Tape Replica: %4."
19054	Informational	[Remote Copy] The replica of the virtual tape %1 has been moved to the virtual library %2 on the remote server successfully.
19055	Informational	"[Remote Copy] The virtual tape has been copied to the remote server successfully. Server: %1, Virtual Tape: %2, Remote Server: %3, Tape Replica: %4."
19056	Error	"[Remote Copy] The copying of the virtual tape to the remote server has failed while %1. Error: %2. (Server: %3, Virtual Tape: %4, Remote Server: %5, Tape Replica: %6)"
19057	Error	[Remote Copy] The copying of the virtual tape to the remote server cannot proceed -- unable to connect to remote server %1.
19058	Error	[Remote Copy] The copying of the virtual tape to the remote server cannot proceed -- virtual tape %1 no longer has a replica or the replica does not exist.
19059	Error	[Remote Copy] The copying of the virtual tape to the remote server cannot proceed -- virtual tape %1 no longer has a replica or the replica does not exist.
19060	Error	[Remote Copy] The copying of the virtual tape to the remote server cannot proceed -- unable to open configuration file.
19061	Error	[Remote Copy] The copying of the virtual tape to the remote server cannot proceed -- unable to allocate memory.
19062	Error	[Remote Copy] The copying of the virtual tape to the remote server cannot proceed -- unexpected error %1.
19063	Error	[Remote Copy] The copying of the virtual tape %1 to the remote server has been manually aborted by user
19064	Error	[Remote Copy] The copying of the virtual tape to the remote server cannot proceed -- failed to load the virtual tape %1.
19065	Error	[Remote Copy] The copying of the virtual tape to the remote server cannot proceed -- virtual tape %1 is in the drive.
19066	Error	[Remote Copy] The copying of the virtual tape to the remote server cannot proceed -- failed to set initialization status in VirtualLibrary System for virtual tape %1.
19200	Error	Console (%1): Failed to get the key list.
19201	Error	Console (%1): Failed to get the key.
19202	Error	Console (%1): Failed to create key %2.
19203	Informational	Console (%1): Key %2 has been created successfully.

Trap	Severity	Message
19204	Error	Console (%1): Failed to delete Key %2.
19205	Informational	Console (%1): Key %2 has been deleted successfully.
19206	Error	Console (%1): Failed to update information for key %2.
19207	Informational	Console (%1): Information for key %2 has been updated successfully.
19208	Error	Console (%1): Failed to create key package %2.
19209	Informational	Console (%1): Key package %2 has been created successfully.
19210	Error	Console (%1): Failed to get key package information.
19211	Error	Console (%1): Failed to save keys from key package.
19212	Informational	Console (%1): %2 keys from key package have been saved successfully.
20000	Informational	SAN/IP driver started.
20001	Informational	SAN/IP driver stopped.
20002	Error	SAN/IP driver failed to initialize.
21000	Informational	SAN SCSI driver started.
21001	Informational	SAN SCSI driver stopped.
21002	Error	SAN SCSI driver failed to initialize.
21010	Warning	SAN SCSI received an abort request.
21011	Warning	SAN SCSI received a reset bus request for a special command.
21012	Warning	SAN SCSI received a reset bus request.
21013	Warning	SAN SCSI failed to send a SCSI command.
21014	Warning	SAN SCSI failed to receive a SCSI reply.
21015	Warning	SAN SCSI failed to attach to a virtual device.
21016	Warning	SAN SCSI failed to detach from a virtual device.
21017	Warning	SAN SCSI failed to connect to a VTL Server.
21018	Warning	"SAN SCSI received a disconnect request. This may be from the Client Monitor or due to a network failure, VTL Server shutdown/failover, or a change in a virtual device."
21019	Warning	SAN SCSI received an unsupported request.
22000	Informational	Fibre Channel Authentication started with %1.
22001	Error	"Fibre Channel Authentication error %1, at %2."
22002	Informational	Fibre Channel Authentication stopped with %1.
22003	Warning	Fibre Channel Authentication warning from system %1.
22004	Error	Fibre Channel Authentication error. Client Name does not match on Server %1.
22005	Error	Fibre Channel Authentication error. Signature does not match on Server %1.
25000	Informational	%1 started.

