



# Sun StorageTek Virtual Tape Library

VTL Plus 2.0 Update 2

**User Guide**

96267  
Rev HH  
July 2009





# Virtual Tape Library

---

## VTL Plus 2.0 (Update 2) User Guide

Sun Microsystems, Inc.  
[www.sun.com](http://www.sun.com)

Part No. 96267  
July 2009, Revision HH

Submit comments about this document at: [g1sfs@sun.com](mailto: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 2008 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 licenciées 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.



Adobe PostScript

# Revision History

---

Name	Part #	Revision	Date	Comments
VTL Plus 2.0 User Guide	96267	A	Mar 2007	
		B	Aug 2007	
		C	Feb 2008	Major revision. Covers VTL Plus 2.0
		D	Mar 2008	Major revision to commandline appendix
		E	May 2008	Updated to VTL Plus 2.0 Update 1
		H	December 2008	Updated to VTL Plus 2.0 Update 2
		HH	July 2009	Minor revisions for Update 2

---



# About this book

---

This book introduces tape virtualization and guides you through the administration of Sun StorageTek VTL Plus 2.0 Update 2 solutions.

## 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).

## Additional Information

Sun Microsystems, Inc. (Sun) offers several methods for you to obtain additional information.

### Sun's External Web Site

Sun's external Web site provides marketing, product, event, corporate, and service information. The external Web site is accessible to anyone with a Web browser and an Internet connection.

The URL for the Sun external Web site is:

<http://www.sun.com>

The URL for Sun StorageTek brand-specific information is:

<http://www.sun.com/storagetek>

### Product Publications

The Sun Documentation Web site provides online access to Sun product publications:

<http://www.docs.sun.com>

To order hardcopy versions of Sun publications, contact a Sun sales or marketing representative.

### Sun Confidential: Internal Only Publications

Sun proprietary internal only documents are available to Sun employees inside the Sun network at:

<http://docs.sfbay/app/docs>

### SDP Support Wiki

The Sun Service Delivery Platform (SDP) Support Wiki is available to Sun employees inside the Sun network at:

<https://csa-wiki.east.sun.com/display/SDP/Home>



## Partners Site

The Sun Partners site is a web site for partners with a Sun Partner Agreement. This site provides information about products, services, customer support, upcoming events, training programs, and sales tools to support partners. Access to this site, beyond the Partners Login page, is restricted. On the Partners Login page, Sun employees and current partners who do not have access can request a login ID and password and prospective partners can apply to become Sun StorageTek resellers.

The URL for partners with a Sun Partner Agreement is:

<http://www.sun.com/partners/>

## Third-Party Web Sites

Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

## Customer Support

Customer support is available 24 hours a day, seven days a week, to customers with Sun or StorageTek maintenance contracts and to Sun employees. The URL for SunStorageTek support is:


<http://www.sun.com/storagetek/support>


## Customer-initiated Maintenance

Customer-initiated maintenance begins with a telephone call from you to Sun Microsystems StorageTek Support. You receive immediate attention from qualified Sun personnel, who record problem information and respond with the appropriate level of support.

To contact Sun Microsystems StorageTek Support about a problem:

1. Use the telephone and call:

 **800.872.4786 (1.800.USA.4SUN)** (inside the United States)

 **800.722.4786** (Canada)

For international locations, go to

<http://www.sun.com/service/contacting/solution.html>

for the appropriate telephone number.

2. Describe the problem to the call taker. The call taker will ask several questions and will either route your call to or dispatch a support representative.

If you have the following information when you place a service call, the process will be much easier:

- Account name
- Site location number
- Contact name
- Telephone number
- Equipment model number
- Device address
- Device serial number (if known)
- Urgency of problem
- Fault Symptom Code (FSC)
- Problem description

## Sun's Worldwide Offices

You may contact any of Sun's worldwide offices to discuss complete storage, service, and support solutions for your organization. You can find address and telephone number information on Sun's external Web site at:

<http://www.sun.com/worldwide/>

## Commenting on this book

Sun welcomes your comments and suggestions for improving this book. Contact us at [glstfs@sun.com](mailto:glstfs@sun.com). Please include the title, part number, issue date, and revision.

# Contents

---

## Introduction

Sun StorageTek VirtualTape Library overview .....	1
Planning your VTL deployment .....	1
VTL configurations for disk-to-disk-to-tape backup .....	2
Standard VTL Configuration .....	2
Advanced VTL Configuration .....	3
Automated Tape Caching VTL Configuration .....	4
VTL components .....	5
Sun VTL Operational Restrictions .....	5

## SAN Zoning for VTL

Zoning for standard-availability systems .....	6
Zoning for high-availability systems .....	6
WWPN zoning (soft zoning) .....	6
Port zoning (hard zoning) .....	7

## Basic Features

Launching the VTL console .....	11
Populating the console .....	11
Discovering VTL server nodes .....	11
Adding a server node to the console tree .....	12
Deleting a server node from the console tree .....	12
Search for tapes .....	13
Understanding the objects in the tree .....	13
VirtualTape Library System object .....	13
Virtual Tape Libraries .....	13
Virtual Tape Drives .....	13
Virtual Vault .....	13
Import/Export Queue .....	13
Physical Tape Libraries .....	14
Physical Tape Drives .....	14
Replica Resources .....	14
Physical Tape Database .....	14
Database .....	14
SAN Clients object .....	14
Reports object .....	14
Create a report .....	15
View a report .....	15
Export data from a report .....	15
Physical Resources object .....	15

---

Rescan physical devices	16
Create virtual tape libraries	17
Create virtual tapes	23
How virtual tapes are allocated from multiple LUNs	25
Round Robin Logic with Tape Capacity on Demand disabled	25
Round Robin Logic with Tape Capacity on Demand enabled	25
Considerations	26
Add SAN Clients (backup servers)	27
Assign virtual tape libraries to clients	28
Assign physical libraries/drives to VTL	29
Import/Export tapes	30
Import a physical tape	30
Export data to a physical tape	32
Export manually	32
Auto Archive function	34
Stacking virtual tapes	36
Encrypt data that is exported to physical tapes	38
Create a key	40
Change a key name or password	41
Delete a key	41
Export a key	42
Import a key	43
Shred a virtual tape	45
Mirror the VTL database	46
Check mirroring status	46
Replace a failed disk	47
Fix a minor disk failure	47
Replace a disk that is part of an active mirror configuration	47
Swap the primary disk with the mirrored copy	47
Remove a mirror configuration	47
Mirroring and Failover	47
Set Console options	48
Manage Administrators	49
Virtual tape drive compression	51
Enable/disable compression	51
View the Event Log	53
Sort the Event Log	54
Filter the Event Log	54
Print/export the Event Log	54
Refer to the Attention Required tab	55
Set Server properties	56
Apply software patch updates	56
Configure VTL to send SNMP traps	57

## Failover

Overview	58
Failover terminology	61
Failover requirements	63

---

Backup server failover configuration .....	65
Windows 2000 .....	65
HP-UX .....	65
AIX .....	65
Failover setup .....	66
Check Failover status .....	71
When failover occurs .....	71
Make changes to the servers in your failover configuration .....	72
Change your failover intervals .....	72
Force a takeover by a secondary server .....	73
Manually initiate a recovery to your primary server .....	73
Suspend/resume failover .....	73
Failover server disaster recovery .....	73
Remove a failover configuration .....	75
Resuming backups after failover/failback .....	76
BakBone NetVault™ .....	76
CommVault Galaxy™ .....	76
CA ARCserve® .....	76
HP OpenView Storage Data Protector .....	76
IBM® Tivoli® Storage Manager .....	76
EMC NetWorker® .....	77
Symantec Backup Exec™ .....	77
Veritas NetBackup™ .....	77
Fibre Channel port behavior during failover .....	78
Sample environment .....	78
Before failover .....	78
When failover occurs .....	78
After failover .....	79
IP address behavior during failover .....	80
Sample environment .....	80
After failover is configured .....	80
When failover occurs .....	80
After failover .....	80
Port swapping for Brocade switches .....	81
HP-UX .....	83
PreTakeOver script .....	83
PreRecovery script .....	83

## Replicate Data

Auto Replication .....	85
Remote Copy .....	86
Replication .....	87
Remote Replication .....	87
Local Replication .....	87
Replication requirements .....	88
Port requirements for replication .....	88
Setup .....	89
Check replication status .....	94

---

Promote a replica resource . . . . .	95
Change your replication configuration options . . . . .	96
Suspend/resume replication schedule . . . . .	96
Stop a replication in progress . . . . .	96
Manually start the replication process . . . . .	96
Remove a replication configuration . . . . .	96
Replication and Failover . . . . .	96
Consolidating tapes from multiple locations to a single data center . . . . .	97

## Automated Tape Caching

Tape caching policies . . . . .	99
Create/change a tape caching policy . . . . .	99
Set global tape caching options . . . . .	103
Disable a policy . . . . .	103
Create a cache for your physical tapes . . . . .	104
Create virtual tapes . . . . .	105
Force migration to physical tape . . . . .	105
Reclaim disk space manually . . . . .	105
Renew cache for a direct link tape . . . . .	105
Recover data using the Automated Tape Caching option . . . . .	107

## Fibre Channel Target Mode

Overview . . . . .	109
Installation and configuration overview . . . . .	110
Configure Fibre Channel hardware on server . . . . .	111
Ports . . . . .	111
Zoning . . . . .	111
Switches . . . . .	112
Persistent binding . . . . .	114
VSA . . . . .	114
QLogic HBAs . . . . .	115
QLogic Multi-ID HBAs . . . . .	117
Multi-ID Driver Failover Configuration . . . . .	117
QLA2X00FS.CONF file . . . . .	118
Configure Fibre Channel hardware on clients . . . . .	120
NetWare clients . . . . .	120
HBA settings for Fibre Channel clients . . . . .	121
Windows 2000/2003 . . . . .	121
HP-UX 10, 11, and 11i . . . . .	122
AIX 4.3 and higher . . . . .	122
Linux – all versions . . . . .	122
Solaris 7, 8, 9, and 10 . . . . .	123
NetWare – all versions . . . . .	123
Verify your hardware configuration . . . . .	124
Set QLogic ports to target mode . . . . .	129
Single port QLogic HBAs . . . . .	129

---

Multi port QLogic HBAs .....	129
Associate World Wide Port Names with clients .....	131

## **iSCSI Clients**

Overview .....	133
Supported platforms .....	133
Windows configuration .....	134
Requirements .....	134
Enable iSCSI .....	134
Register client initiators with your VTL server .....	135
Add your iSCSI client .....	136
Create targets for the iSCSI client to log onto .....	137
Log the client onto the target .....	138
Disable iSCSI .....	138
Linux client configuration .....	139
Prepare the iSCSI initiator .....	139
Add your iSCSI client .....	139
Create targets for the iSCSI client to log onto .....	140
Log the client onto the target .....	141

## **NDMP Backup Support**

Overview .....	142
Configure NDMP Backup Support .....	142

## **ACSLs and Library Station Configuration**

Overview .....	144
Hardware configuration .....	145
Configure VTL to work with ACSLS .....	145
Add/remove tapes .....	146

## **Email Alerts**

Configure Email Alerts .....	147
Modify Email Alerts properties .....	151
Script/program trigger information .....	152
Customize email for a specific trigger .....	152
New script/program .....	152

## **Command Line**

Using the command line utility .....	154
Commands .....	154
Common arguments .....	155
Login/logout to the VTL Server .....	156

---

Virtual devices / Clients	.157
Automated tape caching	.171
System configuration	.175
Import/Export	.177
Replication	.181
Physical devices	.187
Reports	.193
Event Log	.200
Technical support	.201

## Appendix

System security	.202
Console installation	.204
Prerequisite	.204
Installing the console on Solaris platforms	.204
Installing the console on Linux platforms	.205
Installing the console on Microsoft Windows platforms	.205
Launching the VTL console on a remote host	.206
VTL private network addresses	.207
VTL service laptop	.207
VTL Plus 2.0 appliance	.207
VTL Value appliance	.208
VTL Plus 1.0 appliance	.208
ILOM command reference	.210
SNMP traps	.212

## Troubleshooting

General Console operations	.238
Physical resources	.240
Logical resources	.241
Client cannot see tape library/drive as provisioned by VTL	.243
Import/Export	.245
Take an X-ray of your system for technical support	.246

## Index



# *Introduction*

---

## **Sun StorageTek VirtualTape Library overview**

Sun StorageTek VirtualTape Library (VTL) increases the speed and reliability of backups that use standard third party backup applications by leveraging disk to emulate industry standard tape libraries. VTL leverages your existing Fibre Channel or IP SAN to transfer data to and restore data from a disk-based virtual tape at ultra-high speeds.

Since VTL uses disk to back up data, it eliminates the media and mechanical errors that can occur with physical tapes and drives. And, because VTL can emulate more tape drives than your physical tape library really has, more backup streams can run simultaneously, enabling organizations to easily complete their backups within the allotted backup window.

Because you may already have physical tapes that you would like to protect, data from physical tapes can be imported into your virtual tape system. If you ever need to recover files from a physical tape, you can use VTL to access those tapes for immediate recovery.

For additional data protection, the data on virtual tapes can be exported to physical tapes for long-term data archiving. Data can also be copied to physical tapes using your backup application's copy function.

## **Planning your VTL deployment**

When planning your VTL deployment, you need to determine what type of configuration best suits your organization. In addition to disk-to-disk, the flexibility of Sun StorageTek VTL supports three possible disk-to-disk-to-tape (D2D2T) configurations.

In a D2D2T scenario with Sun StorageTek VTL, you choose your preferred configuration of the various components— your third party backup software, the VTL appliance, the disk storage managed by VTL for use as the virtual tape library, and one or more physical tape libraries. Regardless of which configuration you choose, VTL makes it easy for you to manage both virtual tapes and physical tapes.

---

## VTL configurations for disk-to-disk-to-tape backup

- **Standard Configuration** - Backup software runs on a backup server and manages all tapes—virtual and physical. Data is copied to physical tape using the backup software's tape copy function.
- **Advanced Configuration** - Backup software runs on a backup server and manages the backup to virtual tape. VTL manages the disk storage and the export of data to the physical tape library.
- **Automated Tape Caching Configuration:** As in the *Advanced Configuration*, backup software runs on a backup server and transparently manages the backup to virtual tape. In addition, this configuration provides the backup application with transparent access to data regardless of whether the data is on disk or on tape. Flexible migration policies determine when data will be moved to physical tape.

### Standard VTL Configuration



In the Standard VTL Configuration, the backup software manages all tapes—virtual and physical—by treating the virtual tape library as though it were just another standalone tape library attached to the backup server. To copy data from virtual to physical tapes, the backup software's *Tape Copy* function is utilized.

In this configuration, the backup software runs on an existing backup server.

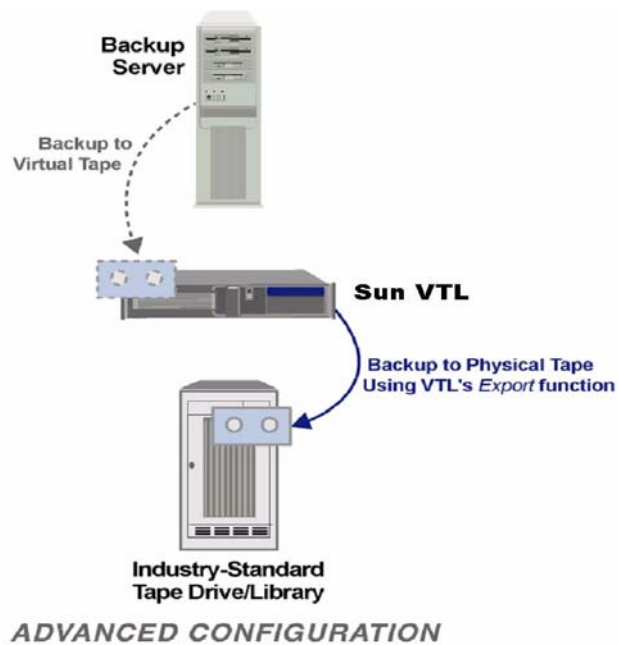
The Standard VTL Configuration is ideal for organizations that already have a backup process in place with which they are comfortable but which is not meeting all of their backup objectives. Adding a VTL appliance as another tape library allows you to easily increase your parallel backup streams and take advantage of VTL's

---

rapid data recovery without having to alter your current configuration. With the backup application managing the entire backup process, virtual tapes and physical tapes are seen in the same way: a virtual tape is *just another tape*.

With the Standard VTL Configuration, backups to virtual tapes occur quickly. Then, at a later time, the backup server can copy the data to physical tapes without impacting the production environment. Because the backup server performs the tape copying function in addition to backups, additional overhead can be incurred by the backup server. Therefore, it is best to perform tape copying at off-peak hours.

### Advanced VTL Configuration



In the Advanced VTL Configuration, the backup software manages backups to the virtual tape library while the VTL appliance controls the export of data from virtual tapes to physical tapes.

VTL dramatically accelerates backups by acting as a *de facto* cache to your physical tape library and enables data to be moved to physical tapes as a background process without impacting production servers. This is an innovative approach to backup that addresses the limitations of conventional tape backup. Moreover, since VTL manages the export of data from virtual to physical tapes, there is no additional overhead for the backup server.

As in the Standard VTL Configuration, the backup software runs on an existing backup server.

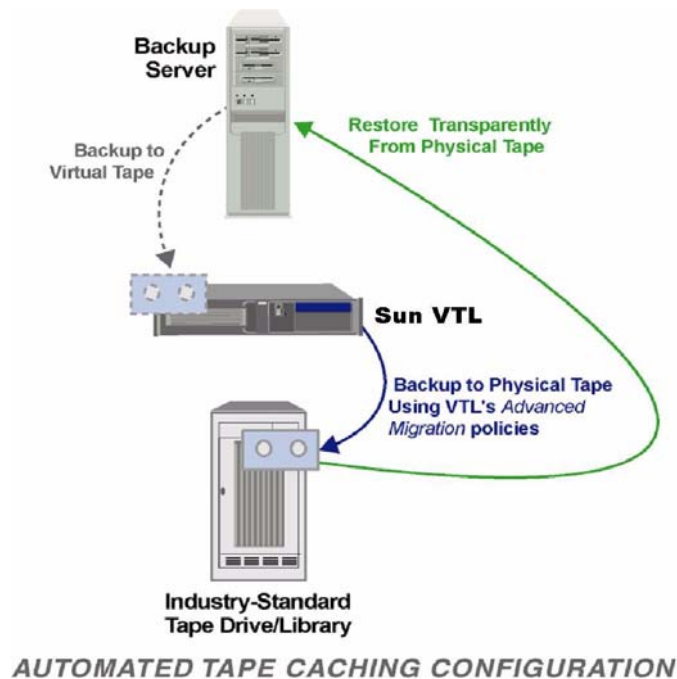
With the Advanced VTL Configuration, backups to virtual tapes occur very quickly. Then, at a later time, when you are done using a given tape, you can export data to physical tape for offsite vaulting or disaster recovery without impacting the production environment. VTL can also be set up in Auto Archive mode so that after each backup to virtual tape completes, data is automatically exported to physical tape.

The Advanced VTL Configuration requires you to set up the initial physical tape library emulation from within the VTL Console so that there is a 1:1 mapping, with identical barcodes, between virtual and physical tapes. This enables the backup software to keep track of backup tapes and prevents tapes from being created that would be unidentifiable by the backup software.

Whenever data is written to physical tape, the virtual tape can then be deleted or the copy can be left on the virtual tape for rapid recovery. The physical tape will always have the same barcode as its virtual tape counterpart. This gives you the flexibility to easily restore from either virtual or physical tape.

When it comes time to restore, the backup software identifies the barcode of the tape containing the needed data. If the data still resides on virtual tape (it was never exported or it was exported with the virtual tape left intact), it can be restored very quickly because it is being read from disk. If the data is only on physical tape, the tape must first be re-imported into VTL with a few simple keystrokes in the VTL Console so that the backup software can access it and restore in its usual manner.

## *Automated Tape Caching VTL Configuration*



---

The Automated Tape Caching option enhances the functionality of VTL by acting as a cache to your physical tape library, providing transparent access to data regardless of its location.

With the Automated Tape caching option, tapes will always appear to be inside virtual libraries and will be visible to the backup application regardless of whether the data is actually on disk or tape. This means that the backup application will always have direct access to data regardless of whether the data is on disk or on physical tape.

As in the Advanced VTL Configuration, backup software runs on a backup server and transparently manages the backup to virtual tape.

In this configuration, VTL acts as a transparent cache to the physical tape library, dramatically accelerating backups while enabling the data to be written to physical tapes, as a background process without impacting production servers, based on extremely flexible migration policies (age of data, time of day, disk space, end of backup, etc.). The Automated Tape Caching Option also provides very flexible space reclamation policies (free space immediately upon migration, after specified retention period, when run out of space, etc.)

## VTL components

There are three components to VTL:

- VTL Server - Manages the VTL system.
- VTL Console - The graphical administration tool where you configure VTL, add/configure clients, set properties, and manage the import/export of tapes.
- VTL Clients - The backup servers that use the VTL. VTL supports Fibre Channel, SCSI, and iSCSI backup servers on most major platforms.

## Sun VTL Operational Restrictions

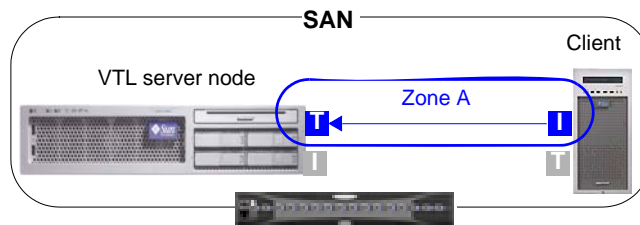
VTL Plus and VTL Prime are appliances running a specialized version of Solaris 10 on Sun Servers with Sun disk arrays. They use specific versions of software, firmware and configuration scripts that have been tuned for VTL. These cannot be viewed as individual components such as Solaris 10 on a server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

# SAN Zoning for VTL

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

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.

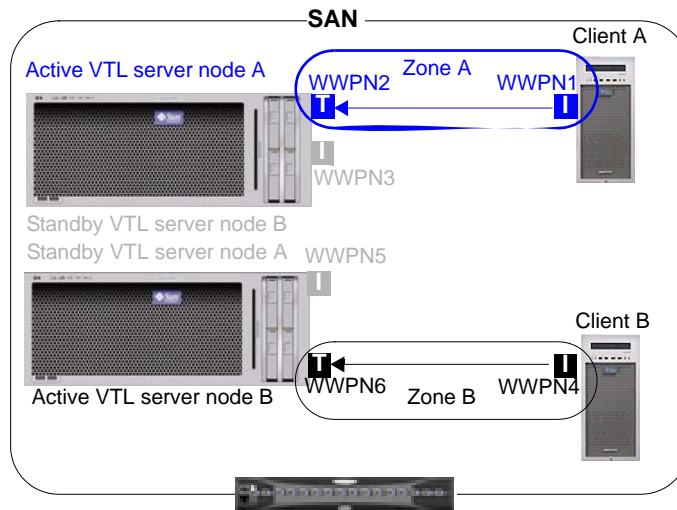
## Zoning for high-availability systems

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).

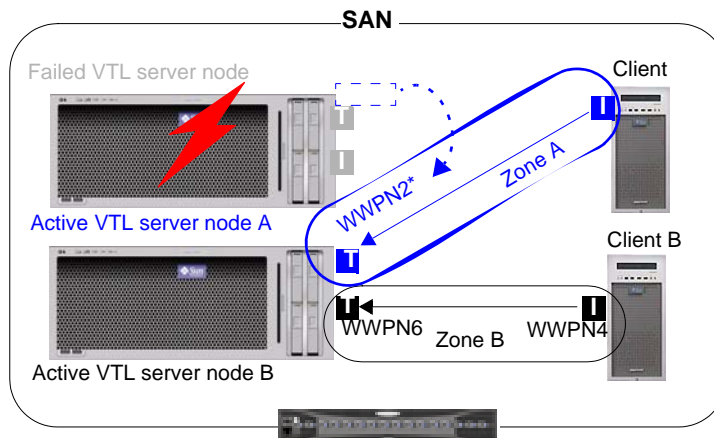
## WWPN zoning (soft zoning)

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.

The figure below shows a soft-zoned SAN before VTL failover:

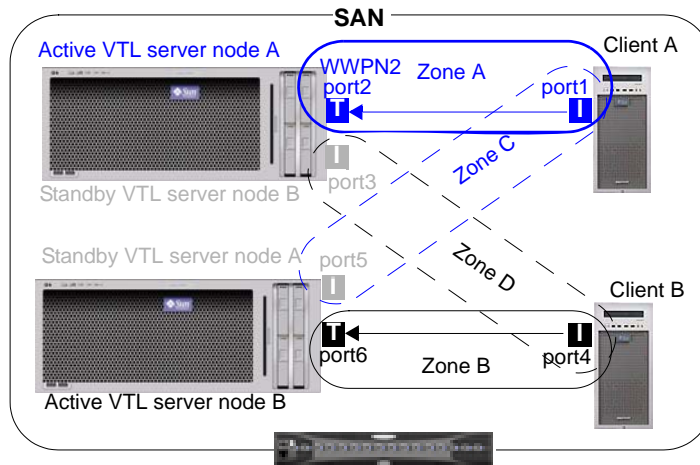


During failover, the zone still contains only one initiator and one target at a time. But the target WWPN is remapped from a port on the failed server node to a physical port on the standby server. The standby physical port spoofs the WWPN of the failed port, so zoning does not change. The figure below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



## Port zoning (hard zoning)

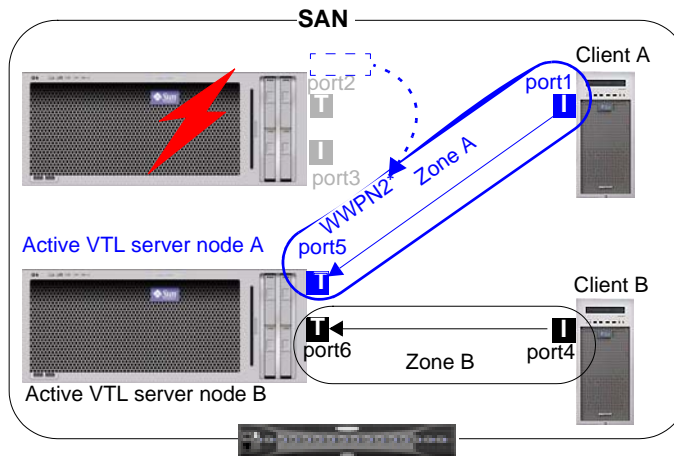
A hard-zoned SAN maps initiator to target using a physical port address. This port-to-port zoning establishes a fixed, physical route through the SAN. So, since each SAN zone can contain only one initiator and one target, you must provide two zones for each initiating client. The figure below shows a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





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

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

# Basic Features

The VTL Console displays the configuration for your VTL appliance.

The 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 (see “Appendix” on page 202). Note, however, that no more than two (2) instances of the console can access the same VTL server at the same time.

The console information is organized in a familiar Explorer-like tree view.

The screenshot shows the StorageTek Virtual Tape Library Console interface. On the left is a tree view with the following structure:

- VTL Servers
  - VTLServer232 (selected)
  - VirtualTape Library System
    - SAN Clients
    - Reports
    - Physical Resources
  - VTLserver238

The main area displays the configuration for VTLServer232. It includes tabs for General, Event Log, and Version Info. The configuration is presented in a table:

Name	Value
Server Name	VTLServer232
Login Machine Name	10.6.2.232
Login User Name	root
O.S. Version	SunOS 5.10
Kernel Version	SunOS 5.10 Generic_118855-14 i86pc
Processor 1 - 2	AMD Opteron(tm) Processor 850 2389 MHz
Network Interface	bge0 - mtu 1500 inet 10.6.2.232 mac 0:9:3d:14:77:28
Protocol(s)	Fibre Channel
Admin Mode	Read/Write
Server Status	Online
System Up Time	2 days 28 minutes 40 seconds
VTL Up Time	1 day 21 hours 46 minutes 54 seconds
Fibre Channel WWPN	21-00-00-e0-8b-81-a4-36 [initiator]
Fibre Channel WWPN	21-01-00-e0-8b-a1-a4-36 [target]
Fibre Channel WWPN	21-00-00-e0-8b-83-61-8f [target]
Fibre Channel WWPN	21-01-00-e0-8b-a3-61-8f [initiator]
Fibre Channel WWPN	21-02-00-e0-8b-c3-61-8f [initiator]
Fibre Channel WWPN	21-03-00-e0-8b-e3-61-8f [initiator]

Below the table is a section for System Drive Usage, showing a pie chart and a table:

System / VTL Log Drive (/dev/dsk/c110d0s0)	System Log	0.25%
Disk capacity:	17.73 GB	0.00%
Space available:	14.52 GB	17.82%
	Free	81.93%

The pie chart shows the distribution of disk space: Free (81.93%, green), Others (17.82%, yellow), VTL Logs (0.00%, blue), and System Log (0.25%, red). A Refresh button is located below the table.

The status bar at the bottom shows: 11/06/2006 12:59:28 [VTLServer232] Logged in | Server:VTLServer232 | 2:02 PM

The tree allows you to navigate the various VTL appliances and their configuration objects. You can expand or collapse the display to show only the information that you wish to view. To expand an item that is collapsed, click on the symbol next to the item. To collapse an item, click on the symbol next to the item. Double-clicking on the item will also toggle the expanded/collapsed view of the item.

You need to connect to a server before you can expand it.

---

When you highlight any object in the tree, the right-hand pane contains detailed information about the object. You can select one of the tabs for more information.

The Console log located at the bottom of the window displays information about the local version of the Console. The log features a drop-down box that allows you to see activity from this Console session.

