



Virtual Tape Library

VTL User Guide

Sun Microsystems, Inc.
www.sun.com

Part No. 96267
Feb 2008, Revision E

Submit comments about this document at: g1sfs@sun.com

Copyright 2008 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, AnswerBook2, docs.sun.com, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and in other countries.

AMD Opteron is a trademark or registered trademark of Advanced Microdevices, Inc.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and in other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government Rights—Commercial use. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, Californie 95054, Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. a les droits de propriété intellectuels relatants à la technologie qui est décrit dans ce document. En particulier, et sans la limitation, ces droits de propriété intellectuels peuvent inclure un ou plus des brevets américains énumérés à <http://www.sun.com/patents> et un ou les brevets plus supplémentaires ou les applications de brevet en attente dans les Etats-Unis et dans les autres pays.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, AnswerBook2, docs.sun.com, et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

AMD Opteron est une marque de fabrique ou une marque déposée de Advanced Microdevices, Inc.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licences de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.

Revision History

Short Name	Part Number	Dash	Date	Comments
VTL User Guide	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

Contents

Revision History	iii
Contents	v
About this book	ix
1. Introduction: VTL appliances and enterprise data-protection	1
Features	2
Advantages of VTL tape virtualization	3
Shorter runtimes and reduced dependency on backup windows	4
Shorter run times for non-sequential backup jobs	4
Improved reliability	5
Better utilization of tape subsystems	5
True tape virtualization with dynamically allocated disk space	6
Key VTL features and options	6
NDMP support	7
VTL high-availability option	7
Automated Tape Caching	10
Virtual tape replication	10
VTL Secure Tape encryption option	12

2. Understanding VTL zoning	13
Zoning for standard-availability systems	13
Zoning for high-availability systems	14
3. Using the VTL console	17
Running the VTL console application	18
Populating the console	18
Understanding the VTL console interface	20
Virtual Tape Library System	22
SAN Clients	23
Reports	23
Physical Resources	24
4. VTL operations	25
Managing network connectivity	25
Managing virtual libraries	31
Configuring physical libraries and devices	32
Configuring and provisioning virtual libraries	37
Creating virtual tapes	51
Connecting virtual libraries with storage clients	59
Backing up the VTL system configuration	65
Recovering the server configuration	69
Protecting VTL metadata	69
Administering user accounts and passwords	72
Managing tapes	74
Locating virtual tapes	75
Replicating tapes	75
Copying tapes	92
Moving tapes between virtual and physical libraries	95

Managing tape caching	107
Creating and viewing reports	110
Encrypting and shredding data	114
Working with the Event Log	122
Using the Attention Required tab	125
Managing VTL servers	127
5. Installing the VTL console	129
6. Recovery following a system failure	133
Failback	133
Resuming backups following a failover/failback	144
7. Configuring email notifications	145
8. Updating VTL software	151
A. VTL command line reference	155
Typographical conventions	155
Usage	155
Common arguments	156
Login and logout	156
Virtual devices - client commands	157
Virtual devices - VTL server commands	165
Import/Export	180
Replication	182
Replication	190
Physical devices	196
Fibre Channel	200
Reports	201
Failover	203

Server configuration	205
Event Log	206
Technical support	207
B. Required ports	209
C. Troubleshooting	211
Problems during console operations	211
Problems affecting physical resources	214
Problems with virtual resources	215
Problems during import/export operations	219
Taking an X-ray for technical support	221
D. SNMP traps	225
E. ILOM command reference	261

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 <code>.login</code> file. Use <code>ls -a</code> to list files. <code>% You have mail.</code>
<i>AaBbCc123</i> <i>AaBbCc123</i>	Oblique text is used for variables that stand for real names or values and for book titles.	To delete a file, type: <code>rm filename.</code>
ABCD	Bold, san-serif text indicates callouts in illustrations.	Click <code>Submit</code> (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.

Note – The Customer Resource Center will be migrating to servers within the SunSolve support environment shortly after this document appears. But the above URL will be automatically redirected to the new location.

Using the VTL Wiki to obtain additional information

The VTL Wiki <<http://wikihome.sfbay.sun.com/vtlwiki/Wiki.jsp>> hosts links to a wide range of marketing, support, and technical resources, documents, and tools, as well as an extensive FAQ section with answers to Frequently Asked Questions.

Commenting on this book

Sun welcomes your comments and suggestions for improving this book. Contact us at glsf@sun.com. Please include the title, part number, issue date, and revision: *VTL User Guide*, part number 96267 (Feb 2008 revision E).

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 3
- a more in-depth look at selected, “Key VTL features and options” on page 6.

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.

- Software-based data compression

Compression software based on the LZO algorithm can, when necessary, 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. Conversely, a significant proportion of incompressible file types, such as ZIP archives, GIF images, and JPG images will reduce the attainable compression significantly.

- 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.

- CallHome support

The VTL CallHome 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

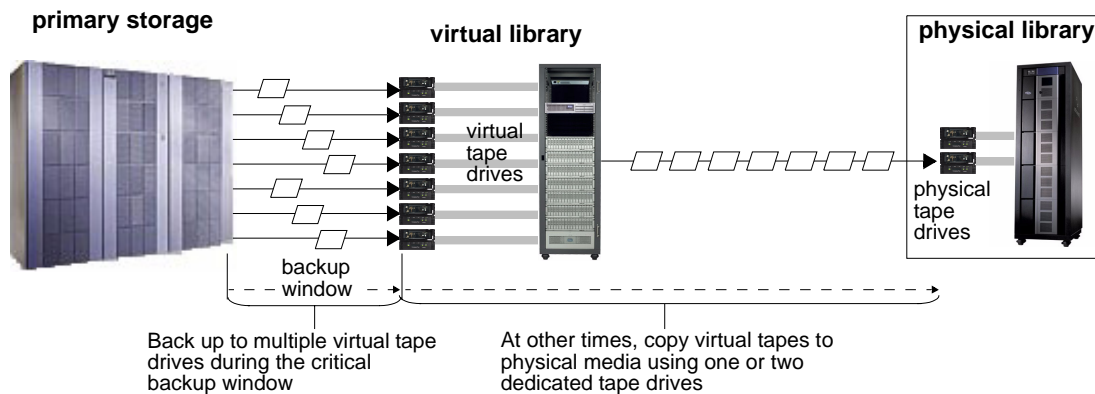
Adding Sun StorageTek VirtualTape Library appliances to an existing tape-based backup architecture can thus realize the following advantages:

- “Shorter runtimes and reduced dependency on backup windows” on page 4
- “Shorter run times for non-sequential backup jobs” on page 4
- “Improved reliability” on page 5
- “Better utilization of tape subsystems” on page 5
- “True tape virtualization with dynamically allocated disk space” on page 6.

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



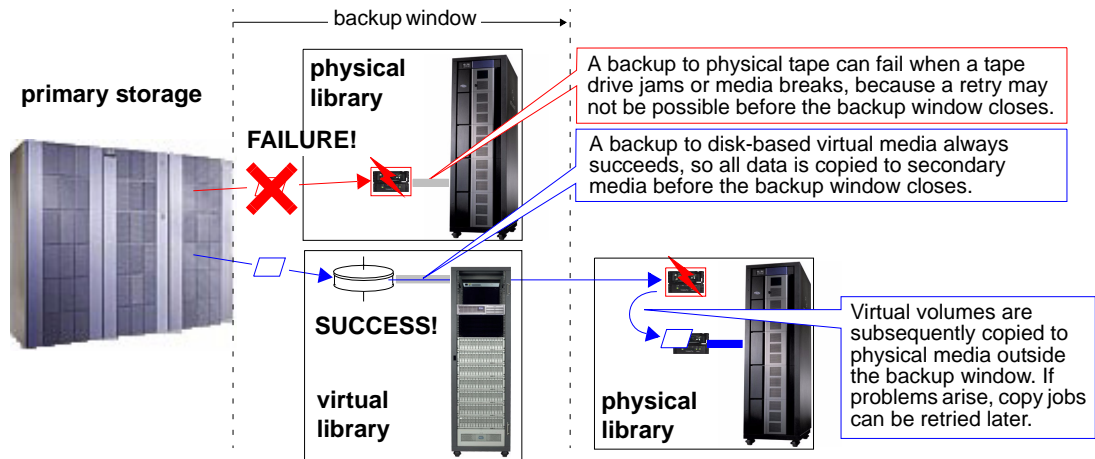
Shorter run times for non-sequential backup jobs

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

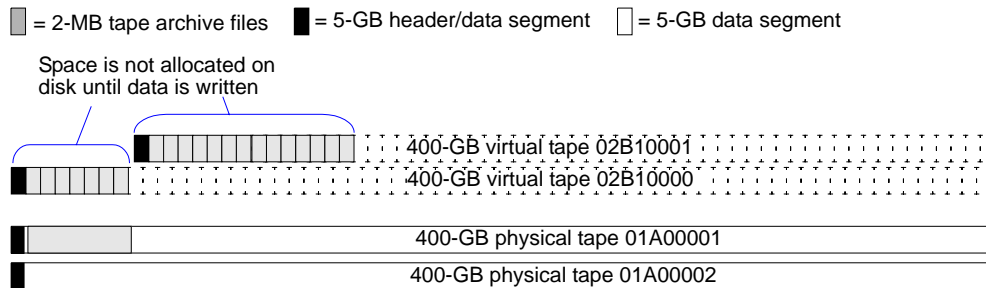


Better utilization of tape subsystems

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.

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 LTO-III 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).



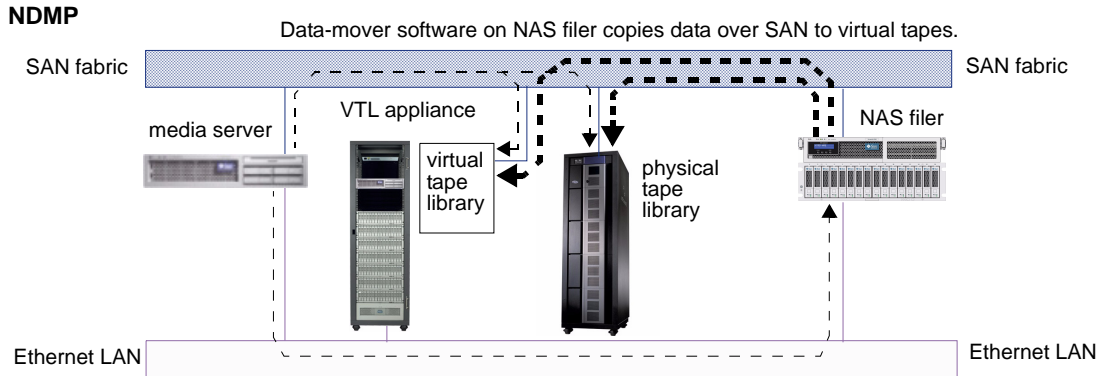
This approach to space allocation has two major advantages. First, it minimizes wasted disk capacity. Second, and perhaps more importantly, it maximizes array performance and reliability. Dividing data into multiple segments distributes it more evenly across the array, involves more volume groups in each I/O, and reduces the average length of each seek during I/O.

Key VTL features and options

- “NDMP support” on page 7
- “VTL high-availability option” on page 7
- “Automated Tape Caching” on page 10
- “Virtual tape replication” on page 10
- “VTL Secure Tape encryption option” on page 12.

NDMP support

Sun VTL virtual tape library SAN clients can include Network Attached Storage (NAS) filers. NDMP agent software on the filer moves data over the SAN to the virtual tape volumes mounted by the backup media server:



Installation of NDMP agent software on the VTL appliance itself is not supported.

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:

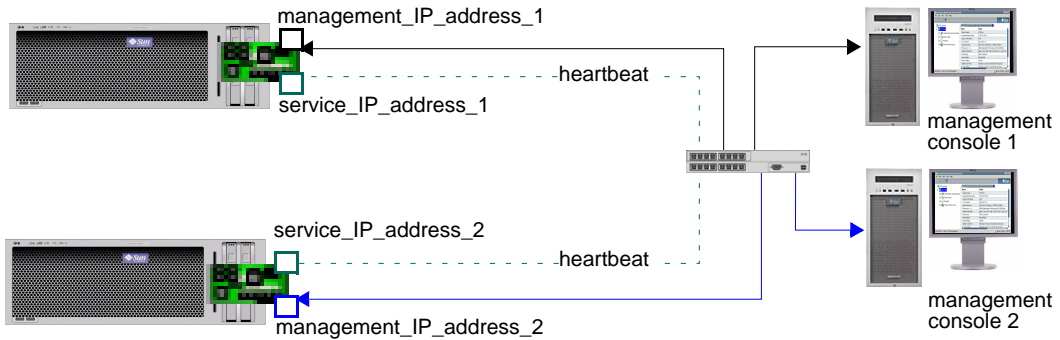
- “Server node failover” on page 7
- “Management path failover” on page 8
- “Storage path failover” on page 9.

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.

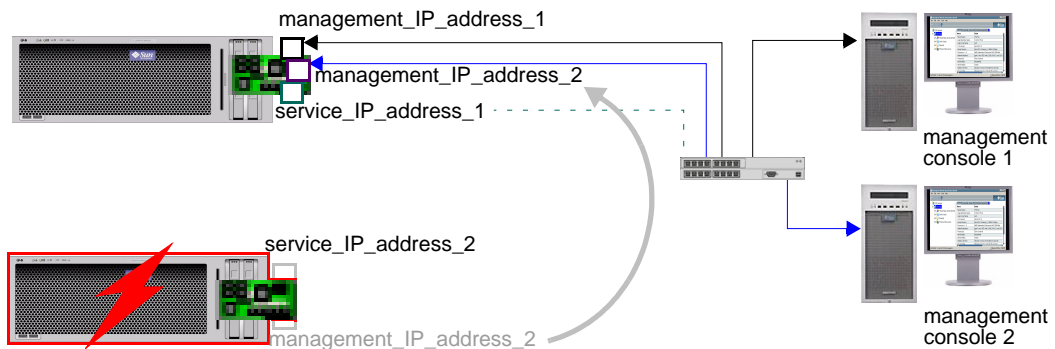
Service IP addresses carry heartbeat information between VTL nodes and management IP addresses carry commands between nodes and VTL management consoles



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.

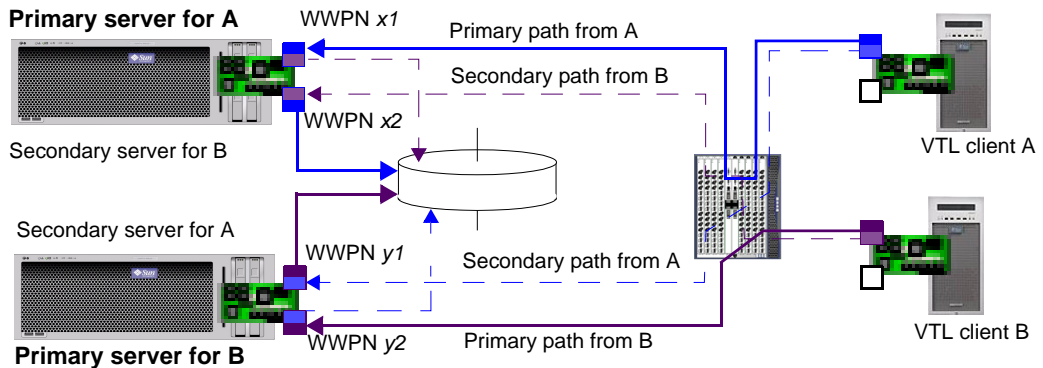
If the heartbeat signal is lost, the management IP address for the failed node transfers to the healthy node



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 11
- “Replication” on page 11
- “Remote Copy” on page 12.

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 47). 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.

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.

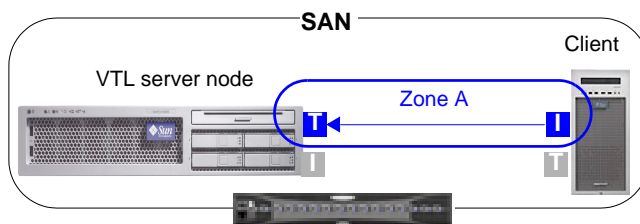
Understanding VTL zoning

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 13
- “Zoning for high-availability systems” on page 14.

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

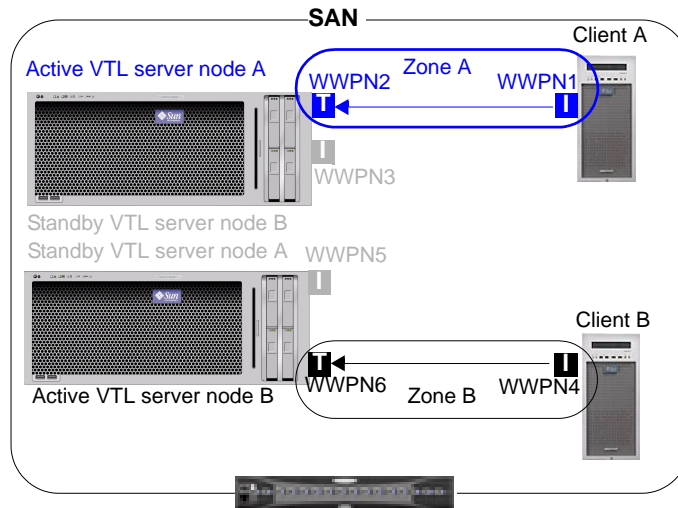
Zoning a high-availability system is slightly more complex than zoning a standard system, due to the need for redundant paths between initiators and targets. Once again, each SAN zone can have only one initiator and one target. But the total number of zones you need depends on whether the SAN is soft-zoned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

- “WWPN zoning (soft zoning)” on page 14
- “Port zoning (hard zoning)” on page 15.

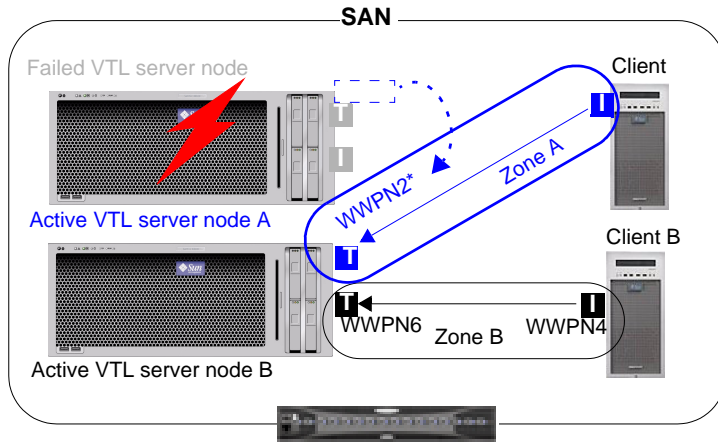
WWPN zoning (soft zoning)

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:

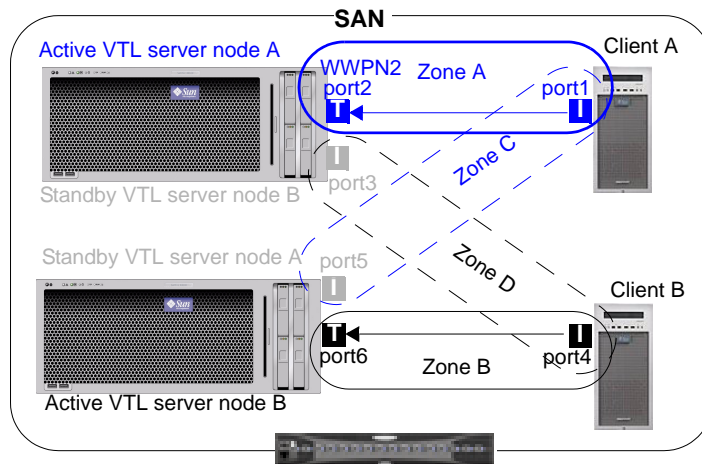


During failover, the zone still contains only one initiator and one target at a time. But the target WWPN is remapped from a port on the failed server node to a physical port on the standby server. The standby physical port spoofs the WWPN of the failed port, so zoning does not change. The figure below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



Port zoning (hard zoning)

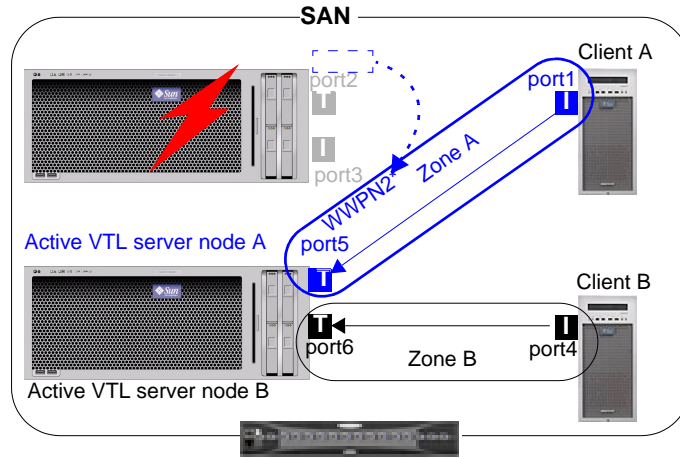
A hard-zoned SAN maps initiator to target using a physical port address. This port-to-port zoning establishes a fixed, physical route through the SAN. So, since each SAN zone can contain only one initiator and one target, you must provide two zones for each initiating client. The figure below shows a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



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 129.

The following sections explain how you use the console application:

- “Running the VTL console application” on page 18
- “Populating the console” on page 18
- “Understanding the VTL console interface” on page 20.

Note – For information on the text-based, VTL command line user interface, see Appendix A, “VTL command line reference” on page 149.

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

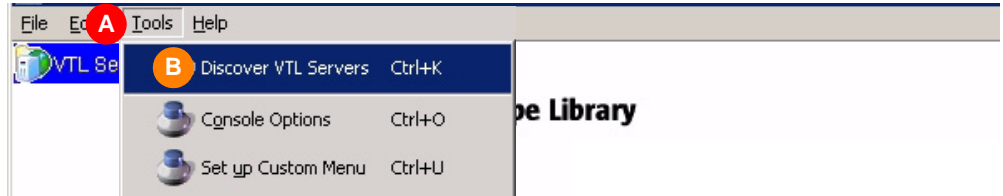
Once the console is running, you can specify the VTL servers that you want to see in the object tree at the left side of the VTL console. You can discover, add, or remove servers:

- “Discovering VTL server nodes” on page 18.
- “Adding a server node to the console tree” on page 19
- “Deleting a server node from the console tree” on page 20

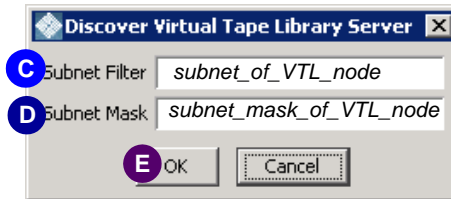
▼ Discovering VTL server nodes

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)**.

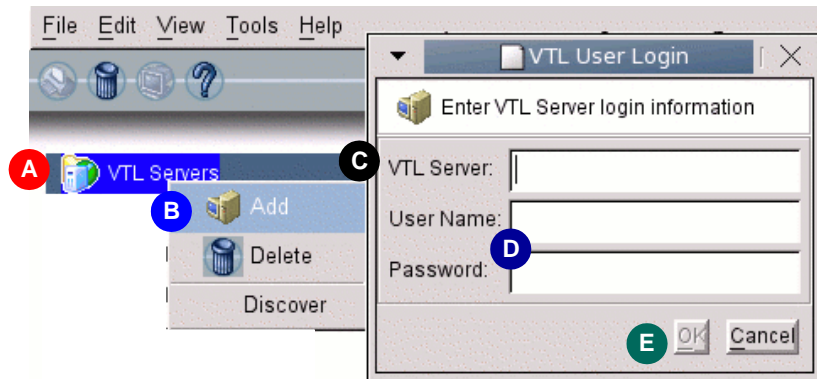


After a short wait, the VTL console application discovers the appliance and adds it to the list on the left side of the graphical user interface (GUI).

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.

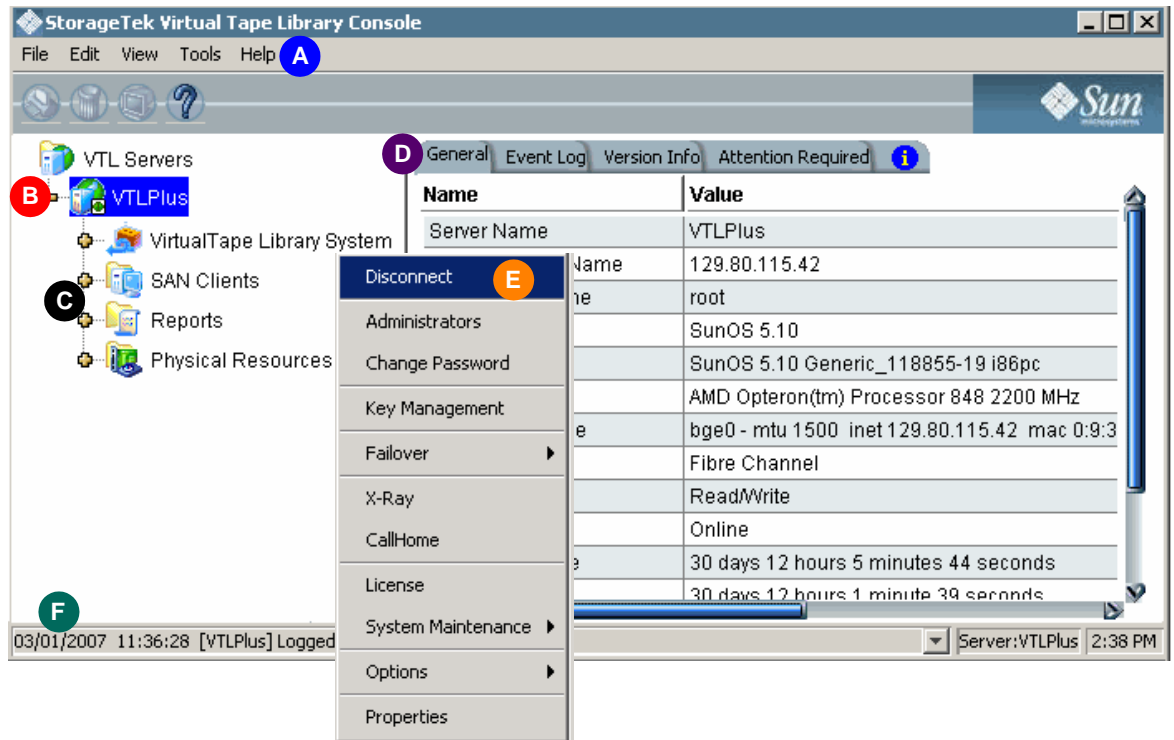
Stop here.

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 22
- “SAN Clients” on page 23
- “Reports” on page 23
- “Physical Resources” on page 24.

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 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 ("Direct") device.
	The F icon indicates that this is shared storage and is being used by another server. The <code>Owner</code> field lists the other server.

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 25
- “Managing virtual libraries” on page 31
- “Managing tapes” on page 74
- “Managing tape caching” on page 107
- “Creating and viewing reports” on page 110
- “Encrypting and shredding data” on page 114
- “Working with the Event Log” on page 122
- “Managing VTL servers” on page 127.

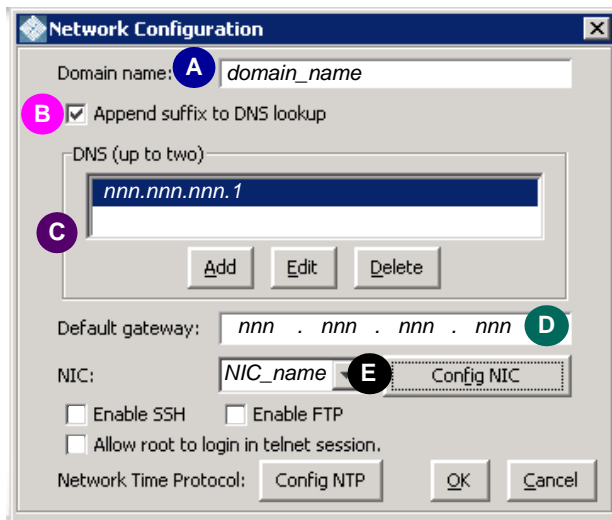
Managing network connectivity

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 26
- “Setting the VTL server node host name” on page 28
- “Obtaining SAN interface configuration information” on page 29
- “Administering SAN client connections” on page 30.

▼ 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.

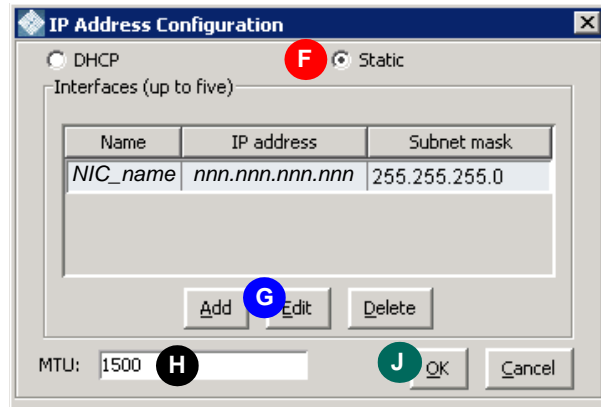


2. Enter IP address information for the Domain Name Server (if used) in the DNS section (C above), using the Add and Edit buttons.
3. Enter the IP address of the Default gateway (D above).
4. Select the *NIC_name* Ethernet interface, and push the Config NIC button (E above).

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.

- When the IP Address Configuration property sheet appears, click the Static radio button (F below).



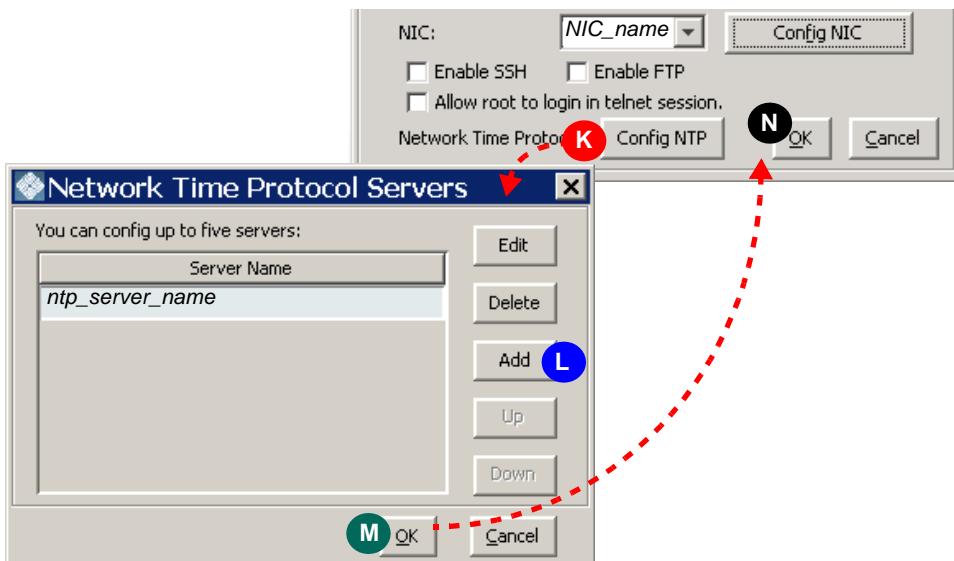
- Click the Edit button (G above), and enter the IP address that the customer provided.

- Leave the MTU text field (H above) as set by the factory.

- Press OK (J above).

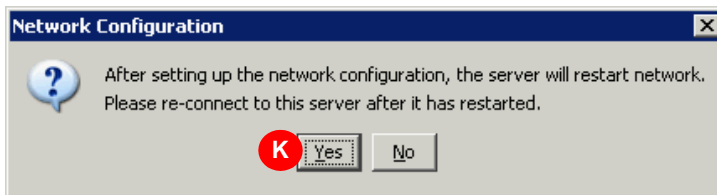
You return to the Network Configuration property sheet.

- 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).



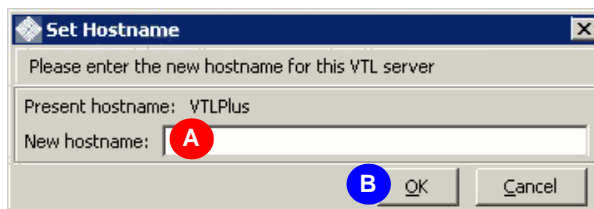
The network should restart automatically.

12. Reconnect to the VTL server node.

Stop here.

▼ Setting the VTL server node host name

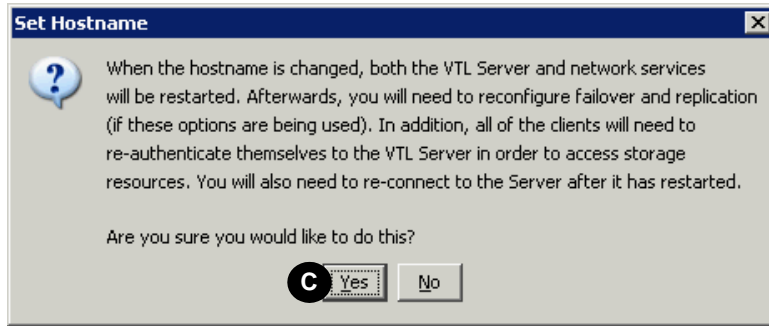
1. When the `Set Hostname` dialog appears, enter a valid name for your VTL appliance (A below).



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)**.



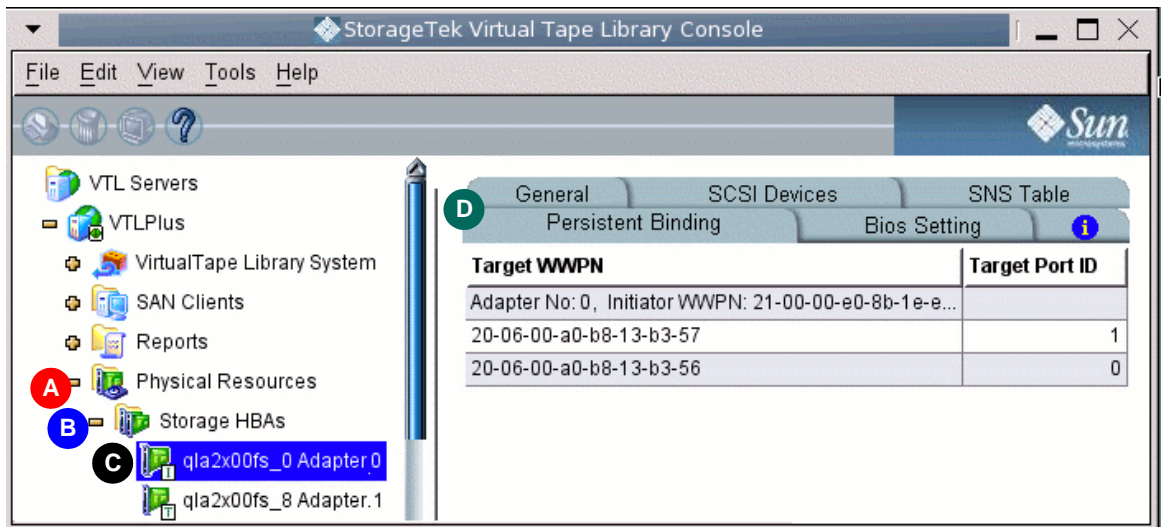
4. Log back in to the server to continue working.

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 59.

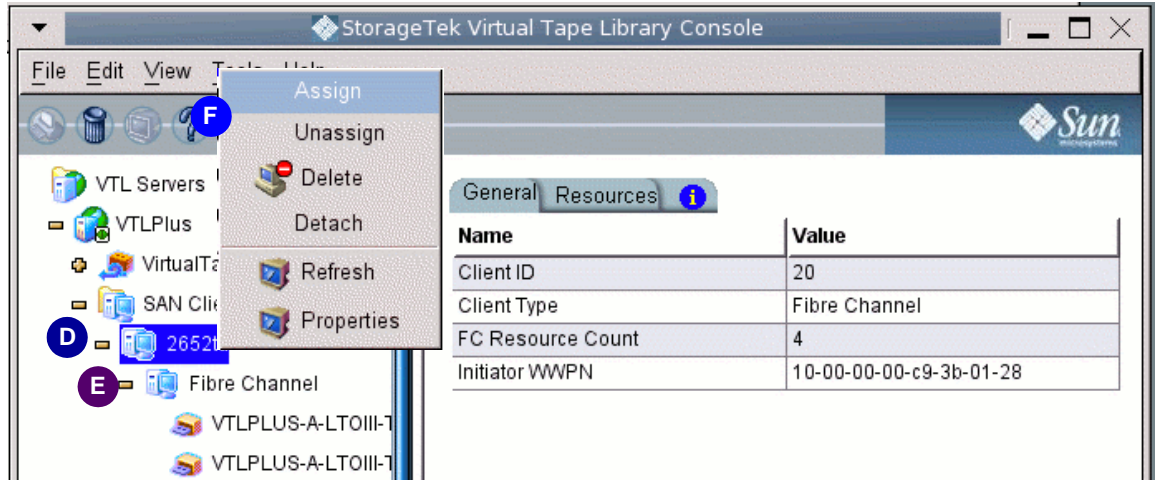
1. In the tree-view pane of the VTL console, select SAN Clients (A below) and click on the name of the client (B).

The screenshot shows the StorageTek Virtual Tape Library Console interface. On the left, a tree view shows the hierarchy: VTL Servers > VTLPlus > VirtualTape Library System > SAN Clients. A red circle 'A' is around the 'SAN Clients' folder, and a black circle 'B' is around the client '2652ta'. On the right, the 'General' tab is selected, and a table displays the client's configuration details.

Name	Value
Client ID	20
Client Type	Fibre Channel
FC Resource Count	4
Initiator WWPN	10-00-00-00-c9-3b-01-28

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 37 (includes “Creating virtual tape libraries” on page 39 and “Creating virtual tapes” on page 51)
- “Connecting virtual libraries with storage clients” on page 59.

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 32.
- If you are using a shared library, see “Managing ACSLS and Library Station tape pools” on page 36.