Trap	Severity	Message
25001	Error	%1 failed to start -- %2.
25002	Informational	%1 paused.
25003	Error	%1 failed to pause -- %2.
25004	Informational	%1 resumed.
25005	Error	%1 failed to resume -- %2.
25006	Informational	%1 stopped.
25007	Error	%1 failed to stop -- %2.
25008	Informational	%1 shutdown.
25009	Informational	%1 starting.
25010	Informational	%1 stopping.
25011	Error	Failed to open service manager -- %1.
25012	Error	Failed to open service -- %1.
26000	Error	Failed to create TCP socket.
26001	Error	Failed to bind TCP socket.
26002	Error	Failed to create TCP service.
26003	Error	Failed to create TCP thread.
26100	Error	Failed to access the %1 driver -- %2.
26101	Error	The SAN SCSI driver is the wrong version for this VTL SAN Client. Driver version %1 will not work with client version %2.
26102	Error	Failed to open the %1 driver -- %2.
26103	Error	Failed to start the %1 driver.
26104	Error	Failed to stop the %1 driver.
26105	Error	SAN SCSI cannot connect to VTL Server %1 -- %2.
26106	Error	SAN SCSI cannot attach to VTL SAN device %1/%2 -- %3.
26107	Error	SAN SCSI cannot detach from VTL SAN device %1/%2 -- %3.
26108	Error	SAN SCSI cannot disconnect from VTL Server %1 -- %2.
26110	Error	Failed to rescan SCSI port %1 -- %2.
26200	Error	Failed to access '%1' -- %2.
26201	Error	Failed to read the drive layout for '%1' -- %2.
26202	Error	Failed to assign drive %1 to drive letter %2. It is already in use.
26203	Error	Failed to access drive %1 -- %2.
26204	Error	Failed to dismount drive %1 -- %2.
26205	Error	Failed to lock drive %1 -- %2.
26206	Error	Failed to unlock drive %1 -- %2.

Trap	Severity	Message
26207	Error	Failed to define device %1 -- %2.
26208	Error	Failed to undefine device %1 -- %2.
26209	Error	Drive %1 is busy and cannot be detached. The SAN Client cannot stop at this time.
26210	Informational	Both %1 and %2 have the same disk signature (%3).
27000	Error	Failed to connect to VTL Server '%1' -- %2.
27001	Error	Failed to get the version of VTL Server '%1' -- %2.
27002	Error	Failed to get the information for VTL Server '%1' -- %2.
27003	Error	Failed to get the number of adapters for VTL Server '%1' -- %2.
27004	Error	Failed to get the information for VTL Server '%1' adapter %3 -- %2.
27005	Error	Failed to get the number of devices for VTL Server '%1' -- %2.
27006	Error	Failed to get the information for VTL Server '%1' device %3 -- %2.
27007	Error	Failed to get the list of IP addresses for VTL Server '%1' -- %2.
27008	Error	Failed to get the media information for VTL Server '%1' device %3 -- %2.
28001	Error	Failed to add VTL Server '%1' -- %2.
28002	Error	Failed to add VTL Server '%1' adapter %2 -- %3.
28003	Error	Failed to add VTL Server '%1' adapter %2 channel %3 -- %4.
28004	Error	Failed to add VTL Server '%1' device %2 -- %3.
28005	Error	Failed to add VTL Server '%1' device %2 volume %3 -- %4.
29101	Informational	VTL Server '%1' failed over.
29102	Informational	VTL Server '%1' recovered from failover.
29401	Informational	Backing up VTL Server '%1' device %2.
29402	Informational	Backed up VTL Server '%1' device %2.
29403	Warning	Backup of VTL Server '%1' device %2 failed.
29404	Warning	"VTL Notify user specified error %1, description '%2'."
29405	Error	"Notify Timeout error, waiting on %1, timeout set to %2."
29406	Warning	Notify Error waiting on %1.
40000	Informational	TLE Module Started
40001	Informational	TLE Module Stopped
40002	Error	Block list full on Drive %1
40003	Error	"Corrupt Repository, Rep VID %1"
40004	Error	Unsupported device [%1][%2][%3]
40005	Error	"Load Drive failed. Lib %1, Drive %2"
40006	Error	"TDE get drive info failed, Drive %1, EC %2"