## 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 &
```

## Populating the console

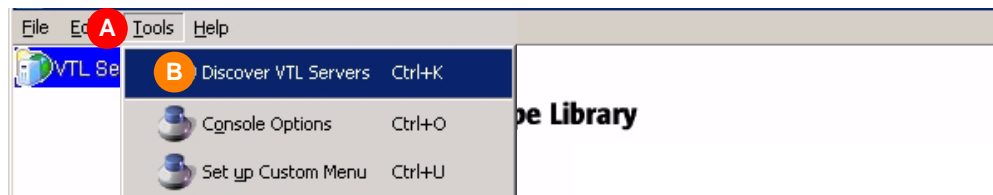
Once the console is running, you can specify the VTL servers that you want to see in the object tree at the left side of the VTL console. You can discover, add, or remove servers.

Note, however, that no more than two (2) instances of the console can access the same VTL server at the same time

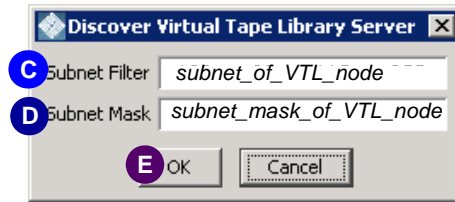
## Discovering VTL server nodes

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).



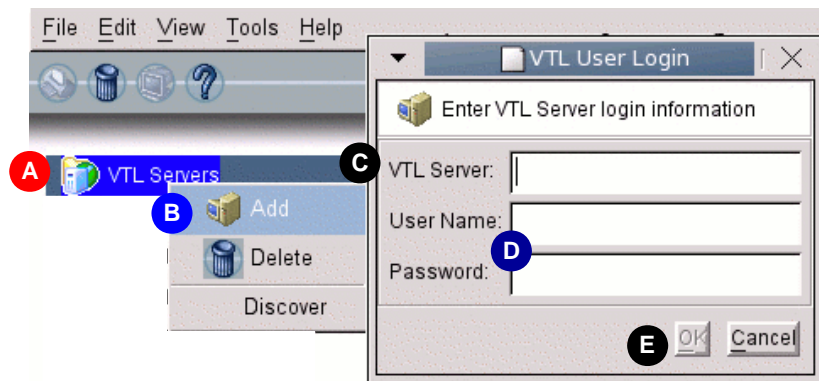
2. When the `Discover Virtual Tape Library Server` dialog appears, enter the subnet filter (C below) and subnet mask (D) for the VTL appliance. Then press `OK` (E).



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).

## 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).

## Deleting a server node from the console tree

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

1. From the context menu, select `Delete`.
2. When the confirmation dialog appears, select `Yes`.

---

## Search for tapes

The Console has a search feature that helps you find any virtual tape. To search:

3. Select *Edit* menu --> *Find*.
4. Enter the full barcode.

Once you click *Search*, you will be taken directly to that tape in the tree.

## Understanding the objects in the tree

### *VirtualTape Library System object*

The *VirtualTape Library System* object contains all of the information about your VTL system:

#### Virtual Tape Libraries

This object lists the virtual tape libraries that are currently available. Each virtual tape library consists of one or more virtual tape drives and one or more virtual tapes. Each virtual tape library and drive can be assigned to one or more backup servers (SAN clients). Each library's virtual tapes are sorted in barcode order.

For each library, you can:

- Create/delete virtual tapes
- Create/delete virtual tape drives
- Enable replication for tapes in the library
- Set Automated Tape Caching policies (if you are using this option)
- Set tape properties for the library (enable/modify tape capacity on demand, change maximum tape capacity)

For each virtual tape, you can:

- Move the virtual tape to a slot, drive, or to the virtual vault
- Enable replication for that tape or make a single remote copy
- Change tape properties (change barcode, enable/modify tape capacity on demand, enable write protection, and configure Auto Archive/Replication)

#### Virtual Tape Drives

This object lists the standalone virtual tape drives that are currently available. Each virtual tape drive can be assigned to one or more backup servers (SAN clients). For each virtual tape drive, you can create/delete virtual tapes.





#### Virtual Vault

This object lists the virtual tapes that are currently in the virtual vault. The virtual vault is a tape storage area for tapes that are not inside a virtual tape library. Virtual tapes will only appear in the virtual vault after they have been moved from a virtual tape library. Virtual tapes in the vault can be replicated, exported to a physical tape, or moved to a virtual library or standalone drive. There is no limit to the number of tapes that can be in the virtual vault. Tapes in the vault are sorted in barcode order.

#### Import/Export Queue

This object 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.

- 
- Physical Tape Libraries      This object lists the physical tape libraries that are available to VTL. For each physical tape library, you can inventory the slots and import or move a tape. For each physical tape, you can export the physical tape, copy the physical tape to a virtual tape, or link the physical tape to a virtual tape for direct access.
  
  - Physical Tape Drives      This object lists the standalone physical tape drives that are available to VTL. For each physical tape drive, you can check for a physical tape and eject the physical tape. For the physical tape, you can eject a physical tape, copy the physical tape to a virtual tape, or link the physical tape to a virtual tape for direct access.
  
  - Replica Resources      This object lists the Replica Resources that are on this VTL server. Replica Resources store data from virtual tapes that has been replicated from a remote server. Clients do not have access to Replica Resources.
  
  - Physical Tape Database      The physical tape database maintains a history of all physical tapes that were used for export jobs (including stacked tapes). Physical tape entries can be removed from the database by manually purging them.
  
  - Database      This object contains configuration information for the VTL. The database can be mirrored for high availability. Refer to '[Mirror the VTL database](#)' for more detailed information.
  
  - VirtualTape icons      The following table describes the icons that are used to describe virtual tape drives and virtual tapes in the console:

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

### *SAN Clients object*

SAN clients are the backup servers that use the VTL. VTL supports Fibre Channel and iSCSI backup servers. For client configuration information, refer to the appropriate sections in this guide.

### *Reports object*

VTL provides reports that offer a wide variety of information:

- Throughput

- Physical resources - allocation and configuration
- Disk space usage
- Fibre Channel adapters configuration
- Replication status
- Virtual tape/library information
- Job status

- Create a report
1. To create a report, right-click on the *Reports* object and select *New*.
  2. Select a report.  
Depending upon which report you select, additional windows appear to allow you to filter the information for the report.
  3. If applicable, set the date or date range for the report and indicate which SAN Resources (physical tape libraries/drives) and Clients to use in the report.  
Selecting *Past 30 Days*, or *Past 7 Days* will create reports that generate data relative to the time of execution.  
*Include All SAN Resources and Clients* – Includes all current and previous configurations for this server (including physical tape libraries/drives and clients that you may have changed or deleted).  
*Include Current Active SAN Resources and Clients Only* – Includes only those physical tape libraries/drives and clients that are currently configured for this server.  
The *Replication Status Report* has a different dialog that lets you specify a range by selecting starting and ending dates.
  4. Enter a name for the report.
  5. Confirm all information and click *Finish* to create the report.
- View a report
- When you create a report, it is displayed in the right-hand pane and is added beneath the *Reports* object in the configuration tree.
- Expand the *Reports* object to see the existing reports available for this server.
- When you select an existing report, it is displayed in the right-hand pane.
- Export data from a report
- You can save the data from the server and device throughput and usage reports. The data can be saved in a comma delimited (.csv) or tab delimited (.txt) text file. To export information, right-click on a report that is generated and select *Export*.

## *Physical Resources object*







Physical resources are all of your SCSI adapters/FC HBAs and storage devices. Storage devices include hard disks, tape drives, and tape libraries. Hard disks are used for creating virtual tape libraries/drives and virtual tapes.

---

From *Physical Resources*, you can prepare new hardware and rescan devices.

Physical  
resource icons

The following table describes the icons that are used to describe physical resources in the console:

Icon	Description
	The T icon indicates that this is a target port.
	The I icon indicates that this is an initiator port.
	The red arrow indicates that this Fibre Channel HBA is down and cannot access its storage.
	The V icon indicates that this disk has been virtualized.
	The D icon indicates that this is a physical tape library or drive.
	The F icon indicates that this is shared storage and is being used by another server. The <i>Owner</i> field lists the other server.

## Rescan physical devices

1. To rescan devices, right-click on *Physical Resources* and select *Rescan*.

You only rescan at the adapter level but Solaris only supports a system rescan, which rescans all adapters.

2. Determine what you want to rescan.

If you are discovering new devices, set the range of adapters, SCSI IDs, and LUNs that you want to scan.

*Use Report LUNs* - The system sends a SCSI request to LUN 0 and asks for a list of LUNs. Note that this SCSI command is not supported by all devices.

*Stop scan when a LUN without a device is encountered* - This option will scan LUNs sequentially and then stop after the last LUN is found. Use this option only if all of your LUNs are sequential.



## Create virtual tape libraries

You can create a virtual tape library in the following two ways:

- Use the configuration wizard - If you have already configured your system, you can launch the wizard by right-clicking on the *VirtualTape Library System* object in the console and selecting *Configuration Wizard*.
- Right-click on the *Virtual Tape Libraries* object and select *New*.



Note: If you have recently added additional storage to your VTL system, before you can use it to create a virtual tape library, you must reserve it for virtual use. To do this: Right-click on *Physical Resources* and select *Prepare Devices*. Set hard drives to *Reserved for Virtual Device*.

1. Select the tape library that you are emulating.

Vendor ID	Product ID	Revision	Maximum Drives	Maximum Slots
STK	L700	3.05	20	678

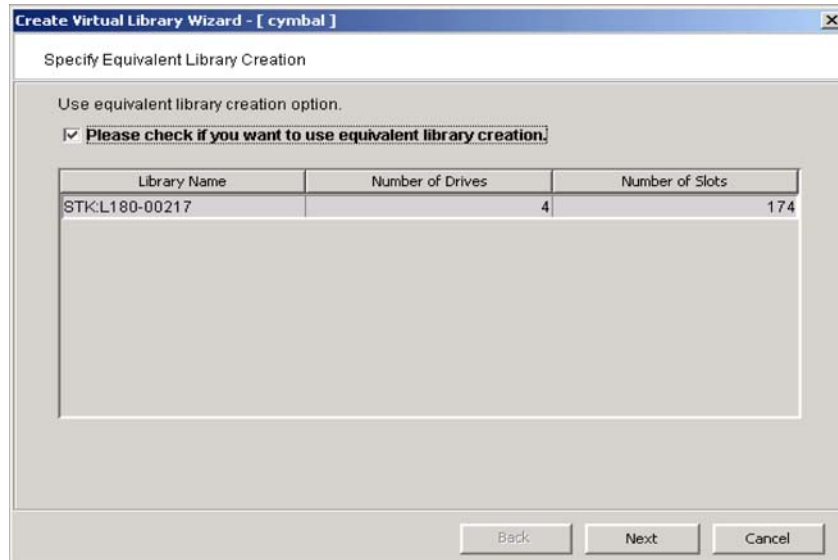
If you have a physical tape library, you should create a virtual tape library that resembles it. This way the virtual tapes will use the same format as those of the physical tapes. This is important for importing and exporting functions and guarantees that your backup application will accept the tapes.

If you are using the *Automated Tape Caching* option, you will only see your available (not already configured) physical tape libraries listed. Select the check box and the system will automatically match your virtual library to the physical library.

Note: Sun has certified the Sun VTL virtual tape library with backup vendors. Customers should use only this library (it can be configured with whatever drives and however many cartridges they need, but it is preconfigured with the same characteristics as a Sun L700 library). For backend libraries, Sun will only support Sun StorageTek branded library types.



Note: The automatic matching of virtual libraries to physical libraries is not available for ACSLS-managed libraries.



2. Enter information about the tape drives in your library.

*Virtual Drive Name Prefix* - The prefix is combined with a number to form the name of the virtual drive.

*Total Virtual Drives* - Determines the number of virtual tape drives available. This translates into the number of concurrent backup jobs that can run. Backup software licensing considerations may affect the number of tape drives you wish to present to each client server. This number can exceed the standard number of drives for the library as long as the backup software supports it.

3. If you are using the Automated Tape Caching option, select *Enable Automated Tape Caching* and specify your migration and reclamation triggers.

For detailed information about Automated Tape Caching, refer to '[Automated Tape Caching](#)'.

4. (Non Tape Caching environments) Determine if you want to use auto archive/replication for this virtual library.

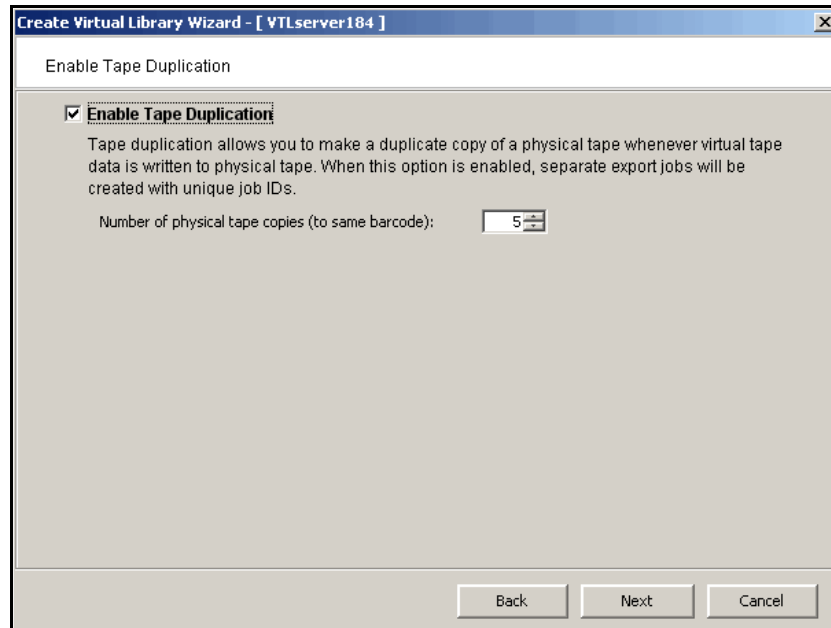
The screenshot shows the 'Create Virtual Library Wizard' dialog box with the title 'Create Virtual Library Wizard - [ VTL-NewYorkOffice ]'. The main heading is 'Enter Virtual Library Information.' Below this, there are two main sections: 'Auto Archive / Replication' and 'Auto Replication'. The 'Auto Archive / Replication' section is active, indicated by a checked checkbox. It contains two radio buttons: 'Auto Archive' (selected) and 'Auto Replication'. Under 'Auto Archive', there are two sub-radio buttons: 'Copy' and 'Move' (selected). Below these is a text box for 'The grace period before deleting the tape' with a value of '7' and a unit dropdown set to 'day(s)'. There are two checkboxes: 'Export physical tapes to IE slots after export' (checked) and 'Encrypt data when exporting to physical tape with the selected key.' (unchecked). Below the second checkbox is a 'Select a Key:' dropdown menu. The 'Auto Replication' section is inactive. It has two radio buttons: 'Auto Replication' (selected) and 'Auto Archive'. Under 'Auto Replication', there are two sub-radio buttons: 'Copy' (selected) and 'Move'. Below these is a text box for 'The grace period before deleting the tape' with a value of '0' and a unit dropdown set to 'day(s)'. Below this is a 'Remote server name:' dropdown menu with an 'Add' button next to it. At the bottom of the dialog are three buttons: 'Back', 'Next', and 'Cancel'.

You can select either *Auto Archive* or *Auto Replication* for a virtual library, but not both.

*Auto Archive* writes data to physical tape whenever a virtual tape is *moved* to an IE slot by a backup application or other utility after a backup. (You will see the tape in the virtual vault.) In order to use *Auto Archive* the physical tape library must support barcodes because when VTL attempts to export to physical tape it must find a matching barcode in a physical library (you do not need to specify which physical library). If you select *Auto Archive*, determine if you want the virtual tape copied (retained) or moved (removed) after the data is transferred. If you select *Move*, indicate how long to wait before deleting it. Also, indicate if you want to export your *physical* tapes to the library's import/export slots after archiving. You can encrypt the data while exporting as long as you have created at least one key. (For more information, refer to ['Encrypt data that is exported to physical tapes'](#).)

*Auto Replication* replicates data to another VTL server whenever a virtual tape is moved to an IE slot from a virtual library (such as from a backup application or other utility). If selected, determine whether you want the virtual tape copied (retained) or moved (removed) after the data is replicated. If you select *Move*, indicate how long to wait before deleting it. Also, select the remote server from the list of existing target servers. You can also click *Add* to add another VTL server.

5. Indicate if you want to use tape duplication.



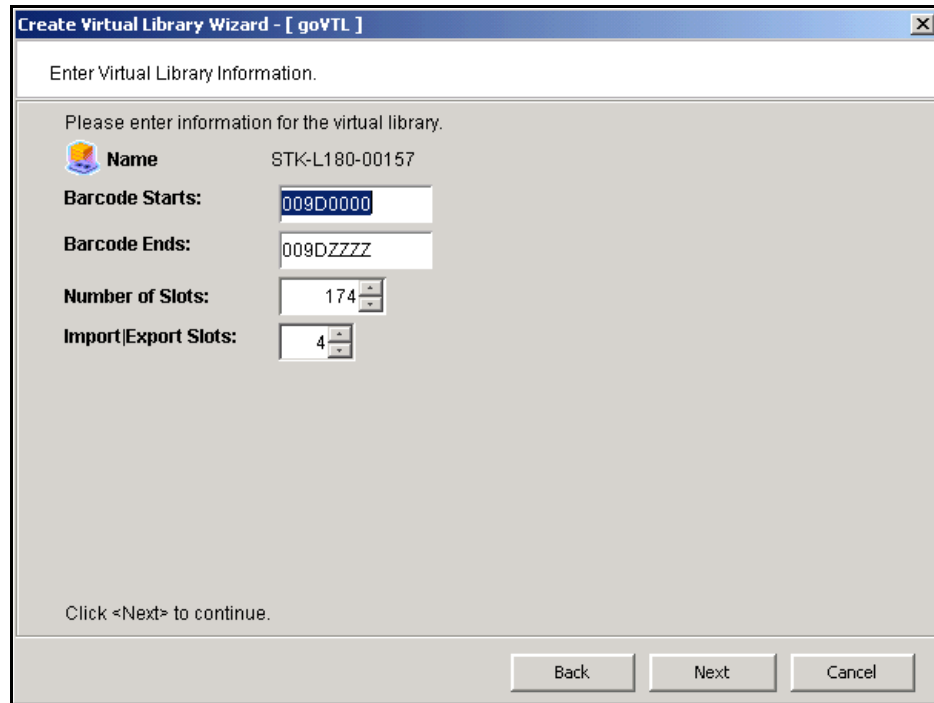
Tape duplication allows you to make up to five duplicate copies of a physical tape whenever virtual tape data is exported to physical tape. You must have at least two identical physical libraries (same model, same number of drives, same tapes with the same barcodes). When data is exported, separate export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

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

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

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

6. Enter barcode information for the virtual library.



Enter Virtual Library Information.

Please enter information for the virtual library.

**Name** STK-L180-00157

**Barcode Starts:** 009D0000

**Barcode Ends:** 009DZZZZ

**Number of Slots:** 174

**Import|Export Slots:** 4

Click <Next> to continue.

Back Next Cancel

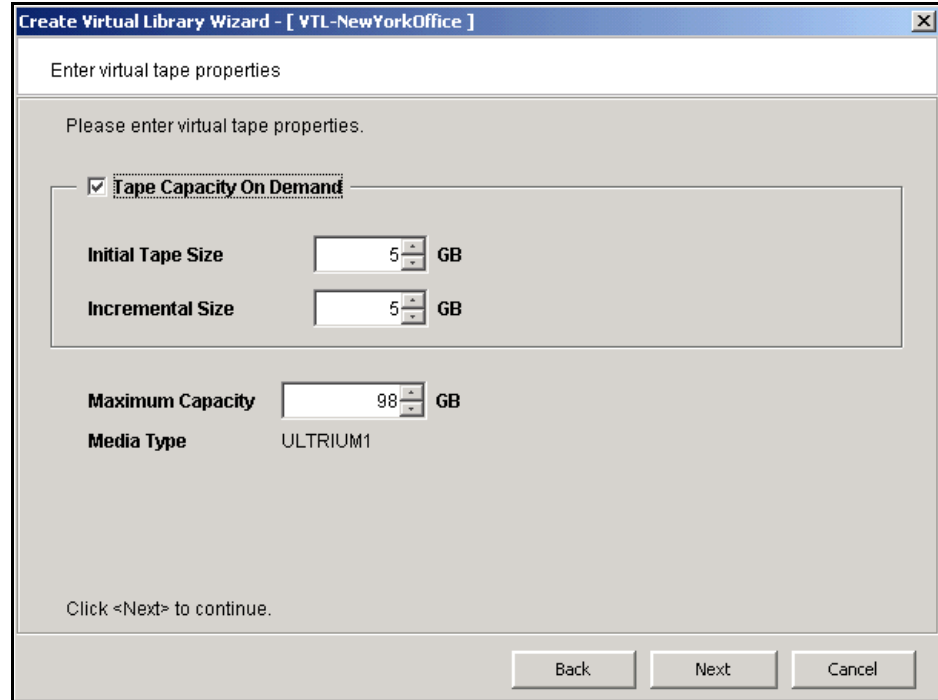
*Barcode Starts/Ends* - Indicate a range of barcodes that will be used when creating virtual tapes. By default, barcodes increment in an alphanumeric sequence; for example, **XXX0009** to **XXX000A**. In order to set the barcode to increment in a numeric sequence (**XXX0009** to **XXX0010**), you have to set the last three digits of the *Barcode Ends* field to **999**; for example, **XXX0999**

Note that for IBM libraries, the default barcode range is set to six characters.

*Slot* - Maximum number of tape slots in your tape library.

*Import/Export Slots* - Number of slots used to take tapes in and out of the bin.

7. Enter the guidelines for expanding virtual tape capacity.



*Tape Capacity On Demand* - Allows you to create small resources for your tapes and then automatically allocate additional space when needed. This can save considerable amounts of disk space without affecting system performance. If you do not select this option, VTL will allocate each virtual tape at the full size of the tape you are emulating.

*Initial Tape Size/Incremental Size* - Enter the initial size of each resource and the amount by which it will be incremented.

*Maximum Capacity* - Indicate the maximum size for each tape.

- If you will *not* be exporting data to physical tape, you can enter any maximum capacity.
- If you *will* be exporting data to physical tape but you will not be using VTL's compression, you can enter any maximum capacity, but if you enter a capacity that exceeds the native uncompressed capacity for the media, you may not be able to export to physical tape.
- If you *will* be exporting data to physical tape *and you will* be using VTL's software compression, you should set the maximum capacity to 10-15% less than the uncompressed capacity of the selected media. This is because VTL's compression algorithm can vary depending upon the dataset; certain file types (ZIP, PDF, GIF, RAR, etc.) are already compressed and cannot be compressed further.

8. Verify all information and then click *Finish* to create the virtual tape library.

You will be prompted to create virtual tapes. Answer *Yes* to continue. Refer to the following section for more information about creating virtual tapes.

---

## Create virtual tapes

You can create virtual tapes in the following two ways:

- Use the configuration wizard - If you have already configured your system, you can launch the wizard by right-clicking on the *VirtualTape Library System* object in the console and selecting *Configuration Wizard*.
  - Right-click on a virtual tape library or on the *Tapes* object and select *New Tape(s)*.
1. Select how you want to create the virtual tape(s).

*Custom* lets you select which physical device(s) to use and lets you designate how much space to allocate from each.

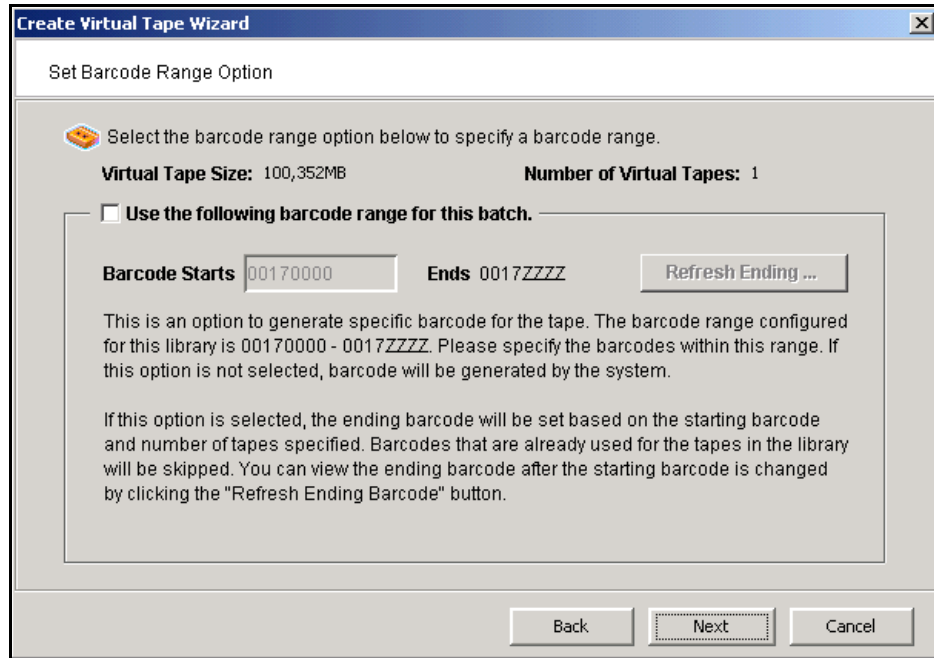
*Express* automatically creates the resource(s) for you using an available device(s). If you select *Express*, you can create multiple virtual tapes at the same time.
  2. Specify which physical device should be used to create the virtual tapes.
  3. If *Auto Archive* is enabled for the virtual library, select the physical tape(s) you want to match.

This enables you to have a physical tape with a barcode that matches your virtual tape. This is important for exporting functions.
  4. If *Auto Replication* is enabled for the virtual library and you want it enabled for this/these tapes, select the target server.

You will be asked to confirm the hostname/IP address and indicate how long the system should attempt to replicate data before timing out and how often it should attempt to retry before skipping a scheduled replication.

Then, indicate if you want to use the *Compression* and/or *Encryption* options. The *Compression* option provides enhanced throughput during replication by compressing the data stream. The *Encryption* option secures data transmission over the network during replication.
  5. Depending upon which method you selected, specify the size of the tape(s), name, and number of tapes to create.

6. If desired, set a barcode range for the virtual tapes you are creating.



7. Verify all information and then click *Finish* to create the virtual tape(s).



---

## How virtual tapes are allocated from multiple LUNs

*Round Robin Logic* is the algorithm VTL uses when allocating new tapes from multiple LUNs. This logic ensures that tapes are evenly distributed across all LUNs rather than having multiple tapes allocated on a single LUN, which will decrease the performance of the storage unit.

VTL chooses the LUN from which the tape will be allocated according to the amount of space the LUN has available. The LUN with the most available space will be selected for the tape. You can view the amount of available space on each LUN by highlighting Storage Devices under Physical Resources in the left pane of the VTL Console. When a virtual tape is deleted, the allocated space will be freed on its specified LUN.

Note that it is possible for a virtual tape to be created from multiple LUNs. This will happen if a virtual tape has a larger capacity than the available space of the initial LUN from which the tape is allocated.

### *Round Robin Logic with Tape Capacity on Demand disabled*

When Tape Capacity on Demand is disabled, the entire capacity of the virtual tape will be allocated on the LUN at once. There is no way for VTL to free any unused allocated space on the LUN unless the virtual tape is deleted.

As an example, let us say that the user has three LUNs: LUN1, LUN2, and LUN3. LUN1 has a total of 100 GB available. LUN2 has a total of 200 GB available. LUN3 has a total of 300 GB available. When the user attempts to create a tape that is 200 GB, it will be allocated from LUN3 because this LUN has the most available space. When this tape is created, the available space on LUN3 will become 100 GB. When the user attempts to create a second tape that is 100 GB, it will be allocated from LUN2 because this LUN currently has the most available space.

### *Round Robin Logic with Tape Capacity on Demand enabled*

When Tape Capacity on Demand is enabled, the user has the option to specify the following values: Initial Tape Size, Incremental Size, and Maximum Capacity.

Only the Initial Tape Size of the virtual tape will be allocated on the LUN. The Incremental Size tells VTL how much additional space needs to be allocated as the tape expands.

The Tape Capacity on Demand logic attempts to expand the tape on the same LUN, provided there is enough space available. If there is not enough space available, VTL will expand the virtual tape across another LUN using the round robin logic and the LUN selected will be the one with the most available space.

VTL will allocate the minimum amount of space that the virtual tape needs, depending upon how much data is written and the incremental size specified.

---

If the user decides to erase all of the data on the tape, VTL will free up the allocated space, except for the initial size. The initial size will remain allocated. If the user decides to erase a portion of the tape, the allocated space will be freed up until the rewind point on the tape.

### *Considerations*

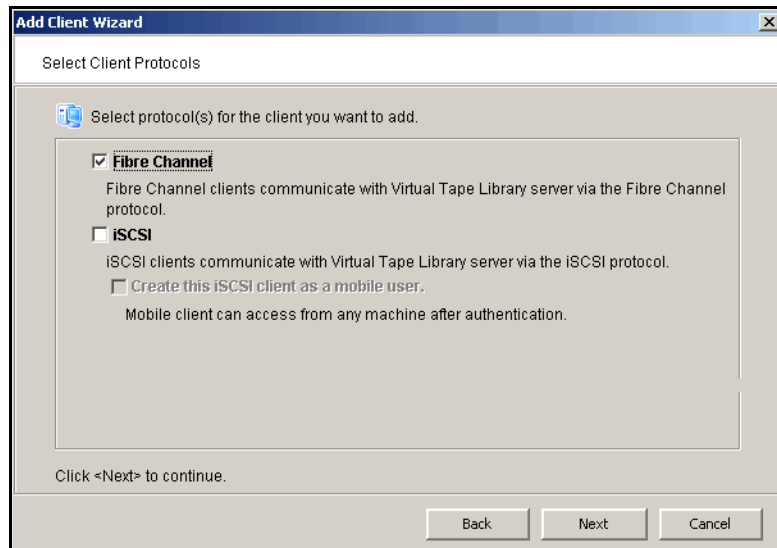
Initially, tape creation will use round robin logic because each LUN has exactly one segment. Once the LUNs start to have holes and different segments are deleted, the round robin logic will begin to diminish. This is because VTL will need to take into account the segments that become available. Therefore, VTL will consider larger segments on a LUN to be the preferred choice in allocating space. At times, even if a LUN has more space available, it will not be the preferred choice by VTL to allocate a tape. Instead, VTL will choose a LUN with a larger segment size.

---

## Add SAN Clients (backup servers)

You can add SAN Clients in the following two ways:

- Use the configuration wizard - If you have already configured your system, you can launch the wizard by right-clicking on the *VirtualTape Library System* object in the console and selecting *Configuration Wizard*.
  - Right-click on the *SAN Clients* object and select *Add*.
1. Enter the client name.
  2. Select the protocol being used by the client.



3. Identify your backup server.

**For Fibre Channel clients**, click *Next* and select the *initiator* WWPN for the client. Note that if the client WWPN is in a zone, it will automatically let you select initiators only from that zone. In addition, if there is only one initiator WWPN in the client, VTL will automatically select it for you and the dialog will not be displayed.

Click *Next* and set Fibre Channel options.

*Enable Volume Set Addressing* may be required for particular Fibre Channel clients, such as HP-UX clients that require VSA to access storage devices.

Note: *IBM i-Series Server* and *Celerra* are not supported options for Sun VTL.

**For iSCSI clients**, specify if the client is a mobile client. A mobile client is simply a username and password that can be used to authenticate to the VTL server from any iSCSI client machine. If this a mobile client, you will have to enter a username and password on the next dialog.

If this is a stationary (not mobile) client, click *Next* and select the initiator that the client uses. If the initiator does not appear, you can manually add it.

Click *Next* and add/select users who can authenticate for this client. When you add users, you will have to enter a name and password for each.

If you select *Allow Unauthenticated Access*, the VTL Server will recognize the client as long as it has an authorized initiator name. With authenticated access, an additional check is added that requires the user to type in a username and password. More than one username/password pair can be assigned to the client, but they will only be useful when coming from the machine with an authorized initiator name.

4. Click *Finish* when you are done.

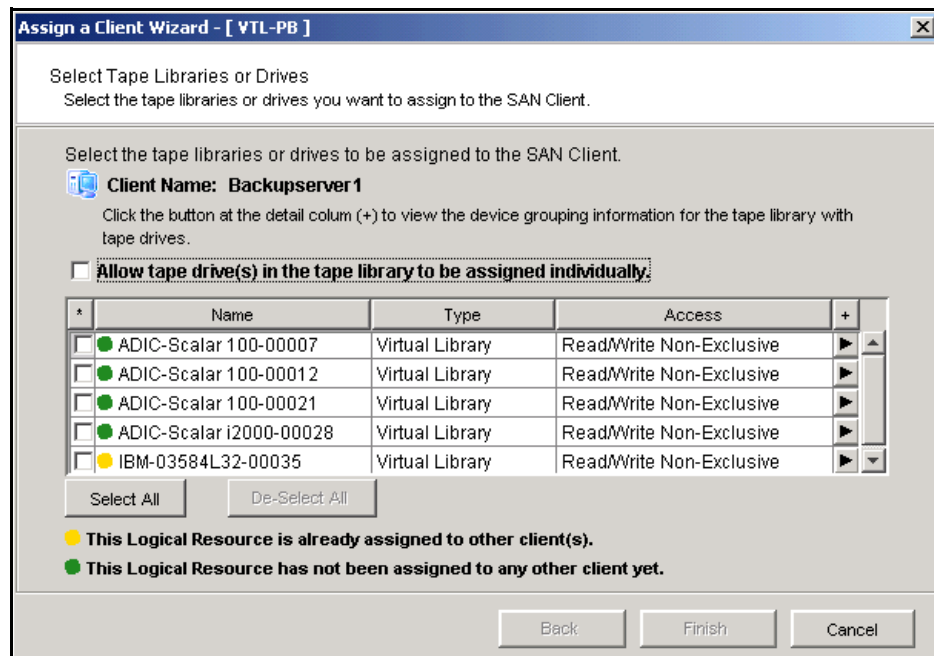
## Assign virtual tape libraries to clients

You can assign virtual tape libraries to clients in the following three ways:

- Use the configuration wizard - If you have already configured your system, you can launch the wizard by right-clicking on the *VirtualTape Library System* object in the console and selecting *Configuration Wizard*.
- Right-click on a SAN Client and select *Assign*.

Note: The *Everyone* generic client is not a supported option for SUN VTL. It may be used in a test environment but for security purposes it should not be used in a production environment.

- Right-click on a virtual tape library and select *Assign*.
1. Assign virtual tape libraries/drives to your backup clients.



You can assign the entire library to a backup client or you can assign individual tape drives.

- 
2. Click *Finish* when you are done.

**(FC version only)** After configuring VTL, you should perform a device scan on your backup server. The steps to do this vary according to the server's operating system.

For Windows, *Control Panel --> Computer Management --> Device Manager -->* right-click on the device in the right pane --> *Scan for hardware changes*.

## Assign physical libraries/drives to VTL

If you will be importing data from physical tapes into your virtual tape library or exporting virtual tapes to physical tapes, you must assign your physical tape libraries/drives to VTL.

1. Assign physical libraries/drives to VTL in one of the following two ways:
  - Use the configuration wizard - You can launch the wizard by right-clicking on the *Virtual Tape Library System* object in the console and selecting *Configuration Wizard*. Press *Skip* to advance to *Step 4* and click *Next* for *Step 5*.
  - Right-click on the *Physical Tape Libraries* object or the *Physical Tape Drives* object and select *Assign*.
2. Select the physical libraries/drives to be assigned to VTL.
3. Click *Finish/Assign* to assign.

This process also inventories the physical tapes in your library/drive so that you can create virtual tapes that match your physical tapes.

---

## Import/Export tapes

One of the advantages of using a virtual tape library is that you can protect data on your existing physical tapes by importing them into your virtual tape system.

If you need to recover files from a physical tape, you can use the import function to directly access the physical tape for immediate recovery.

In addition, the data on virtual tapes can be exported to physical tapes for long-term data archiving.

### *Import a physical tape*

The import function allows you to:

- Copy the contents of a physical tape to a virtual tape
- Directly access a physical tape without copying the entire tape
- Recycle a physical tape

Important Note: Tape caching must be disabled prior to using the import function.

To import a tape:

1. Right-click on your physical tape library/drive and select *Import Tape*.

2. Select which virtual library and slot to import into.

Be sure to pick a drive/library with the same tape size capacity.

3. Select how you want the data copied.

*Copy Mode* - Copies the entire contents of a physical tape onto a virtual tape and leaves the physical tape unchanged.

*Direct Access Mode* - Links a physical tape to its virtual counterpart. This gives the backup application immediate access to the tape data without waiting for a complete copy. This is useful when you need to restore a small amount of data from a physical tape.

*Recycle Mode* - Recycles a physical tape after its retention period has been reached. If you import a tape in recycle mode and the virtual tape is subsequently initialized, the physical tape is now considered recycled and can be used for future export operations.

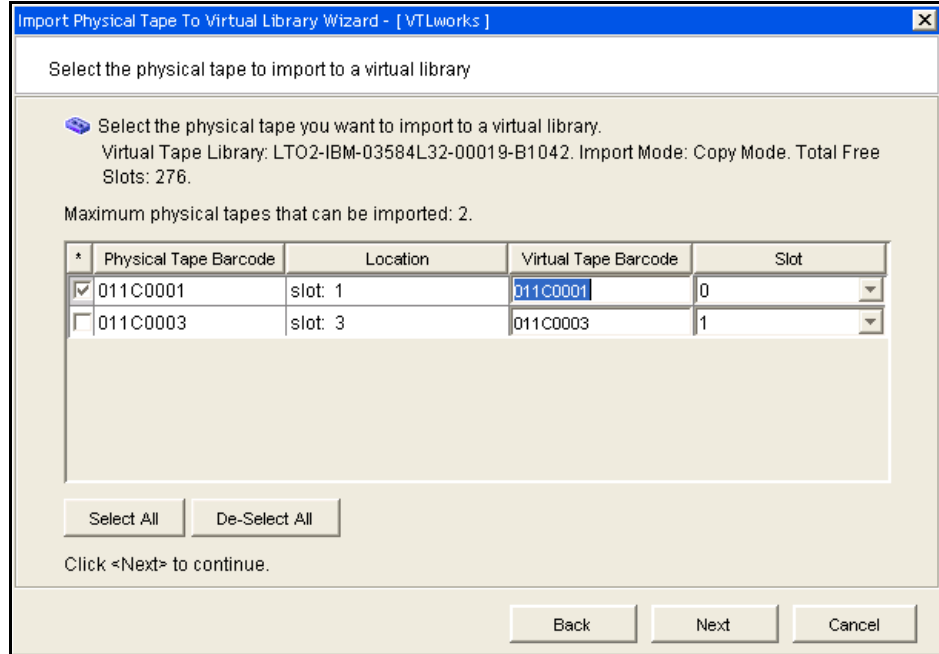
4. Specify whether or not to decrypt the data on the tape.

You can select this option only if at least one key exists. (For more information, refer to '[Encrypt data that is exported to physical tapes](#)'.) If you select this option, you must select the key to use.



Note: Selecting this option if the data was not previously encrypted, or an incorrect key is selected, or an invalid password is provided, will import data that is indecipherable. Clearing this option will not decrypt data on the tape.

5. Select the physical tape you want to import.



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.

6. Verify the information and then click *Finish* to import the tape.

---

## Export data to a physical tape

Moving data from virtual tape to physical tape can be accomplished in several ways:

- From your backup software using the software's own *Tape Copy* function
- Using VTL's export function, either manually or automatically after each backup using the Auto Archive function

Alternatively, the VTL Automated Tape Caching option provides a cache to your physical tape library, providing transparent access to data regardless of its location. The Automated Tape Caching option provides advanced flexibility that allows you to set up policies that automatically trigger data migration to physical tapes.

The VTL export methods are explained below. Refer to ['Automated Tape Caching'](#) for more information about Automated Tape Caching.

### Export notes:

- You cannot use the VTL export functions if you are using the Automated Tape Caching option.
- Because some third-party backup applications alter what they write to the tape depending on the type of cartridge used, VTL only exports tapes to *like* media. You cannot export to a dissimilar physical tape. This guarantees that the backup application will accept the tape as valid; from the backup application's point of view, there is no difference between the virtual and physical tape.

### *Export manually*

To manually export data:

1. Right-click on a virtual tape and select *Move to Vault*.
2. Select the tape(s) you want to move.



- If you have not already done so, inventory the physical tapes in your library by right-clicking on the physical library and selecting *Inventory*.

Barcode	In Slot
012DZ000	0
012DZ001	1
012DZ002	2
012DZ003	3
012DZ004	4
012DZ005	5
012DZ006	6

This is what you will see if the tape library supports barcodes.

Barcode	In Slot
	0
	1
	2
	4
	6

This is what you will see if the tape library does not support barcodes.

- Right-click on the virtual tape under *Virtual Vault* and select *Export Tape*.
- Select the physical tape library to which you want to export.
- Select how you want the data exported.
 

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

*Copy Mode* - Copies the contents of the virtual tape to its physical counterpart and retains the virtual tape after the data is transferred.
- Select or clear the *Eject physical tapes to I/E slots after export* check box.
- Select *Encrypt data when exporting to physical tape with the selected key* if you want to encrypt the data on the tape.
 

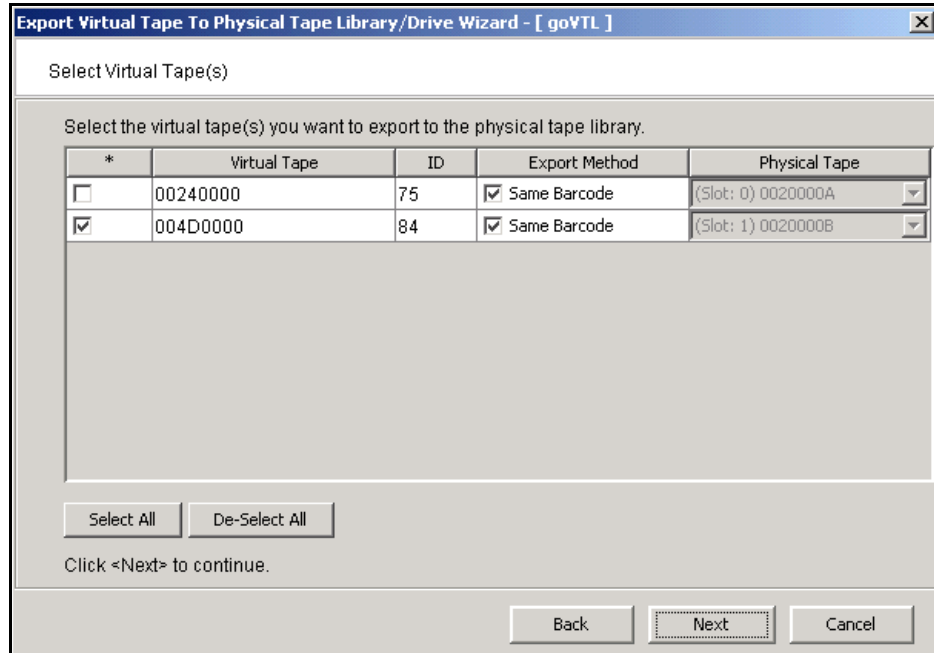
You can select this option only if at least one key has been created. If you select this option, you must select the key to use. All the data on the tape will be indecipherable until is imported back to a virtual tape library and decrypted using the same key.

Note that when you encrypt data, physical tape drive compression is disabled; it will be enabled if you do not encrypt data.
- Indicate if you want to enable tape duplication.
 

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

same number of drives, same tapes with the same barcodes). When data is exported, separate export jobs will be created for each physical library and each job will have a unique job ID.

10. Select the virtual tape you want to export.




If your physical tape drive/library uses barcodes, we highly recommend that you select to use the same barcode as the physical tape.

If your physical tape drive/library does not use barcodes, you can then select which slot to use for the physical tape.

11. Verify the information and then click *Finish* to export the tape.

## Auto Archive function

*Auto Archive* writes data to physical tape whenever a virtual tape is exported from a virtual library (by a backup application or other utility after a backup). In order to use *Auto Archive* the physical tape library must support barcodes because when VTL attempts to export to physical tape it must find a matching barcode in a physical library (you do not need to specify which physical library).

 Note: You can use Auto Archive only if you are not currently using the Automated Tape Caching option or the Auto Replication feature on this virtual tape library.

To set Auto Archive:

1. Right-click on a virtual tape library and select *Properties*.
2. Select the *Auto Archive* checkbox.

- 
3. Determine if you want the virtual tape copied (retained) or moved (removed) after the data is transferred.

If you select *Move*, indicate how long to wait before deleting it.

4. Indicate if you want to export your *physical* tapes to the library's import/export slots after archiving.

5. Indicate if you want to encrypt the data on the tape.

You can encrypt the data only if at least one key already exists. If you choose to encrypt the data, you must specify which key to use. (For more information, refer to ['Encrypt data that is exported to physical tapes'](#).)

---

## Stacking virtual tapes

Tape stacking allows multiple virtual tapes to be exported to a single physical tape in a physical tape library, maximizing physical tape usage and allowing the conversion of virtual media with a smaller capacity to physical media with a higher capacity (i.e. DLT to LTO).

Tape stacking is a tool for archival purposes only. Backup applications will not have direct access to stacked tapes. While VTL's direct access mode links a physical tape to its virtual counterpart, restoring from a stacked tape will require importing data from a stacked tape back to virtual tape. You cannot use VTL's direct access mode for stacked tapes.

### Notes:

- You can only use Tape Stacking if you are not currently using the Automated Tape Caching option on this virtual tape library.
- Tape Stacking does not append data to a physical tape. When a job is submitted, any data on that physical tape will be overwritten and the tape will only hold the data from the last successful job.

To stack virtual tapes:

1. Move the tape(s) you want to stack to the virtual vault.
2. Right-click on the tape in the virtual vault and select *Export with stacking*.
3. Select the physical tape library to which you want to export.
4. Select how you want the data exported.

*Move Mode* - Copies the contents of the virtual tape to its physical counterpart and then removes the virtual tape from the system. Specify a grace period if you want to keep the virtual tape for a time before deleting it.

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

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

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

5. Select the virtual tape(s) you want to export.
6. Select the physical tape to which you want to export.
7. Verify the information and then click *Finish* to export the tape.

You can check the Import/Export queue to watch the progress of the job.

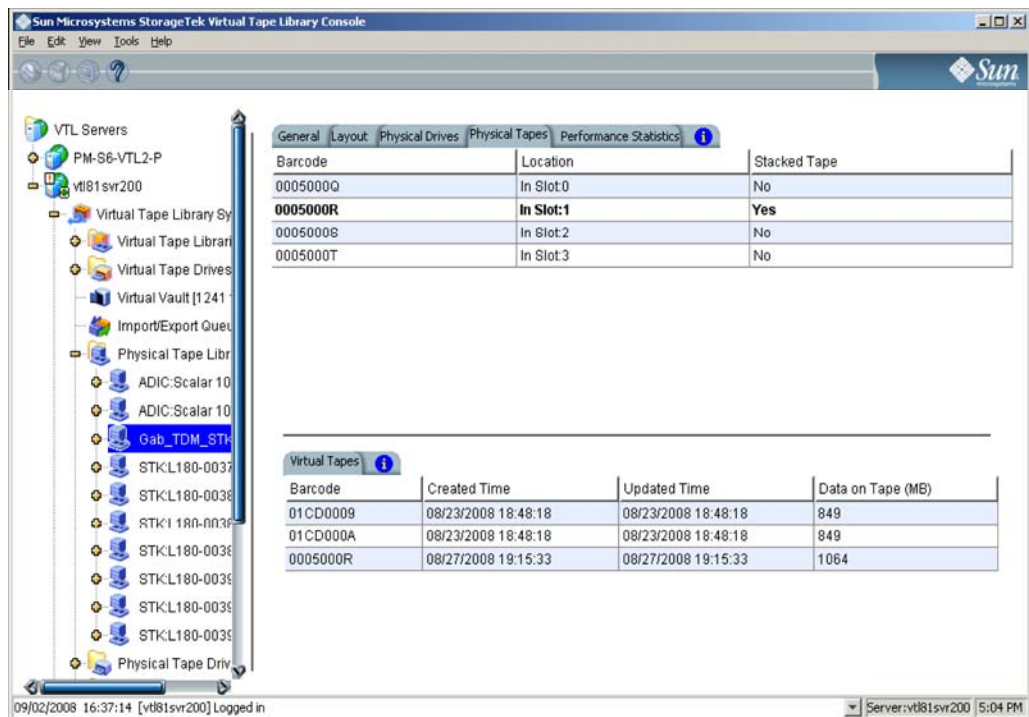
The screenshot displays the Sun Microsystems StorageTek Virtual Tape Library Console. The interface includes a navigation tree on the left with categories like VTL Servers, Virtual Tape Libraries, and Physical Tape Libraries. The main area shows a table of jobs with columns for Job ID, Type, Virtual Barcode, Physical Barcode, Start Time, and Status. A detailed view of an 'Import/Export Job' is shown below the table, listing various attributes such as ID, Type, Mode, and progress percentage.

Job ID	Type	Virtual Barcode	Physical Barcode	Start Time	Status
Jo...	Export to Physical Library with Stac...		0005000R (In dr...	09/03/2008 1...	Running
Jo...	Export to Physical Tape Library (Copy)	03140000	0005000T	08/29/2008 1...	Completed
Jo...	Export to Physical Tape Library (Copy)	0005000S	D005000S	08/29/2008 1...	Completed
Jo...	Export to Physical Tape Library (Copy)	0005000S	1005000S	08/29/2008 1...	Completed
Jo...	Export to Physical Tape Library (Copy)	0005000S	0005000S	08/29/2008 1...	Completed
Jo...	Export to Physical Tape Library (Copy)	0005000Q	D005000Q	08/29/2008 1...	Completed
Jo...	Export to Physical Tape Library (Copy)	0005000Q	1005000Q	08/29/2008 1...	Completed
Jo...	Export to Physical Tape Library (Copy)	0005000Q	0005000Q	08/29/2008 1...	Completed
Jo...	Export to Physical Tape Library (Copy)	0005000S	D005000S	08/29/2008 1...	Completed
Jo...	Export to Physical Tape Library (Copy)	0005000S	1005000S	08/29/2008 1...	Completed

Name	Value
ID	625
Type	Export to Physical Library with Stacking
Mode	Copy
Virtual Tape Barcode (0)	01CD0009
Virtual Tape Barcode (1)	01CD000A
Virtual Tape Barcode (2)	0005000R
Physical Library Name (ID)	Gab_TDM_STK:L180-00400 (400)
Physical Tape Barcode	0005000R
Status	Running
Start Time	09/03/2008 16:27:15
Elapsed Time (seconds)	23 seconds
Data Transferred (MB)	2,679 MB
Percent Complete for tape: 0005000R	97%
Description	Export virtual tapes to a stacked physical tape in physical library

Afterwards, you can look on the *Physical Tapes* tab for the physical tape library to see which tapes are stacked. Highlight a tape to see which virtual tapes are stacked on each physical tape.



You can also see the stacked tapes from the *Physical Tape Database* object. When you highlight a tape, a list of virtual tapes that are stacked on the physical tape appears.


## Encrypt data that is exported to physical tapes

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.

---

## Create a key

To create a key to use for data encryption:

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

Enter the following information and click <Ok> to create a new key.

**Key Name (1-32):** NYoffice

**Secret Phrase (25-32):** Backup tapes sent to Connecticut  
A unique phrase with minimum of 25 characters to be used to generate the key.

**New Password (10-16):** \*\*\*\*\*

**Confirm Password (10-16):** \*\*\*\*\*

**Password Hint (0-32):** Where my mother was born  
A description up to 32 characters to be used as a hint to help the user to remember the password.

OK Cancel

3. In the *Key Name* text box, type a unique name for the key (1–32 characters).
4. In the *Secret Phrase* text box, type the phrase (25–32 characters, including numbers and spaces) that will be used to encrypt the data.



Note: We recommend that you save your secret phrase somewhere because once you have created a key, you cannot change the secret phrase associated with that key.

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

You will need to provide this password in order to change the key name, password, or password hint, or to delete or export the key.

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

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

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

7. Click *OK*.



---

## Change 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*.

## Delete 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.

To delete a key:

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*.

---

## Export 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.

To export a 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.

Alternatively, you can click , select the desired directory, and click *Save*.

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.

## *Import 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.

Alternatively, you can click , select the file in the appropriate location, and click *Open*.

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.

---

## Shred 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.
2. Select the tape(s) you want to shred.

For a single tape, right-click on the tape in the virtual vault and select *Tape Shredding --> Shred Tape*.

For multiple tapes, highlight all of the tapes you want, right-click, and select *Tape Shredding --> Shred Tapes*.

3. If desired, select the option to delete the tape after shredding it.
4. Type *YES* to confirm and click *OK*.

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.

## Mirror the VTL database

Mirroring the VTL database protects your configuration if the disk storing the database is lost.

With mirroring, each time data is written to the VTL database, the same data is simultaneously written to the mirrored copy. This disk maintains an exact copy of the database. In the event that the database is unusable, VTL seamlessly swaps to the mirrored copy.

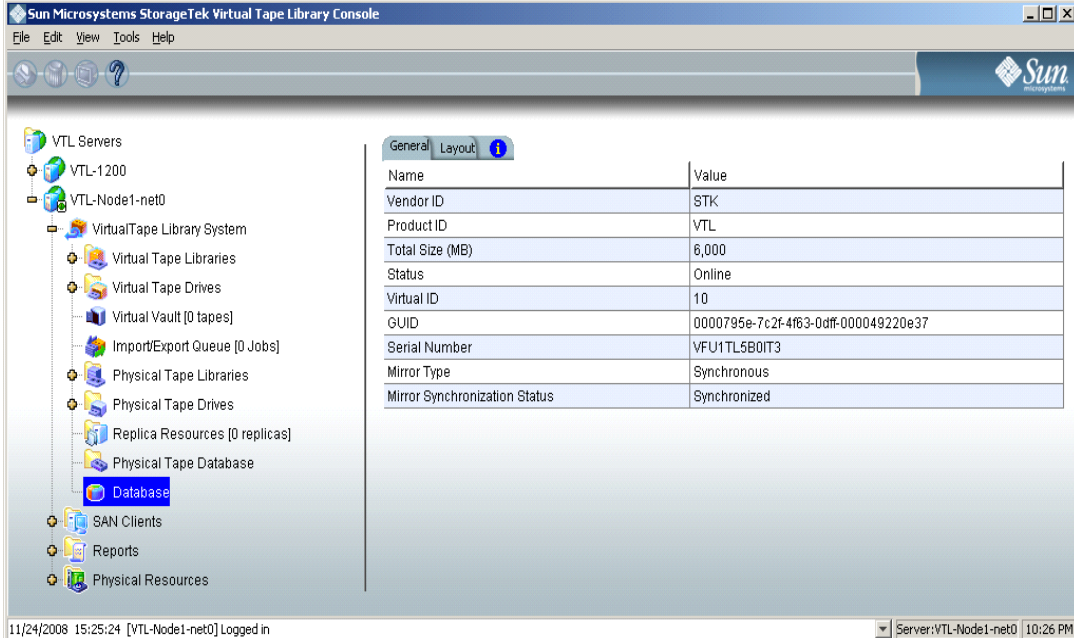
The mirror can be defined with disks that are not necessarily identical to each other in terms of vendor, type, or even interface (SCSI, FC, iSCSI).

To set mirroring:

1. Right-click on the *Database* object (under the *Virtual Tape Library System* object) and select *Mirror --> Add*.
2. Select the physical device to use for the mirror.
3. Confirm that all information is correct and then click *Finish* to create the mirroring configuration.

Check mirroring status

You can see the current status of your mirroring configuration by checking the *General* tab of the database.



The screenshot shows the Sun Microsystems StorageTek Virtual Tape Library Console interface. The left pane displays a tree view of the VTL configuration, with the 'Database' object selected under the 'Virtual Tape Library System' node. The right pane shows the 'General' tab for the selected database, displaying a table of configuration parameters and their values.

Name	Value
Vendor ID	STK
Product ID	VTL
Total Size (MB)	6,000
Status	Online
Virtual ID	10
GUID	0000795e-7c2f-4f63-0dff-000049220e37
Serial Number	VFU1TL5B0IT3
Mirror Type	Synchronous
Mirror Synchronization Status	Synchronized

- *Synchronized* - Both disks are synchronized. This is the normal state.

---

	<ul style="list-style-type: none"> <li>• <i>Not synchronized</i> - A failure in one of the disks has occurred or synchronization has not yet started. If there is a failure in the primary database VTL swaps the to the mirrored copy.</li> <li>• If the synchronization is occurring, you will see a progress bar along with the percentage that is completed.</li> </ul>
Replace a failed disk	<p>If one of the mirrored disks has failed and needs to be replaced:</p> <ol style="list-style-type: none"> <li>1. Right-click on the database and select <i>Mirror --&gt; Remove</i> to remove the mirroring configuration.</li> <li>2. Physically replace the failed disk. The failed disk is always the mirrored copy because if the primary database disk fails, VTL swaps the primary with the mirrored copy.</li> <li>3. Right-click on the database and select <i>Mirror --&gt; Add</i> to create a new mirroring configuration.</li> </ol>
Fix a minor disk failure	<p>If one of the mirrored disks has a minor failure, such as a power loss:</p> <ol style="list-style-type: none"> <li>1. Fix the problem (turn the power back on, plug the drive in, etc.).</li> <li>2. Right-click on the database and select <i>Mirror --&gt; Synchronize</i>. This re-synchronizes the disks and re-starts the mirroring.</li> </ol>
Replace a disk that is part of an active mirror configuration	<p>If you need to replace a disk that is part of an active mirror configuration:</p> <ol style="list-style-type: none"> <li>1. If you need to replace the primary database's disk, right-click on the database and select <i>Mirror --&gt; Swap</i> to reverse the roles of the disks and make it a mirrored copy.</li> <li>2. Select <i>Mirror --&gt; Remove</i> to cancel mirroring.</li> <li>3. Replace the disk.</li> <li>4. Right-click on the database and select <i>Mirror --&gt; Add</i> to create a new mirroring configuration.</li> </ol>
Swap the primary disk with the mirrored copy	<p>Right-click on the database and select <i>Mirror --&gt; Swap</i> to reverse the roles of the primary database disk and the mirrored copy. You will need to do this if you are going to perform maintenance on the primary database disk or if you need to remove the primary database disk.</p>
Remove a mirror configuration	<p>Right-click on the database and select <i>Mirror --&gt; Remove</i> to delete the mirrored copy and cancel mirroring. You will not be able to access the mirrored copy afterwards.</p>
Mirroring and Failover	<p>If mirroring is in progress during failover/recovery, after the failover/recovery the mirroring will restart from where it left off.</p>

---

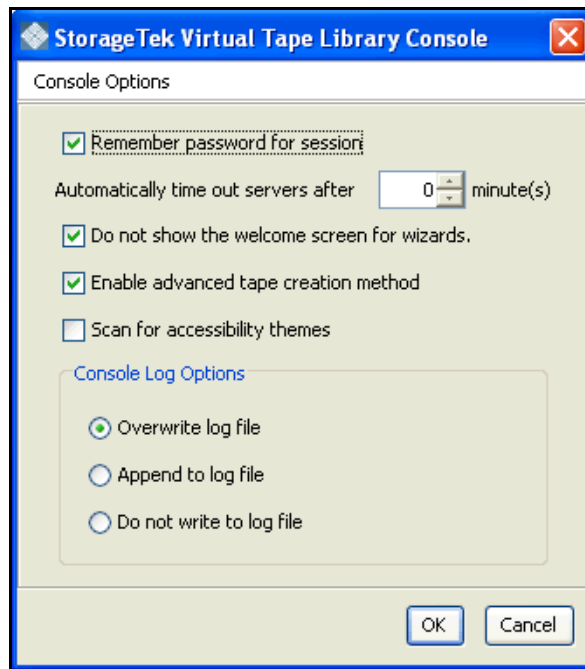
If the mirror is synchronized but there is a Fibre disconnection between the server and storage, the mirror may become unsynchronized. It will resynchronize automatically after failover/recovery.

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

## Set Console options

To set options for the Console:

1. Select *Tools* --> *Console Options*.



2. Make any necessary changes.

*Remember password for session* - If the Console is already connected to a server, when you attempt to open a second, third, or subsequent server, the Console will use the credentials that were used for the last successful connection. If this option is unchecked, you will be prompted to enter a password for every server you try to open.

*Automatically time out servers after nn minute(s)* - The Console will collapse a server that has been idle for the number of minutes you specify. If you need to access the server again, you will have to reconnect to it. The default is 10 minutes. Enter 00 minutes to disable the timeout.

*Do not show the welcome screen for wizards* - Each wizard starts with a welcome screen that describes the function of the wizard. Determine whether or not you want the welcome screen to be displayed.

*Enable Advanced Tape Creation Method* - With *Advance Tape Creation* enabled, you are offered advanced options when creating tapes, such as capacity-on-



---

demand settings for virtual libraries, tape capacity of tapes, and device, name, and barcode selection for each tape that is created.

*Scan for Accessibility Themes* - Select if your computer uses *Windows Accessibility Options*.

*Console Log Options* - The Console log (vtlconsole.log) is kept on the local machine and stores information about the local version of the Console. The Console log is displayed at the very bottom of the Console screen. The options affect how information for each Console session will be maintained:

*Overwrite log file* - Overwrite the information from the last Console session when you start a new session.

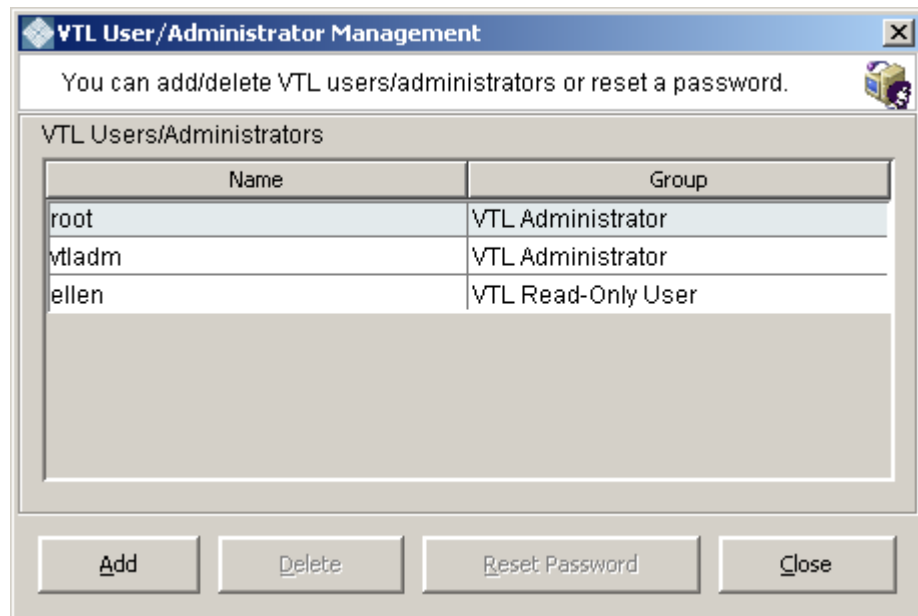
*Append to log file* - Keep all session information.

*Do not write to log file* - Do not maintain a Console log.

## Manage Administrators

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

1. Right-click on the server and select *Administrators*.



- The root user has full Console access. In addition to adding or deleting administrators and changing administrator passwords, the root user has authority to perform system maintenance functions (network configuration, setting the hostname and date and time, restarting VTL and the network, and rebooting or halting VTL). Also, only root can access VTL command line interface commands that begin with "vtl".

- 
- *VTL Administrators* other than root may access all administrator functions except for those reserved for root (listed above).
  - *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. Select the appropriate option.

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 root user or change the root user's password from this screen. Use the *Change Password* option instead.

---

## Virtual tape drive compression

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

VTL supports two types of compression:

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

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



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

Enable/disable  
compression

To enable or disable compression:

1. Enable tape drive compression in your backup application.
2. If you are using hardware compression, install a certified compression card in your VTL server.
  - A VTL 1200 or 1202 can have one compression card per server node
  - A VTL 2600 or 3600 can have two compression cards per server node

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

3. In the VTL Console, right-click on *VirtualTape Library System* and select *Properties*.
4. Select the *Enable VirtualTape Library compression mode* checkbox and specify whether you are using *Software* or *Hardware* compression.

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

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


---

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

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

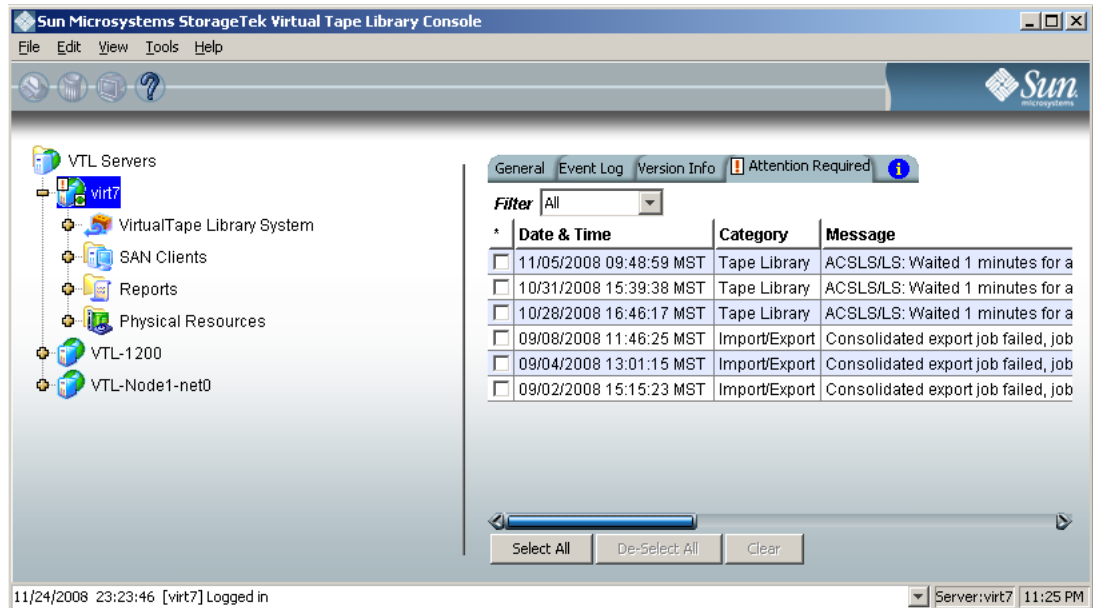
Windows — On Windows servers select the option in your backup software to enable or disable hardware tape drive compression. If global VTL compression is disabled, it is possible to enable individual drive compression, but it will have no effect.

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

 IBM-ULT3580-TD1-00841

## View 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><b>I:</b> This is an informational message. No action is required.</p> <p><b>W:</b> 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><b>E:</b> 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><b>C:</b> 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.

---

Sort the Event Log	When you initially view the Event Log, all information is displayed in chronological order (most recent at the top). If you want to reverse the order (oldest at top) or change the way the information is displayed, you can click on a column heading to re-sort the information. For example, if you click on the <i>ID</i> heading, you can sort the events numerically. This can help you identify how often a particular event occurs.
Filter the Event Log	By default, all informational system messages, warnings, and errors are displayed. To filter the information that is displayed: <ol style="list-style-type: none"><li>1. Right-click on a server and select <i>Event Log --&gt; Filter</i>.</li><li>2. Select which message types you want to include.</li><li>3. Search for records that contain/do not contain specific text.</li><li>4. Specify the maximum number of lines to display.</li><li>5. Select a time or date range for messages.</li></ol>
Print/export the Event Log	You can print the Event Log to a printer or save it as a text file. These options are available (once you have displayed the Event Log) when you right-click on the server and select the <i>Event Log</i> options.


---

## Refer to the Attention Required tab

The *Attention Required* tab displays information that may require your attention, such as:

- Physical library failures
- Hardware appliance errors
- Replication errors

It also notifies you when an import/export job has completed.

The *Attention Required* tab only appears for a VTL server when an error/notification occurs; it will not appear at other times. When the tab does appear, you will see an exclamation icon on the server.  VTL

Clear issues  
from the list

After you have resolved an issue, you can click the check box next to it and click the *Clear* button. You can clear individual issues or you can click the box next to one of the categories to delete all issues in that section.

---

## Set Server properties

To set properties for a specific server:

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 '[Configure VTL to send SNMP traps](#)' for more information.
4. 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.

## Apply software patch updates

You can apply patches to your VTL server through the Console.

Add patch      To apply a patch:

1. Download the patch onto the computer where the Console is installed.
2. Highlight an VTL server in the tree.
3. Select *Tools* menu --> *Add Patch*.
4. Confirm that you want to continue.
5. Locate the patch file and click *Open*.

The patch will be copied to the server and installed.

Rollback patch      To remove (uninstall) a patch and restore the original files:

1. Highlight an VTL server in the tree.
2. Select *Tools* menu --> *Rollback Patch*.
3. Confirm that you want to continue.
4. Select the patch and click *OK*.



---

## Configure VTL to send 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.
- Informational – 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.

# Failover

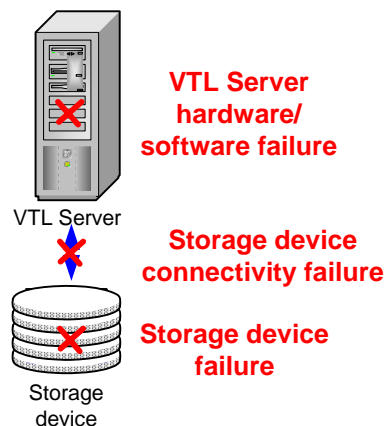
## Overview

To support mission-critical computing, VTL Failover provides high availability for the entire storage network, protecting you from a wide variety of problems, including:

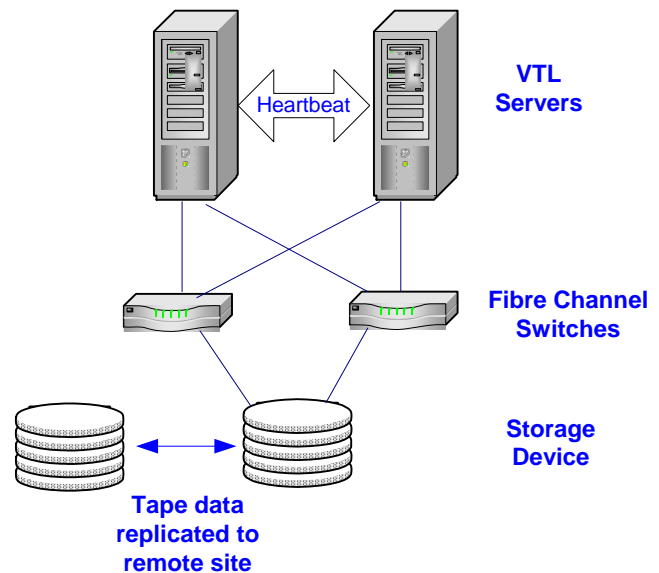
- [Storage device path failure](#)
- [VTL Server failure \(including storage device failure\)](#)

The following illustrates a basic VTL configuration with potential points of failure and a high availability configuration, where VTL's high availability options work with redundant hardware to eliminate the points of failure:

### Basic VTL Configuration With Points of Failure



### High-Availability VTL Configuration (No Points of Failure)




## Storage device path failure

A storage device path failure can occur due to a cable or switch/router failure.

You can eliminate this potential point of failure by providing a multiple path configuration, using multiple Fibre Channel switches, and/or multiple adapters, and/or storage devices with multiple controllers. In a multiple path configuration, VTL automatically detects all paths to the storage devices. If one path fails, VTL automatically switches to another.

---

 Note: Fibre Channel switches can demonstrate different behavior in a multiple path configuration. Before using this configuration with VTL, you must verify that the configuration can work on your server *without* the VTL software. To verify:

1. Use the hardware vendor's utility to see the devices after the driver is loaded.  
You can also use Solaris' `cfgadm -alv` command.
2. Use the hardware vendor's utility to access the devices.
3. Unplug the cable from one device and use the utilities listed above to verify that everything is working.
4. Repeat the test by reversing which device is unplugged and verify that everything is still working.

### *VTL Server failure (including storage device failure)*

VTL's Failover option provides high availability for VTL operations by eliminating the down time that can occur should a VTL server (software or hardware) fail.

In the VTL failover design, a VTL server is configured to monitor another VTL server. In the event that the server being monitored fails to fulfill its responsibilities to the SAN Clients it is serving, the monitoring server will seamlessly take over its identity.

VTL uses a unique monitoring system to ensure the health of the VTL servers. This system includes a self-monitor and an intelligent heartbeat monitor.

The *self-monitor* is part of all VTL servers, not just the servers configured for failover and provides continuous health status of the server. It is part of the process that provides operational status to any interested and authorized parties, including the Console and supported network management applications through SNMP. The self-monitor checks the VTL processes and connectivity to the server's storage devices.

In a failover configuration, VTL's intelligent *heartbeat monitor* continuously monitors the primary server through the same network path that the server uses to serve its clients.

When the heartbeat is retrieved, the results are evaluated. There are several possibilities:

- All is well and no failover is necessary.
- The self-monitor detects a *critical error in the VTL server processes* that is determined to be fatal but does not affect the network interface. In this case, the secondary will inform the primary to release its VTL identity and will take over serving the failed server's clients.
- The self-monitor detects a *storage device connectivity failure* but cannot determine if the failure is local or applies to the secondary also. In that case the device error condition will be reported through the heartbeat. The secondary will check to see if it can successfully access the device. If it

---

can, it attempts to access all devices. If it can successfully access all devices, the secondary initiates a failover. If it cannot successfully access all devices, no failover occurs.

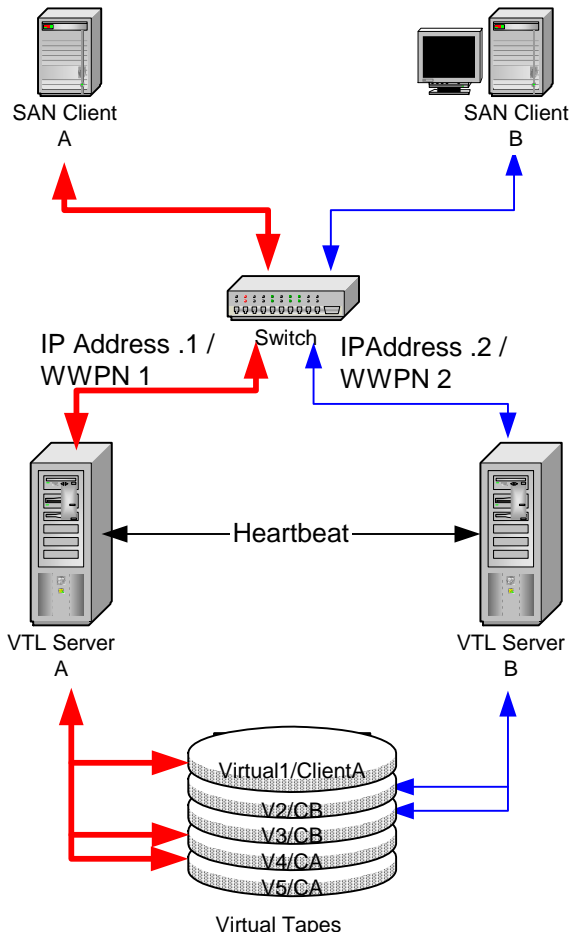
Because the heartbeat shares the same network path as the server's clients, it is determined that clients cannot access their resources whenever the heartbeat cannot be retrieved. This is considered a *Catastrophic failure* because the server or the network connectivity is incapacitated. In this case the secondary will immediately initiate a failover.

---

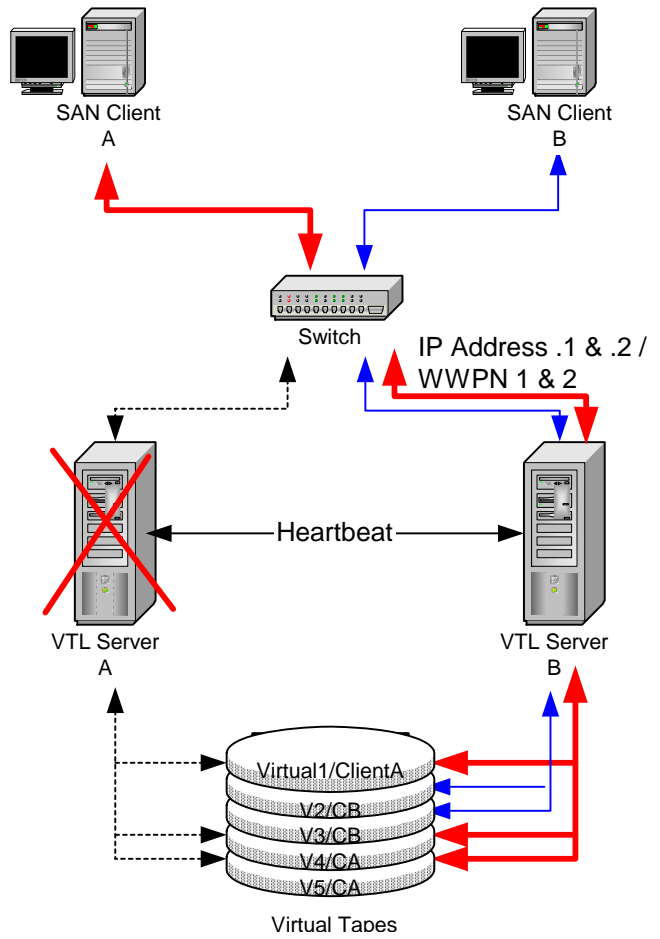
## Failover terminology

Primary/ Secondary VTL servers	<p>VTL's Primary and Secondary servers are separate, independent VTL servers that each have their own assigned clients. In <i>Active-Passive Failover</i>, the primary VTL server is monitored by the Secondary VTL server. In the event the primary server fails, the secondary takes over.</p> <p>In <i>Active-Active Failover (or Mutual Failover)</i>, both servers are configured to monitor each other. The terms <i>Primary</i> and <i>Secondary</i> are purely from the client's perspective. Each server is <i>primary</i> to its own clients and <i>secondary</i> to the other's clients. Each server normally services its own clients. In the event one server fails, the other will take over and serve the failed server's clients.</p>
Failover/ Takeover	<p>Failover/takeover is the process that occurs when the secondary server takes over the identity of the primary. Failover will occur under the following conditions:</p> <ul style="list-style-type: none"><li>• One or more of the VTL processes goes down.</li><li>• There is a network connectivity problem, such as a defective HBA or a loose network cable.</li><li>• There is a storage path failure or power failure.</li></ul> <p>There is a three minute delay after failover occurs. During this time, no I/O is permitted.</p>
Recovery	<p>The process when the secondary server releases the identity of the primary to allow the primary to restore its operation.</p> <p>There is a three minute delay during recovery. During this time, no I/O is permitted.</p> <p>You must reboot the primary server before recovering.</p>
Auto Recovery	<p>Auto Recovery occurs after a failover, when control is returned to the primary server once the secondary server determines that the primary server has recovered. It determines this by continually monitoring the primary server, even after the failover.</p> <p>If failover is caused by loss of network connectivity, auto recovery will occur when all heart monitoring connections are restored. If you are using multiple IP addresses for health monitoring, all network connections must be restored to initiate auto recovery.</p> <p>Once control has returned to the primary server, the secondary server returns to its normal monitoring mode.</p> <p>You must reboot the primary server before recovering.</p>

### Mutual Failover Configuration



### Failover to VTL Server B



This diagram illustrates a VTL failover configuration. When server A fails, server B takes over and serves the clients of server A in addition to its own clients.

## Failover requirements

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

- You must have two VTL servers.
- The failover pair should be installed with identical operating system versions and must have identical storage configurations.
- The servers need access to all common virtual devices but devices cannot be owned by both servers. This means that storage devices must be attached in a multi-host SCSI configuration or attached on a Fibre loop or switched fabric. In this configuration, both servers can access the same devices at the same time (both read and write). You will see something similar to the following when you look at the physical storage in the Console.

The same Fibre Channel device is shown from both servers (primary and secondary). The V icon indicates the disk is virtualized and owned by that server. The F icon indicates shared storage that is being used by another server. The *Owner* field lists the other server.

Product ID	BladeCtrl B210
Firmware Revision	0542
SCSI Address	1:0:1:4
Total Sectors	1,467,514,218
Sector Size (Bytes)	512
Total Size (MB)	716,560
Owner	VTLServer234

Product ID	BladeCtrl B210
Firmware Revision	0542
SCSI Address	1:0:1:3
Total Sectors	1,467,514,218
Sector Size (Bytes)	512
Total Size (MB)	716,560
Owner	VTLServer232

- Both servers must have Fibre Channel target mode enabled.
- Both servers must have exactly the same VTL options licensed.
- Physical drives cannot be shared among VTL servers. Physical drives should be visible to the other server but not assigned to VTL.
- Both servers must be able to access the VTL database resource.
- (SCSI only) Termination should be enabled on each adapter, but not on the device, in a shared bus arrangement.
- Both servers must reside on the same network segment, because in the event of a failover, the secondary server must be reachable by the clients of the primary server. This network segment must have at least one other device that generates a network ping (such as a router, switch, or server). This allows the secondary server to detect the network in the event of a failure.
- You need to reserve an IP address for each network adapter in your failover servers. The IP address must be on the same subnet as the server. These IP addresses are used by the servers to monitor each other's health. The health monitoring IP address remains with the server in the event of failure so that the server's health can be continually monitored. After failover, the

---

health monitoring IP address still exists until the network services are restarted. Note: VTL clients and the Console should not use the health monitoring IP address to connect to a server.

- A standby initiator port needs to be available. This port needs to be connected to the same FC switch as the target port and should not be zoned to anything else.
- The primary and secondary servers should use the exact same Target Port ID scheme on the matching WWPNs. We recommend using the same initiator adapter numbers on both sides to connect to the same storage, so the ACSL of all the devices will look identical on both sides.
- You must use static IP addresses for your failover configuration. We also recommend that the IP addresses of your servers be defined in a DNS server so they can be resolved.
- The first time you set up a failover configuration, the secondary server must not have any logical resources (including virtual tapes, drives, or libraries) or clients.



---

## Backup server failover configuration

While failover and failback are transparent for the VTL server, some configuration may be necessary for your backup server in order for physical devices to be accessed after failover. The configuration varies by backup application and operating system. To ensure that physical devices can be accessed after failover, we recommend you follow the instructions below.

### *Windows 2000*

Veritas NetBackup	In order for NetBackup to access VTL devices after failover, set the backup server's Fibre Channel HBA timeout value to a higher value (such as 250 seconds).
----------------------	---

### *HP-UX*

All backup software	HP-UX uses the FC port ID as its target ID. VTL failover will change the FC switch port ID.
------------------------	---

Cisco switches automatically support switch port swapping.

If you are using a Brocade switch model 3900 and up (3900, 12000, 24000, 4100, etc.) with a Tachyon adapter, you have to manually set up a port swapping script. Refer to '[Port swapping for Brocade switches](#)' for more information.

### *AIX*


All backup software	AIX uses the FC port ID to generate its local ID. VTL failover will change the FC switch port ID.
------------------------	---

If you are using AIX 4.3, 5.1, or 5.2 with a Brocade switch model 3900 and up with a Tachyon adapter, you have to manually set up a port swapping script. Cisco switches automatically support switch port swapping. Refer to '[Port swapping for Brocade switches](#)' for more information.

If you are using AIX 5.3 with a Brocade switch model 3900 and up, you must enable the dynamic tracking option.

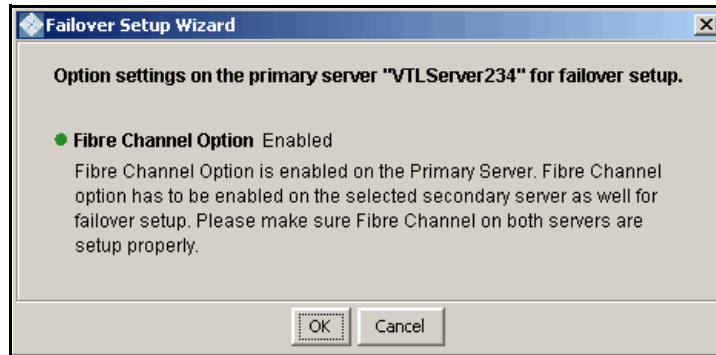
Note that TSM 5.4 supports VTL failover without a port swapping script.

## Failover setup

 Notes:

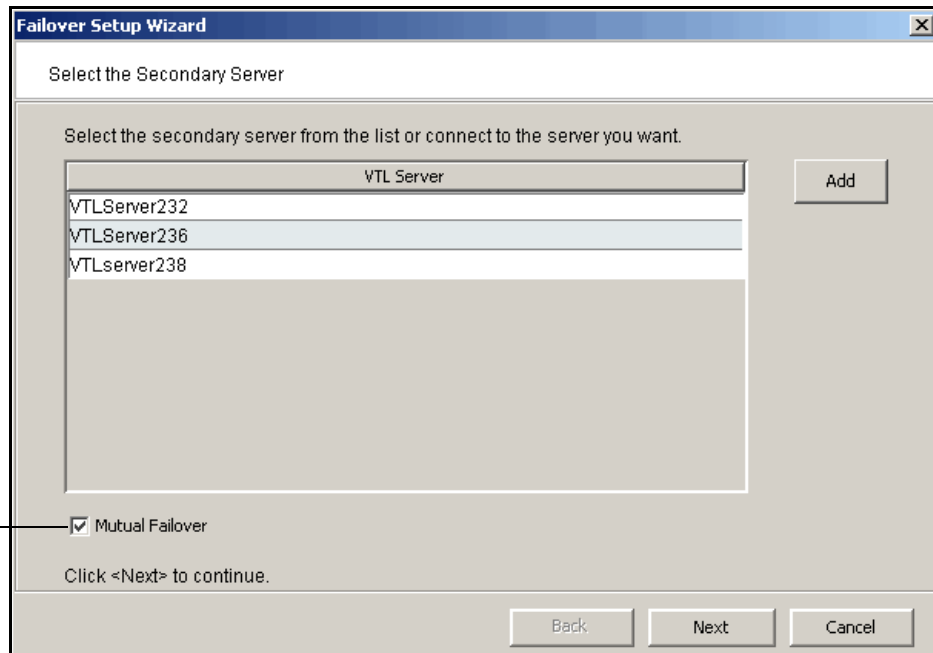
- You will need to know the IP addresses of the failover servers. You will also need the health monitoring IP addresses. It is a good idea to gather this information and find available IP addresses before you begin the setup.
  - If you have not already done so, enable Fibre Channel on both the primary and secondary servers.
  - If you have not already done so, on both the primary and secondary servers, enable target mode for any initiator that is zoned with your backup server. Refer to '[Switch to target mode](#)' for more information.
1. Right-click on one of the servers that will be part of the failover configuration and select *Failover --> Failover Setup Wizard*.

You will see a screen similar to the following that shows you a status of options on your server.



2. Select the secondary server.

Select if you want both servers to monitor each other.



If it hasn't already been named accordingly, the secondary server will be renamed.

3. Check the *Include this Network Adapter for failover* box if you want this network adapter monitored for failover.

Failover Setup Wizard

Enter the IP address of the Server

Enter the IP addresses that the clients will use to access the servers.  
Adapter: 1, Subnet Mask: 255.255.255.0, Subnet: 10.6.2.0

IP address for the server: VTLServer234 10 . 6 . 2 . 234

IP address for the server: VTLServer236 10 . 6 . 2 . 236

The above addresses will be used by the VTL SAN Clients and the VTL Console to access the VTL Servers. If the Console is logged into VTL using a DNS name, the default addresses above were resolved using DNS. When a failover occurs, both addresses will be assumed by the surviving VTL Server.

Include this Network Adapter for failover.

Click <Next> to continue.

Back Next Cancel

The dialog also shows the corresponding IP address on the secondary server, the IP address to which the system will fail over.

If you uncheck the *Include this Network Adapter for failover* box, the wizard will display the next card it finds. You must choose at least one.



Notes:

- If you change the Server IP addresses while the Console is connected using those IP addresses, the Failover wizard will not be able to successfully create the configuration.
- Because failover can occur at any time, you should use only those IP addresses that are configured as part of the failover configuration to connect to the server.

4. Enter the health monitoring IP address you reserved for the selected network adapter.

Failover Setup Wizard

Enter Monitor IP Addresses for the Servers

Enter the IP addresses that will be used to service the servers.  
Adapter: 1, Subnet Mask: 255.255.255.0, Subnet: 10.6.2.0

Monitor IP address for the server: VTLServer234 10 . 6 . 2 . 201

Monitor IP address for the server: VTLServer236 10 . 6 . 2 . 205

These IP addresses are used exclusively by the VTL Servers to monitor each other's health. The address continues to be owned by the respective VTL Server even when a failover occurs. Each VTL Server will maintain the respective monitor IP address in addition to the existing IP address.

**Warning! VTL SAN Clients and VTL Console must not use these addresses to connect to the VTL Server.**

Click <Next> to continue.

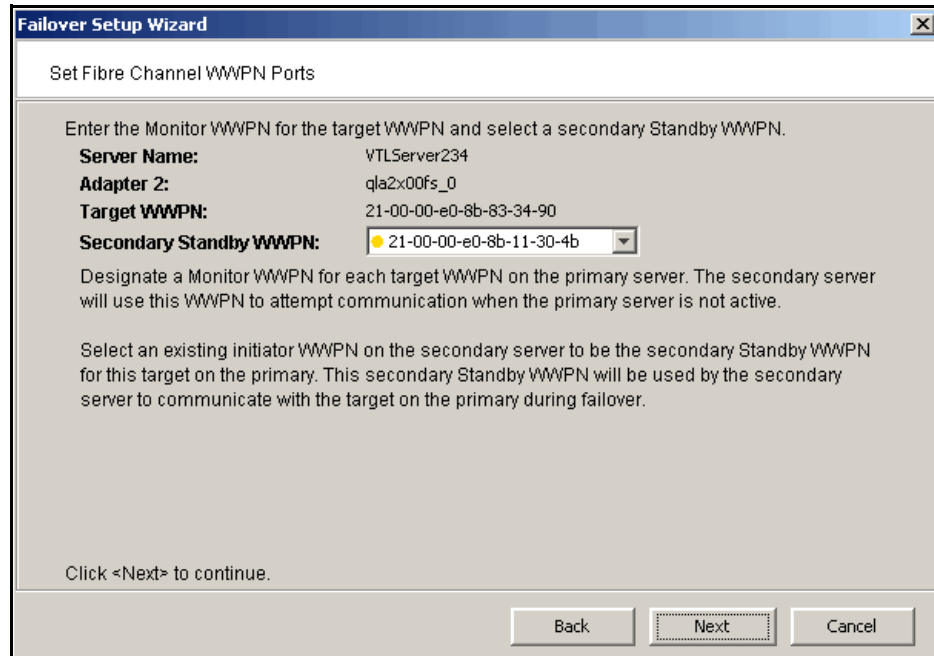
Back Next Cancel

This IP address will be used to continuously monitor the other server. The health monitoring IP address remains with the server in the event of failure so that the server's health can be continually monitored. After failover, the health monitoring IP address still exists until the network services are restarted.

You must use static IP addresses.

5. If you want to use additional network adapter cards, repeat steps 4 and 5.

6. Select the initiator on the secondary server that will function as a standby in case the target port on your primary server fails.

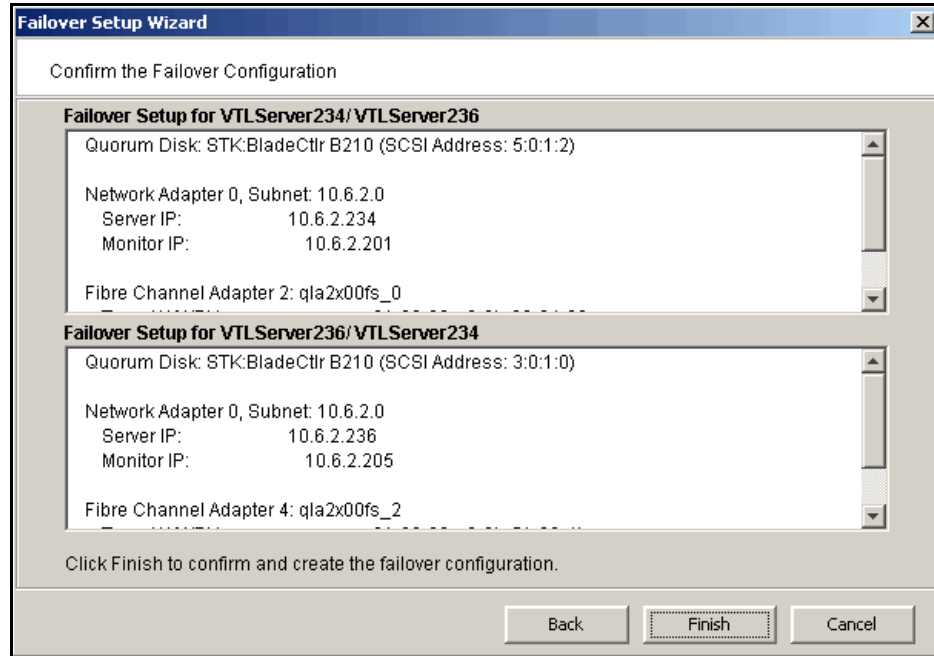


The proper adapter is usually selected for you, but you should confirm that the adapter shown is not the initiator on your secondary server that is connected to the storage array, and also that it is not the target adapter on your secondary server.

There should not be any devices attached to this initiator.

7. Set up the standby adapter for the secondary server.

8. Confirm all of the information and then click *Finish* to create the failover configuration.



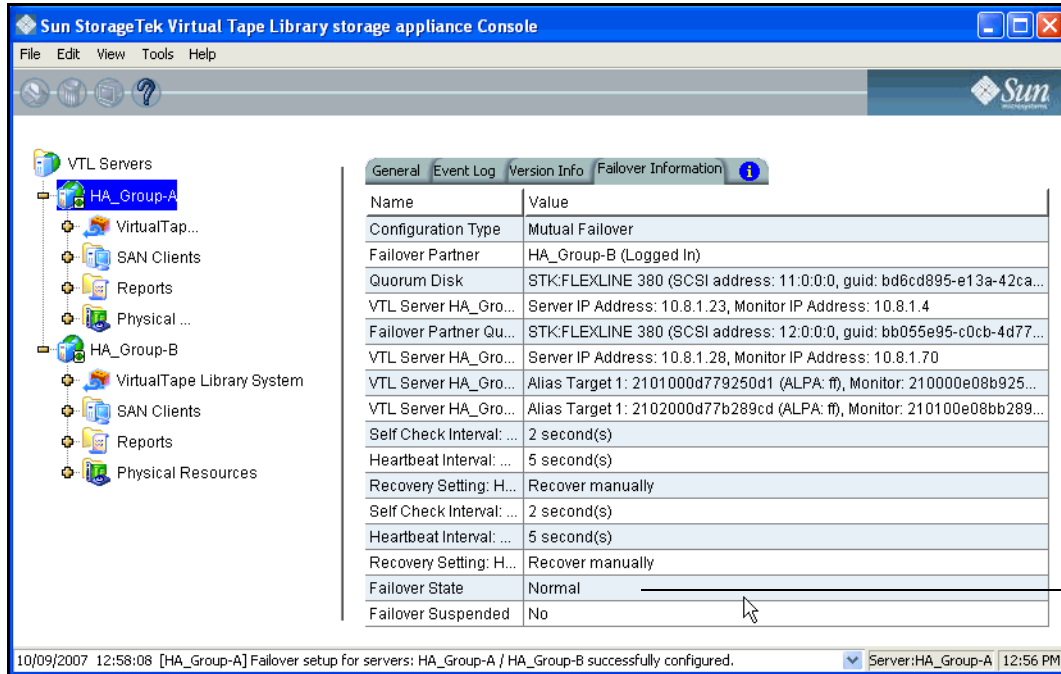
Once your configuration is complete, each time you connect to either server in the Console, you will automatically be connected to the other as well.



Note: If the setup fails during the setup configuration stage (for example, the configuration is written to one server but then the second server is unplugged while the configuration is being written to it), use the *Remove Failover Configuration* option to delete the partially saved configuration. You can then create a new failover configuration.

## Check Failover status

You can see the current status of your failover configuration, including all settings, by checking the *Failover Information* tab for the server.



Failover settings, including which IP addresses are being monitored for failover.

Current status of failover configuration.

In addition, VTL uses different colors to indicate the failover status:

- Black server name - Normal operations.
- Red server name - The server is currently in failover mode and has been taken over by the secondary server.
- Green server name - The server is currently in failover mode and has taken over the primary server's resources.
- Yellow dot next to server name - The user has suspended failover on this server. The current server will NOT take over the primary server's resources even it detects abnormal condition from the primary server.

Failover events are also written to the primary server's Event Log, so you can check there for status and operational information, as well as any errors. You should be aware that when a failover occurs, the console will show the failover partner's Event Log for the server that failed.

## When failover occurs

When failover occurs, the secondary server takes over the identity of the primary. The primary server must be rebooted before recovering back from the secondary server to the primary server.

---

## Make changes to the servers in your failover configuration

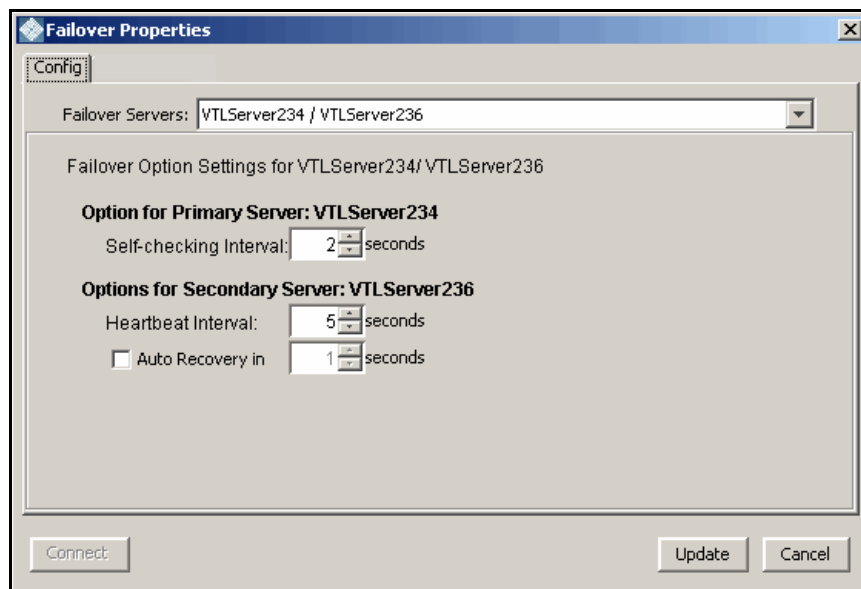
The first time you set up your failover configuration, the secondary server cannot have any logical resources (tape or Replica Resources) or clients assigned to it. Afterwards, you may want to add resources, create virtual devices, and assign clients to the server.

In order to make any of these changes, you must be running the console with write access to both servers. VTL will automatically "log on" to the failover pair when you attempt any configuration on the failover set. While it is not required that both servers have the same username and password, the system will try to connect to both servers using the same username and password. If the servers have different usernames/passwords, it will prompt you to enter them before you can continue.

If you make a change to a physical device (such as if you add a network card that will be used for failover), you will need to re-run the Failover wizard.

## Change your failover intervals

Right-click on the server and select *Failover --> View/Update Failover Options* to change the intervals (heartbeat, self-checking, and recovery) for this configuration.



Note: We recommend keeping the *Self-checking Interval* and *Heartbeat Interval* set to the default values. Changing the values can result in a significantly longer failover and recovery process.

The *Self-checking Interval* determines how often the primary server will check itself.

The *Heartbeat Interval* determines how often the secondary server will check the heartbeat of the primary server.

If enabled, *Auto Recovery* determines how long to wait before returning control to the primary server once the primary server has recovered.





Note: If you disable Auto Recovery, you will have to manually initiate a recovery for all failures except physical network cable failures. Regardless of what you select here, these types of failures will initiate an automatically recovery once the problem has been fixed.

## Force a takeover by a secondary server

Select *Failover --> Start Takeover* to initiate a failover to the secondary server. You may want to do this if you are taking your primary server offline, such as when you will be performing maintenance on it.

## Manually initiate a recovery to your primary server

Select *Failover --> Stop Takeover* if your failover configuration was not set up to use VTL's Auto Recovery feature and you want to force control to return to your primary server or if you manually forced a takeover and now want to recover to your primary server. Be sure to reboot the primary server before recovering.

## Suspend/resume failover

Select *Failover --> Suspend Failover* to stop monitoring your servers. Select *Failover --> Resume Failover* to restart the monitoring.

## Failover server disaster recovery

In the event of a failover, the primary server will go down for some reason and the secondary server will assume the role of the primary server. The following steps explain how to rebuild/repair a primary server in the event of such a disaster:

1. Using the VTL Console, attempt to connect to the primary server to save its configuration.  

This information will actually be retrieved from the surviving server which keeps an updated copy of the primary server's configuration.
2. Disable Auto Recovery from the surviving server so the primary server can be rebuilt.
3. Perform the necessary repair/maintenance on the downed server, the former primary server, (for example, replace the machine, replace the hard drive, install the operating system, etc.).
4. Configure the newly-built/repared primary server to use the original primary server's heartbeat IP addresses.
5. Install and start the VTL server on the newly-built/repared primary server.
6. From the VTL Console, connect to the newly-built/repared primary server via the heartbeat IP address configured in step 4.

---

Select the *Edit* menu --> *Add* and type in the original primary server's heartbeat address in the *VTL User Logon* dialog.

7. Once connected to the newly-built/repaired primary server (using its heartbeat IP address), restore the original primary server's configuration saved in step 1.
8. Restart the VTL server on the newly-built/repaired primary server to use the restored configuration.
9. From the VTL Console, reconnect to the newly-built/repaired primary server by using the original primary server's virtual IP address.

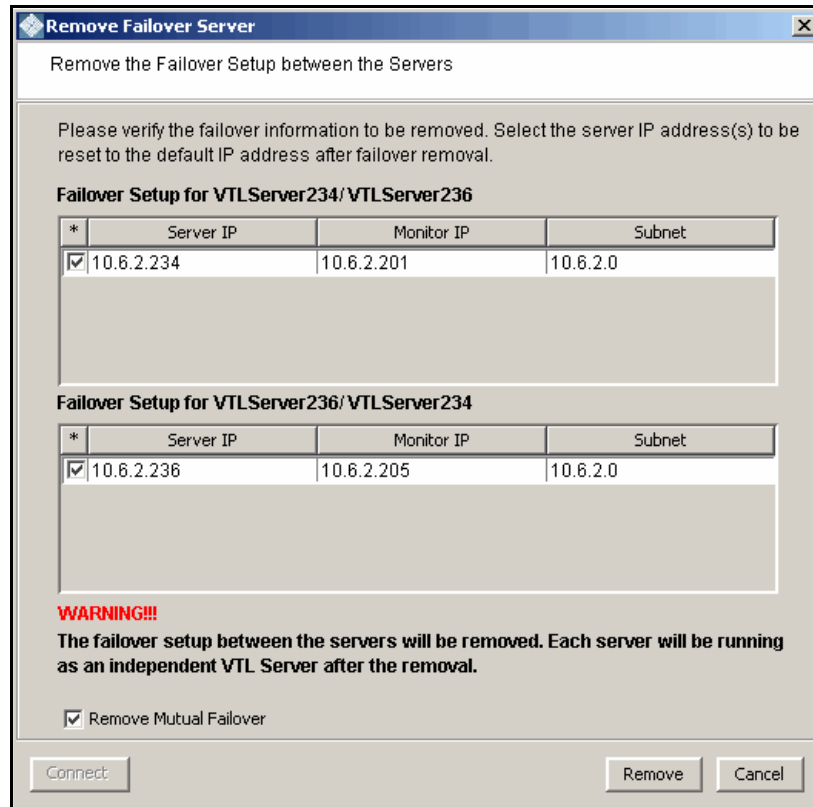
Select the *Edit* menu --> *Add* and type the original primary server's virtual IP address in the *VTL User Logon* dialog.

10. Enable Auto Recovery on the surviving server in order for the newly-built/repaired primary server to become the primary server.

Alternately, you can manually initiate a recovery to your primary server. Select *Tools -> Failover -> Stop Takeover* if your failover configuration was configured not to use VTL's Auto Recovery and you want to force control to return to your primary server.

## Remove a failover configuration

Right-click on one of your failover servers and select *Failover --> Remove Failover Server* to remove the selected server from the failover configuration.



If everything is checked, as in the example above, this eliminates the failover relationship and removes the health monitoring IP addresses from the servers and restores the server IP addresses. If you uncheck the IP address(es) for a server, the health monitoring address becomes the server IP address.

---

## Resuming backups after failover/failback

When failover and recovery occur, there is a three minute delay. During this time, no I/O is permitted and all backup jobs (including import/export and replication) will fail.

While failover and failback are transparent for the VTL server, after failover/failback occurs, you may need to take some action in your backup application in order for it to work properly with VTL. The action you take varies by backup application and operating system. We have described some of the actions we have used. Your environment may differ. Refer to the documentation that came with your backup application for more details.

### *BakBone NetVault™*

After failover/failback occurs, if the Windows Device Manager hangs, you must reboot your NetVault server.

Once devices are visible by both the operating system and NetVault, if the NetVault job hangs while waiting to connect to the tape media, reboot your NetVault server.

### *CommVault Galaxy™*

If Galaxy has pending jobs, right-click on each job to resume it.

On Windows, before resuming the jobs, you should scan for hardware changes through the Windows Device Manager and confirm that the tape drives are back.

### *CA ARCserve®*

After failover/failback occurs, if the operating system and/or ARCserve losses devices, stop the ARCserve tape engine, rescan the operating system, and then restart the ARCserve tape engine. If you still cannot see devices, reboot your ARCserve server.

Once devices are visible by both the operating system and ARCserve, start ARCserve, eject all tapes from their drives and then re-inventory the library.

### *HP OpenView Storage Data Protector*

During failover/failback, backup jobs may fail. When this occurs, the tape will be marked as *poor* quality and it will stay in the tape drive. Manually move the tape back to the slot.

### *IBM® Tivoli® Storage Manager*

After failover/failback occurs, reboot the Tivoli Storage Manager machine to get the devices back before submitting any jobs.

---

## *EMC NetWorker®*

After failover/failback, NetWorker will mark the tape for the current backup job as *full* and will use a new blank tape to continue the backup job.

## *Symantec Backup Exec™*

If Backup Exec has stalled jobs, reboot the Backup Exec server.

If there are no stalled jobs, but drives are down during failover or failback, everything should recover normally.

## *Veritas NetBackup™*

On Windows, if NetBackup has stalled jobs, reboot the NetBackup server. After rebooting, check the NetBackup tape drive/library status and restart NetBackup services, if needed.

On Windows, if drives are failed or missing, bringing up the drives should be sufficient. However, if one or more of the drives cannot be brought up, reboot the NetBackup server.

On Solaris, jobs usually fail *gracefully* and subsequent jobs start without problem.

---

## Fibre Channel port behavior during failover

This section discusses the status of Fibre Channel ports during and after failover.

### *Sample environment*

- There are two appliances, "A" and "B", which act as failover partners.
- Each appliance has two Target Ports (T1 and T2 for A, and T3 and T4 for B).
- Each appliance has two Standby Ports (S1 and S2 for A, and S3 and S4 for B).

Note: T1, T2, T3, T4, S1, S2, S3, and S4 represent WWPNs.

### *Before failover*

#### **Appliance A**

- T1 and T2 are set to Target Mode.
- S1 and S2 are set to Initiator Mode.
- There are four FC WWPN entries coming from A to the switch (T1, T2, S1, S2).

#### **Appliance B**

- T3 and T4 are set to Target Mode.
- S3 and S4 are set to Initiator Mode.
- There are four FC WWPN entries coming from B to the switch (T3, T4, S3, S4).

#### **Port status**

- A = T1 T2 S1 S2
- B = T3 T4 S3 S4

### *When failover occurs*

#### **Server A fails over to B**

Target mode ports are unloaded from server A's T1 and T2 ports and these WWPNs disappear from the FC switch.

- A = 00 00 S1 S2
- B = T3 T4 S3 S4

Immediately, ports T1 and T2 will be spoofed with "temporary"/monitoring WWPN ports (X1 and X2) and they re-appear on the FC switch as initiator mode ports with two new WWPNs, different from the original WWPNs of T1 and T2.

- A = X1 X2 S1 S2
- B = T3 T4 S3 S4

S3 and S4 (previously in initiator mode) are then unloaded from server B and their WWPNs disappear from the FC switch.

- 
- A = X1 X2 S1 S2
  - B = T3 T4 00 00

Immediately, both S3 and S4 will be spoofed/impersonated with the original WWPNs from T1 and T2 and they will be reloaded as target ports. They will then re-appear as target ports (the original WWPNs coming from T1 and T2) after failover:

- A = X1 X2 S1 S2
- B = T3 T4 T1 T2

Note: There are never any duplicate WWPN entries in the FC switch.

## *After failover*

### **Server B stops takeover of server A**

Target mode ports T1 and T2 are unloaded from server B and these WWPNs disappear from the FC switch.

- A = X1 X2 S1 S2
- B = T3 T4 00 00

Immediately, ports S3 and S4 will regain their original WWPN ports and they appear on the FC switch as initiator mode ports.

- A = X1 X2 S1 S2
- B = T3 T4 S3 S4

The "temporary"/monitoring WWPN ports (X1 and X2) are unloaded from server A and these WWPNs disappear from the FC switch.

- A = 00 00 S1 S2
- B = T3 T4 S3 S4

Immediately, both T1 and T2 will be loaded with their original WWPNs and they will then re-appear on the FC switch as target ports.

- A = T1 T2 S1 S2
- B = T3 T4 S3 S4

Note: There are never any duplicate WWPN entries in the FC switch.

---

## IP address behavior during failover

This section discusses the status of IP addresses during and after failover.

### *Sample environment*

- There are two appliances, "A" and "B", which act as failover partners.
- Each appliance has two IP addresses (A1 and A2 for A, and B1 and B2 for B).

Note: A1, A2, B1, and B2 represent IP addresses.

### *After failover is configured*

#### **Appliance A**

- A1 and A2 are virtual IP addresses to which the client connects.
- A1' and A2' are IP addresses used for monitoring.

#### **Appliance B**

- B1 and B2 are virtual IP addresses to which the client connects.
- B1' and B2' are IP addresses used for monitoring.

### *When failover occurs*

#### **Server A fails over to B**

A1 and A2 are unloaded from server A.

- A = A1' A2'
- B = B1' B1 B2' B2

After server B takes over for server A, A1 and A2 are added to server B.

- A = A1' A2'
- B = B1' B1 A1 B2' B2 A2

Note: There are never any duplicate IP addresses.

### *After failover*

#### **Server B Stops Takeover of Server A**

A1 and A2 are unloaded from server B.

- A = A1' A2'
- B = B1' B1 B2' B2

After server A recovers, A1 and A2 are added to server A.

- A = A1' A1 A2' A2
- B = B1' B1 B2' B2

Note: There are never any duplicate IP addresses.



---

## Port swapping for Brocade switches

In a failover setup, the client driver recognizes the drives by port ID instead of WWPN. When failover occurs, as the standby adapters on the secondary are connecting to different port IDs, the client is no longer be able to see the drives.

While Cisco switches automatically swap ports, if you are using a Brocade switch, you need to create the following port swapping scripts:

- A pre-takeover script to switch port IDs when failover occurs.
- A pre-recovery script to change the port IDs back before failback occurs.

This section contains instructions and sample scripts that can be used on AIX or an HP-UX clients using a Tachyon adapter with Brocade switch models, 3900, 12000, 24000, 4100, etc. The scripts should be configured during deployment.

The following port swapping files can be found in `/usr/local/vtl/bin`:

- `port_enable_disable.sh`
- `portswap.sh`
- `preRecovery.portswap`
- `preTakeOver.portswap`



Notes:

- Tape drive multi-pathing is not supported with port swapping. Even though you can configure VTL to assign one drive to two paths, failover will not be transparent, meaning that when the backup job fails, the client will need to be reconfigured to use the device from the second path.
- Brocade switches running 5.01x firmware do not allow for SSH login without a password. Therefore, port swapping scripts will not work.
- Port swapping scripts are not valid for older McData switches.

To configure port swapping:

1. If you haven't already done so, set up failover on your VTL server.
2. Verify that SSH is installed on both VTL servers (SSH is installed by default).
3. Set up switch zoning.
4. Build SSH host-based authentication between VTL servers and the Brocade switch.

To do this:

- SSH to the Brocade switch using the "root" user account (the default password is: *password*).
- On both VTL servers, run: `ssh-keygen -t rsa`, which generates two files in `/.ssh`: `id_rsa` and `id_rsa.pub`.
- On both VTL servers, run: `ssh root@<switch IP address>`. After logging in to the switch, exit from SSH. This step will populate VTL servers as "known hosts" to the Brocade switch.

- Append both VTL servers' `/.ssh/id_rsa.pub` to Brocade switch's `/root/.ssh/authorized_keys`.

From the Brocade switch:

```
#scp root@[ipstor address]:/.ssh/id_rsa.pub /root/tmp_id_rsa.pub
#cat /root/tmp_id_rsa.pub >> /root/.ssh/authorized_keys
```

- Repeat these steps for other Brocade switches, if any(\*). If you can SSH to the switch from VTL server without prompting password, the shared secret is exchanged properly.

(\*) The portswap command will only work within one switch. You can have multiple pairs of target and standby ports located on different switches but the target-standby ports of each pair need to be located on the same Brocade switch.

5. Copy `portswap.sh` to both VTL servers and change its mode:

```
#cp portswap.sh $ISHOME/bin
#chmod 500 $ISHOME/bin/portswap.sh
```

6. Copy `port_enable_disable.sh` to both VTL servers and change its mode:

```
#cp port_enable_disable.sh $ISHOME/bin
#chmod 500 $ISHOME/bin/port_enable_disable.sh
```

7. Copy `preRecovery.portswap` to the primary server, rename, and change its mode:



Note: Be sure to make a backup copy of the original `preRecovery`.

```
#cp preRecovery.portswap $ISHOME/bin/preRecovery
#chmod 500 $ISHOME/bin/preRecovery
```

8. Copy `preTakeOver.portswap` to the secondary server, rename, and change its mode:



Note: Be sure to make a backup copy of the original `preTakeOver`.

```
#cp preTakeOver.portswap $ISHOME/bin/preTakeOver
#chmod 500 $ISHOME/bin/preTakeOver
```

9. Use the `switchshow` command to collect the area/slot/port information.

For Brocade 12000 ONLY, the portswap command requires the slot/port as the input parameter.

10. Confirm switch port connection(s) and fill in the following information in `preRecovery` and `preTakeOver` accordingly:

- IP address for switch(es)
- Area ID (if no area ID, put any one of the ports to be swapped)
- Ports to be swapped

You will need one line for each target-standby port pair.

11. Run `$ISHOME/bin/preTakeOver` to make sure port IDs are swapped correctly.

12. Run `$ISHOME/bin/preRecovery` to make sure port IDs are swapped back.

13. Take x-rays of VTL servers for your records.

---

## HP-UX

HP-UX is very sensitive to "target ID", not only switch port ID but also the VTL target port's hard\_loop ID. If the target is using loop mode, the hard\_loop ID for the target port and its standby port must match. The default HBA BIOS setting will not provide you a pair of identical hard\_loop IDs.

Point-to-point topology is recommended with QLogic HBAs.

For Brocade 3900 and 4100 switches, area\_id must be one of the port IDs that will swap. For example:

```
portswap.sh swapped 10.1.1.60 10 10 11 &
```

For Brocade 12000 or 24000 switches, the format must be:

```
portswap.sh normal <switch IP> <area id> <slot1/port 1> <slot2/port 2>
```

Use the switchshow command to find out area, slot, and port IDs.

If multiple ports need to be swapped, use multiple lines of portswap.sh commands. For example:

```
portswap.sh normal 10.1.1.60 10 10 11 &
portswap.sh normal 10.1.1.60 12 12 13 &
```

### *PreTakeOver script*

The following is a sample preTakeOver script:

```
#!/bin/sh

logger -p daemon.notice preTakeOver: start

# syntax here is:
#   portswap.sh normal <switch IP> <area id> <[slot1/]port 1> <[slot2/
]port 2>
#           <[slot3/]port 3> <[slot4/]port 4> [ ... ]]
# example:
#   portswap.sh normal 10.1.1.60 49 4/1 4/2 &
# or
#   portswap.sh normal 10.1.1.60 28 27 28 &

portswap.sh normal xx.xx.xx.xx area_xx port1 port2 &
sleep 10

logger -p daemon.notice preTakeOver: end
```

### *PreRecovery script*

The following is a sample preRecovery script:

```
#!/bin/sh

logger -p daemon.notice preRecovery: start
```

---

```
# syntax here is:
#   portswap.sh swapped <switch IP> <area id> <[slot1/]port 1>
<[slot2/]port 2>
#   [ <[slot3/]port 3> <[slot4/]port 4> [ ... ] ]
# example:
#   portswap.sh swapped 10.1.1.60 49 4/1 4/2 &
# or
#   portswap.sh swapped 10.1.1.60 28 27 28 &