Managing direct-attached physical tape storage

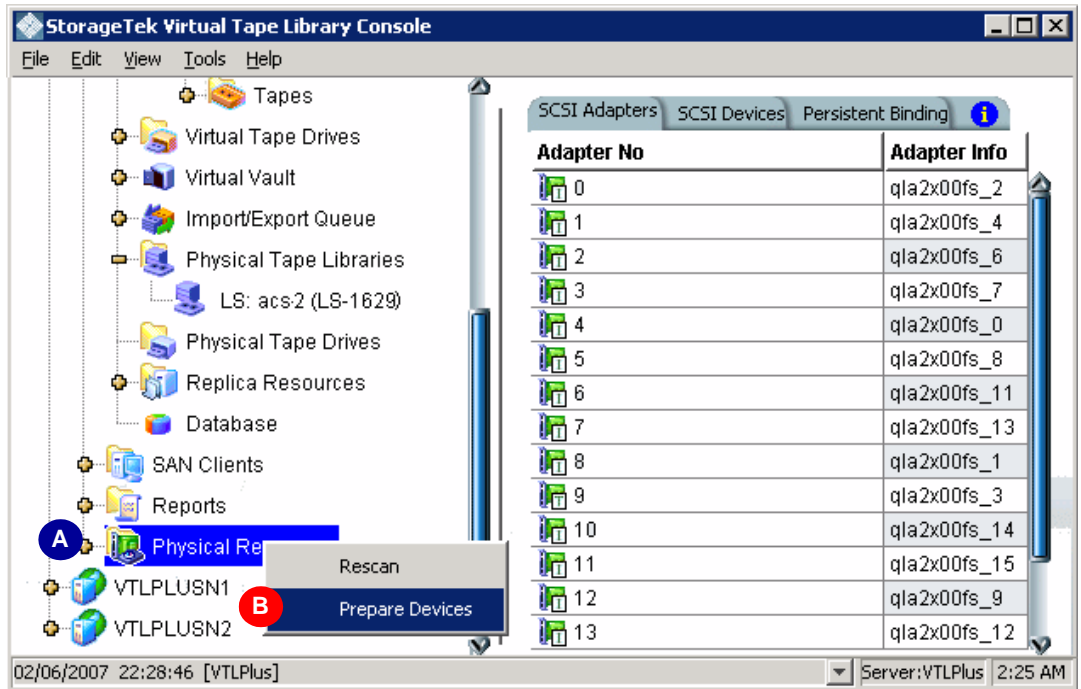
If you have a direct-attached library or device, you must assign the library or device to VTL using the VTL console software. Carry out the following tasks:

- “Preparing physical libraries and devices for assignment” on page 32
- “Assigning direct-attached physical tape libraries/devices” on page 35.

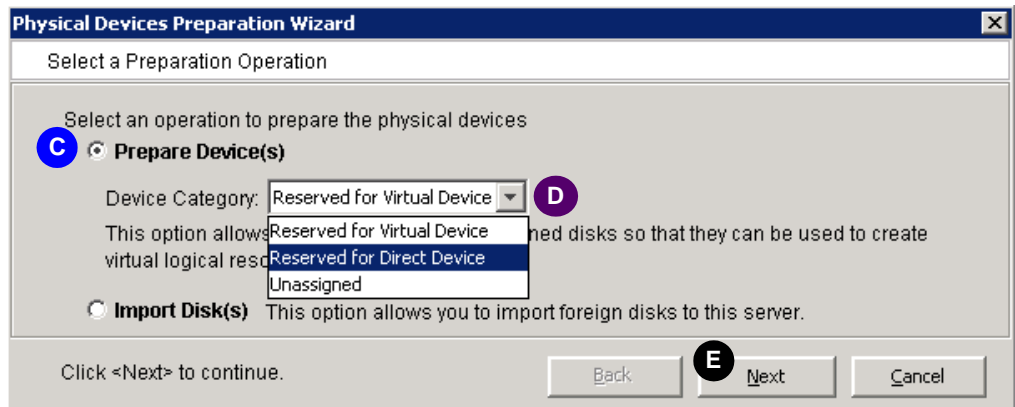
▼ Preparing physical libraries and devices for assignment

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).



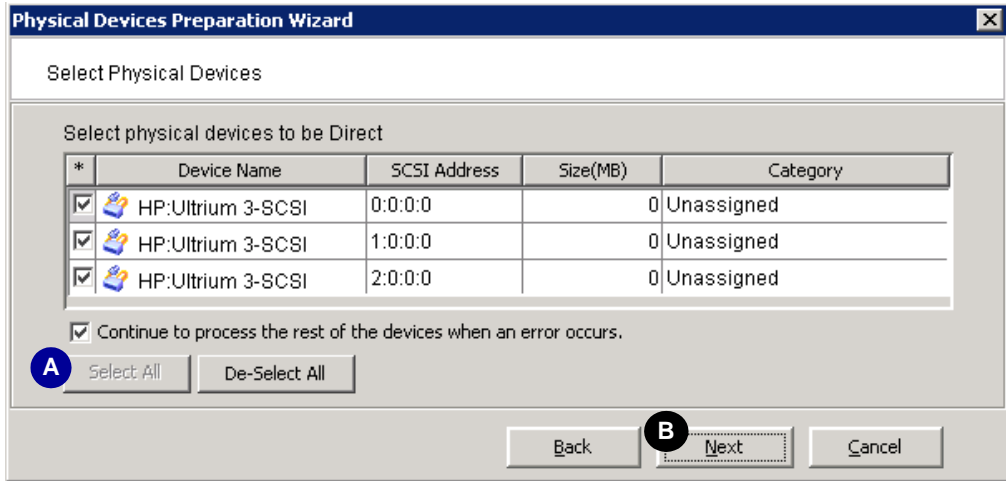
3. When the Select a Preparation Operation dialog appears, click the Prepare Device(s) radio button (C below).



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

- 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.

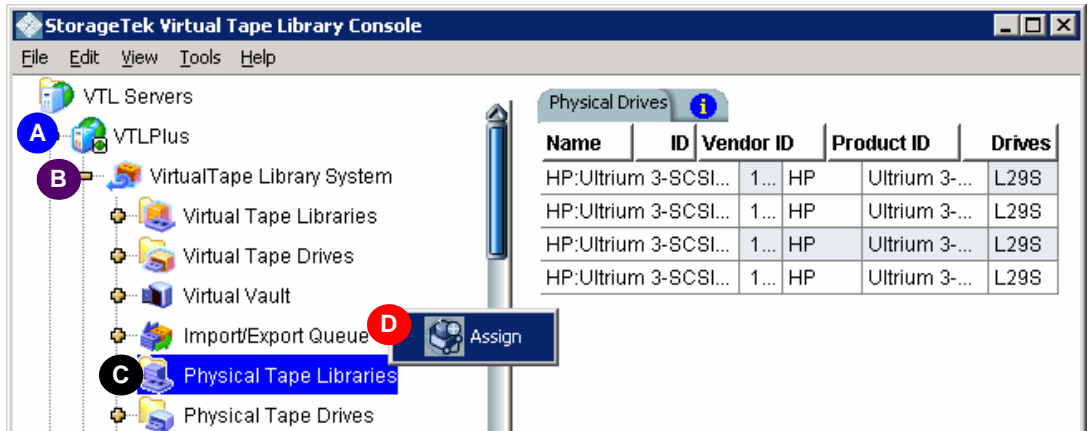


- When the **Prepare Device** panel appears, press **Finish**.

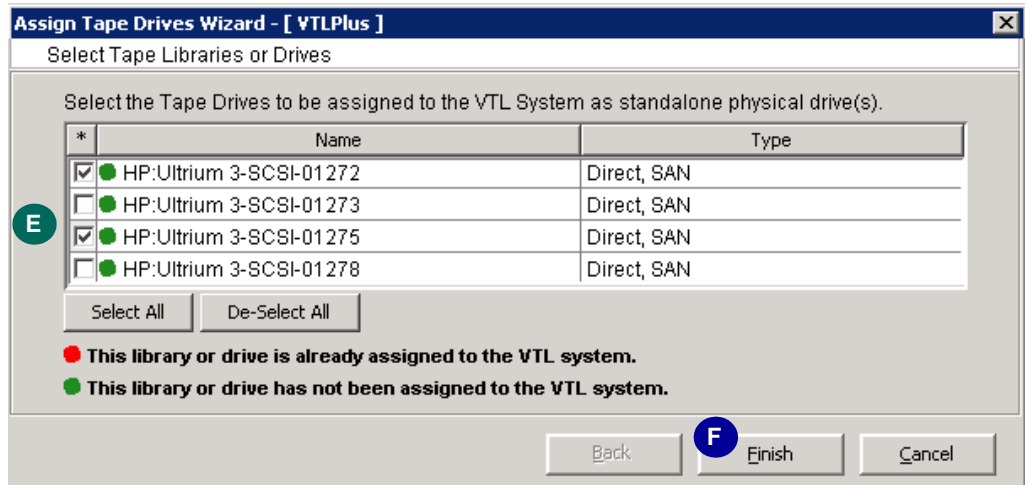
Next task: "Assigning direct-attached physical tape libraries/devices" on page 35.

▼ 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).

The screenshot shows the StorageTek Virtual Tape Library Console interface. On the left, the object tree is expanded to show the following structure:

- VTL Servers
 - VTLPlus (A)
 - VirtualTape Library System (B)
 - Virtual Tape Libraries
 - Virtual Tape Drives
 - Virtual Vault
 - Import/Export Queue
 - Physical Tape Libraries (C)
 - LS:acs-2 (LS-1629) (D)
 - Physical Tape Drives
 - Replica Resources
 - Database

A context menu is open over the 'LS:acs-2 (LS-1629)' item, showing the following options:

- Assign
- Unassign
- Rename
- Import Tape
- Inventory (E)**
- Move Tape
- Reset

The main window displays a table with the following data:

Name	Value
Vendor ID	STK
Product ID	129.80.115.112:2
Status	Online
Virtual ID	1629
Slots	4096
IE Slots	0
IP Address	129.80.115.112
ACS ID	2

Stop here.

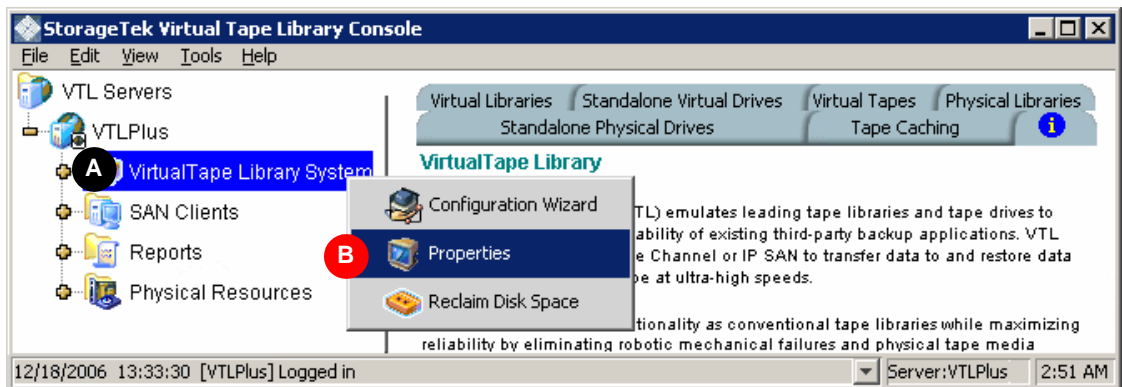
Configuring and provisioning virtual libraries

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 37
- “Creating virtual tape libraries” on page 39
- Setting up optional functionality (see “Configuring Automated Tape Caching” on page 42, “Setting up the Auto Archive feature” on page 46, or “Setting up the Auto Replication option” on page 47)
- “Generating the virtual library” on page 48
- “Creating virtual tapes” on page 51.

▼ 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).



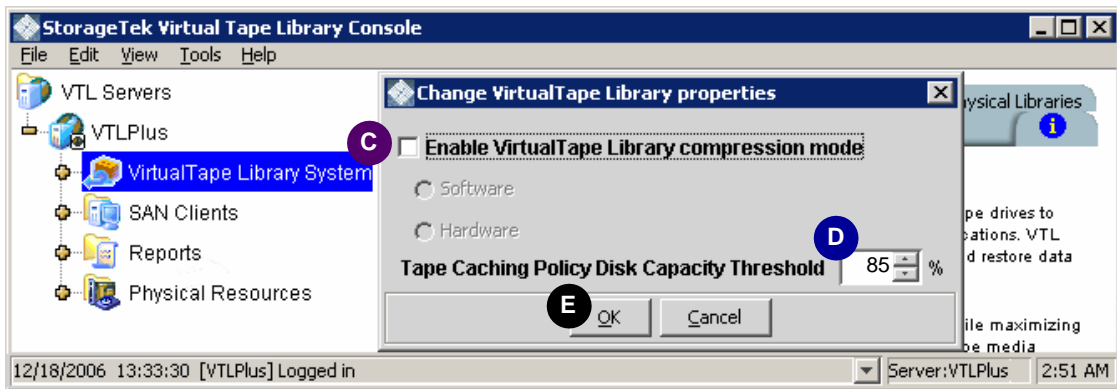
2. When the Change VirtualTape Library properties sheet appears, if you wish to use VTL compression software, check the Enable Virtual Tape Library compression mode check box (C below).

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.

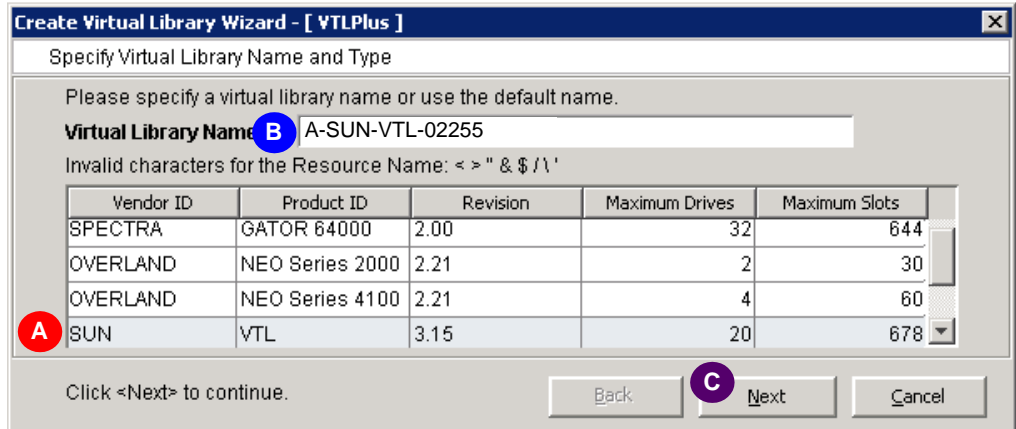
4. Press OK (E above).

Stop here.

▼ Creating virtual tape libraries

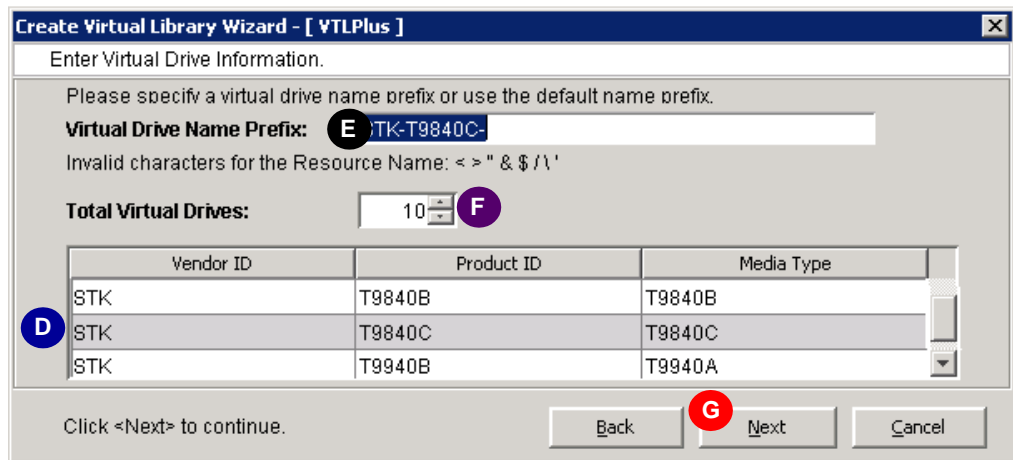
1. When the **Create Virtual Library Wizard** appears, select the type of library that you want to emulate (**A** below), enter a **Virtual Library Name** (**B**) or use the default, and press **Next** (**C**).

Select 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.



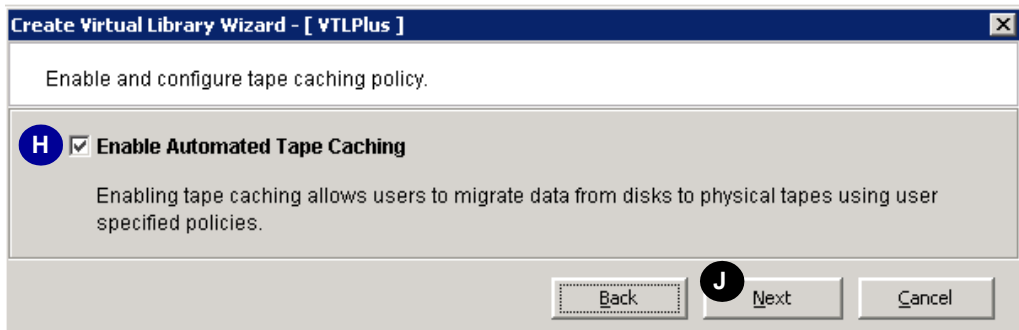
Management is easier when you give libraries and the virtual tapes they hold a common alphabetical prefix, such as the **A-** prefix shown in the example (**A** above).

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**).

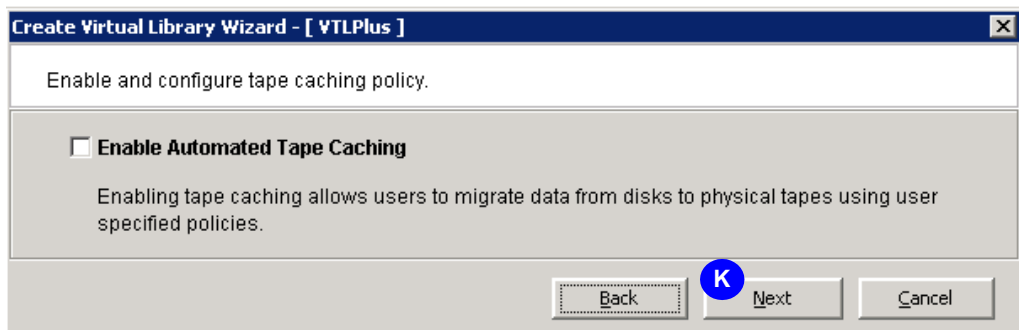


If you plan to attach a physical tape library to the VTL appliance for tape import or export, emulate the physical library so that virtual tapes will be compatible with their physical counterparts.

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

Next task:

- If you are going to configure tape caching on this virtual library, go to “Configuring Automated Tape Caching” on page 42.
- If you are going to use the automatic archiving features, go to “Setting up the Auto Archive feature” on page 46.
- If you are going to use the automatic replication feature, go to “Setting up the Auto Replication option” on page 47
- Otherwise, go to “Generating the virtual library” on page 48.

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 streams, 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 policies 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 42
- “Creating state- and event-based migration policies” on page 43.

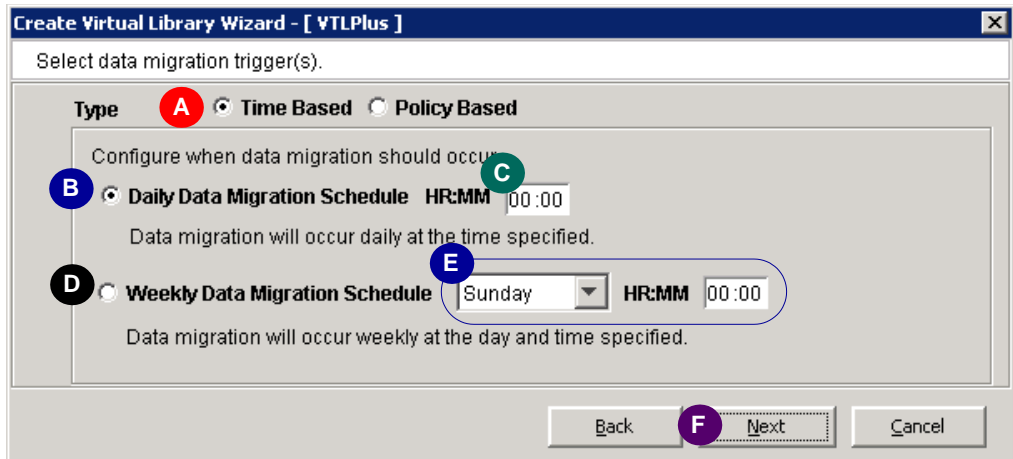
Then go to “Creating a reclamation policy” on page 45.

▼ 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).

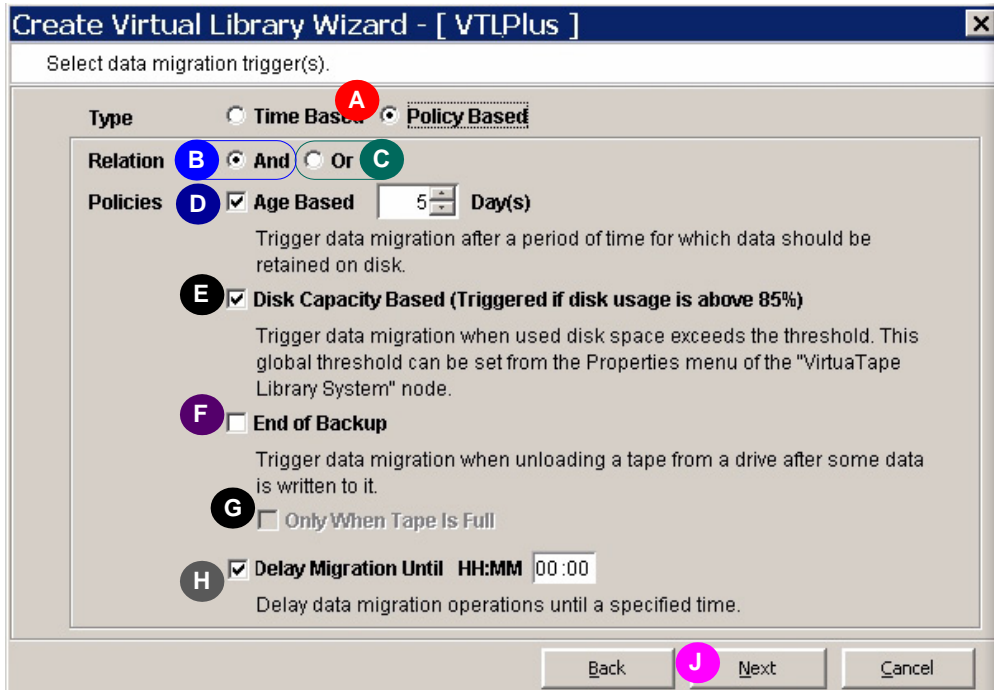
Next task: “Creating a reclamation policy” on page 45.

▼ 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).



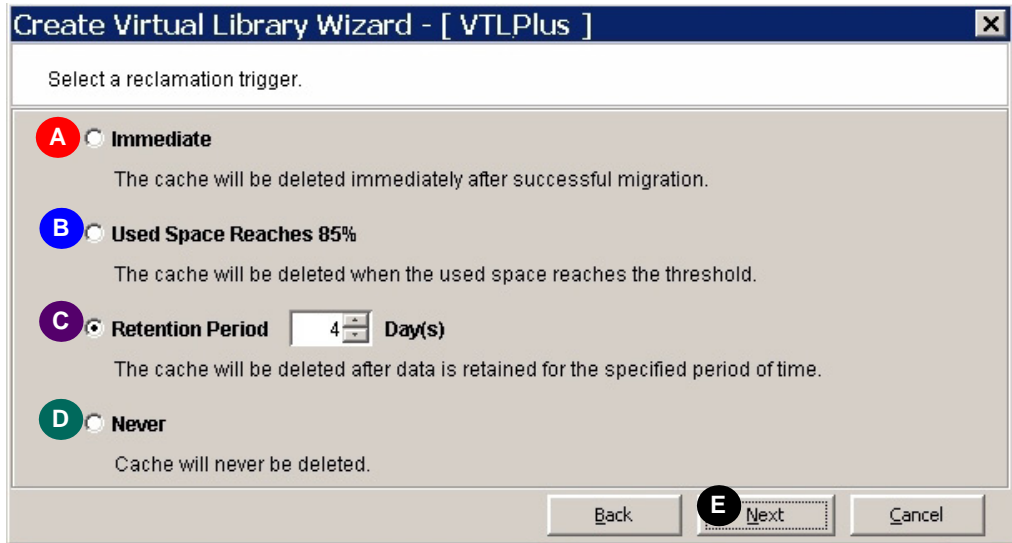
3. To migrate data when ONE OR MORE of the conditions specified is satisfied, click the the Or radio button (C above).
4. To trigger migration based on the age of the data, check the Age Based check box, and use the spinner control to select the desired number of days (D above).
5. To trigger migration 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" on page 45.

▼ 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).

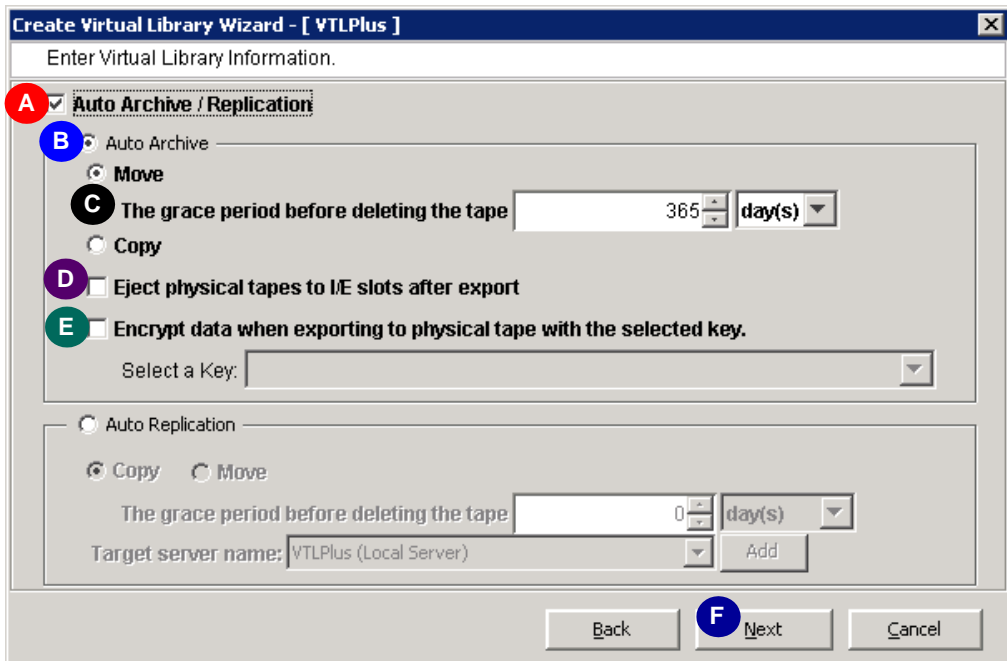


2. If you choose to specify a Retention Period, use the spinner control (B above) to specify the number of Day(s).
3. Then press Next (C above).

Next task: “Generating the virtual library” on page 48.

▼ 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 48.

▼ 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 48.

▼ Generating the virtual library

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

Enter exactly six (6) characters when emulating Sun StorageTek libraries—neither more nor less.

Hint: management is easier when you give libraries and the virtual tapes they hold a common alphabetical prefix, such as the A prefix shown in the example below.

The screenshot shows a Windows-style dialog box titled "Create Virtual Library Wizard - [VTLPlus]". The main area is titled "Enter Virtual Library Information." and contains the following fields:

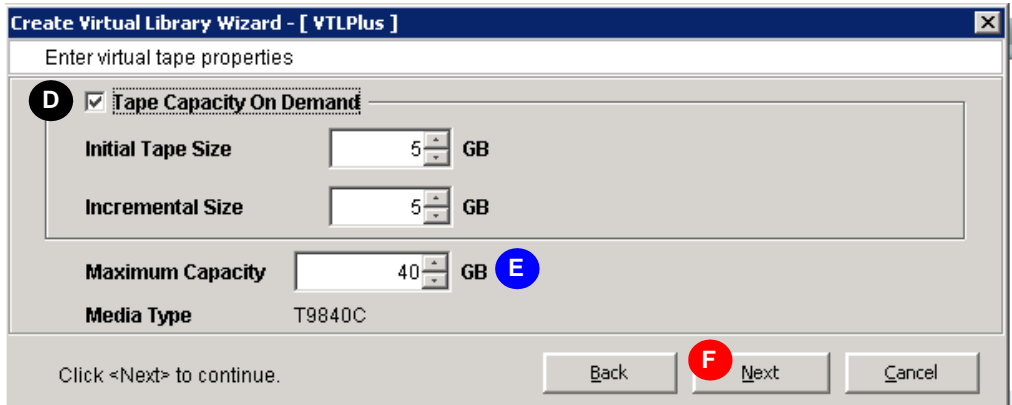
- Name:** SUN-VTL-02276
- Barcode Starts:** A00000 (The letter 'A' is circled in red and labeled 'A').
- Barcode Ends:** A99999 (The letter 'A' is circled in blue and labeled 'B').
- Number of Slots:** 678
- Import/Export Slots:** 20

At the bottom, there are three buttons: "Back", "Next" (circled in black and labeled 'C'), and "Cancel". A message at the bottom left says "Click <Next> to continue."

2. **Enter a Barcode Ends value in the text field provided (B above).**
3. **Press Next (C above).**

Do not change properties (such as the number of slots) if you have chosen to emulate a particular physical library (such as a Sun StorageTek SL500) rather than the generic Sun VTL library. From an application or client point of view, virtual and physical instances of a given library should be functionally identical. If they are not, clients and applications may behave in unanticipated ways.

4. When the Enter virtual tape properties dialog appears, check the Tape Capacity On Demand check box (D below).



We recommend capacity on demand for most users.

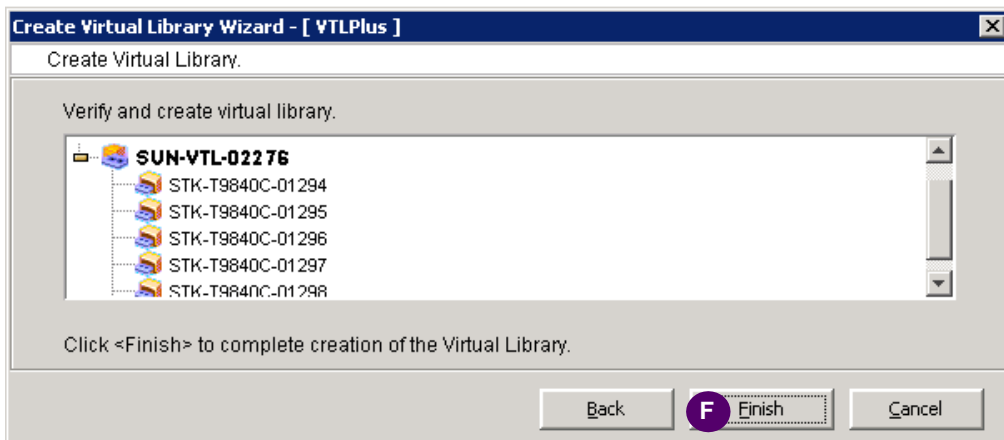
5. If you have enabled software compression, use the spinner control (E above) to reduce the Maximum Capacity to 85-90% of the uncompressed capacity of the selected media.

In the example above, we would reduce maximum capacity to 34-36 GB when using compression.

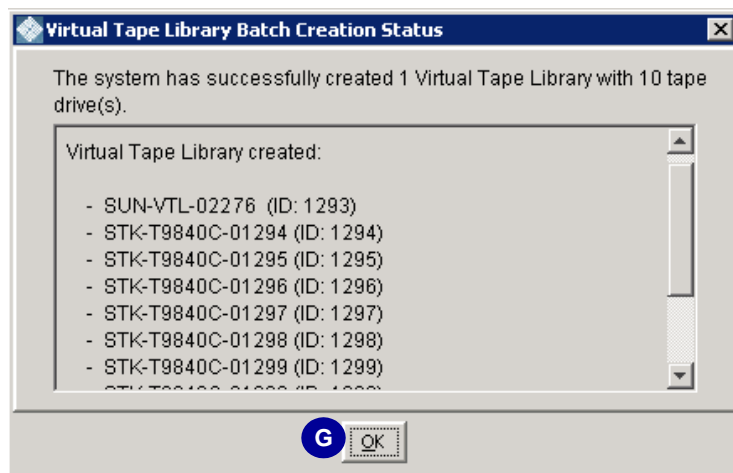
Leaving the recommended margin is important, because the compression ratio possible with any given dataset is difficult to predict. A dataset that happens to contain a significant number of incompressible file types (such as ZIP and RAR archives, PDF documents, GIF and JPG images, and many binary files) will not compress as much as a dataset that contains only compressible data.

6. Otherwise, accept the default values for all settings. In particular, do not increase Maximum Capacity beyond the capacity of the emulated Media Type. If you do, you risk over-subscribing the disk, and clients and applications may behave in unanticipated ways.
7. Press Next (E above).

8. When the confirmation screen appears, press **Finish (F below)**.



9. When the Batch Creation Status panel appears, press **OK (G below)**.

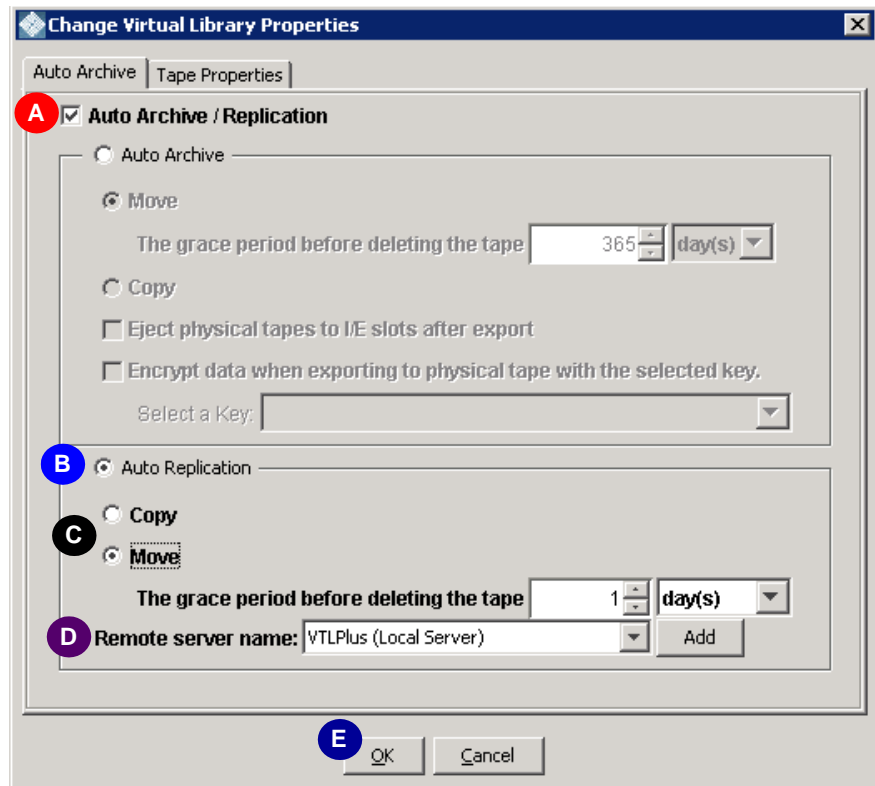


Next task: If you decided to create tapes, go to “Creating virtual tapes” on page 51.

▼ 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.

- 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).



- 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).
- 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).
- Press OK (E above).

Stop here.

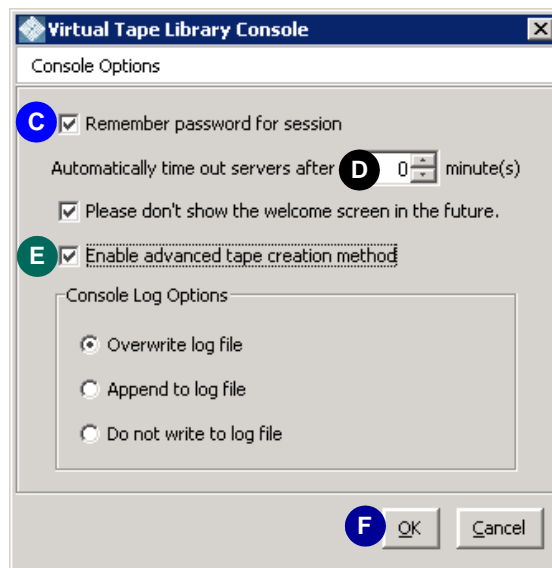
Creating virtual tapes

Follow the procedures outlined below:

- “Enabling the advanced tape creation method” on page 52
- “Setting replication parameters for virtual tape volumes” on page 56
- “Launching the virtual tape batch creation process” on page 59.

▼ 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

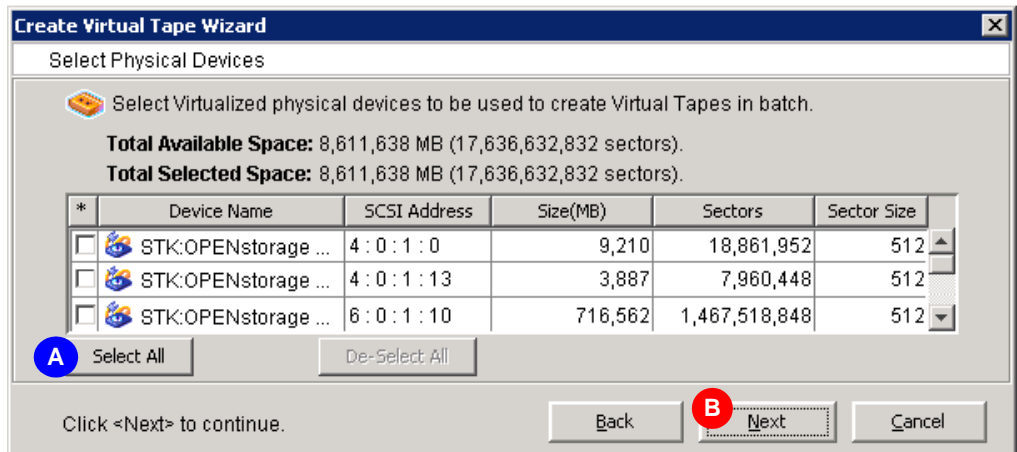
result, the software will let you create as many *increment-sized* tapes as will fit in the available disk space, up to the maximum number of slots defined for the library (658 for the Sun VTL library type). If you accept this number and create the tapes, the system will run out of disk space long before 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: “Creating virtual tapes” on page 53.