Trap	Severity	Message
40007	Error	"Unload tape from drive failed, Drive %1, EC %2"
40008	Error	Failed to create new tape in Virtual Library %1
40009	Error	"HW Error with Move Medium command, Lib %1, SrcEle %2 DestEle %3"
40010	Error	Attach to tape %1 failed
40011	Error	"Failed to read from Virtual Tape. Tape VID %1, EC %2"
40012	Informational	Unsupported SCSI command %1
40013	Error	"Export Tape failed, not enough memory. Job id %1"
40014	Error	"Read tape info failed. Tape VID %1, EC %2"
40015	Error	"Export tape failed, unsupported block size %1"
40016	Error	"Failed to write to Virtual Tape. Tape VID %1, EC %2"
40017	Error	"Failed to write to Physical Tape. Drive VID %1, EC %2"
40018	Error	"Failed to load Physical Tape. Lib VID %1, Drive VID %2, BC %3"
40019	Error	"Failed to write to Virtual Tape. Tape VID %1, EC %2"
40020	Warning	Job %1 cancelled
40021	Error	Failed to locate Virtual Library %1
40022	Error	"Failed to get Physical Tape block size. Drive VID %1, EC %2"
40023	Error	"Import failed, not enough memory %1"
40024	Informational	"Import job %1 completed successfully, VLib VID %2, VLib slot %3, DestTape [%4] SrcTape [%5] Throughput %6 MB/min"
40025	Informational	"Export job %1 completed successfully. SrcTape [%2], DestTape [%3] Throughput %4 MB/min"
40026	Informational	"Export Job %1 submitted to Physical Library %2. SrcTape [%3], DestSlot [%4], %5"
40027	Informational	"Direct Access Import completed successfully. VLib VID %1, Physical Drive VID %2, Slot %3, DestTape [%4], %5"
40028	Informational	"Import job submitted. Job id %1, VLib VID %2, Slot %3, DestTape [%4], %5"
40029	Error	Not enough memory to complete the operation
40030	Error	"Failed to read from repository. Rep VID %1, EC %2"
40031	Error	"Failed to write to repository. Rep VID %1, EC %2"
40032	Warning	Physical Tape %1 not available to start auto archive job. Waiting for tape...
40033	Informational	Export job %1 active. Tape Drive used %2
40034	Informational	Import job %1 active. Tape drive used %2
40035	Informational	Successfully attached to repository %1
40036	Error	Failed to attach to repository %1
40037	Informational	"Physical Library assigned to exclusive use for TLE. Vid %1, [%2][%3]"

Trap	Severity	Message
40038	Informational	"Physical Library unassigned. Vid %1, [%2][%3]"
40039	Error	Read Element command to Physical Library %1 failed. EC %2
40040	Error	Attach to device %1 failed. EC %2
40041	Informational	"Physical Tape Drive assigned to exclusive use for VTL. VID %1, [%2][%3]"
40042	Informational	"Physical Tape Drive unassigned. Vid %1, [%2][%3]"
40043	Error	"Move Medium command failed in Physical Library %1. SrcEle %2, DestEle %3, EC %4"
40044	Error	Unload command failed on Physical Tape Drive %1. EC %2
40045	Error	Read from Physical Tape Drive %1 failed. EC %2
40046	Error	Write to Physical Tape Drive %1 failed. EC %2
40047	Error	Write FM to Physical Tape Drive %1 failed. EC %2
40048	Error	"Mode sense command to Physical device %1 failed. Pagecode %2, EC %3"
40049	Error	Mode select command to Physical device %1 failed. EC %2
40050	Error	Rewind command to Physical Tape Drive %1 failed. EC %2
40051	Error	Inquiry command to Physical device %1 failed. EC %2
40052	Informational	Inventory of Physical Library %1 completed successfully
40053	Informational	Virtual Library %1 initialized. [%2][%3]
40054	Informational	Virtual Tape Drive %1 initialized. [%2][%3]
40055	Informational	Virtual Tape Drive %1 deleted from Virtual Library %2
40056	Informational	Virtual Tape Drive %1 created successfully in Virtual Library %2
40057	Informational	Virtual Library %1 created successfully. [%2][%3]
40058	Informational	Virtual Library %1 deleted successfully. [%2][%3]
40059	Informational	"Virtual Tape added to Virtual Library %1, slot %2. Total Tapes in Library %3. %4 %5"
40060	Informational	Stand alone Virtual Tape Drive %1 created successfully. [%2][%3]
40061	Informational	Stand alone Virtual Tape Drive %1 deleted. [%2][%3]
40062	Informational	Virtual Tape %1 moved to vault from device %2
40063	Informational	Virtual Tape %1 from vault imported to Virtual Library %2 slot %3
40064	Informational	Virtual Tape %1 from vault imported to Virtual Tape Drive %2
40065	Error	"Read data from Virtual Tape failed. Attach handle %1, EC %2"
40066	Error	"Write data to Virtual Tape failed. Attach handle %1, EC %2"
40067	Error	Failed to add Physical Drive %1 to repository %2. EC %3
40068	Error	Cannot create new Tape. EC %1
40069	Error	Cannot expand Tape %1. EC %2