portswap.sh swapped xx.xx.xx.xx area_xx port1 port2 &
sleep 10

logger -p daemon.notice preRecovery: end
```

# Replicate Data

Replicating data protects the information on a virtual tape by maintaining a copy of the virtual tape on the same VTL server or on another VTL server.

There are three methods to replicate tape data in VTL; two provide automatic replication and one is a manual process that can be used if you are not using the automatic methods:

Feature	Automatic/Manual	Description
Auto Replication	Automatic	Replicates the contents of a single tape whenever a virtual tape is exported from a virtual library (such as from a backup application or other utility).
Replication	Automatic	Replicates <i>changed</i> data from a primary virtual tape to the same VTL server or another VTL server at prescribed intervals, based on user defined policies.
Remote Copy	Manual	Replicates the contents of a single tape <i>on demand</i> .

## Auto Replication

*Auto Replication* replicates the contents of a single tape whenever a virtual tape is exported from a virtual library (such as from a backup application or other utility).

*Auto Replication* is enabled when you create a virtual tape library. If it is enabled for a library, when you create tapes for the library, you can enable/disable *Auto Replication* for the individual tape.

If you want to enable *Auto Replication* for an existing library:


1. Right-click on a virtual tape library and select *Properties*.
2. Select *Auto Replication*.
3. Select whether you want the virtual tape copied (retained) or moved (removed) after the data is replicated.

If you select to move it, indicate how long to wait before deleting it

4. Select the target server.

## Remote Copy

You can copy the contents of a single tape whenever you need to. Because the *Remote Copy* feature replicates the full tape rather than appending to an existing virtual tape, you can only copy a tape if there is no virtual tape on the target server with the same barcode. Therefore, if you have copied this tape before, you must delete the copy from the target server before continuing.

 Note: You cannot copy a tape that is configured for replication or *Auto Replication/ Auto Archive*.

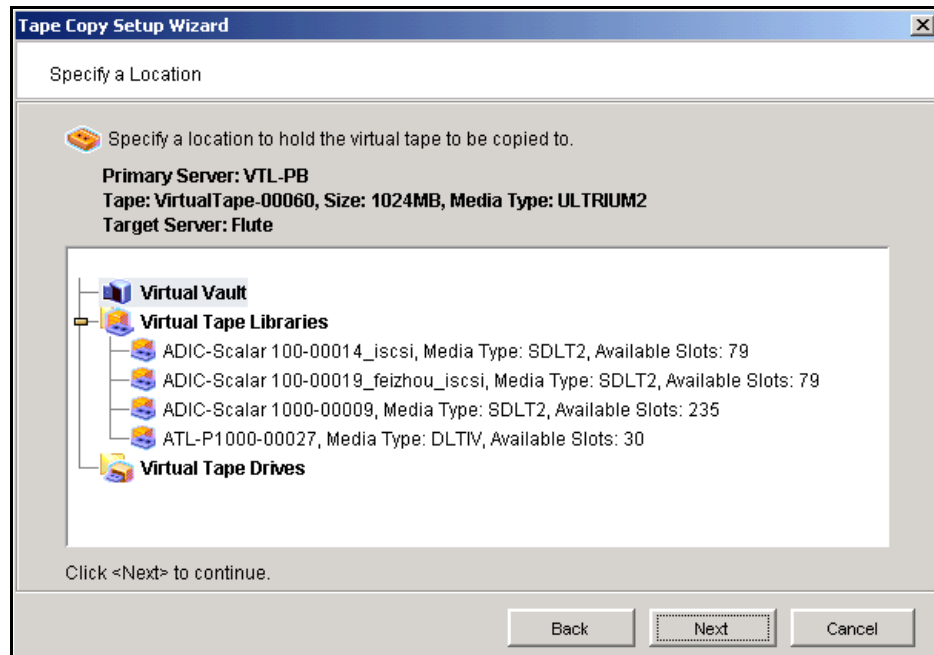
1. Right-click on a tape and select *Remote Copy*.

2. Select if you want to copy to a local or remote server.

If you select to copy to a remote server, you will have to select the server. If the server you want does not appear on the list, click the *Add* button.

3. Confirm/enter the target server's IP address.

4. Select a location for the copied tape.



You can select a tape library or the virtual vault.

If you select a tape library, the media must be compatible.

5. Confirm that all information is correct and then click *Finish* to create the copy.

## Replication

Replication is a process that protects the data on a virtual tape by maintaining a copy of a virtual tape.

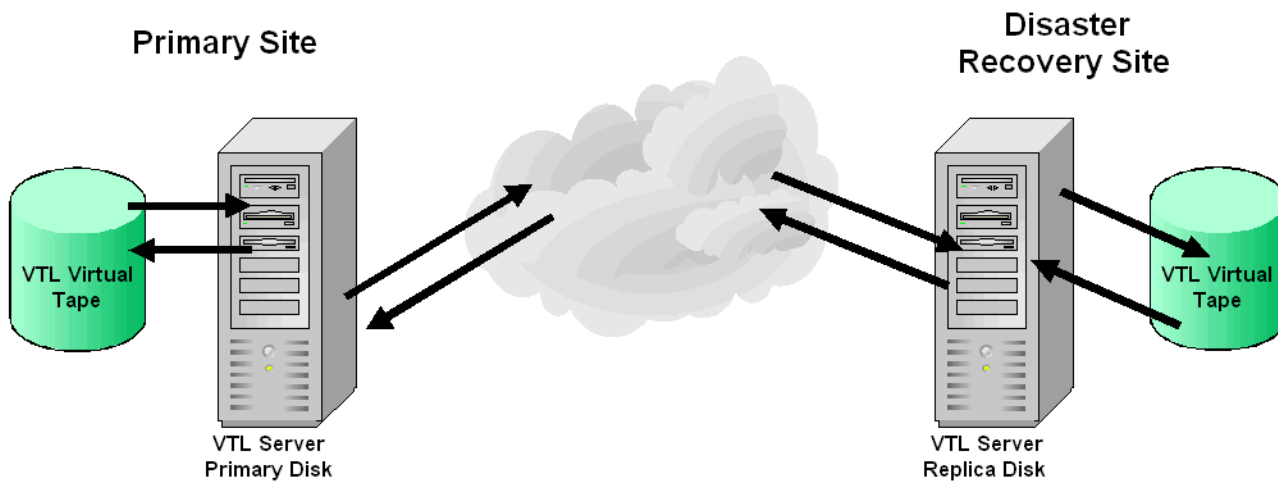
At prescribed intervals, when the tape is not in use, changed data from the *primary* virtual tape is transmitted to the *replica resource* on the target server so that they are synchronized. The target server is usually located at a remote location. Under normal operation, backup clients do not have access to the replica resource on the target server.

If a disaster occurs and the replica is needed, the administrator can *promote* the replica to become the primary virtual tape so that clients can access it.

VTL offers two types of replication, *Remote Replication* and *Local Replication*. Both types can be enhanced with the *Compression* and/or *Encryption* options.

**Remote Replication** Remote Replication allows fast, data synchronization of storage volumes from one VTL server to another over the IP network.

With Remote Replication, the replica disk is located on a separate VTL server, called the *target server*.

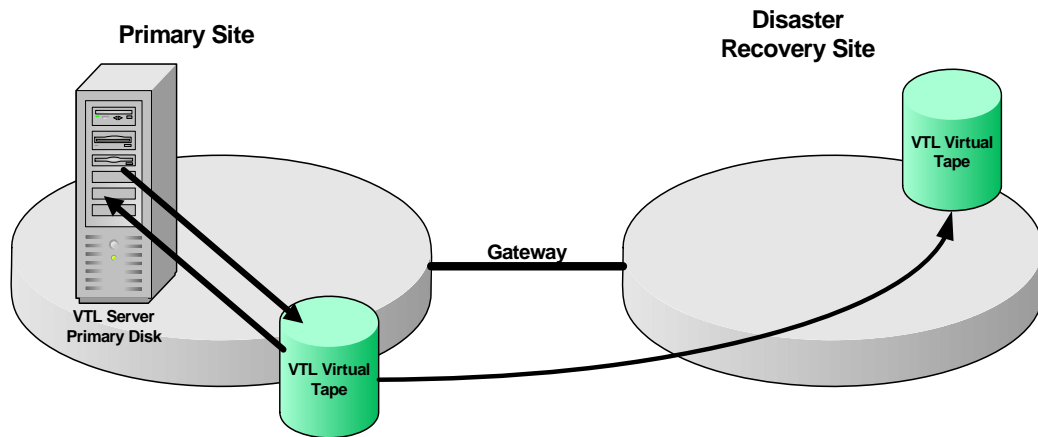


**Local Replication** Local Replication allows fast, data synchronization of storage volumes within one VTL server. Because there is only one VTL server, the primary and target servers are the same server.

Local Replication can be used to maintain a local copy of virtual tape data or it can be used to maintain a remote copy within metropolitan area Fibre Channel SANs.

---

With Local Replication, the replica disk can be connected to the VTL server via a gateway using edge routers or protocol converters.



### *Replication requirements*

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

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

### *Port requirements for replication*

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

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

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

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



---

port, regardless of whatever IP addresses you have set for the replication ports. The same holds true for the target server. Replication traffic will go to the principle port on the target server, the one that is used for management traffic.

To set the addresses, do not use Solaris commands like `ifconfig`. Set the IP addresses from within the VTL console. Log in with root permissions and right-click on the server name so that a menu pops up and allows you to select "System Maintenance." From within "System Maintenance," select "Network." Select the interface you want to configure (net2 or net3), assign the port the proper address, netmask and gateway. Configure the second port with its own address, but use the same netmask and gateway.

When you set up replication, select the target server's IP addresses that are to be used for replication. Do not use the target server's main management port. The replication IPs must be on a different subnet than the management IPs.

If you follow these instructions, replication traffic will have two ports to use on both ends and replication traffic will not be competing with traffic for VTL management or internal VTL management. The best performance will come if you are able to dedicate the network segment for replication and not have the replication traffic.

## Setup

You must enable replication for each virtual tape that you want to replicate.

1. Right-click on a virtual tape and select *Replication --> Add*.

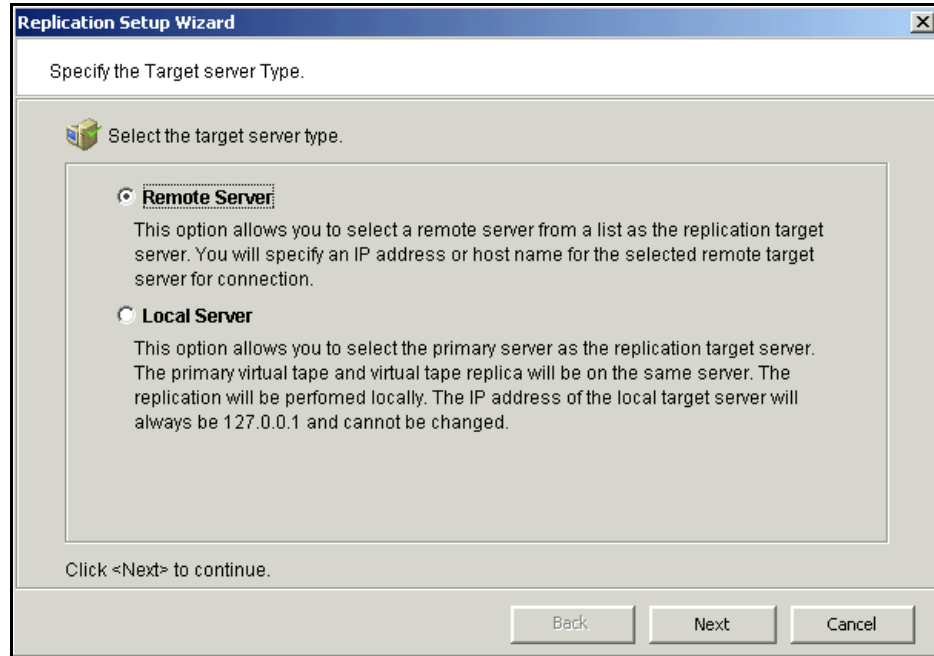
To enable replication for multiple virtual tapes in the same virtual tape library, right-click on the virtual tape library and select *Replication --> Add*.

Each virtual tape can only have one replica resource.

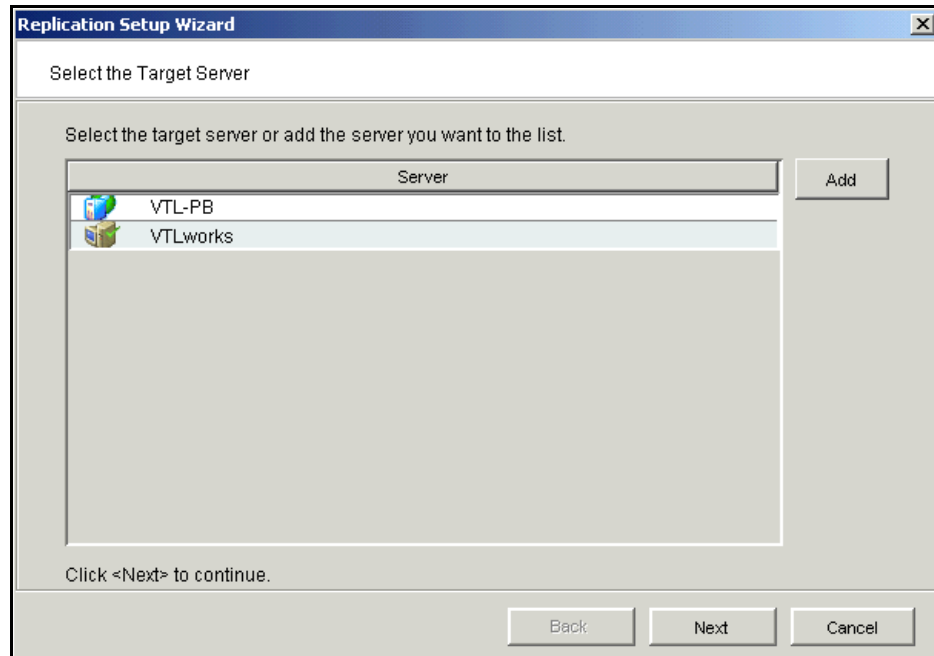


Note: If you get a message that Replication cannot be enabled because *Auto Archive/Replication* is enabled, you must first disable *Auto Archive/Replication* for the tape. To do this, right-click on the tape (or virtual tape library for all tapes) and select *Properties* and go to the *Auto Archive/Replication* tab.

2. Indicate whether you want to use remote replication or local replication.



3. Select the server that will contain the replica.

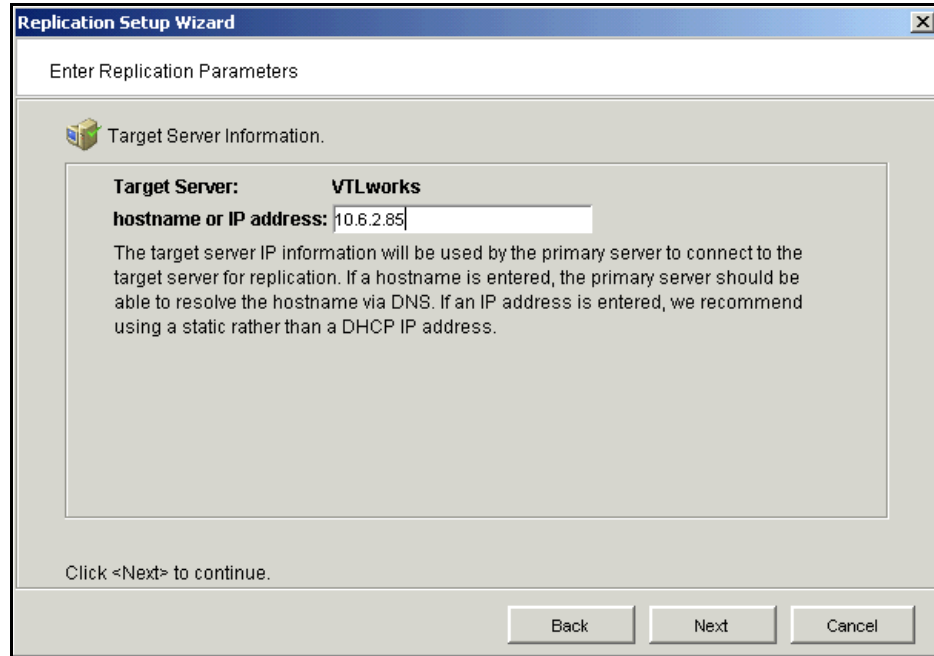


If the server you want does not appear on the list, click the *Add* button.

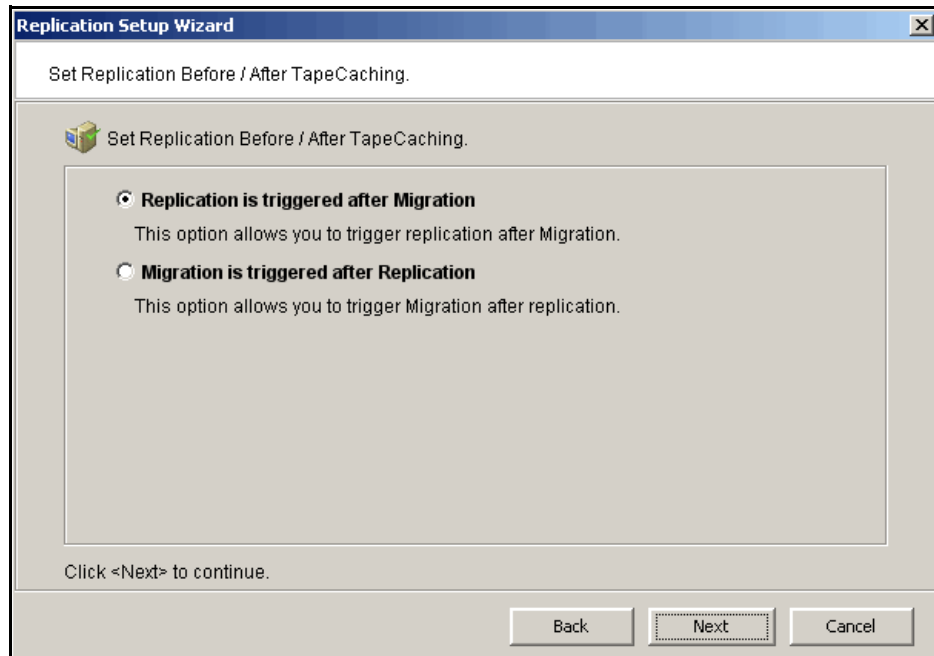


Note: For Solaris systems, the target server must be a 64-bit server.

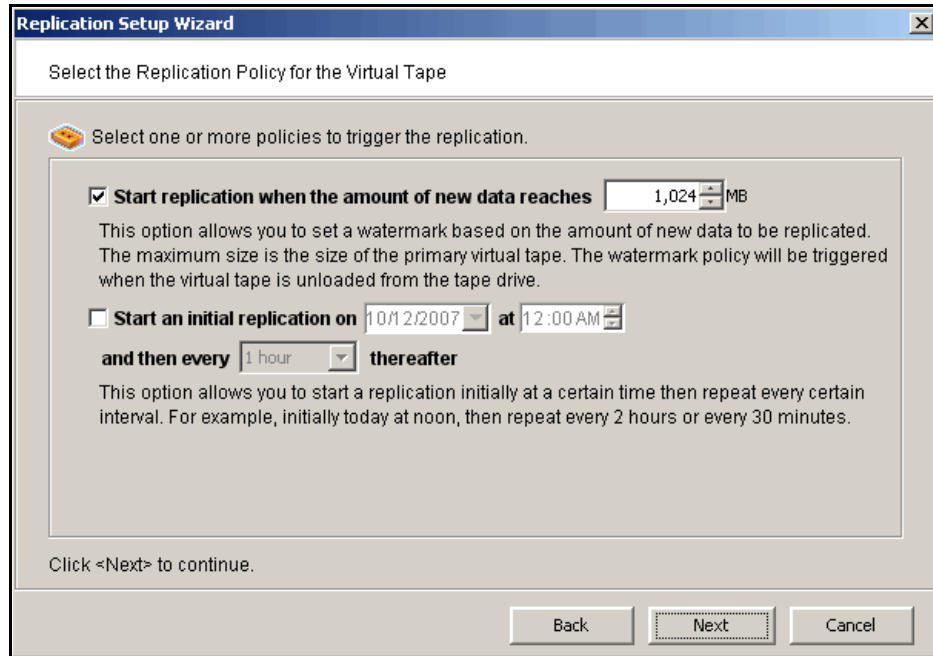
4. Confirm/enter the target server's IP address.



5. (Tape caching is enabled) Configure whether replication should occur before or after migration.



6. (Tape caching is not enabled) Configure how often, and under what circumstances, replication should occur.



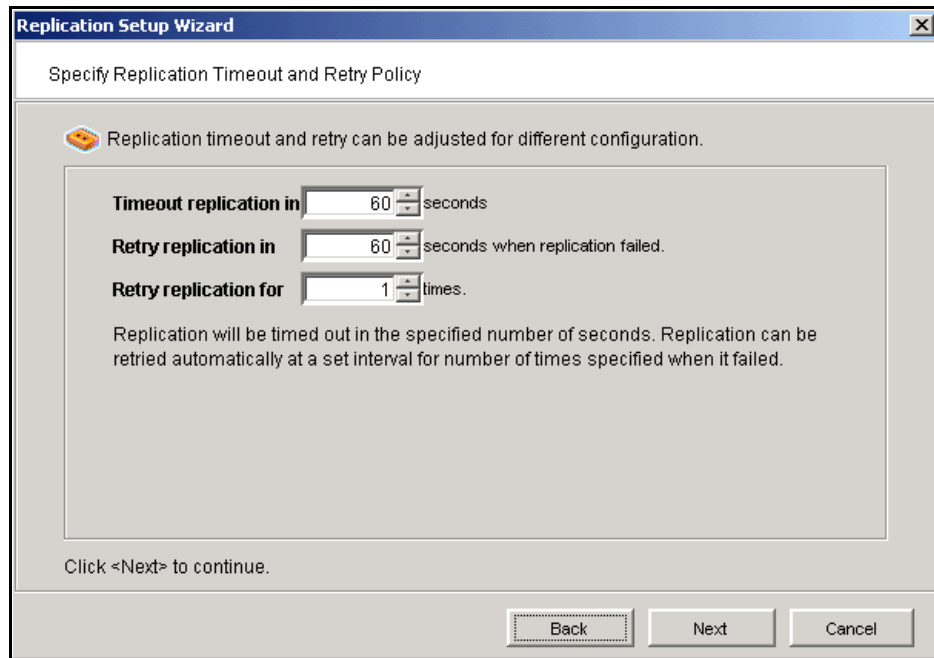
You must select at least one policy, but you can have multiple.

*Start replication when the amount of new data reaches* - If you enter a watermark value, when the value is reached, replication of the changed data will begin as soon as the virtual tape is back in the library.

*Start an initial replication on mm/dd/yyyy at hh:mm and then every n hours/minutes thereafter* - Indicate when replication should begin and how often it should be repeated.

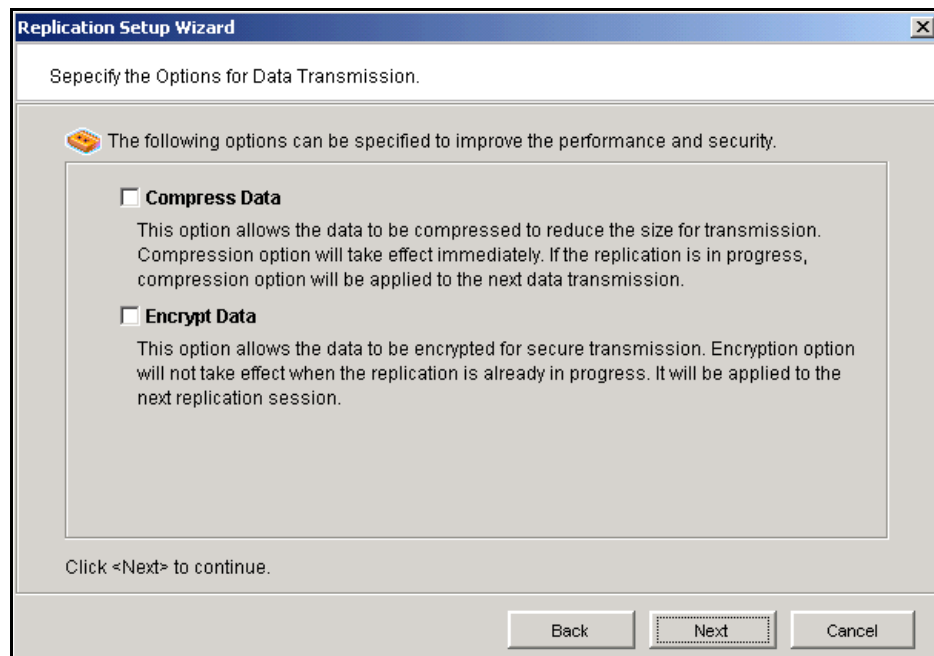
If a replication is already occurring when the next time interval is reached, the new replication request will be ignored.

7. Indicate what to do if a replication attempt fails.



Replication can only occur when the virtual tape is in the vault and is not in use. Indicate how long the system should attempt to replicate data before timing out and how often it should attempt to retry before skipping a scheduled replication.

8. (Remote Replication only) Indicate if you want to use *Compression* and/or *Encryption*.



The *Compression* option provides enhanced throughput during replication by compressing the data stream.

The *Encryption* option secures data transmission over the network during replication. Initial key distribution is accomplished using the authenticated Diffie-Hellman exchange protocol. Subsequent session keys are derived from the master shared secret, making it very secure.

9. Enter a name for the replica resource.

Enter the Tape Replica Resource Name

**Tape Resource: VirtualTape-00158 (ID: 158), Size: 5,120MB.**

Physical device(s) selected for the Tape Replica Resource.

**Tape Replica Resource Name:** throgneck2-VirtualTape-00158

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

Device Name	SCSI Address	First Sector	Last Sector	Size(MB)
SEAGATE:ST336605FC	5:0:10:0	16822272	27308031	5120

Click <Next> to continue.

Back Next Cancel

The name is not case sensitive.

10. Confirm that all information is correct and then click *Finish* to create the replication configuration.



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.

## Check replication status

There are several ways to check replication status:

- *Replication* tab of the primary virtual tape - displays the policies set for replication as well as the replication status.
- *General* tab of the Replica Resource on the target server - displays status of replication in progress.
- Event Log - displays status and operational information, as well as any errors.
- Replication Status Report - can be run from the *Reports* object. It provides a centralized view for displaying real-time replication status for all tapes enabled for replication. It can be generated for an individual tapes, multiple tapes, source server or target server, for any range of dates. This report is useful for administrators managing multiple servers that either replicate data or are the recipients of replicated data. The report can display information

about existing replication configurations only or it can include information about replication configurations that have been deleted or promoted (you must select to view all replication activities in the database). The following is a sample *Replication Status Report*:

Replication Status

---

**Replication Status Report**  
**Primary Server: throgsneck2, TAPE Resources**  
*06/23/2004-06/23/2004*

Report Date: 06/23/2004  
Report Sort: Sort by target server name, then by target disk name, then by log date and time.

Primary Server: throgsneck2 (10.3.3.161)  
Primary Disk: VirtualTape-00160 (ID: 160)  
Target Server: VTLworks (10.6.2.85)  
Target Disk: throgsneck2-VirtualTape-00160 (ID: 483)

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						
06/23 15:58:27	Idle	06/23/04 15:58:25-06/23/04 15:58:26	5120	admin.		n/a

## Promote a replica resource

If a replica resource is needed, the administrator can *promote* the replica to become a usable virtual tape. After promotion, the virtual tape is put into the virtual vault so that you can move it to any virtual library on *that* server (formerly the target server). If you need to get the virtual tape back to the formerly primary server, you must replicate it back to that server.

Promoting a replica resource breaks the replication configuration. Once a replica resource is promoted, it cannot revert back to a replica resource.

You must have a valid replica resource in order to promote it. For example, if a problem occurred (such as a transmission problem or the replica resource failing) during the first and only replication, the replicated data would be compromised and therefore could not be promoted to a primary virtual tape.

You cannot promote a replica resource while a replication is in progress.

1. In the Console, locate the target server, right-click on the appropriate Replica Resource and select *Replication --> Promote*.
2. Confirm the promotion and click *OK*.
3. From the client, rescan devices or restart the client to see the promoted virtual tape.

---

## Change your replication configuration options

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 the configuration:

1. Right-click on the primary virtual tape and select *Replication --> Properties*.
2. Make the appropriate changes and click *OK*.

## Suspend/resume replication schedule

You can suspend future replications from automatically being triggered by your replication policies (watermark, interval, time). This will not stop a replication that is currently in progress. You can still manually start the replication process while the schedule is suspended. To suspend/resume replication, right-click on the primary virtual tape and select *Replication --> Suspend* (or *Resume*).

You can see the current settings by checking the *Replication Schedule* field on *Replication* tab of the primary virtual tape.

## Stop a replication in progress

To stop a replication that is currently in progress, right-click on the primary virtual tape and select *Replication --> Stop*.

## Manually start the replication process

To force a replication that is not scheduled, select *Replication --> Synchronize*.

## Remove a replication configuration

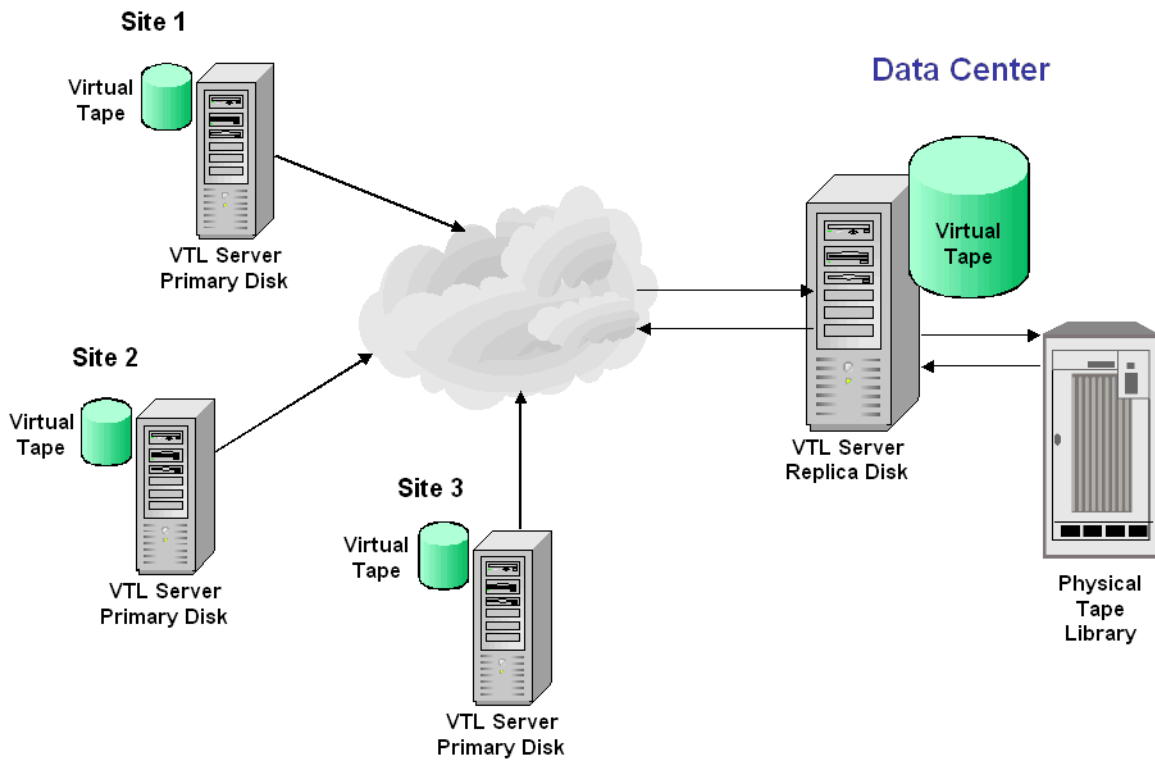
Right-click on the primary virtual tape and select *Replication --> Remove*. This allows you to remove the replication configuration on the primary and either delete or promote the replica resource on the target server at the same time.

## Replication and Failover

If replication is in progress and a failover occurs at the same time, the replication will stop. After failover, replication will start at the next normally scheduled interval. This is also true in reverse, if replication is in progress and a recovery occurs at the same time.



## Consolidating tapes from multiple locations to a single data center



The following information is for environments with multiple VTL locations *without* physical tape libraries that replicate tape data to a remote VTL server that *has* a physical tape library that supports barcodes.

In this environment, if you will be exporting tapes from the remote VTL server to the physical tape library, you want to make sure that when you create tapes on the primary servers (at the multiple VTL locations *without* physical tape libraries), you match the barcodes of the tapes on the physical library attached to the target server.

# Automated Tape Caching

---

The Automated Tape Caching option enhances the functionality of VTL by acting as a cache to your physical tape library, providing transparent access to data regardless of its location.


With the Automated Tape caching option, tapes will always appear to be inside virtual libraries and will be visible to the backup application regardless of whether the data is actually on disk or tape. This means that the backup application will always have direct access to data regardless of whether the data is on disk or on physical tape.

The Automated Tape Caching option also provides advanced flexibility that allows you to set up policies that automatically trigger data migration to physical tapes based on criteria, such as the number of days that data has been on disk or the amount of used disk space.

With Automated Tape Caching, you can not only determine which events will activate the action, but also when it will occur. For example, you can set the policy to migrate the data immediately or at a specific time or day. This enables data to be written to physical tapes as a background process without impacting production servers.

You can also set up a reclamation policy that allows you to specify when the data that has been migrated to physical tape can be deleted from the disk to make space for new backups.

In order to use Automated Tape Caching, you must enable the option, set your migration and reclamation policies, and create a cache for each of your physical tapes. You may have done this during the initial setup wizard when you first launched VTL. If not, the instructions below will show you how.

 Note: You can use Automated Tape Caching only if you are not currently using the Auto Archive/Replication feature on this virtual tape library.

---

## Tape caching policies

A tape caching policy contains the data migration triggers and reclamation triggers for a virtual tape library. The tape caching policy affects how data will be read/written from/to tapes.

### **Scenario 1: Data on virtual tape. Data not written to physical tape.**

If the data has not been written to physical tape, reads will be from the virtual tape. Writes will either append or rewrite the virtual tape.

### **Scenario 2: Data written to physical tape. Virtual tape not reclaimed.**

If the data has been written to physical tape but is still retained on the virtual tape, reads will be from the virtual tape. Writes to the tape will either append or rewrite the virtual tape (and start the clock over on the migration policy).

### **Scenario 3: Data written to physical tape. Virtual tape reclaimed.**

If the data has been written to physical tape and the virtual tape has been reclaimed, reads will be directly from the *direct link* tape. A *direct link* tape is not an actual tape but a link to a physical tape. If you overwrite the beginning of the tape, VTL will create a new virtual tape, which breaks the *direct link* tape and starts the clock over on the migration policy. If you try to append to the tape, VTL will append data on the physical tape.

## Create/change a tape caching policy

To create or change a tape caching policy:

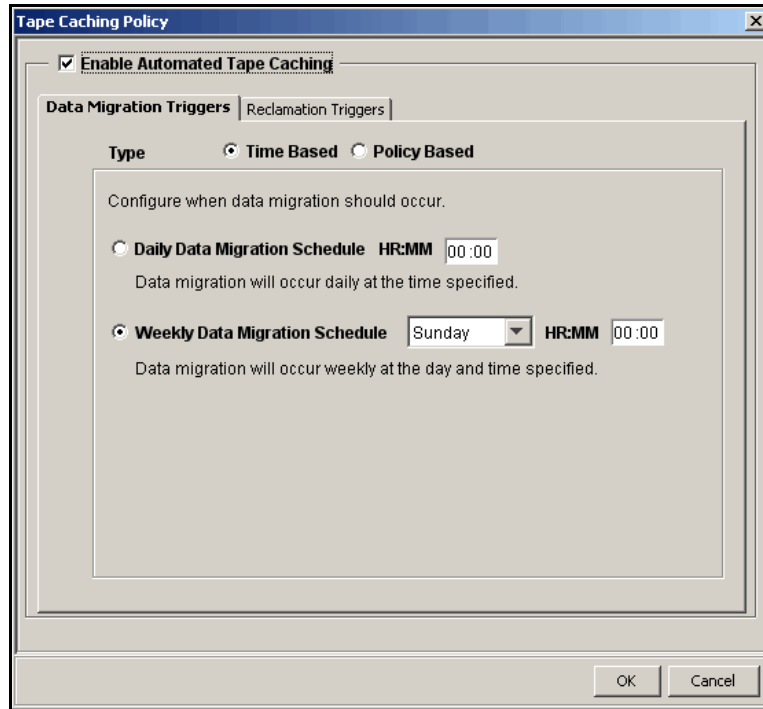
1. Right-click on a virtual tape library and select *Automated Tape Caching*.
2. If necessary, select the *Enable Automated Tape Caching* check box.
3. On the *Data Migration Triggers* tab, select the type of data migration triggers that you want to set.

Data migration triggers control when data in the cache will be copied to physical tape.



Note: Regardless of which triggers you set, there must be at least 1 MB of data on the tape in order to trigger data migration.

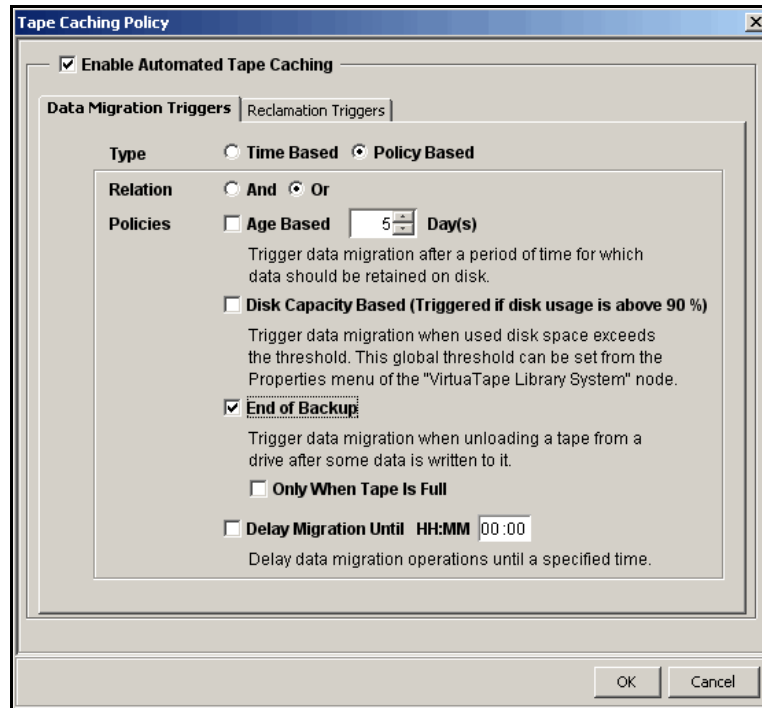
For *Time Based* triggers, specify when data migration should actually occur.



*Daily Data Migration Schedule* - Migration occurs at a specific time of day. Type the hour and minute (in 24-hour format) in the box. For example, if you want the migration to occur at 11:30 p.m., you would type 23:30. Note that if the specified time has already elapsed when the trigger occurs, the migration will occur at that time on the next day.

*Weekly Data Migration Check Schedule* - Migration occurs on a specific day of the week. Specify the day of the week from the list and type the hour and minute (in 24-hour format) in the text box. Note that if the specified time has already elapsed when the trigger occurs, the migration will occur at the next scheduled day and time.

For *Policy Based* triggers, determine what criteria will trigger migration.



Click *And* if all the selected criteria must be met to initiate the data migration, or click *Or* if meeting any one of them will initiate the data migration.

For example, if you select both *Age Based* and *Disk Capacity Based*, and select *And*, data migration will occur only when both the specified number of days has elapsed and the specified disk capacity has been reached. If you select *Or*, the occurrence of either one of those events will trigger the data migration.

*Age Based* - Migration will occur when the data has been on the virtual disk for a specified number of days. Specify the desired number of days in the list box.

*Disk Capacity Based* - Migration will occur when the used disk space exceeds the specified disk capacity. The actual percentage is a global variable which is set for all virtual tape libraries. To change the number, right-click *Virtual Tape Library System* in the tree, click *Properties*, and type the desired percentage in the *Tape Caching Policy Disk Capacity Migration Threshold* box.

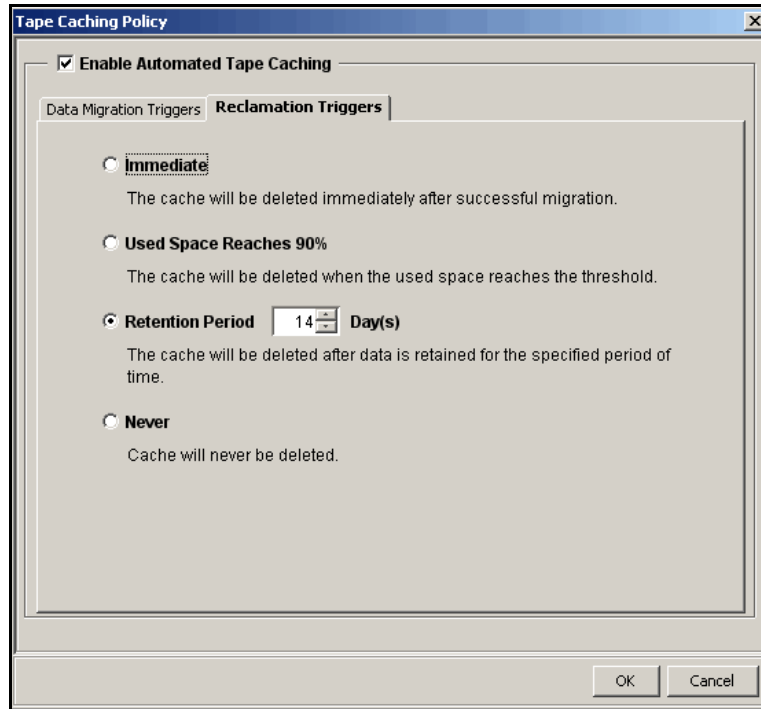


Note: The *Tape Caching Policy Disk Capacity Threshold* setting affects other capacity-based actions as well.

*End of Backup* - Migration will occur when a backup has completed and the virtual tape has been moved out of the virtual drive. If you select *Only When Tape is Full*, migration will only occur if the tape is full.

*Delay Migration Until* - Migration will be delayed until the time you specify after one of the above policies has been triggered. You may want to select a time when system usage is very light. Type the hour and minute (in 24-hour format) in the box.

- Click the *Reclamation Triggers* tab and specify when the data that has been migrated to physical tape can be deleted to free up cache disk space.



Note that after the reclamation is completed, the tape will become a *direct link* tape. A direct link tape is not an actual tape but a link to a physical tape. If your backup application ever overwrites the direct link tape, VTL will automatically start caching the physical tape.

*Used Space Reaches n%* - Cache disk space is freed up when the used space reaches this threshold. The actual percentage is a global variable which is set for all virtual tape libraries. To change the number, right-click *Virtual Tape Library System* in the tree, click *Properties*, and type the desired percentage in the *Tape Caching Policy Disk Capacity Reclamation Threshold* box.

*No More Space* - Cache disk space is freed up when additional space is needed. The oldest virtual tape that has been used least recently will be deleted.

*Retention Period* - Cache disk space is freed up after a specified number of days has elapsed. Specify the number of days that the data should be retained.

*Never* - Cache disk space is never freed up.

- Click *OK*.

The policy takes effect immediately.



Note: When you move a tape from the virtual tape library to a vault, it retains the Tape Caching policy associated with the original virtual tape library.

---

## Set global tape caching options

You can set global tape caching options for all virtual tape libraries. To do this:

1. Right-click on *VirtualTape Library System* and select *Properties*.
2. Set the global migration and reclamation thresholds.

*Migration Threshold* - Migration will occur when the used disk space exceeds the specified disk capacity.

*Reclamation Threshold* - Cache disk space is freed up when the used space reaches this threshold.

## Disable a policy

To disable a tape caching policy:

1. Right-click on a virtual tape library and click *Automated Tape Caching*.
2. Clear the *Enable Automated 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.

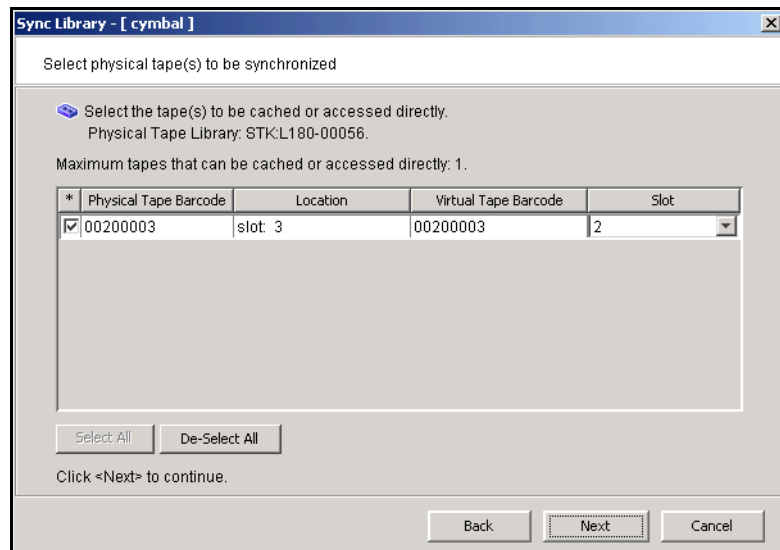
3. Click *OK*.

## Create a cache for your physical tapes

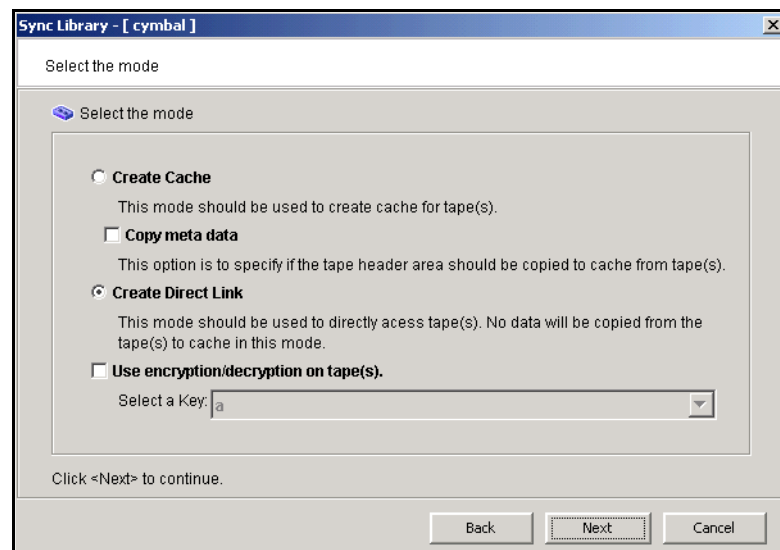
With the Automated Tape Caching option, data is stored on disk before being migrated to physical tape. In order to do this, you must create a cache for each of your physical tapes.

Do the following to create a cache for a physical tape:

1. Right-click on your virtual tape library and select *Sync Library*.
2. If you have multiple libraries, select the appropriate physical library.
3. Select the physical tape(s) for which you want to create a cache.



4. Select *Create Cache* and indicate if you want to use encryption.





---

*Copy meta data* - Copies the tape header from the physical tape to the cache. Select this option if your backup application requires a tape header to identify a tape.

*Use encryption/decryption on tape(s)* - Select if you want to encrypt the data on the tape. You can select this option only if at least one key has been created. If you select this option, you must select the key to use. All the data on the tape will be indecipherable until is imported back to a virtual tape library and decrypted using the same key. For more information about encryption, refer to [‘Encrypt data that is exported to physical tapes’](#).

5. Specify which physical device should be used to create the cache.
6. Specify a prefix, size, and starting number for the cache.
7. Confirm all information and click *Finish*.

## Create virtual tapes

Even though you are using Automated Tape Caching for your tape library, you can still create *uncached* virtual tapes that will not be migrated to physical tapes. This can be useful for a single backup that is not part of your normal backup routine. You can create one or more virtual tapes by right-clicking on a virtual tape library or on the *Tapes* object and selecting *New Tape(s)*.

Note that if you create virtual tapes, they cannot match the barcodes of your physical tapes.

## Force migration to physical tape

You can manually cause data in a cache to be migrated to physical tape. To do this, right-click on a virtual tape cache and select *Migrate to Physical Tape*. Note that this will overwrite all data on the physical tape.

## Reclaim disk space manually

You can manually cause the data that has been migrated to physical tape to be deleted to free up cache disk space. To do this for a single cache, right-click on a virtual tape cache and select *Reclaim Disk Space*. Note that this will overwrite all data in the cache.

To do this for multiple tape caches, right-click on the *VirtualTape Library System* object and select *Reclaim Disk Space*.

## Renew cache for a direct link tape

If your backup application ever overwrites the direct link tape, VTL will automatically start caching the physical tape. This eliminates the direct link and creates a cache for the physical tape.

---

You can also manually renew the cache for a direct link tape. To do this, right-click on a direct link tape and select *Renew Cache*.

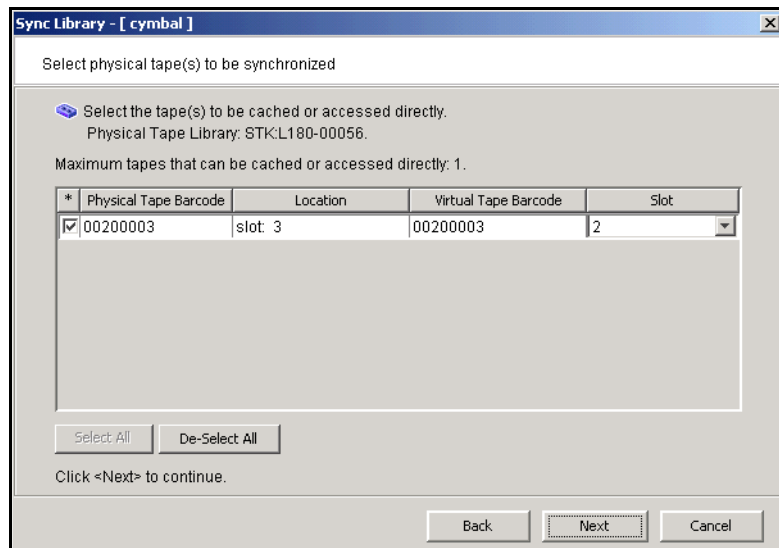
---

## Recover data using the Automated Tape Caching option

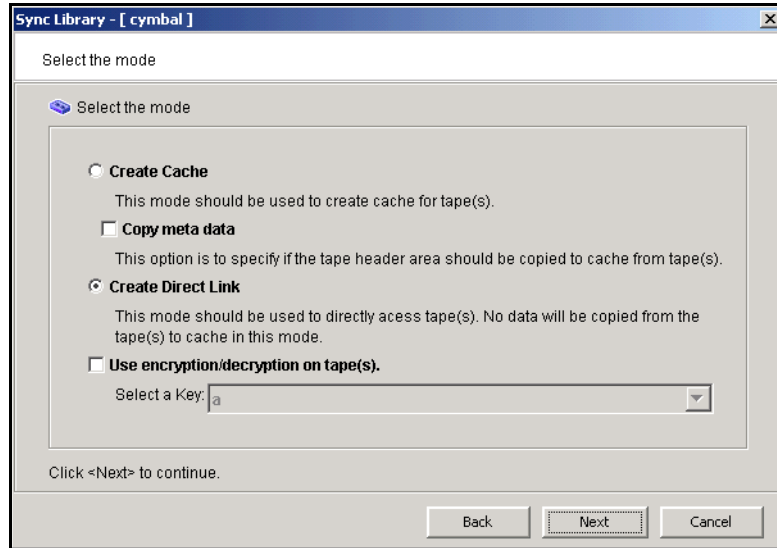
In a cached environment, tapes are always visible to the backup application regardless of whether the data is actually on disk or on a physical tape in the physical tape library. When it comes time to restore data, your backup application will seamlessly read the data from disk (if it is still there) or from the physical tape.

However, if the data is no longer on disk and the physical tape has been ejected from the physical tape library, you have to create a link to the physical tape. To do this:

1. Right-click on your virtual tape library and select *Sync Library*.
2. If you have multiple libraries, select the appropriate physical library.
3. Select the physical tape from which you need to restore data.



4. Select *Create Direct Link*.



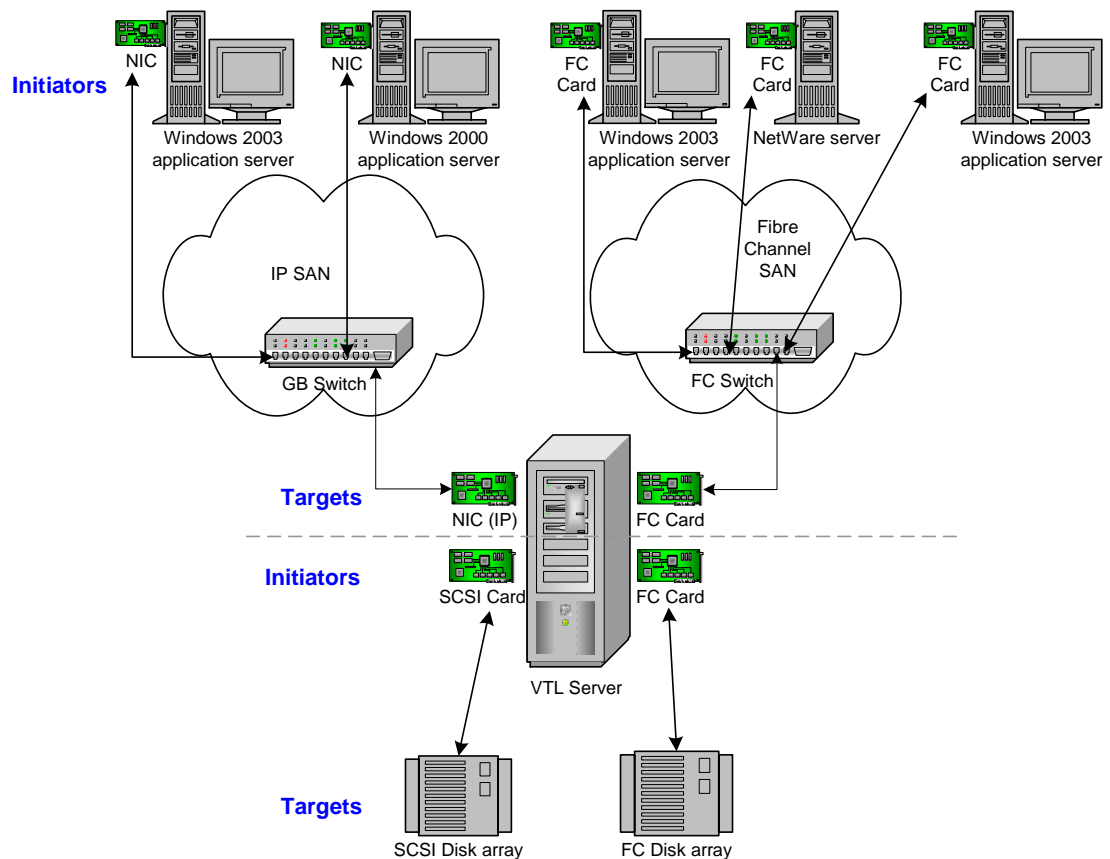
If the data was encrypted before being migrated, select the appropriate key to decrypt the data.

# Fibre Channel Target Mode

## Overview

Just as the VTL server supports different types of storage devices (such as SCSI, Fibre Channel, and iSCSI), the VTL server is protocol-independent and supports multiple outbound target protocols, including Fibre Channel Target Mode.

This chapter provides configuration information for Fibre Channel Target Mode as well as the associated Fibre Channel SAN equipment.



As you can see from the illustration above, an application server can be either an iSCSI client or a Fibre Channel client, but not both. Using separate cards and switches, you can have all types of VTL Clients (FC and iSCSI) on your network.

**Important Note:** Sun has configured the VTL for operation and no further configuration should be necessary. Any questions about changes to the settings should be given to Sun's VTL Backline Support before they are tried at the customer's location. Changing settings without a prior review can and has resulted in losses to connectivity and data.

---

## Installation and configuration overview

The installation and configuration of Fibre Channel Target Mode involves several steps. Where necessary, detailed information appears in subsequent sections.

1. [Configure Fibre Channel hardware on server.](#)
2. [Configure Fibre Channel hardware on clients.](#)
3. [Verify your hardware configuration.](#)
4. Enable Fibre Channel Target Mode.

This is done in the configuration wizard. If it was not, do the following:

- In the Console, highlight the VTL Server that has the FC HBAs.
- Right-click on the Server and select *Options --> Enable FC Target Mode*. An *Everyone\_FC* client will be created under *SAN Clients*. This is a generic client that you can assign to all (or some) of your tape libraries/drives. It allows any WWPN not already associated with a Fibre Channel client to have read/write non-exclusive access to any tape libraries/drives assigned to *Everyone\_FC*.

5. [Set QLogic ports to target mode.](#)

6. Add Fibre Channel clients.

You can add clients in the following two ways:

- Use the configuration wizard - If you have already configured your system, you can launch the wizard by right-clicking on the *VirtualTape Library System* object in the console and selecting *Configuration Wizard*.
- Right-click on the *SAN Clients* object and select *Add*.

7. (Optionally) [Associate World Wide Port Names with clients.](#)

8. For security purposes, assign specific virtual tape libraries/drives to specific clients.

Note: The *Everyone* generic client is not a supported option for SUN VTL. It may be used in a test environment but for security purposes it should not be used in a production environment.

9. Trigger a device rescan or reboot client machine to access new devices.

In order to see the new devices, after you have finished configuring your Fibre Channel Clients, you will need to trigger a device rescan or reboot the Client machine, depending upon the requirements of the operating system.

---

## Configure Fibre Channel hardware on server

VTL supports the use of QLogic HBAs for the VTL server.

### Ports

Your VTL appliance will be equipped with several Fibre Channel ports. Some of these ports will interface with storage arrays. Others will interface with physical tape libraries, while the remaining ports will interface with backup (media) servers.

The ports that connect to storage arrays are commonly known as *Initiator Ports*.

The ports that will interface with the backup servers' FC initiator ports will run in a different mode known as *Target Mode*.

The ports that are connected to physical tape libraries are known as *Library Connection Ports*.

You should NEVER use the same port to connect to both a disk array and a physical tape library - use a different initiator port for each purpose. In other words, the same FC port CANNOT be both an Initiator Port and a Library Connection Port.

### Zoning



Note: If a port is connected to a switch, we highly recommend the port be in at least one zone.

There are two types of zoning that can be configured on each switch, hard zoning (based on port #) and soft zoning (based on WWPNs).

Hard zoning is zoning using the port number of the switches. With hard zoning, if a zone has two ports (0 and 1) and port 0 goes down for some reason, you will need to remove the current zoning configuration, move the plug to another valid port, re-zone, and then enable the new zoning configuration.

Soft zoning uses the WWPN in the configuration. The WWPN remains the same in the zoning configuration regardless of the port location. If a port fails, you can simply move the cable from the failed port to another valid port without having to reconfigure the zoning.

VTL requires isolated zoning where one initiator is zoned to one target in order to minimize I/O interruptions by non-related FC activities, such as port login/out and resets.

For example, for the case of upstream (to client) zoning, if there are two client initiators and two VTL targets on the same FC fabric and if it is desirable for all four path combinations to be established, you should use four specific zones, one for each path (Client\_Init1/VTL\_Tgt1, Client\_Init1/VTL\_Tgt2, Client\_Init2/VTL\_Tgt1, and Client\_Init2/VTL\_Tgt2). You cannot create a single zone that includes all four ports. The four-zone method is cleaner because it does not allow the two client

---

initiators nor the two VTL target ports to see each other. This eliminates all of the potential issues such as initiators trying to log in to each other under certain conditions.

The same should be done for downstream (to storage) zoning. If there are two VTL initiators and two storage targets on the same fabric, there should be four zones (VTL\_Init1/Storage\_Tgt1, VTL\_Init1/Storage\_Tgt2, VTL\_Init2/Storage\_Tgt1, and VTL\_Init2/Storage\_Tgt2).

If hard zoning is used, it is necessary to create zones for each standby target, doubling the number of upstream zones. This extra set of zones is not necessary in the case of soft zoning because zones are defined by WWPN combinations. In a failover event, the standby ports assume the WWPNs of the target ports of the failed VTL server. Therefore, the single set of soft zones is still valid.

Additionally, make sure that storage devices to be used by VTL are not zoned to clients (backup servers). Ports on storage devices to be used by VTL should be zoned to VTL's initiator ports while the clients are zoned to VTL's target ports. Make sure that from the storage unit's management GUI (such as SANtricity and NaviSphere), the LUNs are re-assigned to VTL as the "host". VTL will virtualize these LUNS. VTL can then define virtual tapes out of these LUNS and further provision them to the clients.

Do not zone a FC switch that forces a VTL FC port to act as both an initiator port and a library connection port. Use a different initiator port for each device.

## Switches

For the best performance, if you are using 2 or 4 Gig switches, all of your cards should be 2 or 4 Gig cards. Examples of 2 Gig cards include the QLogic 2300 and Emulex LP952L. Examples of 4 Gig cards include the QLogic 24xx.

**Storage array** Connect an FC cable from a port on the storage array to an FC port on the FC switch.

If the storage array has active-active or active-passive controllers, the option is available to connect a second cable from the storage array to the FC switch or connect two FC cables from the VTL appliance to the FC switch to create redundant paths.

**Physical tape library** The physical tape library may already be attached to the FC switch before the deployment. In this case, only FC switch zoning requires modification and no re-cabling is required.

Connect an FC cable from a port on the physical tape library to an FC port on the FC switch. VTL currently supports one physical path to a tape library.

**Backup servers** Typically, backup servers are already connected to the FC switch before the deployment. In this case, only FC switch zoning requires modification. Connect an FC cable from each backup server to an FC port on the FC switch.



---

Configure a FC switch using soft zoning

The following are generic FC zoning steps applicable to any FC switch hardware. Refer to hardware or vendor documentation for specific zoning instructions for your FC switch.

1. Access the FC switch via its web interface and log in if necessary.
2. Access the Name Server Table.
3. Access the zoning configuration and log in if necessary.
4. Using previously recorded FC HBA information, look for the WWPNs for the adapters from the VTL appliance, storage array, and backup servers.
5. Create aliases for each WWPN.  
Note that some switches (i.e. McData) do not use aliasing.
6. Create zones for your configuration, for example:
  - Zone 1: VTL WWPN (initiator)->storage array WWPN (target)
  - Zone 2: VTL WWPN (initiator)->Tape Library WWPN (target)
  - Zone 3: VTL WWPN (target)->backup server WWPN (initiator)
7. Save the configuration.

Configure a FC switch using hard zoning

Follow the steps above but use the port number in place of the WWPN.

Configure a FC switch for failover

In order to for VTL's failover to function successfully, you must configure the FC zoning.

Hard zoning requirements:

- Do not put more than two ports in a hard zone.
- For each zone with a target port, you must create a matching zone using the same client host initiator port and the designated standby port from the secondary VTL appliance.

Soft zoning requirements:

- Do not put more than two WWPNs in a single zone.
- Matching zones for dedicated standby ports are not necessary with soft zoning, since each appropriate WWPN is spoofed when necessary for failover use.

---

## Persistent binding

Persistent binding is automatically enabled for all QLogic HBAs connected to storage device targets upon the discovery of the device (via a Console physical device rescan with the *Discover New Devices* option enabled). However, persistent binding will not be SET until the HBA is reloaded. You can reload HBAs by rebooting the VTL server.

Without persistent binding, there is a risk that the wrong storage controller port will be accessed when the VTL appliance is rebooted (or VTL HBA driver is reloaded).

## VSA

Some storage devices (such as EMC Symmetric storage controller and older HP storage) use VSA (Volume Set Addressing) mode. This addressing method is used primarily for addressing virtual buses, targets, and LUNs. If your storage device uses VSA, you must enable it through the console.

Incorrect use of VSA can lead to problems seeing the disks at the HBA level. If the HBA cannot see the disks, VTL is not able to access and manage them. This is true both ways: (1) the storage requires VSA, but it is not enabled and (2) the storage does not use VSA, but it is enabled.

To determine if the storage device that is being provisioned by VTL has VSA mode, use the storage's own management utility.

To enable VSA, right-click on *Physical Resources* or a specific adapter and select *Target Port Binding*. Click the *VSA* checkbox for the appropriate storage device targets.

Some clients, such as HP-UX clients, use VSA mode. In order for these clients to access VTL, you must enable VSA on the VTL's target ports (this is done when you enable Target Mode on an HBA port from the Console). Otherwise, for example, HP-UX (10, 11, 11i) Fibre Channel Clients using HP Tachyon Fibre Channel HBAs cannot detect more than eight LUNs (eight VTL virtual tape drives and robotic arm).

## QLogic HBAs

Target mode settings The table below lists the recommended settings (changes are indicated in bold) for QLogic HBA target mode. These values are set in the qla2x00fs.conf file and will override those set through the BIOS settings of the HBA.

For initiators, consult the best practice guideline from the storage vendor. If an initiator is to be used by multiple brands, the best practice is to select a setting that best satisfies all brands. If this is not possible, consult Sun technical support for advice, or separate the conflicting storage units to their own initiator connections.

Name	Default	Recommendation
frame_size	2 (2048byte)	2 (2048byte)
loop_reset_delay	0	0
adapter_hard_loop_id	0	<b>0</b>
connection_option	1 (point to point)	<b>1 (point to point)</b>
hard_loop_id	0	<b>0-124</b> Make sure that both primary target adapter and secondary standby adapter are set to the SAME value
fibre_channel_tape_support	0 (disable)	1 (enable)
data_rate	2 (auto)	<b>Based on the switch capability – 0 (1 Gig), 1 (2 Gig), 2 (auto), or 2 (4Gig)</b>
execution_throttle	255	255
LUNs_per_target	256	256
enable_lip_reset	1 (enable)	1 (enable)
enable_lip_full_login	1 (enable)	1 (enable)
enable_target_reset	1 (enable)	1 (enable)
login_retry_count	8	8
port_down_retry_count	8	8
link_down_timeout	45	45
extended_error_logging_flag	0 (no logging)	0 (no logging)
interrupt_delay_timer	0	0
iocb_allocation	512	512
enable_64bit_addressing	0 (disable)	0 (disable)
fibrechannelconfirm	0 (disable)	0 (disable)
class2service	0 (disable)	0 (disable)

Name	Default	Recommendation
acko	0 (disable)	0 (disable)
responsetimer	0 (disable)	0 (disable)
fastpost	0 (disable)	0 (disable)
driverloadadrisccode	1 (enable)	1 (enable)
q12xmaxqdepth	32	32 (configurable through the VTL Console)
max_srbs	4096	4096
q12xfailover	0	0
q12xlogintimeout	20 seconds	20 seconds
q12xretrycount	20	20
q12xsuspendcount	10	10
q12xdevflag	0	0
q12xplogiabsentdevice	0 (no PLOGI)	0 (no PLOGI)
busbusytimeout	60 seconds	60 seconds
displayconfig	1	1
retry_gnnft	10	10
recoverytime	10 seconds	10 seconds
fallbacktime	5 seconds	5 seconds
bind	0 (by Port Name)	0 (by Port Name)
qfull_retry_count	16	16
qfull_retry_delay	2	2
q12xloopupwait	10	10

---

## QLogic Multi-ID HBAs

With a Multi-ID HBA, each port can be both a target and an initiator (*dual mode*). When using a Multi-ID HBA, there are two WWPNs, the *base* port and the *alias*.



Important notes:

- Multi-ID driver - The Multi-ID driver is installed by default for the VTL 1202 and 3600 appliances. It is not installed for VTL1200 or 2600 appliances, nor does it exist as an option for the upgrades of VTL Plus 1.0 hardware running VTL Plus 2.0 software.
- You should not use the Multi-ID driver if you intend to directly connect a target port to a client host.
- With dual mode, clients will need to be zoned to the alias port (called *Target WWPN*). If they are zoned to the base port, clients will not see any devices.
- You will only see the alias port when that port is in target mode.
- You will only see the alias once all of the VTL services are started.
- If you are using the QLogic Multi-ID driver with loop-only mode, you will not be able to use a McData Director class switch. The standard point-to-point driver is required for this configuration.

### Multi-ID Driver Failover Configuration

When target mode is enable with MID, there are two WWPNs:

1. Monitor WWPN - used as "standby" failover port

The Monitor WWPN is the same as the base WWPN and just like the initiator wwpn use for standby.

Select the failover partner's Monitor WWPN as the primary server's standby target WWPN in the failover setup.

2. Target WWPN - used as primary port to SAN clients (backup apps)

Pick Target WWPN for SAN client configuration and switch zones.

Note: You will only see one WWPN if you do not enable the target mode.

---

## QLA2X00FS.CONF file

The *qla2x00fs.conf* file is used to adjust settings for FC adapters installed on the VTL appliance. Refer to 'QLogic HBAs' for recommended target settings.

1. Determine the HBA settings to change.
2. Back up the *qla2x00fs.conf* file:
3. Modify *qla2x00fs.conf* using the *vi* editor.
4. Save the *qla2x00fs.conf* file.
5. Update driver properties and reboot VTL:

```
update_drv -f qla2x00fs
reboot
```

You must reboot the VTL server for the changes in the *qla2x00fs.conf* file to take effect and to recognize the new settings.

**Link speed** In the *qla2x00fs.conf* file, the link speed is set to auto-negotiate by default for every FC port. You must manually update this and match the link speed with the switch speed.

```
# Fibre Channel Data Rate Option
# 0 = 1 gigabit/second
# 1 = 2 gigabit/second
# 2 = Auto-negotiate
# 3 = 4 gigabit/second
hba0-fc-data-rate=2;
```

It may be necessary to manually set the port switch speed on the FC switch as well.

If you are attaching a tape library or storage array directly to the VTL appliance, adjust the link speed for all FC ports (VTL and/or tape library). Check with your vendor to obtain any recommended FC HBA settings.

**Device identification** Typically, Solaris will assign its own device numbers, such as c1 and c2 (controller 1 and 2), etc. These controller numbers were assigned when Solaris first discovered a new adapter. However, the VTL appliance does not identify the same devices in the same way.

VTL will identify QLogic adapters as hba0, hba1, hba2, and so on in the *qla2x00fs.conf* file.

Settings for each individual FC port (for example, hba0 or hba1) can be modified in *qla2x00fs.conf*.

To identify which adapter belongs to which HBA in *qla2x00fs.conf*:

1. Run the following command:

For example:

---

```
ispdev | grep qla2x00fs
```

This command will output all QLogic adapters with the assigned adapter #, qla2x00fs instance #, device path, WWPN, mode, and other properties, if available.

```
adapter2 qla2x00fs0 /devices/pci@1d,0/pci1022,7450@1/pci1014,1a7@1/pci1077,102@4 210000e08b833490 initiator | |
adapter3 qla2x00fs1 /devices/pci@1d,0/pci1022,7450@1/pci1014,1a7@1/pci1077,102@4,1 210100e08ba33490 initiator | |
adapter4 qla2x00fs2 /devices/pci@1d,0/pci1022,7450@1/pci1014,1a7@1/pci1077,102@6 210200e08bc33490 initiator | |
adapter5 qla2x00fs3 /devices/pci@1d,0/pci1022,7450@1/pci1014,1a7@1/pci1077,102@6,1 210300e08be33490 initiator | |
```

For example, in the above example, adapter2 is mapped to qla2x00fs instance0, which is also referred to as hba0 in the *qla2x00fs.conf* file.

```
adapter2->qla2x00fs0(hba0)
adapter3->qla2x00fs1(hba1)
adapter4->qla2x00fs2(hba2)
adapter5->qla2x00fs3(hba3)
```

2. Run the following command to determine which physical port belongs to each adapter number in *qla2x00fs.conf*.

```
tail -f /var/adm/messages and unplug the FC port.
```

You will see a loop down message like the one below.

```
"Oct 1 14:54:38 SUN81sf029 qla2x00fs: [ID 376780 kern.notice]
QLA2x00fs(4): LOOP DOWN"
```

The 4 is the instance number in the above example.

Data rate 

1. Scroll down to the appropriate section.

2. Search for *data\_rate*.

It should look like this:

```
# Fibre Channel Data Rate Option
# 0 = 1 gigabit/second
# 1 = 2 gigabit/second
# 2 = Auto-negotiate
# 3 = 4 gigabit/second
hba0-fc-data-rate=2;
```

3. For the adapter to be configured (i.e., hba4), change the value:

```
hba4-fc-data-rate=1;
```

The hba0-fc-data-rate should be left untouched. It is the default setting for the rest of ports.

4. Repeat for each adapter to be configured.

---

## Configure Fibre Channel hardware on clients

Fabric topology (For all clients *except* Solaris SPARC clients) When setting up clients on a Fibre Channel network using a Fabric topology, we recommend that you set the topology that each HBA will use to log into your switch to *Point-to-Point Only*.

If you are using a QLogic 2200 HBA, the topology is set through the QLogic BIOS: Configure Settings --> Extended Firmware settings --> Connection Option: *Point-to-Point Only*



Note: We recommend hard coding the link speed of the HBA to be in line with the switch speed.

### *NetWare clients*

Built into the latest QLogic driver is the ability to handle VTL failover. HBA settings are configured through `nwconfig`. Do the following after installing the card:

1. Type `nwconfig`.
2. Go to *Driver Options* and select *Config disk* and *Storage device drivers*.
3. Select *Select an Additional Driver* and type the path for the updated driver (i.e `sys:\qllogic`).
4. Set the following parameters:
  - Scan All Luns = yes
  - FailBack Enabled = yes
  - Read configuration = yes
  - Requires configuration = no
  - Report all paths = yes
  - Use Portnames = no
  - Qualified Inquiry = no
  - Report Lun Zero = yes
  - GNFT SNS Query = no
  - Console Alerts = no



---

## HBA settings for Fibre Channel clients

This section provides recommended settings for clients that are connected to VTL.

For QLogic HBAs, you can modify the BIOS settings using the SANsurfer tool. For Emulex HBAs, using the miniport drivers is supported. We do not support FC port drivers.

For all HBAs that support persistent binding, persistent binding should be configured. Check with the HBA vendor for persistent binding procedures.

We recommend that you reload the driver (reboot) in order for changes to be made effective for most operating systems, such as Windows, Linux, and Solaris. It is not necessary to reboot AIX clients since there are no BIOS settings that need to be configured. For HP-UX, you will not be required to reboot unless you are using an Emulex HBA since you will need to recompile the kernel.

Below are charts for different types of HBAs for different types of clients. These settings apply for cluster and non-cluster environments unless specified.

### Windows 2000/2003

HBA Card Type	Setting
QLogic	Login Retry Count = 180 Port Down Retry Count = 251805 Link Down Count = 30 Enable Target Reset = True FrameSize = 2048 Execution Throttle = 255 LUNS per target = 64 Tape mode = Enable Queue depth = 32
Emulex	Node Timeout = 30 Link Timeout = 30 Reset FF = 1 (true)

LUNS per target

The *LUNS per target* should be set to 64. You can set this value to 256 because we use Report LUN upstream. However, this is dependent on your requirements and is based on the number of LUNs.

---

## HP-UX 10, 11, and 11i

HBA Card Type	Settings
Emulex	Node timeout = 30 Link timeout = 30 scsi timeout = 30 Port swapping not required
Tachyon	scsi timeout = 30

For Tachyon HBAs, you must use port swapping scripts for special switches, such as the Brocade 3900 / 12000 with firmware 4.1.2b. Cisco switches can detect the port change automatically so there is no need to use port swapping scripts with Cisco switches.

## AIX 4.3 and higher

HBA Card Type	Settings
IBM	Retry Timeout = 30
Emulex	Retry Timeout = 30
Cambex	Retry Timeout = 30

There are no BIOS or OS level changes that can be made for AIX.

## Linux – all versions

HBA Card Type	Settings
QLogic	Login Retry Count = 180 Port Down Retry Count = 180 Link Down Count = 30 Enable Target Reset = True FrameSize = 2048 Execution Throttle = 255 LUNS per target = 256 Tape mode = Enable Queue depth = 32
Emulex	Node Timeout = 30 Link Timeout = 30 Disk timeout value = 60

There are no OS level modifications to be made for a Linux client.

Solaris 7, 8, 9, and 10

HBA Card Type	Settings
QLogic	Login Retry Count = 8 Port Down Retry Count = 8 Link Down Count = 30 Enable Target Reset = True FrameSize = 2048 Throttle = 255 LUNS per target = 256 Tape mode = Enable Queue depth = 32
Emulex	Node Timeout = 30 Link Timeout = 30 Disk timeout value = 60

The changes indicated above should be changed in the \*.conf files for their respective HBAs.

NetWare – all versions

HBA Card Type	Settings
QLogic	Port Down Retry Count = 30 Link Down Retry = 30 /XRetry = 60 /XTimeout = 120 /PortDown = 120 Set Multi-Path Support = ON Link Down Retry= 30

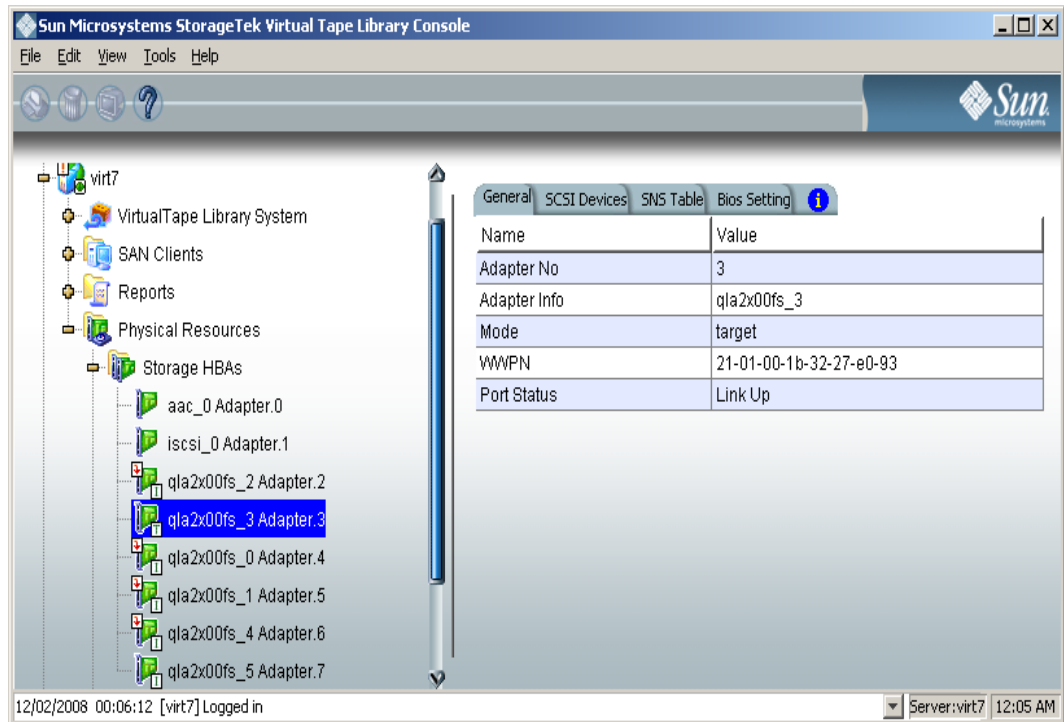
The settings indicated above should be modified at the ql23xx driver line in the startup.ncf file. The /ALLPATHS and /PORTNAMES options are required if an upper layer module is going to handle failover (it expects to see all paths).

The *Port Down Retry Count* and *Link Down Retry* is configurable in the BIOS whereas the */XRetry*, */XTimeout*, and */PortDown* values are configured by the driver. The *Port Down Retry Count* and the */Portdown* values combined will approximately be the total disk timeout.

## Verify your hardware configuration

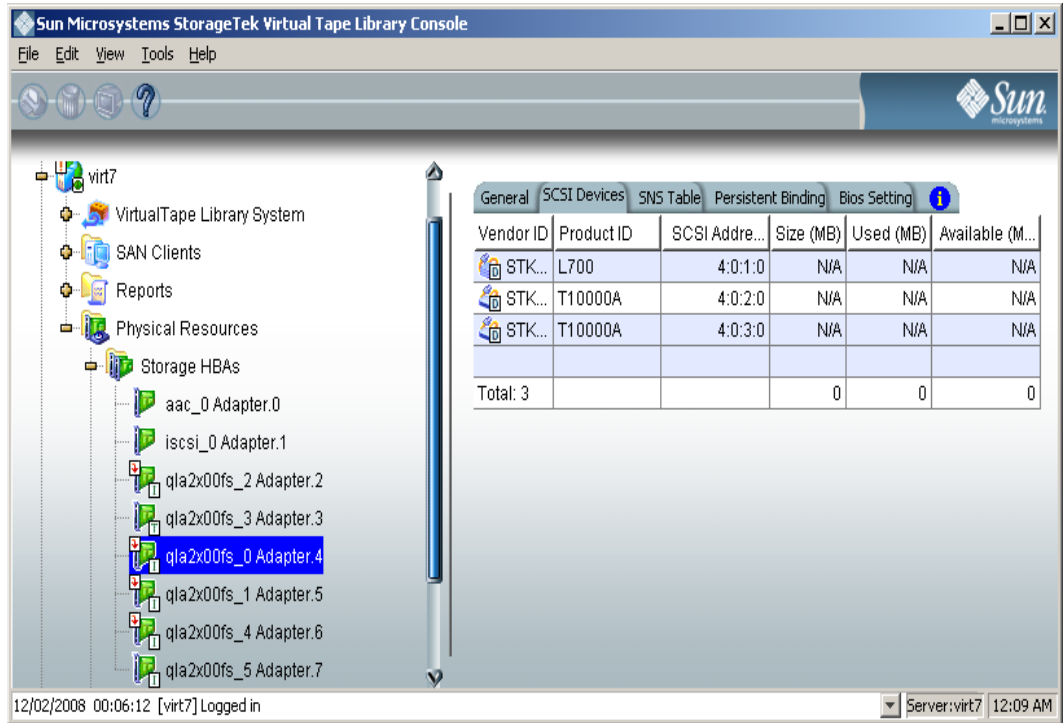
After all of your Fibre Channel hardware has been configured, you should verify that everything is set correctly. You can do this in the VTL console by highlighting a port under *Physical Resources*.

General tab The General tab displays information about the port, including mode (target or initiator), status, and WWPN

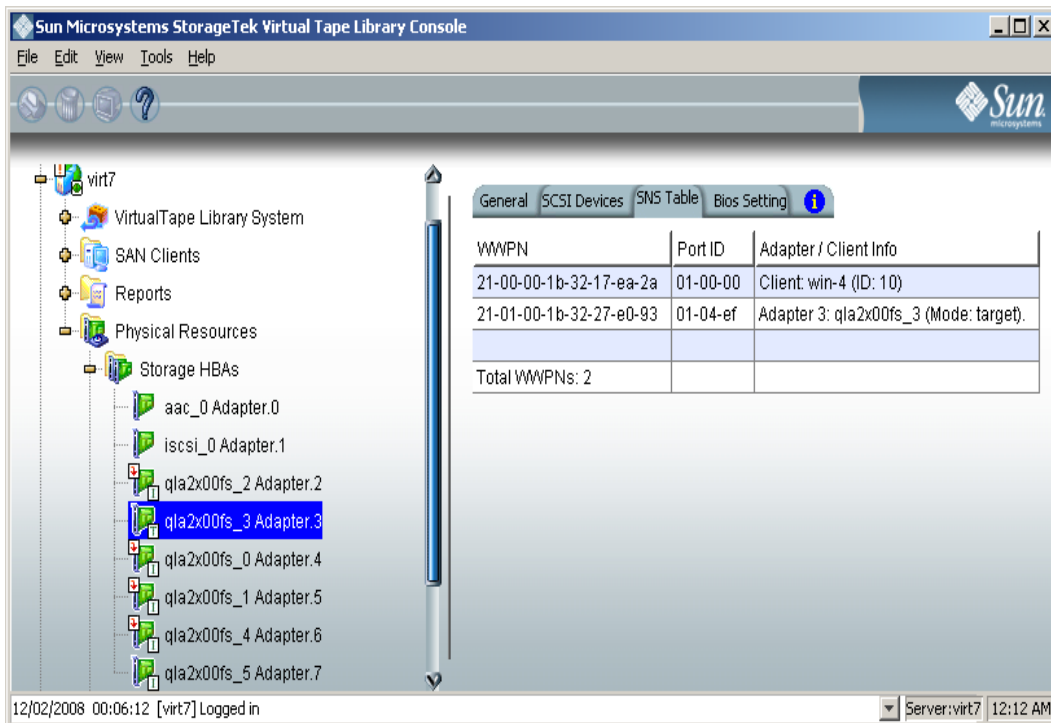


SCSI Devices  
tab

The SCSI Devices tab lists the SCSI storage devices attached to this adapter. If you expect to see a device that is not listed, right-click on the adapter and select *Rescan*

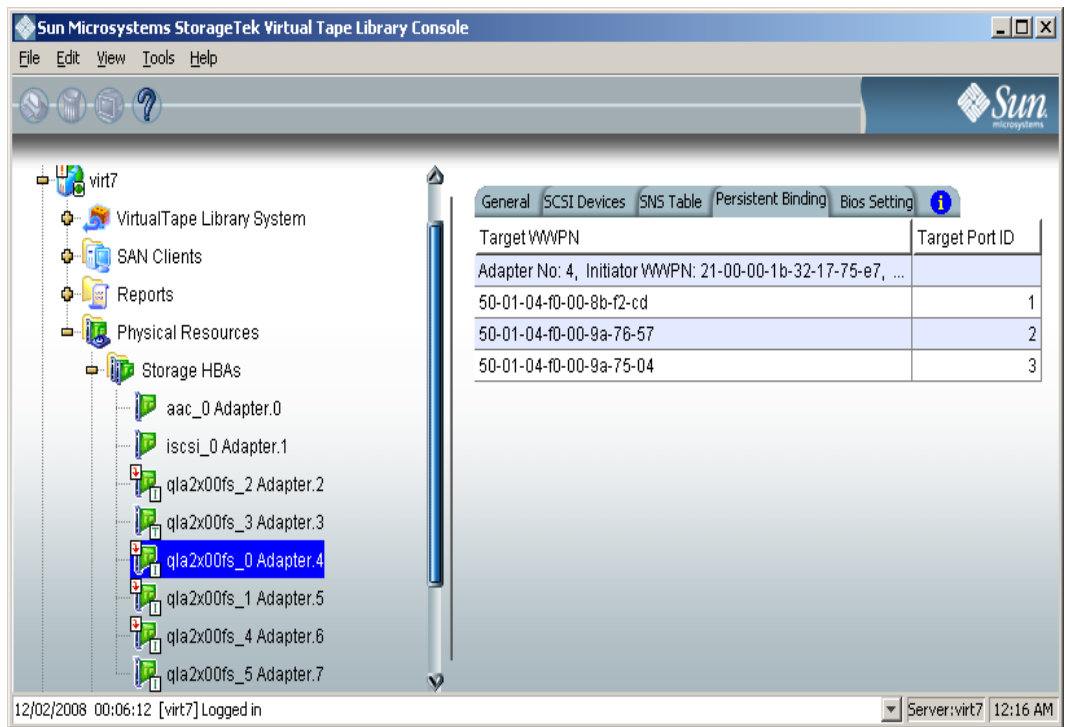


SNS Table tab The SNS Table tab lists the ports to which this adapter is zoned. VTL queries the switch for its Simple Name Server (SNS) database and displays this information. If you expect to see a WWPN that is not listed, right-click on the adapter and select *Refresh SNS*.

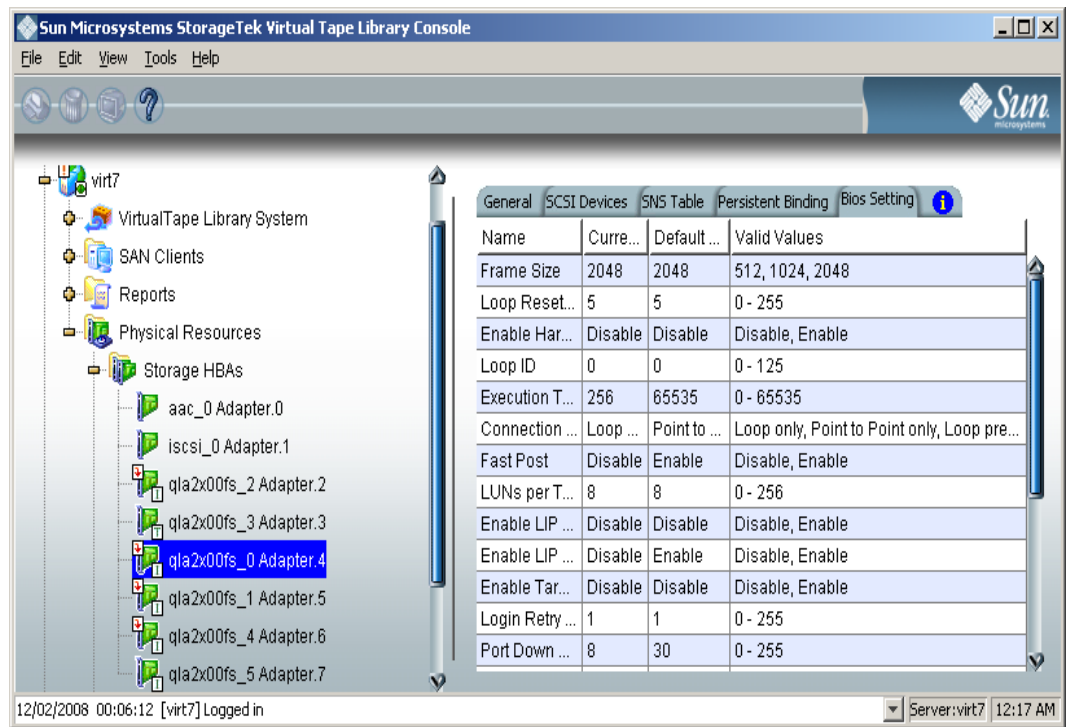


Persistent Binding tab

(Initiator ports only) The Persistent Binding tab lists all of the target ports to which this adapter is bound.



Bios Setting tab The Bios Setting tab lists all of the HBA settings for this adapter so that you can confirm what is set.





---

## Set QLogic ports to target mode

### *Single port QLogic HBAs*

By default, all QLogic point-to-point ports are set to initiator mode, which means they will initiate requests rather than receive them. Determine which ports you want to use in target mode and set them to become target ports so that they can receive requests from your Fibre Channel Clients.

For VTL Failover, you should have at least three Fibre Channel cards in initiator mode, one of which is attached to your storage device. (If your storage is SCSI, you do not need a third card.)

You need to switch one of those initiators into target mode so your clients will be able to see the VTL Server. You will then need to select the equivalent adapter on the secondary server and switch it to target mode.



Note: If a port is in initiator mode and has devices attached to it, that port cannot be set for target mode.

To set a port:

1. In the Console, expand *Physical Resources*.
2. Right-click on a HBA and select *Options --> Enable Target Mode*.  
You will get a *Loop Up* message on your VTL Server if the port has successfully been placed in target mode.
3. When done, make a note of all of your WWPNs.

It may be convenient for you to highlight your server and take a screenshot of the Console.

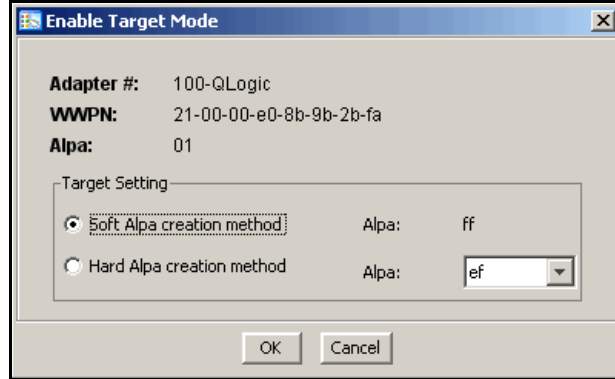
### *Multi port QLogic HBAs*

With a multi-ID HBA, each port can be both a target and an initiator. To use target mode, you must enable target mode on a port.

To set target mode:

1. In the Console, expand *Physical Resources*.

2. Right-click on a multi-ID HBA and select *Options --> Enable Target Mode*.



Note: If you want to spoof a multi-ID WWPN, enter the spoofed target WWPN to replace the default *Target WWPN*.

All targets must use either the soft or hard Alpa (Arbitrated Loop Physical Address) creation method. You cannot mix and match.

*Soft Alpa creation method* - HBA firmware generates Alpa addresses.

*Hard Alpa creation method* - You have to specify Alpa addresses.

3. Click *OK* to enable.

Afterwards, you will see two WWPNs listed for the port. The first is the base WWPN and the second is the Target WWPN (also known as the alias port). Clients need to be zoned to this port in order to see devices.

## Associate World Wide Port Names with clients

Similar to an IP address, the WWPN uniquely identifies a port in a Fibre Channel environment. Unlike an IP address, the WWPN is vendor assigned and is hardcoded and embedded.

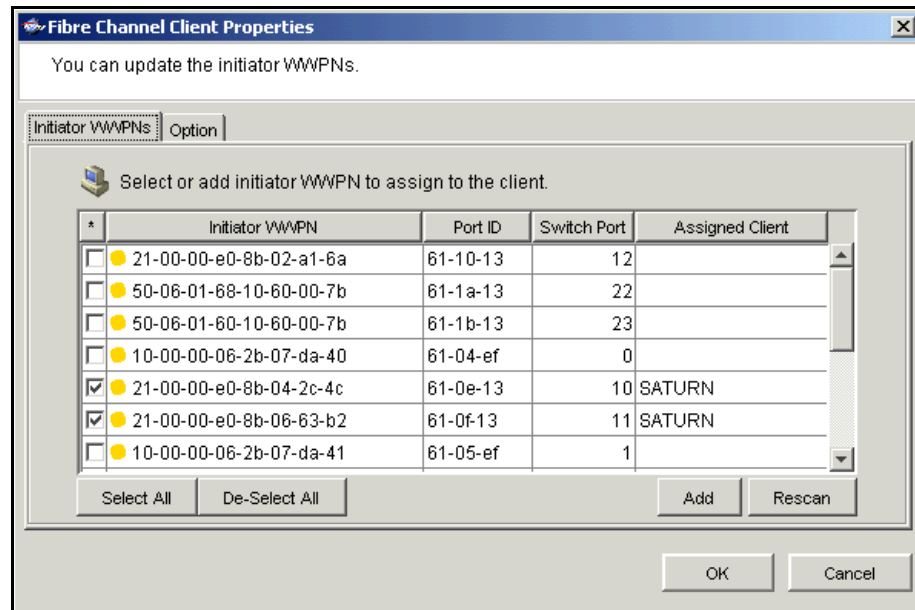
Depending upon whether or not you are using a switched Fibre Channel environment, determining the WWPN for each port *may* be difficult.

- If you are using a switched Fibre Channel environment, VTL will query the switch for its Simple Name Server (SNS) database and will display a list of all available WWPNs. You will still have to identify which WWPN is associated with each machine.
  - If you are not using a switched Fibre Channel environment, you can manually determine the WWPN for each of your ports. There are different ways to determine it, depending upon the hardware vendor. You may be able to get the WWPN from the BIOS during bootup or you may have to read it from the physical card. Check with your hardware vendor for their preferred method.
4. For security purposes, assign specific WWPNs to specific clients.

Note: The *Everyone* generic client is not a supported option for SUN VTL. It may be used in a test environment but for security purposes it should not be used in a production environment.

Do the following for each client for which you want to assign specific virtual devices:

1. Highlight the Fibre Channel Client in the Console.
2. Right-click on the Client and select *Properties*.



3. Select the Initiator WWPN(s) belonging to your client.

Here are some methods to determine the WWPN of your clients:

---

- Most Fibre Channel switches allow administration of the switch through an Ethernet port. These administration applications have utilities to reveal or allow you to change the following: Configuration of each port on the switch, zoning configurations, the WWPNs of connected Fibre Channel cards, and the current status of each connection. You can use this utility to view the WWPN of each Client connected to the switch.

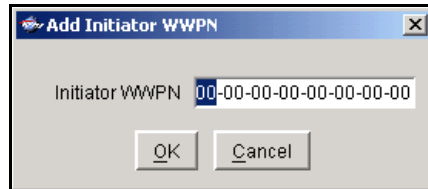
- When starting up your Client, there is usually a point at which you can access the BIOS of your Fibre Channel card. The WWPN can be found there.

- The first time a new Client connects to the VTL Server, the following message appears on the server screen:

FSQLtgt: New Client WWPN Found: 21 00 00 e0 8b 43 23 52

4. If necessary, click *Add* to add WWPNs for the client.

You will see the following dialog if there are no WWPNs in the server's list. This could occur because the client machines were not turned on or because all WWPNs were previously associated with clients.



# *iSCSI Clients*

---

## Overview

Just as the VTL server supports different types of storage devices (such as SCSI, Fibre Channel, and iSCSI), the VTL server is protocol-independent and supports multiple outbound target protocols, including iSCSI Target Mode.

iSCSI builds on top of the regular SCSI standard by using the IP network as the connection link between various entities involved in a configuration. iSCSI inherits many of the basic concepts of SCSI. For example, just like SCSI, the entity that makes requests is called an *initiator*, while the entity that responds to requests is called a *target*. Only an initiator can make requests to a target; not the other way around. Each entity involved, initiator or target, is uniquely identified.

By default, when a client machine is added as an iSCSI client of a VTL server, it becomes an iSCSI initiator.

The initiator name is important because it is the main identity of an iSCSI initiator.

## *Supported platforms*

iSCSI target mode is supported for the following platforms:

- [Windows](#)
- [Linux](#)

---

# Windows configuration

## Requirements

- A VTL server with an Ethernet adapter installed.
- A Windows client machine.
- You must install an iSCSI software initiator on each of your client machines. iSCSI initiator software/hardware is available from many sources and needs to be installed and configured on all clients that will access shared storage. For Windows hosts, you can download from Microsoft's website: <http://www.microsoft.com/windowsserversystem/storage/iscsi.msp>

## Enable iSCSI

In order to add a client using the iSCSI protocol, you must enable iSCSI for your VTL server.

In the VTL Console, right-click on your VTL server, select *Options --> Enable iSCSI*.

As soon as iSCSI is enabled, a new SAN client called *Everyone\_iSCSI* is automatically created on your VTL server. This is a special SAN client that does not correspond to any specific client machine. Using this client, you can create iSCSI targets that are accessible by any iSCSI client that connects to the VTL server. While such a publicly available target is convenient, it should be avoided, or at least configured with the proper read/write access, so that there will be no data corruption if two or more clients use the *Everyone\_iSCSI* client simultaneously.

Before an iSCSI client can be served by a VTL server, the two entities need to mutually recognize each other. The following sections take you through this process.

---

## Register client initiators with your VTL server

This enables the VTL server to see the available initiators. The following steps are for the Microsoft iSCSI Initiator. If you are using a different iSCSI initiator, refer to the documentation provided by the vendor.

You can also manually add your initiators through the *Add Client wizard* in the VTL Console.

1. Run *Microsoft iSCSI Initiator* on the Windows client machine.

You can find the program in the Control Panel or on your desktop (if you are the user that installed it).

2. Click *Add* on the *Target Portals* tab and enter the VTL server's IP address or name (if resolvable).

Use the default socket.

3. Click *Advanced* and go to the *General* tab.

In the *CHAP logon information* section, you can see the iSCSI initiator name of the client machine automatically filled in as the user name. Note that it is possible to change the initiator name of the machine by going to the *Initiator Settings* tab. However, it should be avoided because the default name is the one most appropriate according to the iSCSI standard as well as common practices. Altering it can possibly introduce unnecessary complications.

If the client machine is a mobile client, select *CHAP logon information* and replace the initiator name with a user name that belongs to one of the VTL server's mobile clients.

It can still obtain iSCSI targets by authenticating as a mobile client. In this case, in *Target secret*, enter the corresponding password. Then, click *OK* to finish adding the target portal.



Note: If the client machine is *not* a mobile client, do not select *CHAP logon information*.

4. Click *OK* to add the client.

When you click *OK*, any iSCSI target assigned to the client will appear on the *Available Targets* tab. However, since no actual iSCSI target has been assigned to the VTL server's iSCSI clients yet, the *Available Targets* tab will currently be blank.

---

## Add your iSCSI client

1. Right-click on *SAN Clients* and select *Add*.

2. Select *iSCSI* and determine if the client is a mobile client.

Stationary iSCSI clients corresponds to specific iSCSI client initiators, and consequently, the client machine that owns the specific initiator names. Only a client machine with a correct initiator name can connect to the VTL server to access the resources assigned to this stationary client.

A *mobile* client is simply a username and password that a user can use to authenticate to the VTL server from any iSCSI client machine. Note that when you right-click on a mobile client in the VTL Console, the *Properties* option is grayed out because the properties, such as the list of assigned iSCSI initiator names, do not apply to mobile clients. If you want to change the username or password for a mobile client, you must delete the current one and then recreate it with the desired username and password.

3. Determine how the client should be named.

You can create the name from the initiator name or enter a custom name.

4. Select the initiator that this client uses.

If the initiator does not appear, you can manually add it.

5. Add/select users who can authenticate for this client.

Click *Add* to add users. You will have to enter a name and password for each.

For unauthenticated access, select *Allow Unauthenticated Access*. With unauthenticated access, the VTL server will recognize the client as long as it has an authorized initiator name. With authenticated access, an additional check is added that requires the user to type in a username and password. More than one username/password pair can be assigned to the client, but they will only be useful when coming from the machine with an authorized initiator name.

6. Confirm all information and click *Finish*.



---

## Create targets for the iSCSI client to log onto

1. In the VTL Console, create at least one virtual iSCSI device (i.e. a virtual tape library) that can be used for iSCSI clients but do not assign it/them to the iSCSI clients until a target is created.
2. Right-click on an iSCSI client and select *Create Target*.
3. Enter a new target name for the client or accept the default.
4. Select the IP address of the VTL server.
5. Use the default starting LUN.  
LUN IDs must start with zero.  
Once the iSCSI target is created for a client, LUNs can be assigned under the target using available virtual iSCSI devices.
6. Confirm all information and click *Finish*.
7. Select *Yes* to assign a resource to the new target.
8. Select the virtual iSCSI device(s) to be assigned to the client.  
You can only assign a device to a client once even if the client has multiple targets. You cannot assign the same device to the same client more than once.
9. If needed, change the LUN for the resource.
10. Confirm all information and click *Finish*.

---

## Log the client onto the target

The following steps are for the Microsoft iSCSI Initiator. If you are using a different iSCSI initiator, refer to the documentation provider by the vendor.

1. To see the iSCSI targets from the client machine, run *Microsoft iSCSI Initiator* again.
2. Since the VTL server is already added as a target portal, go to the *Available Targets* tab and click *Refresh* to get the latest status.  
Assigned iSCSI targets should now appear.
3. Click *Log On* and select *Automatically restore this connection when the system reboots* if it is desirable to have a persistent target.
4. Click *Advanced* and select *CHAP logon information*.

If the iSCSI target is assigned to a mobile client from the VTL server, enter the authentication credential for that mobile client.

If the target is assigned to this particular client machine, and *authenticated access* is used, enter an assigned username and password for this client. This should be the same username/password that you entered when you added the client in the VTL Console.

Once logged on, the status of an iSCSI target should change to *Connected*.

The *Active Sessions* tab lists all of the iSCSI targets that are already in *Connected* status. It also allows the client machine to log off from each iSCSI target.

## Disable iSCSI

To disable iSCSI for a VTL server, right-click on the server node in the VTL Console, and select *Options --> Disable iSCSI*.

Note that before disabling iSCSI, all iSCSI initiators and targets for this VTL server must be removed.

---

# Linux client configuration

## Prepare the iSCSI initiator

You must install and configure an iSCSI software initiator on each of your Linux client machines.

1. Download the latest production iSCSI initiator from the following website: <http://sourceforge.net/projects/linux-iscsi/>

2. Extract the files from the .gz file that you downloaded by typing:

```
tar xfvz filename
```

For example: `tar xfvz linux-iscsi-3.4.3.gz`

3. Compile the iSCSI initiator.

To do this, go to the newly created directory (such as `linux-iscsi-3.4.3`) and type the following commands:

```
make clean
make
make install
```

4. Edit the `/etc/iscsi.conf` file.

If you are **not using CHAP**, add the following line to the end of the file:

```
DiscoveryAddress=IP address of VTL server
```

For example: `DiscoveryAddress=192.10.10.1`

If you are **using CHAP**, add the following lines to the end of the file:

```
DiscoveryAddress=IP address of VTL server
OutgoingUsername=CHAP username
OutgoingPassword=CHAP password
```

You must make a note of the CHAP username and password because you will have to enter it in the VTL Console.

5. Start the initiator by typing:

```
/etc/init.d/iscsi start
```

## Add your iSCSI client

1. In the VTL Console, right-click on *SAN Clients* and select *Add*.
2. Enter a name for the client.
3. Click *Find* to locate the client machine.

The IP address of the machine with the specified host name will be automatically filled in if the name is resolvable.

- 
4. Select *iSCSI* and determine if the client is a mobile client.

Stationary iSCSI clients corresponds to specific iSCSI client initiators, and consequently, the client machine that owns the specific initiator names. Only a client machine with a correct initiator name can connect to the VTL server to access the resources assigned to this stationary client.

A *mobile* client is simply a username and password that a user can use to authenticate to the VTL server from any iSCSI client machine. Note that when you right-click on a mobile client in the VTL Console, the *Properties* option is grayed out because the properties, such as the list of assigned iSCSI initiator names, do not apply to mobile clients.

5. Select the initiator that this client uses.

If the initiator does not appear, you can manually add it.

6. Enter/select users who can authenticate for this client.

Click *Add* to add users. You will have to enter a name and password for each.

For unauthenticated access, select *Allow Unauthenticated Access*. With unauthenticated access, the VTL server will recognize the client as long as it has an authorized initiator name. With authenticated access, an additional check is added that requires the user to type in a username and password. More than one username/password pair can be assigned to the client, but they will only be useful when coming from the machine with an authorized initiator name.

7. Confirm all information and click *Finish*.

## Create targets for the iSCSI client to log onto

1. In the VTL Console, create at least one virtual iSCSI device (i.e. a virtual tape library) that can be used for iSCSI clients but do not assign them to the iSCSI clients until a target is created.

2. Right-click on an iSCSI client and select *Create Target*.

3. Enter a new target name for the client or accept the default.

4. Select the IP address of the VTL server.

5. Select the iSCSI device(s) to be assigned to the client.

6. Use the default starting LUN.

LUN IDs must start with zero.

Once the iSCSI target is created for a client, LUNs can be assigned under the target using available iSCSI devices.

7. Confirm all information and click *Finish*.

---

## Log the client onto the target

On the client machine, type the following command to log the client onto the target:

```
/etc/init.d/iscsi reload
```

Afterwards, you can display a list of all the disks that this client can access (including the target) by typing:

```
cat /proc/scsi/scsi
```

# NDMP Backup Support

---

## Overview

The *NDMP Backup Support* option allows certified backup applications and industry standard NAS devices (i.e. NetApp filers) to perform backup and restore using the NDMP protocol over an IP network.

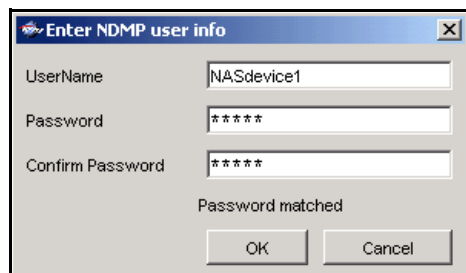
With NDMP Backup Support, the VTL appliance acts as an NDMP Tape Service, centralizing management by eliminating locally attached tape devices from each NAS device. When a backup occurs, data is moved from the NDMP Data Service device directly to the virtual library.

- ⓘ Note: This option is not needed when presenting a virtual tape library over FC to a NDMP filer as a replacement for a physical library.

## Configure NDMP Backup Support

To configure NDMP Backup:

1. Right-click on your VTL server and select *Options --> NDMP --> Enable NDMP*.
2. Enter the username and password the backup server will use to talk to NDMP.

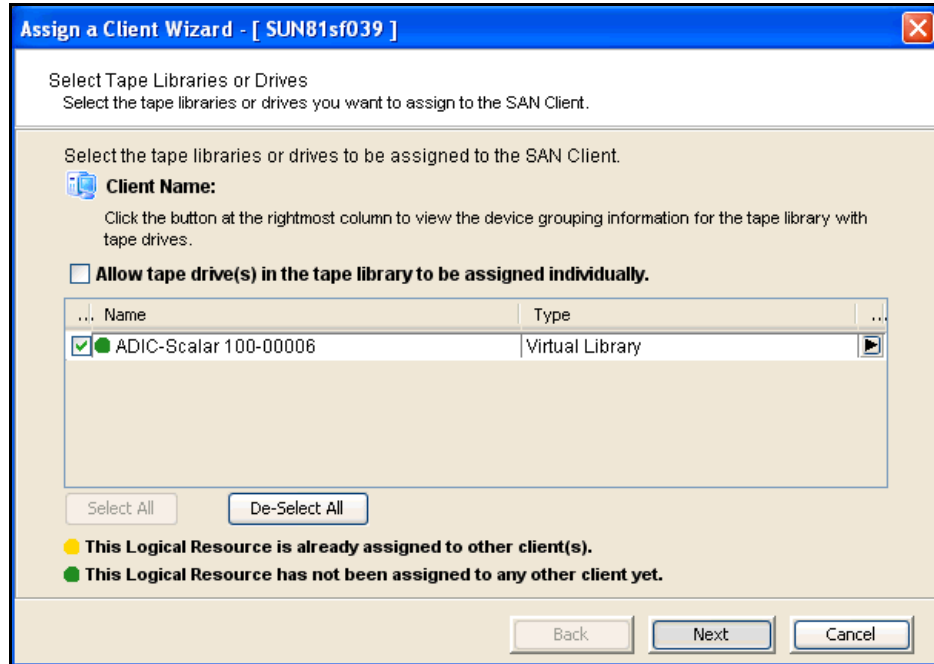


The screenshot shows a dialog box titled "Enter NDMP user info". It contains three text input fields: "UserName" with the text "NASdevice1", "Password" with "\*\*\*\*\*", and "Confirm Password" with "\*\*\*\*\*". Below these fields, the text "Password matched" is displayed. At the bottom of the dialog are two buttons: "OK" and "Cancel".

You must enter the same username/password into the NDMP module in your backup application.

3. Right-click on *HostedBackupClient* and select *Assign* to assign virtual libraries to this client.

4. Select the virtual libraries or drives that this client will use.



*HostedBackupClient* can have any number of virtual libraries assigned to it. Conversely, libraries assigned to the *HostedBackupClient* can also be assigned to other clients.

5. Confirm all information and click *Finish*.

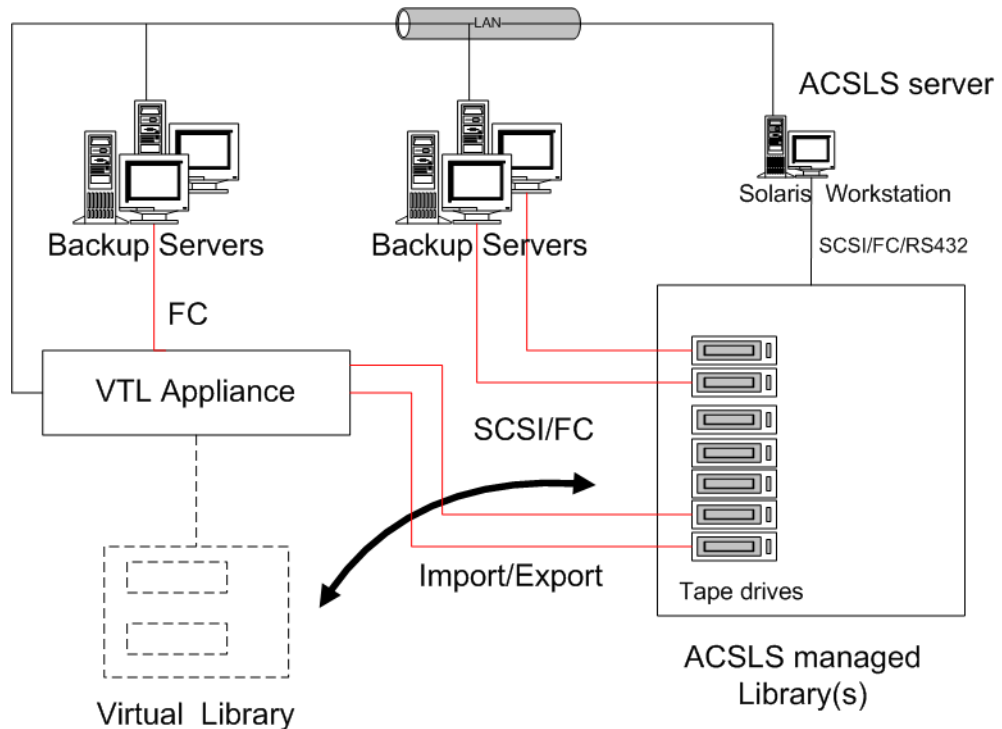
The backup application will now see the devices as local devices. If you have a physical library attached to the VTL server, you will be able to see it from the backup application.

# ACSL S and Library Station Configuration

## Overview

ACSL S Manager™ and Library Station software manages heterogeneous StorageTek tape libraries.

The ACSLS/Library Station option works with ACSLS/Library Station-managed tape libraries, allowing the system to share ACSLS/Library Station-managed libraries among the VTL server and your backup servers. This makes it possible to import data from physical tapes and export data on virtual tapes to physical tapes.





---

## Hardware configuration

1. Physically connect the tape drives that will be assigned to the VTL appliance.



Note: Physical tape drives cannot be shared with VTL appliances or other applications.

2. (ACSLs only) Create at least one storage pool on the ACSLS server for VTL and assign tapes to it.

If you have already created a pool, you can use that one.

3. Make a note of the following:

- ACS IDs, LSM IDs, Panel IDs, and Device IDs of the libraries that hold the tape drives connected to VTL. You can run the `cmd.proc` utility on your ACSL server to determine the IDs. For Library Station users, check with your Library Station administrator to determine the IDs.
- IP address of the ACSLS/Library Station server.
- (ACSLs only) IDs of the storage pools to be assigned to the VTL appliance.

4. Make sure that the VTL server and the ACSLS/Library Station server can communicate with each other.

## Configure VTL to work with ACSLS

The following instructions give you an overview of the steps you must follow to configure your ACSLS/Library Station option. Refer to the appropriate sections in this User Guide for more detailed information.

1. Launch the VTL console and connect to the VTL appliance.
2. Right-click on your VTL server and select *System Maintenance --> Network Configuration* to make sure DNS is configured properly.

Enter the *Domain Name*, select *Append suffix to DNS lookup* and enter the DNS server IP address.

3. Right-click on the *Physical Tape Libraries* object and select *Add ACSLS/Library Station*.

**Add ACSLS Library/Library Station**

Specify one ACSLS library or Library Station to add into the VTL system.

Library Station

IP Address of ACSLS:

ACS ID:

Pool ID:

OK Cancel

- 
4. Enter the IP address of the ACSLS/Library Station server; the ACS ID and the Pool ID of the ACSLS/Library Station library.

Once completed, the server automatically does an inventory to obtain a list of physical tapes.

5. Assign your physical tape drives to your ACSLS/Library Station tape library.

You will have to enter the *Drive ID* for each. The *Drive ID* is comprised of the drive's ACS ID, LSM ID, Panel ID, and Device ID in the format n,n,n,n

You can run the `cmd.proc` utility on your ACSL server to determine the IDs. For Library Station users, check with your Library Station administrator to determine the IDs. You may want to supply the administrator with the drive's SCSI address to help him determine the IDs.

## Add/remove tapes

Whenever you add or remove tapes from an ACSLS/Library Station pool, you must inventory the tapes through the VTL Console (right-click on the physical library and select *Inventory*).

# Email Alerts

VTL includes a unique customer support utility that proactively identifies and diagnoses potential system or component failures and automatically notifies system administrators via email.

Using pre-configured scripts (called *triggers*), Email Alerts monitors a set of pre-defined, critical system components (memory, disk, etc.). With its open architecture, administrators can easily register new elements to be monitored by these scripts.

When an error is triggered, Email Alerts generates an email and sends it to a system administrator.

With Email Alerts, system administrators are able to take corrective measures within the shortest amount of time, ensuring optimum service uptime and IT efficiency.

## Configure Email Alerts

1. In the Console, right-click on your VTL server and select *Options --> Enable Email Alerts*.
2. Enter general information for your Email Alerts configuration.

Configure Email Alerts Wizard

Set Email Alerts General Properties

Email Alerts General Configuration

SMTP Server: localhost SMTP Port: 25

SMTP Server supports authentication

SMTP User Name: [ ] SMTP Password: [ ] Retype Password: [ ]

From: root@xyz.com

To: support@xyz.com

CC: [ ]

Subject: Email Alerts Automatic Report

Interval: 1 day 0 hour 0 minute

Note: Interval indicates how frequently the Email Alerts triggers and the System Log will be checked.

Click <Next> to continue. [Test]

[Back] [Next] [Cancel]

**SMTP Server** - Specify the mail server that Email Alerts should use to send out notification emails.

**SMTP Port** - Specify the mail server port that Email Alerts should use.

*SMTP Server supports authentication* - Indicate if the SMTP server supports authentication.

*SMTP Username/Password* - Specify the user account that will be used by Email Alerts to log into the mail server.

*From* - Specify the email account that will be used in the “From” field of emails sent by Email Alerts.

*To* - Specify the email address of the account that will receive emails from Email Alerts. This will be used in the “To” field of emails sent by Email Alerts.

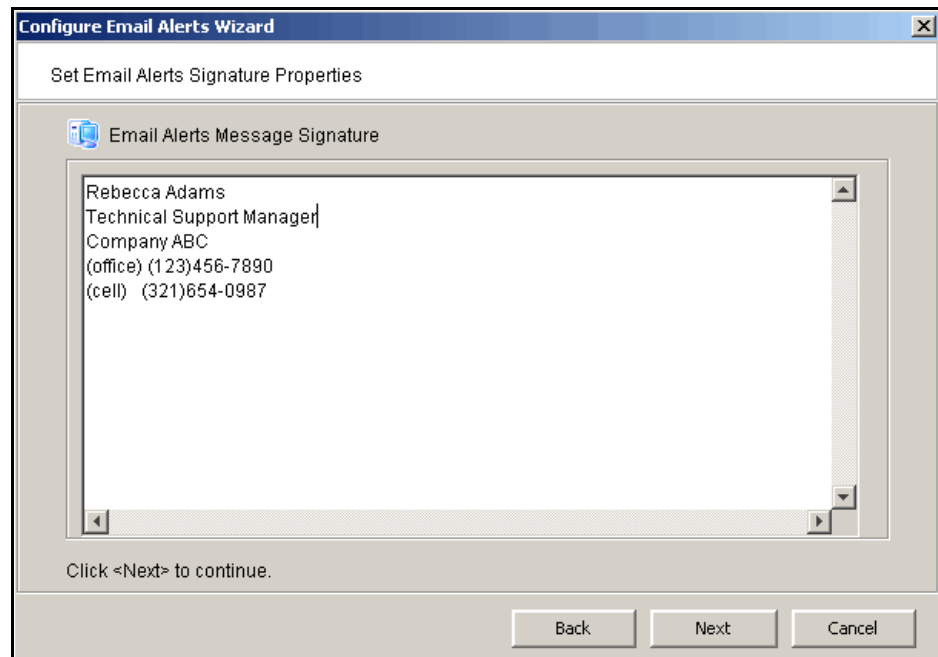
*CC* - Specify any other email accounts that should receive emails from Email Alerts.

*Subject* - Specify the text that should appear on the subject line.

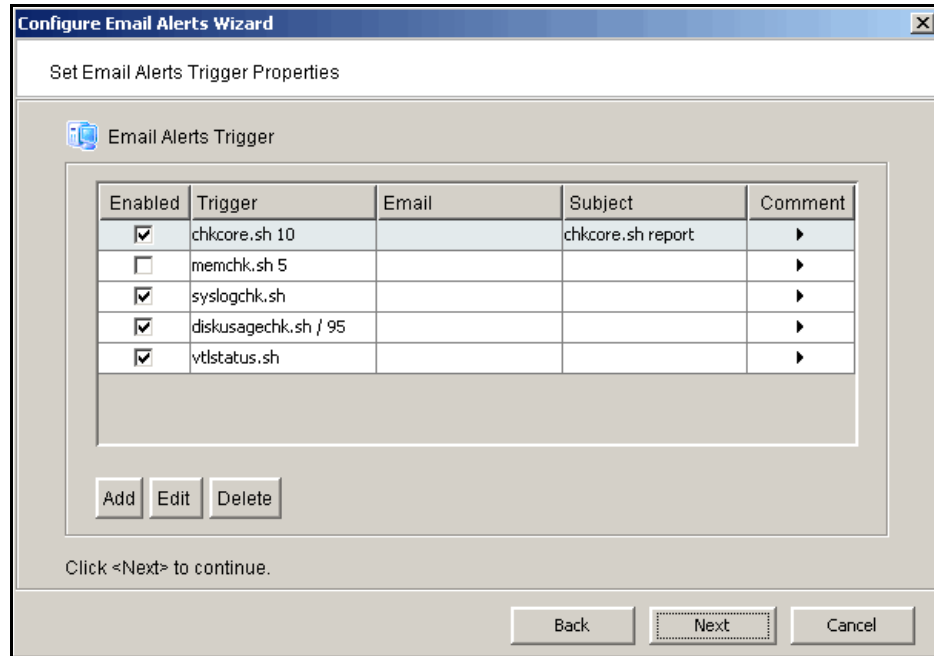
*Interval* - Specify how frequently the Email Alerts triggers and the System Log should be checked.

*Test* - Click the *Test* button to send a test Email Alerts email.

3. On the *Signature* dialog, enter the contact information that should appear in each Email Alerts email.



- On the *Trigger* dialog, set the triggers that will cause Email Alerts to send an email.



Triggers are the scripts/programs that perform various types of error checking. By default, scripts/programs are included that check for low system memory, low disk space, and relevant new entries in the system log.

The following are the default scripts that are provided:

**chkcore.sh 10** (Core file check) - This script checks to see if a new core file has been created by the operating system in the bin directory of VTL. If a core file is found, Email Alerts compresses it, deletes the original, and sends an email report but does not send the compressed core file (which can still be large). If there are more than 10 (variable) compressed core files, they will all be deleted.

**memchk.sh 5** (Memory check) - This script takes in a percentage as the parameter and checks whether the available system memory is below this percentage. If yes, Email Alerts sends an email report.

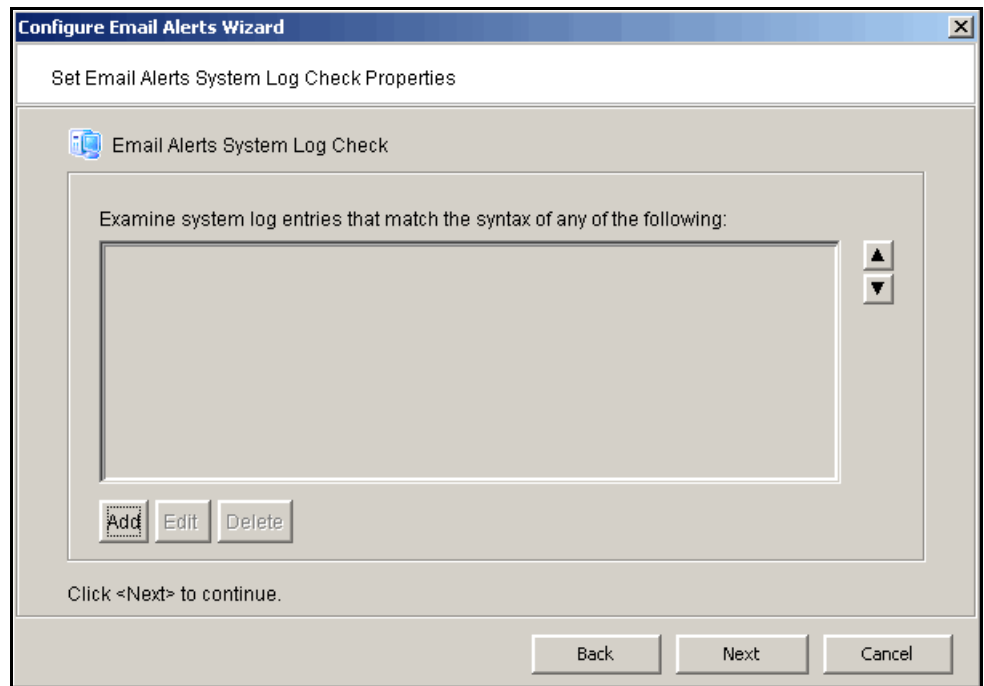
**syslogchk.sh** (System log check) - This script looks at the system log for specific entries that it needs to report on. This is determined by information specified on the *System Log Check* dialog. If matches are found, Email Alerts sends an email report.

**diskusagechk.sh / 95** (Disk usage check) - This script checks the disk space usage of the root file system. If the current percentage is over the specified percentage (default is 95), Email Alerts sends an email report. You can add multiple diskusagechk.sh triggers for different mount points (for example, /home could be used in another trigger).

**vtlstatus.sh** (VTL status check) - This script calls “vtl status” and checks if any module of VTL has stopped. If so, Email Alerts sends an email report.

If you need to modify an existing script or create a new script/program, refer to [‘Script/program trigger information’](#) for more information.

5. On the *System Log Check* dialog, indicate the terms that should be tracked in the system log by Email Alerts.



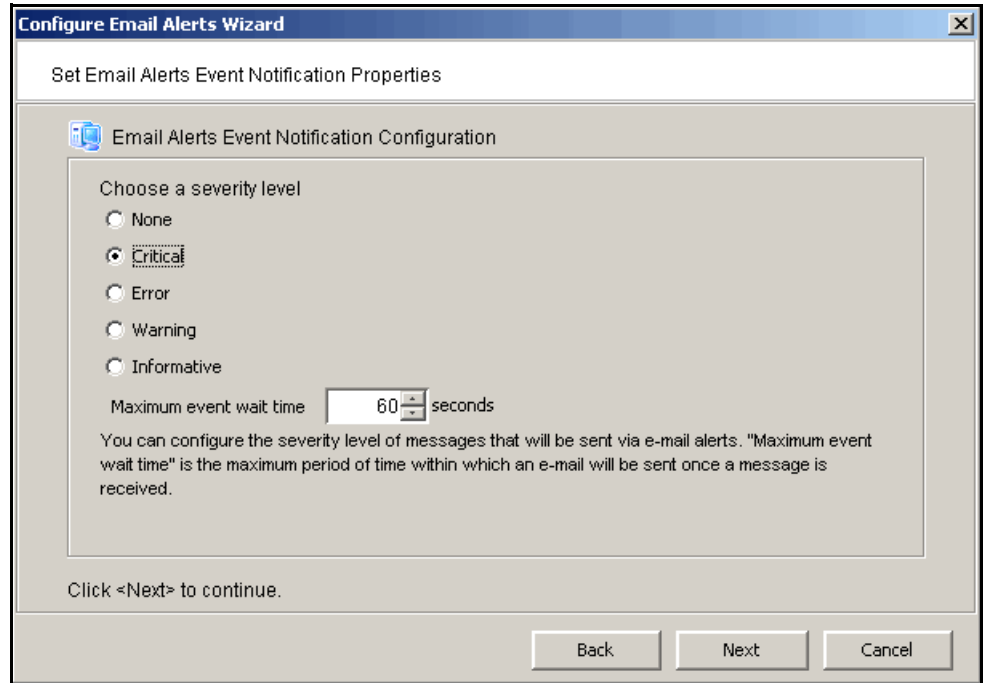
The system log records important events or errors that occur in the system, including those generated by VTL.

This dialog allows you to rule out entries in the system log that have nothing to do with VTL, and to list the types of log entries generated by VTL that Email Alerts needs to examine. Entries that do not match the entries here will be ignored, regardless of whether or not they are relevant to VTL.

The trigger for monitoring the system log is `syslogchk.sh`. To inform the trigger of which specific log entries need to be captured, you can specify the general types of entries that need to be inspected by Email Alerts.

Each line is a regular expression. The regular expression rules follow the pattern for AWK (a standard Unix utility).

6. On the *Event Notification Configuration* dialog, indicate the severity level of messages that should be sent as email alerts by Email Alerts.



If you select *None*, no messages will be sent via email.

*Maximum event wait time* is the maximum period of time within which an e-mail will be sent once a message is received.

7. Confirm all information and click *Finish* to enable Email Alerts.

## Modify Email Alerts properties

Once Email Alerts is enabled, you can modify the information by right-clicking on your VTL server and selecting *Email Alerts*.

Click on the appropriate tab to update the desired information.

---

## Script/program trigger information

Email Alerts uses script/program triggers to perform various types of error checking. By default, scripts/programs are included that check for low system memory, changes to the VTL XML configuration file, and relevant new entries in the system log.

### *Customize email for a specific trigger*

You can specify an email address to override the default *To* address or a text subject to override the default *Subject*. To do this:

1. Right-click on your VTL server and select *Email Alerts*.
2. Select the *Trigger* tab.
3. For an existing trigger, highlight the trigger and click *Edit*.  
For a new trigger, click *Add*.
4. Check the *Redirect Notification Without Attachment* checkbox.
5. Enter the alternate email address or subject.

If you specify an email address, it overrides the return code. Therefore, no attachment will be sent, regardless of the return code.

### *New script/program*

The trigger can be a shell script or a program (Java, C, etc.). If you create a new script/program, you must add it in the Console so that Email Alerts knows of its existence.

To do this:

1. Right-click on your VTL server and select *Email Alerts*.
2. Select the *Trigger* tab.
3. Click *Add*.
4. Click *Browser* to locate the shell script/program.
5. If required, enter an argument for the trigger.

You can also enter a comment for the trigger and specify alternate email information.



---

Return codes	Return codes determine what happens as a result of the script's/program's execution. The following return codes are valid: <ul style="list-style-type: none"><li>• 0: No action is required and no email is sent.</li><li>• Non-zero: Email Alerts sends an email.</li></ul>
Output from trigger	In order for a trigger to send useful information in the email body, it must redirect its output to the environment variable \$IPSTORCLHMLOG.
Sample script	The following is the content of the VTL status check trigger, vtlstatus.sh:

```
#!/bin/sh
RET=0
if [ -f /etc/.is.sh ]
then
    . /etc/.is.sh
else
    echo Installation is not complete. Environment profile is missing in
/etc.
    echo
    exit 0 # don't want to report error here so have to exit with error
code 0
fi
$ISHOME/bin/vtl status | grep STOPPED >> $VTLCCLHMLOG
if [ $? -eq 0 ] ; then
    RET=1
fi
exit $RET
```

If any VTL module has stopped, this trigger generates a return code of 1 and sends an email.

# Command Line

---

VirtualTape Library (VTL) provides a simple utility that allows you to perform some of the more common VTL functions at a command line instead of through the VTL Console. You can use this command line utility to automate many tasks, as well as integrate VTL with your existing management tools.

## Using the command line utility

Type `iscon` at the command line to display a list of commands. Each command must be combined with the appropriate long or short arguments (ex. Long: `--server-name` Short: `-s servername`) that are described in this chapter.

If you type the command name (for example, `c:\iscon importtape`), a list of arguments will be displayed for that command.

## Commands

On the following pages is a list of commands you can use to perform VTL functions from the command line. You should be aware of the following as you enter commands:


- Type each command on a single line, separating arguments with a space.
- You can use either the short or long arguments.
- Variables are listed in `<>` after each argument.
- Arguments listed in brackets `[ ]` are optional.
- The order of the arguments is irrelevant.
- Arguments separated by `|` are choices. Only one can be selected.
- For a value entered as a literal, it is necessary to enclose the value in quotes (double or single) if it contains special characters such as `*`, `<`, `>`, `?`, `|`, `%`, `$`, or space. Otherwise, the system will interpret the characters with a special meaning before it is passed to the command.
- Literals cannot contain leading or trailing spaces. Leading or trailing spaces enclosed in quotes will be removed before the command is processed.

---

## Common arguments

The following arguments are used by many commands. For each, a long and short variation is included. You can use either one. The short arguments **ARE** case sensitive. For arguments that are specific to each command, refer to the section for that command.

Short Argument	Long Argument	Value/Description
-s	--server-name	VTL Server Name (hostname or IP address)
-u	--server-username	VTL Server Username
-p	--server-password	VTL Server User Password
-c	--client-name	VTL Client Name
-v	--vdevid	VTL Virtual Device ID

 Note: You only need to use the --server-username (-u) and --server-password (-p) arguments when you log into a server. You do not need them for subsequent commands on the same server during your current session.

---

## Login/logout to the VTL Server

### *Log in to the VTL Server*

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

```
iscon login [--server-name=<server-name> --server-username=<username>  
--server-password=<password>|--environment] [--rpc-timeout=<rpc-timeout>]
```

#### **Description:**

This command allows you to log into the specified VTL Server with a given username and password. Once successfully logged into the server, `-u` (`--server-username`) and `-p` (`--server-password`) are not necessary for the other CLI commands with optional `-u` and `-p` arguments.

By default, Manufacturing sets up the "root" and "vtl" accounts to be able to log in and execute the iscon commands. Only "vtl" can log in from a remote session over ssh; "root" access is disabled by default for remote login.

In order to use the `-e` (`--environment`) parameter, you must set the following three environment variables:

- ISSERVERNAME
- ISUSERNAME
- ISPASSWORD

After setting these variables, the environment parameter can be used in the login command in place of `-s <server-name> -u <user-name> -p <password>`. Therefore, you could type the following to log in: `iscon login -e`

To set these environment variables in the bash shell, you must set three variables as follows:

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

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

### *Log out from the VTL Server*

```
iscon logout -s <server-name> [-X <rpc-timeout>]
```

```
iscon logout --server-name=<server-name> [--rpc-timeout=<rpc-timeout>]
```

#### **Description:**

This command allows you to log out from the specified VTL Server. If the server was not logged in or you have already logged out from the server when this command is issued, error 0x0902000f will be returned. After logging out from the server, the `-u` and `-p` arguments will not be optional for the server commands.

---

## Virtual devices / Clients

### *Get virtual device list*

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

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

#### **Description:**

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

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

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

`-A` (`--long-physical-layout`) displays the physical layout when `-l` (`--longlist`) is specified.

`-C` (`--long-client-list`) displays the assigned client list when `-l` (`--longlist`) option is specified.

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

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

### *Get Client virtual device list*

```
iscon getclientvdevlist -s <server-name> [-u <username> -p <password>]
-c <client-name> [-t <client-type>] [-l [-M <output-delimiter>] ]
[-X <rpc-timeout>]

iscon getclientvdevlist --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--client-name=<client-name> [--client-type=<client-type>]
[--longlist [--output-delimiter=<output-delimiter>] ] [--rpc-timeout=<rpc-timeout>]
```

#### **Description:**

This command retrieves and displays information about all virtual devices assigned to the client from the specified server. The default output format is a list with heading. Use `-c` (`--client-name`) to specify a client name or `*` for all clients. `-t` (`client-type`) is the type of the client protocol to be retrieved in one of the following values: *SCSI*, *FC*, or *ISCSI*. The client type will only take effect when the client name is `*`. Be aware that in some platforms you are required to enclose the `"**"` in double quote to take it as a literal.

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

---

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

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

## Add client

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

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

### Description:

This command allows you to add a client to the specified server. -c (--client-name) is a unique client name for the client to be created. The maximum length of the client name is 64. The following characters are invalid for a client name: <>"&\$/\'

-l (--initiator-wwpns) is the option to set the initiator WWPNs. An initiator WWPN is a 16-byte Hex value. Separate initiator WWPNs with commas if more than one initiator WWPN is specified. For example:  
13af35d2f4ea6fbc,13af35d2f4ea6fad

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

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

-C (--enable-Celerra) is an option to support Celerra with the following values: *on* or *off* (default).

Enabling Celerra will automatically disable VSA and iSeries, and vice versa.

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

## Delete client

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

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

### Description:

This command allows you to delete a client from the specified server. -c (--client-name) is the name of the client to be deleted.

---

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

## Get client properties

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

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

### Description:

This command gets client properties. -c (--client-name) is required to specify the client name.

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

## Assign virtual device

```
iscon assignvdev -s <server-name> [-u <username> -p <password>]
-v <vdevid> -c <client-name> -a <access-mode> [-y]
[-I <initiatorWWPN|*>] [-T <targetWWPN|*>] [-l <lun>] [-X <rpc-timeout>]
```

```
iscon assignvdev --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --vdevid=<vdevid>
--client-name=<client-name> --access-mode=<access-mode> [--vlib-only]
[--initiatorWWPN=<initiatorWWPN|*>] [--targetWWPN=<targetWWPN|*>] [--lun=<lun>]
[--rpc-timeout=<rpc-timeout>]
```

### Description:

This command allows you to assign a virtual device on a specified server to a client.

-v (--vdevid) is required to specify the virtual device ID of the virtual tape library or virtual tape drive to be assigned.

-c (--client-name) is required to specify the client to which the virtual tape library or drive will be assigned.

The values for <access-mode> are: *ReadOnly*, *ReadWrite*, *ReadWriteNonExclusive*. The values for the short format are: *R/W/N*.

-y (--vlib-only) is an option that allows you to assign the virtual tape library to the client without assigning all of the virtual tape drives in the library. The default is to assign all of the virtual tape drives in the library.

-I (--initiatorWWPN) and -T (--targetWWPN) are options for Fibre Channel clients. The initiator WWPN or target WWPN is a 16-byte hex value or "\*" for all. For example, 13af35d2f4ea6fbc. The default is "\*" if it is -I or the -T option is not specified.

-l (--lun) is another option for Fibre Channel clients. The range is between 0 and 15. The next available LUN will be assigned if it is not specified.

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

---

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

## ***Unassign virtual device***

```
iscon unassignvdev -s <server-name> [-u <username> -p <password>]  
-v <vdevid> -c <client-name> [-y] [-f] [-X <rpc-timeout>]
```

```
iscon unassignvdev --server-name=<server-name> [--server-username=<username>]  
[--server-password=<password>] --vdevid=<vdevid> --client-name=<client-name>  
[--vlib-only] [--force] [--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command allows you to unassign a virtual device on the specified server from a client.

-v (--vdevid) is required to specify the virtual device ID of the virtual tape library or drive to be unassigned.

-c (--client-name) is required to specify the client name from which to unassign the library or drive.

-y (--vlib-only) is an option that allows you to unassign the virtual tape library to the client without unassigning all of the virtual tape drives in the library. The default is to unassign all of the virtual tape drives in the library.

The -f (--force) option is required to unassign the virtual device when the client is connected and the virtual device is attached. An error will be returned if the force option is not specified.

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

## ***Create virtual device***

```
iscon createvdev -s <server-name> [-u <username> -p <password>]  
-I <ACSL> [-n <vdevname>] [-X <rpc-timeout>]
```

```
iscon createvdev --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]  
--scsiaddress=<ACSL> [--vdevname=<vdevname>] [--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command allows you to create a direct virtual device, such as virtual tape library or virtual tape drive.

-I (--scsiaddress) is required to specify the SCSI address of the virtual tape library or virtual tape drive in the following format: ACSL=#:#:#:# (adapter:channel:id:lun)

-n (--vdevname) is an option to specify the direct virtual device name. A default name will be generated if the name is not specified. The maximum length is 64. Leading and trailing spaces will be removed. Enclose the name in double quotes. The following characters are invalid for the direct virtual device name: <>"&\$/\'

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 300 seconds.



---

## Delete virtual device

```
iscon deletevdev -s <server-name> [-u <username> -p <password>]  
-v <vdevid> [-d] [-f] [-X <rpc-timeout>]]
```

```
iscon deletevdev --server-name=<server-name>  
[--server-username=<username> --server-password=<password>] --vdevid=<vdevid>  
[--delete-virtual-tapes] [--force] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command allows you to delete a virtual tape library, virtual tape drive, standalone virtual tape drive, or virtual tape.

In order to delete a virtual tape drive from a virtual tape library, the virtual tape drive must have the highest element number in the library.

-v (--vdevid) is required to specify the virtual device ID.

A virtual device cannot be deleted if any of the following conditions apply:

- The specified virtual device is a virtual tape library or a virtual tape drive and there are clients currently connected to the library or drive.
- The specified virtual device is a virtual tape configured for replication, unless the -f (--force) option is used.
- The specified virtual device is the only existing virtual tape drive in the parent virtual tape library.

-d (--delete-virtual-tapes) is an option to delete all of the existing virtual tapes from a virtual tape library, a standalone virtual tape drive, or a loaded virtual tape drive selected for deletion. By default, the virtual tapes are moved to the vault, or, if a loaded virtual tape drive is selected, back to the library.

-f (--force) is an option to force the deletion of a virtual tape configured for replication. The corresponding virtual tape replica will not be deleted or promoted.

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

## Get supported virtual libraries

```
iscon getsupportedvlibs -s <server-name> [-u <username> -p <password>]  
[-l [-t <vlib-type>] [-c][M <output-delimiter>] ] [-X <rpc-timeout>]
```

```
iscon getsupportedvlibs --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]  
[--longlist [--vlib-type=<vlib-type>] [--compatible-drive-list]  
[--output-delimiter=<output-delimiter>] ] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command retrieves information about all supported virtual tape libraries.

Note: Sun has certified the Sun VTL virtual tape library with backup vendors. Customers should use only this library (it can be configured with whatever drives and however many cartridges they need, but it is preconfigured with the same characteristics as a Sun L700 library). For backend libraries, Sun will only support Sun StorageTek branded library types.

---

-l (--longlist) can be specified to get the supported library information in a long format. The default is to display the information in a list format.

-t (--vlib-type) is an option with the -l (--longlist) option to get the detail library information for a specific library. The format for the <vlib-type> is: <vendorID>:<productID>. For example, ADIC:Scalar 100

-c (--compatible-drive-list) is an option to display the compatible drives in a tabular format instead of the default long format.

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

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

## ***Get supported virtual drives***

```
iscon getsupportedvdrives -s <server-name> [-u <username> -p <password>]
[-l [-M <output-delimiter>] ] [-X <rpc-timeout>]
```

```
iscon getsupportedvdrives --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--longlist [--output-delimiter=<output-delimiter>] ] [--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command retrieves information about all supported virtual tape drives.

-l (--longlist) can be specified to get the supported drive information in a long format. The default is to display the information in a list format.

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

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

## ***Create virtual tape library***

```
iscon createvirtuallibrary -s <server-name> [-u <username> -p <password>]
-t <vlib-type> [-n <vlib-name>] -d <vdrive-type> [-r <vdrive-name-prefix>]
[-R <num-of-drives>] [-A <auto-archive-mode> [-Y <days>] [-J] | -N <auto-repl-mode>]
-S <target-name> [-M <#[D|H|M]>] ] [-B <barcode-range>] [-T <num-of-slots>]
[-E <import-export-slots>] [-D -I <initial-size> -C <increment-size>]
[-m <max-capacity>] [-L <on|off>] [-k <key-name> -W <key-password>] [-X <rpc-timeout>]
```

```
iscon createvirtuallibrary --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--vlib-type=<vlib-type> [--vlib-name=<vlib-name>] --vdrive-type=<vdrive-type>
[--vdrive-name-prefix=<vdrive-name-prefix>] [--num-of-drives=<num-of-drives>]
[--auto-archive-mode=<auto-archive-mode> [--delay-delete-days=<days>]
[--auto-eject-to-ie] | --auto-replication=<auto-repl-mode> --target-name=<target-name>
[--delay-delete-time=<#[D|H|M]>] ] [--barcode=<barcode-range>]
```

---

```
[--num-of-slots=<num-of-slots>] [--import-export-slots=<import-export-slots>]
[--capacity-on-demand --initial-size=<initial-size> --increment-size=<increment-size>]
[--max-capacity=<max-capacity>] [--auto-loader=<on|off>]
[--key-name=<key-name> --key-password=<key-password>] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command creates a virtual tape library.

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

-n (--vlib-name) is optional. A default name will be provided in the format of <vendorID>-<productID>-<vid> if it is not specified.

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

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

-R (--num-of-drives) can also be specified up to the maximum number of drives supported by the library. The default is 1 if it is not specified.

-A (--auto-archive-mode) is an option with one of the following values: *copy* or *move*.

-Y (--delay-delete-days) is an option for move mode to specify the number of days to wait before deletion. The maximum is 365 days.

-J (--auto-eject-to-ie) is an option to be specified with -A (--auto-archive-mode) to eject the tape to the import/export (IE) slot after the export job.

-N (--auto-replication) is an option with one of the following values: *replication* or *remotemove*.

-S (--target-name) is the remote server name for auto-replication. It is required for auto-replication.

-M (--delay-delete-time) is an option for *remotemove* mode to specify a time to wait before deletion. It can be specified in days(D), hours(H) or minutes(M). For example, 2D, 10H, 150M. The default value is one day.

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

Barcode is an alpha-numeric value with a length of 4 to 12. <barcodeB> and <barcodeE> have to be the same length.

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

-T (--num-of-slots) and -E (--import-export-slots) are optional. The <num-of-slots> can exceed the maximum number of slots supported by the specified library type, but it is limited to 65536. The <--import-export-slots> cannot exceed the maximum number of IE slots supported by the specified library type. The default is to use the maximum number of slots supported by the specified library type.

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

-I (--initial-size) and -C (--increment-size) are options to be specified with <capacity-on-demand> option. The default value for both options is 5 GB. The <--increment-size> cannot be less than 5 GB.

---

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

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

-L (--auto-loader) is an option to set the auto-loader for those libraries that support the feature. The default value is *off*.

-k (--key-name) and -W (--key-password) are options for tape encryption support to be set in conjunction with Auto-Archive Mode. Specify the key name and key password of the encryption key if you wish to encrypt the data when exporting the virtual tape to the physical tape.

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

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

## **Add virtual tape drive**

```
iscon addvirtualdrive -s <server-name> [-u <username> -p <password>]
-L <tape-library-vid> [-r <vdrive-name-prefix>] [-R <num-of-drives>] [-X <rpc-timeout>]
```

```
iscon addvirtualdrive --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--tape-library-vid=<tape-library-vid> [--vdrive-name-prefix=<vdrive-name-prefix>]
[--num-of-drives=<num-of-drives>] [--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command adds a virtual tape drive to a specify virtual tape library.

-L (--tape-library-vid) is required to specify the virtual tape library to add the virtual tape drive(s).

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

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 300 seconds.

## **Create standalone tape drive**

```
iscon createstandalonedrive -s <server-name> [-u <username> -p <password>]
-d <vdrive-type> [-r <vdrive-name-prefix>] [-R <num-of-drives>]
[-D -I <initial-size> -C <increment-size>] [-m <max-capacity>] [-X <rpc-timeout>]
```

```
iscon createstandalonedrive --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--vdrive-type=<vdrive-type> [--vdrive-name-prefix=<vdrive-name-prefix>]
[--num-of-drives=<num-of-drives>] [--capacity-on-demand --initial-size=<initial-size>
--increment-size=<increment-size>] [--max-capacity=<max-capacity>]
[--rpc-timeout=<rpc-timeout>]
```

### **Description:**

---

This command creates a standalone virtual tape drive.

`-d (--vdrive-type)` is required to specify the type of tape drive to be created in the following format:  
`<vdendorID>:<productID>`

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

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

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

`-l (--initial-size)` and `-C (--increment-size)` are options to be specified with `<capacity-on-demand>` option. The default value for both options is 5 GB. The `<--increment-size>` cannot be less than 5 GB.

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

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

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

## Create virtual tape

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

```
iscon createvirtualtape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--parent-vid=<parent-vid> [ [--size-gb=<#(GB)>] [--scsiaddress=<ACSL>] ]
[--vdevname=<vdevname>] [--barcode=<barcode | barcode-range>] [--count=<count>]
[--enable-auto-archive --plib-vid=<plib-vid>
--physical-tape-barcode=<physical-tape-barcode>
[--auto-eject-to-ie] | --enable-auto-remotecopy
--target-name=<target-name> [--target-username=<target-username>
--target-password=<target-password>] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command creates a virtual tape.

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

`-g (--size-gb)` is an option to specify the size in GB. The size of the virtual tape will be the size configured in the properties of the virtual tape library or virtual tape drive if it is not specified. This option cannot be specified if the capacity on demand option is not enabled at parent level.

`-l (--scsiaddress)` is an option to specify specific physical devices to be used to create a virtual device. It can be a list of ACSLs separated by a comma or a file enclosed in `<>` containing an ACSL on each line.  
ACSL=#:#:# (adapter:channel:id:lun)

---

-n (--vdevname) is an option to specify the virtual tape name or prefix when creating more than one tape. The maximum length of the virtual device name is 64. Leading and trailing spaces will be removed. Enclose the name in double quotes to ensure the proper name. The following characters are invalid for the name: <>"&\$\^

-B (--barcode) is an option to either set the virtual tape with the provided barcode or create virtual tapes in batch mode configured with barcodes from the specified barcode range. The argument must be within the barcode range configured for the library and must not contain used barcodes. When provided as a barcode range, the option creates a virtual tape for each barcode in the range.

-t (--count) is an option to create multiple virtual tapes having the barcode automatically chosen from within the barcode range configured at library level. The library must have the required number of free slots available. If combined, "count" and "barcode" options must agree in number.

If the parent library has the auto-archive/remotecopy property enabled, use the following options to provide additional information for virtual tape creation:

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

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

-b (--physical-tape-barcode) is required to specify the list of physical tape barcode(s) when the auto-archive option is specified. Separate multiple barcodes with commas. For example,  
-b 00010001,00010009,0001000A

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

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

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

The *count* and *barcode* options cannot be specified when the -A (--enable-auto-archive) option is specified because the number of tapes will be obtained from the list of barcodes specified with -b (--physical-tape-barcode) option.

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

## ***Move virtual tape***

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

```
iscon movevirtualtape --server-name=<server-name>  
[--server-username=<username> --server-password=<password>] --vdevid=<vdevid>  
[--tape-library-vid=<tape-library-vid> | --tape-drive-vid=<tape-drive-vid> |  
--slot-no=<slot-no>] [--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command moves a virtual tape to a different location.

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

---

-L (--tape-library-vid) is the virtual library to move to. It is not required if the virtual tape is moved within the library.

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

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

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

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

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

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

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

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

- Standalone Tape Drive -> Vault

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

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

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

## ***Tape copy***

```
iscon tapecopy -s <server-name> [-u <username> -p <password>]  
-v <source-vdevid> -S <target-name> [-U <target-username> -P <target-password>]  
[-L <tape-library-vid> | -D <tape-drive-vid>] [-n <vdevname>] [-f]  
[-X <rpc-timeout>]
```

```
iscon tapecopy --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]  
--source-vdevid=<source-vdevid> --target-name=<target-name>  
[--target-username=<target-username> --target-password=<target-password>]  
[--tape-library-vid=<tape-library-vid> | --tape-drive-vid=<tape-drive-vid>]  
[--vdevname=<vdevname>] [--force] [--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command copies a tape.

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

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

---

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

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

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

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

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

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

## Set tape duplication

```
iscon setvirtuallibrarytapeduplication -s <server-name> [-u <username> -p <password>]
-v <vdevid> -Z <on|off> -Q <num-of-copies> [-X <rpc-timeout>]
```

```
iscon setvirtuallibrarytapeduplication --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--vdevid=<vdevid> --tape-duplication=<on|off> --num-of-copies=<num-of-copies>
[--rpc-timeout=<rpc-timeout>]
```

### Description:

This command sets the Tape Duplication property for a virtual tape library.

-v (--vdevid) is required in order to identify the virtual library.

-Z (--tape-duplication) is required in order to enable or disable the Tape Duplication property: *on* (enable) or *off* (disable).

-Q (--num-of-copies) is an option to specify the number of copies to be made using the same barcode if tape duplication option is enabled. The maximum value is 5. The default value is 1.

The virtual library must have the Auto Archive or Tape Caching property enabled in order to enable tape duplication.

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

## Set tape properties

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



---

```
iscon settapeproperty --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --vdevid=<vdevid>
[--barcode=<barcode>] [--force] [--full-capacity] [--tape-write-protect=<on|off>]
[--auto-archive-mode=<auto-archive-mode> [--delay-delete-days=<days>]
[--auto-eject-to-ie] | --auto-replication=<auto-repl-mode> --target-name=<target-name>
[--server-username=<username> --server-password=<password>]
[--delay-delete-time=<#[D|H|M]>] ] [--key-name=<key-name> --key-password=<key-password> |
--disable-key] [--tape-duplication=<on|off> --num-of-copies=<num-of-copies>]
[--rpc-timeout=<rpc-timeout>]
```

### Description:

This command sets tape properties.

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

-B (--barcode) is the option to specify the new barcode for the tape. -f (--force) option is required if the new barcode is not in the barcode range specified for the parent library. Barcode is an alpha-numerical value with a length of 4 to 12.

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

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

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

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

-Y (--delay-delete-days) is an option for *move* mode to specify the number of days to wait before the deletion. The maximum is 365 days.

-J (--auto-eject-to-ie) is an option for auto-archive mode in order to enable or disable the ejection of the physical tape to the IE slot after a successful archive job: *on* (enable) or *off* (disable).

-N (--auto-replication) is an option with one of the following values: *localcopy*, *localmove*, *replication*, *remotemove*, or *none*.

-S (--target-name) is the remote server name for auto-replication. It is required for auto-replication.

-U (--target-username) and -P (--target-password) are options to specify a different user ID and password to log in to the remote server.

-M (--delay-delete-time) is an option for auto-replication move mode to specify up to 30 days of retention period before deletion. The default value is 1 day. The value can be specified in days(D), hours(H) or minutes(M). For example: 2D, 10H, 150M.

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

-k (--key-name), -W (--key-password) and -d (--disable-key) are options for tape encryption support to be set in conjunction with Auto-Archive Mode. Specify the key name and key password of the encryption key if you wish to encrypt the data when exporting the virtual tape to the physical tape. Specify -d (--disable-key) if you wish to disable tape encryption for this tape.

-Z (--tape-duplication) is an option to set the Tape Duplication property with one of the following values: *on* (enable), *off* (disable), or *inherit*.

---

-Q (--num-of-copies) is an option to specify the number of copies to be made using the same barcode if the tape duplication option is enabled. The maximum value is 5. The default value is 1.

Tape Duplication can be enabled only if the virtual library hosting the virtual tape has the Tape Caching property enabled or the virtual tape has the Auto Archive property enabled.

At least one of the properties has to be specified.

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

---

## Automated tape caching

### Set tape caching

```
iscon settapecaching -s <server-name> [-u <username> -p <password>]
-L <library-vid> -t <tape-caching-enable> [-S <start-time>][-W <day-of-the-week>]
[-b <and-or>] [[-e][-f]][-c <disk-capacity>][-d <days-old>]
[-R <retention-days> | -I | -M | -N] [-X <rpc-timeout>]
```

```
iscon settapecaching --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--tape-library-vid=<library-vid> [--start-time=<start-time>]
[--day-of-the-week=<day-of-the-week>] --tape-caching-enable=<tape-caching-enable>
[--trigger-combine=<and-or>] [--end-of-backup] [--tape-full]]
[--disk-capacity=<disk-capacity>] [--days-old=<days-old>]
[--retention-days=<retention-days> | --immediately | --no-more-space | --never]
[--rpc-timeout=<rpc-timeout>]
```

#### Description:

This command can be used in order to enable, disable, or change the Automated Tape Caching policy for a virtual tape library.

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

Set -t (--tape-caching-enable) to 1 for enable or 0 to disable.

If the *disable* option is used all other arguments will be ignored.

The *enable* option must be used in order to set or change the tape caching policy.

Time based data migration triggers:

-S (--start-time) alone can be used to start daily migrations at the time specified. The default value is 00:00(am)(hh:mm). When combined with other data migration triggers, the -S option will delay the migration execution to the specified time.

-W (--day-of-the-week) can be used to start weekly migrations on the specified day at 00:00(am): Sunday: 0, Monday: 1, ..., Saturday: 6. The default value is -1. This option is ignored if Policy Based triggers are used.

Policy based data migration triggers:

-b (--trigger-combine) tells how trigger policies are combined (specified by -e, -c, -d). 1 -- and; 0 -- or. The default value is 1 (and).

-e (--end-of-backup) triggers data migration when unloading a tape from a drive after some data is written to it.

-f (--tape-full) applies to -e options. Data is migrated only if the tape becomes full.

-c (--disk-capacity) triggers data migration when disk usage percentage is above the global disk space threshold.

-d (--days-old) triggers data migration after data was retained on disk for (days-old) days (up to 3650 days).

Reclamation triggers:

---

-R (retention-days) determines the number of days virtual tapes will be kept in the system before they are deleted.

Select -I (--immediately) and virtual tapes will be deleted immediately after data migration completes.

Select -M (--no-more-space) and virtual tapes will be deleted when disk space is needed to create (or expand) a virtual tape. The last used will be deleted.

Select -N (--never) and virtual tapes will never be deleted.

The reclamation triggers are exclusive.

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

## Sync physical tapes

```
iscon syncphysicaltape -s <server-name> [-u <username> -p <password>]
-l <plib-vid> -b <physical-tape-barcode> -L <virtual-tape-library-id>
-t <virtual-tape-slot-no> [-M <sync-mode>] [-k <key-name> -W <key-password>]
[-I <ACSL list>] [-n <vdevname>] [-g <#(GB)>] [-X <rpc-timeout>]
```

```
iscon syncphysicaltape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--plib-vid=<physical-tape-library-vid> --physical-tape-barcode=<physical-tape-barcode>
--tape-library-vid=<virtual-tape-library-id>
--virtual-tape-slot-no=<virtual-tape-slot-no> [--sync-mode=<sync-mode>]
[--key-name=<key-name> --key-password=<key-password>] [--scsiaddress=<ACSL list>]
[--vdevname=<vdevname>] [--size-gb=<#(GB)>] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command creates a synchronized virtual tape for the specified physical tape. The physical tape must be from the specified physical tape library and the virtual tape will be created in the specified virtual tape library. The virtual tape library must have the tape caching feature enabled.

-l <--plib-vid> is the virtual ID of the physical tape library where the physical tapes are located.

-b <--physical-tape-barcode> is the barcode of the physical tape. The virtual tape will be created with the same barcode. The barcode must not be in use by any other virtual tape in the system. If the barcode contains leading or trailing space characters, it must be enclosed in double quotes.

-L <--tape-library-vid> is the ID of the virtual tape library where the virtual tapes will be created.

-t <--virtual-tape-slot-no> is an option to provide an empty destination slot for the virtual tape. Not for "-M cache" mode.

[-M <--sync-mode>] is an option to select the synchronization mode from one of the following values (default is "cache"):

- cache (create cache)
- metadata (create cache and copy meta data)
- directlink (create direct link )

-k (--key-name) and -W (--key-password) are options for tape encryption support. If the tape to be synchronized was encrypted through the system, you need to specify the key name and the key password of the encryption key to decrypt the data on the imported tape.

---

[*-l* <--scsiaddress>] is the option to specify which physical devices to be used to create the virtual device. It can be a list of ACSLs separated with commas. ACSL=#:#:# (adapter:channel:id:lun)

*-n* (--vdevname) is an option to specify the virtual tape name or prefix when creating more than one tape. The maximum length of the virtual device name is 64. Leading and trailing spaces will be removed. Please enclose the name in double quotes to ensure the proper name. The following characters are invalid for the name: <>"&\${'`

*-g* (--size-gb) is an option to specify the initial size, in GB, of the virtual tapes, if the capacity-on-demand property for the virtual tape library is enabled. The default is 1 GB

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

## ***Migrate virtual tapes***

```
iscon migratevirtualtapes -s <server-name> [-u <username> -p <password>]
-T <tape-vid-list> [-f] [-X <rpc-timeout>]
```

```
iscon migratevirtualtapes --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--tape-vid-list=<tape-vid-list> [--tape-full] [--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command migrates the specified virtual tapes to the physical libraries they are synchronized with.

*-T* (--tape-vid-list) is a list of virtual tape ID(s) separated with commas.

*-F* (--tape-full) is an option to force full tape migration. By default, the migration operation is incremental.

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

## ***Reclaim disk space***

```
iscon reclaimtapes -s <server-name> [-u <username> -p <password>]
-T <tape-vid-list> [-X <rpc-timeout>]
```

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

### **Description:**

This command reclaims the disk space occupied by the specified migrated virtual tapes.

*-T* (--tape-vid-list) is required to specify the ID of the virtual tapes to be reclaimed, separated with commas.

*-X* (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 300 seconds.

---

## Renew cache

```
iscon renewcache -s <server-name> [-u <username> -p <password>]  
-v <vdevid> [-M <metadata>] [-k <key-name> -W <key-password>] [-I <ACSL>] [-n <vdevname>]  
[-g <#(GB)>] [-X <rpc-timeout>]
```

```
iscon renewcache --server-name=<server-name>  
[--server-username=<username> --server-password=<password>] [--import-mode=<metadata>]  
[--key-name=<key-name> --key-password=<key-password>] [--scsiaddress=<ACSL>]  
[--vdevname=<vdevname>] [--size-gb=<#(GB)>] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command converts a virtual stub tape into a virtual cache tape.

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

-M (--import-mode) is an option to specify that the header area should be copied from the physical tape to the new virtual tape cache. The value of this option must be: *metadata*.

-k (--key-name) and -W (--key-password) are options for tape encryption support. If the tape to be renewed was encrypted through the system, you need to specify the key name and the key password of the encryption key to decrypt the data.

The following properties of the virtual cache tape can be set if the "-M" option is not specified:

-I (--scsiaddress) is the option to specify which physical devices should be used to create the virtual device. It can be a list of ACSLs separated with commas or a file enclosed in <> containing an ACSL on each line.  
ACSL=#:#:# (adapter:channel:id:lun)

-n (--vdevname) is an option to specify the virtual tape name or prefix when creating more than one tape. The maximum length of the virtual device name is 64. Leading and trailing spaces will be removed. Enclose the name in double quotes to ensure it is properly parsed and interpreted. The following characters are invalid for the name:  
<>"&\${\`

-g (--size-gb) is an option to specify the size in GB. The size of the virtual tape will be the size configured in the properties of the virtual tape library or virtual tape drive if it is not specified. This option cannot be specified if the capacity-on-demand option is not enabled at library level.

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

---

## System configuration

### Add a license keycode

```
iscon addlicense -s <server-name> [-u <username> -p <password>] -k <license-keycode>
[-X <rpc-timeout>]
```

```
iscon addlicense --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --license=<license-keycode>
[--rpc-timeout=<rpc-timeout>]
```

#### Description:

This command adds a license keycode.

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

### Remove a license keycode

```
iscon removelicence -s <server-name> [-u <username> -p <password>] -k <license-keycode>
[-X <rpc-timeout>]
```

```
iscon removelicence --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --license=<license-keycode>
[--rpc-timeout=<rpc-timeout>]
```

#### Description:

This command removes a license keycode.

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

### Get VTL info

```
iscon getvtlinfo -s <server-name> [-u <username> -p <password>]
[-T <vtl-info_type> [-L <tape-library-vid>]] [-F <vtl-info-filter>] [-l [-M]]
[-X <rpc-timeout>]
```

```
iscon getvtlinfo --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--vtl-info-type=<vtl-info-type> [--tape-library-vid=<tape-library-vid>] ]
[--vtl-info-filter=<vtl-info-filter>]
[--longlist [--ouput-delimiter=<output-delimiter>] ] [--rpc-timeout=<rpc-timeout>]
```

#### Description:

This command retrieves VTL information.

-T (--vtl-info-type) is the VTL information type with one of the following values: *VLIBS* or *VDRIVES* or *VAULT* or *PLIBS* or *PDRIVES*.

- *VLIBS* = display virtual tape libraries only.

- 
- VDRIVES = display standalone virtual tape drives only
  - VAULT = display virtual tape vault only.
  - PLIBS = display physical tape libraries only.
  - PDRIVES = display standalone physical tape drives only.

The default is to display all the information.

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

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

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

For example: -F "library,drive,tape" or --vtl-info-filter="library,drive,tape"

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

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

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

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



---

## Import/Export

### *Import tape*

```
iscon importtape -s <server-name> [-u <username> -p <password>]
[-M <import-mode>] -v <plib-or-pdrive-vid> [-B <barcode> | -l <slot-no>]
-L <tape-library-vid> [-b <virtual-tape-barcode>] -t <virtual-tape-slot-no>
[-j <job-description>] [-k <key-name> -W <key-password>] [-X <rpc-timeout>]
```

```
iscon importtape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--import-mode=<import-mode>] --plib-or-pdrive-vid=<plib-or-pdrive-vid>
[--barcode=<barcode> | --slot-no=<slot-no>] --tape-library-vid=<tape-library-vid>
--virtual-tape-slot-no=<virtual-tape-slot-no>
[--virtual-tape-barcode=<virtual-tape-barcode>] [--job-description=<job-description>]
[--key-name=<key-name> --key-pasword=<key-password>] [--rpc-timeout=<rpc-timeout>]
```

#### **Description:**

This command imports the data from a tape into the VTL.