▼ Creating virtual tapes

1. When the **Select Physical Devices** dialog appears, press **Select All** (A below).



2. Press **Next** (B).

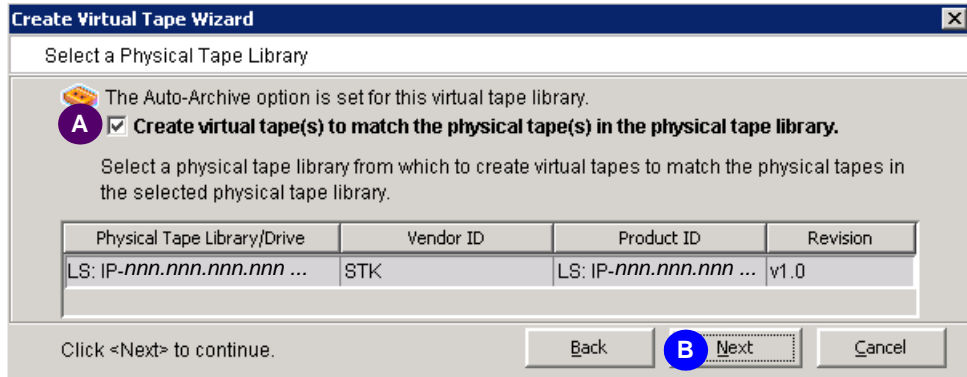
Next task: at this point, the behavior of the configuration wizard depends on the configuration of the virtual library:

- 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 54.
- Otherwise, the wizard skips directly to the **Specify Batch Mode Information** dialog. So go to “Allocating disk space to virtual tapes” on page 55.

▼ Setting Auto Archive parameters for virtual tape volumes

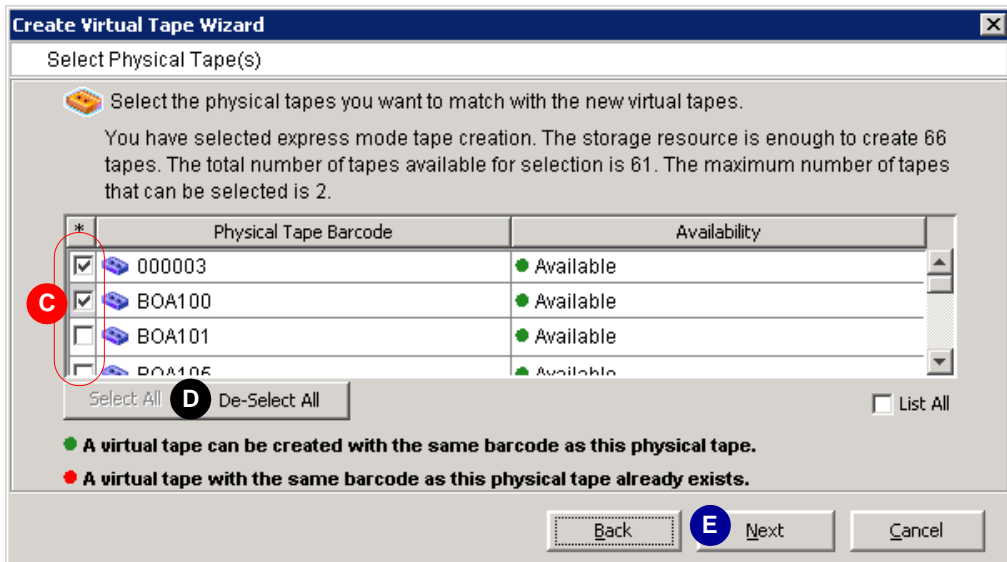
If the new virtual tapes will reside in a library that has the Auto Archive option enabled, proceed as follows.

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 55.

▼ 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).

Management is easier when you give libraries and the virtual tapes they hold a common alphabetical prefix, such as the A prefix shown in the example above (A).

Create Virtual Tape Wizard

Specify Batch Mode Information

Enter the information required to create the Virtual Tapes.

Virtual Tape Name Prefix: A-T9840C- **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: A-T9840C-

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

Virtual Tape Size: 36 GB

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

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.

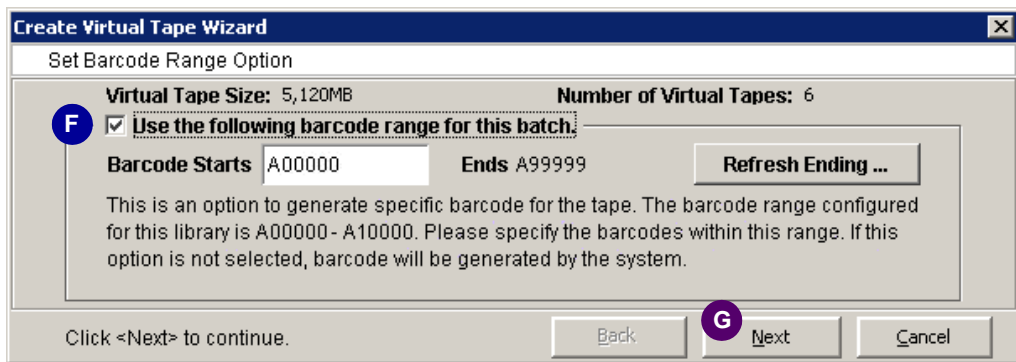
Back **E** Next Cancel

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).



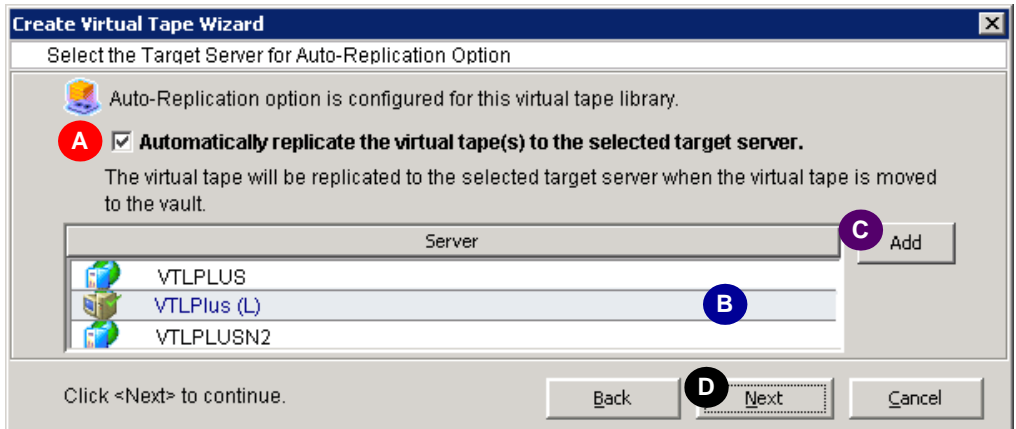
Next task:

- If you are using the Auto-Replication feature, go to “Setting up the Auto Replication option” on page 47.
- Otherwise, go to “Launching the virtual tape batch creation process” on page 59.

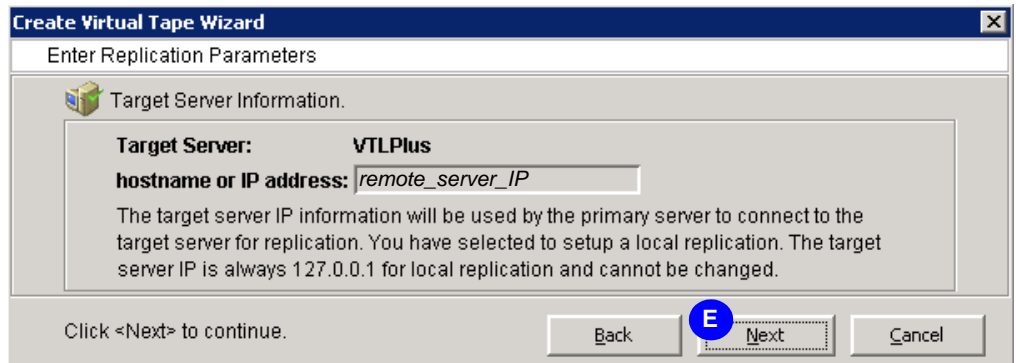
▼ **Setting replication parameters for virtual tape volumes**

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

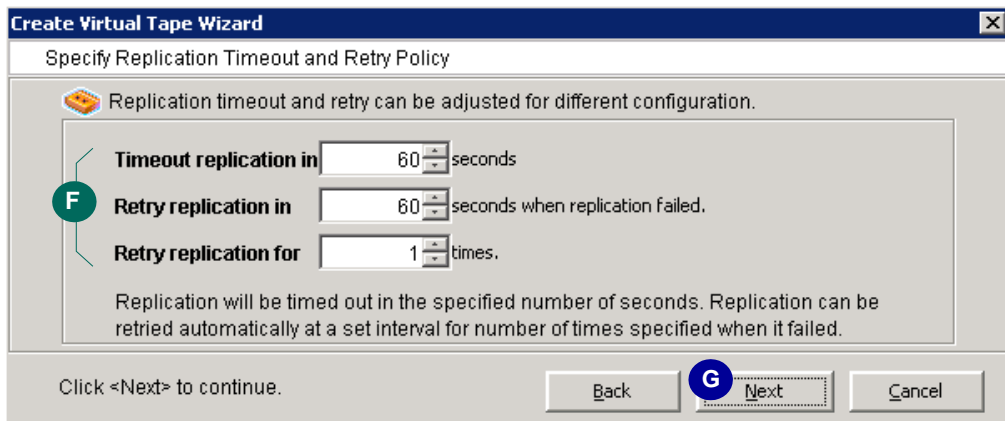
1. When the Select Target Server for Auto-Replication Option dialog appears, check the Automatically replicate the virtual tape(s) to the selected target server check box (A below).



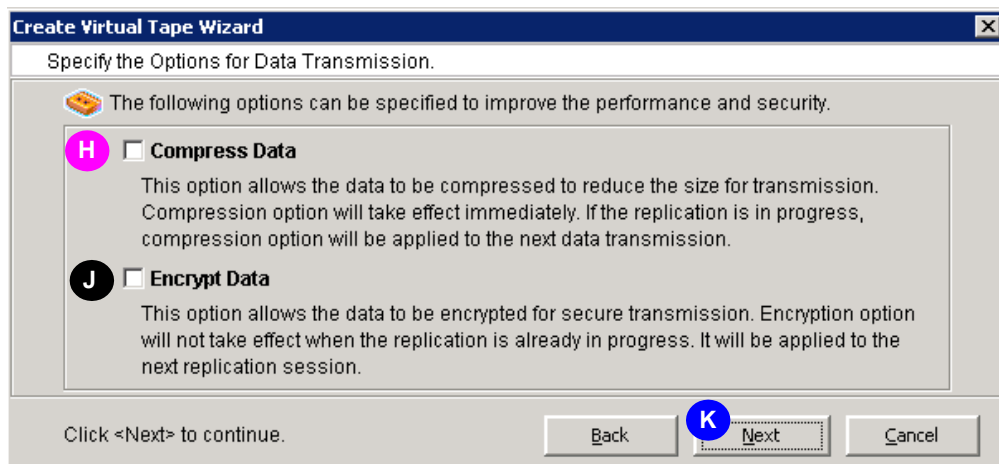
2. Select the remote server from the list (B above), or press Add to add a server to the list (C). Press Next (D).
3. When the Target Server Information panel appears, press Next (E below).



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.



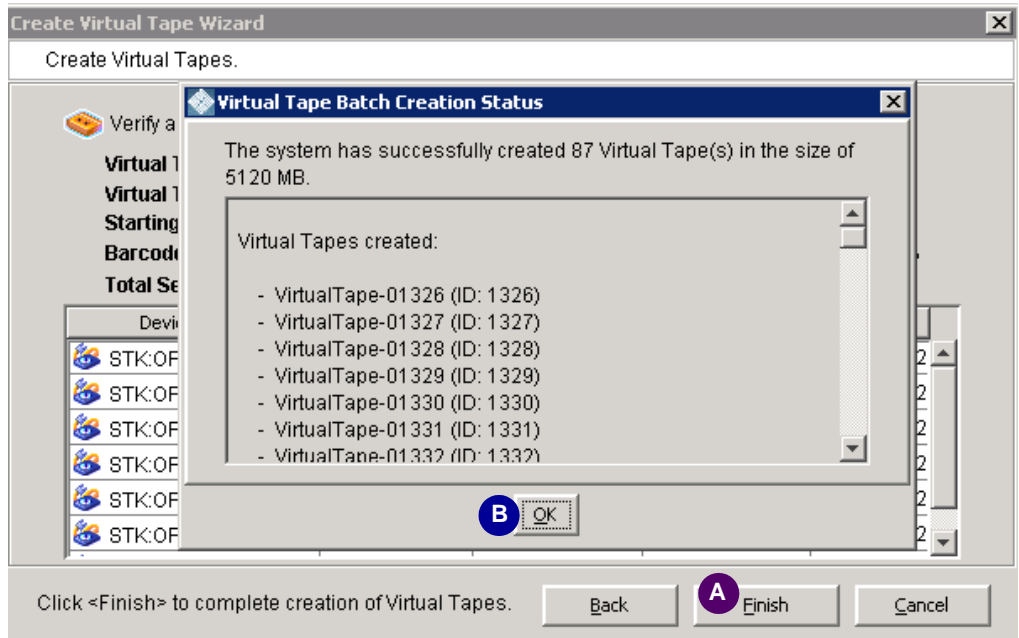
6. Check the Encrypt Data check box (J above) to enable encrypted transmissions. Encryption software is often necessary when replicating data over insecure links. However, assess requirements carefully. Consider the operational impact of the additional processor workload and consequent reductions in throughput before enabling this option.

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

Next task: “Launching the virtual tape batch creation process” on page 59.

▼ 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

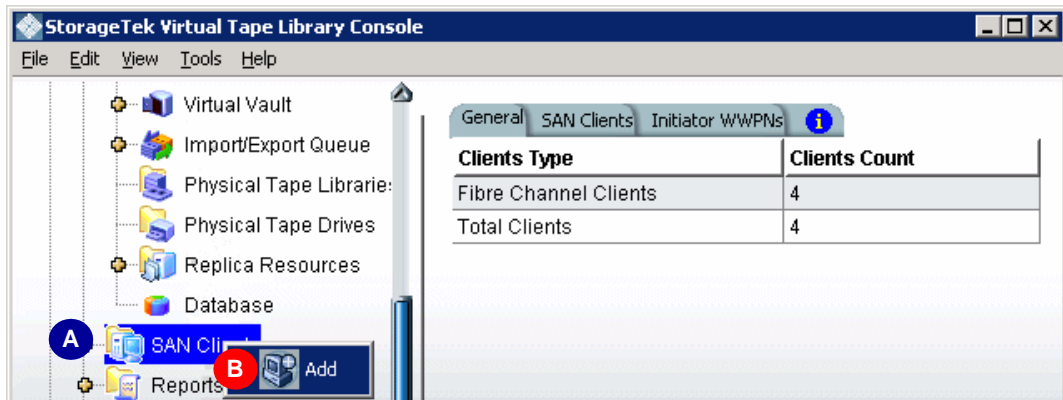
To connect virtual libraries with client machines (typically backup application or NDMP agent hosts), carry out the following tasks:

- “Starting the Add Client Wizard” on page 60

- “Adding SAN clients” on page 61
- “Assigning virtual libraries to storage clients” on page 64.

▼ Starting the Add Client Wizard

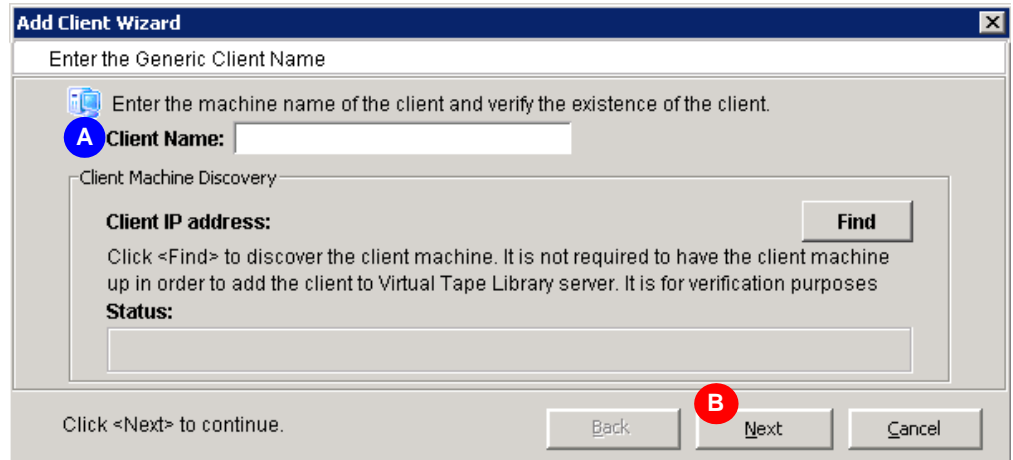
1. In the tree menu of the VTL console, select the VTL server branch.
2. Right-click the SAN Clients branch (**A** below).
3. Select Add from the context menu (**B** below).



Next task: “Adding SAN clients” on page 61.

▼ Adding 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).



Add Client Wizard

Enter the Generic Client Name

Enter the machine name of the client and verify the existence of the client.

A Client Name:

Client Machine Discovery

Client IP address: **Find**

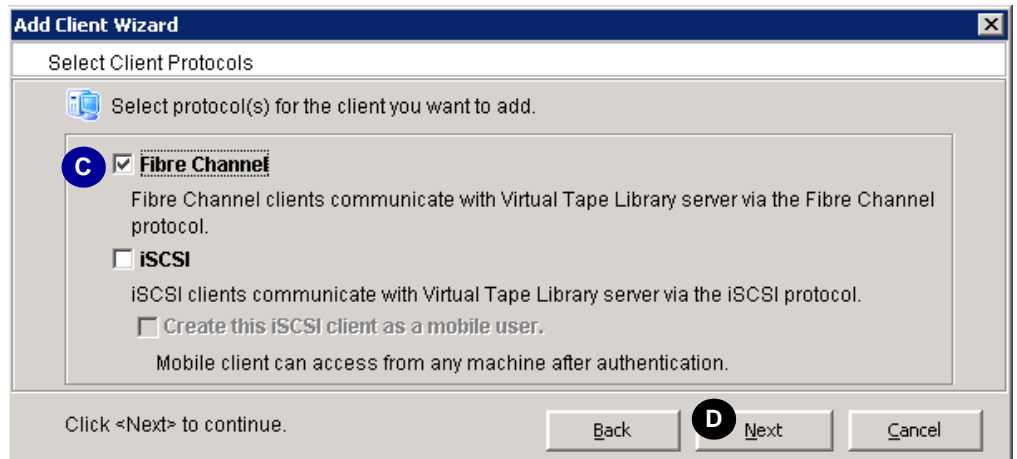
Click <Find> to discover the client machine. It is not required to have the client machine up in order to add the client to Virtual Tape Library server. It is for verification purposes

Status:

Click <Next> to continue.

B Back Next Cancel

2. When the Select Client Protocols dialog appears, check the Fibre Channel check box (C below), and press Next (D).



Add Client Wizard

Select Client Protocols

Select protocol(s) for the client you want to add.

C **Fibre Channel**
Fibre Channel clients communicate with Virtual Tape Library server via the Fibre Channel protocol.

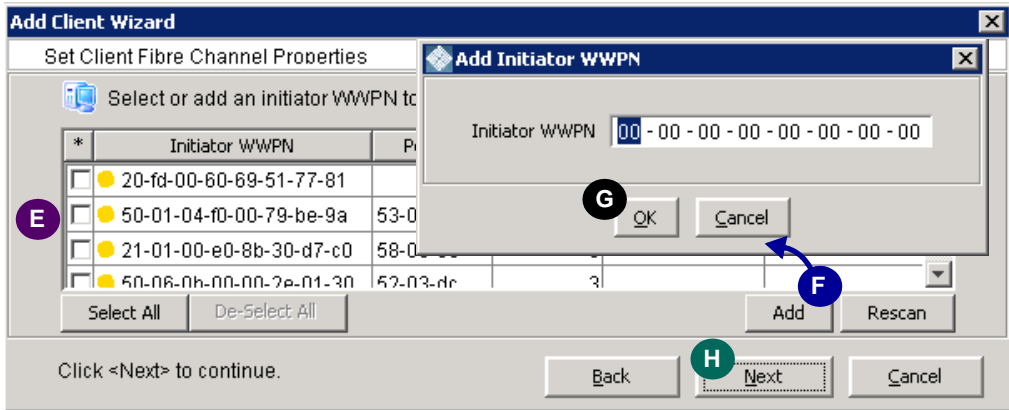
iSCSI
iSCSI clients communicate with Virtual Tape Library server via the iSCSI protocol.

Create this iSCSI client as a mobile user.
Mobile client can access from any machine after authentication.

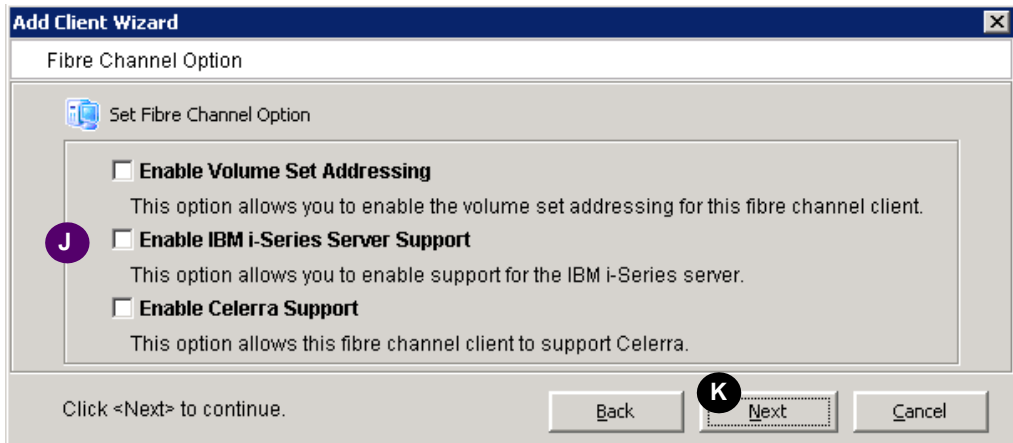
Click <Next> to continue.

D Back Next Cancel

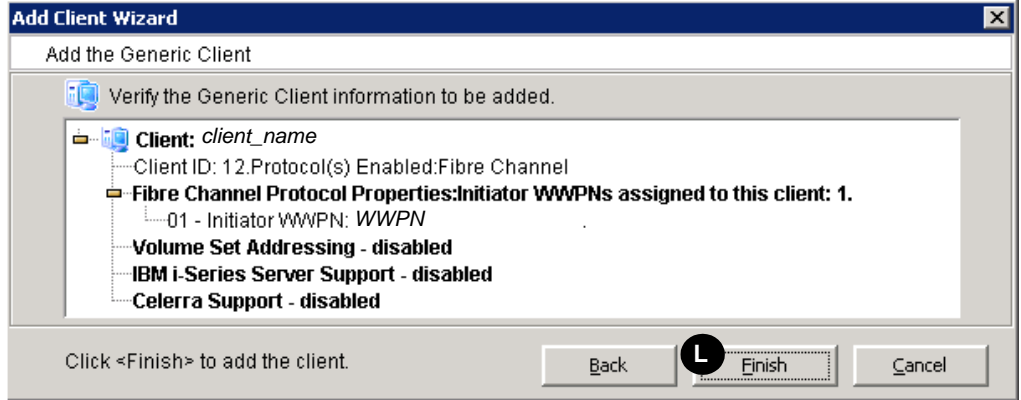
- When the Set Client Fibre Channel Properties property sheet appears, select the World Wide Port Name (WWPN) of the initiator by checking the corresponding check box (E below), or press the Add button (F), enter a new Initiator WWPN, and press OK (G). Then press Next (H).



- 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).



- When the Add the Generic Client summary screen appears, press Finish (L below) to add the client.

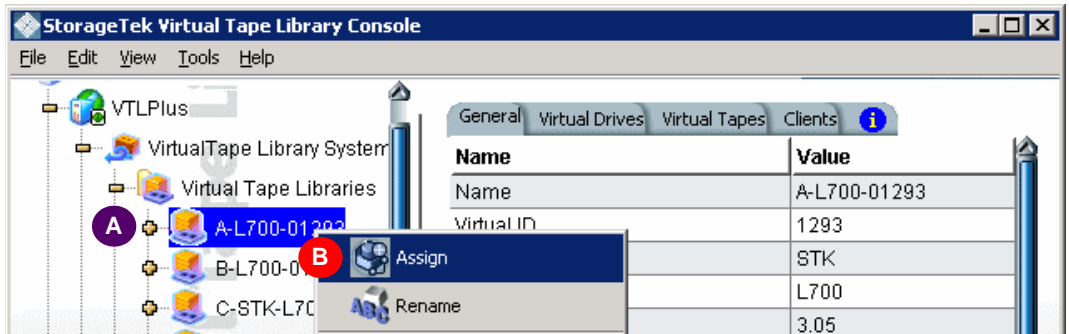


Next task: “Starting the Assign a Virtual Tape Library Wizard” on page 63.

▼ 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.

- 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).

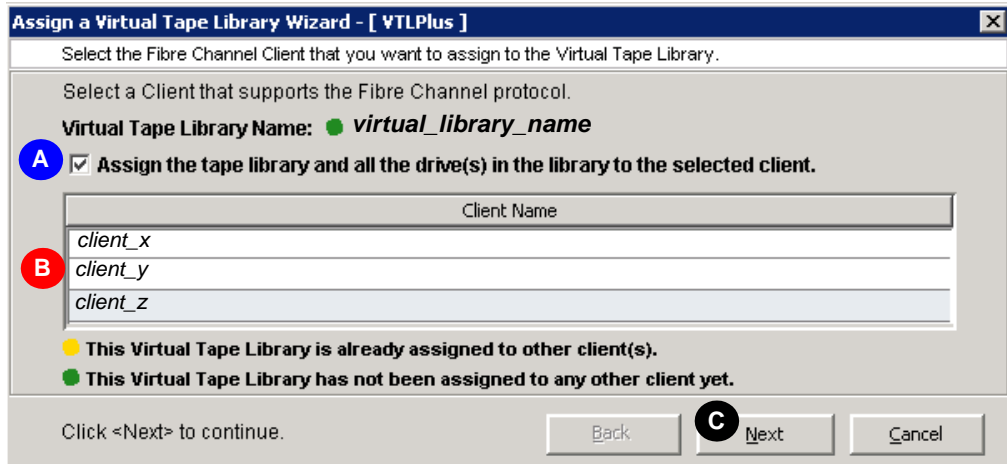


- Press Next (B above).

Next task: “Assigning virtual libraries to storage clients” on page 64

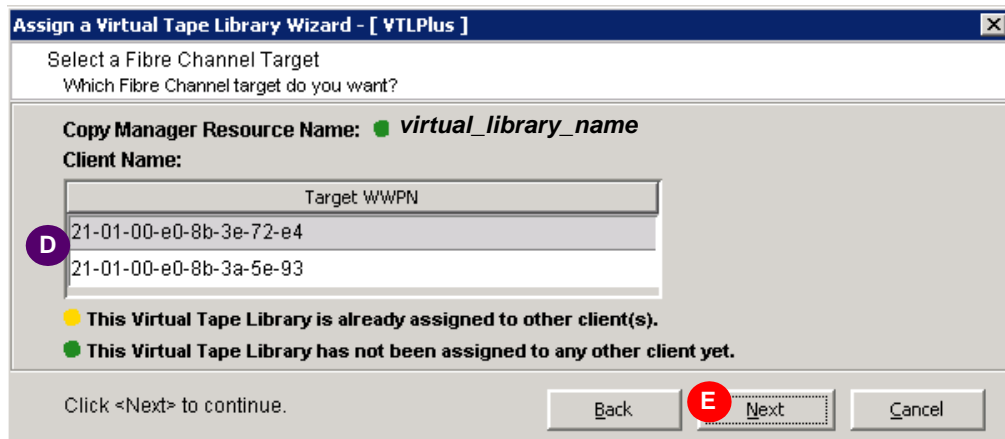
▼ Assigning virtual libraries to storage clients

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).

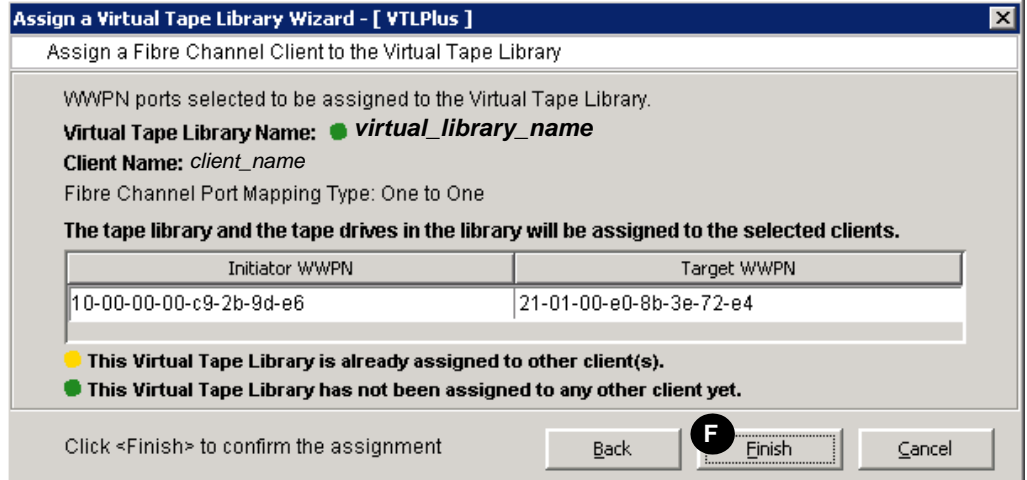


As a general rule, assign one library per client.

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).



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.

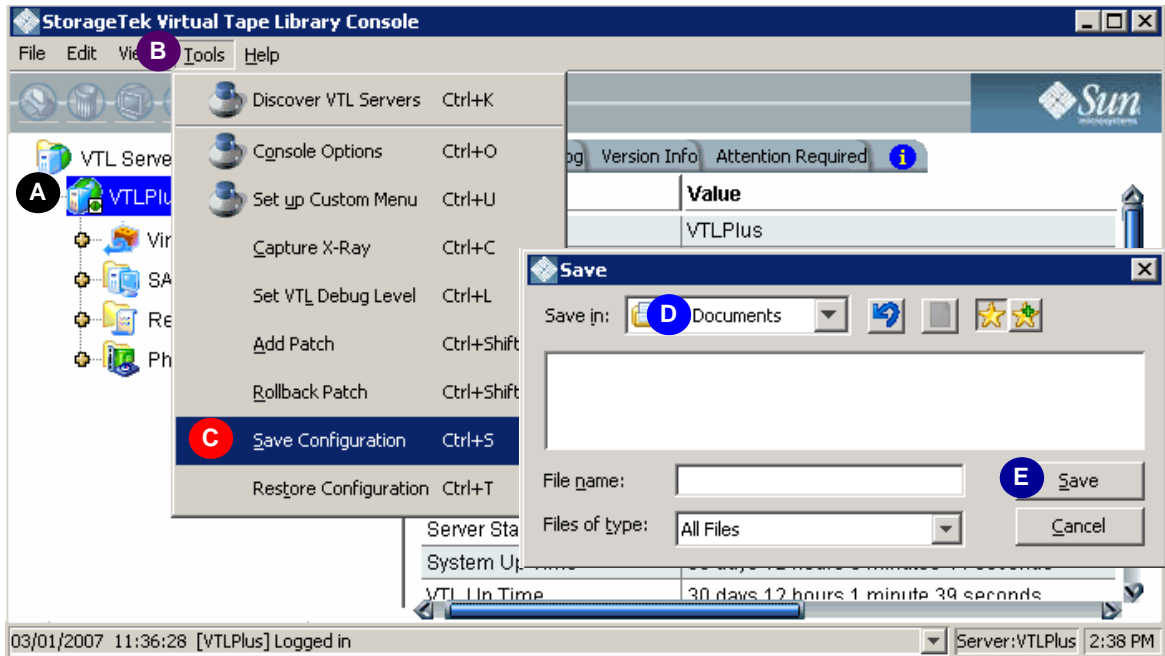
Backing up the VTL system configuration

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 66
- “Automatically backing up the VTL configuration” on page 66.

▼ Manually saving the VTL configuration

1. In the object tree of the VTL console, highlight the VTL server node (A below).



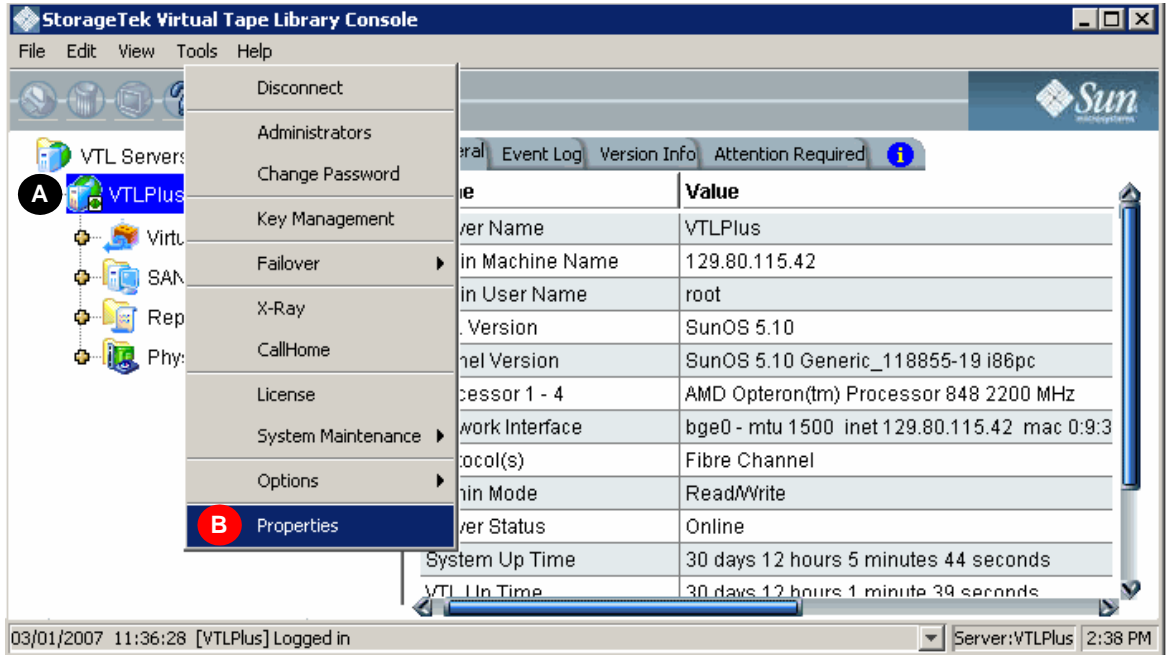
2. From the VTL main menu, select Tools (B above).
3. From the submenu, select Save Configuration (C above).
4. When the Save dialog appears, supply a filename (D above), and press Save (E).

Stop here.

▼ Automatically backing up the VTL configuration

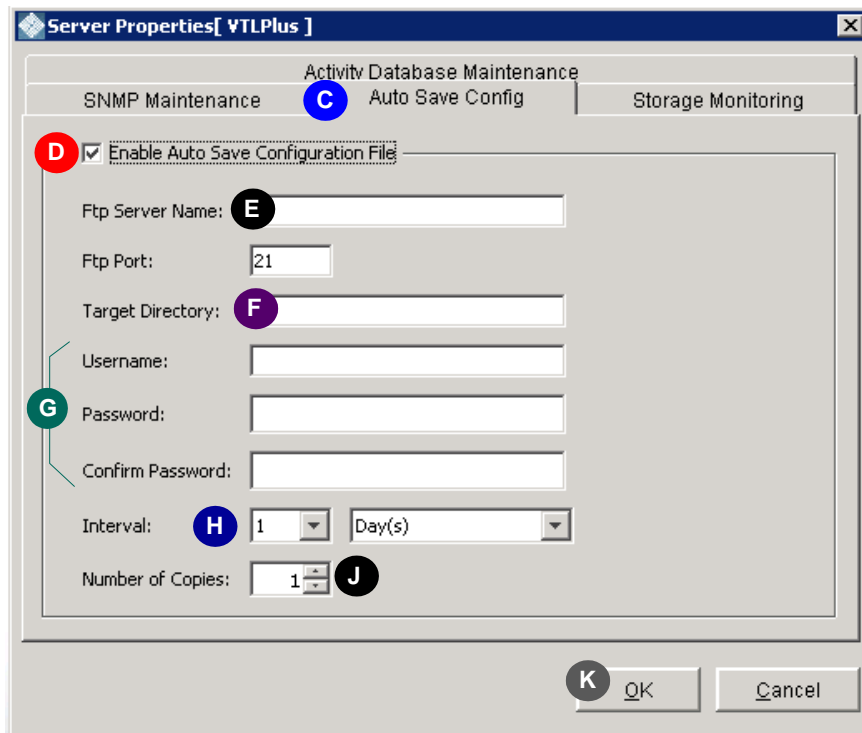
To insure that the VTL configuration is always protected, use the Auto Save feature to periodically create a point-in-time snapshot of the VTL configuration on another server.

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.

Notes:

- 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.