Trap	Severity	Message
40070	Error	Cannot delete Tape %1
40071	Error	"Cannot import Tape, dest slot %1 in Virtual Library %2 is full"
40072	Informational	"Properties of Tape %1 has been changed. Barcode %2, MaxCapacity %3 MB"
40073	Informational	"Tape Created in Stand Alone Virtual Tape Drive. Tape VID %1, Drive VID %2"
40074	Error	"Export to Physical Tape failed. Job ID %1, EC %2, SrcTape [%3] DestTape [%4]"
40075	Informational	"Export Job %1 submitted to Physical stand alone Tape Drive %2, SrcTape [%3], %4"
40076	Error	"Import Physical Tape failed. Job ID %1, EC %2, SrcTape [%3] DestTape [%4]"
40077	Error	Import Physical Tape failed. Duplicate Virtual Tape Barcode. Job ID %1 DestTape [%2]
40078	Error	Import Physical Tape failed. Duplicate Virtual Tape Barcode. Dest Tape [%1]
40079	Informational	"Deleted tape marked for delayed deletion. Tape [%1], VID %2"
40080	Warning	Tape drive %1 in physical library %2 not accessible. Locked by other party
40081	Warning	Tape [%1] in physical library %2 not accessible. Locked by other party
40082	Warning	Slot %1 in physical library %2 not accessible. Locked by other party
40083	Warning	Inventory physical library %1: Tape [%2] or Slot %3 not accessible. Locked by other party
40084	Warning	Tape [%1] is blank. Cannot export blank tapes
40085	Error	Reverse block command failed on physical tape drive VID %1 Error [%2]
40087	Error	Error in retrieving the hostname of this VTL server. Error: %1
40088	Error	Failure in looking up the IP address of the VTL server (%1). Please verify that DNS is configured correctly for both ACSLS and VTL server. Error: %2
40089	Error	Out of system resources. Could'nt fork a process. Error: %1
40090	Error	Failed to execute a program. Error: %1
40091	Error	Failed to open %1. Error: %2
40092	Error	DNS configuration for VTL server is incorrect. DNS or /etc/hosts is returning %1 as the IP of VTL server (%2)
40093	Error	Failed to successfully query %1 server with IP %2. Error received: %3.
40094	Error	Waited %1 seconds to get a response to a query from %2 (%3). Timing out.
40095	Error	Failed to mount %1 on drive %2. Error from %3 (%4): %5.
40096	Error	Waited %1 seconds to get a response from %2 (%3) after trying to mount %4 on drive %5. Timing out.
40097	Error	Failed to dismount %1 from drive %2. Error from %3 (%4): %5.
40098	Error	Waited %1 seconds to get a response from %2 (%3) after trying to dismount %4 from drive %5. Timing out.
40099	Error	Failed to retrieve drive information in ACS %1. Error from %2 (%3): %4.