Important Note: Tape caching must be disabled prior to using the import function.

-M (--import-mode) is an option in one of the following values: *copy* (default) or *direct-access* or *recycle*.

-v (--pdrive-or-pdrive-vid) is required to specify the virtual device ID of the physical tape library or physical tape drive from which the physical tape is to be imported.

If the physical tape is from a physical tape library, either <barcode> or <slot-no> of the physical tape should be specified with -B (--barcode) or -l (--slot-no) to identify the physical tape. If the barcode contains leading or trailing space characters, it must be enclosed in double quotes. No physical tape information is required if the physical tape is imported from a standalone physical tape drive.

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

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

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

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

-k (--key-name) and -W (--key-password) are options for tape encryption support. If the tape to be imported was encrypted through the system, you need to specify the key name and the key password of the encryption key to decrypt the data on the imported tape.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 300 seconds.

---

## Export virtual tape

```
iscon exportvirtualtape -s <server-name> [-u <username> -p <password>] -v <vdevid>
-L <tape-library-vid> -b | -B <barcode> | -l <slot-no>
[-M <export-mode> [-Y <days>] ] [-j <job-description>] [-f] [-J]
[-k <key-name> -W <key-password>] [-Z <on> -Q <num-of-copies>] [-X <rpc-timeout>]
```

```
iscon exportvirtualtape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--vdevid=<vdevid> --tape-library-vid=<tape-library-vid>
--same-barcode | --barcode=<barcode> | --slot-no=<slot-no>
[--export-mode=<export-mode>] [--delay-delete-days=<days>] ]
[--job-description=<job-description>] [--force] [--auto-eject-to-ie]
[--key-name=<key-name> --key-password=<key-password>]
[--tape-duplication=<on> --num-of-copies=<num-of-copies>] [--rpc-timeout=<rpc-timeout>]
```

### Description:

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

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

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

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

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

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

-Y (--delay-delete-days) is an option for *move mode* to specify the number of days to wait before deletion. The maximum is 365 days. The default value is 365 days.

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

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

-J (--auto-eject-to-ie) is an option to eject the tape to the IE slot after the export job.

-k (--key-name) and -W (--key-password) are options for tape encryption support. Specify the key name and key password of the encryption key if you wish to encrypt the data when exporting the virtual tape to the physical tape.

-Z (--tape-duplication) is an option to enable tape duplication with the following value: *on*.

-Q (--num-of-copies) is an option to specify the number of copies to be made using the same barcode if the tape duplication option is enabled. The maximum value is 5. The default value is 1.

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

---

## Get import/export job status

```
iscon getimportexportjobstatus -s <server-name> [-u <username> -p <password>]
[-j <job-id-list>] [-T <job-type> -S <job_status>] [-X <rpc-timeout>]

iscon getimportexportjobstatus --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--job-id-list=<job-id-list>] | [--job-type=<job_type> --job_status=<job_status>]
[--rpc-timeout=<rpc-timeout>]
```

### Description:

This command displays the status of the import/export jobs present in the queue. If no filters are specified, the command displays all the jobs that are in the queue.

-j <--job-id-list> is an optional list of job IDs separated with commas. The command displays the status of specified jobs only. All other filters are ignored.

-T <--job-type> is an optional job type based filter. The command displays those jobs matching the provided type. The accepted job type values are: IMPORT, EXPORT, or OTHER.

-S <--job\_status> is an optional job status based filter. The command displays those jobs matching the provided status. The accepted job status values are: FAILED, HOLD, READY, or OTHER.

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

## Resume import/export jobs

```
iscon resumeimportexportjobs -s <server-name> [-u <username> -p <password>]
-j <job-id-list> [-X <rpc-timeout>]

iscon resumeimportexportjobs --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --job-id-list=<job-id-list>
[--rpc-timeout=<rpc-timeout>]
```

### Description:

This command resumes specified import/export jobs. The jobs must be held in the import/export queue in a suspended state.

-j <--job-id-list> is a list of job IDs separated with commas.

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

## Delete import/export jobs

```
iscon deleteimportexportjobs -s <server-name> [-u <username> -p <password>]
-j <job-id-list> [-X <rpc-timeout>]

iscon deleteimportexportjobs --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --job-id-list=<job-id-list>
[--rpc-timeout=<rpc-timeout>]
```

---

**Description:**

This command deletes specified import/export jobs. The jobs must be held in the import/export queue.

-j <--job-id-list> is a list of job IDs separated with commas.

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

## ***Suspend import/export jobs***

```
iscon suspendimportexportjobs -s <server-name> [-u <username> -p <password>]  
-j <job-id-list> [-X <rpc-timeout>]
```

```
iscon suspendimportexportjobs --server-name=<server-name>  
[--server-username=<username> --server-password=<password>] --job-id-list=<job-id-list>  
[--rpc-timeout=<rpc-timeout>]
```

**Description:**

This command suspends specified import/export jobs. The jobs must be held in the import/export queue and must be idle.

-j <--job-id-list> is a list of job IDs separated with commas.

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

## ***Cancel import/export jobs***

```
iscon cancelimportexportjobs -s <server-name> [-u <username> -p <password>]  
-j <job-id-list> [-X <rpc-timeout>]
```

```
iscon cancelimportexportjobs --server-name=<server-name>  
[--server-username=<username> --server-password=<password>] --job-id-list=<job-id-list>  
[--rpc-timeout=<rpc-timeout>]
```

**Description:**

This command cancels specified import/export jobs. The jobs must be held in the import/export queue and must be running.

-j <--job-id-list> is a list of job IDs separated with commas.

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

---

# Replication

## Create a replica

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

```
iscon createreplication --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--source-vdev-id=<source-vdev-id> --target-name=<target-name>
[--target-username=<target-username> --target-password=<target-password>]
[--watermark=<watermark(MB)> | [--date=<YYYYMMDDHHMM> --interval=<#[H|M]>]] |
[--repl-first <on>] [--replication-timeout=<timeout>]
[--replication-retry-interval=<retry-in>] [--replication-retry-count=<retry-for>]
[--compression=<on|off>] [--encryption=<on|off>] [--force] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command allows you to set up a replication configuration.

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

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

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

The replication configuration requires a trigger policy to be set. If no trigger policy is specified, the command will automatically apply the appropriate default policy based on the tape caching property of the specified virtual tape.

Any combination of the following two options can be used to set up a replication trigger policy for a virtual tape with the tape caching property disabled. The default policy is 1024 MB watermark.

`-w` (`--watermark`) is a data size based trigger in MB. The watermark is checked when the tape is unloaded from the tape drive and the replication is triggered if the amount of new data on the tape has reached the specified watermark.

`-d` (`--date`) combined with `-i` (`--interval`) is a time based trigger. The replication is triggered at the time specified by date and then repeated every interval. `-d` (`--date`) format is YYYYMMDDHHMM and `-i` (`--interval`) format is a number followed by H for hours or M for minutes (e.g. `-i 2H` or `--interval=120M`). The default value for interval is 1H (one hour).

`-r` (`--repl-first`) is an option to replicate the virtual tape before it is migrated. Use "on" in order to enable this policy or "off" to have tape migration executed first. The default policy is to replicate the virtual tape after it is migrated.

Replication is retried based on the timeout policy:

- `-t` (`--replication-timeout`) in seconds (default 60).
- `-I` (`--replication-retry-interval`) in seconds (default 60).
- `-C` (`--replication-retry-count`) retry count (default 1).

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

---

-e (--encryption) is an option for remote replication only to set encryption with one of the values: *on* or *off*.

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

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

## **Promote a replica**

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

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

### **Description:**

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

Specify either the primary server and the source virtual tape ID or the target server and the tape replica ID. The user name and password must be provided for both servers, if the servers were not registered using the login command.

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

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

-f (--force) is an option to enforce the promotion if the source virtual tape is no longer available or the tape replica is in invalid state, if you are sure the data on the tape replica is useful.

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

## **Remove replication**

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

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

This command allows you to remove the replication configuration from the primary disk on the primary server and delete the replica disk on the target server.

---

Specify either the primary server and the source virtual tape ID or the target server and the tape replica ID. The user name and password must be provided for both servers, if the servers were not registered using the login command.

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

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

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

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

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

## ***Suspend replication***

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

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

### **Description:**

This command allows you to suspend scheduled replications for a virtual device that will be triggered by your replication policy. It will not stop a replication that is currently in progress.

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

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

## ***Resume replication***

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

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

### **Description:**

This command allows you to resume replication for a virtual device that was suspended by the *suspendreplication* command. The replication will then be triggered by the replication policy once it is resumed.

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

---

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

## Set replication properties

```
iscon setreplicationproperties -s <server-name> [-u <username> -p <password>]
-v <source-vdevid> [-w <watermark(MB)> | [-d <YYYYMMDDHHMM> -i <#[H|M]>]] |
[-r <on|off>] [[-t <timeout>] [-I <retry-in>]] [-C <retry-for>]] [-c <on|off>]
[-e <on|off>] [-X <rpc-timeout>]
```

```
iscon setreplicationproperties --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--source-vdevid=<source-vdevid>
[--watermark=<watermark(MB)> | [--date=<YYYYMMDDHHMM> --interval=<#[H|M]>]] |
[--repl-first <on|off>] [--replication-timeout=<timeout>] [--replication-retry-
interval=<retry-in>] [--replication-retry-count=<retry-for>][--compression=<on|off>]
[--encryption=<on|off>] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command allows you to change the replication policy for the specified virtual tape.

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

Any combination of the following two options can be used to set up a replication trigger policy for a virtual with the tape caching property disabled.

-w (--watermark) is a data size based trigger in MB. The watermark is checked when the tape is unloaded from the tape drive and the replication is triggered if the amount of new data on the tape has reached the specified watermark.

-d (--date) combined with -i (--interval) is a time based trigger. The replication is triggered at the time specified by date and then repeated every interval. -d (--date) format is YYYYMMDDHHMM and -i (--interval) format is a number followed by H for hours or M for minutes (e.g. -i 2H or --interval=120M).

To delete a watermark trigger specify 0 for the watermark. To delete a time based trigger specify NA for date. At least one trigger must remain active.

The date argument is not required if you are only changing the interval.

For virtual tapes having the tape caching property enabled, replication is triggered based on the tape caching policy:

-r (--repl-first) is required to replicate the virtual tape before it is migrated. Use "on" in order to enable this policy or "off" to have tape migration executed first.

The replication retry policy can be changed using the following options:

- -t (--replication-timeout) in seconds (default 60).
- -I (--replication-retry-interval) in seconds (default 60).
- -C (--replication-retry-count) retry count (default 1).

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



---

-e (--encryption) is an option for remote replication only to set the encryption with one of the values: *on* or *off*.

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

## ***Get replication properties***

```
iscon getreplicationproperties -s <server-name> [-u <username> -p <password>]  
-v <source-vdevid> [-X <rpc-timeout>]
```

```
iscon getreplicationproperties --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]  
--source-vdevid=<source-vdevid> [--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command allows you to get the replication properties for a virtual device configured for replication.

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

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

## ***Get replication status***

```
iscon getreplicationstatus -S <target-name> [-U <username> -P <password>]  
-V <replicaid> [-X <rpc-timeout>]
```

```
iscon getreplicationstatus --target-name=<target-name>  
[--target-username=<username> --target-password=<password>]  
--replicaid=<replicaid> [--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command shows the replication status.

-S (--target-name) is the target server and -V (--replicaid) is ID of the tape replica, both of which are required.

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

## ***Start replication***

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

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

### **Description:**

---

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

-v (--source-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.

## ***Stop replication***

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

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

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

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

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

---

## Physical devices

### *Inventory physical tape library*

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

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

#### **Description:**

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

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

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

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

### *Get physical tape list*

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

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

#### **Description:**

This command displays a list of physical tapes located in the specified physical tape library.

-l (--plib-vid) is the ID of the physical tape library.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 300 seconds.

### *Move physical tape*

```
iscon movephysicaltape -s <server-name> [-u <username> -p <password>]  
-m <move-operation> -L <physical-tape-library-vid>  
-B <physical-tape-barcode> | -l <from-location-id> -t <to-location-id>  
[-X <rpc-timeout>]
```

```
iscon movephysicaltape --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]  
--move-operation=<move-operation> --tape-library-vid=<physical-tape-library-vid>  
--physical-tape-barcode=<barcode> | --from-location-id=<from-location-id>  
--to-location-id=<to-location-id> [--rpc-timeout=<rpc-timeout>]
```

---

**Description:**

This command moves a physical tape to a new location.

-m(--move-operation) is one of the following operations:

- DriveToSlot
- SlotToSlot
- SlotToDrive
- IESlotToSlot
- SlotToIESlot

-L(--tape-library-vid) is the physical library virtual ID where the tape is located.

-B(--physical-tape-barcode) identifies the physical tape to be moved. If barcode is not provided, the current tape location must be provided accordingly to the requested operation.

-l(--from-location-d) is the current slot or import/export (IE) slot number, or the physical drive virtual ID.

-t(--to-location-id) is the destination slot or IE slot number or the physical drive virtual ID. This does not apply to the IESlot. If the destination is the IESlot, the physical tape will be moved to the first available IESlot.

-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 60 seconds.

## ***Eject physical tape***

```
iscon ejectphysicaltape -s <server-name> [-u <username> -p <password>]  
-L <physical-tape-library-vid> -B <physical-tape-barcode-list>  
[-A <acs-lsm-cap>] [-X <rpc-timeout>]
```

```
iscon ejectphysicaltape --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]  
--tape-library-vid=<physical-tape-library-vid>  
--tape-barcode-list=<physical-tape-barcode-list> | [--acs-lsm-cap=<acs-lsm-cap>]  
[--rpc-timeout=<rpc-timeout>]
```

**Description:**

This command ejects physical tapes from the specified library.

-L(--tape-library-vid) is the physical library virtual ID where the tapes are located.

-B(--tape-barcode-list) identifies the physical tapes to be ejected. This argument can be a list of barcodes separated with commas. The list should be enclosed in double quotes.

-A <--acs-lsm-cap> is an optional argument representing the Cartridge Access Port for the Automated Cartridge System Library Software libraries. The format of the argument is acs:lsm:cap

-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 10,800 seconds.

---

## Assign physical resource to VTL

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

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

### Description:

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

-I (--scsiaddress) is required in order to identify the physical tape library or the physical tape drive to be assigned to VTL.

-L (--tape-library-vid) is an option to specify the physical tape library as a parent when assigning physical tape drive to physical tape library that is already assigned to VTL.

The physical tape library information can be retrieved by issuing the *getvtlinfo* command.

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

## Unassign physical resource from VTL

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

```
iscon unassignresourcefromvtl --server-name=<server-name>  
[--server-username=<username> --server-password=<password>] --vdevid=<vdevid>  
[--preserve-directlink] [--rpc-timeout=<rpc-timeout>]
```

### Description:

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

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

-q (--preserve-directlink) is an option to preserve the direct linked tapes for physical tape libraries.

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

## Get physical device information

```
iscon getpdevinfo -s <server-name> [-u <username> -p <password>]  
[-F [-M | -C <category>] | [-a] [-A] [-I <ACSL>] ] [-o <output-format>]  
[-X <rpc-timeout>]
```

```
iscon getpdevinfo --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]
```

---

```
[--config [--include-system-info | --category=<category>] |
[--allocated-list] [--available-list] [--scsiaddress=<ACSL>] ]
[--output-format=<output-format>] [--rpc-timeout=<rpc-timeout>]
```

### Description:

-F (--config) is an option to get the physical device configuration information. The default is to exclude the system device information.

-M (--include-system-info) is an option to include the system device information.

-C (--category) is an option to be used as a filter to get the configuration information for the specified category with one of the values: *virtual* (default) or *service-enabled* or *direct*.

The -M (--include-system-info) and -C (--category) options are mutually exclusive.

-o (--output-format) is the option to specify the output format. The <output-format> for the -F (--config) option is one of the following values: *list* or *detail* or *guid* or *scsi*.

-a (--allocated-list) is an option to get the allocated physical device information.

-A (--available-list) is an option to get the available physical device information.

-l (--scsiaddress) is an option to specify the SCSI address as a device filter in the following format:  
<ACSL>=#: #: #: # (adapter:channel:id:lun)

The <output-format> for the -a (--allocated-list) and the -A (--available-list) options is one of the following values: *list* or *detail* or *size-only*.

-F (--config), and -a (--allocated-list) and/or -A (--available-list) are mutually exclusive. You can either get the configuration information or get the allocation information. When getting the allocation information, you can specify either -a (--allocated-list), or -A (--available-list) or both. The default is to display both the device allocation and availability information if none of the options is specified.

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

## Rescan physical devices

```
iscon rescandevices -s <server-name> [-u <username> -p <password>]
[-a <adapter-range>] [-i <scsi-range>] [-l <lun-range>] [-L] [-X <rpc-timeout>]
```

```
iscon rescandevices --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--adapter-range=<adapter-range>] [--scsi-range=<scsi-range>] [--lun-range=<lun-range>]
[--sequential] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command allows you to rescan the physical resource(s) on the specified server to get the proper physical resource configuration.

-a (--adapter-range) is the adapter or adapter range to be rescanned. The default is to rescan all adapters, if it is not specified. For example: -a 5 or -a 5-10

---

-i (--scsi-range) is the starting SCSI ID and ending SCSI ID to be rescanned. The default is to rescan all the SCSI IDs if the range is not specified. For example: -i 0-5

-l (--lun-range) is the starting LUN and ending LUN to be rescanned. The default is not to rescan any LUN if it is not specified. For example: -l 0-10

-L (--sequential) is an option to rescan sequentially.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 300 seconds.

## ***Import disk***

```
iscon importdisk -s <server-name> [-u <username> -p <password>]
-i <guid> | -I <ACSL> [-X <rpc-timeout>]
```

```
iscon importdisk --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--scsiaddress=<ACSL> | --guid=<guid> [--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command allows you to import a foreign disk to the specified server. A foreign disk is a virtualized physical device containing VTL logical resources previously set up on a different VTL server. If the previous server is no longer available, the disk can be set up on a new VTL server and the resources on the disk can be imported to the new server to make them available to clients.

The <guid> is the unique identifier of the physical device. <ACSL> is the SCSI address of the physical device in the following format: `#:#:#: (adapter:channel:scsi id:lun)`

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 300 seconds.

## ***Prepare physical device for VTL server***

```
iscon preparedisk -s <server-name> [-u <username> -p <password>]
[-U <target-username> -P <target-password>] -i <guid> | -I <ACSL>
-C <category> [-N <new-guid>] [-X <rpc-timeout>]
```

```
iscon preparedisk --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--target-username=<username> --target-password=<password>]
--scsiaddress=<ACSL> | --guid=<guid> --category=<category> [--new-guid=<new-guid>]
[--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command allows you to prepare a physical device to be used by an VTL server or reserve a physical device for other usage.

The <guid> is the unique identifier of the physical device. <ACSL> is the SCSI address of the physical device in the following format: `#:#:#: (adapter:channel:scsi id:lun)`

---

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

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

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

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

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 300 seconds.



---

## Reports

### *Server throughput report*

```
iscon createserverthroughputreport -s <server-name> [-u <username> -p <password>] [-z <report period>] | [-D <date-range>] [-o <filename>] [-f] [-X <rpc-timeout>]
```

```
iscon createserverthroughputreport --server-name=<server-name> [--server-username=<username> --server-password=<password>] [--report-period=<report-period>] | [--date-range=<date-range>] [--output-file=<filename>] [--force] [--rpc-timeout=<rpc-timeout>]
```

#### **Description:**

This command creates a report that displays throughput data and configuration information for a specific server.

-z (--report-period) is the period of time that the report should cover. The accepted values are:

- t - today
- y - yesterday
- 7 - last seven days
- 30 - last thirty days

-D (--date-range) is the starting date and ending date in the following format (maximum 30 days):  
YYYYMMDD-YYYYMMDD or YYYYMMDD

Either -z (--report-period) or -D (--date-range) can be specified, but not both. The date option is applied to the server local time. The default value is: "-z t" (today).

-o (--output-file) is the file name used to save the report data. If an output filename is not specified, the default filename is: ServerThroughput-server-MM-DD-YYYY-hh-mm-ss[.#]

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

Specify the -f (--force) option if you want to overwrite the existing file if the output file already exists.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The default RPC timeout is 300 seconds.

### *SCSI channel throughput report*

```
iscon createscsichannelthroughputreport -s <server-name> [-u <username> -p <password>] [-z <report period>] | [-D <date-range>] -t <adapter-no> [-o <filename>] [-f] [-X <rpc-timeout>]
```

```
iscon createscsichannelthroughputreport --server-name=<server-name> [--server-username=<username> --server-password=<password>] [--report-period=<report-period>] | [--date-range=<date-range>] --adapter-no=<adapter-no> [--output-file=<filename>] [--force] [--rpc-timeout=<rpc-timeout>]
```

#### **Description:**

This command creates a report that displays the throughput values for a specific SCSI/Fibre channel.

---

-t (--adapter-no) is required in order to identify the requested SCSI/Fibre Channel adapter.

-z (--report-period) is the period of time that the report should cover. The accepted values are:

- t - today
- y - yesterday
- 7 - last seven days
- 30 - last thirty days

-D (--date-range) is the starting date and ending date in the following format (maximum 30 days):  
YYYYMMDD-YYYYMMDD or YYYYMMDD

Either -z (--report-period) or -D (--date-range) can be specified, but not both. The date option is applied to the server local time. The default value is: "-z t" (today).

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: SCISChannelThroughput-server-MM-DD-YYYY-hh-mm-ss[.#]

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

Specify the -f (--force) option if you want to overwrite the existing file if the output file already exists.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The default RPC timeout is 300 seconds.

## ***Device throughput report***

```
iscon createdevicethroughputreport -s <server-name> [-u <username> -p <password>]  
-I <ACSL> [-z <report period>] | [-D <date-range>] [-o <filename>] [-f]  
[-X <rpc-timeout>]
```

```
iscon createdevicethroughputreport --server-name=<server-name>  
[--server-username=<username> --server-password=<password>] --scsiaddress=<ACSL>  
[--report-period=<report-period>] | [--date-range=<date-range>]  
[--output-file=<filename>] [--force] [--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command creates a report that displays throughput values for a specific device.

-I <ACSL> (--scsiaddress) is the LUN address of the device.

-z (--report-period) is the period of time that the report should cover. The accepted values are:

- t - today
- y - yesterday
- 7 - last seven days
- 30 - last thirty days

-D (--date-range) is the starting date and ending date in the following format (maximum 30 days):  
YYYYMMDD-YYYYMMDD or YYYYMMDD

Either -z (--report-period) or -D (--date-range) can be specified, but not both. The date option is applied to the server local time. The default value is: "-z t" (today).

---

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: SCSIDeviceThroughput-server-MM-DD-YYYY-hh-mm-ss[.#]

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

Specify the -f (--force) option if you want to overwrite the existing file if the output file already exists.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The default RPC timeout is 300 seconds.

## ***Physical resources configuration report***

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

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

### **Description:**

This command creates a report that displays the physical resources configuration for a specific server. This report lists all of the physical resources on this server, including each physical adapter and physical device.

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: PhysicalResourcesConfiguration-server-MM-DD-YYYY-hh-mm-ss[.#]

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

Specify the -f (--force) option if you want to overwrite the existing file if the output file already exists.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The default RPC timeout is 300 seconds.

## ***Disk usage report***

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

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

### **Description:**

This command creates a report that displays the amount of disk space used by disk libraries on a specific server.

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: DiskSpaceUsage-server-MM-DD-YYYY-hh-mm-ss[.#]

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

Specify the -f (--force) option if you want to overwrite the existing file if the output file already exists.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The default RPC timeout is 300 seconds.

---

## ***Physical resources allocation report***

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

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

### **Description:**

This command creates a report that displays the physical resource allocation for a specific server.

-o (--output-file) is file name used to save the report data. If the output filename is not specified, the default filename is: PhysicalResourcesAllocation-server-MM-DD-YYYY--hh-mm-ss[.#]

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

Specify the -f (--force) option if you want to overwrite the existing file if the output file already exists.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The default RPC timeout is 300 seconds.

## ***Specific physical resource allocation report***

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

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

### **Description:**

This command creates a report that displays the physical resource allocation of a specific device on a specific server.

-I <ACSL> (--scsiaddress) is the LUN address of the device.

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: PhysicalResourceAllocation-server-MM-DD-YYYY--hh-mm-ss[.#]

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

Specify the -f (--force) option if you want to overwrite the existing file when the output file already exists.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The default RPC timeout is 300 seconds.

---

## ***Fibre Channel adapter configuration report***

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

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

### **Description:**

This command creates a report that displays the Fibre Channel adapter configuration for a specific server.

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: FCAdaptersConfig-server-MM-DD-YYYY-hh-mm-ss[#]

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

Specify the -f (--force) option if you want to overwrite the existing file if the output file already exists.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The default RPC timeout is 300 seconds.

## ***Replication status report***

```
iscon createreplicationstatusreport -s <server-name> [-u <username> -p <password>]
[-D <date-range>] [-r <repl-resource-type> | -R <resourceList>] [-o <outputFilename>]
[-f] [-X <rpc-timeout>]
```

```
iscon createreplicationstatusreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--date-range=<date-range>]
[--repl-resource-type=<repl-resource-type> | --resource-list=<resourceList>]
[--output-file=<outputFilename>] [--force] [--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command creates a report that displays the status of a specified resource on a specific server.

-D (--date-range) is an option to specify the date range to be queried. The date format is YYYYMMDD or YYYYMMDD-YYYYMMDD. If date range is not specified, the default is today's date.

-r (--repl-resource-type) is an option to specify a generic resource type to be queried. It can be one of the following:

- TAPE
- TAPEReplica

The default value is TAPE.

-R <--resource-list> in an option to report the status of the specified resources only. The argument can be a list of virtual identifiers separated with commas or the name of a file enclosed in <> containing the resource ID on each line. All the resources must be of the type specified by "-r".

- Example 1: -R 10000005,10000006
- Example 2: -R "<res\_id\_file.txt>"

---

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: ReplicationStatus-server-MM-DD-YYYY-hh-mm-ss[.#]

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

Specify the -f (--force) option if you want to overwrite the existing file if the output file already exists.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The default RPC timeout is 300 seconds.

## ***Virtual library information report***

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

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

### **Description:**

This command creates a report that displays all of the virtual libraries for a specific server.

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: VirtualLibraryInfo-server-MM-DD-YYYY-hh-mm-ss[.#]

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

Specify the -f (--force) option if you want to overwrite the existing file if the output file already exists.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The default RPC timeout is 300 seconds.

## ***Virtual tape information report***

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

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

### **Description:**

This command creates a report that displays all of the virtual tapes for a specific server.

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: VirtualTapeInfo-server-MM-DD-YYYY-hh-mm-ss[.#]

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

Specify the -f (--force) option if you want to overwrite the existing file if the output file already exists.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The default RPC timeout is 300 seconds.

---

## Create job report

```
iscon createjobreport -s <server-name> [-u <username> -p <password>]
[-z <report period>] | [-D <date-range>] [-o <filename>] [-f] [-X <rpc-timeout>]
```

```
iscon createjobreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--report-period=<report-period>] | [--date-range=<date-range>]
[--output-file=<filename>] [--force] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command creates a report that displays all of the jobs executed during a selected period of time for a specific server.

-z (--report-period) is the period of time that the report should cover. The accepted values are:

- t - today
- y - yesterday
- 7 - last seven days
- 30 - last thirty days

-D (--date-range) is the starting date and ending date in the following format (maximum 30 days):  
YYYYMMDD-YYYYMMDD or YYYYMMDD

Either -z (--report-period) or -D (--date-range) can be specified, but not both. The date option is applied to the server local time. The default value is: "-z t" (today).

-o (--output-file) is the file name used to save the report data. If the output filename is not specified, the default filename is: JobReport-MM-DD-YYYY-hh-mm-ss[.#]

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

Specify the -f (--force) option if you want to overwrite the existing file if the output file already exists.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The default RPC timeout is 300 seconds.

---

## Event Log

### *Get Event Log*

```
iscon geteventlog -s <server-name> [-u <username> -p <password>]  
[-D <date-range>] [-F <fileFormat>] [-o <filename>] [-H] [-f] [-X <rpc-timeout>]
```

```
iscon geteventlog --server-name=<server-name>  
[--server-username=<username> --server-password=<password>] [--date-range=<date-range>]  
[--file-format=<fileFormat>] [--include-heading] [--output-file=<filename>] [--force]  
[--rpc-timeout=<rpc-timeout>]
```

#### **Description:**

This command gets the event log.

-D (--date-range) is the starting date/time and ending date/time in the following format:  
YYYYMMDDhhmmss-YYYYMMDDhhmmss or YYYYMMDDhhmmss

-F (--fileFormat) is one of the following formats: *csv* (default) or *txt*.

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

-o (--output-file) is the full path of the file name to save the event log data. If an output filename is not specified, the default filename is: eventlogYYYY-MM-DD-hh-mm-<servername>[.#]

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

Specify the -f (--force) option if you want to overwrite the existing file if the output file already exists.

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



---

## Technical support

### Get X-Ray

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

iscon getxray --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--get-log=<#|all|YYMMDDhhmm-YYMMDDhhmm>] [--rescan-for-xray] [--output-file=<filename>]
[--force] [--rpc-timeout=<rpc-timeout>]
```

#### Description:

This command allows you to get X-ray information from the VTL Server for diagnostic purposes. Each X-ray contains technical information about your server, such as server messages and a snapshot of your server's current configuration and environment. You should not create an X-ray unless you are requested to do so by your Technical Support representative.

-l (--get-log) is a filter to get the specified log messages.

- # = number of lines
- all = all the log messages
- YYMMDDhhmm-YYMMDDhhmm = log messages in date/time range

The default is to get all the log messages.

-r (--rescan-for-xray) is an option to rescan the physical devices before the xray is taken. The default is not to rescan the devices.

-o (--output-file) is the full path of the file name to save the xray to. The default output filename format is: xray-YYYY-MM-DD-hh-mm-<servername>.tar.gz

Specify the -f (--force) option if you want to overwrite the existing file if the output file already exists. Otherwise, an error will be returned.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 300 seconds.

### Get attention required information

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

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

#### Description:

This commands displays the attention required messages.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 in seconds for the RPC timeout. The system will retry the command for the amount of time specified if the server does not respond. The default RPC timeout is 300 seconds.

# Appendix

---

This appendix contains information about system security, VTL Server operating system installation, and VTL Console installation.

## System security

VTL uses the following ports. Network firewalls should allow access through these ports for successful communications. In order to maintain a high level of security, you should disable all unnecessary ports. The only ports required by VTL are:

Port	Purpose
TCP port 11576	Used for VTL Console to VTL appliance management communication
UDP port 11577	Used for IP replication
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 port 3260	Used for iSCSI
UDP port 25	Used for sendmail (Email Alerts)
TCP port 25	Used for sendmail (Email Alerts)
UDP port 22	Used for SSH
TCP port 22	Used for SSH
UDP port 23	Used for TELNET
TCP port 23	Used for TELNET
UDP port 20	Used for FTP
TCP port 20	Used for FTP
UDP port 21	Used for FTP
TCP port 21	Used for FTP
UDP port 111	PortMapper (ACSLs)*
TCP port 111	PortMapper (ACSLs)*

Port	Purpose
UDP port 6666	Areca FalconStor Raid Controller #1 (Appliances with built in storage)
TCP port 6666	Areca FalconStor Raid Controller #1 (Appliances with built in storage)
UDP port 6667	Areca FalconStor Raid Controller #2 (Appliances with built in storage)
TCP port 6667	Areca FalconStor Raid Controller #2 (Appliances with built in storage)
UDP port 6668	Areca FalconStor Raid Controller #3 (Appliances with built in storage)
TCP port 6668	Areca FalconStor Raid Controller #3 (Appliances with built in storage)
TCP 11576	SANClient
TCP 11582	SANClient
TCP 11762	SANClient

\*Note: PortMapper requires dynamic ports to be open. This requires the ACSLS to be in the same VLAN with ACSLS server.

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.

Note: There is a script to disable unused ports. It is located in the /software/security folder, as is one to undo the restrictions. You should run this script (disableUnusedServices.ksh) periodically to make sure the ports remain closed.

---

## Console installation

The Console is the graphical administration tool where you configure VTL, add/configure clients, set properties, and manage the import/export of tapes.

The Console is a Java application that can be run on many platforms that support the Java 2 Runtime Environment (JRE) version.

The computer that runs the Console needs connectivity to the network segment where VTL is running. This is because it communicates directly with the server and clients (backup servers). The Console may be installed on any number of machines, including the clients themselves, provided that they have a Graphical User Interface.

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.

## Prerequisite

Before you install the console, there is a required patch you must perform that changes the IPStorConsole.jar file. Procedures for how to do this are in the VTL Plus 2.0 Update 2 release notes.

## 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
```

- 
- 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
```

- To launch the console, enter the following command:

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

## Installing the console on Linux platforms

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

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

- 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.

- To launch the console, enter the following command:

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

## 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.

- 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.

- 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.

## 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 &
```

## VTL private network addresses

This appendix lists the private IP addresses factory-assigned to the components of the VTL system.

### VTL service laptop

Device	Port	Connectivity (to device, port)	IP address	Subnet mask	Comments
<b>laptop</b>	LAN	VTL LAN switch (to NETMGT on Node1 or Node2)	10. 0 . 0 . 77	255.255.255. 0	Port name varies on different laptops.

### VTL Plus 2.0 appliance

Device	Port	Connectivity (to device, port)	IP address	Subnet mask	Comment	
<b>LAN switch</b>	1	Node1, NET 1				
	2	Node1, NETMGT				
	3	Node2, NET 1				
	4	Node2, NETMGT				
	5	Controller1A, 1				
	6	Controller1B, 1				
	7	Controller2A, 1				
	8	Controller2B, 1				
	9	Controller3A, 1				
	10	Controller3B, 1				
	11	Controller4A, 1				
	12	Controller4B, 1				
	13	Controller5A, 1				
	14	Controller5B, 1				
	15	Controller6A, 1				
	16	Controller6B, 1				
	17	Controller7A, 1				
	18	Controller7B, 1				
	19	Controller8A, 1				
	20	Controller8B, 1				
	21		VTL SAN switch, 1			
	22		VTL SAN switch, 2			
<b>Node1</b>	NET 0	nge0	customer LAN	192. 168. 1. 1	255.255.255.0	
	NET 1	nge1	VTL LAN switch, 1	10. 0. 0. 101	255.255.255.0	
	NET 2	e1000g0	VTL replication host	192. 168. 0. 100	255.255.255.0	
	NET 3	e1000g1	VTL replication host	192. 168. 0. 101	255.255.255.0	
	NETMGT		VTL LAN switch, 2	10. 0. 0. 102	255.255.255.0	ILOM (on GRASP board)

Device	Port	Connectivity (to device, port)	IP address	Subnet mask	Comment
<b>Node2</b>	NET 0	nge0	customer LAN	192. 168. 1. 10	255.255.255.0
	NET 1	nge1	VTL LAN switch, 3	10. 0. 0. 111	255.255.255.0
	NET 2	e1000g0	VTL replication host	192. 168. 0. 110	255.255.255.0
	NET 2	e1000g1	VTL replication host	192. 168. 0. 111	255.255.255.0
	NETMGT		VTL LAN switch, 4	10. 0. 0. 112	255.255.255.0
<b>Controller1A</b>	ETH1		VTL LAN switch, 5	10. 0. 0. 1	255.255.255.0
<b>Controller1B</b>	ETH1		VTL LAN switch, 6	10. 0. 0. 2	255.255.255.0
<b>Controller2A</b>	ETH1		VTL LAN switch, 7	10. 0. 0. 3	255.255.255.0
<b>Controller2B</b>	ETH1		VTL LAN switch, 8	10. 0. 0. 4	255.255.255.0
<b>Controller3A</b>	ETH1		VTL LAN switch, 9	10. 0. 0. 5	255.255.255.0
<b>Controller3B</b>	ETH1		VTL LAN switch, 10	10. 0. 0. 6	255.255.255.0
<b>Controller4A</b>	ETH1		VTL LAN switch, 11	10. 0. 0. 7	255.255.255.0
<b>Controller4B</b>	ETH1		VTL LAN switch, 12	10. 0. 0. 8	255.255.255.0
<b>Controller5A</b>	ETH1		VTL LAN switch, 13	10. 0. 0. 9	255.255.255.0
<b>Controller5B</b>	ETH1		VTL LAN switch, 14	10. 0. 0. 10	255.255.255.0
<b>Controller6A</b>	ETH1		VTL LAN switch, 15	10. 0. 0. 11	255.255.255.0
<b>Controller6B</b>	ETH1		VTL LAN switch, 16	10. 0. 0. 12	255.255.255.0
<b>Controller7A</b>	ETH1		VTL LAN switch, 17	10. 0. 0. 13	255.255.255.0
<b>Controller7B</b>	ETH1		VTL LAN switch, 18	10. 0. 0. 14	255.255.255.0
<b>Controller8A</b>	ETH1		VTL LAN switch, 19	10. 0. 0. 15	255.255.255.0
<b>Controller8B</b>	ETH1		VTL LAN switch, 20	10. 0. 0. 16	255.255.255.0
<b>SAN switch</b>	1		VTL LAN switch, 21	10. 0. 0. 50	255.255.255.0
	2		VTL LAN switch, 22	10. 0. 0. 51	255.255.255.0

## VTL Value appliance

Device	Port	Connectivity (to device, port)	IP address	Subnet mask	Comments
<b>system</b>	Net 0		10. 0 . 0 . 10	255.255.255.0	The operating system prefixes the port number with e1000g:
	NETMGT		10. 0 . 0 .100	255.255.255.0	e1000g0.

## VTL Plus 1.0 appliance

Device	Port name	Port label	Connectivity (to device, port)	IP address	Subnet mask
<b>Node1</b>	BG0	eth0		10. 0 . 0 . 10	255.255.255.0
	BG1	eth1		10. 0 . 0 . 11	255.255.255.0
		mgmt		10. 0 . 0 .100	255.255.255.0
<b>Node2</b>	BG0	eth0		10. 0 . 0 . 20	255.255.255.0
	BG1	eth1		10. 0 . 0 . 21	255.255.255.0



---

Device	Port name	Port label	Connectivity (to device, port)	IP address	Subnet mask
		mgmt		10. 0 . 0 .200	255.255.255.0
<b>Controller1A</b>				10. 0 . 0 . 1	255.255.255.0
<b>Controller1B</b>				10. 0 . 0 . 2	255.255.255.0
<b>Controller2A</b>				10. 0 . 0 . 3	255.255.255.0
<b>Controller2B</b>				10. 0 . 0 . 4	255.255.255.0

---

# 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
<b>User Commands</b>	
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>
<b>Network and Serial Port Setting Commands</b>	
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>
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=integer commitpending=true</code>
<b>Alert Commands</b>	
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=ipaddress level=down critical major minor</code>
<b>System Management Access Commands</b>	
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=portnumber securerredirect enabled disabled servicestate=enabled disabled</code>
Display information about HTTPS access.	<code>show /SP/services/https</code>

---

Description	Command
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>
<b>SNMP Commands</b>	
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>
Delete this device from an SNMP public community.	<code>delete /SP/services/snmp/communities/public/<i>Comm1</i></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/<i>Comm2</i></code>
<b>Host System Commands</b>	
Delete this device from an SNMP private community.	<code>delete /SP/services/snmp/communities/private/<i>Comm2</i></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>
<b>Clock Settings</b>	
Set the ILOM clock to synchronize with a primary NTP server.	<code>set /SP/clients/ntp/server/1 address=<i>ntpIPAddress</i></code>
Set the ILOM clock to synchronize with a secondary NTP server.	<code>set /SP/clients/ntp/server/2 address=<i>ntpIPAddress2</i></code>

---

---

# SNMP traps

The VTL product family defines the following Simple Network Management Protocol (SNMP) traps.

Trap	Severity	Message
9	Error	SCSI Port Error -- %1.
1000	Error	Socket connection could not be terminated properly -- %1.
1001	Error	Socket connection could not be terminated properly due to error during shutdown -- %1.
1002	Error	Unexpected interrupt occurred.
1003	Informational	"VTL Server has detected virtual device[%1] at SCSI %2, channel %3, ID %4, LUN %5."
1004	Informational	VTL Server has not detected any virtual device.
1005	Error	Out of kernel resources. Failed to get major number for VTL SCSI device.
1006	Error	Failed to allocate memory.
1007	Error	Failed to set up the network connection due to an error in SANRPC_Init -- %1.
1008	Error	Failed to set up the network connection due to an error in SANRPCListen -- %1.
1009	Informational	There are %1 real device(s) associated with virtual device [%2].
1010	Informational	Real Device[%1 %2 %3 %4].
1011	Error	Error while writing -- write(%1) result = 0x%2 cmd = 0x%3.
1012	Error	Error while reading -- read(%1) result = 0x%2 cmd = 0x%3.
1013	Informational	VTL Server [Build %1] is running on Linux %2.
1014	Informational	VTL Server has been shut down.
1015	Informational	"Maximum SCSI devices reached. On your VTL Server, verify with the command: cat /proc/scsi/scsi"
1016	Informational	Primary virtual device %1 has failed. VTL is switching to the secondary virtual device.
1017	Informational	Secondary virtual device %1 has failed.
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.

Trap	Severity	Message
1030	Error	Failed to start replication -- replication is already in progress for virtual tape %1.
1031	Error	Failed to start replication -- replication control area not present on virtual tape %1.
1032	Error	Failed to start replication -- replication control area has failed for virtual tape %1.
1034	Error	Replication failed for virtual device %1 -- the network transport returned error %2.
1035	Error	Replication failed for virtual device %1 -- the local disk failed with error %2.
1038	Error	Replication failed for virtual device %1 -- the local server could not allocate memory.
1039	Error	Replication failed for virtual device %1 -- the replica failed with error %2.
1040	Error	Replication failed for virtual device %1 -- failed to set the replication time.
1041	Informational	Mirror synchronization started for virtual device %1.
1042	Informational	Mirror synchronization finished for virtual device %1.
1043	Error	A SCSI command terminated with a non-recoverable error condition that was most likely caused by a flaw in the medium or an error in the recorded data. Please check the system log for additional information.
1044	Error	"A SCSI command terminated with a non-recoverable hardware failure (for example, controller failure, device failure, parity error, etc.). Please check the system log for additional information."
1045	Informational	Rescan replica has completed for virtual device %1
1046	Error	Rescan replica has failed for virtual device %1 -- the local device failed with error %2.
1047	Error	Rescan replica has failed for virtual device %1 -- the replica device failed with error %2.
1048	Error	Rescan replica has failed for virtual device %1 -- the network transport returned error %2.
1049	Error	Rescan replica cannot proceed -- replication control area not present on virtual device %1
1050	Error	Rescan replica cannot proceed -- replication control area has failed for virtual device %1
1051	Error	Rescan replica cannot proceed -- a merge is in progress for virtual device %1
1052	Error	Rescan replica failed for virtual device %1 -- replica status returned %2
1053	Error	Rescan replica cannot proceed -- replication is already in progress for virtual device %1
1054	Error	Replication cannot proceed -- a merge is in progress for virtual device %1
1055	Error	Replication failed for virtual tape %1 -- replica status returned %2
1056	Error	Replication control area exchange failed for virtual tape %1 -- the error code is %2
1057	Informational	Replication control area exchange has completed for virtual tape %1
1058	Informational	Replication has finished for virtual tape %1. %2 KB in %3 seconds (%4KB/sec)
1059	Error	Replication failed for virtual tape %1 -- start replication returned %2
1060	Error	Rescan replica failed for virtual device %1 -- start scan returned %2
1061	Warning	I/O path failure detected. Alternate path will be used. Failed path (A.C.S.L): %1; New path (A.C.S.L): %2

---

Trap	Severity	Message
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.
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.

---

---

Trap	Severity	Message
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.
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.

---

Trap	Severity	Message
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."
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.
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.



---

Trap	Severity	Message
11021	Informational	Auto save configuration enabled: ftp_server=%1 port=%2 directory=%3 interval=%4 copies=%5.
11022	Informational	Auto save configuration disabled.
11030	Error	Auto save configuration: cannot setup crontab.
11031	Error	Auto save configuration: cannot create the running script %1.
11032	Error	Auto save configuration: cannot connect to ftp server %1 port %2.
11033	Error	Auto save configuration: cannot login user %1.
11034	Error	Auto save configuration: directory %1 doesn't exist.
11035	Error	Auto save configuration: failed to copy %1 to ftp server.
11036	Error	Auto save configuration: failed to delete old file %1 from ftp server.
11037	Informational	Automated Tape Caching is %1 for virtual library %2.
11100	Informational	SAN Client (%1): SAN Client added.
11101	Error	SAN Client (%1): Failed to add SAN Client.
11102	Informational	SAN Client (%1): Authentication succeeded.
11103	Error	SAN Client (%1): Authentication failed.
11104	Error	Too many SAN Client connections.
11105	Informational	SAN Client (%1): Logged in.
11106	Error	SAN Client (%1): Failed to log in.
11107	Error	SAN Client (%1): Illegal access.
11108	Informational	SAN Client (%1): Logged out.
11109	Error	SAN Client (%1): Failed to open file %2.
11110	Error	SAN Client (%1): Failed to get hostname.
11111	Error	SAN Client (%1): Failed to resolve hostname %2.
11112	Error	SAN Client (%1): Failed to parse configuration file %2.
11113	Error	SAN Client (%1): Failed to restart authentication module.
11114	Error	SAN Client (%1): Failed to allocate memory.
11115	Error	"SAN Client (%1): License conflict -- Number of CPU's approved: %2, number of CPU's used: %3."
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.

---

---

Trap	Severity	Message
11211	Error	Console (%1): Failed to save file %2.
11212	Error	Console (%1): Failed to create index file %2 for Event Log.
11213	Error	Console (%1): Illegal time range (%2 - %3) for Event Log.
11214	Error	Console (%1): Failed to get Event Log (%2 - %3).
11215	Error	Console (%1): Failed to open directory %2.
11216	Error	Console (%1): Out of system resources. Failed to fork process.
11217	Error	Console (%1): Failed to execute program %2.
11218	Error	Console (%1): Failed to remove file %2.
11219	Error	Console (%1): Failed to add device %2.
11220	Error	Console (%1): Failed to remove device %2.
11221	Error	Console (%1): Failed to add SAN Client (%2) to virtual device %3.
11222	Error	Console (%1): Failed to remove SAN Client (%2) from virtual device %3.
11223	Informational	Console (%1): Logged in with read/write privileges.
11224	Informational	Console (%1): Logged in with read only privileges.
11225	Informational	Console (%1): Logged out.
11226	Informational	Console (%1): Configuration file %2 saved.
11227	Informational	Console (%1): Virtual device %2 added.
11228	Informational	Console (%1): Virtual device %2 removed.
11229	Informational	Console (%1): SAN Client (%2) added to virtual device %3.
11230	Informational	Console (%1): SAN Client (%2) removed from virtual device %3.
11231	Error	Console (%1): Failed to get CPU status.
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.

---

Trap	Severity	Message
11251	Error	Console (%1): Failed to update password for user %2.
11252	Informational	Console (%1): Password for user %2 updated.
11253	Error	Console (%1): Failed to modify virtual device %2.
11254	Informational	Console (%1): Virtual device %2 modified.
11255	Error	Console (%1): Failed to modify virtual device %3 for SAN Client (%2).
11256	Informational	Console (%1): Virtual device %3 for SAN Client (%2) modified.
11257	Error	Console (%1): Failed to add SAN Client (%2).
11258	Informational	Console (%1): SAN Client (%2) added.
11259	Error	Console (%1): Failed to delete SAN Client (%2).
11260	Informational	Console (%1): SAN Client (%2) deleted.
11261	Error	Console (%1): Failed to get SAN Client connection status for virtual device %2.
11262	Error	Console (%1): Failed to parse configuration file %2.
11263	Error	Console (%1): Failed to restore configuration file %2.
11264	Informational	Console (%1): Configuration file %2 restored.
11265	Error	Console (%1): Failed to restart IOCore module.
11266	Error	Console (%1): Failed to erase partition of virtual device %2.
11267	Informational	Console (%1): Virtual device %2 partition erased.
11268	Error	Console (%1): Failed to update meta information of virtual device %2.
11269	Error	Console (%1): Failed to get ID for SAN Client (%2).
11270	Error	Console (%1): Failed to add mirror for virtual device %2.
11271	Informational	Console (%1): Mirror added for virtual device %2.
11272	Error	Console (%1): Failed to remove mirror for virtual device %2.
11273	Informational	Console (%1): Mirror removed for virtual device %2.
11274	Error	Console (%1): Failed to stop mirroring for virtual device %2.
11275	Informational	Console (%1): Mirroring stopped for virtual device %2.
11276	Error	Console (%1): Failed to start mirror synchronization for virtual device %2.
11277	Informational	Console (%1): Mirror synchronization for virtual device %2 started.
11278	Error	Console (%1): Failed to swap mirror for virtual device %2.
11279	Informational	Console (%1): Mirror swapped for virtual device %2.
11280	Error	Console (%1): Failed to create shared secret for VTL Server %2.
11281	Informational	Console (%1): Shared secret created for VTL Server %2.
11282	Error	Console (%1): Failed to change device category for physical device %2 to %3.
11283	Informational	Console (%1): Device category changed for physical device %2 to %3.
11284	Error	Console (%1): Failed to get raw device name for physical device %2.
11285	Error	Console (%1): Failed to execute failover command (%2).
11286	Informational	Console (%1): Failover command executed (%2).
11287	Error	Console (%1): Failed to set failover mode (%2).
11288	Informational	Console (%1): Failover mode set (%2).
11289	Error	Console (%1): Failed to restart VTL Server module.
11290	Informational	Console (%1): VTL Server module restarted.

---

Trap	Severity	Message
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.
11400	Error	Failed to communicate with the Self-Monitor module.
11401	Error	Failed to release IP address %1.
11402	Error	Failed to read %1.
11403	Error	Failed to retrieve authentication information.
11404	Error	Failed to merge authentication information.
11405	Error	Failed to obtain IP address %1.
11406	Error	Failed to prepare the failover configuration package -- %1.
11407	Error	Failed to extract the failover configuration package -- %1.
11408	Warning	Synchronizing the system time with %1. A system reboot is recommended.
11500	Error	Out of disk space to expand virtual tape %1.
11501	Error	Failed to expand virtual tape %1: maximum segment exceeded (error code %2).
11502	Error	Failed to expand virtual tape %1 (segment allocation error code %2).
11503	Informational	Expand %1 by %2 MBytes.
11504	Error	Failed to expand virtual tape id %1 by %2 MBytes.
11505	Error	Failed to change virtual tape %1 to direct link mode.
11507	Error	Console (%1): Failed to create X-Ray file.
11508	Error	Console (%1): Failed to set the properties for the VTL Server.