Protecting VTL metadata

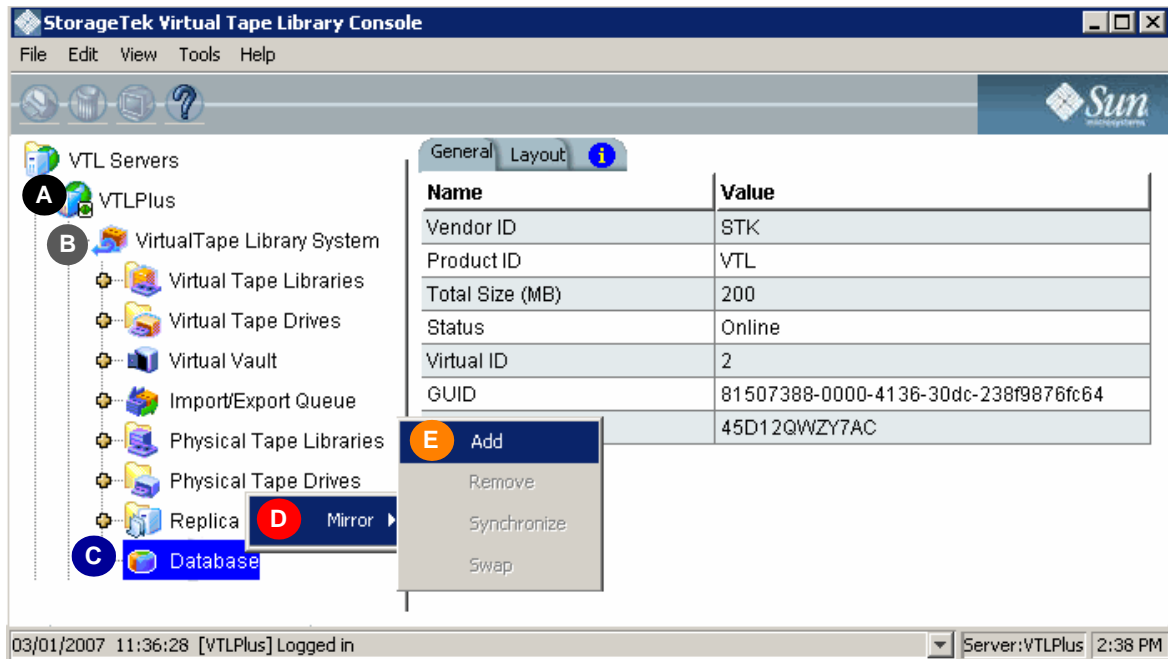
The VTL database holds the metadata that maps data stored on virtual tape to locations on the physical, random-access disk media. Without this critical information, virtual tape data cannot be recovered, so protecting it is essential.

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.

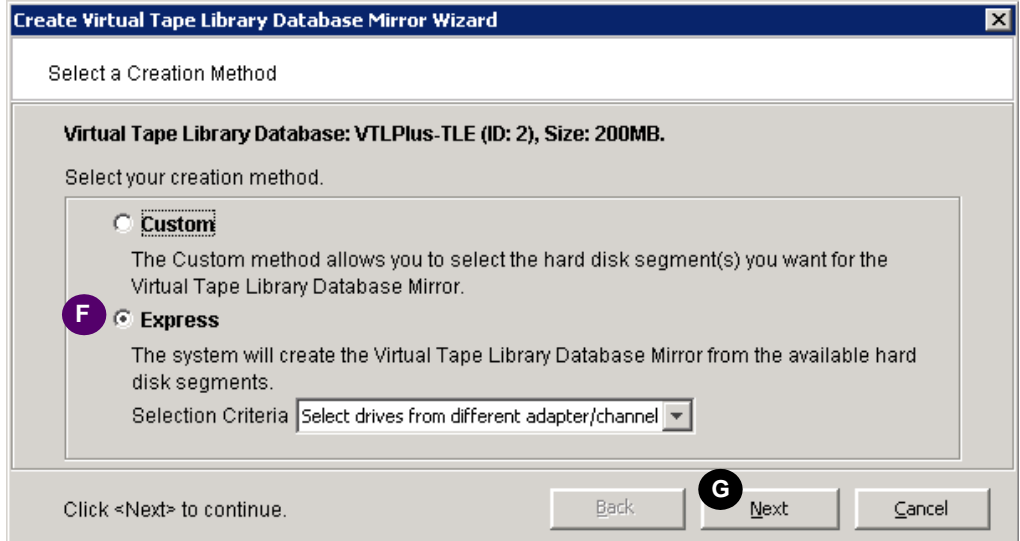
▼ Mirroring the VTL database

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).

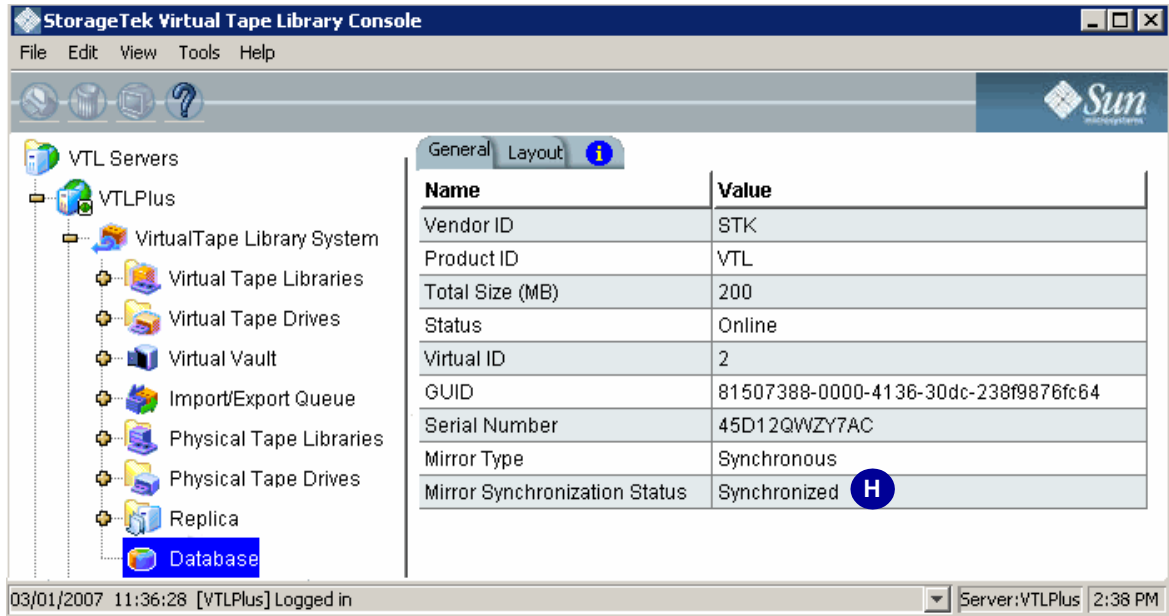
5. When the **Select a Creation Method** dialog appears, select **Express** (F below), and press **Next** (G).



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 accounts and passwords

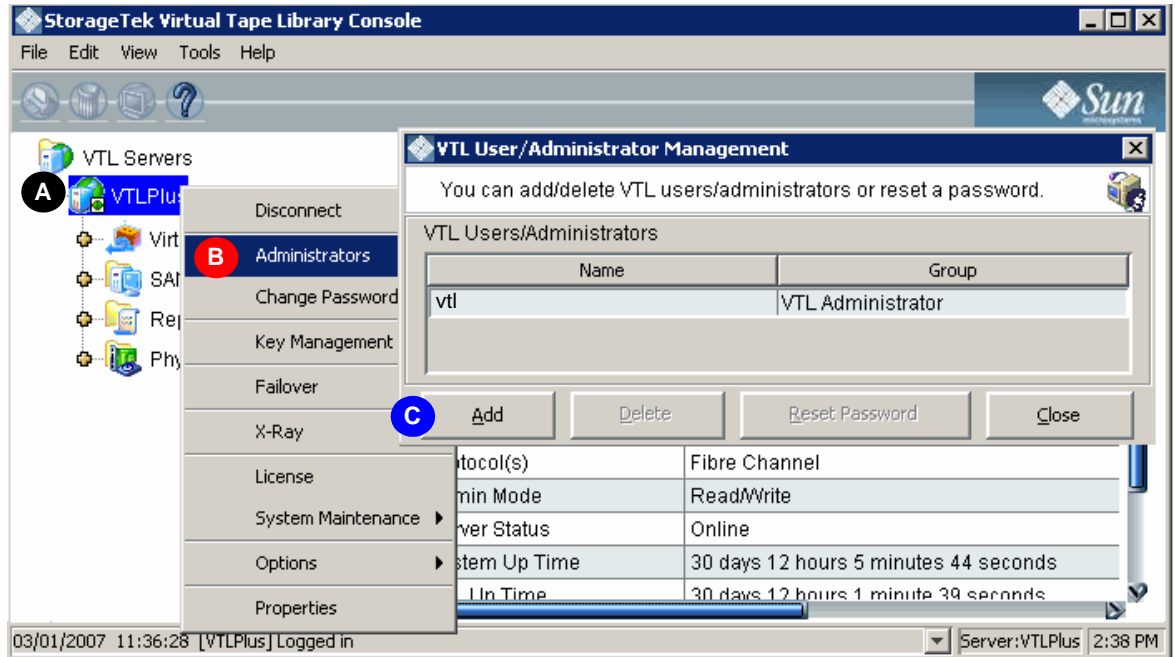
You can perform the following tasks from the VTL console:

- “Managing administrators” on page 73
- “Changing administrator passwords” on page 74.

▼ 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).

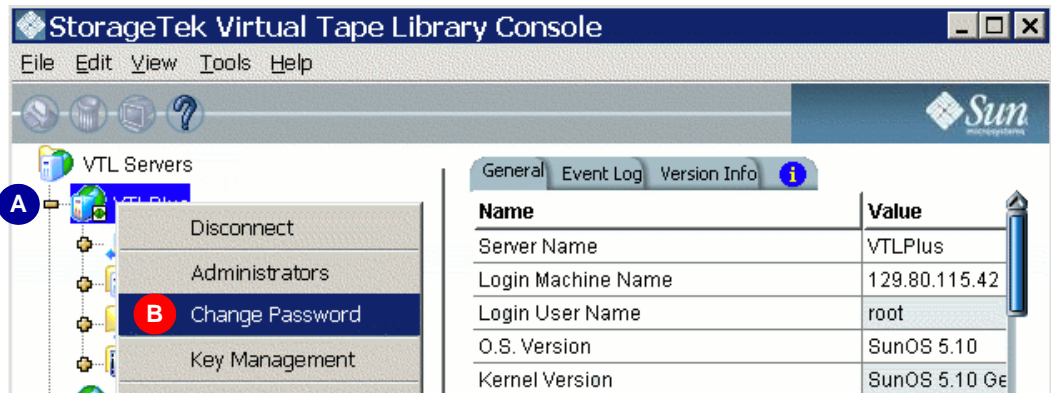
When you add an administrator, the name must adhere to the naming convention of the operating system running on your VTL Server. Refer to your operating system's documentation for naming restrictions.

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

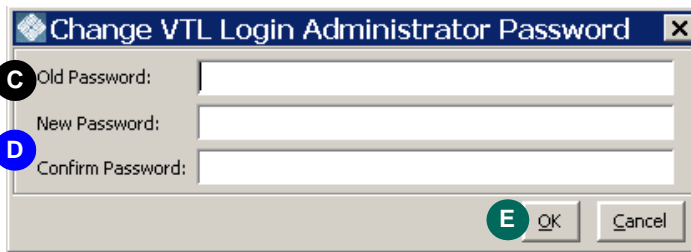
Stop here.

▼ 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.

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:

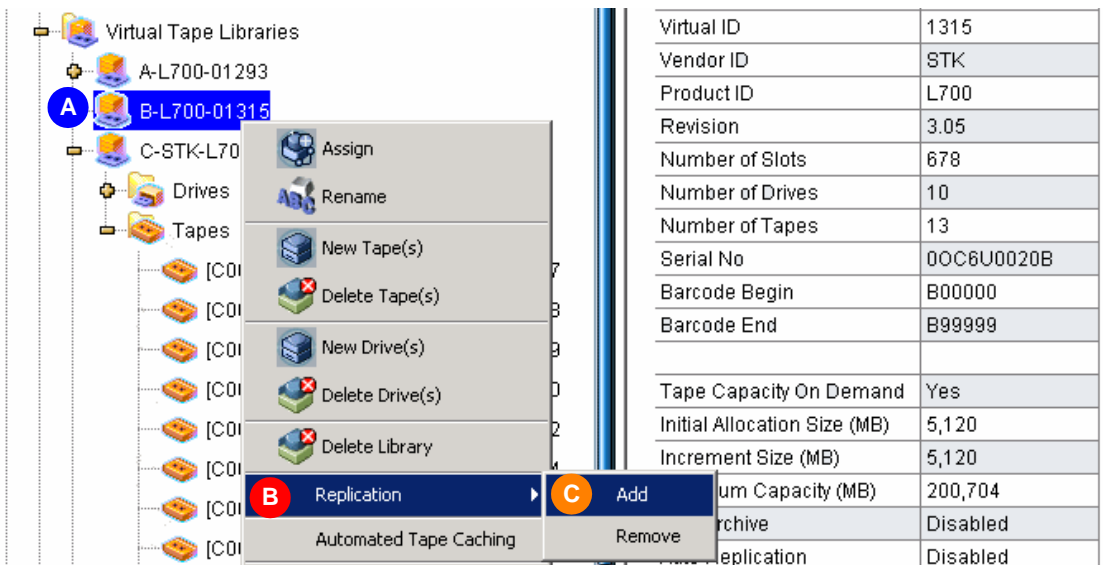
- “Setting up tape replication for multiple tapes” on page 75
- “Setting up replication for individual tapes” on page 81
- “Manually synchronizing replicas (manual replication)” on page 87
- “Stopping a replication that is already under way” on page 87
- “Manually synchronizing replicas (manual replication)” on page 87
- “Checking replication status from the target VTL server” on page 89
- “Checking replication status with a report” on page 89
- “Changing replication properties” on page 90
- “Deleting a replication configuration” on page 91
- “Promoting a replica resource” on page 91.

▼ Setting up tape replication for multiple tapes

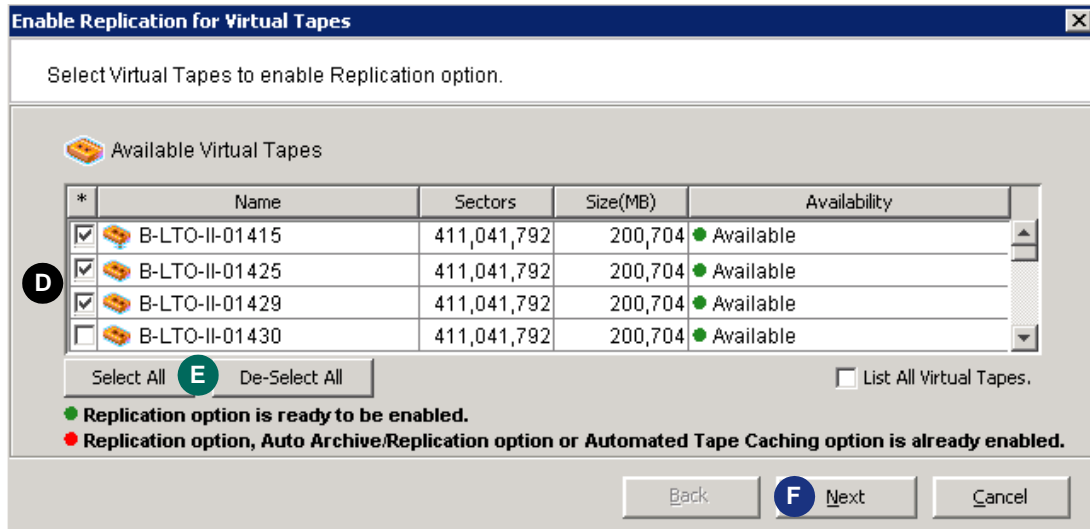
1. Before continuing, make sure that you have write access to both the primary (local) and target (remote) VTL servers and that there is enough space available on the target for the replica resources you intend to create.
2. In the object tree of the VTL console, expand the VTL server node.
3. Under 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).

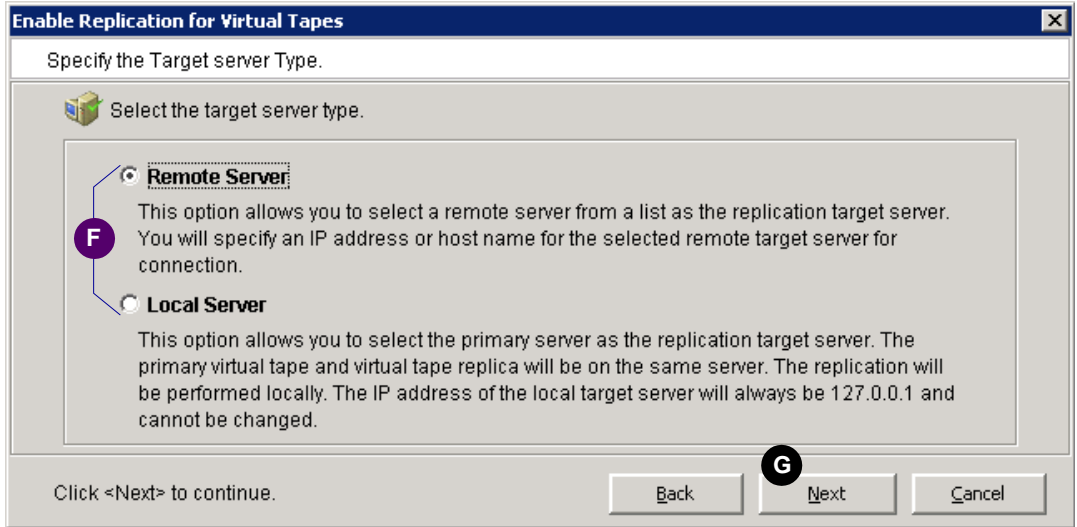
5. From the context menus, select Replication (B below), Add (C).



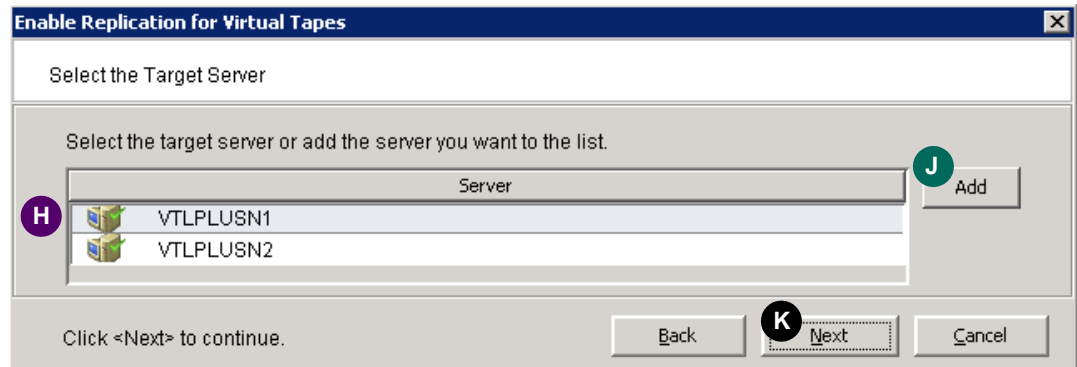
6. When the Select Virtual Tapes to enable Replication... panel appears, use the check boxes (D below) and/or selection buttons to select tapes (E). Press Next (F).



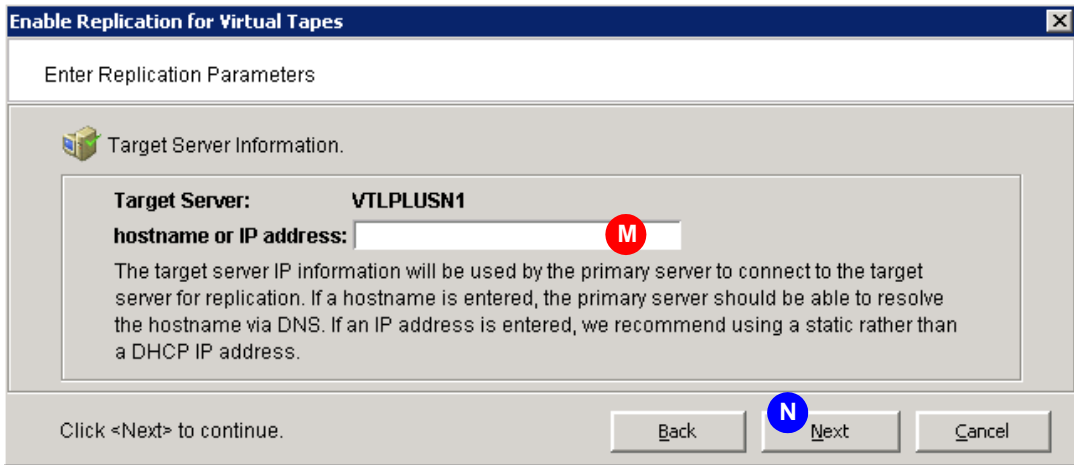
- When the Specify the Target server Type panel appears, click the radio button for a Remote or Local Server (G below). Then press Next (H).



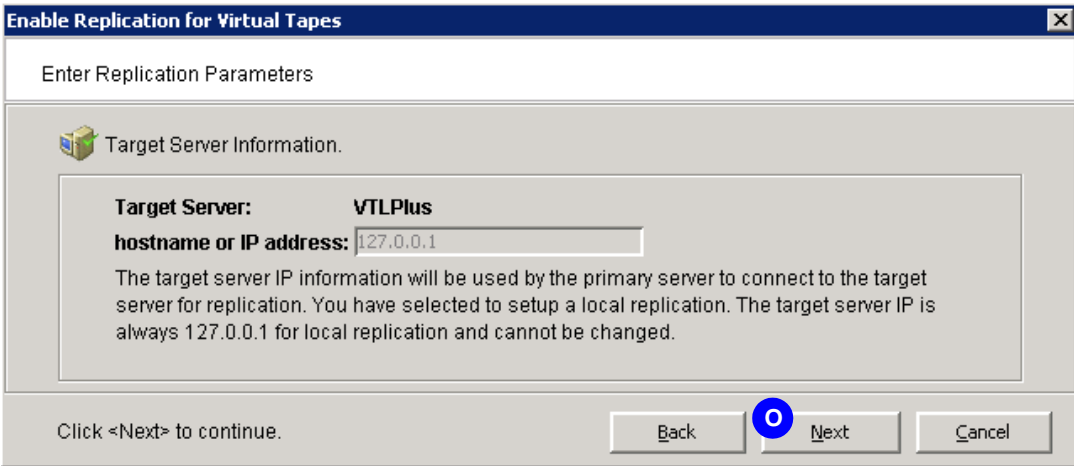
- When the Select Target Server panel appears, use the list (J below) to select or server or press Add (K) to add one to the list. Press Next (L).



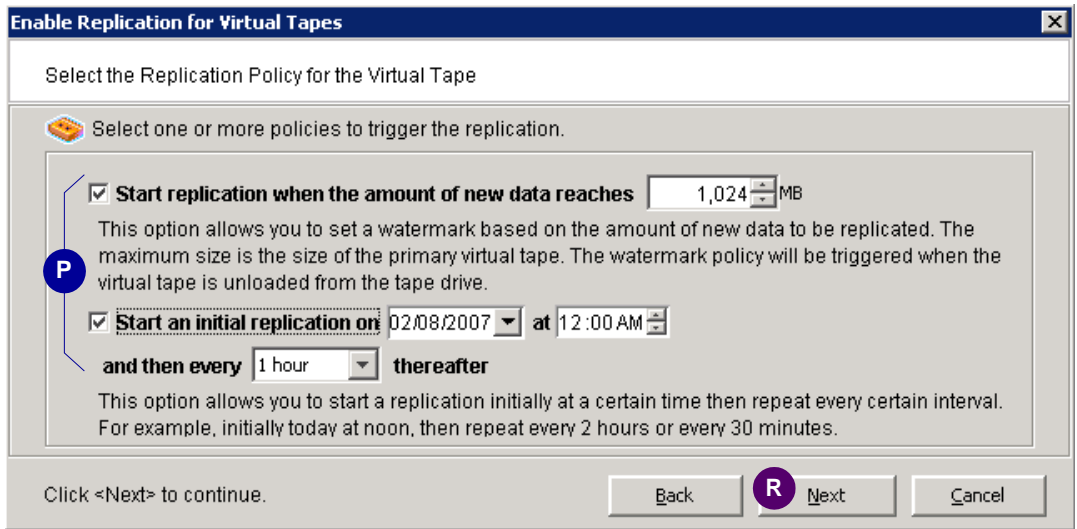
9. If you chose the **Remote Server** option above, in Step 7, edit the IP address of the remote VTL server in the space provided (M below), if necessary, then press Next (N).



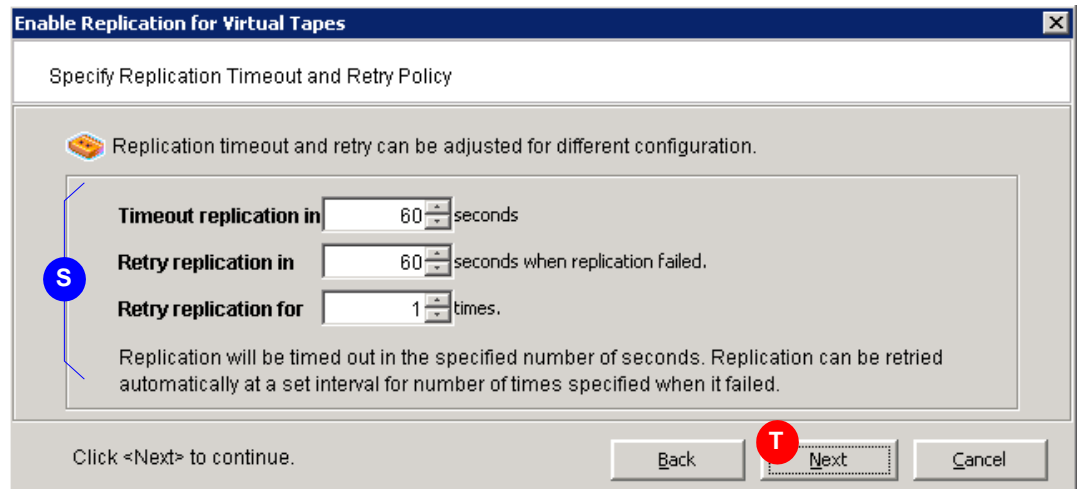
10. If you chose the **Local Server** option above, in Step 7, press Next (O below).



- 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)**.

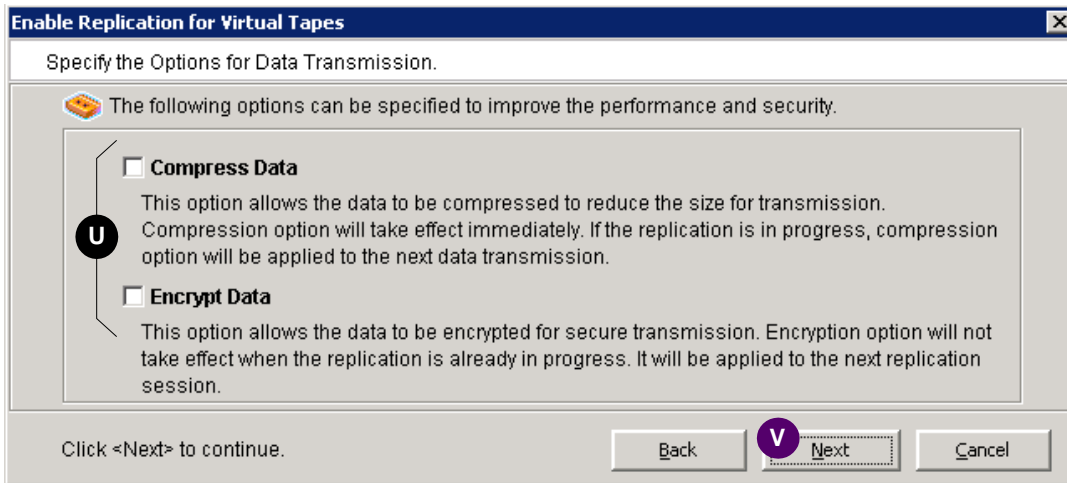


- When the **Select the Replication Timeout and Retry Policy** panel appears, use the **spinner controls** provided to define the policy you want to apply (S below). Press **Next (T)**.

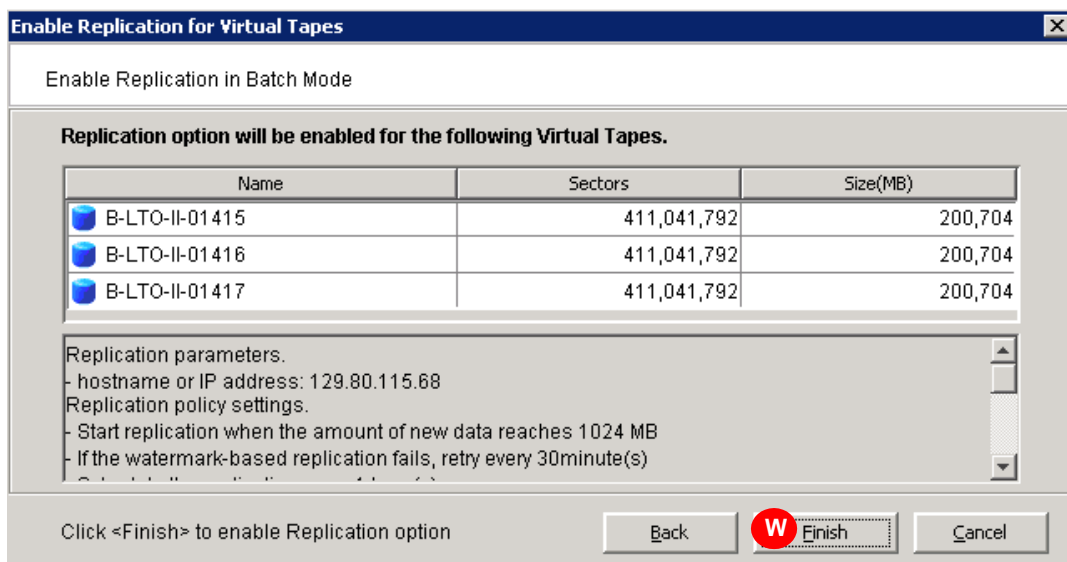


13. When the Specify the Options for Data Transmission panel appears, use the check boxes provided to select the options you want to use (U below). Press Next (V).

Remember that compression and encryption are CPU-intensive software processes that reduce system throughput. Use them judiciously, when necessary.



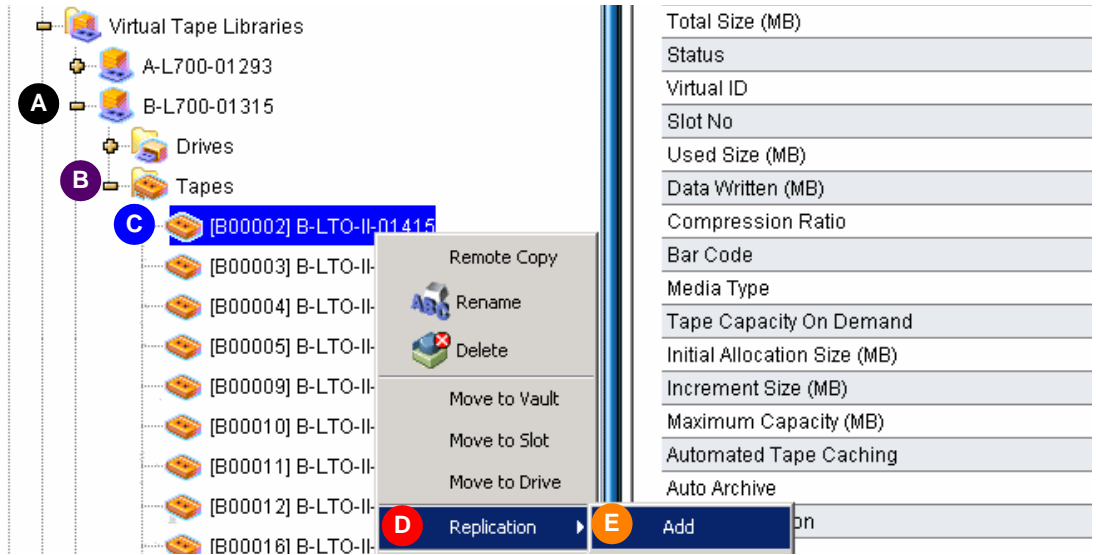
14. When the confirmation panel appears, press Finish (W below).



Stop here.

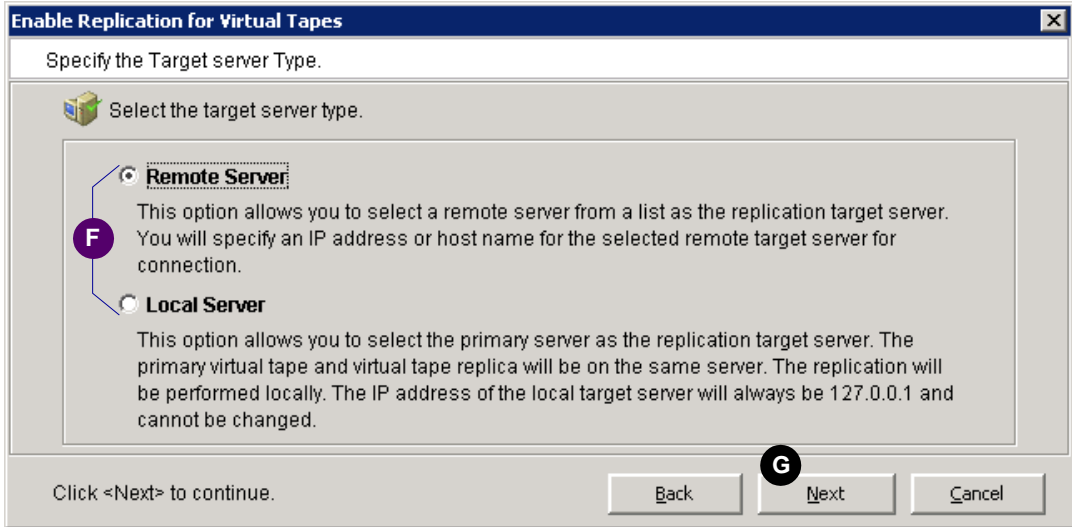
▼ Setting up replication for individual tapes

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), and open the Tapes node (B).

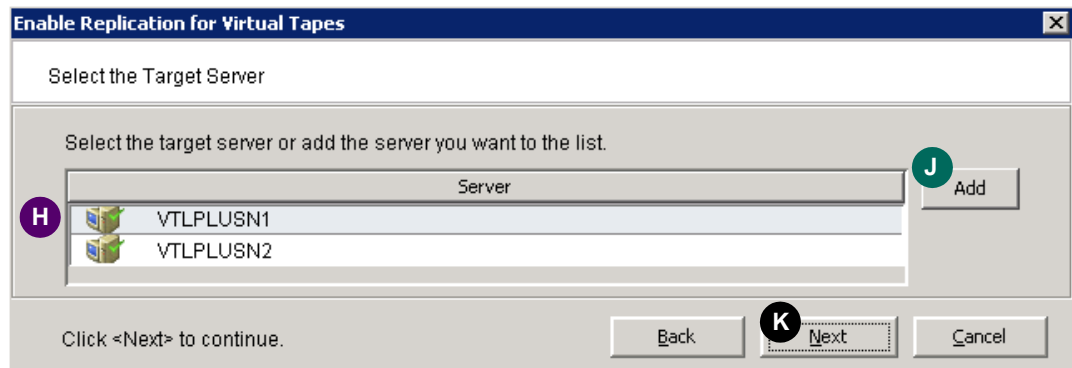


3. Right-click on the virtual tape for which you want to enable replication (C above).
4. From the context menus, select Replication (D above), then select Add (E).

- 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).



- 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).



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 [X]

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).

Enable Replication for Virtual Tapes [X]

Enter Replication Parameters

Target Server Information.

Target Server: VTLPlus

hostname or IP address:

The target server IP information will be used by the primary server to connect to the target server for replication. You have selected to setup a local replication. The target server IP is always 127.0.0.1 for local replication and cannot be changed.

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

- 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)**.

Enable Replication for Virtual Tapes

Select the Replication Policy for the Virtual Tape

Select one or more policies to trigger the replication.

N **Start replication when the amount of new data reaches** 1,024 MB
 This option allows you to set a watermark based on the amount of new data to be replicated. The maximum size is the size of the primary virtual tape. The watermark policy will be triggered when the virtual tape is unloaded from the tape drive.

Start an initial replication on 02/08/2007 **at** 12:00 AM
and then every 1 hour **thereafter**
 This option allows you to start a replication initially at a certain time then repeat every certain interval. For example, initially today at noon, then repeat every 2 hours or every 30 minutes.

Click <Next> to continue.

Back **P** Next Cancel

- 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)**.

Enable Replication for Virtual Tapes

Specify Replication Timeout and Retry Policy

Replication timeout and retry can be adjusted for different configuration.

Q **Timeout replication in** 60 seconds

Retry replication in 60 seconds when replication failed.

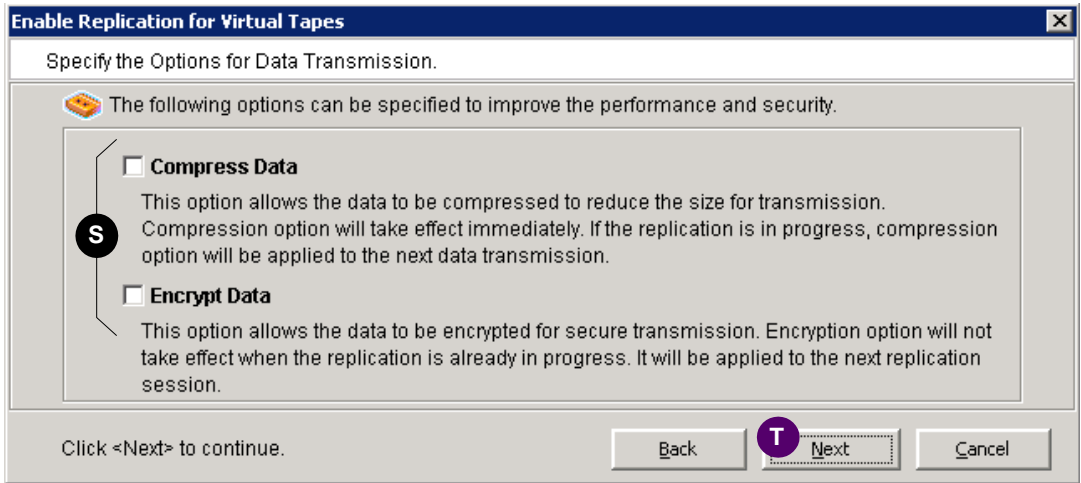
Retry replication for 1 times.