Trap	Severity	Message
40100	Error	Waited %1 seconds to get a response from %2 (%3) after trying to retrieve drive information in ACS %4. Timing out.
40101	Error	Failed to retrieve volume information in ACS %1 and Pool %2. Error from %3 (%4): %5.
40102	Error	Waited %1 seconds to get a response from ACSLS (%2) after trying to retrieve volume information in ACS %3 and Pool %4. Timing out.
40103	Error	Failed to retrieve LSM information in ACS %1. Error from %2 (%3): %4.
40104	Error	Waited %1 seconds to get a response from %2 (%3) after trying to retrieve LSM information in ACS %4. Timing out.
40105	Error	%1: The number of drives %2 is more than max supported (%3).
40106	Error	%1: The number of volumes %2 is more than max supported (%3).
40107	Informational	%1: Successfully mounted %2 on drive %3
40108	Informational	%1: Successfully dismounted %2 from drive %3
40109	Error	"Log sense command to Physical device %1 failed. Pagecode %2, EC %3"
40110	Error	Failed to retrieve volume information in ACS %1. Error from %2 (%3): %4.
40111	Error	Waited %1 seconds to get a response from Library Station (%2) after trying to retrieve volume information in ACS %3. Timing out.
40112	Warning	Physical Tape %1 not available to start tape caching job. Waiting for tape...
40113	Warning	A Manual Export job is not allowed because tape <%1> has tape caching set.
40114	Warning	The export job is not allowed because physical tape [%1] in library [%2][%3] is being used by tape caching.
40115	Informational	Please add tapes.
40116	Error	Hardware compression failed. EC [%1]
40117	Error	Hardware decompression failed. EC [%1]
40118	Error	Software decompression of a block compressed using hardware failed. EC [%1]
40119	Informational	Global [%1] Compression %2 on Repository %3
40120	Warning	The tape [%1] has no data. No export job will be submitted.
40121	Warning	"The direct link tape VID %1, BarCode [%2] has been deleted."
40122	Informational	"Export Job %1 submitted to Physical Library %2. SrcTape [%3], DestTape [%4], DestSlot [%5], %6"
40123	Error	"Failed to load tape because it is a cleaning tape. Lib VID %1, Drive VID %2, BC %3"
40124	Error	Write command to Configuration Repository Failed. Please check repository LUNs
40125	Informational	Disk space allocated for tape VID %1 Barcode [%2] in library VID %3 has been reclaimed successfully
40126	Error	Failed to reclaim the tape VID %1 Barcode [%2] in library VID %3.

Trap	Severity	Message
40127	Informational	Disk space allocated for tape VID %1 Barcode [%2] in vault has been reclaimed successfully
40128	Error	Failed to reclaim disk space allocated for tape VID %1 Barcode [%2] in vault
40129	Informational	No Free physical drive to load direct link tape VID %1 BarCode [%2].
40130	Warning	Unable to renew cache for tape VID %1. Data will be redirected to physical tape [%2].
40131	Informational	The tape shredding job is successful on the tape [%1].
40132	Informational	The tape shredding job was failed on the tape [%1].
40133	Error	Unable to move tape [%1] to IE slot.
40134	Error	Unable to mount tape [%1] in library [%2] VID %3.
40135	Error	Unable to dismount tape [%1] in library [%2] VID %3.
40136	Error	Space command to Physical Library %1 failed. EC %2.
40137	Error	Failed to add import/export job to the job queue. Maximum of 127 jobs reached. Job ID:%1 Physical tape barcode:[%2].
40138	Informational	The maximum number of slots supported in this library [%1 %2] are %3.
40139	Warning	Door opened condition reported on Physical Library VID-%1 %2 %3.
40140	Informational	Start tape shredding on tape [%1] VID:%2.
40141	Informational	The tape shredding job is cencelled on the tape [%1] VID:%2.
50000	Error	iSCSI: Missing targetName in login normal session from initiator %1
50001	Informational	iSCSI: Login request to target %1 from initiator %2.
50002	Error	iSCSI: Login request to nonexistent target %1 from initiator %2
50003	Error	iSCSI: iSCSI CHAP authentication method rejected. Login request to target %1 from initiator %2

ILOM command reference

The following table summarizes Integrated Lights Out Manager (ILOM) commands you can use to manage the service processor. For more information on ILOM commands, see the *ILOM Administration Guide*.