---

Trap	Severity	Message
11509	Informational	Console (%1): Properties set for the VTL Server.
11510	Error	Console (%1): Failed to save report -- %2.
11511	Error	Console (%1): Failed to get the information for the NIC.
11512	Error	"Console (%1): Failed to add a replica for virtual tape %2 to VTL Server %3 (watermark: %4 MB, time: %5, interval: %6, watermark retry: %7, suspended: %8)."
11513	Informational	"Console (%1): Replica for virtual tape %2 was added to VTL Server %3 (watermark: %4 MB, time: %5, interval: %6, watermark retry: %7, suspended: %8)."
11514	Error	"Console (%1): Failed to remove the replica for virtual tape %2 from VTL Server %3 (watermark: %4 MB, time: %5, interval: %6, watermark retry: %7, suspended: %8)."
11515	Informational	"Console (%1): Replica for virtual tape %2 was removed from VTL Server %3 (watermark: %4 MB, time: %5, interval: %6, watermark retry: %7, suspended: %8)."
11516	Error	Console (%1): Failed to create the virtual tape replica %2.
11517	Informational	Console (%1): Virtual tape replica %2 was created.
11518	Error	Console (%1): Failed to start replication for virtual tape %2.
11519	Informational	Console (%1): Replication for virtual tape %2 started.
11520	Error	Console (%1): Failed to stop replication for virtual tape %2.
11521	Informational	Console (%1): Replication for virtual tape %2 stopped.
11522	Error	Console (%1): Failed to promote virtual tape replica %2 to a virtual tape.
11523	Informational	Console (%1): Virtual tape replica %2 promoted to a virtual tape.
11524	Error	Console (%1): Failed to run VTL Server X-Ray.
11525	Informational	Console (%1): VTL Server X-Ray has been run.
11530	Error	Console (%1): Failed to back up configuration files.
11531	Informational	Console (%1): Backed up Configuration files successfully.
11532	Error	Console (%1): Failed to restore configuration files.
11533	Informational	Console (%1): Restored VTL configuration files successfully.
11534	Error	Console (%1): Failed to reset the umap for virtual device %2.
11535	Error	"Console (%1): Failed to update the replication parameters for virtual tape %2 to VTL Server %3 (watermark: %4 MB, time: %5, interval: %6, watermark retry: %7, suspended: %8)."
11536	Informational	"Console (%1): Replication parameters for virtual tape %2 to VTL Server %3 updated (watermark: %4 MB, time: %5, interval: %6, watermark retry: %7, suspended: %8)."
11537	Error	Console (%1): Failed to claim physical device %2.
11538	Informational	Console (%1): Physical device %2 has been claimed.
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.

Trap	Severity	Message
11546	Error	Console (%1): Failed to mark the replication for virtual tape %2.
11547	Informational	Console (%1): Replication for virtual tape %2 is marked in sync.
11548	Error	Console (%1): Failed to determine if data was written to virtual device %2.
11549	Error	"Console (%1): Failed to set option ""%2 %3.""
11550	Informational	"Console (%1): Option ""%2 %3"" set."
11553	Error	Console (%1): Failed to get login user list.
11554	Error	Console (%1): Failed to set failover option <selfCheckInterval: %d sec>.
11555	Informational	Console (%1): Failover option <self check interval: %2 sec> has been set.
11560	Error	Console (%1): Failed to get licenses.
11561	Error	Console (%1): Failed to add license %2.
11562	Informational	Console (%1): License %2 added.
11563	Error	Console (%1): Failed to remove license %2.
11564	Informational	Console (%1): License %2 removed.
11565	Error	Console (%1): Failed to check licenses -- option mask %2.
11566	Error	"Console (%1): License conflict -- Number of CPU's available: %2, number of CPU's used: %3."
11567	Error	Console (%1): Failed to clean up failover server directory %2.
11568	Error	Console (%1): Failed to set (%2) I/O Core for failover -- Failed to create failover configuration.
11569	Error	Console (%1): Failed to set %2 to Fibre Channel mode %3.
11570	Informational	Console (%1): Set %2 to Fibre Channel mode %3.
11571	Error	Console (%1): Failed to assign Fibre Channel device %2 to %3 (rolled back).
11572	Error	Console (%1): Failed to assign Fibre Channel device %2 to %3 (not rolled back).
11573	Informational	Console (%1): Fibre Channel device %2 assigned to %3.
11574	Error	Console (%1): Failed to unassign Fibre Channel device %2 from %3 (rolled back) and returns %4.
11575	Error	Console (%1): Failed to unassign Fibre Channel device %2 from %3 (not rolled back) and returns %4.
11576	Informational	Console (%1): Fibre Channel device %2 unassigned from %3.
11577	Error	Console (%1): Failed to get Fibre Channel target information.
11578	Error	Console (%1): Failed to get Fibre Channel initiator information.
11579	Error	Console (%1): Failed to set %2 to Fibre Channel authentication mode %3.
11580	Informational	Console (%1): Set %2 Fibre Channel Properties.
11583	Informational	Console (%1): Failed to update Fibre Channel client (%2) WWPNs.
11584	Informational	Console (%1): Fibre Channel client (%2) WWPNs updated.
11585	Error	Console (%1): Failed to set Fibre Channel option %2.
11586	Informational	Console (%1): Set Fibre Channel option to %2.
11587	Error	Console (%1): Failed to demote virtual device %2 to a replica.
11588	Informational	Console (%1): Virtual device %2 demoted to a replica.
11589	Error	Authentication failed to connect to client %1 and returned %2.
11592	Error	Console (%1): Failed to sync replication status for virtual tape %2 to the new target server.

Trap	Severity	Message
11594	Error	Console (%1): Failed to set CallHome option %2.
11595	Informational	Console (%1): Set CallHome option to %2.
11596	Error	Console (%1): Failed to set hostedbackup option %2.
11597	Informational	Console (%1): Set hostedbackup option to %2.
11598	Informational	Console (%1): Failed to set hostedbackup option %2 because of conflicting adapter number %3.
11599	Informational	Console (%1): Set ndmp option to %2.
11616	Informational	Console (%1): Replication schedule for virtual tape %2 id %3 suspended.
11617	Informational	Console (%1): Replication schedule for virtual tape %2 id %3 resumed.
11632	Error	"Console (%1): Failed to set failover option on secondary server <heartbeatInterval: %2 sec, autoRecoveryInterval: %3 sec>."
11633	Error	"Console (%1): Failed to set failover option on secondary server <heartbeatInterval: %2 sec, autoRecoveryInterval: disabled>."
11634	Informational	"Console (%1): Failover option on secondary server <heartbeatInterval: %2 sec, autoRecoveryInterval: %3 sec> has been set."
11635	Informational	"Console (%1): Failover option on secondary server <heartbeatInterval: %2 sec, autoRecoveryInterval: disabled> has been set."
11648	Error	Failed to get inquiry string on SCSI device %1.
11649	Error	Failed to convert inquiry string on SCSI device %1.
11650	Error	Failed to get capacity size for SCSI device %1.
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.

Trap	Severity	Message
11699	Error	Console (%1): Failed to get port mapping for adapter no %2 persistent binding.
11702	Informational	VirtualTape Library Emulation option was enabled successfully.
11703	Informational	VirtualTape Library Emulation option was disabled successfully.
11704	Error	Console (%1): The configuration file update for %2 %3(s) was rolled back.
11705	Error	Console (%1): The disk partition update for %2 %3(s) was rolled back.
11706	Error	Console (%1): The device creation for %2 %3(s) was rolled back.
11707	Error	Console (%1): Failed to create %2 %3(s). Error: %4.
11708	Informational	Console (%1): %2 %3(s) created successfully.
11709	Error	Console (%1): The configuration file update for replication setup for %2 %3(s) was rolled back.
11710	Error	Console (%1): The disk partition update for replication setup for %2 %3(s) was rolled back.
11711	Error	Console (%1): The replication setup for %2 %3(s) was rolled back.
11712	Error	Console (%1): Failed to configure replication for %2 %3(s). Error: %4.
11713	Informational	Console (%1): Replication for %2 %3(s) configured successfully.
11714	Error	Console (%1): The configuration file update for replication removal for %2 %3(s) was rolled back.
11715	Error	Console (%1): The disk partition update for replication removal for %2 %3(s) was rolled back.
11716	Error	Console (%1): The replication removal for %2 %3(s) was rolled back.
11717	Error	Console (%1): Failed to remove replication for %2 %3(s). Error: %4.
11718	Informational	Console (%1): Replication for %2 %3(s) removed successfully.
11719	Error	Console (%1): The configuration file update for deleting %2 %3(s) was rolled back.
11720	Error	Console (%1): The disk partition update for deleting %2 %3(s) was rolled back.
11721	Error	Console (%1): The deletion of %2 %3(s) was rolled back.
11722	Error	Console (%1): Failed to delete %2 %3(s). Error: %4.
11723	Informational	Console (%1): %2 %3(s) are deleted successfully.
11724	Error	Console (%1): The configuration file update for promoting %2 %3(s) was rolled back.
11725	Error	Console (%1): The disk partition update for promoting %2 %3(s) was rolled back.
11726	Error	Console (%1): The promotion of %2 %3(s) was rolled back.
11727	Error	Console (%1): Failed to promote %2 %3(s). Error: %4.
11728	Informational	Console (%1): %2 %3(s) are promoted successfully.
11729	Error	Console (%1): Failed to update replication properties for %2 %3(s). Error: %4.
11730	Informational	Console (%1): Replication properties for %2 %3(s) are updated successfully.
11731	Error	Console (%1): Failed to update replica properties for %2 %3(s). Error: %4.
11732	Informational	Console (%1): Replica properties for %2 %3(s) are updated successfully.
11733	Informational	Console (%1): Virtual library %2 created successfully.
11734	Error	Console (%1): The configuration file update for virtual library creation was rolled back.
11735	Error	Console (%1): Adding virtual library to the system was rolled back.



---

Trap	Severity	Message
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.
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.

---

---

Trap	Severity	Message
12008	Error	Wrong file format %1.
12009	Error	Missing parameter %1.
12010	Error	Invalid parameter %1.
12011	Error	Wrong status for file %1.
13000	Informational	"VTL Failover Module started -- [Primary %1, IP %3, Heartbeat %4][Secondary %2] (HBInterval %5)(AutoRecovery %6)"
13001	Informational	The VTL Console has requested that this server take over for the primary server.
13002	Informational	Transferring primary static configuration to secondary.
13003	Informational	Transferring primary dynamic configuration to secondary.
13004	Informational	Transferring primary credential information to secondary.
13005	Informational	Taking over tasks for the primary server.
13006	Informational	The primary VTL Server is recovering.
13007	Informational	Restoring this server to its original configuration.
13008	Informational	VTL Failover Module stopped.
13009	Informational	Synchronizing the VTL configuration with the primary server.
13100	Error	fail to retrieve primary's heartbeat information.
13101	Error	Failed to communicate with primary. Error: %1
13102	Error	Failed to run %1.
13103	Informational	The system times of the failover pair differ by more than %1 second(s).
13300	Error	Failed to authenticate to the primary server -- Failover Module stopped.
13301	Error	Failed to authenticate to the local server -- Failover Module stopped.
13302	Error	Failed to transfer primary static configuration to secondary.
13303	Error	Failed to transfer primary dynamic configuration to secondary.
13304	Error	Failed to rename file %1.
13305	Error	Failed to write to file %1.
13306	Error	Failed to open file %1.
13307	Error	Failed to transfer primary credential information to secondary.
13308	Error	Invalid failover configuration detected. Failover will not occur.
13309	Error	Primary server failed to respond command from secondary. Error: %1.
13310	Error	Failed to copy from %1 to %2.
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.

---

Trap	Severity	Message
13500	Informational	VTL Self-Monitor Module started -- (%1)(%2)
13501	Informational	all VTL related processes and resources function normally
13502	Informational	Take back the virtual IP address: %1.
13503	Warning	No heartbeat request detected for %1 seconds.
13504	Informational	Stopping Self-Monitor module.
13600	Informational	Releasing virtual IP address: %1.
13700	Error	Failed to allocate memory -- Self-Monitor Module stopped.
13701	Error	Failed to release virtual IP address. Error: %1. Retrying the operation.
13702	Error	Failed to add virtual IP address: %1. Retrying the operation.
13703	Error	Failed to stop VTL Self-Monitor Module.
13704	Error	VTL module failure detected. Condition: %1.
13710	Warning	"The Live Trial period has expired for VTL Server %1. Please contact Sun Microsystems, Inc. or its representative to purchase a license."
13711	Warning	"The following options are not licensed: %1. Please contact Sun Microsystems, Inc. or its representative to purchase a license."
13800	Critical	Primary server failure detected. Failure condition: %1
13801	Informational	Secondary server will take over primary server operation.
13802	Informational	Manual failover initiated.
13803	Informational	Primary acknowledged takeover request. Resources are released.
13804	Informational	Quorum disk failed to release to secondary.
13805	Informational	Virtual drives released successfully.
13808	Informational	IP address released successfully.
13809	Informational	Failover completed successfully.
13810	Informational	Primary server restored. Waiting for failback.
13811	Informational	Primary server failback initiated.
13812	Informational	Server IP address add successfully.
13814	Informational	Quorum disk returned to primary.
13815	Informational	Virtual drives added successfully.
13816	Informational	Primary server restored.
13817	Critical	Primary server failback was unsuccessful. Failed to update the primary configuration.
13818	Error	Quorum disk negotiation failed.
13820	Warning	Failed to detect primary server heartbeat.
13821	Error	Failed to contact other entities in network. Assume failure in secondary side. Failover not initiated.
13822	Warning	Secondary will not take over because storage connectivity is not 100%.
13823	Warning	Primary failed to acknowledge takeover request in time. Secondary will take over forcefully.
13824	Informational	Environment variable ISFCFORPCTO set to %1
13825	Informational	Environment variable ISFOQUORUMREQ set to %1
13826	Informational	Environment variable ISFOQUORUMCON set to %1
13827	Error	Fail to stop quorum updating process. PID: %1. Maybe due to storage device or connection failure.

---

Trap	Severity	Message
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.
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

---

---

Trap	Severity	Message
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.
13878	Error	Primary server has invalid failover configuration.
13879	Critical	Secondary server detect kernel module failure, reboot machine may need.
15050	Error	Server ioctl call %1 failed on vdev id %2: Invalid Argument (EINVAL).
15051	Error	Server ioctl call %1 failed on vdev id %2: I/O error (EIO).
15052	Error	Server ioctl call %1 failed on vdev id %2: Not enough memory space (ENOMEM).
15053	Error	Server ioctl call %1 failed on vdev id %2: No space left on device (ENOSPC).
15054	Error	Server ioctl call %1 failed on vdev id %2: Already existed (EEXIST).
15055	Error	Server ioctl call %1 failed on vdev id %2: Device or resource is busy (EBUSY).
16001	Error	Console(%1): Converting file system failed: %2.
17001	Error	Rescan replica cannot proceed due to replication already in progress.
17002	Error	Rescan replica cannot proceed due to replication control area missing.
17003	Error	Rescan replica cannot proceed due to replication control area failure.
17004	Error	Replication cannot proceed due to replication control area failure.
17005	Error	Replication cannot proceed due to replication control area failure.
17006	Error	Rescan replica cannot proceed due to replication control area failure.
17007	Error	Rescan replica failed.
17008	Error	Replication failed.
17009	Error	Failed to start replica rescan.
17010	Error	Failed to start replication.
17011	Error	Rescan replica failed due to network transport error.
17012	Error	Replicating replica failed due to network transport error.
17013	Error	Rescan replica failed due to local disk error.
17014	Error	Replication failed due to local disk error.
17017	Error	Rescan replica failed due to replica failed with error.
17018	Error	Replication failed due to replica failed with error.
17019	Error	Replication control area exchange failed with error.
17020	Error	Replication failed with error.
19000	Informational	"The replication configuration has been created successfully. Primary Server: %1, Virtual Tape: %2, Target Server: %3, Virtual Tape Replica: %4."
19001	Informational	"The failover configuration has been created successfully. Primary Server: %1, Secondary Server: %2"

---

Trap	Severity	Message
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.
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.

---

Trap	Severity	Message
19208	Error	Console (%1): Failed to create key package %2.
19209	Informational	Console (%1): Key package %2 has been created successfully.
19210	Error	Console (%1): Failed to get key package information.
19211	Error	Console (%1): Failed to save keys from key package.
19212	Informational	Console (%1): %2 keys from key package have been saved successfully.
20000	Informational	SAN/IP driver started.
20001	Informational	SAN/IP driver stopped.
20002	Error	SAN/IP driver failed to initialize.
21000	Informational	SAN SCSI driver started.
21001	Informational	SAN SCSI driver stopped.
21002	Error	SAN SCSI driver failed to initialize.
21010	Warning	SAN SCSI received an abort request.
21011	Warning	SAN SCSI received a reset bus request for a special command.
21012	Warning	SAN SCSI received a reset bus request.
21013	Warning	SAN SCSI failed to send a SCSI command.
21014	Warning	SAN SCSI failed to receive a SCSI reply.
21015	Warning	SAN SCSI failed to attach to a virtual device.
21016	Warning	SAN SCSI failed to detach from a virtual device.
21017	Warning	SAN SCSI failed to connect to a VTL Server.
21018	Warning	"SAN SCSI received a disconnect request. This may be from the Client Monitor or due to a network failure, VTL Server shutdown/failover, or a change in a virtual device."
21019	Warning	SAN SCSI received an unsupported request.
22000	Informational	Fibre Channel Authentication started with %1.
22001	Error	"Fibre Channel Authentication error %1, at %2."
22002	Informational	Fibre Channel Authentication stopped with %1.
22003	Warning	Fibre Channel Authentication warning from system %1.
22004	Error	Fibre Channel Authentication error. Client Name does not match on Server %1.
22005	Error	Fibre Channel Authentication error. Signature does not match on Server %1.
25000	Informational	%1 started.
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.

---

Trap	Severity	Message
25012	Error	Failed to open service -- %1.
26000	Error	Failed to create TCP socket.
26001	Error	Failed to bind TCP socket.
26002	Error	Failed to create TCP service.
26003	Error	Failed to create TCP thread.
26100	Error	Failed to access the %1 driver -- %2.
26101	Error	The SAN SCSI driver is the wrong version for this VTL SAN Client. Driver version %1 will not work with client version %2.
26102	Error	Failed to open the %1 driver -- %2.
26103	Error	Failed to start the %1 driver.
26104	Error	Failed to stop the %1 driver.
26105	Error	SAN SCSI cannot connect to VTL Server %1 -- %2.
26106	Error	SAN SCSI cannot attach to VTL SAN device %1/%2 -- %3.
26107	Error	SAN SCSI cannot detach from VTL SAN device %1/%2 -- %3.
26108	Error	SAN SCSI cannot disconnect from VTL Server %1 -- %2.
26110	Error	Failed to rescan SCSI port %1 -- %2.
26200	Error	Failed to access '%1' -- %2.
26201	Error	Failed to read the drive layout for '%1' -- %2.
26202	Error	Failed to assign drive %1 to drive letter %2. It is already in use.
26203	Error	Failed to access drive %1 -- %2.
26204	Error	Failed to dismount drive %1 -- %2.
26205	Error	Failed to lock drive %1 -- %2.
26206	Error	Failed to unlock drive %1 -- %2.
26207	Error	Failed to define device %1 -- %2.
26208	Error	Failed to undefine device %1 -- %2.
26209	Error	Drive %1 is busy and cannot be detached. The SAN Client cannot stop at this time.
26210	Informational	Both %1 and %2 have the same disk signature (%3).
27000	Error	Failed to connect to VTL Server '%1' -- %2.
27001	Error	Failed to get the version of VTL Server '%1' -- %2.
27002	Error	Failed to get the information for VTL Server '%1' -- %2.
27003	Error	Failed to get the number of adapters for VTL Server '%1' -- %2.
27004	Error	Failed to get the information for VTL Server '%1' adapter %3 -- %2.
27005	Error	Failed to get the number of devices for VTL Server '%1' -- %2.
27006	Error	Failed to get the information for VTL Server '%1' device %3 -- %2.
27007	Error	Failed to get the list of IP addresses for VTL Server '%1' -- %2.
27008	Error	Failed to get the media information for VTL Server '%1' device %3 -- %2.
28001	Error	Failed to add VTL Server '%1' -- %2.
28002	Error	Failed to add VTL Server '%1' adapter %2 -- %3.
28003	Error	Failed to add VTL Server '%1' adapter %2 channel %3 -- %4.
28004	Error	Failed to add VTL Server '%1' device %2 -- %3.



Trap	Severity	Message
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"
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"

Trap	Severity	Message
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]"
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

Trap	Severity	Message
40068	Error	Cannot create new Tape. EC %1
40069	Error	Cannot expand Tape %1. EC %2
40070	Error	Cannot delete Tape %1
40071	Error	"Cannot import Tape, dest slot %1 in Virtual Library %2 is full"
40072	Informational	"Properties of Tape %1 has been changed. Barcode %2, MaxCapacity %3 MB"
40073	Informational	"Tape Created in Stand Alone Virtual Tape Drive. Tape VID %1, Drive VID %2"
40074	Error	"Export to Physical Tape failed. Job ID %1, EC %2, SrcTape [%3] DestTape [%4]"
40075	Informational	"Export Job %1 submitted to Physical stand alone Tape Drive %2, SrcTape [%3], %4"
40076	Error	"Import Physical Tape failed. Job ID %1, EC %2, SrcTape [%3] DestTape [%4]"
40077	Error	Import Physical Tape failed. Duplicate Virtual Tape Barcode. Job ID %1 DestTape [%2]
40078	Error	Import Physical Tape failed. Duplicate Virtual Tape Barcode. Dest Tape [%1]
40079	Informational	"Deleted tape marked for delayed deletion. Tape [%1], VID %2"
40080	Warning	Tape drive %1 in physical library %2 not accessible. Locked by other party
40081	Warning	Tape [%1] in physical library %2 not accessible. Locked by other party
40082	Warning	Slot %1 in physical library %2 not accessible. Locked by other party
40083	Warning	Inventory physical library %1: Tape [%2] or Slot %3 not accessible. Locked by other party
40084	Warning	Tape [%1] is blank. Cannot export blank tapes
40085	Error	Reverse block command failed on physical tape drive VID %1 Error [%2]
40087	Error	Error in retrieving the hostname of this VTL server. Error: %1
40088	Error	Failure in looking up the IP address of the VTL server (%1). Please verify that DNS is configured correctly for both ACSLS and VTL server. Error: %2
40089	Error	Out of system resources. Could'nt fork a process. Error: %1
40090	Error	Failed to execute a program. Error: %1
40091	Error	Failed to open %1. Error: %2
40092	Error	DNS configuration for VTL server is incorrect. DNS or /etc/hosts is returning %1 as the IP of VTL server (%2)
40093	Error	Failed to successfully query %1 server with IP %2. Error received: %3.
40094	Error	Waited %1 seconds to get a response to a query from %2 (%3). Timing out.
40095	Error	Failed to mount %1 on drive %2. Error from %3 (%4): %5.
40096	Error	Waited %1 seconds to get a response from %2 (%3) after trying to mount %4 on drive %5. Timing out.
40097	Error	Failed to dismount %1 from drive %2. Error from %3 (%4): %5.
40098	Error	Waited %1 seconds to get a response from %2 (%3) after trying to dismount %4 from drive %5. Timing out.
40099	Error	Failed to retrieve drive information in ACS %1. Error from %2 (%3): %4.
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.

Trap	Severity	Message
40103	Error	Failed to retrieve LSM information in ACS %1. Error from %2 (%3): %4.
40104	Error	Waited %1 seconds to get a response from %2 (%3) after trying to retrieve LSM information in ACS %4. Timing out.
40105	Error	%1: The number of drives %2 is more than max supported (%3).
40106	Error	%1: The number of volumes %2 is more than max supported (%3).
40107	Informational	%1: Successfully mounted %2 on drive %3
40108	Informational	%1: Successfully dismounted %2 from drive %3
40109	Error	"Log sense command to Physical device %1 failed. Pagecode %2, EC %3"
40110	Error	Failed to retrieve volume information in ACS %1. Error from %2 (%3): %4.
40111	Error	Waited %1 seconds to get a response from Library Station (%2) after trying to retrieve volume information in ACS %3. Timing out.
40112	Warning	Physical Tape %1 not available to start tape caching job. Waiting for tape...
40113	Warning	A Manual Export job is not allowed because tape <%1> has tape caching set.
40114	Warning	The export job is not allowed because physical tape [%1] in library [%2][%3] is being used by tape caching.
40115	Informational	Please add tapes.
40116	Error	Hardware compression failed. EC [ %1 ]
40117	Error	Hardware decompression failed. EC [ %1 ]
40118	Error	Software decompression of a block compressed using hardware failed. EC [ %1 ]
40119	Informational	Global [%1] Compression %2 on Repository %3
40120	Warning	The tape [%1] has no data. No export job will be submitted.
40121	Warning	"The direct link tape VID %1, BarCode [%2] has been deleted."
40122	Informational	"Export Job %1 submitted to Physical Library %2. SrcTape [%3], DestTape [%4], DestSlot [%5], %6"
40123	Error	"Failed to load tape because it is a cleaning tape. Lib VID %1, Drive VID %2, BC %3"
40124	Error	Write command to Configuration Repository Failed. Please check repository LUNs
40125	Informational	Disk space allocated for tape VID %1 Barcode [%2] in library VID %3 has been reclaimed successfully
40126	Error	Failed to reclaim the tape VID %1 Barcode [%2] in library VID %3.
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].

---

<b>Trap</b>	<b>Severity</b>	<b>Message</b>
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

---

# Troubleshooting

---

## General Console operations

### *The VTL Console is unable to connect to a VTL server*

There are several operations that occur when the Console connects to the server. A dialog indicates the current step. If there is a failure, the word *Failed* appears at the end of the step. Determining the current phase of connection can help you pinpoint the problem. It is also possible that the server is busy. Wait for a while and retry. At what step did the connection fail?

- **Connecting to the VTL server** - If the IP address of the server has recently changed, delete the server from the Console and re-add it. If you entered a server name, try entering its IP address instead. If this does not help or if the IP address has not changed, ping the target machine.

If ping does not reply, ping other machines in the same subnet. If there is still no response, there is a network problem. Run a network command or utility to show the status of the network.

- **Verifying user name and password** - Check the user name and the password. You may use the root password or any other administrator or read-only user that you have created with VTL previously. Make sure the user name and password exist on the server by opening a local session. The password is case-sensitive. Make sure the *Caps Lock* key is not pressed on the keyboard.

From the machine where VTL Console is installed open a SSH session to the VTL server. Log on to the server with the same user name and password. If the connection between the two machines is fine, the Console should be able to connect to the server unless some important server module is not running, such as the communication module. To see the status of all modules, at the machine where VTL server is running, go to the system console and type: `vtl status`.

If a module has stopped, restart it with the command:

```
vtl restart <module name>
```

Afterwards, go back to the Console and retry connecting to the server.

- **Retrieving the server configuration** - If there is something wrong with the configuration, an error message may appear. Contact technical support.
- **Checking the VTL license** - Contact technical support.
- **Expanding the VTL server node** - This may be due to high memory usage. Check the memory consumption on the machine. If it is very high, stop all unnecessary processes. If the problem persists or if the memory consumption is normal, contact technical support.

---

## *Requested operations cannot be performed from the Console*

### Check server activity

Sometimes the VTL server is very busy with operations that cause high CPU utilization (such as expanding tapes or data *compression*).

You can check the Event Log or syslog (`/var/adm/messages`) for messages that show you the current activity of the system.

If you see messages such as *Server Busy* or *RPC Timeout*, you should wait awhile and retry your action after the current operation finishes.

If the problem persists or the server is not really busy, contact technical support.

## *Console operations are very slow*

### Check Console machine memory usage

On the machine where you are using the VTL Console, use the appropriate system utility (such as Task Manager) to show the memory usage of all running processes. If the memory usage is unusual, stop all unnecessary processes from running or provide more memory.

### Check server activity

Sometimes the VTL server is very busy performing heavy processing. You can check the Event Log or syslog (`/var/adm/messages`) for excessive pending SCSI commands on a single SCSI queue that may delay update requests coming from the Console. Also, try starting a second instance of the Console. If the second Console cannot establish connections, that means the server is busy with previous RPC operations.

If this is the case, you should wait awhile and retry your action after the current processing finishes.

If the problem persists or the server is not really busy, contact technical support.

---

## Physical resources

### *The VTL Console does not show physical storage devices as expected*

There are several steps to try when physical storage devices have been connected/assigned to the VTL server yet they are not showing in the VTL Console.

- |                           |  |
|---------------------------|--|
| Rescan devices            | Perform a rescan from the VTL Console (right-click on the <i>Physical Resources</i> object and select <i>Rescan</i> ). Make sure that the <i>Discover New Devices</i> option is specified. By default, Solaris rescans all adapters.   |
| Check system log messages | Check the Event Log or syslog ( <code>/var/adm/messages</code> ) for error messages that may correspond to the rescan operation and report failures on SCSI devices. It may be that even though the devices were discovered, they were not accessible due to errors.   |
| Check device type         | For external <b>SCSI devices</b> , make sure you check the following: <ul style="list-style-type: none"><li>• Make sure the system is powered on. Perform a power cycle to make sure.</li><li>• Physically make sure all the cable connectors are securely plugged in.</li><li>• Verify SCSI termination. This can be quite involved. If you are not sure, you may have to contact the manufacturer of the devices and have their representatives assist with the troubleshooting.</li></ul> |

Once the above conditions are verified, determine the SCSI HBA and the proper driver for it. This can normally be accomplished by going to the website of the HBA manufacturer. From the server console, make sure the correct driver for the HBA is loaded properly. If not sure, unload and load the driver again. While doing that, look into the syslog to see if any error messages have been logged corresponding to the action of loading the driver. Under some circumstances, the system may need to be power cycled (not just rebooted) to properly load the drive.

Some **Fibre Channel devices** use VSA (Volume Set Addressing) mode. This addressing method is used primarily for addressing virtual buses, targets, and LUNs. If this is the case, make sure to enable VSA on the VTL initiator driver and use persistent binding. Otherwise, VTL cannot manage the storage.

### *Client does not see any devices*

When using a Mutli-ID HBA with dual mode, clients will need to be zoned to the *alias* port. If they are zoned to the *base* port, clients will not see any devices for you to assign. To correct this problem, check the zoning.




---

## Logical resources

### *Virtual tapes are displayed as "offline" on the Console*

If a physical resource that was used to create the virtual tape is missing, the tape's status will be offline (missing segment).

From the VTL Console determine which physical resources comprise this virtual drive. To do this, highlight the tape in the tree and check the *Layout* tab or look under the *Storage Devices* object for the  icon. For each physical device, check that:

- It is turned on
- It still exists (has not been removed)
- It is in a normal state and does not show any failure
- There is no failure at the connection level. Check FC connectivity to VTL to make sure that each physical resource is accessible.

### *Tape expansion does not work*

**Check device size** Highlight the tape in the Console and check that the *Total Size* field shows the correct size of the expanded tape device.

**Correct size - check client os** If the Console shows the correct size of the expanded virtual tape, the expansion has succeeded but the client machine is having trouble seeing the new size.

Make sure the client machine has been refreshed to see the updated status of its drives. You need to run the utility corresponding to your operating system to rescan the device and discover its new size.

Once the operating system has recognized the new space on the virtual disk, the file system or the application on the device has to be expanded also. If the file system or the application supports expansion, use the corresponding utility to expand it.

- *Windows NT clients* - You must restart your Windows NT client after expanding a virtual device in order for the expanded area to become available.
- *Windows 2000 clients* - Go to Windows Disk Management. If it does not show any unallocated space at the end of the virtual device, you must run a "Rescan Disks" command from the Disk Management GUI in order to discover changes to disk size.
- *Windows 2000 Dynamic Disks* - Expansion of dynamic disks using the Expand SAN Resource Wizard is not supported for clients. Due to the nature of dynamic disks, it is not safe to alter the size of the virtual device. However, dynamic disks do provide an alternative method to extend the dynamic volume:
  1. Create a new SAN Resource and assign it to the VTL client. This additional disk which will be used to extend the dynamic volume.
  2. Use Disk Manager to write the disk signature and upgrade the disk to "Dynamic".

---

3. Use Disk Manager to extend the dynamic volume. The new SAN Resource should be available in the list box of the Dynamic Disk expansion dialog.

- *Solaris clients* - Label the disk with the new geometry using the utility `$IPSTORCLIENT/bin/labeldisk`.
- *AIX clients* - Expanding a virtual disk will not change the size of the existing AIX volume group. To expand the volume group, a new disk has to be assigned and the `extendvg` command has to be used to enlarge the size of the volume group.
- *Linux clients* - On the client machine's system console, type `rmmod FC HBA driver` and `insmod FC HBA driver`. This unloads and reloads the driver for the FC HBA and causes Linux to rescan all devices on that HBA, allowing it to recognize any new device size. If this method is not feasible, such as when the boot disk is running on the FC HBA, contact technical support.

Incorrect size -  
check Event  
Log

If the Console does not show the correct size of the expanded virtual tape, the expansion was probably not successful. Check the Event Log to look for any error messages regarding the expansion. Errors may appear if:

- There is not enough physical disk space for the expansion. Add more physical storage or change the size of expansion.
- The physical partition is invalid. Check the storage device.
- An IO error occurred.
- An RPC timeout occurred when the expand command was issued. Try the following operation to see if the server is busy:
  - On the VTL server, run the command `top` or `ps -x`
  - Find and stop any unnecessary processes. If you find that the server is too busy, wait to see if the problem persists.

If it is possible to correct the problem, try to do so and then expand the virtual tape again. If it still does not work or if the Event Log does not show any errors relating to the expansion, contact technical support.

---

## Client cannot see tape library/drive as provisioned by VTL

Check device discovery by os

Check if the client's operating system sees the device or if it is the backup software that does not see the tape library or drive. Depending on the OS, the new device is indicated in the different ways:

- **Windows** - Tape libraries appear under *Medium Changers* and tape drives under *Tape drives*. Usually the tape drive is indicated as `ltape<index>`.
- **Linux** - The tape library is usually indicated by `/dev/sg<index>` (the `sg` module should be loaded) and the tape drive by `/dev/st/<index>`, `/dev/nst/<index>`, and `/dev/sg/<index>` (The `st` module should be loaded).
- **Solaris** - The tape library is usually indicated by `/dev/sg<index>` (the `sg` module should be loaded) and the tape drive by `/dev/rmt/<index>` (the `st` module should be loaded).
- **HP-UX** - The tape library is usually indicated by `/dev/rac/cXtXdX` (the `schgr` driver must be loaded) and the tape drive by `/dev/rmt/<index>` (the `stape` driver should be loaded).
- **AIX** - The tape device is usually indicated by `/dev/rmt<index>` (for LTO1/LTO2) or `/dev/mt<index>` (for DLT/SDLT).

Operating system does not see device

If the operating system does not see the device, you need to troubleshoot virtual device discovery. To do this, in the Console, select the virtual device. Check the device status. If the device status is *offline*, that is the problem as clients cannot see an offline device. Refer to the ['Virtual tapes are displayed as "offline" on the Console'](#) section for more information.

If the device status is *online*, check the client configuration.

- **Check client assignment** - From the Console, right-click on the specific client. If you do not see virtual devices on the *Resources* tab, assign them to that client. To share a device between several clients the mode should be *Read/Write non-exclusive*, otherwise device attachment fails.
- **Check WWPN** - From the Console, right-click the client and select *Properties*. Record initiator and target WWPNs. Highlight the *Physical Resources* object and locate the HBA that matches the recorded target HBA WWPN. Highlight the *SNS table* tab for that HBA and look for the WWPN that matches the recorded initiator WWPN. If the WWPN is not correct, unassign the client and assign it again using the appropriate mapping type. If multiple HBAs exist, either from the client host or from the VTL target, look up all entries from all target SNS tables.
- **Check VSA addressing** - Some hosts use VSA (Volume Set Addressing) mode. This addressing method is used primarily for addressing virtual buses, targets, and LUNs. If this is the case, make sure to enable VSA on the VTL target driver. Otherwise some clients cannot detect more than eight LUNs on VTL virtual devices.

Operating system sees device

If the operating system sees the device but the **backup software does not see the device at all**, you need to check the drivers for the backup software. Make sure the driver used corresponds to the nature of the library and also the tape drive. Some

---

backup products recommend using specific versions of drivers. Refer to the backup software manual for such settings or any necessary upgrade. Also, make sure that multiple backup software is not installed on the same backup server as they may conflict with each other.

If the operating system sees the device but the **backup software does not see the device in the expected place**, you need to check serialization. VTL libraries support serialization. Serialization is the conversion of the content of an object into a sequential stream. It identifies the owner of each component, such as robot, slots, and tape drives. If the device appears in the backup software, but it is not attached to the expected component, it may be related to the serialization. Refer to your backup software manual for any patch or upgrade related to serialization on the backup software.

### *Client sees the tape library/drive but cannot access it*

Check device access by OS

Check if the client's operating system can access the device or if it is the backup software that cannot access the tape library or drive.

Depending on the OS you can use a raw device utility. Most of these tools work with tape drives; they are not capable of moving tapes into the drives. Even if some can move tapes, you need to know the exact address of the tape and the drive.

We recommend that you use the Console to put a tape in a drive before running these tools. Also, stop the backup software before you use these utilities:

- **Windows** - For IBM Ultrium devices you can use `ntutil`, a command line tool that can check the tape device.
- **Unix systems** - You can use the `mt` or `tar` commands to access the tape device, for example: `mt -f /dev/rmt/0 status`

OS cannot access device

If the operating system *cannot access* the device, you need to troubleshoot virtual device access.

- Go to the storage to verify that it is not in error or in an abnormal state. The assigned devices have to be in read/write mode.
- Check the Event Log or syslog (`/var/adm/messages`) for message indicating IO errors. Such messages usually begin with `log_scsi_error`.
- Check client driver - Go to the client machine and check the adapter driver version. It should be certified for use with VTL.

OS can access device

If the operating system *can access* the device, you need to troubleshoot the backup software. Verify that you have the correct drivers.

### *Client can no longer access the tape library/drive*

Client machines may lose device access if you switch between a Multi-ID HBA and a single-ID HBA. If this occurs, you should reboot the client machine.

---

## Import/Export

### *Import/Export does not work as expected*

**Check tape capacity mismatch** When you Import/export data between a physical tape device and a virtual device, you must make sure the tape devices are of the same type and the same capacity. If they do not have the same capacity, an end-of-media-hit condition occurs and import/export fails.

If data compression is used, make sure the *actual* capacity matches, not just the *compressed* capacity. Import/export will fail when the destination does not have enough space to hold uncompressed data coming from source.

**Check job status** Highlight the *Import/Export Queue* and search for a job related to this operation. The job appears in this queue only during its execution; once it is completed, it is no longer in the queue. If the job is in progress, wait until it is completed. If the job is not there and the import/export operation is not done, look at Console Event Log to see if there are any job failure messages.

**Check barcodes of virtual tapes** When you import data from a physical tape, make sure the virtual tapes have different barcodes. Otherwise, the import operation fails. Use the *Inventory* feature in the Console to get the updated bar codes and status from the physical library.

**Check physical tape library and device status** Make sure the physical tape library does not show any abnormal situation. For example, the tape drives may require cleaning or tapes may need to be moved to the proper location.

**Check element address on the physical library** 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.

For example, an import job cannot be executed and the physical library has two DLT 8000 drives with the following configuration:

```
Library SCSI ID: 1
Drive at element address 1200: SCSI ID 10
Drive at element address 1201: SCSI ID 09
```

```
VTL Resources:
ABC-00003
DLT8000-0008: SCSI ID 09
DLT8000-0009: SCSI ID 10
```

In this case you need to unassign tape drives, select first DLT8000-0009, assign it, then select DLT8000-0008, and assign it to the physical library ABC-00003.

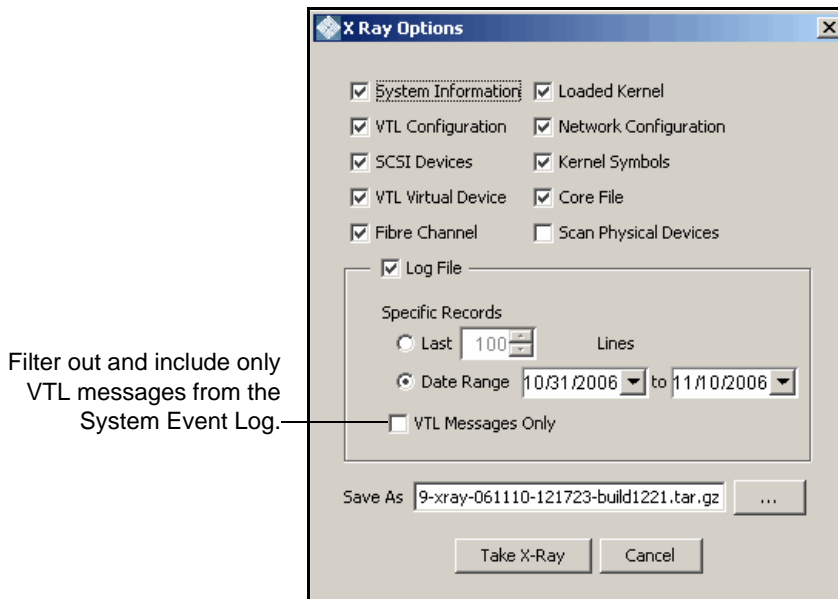
**Check system log for errors** Check the Event Log or syslog (*/var/adm/messages*). Look for error messages relating to the physical tape library or drive. If you find error messages but cannot find the cause, contact technical support.

## Take an X-ray of your system for technical support

Taking an X-ray of your system is useful for your technical support team to help solve system problems. 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.

To create an X-ray file:

1. In the Console, right-click on your VTL server and select *X-Ray*.



2. Based on the discussion with your Technical Support representative, select the options you want to include and set the file name.
3. Click the *Take X-Ray* button.

# Index

---

## A

### ACSLS

- Add/remove tapes 146
- Configure VTL and ACSLS 145
- Hardware configuration 145
- Overview 144

### Activity Log 56

### Administrator

- Management 49

### Alias 58

### Assign physical tape libraries

- Command line 189

### Attention required tab 55

### Auto archive 19, 34

### Auto expansion 22

### Auto replication 19, 85

### Automated Tape Caching 98

- Change policy 99
- Create cache for physical tapes 104
- Create policy 99
- Create virtual tapes 105
- Direct link tape 102
- Disable policy 103
- Encryption 105
- Force migration 105
- Global options 103
- Policy based triggers 101
- Reclaim disk space manually 105
- Reclamation triggers 102
- Recover data 107
- Renew cache 105
- Thresholds 103
- Time based triggers 100

## B

### Backup server

- Device scan 29

## C

### Cache 98

### CLI

- commands
  - network and serial port 210

### Client 5, 14, 243

- Add 27
- HBA settings 121
- iSCSI 133

VTL Plus 2.0 (Update 2) User Guide • July 2009 • 96267 • Rev HH

### NetWare

- QLogic driver 120

### COD

- Virtual tapes 22

### Command line

- Commands 154
- Common arguments 155
- Event Log 200
- Export tape 177
- Import tape 177
- Login/logout 156
- Physical devices 187
- Remote copy 181
- Usage 154
- Virtual devices-client 157
- X-ray 201

### Components 5

### Compression

- Disable 51
- Enable 51
- Virtual tape drive 51

### Configuration

- Planning 1

### Connect

- VTL appliance 205

### Console 5, 238

- Administrator Management 49
- Connect to server after failover 67
- Installation 204
  - Windows NT, XP, or 2000 205
- Launch 11, 13, 206
- Log 49
- Overview 10
- Pre-installation 204
- Rescan devices 16
- Server
  - Properties 56

### Copy mode 30

### Create 99

## D

### Database 14

### Deployment

- Advanced configuration 3
- Automated Tape Caching configuration 4
- Planning 1
- Standard configuration 2

- 
- Device scan 29
  - Devices
    - Rescan 16
  - Direct access mode 30
  - Direct access tapes 30
  - Direct link tape 102
  - Disaster recovery
    - Failover server 73
    - Replication 87
  - Duplicate tapes 20
  - E**
  - Email Alerts 147
    - Configuration 147
    - Message severity 151
    - Modifying properties 151
    - System log check 150
    - Triggers 149, 152
      - Customize email 152
      - New script 152
      - Output 153
      - Return codes 153
      - Sample script 153
  - Encryption
    - Cached tapes 105
  - Event Log 53, 200
    - Export 54
    - Filter information 54
    - Print 54
    - Sort information 54
  - Export to tape 32
    - Auto archive 34
    - Command line 178
    - Manually 32
    - Stacking 36
  - F**
  - Failover 58
    - And Mirroring 47
    - Assign clients to secondary server 72
    - Auto recovery 61
    - Connect to primary after failover 67
    - Disaster recovery 73
    - Fibre Channel port behavior 78
    - Force a takeover 73
    - Heartbeat monitor 59
    - Intervals 72
    - IP address behavior 80
    - Manually initiate a recovery 73
    - Primary/secondary servers 61
    - Rebuild primary 73
    - Recovery 61
    - Remove configuration 75
    - Replication note 96
    - Requirements 63
    - Resuming backups after failover/failback 76
    - Self-monitor 59
    - Server changes 72
    - Server failure 59
    - Setup 66
    - Status 71
    - Storage device failure 59
    - Storage device path failure 58
    - Suspend/resume 73
    - Terminology 61
  - Fibre Channel Target Mode 109
    - Client HBA settings 121
      - AIX 122
      - HP-UX 122
      - Linux 122
      - NetWare 123
      - Solaris 123
      - Windows 121
    - Data rate 119
    - Fabric topology 120
    - fshba.conf
      - Device identification 118
    - Hardware configuration 120
      - Server 111
    - Initiator mode 129
    - Installation and configuration 110
    - Link speed 118
    - Multi-ID
      - Ports 129
    - NetWare clients
      - QLogic driver 120
    - Persistent binding 114
      - Clients 121
    - Ports 111
    - qla2x00fs.conf 118
    - QLogic configuration 115
    - QLogic ports 129
    - Server HBA settings 115
    - Switches 112
      - Configure for failover 113
      - Configure for hard zoning 113
      - Configure for soft zoning 113
    - Target mode 129



---

- Target port binding 114
- Zoning 111

## H

- HBA
  - Multi-ID 117

## I

- Icons 15
- ILOM
  - command reference 210
- Import disk
  - Command line 191
- Import tape 30
  - Command line 177
- Import/export 245
- Import/export queue 13
- Installation
  - Console 204
- Introduction 1
- Inventory slots
  - Command line 187
- iSCSI Target Mode 133
- Initiators 133
- Linux
  - Add iSCSI client 139
  - Configuration 139
  - Create targets for iSCSI client 140
  - Log client onto target 141
  - Prepare iSCSI initiator 139
- Mobile client 140
- Stationary client 140
- Targets 133
- Windows
  - Configuration 134
  - Disable 138
  - Enable 134
  - Mobile client 27, 136
  - Requirements 134
  - Stationary client 136

## L

- Local Replication 87
- Logical resources 241
- Logs 49
  - Console 49

## M

- Messages

- SNMP 57

- Mirroring
  - And Failover 47
  - Fix minor disk failure 47
  - Remove configuration 47
  - Replace disk in active configuration 47
  - Replace failed disk 47
  - Status 46
  - Swap 47
- Multi-ID
  - HBA 117

## N

- NDMP backup 142
  - Configuration 142
- NetWare Client
  - QLogic driver 120

## O

- Offline tapes 241

## P

- Passwords
  - Add/delete administrator password 49
  - Change administrator password 49
- Patch
  - Apply 56
  - Rollback 56
- Path failure 58
- Persistent binding 114
  - Clients 121
- Physical device
  - Assign 29
- Physical resources 15, 240
  - Icons 15
- Physical tape
  - Stacking 36
- Physical tape database 14
- Physical tape drives 14
- Physical tape duplication 20
- Physical tape libraries 14
  - Command line 189
- Port Requirements 88
- Port swapping 81
- Ports 202, 207
- Pre-installation 6
- Prepare physical device
  - Command line 191

---

## Q

### QLogic

- Configuration 115
- Ports 129
- Target mode settings 115

## R

### Recovery

- Automated Tape Caching 107

### Recycle mode 30

### Remote copy 86

### Remote Replication 87

### Replica resources 14

### Replication 85, 87

- Change configuration options 96
- Failover note 96
- Force 96
- Local 87
- Policies 92
- Primary tape 87
- Promote 95
- Remote 87
- Remove configuration 96
- Replica resource 87
- Requirements 88
- Resume schedule 96
- Setup 89
- Start manually 96
- Status 94
- Stop in progress 96
- Suspend schedule 96

### Reports 14

- Create 15
- Export data 15
- View 15

### Rescan

- Command line 190
- Devices 16

### Round Robin Logic 25

## S

### SAN Client 14

- Add 27
- iSCSI 133

### SAN zoning for VTL systems 6

### SCSI

- Aliasing 58

### Search

- Tapes 13

### Secure tape option 38

### Security

- Ports 202, 207
- System 202, 207

### Server

- Properties 56

### Shred

- Virtual tapes 45

### SNMP 57

- Traps 56

### Software updates

- Add patch 56
- Rollback patch 56

### Stacking

- Virtual tapes 36

### Standalone tape drive

- Command line 164

### Storage device path failure 58

### Storage monitoring 56

### Sun VTL Operational Restrictions 5

## T

### Tape 99

### Tape capacity-on-demand 22

### Tape duplication 20

### Tape encryption keys 38

- Change 41
- Create 40
- Delete 41
- Export 42
- Import 43

### Tape expansion 241

### Tapes

- Command line 165, 166
- Move 166
- Search 13
- Stacking 36
- Write protect 13

### Target mode settings

- QLogic 115

### Target port binding 114

### Traps 57

### Troubleshooting 238, 240, 241, 243, 245, 246

## U

### Unassign physical tape libraries

- Command line 189

---

## **V**

- Virtual tape drives 13
  - Command line 162, 164
- Virtual tape libraries 13
  - Command line 161, 162
  - Create 17
- Virtual tapes
  - Create 23
  - How they are allocated 25
  - Shred 45
  - Stacking 36
- Virtual vault 13
- Volume set addressing 114
- VSA 114
- VTL appliance 5
  - Connect 205
- VTL failover
  - Backup server configuration 65
  - Best practices 65
  - Port swapping 81
- VTL info
  - Command line 175
- vtlconsole.log 49

## **W**

- World Wide Port Names 131
- Write
  - protection 13
- WWPN 131

## **X**

- X-ray 201
- Xray 246

## **Z**

- Zoning 111

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web [sun.com](http://sun.com)



ARGENTINA: 5411-4317-5636 • AUSTRALIA: 1-800-550-786 • AUSTRIA: 43-1-601-26-0 • BALKANS: 301-6188-111 • BELGIUM: 32-2-704 89 83 • BRAZIL: 55-11-51872100 • BRUNEI: 65-216-8333 • CANADA: 1-800-422-8020 (GENERAL); 416-964-2001 (LEARNING MANAGEMENT SYSTEM SALES, TORONTO) • CHILE: 562-372-4500 • COLOMBIA: 571-629-2323  
CZECH REPUBLIC: 420-2-33009311 • DENMARK: 45-4556-5040 • EGYPT: 00-202-570-9442 • FINLAND: 358-9-525-551 • FRANCE: 33-1-41-33-17-17 • GERMANY: 49-89-460-08-2788 • GREECE: 30-01-6188101 • HONG KONG: 852-2877-7077 • HUNGARY: 361-202-4415 • INDIA: 91-80-229-8989 • INDONESIA: 65-216-8333 • IRELAND: 353-1-668-4377  
ISRAEL: 972-9-9710500 • ITALY: 39-02-9259511 • JAPAN: 81-3-5779-1820 • KOREA: 82-2-3453-6602 • MALAYSIA: 603-2116-1887 • MIDDLE EAST: 00-9714-3366333 • MEXICO: 525-261-0344 • NETHERLANDS: 31-33-4515200 • NEW ZEALAND: 0800-786-338 • NORTH WEST AFRICA: 00-9714-3366333 • NORWAY: FROM NORWAY: 47-22023950, TO NORWAY: 47-23369650 • PAKISTAN: 00-9714-3366333 • PEOPLE'S REPUBLIC OF CHINA: 8610-6803-5588 • PHILIPPINES: 632-885-7867 • POLAND: 48-22-8747848 • PORTUGAL: 351-21-413-4000 • RUSSIA: 7-095-935-8411 • SAUDI ARABIA: 00-9714-3366333 • SINGAPORE: 65-216-8300 • SOUTH AFRICA: 27-11-256-6300 • SPAIN: 34-902-210-412 • SRI LANKA: 65-2168333 • SWEDEN: 46-8-631-22-00 • SWITZERLAND: 41-1-908-90-50 (GERMAN) 41-22-999-0444 (FRENCH) • TAIWAN: 886-2-25185735 • THAILAND: 662-344-6855 • TURKEY: 90-212-335-22-00 • UNITED KINGDOM: 44-1276-416-520 • UNITED STATES: 1-800-422-8020 • VENEZUELA: 582-905-3800 • VIETNAM: 65-216-8333 • WORLDWIDE HEADQUARTERS: 1-650-960-1300

**SUN™** THE NETWORK IS THE COMPUTER ©2006 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, and the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