Replication will be timed out in the specified number of seconds. Replication can be retried automatically at a set interval for number of times specified when it failed.

Click <Next> to continue.

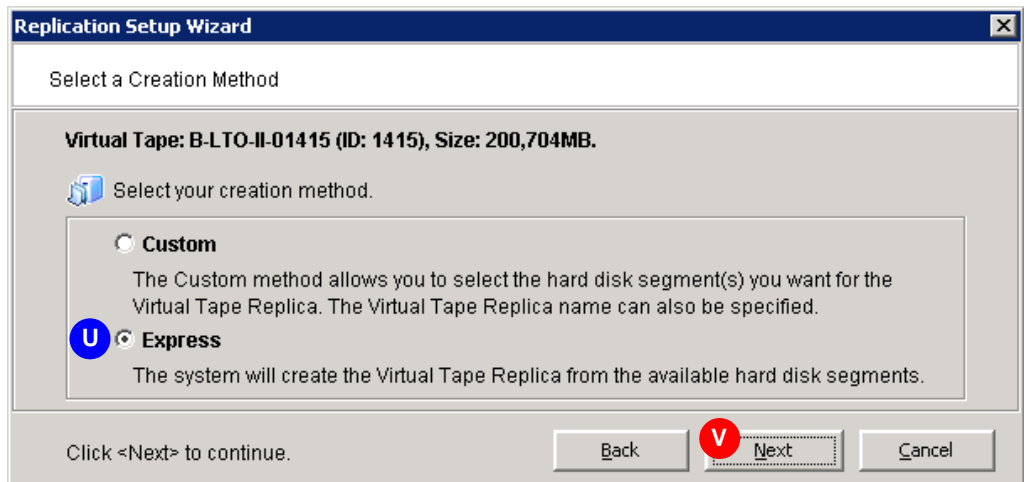
Back **R** Next Cancel

- 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).



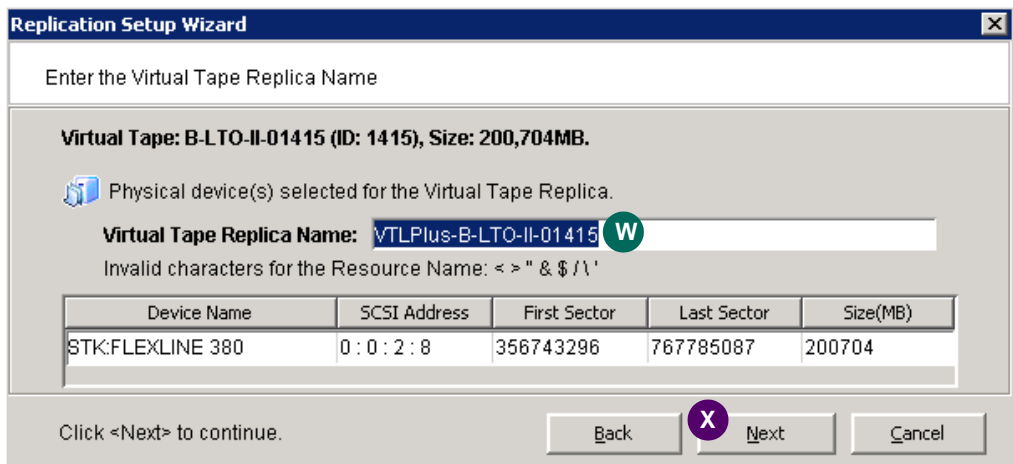
Remember that compression and encryption are CPU-intensive software processes that reduce system throughput. Use them judiciously, when necessary.

- When the Select a Creation Method panel appears, click the Express radio button (U below), and press Next (V).

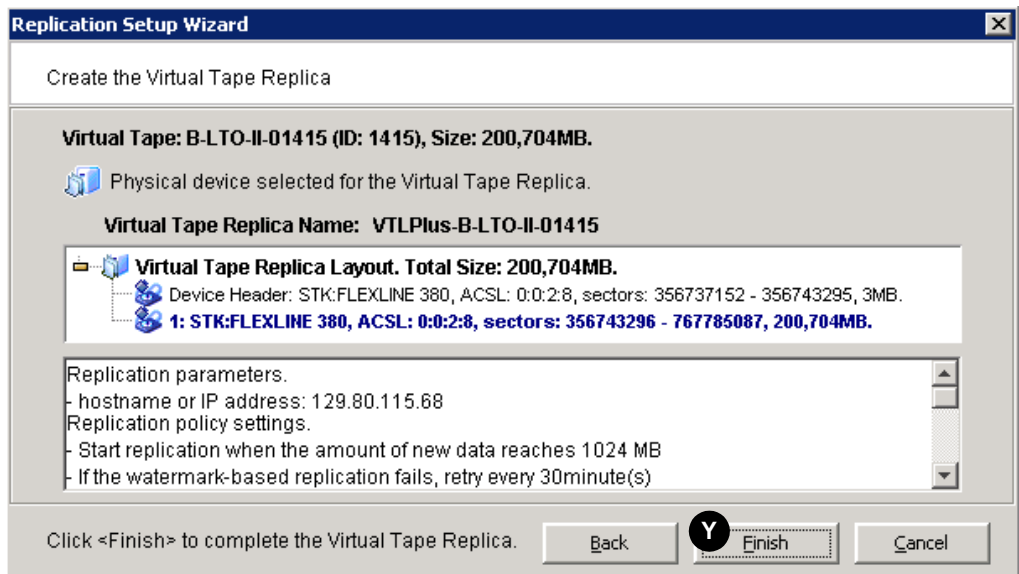


The Sun StorageTek VTL appliance includes an integrated RAID device, so there is no advantage to manually selecting target volumes using the Custom method. The Custom method may also result in load balancing problems and significantly greater management overhead.

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).



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.

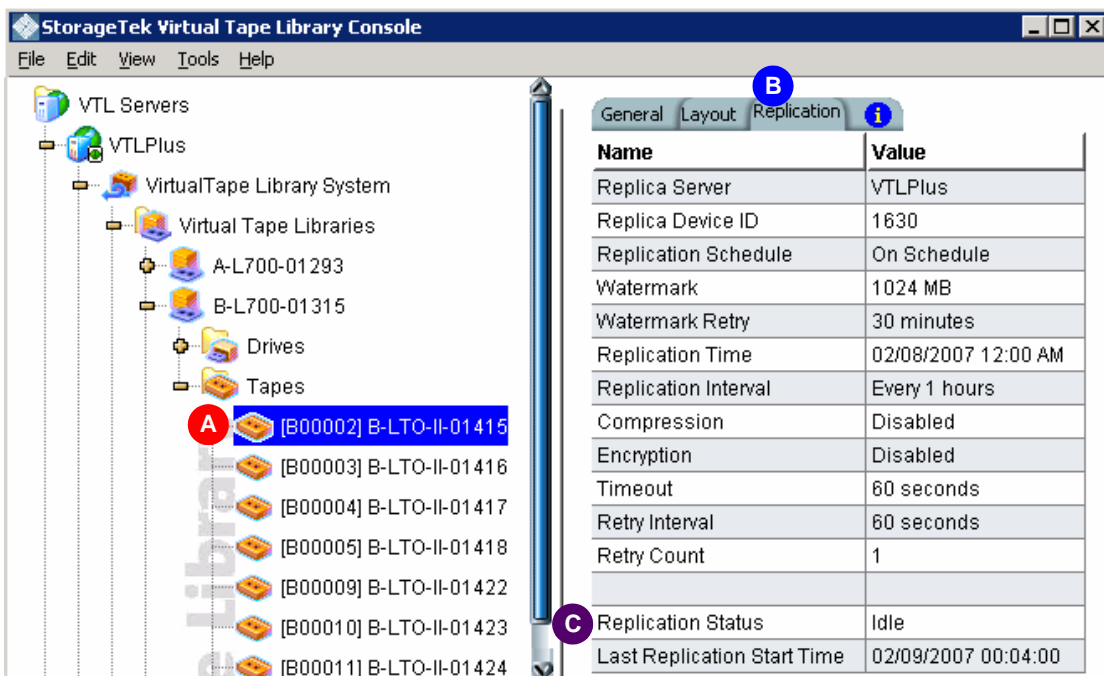
▼ Stopping a replication that is already under way

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).



The screenshot shows the StorageTek Virtual Tape Library Console interface. On the left, the object tree is expanded to show the 'Tapes' folder under the 'Virtual Tape Libraries' node. The primary virtual tape '[B00002] B-LTO-II-01415' is selected and highlighted in blue, with a red circle 'A' next to it. On the right, the 'Replication' tab is selected in the properties sheet, with a blue circle 'B' above it. The 'Replication Status' row is highlighted in the table, with a purple circle 'C' next to it.

Name	Value
Replica Server	VTLPlus
Replica Device ID	1630
Replication Schedule	On Schedule
Watermark	1024 MB
Watermark Retry	30 minutes
Replication Time	02/08/2007 12:00 AM
Replication Interval	Every 1 hours
Compression	Disabled
Encryption	Disabled
Timeout	60 seconds
Retry Interval	60 seconds
Retry Count	1
Replication Status	Idle
Last Replication Start Time	02/09/2007 00:04:00

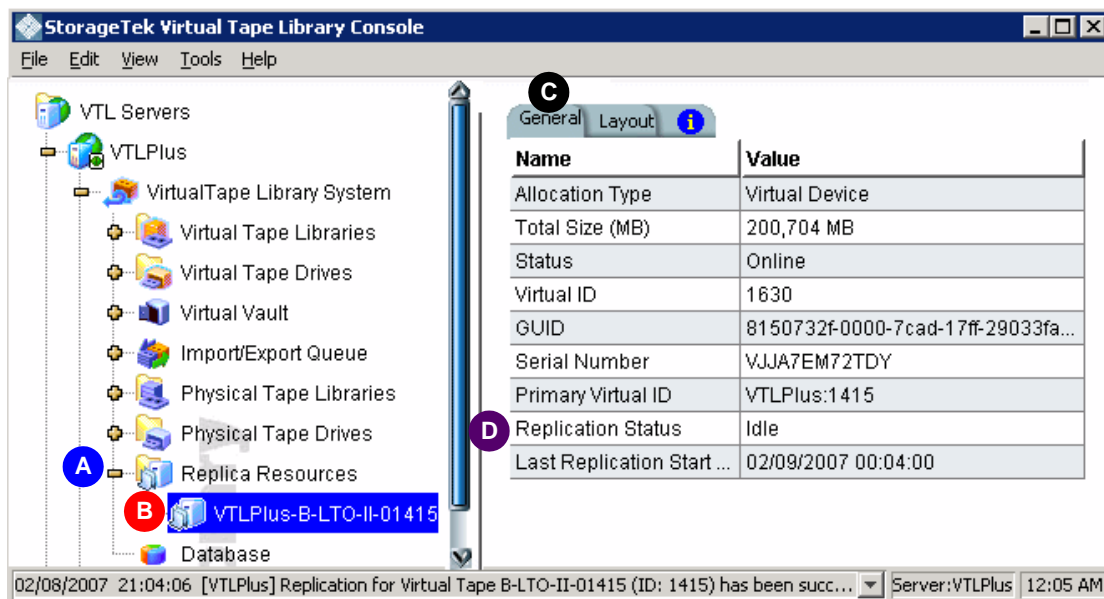
2. In the properties sheet at the right, select the Replication tab (B above).

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 111 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.

Replication Status

Replication Status Report

Primary Server: *server_name*, TAPE Resources
12/23/2006 - 12/23/2006

Report Date: 12/23/2006
 Report Sort: Sort by target server name, then by target disk name, then by log date and time.

Primary Server: *server_name* (*nnn.nnn.nnn.nnn*)
 Primary Disk: VirtualTape-00160 (ID: 160)
 Target Server: *target_name* (*ppp.ppp.ppp.ppp*)
 Target Disk: STK:FLEXLINE380

Policy: Watermark: 100 MB, Retry: 0 Minutes, Interval: 0 Hours, Replication Time: N/A

Log Time	Status	Last Replication Time	Repl. Data(KB)	Trigger	Next Repl. Time	Next Trigger
Year 2004	A					
06/23 15:58:27		Idle	06/23/04 15:58:25-06/23/04 15:58:26	5120 admin.		n/a

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:

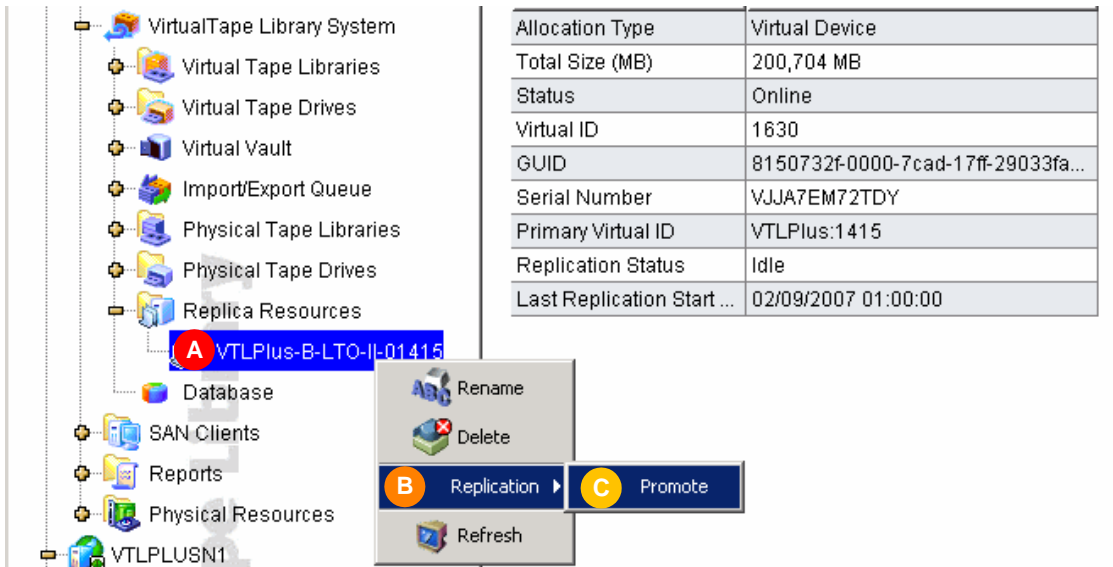
- move the virtual tape to a virtual library on the local server
- replicate the virtual tape back to the original source server.

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

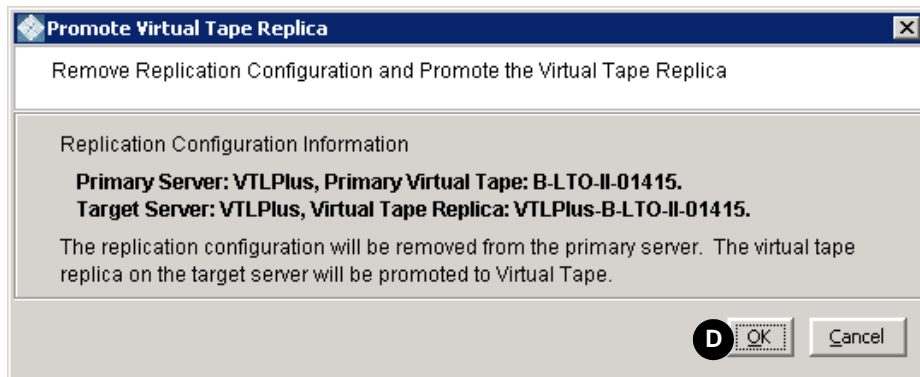
In order to maintain the integrity of restored data, the VTL software will not promote an invalid replica resource, such as a replica that has been damaged or left incomplete by a transmission fault. It will likewise refuse to promote a replica resource while a replication is still in progress.

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.

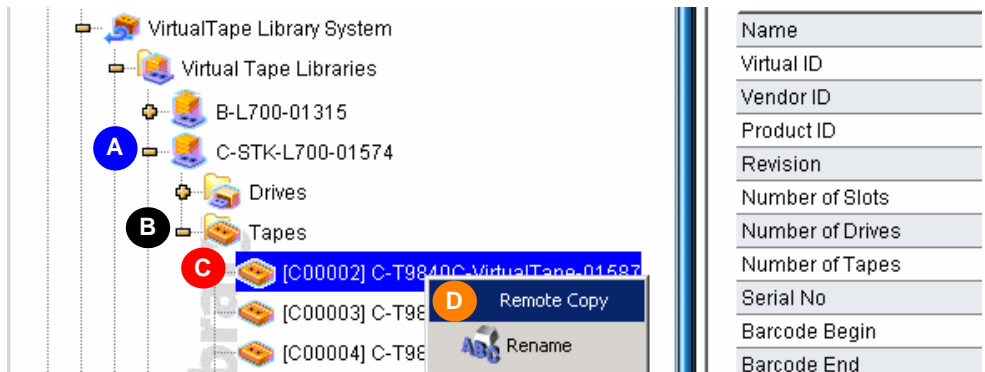
You can only copy tapes with barcodes that are not found on the remote server. If a copy exists and you wish to proceed, you must first delete the existing remote copy copy.

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

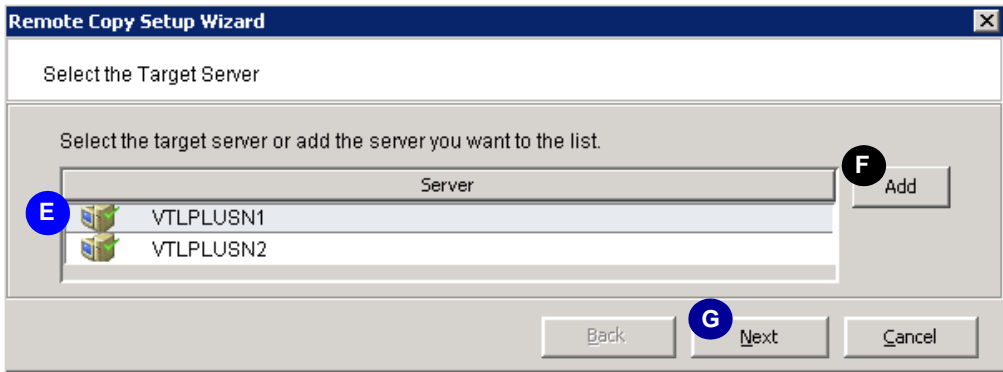
To copy tapes to a remote server, proceed as follows.

▼ Copying a tape to a remote server

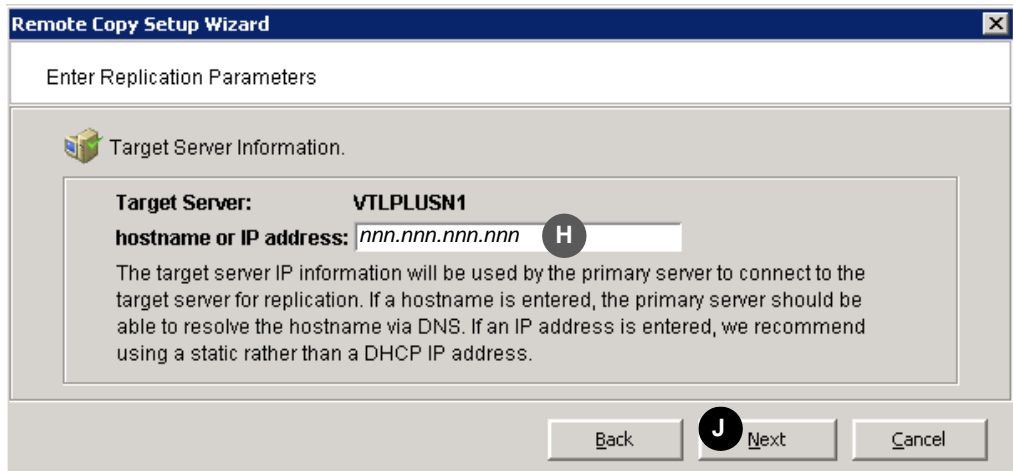
1. In the object tree of the VTL console, expand the VTL server node.
2. Under the VTL server, expand the Virtual Tape Library System and Virtual Tape Libraries nodes.
3. Under the Virtual Tape Libraries node, right-click on the virtual tape library that you want to enable (A below), and expand the Tapes node.
4. Right-click on the virtual tape that you want to copy (B below), and select Remote Copy from the context menu (D).



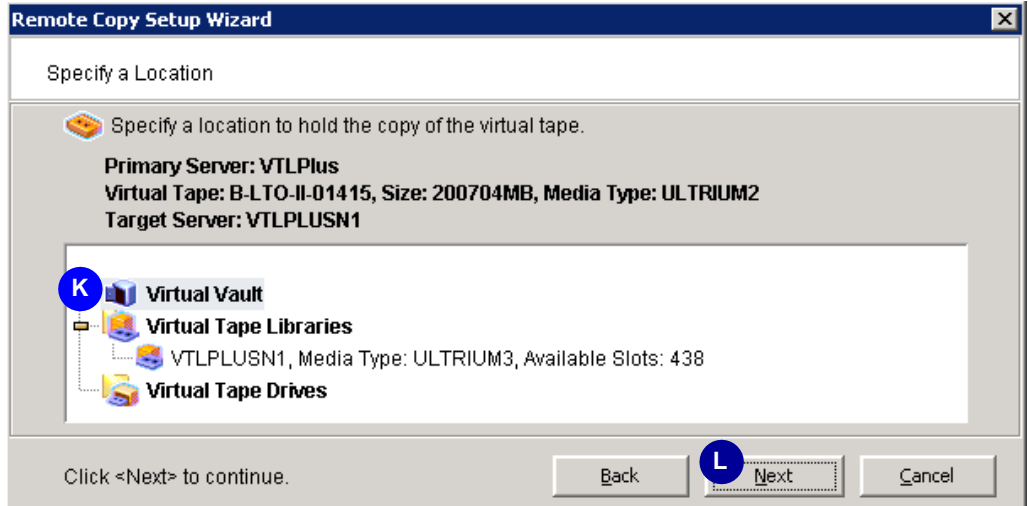
- When the **Select the Target Server** panel appears, use the list to select the server where you want to copy the tape (E below) or press **Add (F)** to add a server to the list. Then press **Next (G)**.



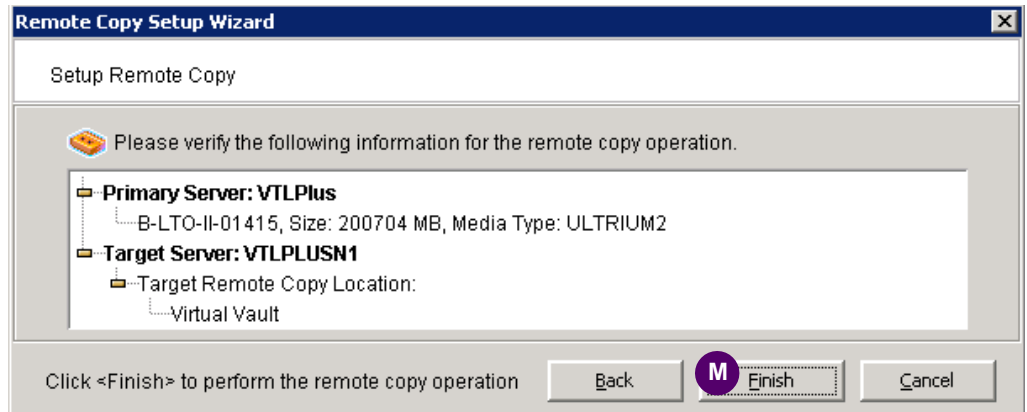
- When the **Enter Replication Parameters** panel appears, edit the IP address if necessary (H below), then press **Next (J)**.



- When the Specify a Location panel appears, select a location on the remote server (K below), and press Next (L).



- 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.

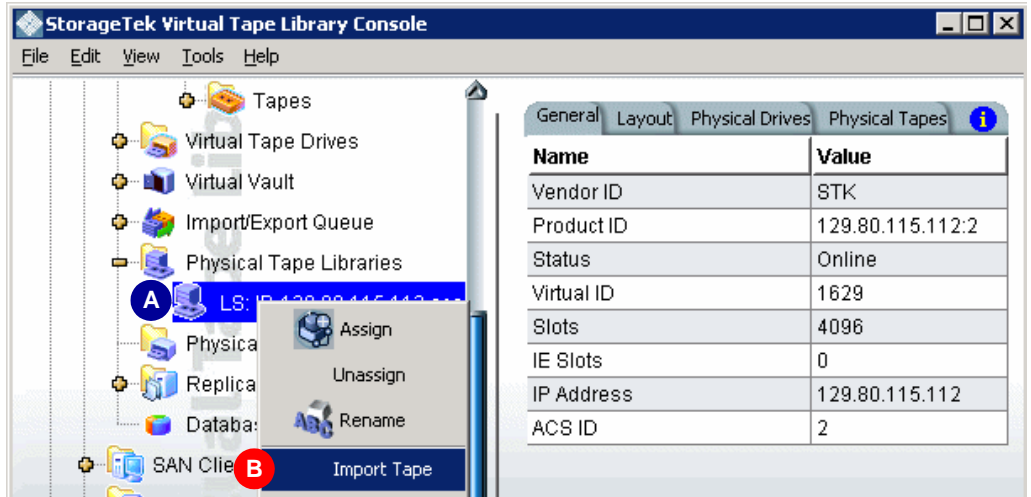
Up to 32 import/export jobs can run concurrently, although, in practice, this is generally limited to something less by the number of physical tape drives available on the attached library.

This section holds instructions for the following tasks:

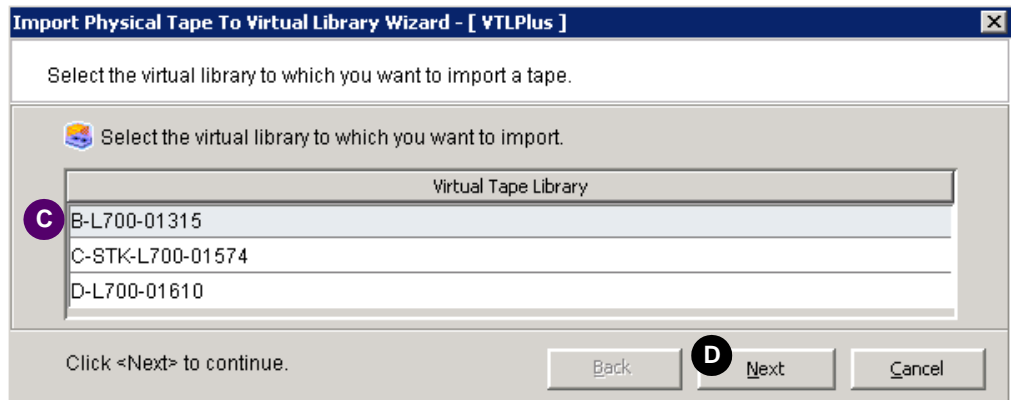
- "Importing a physical tape into a virtual library" on page 97
- "Importing cartridges in an IBM iSeries environment" on page 103
- "Exporting virtual tape to physical tape" on page 103
- "Exporting cartridges to the virtual vault in an IBM iSeries environment" on page 107.

▼ 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 menu (B).

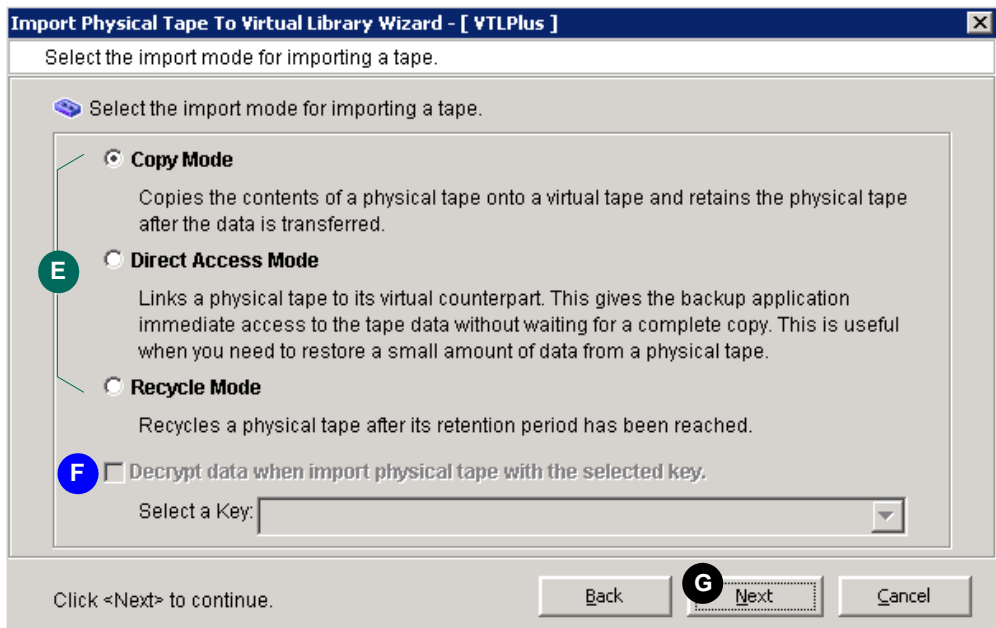


2. When the **Select virtual library ...** panel appears, use the list to select a virtual library that holds volumes of the same capacity as the volume you want to import (C below). Press **Next** (D).



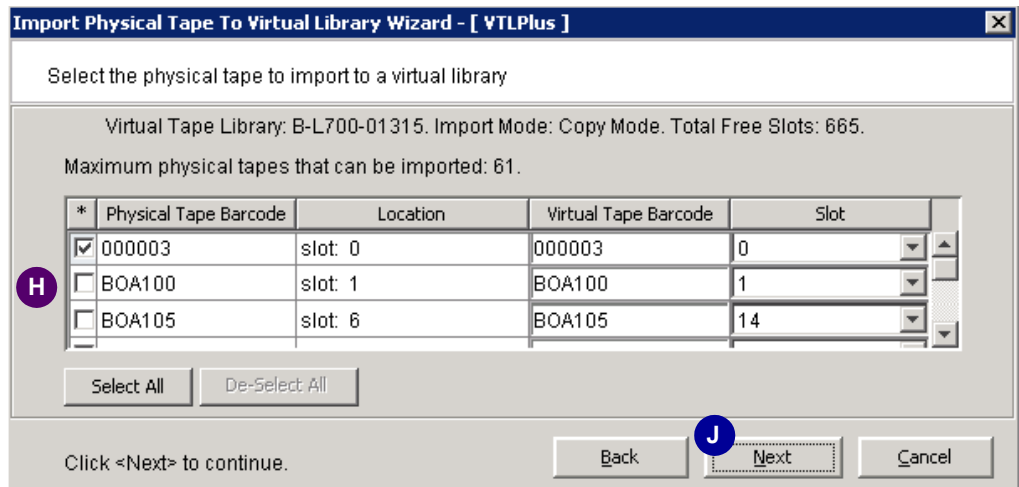
VTL exports tapes to like media only. You cannot export to a dissimilar physical tape.

3. When the **Select the import mode ...** panel appears, click the radio button that corresponds to the behavior you want (E below).



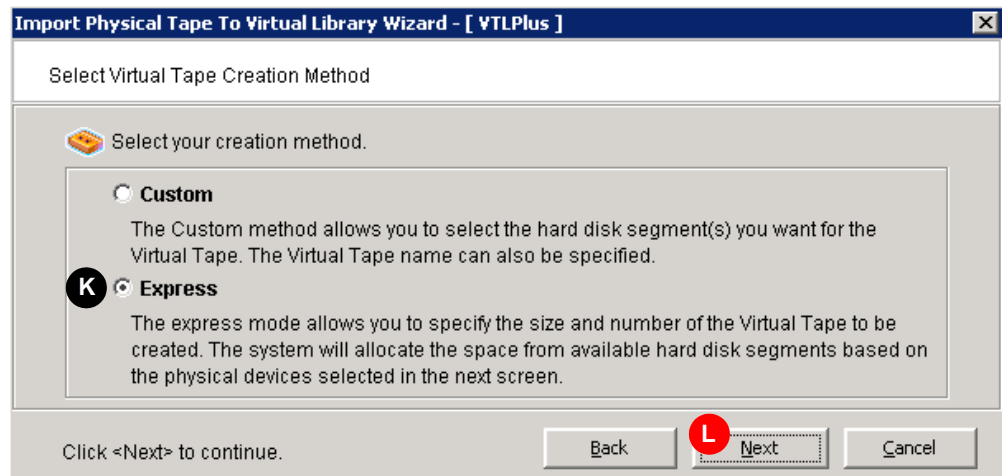
4. If the tape is encrypted and you wish to decrypt it, check the **Decrypt data ...** check box (F above), and enter the correct key.
 If the data was not previously encrypted, imported data is unusable. If you supply an incorrect key or if you enter an invalid password when challenged, the imported data is not decrypted.
5. Press **Next** (G above).

- 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.

- 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)**.

The screenshot shows the 'Select Physical Devices' panel. It includes a title bar, a close button, and a header 'Select Physical Devices'. Below the header, there is an instruction: 'Select Virtualized physical devices to be used to create Virtual Tapes in batch.' Two summary lines are present: 'Total Available Space: 2,731,202 MB (5,593,500,288 sectors).' and 'Total Selected Space: 2,731,202 MB (5,593,500,288 sectors).' A table lists four devices, each with a checked checkbox. A blue circle with the letter 'M' is positioned to the left of the table. Below the table are 'Select All' and 'De-Select All' buttons. At the bottom, there is a 'Click <Next> to continue.' instruction, a 'Back' button, a 'Next' button with a blue circle and 'N' above it, and a 'Cancel' button.

* <input checked="" type="checkbox"/>	Device Name	SCSI Address	Size(MB)	Sectors	Sector Size
<input checked="" type="checkbox"/>	STK:OPENstorage ...	4 : 0 : 1 : 0	9,210	18,861,952	512
<input checked="" type="checkbox"/>	STK:OPENstorage ...	8 : 0 : 1 : 7	32,515	66,590,592	512
<input checked="" type="checkbox"/>	STK:OPENstorage ...	8 : 0 : 1 : 11	317,094	649,408,384	512
<input checked="" type="checkbox"/>	STK:OPENstorage ...	10 : 0 : 1 : 4	114,441	234,375,040	512

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).

The screenshot shows the 'Specify Batch Mode Information' panel. It includes a title bar, a close button, and a header 'Specify Batch Mode Information'. Below the header, there is an instruction: 'Enter the information required to create the Virtual Tapes.' The 'Virtual Tape Name Prefix' field contains 'A-T9840C-' with a red circle and 'P' above it. Below this field is the text 'Invalid characters for the Resource Name: < > " & \$ / \ \''. The 'Virtual Tape Size' is set to '5 GB'. The 'Starting Number' is '1630' and the 'Number of Virtual Tapes' is '1 (Maximum: 533)'. A summary line reads 'Total Selected Space: 2,869,932 MB (5,877,620,096 sectors)'. A table lists three devices. At the bottom, there is a checked checkbox for 'Use default ID for Starting Number.' and three buttons: 'Back', 'Next', and 'Cancel'.

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

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).

Import Physical Tape To Virtual Library Wizard - [VTLPlus]

Specify Batch Mode Information

Enter the information required to create the Virtual Tapes.

Virtual Tape Name Prefix: A-T9840C-

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

Virtual Tape Size: Q 40 GB R

Starting Number: 1630 **Number of Virtual Tapes:** 1 (Maximum: 66) S

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

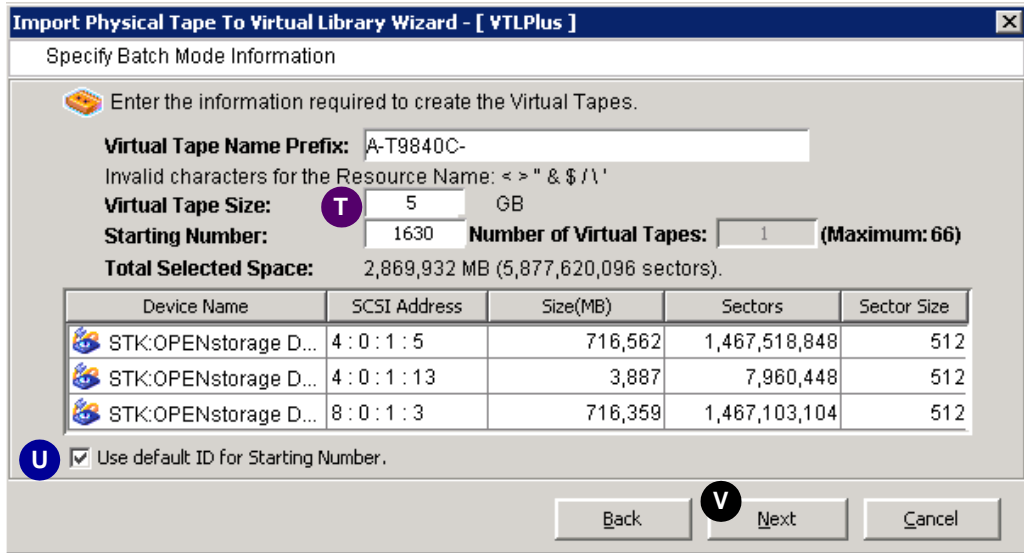
Device Name	SCSI Address	Size(MB)	Sectors	Sector Size
STK:OPENstorage D...	4 : 0 : 1 : 5	716,562	1,467,518,848	512
STK:OPENstorage D...	4 : 0 : 1 : 13	3,887	7,960,448	512
STK:OPENstorage D...	8 : 0 : 1 : 3	716,359	1,467,103,104	512

Use default ID for Starting Number.