Description	Command
User Commands	
Add a local user.	`create /SP/users/`*`user1`*` password=`*`password`*` role=administrator|operator`
Delete a local user.	`delete /SP/users/`*`user1`*
Change a local user's properties.	`set /SP/users/`*`user1`*` role=operator`
Display information about all local users.	`show -display [targets|properties|all] -level [value|all] /SP/users`
Display information about LDAP settings.	`show /SP/clients/ldap`
Change LDAP settings.	`set /SP/clients/ldap binddn=`*`proxyuser`*` bindpw=`*`proxyuserpassword`*` defaultrole=administrator|operator ipaddress=`*`ipaddress`*
Network and Serial Port Setting Commands	
Display network configuration information.	`show /SP/network`
Change network properties for the ILOM. Changing certain network properties, like the IP address, disconnects your active session.	`set /SP/network pendingipaddress=`*`ipaddress`*` pendingipdiscovery=dchp|static pendingipgateway=`*`ipgateway`*` pendingipnetmask=`*`ipnetmask`*` commitpending=true`
Display information about the external serial port.	`show /SP/serial/external`
Change the external serial port configuration.	`set /SP/serial/external pendingspeed=`*`integer`*` commitpending=true`
Display information about the serial connection to the host.	`show /SP/serial/host`

Description	Command
Change the host serial port configuration. Note: This speed setting must match the speed setting for serial port 0, COM1 or /dev/ttyS0 on the host operating system.	`set /SP/serial/host pendingspeed=integer commitpending=true`
Alert Commands	
Display information about PET alerts. You can configure up to 15 alerts.	`show /SP/alert/rules/1...15`
Change alert configuration.	`set /SP/alert/rules/1...15 destination=ipaddress level=down|critical|major|minor`
System Management Access Commands	
Display information about HTTP settings.	`show /SP/services/http`
Change HTTP settings, such as enabling automatic redirection to HTTPS.	`set /SP/services/http port=portnumber secureredirect enabled|disabled servicestate=enabled|disabled`
Display information about HTTPS access.	`show /SP/services/https`
Change HTTPS settings.	`set /SP/services/https port=portnumber servicestate=enabled|disabled`
Display SSH DSA key settings.	`show /SP/services/ssh/keys/dsa`
Display SSH RSA key settings.	`show /SP/services/ssh/keys/rsa`
SNMP Commands	
Display information about SNMP settings. By default, the SNMP port is 161 and v3 is enabled.	`show /SP/services/snmp engineid=snmpengineid port=snmpportnumber sets=enabled|disabled v1=enabled|disabled v2c=enabled|disabled v3=enabled|disabled`
Display SNMP users.	`show /SP/services/snmp/users`
Add an SNMP user.	`create /SP/services/snmp/users/snmpusername authenticationpassword=password authenticationprotocol=MD5|SHA permissions=rw|ro privacypassword=password privacyprotocol=none|DES`
Delete an SNMP user.	`delete /SP/services/snmp/users/snmpusername`
Display information about SNMP public (read-only) communities.	`show /SP/services/snmp/communities/public`
Add this device to an SNMP public community.	`create /SP/services/snmp/communities/public/comm1`
Delete this device from an SNMP public community.	`delete /SP/services/snmp/communities/public/comm1`
Display information about SNMP private (read-write) communities.	`show /SP/services/snmp/communities/private`
Add this device to an SNMP private community.	`create /SP/services/snmp/communities/private/comm2`

Description	Command
Host System Commands	
Delete this device from an SNMP private community.	`delete /SP/services/snmp/communities/private/`*`comm2`*
Start the host system.	`start /SYS`
Stop the host system.	`stop /SYS`
Reset the host system.	`reset /SYS`
Start a session to connect to the host console.	`start /SP/console`
Stop the session connected to the host console.	`stop /SP/console`
Clock Settings	
Set the ILOM clock to synchronize with a primary NTP server.	`set /SP/clients/ntp/server/1 address=`*`ntpIPaddress`*
Set the ILOM clock to synchronize with a secondary NTP server.	`set /SP/clients/ntp/server/2 address=`*`ntpIPaddress2`*

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN **Web** sun.com