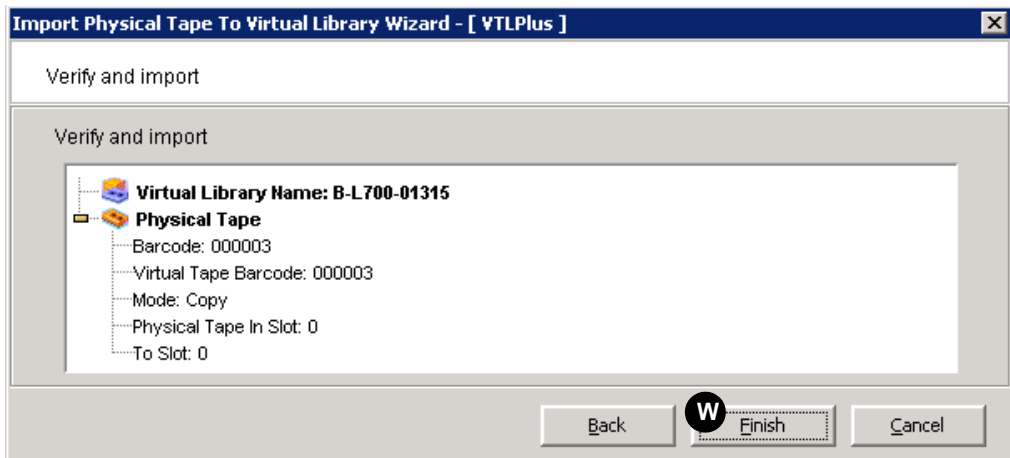
Back
Next
Cancel

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 103. 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 97.
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)
```

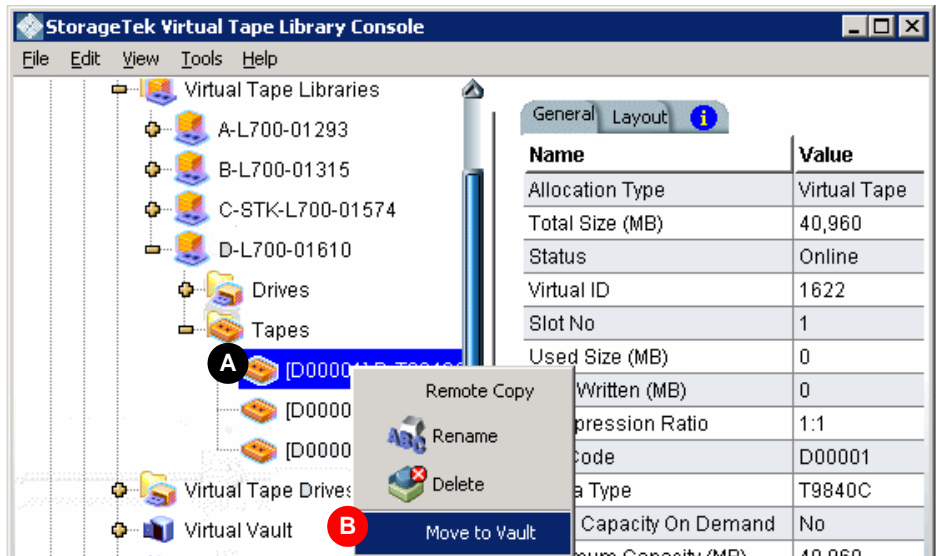
```
ADDTAPCTG DEV(library_device_name ) CTG(cartridge_identifier ) CGY(*SHARE400)
CHKVOL (*NO)
```

The tape status changes from INSERT to AVAILABLE.

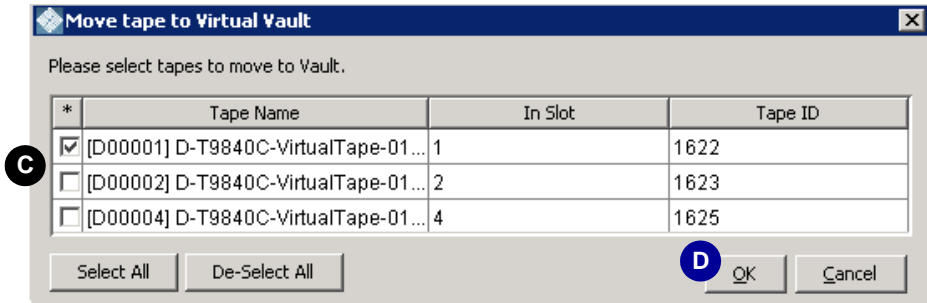
Stop here.

▼ Exporting virtual tape to physical tape

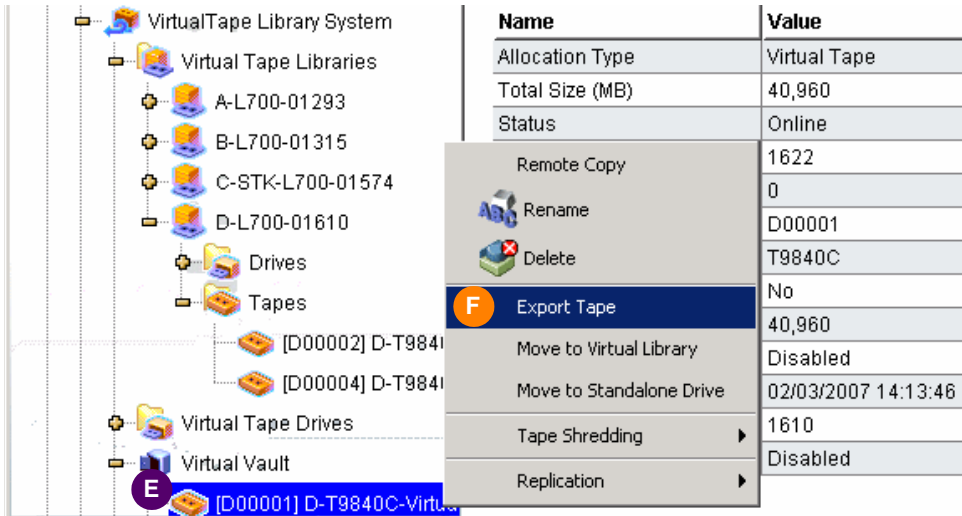
1. In the object tree of the VTL console, right-click on the virtual tape node that you want to export (A below), and select Move to Vault from the context menu (B).



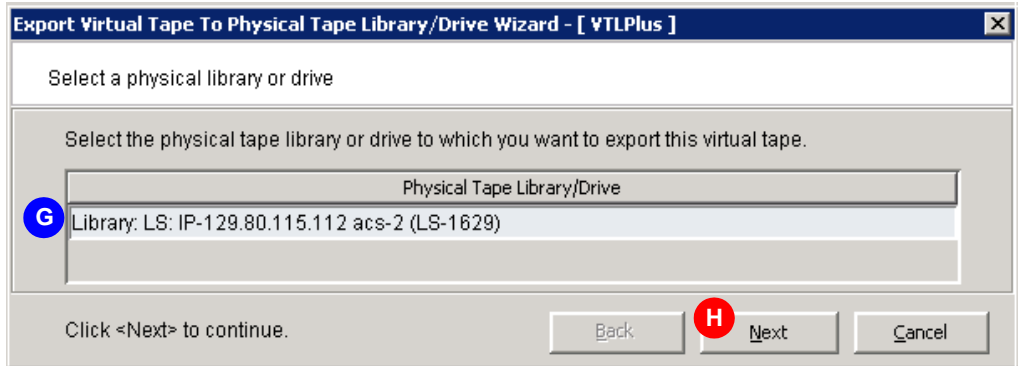
- When the Move Tape to Virtual Vault dialog appears, select the tape(s) that you want to move using the check boxes and/or selection buttons provided (C below). Press OK (D).



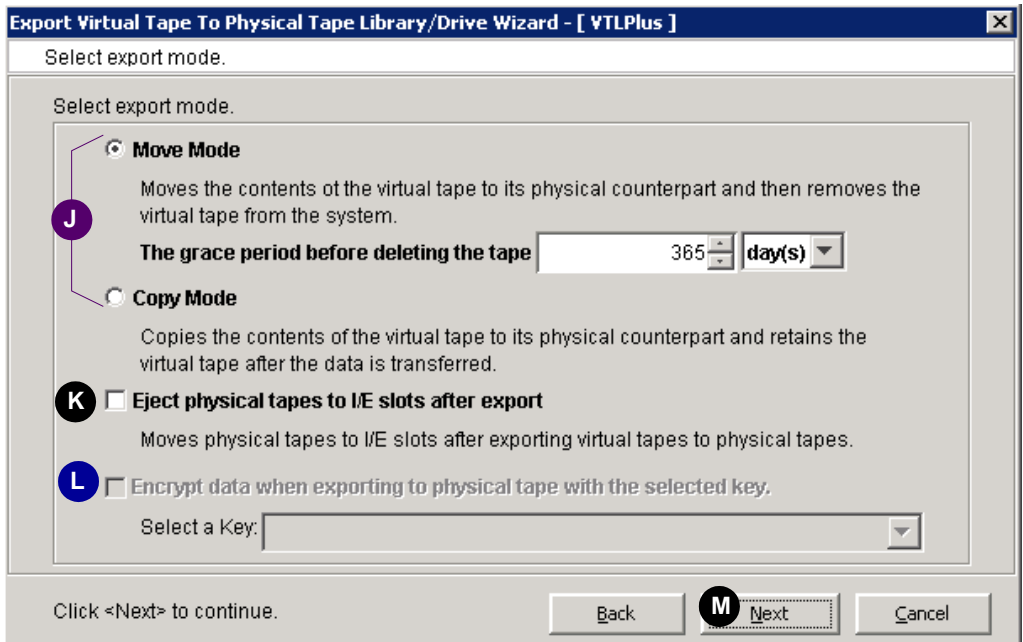
- Now, in the object tree of the VTL console, open the Virtual Vault node, and right-click the virtual tape that you want to export (E below). Select Export Tape from the context menu (F)



- 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)**.

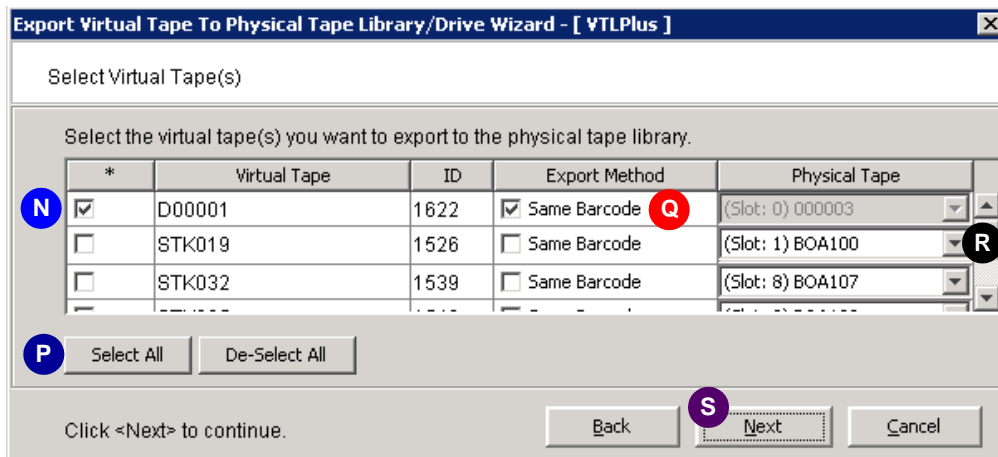


- When the **Select export mode** panel appears, select the desired export behavior by clicking either the **Move** radio button (and setting the grace period using the spinner and list controls provided) or the **Copy** radio button (J below).

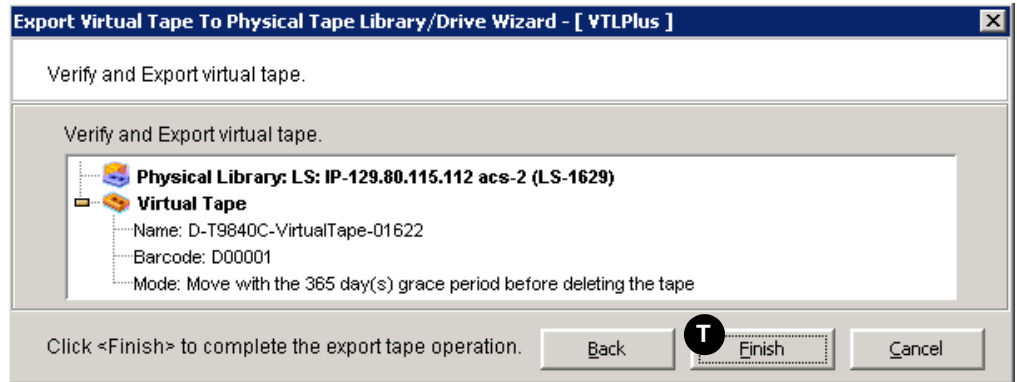


- If you wish to move the physical tapes to an import/export slot after the export operation is complete, check the **Eject physical tapes ...** check box (K above).

7. If you wish to encrypt the physical tape, check the `Encrypt data ...` check box, and supply a key using the control provided (L above).
8. Press **Next** (M above).
9. 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).
10. 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.
11. 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.
12. Press **Next** (S below).



13. 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 108
- “Manually freeing cache space” on page 108
- “Renewing cache for a directly linked tape” on page 108
- “Relinking physical tapes” on page 109

▼ 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.

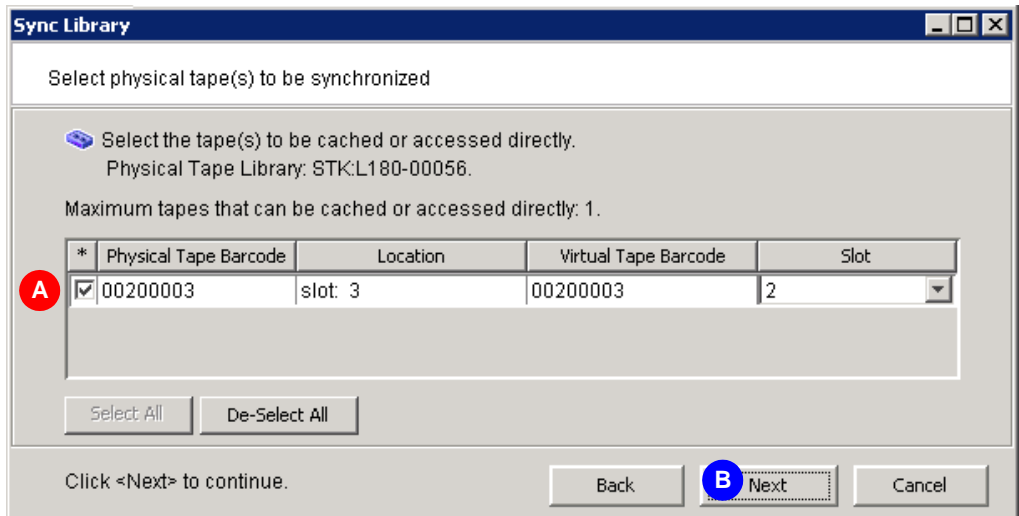
Stop here.

▼ 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.

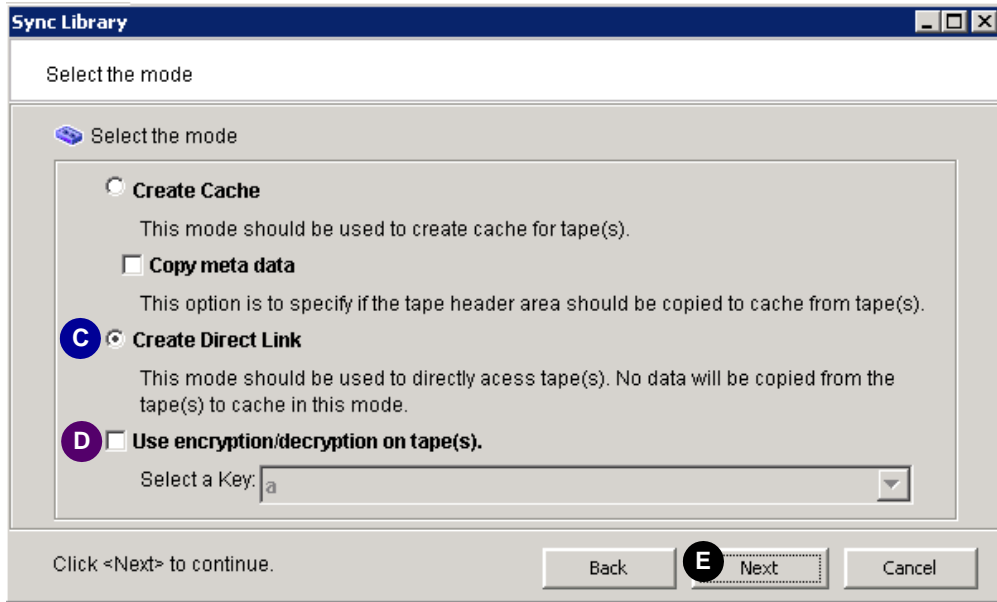
Note – Once the physical tape is reloaded in a library, the backup application can inventory access the library and access the tape directly, if necessary.

- 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).

- When the select the mode panel appears, click the `Create Direct Link` radio button (C below).



- 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).

- Press `Next` (E above), then `Finish`.

Stop here.

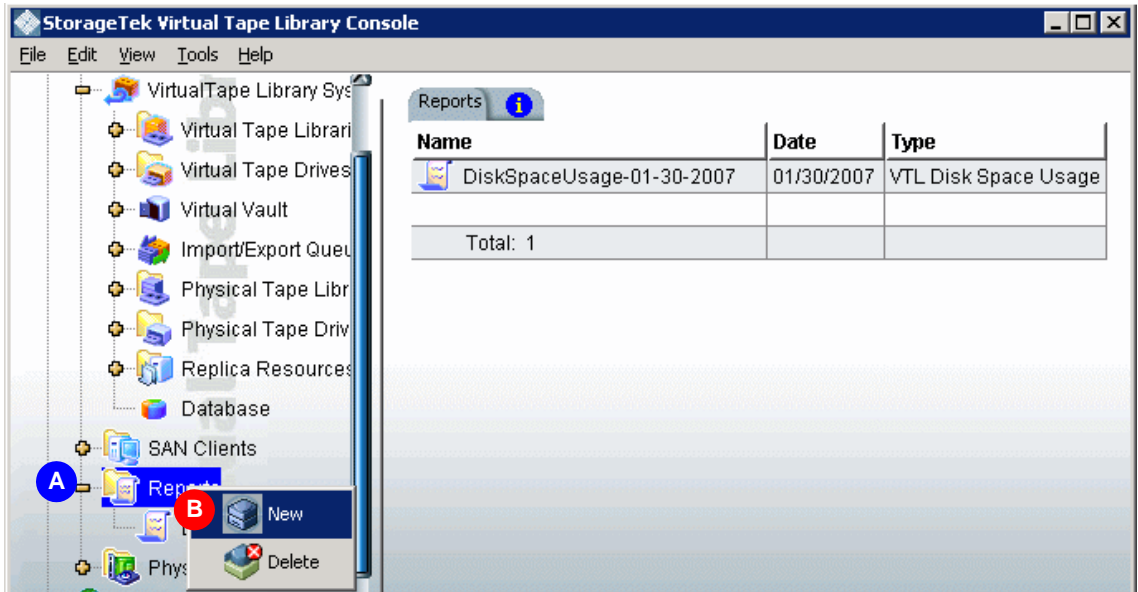
Creating and viewing reports

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

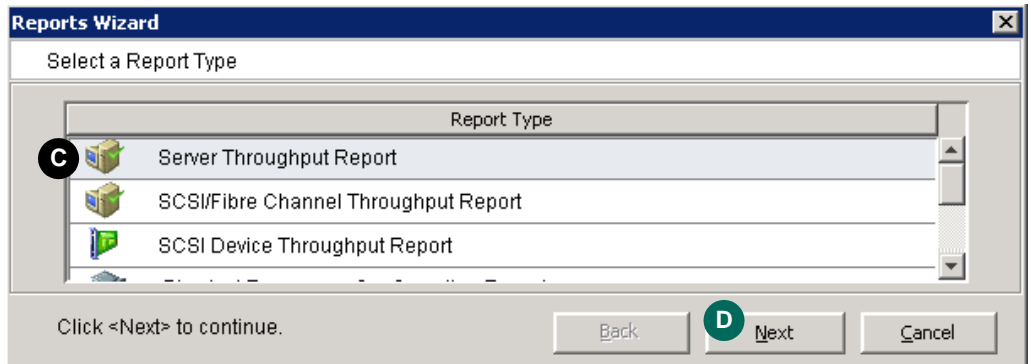
- "Creating a report" on page 111
- "Viewing a report" on page 113
- "Exporting data from a report" on page 114.

▼ Creating a report

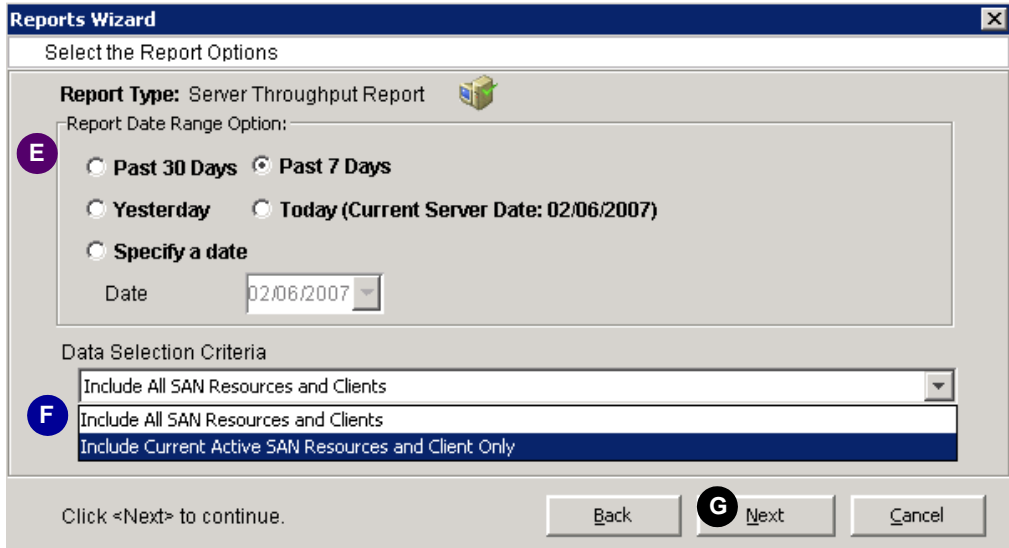
1. In the object tree of the VTL console, right-click on the **Reports** node (A below), and select **New** from the context menu (B).



2. When the **Select a Report Type** dialog appears, select a type from the list (C below). Press **Next** (D).



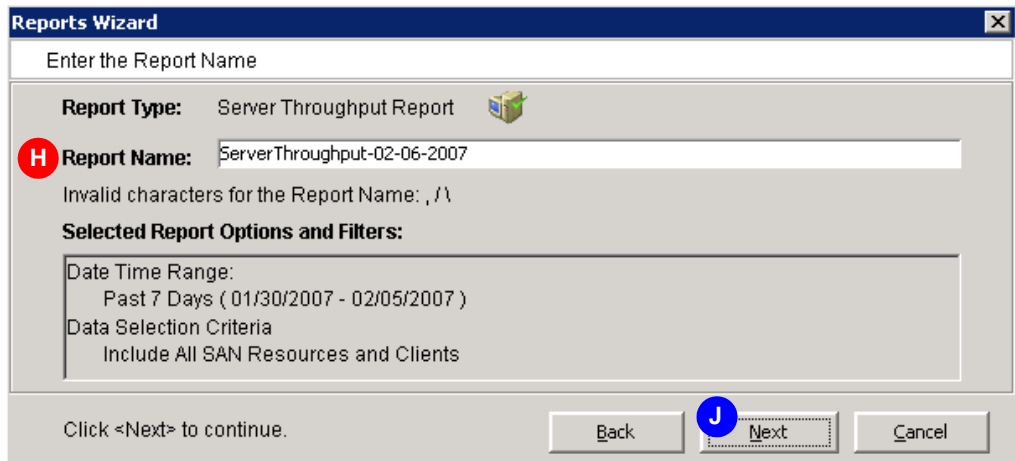
3. When the **Select Report Options** panel appears, select the desired report properties using the controls provided (E and F below). Press **Next (G)**.



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)**.



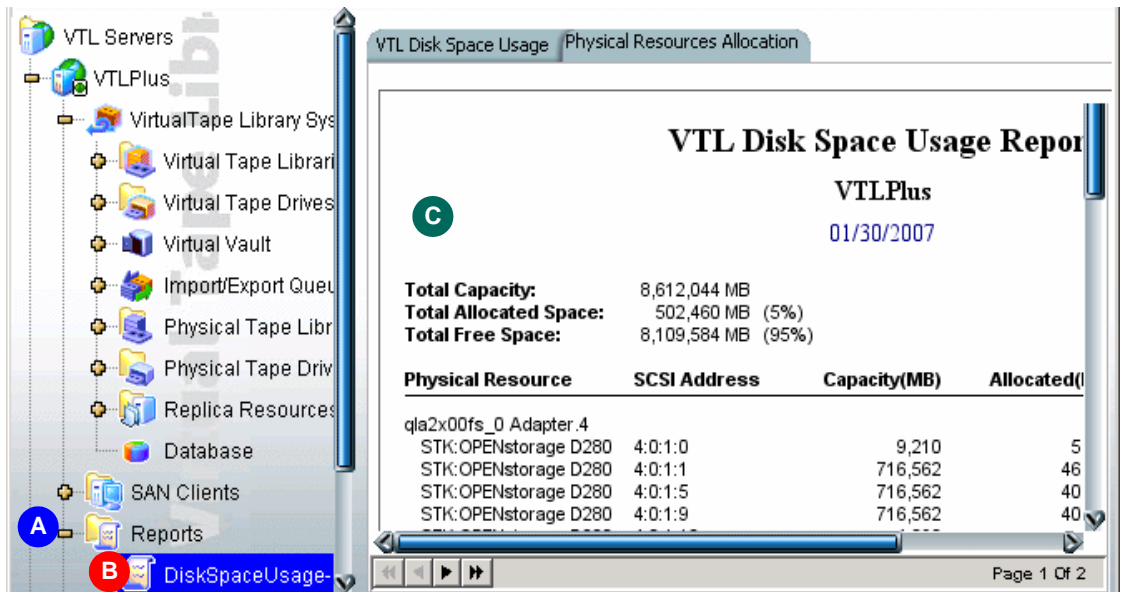
5. When the Create the Report panel appears, press Finish (K below).



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).

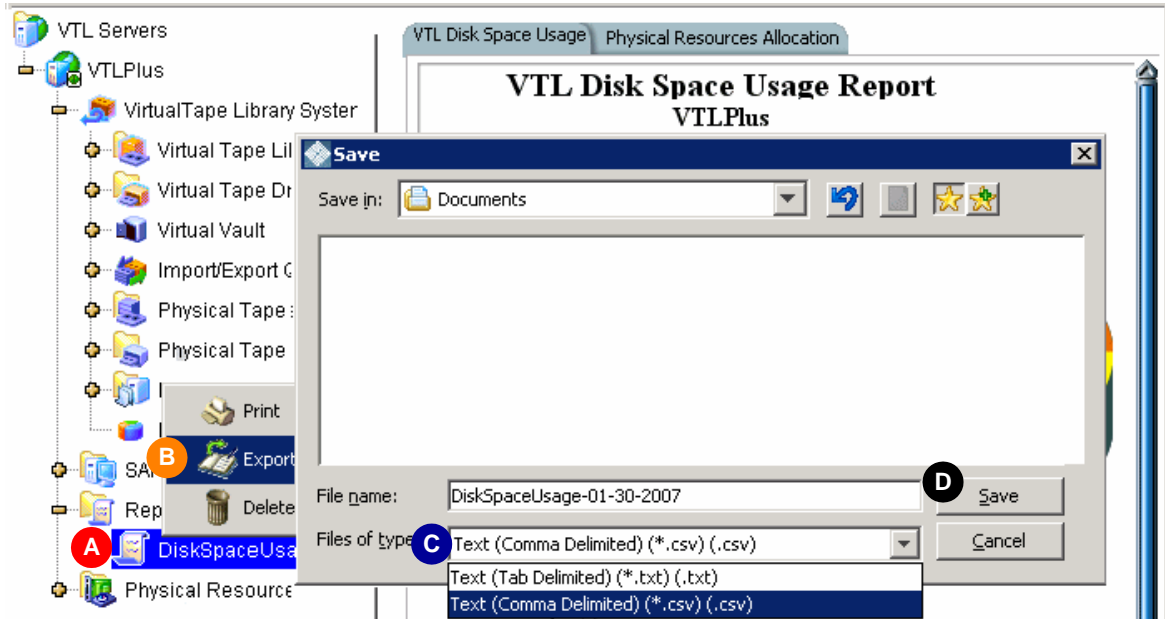
The desired report appears in the right-hand pane of the console (C above).

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 115
- “Changing a key name or password” on page 116
- “Deleting a key” on page 117
- “Exporting a key” on page 118
- “Importing a key” on page 119
- “Shredding a virtual tape” on page 120.

▼ 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.

- 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.

- 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.

- 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.

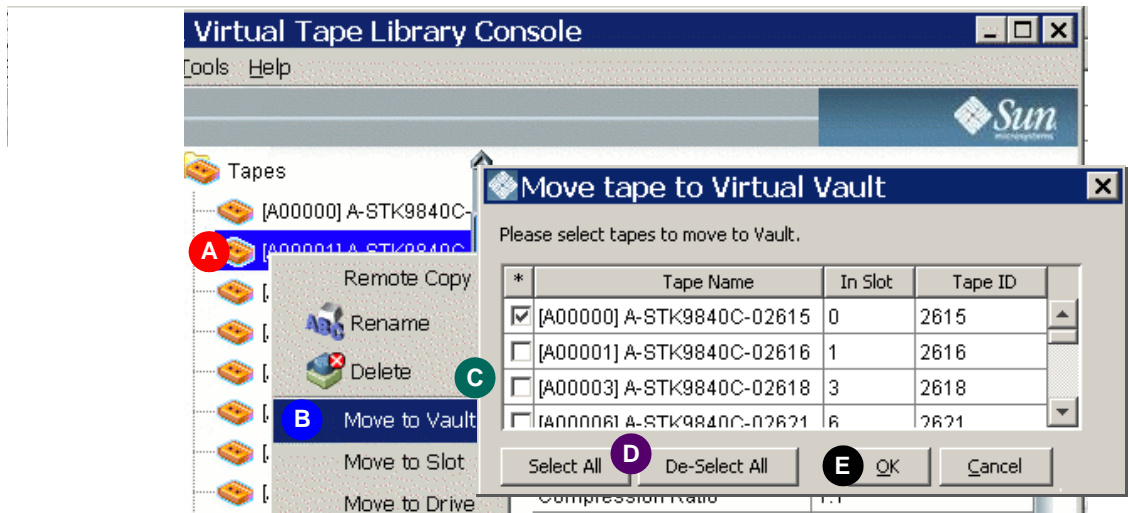
▼ Shredding a virtual tape

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.

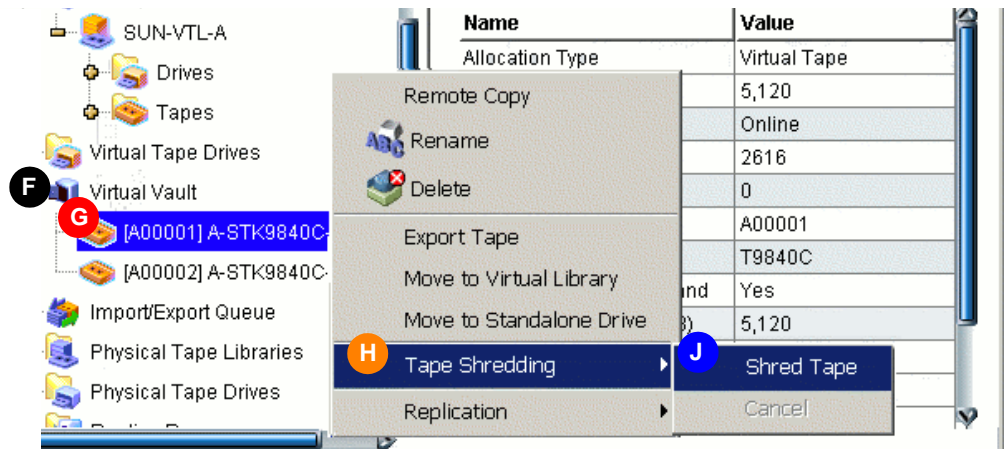
Shredding a virtual tape destroys all data on the tape, making it impossible to recover the data. Tape shredding uses a military standard to destroy data on virtual tapes by overwriting it with a random patterns of bits, rendering the data unreadable.

To shred tapes:

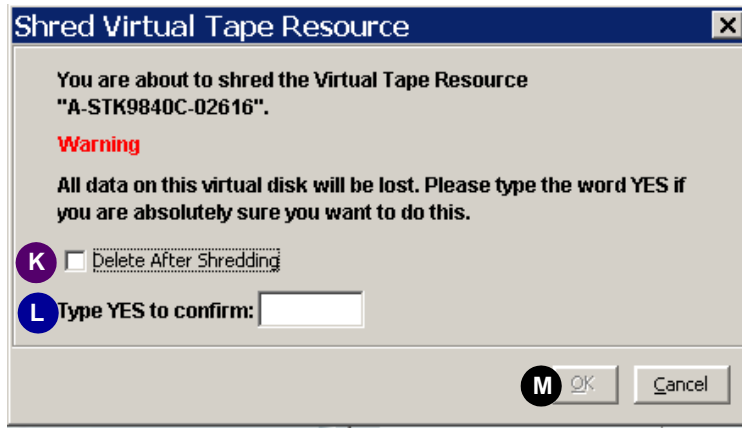
1. Move the tape(s) you want to shred to the virtual vault. In the object tree of the VTL console, start by right-clicking on a tape that you want to shred (A below), and select Move to Vault (B) from the context menu.



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	<p>I: This is an informational message. No action is required.</p> <p>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.</p> <p>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.</p> <p>C: These are critical errors that stop the system from operating properly.</p>
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 123
- “Sorting an event log” on page 123
- “Quickly printing an event log” on page 124
- “Filtering, exporting, purging, and printing an event log” on page 124

▼ 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.

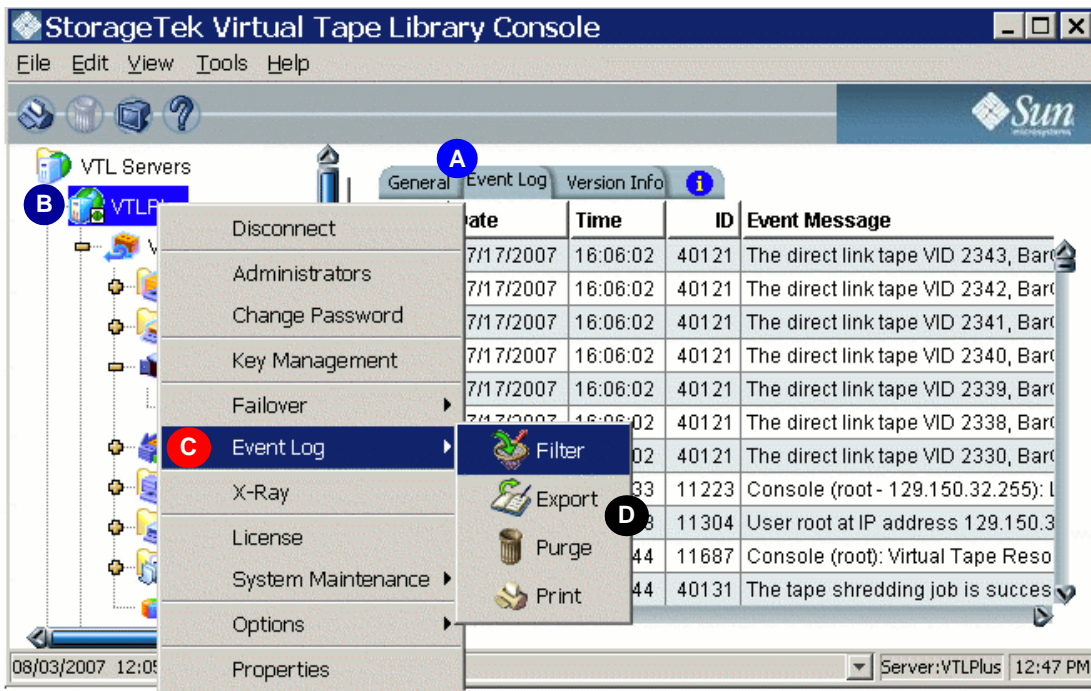
▼ Quickly printing an event log

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

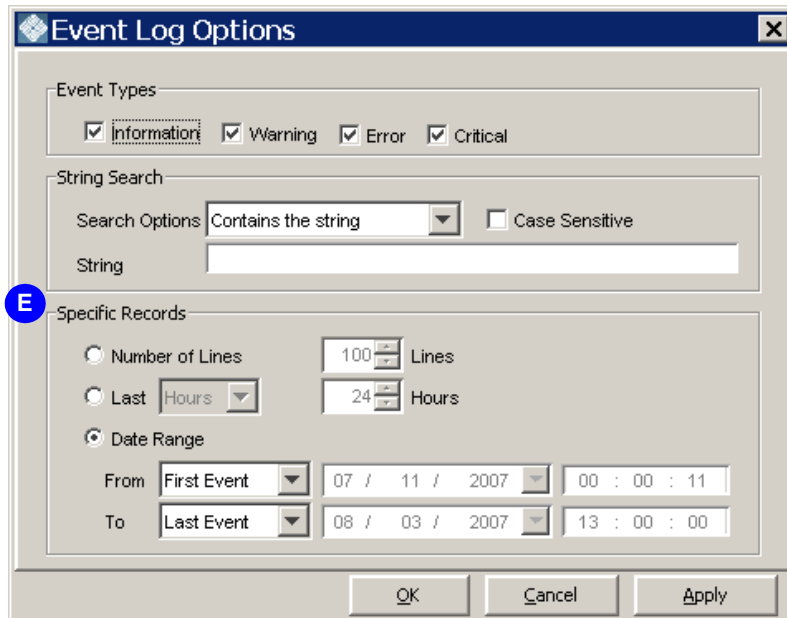
1. With the **Event Log** tab (A below) of the server open, right-click on the server icon in object tree of the VTL console (B).



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.

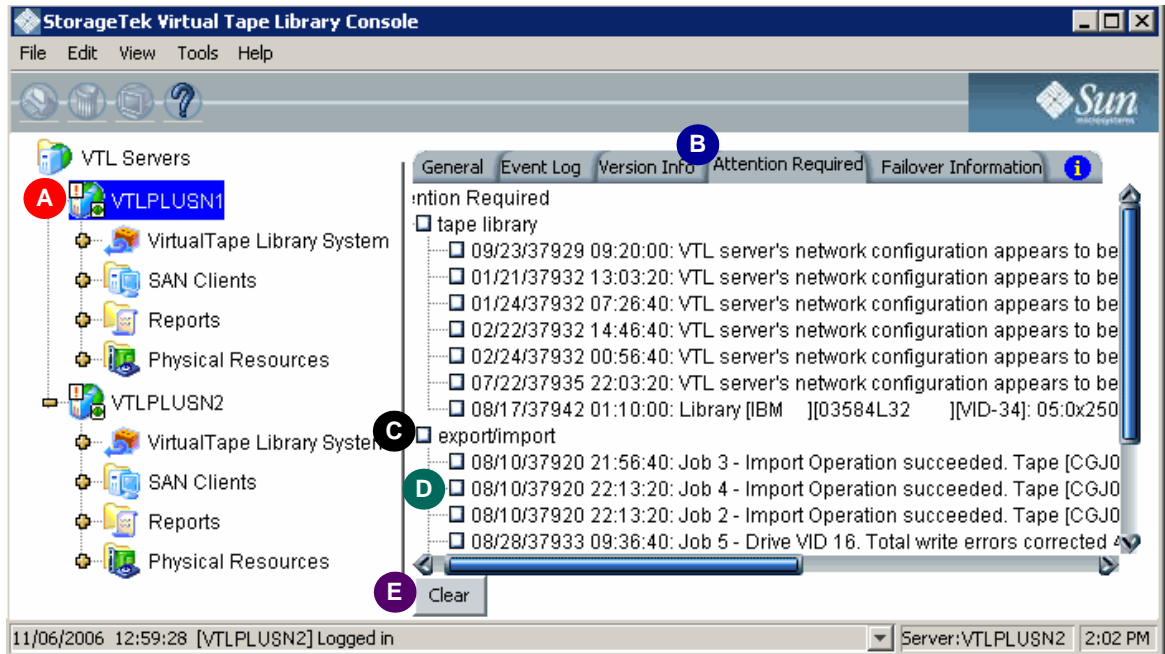
Using the Attention Required tab

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 in the following ways:

- “Accessing the Attention Required tab” on page 126
- “Clearing issues from the Attention Required list” on page 126.

▼ 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 127
- “Configuring SNMP traps” on page 127.

▼ 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 127 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 66 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 149.” on page 129
- “Installing the console on Linux platforms” on page 130
- “Installing the console on Microsoft Windows platforms” on page 130.

Note – For information on the text-based, VTL command line user interface, see Appendix A, “VTL command line reference” on page 149.

▼ 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 133
- “Resuming backups following a failover/failback” on page 144.

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 accidentally 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, `VTLPLUS1`:

```
[mgt_host]user# ssh vtladmin@nnn.nnn.nnn.nnw
Connecting to nnn.nnn.nnn.nnw ...
Password:
```

where *nnn.nnn.nnn.nnn* 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 VTLPLUS1 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, `VTLPLUS1`:

```
[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 VTLPLUS1 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 accidentally 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.nm (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:

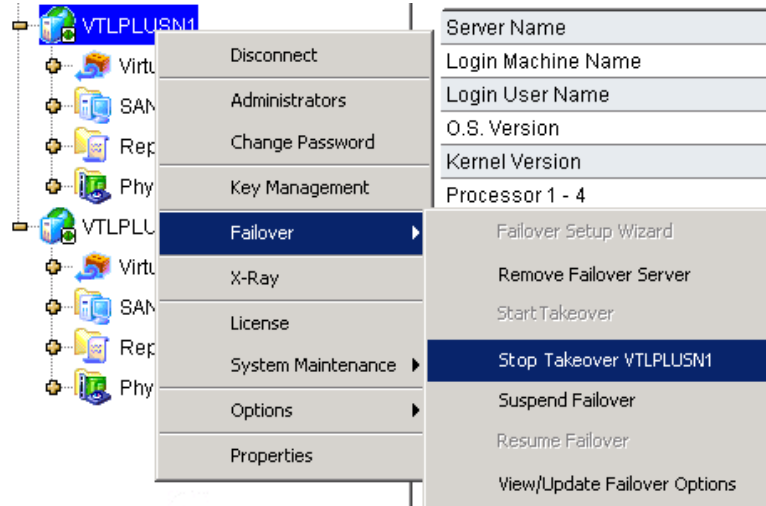
```
[VTL_Plus]vtladmin# vtl stop all
...
[VTL_Plus]vtladmin# vtl start
```

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 nn.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 accidentally 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 144.

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 notifications

You can configure VTL appliances to send automatic notifications to local system administrators via email whenever system problems arise.

▼ Configuring email notifications

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**).

The screenshot shows the "Configure Email Alerts Wizard" dialog box with the title "Set Email Alerts General Properties". The main area is titled "Email Alerts General Configuration".

Fields and controls:

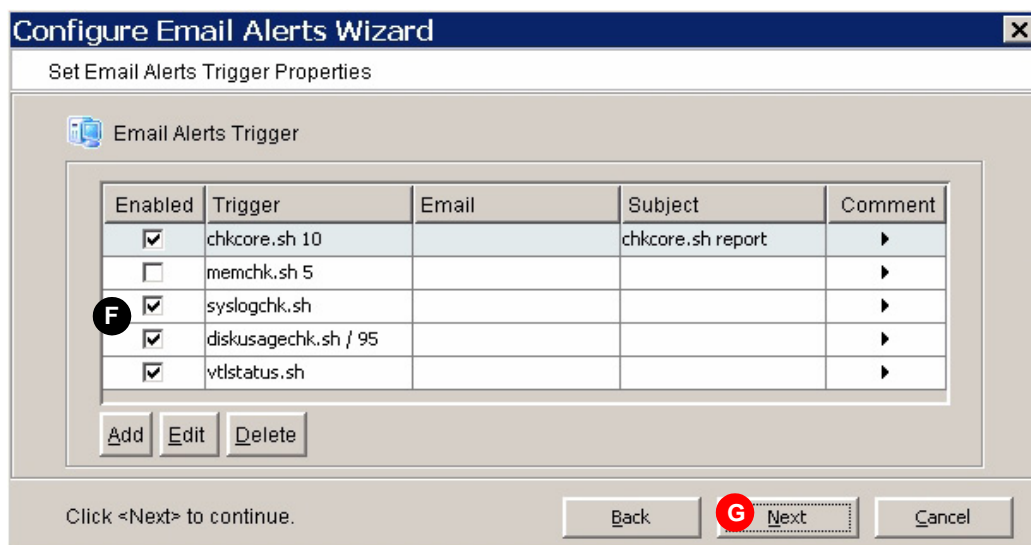
- A** SMTP Server: SMTP Port:
- SMTP Server supports authentication
- SMTP User Name:
- SMTP Password: Retype Password:
- From: **B**
- To: **C**
- CC:
- Subject:
- Interval: **D** day hour minute
- Note: Interval indicates how frequently the Email Alerts triggers and the System Log will be checked.

Buttons at the bottom: "Click <Next> to continue.", "Test", "Back", **E** "Next", "Cancel".

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 (C below). Then press `Next` (D).

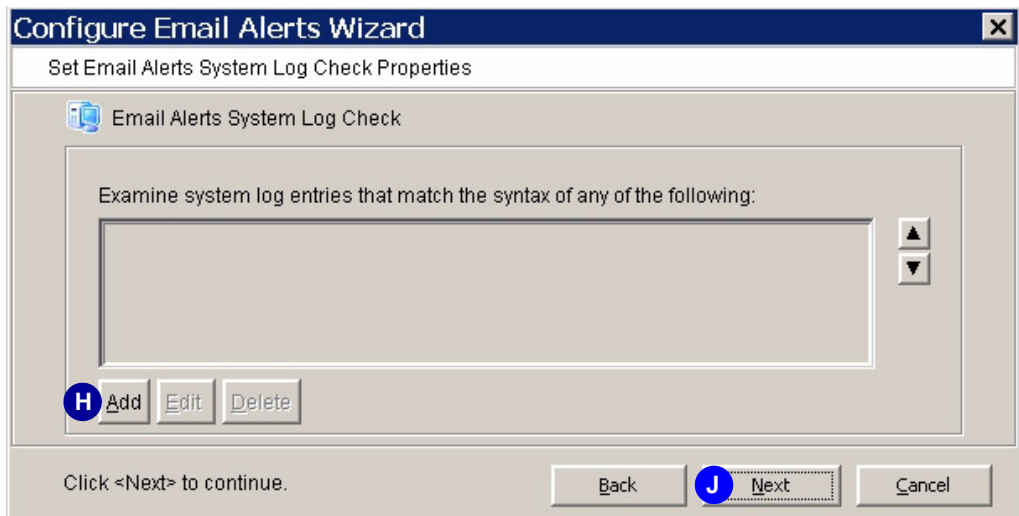


Default scripts include the following:

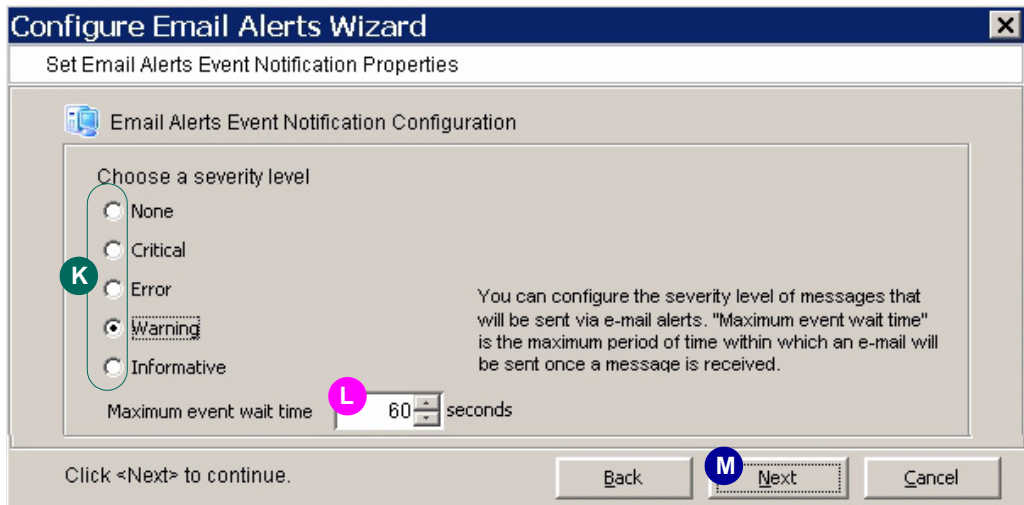
- `chkcore.sh 10` notifies the administrator if a new core file is found in the VTL `bin` directory. New core files are compressed and the originals are deleted, along with older compressed core files that exceed the maximum (10 is the default).
- `kfsnmem.sh 10` notifies the administrator if the maximum 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 **Email Alerts Event Notification Configuration** 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:

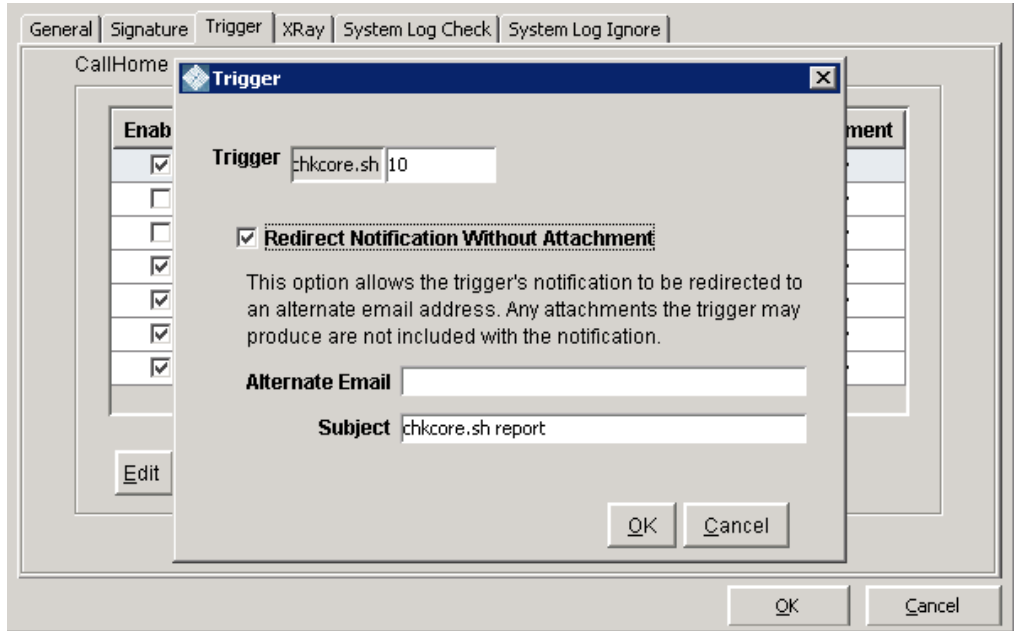
1. In the object tree of the VTL console, right-click on the VTL server node.
2. Select **Email Alerts** from the context menu.
3. When the property sheet appears, click on the appropriate tab to make your changes.

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 CallHome > Trigger.



If you specify an email address, it overrides the return code: no attachments are sent.

2. To modify an existing trigger, highlight the trigger, and press **Edit**.
3. To create a new trigger, press **Add**.

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-vtxxxxxxsolarisnn`, 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 same name, plus the suffix `.txt`.

All patches are applied using the VTL console software, as follows.

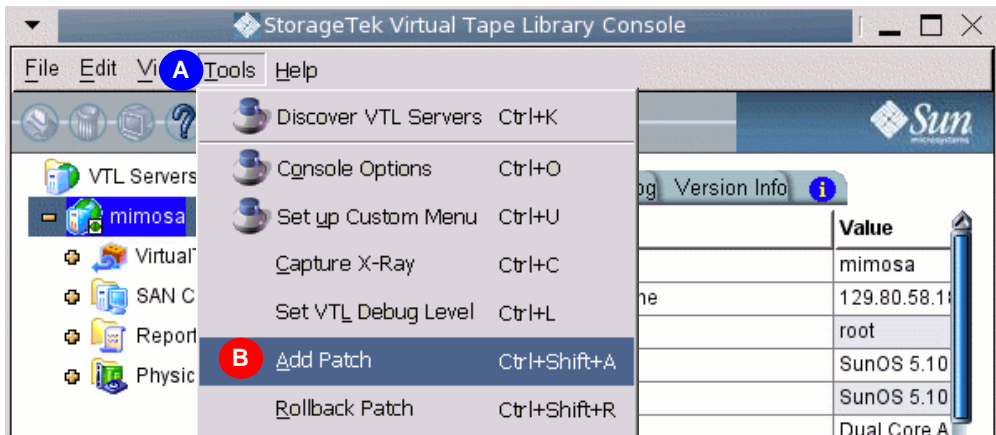
- 1. Understand the behavior of each patch before proceeding; read the accompanying text file (the “readme”).**

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.**

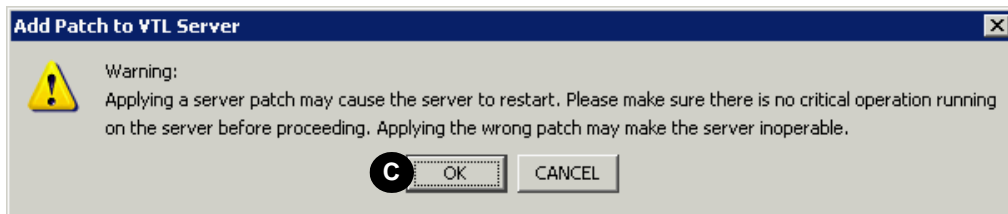
Processes will stop when the server software restarts.

3. Then, from the VTL console main menu, select **Tools** (A below).

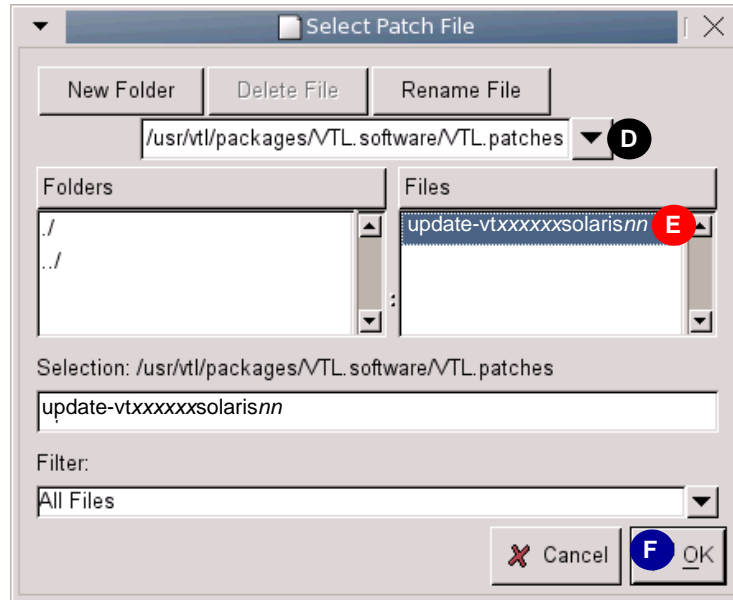


4. From the submenu, select **Add Patch** (B above).

5. When the warning notice appears, click **OK** (C below) to continue.

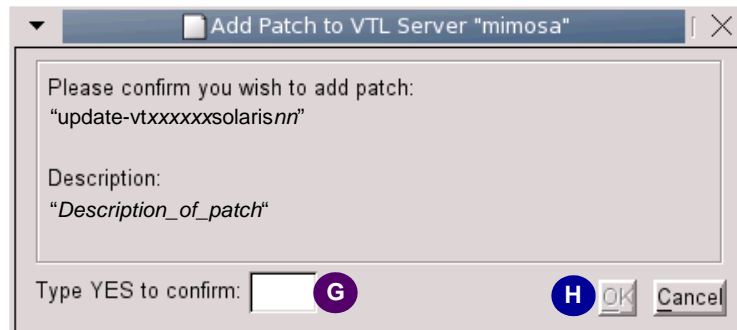


6. Locate the subdirectory where the patch files reside (D below), select the patch file (E), and press Open (F).



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.

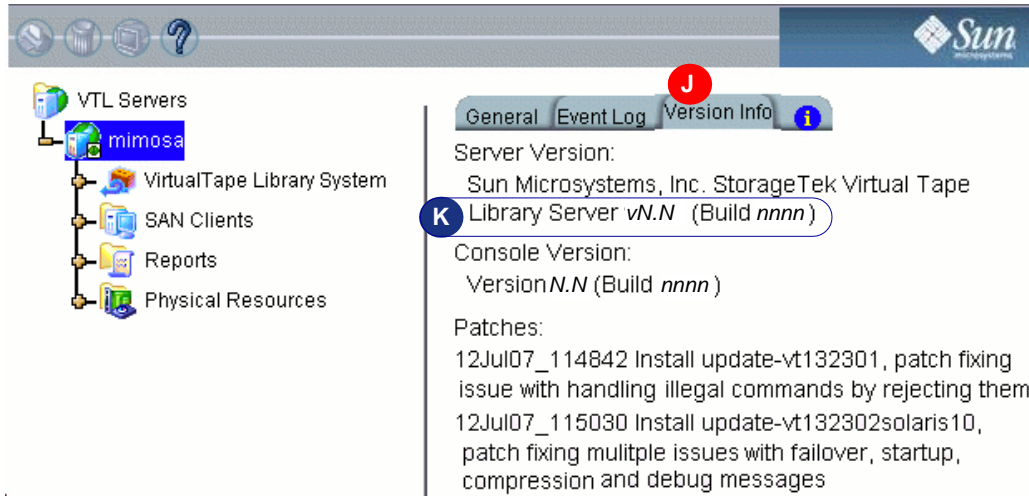
7. When the confirmation dialog appears, type YES in the text box (G below), and press OK (H).



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

Virtual Tape 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.

Typographical conventions

In this section, the following conventions are used in command descriptions:

- Variable parameters are shown enclosed in pointy brackets (<>).
- Arguments listed in brackets [] are optional.
- Alternatives are displayed as pipe (|) delimited lists.

Usage

- Entering `iscon` displays a list of commands.
- Entering `iscon <commandname>` displays a list of arguments for the specified command.
- Enter each command on a single line, separating arguments with spaces.
- Arguments have interchangeable long and short forms, introduced, respectively, by the `--` and the `-` symbols.
- Variable parameters following their corresponding argument.
- The order of the arguments is not significant.
- Enclose literal values that contain control characters, such as `*`, `<`, `>`, `?`, `|`, `%`, `$`, and spaces, in double or single quotation marks.
- Literals cannot contain leading or trailing spaces. Leading or trailing spaces enclosed in quotes are stripped.
- Short arguments are case sensitive.

Common arguments

The following arguments are common to many commands.

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	--vdevvid	VTL Virtual Device ID

The `--server-username` (-u) and `--server-password` (-p) arguments are only used when logging into a server. You do not need them for the remainder of the session.

Login and logout

Name: **Login**

Syntax:

```
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 in to the specified VTL Server with a given username and password. After a successful login, the username and password are not necessary for remainder of the session.

To use the `-e` (`--environment`) parameter in place of in place of `-s <server-name> -u <user-name> -p <password>`, you must set the following environment variables:

- ISSERVERNAME
- ISUSERNAME
- ISPASSWORD

To set environment variables in the bash shell, use the following syntax:

- `export ISSERVERNAME=10.1.1.1`
- `export ISUSERNAME=administrative_login`
- `export ISPASSWORD=password`

`-X (--rpc-timeout)` specifies an RPC timeout in seconds (range: 1..30000). The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30.

Name: **Log out**

Syntax:

```
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 - client commands

Name: **getvdevlist**

Syntax:

```
iscon getvdevlist -s <server-name> [-u <username> -p <password>] [-l [-v <vdevid> | -n <vdevname>] [-a | -A] [-c | -C] [-M <output-delimiter>] ] [-X <rpc-timeout>]
```

```
iscon getvdevlist --server-name=<server-name> [--server-username=<username> --server-password=<password>] [--longlist [--vdevid=<vdevid> | --vdevname=<vdevname>] [--client-list | --long-client-list] [--physical-layout | --long-physical-layout] [--output-delimiter=<output-delimiter>] ] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command retrieves and displays information about all virtual devices or a specific virtual device from the specified server. The default output format is a list with a heading.

The `-l` (`--longlist`) optional argument displays detailed information for each virtual device. Additional options can be specified along with the `-l` (`--longlist`) option to display the physical device layout and/or the assigned client information.

`-v` (`--vdevid`) or `-n` (`--vdevname`) are options to display only the specified virtual device information when `-l` (`--longlist`) is specified.

`-a` (`--physical-layout`) or `-A` (`--long-physical-layout`) are options to display the physical layout when `-l` (`--longlist`) is specified.

`-c` (`--client-list`) or `-C` (`--long-client-list`) are options to display the assigned client list when `-l` (`--longlist`) option is specified.

`-M` (`--output-delimiter`) can be specified when `-l` is specified to replace the linefeed with the specified delimiter. The maximum length of the delimiter is 8.

`-X` (`--rpc-timeout`) specifies an RPC timeout in seconds (range: 1..30000). The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: `getclientvdevlist`

Syntax:

```
iscon getclientvdevlist -s <server-name> [-u <username> -p  
  <password>] -c <client-name> [-t <client-type>] [-l [-a | -A] [-  
  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 [--  
  physical-layout | --long-physical-layout] [--output-delimiter=  
  <output-delimiter>] ] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command retrieves and displays information about all virtual devices assigned to the client from the specified server. The default output format is a list with heading. Use `-c` (`--client-name`) to specify a client name or `*` for all clients. `-t` (`client-type`) is the type of the client protocol to be retrieved in one of the

following values: SCSI, FC, or iSCSI. The client type will only take effect when the client name is *. Be aware that in some platforms you are required to enclose the "*" in double quote to take it as a literal.

-l (--longlist) is an option to display the long format.

-a (--physical-layout) or -A (--long-physical-layout) is an option to display the physical layout when -l (--longlist) is specified.

-M (--output-delimiter) can be specified when -l is specified to replace the linefeed with the specified delimiter. The maximum length of the delimiter is 8.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: addclient

Syntax:

```
iscon addclient -s <server-name> [-u <username> -p <password>] -c
<client-name> [-t <client-type>] [-I <initiator-wwpns>] [-a
<on|off>] [-A <on|off>] [-X <rpc-timeout>]
```

```
iscon addclient --server-name=<server-name> [--server-username=
<username> --server-password=<password> --client-name=<client-
name> [--client-type=<client-type>] [--initiator-wwpns=
<initiator-wwpns>] [--enable-VSA=<on|off>] [--enable-AS400=
<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: <>"&\$/\'

-t (--client-type) is an option to specify the type of the client protocol: SCSI, iSCSI, or FC.

-I (--initiator-wwpns), -a (--enable-VSA) and -A (--enable-AS400) are options for Fibre Channel clients, which can be set when the client type is FC.

-I (--initiator-wwpns) is the option to set the initiator WWPNS. An initiator WWPNS is a 16-byte hexadecimal value. Separate the initiator WWPNS by comma if more than one initiator WWPNS is specified. For example:

```
13af35d2f4ea6fbc,13af35d2f4ea6fad
```

-a (--enable-VSA) is an option for Volume Set Addressing with the following values: on or off (default).

-A (--enable-AS400) is an option to support IBM iSeries Server with the following values: on or off (default).

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **deleteclient**

Syntax:

```
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 if it is not specified.

Name: **getclientprop**

Syntax:

```
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 if it is not specified.

Name: **setfcclientprop**

Syntax:

```
iscon setfcclientprop -s <server-name> [-u <username> -p  
    <password>] -c <client-name> [-I <initiator-wwpns>] [-a <on|off>]  
    [-A <on|off>] [-X <rpc-timeout>]
```

```
iscon setfcclientprop --server-name=<server-name> [--server-  
    username=<username> --server-password=<password>] --client-  
    name=<client-name> [--initiator-wwpns=<initiator-wwpns>] [--  
    enable-VSA=<on|off>] [--enable-AS400=<on|off>] [--rpc-timeout=  
    <rpc-timeout>]
```

Description:

This command allows you to set Fibre Channel client properties. -c (--client-name) is required.

-I (--initiator-wwpns) is the option to set the initiator WWPNS for the client. An initiator WWPNS is a 16-byte hexadecimal value. Separate the initiator WWPNS with a comma if more than one initiator WWPNS is specified. For example:
13af35d2f4ea6fbc,13af35d2f4ea6fad

To clear the initiator WWPNS from the Fibre Channel client properties, specify * as the initiator WWPNS list.

-a (--enable-VSA) is an option for Volume Set Addressing with the following values: on and off.

-A (--enable-AS400) is an option to support IBM iSeries Server with the following values: on and off.

This option cannot be set if the client is already assigned to virtual devices.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **assignvdev**

Syntax:

```
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 hexadecimal 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 it is not specified.

-M (--output-delimiter) can be specified when -l is specified to replace the linefeed with the specified delimiter. The maximum length of the delimiter is 8.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **unassignvdev**

Syntax:

```
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 if it is not specified.

Name: **createvdev**

Syntax:

```
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 30 seconds if it is not specified.

Name: **deletevdev**

```
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 direct virtual device, such as virtual tape library or virtual tape drive. The virtual device cannot be deleted if there are clients currently connected to the library or drive.

-v (`--vdevid`) is required to specify the virtual tape, library, or virtual tape drive to be deleted.

-d (`--delete-virtual-tapes`) is an option to delete the associated tapes. -f (`--force`) option is required to delete the tapes. If this option is not specified, the tapes will be moved to the vault.

The `force` option is required to delete the resource if any of the following conditions applies:

- The virtual device is a virtual tape and is configured as a primary replica. The replica will be promoted as long as the replication is not in progress. Otherwise, the replica will be deleted.
- The virtual device is a virtual tape library or a virtual tape drive, and -d (`--delete-virtual-tapes`) option is specified to delete the tapes.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Virtual devices - VTL server commands

Name: **enableVTL**

Syntax:

```
iscon enableVTL -s <server-name> [-u <username> -p <password>] [ [-m <#(MB)>] [-I <ACSL>] | -M <custom-method> | -L <custom-layout>] [-c] [-X <rpc-timeout>]
```

```
iscon enableVTL --server-name=<server-name> [--server-username=<username> --server-password=<password>] [ [--size-mb=<#(MB)>] [--scsiaddress=<ACSL>] | --custom-method=<custom-method> | --custom-layout=<custom-layout>] [--compression] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command enables VTL. A repository will be created for the VTL system. The size of the repository and the physical devices to be used for allocation can be specified. -m (--size-mb) is the size in MB. The default is 200 MB if it is not specified.

-I (--scsiaddress) is the option to specify a specific physical device to be used to create the repository in the format:

ACSL=#:#:#:# (adapter:channel:id:lun)

The -M (--custom-method) and -L (--custom-layout) are options for specific physical segments, which can be a list or a file enclosed in <> containing physical segment in each line. The format of the physical segment for <custom-mode> is:

adapter:channel:scsi-id:lun:first-sector:size-in-MB

The format for <custom-layout> is: adapter:channel:scsi-id:lun:first-sector:last-sector.

-m, -I options cannot be specified with the -M or -L option.

-c (--compression) is an option to set compression. The default is no compression.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **disableVTL**

Syntax:

```
iscon disableVTL -s <server-name> [-u <username> -p <password>] [-X <rpc-timeout>]
```

```
iscon disableVTL --server-name=<server-name> [--server-username=<username> --server-password=<password>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command disables VTL. All virtual tape libraries, virtual tape drives, virtual tapes, and tape replicas have to be deleted and the Hosted Backup option has to be disabled before the VTL can be disabled.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **getvtlinfo**

Syntax:

```
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 displays virtual tape libraries only.
- VDRIVES displays standalone virtual tape drives only
- VAULT displays virtual tape vault only.
- PLIBS displays physical tape libraries only.
- PDRIVES displays standalone physical tape drives only.

The default is to display all the information.

-L (--tape-library-vid) is an option to specify the virtual tape library when VLIBS is specified, or to specify the physical tape library when PLIBS is specified.

-F (--vtl-info-filter) is an additional filter that can be combined using the following values separated by comma: library or drive or tape.

- library = include physical and/or virtual library information.
- drive = include physical and/or virtual drive information.
- tape = include physical and/or virtual tape information.

For example:

```
-F "library,drive,tape"
--vtl-info-filter="library,drive,tape"
```

The default is to display all of the information that applies. There will be an error if <vtl-info-type> is specified and the <vtl-info-filter> specified does not apply. For example, "library" does not apply to "VDRIVES".

-l (--longlist) is an option to display the information in a detail format.

-M (--output-delimiter) can be specified when -l is specified to replace the linefeed with the specified delimiter. The maximum length of the delimiter is 8.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **getsupportedvlibs**

Syntax:

```
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 if it is not specified.

Name: **getsupportedvdrives**

Syntax:

```
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 if it is not specified.

Name: `createvirtuallibrary`

Syntax:

```
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] [-E
<import-export-slots>] [-D -I <initial-size> -C <increment-size>]
[-m <max-capacity>] [-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-range=<barcode-
range>] [--num-of-slots=<num-of-slots>] [--export-to-ptape] [--
import-export-slots=<import-export-slots>] [--capacity-on-
demand --initial-size=<initial-size> --increment-size=
<increment-size>] [--max-capacity=<max-capacity>] [--key-name=
<key-name> --key-password=<key-password>] [--rpc-timeout=<rpc-
timeout>]
```

Description:

This command creates a virtual tape library.

-t (--vlib-type) is required in the following format:
<vendorID>:<productID>

-n (--vlib-name) is optional. If a name is not supplied, a default name is entered in the format: <vendorID>-<productID>-<vid>

-d (--vdrive-type) is required to specify the type of tape drive to be created in the library. The format of <vdrive-type> is <vendorID>:<productID>

-r (--vdrive-name-prefix) is an option to specify the prefix of the virtual drive. The default prefix is in the format: <drive-vendorID>-<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 15 days.

-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.

-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

-B (--barcode-range) can be specified in the following format: <barcodeB>-<barcodeE>

Barcode is an alpha-numeric value with a length of 6 to 8. <barcodeB> and <barcodeE> have to be the same length.

<barcodeE> has to be greater than <barcodeB>. A default <barcode-range> will be generated if it is not specified.

-T (--num-of-slots), -e (--export-to-tape) and -E (--import-export-slots) are optional. The range of the <num-of-slots> and <import-export-slots> is between 1 and the maximum number supported by the specified library type. The default for the library will be used if it is not specified.

-D (--capacity-on-demand) is an option to expand the virtual tape when needed. The default is to create the virtual tape with the maximum capacity if it is not specified.

-I (--initial-size) and -C (--increment-size) are options to be specified with <capacity-on-demand> option.

-m (--max-capacity) is an option to specify the maximum capacity of the virtual tape. The maximum capacity configured for the specified type of virtual library will be used if it is not specified.

The unit of <max-capacity>, <initial-size> and <increment-size> are all in GB.

A virtual device ID will be assigned to the virtual library when it is created successfully.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **addvirtualdrive**

Syntax:

```
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: <drive-vendorID>-<drive-productID>-<vid>

-R (--num-of-drives) is optional, the default is 1 if it is not specified.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **createstandalone drive**

Syntax:

```
iscon createstandalone drive -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 createstandalone drive --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: <vendorID>:<productID>

-r (--vdrive-name-prefix) is an option to specify the prefix of the virtual drive. The default prefix is in the format: <drive-vendorID>-<drive-productID>-<vid>

-R (--num-of-drives) can be specified to create multiple drives of the same type. The default is 1 if it is not specified. The maximum number of drives is 10.

-D (--capacity-on-demand) is an option to expand the virtual tape when needed. The default is to create the virtual tape with the maximum capacity if it is not specified.

-I (--initial-size) and -C (--increment-size) are options to be specified with <capacity-on-demand> option.

-m (--max-capacity) is an option to specify the maximum capacity of the virtual tape. The maximum capacity configured for the specified type of virtual tape drive will be used if it is not specified.

The unit of <max-capacity>, <initial-size> and <increment-size> are all in GB.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: createVirtual Tape

Syntax:

```

iscon createVirtual Tape -s <server-name> [-u <username> -p
<password>] -v <parent-vid> [ [-g <#(GB)> [-I <ACSL>] ] [-n
<vdevname>] [-B <barcode>] [-A -l <plib-vid> -b <physical-tape-
barcode> [-j] | -N [-S <target-name>] [-U <target-username> -P
<target-password>] [-c <on|off>] [-e <on|off>] ] [-t <count>] [-X
<rpc-timeout>]

```



```

iscon createVirtual Tape --server-name=<server-name> [--server-
username=<username> --server-password=<password>] --parent-vid=
<parent-vid> [ [--size-gb=<#(GB)>] [--scsiaddress=<ACSL>] ] [--
vdevname=<vdevname>] [--barcode=<barcode>] [--enable-auto-
archive --plib-vid=<plib-vid> --physical-tape-barcode=<physical-
tape-barcode> [--auto-eject-to-ie] | --enable-auto-replication
--target-name=<target-name> --target-username=<target-
username> --target-password=<target-password>] [--compression=
<on|off>] [--encryption=<on|off>] ] [--count=<count>] [--rpc-
timeout=<rpc-timeout>]

```

Description:

This command creates a virtual tape.

-v (--parent-vid) is the virtual device id of the virtual tape library or standalone tape drive.

-g (--size-gb) is an option to specify the size in GB. The size of the virtual tape will be the size configured in the properties of the virtual tape library or virtual tape drive if it is not specified.

-I (--scsiaddress) is 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 specify the barcode range for the tape(s). The format for the barcode range is BBBB BBBB-EEEEEEEE. This option cannot be specified when -A (--enable-auto-archive) option is specified.

-A (--enable-auto-archive) is an option when the parent library is enabled with auto-archive option.

-l (--plib-vid) is required when <auto-archive-mode> is specified. It is the physical tape library where the tape will be exported to automatically.

-b (--physical-tape-barcode) is required to specify the list of physical tape barcode(s) when auto-archive option is specified. Separate barcodes by comma for more than one physical tape. For example: -b 00010001,00010009,0001000A

-e (--auto-eject-to-ie) is optional when <auto-archive-mode> is specified.

-N (`--enable-auto-replication`) is an option when the parent library is enabled with the `auto-replication` option.

-S (`--target-name`) can be specified when `auto-replication` option is specified. The default remote server from the parent library will be used if it is not specified.

-c (`--compression`) and -e (`--encryption`) can be specified when `auto-replication` option is specified.

-c (`--compression`) is an option to enable or disable compression with one of the values: `on` or `off`.

-e (`--encryption`) is an option to enable or disable encryption with one of the values: `on` or `off`.

-t (`--count`) is an option to create multiple tapes in a virtual tape library. This option cannot be specified when -A (`--enable-auto-archive`) option is specified because the number of tapes will be obtained from the list of barcodes specified with -b (`--physical-tape-barcode`) option.

If a barcode range is specified with -B (`--barcode`) option and -t (`--count`) option is also specified, `<count>` will be served as the maximum number of tapes to be created. If the number of the barcodes from the specified range is less than the `<count>`, an error will be returned to indicate that there are not enough barcodes for the specified number of tapes.

If neither barcode nor count is specified, the default `<count>` will be 1.

-X (`--rpc-timeout`) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **moveVirtual Tape**

Syntax:

```
iscon moveVirtual Tape -s <server-name> [-u <username> -p
  <password>] -v <vdevvid> [-L <tape-library-vid> | -D <tape-drive-
  vid> | -l <slot-no>] [-X <rpc-timeout>]
```

```
iscon moveVirtual Tape --server-name=<server-name> [--server-
  username=<username> --server-password=<password>] --vdevvid=
  <vdevvid> [--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 (--vdev-id) is required to specify the ID of the virtual tape to be moved.

-L (--tape-library-vid) is the virtual library to move to.

-D (--tape-drive-vid) is the virtual drive in a library or the standalone drive to move to.

-l (--slot-no) is the slot in a library to move to.

If none of the above locations are specified, the vault will be assumed to be the new location.

If the tape is in a slot in a library, it can be moved to a different slot or a drive in the library, or it can be moved to the vault.

- Vlib Slot -> Tape drive (in the library only)
- Vlib Slot -> Slots in same library
- Vlib Slot -> Vault

If it is in a drive in the library, it can be moved to an available slot in the library or to the vault.

- Vlib Drive -> Slots in same library
- Vlib Drive -> Vault

If the tape is in a standalone drive, it can only be moved to the vault.

- Standalone Tape Drive -> Vault

If the tape is in the vault, it can be moved to an available slot in a library, or an available standalone drive.

- Vault -> Vlib (First available slot)
- Vault -> Standalone Tape Drive

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **plibinventory**

Syntax:

```
iscon plibinventory -s <server-name> [-u <username> -p <password>]  
[-L <tape-library-vid>] [-X <rpc-timeout>]
```

```
iscon plibinventory --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--tape-library-vid=<tape-library-vid>] [--rpc-timeout=<rpc-
timeout>]
```

Description:

This command performs an inventory of the physical tapes in a physical tape library.

-L (--tape-library-vid) is an option to specify the physical tape library to perform the inventory.

Inventory operation will be performed for all the physical tape libraries if -L (--tape-library-vid) is not specified.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **assignresourcetovtl**

Syntax:

```
iscon assignresourcetovtl -s <server-name> [-u <username> -p
<password>] -v <vdevid> [-L <tape-library-vid>] [-X <rpc-
timeout>]
```

```
iscon assignresourcetovtl --server-name=<server-name> [--server-
username=<username> --server-password=<password>] --vdevid=
<vdevid> [--tape-library-vid=<tape-library-vid>] [--rpc-
timeout=<rpc-timeout>]
```

Description:

This command assigns a physical tape library or drive to VTL.

-v (--vdevid) is required to specify the ID of the physical tape library or the physical tape drive to be assigned to the VTL system.

-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 if it is not specified.

Name: **unassignresourcefromvtl**

Syntax:

```
iscon unassignresourcefromvtl -s <server-name> [-u <username> -p  
          <password>] -v <vdevvid> [-X <rpc-timeout>]
```

```
iscon unassignresourcefromvtl --server-name=<server-name> [--  
  server-username=<username> --server-password=<password>] --  
  vdevvid=<vdevvid> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command unassigns a physical tape library or drive from VTL.

-v (--vdevvid) is required to specify the ID of the physical tape library or the physical tape drive to be unassigned from VTL.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **tapecopy**

Syntax:

```
iscon tapecopy -s <server-name> [-u <username> -p <password>] -v  
  <source-vdevvid> -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-vdevvid=  
  <source-vdevvid> --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-vdevvid) is required to specify the ID of the virtual tape to be copied from.

-S (--target-name) is required to specify the target server name where the remote tape copy will be created and copied to.

-U (--target-username) and -P (--target-password) are optional for connection and login to the target server if the target server was not logged in with login command.

-L <tape-library-vid> and -D <tape-drive-vid> are options to move the tape copy to the virtual tape library or virtual tape drive when the copy is completed.

-n (--vdevname) is an option to specify the virtual tape name of the tape copy. The maximum length of the virtual device name is 64. Leading and trailing spaces will be removed. Enclose the name in double quotes. The following characters are invalid for the name: <>"&\$/\ '

A default name with the primary server and source virtual tape name will be generated if it is not specified.

-f (--force) option is required when the tape is scheduled to be deleted. The deletion schedule for the virtual tape will be removed and the replication will be configured.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: `settapeproperty`

Syntax:

```
iscon settapeproperty -s <server-name> [-u <username> -p
<password>] -v <vdevvid> [-B <barcode>] [-f] [-F] [-w <on|off>] [-
A <auto-archive-mode> [-Y <days>] [-j] | -N <auto-repl-mode> -S
<target-name> [-U <target-username> -P <target-password>] [-M
<#[D|H|M]>] ] [-k <key-name> -W <key-password> | -d] [-X <rpc-
timeout>]
```

```
iscon settapeproperty --server-name=<server-name> [--server-
username=<username> --server-password=<password>] --vdevvid=
<vdevvid> [--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] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command sets tape properties.

`-v` (`--vdev`) is required to specify the ID of the virtual tape to set the properties.

`-B` (`--barcode`) is the option to specify the new barcode for the tape. `-f` (`--force`) option is required if the new barcode is not in the barcode range specified for the parent library.

`-F` (`--full-capacity`) is an option to expand the tape to the maximum capacity and turn off the `<capacity-on-demand>` option if it is enabled for the virtual tape.

`-w` (`--tape-write-protect`) is an option to turn on and off the tape write protection with the following values: `on` or `off`.

`-A` (`--auto-archive-mode`) is an option with one of the following values: `copy` or `move` or `inherited` or `none`.

- "none" is the value to turn off the `auto-archive` mode if the virtual tape is enabled with `auto-archive` option.
- "inherited" can only be specified when the parent library is enabled with `auto-archive` option.

`-Y` (`--delay-delete-days`) is an option for `move` mode to specify the number of days to wait before the deletion. The maximum is 15 days.

`-j` (`--auto-eject-to-ie`) is an option to be specified for `auto-archive` mode to eject the tape to the IE slot after the export job.

`-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.

`-N` (`--auto-replication`) is an option with one of the following values: `remotecopy`, `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 `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

-A (`--auto-archive-mode`) cannot be specified if `auto-replication` is enabled for the tape.

At least one of the properties has to be specified.

-X (`--rpc-timeout`) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Import/Export

Name: `importtape`

Syntax:

```
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-password=<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. The physical tape information is not required if it is from a physical tape drive.

-L (--tape-library-vid) is the virtual device ID of the virtual tape library to which the physical tape is to be imported.

-t (--virtual-tape-slot-no) is required for the virtual tape location.

-b (--virtual-tape-barcode) is optional when the physical tape from a physical tape library contains barcode. It is required if the physical tape does not have a barcode or when it is from a physical tape drive.

-j (--job-description) is an option to specify a description for the tape import job.

-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 30 seconds if it is not specified.

Name: exportVirtual Tape

Syntax:

```
iscon exportVirtual Tape -s <server-name> [-u <username> -p  
<password>] -v <vdevid> -L <tape-library-vid> [-M <export-mode>]  
-b | -B <barcode> | -l <slot-no> [-j <job-description>] [-f] [-k  
<key-name> -W <key-password>] [-X <rpc-timeout>]
```

```
iscon exportVirtual Tape --server-name=<server-name> [--server-  
username=<username> --server-password=<password>] --vdevid=  
<vdevid> --tape-library-vid=<tape-library-vid> [--export-mode=  
<export-mode>] --same-barcode | --barcode=<barcode> | --slot-no=  
<slot-no> [--job-description=<job-description>] [--force] [--  
key-name=<key-name> --key-pasword=<key-password>] [--rpc-  
timeout=<rpc-timeout>]
```

Description:

This command exports the information from a virtual tape to a physical tape.

-v (--vdev-id) is required to specify the ID of the virtual tape to be exported to the physical tape.

-L (--tape-library-vid) is also required to specify the ID of the target physical tape library.

-M (--export-mode) is an option with one of the following values: copy (default) or move.

One of the three export methods below is required to select the physical tapes:

- -b (--same-barcode) is the option to select a physical tape with the same barcode of the virtual tape if a physical tape with the same barcode exists.
- -B (--barcode) is the option to specify the barcode of an available physical tape in the physical tape library.
- -l (--slot-no) is the option to specify the slot number of an available physical tape in the physical tape library.

-j (--job-description) is an option to specify a description for the tape export job.

-f (--force) is required when the tape is scheduled to be deleted.

-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.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Replication

Name: **createreplication**

Syntax:

```
iscon createreplication -s <server-name> [-u <username> -p
  <password>] -v <source-vdev-id> -S <target-name> [-U <target-
  username> -P <target-password>] [-w <watermark(MB)> [-r
  <watermark-retry>]] [-d <YYYYMMDDHHMM> -i <#[H|M]>] [-c <on|off>]
  [-e <on|off>] [-f] [-X <rpc-timeout>]
```

```
iscon createreplication --server-name=<server-name> [--server-
  username=<username> --server-password=<password>] --source-
  vdev-id=<source-vdev-id> --target-name=<target-name> [--target-
```

```
username=<target-username> --target-password=<target-password>]
[--watermark=<watermark(MB)> [--watermark-retry=<watermark-
retry>]] [--date=<YYYYMMDDHHMM> --interval=<#[H|M]> [--
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.

-w (--watermark), -r (--watermark-retry), -T (replication-time), and -i (--interval) are options for replication policy.

Replication will be triggered based on one or more of the three policies:

- Watermark in MB with watermark retry in minutes. The default is 30 minutes if watermark is specified. For example:
-w 50 -r 30, --watermark=50 --watermark-retry=30
- Replication date in YYYYMMDDHHMM. For example:
-d 200712251719, --date=200712251719
- Replication interval in Hours (H) or Minutes (M). The interval MUST be one of 1H, 2H, 3H, 4H, 8H, 12H, 24H, 10M, 12M, 15M, 20M, 30M, or any minutes equal to the hours in the list. For example:
-i 2H, -i 120M, --interval=2H, --interval=120M

The default policy is to replicate at 12:00 every day if none of the policies are specified.

-c (--compression) is an option to enable or disable compression with one of the values: on or off.

-e (--encryption) is an option to enable or disable encryption with one of the values: on or off.

-f (--force) option is required when the tape is scheduled to be deleted. The deletion schedule for the virtual tape will be removed and the replication will be configured.

`-X (--rpc-timeout)` is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **promotereplica**

Syntax:

```
iscon promotereplica -s <server-name> [-u <username> -p <password>]
-v <vdevid> | -S <target-name> [-U <target-username> -P <target-
password>] -v <replicaid> [-f] [-X <rpc-timeout>]
```

```
iscon promotereplica --server-name=<server-name> [--server-
username=<username> --server-password=<password>] --vdevid=
<vdevid> | --target-name=<target-name> [--target-username=
<target-username> --target-password=<target-password>] --
replicaid=<replicaid> [--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to promote a replica to a regular virtual device if the primary disk is available and the replica disk is in a valid state.

`-v (--vdevid)` is the ID of the source virtual tape and `-v (--replicaid)` is the ID of the tape replica.

Either the primary server with the source virtual tape or the target server with the tape replica can be specified for promotion, but not both.

If the source virtual tape is still valid and available, and the tape replica is in an invalid state, the tape replica can be promoted with the force option. But, it is recommended to synchronize the tape replica with the source virtual tape first unless the source virtual tape is physically defective or unavailable.

If the source virtual tape is no longer available, the tape replica can be promoted with the force option even when it is in invalid state if you are sure the data on the tape replica is useful.

`-X (--rpc-timeout)` is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **removerepliation**

Syntax:

```
iscon removerepliation -s <server-name> [-u <username> -p  
  <password>] -v <vdevid> | -S <target-name> [-U <target-username>  
  -P <target-password>] -v <replicaid> [-f] [-X <rpc-timeout>]
```

```
iscon removerepliation --server-name=<server-name> [--server-  
  username=<username> --server-password=<password>] --vdevid=  
  <vdevid> | --target-name=<target-name> [--target-username=  
  <target-username> --target-password=<target-password>] --  
  replicaid=<replicaid> [--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to remove the replication configuration from the primary disk on the primary server and delete the replica disk on the target server. Either primary server with source virtual tape or the target server with the tape replica can be specified, but not both.

-v (--vdevid) is the ID of the source virtual tape and -v (--replicaid) is the ID of the tape replica.

If the target server no longer exists or cannot be connected to, only the replication configuration on the primary server will be removed.

If the primary server no longer exists or cannot be connected to, only the tape replica will be deleted.

-f (--force) option has to be specified when either the primary server or target server no longer exists or cannot be connected.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **suspendreplication**

Syntax:

```
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 if it is not specified.

Name: resumereplication

Syntax:

```
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 if it is not specified.

Name: setreplicationproperties

Syntax:

```
iscon setreplicationproperties -s <server-name> [-u <username> -p  
  <password>] -v <source-vdevid> [-w <watermark(MB)> [-r <watermark-  
  retry>]] [-d <YYYYMMDDhhmm>] [-i <#[H|M]>] [-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)> [--  
watermark-retry=<watermark-retry>]] [--date=<YYYYMMDDhhmm>] [--  
interval=<#[H|M]>] [--compression=<on|off>] [--encryption=  
<on|off>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to set the replication policy for a virtual device configured for replication.

-v (--source-vdevid) is required to specify the ID of the source virtual tape.

-w (--watermark), -r (--watermark-retry), -T (replication-time), and -i (--interval) are options for replication policy.

Replication will be triggered based on one or more of the three policies:

- Watermark in MB with watermark retry in minutes. The default is 30 minutes if watermark is specified. For example:
-w 50 -r 30, --watermark=50 --watermark-retry=30
- Replication date in YYYYMMDDHHMM. For example:
-d 200712251719, --date=200712251719
- Replication interval in Hours (H) or Minutes (M). The interval MUST be one of 1H, 2H, 3H, 4H, 8H, 12H, 24H, 10M, 12M, 15M, 20M, 30M, or any minutes equal to the hours in the list. For example:
-i 2H, -i 120M, --interval=2H, --interval=120M

At least one of the properties has to be specified.

To unset the watermark, specify 0 for the watermark. To unset the replication time, specify NA instead of the time. To unset the interval, specify 0 for the interval.

The watermark retry value will be ignored if the watermark is not set.

-c (--compression) is an option to enable or disable compression with one of the values: on or off.

-e (--encryption) is an option to enable or disable encryption with one of the values: on or off.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **getreplicationproperties**

Syntax:

```
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 if it is not specified.

Name: **getreplicationstatus**

Syntax:

```
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 the ID of the tape replica, both of which are required.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **startreplication**

Syntax:

```
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 if it is not specified.

Name: **stopreplication**

Syntax:

```
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>]
```

Description:

This command allows you to stop the replication that is in progress for a virtual device.

-v (--source-vdevid) is the ID of the source virtual tape on the primary server to stop.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Replication

Name: **Create a replica**

```
iscon createreplication -s <server-name> [-u <username> -p
<password>] -v <source-vdev> -S <target-name> [-U <target-
username> -P <target-password>] [-w <watermark(MB)> [-r <watermark-
retry>]] [-T <hh:mm>] [-i <#[H|M]>] [-c <on|off>] [-e <on|off>] [-
f] [-X <rpc-timeout>]
```

```
iscon createreplication --server-name=<server-name> [--server-
username=<username> --server-password=<password>] --source-
vdev=<source-vdev> --target-name=<target-name> [--target-
username=<target-username> --target-password=<target-password>] [-
-watermark=<watermark(MB)> [--watermark-retry=<watermark-retry>]]
[--replication-time=<hh:mm>] [--interval=<#[H|M]>] [--compression=
<on|off>] [--encryption=<on|off>] [--force] [--rpc-timeout=<rpc-
timeout>]
```

Description:

This command allows you to set up a replication configuration.

-v (--source-vdev) is required to specify the ID of the virtual tape to be configured for replication.

-S (--target-name) is required to specify the target server name.

-U (--target-username) and -P (--target-password) are optional for connection and login to the target server if the target server are not logged in with a login command.

-w (--watermark), -r (--watermark-retry), -T (replication-time), and -i (--interval) are options for replication policy.

Replication will be triggered based on one or more of the three policies:

- Watermark in MB with watermark retry in minutes. The default is 30 minutes if watermark is specified. For example:
-w 50 -r 30, --watermark=50 --watermark-retry=30
- Replication time in hh:mm. For example:
-T 12:00, --replication-time=12:00
- Replication interval in Hours (H) or Minutes (M). For example:
-i 2H, -i 120M, --interval=2H, --interval=120M

The default policy is to replicate at 12:00 every day if none of the policies are specified.

-c (--compression) is an option to enable or disable compression with one of the values: on or off.

-e (--encryption) is an option to enable or disable encryption with one of the values: on or off.

-f (--force) option is required when the tape is scheduled to be deleted. The deletion schedule for the virtual tape will be removed and the replication will be configured.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: Promote a replica

```
iscon promotereplica -s <server-name> [-u <username> -p <password>]
-v <vdevid> | -S <target-name> [-U <target-username> -P <target-
password>] -v <replicaid> [-f] [-X <rpc-timeout>]
```

```
iscon promotereplica --server-name=<server-name> [--server-username=
<username> --server-password=<password>] --vdevid=<vdevid> | --
target-name=<target-name> [--target-username=<target-username> --
target-password=<target-password>] --replicaid=<replicaid> [--
force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to promote a replica to a regular virtual device if the primary disk is available and the replica disk is in a valid state.

-v (--vdevid) is the ID of the source virtual tape and -v (--replicaid) is the ID of the tape replica.

Either the primary server with the source virtual tape or the target server with the tape replica can be specified for promotion, but not both.

If the source virtual tape is still valid and available, and the tape replica is in an invalid state, the tape replica can be promoted with the force option. But, it is recommended to synchronize the tape replica with the source virtual tape first unless the source virtual tape is physically defective or unavailable.

If the source virtual tape is no longer available, the tape replica can be promoted with the force option even when it is in invalid state if you are sure the data on the tape replica is useful.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: Remove replication

```
iscon removereplication -s <server-name> [-u <username> -p  
  <password>] -v <vdevid> | -S <target-name> [-U <target-username> -  
  P <target-password>] -v <replicaid> [-f] [-X <rpc-timeout>]
```

```
iscon removereplication --server-name=<server-name> [--server-  
  username=<username> --server-password=<password>] --vdevid=  
  <vdevid> | --target-name=<target-name> [--target-username=<target-  
  username> --target-password=<target-password>] --replicaid=  
  <replicaid> [--force] [--rpc-timeout=<rpc-timeout>]
```

This command allows you to remove the replication configuration from the primary disk on the primary server and delete the replica disk on the target server. Either primary server with source virtual tape or the target server with the tape replica can be specified, but not both.

-v (--vdevid) is the ID of the source virtual tape and -v (--replicaid) is the ID of the tape replica.

If the target server no longer exists or cannot be connected to, only the replication configuration on the primary server will be removed.

If the primary server no longer exists or cannot be connected to, only the tape replica will be deleted.

-f (--force) option has to be specified when either the primary server or target server no longer exists or cannot be connected.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: 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-vdev`) is the ID of the source virtual tape on the primary server to be suspended.

`-X` (`--rpc-timeout`) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: Resume replication

```
iscon resumereplication -s <server-name> [-u <username> -p
<password>] -v <vdev> [-X <rpc-timeout>]
```

```
iscon resumereplication --server-name=<server-name> [--server-
username=<username> --server-password=<password>] --vdev=
<vdev> [--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-vdev`) is the ID of the source virtual tape on the primary server to be resumed.

`-X` (`--rpc-timeout`) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: Set replication properties

```
iscon setreplicationproperties -s <server-name> [-u <username> -p
<password>] -v <source-vdev> [-w <watermark(MB)> [-r <watermark-
retry>]] [-T <hh:mm>] [-i <#[H|M]>] [-c <on|off>] [-e <on|off>] [-
X <rpc-timeout>]
```

```
iscon setreplicationproperties --server-name=<server-name> [--
server-username=<username> --server-password=<password>] --
source-vdev=<source-vdev> [--watermark=<watermark (MB)> [--
```

```
watermark-retry=<watermark-retry>]] [--replication-time=<hh:mm>]
[--interval=<#[H|M]>] [--compression=<on|off>] [--encryption=
<on|off>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to set the replication policy for a virtual device configured for replication.

-v (--source-vdevid) is required to specify the ID of the source virtual tape.

-w (--watermark), -r (--watermark-retry), -T (replication-time), and -i (--interval) are options for replication policy.

Replication will be triggered based on one or more of the three policies:

- Watermark in MB with watermark retry in minutes. The default is 30 minutes if watermark is specified. For example, -w 50 -r 30, --watermark=50 --watermark-retry=30
- Replication time in hh:mm. For example, -T 12:00, --replication-time=12:00
- Replication interval in Hours(H) or Minutes(M). For example, -i 2H, -i 120M, --interval=2H, --interval=120M

At least one of the properties has to be specified.

To unset the watermark, specify 0 for the watermark. To unset the replication time, specify NA instead of the time. To unset the interval, specify 0 for the interval.

The watermark retry value will be ignored if the watermark is not set.

-c (--compression) is an option to enable or disable compression with one of the values: on or off.

-e (--encryption) is an option to enable or disable encryption with one of the values: on or off.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **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-vdev) is required to specify the ID of the source virtual tape.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: 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 the ID of the tape replica, both of which are required.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: Start replication

```
iscon startreplication -s <server-name> [-u <username> -p  
  <password>] -v <vdev> [-X <rpc-timeout>]
```

```
iscon startreplication --server-name=<server-name> [--server-  
  username=<username> --server-password=<password>] --vdev=  
  <vdev> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to start replication on demand for a virtual device.

-v (--source-vdev) is the ID of the source virtual tape on the primary server to start.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: 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>]
```

Description:

This command allows you to stop the replication that is in progress for a virtual device.

-v (--source-vdevid) is the ID of the source virtual tape on the primary server to stop.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Physical devices

Name: getpdevinfo

```
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 if it is not specified.

Name: **rescandevices**

Syntax:

```
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 the adapters if it is not specified. For example:

```
-a 5
-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
```

If you want the system to rescan the device sequentially, you can specify the -L (--sequential) option. The default is not to rescan sequentially.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **importdisk**

Syntax:

```
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 30 seconds if it is not specified.

Name: `preparedisk`

Syntax:

```
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 format: `##:##:##` (adapter:channel:scsi id:lun)

Either `-i` (`--guid`) or `-I` (`--scsiaddress`) has to be specified.

`-C` (`--category`) is the required to specify the new category for the physical device in one of the following values: `unassigned` or `virtual` or `direct` or `service-enabled`.

-N (--new-guid) is an option to specify the new guid for the physical device if the new category is "virtual".

If the server is set up for failover, the failover partner has to be rescanned after the disk preparation.

<target-username> and <target-password> are options to specify the user name and password for the failover partner.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Fibre Channel

Name: **enablefc**

Syntax:

```
iscon enablefc -s <server-name> [-u <username> -p <password>] [-X  
  <rpc-timeout>]
```

```
iscon enablefc --server-name=<server-name> [--server-username=  
  <username> --server-password=<password>] [--rpc-timeout=<rpc-  
  timeout>]
```

Description:

This command enables Fibre Channel on the specified server.

-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 30 seconds if it is not specified.

Name: **switchfcportmode**

Syntax:

```
iscon switchfcportmode -s <server-name> [-u <username> -p  
  <password>] -t <adapter-no> -m <wwpn-mode> [-X <rpc-timeout>]
```

```
iscon switchfcportmode --server-name=<server-name> [--server-  
  username=<username> --server-password=<password>] --vdevid=  
  <vdevid> --vdevname=<vdevname> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command lets you set a port to target or initiator mode.

- `-m 0` switches the port to initiator mode
- `-m 1` switches the port to target mode

`-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 30 seconds if it is not specified.

Reports

Name: `getreportdata`

Syntax:

```
iscon getreportdata -s <server-name> [-u <username> -p <password>]
  [-T <report-type>] [-d <date>] [-I #[D|W|M] ] [-c <client-name> |
  -C <clientList>] [-v <vdevid>] -R <resourceList> [-N] [-o
  <outputFilename>] [-F <fileFormat>] [-H] [-f] [-X <rpc-timeout>]
```

```
iscon getreportdata --server-name=<server-name> [--server-
  username=<username> --server-password=<password>] [--report-
  type=<report-type>] [--date=<date>] [--units=#[<D|W|M>] ] [--no-
  system-info] [--client-name=<client-name> | --client-list=
  <clientList>] [--vdevid=<vdevid> | --resource-list=
  <resourceList>] [--include-heading] [--file-format=
  <fileFormat>] [--output-file=<outputFilename>] [--force] [--
  rpc-timeout=<rpc-timeout>]
```

Description:

This command produces a report.

`-T` (`--report-type`) is an option to specify which report you want. It can have one of the following values:

- `ServerThroughputReport` (default)
- `ClientThroughputReport`
- `ResourceThroughputReport`

`-d` (`--date`) is an option to specify the date in the format: YYYYMMDD. The default is today's date.

The units of time can be specified in three different units:

- D = Day
- W = Week
- M = Month

-c (--clientName) is required for the ClientThroughputReport.

-v (--vdevId) is required for the ResourceThroughputReport.

-R (--resource-list) can be either a list of resource IDs separated by commas, or "*" for all the resources, or a filename enclosed in <> containing a resource ID on each line. For example:

-R 1,3,5,10 or -R "<res_id_file.txt>"

For the ClientThroughputReport, only the resources assigned to the client can be specified.

-C (--clientList) can be either a list of client names separated by commas, or "*" for all the clients or a filename enclosed in <> containing a client name on each line. For example:

-C client1,client2 or -C "<client_file.txt>"

For the ResourceThroughputReport, only the clients assigned to the resource can be specified.

System information includes memory and CPU usage information on the server. The default is to include the system information for the ServerThroughputReport. The information will not be included for the ClientThroughputReport.

-N (--no-system-info) allows you to exclude the information. It can only be specified for the ServerThroughputReport.

-H (--include-heading) is the option to include the data heading.

-F (--fileFormat) is one of the following:

- csv (default)
- txt

-o (--output-file) is the full path of the file name to save the report data to. If output filename is not specified, the default filename is: ServerThroughputYYYY-MM-DD[. #]

[. #] is the additional suffix when there is a duplicate.

Specify 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 30 seconds if it is not specified.

Failover

Name: `getfailoverstatus`

Syntax:

```
iscon getfailoverstatus -s <server-name> [-u <username> -p  
    <password>] [-X <rpc-timeout>]
```

```
iscon getfailoverstatus --server-name=<server-name> [--server-  
    username=<username> --server-password=<password>] [--rpc-  
    timeout=<rpc-timeout>]
```

Description:

This command shows you the current status of your failover configuration. It also shows all Failover settings, including which IP addresses are being monitored for failover. Failover status can be obtained from either the failover primary server or the failover secondary server.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: `suspendfailover`

Syntax:

```
iscon suspendfailover -s <server-name> [-u <username> -p  
    <password>] [-X <rpc-timeout>]
```

```
iscon suspendfailover --server-name=<server-name> [--server-  
    username=<username> --server-password=<password>] [--rpc-  
    timeout=<rpc-timeout>]
```

Description:

This command suspends your failover configuration. Failover can only be suspended from the secondary failover server. Specify the secondary server name or IP address to suspend failover.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **resumefailover**

Syntax:

```
iscon resumefailover -s <server-name> [-u <username> -p <password>]
[-X <rpc-timeout>]
```

```
iscon resumefailover --server-name=<server-name> [--server-
username=<username> --server-password=<password>] [--rpc-
timeout=<rpc-timeout>]
```

Description:

This command resumes a suspended failover configuration. Failover can only be resumed from the secondary failover server. Specify the secondary server name or IP address to resume failover.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **starttakeover**

Syntax:

```
iscon starttakeover -s <server-name> [-u <username> -p <password>]
[-f] [-X <rpc-timeout>]
```

```
iscon starttakeover --server-name=<server-name> [--server-username=
<username> --server-password=<password>] [--force] [--rpc-
timeout=<rpc-timeout>]
```

Description:

This command initiates failover to the secondary server in a failover configuration. Takeover can only be performed from the secondary failover server. Specify the secondary server name or IP address to start failover.

Auto recovery will not take effect when the failover primary server is taken over manually. If auto recovery is set, the -f (-force) option is required to start takeover.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Name: **stoptakeover**

Syntax:

```
iscon stoptakeover -s <server-name> [-u <username> -p <password>]
[-X <rpc-timeout>]
```

```
iscon stoptakeover --server-name=<server-name> [--server-username=
<username> --server-password=<password>] [--rpc-timeout=<rpc-
timeout>]
```

Description:

This command initiates failback in a failover configuration. This operation can only be performed from the secondary failover server. Specify the secondary server name or IP address to stop.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Server configuration

Name: **saveconfig**

Syntax:

```
iscon saveconfig -s <server-name> [-u <username> -p <password>] [-
o <filename>] [-f] [-X <rpc-timeout>]
```

```
iscon saveconfig --server-name=<server-name> [--server-username=
<username> --server-password=<password>] [--output-file=
<filename>] [--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command saves the configuration of your VTL Server. You should save the configuration any time you change it, including any time you add/change/delete a client or resource, or assign a client.

-o (--output-file) is the full path of the file name to save the configuration to.

The default output filename is: config-YYYY-MM-DD-hh-mm-
<servername>.tar.gz

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 30 seconds if it is not specified.

Name: **restoreconfig**

Syntax:

```
iscon restoreconfig -s <server-name> [-u <username> -p <password>]
-i <filename> [-X <rpc-timeout>]
```

```
iscon restoreconfig --server-name=<server-name> [--server-
username=<username> --server-password=<password>] --input-file=
<filename> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command restores the configuration of the VTL server. Specify the configuration file name that was saved with `saveconfig` command.

Restoring a configuration overwrites existing virtual device and client configurations for that server. VTL partition information will not be restored. This feature should only be used if your configuration is lost or corrupted.

`-X` (`--rpc-timeout`) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 30 seconds if it is not specified.

Event Log

Name: **geteventlog**

Syntax:

```
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 if it is not specified.

Technical support

Name: **getxray**

Syntax:

```
iscon getxray -s <server-name> [-u <username> -p <password>] [-l
<#|all|YMMDDhhmm-YYMMDDhhmm>] [-M] [-r] [-o <filename>] [-f] [-
X <rpc-timeout>]
```

```
iscon getxray --server-name=<server-name> [--server-username=
<username> --server-password=<password>] [--get-log=
<#|all|YMMDDhhmm-YYMMDDhhmm>] [--get-storage-message-only] [--
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.

- `#` specifies the number of lines
- `all` specifies all log messages
- `YYMMDDhhmm-YYMMDDhhmm` specifies log messages in a date/time range

The default is to get all the log messages.

`-M (--get-storage-message-only)` is an option to get the message only.

`-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 30 seconds if it is not specified.

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 port 11578 - Used for encryption.
- UDP port 11579 - 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 211
- “Problems affecting physical resources” on page 214
- “Problems with virtual resources” on page 215
- “Problems during import/export operations” on page 219
- “Taking an X-ray for technical support” on page 221

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, go to “The operating system cannot detect the device” on page 217.
 3. If the operating system does show the device, go to “Applications cannot see the device” on page 217.

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 215.
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 218.

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 218.

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 219.
6. If you can access the device, go to “The operating system can access the device.” on page 219.

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 220.

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 220.

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 220.

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. If 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 221.

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 221.

Case: Some other system error is causing the problem

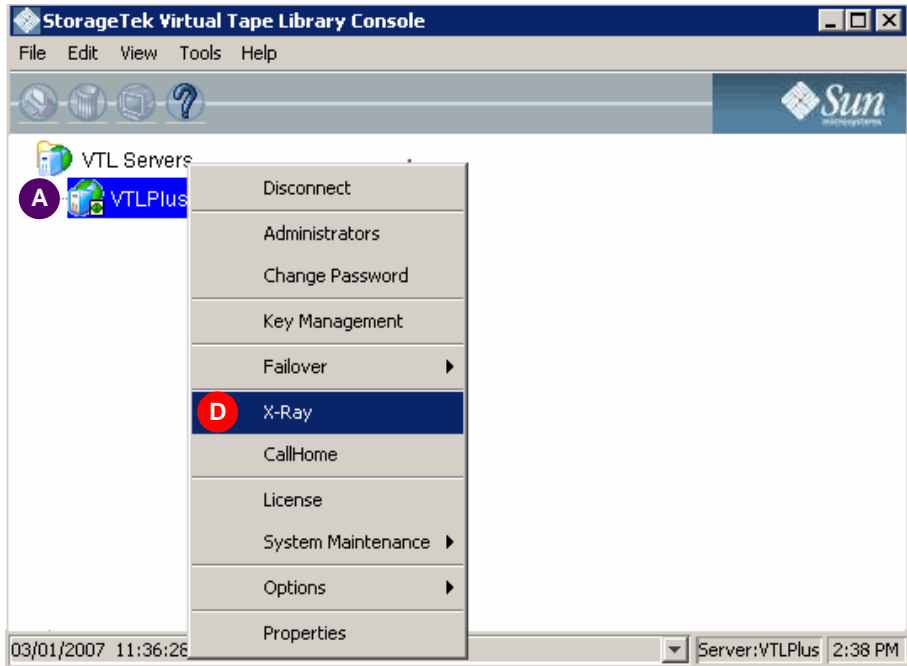
1. If problems persist after other possibilities have been exhausted, examine the VTL Event Log or the server syslog (`/var/adm/messages`) for error messages that relate to the physical tape library or drive.
2. If you find error messages, correct the issues if possible. Stop here, and retry the import/export 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.

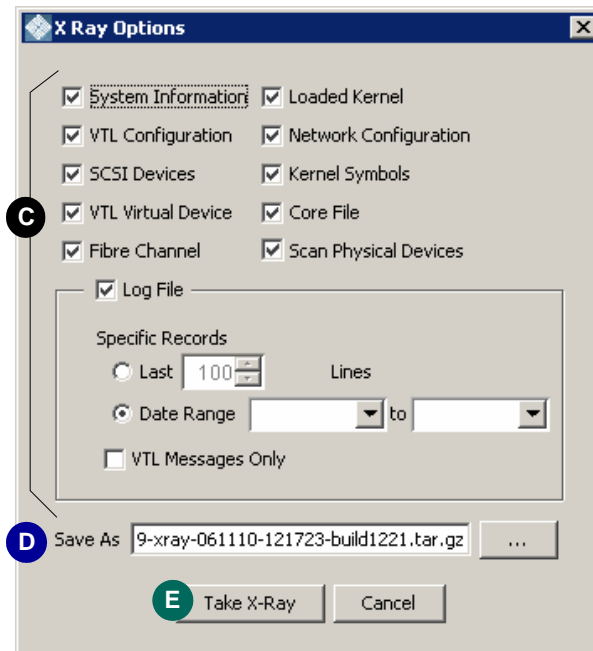
▼ Taking an X-Ray

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.

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.

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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.
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

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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.
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."

Trap	Severity	Message
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.
11006	Error	VTL communication module failed to start.

Trap	Severity	Message
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.

Trap	Severity	Message
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."
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.

Trap	Severity	Message
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.
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).

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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.
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)."

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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.

Trap	Severity	Message
11650	Error	Failed to get capacity size for SCSI device %1.
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.

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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.
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)

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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.

Trap	Severity	Message
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."
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.

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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"
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"

Trap	Severity	Message
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]"
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]"

Trap	Severity	Message
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
40070	Error	Cannot delete Tape %1

Trap	Severity	Message
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't 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)

Trap	Severity	Message
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.
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.

Trap	Severity	Message
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.
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].

Trap	Severity	Message
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 cancelled 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.	<code>create /SP/users/user1 password=password role=administrator operator</code>
Delete a local user.	<code>delete /SP/users/user1</code>
Change a local user's properties.	<code>set /SP/users/user1 role=operator</code>
Display information about all local users.	<code>show -display [targets properties all] -level [value all] /SP/users</code>
Display information about LDAP settings.	<code>show /SP/clients/ldap</code>
Change LDAP settings.	<code>set /SP/clients/ldap binddn=proxyuser bindpw=proxyuserpassword defaultrole=administrator operator ipaddress=ipaddress</code>
Network and Serial Port Setting Commands	
Display network configuration information.	<code>show /SP/network</code>
Change network properties for the ILOM. Changing certain network properties, like the IP address, disconnects your active session.	<code>set /SP/network pendingipaddress=ipaddress pendingipdiscovery=dhcp static pendingipgateway=ipgateway pendingipnetmask=ipnetmask commitpending=true</code>
Display information about the external serial port.	<code>show /SP/serial/external</code>
Change the external serial port configuration.	<code>set /SP/serial/external pendingspeed=integer commitpending=true</code>

Description	Command
Display information about the serial connection to the host.	<code>show /SP/serial/host</code>
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.	<code>set /SP/serial/host pendingspeed=<i>integer</i> commitpending=true</code>
Alert Commands	
Display information about PET alerts. You can configure up to 15 alerts.	<code>show /SP/alert/rules/1...15</code>
Change alert configuration.	<code>set /SP/alert/rules/1...15 destination=<i>ipaddress</i> level=down critical major minor</code>
System Management Access Commands	
Display information about HTTP settings.	<code>show /SP/services/http</code>
Change HTTP settings, such as enabling automatic redirection to HTTPS.	<code>set /SP/services/http port=<i>portnumber</i> secureredirect enabled disabled servicestate=enabled disabled</code>
Display information about HTTPS access.	<code>show /SP/services/https</code>
Change HTTPS settings.	<code>set /SP/services/https port=<i>portnumber</i> servicestate=enabled disabled</code>
Display SSH DSA key settings.	<code>show /SP/services/ssh/keys/dsa</code>
Display SSH RSA key settings.	<code>show /SP/services/ssh/keys/rsa</code>
SNMP Commands	
Display information about SNMP settings. By default, the SNMP port is 161 and v3 is enabled.	<code>show /SP/services/snmp engineid=<i>snmpengineid</i> port=<i>snmpportnumber</i> sets=enabled disabled v1=enabled disabled v2c=enabled disabled v3=enabled disabled</code>
Display SNMP users.	<code>show /SP/services/snmp/users</code>
Add an SNMP user.	<code>create /SP/services/snmp/users/<i>snmpusername</i> authenticationpassword=<i>password</i> authenticationprotocol=MD5 SHA permissions=rw ro privacypassword=<i>password</i> privacyprotocol=none DES</code>
Delete an SNMP user.	<code>delete /SP/services/snmp/users/<i>snmpusername</i></code>
Display information about SNMP public (read-only) communities.	<code>show /SP/services/snmp/communities/public</code>
Add this device to an SNMP public community.	<code>create /SP/services/snmp/communities/ public/<i>comm1</i></code>

Description	Command
Delete this device from an SNMP public community.	<code>delete /SP/services/snmp/communities/public/comm1</code>
Display information about SNMP private (read-write) communities.	<code>show /SP/services/snmp/communities/private</code>
Add this device to an SNMP private community.	<code>create /SP/services/snmp/communities/private/comm2</code>
Host System Commands	
Delete this device from an SNMP private community.	<code>delete /SP/services/snmp/communities/private/comm2</code>
Start the host system.	<code>start /SYS</code>
Stop the host system.	<code>stop /SYS</code>
Reset the host system.	<code>reset /SYS</code>
Start a session to connect to the host console.	<code>start /SP/console</code>
Stop the session connected to the host console.	<code>stop /SP/console</code>
Clock Settings	
Set the ILOM clock to synchronize with a primary NTP server.	<code>set /SP/clients/ntp/server/1 address=ntpIPAddress</code>
Set the ILOM clock to synchronize with a secondary NTP server.	<code>set /SP/clients/ntp/server/2 address=ntpIPAddress2</code>

